Seqrite Endpoint Security 7.1

管理者ガイド

SEPS SME
SEPS ビジネス
SEPS トータル
SEPS エンタープライズスイート

www.seqrite.jp

著作権情報

商標

ライセンス条項

本文書について

改訂履歴

バージョン	変更日	改訂者	処置
1.0	2016年11月	QA およびテクニカルライター	EPS 7.1 リリース

文書規約

本ユーザーガイドには、Windows オペレーティングシステムに Seqrite Endpoint Security をインストールしてお使いいただく上で必要な情報がすべて記載されています。次の表では、本ガイドの作成にあたって使用した規定について記載しています。

規定	意味
太字フォント	太字はメニュータイトル、ウィンドウタイトル、チェックボックス、ドロップダウンメニュー、ダイアログ、ボタンの名称、ハイパーリンクなどを表します。
	この記号は注意を表します。対象のトピックに関連する重要なポイントを補足したり、ただし書きを強調したりします。

目次

Chapter

1

Seqrite Endpoint Security の紹介

あらゆる組織では、貴重なデータやリソースのセキュリティが重要な課題となります。今やウェブ技術はあらゆる組織でビジネスプロセスの不可欠な要素となっています。こうした状況により、組織は新たな未知の脅威や攻撃にさらされやすくなります。Seqrite Endpoint Security (SEPS) は、悪意のある多様な脅威（ウイルス、トロイの木馬、ワーム、バックドア、スパイウェア、リスクウェア、アダルトコンテンツ、ハッカーなど）に対抗して、小規模ネットワークから大企業レベルのネットワークまで包括的に保護するセキュリティソリューションを提供するように設計されています。

SEPS は、デスクトップ、ノートパソコン、およびネットワークサーバーを統合するウェブベースのマネジメントソリューションです。ネットワーク内のあらゆるクライアントおよびサーバーにアクセスし、それらを遠隔操作で管理することができます。クライアントおよびサーバー上で、アンチウイルスソフトウェアアプリケーションの展開、セキュリティポリシーの設定、シグネチャパターンのアップデート、ソフトウェアのアップデートを行うことができます。また、クライアントを監視して組織内にポリシー違反やセキュリティ脅威が存在するかどうかを確認し、ネットワーク全体のセキュリティを確保するための適切な処置をとることができます。

Seqrite Endpoint Security の機能の仕方?

Seqrite Endpoint Security (SEPS) はクライアント/サーバーアーキテクチャで機能し、ネットワークに展開されたすべてのクライアントエージェントをコンソールで管理します。コンソールおよびクライアントエージェントは、Microsoft Windows オペレーティングシステムのほぼすべてのタイプにインストールすることができます。クライアントエージェントは、Linux および Mac オペレーティングシステム (OS) のマシンにインストールすることもできます。コンソールおよびクライアントエージェントのシステム要件に関する詳細な説明については、システム要件をご覧ください。

SEPS は、管理者が Seqrite を指定のコンピュータ、グループ、またはドメイン（同一のドメイン内）に遠隔操作で展開する際に役立ちます。Seqrite Antivirus のサーバーコピーがアップデートされると、サーバーからアップデートするように設定されたすべてのコンピュータは、お客様による作業なしに自動的にアップデートされます。SEPS がこれらのプロセスを監視し、管理者が Seqrite Antivirus がインストールされたコ

ンピュータ、Seqrite のウイルスデータベースの日付、ウイルス対策が有効化どうか、およびウイルスがワークステーションのメモリでアクティブであるかどうかを確認できるようにします。アクティブなウイルスがワークステーションのメモリ内で検出された場合、そのワークステーションはネットワークから切断されます。ワークステーションから Seqrite のアンインストールが検出された場合、お客様による作業なしに遠隔操作で Seqrite が再インストールされます。これにより、コンピュータとネットワークはウイルスの脅威から保護されます。

本リリースの新機能

Seqrite Endpoint Security 7.1 は以下の新機能を提供します:

1. Azure または AWS クラウドサーバーで Seqrite EPS サーバーをインストールすることができます。このインストールをパブリックインストールと呼びます。
2. クライアントパッケージャの作成方法はインストールモードにより変わります。
3. リダイレクト設定での変更。
4. 分散 EPS 環境におけるパッチ管理サーバーの設定。
5. アセット管理
   - アセット管理用にカスタマイズされたレポート。
   - プロダクトキーは Windows OS に表示されます。この機能は Windows Vista 以降の OS でサポートされます。
   - プロダクトキーは MS オフィスに表示されます。この機能は MS Office 2010 ～ 2016 でサポートされます。
   - インストールされた MS オフィスのライセンスステータスはライセンスなし / ライセンスあり / OOBGrace / OOTGrace/ NonGenuineGrace / 通知 / ExtendedGrace と表示されます。
6. データ喪失防止
   - 以下の DLP 機能が追加されます:
     - 特定グループの DLP
     - カスタム拡張子
     - ドメイン例外
     - アプリケーション例外
     - ネットワーク共有例外

       ドメイン例外は Windows プラットフォーム上の Outlook と Thunderbird メールクライアントのみサポートします。

       カスタム拡張子、アプリケーション例外およびネットワーク共有例外は Windows プラットフォームでサポートされます。
   - DLP では、プリントスクリーンが使用されると、ポップアップが表示され、レポートが生成されます。

- データがローカルドライバからネットワーク共有またはリムーバブルドライブへ送信されるときにのみ DLP データは監視されます。データがネットワーク共有またはリムーバブルドライブからローカルドライバへ送信されるときには DLP データは監視されません。

7. スタンドアロンアップデートマネージャー (STUM) の自動サイト作成
   - IIS がシステムにインストールされていない場合、スタンドアロンアップデートマネージャー のインストール処理が行われている時に IIS が自動的にインストールされます。
   - IIS サイトは HTTP プロトコルを指定して設定されます。
   - Windows XP と 2003 OS の場合、IIS は手動でインストールされ、ポート 80 を指定して設定されなければなりません。
   - スタンドアローンアップデートマネージャーは Windows Home Editions ではサポートされません。
   - EPS コンソールでは、クライアントエージェントでインストールされた場合、STUM アップデート URL は取得されません。
   - アップデートマネージャに自動カスタムスケジュラーを設定することができます。
8. アップデートマネージャ帯域幅の制御。帯域幅の範囲は 64kbps～8192kbps に制御されます。
9. EPS コンソールから以下のアップデートマネージャ設定も管理できます:
   - サービスパックのダウンロード
   - スケジュール設定
   - 帯域幅の設定
   - アップデートをダウンロードするプラットフォームリスト
10. ライセンス関連の変更
    - DLP パックは特定のエンドポイントに割り当てることができます。
    - DLP カウントは、有効化、更新、 追加、AddPack トランザクション時に追加できます。
    - DLP カウントは更新手続きの時に減らすことができます。
11. Web コンソールパスワードのリセット
    - EPS コンソールログインページに［パスワードを忘れた場合］リンクが追加されます。このリンクを使用して Web コンソールパスワードをリセットできます。
    - SMTP 設定が行われていない場合、ユーザーはパスワードリセットツールを使用してリセットすることができます。パスワードリセットツールはインストール場所にあります。

- ログイン試行回数は 6 回までです。6 回ログインに失敗すると、そのユーザーアカウントは 6 時間ロックされます。

12. 複数のエンドポイントをパッチ管理除外リストに追加できます。
13. Linux クライアント
    - Linux 用の新しい OS サポート -
        - RHEL -6.2、6.3、6.4、6.6、6.7、6.8、7.0、7.1 および 7.2 (32 ビットと 64 ビット)
        - CentOS -6.3 (32 ビット)
        - Fedora -18 (32 ビット)
        - Ubuntu -10.10 (64 ビット)
        - openSUSE-11.4 (64 ビット)
        - openSUSE-12.3 (64 ビット)
        - Ubuntu -11.4 (32 & 64 ビット)
        - SUSE -11.00, 12.00 (32 ビットと 64 ビット)
    - Linux クライアントでクライアントパッケージャを作成するための規定

利用可能な系統

Seqrite Endpoint Security には以下の系統があります:

- SME (中小企業エディション)
- ビジネス
- トータル
- エンタープライズスイート

以下の表は、これらのタイプで利用可能な機能を示しています:

機能	ステータス			
	SME	ビジネス	トータル	エンタープライズスイート
不正侵入防御・検知システム (IDS/IPS) 保護	✓	✓	✓	✓
ファイアウォール	✓	✓	✓	✓
フィッシング対策	✓	✓	✓	✓
ブラウジング保護	✓	✓	✓	✓
SME 通知	✓	✓	✓	✓
脆弱性スキャン (VS)	✓	✓	✓	✓
クライアントのローミ	✓	✓	✓	✓

ング				
アセット管理	X	✓	✓	✓
アンチスパム	X	✓	✓	✓
ウェブセキュリティ	X	✓	✓	✓
高度なデバイスコントロール	X	✓	✓	✓
アプリケーションコントロール	X	X	✓	✓
チューンアップ	X	X	✓	✓
PC2 モバイル	X	X	✓	✓
ファイル活動モニター (FAM)	X	X	✓	✓
パッチ管理	X	X	✓	✓
DLP	X	X	X	✓

機能パック定義:

パック名	機能	系統
DLP	データ喪失防止 + 保存データスキャンレポート	ビジネスおよびトータルエディションでは DLP 機能を利用できます。DLP を利用するには、SME をビジネスまたはトータルにアップグレードする必要があります。

ネットワーク展開シナリオ

ネットワークの設定は、組織の規模とアーキテクチャによって異なります。サーバー 1 台と複数のクライアントというシンプルなネットワーク設定を好む組織もあれば、サブネットや DHCP サーバーを持つネットワーク設定を好む組織もあります。また、巨大なネットワークの組織では、複数の LAN カードを持つ 1 台のサーバーが、異なる IP 範囲を持つネットワークの要求に応えることもあります。

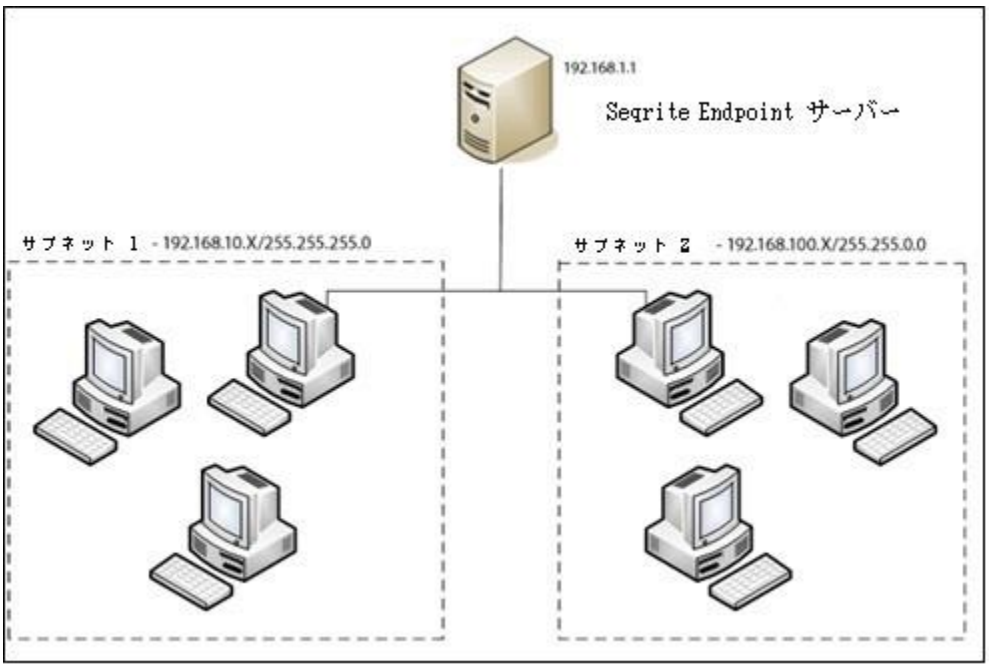
Seqrite は、組織によって様々なネットワーク設定の課題があることを認識しています。そのため、当社は以下の主な 3 つのネットワークセットアップを推奨しています:

シナリオ 1

スタティック IP アドレスでサブネットが設定されたネットワークへの Seqrite Endpoint Security のインストール。

ネットワーク設定の説明

ネットワーク全体はスタティック IP アドレスで設定され、ネットワークはメインサーバーに接続されたサブネットで構成されています。Seqrite Endpoint Security はサーバーにインストールされ、Seqrite クライアントエージェントはサブネットのエンドポイントシステムに展開されます。



Seqrite 推奨事項

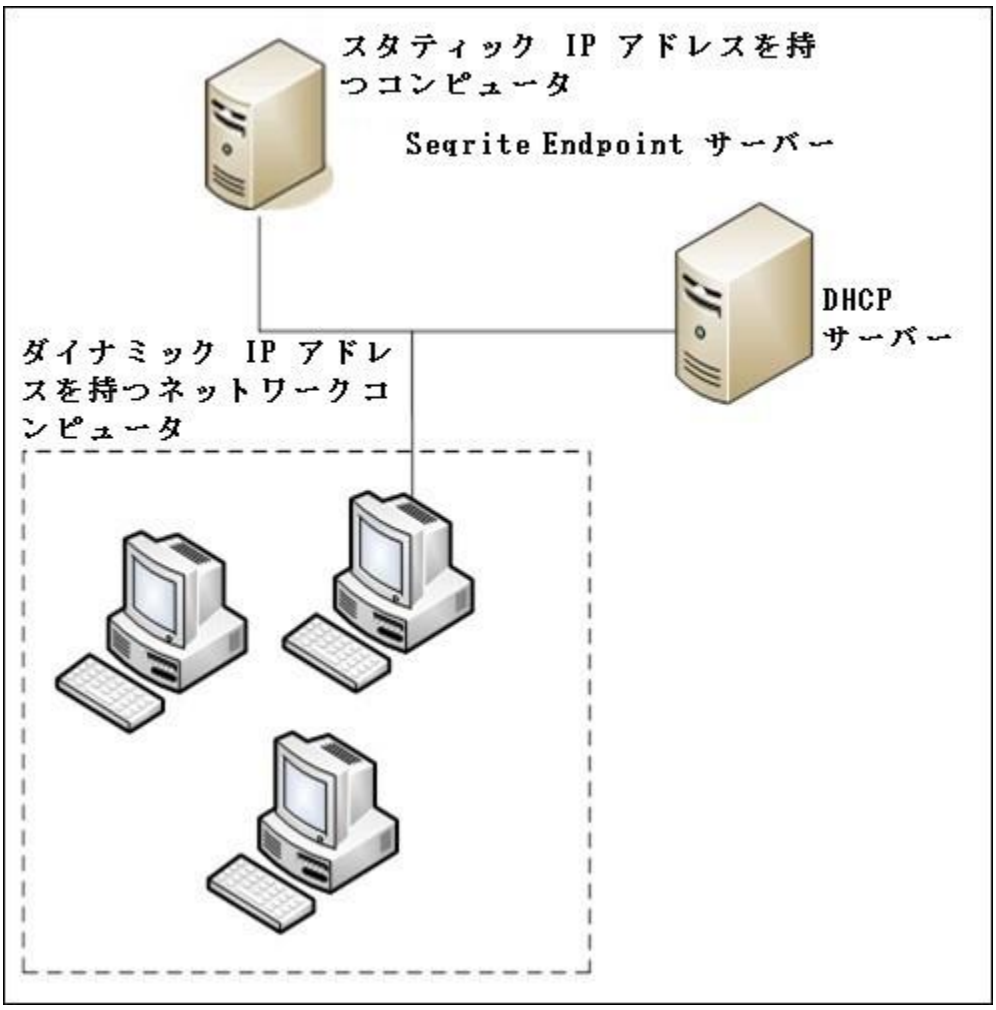
- インストール前に、サーバーとエンドポイントが接続されていることを確認します。これは、サーバーからエンドポイントへの ping およびエンドポイントからサーバーへの ping を実行することによって確認します。
- サーバーシステムは、スタティック IP アドレスで設定する必要があります。
- Seqrite Endpoint Security のインストール時に、[サーバー情報] 画面で IP アドレスを選択します。

シナリオ 2

DHCP サーバーでエンドポイントが設定されたネットワークへの Seqrite Endpoint Security のインストール。

ネットワーク設定の説明

ネットワーク全体は DHCP サーバーで設定されています。Seqrite Endpoint Security はサーバーシステムにインストールされ、Seqrite エンドポイントエージェントはエンドポイントシステムに展開されます。

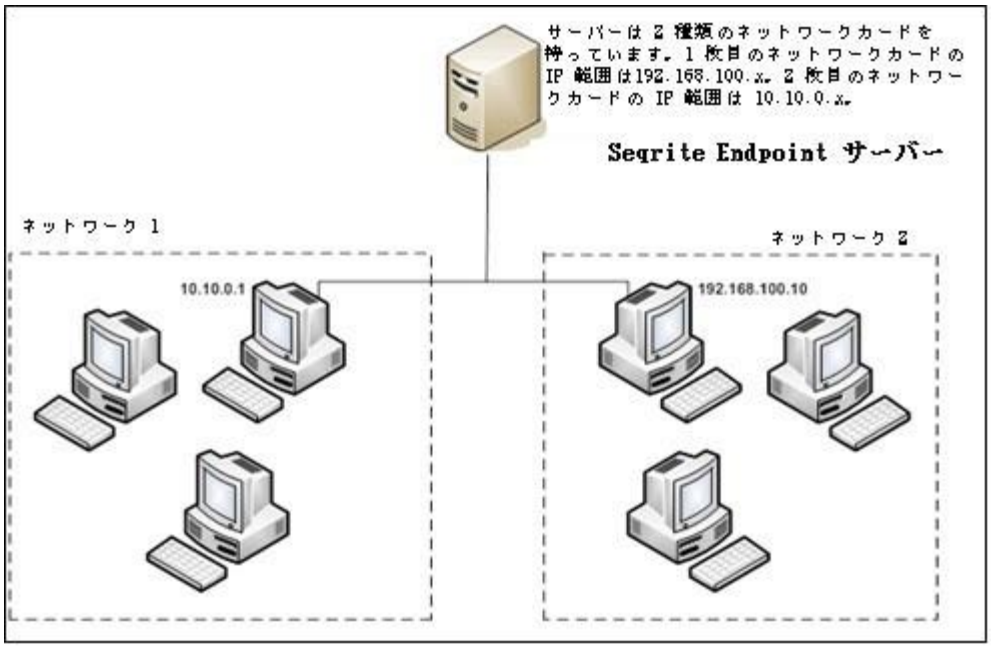


シナリオ 3

2 枚のネットワークカードを使って、サーバーに Seqrite Endpoint Security をインストールします。

ネットワーク設定の説明

サーバーは 2 種類のネットワークカードで構成され、それぞれ異なる IP 範囲のネットワークに対応します（例:一方のネットワークは 10.10.0.1 の IP 範囲を持ち、他方のネットワークは 192.168.100.10 の IP 範囲を持つ)。Seqrite Endpoint Security は 2 種類のネットワークカードにインストールされ、Seqrite クライアントは両方のネットワークのすべてのエンドポイントシステムにインストールされます。



