



Dominion® SX



ユーザ ガイド リリース 3.1

Copyright © 2007 Raritan, Inc.

DSX-0M-J

2007 年 4 月

255-60-2000-00

著作権と商標に関する情報

この文書には、著作権で保護されている固有の情報が含まれています。無断で転載することは禁じられています。この文書のどの部分も Raritan, Inc.より事前に書面による承諾を得ることなく複製、複製、他の言語へ翻訳することを禁じます。

© Copyright 2007 Raritan、CommandCenter、RaritanConsole、Dominion、Raritan 社のロゴは、Raritan, Inc.の商標です。無断で転載することは、禁じられています。Java は Sun Microsystems, Inc.の登録商標、Internet Explorer は Microsoft Corporation の登録商標です。Netscape および Netscape Navigator は Netscape Communication Corporation の登録商標です。すべての商標は各所有者の所有物です。

FCC 情報

この装置は試験済みであり、FCC 規則の Part 15 に規定された Class A デジタル装置の制限に準拠していることが証明されています。これらの制限は、商業環境に設置した場合に有害な干渉を防止するために規定されています。この装置は、無線周波数を生成、利用、および放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信に対して有害な干渉を引き起こす可能性があります。この装置を居住環境で使用した場合、有害な干渉を引き起こす可能性があります。

VCCI 情報(日本)

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan 社は、事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が関与しない範囲での使用や、通常の使用条件以外での使用による製品の故障について、一切の責任を負いません。



北米および南米におけるサポートは、次の Raritan テクニカル サポートまでご連絡ください。

電話 (732)764-8886、ファックス (732)764-8887、電子メール tech@raritan.com

米国東海岸時間の月曜日～金曜日の午前 8 時～午後 8 時に、
テクニカル サポートにご連絡ください。

その他の国でのサポートについては、このガイドの最終
ページにある各地域の Raritan までご連絡ください。

安全基準

ラリタン製品を安全にご利用いただき、重大な感電事故や機器の破損の可能性を避けるために、以下のことにご注意ください。

- 製品の構成には、2 線式の電源コードは使用しないでください。
- コンピュータやモニタの AC 電源コンセントの極性が合っていて、正しく接地されていることを確認してください。
- コンピュータとモニタの両方とも、接地されている電源コンセントのみを使用してください。
- バックアップ用の UPS を使用している場合、コンピュータ、モニタ、その他の装置には電源コンセントから電源を供給しないでください。

ラック マウント安全基準

ラック マウントが必要なラリタン製品を使用する場合、以下のことに注意してください。閉め切ったラック環境内の温度は室温より高くなる場合があります。装置で指定された最高動作温度を超えないようにしてください(「付録 A: 仕様」を参照してください)。

- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機械的荷重が均一になるように注意してください。
- 装置を電源に接続する際は、回路に過剰な電流が流れないように注意してください。
- すべての装置を正しく接地してください。特に、電源タップ(直接接続を除く)を分岐回路に接続する場合など、電源への接続には注意してください。

目次

まえがき	XV
対象	XV
規定	XV
略語	XV
注意事項	XVI
第 1 章: はじめに	1
Dominion SX の概要	1
製品の特長	2
総合的なコンソール管理	2
強力なセキュリティとユーザ認証	2
選択できる接続方法	2
シンプルな操作	3
パッケージの内容	3
第 2 章: インストール	5
インストールの前に	5
クライアントの設定	5
ハードウェアのインストール	6
初期設定用のための Dominion SX の物理的インストール	6
LED の状態	6
グラフィカル ユーザ インタフェース(GUI)を使用した初期設定	7
コマンドライン インタフェースを使用した初期設定	9
日付と時刻の設定	9
ネットワーク設定	10
第 3 章: ソフトウェアの初期設定	11
Dominion SX のソフトウェアの初期設定	11
日付と時刻の設定	12
ネットワーク設定	13
設置	14
LAN 接続	14
モデム接続(オプション)	14
第 4 章: ネットワーク設定とサービス	15
基本的なネットワークの設定方法	15
DSX への名前付け	15
DSX のネットワーク設定	15
検出ポートの変更	16
ネットワーク サービス設定	16
ネットワーク サービス設定の変更	17
モデム アクセスの設定	18
IP 転送と静的ルートの設定	18
IP 転送の有効化	18
新しい静的ルートの追加	19
静的ルートの削除	20
第 5 章: ユーザ プロファイルとユーザ グループ	21
ユーザ プロファイルの管理	21
ユーザ プロファイル リストの表示	21
ユーザ プロファイルの作成	22
ユーザ プロファイルの変更	23
ユーザ プロファイルの削除	23
ユーザ グループの管理	23
ユーザ グループ リストの表示	24
ユーザ グループの作成	24
ユーザ グループの変更	25
ユーザ グループの削除	25

第 6 章: リモート認証	27
RADIUS の設定.....	27
LDAP の設定.....	28
TACACS+ の設定.....	29
第 7 章: ポート設定とポート アクセス アプリケーション	31
ポート キーワード.....	31
ポート設定.....	32
ダイレクト ポート アクセス.....	33
匿名ポート アクセス.....	34
Raritan Serial Console.....	35
Java を使用する際の Raritan Serial Client の要件.....	35
Java Runtime Environment(JRE).....	35
Java アプレットとメモリに関する考慮事項.....	36
Raritan Serial Client インタフェース.....	38
エミュレータ.....	39
編集.....	45
ツール.....	46
チャット.....	47
ヘルプ.....	48
スタンドアロン Raritan Serial Console のインストール.....	49
スタンドアロン Raritan Serial Client の要件.....	49
Windows OS 変数の設定.....	50
Linux OS 変数の設定.....	53
UNIX OS 変数の設定.....	53
Windows へのスタンドアロン RSC のインストール.....	54
Windows システムにおける RSC の起動.....	55
Sun Solaris への RSC のインストール.....	56
Sun Solaris における RSC の起動.....	57
第 8 章: セキュリティ	59
セキュリティ設定.....	59
ログイン設定.....	60
ローカル認証.....	60
ログイン処理.....	60
強力なパスワード設定.....	61
Kerberos 設定.....	61
証明書.....	62
証明書署名リクエストの生成.....	62
ユーザ キーのインストール.....	63
ユーザ証明書のインストール.....	63
SSL クライアント証明書.....	64
クライアント証明書による認証の有効化.....	65
新しい信頼できる証明機関のインストール.....	65
ユーザが追加した証明機関の削除.....	65
証明機関の表示.....	65
クライアント証明書失効リスト(CRL)の管理.....	65
DSX への新しい証明書失効リストの追加.....	65
DSX からの証明書失効リストの削除.....	66
証明書失効リストの表示.....	66
バナー.....	66
セキュリティ プロファイル.....	67
セキュリティ プロファイルについて.....	67
セキュリティ プロファイルの選択.....	67
カスタム プロファイルの編集.....	68
ファイアウォール.....	69
ファイアウォールの有効化.....	69
IPTables ルールの追加.....	70

第 9 章: ログ	71
ローカル イベント ログの設定.....	71
イベント ログ ファイルの有効化.....	71
システム ログの有効化.....	71
ポート ログの有効化.....	72
入力ポート ログの設定.....	74
暗号化の設定.....	74
SMTP ログの設定.....	75
SMTP ログの有効化.....	75
新しい SMTP イベントの選択.....	76
SMTP ログのテスト.....	76
NFS ログの設定.....	77
SNMP ログの設定.....	77
SNMP ログの有効化.....	77
新しい SNMP 送信先の作成.....	78
第 10 章: メンテナンス	79
ローカル イベント ログの管理.....	79
ローカル イベント ログの表示.....	79
イベント ログのクリア.....	80
イベント ログの送信.....	80
設定レポートの表示.....	81
DSX のバックアップとリストア.....	81
DSX のバックアップ.....	81
DSX のリストア.....	82
DSX ファームウェアのアップグレード.....	83
現在のファームウェア バージョンの表示.....	83
ファームウェアのアップグレード.....	83
ファームウェアのアップグレード履歴の表示.....	85
DSX でのファクトリ リセットの実行.....	85
DSX のレポート.....	85
第 11 章: 診断	87
ネットワーク インフラストラクチャ ツール.....	87
アクティブなネットワーク インタフェースのステータス.....	87
ネットワーク統計.....	88
ホストへの ping.....	89
ホストへのトレース ルート.....	89
管理者ツール – プロセス ステータス.....	90
第 12 章: コマンドライン インタフェース	91
コマンドライン インタフェースの概要.....	91
CLI を使用した Dominion SX へのアクセス.....	94
Dominion SX への SSH 接続.....	94
Windows PC からの SSH アクセス.....	94
UNIX ワークステーションからの SSH アクセス.....	94
Dominion SX への Telnet 接続.....	95
Telnet の有効化.....	95
Windows PC からの Telnet アクセス.....	95
Dominion SX へのローカル ポート接続.....	96
ポート設定.....	96
接続.....	96
ローカル ポート パラメータの変更.....	96
ログイン.....	96
CLI の操作方法.....	98
コマンドのオートコンプリート.....	98
CLI 構文 – ヒントとショートカット.....	98
すべてのコマンドライン インタフェース レベルの共通コマンド.....	99
show コマンド.....	99

初期設定	100
パラメータの設定	100
日付と時刻の設定	100
ネットワーク パラメータの設定	101
CLI プロンプト	101
CLI コマンド	101
セキュリティに関する問題	102
ユーザとグループの設定	103
コマンドライン インタフェースの許可	103
ターゲット接続と CLI	104
ターゲットでのエミュレーションの設定	104
エスケープ シーケンスの設定	104
CLI を使用したポート共有	104
Dominion SX コンソール サーバの管理	105
設定コマンド	105
承認と認証(AA)サービスの設定	105
リモート サービス	105
LDAP 設定メニュー	106
RADIUS コマンド	107
TACACPLUS コマンド	107
イベントの設定	107
ログの設定	108
cleareventlog コマンド	108
eventlogfile コマンド	108
eventsyslog コマンド	109
nfsget コマンド	109
nfssetkey コマンド	109
portlog コマンド	110
sendeventlog コマンド	111
vieweventlog コマンド	112
モデムの設定	112
ネットワークの設定	114
ethernetfailover コマンド	115
interface コマンド	115
ipforwarding コマンド	116
name コマンド	116
ports コマンド	116
route コマンド	117
routeadd コマンド	117
routedelete コマンド	117
NFS の設定	118
ポートの設定	119
ports の設定メニュー	119
ports config コマンド	119
ports keywordadd コマンド	121
ports keyworddelete コマンド	121
サービスの設定	122
dpa コマンド	122
encryption コマンド	124
http コマンド	125
https コマンド	125
logout コマンド	125
lpa コマンド	126
ssh コマンド	126
telnet コマンド	127
SNMP の設定	127
SNMP add コマンド	127
SNMP delete コマンド	128
snmp コマンド	128
時間の設定	128
clock コマンド	129
ntp コマンド	129
timezonelist コマンド	130

ユーザの設定	130
addgroup コマンド	130
adduser コマンド	130
deletegroup コマンド	131
deleteuser コマンド	131
editgroup コマンド	132
edituser コマンド	132
groups コマンド	133
users コマンド	133
接続コマンド	133
診断コマンド	134
IPMI コマンド	134
IPMIDISCOVER	134
IPMITOOL	135
listports コマンド	137
メンテナンス コマンド	138
backup コマンド	138
cleareventlog コマンド	139
factoryreset コマンド	139
firmware コマンド	139
logoff コマンド	140
password コマンド	140
reboot コマンド	140
restore コマンド	141
sendeventlog コマンド	141
upgrade コマンド	142
upgradehistory コマンド	142
userlist コマンド	142
vieweventlog コマンド	142
セキュリティ コマンド	143
banner コマンド	143
ftpgetbanner コマンド	143
certificate コマンド メニュー	144
firewall コマンド	145
IPtables コマンド	145
kerberos コマンド	147
loginsettings コマンド	149
idletimeout コマンド	149
inactiveloginexpiry コマンド	149
invalidloginretries コマンド	149
localauth コマンド	150
lockoutperiod コマンド	150
singleloginperuser コマンド	151
strongpassword コマンド	151
unauthorizedportaccess コマンド	152
securityprofiles コマンド	152
profiledata コマンド	153
第 13 章: Intelligent Platform Management Interface	155
IPMI デバイスの検出	155
IPMI 設定	156
第 14 章: 電源制御	159
ポート電源の関連付け	159
ポート電源の関連付けの作成	159
ポート電源の関連付けの削除	160
電源タップの設定	160
電源の関連付けグループ	161
電源制御	162
電源の関連付け	162
電源タップの電源制御	163
電源タップのステータス	164

第 15 章: ユース ケース	165
ケース 1. Web ブラウザを介した DSX ファームウェアのアップグレード.....	165
ケース 2. SSH を介したダイレクト ポート アクセスの設定および使用.....	165
ケース 3. RSC を介した排他的書き込みアクセスの使用.....	166
ケース 4. LDAP の設定.....	166
ケース 5. 電源の関連付けグループの作成.....	166
ケース 6. DSX のファクトリ リセットの実行.....	167
ケース 7. DSX のユーザ プロファイルの管理.....	167
ケース 8. RSC を介した DSX のポート アクセスへのアクセス.....	167
ケース 9. ポート設定.....	168
ケース 10. SX ポートへの CLI/SSH 接続.....	169
付録 A: 仕様	171
Dominion SX のモデルおよび仕様.....	171
動作要件.....	173
ブラウザの要件(テスト済み対応ブラウザ).....	173
接続性.....	174
Dominion SX シリアル RJ-45 のピン配列.....	175
DB9F Nulling Serial Adapter のピン配列.....	175
DB9M Nulling Serial Adapter のピン配列.....	176
DB25F Nulling Serial Adapter のピン配列.....	176
DB25M Nulling Serial Adapter のピン配列.....	176
Dominion SX ターミナル ポート.....	177
Dominion SX16 および SX32 のターミナル ポート.....	178
付録 B: システム デフォルト	179
付録 C: 証明書	181
デフォルトの SX 証明機関の設定.....	181
IE ブラウザ用の CA ルートのインストール.....	181
証明書の受諾(セッション ベース).....	181
Internet Explorer への Dominion SX サーバ証明書のインストール.....	182
Internet Explorer での受諾済み証明書の削除.....	183
Netscape Navigator 用の Dominion SX サーバ証明書のインストール.....	183
証明書の受諾(セッションベース).....	184
Netscape Navigator への Dominion SX サーバ証明書のインストール.....	184
受諾した証明書の削除.....	184
サードパーティのルート証明書のインストール.....	185
Internet Explorer へのサードパーティのルート証明書のインストール.....	185
Netscape Navigator へのサードパーティのルート証明書のインストール.....	186
署名するサードパーティ CA の CSR の生成.....	186
SX へのサードパーティ証明書のインストール.....	187
SX へのクライアント ルート証明書のインストール.....	187
Internet Explorer へのクライアント証明書のインストール.....	187
付録 D: サーバ設定	189
Microsoft IAS RADIUS サーバ.....	189
IAS RADIUS サーバを使用するための Dominion SX の設定.....	189
IAS ポリシーの作成.....	190
Cisco ACS RADIUS サーバ.....	191
Cisco ACS サーバを使用するための Dominion SX の設定.....	191
Cisco ACS サーバの設定.....	192
TACACS+サーバ設定.....	193
CiscoSecure ACS.....	193
Active Directory.....	195

付録 E: モデム設定	197
クライアント ダイアルアップ ネットワークの設定	197
Windows NT のダイアルアップ ネットワーク設定	197
Windows 2000 のダイアルアップ ネットワーク設定	199
Windows XP のダイアルアップ ネットワーク設定	202
付録 F: トラブルシューティング	205
ページへのアクセス	205
ファイアウォール	206
ログイン	207
ポート アクセス	207
アップグレード	208
モデム	208

目次

図 1 Dominion SX16 本体.....	1
図 2 DSXA-32 の背面.....	6
図 3 証明書情報.....	7
図 4 DSX ログイン画面	8
図 5 Restricted Service Agreement(制限付きサービス契約)画面	8
図 6 Change Password(パスワードの変更)画面.....	8
図 7 オペレータ/監視者用の Dominion SX Port Access(ポート アクセス)画面	11
図 8 管理者用の Dominion SX Port Access(ポート アクセス)画面	11
図 9 Setup(セットアップ)画面.....	11
図 10 Date/Time Configuration(日付と時刻の設定)画面.....	12
図 11 Network Configuration(ネットワーク設定)画面.....	13
図 12 Network Basic Settings and Ports(ネットワーク基本設定とポート)画面	15
図 13 Network Service Settings(ネットワーク サービス設定).....	17
図 14 Modem Settings(モデム設定)画面	18
図 15 IP Forwarding(IP 転送)パネル.....	18
図 16 Static Routes List(静的ルート リスト).....	19
図 17 Static Route(静的ルート)画面	19
図 18 User List(ユーザ リスト)画面.....	21
図 19 New User(新規ユーザ)画面	22
図 20 Group List(グループ リスト)画面.....	24
図 21 New Group(新規グループ)画面	24
図 22 RADIUS パネル	27
図 23 [LDAP]パネル	28
図 24 TACACS+パネル.....	29
図 25 Port Keywords(ポート キーワード)画面	31
図 26 Port Configuration(ポート設定)画面.....	32
図 27 Edit Port(ポートの編集)画面.....	32
図 28 Direct Port Access Mode(ダイレクト ポート アクセス モード)フィールド	33
図 29 Port Access(ポート アクセス)画面.....	35
図 30 Java Runtime Settings 画面.....	36
図 31 Raritan Serial Client ウィンドウ	38
図 32 [エミュレータ]ドロップダウン メニュー	39
図 33 接続終了の警告	39
図 34 一般設定ウィンドウ.....	40
図 35 表示設定ウィンドウ.....	41
図 36 表示設定: GUI フォントのプロパティ	42
図 37 接続中のユーザー ウィンドウ.....	44
図 38 編集コマンド - テキストのコピー、貼り付け、すべて選択	45
図 39 ツール メニュー	46
図 40 ログの開始コマンド ウィンドウ	46
図 41 キー入力の送信.....	47
図 42 SecureChat コマンドとユーザ チャット ウィンドウ	48
図 43 バージョン情報ウィンドウの例.....	49
図 44 Windows OS: システムのプロパティ.....	50
図 45 Windows OS: 新しいシステム変数	51
図 46 Windows OS: システム変数の編集	52
図 47 Windows OS: CLASSPATH 変数	52

図 48 Sun Solaris の JRE バージョンの確認	53
図 49 Windows における RSC インストールの進捗状況画面	54
図 50 RSC の Windows ショートカット指定画面	55
図 51 スタンドアロン RSC ログイン画面	55
図 52 ポートに接続されたスタンドアロン RSC ウィンドウ	56
図 53 Security Settings(セキュリティ設定)画面	59
図 54 Login Settings(ログイン設定)画面	60
図 55 Kerberos 設定	61
図 56 証明書署名リクエスト	62
図 57 Install User Key(ユーザ キーのインストール)	63
図 58 Install User Certificate(ユーザ証明書のインストール)	63
図 59 SSL Client Certificate(SSL クライアント証明書)画面	64
図 60 Banner(バナー)画面	66
図 61 Security Profiles(セキュリティ プロファイル)	67
図 62 Edit Custom Security Profile(カスタム セキュリティ プロファイルの編集)画面	68
図 63 Firewall(ファイアウォール)画面	69
図 64 Event Log(イベント ログ)パネル	71
図 65 Event Log(イベント ログ)パネル	71
図 66 Port Logging(ポート ログ)パネル	72
図 67 サンプル出力ファイル	73
図 68 Input Port Logging(入力ポート ログ)パネル	74
図 69 Encryption(暗号化)パネル	74
図 70 SMTP Settings(SMTP 設定)パネル	75
図 71 New SMTP Event(新規 SMTP イベント)パネル	76
図 72 NFS Settings(NFS の設定)画面	77
図 73 SNMP Settings(SNMP 設定)パネル	78
図 74 SNMP Destination(SNMP 送信先)パネル	78
図 75 イベント ログ	79
図 76 Send Event Log(イベント ログの送信)画面	80
図 77 Backup(バックアップ)画面	81
図 78 Restore(リストア)画面	82
図 79 Firmware Version(ファームウェア バージョン)	83
図 80 Firmware Upgrade(ファームウェアのアップグレード)画面	84
図 81 Firmware Upgrade History(ファームウェアのアップグレード履歴)画面	85
図 82 Diagnostics(診断)画面	87
図 83 Active Network Interface Status(アクティブなネットワーク インタフェースのステータス)	87
図 84 Network Statistics(ネットワーク統計)	88
図 85 Ping Host(ホストへの Ping)	89
図 86 Trace Route to Host(ホストへのトレース ルート)	89
図 87 Process Status(プロセス ステータス)	90
図 88 管理者ログインのサンプル	97
図 89 オペレータまたは監視者ログインのサンプル	97
図 90 1 IPMI 画面	155
図 91 Discover IPMI Devices(IPMI デバイスの検出)画面	155
図 92 IPMI Configuration(IPMI 設定)	156
図 93 Port Power Association(ポート電源の関連付け)画面	159
図 94 Power Strip Configuration(電源タップ設定)画面	160
図 95 Power Association Groups(電源の関連付けグループ)画面	161

図 96 Power Control(電源制御).....	162
図 97 Associations Power Control(電源の関連付け).....	162
図 98 Power Strip Power Control(電源タップ電源制御).....	163
図 99 Power Strip Status(電源タップのステータス).....	164
図 100 TACACS+の Cisco ACS AAA クライアント.....	193
図 101 Cisco ACS インタフェース設定.....	194
図 102 TACACS+のプロパティ.....	194
図 103 TACACS+設定.....	195
図 104 ダイアルアップ ネットワーク画面.....	197
図 105 新しい電話帳のエントリ画面.....	198
図 106 ダイアルアップのセキュリティ表示.....	199
図 107 Windows 2000 ネットワークとダイアルアップ接続.....	199
図 108 ネットワーク接続の種類.....	200
図 109 デバイスの選択.....	200
図 110 ダイアルする電話番号.....	201
図 111 接続の利用範囲.....	201
図 112 ネットワーク接続の種類.....	202
図 113 デバイスの選択.....	202
図 114 インターネット接続.....	203
図 115 接続名.....	203
図 116 ダイアルする電話番号.....	204
図 117 インターネット アカウント情報.....	204

表目次

表 1 工場出荷時のデフォルト ネットワーク設定	5
表 2 Java 実行時のパラメータ	36
表 3 すべての CLI レベルの共通コマンド	99
表 4 使用可能な CLI コマンド	101
表 5 設定: 認証コマンド: ldap	105
表 6 ldap コマンド	106
表 7 設定: events コマンド	107
表 8 eventlogfile コマンド	108
表 9 eventsyslog コマンド	109
表 10 nfsget コマンド	109
表 11 nfssetkey コマンド	110
表 12 portlog コマンド	110
表 13 sendeventlog コマンド	111
表 14 設定: モデムコマンド	112
表 15 設定: network コマンド	114
表 16 interface コマンド	115
表 17 ipforwarding コマンド	116
表 18 name コマンド	116
表 19 ports コマンド	116
表 20 route コマンド	117
表 21 routeadd コマンド	117
表 22 routedelete コマンド	117
表 23 nfs コマンド	118
表 24 ポートの設定コマンド	119
表 25 ports keywordadd コマンド	121
表 26 ports keyworddelete コマンド	121
表 27 dpa コマンド	122
表 28 encryption コマンド	124
表 29 http コマンド	125
表 30 lpa コマンド	126
表 31 ssh コマンド	126
表 32 telnet コマンド	127
表 33 SNMP add コマンド	127
表 34 SNMP delete コマンド	128
表 35 snmp コマンド	128
表 36 clock コマンド	129
表 37 ntp コマンド	129
表 38 addgroup コマンド	130
表 39 adduser コマンド	130
表 40 deletegroup コマンド	131
表 41 deleteuser コマンド	131
表 42 editgroup コマンド	132
表 43 edituser コマンド	132
表 44 接続コマンド	133
表 45 診断コマンド	134
表 46 ipmidiscover コマンド	134
表 47 ipmitool コマンド	135

表 48 listports コマンド.....	137
表 49 backup コマンド.....	138
表 50 logoff コマンド.....	140
表 51 password コマンド.....	140
表 52 restore コマンド.....	141
表 53 sendeventlog コマンド.....	141
表 54 upgrade コマンド.....	142
表 55 banner コマンド.....	143
表 56 ftpgetbanner コマンド.....	143
表 57 certificate client コマンド.....	144
表 58 certificate server コマンド.....	144
表 59 firewall コマンド.....	145
表 60 iptables コマンド.....	145
表 61 kerberos コマンド オプション.....	147
表 62 loginsettings コマンド.....	149
表 63 inactiveloginexpiry コマンド.....	149
表 64 invalidloginretries コマンド.....	150
表 65 lockoutperiod コマンド.....	150
表 66 singleloginperuser コマンド.....	151
表 67 strongpassword コマンド.....	151
表 68 unauthorizedportaccess コマンド.....	152
表 69 securityprofiles コマンド.....	152
表 70 profiledata コマンド.....	153
表 71 Dominion SX の仕様.....	171
表 72 Dominion SX の外形寸法と重量.....	172
表 73 Dominion SX の動作要件.....	173
表 74 ブラウザの要件.....	173
表 75 接続性.....	174
表 76 Dominion SX RJ-45 のシリアル ピン配列とシグナル.....	175
表 77 DB9F Nulling Serial Adapter のピン配列.....	175
表 78 DB9M Nulling Serial Adapter のピン配列.....	176
表 79 DB25F Nulling Serial Adapter のピン配列.....	176
表 80 DB25M Nulling Serial Adapter のピン配列.....	176
表 81 Dominion SX ターミナル ポートのピン配列 - 1 番目のポート.....	177
表 82 Dominion SX ターミナル ポートのピン配列 - 2 番目のポート.....	177
表 83 Dominion SX16 および SX32 のターミナル ポートのピン配列.....	178
表 84 Dominion SX のシステム デフォルト.....	179
表 85 ポート アクセスの開始.....	180
表 86 ページへのアクセスに関するトラブルシューティング.....	205
表 87 ファイアウォールに関するトラブルシューティング.....	206
表 88 ログインに関するトラブルシューティング.....	207
表 89 ポート アクセスに関するトラブルシューティング.....	207
表 90 アップグレードに関するトラブルシューティング.....	208
表 91 モデムに関するトラブルシューティング.....	208

まえがき

『Dominion SX ユーザ ガイド』では、Dominion SX セキュア コンソール サーバの設置、セットアップおよび設定、ルータ、サーバ、スイッチ、VPN、および電源タップなどのデバイスへのアクセス、ユーザおよびセキュリティの管理、Dominion SX セキュア コンソール サーバの保守と診断に必要な情報について説明します。

対象

このガイドは主にインフラストラクチャの管理者、およびセキュア コンソール サーバなどのデバイスの導入や設定を行う担当者を対象に書かれています。その他に、Dominion SX を使用して他のデバイスにアクセスするオペレータや監視者の方にも役立つ内容が記載されています。

規定

このガイドで使用される規定は次のとおりです。

例	説明
/usr/local/java	等幅フォントの文字は、ファイル名、パス、ディレクトリ、または画面に表示される文字を表します。
Enter	太字の文字は、メニュー項目、キーワード、およびキーボードのキーを表します。
<ip アドレス>	等幅フォントの斜体文字は、コマンドでユーザが値を変更すべき箇所を表します。

略語

このガイドで使用される略語は次のとおりです。

略語	意味
AD	Active Directory(アクティブ ディレクトリ)
CC	Command Center(コマンド センター)
CLI	Command Line Interface(コマンドライン インタフェース)
CSC	Common Socket Connection(コモン ソケット コネクション)
DPA	Direct Port Access(ダイレクト ポート アクセス)
HTTP	Hypertext Transfer protocol(ハイパーテキスト転送プロトコル)
HTTPS	HTTP Secure(HTTP over SSL)(HTTP セキュア(HTTP オーバーSSL))
LAN	Local Area Network(ローカル エリア ネットワーク)
LDAP	Lightweight Directory Access Protocol(ライトウエイト ディレクトリ アクセス プロトコル)
LDAP/S	Lightweight Directory Access Protocol/Secure(ライトウエイト ディレクトリ アクセス プロトコル/セキュア)
NFS	Network File System(ネットワーク ファイル システム)
NTP	Network Time Protocol(ネットワーク タイム プロトコル)
PPP	Point to Point Protocol(ポイント ツー ポイント プロトコル)
RADIUS	Remote Authentication Dial In User Service(リモート認証ダイヤルイン ユーザ サービス)
RSC	Raritan Serial Console

略語	意味
SMTP	Simple Mail Transfer Protocol(簡易メール転送プロトコル)
SSH	Secure Shell(セキュア シェル)
SSL	Secure Sockets Layer Protocol(セキュア ソケット レイヤ プロトコル)
SNMP	Simple Network Management Protocol(簡易ネットワーク管理プロトコル)
TACACS+	Terminal Access Controller Access Control System(PLUS)(ターミナル アクセス コントローラ アクセス コントロール システム(PLUS))
TLS	Transport Layer Security(トランスポート レイヤ セキュリティ)
UTC	Universal Time Coordinated(協定世界時)
VLAN	Virtual Local Area Network(仮想ローカル エリア ネットワーク)
VPN	Virtual Private Network(仮想プライベート ネットワーク)

注意事項

重要: ユーザに影響を及ぼす可能性、故障の危険、および保証やサービス対象の条件から外れる可能性のある行動についての警告です。

注: 本文の内容を補足する一般的な情報です。

第 1 章: はじめに

Dominion SX の概要

Dominion SX シリーズはシリアルデバイス専用のリモートソリューションを提供いたします。LAN/WAN、インターネット、ダイヤルアップ モデム等のすべてのネットワーク デバイス経由で、便利でセキュアなリモート アクセスとコントロールを提供します。

Dominion SX には次のような特徴があります。

- ターゲット デバイスにソフトウェア エージェントをインストールすることなく、しかもネットワークに大きな負荷をかけないソリューションを提供します。
- シリアル ポート経由で、どのようなネットワーク デバイス(サーバ、ファイアウォール、ロード バランサ、など)とも接続し、Web ブラウザを使用してデバイスをリモートかつ安全に管理する機能を提供します。

Dominion SX は標準 1U 19 インチ ラックマウント シャーシに装着できる、完全に構成されたスタンドアロン製品です。



図 1 Dominion SX16 本体

製品の特長

総合的なコンソール管理

- リモート管理: 1 つの IP アドレスを使用するだけで、セキュア ソケット シェル(SSH)、Telnet、ローカル ポート、Web ブラウザから最大 48 までのターゲット デバイス(モデルによる)にアクセス、監視、管理、トラブルシューティングを行うことができます。
- ダイレクト ポート アクセス: ポート単位の TCP/IP アドレス、または 1 つの IP アドレスと TCP ポート番号を使用したダイレクト ポート アクセスを実現しています。
- 通知: 電子メール警告による通知メッセージを作成できます。
- 共同管理とトレーニング: 1 ポートあたり最大 10 人のユーザによる同時アクセスが可能です。
- SecureChat™: 他のセキュア ソケット レイヤ(SSL)ユーザへセキュアに「インスタント メッセージ」を送ります。また、デバイス管理、トラブルシューティング、トレーニング活動に活用できます。
- 履歴の入手: デバッグに役立つ最近のコンソール履歴を 256KB(64MB SDRAM の場合は 64KB、128MB SDRAM の場合は 256KB)の容量まで入手できます。
- VT100、VT220、VT 320、および ANSI ターミナル エミュレーションがサポートされます。
- 5,000 行のコピー ペースト バッファを使用可能です。
- ローカル ポート アクセス。
- SNMP トラップ。
- SYSLOG。
- ネットワーク ファイル システム(NFS)サーバにログを記録できます。
- 総合的な SNMP トラップ。
- キーワードでトリガされるポート アラート。
- 3 レベルのユーザ アクセス:
 - 管理者: コンソール ウィンドウへの読み書きのアクセス可能、本体の設定変更も可能。
 - オペレータ: コンソール ウィンドウへの読み書きのアクセス可能、本体の設定変更はできません(パスワードのみ変更可)。
 - 監視者: コンソール ウィンドウへ読み取り専用でアクセス可能。本体の設定変更はできません(パスワードのみ変更可)。

強力なセキュリティとユーザ認証

- SSHV2 をサポート。
- 暗号化によるセキュリティ: 128 ビットの SSL ハンドシェイク プロトコルおよび RC4 暗号化。
- ユーザ認証のセキュリティ: ローカル データベース、リモート認証。
- RADIUS、TACACS+、LDAP、LDAP(S)、Microsoft Active Directory、NTP をサポート。
- ユーザごとに定義され、インストール可能なセキュリティ認証をサポート。

選択できる接続方法

- モデム接続(オプション): ネットワークが故障したときのための緊急リモート アクセス用です。
- ターゲット デバイス接続: RJ45 ベースの CAT 5 ケーブル配線で簡単接続、また Raritan のシリアル ポート アダプタが使用可能です。
- 「クラッシュ カート」用ローカル アクセス。

シンプルな操作

- Telnet
- SSH
- ブラウザ ベースのインタフェース: 新しい GUI では、直感的にターゲット デバイスにアクセスできます(適切なボタンをクリックして目的のターゲット デバイスを選びます)。
- アップグレード: Command Center(CC)および SSH と統合された、FTP 経由での組み込みファームウェア アップグレード機能。

パッケージの内容

出荷時の Dominion SX には次のものが含まれています。

- Dominion SX 本体とラック マウント キット(ラック マウント キットは本体によってはオプションとなります。)
- Dominion SX のインストールおよび操作方法に関する情報が収められた『Raritan Dominion SX ユーザ ガイド』の CD-ROM
- 印刷版『Dominion SX クイック セットアップ ガイド』
- 電源コード
- リリース ノート
- 梱包リスト
- RJ45 ループバック プラグ
- 一部の本体には、DB9 ファクトリ リセット アダプタが付属(他の本体はリセット スイッチがあるためアダプタは不要)

空白ページ

第 2 章: インストール

Dominion SX をネットワークに初期インストールする方法には、次の 2 つがあります。

- VT100 または同等のシリアル ケーブルを使用する方法(ハイパーターミナルを搭載した PC など)。
- Ethernet を使用する方法(インストール用コンピュータで使用)。

このセクションでは、LAN 上で Dominion SX を使用する設定について必要な手順を説明しています。次の表に、Dominion SX の工場出荷時のデフォルト ネットワーク設定を示します。本体をネットワークに接続したら、これらのデフォルト設定を使用して、Dominion SX に対して通常の使用に合わせた設定を行うことができます。

表 1 工場出荷時のデフォルト ネットワーク設定

デフォルト ネットワーク設定	
インターネット アドレス(IP)	192.168.0.192
ゲートウェイ アドレス	192.168.0.192
サブネット マスク	255.255.255.0
CSC ポート アドレス	5000
CC 検出用ポート アドレス	5000
ユーザ名	admin(すべて小文字)
パスワード	raritan(すべて小文字)

インストールの前に

ターゲット サーバのシリアル コンソール、またはコンソール ポートのあるシリアル管理デバイスに接続する正しいケーブルが用意されていることを確認します。

次のセクションでは、Dominion SX の設定を完了するのに必要な情報について説明しています。設定手順を実行する前に、すべての必須設定情報を取得してください。不明確な情報がある場合は、担当のシステム管理者にお問い合わせください。

クライアントの設定

1. インストール用コンピュータの Web ブラウザの**プロキシ**を無効にします。
「no Proxies(プロキシなし)」を使用するか、プロキシが設定されていない URL のリストに **192.168.0.192** を一時的に追加します。
2. インストール用コンピュータの Web ブラウザで、**Java アプレットの実行**を有効にして、コンソール クライアント アプリケーション(RSC)を使用できるようにします。
3. 同一サブネット上にあるインストール用コンピュータの Web ブラウザで、アドレス/ロケーション フィールドに URL **https://192.168.0.192** を入力して本体にアクセスします。

ハードウェアのインストール

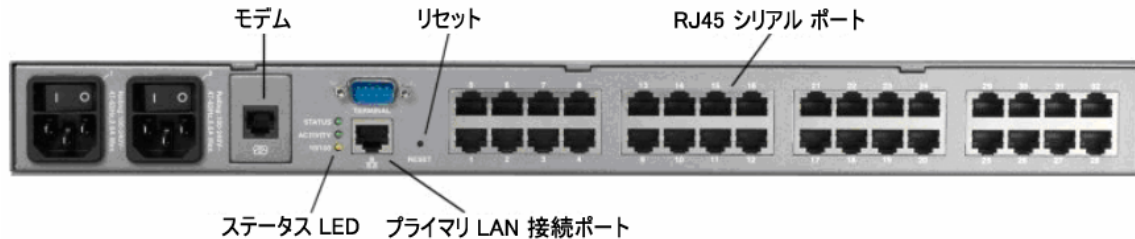


図 2 DSXA-32 の背面

初期設定用のための Dominion SX の物理的インストール

1. ネットワーク カードのついたコンピュータとクロスケーブルを使用します。このコンピュータは「インストール用コンピュータ」となります。
2. 本体を適切な方法で実装します。この本体はラック マウントが簡単にできるように設計されているので、ラック マウントを推奨しています。
3. クロス ネットワーク LAN ケーブルを、本体の後ろ側にあるプライマリ LAN 接続ポート(2 つの Ethernet インタフェースがあるモデルでは LAN 1)につなぎます。
4. ネットワーク LAN ケーブルのもう一方の端をインストール用コンピュータのネットワーク カードに接続します。
5. 外部電源コードのメス プラグを本体の後ろ側に接続します。
6. 外部電源コードのオス プラグを、電源供給コンセントに接続します。
7. Dominion SX 本体の電源を投入します。

注 本体はハードウェアとファームウェアのセルフテストを行い、その後ソフトウェアのブート シーケンスを開始します。ブート シーケンスは短時間で終了し、完了するとライトがつき、点灯の状態を維持します。

ハードウェアおよびファームウェアのセルフテストとソフトウェア ブート シーケンスが完了したら、次のセクションで説明するように、グラフィカル ユーザ インタフェース(GUI)またはコマンドライン インタフェース(CLI)を使用して初期設定タスクを実行します。

LED の状態

Dominion SX 本体の前面パネルにあるモデル名ラベルの右横に、LED インジケータがあります。次の 3 つの状況で、青色の LED インジケータが点滅します。

1. Ethernet パケットが送受信されているとき。
2. シリアル データが送受信されているとき。
3. watchdog タイマーが 0 にリセットされるとき。watchdog タイマーが一定の値に達して 0 にリセットされるときに、LED は周期的に点滅します。

グラフィカル ユーザ インタフェース(GUI)を使用した初期設定

グラフィカル ユーザ インタフェースから Dominion SX 本体を初期設定するには、以下の手順に従います。

ネットワーク アクセス

1. インストール用コンピュータで、192.168.0.192 へのルートが設定されており、IP アドレス 192.168.0.192 と通信可能であることを確認します。
2. Windows でルーティング テーブルを確認するには、インストール用コンピュータのコマンド ウィンドウで `route print` コマンドを入力します。192.168.0.192 がゲートウェイ リストにある場合は、手順 3 に進みます。ない場合は、適切な DOS または UNIX CLI コマンドを使用してゲートウェイ リストに 192.168.0.192 を追加します。
 - Windows 98/2000/NT システムの場合: `route add 192.168.0.192 <INSTALLATION COMPUTER IP ADDRESS>`
[例: `route add 192.168.0.192 15.128.122.12`]
 - UNIX(Sun Solaris など)システムの場合:
`route add 192.168.0.192 <CLIENT_HOST IP ADDRESS> -interface`
[例: `route add 192.168.0.192 15.128.122.12 -interface`]
3. 「**ping 192.168.0.192**」と入力します。Dominion SX 本体から応答があった場合は、手順 4 に進みます。エラーが発生した場合、デフォルト IP アドレスが正しく入力されていて、その IP アドレスへのルートが存在することを確認します。
4. インストール用コンピュータでブラウザを起動し、Web ブラウザのアドレス ボックスに工場出荷時のデフォルト IP アドレス **192.168.0.192** を入力し、本体へ接続します。
5. コンピュータにセキュリティ画面が表示された後、ログイン可能になります。
6. Security Alert-Certificate(セキュリティ警告 - 証明書)画面で[View Certificate(証明書の表示)]をクリックすると、Certificate(証明書)画面が表示されます。

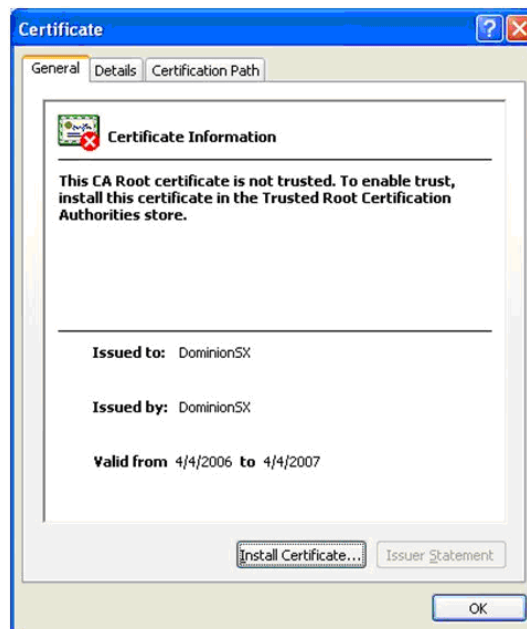


図 3 証明書情報

証明書のインストールについては、「第 8 章: セキュリティ」および「付録 C: 証明書」を参照してください。

セキュリティ警告画面および証明書情報画面の表示を終了すると、ログイン画面が表示されます。



図 4 DSX ログイン画面

7. デフォルトのユーザ名 admin とパスワード raritan でログインします。すべて小文字を使用します。Restricted Service Agreement(制限付きサービス契約)画面が表示されます。



図 5 Restricted Service Agreement(制限付きサービス契約)画面

注 ログイン後に「Accept(受け入れる)」をクリックすると、デフォルトのパスワードを変更するように求められます。

Change Password(パスワードの変更)画面が表示されます。

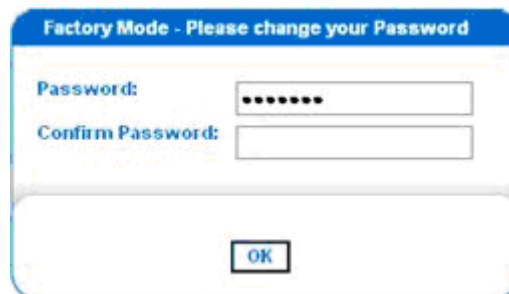


図 6 Change Password(パスワードの変更)画面

8. 安全な新しいパスワードを入力し、確認のためにもう一度入力します(新しいパスワードは覚えておいてください)。
9. [OK]をクリックします。
10. [Exit(終了)]をクリックします。
11. 新しいパスワードを使用して再度ログインします。

Dominion SX の Port Access(ポート アクセス)画面が表示されます(「第 3 章: ソフトウェアの初期設定」を参照)。

コマンドライン インタフェースを使用した初期設定

コマンドライン インタフェースから Dominion SX 本体を初期設定するには、以下の手順に従います。

1. インストール用コンピュータのシリアル ポートと、Dominion SX のターミナル シリアル ポートを接続します。このポートは、ほとんどのモデルでは DB-9 オス ポートとなります。しかし、DSXA-48 を含むすべての二重化電源、二重化 LAN モデルでは、ターミナルポートには RJ45 コネクタを使用します。
2. ハイパーターミナルなどのターミナル エミュレーション プログラムを開き、Dominion SX 本体に接続します。シリアル通信パラメータは、9600 bps、パリティなし、8 データ ビット、ストップ ビット 1、フロー制御なしです。
3. Dominion SX の電源を入れます。
4. プロンプトが表示されたら、デフォルトのユーザ名 `admin` とデフォルトのパスワード `raritan` を使用してログインします。
ログインすると、パスワードを変更するように求められます。
5. 新しいパスワードを入力し、確認のためにもう一度入力します(このパスワードは覚えておいてください)。

Dominion SX 本体のステータスとシリアル チャンネル ポートを示す画面が表示されます。

注 入力したパスワードがパスワード規則に従っていない場合、警告としてエラー メッセージが表示されます。その場合、ログアウトして、パスワード設定を最初からやり直す必要があります。

ネットワーク アクセス

1. インストール用コンピュータで、192.168.0.192 へのルートが設定されており、IP アドレス 192.168.0.192 と通信可能であることを確認します。
2. Windows でルーティング テーブルを確認するには、インストール用コンピュータのコマンド ウィンドウで `route print` コマンドを入力します。192.168.0.192 がゲートウェイ リストにある場合は、手順 3 に進みます。ない場合は、適切な DOS または UNIX CLI コマンドを使用してゲートウェイ リストに 192.168.0.192 を追加します。
 - Windows 98/2000/NT システムの場合: `route add 192.168.0.192 <INSTALLATION COMPUTER IP ADDRESS>`
[例: `route add 192.168.0.192 15.128.122.12`]
 - UNIX(Sun Solaris など)システムの場合:
`route add 192.168.0.192 <CLIENT_HOST IP ADDRESS> -interface`
[例: `route add 192.168.0.192 15.128.122.12 -interface`]
3. 「`ping 192.168.0.192`」と入力します。Dominion SX 本体から応答があった場合は、手順 4 に進みます。エラーが発生した場合、デフォルト IP アドレスが正しく入力されていて、その IP アドレスへのルートが存在することを確認します。
4. インストール用コンピュータでブラウザを起動し、Web ブラウザのアドレス ボックスに工場出荷時のデフォルト IP アドレス 192.168.0.192 を入力し、本体へ接続します。

日付と時刻の設定

1. 「`Configuration`」と入力して、本体の設定を変更します。
2. 「`Time`」と入力して、日付と時刻の設定を選択します。
3. 「`Timezonelist`」と入力して、使用するタイム ゾーンに対応する番号コードを見つけます。

- 「clock[tz timezone][datetime datetime-string]」と入力します。たとえば、次のようになります。

```
admin > Config > Time > clock tz 9 datetime "2007-02-05 09:22:33"
```

この例では、9 はタイム ゾーン コードで(手順 3)、“2007-02-05 09:22:33”は“YYYY-MM-DD HH:MM:SS”形式(引用符も必要)の日付と時刻を表す文字列です。

ネットワーク設定

- 「**Configuration**」と入力して、本体の設定を変更します。
- 「**Network**」と入力して、ネットワーク設定を選択します。
- 次を入力します。


```
admin > Config > Network > interface enable true if lan1 ip
192.16.151.12 mask 255.255.255 gw 192.168.51.12
```

 正しくデータを入力すると、レポートに新しいネットワーク設定が表示され、本体のレポートを求められます。
- 「yes」と入力して Dominion SX をレポートします。
- この時点で、シリアル ケーブルを外すことができます。
- 新しい IP アドレスとパスワードを使用して、インストール用コンピュータから Dominion SX に再接続し、次に進みます。

ユーザ設定

- 「**Configuration**」と入力して、本体の設定を変更します。
- 「**Users**」と入力して、ユーザ設定を選択します。

ユーザ グループの追加

「addgroup name <group name> class <class type> ports <n1,n2,n3...>」と入力します。ここで、<グループ名>はグループの名前で、<クラス タイプ>は次のいずれかになります。

- オペレータの場合は Op
- 監視者の場合は Ob

<n1,n2,n3...>は、このグループがアクセス可能なポート番号のリストで、カンマで区切り、スペースは挿入しません。同じパラメータを使用してポートの範囲を設定したり、ワイルドカードのアスタリスク(*)を使用することもできます。たとえば、次のように設定できます。

- “config port 3-7 exitstring #0”(これにより、ポート 3,4,5,6,7 で終了文字列が無効になります。)
- config port * bps 115200(これにより、すべてのポートの通信速度が 115200 bps に設定されます。)

ユーザの追加

- 「adduser user <user name> fullname <full name> group <group name> password <password> info <information> dialback <dialback number> active <status> ...」と入力します。ここで、<user name>はユーザのログイン名、<full name>はユーザのわかりやすい名前(スペース使用不可)、<group name>はユーザに割り当てるグループ、<password>はユーザのパスワード、<information>はその他の情報(オプション、スペース使用不可)、<dialback number>はユーザの電話番号(オプション)、<status>は true または false(ユーザにログインを許可するかどうか)です。
- 「top」と入力して、トップ レベルの CLI メニューに戻ります。

第 3 章: ソフトウェアの初期設定

ハードウェアをインストールしたら、ソフトウェアの初期設定を行います。これを行うには、ブラウザまたはコマンドライン インタフェースから Dominion SX にログインします(CLI の情報については「第 12 章:コマンドライン インタフェース」を参照)。

Dominion SX のソフトウェアの初期設定

1. 新しいパスワードを使用して Dominion SX にログインします。次のように、ユーザの種類にしたがって Port Access(ポート アクセス)画面が表示されます。

Port Access

A No	Name	Status
1	Port1	Up
2	Port2	Up
3	Port3	Up
4	Port4	Up

図 7 オペレータ/監視者用の Dominion SX Port Access(ポート アクセス)画面

Port Access

A No	Name	Status
1	Port1	Up
2	Port2	Up
3	Port3	Up
4	Port4	Up

図 8 管理者用の Dominion SX Port Access(ポート アクセス)画面

2. [Setup(セットアップ)]タブをクリックします。Setup(セットアップ)画面が表示されます。この画面には、Configuration(設定)画面および Logging(ログ)画面へのリンクがあります。

Configuration
Remote Authentication
Network
Services
Modem
Static Routes
Date / Time
Port Configuration
Port Keywords
Logging
Log
Events
NFS
SNMP

図 9 Setup(セットアップ)画面

重要: 各設定タスクを完了したら、Setup(セットアップ)タブに戻って次の設定タスクを実行する必要があります。

日付と時刻の設定

1. Setup(セットアップ)画面の[Configuration(設定)]セクションで[Date / Time(日付と時刻)]をクリックします。Date / Time Configuration(日付と時刻の設定)画面が表示されます。

図 10 Date/Time Configuration(日付と時刻の設定)画面

2. [UTC Offset(UTC オフセット)]ドロップダウン メニューから適切なタイム ゾーンを選択します。
3. 次のいずれかを選択します。
 - User Specified Time(ユーザによる時刻定義) – このラジオ ボタンをクリックして、対応するフィールドに手動で日付と時刻を入力します。
 - Synchronize with NTP Server(NTP サーバと同期) – このラジオ ボタンをクリックして、[Primary Time Server(プライマリ タイム サーバ)]にネットワーク タイム プロトコル(NTP)サーバの IP アドレスを入力します。バックアップ NTP サーバが存在する場合は、Secondary Time Server(セカンダリ タイム サーバ)フィールドにその IP アドレスを入力します。
4. Interface(インタフェース)フィールドにインタフェース名を入力します。
5. [OK]をクリックします。

注: 証明書の生成などの機能は、正しいタイムスタンプに依存するものがあります。タイムスタンプは、証明書の有効期間を確認するのに使用されます。また、Syslog および NFS ログ記録機能でも、システムに設定された時間をログ エントリの時間記録として使用します。

[OK]をクリックすると、次のいずれかの画面が表示されます。

- 確認画面。設定内容が表示され、画面の上部に次の確認メッセージが表示されます。
Date / Time Settings successfully applied.(日付と時刻の設定が正しく適用されました。)
- エラー画面。元の Date / Time(日付と時刻)画面と、次のエラー メッセージが表示されます。
Date / Time Settings NOT successfully applied.(エラー: 日付と時刻の設定が正しく適用されませんでした。)

ネットワーク設定

1. Setup(セットアップ)画面の[Configuration(設定)]セクションで[Network(ネットワーク)]をクリックします。Network Configuration(ネットワーク設定)画面が表示されます。

注 二重化 LAN モデルの場合は、[Eth Failover(Eth フェイルオーバー)]チェック ボックスがあり、デフォルトでオンになっていますが、これをオフにすることができます。下の画面は単一 LAN モデルであるため、このチェック ボックスは表示されていません。

Network Basic Settings	Ports
IP Address: 192.168.51.194	CSC Port: 5000
Subnet Mask: 255.255.255.0	Discovery Port: 5000
Gateway IP Address: 192.168.51.126	
Mode: Auto	
Domain: raritan.com	
Unit Name: DominionSX	
OK Cancel	

図 11 Network Configuration(ネットワーク設定)画面

注 ネットワーク管理者は通常、以下のパラメータ用に値を割り当てています。

2. 次のフィールドにデータを入力します。
 - **IP Address**(IP アドレス): この本体のネットワーク アドレス
 - **Subnet Mask**(サブネット マスク): この本体が存在するネットワークのサブネット マスク
 - **Gateway IP Address**(ゲートウェイ IP アドレス): この本体のデフォルト ゲートウェイ
3. [Mode(モード)]ドロップダウン メニューからモードを選択します。
4. **Domain**(ドメイン)フィールドにドメイン名を入力します。
5. **Unit Name**(本体の名前)フィールドに本体の名前を入力します。
6. [Ports(ポート)]セクションで、次のように入力します。
 - **CSC Port**(CSC ポート)フィールドに「5000」または別のポート番号を入力します。
 - **Discovery Port**(検出ポート)フィールドに「5000」または別のポート番号を入力します。
7. [OK]をクリックします。

確認画面またはエラー画面のどちらかが表示されます。

1. 確認ウィンドウが表示されたら[OK]をクリックします。確認画面が表示された後、設定を更新するために Dominion SX は自動的に接続を切断し、再起動します。
2. SX 本体とコンピュータの間のクロスケーブルを取り外します。
3. Cat 5 ストレート ケーブルの一方の端を SX に接続します。
4. ケーブルのもう一方の端をネットワークに接続します。
5. 新しく割り当てられた IP アドレスを使用して SX 本体にアクセスします。

設置

1. Dominion SX には、LAN 接続またはモデム接続(オプション)を利用してリモートでアクセスできます。
2. Dominion SX からは、シリアル接続でのみターゲット デバイスにアクセスできます。

LAN 接続

ソフトウェア初期設定の段階を終えたら、DSX 本体を LAN 上でのオペレーション用に設定します。

1. 本体で使用するネットワークに接続している、Ethernet ケーブルがあることを確認します。
2. 本体を適切な方法で実装します。
3. LAN ケーブルを、本体の後ろ側にあるプライマリ LAN 接続ポート(LAN 1)につなぎます。本体にフェイルオーバー モジュールがある場合は、セカンダリ ネットワーク LAN 接続ポート(LAN 2)にもつなぎます。
4. Web ブラウザを使用してデバイスに接続し、簡単な接続確認を行います。
5. アドレス ラインに「https://<IPAddress>」と入力します。<IPAddress>は、本体に既に設定されている IP アドレスです。

本体が適切に設定され、ネットワークから接続可能であることが確認できると、ログイン表示が表示されます。

6. ユーザ名 **admin** と前の手順で作成したパスワードを使用してログインします。
7. ホーム ページで、[Setup(セットアップ)]タブをクリックし、DSX と各コンソール ポートを設定するための各種設定オプションを選択します。

モデム接続(オプション)

DSX でモデム選択を設定するには、次の手順に従います。

1. モデム ポートに電話線を接続します。
2. この線の電話番号は、クライアントのダイヤルアップ ネットワーク設定を行う際に必要になるのでメモしておいてください。

詳細については、「付録 E: モデム設定」を参照してください。

第 4 章: ネットワーク設定とサービス

この章では、DSX の基本的なネットワーク設定方法と、さまざまなアクセス プロトコル(SSH、telnet など)の設定方法について説明します。さらに、DSX でのモデム接続の設定方法と、IP 転送を有効化して静的ルートを作成する方法についても説明します。

