SEQRITE

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

商標

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（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。

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

トへ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 や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。Seqrite 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。

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、www.seqrite.com/eula を参照してください。

目次

Chapter

1

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。

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。

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。

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。

2. 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。
4. 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. ［追加］をクリックします。

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。

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。

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。

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。

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。

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。

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。

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。

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。

Chapter

3

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 へアクセスする方法は 2 つあります。

- ウェブ経由で Terminator へアクセスする
- CLI 経由で Terminator へアクセスする

ウェブ経由で Terminator へアクセスする

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 へアクセスする

ウェブインターフェースを使用して Seqrite Terminator へログインする他に、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 へ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

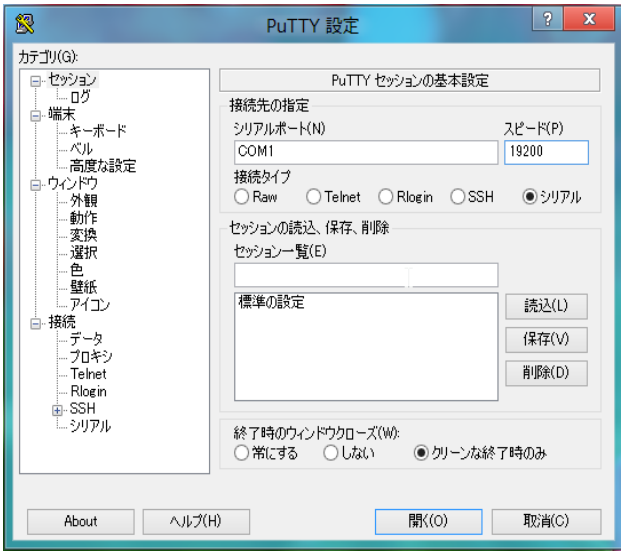
- **直接接続**:キーボードとモニターを、VGA またはコンソールケーブル（COM ポート）を使用して直接 Seqrite Terminator へ接続できます。

  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。

  - ボーレートを 19,200 に設定します。

- 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:



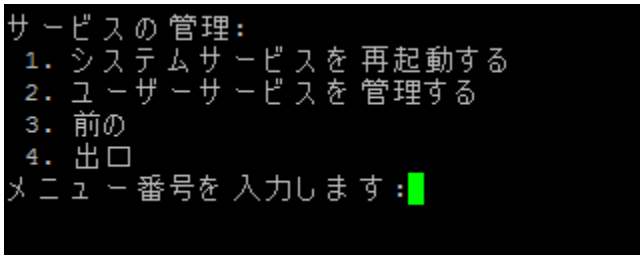
- **リモート接続**:次の方法で、Seqrite Terminator へリモート接続できます:
  - リモートログインユーティリティを使用して、CLI コンソールへアクセスします。
  - 「Telnet xxx.xxx.xxx.xxx」と入力します。xxx.xxx.xxx.xxx は Terminator サーバーの IP アドレスです。

    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。

タブ	機能
オプション	**ウェブパスワードの変更** – ユーザーのパスワードを変更します。 [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。 **現在のパスワード**: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。 **新しいパスワード**:設定したい新しいパスワードを入力します。 **パスワードの再入力**: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。 **新しいパスワード**:設定したい新しい CLI パスワードを入力します。 **パスワードの再入力**: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。 **SSL 証明書** – 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	**ヘルプ** – 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。 **ライセンス情報** – 現在のライセンス情報を表示します。 **サポート** – 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。 **ログアウト**:デバイスからログアウトします。

Chapter

4

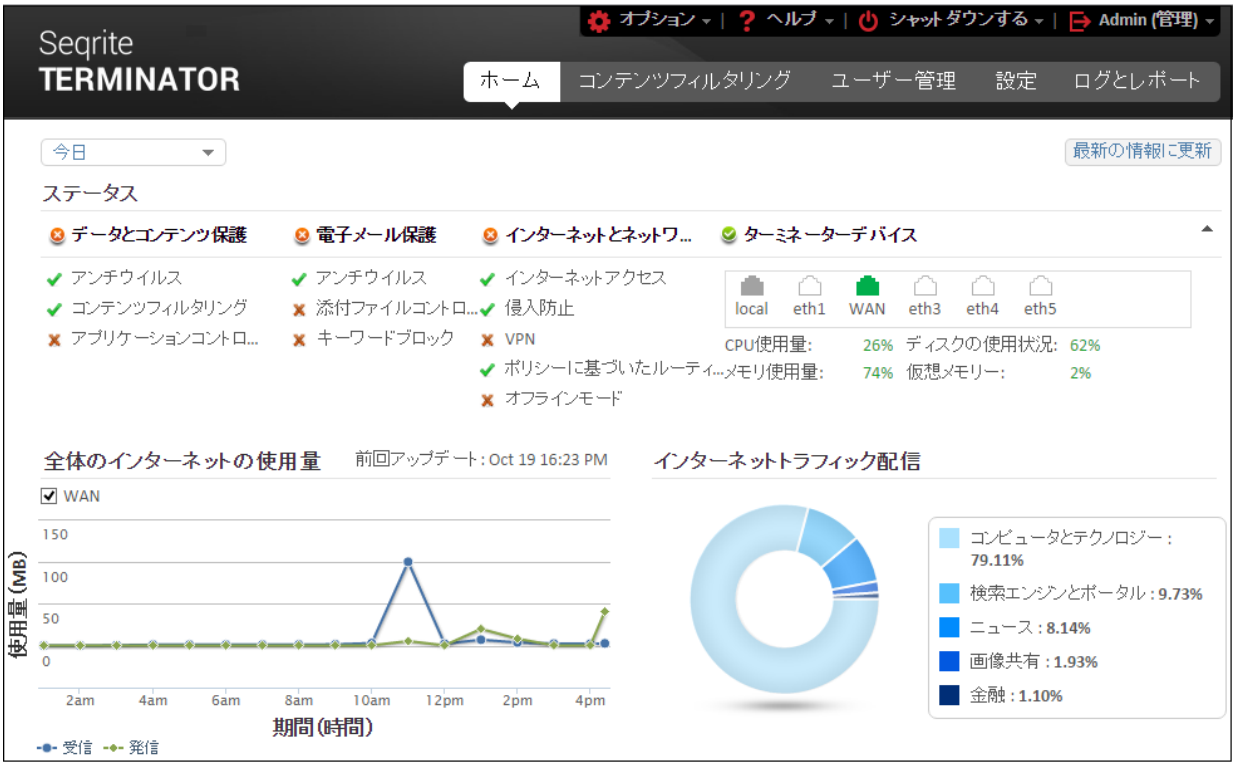
ダッシュボード

ホームページ（ダッシュボード）は、Seqrite Terminator へ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



- **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

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。

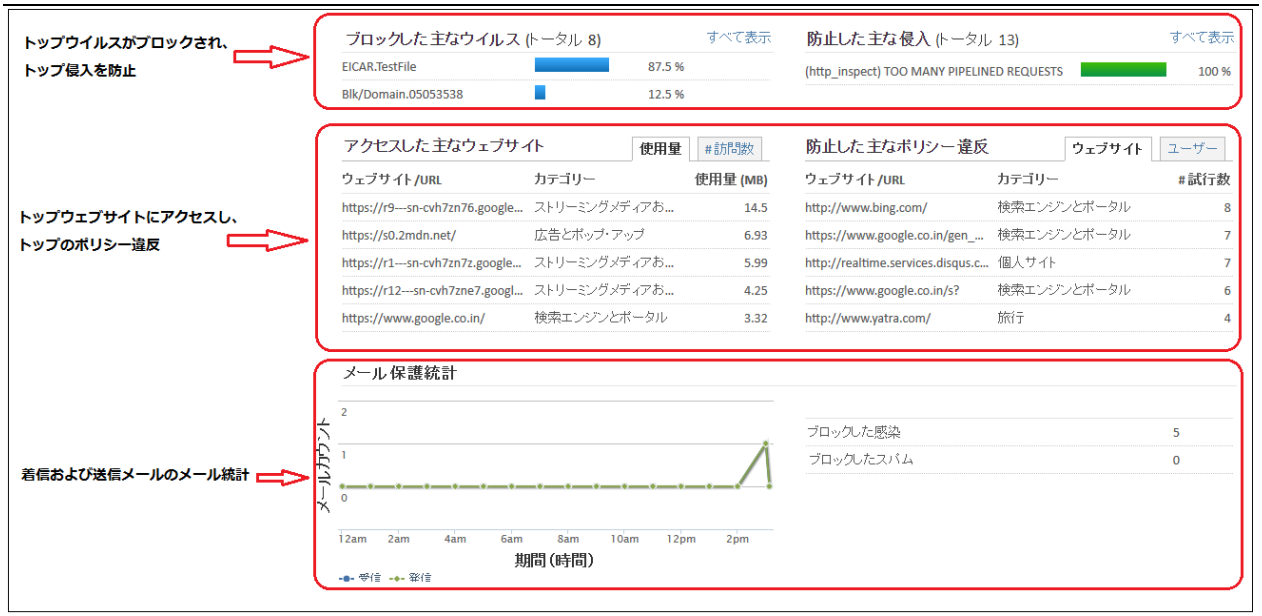
✖	モジュールが無効であるか、有効だが実行されていないことを示しています。

- **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。
	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



- **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

5

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] へログオンします。次に示すページが表示されます。

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 [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]** へログオンします。

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。

4. サービス定義の **[名前]** を入力します。

5. **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。

7. **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]** へログオンします。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、インターネットへ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 2^32 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]** へログオンします。デフォルトでは、IPv6 サポートは無効化されています。

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**] へログオンします。
2. [**6～4**] をクリックします。次のページが表示されます。

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] へログオンします。インターフェースのリストが表示されます。

2. 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。

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。

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、IPv6 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、IPv6 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、IPv6 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]** へログオンします。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。
3. **[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]** へログオンします。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。

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。

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]** へログオンします。[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。

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。

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:

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]** へログオンします。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。

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]** へログオンします。[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]** へログオンします。[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]** へログオンします。[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]** へログオンします。[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。

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]** へログオンします。[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]** へログオンします。次に示す画面が表示されます。

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、インターフェース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**］へログオンします。

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。

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 Eth0 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。

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 Eth0 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]** へログオンします。
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。

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]** へログオンします。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]** へログオンします。

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。

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。

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

- スタティックルーティング
- 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。

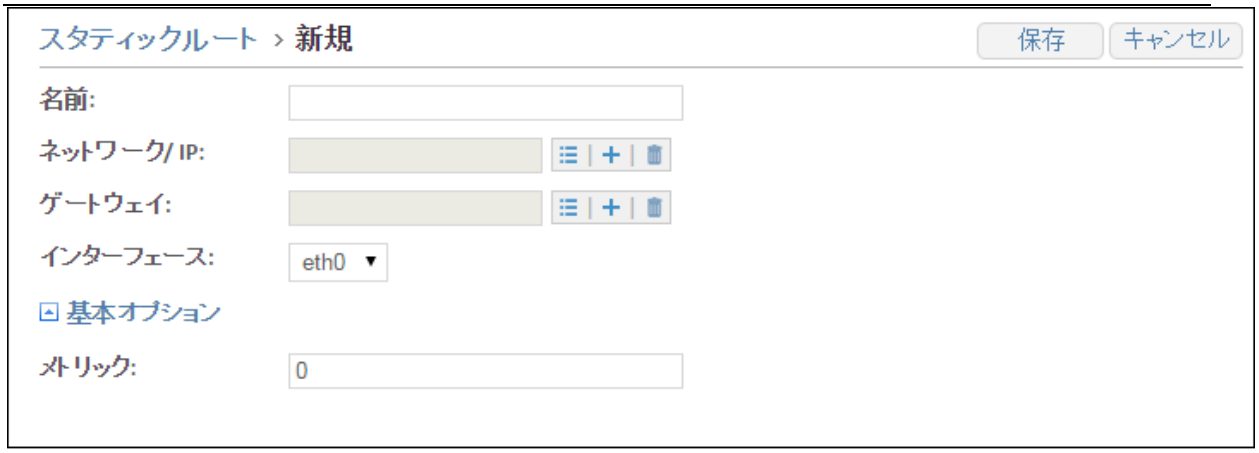
Terminator のスタティックルート機能により、パケットを特定の宛先へ転送するために Terminator が使用可能なルートを設定できます。スタティックルートにより、設定されているデフォルトゲートウェイ以外のゲートウェイを使用して、パケットが宛先へ転送されます。Terminator を使用すると、ルートの追加や削除が可能です。ルートを OFF に設定すると、そのスタティックルートは、デバイスのルーティングテーブルから削除されます。

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] へログオンします。[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。

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。



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。
7. ［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]** へログオンします。

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] へログオンします。
2. [追加] をクリックします。次のページが表示されます。

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)定義(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） へ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]** へログオンします。
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]** へログオンします。
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]** へログオンします。

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。

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]** へログオンします。[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。

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。

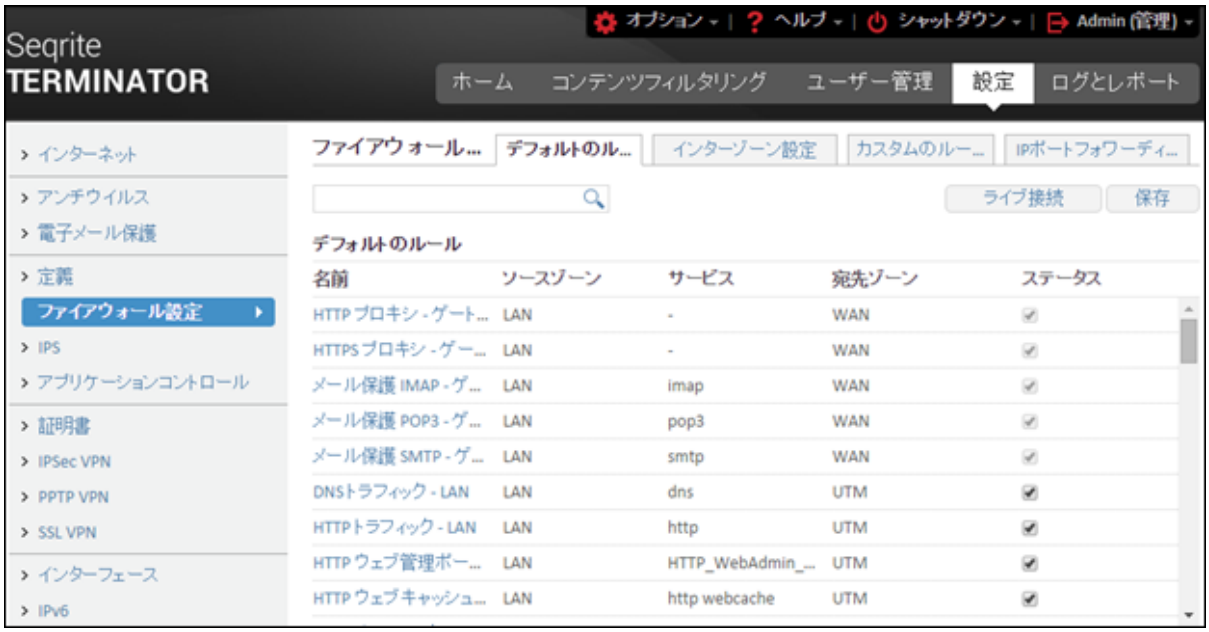
デフォルトのファイアウォールルール

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]** へログオンします。次のページが表示されます。



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]** へログオンします。次のページが表示されます。

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。

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]** へログオンします。次のページが表示されます。

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]** へログオンします。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。