Seqrite の推奨事項

- インストール前に、サーバーとエンドポイントが接続されていることを確認します。これは、サーバーからエンドポイントへの ping およびエンドポイントからサーバーへの ping を実行することによって確認します。IP アドレスとコンピュータ名で ping を試行します。
- サーバーシステムは、スタティック IP アドレスで設定する必要があります。
- Seqrite Endpoint Security のインストール時に、[サーバー情報] 画面でドメイン名を選択します。ターゲットサーバーのドメイン名を指定します。また、エンドポイントが DNS サーバー (エンドポイント IP アドレスで FQDN を解決できるサーバー) にアクセスできる場合には、サーバーの完全修飾ドメイン名 (FQDN) を使用することもできます。

Chapter

2

はじめに

Seqrite Endpoint Security (SEPS) は、簡単にインストールできる使いやすい製品です。インストールの際には各画面をよく読み、指示に従ってください。

前提条件

SEPS をコンピュータにインストールする際は下記のガイドラインに従ってください:

- 他のすべてのアンチウイルスソフトウェア/ハードウェアをサーバーおよびエンドポイントから削除した上で、Seqrite EPS のインストールを続行することをお勧めします。複数のアンチウイルスプログラムがインストールされていると、システムが誤作動を起こす可能性があります。
- Seqrite EPS インストールを続行する前に、すべてのプログラムを終了してください。
- ネットワークは TCP/IP プロトコルで設定する必要があります。
- Microsoft ネットワークで共有されるファイルおよびプリンタをインストールしなければなりません。
- Seqrite EPS サーバーにインストールするには、サーバーに対する管理者またはドメイン管理者の権限が必要です。
- ログインスクリプトのセットアップを使用するために、Windows Server 2012 R2 / Windows Server 2012 / Windows 2008 Server R2 / Windows 2008 Server / Windows 2003 Server / Windows 2000 Advanced Server / Windows 2000 Server を Active Directory サービスで適切に設定する必要があります。

SEPS サーバーの　システム要件

Seqrite Endpoint Security サーバーのシステム要件は以下の通りです:

一般要件

SEPS サーバーがインストールされているコンピュータは以下の要件を満たさなければなりません。

コンポーネント	要件
プロセッサ	**最小限**: 1 GHz 32 ビット (x86) または 64 ビット (x64) Intel Pentium **推奨**: 2 GHz 32 ビット (x86) または 64 ビット (x64) Intel Pentium 以上
RAM	**最小限**: 2 GB **推奨**: 4 GB 以上
ハードディスク容量	**最小限**: ディスクの空き容量 4800 MB **推奨**: ディスクの空き容量 10000 MB
ウェブブラウザ	• Internet Explorer 7、8、9、10 または 11 • Google Chrome 45、46 または 47 • Mozilla Firefox 38、39 または 40
ディスプレイ	1024 X 768

- クライアントが 25 以上ある場合、Seqrite は Windows サーバーオペレーティングシステムで EPS サーバーとパッチ管理サーバーをインストールされることを推奨します。
- クライアントが 500 以上ある場合、Seqrite は専用の Web サーバー (IIS) を推奨します。

オペレーティングシステム要件

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32 ビット / 64 ビット)
- Microsoft Windows 8.1 Professional/Enterprise (32 ビット/64 ビット)
- Microsoft Windows 8 Professional/Enterprise (32 ビット/64 ビット)
- Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32 ビット / 64 ビット)
- Microsoft Windows Vista Home Premium / Business / Enterprise / Ultimate (32 ビット / 64 ビット)
- Microsoft Windows XP 32 ビット SP3、64 ビット SP1 および SP2 / Professional Edition (32 ビット / 64 ビット)
- Microsoft Windows Server 2012 R2 Standard/Datacenter (64 ビット)
- Microsoft Windows MultiPoint Server 2012 Standard (64 ビット)

- Microsoft Windows Server 2012 Standard/Essentials/Foundation/Storage Server/Datacenter (64 ビット)
- Microsoft Windows SBS 2011 Standard/Essentials
- Microsoft Windows 2008 Server R2 Web/Standard/Enterprise/Datacenter (64 ビット)
- Microsoft Windows 2008 Server Web/Standard/Enterprise (32 ビット/64 ビット)/Datacenter (64 ビット)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web/Standard/Enterprise (32 ビット/64 ビット)

SEPS サーバーで必要な追加のソフトウェア

Seqrite EPS サーバーの場合、コンピュータシステムに Microsoft IIS Web サーバーと Microsoft .NET Framework 4.0 がインストールされていなければなりません。

Web サーバー	要件
IIS	IIS Version 10 (Windows 10)
	IIS Version 8.5 (Windows 8.1 および Windows Server 2012 R2)
	IIS Version 8.0 (Windows 8 および Windows Server 2012)
	IIS Version 7.5 (Windows 7 および Windows Server 2008 R2)
	IIS Version 7.0 (Windows Vista および Windows Server 2008)
	IIS Version 6.0 (Windows Server 2003)
	IIS Version 5.1 (Windows XP SP3)

EPS インストーラは必要な IIS コンポーネントをインストールします。

Java Runtime Environment (JRE) 要件

Web Java Runtime Environment (JRE) では、ウェブページを介したインストールとデバイス機能の追加を行うために以下が必要です:

OS バージョン	要件	JRE
32 ビット	32 ビット	JRE 7、JRE 8
64 ビット	32 ビット	32 ビット JRE 7、32 ビット JRE

		8
	64 ビット	64 ビット JRE 7、64 ビット JRE 8

Seqrite EPS クライアントのシステム要件

Seqrite Endpoint Security クライアントのシステム要件は以下の通りです:

一般要件

SEPS クライアントがインストールされているコンピュータは以下の要件を満たさなければなりません。

コンポーネント	要件
プロセッサ	**最小限**: Windows Vista 用 1 GHz 32 ビット (x86) または 64 ビット (x64) プロセッサ **推奨**: Windows Vista 以降用 2 GHz 32 ビット (x86) または 64 ビット (x64) プロセッサ
RAM	**最小限**: 1 GB **推奨**: 2 GB 以上
ハードディスク容量	3200 MB
ウェブブラウザ	Internet Explorer 5.5 以上

オペレーティングシステム要件

Seqrite Endpoint Security クライアントは、以下のいずれかのオペレーティングシステムを持つコンピュータシステムにインストールすることができます:

- Microsoft Windows 10 Home / Pro / Enterprise / Education (32 ビット / 64 ビット)
- Microsoft Windows 8.1 Professional/Enterprise (32 ビット/64 ビット)
- Microsoft Windows 8 Professional/Enterprise (32 ビット/64 ビット)
- Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32 ビット / 64 ビット)
- Microsoft Windows Vista Home Basic/ Premium / Business / Enterprise / Ultimate (32 ビット / 64 ビット)

- Microsoft Windows XP Home (32-bit) / Professional Edition (32 ビット / 32 ビット)
- Microsoft Windows Server 2012 R2 Standard/Datacenter (64 ビット)
- Microsoft Windows MultiPoint Server 2012 Standard (64 ビット)
- Microsoft Windows Server 2012 Standard/Essentials/Foundation/Storage Server/Datacenter (64 ビット)
- Microsoft Windows SBS 2011 Standard/Essentials
- Microsoft Windows 2008 Server R2 Web/Standard/Enterprise/Datacenter (64 ビット)
- Microsoft Windows 2008 Server Web/Standard/Enterprise (32 ビット/64 ビット)/Datacenter (64 ビット)
- Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- Microsoft Windows Server 2003 Web/Standard/Enterprise (32 ビット/64 ビット)
- Microsoft Windows 2000 SP 4 Professional/Server/Advanced Server

Mac OS 用システム要件

Mac OS にインストールされた Seqrite EPS クライアントのソフトウェアとハードウェア要件。

コンポーネント	要件
MAC OS	Mac OS OS X、10.6、10.7、10.8、10.9、10.10、10.11、10.12
プロセッサ	Intel または互換プロセッサ
RAM	**最小限**: 512 MB **推奨**: 2 GB 以上
ハードディスク容量	1200 MB

Linux OS 用システム要件

Linux OS にインストールされた Seqrite EPS クライアントのソフトウェアとハードウェア要件:

コンポーネント	Linux OS バージョン	要件
Linux OS	32 ビット	• BOSS 6 • Fedora 14、18、19、20、21 • openSUSE 11.4、12.2、12.3 • Linux Mint 13、14、15、16、17.3 • Ubuntu 10.10、12.04 LTS、12.04.3 LTS、13.04、13.10、14.04、14.10 および 15.04 • CentOS 6.3、6.4、6.5
	64 ビット	• Fedora 14、18、19、20、21 • openSUSE 11.4、12.2、12.2 • Linux Mint 13、14、15、16、17.3 • Ubuntu 10.10、11.4、12.04.2 LTS、13.04、13.10、14.04、14.10 および 15.04 • CentOS 6.3、6.4、6.5
プロセッサ		Intel または互換プロセッサ
RAM		**最小限**: 512 MB **推奨**: 1 GB 以上
メモリ		300 Mhz 以上
ハードディスク容量		1200 MB

システム要件に関する詳細を確認するには、http://www.seqrite.jp にアクセスしてください。

Windows オペレーティングシステムでの Seqrite Endpoint Security サーバーのインストール

Seqrite Endpoint Security サーバーのインストールを開始するには、以下の手順に従ってください:

1. ソフトウェアライセンス証書に記載されている URL から Seqrite Endpoint Security にセットアップダウンローダをダウンロードし、実行します。
2. セットアップを実行します。
3. Seqrite セットアップダウンローダで、以下の手順に従ってください:

i. [**セットアップをダウンロードするディレクトリの選択**]で、セットアップをダウンロードする場所を選択します。

ii. [**ダウンロードの完了後セットアップを開始**] チェックボックスは初期設定で選択されています。この設定により、ダウンロードの完了後すぐにインストールが開始されます。

iii. SEPS を後でインストールしたい場合は、[**ダウンロードの完了後セットアップを開始**] チェックボックスのチェックを外します。[**ダウンロードの完了後フォルダの位置を開く**] を選択します。

iv. [**ダウンロード**] をクリックします。ダウンロード時間とダウンロードの経過が表示されます。ダウンロードが終了すると、「Seqrite Endpoint Security セットアップが正常にダウンロードされました」というメッセージが表示されます。

4. [**ダウンロードの完了後セットアップを開始**] オプションチェックボックスが選択されている場合、セットアップのダウンロード後、SEPS セットアップウィザードがすぐに起動されます。

   [**ダウンロードの完了後フォルダの位置を開く**] オプションが選択されている場合、フォルダーが開きます。インストーラファイルを選択してダブルクリックします。SEPS セットアップウィザードが起動します。

5. Seqrite Endpoint Security に関する情報を読みます。[**次へ**] をクリックします。

6. 使用許諾契約書が表示されます。使用許諾契約書はよくお読みください。Seqrite Endpoint Security をインストールして使用されると、Seqrite Endpoint Security エンドユーザーライセンス条項に正式に同意されたものと見なされます。

   [**同意する**] を選択して使用許諾契約書に同意し、[**次へ**] をクリックします。

7. Seqrite EPS サーバーを使用される場合、インストールを完了するにはコンピュータシステムに Microsoft .NET Framework 4.0 および Microsoft IIS Web サーバーがインストールされていなければなりません。

   .NET と IIS の両方がすでにインストールされている場合、SEPS セットアップウィザードが続行されます。

   .NET、IIS または必要なコンポーネントのいずれか一つがインストールされていない場合、[前提条件確認] 画面が表示されます。この画面には、インストールの続行に必要なインストールされたコンポーネントや不足しているコンポーネントが表示されます。[**次へ**] をクリックします。

   このウィザードは .NET と IIS コンポーネントのインストールをサポートします。

   .NET フレームワークをインストールするには、以下の手順に従ってください。

   .NET フレームのインストール画面が表示されます。

   i. [**次へ**] をクリックして、,NET フレームワークのインストールを続行します。

ii. [Microsoft .NET フレームワーク 4 セットアップ] 画面で [**ライセンス条項を読み同意しました**] チェックボックスを選択して [**インストール**] をクリックします。

インストールが行われます。

iii. [Microsoft .NET フレームワーク 4 セットアップ] 画面で [**完了**] をクリックします。

iv. システムが再起動します。

v. インストールファイルから再度 Endpoint Security のインストールを開始します。

IIS をインストールするには、以下の手順に従ってください。

i. IIS のインストール画面が表示されます。

[前提条件 - インターネットインフォメーションサービス (IIS)] 画面で [**次へ**] をクリックします。

IIS がシステムで設定されます。

ii. [**次へ**] をクリックして SEPS セットアップウィザードを続行します。

Windows Server 2003 と XP で IIS を有効にする場合、Windows Server 2003 と XP での IIS の有効化を参照してください。

8. デフォルトフォルダではない別のフォルダに Seqrite Endpoint Security サーバーをインストールしたい場合は [**参照**] をクリックします。デフォルトパスでデフォルトインストールを続行する場合は、[**次へ**] をクリックします。

ウイルス対策のために Seqrite Endpoint Security インストーラはシステムメモリをスキャンし、インストールされたシステムコンポーネントを確認します。

SEPS のインストール時に別のアンチウィルスソフトウェアがコンピュータに既に存在している場合、既存のアンチウィルスソフトウェアをアンインストールするようメッセージが表示されます。

既存のアンチウィルスソフトウェアが削除されるまで SEPS サーバーインストールは実行されません。

9. [サーバー情報] 画面で、以下の手順に従ってください:

i. [サーバー設定] セクションで、次のうちの 1 つを選択し、情報を提供します:

ドメイン名:リストから**モデル名**を選択します。また、エンドポイントが DNS サーバー (エンドポイント IP アドレスで FQDN を解決できるサーバー) にアクセスできる場合には、サーバーの完全修飾ドメイン名 (FQDN) を使用することもできます。

ネットワークが DHCP を使用して設定されている場合、ドメイン名を選択します。

IP アドレス:リストからサーバーの **IP アドレス**を選択します。

ii. AWS/Azure プラットフォームでホストされているシステムに Seqrite Endpoint Security をインストールしている場合、[**パブリックインストール**] チェックボックスを選択します。

推奨事項

- エンドポイントをローカル（プライベート）に展開する場合、Seqrite はプライベート IP にインストールすることを推奨します。
- エンドポイントをローカルとリモートに展開する場合、Seqrite はプライベート IP をパブリック IP に変換してからインストールされることを推奨します。この場合、リモートクライアントにクライアントパッケージャを作成しているときに、別の IP アドレスかドメイン名が提供されます。
- すべてのエンドポイントをリモートに展開する場合、Seqrite はパブリックインストールを推奨します。

iii. HTTP セクションにポート番号が表示されます。HTTP ポート番号では、サーバーのリスニングポートとして使用するポートです。このコンソールを起動するための Seqrite Endpoint Security サーバーアドレスは以下の通りです。

- Windows XP の場合: http://{Seqrite_Endpoint_Security_Server_name}/qhscan71
- 他の OS の場合: http://{Seqrite_Endpoint_Security_Server_name}:{port number}

iv. SSL セクションで、[**Enable Secure Socket Layer**] チェックボックスがデフォルトで選択されていると、**SSL ポート**番号が表示されます。

このポート番号はサーバーのリスニングポートとして機能します。このコンソールを起動するための Seqrite Endpoint Security サーバーアドレスは以下の通りです。

- Windows XP の場合: http://{Seqrite_Endpoint_Security_Server_name}/qhscan71
- 他の OS の場合: https://{Seqrite_Endpoint_Security_Server_name}:{port number}

以下のポートを使用しないでください。

- ポート番号 0-1023
- MySQL ポート 62222

v. [**次へ**] をクリックします。

vi. ウェブサーバー設定の確認を求めるメッセージが表示されます。

10. 確認するには、[**はい**] をクリックします。

必要に応じて、設定を変更することができます。

11. パブリックインストールを選択している場合、リモートクライアントが EPS サーバーと通信するために使用するターゲットサーバーの**ドメイン名または IP アドレス**を指定します。

    デフォルトで、ドメイン名/IP アドレスの EPS サーバーで通信するために設定されるクライアントパッケージャでクライアントがインストールされます。

12. **[次へ]** をクリックします。

13. [プロキシ設定] 画面が表示されます。

    ネットワークでプロキシサーバーをお使いの場合、または Socks バージョン 4 および 5 のネットワークをお使いの場合には、プロキシと SOCKS V4 および SOCKS V 5 サーバーの IP アドレス（またはドメイン名）とポートを［接続設定］に入力する必要があります。ユーザー名とパスワードはログオンに必須です。

    SEPS モジュール、登録ウィザード、アップデートマネージャ、およびマネージャはインターネット接続に以下の設定を使用します。

    プロキシ設定を有効化および設定するには:

    i. **[プロキシ設定を有効にする]** チェックボックスを選択します。

    ii. 設定に従い、プロキシのタイプとして HTTP プロキシ、Socks V 4 または SOCKS V 5 を選択します。

    iii. [プロキシサーバー] テキストボックスに、プロキシサーバーの IP アドレスまたはドメイン名を入力します（例えば、proxy.yourcompany.com など)。

    iv. **[ポート]** テキストボックスに、プロキシサーバーのポート番号(例: 80) を入力します。

    v. **[ユーザー名]** と **[パスワード]** テキストボックスに、プロキシサーバー認証を入力します。

    vi. **[次へ]** をクリックします。

14. [クライアントインストール設定] 画面が表示されます。

    この画面で指定したパスに従い、Seqrite クライアントがエンドポイントにインストールされます。以下の設定が表示されます:

    - デフォルトのエンドポイントインストールパスが表示されます。パスは %PROGRAMFILES% または %BOOTDRIVE% variable のいずれかの変数で指定することができます。例を挙げます。%PROGRAMFILES%¥Seqrite¥Seqrite または %BOOTDRIVE%¥Seqrite。

    - クライアントエージェント通信ポート番号が表示されます。

      Seqrite クライアントはこのポート番号を使用してサーバーと通信し、重要な指示（スキャン、アップデートなど）を取得したり Seqrite Endpoint Sec

urity サーバーにログを送信したりします。そのため、このポート番号がネットワーク内の他のアプリケーションで使用されないようにしてください。

［**次へ**］をクリックします。

15. 確認のための確認ダイアログボックスが表示されます。必要に応じてポート番号を変更できます。

    確認するには、［**はい**］をクリックします。

16. 認証画面が表示されます。

    ウェブコンソールにアクセスするための Seqrite Endpoint Security 管理者パスワード、およびエンドポイント側のエンドポイント設定にアクセスするためのエンドポイントパスワードを作成します。ただし、管理者とエンドポイントのパスワードは別のものにする必要があります。同じものにすると、インストールは続行できません。

    i. エンドポイントセキュリティ管理者パスワードセクションの［**パスワードと確認用パスワード**］テキストボックスにパスワードを入力します。

    ii. クライアントパスワードセクションの［**パスワードと確認用パスワード**］テキストボックスにパスワードを入力します。

    これにより、無許可のユーザーがウェブコンソールにアクセスして設定を変更したりエンドポイントを削除したりすることはできなくなります。

    iii. ［**次へ**］をクリックします。

17. インストール概要画面が表示されます。必要に応じて、設定を変更することができます。

    ［**次へ**］をクリックします。

18. システムで Seqrite Endpoint Security のインストールを続行すると、システムのネットワーク接続が一時的に無効になることを示す確認ダイアログボックスが表示されます。