基本的なネットワークの設定方法

基本的なネットワーク設定と検出ポートの設定を行うには、[Setup(セットアップ)]タブをクリックして [Network(ネットワーク)]をクリックします。Network Basic Settings and Ports(ネットワーク基本設定とポート)画面が表示されます(図 12)。

Network Basic Settings	Ports
IP Address: <input type="text" value="192.168.50.132"/>	CSC Port: <input type="text" value="5000"/>
Subnet Mask: <input type="text" value="255.255.255.0"/>	Discovery Port: <input type="text" value="5000"/>
Gateway IP Address: <input type="text" value="192.168.50.126"/>	
Mode: <input type="text" value="100 Mbps"/> ▼	
Domain: <input type="text"/>	
Unit Name: <input type="text" value="DominionSX"/>	

図 12 Network Basic Settings and Ports(ネットワーク基本設定とポート)画面

DSX への名前付け

DSX 本体に名前を付けて識別しやすくするには、次の手順に従います。

1. Unit Name(本体の名前)フィールドに名前を入力します。
2. [OK]をクリックします。

DSX のネットワーク設定

ネットワーク設定を行うには、次の手順に従います。

1. IP address(IP アドレス)フィールドに DSX の IP アドレスを入力します。
2. **Subnet Mask**(サブネット マスク)フィールドにサブネット マスクを入力します。
3. **Gateway IP Address**(ゲートウェイ IP アドレス)フィールドにゲートウェイ ルータの IP アドレスを入力します。
4. **Mode**(モード)フィールドのドロップダウン メニューから速度を選択します。[Auto(自動)](デフォルト)または[100 Mbps]を選択できます。
5. **Domain**(ドメイン)フィールドにドメイン名を入力します。
6. [OK]をクリックします。

検出ポートの変更

DSX には、次の 2 つの検出ポートがあります。

- TCP 5000 Common Socket Connection(CSC)検出
- UDP 5000 Command Center(CC)検出

これらのポートのいずれかが別のアプリケーションによって使用されている場合、該当するフィールドの DSX の検出ポート番号を変更して[OK]をクリックします。

ネットワーク サービス設定

次の表に、各アクセス サービスのデフォルト設定を示します。

サービス	デフォルト設定
HTTP	有効。デフォルト ポートは 80 です。この値は変更できます。 HTTPS リダイレクトはデフォルトで有効になっています。HTTPS も有効に設定されている場合、すべての HTTP リクエストは自動的に HTTPS ポート(次を参照)にリダイレクトされます。
HTTPS	有効。デフォルト ポートは 443 です。この値は変更できます。 Encryption(暗号化)は SSL に設定されていますが、TLS に変更できません。
Telnet	セキュリティ上の理由から無効になっています。この設定を有効にして、ポートを設定することができます。
Local Port Access(ローカル ポート アクセス)	有効。ボーレートは 9600 bps に設定されていますが、この値を変更することは可能です。
Direct Port Access(ダイレクト ポート アクセス)	アクセス モードは IP に設定されていますが、[Normal(通常)]または[TCP port(TCP ポート)]に変更できます。

ネットワーク サービス設定の変更

1. **[Setup(セットアップ)]**タブをクリックし、**[Services(サービス)]**をクリックします。Network Service Settings(ネットワーク サービス設定)画面が表示されます。

Network Service Settings

Enable HTTP

Enable HTTP to HTTPS Redirect

HTTP Port:
80

Enable HTTPS

HTTPS Port:
443

Encryption:
SSL

Enable TELNET Access

Telnet Port:
23

Enable SSH Access

SSH Port:
22

Enable Local Port Access

Baud Rate:
9600

Direct Port Access Mode:
IP

OK Cancel

図 13 Network Service Settings(ネットワーク サービス設定)

2. 該当するフィールドに必要な変更を加えます。
3. **[OK]**をクリックします。

モデム アクセスの設定

DSX には、モデム経由でアクセスできます。この設定を行うには、次の手順に従います。

1. **[Setup(セットアップ)]**タブをクリックし、**[Modem(モデム)]**をクリックします。Modem Settings(モデム設定)画面が表示されます。

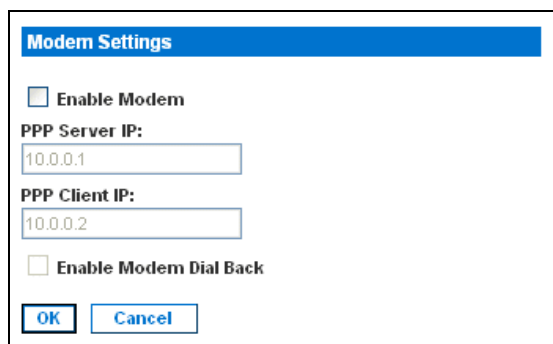


図 14 Modem Settings(モデム設定)画面

2. **[Enable Modem(モデムを有効にする)]**チェック ボックスをオンにして、モデム アクセスを有効にします。
3. PPP Server IP(PPP サーバ IP)フィールドに、Point-to-Point(PPP)サーバの IP アドレスを入力します。デフォルトの IP アドレスは 10.0.0.1 です。
4. **PPP Client IP(PPP クライアント IP)**フィールドに、PPP クライアントの IP アドレスを入力します。デフォルトの IP アドレスは 10.0.0.2 です。
5. モデムのダイヤル バックを有効にする場合は、**[Enable Modem Dial Back(モデムのダイヤル バックを有効にする)]**チェック ボックスをオンにします。
6. **[OK]**をクリックします。モデム アクセスが有効になります。

IP 転送と静的ルートの設定

IP 転送を有効にすることができます。また、DSX に LAN ポートが 2 つある場合や、モデム アクセスが設定されている場合は、静的ルートを作成することもできます。

IP 転送の有効化

IP 転送を有効にするには、次の手順に従います。

1. **[Setup(セットアップ)]**タブをクリックし、**[Static Routes(静的ルート)]**をクリックします。Static Routes(静的ルート)画面が表示されます。この画面は、IP Forwarding(IP 転送)パネルと Static Routes List(静的ルート リスト)から構成されています。
2. IP Forwarding(IP 転送)パネルに移動し、**[Enable IP Forwarding(IP 転送の有効化)]**チェック ボックスをオンにします。

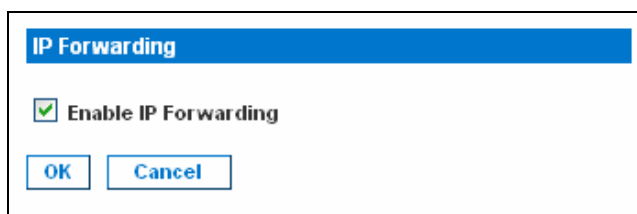


図 15 IP Forwarding(IP 転送)パネル

3. **[OK]**をクリックします。IP 転送が有効になります。

新しい静的ルートの追加

新しい静的ルートを追加するには、次の手順に従います。

1. [Setup(セットアップ)]タブをクリックし、[Static Routes(静的ルート)]をクリックします。Static Routes(静的ルート)画面が表示されます。この画面は、IP Forwarding(IP 転送)パネルと Static Routes List(静的ルート リスト)から構成されています。

Static Route List

Interface	Destination	Mask	Gateway	MTU	Window	IRTT	Flags
<input type="checkbox"/> LAN	0.0.0.0	0.0.0.0	192.168.50.126	0	0	0	0

図 16 Static Routes List(静的ルート リスト)

2. Static Routes List(静的ルート リスト)に移動して[Add New Route(新規ルートの追加)]をクリックします。Static Routes(静的ルート)画面が表示されます。

Route

Interface:
LAN 1

Destination:

Mask:

Gateway:

MSS:

Window:

IRTT:

Flags:
Host

図 17 Static Route(静的ルート)画面

3. LAN インタフェースが 1 個の DSX では、Interface(インタフェース)フィールドに自動的に[LAN1]と表示されます。LAN インタフェースが 2 個ある DSX では、Interface(インタフェース)フィールドのドロップダウン メニューから目的のインタフェースを選択します。
 - LAN1 = eth0
 - LAN2 = eth1
4. **Destination**(送信先)、**Mask**(マスク)、および **Gateway**(ゲートウェイ)の各フィールドに、送信先ホストの IP アドレス、サブネット マスク、ゲートウェイを入力します。
5. **MSS** フィールドに、TCP 最大セグメント サイズ(MSS)を入力します。
6. **Window**(ウィンドウ)フィールドに、このルートを経由する接続の TCP ウィンドウのサイズをバイト単位で入力します。
7. **IRTT** フィールドに、このルートを経由する TCP 接続の初期ラウンド トリップ タイム(IRTT)をミリ秒単位(1-12000)で入力します。
8. [**Flags**(フラグ)]ドロップダウン メニューからルート タイプを選択します。
 - [**Host**(ホスト)]は、このルートがホスト マシン用であることを意味します。
 - [**Net**(ネット)]は、このルートがサブネット用であることを意味します。
9. [**OK**]をクリックします。

静的ルートの削除

静的ルートを削除するには、次の手順に従います。

1. [**Setup**(セットアップ)]タブをクリックし、[**Static Routes**(静的ルート)]をクリックします。Static Routes(静的ルート)画面が表示されます。この画面は、IP Forwarding(IP 転送)パネルと Static Routes List(静的ルート リスト)から構成されています。
2. Static Routes List(静的ルート リスト)に移動して、削除するルートの横にあるチェック ボックスをオンにします。
3. [**Delete**(削除)]をクリックします。削除を確認するプロンプトが表示されます。
4. [**OK**]をクリックします。ルートが削除されます。

第 5 章: ユーザ プロファイルとユーザ グループ

この章では、ユーザ プロファイルとユーザ グループを作成および管理する方法について説明します。

ユーザ プロファイルの管理

ユーザ プロファイルの機能は、次の 2 つを目的として提供されています。

- ユーザが、ユーザ名とパスワードを使用して DSX にログインできるようにする。
- ユーザをユーザ グループに関連付ける。ユーザ グループにより、ユーザがアクセス可能な機能とポートが決まります。

DSX には、出荷時にユーザ プロファイル(admin ユーザ)が 1 つ組み込まれています。このプロファイルは Admin ユーザ グループと関連付けられており、システムおよびポートに対する完全な権限を持っています。このプロファイルを変更または削除することはできません。

他のユーザ プロファイルは、必要な数だけ作成できます。DSX にログインする人ごとに別々のユーザ プロファイルを作成することも、限られた数のプロファイルを作成して複数の人が各プロファイルを使用するようにすることもできます。

ユーザ プロファイル リストの表示

1. 既存のユーザ プロファイル リストを表示するには、[User Management(ユーザ管理)]タブをクリックして[User List(ユーザ リスト)]をクリックします。User List(ユーザ リスト)画面が表示されます(図 18)。

User List

<input type="checkbox"/>	Username	Full Name	Dialback	Group	Active
<input type="checkbox"/>	Alexander	Alexander		Designers	Yes
<input type="checkbox"/>	Andre	Andre		Managers	Yes
<input type="checkbox"/>	Charle	Charles Kord		Designers	Yes
<input type="checkbox"/>	Elaine	Elaine		Admin	Yes
<input type="checkbox"/>	Emma	Emma Kall		Admin	Yes
<input type="checkbox"/>	Lauren	Lauren		Managers	Yes
<input type="checkbox"/>	Maureen	Maureen Rand		Admin	Yes
<input type="checkbox"/>	Stan	Stan		Admin	Yes
<input type="checkbox"/>	Vic	Victor		Admin	Yes
	admin	Administrator		Admin	Yes

Delete Add New User

図 18 User List(ユーザ リスト)画面

2. User List(ユーザ リスト)画面には、これまでに作成されたすべてのユーザ プロファイルが表示され、プロファイルごとに次の情報が表示されます。
 - ユーザ名
 - フル ネーム
 - ダイヤル バック番号(定義されている場合)
 - ユーザ グループ
3. User List(ユーザ リスト)画面には、ユーザ プロファイルがアクティブか非アクティブかどうかについても示されます。

ユーザ プロファイルの作成

新しいユーザ プロファイルを作成するには、次の手順に従います。

1. [User Management(ユーザ管理)]タブをクリックし、[User List(ユーザ リスト)]をクリックします。User List(ユーザ リスト)画面が表示されます(図 18)。
2. [Add New User(新規ユーザの追加)]をクリックします。New User(新規ユーザ)画面が表示されます。

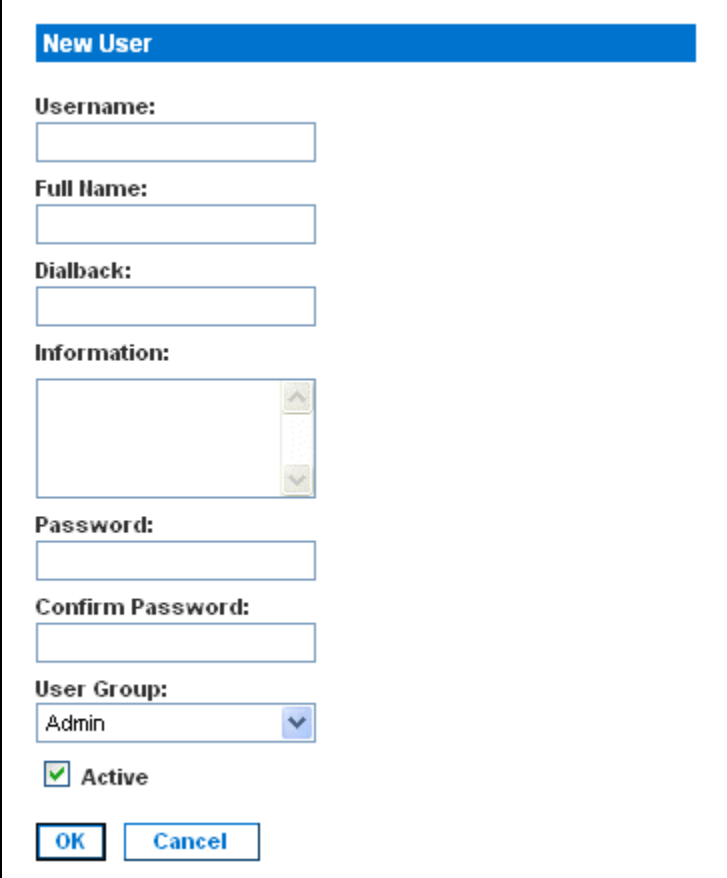


図 19 New User(新規ユーザ)画面

3. Username(ユーザ名)フィールドにログイン名を入力します。これは、ユーザが DSX へのログイン時に入力する名前です。このフィールドは必須です。
 - 任意の数の文字を入力できます(最大 255 文字)。
 - “><”を除く出力可能なすべての文字を入力できます。
 - ユーザ名では大文字と小文字が区別されます。
4. Full Name(フル ネーム)フィールドにユーザのフル ネームを入力します。このフィールドは必須です。
5. Dialback(ダイヤル バック)フィールドにユーザの電話番号を入力します。このフィールドはオプションです。
6. Information(情報)フィールドにユーザ プロファイルに関するコメントを入力します。このフィールドは、プロフィールを識別するのに役立ちます。このフィールドはオプションです。
7. Password(パスワード)フィールドにパスワードを入力し、Confirm Password(パスワードの確認)フィールドにパスワードを再入力します。このフィールドは必須です。
 - 任意の数の文字を入力できます(最大 16 文字)。
 - 出力可能なすべての文字を入力できます。

- パスワードは、大文字と小文字が区別されます。

注 強力なパスワード機能が有効な場合、他のパスワード要件が適用されます。詳細については、第 8 章を参照してください。

8. User Group(ユーザ グループ)フィールドのドロップダウン メニューから、ユーザ グループを選択します。デフォルトでは Admin グループが入力されています。

ヒント 必要なユーザ グループがまだ作成されていない場合、ユーザ グループを作成した後に、ユーザ プロファイルに戻ってそのグループを選択できます。ここでは、デフォルトのままにします。

9. このプロファイルをすぐにアクティブにするかどうかを決定します。デフォルトでは[Active(アクティブ)]チェック ボックスがオンになっています。このアカウントを無効にするには、このチェック ボックスをオフにします。必要な場合は、いつでもこの画面に戻ってユーザをアクティブにすることができます。
10. [OK]をクリックします。ユーザ プロファイルが作成されます。作成されたユーザ プロファイルは、User List(ユーザ リスト)画面に表示されます。

ユーザ プロファイルの変更

既存のユーザ プロファイルを変更するには、次の手順に従います。

1. [User Management(ユーザ管理)]タブをクリックし、[User List(ユーザ リスト)]をクリックします。User List(ユーザ リスト)画面が表示されます(図 18)。
2. 編集するプロファイルのユーザ名をクリックします。Edit User(ユーザの編集)画面が表示されます。この画面は、New User(新規ユーザ)画面と全く同じ構成です(図 19)。
3. Username(ユーザ名)フィールドを除くすべてのフィールドを変更できます。
4. セキュリティ上の理由から、パスワードは表示されません。プロファイルのパスワードを変更するには、Password(パスワード)および Confirm Password(パスワードの確認)の各フィールドに新しいパスワードを入力します。これらのフィールドをそのままにした場合、パスワードは変更されません。
5. 変更が完了したら[OK]をクリックします。ユーザ プロファイルが変更されます。

ユーザ プロファイルの削除

既存のユーザ プロファイルを削除するには、次の手順に従います。

1. [User Management(ユーザ管理)]タブをクリックし、[User List(ユーザ リスト)]をクリックします。User List(ユーザ リスト)画面が表示されます(図 18)。
2. 削除するユーザ プロファイルの左側にあるチェック ボックスをオンにします。複数のユーザ プロファイルを選択できます。
3. [Delete(削除)]をクリックします。削除を確認するプロンプトが表示されます。
4. [OK]をクリックします。選択したユーザ プロファイルが削除されます。

ユーザ グループの管理

ユーザ グループの機能は、次の 2 つの目的から提供されています。

- グループに関連付けられているユーザが実行可能なシステム機能を決定する。
- グループに関連付けられているユーザがアクセス可能なポートを決定する。

DSX には、出荷時にユーザ グループ(Admin ユーザ グループ)が 1 つ組み込まれています。このグループに関連付けられたユーザは、すべてのシステム機能を実行し、すべてのポートにアクセスすることができます。このグループを変更または削除することはできません。

他のユーザ グループは、必要な数だけ作成できます。

ユーザ グループ リストの表示

既存のユーザ グループ リストを表示するには、[User Management(ユーザ管理)]タブをクリックして [User Group List(ユーザ グループ リスト)]をクリックします。Group List(グループ リスト)画面が表示されます(図 20)。

Group List

Group	Class
Admin	Administrator
<input type="checkbox"/> Designers	Observer
<input type="checkbox"/> Managers	Operator
<input type="checkbox"/> Support	Operator
<input type="checkbox"/> Writers	Operator

Delete Add New User Group

図 20 Group List(グループ リスト)画面

Group List(グループ リスト)画面には、これまでに作成されたすべてのユーザ グループが表示され、グループごとにグループの名前とクラスが表示されます。

ユーザ グループの作成

新しいユーザ グループを作成するには、次の手順に従います。

- [User Management(ユーザ管理)]タブをクリックし、[User Group List(ユーザ グループ リスト)]をクリックします。Group List(グループ リスト)画面が表示されます(図 20)。
- [Add New Group User(新規ユーザ グループの追加)]をクリックします。New Group(新規グループ)画面が表示されます。

New Group

Group Name:

Class:

Port Access:

Select All

01: Port1 02: Port2

03: Port3 04: Port4

図 21 New Group(新規グループ)画面

- Group Name(グループ名)**フィールドにグループ名を入力します。
 - 任意の数の文字を入力できます(最大 255 文字)。
 - すべての文字と数字に加えて、アンダースコア文字(_)を入力できます。
 - ユーザ名では大文字と小文字が区別されます。
- Class(クラス)**フィールドのドロップダウン メニューからクラスを選択します。次のいずれかを選択します。
 - Operator(オペレータ): デフォルトのオプションです。オペレータ クラスに関連付けられたユーザには、コンソール ウィンドウへの書き込み/読み取りアクセス権がありますが、ユーザ自身のパスワード以外のシステム設定パラメータを変更することはできません。

- Observer(監視者): 監視者クラスに関連付けられたユーザには、コンソール ウィンドウへの読み取り専用アクセス権がありますが、ユーザ自身のパスワード以外のシステム設定パラメータを変更することはできません。
5. このグループに関連付けられているユーザがアクセス可能なポートを選択します。すべてのポートを選択することも、個別のポートの組み合わせを選択することもできます。
 6. **[OK]**をクリックします。ユーザ グループが作成されます。作成されたユーザ グループは、Group List(グループ リスト)画面に表示されます。

ユーザ グループの変更

既存のユーザ グループを変更するには、次の手順に従います。

1. **[User Management(ユーザ管理)]**タブをクリックし、**[User Group List(ユーザ グループ リスト)]**をクリックします。Group List(グループ リスト)画面が表示されます(図 20)。
2. 編集するグループのグループ名をクリックします。Edit Group(グループの編集)画面が表示されます。この画面は、New Group(新規グループ)画面と全く同じ構成です(図 21)。
3. **Group Name(グループ名)**フィールドを除くすべてのフィールドを変更できます。
4. 変更が完了したら**[OK]**をクリックします。ユーザ グループが変更されます。

ユーザ グループの削除

既存のユーザ グループを削除するには、次の手順に従います。

1. **[User Management(ユーザ管理)]**タブをクリックし、**[User Group List(ユーザ グループ リスト)]**をクリックします。Group List(グループ リスト)画面が表示されます(図 20)。
2. 削除するユーザ グループの左側にあるチェック ボックスをオンにします。複数のユーザ プロファイルを選択できます。
3. **[Delete(削除)]**を選択します。削除を確認するプロンプトが表示されます。
4. **[OK]**をクリックします。選択したユーザ グループが削除されます。

空白ページ

第 6 章: リモート認証

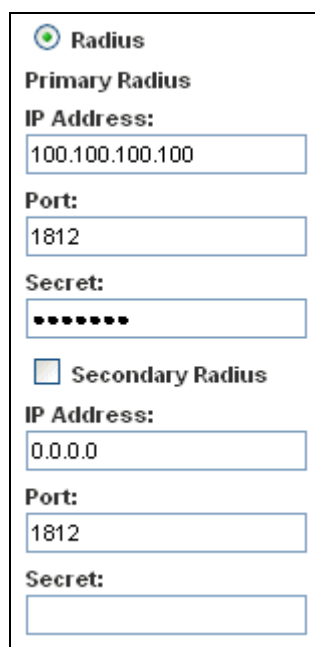
この章では、RADIUS、LDAP、および TACACS+ の各認証を設定する方法について説明します。

ヒント: リモート認証を設定する場合、ローカル認証は有効のままにしておくことをお勧めします。認証リクエストが DSX に到達すると、まずリモートでユーザを検索して認証し、次にローカルでユーザを検索して認証を行います。ローカル認証を有効のままにすると、リモート認証の設定が間違っていたり使用できない場合でも、ローカルで認証できるので DSX からロックアウトされなくなります。

RADIUS の設定

ローカル認証の代わりに、Remote Dial-In User Service(RADIUS)を使用して DSX ユーザを認証することができます。RADIUS を設定するには、次の手順に従います。

1. [Setup(セットアップ)]タブをクリックし、[Remote Authentication(リモート認証)]をクリックします。Remote Authentication(リモート認証)画面が表示されます。この画面には、RADIUS パネルが含まれています。



The screenshot shows a configuration window titled "Radius". It contains two sections: "Primary Radius" and "Secondary Radius". Each section has input fields for "IP Address", "Port", and "Secret". The "Primary Radius" section has the IP address "100.100.100.100", Port "1812", and a masked secret "*****". The "Secondary Radius" section has the IP address "0.0.0.0", Port "1812", and an empty secret field. There is a checkbox for "Secondary Radius" which is currently unchecked.

図 22 RADIUS パネル

2. RADIUS パネルで、[RADIUS]ボタンをクリックして RADIUS 認証を有効にします。
3. **Primary Radius**(プライマリ RADIUS)に次の情報を入力します。
 - RADIUS サーバの IP アドレス
 - RADIUS サーバが受け入れるポート(デフォルトは 1812)
 - 共有の暗号化キー
4. バックアップ RADIUS サーバがある場合、**Secondary Radius**(セカンダリ RADIUS)フィールドにも同じ情報を入力します。
5. [OK]をクリックします。RADIUS 認証が有効になります。

LDAP の設定

ローカル認証の代わりに、Lightweight Directory Access Protocol(LDAP)を使用して DSX ユーザを認証することができます。LDAP を設定するには、次の手順に従います。

1. **[Setup(セットアップ)]**タブをクリックし、**[Remote Authentication(リモート認証)]**をクリックします。Remote Authentication(リモート認証)画面が表示されます。この画面には、LDAP パネルが含まれています。

The image shows two panels for LDAP configuration. The left panel is titled 'LDAP' and 'LDAPS Certificate Settings'. It contains fields for 'Primary LDAP' with 'IP Address' (0.0.0.0), 'Port' (389), 'Secret', 'Base DN', 'Query', 'Search', and 'Dialback Query String'. The right panel is titled 'Secondary LDAP' and contains fields for 'IP Address' (0.0.0.0), 'Port' (389), 'Secret', 'Base DN', 'Query', 'Search', and 'Dialback Query String'.

図 23[LDAP]パネル

2. LDAP パネルで、[LDAP]ボタンをクリックして LDAP 認証を有効にします。
3. Primary LDAP(プライマリLDAP)で、**IP Address**(IP アドレス)フィールドおよび **Port**(ポート)フィールドに、LDAP サーバの IP アドレスと、LDAP サーバが受け入れるポート(デフォルトは 389)を入力します。
4. **Secret**(秘密)フィールドに、ディレクトリ サーバ/マネージャにアクセスするためのルート パスワードを入力します。このフィールドの名前はディレクトリ サーバに依存します。たとえば、Microsoft Windows Active Directory では「**Password**(パスワード)」ですが、SUN iPlanet ディレクトリ サーバでは「**Secret**(秘密)」という呼び名が使われます。
5. **Base DN**(ベース DN)フィールドに、サーバにバインドする「ルート」ポイントを入力します。これは、ディレクトリ マネージャ DN(たとえば、BaseDn: cn=Directory Manager)と同じものです。
6. **Query**(照会)フィールドに文字列を入力します。同じ文字列が属性として **Search**(検索)フィールドに追加されていることを確認します。たとえば、認証照会文字列が DominionSX の場合、DominionSX という属性が **Search**(検索)フィールドで指定されているドメインに追加されている必要があります。さらに、これらの設定を正しく機能させるには、Windows Active Directory のユーザグループとマップするユーザ グループが DSX で作成されている必要があります。
7. **Search**(検索)フィールドに、検索を開始するドメイン名を入力します。**Search**(検索)フィールドは、Base DN(ベース DN)のサブツリーで、UID などのユーザ情報へのパス検索を行い、検索にかかる時間を短縮します。

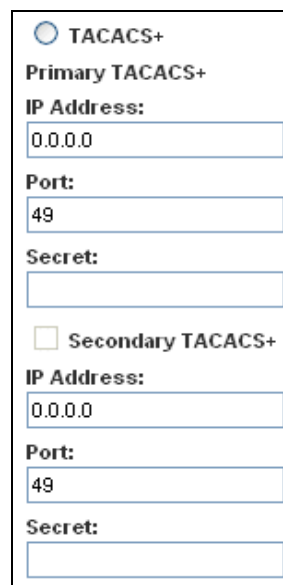
つまり、これはドメイン名です。ユーザ名の検索が開始される場所です。ユーザ名はこのドメインで作成され(たとえば、Search: dc=raritan, dc=com)、Dominion SX からの LDAP 認証照会が処理されます。

8. モデムを使用して LDAP サーバに接続している場合、**Dialback Query String**(ダイヤル バック照会文字列)フィールドにダイヤル バック文字列を入力します。
9. バックアップ LDAP サーバがある場合、**Secondary LDAP**(セカンダリ LDAP)フィールドにも同じ情報を入力します。
10. **[OK]**をクリックします。LDAP 認証が有効になります。

TACACS+の設定

ローカル認証の代わりに、Terminal Access Controller Access-Control System Plus(TACACS+)を使用して DSX ユーザを認証することができます。TACACS+を設定するには、次の手順に従います。

1. **[Setup(セットアップ)]**タブをクリックし、**[Remote Authentication(リモート認証)]**をクリックします。Remote Authentication(リモート認証)画面が表示されます。この画面には、TACACS+パネルが含まれています。



The image shows a configuration window for TACACS+. At the top, there is a radio button labeled 'TACACS+' which is selected. Below it, the 'Primary TACACS+' section is visible, containing three input fields: 'IP Address' with the value '0.0.0.0', 'Port' with the value '49', and 'Secret' which is empty. Below this is a radio button for 'Secondary TACACS+' which is not selected. This section also has three input fields: 'IP Address' with '0.0.0.0', 'Port' with '49', and 'Secret' which is empty.

図 24 TACACS+パネル

2. TACACS+パネルで、**[TACACS+]**ボタンをクリックして TACACS+認証を有効にします。
3. Primary TACACS+(プライマリ TACACS+)で、**IP Address**(IP アドレス)フィールドおよび **Port**(ポート)フィールドに、TACACS+サーバの IP アドレスと、TACACS+サーバが受け入れるポート(デフォルトは 49)を入力します。
4. **Secret**(秘密)フィールドに、ディレクトリ サーバ/マネージャにアクセスするためのルート パスワードを入力します。このフィールドの名前はディレクトリ サーバに依存します。たとえば、Microsoft Windows Active Directory では「**Password**(パスワード)」ですが、SUN iPlanet ディレクトリ サーバでは「**Secret**(秘密)」という呼び名が使われます。
5. バックアップ TACACS+サーバがある場合、**Secondary TACACS+**(セカンダリ TACACS+)フィールドにも同じ情報を入力します。
6. **[OK]**をクリックします。TACACS+認証が有効になります。

空白ページ

第 7 章: ポート設定とポート アクセス アプリケーション

ポート設定では、管理者はリモート ターゲット デバイスと通信するためにシリアル ポートやコンソール ポート設定を定義することができます。

注 Raritan Serial Console(RSC)には、Port(ポート)画面からアクセスできます。RSC については、この章の「Raritan Serial Console」セクションを参照してください。

ポート キーワード

ポート キーワードを作成して、それらを次のものと関連付けることができます。

- イベント
- ローカル/リモートの syslog メッセージ
- SNMP トラップ

ポート キーワードは、フィルタとして機能します。キーワードが検出されると、そのときに初めてそれに対応するメッセージがローカル/NFS ポート ログに記録されます。対応するイベントは SMTP(設定されている場合)経由で送信され、対応するトラップは SNMP(設定されている場合)経由で送信されます。

これは、ローカル/リモート NFS ログ記録に非常に役立ちます。必要な情報だけ記録されて不要なメッセージが記録されないのので、追跡しやすくなります。

注 SMTP 通知(event.amp.keyword)は、Event configuration(イベント設定)ページで選択します。

1. [Setup(セットアップ)]タブをクリックし、[Port Keywords(ポート キーワード)]をクリックします。Port Keywords(ポート キーワード)画面が表示されます。

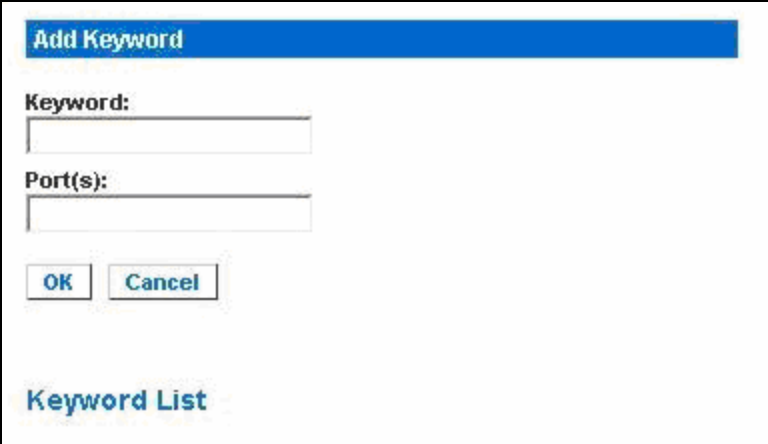


図 25 Port Keywords(ポート キーワード)画面

2. **Keyword**(キーワード)フィールドにキーワードを入力します。
3. **Port(s)**(ポート)フィールドに、そのキーワードと関連付けるポートを入力します。
4. [OK]をクリックします。

ポート設定

1 つまたは複数のポートを設定するには、次の手順に従います。

1. **[Setup(セットアップ)]**タブをクリックし、**[Port Configuration(ポート設定)]**をクリックします。Port Configuration(ポート設定)画面が表示されます。

Port Configuration

<input type="checkbox"/>	A No	Name	Application	Baud Rate	Parity Bits	X on / X off	HW Flow
<input type="checkbox"/>	1	Port1	RaritanConsole	9600	None/8	Enabled	Disabled
<input type="checkbox"/>	2	Port2	RaritanConsole	9600	None/8	Disabled	Disabled
<input type="checkbox"/>	3	Port3	RaritanConsole	9600	None/8	Disabled	Disabled
<input type="checkbox"/>	4	Port4	RaritanConsole	9600	None/8	Disabled	Disabled

図 26 Port Configuration(ポート設定)画面

2. 設定するポートを選択します。ポートを 1 つ選択します。ポート設定がすべて同じであれば複数のポートを選択できます。
 - 特定のポートを選択するには、ポート番号の左側にあるチェック ボックスをオンにし、**[Edit(編集)]**をクリックします。
 - すべてのポートを選択するには、**[Select All(すべて選択)]**をクリックします。Edit Port(ポートの編集)画面が表示されます。

Port 1

Name:

Application:

Baud Rate:

Parity Bits:

Flow Control:

Detect:

Exit Command:

Escape Mode:

Escape Character:

Emulation:

DPA IP Address:

DPA SSH TCP Port:

DPA Telnet TCP Port:

図 27 Edit Port(ポートの編集)画面

3. ポートの値が、ターゲット システムのシリアル ポート設定にある最初の 3 つの値と一致していることを確認します。
 - [Baud Rate(ボーレート)]ドロップダウン メニューから[Baud Rate(ボーレート)]を選択します。

注 ローカル ポート アクセスでサポートされる最小ボーレートは 9600 です。

- [Parity Bits(パリティ ビット)]ドロップダウン メニューから[Parity Bits(パリティ ビット)]を選択します。
 - [Flow Control(フロー制御)]ドロップダウン メニューから[Flow Control(フロー制御)]を選択します。
4. **Detect(検出)**フィールドで、Dominion SX がターゲットへの物理的な接続を検出するかどうかを指定します。デフォルトは「検出しない」です。この設定を変更するには、Detect(検出)フィールドのドロップダウン メニューから[Detect Physical Connection to the Target(ターゲットへの物理的接続を検出する)]を選択します。
 5. **Exit Command(終了コマンド)**フィールドにコマンドを入力します。これは、ポート切断が発生した場合に、システムに送信されるコマンド(例: logout)です。
 6. エスケープ モードを選択します。デフォルトは[None(なし)]です。次のように変更します。
 - Escape Mode(エスケープ モード)フィールドのドロップダウン メニューから[control(コントロール)]を選択します。
 - [Escape Character(エスケープ文字)]にエスケープ文字を入力します。Dominion SX のデフォルトは)(閉じ角かっこ)です。
 7. Emulation(エミュレーション)フィールドのドロップダウン メニューからターミナル エミュレーション タイプを選択します。次のいずれかを選択します。
 - VT100
 - VT220
 - VT320
 - ANSI
 8. Direct Port Access(DPA)を使用する場合は、DPA IP アドレスに加えて、次のいずれか、または両方を入力する必要があります。
 - DPA SSH TCP Port(DPA SSH TCP ポート)フィールドに、ポート番号(7700 など)を入力します。
 - DPA Telnet TCP Port(DPA Telnet TCP ポート)フィールドに、ポート番号(8800 など)を入力します。
 9. [OK]をクリックします。

ダイレクト ポート アクセス

ダイレクト ポート アクセスを設定するには、次の手順に従います。

1. [Setup(セットアップ)]タブをクリックし、[Services(サービス)]をクリックします。Network Service Settings(ネットワーク サービス設定)画面が表示されます。**Direct Port Access Mode(ダイレクト ポート アクセス モード)**フィールドが画面の下部に表示されます。



図 28 Direct Port Access Mode(ダイレクト ポート アクセス モード)フィールド

2. **Direct Port Access Mode**(ダイレクト ポート アクセス モード)フィールドに移動します。デフォルトは[Normal(通常)]で、無効を意味します。DPA を有効にするには、ドロップダウン メニューから[IP]または[TCP Port(TCP ポート)]を選択します。
3. [OK]をクリックしてこの情報を保存します。画面に次のメッセージが表示されます。
The system will need to be rebooted for changes to take effect. (変更を有効にするためにはシステムをリブートする必要があります。)
4. すぐにリブートするか、DPA の設定がすべて完了してからシステムをリブートします。
5. [Setup(セットアップ)]タブをクリックし、[Port Configuration(ポート設定)]をクリックします。Port Configuration(ポート設定)画面が表示されます(図 26)。
6. ダイレクト ポート アクセスを設定するポートを選択します。
 - 特定のポートを選択するには、ポート番号の左側にあるチェック ボックスをオンにします。複数のポートを選択することもできます。ポートの選択が終わったら[Edit(編集)]をクリックします。
 - すべてのポートを選択するには、[Select All(すべて選択)]をクリックします。
 Edit Port Configuration(ポート設定の編集)画面が表示されます(図 27)。DPA フィールドが画面の下部に表示されます。
7. 該当するフィールドに、DSX の DPA IP アドレスを入力し、SSH と Telnet に使用する DPA ポートを入力します。
8. [OK]をクリックしてこの情報を保存します。
9. DSX 本体をリブートします。ダイレクト ポート アクセスの設定を有効にするには、DSX 本体をリブートする必要があります。

匿名ポート アクセス

匿名ポート アクセスを使用すると、ユーザはパスワードを入力しなくても DPA 用に設定されたポートにアクセスできます。この機能を有効にするには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Login Settings(ログイン設定)]をクリックします。Login Settings(ログイン設定)画面が表示されます(図 54)。
2. 画面の下部にある[Anonymous Port Access(匿名ポート アクセス)]チェック ボックスがオンになっていることを確認します。
3. [User Management(ユーザ管理)]タブをクリックし、[User Group List(ユーザ グループ リスト)]をクリックします。Group List(グループ リスト)が表示されます(図 20)。

注 ユーザ グループについて詳しくは、第 5 章を参照してください。

4. [Add New Group User(新規ユーザ グループの追加)]をクリックします。New Group(新規グループ)画面が表示されます(図 21)。
5. **Group Name**(グループ名)フィールドに「Anonymous」と入力します。
6. **Class**(クラス)フィールドのドロップダウン メニューから[Observer(監視者)]を選択します。
7. **Port Access**(ポート アクセス)フィールドで、匿名ポート アクセスを行うポートを選択します。
8. [OK]をクリックします。

重要: 新しいダイレクト ポート アクセスの設定を適用するには、Dominion SX 本体をリブートする必要があります。

Raritan Serial Console

Raritan Serial Client(RSC)を起動するには、次の手順に従います。

1. [Port Access(ポート アクセス)]タブを選択します。

Port Access

No	Name	Status
1	Port1-RedHatLinux7	Up
2	Port2-RedHatLinux	Up
3	Port3	Up
4	Port4	Up
5	Port5	Up
6	Port6	Up
7	Port7-HP8000 Switch	Up
8	Port8	Up

図 29 Port Access(ポート アクセス)画面

2. 「Port1」または「Port2」など、RSC のアクセスに使用するポートの名前をクリックします。

注 *https* を使用して RSC に接続する場合のみ、Security(セキュリティ)ポップアップ画面が表示されません。

3. [Yes(はい)]をクリックします。Warning – Security(警告 - セキュリティ)ポップアップ画面が表示されます。
4. [Yes(はい)]をクリックして、Port(ポート)画面から Raritan Serial Client にアクセスします。

注 [Always(常に)]をクリックすると、それ以降のアクセス時に Security(セキュリティ)画面は表示されなくなります。

Raritan Serial Console ウィンドウが表示されます。この章の「Raritan Serial Client インタフェース」セクションを参照してください。

Java を使用する際の Raritan Serial Client の要件

Raritan Serial Client(RSC)を使用するには、512 MB 以上の RAM を搭載した 1 GHz の PC が必要です。ターゲット(管理デバイス)にアクセスするためには、RSC を使用する前に Java をインストールする必要があります。

Java Runtime Environment(JRE)

RSC は、JRE バージョン 1.4.2_05 以降(JRE バージョン 1.5.0_02 を除く)で動作します。最大のパフォーマンスを得るためには、JRE 1.5.0(前述のとおり 1.5.0_02 は除く)の使用をお勧めします。

使用するオペレーティング システムとブラウザでは、いくつかの JRE 設定を調整してシステムのメモリに関する問題を防ぐことができます。

注 RSC は、JRE バージョン 1.5.0_02 はサポートしません。

JRE をダウンロードすると、JRE の構成に関する指示が提供されます。次の Java Web ページにアクセスして、お使いのシステムにインストールされている JRE のバージョンを確認してください。

<http://www.java.com/en/download/help/testvm.xml>

重要: RSC をブラウザから起動する場合は Java アプレット キャッシングを無効にし、Java によってシステムのメモリに問題が発生しないよう、次の手順を行うことを強くお勧めします。

Java アプレットとメモリに関する考慮事項

通常、ブラウザ ベースの RSC では、Java アプレットの実行時のパラメータを変更する必要はありません。Web ブラウザを介して RSC を実行しているときに、「Out of Memory」エラーが発生する場合は、次の手順を行います。

- Java アプレットの実行時の設定を変更します。
- 次のリンクにアクセスして、Java コントロール パネルを使用した実行時の設定方法を参照します。

<http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>

http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer_guide/control_panel.html

複数の Dominion SX ターゲットにアクセスするために、より多くの RSC アプレットを起動できるようにするには、次の手順を行って、ヒープの設定を増やします。

1. Java コントロール パネルを起動します。Java コントロール パネルへのアクセス方法は次のとおりです。
 - [詳細設定(Advanced)]タブ(JRE 1.4.x の場合)
 - [Java]タブ(JRE 1.5 の場合)
2. [Java Runtime Settings]に移動します。

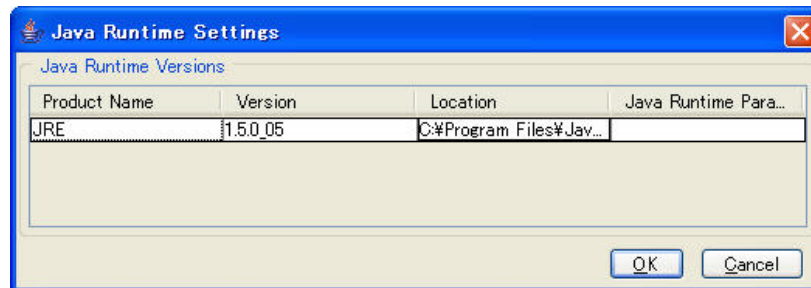


図 30 Java Runtime Settings 画面

3. 次の表に記載されている構文を使用して、Java の実行時のパラメータ値を挿入します。この表には、標準ではないオプションが含まれています。

表 2 Java 実行時のパラメータ

値 - 構文	説明	デフォルト値／コメント
-Xms<Size> (単位: バイト)	Java ヒープの初期値を設定	2097152(2 MB) <ul style="list-style-type: none"> • -server フラグを使用すると、デフォルト サイズを 32 MB まで増やせます。 • 値は、1024 バイト(1 KB)の倍数で、これより大きい値を指定する必要があります。 • メガバイトを表す場合は「m」または「M」、キロバイトを表す場合は「k」または「K」を付けます。
-Xms<Size> (単位: バイト)	Eden 生成のための Java ヒープの初期値を設定	640 KB <ul style="list-style-type: none"> • -server フラグを使用すると、デフォルト サイズを 2 MB まで増やせます。 • メガバイトを表す場合は「m」または

		「M」、キロバイトを表す場合は「k」または「K」を付けます。
-Xms<Size> (単位: バイト)	Java ヒープの最大値を設定 -	64 MB <ul style="list-style-type: none"> • -server フラグを使用すると、デフォルト サイズを 128 MB まで増やせます。 • 最大ヒープの限度は約 2 GB(2048 MB)です。 • メガバイトを表す場合は「m」または「M」、キロバイトを表す場合は「k」または「K」を付けます。

コマンドの例:

-Xms128M -Xmn128M -Xmx512M

さらに詳しい情報、およびその他の標準ではないオプションについては、次のリンクを参照してください。

<http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/java.html>

<http://java.sun.com/docs/hotspot/VMOptions.html>

Raritan Serial Client インタフェース

重要: 通常、Raritan Serial Client(Console)画面は、ポート画面の後ろに表示される別のウィンドウに表示されます。Windows では、Java のバージョンによっては、この画面がポート画面の前に表示される場合があります。

Port Access(ポート アクセス)画面を最小化して、Raritan Serial Console 画面にアクセスします。RSC のドロップダウン メニューから、次の機能を利用できます。

- フォントやウィンドウ サイズなどのエミュレーション設定の変更
- セッションの履歴管理
- ポートに対する書き込みアクセス権のリクエスト
- ポートに対する書き込みロックの取得
- ブレーク信号の送信(Solaris サーバ用)
- 現ポートに接続しているユーザのリスト取得
- ウィンドウ内のテキスト編集
- ターゲット デバイスからのクライアント ワークステーション ベースのデータ ログ管理
- キー入力(組み合わせ)の送信
- テキスト ファイルの送信
- Power Distribution Unit(PDU)への電源再投入のコマンドの送信
- 同一ポート上の他のユーザとのチャット
- ヘルプの表示

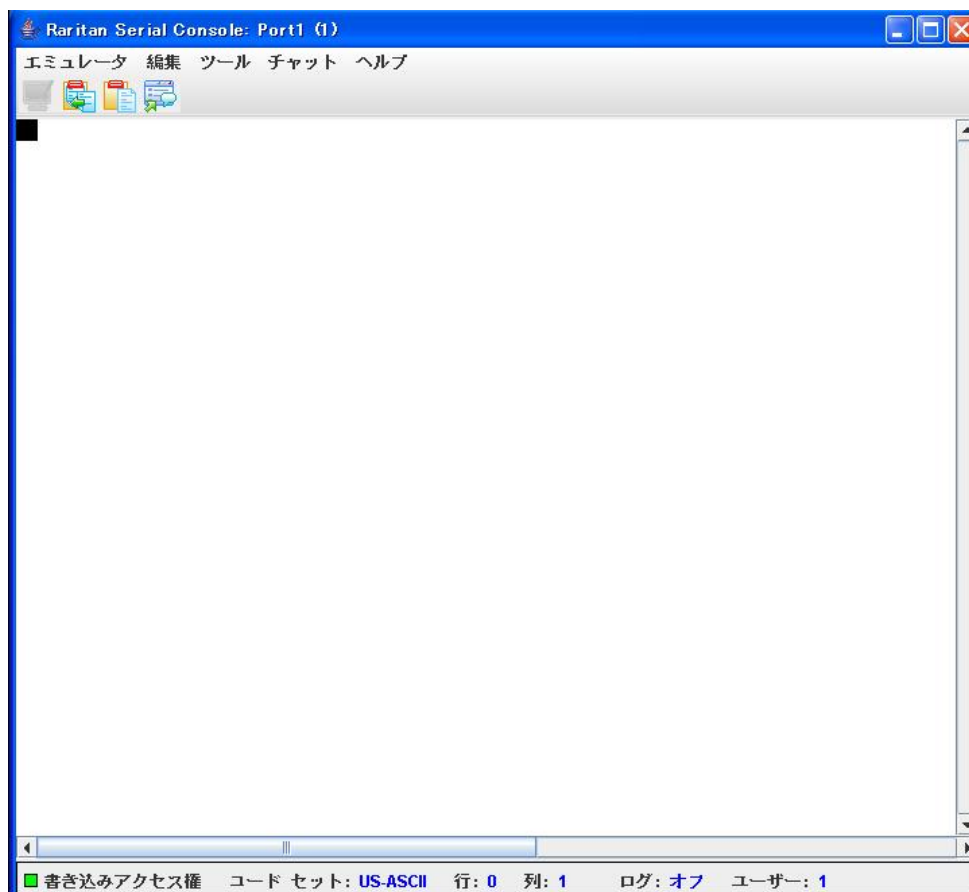


図 31 Raritan Serial Client ウィンドウ

エミュレータ

1. RSC を初めて起動する場合は、起動前にユーザのアイドル タイムアウトのデフォルト設定を変更します。変更せずに起動すると 10 分後にタイムアウトが発生し、ホストとの接続が終了した旨のメッセージが表示されます。アイドル タイムアウトの設定を変更する方法については、『Dominion SX ユーザ ガイド』の「セキュリティ」を参照してください。
2. [エミュレータ]ド롭ダウン メニューをクリックして、コマンドのリストを表示します。

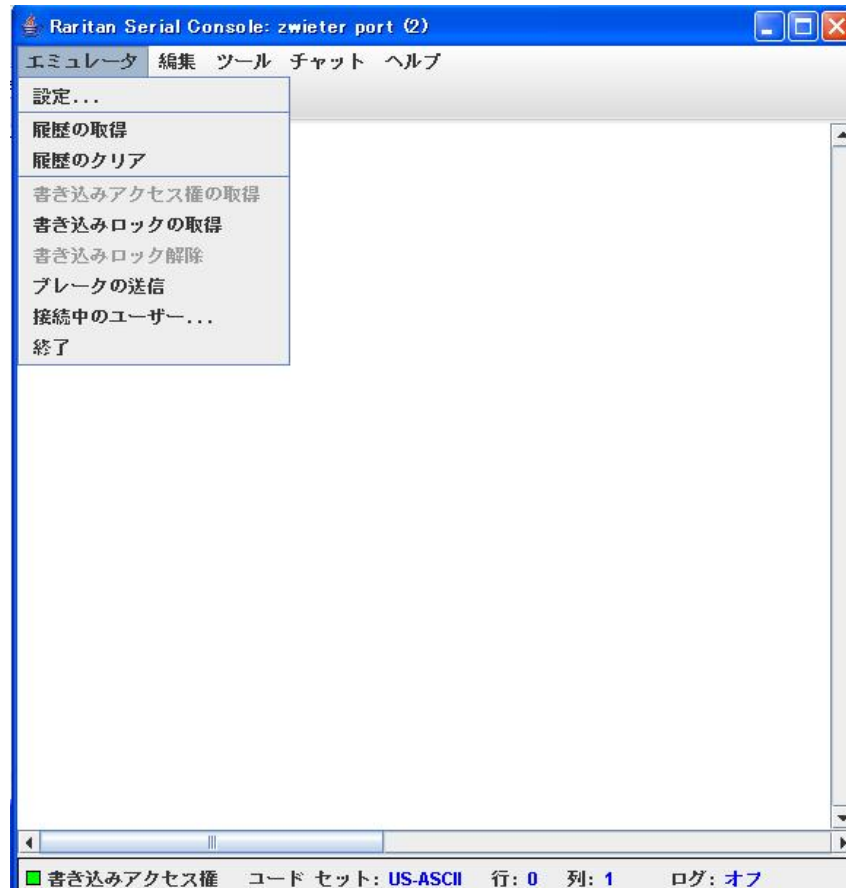


図 32 [エミュレータ]ド롭ダウン メニュー

重要: RSC の使用を開始する前に、Dominion SX GUI でユーザのアイドル タイムアウトのデフォルト設定を変更する必要があります。変更せずに使用を開始すると 10 分後にタイムアウトが発生し、ホストとの接続が終了した旨のメッセージが表示されます。アイドル タイムアウトの設定を変更する方法については、『Dominion SX ユーザ ガイド』の「セキュリティ」の章を参照してください。

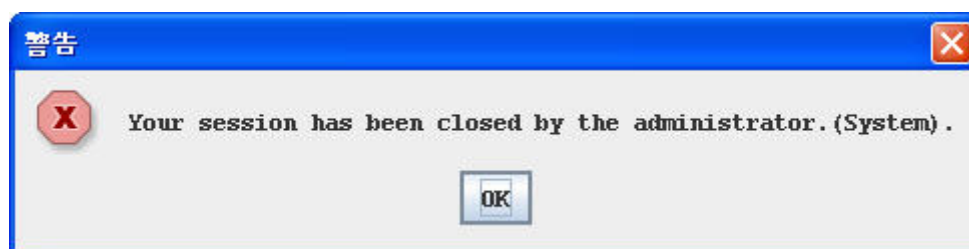


図 33 接続終了の警告

3. Idletimeout のデフォルト設定を変更してから、RSC を起動します。

注 RSC の Idletimeout が経過すると、Dominion SX の Idletimeout 期間が開始します。

設定

注 ターミナル エミュレーションは、管理者が [Setup(セットアップ)]メニューの [Port Configuration(ポート設定)]メニューを使用して設定します。

1. [エミュレータ]メニューの [設定] をクリックします。設定画面の [一般] タブにデフォルトの設定が表示されます。



図 34 一般設定ウィンドウ

2. [メイン メニューのショートカット] で、デフォルトの [なし] を選択するか、[メイン メニュー ショートカット] ドロップダウン メニューから次のいずれかを選択します。
 - F10
 - Alt
3. [終了時に確認ダイアログを表示] チェック ボックスをデフォルトのままオンにしておくか、またはオフにします。
4. [ターミナル サイズ] をデフォルトのままにするか、または [ターミナル サイズ] ドロップダウン メニューからサイズを選択します。
5. [バック スペースで送信] をデフォルトの「ASCII DEL」のままにするか、または [バック スペースで送信] ドロップダウン メニューから [Control-H] を選択します。

6. [履歴バッファのサイズ]をデフォルトの「200」のままにするか、または矢印キーを使用してバッファ サイズを変更します。
7. [カーソルの種類]をデフォルトの[ブロック カーソル]のままにするか、または[ライン カーソル]を選択します。
8. [OK]をクリックします。