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。 **受け入れる**: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。 **破棄する**: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。 **拒否する**: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	[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。[送信元ゾーン] リストには、[LAN]、[WAN]、[DMZ]、[VPN]、[UTM]、[ブリッジ] が含まれています。
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]** 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へ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]** へログオンします。[転送] 画面が表示されます。

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]** へログオンします。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。

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

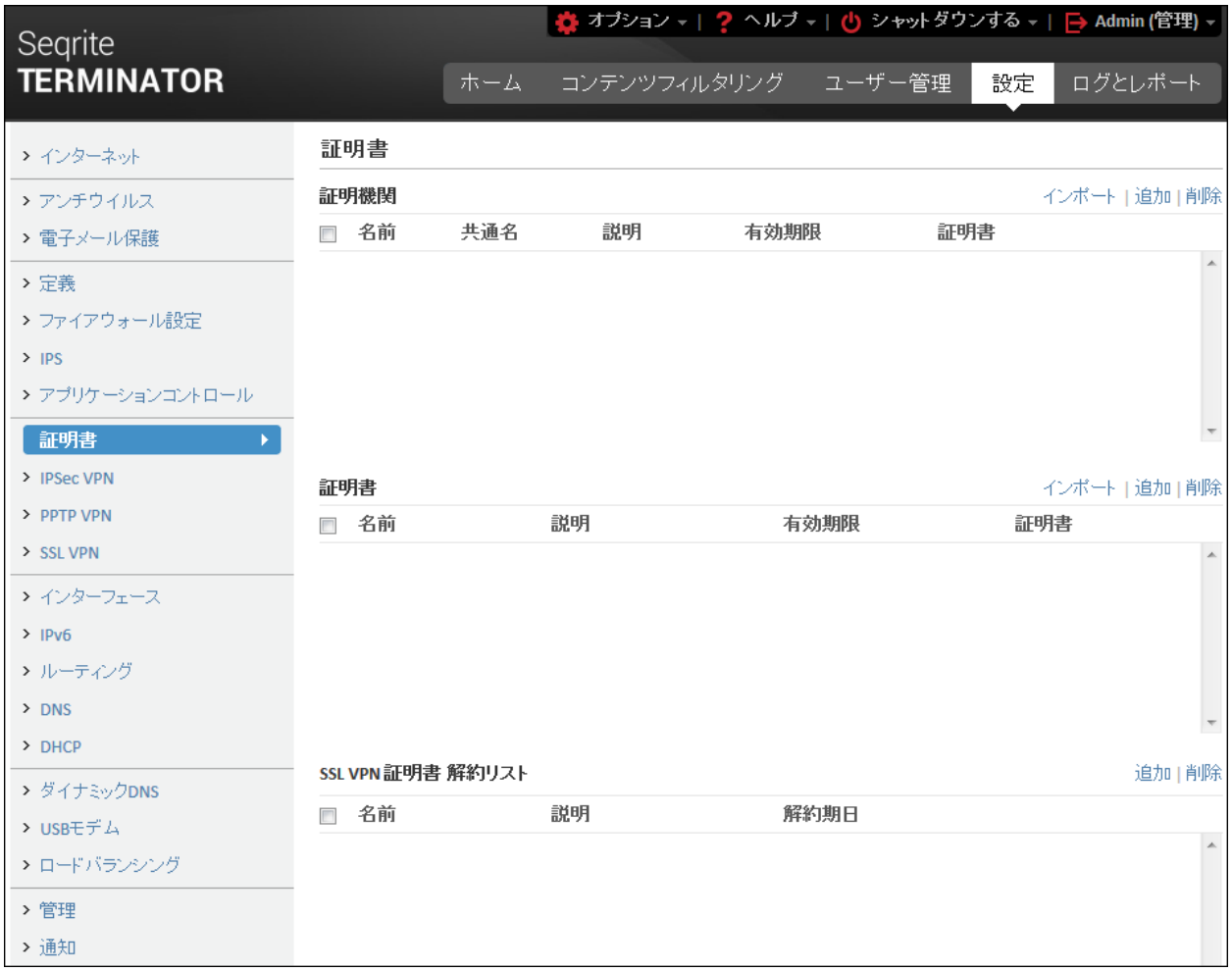
証明書は、セキュリティ目的で使用される電子メッセージに添付される文書です。証明書は一般的に、ユーザーが送信するメッセージの合法性を検証し、返信を暗号化する手

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]** へログオンします。次のページが表示されます。



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。

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。

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

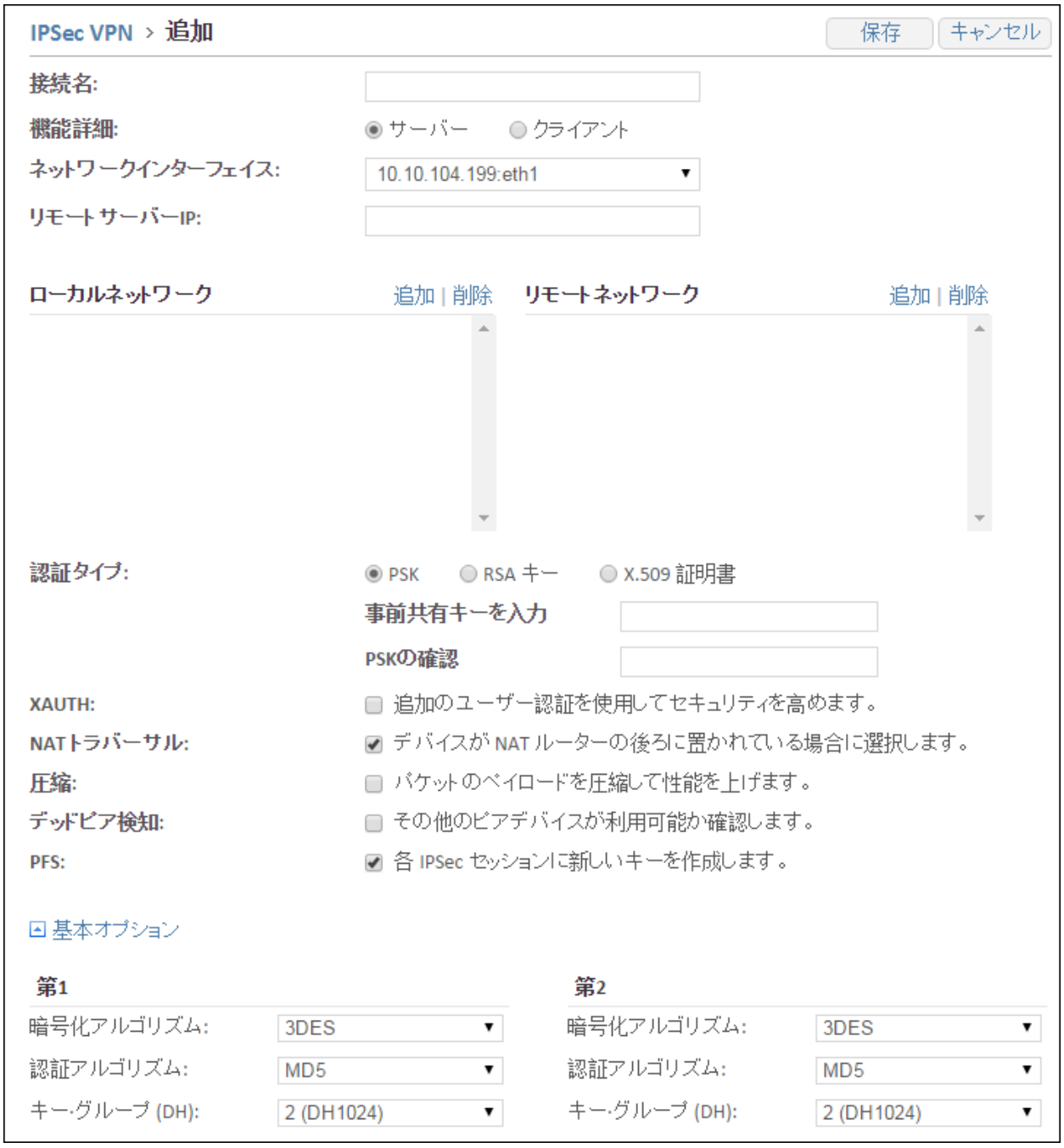
サイト間 IPSec VPN 接続を使用して、様々なブランチネットワークをリモートネットワークにアクセスさせることができます。

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]** へログオンします。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。

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。



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
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。

	• 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。 • 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トサーバーとして動作します。
インターフェース	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。 • **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。 • **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。 • **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すると、証明書を選択し、［リモートクライアント ID］欄に**リモートクライアントの証明書 ID** を入力しなければなりません。
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	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。
デッドピアの検出	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。 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]** へログオンします。次に示す画面が表示されます。

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]** へログオンします。
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。

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。
7. 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] へログオンします。次の画面が表示されます。

2. 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。

3. 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。 • 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	［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は、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]** へログオンします。サイト間の設定ページが表示されます。

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。
3. 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。

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:

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:

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]** へログオンします。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. ［**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。

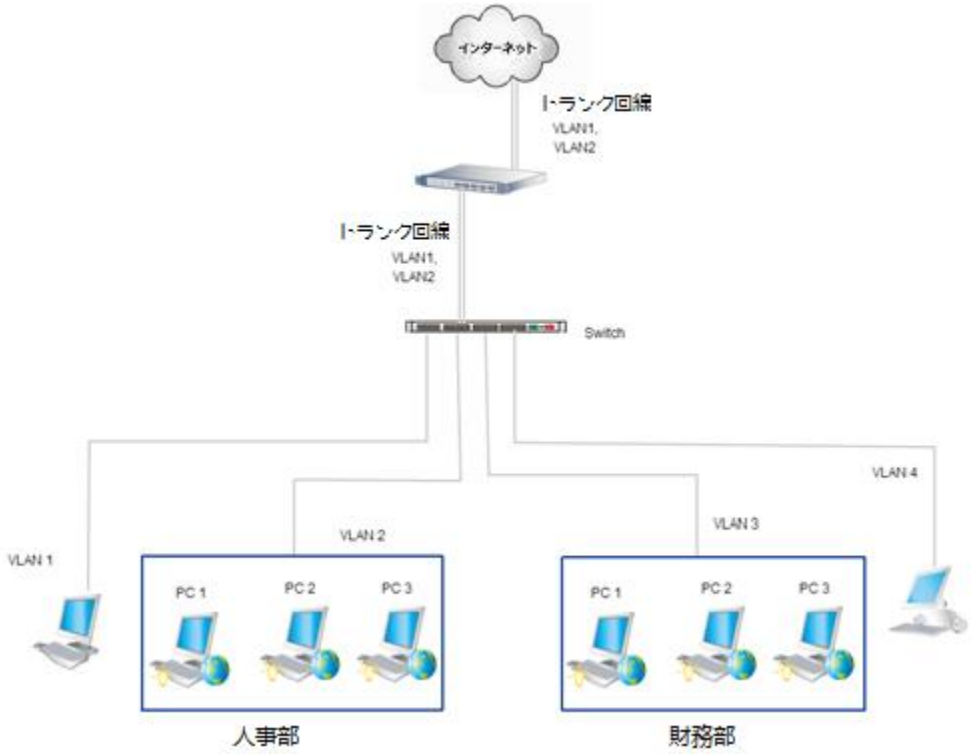
3. ［**接続名**］を入力します。
4. ［**ユーザー名**］および［**パスワード**］テキストボックスに、ユーザー名とパスワードを入力します。［**パスワードの再入力**］テキストボックスに、パスワードを再入力します。これらは認証に使用されます。
5. リストに表示されている**ローカルネットワーク**を選択します。
6. 必要なら、［**追加コマンド**］を追加します。
7. ［**保存**］をクリックします。

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] へログオンします。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。

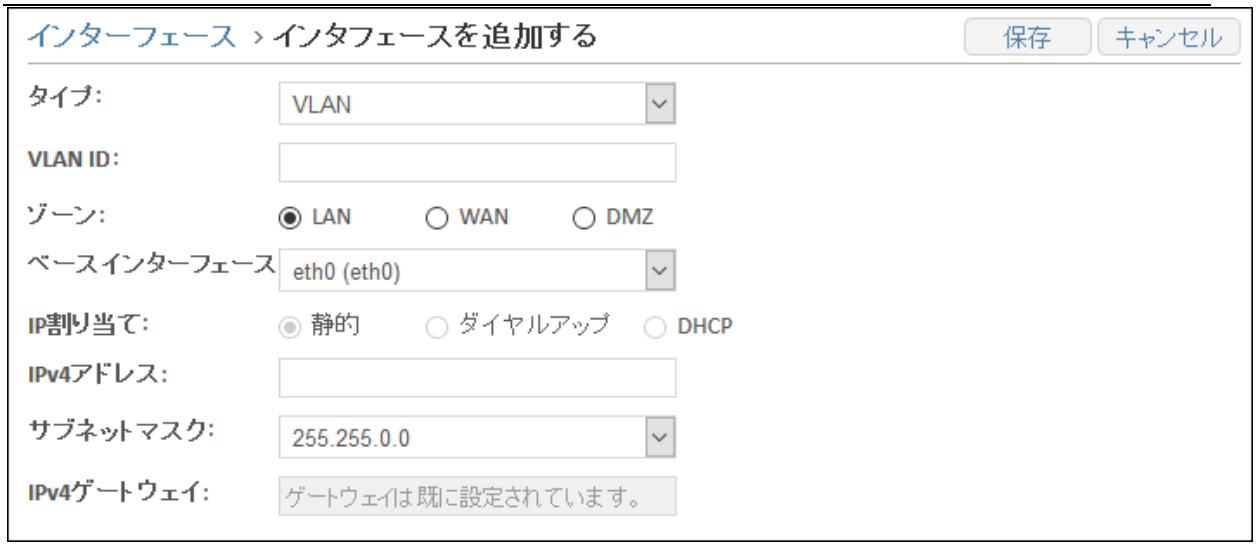
VLAN-WAN:外部ネットワーク（インターネット)/ISP 用。

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]** へログオンします。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 **[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。

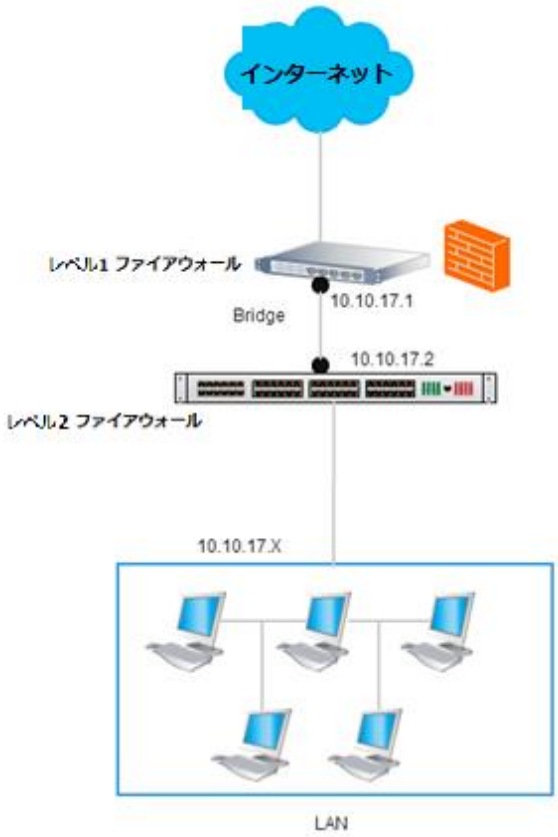
ii. IP 割り当てとして［ダイヤルアップ］を選択した場合、ISP から提供される［ユーザー名］と［パスワード］を入力する必要があります。