    インストールを続行するには、［**OK**］をクリックします。

19. インストールプロセスが開始されます。［**お読みください**］情報画面が表示されます。Seqrite Endpoint Security に関する重要な情報をお読みください。

    ［**次へ**］をクリックします。

20. Seqrite Endpoint Security を登録して アップデートマネージャを設定するには、［**次へ**］をクリックします。これらのタスクを後で実行する場合は、これらのオプションをクリアします。

21. インストールを完了するには、［**終了**］をクリックします。

Windows Server 2003 と XP で IIS を有効にする場合

1. ［**スタート**］>［**設定**］>［**コントロールパネル**］をクリックします。

2. コントロールパネルで［**プログラムの追加と削除**］をダブルクリックします。
3. ［プログラムの追加と削除］ダイアログボックスの左側パネルで［**Windows コンポーネントの追加/削除**］をクリックします。
4. Windows コンポーネントページのコンポーネントボックスで、［**アプリケーションサーバー/インターネットインフォメーションサービス (IIS)**］＞［**次へ**］の順にクリックします。
5. インストールが完了するのを待ち、完了したらウィザードを閉じます。

Windows Server 2003 と Windows XP で IIS をインストールする場合、OS インストール用の CD が必要になることがあります。

複数の Seqrite Endpoint Security サーバーのインストール

複数の Seqrite Endpoint Security サーバーのインストールは、Seqrite Endpoint Security 独自の機能です。管理者は、以前のバージョンの Seqrite Endpoint Security がインストールされたシステムに最新バージョンをインストールできます。この機能により、管理者は簡単な方法で最新バージョンの Seqrite Endpoint Security に移行できます。

Seqrite Endpoint Security を最新バージョンにアップグレードする場合

Seqrite Endpoint Security は、以下の方法でアップグレードすることができます:

1. 以前のバージョンの Seqrite Endpoint Security がインストールされたシステムに Seqrite Endpoint Security をインストールします。
2. Seqrite Endpoint Security が以前のバージョンを検出し、次のメッセージが表示されます。

3. マルチサーバーインストールを続行するには［**はい**］をクリックします。

   最新バージョンの Seqrite Endpoint Security のインストールが完了した後、以前のバージョンの Seqrite Endpoint Security を開き、以下の手順に従います:

   i. ［**管理者設定**］>［**サーバー**］>［**リダイレクト**］を表示します。

   ii. ［**サーバー名/IP**］テキストボックスで、最新のバージョンの Seqrite Endpoint Security のサーバー名または IP アドレスを入力します。

   より新しいバージョンの EPS が DHCP ベースの IP にインストールされている場合、Seqrite はサーバイー名を使用することを推奨します。

   iii. ［ポート］テキストボックスに、最新バージョンの Endpoint Security のポート番号を入力します。

   iv. ［**適用**］をクリックします。

   これで、すべての Seqriteエンドポイントに最新バージョンの Seqrite Endpoint Security に関する通知が送信され、それらのエンドポイントは最新バージョンにリダイレクトされます。

   ネットワークに以前のバージョンの SEPS が存在する場合、最新バージョンの Seqrite Endpoint Security を確認します。検出された場合、インストールプロセスで以前のバージョンの SEPS が自動的にアンインストールされ、最新のバージョンがインストールされます。

4. すべてのエンドポイントがアップグレードされたら、以前のバージョンの Seqrite Endpoint Security サーバーをアンインストールします。

アンインストールする前に、Seqrite Endpoint Security サーバーのプロダクトキーと有効化番号をメモしておいてください。これらは、最新バージョンの Seqrite Endpoint Security を再有効化する際に必要になります。

5. 以前のバージョンの Seqrite Endpoint Security をアンインストールしたら、既存のプロダクトキーを使って最新バージョンの Seqrite Endpoint Security を再有効化します。

** すべてのエンドポイントを最新バージョンの SEPS にアップグレードできる期限は 30/60/90 日間です。デフォルトでは 60 日設定されています。この設定は、マルチサーバーモードが使用されている場合に新しいバージョンの EPS サーバーで、[管理者設定] > [サーバー] > [一般] > [マルチサーバー移行期間] から行えます。

Chapter

3

インストール後のタスク

コピーを有効にするためのインストール終了後、Seqrite Endpoint Security を速やかに登録しなければなりません。そうしないと、エンドポイントの展開が開始されません。

登録

Seqrite Endpoint Security は登録が簡単です。

オンライン登録

システムがインターネットに接続されている場合、以下の方法を使用してオンラインで Seqrite Endpoint Security を登録できます:

1. **[スタート]>[プログラム]>[Seqrite EPS コンソール]>[Seqrite EPS コンソールをアンインストールする]** の順に選択します。
2. 登録ウィザードで、プロダクトキーを入力し、[次へ] をクリックします。
3. [購入先]、[登録名]、および [名前] テキストボックスに該当する情報を入力します。
4. **[次へ]** をクリックします。
5. 個人情報（会社メールアドレス、管理者メールアドレス、連絡先番号、所在地の詳細など）を入力します。
6. **[次へ]** をクリックします。

   お客様が入力された情報の確認画面が表示されます。必要に応じて、情報を変更することができます。情報を変更するには、[**戻る**] をクリックして前の画面に戻り、必要な変更を加えます。
7. 確認するには、**[次へ]** をクリックします。

   コピーが登録され、有効にされるまで数秒かかります。このプロセスが完了するまでインターネット接続を解除しないでください。

有効化が正常に完了すると、ライセンス有効期限情報を示すメッセージが表示されます。

8. 登録ウィザードを閉じるには、[**終了**] をクリックします。

プロダクトキーは、ユーザーガイドに記載されているか、または箱の中に入っています。クレジットカードを使用してソフトウェアをオンラインで購入した場合は、プロダクトキーは受注確認メールに記載されています。

インターネット設定

登録ウィザードを開くと、直接インターネット接続が試行されます。デフォルトのインターネット接続がない場合、「**システムはインターネットに接続されていません。インターネットに接続してから、もう一度試してください。**」というメッセージが表示されます。

別の方法でインターネットに接続できる場合は、以下の手順に従ってインターネットに接続し、オンラインで登録します:

1. [**インターネット設定**] ボタンをクリックします。

   [プロキシ設定を構成する] 画面が表示されます。

2. インターネットのプロキシ設定を行うには、[**プロキシ設定を有効にする**] を選択します。

   プロキシ設定の詳細が有効になります。

3. [サーバー] テキストボックスに、サーバー名を入力します。
4. [ポート] テキストボックスに、ポート番号を入力します。

   ファイアウォールまたはプロキシサーバーを使用する場合、認証ルールも入力できます。この場合、[認証] セクションにユーザー名とパスワードを入力します。

5. 設定を保存するには、[OK] をクリックします。
6. [**インターネット接続の再試行**] をクリックします。

インターネットに接続されている場合は、オンラインで製品の登録を行うことができます。

再有効化

このセクションには、以下の項目が含まれています:

Seqrite Endpoint Security の再有効化

再有効化機能は、お客様にご購入いただいた製品をライセンス有効期限が終了するまで確実にお使いいただけるようにするための機能です。Seqrite Endpoint Security をアンインストールされ長けれども再度インストールする場合、または別のエンドポイント

に Seqrite Endpoint Security をインストールする場合。このような場合、Seqrite Endpoint Security を再有効化しなければなりません。

再有効化プロセスは有効化プロセスと似ていますが、個人情報を再度すべて入力する必要がないという点が異なります。プロダクトキーを送信すると、詳細な情報が表示されます。詳細を確認し、プロセスを終了します。

アップデートマネージャの設定

アップデートマネージャは Seqrite Endpoint Security に統合されたツールです。このツールは Seqrite Endpoint Security のアップデートのダウンロードと管理に使われます。アップデートマネージャは柔軟性があり、アップデートを任意のエンドポイントにダウンロードできます。すべての Seqrite Endpoint Security クライアントはアップデートをこの集中管理された場所から取り込みます。アップデートマネージャは機能強化またはバグ修正のために自動的に Seqrite Endpoint Security をアップデートします。

アップデートマネージャへのアクセス

アップデートマネージャを開くには、**[スタート]>[プログラム]>[Seqrite EPS Console]>[アップデートマネージャ] の順に選択します。**

アップデートマネージャの機能

アップデートマネージャには以下の機能があります:

- ステータス
- 設定
- 接続設定
- レポート

ステータス

[ステータス] には、アップデートマネージャがダウンロードした最新のアップデートに関する情報が表示されます。Endpoint Seqrite Security の製品バージョン、サービスパック、およびウイルスデータベースの日付を表示します。

設定

アップデートマネージャをカスタマイズおよび設定できます。

[設定] セクションを表示するには、以下の手順に従ってください:

1. **[スタート]>[プログラム]>[Seqrite EPS コンソール] >[アップデートマネージャ]** の順に選択します。
2. **[設定]** をクリックします。

3. スーパー管理者パスワードを入力して、[OK] をクリックします。
4. アップデートを自動的に取得するには、[**自動アップデートを有効にする**] チェックボックスを選択します。

   本機能はデフォルトで有効になっています。Seqrite では本機能を無効にしないことをお勧めします。
5. 以下のオプションからアップデートモードを選択します:
   - **インターネットセンター:**お使いのシステムにデフォルトのインターネットセンターからアップデートをダウンロードします。
   - **特定の URL:**エンドポイントは、接続されたシステムでダウンロードされたアップデートのある特定のエンドポイントからアップデートを取得します。
     - [サーバー] テキストボックスに URL を入力します。
     - [ポート] テキストボックスに、ポート番号を入力します。

     インターネット接続でシステムにアップデートする場所には、msg32.htm ファイルが存在する必要があります。

     msg32.htm ファイルを作成するには、テキストファイル名を msg32.htm ファイルに変更します。
   - **指定されたパス:**インターネット接続無しにお使いにコンピューターで特定のローカルフォルダーからアップデートを取得します。アップデートがコピーされる場所からローカルフォルダーのパスを指定できます。

     例えば、他のシステムにダウンロードしたアップデートがある場合、それを CD/DVD またはペンドライブにコピーしてローカルフォルダに貼り付けることができます。そうすると、アップデートマネージャがそのローカルフォルダのパスからアップデートを取り込みます。

     i. [**指定されたパスから選択**] オプションを選択します。

     ii. アップデートをコピーしなければならない場所からフォルダのパスを入力または参照します。
6. [**Seqrite Endpoint Security サービスパックのダウンロード**] チェックボックスを選択します。本機能はデフォルトで有効になっています。
7. ダウンロード速度を制限したい場合は、[**ダウンロード速度を制限する (キロビット/秒)**] チェックボックスを選択します。テキストボックスに速度を入力します。
8. [**アップデートのダウンロード先**] ボックスに記載されたパスを確認します。すべての Seqrite Endpoint Security 製品は、アップデートをこの集中管理された場所から取り込みます。
9. 以下のチェックボックスを選択します:

- **新しいアップデートをダウンロードする前に常にバックアップを作成する:**既存のアップデートのバックアップを作成してから、新しいアップデートをダウンロードします。このバックアップは、前回のアップデートへのロールバックが必要な場合に使用します。本機能はデフォルトで有効になっています。
- **レポートを削除するまでの日数:**選択された時間間隔に従ってレポートを削除します。本機能はデフォルトで有効になっています。初期設定の同期間隔は、10日です。

10. Seqrite Endpoint Security 設定への不正アクセスを防ぐために、パスワード保護を有効にしなければなりません。[**パスワード保護を有効にする**] チェックボックスを選択します。パスワードを入力して [OK] をクリックします。
11. 変更を保存するには、[**適用**] をクリックします。確認ダイアログボックスで [**はい**] をクリックします。

初期設定を復元するには、[**初期設定**] ボタンをクリックします。

以下の 2 つのボタンがいつでも使用できます:

- 今すぐ更新
- ロールバック

欄	定義
今すぐ更新	Seqrite Endpoint Security のアップデートをダウンロードします。
ロールバック	アップデートマネージャを前回のアップデート状態にロールバックします。最新のアップデートが削除されます。この機能は、アップデートマネージャの設定セクションで [**新しいアップデートをダウンロードする前に常にバックアップを作成する**] オプションが選択されている場合のみ使用できます。アップデートマネージャをロールバックする手順は以下の通りです: • [**ロールバック**] ボタンをクリックします。 Endpoint Security 用の Seqrite 製品が表示されます。 • ロールバックする製品を確認してから、表示された画面で [**ロールバック**] ボタンをクリックします。[**閉じる**] をクリックしてダイアログを終了することもできます。

アップデートマネージャのスケジュールスキャン

スケジュールスキャンを使用して、特定の頻度でアップデートマネージャのアップデートスケジュールを定義できます。

アップデートマネージャスケジュールスキャンを設定するには、以下の手順に従ってください:

1. **[スタート]**>**[プログラム]**>**[Seqrite EPS コンソール]** >**[アップデートマネージャ]** の順に選択します。
2. **[設定]** をクリックします。
3. スーパー管理者パスワードを入力して、**[OK]** をクリックします。
4. **[設定]** をクリックします。

   [アップデートマネージャスケジューラ] ダイアログが表示されます。
5. **カスタム**オプションを選択して以下のオプションを設定します:
   i. **[頻度]** で、[毎日] または [毎週] オプションを選択します。
   毎週オプションを選択した場合、リストから毎日を選択します。
   ii. **[開始時刻]** で、時刻を時間と分で設定します。
   iii. アップデートマネージャのスキャンを繰り返したい場合、**[アップデートを繰り返す]** チェックボックスを選択して、スキャンを繰り返す日にちを設定します。
6. **[適用]** をクリックします。

接続設定

ネットワークでプロキシサーバーが使用されている場合、[接続設定] にプロキシサーバーの IP アドレス（またはドメイン）およびポート番号を指定する必要があります。

[接続設定] セクションを表示するには、以下の手順に従ってください:

1. **[スタート]**>**[プログラム]**>**[Seqrite EPS コンソール]** >**[アップデートマネージャ]** の順に選択します。
2. **[接続設定]** をクリックします。
3. [**パスワード**] ボックスにスーパー管理者パスワードを入力して、**[OK]** をクリックします。[接続設定] ページが表示されます。
4. HTTP プロキシ設定を有効にするには、以下の手順に従ってください:
   i. **接続タイプ**リストで HTTP を選択します。
   ii. **[プロキシを有効にする]** チェックボックスを選択します。
   iii. リストから**プロキシタイプ**を選択します。
   iv. **[サーバー]** テキストボックスに、プロキシサーバーの IP アドレスまたはドメイン名（例えば、proxy.yourcompany.com など）を入力します。
   v. **[ポート]** テキストボックスに、プロキシサーバーのポート番号(例: 80) を入力します。

vi. 必要に応じて、 ファイアウォールまたはプロキシサーバーセクションで、［**ユーザー名**］および［**パスワード**］ボックスにログオン情報を入力します。

vii. 変更を保存するには、［**適用**］をクリックします。確認ダイアログボックスで［**はい**］をクリックします。

初期設定を復元するには、［**初期設定**］ボタンをクリックします。

レポート

［レポート］セクションには、アップデートまたはロールバック活動のログが記録されます。このレポートには、アップデートまたはロールバック活動の日付、時刻、およびステータスなどの詳細が記載されています。

レポートを表示するには、以下の手順に従ってください:

1. ［**スタート**］>［**プログラム**］>［**Seqrite EPS コンソール**］>［**アップデートマネージャ**］の順に選択します。
2. ［**レポート**］をクリックします。

レポートで以下の操作を実行できます:

欄	説明
表示	レポートを選択して［**表示**］をクリックし、ダウンロードされたアップデートまたはロールバックの詳細をすべて取得します。
削除	レポートを選択して［**削除**］をクリックし、レポートを削除します。
すべて削除	［**すべて削除**］をクリックして、セクション内のすべてのレポートを削除します。
前へ	前のレポートを表示します。
次へ	次のレポートを表示します。
別名で保存	レポートのコピーをテキスト形式でローカルコンピュータに保存します。
印刷	レポートのコピーを印刷します。
閉じる	レポートウィンドウを閉じます。

Azure または AWS クラウドマシンでのポートの設定

EPS サーバーとクライアントの間の通信を確立するためのポートを設定しなければなりません。EPS が展開されるクラウドマシンに含まれる EPS サーバーのすべてのポート、データベース、パッチサーバー、およびアップデートマネージャを許可します。

Azure または AWS マシンから以下のポートを許可します:

- EPS コンソール – 9105

- CGI - 6799
- ダウンロード - 8095
- 通信 - 5051
- MySQL - 62222
- パッチサーバー - 6201
- パッチサーバー HTTP - 3698

Seqrite Endpoint Security サーバーのアンインストール

Seqrite Endpoint Security をアンインストールすると、お使いのシステムや重要なデータがウイルスの脅威にさらされる可能性があります。Seqrite Endpoint Security をアンインストールする必要がある場合は、以下の手順に従ってください:

1. **[スタート]>[プログラム]>[Seqrite EPS コンソール]>[EPS コンソールをアンインストールする]** の順に選択します。
2. Seqrite Endpoint Security アンインストーラにより、パスワードの入力が求められます。

   [パスワード] ボックスに**スーパー管理者パスワード**を入力します。
3. **[次へ]** をクリックします。

   アンインストール後、プロダクトキーが表示されます。

   Seqrite Endpoint Security を再インストールする際に必要となる場合があるため、このプロダクトキーはメモしておいてください。[**今すぐシステムを再起動する**] を選択してすぐにシステムを再起動するか、[**後でシステムを再起動する**] を選択して後でコンピュータを再起動します。
4. Seqrite Endpoint Security のアンインストールを完了するには、**[終了]** をクリックします。

- ログインスクリプトのセットアップで、エンドポイントをインストールするスクリプトをドメインサーバーに割り当てている場合、ログインスクリプトのセットアップでスクリプトを消去してからアンインストールを続行してください。
- アンインストールを続行する前に、すべての実行中のプログラムを必ず終了してください。

Chapter

4

Seqrite Endpoint Security ダッシュボードについて

Seqrite Endpoint Security はウェブベースのグラフィカルコンソールを備えています。このコンソールではエンドポイントの現在の診断状況が表示され、すぐに対応が必要なセキュリティ状況を確認することができます。

このセクションではウェブコンソールの操作方法を説明します。

Seqrite Endpoint Security ウェブコンソールへのログオン

ウェブコンソールにログオンするには、以下の手順に従ってください:

1. **[スタート] > [プログラム] > [Seqrite EPS コンソール]** の順に選択します。

   また、以下を実行してログオンすることもできます:

   ネットワーク内にあるコンピューターのブラウザを開き、以下の一つを実行します:

   - アドレスバーで、SEPS サーバー名または IP アドレスを以下の URL フォーマットで入力します:
     - XP の場合: http://{Seqrite_Endpoint_Security_サーバー_名 または IP アドレス}/qhscan71
     - 他の OS の場合: http://{Seqrite_Endpoint_Security_サーバー_名または IP アドレス}:{ポート番号}
   - お使いのシステムが SSL を使用している場合、アドレスバーで SEPS サーバー名または IP アドレスを以下の URL フォーマットで入力します:
     - XPの場合: https://{Seqrite_Endpoint_Security_サーバー_名または IP アドレス}/qhscan71
     - 他の OS の場合: https://{Seqrite_Endpoint_Security_Server_name or IP address }:{port number}