表示設定

1. [エミュレータ]メニューに戻り、[設定]に続いて[表示]タブをクリックします。

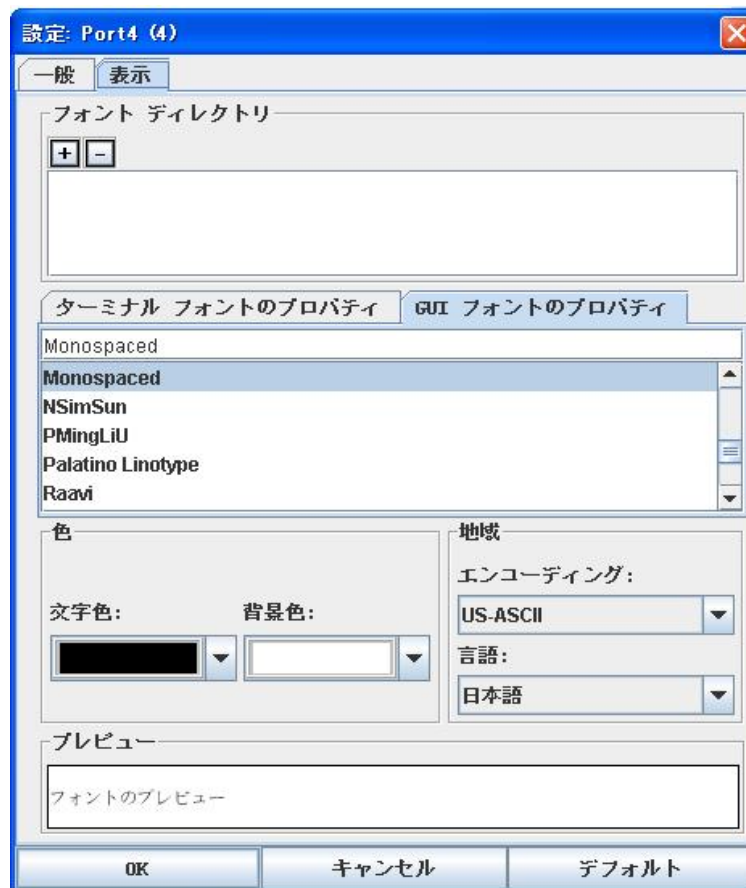


図 35 表示設定ウィンドウ

2. [デフォルト]をクリックして、デフォルト設定を選択します。[OK]をクリックして表示設定ウィンドウを閉じます。表示設定を変更する場合は、次の手順を行います。
3. [ターミナル フォントのプロパティ]をデフォルトの[Arial]のままにするか、または[ターミナル フォントのプロパティ]のリストをスクロールして、フォントを選択します。
4. [アンチエイリアス フォント]チェック ボックスをデフォルトのままオンにするか、またはオフにします。
5. フォントのサイズを変更する場合は、[フォント サイズをロック]チェック ボックスをオンにして、[フォント サイズ]ドロップダウン メニューからフォント サイズを選択します。

6. [GUI フォントのプロパティ]タブをクリックして、デフォルトの[Monospaced(等幅)]のままにするか、または[GUI フォントのプロパティ]のリストをスクロールして、フォントを選択します。

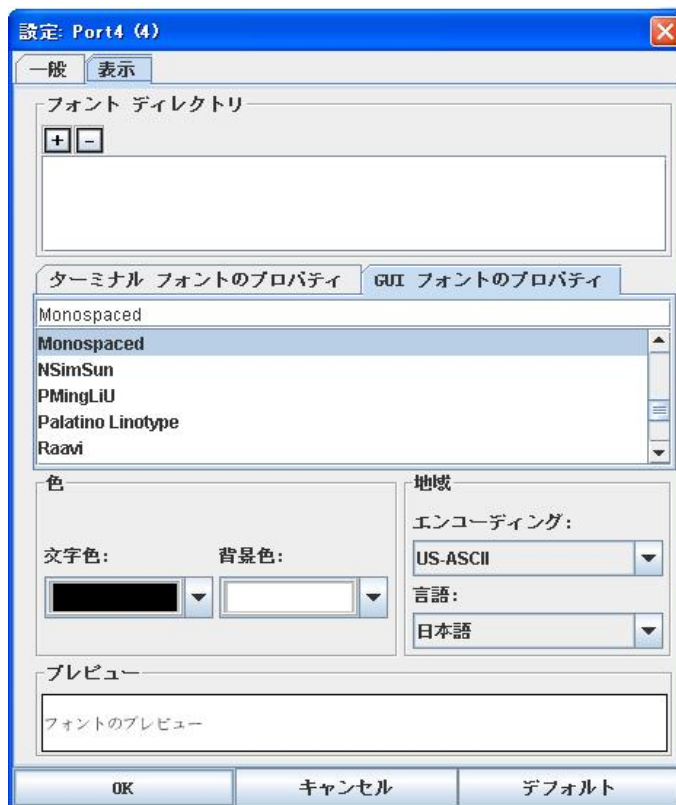


図 36 表示設定: GUI フォントのプロパティ

7. 次のドロップダウン メニューから、それぞれ適切な項目を選択します。
- 文字色
 - 背景色
8. [エンコーディング]ドロップダウン メニューから、次のいずれかを選択します。
- US-ASCII
 - ISO-8859-1
 - ISO-8859-15
 - UTF-8
9. [言語]ドロップダウン メニューから、次のいずれかを選択します。
- 英語
 - ブルガリア語
 - 日本語
 - 韓国語
 - 中国語
10. [OK]をクリックして、表示設定ウィンドウを閉じます。言語の設定を変更した場合は、表示設定ウィンドウを閉じたときに指定した言語に変わります。

注 ローカライズのサポートが原因で、RSC を起動したときに認識できない文字が表示されたり、画面がぼやけたりする場合は、フォントを Courier New に変えてみてください。

履歴の取得

履歴情報は、ターゲット デバイスのデバッグ、トラブルシュート、または管理を行う場合に便利です。履歴の取得機能を使用すると、次の操作を行うことができます。

- ターゲット デバイスとの双方向のコンソール メッセージを表示して、コンソール セッションの最近の履歴を表示する。
- 最近のコンソール メッセージ履歴を 256 KB(64 MB SDRAM のモジュールの場合のみ 64 KB、128 MB SDRAM モジュールの場合は 256 KB)の容量まで表示できます。これにより、ユーザはターゲット デバイスの長時間にわたるイベントの履歴を表示できます。

エントリがサイズの制限に到達すると履歴の最初に戻り、最も古いデータが最新データで上書きされます。

注[Maintenance(メンテナンス)], [Configuration(構成)]メニューの順に選択して、お使いの本体のメモリを確認してください。

履歴データは、履歴をリクエストしたユーザにのみ表示されます。

セッション履歴を表示するには、[エミュレータ]メニューの[履歴の取得]をクリックします。

履歴のクリア

履歴をクリアするには、[エミュレータ]メニューの[履歴のクリア]をクリックします。

書き込みアクセス権の取得

管理者とオペレータのみが書き込みアクセス権を取得できます。書き込みアクセス権を持っているユーザは、ターゲット デバイスにコマンドを送信できます。書き込みアクセス権は、[書き込みアクセス権の取得]コマンドを使用して、Raritan Serial Client で作業中の他のユーザが受け継ぐことができます。

11. 書き込みアクセス権を有効にするには、[エミュレータ]メニューの[書き込みアクセス権の取得]をクリックします。

- これで、ターゲット デバイスへの書き込みアクセス権を取得できました。
- 他のユーザが書き込みアクセス権を受け継ぐと、次のようになります。
 - a. ステータス バーの[書き込みアクセス権]の前に赤いブロックが表示されます。
 - b. 現在書き込みアクセス権を持っているユーザに対して、コンソールへのアクセス権が他のユーザに受け継がれたことを通知するメッセージが表示されます。

書き込みロックの取得

1. 書き込みロックを取得するには、[エミュレータ]メニューの[書き込みロックの取得]をクリックします。
2. 書き込みロックの取得を利用できない場合は、リクエスト拒否のメッセージが表示されます。

書き込みロック解除

書き込みロック解除を取得するには、[エミュレータ]メニューの[書き込みロック解除]をクリックします。

ブレークの送信

Sun Solaris サーバなどのターゲット システムでは、OK プロンプトを生成する際に NULL 文字(ブレーク)を送信する必要があります。これは、Sun キーボードから STOP-A を発行することと同じです。

- 管理者特権を持つユーザのみがブレークを送信できます。
- オペレータや監視者であるユーザはブレークを送信できません。

Sun Solaris サーバへ意図的な「ブレーク」を送信するには、次の手順を行います。

1. 書き込みアクセス権を持っていることを確認します。アクセス権がない場合は、前のセクションに記載されている、書き込みアクセス権の取得方法を参照してください。
2. [エミュレータ]メニューの[ブレークの送信]をクリックします。
[ブレークの送信の確認応答]ポップアップ ウィンドウが表示されます。
3. [OK]をクリックします。

接続中のユーザー

[接続中のユーザー]コマンドを使用すると、現在同じポートにアクセスしている他のユーザのリストを表示できます。

1. 接続中のユーザを表示するには、[エミュレータ]メニューの[接続中のユーザー]をクリックします。



図 37 接続中のユーザー ウィンドウ

2. コンソールへの書き込みアクセス権を持っているユーザ名の横の[書き込みアクセス権]欄のチェックボックスがオンになっています。
3. [閉じる]をクリックして接続中のユーザー ウィンドウを閉じます。

終了

1. Raritan Serial Console を終了するには、[エミュレータ]メニューの[終了]をクリックします。
終了の確認画面が表示されます。
2. [Yes]をクリックします。

編集

[コピー]、[貼り付け]、[すべて選択]コマンドを使用すると、重要なテキストの再配置または再利用、あるいはその両方ができます。

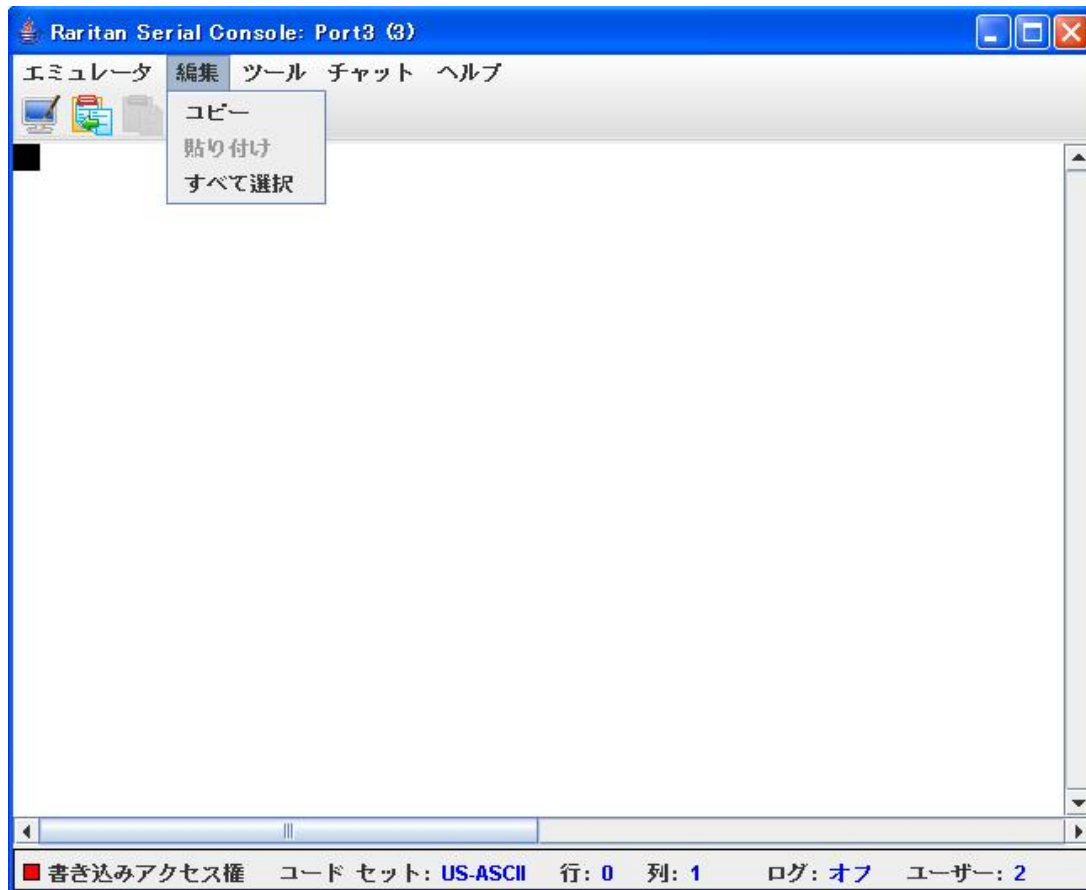


図 38 編集コマンド - テキストのコピー、貼り付け、すべて選択

すべてのテキストをコピーおよび貼り付けるには、次の手順に従います。

1. [編集]メニューの[すべてを選択]をクリックします。
2. [編集]メニューの[コピー]をクリックします。
3. テキストを貼り付ける場所にカーソルを置きます。
4. 1 回クリックして、その場所をアクティブにします。
5. [編集]メニューの[貼り付け]をクリックします。

注 テキストのすべてまたは一部をハイライト、コピー、貼り付ける場合のショートカット キーは次のとおりです。

- コピーするテキストをマウスでクリックしてドラッグします。
- CTRL キーを押しながら C キーを押してコピーします。
- そのテキストを貼り付ける場所にカーソルを置き、クリックしてその場所をアクティブにします。
- CTRL キーを押しながら V キーを押して貼り付けます。

Raritan Serial Client でコピーできるテキストは、最大 9,999 行です。

ツール

1. [ツール]ドロップダウン メニューをクリックして、コマンドのリストを表示します。



図 39 ツール メニュー

ログの開始

ログの開始機能を使用すると、ターゲット デバイスからコンソールの RAW データを収集し、お使いのコンピュータにファイルとして保存できます。RSC を起動すると、ステータス バーのログ インジケータに、ログのオン/オフが表示されます。

1. [ツール]メニューの[ログの開始]をクリックします。
2. 既存のファイルを選択するか、[RSC ログの保存]ダイアログ ボックス内に新規ファイル名を入力します。
 - ログ用に既存のファイルを選択した場合、データはファイル内のコンテンツに付加されます。
 - 新規ファイル名を入力した場合は、新しいファイルが作成されます。

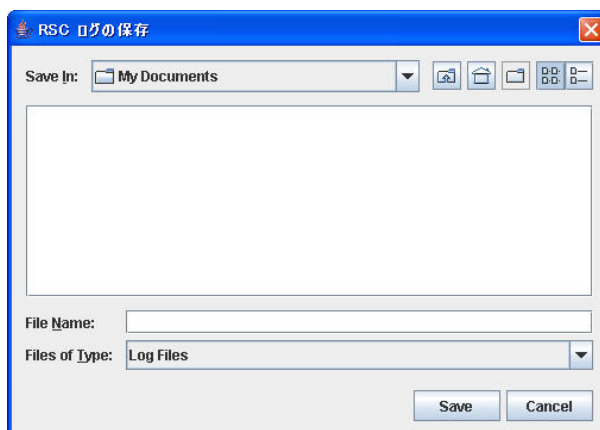


図 40 ログの開始コマンド ウィンドウ

3. ファイルを選択、あるいは作成した後に[Save(保存)]をクリックします。

ログの停止

[ツール]メニューの[ログの停止]をクリックします。これによって、ログが停止します。

キー入力の送信

1. [ツール]メニューの[キー入力の送信]をクリックします。
キー入力の送信画面が表示されます。



図 41 キー入力の送信

2. キー入力の組み合わせを入力し、[キー コード]ドロップダウン メニューからキー コード名を選択します。
3. キー入力の組み合わせを送信します。

テキスト ファイルの送信

1. [ツール]メニューの[テキスト ファイルの送信]をクリックします
テキスト ファイルの送信画面が表示されます。
2. テキスト ファイルが保存されているディレクトリを開きます。
3. テキスト ファイルのファイル名をクリック、または入力します。
4. [Open(開く)]をクリックします。
 - [Open(開く)]ダイアログ ボックスで[Open(開く)]をクリックすると、選択したファイルが直接ポートに送信されます。
 - ループバック プラグが挿入されている場合は、ファイルが表示されます。
 - ターゲットが接続されていない場合は、画面には何も表示されません。

チャット

SSL 経由でブラウザを使用してアクセスしている場合、チャットと呼ばれる双方向の会話機能を使って、同じポートを使用している他のユーザと会話ができます。このオンラインの会話を利用して、トレーニングや診断の共同作業を行うことができます。チャット メッセージの長さは、300 文字までです。

注 チャットが開始されると、そのポートにログインしているすべての SSL ユーザのモニタにチャット ウィンドウが表示されます。1 人のユーザが 1 つのポートに複数回ログインしている場合、そのユーザに対してチャット メッセージは表示されません。

チャットを使用するには、次の手順に従います。

1. [チャット]メニューの[チャット]をクリックします。

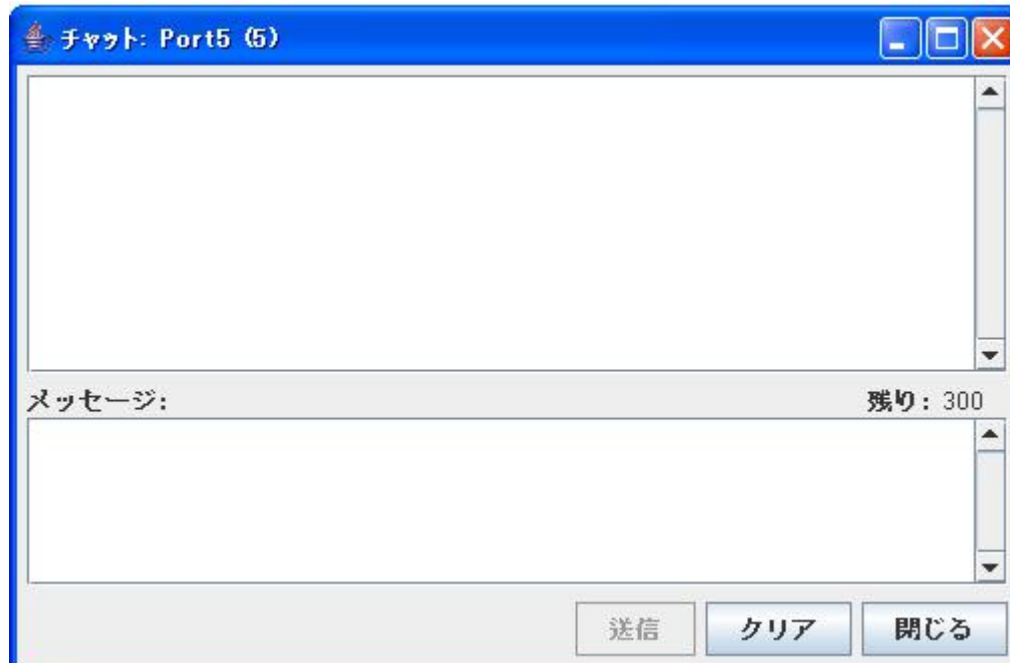


図 42 SecureChat コマンドとユーザ チャット ウィンドウ

2. [メッセージ]テキスト フィールドにメッセージを入力します。
3. [送信]をクリックするか、**ENTER** キーを押してメッセージを送信します。
4. 入力したテキストを削除する場合は[クリア]、チャットを終了してメッセージ ウィンドウを閉じる場合は[閉じる]をクリックします。

ヘルプ

ヘルプ トピックには、Raritan Serial Console の操作に関するオンライン アシスタンス、および Raritan Serial Console のリリース情報が含まれています。

ヘルプ トピック

ヘルプ トピックにアクセスするには、次の手順に従います。

1. [ヘルプ]メニューの[ヘルプ トピック]をクリックします。
2. 目次が表示されているウィンドウの右側にあるナビゲーション バーをスクロールしてトピックを探すか、リンクをクリックします。
3. 終了したらウィンドウを閉じます。

バージョン情報

バージョン情報ウィンドウには、コンソール端末のエミュレーション ソフトウェアのバージョン情報(名前と改訂番号)および著作権情報が表示されます。技術的サポートが必要な場合や、ソフトウェアのアップグレードを行うために Raritan に連絡するときに、この情報を求められることがあります。

バージョン情報を表示するには、次の手順に従います。

1. [ヘルプ]メニューの[バージョン情報]をクリックします。
[Raritan Serial Console]ドロップダウン メニューの一番上に、バージョン情報のメッセージが表示されます。



図 43 バージョン情報ウィンドウの例

2. [OK]をクリックして、バージョン情報ウィンドウを閉じます。

スタンドアロン Raritan Serial Console のインストール

注 スタンドアロン Raritan Serial Client は、次の Raritan サポート Web サイトからダウンロードできません。<http://www.raritan.co.jp/support>

スタンドアロン Raritan Serial Client(RSC)を使用すると、Dominion SX GUI アプリケーションを介さずにターゲット デバイスと直接接続することができます。Dominion SX のアドレスとポート番号(ターゲット)を指定するだけで接続できます。

このセクションでは、スタンドアロン Raritan Serial Client(RSC)をインストールする手順を説明します。

スタンドアロン Raritan Serial Client の要件

Raritan Serial Console を使用するには、次の要件を満たす必要があります。

- RSC は、JRE バージョン 1.4.2_05 以降(JRE バージョン 1.5.0_02 を除く)で動作します。最大のパフォーマンスを得るためには、JRE 1.5.0(前述のとおり 1.5.0_02 は除く)の使用をお勧めします。
- お使いのオペレーティング システムとブラウザによっては、システム構成を調整する必要がある場合があります。JRE をダウンロードすると、JRE の構成に関する指示が提供されます。
<http://www.java.com/en/download/help/testvm.xml> にアクセスして、お使いのシステムに現在インストールされている JRE のバージョンを確認してください。

互換性のある JRE のバージョンがインストールされていない場合は、<http://www.java.com> にアクセスし、[Download Now]ボタンをクリックしてください。

注 RSC は、JRE バージョン 1.5.0_02 はサポートしません。

- 512 MB 以上の RAM を搭載した 1 GHz の PC。
- コマンドラインから Java を起動できることを確認。そのためには、環境変数を設定する必要があります。Java がインストールされているパスを書き留めておきます(このパス情報は後で必要になります)。

Windows OS 変数の設定

1. [スタート]メニューから[コントロール パネル]を開き、[システム]を選択します。
2. [詳細設定]タブの[環境変数]をクリックします。

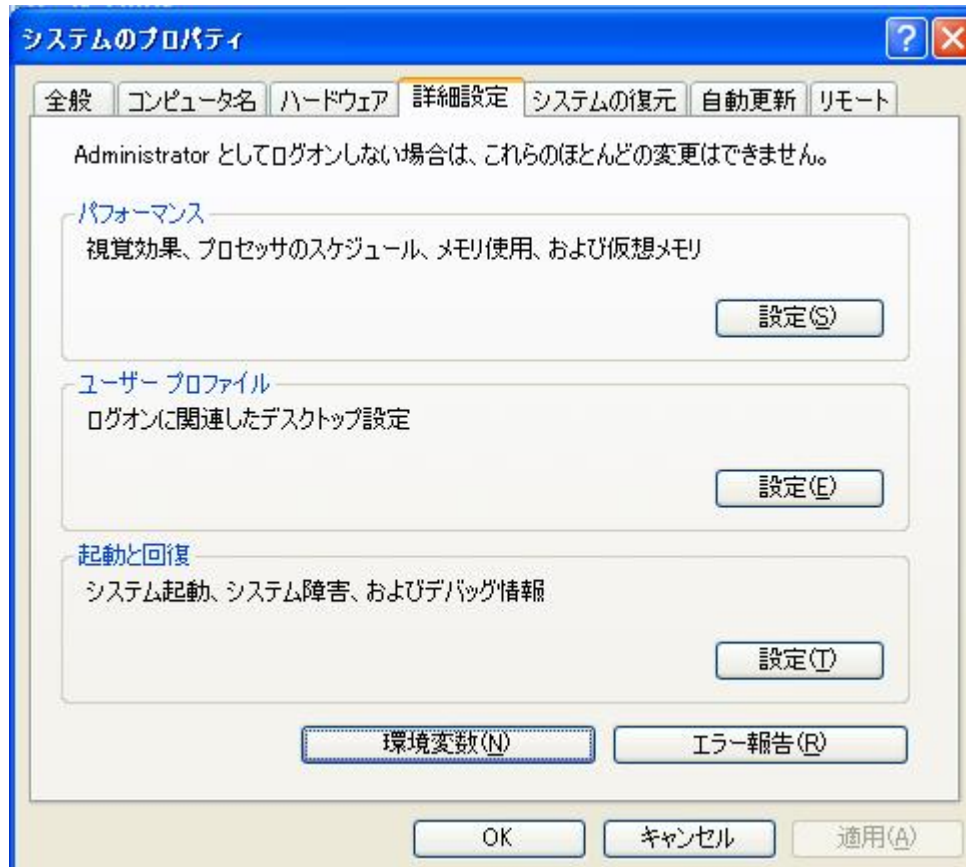


図 44 Windows OS: システムのプロパティ

3. [システム環境変数]セクションの[新規]をクリックします。
4. [新しいシステム変数]ダイアログ ボックスで、[変数名]テキスト ボックスに「JAVA_HOME」、[変数値]テキスト ボックスに先ほど書き留めておいたパスを入力します。

5. [OK]をクリックします。



図 45 Windows OS: 新しいシステム変数

6. PATH 変数を選択して、[編集]をクリックします。
7. 現在の変数値の後ろに「%JAVA_HOME%\bin」を追加します。stringの最後の値と新しい値の間に必ずセミコロン(;)を入力してください。

8. [OK]をクリックします。



図 46 Windows OS: システム変数の編集

9. CLASSPATH 変数を選択して、[編集]をクリックします。
CLASSPATH 変数値にピリオド(.)が含まれており、正しく設定されていることを確認します。何らかの理由で CLASSPATH 変数が定義されていない場合は、CLASSPATH 変数を作成します。

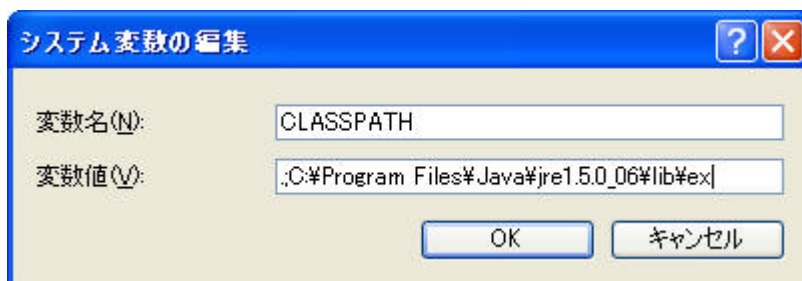


図 47 Windows OS: CLASSPATH 変数

Linux OS 変数の設定

現在のユーザのみに Java を設定する場合は、「/home/Username」フォルダにある「.profile」ファイルを開き、編集します。

すべてのユーザに対して Java を設定する場合は、お使いのコンピュータの「/etc」フォルダにある「.profile」ファイルを開きます。

1. PATH を設定するラインを見つけます。

例: `export PATH=$PATH:/home/username/somefolder`

2. このラインの前に「JAVA_HOME」を設定し、これを PATH に含めるよう変更します。
そのためには、次のラインを追加します。

export

JAVA_HOME=/home/username/j2sdk1.4.2/

export PATH=\$PATH:\$JAVA_HOME/bin

3. ファイルを保存して、設定を完了します。

UNIX OS 変数の設定

Sun Solaris に最新の JRE バージョンがインストールされていることを確認するには、次の手順を行います。

1. Sun Solaris デスクトップのターミナル ウィンドウを起動します。
2. コマンドラインで「`java -version`」と入力し、**Enter** キーを押します。現在インストールされている Java Runtime Environment(JRE)のバージョンが表示されます。
 - パス変数が Java バイナリのインストールされている場所に設定されていない場合は、JRE のバージョンが表示されないことがあります。
 - パスを設定する場合: PATH 変数を設定する必要があります。ここでは、JRE 1.4.2_05 が「/usr/local/java」にインストールされていると仮定します。
 - bash シェルのパスを設定する場合:
`export PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin.`
 - tcsh または csh のパスを設定する場合:
`set PATH =($PATH /usr/local/java/j2re1.4.2_05/bin).`
 - これらのコマンドは、ログイン時にターミナルに入力することもできますが、コマンドを、bash シェルの場合は「.bashrc」に、csh または tcsh の場合は「.cshrc」に追加することもできます。追加しておく、ログイン時に PATH がすでに設定された状態になります。詳細については、お手元のシェルに関する文書を参照してください。



図 48 Sun Solaris の JRE バージョンの確認

3. JRE がバージョン 1.4.2_05 以降(ただし、バージョン 1.5.0_02 を除く)の場合は、RSC のインストールを続行します。バージョンが古い場合は、Sun の Web サイト(<http://java.sun.com/products/>)にアクセスし、最新の Runtime Environment をダウンロードします。

Windows へのスタンドアロン RSC のインストール

RSC をインストールするには管理者特権が必要です。

1. Windows コンピュータにログオンします。
2. インストール ファイル RSC-installer.jar をダウンロード(場所がわかっている場合はそこからコピー)します。
3. 実行可能ファイルをダブルクリックして、インストール プログラムを起動します。スプラッシュ画面が表示されます。
4. [Next(次へ)]をクリックします。インストール パスを指定する画面が表示されます。
5. 必要に応じて、パスを変更します。
6. [Next(次へ)]をクリックします。インストールの進捗状況を表す画面が表示されます。

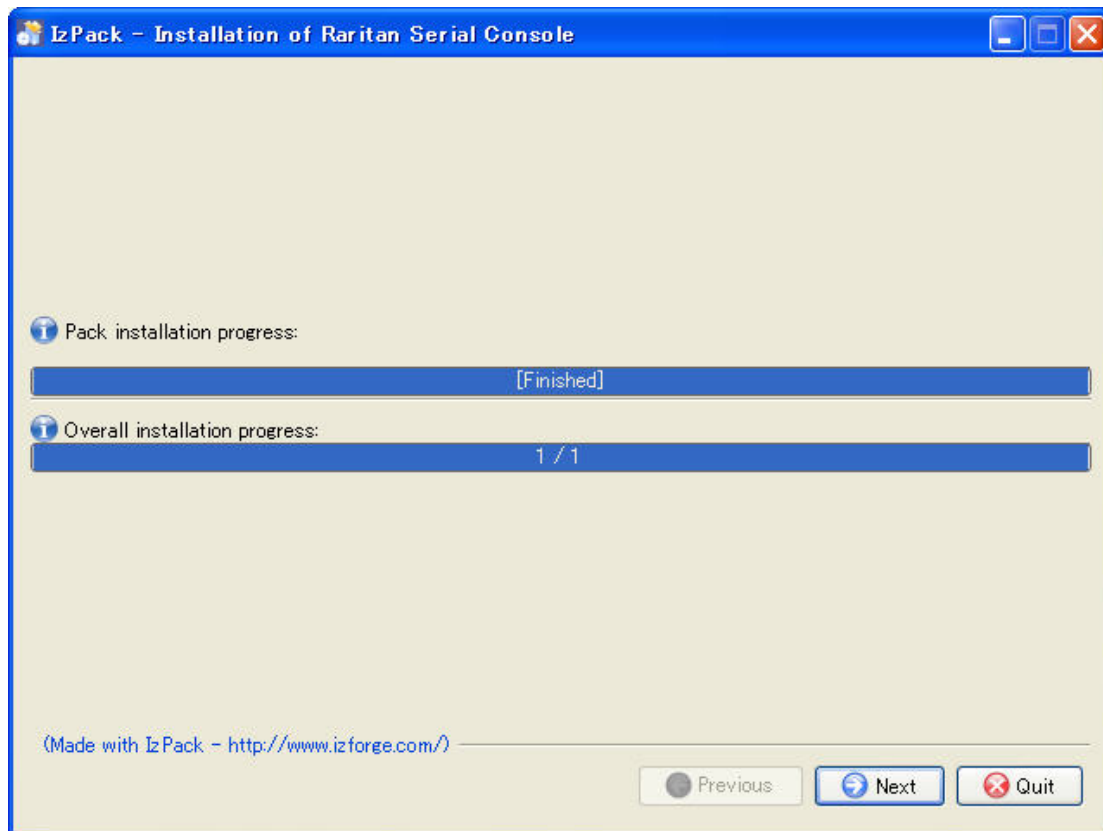


図 49 Windows における RSC インストールの進捗状況画面

7. [Next(次へ)]をクリックします。Windows のショートカットを指定する画面が表示されます。

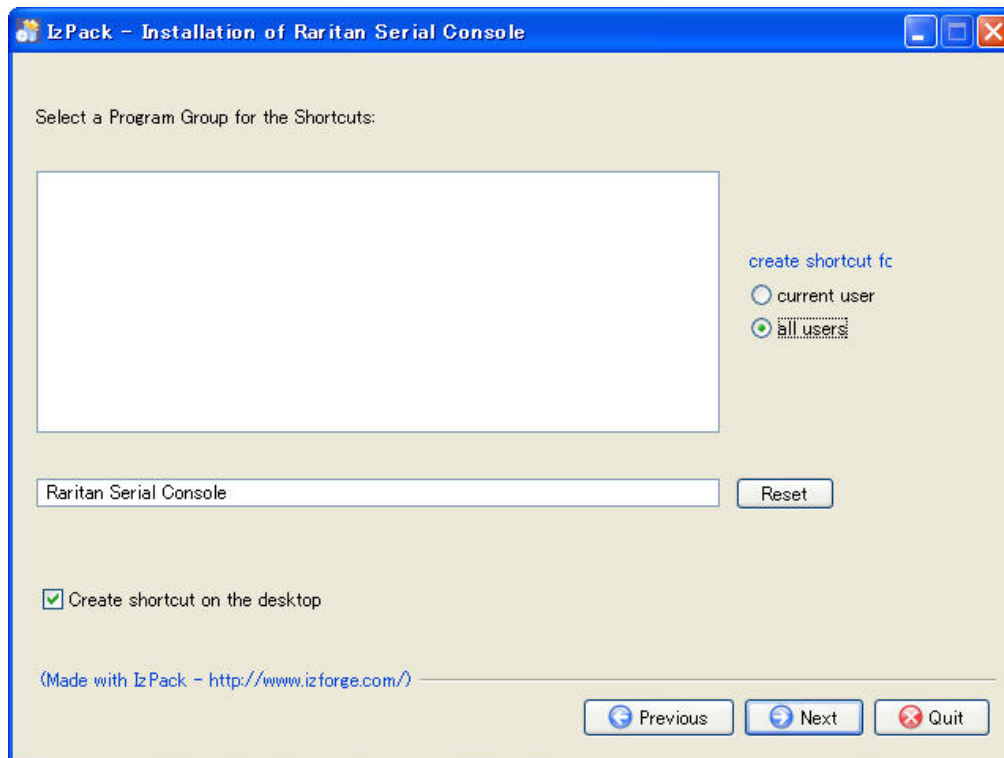


図 50 RSC の Windows ショートカット指定画面

8. ショートカットのプログラム グループを指定します。
9. [Next(次へ)]をクリックします。インストールの完了を報告する画面が表示されます。
10. [Done(終了)]をクリックします。

Windows システムにおける RSC の起動

1. ショートカットをダブルクリックするか、[スタート]ボタン、[プログラム]の順にクリックして、スタンドアロン RSC を起動します。Raritan Serial Console へのログイン接続プロパティ ウィンドウが表示されます。



図 51 スタンドアロン RSC ログイン画面

2. Dominion SX IP アドレス、アカウント情報、およびターゲット(ポート)を入力します。
3. [開始]をクリックします。ポートに接続された状態で RSC が開きます。

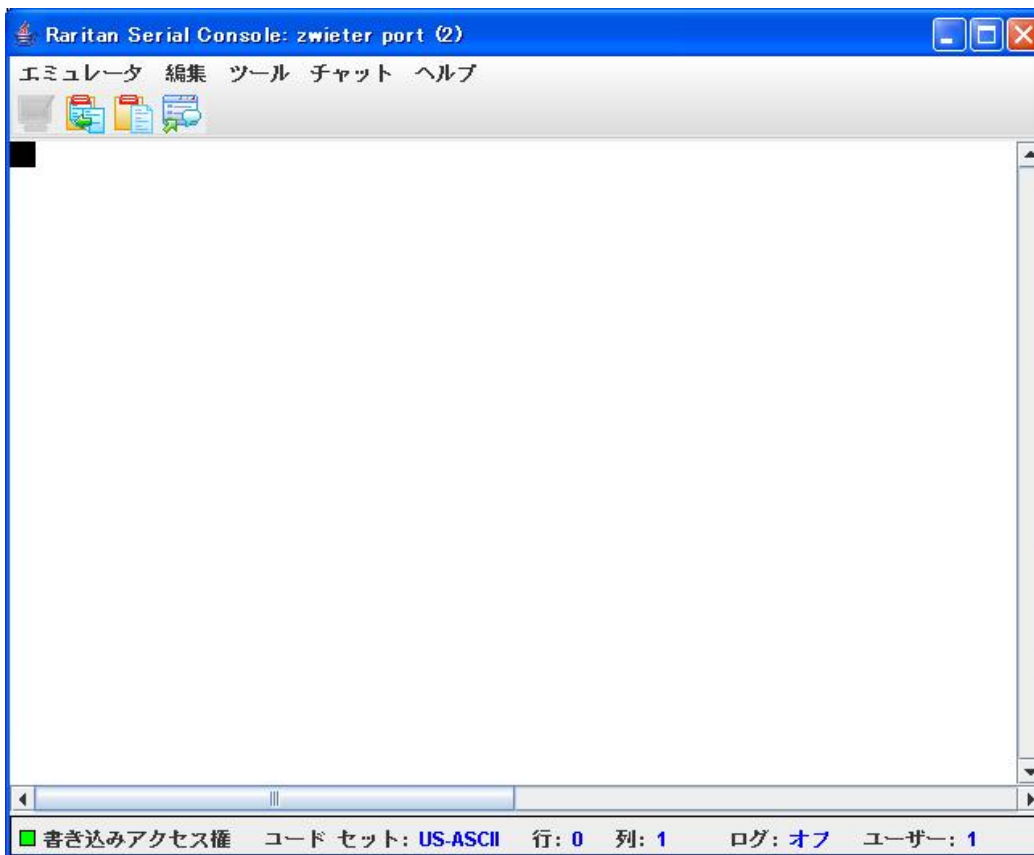


図 52 ポートに接続されたスタンドアロン RSC ウィンドウ

注 ローカライズのサポートが原因で、RSC ウィンドウに認識できない文字が表示されたり、画面がぼやけたりする場合は、フォントを Courier New に変えてみてください。変更するには、[エミュレータ]、[設定]、[表示]の順に選択し、[ターミナル フォントのプロパティ]または[GUI フォントのプロパティ]に「Courier New」を選択してください。

Sun Solaris への RSC のインストール

RSC をインストールするには管理者特権が必要です。

1. Sun Solaris コンピュータにログオンします。
2. インストール ファイル RSC-installer.jar をダウンロード(場所がわかっている場合はそこからコピー)します。
3. ターミナル ウィンドウを開き、インストーラが保存されているディレクトリに移動します。
4. 「`java -jar RSC-installer.jar`」と入力して ENTER キーを押し、インストーラを実行します。
5. 初期画面が起動したら、[Next(次へ)]をクリックします。

6. Set Installation Path(インストール パスの設定)画面が表示されます。
 - a) RSC をインストールするディレクトリを選択して、[Next(次へ)]をクリックします。
 - b) [Browse(参照)]をクリックして、デフォルト以外のディレクトリに移動します。
 - c) インストールが完了したら、[Next(次へ)]をクリックします。
 - d) もう一度[Next(次へ)]をクリックします。これでインストールが完了しました。最終画面にアンインストール プログラムの場所と、自動インストール スクリプトを生成するオプションが表示されます。
 - e)[Done(終了)]をクリックして、インストール ウィンドウを閉じます。

Sun Solaris における RSC の起動

1. ターミナル ウィンドウを開き、RSC をインストールしたディレクトリに移動します。
2. 「./start.sh」と入力して ENTER キーを押し、RSC を起動します。
3. デバイスをダブルクリックして接続を確立します。
4. ユーザ名とパスワードを入力します。
5. [OK]をクリックしてログインします。

空白ページ

第 8 章: セキュリティ

コンソール サーバのセキュリティに対応するには、多くの考慮すべき要素があります。セキュリティに関するいくつかの側面を以下に示します。

- オペレータ コンソールおよび DSX 本体間で送信されるデータ トラフィックを暗号化する。
- ユーザの認証と承認を行う。
- 操作に関するデータをログに記録して、後でそれを監査目的で参照できるようにする。場合によっては、行政機関の規制または社内規定に準拠するためにこのデータが必要になります。
- リモート NFS サーバに送信されるポート データ ログを暗号化する。
- セキュリティ プロファイル。
- 「Man in the Middle 攻撃」。

Dominion SX の管理者には、次のツールを使用したセキュリティ機能が提供されます。

- ログイン認証および処理パラメータの指定
- Kerberos 設定
- 証明書の仕様
- 表示するバナー
- セキュリティ プロファイルの管理
- ファイアウォール ルールの管理

セキュリティ設定

[Security(セキュリティ)]タブを選択して、セキュリティ関連ツールを表示します。Security Settings(セキュリティ設定)画面が表示されます。



図 53 Security Settings(セキュリティ設定)画面

ログイン設定

Security Settings(セキュリティ設定)画面の[Login Settings(ログイン設定)]をクリックすると、Login Settings(ログイン設定)画面が表示されます。この画面には、[Local Authentication(ローカル認証)]、[Login Handling(ログイン処理)]、および[Strong Password Settings(強力なパスワード設定)]の各パネルが表示されます。

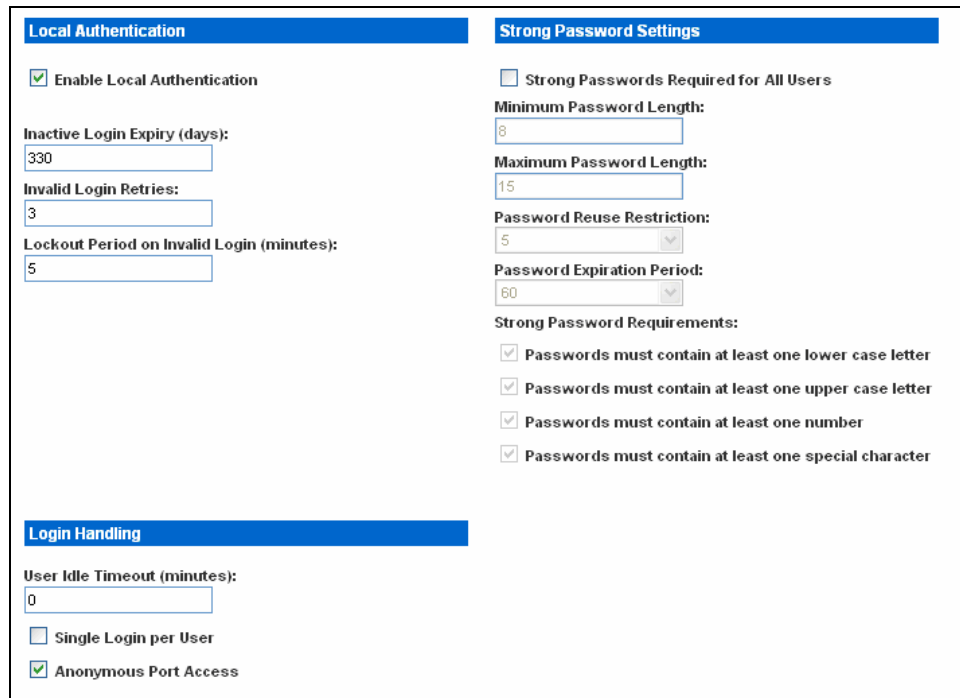


図 54 Login Settings(ログイン設定)画面

ローカル認証

1. Local Authentication(ローカル認証)パネルに移動し、[Enable Local Authentication(ローカル認証を有効にする)]チェック ボックスをオンにします。
2. 次の各フィールドには、ローカル認証のデフォルト値が表示されます。
 - **Inactive Login Expiry(days): 330**
 - **Invalid Login Retries: 3**
 - **Lockout Period on Invalid Login(minutes): 5**
3. システムのデフォルト値を受け入れるか、独自の値を入力します。

ログイン処理

1. Login Handling(ログイン処理)パネルに移動して、User Idle Timeout(minutes)(ユーザ アイドルタイムアウト(分))フィールドに値を入力します。これは、ユーザがタイムアウトとなる休止状態の長さ(期間)を示します。デフォルトは0です。これは、この機能が事実上無効であることを示しています。
2. 単一ログインのみを有効にするには、[Single Login per User(ユーザごとに単一ログインのみを許可する)]チェック ボックスをオンにします。一度に1人のユーザだけが同じプロファイルを使用してログインできます。
3. [Anonymous Port Access(匿名ポート アクセス)]チェック ボックスをオンにして、この機能を有効にします。匿名ユーザ グループはデフォルトで作成されています。このグループは、管理者であって

も削除することはできません。このグループは、[Anonymous Port Access(匿名ポート アクセス)]がオンの場合はグループ リストに表示され、オフの場合は表示されません。

注 匿名ポート アクセスの詳細については、第 7 章を参照してください。

強力なパスワード設定

強力なパスワードを有効にするには、Strong Password Settings(強力なパスワード設定)パネルに移動して、強力なパスワードの要件を選択します。最大長と最小長、および特殊文字の要件を指定できます。

Kerberos 設定

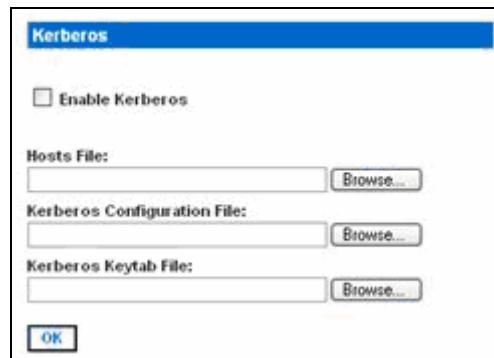


図 55 Kerberos 設定

1. [Enable Kerberos(Kerberos を有効にする)]チェック ボックスをオンにします。
2. **Hosts File**(ホスト ファイル)フィールドに、ホスト ファイルに付ける名前を入力するか、[Browse(参照)]ドロップダウン メニューをクリックしてファイルを選択します。
3. **Kerberos Configuration File**(Kerberos 設定ファイル)フィールドに、Kerberos 設定ファイルに付ける名前を入力するか、[Browse(参照)]ドロップダウン メニューをクリックしてファイルを選択します。
4. **Kerberos Keytab File**(Kerberos キータブ ファイル)フィールドに、Kerberos キータブ ファイルに付ける名前を入力するか、[Browse(参照)]ドロップダウン メニューをクリックしてファイルを選択します。
5. [OK]をクリックします。

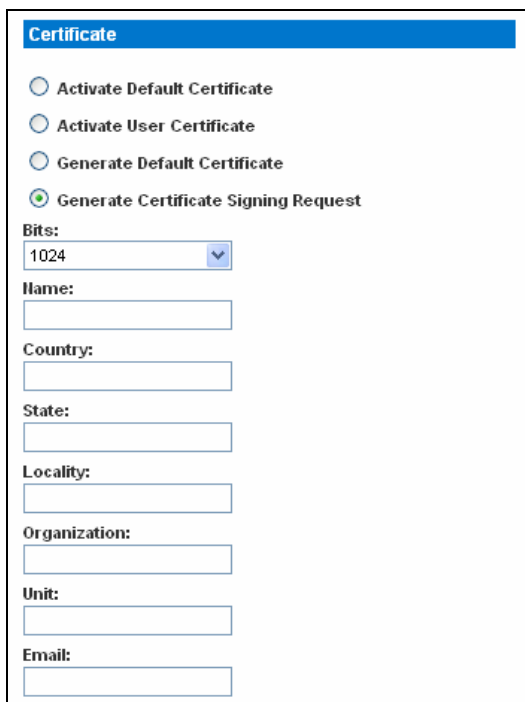
証明書

証明書機能を使用して、証明書署名リクエスト(CSR)の生成、DSX へのユーザ キーのインストール、および DSX へのユーザ証明書のインストールを行うことができます。

証明書署名リクエストの生成

証明書署名リクエスト(CSR)を生成するには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Certificate(証明書)]をクリックします。Certificate(証明書)画面が表示されます。



The screenshot shows a window titled "Certificate" with a blue header. It contains four radio button options: "Activate Default Certificate", "Activate User Certificate", "Generate Default Certificate", and "Generate Certificate Signing Request" (which is selected). Below these are several input fields: "Bits" (a dropdown menu set to "1024"), "Name:", "Country:", "State:", "Locality:", "Organization:", "Unit:", and "Email:".