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。

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。

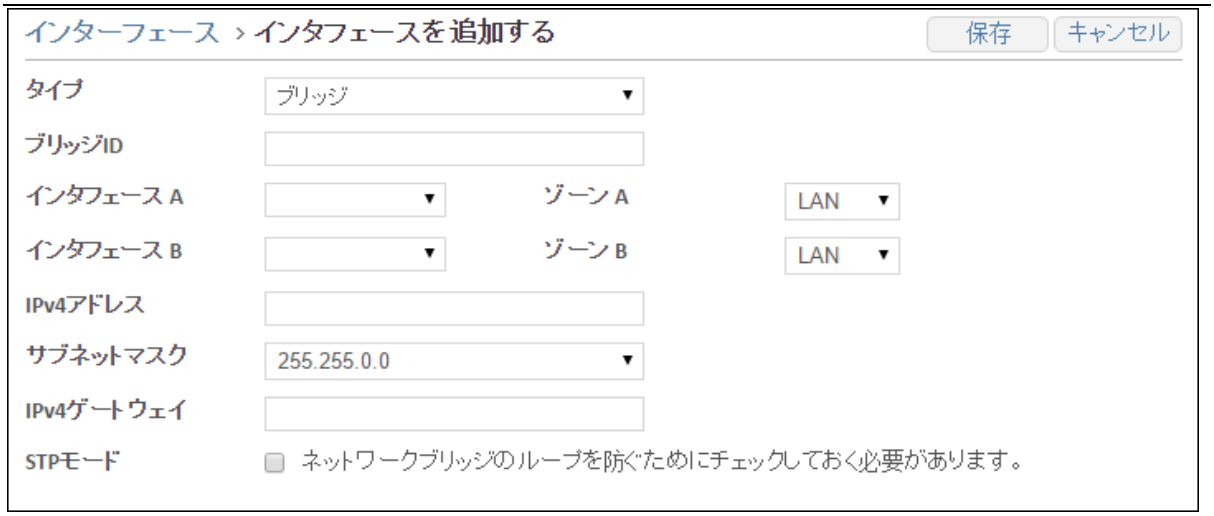


Seqrite Terminator ブリッジインターフェースは、次の用途に使用できます:

- **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]** へログオンします。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［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。

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]** へログインします。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。

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]** へログオンします。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 ヘッダ情報を含める	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。  オフラインにしたいサービスを選び、**[保存]** をクリックします。 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。（詳細はインターネットクォータ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。

Chapter

6

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。

[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へ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]** へログオンします。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。

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。
認証タイプ	認証手法として、ローカルまたは認証サーバー (Active Directory 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。
パスワード	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 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。
パスワードの確認	確認のため、パスワードを再入力します。
ステータス	[有効]:ユーザーは認証を受けることができ、Terminator へログイ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 へログインできず、インターネットへアクセスできません。
グループの選択	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。
インターネットクォータ	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ォ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。
同時ログイン	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 のバインディング	設定に従い、ユーザー名を特定の IP アドレス、MAC アドレス、または両方にバインドします。 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。
コンテンツフィルタリング	[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] に設定すると、ユーザーへ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]** へログオンします。
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。

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**] へログオンします。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。

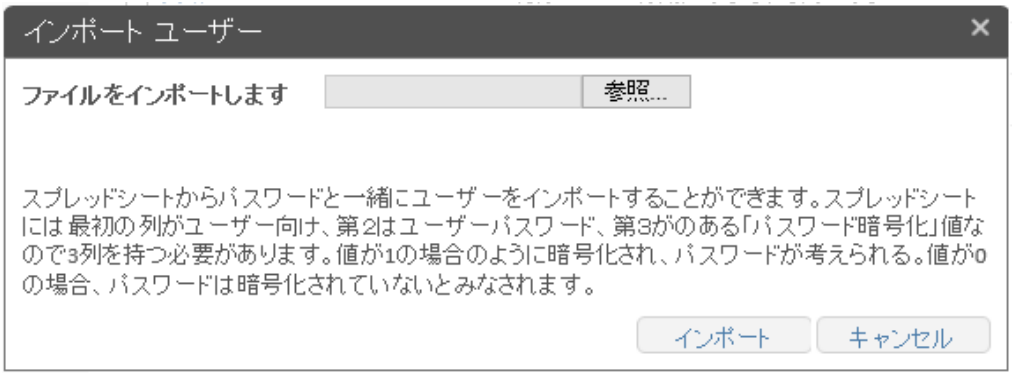
1. Seqrite [Terminator] > **[ユーザー管理]** > **[ユーザー]** へログオンします。ユーザー管理ページが表示されます。
2. このページには、ユーザーのリストが、ユーザー名、グループ名、認証、ステータス、IP/MAC バインドのステータス、コンテンツフィルタリングが有効かどうか、および作成済みの場合はメール ID とともに表示されます。
3. ユーザー名を選択して、**[ログアウト]** をクリックします。ユーザーはネットワークからログアウトされます。

   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]** へログオンします。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. **[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。



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。

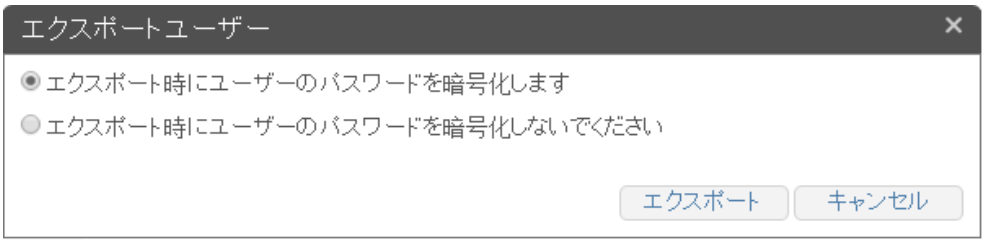
	A	B	C	D
1	User Name	Password	Password Encryption	
2	user1	YWRtaW5AMTIz	1	
3	user2	YWRtaW5AMTIz	1	
4	user3	YWRtaW5AMTIz	1	
5				
6				

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]** へログオンします。デフォルトでは、ユーザー管理ページが表示されます。
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. 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]** へログオンします。次の画面が表示されます。

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
ゲストユーザーを有効にする	このオプションを選択すると、Terminator でゲストユーザーの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。
失効後に自動削除	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。

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]** へログオンします。[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。

2. **[追加]** をクリックします。

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
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(詳細は時間カテゴリを参照してください。)
ユーザーを追加	**ユーザー単位**:[ユーザー単位] でのユーザー追加を選択すると、[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 を入力します。 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、**[削除]** オプションを使用します。
パスワードの変更	このオプションは、[ユーザー単位] オプションでのみ表示されます。このオプションは、そのグループのユーザーがパスワードの変更を許可されるかどうかを指定するために使用します。
インターネットアクセス	**無制限**:[無制限] を選択すると、ユーザーは制限なしにインターネットを参照できます。 **制限付きのアクセス**:[制限付きアクセス] を選択すると、ユーザーは設定されている制限に従ってのみ参照できます。この場合、次のサブオプションも設定する必要があります。 グループとユーザーの帯域幅 (KB/秒単位) **最大グループ帯域幅**:このグループのユーザーが利用可能な帯域幅 (合計) の上限です。この機能によってグループの帯域幅使用を制限できます。

フィールド	説明
	最大ユーザー帯域幅:このグループの各ユーザーが利用可能な最大の帯域幅です。このオプションは、グループのユーザーが利用可能な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、**参照時間**を無制限に設定、または指定した時間に制限できます。
インターネットクォータ	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ん。 **[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	**カテゴリによる**:このオプションを選択すると、ユーザーは許可されたカテゴリのウェブサイトのみを参照できます。次のサブオプションがあります。 **[許可されるカテゴリ]** からカテゴリを選択し、リスト間の矢印ボタンを使用して**[禁止されるカテゴリ]**のリストへ移動します。逆方向へも移動できます。 **[カテゴリで検索]** 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、URL 分類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、そのドメインを選択し、右上にある**[削除]**をクリックします。 注意:このオプションを選択すると、そのグループではリ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。
ホワイトリスト/ブラックリスト	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 [削除] 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] へログオンします。
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。次に示す画面が表示されます。

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] へログオンします。[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。

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:

1. Seqrite [Terminator] > **[ユーザー管理] > [グループ]** へログオンします。[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. Seqrite [Terminator] > **[ユーザー管理] > [時間カテゴリ]** へログインします。

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。

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]** へログオンします。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. **[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。

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

4. 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]** へログオンします。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。

5. 必要に応じて、次の操作のいずれかを行います:

   i. Terminator へ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 へインポートされます。

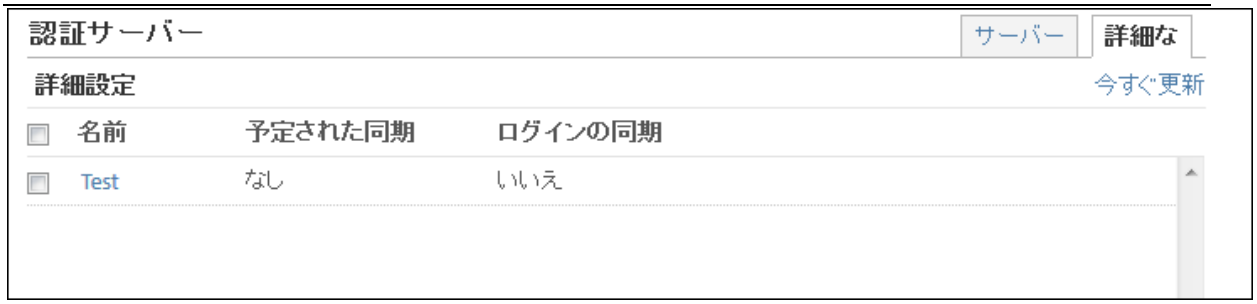
   ii. グループを削除するには、グループを選択して **[削除]** をクリックします。選択したグループが、Terminator から削除されます。

認証サーバーの削除

1. Seqrite [Terminator] > **[ユーザー管理]** > **[認証サーバー]** へログオンします。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。
3. 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]** へログオンします。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。

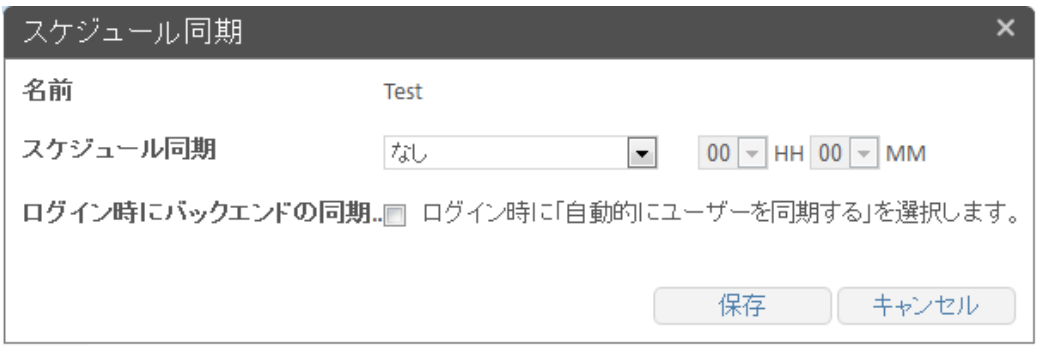


3. Terminator と同期するサーバーを選択し、**[今すぐアップデート]** をクリックします。Terminator のユーザーリストが、サーバーのユーザーリストと同期されます。

Seqrite 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]** へログオンします。
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。



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**］へログオンします。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。

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。

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。 **アップロード & ダウンロードクォータ**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。 以下のオプションが使用できます。 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。 毎月:月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、月の始めの日と月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。**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、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。

- アンチウイルス: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。
- URL フィルタリング: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。
- MIME フィルタリング: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。
- アプリケーションコントロール: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。
- 侵入防止システム: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]** へログオンします。

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。
4. **[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、インターネットの設定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] へログオンします。次のページが表示されます。

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。
4. 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。

5. 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。

6. 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。

7. 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]** へログオンします。次のページが表示されます。

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。
4. 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

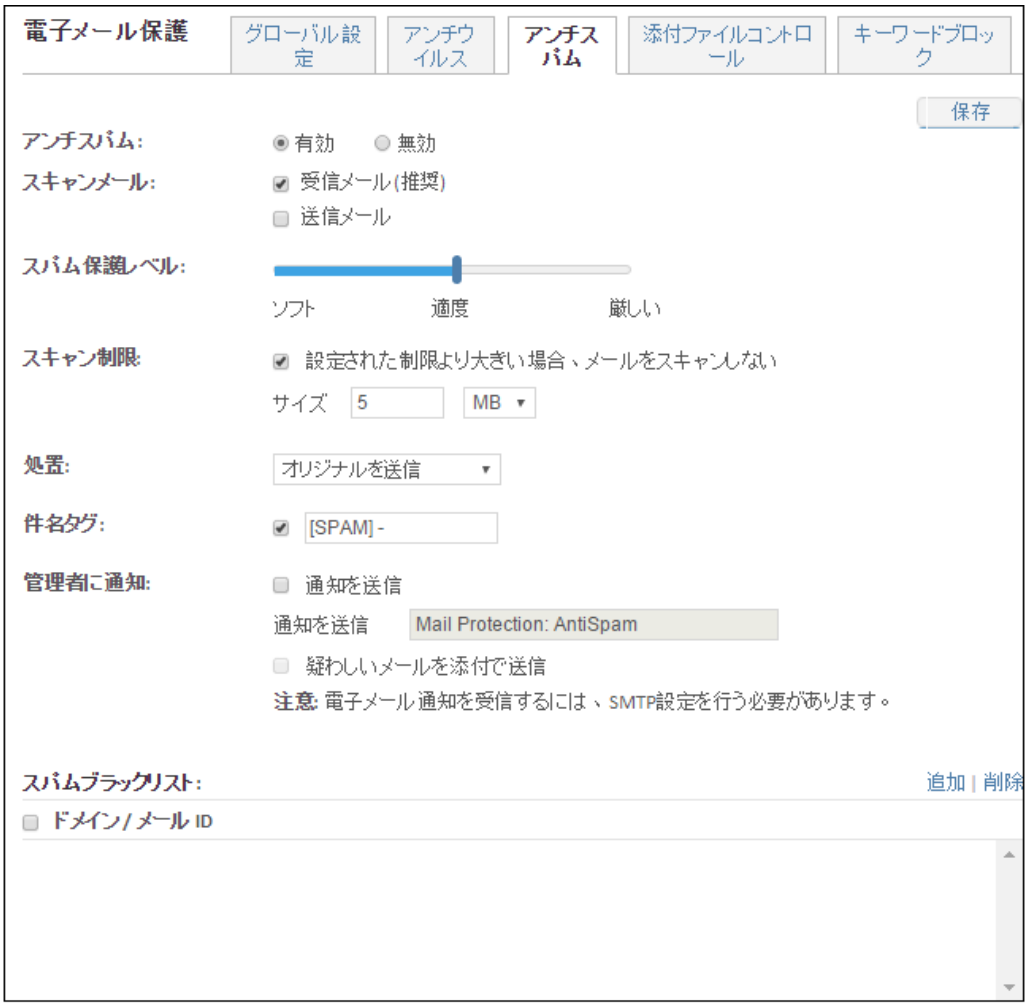
メールのスパムは、一方的に送り付けられる大量のメール（UBE)、ジャンクメール、または一方的に送り付けられる商用メール （UCE） とも呼ばれ、要求されていないメールメッセージを、多くの場合には商業的な内容で、多くの受信者へ無差別に、大量に送り付ける方法です。アンチスパムは、各種の技法を使用して、メールのスパムや、一方的に送り付けられる大量のメールがメールシステムへ入り込むことを防止します。