［Seqrite Endpoint Security アカウントログイン］ウィンドウが表示されます。

2. ［**ユーザー名**］テキストボックスに**管理者**としてユーザー名を入力し、［**パスワード**］テキストボックスにスーパー管理者パスワードを入力します。
3. ［**ログイン**］ボタンをクリックします。

   ウェブコンソールが表示され、ネットワークの現在の診断状況の概要が表示されます。

ウェブコンソールパスワードのリセット

以下のいずれかの方法でウェブコンソールパスワードをリセットすることができます:

- ［パスワードを忘れた場合］リンクを使用する
- パスワードリセットツールを使用する

［パスワードを忘れた場合］リンクを使用したウェブコンソールパスワードのリセット

ウェブコンソールパスワードをリセットするには、以下の手順に従ってください:

1. ［アカウントログイン］ウィンドウで、［**パスワードを忘れた場合**］リンクをクリックします。
2. ［リセットパスワードウィンドウ］でユーザー名を入力します。
3. ［**予備のメールアドレスに送信**］ボタンをクリックして、仮パスワードを生成します。仮パスワードが登録したメール ID に送られます。
4. ［**仮パスワード**］テキストボックスで、仮パスワードを入力します。
5. ［**送信**］をクリックします。
6. 新しいウィンドウの［**新しいパスワード**］と［**パスワードの確認**］ボックスに新しいパスワードを入力して前のパスワードリセットします。
7. ［**送信**］をクリックします。

   新しいパスワードでウェブコンソールにログオンできます。

SMTP 設定が行われていない場合、ユーザーはパスワードリセットツールを使用してリセットすることができます。

パスワードリセットツールを使用したウェブコンソールパスワードのリセット

パスワードリセットツールを使用してウェブコンソールのパスワードをリセットするには、ユーザーは EPS がインストールされているマシンの管理者権限を保持していなければなりません。

ウェブコンソールパスワードをリセットするには、以下の手順に従ってください:

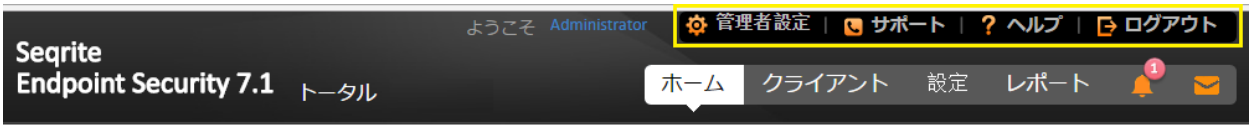
1. <インストール先>/ Admin/resetpwd.exe. を表示します。<インストール先> は、Seqrite Endpoint Security がインストールされたパスを示します。
2. resetpwd.exe ファイルを実行します。
3. [コンソールパスワードリセットツール] ウィンドウで、Windows ホスト名¥管理者ユーザーとパスワードを入力、またはドロップダウンリストで [ホスト名¥管理者] を選択することができます。
4. **[次へ]** をクリックします。
5. 新しいウィンドウの **[新しいパスワード]** と **[パスワードの確認]** ボックスに新しいパスワードを入力して前のパスワードリセットします。
6. **[パスワードを変更する]** をクリックします。

   新しいパスワードでウェブコンソールにログオンできます。

ログイン試行回数は 6 回までです。6 回ログインに失敗すると、そのユーザーアカウントは 6 時間ロックされます。

ウェブコンソールのエリア

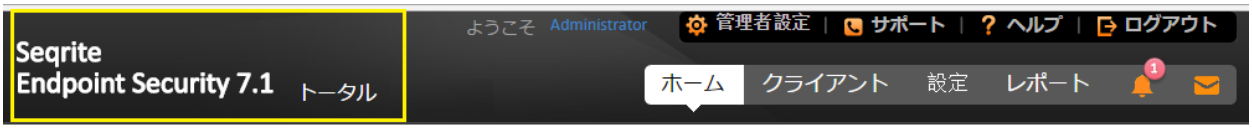
Seqrite Endpoint Security コンソールにログオンすると、デフォルトでホームページが表示されます。コンソールには、以下のようなオプションが表示されます:



黄色でハイライト表示された右上端のメニューバーには、以下のオプションが含まれます。これは全ページ共通です:

メニュー	説明
管理者設定	サーバーやエンドポイントなどの機能に関連した設定を行えます。
サポート	Seqrite が提供するすべてのサポートオプションを確認できます。
ヘルプ	すべての機能の動作および設定方法について説明するヘルプファイルがあります。
ログアウト	このボタンで現在のセッションからログアウトできます。

製品名:



[製品名] セクションには、以下の項目があります:

メニュー	説明
製品名とバージョン	製品名と現在のバージョンが表示されます。

タブ:

ウェブコンソールのユーザーインターフェースには、以下のページへのリンクも含まれます:

ページ	説明
ホーム	ホームページにアクセスできます。このページが Seqrite Endpoint Security ダッシュボードです。
クライアント	エンドポイントステータスおよびエンドポイントアクションに関連する設定を行えます。
設定	エンドポイント設定およびスケジュール設定に関連する設定を行えます。
レポート	必要なすべての機能に関するレポートを生成できます。
アラート (ベルのアイコン)	以下の重大な状況に関するアラートメッセージが表示されます: • アップデートマネージャがアップデートされていません • ライセンスが失効しました • ライセンスの上限を超えています • ライセンスの有効期限が近づいています • 新しいサービスパックが使用可能です • SMS クレジット制限が最大値に達しました。
メッセンジャー	セキュリティ情報、新しくリリースされたサービスパック、新しくリリースされた SEPS のバージョンなどに関するメッセージが表示されます。

ダッシュボードエリア

ホームページのダッシュボードエリアには、以下のウィジェットが用意されています:

概要

機能	説明
製品バージョン	製品バージョンとビルド番号が表示されます。ビルド番号はトラブルシューティングの際に役立ちます。SEPS　サービスパック情報を確認できます。ウイルスデータベースの日付も表示され、使用しているバージョンがアップデートされたものか、またはアップデートが必要かどうかを確認できます。
アップデートマネージャ	アップデートマネージャを実行するためのリンクです。詳細については、アップデートマネージャを参照してください。
ライセンスの表示	以下の項目へのリンクが表示されます: • ステータス:現行のライセンシー情報、インストール番号、プ

機能	説明
	ロダクトキー、製品タイプ、有効期限、許可された最大エンドポイント数が表示されます。 • ライセンス注文フォーム:新しい機能/ライセンスを注文するためのライセンス注文フォームを表示します。 • ライセンス履歴:ライセンス履歴の詳細を表示します。
脅威レベル	ネットワークの現在の脅威レベルを表示します。脅威レベルは次の通りです: • 正常:エンドポイントの 12 % で過去 24 時間にウイルス感染が検出されたことを示します。 • 上昇:エンドポイントの 24% で過去 24 時間にウイルス感染が検出されたことを示します。 • 高:エンドポイントの 36% で過去 24 時間にウイルス感染が検出されたことを示します。 • 致命的:36 % を超えるエンドポイントで過去 24 時間にウイルス感染が検出されたことを示します。 重要:脅威レベル警告が高または致命的になった場合、ネットワーク全体のスキャンを実行することをお勧めします。
アラート	ネットワークの健全性に対してすぐに対策が必要な場合、アラートが表示されます。[**詳細**] リンクをクリックして、すべてのアラートを確認します([詳細] リンクは複数のアラートがある場合に表示されます)。適切な対策をとり問題を解決できます。

ネットワークの健全性

機能	説明
ネットワークの健全性	ウィルスやフィッシングのカテゴリでネットワークの健全性をグラフで表示します。各タブをクリックしてカテゴリの詳細を表示します。 現在、システムがどれくらい安全かを示します。このステータスは、4 レベルのグリッドに、色付きのドットで表示されます（緑が最も低いレベル、赤が最も高いレベルというように、レベルが上昇していきます)。これらの色付きのドットは、以下の状態を示しています: • 緑（正常):エンドポイントが感染しておらず、安全であることを示します。 • 黄色（上昇):エンドポイントが低レベルで感染していることを示します。 • オレンジ（高):エンドポイントが高レベルで感染しているこ

	とを示します。すぐに対策が必要です。 • 赤（致命的):エンドポイントが致命的レベルで感染していることを示します。すぐに対策が必要です。 右側のフレームには表が表示され、主な攻撃、タイプ、影響を受けたエンドポイントの総数を確認できます。
ドロップダウンリスト表示	選択した期間のネットワークの健全性をグラフで表示します。グラフは以下の期間で確認できます: • 過去 7 日間:過去 7 日間のレポートを表示します。 • 今日:当日の感染レポートを表示します。 • 過去 15 日間:過去 15 日間のレポートを表示します。 • 過去 30 日間:過去 30 日間のレポートを表示します。
主な攻撃	コンピューターに対する主な攻撃の、攻撃名、タイプ、影響を受けたエンドポイントの数を表示します。エンドポイント数をクリックするとウィンドウが開き、実際に影響を受けたエンドポイントに関する詳細が表示されます。

ステータス

機能	説明
[ステータス]タブ	以下のカテゴリに関する情報が表示されます: • 保護 • 接続 • アップデート
保護	ネットワークに展開したエンドポイントの数、ネットワーク全体の保護されていないエンドポイントの数、およびクライアントの展開に失敗したエンドポイントの数が表示されます。
接続	システムに登録された接続の総数が、オンライン、オフライン、切断されたエンドポイントに分けて表示されます。さらに、オフラインのエンドポイント、切断されたエンドポイント、およびローミングエンドポイントに関する情報、前回コンピュータに接続された日時も表示されます。
アップデート	ウイルス定義が最新ではないエンドポイントの数が表示されます。 カテゴリの下にある数字をクリックすると、エンドポイント名、ドメイン、IP アドレス、ウイルスデータベースの日付に関する情報を確認できます。
一覧	[一覧]をクリックすると、ネットワークに接続された、保護されていないエンドポイントの一覧が生成されます。 注意:この処理には時間がかかる場合があります。該当する全エンド

	ポイント一覧へのリンクが、エンドポイント名、ドメイン名、オペレーティングシステムプラットフォーム名とともに表示されます。

セキュリティ

機能	説明
[セキュリティ] タブ	以下の対策ステータスが表示されます: • ウイルス対策 • フィッシング対策 • ブラウジング保護
ウェブセキュリティ	過去 7 日間にブロックされた主なウェブサイトカテゴリ 5 つに関する情報（グラフ）と、過去 7 日間にブロックされた主なウェブサイト 5 つの一覧（表）が、URL、タイプ、数を示すコラムとともに表示されます。 注意:この機能はオプションです。ウェブセキュリティ機能のライセンスを購入した場合のみ表示されます。詳細については、ウェブセキュリティを参照してください。
データ喪失防止	過去 7 日間にデータ漏えいが試みられた回数、漏えいを試みた主なユーザーの一覧が表示されます。 注意:この機能はオプションです。DLP 機能のライセンスを購入した場合のみ表示されます。詳細については、データ喪失防止を参照してください。
脆弱性	影響を受けたエンドポイントの数と主な脆弱性の比較一覧、重大度レベル、検出された総数が表示されます。同じデータを視覚的に表示するウィジェットも表示されます。
パッチ管理	重大度別に欠落しているパッチとインストールされているパッチの数を表示します。

遵守状況

機能	説明
高度なデバイスコントロール	過去 7 日間にポリシーに違反した主なデバイスタイプ、ポリシー違反に関わった主なユーザー 5 名の一覧が、ユーザー名、エンドポイント名、違反の数とともに表示されます。
アプリケーションコントロール	過去 7 日間にブロックされた主なアプリケーションに関する情報、ブロックされたアプリケーションへのアクセスを試みた主なユーザー 5 名の一覧が、ユーザー名、エンドポイント名、数とともに表示されます。

アセット

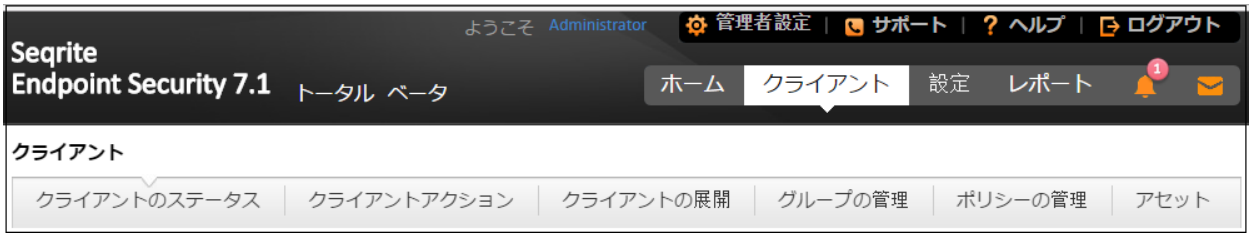
機能	説明
ハードウェア変更	Windows と Linux オペレーティングシステムのエンドポイントのみに、SEPS 7.1 エンドポイントで検出されたハードウェア変更の数が表示されます。
ソフトウェア変更	Windows と Linux オペレーティングシステムのエンドポイントのみに、SEPS 7.1 エンドポイントで検出されたソフトウェア変更の数が表示されます。
プラットフォーム	プラットフォームにインストールされたエンドポイントの総数に関する情報が表示されます。 棒グラフのコラムをクリックすると、特定のカテゴリに関連する情報が詳しく表示されます。エンドポイント IP アドレスが、インストールされたプラットフォームとともに表示されます。 注意:この機能は Windows、Linux、Mac オペレーティングシステムのエンドポイントすべてに対応します。
インストールされたソフトウェア	ソフトウェアがインストールされたエンドポイントの数が表示されます。これは棒グラフ形式でも表示されます。表示を切り替えて、インストールが最も少ないソフトウェアの数とインストールが最も多いソフトウェアの数を比較することもできます。棒グラフのコラムをクリックすると、カテゴリに関連する情報がさらに表示されます。エンドポイント IP アドレスが、ソフトウェア名とともに表示されます。この機能は Windows と Linux オペレーティングシステムのエンドポイントにのみ対応しています。

Chapter

5

クライアント

クライアントページの機能を使用して、ネットワークに展開したすべてのクライアントの管理と制御が行えます。クライアントの現在のステータスを検証し、様々な活動を実行できます。エンドポイントコンピュータのスキャン、ソフトウェアアプリケーションのアップデート、システムパフォーマンスの向上、Seqrite Endpoint Security クライアントのインストールおよびアンインストールを遠隔操作で行えます。また、エンドポイントグループの管理、スキャンポリシーの作成と適用なども行えます。



上野画面で示されているように、[クライアント] タブでは、以下の機能が提供されています:

- クライアントのステータス
- クライアントアクション
- クライアントの展開
- グループの管理
- ポリシーの管理
- アセット

[クライアントのステータス] タブ

[クライアントのステータス] タブには、ネットワーク内にある全エンドポイントの現在のステータスが表示されます。ステータスには、エンドポイント名、グループ名、ドメイン名、IP アドレスおよび MAC アドレスがあります。保護ステータス、インストールステータス、製品のバージョン、ウイルスデータベースの日付、前回スキャン日、保護ポリシー、有効になっているセキュリティ機能もタブに表示されます。

クライアントのステータスを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントステータス]** を表示します。
3. 左側のフレームの EPS コンソールの下でグループ名を選択します。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
4. エンドポイントを選択して、**[ステータスの表示]** をクリックします。

   選択したエンドポイントのステータスが表示されます。

   ステータスには［インストーラログの表示］リンクも含まれ、そのリンクから Seqrite がクライアントエンドポイントにインストールされているかどうかを確認できます。［インストーラログの表示］リンクをクリックして、クライアントの展開に失敗した理由を確認できます。

   一度に複数のエンドポイントを選択してオフラインクライアントを削除することができます。

   必要に応じて、ステータスをエクスポートまたは印刷することができます。

項目	定義
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
ステータスの表示	クライアントのステータスが表示されます。
クライアントの削除	オフラインのクライアントをグループから削除できます。
検索	エンドポイント名でクライアントを検索できます。
CSV	CSV 形式でレポートを保存できます。

［クライアントアクション］タブ

［クライアントアクション］タブにある機能を使用することで、遠隔操作によるエンドポイントのスキャン、ウイルス定義のアップデート、エンドポイントのパフォーマンス向上が可能です。ネットワーク内のエンドポイントにインストールされた無許可のアプリケーションを特定するなど、セキュリティポリシーの遵守状況を検証することもできます。

エンドポイントを個別またはグループで遠隔スキャンしたり、スキャン設定をカスタマイズしたり、自由にスキャンを停止したりできます。ディスク容量やレジストリエントリのクリーンアップ、次回起動時のスケジュールデフラグによって、エンドポイントのパフォーマンスを向上することができます。エンドポイントの SEPS ウイルスデータベースをアップデートし、エンドポイントに無許可のアプリケーションがインストールされていないかなど、セキュリティ遵守状況を検証することができます。

次の表では、クライアントアクションの機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
スキャン	✓	✓	✓
アップデート	✓	✓	✓
保存データスキャン	✓	✓	X
一次デバイスアクセス	✓	✓	X
チューンアップ	✓	X	X
アプリケーションコントロールスキャン	✓	X	X
脆弱性スキャン	✓	X	X
パッチスキャン	✓	X	X
パッチのインストール	✓	X	X

スキャン

ネットワーク内の任意のエンドポイントを遠隔スキャンできます。事前設定されたポリシーを使用して手動スキャンを開始できます。この機能により、各ターゲットエンドポイントを個別監視する追加タスクを削減することができます。

スキャンを開始するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントアクション]**>**[スキャン]** を表示します。

   すべてのグループを表示したウィンドウが開きます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
3. Endpoint Security コンソールで、グループを選択します。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
4. スキャンを開始するには、**[スキャン開始を通知する]** をクリックします。

   選択したエンドポイントの遵守状況がスキャンされます。

   必要なときにはいつでも、[スキャン停止を通知する] をクリックしてスキャンを停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。

サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
スキャン設定	スキャン設定をカスタマイズできます。
スキャン開始を通知する	クライアントにスキャンの開始を通知できます。
スキャン停止を通知する	クライアントにスキャンの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。
すべてスキャン	このボタンをシングルクリックしてすべてのエンドポイントをスキャンすることができます。

スキャン設定

この機能により、クライアントマシンのスキャン設定をカスタマイズできます。

スキャン設定を行うには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントアクション]**>**[スキャン]** を表示します。
3. ［スキャン］画面で、**[スキャン設定]** をクリックします。
4. ［スキャン設定］画面で、以下の手順を実行してください:
   i. ［スキャン方法］セクションで、［クイックスキャン］または［システム全体のスキャン］を選択します。

      ［クイックスキャン］はオペレーティングシステムがインストールされたドライブをスキャンし、［システム全体のスキャン］はすべての固定ドライブをスキャンします。
   ii. ［自動］または［高度なスキャン］のいずれかのスキャンモードをクリックします。