図 56 証明書署名リクエスト

2. [Generate a Certificate Signing Request(証明書署名リクエストの生成)]チェック ボックスをオンにします。
3. Bits(ビット)フィールドのドロップダウン メニューをクリックします。デフォルトの「1024」のままにするか、「512」に変更します。
4. 対応するフィールドに次の情報を入力します。
 - 名前
 - 国
 - 州
 - ローカリティ(地域)
 - 部署
 - 電子メール アドレス
5. デフォルトの証明書または CSR を表示するには、該当するラジオ ボタンをクリックします。
6. [OK]をクリックします。CSR が生成されます。

ユーザ キーのインストール

DSX にユーザ キーをインストールするには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Certificate(証明書)]をクリックします。Certificate(証明書)画面が表示されます。



図 57 Install User Key(ユーザ キーのインストール)

2. [Install User Key(ユーザ キーのインストール)]チェック ボックスをオンにします。
3. 対応するフィールドに次の情報を入力します。
 - キーを使用するホストの IP アドレス
 - ホストでのログイン名とパスワード
 - キーが含まれるファイルのパスとファイル名
4. [OK]をクリックします。

ユーザ証明書のインストール

DSX にユーザ証明書をインストールするには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Certificate(証明書)]をクリックします。Certificate(証明書)画面が表示されます。




図 58 Install User Certificate(ユーザ証明書のインストール)

2. [Install User Certificate(ユーザ証明書のインストール)]チェック ボックスをオンにします。
3. 対応するフィールドに次の情報を入力します。
 - 証明書を使用するホストの IP アドレス
 - ホストでのログイン名とパスワード
 - 証明書が含まれるファイルのパスとファイル名
4. [OK]をクリックします。

SSL クライアント証明書

SSL セキュリティ証明書は、接続先のデバイスが接続を認可されたデバイスであることを確認するために、ブラウザ アクセスで使われます。SSL 証明書の詳細については、「付録 C: 証明書」を参照してください。このセクションでは、証明書の設定方法についてのみ説明します。SSL 証明書の詳細については、次の URL を参照してください。

<http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.msp?mfr=true>

Enable SSL Client Certificates

Install Certificate Authority

IP Address:

Login:

Password:

Remote Path:

Remote File:

CA Name:

Remove Certificate Authority

CA Name:

View Certificate Authority

CA Name:

Add Certificate Revocation List

IP Address:

Login:

Password:

Remote Path:

Remote File:

Url:

CRL Name:

Delete Certificate Revocation List

CRL Name:

View Certificate Revocation List

CRL Name:

図 59 SSL Client Certificate(SSL クライアント証明書)画面

クライアント証明書による認証の有効化

クライアント証明書による認証を有効するには、次の手順に従います。

1. [Enable SSL Client Certificates(SSL クライアント証明書を有効にする)]チェック ボックスをオンにします。
2. [OK]をクリックして、クライアント証明書による認証を有効にします。

新しい信頼できる証明機関のインストール

新しい信頼できる証明機関(CA)を DSX にインストールするには、アクセス可能な FTP サーバ上にその CA 証明書が存在している必要があります。

1. [Install Certificate Authority(証明機関のインストール)]チェック ボックスをオンにします。
2. FTP サーバから証明書を取得するのに必要なデータを入力します。
3. [OK]をクリックして CA 証明書を取得し、DSX にインストールします。

ユーザが追加した証明機関の削除

ユーザが追加した CA を DSX から削除するには、次の手順に従います。

1. [Remove Certificate Authority(証明機関の削除)]チェック ボックスをオンにします。
2. CA Name(CA 名)フィールドに、CA 証明書を追加したときに指定した名前を入力します。
3. [OK]をクリックして証明書を削除します。

証明機関の表示

CA を表示するには、次の手順に従います。

1. [View Certificate Authority(証明機関の表示)]チェック ボックスをオンにします。
2. CA Name(CA 名)フィールドに、表示する CA の名前を入力します。
3. [OK]をクリックして、CA のリストを取得します。

クライアント証明書失効リスト(CRL)の管理

DSX には、VeriSign および Thawte CA の各証明書と、CRL があらかじめインストールされています。ユーザがカスタムの CA を DSX に追加した場合、失効した証明書を追跡するために、対応する CRL を追加する必要があります。失効したときに CRL を自動的に取得する場合は、DSX が接続可能な Web サーバから取得する必要があります。

DSX への新しい証明書失効リストの追加

新しい CRL を DSX に追加するには、アクセス可能な FTP サーバ上に CRL リストが存在している必要があります。

1. [Add Certificate Revocation List(証明書失効リストの追加)]をクリックします。
2. FTP サーバにアクセスするための情報をフィールドに入力します。
 - CRL Name(CRL 名)フィールドには、CA の追加時に使用した名前と同じ名前を入力します。
 - URL フィールドには、HTTP サーバの IP アドレスを数値ドット表記で入力します。
3. [OK]をクリックして、CRL を追加します。

DSX からの証明書失効リストの削除

SX から CRL を削除するには、次の手順に従います。

1. [Delete Certificate Revocation List(証明書失効リストの削除)]チェック ボックスをオンにします。
2. CRL Name(CRL 名)フィールドに、この CRL が属する CA の名前を入力します。
3. [OK]をクリックして、CRL を削除します。

証明書失効リストの表示

CRL を表示するには、次の手順に従います。

1. [View Certificate Revocation List(証明書失効リストの追加)]チェック ボックスをオンにします。
2. [OK]をクリックして、CRL のリストを取得します。

バナー

Dominion SX では、ログイン後に表示されるカスタマイズ可能な「Welcome(ようこそ)」バナー(最大 5000 ワード、各行 8 ワード以下)がオプションでサポートされます。バナーにより、ユーザがログインした場所を識別できます。さらに、承諾バナーを追加して、ユーザがコンソール サーバの操作に進む前に、提示された条件を受諾するように求めることもできます。

図 60 Banner(バナー)画面

1. 次のフィールドのいずれかをオンにします。
 - Display Restricted Service Banner(制限付きサービス バナーを表示する)
 - Require Acceptance of Restricted Service Banner(制限付きサービス バナーの承諾が必要)
2. 次のフィールドのいずれかをオンにします。
 - Restricted Service Banner Message(制限付きサービス バナー メッセージ)
 - Restricted Service Banner File(制限付きサービス バナー ファイル)

3. **[Restricted Service Banner File(制限付きサービス バナー ファイル)]**をオンにした場合は、**[参照]**ドロップダウン メニューをクリックします。
4. DSX ログイン画面で表示する制限付きサービス バナー メッセージが含まれるファイルを探して選択します。
5. **[OK]**をクリックします。

セキュリティ プロファイル

DSX には、3 種類のセキュリティ プロファイルが用意されています。これらのプロファイルでは、すべてのユーザに自動的に適用される基本的な許可を定義することにより、ユーザおよびグループに許可を簡単に割り当てることができます。

セキュリティ プロファイルについて

3 種類のセキュリティ プロファイルは以下のとおりです。

- Standard(標準) – 「カスタム」のデフォルトです。
- Secure(セキュア) – 「カスタム」のすべての機能がオンになっています。
- Custom(カスタム) – ユーザが設定できるプロファイルです。

標準プロファイルまたはセキュア プロファイルを有効にした場合は、いずれの機能も有効または無効に手動で切り替えることはできません。そのような変更を加えるには、プロファイルを無効にする必要があります。

あるプロファイルが無効にした場合、そのプロファイルで設定されていた機能はプロファイルが有効であったときの状態のまま保持されます。たとえば、デフォルトの[TLS Required(TLS が必要)]機能をオフにして、セキュア プロファイルを有効にした場合、この機能はオンになります。その後、セキュア プロファイルを無効にしても、[TLS Required(TLS が必要)]機能はオンのままになります。

セキュリティ プロファイルの選択

セキュリティ プロファイルを選択するには、次の手順に従います。

1. **[Security(セキュリティ)]**タブをクリックし、**[Security Profiles(セキュリティ プロファイル)]**をクリックします。Security Profiles(セキュリティ プロファイル)画面が表示されます。

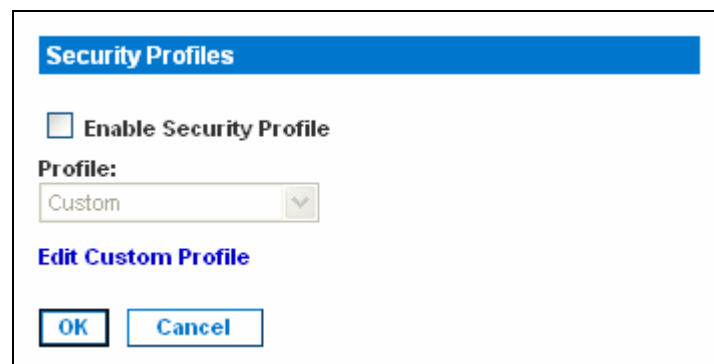


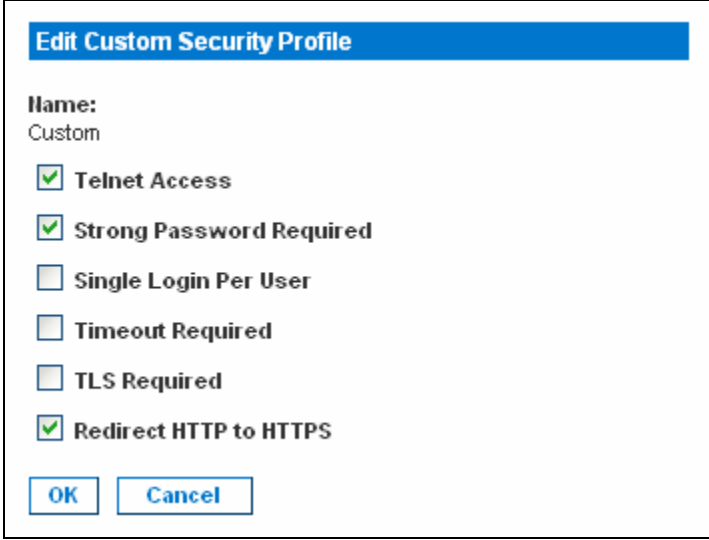
図 61 Security Profiles(セキュリティ プロファイル)

2. **[Enable Security Profile(セキュリティ プロファイルを有効にする)]**チェック ボックスをオンにします。
3. **Profile(プロファイル)**フィールドのドロップダウン メニューからプロファイルを選択します。
4. **[OK]**をクリックします。

カスタム プロファイルの編集

カスタム プロファイルを編集するには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Security Profiles(セキュリティ プロファイル)]をクリックします。Security Profiles(セキュリティ プロファイル)画面が表示されます。
2. [Edit Custom Profile(カスタム プロファイルの編集)]リンクをクリックします。Edit Custom Security Profile(カスタム プロファイルの編集)画面が表示されます。



Edit Custom Security Profile

Name:
Custom

Telnet Access

Strong Password Required

Single Login Per User

Timeout Required

TLS Required

Redirect HTTP to HTTPS

図 62 Edit Custom Security Profile(カスタム セキュリティ プロファイルの編集)画面

3. 次のフィールドのいずれか、またはすべてをオンにします。
 - Telnet Access(Telnet アクセス)
 - Strong Password Required(強力なパスワードが必要)
 - Single Login Per User(ユーザごとに単一ログインのみを許可する)
 - Timeout Required(タイムアウトの設定が必要)
 - TLS Required(TLS が必要)
 - Redirect HTTP to HTTPS(HTTP を HTTPS にリダイレクトする)
4. [OK]をクリックします。

ファイアウォール

DSX にはファイアウォール機能が用意されており、IP ネットワークを保護し、内部ルータと LAN 1、LAN 2、およびダイヤル モデム インタフェースの間のアクセスの制御を行うことができます。

ファイアウォールの有効化

ファイアウォールを有効にするには、次の手順に従います。

1. [Security(セキュリティ)]タブをクリックし、[Firewall(ファイアウォール)]をクリックします。Firewall(ファイアウォール)画面が表示されます。Firewall(ファイアウォール)画面には、既存の IPTables ルールが表示されます。

Firewall		Add / Delete IPTables Rule	
<input type="checkbox"/> Enable Firewall		IPTables Command:	
OK	Cancel	Apply	Cancel
IPTables Rules			
Chain INPUT (policy ACCEPT)			
target	prot opt source		destination
Chain FORWARD (policy ACCEPT)			
target	prot opt source		destination
Chain OUTPUT (policy ACCEPT)			
target	prot opt source		destination
Save			

図 63 Firewall(ファイアウォール)画面

2. [Enable Firewall(ファイアウォールを有効にする)]チェック ボックスをオンにします。
3. [OK]をクリックします。

注 二重化 LAN 本体の IP 転送を有効にする場合は、IPTables ルールを使用して LAN インタフェース間で転送されるトラフィックのポリシーを作成してください。

IPTables ルールの追加

IPTables ルールを追加するには、次の手順に従います。

1. **[Security(セキュリティ)]**タブをクリックし、**[Firewall(ファイアウォール)]**をクリックします。Firewall(ファイアウォール)画面が表示されます。Firewall(ファイアウォール)画面には、デフォルトのIPTables ルールが表示されます。
2. **Add/Delete IP Tables Rule**(IPTables ツールの追加または削除)フィールドに移動して、ルールを入力します。
3. **[Apply(適用)]**をクリックし、**[Save(保存)]**をクリックします。追加ルールが画面に表示されます。
4. 必要な場合は、デフォルト ルールの一部またはすべてを削除します。
5. 必要な場合は、新しいルールを追加します。

注 ルールは、*IPTables* コマンドを使用してカーネルに追加されます。これらのルールはすぐに適用されますが、**[Save(保存)]**ボタンをクリックした場合のみ恒久的に保持されます。

注 ルールに誤りがある場合、結果として本体にアクセスできなくなります。保存アクションにより、ルールに誤りがあった場合に元の状態に戻すことが可能になります。システムをリポートしてください。ルールを保存しなかった場合、リポート時にそれらのルールは失われます。

第 9 章: ログ

この章では、各種の DSX ログを有効化および設定する方法について説明します。

ローカル イベント ログの設定

ローカル ログ設定を行うには、[Setup(セットアップ)]タブをクリックして[Log(ログ)]をクリックします。Log Settings(ログ設定)画面が表示されます。この画面には、個別のログ パネルが多数含まれています。

イベント ログ ファイルの有効化

この機能を使って、イベント ログ メッセージを DSX 本体にローカルで保存できます。この機能を設定するには、次の手順に従います。

1. Event Log(イベント ログ)パネルに移動し、[**Enable Event Log File**(イベント ログ ファイルを有効にする)]チェック ボックスをオンにします(この機能を無効にするには、このチェック ボックスをオフにします)。

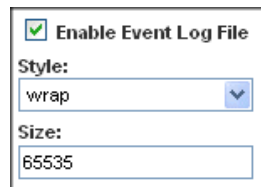


図 64 Event Log(イベント ログ)パネル

2. **Style**(スタイル)フィールドで、ログ ファイルのスタイルを選択します。これにより、ファイル サイズが最大に達したときのファイルの処理方法が決まります。次のいずれかを選択します。
 - **wrap**: このスタイルを選択すると、ログ ファイルの最後に到達したときにファイルの先頭に戻ってログを記録します。
 - **flat**: このスタイルを選択すると、ファイルの最後に到達したときにログの記録を停止します。
3. **Size**(サイズ)フィールドに、ファイルの最大サイズを入力します。デフォルトのサイズは 65535 バイトです。
4. [OK]をクリックします。

システム ログの有効化

この機能では、イベント ログ メッセージをリモートの Syslog サーバに送信します。Dominion SX 本体から生成されたメッセージは、より効率的な解析を行うために Syslog サーバの LOCAL0 チャンネルに送信されます。この機能を設定するには、次の手順に従います。

1. System Logging(システム ログ)パネルに移動し、[**Enable System Logging**(システム ログを有効にする)]チェック ボックスをオンにします(この機能を無効にするには、このチェック ボックスをオフにします)。

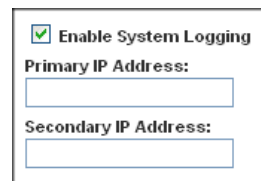


図 65 Event Log(イベント ログ)パネル

2. **Primary IP Address**(プライマリ IP アドレス)フィールドに、リモート Syslog サーバの IP アドレスを入力します。
3. バックアップの Syslog サーバがある場合は、**Secondary IP Address**(セカンダリ IP アドレス)フィールドにその IP アドレスを入力します。
4. **[OK]**をクリックします。

ポート ログの有効化

NFS ログを有効に設定した後(後の「NFS ログの設定」を参照)、ポート ログを設定する必要があります。

この機能を使って、ポート データをネットワーク ファイル システム(NFS)サーバにログを記録することができます。これにより、ネットワークを介してログ ファイルを保存し、そのログ ファイルにアクセスすることが可能になります。

NFS では、ファイル共有がサポートされます。これは、他のユーザがアクセス可能なファイルをネットワーク上に保存できると同時に、セキュリティで保護されたファイルは DSX 本体上に保持できることを意味します。NFS では、ユーザが参照できるようにポート セッションが保存されるだけでなく、ユーザがポートから接続または切断したときにメッセージが追加されます。

ポート ログを設定するには、次の手順に従います。

1. Port Logging(ポート ログ)パネルに移動し、**[Enable Port Logging(ポート ログを有効にする)]**チェック ボックスをオンにします(この機能を無効にするには、このチェック ボックスをオフにします)。

<input checked="" type="checkbox"/> Enable Port Logging
Prefix: domSX-NFS
Size (bytes): 65535
Timestamp (Interval): 20
NFS Update Frequency (seconds): 20
Out Directory: output

図 66 Port Logging(ポート ログ)パネル

2. **Prefix**(プレフィックス)フィールドに、NFS サーバ上のポート データ ファイルの名前に付けるプレフィックスを入力します。
3. **Size**(サイズ)フィールドに、許可する最大のファイル サイズを入力します。このサイズに達すると、ポート ログ データを保存するために、新しいファイルが作成されます。値 0 を入力した場合、新しいファイルは作成されません。
4. **Timestamp(Interval)**(タイムスタンプ(間隔))フィールドに、ログ ファイル内で次のタイムスタンプ メッセージを記録するまでの間隔(秒)を入力します。値 0 を入力した場合、ログ ファイル内のタイムスタンプが無効になります。最大値は 99999 です。このフィールドはオプションです。
5. **NFS Update Frequency(seconds)**(NFS 更新間隔(秒))フィールドに、ポート ログ ファイルで次の更新が発生するまでの間隔(秒)を入力します。データは、内部バッファがいっぱいになるか、このタイムスタンプが発生するまでバッファされます。その後、データがファイルに書き込まれます。その結果、

すべての文字が NFS サーバへの書き込みとしてトリガされるようなポート アクティビティによる、過大なネットワーク トラフィックの発生を防ぐことができます。

6. **Out Directory**(出力ディレクトリ)フィールドに、設定対象の NFS サーバ上にある、出力ポート データの書き込みを行うサブディレクトリを入力します。これはデフォルトのログ ファイルで、ユーザが参照可能なポート セッションが含まれています。
7. **[OK]**をクリックします。

図 67 に、出力ファイルの例を示します。

```

Mon Nov 06-2006 13:46:20 ----- admin connected to port-----
Mon Nov 06-2006 13:46:21 ----- admin got write access -----
Password:
Authentication failure.
Username: admin
Password:
Authentication successful.

-----

Welcome to the DominionSX.[Model: SX32]
UnitName:sx181  FirmwareVersion:3.0.1.5.1  Serial:WAOF300029
IP Address:192.168.51.181  UserIdletimeout:5min

Port Port  Port Port  Port Port
No. Name  No. Name  No. Name
1 - Port1[U] 2 - Port2[U] 3 - Port3[U]
4 - Port4[U] 5 - Port5[U] 6 - Port6[U]
7 - Port7[U] 8 - Port8[U] 9 - Port9[U]
10 - Port10[U] 11 - Port11[U] 12 - Port12[U]
13 - Port13[U] 14 - Port14[U] 15 - Port15[U]
16 - Port16[U] 17 - Port17[U] 18 - Port18[U]
19 - Port19[U] 20 - Port20[U] 21 - Port21[U]
22 - Port22[U] 23 - Port23[U] 24 - Port24[U]
25 - Port25[U] 26 - Port26[U] 27 - Port27[U]
28 - Port28[U] 29 - Port29[U] 30 - Port30[U]
31 - Port31[U] 32 - Port32[U]
Current Time: Mon Nov 6 16:34:35 2006

admin > log
admin >
-- sx240_16ports UP -- Mon Nov 06-2006 13:46:38
lgo^G
admin > logout

Username:

Mon Nov 06-2006 13:46:47 ----- admin disconnected from port -----

```

図 67 サンプル出力ファイル

入力ポート ログの設定

入力ポート ログを有効にするには、次の手順に従います。

1. Input Port Logging(ポート ログ)パネルに移動し、[**Enable Input Port Logging**(入力ポート ログを有効にする)]チェック ボックスをオンにします(この機能を無効にするには、このチェック ボックスをオフにします)。

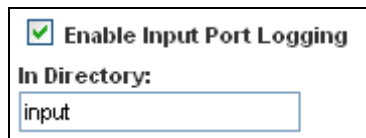


図 68 Input Port Logging(入力ポート ログ)パネル

2. **In Directory**(入力ディレクトリ)フィールドに入力用のディレクトリを入力します。
3. [**OK**]をクリックします。

暗号化の設定

暗号化の設定を行うには、次の手順に従います。

1. Encryption(暗号化)パネルに移動して、[**Encryption**(暗号化)]チェック ボックスをオンにします(この機能を無効にするには、このチェック ボックスをオフにします)。



図 69 Encryption(暗号化)パネル

2. デフォルトの暗号化キーを受け入れるか、**NFS Encryption Key(RC4)**(NFS 暗号化キー(RC4))フィールドに新しい暗号化キーを入力します。
3. [**OK**]をクリックします。

SMTP ログの設定

SMTP ログを設定するには、[Setup(セットアップ)]タブをクリックして、[Events(イベント)]をクリックします。SMTP Logging(SMTP ログ)画面が表示されます。この画面には、SMTP Settings(SMTP 設定)パネルと New SMTP Event(新規 SMTP イベント)パネルが表示されます。

SMTP ログの有効化

SMTP ログを有効にするには、次の手順に従います。

1. SMTP Settings(SMTP 設定)パネルに移動し、[Enable SMTP Server(SMTP サーバを有効にする)]チェック ボックスをオンにして SMTP ログを有効にします。



図 70 SMTP Settings(SMTP 設定)パネル

2. **SMTP Server IP Address**(SMTP サーバの IP アドレス)フィールドに、SMTP サーバの IP アドレスを入力します。
3. **Username**(ユーザ名)フィールドおよび **Password**(パスワード)フィールドに、ユーザ名とパスワードを入力します。これらは、SMTP サーバへのアクセスに必要です。
4. **Source Address**(ソース アドレス)フィールドに、ソース アドレスを入力します。
5. **[OK]**をクリックします。

新しい SMTP イベントの選択

新しい SMTP イベントを選択するには、次の手順に従います。

1. **New SMTP Event**(新規 SMTP イベント)パネルに移動して、**Event**(イベント)フィールドから新規イベントを選択します。

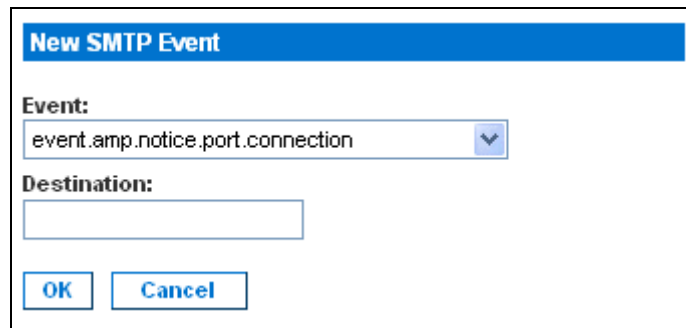


図 71 New SMTP Event(新規 SMTP イベント)パネル

選択可能なイベントは次のとおりです。

- event.amp.notice.port.connection
- event.amp.notice.user.logoff
- event.amp.notice.backup
- event.amp.notice.restore
- event.amp.notice.config.directaccesslockout
- event.amp.notice.reboot
- event.amp.notice.boot
- event.amp.notice.config.datacom
- event.amp.notice.config
- event.amp.notice.upgrade
- event.amp.keyword
- event.amp.strongpassword
- event.amp.banner
- event.amp.firewall
- event.amp.iptablesaved
- event.amp.security.clientauth
- event.amp.security.clientcert.ca
- event.amp.security.clientcert.crl.expired
- event.amp.security.clientcert.crl.updated

2. **Destination**(送信先)フィールドに、イベントの送信先電子メール アドレスを入力します。
3. [OK]をクリックします。

SMTP ログのテスト

Dominion SX 本体が SMTP サーバを使用してメッセージを送信できるようにするには、正確な SMTP サーバ情報を入力することが重要です。

情報が正しく、またメッセージの送信が正常に行われることを検証するには、次の手順に従います。

1. 次のようなイベントを選択して、テスト メールを送信します。
event.amp.notice.port connection
2. ポートに接続して、メッセージが意図された電子メールの送信先で受信されたかどうかを確認します。問題がある場合は、SMTP の管理者に問い合わせ、SMTP サーバの IP アドレスと認証情報が正しいかどうかを確認してください。

NFS ログの設定

ネットワーク ファイル システム(NFS)ログを使用して、すべてのポート アクティビティを NFS 共有ディレクトリのログに記録できます。すべてのユーザ アクティビティと、ユーザ ポート ログインおよびログアウトがログに記録されます。ログ ファイルには、次の 2 種類があります。

- **入力:** ユーザによるすべての入力(キー入力)が記録されます。
- **出力:** サーバからコンソール サーバに送信されるすべてのメッセージが記録されます。これには、管理対象デバイスまたはサーバからエコー バックされるすべてのユーザ入力も含まれます。

ポート ログも有効にする必要があります。ポート ログの詳細については、前の「ポート ログの有効化」を参照してください。

注 ポート ログが機能するには、書き込み権限を持つエクスポート ディレクトリが NFS サーバに必要です。

NFS ログを設定するには、次の手順に従います。

1. [Setup(セットアップ)]タブをクリックし、[NFS]をクリックします。NFS Settings(NFS の設定)画面が表示されます。

図 72 NFS Settings(NFS の設定)画面

2. [Enable NFS(NFS を有効にする)]チェック ボックスをオンにして、NFS ログを有効にします。
3. **Primary IP**(プライマリ IP)フィールドに NFS サーバの IP アドレスを入力し、**Primary Directory**(プライマリ ディレクトリ)フィールドにログ ファイルへのパスを入力します。
4. バックアップ NFS サーバがある場合、**Secondary IP**(セカンダリ IP)フィールドおよび **Secondary Directory**(セカンダリ ディレクトリ)フィールドにバックアップ サーバの同じ情報を入力します。プライマリ サーバに障害が発生した場合、ポート ログはセカンダリ サーバにリダイレクトされます。
5. [OK]をクリックします。

SNMP ログの設定

DSX では、簡易ネットワーク管理プロトコル(SNMP)のトラップおよびログがサポートされています。

SNMP ログの有効化

SNMP ログを有効にするには、次の手順に従います。

1. [Setup(セットアップ)]タブをクリックし、[SNMP]をクリックします。SNMP 画面が表示されます。
2. **SNMP Settings**(SNMP 設定)パネルに移動し、[Enable SNMP(SNMP を有効にする)]チェック

ボックスをオンにして SNMP 機能を有効にします。

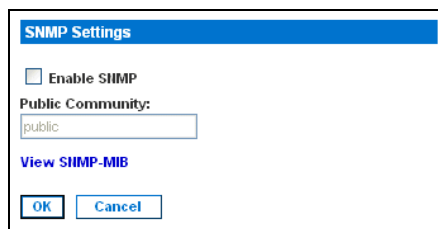

 A dialog box titled "SNMP Settings" with a blue header. It contains a checkbox labeled "Enable SHMP" which is currently unchecked. Below it is a text field labeled "Public Community:" containing the text "public". Underneath the text field is a blue link labeled "View SHMP-MIB". At the bottom of the dialog are two buttons: "OK" and "Cancel".

図 73 SNMP Settings(SNMP 設定)パネル

3. **Public Community**(パブリック コミュニティ)フィールドに、SNMP パブリック コミュニティを入力します。デフォルトは「Public」です。パブリック コミュニティにより、SNMP 警告を受け取る SNMP 管理ステーションが決まります。
4. [OK]をクリックします。

新しい SNMP 送信先の作成

SNMP 送信先により、SNMP トラップを受け取る SNMP 管理ステーションが決まります。新しい SNMP 送信先を作成するには、次の手順に従います。

1. SNMP Destination(SNMP 送信先)パネルに移動し、**IP Address**(IP アドレス)フィールドに新しい送信先の IP アドレスを入力します。


 A dialog box titled "New Destination" with a blue header. It contains two text fields: "IP Address:" and "Port:". The "Port:" field contains the number "162". At the bottom of the dialog are two buttons: "OK" and "Cancel".

図 74 SNMP Destination(SNMP 送信先)パネル

2. デフォルトでは、新しい送信先は標準の SNMP ポート番号 162 を使用します。必要に応じて別のポートに変更することもできます。その場合は、**Port**(ポート)フィールドに別のポート番号を入力します。
3. [OK]をクリックします。

注 *SNMP Management Information Base(MIB)*を表示するには、*SNMP Settings(SNMP 設定)*パネルで[View SNMP-MIB(SNMP-MIB の表示)]リンクをクリックします(図 73)。

第 10 章: メンテナンス

この章で説明する Dominion SX のメンテナンス機能を使用して、管理者は次のタスクを実行できます。

- イベントログの管理
- 設定レポートの表示
- SX 本体の設定のバックアップとリストア
- ファームウェアのアップグレードとアップグレード履歴の追跡
- 工場出荷時の設定にリセット
- 本体のリポート

ローカル イベント ログの管理

DSX では、イベント ログの内容の表示、ログのクリア、リモート FTP サーバへのログの送信を行うことができます。

ローカル イベント ログの表示

ローカル イベント ログの内容を表示するには、[Maintenance(メンテナンス)]タブをクリックし、[View Event Log(イベント ログの表示)]をクリックします。イベント ログが表示されます。図 75 に、一般的なイベント ログを示します。

Date/Time	Event
Feb 1 16:30:35	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Logging.
Feb 1 16:30:35	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 1 16:30:40	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for DominionSX.
Feb 5 11:12:23	DominionSX DomSX: DominionSX notice SXRebootCompleted
Feb 5 11:12:25	DominionSX DomSX: DominionSX notice SXSystemReady
Feb 5 11:13:24	DominionSX DomSX: DominionSX info SXUserLogin LAN Local Elaine 192.168.50.153
Feb 5 12:02:04	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for SNMP.
Feb 5 12:02:04	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 5 12:02:09	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for SNMP.
Feb 5 12:40:16	DominionSX DomSX: DominionSX notice SXUserDeleted Admin user deleted user "Tricia"
Feb 5 12:40:16	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 5 12:40:45	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Group.
Feb 5 12:53:51	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Device.
Feb 5 12:53:59	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Interface.
Feb 5 12:54:00	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for CSCDiscovery.
Feb 5 12:54:00	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for CSC.
Feb 5 12:55:23	DominionSX DomSX: DominionSX notice SXRebootCompleted
Feb 5 12:55:25	DominionSX DomSX: DominionSX notice SXSystemReady
Feb 5 12:56:20	DominionSX DomSX: DominionSX info SXUserLogin LAN Local Elaine 192.168.50.153
Feb 5 13:04:37	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.

図 75 イベント ログ

注 ログ内のイベント数が多く一度に画面に表示できない場合は、画面上部の Event Log(イベント ログ)の下に[Next(次へ)]リンクが追加され、このリンクをクリックすると次のページが表示されます。

各イベントに対して、ログにはそのイベントが記録された日時と簡単な説明が表示されます。一般的なイベントを次に示します。

Feb 5 12:55:23 DominionSX DomSX: DominionSX notice SXRebootCompleted

Feb 5 12:55:25 DominionSX DomSX: DominionSX notice SXSystemReady

Feb 1 16:30:35 DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Logging

イベント ログのクリア

イベント ログをクリアするには、次の手順に従います。

1. [Maintenance(メンテナンス)]タブをクリックし、[Clear Event Log(イベント ログのクリア)]をクリックします。クリア操作を行うかどうかを確認するプロンプトが表示されます。
2. [Yes(はい)]をクリックします。ログのすべての内容がクリアされます(クリアしない場合は[No(いいえ)]をクリックします)。

イベント ログの送信

イベント ログの内容をリモート FTP サーバに送信するには、次の手順に従います。

1. [Maintenance(メンテナンス)]タブをクリックし、[Clear Event Log(イベント ログのクリア)]をクリックします。Send Event Log(イベント ログの送信)画面が表示されます。

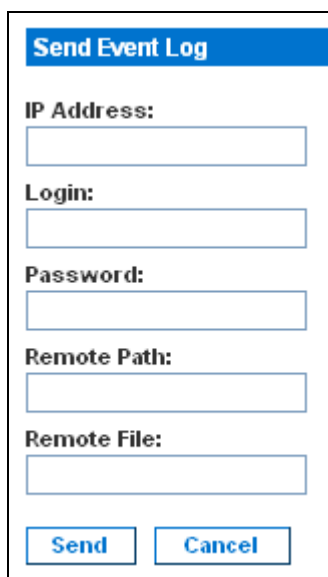


図 76 Send Event Log(イベント ログの送信)画面

2. **IP address**(IP アドレス)フィールドに、FTP サーバの IP アドレスを入力します。
3. **Login**(ログイン)および **Password**(パスワード)フィールドに、FTP サーバのログイン名とパスワードを入力します。これは、FTP サーバにアクセスするのに必要です。
4. **Remote Path**(リモート パス)フィールドに、イベント ログを保存する場所のパスを入力します。
5. **Remote File**(リモート ファイル)フィールドに、イベント ログを保存するファイル名を入力します。
6. [Send(送信)]をクリックします。

設定レポートの表示

設定レポートは、DSX 本体に関する詳細な情報が記載されているレポートです。レポートを表示するには、[Maintenance(メンテナンス)]タブをクリックし、[Configuration Report(設定レポート)]をクリックします。レポートには、次の情報が表示されます。

- バージョンおよびファームウェア情報
- ポート設定
- ユーザおよびグループ設定
- HTTP、HTTPS、SSH、および Telnet の各設定
- RADIUS、LDAP、TACACS+、および Kerberos の各設定
- ローカル認証の設定
- その他の設定

DSX のバックアップとリストア

DSX をバックアップすると、DSX 設定のコピー(ネットワーク設定を除く)が作成され、そのコピーが FTP サーバに書き込まれます。必要に応じてリストア操作を行い、ファイルを回復できます。

DSX のバックアップ

DSX 本体をバックアップするには、次の手順に従います。

1. [Maintenance(メンテナンス)]タブをクリックし、[Backup(バックアップ)]をクリックします。Backup(バックアップ)画面が表示されます。

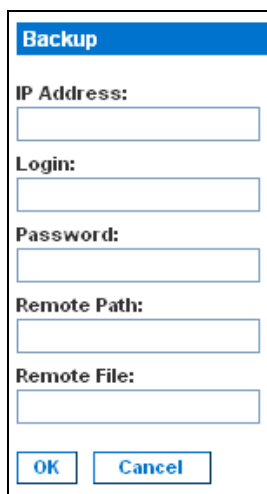


図 77 Backup(バックアップ)画面

2. **IP Address**(IP アドレス)フィールドに、バックアップを書き込むターゲット FTP サーバの IP アドレスを入力します。
3. **Login**(ログイン)フィールドに、バックアップの保存先システムでのアカウントのログイン名を入力します。
4. **Password**(パスワード)フィールドに、バックアップの保存先システムでのアカウントのパスワードを入力します。
5. **Remote Path**(リモートパス)フィールドに、バックアップファイルのパスを入力します。
6. **Remote File**(リモートファイル)フィールドに、バックアップを保存するファイルの名前を入力します。
7. [OK]をクリックします。

DSX のリストア

DSX をリストアすると、バックアップされた DSX 設定のコピーが FTP サーバから取得され、そのファイルが DSX に書き込まれます。リストア操作を実行するには、次の手順に従います。

1. **[Maintenance(メンテナンス)]**タブをクリックし、**[Restore(リストア)]**をクリックします。Restore(リストア)画面が表示されます。

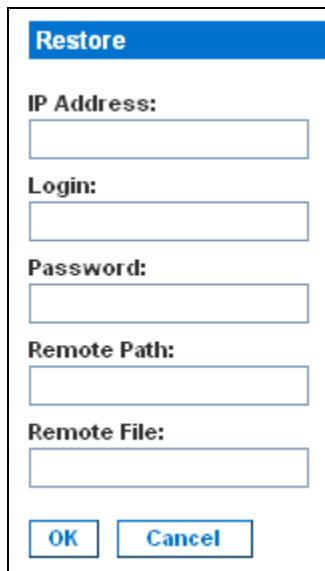


図 78 Restore(リストア)画面

2. **IP Address**(IP アドレス)フィールドに、リストア データを取得するソース FTP サーバの IP アドレスを入力します。
3. **Login**(ログイン)フィールドに、リストア データの保存先システムでのアカウントのログイン名を入力します。
4. **Password**(パスワード)フィールドに、リストア データの保存先システムでのアカウントのパスワードを入力します。
5. **Remote Path**(リモート パス)フィールドに、リストア ファイルのパスを入力します。
6. **Remote File**(リモート ファイル)フィールドに、リストア データを保存するファイルの名前を入力します。
7. **[OK]**をクリックします。

DSX ファームウェアのアップグレード

DSX で現在実行されているファームウェアのバージョンの表示、新しいバージョンへのファームウェアのアップグレード、およびファームウェアのアップグレード履歴の表示を行うことができます。

現在のファームウェア バージョンの表示

DSX 本体で実行されているファームウェアの現在のバージョンを表示するには、[Maintenance(メンテナンス)]タブをクリックし、[Firmware Version(ファームウェア バージョン)]をクリックします。Firmware Version(ファームウェア バージョン)画面が表示されます。この画面には、ファームウェア バージョン、RSC、カーネル、および PMON が表示されます。

Firmware Version	
Firmware Version:	3.1.0.1.2
RSC:	1.0.0.5.2
Kernel:	2.4.12
PMON:	2.0.1

図 79 Firmware Version(ファームウェア バージョン)

ファームウェアのアップグレード

ファームウェアのアップグレードを実行する前に、次の手順を実行する必要があります。

1. WinZip 形式のアップグレード ファイルを、ローカル FTP サーバのフォルダにダウンロードします。
2. FTP サーバの IP アドレスを取得します。
3. アップグレード ファイルへのパスを取得します。これは、FTP サーバ上に抽出されたアップグレード ファイル(たとえば、cert_pact.tgz など)へのパスです。
4. FTP サーバへの「匿名」アクセスがサポートされていない場合は、ユーザ アカウントを取得します(オプション)。

ファームウェア アップグレード機能を使用して、Dominion SX 本体のファームウェアを新しいバージョンにアップグレードすることができます。アップグレードでは、ユーザ定義設定が保持されます。アップグレードの完了後に、本体を再設定する必要はありません。

重要: アップグレード中は、本体のいかなる機能にもアクセスしないようにしてください。これはリセットおよび終了を含みますが、それだけとは限りません。アップグレード手順を中断すると、メモリ破損の原因となったり本体が機能しなくなる可能性があります。これらの行動は、保証またはサービス契約を無効にすることがあり、そのような場合は、本体の修理費または／および交換費用はすべてユーザの負担となります。

注 アップグレードの多くは FTP サーバから「匿名」で実行できます。

アップグレードを実行するには、次の手順に従います。

1. [Maintenance(メンテナンス)]タブをクリックし、[Firmware Upgrade(ファームウェアのアップグレード)]をクリックします。Firmware Upgrade(ファームウェアのアップグレード)画面が表示されます。




図 80 Firmware Upgrade(ファームウェアのアップグレード)画面

2. IP address(IP アドレス)フィールドに、FTP サーバの IP アドレスを入力します。
3. Login(ログイン)フィールドにログイン名を入力します。
4. Password(パスワード)フィールドにパスワードを入力します。
5. File Path(ファイル パス)フィールドに、ファームウェア ファイルへのパスを入力します (/home/downloads/firmware/UpgradePack_2.5.6_3.1.0.5.2/Pack1of1 など)。
6. [Upgrade(アップグレード)]をクリックします。

アップグレードには約 20 分かかります。アップグレードの約半分が終了すると、SX 本体がリポートします。リポート後、アップグレードはさらに 20 分前後続きます。

アップグレードが開始されると、アップグレード ステータス メッセージによってアップグレードの進捗状況が示されます。ファイルがコピーされ、本体はリセットされます。次のメッセージが表示されます。

Upgrade is Complete, The unit is now resetting.(アップグレードが完了しました。本体はリセットされました。)

DSX の青色のライトが消え、追加のファイルの抽出中に一度点滅した後、再度点灯し、その後は点灯したままになります。自動的にログアウトされます。その後、新しいファームウェアが実行されるようになります。

注 アップグレードに失敗した場合は、失敗の詳細を示すエラー メッセージが表示されます。

ファームウェアのアップグレード履歴の表示

DSX 本体のファームウェアのアップグレード履歴を表示するには、[Maintenance(メンテナンス)]タブをクリックし、[Firmware Upgrade History(ファームウェアのアップグレード履歴)]をクリックします。Firmware Upgrade History(ファームウェアのアップグレード履歴)画面が表示されます。画面には、これまでのファームウェア アップグレードの各バージョンと、アップグレードが実行された日時が表示されます。

Name
3.1.0.1.2 Tue Feb 20 16:15:19 2007
3.1.0.1.5 Thu Mar 15 15:14:32 2007

図 81 Firmware Upgrade History(ファームウェアのアップグレード履歴)画面

DSX でのファクトリ リセットの実行

ファクトリ リセットを実行すると、DSX 本体がデフォルトの工場出荷時の設定に戻ります。この操作を行うと、DSX 本体のすべてのデータおよび設定が消去されて出荷時の状態に戻るため、この操作の実行するときには十分に注意してください。

ファクトリ リセットを実行するには、[Maintenance(メンテナンス)]タブをクリックし、[Factory Reset(ファクトリ リセット)]をクリックします。リセットするかどうかを確認するプロンプトが表示されます。[Yes(はい)]をクリックして続行します。リセットしない場合は[No(いいえ)]をクリックします。

注 ファクトリ リセットを実行する際に、DSX GUI へのログインに必要な管理者パスワードがわからない場合は、DSX ハードウェアからのリセットを試してみてください。ハードウェアからのリセットを行うには、DSX 本体の背面パネルにある RESET ホールにピンを挿入し、そのまま約15 秒間待ちます。この操作を行うことにより、DSX が工場出荷時の設定にリセットされます。

DSX のリポート

リポートを実行すると、DSX の電源がオフになり、その後再び電源がオンになります。リポートを行うと、現在ログインしているユーザがすべてシステムからログオフされるため、この操作は注意して行ってください。

リポートを実行するには、[Maintenance(メンテナンス)]タブをクリックし、[Reboot(リポート)]をクリックします。リポートするかどうかを確認するプロンプトが表示されます。[Yes(はい)]をクリックして続行します。リポートしない場合は[No(いいえ)]をクリックします。

空白ページ

第 11 章: 診断

診断機能は、ネットワークのテストとプロセスの監視を行うツールによって管理者に提供されます。

[Diagnostics(診断)]タブを選択して、Diagnostics(診断)画面を表示します。この画面には、ネットワーク インフラストラクチャ ツールおよび管理者ツールへのリンクが表示されます。



図 82 Diagnostics(診断)画面

ネットワーク インフラストラクチャ ツール

ネットワーク インフラストラクチャ ツールを使用すると、アクティブなネットワーク インタフェースのステータスと重要なネットワーク統計を表示できます。さらに、ping やトレース ルートコマンドを実行することもできます。

アクティブなネットワーク インタフェースのステータス

1. Diagnostics(診断)画面の[Status of Active Network Interfaces(アクティブなネットワーク インタフェースのステータス)]をクリックします。アクティブなネットワーク インタフェースに関するステータス情報が表示されます。

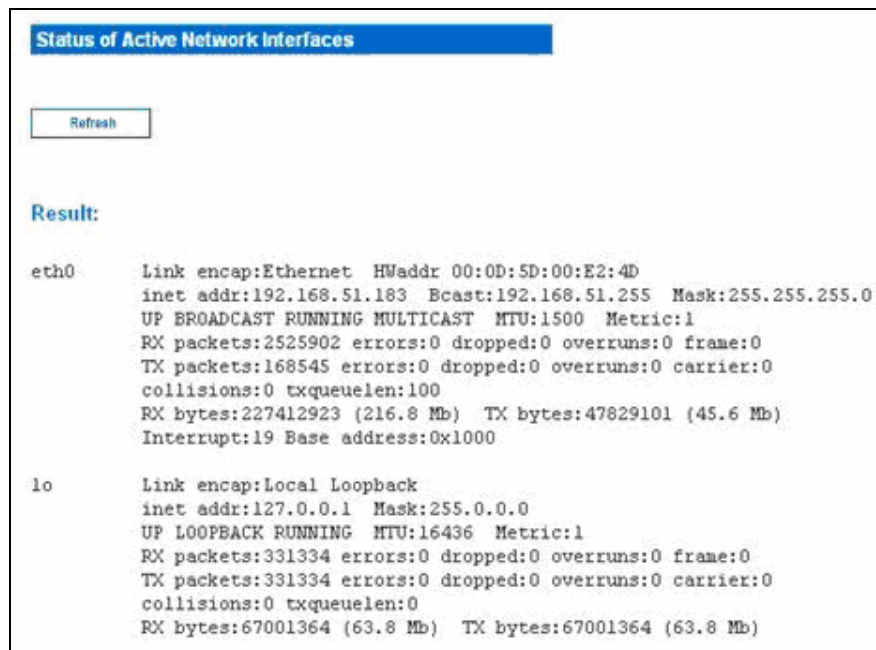


図 83 Active Network Interface Status(アクティブなネットワーク インタフェースのステータス)

2. [Refresh(更新)]をクリックして情報を更新します。

ネットワーク統計

1. **Diagnostics(診断)**画面の[Network Statistics(ネットワーク統計)]をクリックします。ネットワーク統計が表示されます。

Network Statistics

Options:
 ▼

Result:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 *:5000                  *:*                      LISTEN
tcp      0      0 *:www                   *:*                      LISTEN
tcp      0      0 *:ssh                    *:*                      LISTEN
tcp      0      0 *:telnet0                *:*                      LISTEN
tcp      0      0 *:443                    *:*                      LISTEN
tcp      0      0 192.168.50.132:443     192.168.58.88:2298     TIME_WAIT
tcp      0      0 localhost:5000          localhost:1363         ESTABLISHED
tcp      0      0 192.168.50.132:443     192.168.58.88:2299     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2296     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2297     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2302     ESTABLISHED
tcp      0      0 localhost:1363          localhost:5000         ESTABLISHED
tcp      0      0 192.168.50.132:443     192.168.58.88:2292     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2300     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2293     TIME_WAIT
tcp      0      0 192.168.50.132:443     192.168.58.88:2301     ESTABLISHED
udp      0      0 *:5000                  *:*                      LISTEN

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State      I-Node Path
unix  2      [ ACC ] STREAM   LISTENING  48       /dev/log
unix  2      [ ACC ] STREAM   LISTENING  122      /tmp/internal_rdma
unix  2      [ ACC ] STREAM   LISTENING  130      /tmp/filterSock
unix  2      [ ACC ] STREAM   LISTENING  173      /tmp/.150
unix  3      [ ]     STREAM   CONNECTED  17371    /dev/log
unix  3      [ ]     STREAM   CONNECTED  17370
unix  3      [ ]     STREAM   CONNECTED  59       /dev/log
unix  3      [ ]     STREAM   CONNECTED  47
```

図 84 Network Statistics(ネットワーク統計)

2. デフォルトでは、すべての統計が表示されます。特定の統計を表示するには、**Options(オプション)**フィールドのドロップダウンメニューからエントリを選択します。次のいずれかを選択します。
 - Route(ルート)
 - Interfaces(インタフェース)
 - Groups(グループ)
 - Statistics(統計)
 - Program(プログラム)
3. **[Refresh(更新)]**をクリックして情報を更新します。

ホストへの ping

1. Diagnostics(診断)画面の[**Ping Host**(ホストへの Ping)]をクリックします。Ping Host(ホストへの Ping)画面が表示されます。

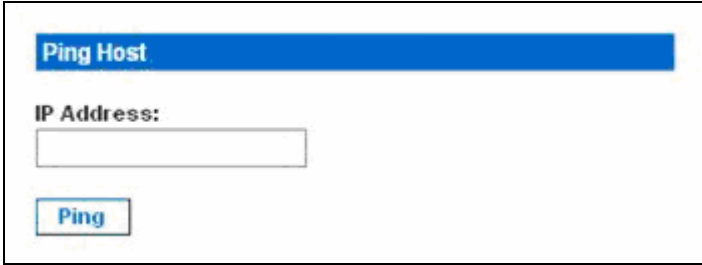


図 85 Ping Host(ホストへの Ping)

2. **IP Address**(IP アドレス)フィールドに、ping の実行先ホストの IP アドレスを入力します。
3. [**Ping**(Ping)]をクリックします。画面に ping の実行結果が表示されます。

ホストへのトレース ルート

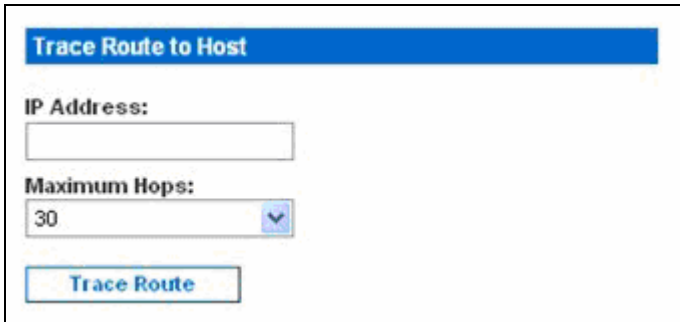
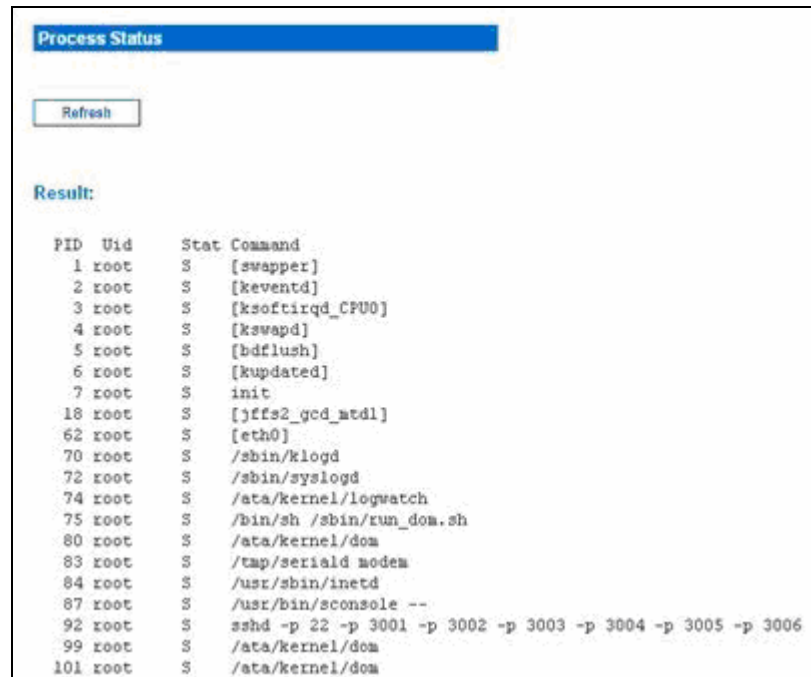


図 86 Trace Route to Host(ホストへのトレース ルート)

1. Diagnostics(診断)画面の[**Trace Route to Host**(ホストへのトレース ルート)]をクリックします。Trace Route to Host(ホストへのトレース ルート)画面が表示されます。
2. **IP Address**(IP アドレス)フィールドに、ホストの IP アドレスを入力します。
3. **Maximum Hops**(最大ホップ数)フィールドのドロップダウン メニューから、最大ホップ数を選択します。
4. [**Trace Route**](トレース ルート)をクリックします。画面にトレース ルートの実行結果が表示されます。

管理者ツール — プロセス ステータス

1. Diagnostics(診断)画面の[Process Status(プロセス ステータス)]をクリックします。画面にリクエストの実行結果が表示されます。



The screenshot shows a window titled "Process Status" with a "Refresh" button. Below the button, the word "Result:" is displayed. A table of process information is shown, with columns for PID, Uid, Stat, and Command.

PID	Uid	Stat	Command
1	root	S	[swapper]
2	root	S	[keventd]
3	root	S	[ksoftirqd_CPU0]
4	root	S	[kswapd]
5	root	S	[bdflush]
6	root	S	[kupdated]
7	root	S	init
18	root	S	[jffs2_gcd_mtd1]
62	root	S	[eth0]
70	root	S	/sbin/klogd
72	root	S	/sbin/syslogd
74	root	S	/ata/kernel/logwatch
75	root	S	/bin/sh /sbin/run_dom.sh
80	root	S	/ata/kernel/dom
83	root	S	/tap/seriald modem
84	root	S	/usr/sbin/inetd
87	root	S	/usr/bin/sconsole --
92	root	S	sshd -p 22 -p 3001 -p 3002 -p 3003 -p 3004 -p 3005 -p 3006
99	root	S	/ata/kernel/dom
101	root	S	/ata/kernel/dom

図 87 Process Status(プロセス ステータス)

2. [Refresh(更新)]をクリックして情報を更新します。

第 12 章: コマンドライン インタフェース

コマンドライン インタフェースの概要

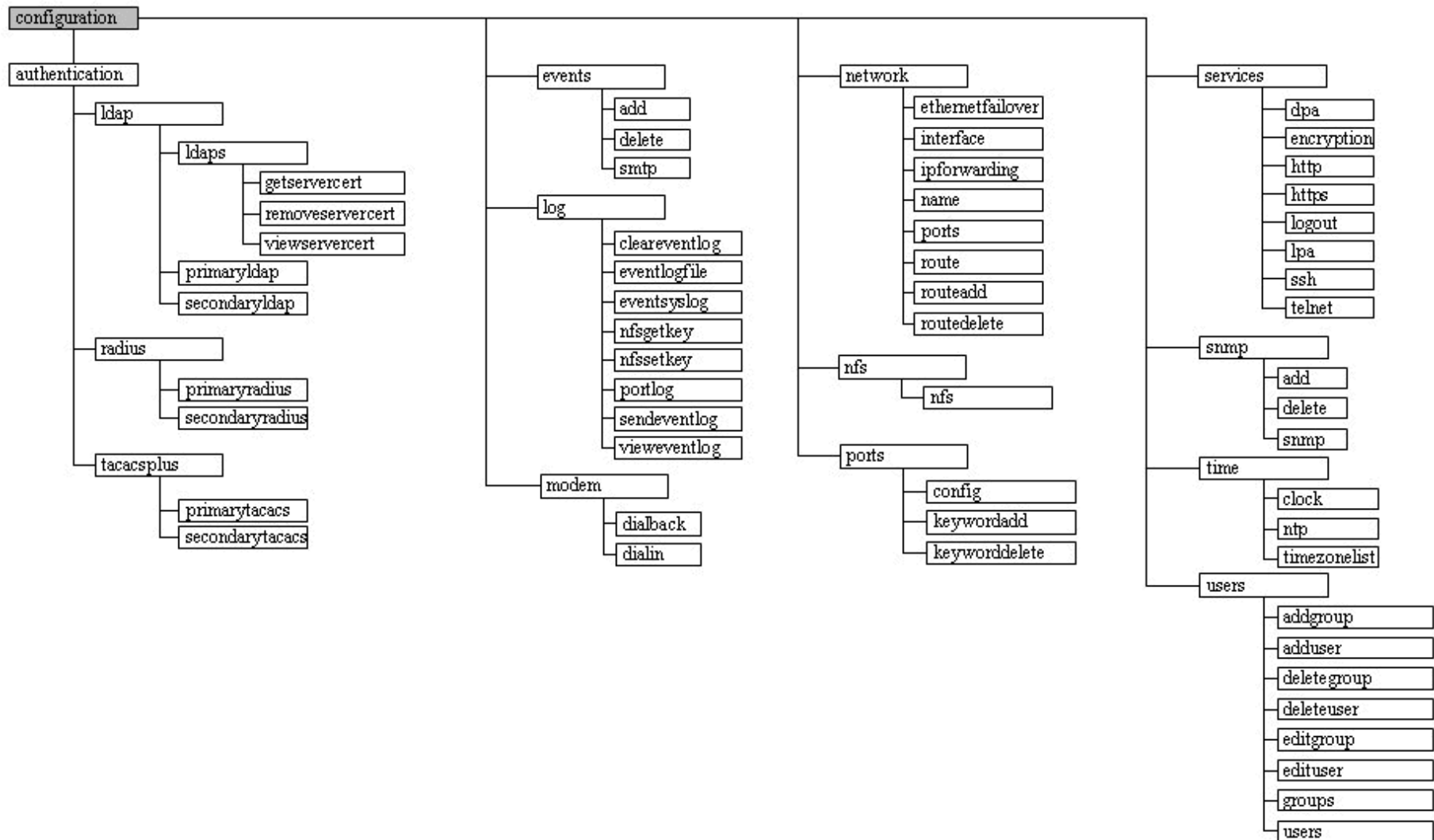
Dominion SX シリアル コンソールでは、次のようなすべてのシリアル デバイスがサポートされます。

- Windows Server 2003 などの(EMS-)緊急用コンソールとして専用システム コンソール(SAC) を使えるサーバや、サーバ BIOS の設定で SAC を利用できる機種
- ルータ
- レイヤ 2 スイッチ
- ファイアウォール
- 電源タップ
- その他のユーザ装置

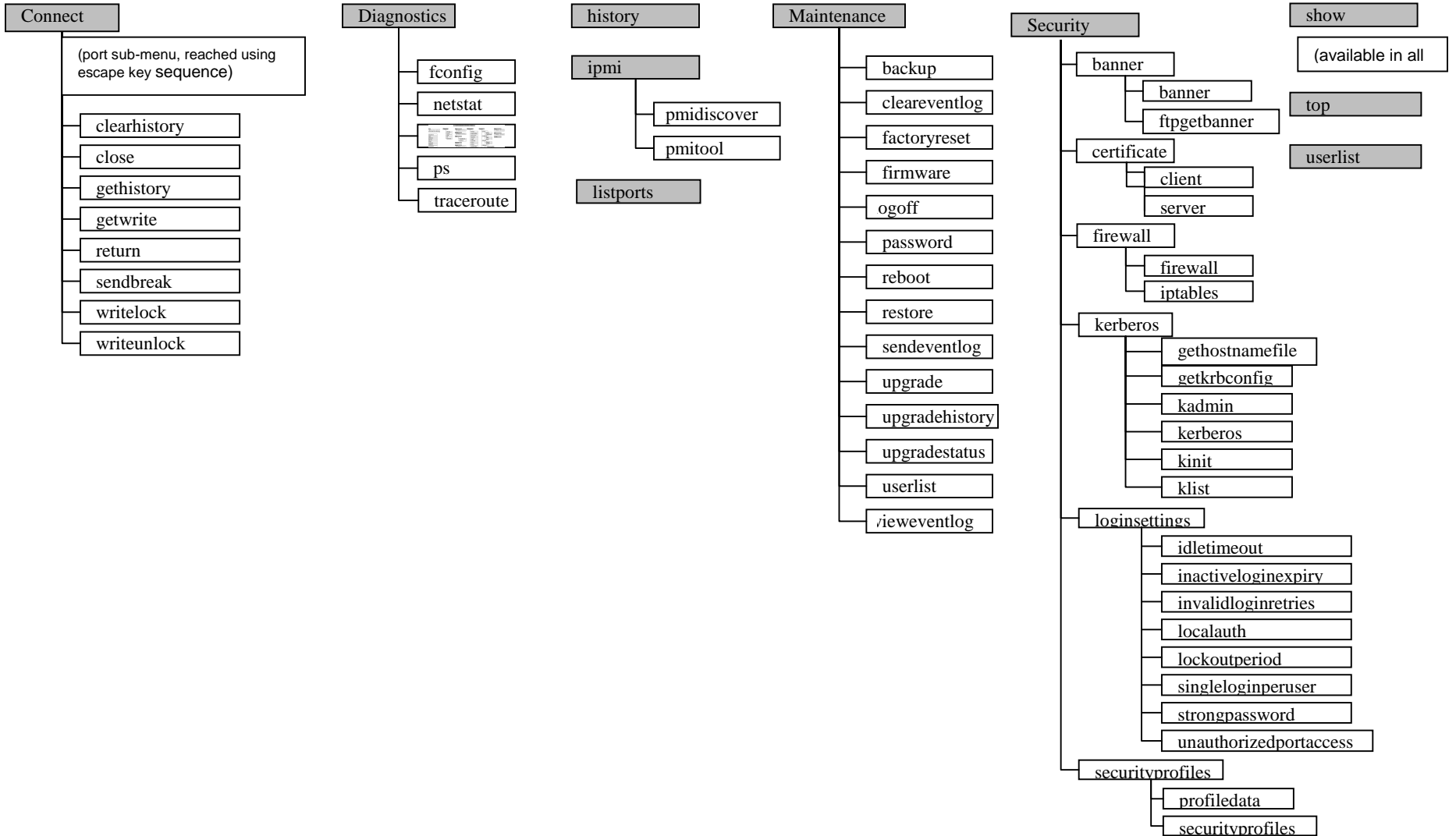
Dominion SX を使用して、管理者やユーザは複数のシリアル デバイスへのアクセス、制御、および管理を行うことができます。コマンドライン インタフェース(CLI)を使用して Dominion SX を設定したり、ターゲット デバイスに接続したりすることができます。RS-232 インタフェースは、1200 bps から 115200 bps までのすべての標準速度で動作します。

注 次の図に、CLI コマンドの概要を示します。すべてのコマンドの定義と、それらコマンドの例が記載されたこの章内のセクションへのリンクが含まれるリストについては、「CLI コマンド」を参照してください。

CLI Command Overview – Part 1



CLI Command Overview – Part 2



共通コマンド top、history、logout、quit、show、および help は、前の図のどの CLI のレベルからでも使用できます。

CLI を使用した Dominion SX へのアクセス

Dominion SX には、次のいずれかの方法を使用してアクセスします。

- IP 接続を介した Telnet
- IP 接続を介した HTTP および HTTPS
- IP 接続を介した SSH(セキュア シェル)
- RS-232 シリアル インタフェースを介したローカル ポート

利用可能な SSH/Telnet クライアントは、次のサイトから取得できます¹。

- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- ssh.com の SSH クライアント - www.ssh.com
- アプレット SSH クライアント - www.netspace.org/ssh
- OpenSSH クライアント - www.openssh.org

Dominion SX への SSH 接続

Dominion SX では、デフォルトで SSHv2 サーバが実行されるように設定されています。SSHv2 への接続には、SSHv2 をサポートする SSH クライアントであればどれでも使用できます。

注 セキュリティ上の理由から、SSH V1 接続は DSX ではサポートされません。

特定の SSH クライアントの設定に関する詳細情報は、本文書では取り扱っていません。

Windows PC からの SSH アクセス

Windows PC から SSH セッションを開くには、次の手順に従います。

1. PuTTY などの SSH クライアント ソフトウェアを起動します。
2. DSX サーバの IP アドレス 192.168.0.192 を入力します。
3. [SSH]を選択します。SSH では、デフォルトの設定ポート 22 を使用します。
4. [Open(開く)]ボタンをクリックします。
5. 次のプロンプトが表示されます。

```
login as:
```

ログイン情報については、「ログイン」セクションを参照してください。

UNIX ワークステーションからの SSH アクセス

UNIX ワークステーションから SSH セッションを開いて、ユーザ admin としてログインするには、次のコマンドを入力します。

```
ssh -l admin 192.168.0.192
```

次のプロンプトが表示されます。

```
password:
```

ログイン情報については、「ログイン」セクションを参照してください。

1 これらのリンクが間違っている場合は、Raritan 社までご連絡ください。弊社では、これらの正しいリンクを提供するよう努力しています。

Dominion SX への Telnet 接続

セキュリティが低く、ユーザ名、パスワードおよびすべてのトラフィックがクリアテキストでネットワーク上に送信されるため、Telnet アクセスはデフォルトで無効になっています。

Telnet の有効化

Telnet を使用して DSX にアクセスする場合は、まず CLI またはブラウザから DSX にアクセスします。

CLI

1. 次のコマンドを使用します。

```
admin > Config > Services > telnet enable true
```

次のメッセージが表示されます。

```
The system will need to be rebooted for changes to take effect  
(変更を有効にするためにはシステムをリブートする必要があります。)
```

注: デフォルトでは、Telnet ポートは 23 に設定されています。次のコマンドを指定することで、ポート番号を変更することができます。

```
admin > Config > Services > telnet enable true port <preferred port  
number>
```

2. システムをリブートします。

ブラウザ(GUI)

[Setup(セットアップ)]>[Services(サービス)]メニューで Telnet アクセスを有効にします。

DSX 本体へのアクセス

Telnet アクセスを有効にすると、Telnet を使用して DSX 本体にアクセスし、残りのパラメータを設定することができます。

Windows PC からの Telnet アクセス

PC から Telnet セッションを開くには、次の手順に従います。

1. [スタート]メニューから[ファイル名を指定して実行]を選択します。
2. [名前]テキスト ボックスに「Telnet」と入力します。
3. [OK]をクリックします。Telnet ウィンドウが開きます。
4. プロンプトで次のコマンドを入力します。

```
Microsoft Telnet> open <IP address>
```

ここで、<IP address> は第 3 章で設定した DSX の IP アドレスです。

5. ENTER キーを押します。次のメッセージが表示されます。

```
Connecting To <IP address>...
```

次のプロンプトが表示されます。

```
login as:
```

ログイン情報については、「ログイン」セクションを参照してください。

Dominion SX へのローカル ポート接続

Dominion SX のローカル ポートは、両端に DB-9F ヌルが装着されたヌル モデム ケーブルを使用して、コンピュータ システム、端末、または他のシリアル対応デバイスの COM ポートに接続する必要があります。

RJ 45 インタフェースがある場合、専用のケーブル(CRLVR)をクライアント コンピュータの ASCSDB9F コネクタで使用します。CRLVR は、ローカル ポートへの RJ45-RJ45 接続を確立する場合(つまり、SX デバイスのローカル ポートをシリアル ターゲットとして別の SX に接続する場合)にも使用できます。

ポート設定

ポート設定(シリアル通信パラメータ)が次のように設定されていることを確認します。

- ビット/秒 = 9600
- データ ビット = 8
- パリティ = なし
- ストップ ビット = 1
- フロー制御 = なし

接続

ローカル ポート接続を行うには、次の手順に従います。

1. ハイパーターミナル アプリケーション、または同等のアプリケーションを開きます。
2. ハイパーターミナルが、Dominion SX 本体に接続されているポートと通信を行うように設定されていることを確認します。
3. フロー制御を無効にします。
4. **ENTER** キーを押すと、次のプロンプトが表示されます。username:

ログイン情報については、「ログイン」セクションを参照してください。

ローカル ポート パラメータの変更

ローカル ポートはデフォルトで有効になっており、2 つのローカル ポートがある本体では両方のシリアルポートで有効で、9600 bps に設定されています。

ローカル ポート パラメータを変更する場合、たとえば、ボーレートを 9600 bps から 115200 bps に変更するには、次のように入力します。

```
admin > Config > Services > lpa enable true 115200
```

ローカル ポート アクセスを無効にするには、次のように入力します。

```
admin > Config > Services > lpa enable false
```

ログイン

ログインするには、次のようにユーザ名 admin を入力します。

```
login as:admin
```

パスワードのプロンプトが表示されます。デフォルトのパスワード **raritan** を入力します。

```
Password:
```

ウェルカム メッセージが表示されます。これにより、管理者としてログインしていることとなります。

```
login as: admin
Password:
Authentication successful.

