

# Seqrite TERMINATOR v1.8

管理者ガイド

2016年4月14日 http://www.seqrite.com

### 著作権情報

Copyright © 2016 Quick Heal Technologies Ltd. All Rights Reserved.

本書のいかなる部分も、事前に Quick Heal Technologies Ltd. (7010 C & D, 7th Floor, Marvel Edge, Viman Nagar, Pune 411014, India)の許可を得ることなく、形態を問わず模造、複製、または変更してはならず、電子的または他のいかなる情報検索システムにも組み込んではならず、いかなる形態であっても伝送してはなりません。

Quick Heal Technologies Ltd. の許可を得ないマーケティング、配布または使用は法 的責任を問われます。

この文書は公開日時点のものであり、Quick Heal によって随時変更される可能性があります。

#### 商標

Seqrite は、Quick Heal Technologies Ltd. の登録商標です。その他のブランドおよ び製品の名称は各所有者の商標です。

### エンドユーザー使用許諾契約書 (EULA)

#### Seqrite Terminator (統合脅威管理/UTM) エンドユーザー使用許諾契約書

重要

Seqrite Terminator (以下「Terminator」とする)をご使用になる前、またはご使用を 試みる前に、本 Seqrite Terminator (統合脅威管理/UTM) エンドユーザー使用許諾契 約書(以下「契約書」とする)を注意深くお読みください。エンドユーザー使用許諾契 約書は製品の有効化時に、または www.seqrite.com/eula からお読みいただけます。

Terminator の使用、または [同意する] オプションの選択、またはいかなる方法であ れ Terminator をインストールしようとする試み/同意 (そうした行為はお客様の同意 および署名行為の一部とみなされます) により、お客様は本契約書に記載されたすべて の契約条件を読み、理解し、同意したことを確認および承認したものとみなされます。 本契約書は、ひとたび「お客様」 [Terminator を使用する予定の (19 歳以上であるか または契約を結ぶ法的能力がある) 個人、または企業もしくは法人 (以下「お客様」と する)] によって承認されると、お客様と QUICK HEAL TECHNOLOGIES PRIVATE LIMITED、 本社インド、プネ、(以下「Quick Heal」とする) との間における法的強制力を持つ契 約書となり、お客様は本契約書に記載され Quick Heal によって不定期に修正される契 約条件に従って Terminator を使用する権利を有するものとします。以下に記載された 契約条件に同意できない部分がある場合は、Terminator をいかなる方法によっても使 用せず、お客様が所有している同一物を使用することなく) 速やかに返却し てください。

Seqrite Terminator は、Quick Heal により開発されたソフトウェア製品です。Quick Heal は、領収書によって確認されるライセンス料金の支払いを約因として、本契約書の契約条件に従い、請求書に記載されているライセンス期間中に Terminator (統合脅 威管理ソリューション)を使用する非独占的かつ譲渡不能の権利をお客様に付与します。 この付与はユーザーマニュアルに記載された技術要件に準じて、本契約の諸条件に従い ます。

#### 1. 期間

お客様は、Terminator の有効化の日付から、請求書詳細に記載された期日までのライ センス期間のみ、Terminator を使用する権利を有します。試用/ベータまたはその他の 契約によってライセンス期間が限定される、試用およびベータライセンスまたはその他 のライセンスを除き、ライセンスの期間は請求書に記載された期間です。

#### 2. 評価および登録

本契約によりお客様は、譲渡不能、非独占的、サブライセンス不能な本ソフトウェア /Terminatorの使用を許諾されます。当該期間を超えて本ソフトウェア/Terminatorを 使用することは、インド国著作権法および国際著作権法の違反に当たります。

#### エンドユーザー使用許諾契約書 (EULA)

Quick Heal は、明示的に付与されていないすべての権利を留保し、すべての知的財産 権および所有権、媒体を問わずすべての複製物を含む本ソフトウェア/Terminator の権 原と所有権を保持します。本ソフトウェア/Terminator と付属資料は Quick Heal の所 有物であり、著作権により保護されています。本ソフトウェアまたは付属資料をコピー することは、明示的に禁止されています。

#### 3. 制限

お客様は、Terminator を保有または管理している間、紛失あるいは損傷の危険につい ての責任を負います。お客様(Seqrite によって承認されていないお客様の被雇用者、 代理人、委託先を含みます)は、次の行為を行わないことに同意します。

- a. Terminator/ソフトウェアの一部または全部をエミュレートしたり、改作したり すること。
- b. Terminator/ソフトウェアをデバッグ、逆コンパイル、改変、翻訳、リバースエ ンジニアリングすること。
- c. 本ソフトウェアのソースコードを明らかにしようとしたり、探り出そうとしたり すること。
- d. 適用可能な法律によって放棄不可能な権利がお客様に付与されている場合を唯一 の例外として、Terminator/ソフトウェアまたはその任意の箇所に基づく派生著 作物を作成すること。
- e. Terminator、ソフトウェアのラベルやマークに付された著作権情報または所有権 情報を、削除したり修正したりすること。
- f. 本ソフトウェアの任意の箇所を人間が解読可能な形式に変換すること。
- g. 第三者に Terminator/ソフトウェアを実演、コピー、販売すること。
- h. Terminator/ソフトウェアの性能や品質に関する情報を第三者に発表したり公開 したりすること。
- i. Terminator/ソフトウェアの一部/全部をサブライセンス、賃借、賃貸すること。
- j. 許諾されていない目的や違法な目的で使用すること。
- k. 本契約におけるお客様の権利または義務を譲渡または移譲すること。
- 4. 有効化/インストール
  - a. Seqrite は Terminator をオンサイトまたはリモートサポートでインストールし ます。Terminator のクイックスタートガイドに記載された手順に従ってくださ い。Seqrite は、本ソフトウェアのインストール中に発生したあらゆるデータの 損失や利益の逸失について責任を明示的に否認します。お客様のデバイスを改造 するか、またはそのデバイスにインストールされている他社のソフトウェアを改 変/改造すると、ソフトウェアの有効化またはライセンスキーファイルのインス トールが再度必要となる場合があります。また場合によっては Seqrite サポー

トヘご連絡いただく必要があります。Seqrite はライセンスとソフトウェアの妥当性/合法性を確認する権利を留保します。

- b. Seqrite は、登録時にユーザーにより送信されたデバイスを確認します。確認に 関して問題があった場合、製品の有効化/インストールは行われません。この確 認プロセスは製品の有効化に必須です。
- 5. 第三者のウェブサイトへのリンク/アプリケーション

ソフトウェア/Terminator 製品には、第三者のウェブサイトへのリンクおよびオープン ソースのフリーアプリケーションが含まれている場合があり、本ソフトウェア /Terminator の使用者であるお客様は、こうした第三者ウェブサイト/オープンソース アプリケーションにリダイレクトされる可能性があります。第三者のウェブサイト/ア プリケーションは Seqrite の管理下にあるものではなく、Seqrite は第三者のいかな るウェブサイトに含まれる内容/いかなるリンク、およびアプリケーションの使用につ いて責任を負いません。Seqrite は、お客様の利便性のためにのみ第三者のウェブサイ トへのリンク/アプリケーションの使用を提供しているにすぎず、これが原因で発生す る損失・損害の責任は負わないものとします。

#### 6. オープンソースソフトウェアライセンス

本ソフトウェア/Terminator には、GNU General Public License Version 2 (GPL v2)、 Apache license V2, OpenVPN License, BSD 2.0, IBM Public License 1.0, ISC, GNU Lesser General Public License 2.1 (LGPL 2.1), MIT, The OpenLDAP Public License, OpenSSL Combined License, The PHP License, version 3.01, ZLIB/LIBPNG LICENSE 🗞 その他同様のフリーソフトウェアライセンスによってユーザーにライセンス(またはサ ブライセンス)されるソフトウェアプログラム(以下「オープンソースソフトウェア」 とする)が含まれている可能性があります。これらのライセンスは特にユーザーに特定 プログラムあるいはその一部のコピー、改変、再配布、およびソースコードへのアクセ スを許可します。Segrite は、アップデートを提供する目的かどうかにかかわらず、あ らゆるバージョンのあらゆるオープンソースソフトウェアを使用または選択する権利を 有します。いずれかのソフトウェアを実行可能なバイナリ形式で配布する際に、そうし たライセンスにより、そのユーザーにソースコードも提供することが求められている場 合、ソースコードは tpsrc@quickheal.com に要求を送信することで入手できるか、ま たは本ソフトウェアとともに提供されます。オープンソースソフトウェアの情報および ライセンスは、www.seqrite.com/eula で確認できます。オープンソースソフトウェア のライセンスにより、オープンソースソフトウェアを使用、コピー、または改変する権 利を権利者が提供するように求められ、その権利が、本契約によって付与されている権 利よりも広範囲におよぶ場合、こうした権利は本契約の権利および制限に優先して適用 されます。

提供される各ライセンスとともに本ソフトウェアで使用されるオープンソースアプリケーションのリストを本契約書の最後に示します。このリストは、Seqrite によって随時 更新される場合があります。

V

7. サポート

Seqrite は本ソフトウェア/Terminator の使用時にサポート機能を提供します(たとえ ば、技術サポートチームとのライブチャット、お客様の判断により技術サポートチーム が行うデバイスへのリモートアクセスなど)。本サポートのご利用はお客様の単独の判 断によるものであり、お客様はリモートサポートを利用する前にお客様のデバイスに存 在する既存のデータ/ソフトウェア/プログラムのバックアップを取ることに単独で責任 を負います。Seqrite は、このサポートのプロセス全体を通して発生したデータの損失 とデータ/所有物に対する直接/間接的/派生的損失または損害に対し、一切の責任を負 わないものとします。Seqrite はサポートの提供に関していかなる保証もするものでは なく、技術サポートチームがある時点において問題が対象範囲外であると判断した場合、 Seqrite は単独の裁量においてこのようなサポートを保留、停止、終了または拒否しま す。

8. 電子メール/電子通信

お客様がソフトウェア/Terminator の有効化/インストールを通してソフトウェア /Terminator を登録した後、Seqrite は電子メールその他任意の電子通信機器を介して 登録プロセス時にご提供いただいた連絡先に基づいてお客様に連絡させていただく場合 があります。この連絡は、お客様の利便性向上のために行われる製品の検証を目的とす るものです。

9. SEQUITE のステータスアップデート

正規ライセンス版コピーのアップデートのたびに、Seqrite アップデートモジュールが 現在の製品ステータス情報を Seqrite インターネットセンターに送信します。インタ ーネットセンターに送信される情報には、監視サービスが想定どおりに動作しているか など、Seqrite 保護の診断状況が含まれます。この情報は、正規ライセンス版をご利用 のお客様により良い技術サポートを迅速に提供するために使用されます。

登録されたお客様全員に、ライセンス有効化を行った日からライセンス期間が満了する まで無償でアップデートが提供されます。

10.情報の収集

Seqrite ソフトウェア/Terminator は、お客様からの許可の下、または許可なしに、個 人を特定できる情報を含むか否かにかかわらず、統計目的のために、または悪質な動作 パターン、本質的に不正なウェブサイト、およびその他のインターネットセキュリティ 脅威/リスクを特定および検出する Seqrite 製品の能力、効果、性能の強化と評価のた めに、以下の情報を収集する場合があります。登録中にエンドユーザーによって入力さ れたパスワードは、Seqrite サーバーには保存されません。これらの情報は、ここに記 載されている場合を除き、個人を特定できる情報と関連付けられることはありません。 情報には以下のものが含まれますが、それらに限定されません。

a. ソフトウェア/Terminator によって、マルウェアの動作パターンを持っているものと判断される可能性がある、あらゆるタイプの実行可能ファイル。

- b. ソフトウェアのインストール時にエラーが発生したか、またはインストールが正 常に完了したかなど、ソフトウェア/Terminator のステータスに関連するあらゆ るタイプの情報。
- c. エンドユーザーが閲覧したウェブサイトのうち、ソフトウェアによって本質的または潜在的に不正なものとみなされるウェブサイトの URL のタイプ。
- d. ソフトウェアによって、不正なものでありセキュリティリスク/脅威をもたらす 可能性があるとみなされる、あらゆるタイプの情報。
- e. ソフトウェア/Terminator がインストールされているデバイスのメディアアクセス制御(MAC)アドレスと、全地球測位システム(GPS)を特定するための、あらゆるタイプの情報。
- f. インターネットプロトコル (IP) アドレスを特定するためのあらゆるタイプの情報と、効果的なライセンス管理、および製品の機能と使い勝手の向上に必要な情報。
- g. お客様は、上記のように収集された情報/データが、潜在的なインターネットの セキュリティリスクを解析、防止、検出するために使用されること、収集された 傾向についてあらゆるタイプのデータ/レポート/プレゼンテーションを公表する こと、および意識を向上させるために他の組織やベンダーとデータを共有するこ とを承認するものとします。

#### 11.限定保証および免責事項

本ソフトウェア/Terminator パッケージは、パッケージの商品性および適合性の黙示的 保証を含むがこれに限定されない、一切の明示的または黙示的な保証を行うことなく提 供されます。Seqrite またはそのサプライヤは、本ソフトウェアパッケージを使用した こと、または使用できなかったことに起因するデータの損失、利益逸失、またはその他 のデータ/所有物の損害を含む、直接的、間接的、または結果的な損害について、お客 様またはその他の者に対して一切の責任を負いません。Seqrite はどのような法的手続 きにも協力する権利を有し、お客様による本ソフトウェアの使用に関連する文書や情報 を提供することがあります。上記の免責事項および制限事項は、お客様が本ソフトウェ アを受け入れるか否かにかかわらず適用されます。

本書は Seqrite Terminator エンドユーザー使用許諾契約書の簡略版/抜粋です。実際 にソフトウェアを使用する前に、当社のソフトウェア使用許諾契約書の詳細な諸条件を お読みになることをお勧めします。Seqrite Terminator エンドユーザー使用許諾契約 書の詳細版については、<u>www.seqrite.com/eula</u>を参照してください。

概要	1
統合脅威管理 (UTM) について	1
Terminator の機能	1
登録ウィザード	4
使用許諾契約書	5
インターフェース	5
DNS	7
パスワード変更	7
日時	8
プロダクトキー	9
Terminator へのアクセス	13
Seqrite Terminator へのログイン	13
ウェブ経由で Terminator ヘアクセスする	13
コマンドラインインターフェース (CLI) 経由で Terminator ヘアクセスする	14
Seqrite Terminator の操作 (ウェブ)	16
ダッシュボード	19
通知、ステータス、インターネット使用量	19
統計の領域	22
ネットワーク設定	24
定義	24
定義の追加	24
定義の削除	27
IPv6	27
IPv6 の有効化	28
6 to 4 トンネルの有効化	29
インターフェース	30
インターフェースの設定	30

インターフェースの削除	34
エイリアスの追加	34
USB モデム	35
DNS	37
グローバル DNS サーバー	38
スタティック DNS	40
ダイナミック DNS	41
DHCP	42
ルーティング	47
スタティックルーティング	47
ポリシーに基づいたルーティング (PBR)	48
負荷分散とフェールオーバー	54
ファイアウォール	55
デフォルトのファイアウォールルール	56
インターゾーン設定	57
カスタムファイアウォールルール	59
IP ポート転送	63
VPN	66
証明書	66
IPSec	69
PPTP VPN	75
SSL VPN	76
VLAN	85
ブリッジ	87
リンクアグリゲーション	90
インターネット設定と除外	93
ID 管理/ユーザーとグループ	97
ユーザー管理	98
ユーザーの追加	98
ユーザーの編集	100

ユーザーの削除	101
ユーザーの強制ログアウト	102
ユーザーのインポート	102
ゲストユーザー設定	103
グループの管理	105
グループの追加	105
グループの編集	109
グループの削除	109
グループの検索	109
時間カテゴリ	110
認証サーバー	111
新しいサーバーの追加	111
設定済みの認証サーバーからユーザーをインポートまたは削除する	113
認証サーバーの削除	114
Seqrite Terminator と認証サーバーとの同期	114
Seqrite Terminator と認証サーバーとの同期のスケジュール	115
インターネットクォータ	115
コンテンツフィルタリングと保護	119
アンチウイルス	120
メール保護	121
グローバル設定	121
アンチウイルス	123
アンチスパム	125
添付ファイル管理	127
キーワードブロック	129
URL のフィルタリング	132
カテゴリに基づいたウェブサイトのブロック (URL 分類)	132
ホワイトリスト	133
ブラックリスト(ブロックのカスタマイズ)	134
MIME フィルタリング	135

デフォルトの MIME フィルタリング	136
カスタムの MIME フィルタリング	136
キーワードブロック	137
アプリケーションコントロール	139
侵入防止システム (IPS)	140
デフォルトのルール	141
カスタムのルール	142
デバイスの管理	146
管理者	146
日時の設定	146
管理者設定	147
管理者の追加	148
管理者プロファイル	150
ウェブポータルのカスタマイズ	152
SMTP 設定	154
アップデート	156
サービスアップデートの設定	156
システムアップデートの設定	157
手動アップデートの設定	157
バックアップと復元	160
出荷時設定へのリセット	165
ライセンス情報ページ	165
ライセンスの更新	168
Seqrite Cloud の有効化	168
ログとレポート	171
インターネット使用量	171
ウェブサイトアクセスレポート	173
メール保護	177
ウェブ保護	178
侵入防止	179

ポリシー違反活動	180
帯域幅使用量	181
アプリケーションコントロール	182
ファイアウォールレポート	183
アップデート	184
ログビューア	185
レポートを削除する	188
通知	189
通知メディア	189
メール通知	189
SMS 通知	190
通知の設定	193
コマンドラインインターフェース (CLI)	196
CLI を使用して Seqrite Terminator を設定する	196
Terminator の設定と管理	197
Terminator の設定と管理 ウェブ管理	197 198
Terminator の設定と管理 ウェブ管理 ネットワーク設定	197 198 199
Terminator の設定と管理 ウェブ管理 ネットワーク設定 CLI を使用してサービスを管理する	197 198 199 202
Terminator の設定と管理. ウェブ管理 ネットワーク設定. CLI を使用してサービスを管理する. CLI によるトラブルシューティング.	197 198 199 202 204
Terminator の設定と管理.         ウェブ管理.         ネットワーク設定.         CLI を使用してサービスを管理する.         CLI によるトラブルシューティング.         データベースユーティリティのトラブルシューティング.	197 198 199 202 204 205
Terminator の設定と管理.         ウェブ管理.         ネットワーク設定.         CLI を使用してサービスを管理する.         CLI によるトラブルシューティング.         データベースユーティリティのトラブルシューティング.         ネットワークツールのトラブルシューティング.	197 198 199 202 204 205 206
Terminator の設定と管理. ウェブ管理. ネットワーク設定. CLI を使用してサービスを管理する. CLI によるトラブルシューティング. データベースユーティリティのトラブルシューティング. ネットワークツールのトラブルシューティング. デバッグ情報のトラブルシューティング.	197 198 199 202 204 205 206 207
Terminator の設定と管理. ウェブ管理. ネットワーク設定. CLI を使用してサービスを管理する. CLI によるトラブルシューティング. データベースユーティリティのトラブルシューティング. ネットワークツールのトラブルシューティング. デバッグ情報のトラブルシューティング.	197 198 202 204 205 206 207 208
Terminator の設定と管理 ウェブ管理 ネットワーク設定 CLI を使用してサービスを管理する CLI によるトラブルシューティング データベースユーティリティのトラブルシューティング ネットワークツールのトラブルシューティング デバッグ情報のトラブルシューティング トラブルシューティング.	197 198 202 204 205 206 207 208 208
Terminator の設定と管理 ウェブ管理 ネットワーク設定 CLI を使用してサービスを管理する CLI によるトラブルシューティング データベースユーティリティのトラブルシューティング ネットワークツールのトラブルシューティング デバッグ情報のトラブルシューティング. サポート. トラブルシューティング メールサポート.	197 198 202 204 205 206 207 208 208 208
Terminator の設定と管理.         ウェブ管理.         ネットワーク設定.         CLI を使用してサービスを管理する.         CLI によるトラブルシューティング.         データベースユーティリティのトラブルシューティング.         ボットワークツールのトラブルシューティング.         デバッグ情報のトラブルシューティング.         サポート.         トラブルシューティング.         電話サポート.	197 198 202 204 205 206 207 208 208 208 209
Terminator の設定と管理.         ウェブ管理.         ネットワーク設定.         CLI を使用してサービスを管理する.         CLI によるトラブルシューティング.         データベースユーティリティのトラブルシューティング.         ボットワークツールのトラブルシューティング.         デバッグ情報のトラブルシューティング.         サポート.         トラブルシューティング.         メールサポート.         電話サポート.         リモートサポート.	197 198 202 204 205 206 207 208 208 208 209 209



概要

### 統合脅威管理 (UTM) について

今日の世界ではセキュリティの脅威がますます増大しつつあり、管理者はファイアウォ ール、侵入防止システム、アンチウイルスなど、いくつものセキュリティソリューショ ンを必要としています。統合脅威管理(UTM)とは、統合されたネットワークセキュリ ティ製品で、すべてのセキュリティソリューションを1 つのソリューションとしてネ ットワーク管理者向けに提供し、その複雑性を低減します。

この統合ソリューションにより、管理者はすべての管理、監視、ログ記録を 1 か所で 行えるようになります。これによって、いくつものセキュリティソリューションを展開 して監視するために必要な時間とコストを削減できます。

#### Terminator の機能

Seqrite Terminator は UTM ソリューションで、各種のセキュリティソリューションを 単一のセキュリティアプライアンスに統合したものです。Seqrite Terminator には次 の保護機能が含まれています:

保護機能	運用分野の説明
アンチウイルス	コンピュータウイルス、コンピュータワーム、トロイの木馬、ス パイウェア、アドウェア、その他のマルウェアを防止、検出、削 除します。ウイルスに感染したファイルの修復を試み、または削 除します。
アンチスパム	追加料金による機能です。すべてのコンテンツを自動的にスキャンし、スパムやフィッシングのメールを削除して、フィッシング やスパムの攻撃からシステムを保護します。
ファイアウォール	特定のルールに基づいてネットワークトラフィックを許可または 拒否し、正当な通信は通過を許可しながら、認可されていないア クセスからネットワークを保護します。

保護機能	運用分野の説明
ウェブ/URL フィ ルタ	先制的なセキュリティ手法として、ウェブサイトのフィルタリン グによりネットワークを保護し、不適切なウェブサイトやコンテ ンツの閲覧を防止します。
侵入防止システム (IPS)	ネットワークへの侵入を検出および防止して、ネットワークを保 護します。システムへ侵入する可能性があるハッカーから、シス テムを保護します。

さらに、Seqrite Terminator では安全な作業環境を推進するため、次のような機能が 提供されます:

機能	説明
ゲートウェイで のメール保護	送信および受信されるメールメッセージと、その添付ファイルをス キャンします。組み込まれているスパムフィルタにより、受信され るメールメッセージに対して一連のテストが実行されます。 Terminator は POP3、IMAP、SMTP プロトコルをサポートしていま す。
仮想プライベー トネットワーク (VPN)	リモートオフィスやローミングユーザーが、公共アクセス可能なネ ットワーク(インターネット)を経由して、所属する組織のネット ワークへ安全にアクセスして通信できます。
帯域幅管理	帯域幅の割り当てを許可し、帯域幅の使用を最適化します。グルー プ間の使用量をベースにして割り当てを実行できるため、企業の帯 域幅コストを削減できます。
ダイナミックホ ストコンフィギ ュレーションプ ロトコル (DHCP)	Terminator は DHCP サーバーとして機能し、ホストへ IP アドレス を割り当て、IT 管理者が構成に費やす時間を減らします。
負荷分散	Terminator で複数の ISP を使用できます。この機能により、トラフィックを重み付けと優先度に基づいて複数の ISP ラインに分散できます。
IP ポート転送	リモートコンピュータから、LAN 内の特定のコンピュータやサービ スへ接続できるようにします。

機能	説明
コンテンツフィ ルタリング	ウェブサイトにフィルタリングを適用し、ネットワークからアクセ スできる URL やドメインのホワイトリストを作成できます。同様 に、ウェブサイト、URL、ドメインのブラックリストを作成し、そ れらへのアクセスを禁止できます。
ログとレポート	使いやすいウェブベースの構成により、包括的なログ記録とレポー トを使用できます。
リンクの自動フ ェールオーバー	ISP ラインのいずれかに障害が発生した場合、非アクティブな ISP からアクティブな ISP のラインへ自動的にデータトラフィックを 振り替えます。
ポリシーに基づ いたルーティン グ	管理者が指定した基準に基づいてルーティングを決定するための機 能です。通過するネットワークトラフィックが指定された基準を満 たしている場合、トラフィックはターゲットのネットワークインタ ーフェースのリンク、またはターゲットのゲートウェイを経由して 転送されます。
アプリケーショ ンの分類とコン トロール	この機能により、アプリケーションへのアクセスを許可またはブロ ックするルールを必要に応じて設定し、アプリケーションへのアク セスをコントロールできます。

Chapter 2

### 登録ウィザード

Seqrite Terminator アプライアンスは、操作する前にライセンスを登録し、ネットワークを設定する必要があります。Terminator のウェブインターフェースから正常にログインすると、登録ウィザードが表示されます。このウィザードで、ネットワークインターフェース、DNS、アプライアンスの日時、およびアプライアンスのパスワードを設定し、登録手続きを完了できます。

登録ウィザード	🗳 オブション -	×
ತರ್ಶಕ	登録ウィザードへようこそ	
使用許諾契約書		
インターフェース		
DNS		
バスワード変更	URLフィルタリング SECPITE	
日時		
登録		
完了		
	このウィザードを使用して、ネットワークインターフェース、DNS、日時、アブライアンスのバスワードの設定を行い、登録 ロセスを完了できます。	<b>क</b> ⁻.
	戻るの次	

ウィザードの右側にある [オプション] ボタンで以下のオプションを利用できます。

- ヘルプ:Terminator の使用方法を案内するヘルプファイルのセットです。
- シャットダウン:デバイスをシャットダウンできます。
- 再起動:デバイスを再起動できます。
- ログアウト:デバイスからログアウトします。
- システム情報:システム情報を閲覧できます。
- 診断ツール:Terminator の別のモジュールのデバッグ情報を収集できます。

以下に記載する手順に従い、ネットワーク設定をセットアップし、Terminator を登録 します。

#### 使用許諾契約書

最初の手順は、ユーザー使用許諾契約書に同意することです。登録ウィザードの[よう こそ]画面で[次へ]ボタンをクリックすると、ユーザー使用許諾契約書が表示されま す。使用許諾契約書をよく読み、契約条件を受け入れるために[同意する]チェックボ ックスを選択し、[次へ]をクリックします。

き録ウィザード	🐴 オブション -
ತ್ರಾವ <del>ಕ</del>	使用許諾契約書
使用許諾契約書	
インターフェース	Segrite Terminator (UTM)エンドユーザー使用許諾契約書
DNS	
バスワード変更	Segrite Terminator (以下「Terminator」とする) をご使用になる前、またはご使用を試みる前に、本
日時	Seqrite Terminator (統合脅威管理/UTM) エンドユーザー使用許諾契約書 (以下「契約書」とする)を注意深くお読みください。
登録	Terminatorの使用、または [同意する] オブションの選択、またはいかなる方法であれ Terminatorをイ
完了	ンストールしようとする試み/同意(そうした行為はお客種の同意および著名行為の一部とみなされま す)により、お客様は本契約書に記載されたすべての契約条件を読み、理解し、同意したことを確認お よび承認したものとみなされます。本契約書は、ひとたび「お客様」[Terminatorを使用する予定の(19 歳以上であるかまたは契約を結ぶ法的能力がある)個人、または企業、または法人(以下「お客様」と いいます)]によって承認されると、お客様およびQUICK HEAL TECHNOLOGIES LIMITED.(正式名称 OHICK HEAL TECHNOLOGIES PRIVATE LIMITED)、本社インドーブネー(い下「Sacrital とい)ます)との「
	☑ 同意する
	展る」(次へ

#### インターフェース

次の手順で、登録ウィザードでインターフェースの設定を行います。[使用許諾契約書] 画面で [次へ] ボタンをクリックすると、インターフェース画面が表示されます。 注意:インターネット接続のインターフェースは緑色で示されます。

#### Terminator へのアクセス

登録ウィザード							🌼 रा	ブション - ×
432 <del>7</del>	インターフ	ェース					追加	削除
使用許諾契約書	▶ 名前	ゾーン	ノ ステータ	<sup>1</sup> ス IPアドレス	ゲートウェイ	「P割り当	て デフォルト	յի–ի
インターフェース	🗌 eth0	LAN	オンオフ	192.168.40.1		静的		
DNS	🗌 eth1	WAN	オン	10.10.105.171	10.10.104.1	静的	デフォルト	
バスワード変更	eth2							<u> </u>
日時	eth3							<u> </u>
登録	eth4							<u> </u>
完了	🗌 eth5							Ô
							<u>ل</u>	え 次へ

1. インターフェースを設定するには、LAN の場合 eth0、WAN の場合 eth1 などのイン ターフェース名をクリックします。

登録ウィザード			🖨 オプション 👻 🗙
ತರಿಕ	インターフェース、	編集 eth1	保存 キャンセル
使用許諾契約書	インタフェース名	eth1	
インターフェース	ゾーン	◯ LAN ( ) WAN ( ) DMZ	
DNS	旧割り当て	<ul> <li></li></ul>	
バスワード変更	IPv4アドレス	10.10.104.167	
日時	サブネットマスク	255.255.252.0 🗸	
登録	IPv4ゲートウェイ	10.10.104.1	
完7	ハードウェアアドレス	00:0B:AB:63:FE:1C	
			戻る 次へ

- インターフェース名を入力し、ゾーンと IP 割り当てを選択します。LAN インター フェースの場合、IP 割り当てはスタティックのみとなります。WAN の場合、スタテ ィック、ダイアルアップ、または DHCP のいずれかが可能です。
- 3. [保存] をクリックして、変更を保存します。
- インターフェイス、エイリアス、VLAN、ブリッジ、および Link アグリゲーション を追加することもできます。[追加する] をクリックして新しいインターフェイスを 追加します。(インターフェイスの追加に関する詳細は、インターフェイスセクショ ンを参照してください。)

5. [次へ]をクリックして、DNS 設定を行う次の手順に進みます。

DNS

この手順では、デフォルトのドメイン名サーバー設定をオーバーライドします。ISP で 提供される DNS、または使用したい DNS を入力できます。現在のサーバーがダウンし た場合、DNS の優先順位を変更して、別の DNS サーバーを試すこともできます。

1.	「近川」	875	199	しより。	
	TH ARA				

19x7779 Tr		1 V V V V V
ようこそ	DNS	
使用許諾契約書	追加   肖购	👔 優先度を変更しました 🛛 🚺 🚹
インターフェース	DNSの名前	
DNS	DNSを入力してください 道加     B8.8.8	×
バスワード変更		
日時		
製品キー		Ŧ
完了		
		戻る)次へ

2. テキストボックスに [DNS 名] を入力して [追加] をクリックします。リストにその DNS が追加されます。

3. **[次へ]** をクリックします。

注意:DNS リストを空欄にすることはできません。少なくとも 1 つの DNS エントリが 必要です。デフォルトエントリ 8.8.8.8 が存在します。

パスワード変更

ウェブと CLI インターフェースのデフォルトアプライアンスパスワードを変更しなけ ればなりません。[DNS 設定] 画面の [次へ] ボタンをクリックすると、[パスワード変 更] 画面が表示されます。

登録ウィザード	🌼 オブション 🗸 🗙
452 <del>7</del>	ウェブバスワード変更
使用許諾契約書	古いパスワード
インターフェース	新しいパスワード
DNS	パスワードの再入力
バスワード変更	
日時	CLIバスワード変更
音録	新しいパスワード
<u></u> 宗7	パスワードの再入力
	☑ この手順をスキップ
	*注意:次回のログインではこれらの新しいパスワードを使用してください。
	戻る」次へ

- 1. ウェブと CLI インターフェースに新しいパスワードを設定します。
- 2. 【次へ】 をクリックすると、新しいパスワードが保存されます。次にウェブまたは Terminator の CLI インターフェースにログインしたときは、新しいパスワードを 使用しなければなりません。

日時

パスワードを変更後、アプライアンスの日時を設定しなければなりません。[パスワード変更] 画面で [次へ] をクリックすると、[日時] 画面が表示されます。[日時] 画面 では、アプライアンスの現在の日時が表示され、異なる地域ごとにアプライアンスの日時を設定できます。NTP サーバーと日時を同期させることもできます。

登録ウィザード			🌻 オプション 🕤 🗙
ಚರಿವ <del>ನ</del>	日時		
使用許諾契約書	現在の日付:	2015-10-15 13:56:10	
インターフェース	タイムゾーン:	Asia/Tokyo	
DNS	日付と時刻を設定します:	● マニュアル  ◎ NTP サーバーと同期します	
パスワード変更		日付: 15 • 10月 • 2015 •	
日時		時刻: 13 ▼ HH 56 ▼ MM	
登録			
完了			
			戻る次へ

- 1. アプライアンスを導入する地域に基づいて、[タイムゾーン]を選択します。
- 2. 以下の 2 つの方法の 1 つを使用して日時を設定します。
  - **手動**:日時選択ボックスで日時を設定するオプションを選択します。または、以下の方法を選択します。
  - NTP サーバーと同期:このオプションを選択すると、アプライアンスの時間が事前に定義された NTP サーバー (asia.pool.ntp.org & in.pool.ntp.org) と自動的に同期、または新しい NTP サーバーが追加されます。

[今すぐ同期] をクリックすると、リストされた NTP サーバーとアプライアンス の時計が同期されます。アプライアンスの時間は、最低限の時差で NTP サーバ ーと同期されます。

3. [次へ] をクリックします。

#### プロダクトキー

アプライアンスを登録している間に、使用されているアプライアンスのプロダクトキー を提供しなければなりません。[日時] 設定画面で [次へ] をクリックすると、[プロダ クトキー] 画面が表示されます。

1. 有効なプロダクトキーを入力して、[次へ] をクリックします。プロダクトキーは、 ユーザーガイドの表紙の内側にあります。

登録ウィザード	4	オブション -	×
(ಚನಿವ <del>ನ</del>	ブロダクトキー		
使用許諾契約書	ブロダクトキー*:		
インターフェース			
DNS			
バスワード変更	ブロダクトキーは 保証書に記載されています.		
日時			
プロダクトキー			
完了			
		戻る次へ	

2. 新しいアプライアンスを登録する場合、[カスタマ詳細] 画面が表示されます。

登録ウィザード				🚦 オプション - 🛛 🗙
ತಿರ <del>್</del> ಶಿಕ	登録情報			
使用許諾契約書	登録情報を入力してください。	,		
インターフェース	会社名*			
DNS	会社電子メール*			
バスワード変更	会社電子メールの再入力*			
日時	電話番号*			
プロダクトキー	管理者電子メール*			
登録情報	*	日本	<b>v</b>	
詳細情報の確認	都道府県*	東京都	Ŧ	
完了	市町村*	名古屋市		
	購入先			
				戻る次へ

3. 必要な詳細を入力し、[次へ]をクリックします。

注意:赤いアスタリスクの付いた欄は必須です。

4. [次へ]をクリックすると、[確認詳細]画面が表示されます。

登録ウィザード			🝦 オプション 🗸 🗙 🕹
_±3こ <del>र</del>	詳細情報の確認		
使用許諾契約書	登録要求を送信する準	備ができました。	
インターフェース	プロダクトキー	****	
DNS	会社名	スズキ	
パスワード変更	会社電子メール	abc@xyz.com	
日時	電理者電子メール	admin@sample.com	
プロダクトキー	購入先	スズキ	
登録情報	市町村都道府県	東京 三重県	
詳細情報の確認	国	日本	
完了			
			戻る」次へ

5. Terminator を最新バージョンにアップデートした場合、または組織で特定の問題が ある場合、アプライアンスを再度有効化させなければなりません。再度有効化させ ると、プロダクトキーを入力した後に、以下の画面が表示されます。

登録ウィザード		🛟 オプション - 🛛 🗙
ತರ್ಧಕ	詳細情報の確認	
使用許諾契約書	指定されたブロダクトキーは、以下の詳細ですでに登録されています。	
インターフェース	<b>ブロダクトキー XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</b>	
DNS	ライセンス有効期限 09 December 2016	
バスワード変更	登録を持行するには 1次へ1をクリックにます。	
日時		
プロダクトキー		
詳細情報の確認		
完了		
		戻る次へ

- 6. 詳細を確認し、[次へ] をクリックします。
- 7. ハードウェアを交換する場合、登録時に返品確認 (RMA) を提供しなければなりません。交換用のハードウェアと一緒に RMA コードを受け取ります。この場合、以下の 画面が表示されます。

登録ウィザード	オプション -	×
ತರ್ರದ	詳細情報の確認	
使用許諾契約書	指定されたプロダクトキーは、以下の詳細ですでに登録されています。	
インターフェース	プロダクトキー xxxxxxxxxxxxxxxxx 会社名 Segrite Terminator	
DNS	ライセンス有効期限 14 September 2016	
バスワード変更	このアプライアンスを有効化するには、交換ハードウェアとともに受領した返品確認 (RMA) コードを入力してください。	
日時		
製品キー 詳細情報の確認	登録を続行するには、[次へ]をクリックします。	
完了		
	戻る」次へ	

- 8. [RMA コード] を入力し、[次へ] をクリックします。
- 9. 正常に登録されると、[ライセンス有効期限] 画面が表示されます。

_ 登録ウィザード	🌼 オブション 🗸 🗙
ತರಿವರ್	完了
使用許諾契約書	登録は正常に完了しました。
インターフェース	
DNS	ライセンス有効期限 14 September 2016
バスワード変更	
日時	
製品キー	
詳細情報の確認	
完了	
	戻る 完了

10. [終了] をクリックして、アプライアンスの登録手順を完了させます。[終了] をク リックすると、ログアウトします。新しいパスワードで再度ログインします。

機能の使い方、その他の関連情報の詳細は、Seqrite Terminator の [ヘルプ] セクションをご覧ください。

技術サポートがさらに必要な場合は、Seqrite Terminator 技術サポートセンターにお 問い合わせください。



### Terminator へのアクセス

Seqrite は組織内の様々なネットワーク設定を踏まえ、代表的な 3 種類のネットワーク設定用インストールを推奨しています。ネットワークのセットアップと Terminator の登録の詳細については、『Seqrite Terminator スタートガイド』または『Seqrite Terminator クックブック』を参照してください。

### Seqrite Terminator へのログイン

Terminator ヘアクセスする方法は 2 つあります。

- <u>ウェブ経由で Terminator ヘアクセスする</u>
- <u>CLI 経由で Terminator ヘアクセスする</u>

#### ウェブ経由で Terminator ヘアクセスする

1. ウェブブラウザを開始し、デバイスの IP アドレスをアドレスバーへ入力します。 ログインページが表示されます。



- 2. テキストボックスに [ユーザー名] および [パスワード] を入力します。
- 3. [ ログイン] をクリックすると、ホームページが表示されます。

コマンドラインインターフェース (CLI) 経由で Terminator ヘア クセスする

ウェブインターフェースを使用して Seqrite Terminator ヘログインする他に、端末エ ミュレータや Putty などのクライアントを使用して、コマンドラインインターフェー ス (CLI) から Seqrite Terminator ヘログインすることもできます。CLI コンソール は、特定の Seqrite Terminator コンポーネントを管理、監視、制御するための各種ツ ールを提供します。

Seqrite Terminator CLI コンソールには、次に示すデフォルトの資格情報を使用して、2 つの方法でアクセスできます:

ユーザー名: admin

パスワード: admin@123

• **直接接続**:キーボードとモニターを、VGA またはコンソールケーブル (COM ポート) を使用して直接 Seqrite Terminator へ接続できます。

VGA を使用して Terminator を接続するとき、ブートデバイスは SATA:3M San-Disk SDCFH-003G にする必要があります。

コンソールケーブルを使用して Terminator を接続するときは、CLI にアクセスするため Putty で次の設定を行ってください。

o ボーレートを 19,200 に設定します。

8	PuTTY 設定	? ×
カテゴリ(G):		
日- ゼッション	<ul> <li>ローカルシリアルボー</li> <li>シリアルボートの選択</li> </ul>	-トの設定
ーキーボード - キーボード - ベル	接続先のシリアルポート(L)	COM1
- 高度な設定	シリアルポートの設定	
	通信速度 (ボー)(S)	19200
	データ長 (ビット)(B)	8
選択	ストップビット(T)	1
壁紙	パリティ(P)	なし 🗸
□-接続	フロー制御(F)	XON/XOFF 🗸
- テータ - プロキシ - Telnet - Rlogin ⊕ SSH - シリアル		
About ヘルプ(H	() 開(((	O) 取消(C)

o 図に示すように、接続タイプとして [シリアル] を選択します:

8	PuTTY 設定	? X
カテゴリ(G):		
日- セッション	PuTTY セッションの基本設定	
	接続先の指定	
ーキーボード	シリアルポート(N)	スピード(P)
ベル 	COM1	19200
□-ウィンドウ □-外観	接続タイプ 〇 Raw 〇 Telnet 〇 Rlogin 〇 SSH	● シリアル
·····································	セッションの読込、保存、削除 セッション一覧(E)	
	標準の設定	読込(L)
データ		保存(V)
ー・ブロギシ ー・Telnet ー・Rlogin		肖J『除(D)
⊕-SSH └─ジリアル	※7時のウィンドウクローズ(W): ○常にする ○しない ●クリーンな終	了時のみ
About ヘルプ(ト	)) 開((0)	取消(C)

- **リモート接続**:次の方法で、Seqrite Terminator ヘリモート接続できます:
  - リモートログインユーティリティを使用して、CLI コンソールへアクセスします。
  - o 「Telnet xxx. xxx. xxx. xxx」と入力します。 xxx. xxx. xxx は Terminator サーバーの IP アドレスです。

注意:デフォルトでは Telnet は無効化されています。

 SSH クライアントを使用して CLI コンソールへアクセスします。SSH クライ アントを使用して、Seqrite Terminator の CLI コンソールへアクセスでき ます。.