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**］へログオンします。次に示す画面が表示されます。



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。
9. 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。

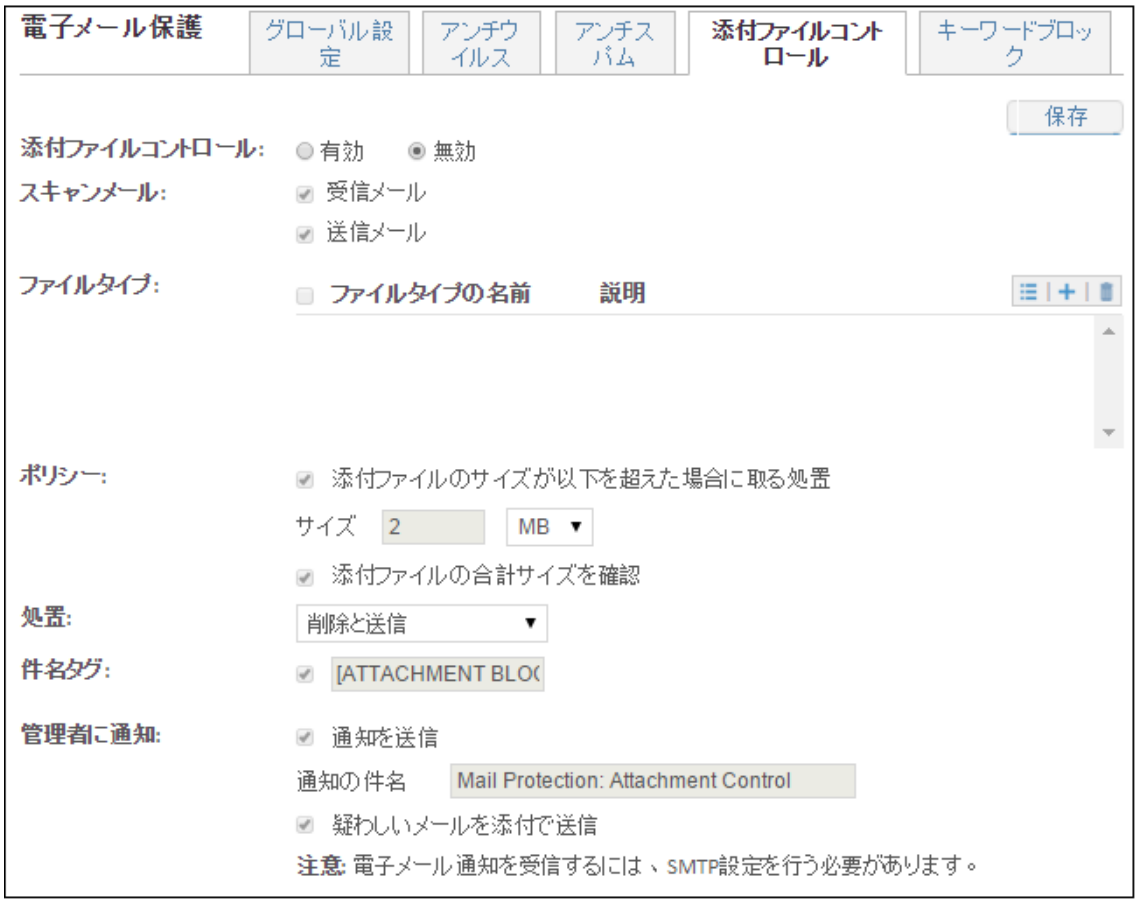
   スパムのブラックリストにメール ID を入力するには、スパムのブラックリストセクションで **[追加]** をクリックします。指定のテキストボックスにメール ID を入力し、**[保存]** をクリックします。
10. [アンチスパム] ページの設定を保存するには、ページの右側で **[保存]** をクリックします。

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。

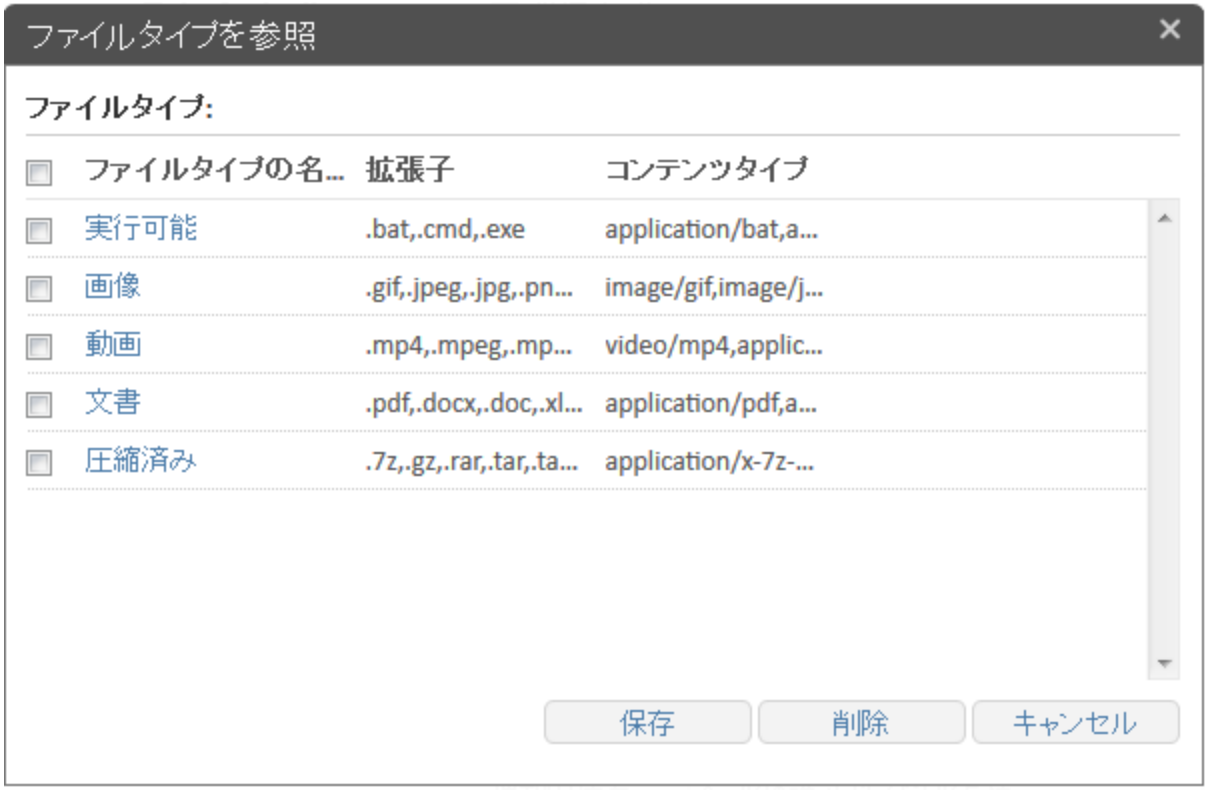
1. [Seqrite Terminator]> **[設定]** > **[メール保護]** > **[添付ファイル管理]** へログオンします。次に示す画面が表示されます。



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。
4. 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スキャンされます。メールに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。



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]** へログインします。[キーワードのブロック] ページが表示されます。

2. **[キーワードブロック]** を有効に設定します。
3. 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。

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	**次で始まる**: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。 **完全一致**: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。
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]** へログオンします。[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。

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。
4. 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]** へログオンします。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。

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**］へログオンします。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。
2. 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**］へログオンします。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。

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]** へログオンします。[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**］へログオンします。［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。

2. ［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］ へ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**］へログオンします。［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。

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**］へログオンします。［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] へログオンします。[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。

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
ルックアップタイプ	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を選択します。
キーワード一致オプション	**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。 **次を含む**: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、アンチウィルス.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]** へログオンします。[アプリケーションコントロール] 画面が表示されます。

2. 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] へログオンします。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。

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］**へログオンします。［カスタム IPS］画面が表示されます。

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。

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]** へログオンします。[カスタム IPS] 画面が表示されます。
2. 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。

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]** へログオンします。[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]** へログオンします。[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。

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]** へログオンします。[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。

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

8

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。

- 日時: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。
- 管理者設定: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。
- 管理者プロファイル: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］** へログオンします。

   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。

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、タイムゾーンを選択します。
日時の設定	• 手動:ドロップダウンから日時を選択します。  • 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。
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 サーバーとアプライアンスのクロックとを同期します。最も時差の少ない NTP サーバーと日時が同期されます。

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]** へログオンします。[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。

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 へ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]** へログオンします。[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。

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 へログインします。
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、管理者プロファイル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。

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 へログオンします。[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。

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 へログオンします。
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。

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 へログオンします。
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]** へログオンします。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。

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。*空白は使用できません。英数字のみを使用できます。*
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。*

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 へログオンします。

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
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]** へログオンします。

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**］へログオンします。

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。

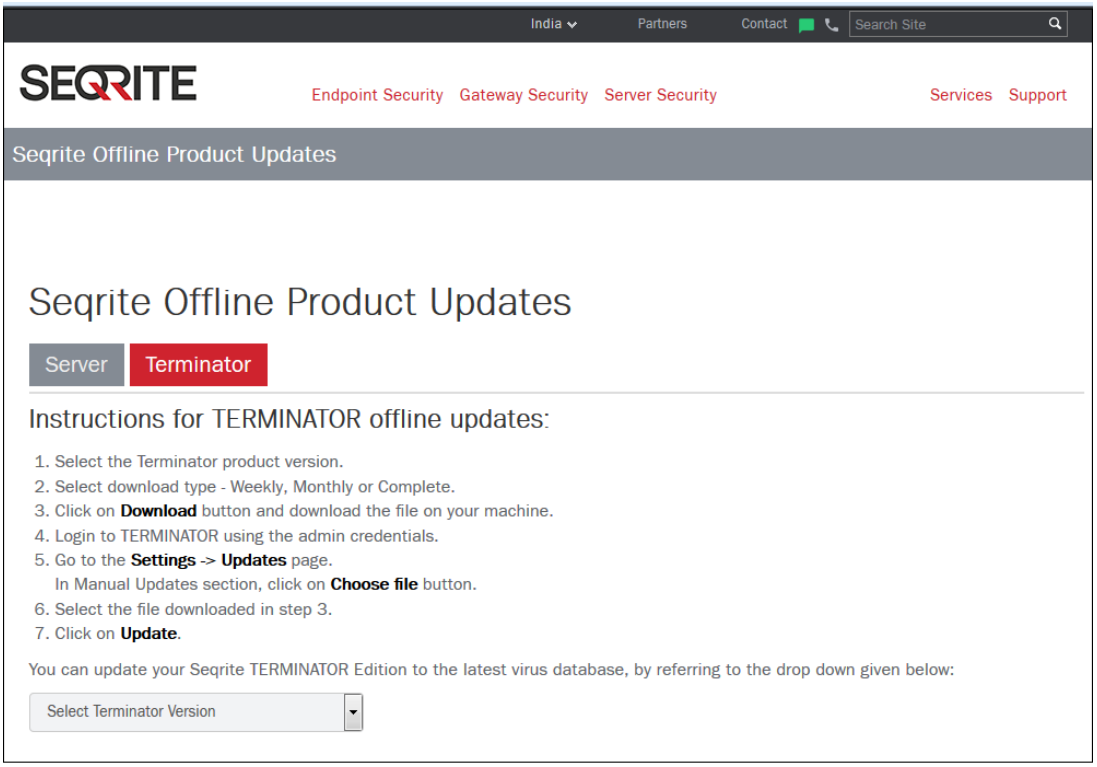
手動アップデートの設定

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:

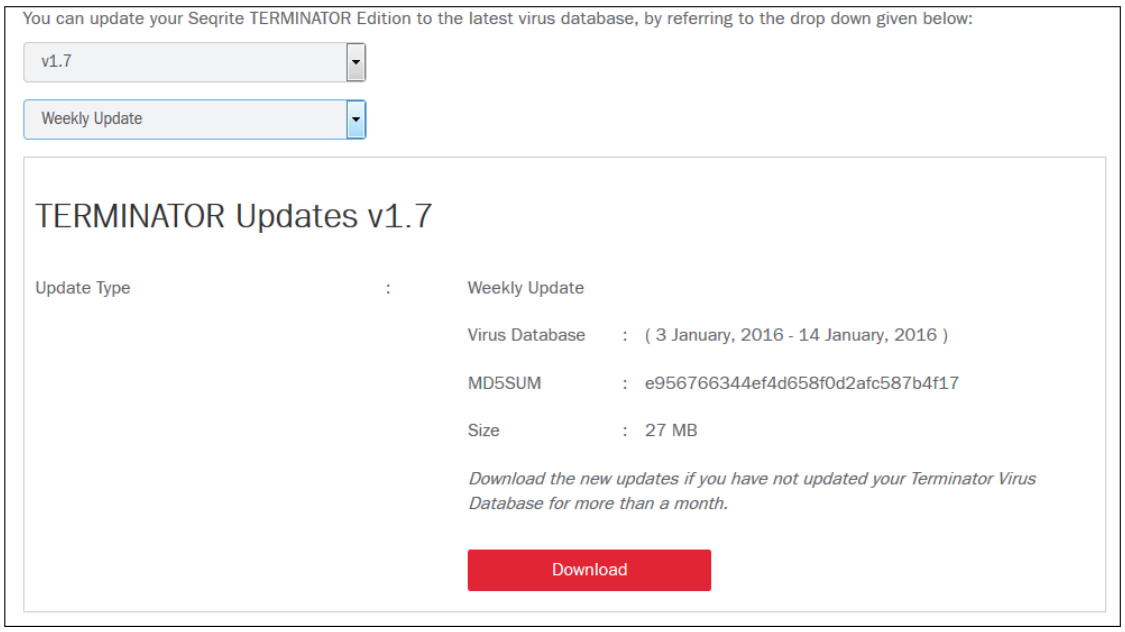
1. Seqrite Terminator > **設定** > **アップデート**にログオンします。

2. 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。



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。
6. 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。



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。
8. 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］** へログオンします。［バックアップ設定］ページが表示されます。

2. 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**］へログオンします。［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。

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。

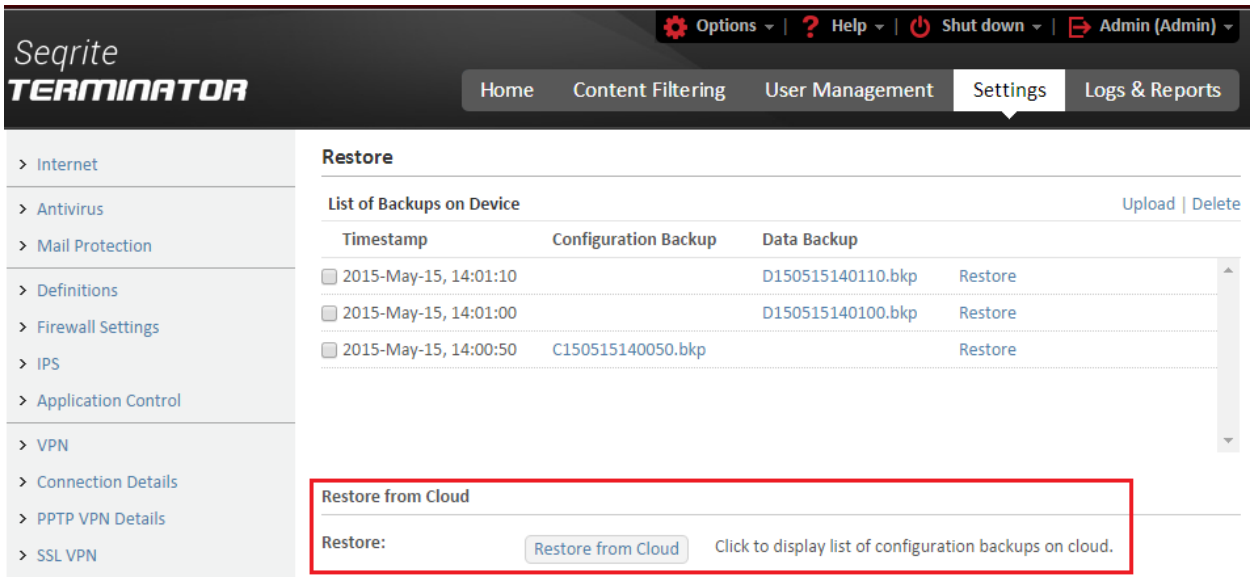
バックアップの復元

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]** へログオンします。[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。