-----
Welcome to the DominionSX[Model: SX4]
UnitName: DominionSX FirmwareVersion: 3.0.0.5.1 Serial: WACEA00008
IP Address: 192.168.51.194 UserIdleTimeout: 99min
-----

Port Port      Port Port
No. Name      No. Name
1 - Port1[U]  2 - Port2[U]
3 - Port3[U]  4 - Port4[U]

Current Time: Wed Sep 20 16:17:15 2006

admin >
```

図 88 管理者ログインのサンプル

```
3. Password:
4. Authentication successful.
5. -----
Welcome to the DominionSX[Model: SX4]
UnitName: DominionSX FirmwareVersion: 3.0.0.5.1 Serial: WACEA00008
IP Address: 192.168.51.194 UserIdleTimeout: 99min
6. -----
7.
8. Port Port      Port Port
9. No. Name      No. Name
10. 1 - Port1[U]  2 - Port2[U]
11. 3 - Port3[U]  4 - Port4[U]
12.
13. Current Time: Wed Sep 20 16:05:50 2006
14.
15.
16. Janet >
```

図 89 オペレータまたは監視者ログインのサンプル

次の「[CLI の操作方法](#)」セクションの内容を確認したら、[初期設定](#)タスクを実行します。

CLI の操作方法

CLI を使用する前に、CLI の操作方法と構文について理解しておく必要があります。さらに、キーストロークの組み合わせを使用すると CLI をより簡単に使用できます。

コマンドのオートコンプリート

CLI では、コマンドの一部を入力した場合のオートコンプリートがサポートされています。コマンドの最初の数文字を入力した後に、TAB キーを押して、入力した文字と一意の一致が見つかった場合、その入力内容はオートコンプリートされます。

- 一致が見つからない場合、そのレベルで有効なエントリが表示されます。
- 複数の一致が見つかった場合も、有効なエントリが表示されます。
- 追加のテキストを入力して一意なエントリと一致させてから TAB キーを押し、入力をオートコンプリートすることもできます。

CLI 構文 – ヒントとショートカット

ヒント

- コマンドは、アルファベット順にリストされます。
- コマンドでは、大文字と小文字が区別されません。
- パラメータ名は、アンダースコアのない単一の語です。
- 引数なしのコマンドを入力すると、デフォルトでそのコマンドに現在設定されている内容が表示されます。
- コマンドの後ろに疑問符(?)を入力すると、そのコマンドのヘルプが表示されます。
- 縦棒記号(|)は、オプション内の選択肢か、キーワードまたは引数の必須のセットを示しています。

ショートカット

- 前回の入力内容を表示するには、上矢印キーをクリックします。
- 直前に入力した文字を削除するには、BACKSPACE キーを使用します。
- 間違ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、CTRL キーを押しながら C キーを押します。
- コマンドを実行するには、ENTER キーを使用します。
- コマンドのオートコンプリートを使用するには、TAB キーを押します。

```
admin > Conf
```

この場合、admin > Config > プロンプトが表示されます。

すべてのコマンドライン インタフェース レベルの共通コマンド

表 3 に、すべての CLI レベルで使用可能なコマンドを示します。これらのコマンドは、CLI について学習するのにも役立ちます。

表 3 すべての CLI レベルの共通コマンド

コマンド	説明
top	CLI 階層のトップ レベル、または「username」プロンプトに戻ります。
history	ユーザが DSX CLI に入力した直近の 200 個のコマンドが表示されます。
show	指定したパラメータの設定が表示されるか、あるいはデフォルトですべての設定が表示されます。
help	CLI 構文の概要が表示されます。
quit	1 つ前のレベルに戻ります。
logout	ユーザ セッションからログアウトします。

show コマンド

show コマンドを実行すると、各種構成に関する設定項目が表示されます。このコマンドは、すべてのレベルで使用できます。

show コマンドの構文は、次のとおりです。

```
show[localauth | ldap | radius | tacacs | smtp | network | nfs |
modem | port | http | lpa | ssh | telnet | snmp | ntp |
users | groups | idletimeout | events][all]<>
```

コマンドの例

次のコマンドでは、SX 本体の全般設定が表示されます。

```
admin > show
```

```
Dominion SX4[64Mb] Serial: WACEA00008
Current time: 2006-09-20 23:08:42
```

```
-----
Date /Time Settings:
```

```
  Date : 2006-09-20 23:08:42
```

```
  Timezone : 13
```

```
Version Information :
```

```
Firmware Version : 3.0.0.1.15
```

```
Kernel Version : 2.4.12
```

```
PMON Version: 2.0.1
```

```
RSC Version: 1.0.0.1.16
```

初期設定

Dominion SX 本体は、出荷時に工場出荷時の設定が行われています。最初に本体の電源をオンにして接続したときに、次の基本パラメータを設定して、ネットワークを介して安全にデバイスにアクセスできるようにする必要があります。

1. 管理者パスワードをリセットします。
すべての Dominion SX 本体は同じデフォルト パスワードで出荷されているので、セキュリティ違反を防ぐために admin のパスワードは必ず変更してしてください。admin のパスワードを、「raritan」から DSX デバイスを管理する管理者が決めたパスワードに変更します。
2. IP アドレス、サブネット マスク、ゲートウェイ IP アドレスを割り当て、リモート アクセスを可能にします。
3. 日付と時刻を設定します。

これらのパラメータを設定すると、ローカル コンソール ポートとネットワーク経由のどちらからでも次の領域を設定できます。

- サービス
- セキュリティ
- ユーザ
- シリアル ポート

パラメータの設定

パラメータを設定するには、管理者特権でログインする必要があります。トップ レベルに "Username" > プロンプトが表示されます。初期設定では "admin" > です。ユーザが別のユーザ名でログインした場合、admin ではなくそのユーザ名が表示されます。top コマンドを入力して、メニューのトップ レベルに戻ります。

日付と時刻の設定

注 ログ エントリおよびイベントに正しいタイムスタンプを記録するために、日付と時刻を正確に設定することが重要になります。

top コマンドを入力して、メニューのトップ レベルに戻ります。次のコマンドを使用して、現在の日付と時刻の設定を表示します。

```
admin > Config > Time > clock
```

現在の設定内容が表示されます。たとえば、次のようになります。

```
Date /Time Settings:  
Date: 2006-09-20 23:20:24  
Timezone: 13
```

次の手順に従って、日付と時刻を設定します。

1. admin > Config > Time > timezonelist
2. admin > Config > Time > clock tz 21 datetime 2006-09-23 13:22:33

ネットワーク パラメータの設定

ネットワーク パラメータは、[interface](#) コマンドを使用して設定します。

```
admin > Config > Network > interface enable true if lan1 ip
192.16.151.12 mask 255.255.255 gw 192.168.51.12
```

コマンドが受け付けられると、本体は自動的にリブートして接続を切断します。新しい IP アドレス、ユーザ名 admin、出荷時のデフォルト パスワードの再設定のセクションで入力したパスワード newp/w を使用して、本体に再接続する必要があります。

重要: パスワードを忘れた場合は、背面のリセット ボタンを使用して工場出荷時の設定にリセットし、初期設定タスクを再度実行する必要があります。

これで、Dominion SX の基本設定が完了しました。SSH、GUI を使用してリモートで、またはローカル シリアル ポートを使用してローカルに Dominion SX にアクセスできるようになりました。次に、管理者はユーザとグループ、サービス、セキュリティ、およびシリアル ターゲットが接続される DSX のシリアル ポートを設定する必要があります。

CLI プロンプト

コマンドライン インタフェースのプロンプトには、現在のコマンド レベルが表示されます。プロンプトのルート部分はログイン名です。次のコマンドでは、admin がルート部分になります。

```
admin > Config > Port >
```

CLI コマンド

表 4 に、使用可能なすべての CLI コマンドのリストと説明を示します。

表 4 使用可能な CLI コマンド

コマンド	説明
backup	コンソール サーバの設定をバックアップするシステムコマンドです。
cleareventlog	ローカル イベント ログの内容をクリアします。
config	ポートの設定コマンドです。 設定メニューに切り替えます。
connect	ポートに接続します。
diagnostics	診断コマンド メニューに切り替えます。
encryption	HTTPS の暗号化方法を選択します。
eventlogfile	ローカル イベント ログを制御および設定します。
eventsyslog	システム イベント ログを制御します。
factory_reset	工場出荷時の設定をリセットするシステムコマンドです。
firmware	ファームウェアのバージョンを表示するシステムコマンドです。
help	CLI 構文の概要が表示されます。
history	現在のセッションのコマンドラインの実行履歴が表示されます。
http	http 接続を有効にします。
ifconfig	ネットワーク設定の詳細を表示します。
interface	DSX のネットワーク インタフェースを設定します。
ipmi	IPMI 設定を行うためのコマンドです。

listports	アクセス可能なポートがリストされます。
Kerberos	Kerberos ベースのネットワーク認証を行います。
ldap	LDAP 設定を行います。
localauthentication	ローカル認証の設定を行います。
logout	現在の CLI セッションをログアウトします。
maintenance	システム メンテナンスコマンドに切り替えます。
netstat	ネットワーク接続情報を出力します。
nfsget	暗号化キーを生成します。
nfssetkey	ログデータの暗号化を有効にします。
password	現在のユーザのパスワードを設定します。
ping	リモート システムへの ping を実行します。
portlog	ポート データのログ機能の有効化や設定を行います。
ps	システム プロセスのステータスを表示します。
quit	前のコマンドに戻ります。
radius	RADIUS 設定メニューに切り替えます。
reboot	システムをリブートするためのシステムコマンドです。
restore	システムをリストアするためのシステムコマンドです。
security	セキュリティ メニューに切り替えます。
sendeventlog	リモート FTP サーバにローカル イベント ログを送信します。
show	設定オプションを表示します。
tacacsplus	TACACS+ 設定メニューに切り替えます。
telnet	Telnet 通信を有効にして、ポートを指定します。
top	ルート メニューに戻ります。
traceroute	リモート システムへのルートを出力します。
upgrade	ファームウェアをアップグレードするためのシステムコマンドです。
upgradehistory	アップグレードの実行履歴を表示するためのシステムコマンドです。
userlist	ユーザを一覧で表示します。
vieweventlog	ローカル イベント ログを表示します。

セキュリティに関する問題

コンソール サーバのセキュリティに対応するには、多くの考慮すべき要素があります。

- オペレータ コンソールおよび DSX 本体間で送信されるデータ トラフィックを暗号化する。
- ユーザの認証と承認を行う。
- 操作に関するデータをログに記録して、後でそれを監査および参照目的で使用できるようにする。場合によっては、行政機関の規制または社内規定に準拠するためにこのデータが必要になります。
- リモート NFS サーバに送信されるポート データ ログを暗号化する。
- セキュリティ プロファイル。
- 「Man in the Middle 攻撃」。

Dominion SX では、これらの各要素がサポートされますが、一般利用する前にこれらの設定を行う必要があります。

トラフィックの暗号化の設定

オペレータ コンソールと DSX 本体間のトラフィックの暗号化は、使用するアクセス方法により決まります。デフォルトでは、SSH および暗号化されたブラウザ アクセス(HTTPS)が有効になっています。SSH と HTTPS では、定義上、リンクの両端間のトラフィックで 128 ビット暗号化がサポートされています。暗号化された接続を受け入れるには、手動で HTTP および Telnet サービスを有効にする必要があります。

ウェルカム バナーの設定

Dominion SX では、ログイン後に表示されるカスタマイズ可能なウェルカム バナー(最大 6000 ワード)がオプションでサポートされます。バナーにより、ユーザがログインした場所を識別できます。さらに、承諾バナーを追加して、ユーザがコンソール サーバの操作に進む前に、提示された条件を受諾するように求めることもできます。

SSL セキュリティ証明書の定義

SSL セキュリティ証明書は、接続先のデバイスが接続を認可されたデバイスであることを確認するために、ブラウザ アクセスで使われます。このセクションでは、コンソール サーバの証明書を設定する方法についてのみ説明します。SSL 証明書の詳細については、付録 C を参照してください。

ファイアウォール保護の有効化

Dominion DSX にはファイアウォール機能が用意されており、IP ネットワークを保護し、内部ルータと LAN 1、LAN 2、およびダイヤル モデム インタフェースの間のアクセスの制御を行うことができます。

セキュリティ プロファイルの有効化

Dominion SX では、ユーザやグループへの権限の割り当てを容易にするセキュリティ プロファイルを定義できます。セキュリティ プロファイルには、次の 3 種類があります。そのうちの 2 種類は定義済みの、標準プロファイルとセキュア プロファイルです。もう 1 種類は、独自に定義したカスタム プロファイルで、1 つのセキュリティ プロファイルを割り当てることによってすべての権限を割り当てることができます。複数のカスタム セキュリティ プロファイルを定義できます。

ログおよび警告の設定

Dominion SX のセキュリティ機能の一部として、データをログに記録する機能と、ユーザ、Dominion SX、およびターゲット デバイス間のアクティビティに基づいて警告を生成する機能が用意されています。これらの機能を使用すると、監査証跡によってシステムで何が起きたのかを確認し、誰がどのアクションをいつ実装したのかを判定することができます。

これらの機能は、イベント ログと SNMP トラップにより提供されます。イベントは、Syslog を使用してローカルで記録できます。ローカル イベントは、256 KB のポート バッファごとに保持され、FTP サーバへの保存、確認、クリア、または定期的な送信を行うことができます。

ユーザとグループの設定

ユーザとグループは関連しています。Dominion SX では、管理者が共通の許可と属性を持つグループを定義できます。管理者は、グループの定義後、そのグループにユーザを追加できます。各ユーザには、そのグループの属性と許可が設定されます。グループを有効にすると、各ユーザに対して許可を設定する必要がなくなるため、ユーザの設定にかかる時間を節約できます。

コマンドライン インタフェースの許可

管理者は、すべてのコマンドを実行できます。

オペレータと監視者は、次のコマンドのみ実行できます。

- connect
- help

- listports
- logout
- password

ターゲット接続と CLI

Dominion SX 本体の目的は、承認されたユーザが、connect コマンドを使用してさまざまなターゲットデバイスへの接続を確立できるようにすることです。ターゲットに接続する前に、ターミナル エミュレーションとエスケープ シーケンスを設定する必要があります。ターゲットが切断されると、該当する切断メッセージが表示されます。Dominion SX 本体には、ユーザ間でポートを共有する機能も用意されています。

ターゲットでのエミュレーションの設定

ターゲットでエミュレーションを設定するには、次の手順に従います。

- ホストで使用されているエンコードが、ターゲット デバイスに設定されているエンコードと同じであることを確認します。たとえば、SUN Solaris サーバの文字セット設定が ISO8859-1 になっている場合、ターゲット デバイスも ISO8859-1 に設定してください。
- Dominion SX シリアル ポートに接続されているターゲット ホストのターミナル エミュレーションが、VT100、VT220、VT320、または ANSI に設定されていることを確認します。

ほとんどの UNIX システムでは、「export TERM=vt100」(または vt220|vt320|ansi)を実行すると、UNIX ターゲット デバイスで推奨されるターミナル エミュレーション タイプに設定されます。たとえば、HP-UX サーバのターミナル タイプ設定が VT100 になっている場合、アクセス クライアントも VT100 に設定してください。

Dominion SX 本体でのターミナル エミュレーションの設定は、特定のターゲット デバイスのポート設定に関連付けられたプロパティです。クライアント ソフトウェア(Telnet または SSH クライアントなど)のターミナル エミュレーションの設定で、ターゲット デバイスがサポート可能であることを確認してください。

エスケープ シーケンスの設定

エスケープ シーケンスを設定するには、Dominion SX サーバに設定されているデフォルトのエスケープ シーケンスが、アクセス クライアントまたはホスト オペレーティング システムのキー シーケンスと競合しないようにします。エスケープ キー シーケンスはユーザ設定が可能です。デフォルトのエスケープ キー シーケンス ^] (プログラム可能)を押すと、コンソールのサブモードが表示されます。

エスケープ シーケンスは、ポート単位でプログラムすることができます。これは、異なるターゲット オペレーティング システムおよびホスト アプリケーションでは、異なるエスケープ キー シーケンスを認識することがあるためです。

CLI を使用したポート共有

アクセス クライアント ユーザは、他の認証され、認可されたユーザとポートを共有することができます。そのユーザがアクセス クライアント ユーザ(RSC)か SSH/Telnet ユーザであるかは関係ありません。ポート共有は、トレーニングや、アプリケーションのトラブルシューティングに利用されます。

- ユーザは、ポート共有セッション中に、書き込みアクセスを持つのか、あるいは読み取り専用アクセスなのかをリアルタイムで通知されます。
- ユーザは、ポートへの書き込み許可をリクエストすることができます。

Dominion SX コンソール サーバの管理

設定コマンド

注 CLI コマンドは、SSH、Telnet、ローカル ポート アクセスのどのセッションでも同じです。

設定メニューで使用可能なコマンドを使用して Dominion SX を設定できます。

設定メニューでは、次のコマンドを使用できます。

- authentication
- events
- log
- modem
- network
- nfs
- ports
- services
- snmp
- time
- users

承認と認証(AA)サービスの設定

Dominion SX は、ローカルとリモート両方の認証と承認(AA)サービスをサポートします。AA のローカルデータベースは、不正なアクセスを防ぐために暗号化された形式で保存されます。

リモート サービス

リモート サービスについて、Dominion SX では LDAP、Active Directory、TACACS+、および Kerberos をサポートします。また、Dominion SX サーバは、コンソール サーバの保護を強化する、さらにレベルの高いセキュリティ サービスもサポートします。こうしたサービスには、次のものがあります。

- 非アクティブ ユーザのアイドル タイムアウト
- ユーザ定義の証明書
- セキュリティ プロファイル

表 5 設定: 認証コマンド: ldap

コマンド	説明
ldaps	getservercert removecert viewcert
primaryldap	
secondaryldap	
radius	primaryradius secondaryradius
tacacsplus	primarytacacs secondarytacacs

注

LDAP サーバを設定する場合、サーバの照会文字列形式には、SX で設定されたグループの名前を含める必要があります。

RADIUS サーバを設定する場合、サーバのユーザの Filter-ID は、
"raritan:G{GroupOnSX};D{DialbackNumber}" という形式にする必要があります。

TACACS+サーバを設定する場合、サーバのユーザの user-group 形式には、DSX で設定されたグループの名前を含める必要があります。

"op:1:2:4"または"a:*"という古い形式(SX 2.5 以前のリリース)を使用する場合、システムにはログインできますが、ユーザ タイプとその制限に従ってポートにアクセスできるかどうか制限されます。現時点では、DSX にはグループに関するデータベース情報がないので、ログイン後、バナーに次のメッセージが表示されます。

Error: Cannot get group information(エラー: グループ情報を取得できません)

クライアント側からはどのポートが制限されているかがわからないため、ポート表示にはすべてのポートが表示されます。

LDAP 設定メニュー

ldap 設定メニューを使用すると、ldap と ldaps を設定できます。

ldap コマンドを実行するには、次のプロンプトで「ldap」と入力します。

```
admin > Config > Authentication > ldap
```

ldap コマンドのオプションについては、表 6 を参照してください。

表 6 ldap コマンド

コマンド オプション	説明
ldaps	次のコマンドを含む ldaps メニューに切り替えます。 getservercert – FTP による ldap 証明書の取得 removecert – LDAPS 証明書の削除 viewcert – LDAPS 証明書の表示
primaryldap	プライマリ ldap を設定するときに使用します。
secondaryldap	セカンダリ ldap を設定する場合に使用します。

LDAP コマンドの例

```
admin > Config > Authentication > ldap
admin > Config > Authentication > ldap > ldaps
admin > Config > Authentication > ldap > ldaps > viewcert
```

RADIUS コマンド

radius メニューでは、RADIUS サーバへのアクセスを設定するのに使用するコマンドを操作できます。

radius メニューコマンドの構文は、次のとおりです。

```
primaryradius
```

RADIUS コマンドの例

```
admin > Config > Authentication > radius > primaryradius
```

TACACPLUS コマンド

tacacsplus メニューでは、TACACS+へのアクセスを設定するのに使用するコマンドを操作できます。

tacacsplus コマンドの構文は、次のとおりです。

```
primarytacacs <>
```

コマンドの例

```
admin > Config > Authentication > radius > primarytacacs
```

イベントの設定

events メニューでは、SMTP イベントと SMTP サーバを設定するのに使用するコマンドを操作できます。

表 7 設定: events コマンド

コマンド オプション	説明
add	SMTP イベントを追加します。
delete	SMTP イベントを削除します。
smtp	SMTP サーバを設定します。

events メニューコマンドの例

```
admin > Config > events  
admin > Config > events > add  
admin > Config > events > smtp
```

ログの設定

log コマンドを設定すると、管理者が次のコマンドを使って Dominion SX サーバのログ機能を管理できるようになります。

- cleareventlog
- eventlogfile
- eventsyslog
- nfsget
- nfssetkey
- portlog
- sendeventlog
- vieweventlog

cleareventlog コマンド

cleareventlog コマンドは、ローカル イベント ログの内容をクリアします。

cleareventlog コマンドの構文は、次のとおりです。

```
cleareventlog
```

cleareventlog コマンドの例

```
admin > Config > Log > cleareventlog
```

eventlogfile コマンド

eventlogfile コマンドは、ローカル ログへのイベント ログ記録の制御および設定を行います。

eventlogfile コマンドの構文は、次のとおりです。

```
eventlogfile[enable <true|false>][size value][style <wrap|flat>]
```

eventlogfile コマンドのオプションについては、表 8 を参照してください。

表 8 eventlogfile コマンド

コマンド オプション	説明
enable <true false>	システム イベント ログ記録を有効または無効にします。
size value	ローカル ログ ファイルの最大サイズ(バイト)
style <wrap flat>	ログ ファイルが最大サイズに達したときに行う操作を指定します。 wrap を指定すると、ログがファイルの最後に到達したときに先頭に戻って記録します。 flat を指定すると、ログがファイルの最後に到達したときにログの記録を停止します。

eventlogfile コマンドの例

```
admin > Config > Log > eventlogfile enable true size 256000 style wrap
```

eventsyslog コマンド

eventsyslog コマンドは、システム イベント ログ記録を制御します。

eventsyslog コマンドの構文は、次のとおりです。

```
eventsyslog[enable <true|false>][][secondary ip <ip>]
```

eventsyslog コマンドのオプションについては、表 9 を参照してください。

表 9 eventsyslog コマンド

コマンド オプション	説明
enable <true false>	システム イベント ログ記録を有効または無効にします。
primary ip <ip>	プライマリ FTP サーバ アドレス
secondary ip <ip>	セカンダリ FTP サーバ アドレス

eventsyslog コマンドの例

```
admin > Config > Log > eventsyslog enable true primaryip 192.168.134.11  
secondaryip 192.168.245.11
```

nfsget コマンド

nfsget コマンドは、ポート ログ データを暗号化するのに使用する NFS 暗号化キーを取得します。取得したキー値を **nfssetkey** コマンドへの入力として使用します。

nfsget コマンドの構文は、次のとおりです。

```
nfsgetkey[type <rc4|aes128>]
```

次の表に、nfsget コマンドのオプションを示しています。

表 10 nfsget コマンド

コマンド オプション	説明
type <rc4 aes128>	暗号化に使用される暗号化キーのタイプ(rc4 または aes128)

nfsget コマンドの例

```
admin > Config > Log > nfsgetkey type aes128
```

nfssetkey コマンド

nfssetkey コマンドは、暗号化のタイプとキーを設定します。NFS は、安全でないことで有名です。つまり、NFS に簡単にアクセスしてデータを悪用できます。Dominion SX を使用すると、管理者が、NFS サーバに保存されているデータを暗号化できるようになります。したがって、不審なデータ アクセスがあっても、暗号化に使用した暗号化キーがなければそのデータは何の役にも立ちません。

暗号化キーは、DSX でしか設定および取得することはできません。

nfssetkey コマンドの構文は、次のとおりです。

```
nfssetkey[type <rc4|aes128>][key string]
```

nfssetkey コマンドのオプションについては、表 11 を参照してください。

表 11 nfssetkey コマンド

コマンド オプション	説明
type <rc4 aes128>	使用される暗号化タイプ
key string	暗号化に使用されるキー文字列を指定します。

注 aes128 は、3.0 ではサポートされていません。

コマンドの例

```
admin > Config > Log > nfssetkey type aes128 key
D2F05B5ED6144138CAB920CD
```

portlog コマンド

portlog コマンドは、ポート データのログ機能の有効化や設定を行います。

portlog コマンドの構文は、次のとおりです。

```
portlog[enable <true|false>][prefix name][size value][timestamp
interval][update interval][inputlog <true|false>][indir
name][outdir name][encrypt <true|false>]
```

portlog コマンドのオプションについては、表 12 を参照してください。

表 12 portlog コマンド

コマンド オプション	説明
enable <true false>	リモート NFS サーバへのポート データのログ記録を有効／無効にします。
prefix name	ログ ファイル名のプレフィックス
size value	ログ ファイルの最大サイズ(バイト)
timestamp interval	ログ ファイル内で次のタイムスタンプを記録するまでの間隔(秒)。値 0 を指定すると、タイムスタンプのログ記録が無効になります。最大値は 99999 です。
update interval	ログ ファイル内で次のタイムスタンプを記録するまでの間隔(秒)。デフォルトの間隔は 30 で、最大値は 99999 です。
inputlog <true false>	ポートでのユーザ入力データのログ記録を有効／無効にします。入力とは、ターゲットに送信されるデータ、つまり、ユーザが入力するキー入力のことです。
indir name	入力ログを保存するファイル名(SX1Input)
outdir name	出力ログを保存するファイル名(SX1Output)。出力とは、ターゲットから DSX ポートに送信されるデータのことです。
encrypt <true false>	リモート NFS サーバに送信されるログ データの暗号化を有効／無効にします。

portlog コマンドの例

```
admin > Config > Log > portlog enable true prefix DomSX1 size 1000000
timestamp 1 update 20 inputlog false indir /nfs SX DomIn outdir SXDom
Out encrypt true
```

次のコマンドでは、portlog のデフォルトの値が表示されます。

```
admin > Config > Log > portlog
```

Portlog Settings:

```
Enable: false
File Prefix: domSX-NFS
File Size: 65535
UpdateFrequency: 20
TimestampFrequency: 20
Input Log Enable: false
Input Log Directory: input
Output Log Directory: output
Encrypted: false
```

sendeventlog コマンド

sendeventlog コマンドは、ローカル ログ ファイルをリモート FTP サーバに送信します。

sendeventlog コマンドの構文は、次のとおりです。

```
sendeventlog[ip ipaddress][login login][password password][path
pathname][file filename]
```

sendeventlog コマンドのオプションについては、表 13 を参照してください。

表 13 sendeventlog コマンド

コマンド オプション	説明
ip ipaddress	FTP サーバ IP アドレス
login login	FTP サーバ ログイン名
password password	FTP サーバ パスワード
path pathname	FTP サーバ パス(/ftphome など)
file filename	ログを保存する、FTP サーバ上のファイル名(sxlogfile など)

sendeventlog コマンドの例

```
admin > Config > Log > sendeventlog 72.236.162.187 login acy password
pasraritansword path sxlogfile file log 32
```

vieweventlog コマンド

vieweventlog コマンドは、ローカル ログ ファイルを表示します。

vieweventlog コマンドの構文は、次のとおりです。

```
vieweventfile
```

vieweventlog コマンドの例

```
admin > Config > Log > vieweventlog
```

モデムの設定

modem メニューでは、モデム アクセスの設定に使用するコマンドを操作できます。コールバック(ダイヤルバック)は、コールの発信元が最初のダイヤル インへの応答として2回目のコールで即座にコールバックされると発生します。先にモデム ダイヤル インを設定してから、ダイヤル バックを有効にします。ダイヤル インとダイヤル バックは、モデム通信用に使用するデバイス(ローカル、RADIUS、LDAP、または TACACS+)で有効にする必要があります。

表 14 設定: モデムコマンド

コマンド	説明
dialback	モデムのダイヤル バックを有効または無効にします。この機能を動作させるには、モデムを有効にする必要があります。
dialin	モデムおよび PPP 設定を有効または無効にします。 [<enable disable>][server IP][client IP]

modem メニューコマンドの例

```
admin > Config > modem > dialin enable true serverip 10.0.13.211
clientip 10.0.13.212
admin > Config > modem > dialback enable true
admin > Config> Modem > show modem
```

Modem Settings:

```
Dialin Enabled: 1
Server IP : 10.0.13.211
Client IP : 10.0.13.212
```

```
Dialback : Enabled
```

ローカル ユーザを使用したダイヤル バック

モデム接続を確立するには、ダイヤル イン認証に使用されるローカル ユーザを設定する必要があります。新規ユーザを追加するか、ダイヤル バックが正しく機能するように既存のユーザを再設定することができます。ユーザ(ダイヤル バック番号が 129)を正しく設定するには、次のような設定にする必要があります。

User Settings:

```
Login : Modem
```

```
Name : Dialback
Info: SX
Dialback: 129
Group :Admin
Active : 1
```

モデム通信用に使用するデバイスでダイヤル インとダイヤル バックを有効にする必要があります。

この設定を行うと、モデム接続を確立できるようになります。ユーザは、さまざまなタイプのモデム ダイヤルアップ クライアントを使用して、SX デバイスにモデム経由で接続できます。

リモート RADIUS ユーザを使用したダイヤル バック(Cistron RADIUS v1.6.7)

モデム通信用に使用するデバイスでダイヤル インとダイヤル バックを有効にする必要があります。プライマリ(またはセカンダリ、あるいは両方の)RADIUS サーバの設定を正しく行い、SX デバイスでその設定を有効にする必要があります。

```
admin > Config > Authentication > RADIUS > primaryradius
```

RADIUS Server Settings

Primary Server

```
Enabled - true
IP Address - 10.0.0.188
Port - 1812
Secret - qazlwsx
```

リモート RADIUS サーバでのユーザの設定には、次の行が含まれている必要があります。

```
Filter-Id = "raritan:G{<local user group>}:D{<number for dialback>}"
```

リモート LDAP ユーザを使用したダイヤル バック(OpenLdap v.2 および v.3)

モデム通信用に使用するデバイスでダイヤル インとダイヤル バックを有効にする必要があります。プライマリ(またはセカンダリ、あるいは両方の)LDAP サーバの設定を正しく行い、SX デバイスでその設定を有効にする必要があります。

LDAP Server Settings

Primary Server

```
Enabled - true
IP Address - 10.0.0.188
Port - 389
Secret - root
Base DN - cn=root,o=bianor
Base Search - o=bianor
Auth Query String -rciusergroup
```

Dialback Query String - telephoneNumber

リモート LDAP サーバでのユーザの設定は、上の画像のようにする必要があります。

リモート TACACS ユーザを使用したダイヤル バック(Tacacs+ v.4.0.3a)

モデム通信用に使用するデバイスでダイヤル インとダイヤル バックを有効にする必要があります。プライマリ(またはセカンダリ、あるいは両方の)TACACS サーバの設定を正しく行い、SX デバイスでその設定を有効にする必要があります。

Primary Server

```
Enabled - true
IP Address - 10.0.0.188
Port - 49
Secret - alabala
```

リモート TACACS サーバでのユーザの設定には、次の行が含まれている必要があります。

```
user-dialback='129'
```

ネットワークの設定

network メニューコマンドは、SX ネットワーク アダプタを設定するのに使用します。

表 15 設定: network コマンド

コマンド	説明
ethernetfailover	ネットワーク フェイルオーバーを有効または無効にします。
interface	SX 本体のネットワーク インタフェースを設定します。
ipforwarding	IP 転送設定
name	ネットワーク名設定
ports	ネットワーク ポート設定
route	カーネル ルーティング テーブルを表示します。
routeadd	カーネル ルーティング テーブルにルートを追加します。
routedelete	カーネル ルーティング テーブルのルートを削除します。

ethernetfailover コマンド

ethernetfailover コマンドは、LAN 間のフェイルオーバー機能を有効または無効にするのに使用します。

ethernetfailover コマンドの構文は、次のとおりです。

```
ethernetfailover <enable|disable> <interval>
```

interface コマンド

interface コマンドは、Dominion SX ネットワーク インタフェースを設定するのに使用します。このコマンドが受け付けられると、本体は自動的にリポートして接続を切断します。次に、新しい IP アドレスおよびユーザ名 admin と出荷時のデフォルト パスワードの再設定のセクションで入力したパスワード newp/w を使用して再接続する必要があります。

interface コマンドの構文は、次のとおりです。

```
interface[enable <true|false>][if <lan1 | lan2>][ip ipaddress][mask subnetmask][gw ipaddress][mode <auto | 100fdx>]
```

このネットワークコマンドのオプションについては、表 16 を参照してください。

表 16 interface コマンド

コマンド オプション	説明
enable <true false>	インタフェースを有効または無効にします。
if <lan1 lan2>	設定する LAN インタフェースを選択します。
ip ipaddress	IP ネットワークからのアクセス用に割り当てられた、DSX の IP アドレス
mask subnetmask	IP 管理者から取得したサブネット マスク
gw ipaddress	IP 管理者から取得したゲートウェイ IP アドレス
mode <auto 100fdx>	Ethernet モードを自動検出または 100Mbps 全二重(100fdx)に設定します。

interface コマンドの例

次のコマンドでは、インタフェース番号 1 を有効にして、IP アドレス、サブネット マスク、およびゲートウェイアドレスを設定し、モードを自動検出に設定します。

```
admin > Config > Network > interface enable true if lan1 ip
192.16.151.12 mask 255.255.255 gw 192.168.51.12 mode auto
```

ipforwarding コマンド

ipforwarding コマンドは、2 つのネットワーク間の転送機能を設定するのに使用します。

ipforwarding コマンドの構文は、次のとおりです。

```
ipforwarding <>
```

このネットワークコマンドのオプションについては、表 17 を参照してください。

表 17 ipforwarding コマンド

コマンド オプション	説明

ipforwarding コマンドの例

次のコマンドでは、IP 転送を有効にします。

```
admin > Config > Network > ipforwarding
```

name コマンド

name コマンドは、ネットワーク名を設定するのに使用します。

name コマンドの構文は、次のとおりです。

```
name <>
```

このネットワークコマンドのオプションについては、表 18 を参照してください。

表 18 name コマンド

コマンド オプション	説明

name コマンドの例

次のコマンドでは、ネットワーク名を設定します。

```
admin > Config > Network > name
```

ports コマンド

ports コマンドは、ネットワーク ポートを設定するのに使用します。

ports コマンドの構文は、次のとおりです。

```
ports <>
```

このネットワークコマンドのオプションについては、表 19 を参照してください。

表 19 ports コマンド

コマンド オプション	説明

ports コマンドの例

ports コマンドの例を次に示します。

```
admin > Config > Network > ports
```

route コマンド

route コマンドは、カーネル ルーティング テーブルを表示するのに使用します。

このコマンドの構文は、次のとおりです。

```
route <>
```

このコマンドのオプションについては、表 20 を参照してください。

表 20 route コマンド

コマンド オプション	説明

route コマンドの例

次のコマンドでは、ルート テーブルを表示します。

```
admin > Config > Network > route
```

routeadd コマンド

routeadd コマンドは、カーネル ルーティング テーブルにルートを追加するのに使用します。

このコマンドの構文は、次のとおりです。

```
routeadd <>
```

このコマンドのオプションについては、表 21 を参照してください。

表 21 routeadd コマンド

コマンド オプション	説明

routeadd コマンドの例

次のコマンドでは、ルート テーブルにルートを追加します。

```
admin > Config > Network > routeadd
```

routedelete コマンド

routedelete コマンドは、カーネル ルーティング テーブルからルートを削除するのに使用します。

routedelete コマンドの構文は、次のとおりです。

```
routedelete <>
```

このコマンドのオプションについては、表 22 を参照してください。

表 22 routedelete コマンド

コマンド オプション	説明

routedelete コマンドの例

次のコマンドでは、ルート テーブルからルートを削除します。

```
admin > Config > Network > routedelete
```

NFS の設定

nfs コマンドを使用すると、ターゲット デバイスからのすべてのキー入力をネットワーク内のリモート NFS サーバのログに記録できます。このログは、後で確認できます。

```
admin > Config > NFS > nfs
```

nfs コマンドの構文は、次のとおりです。

```
nfs[enable <true|false>][primaryip primaryip][secondaryip  
secondaryip][primarydir primarydir][secondarydir  
secondarydir][option option]
```

nfs コマンドのオプションについては、表 23 を参照してください。

表 23 nfs コマンド

コマンド オプション	説明
enable <true false>	NFS ログ記録を有効または無効にします。
primaryip primaryip	プライマリ NFS サーバの IP アドレス
secondaryip secondaryip	セカンダリ NFS サーバの IP アドレス
primarydir primarydir	プライマリ サーバのマウント ディレクトリ
secondarydir secondarydir	セカンダリ サーバのマウント ディレクトリ
option option	softmount hardmount

コマンドの例

次のコマンドでは、現在の NFS 設定を表示します。

```
admin > Config > NFS > nfs
```

NFS Settings :

```
Enable : 0  
Primary IP : 0.0.0.0  
Primary Directory: /export/domSX/  
Secondary IP : 0.0.0.0  
Secondary Directory: /export/domSXLog/
```

リモート NFS ログ記録を有効にして NFS サーバを設定するには、次のコマンドを使用します。

```
admin > Config > NFS >nfs enable true primaryip 72.236.162.172  
secondaryip 72.236.161.173 primarydir /nfs/domlogging1 secondarydir  
/nfs/domlogging2 option softmount
```


ポートの設定

ports の設定メニュー

ターゲット シリアル ポートは、ports メニューを使用して CLI から設定します。ポートの物理的性質の定義の他に、その他のサービスについても定義します。こうしたサービスには、次のものがあります。

- ブレークを送信してエミュレータへのアクセスを行うポートから切断したり、またはマルチユーザ機能を制御するために使用するエスケープ シーケンス(例: CTRL a)。
- アイドル タイムアウトが発生したときにターゲットに送信される終了文字列を設定します。終了文字列を送信すると、ポートが DSX から切断されますが、次のユーザ ログイン時にこのポートにログインする場合はターゲットにも同様にログインする必要があります(Cisco ルータの終了文字列の例: logout)。
- ダイレクト ポート アドレス指定に使用されるアドレスを定義します。ダイレクト ポート アドレス指定には、1 つのポートに個別の IP アドレスまたは固有の TCP ポート アドレスを使用できます。ダイレクト ポート アドレス指定は、Telnet と SSH でサポートされています。この機能の詳細については、ダイレクト ポート アドレス指定のセクションを参照してください。

ports config コマンド

config コマンドの構文は、次のとおりです。

```
config[port <number|range|*>][name string][bps value][parity
<none|even|odd>][flowcontrol <none|hw|sw>][detect
<true|false>][escapemode <none|control>][escapechar
char][emulation type][exitstring <cmd[#delay;]>][dpaip
ipaddress][telnet port][ssh port]
```

このコマンドのオプションについては、表 24 を参照してください。

表 24 ポートの設定コマンド

コマンド オプション	説明
port <number range *>	単一のポートまたはポートの範囲(「1-n」または「1,3,4」。すべてのポートの場合は「*」)
name string	ポート名
bps value	ポート速度(ビットレート)(ビット/秒): (1200 1800 2400 4800 9600 19200 28800 38400 57600 115200)
parity <none even odd>	ポートのパリティ タイプ
flowcontrol <none hw sw>	ポートのフロー制御タイプ (hw = ハードウェア フロー制御 sw = X on / X off)
detect <true false>	ポート接続の検出を有効または無効にします。
escapemode <none control>	CTRL キー(escapemode=control)または単一のキー(escapemode=none)をエスケープ シーケンスとして使用します(たとえば、Ctrl-]=> escapemode=control, escapechar=]など)。
escapechar char	エスケープ文字
emulation type	ターゲット エミュレーション タイプ: VT100 VT220 VT320 ANSI

exitstring <cmd[#delay;]>	ポート セッションを閉じるときに終了文字列を実行します。たとえば、config port 1 exitstring logout(終了時に logout を実行する)、config port 1 exitstring #0(ポートの終了文字列を無効にする)のように指定します。
dpaip ipaddress	ダイレクト ポート アクセス用に割り当てられた IP アドレス
telnet port	Telnet 経由でのダイレクト ポート アクセス用に割り当てられた TCP ポート
ssh port	ssh 経由でのダイレクト ポート アクセス用に割り当てられた TCP ポート

コマンドの例

```
admin > ports config port 1 name ldl bps 115000 parity odd flowcontrol
hw detect true escapemode none emulation VT100
```

次のコマンドでは、ポート 1 の現在の設定を表示します。

```
admin > Config > Port > config port 1
```

Port number 1:

```
Name: Port1
BPS: 115200
Parity: 0
Flow control: 0
RSC Terminal Emulation: VT100
Disconnect: Disabled
Application: RaritanConsole
Exit String: show strongpassword
Escape: Control-]
DPA:
    IP: 0.0.0.0
    Telnet Port: 0
    SSH Port: 0
```

次の例では、管理者が DPA モードの IP を選択した場合に DPA ポートを設定します。ダイレクト ポート アクセス用の IP アドレスは、次のコマンドを使用して割り当てられます。

```
admin > Config > Port > config port 1 dpaip 10.0.13.240
```

Port 1: Configuration Saved

DPA changes will not be available until after the SX is rebooted.

1. 次の例では、管理者が DPA モードの TCP ポートを選択した場合に DPA ポートを設定します。管理者は、ダイレクト ポート アクセス用に割り当てられた SSH または Telnet ポート値を設定する必要があります。

```
admin > Config > Port > config port 1 ssh 7700 telnet 8800
```

Port 1: Configuration Saved

DPA changes will not be available until after the SX is rebooted.

その他の DPA TCP ポート オプション:

```
config <port *> <ssh tcpport>
config <port portnumber> <ssh tcpport>
config <port port_range> <ssh tcpport>
config <port *> <telnet tcpport>
config <port portnumber> <telnet tcpport>
config <port port_range> <telnet base_tcpport>
```

ひとまとまりの連続するポート番号を使用してすべてのポートを設定する場合に、<port *>コマンドを使用できます。port_range を指定した場合は、ひとまとまりの連続するポート番号が使用されます。指定した base_tcpport の値が、開始値として使用されます。個別のポートを設定する場合は、<port portnumber>コマンドを使用できます。

ports keywordadd コマンド

ポートごとにキーワードを設定できます。ポートのキーワードを設定した後、対応するイベントが通知用に選択されている場合は、ポートに接続されているターゲットからのデータでこのキーワードが検出されると、SMTP 通知が送信されます。

keywordadd コマンドの構文は、次のとおりです。

```
keywordadd
```

このコマンドのオプションについては、表 25 を参照してください。

表 25 ports keywordadd コマンド

コマンド オプション	説明

コマンドの例

```
admin > ports > keywordadd
```

ports keyworddelete コマンド

keyworddelete コマンドでは、既存のキーワードを削除します。

keyworddelete コマンドの構文は、次のとおりです。

```
keyworddelete
```

このコマンドのオプションについては、表 26 を参照してください。

表 26 ports keyworddelete コマンド

コマンド オプション	説明

コマンドの例

```
admin > ports > keywordadd
```

サービスの設定

次のコマンドを使用して、Dominion SX サーバ サービスを設定できます。

- DPA
- Encryption
- HTTP
- HTTPS
- Logout
- LPA
- SSH
- Telnet

dpa コマンド

TCP ポートの許容範囲は 1024～65535 です。

モード パラメータを指定せずに実行すると、現在の dpa タイプが表示されます。

dpa コマンドの一般的な構文は、次のとおりです。

```
dpa[mode <Normal|IP|TCPPort>]
```

TCP ポート番号を使用してポートに直接アクセスするための構文は、次のとおりです。

```
ssh -l sx_user -p tcp_port_N sx_ip_addr sx_user@sx_ip_addr's
password: <prompted by ssh>
```

```
telnet -l sx_user sx_ip_addr tcp_port_N Password: <prompted by telnet>
```

ポートごとに割り当てられた IP アドレスを使用してポートに直接アクセスするための構文は、次のとおりです。

```
ssh -l sx_user dpa_ip_addr sx_user@dpa_ip_addr's password: <prompted
by ssh>
```

```
telnet -l sx_user dpa_ip_addr Password: <prompted by telnet>
```

dpa コマンドのオプションについては、表 27 を参照してください。

表 27 dpa コマンド

コマンド オプション	説明
mode <IP TCPPort>	ポートごとのダイレクト ポート アクセス タイプ モード。 IP - ssh/telnet/http/https を介して固有の IP アドレスでターゲット ポートに直接アクセスします。 TCP ポート - ssh/telnet を介して固有の TCP ポートでターゲット ポートに直接アクセスします。
port_range	ひとまとまりの連続する IP アドレス
base_dpaip	ひとまとまりの連続する IP アドレスの開始値
IP address	ポートの IP アドレスが 0.0.0.0 と指定された場合、そのポートの IP アクセスは無効になります。つまり、ポートに IP アドレスが割り当てられていないのと同じことです。

dpa コマンドの例

次の例では、DPA モードの IP を選択します。

```
admin > Config > Services > dpa mode IP
```

注: DPA モードとポートの DPA 設定を変更した場合は、新しい設定を適用するために SX デバイスをリブートする必要があります。DPA の変更は、DSX がリブートされるまで有効になりません。

DPA 接続に成功すると、次のように表示されます。

```
ssh admin@10.0.13.240
Password:
Authentication successful.
```

```
Starting DPA for port 1
Authentication successful.
Escape Sequence is: Control-]
```

```
You are now master for the port.
```

「匿名」グループに割り当てられている一連のポートに対する unauthorizedportaccess の有効化

許可のないポート アクセスは、設定済みの DPA 方式でのみ行うことができます。次のコマンドを使用してください。

```
admin > Security > LoginSettings > unauthorizedportaccess enable true
```

unauthorizedportaccess を有効にすると、匿名グループが自動的に有効になり、ユーザは各自の要件に従って匿名グループを設定できます。

```
admin > Security > LoginSettings > unauthorizedportaccess
```

```
Unauthorized Port Access Settings:
```

```
    Enable: 1
```

```
Group Settings:
```

```
    Name: Anonymous
```

```
    Class: Observer
```

```
    Ports:
```

匿名グループを設定するには、`config > user` メニューで次のコマンドを実行します。

```
admin > Config > User > editgroup name Anonymous class op ports
1,2,3,4,5
```

```
Editing group...
```

```
Group Anonymous: Configuration Saved
```

「匿名」グループが正しく設定されます。

DPA 匿名アクセス:

DPA は既に設定済みです(DPA の設定のセクションを参照してください)。

DPA モードは IP で、IP 10.0.13.240 がポート 1 に割り当てられています。

匿名ポート アクセスでシリアル ポートにアクセスする場合は、以下に示すように、ユーザ名に「Anonymous」を指定し、パスワードには何も指定しないでください(ユーザ名とパスワードのどちらのフィールドも指定しない場合は、匿名アクセスが許可されます)。

```
ssh -l Anonymous 10.0.13.240
```

```
Password:
```

```
Authentication successful.
```

```
Starting DPA for port 1
```

```
Authentication successful.
```

```
Escape Sequence is: Control-]
```

```
You are now master for the port..
```

encryption コマンド

encryption コマンドは、HTTPS の暗号化のタイプを設定します。

注 このプロトコルの出荷時のデフォルト値は SSL です。

encryption コマンドの構文は、次のとおりです。

```
encryption[prot <TLS|SSL>]
```

encryption コマンドのオプションについては、表 28 を参照してください。

表 28 encryption コマンド

コマンド オプション	説明
prot <TLS SSL>	TLS または SSL 暗号化を選択します。

encryption コマンドの例

次の例では、HTTPS の SSL 暗号化を設定します。

```
admin > Config > Services > encryption prot SSL
```

http コマンド

http コマンドは、http アクセスやリダイレクト機能を制御したり、ポートを定義するのに使用します。

http コマンドの構文は、次のとおりです。

```
http[enable <true|false>][port value][redirect <true|false>]
```

http コマンドのオプションについては、表 29 を参照してください。

表 29 http コマンド

コマンド オプション	説明
enable <true false>	HTTP アクセスを有効または無効にします。
port value	HTTP サーバのデフォルトの待受ポート(tcp)
redirect <true false>	HTTP から HTTPS へのリダイレクト機能を有効または無効にします。

http コマンドの例

次の例では、http アクセスおよび https へのリダイレクト機能を有効にして、デフォルトのポートを 2 に設定します。

```
admin > Config > Services > http enable true port 2 redirect true
```

https コマンド

https コマンドは、https アクセスの制御やポートの定義に使用します。

https コマンドの構文は、次のとおりです。

```
https[enable <true|false>][port value]
```

次の表に、https コマンドのオプションを示しています。

https コマンド

コマンド オプション	説明
enable <true false>	HTTPS アクセスを有効または無効にします。
port value	HTTPS サーバのデフォルトの待受ポート(tcp)

https コマンドの例

```
admin > Config > Services > https
```

```
Https Settings:
```

```
  Enabled : true
```

```
  Port   : 443
```

logout コマンド

logout コマンドは、現在の CLI セッションをログアウトする場合に使用します。

どのコマンド レベルからでもログアウトできます。

lpa コマンド

lpa コマンドは、ローカル ポート アクセス設定の表示や設定に使用します。Dominion SX 本体には、モデルの種類によって 1 つまたは 2 つのローカル ポートがあります(DB9-M および RJ45-F の各ポートのピン配列については、付録 B を参照してください)。

lpa コマンドの構文は、次のとおりです。

```
lpa[enable <true|false>][bps value]
```

lpa コマンドのオプションについては、表 30 を参照してください。

表 30 lpa コマンド

コマンド オプション	説明
none	lpa コマンドに何もパラメータを指定しなかった場合は、現在の LPA 設定が表示されます。
enable <true false>	ローカル ポート アクセスを有効または無効にします。
[bps value]	ローカル ポート速度(ビットレート)(ビット/秒)。次の値を指定できます。 (1200 1800 2400 4800 9600 19200 28800 38400 57600 115200)

lpa コマンドの例

次のコマンドでは、ローカル ポート アクセスを有効にしてボーレートを設定します。

```
admin > Config > Services > lpa enable true 115200
```

ssh コマンド

ssh コマンドの構文は、次のとおりです。

```
ssh[enable <true|false>][port value]
```

ssh コマンドのオプションについては、表 31 を参照してください。

表 31 ssh コマンド

コマンド オプション	説明
enable <true false>	SSH アクセスを有効または無効にします。
port value	SSH サーバの tcp 待受ポート

ssh コマンドの例:

```
admin > Config > Services > ssh enable true port 4
```

上のコマンドを入力すると、次のメッセージが表示されます。

The system will need to be rebooted for changes to take effect.

telnet コマンド

telnet コマンドの構文は、次のとおりです。

```
telnet[enable <true|false>][port value]
```

次の表に、telnet コマンドのオプションを示しています。

表 32 telnet コマンド

コマンド オプション	説明
enable <true false>	Telnet アクセスを有効または無効にします。
port value	Telnet サーバの tcp 待受ポート

telnet コマンドの例

次のコマンドでは、ポート 23 での telnet アクセスを有効にします。

```
admin > Config > Services > telnet enable true port 23
```

SNMP の設定

Dominion SX サーバは、定義済みの SNMP サーバに SNMP 警告を送信できます。Raritan SNMP MIB は、Raritan Web サイトのサポート セクションの FAQ(よくある質問)から取得できます (<http://www.raritan.com/downloads/SX-MIB.txt>)。次のコマンドで、SNMP 機能を設定します。

- add
- delete
- snmp

SNMP add コマンド

add コマンドは、トラップ受信者を追加します。受信者とは、オプションのスペース区切りポート番号を持つ IP アドレスです。トラップは、同じ IP アドレスを持つ複数のポートに送信できます。

add コマンドの構文は、次のとおりです。

```
add[dest ipaddress][port value]
```

add コマンドのオプションについては、表 33 を参照してください。

表 33 SNMP add コマンド

コマンド オプション	説明
dest ipaddress	SNMP 送信先 IP アドレス
port value	SNMP 送信先ポート

SNMP add コマンドの例

```
admin > Config > SNMP > add 72.236.162.33 78
```

SNMP delete コマンド

SNMP delete コマンドは、トラップ受信者を削除します。受信者とは、オプションのスペース区切りポート番号を持つ IP アドレスです。ポート番号を持つ受信者を削除する場合は、そのポート番号も delete コマンドで指定します。トラップは、同じ IP アドレスを持つ複数のポートに送信できます。

SNMP delete コマンドの構文は、次のとおりです。

```
delete[dest ipaddress]
```

SNMP delete コマンドのオプションについては、表 34 を参照してください。

表 34 SNMP delete コマンド

コマンド オプション	説明
dest ipaddress	削除する SNMP 送信先 IP アドレス

SNMP delete コマンドの例

```
admin > Config > SNMP > delete 72.236.162.33
```

snmp コマンド

snmp コマンドは、SNMP トラップを制御し、トラップの送信に使われるコミュニティ名を指定します。

snmp コマンドの構文は、次のとおりです。

```
snmp[enable <true|false>][public community-string]
```

snmp コマンドのオプションについては、表 35 を参照してください。

表 35 snmp コマンド

コマンド オプション	説明
enable <true false>	SNMP を有効または無効にします。
public community-string	コミュニティ文字列

snmp コマンドの例

```
admin > Config > SNMP > snmp enable true public XyZZy1
```

時間の設定

時間関連の設定モードコマンドは、次のとおりです。

- clock
- ntp
- timezonelist

clock コマンド

clock コマンドを使用して、管理者はサーバの日付と時刻を設定できます。

clock コマンドの構文は、次のとおりです。

```
clock[tz tz][datetime datetime][timezonelist]
```

clock コマンドのオプションについては、表 37 を参照してください。

表 36 clock コマンド

コマンド オプション	説明
tz tz	タイム ゾーン インデックスは、対象となるタイム ゾーンに対応する番号です。
datetime datetime	コンソール サーバ 本体の日付と時刻の文字列。「YYYY-MM-DD HH:MM:SS」という形式で入力します。
timezonelist	このオプションを使用すると、タイム ゾーンとインデックス値のリストが表示されます。インデックス値を使用する場合は、[tz]オプションを指定してください。

コマンドの例

次の例では、Dominion SX の日付と時刻を、タイム ゾーン 21 の 2006 年 7 月 12 日午前 9 時 22 分 33 秒に設定します。

```
admin > Config > Time > clock tz 21 datetime 2006-07-12 09:22:33
```

ntp コマンド

ntp コマンドを使用して、管理者は、ネットワーク タイム プロトコル(NTP)サーバを使って SX のクロックを基準クロックに同期するかどうかを決定できます。

このコマンドの構文は、次のとおりです。

```
ntp[enable <true|false>][primaryntpip][secondaryntpip]
```

このコマンドのオプションについては、表 37 を参照してください。

表 37 ntp コマンド

コマンド オプション	説明
enable <true false>	NTP の使用を有効または無効にします。
primaryntpip	最初に使用する NTP サーバ
secondaryntpip	プライマリ NTP サーバが使用できない場合に使用する NTP サーバ

コマンドの例

次の例では、NTP を有効にします。

```
admin > Config > Time > ntp enable true primaryntpip 132.163.4.101
```

timezonelist コマンド

timezonelist コマンドは、タイムゾーンと対応するインデックス値のリストを返します。返されたインデックス値は、clock コマンドの一部に使われます。

このコマンドの構文は、次のとおりです。

```
timezonelist
```

ユーザの設定

次のコマンドを使用して、管理者はユーザを管理できます。

- addgroup
- adduser
- deletegroup
- deleteuser
- editgroup
- edituser
- groups
- users

addgroup コマンド

addgroup コマンドは、一般的な権限を持つグループを作成します。

addgroup コマンドの構文は、次のとおりです。

```
addgroup[name groupname][class <op|ob>][ports <number|range|*>]
```

addgroup コマンドのオプションについては、表 38 を参照してください。

表 38 addgroup コマンド

コマンド オプション	説明
name groupname	グループ名
class <op ob>	グループ ユーザ クラス<op>(オペレータ)または<ob>(監視者)
ports <number range *>	グループに割り当てられるポート。単一のポートまたはポートの範囲 (「1-n」または「1,3,4」。すべてのポートの場合は「*」)

コマンドの例

```
admin > Config > User > addgroup name unixgroup class op ports 1, 3
```

adduser コマンド

adduser コマンドは、指定したユーザに関する情報を管理するのに使用します。

adduser コマンドの構文は、次のとおりです。

```
adduser[user loginname][fullname user's-fullname][group  
name][dialback phonenumber][password password][info  
user-information][active <true|false>]
```

adduser コマンドのオプションについては、表 39 を参照してください。

表 39 adduser コマンド

コマンド オプション	説明
user loginname	ログイン名(必須)
fullname user's-fullname	ユーザのフルネーム(必須)

group name	ユーザに関連付けるグループ(必須)
dialback phonenumber	このユーザのダイヤル バック電話番号(オプション)
password password	ユーザのパスワード(必須)
info user-information	その他のユーザ情報
active <true false>	ユーザ アカウントを有効または無効にします。

adduser コマンドの例

次の例は、ユーザの追加方法を示しています。

```
admin > Config > User > adduser user jjones fullname John-Jones group
unix dialback 12146908003 password 123abc info AP-Systems active true
```

deletegroup コマンド

deletegroup コマンドでは、既存のグループを削除します。

deletegroup コマンドの構文は、次のとおりです。

```
deletegroup[name groupname]
```

deletegroup コマンドのオプションについては、表 40 を参照してください。

表 40 deletegroup コマンド

コマンド オプション	説明
name groupname	グループ名

コマンドの例

```
admin > Config > User > deletegroup name unixgroup
```

deleteuser コマンド

deleteuser コマンドは、指定したユーザを削除するのに使用します。

deleteuser コマンドの構文は、次のとおりです。

```
adduser[user loginname]
```

deleteuser コマンドのオプションについては、表 41 を参照してください。

表 41 deleteuser コマンド

コマンド オプション	説明
user loginname	ログイン名(必須)

deleteuser コマンドの例

次の例は、ユーザの削除方法を示しています。

```
admin > Config > User > deleteuser user jjones
```

editgroup コマンド

editgroup コマンドでは、既存のグループを編集します。

editgroup コマンドの構文は、次のとおりです。

```
editgroup[name groupname][class <op|ob>][ports <number|range|*>]
```

editgroup コマンドのオプションについては、表 42 を参照してください。

表 42 editgroup コマンド

コマンド オプション	説明
name groupname	グループ名
class <op ob>	グループ ユーザ クラス<op>(オペレータ)または<ob>(監視者)
ports <number range *>	グループに割り当てられるポート。単一のポートまたはポートの範囲 (「1-n」または「1,3,4」。すべてのポートの場合は「*」)

コマンドの例

```
admin > Config > User > editgroup name unixgroup class op ports 1,4
```

edituser コマンド

edituser コマンドは、指定したユーザに関する情報を管理するのに使用します。

edituser コマンドの構文は、次のとおりです。

```
edituser[user loginname][fullname user's-fullname][group  
name][dialback phonenumber][password password][info  
user-information][active <true|false>]
```

edituser コマンドのオプションについては、表 43 を参照してください。

表 43 edituser コマンド

コマンド オプション	説明
user loginname	ログイン名(必須)
fullname user's-fullname	ユーザのフル ネーム
group name	ユーザに関連付けるグループ
dialback phonenumber	このユーザのダイヤル バック電話番号
password password	ユーザのパスワード
info user-information	その他のユーザ情報
active <true false>	ユーザ アカウントを有効または無効にします。

edituser コマンドの例

次の例は、ユーザのパスワードを変更する方法について示しています。

```
admin > Config > User > edituser user admin password newp/w
```

groups コマンド

groups コマンドは、既存のグループの詳細を表示します。

groups コマンドの構文は、次のとおりです。

```
groups
```

コマンドの例

```
admin > Config > User > groups
```

users コマンド

users コマンドは、既存のユーザの詳細を表示します。

users コマンドの構文は、次のとおりです。

```
users
```

users コマンドの例

```
admin > Config > User > users
```

接続コマンド

接続コマンドを使用して、ポートおよびポートの履歴にアクセスできます。

表 44 接続コマンド

コマンド	説明
connect	ポートに接続します。エスケープ キー シーケンスを使用すると、ポート サブメニューを表示できます。
clearhistory	このポートの履歴バッファをクリアします。
close	このターゲット接続を閉じます。
gethistory	このポートの履歴バッファを表示します。
getwrite	ポートの書き込みアクセスを取得します。
return	ターゲット セッションに戻ります。
sendbreak	接続したターゲットにブレークを送信します。
writelock	このポートへの書き込みアクセスをロックします。
writeunlock	このポートへの書き込みアクセスのロックを解除します。

診断コマンド

診断コマンドを使用して、問題のトラブルシューティング用の情報を収集できます。

表 45 診断コマンド

コマンド	説明
ifconfig	ネットワーク設定の詳細を表示します。
netstat	ネットワーク接続情報を出力します。
ping	リモート システムへの ping を実行します。
ps	システム プロセスのステータスを表示します。
traceroute	ホストまでのネットワーク ルートをトレースします。 [-dnrv][-m maxttl][-p port#][-q nqueries][-s srcaddr][-t tos][-w wait]host[data size]

IPMI コマンド

IPMIDiscover コマンドおよび IPMITool コマンドは、IPMI をサポートするデバイス进行操作できます。

IPMIDISCOVER

ipmidiscover ツールは、ネットワーク内の Intelligent Platform Management Interface(IPMI)サーバを検出するのに使用します。

- IP アドレスの範囲は、startIP と endIP を使用して設定できます。
- Administrator グループに属しているユーザだけが IPMI のサポートを設定できます。IPMI バージョン 2.0 がサポートされています。

ipmidiscover ツールの構文は、次のとおりです。

```
ipmidiscover[OPTIONS]startIP endIP
```

IPMI バージョン 2.0 をサポートしている、検出されたターゲットがすべて表示されるので、ユーザはいずれかを選択して IPMI の操作を実行できます。

このコマンドのオプションについては、表 46 を参照してください。

表 46 ipmidiscover コマンド

コマンド	説明
[OPTIONS]	次の 2 つのオプションがサポートされています。 -t 検出完了までのタイムアウト[秒] -i ping の実行間隔[秒]
startIP	開始 IP アドレス
endIP	終了 IP アドレス

コマンドの例

```
admin> IPMI > ipmidiscover -t 20 10.0.22.1 10.0.22.10
```

```
Discovering IPMI Devices:
```

```
IPMI IP: 10.0.22.2
```

```
IPMI IP: 10.0.22.7
```

IP アドレスの範囲は、別のサブネットにまたがってもかまいません。

IPMITOOL

このコマンドを使用して、リモート システムの IPMI 機能を管理できます。FRU 情報の出力、LAN の設定、センサーの読み取り、およびリモート シャーシの電源管理といった機能があります。ipmitool コマンドでは、IPMI 対応のデバイスを制御します。IPMI デバイスにアクセスするユーザ名は ADMIN で、パスワードは ADMIN です。

ipmitool の構文は、次のとおりです。

```
ipmitool[-c|-h|-v|-V]-I lanplus -H <hostname>[-p <port>]
[-U <username>][-L <privlvl>][[-a|-E|-P|-f <password>]
[-o <oemtype>][-C <ciphersuite>]
```

このコマンドのオプションについては、表 47 を参照してください。

表 47 ipmitool コマンド

コマンド オプション	説明
-c	出力を CSV(カンマ区切り)形式で提供します。このオプションは、どのコマンドでも使用できるわけではありません。
-h	コマンドラインからの基本的な使用方法についてのヘルプを表示します。
-v	冗長出力レベルを上げます。このオプションは、デバッグ出力のレベルを上げるために複数回指定できます。3 回指定すると、すべての送受信パケットの hexdump(16 進のダンプデータ)を表示します。
-V	バージョン情報を表示します。
-I <interface>	使用する IPMI インタフェースを選択します。コンパイルされた対応インタフェースは、使用方法のヘルプ出力に表示されます。
-H <address>	リモート サーバのアドレス(IP アドレスまたはホスト名)。このオプションは、lan や lanplus インタフェースで必須です。
[-p <port>]	接続先のリモート サーバの UDP ポート。デフォルト値は 623 です。
[-U <username>]	リモート サーバのユーザ名。デフォルト値は NULL ユーザです。
[-L <privlvl>]	セッションの特権レベルを強制的に設定します。CALLBACK、USER、OPERATOR、ADMIN を設定できます。デフォルト値は ADMIN です。

<p>[-a -E -P -f <password>]</p>	<p>-a リモート サーバのパスワードの入力を求めるプロンプトが表示されます。</p> <p>-E リモート サーバのパスワードは、環境変数 IPMI_PASSWORD で指定されます。</p> <p>-P <password> リモート サーバのパスワードは、コマンドラインで指定されます。この場合、パスワードはプロセス リストには表示されません。</p> <p>-f <password_file> リモート サーバのパスワードが保存されているファイルを指定します。このオプションが指定されていない場合、または password_file が空の場合、パスワードのデフォルト値は NULL になります。</p>
<p>[-o <oemtype>]</p>	<p>サポートする OEM タイプを選択します。通常、これを行うには、コードに若干の手直しを加えてさまざまなメーカーの各種 BMC に対応させる必要があります。-o リストを使用して現在サポートされている OEM タイプのリストを確認します。</p>
<p>[-C <ciphersuite>]</p>	<p>IPMIv2 lanplus 接続に使用する、リモート サーバの認証、整合性の確認、および暗号化を行うためのアルゴリズム。IPMIv2 仕様の表 22-19 を参照してください。デフォルトは 3 で、RAKP-HMAC-SHA1 認証、HMAC-SHA1-96 整合性確認、および AES-CBC-128 暗号化のアルゴリズムを指定します。</p>
<p><command></p>	<p>raw - RAW IPMI リクエストを送信して応答を出力します。</p> <p>i2c - I2C マスター読み書きコマンドを送信して応答を出力します。</p> <p>lan - LAN チャンネルを設定します。</p> <p>chassis - シャーシのステータスを取得し、電源のステータスを設定します。</p> <p>power - シャーシ電源コマンドへのショートカット</p> <p>event - 定義済みのイベントを mc に送信します。</p> <p>mc - 管理コントローラのステータスを設定してグローバルで有効にします。</p> <p>sdr - センサー データ リポジトリのエントリと読み取り値を出力します。</p> <p>sensor - 詳細なセンサー情報を出力します。</p> <p>fru - 組み込みの FRU を出力し、FRU ロケータの SDR をスキャンします。</p> <p>sel - システム イベント ログ(SEL)を出力します。</p> <p>pef - Platform Event Filtering(PEF)を設定します。</p> <p>sol - IPMIv2.0 Serial-over-LAN を設定して接続します。</p> <p>tsol - Tyan IPMIv1.5 Serial-over-LAN を設定して接続します。</p> <p>isol - IPMIv1.5 Serial-over-LAN を設定します。</p> <p>user - 管理コントローラユーザを設定します。</p> <p>channel - 管理コントローラのチャンネルを設定します。</p> <p>session - セッション情報を出力します。</p> <p>firewall - ファームウェア ファイアウォール(IPMIv2.0)を設定します。</p> <p>sunoem - Sun サーバの OEM コマンド</p>

	<p>picmg - PICMG/ATCA 拡張コマンドを実行します。</p> <p>fwum - Kontron OEM Firmware Update Manager を使用して IPMC を更新します。</p> <p>shell - 対話型 IPMI シェルを起動します。</p> <p>exec - ファイルからコマンドのリストを実行します。</p> <p>set - shell と exec の実行時変数を設定します。</p>
--	---

コマンドの例

次のコマンドを使用して、ユーザはシャーシのステータスを取得し、電源のステータスを設定できます。

```
admin> IPMI > ipmitool -I lan -H 10.0.22.7 -U ADMIN chassis status
```

Password:

```
System Power      : on
Power Overload    : false
Power Interlock    : inactive
Main Power Fault  : false
Power Control Fault : false
Power Restore Policy: always-off
Last Power Event  : command
Chassis Intrusion : active
Front-Panel Lockout : inactive
Drive Fault       : false
Cooling/Fan Fault : false
```

詳細については、<http://ipmitool.sourceforge.net/manpage.html> を参照してください。

listports コマンド

表 48 listports コマンド

コマンド	説明												
listports	<p>アクセス可能なポートを一覧表示します。</p> <pre>admin > listports</pre> <table> <thead> <tr> <th>Port No.</th> <th>Port Name</th> <th>Port No.</th> <th>Port Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>- Port1[U]</td> <td>2</td> <td>- Port2[U]</td> </tr> <tr> <td>3</td> <td>- Port3[U]</td> <td>4</td> <td>- Port4[U]</td> </tr> </tbody> </table>	Port No.	Port Name	Port No.	Port Name	1	- Port1[U]	2	- Port2[U]	3	- Port3[U]	4	- Port4[U]
Port No.	Port Name	Port No.	Port Name										
1	- Port1[U]	2	- Port2[U]										
3	- Port3[U]	4	- Port4[U]										

最大 23 文字(バイト)のポート名が表示されます。ポート名が 23 文字(バイト)を超える場合は、22 文字(バイト)で切り捨てられ、最後に\$記号が付けられます。

ポート名の後に表示される文字は、各ポートのステータスを示しています。

- A - アクティブ
- B - 使用中
- D - 停止中
- U - 動作中

メンテナン スコマンド

メンテナンス コマンドは、Dominion SX ファームウェアのメンテナンス関連タスクを実行する管理者が使用します。次のコマンドは、システムコマンドです。

- backup
- cleareventlog
- factoryreset
- firmware
- logoff
- password
- reboot
- restore
- sendeventlog
- upgrade
- upgradehistory
- upgradestatus
- userlist
- vieweventlog

backup コマンド

backup コマンドは、Dominion SX 設定のコピーを作成して、ftp サーバにバックアップを書き込みます。現在の SX デバイス設定は、コマンド パラメータで設定した IP アドレスのコンピュータに暗号化形式で保存されます。ネットワーク設定を除く、すべてのデバイス設定がファイルに保存されます。リストア操作が必要になった場合にこのファイルを使って回復できます。

backup コマンドの構文は、次のとおりです。

```
backup[ip IP]<login LOGIN> <passwd PASSWD>[path PATH][file FILE]
```

backup コマンドのオプションについては、表 49 を参照してください。

表 49 backup コマンド

コマンド オプション	説明
[ip IP]	バックアップの書き込み先ターゲット システムの IP アドレス
<login LOGIN>	バックアップの保存先システムでのアカウントのユーザ名
<passwd PASSWD>	バックアップの保存先システムでのアカウントのパスワード
[path PATH]	バックアップ ファイルへのパスを指定します。
[file FILE]	バックアップを保存するファイルの名前を指定します。

backup コマンドの例

次の例では、コンソール サーバ データが IP アドレス 192.168.51.220 のシステムに送信されます。guest アカウントとパスワードが使用されます。このデータは、backupfile という名前のファイルとして guest アカウントのトップ レベルに保存されます。

```
admin > system > backup ip 10.0.0.188 login sx password qazlwsx path /home/ceci file Bac
```

cleareventlog コマンド

cleareventlog コマンドは、ローカル イベント ログの内容をクリアします。

cleareventlog コマンドの構文は、次のとおりです。

```
cleareventlog
```

cleareventlog コマンドの例

```
admin > Config > Log > cleareventlog
```

factoryreset コマンド

factoryreset コマンドは、Dominion SX コンソール サーバをデフォルトの出荷時の設定内容に戻します。

重要: 出荷時の設定に戻すと、すべてのユーザ設定が消去され、Dominion SX への接続が切断されます。この理由は、リブート時に、本体の IP アドレスが出荷時のデフォルトの IP アドレス 192.168.0.192 にリセットされるためです。

factoryreset コマンドの構文は、次のとおりです。

```
factoryreset
```

コマンドの例

```
admin > Maintenance > factoryreset
```

```
Network Settings:
```

```
Name: DominionSX
Domain : raritan.com
CSC Port: 5000
Discover Port: 5000
IP: 192.168.0.192
Net Mask : 255.255.255.0
Gateway : 192.168.0.192
Failover : true
```

```
Do you wish to commit these settings(no/yes)(default: no)
```

firmware コマンド

firmware コマンドは、ファームウェアのバージョンを表示します。

firmware コマンドの構文は、次のとおりです。

```
firmware
```

firmware コマンドの例

```
admin > Maintenance > firmware
```

```
Version Information:
```

```
Firmware Version: 3.0.0.1.15
Kernel Version: 2.4.12
PMON Version: 2.0.1
RSC Version: 1.0.0.1.16
```

logoff コマンド

表 50 logoff コマンド

コマンド	説明
Logoff	ユーザ セッションまたはポート セッションを強制的にログオフ(終了)します。

password コマンド

表 51 password コマンド

コマンド	説明
password	現在のユーザのパスワードを設定します。たとえば、ユーザがログインして現在のパスワードを変更する場合に使用します。

reboot コマンド

reboot コマンドは、Dominion SX コンソール サーバを再起動します。このコマンドは、管理者特権を持つユーザだけが使用できます。すべてのユーザ セッションは警告なしに終了され、確認を必要としません。本体をリブートする前に、すべてのユーザがログオフするように求めることをお勧めします。userlist コマンドを使用して、接続しているユーザやセッションのリストを表示できます。

reboot コマンドの構文は、次のとおりです。

```
reboot
```

reboot コマンドの例

```
admin > Maintenance > reboot
```

次のシステム応答メッセージが表示されます。

```
Rebooting the system will logoff all users.
```

```
Do you want to proceed with the reboot?(no/yes)(default: no)yes
```

restore コマンド

restore コマンドは、システムから Dominion SX システムのコピーを取得し、そのファイルを Dominion SX サーバに書き込みます。

restore コマンドの構文は、次のとおりです。

```
restore[ip IP]<login LOGIN> <passwd PASSWD>[path PATH][file FILE]
```

restore コマンドのオプションについては、表 49 を参照してください。

表 52 restore コマンド

コマンド オプション	説明
[ip IP]	リストア データの取得元となるターゲット システムの IP アドレス
<login LOGIN>	リストア データが保存されているシステムでのアカウントのユーザ名
<passwd PASSWD>	リストア データが保存されているシステムでのアカウントのパスワード
[path PATH]	同じポート密度を持つ同様のシステムにリストアされるバックアップ ファイルへのパスを指定します。
[file FILE]	バックアップ データが保存されているファイルの名前を指定します。

restore コマンドの例

次の例では、コンソール サーバ データが IP アドレス 192.168.51.220 のシステムから取得されます。guest アカウントとパスワードが使用されます。このデータは、backupfile という名前のファイルで guest アカウントのトップ レベルから取得されます。

```
admin > system > restore ip 192.168.51.220 login guest passwd
guestpassword path . file backupfile1
```

sendeventlog コマンド

sendeventlog コマンドは、ローカル ログ ファイルをリモート FTP サーバに送信します。

sendeventlog コマンドの構文は、次のとおりです。

```
sendeventlog[ip ipaddress][login login][password password][path
pathname][file filename]
```

sendeventlog コマンドのオプションについては、表 53 を参照してください。

表 53 sendeventlog コマンド

コマンド オプション	説明
ip ipaddress	FTP サーバの IP アドレス
login login	FTP サーバのログイン名
password password	FTP サーバのパスワード
path pathname	FTP サーバのパス(/ftphome など)
file filename	ログを保存する、FTP サーバ上のファイル名(sxlogfile など)

sendeventlog コマンドの例

```
admin > Config > Log > sendeventlog 72.236.162.187 login acy password
pasraritansword path sxlogfile file log 32
```

upgrade コマンド

注 アップグレードを実行するには、設定済みのリモート *ftp* サーバが必要です。

upgrade コマンドは、システムのあるバージョンを別のバージョンに(たとえば、v2.5 から v3.0 に)アップグレードします。

upgrade コマンドの構文は、次のとおりです。

```
upgrade[ip ipaddress][login login][password password][path
pathname]
```

このコマンドのオプションについては、表 54 を参照してください。

表 54 upgrade コマンド

コマンド オプション	説明
ip ipaddress	FTP サーバの IP アドレス
login login	FTP サーバのログイン名
Password password	FTP サーバのパスワード
Path pathname	FTP サーバのパス(/ftphome/UpgradePack/Pack1of1 など)

upgrade コマンドの例

```
admin > Maintenance > upgrade ip 10.0.0.188 login sx password qazlwsx
path /var/ftp/UpgradePack_2.5.6_3.0.0.1.15/Pack1of1
```

upgradehistory コマンド

upgradehistory コマンドは、前回システムをアップグレードしたときの情報を出力します。

upgradehistory コマンドの構文は、次のとおりです。

```
upgradehistory
```

コマンドの例

```
admin > Maintenance > upgradehistory
```

```
Overall Upgrade History:
3.0.0.1.15   Wed Sep 13 19:07:38 2006
```

userlist コマンド

userlist コマンドは、ログインしているすべてのユーザ、それぞれのソース IP アドレス、および接続しているポートのリストを表示します。

userlist コマンドの構文は、次のとおりです。

```
userlist
```

vieweventlog コマンド

vieweventlog コマンドは、ローカル ログ ファイルを表示します。

vieweventlog コマンドの構文は、次のとおりです。

```
vieweventfile
```


vieweventlog コマンドの例

```
admin > Config > Log > vieweventlog
```

セキュリティ コマンド

Dominion SX では、ランダム ログインを使用することでシステムへの侵入を抑制します。次のセキュリティコマンド メニューを使用して、Dominion SX セキュリティ機能の設定に必要なコマンドを操作できます。

- banner
- certificate
- firewall
- kerberos
- loginsettings
- securityprofiles

banner コマンド

banner コマンドは、ログイン直後のセキュリティ バナーの表示を制御します。

banner コマンドの構文は、次のとおりです。

```
banner[display <true|false>][audit <true|false>]
```

banner コマンドのオプションについては、表 55 を参照してください。

表 55 banner コマンド

コマンド オプション	説明
display <true false>	バナー表示を有効または無効にします。
audit <true false>	バナー表示が有効になっている場合に、バナーの監査を有効または無効にします。

banner コマンドの例

```
admin > Security > banner > banner display true audit false
```

ftpgetbanner コマンド

ウェルカム バナーおよび監査コメントが外部の FTP サイトで保持されている場合は、**ftpgetbanner** コマンドを使用して、DSX から直接対象のサイトに接続してウェルカム バナーを取得します。

ftpgetbanner コマンドの構文は、次のとおりです。

```
ftpgetbanner[ip ipaddress][login login][password password][path pathname]
```

ftpgetbanner コマンドのオプションについては、表 56 を参照してください。

表 56 ftpgetbanner コマンド

コマンド オプション	説明
ip ipaddress	FTP サーバの IP アドレス
login login	FTP サーバのログイン名
password password	FTP サーバのパスワード
path pathname	バナーファイル「banner.txt」の FTP サーバ上のパス(/ftphome/banner.txt など)

コマンドの例

```
admin > Security > Banner> ftpgetbanner ip 72.236.162.171 login
raritan password acy path /ftphome/banner.txt
```

certificate コマンド メニュー

certificate コマンド メニューには、セキュリティ証明書の作成および管理を行うための **client** コマンドと **server** コマンドが用意されています。

certificate コマンドの構文は、次のとおりです。

```
certificate <>
```

注 サードパーティの証明機関で LDAP over SSL を有効にする方法については、<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051> を参照してください。このドキュメントによると、MS Server で作成された証明機関の証明書をやりとりする必要があります。

client コマンドのオプションについては、表 57 を参照してください。

表 57 certificate client コマンド

コマンド オプション	説明
add	ユーザ証明書をインストールします。
addcrl	CA の CRL をインストールします。
clientcert	クライアント側の証明書検証を有効にします。
delete	クライアント CA 証明書を削除します。
deletecrl	クライアント CA の CRL を削除します。
viewcacert	クライアント CA 証明書を表示します。
viewcrl	クライアント CA の CRL 証明書を表示します。

client コマンドの例

```
admin > Security > certificate > client
```

server コマンドのオプションについては、表 58 を参照してください。

表 58 certificate server コマンド

コマンド オプション	説明
activatedefaultcert	デフォルトのシステム SSL 証明書を有効にします。
activateusercert	ユーザ SSL 証明書を有効にします。
generatecsr	デフォルトのシステム証明書を表示します。
generatedefaultcert	デフォルトのシステム SSL 証明書を生成します。
installusercert	ユーザ証明書をインストールします。
installuserkey	ユーザ証明書キーをインストールします。
viewcsr	証明書署名リクエストを表示します。

server コマンドの例

```
admin > Security > certificate > server
```

firewall コマンド

firewall コマンドは、ファイアウォールを有効または無効にすることができます。

firewall コマンドの構文は、次のとおりです。

```
firewall[enable <true|false>]
```

次の表に、firewall コマンドのオプションを示しています。

表 59 firewall コマンド

コマンド オプション	説明
enable <true false>	true または false を使ってファイアウォールを有効または無効にします。

コマンドの例

```
admin > Security > Firewall > firewall enable true
```

注 ファイアウォールを使用する場合は、次の設定を使用してください。

```
Chain FORWARD(policy ACCEPT)
target prot opt source destination
```

二重化 LAN 本体の IP 転送を有効にする場合は、IPTables ルールを使用して LAN インタフェース間で転送されるトラフィックのポリシーを作成してください。

IPtables コマンド

iptables コマンドは、IPv4 パケット フィルタリングおよび Network Address Translation(NAT)の管理ツールです。iptables コマンドを使用すると、Linux の iptables へのインタフェースが得られます。このコマンドのパラメータとオプションは、Linux システムのコマンドと同じです。

iptables コマンドのオプションについては、表 60 を参照してください。

表 60 iptables コマンド

コマンド オプション	説明
-A input	指定したチェーンに 1 つまたは複数のルールを追加します。
--dport	送信先ポート
--flush	iptables をクリアします。
-j target	次のターゲット キーワードに基づいてジャンプします。 ACCEPT - パケットは通過します(つまり、INPUT チェインの場合はローカルスタックで処理され、OUTPUT チェインの場合は送信されます)。 DROP - パケットは停止され、それ以上処理は行われません。 LOG - QUEUE - ユーザ スペース(カーネルでサポートされている場合)にデータグラムを渡します。 RETURN - このチェーンでの処理を終了し、呼び出し元チェーンを再開します(呼び出し元チェーンがない場合は、チェーン ポリシーを実行します)。
-list	現在の iptables を表示します。

--log-prefix DOM_IPACL	
-m state	マッチ拡張モジュールを読み込みます。
-p	トラフィックのプロトコル
-s	ソース アドレス
-save	IP テーブルを保存します。
--state NEW <enter rule to trigger here>	
-t filter	

iptables コマンドの例

iptables は数多くの方法で設定できますが、それらの方法については、このマニュアルでは取り上げていません。以下の例では、iptables で作成した単純な設定オプションをいくつか示します。

次の例では、iptables のログを有効にします。

```
admin > firewall > iptables -A input -t filter -j LOG
--log-prefix DOM_IPACL -m state --state NEW -s <IP>
```

デフォルトのローカル ルールの追加

ローカル アクセス用のデフォルトの iptable ルールを追加するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -t filter -j ACCEPT -s
127.0.0.1
```

IP アドレスによるアクセスの制限

特定の IP アドレス(192.168.1.100)からの SX へのアクセスを制限するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -t filter -j DROP
-s 192.168.1.100
```

IP アドレス接続時のメッセージのログ記録

IP アドレスで SX に接続したときに syslog メッセージを送信するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -t filter -j LOG
--log-prefix DOM_IPACL -m state --state NEW -s 192.168.1.100
```

IP の範囲に基づくアクセスの許可

特定の IP の範囲(192.168.0.1~192.168.0.255)からの SX へのアクセスを許可するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -t filter
-j ACCEPT -s 192.168.0.0/255.255.255.0
```

すべての ICMP トラフィックの無効化

ICMP プロトコルのトラフィックを無効にして、SX が ping に応答しないようにするには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -p icmp -j DROP
```

IP アドレスによる Telnet ポートへのアクセスの抑制

特定の IP アドレスから Telnet ポートにアクセスできないようにするには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -A INPUT -p tcp --dport 23
-j DROP -s 192.168.0.100
```

現在の iptables の表示

現在の iptables ルールセットを表示するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables -list
```

iptables ルールのクリア

iptables ルールをクリアするには、次のコマンドを入力します。

```
admin > Security > firewall > iptables --flush
```

設定の保存

iptables ルールをローカル データベースに保存するには、次のコマンドを入力します。

```
admin > Security > firewall > iptables-save
```

このコマンドは、すべての設定を指定した後に実行してください。

kerberos コマンド

kerberos コマンド メニューを使用して、Kerberos ネットワーク認証プロトコルの設定に使用するコマンドを操作できます。次の表に、kerberos コマンドのオプションを示しています。

表 61 kerberos コマンド オプション

コマンド オプション	説明
gethostnamefile	DNS ファイルに障害が発生した場合に/etc/hosts を取得します。
getkrbconfig	kerberos 5 設定ファイルを取得します。
kadmin	Kerberos admin クライアント
kerberos	Kerberos ベースのネットワーク認証
kinit	Kerberos チケットを取得します。
klist	Kerberos チケットを表示します。

Kerberos と DSX

DSX では、次の手順に従って Kerberos 認証を使用できます。その結果、Kerberos ベースのネットワーク相互認証および対称キー(別名: プライベート キー/秘密キー)暗号化は、リモートユーザ認証用の DSX の CLI と GUI で行うことができます。

Kerberos、KDC、Kadmind のクライアント マシンのセットアップの詳細や、これらのトピックに関連する FAQ については、[MIT Kerberos](http://www.mit.edu/~kerberos/) Web サイトを参照してください。

1. 「krb5.conf」スタンザ ファイルを設定し、getkrbconfig を使用してそのファイルを ftp で転送します (設定方法については、<http://www.faqs.org/faqs/kerberos-faq/general/section-38.html> を参照してください)。
2. kinit を使用してチケットを取得します。
3. kadmin を使用して/etc/krb5.keytab に HTTP/FQDN@REALM および host/FQDN@REALM の各キーを追加します。これらのキーは、起動のたびに変わることはありません。
4. リモート認証および承認は、Kerberos 認証とともに設定できます。HTTP および telnet によるアクセスでは、ユーザ名とパスワードの入力が求められます。現在、Kerberos では、ローカル ユーザ名またはリモート ユーザ名へのマッピングは自動的に行われません。
5. Kerberos を有効にします。
6. リポート後に、DSX ではセキュリティ保護された telnet および HTTP プロトコルによるリモート アクセスが可能となります。

診断のヒント:

- network メニューの name コマンドを使用して DSX の FQDN を設定します。
- services メニューから HTTP リダイレクトを無効にします。
- time メニューと ntp オプションを使用して、DSX、KDC、および Kadmind の各クライアント マシンの時刻を同期します。
- これら 3 種類のマシンは、FQDN に基づいて ping を実行できる必要があります。Kerberos メニューから gethostnamefile を使用してホスト ファイルを取得します。
- klist を使用してチケットの有効期間を確認します。
ほとんどの kadmin エラー メッセージは、チケットの有効期間に関連しています
- kadmin: プリンシパルを一覧表示し、KDC データベースに存在していないプリンシパルがあればそれを追加します。
- ブラウザ ルール: ブラウザでプリンシパルの入力が求められた場合、REALM の部分は含めないでください。
- Telnet アクセス: -x -l と -k オプションを適宜使用します。Telnet では、最初にその認証が出力されます。

キーと定義:

1. KDC、Kadmind、アプリケーション サーバ、およびクライアント マシンについては、MIT Kerberos FAQ(<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>)を参照してください。
2. FQDN: Fully Qualified Domain Name(完全修飾ドメイン名)

注 KDC kadmind の設定方法については、このマニュアルでは取り上げていません。これに関する情報については、このセクションに記載されている参照先をご覧ください。

kerberos コマンドの例

```
1)admin > Security > Kerberos > getkrbconfig ip 192.168.52.197 login
vijay password vijayv path /home/vijay/krb5.conf
Success
```

2)

kadmin: addprinc host/dsx-182.domain.com@REALMkadmin: addprinc [HTTP/dsx-182.raritan.com@RARITAN.COM](http://dsx-182.raritan.com@RARITAN.COM)

loginsettings コマンド

loginsettings コマンド メニューを使用して、システム全体のログイン設定を指定するのに使用するコマンドを操作できます。次の表に、loginsettings コマンドを示しています。

表 62 loginsettings コマンド

コマンド	説明
Idletimeout	システム全体のアイドル タイムアウトを設定します。
inactiveloginexpiry	ローカル ログインの有効期間を設定します。
invalidloginretries	ローカル ログイン再試行の最大回数を設定します。
Localauth	ローカル認証を設定します。
Lockoutperiod	不正なログイン試行のロックアウト期間を設定します。
singleloginperuser	ユーザにつき 1 ログイン セッションに制限します。
strongpassword	強力なパスワード ルールを設定します。
unauthorizedportaccess	許可されていない(匿名)のポート アクセスを設定します。

idletimeout コマンド

idletimeout コマンドでは、システムがユーザの接続を切断するまでの許容アイドルタイムを設定または変更します。

idletimeout コマンドの構文は、次のとおりです。

```
idletimeout time[number value]
```

idletimeout コマンドの例

```
admin > Security > LoginSettings > idletimeout time 99
```

inactiveloginexpiry コマンド

inactiveloginexpiry コマンドは、休止状態になったアカウントの有効期間(日数)を設定します。

inactiveloginexpiry コマンドの構文は、次のとおりです。

```
inactiveloginexpiry[days value]
```

inactiveloginexpiry コマンドのオプションについては、表 63 を参照してください。

表 63 inactiveloginexpiry コマンド

コマンド オプション	説明
days <value>	休止状態になったローカル ユーザのアカウントの有効期間(日数)

コマンドの例

```
admin > Security > LoginSettings > inactiveloginexpiry days 5
```

invalidloginretries コマンド

`invalidloginretries` コマンドでは、アカウントが無効になるログイン試行の失敗回数を指定します。

`invalidloginretries` コマンドの構文は、次のとおりです。

```
invalidloginretries[number value]
```

`invalidloginretries` コマンドのオプションについては、表 64 を参照してください。

表 64 `invalidloginretries` コマンド

コマンド オプション	説明
number value	アカウントが無効になるまでに許容される、失敗ログインの再試行回数

コマンドの例

```
admin > Security > LoginSettings > invalidloginretries number 5
```

localauth コマンド

`localauth` コマンドは、ローカル認証の設定に使用します。

`localauth` コマンドの構文は、次のとおりです。

このコマンドは、まだ実装されていません。

lockoutperiod コマンド

`lockoutperiod` コマンドでは、不正なログイン試行のロックアウト期間を定義します。

`lockoutperiod` コマンドの構文は、次のとおりです。

```
lockoutperiod[time time]
```

`lockoutperiod` コマンドのオプションについては、表 65 を参照してください。

表 65 `lockoutperiod` コマンド

コマンド オプション	説明
time time	アカウントが無効になった後、ユーザがログインできない期間(分)

コマンドの例

```
admin > Security > LoginSettings > lockoutperiod time 120
```


singleloginperuser コマンド

singleloginperuser コマンドは、1 ユーザあたりの複数のログインを有効または無効にします。

singleloginperuser コマンドの構文は、次のとおりです。

```
singleloginperuser[enable <true|false>]
```

このコマンドのオプションについては、表 66 を参照してください。

表 66 singleloginperuser コマンド

コマンド オプション	説明
enable <true false>	1 ユーザあたりの複数のログイン セッションを有効または無効にします。

コマンドの例

```
admin > Security > LoginSettings > singleloginperuser enable true
```

strongpassword コマンド

Dominion SX サーバは、標準のパスワードと強力なパスワードの両方をサポートしています。

- 標準のパスワードには、関連するルールがありません。つまり、パスワードはどのような形式でもかまわず、有効期間はありません。
- 強力なパスワードは、内容、長さ、および有効期間(日数)のルールを設定することによってパスワードの効果を高めます。
- 強力なパスワードを使用する場合は、管理者が、以下のリストから実装するルールを選択できます。
- 強力なパスワードの長さは、15 文字(バイト)までです。

strongpassword コマンドの構文は、次のとおりです。

```
strongpassword[StrongPasswordRulesEnable  
<true|false>][PWUppercaseRequired  
<true|false>][PWLlowercaseRequired <true|false>][PWNumberRequired  
<true|false>][PWSymbolRequired  
<true|false>][PasswordValidityPeriod <#>][PasswordHistoryDepth  
<#>][MinPasswordLength <#>][MaxPasswordLength <#>]
```

strongpassword コマンドのオプションについては、表 66 を参照してください。

表 67 strongpassword コマンド

コマンド オプション	説明
StrongPasswordRulesEnable	true/false
PWUppercaseRequired	true/false
PWLlowercaseRequired	true/false
PWNumberRequired	true/false
PWSymbolRequired	true/false
PasswordValidityPeriod	パスワードの有効期間(日数)
PasswordHistoryDepth	以前設定したのと同じパスワードを再利用できるようになるまでのパスワードの変更回数
MinPasswordLength	最小パスワード長
MaxPasswordLength	最大パスワード長

strongpassword コマンドの例

次の例では、効果のある強力なパスワード ルールを設定します。

- 大文字での入力を必要とする。
- 小文字の入力は不可。
- 数字を含める。
- 記号の入力は不可。
- パスワードの有効期間は設定後 90 日間。
- 以前設定したのと同じパスワードは 5 回パスワードを再設定した後に利用できるようする。それよりも前に同じパスワードを再利用することはできません。
- パスワードは 8～16 文字(バイト)で指定する必要がある。

```
admin > Security > LoginSettings > strongpassword
StrongPasswordRulesEnable true PWUppercaseRequired true
PWLlowercaseRequired false PWNnumberRequired true PWSymbolRequired
false PasswordValidityPeriod 90 PasswordHistoryDepth 5
MinPasswordLength 8 MaxPasswordLength 16
```

unauthorizedportaccess コマンド

unauthorizedportaccess コマンドの構文は、次のとおりです。

```
unauthorizedportaccess[enable <true|false>]
```

次の表に、unauthorizedportaccess コマンドのオプションを示しています。

表 68 unauthorizedportaccess コマンド

コマンド オプション	説明
enable <true false>	「匿名」グループに割り当てられている一連のポートに対する、許可されていないアクセスを有効または無効にします。

unauthorizedportaccess コマンドの例

```
admin > Security > LoginSettings > unauthorizedportaccess enable
disable
```

securityprofiles コマンド

securityprofiles コマンド メニューを使用して、セキュリティ プロファイルの設定と制御に使用するコマンドを操作できます。次の表に、securityprofiles コマンドを示しています。

表 69 securityprofiles コマンド

コマンド	説明
profiledata	セキュリティ プロファイルを表示または変更します。
securityprofiles	セキュリティ プロファイルを有効にして選択します。

profiledata コマンド

profiledata コマンドは、セキュリティ プロファイルを変更または表示するのに使用します。Dominion SX では、ユーザやグループへの権限の割り当てを容易にするセキュリティ プロファイルを定義できます。セキュリティ プロファイルには、次の 3 種類があります。

- そのうちの 2 種類は定義済みの、標準プロファイルとセキュア プロファイルです。
- もう 1 種類は、独自に定義したカスタム プロファイルで、1 つのセキュリティ プロファイルを割り当てることによってすべての権限を割り当てることができます。
複数のカスタム セキュリティ プロファイルを定義できます。

profiledata コマンドの構文は、次のとおりです。

```
profiledata[name <Standard|Secure|Custom>][telnet
<true|false>][strongpass <true|false>][timeout
<true|false>][single <true|false>][redirect
<true|false>][tls_required <true|false>]
```

profiledata コマンドのオプションについては、表 70 を参照してください。

表 70 profiledata コマンド

コマンド オプション	説明
[name <Standard Secure Custom>]	セキュリティ プロファイルのタイプを指定します。
[telnet <true false>]	telnet を有効または無効にします。
[strongpass <true false>]	強力なパスワードを有効または無効にします。
[timeout <true false>]	アイドル タイムアウトを有効または無効にします。
[single <true false>]	ユーザごとの単一ログインを有効または無効にします。
[redirect <true false>]	HTTP から HTTPS へのリダイレクト機能を有効または無効にします。
[tls_required <true false>]	HTTPS の Transport Layer Security(TLS)の強制を有効または無効にします。

profiledata コマンドの例

次の例では、カスタム セキュリティ プロパティを次のように定義します。telnet(無効)、強力なパスワード(有効)、アイドル タイムアウト(有効)、複数のログイン(許可)、HTTP から HTTPS へのリダイレクト機能(無効)、および HTTPS のトランスポート レイヤ セキュリティ(TLS)の強制(有効)。

```
admin > Security > SecurityProfiles > profiledata name Custom telnet
false strongpass true timeout true single false redirect false
tls_required true
```

空白ページ。

第 13 章: Intelligent Platform Management Interface

Intelligent Platform Management Interface(IPMI)を使用して、リモート システムの IPMI 機能を管理できます。この章では次の内容について説明します。

- IPMI デバイスの検出
- IPMI 設定

Intelligent Platform Management Interface(IPMI)を使用して、リモート システムの IPMI 機能を管理できます。



図 90 1 IPMI 画面

IPMI デバイスの検出

ネットワーク上の IPMI サーバを検出するには、次の手順に従います。

1. [IPMI]タブをクリックし、[Discover IPMI Devices(IPMI デバイスの検出)]をクリックします。Discover IPMI Devices(IPMI デバイスの検出)画面が表示されます。



図 91 Discover IPMI Devices(IPMI デバイスの検出)画面

2. Options(オプション)フィールドは空白のままにするか、「-t タイムアウト(秒)」を入力することができます。
3. 対応するフィールドに開始 IP アドレスと終了 IP アドレスを入力します。この IP アドレスの範囲内にある IPMI デバイスがすべて検出されます。
4. [IPMI Discover(IPMI 検出)]ボタンをクリックします。

例

Options(オプション)フィールドに何も入力しなかったときの出力例は、次のとおりです。

結果:

```
Discovering IPMI Devices ...
--- ipmidiscover statistics ---
448 requests transmitted, 0 responses received in time, 100.0% packet
loss
```

IPMI 設定

IPMI 設定を使用して、リモート システムの IPMI 機能を管理できます。FRU 情報の出力、LAN の設定、センサーの読み取り、およびリモート シャーシの電源管理といった機能があります。

1. IPMI 画面の[IPMI Configuration(IPMI 設定)]セクションをクリックして、IPMI 設定情報を取得します。

図 92 IPMI Configuration(IPMI 設定)

2. [Help(ヘルプ)]ボタンをクリックして IPMI 設定情報を取得します。この情報は、IPMIConfiguration(IPMI 設定)画面に表示されます。

ヘルプ:

```
ipmitool version 1.8.7
```

```
usage: ipmitool[options...]
```

```

-h          This help
-V          Show version information
-v          Verbose(can use multiple times)
-c          Display output in comma separated format
-I intf     Interface to use
-H hostname Remote host name for LAN interface
-p port     Remote RMCP port[default=623]
-U username Remote session username
-f file     Read remote session password from file
-S sdr      Use local file for remote SDR cache
-a          Prompt for remote password
-e char     Set SOL escape character
-C ciphersuite Cipher suite to be used by lanplus interface
-k key      Use Kg key for IPMIv2 authentication
-L level    Remote session privilege level[default=ADMINISTRATOR]
-A authtype Force use of auth type NONE, PASSWORD, MD2, MD5 or OEM
-P password Remote session password
-E          Read password from IPMI_PASSWORD environment variable
-m address  Set local IPMB address
-b channel  Set destination channel for bridged request
-l lun      Set destination lun for raw commands
-t address  Bridge request to remote target address
-o oemtype  Setup for OEM(use 'list' to see available OEM types)
-O seloem   Use file for OEM SEL event descriptions
```

Interfaces:

```

open       Linux OpenIPMI Interface[default]
imb        Intel IMB Interface
lan        IPMI v1.5 LAN Interface
```

Commands:

raw	Send a RAW IPMI request and print response
i2c	Send an I2C Master Write-Read command and print response
lan	Configure LAN Channels
chassis	Get chassis status and set power state
power	Shortcut to chassis power commands
event	Send pre-defined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print System Event Log(SEL)
pef	Configure Platform Event Filtering(PEF)
sol	Configure and connect IPMIv2.0 Serial-over-LAN
tsol	Configure and connect with Tyan IPMIv1.5
Serial-over-LAN	
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information
firewall	Configure firmware firewall(IPMIv2.0)
sunoem	OEM Commands for Sun servers
picmg	Run a PICMG/ATCA extended cmd
fwum	Update IPMC using Kontron OEM Firmware Update Manager
shell	Launch interactive IPMI shell
exec	Run list of commands from file
set	Set runtime variable for shell and exec

3. IP Address(IP アドレス)フィールドに IP アドレスを入力します。
4. Username(ユーザ名)フィールドにユーザ名を入力します。
5. Password(パスワード)フィールドにパスワードを入力します。
6. Option(オプション)フィールドにオプションを入力します。
7. Command(コマンド)フィールドにコマンドを入力します。
8. [IPMI Discover(IPMI 検出)]ボタンをクリックします。コマンドの実行結果が表示されます。

空白ページ

第 14 章: 電源制御

電源制御では、電源関連の機能を管理できます。この章では次の内容について説明します。

- 電源制御
- 電源の関連付け
- 電源タップの電源制御
- 電源タップのステータス

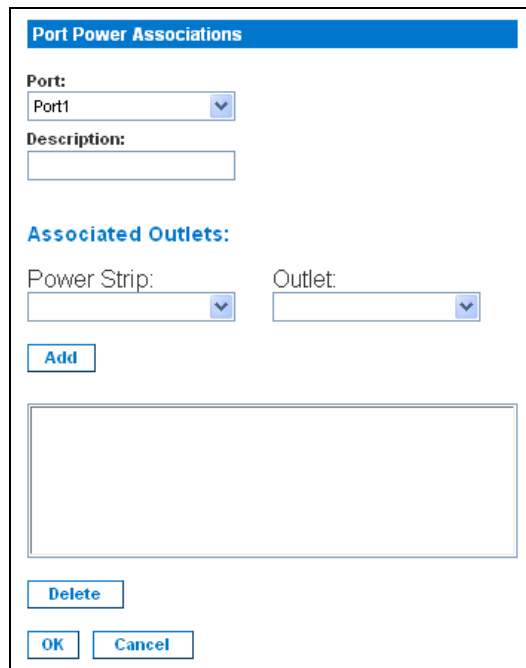
ポート電源の関連付け

DSX に接続されている電源タップの 1 つまたは複数のコンセントを特定の DSX ポートに関連付けることができます。

ポート電源の関連付けの作成

ポート電源の関連付けを作成するには、次の手順に従います。

1. [Setup(設定)]タブをクリックして、[Port Power Association List(ポート電源の関連付けリスト)]をクリックします。
2. [Add(追加)]をクリックします。Port Power Association(ポート電源の関連付け)画面が表示されます。



The screenshot shows a dialog box titled "Port Power Associations". It has a "Port:" dropdown menu with "Port1" selected. Below it is a "Description:" text input field. Underneath is the "Associated Outlets:" section, which includes a "Power Strip:" dropdown menu and an "Outlet:" dropdown menu. At the bottom of the dialog are four buttons: "Add", "Delete", "OK", and "Cancel".

図 93 Port Power Association(ポート電源の関連付け)画面

3. **Port**(ポート)フィールドのドロップダウン メニューからポートを選択します。
4. **Power Strip**(電源タップ)フィールドのドロップダウン メニューから電源タップの名前を選択します。
5. **Outlet**(コンセント)フィールドのドロップダウン メニューからポートに関連付けるコンセントを選択します。
6. [Add(追加)]をクリックします。

ポート電源の関連付けの削除

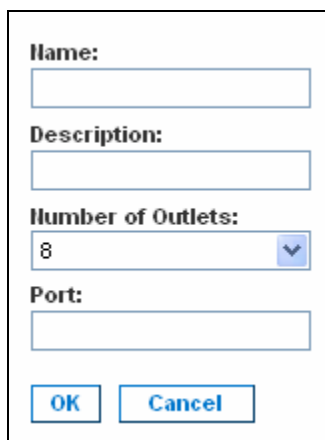
ポート電源の関連付けを削除するには、次の手順に従います。

1. [Setup(設定)]タブをクリックし、[Port Power Association List(ポート電源の関連付けリスト)]をクリックします。
2. [Add(追加)]をクリックします。Port Power Association(ポート電源の関連付け)画面が表示されます。
3. Outlet Association(コンセントの関連付け)のリストで、削除する関連付けを選択します。
4. [Delete(削除)]をクリックします。

電源タップの設定

電源タップを設定するには、次の手順に従います。

1. [Setup(設定)]タブをクリックし、[Power Strip Configuration(電源タップ設定)]をクリックします。
2. [Add(追加)]をクリックします。Power Strip Configuration(電源タップ設定)画面が表示されます。



The image shows a dialog box titled "Power Strip Configuration". It has the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Number of Outlets:** A dropdown menu with "8" selected.
- Port:** A text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

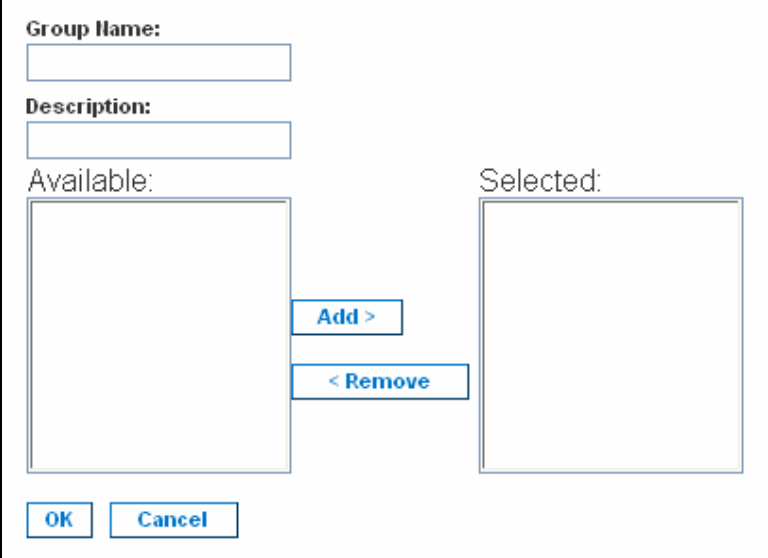
図 94 Power Strip Configuration(電源タップ設定)画面

5. **Name**(名前)フィールドと **Description**(説明)フィールドにそれぞれ名前と説明を入力します。
6. **Number of Outlets**(コンセント数)フィールドのドロップダウンメニューからコンセント数を選択します。
7. **Port**(ポート)フィールドにポート番号を入力します。
8. [OK]をクリックします。

電源の関連付けグループ

電源の関連付けグループを作成するには、次の手順に従います。

1. [Setup(設定)]タブをクリックし、[Power Association Groups List(電源の関連付けグループ リスト)]をクリックします。
2. [Add(追加)]をクリックします。Power Association Groups(電源の関連付けグループ)画面が表示されます。



The screenshot shows a dialog box for creating a Power Association Group. It contains the following elements:

- Group Name:** A text input field.
- Description:** A text input field.
- Available:** An empty list box on the left.
- Selected:** An empty list box on the right.
- Add >** A button between the two list boxes to move items from Available to Selected.
- < Remove** A button between the two list boxes to move items from Selected back to Available.
- OK** and **Cancel** buttons at the bottom left.