注意:SSHv1 と SSHv2 の両方がサポートされています。

• ログインが成功すると、次に示す [メインメニュー] 画面が表示されます:



メニュー項目にアクセスするには、[メニュー番号を入力してください]のプロンプトに対して、メニュー項目に対応する番号を入力し、Enter キーを押します。各サブメニューには[戻る]および[終了]オプションがあります。[戻る]で1レベル上に移動し、[終了]でCLIコンソールを終了します。

登録を行う前は、次のメニューにのみ CLI からアクセスできます:

1. Terminator の設定と管理: ウェブスーパー管理者のパスワードのリセット、イン ターフェースと DNS の設定、および Terminator アプライアンスの再起動とシャッ トダウンを行います。

2. トラブルシューティング: IP の Ping および Traceroute に使用します。

### Seqrite Terminator の操作(ウェブ)

ウェブベースのコンソールから Seqrite Terminator にアクセスすると簡単に操作が行 え、機能やオプションはカテゴリに応じて分類して表示されます。

下の図に示すように、Seqrite Terminator のユーザーインターフェースは次の 5 つの 主なセクションに分類されます。



- ホーム Seqrite Terminator の機能の基本的な要約と、各種の使用状況グラフが 表示されます。
- コンテンツフィルタリング コンテンツフィルタリングの設定、例えばコンテンツ ブロック、ウェブサイトブロック、ブロックのカスタマイズ、ホワイトリストの作 成などを行います。

- **ユーザー管理** ユーザー、ゲストユーザー、グループ、時間カテゴリの詳細、認証 サーバーを設定します。
- 設定 Seqrite Terminator の各種の設定を行います。これにはインターネット設定、メールサーバー設定、ファイアウォール、インターフェース設定、VLAN、VPN などが含まれます。
- ログとレポート インターネット使用量、ウェブサイトアクセス、ウイルス対策、 ポリシー違反などに関するレポートを提供します。

#### 共通のオプション

ユーザーインターフェースの上端には、次のオプションが表示されます。これらのオプ ションはすべてのタブに共通で、どのページからも使用できます。

Sparita			🔅 オブション -   ? ヘルブ	▼ (也) シャットダウ	ンする 🗕	→ Admin (管理) -
TERMINATOR		ホーム	コンテンツフィルタリング	ユーザー管理	設定	ログとレポート
タブ	機能					

[ウェブパスワードの変更]を使用して、現在ログインしている管理 者のパスワードを変更します。ここをクリックすると、次のオプショ ンが表示されます。
<b>現在のパスワード</b> :ログインしている管理者の現在のパスワードを 入力します。
<b>新しいパスワード</b> :設定したい新しいパスワードを入力します。
<b>パスワードの再入力</b> :新しいパスワードを再入力します。
[送信] をクリックするとパスワードが変更され、管理者はログアウトされます。管理者は新しいパスワードでログインする必要があります。
注意:スーパー管理者のウェブパスワードを変更しても、CLI パスワ ードは変更されません。
CLI パスワードのリセット - CLI パスワードをリセットします。CLI には、スーパー管理者ユーザーがアクセスできます。CLI アクセスの パスワードは、このオプションを使用して変更できます。ここをクリ ックすると、次のオプションが表示されます。
<b>新しいパスワード</b> :設定したい新しい CLI パスワードを入力しま す。
<b>パスワードの再入力</b> :新しいパスワードを再入力します。

タブ	機能
	[送信] をクリックすると、CLI パスワードが変更されます。
	<b>SSL 証明書</b> - SSL 証明書をダウンロードします。SeqriteTerminator は自己署名された証明書を使用します。この証明書は .der 形式でダ ウンロードされます。
ヘルプ	<b>ヘルプ</b> - Terminator を使用するための手引きとなる、一連のヘルプ ファイルを参照できます。
	<b>ライセンス情報</b> - 現在のライセンス情報を表示します。
	<b>サポート</b> - 利用できるサポートのオプションにアクセスします。
シャットダ ウン	デバイスをシャットダウンまたは再起動できます。
管理者	ログインしているユーザーの名前と、プロファイルタイプ (読み取 り専用または管理者モード) を表示します。プロファイルタイプが [管理者] の場合、ユーザーは書き込みアクセスを許可され、設定の 変更や保存を実行できます。読み取り専用アクセスのユーザーは、設 定を変更できません。
	<b>ログアウト</b> :デバイスからログアウトします。



### ダッシュボード

ホームページ (ダッシュボード) は、Seqrite Terminator ヘログインしたとき最初に 表示されるページです。ダッシュボードには、Seqrite Terminator により実行されて いる各種の動作のステータスがリアルタイムで表示されます。ホームページのデータは、 [更新] ボタンを使用して最新の値にアップデートできます。

ホームページのダッシュボードは、次の 2 つの部分で構成され、必要に応じて画面を 上下にスクロールして、それぞれの部分にアクセスできます:

- 通知、ステータス、インターネット使用量の領域
- 統計の領域

### 通知、ステータス、インターネット使用量

	Searite	•	オプション   <mark>?</mark> へ	ルブ -   🕛 シャット	- ダウンする 🚽   😝 Admin (管	\$理) -
	TERMINATOR	ホーム コンき	テンツフィルタリング	ブ ユーザー管:	理 設定 ログとレポ	₹ <b>−</b> ト
	今日 ▼ ステータス				最新の情報	に更新
	🧕 データとコンテンツ保護 🛛 🗕 電子メーノ	/保護 🛛 🗕 インターネットと	ネットワ 🔮 ターミ	ネーターデバイス		
	<ul> <li>✓ アンチウイルス</li> <li>✓ アンチウイルス</li> <li>✓ アンチウイルタリング</li> <li>★ 添付ファイ</li> <li>★ アブリケーションコントロ</li> <li>★ キーワート</li> <li>◆なのインターネットの使用量</li> <li>前回</li> </ul>	ルス ✓ インターネットア ルコントロ✓ 侵入防止 ブロック ¥ VPN ✓ ポリシーに基づ × オフラインモード アップデート: Oct 19 16:23 PM	クセス local CPU使用 いたルーティー・メモリ使 ・ インターネット!	eth1 WAN eth3 理: 26% ディ: 用量: 74% 仮想	eth4 eth5 スクの使用状況: 62% メモリー: 2%	
	✓ WAN					
	150				コンビュータとテクノロジー	:
(MB)	100	$\wedge$			79.11% 検索エンジンとボータル : 9	9.73%
重馬	50				ニュース:8.14%	
Ð	0				画像共有 : <b>1.93%</b>	
	2am 4am 6am 8am 10am	12pm 2pm 4pm			金融:1.10%	
	-●- 受信 -●- 発信					

• 通知領域 - 次のような警告と通知が表示されます:

- 利用可能なライセンス数を超過した。
- ライセンスの有効期限が切れた場合。
- アンチウイルスが最新ではありません
- アップデートサービスが実行されていない。

通知が表示される条件と、その説明を次の表に示します。

通知	説明
ユーザー数がライセ ンスの上限を超えて います。サポートす るユーザー数を増や すには、ライセンス をアップグレードし てください。	この通知は、Terminator に現在ログインしているユーザー数 が、ライセンスを受けているユーザー数の上限以上である場 合に表示されます。
アップデートサービ スが実行されていま せん。技術サポート にお問い合わせくだ さい。	この通知は、アンチウイルスデータベースのアップデートサ ービスの実行が停止した場合に表示されます。
アンチウイルスが最 新ではありません。	この通知は、アンチウイルスが 3 日間以上アップデートされ ていない場合に表示されます。[今すぐアップデート] ボタン を使用して、アンチウイルスをアップデートしてください。
Seqrite Terminator ライセンスの有効期 限が近づいていま す。ライセンスを更 新してください。	この通知は、ライセンスの有効期限が近づいたときに表示されます。Terminator のライセンスを更新するよう、管理者に 警告するものです。ライセンスの有効期限が切れる 30 日前から表示されます。
ディスク容量がいっ ぱいです。システム によって削除される 前に既存のレポート をエクスポートして ください。	この通知は、ディスクの使用量が 85% を超えた場合に表示されます。管理者は、クリーンアップ作業としてレポートをダウンロードする必要があります。システムは、ディスク容量を空けるため、最初に最も古いレポートを、次に最も古いログを削除します。
Seqrite Terminator ライセンスの有効期	この通知は、Terminator ライセンスの有効期限が満了したと きに表示されます。Terminator の有効期限が満了すると、ア

ネットワーク設定

通知	説明
限が切れました。ラ イセンスを更新して ください。	ンチウイルスのアップデートサービスとウェブサイトの分類 サービスが停止されます。ライセンスを更新すると、これら のサービスも再開されます。
技術的な問題のた め、IPS サービスが 無効化されました。 技術サポートにお問 い合わせください。	この通知は、技術的な問題のため IPS サービスを開始できな い場合に表示されます。
IPS のアップデート が存在します。今す ぐ更新しますか?	この通知は、IPS のアップデートが利用可能なときに表示され ます。IPS ルールのアップデートチェックは、12 時間ごとに 行うようスケジュールされています。
ログサイズの上限に 近づいています。シ ステムによって削除 される前に、既存の ログをエクスポート してください。	この通知は、アーカイブのログファイルのサイズが 30 MB に 到達した場合に表示されます。ログがこの上限に達すると、 アーカイブからログが削除されます。最も古いログが最初に 削除されます。
ライセンスがブロッ クされています。ア ップデートを受け取 ることができませ ん。カスタマーサポ ートに連絡してくだ さい。	複数のデバイスが同じプロダクトキーを使用しているために ライセンスがブロックされると、この通知が表示されます。

アップデートと問題解決のオプションも存在します。アプリケーションから発行された 警告の数によっては、複数の通知が同時に表示されることもあります。

• ステータス領域 - データとコンテンツの保護、メール、インターネットとネット ワーク、および保護が有効かどうかについて、各種設定の現在のステータスが表示 されます。

ステータ ス	説明
*	モジュールは有効で、実行中です。

×	モジュールが無効であるか、有効だが実行されていないことを示してい
	ます。

 Terminator デバイス - この部分には、Terminator デバイスの各種イーサネット ポートのステータスが表示されます。CPU 使用量、ディスク使用量、メモリ使用量、 および仮想メモリのステータスもリアルタイムで表示されます。

アイコン	説明
	イーサネットケーブルが接続されていることを示しています。
•	イーサネットケーブルが接続され、インターネットが利用可能であるこ とを示しています。
$\square$	イーサネットケーブルが接続されていないことを示しています。

インターネット合計使用量とインターネットトラフィック配信 - 受信および送信
 トラフィックごとのインターネット合計使用量と、インターネットアクセスにおけるコンテンツのカテゴリごとのパーセンテージが表示されます。

### 統計の領域

トップウイルスがプロックされ、 トップ侵入を防止	ブロックした主なウイルス EICAR.TestFile Blk/Domain.05053538	(トータル 8) 87.5 12.5	すべて表示 % %	防止した主な侵入 (トータル (http_inspect) TOO MANY PIPELIN	> 13) IED REQUESTS	すべて表示 100 %
	アクセスした主なウェブサ	イト 使用!	▮ #訪問数	防止した主なポリシー違反	ウェブサイト	ユーザー
	ウェブサイト/URL	カテゴリー	使用量 (MB)	ウェブサイト/URL	カテゴリー	#試行数
トップウェブサイトにアクセスし	https://r9sn-cvh7zn76.google	. ストリーミングメディアお	14.5	http://www.bing.com/	検索エンジンとボータル	8
	https://s0.2mdn.net/	広告とボッブ・アップ	6.93	https://www.google.co.in/gen	検索エンジンとボータル	7
	https://r1sn-cvh7zn7z.google	ストリーミングメディアお	5.99	http://realtime.services.disqus.c	. 個人サイト	7
	https://r12sn-cvh7zne7.googl	. ストリーミングメディアお	4.25	https://www.google.co.in/s?	検索エンジンとポータル	6
	https://www.google.co.in/	検索エンジンとボータル	3.32	http://www.yatra.com/	旅行	4
着信および送信メールのメール統計 💼	メール保護統計 2 1 1 i2am 2am 4am 6am す ・ 受信 → 筆信	- * - * - * - * - * - * - * - * - * - *	Żpm 2pm	ブロックした思染 ブロックしたスパム		5 0

ブロックされた主なウイルスと、阻止された主な侵入 - Seqrite Terminator によってブロックされた主なウイルスと、ネットワークに影響を及ぼすことを阻止された主な侵入動作が表示されます。

- アクセスされた主なウェブサイトと、ポリシーへの主な違反 アクセスされた主 なウェブサイトについて、名前と訪問回数が表示されます。また、ブロックされて いる URL へのアクセスが試みられた回数も表示されます。[ユーザー] タブには、 ブロックされている URL へのアクセスを試みたユーザーのリストが表示されます。
- メール保護の統計 受信および送信メールのスキャン統計が表示されます。
- **ブロックされた感染** 感染した添付ファイル付きのメールがブロックされた回数 が表示されます。

注意:通知領域の上端にあるドロップダウンのオプションを選択すると、過去 24 時間、先週、先月について上記の統計を表示できます。

## Chapter

### ネットワーク設定

#### 定義

定義とは、各種の Terminator モジュールを設定するときに再利用できる、定義済みの ネットワークトラフィックタイプおよびサービスです。Terminator では、次の 2 タイ プの定義を追加できます。

**ネットワークの定義**:ネットワーク全体のサブセットを定義または追加するため使用します。

**サービスの定義**: アプリケーションにより通信に使用されるプロトコルとポートを追加 するため使用します。

[定義] ページには、ネットワーク定義とサービス定義のリストが表示されます。定義 は名前で検索できます。また、定義を追加、編集、削除できます。

#### 定義の追加

ネットワーク定義を追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [定義] ヘログオンします。次に示すページが 表示されます。
#### ネットワーク設定

Searite		🌼 オプション		-   也 シャットダウ	ンする -   📑 管	理(管理)▼
TERMINATOR		ホーム コンテンツ:	フィルタリング	ユーザー管理	設定 ログ。	ヒレポート
> インターネット	定義					
> アンチウイルス	定義名で検索する	5 🔍				
> 電子メール保護	定義リスト					追加 削除
定義 →	□ 名前	カテゴリー 🔻	タイプ 🍷	コメント		
> ファイアウォール設定	Any IPv4	ネットワーク定義	ホスト	任意の IP	v4アドレスと一致	^
> IPS	Any IPv6	ネットワーク定義	ホスト	任意の IP	v6アドレスと一致	
> アプリケーションコントロール	ISAKMP	サービス定義	サービス			
 ▶証明書	L2TP	サービス定義	サービス			
> IPSec VPN	🔲 ah	サービス定義	サービス			
> PPTP VPN	Any	サービス定義	サービス	任意の IP	アドレスと一致	
> SSL VPN	AOL IM	サービス定義	サービス			
・インターフェース	dns	サービス定義	サービス			
	esp	サービス定義	サービス			

2. [追加] をクリックします。[ネットワーク定義の追加] ダイアログボックスが表示 されます。

ネットワーク定義を作成	1		×
カテゴリー:	ネットワーク定義 🔻		
名前:			
タイプ:			
IPv4:			
IPv6:			
コメント:			
		保存	キャンセル

- 3. [カテゴリ] として [ネットワーク定義] を選択します。
- 4. [名前] に定義名を入力します。
- 5. **タイプ: [ネットワーク定義]** カテゴリを選択すると、このオプションが表示されます。

ネットワーク定義には、次の4つのタイプがあります。

- i. ホスト:単一の IP アドレスを定義します。IPv4/IPv6 アドレスを入力します。
- ii. **IP 範囲**:一連の IP アドレスを定義します。IPv4/IPv6 アドレスの範囲を入 力します。

- iii. IP リスト:IP アドレスのランダムなリストを定義します。IPv4/IPv6 アドレ スをコンマで区切って並べたリストを入力します。
- iv. **ネットワーク**:一組の IP アドレスを含むネットワークを定義します。IPv4 ネットワークアドレスを入力し、ドロップダウンからサブネットマスクを選 択します。IPv6 の場合は、IPv6 ネットワークアドレスと IPv6 プレフィッ クス値を入力します。
- 6. 定義の説明は、[**コメント**] テキストボックスに入力します。
- 7. **[保存]** をクリックします。新たに追加されたネットワーク定義は、[定義] ページのリストに表示されます。
- サービス定義を追加するには、以下の手順に従います:
- 1. Seqrite [Terminator] > [設定] > [定義] ヘログオンします。
- 2. [追加] をクリックします。[ネットワーク定義の追加] ダイアログボックスが表示 されます。
- 3. [カテゴリ] として [サービス定義] を選択します。

ネットワーク定義を作り	戊		×
カテゴリー:	サービス定義 🔹		
名前:			
プロトコル:	TCP 🔻		
ソースポート:	◉ 任意 ◎ ボート		
宛先ポート:	◉ 任意 ◎ ボート		
コメント:			
		保存	キャンセル

- 4. サービス定義の [名前] を入力します。
- プロトコル: [サービス定義] カテゴリを選択すると、このオプションが表示されます。ドロップダウンからプロトコルを選択します。プロトコルには、次の 4 つの タイプがあります:
  - i. TCP
  - ii. UDP
  - iii. ICMP
  - iv. IGMP

6. 送信元ポート:[サービス定義] カテゴリを選択すると、このオプションが表示され ます。送信元ポートのオプションを選択します。クライアントは、このポートで通 信用の接続を開始します。

任意:どのポートでも送信元ポートとして設定できます。 ポート:単一のポート、またはポートの範囲を入力できます。

宛先ポート:[サービス定義] カテゴリを選択すると、このオプションが表示されます。宛先ポートのオプションを選択します。通信用の接続は、このポートで受け付けられます。

任意:どのポートでも宛先ポートとして設定できます。

ポート:単一のポート、またはポートの範囲を入力できます。

- 8. コメント:サービス定義の説明を入力します。
- 9. [保存] をクリックします。新たに追加されたサービス定義は、[定義] ページのリ ストに表示されます。

# 定義の削除

定義を削除するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [定義] ヘログオンします。次に示すページが 表示されます。
- 2. 削除する定義を選択し、[削除] をクリックします。
   注意:現在使用されている定義は削除または編集できません。

# IPv6

インターネットプロトコル (IP) では、コンピュータがネットワーク上で通信を行うた めのアドレス指定スキーマが指定されます。インターネットプロトコルは、パケット交 換されるコンピュータ通信ネットワークの相互接続されたシステムで使用するために設 計されています。これによって、パッケージのアドレスを指定して、システムにドロッ プできます。

IP には現在、IPv4 と、IPv6 と呼ばれる新しいバージョンの 2 つがあります。IPv4 (インターネットプロトコルバージョン 4) は、アドレス指定システムを経由してネッ トワーク上のデバイスを識別するため使用される、IP の 4 番目のリビジョンです。 IPv4 は、インターネットヘデバイスを接続するために最も広く展開されているインタ ーネットプロトコルです。IPv4 は 32 ビットのアドレススキーマを使用しているため、 合計 2<sup>32</sup> アドレス (40 億と少しのアドレス) を使用できます。インターネットに接 続するすべてのデバイスには別のアドレスが必要なため、インターネットの成長につれ て、使用されていない IPv4 アドレスが使いつくされることが予想されています。 IPv6 は、インターネットプロトコルの全面的なアップグレードです。より多くのイン ターネットアドレスへの必要に対応するため、新しいインターネットのアドレス指定シ ステムである、インターネットプロトコルバージョン 6 (IPv6) が展開されつつありま す。IPv4 のアドレスは 32 ビットですが、IPv6 ではアドレスの長さが 128 ビットに 増えています。これによって、合計アドレス空間のサイズが 232 (約 43 億) から 2128 (約 340 × 1 兆 × 1 兆 × 1 兆) に増大します。またパケットヘッダのサイズも倍 になり、パケットごとに 20 バイトのオーバーヘッドが増えます。

IPv6 は外部的なデータの表現に「コロン付き 16 進数」(例: 2001:470:20::2)を使用します。これに対して、IPv4 は「ドット付き 10 進数」(例: 123.34.56.78)を使用します。IPv4 と IPv6 のいずれのアドレスも、内部的(メモリまたはワイヤ上)にはビット列(IPv4 では 32 個、IPv6 では 128 個)として表現されます。IPv4 のアドレスは外部的にはそれぞれ 8 ビットの 4 つのフィールドで表現され、各フィールドは3 桁までの 10 進数(0 ~ 255 の値)です。フィールドはドット(".")で区切られます。

Seqrite Terminator は IPv6 の IP フォーマットをサポートしており、有効にできま す。IPv6 を有効にすると、次の設定で IPv6 アドレスを使用できます:

- インターフェース
- DNS
- DHCP
- コンテンツフィルタリング(ブラックリスト/ホワイトリストおよびドメイン)

Seqrite Terminator では、既存の IPv4 ネットワーク上で IPv6 アドレスを自動的に トンネルすることもできます。6 to 4 トンネルにより、IPv4 ネットワーク上で、 IPv6 ドメインをリモートの IPv6 ネットワークへ接続できます。

## IPv6 の有効化

IPv6 を有効にするには、以下の手順に従います:

1. [Seqrite Terminator] > [設定] > [IPv6] ヘログオンします。デフォルトでは、 IPv6 サポートは無効化されています。

Searite	🌞 オブション +   🥐 ヘルブ +   🕐 シャットダウン +   🗗 Admin (管理) +
TERMINATOR	ホーム コンテンツフィルタリング ユーザー管理 設定 ログとレポート
<ul> <li>&gt; インターネット</li> <li>&gt; アンチウイルス</li> </ul>	IPv6     ステータス     6to4       IPv6:     ● 有効 ● 無効     保存
<ul> <li>&gt; 電子メール保護</li> <li>&gt; 京美</li> </ul>	接結性
<ul> <li>/ 正報</li> <li>&gt; ファイアウォール設定</li> <li>&gt; UPS</li> </ul>	6to4: 6to4トンネルは無効になっています
<ul> <li>アプリケーションコントロール</li> </ul>	ガイドライン
> 証明書 > IPSec VPN	インターネットブロトコルバージョン6(IPV6)は、インターネットブロトコル(IP)の最新版です。ここはIPV6のサポートが 有効になっています。有効にされた場合、ここにIPV6情報は提供されています。例 :6to4トンネルのステータス情報
> PPTP VPN > SSL VPN	
<ul> <li>&gt; インターフェース</li> <li>IPv6 ▶</li> </ul>	

2. [有効化]を選択し、[保存]をクリックします。

注意:Terminator で IPv6 サポートを有効にしていないと、IPv6 に関連する設定は いずれも行えません。

## 6 to 4 トンネルの有効化

特定のインターフェースについて IP アドレスのトンネルを有効にするには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [IPv6] ヘログオンします。
- 2. [6~4] をクリックします。次のページが表示されます。

Seqrite <b>TERMINATOR</b>	[	<mark>∲ オプション -</mark>   ホーム コンテンツフィルタリン	? ヘルブ -   () シャットダウン -   → Admin (管理) - ノグ ユーザー管理 設定 ログとレポート
> インターネット	IPv6		ステータス <b>6to4</b>
→ アンチウイルス	6to4:	◎ 有効 ⑧ 無効	保存
<ul> <li>電子メール保護</li> </ul>	インターフェース:		<ul> <li>IPv4ネットワーク上のIPv6トンネリングのために設定 されたパブリックIPインタフェースを選択してくださ</li> </ul>
<b>&gt;</b> 定義			ι).
> ファイアウォール設定			
> IPS	詳細		
> アプリケーションコントロール	サーバーアドレス	192.88.99.1	6~4リレーサーバーを入力してください。デフォルト アドレスは192.88.99.1です。

- 3. [6~4]トンネルの [有効] 選択します。
- 4. インターフェースを選択します。このインターフェースは、IPv4 アドレスを使用す るパブリック WAN の必要があります。6 to 4 トンネルはこのインターフェース上 に作成されます。

5. [詳細] セクションの [サーバーアドレス] を入力します。このオプションにより、 リレーサーバーを設定できます。リレーサーバーを指定することも、デフォルトの 192.88.99.1 を使用することもできます。

# インターフェース

インターフェースは、Terminator 上の物理および仮想ポートです。インターフェース の数は、Terminator のモデルによって異なります。[インターフェース] ページでは、 インターフェース、エイリアス、VLAN、ブリッジの追加、編集、削除が行えます。また は、インターフェースをデフォルトに設定することもできます。

Terminator では、LAN、WAN、DMZ の 3 つのゾーンがサポートされています。各インタ ーフェースは、これらの領域の 1 つに設定する必要があります。

#### ゾーン

LAN:企業の社内ネットワークです。Terminator では、社内ネットワーク用に設定されているインターフェースを、LAN ゾーンの一部として割り当てることができます。

WAN: 社外のネットワーク、すなわちインターネットです。Terminator では、社外ネットワーク用に設定されているインターフェースを、WAN ゾーンの一部として割り当てる ことができます。

DMZ: 中立ゾーン (DMZ) は、信頼できる社内ネットワーク、例えば企業のプライベート LAN と、インターネットなど信頼できない社外ネットワークとの間に配置される小さな サブネットワークです。社内ネットワークに、ウェブサーバーやメールサーバーなど、 信頼できないネットワークやインターネットからアクセスされるサーバーが存在する場 合、これらのサーバーは DMZ ゾーンに配置します。

デフォルトでは、LAN 領域から WAN 領域へ、HTTP、HTTPS、SMTP、POP3、SSH などのト ラフィックが許可されています。領域間トラフィックはすべてブロックされます。

## インターフェースの設定

インターフェースページには、初期状態ですべてのデフォルトインターフェースのリス トが表示されています。これらのインターフェースは、Terminator アプライアンス上 のポートです。デフォルトポートの下に追加されたエイリアスと VLAN インターフェー スは、インターフェースのリストで、ベースインターフェースのサブインターフェース として表示されます。 インターフェースの状態を示すために、次の表に示すカラーが使用されます。

アイコ ン	説明
	イーサネットケーブルが接続されています。
	イーサネットケーブルが接続されており、インターネットが利用可能です。
	イーサネットケーブルがすべてのスレーブに接続されていません。インター ネットは利用可能です(リンクアグリゲーション)。
	イーサネットケーブルがすべてのスレーブに接続されていません(リンクア グリゲーション)。
	イーサネットケーブルが接続されていません。

物理インターフェースを設定するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [インターフェース] ヘログオンします。インタ ーフェースのリストが表示されます。

Searite			🔅 オブシ	/ョン -   <b>?</b> ヘル	ブー   🕛 シャッ	トダウンする -	│ 🔁 Admin (管理	里) -
TERMINATOR		ホーム	コンテンツ	/フィルタリング	ユーザー管	理 設定	ログとレポー	·ŀ
> インターネット	インターフェ	ース					追加 削隊	<del>ہ</del>
▶ アンチウイルス	▶ 名前	ゾーン	ステータス	IPアドレス	ゲートウェイ	IP割り当て	デフォルトルー	ŀ
▶ 電子メール保護	🗌 eth0	LAN	オン	192.168.173.1		静的		۰.
> 定義	🔲 eth1	WAN	オン	10.10.104.167	10.10.104.1	静的	デフォルト	
> ファイアウォール設定	eth2							$\square$
> IPS	eth3							$\hat{\Box}$
> アブリケーションコントロール	eth4							$\square$
➤ 証明書	🗌 eth5							$\cap$
> IPSec VPN								

2. リストのインターフェース名をクリックします。次のページが表示されます。

Seqrite TERMINATOR	木-	☆ オブション -   ? ヘルブ -   ひ シャ ム コンテンツフィルタリング ユーザー <sup>3</sup>	ットダウンする -   - Admin (管理) - 管理 設定 ログとレポート
> インターネット	インターフェース	→ 編集 eth0	保存 キャンセル
> アンチウイルス	インタフェース名	eth0	
<ul> <li>電子メール保護</li> </ul>	ゾーン	IAN OWAN ODMZ	
> 定義	IP割り当て	⑧ 静的	
> ファイアウォール設定	IPv4アドレス	192.168.173.1	
> IPS	サブネットマスク	255.255.255.0	
> アプリケーションコントロール	IPv4ゲートウェイ	WANインターフェイスはIPv4に構成され	
> 証明書	ハードウェアアドレス	00:0B:AB:63:FE:1B	

このページのフィールドの説明を、次の表に示します:

フィールド	説明
インターフェー ス名	インターフェースの名前を設定します。
ゾーン	[LAN]、[WAN]、[DMZ] のいずれかを選択します。
IP 割り当て	[スタティック]、[ダイヤルアップ]、[DHCP] のいずれかを選択し ます。 i. IP 割り当てとして [スタティック] を選択した場合、
	[IPv4 アドレス] と [サブネットマスク] を入力する必要 があります。
	ii.IP 割り当てとして [ダイヤルアップ] を選択した場合、 ISP から提供される [ユーザー名] と [パスワード] を入 力する必要があります。
IPv4 アドレス	このフィールドは、IP 割り当てとして [スタティック] を選択し たときに表示されます。Seqrite Terminator の IPv4 アドレスを 設定します。すべてのクライアントは、そのアドレスを使用して インターネットへアクセスします。
サブネットマス ク	このフィールドは、IP 割り当てとして [スタティック] を選択し たときに表示されます。適切なサブネットマスクを選択します。
IPv4 ゲートウェ イ	このフィールドは、IP 割り当てとして [スタティック] を選択し たときに表示されます。Seqrite Terminator がルーターの背後に 存在する場合、ゲートウェイを設定します。

ネットワーク設定

フィールド	説明
	注意:WAN インターフェースにゲートウェイが設定されている場 合、LAN インターフェースにはゲートウェイを設定できません。
IPv6 アドレス	このフィールドは、IPv6 が有効なときに表示されます。詳細につ いては、 <u>IPv6</u> を参照してください。 IPv6 アドレスを入力します。すべてのクライアントは、そのアド レスを使用してインターネットへアクセスします。
プレフィックス	このフィールドは、IPv6 が有効なときに表示されます。詳細につ いては、 <u>IPv6</u> を参照してください。 プレフィックスを入力します。
IPv6 ゲートウェ イ	このフィールドは、IPv6 が有効なときに表示されます。詳細につ いては、 <u>IPv6</u> を参照してください。 IPv6 ゲートウェイを入力します。
ユーザー名	このフィールドは、IP 割り当てとして [ダイヤルアップ] を選択 したときに表示されます。ISP から提供されたユーザー名を入力 します。
パスワード	このフィールドは、IP 割り当てとして [ダイヤルアップ] を選択 したときに表示されます。ISP から提供されるパスワードを入力 します。
サービス名	このフィールドは、IP 割り当てとして [ダイヤルアップ] を選択 したときに表示されます。ISP から提供されたサービス名を入力 します。

3. [保存] をクリックします。

## インターフェースの削除

インターフェースを削除するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [インターフェース] ヘログオンします。インタ ーフェースのリストが表示されます。
- 2. 削除するインターフェースを選択し、[削除] をクリックします。確認メッセージが 表示されます。
- [OK] をクリックして、インターフェースの削除を確認します。
   注意:インターフェース eth0 は削除できません。インターフェースを削除しても、 設定がクリアされるだけで、ポートは依然としてリストに表示されます。

## エイリアスの追加

インターフェースにエイリアスを追加すると、単一のインターフェースやポートに複数 の IP アドレスを設定できます。エイリアスの追加機能により、ベースインターフェー スに別の ID を与えることができます。ベースインターフェースのゾーンは、エイリア スのゾーンと同じです。

エイリアスを追加するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [インターフェース] ヘログオンします。インタ ーフェースの詳細ページが表示されます。
- 2. [追加] をクリックします。次のページが表示されます。
- 3. インターフェースの [**タイプ**] として [エイリアス] を選択します。

インターフェース >・	保存 キャンセル		
タイプ	別名	¥	
別名ID			
ベースインターフェース	eth0 (eth0)	•	
IPv4アドレス			
サブネットマスク	255.255.0.0	•	
IPv4ゲートウェイ	ゲートウェイは既に設定されています。		

- 4. 次の詳細情報を入力します。
- i. エイリアス Id:エイリアスを識別するため使用される固有の番号です。
- ii. **[ベースインターフェース]**を選択します。設定済みのインターフェースのみを 使用できます。
- iii. [IPv4] IP アドレスを入力します。

- iv. [サブネットマスク] を入力します。
- v. [IPv4 ゲートウェイ] アドレスを入力します。
- 5. [保存] をクリックします。

**注意**:エイリアスインターフェースは、ベースインターフェースのサブインターフ ェースとしてインターフェースリストに表示されます。

▶ 名前	ゾーン	ステータス	IPアドレス	ゲートウェイ	IP割り当て	デフォルトルート
	LAN	オンオフ	192.168.171.1		静的	
□ 別名 2		オン	192.168.45.1		静的	
▼ 🔲 eth1	WAN	オン	10.10.104.167	10.10.104.1	静的	デフォルト 💧
VLAN 22	LAN	オン	192.168.55.1		静的	
🔲 ブリッジ 23		オン	10.10.17.45	10.10.17.1	静的	デフォルト
🔲 bond0	LAN	オン	172.16.10.5		静的	

## USB モデム

ユニバーサルシリアルバス (USB) のワイヤレスモデムを使用すると、コンピュータを 携帯データネットワーク経由でインターネットへワイヤレス接続できます。WAN リンク が停止した場合、この機能を使用してインターネットへアクセスできます。USB を接続 してモデムをスキャンする必要があります。USB 設定はリセットすることもできます。

### USB モデムの設定

USB モデルを設定するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [USB モデム] ヘログオンします。[USB モデム] ページが表示され、[モデムのスキャン] ボタンと [設定のリセット] ボタンが表示されます。

Seqrite <b>TERMINATOR</b>	木	🌞 オブション -   ? イ ム コンテンツフィルタリング	<b>ルブ -   ()</b> シャット ユーザー管理	- <b>ダウン -   ┣ Admin (管)</b> 設定 ログとレポー	<b>里) ▼</b> -ト
> インターネット	USBモデム			構成をリセット	
<ul> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> </ul>		USBモデムをスキャンするための" ムをスキャンするに数秒かかりま <sup>-</sup>	スキャンモデム"ボタン す。	をクリックしてください。USBF	Eデ
<ul> <li>&gt; 定義</li> <li>&gt; ファイアウォール設定</li> </ul>		スキャンモデム			

2. **[モデムのスキャン]** をクリックします。Terminator により USB モデムのスキャンと検出が行われ、設定オプションが表示されます。

USBモデム			構成をリセット
	USBモデム		
	USBモデムが見つかり	しました	
	電話番号:	#777	
	ユーザー名:	internet	
	パスワード:	•••••	
		提出する	

3. 以下の詳細を入力し、[送信] をクリックします:

フィールド	説明
電話番号	USB モデムでダイアルして ISP に接続する番号です。
	以下は、一部のネットワークの電話番号です。
	GSM/W-CDMA -*99#
	CDMA - #777
	LTE - *99#
ユーザー名	USB モデムに ISP から提供されたユーザー名を入力します。
パスワード	USB モデムに ISP から提供されたパスワードを入力します。

4. [送信] をクリックすると、USB が接続され、検出されたモデムの詳細が表示され ます:

USBモデム			構成をリセット
	検出されたUSBモデム		
	IPアドレス:	14.97.80.186	
6.0	ゲートウェイ:	172.29.145.65	
	DNSアドレス:	103.8.44.5	
	DNSアドレス:	103.8.45.5	
	USBモデムは正常に接	続しました。	
	デフォルトルート	接続を切断しま	

- 5. 必要なら、次のオプションを使用できます:
  - 検出された USB モデムをデフォルトルートとして設定する。
  - USB を切断する。
  - USB の設定をリセットする。

注意:USB モデムが認識されない場合、ドライバのインストールが必要な可能性があり ます。ベンダーでドライバのアップデートが配布されているどうか確認してください。 USB モデムを初めて有効化するときは、サポートサービスへの連絡が必要な場合があり ます。

WAN リンクが停止しており、USB モデムが接続されている場合、USB モデムが自動的に デフォルトルートに設定されます。

## DNS

ドメインネームサーバー (DNS) はドメイン名をインターネットプロトコル (IP) アド レスへ変換し、コンピュータはネットワーク上で他のコンピュータを識別するためにそ のアドレスを使用します。ドメイン名はアルファベットで表現されるため、人間にとっ て覚えやすい名前です。しかし、インターネットは IP アドレスを基盤としています。 ユーザーがドメイン名を入力するごとに、そのドメイン名は DNS サービスによって、 対応する IP アドレスへ変換されます。DNS サーバーがあるため、ユーザーは IP アド レスのアドレス帳を独自に保有する必要がありません。その代わりに、ドメインネーム サーバー (DNS サーバーとも呼ばれます) 経由で接続すれば、DNS サーバーの保有して いる膨大なデータベースにより、ドメイン名が IP アドレスへマップされます。このプ ロセスは DNS の名前解決と呼ばれます。DNS サーバーがドメイン名を IP アドレスへ と解決するためです。例えば、ユーザーがブラウザでドメイン名 www.example.com を 入力すると、DNS サーバーはそのドメイン名を IP アドレス、例えば 205.105.232.4 に解決します。 特定のドメイン名の IP アドレスが DNS サーバーに存在しない場合、その DNS サーバーはさらに別の DNS サーバーへ要求を送信します。この手順は、正しい IP アドレスが返されるまで続けられます。

Seqrite Terminator の DNS 機能により、デフォルトのドメインネームサーバー設定を オーバーライドして、ISP から提供された DNS の詳細を入力する、または特定の DNS を使用すると指定することができます。DNS の優先順位も変更できます。この機能によ り、Seqrite Terminator は普段使用している DNS サーバーが利用不能な場合に、別の サーバーの使用を試みることができます。

Seqrite Terminator では、次のタイプの DNS 設定がサポートされています:

- スタティック DNS
- ダイナミック DNS

グローバル DNS サーバー

グローバル DNS サーバーの設定を使用して、ISP から提供された DNS の IP アドレス を追加できます。IPv4 または IPv6 のどちらの IP アドレスも追加できます。IPv4 規 格の IP アドレスは 4 つの数値で、「70.74.251.42」のように 3 つのドットで区切っ て表現されます。IPv6 規格の IP アドレスは 8 つの 16 進数 (base-16) で、次のよ うにコロンで区切って表現されます:

2001:0cb8:85a3:0000:0000:8a2e:0370:7334

注意:IPv6 DNS は、Seqrite Terminator の IPv6 機能を有効にしている場合のみ追加 できます。IPv6 機能の詳細については、IPv6 を参照してください。

デフォルトでは、IP アドレス 8.8.8.8 の DNS が使用されます。

#### グローバル DNS サーバーの追加

グローバル DNS サーバーを追加するには、以下の手順に従います:

1. [Seqrite Terminator] > [設定] > [DNS] ヘログオンします。DNS サーバーのリストが含まれる [DNS の設定] ページが表示されます。

Searite	🌞 オブション -   🥐 ヘルブ -   🕐 シャットダウン -   🖶 Admin (管理) -
TERMINATOR	ホーム コンテンツフィルタリング ユーザー管理 設定 ログとレポート
> インターネット	グローバル         スタティックDNS
▶ アンチウイルス	保存
▶ 電子メール保護	追加 削除  優先度を変更 🔳 🎓
<b>&gt;</b> 定義	□ DNS 名
> ファイアウォール設定	10.10.124.10
> IPS	8.8.8.8
▶ アプリケーションコントロール	
▶ 証明書	•
> IPSec VPN	
> PPTP VPN	ノブツン ユUNS + やツン ユ
> SSL VPN	DNSサーバー: TTLの有効期限が切れるまではDNSは記録されます。TTLの有効 期限が切れる前にDNSキャッシュをクリアにするには、このボタンを
> インターフェース	クリックします。
> IPv6	
▶ ルーティング	
DNS >	

2. [追加] をクリックします。DNS の IP アドレスを、該当のテキストボックスに入力 し、[追加] をクリックします。

#### グローバル DNS サーバーの削除

グローバル DNS サーバーを削除するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [DNS] ヘログオンします。[DNS の設定] ページ に、DNS サーバーのリストが表示されます。
- 2. 削除するサーバーを選択し、[削除] をクリックします。複数のサーバーを選択して、 同時に削除することもできます。

#### 優先度の変更

リストに表示されている DNS サーバーの優先度を変更できます。優先度を変更すると、 IP アドレスを調べるため DNS サーバーを検索する順序が変更されます。最も上に表示 されている DNS サーバーが最も優先度が高く、下端の DNS サーバーは最も優先度が低 くなります。つまり、IP アドレスを調べるとき、リストの最初の DNS サーバーが最初 に検索されます。

DNS サーバーの優先度を変更するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [DNS] ヘログオンします。[DNS の設定] ページ に、DNS サーバーのリストが表示されます。
- 2. 目的の DNS サーバーを選択し、矢印ボタンをクリックして、変更する優先度に応じ てその DNS サーバー名を上または下へ移動します。

#### DNS キャッシュを削除

DNS は、IP アドレスのレコードを一時的に保存するためにキャッシュを使用します。 これらの各レコードには有効期間(TTL:Time-To-Live)が存在し、有効期間が満了する とレコードは削除されます。キャッシュの削除オプションを使用すると、TTL の満了を 待たずに、DNS レコードに加えられた最新の変更をただちに有効にするため、必要に応 じてキャッシュを手動で空にできます。

DNS サーバーを空にするには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [DNS] ヘログオンします。[DNS の設定] ページ に、DNS サーバーのリストが表示されます。
- 2. [キャッシュの削除] をクリックします。キャッシュがフラッシュされ、キャッシュ の内容が削除されます。

## スタティック DNS

ホストの IP アドレスが判明している場合、Terminator にホストのスタティック DNS エントリを追加できます。このホストにアクセスするときは常に、Terminator は追加 された IP アドレスへ解決して返します。

スタティック DNS の追加や削除は、[スタティック DNS] セクションで行います。

#### スタティック DNS エントリの追加

スタティック DNS エントリを追加するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [DNS] ヘログオンします。[DNS の設定] ページ に、DNS サーバーのリストが表示されます。デフォルトではグローバル DNS リスト が表示されます。
- 2. 右上にある [スタティック DNS] をクリックし、[スタティック DNS] ページを表示 します。

Seqrite TERMINATOR	7	<b>е</b> ::	オブション ↓   <b>?</b> ヘルコ ンテンツフィルタリング	<sup>す</sup> -   <b>()</b> シャット ユーザー管	ダウンする →   理 設定	► Admin (管理) -
> インターネット	DNS設定				グローバル	スタティックDNS
> アンチウイルス						保存
▶ 電子メール保護						追加   削除
▶ 定義	□ ホスト名		IPv4アドレス			
> ファイアウォール設定	ホスト名を入力して	ください	IPv4アドレスを入力してくださ	11 追加		×
> IPS						<u>^</u>
▶ アプリケーションコントロール						

3. [追加] をクリックして、新しい DNS エントリを追加します。[ホスト名] ボックス と、[IPv4 アドレス] または [IPv6 アドレス] ボックスに値を入力します。 4. [保存] をクリックします。

#### スタティック DNS エントリの削除

スタティック DNS エントリを削除するには、以下の手順に従います:

- 1. 左側のフレームで、[Seqrite Terminator] > [設定] > [DNS] ヘログオンします。 [DNS の設定] ページに、DNS サーバーのリストが表示されます。デフォルトではグ ローバル DNS リストが表示されます。
- 2. 右上にある [スタティック DNS] をクリックし、[スタティック DNS] ページを表示 します。削除するホストを選択し、[削除] をクリックします。複数のスタティック DNS ホストを選択して、同時に削除することもできます。

## ダイナミック DNS

ダイナミックドメインネームシステム (DDNS) を使用すると、ドメイン名を可変の IP アドレスとリンクできます。このサービスは、Dyndns などの DDNS サービスプロバイ ダによって提供されます。DDNS サービスプロバイダは指定された間隔で DNS サービス と通信を行って IP アドレスの変更を確認し、IP アドレスの変更を反映するため DNS データベースを更新します。この方法によって、ドメイン名の IP アドレスが ISP に よって変更されても、ドメインへアクセスするために変更された IP アドレスを記憶す る必要はありません。

Terminator のダイナミック DNS 機能により、DDNS サービスプロバイダから購入した DDNS アカウントを設定して、WAN インターフェースにバインドできます。

Terminator で DDNS を設定するには、以下の手順に従います:

1. [Seqrite Terminator] > [設定] > [ダイナミック DNS] ヘログオンします。次に示 す画面が表示されます。

Segrite TERMINATOR	+-4	☆ オブション -   ? ^	ヽルブ マ   😃 シャットダウン マ	<mark>┣</mark> Admin (管理) ▼
<ul><li>&gt; インターネット</li></ul>	ダイナミックDNS			保存
> アンチウイルス	ダイナミックDNS:	◎ 有劾   ● 無効		
▶ 電子メール保護	サービスプロバイダー:	ChangelP	•	
<b>&gt;</b> 定義	ホスト名:		(例: abc.dynamicdns.com	)
▶ ファイアウォール設定	ログインユーザー ID:			
> IPS	パスワード:			
> アプリケーションコントロール	WANインターフェイス:	EXT-1: 10.10.104.166	•	
> 証明書	IPアップデート間隔:	30 ▼ 分(最大2時間)		

- 2. [ダイナミック DNS] が [有効] に設定されていることを確認してください。
- 3. [ホスト名]を入力して[ドメイン]を選択します。ドメイン名は、Dynamic DNS サー ビスプロバイダーから提供されます。

- 4. DDNS アカウントの [ログインユーザー ID] と [パスワード] を入力します。
- 5. **[WAN インターフェース]** を選択します。これらは、[インターフェース] セクショ ンで設定した WAN インターフェースです(詳細については、<mark>インターフェース</mark>を参 照してください)。
- 6. **[IP のアップデート間隔]** を分単位で選択します。Terminator は設定された時間の 経過後に DNS を再同期し、IP アドレスに変更が加えられたかどうかをチェックし て、アップデートを行います。
- 7. [保存] をクリックします。

### DHCP

ダイナミックホストコンフィギュレーションプロトコル (DHCP) を使用すると、DHCP サーバーからデバイスにネットワークパラメータを自動的に割り当てることができます。 DHCP サーバー機能は、新しいマシンを簡単にネットワークへ追加できるため便利です。

Seqrite Terminator はネットワークの DHCP サーバーとして動作し、IT 環境で IP ア ドレスを動的に割り当てます。DHCP サーバーを使用すると、IP アドレスが動的に割り 当てられるため、IP アドレス競合の可能性も減らすことができます。

#### DHCP サーバーの追加

DHCP サーバーを追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [DHCP] ヘログオンします。

Seqrite <b>TERMINATOR</b>		ホームコン	🌞 オブション -   <b>?</b> ^ ノテンツフィルタリング	<b>ヘルブ -   () シ</b> + ユーザー管理	<del>//ットダウン -  </del> 昆 設定	➡ Admin (管理) <del>-</del> ログとレポート
> インターネット	DHCP				ţ	ナーバー リース
<ul> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> </ul>	DHCP サーバー	◎ 有効	◉ 無効			保存
▶ 定義	<ul> <li>DHCP ワーパーク</li> <li>サーバー名</li> </ul>	ルスト 開始IP	終了IP	ゲートウェイ	DNS	「戸川」 「別所 ステータス
> ファイアウォール設定	LAN1	192.165.4.11	192.165.4.13	192.165.4.1	192.165.4.1	オン
> IPS	LAN2	192.168.41.12	192.168.41.15	192.168.41.1	192.168.41.1	オン
▶ アプリケーションコントロール	LAN3	172.16.5.14	172.16.5.17	172.16.5.1	172.16.5.1	オン
> 証明書	LAN4	165.145.45.15	165.145.45.18	165.145.45.1	165.145.45.1	オン

- 2. [有効] オプションを選択します。
- 3. [追加] をクリックします。DHCP の追加 画面が表示されます。

DHCP > 編集		保存 キャンセル
サーバー名:	GUEST_machines	
IPバージョン:	IPv4 IPv6	
インターフェース:	eth0 -	
開始IP:	192.168.173.60	
終了IP:	192.168.173.70	
サブネットマスク:	255.255.255.0	
ゲートウェイ:	192.168.173.1	
推奨DNSサーバー:	192.168.173.1	
代替DNSサーバー:		
最小リース時間:	30 分(5分以上の必要があります)	
最大リース時間:	120 分(1440年分を超えないこと)	

このページのフィールドの説明を、次の表に示します。

フィールド	説明
サーバー名	識別のために設定するサーバーの名前。
IP バージョン	ここで IPv4 または IPv6 を選択できます。IPv4 を選択する と DHCPv4 が設定され、特定範囲の IP がクライアントに割 り当てられます。IPv6 を選択すると DHCPv6 が設定され、特 定範囲の IP がクライアントに割り当てられます。
インターフェース	DHCP サーバーが実行されている LAN インターフェース。デ フォルトでは EthO に設定されています。
開始 IP	DHCP の IP アドレス範囲の開始。この IP アドレスは、Eth0 が設定されているのと同じネットワークに存在する必要があ ります。
終了 IP	DHCP の IP アドレス範囲の終了。この IP アドレスは、Eth0 が設定されているのと同じネットワークに存在する必要があ り、Terminator の Eth0 の IP アドレスをこの範囲内に置く ことはできません。
サブネットマスク	クライアントに設定するサブネットマスク。

ネットワーク設定

フィールド	説明
Gateway	デフォルトゲートウェイとしてクライアントに設定されるゲ ートウェイを設定します。デフォルトは Terminator の EthO の IP アドレスです。
優先 DNS サーバー	クライアントへの優先 DNS として設定される DNS。
代替 DNS サーバー	クライアントへのセカンダリ DNS として設定される DNS。
最小リース時間	クライアントがリースの更新を要求するまでのリース時間。
最大リース時間	クライアントから応答がない場合、DHCP サーバーが IP アド レスを解放するまでのリース時間。
リース期間	制限付きまたは制限なしのリース期間を選択できます。制限 付きリース期間を選択すると、以下のオプションが表示され ます。
	最小リース期間: クライアントがリースの更新を要求するリー ス期間。
	最大リース期間: クライアントから応答がない場合に DHCP サ ーバーが解放されるリース期間。

### 4. [保存] をクリックします。

## スタティックリースの追加

スタティックリースを追加すると、IP アドレスを、ユーザーのコンピュータの MAC ア ドレスとバインドし、他の IP アドレスが空いているかどうかに関係なく、設定された IP のみがクライアントへリースされるようにできます。

スタティックリースを追加するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [DHCP] ヘログオンします。
- 2. [スタティックリース] セクションで [追加] をクリックします。

		追加	削除
ホスト名	IPv4アドレス		
		保存	×
			*
			-
	ホスト名	ホスト名 IPv4アドレス	追加 ホスト名 IPv4アドレス 保存

- 3. 次の詳細情報を入力します。
  - i. MAC アドレス:IP アドレスがバインドされるコンピュータの MAC アドレス を設定します。クライアントの MAC アドレスを取得するには、Windows クラ イアントではコマンド "ipconfig /all" を、Linux クライアントでは "ifconfig" を使用します。
  - ii. **ホスト名**:クライアントのホスト名を設定します。
  - iii. IPv4 アドレス:バインドする IPv4 アドレスを設定します。この IP アドレ スが、ユーザーのコンピュータへ割り当てられます。
- 4. [保存] をクリックします。

### DHCP サーバーの削除

DHCP サーバーを削除するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [DHCP] ヘログオンします。DHCP サーバーのリ ストが、サーバー名、開始 IP アドレス、終了 IP アドレス、ゲートウェイ IP ア ドレス、DNS、ステータスボタン付きで表示されます。
- 2. 目的の DNS サーバーを選択し、[削除] をクリックします。

### DHCP リースリストの表示

DHCP 対応のクライアントは、DHCP サーバーから IP アドレスのリースを取得します。 リース期間が満了する前に、DHCP サーバーがクライアントのリースを更新するか、ク ライアントが新しいリースを取得する必要があります。リースは期間の満了後約 1 日 間、DHCP サーバーのデータベースに保持されます。この猶予期間により、クライアン トとサーバーが異なるタイムゾーンに属している、互いの内部クロックが同期していな い、またはリース期間の満了時にクライアントがネットワークに接続していない場合に、 クライアントのリースを保護します。

- DHCP リースの詳細を表示するには、以下の手順に従います:
- 1. Seqrite [Terminator] > [設定] > [DHCP] ヘログオンします。

2. [リース] をクリックします。リースのリストが、IP アドレス、リースの開始時刻、 終了時刻、物理アドレス、ホスト名を含めて表示されます。

Seqrite TERMINATOR		<b>☆ オブ</b> シ ホーム コンデ	<b>/ョン -   ? ヘルブ -</b> ンツフィルタリング	<b>()</b> シャットダウンフ ユーザー管理	する   - ● Admin (管理)
<ul> <li>&gt; インターネット</li> <li>&gt; アンチウイルス</li> </ul>	DHCP DHCP リースリス	\ <b>ŀ</b>			サーバー リース 最新の情報に更新
<ul> <li>電子メール保護</li> </ul>	IPアドレス	開始時刻	終了時刻	物理アドレス	ホスト名
> 完業	192.168.201.1	Tue Mar 17 16:07:35 2	Tue Mar 17 16:09:35 2	fc:aa:14:36:fb:14	Client PC1 ^
<ul> <li>アレイアウォール設定</li> </ul>	192.168.201.10	Thu Mar 12 18:06:01 2	. Thu Mar 12 18:36:01 2	fc:aa:14:8e:db:9f	Client PC2
> IPS	192.168.201	Thu Mar 19 17:41:05 2	. Thu Mar 19 18:11:05 2	94:eb:cd:86:d2:06	Client PC3
<ul> <li>アプリケーションコントロール</li> </ul>	192.168.201.11	Sun Mar 22 17:44:46 2	. Sun Mar 22 18:14:46 2	5c:f3:fc:29:a5:38	Client PC4
• FToR do	192.168.201.12	Wed Mar 18 17:06:58	Wed Mar 18 17:08:58	00:0c:29:7c:95:13	Client PC5
> 証明音					
> オンターフェース					*

3. リストを更新するには、[更新]をクリックします。

# ルーティング

ルーティングは、コンピュータからネットワークを経由して、別のコンピュータへデー タパケットを移動するプロセスです。ルーティングにより、パケットを送信元から宛先 へ送信するための最適なネットワークのパスを選択できます。ルーティングはルーター と呼ばれる専用のデバイスで行われ、手動で設定されるルートテーブルのエントリに記 載されているルート情報、またはダイナミックルーティングアルゴリズムを使用して計 算されるルート情報を使用して、パケットが転送されます。

Segrite Terminator では、次の2タイプのルーティングを設定できます。

- <u>スタティックルーティング</u>
- ポリシーに基づいたルーティング (PBR)

## スタティックルーティング

スタティックルーティングは、2 つのルーター間に明示的なパスを定義するために使用 され、このパスは自動的には更新されません。ネットワークに変更が発生したときは、 手動でスタティックルートを再設定する必要があります。