      自動スキャンは最適なスキャンを実行します。これはデフォルトで選択されています。
   iii. ［高度なスキャンモード］チェックボックスが選択されている場合、すべての関連する属性が有効にされます。以下の操作を実行できます:
      a. ［スキャンする項目を選択する］オプションで、スキャンするファイル、ファイルタイプ（実行可能ファイル、パックファイル、アーカイブファイル）、および受信ボックスを選択します。
      b. ［アーカイブスキャンのレベル］で、スキャンレベルを設定します。

アーカイブファイルでのスキャンレベルを設定できます。初期設定では、スキャンレベルはレベル 2 に設定されています。初期設定のスキャンレベルの数値を上げると、スキャン速度に影響を及ぼすことがあります。

c. 感染したファイルをシステムから削除するには、[アクションを選択する] タブで以下の手順を実施してください:

- 感染したファイルがシステムのアーカイブフォルダで検出された場合、そのファイルを削除、隔離、またはスキップするかを選択します。
- 感染したファイルがシステムのアクティブフォルダ/ドライブで検出された場合、そのファイルを修復、削除、またはスキップするかを選択します。

iv. [アンチマルウェアスキャン設定] で、必要に応じて**[アンチマルウェアスキャンを実行する]** を選択します。

v. [マルウェアが見つかったときに実行する処置を選択する] で、次のいずれかの処置を選択します:

- クリーニング
- スキップ

ここで選択した処置は自動的に実行されます。

vi. [ブートタイムスキャンの設定] で、**[ブートタイムスキャンを実行する]** を選択します。

[ブートタイムスキャンモードを選択] オプションが有効になります。

vii. 次のスキャンオプションの 1 つを選択してください:

- クイックスキャン
- システム全体のスキャン

ブートタイムスキャンの設定は、1 回のみ適用され、保存されません。

viii. スキャン設定を設定した後、**[適用]** をクリックします。

新しい設定が適用されます。

- パックファイルのスキャン、受信ボックスのスキャン、アンチマルウェアスキャン設定、およびブートタイムスキャン設定は、Windows オペレーティングシステムのクライアントのみで使用できます。
- SEPS ウェブコンソールからのスキャン通知は、ユーザーが Mac システムにログオンしていない場合、送信されません。
- SEPS スキャン通知は Linux オペレーティングシステムで「ext」ファイルシステムのみサポートします。

アップデート

この機能を使用して、ネットワーク内の任意のエンドポイント上のクライアントアプリケーションを遠隔操作でアップデートできます。Seqrite はアップデートを定期的にリリースして技術的な問題を修正し、新たな脅威に対する対策を提供しています。このため、定期的に保護ソフトウェアを最新のウイルス定義にアップデートすることをお勧めします。

アップデートを取得するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**クライアント**]>[**クライアントアクション**]>[**アップデート**] を表示します。

   すべてのグループを表示したウィンドウが開きます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
3. Endpoint Security コンソールで、グループを選択します。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
4. エンドポイントを選択して、[**今すぐアップデートを通知**] をクリックします。

   選択したエンドポイントが、最新のウイルス定義で更新されます。

項目	定義
最新状態の Seqrite でないエンドポイントを選択	最新状態のウイルス定義でないエンドポイントをアップデートできます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
今すぐアップデートを通知	エンドポイントに Seqrite のアップデートを通知します。
最新の情報に更新	送信された通知のステータスを更新します。
すべてをアップデート	このボタンをシングルクリックしてすべてのエンドポイントをスキャンすることができます。

SEPS ウェブコンソールからのアップデート通知は、ユーザーが Mac システムにログオンしていない場合、送信されません。

チューンアップ

この機能は、デフラグを実行し、不要なファイルや、無効または古くなったレジストリエントリを消去することで、エンドポイントのパフォーマンスを向上させます。アプリケーションでの作業時にコンピュータがドライブ上に不要なファイルを書き込んだり、ウェブサイトにアクセスしたりすると、コンピュータに一時ファイルが作成されます。このような不要なファイルはメモリ容量を占有するので、エンドポイントの動作が遅く

なります。コンピュータをチューンアップすると不要なファイルが消去され、パフォーマンスが向上します。

- チューンアップ機能は、Windows オペレーティングシステムのクライアントのみで使用できます。
- チューンアップ機能は、Windows Server オペレーティングシステムでは使用できません。

エンドポイントをチューンアップするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアントアクション]>[チューンアップ]** を表示します。

   すべてのグループを表示したウィンドウが開きます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
3. EPS コンソールで、チューンアップ処理を実行するグループを選択します。

   初期設定では、EPS コンソール下に存在するすべてのエンドポイントが表示されます。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
4. エンドポイントを選択して、**[チューンアップ開始を通知する]** をクリックします。

   チューンアップ通知が選択したエンドポイントに送信され、それらのエンドポイントに対してチューンアップが実行されます。

   必要なときにはいつでも、[チューンアップ停止を通知する] をクリックしてチューンアップ活動を停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
チューンアップ設定	チューンアップ設定をカスタマイズできます。
チューンアップ開始を通知する	クライアントにチューンアップの開始を通知できます。
チューンアップ停止を通知する	クライアントにチューンアップの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。
すべてをチューンアップ	このボタンをシングルクリックしてすべてのエンドポイントをチューンアップすることができます。

チューンアップ設定

これらの設定により、ディスク、レジストリエントリなど異なるタイプのクリーンアップを実行するか、次回起動時のデフラグをスケジュールできます。

チューンアップ設定をカスタマイズするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントアクション]**>**[チューンアップ]** を表示します。
3. [チューンアップ] 画面で、**[チューンアップ設定]** ボタンをクリックします。
4. [チューンアップ設定] ポップアップで、次のいずれかを選択します:
   - ディスクのクリーンアップ
   - レジストリのクリーンアップ
   - 次回起動時にデフラグ

   これらのオプションはすべて初期設定で選択されています。
5. 設定を保存するには、**[適用]** をクリックします。

ディスクのクリーンアップ:ハードディスクドライブから無効なファイルや不要なファイルを見つけて削除します。これらのファイルは、ハードディスクの空き容量を占有するとともに、システム速度を大幅に低下させます。ディスククリーンアップは、これらのファイルを削除することによって、他のアプリケーションに使用する空き容量を確保し、システムパフォーマンスを向上させます。この機能は、一時ファイル、インターネットキャッシュファイル、不適切なショートカットファイル、無効な名称のファイル、空のフォルダも削除します。

レジストリのクリーンアップ:適切に実行されなかったアンインストールや存在しないフォント等によって表示される可能性にある、無効または古くなったレジストリエントリをシステムから削除します。しかし、アンインストール時に、これらのレジストリエントリは削除されないことがあります。そのため、システムパフォーマンスが遅くなることがあります。レジストリのクリーンアップは、このような無効なレジストリエントリを削除し、システムパフォーマンスを向上させます。

デフラグ:システムのパフォーマンスを向上させるために、ページファイルやレジストリハイブ等の重要なファイルのデフラグを行います。ファイルはフラグメント（断片）としてばらばらな場所に保管されることが多いため、システムパフォーマンスの低下につながります。デフラグはフラグメント数を減らし、すべてのフラグメントを 1 つの連続した塊にまとめることでシステムパフォーマンスの向上を実現します。

アプリケーションコントロールスキャン

組織により構成されたセキュリティコンプライアンスポリシーが、各エンドポイントで遵守されているかどうかを確認できます。また、実行が許可されたアプリケーション以

外の無許可のアプリケーションをエンドポイントが実行しているかどうかを検証できます。

アプリケーションコントロールスキャン機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

コンプライアンス管理のためにエンドポイントをスキャンするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアントアクション]>[アプリケーションコントロール]** を表示します。

   すべてのグループを表示したウィンドウが開きます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
3. Endpoint Security コンソールで、グループを選択します。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
4. [スキャン設定] ボタンで、スキャン設定を選択します。
5. エンドポイントを選択して、**[スキャン開始を通知する]** をクリックします。

   選択したエンドポイントの遵守状況がスキャンされます。

   必要なときにはいつでも、[スキャン停止を通知する] をクリックしてスキャンを停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
スキャン設定	アプリケーション管理のためにスキャン設定をカスタマイズできます。
スキャン開始を通知する	クライアントにスキャンの開始を通知できます。
スキャン停止を通知する	クライアントにスキャンの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。
すべてスキャン	このボタンをシングルクリックしてすべてのエンドポイントをスキャンすることができます。

スキャン設定

スキャンの環境設定のカスタマイズができます。

スキャン設定をカスタマイズするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントアクション]**>**[アプリケーションコントロール]** を表示します。
3. [アプリケーションコントロールスキャン] 画面で［**スキャン設定**］ボタンをクリックして以下のいずれか一つを選択します:
   - **無許可アプリケーション**:クライアントマシンに存在する無許可アプリケーションのみに対してスキャンを開始します。
   - **無許可および許可アプリケーション**:クライアントマシンに存在する無許可および許可アプリケーション両方に対してスキャンを開始します。
   - **インストール済みのすべてのアプリケーション**:クライアントにインストールされたすべてのプリケーション対してスキャンを開始します。

   アプリケーションコントロールスキャンには、いずれかのオプションを選択できます。

   最初の 2 つのオプションによるスキャンは、時間がかかることがあります。
4. 設定を保存するには、**[適用]** をクリックします。

脆弱性スキャン

ネットワーク内のエンドポイントにインストールされた様々なベンダー（Adobe、Apple、Mozilla、Oracle など）のアプリケーション、およびオペレーティングシステムの既知の脆弱性をスキャンして、セキュリティステータスを評価できます。エンドポイントのアプリケーションおよびオペレーティングシステムのパッチで潜在的な脆弱性を検証することができます。これにより、既知の脆弱性に対してセキュリティ対策を策定し、データ障害からエンドポイントを保護できます。

脆弱性スキャンを有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントアクション]**>**[脆弱性スキャン]** を表示します。
3. [脆弱性スキャン] ページで、**[スキャン設定]** ボタンをクリックします。

   [スキャン設定] ダイアログが開きます。
4. [次のソフトウェアベンダーの脆弱性をスキャンします] で、次のいずれかを選択します:
   - Microsoft アプリケーションおよびその他のベンダーのアプリケーション
   - Microsoft アプリケーションのみ
   - その他のベンダーのアプリケーションのみ
5. 設定を保存するには、**[適用]** をクリックします。

必要なときにはいつでも、[スキャン停止を通知する] をクリックしてスキャンを停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
スキャン設定	脆弱性スキャンのためにスキャン設定をカスタマイズできます。
スキャン開始を通知する	クライアントにスキャンの開始を通知できます。
スキャン停止を通知する	クライアントにスキャンの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。
すべてスキャン	このボタンをシングルクリックしてすべてのエンドポイントをスキャンすることができます。

保存データスキャン

保存データスキャンを使用して、エンドポイントやリムーバブルデバイスにある機密データのスキャンや検出を行うことができます。エンドポイントのドライブやフォルダ、リムーバブルデバイスなど希望する場所をスキャンして機密情報を検出し、検出された機密データに関する情報（ファイルパスや脅威タイプ、一致したテキストなど）を確認できます。

保存データスキャンを実施するには、エンドポイントで DLP を有効にしなければなりません。エンドポイントで DLP を有効にするには、DLP 機能の有効化を参照してください。

スキャン設定

保存データスキャンを有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアントアクション]>[保存データスキャン]** を表示します。
3. スキャンするまたはデフォルトリストで選択したエンドポイント名または IP アドレスを入力します。

   特定のグループからエンドポイントを選択することもできます。

サブグループ内のオフラインクライアントまたはエンドポイント、あるいはその両方を選択したい場合、ページの最後にある必要なチェックボックスを選択することもできます。

4. ［**スキャン設定**］ボタンをクリックして、以下のオプションの一つを選択します:
   - **クイックスキャン**:このオプションを選択してオペレーティングシステムがインストールされているドライブをスキャンします。
   - **システム全体**:このオプションを選択してすべてのドライブをスキャンします。
   - **特定のフォルダをスキャン:**このオプションを選択して特定のフォルダをスキャンします。
     i. ［**設定**］をクリックします。
     ii. スキャンするフォルダのパスを指定します。

     ［**サブフォルダを含める**］チェックボックスを選択してサブフォルダのスキャンを選択することもできます。
     iii. ［**追加**］をクリックします。

     ［**削除**］をクリックしてリストからパスを削除することもできます。
     iv. ［**適用**］をクリックします。
5. ［ファイルタイプ］リストで、データを検索するファイルフォーマットを選択します。
6. スキャンするデータタイプに対し、**機密データ**または**ユーザー定義辞書**、あるいはその両方を選択します。
7. ［**適用**］をクリックします。

［**キャンセル**］をクリックしてダイアログボックスを閉じ、［**デフォルト**］をクリックして選択されているすべてのチェックボックスのチェックを外します。

- 保存データスキャン機能は Windows 2000 オペレーティングシステムでは使用できません。
- メール通知は保存データスキャン機能でサポートされていません。
- DLP 機能パックが EPS サーバーで有効にされている場合のみ、保存データスキャン機能は利用できます。

必要なときにはいつでも、［スキャン停止を通知する］をクリックしてスキャンを停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。

スキャン設定	保存データスキャンのためにスキャン設定をカスタマイズできます。
スキャン開始を通知する	クライアントにスキャンの開始を通知できます。
スキャン停止を通知する	クライアントにスキャンの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。
すべてスキャン	このボタンをシングルクリックしてすべてのエンドポイントをスキャンすることができます。

除外

スキャンするパスを除外または含めることも可能です。

- パスを除外するには、テキストボックスにパスを入力して［**追加**］をクリックします。
- パスを含めるには、テキストボックスにパスを入力して［**削除**］をクリックします。

パッチスキャン

この機能を使用して、ネットワークで欠落しているパッチをスキャンすることができます。

パッチスキャンを有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**クライアント**］>［**クライアントアクション**］>［**パッチのスキャン**］を表示します。
3. ［**スキャン設定**］ボタンをクリックして、以下のオプションの一つを選択します:
   - オンライン（推奨）

     欠落しているパッチをスキャンしている時に、クライアントがパッチサーバーから最新のデータにアクセスします。
   - オフライン

     欠落しているパッチをスキャンしている時に、クライアントがローカルシステムからデータにアクセスします。
4. ［**適用**］をクリックします。
5. スキャンするまたはデフォルトリストで選択したエンドポイント名または IP アドレスを入力します。

   特定のグループからエンドポイントを選択することもできます。

サブグループ内のオフラインクライアントまたはエンドポイント、あるいはその両方を選択したい場合、ページの最後にある必要なチェックボックスを選択することもできます。

6. エンドポイントを選択して、**[スキャン開始を通知する]** をクリックします。

   欠落しているパッチがないか選択したエンドポイントをスキャンします。

Seqrite は、最適なパフォーマンスを実現するために、パッチスキャンにエンドポイントを 100 個同時に選択することを推奨します。

必要なときにはいつでも、**[スキャン停止を通知する]** をクリックしてスキャンを停止することができます。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
スキャン設定	パッチスキャンのスキャン設定をカスタマイズできます。
スキャン開始を通知する	クライアントにスキャンの開始を通知できます。
スキャン停止を通知する	クライアントにスキャンの停止を通知できます。
最新の情報に更新	送信された通知のステータスを更新します。

パッチのインストール

この機能を使用して、選択したエンドポイントで欠落しているパッチをインストールすることができます。

欠落しているパッチをインストールするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント] > [クライアントアクション] > [パッチのインストール]** を表示します。[パッチのインストール] ページが表示されます。欠落しているパッチのリストが表示されます。
3. 以下の表に記載されている 4 つのフィルターを利用してこのリストにフィルタをかけることができます。

   重大度オプション:

重大度	説明
致命的	脆弱性によりユーザーインタラクションなしにコードが実行されます。
重要	脆弱性により、ユーザーデータの機密性、完全性、または利用可能性が侵害される恐れがあります。プロンプトの起源や品質、ユーザビリティに関わらず、警告やプロンプトがクライアントに表示されます。
中	脆弱性の影響は、認証要件や非デフォルト設定のみへの適用といった要素により、かなり軽減されます。
低	脆弱性の影響は、影響を受けたコンポーネントの性質により全面的に軽減されます。
指定されていない	脆弱性は偶発的な不具合となる可能性があります。

カテゴリオプション:

カテゴリ	説明
セキュリティアップデート	製品特有のセキュリティに関する脆弱性に対し広範囲にリリースされる修正プログラム。セキュリティの脆弱性は重大度で評価されます。Microsoft セキュリティ掲示板では、重大度の評価が致命的、重要、中、低で示されています。
アップデートのロールアップ	容易に展開できるようパッケージに含まれているホットフィックスやセキュリティアップデート、アップデートのテスト済みの累積セット。ロールアップは通常、セキュリティなどの特定の場所、またはインターネットインフォメーションサービス（IIS）などの製品のコンポーネントを対象とします。
アプリケーション	アプリケーション（ソフトウェア）は、ユーザーが実行するタスクのために、コンピューターの能力を直接的に十分活用するコンピューターソフトウェアのサブクラスです。
サービスパック	すべてのホットフィックス、セキュリティアップデート、重要なアップデート、およびアップデートのテスト済みの累積セット。また、サービスパックには、製品のリリース後に内部的に検出された問題の追加修正プログラムが含まれていることがあります。サービスパックには、カスタマーから要求された設計変更や機能が限定された数だけ含まれていることもあります。

機能パック	製品リリースで含まれていなかった機能として初めて配布され、通常次の製品リリース時に含まれる新しい製品機能。
アップデート	アップデートは、実行可能な解決策のない重要な問題を抱えている個々の顧客に提供されるコード修正です。
定義のアップデート	製品の定義データベースへの追加定義が含まれる広範かつ頻繁にリリースされるソフトウェアアップデート。定義データベースは、悪質なコードやフィッシングウェブサイト、ジャンクメールなど特定の属性を持つオブジェクトを検出するために通常使用されます。
重要なアップデート	セキュリティに関連しない重要なバグに対処するために特定の問題に対して広範にリリースされる修正プログラム。
ドライバ	デバイスの入出力を制御するソフトウェア。

必須オプションの再起動:

必要な再起動	説明
すべて	すべてのオプションの結果を表示します。
オプション	このパッチではシステムを再起動する必要がありません。
必須	このパッチではシステムを再起動しなければなりません。システムを再起動してパッチを有効にします。
必要な場合あり	このパッチではシステムを再起動する可能性があります。

EULA ステータスオプション:

EULA ステータス	説明
すべて	「同意する」と「同意しない」オプションの結果を表示します。
同意する	エンドユーザー使用許諾契約書に同意します。
同意しない	エンドユーザー使用許諾契約書に同意しません。

特定の結果を得るためにエンドポイント名またはアプリケーション名を指定することもできます。KB ID または掲示板 ID を入力してパッチを検索することができます。