2. 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。



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。

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]** へログオンします。
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]** へログオンします。[出荷時設定へのリセット] 画面が表示されます。

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］** へログインします。
2. ［ライセンス情報］ページが表示されます。

［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。

6. 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。

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**］へログインします。［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。

3. 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

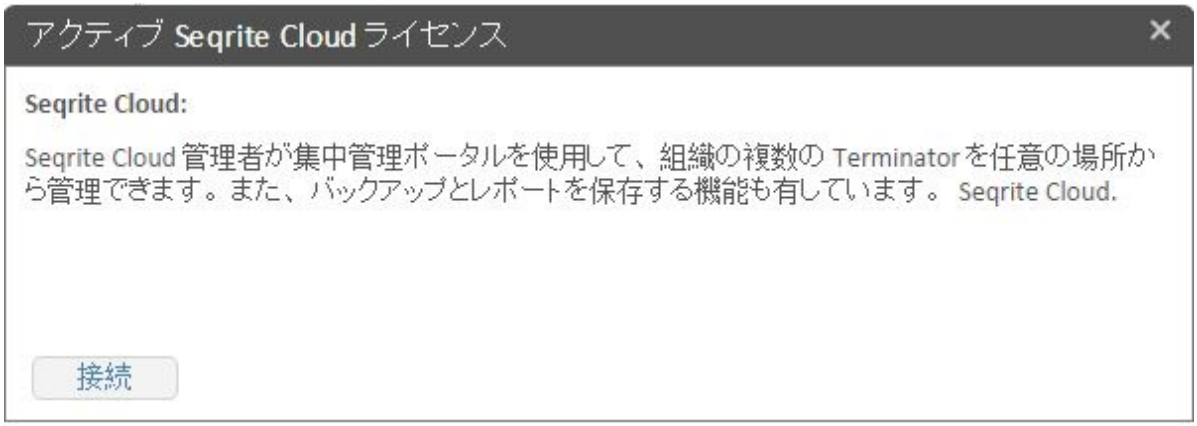
Seqrite Cloud は異なる場所に展開された複数の Terminator の管理・制御をサポートする統合ソリューションです。簡単なクラウド接続により、最新のセキュリティステータスの確認、製品ポリシーの設定、通知の受け取り、重要なネットワークイベントの修正などを単一のダッシュボードから行えます。さらに、Terminator のポリシー設定とバックアップをクラウド上で容易に行えるようになります。

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**］へログオンします。［ライセンス情報］画面が表示されます。

2. 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。



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。

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
- ウェブサイトアクセス
- メール保護
- ウェブ保護
- 侵入防止
- ポリシー違反活動
- 帯域幅使用量
- ファイアウォールレポート
- アップデート
- ログビューア

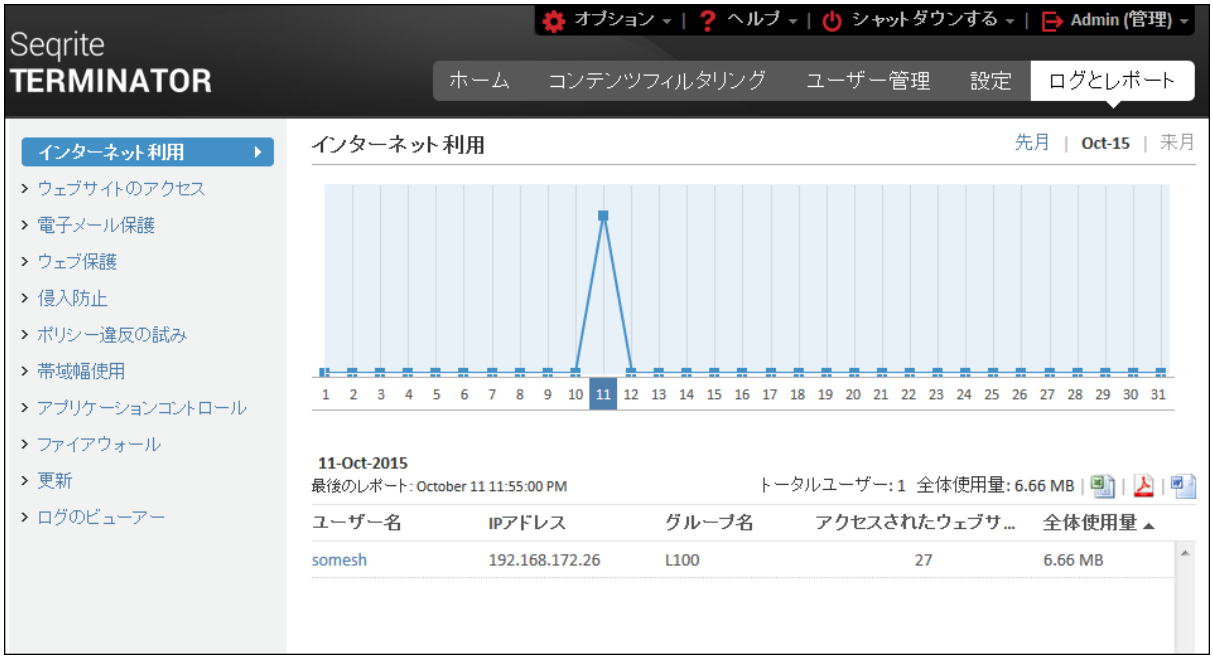
インターネット使用量

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

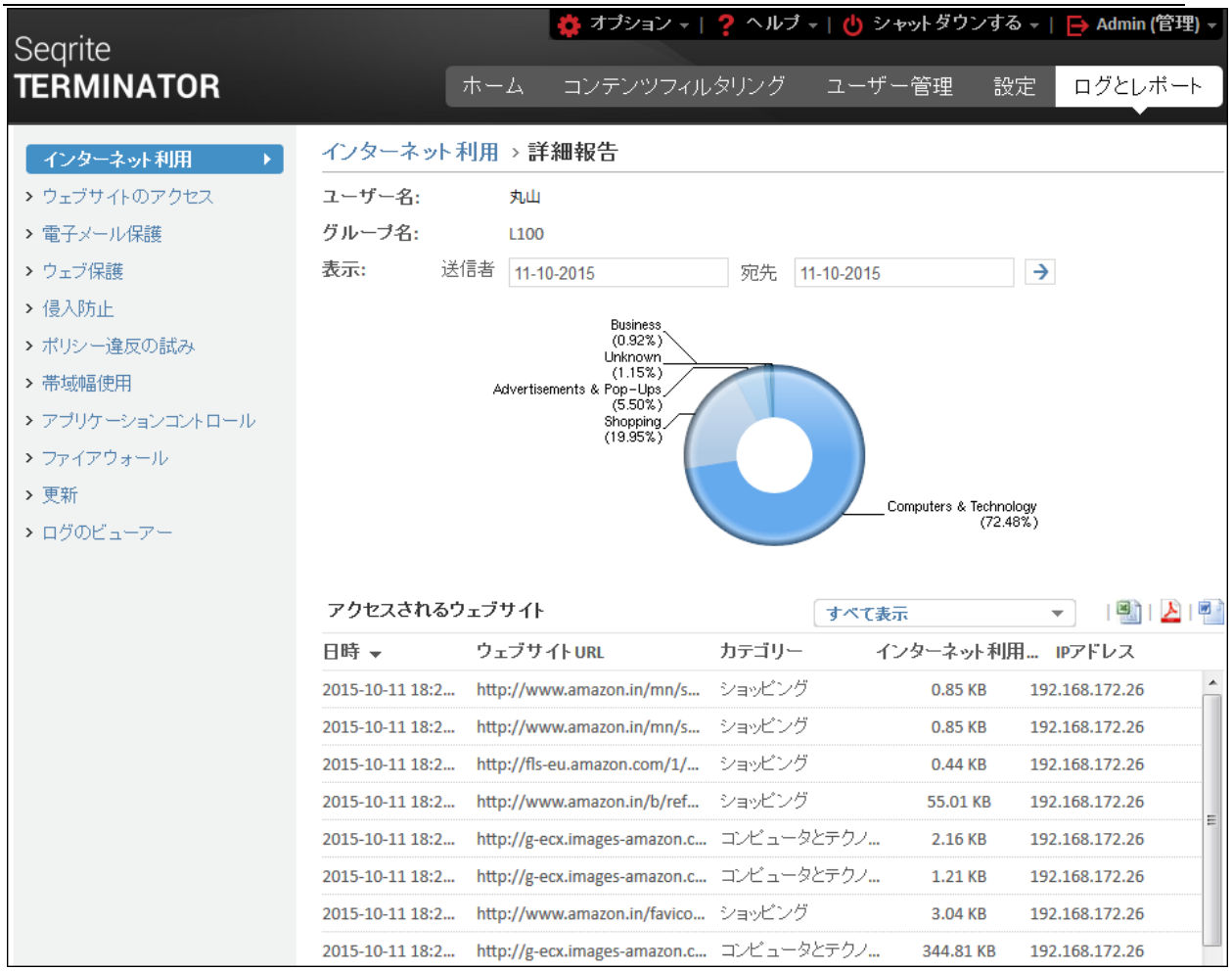
減らすために役立ちます。このレポートは、MS Excel、PDF、MS Word フォーマットでエクスポートできます。

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]** へログオンします。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。