Terminator のスタティックルート機能により、パケットを特定の宛先へ転送するため に Terminator が使用可能なルートを設定できます。スタティックルートにより、設定 されているデフォルトゲートウェイ以外のゲートウェイを使用して、パケットが宛先へ 転送されます。Terminator を使用すると、ルートの追加や削除が可能です。ルートを OFF に設定すると、そのスタティックルートは、デバイスのルーティングテーブルから 削除されます。

### スタティックルートの追加

スタティックルートを追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [ルーティング] ヘログオンします。[スタティ ックルーティング] ページに、追加済みのルートのリストが表示されます。

Seqrite TERMINATOR		🔅 : ホーム コン	オ <b>ブション -   <b>?</b> ヘ /テンツフィルタリン</b>	ルブ →   <b>也</b> シャット グ ユーザー管	ダウンする   <b>      ●</b> A 「理   設定 ロク	dmin (管理) - びとレポート
<ul> <li>インターネット</li> <li>コン デキ・イリー</li> </ul>	ルーティング スタティックルー	-トリスト		スタティ	<b>ックルート</b> ポリシー	ベースルート 追加   削除
<ul> <li>アンナワイルス</li> <li>す 電子メール保護</li> </ul>	□ 名前	ステータス	ネットワ <i>ーク/</i> IP	ゲートウェイ	インターフェース	メトリック
<ul> <li>         ・ 定義         ・         ・         ファイアウォール設定         </li> </ul>	Route 1	オン	10.16.1.121		eth1	0
<ul> <li>▶ IPS</li> <li>▶ アプリケーションコントロール</li> </ul>						

2. [追加] をクリックして、ルートを追加します。[追加] をクリックすると、次のペ ージが表示されます。

スタティックルート	> 新規	保存	キャンセル
名前:			
ネットワーク/ IP:	≅   <b>+</b>   <b>0</b>		
ゲートウェイ:	≅   <b>+</b>   <b>0</b>		
インターフェース:	eth0 🔻		
□ 基本オプション			
አት リック:	0		

- 3. 新しいルートの [名前] を入力します。
- 4. [ネットワーク IP] フィールドを使用して、宛先/ターゲット IP を設定します。各 アイコンを使用して、ネットワーク定義の参照、追加、削除を行えます。
- 5. [ゲートウェイ] フィールドを使用して、ルートの次のホップを設定します。各アイ コンを使用して、ネットワーク定義の参照、追加、削除を行えます。
- 6. ルーティングテーブルの **[インターフェース]** を選択します。パケットはこのイン ターフェース経由で転送されます。
- 「詳細オプション」を使用して、「メトリック」オプションを設定できます。メトリックは、ルートのアドミニストレーティブディスタンスを記述します。スタティックルートのデフォルトのメトリックは1です。この値によって、ルーターはルーティングタイプの優先度を決定することができます。
- 8. [保存] をクリックします。

ポリシーに基づいたルーティング (PBR)

PBR を使用すると、トラフィックフローについて定義済みのポリシーに従い、パケット をルーティングできます。特定のパケットについて、最適のものとは異なるパスを経由 してルーティングする理由がある場合、PBR を使用できます。また、特定のトラフィッ クについてパスを指定し、企業ポリシーに基づいてパケットをルーティングすることも できます。例えば、特定のエンドシステムの ID、アプリケーションプロトコル、また はパケットのサイズに基づいてパスを許可または拒否するようなルーティングポリシー を実装できます。

Terminator の PBR 機能により、インターフェースについて定義済みの基準に従ってト ラフィックをルーティングするように設定するポリシーを作成できます。次の要素に基 づいてルーティングを設定できます。

- 送信元のタイプ
- 送信元のインターフェース
- サービスベース
- 宛先

Seqrite Terminator を通過するネットワークトラフィックが指定された基準を満たしている場合、トラフィックはターゲットのネットワークインターフェースのリンク、またはターゲットのゲートウェイを経由して転送されます。

PBR 基準には、送信元のネットワークインターフェース、送信元 IP アドレス/送信元 ネットワーク/ユーザー/グループ、サービス、時間カテゴリ、宛先ネットワークを組み 合わせて使用できます。このため、管理者は PBR を使用して、パケットの宛先 IP ア ドレス以外にも各種のフィルタに基づいてトラフィックを区別し、ネットワークトラフ ィックを詳細にコントロールできます。

### PBR の有効化

ポリシーに基づいたルーティングを有効にするには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [ルーティング] > [ポリシーに基づいたルート] ヘログオンします。

ル	ーティング	グ				スタティック	ブルート <b>ポリシー</b> /	ベースルート	-
PBR	ステータ	ג (	◉有劾 ◎ ;	無効				保存	
ポ	<b>ポリシーベースルートリスト</b> 追加   削除   順位を変更 <b>↑</b> ↓   保存								
	名前	ステー	ሥーት タ	送信元タイプ	送信元インター	サー	宛先ネットワーク	宛先	
	Loadb	オン	Interface	IP	eth0	ICMPv6	Any	eth1	*
									*
除	外							追加 肖	间除
	名前		ソース		サービス		宛先		
									*

- 2. [PBR ステータス]の [有効] を選択します。
- 3. [保存] をクリックします。

## ルーティングポリシーの追加

ルーティングポリシーを追加するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [ルーティング] > [ポリシーに基づいたルート] ヘログオンします。
- 2. [追加] をクリックします。次のページが表示されます。

1  ▼ ■ 名前	IPアドレス		
1 ▼ 2前	19アドレス		
名前	IPアドレス		
			~
	_		-
ユーザー			
🔲 ユーザー			⊞   8
			~
			*
	74F4// 75X8FF	90.55 小二下	E + ≣ ▲
			-
◎ インターフェー スルート	ト ── ゲートウェイルート		
🔲 名前	IPアドレス		:≡∣₿
			-
□カテゴリー名			:=  8
default			
🔲 名前	ホスト		= + + + =
Any			
	ユーザー         コーザー         関連するサービス         ③ インターフェースルート         名前         カテゴリー名         default         名前	<ul> <li>□ ユーザー</li> <li>□ コーザー</li> <li>□ 関連するサービス プロトコル ソースポート</li> <li>● インターフェースルート ● ゲートウェイルート</li> <li>□ 名前 IPアドレス</li> <li>□ カテゴリー名</li> <li>□ default</li> <li>■ 名前 ホスト</li> <li>■ Any</li> </ul>	<ul> <li>ユーザー</li> <li>■ コーザー</li> <li>■ 関連するサービス ブロトコル ソースボート 宛先ボート</li> <li>● インターフェースルート ● ゲートウェイルート</li> <li>■ 名前 IPアドレス</li> <li>■ カテゴリー名</li> <li>■ default</li> <li>■ 名前 ホスト:</li> <li>■ Any</li> </ul>

このページのフィールドの説明を、次の表に示します:

フィールド	説明
名前	ポリシーに基づいたルートのルールに、一意の名前を付けます。 ルールはこの名前によって識別されます。

フィールド	説明
順位	ポリシーベースルートの各ルールには、すべてのルール間におけ る順位があります。各ルールは、それぞれの順位に基づいて適用 されます。リストで最初の順位にあるルールが最初にネットワー クトラフィックに適用され、このルールが基準を満たす場合、ト ラフィックはルールの記述に従ってターゲットのネットワークイ ンターフェースへ転送されます。
	最初のルールが該当しない場合、その次のルールが適用されま す。このプロセスは、ポリシーに基づいたルーティングの最後の ルールに達するまで繰り返されます。
送信元のイン ターフェース	すべてのローカルネットワークインターフェース (LAN、DMZ、 LAN-LAN ネットワークブリッジインターフェース) はここに表示 されます。リストから、1 つまたは複数の送信元ネットワークイ ンターフェースを選択できます。パケットは、このインターフェ ースから送信されます。
送信元のタイ プ	ポリシーに基づいたルーティングルールは、ユーザー、グルー プ、IP アドレス、IP アドレスの範囲、ネットワーク定義に適用 できます。これらのタイプのうち、いずれかを選択します。
送信元	選択した送信元タイプに従ってリストが表示されます。送信元を 選択します。
サービス	このルールを適用するサービス定義を選択します。サービスは、 送信元ポート、宛先ポート、またはその両方に基づいて識別され ます(サービス定義の詳細については、を参照してください) <u>定義</u> (サービス定義の詳細については、定義を参照してください)。
ルートタイプ	ルートタイプは、インターフェースルートまたはゲートウェイル ートを使用できます。ネットワークインターフェースを経由して ネットワークトラフィックを転送する必要がある場合は、[インタ ーフェースルート] オプションを選択します。[インターフェース ルート] には、WAN インターフェースのみが一覧表示されます。 設定されているネットワークインターフェースのいずれかから到 達可能なゲートウェイ (IP アドレス) ヘネットワークトラフィッ クを転送する必要がある場合は、[ゲートウェイルート] を選択で きます。このリストには、ホストのみが表示されます。
ターゲット	ターゲットには、ネットワークインターフェースまたはルートタ イプに基づいたゲートウェイを使用できます。ターゲットがアク

フィールド	説明
	ティブでない場合、トラフィックはデフォルトのシステムルーテ ィング設定を経由して転送されます。選択されているルートタイ プに基づいて、リストが表示されます。
時間カテゴリ	ポリシーに基づいたルーティングルールを特定の時間について有 効にする場合、該当する時間カテゴリを選択します。[時間カテゴ リ]が選択されていない場合、デフォルトの時間カテゴリに設定 されます。
宛先ネットワ ーク	パケットが転送される宛先です。宛先ネットワークに基づいてト ラフィックを転送できます。選択されない場合、あらゆる宛先ネ ットワークが検討されます。ネットワーク定義のリストのみが表 示されます(ネットワーク定義の詳細については、定義を参照して ください)。

#### 3. [保存] をクリックします。

### ルーティングポリシーの削除

- ルーティングポリシーを削除するには、以下の手順に従います:
- 1. Seqrite [Terminator] > [設定] > [ルーティング] ヘログオンします。
- 2. 削除するポリシーを選択して、[削除] をクリックします。
- 3. 確認を求めるボックスで、[OK] をクリックします。ポリシーが削除されます。

### ポリシーの優先順位の変更

ポリシーの優先順位を変更するには、以下の手順に従います。

- 1. [Terminator] > [設定] > [ルーティング] ヘログオンします。
- 2. 優先順位を変更するポリシーを選択し、[優先順位の変更]の矢印をクリックして、 必要に応じて上または下へ移動して優先順位を変更します。
- 3. [保存] をクリックします。

### PBR への除外の追加

PBR リストページの [除外] セクションを使用して、ポリシーに基づいたルーティング ルールからネットワークトラフィックを除外できます。このネットワークトラフィック について、ポリシーに基づいたルートの除外基準を追加できます。

PBR からインターフェースを除外するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [ルーティング] > [ポリシーに基づいたルート]  $\sim \mu \sigma J \rightarrow \nu \sigma J$  2. [除外] セクションの下にある [追加] リンクをクリックします。

除外⇒追加		保存	キャンセル
名前:			
ソース:	□ 関連するアドレス ホスト		≘ + ₿
			<u>^</u>
_	_		$\sim$
サービス:	□ 関連するサービス プロトコル ソースポート	宛先ボート	≘ + ₿
			^
扇牛.			~
967 <b>6</b> .	└		= + =
			~

3. その除外について、固有の[名前]を入力します。

- 4. 画面のアイコンを使用して**送信元の定義**を選択し、定義の参照、追加、削除を行い ます。
- 5. 画面のアイコンを使用して、送信元の定義を選択します。
- 6. **宛先のネットワーク**を選択します。
- 7. [保存] をクリックします。

# 負荷分散とフェールオーバー

負荷分散は、インターネット接続が複数存在する場合に、インターネットトラフィック を分散するために使用します。インターネット接続に重み付けを設定すると、該当する WAN インターフェースを通過するトラフィックの量を記述するために役立ちます。重み 付けが高くなるほど、その WAN インターフェースで多くのトラフィックの通過が許さ れるようになります。また、WAN インターフェースに優先順位を設定することもできま す。ネットワーク接続の確立に、どのインターフェースを最初に使用するかが、この優 先順位により定義されます。表の最も上にあるインターフェースが、最も優先順位が高 くなります。これにより、負荷分散はすべてのリンクを最適に活用し、ネットワークト ラフィックを分散して、いずれかのリンクに過剰な負荷を負わせることなしに、ユーザ ーへ優れたパフォーマンスを提供するために役立ちます。 Terminator ではフェールオーバー機能も提供され、リンクのいずれかが停止または利 用不能になった場合は、アクティブな他のリンクへトラフィックを転送できます。これ によって、ユーザーは中断なしにインターネットへの接続を使用できるようになります。 注意:負荷分散オプションが有効な場合、デフォルトインターフェースは設定されませ ん。

負荷分散を設定するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [負荷分散] ヘログオンします。[負荷分散] 画 面に、インターネットへ接続されている設定済みインターフェースのリストが表示 されます。

Seqrite <b>TERMINATOR</b>		ホーム	🌞 オプション -   <b>?</b> ^	ヽ <b>ルブ -   ()</b> シャットダウ: ユーザー管理 設	ン -   - Admin (管理) - 定 ログとレボート
> インターネット	ロードバラン:	シング			変更を適応
> アンチウイルス					優先度を変更 🚹 🖡
▶ 電子メール保護	接続名		インターフェース	ኃェイኑ	
	🔲 🥝 eth 1		EXT-1	3 -	編集
> ファイアウォール設定	🔲 🥝 Airtel		EXT-1	1 👻	編集
> IPS	🔲 😣 Tata		EXT-1	1 💌	編集
> アプリケーションコントロール					

- 2. インターフェースを選択し、[編集]をクリックします。
- 3. 各インターフェースについて、[重み付け]の値を選択します。

注意:重み付けが設定されていない場合、負荷はすべての接続に均等に分割されます。 4. [保存]をクリックします。

注意:必要に応じて、[優先順位の変更]ボタンを使用して優先順位を変更できます。

ファイアウォール

ファイアウォールはネットワークセキュリティシステムで、設定されているルールに基 づいて受信および送信ネットワークトラフィックをフィルタリングするために使用しま す。ファイアウォールは、信頼できるセキュアな内部ネットワークと、セキュアでなく 信頼できないとみなされる他のネットワーク(例: インターネット)との間に防壁を築 きます。インターネットへ送られる、またはインターネットから受け取られるパケット はすべてファイアウォールを通過し、パケットごとに検査され、指定されたセキュリテ ィ基準を満たさないものは特定の処置が取られます。

ファイアウォール機能を使用して、Terminator がプライベートネットワークから受信 または送信される情報にフィルタを適用するよう設定できます。Seqrite Terminator ファイアウォールは、ネットワークの各パケットを検査します。その後で、そのパケッ トを宛先へ転送するかどうかを判定します。ファイアウォールは、「すべて拒否してか ら、必要なもののみ許可する」という基本的なルールで動作するため、受信した要求が、 プライベートネットワークのリソースへ直接到達することはできません。Seqrite Terminator ファイアウォールでは、ゾーン、サービス、送信元、宛先アドレスに基づ くルールを作成できます。ゾーンは、セキュリティポリシーが適用される、ネットワー クインターフェースの論理グループです。各ルールは、設定されたアクションに基づい てアクセスを許可/拒否/ドロップします。

## デフォルトのファイアウォールルール

ファイアウォールの一部のゾーンで、デフォルトとして設定されなければならないルー ルがあります。デフォルトルールは Terminator に組み込まれています。[デフォルト ルール] ページには、Terminator に設定されているデフォルトルールのリストが表示 されます。

注意:デフォルトルールが最も優先順位が高く、次にカスタムルール、インターゾーンルールの順に優先されます。

デフォルトのファイアウォールルールを表示するには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [ファイウォールの設定] ヘログオンします。次 のページが表示されます。

Searite		🌞 オナ	ション・  🣍 ヘルフ	ゲート 🕛 シャットダウ	ン   🕞 Admin (管理)
TERMINATOR	*-	ムコンテンツフ	7ィルタリング コ	.ーザー管理 👌	定 ログとレボート
> インターネット	ファイアウォール	デフォルトのル	インターゾーン設定	カスタムのルー	IPボートフォワーディ
<ul> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> </ul>	デフォルトのルール	Q			ライブ接続 保存
> 定義	名前	ソースゾーン	サービス	宛先ゾーン	ステータス
ファイアウォール設定・・	HTTP プロキシ・ゲート	LAN		WAN	2
> IPS	HTTPSプロキシ - ゲー	LAN	-	WAN	2
> アプリケーションコントロール	メール保護 IMAP - ゲ	LAN	imap	WAN	2
> 証明書	メール保護 POP3 - ゲ	LAN	рор3	WAN	2
> IPSec VPN	メール保護 SMTP - ゲ	LAN	smtp	WAN	8
> PPTP VPN	DNSトラフィック - LAN	LAN	dns	UTM	2
> SSL VPN	HTTPトラフィック - LAN	LAN	http	UTM	
> インターフェース	HTTP ウェブ管理ボー	LAN	HTTP_WebAdmin	UTM	2
> IPv6	HTTP ウェブキャッシュ	LAN	http webcache	UTM	2

- 2. 表には、名前、ソースゾーン、サービス名、宛先ゾーン、およびデフォルトファイ アウォールルールのステータスが表示されます。
- 3. [ライブ接続] をクリックして、Terminator で確立された接続のリストを表示します。
- 4. プロトコル、または宛先ポート、またはその両方で接続にフィルタをかけることができま す。また、ソース/宛先 IP アドレスで接続を検索することもできます。

- 5. 確立した接続をドロップするよう選択することができます。[キャンセル] ボタンをクリック して、サービス設定をキャンセルします。
- 6. プロトコルまたは宛先ポート、もしくはその両方による接続にフィルターを設定す ることができます。送信元/宛先 IP アドレスでの接続を検索することもできます。
- 7. 確立された接続を中断するよう選択できます。[キャンセル] ボタンをクリックして サービス設定をキャンセルします。

## インターゾーン設定

インターゾーン設定ページでは、よく知られたグローバルファイアウォールポリシーを シングルクリックで設定できます。このページには、ファイアウォール設定のためのグ ローバルインターゾーン設定を示すマトリックスが表示されます。横の列はソースゾー ンを表し、縦の列は宛先ゾーンを表します。また、5 つのゾーン viz (LAN、WAN、DMZ、 VPN、および UTM) が事前に定義されています。交差するセルは、各ソースゾーンと宛 先ゾーンにペアで許可されるサービスの数を示しています。該当するセルをクリックし て、特定のゾーンの組み合わせでサービスを編集することもできます。

インターゾーン設定ページでグローバル設定をワンクリックすることで、良く知られた サービスを簡単に設定することができます。

グローバルファイアウォールルールを設定するには、以下の手順に従います:

1. Seqrite [Terminator ] > [設定] > [ファイアウォール] > [インターゾーン設定] ヘログオンします。次のページが表示されます。

### ネットワーク設定

				🛟 オプション 🗸	<b>?</b> ヘルプ -   也	シャットダウン -	➡ Admin (管理) -	
Segrite TERMINATOR			ホーム コンき	テンツフィルタリン	·グ ユーザー <sup>・</sup>	管理 設定	ログとレポート	
> インターネット	ファイ	アウォー	<b>ル</b> デフォルトの	)ル <b>インタージ</b>	<b>バーン設定</b> カスタ	ネムのルー IPボ	ートフォワーディ	
▶ アンチウイルス	インターゾーン設定							
▶ 電子メール保護					то			
> 定義			LAN	WAN	DMZ	VPN	UTM	
ファイアウォール設定 > > IPS		LAN	0 サービスを許可	1サービスを許可	0 サービスを許可	0 サービスを許可	1サービスを許可	
<ul> <li>&gt; アブリケーションコントロール</li> <li>&gt; 証明書</li> </ul>	×	WAN	NA	NA	NA	0 サービスを許可	0 サービスを許可	
IPSec VPN     PPTP VPN	FROI	DMZ	0 サービスを許可	0 サービスを許可	0 サービスを許可	0 サービスを許可	0 サービスを許可	
> SSL VPN		VPN	0 サービスを許可	NA	0 サービスを許可	0 サービスを許可	0 サービスを許可	
<ul> <li>インターフェース</li> <li>&gt; IPv6</li> </ul>		UTM	NA	1サービスを許可	NA	0 サービスを許可	NA	
<ul> <li>&gt; ルーティング</li> <li>&gt; DNS</li> </ul>	ログ:		■ インターン	<sup>ッ</sup> ーン設定のログを有	前にする			
> DHCP	NAT:		<ul> <li>✓ 送信バケ</li> </ul>	ットのソース IP アドレ	/スを変換する場合( ● のいす	LAN/DMZ => WAN ()	ゆみ)	
<ul> <li>&gt; ダイナミックDNS</li> <li>&gt; USBモデム</li> </ul>			タイフ: 適用する		U SNAT			
> ロードバランシング								

2. サービスを追加したい特定の指定したソースと宛先ゾーンペアのマトリックスで**セ** ルをクリックします。[定義を参照] ポップアップ画面が表示され、サービス定義リ ストが提示されます。

<del>.</del> ل	ービス定義をフ	ブラウズする				×	
既存定義							
	名前	タイプ	プロトコル	ソースポート	宛先ボート		
1	AOL IM	任意	ТСР	Any	5190	•	
	DHCP	任意	UDP	Any	67 - 68		
1	dns	任意	UDP	Any	53		
1	esp	任意	esp	Any	Any		
	ftp	任意	тср	Any	21		
	Google Talk IM	任意	тср	Any	5222		
	gre	任意	gre	Any	Any		
	http	任意	тср	Any	80		
1	http proxy	任意	тср	Any	8080		
						•	
				0	к <b>+</b> +ンセル	,	

- 3. 指定したソースと宛先ゾーンペアに許可したいサービス定義を選択します。[OK] を クリックします。
- 4. [ログ] チェックボックスを選択し、インターゾーンファイアウォールルールのログ を有効にします。
- 5. 指定したソースと宛先ゾーンペアの LAN から WAN、および DMZ から WAN へのアク セスに NAT を使用して、送信元 IP アドレスを発信パケットに変換します。以下の 2 つのオプションが利用できます:
  - マスカレード:マスカレードでは、IP アドレスが動的に変換されます。このオプションが選択されているとき、送信インターフェース上のアドレスがどのようなものでも、それがすべての送信パケットに適用されます。
  - SNAT:SNAT は、送信パケットにスタティック IP アドレスを適用します。このオ プションでは、送信インターフェースの IP アドレスを入力する必要があります。

## カスタムファイアウォールルール

カスタムファイアウォールルールは、セキュリティポリシーを非常に柔軟に定義し、カ スタマイズできるようにするユーザー定義のルールです。[カスタムファイアウォール] ページで、カスタムファイアウォールルールを閲覧、追加、編集、および削除すること ができます。 注意:同じソースと宛先に複数のルールがある場合、これらのルールの優先順位を変更 することができます。優先順位が一番高いルールが最初に適用されます

## カスタムファイアウォールルールの表示

カスタムファイアウォールルールを表示する場合:

1. Seqrite [Terminator] > [設定] > [ファイアウォール設定] > [カスタムルール] ヘログオンします。次のページが表示されます。

Seqrite TERMINATOR	★ オブション マ   ? ヘルブ マ   ● シャットダウン マ   ● Admin (管理) マ ホーム コンテンツフィルタリング ユーザー管理 設定 ログとレボート
<ul><li>・ インターネット</li></ul>	ファイアウォール… デフォルトのル… インターゾーン設定 カスタムのル… IPボートフォワーディ…
→ アンチウイルス	保存
▶ 電子メール保護	<b>カスタムのルール</b> 追加   削除
<b>&gt;</b> 定義	□ 名前 ソース サービス 宛先 ステー □ ログ アクション 説明
ファイアウォール設定 ▶	
> IPS	
> アプリケーションコントロール	

- 2. [カスタムファイアウォール] ページには、ファイアウォールルールのグループに関 するリストが表示されます。
- 3. [グループ名] をクリックし、特定のグループでファイアウォールルールを表示します。
- 4. ステータス行のボタンでルールのステータスを有効/無効に設定します。
- 5. ログ行でログオプションを選択し、ファイアウォールルールのログを有効にします。
- 6. [保存] をクリックします。

## ファイアウォールルールの追加

ファイアウォールのルールを作成するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [ファイアウォール設定] > [カスタムルール] ヘログオンします。次のページが表示されます。
- 2. [追加] をクリックします。[ファイアウォールの設定の追加] ページが表示されま す。
| カスタムのルール | > 追加  | 保存          | キャンセル                   |
|----------|---|-------------|-------------------------|
| 名前:      |   |             |                         |
| アクション:   | 許可する 🔹  |             |                         |
| ソースゾーン:  | LAN  、 ソースインターフェース                            | : eth0      | *                       |
|          |   |             |                         |
|          |   |             |                         |
| ソース:     | □ 関連するアドレス ホスト                                |             | ≅   <b>+</b>   ∎        |
|          |   |             | <u>^</u>                |
|          |   |             | <b>.</b>                |
| サニビフ・    |   | ر<br>مربط ا |                         |
| 9-LX:    | □   | %元小─►       | = +   ≡                 |
|          |   |             |                         |
|          |   |             | -                       |
| 宛先ゾーン:   | LAN v 宛先インターフェース:                             | eth0        | *                       |
|          |   |             |                         |
|          |   |             | <b>*</b>                |
| 更新先:     | □ 関連するアドレス ホスト                                |             | ⊞   <b>+</b>   <b>m</b> |
|          |   |             | *                       |
|          |   |             | -                       |
| NATを適用:  | □ 送信元 IP アドレスを発信パケットに変換します。                   |             |                         |
|          | タイブ: <ul> <li>マスカレード</li> <li>SNAT</li> </ul> |             |                         |
| 説明:      |   |             |                         |
|          |   |             |                         |
| ログ:      |   |             |                         |

3. このページのフィールドの説明を、次の表に示します。

フィールド	説明
名前	ルールの【名前】を入力します。

フィールド	説明
処置	ルールに従い、トラフィックに対して行われるアクションを 選択します。 アクションは次のいずれかです。
	<b>受け入れる</b> :接続を許容し、パケットがネットワーク上で転送 されることを許可します。
	<b>破棄する</b> :暗黙的にパケットを破棄し、ネットワーク内を通過 しないようにします。ユーザーへの応答は送信されません。
	<b>拒否する</b> :接続を全面的に拒否し、パケットがネットワークを 通過することを禁止します。送信元ホストには、ICMP の宛先 へ到達できないという応答が返送されます。
送信元ゾーン	<ul><li>[送信元ゾーン] リストから、適切な送信元ゾーンを選択します。</li><li>[送信元ゾーン] リストには、[LAN]、[WAN]、[DMZ]、</li><li>[VPN]、[UTM]、[ブリッジ] が含まれています。</li></ul>
送信元のインター フェース	送信元のインターフェースを入力します。
送信元	ルールが適用される送信元ホストまたはネットワークアドレ スを選択します。アイコンを使用して、ネットワーク定義の 参照、追加、削除を行えます。
サービス	サービスは、特定のプロトコル/送信元ポート/宛先ポートの 組み合わせで送信されるインターネットデータのタイプを示 します。アイコンを使用して、サービス定義の参照、追加、 削除を行えます。
宛先領域	[宛先ゾーン] リストから適切な宛先ゾーンを選択します。 [宛先ゾーン] リストには、[LAN]、[WAN]、[DMZ]、[VPN]、 [UTM] および [ブリッジ] が含まれています。
宛先インターフェ ース	宛先インターフェースを入力します。
宛先	ルールを適用する宛先ホストまたはネットワークアドレスを 選択します。アイコンを使用して、ネットワーク定義の参 照、追加、削除を行えます。

フィールド	説明
Nat の適用	このオプションは、送信トラフィックのホストの送信元 IP アドレスを変換するために使用します。次の 2 つのタイプが あります。
	マスカレード:マスカレードでは、IP アドレスが動的に変換 されます。このオプションが選択されているとき、送信イン ターフェース上のアドレスがどのようなものでも、それがす べての送信パケットに適用されます。
	SNAT:SNAT は、送信パケットにスタティック IP アドレスを 適用します。このオプションでは、送信インターフェースの IP アドレスを入力する必要があります。
説明	ファイアウォールルールの説明を入力します。
ロギング	ファイアウォールルールでログを取りたい場合、このオプシ ョンを選択します。

4. [保存] をクリックします。

## ファイアウォールのルールの削除

ファイアウォールのルールを削除するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [設定] > [ファイアウォール設定] > [カスタムルール] ヘログオンします。次に示すページに、ルールのリストが表示されます。
- 2. 削除するファイアウォールのルールを選択し、[削除] をクリックします。

## IP ポート転送

ポートの転送により、ネットワーク管理者はインターネット上での社外との通信すべて に 1 つの IP アドレスを使用し、社内でのタスクにはそれぞれ異なる IP アドレスと ポートを持つ複数の専用サーバーを使用できます。また、ネットワーク上でどのような サービスが実行されているかを外界から隠すためにも役立ちます。

Terminator の IP/ポートの転送機能を使用して、自社ネットワーク上のホストが Terminator の背後にあっても、インターネット(自社ネットワークの外側)からアク セス可能にできます。IP アドレスの全体を転送でき、コンピュータのすべてのポート ヘアクセスを許可することも、特定のポートのみを転送することもできます。IP/ポー ト転送ルールを作成するとき、プロトコルも選択できます。

[IP ポート転送] ページで IP ポート転送ルールを追加、編集、および削除できます。

## IP ポート転送ルールの表示

- IP ポート転送ルールのリストを表示するには、以下の手順に従います:
- 1. Seqrite [Terminator] > [設定] > [ファイアウォール] > [IP ポート転送] ヘログ オンします。[転送] 画面が表示されます。

Seqrite TERMINATOR	☆ オブション -   ? ヘルブ -   ひ シャットダウンする -   → Admin (管理) - ホーム コンテンツフィルタリング ユーザー管理 設定 ログとレポート
> インターネット	ファイアウォール… デフォルトのル… インターゾーン設定 カスタムのル… <b>IPボートフォワーデ…</b>
<ul> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> </ul>	
<b>、</b> 完善	
ファイアウォール設定 ▶	
<ul> <li>▶ IPS</li> <li>▶ アプリケーションコントロール</li> </ul>	

- 2. このページには、IP ポート転送ルールのリストが表示されます。
- 3. ステータス行のボタンでルールのステータスを有効/無効に設定します。
- 4. **ログ**の行でログオプションを選択して、ルールのログを有効にします。
- 5. [保存] をクリックします。

#### IP ポート転送ルールの追加

- IP ポート転送ルールを追加するには、以下の手順に従ってください
- 1. Seqrite [Terminator] > [設定] > [ファイアウォール] > [IP ポート転送] ヘログ オンします。次に示す画面が表示されます。
- 2. [追加]をクリックします。次に示す画面が表示されます。

IPボートフォワーディン	/グ→追加		保存	キャンセル
マップ名前:				
送信元アドレス:	🔲 関連するアドレス	ホスト		≡   <b>+</b>   <b>0</b>
				*
				-
フォワーディングタイプ:	◎ IP : ◎ ボート			
ブロトコルを選択します:	全て	•		
外部IP:	eth1-10.10.104.167	•	ポート :	-
マップIP:		≡ +	# ボート:	-
説明:				
ログイン:				

- 3. [マッピング名] を入力します。
- 4. ソースアドレスを参照または追加します。
- 5. 転送タイプを選択します。
  - [IP] を選択すると、外部 IP を選択して、マップされた IP を参照または追加 する必要があります。
  - [ポート] を選択すると、外部 IP を選択して、ポートとともに、マップされた IP を参照または追加する必要があります。
- 6. [プロトコルの選択] リストからプロトコルを選択します。プロトコルリストには、 [すべて]、[TCP]、[UDP] のオプションがあります。
- 7. **外部 IP** を選択します。外部 IP は、転送で使用される WAN インターフェースの IP アドレスです。パブリックのコンピュータはこの IP アドレスにアクセスします。
- 8. マップされた IP を選択します。マップされた IP は、転送が行われる宛先コンピュータの IP です。IP アドレスを参照、追加、または削除できます。
- 9. ルールの詳細を入力します。
- 10. ルールに関連するアクティビティのログを取る場合は、**ログ**オプションを選択します。
- 11. [保存] をクリックします。

### IP ポート転送ルールの削除

ファイアウォールのルールを削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [ファイアウォール設定] > [IP ポート転送] へ ログオンします。次に示すページに、ルールのリストが表示されます。
- 2. 削除するルールを選択し、[削除] をクリックします。

#### VPN

仮想プライベートネットワーク(VPN)は、企業の社内ネットワークなど2つのプライ ベートネットワークを接続し、インターネット上でデータを転送するために構築される ものです。VPNのシステムは暗号化や他のセキュリティ機構を使用し、許可されたユー ザーのみがプライベートネットワークへアクセスできることと、データを傍聴できない ことを保証します。

VPN によって、リモートユーザーと企業ネットワークとの間でデータを転送するための、 安全で暗号化されたトンネルが提供されます。暗号化されたトンネルを経由して 2 つ の場所の間で転送される情報は、他の誰からも読み取られることはありません。システ ムには、企業のプライベートネットワークを保護するため、いくつかの機構が組み込ま れています。

Seqrite Terminator には仮想プライベートネットワークを作成するための機能が搭載 されているため、インターネット上で組織のネットワークへ安全にアクセスできます。 この機能により、キーや SSL 証明書を共有し、接続時に安全な認証が可能です。さら に、サイト間とリモートの両方の接続を使用して、プライベートネットワークへアクセ スできます。

Seqrite Terminator では、次の 3 タイプの VPN が提供されます。

**IPSec VPN**:この VPN は、レイヤ 3 の IP セキュリティ標準を使用して、クライアント とサーバーとの間に安全なトンネルを作成します。

PPTP VPN:ポイントツーポイントトンネリングプロトコル (PPTP) は、TCP/IP ベースの データネットワーク上に VPN を作成することで、リモートクライアントから民間企業 のサーバーに安全にデータを転送することができるネットワークプロトコルです。この VPN は、クライアントとサーバーを接続するために PPE 認証を使用します。

SSL VPN:この VPN は、SSL 証明書と公開キーインフラストラクチャ (PKI) を使用して、クライアントとサーバーとの間のトンネルで認証と暗号化を行います。

注意:VPN 接続数は、VPN ライセンスバリューにより異なります。

#### 証明書

証明書は、セキュリティ目的で使用される電子メッセージに添付される文書です。証明 書は一般的に、ユーザーが送信するメッセージの合法性を検証し、返信を暗号化する手 段を受信者に提供するために使用されます。自己署名証明書を追加することも、サード パーティの認証局 (CA) が署名した証明書をインポートすることもできます。認証局 (CA) は、メッセージを暗号化するためにセキュリティ証明と公開キーを発行し、管理 する機関です。

Seqrite Terminator で、認証局や証明書を管理できるほか、VPN 接続を開始するときの認証に使用できる自己署名証明書を作成できます。サードパーティの証明書をインポートし、認証局と証明書をダウンロードすることもできます。Seqrite Terminator で、証明書の失効リストを保守できます。

証明書を管理するには、以下を実施します:

1. [Seqrite Terminator] > [設定] > [証明書] ヘログオンします。次のページが表示 されます。

Searite			🌻 オプション 🗸	·   <b>?</b> ヘルプ <del>-</del>   😃 シ	'ャットダウンする 🗸   📑 Admin (管理) 👻
TERMINATOR		ホーム	コンテンツフィ	′ルタリング ユーザ	ー管理 設定 ログとレポート
> インターネット	証明書				
→ アンチウイルス	証明機関				インポート 追加 削除
▶ 電子メール保護	■ 名前	共通名	説明	有効期限	証明書
					*
<ul> <li>&gt; ファイアウォール設定</li> </ul>					
> IPS					
> アプリケーションコントロール					
証明書 ▶					Ŧ
> IPSec VPN	証明書				インボート」追加」削除
> PPTP VPN	■ 名前		説明	有効期限	証明書
> SSL VPN					*
▶ インターフェース					
> IPv6					
▶ ルーティング					
> DNS					~
> DHCP		4776bu - 1			164 Mar
→ ダイナミックDNS	SSL VPN 訨明書	解約リスト		anu	1旦710   自川乐
→ USBモデム	■ 名前		説明	解約期日	
> ロードバランシング					
> 管理					
> 通知					

- 2. このページは以下の 3 つのセクションに分かれます:
  - 認証局
  - 証明書
  - SSL VPN 失効りすと

3. 認証局/証明書を追加するには、該当するセクションで [追加] をクリックします。 [認証局/証明書の追加] のポップアップ画面が表示されます。

認証局を追加しま	ġ			×
名前:	ニックネーム			
有効期限:	[オプション]			
国:	Japan	$\checkmark$		
州:	[オプション]		1	2
所在地名:	[オプション]		4	0
組織名:	[オプション]			
共通名:	ホスト名			
電子メール:	[オプション]			
			ОК	キャンセル

4. 名前、有効期限、国、州、地域名、組織名、ユニット名、通称、メールなどの詳細 を入力し、[OK] をクリックします。

注意:

- 証明書を追加している間に、割り当てられた CA を選択する必要があります。
- 名前と共通名にスペースは使用できません。
- 5. サードパーティの証明書と認証局をインポートできます。証明書/認証局をインポートするには、該当するセクションで [インポート] をクリックします。次に、名前 を入力し、ファイルを選択し、パスワードを入力して [OK] をクリックします。

インポート認証局		×
名前:	ニックネーム	
別名でインボート:	PKCS12	
CA証明書:	参照	
パスワード:		
説明:	說明	
	<b>ок</b> キャンセ	ν

注意:

- 認証局のインポートには、PKCS12、PEM、DER ファイルフォーマットを使用できます。PEM または DER ファイルフォーマットを選択した場合、公開キーをインポートするオプションを取得できます。証明書に署名するためにインポートしたCA を使用するときに、この鍵が必要となります。
- 証明書のインポートには、PKCS12 ファイルフォーマットのみ利用できます。
- 6. SSL VPN 失効リストには、ブラックリストに登録されている接続のリストと説明、 それらが失効リストに追加された日付のリストが表示されます。これは証明書が消 失した、または盗難に遭った場合に、接続を停止するため使用できます。クライア ントの証明書を失効またはブロックするには、[失効リスト] セクションで [追加] をクリックします。既存の接続リストで接続名を選択し、[保存] をクリックします。

## IPSec

Seqrite Terminator では、IPSec VPN を設定でき、これによってメインサーバー(本 社など)とクライアントサーバー(支社オフィスなど)との間にトンネルが構築され、 そのトンネルを経由してデータを送信できるようになります。両端では、アドレス割り 当て、暗号化、認証について設定可能な各パラメータが一致します。IPSec では、事前 共有キー(RSA キーまたは X509 証明書)を使用してトンネルを構築します。そうする ことで、データの暗号化と復号化を行い、スヌーピングを防止します。送信者および受 信者の信頼性が保証されます。

IPSec VPN では 2 タイプの接続が可能です。

- サイト間接続 本社と支社のように離れたサイトを接続します。
- リモートアクセス L2TP / IPSecVPN L2TP (レイヤ 2 トンネルプロトコル)を 使用して、単一の VPN クライアントを VPN サーバーへ接続します。レイヤ 2 トンネルプロトコル (L2TP) は、パケット指向メディアでポイントツーポイント プロトコル (PPP) フレームを送るためにカプセル化する業界規格のトンネルプ ロトコルです。

[ライブログ] ボタンをクリックして、IPSec VPN 接続のライブログを表示することも できます。このログは、IPSec VPN サービスの現在のステータスを表します。

## サイト間 IPSec VPN の追加

サイト間 IPSec VPN 接続を使用して、様々なブランチネットワークをリモートネット ワークにアクセスさせることができます。

IPSec VPN サーバーを追加するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [IPSec VPN] ヘログオンします。VPN 接続のリ ストと共に、[IPSec VPN] 画面が表示されます。VPN 接続の詳細ページには、IPSec VPN 接続の詳細が表示されます。このページで、IPSec VPN の追加と削除も行えます。

Searite			🔅 オブショ	レー ? へル	プー   😃 シャッ	トダウンする	~   📄 Admin (管理) -
TERMINATOR		ホーム	コンテンツフ	フィルタリング	ユーザー管	理設定	ログとレポート
> インターネット	IPSec VPN				サイト間 IPSec VP	N UE-FO	アクセス L2TP/IPSec VPN
<ul> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> </ul>	VPNサーバー:	◎肴	动	無効			保存 ライブログ
> 定義	接続						這力 <b>0 </b> 育川除
> ファイアウォール設定	□ 接続名		ステータス	パブリック IP	リモート ル	ON/OFF	
> IPS	ローサーバー		inactive	10.10.104.167	10.10.104.198	☑ オン	^
> アプリケーションコントロール							
> 証明書							
IPSec VPN							

- 2. VPN サーバーを有効に設定します。
- 3. サイト間 IPSecC VPN を追加するには、[追加] をクリックします。[IPSec VPN の 追加] 画面が表示されます。

IPSec VPN 〉追加		保存(キャンセル)
接続名:		
機能詳細:	● サーバー   ◎ クライアント	
ネットワークインターフェイス:	10.10.104.199:eth1 •	
リモートサーバーIP:		
ローカルネットワーク	追加   削除 リモートネットワーク	追加   削除
	*	*
	¥	*
認証タイプ:	● PSK   ◎ RSA キー   ◎ X.509 証明書	
	事前共有キーを入力	
	PSKの確認	
XAUTH:	🔲 追加のユーザー認証を使用してセキュリテ	ィを高めます。
NATトラバーサル:	デバイスが NAT ルーターの後ろに置かれて	ている場合に選択します。
圧縮:	□ バケットのベイロードを圧縮して性能を上け	"ます。
デッドピア検知:	🔲 その他のビアデバイスが利用可能か確認い	<b>ノます</b> 。
PFS:	☑ 各 IPSec セッションに新しいキーを作成しま	वे .
🛛 基本オプション		
第1	第2	
暗号化アルゴリズム: 3DES	▼ 暗号化アルゴリズム:	3DES 🔻
認証アルゴリズム: MD5	▼ 認証アルゴリズム:	MD5 •
キー・グループ (DH): 2 (DH	1024) ▼ キー・グループ (DH):	2 (DH1024)
このページのフィールドの	説明を、次の表に示します:	
フィールド名 説明		

フィールド名	説明
接続名	[接続名] を入力します。これは、接続を識別するために使用される固 有の名前です。
アクトアズ	サーバーをアクトアズに設定します。

	<ul> <li>サーバー:このオプションを選択すると、サーバーはメインサーバーとして動作します。</li> <li>クライアント:このオプションを選択すると、サーバーはクライアン</li> </ul>		
インターフェース	トサーバーとして動作します。 VPN サーバーを実行する [インターフェース] を選択します。これら		
	は、[インターフェース] セクションで設定した WAN インターフェース です。		
リモートサーバー IP	リモートサーバー IP の入力:これは、VPN サーバーが実行されるリモ ートのパブリック IP です。		
ローカルネットワ ーク。	ローカルネットワークを選択/入力します。複数のローカルネットワー クを選択できます。		
リモートネットワ ークアドレス	リモートネットワークアドレスを選択/入力します。これは、リモート プライベートネットワークのアドレスです。		
認証タイプ	以下のオプションから認証タイプを選択します。		
	<ul> <li>PSK:事前共有キー (PSK) は共有の秘密キーで、安全なネットワーク チャンネルを使用するため、2 つの組織の間で共有されます。この キーは、リモートネットワークユーザーと共有しなければなりません。このオプションを選択した場合、事前共有キーを入力しなけれ ばなりません。</li> </ul>		
	<ul> <li>RSA キー:RSA は、メッセージの暗号化と解読に使用される非対称暗 号アルゴリズムです。非対称とは、2 つの異なるキーがあり、その うちの 1 つがクライアントに渡されることを示します。このオプシ ョンを選択すると、クライアントと「公開キー」を共有しなければ なりません。また、[リモートの公開キーを入力] テキストボックス でクライアントの公開キーを追加しなければなりません。</li> </ul>		
<ul> <li>X. 509 証明書:X. 509 証明書は、証明書に含まれる ID で 公開キーを検証するために、広く受け入れられてい X. 509 公開キーのインフラストラクチャー規格を使用す 証明書です。このオプションを選択すると、証明書を選邦 ートクライアント ID] 欄にリモートクライアントの証明 力しなければなりません。</li> </ul>			
XAuth オプション	上記の認証タイプのほかに、XAuth オプションで追加の認証を加えることもできます。このオプションを選択し、サーバーとして機能するように選択した場合、認証用のユーザー名とパスワードを設定し、それをクライアントと共有しなければなりません。		
	注意:クライアントとして選択した場合、サーバーから提供されたユー ザー名とパスワードを追加しなければなりません。		

NAT トラバーサル	お使いの VPN サーバーがプライベート IP で実行されている場合、ソ ース NAT またはマスカレードされたパケットが VPN サーバーに届くよ うに、NAT トラバーサルオプションを選択します。	
圧縮	<ul> <li>圧縮オプションを選択し、VPN で交換されているパケットのペイロードを圧縮します。</li> <li>デッドピア検出オプションを選択し、VPN で利用可能なクライアント/ サーバーを検出します。このオプションを選択した場合、タイムアウト 期間を秒で指定しなければなりません。また、ピアが非アクティブ(デッド)の場合、失われたリソースを取り戻すための処置を指定する必要 があります。以下のアクションを選択できます。</li> </ul>	
デッドピアの検出		
	保持:接続が同じ状態に保持されます。	
	クリア:すべての接続が削除されます。	
	再起動:現在の接続を停止し、新しい接続を開始します。	
詳細オプション	詳細オプションをクリックして、認証アルゴリズム、暗号化アルゴリズム、およびキーグループ設定を変更します。	
	フェーズ 1 では、ハンドシェイクまたは認証が可能です。フェーズ 2 で実際のトンネルを作成します。[詳細オプション] ダイアログボック スで、ドロップダウンのリストから、[暗号化アルゴリズム]、[認証ア ルゴリズム]、[キーグループ] について利用可能なオプションを選択し ます。これらの詳細は、暗号化プロセスに使用されます。 クライアントとサーバーで同じ設定を使用する必要があります。	

4. 必要なすべてのフィールドに入力したら、[保存]をクリックします。

## リモートアクセス L2TP / IPSec VPN の追加

リモートアクセス L2TP IPSec VPN により、単一の PC/ノートパソコンからリモートネ ットワークにアクセスできるようになります。認証と安全にアクセスするために、事前 共有キーと X.509 証明書を設定できます。自身の事前共有キーを設定し、VPN に接続 可能なユーザーを追加できます。

リモートアクセス L2TP / IPSec VPV アクセスを追加するには、以下の指定の手順に従います:

1. [Seqrite Terminator] > [設定] > [IPSec VPN] > [リモートアクセス L2TP / IPSec VPN] ヘログオンします。次に示す画面が表示されます。

IPSec VPN	サイト間 IPSec VPN リモートアクセス L2TP/IPSec VPN
L2TP/IPSec:	<ul> <li>○ 有効 ● 無効</li> </ul>
リーバーIP:	10.10.104.199:eth1 ▼
仮想IPフール: 認証タイプ:	開始IP 終了IP ● PSK ● X.509 証明書
事則共有キー: □ ユーザー	IPアドレス ステータス 追加   削除

- 2. L2TP/IPSec オプションを有効に設定します。
- 3. サーバー名を入力します。
- 4. **サーバー IP** を入力します。
- 5. 仮想 IP プールを入力します。これらは、プライベートネットワークにアクセスす るためにリモートユーザーに割り当てられる IP アドレスです。
- 6. ドロップダウンリストから**サブネット**を選択します。これは、リモートネットワー クのサブネットマスクです。
- 7. 以下から AuthBy オプションを選択します。

**PSK**:事前共有キー (PSK) は共有の秘密キーで、安全なネットワークチャンネルを使用するため、2 つの組織の間で共有されます。このキーは、リモートネットワーク ユーザーと共有しなければなりません。このオプションを選択した場合、事前共有 キーを入力しなければなりません。

X.509 証明書:X.509 証明書は、証明書に含まれる ID でユーザーの公開キーを検証 するために、広く受け入れられている国際的な X.509 公開キーのインフラストラク チャー規格を使用するデジタル証明書です。このオプションを選択した場合、この 証明書を選択しなければなりません。

- 8. リモートネットワークへのアクセスを許可したいユーザーを追加します。ページの [ユーザー] セクションで [追加] をクリックします。VPN に接続するユーザーが使 用するユーザー名、パスワード、および確認パスワードを入力します。
- 9. [保存] をクリックします。