フィルターと記録の詳細またはそのいずれかを使用して結果を得るには、[**生成**]をクリックします。

4. ［**サブグループ内のパッチを表示**］チェックボックスを選択して、ネットワークを検索することなく、エンドポイントのリストからサブグループにあるパッチ名を表示します。
5. 再起動設定を変更するには、［**システム再起動設定**］ボタンをクリックします。パッチでシステムの再起動が必要な場合のみ、再起動設定を適用できます。
6. ［**システムの自動再起動を許可する**］チェックボックスを選択して、自動的にシステムを再起動します。チェックボックスを外して、システムを手動で再起動します。
7. 欠落しているパッチリストで、インストールするパッチを選択します。
   i. リストの［**影響を受けたエンドポイントの番号**］欄で番号をクリックします。［影響を受けたエンドポイント］ダイアログが表示されます。
   ii. 欠落しているパッチをインストールするエンドポイントを選択します。
   iii. ［**適用**］をクリックします。エンドポイントのリストが保存されます。
8. ［**インストールを開始**］をクリックします。選択を解除するには、［**更新**］をクリックします。
9. パッチのインストールからエンドポイントを除外するには、［**ここをクリック**］リンクをクリックします。［パッチインストールの除外］ダイアログが表示されます。
10. 必要に応じて、［**EPS ネットワークでサーバー OS のあるエンドポイントを除外する**］チェックボックスを選択します。
11. ［**以下のエンドポイントを除外する**］チェックボックスを選択します。
12. 特定のエンドポイントを除外するには、エンドポイント名または IP を入力して［**追加**］をクリックします。
13. ［**適用**］をクリックします。

    除外を削除するには、エンドポイントを選択して［**削除**］をクリックします。

一次デバイスアクセス

この機能を使用して、特定期間クライアントのデバイスに一時的にアクセスすることができます。ユーザーがクライアントのデバイスに一時的にアクセスしたい場合、そのユーザーは管理者に一時アクセス要求を送信することができます。OTP が生成され、共有されます。クライアントはその OTP を使用して特定の期間デバイスにアクセスします。

一次デバイスアクセス機能を有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**クライアント**］>［**クライアントアクション**］>［**一次デバイスアクセス**］を表示します。
3. ［一次デバイスアクセス］ページで、一時アクセスが必要なエンドポイントクライアントを選択します。一度に1 つのエンドポイントのみ選択できます。

4. **[一次デバイスアクセスを許可する]** をクリックします。[OTP の生成] ダイアログが表示されます。
5. **[一次アクセスを許可する時間]** リストで分を選択します。
6. **[OTP の使用時間]** リストで分を選択します。
7. **[生成]** をクリックします。OTP が表示されます。クライアントがオンラインの場合、[**通知**] をクリックすると、クライアントが自動的に OTP を受信します。その時に有効にされた設定ごとに一次アクセスが許可されます。
8. クライアントがオフラインまたはローミング中の場合、通知は無効にされます。メールを使用して OTP を手動でクライアントに送信するには、以下を実行します:
   i. **[メールで通知]** をクリックします。[メール] ダイアログが表示されます。
   ii. **[宛先]** テキストボックスにメール ID を入力します。
   iii. **[メールを送信]** をクリックします。システムのデフォルトメールクライアントが、OTP の詳細を指定してメールを開き、表示します。
   iv. **[送信]** をクリックします。

クライアント側で、OTP が正常に確認された後、一時デバイスアクセスが特定期間有効にされます。

Chapter

6

クライアントの展開

[クライアント] ページの [クライアントの展開] タブで Endpoint Security クライアントを展開できます。

該当する場合、以下の方法の一つを選択して Endpoint Security クライアントを展開します。各方法の説明を以下に記載します。

- Active Directory 経由:Active Directory グループと同期して、エンドポイントセキュリティクライアントを展開します。
- リモートインストール:エンドポイントセキュリティクライアントをリモートからインストールします。
- インストールの通知:クライアントインストールの URL を含んだメール通知を送信します。
- クライアントパッケージャ:手動インストールのためのクライアントインストーラを作成します。
- ログインスクリプト:クライアントインストール用のログインスクリプトを割り当てます。
- ディスクイメージング:エンドポイントセキュリティクライアントをイメージングから展開します。

次の表は、クライアントの展開方法に関する各種オペレーティングシステムのサポートを示します:

機能	クライアント		
	Windows	Mac	Linux
Active Directory 経由	✓	X	X
リモートインストール	✓	✓	X
インストールの通知	✓	✓	X
クライアントパッケージャ	✓	✓	✓

ログインスクリプト	✓	X	X
ディスクイメージング	✓	X	X
リモートアンインストール	✓	✓	✓

Active Directory 経由

この機能を使用して、SEPS サーバーを Active Directory グループと同期することができます。グループが同期されると、ドメインネットワーク下のすべてのエンドポイントにクライアントがインストールされます。定期的なチェックを実行し、ネットワークに新しいエンドポイントが追加されたかを検出します。新しいエンドポイントが追加された場合、そのエンドポイントに自動的にクライアントがインストールされます。

Active Directory グループから特定のエンドポイントを除外して、クライアントがこれらのエンドポイントにインストールされないようにすることもできます。

- このインストール方法は、Microsoft Windows オペレーティングシステムのみで使用できます。
- サーバーを Active Directory と同期するには、コンソールがドメインマシンにインストールされているか、ドメインの一員である必要があります。
- 同期は、Default グループに対しては実行できません。
- 赤色で表示されるグループは、Active Directory とすでに同期されています。
- Active Directory と同期するには、ドメイン管理者の許可が必要です。
- 初期設定の同期間隔は、GLOBAL です。

Active Directory と同期

Active Directory グループと同期するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアント展開]>[Active Directory 経由]** を表示します。

   すべてのグループが表示されたウィンドウが開きます。
3. Endpoint Security コンソールで、グループを選択します。

   すでに同期している場合、右側のフレームに、選択したグループの Active Directory コンテナおよび同期間隔が表示されます。
4. グループを右クリックして、**[Active Directory と同期]** を選択します。

   [ドメインを選択してください] 画面が表示されます。
5. ドメインを選択して、**[次へ]** をクリックします。

認証画面が表示されます。

6. 「ドメイン名/ユーザー名」の形式でユーザー名を指定し、有効なパスワードを入力して、**[次へ]** をクリックします。

   [Active Directory コンテナの選択] 画面が表示されます。

7. **ドメイン名**、または**同期する Active Directory コンテナ**を選択します。

   ドメイン名を選択すると、Active Directory 全体が同期され、任意の Active Directory コンテナを選択すると、選択したコンテナのみが同期されます。

8. **[次へ]** をクリックします。

   [同期] 画面が表示されます。

9. [同期間隔] に、このグループに対して実行する定期的なチェックの時間間隔を入力して、**[終了]** をクリックします。

   時間は、1 ～ 24 時間で指定する必要があります。

   SEPS サーバーは、指定された間隔に従って Active Directory と同期されます。

同期の編集

この機能により、定期的なチェックを実行する時間間隔を柔軟に編集して、ネットワークに新しいエンドポイントが追加されたかを検出できます。

チェックの頻度は、新しいエンドポイントの追加される数と頻度によって変更できます。

時間間隔を編集するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアント展開]**>**[Active Directory 経由]** を表示します。

   すべてのグループが表示されたウィンドウが開きます。

3. EPS コンソールで、同期済みのグループを右クリックして、**[同期の編集]** をクリックします。

   Active Directory との同期に対する認証画面が表示されます。

4. パスワードを入力し、**[次へ]** をクリックします。

   [同期] 画面が表示されます。

5. [同期間隔] テキストボックスに、時間間隔を入力します。

   時間は、1 ～ 24 時間で指定する必要があります。

6. 新しい設定を保存するには、**[終了]** をクリックします。

   新しい同期設定が正常に保存されます。

同期の削除

この機能を使用すると、以下の方法によりグループの同期を削除できます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアント展開]**>**[Active Directory 経由]** を表示します。

   すべてのグループが表示されたウィンドウが開きます。
3. EPS コンソールで、同期済みのグループを右クリックして、**[同期の削除]** をクリックします。

   選択したグループの同期が正常に削除されます。

除外

Active Directory が同期されると、EPS クライアントのインストールからエンドポイントを除外できます。EPS クライアントは除外されたエンドポイントにインストールされません。エンドポイントは、ホスト名、IP アドレス、または IP 範囲によって除外できます。

エンドポイントを除外するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアント展開]**>**[Active Directory 経由]** を表示します。
3. [Active Directory 経由] ページで、**[除外]** ボタンをクリックします。

   エンドポイントを除外する方法に関するオプションのポップアップが表示されます。
4. [エンドポイントの除外] 画面で、次のうちの 1 つを選択します:
   - **ホスト名で除外**:このオプションを選択した場合は、**ホスト名**を入力して、**[追加]** をクリックします。エンドポイントが、[除外されるワークステーション] リストに追加されます。
   - **IP アドレスで除外**:このオプションを選択した場合は、**IP アドレス**を入力して、**[追加]** をクリックします。エンドポイントが、[除外されるワークステーション] リストに追加されます。
   - **IP 範囲で除外**:このオプションを選択した場合は、**開始 IP アドレス**と**終了 IP アドレス**を入力して、**[追加]** をクリックします。エンドポイントが、[除外されるエンドポイント] リストに追加されます。
5. 設定を保存するには、**[保存]** をクリックします。

必要な場合いつでも、除外リストからエンドポイントを削除できます。

リモートインストール

この機能を使用して、Seqrite クライアントを、サポートされるすべての Windows オペレーティングシステム（OS）に展開できます。 Seqrite クライアントを複数のエンドポイントに同時にインストールすることもできます。リモートインストールを続行する前に、次の要件および変更を確認することをお勧めします:

例外ルール

- Windows Vista 以降のオペレーティングシステムでは、リモートインストールは「ビルトイン管理者」アカウントでのみ可能です。Windows Vista（またはそれ以上）を実行しているエンドポイントで「ビルトイン管理者アカウント」を有効にするには、以下の手順に従ってください:
  1. 管理モードでコマンドプロンプトを開きます。
  2. 「net user administrator/active:yes」と入力して、**[入力]** を押します。
  3. **[コントロール パネル]**>**[ユーザーアカウント]** から、「ビルトイン管理者」のパスワードを変更します。
- Windows XP Professional Edition への Seqrite Endpoint Security クライアントのリモートインストールについては、以下の手順に従ってください:
  1. ［マイコンピュータ］を開きます。
  2. **[ツール]**>**[フォルダ]** を表示します。
  3. ［表示］タブをクリックします。
  4. **[簡易ファイルの共有を使用する]** オプションを無効にします。
  5. **[適用]** をクリックして、**[OK]** をクリックします。
- Seqrite のリモートインストールは、Windows XP Home Edition ではサポートされていません。Seqrite クライアントを Windows XP Home Edition にインストールするには、Seqrite Endpoint Security で提供される他のインストール方法（インストールの通知、ログインスクリプト、クライアントパッケージャなど）を使用できます。
- Windows XP 以上のオペレーティングシステムでユーザーのパスワードが設定されていない場合、リモートインストールはサポートされません。
- ドメインコントローラ下のシステムに Seqrite クライアントをインストールするには、「ドメイン名¥ユーザー名」の形式でユーザー名を指定してください。「ドメイン名」はドメインコントローラの名前であり、「ユーザー名」はドメイン管理者の名前です。

リモートインストールについては、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]**>**[クライアントの展開]**>**[リモートインストール]** を表示します。

   [リモートインストール] ページが開きます。
3. 以下のいずれかの方法でリモートインストールを起動できます:
   - コンピュータごとのリモートインストール

   i. [ネットワークプレース] で、エンドポイントを選択して、**[追加]** をクリックします。複数のエンドポイントを選択できます。コンピュータの検索ユーティリティでエンドポイントを検索することもできます。

   ネットワーク内の任意のエンドポイントを、ネットワークを列挙することなく検索できます。

   エンドポイントを追加するには、管理者権限のあるターゲットエンドポイントのユーザー認証情報を提供する必要があります。

   ii. [ネットワークパスワードを入力してください] ダイアログで、ターゲットエンドポイントのユーザー認証情報を入力して、**[OK]** をクリックします。

   これらの手順を選択したエンドポイントすべてに繰り返します。

   入力したユーザー認証情報が正しいと、ターゲットエンドポイントが [保護対象として選択されたエンドポイント] リストに表示されます。

   この場合、エンドポイントのユーザー認証情報を忘れた、または誤ったユーザー認証情報を指定した場合、[スキップ] ボタンをクリックして次のエンドポイントに進み、ユーザー認証情報を指定することができます。

   - IP アドレスによるリモートインストール

   i. **[IP アドレスによって追加]** ボタンをクリックします ([ネットワークプレース] リストからコンピュータを選択する必要はありません)。

   ii. [IP アドレスによってコンピュータを追加] ダイアログで、次のいずれかのオプションを選択します:
      - **IP アドレス範囲によって追加**:このオプションを選択すると、開始 IP アドレスオプションおよび終了 IP アドレスオプションで IP アドレスの範囲を指定する必要があります。これは、連続した IP アドレスの範囲で使用できる多数のエンドポイントに 1 回で Seqrite クライアントをインストールする場合に便利です。
      - **IP アドレスによる追加**:このオプションを選択した場合、ターゲットエンドポイントの IP アドレスを指定する必要があります。
4. IP アドレスを入力してから、**[次へ]** をクリックします。

   クライアントをインストールするすべてのエンドポイントに対して、ユーザーアカウントオプションを使用してユーザー認証情報を入力する必要があります。

5. ［IP アドレスによるコンピュータを追加］の［ユーザーアカウント］で、**［追加］**をクリックします。

   ［ユーザーの追加］ダイアログが開きます。

6. ［ユーザーの追加］ダイアログで、ユーザー認証情報を入力して、**［OK］**をクリックします。

   クライアントをインストールするすべてのコンピュータに対してこれらの手順を繰り返します。

7. ［ユーザーアカウント］リストで、**［終了］**をクリックします。

   すべてのエンドポイントが［保護対象として選択されたエンドポイント］リストに追加されます。

8. **［インストール］**をクリックします。

   Seqrite クライアントエージェントのインストールステータスは、［インストールステータスの表示］リンクから表示することができます。

- リモートインストール機能は、Windows オペレーティングシステムのクライアントのみで使用できます。
- ローミングサービスでリモートインストールはサポートされません。

インストールのステータスの表示

リモートインストールプロセスを使用して Seqrite クライアントを展開すると、［インストールステータスの表示］リンクからクライアントのインストールを追跡することができます。［結果］欄からインストールの詳細情報を取得することができます。必要に応じて、［リモートインストールステータスページ］を表示してそのページを更新し、複数のエンドポイントの最新のインストールステータスを得ることができます。

そのページでは、インストールを停止するためのオプションも提供されています。インストールがまだ開始されておらず、保留状態のエンドポイントに対してインストールを停止できます。進行中のインストールを停止することはできません。

インストールのステータスを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［クライアント］**>**［クライアント展開］**>**［リモートインストール］**を表示します。

   ［リモートインストール］ページが開きます。

3. **［インストールステータスの表示］**リンクをクリックします。

   ［リモートインストールステータス］ページが表示されます。

   そのページには以下の欄が表示されています:

   - エンドポイント名:エンドポイントの名前を表示します。
   - ドメイン:ドメイン名を表示します。

- 日/時:インストールステータスの日時を表示します。
- 結果:インストールステータスを表示します。インストールに失敗すると、その理由も表示されます。

このページには以下のような様々なボタンも表示されます:

- 更新:[更新] を押すと、複数のエンドポイントのクライアントインストールの最新の結果が表示されます。
- インストールを停止する:実際に開始されていない保留中のインストールを停止します。進行中のインストールを停止することはできません。
- 削除:このオプションを使用して、成功した/失敗した/停止されたクライアントインストールに関する［結果］欄のインストール情報を削除することができます。
- 閉じる:このボタンを押して［インストールステータス］ページを閉じます。

インストールの通知

この機能を使用して、ネットワーク内のエンドポイントに Seqrite Endpoint Security クライアントをインストールするようにメール通知を送信できます。将来の通知用にメッセージを入力し、保存しておくことができます。このメッセージは必要に応じていつでも編集できます。

クライアントに Seqrite クライアントのインストールを通知するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアント展開]>[インストールの通知]** を表示します。

   ［インストールを通知する］画面が表示されます。
3. ［宛先］フィールドに、メールアドレスを入力します。宛先が複数の場合は、メールアドレスをセミコロン（;）で区切ります。

   必要に応じてメッセージの件名を修正します。
4. **［通知を送信］** をクリックします。

   システムで使用しているデフォルトのメールプログラムが開きます。そのメールプログラムを使用してメールを送信します。

   ユーザーは、メールに記載されている Seqrite クライアントのインストールウェブページのリンクをクリックします。
5. **［ダウンロード］** ボタンをクリックしてクライアントインストールユーティリティをダウンロードします。cainstlr.exe ファイルを実行します。

Seqrite クライアントのインストールが終了すると、Seqrite Antivirus のインストールが Seqrite クライアントによって開始されます。

- インストールの通知機能は、Microsoft Windows および Mac オペレーティングシステムのクライアントのみで使用できます。
- 通知インストールユーティリティをダウンロードするには、以下の通りに Internet Explorer 設定を行わなければなりません:

  - **Windows Server 2008 用の Internet Explorer 設定**:
    - サーバーマネージャーを使用して、IE ESC を設定してから管理者とユーザーの両方をオフにします。
    - Internet Explorer から、[ツール] > [インターネットオプション] > [詳細] タブを表示します。以下のチェックボックスのチェックを外して、**ダウンロードしたプログラムの署名を確認します。**
  - **Windows Server 2003 用の Internet Explorer 設定:**

    Internet Explorer から、[ツール] > [インターネットオプション] > [詳細] タブを表示します。**[ディスクに暗号化されたページを保存しない]** と **[ブラウザを閉じたときに一時インターネットファイルフォルダーを空にする]** のチェックボックスのチェックを外します。
  - **Internet Explorer のその他のセキュリティ設定**:

    有効にされるその他のインターネットオプションは以下の通りです。
    - カスタムレベルセキュリティ設定で**ファイルのダウンロード**機能を有効にします。
    - **[署名が無効であってもソフトウェアの実行またはインストールを許可する]** チェックボックスを選択して、高度なセキュリティ設定を有効にします。
    - クライアントに通知ユーティリティがシステムにダウンロードされると、Internet Explorer の設定を前の状態に戻すことができます。

クライアントパッケージャ

クライアントパッケージャは、Seqrite クライアントのセットアップおよびアップデートファイルを自己解凍ファイルに圧縮し、メール、CD-ROM、または同様のメディアで簡単に配布できるようにします。デフォルトのメールクライアントを開くメール機能もあり、クライアントパッケージャツールからパッケージを送信できます。クライアントパッケージャは、最小限のオプションを使用して組織外のクライアントに対して作成することもできます。

Seqrite Endpoint Security 7.1 では、クライアントパッケージャは、Seqrite インストーラの有無に関わらず作成できます。MSI ベースのクライアントパッケージャを使用して作成することもできます。Seqrite インストーラを含むクライアントエージェントインストーラは、Endpoint Security サーバーから Seqrite インストーラをダウンロードするネットワークの帯域幅に制限がある場合に役立ちます。このような場合、Seqr

ite インストーラを含むクライアントエージェントインストーラを作成し、エンドポイントでの展開用に CD/DVD に記録するか、または USB リムーバブルディスクにコピーすることができます。しかし、インストーラ付きのクライアントパッケージャはメールで配布できません。

パッケージを受信したユーザーは、セットアッププログラムをダブルクリックするだけでインストールを開始できます。クライアントパッケージャ経由でインストールされた Seqrite クライアントは、Seqrite Endpoint Security サーバーと通信します。