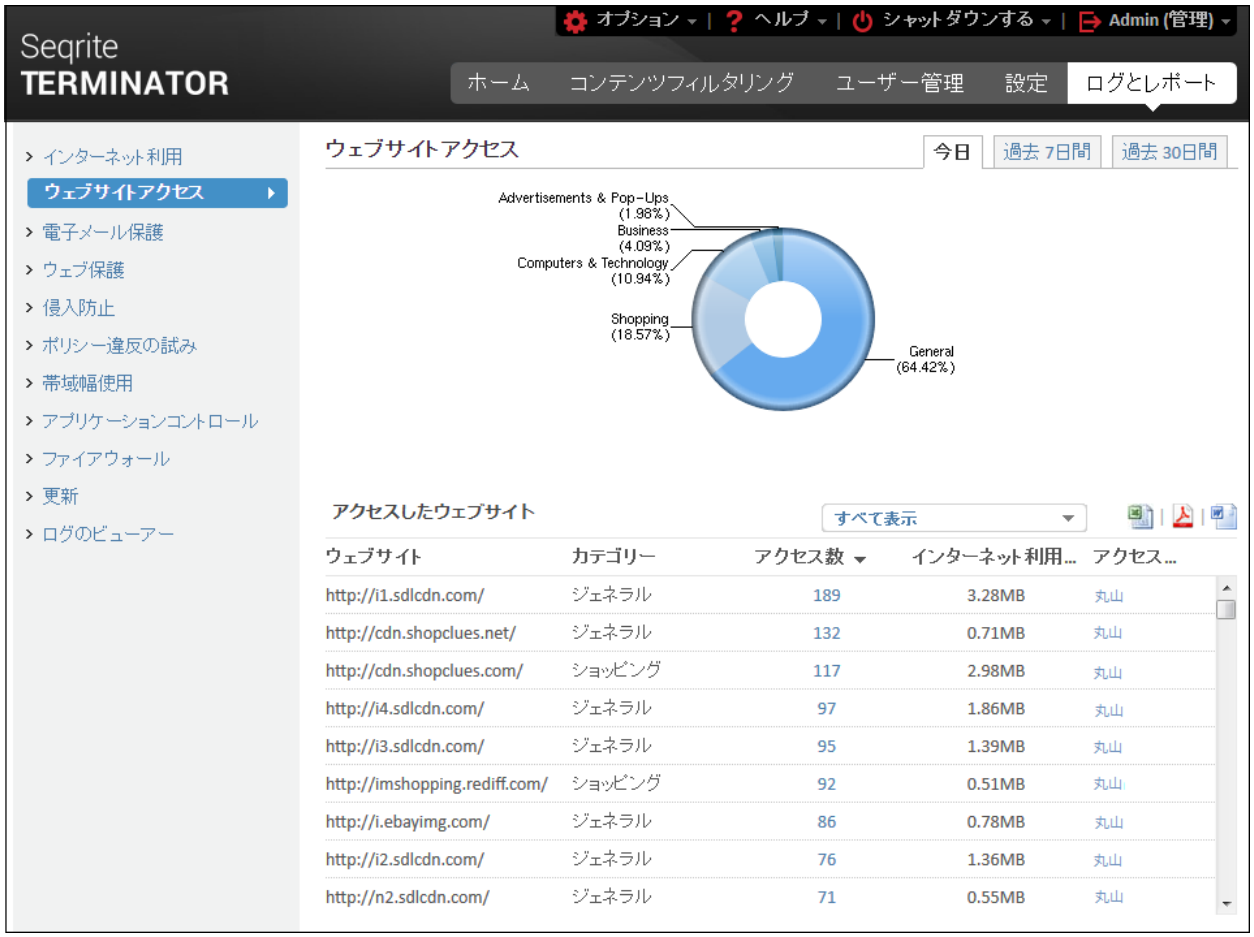


ウェブサイトアクセスレポート

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。

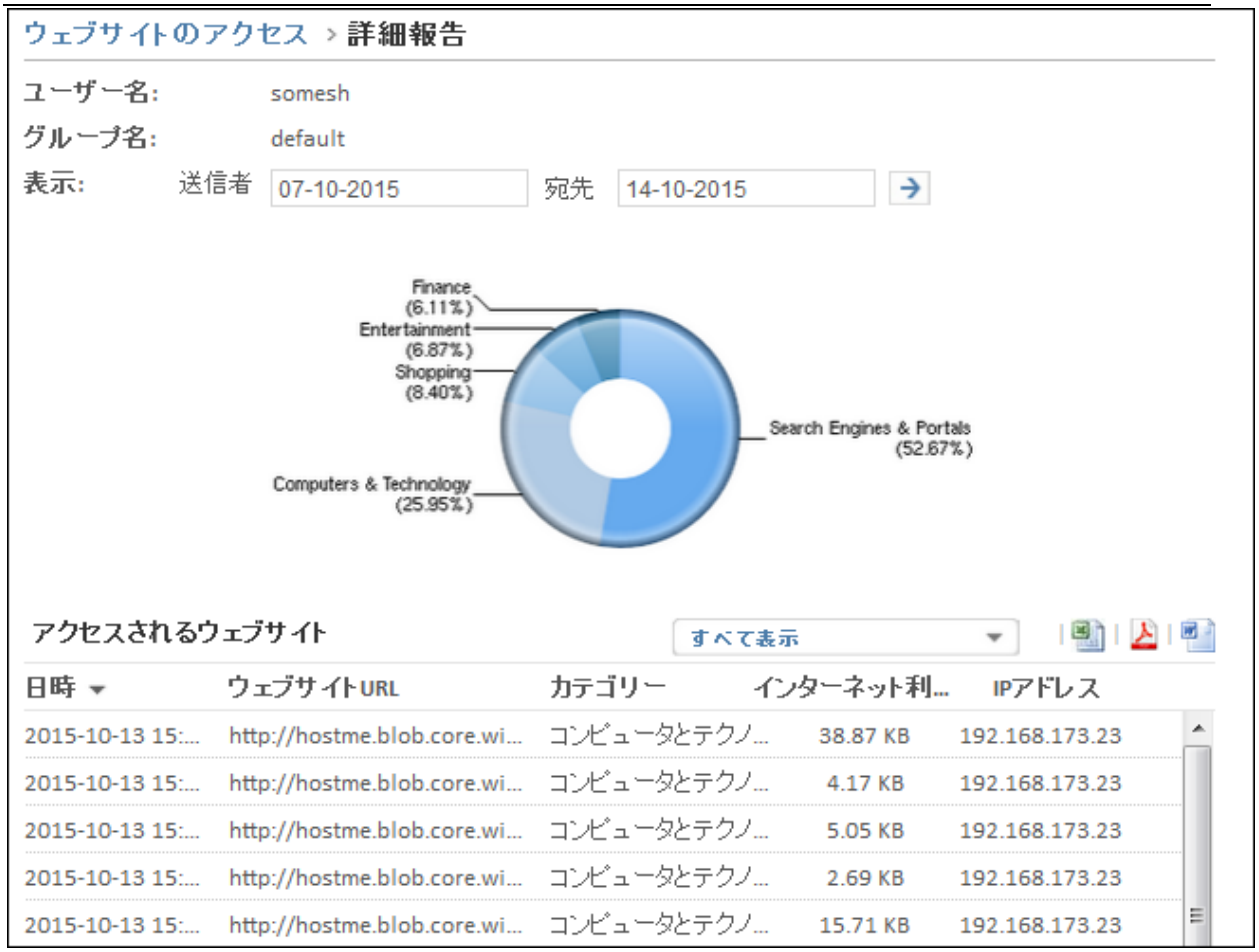
ウェブサイトアクセスレポートを表示するには、以下の手順に従います。

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



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。

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。

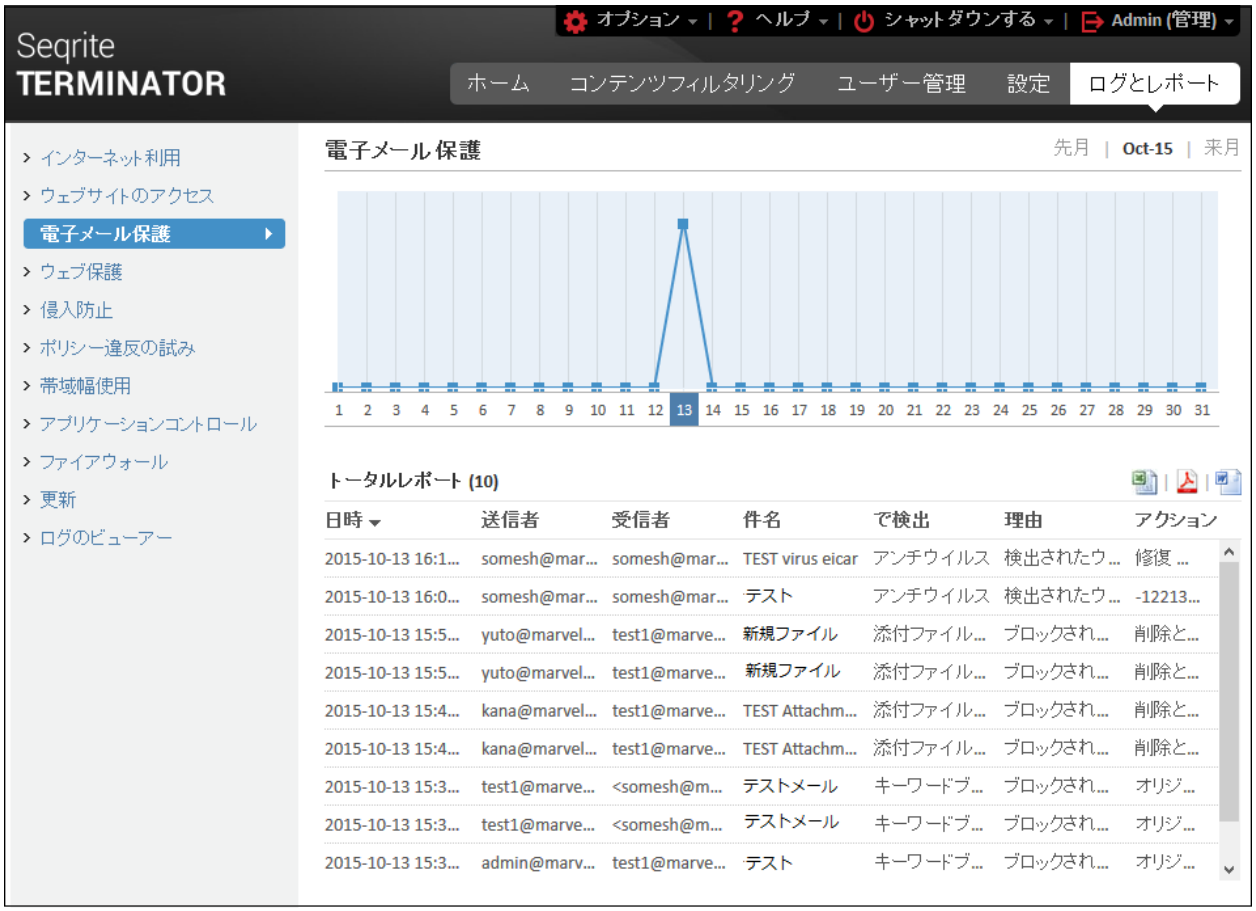

ウェブサイトのアクセス › 詳細報告
ユーザー名: somesh
グループ名: default
表示: 送信者 07-10-2015 宛先 14-10-2015
Finance (6.11%)
Entertainment (6.87%)
Shopping (8.40%)
Computers & Technology (25.95%)
Search Engines & Portals (52.67%)
アクセスされるウェブサイト
すべて表示
日時 ウェブサイトURL カテゴリー インターネット利... IPアドレス
2015-10-13 15:... http://hostme.blob.core.wi... コンピュータとテクノ... 38.87 KB 192.168.173.23
2015-10-13 15:... http://hostme.blob.core.wi... コンピュータとテクノ... 4.17 KB 192.168.173.23
2015-10-13 15:... http://hostme.blob.core.wi... コンピュータとテクノ... 5.05 KB 192.168.173.23
2015-10-13 15:... http://hostme.blob.core.wi... コンピュータとテクノ... 2.69 KB 192.168.173.23
2015-10-13 15:... http://hostme.blob.core.wi... コンピュータとテクノ... 15.71 KB 192.168.173.23

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]** へログオンします。次のページが表示されます。

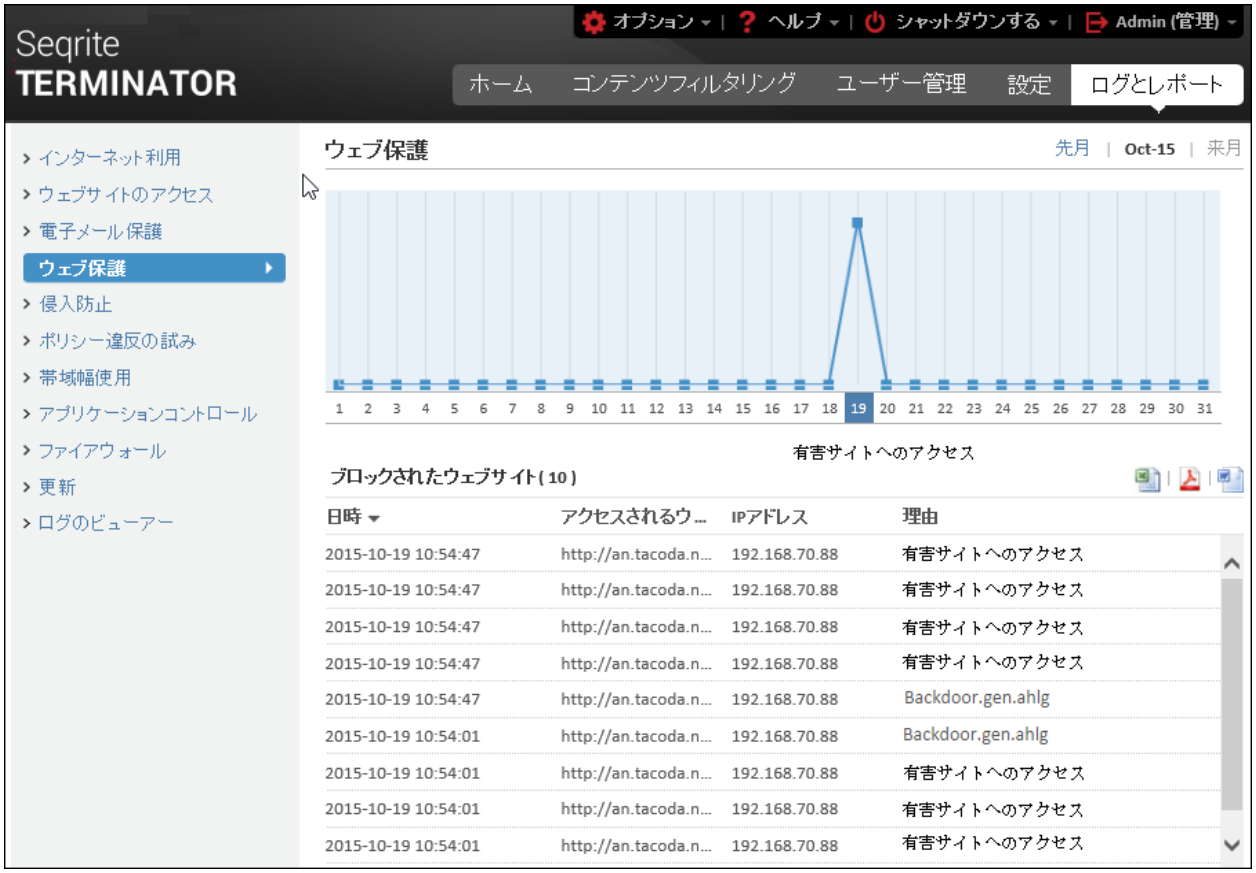


ウェブ保護

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]** へログオンします。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。

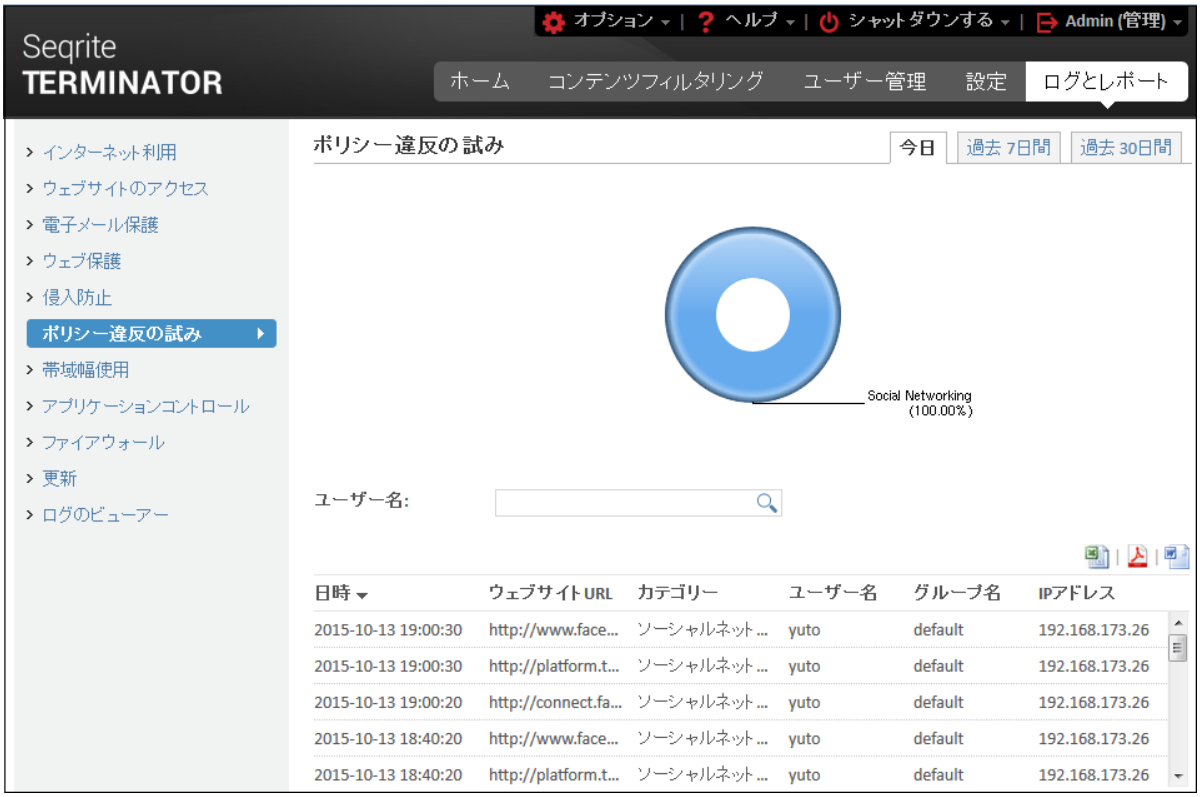
1. Seqrite [Terminator] > **[ログとレポート]** > **[侵入防止]** へログオンします。次のページが表示されます。