### PPTP VPN

ポイントツーポイントトンネリングプロトコル (PPTP) は、シングル PC アクセス用に 仮想プライベートネットワークを実装するための手法です。Seqrite Terminator では、 PPTP VPN を使用して単一の PC をプライベートネットワークへ接続できます。PPTP は、 接続用のセキュアなトンネルを作成するためにプレーンテキスト認証と MPPE 暗号化を 使用します。

[ライブログ] ボタンをクリックして、PPTP VPN 接続のライブログを表示することもで きます。このログは、PPTP VPN サービスの現在のステータスを表します。

#### PPTP VPN の追加

新しい PPTP VPN 接続を追加するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [PPTP VPN] ヘログオンします。
- 2. [追加] をクリックします。次に示すような、PPTP リモートネットワークアクセス の新しい接続画面が表示されます。

Searite			🏟 オプション   <b>?</b>	ヘルプ -   🕛 シャット	<sup>ダ</sup> ウン <del>▼</del>   📑 Admin (管理)	-
TERMINATOR		トーム コン	テンツフィルタリング	ユーザー管理	設定 ログとレポート	
> インターネット	PPTP VPN				保存 ライブロ	グ
> アンチウイルス	PPTP VPN:	◉ 有劾	● 無効			
▶ 電子メール保護	仮想IPブール:	開始IP	- 終了IP	サブネット選	択 ▼	
<b>&gt;</b> 定義	プライマリ DNS:	[オプション]				
> ファイアウォール設定	セカンダリ DNS:	[オプション]				
> IPS	プライマリ WINS:	[オブション]				
▶ アプリケーションコントロール	セカンダリ WINS:	[オプション]				
> 証明書						
> IPSec VPN	□ ユーザー			追加 削除		
PPTP VPN	ユーザー名を入た	5				
> SSL VPN	パスワードを入力					
→ インターフェース	バスワードの再入		保存	×		
> IPv6						
▶ ルーティング						
> DNS						
> DHCP						

- 3. 接続名を入力します。
- 4. [仮想 IP pool] を入力します。これらは、プライベートネットワークにアクセスす るためにリモートユーザーに割り当てられる IP アドレスです。
- 5. プライマリ/セカンダリ DNS サーバーの IP アドレスを入力します。

- 6. プライマリ/セカンダリ WINS サーバーの IP アドレスを入力します。
- PPTP VPN にアクセスできるユーザーを追加するには、[ユーザー] セクションで [追加] をクリックします。ユーザーのユーザー認証に必要なユーザー名、パスワード、確認用パスワードを入力します。
- 8. [保存] をクリックします。

#### SSL VPN

セキュアソケットレイヤ仮想プライベートネットワーク (SSL VPN) は、認証に SSL 証 明書を使用する VPN 形式です。この VPN を使用するには、エンドユーザーのコンピュ ータに roadwarrior クライアントをインストールする必要があります。リモートユー ザーは、SSL VPN を使用してウェブアプリケーション、クライアント/サーバーアプリ ケーション、内部ネットワーク接続にアクセスできます。

Seqrite Terminator には SSL VPN 機能が搭載されており、サードパーティの証明書を インポートするか、自己署名された証明書を作成できます。また、SSL VPN では次のタ イプの接続を使用できます。

- サイト間
- シングル PC のリモート接続

#### SSL VPN サーバーの設定

SSL VPN サーバーの設定を行うには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [SSL VPN] ヘログオンします。次の画面が表示 されます。

SSL VPN			<b>サーバー設定</b> サイト間 リモートアクセス
証明機関			
SSL VPN デフォルト CA:	選ぶ		T
	デフォルトの設	定 すべての掛	き続証明書はこの認証権限で署名されます。
サーバー設定			
SSL VPNサーバー:	◎ 有効 ⑧ 無刻	边	保存
インターフェース:	eth1-10.10.104.	58	T
プロトコル:	○ TCP ● U	IDP	
ポート:	1194		
仮想IPブール:	ネットワーク:		
	サブネット:	255.255.0.0	T
□ 基本オブション			
暗号:	BLOWFISH		•
認証アルゴリズム:	MD5		T
DH パラメーター:	1024		V
最大クライアント:	5		T
VPN 圧縮:	🖉 SSL VPNトラフ	パックの圧縮	
CNを複製:	🔲 ユーザーごと	に複数の同時接	続を可能にする
クライアント間:	■ リモートシステムの任意のペア間の接続性に可能します		
デッドビア検知:	🕢 オフラインリモ	ヨートシステムを枯	食出します
	間隔:	20	秒.
	切断の後:	60	秒.
サービスの種類:	🔲 SSL VPNトラフ	ィックのためにτα	sビットを保存する。

- SSL VPN の認証局を選択し、[デフォルトの設定] ボタンでデフォルトに設定します。
   注意:この認証局が、すべての SSL VPN 接続証明書に署名します。
- デフォルトでは、SSL VPN サーバーは無効です。[有効] オプションを選択し、サーバーを有効にします。
   詳細オプションの説明を、次の表に示します:

フィールド	説明		
インターフェース	ドロップダウンのリストから [インターフェース] を選択しま す。SSL VPN は、この WAN インターフェースで接続を受け付 けます。		
プロトコル	必要に応じて、[プロトコル]の [TCP] または [UDP] を選択 します。		
	<ul> <li>TCP:リモート SSL VPN サーバーが TCP で実行されている場合、このプロトコルを選択します。</li> </ul>		
	<ul> <li>UDP:リモート SSL VPN サーバーが UDP で実行されてい る場合、このプロトコルを選択します。</li> </ul>		
ポート	[ポート] 番号には、デフォルトの SSL VPN ポートが表示され ます。		
仮想 IP プール	[仮想 IP プール]のネットワークアドレスを入力します。こ れらのアドレスは、SSL VPN クライアントに割り当てられま す。該当するサブネットを選択します。		
暗号	暗号化と復号を実行するためのアルゴリズムです。ネットワ ークで使用する暗号のタイプを選択します。		
認証アルゴリズ ム	ネットワークのデータ認証アルゴリズムを選択します。		
DH パラメータ	Diffie-Hellman キー交換パラメータにより、2 つの組織が互いに相手に対して事前の知識がない場合でも、安全でない通信チャンネルを使用して、共有の秘密キーを共同で構築できます。DH パラメータの長さを選択します。		
最大クライアン ト数	VPN クライアントに接続できるクライアントの最大数。		
VPN 圧縮	SSL PVN でデータを圧縮する場合、このパラメータを選択します。		
CN の複製	各ユーザーの同時接続を行う場合、このオプションを選択し ます。		
クライアント間	任意のリモートシステムのペア間で接続を可能にするに このオプションを選択します。		

フィールド	説明
デッドピアの検 出	Terminator でオフラインのリモートシステムを検出するに は、このオプションを選択します。
サービスの種類	このオプションを選択して、SSL VPN トラフィックの ToS ビ ットを保存します。

4. [保存] をクリックします。

### SSL VPN にサイト間接続を追加する

VPN ネットワークにサイトを追加すると、サイト間接続が可能になります。接続タイプ としてサーバーまたはクライアントを指定し、ローカルネットワークまたはリモートネ ットワークからネットワークを追加する必要があります。

サイト間接続を追加するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [SSL VPN] > [サイト間] ヘログオンします。サ イト間の設定ページが表示されます。

Seqrite		<b>¢</b>	オプション   <b>?</b> ^	√ルプ <del>-</del>   ( <u>し</u> シ	/ャットダウン ▼	🔁 Admin (管理) ▼
TERMINATOR		ホーム コンテン	ソフィルタリング	ユーザー管	理設定	ログとレポート
<ul><li>インターネット</li></ul>	SSL VPN			サーバー言	定 サイト間	リモートアクセス
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	サイト間					追加   削除
<ul> <li>アラブライルス</li> <li>アラブライルス</li> </ul>	□ 接続名	結合方式	現在の状態	ステータス	パッケージ	
	- Test	サーバー接続	無効になって	オフ	ダウンロード	*
▶ 正我						
> ファイアウォール設定						
> IPS						

- 2. [追加]をクリックします。サイト間接続の追加ページが表示されます。
- 使用する接続タイプとして、[サーバー] または [クライアント] を選択します。
   サーバータイプを選択すると、次に示す画面が表示されます。

サイトからサイトへの	> 追加		保存	キャンセル
結合方式: 接続名:	サーバー			
ローカルネットワーク:	<ul> <li>すべて選択</li> <li>atbo: 192 168 173 0/255 255 25</li> </ul>	5.0 .		
		-		
リモートネットワーク:	🔲 すべて選択	追加 削除する		
		-		
追加コマンド:				

このページのフィールドの説明を、次の表に示します:

フィールド	説明	
接続名	接続を識別するための固有の名前を入力します。	
ローカルネットワー ク	[ローカルネットワーク] セクションのリストに表示され ているローカルネットワークを選択します。	
リモートネットワーク	[リモートネットワーク] セクションの下に表示されるリ ストから、リモートネットワークを選択します。追加する ネットワークがリストに表示されていない場合、[追加] ボタンを使用してネットワークを追加します。同様に、 [削除] ボタンを使用して、必要のなくなったネットワー クを削除できます。	
追加コマンド	必要に応じて、追加コマンドを追加します。 例を挙げます。 ルートゲートウェイ 10.10.16.1	

	ifconfig-push 10.10.16.53 10.10.16.54
	リダイレクトゲートウェイ〈def1   local   bypass-dhcp   bypass-dns〉
	dhcp オプション DNS 10.10.16.100
	dhcp オプション WINS 10.10.16.200
	ルート 10.10.16.0 255.255.255.0

4. 接続タイプとして [**クライアント**] を選択すると、次のオプションが表示されます:

サイトからサイトへのつ	保存 キャンセル	
結合方式:	クライアント 🔽	
設定:	◉ アップロード ○ マニュアル	
	参照	

- 5. PKG ファイルをアップロードするか、手動で設定を選択できます。PKG ファイルが ある場合、[アップロード] オプションを選択します。[ファイルの選択] をクリッ クし、ユーザーの詳細を含む Excel ファイルを参照します。
- 6. [手動] オプションを選択した場合、次の詳細を設定する必要があります:

Searite		🔅 オプション -   ?	ヘルブ・  😃 シャットダ	ウンする 📲 🗧	▶ Ashish (管理) 👻
TERMINATOR	*	ーム コンテンツフィルタリン	ノグ ユーザー管理	設定	コグとレポート
> インターネット	サイトからサイトへ	√の → 追加	(	保存	キャンセル
> アンチウイルス	結合方式:	クライアント 🔽			
▶ 電子メール保護	設定:	○ アップロード ● マニ	ニュアル		
> 定義		接続名:			
> ファイアウォール設定		リモートサーバーP:			
> IPS			🗌 追加リモートサーバ	-IP	
> アプリケーションコントロール		プロトコル:	● TCP ○ UD	Р	
▶ 証明書		术:			
> IPSec VPN		輸入証明書:	証明書 🗸		
> PPTP VPN		cA評明書:		参照	
SSL VPN		クライアント証明書:		参照	
> インターフェース		クライアント証明書キー:		参照	
> IPv6		国井木ナキション			
> ルーティング		□ 巫4-5 / ノノヨノ フーザータ・			
> DNS					
> DHCP					
> ダイナミックDNS		四日7:	DES	$\checkmark$	
➤ USBモデム		語証アルゴリズム:	MD5	~	
> 山一下ハランシンク		VPN压縮	□ 圧縮機SSL VPN交通		
> 管理					

フィールドの説明を、次の表に示します:

フィールド	説明
接続名	接続の名前を入力します。
リモートサーバー IP	リモート SSL VPN サーバーをバインドするリモートサイトの IP アドレスを入力します。
追加リモートサー バー IP	リモート SSL VPN サーバーを複数の IP にバインドする場合、IP を追加します。
プロトコル	TCP:リモート SSL VPN サーバーが TCP で実行されている場 合、このプロトコルを選択します。 UDP:リモート SSL VPN サーバーが UDP で実行されている場 合、このプロトコルを選択します。
ポート	リモート SSL VPN サーバーが実行されるポートを追加しま す。

フィールド	説明
証明書をインポー トします	[証明書]:CA 証明書、クライアント証明書、クライアント証 明書キーの 3 つのファイルをインポートできます。これらの ファイルは.pem または.crt 形式です。
	PKCS#12:.p12 形式で証明書をインポートし、ファイルのパス ワードを入力します。

7. 次に示す [詳細] オプションも設定できます。この設定は両サイドで一致する必要 があります。

フィールド	説明
ユーザー名	サードパーティの SSL VPN サーバーにより、接続用に提供さ れたユーザー名。
パスワード	サードパーティの SSL VPN サーバーにより、接続用に提供さ れたパスワード。
暗号	暗号アルゴリズムでパケットを暗号化します。この設定は両 サイドで一致する必要があります。
認証アルゴリズム	特定のアルゴリズムでパケットを認証します。この設定は両 サイドで一致する必要があります。
VPN 圧縮	送信データを圧縮したい場合、[SSL VPN トラフィックを圧 縮]チェックボックスを選択します。

- 8. [保存] をクリックします。
- 9. SSL サイト間接続の詳細を追加すると、その接続がリストに表示されるようになり ます。接続ステータスを [ON] または [OFF] に変更できます。
- 10. 設定パッケージをダウンロードするには、[**ダウンロード**] リンクをクリックします。 このパッケージは、クライアントが SSL VPN へ接続するときの認証に使用されます。

#### SSL VPN 用にシングル PC のリモートアクセスを設定する

シングル PC のリモートアクセスを設定するには、以下の手順に従います:

1. [Seqrite Terminator] > [設定] > [SSL VPN] > [リモートアクセス] ヘログオンし ます。SSL VPN リモートアクセス接続のリストが表示されます。現在の接続はリス トに表示されます。

Seqrite <b>TERMINATOR</b>		ಸ−ム ⊐ು	🌞 オプション、	-  <b>? ヘルブ -</b> リング ユー <sup>-</sup>	<ul> <li>● シャットダウンマ</li> <li>ザー管理</li> <li>設定</li> </ul>	<mark> →</mark> Admin (管理) <del>-</del> ログとレポート
> インターネット	SSL VPN			サ・	-バー設定 サイト間	リモートアクセス
、アンチウイルフ	リモートアクセン	t				追加   削除
<ul> <li>ケラブラール(A)</li> <li>オール(A)</li> </ul>	□ 接続名	現在の状	「態 ステータ	ス パッケージ		
	Connection	非アクテ	ィブな オン	ダウンロー	U.	*
> 正義						
> ファイアウォール設定						
> IPS						
> アプリケーションコントロール						

2. [追加]をクリックします。リモートアクセスの追加設定ページが表示されます。

遠隔操作 > 追加		保存 キャンセル
接続名:		
ユーザー名:		
パスワード:		
バスワードの再入力:		
ローカルネットワーク:	回 すべて選択	
	eth0:192.168.171.0/255.255.255.0	
	Ξ	E
X44		-
追加コマント:		
	.41	

- 3. [接続名] を入力します。
- 4. [**ユーザー名**] および [パスワード] テキストボックスに、ユーザー名とパスワード を入力します。[パスワードの再入力] テキストボックスに、パスワードを再入力し ます。これらは認証に使用されます。
- 5. リストに表示されているローカルネットワークを選択します。
- 6. 必要なら、[追加コマンド]を追加します。
- 7. [保存] をクリックします。

#### SSL VPN 用のリモートアクセスサイトを削除する

- 1. [Seqrite Terminator] > [設定] > [SSL VPN] > [リモートアクセス] ヘログオンし ます。SSL VPN リモートアクセス接続のリストが表示されます。現在の接続はリス トに表示されます。
- 2. 削除する SSL VPN 接続を選択して、[削除] をクリックします。

## VLAN

仮想ローカルエリアネットワーク(VLAN)は同じ要件の組を持つワークステーション、 サーバー、ネットワークデバイスのグループで、地理的な場所に関わらず同じ LAN 上 に存在するように見えます。VLAN により、コンピュータのネットワークが、単一の LAN 上に存在しているのと同様に環境内で通信が行えます。VLAN を実装することで、 拡張性とセキュリティを実現でき、ネットワークの管理が簡単になり、ネットワークの 要件が変化した場合や、ワークステーションやサーバーのノードの場所が変更された場 合にも迅速に適合可能になります。



#### VLAN の追加

Terminator に VLAN を追加すると、ネットワークセグメントを増やすために役立ちま す。VLAN 機能により、単一のインターフェースに複数の VLAN インターフェースを設 定できます。Seqrite Terminator は、802.1q VLAN 規格をサポートしています。 次のタイプの VLAN を作成できます。 VLAN-LAN:ローカルネットワーク用。

VLAN-WAN:外部ネットワーク (インターネット)/ISP 用。

VLAN-DMZ:中立ゾーン用。これは、企業のプライベートネットワークと社外のパブリックネットワークとの間に存在する中間のゾーンです。

注意:インターフェースを追加しても、Terminator の物理ポートは追加されません。ポート数は、Terminator モデルによって決定されるデフォルトポート数と同じです。

VLAN インターフェースを追加するには、以下の手順に従います:

- 1. Seqrite[Terminator] > [設定] > [インターフェース] ヘログオンします。インタ ーフェースの詳細ページが表示されます。
- 2. [追加] をクリックします。次のページが表示されます。

インターフェース >	インタフェ	ースを追加	する		保存	キャンセル
タイプ:	VLAN			$\sim$		
VLAN ID:						
ゾーン:	LAN	⊖ WAN		ΜZ		
ベースインターフェース	th0 (eth0	)		$\sim$		
19割り当て:	● 静的	○ ダイヤノ	レアップ	⊖ DHCP		
IPv4アドレス:						
サブネットマスク:	255.255.0	.0		$\sim$		
IPv4ゲートウェイ:	ゲートウェイ	は既に設定され	ています	0		

- 3. インターフェースのタイプとして [VLAN] を選択します。
- 4. [VLAN] を選択してから、次の詳細を入力します:
  - i. **[VLAN ID]** を入力します。値は 2 ~ 4094 の範囲です。
  - ii. 運用のゾーンとして、[LAN]、[WAN]、[DMA]のいずれかを選択します。
  - iii. **[ベースインターフェース]**を選択します。これは物理ポートです。設定 済みと未設定のネットワークインターフェースすべてが、ここに表示されます。
- 5. **[IP 割り当て]**のタイプとして、[スタティック]、[ダイヤルアップ]、[DHCP]のい ずれかを選択します。

注意:LAN および DMZ インターフェースでは、IP 割り当ては常にスタティックです。

i. IP 割り当てとして [スタティック] を選択した場合、[IPv4 アドレス] と [サ ブネットマスク] を入力する必要があります。

- ii. IP 割り当てとして [ダイヤルアップ] を選択した場合、ISP から提供される [ユ ーザー名] と [パスワード] を入力する必要があります。
- 6. [保存] をクリックします。

注意:各 VLAN インターフェースは、ベースインターフェースのサブインターフェー スとしてインターフェースリストに表示されます。

インターフェー	ス					追加創除
▶ 名前	ゾーン	ステータス	IPアドレス	ゲートウェイ	旧割り当て	デフォルトルート
▼ □ eth0	LAN	<b>オン</b> オフ	192.168.171.1		静的	
🔲 別名 2		オン	192.168.45.1		静的	
▼ ■ eth1	WAN	オン	10.10.104.167	10.10.104.1	静的	デフォルト 💼
VLAN 22	LAN	オン	192.168.55.1		静的	
🔲 ブリッジ 23		オン	10.10.17.45	10.10.17.1	静的	デフォルト
Dond0	LAN	オン	172.16.10.5		静的	Â

# ブリッジ

ブリッジインターフェースを使用して、1 つの論理ネットワーク内にある 2 つのネッ トワークセグメントを接続、またはコリジョンドメインを破棄します。Seqrite Terminator は、ネットワークブリッジインターフェースの設定として、IEEE 802.1D 規格に対応しています。ファイアウォール/ルーターがすでに存在し、その置き換えを 希望しない場合、Terminator をブリッジモードに設定できます。Terminator は混在モ ード設定に対応しており、このモードではデバイスにブリッジモードとルーターモード の両方を同時に設定できます。ブリッジは、未設定のインターフェースにのみ設定でき ます。



Seqrite Terminator ブリッジインターフェースは、次の用途に使用できます:

- 透過式ゲートウェイ:Seqrite Terminator デバイスは、ネットワークブリッジを 通過するトラフィックに対して、上流のルーター、ファイアウォール、UTM と透 過的に動作します。同デバイスを LAN-WAN ブリッジとして設定できます。この 場合、ルーターで終端するネットワークインターフェースは WAN 領域となり、 ローカルネットワーク用スイッチで終端するインターフェースは LAN 領域とな ります。
- ローカルネットワークセグメントブリッジ:この場合、Seqrite Terminator デバイスは、LAN-LAN、LAN-DMZ、DMZ-DMZ ブリッジなどの内部メッセージセグメントに接続されます。

ブリッジインターフェースを追加するには、以下の手順に従います:

- 1. Seqrite[Terminator] > [設定] > [インターフェース] ヘログオンします。インタ ーフェースの詳細ページが表示されます。
- 2. [追加] をクリックします。次のページが表示されます。

インターフェース >	インターフェース > インタフェースを追加する 保存 キャンセル				
タイプ	ブリッジ	•			
ブリッジID					
インタフェース A	•	ゾーンA	LAN 🔻		
インダフェース B	•	ゾーン B	LAN 🔻		
IPv4アドレス					
サブネットマスク	255.255.0.0	•			
IPv4ゲートウェイ					
STPモーŀ	🔲 ネットワークブリッジ	のループを防ぐため!;	チェックしておく必要があります。		

- 3. インターフェースの [**タイプ**] として [ブリッジ] を選択します。
- 4. [ブリッジ] を選択してから、次の詳細を入力します。ブリッジを追加するには、 Terminator ポートが 2 つ必要です。
- 5. **ブリッジ ID**:値は 0 ~ 100 の範囲です。ブリッジを識別するため使用される固有 の番号です。
- 6. [インターフェース A] と、対応する [ゾーン] を選択します。
- 7. [インターフェース B] と、対応する [ゾーン] を選択します。
- 8. [IPv4 アドレス] を入力します。
- 9. [サブネットマスク] を入力します。
- 10. Terminator がルーターの背後に存在する場合、Seqrite[IPv4 ゲートウェイ] を設 定します。
- 11. 必要に応じて、[STP モード] を有効にします。このオプションは、[ブリッジ] オ プションでのみ表示されます。このモードを有効にすると、ネットワークブリッジ のループを防止するために役立ちます。
- 12. [保存] をクリックします。

インターフェー	-ス					追加 削除	
▶ 名前	ゾーン	ステータス	IPアドレス	ゲートウェイ	IP割り当て	デフォルトルート	
▼	LAN	オンオフ	192.168.171.1		静的		h
🔲 別名 2		オン	192.168.45.1		静的		
▼ 🔲 eth1	WAN	オン	10.10.104.167	10.10.104.1	静的	デフォルト 🧴	
VLAN 22	LAN	オン	192.168.55.1		静的		
🔲 ブリッジ 2	3	オン	10.10.17.45	10.10.17.1	静的	デフォルト	
bond0	LAN	オン	172.16.10.5		静的	Ĺ	<u>`</u>

# リンクアグリゲーション

リンクアグリゲーションは、複数の並列したネットワークインターフェースを組み合わ せて、ネットワークのスループットを上げるための技法です。高速ネットワークで、大 量のデータを高速かつ安価に転送するため使用されます。リンクアグリゲーションによ って、ハードウェアデバイスの変更なしにネットワークが拡張され、容量が増えると同 時に、速い転送速度が維持されるため、コストを削減できます。

リンクアグリゲーション機能には、次の2つの利点があります。

**負荷分散**: ネットワークトラフィックの負荷が 2 つ以上のネットワークインターフェー スに分散され、それらは単一の接続に見えるため、冗長性が得られ、信頼性が向上しま す。

フェールオーバー:2 つ以上のネットワークインターフェースを組み合わせることで、 フォールトトレランスが提供されます。ネットワークインターフェースのいずれかに障 害が発生した場合、トラフィックは他のネットワークインターフェースへ自動的に振り 分けられます。

リンクアグリゲーションインターフェースを作成するには、以下の手順に従います:

- 1. [Seqrite Terminator] > [設定] > [インターフェース] ヘログインします。インタ ーフェースページが表示されます。
- 2. [追加]をクリックします。インターフェースの追加ページが表示されます。

インターフェース >	インタフェースを追加する 保存 キャンセル
タイプ	リンクアグリゲーション
リンクアグリゲーショ ン ID	
リンクアグリゲーショ ンモード	802.3ad (LACP)
ハッシュ送信ポリシー	Layer 2
スレーブインター	<ul> <li>□ 名前</li> <li>□ eth2</li> <li>□ eth3</li> <li>□ eth4</li> </ul>
ゾーン IP割り当て IPv4アドレス サブネットマスク IPv4ゲートウェイ	<ul> <li>LAN ② WAN ② DMZ</li> <li>静的 ③ DHCP</li> <li>255.255.0.0</li> <li>WANインターフェイスJはIPv4Iに構成され</li> </ul>

このページのフィールドの説明を、次の表に示します:

フィールド	説明
タイプ	ドロップダウンから、インターフェースのタイプとして[リン クアグリゲーション]を選択します。
リンクアグリゲー ション ID	リンクアグリゲーション ID を入力します。識別用の固有の番 号で、範囲は 0 ~ 99 です。
リンクアグリゲー ションモード	リンクアグリゲーションモードを選択します。このモードは、 適用されるボンディングのポリシーを決定します。リンクアグ リゲーションで使用可能なモードは次の通りです。
	802.3ad (LACP):IEEE 802.3ad ダイナミックリンクアグリゲー ション。802.3ad 規格に従い、アクティブなアグリゲータのす べてのスレーブを利用します。このモードでは、負荷分散とフ ォールトトレランスが提供されます。このモードには、IEEE 802.3ad LACP をサポートするスイッチが必要です。
	ラウンドロビン:このモードは、利用可能な最初のスレーブから最後のものへ、順番にパケットを転送します。このモードでは、負荷分散とフォールトトレランスが提供されます。

フィールド	説明
	Xor:このモードでは、送信ハッシュポリシーに基づいてパケットが転送されます。このモードでは、負荷分散とフォールトトレランスが提供されます。
	ブロードキャスト:このモードでは、すべてのパケットをすべ てのスレーブインターフェースで転送します。このモードで は、フォールトレランスが提供されます。
	アクティブ-バックアップ:リンクアグリゲーションインターフ ェースのうち、1 つのスレーブだけがアクティブです。アクテ ィブなスレーブに障害が発生した場合、その場合だけ別のスレ ーブがアクティブになります。このモードでは、フォールトレ ランスが提供されます。
ハッシュ送信ポリ シー	転送ハッシュポリシーを選択します。このオプションは、 802.3ad および Xor モードを選択した場合のみ表示されま す。利用可能な転送ハッシュポリシーは次の通りです。
	レイヤ 2:ハードウェア MAC アドレスの XOR を使用してハッ シュを生成します。このアルゴリズムでは、特定のネットワー クピアへのトラフィックがすべて、同じスレーブ上に配置され ます。
	レイヤ 2 + 3:このポリシーは、レイヤ 2 と レイヤ 3 (MAC お よび IP アドレス)プロトコル情報を組み合わせてハッシュを 生成します。このアルゴリズムでは、特定のネットワークピア へのトラフィックがすべて、同じスレーブ上に配置されます。
スレーブインター フェース	スレーブインターフェースは未設定の物理ポートで、アグリゲ ーション/結合が可能です。1 つのリンクアグリゲーションイ ンターフェースに、最少 2 つ、最大 8 つの物理ポートをアグ リゲーションできます。リンクアグリゲーションインターフェ ースから設定されたスレーブインターフェースは、リンクアグ リゲーションインターフェースが削除されるまでは、削除でき ません。 これらのインターフェース上には、VLAN インターフェースを 設定できません。
ゾーン	[ゾーン] を選択します。ゾーンは、[LAN]、[WAN]、[DMZ] の いずれかです。

フィールド	説明
IP 割り当て	IP 割り当てを選択します。IP 割り当てタイプは、[スタティ ック] または [DHCP] です。
IPv4 アドレス	IP アドレスを入力します。
サブネットマスク	サブネットマスクを入力します。IP を指定した場合のみ必要 です。
IPv4 ゲートウェイ	ゲートウェイを入力します。IP を指定し、ゾーンが WAN の場 合のみ必要です。

3. [保存] をクリックします。

注意:

- VLAN とエイリアスは、リンクアグリゲーションインターフェース上に設定できます。
- ブリッジは、リンクアグリゲーションインターフェース上に設定できません。
- アクティブ-バックアップモードを除き、リンクアグリゲーションが動作するには、スイッチでの設定が必要です。

インターフェ	ース					追加	削除
▶ 名前	ゾーン	/ ステーダ	<sup></sup> ス IPア <mark>ド</mark> レス	ゲートウェイ	「時間り当て	デフォルト	ルート
eth0	LAN	オンオフ	192.168.1.200		静的		
🗌 eth1	WAN	オン	10.10.104.207	10.10.104.1	静的	デフォルト	
🔲 eth3	WAN	オン	192.168.0.100	192.168.0.1	DHCP	デフォルト	
bond2	LAN	オン	192.168.45.1		静的		Ē.

# インターネット設定と除外

ユーザーのインターネットアクセスを制御できます。ユーザーの役職と必要性に合わせ て、直接または部分的アクセスを提供できます。例えば、取締役やヴァイスプレジデン トにはフィルタリングなしの直接アクセスが必要な場合でも、他のユーザーにはコンテ ンツフィルタリング後にアクセスを提供できます。また、自分たちの企業のドメインを ブロック対象から外すことができます。

インターネット設定を行うには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] ヘログオンします。デフォルトでは、インターネット設定のページが表示されます。インターネット設定のページには、Terminator サーバーの IP アドレスとポートが表示されます。

このページのフィールドの説明を、次の表に示します:

フィールド	説明
ダイレクトインター ネットアクセス	ネットワークに存在するコンピュータの IP アドレスを [直接 インターネットアクセス] リストに追加すると、そのコンピュ ータはフィルタリングなしでインターネットへアクセスできま す。このリストに含まれている IP アドレスには、コンテンツ やウェブのフィルタリングポリシーは適用されません。この機 能を、企業の取締役や副社長などのキーパーソンのコンピュー タやノートパソコンに対して使用すると、それらのユーザーは 制限なしにインターネットへアクセスできます。このリストに は、単一の IP アドレス、または IP アドレスの範囲を追加で きます。 注意:ユーザーのブラウザにはプロキシを設定できません。
ダイレクトアクセス ウェブドメイン	このセクションを使用して、制限なしのアクセス、またはウェ ブのフィルタリングなしに直接アクセスが必要なウェブサイト を追加します。この機能は、企業のウェブサイトに使用できま す。
無効な証明書を持つ URL を除外	自己署名された証明書を使用している内部のサイトや、サイト の内部ドメイン名が公開の証明書名と異なる場合に、特定の証 明書エラーが発生することがあります。[追加]または[削除] をクリックして、このようなドメインを除外または削除しま す。 注意:証明書エラーの無視は、セキュリティの問題となりま す。これらを共有プロキシ内で除外するのはきわめて危険な行 為です。自分が承認された所有者であるドメインを除いて、無 効な証明書を持つ URL を除外するのは避けてください。自分が 所有者である場合は、除外の前に証明書の問題を解決するよう 試みてください。
許可される通常トラ フィック	このセクションは、オープンアクセス用のポート番号を追加す るために使用します。ユーザーは、これらのポート上で実行さ れるウェブサイトにアクセスできます。デフォルトの HTTP ポ ート 80 は追加済みで、削除することはできません。
許可された安全なト ラフィック	このセクションは、安全なトラフィック用のポート番号を追加 するために使用します。ユーザーは、これらのポート上で実行 される安全なウェブサイトにアクセスできます。HTTPS ポート 443 はデフォルトポートで、削除できません。

フィールド	説明
安全なトラフィック のバイパス	このオプションを選択すると、監視や制御を受けず、すべての HTTPS ウェブサイトに直接アクセスできます。 注意:ブラウザにはプロキシを設定できません。
アップデートサイト の Seqrite バイパス	このオプションを選択すると、アップデートの取得に使用され るすべての Seqrite サイトへ、監視や制御を受けず直接アクセ スできます。この機能により、ネットワークに展開されている すべての Seqrite Terminator 製品を、ユーザーが意識するこ となくアップデートできます。
X-Forwarded-For へ ッダ情報を含める	エンドユーザーのプライバシーを強化するため、"X- Forwarded-For" HTTP ヘッダを取り除くよう Terminator を設 定できます。デフォルトでは、このオプションは Terminator で有効です。このオプションを無効にすると、送信される要求 の HTTP ヘッダから、エンドユーザーのホストの IP 情報が削 除されます。既存のファイアウォールを使用する場合、特にブ リッジモードでは、このオプションを有効のままにしておくこ とが必要な可能性があります。
デバイス オフライ ンモード	インターネットからサービスを停止する場合、デバイスオフラ インモードを選択できます。[設定サービス] ボタンでオフライ ンに設定できるサービスを選択することもできます。 [設定サービス] ボタンをクリックすると、サービスリストが表 示されます。 サービスを設定 * * * * * * * * * * * * * * * * * *
	す。 注意:デバイスオフラインモードが選択されている場合のみ、 これらのサービスはオフラインになります。

フィールド	説明
デバイスインターネ ットクォータの有効 化	このオプションを使用して、Terminator でインターネットクォ ータを有効にできます。このオプションを選択し、Terminator に適用したいインターネットポリシーを設定します。[設定を 行う] をクリックしてデバイスインターネットクォータポリシ ーを作成します。(詳細は <u>インターネットクォータ</u> を参照してく ださい。) 注意: このクォータポリシーは、ユーザー/グループクォータポリシ ーよりも重要性が高いポリシーです。デバイスインターネット クォータが完全に消費されると、すべてのユーザーがログアウ トされ、インターネットアクセスが拒否されます。

2. [保存] をクリックします。

注意:一部のポートは定義済みで、これらは削除できません。ポート 80 はデフォルトで、[許可される通常トラフィック] に表示されます。同様に、ポート 443 はデフォルトで [許可された安全なトラフィック] に設定されています。
# ID 管理/ユーザーとグループ

ユーザーとグループを作成し、ユーザー管理ページを使用してグループにインターネットへのアクセスポリシーを適用できます。ネットワーク上で、インターネットの使用を コントロールおよび制限するため、次のような操作が行えます。

- ユーザーを作成し、特定のグループへ割り当てる。
- グループ単位で、ウェブサイトへ制限付きのアクセスを許可する。
- グループに対して、制限付きのアクセス許可で、それぞれ別の時間枠を割り当てる。
- ユーザーやグループへ帯域幅の使用量を割り当てる。この機能により、帯域幅の使用量を常に把握でき、統計レポートも作成できます。
- ネットワークについてインターネットトラフィックのポリシーを作成し、ユーザー
   管理機能を使用してインターネットアクセスを定義して制限する。
- インターネットの使用に関する組織のルールとポリシーを維持する。
- ゲストユーザーアカウントと、そのインターネットアクセスを作成して管理する。
- ユーザーに認証サーバーを割り当てる。

ユーザー管理ページは、次のセクションに分けられます。

- ユーザー
- ゲストユーザー設定
- グループ
- 時間カテゴリ
- 認証サーバー
- インターネットクォータ

これらの各セクションから、設定と管理の詳細オプションにアクセスできます。

# ユーザー管理

ユーザー管理機能では、ユーザーの作成、編集、削除と、ユーザーを特定のグループへ 割り当てることができます。ユーザーはローカルで作成するか、認証サーバーからイン ポートできます。ユーザーページには、ユーザー名、グループ名、認証、ログインステ ータス、IP/MAC バインドの詳細、コンテンツフィルタリングのステータスなど、ユー ザーの詳細情報が表示されます。このページには、ログインしているユーザーの総数も 表示されます。

注意:ログインしていない場合、ネームワイズユーザーはインターネットを閲覧したり、 メールにアクセスしたりすることができません。

Seqrite <b>TERMINATOR</b>		ホーム =	<b>☆ オブシ</b> ョ コンテンツフィル	<b>シ</b> ▼  <b>? ヘルブ</b> ▼ レタリング ユー	<b>也</b> シャットダウ ザー管理 誘	ン     Admin (管理 定 ログとレポー	<b>里) -</b> -ト
ユーザー ・	ユーザー					インポート エクスポ	(
> ゲストユーザー	ユーザー名で様	读索	0				
> グループ	ログイン中のユーザーの合計:0						
▶ 時間力テゴリ ▶ 認知####################################	ユーザーリスト					追加 削除 ログ	アウト
<ul> <li>・ model シークト</li> <li>&gt; インターネットクォータ</li> </ul>	□ユーザー名	グループ名 🔻	認証	ステータス	IP/MACバインド	コンテンツフィルタリン	ング
	□ テスト	quota_grp	ローカル	有効になっています	192.168.100.128	有効になっています	*
	□ テスト 2	quota_grp	ローカル	有効になっています	なし	有効になっています	
	■ テスト3	quota_grp	ローカル	有効になっています	なし	有効になっています	
	🔲 dtest	default	ローカル	有効になっています	なし	有効になっています	

#### [ステータス] フィールドには以下のオプションがあります:

フィールド	説明
有効	ユーザーが有効な状態で、Terminator にログオンしてインターネ ットヘアクセスできることを示しています。
無効	管理者によってユーザーが無効にされており、インターネットへ アクセスするため Terminator にログインできないことを示してい ます。
ログイン中	現在ユーザーがログイン中であることを示します。管理者は[ユー ザーリスト]からユーザーを選択して[ログアウト]ボタンをクリ ックすることで、ユーザーを強制的にログアウトさせることがで きます。

ユーザーの追加

新しいユーザーを追加するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [ユーザー管理] > [ユーザー] ヘログオンします。ユー ザー管理ページが表示されます。
- 2. 右上の [追加] をクリックします。[ユーザーの追加] 画面が表示されます。

ユーザー > 追加		保存 キャンセル
ユーザー名:	ユーザー名を入力してください	
認証タイプ:	ローカル	
バスワード:	*****	
バスワードの再入力:	***	
ステータス:	● 有効 ○ 無効	
グループを選択します。:	default グループを追加する	
インターネットクォータ:	□ グループクォータポリシーを適用します	
	ボリシー: - 選ぶ -	
同時ログイン:	□ 許可	
IP& MACバインディング:	tal.	
コンテンツフィルタリング:	● 有効 ○ 無効	
説明:	説明をタイプします	

このページのフィールドの説明を、次の表に示します:

フィールド	説明
ユーサー名	[ <b>ユーザー名</b> ] を入力します。
認証タイ	認証手法として、ローカルまたは認証サーバー (Active Directory
プ	または LDAP) 経由を選択します。
	[ローカル] が選択されている場合、ユーザーはローカルに作成さ
	れ、Terminator にユーザー名とパスワードが保存されます。
	ユーザーが認証サーバー経由で認証される場合、ユーザー名は認証
	サーバー上のユーザー名と同一にする必要があります。
パスワー	パスワードを入力します。パスワードは英数字で、長さが 6 ~ 20
ド	文字で、特殊文字が最低 1 つ含まれている必要があります。
パスワー	確認のため、パスワードを再入力します。
ドの確認	
ステータ	[有効]:ユーザーは認証を受けることができ、Terminator ヘログイ
ス	ンしてインターネットへアクセスできます。

フィール ド	説明
	無効:ユーザーは Terminator ヘログインできず、インターネットへ
	アクセスできません。
グループ	ユーザーへ割り当てるグループを選択します。グループによってポ
の選択	リシーも適用されます。
	注意:すでに作成済みのグループのみを選択できます。
インター	オプションを選択して、選択したグループと同じインターネットク
ネットク	オータポリシーを適用できます。このオプションをクリアし、特定
オータ	のドロップダウンリストで個々のインターネットクォータポリシー
	を選択することができます。
同時ログ	このオプションを使用すると、ユーザーは複数のシステムから同時
イン	にログインできます。同時にログインできる最大数は、無制限また
	はカスタマイズに設定できます。カスタマイズを選択した場合、同
	時にログイン可能な最大数を設定できます。
IP と MAC	設定に従い、ユーザー名を特定の IP アドレス、MAC アドレス、ま
のバイン	たは両方にバインドします。
ディング	注意:ユーザーが IP または MAC アドレスにバインドされている場
	合、そのユーザーは設定済みの IP または MAC アドレスを持つシス
	テムからのみログインできます。ユーザーは、IPv4、IPv6、または
	両方のアドレスにバインドできます。
コンテン	[有効] に設定すると、ユーザーに割り当てられているグループの設
ツフィル	定に従い、コンテンツがフィルタリングされます。[無効] に設定す
タリング	ると、ユーザーヘコンテンツフィルタリングルールは一切適用され
	ません。
説明	ユーザーの詳細を入力します。

3. **[保存]** をクリックします。新しいユーザーが作成され、ユーザー管理ページのリ ストに表示されます。

### ユーザーの編集

ユーザーを編集するには、以下の手順に従います:

- 1. Seqrite [Terminator] > [ユーザー管理] > [ユーザー] ヘログオンします。
- 2. [ユーザー] ページに表示されるリストの**ユーザー名**をクリックします。次に示す画 面が表示されます。

ユーザー > 編集		保存	キャンセル
ユーザー名:	テスト		
認証タイブ:	ローカル		
パスワード:	****		
パスワードの再入力:	****		
ステータス:	● 有効 ○ 無効		
グループを選択します:	default ・ グループを追加する		
インターネットクォータ:	☑ グループクォータボリシーを適用します		
同時ログイン:	計可		
IP& MACバインディング:	<i>ta</i> L		
コンテンツフィルタリング:	<ul> <li>● 有効</li> <li>● 無効</li> </ul>		
説明:	説明をタイプします		

3. ユーザーの詳細に必要な変更を加え、[保存]をクリックします。

注意:ユーザーを編集中はユーザー名を変更できません。

異なるインターネットクォータポリシーを選択している場合、以前のデータ使用量 をリセットするか、以前のデータ使用量を継続して使用するかを選択することがで きます。例えば、あるユーザーに、毎日のインターネット使用量が 100MB というポ リシーが割り当てられており、そのユーザーが 70MB のデータを使用しているとし ます。編集中に新しいポリシーが選択された場合、以前のデータ使用量をリセット すると、70 MB のデータ使用量は削除されます。

ユーザーの削除

ユーザーを削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [ユーザー管理] > [ユーザー] ヘログオンします。ユーザ ー管理ページが表示されます。
- 2. このページには、ユーザーのリストが、ユーザー名、グループ名、認証、ステータ ス、IP/MAC バインドのステータス、コンテンツフィルタリングのステータスを含め て表示されます。
- 3. ユーザーを削除するには、ユーザーを選択して [削除] をクリックします。選択し たユーザーが削除されます。

注意:複数のユーザーを選択して削除することもできます。

ユーザーの強制ログアウト

ユーザーを強制的にログアウトするには、以下の手順に従います。

- 1. Seqrite [Terminator] > [ユーザー管理] > [ユーザー] ヘログオンします。ユーザ ー管理ページが表示されます。
- このページには、ユーザーのリストが、ユーザー名、グループ名、認証、ステータス、IP/MAC バインドのステータス、コンテンツフィルタリングが有効かどうか、および作成済みの場合はメール ID とともに表示されます。
- 3. ユーザー名を選択して、**[ログアウト]** をクリックします。ユーザーはネットワーク からログアウトされます。

注意:複数のユーザーを選択して強制的にログアウトすることもできます。

ユーザーのインポート

Excel シートから詳細をインポートして、ユーザーを追加できます。ユーザーをインポートするには、以下の手順に従います:

- 1. Seqrite [Terminator] > [ユーザー管理] > [ユーザー] ヘログオンします。ユーザ ー管理ページが表示されます。
- このページには、ユーザーのリストが、ユーザー名、グループ名、認証、ステータス、IP/MAC バインドのステータス、コンテンツフィルタリングのステータスを含めて表示されます。
- 3. **[インポート]** をクリックします。[ユーザーのインポート] ダイアログボックスが 表示されます。

インポート ユーザー		×
ファイルをインポートします	参照	
スプレッドシートからパスワード には 最初の 列がユ ーザー向け ので3列を持つ必要があります の場合、パスワードは暗号化さ	と一緒にユーザーをインポートする 、第2はユーザーパスワード、第3; 。値が1の場合のように暗号化され れていないとみなされます。	ことができます。スプレッドシート がのある「パスワード暗号化」値な 、パスワードが考えられる。値が0 インポート キャンセル

4. [ファイルの選択] をクリックし、ユーザーの詳細を含む Excel ファイルを参照し ます。

注意:スプレッドシートには 3 つの列が含まれている必要があります。最初の列はユー ザー名、2 番目の列はパスワード、3 番目の列はパスワード暗号化の値です。パスワー ド暗号化列の値は 0 または 1 にする必要があります。パスワード暗号化が 0 の場合、 パスワードは通常のテキストです。パスワード暗号化が 1 の場合、パスワードは暗号 化されます。

	A	В	С	D
1	User Name	Password	Password Encryption	
2	user1	YWRtaW5AMTIz	1	
3	user2	YWRtaW5AMTIz	1	
4	user3	YWRtaW5AMTIz	1	
5				
6				

5. **[インポート]** をクリックします。[ユーザーのインポート] ダイアログボックス に、ユーザーが正しく追加されたことを示すメッセージが表示されます。これらの ユーザーは、[ユーザー] リストに表示されます。

#### ユーザーのエクスポート

ユーザーの詳細を Excel シートにエクスポートするには、以下の手順に従います:

- 1. Seqrite [Seqrite Terminator] > [ユーザー管理] > [ユーザー] ヘログオンしま す。デフォルトでは、ユーザー管理ページが表示されます。
- このページには、ユーザーのリストが、ユーザー名、グループ名、認証、ステータス、IP/MAC バインドのステータス、コンテンツフィルタリングのステータスを含めて表示されます。
- 3. Excel シートへ詳細をエクスポートするユーザーを選択し、[エクスポート] をクリ ックします。[ユーザーのエクスポート] ダイアログボックスが表示されます。



- 4. [ユーザーのエクスポート] ダイアログボックスで、ユーザーのパスワードを暗号化 するかどうを選択し、[エクスポート] をクリックします。
- 5. ユーザーの詳細を含む、exported\_users.xls という名前の MS Excel ファイルがコ ンピュータへダウンロードされます。

# ゲストユーザー設定

ゲストユーザーは登録されていないユーザーで、特定の時間についてインターネットへ アクセスするためにデフォルトのアクセス許可を与えられます。

Terminator のゲストユーザーのセクションでは、ゲストユーザーにインターネットへのアクセスを提供するため、一般的なパラメータを設定できます。ゲストユーザーは、

有効期間が満了すると、インターネットへのアクセスが許可されなくなります。また、 ゲストユーザーが自動的に削除されるようにも設定できます。

注意:SMS 機能を購入されている場合のみ、ゲストユーザー機能を利用できます。 設定は次の手順で行います:

1. [Seqrite Terminator] > [ユーザー管理] > [ゲストユーザー設定] ヘログオンしま す。次の画面が表示されます。

Seqrite		🌞 オブション -   <b>?</b> ヘルブ -   🖖 シャットダウン -   🕞 Admin (管理) -			
TERMINATOR	ホーム	コンテンツフィルタリング	ユーザー管理	設定	ログとレポート
> ユーザー	ゲストユーザー				保存
<b>ゲストユーザー →</b> → グループ	ゲストユーザーを有効にする: 有効期間:	7   □   00   ▼   時間			
<ul> <li>&gt; 時間カテゴリ</li> <li>&gt; 認証サーバー</li> </ul>	失効後に自動削除:				

2. 設定オプションの説明を、次の表に示します:

フィールド	説明
ゲストユーザー	このオプションを選択すると、Terminator でゲストユーザーの
を有効にする	登録が有効になります。
ユーザー有効性	ゲストユーザーの有効期間を設定します。失効するとゲストユ ーザーはインターネットにアクセスできなくなります。
失効後に自動削	失効時にゲストユーザーの情報を自動的に削除するにはこのオ
除	プションを選択します。

- 3. [ゲストユーザーを有効にする] オプションを選択すると、ユーザーログインページ に [ゲストアカウントの作成] リンクが表示されます。
- 4. [ゲストアカウントの作成] リンクをクリックすると、次に示す画面が表示されます。