図 95 Power Association Groups(電源の関連付けグループ)画面

3. **Group Name**(グループ名)フィールドと **Description**(説明)フィールドにそれぞれ名前と説明を入力します。
4. **Number of Outlets**(コンセント数)フィールドのドロップダウンメニューからコンセント数を選択します。
5. [OK]をクリックします。

電源制御

[Power Control(電源制御)]タブを選択して電源制御関連のツールを表示します。



図 96 Power Control(電源制御)

電源の関連付け

[Power Control(電源制御)]メニューの[Associations Power Control(電源の関連付け)]をクリックして、電源の関連付けを管理するツールにアクセスします。

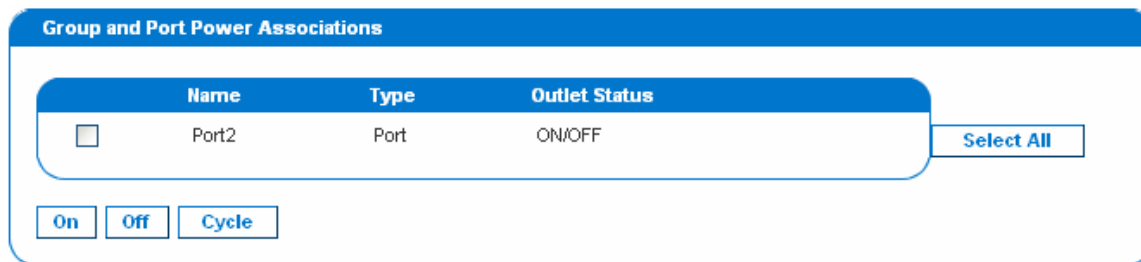


図 97 Associations Power Control(電源の関連付け)

注 電源のオン/オフ操作を実行するときに、電源を切ってから入れ直すまでの設定済みの間隔が最大で約5秒長くなり、動作遅延時間(動作までにかかる最短時間)となります。電源の再投入を選択すると、関連付けられたすべてのコンセントの電源が順番にオフになり、その後順番にオンになります。電源回復までの時間により、コンセントの電源をオフにした後に再びオンにするのに必要な最短時間が決まるため、この時間は管理者が指定します。つまり、実際の遅延時間は、動作遅延時間と管理者が指定した遅延時間を合わせた時間になります。

電源タップの電源制御

[Power Control(電源制御)]メニューの[Power Strip Power Control(電源タップの電源制御)]をクリックして、電源タップを管理するツールにアクセスします。

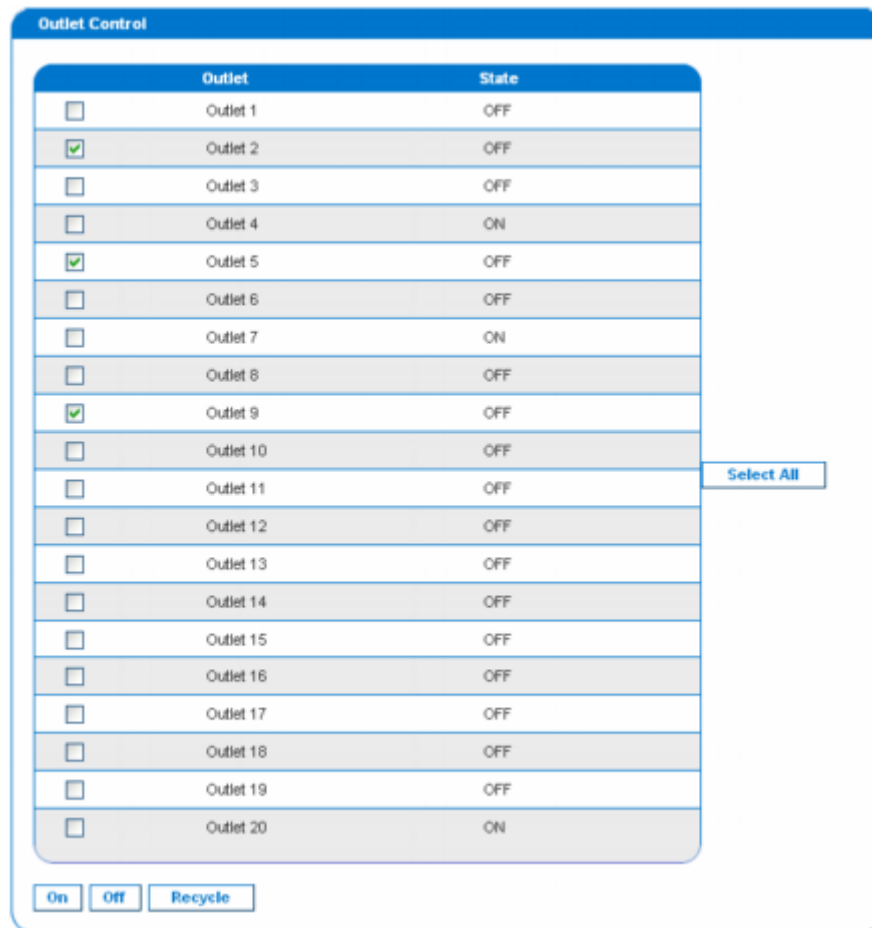


図 98 Power Strip Power Control(電源タップ電源制御)

電源タップのステータス

[Power Control(電源制御)]メニューの[Power Strip Status(電源タップのステータス)]をクリックして、電源タップのステータスを確認します。

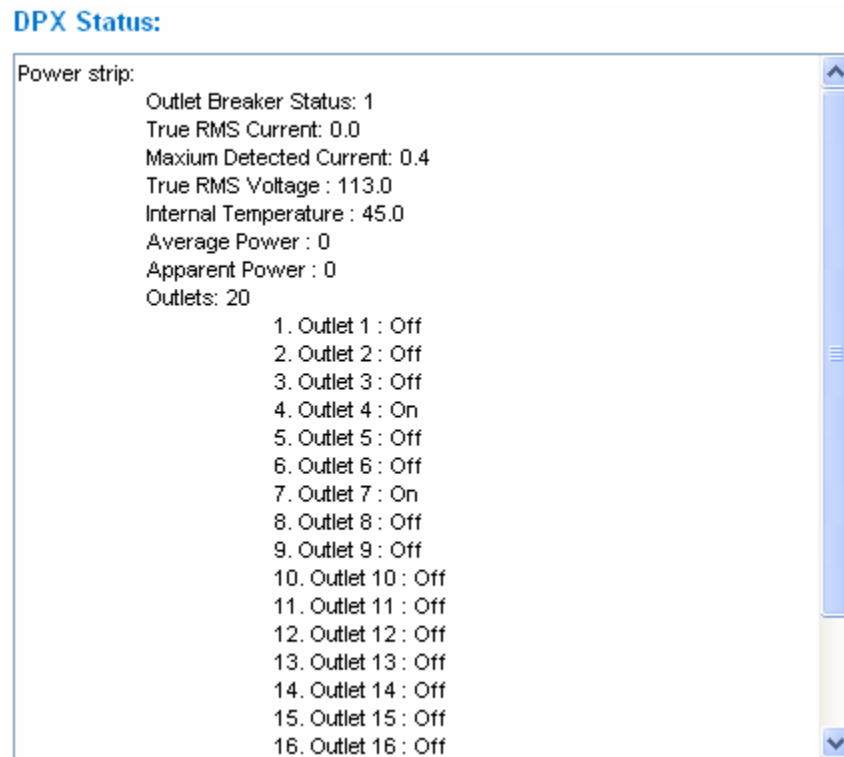


図 99 Power Strip Status(電源タップのステータス)

第 15 章: ユース ケース

この章では、ユーザが DSX 本体の実際の操作にすぐに慣れるように、一般的な 10 種類のユース ケースについて説明します。各ケースで入力するデータは、例として作成されたものなので、さまざまな状況に応じて変わる可能性があることに注意してください。

ケース 1. Web ブラウザを介した DSX ファームウェアのアップグレード

1. 目的: 機能拡張やサービス修正プログラム用に DSX ファームウェアのバージョンをアップグレードします。
2. 最新バージョンのファームウェアを入手するには、Raritan のサポート Web サイトを確認してください (<http://www.raritan.com/support/firmwareupgrades> の [Dominion Family] を選択して SX を検索)。
3. UpgradePack として保存されている新しい SX ファームウェアを Raritan のサポート Web サイトから FTP サーバ (FileZilla サーバなど) にダウンロードします。ここでは、FTP サーバの IP アドレスは 192.168.51.204 であると仮定しています。zip ファイルを FTP ルート ディレクトリの下にあるフォルダ (`¥home¥downloads¥firmware¥UpgradePack_2.5.6_3.1.0.5.2¥Pack1of1` など) に抽出します。このフォルダに自分の FTP ユーザ アカウントでアクセスできることを確認してください。
4. 次に、Web ブラウザを介して SX にログインします。[Maintenance(メンテナンス)] の [Firmware Upgrade(ファームウェアのアップグレード)] を選択します。FTP サーバの IP アドレス (192.168.51.204 など)、FTP ユーザ名とパスワード、および抽出したファイルの保存先である FTP フォルダのパス (この例では `/UpgradePack_2.5.6_3.1.0.5.2¥Pack1of1`) を入力し、[Upgrade(アップグレード)] をクリックします。
5. ファームウェアのアップグレードが完了したら、SX にログインし、[Maintenance(メンテナンス)] の [Firmware Upgrade(ファームウェアのアップグレード)] を選択して、ファームウェアのバージョンをもう一度確認します。また、[Maintenance(メンテナンス)] の [Firmware Upgrade History(ファームウェアのアップグレード履歴)] を選択して、ファームウェアのアップグレード履歴を確認することもできます。
6. 詳細については、第 10 章の「[DSX ファームウェアのアップグレード](#)」セクションを参照してください。

ケース 2. SSH を介したダイレクト ポート アクセスの設定および使用

1. 目的: DSX GUI を使用せずにユーザが SSH でシリアル ターゲットに直接アクセスできるようにします。
2. ユーザは、SX の DPA または任意のポートに使用する、SX の IP アドレスまたは TCP ポートを選択することができます。ネットワーク管理者には予備の IP アドレスがないので、別のポートで SX IP アドレスを再利用します。
3. SX にログインし直して、[Setup(設定)] の [Port Configuration(ポート設定)] を選択し、DPA に対応しているポートを選択します。
4. SSH クライアントの接続先となる [DPA SSH TCP Port(DPA SSH TCP ポート)] を編集して、[OK] をクリックします。
5. Web ブラウザを介して SX にログインします。[Setup(設定)] の [Services(サービス)] ページで、[Direct Port Access Mode(ダイレクト ポート アクセス モード)] の [TCP port(TCP ポート)] を選択して、[OK] をクリックします。
6. Plink、PuTTY などの SSH クライアントを起動します。IP アドレスを入力し、接続するデフォルトの TCP ポートを有効なポートに変更します (`plink -ssh -P 2203 192.168.51.9` など)。
7. 詳細については、第 7 章の「[ダイレクト ポート アクセス](#)」セクションを参照してください。

ケース 3. RSC を介した排他的書き込みアクセスの使用

1. 目的: 自分だけがユーザとしてシリアル ターゲットに書き込めるようにします。
2. Web ブラウザを介して SX にログインすると、[Port Access(ポート アクセス)]タブがデフォルトで選択されます。
3. ポート 4 に接続するには、[Port 4(ポート 4)]というラベルのハイパーリンクをクリックします。
4. 次に、Raritan Serial Console(RSC)アプリケーション ウィンドウが、書き込みアクセスが有効な状態(ウィンドウ下部のステータス行に緑色のアイコンで示される)で起動します。ただし、ポートが別のユーザに占有されている場合は除きます。
5. RSC ウィンドウで、[エミュレータ]の[書き込みロックの取得]を選択します(他のユーザが以前に書き込みアクセス権を取得していた場合は、最初に RSC の[エミュレータ]メニューから[書き込みアクセス権の取得]を実行してください)。これで、ステータス行のアイコンは、書き込みアクセス(ロック)になります。つまり、どのユーザもポート接続を表示することしかできない状態となります。
6. ポートに接続されているデバイスにログインし、RSC パネルを使用してデバイスとやりとりしてみてください。
7. 詳細については、第 7 章の「[書き込みアクセス権の取得](#)」セクションを参照してください。
8. RSC ウィンドウで書き込みロックを解除するには、[エミュレータ]の[書き込みロック解除]を選択します。これにより、ステータス行のアイコンが、再度書き込みアクセス権を示すようになります。つまり、特権を持つ他のユーザが書き込みアクセス権を取得できるようになります。

ケース 4. LDAP の設定

1. 目的: ログイン認証で LDAP サーバまたは Active Directory サーバを使用するように DSX を設定します。
2. Web ブラウザを介して SX にログインし、[Setup(設定)]の[Remote Authentication(リモート認証)]を選択します。
3. LDAP サーバにバックアップ サーバがある場合は、セカンダリ LDAP サーバに同じパラメータ(IP アドレス以外)を入力します。
4. [OK]をクリックして変更を確定します。
5. 詳細については、第 6 章の「[LDAP の設定](#)」セクションを参照してください。

ケース 5. 電源の関連付けグループの作成

1. 目的: ターゲット サーバを、物理的に接続する複数の電源コンセントに関連付けます。
2. Web ブラウザを介して SX にログインした後に、電源タップが既に設定されていることを確認してください(電源タップを追加するには、[Setup(設定)]の[Power Strip Configuration(電源タップ設定)]ページの[Add(追加)]をクリックします。詳細については、第 14 章の「[電源タップの設定](#)」セクションを参照してください)。次に、[Setup(設定)]の[Port Power Association List(ポート電源の関連付けリスト)]ページにある[Add(追加)]をクリックします。
3. [Port(ポート)]のドロップダウン メニューから、コンセントを関連付ける、二重化電源のサーバ デバイスに接続されている SX ポートを選択し、その説明として「Internal Web Server Pronto」などと入力します(詳細については、第 14 章の「[ポート電源の関連付け](#)」セクションを参照してください)。
4. デバイスが電源に接続されている方法に合わせてドロップダウン メニューから電源タップとコンセントを選択します。次に、[Add(追加)]ボタンをクリックすると、「[Power Strip Name(電源タップ名)]\#[outlet 1(コンセント 1)]」の形式でテキスト ボックスに情報が表示されます。同じ電源タップと別のコンセントを選択し、[Add(追加)]ボタンをクリックしてそれを追加します。「[Power Strip

Name(電源タップ名)¥[outlet 2(コンセント 2)]」の形式でテキスト ボックスに別の行が表示されま
す。[OK]をクリックして変更を確定します。

5. [Setup(設定)]の[Power Association Groups List(電源の関連付けグループ リスト)]ページの
[Add(追加)]をクリックします(詳細については、「[電源の関連付けグループ](#)」セクションを参照してくだ
さい)。
6. グループ名と説明を入力して、[Available(使用可能なポート)]ボックスからポート ID を選択し(複
数選択可能)、[Add(追加)]ボタンをクリックして[Selected(選択したポート)]に追加し
ます。
7. [OK]をクリックして変更を確定します。
8. 最初に電源タップを DSX 管理に追加する方法の詳細については、「[電源タップの設定](#)」セクション
を参照してください。電源タップを DSX 管理に追加していない場合は、「[ポート電源の関連付け](#)」
セクションを参照して、DSX ポートに接続されているターゲット サーバに電源タップのコンセントをマ
ップしてください。また、同じターゲット サーバに物理的に接続されている複数の電源コンセントをグ
ループ化する方法の詳細については、「[電源の関連付けグループ](#)」セクションを参照してください。

ケース 6. DSX のファクトリ リセットの実行

1. 目的: GUI を介して DSX の設定を出荷時のデフォルト値に戻します。
2. Web ブラウザを介して各自のログイン ユーザ名とパスワード(admin/raritan など)で SX にログインし
ます。
3. [Maintenance(メンテナンス)]の[Factory Reset(ファクトリ リセット)]を選択します。リセットを実行す
るかどうかを確認するプロンプトが表示されます。
4. デフォルトの設定でリポートするので、DSX 本体の電源はオフにしないでください。
5. 本体がリポートされると、ログイン ページにリダイレクトされます。リセット後に初めてログインしようと
すると、現在出荷時のデフォルトのモードになっていることが画面に表示され、デフォルトのユーザ名
とパスワードでログインした後にパスワードを変更するように求めるプロンプトが表示されます。
6. 詳細については、第 10 章の「[DSX でのファクトリ リセットの実行](#)」セクションを参照してください。

ケース 7. DSX のユーザ プロファイルの管理

1. 目的: DSX ユーザの作成、更新、または削除を行います。
2. Web ブラウザを介して各自のログイン ユーザ名とパスワード(admin/raritan など)で SX にログインし
ます。
3. [User Management(ユーザ管理)]の[User List(ユーザ リスト)]を選択すると、作成したユーザ プロ
ファイルの一覧ページが表示されます。
4. ユーザ プロファイルを作成するには、[Add New User(新規ユーザの追加)]ボタンをクリックし
ます。
5. 既存のユーザ プロファイルを変更する方法の詳細については、「[ユーザ プロファイルの変更](#)」セクシ
ョンを参照してください。
6. 既存のユーザ プロファイルを削除する方法の詳細については、「[ユーザ プロファイルの削除](#)」セクシ
ョンを参照してください。
7. 詳細については、第 5 章の「[ユーザ プロファイルの作成](#)」セクションを参照してください。

ケース 8. RSC を介した DSX のポート アクセスへのアクセス

1. 目的: Raritan Serial Client(RSC)を介して DSX シリアル ターゲットにアクセスします。
2. Web ブラウザを介して各自のログイン ユーザ名とパスワード(admin/raritan など)で SX にログインします。
3. [Port Access(ポート アクセス)]タブを選択して、アクセスするポート名 ([Port 1(ポート1)]など)をクリックします。
4. [YES(はい)]を選択し、表示されるセキュリティの警告を受諾して進みます。
5. Raritan Serial Console(RSC)が別のウィンドウで起動されるので、ENTER キーを押してセッションを「開始」します。
6. RSC ウィンドウ/コンソールでターゲット システムのネイティブコマンドを入力します。
7. [エミュレータ]の[終了]を選択します。次に、[終了の確認]ダイアログ ボックスで[はい]を選択すると、RSC ウィンドウが閉じます。
8. 詳細については、第 7 章の「[Raritan Serial Console](#)」セクションを参照してください。

ケース 9. ポート設定

1. 目的: DSX のシリアル ポートを設定し、ポートに接続されているシリアル ターゲットに合わせて正しいシリアル通信パラメータ(ボーレート、データ ビット、ストップ ビット、フロー制御など)および端末エミュレーション モードを指定します。また、ターゲットを識別しやすいようにポートに名前を付けます。
2. Web ブラウザを介して各自のログイン ユーザ名とパスワード(admin/raritan など)で SX にログインします。
3. [Setup(設定)]の[Port Configuration(ポート設定)]ページを選択し、設定するポート番号に関連付けられているチェック ボックスをチェックして、[Edit(編集)]をクリックします。
4. 詳細については、第 7 章の「[ポート設定](#)」セクションを参照してください。

ケース 10. SX ポートへの CLI/SSH 接続

1. 目的: テキスト ベースのコマンドラインを使用して SX 本体や SX ポートにアクセスします。
2. Windows PC からの SSH アクセス
 - a. SSH クライアント ソフトウェア(Plink、PuTTY など)を起動します。
 - b. DSX サーバの IP アドレス(192.168.0.192 など)および TCP ポート(該当する場合)を入力します。
 - c. SSH(デフォルトの設定ポート 22 を使用)を選択して、[Open(開く)]ボタンをクリックします。
 - d. プロンプトが表示されたら、次のようにユーザ名とパスワードを入力します。

```
login as: admin
password: raritan(デフォルト値)
```
 - e. コンソールに、SX 本体のすべてのポートおよびポート番号が表示されます。
 - f. たとえば、プロンプトでポート番号を次のように入力します。

```
admin> 1
```
 - g. SX コンソールに戻るには、エスケープ シーケンス文字を入力します。たとえば、CTRL キーと右角かっこキー(])を同時に押します。
 - h. ターゲットのシリアル コンソール セッションを終了するには、文字「q」を入力して終了します。SX コンソールにリダイレクトされ、ポート シリアル コンソール セッションがすぐに閉じられます。
3. UNIX ワークステーションからの SSH アクセス
 - a. 次のコマンドを入力してログインします。

```
ssh -l admin 192.168.0.192
```
 - b. admin ユーザ名とパスワードを入力します。

```
login as: admin
```

パスワードのプロンプトが表示されます。デフォルトのパスワード「raritan」を入力します。
 - c. コンソールに、SX 本体のすべてのポートおよびポート番号が表示されます。
 - d. たとえば、プロンプトでポート番号を次のように入力します。

```
admin> 1
```
 - e. SX コンソールに戻るには、エスケープ シーケンス文字を入力します。たとえば、CTRL キーと右角かっこキー(])を同時に押します。
 - f. ターゲットのシリアル コンソール セッションを終了するには、文字「q」を入力して終了します。SX コンソールにリダイレクトされ、ポート シリアル コンソール セッションがすぐに閉じられます。
4. 詳細については、第 12 章の「[Dominion SX への SSH 接続](#)」セクションを参照してください。

空白ページ

付録 A: 仕様

この付録の各セクションでは次の内容について説明します。

- DSX の各モデルおよび仕様
- 動作要件およびテスト済みブラウザの要件
- 一般的なベンダのモデルに DSX を接続するための DSX ハードウェア
- DSX シリアル RJ-45 のピン配列
- DB9 および DB25 の Nulling Serial Adapter のピン配列
- DSX ターミナル ポート

Dominion SX のモデルおよび仕様

次の表に、本体に装備されているポート数(4~48)別の Dominion SX の各モデルを示します。

表 71 Dominion SX の仕様

モデル	ポート	内蔵モデム	ローカル ポート	ETHERNET ポート	電源
DSX4	4	なし	2	1	一重化 AC
DSXB-4-M	4	あり	1	1	一重化 AC
DSXB-4-DC	4	あり	2	1	一重化 DC
DSXB-4-DCM	4	あり	1	1	一重化 DC
DSX8	8	なし	1	1	一重化 AC
DSXA-8	8	あり	1	1	二重化 AC
DSXB-8-M	8	あり	1	1	一重化 AC
DSXB-8-DC	8	なし	2	1	一重化 DC
DSXB-8-DCM	8	あり	1	1	一重化 DC
DSX16	16	あり	1	1	一重化 AC
DSXA-16	16	あり	1	1	一重化 AC
DSXA-16-DC	16	あり	1	1	一重化 DC
DSXA-16-DL	16	なし	2	2	二重化 AC
DSXA-16-DLM	16	あり	1	2	二重化 AC
DSX32	32	あり	1	1	一重化 AC
DSXA-32	32	あり	1	1	二重化 AC
DSXA-32-AC	32	なし	2	1	二重化 AC
DSXA-32-DC	32	あり	1	1	二重化 DC
DSXA-32-DL	32	なし	2	2	二重化 AC
DSXA-32-DLM	32	あり	1	2	二重化 AC
DSXA-48	48	あり	1	2	二重化 AC
DSXA-48-AC	48	なし	2	2	二重化 AC
DSXA-48-DC	48	あり	1	2	二重化 DC

次の表に、Dominion SX の各モデル、それぞれの外形寸法、および重量を示します。

表 72 Dominion SX の外形寸法と重量

モデル	外形寸法 (幅)x(奥行き)x(高さ)	重量
DSX4	290 mm x 270 mm x 44 mm	2.08 kg
DSXB-4-M	290 mm x 270 mm x 44 mm	2.08 kg
DSXB-4-DC	290 mm x 270 mm x 44 mm	2.08 kg
DSXB-4-DCM	290 mm x 270 mm x 44 mm	2.22 kg
DSX8	290 mm x 270 mm x 44 mm	2.17 kg
DSXA-8	440 mm x 290 mm x 44 mm	3.60 kg
DSXB-8-M	290 mm x 270 mm x 44 mm	2.17 kg
DSXB-8-DC	290 mm x 270 mm x 44 mm	2.17 kg
DSXB-8-DCM	290 mm x 270 mm x 44 mm	2.25 kg
DSX16	288 mm x 270 mm x 44 mm	4.35 kg
DSXA-16	440 mm x 290 mm x 44 mm	3.69 kg
DSXA-16-DC	440 mm x 290 mm x 44 mm	3.51 kg
DSXA-16-DL	440 mm x 290 mm x 44 mm	3.86 kg
DSXA-16-DLM	440 mm x 290 mm x 44 mm	3.86 kg
DSX32	438 mm x 288 mm x 44 mm	4.53 kg
DSXA-32	288 mm x 270 mm x 44 mm	3.98 kg
DSXA-32-AC	438 mm x 288 mm x 44 mm	3.98 kg
DSXA-32-DC	440 mm x 290 mm x 44 mm	3.95 kg
DSXA-32-DL	440 mm x 290 mm x 44 mm	3.95 kg
DSXA-32-DLM	440 mm x 290 mm x 44 mm	3.95 kg
DSXA-48	440 mm x 290 mm x 44 mm	4.04 kg
DSXA-48-AC	440 mm x 290 mm x 44 mm	4.04 kg
DSXA-48-DC	440 mm x 290 mm x 44 mm	4.04 kg

動作要件

次の表に、DSX の動作要件を示します。

表 73 Dominion SX の動作要件

動作要件	説明
電源	100V/200V 自動切換え: 50～60 Hz または DC 電源モデルでは-36～72V DC
動作温度	0° ～40° C(32° ～104° F)
動作湿度	20%～85% RH、ただし結露しないこと
動作高度	0～3,048 m のどの高度でも適切に作動
ネットワーク	10/100 Ethernet Base-T 1 本または 2 本、RJ-45 接続
モデム(オプション)	専用モデム DB9M ポート - 多数のモデル: 統合 56K V.92(RJ11 ポート)
プロトコル(オプション)	TCP/IP、RADIUS、SNMP、SMTP、PAP、TACACS+、NFS、HTTP、HTTPS、SSL、SSH、PPP、NTP、LDAP、LDAP(S)、KerberosV5

ブラウザの要件(テスト済み対応ブラウザ)

次の表に、DSX でテスト済みのブラウザを示します。

表 74 ブラウザの要件

プラットフォーム	ブラウザ
WIN XP Professional SP2 - SUN JRE 1.5.0_06	IE 6.0
	IE 7.0
	Firefox 2.0
WIN XP Home Edition SP2 - SUN JRE 1.5.0_06	IE 6.0
	IE 7.0
	Netscape 7.1
	Firefox 1.5.0.1
	Mozilla 1.6
WIN 2000 Professional SP4 - SUN JRE 1.5.0_06	IE 6.0
	Firefox 1.5.0.1
WIN 2000 Professional SP2 - SUN JRE 1.4.2_05	IE 6.0
Fedora Core 4 JRE 1.4.2_05	Mozilla 1.6
	Netscape 7.1
Slackware 10.2	Firefox 1.5.0.6
FreeBSD 6.1	Firefox 1.5.0.7

接続性

次の表に、Dominion SX を一般的なベンダ／モデルの組み合わせと接続するのに必要な DSX ハードウェア(アダプタやケーブル)を示します。

表 75 接続性

ベンダ	デバイス	コンソールコネクタ	シリアル接続
Checkpoint	ファイアウォール	DB9M	ASCSD9F アダプタと CAT5 ケーブル
Cisco	PIX ファイアウォール		
Cisco	Catalyst	RJ-45	CRLVR-15 ロールオーバー ケーブル、または CRLVR-1 アダプタ ケーブルと CAT5 ケーブル Dominion SX-48 の各モデルのターミナルポート(RJ-45 コネクタ タイプ)を別の Dominion SX に接続するための CRLVR-1 ケーブル
Cisco	ルータ	DB25F	ASCSD25M アダプタと CAT5 ケーブル
Hewlett Packard	UNIX サーバ	DB9M	ASCSD9F アダプタと CAT5 ケーブル
Silicon Graphics	Origin		
Sun	SPARCStation	DB25F	ASCSD25M アダプタと CAT5 ケーブル
Sun	Netra T1	RJ-45	CRLVR-15 ケーブル、または CRLVR-1 アダプタ ケーブルと CAT5 ケーブル
Sun	Cobalt	DB9M	ASCSD9F アダプタと CAT5 ケーブル
各種ベンダ	Windows NT		
Raritan	RPCU	RJ-45	CSCSPCS-10 ケーブルまたは CSCSPCS-1 アダプタ ケーブル

一般的に使われるケーブルやアダプタの一覧については、
<http://www.raritan.com/support> を参照してください。

Dominion SX シリアル RJ-45 のピン配列

ポート密度を最大にしてシンプルな UTP(カテゴリ5)配線を可能にするために、Dominion SX では、コンパクトな RJ-45 ポート経由でのシリアル接続を実現できます。ただし、RJ45 接続でのシリアル データ送信には、広く採用されている業界標準は存在しません。

次の表に、DSX の背面にある RJ-45 コネクタのピン配列を示します。

表 76 Dominion SX RJ-45 のシリアル ピン配列とシグナル

RJ-45 ピン	シグナル
1	RTS
2	DTR
3	TxD
4	GND
5	シグナル GND
6	RxD
7	DSR
8	CTS

Dominion SX シリアル ピン配列(RJ-45)に関する最新の情報については、次のリンクを参照してください。

<http://www.raritan.com/support>

DB9F Nulling Serial Adapter のピン配列

表 77 DB9F Nulling Serial Adapter のピン配列

RJ-45(メス)	DB9(メス)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB9M Nulling Serial Adapter のピン配列

表 78 DB9M Nulling Serial Adapter のピン配列

RJ-45(メス)	DB9(オス)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB25F Nulling Serial Adapter のピン配列

表 79 DB25F Nulling Serial Adapter のピン配列

RJ-45(メス)	DB25(メス)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

DB25M Nulling Serial Adapter のピン配列

表 80 DB25M Nulling Serial Adapter のピン配列

RJ-45(メス)	DB25(オス)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

Dominion SX ターミナル ポート

すべての Dominion SX モデル(DSX16と DSX32 を除く)では、2 つの DB9M シリアル ポートのピン配列は同じです。これは、シリアル ポートを 2 つ備えているモデルに当てはまります。すべての二重化 LAN(二重化電源)モデルに RJ-45 シリアル ポートが装備されています。DSX16と DSX32 の各モデルには、外部 DB9M シリアル ポート(TERMINAL というラベルが付いている)が 1 つしかありません。すべての二重化 LAN(二重化電源)モデルに RJ-45 シリアル ポートが装備されています。DSX16と DSX32 の各モデルには、外部 DB9M シリアル ポート(TERMINAL というラベルが付いている)が 1 つしかありません。

どちらのポートも、VT100ターミナルまたは同等のターミナル(ハイパーターミナル、Linux の Minicom などの VT100 エミュレーション ソフトウェアを実行する PC)をサポートしています。ローカル ポート アクセスを有効にし、ポートが正常に機能するように、管理対象デバイスと同じ速度に設定する必要があります。SSH または Telnet が利用できる場合は、lpa コマンドを使用して GUI や CLI からローカル ポート アクセスを有効または無効にすることができます。Dominion SX 本体の Telnet サーバは、デフォルトでは無効になっています。

ターミナル ポートを 2 つ備えるモデルでは、RI シグナルを使用するポートでのみ外付けモデムをサポートします。シリアル ポートが 1 つしかないモデルにはモデムが内蔵されています。外部アクセス可能なシリアル ポートでは RI シグナルを使用していないので、VT100ターミナルや同等のターミナルなどのデバイスのみをサポートします。

次の表に、1 番目の DB9M シリアル ポートのピン配列を示します。

表 81 Dominion SX ターミナル ポートのピン配列 - 1 番目のポート

DB9M ピン	シグナル
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

2 番目の DB9M シリアル ポートでは、次の表に示す 2 つのピンのみをサポートします(ピン 4 とピン 7 は「H(ハイ)」に固定されています)。

表 82 Dominion SX ターミナル ポートのピン配列 - 2 番目のポート

DB9M ピン	シグナル
1	
2	RxD
3	TxD
4	DTR(H)
5	GND
6	

7	RTS(H)
8	
9	

Dominion SX16 および SX32 のターミナル ポート

DSX16 および DSX32 には Ring Indicator(RI)シグナルが存在しないため、DSX16 や DSX32 のターミナル ポートにはモデムを接続しないでください。これらのモデルは、内蔵モデムを搭載しており、そのモデムを有効または無効にすることができます。モデムは、デフォルトでは無効となっています。

表 83 Dominion SX16 および SX32 のターミナル ポートのピン配列

DB9M ピン	色	シグナル
1	茶	GND
2	赤	RxD
3	橙	TxD
4	—	—
5	緑	GND
6	接続なし	
7	紫	RTS
8	灰	CTS
9	青	BUSY - ファクトリ リセット プラグ用に予約済み

以下は、Dominion SX16 および SX32 のターミナル ポートに関する追加情報です。

- ピン 1 とピン 9 は、2004 年 8 月以降に出荷された本体を出荷時の設定に戻す場合に使われます。
- 2004 年 8 月より前に出荷された本体は、RESERVED(TERMINAL/RESERVED ではない)というラベルの付いた DB9M ポートを備えています。その理由は、このポートが、各 SX 本体に付属するファクトリ リセット アダプタを使用して、本体を出荷時の設定に戻す場合に使用されていたからです。ピン 1 とピン 6 はファクトリ リセットに使われていました。こうした初期本体のリセット アダプタは、現在の本体とは異なり、ローカル ポート機能を備えています。
- SX2.2(またはそれ以降の)リリースで出荷された DSX16 と DSX32 の本体は、ローカル ポート機能をサポートしています。
- SX2.5 までの DSX の各バージョンでは、ローカル ポートは出荷時の設定で無効となっています。
- DSX3.1 またはそれ以降のバージョンでは、ローカル ポートはデフォルトで有効となっています。

付録 B: システム デフォルト

この付録では、システム デフォルトおよびポート アクセスの手順について説明します。

表 84 Dominion SX のシステム デフォルト

項目	デフォルト
IP アドレス	192.168.0.192
サブネット マスク	255.255.255.0
CSC ポート アドレス(TCP)	5000
CC 検出用ポート アドレス(UDP)	5000
工場出荷時のユーザ名	admin
工場出荷時のパスワード	raritan
一般設定	
ダイレクト ポート アクセス(DPA)	標準モード(オフ)
TACACS+	無効
RADIUS	
LDAP	
ローカル ポート アクセス	
HTTP	有効
HTTPS	
SSH	
Syslog	
イベント通知	無効
ダイヤル バック	
IP-ACL	
モデム	
NTP	
Telnet	
SMTP	
SNMP	
NFS にログ	
シリアル ポート	
ポー レート	9600
パリティ	なし
フロー制御	なし

ポート アクセスを開始する場合は、次の情報を使用してください。

表 85 ポート アクセスの開始

ポート アクセスの開始手段	開いたままにしておくポートと閉じるポート	通信方向
HTTP	ポート 80、443、および 5000 は、本体が動作するためにファイアウォールで開いておく必要があります。ポート 5000 は設定可能です。	双方向
HTTPS SSL(S)のみ	TCP ポート 443 が開いている必要があります。ポート 80 は閉じてかまいません。	双方向
SSH	TCP ポート 22 が開いている必要があります。	双方向
Telnet	TCP ポート 23 が開いている必要があります。	双方向
RADIUS	TCP ポート 1812 が開いている必要があります。	送信
LDAP	ポート 389 が開いている必要があります。	送信
SNMP	ポート 162 が開いている必要があります。	送信
TACACS+	ポート 49 が開いている必要があります。	送信
注意:		
FTP アップグレードの場合	ポート 21 が開いている必要があります。	送信
syslog の場合	UDP ポート 514 が開いている必要があります。	送信

NFS ログ記録、LDAP サーバなどを使用する場合は、さらにポートを開く必要があります。これらのポートは、ネットワーク トポロジ、VLAN(Virtual Local Area Network)、ファイアウォール設定など、インストール形態によって異なります。サイト固有の情報および設定については、ネットワーク管理者にお問い合わせください。

付録 C: 証明書

この付録の各セクションでは、証明書および証明機関(CA)について説明し、次の操作を行う手順を示します。

- Dominion SX の CA 証明書をブラウザ証明書にインストールする
- IE ブラウザ用の SX サーバ証明書をインストールする
- Netscape Navigator 用の SX サーバ証明書をインストールする
- サードパーティのルート証明書をブラウザにインストールする
- ** 署名するサードパーティ CA の CSR を生成する
- ** サードパーティの証明書を SX にインストールする
- ** クライアント ルート証明書を SX にインストールする
- ** クライアント証明書を Internet Explorer にインストールする
- ** クライアント証明書を Netscape Navigator にインストールする

証明機関(CA)とは、第三者によって使用されるデジタル証明書を発行する団体のことです。これらの証明書には、一般的な暗号化に関する文献に記載されているように、パブリック キーとプライベート キーのペアが使用されます。サービスが有料である商用 CA は数多くありますが、Dominion SX は、独自の証明書を生成する無料の CA としての役割を果たします。CA および証明書は、特に SSL において、有効なセキュリティ テクノロジーの一部としてブラウザや Web サーバに組み込むことができます。ブラウザやオペレーティング システムには、インストール済みの信頼できる証明機関のリスト(別名: 信頼できるルート CA ストア)が付属しています。Dominion SX 証明書は、信頼できる CA としてブラウザに追加できます。

デフォルトの SX 証明機関の設定

ブラウザがサーバ証明書を信頼するためには、Dominion SX 本体で生成されたサーバ証明書がブラウザにインストールされている必要があります。

SSL 対応の Dominion SX 本体にアクセスするたびに、New Site Certificate(新規サイト証明書)ウィンドウが開きます。セッションごとにこの証明書を受諾することも、セッション証明書を恒久的に受諾してこのウィンドウが表示されないようにすることもできます。以降の手順では、ブラウザの証明書ストアに SX 本体の証明書をインストールする方法を示しています。

これらの手順は、Dominion SX にアクセスする各クライアント ブラウザに対してアクセスする SX 本体ごとに実行する必要があります。

IE ブラウザ用の CA ルートのインストール

SSL 対応の Dominion SX 本体にアクセスするたびに、New Site Certificate(新規サイト証明書)ウィンドウが開きます。このウィンドウを表示しないようにするには、セッション証明書を恒久的に受諾するか、使用するブラウザにサーバ証明書を直接インストールします。

証明書の受諾(セッション ベース)

Dominion SX 本体に初めて接続すると、証明書の警告画面が表示されます。この証明書は、デフォルトでは前述のようにローカル SX 本体の CA によって署名されており、続行するには、この証明書を受諾する必要があります。この Dominion SX 本体でこのウィンドウを今後表示しないようにするには、使用するブラウザにサーバ証明書をインストールする必要があります。この手順については、後の「**証明書の受諾(セッション ベース)**」セクションを参照してください。

Internet Explorer への Dominion SX サーバ証明書のインストール

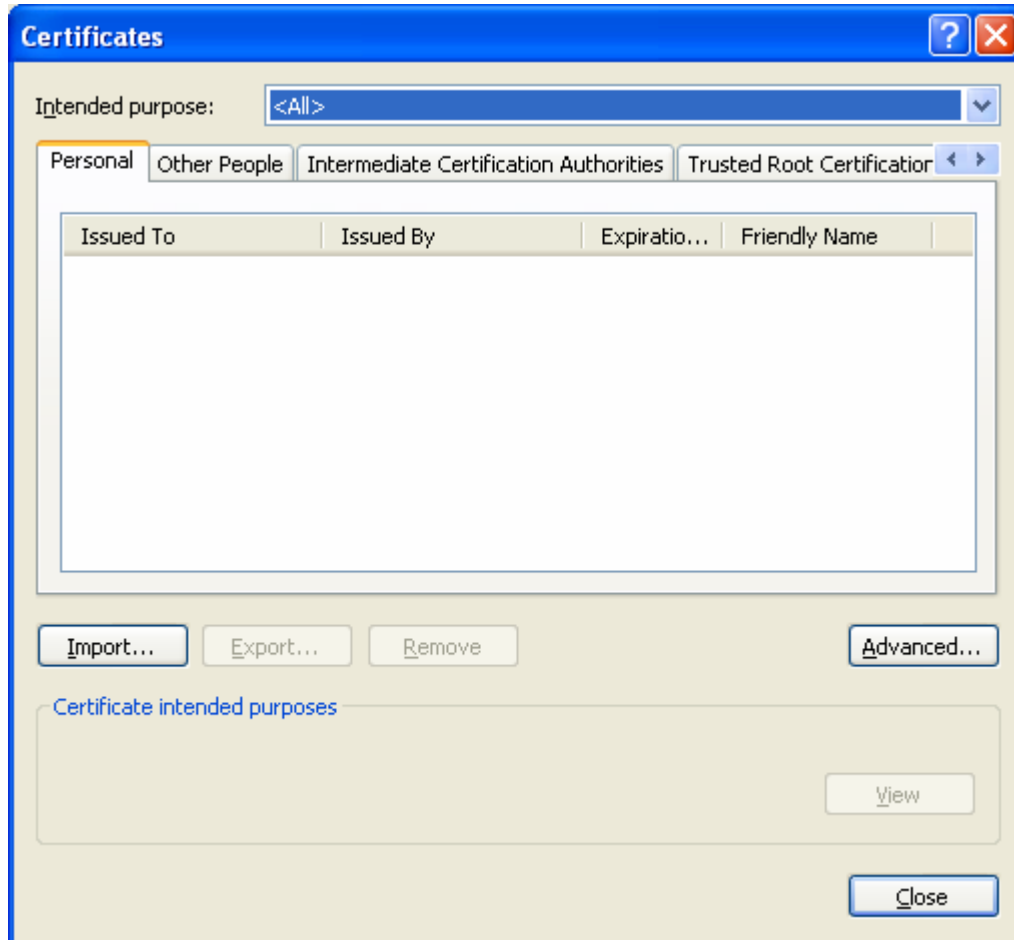
IE に Dominion SX サーバ証明書をインストールして、Dominion SX 本体へのアクセス時に Security Alert(セキュリティ警告)ウィンドウが表示されないようにすることができます。アクセスする SX 本体ごとに、次の手順を実行する必要があります。

1. IE を起動し、Dominion SX 本体に接続します。
2. Security Alert(セキュリティ警告)メッセージが表示されます。[Yes(はい)]を選択します。
3. 必要に応じてユーザ名とパスワードを入力し、本体にログオンします。
4. [Security(セキュリティ)]タブを選択して、[Certificate(証明書)]リンクをクリックします。
5. [View Default Certificate(デフォルト証明書の表示)]ラジオ ボタンをクリックして、[OK]をクリックします。ダイアログ ボックスが開き、証明書の表示の開始、保存、またはキャンセルが求められます。保存を選択し、ファイルの拡張子".cer"を追加します(「CA_ROOT.cer」など)。
6. 「CA_ROOT.cer」ファイルをダブルクリックして開きます。これで証明書が開きます。
7. [Open(開く)]ボタンをクリックし、[Install Certificate(証明書のインストール)]ボタンをクリックします。
8. [Next(次へ)]をクリックします。
9. [Automatically select the certificate store based on the type of certificate(証明書のタイプに基づいて証明ストアを自動的に選択する)]ラジオ ボタンをクリックします。証明書マネージャが自動的に証明書ストアを選択しないようにするには、[Place all certificates in the following store(下記のストアにすべての証明書を保存する)]ラジオ ボタンをクリックし、[Browse(参照)]をクリックしてファイルを選択します。
10. [Next(次へ)]をクリックします。
11. [Finish(完了)]をクリックします。
12. [OK]をクリックします。
13. 証明書をインストールしたら、Dominion SX に接続している IE ブラウザを含む、すべての IE ブラウザを閉じます。その後、新たにIEブラウザを起動して作業を続けます。次回の本体に接続時には、信頼できる証明書の警告ウィンドウは表示されません。

Internet Explorer での受諾済み証明書の削除

以前に受諾した証明書を本体から削除する方法は、Raritan のデフォルト証明書を削除する場合もユーザがインストールしたサードパーティ証明書を削除する場合も同じです。

1. IE を起動して、[ツール]メニューの[インターネット オプション]をクリックします。インターネット オプション ウィンドウが表示されます。
2. [コンテンツ]タブをクリックして、[証明書]をクリックします。証明書ウィンドウが表示されます。



3. 証明書のリストをスクロールし、削除する証明書を選択します。通常、証明書は[ほかの人]タブに表示され、名前で識別します。この名前は、Dominion SX の IP アドレスとなります。
4. [削除]をクリックします。メッセージ ダイアログが表示されます。
5. [はい]をクリックして証明書を削除します。
6. [証明書]ダイアログ ボックスの[閉じる]をクリックして、ダイアログ ボックスを閉じます。
7. [インターネット オプション]ダイアログ ボックスの[OK]をクリックして、ダイアログ ボックスを閉じます。

Netscape Navigator 用の Dominion SX サーバ証明書のインストール

Netscape に Dominion SX サーバ証明書をインストールして、Dominion SX 本体へのアクセス時に Security Alert(セキュリティ警告)ウィンドウが表示されないようにすることができます。各クライアントのブラウザからアクセスする SX 本体ごとに、次の手順を実行する必要があります。

証明書の受諾(セッションベース)

Dominion SX 本体に初めて接続すると、証明書の警告画面が表示されます。この証明書は、デフォルトでは前述のようにローカル SX 本体の CA によって署名されており、続行するには、この証明書を受諾する必要があります。この Dominion SX 本体でこのウィンドウを表示しないようにするには、使用するブラウザにサーバ証明書をインストールする必要があります。この手順については、後の Dominion SX サーバ証明書のインストールのセクションを参照してください。

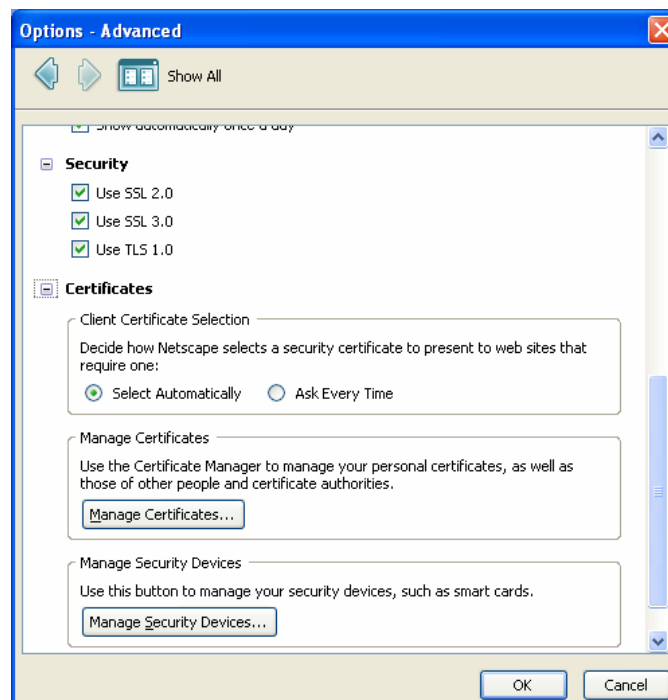
Netscape Navigator への Dominion SX サーバ証明書のインストール

1. Netscape Navigator を起動し、Dominion SX 本体の IP アドレスに接続します。Web Site Certified by an Unknown Authority(不明な認証機関によって証明された Web サイト)ウィンドウが表示されます。
2. [Accept this certificate permanently(この証明書を恒久的に受諾する)]を選択して、[OK]をクリックします。
3. Security Warning(セキュリティ警告)ウィンドウで[OK]をクリックします。
4. これでこのコンピュータで Raritan デフォルト証明書が受諾されました。

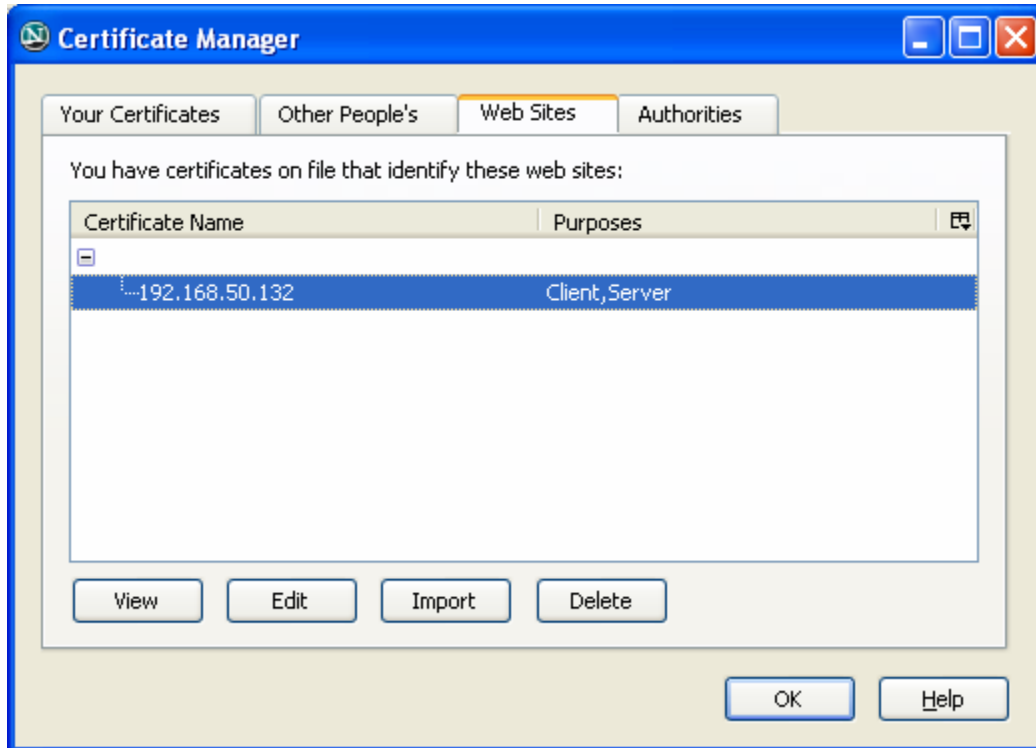
受諾した証明書の削除

以前に受諾した証明書を Dominion SX 本体から削除する方法は、Raritan のデフォルト証明書の削除の場合もユーザがインストールしたサードパーティ証明書の削除の場合も同じです。

1. [Tools(ツール)]メニューの[Options(オプション)]をクリックします。
2. [Advanced(詳細)]パネルを選択して、[Certificates(証明書)]をダブルクリックして開きます。
3. [Manage Certificates(証明書の管理)]セクションで、[Manage Certificates(証明書の管理)]ボタンをクリックします。証明書マネージャが表示されます。



- [Web Sites(Web サイト)]タブを選択し、Dominion SX の IP アドレスでの共通名となっている証明書の名前を選択して、[Delete(削除)]ボタンをクリックします。



- 証明書の削除を確認する Delete Web Site Certificates(Web サイト証明書の削除)ウィンドウで、[OK]をクリックします。
- ウィンドウの左側で、**Certificates(証明書)**に移動して **Web Sites(Web サイト)**をクリックします。
- Options - Advanced(オプション - 詳細)ウィンドウで[OK]をクリックします。

サードパーティのルート証明書のインストール

本体にサードパーティのルート証明書をインストールすると、証明書を発行した証明機関から、対応するルート証明書を取得できます。この方法はどの CA にも使用できますが、ここでは Thawte を例に挙げています。

証明書が発行された CA から、ルート証明書をダウンロードすることができます。ルート証明書は、CA の Web サイトからダウンロード可能です。リンクをクリックしてダウンロードします。よく使われている CA とそのサイトを次に示します。

Thawte Digital Certificate Services	http://www.thawte.com/
VeriSign Incorporated	http://www.verisign.com/

注 CA によっては、ダウンロード用ルート証明書ではなく、テキスト形式のルート証明書コードを提供していることがあります。その場合は、ルート証明書コードを選択してコピーし、Raritan ルート証明書のインストールのセクションに説明されている手順に従って操作してから、次の手順を実行してください。

Internet Explorer へのサードパーティのルート証明書のインストール

Internet Explorer にサードパーティの証明書をインストールするために、前述の「[Internet Explorer への Dominion SX サーバ証明書のインストール](#)」セクションの手順に従って CA 証明書をダウンロードし、インストールすることができます。

Netscape Navigator へのサードパーティのルート証明書のインストール

1. CA の Web サイトでルート証明書のリンクをクリックすると、New Certificate Authority(新規認証機関)ウィンドウが開きます。[Next(次へ)]をクリックし、その後に表示される画面でも[Next(次へ)]をクリックします。
2. 証明フィンガープリントが表示され、CA とダウンロードするルート証明書についての情報が示されます。表示は次のウィンドウに似ています。[Signed by(署名者)]の情報を記録し、[Next(次へ)]をクリックします。
3. [Accept this Certificate Authority for Certifying network sites(Web サイトを証明するためにこの認証機関を信頼する)]チェック ボックスをオンにします。2 番目と3 番目のチェック ボックスは必須ではありません。
4. [Next(次へ)]をクリックし、もう一度[Next(次へ)]をクリックします。認証機関の名称を入力するフィールドには、手順 6 で記録した[Signed by(署名者)]の名称を入力します。
5. [Finish(完了)]をクリックします。これでこのコンピュータに、この CA のルート証明書がインストールされました。
6. ルート証明書が既にインストールされている場合は、エラーが表示されます。現在インストールされている証明書を削除するには、次の手順に従います。
7. Netscape の[Security(セキュリティ)]ボタンまたは左下にあるロック アイコンをクリックし、Security Information(セキュリティ情報)ウィンドウにアクセスします。
8. 左のパネルの **Certificates(証明書)**セクションにある[**Signers(署名者)**]をクリックし、現在インストールされているルート証明書のリストを表示します。
9. インストールする証明書を発行している CA の名前を探します。インストールする CA に対する複数のリストが表示される場合があります。インストールしようとしている証明書と同じ名前のリストを選択します。
10. [Delete(削除)]をクリックして、[OK]をクリックします。
11. CA の Web サイトに戻り、再度ルート証明書をダウンロードして、手順 1~5 を繰り返します。