組織のネットワーク外のクライアントパッケージャからインストールされた Seqrite クライアントは、ローミングサービスを利用して Seqrite Endpoint Security サーバーで通信します。

Windows Seqrite クライアントパッケージの作成

Seqrite クライアントパッケージを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、**[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ]** を表示します。
2. クライアントパッケージャリストで**カスタム**を選択します。

   最小限が選択されている場合、[有効期限] チェックボックスが有効にされますが、他のオプションは無効になります。[有効期限] チェックボックスでインストーラーを使用する規定日を指定することができます。有効期間後は、インストーラの期限が切れます。

   最小限のオプションを選択して、メールで組織のネットワーク外のクライアントパッケージャに送信します。詳細については、Se最小限のクライアントパッケージャの送信をご覧ください。インストーラ付きで作成されたクライアントパッケージャは、容量が大きいためメールで送ることができません。
3. OS プラットフォームで **Windows** を選択します。
4. 必要に応じてセットアップタイプリストからセットアップタイプを選択します。

32 ビット版クライアントパッケージャ用 EXE/32 ビット 64 ビット版クライアントパッケージャ用 EXE/64 ビット	EXE/32 ビットまたは EXE/64 ビットオプションを選択して、パッケージャを実行可能なファイルとして作成します。
32 ビット版クライアントパッケージャ用 MSI/32 ビット 64 ビット版クライアントパッケージャ用 MSI/	MSI/32 ビットまたは MSI/64 ビットオプションを選択して、パッケージャを Microsoft インストーラパッケージとして作成します。これらのパッケージは、以下を経由して Seqrite クライアントを展開できます。 • Active Directory グループポリシー

64 ビット	• Microsoft SMS サーバー

5. 「はい」または「いいえ」を選択して、クライアントパッケージャーにアンチウィルスセットアップを含めるかどうかを指定します。
   - クライアントパッケージャーにアンチウィルスセットアップを含めたい場合は「**はい**」を選択します。この場合、メールでこのパッケージャを配布することはできません。
   - クライアントパッケージャーにアンチウィルスセットアップを含めたくない場合は「**いいえ**」を選択します。このパッケージャはメールで配布することができます。
6. デフォルトグループは、EPS コンソールグループリストからクライアントパッケージャに割り当てられます。

   選択したグループがクライアントパッケージャに割り当てられ、クライアントパッケージャからインストールされたクライアントが、EPS コンソールの選択したグループに移動します。
7. [**参照**] をクリックして、Seqrite クライアントパッケージャを保存するフォルダパスを指定します。
8. **このチェックボックスを選択して、離れた場所にいるクライアントを展開するために EPS サーバーのパブリック IP アドレス/ホスト名を指定します。**

   EPS サーバーのパブリック IP アドレスまたはホスト名を入力します。

   パブリックインストールの場合、チェックボックスとパブリック IP アドレス/ホスト名の欄は表示されません。
9. [**作成**] をクリックします。
10. 「はい」または「いいえ」を選択して、パスワード保護されたクライアントパッケージャーを作成するかどうかを指定します。
    - 「はい」を選択すると、[パスワード] ダイアログが表示されます。以下の手順に従ってください:
      i. パスワードを入力して [**OK**] をクリックします。

         6 ～ 18 文字のパスワードを使用します。パスワードを作成するときは、数字、大文字、小文字、特殊記号を組み合わせて作成します。
      ii. [**パスワードの確認**] ボックスにパスワードを入力します。
      iii. [**OK**] をクリックします。パスワード保護されたクライアントパッケージャが作成されます。

iv. クライアントパッケージャを展開しているときにパスワードを指定します。

- 「いいえ」を選択すると、パスワード保護されていないクライアントパッケージャが作成されます。

パスワード保護は Windows クライアントの EXE セットアップのみに適用できます。

Mac Seqrite クライアントパッケージの作成

Mac Seqrite クライアントパッケージを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、**[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ]** を表示します。
2. クライアントエージェントパッケージリストで、**[カスタム]** を選択します。
3. OS プラットフォームリストで、**[Mac]** を選択します。
4. アンチウィルスセットアップに含まれるリストで「はい」または「いいえ」を選択して、クライアントパッケージャーにアンチウィルスセットアップを含めるかどうかを指定します。
   - クライアントパッケージャにアンチウィルスセットアップを含める場合、「はい」を選択します。この場合、このインストーラをメールで展開することはできません。
   - クライアントパッケージャにアンチウィルスセットアップを含めない場合、「いいえ」を選択します。インストーラはメールで展開することができます。
5. 次のリンクの一つから Mac クライアント版をダウンロードします:

   http://dlupdate.quickheal.com/builds/seqrite/71/jap/mclsetp.zip

   http://download.quickheal.com/builds/seqrite/71/jap/mclsetp.zip

   ダウンロードした Mac クライアント版を「Seqrite¥Endpoint Security¥7.1¥Admin ¥Web¥Build¥」フォルダーにコピーして展開します。
6. **[作成]** をクリックします。
   - クライアントパッケージャにアンチウィルスを含めるよう**「はい」**を選択した場合、MCCLAGAV.TAR ファイルが acmac フォルダーに作成されます。
   - アンチウィルスを含めずにクライアントパッケージャを作成するよう**「いいえ」**を選択した場合、MCCLAGNT.TAR ファイルが acmac フォルダーに作成されます。
7. Mac エンドポイントで上記で作成された TAR ファイルをコピーして展開し、展開されたフォルダで MCLAGNT.DMG ファイルを実行して Seqrite EPS Mac クライアントをインストールしなければなりません。

[インストールの通知] メールに記載されたリンクから管理者が MCCLAGNT.TAR をダウンロードすると、SEPS サーバーの ACMAC フォルダからセットアップがダウンロードされます。

MAC OS のローミングポイントでは、カスタムクライアントパッケージャのみが SEPS クライアントに使用されます。

Seqrite クライアントパッケージャの作成

Seqrite クライアントパッケージを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、**[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ]** を表示します。
2. クライアントエージェントパッケージリストで、**[カスタム]** を選択します。
3. **OS プラットフォーム**リストで **Linux** を選択します。
4. エンドポイント設定ごとに、ドロップダウンリストから 32 ビットまたは 64 ビットの**セットアップタイプ**を選択します。

   選択に従って、ウィンドウに tar ファイルをダウンロードする 32 ビットまたは 64 ビット用のリンクが表示されます。
5. 記載されたリンクから tar ファイルをダウンロードします。
6. エンドポイントの設定に従って、以下のフォルダーに tar ファイルをコピーします:

   32 ビット用 -

   「Seqrite¥Endpoint Security¥7.1¥Admin¥web¥build¥epslin32」

   64 ビット用 -

   「 Seqrite¥Endpoint Security¥7.1¥Admin¥web¥build¥epslin64」
7. **[作成]** をクリックして、クライアントパッケージャを作成します。

   以下のフォルダーで選択されたセットアップタイプに従って、パッケージャが作成されます:

   32 ビット用 -

   「Seqrite¥Endpoint Security¥7.1¥Admin¥web¥build¥epslin32」

   64 ビット用 -

   「Seqrite¥Endpoint Security¥7.1¥Admin¥web¥build¥epslin64」

クライアントエージェントをインストールする場合:

1. Linux システムでクライアントパッケージャをコピーして展開します。

2. 32 ビット用に LinuxSetup32 が作成されます。

   64 ビット用に LinuxSetup64 が作成されます。

3. エンドポイントの設定に従って、Linux クライアントパッケージャ「LinuxSetup32/LinuxSetup64」には以下のファイルが含まれます設定:

   - readme.txt
   - インストール
   - clagnt.ini
   - epslin32.tar.gz または epslin64.tar.gz

4. コマンドプロンプトで、chmod 777 インストールコマンドを入力して、スクリプトを「インストール」する実行権限を与えます。
5. スクリプトのインストールを実行します。

メールでパッケージを送信

クライアントパッケージャのメール機能を使用するには、デフォルトのメールクライアントが必要です。

最小限のクライアントパッケージャの送信

ネットワークを使用せずにメールでサーバーからクライアントパッケージャを送信するには、以下の手順に従います:

1. Seqrite Endpoint Security サーバーで、**[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ]** を表示します。
2. クライアントパッケージャリストで**最小限**を選択します。

   ページ上で幾つかのオプションが無効になります。

3. インストール後にクライアントが管理されるデフォルトグループを選択します。
4. **[参照]** をクリックして、Seqrite クライアントパッケージャを保存するフォルダパスを指定します。
5. **[メールを送信]** をクリックします。

   デフォルトのメールクライアントが開きます。デフォルトの件名およびメッセージが記載されたメールが表示されます。必要に応じて件名およびメッセージを変更できます。

6. [宛先] フィールドに、パッケージの受信者を指定します。

   必要に応じて、組織内の他の受信者に Cc または Bcc で送信できます。

7. **[送信]** をクリックします。

カスタムクライアントパッケージャの送信

内部ネットワークのメールでサーバーからクライアントパッケージャを送信するには、以下の手順に従います:

1. Seqrite Endpoint Security サーバーで、[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ] を表示します。
2. クライアントエージェントパッケージリストで、[カスタム] を選択します。
3. インストール後にクライアントが管理されるデフォルトグループを選択します。
4. [参照] をクリックして、Seqrite クライアントパッケージャを保存するフォルダパスを指定します。
5. [メールを送信] をクリックします。

   デフォルトのメールクライアントが開きます。デフォルトの件名およびメッセージが記載されたメールが表示されます。必要に応じて件名およびメッセージを変更できます。
6. [宛先] フィールドに、パッケージの受信者を指定します。

   必要に応じて、組織内の他の受信者に Cc または Bcc で送信できます。
7. [送信] をクリックします。

Mac クライアントパッケージャとクライアントエージェントインストーラの [メールを送信] ボタンは無効のままとなります。

ログインスクリプト

このセクションには、以下の項目が含まれています。

ログインスクリプトのインストール

この機能を使用して、ユーザーが選択したドメインにログインしたときに Seqrite クライアントをリモートシステムに展開できるように、ログインスクリプトをユーザーに割り当てることができます。QHEPS.BAT というスクリプトをドメイン内の選択したユーザーに割り当てることができます。このスクリプトは、ユーザーが関連するドメインにログオンすると、Seqrite Endpoint Protection をシステムにインストールします。

ログインスクリプト機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

ログインスクリプトのセットアップを開く

ログインスクリプトのセットアップを開くには、次の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、[スタート]>[プログラム]>[Seqrite EPS コンソール] を表示します。
2. [ログインスクリプトのセットアップ] をクリックします。
3. Seqrite Endpoint Security のスーパー管理者パスワードを入力して、[OK] をクリックします。

   ログインスクリプトセットアップアプリケーションが開きます。アプリケーションの左側パネルにネットワーク内のすべてのドメインがツリー構造で表示されます。

ログインスクリプトの割り当て

ログインスクリプトを割り当てるには、以下の手順に従ってください:

1. ログインスクリプトのセットアップを開くには、[ログインスクリプトのセットアップを開く] セクションに記載されている手順に従ってください。
2. 新しい画面で、[ドメイン] をダブルクリックします。
3. [ドメイン名] をクリックします。
4. 選択したドメインの管理者権限を持つユーザーのユーザー名およびパスワードを入力します。選択したドメインのすべてのユーザーのリストが右側のパネルに表示されます。
   i. ログインスクリプトを割り当てるユーザーをリストから選択します。
   ii. すべてのユーザーを選択するには、[すべてをチェック] をクリックします。
   iii. 選択したすべてのユーザーを選択解除するには、[すべて選択解除] をクリックします。
5. 選択したユーザーに割り当てられた既存のログインスクリプトを上書きする場合は、[既存のログインスクリプトに上書きする] を選択します。
6. 選択したユーザーにログインスクリプトを割り当てるには、[適用] をクリックします。

   ユーザーがドメインサーバーにログオンすると、割り当てたログインスクリプトにより Seqrite クライアントがユーザーシステムで展開されます。

- ドメインの管理者権限のないユーザーは、赤色で表示されます。
- ユーザーの結果は、[割り当て済み] または [未割り当て] のいずれかになります。[割り当て済み] の場合、スクリプトがそのユーザーに割り当てられたことを示します。結果が [未割り当て] の場合、スクリプトがそのユーザーに割り当てられていないことを示します。
- Seqrite クライアントは、Windows 2000 以降のオペレーティングシステムで管理者権限を持つユーザーによってのみ展開されます。

7. ログインスクリプトセットアップアプリケーションを終了するには、**[閉じる]** をクリックします。

Mac オペレーティングエンドポイントでの Seqrite Endpoint Security インストール

続行する前に、Mac クライアントパッケージャを作成します（Mac Seqrite クライアントパッケージャの作成を参照してください）

Mac クライアントパッケージャの作成後、管理者は［インストールの通知］を使用して Endpoint Security をインストールできます。

［インストールの通知］によって、ネットワーク内のエンドポイントに Seqrite Endpoint Security クライアントをインストールするようにメール通知を送信できます。

クライアントに Seqrite クライアントのインストールを通知するには、［インストールの通知］を参照してください。

Seqrite Endpoint Security をインストールする前に、インストーラファイルのリンクを含む［インストールを通知する］メッセージが管理者から送信されます。

Seqrite Endpoint Security をインストールするには、以下の手順に従ってください:

1. Mac システムに SEPS クライアントをインストールするには、ブラウザにリンクを入力します（メールで送信されます）。

   インストールの前提条件、およびインストーラファイルのリンク（Mac クライアントのダウンロード）が記載されたウェブページが表示されます。前提条件をよくお読みください。

2. **［Mac クライアントのダウンロード］** リンクをクリックします。

   インストーラを含む MCCLAGNT.TAR, ファイルがダウンロードされます。

3. tar ファイルを保存した場所を表示して、すべてのコンポーネントを解凍します。
4. インストーラファイル（MCLAGNT.DMG）をダブルクリックします。

   インストーラを実行して、Seqrite Endpoint Security のインストールを開始します。

   Seqrite Endpoint Security が正常にインストールされました。

SEPS クライアントがインストールされていても、Mac 用の Seqrite Total Security のスタンドアロンのインストールは実行されます。

Mac システムでの Seqrite Endpoint Security のリモートインストール

以下のいずれかの方法で Seqrite Mac Client Agent をインストールできます:

- Apple リモートデスクまたは Casper を使用下インストール
- セキュアシェルを使用したリモート接続
- ターミナルの使用 (Mac および Linux OS)
- PuTTY の使用 (Windows OS)

Apple リモートデスクまたは Casper を使用したリモートインストール

Apple リモートデスクトップ (ARD) を使用して、ネットワークの Mac クライアントコンピュータにリモートで接続したり、ソフトウェアを送信したり、ソフトウェアをインストールしたりできるほか、他のエンドユーザーをリアルタイムにサポートしたり、様々なタスクを実行したりすることができます。

前提条件

Seqrite Mac クライアントエージェントをインストールする前に、以下の要件を必ず満たしていなければなりません。

- ARD または Casper がインストールされている管理者コンピュータは、Mac OS 10.6 以降/OS X サーバーを備えている必要があります。
- Mac Seqrite クライアントインストーラは Seqrite Endpoint Security (SEPS) サーバーに作成されなければなりません。クライアントインストーラの作成方法は、Mac Seqrite クライアントインストーラの作成を参照してください。
- 管理者は、管理者権限のある Mac クライアントコンピュータでアカウントを持っていなければなりません。
- Mac クライアントコンピュータのリモート管理を有効にします。
- 管理者コンピュータにはパッケージがインストールされていなければなりません。パッケージは、ペイロードやインストール用のバンドルを作成するために使用される Mac OS アプリケーションです。パッケージをダウンロードするには、http://s.sudre.free.fr/Software/Packages/about.html をご覧ください。

クライアントエージェントパッケージの作成

クライアントエージェントパッケージを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、「<installation directory>¥Seqrite¥Endpoint Security 7.1¥Admin¥web¥build」フォルダを指定します。

〈インストール先〉は、Seqrite Endpoint Security がインストールされたパスを示します。

2. acmac フォルダを管理者の Mac コンピュータにコピーします。
3. 管理者の Mac コンピュータで Terminal.app を開き、acmac フォルダを表示します。
4. 以下のコマンドを入力します:

```
cd ./Remote_Installation/PKG
sudo sh ./ClientAgentInstaller/CreatePackage.sh
```

このコマンドを実行するには管理者権限が必要です。

パッケージが正常に作成されると、ClientAgentInstaller.pkg ファイルが「./Remote_Installation/PKG/ClientAgentInstaller/」フォルダに作成されます。

Apple リモートデスクトップまたは Casper を使用したクライアントエージェントのインストール

この手順に従って、 ARD または Casper を使用して、リモート Mac クライアントコンピュータにクライアントエージェントをインスト—することができます。詳細については、該当するソフトウェアアプリケーションの文書を参照してください。

Apple リモートデスクトップを使用した Seqrite Mac クライアントの展開

前のセクションで説明した前提条件のほかに、以下の前提条件に従わなければなりません。

前提条件

Seqrite Mac クライアントを展開する前に、管理者のコンピュータに Apple リモートデスクトップ（ARD）ツールがインストールされていなければなりません。ARD をダウンロードするには、https://www.apple.com/in/remotedesktop/ を参照します。

Apple リモートデスクトップを使用して Seqrite Mac クライアントを展開するには、以下の手順に従わなければなりません:

1. Apple リモートデスクトップを開きます。
2. 利用可能なすべてのコンピュータリストから Mac クライアントコンピュータを選択します。**[インストール]** をクリックしてパッケージを追加します。
3. プラス（+）の記号をクリックして場所を指定します。次に、**ClientAgentInstaller.pkg** を追加して **[インストール]** をクリックし、展開を開始します。

Casper を使用した Seqrite Mac クライアントの展開

前のセクションで説明した前提条件のほかに、以下の前提条件に従わなければなりません。

前提条件

Seqrite Mac クライアントを展開する前に、管理者コンピュータに Casper ツールがインストールされていなければなりません。Casper を使用して、クライアントコンピュータにソフトウェアをインストールしたり、リモートでスクリプトを実行したりすることができます。Casper をダウンロードするには、http://www.jamfsoftware.com/products/casper-suite/ を参照します。

Casper を使用して Seqrite Mac クライアントを展開するには、以下の手順に従わなければなりません:

1. Casper 管理にログオンします。
2. **ClientAgentInstaller.pkg** をウィンドウにドラッグし、**[ファイル]>[保存]** を選択します。
3. Casper リモートにログオンします。
4. [コンピュータ] タブで、利用可能なコンピュータのリストから Mac クライアントコンピュータを選択します。
5. [パッケージ] タブで、**[ClientAgentInstaller.pkg]** を選択します。
6. **[移動]** をクリックします。

セキュアシェルを使用したリモート接続

セキュアシェル (SSH) は、クライアントコンピュータを管理するコマンドラインを使用した安全なデータ通信で Mac クライアントのリモートコンピュータを接続するために使われるネットワークプロトコルです。

ターミナルの使用 (Mac または Linux OS)

Mac または Linux OS を使用している管理者のコンピュータは、この方法を使用してクライアントエージェントをインストールすることができます。

前提条件

Seqrite Mac クライアントエージェントをインストールする前に、以下の要件を必ず満たしていなければなりません。

- 管理者は、管理者権限のある Mac クライアントコンピュータでアカウントを持っていなければなりません。
- リモートログインを有効にして、すべてのユーザーにアクセスを許可、または管理者など特定のユーザーにのみアクセスを許可します。この設定は、Mac コンピュータの [システム環境設定] > [共有] > [リモートログイン] で行えます。