ゲストアカウントを作成		×
ユーザー名:	ユーザー名を入力してください。	
携带電話番号:	+81 携帯電話の番号をここに入力して	
	<ul> <li>694262 S</li> <li>ここにコードを入力</li> </ul>	
		保存 キャンセル

5. 必要な詳細を入力し、[保存]をクリックします。

注意:ゲストユーザーは、定義済みの「ゲスト」というグループに含まれます。ゲス トユーザーは他のグループへ移動したり、他から移動してきたりすることはありま せん。

登録が完了すると、ゲストユーザーはログインのための認証情報が記載された SMS を受け取ります。

グループの管理

グループは、インターネットへアクセスするための同じポリシーを持つユーザーの集合です。ユーザー管理のセクションを使用して、グループに対して次の操作を実行できます。

- 新しいポリシーを持つ新しいグループを追加する。
- ユーザーにグループポリシーを使用する必要がなくなった場合に、グループを削除 する。
- 必要がなくなった場合に、複数のグループを削除する。
- グループを検索して、グループの詳細を確認する。
- インターネットへのアクセスポリシーや、ウェブサイトのホワイトリスト/ブラック リストをグループに適用する。

グループの追加

グループを追加する場合:

1. Seqrite [Terminator] > [ユーザー管理] > [グループ] ヘログオンします。[グル ープ] ページに、グループ名、ユーザー数、設定されている最大のグループ帯域幅、 ユーザーの最大帯域幅などグループの詳細が表示されます。

Seqrite <b>TERMINATOR</b>	ホー2	<mark>⇔ オプション →</mark> → コンテンツフィルタ <sup>1</sup>	<b>? ヘルブ -</b>   <b>()</b> シャッ リング ユーザー管理	トダウン →   🔁 Admin (管 設定 ログとレポ	<b>管理) -</b> ポート
> ユーザー	グループ			道加)	削除
> ゲストユーザー	グループ名で検索してくた	iðu 🔍			
グループ・	□ グループ名	ユーザー数▼	最大グループ帯域幅	最大ユーザー帯域幅	
<ul> <li>・時間リテコリ</li> <li>・認証サニバニ</li> </ul>	default	0	無制限 KB/秒	無制限 KB/秒	*
	guest	0	無制限 KB/秒	無制限 KB/秒	
· 12x=+9F2x=x	□ スズキ	0	無制限 кв/秒	無制限 KB/秒	
	□ さむらい	4	無制限 KB/秒	無制限 KB/秒	

2. [追加] をクリックします。

グループ → <mark>追加</mark>				保存	キャンセル
グループ名:	グループ名を入力				
<b>説明</b> :	説明を入力				
時間カテゴリ	□ すべて選択				∷≣   🛍
	🔲 default				*
					-
ユーザーを追加する。:	● ユーザー   ○ IP				
	ユーザー名で検索	0	ユーザー名で検	索	0
	■ 利田可能なフーザー(0)		□ 関浦フーサ	· (0)	
		*		(0)	*
		⇒			
		+			
	4	* ·	4		
パスワードを変更する:	🖉 ユーザーはこのグルーブからバ	スワードを	変更することがで	きます。	
インターネットアクセス:	<ul> <li>無制限のアクセス</li> <li>制限(</li> </ul>	<b>!</b> きでアクセ	27		
インターネットクォータ:	◉ 無効   ◎ 無効				
ウェブサイトカテゴリー:	◉ カテゴリーによるWebアクセス	● ドメイ	ンによるWebアク	カセス	
	カテゴリから探す	0	カテゴリから探	ŧ	Q
	□ 許可されたカテゴリー(64)		□ 埜止されて	いるカテゴリ	J(0)
	<ul> <li>広告とボッブ・アップ</li> </ul>	*			▲ _
	アルコールとタバコ				
	🔲 アノニマイザ	•			
	アート	-			
	🔲 সঁットネット	-			+
ホワイト/ブラックリスト:	<ul> <li>ホワイトリスト</li> <li>追加</li> </ul>	削除	🛛 ブラックリス	ŀ	追加 削除
		*			*

このページのフィールドの説明を、次の表に示します。

フィールド	説明
グループ名	グループ名を入力します。

フィールド	説明
	注意:グループ名に予約語や特殊文字は使用できません。
説明	グループに説明を加えます。
時間カテゴリ	グループの時間カテゴリを選択します。これは、ユーザーがイン
	ターネットへアクセスできる時間帯です。複数の時間カテゴリを
	選択できます(詳細は <mark>時間カテゴリ</mark> を参照してください。)
ユーザーを追	<b>ユーザー単位</b> :[ユーザー単位] でのユーザー追加を選択すると、
加	[利用可能なユーザー] リストが表示されます。[利用可能なユー
	ザー]からユーザーを選択し、右向き矢印をクリックして、その
	ユーザーを [関連付けされているユーザー] のリストへ移動しま
	す。そのユーザーがグループに関連付けされ、グループポリシー
	が適用されます。
	[利用可能なユーザー] リストのユーザーをすべて選択し、[関連]
	付けされているユーザー] リストへ移動できます。1 人のユーザー
	は、1 つのグループへ割り当てることができます。ユーザーがす
	でに別のグループと関連付けされている場合、そのユーザーの名
	前は [利用可能なユーザー] リストに表示されません。
	IP 単位:[IP 単位] を選択した場合は、次の詳細を入力する必要が
	あります。
	[追加] をクリックし、ユーザーに指定された IP アドレスを選択
	して [保存] をクリックします。
	単一の IP アドレスを指定する場合、開始 IP と終了 IP に同じ
	IP を人力します。
	IP の範囲を定義する場合は、開始 IP アドレスと終了 IP アドレ
	スにそれぞれの IP アドレスを追加します。【保存】をクリックし
	ます。使用されない IP アドレスの範囲を取り除くには、[ <b>則除</b> ]
	オノンヨンを使用しよす。
パスワードの	このオブションは、[ユーザー単位] オブションでのみ表示されま
変更	す。このオフションは、そのクループのユーサーかハスリードの
	変更を計りされるかとうかを指定するにのに使用します。
インターネッ	無制限:[無制限] を選択すると、ユーサーは制限なしにインター
トアクセス	イットを参照でさます。 期間11まのコキュー「期間11キコキュー」を閉想した。
	制限付きのアクセス:[制限付きアクセス] を選択すると、ユーサ
	ーは設定されている制限に使ってのみ参照でさます。この場合、
	びのサノオノンヨンも設定する必要がめります。 ビュープレムーザーの##は毎(WP/びりどけ)
	<b>取八グルーノ 常喫幅</b> ・このグルーノのユーザーか利用り能な常喫幅 (A計)の上間です。この機能にたってガル。その世球幅は田さ地
	(「「「」の上限です。この機能によつ(クルーノの常喫幅使用を削    限できます
	とことであり。

フィールド	説明
	<b>最大ユーザー帯域幅</b> :このグループの各ユーザーが利用可能な最大
	の帝域幅です。このオブジョンは、グループのユーサーが利用す  能た帯域幅を制限するために使用します
	各ユーザーについて、参昭時間を無制限に設定、または指定した
	時間に制限できます。
インターネッ	グループのユーザーに対し、インターネットアクセス制限を設定
トクォータ	できます。以下のオプションが使用できます。
	無効:グループのユーザーに対し、データ使用量の制限をかけませ
	$\lambda_{\circ}$
	[有効]:特定のドロップダウンリストからインターネットアクセス
	ポリシーを選択できます。
ウェブサイト	カテゴリによる:このオプションを選択すると、ユーザーは許可さ
カテゴリ	れたカテゴリのウェフサイトのみを参照できます。次のサフオブ
	ンヨンかめりより。
	「「町日はしのノーノ」からルノーノを選択し、ソヘト間の大印か」 タンを伸田」て「埜止されるカテゴリ」のリストへ移動します。 道
	方向へも移動できます。
	[ <b>カテゴリで検索</b> ] 検索ボックスを使用して、ウェブサイトのカテ
	ゴリを検索します。
	注意:URL 分類がコンテンツフィルタリングで有効にされている場
	合のみグループで URL 分類が利用できます。(詳細は、 <u>URL 分類</u> を
	参照してください。)
	ドメインによる:[追加] ボタンを使用して、ユーザーが安全に参
	照できるドメインを追加します。ドメインをリストから削除する
	には、その下メインを選択し、石上にめる [ 削除] をクリックしま
	9。 注音・このオプションを選択すると そのグループでけりストに追
	加されたドメインのみが許可され、他のウェブサイトはすべてブ
	ロックされます。
ホワイトリス	ホワイトリスト:ホワイトリストは、ユーザーが安全にアクセスで
ト/ブラック	きる、信頼できるウェブサイトのリストです。[追加] ボタンを使
リスト	用して、ウェブサイトをホワイトリストに追加します。
	ホワイトリストからウェブサイトを削除するには、そのウェブサ
	イトを選択して [削除] をクリックします。
	ブラックリスト:ブラックリストは、アクセスすると危険な可能性
	がある、信頼できないウェブサイトのリストです。

フィールド	説明
	[追加] ボタンを使用して、ウェブサイトをブラックリストに追加
	します。ブラックリストからウェブサイトを削除するには、その
	ウェブサイトを選択して <b>[削除]</b> をクリックします。

3. これらのオプションすべての設定が完了したら、[保存]をクリックします。

## グループの編集

グループを編集するには、以下の手順に従います:

- 1. Seqrite [Seqrite Terminator] > [ユーザー管理] > [グループ] ヘログオンしま す。
- 2. グループページに表示されるリストで [グループ名] をクリックします。次に示す 面面が表示されます。
- 3. グループの詳細で必要な変更を行い、[保存]をクリックします。

注意:グループの編集中にグループ名は変更できません。

異なるインターネットクォータポリシーを選択している場合、以前のデータ使用量 をリセットするか、以前のデータ使用量を継続して使用するかを選択することがで きます。例えば、あるグループのユーザーに、毎日のインターネット使用量が 100MB というポリシーが割り当てられており、そのユーザーが 70MB のデータを使 用しているとします。編集中に新しいポリシーが選択された場合、以前のデータ使 用量をリセットすると、70 MB のデータ使用量は削除されます。

### グループの削除

グループを削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [ユーザー管理] > [グループ] ヘログオンします。[グル ープ] ページに、ユーザー数、利用されている最大のグループ帯域幅、ユーザーの 最大帯域幅などグループの詳細が表示されます。
- 2. 削除するグループを選択し、右上にある [削除] をクリックして、選択したグルー プを削除します。複数のグループを同時に選択して削除できます。
   注意:グループが削除されると、ユーザーはデフォルトのグループに割り当てられま

### グループの検索

グループを検索するには、以下の手順に従います:

す。デフォルトおよびゲストのグループは削除できません。

- Seqrite [Terminator] > [ユーザー管理] > [グループ] ヘログオンします。[グル ープ] ページに、ユーザー数、利用されている最大のグループ帯域幅、ユーザーの 最大帯域幅などグループの詳細が表示されます。
- 2. [グループ名で検索] テキストボックスに、検索するグループの名前を入力します。 例えば、「デフォルト」と入力します。グループが自動的に検出されて表示され、 他のグループはリストから除外されます。

# 時間カテゴリ

時間カテゴリは、ユーザーとグループのインターネット閲覧間を定義するために使用します。使用可能なすべての時間カテゴリは、アクセス時間、各カテゴリの説明といった 情報とともに表示されます。

時間カテゴリを作成するには、以下の手順に従います:

1. Segrite [Terminator] > [ユーザー管理] > [時間カテゴリ] ヘログインします。

Sogrita			🔅 オブション -   ? ヘル	レプ -	🔹   🕛 シャットダウンする 🗸   🔁 Admin (管理) 🗸				
TERMINATOR		ホーム	コンテンツフィルタリング		ユーザー管理	設定 ログとし		ポート	
> ユーザー	時間カテゴリ					追加	Ì	削除	
> ゲストユーザー	🔲 カテゴリー名		アクセス時間		説明				
> グループ	default	-	すべての曜日 <mark>(00:00-23:59</mark> )		デフォルトの時間力	テゴリ			
時間カテゴリ ト									
> 認証サーバー									
➤ インターネットクォータ									

2. 右側の [追加] をクリックします。[時間カテゴリの追加] ページが表示されます。

時間カテゴリ >	時間のカテゴリを追加							保存	Ŧ		キャンセル
カテゴリー名:	カテゴリ名を入力										
説明:	説明を入力										
日を <u>選択</u> します:	■ 全て ■ 月曜日 ■ 火曜日	□水	曜日		翟日 (	□金曜		土曜日		曜日	
時間分:	◎ 終日 🛛 ● 時間の範囲を	選択し	ます								
	更新元 12:0	0 PM	宛	先 1	2:00 F	PM					
				Hou	r			M	linut	e	
	AM	00	01	02	03	04	05	00	05	10	
		06	07	08	09	10	11	15	20	25	
	PM	12	13	14	15	16	17	30	35	40	
		18	19	20	21	22	23	45	50	55	

3. [カテゴリ名] と [説明] を入力し、[曜日] と [時間帯] を入力します。

4. [保存] をクリックします。

# 認証サーバー

認証サーバーは、ネットワーク経由でユーザーや、他のシステムに認証サービスを提供 するサーバーです。Seqrite Terminator では、ネットワークの各種グループやユーザ ー用に、LDAP や Active Directory などの認証サーバーを登録できます。また、 Seqrite Terminator が認証サーバーと同期を行うための同期サイクルも設定できます。 この機能では、次の操作も実行できます:

- 認証サーバーを追加または編集する。
- 認証サーバーを削除する。
- Seqrite Terminator と登録済みのサーバーとを同期する。

新しいサーバーの追加

認証サーバーを追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [ユーザー管理] > [認証サーバー] ヘログオンします。登 録済みのサーバーのリストが、IP アドレス、ポート、タイプ、ベース DN、ステー タスの詳細を含めて表示されます。

Searite			¢	オプション -	? ヘルブ -   🔱 シャットダウ	ン   📄 Admin (管理)
TERMINATOR		ホーム コン	·テンツフィ	ルタリング	ユーザー管理 設定	ログとレボート
> ユーザー	認証サーバー	_				サーバー 詳細
▶ ゲストユーザー	サーバー					追加   削除
> グループ	■ 名前	IPアドレス	ボート	タイプ	ベース DN	ステータス
▶ 時間カテゴリ	Server1	14.141.16.16	389	LDAP	OU=test,DC=qhao	d, オン
認証サーバー ▶						
➤ インターネットクォータ						

2. [追加]をクリックすると、サーバーの詳細フォームが表示されます。

認証サーバー > <b>追加</b>	保存	キャンセル
名前	サーバー1	
認証タイプ	LDAP	
IPアドレス	14.141.16.16	
ポート	389	
ベース DN	OU=test,DC=qhad,DC=com	
匿名ログイン	□ 匿名ユーザーとしてLDAPサーバーを接続するために選択します	o
バインド DN	CN=testing,OU=test,DC=qhad,DC=cc	
バインドパスワード	•••••	
	設定テスト	
インポートされたユーザー/	グループのリスト	インボート」削除
🗌 ユーザー/グループ	識別名	$\bigcirc$
		~

3. サーバーの [名前] をフォームに入力し、必要に応じて以下のフィールドに他の詳 細を入力します。このページのフィールドの説明を、次の表に示します:

フィールド	説明
認証タイプ	認証サーバーのタイプとして、[LDAP] または [Active
	Directory]を指定します。
	注意:LDAP を選択すると、Anonymous ログインオプション
	が表示されます。
IP アドレス	新しい認証サーバーの IP アドレスを指定します。
ポート	サーバーへアクセスするためのポート番号を指定します。
ベース DN	ベース識別名を指定します。ベース識別名は、LDAP ツリー
	でユーザーやグループを検索するための基点です。ベース
	DN は、LDAP 表記の完全な識別名で指定する必要があるこ
	とに注意してください(例:
	ou=internet, dc=example, dc=com) $_{\circ}$
バインド DN	LDAP サーバーの認証に使用されるバインド識別名(通常は
	LDAP 管理者)を指定します。バインド DN は
	(CN=administrator,OU=accounts,DC=example,DC=com)の形
	式で指定する必要があります。

フィールド	説明
バインドパスワー	Terminator が認証サーバーと同期するために使用する、バ
F	インドパスワードを指定します。

- すべての詳細を入力してから、[設定のテスト] をクリックします。Terminator は 登録済みの認証サーバーへ接続を試み、成功のメッセージを返します。認証サーバ ーの詳細を保存する前に、ユーザーのグループをインポートまたは削除できます。
   注意:認証サーバーのステータスが OFF の場合、インポートは機能しません。
- 5. [保存] をクリックします。

追加された認証サーバーはすべて、認証サーバーのリストに表示されます。名前、 アドレス、ポート、タイプ、ベース DN、ステータスの概要が表示されます。

ステータスが ON の場合、その認証サーバーは有効で、認証に利用可能です。ステ ータスが OFF の場合、その認証サーバーは無効で、認証に使用できません。

設定済みの認証サーバーからユーザーをインポートまたは削除す る

- 1. Seqrite [Terminator] > [ユーザー管理] > [認証サーバー] ヘログオンします。登 録済みのサーバーのリストが、IP アドレス、ポート、タイプ、ベース DN、ステー タスの詳細を含めて表示されます。
- 2. サーバーが表示されていない場合、右上の [追加] をクリックしてサーバーを追加 します。サーバーの詳細フォームが表示されます。
- 3. サーバーの名前をフォームに入力し、必要に応じて以下のフィールドに他の詳細を 入力します。
- 4. インポート済みのユーザー/グループのリストで、【インポート】 をクリックします。 Terminator が設定済みの認証サーバーへ接続し、ユーザーとグループのリストが表示されます。

インボートユーザー/グループTest		×
認証サーバー		
🖨 🗐 🥁 testou		-
quick 123		
abcd		E
anshaj		
a guideast		
[] _ quick_123		
rahul		Ψ.
選択したユーザー・グループのリスト		
		*
		~
	(D===	+
	1禾仔	++72/2

- 5. 必要に応じて、次の操作のいずれかを行います:
  - i. Terminator ヘグループをインポートするには、グループを選択して【インポート】をクリックします。グループの詳細とユーザーが、Terminator ヘインポートされます。
  - ii. グループを削除するには、グループを選択して [削除] をクリックします。選択 したグループが、Terminator から削除されます。

認証サーバーの削除

- 1. Seqrite [Terminator] > [ユーザー管理] > [認証サーバー] ヘログオンします。登 録済みの認証サーバーのリストが、IP アドレス、ポート、タイプ、ベース DN、ス テータスの詳細を含めて表示されます。
- 2. 削除するサーバーを選択し、[削除] をクリックします。Terminator によりサーバ ーがリストから削除される前に、確認のプロンプトが表示されます。
- サーバーに関連付けられているユーザーを削除するには、ユーザーを選択して [削
   除] をクリックします。認証サーバーに関連付けられているユーザーも、サーバーと同時に削除されます。

### Seqrite Terminator と認証サーバーとの同期

- 1. Seqrite [Terminator] > [ユーザー管理] > [認証サーバー] ヘログオンします。登 録済みのサーバーのリストが、IP アドレス、ポート、タイプ、ベース DN、ステー タスの詳細を含めて表示されます。
- 2. [詳細] をクリックします。

認証サーバー サーバー !				
詳細	細設定		今すぐす	更新
	名前	予定された同期	ログインの同期	
	Test	なし	いいえ	*

3. Terminator と同期するサーバーを選択し、[今すぐアップデート] をクリックしま す。Terminator のユーザーリストが、サーバーのユーザーリストと同期されます。

Segrite Terminator と認証サーバーとの同期のスケジュール

認証サーバーの同期をスケジュールするには、以下の手順に従います:

- 1. Seqrite [Terminator] > [ユーザー管理] > [認証サーバー] > [高度] ヘログオン します。
- 2. [サーバー名] をクリックします。[同期のスケジュール] ダイアログボックスが表示されます。

スケジュール同期	×
名前	Test
スケジュール同期	なし       OO マ HH OO マ MM
ログイン時にバックエンドの同	Ⅰ ログイン時に「自動的にユーザーを同期する」を選択します。
	保存 キャンセル

- 3. [同期のスケジュール] ドロップダウンリストで、必要な同期の周期を選択します。 必要なら、同期の時刻を時間と分で、該当のドロップダウンリストから選択します。
- 4. ログイン時に自動的に同期を有効にするには、[ログイン時にバックエンド同期を 有効にする] オプションを選択します。
- 5. [保存] をクリックします。設定した時間に、Terminator のユーザーリストがサー バーのユーザーリストと同期されます。

インターネットクォータ

インターネットクォータで、グループおよび/またはユーザーのインターネット使用量 を監視し、制御することができます。合計データ転送(アップロード + ダウンロード) またはアップロードまたはダウンロードのどちらかのデータ転送に基づいて、インター ネットクォータポリシーを設定できます。 [インターネットクォータ] ページで、事前に定義されるインターネットクォータポリ シーを作成できます。このポリシーは、グループ/ユーザーに適用されます。グループ/ ユーザーが割り当てられたクォータに達すると、インターネットアクセスがブロックさ れます。

クォータ管理ポリシーを設定する場合:

- 1. Seqrite [Terminator] > [ユーザー管理] > [インターネットクォータ] ヘログオン します。インターネットクォータポリシーのリストと共に [インターネットクォー タ] ページが表示されます。
- 2. インターネットクォータを有効に設定します。

注意:

- インターネットクォータを有効にすると、ネットワークスループットに影響 する可能性があります。
- インターネットクォータを無効にすると、帯域幅使用量レポートが生成されません。

Segrite			🛟 オプション -	<b>?</b> ヘルプ -   也 シ	/ャットダウン   🗗	Admin (管理) -
TERMINATOR		ホーム コン	テンツフィルタリン	グ ユーザー管	理 設定 口	グとレポート
> ユーザー	インターネット	ウォータ				保存
> ゲストユーザー	インターネットクォ	<b>ータ </b> ● 有刻	<b></b>	◎ 無劾		
<ul> <li>シルージ</li> <li>&gt; 時間カテゴリ</li> </ul>	ポリシー					追加 削除
▶ 認証サーバー	□ ポリシー名	タイプ	周期	制限	最大限度	
インターネットクォータ >	🔲 すずぎ	トータル	-0	-	無制限	*
	□ ひろしま	U & D	日々	100   100	無制限   無制限	Į

3. [追加] をクリックすると、[インターネットクォータの追加] ページが表示されま す。

インターネットクォータ >	保存	キャンセル		
ポリシー名:				
クォータタイプ:	◎ 合計クォータ	◉ クォータのアップロード&ダウン		
クォータの頻度:	日々	•		
一日のアップロードの制限:	メガバイト	MB/ユーザー		
一日のダウンロードの制限:	メガバイト	MB/ユーザー		
最大アップロード限度:	◎ 無制限	◉ 制限付ぎ		
	メガバイト	MB/ユーザー		
最大ダウンロード限度:	◉ 無制限	◎ 制限付ぎ		

このページのフィールドの説明を、次の表に示します。

フィールド	説明
クォータタイ プ	合計クォータ(アップロード + ダウンロード)またはアップロードとダウンロードのそれぞれのクォータに基づいて、ポリシーを作成できます。
	合計クォータの場合、アップロードとダウンロードの割合に関わりなく、合計データ量が許可されます。例えば、許可されている合計クォータが 100MB の場合、ユーザーはアップロードとダウンロードの割合に関わりなくそのすべての容量を使用することができます。
	<b>アップロード &amp; ダウンロードクォータ</b> の場合、ユーザーが使用で きる量は、固定されたアップロードとダウンロード量、例えば、 アップロードで 50MB とダウンロードで 50 MB に制限されます。 ユーザーがアップロードとダウンロード使用量のどちらかを使い 果たした場合、アップロードとダウンロードの両方が停止しま す。このページのフィールドの説明を、次の表に示します。アッ プロードとダウンロードのクォータオプションを選択した場合、 選択したクォータ頻度に対し、アップロードとダウンロードのデ ータ制限をそれぞれ指定しなければなりません。
ポリシー名	ポリシー名を入力します。
クォータの頻 度	クォータを更新するサイクル期間を設定できます。インターネットアクセス制限は、最大データ制限により決まります。
	以下のオフションが使用できょう。 1 回:期間に関わりなく設定したデータ量を消費できるワンタイム インターネットアクセス制限を設定できます。例えば、1000MB の データ使用量がユーザーに許可されている場合、この容量を特定 の日/月/年内に消費することができます。 毎日:1 日に適用されるインターネットアクセス制限を設定できま す。
	毎週:週ごとに適用されるインターネットアクセス制限を設定できます。このオプションを選択すると、週の始めの日と週ごとのデ
	ータ制限量(MB)を指定しなければなりません。

フィールド	説明
	毎年:年ごとに適用されるインターネットアクセス制限を設定でき ます。このオプションを選択した場合、年間制限が開始される月 と年間データ制限量を MB 単位で選択する必要があります。
	注意:ある期間に使用されていないデータがあっても、そのデータ は中断されません。例えば、ユーザーが毎日使用できるデータ量 が 100 MB に設定されており、最大使用制限量が 1000 MB である とします。ユーザーが毎日のデータ使用制限量 100 MB のうち 70 MB のデータを消費した場合、残りのデータ使用量は 900 MB では なく、930 MB となります。毎日の使用量ポリシーに基づき、次の 日もそれ以降の日も、ユーザーは 100MB のデータを使用できま す。「1 回」以外の他の頻度でも同じ条件が適用されます。
最大データ制 限	ポリシーに許可される最大データ量です。無制限オプションを選 択することができます。このオプションでは、最大データ使用量 に制限がありません。インターネットにアクセスする際のデータ 量を固定したい場合、制限オプションを選択し、最大限度を MB 単 位で指定します。
最大アップロ ードデータ制 限	クォータタイプでアップロードとダウンロードクォータを選択す ると、この欄が表示されます。これは、ポリシーに許可されるア ップロードデータの最大量です。無制限オプションを選択するこ とができます。このオプションでは、最大アップロードデータ使 用量に制限がありません。 <b>制限</b> オプションを選択し、テキストボ ックスに制限値を入力して、アップロードデータを固定量に制限 することもできます。
最大ダウンロ ードデータの 制限	クォータタイプでアップロードとダウンロードクォータを選択す ると、この欄が表示されます。これは、ポリシーに許可されるダ ウンロードデータの最大量です。無制限オプションを選択するこ とができます。このオプションは、最大ダウンロードデータ使用 量に制限されません。制限オプションを選択し、テキストボック スに制限値を入力して、ダウンロードデータを固定量に制限する こともできます。

4. [保存] をクリックします。

Chapter 7

# コンテンツフィルタリングと保護

ネットワークのユーザーがアクセスすることが望ましくないコンテンツをすべて、フィ ルタリングにより除外できます。コンテンツフィルタリングにより、害意や悪意の有無 に関わらず、セキュリティへの脅威やデータ漏えいからネットワークを保護できます。

この保護機能により、ウェブ脅威をブロックし、マルウェア、ウイルス、フィッシング の攻撃を阻止できます。また、許容されるウェブ使用ポリシーを作成し、強制できます。

以下の Seqrite Terminator 機能は、コンテンツフィルタリングと保護に役立ちます。

- <u>アンチウイルス</u>:システムをスキャンし、ウイルス、トロイの木馬、マルウェア、スパイウェア、および複数の有害なソフトウェアを探します。
- メール保護:受信および送信するメールをすべてスキャンし、ウイルスや脅威、スパム、疑わしい添付ファイル、疑わしいキーワードを探します。
- <u>URL フィルタリング</u>:特定のドメインまたは URL から、特定のウェブサイトへのア クセスを拒否し、受信および送信するすべてのデータについて、セキュリティポリ シーをチェックするのに役立ちます。
- <u>MIME フィルタリング</u>:定義済みの設定に応じて、受信するコンテンツをブロックするのに役立ちます。
- <u>アプリケーションコントロール</u>:安全でない、および生産性が低いアプリケーション を制限します。
- <u>侵入防止システム</u>:組織のネットワークを外部のアプリケーションレベルの攻撃、侵入の試み、マルウェア、脅威から保護します。

コンテンツフィルタリング設定はグローバルで、すべてのユーザーとグループに適用さ れます。

# アンチウイルス

アンチウイルスソフトウェアは、悪意のソフトウェアや、ワーム、トロイの木馬、ルー トキット、スパイウェア、キーロガー、ランサムウェア、アドウェアなどのマルウェア によって引き起こされる感染を防止、検出、削除するために使用されるソフトウェアで す。

[アンチウイルス] ページを使用して、ネットワーク上でアンチウイルスチェックを有 効または無効にできます。ローカルネットワークと HTTPS トラフィックを選択して、 ウイルスをスキャンできます。Terminator がスキャンするファイルのタイプを指定で きます。Terminator が疑わしいファイルや関連する統計をレポートするよう設定でき ます。

1. Seqrite [Terminator] > [設定] > [アンチウィルス] ヘログオンします。

Seqrite <b>TERMINATOR</b>	ホーム	☆ オブション -   ? ヘルブ -   ひ シャットダウン -   → コンテンツフィルタリング ユーザー管理 設定 ロイ	Admin (管理) - グとレポート
> インターネット	アンチウイルス		保存
アンチウイルス ト	ウイルスのスキャン:	<ul> <li>● 有効</li> <li>○ 無効</li> </ul>	
▶ 電子メール保護	トラフィックをスキャン:	🔲 ローカルトラフィックのウイルススキャンを有効にする	
<b>&gt;</b> 定義	スキャナ設定:	● すべてのファ… ○ カスタマイズされたファイルをスキャン	
> ファイアウォール設定	HTTPSトラフィックをスキャン:	♂ HTTPSトラフィックをウイルススキャン	
> IPS		注意: [セキュアなトラフィックをバイバス] が OFF の場合にのみ HTTPS   ャンすることができます。SSL 証明書のインスト ールが必要になる場合	トラフィックをスキ があります。
▶ アブリケーションコントロール			

- 2. ネットワークのウイルスをスキャンするには、 [有効] オプションを選択します。
- 3. ローカルネットワークのウイルススキャンを有効にするには、[トラフィックのス キャン] オプションを選択します。
- [スキャナ設定] オプションを使用して、スキャンするファイルタイプを選択できます。すべてのファイルをスキャンすることも、カスタマイズされたファイルをスキャンすることもできます。カスタマイズされたファイルのオプションを選択すると、ファイルタイプのリストが表示されます。スキャンが必要なファイルタイプを選択します。
- 5. HTTPS トラフィックのスキャンも選択できます。

注意:HTTPS トラフィックは、インターネット設定のセクションで [セキュアなトラ フィックをバイパス] オプションを [OFF] に設定している場合のみスキャンできま す。SSL 証明書のインストールが必要な場合があります(詳細については、<u>インター</u> <u>ネットの設定</u>を参照してください)。

6. [保存] をクリックします。

# メール保護

サイバー侵入は、悪質なファイルや埋め込みリンク、悪質な内容が含まれるメールを使 用してよく行われます。メールで送受信されるコンテンツがネットワークへ適切に分類 されるように保護ポリシーを適用しなければなりません。メールに保護ポリシーを適用 することで、漏洩するデータ量や、ネットワーク上でメールのデータが引き出されるの を最小限に押さえます。メール保護機能は、送受信メールをスキャンしてフィルタリン グし、以下の設定を行います。

- グローバル設定
- アンチウイルススキャニング
- アンチスパムスキャニング
- 添付ファイル管理
- キーワードベースのメールブロック

注意:IMAP サーバーの場合、アンチウイルススキャン機能のみ利用できます。

処置はログが取られ、メールのフィルタリング結果がレポートされます。これらの記録 やレポートは、検査に使用されます。効果的にログを取り、検査することで、セキュリ ティインシデントを特定できるため、管理者はログを確認して、メールが受信拒否にな った理由を知り、メール/コンテンツを許可すべきか判断できます。

### グローバル設定

[グローバル設定] ページで、すべてのタイプのメールスキャニングに適用可能な以下 の設定を行えます。

- メールサーバー SMTP、POP3、および IMAP のリスニングポートとして、メールサ ーバーポートを設定します。
- スキャンされたメールにフッターを追加するよう選択します。
- 通知の送り先のメール ID を入力します。この通知には、疑わしいメールの詳細と 受信拒否されたメールが記載されます。
- ドメイン/メール ID をホワイトリストに加え、該当するドメイン/メール ID の送 受信メールに対し、ウイルス、スパム、添付ファイル管理、およびキーワードブロ ックをスキャンしないようにします。
- ドメイン/メール ID をブラックリストに加え、該当するドメイン/メール ID の送 受信メールを受信拒否します。

メール保護グローバル設定を設定するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [メール保護] ヘログオンします。次のページが 表示されます。

電子メール保護	グローバル設         アンチウ         アンチス           定         イルス         バム	添付ファイルコントロ ール ク
電子メール保護:	● 有効   ○ 無効	
	SWIP     smtp     =   +   iii       POP3     pop3     =   +   iii       IMAP     imap     =   +   iii	ません。
フッター:	<ul> <li>スキャンされたメールにフッターを追加</li> <li>I Virus Free Mail Using Seqrite Termina</li> </ul>	10する ator!
メールIDへ通知:		追加   削除
□ 電子メール	オリジナルメールを転送	
		•
ホワイトリスト:		追加   削除
■ ドメイン / メールID	アンチウイル アンチスバム	添付ファイルコ キーワードブロ
		•
ブラックリスト:		追加   削除
■ ドメイン / メール ID		
		*

- 2. [メール保護] オプションの [有効] を選択します。
- 3. SMTP、POP3、および IMAP にメールサーバーポートを入力します。
- 送受信するすべてのメールメッセージにフッターメッセージを加える場合、[フッ ター]オプションを選択します。指定のテキストボックスで、メールのフッターに 入れたいメッセージを入力します。例えば、メールや添付ファイルがウイルスフリ ーであることを宣言できます。

 感染した疑わしいメールの通知を受け取るメールアドレスを加えることができます。 リストに掲載されたメール ID に、受信拒否された/疑わしいメールを添付ファイル として転送することもできます。[メール ID への通知] セクションで[追加] をク リックします。オリジナルの(疑わしいまたは感染したと思われる)メールを転送 するオプションを選択します。[保存] をクリックします。

注意:メール通知を受信するには、最初に SMTP 設定を行う必要があります。

 ホワイトリストにメールアドレスを追加するには、ホワイトリストセクションで [追加] をクリックします。ホワイトリストのポップアップが表示されます。ドメインまたはメールアドレスをホワイトリストに登録する場合、ホワイトリストタイプを選択します。アドレス欄にドメインアドレス/メールアドレスを入力します。ホワイトリストに登録したいドメイン/メールアドレスのモジュールを選択します。[保存] をクリックします。

注意:SMTP 設定で設定されているメールアドレスがデフォルトでホワイトリストに 登録されています。

- ドメイン/メールアドレスをブラックリストに追加するには、ブラックリストセクションで [追加] をクリックします。メール ID/ドメイン名を入力して、[保存] をクリックします。
- 8. [グローバル設定] ページの右上で [保存] をクリックしてグローバル設定を保存します。

### アンチウイルス

アンチウイルス機能で、送受信されるメールをスキャンすることができます。送信また は受信するどちらかのメールをすべてスキャンするか、または送受信する両方のメール をすべてスキャンするかを選択できます。スキャンできるメールサイズを設定し、サイ ズ制限を超えるメールをウイルススキャンしないように設定することもできます。また、 ウイルスが検出された場合に Terminator が管理者へ通知し、感染したメールに対して 処置を行うように設定できます。

メール保護のためにアンチウイルス設定を行うには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [メール保護] > [アンチウィルス] ヘログオン します。次のページが表示されます。

コンテンツフィルタリング

電子メール保護	<sup>ブローバル</sup> 設 アンチウ アンチス 添付ファイルコントロ キーワードブロッ 定 <b>イルス</b> パム ール ク
アンチウイルス スキャン: スキャンメール:	<ul> <li>● 有効 ● 無効</li> <li>● 受信メール(推奨)</li> <li>■ 送信メール</li> </ul>
スキャン制限:	
検出したウイルスに関する	· 修復 & 送信 ▼
件名夕グ:	✓ [VIRUS REPAIRED]-
管理者に通知	□ 通知を送信
	通知の件名 Mail Protection: Antivirus
	☞ 疑わしいメールを添付で送信
	<b>注意:</b> 電子メール通知を受信するIこは、SMTP設定を行う必要があります。

- 2. アンチウイルススキャニングオプションを有効に設定します。
- 3. 受信するメールまたは送信するメールをスキャンするオプションを選択します。デ フォルトで、受信メールをスキャンするよう設定されています。
- メールのサイズを制限する場合はスキャン制限を設定し、サイズ制限を MB または KB で入力します。指定されたサイズよりも大きいメールについては、ウイルスのス キャンは行われません。

注意:サイズは、メールの MIME サイズです。

- 5. メールで [検出したウイルスに関する処置] を選択します。
  - オリジナルを送信:オリジナルメールが送信されます。このメールはウイルスに 感染している可能性があるため危険です。
  - 修復と送信:このオプションは、悪意のあるメールの修復を試み、受領者に送信 します。
  - 削除と送信:このオプションは、感染した添付ファイルを削除してからメールを 送信します。
  - 送信しない:感染したメールはブロックされます。
- 6. **件名タグ**をスキャンしたメールに挿入するオプションを選択します。指定のテキス トボックスにメールへ挿入したい件名タグを入力します。

- 7. [管理者に通知] オプションを選択して、管理者に感染したメールに関する通知を送 ります。通知メールに件名タグを挿入します。感染した/疑わしいメールを添付して 管理者に送るオプションを選択することもできます。
- 8. [保存] をクリックします。

### アンチスパム

メールのスパムは、一方的に送り付けられる大量のメール(UBE)、ジャンクメール、または一方的に送り付けられる商用メール(UCE)とも呼ばれ、要求されていないメールメッセージを、多くの場合には商業的な内容で、多くの受信者へ無差別に、大量に送り付ける方法です。アンチスパムは、各種の技法を使用して、メールのスパムや、一方的に送り付けられる大量のメールがメールシステムへ入り込むことを防止します。

Seqrite Terminator のアンチスパム機能は、メールをスキャンしてスパムをチェック するために役立ちます。アンチスパムを有効にすると、メールをスパムとみなすのに役 立つスパム対策レベルを設定できます。

注意:この機能は有料で、オプションです。お使いの Terminator のアンチスパム機能 を有効にするには、お客様サポートへ問い合わせてください。

アンチスパムを設定するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [メール保護] > [アンチスパム] ヘログオンし ます。次に示す画面が表示されます。

電子メール保護	グローバル設 アンチウ <b>アンチス</b> 添付ファイルコントロ キーワ 定 イルス <b>バム</b> ール キーワ	ードブロッ ク
		保存
アンチスバム:	● 有効   ○ 無効	
スキャンメール:	☑ 受信メール(推奨)	
	□ 送信メール	
スパム保護レベル:		
	ソフト 適度 厳しい	
スキャン制限:	図 設定された制限より大きい場合、メールをスキャンしない	
	サイズ 5 MB •	
処置:	オリジナルを送信・	
件名9岁:	[SPAM] -	
管理者に通知:	□ 通知を送信	
	通知を送信 Mail Protection: AntiSpam	
	□ 疑わしいメールを添付で送信	
	注意:電子メール通知を受信するには、SMTP設定を行う必要があります。	
スパムブラックリスト:		追加   削除
□ ドメイン/メール ロ		
		<b>^</b>
		-

- 2. [アンチスパム]を [有効] に設定し、すべての受信メールでスパムをスキャンします。
- 3. [メールのスキャン] オプションを選択します。受信メールでのみスパムをスキャン するか、受信メールと送信メールの両方でスパムをスキャンするかを設定できます。
- 4. [スパム対策レベル]を設定します。デフォルトでは、スパム対策レベルは[中]に 設定されており、必要に応じて変更できます。以下のオプションが使用できます。
  - 低:メールは重大度が低い通常のものであることを示します。
  - 中:メールの危険度が中程度であることを示します。かなりの数のメールがスパムとしてタグ付けされます。
  - 高:メールの危険度が高いことを示します。非常に多くのメールがスパムとして タグ付けされます。
- 5. [メールサイズ] のオプションを選択し、メールサイズを指定します。指定されたサ イズよりも大きいメールに対しては、スパムのスキャンが行われません。

注意:注意:サイズは、メールの MIME サイズです。

- 6. 以下の 2 つの処置からスパムメールに適用する処置を選択します。
  - オリジナルを送信:受信者にオリジナルのメールを送信します。
  - 送信しない:SMTP の場合、メールはブロックされます。POP3 の場合、オリジ ナルのメールが件名にスパムタグが挿入されて送信されます。
- 7. スパムメールが検出された場合にメールの件名の先頭に付ける**件名タグ**オプション を選択します。指定されたテキストボックスに件名タグを入力します。
- 8. [管理者に通知] オプションを選択し、スパムメールに関する通知を管理者に送りま す。通知メールに件名タグを挿入します。疑わしいメールを添付して管理者に送る オプションを選択することもできます。
- スパムのブラックリストに、メールアドレスとドメインを追加できます。スパムの ブラックリストに含まれているメールアドレスやドメインから届くメールは、その 内容に関わらずスキャンされます。そのため、このリストに含まれているアドレス やドメインからのメールには「SPAM」のタグが付けられます。この機能は、サーバ ーがオープンリレーを使用し、それが大量メール送信プログラムやウイルスに悪用 されている場合には特に有効にする必要があります。

スパムのブラックリストにメール ID を入力するには、スパムのブラックリストセ クションで [追加] をクリックします。指定のテキストボックスにメール ID を入 力し、[保存] をクリックします。

**10.** [アンチスパム] ページの設定を保存するには、ページの右側で [保存] をクリックします。

### 添付ファイル管理

添付ファイル管理機能は、添付可能なファイルや、SMTP と POP3 でメールを送受信す るファイルをスキャンするために役立ちます。添付ファイルのサイズの制限を指定する ことができます。添付ファイルが指定されたサイズよりも大きい場合、設定された処置 が取られます。この処置は、受信するメールと送信するメールの両方に適用されます。 許可または受信拒否できる添付ファイルの拡張子タイプとコンテンツタイプも指定でき ます。ファイルのコンテンツで、ファイルタイプを特定できます。ファイルの拡張子は 変更することができるため、ファイルタイプと拡張子が一致しない場合は 疑わしいフ ァイルとして受信拒否されます。

添付ファイル管理を設定するには、以下の手順に従います。

1. [Seqrite Terminator]> [設定] > [メール保護] > [添付ファイル管理] ヘログオン します。次に示す画面が表示されます。

コンテンツフィルタリング

電子メール保護	<sup>ブローバル</sup> 設 アンチウ アンチス <b>添付ファイルコント</b> キーワードブロッ 定 イルス パム <b>ロール</b> ク
添付ファイルコントロール: スキャンメール:	<ul> <li>● 有効 ● 無効</li> <li>● 受信メール</li> <li>● 送信メール</li> </ul>
ファイルタイプ:	■ ファイルタイプの名前 説明 ==  +  ■
ポリシー:	<ul> <li>▼</li> <li>※ 添付ファイルのサイズが以下を超えた場合に取る処置</li> <li>サイズ 2 MB ▼</li> <li>◎ 添付ファイルの合計サイズを確認</li> </ul>
処置:	削除と送信    ▼
件名夕グ:	
管理者に通知:	<ul> <li>通知を送信</li> <li>通知の件名</li> <li>Mail Protection: Attachment Control</li> <li>疑わしいメールを添付で送信</li> <li>注意:電子メール通知を受信するには、SMTP設定を行う必要があります。</li> </ul>

- 2. [添付ファイル管理]を [有効] に設定します。
- 3. [メールのスキャン] オプションを選択します。添付ファイル管理のために、受信メ ールのみをスキャンするか、受信メールと送信メールの両方をスキャンするか設定 できます。
- 指定されたサイズのファイルが添付されたメールをスキャンするオプションを選択し、サイズを指定します。指定されたサイズよりも大きなサイズのファイルが添付されたメールが添付されたメールが添付されたファイルの合計サイズを選択することもできます。例えば、2 MB の容量の3 ファイルが添付されたメールがあるとします。この場合、添付ファイルサイズの合計は6 MB となります。

注意:サイズは、メールの MIME サイズです。

5. ファイルタイプを選択します。画面のアイコンでファイルタイプを追加、参照、削除することができます。ファイルタイプには、拡張子とコンテンツタイプが含まれます。

注意:ファイルタイプを削除すると、リストからそのファイルタイプのみが削除され ます。

#### コンテンツフィルタリング

רכ	マイルタイプを参照			×
ファ	イルタイプ:			
	ファイルタイプの名	拡張子	コンテンツタイプ	
	実行可能	.bat,.cmd,.exe	application/bat,a	*
	画像	.gif,.jpeg,.jpg,.pn	image/gif,image/j	
	動画	.mp4,.mpeg,.mp	video/mp4,applic	
	文書	.pdf,.docx,.doc,.xl	application/pdf,a	
	圧縮済み	.7z,.gz,.rar,.tar,.ta	application/x-7z	
				-
			保存 削除 キャンセ	υ

- 6. 以下の 2 つの処置からスパムメールに適用する処置を選択します。
  - オリジナルを送信:オリジナルのメールを送信します。
  - 送信しない:SMTP の場合、メールはブロックされます。POP3 の場合、添付ファ イルなしのオリジナルメールが送信されます。
  - 削除と送信:添付ファイルを削除し、メールを送信します。
- 7. 添付ファイル管理でスキャンされるメールの件名の先頭にタグを付けたい場合、**件 名タグ** オプションを選択します。指定されたテキストボックスに件名タグを入力し ます。
- 8. [管理者に通知] オプションを選択して、悪質なファイルが添付されたメールに関す る通知を管理者に送ります。通知メールに件名タグを挿入します。疑わしいメール を添付して管理者に送るオプションを選択することもできます。
- 9. [添付ファイル管理] ページの右側で [保存] をクリックして設定を保存します。

キーワードブロック

メールの本文と件名でメールコンテンツのフィルタリングを行うことで、より精度の高 いメールのフィルタリングが行えます。暗号化されたコンテンツを使用して、ネットワ ークで発生する通信やネットワークを対象とした通信を制御する可能性のある悪質なコ マンドを非表示にすることができます。例えば、インプラントのコマンドを暗号化して、 メール本文に仕込むことができます。そうした暗号化されたコンテンツが検出されると、 そのメールは受信拒否されます。

キーワードブロック機能は、単語、数字、または頭字語などの文字列を識別します。こ うした文字列は、メールの件名や本文に記載されており、悪意のある通信に使用される 恐れがあります。キーワードブロック機能を使用すると、指定されたキーワードをブロ ックできます。

キーワードのブロックを設定するには、以下の手順に従います:

1. [Seqrite Terminator] > [設定] > [メール保護] > [キーワードブロック] ヘログ インします。[キーワードのブロック] ページが表示されます。

電子メール保護	グローバル設 アンチウ アンチス 添付ファイルコントロ キー <b>フードブロッ</b> 定 イルス パム ール <b>ク</b>
	保存
キーワードブロック:	◎ 有効   ● 無効
スキャンメール:	■ 受信メール
	☞ 送信メール
キーワード・	名前     キーワード     + I I
	-
処置:	送信しない ・
件名夕づ:	KEYWORD MATCHE
管理考虑通知。	□ 通标均许存
日注目に通知。	
	通知の件名 Mail Protection: Keyword Blocking
	☞ 疑わしいメールを添付で送信
	<b>注意:</b> 電子メール 通知を受信するには、SMTP設定を行う必要があります。

- 2. [キーワードブロック]を有効に設定します。
- メールの件名/本文で検索したいキーワードを選択します。画面のプラス (+) アイ コンで新しいキーワードを追加することもできます。このアイコンをクリックする と、[キーワードの追加]のポップアップ画面が表示されます。以下の表は、上記の ポップアップ画面内の記入欄を説明します。

キーワード	×
名前:	
キーワード:	注意:カンマでキーワードを区切ります。
一致オプション:	前方一致   ▼
大文字と小文字を区別	□ 大文字と小文字を区別して検索します
	保存キャンセル