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]** へログオンします。次のページが表示されます。



帯域幅使用量

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。

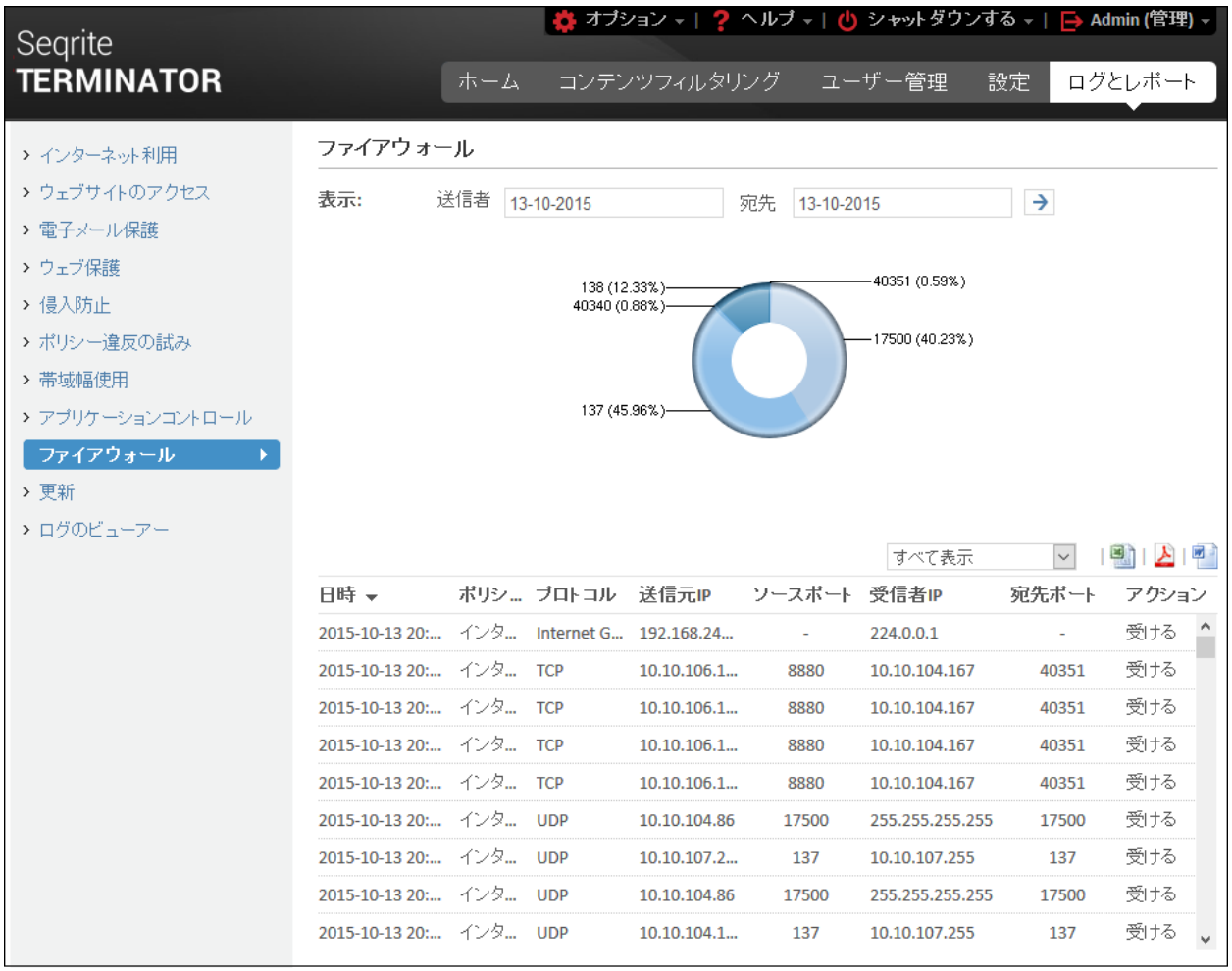
1. Seqrite [Terminator] > **[ログとレポート] > [帯域幅使用量]** へログオンします。次のページが表示されます。

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。



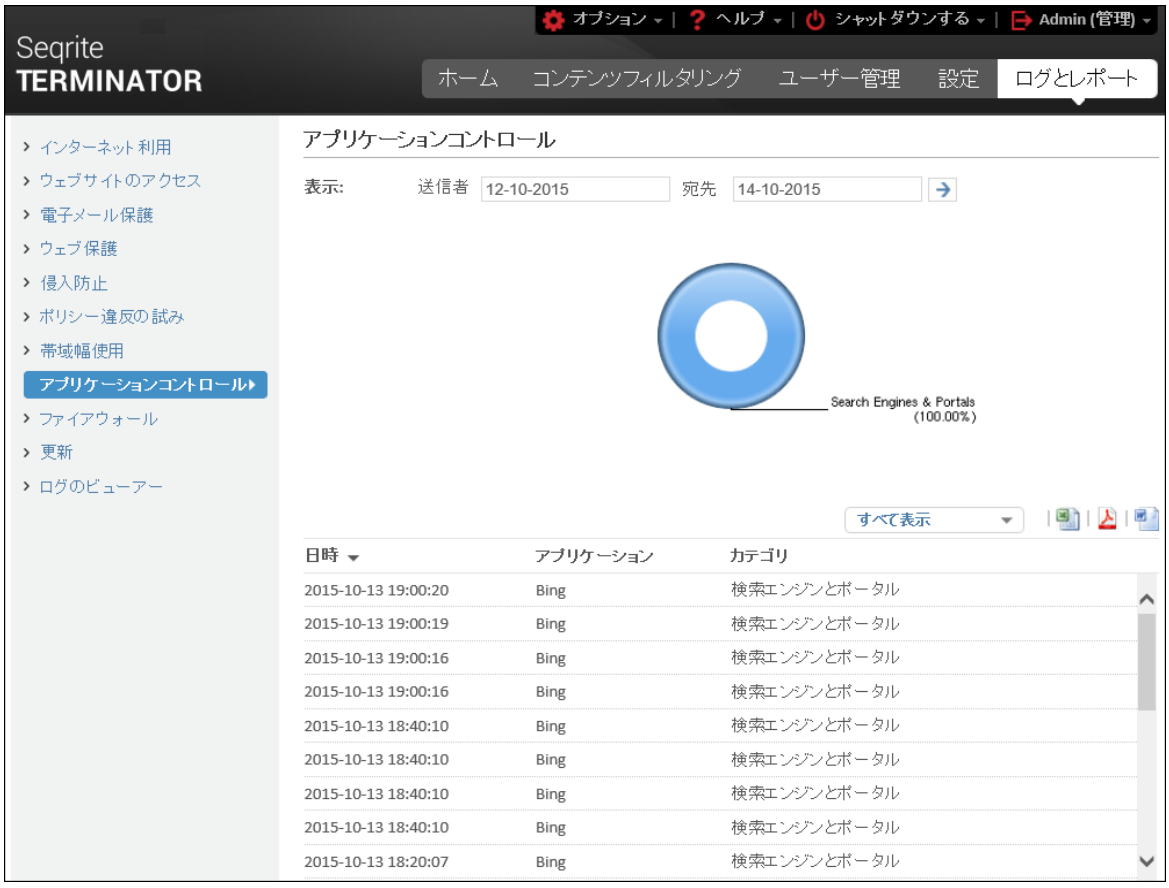
ファイアウォールレポート

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]** へログオンします。次のページが表示されます。



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]** へログオンします。次のページが表示されます。

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]** へログオンします。

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

	日付	管理者名	メッセージ
情報	20/11/2015 04:11:46 PM	admin	からログイン
情報	20/11/2015 04:10:44 PM	admin	からログイン
情報	20/11/2015 04:05:15 PM	admin	からログイン
情報	20/11/2015 03:50:33 PM	admin	からログイン
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
情報	20/11/2015 03:43:07 PM	admin	ログアウト
情報	20/11/2015 03:20:12 PM	admin	管理者「すずき」が正常に編集されました。
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。
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。

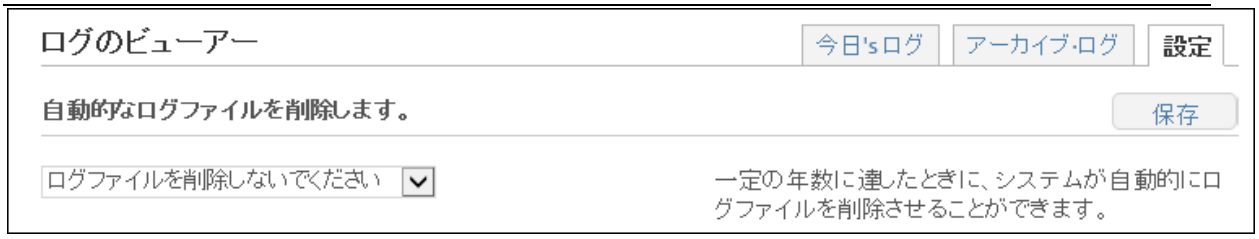
1. ［Terminator］ > **［ログとレポート］** > **［ログビューア］** > **［アーカイブログ］** へログオンします。次に示すように、［アーカイブログ］ ページが表示されます。

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]** へログオンします。次のページが表示されます。



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。

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。

Chapter

10

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
- SMS 通知

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]** へログオンします。メール通知の設定ページが表示されます。

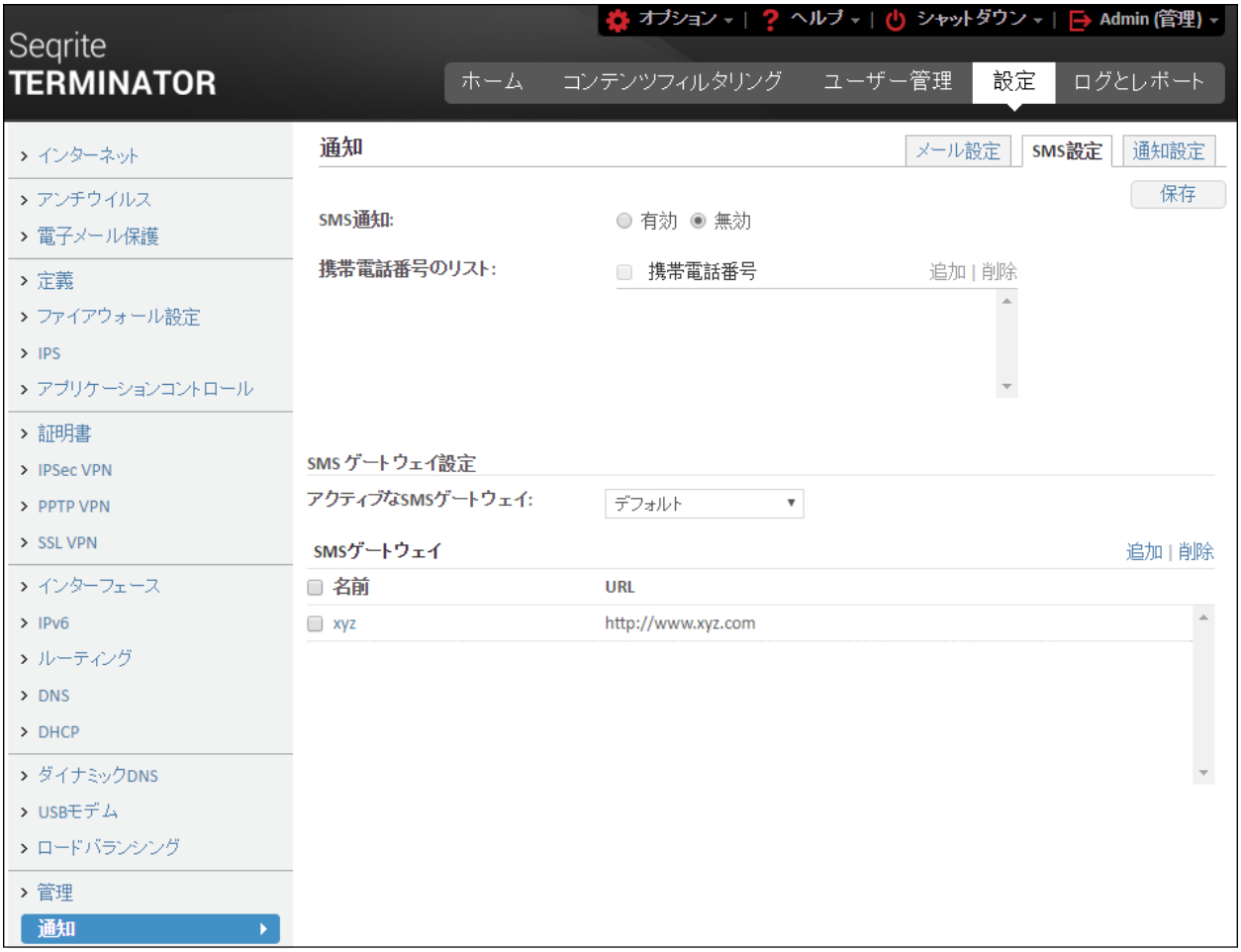
2. メール通知を有効にするには、[**有効**] を選択します。
3. [**メールアドレスから通知**] に入力します。メール通知は、このメールアドレスから送信されます。
4. [**メールアドレスに通知**] に入力します。これは、メール通知の送信先となるメールアドレスのリストです。必要に応じて、[追加] または [削除] を使用してリストを編集します。
5. [**デバイス特定テキスト**] に入力します。これは、通知の送信元であるデバイスの簡単な説明です。
6. [**テストメールを送信**] をクリックします。設定されたメールアドレスへテストメールが送信されます。

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。



2. SMS 通知を有効にするには、[**有効にする**] を選択します。
3. 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。

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

__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。
2. 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。

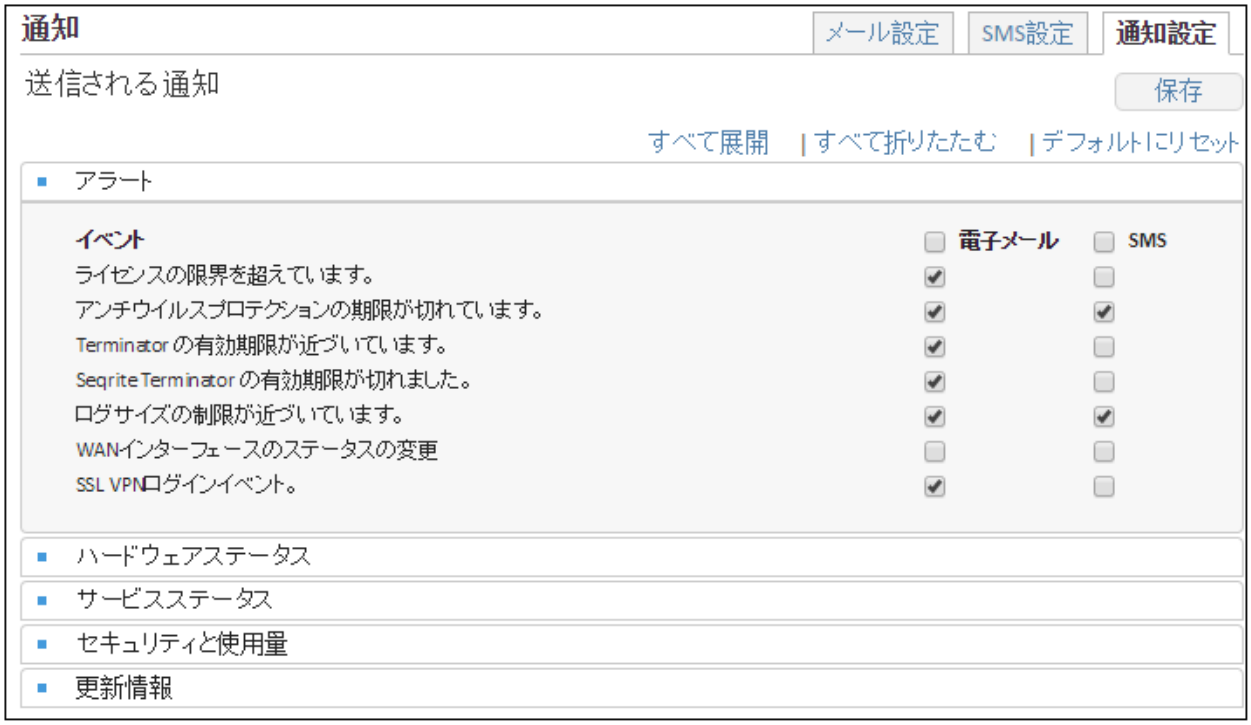
   SMS ゲートウェイ編集ページが表示されます。
3. 必要な変更を加え、[**保存する**] をクリックします。

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] へログオンします。通知設定ページが表示されます。



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。

Chapter

11

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 へアクセスするには、2 つの方法があります。

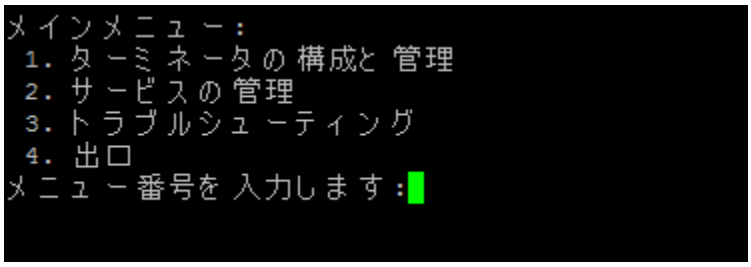
直接コンソール接続:Seqrite Terminator に直接キーボードとモニターを接続します。