署名するサードパーティ CA の CSR の生成

証明書への署名を行う Dominion SX の内部 CA ではなく、SX にサードパーティ CA の証明書 (Verisign など)をインストールするには、署名対象の SX で証明書署名リクエスト(CSR)を生成する必要があります。サードパーティ CA は、この CSR を利用して証明書を生成します。この証明書は、SX で使用するこのサードパーティ証明書用のサードパーティ CA のパブリック キーとともに SX にインストールする必要があります。この証明書とキーは、その後で Dominion SX にもインストールする必要があります。

1. [Security(セキュリティ)]タブで、[Certificate(証明書)]を選択します。
2. [Generate Certificate Signing Request(証明書署名リクエスト(CSR)の生成)]ラジオ ボタンをクリックします。
3. ラジオ ボタンの下にある各パラメータに、ビット、名前などを入力します。電子メール アドレスが必須であることに注意してください。
4. [OK]をクリックします。
5. [View Certificate Signing Request(証明書署名リクエスト(CSR)の表示)]を選択して、ファイルを保存します。
6. CSR をサードパーティ CA から署名してもらい、CA の証明書とパブリック キーを受け取ります。

SX へのサードパーティ証明書のインストール

サードパーティ CA の証明書を SX にインストールするには、署名対象の SX で証明書署名リクエスト (CSR) を生成する必要があります。CA は、この CSR を利用して証明書を生成します。この証明書を、SX で使用するこのサードパーティ証明書用の CA のパブリック キーとともに SX にインストールする必要があります。この証明書とキーは、その後で Dominion SX にもインストールする必要があります。

1. 証明書とパブリック キーをアクセス可能な FTP サーバ上に配置します。
2. [Security(セキュリティ)] タブで、[Certificate(証明書)] を選択します。
3. [Install User Key(ユーザ キーのインストール)] ラジオ ボタンをクリックします。
4. FTP の各パラメータを挿入して CA のパブリック キー ファイルを取得します。
5. [OK] をクリックします。ペインの上部に「User Key Installed(ユーザ キーがインストールされました)」というメッセージが表示されます。
6. [Install User Certificate(ユーザ証明書のインストール)] ラジオ ボタンをクリックします。
7. FTP の各パラメータを入力して CA の署名付き証明書を取得します。
8. [OK] をクリックします。ペインの上部に「User Certificate Installed(ユーザ証明書がインストールされました)」というメッセージが表示されます。
9. SX デバイスを再起動して設定を有効にします。

SX へのクライアント ルート証明書のインストール

クライアント証明書が SX で有効な証明書であると認識されるようにするには、クライアント証明書に署名した CA のルート証明書を、次の手順で SX 本体にインストールする必要があります。

1. クライアント証明書への署名に使われた CA のルート証明書を取得して、それをアクセス可能な FTP サーバ上に配置します。
2. [Security(セキュリティ)] タブで、[SSL Client Certificates(SSL クライアント証明書)] を選択します。
3. [Install Certificate Authority(証明機関のインストール)] を選択します。
4. FTP の各パラメータを入力して CA のルート証明書を取得します。
5. [OK] をクリックします。
6. [Enable SSL Client Certificate(SSL クライアント証明書を有効にする)] チェック ボックスがオンになっていることを確認します。
7. SX デバイスを再起動して設定を有効にします。

Internet Explorer へのクライアント証明書のインストール

Internet Explorer にクライアント証明書をインストールするには、次のリンクで説明されている手順に従ってください。

<http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.msp?mfr=true>

空白ページ

付録 D: サーバ設定

この付録の各セクションでは、次の認証プロトコル向けに Dominion SX 本体や認証サーバを設定する手順について説明します。

- Microsoft インターネット認証サービス(IAS)RADIUS サーバ
- Cisco Access Control Server(ACS)RADIUS サーバ
- TACACS+(Terminal Access Controller Access-Control System Plus)

Microsoft IAS RADIUS サーバ

インターネット認証サービス(IAS)は、Microsoft による RADIUS(Remote Authentication Dial-In User Service)プロトコルの実装です。このセクションの手順では、IAS サーバを使用するように Dominion SX を設定する方法について説明しています。

IAS RADIUS サーバを使用するための Dominion SX の設定

IAS RADIUS サーバを使用するために Dominion SX 本体を設定するタスクは、次のとおりです。

- プライマリ RADIUS サーバ(およびオプションでセカンダリ RADIUS サーバ)の設定
- RADIUS ポートの設定
- IAS 内の IAS クライアント設定に一致する秘密情報(共有シークレット)の設定

次の例は、新規 IAS インストールに基づいた単純な設定について示しています。

注 IAS 設定が既に存在する場合、これらの手順は、実際の手順と異なることがあります。

サーバでの IAS の有効化

1. IAS サーバの[コントロール パネル]で[プログラムの追加と削除]を開きます。
2. [Windows コンポーネントの追加と削除]ボタンをクリックします。
3. [ネットワーク サービス]を選択して、[詳細]ボタンをクリックします。
4. [インターネット認証サービス]チェック ボックスをオンにして、[OK]をクリックします。
5. [次へ]ボタンをクリックして続行し、ウィザードの手順を完了します。

IAS Active Directory アクセス

ドメイン コントローラを使用する場合は、次の手順を使用して、IAS が Active Directory にアクセスするように設定します。

1. IAS を起動します([スタート]、[すべてのプログラム]、[管理ツール]、[インターネット認証サービス]の順に選択)。
2. [インターネット認証サービス(ローカル)]を右クリックし、[Register Server in Active Directory(Active Directory にサーバーを登録)]を選択します。

注 Active Directory の詳細については、Microsoft の URL <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051> を参照してください。

クライアント リストへの Dominion SX の追加

1. インターネット認証サービスで、[RADIUS クライアント]を右クリックし、[新しい RADIUS クライアント]を選択します。
2. DSX 本体のわかりやすい名前と IP アドレスを入力します。
3. [クライアント ベンダ]ドロップダウン メニューで[RADIUS Standard]を選択し、Dominion SX 設定に一致する共有シークレットを入力します。

IAS ポリシーの作成

このセクションでは、RADIUS ユーザに対して Dominion SX へのアクセスを許可するポリシーを作成する手順について説明します。以下の例では、2 つの条件(Dominion SX のクライアント ソース IP アドレスおよび UserID が SX ユーザ グループのメンバーであること)を満たしている必要があります。

- NAS-IP-Address = Dominion SX の IP アドレスを入力
- Windows-Groups = SX ユーザ グループ

注 複数の Dominion SX 本体または Dominion 製品ファミリの各種モデル(DKX、DKSX、または KX101)がある場合は、NAS-IP-Address(NAS IP アドレス)ルールと一致する適切な条件を使用すると、該当する Dominion 本体の正しいポリシーを適用できるようになります。

1. インターネット認証サービスで、[リモート アクセス ポリシー]を右クリックし、[新しいリモート アクセス ポリシー]を選択します。
2. 新しいリモート アクセス ポリシー ウィザードが起動します。[次へ]をクリックします。
3. [カスタム ポリシーを設定する]ラジオ ボタンをクリックして、ポリシー名を入力します。
4. [条件]ダイアログ ボックスが表示されます。[追加]ボタンをクリックします。
5. [NAS-IP-Address]を選択して、[追加]ボタンをクリックします。Dominion SX 本体の IP アドレスを入力します。
6. [Windows-Groups]と値「SX ユーザ グループ」を使用して 2 番目の条件を入力します。[次へ]をクリックします。
7. [リモート アクセス許可を与える]ラジオ ボタンをクリックします。
8. [次へ]をクリックします。[プロファイル]ダイアログ ボックスが表示されます。
9. [プロファイルの編集]ボタンをクリックします。
10. [認証]タブを選択します。他のチェック ボックスをオフにして、[暗号化されていない認証(PAP、SPAP)]チェック ボックスをオンにします。

注 このバージョンの Dominion SX では、チャレンジ認証プロトコル(CHAP)をサポートしていません。

11. [詳細]タブを選択します。[Framed-Protocol]を削除します。

注 各ポリシーには、いくつかの満たすべき条件があります。条件を満たさない場合、IAS は、次のポリシーで条件を調べます。

12. [追加]ボタンをクリックします。RADIUS の属性リストが表示されます。
13. [Filter-Id Name(Filter-Id 名)]を選択して、[Add(追加)]ボタンをクリックします。[Attribute values(属性値)]セクションで[Add(追加)]をクリックします。属性値「Raritan:G{Admin}」を入力します。
14. [OK]をクリックします。

G{}内の値は、DSX のローカル グループの名前(この場合は、デフォルトの Admin グループ)です。

- ダイアル バック機能を使用する場合は、G{}内の値は Raritan:G{Admin}:D{1234567890}と指定できます。1234567890 は、ダイアル バック用の電話番号です。
- 値 Raritan:G{Admin}は、Dominion SX のローカル グループと一致している必要があります。

- Dominion SX は、出荷時にデフォルトの Admin グループが設定されています。
 - Dominion SX 本体でその他のユーザ グループを作成するには、[User Management(ユーザ管理)]の[User Group(ユーザ グループ)]オプションを使用します。
 - 適切なポート アクセスとユーザ クラス(オペレータまたは監視者)を定義できます。Dominion SX 本体にアクセスする RADIUS ユーザを承認するには、グループ名を適宜 Filter-Id 属性値で指定する必要があります。
15. 新しいポリシーを、ポリシー リストの 1 番目(最上位)のポリシーとして表示されるように移動します。

注 必要に応じて、グループのメンバーであるすべてのユーザに対してダイヤルアップ アクセスを許可するポリシーを作成してください(Windows では、ダイヤル インを有効にしたユーザからのアクセスを許可するデフォルトのポリシーが既に設定されている場合があるので、この新しいポリシーはオプションです。新しいポリシーを使用する場合は、そのポリシーがデフォルトのポリシーよりも上に表示されていることを確認してください)。

16. サービスが開始されていることを確認します。
17. ユーザの Active Directory / ローカル アカウントのダイヤル インが、ユーザ プロファイルで有効になっていることを確認します。Windows 2000 のドメイン サーバがネイティブ モードで、IAS が Active Directory に登録されている場合は、[User Profile(ユーザ プロファイル)]の[Dial In(ダイヤル イン)]を設定して、リモート アクセス ポリシーを使用します。

Cisco ACS RADIUS サーバ

Cisco Access Control Server(ACS)は、Dominion SX 本体でサポートされている別の認証ソリューションです。RADIUS をサポートする Dominion SX では、本体とユーザ情報の両方が RADIUS の設定に追加されている必要があります。

Cisco ACS サーバを使用するための Dominion SX の設定

次の手順では、Dominion SX 本体を設定して、Cisco RADIUS サーバで使用するようになります。

1. DSX の画面で[User Management(ユーザ管理)]タブを選択します。
2. [Configuration(設定)]セクションに移動します。
3. [User Group List(ユーザ グループ リスト)]を選択します。
4. [Add New User Group(新規ユーザ グループの追加)]をクリックします。

ポート アクセスとユーザ クラス(オペレータまたは監視者)を定義できます。このユーザ グループは、後で Cisco RADIUS サーバの Filter-Id 属性の値として使われます。Dominion SX には、出荷時のデフォルトのグループ Admin が設定されており、これをこのセクションでは例として使用しますが、任意のローカルグループを、Cisco ACS サーバの Filter-Id 属性の値として使用することもできます。

注 グループ名は、大文字と小文字が区別されるので、RADIUS サーバの Filter-Id 属性で定義されているグループ名と完全に一致させる必要があります。

Cisco RADIUS サーバのバージョン 3.1 でのみテストが実施されましたが、他バージョンの RADIUS サーバでも DSX は動作します。

Cisco ACS サーバの設定

1. ブラウザを使用して Cisco ACS サーバにログオンします。
2. ユーザ名とパスワードを入力します。
3. [Login(ログイン)]をクリックします。
4. 画面の左パネルにある[Network Configuration(ネットワーク設定)]をクリックし、[Add Entry(エントリの追加)]を選択して AAA クライアントを追加と編集を行います。この操作は、RADIUS でアクセスする本体ごとに行う必要があります。
5. [Authenticate Using(認証に使用)]ドロップ ダウン メニューをクリックし、リストから [RADIUS(IETF)]を選択します。
6. [Submit(送信)]をクリックします。
7. 画面の左パネルにある[Interface Configuration(インタフェース設定)]をクリックします。
8. [RADIUS(IETF)]リンクをクリックしてプロパティを編集します。
9. [User(ユーザ)]列と[Group(グループ)]列で、[Filter-Id(Filter-Id)]の前にあるチェック ボックスをオンにします。
10. [Submit(送信)]をクリックします。
11. 新規ユーザを追加して RADIUS(IETF)属性を設定するには、画面の左パネルにある[User Setup(ユーザ設定)]をクリックします。
12. ユーザ名を入力して[Add/Edit(追加と編集)]をクリックします。
13. 既存のユーザを編集するには、画面の左パネルにある[User Setup(ユーザ設定)]をクリックし、[List All Users(すべてのユーザを表示)]をクリックします。
14. リストからユーザを選択します。
15. ユーザを選択したら、ユーザ プロパティのページで、[IETF RADIUS Attribute(IETF RADIUS 属性)]セクションを下へスクロールします。
16. [Filter-Id]チェック ボックスをオンにして、この属性に値「Raritan:G{ Admin}」を追加します。G{ }内の値は、DSX のローカル グループの名前(この場合は、デフォルトの Admin グループ)です。
ダイヤル バック機能を使用する場合は、G{ }内の値に Raritan:G{ Admin}:D{ 1234567890}を指定できます。1234567890 は、ダイヤル バック用の電話番号です。
 - 値 Raritan:G{ Admin}は、Dominion SX 本体のローカル グループと一致している必要があります。
 - Dominion SX は、出荷時にデフォルトの Admin グループが設定されています。
 - Dominion SX 本体でその他のユーザ グループを作成するには、[User Management(ユーザ管理)]の[User Group(ユーザ グループ)]オプションを使用します。
 - 適切なポート アクセスとユーザ クラス(オペレータまたは監視者)を定義できます。また、Dominion SX 本体にアクセスする RADIUS ユーザを承認するには、グループ名を適宜 Filter-Id 属性値で指定する必要があります。
17. [Submit(送信)]をクリックします。

注 Dominion SX で複数の RADIUS ユーザが同じ認証を必要としている場合は、これらのユーザが同じグループに属していれば、Filter-Id 属性とその値を Cisco ACS のグループ レベルで定義することができます。

TACACS+サーバ設定

Dominion SX 本体では、認証サービスとして TACACS+(Terminal Access Controller Access-Control System Plus)を利用できます。

Dominion SX には、追加される新しいサービスと、サーバから戻される 2 つの引数値のペアが必要です。新しいサービス名は `dominionsx` です。有効な認証パラメータは `user-group` です。このユーザにモデムダイヤルバックが設定されている場合、有効なダイヤルバックパラメータは `user-dialback` になります。

- **user-group:** Dominion SX のローカルグループと一致するユーザグループ名を指定します。TACACS+でこの属性に指定したグループ名は、Dominion SX 本体のグループ名と完全に(大文字と小文字は区別される)一致させる必要があります。一致しない場合は、Dominion SX での TACACS+ユーザの認証は失敗します。
- **user-dialback:** ユーザのモデムダイヤルバック番号を指定します。SX のダイヤルバックが有効になっている場合、この電話番号はユーザのコールバック用に使われます。

CiscoSecure ACS

次の手順は、CiscoSecure ACS バージョン 3.2 向けに書かれています。

注: 次の URL を参照してください。

http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007cd49.html#12231

1. Cisco ACS TACACS+のクライアントとして Dominion SX を追加します。

The screenshot shows the 'Add AAA Client' configuration page in the Cisco Secure ACS web interface. The left sidebar contains navigation options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: DominionSX
- AAA Client IP Address: 192.168.56.20
- Key: raritan
- Authenticate Using: TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client

At the bottom of the form, there are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'.

図 100 TACACS+の Cisco ACS AAA クライアント

2. [Interface Configuration(インタフェース設定)]を選択します。

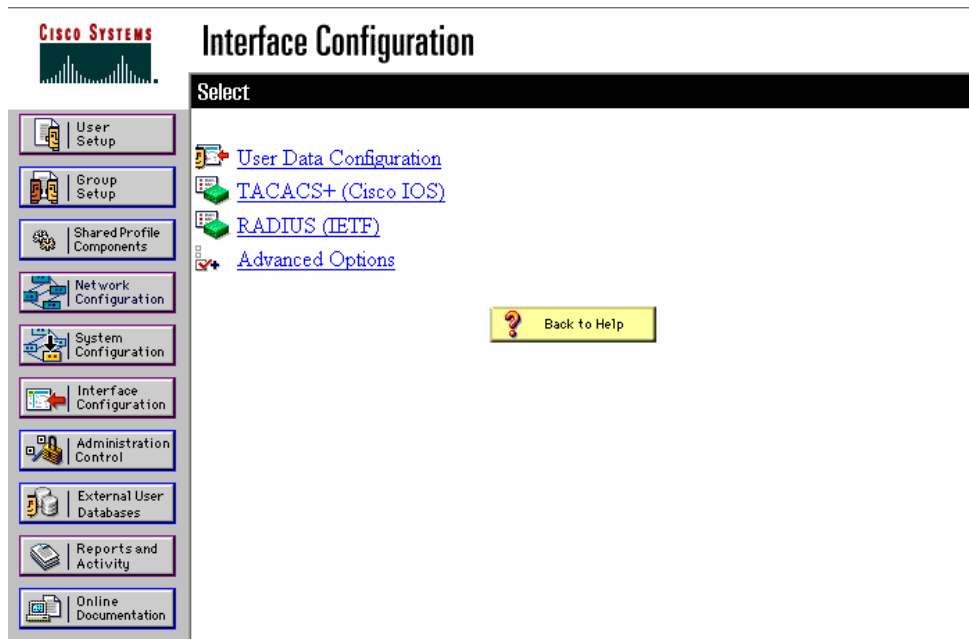


図 101 Cisco ACS インタフェース設定

3. [TACACS+(Cisco IOS)]を選択します。
 4. dominionsx サービスを[New Services(新規サービス)]に追加します。

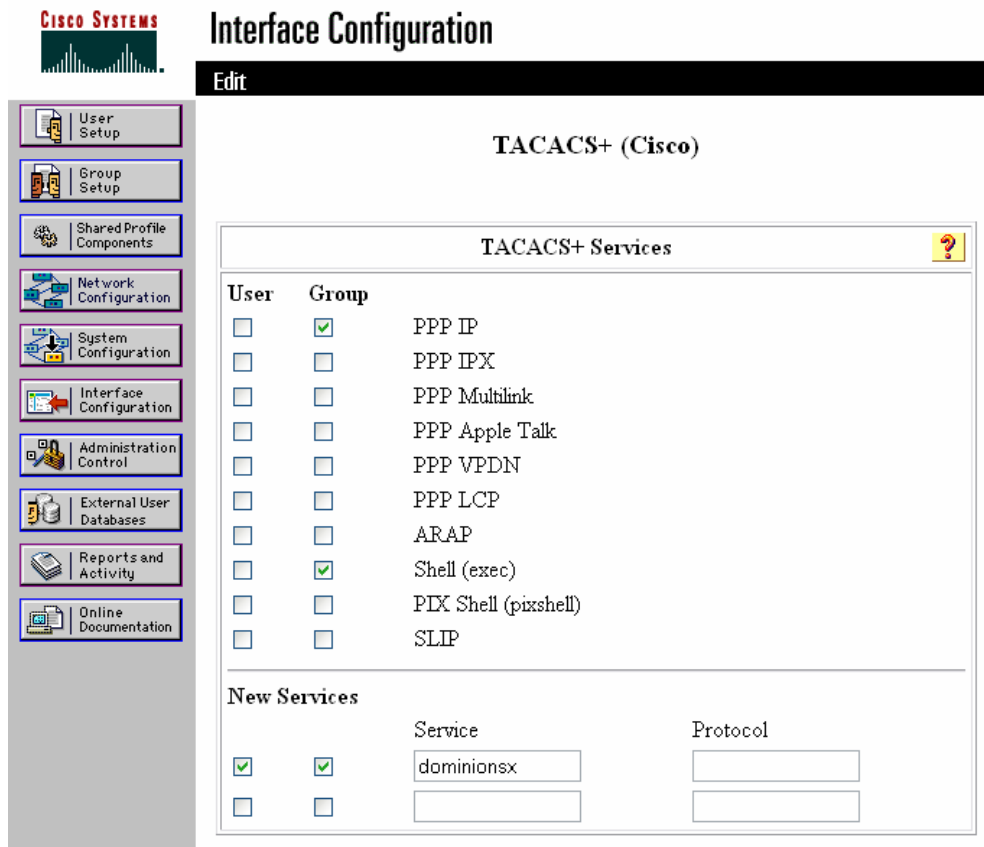


図 102 TACACS+のプロパティ

5. ユーザやグループを追加または編集すると、**dominionsx** サービスが[TACACS+ Settings(TACACS+設定)]に表示されます。このサービスをユーザごと、またはグループごとに有効にするには、[**dominionsx**]と[**Custom Attributes(カスタム属性)**]のチェック ボックスをオンにします。属性(**user-type**)と適切な値をテキスト ボックスに追加します。

注: *user-group* 属性の値は、大文字と小文字が区別されるので、*Dominion SX* 本体のローカル グループ名と完全に一致していることを確認してください。

The screenshot shows the Cisco Systems User Setup web interface. On the left is a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "User Setup" and contains several configuration sections:

- Failed attempts exceed:** A checkbox is unchecked. Below it is a text input field containing the number "5". Underneath, it says "Failed attempts since last successful login: 0". A second checkbox, "Reset current failed attempts count on submit", is also unchecked.
- TACACS+ Settings:** A section with a question mark icon. It contains a checked checkbox for "dominionsx". Below that is another checked checkbox for "Custom attributes". Underneath is a text input field containing "user-group=admin".
- IETF RADIUS Attributes:** A section with a question mark icon. It contains an unchecked checkbox for "[011] Filter-Id" followed by an empty text input field.

図 103 TACACS+設定

Active Directory

Active Directory については、次の Microsoft の URL を参照してください。

<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>

空白ページ

付録 E: モデム設定

クライアント ダイアルアップ ネットワークの設定

Dominion SX と併用するように Microsoft Windows ダイアルアップ ネットワークを設定すると、Dominion SX と同じ PPP ネットワーク上の PC を設定できるようになります。ダイアルアップ接続が確立すると、Web ブラウザを PPP サーバの IP にアクセスさせることで Dominion SX への接続が行われます。モデムのインストール ガイドラインは、次のクライアント ベース システムを対象としています。

- Windows NT
- Windows 2000
- Windows XP

Windows NT のダイアルアップ ネットワーク設定

1. [スタート]、[プログラム]、[アクセサリ]、[ダイアルアップ ネットワーク]の順に選択します。
2. [新規]をクリックします。

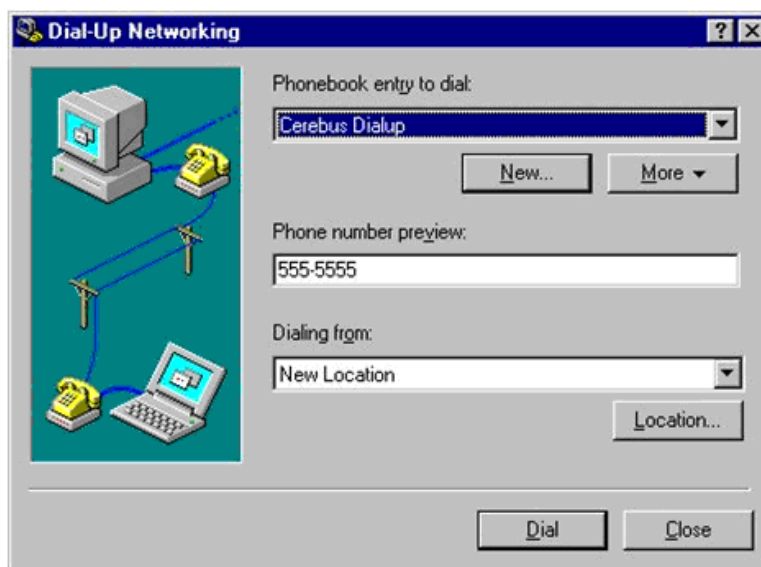


図 104 ダイアルアップ ネットワーク画面

新しい電話帳のエントリ ウィンドウでこの接続の詳細を設定できます。

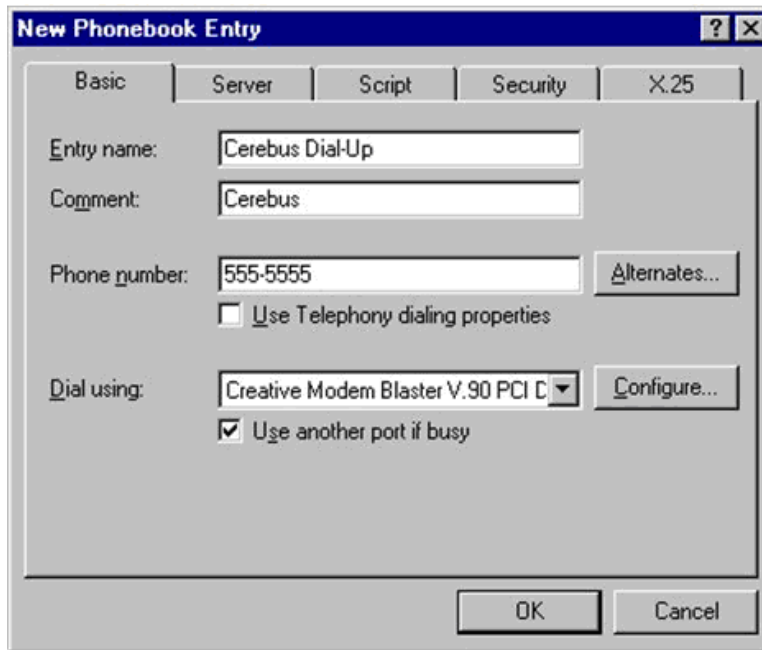


図 105 新しい電話帳のエントリ画面

3. [基本]タブをクリックし、次のフィールドに入力します。
 - **エントリ名**: Dominion SX 接続の名称
 - **電話番号**: Dominion SX に接続している回線の電話番号
 - **ダイヤル方法**: Dominion SX への接続に使用するモデム。選択肢がない場合は、そのワークステーションにモデムがインストールされていないことを示します。
4. [セキュリティ]タブをクリックします。

[セキュリティ]セクションではモデム接続時のセキュリティ レベルを指定します。Dominion SX 本体に接続すると SSL/RC4 で安全が保証されるので、ダイヤルアップ セキュリティは必要ありません。
5. [クリア テキストを含む任意の認証を受け付ける]ラジオ ボタンをクリックします。

6. [OK]をクリックしてダイヤルアップ ネットワークのメイン画面に戻ります。

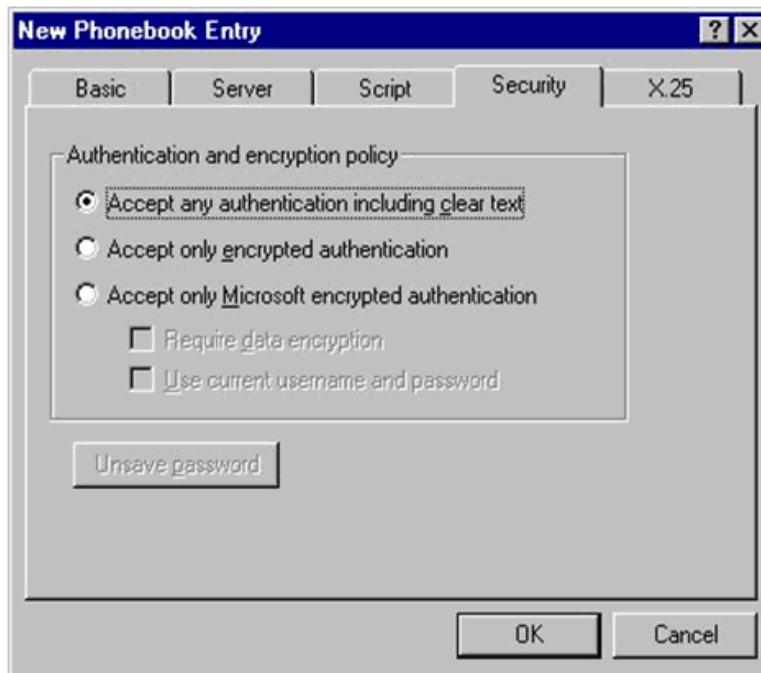


図 106 ダイヤルアップのセキュリティ表示

7. [ダイヤル]をクリックします。エラー メッセージが表示される場合は、Windows NT のユーザ ガイドを参照してください。

Windows 2000 のダイヤルアップ ネットワーク設定

1. [スタート]、[プログラム]、[アクセサリ]、[通信]、[ネットワークとダイヤルアップ接続]の順に選択します。
2. ネットワークとダイヤルアップ接続ウィンドウが表示されたら、[新しい接続の作成]アイコンをダブルクリックします。

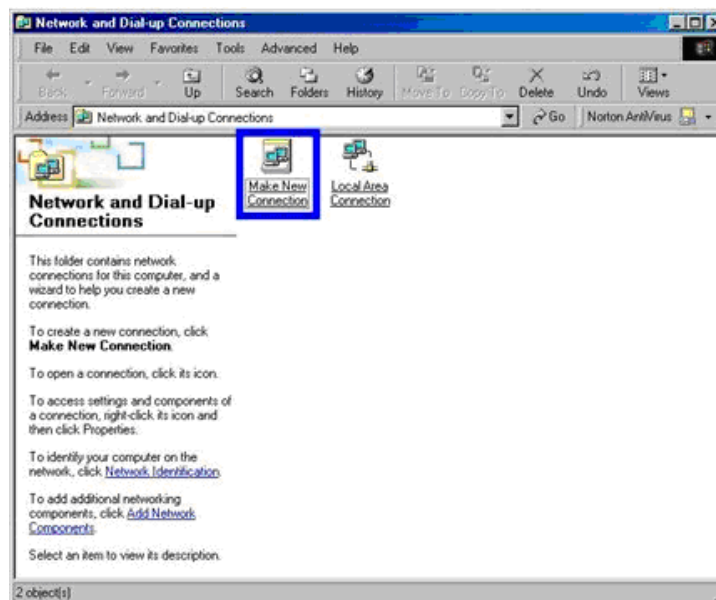


図 107 Windows 2000 ネットワークとダイヤルアップ接続

- [次へ]をクリックし、ネットワークの接続ウィザード ウィンドウの手順に従って、独自のダイヤルアップ ネットワーク プロファイルを作成します。
- [プライベート ネットワークにダイヤルアップ接続する]ラジオ ボタンをクリックし、[次へ]をクリックします。

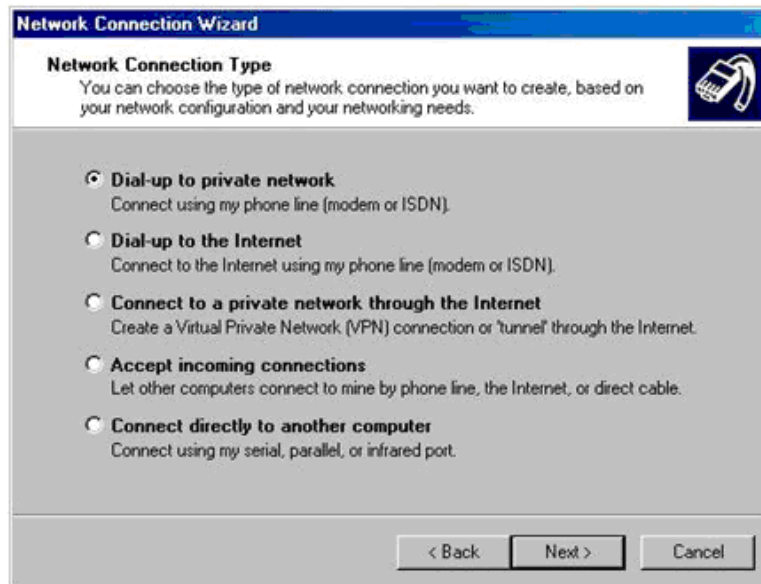


図 108 ネットワーク接続の種類

- Dominion SX との接続に使用するモデムのチェック ボックスをオンにして、[次へ]をクリックします。

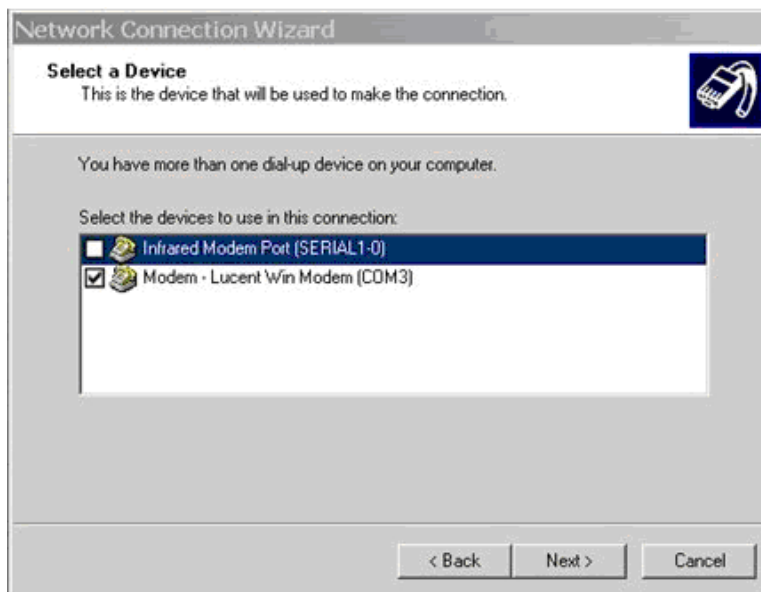


図 109 デバイスの選択

- ダイヤルする市外局番と電話番号を該当するフィールドに入力します。
- [国/地域名と国番号]ドロップダウン メニューの一覧から国または地域を選択します。

8. [次へ]をクリックします。

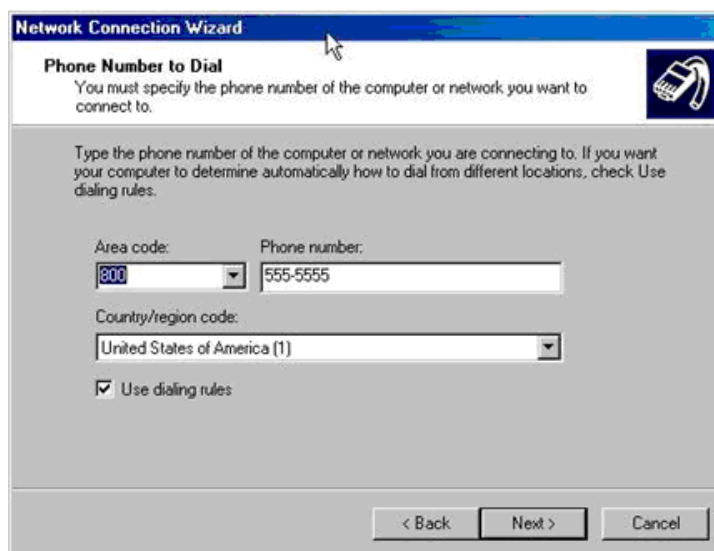


図 110 ダイヤルする電話番号

[接続の利用範囲]画面が表示されます。

1. [接続の利用範囲]画面で、[自分のみ]ラジオ ボタンをクリックします。
2. [次へ]をクリックします。



図 111 接続の利用範囲

これでネットワーク接続が作成されました。

3. ダイヤルアップ接続の名前を入力します。
4. [完了]をクリックします。
5. ダイヤル ウィンドウが表示されたら、[ダイヤル]をクリックしてリモート マシンに接続します。

接続の確立に成功したことを示すウィンドウが表示されます。

エラー メッセージが表示される場合は、Windows 2000 のダイヤルアップ ネットワークのヘルプを参照してください。

Windows XP のダイヤルアップ ネットワーク設定

1. [スタート]、[すべてのプログラム]、[アクセサリ]、[通信]、[新しい接続ウィザード]の順に選択します。
2. [次へ]をクリックし、**新しい接続ウィザードの手順**に従って、独自のダイヤルアップ ネットワーク プロファイルを作成します。
3. [インターネットに接続する]ラジオ ボタンをクリックし、[次へ]をクリックします。

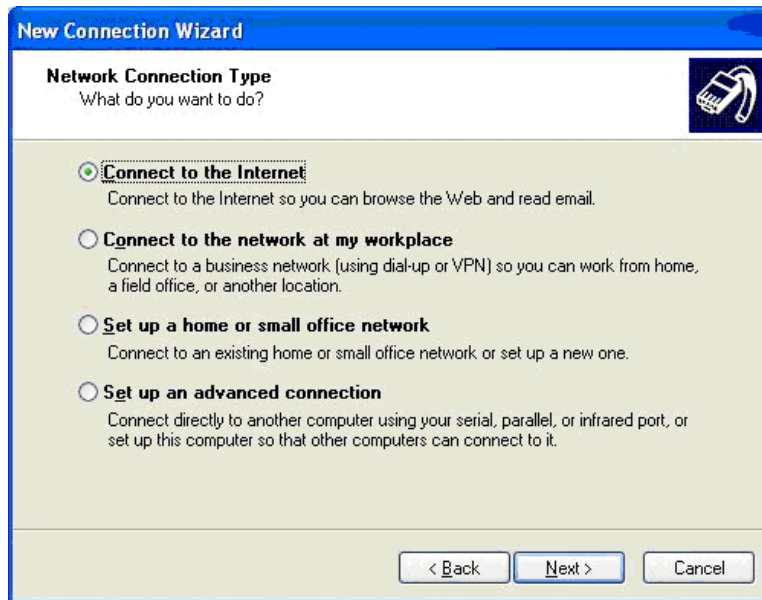


図 112 ネットワーク接続の種類

4. [接続を手動でセットアップする]ラジオ ボタンをクリックし、[次へ]をクリックします。



図 113 デバイスの選択

5. [ダイヤルアップ モデムを使用して接続する]ラジオ ボタンをクリックし、[次へ]をクリックします。

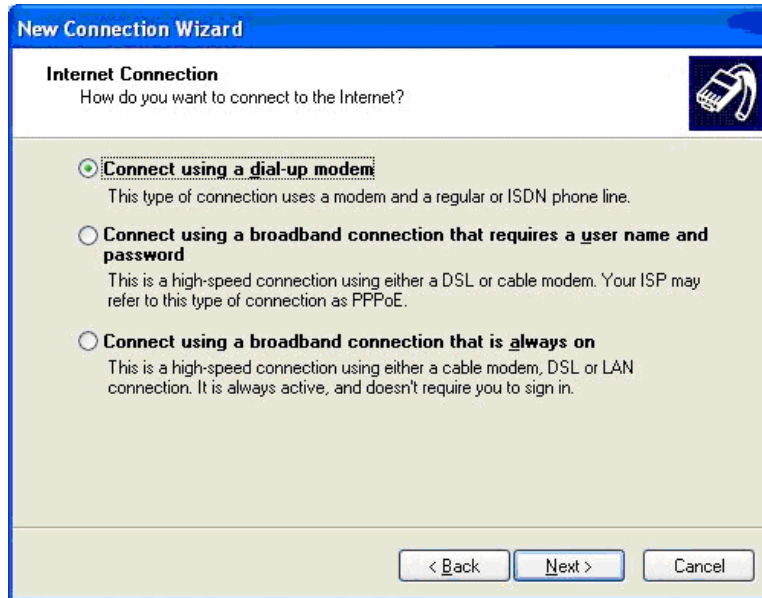


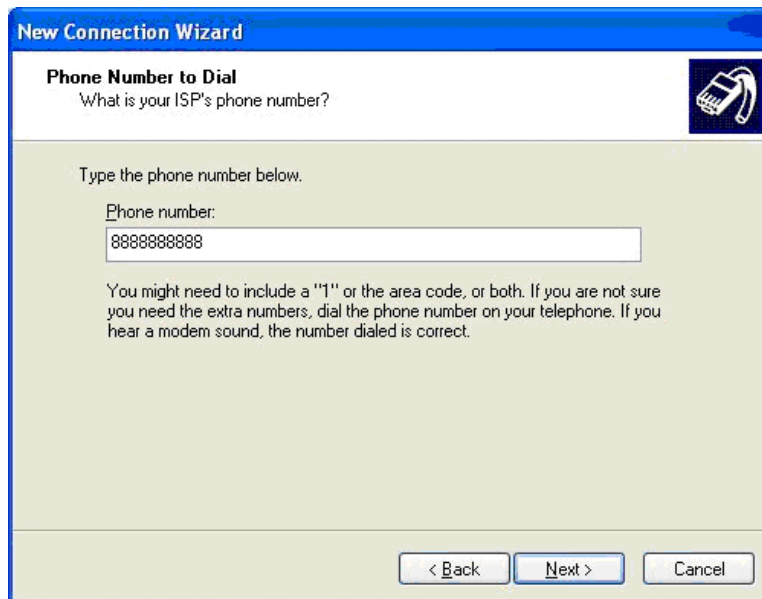
図 114 インターネット接続

6. この特定の接続を識別するための名前を ISP 名フィールドに入力し、[次へ]をクリックします。



図 115 接続名

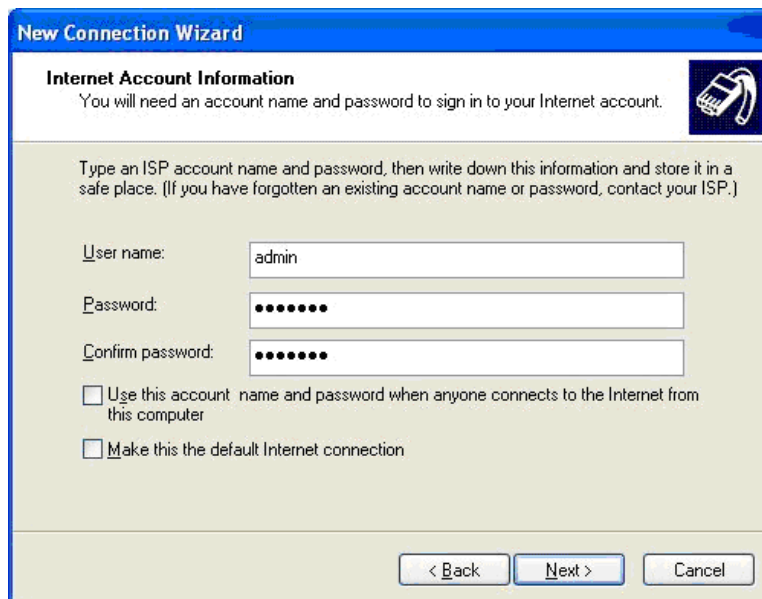
- この接続用の電話番号を電話番号フィールドに入力し、[次へ]をクリックします。



The screenshot shows the 'New Connection Wizard' dialog box with the title 'Phone Number to Dial'. The subtitle asks 'What is your ISP's phone number?'. Below this, it says 'Type the phone number below.' and 'Phone number:' followed by a text input field containing '8888888888'. A note below the field states: 'You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

図 116 ダイヤルする電話番号

- ISP 情報を入力します。ユーザ名とパスワードを該当するフィールドに入力し、確認用にパスワードを再入力します。
- フィールドの下にある該当するオプションのチェック ボックスをオンにして、[次へ]をクリックします。



The screenshot shows the 'New Connection Wizard' dialog box with the title 'Internet Account Information'. The subtitle says 'You will need an account name and password to sign in to your Internet account.' Below this, it says 'Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)' There are three text input fields: 'User name:' with 'admin', 'Password:' with '.....', and 'Confirm password:' with '.....'. Below these are two checkboxes: 'Use this account name and password when anyone connects to the Internet from this computer' (unchecked) and 'Make this the default Internet connection' (unchecked). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

図 117 インターネット アカウント情報

- [完了]をクリックします。
- ダイヤル ウィンドウが表示されたら、[ダイヤル]をクリックしてリモート マシンに接続します。正常に接続されたことを示すウィンドウが表示されます。エラーが発生した場合は、Windows XP のダイヤルアップ ネットワークのヘルプを参照してください。

付録 F: トラブルシューティング

次の表に、問題の説明と推奨される解決方法について記載しています。

ページへのアクセス

表 86 ページへのアクセスに関するトラブルシューティング

問題	解決方法
<p>ログインできない。工場出荷時のデフォルト設定は?(ファームウェア バージョン 2.5 以上を実行している Dominion SX 本体のみ)</p> <p>ログインできない(デフォルト以外)</p>	<p>ユーザ名: admin(すべて小文字) パスワード: raritan(すべて小文字)</p> <ol style="list-style-type: none"> ユーザごとの複数ログインの設定状態を確認します。この設定が無効になっていて、既にセッションが確立されている場合は、新たなセッションを開くと失敗します。 ローカル認証のステータスを確認します。この設定が有効になっていない場合は、リモート ユーザのみがログインできます。
<p>Dominion SX へアクセスしても応答がない</p>	<p>任意のブラウザで本体に到達できない場合は、次のトラブルシューティング リストに従って操作を行ないます。</p> <ol style="list-style-type: none"> 本体に電源が入っていることを確認します。 本体がネットワークに正しく接続されていることを確認します。 その本体とのネットワーク通信を確認するために、同じネットワーク上のコンピュータから本体への ping を実行します。 <ul style="list-style-type: none"> ping が機能しない場合は、ネットワーク管理者にお問い合わせください。ネットワーク設定に本体との通信を妨げる問題があるかもしれません。 ping に成功した場合は、以下のトピックを参考にしてください。
<p>DNS エラーやアクセス エラー</p>	<p>Internet Explorer を使用して Dominion SX URL に接続すると、Web ページで DNS エラーやアクセス エラーが表示されます。</p> <p>インストールされた Dominion SX 証明書を削除して、ブラウザを再起動してください。</p>
<p>サポートされていない暗号化</p>	<p>この本体では 128 ビット SSL 暗号化のみをサポートします。</p> <ul style="list-style-type: none"> Internet Explorer の場合は、[ヘルプ]の[バージョン情報]を表示して、ブラウザの SSL の最大ビット強度を確認します。強度が不足している場合は、ブラウザのアップグレードをお勧めします。 Netscape の場合は、[Communicator]、[Tools(ツール)]、[Security Info(セキュリティ情報)]、[SSL v3.0 Configuration(SSL v3.0 の設定)]の順に選択して表示し、128 ビット SSL がサポートされていることを確認してください。

問題	解決方法
超過したユーザの数	<p>この本体には、いつでも指定された数のログイン ページだけが認証されるようにするセキュリティ対策が施されています。本体にログインする際、この数に達すると、ポップアップ ウィンドウで、最大ユーザ数を超過したことが示されます。これは本体の正常な動作です。</p> <p>数分待つてから、ログインし直してください。ブラウザのログオンを成功させるには、再読み込み、または<SHIFT キーを押しながら[更新]をクリック>の操作が必要になることもあります。</p>

ファイアウォール

表 87 ファイアウォールに関するトラブルシューティング

問題	解決方法
Web ページにアクセスできない	<p>本体をファイアウォール経由で動作させるためには、ポート 80(http 用)と 443(https 用)のアクセスを許可する必要があります。</p> <p>システム管理者に問い合わせ、ポート 80 および 443、または独自に設定されたポートへのアクセス権をリクエストしてください。</p>
ログイン失敗	<p>Dominion SX の設定可能なポート ネットワーク パラメータ(デフォルト値 51000)を使用して接続できるようにするには、ファイアウォールを設定する必要があります。ファイアウォールがこれらの接続を許可しない場合は、ログインが失敗したことをアプレットが示します。</p> <p>システム管理者に問い合わせ、設定可能なポートでの接続許可をリクエストしてください。</p>
SSL セキュリティ警告	<p>SSL 証明書には、インターネット アドレス(IP)が組み込まれています。ファイアウォールで Network Address Translation(NAT)を実行する場合、SSL 証明書の IP アドレスが、セキュリティ警告を生成するブラウザで認識される IP アドレスと一致しません。</p> <p>これは通常の動作です。</p> <p>この警告メッセージは、本体の動作には影響しません。</p>

ログイン

表 88 ログインに関するトラブルシューティング

問題	解決方法
ログイン失敗	<p>セキュリティを高めるために、本体のログイン画面は 3 分後に期限切れになります。したがって、この期間以降のログインはすべて失敗します。このタイマーをリセットするには、ブラウザの再読み込みを行います。</p> <p>SHIFT キーを押しながら、ブラウザの[Reload(再読み込み)]をクリックします。これで本体自体から(ローカル キャッシュからではなく)ログイン画面が更新され、本体にログインできます。</p>
RADIUS ユーザ	<p>RADIUS 認証をサポートするように設定できます。ローカル ユーザとして定義されていないユーザは、RADIUS が有効なときには RADIUS ユーザとみなされます。</p> <p>なんらかの理由で、RADIUS サーバでユーザ認証ができない場合、本体は RADIUS サーバからの認証リクエストの結果を受け取るまで、ユーザのログインを許可しません。</p> <p>認証は最大で 20 秒ほどかかります。ユーザがログインに成功するまで、または認証拒否のメッセージが表示されるまでお待ちください。</p>

ポート アクセス

表 89 ポート アクセスに関するトラブルシューティング

問題	解決方法
ポート アクセス更新	<p>ポート アクセス リストの更新は自動的にには行われません。ポート アクセス リストは、ユーザが[Port Access(ポート アクセス)]をクリックしたときにのみ更新されます。したがって、ユーザが許可を取り消されても、[Port Access(ポートアクセス)]ボタンをクリックするまではポート アクセス画面にこうした変更が表示されない可能性があります。</p> <ul style="list-style-type: none"> 新しい制限を適用するには、ログアウトしてからもう一度ログインする必要があります。これにより、制限したポートが表示されなくなります。 できる限り、管理者が既に本体にログインしているユーザのポート アクセス権を変更しないようにすることをお勧めします。

アップグレード

表 90 アップグレードに関するトラブルシューティング

問題	解決方法
FTP – サーバにアクセスできない	<p>アップグレード パネルで指定した FTP サーバにアクセスできないか、設定が間違っている場合は、FTP サーバからの応答を受信するか、タイムアウトが発生するまでアップグレード処理は中断されます。</p> <p>FTP サーバのアクセス不能メッセージが表示されるまでお待ちください。</p>
FTP – ファイルが見つからない	<p>アップグレード パスで指定されたディレクトリにアップグレード ファイルのパッケージが必要です。このパッケージには、追加されるすべてのファイルと「upgrade.cnf」ファイルが必要です。このファイルが存在しない場合、あるいは指示された場所にそのファイルのコンテンツがない場合は、「ファイルが見つからない」というメッセージが表示されます。</p> <p>アップグレード パッケージが正しいディレクトリにあることを確認し、アップグレード パスと FTP サーバの IP アドレスを確認してください。</p> <p>それでもアップグレードが機能しない場合は、アップグレード パッケージを再度インストールし、再試行してください。</p>

モデム

表 91 モデムに関するトラブルシューティング

問題	解決方法
ログイン失敗	<p>この本体では、接続スピードが 28.8 Kbps 以上のモデムを介した Web ブラウザアクセスをサポートしています。ボーレートが不十分な場合、ユーザはモデムを介して本体にログオンすることができません。</p> <p>ブラウザ ベースのモデム認証(ログイン)には、最低でも 28.8 Kbps の接続スピードが推奨されています。SSH または Telnet を使用した CLI ベースでのアクセスについては、9600 bps 程度の速度でも十分です。</p>

255-60-2000-00

本社

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel.(732)764-8886
Fax.(732)764-8887
Email: sales@raritan.com
Web: raritan.com

Raritan America

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel.(732)764-8886
Fax.(732)764-8887
Email: sales@raritan.com
Web: raritan.com

アジア太平洋

Raritan Asia Pacific, Inc.
5F, 121, Lane 235, Pao-Chiao Road, Hsin
Tien 231,
Taipei, Taiwan, ROC
Tel.(886)28919-1333
Fax.(886)28919-1338
Email: sales.asia@raritan.com
Web: raritan-ap.com

Raritan 中国事業所

Raritan Beijing
No. 35 Financial St, Xicheng District
Room 1035, Block C,
Corporate Square
Beijing 100032, China
Tel.(86)10-8809-1890
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Shanghai

Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai, China(200030)
Tel.(86)21 5425-2499
Fax.(86)21 5425-3992
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan Guangzhou

1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou(510075), China Raritan
Tel.(86)20 8755-5581
Fax.(86)20 8755-5571
Email: sales.china@raritan.com
Web: raritan.com.cn

Raritan 韓国

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel.(82)2 557-8730
Fax.(82)2 557-8733
Email: sales.korea@raritan.com
Web: raritan.co.kr

日本ラリタン東京本社

〒104-0033
東京都中央区新川 1-26-2
新川 NS ビルディング 4F
Tel. 03-3523-5991
Fax. 03-3523-5992
Email: sales@raritan.co.jp
Web: raritan.co.jp

西日本営業所

〒541-0048
大阪市中央区瓦町 4-6-8
大阪化学繊維会館 3F
Tel. 03-3523-5993
Fax. 03-3523-5992
Email: raritan.co.jp

Raritan オーストラリア事業所

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australia
Tel.(61)3 9866-6887
Fax.(61)3 9866-7706
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan Sydney

Suite 1, Level 9,
75 Miller Street North Sydney
PO Box 591,
North Sydney, NSW 2059,
Australia
Tel:(61)2-9029-2558
Email:(61)2-8012-1103
Email: sales.au@raritan.com
Web: raritan.com.au

Raritan インド

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli Gurgaon
Rd, Gurgaon 122 002
Haryana, India
Tel.(91)124 410-7881
Fax.(91)124 410-7880
Email: enquiry.india@raritan.com
Web: raritan.co.in

Raritan 台湾

5F, 121, Lane 235, Pao-Chiao Road
Hsin-Tien City
Taipei Hsien, Taiwan, ROC
Tel.(886)28919-1333
Fax.(886)2 8919-1338
Email: sales.taiwan@raritan.com
Web: raritan.com.tw

Raritan シンガポール

350 Orchard Road
#11-08, Suite 21, Shaw House
Singapore 238868
Tel:(65)6725 9871
Fax:(65)6725 9872
Email: sales.ap@raritan.com
Web: raritan-ap.com

ヨーロッパ

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel.(31)10-284-4040
Fax.(31)10-284-4049
Email: sales.europe@raritan.com
Web: www.raritan.fr
www.raritan.de

Raritan フランス

120 Rue Jean Jaures
92300 Levallois-Perret, France
Tel.(33)14-756-2039
Fax.(33)14-756-2061
Email: sales.france@raritan.com
Web: www.raritan.fr

Raritan Deutschland GmbH

LichtstraBe 2
D-45127 Essen, Germany
Tel.(49)201-747-98-0
Fax.(49)201-747-98-50
Email: sales.germany@raritan.com
Web: www.raritan.de

Raritan イタリア

Via dei Piatti 4
20123 Milan
Italy
Tel.(39)02-454-76813
Fax.(39)02-861-749
Email: sales.italy@raritan.com
Web: raritan.it
www.raritan.info

Raritan カナダ

Raritan Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Canada
Tel. 1-905-949-3650
Email: sales.canada@raritan.com
Web: raritan.ca

Raritan U.K.

9th Floor, 12-20 Camomile St
London EC3A 7EX, United Kingdom
Tel.(44)(0)20-7614-7700
Email: sales.uk@raritan.com
Web: raritan.co