フィールド	説明
名前	キーワード名を入力します。この名前は識別に使用されます。
キーワード	キーワードを入力します。
一致オプション	<b>次で始まる</b> :指定されたキーワードで始まる言葉でメールを検 索します。例えば、「son」というキーワードを入力した場 合、son、sony、sonic などの単語が含まれるメールがブロッ クされ、person、peterson などの単語が含まれるメールはブ ロックされません。
	次で終わる:指定されたキーワードで終わる言葉でメールを検索します。例えば、キーワードとして「son」を追加した場合、sony、sonic などの単語が含まれるメールはブロックされません。しかし、son、person、peterson などの単語が含まれるメールはブロックされます。
	<b>完全一致</b> :キーワードと完全に一致する用語を含むメールを検索します。指定されたキーワードと完全に一致する言葉がメールに含まれる場合、そのメールはブロックされます。 中間:指定したキーワードを含む文でメールを検索します。
十女学と小女学	キーロード検索で十文字と小文字を区別するには、このオプシ
を区別する	マーシート検索で入文子と小文子を区別するには、このオブシ ョンを選択します。例えば、ブロックするキーワードとして 「Ocean」を入力し、大文字と小文字を区別するとしてマーク した場合、OCEAN、oCean、OceAn などの単語はブロックされま せん。

4. 指定されたキーワードが含まれるメールに適用する処置を選択します:

• オリジナルを送信:オリジナルメールを送信します。

- 送信しない:指定されたキーワードが検出されると、そのメールはブロックされます。
- 5. 添付ファイル管理でスキャンされるメールの件名の先頭にタグを付けたい場合、**件 名タグ** オプションを選択します。指定されたテキストボックスに件名タグを入力し ます。
- 6. [管理者に通知] オプションを選択し、キーワードブロックメールに関する通知を管 理者に送ります。通知メールに件名タグを挿入します。疑わしいメールを添付して 管理者に送るオプションを選択することもできます。
- 7. [キーワードのブロック]ページの右側で [保存]をクリックして設定を保存します。

# URL のフィルタリング

次のような理由から、ネットワーク上の一部のウェブサイトをブロックすることが必要 な場合があります:

- コンテンツが不適切で、その性質上不快または違法な可能性がある。
- エンターテイメントのウェブサイトで、コンテンツをストリーミングしているため、 企業の帯域幅の浪費につながる。
- ソーシャルネットワークサイトで、従業員にとって生産的でない。
- 信頼できないウェブサイトで、マルウェア、トロイの木馬、ウイルスが存在する。
- 組織での作業効率を上げるため、利用できるウェブサイトを制限する。

コンテンツフィルタリングでは、ウェブサイトが許可と拒否のカテゴリにグループ分け されます。これらのカテゴリ間でコンテンツに基づいてウェブサイトを移動できます。 例えば、広告、求人、ダウンロードなどのサイトを拒否カテゴリへ移動できます。

### カテゴリに基づいたウェブサイトのブロック (URL 分類)

カテゴリに基づいたブロックでは、そのウェブサイトやページが属するカテゴリに基づ いてウェブサイトをブロックします。ブロックされているページやウェブサイトへアク セスすると、ブロックポリシーに従ってページがブロックされたことを示すメッセージ が表示されます。これは、ポリシー違反レポートのエントリにも記録されます。デフォ ルトの拒否リストには、マルウェア、ボットネット、感染の危険、フィッシング・詐欺 などのカテゴリが含まれます。

ウェブサイトのブロックは、様々な理由で便利です。この機能を使用して、ネットワー クを保護したり、攻撃的なコンテンツを含む不適切なウェブサイトやソーシャルネット ワークサイトなどへのアクセスを防いだりできます。ウェブサイトブロックは限られた サイトへのアクセスを制限するため、組織的作業の効率を高めるのに役立ちます。

カテゴリに基づいてウェブサイトをブロックするには、以下の手順に従います:
1. Seqrite [Terminator] > [コンテンツフィルタリング] > [URL 分類] ヘログオンし ます。[ウェブサイトのブロック] オプションページに、許可および禁止されている ウェブサイトのカテゴリのリストが表示されます。

Searite		🔅 オブション	<b>-   ?</b>	ヘルプ -   😃 シャッ	トダウン	┣ Admin (管理) -
TERMINATOR	ホーム	コンテンツフィルタ	マリング	ユーザー管理	設定	ログとレボート
> コンテンツブロッキング	URL 分類					変更を保存
URL分類 ▶ > カスタマイズブロッキング	URL分類	●有劾 ◎ 無劾				
> ホワイトリスト	許可されたウェブサイトカテ	ゴリー (60)		拒否されたウェブサイ	いのカテゴリ	J — (4 )
> キーワードブロック	□ すべて選択			□ すべて選択		
	□ 広告とポップ・アップ		<b>A</b>	🔲 ボットネット		*
	□ アルコールとタバコ			■ 感染の危険		
	□ アノニマイザ			🔲 マルウェア		
	□ ァート			□ フィッシングと詐欺		
	□ ビジネス					
	□ チャット					
	□ 児童虐待の画像					
	□ コンビュータとテクノロジー	•				
	□ 犯罪活動					
	□ カルト					_
						*

- 2. URL 分類オプションを有効に設定します。
- 3. ブロックするウェブサイトのカテゴリを選択します。[カテゴリで検索] テキストボ ックスに名前を入力し、カテゴリで検索することもできます。
- 右向き矢印ボタンをクリックして、選択したカテゴリを [拒否されるウェブサイト のカテゴリ] リストへ移動します。カテゴリを [許可されるウェブサイトのカテゴ リ] へ移動するには、カテゴリを選択してから左向き矢印ボタンをクリックします。
- 5. [変更を保存] をクリックします。

注意:デバイスがオフラインモードで、ウェブセキュリティサービスがオフラインに 設定されている場合、URL 分類は使用できません。

### ホワイトリスト

ユーザーの職務プロファイルや業務の要件に基づいて、一部のウェブサイトへアクセス を許可できる場合があります。これらのウェブサイトをホワイトリストへ追加すると、 ネットワークのユーザーはリストに含まれているサイトへ必ずアクセスできます。ウェ ブサイトのドメイン名、URL、IP アドレスを追加できます。

ホワイトリストにウェブサイトを追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [コンテンツフィルタリング] > [ホワイトリスト] ヘロ グオンします。このページには、ホワイトリストに追加されているドメイン、ウェ ブサイト、URL のリストが表示されます。

コンテンツフィルタリング

Seqrite <b>TERMINATOR</b>	ホーム	オブション -   ? ヘル     コンテンツフィルタリング	<b>/ブ -   ()</b> シャットダウ: ブ ユーザー管理	ンする <b>-   ┣ Admin (管理) -</b> 設定 ログとレポート
▶ コンテンツをブロックします。	ホワイトリスト			変更を保存する
▶ URL分類	ドメインリスト	追加   削除する	URLリスト	追加 削除する
> カスタマイズブロッキング	■ ドメイン名		🔲 ウェブサイト/URL	
	ドメイン名を入力してくださ	い。保存 ×		*
> キーワートフロック	google.com	*		
	quickheal.com			

- 2. ドメインリストまたは URL リストで [追加] をクリックすると、テキストボック スが表示されます。ホワイトリストに追加するドメイン名、URL、または IP アドレ スを入力します。
- 3. [保存] をクリックします。
- 4. 右上の [変更を保存] をクリックし、変更を保存します。

#### ホワイトリストからウェブサイトを削除する

- 1. Seqrite [Terminator] > [コンテンツフィルタリング] > [ホワイトリスト] ヘログ オンします。このページには、ホワイトリストに追加されているウェブサイトのリ ストが表示されます。
- ホワイトリストから削除するドメイン名、ウェブサイト、または URL を選択し、
   [削除] をクリックします。
- 3. 右上の [変更を保存] をクリックし、変更を保存します。

## ブラックリスト(ブロックのカスタマイズ)

Seqrite Terminator のこの機能を使用して、ネットワークのユーザーによるアクセス が望ましくないサイトをブロックできます。ブロックするサイトを指定するには、その サイトの URL、ドメイン名、または IP アドレスを追加します。

ウェブサイトの URL またはドメイン名をブロックするには、以下の手順に従います:

- 1. Seqrite [Terminator] > [コンテンツフィルタリング] > [ブロックのカスタマイ ズ] ヘログオンします。このページには、ブロックされているウェブサイトのドメ インと URL のリストが表示されます。
- 2. [ドメインリスト] の部分で、[追加] をクリックします。

コンテンツフィルタリング

Seqrite TERMINATOR	<b>*</b> ホーム コン	オブション •   <b>?</b> ^」 テンツフィルタリング	レヺ <del>-</del>   <b>()</b> シャットダウンす ユーザー管理 言	する   - ➡ Admin (管 役定 ログとレポー	理) - ート
> コンテンツをブロックします。	カスタマイズブロッキング			変更を保存	する
▶ URL分類	ドメインリスト	追加   削除する	URLリスト	追加   肖鹏	余する
	□ ドメイン名		🗌 ウェブサイト/URL		
> ホワイトリスト > キーロービブロック	ドメイン名を入力してください。保存	×	ここにURLを入力する	保存	×
· +->-r>uwy	facebook.com	~	chrome.goolge.com/we	ebstore/category/a	~
	linkedin.com				

3. 指定のテキストボックスに、ブロックするドメイン名または IP アドレスを入力し ます。例えば、「google.com」と入力します。URL または IP アドレスをブロック するには、[ウェブサイト/URL] リストの下に URL または IP アドレスを追加しま す。

ウェブサイトや URL を「http://」付きで入力すると、その部分が取り除かれてか らリストへ追加されます。

4. [保存] をクリックします。ブロックされるドメイン名のリストへ、そのドメイン名 または URL が追加されます。

## ブロックされるリストからウェブサイトの URL またはドメイン名を削除 する

ブロックされるリストから URL またはドメイン名を削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [コンテンツフィルタリング] > [ブロックのカスタマイズ] ス] ヘログオンします。[ブロックのカスタマイズ] オプションページに、ブロック されているウェブサイトのドメインと URL のリストが表示されます。
- 2. [ドメインリスト] の部分で、ブロックリストから削除するウェブサイトまたは URL を選択し、[削除] をクリックします。
- 3. [変更を保存] をクリックします。ブロックされているドメイン名のリストから、そのドメイン名または URL が削除されます。

## MIME フィルタリング

Seqrite Terminator のコンテンツのブロック機能を使用し、ファイルタイプに基づい てコンテンツをブロックできます。MIME タイプまたは拡張子に基づいてファイルをブ ロックできます。一部の MIME タイプはカテゴリにグループ分けされています(例: Audio-.WMV、.WMA、.MP4、.MP3)。

指定したカテゴリのファイルタイプを、ネットワーク上で許可または拒否できます。 [カスタムのカテゴリ] リストでは、特定の拡張子を追加または削除できます。[許可さ れるカテゴリ] にマークされているコンテンツは、ユーザーに対してブロックされません。ただし、拒否されるカテゴリおよびカスタムのカテゴリのコンテンツはすべて、ユ ーザーに対してブロックされます。

## デフォルトの MIME フィルタリング

MIME タイプをブロックまたはブロック解除するには、以下の手順に従います:

1. Seqrite [Terminator] > [コンテンツフィルタリング] ヘログオンします。[コンテ ンツのブロック] ページが表示されます。このページには、許可および拒否される カテゴリのリストが表示されます。

Searite		🔅 オプション 🗸	?	ヘルブ -   😃 シャット	ダウン 👻	┣ Admin (管理) -
TERMINATOR	ホーム	コンテンツフィルタリン	ノグ	ユーザー管理	設定	ログとレポート
コンテンツブロッキング ト	コンテンツブロッキング					変更を保存
<ul> <li>ウェブサイトブロッキング</li> <li>カスタマイズブロッキング</li> </ul>	許可されたカテゴリー(8)			否定されたカテゴリー □ すべて選択	(0)	
<ul> <li>ホワイトリスト</li> <li>キーワードブロック</li> </ul>	<ul> <li>■ アプリケーション</li> <li>■ オーディオ</li> </ul>	<b>^</b>	•			<u>ـ</u>
	<ul> <li>フラッシュ_ファイル</li> <li>フラッシュ_ビデオ</li> </ul>		+			
		•				Ŧ
	カスタムカテゴリ	追加 削除				
		*				

- [許可されるカテゴリ]から、拒否するコンテンツタイプを選択し、右向き矢印ボタンをクリックして [拒否されるカテゴリ]リストへ移動します。同様に、[拒否されるカテゴリ]から [許可されるカテゴリ] ヘコンテンツカテゴリを移動するには、コンテンツタイプを選択し、左向き矢印ボタンをクリックします。
- 3. [変更を保存] をクリックします。

## カスタムの MIME フィルタリング

ブロックする必要のあるファイルタイプの拡張子を追加できます。拡張子は、ドットなしで入力します。例えば、「exe」や「tar」の形式で入力します。

ブロックするカスタムのファイル拡張子を追加するには、以下の手順に従います:

1. Seqrite [Terminator] > [コンテンツフィルタリング] ヘログオンします。[コンテ ンツのブロック] ページに、許可および拒否されるカテゴリのリストが表示されま す。

#### コンテンツフィルタリング

Seqrite <b>TERMINATOR</b>	ホーム コン	☆ オブション ▼   *	? ヘルブ -   <b>⊍</b> シャッ  グ ユーザー管理	・ダウン ->   <b>-&gt;</b> Admin (管理) - 設定 ログとレポート
<ul> <li>コンテンツブロッキング</li> <li>&gt; ウェブサイトブロッキング</li> <li>&gt; カスタマイズブロッキング</li> <li>&gt; ホワイトリスト</li> <li>&gt; キーワードブロック</li> </ul>	コンテンツブロッキング 許可されたカテゴリー(8) すべて選択 アブリケーション オーディオ フラッシュ_ファイル フラッシュ_ビデオ		否定されたカテゴリー ■ すべて選択 →	変更を保存 -(0) 
	<b>カスタムカテゴリ</b> <ul> <li><b>拡張子</b></li> <li>拡張子を入力してください 保</li> <li>.exe</li> <li>.tar</li> </ul>	追加   削除 存 ×		

- 2. [カスタムのカテゴリ] リストで [追加] をクリックし、ブロックするファイルの拡 張子を指定のテキストボックスへ入力します。[保存] をクリックして、カスタムの カテゴリをリストに保存します。
- 3. [変更を保存] をクリックし、追加したカテゴリまたはファイルタイプを保存します。

カスタムのファイル拡張子をブロックから取り除く

- 1. Seqrite [Terminator] > [コンテンツフィルタリング] ヘログオンします。[コンテ ンツのブロック] オプションページに、許可および拒否されるカテゴリのリストが 表示されます。
- 2. [カスタムのカテゴリ] リストで、ブロックリストから削除する拡張子タイプを選択 し、[削除] をクリックします。
- 3. [変更の保存] をクリックして変更を保存します。

キーワードブロック

キーワードは単語、数値、頭字語などの文字列で、検索エンジンにより検索できるもの、 またはウェブサイトの URI に含まれているキーワードです。Seqrite Terminator では、 キーワードに基づいて HTTP/HTTPS コンテンツをブロックできます。

キーワードのブロック機能を使用すると、検索エンジンや、ウェブサイトの URI のキ ーワードをブロックできます。例えば、キーワードのリストに「Hacking」を追加する と、検索エンジンでそのキーワードがブロックされるか、または URI アドレスに 「Hacking」というキーワードを含むウェブサイトがブロックされます。

キーワードのブロックを設定するには、以下の手順に従います。

- 1. [Seqrite Terminator ] > [コンテンツフィルタリング] > [キーワードのブロック] ヘログオンします。[キーワードのブロック] ページが表示されます。
- 2. [追加] をクリックします。テキストボックスにキーワードを入力します。

Seqrite <b>TERMINATOR</b>	ホーム	☆ オプション -   ?	ヽ <b>ルブ -   ()</b> シャット ユーザー管理	ダウン -   <mark>-&gt;</mark> Admin (管理) - 設定 ログとレポート
<ul> <li>コンテンツブロッキング</li> <li>URL分類</li> <li>カスタマイズブロッキング</li> <li>ホワイトリスト</li> <li>キーワードブロック ▶</li> </ul>	<ul> <li>キーワードブロック</li> <li>検索キーワード</li> <li>キーワードリスト</li> <li>すべて選択</li> <li>キーワードの入力</li> <li>さむらい</li> <li>すずぎ</li> </ul>	<b>へ</b> 保存	追加	保存   削除   インボート   エクスボート ×
	<ul> <li>ひろしま</li> <li>検索タイプ</li> <li>キーワードー致オプション</li> <li>大文字と小文字を区別する</li> </ul>	<ul> <li>検索エンジン</li> <li>リロロ</li> <li>サーワード全体</li> <li>前方一致</li> <li>後方一致</li> <li>サーワードを含む</li> <li>大文字と小文字を区別して</li> </ul>	「検索します	

3. [保存] をクリックすると、キーワードがリストに追加されます。

注意:.csv ファイルからキーワードのリストをインポートすると、複数のキーワードを追加できます。また、.csv ファイルフォーマットでキーワードをエクスポートすることもできます。

4. このページのフィールドの説明を、次の表に示します:

フィールド	説明
ルックアップタ	検索エンジンと URI のどちらでキーワードをブロックするか
イプ	を選択します。
キーワードー致	単語全体:キーワード全体が同じである検索クエリやウェブサ
オプション	イトの URI をブロックします。
	次で始まる:指定されたキーワードで始まる単語の検索クエリ や URI をブロックします。例えば、キーワードとして「son」 を追加した場合、sony、sonic などの単語は検索および URI か

	らブロックされ、person や peterson などの単語はブロック されません。
	次で終わる:指定されたキーワードで終わる単語の検索クエリ や URI をブロックします。例えば、キーワードとして「son」 を追加した場合、sony や sonic などの単語は検索および URI からブロックされません。しかし、person や peterson など の単語はブロックされます。
	<b>次を含む</b> :キーワードを含む検索やウェブサイトの URI をブロ ックします。
大文字と小文字 を区別する	キーワード検索で大文字と小文字を区別するには、このオプシ ョンを選択します。例えば、ブロックするキーワードとして 「Ocean」を追加し、大文字と小文字を区別するとしてマーク した場合、OCEAN、oCean、OceAn などの単語はブロックされま せん。

注意:HTTPS キーワードをブロックするには、「HTTPS トラフィックのウイルス をスキャンする」を有効にする必要があります(詳細については、<u>アンチウィル</u> <u>ス</u>.を参照してください)。

## アプリケーションコントロール

Seqrite Terminator のアプリケーションコントロールは、監視対象のネットワーク環 境で安全でない、および生産性が低いアプリケーションを制限し、インターネット帯域 幅の消費を削減するために使用します。800 を超えるアプリケーションのデータベース が用意されており、ネットワーク管理者はこれらのアプリケーションをブロックできま す。これらのアプリケーションにはウェブベースのものと、スタンドアロンのアプリケ ーションがあります。さらに、これらの動作はログへ記録されるため、動作の追跡やト レースに役立ちます。

アプリケーションコントロールを有効にするには、以下の手順に従います:

1. Seqrite [Terminator] > [設定] > [アプリケーションコントロール] ヘログオンし ます。[アプリケーションコントロール] 画面が表示されます。

### コンテンツフィルタリング

Seqrite			🌞 オプション -   <b>?</b> ^	ルプ・  🕛 シャット	ダウン   📑 Admin (管理)
TERMINATOR		ホーム コン	ノテンツフィルタリング	ユーザー管理	設定 ログとレポート
<ul> <li>インターネット</li> </ul>	アプリケーシ	ョンコントロール			保存
	アプリケーション	/⊐:/⊦ถ−ル 0	有劾 💿 無劾		
▶ 電子メール保護			-		
<b>&gt;</b> 定義	アブリケーショ:	ン名で検索	Q		
> ファイアウォール設定	コントロールされ	いたアプリケーション			
> IPS	晤 🔻 🏾 ア	ブリケーション	カテゴリ 🔻	説明	
アプリケーションコントロール	A	P	ブロトコル	ウェブサーバーと	<u>と</u> サーブレットリポジトリ。
	) AI	mazon	ショッピング	書籍、その他の	多くの商品を扱うオンラ
> IPSec VPN	A	NSA Notify	プロトコル	ANSA Rex プロト:	コル通知。
> PPTP VPN		ople アップデート	コンビュータとテクノロジー	Apple のソフトウ	ェアアップデートツール。
> SSL VPN	) A	vira ダウンロード/	コンビュータとテクノロジー	Avira Antivirusン	フトウェアのダウンロー
	) Ba	ackpack	コンビュータとテクノロジー	ビジネスを中心と	する情報管理とソーシ
	) Bi	ng	検索エンジンとポータル	Microsoft のイン	ターネット検索エンジン。
> IPV6	) BI	TS	プロトコル	Microsoft更新ブ	ログラム向けのファイル
> ルーティンク	) C/	AICCI	コンビュータとテクノロジー	Computer Associ	atesシステム間の通信。
> DNS					
> DHCP	***. ¬-1114-				
→ ダイナミックDNS	L思: アンワクト	-ンヨノコノトロール?	「月20月9月~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	スルーンツトル記留す	マリ月87生かめツます。

- アプリケーションコントロール機能を有効または無効にするには、[有効] または [無効] ラジオボタンをクリックします。
- 3. デフォルトでは、コントロール対象のアプリケーションすべてが許可されています。 ブロックするアプリケーションの名前を選択します。
- 4. [保存] をクリックします。選択したアプリケーションがブロックされます。

# 侵入防止システム (IPS)

侵入防止システムは、組織のネットワークを外部のアプリケーションレベルの攻撃、侵入の試み、マルウェア、脅威から保護する、ネットワークセキュリティシステムです。 IPS は、受信するネットワークトラフィックを監視し、脅威の可能性を識別して、あら かじめ設定されているルールに従って処理します。IPS は、悪意のものと判定したパケ ットをドロップし、それ以後にその IP アドレスまたはポートからのトラフィックをす べてブロックすることがあります。

Seqrite Terminator には侵入防止システム(IPS)が搭載されており、攻撃者がシステムの脆弱性を悪用してアプリケーションやマシンを中断またはコントロールしようとする試みを監視して、ブロックします。IPS には、あらかじめシグネチャの組が設定されており、ネットワークへ到着するデータパケットのシグネチャと一致が行われます。受信したシグネチャのいずれかが既存のシグネチャと一致した場合、Terminator はそのパケットをドロップするか、アラームをセットアップします。

Seqrite IPS は、事前のプログラムによって次のようなアクションを実行できます。

- 悪意のある IP アドレスから送信された、悪意のトラフィックをブロックし、ドロ ップする。
- 悪意のある IP やネットワークをブラックリストとしてマークする。
- 正常な IP やネットワークをホワイトリストとしてマークする。
- 各種の悪意の動作からネットワークを保護する。

## デフォルトのルール

IPS を設定するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [IPS] ヘログオンします。次に示すようなページに、シグネチャグループ、現在のステータス、アクション、説明のリストが表示されます。

Sparito			🔅 オブ	ション -   ? ^	ルプ・  🕛 シャットク	ジウン ▼   📑 Admin (管理) ▼
TERMINATOR	T	к-Д	コンテンツフ	マルタリング	ユーザー管理	設定 ログとレポート
> インターネット	IPS					設定詳細
> アンチウイルス						保存
▶ 電子メール保護	IPS ®	有効	◎ 無効			
▶ 定義	シグネチャー					
> ファイアウォール設定	グループ名		ステータス	アクション	説明	
IPS <b>&gt;</b>	ActiveX		オン	廃棄する ▼	ActiveXコンポーネ	ントの脆弱性シグネチャ
▶ アプリケーションコントロール	攻撃レスポンス		オン	廃棄する ▼	攻撃応答をブロッ	クするためのルール
> 証明書	Botcc Portgrouped		オン	廃棄する ▼	Shadowserver.org	および Abuse.ch によっ…
> IPSec VPN	ボットネット		オン	廃棄する ▼	ボットネットワーク	セキュリティ脅威をブロ
> PPTP VPN	チャット		オフ	警告 ▼	様々なチャットの>	シャセンジャーのための…
> SSL VPN	Ciarmy		オン	廃棄する ▼	トップ攻撃者を特別	言されたCiarmy.comを
> インターフェース	感染の危険のある柿	자	オン	廃棄する ▼	敵対的または侵害	『のホストをブロックす…
> IPv6	最新の出来事		オン	廃棄する ▼	現在イベントのル	ール
▶ ルーティング	DNS		オン	廃棄する ▼	DNSI攻撃防止の規	浿」
> DNS	DOS		オン	廃棄する ▼	インバウンドのD೦	s活動のためのルール
> DHCP						

- 2. 表示されるシグネチャグループについて、必要に応じてステータスとアクションを 設定します。アクションは、次のいずれかに設定できます。
  - アラート:トラフィックはネットワークに流入を続けますが、[ログとレポート] にアラートとして表示されます。
  - 廃棄有害なトラフィックがブロックされ、[ログとレポート] にブロック済みと して表示されます。

3. [保存] をクリックします。

#### カスタムのルール

Seqrite Terminator IPS の既存のシグネチャに新しいシグネチャを追加する、または 独自のカスタムのシグネチャを追加することが必要な場合があります。この操作は、 [IPS] ページの [詳細] タブで行います。

侵入防止のためにカスタムのシグネチャを追加するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [IPS] > [高度] ヘログオンします。[カスタム IPS] 画面が表示されます。

IPS				設定詳細な
カスタムIPS				追加 削除する
■ 署名 7	マテータス	説明		
Test	オン	試験概要	要	*
				-
ホワイトリスト/ブラックリスト				
🔲 ホワイトリスト	追加」	削除する	🔲 ブラックリスト	追加」削除する
12.1.1.1/16		*	1.1.1/16	*
		$\nabla$		Ŧ
ログを設定する				保存
ホワイトリストのログを有効にする				
ブラックリストログを有効化	<b>V</b>			
スキャンの種類				保存
✓ WANからの交通				
🔲 WANからの交通				
🔲 LAN内の交通				

2. [追加] をクリックします。カスタム IPS のシグネチャ画面が表示されます。

	ホーム	☆ オブション -   ? ヘルブ コンテンツフィルタリング	▼   <b>()</b> シャットダウ ユーザー管理	ンする - I 設定	▶ 管理 (管理) ▼
IPS > 新しい				保存	キャンセル
署名:					
説明:					
カスタムルール:					
		テスト署名			
	<mark>IPS &gt; 新しい</mark> 署名: 説明: カスタムル <i>ー</i> ル:	ホーム IPS > 新しい 署名: 説明: カスタムルール:	* オブション・ ! ? ヘルブ         ホーム       コンテンツフィルタリング         IPS > 新しい         署名:         説明:         カスタムルール:         テスト署名	★ オブション -   ? ヘルブ -   ④ シャットダウ     ホーム コンテンツフィルタリング ユーザー管理     IPS > 新しい     習名:     説明:     カスタムルール:     テスト署名	☆ オブション -   ? ヘルブ -   ④ シャットダウンする -   ホーム コンテンツフィルタリング ユーザー管理 設定   IPS > 新しい   深名:   説明:   カスタムルール:   テスト署名

3. シグネチャ名、説明、およびシグネチャを、[カスタムルール] テキストボックスに 入力します。

注意:シグネチャの意味を明確にするため、シグネチャ名は一意にする必要がありま す。シグネチャは次のフォーマットにする必要があります。

alert/drop <プロトコル> <ソース IP> <ソースポート> -> <宛先 IP> <宛先ポート > (msg:"<署名が一致したときに表示されるメッセージ>"; content:"<パケットの一 致するコンテンツ>"; sid:"<0 to 4294967295>")

注意:シグネチャの基準には、キーワード:"値"形式の各種のパラメータを含めることができます。

シグネチャが有効で、スペルや構文の誤りを含まないように注意してください。

- 4. [シグネチャのテスト] をクリックして、シグネチャをテストします。これでシグネ チャが有効かどうかわかります。
- 5. シグネチャが検証されたら、[保存] をクリックして Terminator ベータベースへ追加します。

#### ホワイトリスト/ブラックリスト

インターネットの用語では、ホワイトリストとは無害または正当なものとみなされる IP アドレスのリストを指す一般的な名前です。ホワイトリストは、ネットワークセキ ュリティシステムで、ユーザーがパケットをやり取りする IP アドレスのリストを作成 するために多く使用されます。このリストに含まれているアドレスから受信したパケッ トは、フィルタリングにより除外やブロックされることなく、宛先への配信が許可され ます。

ブラックリストには、システムの脆弱性の悪用、脅威の危険性、または侵入者として知られている IP アドレスのリストが含まれています。ブラックリストの目的は、侵入者や、悪意のものと疑われるサイトが、ネットワークのマシンと通信を試みることを防止することです。このリストに含まれている IP アドレスは、ネットワークとの接続を許

可されません。Terminator の IPS ホワイトリストやブラックリストに、IP アドレス を追加や削除できます。

#### ホワイトリスト/ブラックリストへの IP アドレスの追加

ホワイトリスト/ブラックリストに IP アドレスを追加するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [IPS] > [高度] ヘログオンします。[カスタム IPS] 画面が表示されます。
- ホワイトリストに IP アドレスを追加するには、[ホワイトリスト]のセクションで
   [追加]をクリックします。同様に、ブラックリストに IP アドレスを追加するには、
   [ブラックリスト]のセクションで
   [追加]をクリックします。

ホワイトリスト/ブラ	ラックリスト					
🔲 ホワイトリスト		追加   削除する	🔲 ブラックリスト		追加 削除す	する
	/ 255.255.0.0	▼ 保存× <sup>^</sup>		/ 255.255.0.0	▼ 保存×	*
-						
		-				-

- 3. IP アドレスを追加し、対応するサブネットを選択します。
- 4. [保存] をクリックします。IP アドレスが該当のリストに追加されます。

### ホワイトリスト/ブラックリストからの IP アドレスの削除

ホワイトリスト/ブラックリストから IP アドレスを削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [IPS] > [高度] ヘログオンします。[カスタム IPS] 画面が表示されます。ホワイトリスト/ブラックリストに、リストへ追加済み の IP アドレスが表示されます。
- 2. リストから削除する IP アドレスを選択し、[削除] をクリックします。該当のリストから、IP アドレスが削除されます。
- 3. [保存] をクリックします。

#### ホワイトリスト/ブラックリストでログを有効にする

- 1. Seqrite [Terminator] > [設定] > [IPS] > [高度] ヘログオンします。[カスタム IPS] 画面が表示されます。
- 2. [ログ設定]の部分で、有効にするログを選択します。ブラックリストとホワイトリ ストの両方でログを有効にするには、両方のオプションを選択します。

ログ設定	保存
ホワイトリストログを有効化	
ブラックリストログを有効化	

3. [保存] をクリックします。

## スキャンするトラフィックタイプの設定

組織では、インターネットのすべての送信および受信トラフィックや、イントラネット のトラフィックを監視することが必要な場合があります。この機能を使用して、すべて の、または個々のトラフィックタイプを監視できます。各タイプのトラフィックのスキ ャンを設定するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [IPS] > [高度] ヘログオンします。[カスタム IPS] 画面が表示されます。
- 2. [スキャンタイプ] 領域で、Terminator によりスキャンするトラフィックのタイプ を選択します。

スキャンの種類	保存
WANからのトラフィック	
🔲 พลทกตรรวกษา	
■ LAN内のトラフィック	

デフォルトでは、受信トラフィック、つまり WAN から到着するトラフィックのスキャンが選択されています。

3. [保存] をクリックします。

## Chapter

# デバイスの管理

## 管理者

Seqrite Terminator の[管理] ページでは、Terminator の外観と操作性のカスタマイ ズ、ランディングメッセージの提供、およびセッションのタイムアウトの設定を行うオ プションが提供されます。このページでは、管理者プロファイルの追加、管理者設定お よび SMTP 設定の管理も行えます。

[管理] ページには、次のサブオプションがあります。

- <u>日時</u>:アプライアンスの日時を変更する。
- ポータルをカスタマイズ:要件に従いウェブポータルをカスタマイズする。
- <u>管理者設定</u>:アプライアンスアクセスの設定、管理者ユーザーの追加、パスワー ドの強度の設定を行う。
- <u>管理者プロファイル</u>:アクセスのレベルが異なる、新しい管理者プロファイルを 追加する。
- SMTP 設定:SMTP サーバーのパラメータを設定する。

## 日時の設定

各種の地域設定に応じてアプライアンスの日時を設定することや、NTP サーバーと同期 することができます。

日時を設定するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [管理] > [日時] ヘログオンします。

このページのフィールドの説明を、次の表に示します。

フィールド	説明
現在の時刻	アプライアンスの現在のシステム時刻が表示されます。

デバイスの管理

タイムゾーン	アプライアンスが展開されている地域に従い、タイムン 択します。	バーンを選		
日時の設定	<ul> <li>手動:ドロップダウンから日時を選択します。</li> </ul>			
	現在の日付: 2015-11-20 15:12:06			
	タイムゾーン: Asia/Tokyo 🔻			
	日付と時刻の設定: ● マニュアル ● NTPサーバーと	:同期		
	<b>日付:</b> 20 ▼ 11 月 ▼ 時初: 15 ▼ 時 12 ▼	2015 <b>▼</b> 分		
	<ul> <li>NTP サーバーと同期:このオプションを選択すると、アプライアンスの時刻が NTP サーバーと自動的に同期されます。 asia.pool.ntp.org や in.pool.ntp.sorg など定義済みの NTPサーバーを使用して時刻を同期するか、新しい NTP サーバーを追加します。</li> </ul>			
今すぐ同期	このボタンを使用して、リストに含まれている NTP サー プライアンスのクロックとを同期します。最も時差の少 サーバーと日時が同期されます。	ーバーとア >ない NTP		

2. [保存] をクリックします。

注意:変更された日時は、以前に作成されたレポートには反映されないため、レポート の時刻に不整合が発生することがあります。

## 管理者設定

アプライアンスのアクセスポートの制御や、管理グループへのユーザーの追加を行えま す。[管理者設定]ページを使用して、次の操作を実行できます。

- 選択したプロトコルを使用した WAN 経由での Terminator へのアクセスを制限 する。
- パスワードの強度を強または弱に設定する。
   注意:パスワードの強度の設定は、Terminatorのすべてのモジュールに適用されます。

 管理者リストの管理、すなわち管理者ユーザーの追加、削除、または強制ログア ウトを行う。

#### 管理者アクセスの設定

管理者に対するアプライアンスアクセスを設定するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [管理] > [管理者設定] ヘログオンします。[管 理者設定] ページが表示されます。このページの管理者リストには、管理者として ログインしているユーザーの数が表示されます。

管理	日時 ポータルをカスタマ	7イズします <b>管理者設定</b> 管理ブロファイル SMTP設定
アブライアンスアクセス	: 🗹 HTTP 88 🗹	保存 WANIこよってアクセスを許可します
	✓ HTTPS 543	WANによってアクセスを許可します
バスワードの強度:	● 強い   ○ 弱い	6~20記号と数字を組み合わせた強力なバスワードを使用し てください。
管理者リスト		追加   削除   ログアウト
🗌 ユーザー名	プロファイル	ステータス
admin	Super Admin	ログインされました - 書き込みアクセス

2. 次のフィールドを使用して、WAN 経由のアクセスのタイプを選択します。

フィールド	説明
プロトコル	HTTP と HTTPS からプロトコルを少なくとも 1 つ選択します。
ポート	Terminator ヘアクセスするためのポート番号を入力します。デ フォルトは 88 で、利用可能なポート番号のどれにでも変更でき ます。
WAN	このオプションを使用して、選択したプロトコルを使用する WAN 経由のアプライアンスアクセスを有効または無効にします。

3. 必要に応じて、[パスワードの強度]を選択します。強力なパスワードには、数字 と特殊文字を組み合わせた 6 ~ 20 文字の文字列を使用してください。

## 管理者の追加

管理者を追加するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [管理] > [管理者設定] ヘログオンします。[管 理者設定] ページが表示されます。 2. [管理者リスト]の[追加]をクリックします。管理者の追加ページが表示されます。

管理 > 追加		(	保存(キャンセル)
ユーザー名:			
本名:			
パスワード:			
パスワードの再入力:			
プロファイルタイプ:	Administrator	T	
ステータス:	◉ 有効 ◎ 無効		
電子メール:			と連絡先電話番号
連絡先番号:		ן וגאעק (,) מענען (,) מענען (	ξġ 。
⊐メント:			

このページのフィールドの説明を、次の表に示します。

フィールド	説明
ユーザー名	ユーザー名を入力します。管理者は、このユーザー名を使用し て Terminator ヘログインします。
本名	管理者ユーザーの本名を入力します。ユーザー名と本名が同一 である必要はありません。
パスワード	パスワードを入力します。
パスワードの確 認	確認のため、パスワードを再入力します。
プロファイルタ イプ	ドロップダウンリストから、プロファイルタイプを選択しま す。
	管理者:この管理者ユーザーには Terminator の読み取り/書き 込みアクセスが与えられます。
	読み取り専用:この管理者ユーザーには Terminator の読み取り 専用アクセスが与えられます。
	(詳細については、 <mark>管理者プロファイル</mark> を参照してください)。
ステータス	管理者のステータスを選択します。ステータスが [無効] の管 理者はログインできません。

デバイスの管理

フィールド	説明
メール	メールアドレスのコンマ区切りリストを入力します。
連絡先電話番号	連絡先電話番号のコンマ区切りリストを入力します。
コメント	管理者ユーザーの説明を入力します。

3. [保存] をクリックします。

#### 管理者の削除とログアウト

- 1. [スーパー管理者] > [設定] > [管理] > [管理者設定] から Seqrite Terminator ヘログオンします。[管理者設定] ページが表示されます。管理者リストに、管理者 としてログインしているユーザーの数が表示されます。
- 2. 削除またはログアウトする管理者ユーザーを選択し、必要に応じて [削除] または [ログアウト] をクリックします。
- 3. [保存] をクリックします。

## 管理者プロファイル

このセクションでは、ウェブ管理者プロファイルを管理できます。ウェブ管理者ユーザ ーが持つ権限を定義できます。このセクションを使用して、管理者プロファイルを作成、 編集、削除できます。定義済み管理者プロファイルには3種類あります。

**スーパー管理者**:このユーザータイプはポータルへの完全アクセス権を有しており、シ ステムにあらゆる変更を加えることができます。

**管理者**:このユーザータイプは、ポータルへの完全アクセス権を有しています (システム設定以外)。

読み取り専用:このユーザータイプは、ウェブポータルのすべてにおいて閲覧のみ可能 で、作成、編集、削除のようなシステムの変更はできません。

これらの管理者プロファイルは、次に示すように、管理者の追加ページにあるプロファ イルタイプのリストに表示されます。

Seqrite <b>TERMINATOR</b>	赤	♣ オブション -   ? ヘルブ -   ● シャットダウン -   → Ac ム コンテンツフィルタリング ユーザー管理 設定 ログ	dmin (管理) → とレポート
<ul> <li>・ インターネット</li> <li>・ アンチウイルス</li> </ul>	管理	日時 ボータルをカス 管理者設定 <b>管理ブロファイル</b>	SMTP設定 追加   削除
▶ 電子メール保護	□ プロファイル名	説明	
 > 完盖	Administrator	このユーザータイプは、ボータルへの完全アクセス権を有し…	
・ <sup>ルーチル</sup> <b>&gt;</b> ファイアウォール設定	Readonly	このユーザータイプは、ウェブポータルのすべてにおいて閲	
> IPS	Super Admin	このユーザータイブはボータルへの完全アクセス権を有して	

## 管理者プロファイルの作成:

管理者プロファイルを作成するには、以下の手順に従います。

- 1. [スーパー管理者] > [設定] > [管理] > [管理者プロファイル] から Seqrite Terminator ヘログオンします。
- 2. [追加] をクリックして、新しい管理者プロファイルを追加します。モジュールのリ ストが表示されます。
- 3. 新しいプロファイルの [プロファイル名] を入力します。
- 4. 指定のテキストボックスに [説明] を入力します。

管理 > 追加			保存(キャンセル)
プロファイル名: 説明:		2	
モジュールのリスト	読み取り専用	読み取り/書き込み	
コンテンツフィルタリング	۲	0	
コンテンツブロッキング	۲	0	
ウェブサイトブロッキング	۲	0	
カスタマイズブロッキング	۲	0	
ホワイトリスト	۲	0	
キーワードブロック	۲	0	
ユーザー管理	۲	0	
ユーザー	۲	0	
グループ	۲	0	
時間カテゴリ	۲	0	
認証サーバー	۲	0	
ゲストユーザー	۲	0	
インターネットクォータ	۲	0	
設定	۲	Θ	
インターネット	۲	0	
アンチスパム	۲	0	······

5. モジュールのリストで、新しいプロファイルがアクセスできるモジュールを選択し ます。このリストには、Terminator の様々なモジュールに対する権限レベルが表示 されます。各モジュールについて [読み取り専用] または [読み取り/書き込み] を 選択し、新しい管理者プロファイルに対して、そのモジュールへのアクセスを許可 します。 読み取り専用アクセス:ページを参照できます。

読み取り/書き込みアクセス:作成、編集、削除など、システムへの変更を加えるこ とが許可されます。

6. [保存] をクリックします。

## 管理者プロファイルの削除

- 1. [スーパー管理者] > [設定] > [管理] > [管理者プロファイル] から Seqrite Terminator ヘログオンします。
- 2. 削除する管理者プロファイルを選択して、[削除]をクリックします。

注意:削除した管理者プロファイルは読み取り専用ユーザータイプに変更されます。 定義済み管理者プロファイルを削除することはできません。

# ウェブポータルのカスタマイズ

この機能を使用して、Terminator ウェブポータルをカスタマイズできます。

ウェブポータルをカスタマイズするには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [管理] ヘログオンします。デフォルトでは、 [ポータルをカスタマイズ] ページが表示されます。

管理		日時 ポータルを	カス管理者設定	管理プロファイル SMTP設定
				保存
設定されたタイトル:	◉ デフォルト	🔘 カスタム		
製品口二:	● デフォルト	◎ ブラウズ		快適な使用のために幅未満300ビ クセル、透明な背景で90PX未満
	Seq	rite		のPNGファイルをアップロードして ください。
	TER	MINAT	OR	
会社口ゴ:	◉ デフォルト	◎ ブラウズ		快適な使用のために幅未満100ビ クセル、透明な背景で35PX未満
	SEQRI	ГЕ		のPNGファイルをアップロードして ください。
アイゴン:	◉ デフォルト	◎ ブラウズ (0)	:0の画像をアップロード	します。
ユーザータイムアウト:	60 分			
ランディングメッセージ	div class="le class="loginle class="loginle	eftBlock loginleftBlock" conBlock"> <sp contentBlock"&gt;<h1>イン</h1></sp 	> <ul><li><span an ゆーネットアクセス</span </li></ul>	* *
ダッシュボードのメッセ ージ:	<h1>ようこそ!</h1>			
管理者の連絡先:	さらに詳細な報	「報に関しましては、シス	テム管理者に連絡してく	ださい。
<mark>注意:</mark> ページ"%s "はブき	ランド名に置き拶	れることになります。		

2. このページのフィールドについて、次の表で説明します。

フィールド	説明
タイトルの設定	サイトタイトルを企業または組織の名前、組織の簡単な説明、 またはそれらを組み合わせたものにできます。このタイトルは カスタムオプションを使用して変更でき、デフォルトのままに しておくこともできます。 <i>空白は使用できません。英数字のみ</i> を使用できます。
製品ロゴ	管理者はこのオプションを使用して、デフォルトのロゴを設定 したり、ユーザーウェブポータル用に新しいロゴをアップロー ドしたりできます。このロゴは背景が透明で、大きさは 300 × 90 ピクセルにする必要があります。

デバイスの管理

フィールド	説明
会社ロゴ	管理者はこのオプションを使用して、会社のデフォルトのロゴ を設定したり、ユーザーウェブポータル用に新しいロゴをアッ プロードしたりできます。このロゴは背景が透明で、大きさは 100 × 35 ピクセルにする必要があります。会社ロゴはフッタ に表示されます。
アイコン(ファ ビコン)	デフォルトとカスタムの 2 つのオプションがあります。管理者 はこのオプションを使用して、デフォルトのファビコンを設定 でき、ユーザーウェブポータル用に新しいファビコンをアップ ロードすることもできます。
ユーザーのタイ ムアウト	このオプションを使用し、ユーザーのアイドルセッションにつ いて、デフォルトのタイムアウト時間を分単位で設定できま す。
ランディングメ ッセージ	ウェブサイトのランディングメッセージとして、サイトの趣旨 を簡単に記述するという手法があります。このメッセージは、 ユーザーがログインする前にログインページに表示されます。
ダッシュボード のメッセージ	このメッセージは、ユーザーがウェブポータルにログインする 際に表示されます。
管理者の連絡先	管理者の詳細を入力できます。このメッセージは、エラーページに表示されます。管理者は、このメッセージをカスタマイズできます。

3. [保存] をクリックします。

## SMTP 設定

[SMTP 設定] ページでは、管理者がメールの通知を受け取るために使用される、メール アカウントを設定できます。

1. Seqrite [スーパー管理者] > [設定] > [管理] > [SMTP 設定] として、Terminator ヘログオンします。

管理		日時	ポータルをカス	管理者設定	管理プロファイル	SMTP設定
						保存
ステータス:	◉ 有効	◎ 無効				
サーバーアドレス:						
サーバーポート:						
暗号化の種類:	なし	¥				
メールアドレス:						
認証を要求:						
ユーザー名:						
パスワード:						
	テストメー	ール送信				

このページのフィールドの説明を、次の表に示します。

フィールド	説明
ステータス	SMTP ステータスを選択します。ステータスが無効な場合、メール通知は送信されません。
サーバーアドレス	SMTP サーバーアドレスを入力します。サーバーアドレスはド メイン名または IP アドレスです。
サーバーのポート	SMTP サーバーのポート番号を入力します。
暗号化タイプ	ドロップダウンリストから暗号化の種類を選択します。
認証を要求	[認証を要求] チェックボックスが選択されていると、SMTP サーバー認証にユーザー名とパスワードが必要になります。
メールアドレス	これが管理者のメールアドレスです。すべてのメール通知が このメールアドレスに送られます。 注意:このメールアドレスがメール保護対象としてデフォルト
	でホワイトリストに登録されます。
ユーザー名	ユーザー名を入力します。有効なメールアドレスの必要があります。SMTP サーバー認証には、ユーザー名とパスワードが必要です。
パスワード	パスワードを入力します。これは、メールの通知を受け取る ため設定したメールアカウントのパスワードです。

2. [保存] をクリックします。

# アップデート

[アップデート] ページで Terminator サービスとシステムアップデートを管理できま す。サービスのアップデートには、アンチウイルスと IPS/IDS シグネチャのアップデ ートが含まれ、システムアップデートには新しいデバイスバージョンのアップデートが 含まれます。

サービスアップデートを自動で行うように設定できるほか、[今すぐアップデート] ボ タンでいつでもサービスをアップデートすることもできます。また、システムアップデ ートが自動的にインストールされるように設定したり、アップデートの通知を取得して 都合のいい時にアップデートをインストールしたりすることも可能です。

Seqrite ウェブサイトから最新のアップデートファイルをダウンロードして、アップデ ートページで Terminator を手動でアップデートすることもできます。

サービスアップデートの設定

サービスアップデートを設定するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [アップデート] ヘログオンします。

Seqrite		J	🌞 オプション	/ -   <b>?</b> ^	ルブ・  😃 シャッ	トダウン - 	➡ Admin (管理) ▼
TERMINATOR	一	- <sub>A</sub>	コノテノツフィル	×977	ユーサー官理	設正	ロクとレホート
> インターネット	アップデート						保存
> アンチウイルス	サービスアップデート						
▶ 電子メール保護	名前	自動ア	<b>゚ップデートモード</b>				
→ 定義	アンチウィルスシグ		4	▶すく"更新			
> ファイアウォール設定	IPS/IDS シグネチャ	•	4	▶すく"更新			
> IPS							
▶ アプリケーションコントロール							
▶ 証明書	システムアップデート						
> IPSec VPN	◎ アップデートをイン	ストールし	しない し				
> PPTP VPN	<ul> <li>アップデートを自動</li> <li>マップデートが利用</li> </ul>	でインスト	トール ::- <i>t-</i> ら:酒切				
> SSL VPN		円目El Cra	よう /こう <u>/囲</u> 大山				
→ インターフェース	今すぐ更新						

- 2. [オン] または [オフ] ボタンをクリックして各サービスで自動アップデートモード を有効/無効にします。
- 3. [今すぐアップデート] ボタンをクリックして、特定のサービスの利用可能なアッ プデートをインストールします。