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、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ェースへアクセスする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。

各メニューの説明を、次の表に示します。

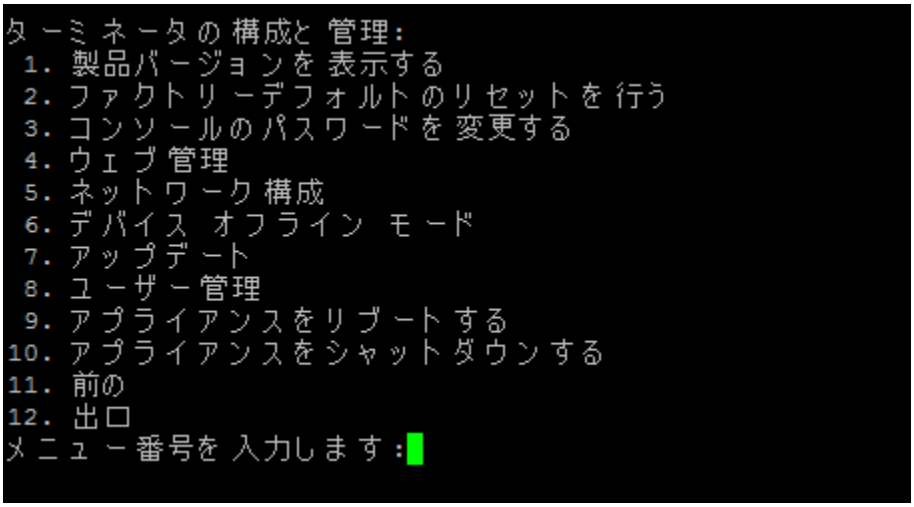
メニュー	説明
Terminator の設定と管理	Terminator で利用可能な各種サービスの設定と管理を行います。
サービスの管理	Terminator の各種サービスを管理します。
トラブルシューティング	各種のサービスのトラブルシューティングを行います。
終了	CLI コンソールを終了します。

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]** へログインします。



各メニューの説明を、次の表に示します。

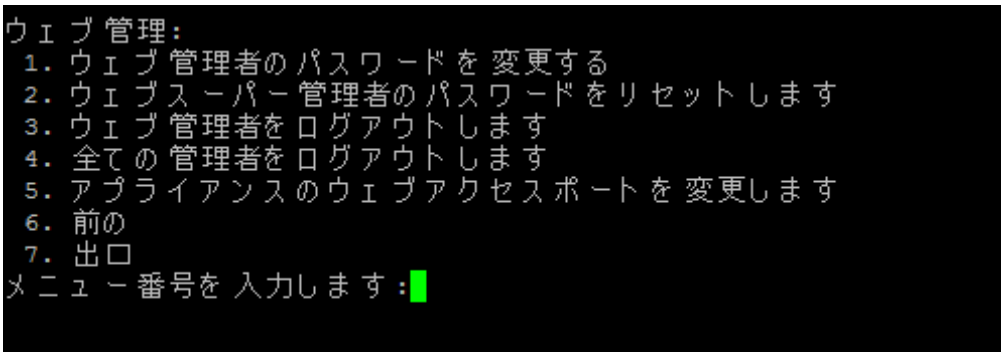
メニュー	説明
製品バージョンを表示	このオプションを使用して、Seqrite Terminator の製品バージョンを表示します。

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。

1. ［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］** へログインします。



［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。

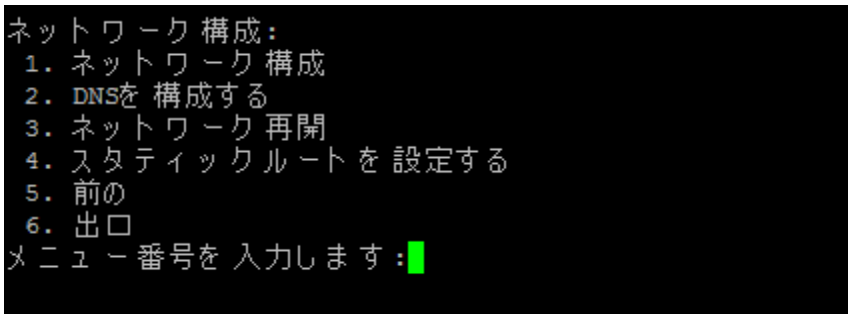
メニュー	説明

ウェブ管理者パスワードの変更	このオプションを使用して、Terminator のウェブ管理者パス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アウト	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ウトさせます。
すべての管理者をログアウト	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]** へログインします。



［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。

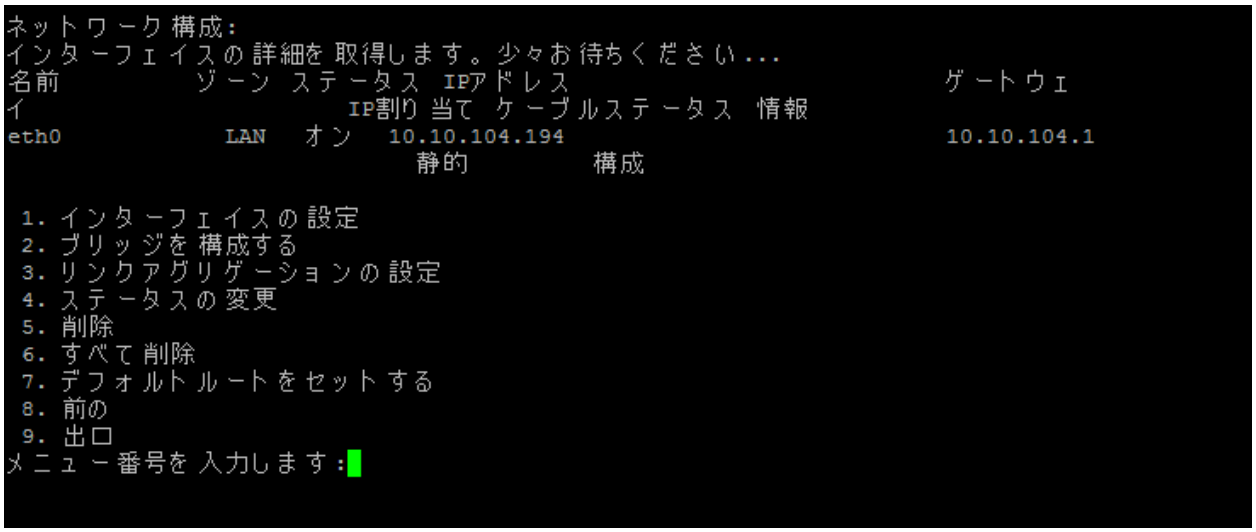
メニュー	説明
ネットワークを設定	このオプションを使用して、Seqrite Terminator ネットワークを設定します。LAN および WAN インターフェースを設定できます。
DNS の設定	このオプションを使用して、DNS を設定します。

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。
スタティックルートの設定	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］**へログインします。



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。

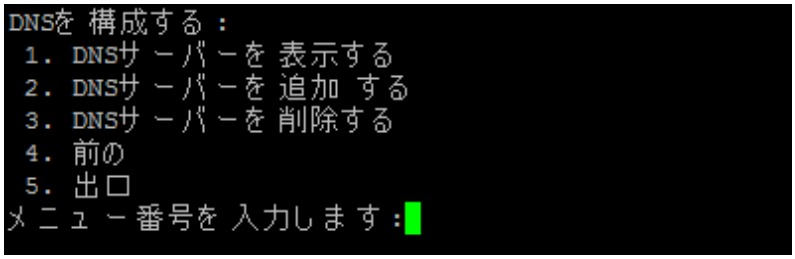
メニュー	説明
インターフェースを設定	このオプションを使用して、Seqrite Terminator インターフェースを設定します。
ブリッジを設定	このオプションを使用して、2 つのインターフェース間のブリッジを設定します。
リンクアグリゲーションの設定	このオプションを使用して、リンクアグリゲーションインターフェースを設定します。
インターフェースステータスの変更	このオプションを使用して、インターフェースを有効または無効にします。

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。
すべてのインターフェースの削除	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除します。
デフォルトルートの設定	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。

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] > [DNS を設定]** へログインします。



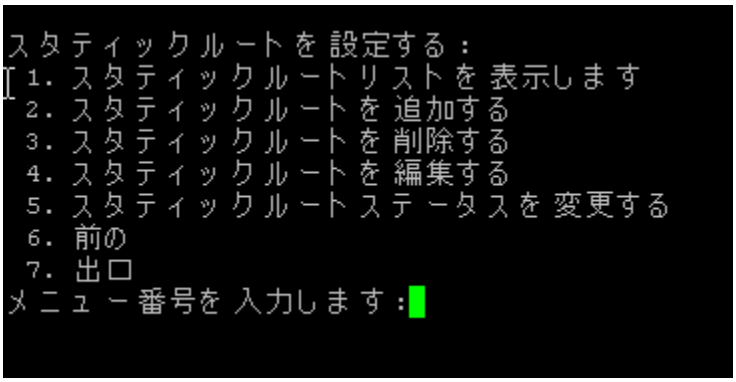
[DNS を設定] で利用可能な各種のメニューの説明を、次の表に示します。

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]** へログインします。

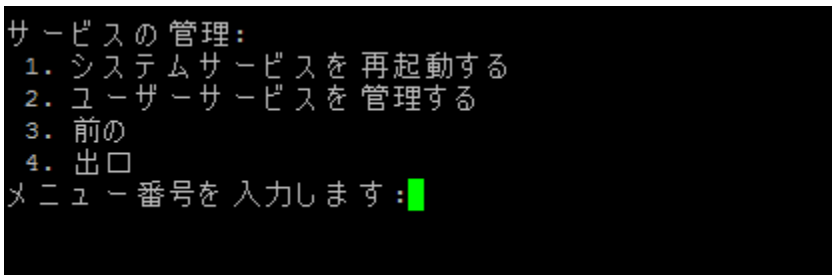


［スタティックルートを設定］で利用機能なオプションの説明を、次の表に示します。

メニュー	説明
スタティックルートリストの表示	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認できます。
スタティックルートの追加	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す。
スタティックルートの削除	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す。
スタティックルートを編集	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す。
スタティックルートステータスを変更	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を変更します。

CLI を使用してサービスを管理する

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］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	説明

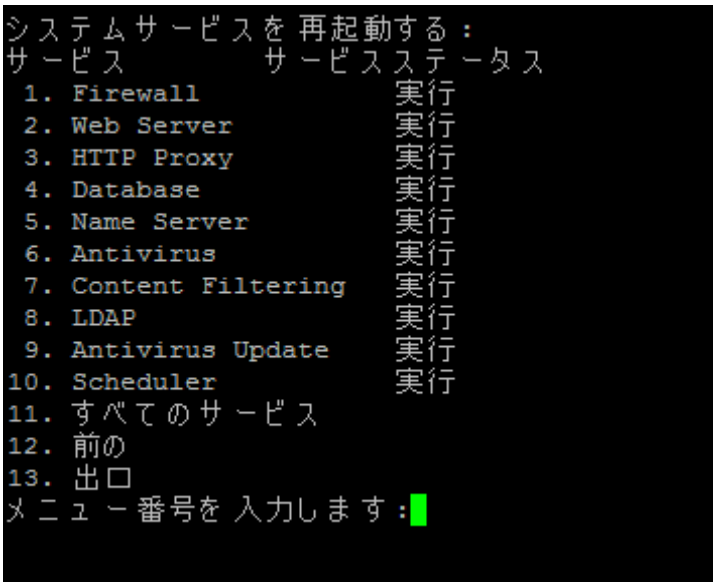
システムサービスを再起動	このオプションを使用して、システムサービスを再起動します。
ユーザーサービスの管理	このオプションを使用して、次のようなユーザーサービスを管理します。 • IPS • アプリケーションコントロール • ポリシーに基づいたルーティング

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              サービスステータス
 1. IPS                               使用可能              実行
 2. Application Control               使用不可能            止められる
 3. Policy Based Routing              使用可能              実行
 4. 前の
 5. 出口
メニュー番号を入力します：
```

［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。
アプリケーションコントロール	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有効化、無効化、または再起動します。
ポリシーに基づいたルーティング	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。

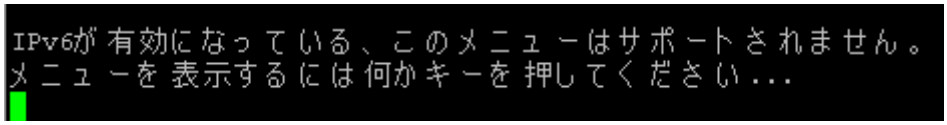
注意:IPv6 が有効な場合、CLI コンソールから次のモジュールへはアクセスできません。

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

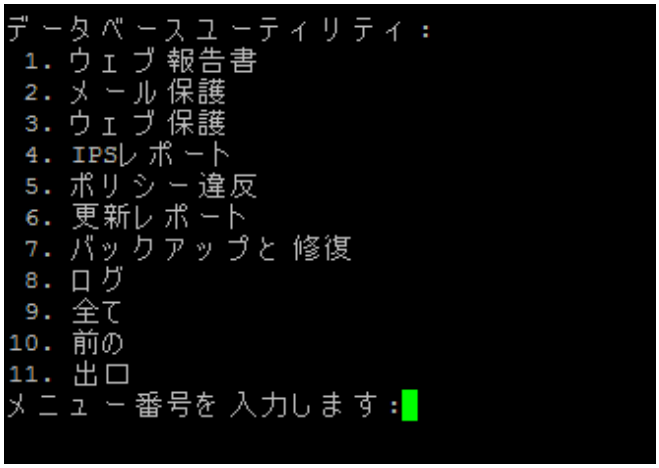
システムで IPv6 が有効な場合、次のメッセージが表示されます。



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］**へログインします。
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。



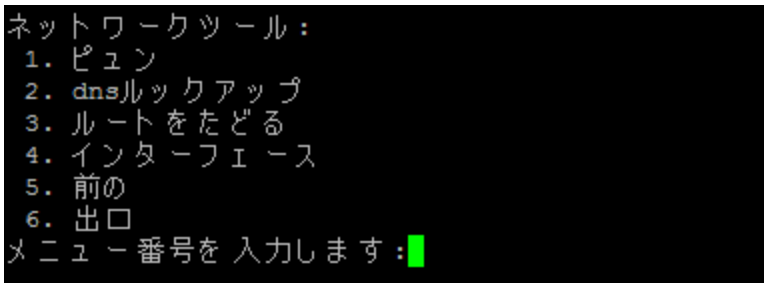
［データベースユーティリティ］で利用可能な各種のメニューの説明を、次の表に示します。

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］**へログオンします。



［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]** へログインします。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。

Chapter

12

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]** へログオンします。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。

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. Seqrite［Terminator］>**［ヘルプ］**>**［サポート］**へログインします。
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~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］>**［ヘルプ］**>**［サポート］**へログインします。
2. **［リモートサポート］**ボタンをクリックします。

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.seqrite.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、http://www.seqrite.com/int_techsupp をご覧ください。

お客様の国内の販売店を調べるには、http://www.seqrite.com/locate-dealer 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。www.seqrite.com

インデックス

キ

グ

ゲ

コ

サ

ス

ダ

デ

ド

ト

ネ

バ

フ

ブ

ポ

ホ

メ

ユ

リ

ル

レ

ロ

ワ

仮

侵

保

出

単

定

帯

復

操

日

時

本

管

統

証

認

負

通

除

電