## システムアップデートの設定

システムアップデートを設定するには、以下の手順に従います。

1. [Seqrite Terminator] > [設定] > [アップデート] ヘログオンします。

Seqrite TERMINATOR	*	:-4	☆ オブション →   ?	<b>ヘルブ - ∣ () シャット</b> ユーザー管理	<b>ダウン →</b> 設定	➡ Admin (管理) →
<ul> <li>&gt; インターネット</li> <li>&gt; アンチウイルス</li> <li>&gt; 電子メール保護</li> <li>&gt; 定義</li> <li>&gt; ファイアウォール設定</li> <li>&gt; IPS</li> <li>&gt; アプリケーションコントロール</li> </ul>	<b>アッブデート</b> サービスアップデート 名前 アンチウィルスシグ IPS/IDSシグネチャ	白動, 又 又	<b>アップデートモード</b>			保存
<ul> <li>&gt; 証明書</li> <li>&gt; IPSec VPN</li> <li>&gt; PPTP VPN</li> <li>&gt; SSL VPN</li> <li>&gt; インターフェース</li> </ul>	<b>システムアップデート</b> アップデートをイン アップデートを自動 アップデートが利用 今すぐ更新	マトール かでインス 月可能に	しない ストール なったら通知			

- 2. システムアップデートの以下のオプションを選択できます。
  - アップデートをインストールしない:システムアップデートはインストールされ ません。
  - 自動でアップデートをインストール:4 時間間隔でシステムアップデートは確認 されます。また、利用可能なアップデートがある場合、システムは自動的にイン ストールされます。
  - アップグレードが利用可能になったら通知:システムアップデートの通知は、 [システムアップデート] セクションとダッシュボードの [通知] セクションに 表示されます。[今すぐアップデート] ボタンをクリックした場合にのみ、シス テムアップデートはインストールされます。
  - システムアップデートがある場合は、[今すぐアップデート] ボタンをクリック してシステムアップデートをインストールしてください。

手動アップデートの設定

手動アップデートを設定する場合、以下の手順に従います:

1. Seqrite Terminator > 設定 > アップデートにログオンします。

Cogrito		🍦 オプション 🗸	<b>?</b> ヘルプ -   🕛	シャットダウン   📑 Admin (	管理) -
TERMINATOR	ホーム	コンテンツフィルタリ	ング ユーザー	管理 設定 ログとレオ	ť.−⊦
<ul> <li>インターネット</li> </ul>	アップデート				保存
→ アンチウイルス	サービスアップデート				
▶ 電子メール保護	名前	自動アップデートモー <mark>ド</mark>		前回アップデート	
	アンチウィルスシグネチャ		今すぐ更新	2016-1-22 7:19	
> ファイアウォール設定	IPS/IDS シグネチャ		今すぐ"更新	2016-01-22 00:00	
> IPS					
▶ アプリケーションコントロール					
▶ 証明書	システムアップデート				
> IPSec VPN	◎ アップデートをインストール	しない			
> PPTP VPN	<ul> <li>アップデートを自動でインス</li> <li>フィプデートが利用可能に</li> </ul>	いール			
> SSL VPN	● アッノナートか利用可能に	(よう /こつ )進大山			
> インターフェース	今すぐ更新				
> IPv6	(千新고, 귀국, 미				
▶ ルーティング	<u>于動アップテート</u>				
> DNS	1.7バージョンの最新のアップ:	デートをダウンロードする場	易合 Click Here		
> DHCP	ファイルのアップロ <b>ファイ</b> ル	ル <b>を選択</b> 選択されていまう	<u>ಕ</u> ん		
→ ダイナミックDNS	ダウンロードしたファイルを選	択してから?更新?をクリック	フします。		
→ USBモデム	更新				
> ロードバランシング					
> 管理					
> 通知					
➤ バックアップ					
> 復元					
> ファクトリーリセット					
更新 ▶					

- 手動アップデートセクションで [ここをクリック] リンクをクリックしてアップデ ートファイルをダウンロードします。
- 3. [ここをクリック] リンクをクリックすると、以下のページで新しいタブが開きます。

		India 🗸	Partners	Contact 📁 📞	Search Site	٩
SEQRITE	Endpoint Security	Gateway Security	Server Security		Services	Support
Seqrite Offline Product Upda	ates					
Segrite Offline F	Product U	pdates				
Server Terminator						
Instructions for TERMIN	NATOR offline	updates:				
<ol> <li>Select the Terminator product ve</li> <li>Select download type - Weekly, I</li> <li>Click on <b>Download</b> button and d</li> <li>Login to TERMINATOR using the</li> <li>Go to the <b>Settings -&gt; Updates</b> p In Manual Updates section, click</li> </ol>	ersion. Monthly or Complete lownload the file on admin credentials. page. k on <b>Choose file</b> but	your machine. ton.				
6. Select the file downloaded in ste	ер 3.					
7. Click on Update.						
You can update your Seqrite TERMI	INATOR Edition to th	e latest virus datab	ase, by referring	to the drop dow	n given below:	
Select Terminator Version	•					

- 4. [Terminator] タブをクリックします。
- 5. Terminator のバージョンを選択します。
- 毎週、毎月、コンプリートのなかからアップデートタイプを選択します。アップデートタイプは、前回のアップデートの内容により決まります。サービスアップデートセクションに表示される最終更新日に基づいて適切なアップデートタイプを選択します。

You can update your Seqrite TERMINATOR Edition to t	the latest virus database, by referring to the drop down given below:
v1.7	
Weekly Update	
TERMINATOR Updates v1.7	
Update Type :	Weekly Update
	Virus Database : ( 3 January, 2016 - 14 January, 2016 )
	MD5SUM : e956766344ef4d658f0d2afc587b4f17
	Size : 27 MB
	Download the new updates if you have not updated your Terminator Virus Database for more than a month.
	Download

- 7. [ダウンロード] をクリックします。tar ファイルがダウンロードされます。
- アップデートページの手動アップデートセクションでファイルを選択し、[アップデ ート]をクリックします。

注意:

- ファイルの拡張子を変更しないでください。
- デバイスに十分な空きがない場合は、ファイルを取り出し、個々にアップロードしてください。

# バックアップと復元

Seqrite Terminator では設定とデータをバックアップでき、Terminator がクラッシュ した場合や、以前の設定に戻したい場合に役立ちます。Terminator のデフォルト設定、 ユーザー定義設定、ユーザーデータベース設定をバックアップし、技術的な問題が発生 したときに再利用するため保存できます。

バックアップを作成するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [バックアップ] ヘログオンします。[バックア ップ設定] ページが表示されます。

## デバイスの管理

Operative		🔅 オプショ	シェー ? ^	ルブ・  🕛 シャッ	ダウン・	🕞 Admin (管理) -
SEGRITE		」 コ`ノテ`ノツフィ」	レタリング	ザー管理	設定	ログとレポート
					HAX/A	HVCDAN I
> インターネット	バックアップ					
→ アンチウイルス						削除
▶ 電子メール保護	日時	設定のバッ ケアップ	データバ・	ックアップ		
▶ 定義						<b>^</b>
> ファイアウォール設定						
> IPS						
▶ アプリケーションコントロール						
> 証明書						-
> IPSec VPN	バックアップ設定					バックアップ
> PPTP VPN	□ 全て					
> SSL VPN	□ 設定のバックアップ					
> インターフェース	□ テータ					
> IPv6	自動バックアップ設定					保存
> ルーティング	スケジュール設定:	调 🔻				
> DNS		□曜日 ▼				
> DHCP			- ^			
> ダイナミックDNS	."		• 71			
> USBモデム	ハックアッフ教の上限:	10				
> ロードハランシンク						
> 管理						
> 通知						
バックアップ ト						

2. 作成するバックアップのタイプを選択します。これは次のいずれかです。

タイプ	説明
すべて	Terminator の設定とレポートのバックアップが作成されます。
設定	Terminator 設定(インターフェースとスタティックルートを除 く)のバックアップが作成されます。
データ	レポート (ログビューアを除く) のバックアップが作成されま す。

3. [バックアップ] をクリックします。内蔵の CF フラッシュカードにバックアップが 作成されます。

注意:[バックアップ] ページには、設定バックアップであるかデータバックアップであるかを問わず、以前に作成したバックアップすべてのリストが、バックアップされた日時とバックアップのタイプとともに表示されます。[設定バックアップ/データバックア

ップ]欄のバックアップファイルリンクをクリックして、バックアップファイルをダウ ンロードできます。

#### 自動設定バックアップ

この機能により、スケジュールした時刻にシステム設定を自動的にバックアップするよう Terminator を設定できます。このバックアップはデバイスに保存され、いつでも必要なときにシステム設定を復元するために使用することができます。

注意:自動バックアップには、レポートや、システムの他のデータは含まれません。

自動設定バックアップを設定するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [バックアップ] ヘログオンします。[バックア ップ設定] ページが表示されます。
- 2. [自動設定バックアップ] で、バックアップを作成する頻度を設定します。

自動設定バックアップ		保存
バックアップ頻度が無効	週 🗸	
	月曜日 🗸	
	12 🗸 時間	00 🗸 分
バックアップ数の上限を	10	

3. [バックアップ頻度]を選択します。これは次のいずれかです。

周波数	説明
なし	自動バックアップを無効にします。このオプションを選択すると、 Terminator はバックアップを作成しません。
毎日	選択した時間に毎日バックアップを作成するよう、Terminator を設 定します。毎日のバックアップを行う時刻(時間および分)を選択し ます。
毎週	毎週 1 回バックアップを作成するよう、Terminator を設定します。 バックアップを行う曜日と時刻(時間および分)を選択します。この オプションがデフォルトで、バックアップは毎週月曜日の 12:00 PM (JST)に行われます。
毎月	毎月 1 回バックアップを作成するよう、Terminator を設定します。 バックアップを行う日付と時刻(時間および分)を選択します。

4. Terminator に保存できるバックアップの最大数を、[最大保存バックアップ数] フィールドに入力します。

バックアップ数の上限は 100 またはそれ未満に設定することができます。バックア ップ数が上限に達した場合は、最も古いバックアップが自動的に削除されます。

### バックアップの復元

この機能を使用して、以前に作成したバックアップから、破損したデータを再構築できます。すべての設定とレポートのバックアップが Terminator に保存されます。復元オプションで、Terminator の設定とレポートを復元することができます。

バックアップを復元するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [復元] ヘログオンします。[設定の復元] ページに、以前に作成されたバックアップすべてのリストが、作成された日時とタイプとともに表示されます。

Seqrite TERMINATOR	<b>ホー</b>	🌞 オプション ム コンテンツフィルタ	▼  <b>? ヘルブ -</b>   <b>()</b> ミ マリング ユーザー管	<del>/ャットダウン →</del> <sup>•</sup> 理 設定	<mark>▶ Admin (管理) ↓</mark> ログとレポート
<ul> <li>・ インターネット</li> <li>・ アンチウイルス</li> </ul>	復元 デバイス上のバックアッ	プのリスト			アップロード   削除
▶ 電子メール保護	タイムスタンプ	設定のバックアップ	データバックアップ		*
<ul> <li>&gt; 定義</li> <li>&gt; ファイアウォール設定</li> <li>&gt; IPS</li> </ul>	2015-Oct-14, 22:53:59	C141015225359.bkp	D141015225359.bkp	没元します	

- 復元するバックアップのタイプを選択し、[復元] をクリックします。バックアップ オプションを使用して以前にダウンロードしたバックアップファイルをアップロー ドすることもできます。[アップロード] ボタンを使用してバックアップファイルを 参照し、アップロードします。
- 3. クラウドサービスを有効にされている場合、クラウドからバックアップを復元する こともできます。
- 4. 以下の図で示されているように、[復元] ページで [クラウドから復元] オプション をクリックします。

## デバイスの管理

Coarito			🛟 Optio	ons -   <b>?</b> Help -   🔱	Shut down 👻	Admin (Admin) 👻
TERMINATOR	На	ome Content	Filtering	User Management	Settings	Logs & Reports
> Internet	Restore					
> Antivirus	List of Backups on Dev	ice				Upload   Delete
> Mail Protection	Timestamp	Configuratio	n Backup	Data Backup		
> Definitions	🔲 2015-May-15, 14:01:	10		D150515140110.bkp	Restore	*
> Firewall Settings	2015-May-15, 14:01:	00		D150515140100.bkp	Restore	
> IPS	🔲 2015-May-15, 14:00:	50 C150515140	050.bkp		Restore	
> Application Control						
> VPN						~
> Connection Details	Restore from Cloud					
> PPTP VPN Details						
> SSL VPN	Restore:	Restore from C	loud Clie	ck to display list of configur	ation backups on o	cloud.

- 5. クラウドバックアップリストポップアップが表示されます。このリストには、以下 のバックアップが含まれます。
  - 複製:これはデフォルトのバックアップで、Terminator で設定が変更されると自動的に更新されます。
  - オンデマンド:設定とデータのバックアップが**すべて**手動で行われます。

クラウドバックアップ一覧				×
バックアップ時間	タイブ	サイズ(KB)		
2015-05-21 12:22:27- Replica	スケジュール	566	復元し	
2015-05-22 16:32:43	スケジュール	567	復元し	
2015-05-21 17:50:19	オンデマンド	232	復元し	
2015-05-20 16:50:48	スケジュール	563	復元し	
2015-05-18 16:28:41	スケジュール	563	復元し	Ţ
				キャンセル

6. 復元したいバックアップで [復元] をクリックします。

### バックアップの削除

バックアップを削除するには、以下の手順に従います。

- 1. Seqrite [Terminator] > [設定] > [復元] ヘログオンします。
- 2. 削除するバックアップを選択し、[削除] をクリックします。選択したバックアップ が削除されます。

出荷時設定へのリセット

出荷時設定へのリセットを使用して、Terminator を出荷時の状態に戻すことができま す。インターフェースのリセットと登録削除のオプションが用意されています。[出荷 時設定へのリセット] を選択すると、Terminator のすべての設定、ユーザー定義設定、 およびレポートが失われます。

1. Seqrite [Terminator] > [設定] > [出荷時設定へのリセット] ヘログオンします。 [出荷時設定へのリセット] 画面が表示されます。

Seqrite		☆ オプション -   ? ·	ヘルプ -   🕛 シャッ	ダウン 🔻	🔁 Admin (管理) 🚽
TERMINATOR	ホーム	コンテンツフィルタリング	ユーザー管理	設定	ログとレポート
> インターネット	ファクトリーリセット				保存
→ アンチウイルス	会社名:	Quickheal			
▶ 電子メール保護	製品キー:	x0000000000000000000000000000000000000			
	インターフェースをリセット	เมเม≂์ ▼			
> ファイアウォール設定	登録を削除	เงเงえ ▼			

- 2. インターフェースをリセットするかどうかを選択します。[はい]を選択すると、現 在の IP アドレスが削除され、Terminator のデフォルト IP が使用されます。
- 3. 登録を削除するかどうかを選択します。[はい] を選択すると、Terminator の登録 が削除されます。Terminator を使用するには、再度登録を行う必要があります。
- 4. [保存] をクリックします。

# ライセンス情報ページ

[ライセンス情報] ページには、Terminator に関するライセンス情報が表示されます。 このページでは以下のような詳細情報を確認できます。

**ライセンス情報**:会社名、製品名、プロダクトキー、製品バージョン、モデル、ライセンス有効期限などが表示されます。

**サービス詳細**:ライセンス数、VPN 数、アンチスパム、Seqrite クラウドサービスなど、 選択されているサービスが表示されます。 [ライセンス情報] ページでは、ライセンス情報の更新、ライセンス履歴の確認、オン ラインおよびオフラインでのライセンス更新、Seqrite クラウドサービスの有効化が可 能です。

ライセンス情報を表示するには、以下の手順に従ってください。

- 1. [Seqrite Terminator] > [ヘルプ] > [ライセンス情報] ヘログインします。
- 2. [ライセンス情報] ページが表示されます。

			🙀 オプション 🕞 🣍 ヘルブ	▼   😃 シャットダウ	ンする 🗸   🔁 Admin (管理) 🗸
Seqrite					
TERMINAT	OR	ホーム	コンテンツフィルタリング	ユーザー管理	設定 ログとレポート
ライセンス情報					<b>ステータス</b> 注文フォーム
会社名:	Customer_Name		製品バージョン:	1.7.0.23	
製品名:	Seqrite Terminator		モデル:	T1S	
ブロダクトキー:	xxxxxxxxxxxxxxxxxxxx		ライセンス有効期限:	14 October 2016	
サービス情報					
シリアルナンバー	サービス名		#ライセンス		
1	ライセンスユーザー		25		
2	仮想プライベートネットワーク		5		
3	アンチスバム		-		
ライヤンフ 博想の マ	シゴデニレ ニスセンフ 履歴	オフラインで	のライヤッフの更新		

[ライセンス情報] セクションの各欄の説明を、次の表に示します。

会社名	会社名を表示します。
製品名	製品名を表示します。
プロダクトキー	プロダクトキーを表示します。
製品バージョン	Terminator のバージョンを表示します。
モデル	Terminator のモデルタイプを表示します。
ライセンス有効期 限	ライセンスの有効期限の日付を表示します。この日付を過ぎ るとライセンスの有効期限が切れ、更新が必要になります。

- 3. [サービス情報] セクションには、選択されているサービスの情報が表示されます。 例えば、アンチスパムを購入している場合、このセクションに表示されます。
- 4. ライセンスの更新、サービスの追加/削除、ユーザーの追加/削除などを行った場合、 [ライセンス情報を更新] ボタンをクリックして変更を適用します。

5. サービスの更新、追加、削除などのライセンス活動情報を表示するには、[ライセンス履歴] ボタンをクリックします。ライセンス履歴のポップアップが表示されます。

イセンス履歴情報		
日付	活動	詳細
01 October 2015	ライセンスが再有効化	ライセンスが再有効化されました.
28 September 2015	ライセンスが再有効化	ライセンスが再有効化されました.
25 September 2015	ライセンスが再有効化	ライセンスが再有効化されました.
23 September 2015	ライセンスが有効化さ	期間: 12 月 ユーザー: 15 機能: 仮想プライベートネットワーク
		ОК

インターネットに接続されていない場合は、オフラインでライセンスを更新できます。[オフラインでライセンスを更新] ボタンをクリックします。オフラインでのライセンス更新のポップアップが表示されます。ポップアップに示された手順に従って、オフラインでライセンスを更新します。

オフラインでのライセンスの 更新	×
以下のリンクをクリックして、オフライン更新フォームに入力します。 http://www.seqrite.com/offline_renewal フォームを完了するには次の情報を記入する必要があります。 インストール番号: 1CEF6B2C857E4F4586CED14D7A929BAA	
デバイス番号: HAZ0000BAB651061CA06	
フォームの記入後、ライセンスキーファイルが送信されます。ライセンスキーファイルを入手したら [参照]をクリックして、ファイルの位置を指定してください。	`
ライセンスキーファイル: 参照	
提出するキャンセル	

## ライセンスの更新

[ライセンス情報] ページの [注文フォーム] タブから、Terminator ライセンスの更新 や、ライセンスへのユーザー追加が行えます。ライセンスを更新するには、以下の手順 に従ってください。

- 1. [Seqrite Terminator] > [ヘルプ] > [ライセンス情報] ヘログインします。[ライ センス情報] ページが表示されます。
- 2. [注文フォーム] タブをクリックします。ライセンスの更新ページが表示されま す。

Seqrite <b>TERMINATOR</b>	ホーム	☆ オプション →   コンテンツフィル	<b>? ヘルブ</b> .タリング	-   <b>()</b> シャットダ ユーザー管理	ウンする <del>-</del>   ! 設定	➡ Admin (管理) マ ログとレポート
ライセンス情報					ステータン	え 注文フォーム
ライセンス注文フォーム このページでは、アプライアンスライセンスの更新、新しい 以下を行います: ③ ライセンスを更新する ③ 新しいユーザーのライセンスを追加する 注文する	ユーザーライ	、センスの追加、Seqrite	. Terminator ए	の追加機能の購入な	ビテラことができ	≝ます。

- Terminator のライセンスを更新するには、[ライセンスを更新する] オプションを 選択します。ライセンスにユーザーを追加するには、[新しいユーザーのライセン スを追加する] オプションを選択します。
- 4. [注文する] をクリックします。

## Seqrite Cloud の有効化

Seqrite Cloud は異なる場所に展開された複数の Terminator の管理・制御をサポート する統合ソリューションです。簡単なクラウド接続により、最新のセキュリティステー タスの確認、製品ポリシーの設定、通知の受け取り、重要なネットワークイベントの修 正などを単一のダッシュボードから行えます。さらに、Terminator のポリシー設定と バックアップをクラウド上で容易に行えるようになります。

注意:この機能は有料で、オプションです。お使いの Terminator でクラウド機能を有効にするには、お客様サポートへ問い合わせてください。

Seqrite Cloud を有効化して Terminator 向け各種サービスを利用するには、以下の手順に従ってください。

1. Seqrite [Terminator] > [ヘルプ] > [ライセンス情報] ヘログオンします。[ライ センス情報] 画面が表示されます。
| Searite                  |                              |          | 🌼 オブション 🛛   🤶 ヘルコ              | チャー 🕐 シャットダウ                   | ウンする - | 🕞 Admin (管理) →  |
|--------------------------|------------------------------|----------|--------------------------------|--------------------------------|--------|-----------------|
| TERMINA                  | TOR                          | ホーム      | コンテンツフィルタリング                   | ユーザー管理                         | 設定     | ログとレポート         |
| ライセンス情報                  |                              |          |                                |                                | ステータ   | <b>ス</b> 注文フォーム |
| 会社名:<br>製品名:<br>プロダクトキー: | UTM_QA<br>Seqrite Terminator |          | 製品バージョン:<br>モデル:<br>ライセンス有効期限: | 1.6.2.25<br>T1H<br>15 May 2016 |        |                 |
| サービス情報                   |                              |          |                                |                                |        |                 |
| シリアルナンバー                 | サービス名                        | 3        | #ライセンス                         |                                |        |                 |
| 1                        | ライセンスユーザー                    |          | 750                            |                                |        |                 |
| 2                        | 仮想ブライベートネットワーク               |          | 20                             |                                |        |                 |
| 3                        | アンチスパム                       |          | -                              |                                |        |                 |
| 4                        | Segrite Cloud                |          |                                |                                |        |                 |
| ライセンス情報のア                | ッブデート ライセンス履歴                | オフラインでのラ | イセンスの更新                        |                                |        |                 |
| ☑ Seqrite Cloud の接       | 結だを有効にする。                    |          |                                |                                |        | 保存              |
| Seqrite Cloud ステータ       | は: 接続されています                  |          |                                |                                |        |                 |

Seqrite Cloud サービスを利用するには、最初に有効化が必要になります。[クラウドを有効化] ボタンをクリックします。クラウドプラットフォーム情報のポップアップが表示されます。

アクティブ Seqrite Cloud ライセンス	×
Seqrite Cloud:	
Seqrite Cloud 管理者が集中管理ポータルを使用して、組織の複数の Terminator を任意の場所から管理できます。また、バックアップとレポートを保存する機能も有しています。 Seqrite Cloud.	Y
接続	

3. [接続] をクリックすると、OTP ポップアップが表示され、ご登録のメール ID に OTP が送信されます。

アクティブ Seqrite Cloud ライセンス	×
ワンタイムバスワード (OTP): 登録済み電子メール ID に送信された OTP を入力してください。 OTP を入力してください:	
	続ける

- 4. 登録したメール ID で受け取る OTP を入力し、[続ける] をクリックします。
- 5. これにより、OTP の確認が行われます。確認が正常に完了すると、Cloud サービス が有効化されます。



6. [Seqrite Cloud **への接続を有効化**] 欄からクラウドサービスを有効化/無効化でき ます。

Chapter 9

# ログとレポート

Seqrite Terminator では、各種のモジュールについて広範なレポートとログが提供されます。これらのレポートとログはトラブルシューティングに非常に役立つ他、レポートを使用して決定を行い、正式なポリシーを策定することができます。インターネット使用量、ウェブサイトアクセス、メール保護などに関する詳細なレポートが入手できます。こうしたレポートはすべて.XLS、.PDF、または.DOC 形式でエクスポートもできるため、様々な用途に活用できます。

Terminator では、次のタイプのレポートが利用可能です。

- インターネット使用量
- <u>ウェブサイトアクセス</u>
- メール保護
- ウェブ保護
- <u>侵入防止</u>
- ポリシー違反活動
- 带域幅使用量
- <u>ファイアウォールレポート</u>
- <u>アップデート</u>
- ログビューア

# インターネット使用量

このレポートは、月別のインターネット使用量データを提供します。ユーザーの合計数、 合計使用量、ユーザー名、ユーザーの IP アドレス、ユーザーの属するグループ、ユー ザーがアクセスしたウェブサイトの総数、インターネット合計使用量などの詳細が提供 されます。1 日の各時間帯における実際の帯域幅使用量や、各システムの使用量も提供 されます。このレポートをカスタマイズして、大きなトラフィックが発生する理由を突 き止めることができます。この結果に基づいて帯域幅使用量に関する決定を行い、企業 ポリシーを作成できるため、不要な、または業務に関係のないインターネット使用量を 減らすために役立ちます。このレポートは、MS Excel、PDF、MS Word フォーマットで エクスポートできます。

インターネット使用量のログを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [インターネット使用量] ヘログオン します。次のページが表示されます。



2. ユーザー名をクリックすると、そのユーザーの詳細なインターネット使用量のレポ ートが表示されます。

### ログとレポート

Searite		🔅 オプション 🗸	<b>?</b> ヘルプ -   也 シ	ャットダウンする	5 👻   📑 Admin (	(管理) -
TERMINATOR		ホーム コンテンツフィル	タリング ユーザ	一管理 設	定 ログとレオ	ボート
インターネット利用 ・	インターネットオ	利用→詳細報告				
> ウェブサイトのアクセス	ユーザー名:	丸山				
> 電子メール保護	グループ名:	L100				
> ウェブ保護	<b>表示:</b> 送	信者 11-10-2015	宛先 11-10-2015		$\rightarrow$	
▶ 侵入防止		Business				
▶ ポリシー違反の試み		(0.92%) Unknown				
> 帯域幅使用		(1.15%) Advertisements & Pop-Ups				
> アプリケーションコントロール		(5.50%) Shopping (19.95%)				
> ファイアウォール		(10.00 K)				
<b>&gt;</b> 更新				Computers & Technol	logy	
▶ ログのビューアー				(72.4)	8%)	
	アクセスされるウ	ェブサイト	すべて表	<b></b>	▼   <b>®</b>	<u>&gt;</u>
	日時 ▼	ウェブサイト URL	カテゴリー イ	ンターネット 利用	月 IPアドレス	
	2015-10-11 18:2	http://www.amazon.in/mn/s	ショッピング	0.85 KB	192.168.172.26	<b>^</b>
	2015-10-11 18:2	http://www.amazon.in/mn/s	ショッピング	0.85 KB	192.168.172.26	
	2015-10-11 18:2	http://fls-eu.amazon.com/1/	ショッピング	0.44 KB	192.168.172.26	
	2015-10-11 18:2	http://www.amazon.in/b/ref	ショッピング	55.01 KB	192.168.172.26	_
	2015-10-11 18:2	http://g-ecx.images-amazon.c	コンビュータとテクノ	2.16 KB	192.168.172.26	=
	2015-10-11 18:2	http://g-ecx.images-amazon.c	コンビュータとテクノ	1.21 KB	192.168.172.26	
	2015-10-11 18:2	http://www.amazon.in/favico	ショッピング	3.04 KB	192.168.172.26	
	2015-10-11 18:2	http://g-ecx.images-amazon.c	コンビュータとテクノ	344.81 KB	192.168.172.26	

# ウェブサイトアクセスレポート

このレポートには、特定の日、過去 7 日間、過去 30 日間にユーザーがアクセスした ウェブサイトの情報が表示されます。また、カテゴリごとのウェブサイトアクセスレポ ート、訪問の回数、およびそれらのサイトを頻繁に訪問するユーザーのリストも表示さ れます。このレポートは、MS Excel、PDF、MS Word フォーマットでエクスポートでき ます。

ウェブサイトアクセスレポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [ウェブサイトアクセス] ヘログオン します。次のページが表示されます。

#### ログとレポート

Searite		🛟 オブション -   ?	・ヘルプ   也 シ+	ァットダウンする ▼   [	➡ Admin (管理) -
TERMINATOR	ホーム	コンテンツフィルタ	リング ユーザ-	-管理 設定	ログとレポート
> インターネット利用	ウェブサイトアクセス			今日 過去 7日間	間 過去 30日間
<b>ウェブサイトアクセス</b> > 雷子メール保護	Advertise	ments & Pop-Ups (1.98%) Business			
<ul> <li>ウェブ保護</li> </ul>	Сотри	(4.09%) uters & Technology (10.94%)			
▶ 侵入防止		Shopping			
▶ ポリシー違反の試み		(10.5/%)	(6	General 4.42%)	
> 帯域幅使用					
> アプリケーションコントロール					
> ファイアウォール					
> 更新	アクセスしたウェブサイト		すべて表示	<del>.</del> •	] 🖳   🛃   🕋
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト	カテゴリー	すべて表示 アクセス数 マ	、 ▼	〕 📳   🌽   🕋 アクセス
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://i1.sdlcdn.com/	<b>カテゴリー</b> ジェネラル	すべて表示 アクセス数 ▼ 189	★ ▼ インターネット利用 3.28MB	副    上    副 アクセス
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://i1.sdlcdn.com/ http://cdn.shopclues.net/	<b>カテゴリー</b> ジェネラル ジェネラル	すべて表示 アクセス数 マ 189 132	インターネット利用 3.28MB 0.71MB	<ul> <li>・</li> <li>・</li></ul>
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://il.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/	<b>カテゴリー</b> ジェネラル ジェネラル ショッピング	アクセス数 ▼ 189 132 117	Tンターネット利用 3.28MB 0.71MB 2.98MB	<ul> <li>●</li> <li>●</li></ul>
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://i1.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/ http://i4.sdlcdn.com/	<b>カテゴリー</b> ジェネラル ジェネラル ショッピング ジェネラル	すべて表示 アクセス数 マ 189 132 117 97	★ ▼ インターネット利用 3.28MB 0.71MB 2.98MB 1.86MB	<ul> <li>・</li> <li>・</li></ul>
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://il.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/ http://i4.sdlcdn.com/ http://i3.sdlcdn.com/	<b>カテゴリー</b> ジェネラル ジェネラル ショッピング ジェネラル ジェネラル	すべて表示 アクセス数 マ 189 132 117 97 95	<ul> <li>インターネット利用</li> <li>3.28MB</li> <li>0.71MB</li> <li>2.98MB</li> <li>1.86MB</li> <li>1.39MB</li> </ul>	<ul> <li>●</li> <li>●</li></ul>
<ul> <li>▶ 更新</li> <li>&gt; ログのビューアー</li> </ul>	アクセスしたウェブサイト ウェブサイト http://i1.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/ http://i4.sdlcdn.com/ http://i3.sdlcdn.com/ http://i3.sdlcdn.com/	<b>カテゴリー</b> ジェネラル ジェネラル ショッピング ジェネラル ジェネラル ショッピング	すべて表示 アクセス数 ▼ 189 132 117 97 95 92	★ ▼ インターネット利用 3.28MB 0.71MB 2.98MB 1.86MB 1.39MB 0.51MB	<ul> <li>・</li> <li>・</li></ul>
▶ 更新 ▶ ログのビューアー	アクセスしたウェブサイト ウェブサイト http://i1.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/ http://i4.sdlcdn.com/ http://i3.sdlcdn.com/ http://ii.shopping.rediff.com/ http://i.ebayimg.com/	カテゴリー         ジェネラル         ジェネラル         ショッピング         ジェネラル         ジェネラル         ジョッピング         ジェネラル         ジョッピング         ショッピング         ジェネラル         ジョッピング         ショッピング         ジェネラル	すべて表示 アクセス数 マ 189 132 117 97 95 92 86	<ul> <li>インターネット利用</li> <li>3.28MB</li> <li>0.71MB</li> <li>2.98MB</li> <li>1.86MB</li> <li>1.39MB</li> <li>0.51MB</li> <li>0.78MB</li> </ul>	<ul> <li>●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●</li></ul>
> 更新 > ログのビューアー	アクセスしたウェブサイト ウェブサイト http://il.sdlcdn.com/ http://cdn.shopclues.net/ http://cdn.shopclues.com/ http://i4.sdlcdn.com/ http://i3.sdlcdn.com/ http://i.ebayimg.com/ http://i2.sdlcdn.com/	カテゴリー         ジェネラル         ジェネラル         ショッピング         ジェネラル         ジェネラル         ジョッピング         ジェネラル         ジョッピング         ジョッピング         ジェネラル         ジョッピング         ジェネラル         ジェネラル         ジェネラル         ジェネラル         ジェネラル         ジェネラル	すべて表示 アクセス数 ▼ 189 132 117 97 95 92 86 76	★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	<ul> <li>●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●</li></ul>

2. **[アクセス数]** をクリックすると、次のようなウェブサイトへの訪問の詳細レポートが表示されます。

ウェブサイトのアク	セス > 詳細報告			
ウェブサイト:	http://i1.sdlcdn.com/			
カテゴリー <mark>:</mark>	ジェネラル			
<b>表示:</b> 送信者	11-10-2015	宛先 11-10-2015		<b>→</b>
日時 ▼	ウェブサイトURL	ユーザー名	IPアドレス	🞒   🧏   劑 インターネ
2015-10-11 04:01:15	http://i1.sdlcdn.com/img/bra.	丸山	192.168.171.12	1 5.12 KB 🔺
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 13.28 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/static/i	丸山	192.168.171.12	1 30.21 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 13.68 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 15.96 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 11.54 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 17.21 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/static/i	丸山	192.168.171.12	1 9.96 KB
2015-10-11 04:00:51	http://i1.sdlcdn.com/img/ma.	丸山	192.168.171.12	1 13.77 KB 🗸

3. ウェブサイトへのアクセスレポートページで **[アクセスの多いユーザー]**列の**ユー ザー名**をクリックすると、そのウェブサイトへ頻繁にアクセスしているユーザーの 詳細レポートが表示されます。



## メール保護

Seqrite Terminator は、受信および送信するメールの添付ファイルが感染していない かどうかをスキャンします。メール保護レポートには、受信および送信メールのスキャ ンプロセスについての統計が表示され、これには感染したメールが送信または受信され た日時、送信者、受信者、件名、存在する場合は添付ファイル、および行われた処置の 詳細が含まれます。このレポートは、Excel、PDF、Word フォーマットでエクスポート できます。

メール保護レポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [メール保護] ヘログオンします。次 のページが表示されます。

Searite		<b>\$</b>	オプション -	<b>?</b> ヘルプ -   (	<b>シャット</b> ダウン	/する -   🔁 A	dmin (管理) -
TERMINATOR		ホーム コン	/テンツフィルタ	マリング ユ <sup>、</sup>	ーザー管理	設定 ログ	どしポート
> インターネット利用	電子メール保護	É				先月   (	<b>Oct-15</b>   来月
> ウェブサイトのアクセス							
電子メール保護 →			7				
▶ ウェブ保護							
▶ 侵入防止							
▶ ポリシー違反の試み							
> 帯域幅使用							
> アプリケーションコントロール	1 2 3 4 5	6 7 8 9 10	0 11 12 13 14	15 16 17 18 19	20 21 22 23	24 25 26 27 28	29 30 31
> ファイアウォール	トークルレポート	(10)					
<ul><li>&gt; ファイアウォール</li><li>&gt; 更新</li></ul>	トータルレポート	(10) 送信 <del>业</del>	<b>惑</b> 信 <b>半</b>	件夕	で絵中	珊山	📓   🎽   🚰
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼	(10) 送信者	受信者	件名	で検出	<b>理由</b>	<ul> <li>         ・</li> <li>         ・</li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 マ 2015-10-13 16:1	(10) 送信者 somesh@mar	受信者 somesh@mar	件名 TEST virus eicar	<b>で検出</b> アンチウイルス	<b>理由</b> 検出されたウ	<ul> <li>・</li> <li>・</li></ul>
<ul> <li>&gt; ファイアウォール</li> <li>&gt; 更新</li> <li>&gt; ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 16:0	(10) 送信者 somesh@mar somesh@mar	受信者 somesh@mar somesh@mar	件名 TEST virus eicar テスト	<b>で検出</b> アンチウイルス アンチウイルス	<b>理由</b> 検出されたウ 検出されたウ	<ul> <li>・</li> <li>・</li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 16:0 2015-10-13 15:5	(10) 送信者 somesh@mar somesh@mar yuto@marvel	受信者 somesh@mar somesh@mar test1@marve	件名 TEST virus eicar テスト 新規ファイル	で検出 アンチウイルス アンチウイルス 添付ファイル	<b>理由</b> 検出されたウ 検出されたウ ブロックされ	<ul> <li>・</li> <li>・</li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 15:5 2015-10-13 15:5	(10) 送信者 somesh@mar somesh@mar yuto@marvel yuto@marvel	受信者 somesh@mar somesh@mar test1@marve test1@marve	件名 TEST virus eicar テスト 新規ファイル 新規ファイル	<b>で検出</b> アンチウイルス アンチウイルス 添付ファイル 添付ファイル	<b>理由</b> 検出されたウ 検出されたウ ブロックされ ブロックされ	<ul> <li>・</li> <li>・</li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 16:0 2015-10-13 15:5 2015-10-13 15:5	(10) 送信者 somesh@mar somesh@mar yuto@marvel yuto@marvel kana@marvel	受信者 somesh@mar somesh@mar test1@marve test1@marve test1@marve	件名 TEST virus eicar テスト 新規ファイル 新規ファイル TEST Attachm	で検出 アンチウイルス アンチウイルス 添付ファイル 添付ファイル	<b>理由</b> 検出されたウ 検出されたウ ブロックされ ブロックされ	<ul> <li>・・     <li>・     <li>・・     </li> </li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 16:0 2015-10-13 15:5 2015-10-13 15:5 2015-10-13 15:4	(10) 送信者 somesh@mar somesh@mar yuto@marvel kana@marvel kana@marvel	受信者 somesh@mar somesh@mar test1@marve test1@marve test1@marve	件名 TEST virus eicar テスト 新規ファイル 新規ファイル TEST Attachm TEST Attachm	で検出 アンチウイルス アンチウイルス 添付ファイル 添付ファイル 添付ファイル 添付ファイル	<b>理由</b> 検出されたウ 検出されたウ ブロックされ ブロックされ ブロックされ	<ul> <li>・</li> <li>・</li></ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 16:0 2015-10-13 15:5 2015-10-13 15:5 2015-10-13 15:4 2015-10-13 15:3	(10) 送信者 somesh@mar somesh@mar yuto@marvel yuto@marvel kana@marvel kana@marvel test1@marve	受信者 somesh@mar somesh@mar test1@marve test1@marve test1@marve test1@marve	件名 TEST virus eicar テスト 新規ファイル 新規ファイル TEST Attachm TEST Attachm	で検出 アンチウイルス アンチウイルス 添付ファイル… 添付ファイル… 添付ファイル… キーワードブ…	理由 検出されたウ 検出されたウ ブロックされ ブロックされ ブロックされ ブロックされ	<ul> <li>・ 込 ー</li> <li>・ アクションン</li> <li>・ 12213</li> <li>・ 消除と</li> <li>・ 消除と</li> <li>・ 消除と</li> <li>・ 消除と</li> <li>・ 消除と</li> <li>・ パリジ</li> </ul>
<ul> <li>ファイアウォール</li> <li>更新</li> <li>ログのビューアー</li> </ul>	トータルレポート 日時 ▼ 2015-10-13 16:1 2015-10-13 15:5 2015-10-13 15:5 2015-10-13 15:4 2015-10-13 15:4 2015-10-13 15:3 2015-10-13 15:3	(10) 送信者 somesh@mar somesh@mar yuto@marvel yuto@marvel kana@marvel kana@marvel test1@marve	受信者         somesh@mar         somesh@marve         test1@marve         test1@marve         test1@marve         somesh@marve <somesh@m< td=""></somesh@m<>	件名 TEST virus eicar テスト 新規ファイル 新規ファイル IEST Attachm TEST Attachm テストメール テストメール	<b>で検出</b> アンチウイルス アンチウイルス 添付ファイル… 添付ファイル… 添付ファイル… キーワードブ… キーワードブ…	理由 検出されたウ 検出されたウ ブロックされ ブロックされ ブロックされ ブロックされ ブロックされ	<ul> <li>・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>

# ウェブ保護

ウェブ保護レポートには、ブロックしたウェブサイト、そのウェブサイトにアクセスした日付と時刻、アクセスしたウェブサイトの URL、ユーザーの IP アドレスについての情報が含まれています。この情報をもとに、サイトがブロックされた理由を分析できます。ユーザーがアクセスしたフィッシングサイトや、不正および有害なウェブサイトについての詳細も含まれています。

ウェブ保護レポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [ウェブ保護] ヘログオンします。次のページが表示されます。次のページが表示されます。



# 侵入防止

侵入防止レポートは、Terminator によって防止された侵入についての情報を提供しま す。侵入が防止された時間、シグネチャ名、活動、活動の優先度、プロトコル情報、そ の他の詳細が含まれています。さらにセキュリティポリシーの問題を特定して既存の脅 威を記録し、セキュリティポリシー違反から個別のユーザーを見つけ出します。

ポリシー違反レポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [侵入防止] ヘログオンします。次の ページが表示されます。

Seqrite			🌞 オブ	ション -	<mark>?</mark> ^л	プ -   也	シャットダウ	シする 🗕 🛛 🗧	﴾ Admin (管理) ▼
TERMINATOR		ホー2	A コンテ	ンツフィ	ルタリング	" ユー	ザー管理	設定	コグとレポート
> インターネット利用	侵入防止								
> ウェブサイトのアクセス	表示:	送信者	13-10-2015		宛先	13-10-20	15	<b>→</b>	
➤ 電子メール保護									
> ワェブ保護									
<ul> <li>・ ボリシー違反の試み</li> </ul>									
<ul> <li>▶ 帯域幅使用</li> </ul>									
> アプリケーションコントロール							(spp. reputatio	nn) nackets blacklis	ł
> ファイアウォール							_ (obb_) obgrand	(100.00	%)
> 更新									
> ログのビューアー							すべて表	<u>र</u>	🖳   ≽   🕋
	日時 ▼	署名	アクテ	優先	ブロト	送信元IP	ソースポ	受信者IP	宛先ボ
	2015-10-13 17:	(spp_re	<u>-</u>	2	ICMP	10.10.10	-	10.10.104.167	- *
	2015-10-13 17:	(spp_re	·	2	ICMP	10.10.10		10.10.104.169	) -

## ポリシー違反活動

ポリシー違反レポートには、企業で設定され、実装されているポリシーに違反するイン ターネットへのアクセスの試みについての情報が表示されます。このレポートは、特定 の1日、過去7日間、過去30日間について入手できます。レポートには、違反の日 付と時刻、ウェブサイトのURL、サイトのカテゴリが含まれています。このレポートに よって、ユーザー名、グループ名、ポリシーに違反するユーザーのIPアドレスを一緒 にマップできます。このレポートは、Excel、Word、PDFフォーマットでエクスポート できます。

ポリシー違反レポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [ポリシー違反活動] ヘログオンしま す。次のページが表示されます。

Searite		🔅 オブシ	ョン   <mark>?</mark> ヘルプ	・1 😃 シャッ	トダウンする 🗸	┣ ➡ Admin (管理	<b>里)</b> -
TERMINATOR	*	ーム コンテン	ツフィルタリング	ユーザー管	寶理 設定	ログとレボー	÷
<ul> <li>・ インターネット利用</li> <li>・ ウェブサイトのアクセス</li> <li>・ 電子メール保護</li> <li>・ ウェブ保護</li> <li>・ 侵入防止</li> <li>・ ポリシー違反の試み </li> <li>▶</li> <li>・ 帯域幅使用</li> <li>・ アブリケーションコントロール</li> <li>&gt; ファイアウォール</li> <li>&gt; 更新</li> </ul>	ボリシー違反の言	式み		Socia	今日 過去 7[ J Networking (100.00%)	3間 過去 30日	
. цужец у						B)   😕	
	日時▼	ウェブサイトURL	カテゴリー	ユーザー名	グループ名	IPアドレス	
	2015-10-13 19:00:30	http://www.face	ソーシャルネット	yuto	default	192.168.173.26	*
	2015-10-13 19:00:30	http://platform.t	ソーシャルネット	yuto	default	192.168.173.26	
	2015-10-13 19:00:20	http://connect.fa	ソーシャルネット	yuto	default	192.168.173.26	
	2015-10-13 18:40:20	http://www.face	ソーシャルネット	yuto	default	192.168.173.26	
	2015-10-13 18:40:20	http://platform.t	ソーシャルネット	yuto	default	192.168.173.26	-

# 带域幅使用量

帯域幅使用量のレポートには、インターネットの帯域幅使用量についての情報が表示されます。一定の時間にユーザーが使用した帯域幅の情報を提供します。このレポートは、 当日、過去 7 日間、過去 30 日間について入手できます。このレポートを使用して、 帯域幅使用量についてのポリシーを策定できます。

帯域幅使用量レポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [帯域幅使用量] ヘログオンします。 次のページが表示されます。

Cogrito			🔅 オブション -   <mark>?</mark> ヘルプ	-   🕛 シキ	<b>灬トダウンす</b>	る -	➡ Admin (管理) -
TERMINATOR		ホーム	コンテンツフィルタリング	ユーザー	-管理 :	没定	ログとレポート
> インターネット利用	帯域幅使用				今日	過去 7日間	引 過去 30日間
> ウェブサイトのアクセス							📑 ا ≽ ا
> 電子メール保護	ユーザー	アップロ	—	ダウン	ㅁㅡᅣ" (MB)	•	
▶ ウェブ保護	somesh	0.91		20.34			
▶ 侵入防止	192.168.173.23	0.16		9.99			
▶ ボリシー違反の試み							
帯域幅使用 ▶							
> アプリケーションコントロール							
> ファイアウォール							
<b>&gt;</b> 更新							
▶ ログのビューアー							

# アプリケーションコントロール

アプリケーションコントロールレポートは、Terminator によって防止されたアプリケ ーションについての情報を提供します。防止されたアプリケーションのタイムスタンプ、 アプリケーション名、および関連するカテゴリについての詳細が含まれています。

アプリケーションコントロールレポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [アプリケーションコントロール] へ ログオンします。次のページが表示されます。

Searite			🔅 オブ:	/ヨン -   ?	ヘルプ -   (	) シャットダウン™	する <del>-</del>   🔁 A	dmin (管理) -
TERMINATOR		ホーム	コンテン	ハツフィルタリ	ング ユー	-ザー管理	設定 ロク	"とレポート
> インターネット利用	ファイアウォー	-ル						
> ウェブサイトのアクセス	表示: 道	送信者 13	3-10-2015		宛先 13-10-2	2015	<b>→</b>	
<ul> <li>電子メール保護</li> <li>ウェブ保護</li> </ul>								
▶ 侵入防止			138 (12 40340 (0	33%)		— 40351 (0.59%)		
▶ ポリシー違反の試み						— 17500 (40.23%)		
> 帯域幅使用								
▶ アプリケーションコントロール			137 (45	.96%)				
ファイアウォール・								
> 更新								
> ログのビューアー						すべて表示	~	🗐 i 📐 i 🖻
	日時 ▼	ポリシ	プロトコル	送信元IP	ソースポート	受信者IP		アクション
	2015-10-13 20:	インタ	Internet G	192.168.24	-	224.0.0.1	-	受ける ^
	2015-10-13 20:	インタ	ТСР	10.10.106.1	8880	10.10.104.167	40351	受ける
	2015-10-13 20:	インタ	тср	10.10.106.1	8880	10.10.104.167	40351	受ける
	2015-10-13 20:	インタ	тср	10.10.106.1	8880	10.10.104.167	40351	受ける
	2015-10-13 20:	インタ	ТСР	10.10.106.1	8880	10.10.104.167	40351	受ける
	2015-10-13 20:	インタ	UDP	10.10.104.86	17500	255.255.255.25	5 17500	受ける
	2015-10-13 20:	インタ	UDP	10.10.107.2	137	10.10.107.255	137	受ける
	2015-10-13 20:	インタ	UDP	10.10.104.86	17500	255.255.255.25	5 17500	受ける
	2015-10-13 20:	インタ	UDP	10.10.104.1	137	10.10.107.255	137	受ける 🗸

# ファイアウォールレポート

ファイアウォールレポートには、ファイアウォール ルールでログオプションが有効に されている場合、ファイアウォールルールにマッチする、インターネットアクセス/ト ラフィックの情報が表示されます。ファイアウォールレポートを表示する期間を選択で きます。日時、ポリシー名、ソース IP、ソースポート、宛先 IP、宛先ポート、処置な どの詳細がファイアウォールレポートに表示されます。

このページには、Terminator からアクセスされる上位 5 つのサービス (宛先ポート) を示した円グラフも表示されます。このレポートを XLS、ワード、および PDF フォー マットでダウンロードすることもできます。

ファイアウォールレポートを表示するには、以下の手順に従います。

1. Seqrite [Terminator] > [ログとレポート] > [ファイアウォール] ヘログオンしま す。次のページが表示されます。

Sogrito			🔅 オブション -	·   <b>?</b> へルナ	・ -   😃 シャッ	トダウンする 🗸	│ 🔁 Admin (管理) 🔻
TERMINATOR		ホーム	コンテンツフィル	ルタリング	ユーザー管	理 設定	ログとレポート
▶ インターネット利用	アプリケーシ	ョンコントロ	ール				
> ウェブサイトのアクセス	表示:	送信者 12-1	0-2015	宛先 14-	10-2015	<b>→</b>	
▶ 電子メール保護							
▶ ウェブ保護							
▶ 侵入防止							
▶ ボリシー違反の試み							
> 帯域幅使用							
アブリケーションコントロール					Search E	ngines & Portals	
> ファイアウォール						(100.00%)	
▶ 更新							
▶ ログのビューアー							
					व/	て表示	× 1911 🕹 1 🖭
	日時 ▼		アブリケーション	カテ	ゴリ		
	2015-10-13 19:0	0:20	Bing	検索	エンジンとボータ	UL	<u>^</u>
	2015-10-13 19:0	0:19	Bing	検索	<b>エンジンとボー</b> タ	บป	
	2015-10-13 19:0	0:16	Bing	検索	<b>エンジン</b> とボータ	UL	
	2015-10-13 19:0	0:16	Bing	検索	エンジンとボータ	01J	
	2015-10-13 18:4	0:10	Bing	検索	<b>エンジンと</b> ボータ	υL	
	2015-10-13 18:4	0:10	Bing	検索	エンジンとボータ	171J	
	2015-10-13 18:4	0:10	Bing	検索	エンジンとボータ	17L	
	2015-10-13 18:4	0:10	Bing	検索	エンジンとボータ	บป	
	2015-10-13 18:2	0:07	Bing	検索	エンジンとボータ	บป	$\sim$

# アップデート

このレポートは、アンチウイルスおよび IPS シグネチャのアップデートの日時につい ての情報を表示します。アップデートが成功すると、アップデートタイプ、バージョン アップデートの場合はアンチウイルスエンジンのバージョン、および期間についてのレ ポートが生成されます。このレポートを使用して、アンチウイルスや IPS シグネチャ の最新のアップデートがシステムに適用されているかどうかをチェックできます。この レポートは、画面のアイコンを使用して Excel、PDF、Word フォーマットでエクスポー トできます。

- アップデートレポートを表示するには、以下の手順に従います。
- 2. Seqrite [Terminator] > [ログとレポート] > [アップデート] ヘログオンします。 次のページが表示されます。

O a switz			トオプション   ? '	ヘルプ -   🕛 シャット	ダウン 📲 📑 Admin (管理	里) -
Sequite TERMINATOR	木-	ーム コンテ	ンツフィルタリング	ユーザー管理	設定ログとレポー	-
> インターネット利用	更新					
> ウェブサイトアクセス テスト・ボルドサ					🗐   ≽	
<ul> <li>         ・ 電子メール保護         、         ・ ブル滞     </li> </ul>	日時▼	更新タイプ	エンジンバージョン	更新元	宛先	
> ワエノ1未設 、 / = ) 1 ☆ 止	2015-11-20 13:08:58	AV Engine	15.00	2015-10-15 11:25:00	2015-11-20 09:00:19	*
2 使八切止 、ポリシー造反の試み	2015-10-14 00:01:50	IPS Engine	2.9.5.5	2015-10-13 00:00:00	2015-10-14 00:00:00	
<ul> <li>・ホリン 建(0) m()</li> <li>・帯域幅使用量</li> <li>・アプリケーションコントロール</li> </ul>						
> ファイアウォール						
更新 ▶						
> ログビュ−ア						Ŧ

### ログビューア

Seqrite Terminator のログビューアを使用して、システムのログファイルをダウンロ ードして参照できます。また、必要のないログを選択してクリアできます。ログビュー アには、すべてのシステムログが、サービスやイベントごとにグループ分けして表示さ れます。

ログは、今日のログ(現在のログ)とアーカイブログの 2 つのタブにグループ分けし て表示されます。

#### [今日のログ] タブ

今日のシステムログが表示されます。これらのログには、Terminator により生成されるメッセージ、ユーザーの活動、管理者の活動、アップデートの他、VPN、DHCP、インターフェースに関連するログが含まれます。必要に応じてログをダウンロードでき、選択して削除することもできます。

#### [アーカイブログ] タブ

このセクションには、イベントやサービスのログがモジュールごとに表示されます。ロ グを月別に参照することもできます。必要に応じて、ログのダウンロードや削除を実行 できます。

[設定] タブ - 古いログファイルのパージ (削除)

[ログビューア] ページの [設定] タブでは、古いログを自動的に削除するためのパー ジサイクルを設定できます。1 日経過したログ、7 日経過したログ、15 日以上経過し たログ、30 日以上経過したログを自動的に削除するよう設定できます。

#### 今日のログの表示

1. [Terminator] > [ログとレポート] > [ログビューア] ヘログオンします。

Searite		🌼 オプション -   ? ・	ヘルブ ៹   😃 シャットダウン ៹	/   🔁 Admin (管理) 🗸
TERMINATOR	ホーム	コンテンツフィルタリング	ユーザー管理 設定	ログとレポート
> インターネット利用	ログビューア		今日's ログ ア	ーカイブログ 設定
> ウェブサイトアクセス				ダウンロード   クリア
▶ 電子メール保護	🔲 モジュール名	サイズ	イベントの数	
▶ ウェブ保護	□ システムメッセージ	0 Bytes	0	<b>^</b>
> 侵入防止	□ ユーザーイベント	0 Bytes	0	
<ul> <li>ボリシー達反の試み</li> </ul>	□ 管理イベント	1.82 KB	34	
> 帯域幅使用量	□ 更新	147 Bytes	2	
<ul> <li>アブリケーションコントロール</li> </ul>	VPN	0 Bytes	0	
<ul> <li>ファイアウォール</li> </ul>	DHCP	0 Bytes	0	
> 更新	□ インターフェース	212 Bytes	3	
				*

- 2. [今日のログ] ページに、Terminator サブシステムの各種のログが、モジュール名、 ログサイズ、ログカウントとともに表示されます。
- 3. 特定のモジュールについて今日のログを表示するには、モジュール名をクリックし ます。そうすると、ポップアップウィンドウが開き、今日の詳細なシステムログが 表示されます。

管理イベント			
<b>.</b>	日付 🗸	管理者名 🔻	メッセージ
i 情報	20/11/2015 04:11:46 PM	admin	からログイン
(1) 情報	20/11/2015 04:10:44 PM	admin	からログイン
(1) 情報	20/11/2015 04:05:15 PM	admin	からログイン
(1) 情報	20/11/2015 03:50:33 PM	admin	からログイン
(1) 情報	20/11/2015 03:49:23 PM	admin	からログイン
😣 エラー	20/11/2015 03:49:19 PM	-	10.10.104.198から管理者の無効なログオンを試行する
(1) 情報	20/11/2015 03:43:07 PM	admin	ログアウト
(1) 情報	20/11/2015 03:20:12 PM	admin	管理者「すずぎ」が正常に編集されました。
(1) 情報	20/11/2015 03:19:56 PM	admin	新しい管理者「すずき」が正常に追加されました。
(1) 情報	20/11/2015 02:33:05 PM	admin	からログイン

詳細ログには、次の詳細が含まれます。

- a. ヘッダにはモジュールの名前、サイズ、ログカウントが表示されます。
- b. ページの最初の列には、生成された各ログの重大度が表示されます。ここで、 [すべて]、[情報]、[警告]、[エラー]、[致命的] といった重大度に応じてログ をフィルタリングできます。
- c. 2 番目の列には、ログが生成された日付と時刻が表示され、その順番で並べ替えることができます。
- d. 3 番目の列には管理者の名前が表示されます。
- e. 最後の列には、ログの実際のメッセージが表示されます。

#### アーカイブログの表示

アーカイブログを表示するには、以下の手順に従います。

1. [Terminator] > [ログとレポート] > [ログビューア] > [アーカイブログ] ヘログ オンします。次に示すように、[アーカイブログ] ページが表示されます。

ログとレポート

ログのビューアー		今日'sログ <b>アーカイブログ</b> 設定
		ダウンロード   削除
モジュール名 ユーザーイベント 🔻		先月   May-2015   来月
□日付	サイズ	イベルの教
□ 16-06-2013	73 Bytes	1
14-06-2013	6.36 KB	86
13-06-2013	569 Bytes	8
11-06-2013	1.77 KB	24
10-06-2013	7.30 KB	100
09-06-2013	133 Bytes	2
07-06-2013	5.08 KB	70
06-06-2013	3.13 KB	44
05-06-2013	5.88 KB	84

- 2. ドロップダウンから**モジュール名**を選択します。選択したモジュールについて、今 月のログが表示されます。
- 3. 前の月や次の月のログも表示できます。

#### ログファイルの自動削除

Terminator が古いログファイルを自動的に削除するよう設定するには、以下の手順に 従います。

1. [Terminator] > [ログとレポート] > [ログビューア] > [設定] ヘログオンします。 次のページが表示されます。

ログのビューアー	今日'sログ アーカイブ・ログ 設定
自動的なログファイルを削除します。	保存
ログファイルを削除しないでください 🔽	一定の年数に違したときに、システムが自動的にロ グファイルを削除させることができます。

2. ドロップダウンから期間を選択します。ログを削除したい場合は、[保存] をクリッ クします。Terminator は、指定された時間が経過するとログファイルを自動的に削 除します。

### レポートを削除する

レポートの削除セクションで、指定した期間の複数モジュールのレポートを削除できます。 レポートを削除するには、以下の手順を実施します。

1. ログとレポート > レポートの削除を開きます。

Sogrito	🌞 オブション 🤋  ヘルブ 🗸 📋 シャットダウン 🗸	🔁 Admin (管理) 🚽
TERMINATOR	ホーム コンテンツフィルタリング ユーザー管理 設定	ログとレポート
> インターネット利用	レポートを削除します	削除
> ウェブサイトアクセス		
▶ 電子メール保護	□ インターネット 使用量とウェブサイト アクセス	
> ウェブ保護	■ 電子メール保護	
> 侵入防止	□ ウェブ保護	
▶ ポリシー違反の試み	□ 侵入防止	
> 帯域幅使用量	□ ポリシー違反の試み	
> アプリケーションコントロール	□ 帯域幅使用量	
> ファイアウォール	アプリケーションコントロール	
<b>&gt;</b> 更新	ファイアウォール	
> ログビューア	□ 更新	
レポートを削除します	期間: 削除レポート 全て ▼	
	<b>注意:</b> 削除する前にレポートをバックアップすることを推奨します。	

- 2. 削除したいレポートのモジュールを選択します。
- 3. 期間を選択します。以下の選択肢から選択できます。
  - a. すべて: 選択したモジュールのすべてのレポートを削除できます。
  - b. 今日以外:今日のレポート以外の選択したモジュールのすべてのレポートを削除できま す。
  - c. 指定日まで:指定日までの選択したモジュールのレポートを削除できます。

例:

「指定日まで」のオプションで2016年3月15日を選択した場合、最初から2016年3月 15日までのレポートを削除できます。

4. [削除する] をクリックします。

注意:削除する前にレポートのバックアップを取ることを推奨します。



# 通知

Seqrite Terminator からの通知は、ゲートウェイレベルで発生するセキュリティ関連 のすべてのイベントについて、メールや SMS で即座に伝えるものですこれらのイベン トはエラー、警告、情報のカテゴリに分類されます。

これらの通知は、システムで生成されるイベントについて、管理者により指定された通 りに行われます。システムアラート、ハードウェアステータス、サービスステータス、 セキュリティ、使用量、アップデート情報について通知を行うように設定できます。

# 通知メディア

システムイベントの種類ごとに、その通知を受け取る方法を Terminator で設定できます。Terminator では、次の 2 つのタイプの通知がサポートされています。

- メール通知
- <u>SMS 通知</u>

#### メール通知

システムで生成されるイベントについて、Terminator がメールで通知を送信するよう 設定できます。この設定は、[メール通知] セクションを使用して行います。メール通 知を設定する前に、SMTP が設定済みであることを確認してください(詳細については、 SMTP 設定を参照してください)。

メール通知を設定するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [通知] ヘログオンします。メール通知の設定ペ ージが表示されます。

Searite		🔅 オプション -   🣍 🔨	ルブ・ 🛛 🕐 シャットダウン	ヽ-   🗗 Admin (管理) -
TERMINATOR	ホーム コン	テンッフィルタリング	ユーザー管理 設	定 ログとレポート
<ul> <li>インターネット</li> </ul>	通知		メール設定	SMS設定 通知設定
<ul> <li>アンチウイルス</li> <li>電子メール 保護</li> <li>定義</li> </ul>	電子メール通知: 電子メールアドレスに通知します:	◎ 有効 ● 無効 ◎ 電子メールアドレス	追加∣削除	保存
<ul> <li>ファイアワォール設定</li> <li>IPS</li> <li>アプリケーションコントロール</li> <li>* オロッカ</li> </ul>	デバイス特定テキスト:		-	
> 証明音 > IPSec VPN > PPTP VPN > SSL VPN	注意:電子メール通知を受信すること	「テストメール送信」 、SMTP設定を行う必要がる	⊘	
<ul> <li>・ インターフェース</li> <li>&gt; IPv6</li> <li>&gt; ルーティング</li> </ul>				
<ul> <li>&gt; DNS</li> <li>&gt; DHCP</li> <li>&gt; ダイナミックDNS</li> </ul>				
<ul> <li>&gt; USBモデム</li> <li>&gt; ロードバランシング</li> <li>&gt; 管理</li> </ul>				
<ul> <li>通知 ▶</li> <li>・ バックアップ</li> </ul>				

- 2. メール通知を有効にするには、[有効]を選択します。
- 3. [メールアドレスから通知] に入力します。メール通知は、このメールアドレスから 送信されます。
- 4. [メールアドレスに通知] に入力します。これは、メール通知の送信先となるメール アドレスのリストです。必要に応じて、[追加] または [削除] を使用してリストを 編集します。
- 5. [デバイス特定テキスト] に入力します。これは、通知の送信元であるデバイスの簡 単な説明です。
- 6. [テストメールを送信] をクリックします。設定されたメールアドレスへテストメー ルが送信されます。

#### SMS 通知

SMS を送信するように Terminator を設定することができます。または、システム生成イベン トやゲストユーザー認証用に SMS ゲートウェイを追加して SMS 通知を送ることができます。 SMS 通知を送るように Terminator を設定するには、以下の手順を実施します。

注意:Terminator の SMS ゲートウェイを設定し、SMS 通知機能を Terminator で有効にするに は、Terminator サポートチームに問い合わせなければなりません。 1. Seqrite Terminator > 設定 > 通知 > SMS 設定にログオンします。SMS 通知の設定ページが 表示されます。

Cogrito		🔅 オブション   ? へり	レブ -   😃 シャットダウン -	┣ Admin (管理) -
TERMINATOR	ホーム	コンテンツフィルタリング	マーザー管理 設定	ログとレポート
> インターネット	通知		メール設定 SMS	<b>設定</b> 通知設定
▶ アンチウイルス				保存
▶ 電子メール保護	SMS <u>J</u> 祖失LI:	◎ 有効 ● 無効		
<b>&gt;</b> 定義	携帯電話番号のリスト:	□ 携帯電話番号	追加 削除	
> ファイアウォール設定			*	
> IPS				
▶ アプリケーションコントロール	_		Ψ.	
> 証明書				
> IPSec VPN	SMSゲートウェイ設定			
> PPTP VPN	アクティブなSMSゲートウェイ:	デフォルト・		
> SSL VPN	smsゲートウェイ			追加 削除
> インターフェース	□ 名前	URL		
> IPv6	🔲 хуг	http://www.xyz.com		*
▶ ルーティング				
> DNS				
> DHCP				
→ ダイナミックDNS				-
> USBモデム				
▶ ロードバランシング				
> 管理				
通知				

- 2. SMS 通知を有効にするには、[有効にする]を選択します。
- 通知を受け取りたいモバイルの番号を入力します。リストを管理するために、必要に応じて[追加する]または[削除する]を使います。
   注意:デフォルト SMS ゲートウェイの場合、サポートされている国別コードは +91 と +971 です。
- 4. **残りの SMS** カウントでは、Terminator から送信可能な SMS 通知の合計数が表示されます。 この SMS カウントは、デフォルト SMS ゲートウェイにのみ表示されます。
- 5. 有効な SMS ゲートウェイを選択します。

複数の SMS ゲートウェイを選択し、[削除する] をクリックして SMS ゲートウェイを削除 することができます。

6. [保存する] をクリックします。

#### SMS ゲートウェイを追加する

SMS ゲートウェイ機能の追加で、サードパーティーのゲートウェイを Terminator で使用する ことができます。Terminator では SMS 通知とゲストユーザー認証がデフォルトで使用されて います。

SMS ゲートウェイを追加するには、以下の手順を実施します。

1. 設定 > 通知> SMS 設定を開きます。

2. SMS ゲートウェイ設定セクションで [追加する] をクリックします。

SMS ゲートウェイを追加するためのページが表示されます。

SMSゲートウェイ > 追	加	Save	ancel
名前:	ゲートウェイ名を入力します		
URL:	ゲートウェイURLを入力します		
HTTPメンッド:	● 取得 ○ ポスト		
バラメーターを要求します		例を表示します   Add	Delete
□ バラメーターキー	值		
Enter Key	- Enter Value	保存	×
🔲 User	User 1		*
🔲 mbno	_MOBILE_NUMBER		
📄 mseg	_MESSAGE_		
			Ŧ
<b>ロ</b> グ:	🔲 SMSゲートウェイレスポンスのログを有効にします		
SMSをテストします			

- 3. ゲートウェイの名前を入力します。
- 4. SMS ゲートウェイの URL を入力します。
- 5. HTTP メソッドを選択します。
- 6. パラメーターキーとその値を追加します。

注意:

このパラメーターは、SMS ゲートウェイを設定するサービスプロバイダーから提供されます。 メッセージの送信中、実行時に置き換えられる以下のプレースホルダーを使用できます。

プレースホルダー	意味
----------	----

通知

MESSAGE	このプレースホルダーは、SMS の送信中にメッセー ジテキストに置き換えられます。このメッセージテ キストには、テスト SMS、通知、またはゲストユー ザー認証が含まれます。
COUNTRY_CODE	このプレースホルダーは、SMS の送信中に国別コー ドに置き換えられます。
MOBILE_NUMBER	このプレースホルダーは、SMS の送信中にモバイル 番号に置き換えられます。
COUNTRY_CODE_MOBILE_NUMBER	このプレースホルダーは、SMS のレシーバーを表す ために、連結された国別コードとモバイル番号に置 き換えられます。

Terminator でサードパーティーの SMS ゲートウェイを設定するには、以下の 2 つのプレ ースホルダーが必要なほか、要求パラメーターの下に追加されなければなりません。

\_\_\_MOBILE\_NUMBER\_\_\_

\_\_\_MESSAGE\_\_\_

- 7. SMS ゲートウェイレスポンスのロギングを有効にしたい場合は、**ロギング**オプションを選択 します。
- 8. SMS ゲートウェイが設定されている場合は、[SMS テスト] ボタンをクリックし、テストメ ッセージを送信して確認します。
- 9. [保存] をクリックして、SMS ゲートウェイ設定を保存します。

### SMS ゲートウェイを編集する

SMS ゲートウェイを編集するには、以下の手順を実施します。

- 1. 設定 > 通知> SMS 設定を開きます。
- SMS ゲートウェイ設定セクションで、SMS ゲートウェイ名をクリックします。
   SMS ゲートウェイ編集ページが表示されます。
- 3. 必要な変更を加え、[保存する] をクリックします。

### 通知の設定

システム、ハードウェアステータス、サービスステータス、セキュリティ、使用量、ア ップデート情報に関連するイベントやアラートについて、通知タイプとしてメールと SMS のどちらを送信するかを設定できます。

通知を設定するには、以下の手順に従います。

1. Seqrite [Terminator] > [設定] > [通知] > [通知の設定] ヘログオンします。通 知設定ページが表示されます。

			_
通知		メール設定 SMS設定	通知設定
送信される通知			保存
	すべて展開	すべて折りたたむ  デ:	フォルトにリセット
• アラート			
<b>イベント</b> ライセンスの限界を招えています。		□ 電子メール	SMS
アンチウイルスプロテクションの期限が切れています。			
Terminatorの有効期限が近ついています。 Segrite Terminatorの有効期限が切れました。		<b>S</b>	
ログサイズの制限が近づいています。 WANインターフェースのステータスの変更			
SSL VPNログインイベント。			
<ul> <li>ハードウェアステータス</li> </ul>			
<ul> <li>サービスステータス</li> </ul>			
■ セキュリティと使用量			
■ 更新情報			

2. タブをクリックして、イベントを展開して表示します。イベントについて、通知タ イプとして [メール] または [SMS] を選択します。それぞれの通知タイプについて 以下で説明します。

**アラート**:Seqrite Terminator からの警告、または致命的なシチュエーションで、 管理者へ通知が送信されます。例えば、管理者が「アンチウイルスが最新ではあり ません」のアラートについて、メールおよび SMS での通知を設定していると、アン チウイルスが期限切れになった場合に、メールと SMS が管理者へ送信されます。

**ハードウェアステータス**:管理者は、ハードウェアステータスについての通知を受け取ります。ディスク使用量が 85% に到達すると通知が送信されます。また、CPU 使用量が 90% に到達した場合も通知が送信されます。

サービスステータス:重要なサービスの実行が停止し、ネットワークのセキュリティに支障が出ると、管理者へ通知が送信されます。主なものには HTTP プロキシサービス、コンテンツフィルタリングサービス、アンチウイルスサービス、IPS サービス、メール保護サービスがあります。

**セキュリティと使用量**:ネットワークのセキュリティに支障が発生している、また はインターネット使用量が設定された値を超えている場合、管理者へ通知が送信さ れます。主なものとして、インターネット合計使用量、ブロックしたウイルス数の 合計、防止した侵入の合計、メール保護統計があります。 **アップデート情報:**IPS、アンチウイルス、Terminator 製品アップデートに関する通知が送信されます。

- 3. [すべて展開] リンクをクリックすると、すべてのタブのイベントを表示できます。
- 4. 通知タイプを選択してから、[保存]をクリックします。
- 5. [デフォルトにリセット] リンクをクリックすると、通知の設定をデフォルト設定に 戻すことができます。



# コマンドラインインターフェース (CLI)

コマンドラインインターフェース (CLI) は、ソフトウェアやオペレーティングシステ ムの操作に使用される、テキストベースのインターフェースです。ユーザーは視覚的な プロンプトに対して、インターフェースへ 1 行のコマンドを入力し、同じ方法で応答 が返されます。

## CLI を使用して Seqrite Terminator を設定する

コマンドラインインターフェース (CLI) コンソールは、特定の Seqrite Terminator コンポーネントを管理、監視、制御するための各種ツールを提供します。CLI コンソー ルで Seqrite Terminator ヘアクセスするには、2 つの方法があります。

**直接コンソール接続**:Seqrite Terminator に直接キーボードとモニターを接続します。 **リモート接続**:以下の 2 通りのリモート接続が可能です。

- リモートログインユーティリティ(TELNET)経由で CLI コンソールにアクセス する。
- SSH クライアントを使用して CLI コンソールにアクセスする

(詳細については、<u>コマンドラインインターフェース(CLI)を使用して管理インターフ</u> <u>エースへアクセスする</u>を参照してください)

CLI へのログインが成功すると、次に示す [メインメニュー] 画面が表示されます。



メニュー項目にアクセスするには、[メニュー番号を入力してください]のプロンプト に対して、メニュー項目に対応する番号を入力し、Enter キーを押します。

各サブメニューには [戻る] および [終了] オプションがあります。[**戻る**] で 1 レベ ル上に移動し、[**終了**] で CLI コンソールを終了します。

メニュー	説明
Terminator の設定 と管理	Terminator で利用可能な各種サービスの設定と管理を行います。
サービスの管理	Terminator の各種サービスを管理します。
トラブルシューテ ィング	各種のサービスのトラブルシューティングを行います。
終了	CLI コンソールを終了します。

## Terminator の設定と管理

Seqrite Terminator の CLI コンソールには、利用可能な各種のサービスを設定および 管理するためのオプションが用意されています。

Terminator の設定と管理を行うには、以下の手順に従います。

1. [コマンドラインインターフェース] > [Terminator の設定と管理] ヘログインしま す。

ターミネータの 構成と 管理:
1.製品バージョンを表示する
2. ファクトリーデフォルトのリセットを行う
3.コンソールのパスワードを 変更する
4. ウェブ管理
5. ネット ワーク 構成
◎ デバイス オフライン モード
フ. アップデート
8. ユーザー 管理
9. アプライアンスをリブートする
10.アプライアンスをシャットダウンする
11. 前の
12. 出口
メニュ - 番号を入力します :_

各メニューの説明を、次の表に示します。

メニュー	説明
製品バージョン	このオプションを使用して、Seqrite Terminator の製品バージョ
を表示	ンを表示します。

出荷時デフォル ト設定にリセッ ト	このオプションを使用して、Seqrite Terminator を出荷時デフォ ルト設定にリセットします。
コンソールパス ワードの変更	このオプションを使用して、コンソールパスワードを変更しま す。
ウェブ管理	このオプションから、ウェブ管理の各種のオプションを使用でき ます。
ネットワーク設 定	このメニューを使用してネットワークを設定します。
ユーザー管理	このメニューを使用して、Seqrite Terminator ユーザーを管理し ます。
アプライアンス の再起動	このオプションを使用して、Seqrite Terminator アプライアンス を再起動します。
アプライアンス のシャットダウ ン	このオプションを使用して、Seqrite Terminator アプライアンス をシャットダウンします。

### ウェブ管理

CLI コンソールには、ウェブ管理を行うための各種オプションが用意されています。

 [コマンドラインインターフェース] >[Terminator の設定と管理] > [ログビュー ア] > [ウェブ管理] ヘログインします。

ウェ	ブ 管理:
1.	ウェブ 管理者のパスワードを 変更する
2.	ウェ ブス ーパー 管理者の パスワ ードをリ セット しま す
з.	ウェブ 管理者をログアウトします
4.	全ての 管理者をログアウトします
5.	アプライアンスのウェブアクセスポートを 変更します
6.	前の
7.	
ЧĽ	ュー番号を入力します:

[ウェブ管理] で利用可能なオプションの説明を、次の表に示します。

メニュー	説明
------	----

ウェブ管理者パスワ	このオプションを使用して、Terminator のウェブ管理者パス
ードの変更	ワードを変更します。
ウェブスーパー管理 者パスワードをリセ ット	このオプションを使用して、Seqrite Terminator のウェブス ーパー管理者パスワードをリセットします。
ウェブ管理者をログ	このオプションを使用して、管理者名でウェブ管理者をログア
アウト	ウトさせます。
すべての管理者をロ	このメニューを使用して、すべてのウェブ管理者をログアウト
グアウト	させます。
アプライアンスのウ ェブアクセスポート の変更	このオプションを使用して、プロトコルのポート番号を変更し ます。

### ネットワーク設定

Seqrite Terminator の CLI コンソールには、ネットワーク用の各種のオプションが用 意されています。これらのオプションを使用して、ネットワーク、DNS、スタティック ルートを設定でき、ネットワークを再起動することもできます。

1. コマンドラインインターフェース > [Terminator を設定・管理] > [ネットワーク 設定] ヘログインします。

ネット ワーク 構成:	
1. ネット ワーク 構成	
2. DNSを 構成する	
3. ネットワーク 再開	
4. スタティックルートを 設定する	
5. 前の	
6. 出口	
メニュ ー 番号を 入力しま す :	

[ネットワーク設定] で利用可能なオプションの説明を、次の表に示します。

メニュー	説明
ネットワークを設 定	このオプションを使用して、Seqrite Terminator ネットワー クを設定します。LAN および WAN インターフェースを設定で きます。
DNS の設定	このオプションを使用して、DNS を設定します。

ネットワークの再 起動	このオプションを使用して、ネットワークを再起動します。
スタティックルー	このオプションを使用して、スタティックルートを設定しま
トの設定	す。

#### ネットワークを設定

CLI コンソールから Seqrite Terminator ネットワークを設定するには、以下の手順に 従います。

1. [コマンドラインインターフェース] >[Terminator の設定と管理] > [ネットワーク 設定] > [ネットワークを設定] ヘログインします。

ネットワーク構成 インターフェイス( 名前 ゾ イ eth0 1	: の詳細を取得します。少々お待ちください ーン ステータス IPアドレス IP割り当て ケーブルステータス 情報 LAN オン 10.10.104.194 静的 構成	ゲートウェ 10.10.104.1
1. インターフェー 2. ブリッジを構 3. リンクアグリー 4. ステータスの 5. 削除	イスの 設定 成する ゲーションの 設定 変更	
6. すべて 削除 7. デフォルトル 8. 前の 9. 出口 メニュー番号を入:	ートをセット する 力します : <mark>-</mark>	

このオプションはインターフェース情報を取得し、次の表に示すような各種のオプションを提供します。

メニュー	説明
インターフェース	このオプションを使用して、Seqrite Terminator インターフ
を設定	ェースを設定します。
ブリッジを設定	このオプションを使用して、2 つのインターフェース間のブ リッジを設定します。
リンクアグリゲー	このオプションを使用して、リンクアグリゲーションインタ
ションの設定	ーフェースを設定します。
インターフェース	このオプションを使用して、インターフェースを有効または
ステータスの変更	無効にします。

メニュー	説明
インターフェース またはブリッジの 削除	このオプションを使用して、インターフェースまたはブリッ ジを削除します。
すべてのインター	このオプションを使用して、すべてのインターフェースを削
フェースの削除	除します。
デフォルトルート	このオプションを使用して、インターフェースをデフォルト
の設定	ルートとして設定します。

#### DNS の設定

CLI コンソールで DNS を設定できます。DNS を設定するには、以下の手順に従います。

 コマンドラインインターフェース > [Terminator を設定・管理] > [ネットワーク 設定] > [DNS を設定] ヘログインします。



[DNS を設定] で利用可能な各種のメニューの説明を、次の表に示します。

メニュー	説明
DNS サーバーの表示	DNS サーバーについての情報を表示します。
DNS サーバーの追加	このメニューを使用して DNS サーバーを追加します。
DNS サーバーの削除	このメニューを使用して、DNS サーバーを削除します。

#### スタティックルートの設定

Seqrite Terminator の CLI コンソールには、スタティックルートを設定するための各種のオプションが用意されています。スタティックルートを設定するには、以下の手順に従います。

1. [コマンドラインインターフェース] >[Terminator の設定と管理] > [ネットワー ク設定] > [スタティックルートを設定] ヘログインします。

スタティックルートを 設定する:
Ţ1・スタティックルートリストを表示します
~2.スタティックルートを 追加する
3 . スタティックルートを 削除する
4. スタティックルートを 編集する
5. スタティックルートステータスを 変更する
6. 前の
7. 出口
メニュ - 番号を入力します :

[スタティックルートを設定] で利用機能なオプションの説明を、次の表に示します。

メニュー	説明
スタティックルート	このオプションを使用して、スタティックルートの一覧を確
リストの表示	認できます。
スタティックルート	このオプションを使用して、スタティックルートを追加しま
の追加	す。
スタティックルート	このオプションを使用して、スタティックルートを削除しま
の削除	す。
スタティックルート	このオプションを使用して、スタティックルートを編集しま
を編集	す。
スタティックルート	このオプションを使用して、スタティックルートのステータ
ステータスを変更	スを変更します。

## CLI を使用してサービスを管理する

説明

CLI コンソールには、次のスクリーンショットに示すように、Seqrite Terminator の 各種サービスを管理するためのオプションが用意されています。

サービスの 管理:
1.システムサービスを 再起動する
2.ユ ーザ ーサ ービスを 管理する
3. 前の
4. 出口
メニュ - 番号を入力します :-

[サービスの管理]で使用できる各種メニューの説明を、次の表に示します。

メニュー

システムサービス を再起動	このオプションを使用して、システムサービスを再起動します。
ユーザーサービス の管理	このオプションを使用して、次のようなユーザーサービスを管理 します。 • IPS • アプリケーションコントロール • ポリシーに基づいたルーティング

CLI

#### システムサービスを再起動

[システムサービスを再起動] を使用すると、どのシステムサービスも CLI から再起動 できます。

サービスを再起動するには、以下の手順に従います。

1. コマンドラインインターフェース > [サービスの管理] > [システムサービスを再起 動] を選択します。



2. リストからメニュー番号を入力し、目的のサービスを再起動します。

#### ユーザーサービスの管理

このメニューを使用して、各種のユーザーサービスを管理できます。

1. コマンドラインインターフェース > [サービスの管理] > [ユーザーサービスの管理] へログオンします。

ユーザーサービスを 管理する:		
サービス	構成状態	<u>サー</u> ビスステータス
1. IPS	使用可能。	美行
<ol><li>Application Control</li></ol>	使用不可能	止められる
<ol><li>Policy Based Routing</li></ol>	使用可能	実行
4. 前の		
5. 出口		
メニュ - 番号を入力します :		

[ユーザーサービスの管理]で利用可能な各種メニューの説明を、次の表に示します。

メニュー	説明
IPS	このオプションを使用して、IPS を有効化、無効化、または再 起動します。
アプリケーション	このオプションを使用して、アプリケーションコントロールを
コントロール	有効化、無効化、または再起動します。
ポリシーに基づい	このオプションを使用して、ポリシーに基づいたルーティング
たルーティング	を有効化、無効化、または再起動します。

# CLI によるトラブルシューティング

Seqrite Terminator の CLI コンソールには、次のスクリーンショットに示すように、 各種サービスのトラブルシューティングを行うためのオプションが用意されています。

〈画像〉

トラブルシューティングに使用されるコマンドの説明を、次の表に示します。

メニュー	説明
リモートサポート を開始	このオプションを使用して、リモートサポートを開始します。
データベースユー ティリティ	このオプションには、様々なデータベースユーティリティが用意 されています。
システム情報	このオプションを使用してシステム情報を確認できます。
デバッグ情報	このオプションを使用して Terminator の別のモジュールのデバ ッグ情報を集めます。
ネットワークツー ル	このオプションを使用して、利用可能なネットワークツールを表 示できます。
注意:IPv6 が有効な場合、CLI コンソールから次のモジュールへはアクセスできません。 Terminator の設定と管理 >> 出荷時デフォルト設定にリセット Terminator の設定と管理 >> ネットワーク設定 トラブルシューティング

システムで IPv6 が有効な場合、次のメッセージが表示されます。

⊥Pv6が 有効になっている、このメニューはサポートされません。 メニューを 表示するには 何かキーを 押してください ・・・

データベースユーティリティのトラブルシューティング

データベースユーティリティのトラブルシューティングを行うには、以下の手順に従い ます。

- 1. [コマンドラインインターフェース] >[トラブルシューティング] > [データベース ユーティリティ] ヘログインします。
- 2. Terminator CLI コンソールには、次のスクリーンショットに示すように、各種のデ ータベースユーティリティが用意されています。

データベースユーティリティ:
1. ウェブ 報告書
2. メール保護
3. ウェブ 保護
4. IPSレポート
5.ポリシー違反
6. 更新レポート
7. バックアップと 修復
8.ログ
9.全て
10. 前の
11. 出口
メニュ - 番号を入力します:

[データベースユーティリティ] で利用可能な各種のメニューの説明を、次の表に示します。

メニュー	説明
ウェブレポート	このオプションを使用して、ウェブレポート用データベースを 修復またはクリーニングします。
メール保護	このオプションを使用して、メール保護用データベースを修復 またはクリーニングします。
ウェブ保護	このオプションを使用して、ウェブ保護用データベースを修復 またはクリーニングします。
IPS レポート	このオプションを使用して、IPS レポート用データベースを修 復またはクリーニングします。
ポリシー違反	ユーザーはこのオプションを使用して、ポリシー違反用データ ベースを修復またはクリーニングできます。
アップデートレ ポート	このオプションを使用して、アップデートレポート用データベ ースを修復またはクリーニングします。
バックアップと 復元	このオプションを使用して、バックアップと復元用データベー スを修復またはクリーニングします。
ログ	このオプションを使用して、ログ用データベースを修復または クリーニングします。
すべて	このオプションを使用して、全モジュール用のデータベースを 修復またはクリーニングします。

ネットワークツールのトラブルシューティング

ネットワークツールのトラブルシューティングを行うには、以下の手順に従います。

1. [コマンドラインインターフェース] >[トラブルシューティング] > [ネットワーク ツール] ヘログオンします。

ネットワークツール:	
1. ピュン	
2. dnsルックアップ	
3. ルートをたどる	
4.インターフェース	
5. 前の	
6. 出口	
メニュ - 番号を入力します :	

CLI

[ネットワークツール] で利用可能な各種のメニューの説明を、次の表に示します。

メニュー	説明
Ping	このオプションを使用して、特定の IP アドレスに ping を実行 します。
DNS ルックアッ プ	このオプションを使用して、特定の IP アドレスをルックアップ します。
Traceroute	このオプションを使用して、ネットワークホストに対するトレー スルートパケットを実行します。
インターフェー ス	このオプションを使用して、設定済みのインターフェースについ て必要なすべての情報を表示します。

### デバッグ情報のトラブルシューティング

Seqrite Terminator を使用して、トラブルシューティングに使用できる設定ファイル、 ログファイル、サービスステータス、別のモジュールのデータベース記録などのデバッ グ情報を集めることができます。このデバッグ情報をダウンロードし、サポートチーム に送らなければなりません。

デバッグ情報を集めるには、以下の手順に従ってください。

- 1. [コマンドラインインターフェース] >[トラブルシューティング] > [デバッグ情報] ヘログインします。モジュールリストが表示されます。
- 2. [メニュー番号を入力してください]のプロンプトに対して、メニュー項目に対応す る番号を入力し、Enter キーを押します。複数のモジュールのデバッグ情報を集め たい場合、メニュー番号をコンマで区切ります。
- 3. デバッグ情報は .dbg ファイルに集められ、URL が作成されます。
- 4. ブラウザで URL を入力し、デバッグ情報ファイルをダウンロードします。ダウンロ ードが完了すると、ダウンロードしたファイルはサポートチームと共有されます。

# サポート

サポートページで、Terminator に関連する問題や課題を報告することができます。以下のサポートを利用することができます。

**トラブルシューティング:**診断ツールで、トラブルシュートを実行できるほか、ホスト /IP アドレスが利用できるか確認できます。

**メールサポート:**このサポートタイプを使用して、問題に関するチケットを技術サポートチームに送信できます。

**電話サポート:**このサポートタイプでは、技術サポートセンターに問い合わせて素早く サポートを受けることができます。

**リモートサポート:**このサポートタイプを使用して、サポート担当者が Terminator デ バイスに接続してアクセスできるほか、問題のトラブルシューティングを行うことがで きます。

## トラブルシューティング

サポートチケットを送信する前に、診断ツールでホスト/IP アドレスが利用できるかどうか確認し、検証しなければなりません。IP アドレスへの接続は次のようにして確認することができます。

- 1. [Seqrite Terminator] >[ヘルプ] > [サポート] ヘログオンします。サポートページが表示されます。
- 2. [診断ツール] をクリックします。次のページが表示されます。

Seqrite TERMINATOR	ホーム	🌞 オプション	<b>ヘルプ -</b> リング	<b>()</b> シャットダウン ユーザー管理	/する   設定	► Admin (管理) -
					日付: 13-	Oct-2015 17:05:36 PM
ウェブサポート > 診断ツール						
ホスト/ IPアドレスアベイラビリティをチェックします						
IP /ドメイン名を入力します	; google.co	om				
ビュン ルートをたどる						

- 3. IP/ドメインを入力します。
- 4. [ピン]を入力してホストに接続できるか確認します。
- 5. [経路を調査] をクリックして、経路(パス)とパケット中継での遅れを確認します。

メールサポート

このリンクを使用して、Seqrite Terminator で発生した問題に関するチケットを送信 できます。チケットを送信するには、以下の手順に従います。

1. Sequite [Terminator] >  $[\land \nu \tau]$  >  $[\forall \tau - h]$   $\land \nu \tau \tau$ 

2. [チケットを送信する] をクリックします。

電話サポート

電話によるサポートでは、Seqrite 技術担当者から素早くサポートを得るために電話で ご連絡いただくことができます。

電話でのサポートを希望される場合は、次の番号にお電話ください:

#### 03-6228-3983

サポートチームにお電話いただける日時

月曜日から土曜日

午前 10:00<sup>~</sup>午後 6:30 (JST)

### リモートサポート

Seqrite 技術サポートチームは、場合によってリモートサポートも提供しています。こ のサポートモジュールは、インターネット経由でお客様のコンピュータシステムへ簡単 に接続し、遠隔操作で技術サポートを行います。これにより、Seqrite の技術担当者は お客様の問題を解決するため、効果的なサポートを提供できます。

- リモートサポートを利用するには、以下の手順に従ってください。
- 1. Seqrite [Terminator] >  $[\land \nu \tau]$  >  $[\forall \tau h]$   $\land \nu \tau f$
- 2. [**リモートサポート**] ボタンをクリックします。

Searite		🌞 オブション -   <b>?</b> ヘルブ -   🕐 シャットダウンする -   🖶 Admin (管理) -					
TERMINATOR		ホーム	コンテンツフィルタリング	ユーザー管理	設定 ログとし	レキート	
サポート、清隔サポー	- <b>k</b>						
問題の詳細説明:							
	接続	停止					

3. [問題の詳細説明] を入力し、[チケットを送信する] をクリックします。Seqrite のサポート担当者は、問題を解決するためにお客様のシステムにリモートアクセス します。

### サポート連絡先

Seqrite では、登録済みユーザーを対象に広範な技術サポートを提供しています。お電話の際には、Seqrite のサポート担当者から効率的なサポートを受けられるように、必要な詳細をすべてお手元にご用意いただくことをお勧めします。

#### 電話対応の受付時間

Seqrite は、午前 10 時 00 分から午後 6 時 30 分 (インド標準時間) まで技術サポ ートを提供しています。

### お問い合わせ先電話番号

Seqrite インド国内のユーザーは、03-6228-3983 へお電話ください。

#### インド国外でのサポート

オンラインでの質問の提出や、オンラインチャットの利用については、 http://www.segrite.com/contact\_support をご覧ください(24 時間 365 日対応)。

世界各国の技術サポートの電話番号は、<u>http://www.seqrite.com/int\_techsupp</u>をご覧 ください。

お客様の国内の販売店を調べるには、<u>http://www.seqrite.com/locate-dealer</u> にアク セスしてください。

#### 電話サポートに必要な情報

• 製品が入っていた箱に同梱されているプロダクトキー。オンラインで購入された場合は、注文確認のメールにプロダクトキーが記載されています。

- お使いのコンピュータシステムについての情報: 製品機種、プロセッサのタイプ、 RAM 容量、ハードドライブ容量と空き領域、その他の周辺機器についての情報。
- オペレーティングシステム:名称、バージョン番号、言語。
- インストールされたアンチウイルスソフトウェアやウイルスデータベースのバージョン。
- お使いのシステムにインストールされているソフトウェア。
- ネットワーク接続の有無。接続されている場合は、システム管理者にまずご連絡く ださい。管理者が問題を解決できない場合は、管理者から Seqrite 技術サポートへ ご連絡ください。
- 問題の詳細:最初に問題が発生したのはいつですか?問題が発生したとき、どのよう な操作をしていましたか?

### 技術サポート担当者にお伝えいただく内容

サポート担当者は、お客様からの情報に基づいて解決策を提示するため、できるだけ具体的かつ多くの詳細な情報をお伝えください。

### 本社連絡先

Quick Heal Technologies Limited

(旧会社名 Quick Heal Technologies Pvt. Ltd.)

レジストリオフィス:Office No. 7010 C & D, 7th Floor,

Marvel Edge, Viman Nagar, Pune 411014.

Email: info@seqrite.com

詳細については、次の URL を参照してください。<u>www.seqrite.com</u>

# インデックス

### 6

6to4	トンネルの有効化31	

### С

### D

DHCP	4
DHCP サーバーの追加4	4
DNS	9
DNS キャッシュの削除4	1

### Ι

ID	管理91
ΙP	ポート転送60
IPS	ec62
IPv	ö
IPv	うの有効化31

### M

MIME	フィルタ	リング		8
------	------	-----	--	---

### Р

PBR.			 	 	 50
PBR	の有効	勋化.	 	 	 50
PPTP	VPN.		 	 	 66

### S

SMS 通知159
SMTP 設定137
SSL VPN
SSL VPN サーバーの設定68

### Т

Terminator	の機能12	2
Terminator	へのアクセス1	5

### U

URL	のフィルタリング	114
USB	モデム	37
UTM		12

### V

VLA	N.		 	 																	78
VPN			 	 																	62

### ア

アップデート					154
アプリケーションコントロー	- <i>IV</i> .			122,	153
アンチウイルス	22,	109,	110,	154,	161
アンチスパム					112

### イ

インターネット使用量	 144
インターネット設定	 . 88
インターフェース	 . 32
インターフェースの削除	 . 36
インターフェースの設定	 . 33

### ウ

ウェブサイトアクセスレポート	146
ウェブポータルのカスタマイズ	136
ウェブ保護	150

### エ

エイ	IJ	T	ア	ς.	•		• •			•	•			•	•	 			•			36

### 才

オンラインサポートチケット......174

### 力

カスタムの MIME フィルタリング..... 119 カテゴリに基づいたウェブサイトブロック..... 115

### インデックス

#### キ

キーワードブロック		
-----------	--	--

### グ

グループ		 	91
グループの管理		 	98
グローバル DNS	サーバー	 	39

### ゲ

ゲストユーザー設定	97
-----------	----

#### コ

コマンドラインインターフェース	163
コンテンツフィルタリング	109

#### サ

サイ	$\mathbb{P}$	間																	 	. 1	70	1
サポ	_	$\mathbb{P}$																		1′	74	

### ス

スタティ	イツ	クI	ONS	5		•	 		•				•			. 41
スパム	ブラ	ック	IJ	ス	$\mathbb{P}$		 		•							114

### ダ

ダイナミック	DNS .	 	 	 	 	 	•	 		42
ダッシュボー	ド	 	 	 	 	 		 		21

### デ

デバイスの管	理			 129
デフォルトの	MIME 💈	フィルタ	リング	 118

### ド

ドメインネームサーバー	ドメインネームサー	バー			39
-------------	-----------	----	--	--	----

### $\mathbb{P}$

トラブルシューティング ......165

### ネ

ネットワーク設定.....26

### バ

バックアップ......138

### フ

ファイアウォール	56
ファイウォール	60
フェールオーバー	55

### ブ

ブラックリス	<u>۴</u>	 117
ブリッジ		 81

### ポ

ポリシーベースルーティング5	0
ポリシー違反活動15	$\mathbf{i}1$

#### 朩

```
ホワイトリスト......116
```

### メ

```
メール保護.....109, 111, 149, 167
```

#### ユ

ユーザーg	91
ユーザー管理9	92

### IJ

IJ	リモートサポート	174
IJ	リンクアグリゲーション	. 84

#### ル

ルーティング	48
ルーティングポリシーの削除	54

#### レ

レポー	Ь.											 			 144

#### П

ログ	
ログイン	
ログビューア	

### ワ

ワイヤレスユニバーサルシリアルバス......37

### インデックス

仮	
・ワーク62 ・トワーク	時間:
<b>侵</b> 151	本社
保	管理
出	管理
·	
<b>声</b>	統合相
1	証明
定	
	認証
帯	負荷
復	通知. 通知(
操	除外.
<b>H</b> 129	電子)
	<ul> <li>仮</li> <li>ワーク</li></ul>

カテゴリ	<b>時</b>
<i>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</i>	本
車絡先	······ 177 管
者 者の追加 者プロファイル 者設定	
日 [1] 人	統
肖威官理	
青の官理	認
····	<u>角</u>
分散	55 通
の設定	
	。 
メール通知	158