- セキュアシェル（SSH）が使用するポート（デフォルトは TCP ポート 22）をブロックしないようにファイアウォールを設定します。このポートでリモートログインに必要な通信が可能となります。
- Mac ファイアウォールを使用している場合、ステルスモードを無効にします。ステルスモードを有効にすると、リモートプッシュインストールは検索ネットワークでクライアントを検出できなくなります。
- Mac コンピュータでステルスモードを無効にするには、お使いの Mac オペレーティングシステムバージョンに該当する以下の Apple ナレッジベースの記事を参照してください。
    - OS X 10.8 Mountain Lion の場合: 使用しているコンピュータが他の人に検出されるのを防止するを参照してください。
    - OS X 10.9 Mavericks の場合:使用している Mac が他の人に検出されるのを防止するを参照してください。
    - OS X 10.10 Yosemite の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。
    - OS X 10.11 El Capitan の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。
    - macOS Sierra 10.12 の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。
- Mac Seqrite Client インストーラは Seqrite Endpoint Security サーバーに作成されなければなりません。クライアントインストーラの作成方法は、Mac Seqrite クライアントインストーラの作成を参照してください。

Seqrite Mac クライアントエージェントのインストール

ターミナルを使用して Seqrite Mac クライアントエージェントをインストールするには、以下の手順に従わなければなりません:

1. Seqrite Endpoint Security サーバーで、「<installation directory>¥Seqrite¥Endpoint Security 7.1¥Admin¥web¥build」フォルダを指定します。

   〈インストール先〉は、Seqrite Endpoint Security がインストールされたパスを示します。

2. acmac フォルダを管理者の Mac コンピュータにコピーします。
3. 管理者の Mac コンピュータでターミナルを開き、acmac/Remote_Installation フォルダを表示します。
4. 以下のコマンドを入力します。

   sh ./Scripts/copy.sh 〈ユーザー名〉〈ip_アドレス〉

   パラメーターの詳細

sh ./Scripts/copy.sh はスタティックです。

〈**ユーザー名**〉では、「テスト」などリモート Mac コンピュータのユーザー名を指定します。

〈**ip_アドレス**〉では、「10.10.0.0」などリモート Mac コンピュータの IP アドレスを指定します。

例: sh ./Scripts/copy.sh 「テスト」「10.10.0.0」。

5. リモートコンピュータのパスワードを入力して接続します。
6. **sudo コマンド「sh /tmp/install.sh」**を入力します。
7. プロンプトが表示されたら、リモートコンピュータのパスワードを入力します。
8. exit コマンドを入力してリモート SSH セッションを閉じます。
9. 手順 4 ～ 8 を繰り返して、Seqrite Mac クライアントエージェントを別のリモートコンピュータにインストールします。

PuTTY の使用 (Windows OS)

Windows OS がインストールされている管理者 コンピュータでは、この方法を使用してクライアントエージェントをインストールできます。

前提条件

Seqrite Mac クライアントエージェントをインストールする前に、以下の要件を必ず満たしていなければなりません:

- 管理者は、管理者権限のある Mac クライアントコンピュータでアカウントを持っていなければなりません。
- リモートログインを有効にして、すべてのユーザーにアクセスを許可、または管理者など特定のユーザーにのみアクセスを許可します。この設定は、Mac クライアントコンピュータの［システム環境設定］>［共有］>［リモートログイン］で行えます。
- セキュアシェル (SSH) が使用するポート (デフォルトは TCP ポート 22) をブロックしないようにファイアウォールを設定します。このポートでリモートログインに必要な通信が可能となります。
- Mac ファイアウォールを使用している場合、ステルスモードを無効にします。ステルスモードを有効にすると、リモートプッシュインストールは検索ネットワークでクライアントを検出できなくなります。
- Mac コンピュータでステルスモードを無効にするには、お使いの Mac オペレーティングシステムバージョンに該当する以下の Apple ナレッジベースの記事を参照してください。
    - OS X 10.8 Mountain Lion の場合: 使用しているコンピュータが他の人に検出されるのを防止するを参照してください。

- OS X 10.9 Mavericks の場合:使用している Mac が他の人に検出されるのを防止するを参照してください。
- OS X 10.10 Yosemite の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。
- OS X 10.11 El Capitan の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。
- macOS Sierra 10.12 の場合: 使用している Mac が他の人に検出されるのを防止するを参照してください。

- Mac Seqrite Client インストーラは Seqrite Endpoint Security サーバーに作成されなければなりません。クライアントインストーラの作成方法は、Mac Seqrite クライアントインストーラの作成を参照してください。

Seqrite Mac クライアントエージェントのインストール

PuTTY を使用して Seqrite Mac クライアントエージェントをインストールするには、以下の手順に従わなければなりません:

1. Seqrite Endpoint Security サーバーで、**cmd.exe** を開き、「<installation directory>¥Seqrite¥Endpoint Security 7.1¥Admin¥web¥build¥acmac」フォルダを表示します。

   〈インストール先〉は、Seqrite Endpoint Security がインストールされたパスを示します。

2. 以下のコマンドを入力します:

   .¥Remote_Installation¥Softwares¥pscp.exe .¥MCCLAGNT.TAR .¥Remote_Installation¥Scripts¥install.sh <username>@<ip_address>:/tmp/

   パラメーターの詳細

   〈**ユーザー名**〉では、「テスト」などリモート Mac クライアントコンピュータのユーザー名を指定します。

   〈**ip_アドレス**〉では、「10.10.0.0」などリモート Mac クライアントコンピュータの IP アドレスを指定します。

   例:**.¥Remote_Installation¥Softwares¥pscp.exe .¥MCCLAGNT.TAR.¥Remote_Installation¥Scripts¥install.sh test@10.10.0.0:/tmp/.**

3. **.¥Remote_Installation¥Softwares¥putty.exe** を開きます。
4. リモート Mac クライアントコンピュータの IP アドレスを入力し、**[開く]** をクリックします。
5. [PuTTY ターミナル] ウィンドウで、リモートコンピュータの管理者ユーザーのユーザー名とパスワードを入力します。

6. リモートコンピュータに接続されたら、**sudo コマンド「sh /tmp/install.sh」**を入力します。
7. **exit** コマンドを入力して、SSH 接続を閉じます。
8. 手順 2 ～ 7 を繰り返し、別の Mac クライアントコンピュータにインストールします。

Mac Seqrite クライアントインストーラの作成

Mac Seqrite クライアントインストーラ（.TAR ファイル）を作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security サーバーで、**[スタート]>[プログラム]>[Seqrite EPS コンソール]>[クライアントパッケージャ]** を表示します。
2. クライアントエージェントパッケージリストで、**[カスタム]** を選択します。
3. OS プラットフォームリストで、**[Mac]** を選択します。
4. アンチウィルスセットアップに含まれるリストで「はい」または「いいえ」を選択して、クライアントパッケージャにアンチウィルスセットアップを含めるかどうかを指定します。
   - クライアントパッケージャにアンチウィルスセットアップを含める場合、「はい」を選択します。この場合、このインストーラをメールで展開することはできません。
   - クライアントパッケージャにアンチウィルスセットアップを含めない場合、「いいえ」を選択します。インストーラはメールで展開することができます。
5. 次のリンクの一つから Mac クライアント版をダウンロードします:
   - http://dlupdate.quickheal.com/builds/seqrite/71/jap/mclsetp.zip
   - http://download.quickheal.com/builds/seqrite/71/jap/mclsetp.zip

   ダウンロードした Mac クライアント版を「Seqrite¥Endpoint Security¥7.1¥Admin¥build¥」フォルダにコピーして展開します。
6. **[作成]** をクリックします。
   - 「はい」を選択してアンチウィルスをクライアントパッケージャに含める場合、MCCLAGAV.TAR ファイルは acmac フォルダに作成されます。
   - 「いいえ」を選択してアンチウィルスなしにクライアントパッケージャを作成する場合、MCCLAGNT.TAR ファイルは acmac フォルダに作成されます。
7. Mac エンドポイントで上記で作成された TAR ファイルをコピーして展開し、展開されたフォルダで MCLAGNT.DMG ファイルを実行して Seqrite EPS Mac クライアントをインストールしなければなりません。

［インストールの通知］メールに記載されたリンクから管理者が MCCLAGNT.TAR をダウンロードすると、SEPS サーバーの ACMAC フォルダからセットアップがダウンロードされます。

MAC OS がインストールされたエンドポイントでローミングを行う場合、EPS クライアントのインストールにはカスタムクライアントパッケージャのみご利用いただけます。

Linux ベースエンドポイントでのクライアントのインストール

Linux エンドポイントには、管理者が手動で Seqrite クライアントをインストールする必要があります。

Linux エンドポイントで Seqrite クライアントをインストールするには、以下の手順を実施してください:

1. エンドポイントの機器構成に合わせた手順に従います:
   - 32 ビット版 Linux エンドポイントには、次の URL から「epslin32.tar.gz」ファイルをダウンロードします:
     - http://dlupdate.quickheal.com/builds/seqrite/71/jap/epslin32.tar.gz
     - http://download.quickheal.com/builds/seqrite/71/jap/epslin32.tar.gz

     Seqrite EPS サーバーインストールフォルダ内の 「Seqrite¥Endpoint Security 7.1¥Admin¥Web¥build¥epslin32」フォルダにコピーします。
   - 64 ビット版 Linux エンドポイントには、次のリンクから「epslin64.tar.gz」ファイルをダウンロードします:
     - http://dlupdate.quickheal.com/builds/seqrite/71/jap/epslin64.tar.gz
     - http://download.quickheal.com/builds/seqrite/71/jap/epslin64.tar.gz

     Seqrite EPS サーバーインストールフォルダ内の「Seqrite¥Endpoint Security 7.1¥Admin¥web¥build¥epslin64」フォルダにコピーします。
2. クライアントパッケージャを（設定に従って）作成します。
3. Linux エンドポイントにクライアントパッケージャをコピーします。
4. Linux エンドポイントでターミナルを開き、ルートユーザーとしてログインします。

   クライアントパッケージャを保存したパスを探します。

5. クライアントパッケージャを展開して、展開したフォルダのパスを探します。
6. ./install コマンドを入力して、Seqrite のインストールスクリプトを実行します。

   インストールスクリプトは以下を実行します:

   - 必要なファイルを、/usr/lib/Seqrite フォルダにコピーします。
   - Seqrite クライアントを正常にインストールします。

   これで、Seqrite クライアントのインストールが完了します。

- オンライン保護は、Linux 2.6 カーネルと互換性のある Dazuko に依存します。
- オンライン保護は、カーネルバージョン 2.6 * の 32 ビット版オペレーティングシステムと互換性があります。
- Seqrite GUI スキャナーは、32 ビットエンドポイントでのみ利用でき、64 ビットエンドポイントでは利用できません。Seqrite設定は、コマンドラインインターフェイスを使用して、64 ビットエンドポイントで設定できます。

インストール後:

- ./install script によってオンライン保護がインストールされていない場合、--online parameter を付けて ./install script スクリプトを実行してオンライン保護をインストールできます。Dazuko の自動インストールが失敗した場合、dazuko ファイルを指定するよう求められます。Seqrite オンライン保護（qhdaemon）にはアクセス制御を可能にする無料のソフトウェアプロジェクトである Dazuko が必要です。qhdaemon を使用するために、Dazuko をカーネルモジュールとしてコンパイルするか、またはカーネルにコンパイルする必要があります。詳細は http://dazuko.org をご覧ください。
- Seqrite オンライン保護の設定。Seqrite オンライン保護は、「configqhonline」を /usr/lib/Seqrite/Seqrite から実行して後で設定できます。

ディスクイメージング

Sysprep などのディスクイメージングを通じて、Seqrite Endpoint Security クライアントを展開することもできます。

ディスクイメージングを通じて展開するには、以下の手順に従ってください:

1. ディスクイメージングのソースとして使用されるコンピュータをネットワークから切断するか、このコンピュータが Seqrite Endpoint Security サーバーと通信できないことを確認します。
2. オペレーティングシステムやその他のアプリケーションをインストールします。
3. クライアントをインストールします。

   クライアントをインストールするには、以下の手順に従ってください:

i. AV ビルドなしにクライアントパッケージャを作成します。
ii. AV ビルドを含むクライアントパッケージャを作成します。

4. ディスクイメージを作成します。

注意:すべての Seqrite Endpoint Security クライアントには GUID（グローバル一意識別子）があります。Seqrite Endpoint Security クライアントが（ディスクイメージングのソースであるエンドポイントへのインストール後に）Seqrite Endpoint Security サーバーと通信した場合、サーバーはこのクライアントに GUID を自動的に割り当てます。クライアントがディスクイメージングされた場合、Seqrite Endpoint Security サーバーは、複数のエンドポイントにイメージを展開した後、クライアントを一意に識別できません。これを回避するため、ディスクイメージングのソースであるコンピュータにインストールされたとき、Seqrite Endpoint Security クライアントが Seqrite Endpoint Security サーバーと通信できないことを確認します。

ディスクイメージング機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

ファイアウォール例外ルール

Windows および Linux などのオペレーティングシステムには、固有のファイアウォールがバンドルされています。オペレーティングシステムにバンドルされたファイアウォールを保持する場合は、これらのシステムに対して Seqrite Endpoint Security を使用して例外を作成できます。これらの例外ルールは、Seqrite Endpoint Security のインストール時に作成されます。Seqrite Endpoint Security がインストールされたシステムでは、インストール時に例外が自動的に作成されます。Seqrite クライアントの場合、例外は Seqrite クライアントの展開時に自動的に作成されます。

Seqrite Endpoint Security を使用したシステムには、サーバー、クライアント、およびシステムに設定された Endpoint Security サイトに対する 3 つの例外ルールが必要です。

サーバーに対する例外ルールは、次の通りです:

- Agent Server 7.1
- Client Agent 7.1
- Endpoint Security Site Port 7.1

Seqrite クライアントを使用したコンピュータには、例外ルールを 1 つ作成する必要があります。クライアントに対する例外ルールは、次の通りです:

- Client Agent 7.1

クライアントシステムが Linux ベースのシステムの場合、例外ルールはファイアウォールにポート番号として作成されます。

リモートアンインストール

リモートアンインストールを使用すると、ネットワークのコンピュータから遠隔操作で Seqrite クライアントとアンチウイルスプログラムを削除できます。

リモートアンインストール機能は、Microsoft Windows、Mac、および Linux オペレーティングシステムのクライアントで使用できます。

リモートアンインストールを通じてクライアントを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[クライアントの展開]>[リモートインストール]** を表示します。

   [リモートアンインストール] ダイアログが開き、すべてのグループが表示されます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
3. Seqrite クライアントをアンインストールするエンドポイントを選択します。すべてのエンドポイントから Seqrite クライアントをアンインストールするには、[エンドポイント名] 欄にあるチェックボックスを選択します。

   [オフラインクライアントを表示] を選択して、オフラインの、またはネットワーク内に存在しないエンドポイントからのアンインストールをスケジュールすることもできます。[サブグループ内のエンドポイントを表示] を選択して、ネットワークを検索することなく、エンドポイントのリストからサブグループにあるエンドポイント名を表示します。
4. **[アンインストール開始通知]** を選択します。

   アンインストールが開始されます。

アンインストール停止通知

アンインストールが開始されていないエンドポイントにアンインストールを停止する通知を送信するには、以下の手順に従ってください:

1. クライアントを削除する必要のないエンドポイントを選択します。
2. **[アンインストール停止通知]** をクリックします。
3. クライアントのアンインストールを開始していないクライアントは、アンインストールの要求をスキップします。ただし、アンインストールプログラムをすでに実行しているクライアントは、アンインストール処理を停止することはできません。

項目	定義
オフラインクライアントを表示	オンラインでない、またはネットワークから切断されたエンドポイントを表示できます。

サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。

SEPS ウェブコンソールからのリモートアンインストールの通知は、ユーザーが Mac システムにログオンしていない場合、送信されません。

Chapter

7

グループの管理

この機能を使用して、グループおよびサブグループを作成し、グループ（またはサブグループ）にポリシーを適用できます。グループには多数のエンドポイントが含まれ、グループ内のすべてのエンドポイントが同じポリシーを共有します。グループの削除、名前の変更、または異なるグループに異なるポリシーを設定することができます。あるグループから別のグループにエンドポイントを移動することもできます。ひとつの Endpoint Security サーバーから別のサーバーに、グループとそこに割り当てたポリシーをエクスポートまたはインポートすることができます。

グループの追加

新しいグループを追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. ルートノード（例: Endpoint Security）を選択して右クリックします。

   [グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] などのオプションとともにサブメニューが表示されます。有効になっているのは [グループの追加] のみです。
4. **[グループの追加]** を選択します。

   [グループの追加] 画面が表示されます。
5. [グループ名を入力してください] テキストボックスに、グループ名を入力します。
6. **[OK]** をクリックします。

   新しいグループが追加されます。

項目	定義
サブグループ内のエンドポイントを表示	サブグループ内のエンドポイントが表示されます。
検索	名前や IP アドレスでエンドポイントを検索できます。

CSV	CSV 形式でレポートを保存できます。

デフォルトのグループにはサブグループは作成できません。

サブグループの追加

サブグループを追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. EPS コンソールで、グループを選択して右クリックします。

   [グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] などのオプションとともにサブメニューが表示されます。
4. **[グループの追加]** を選択します。

   [グループの追加] 画面が表示されます。
5. [グループ名を入力してください] テキストボックスに、グループ名を入力します。
6. **[OK]** をクリックします。

   サブグループが追加されます。

グループの削除

グループを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. EPS コンソールで、グループを選択して右クリックします。

   [グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] などのオプションとともにサブメニューが表示されます。
4. **[グループの削除]** を選択します。

   確認メッセージが表示されます。
5. **[OK]** をクリックします。

   選択したグループが削除されます。

サブグループを含むグループを削除すると、すべての接続されているサブグループも削除されます。

グループ名の変更

グループ名を変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. EPS コンソールで、グループを選択して右クリックします。

   [グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] などのオプションとともにサブメニューが表示されます。
4. **[グループ名の変更]** を選択します。

   [グループ名の変更] 画面が表示されます。古いグループ名も表示されます。
5. [新しい名前を入力してください] テキストボックスに、新しいグループ名を入力します。
6. **[OK]** をクリックします。

   グループ名が変更されます。ただし、このグループに以前に適用されたポリシーは変更されません。ポリシーを変更するには、新しいポリシーを適用してください。

Active Directory からインポート

この機能を使用して、コンソールに Active Directory 構造をインポートできます。Active Directory ですでに使用可能になっているグループ構造がコンソールで必要な場合に役立ちます。

- Active Directory からインポートするには、コンソールがドメインマシンにインストールされているか、ドメインの一員である必要があります。
- 「Active Directory からインポート」はデフォルトのグループでは実行できません。

Active Directory 構造をインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. EPS コンソールで、グループを右クリックします。

[グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] のオプションが表示されます。

4. **[Active Directory からインポート]** オプションを選択します。

   [アクティブなドメインコントローラ] ダイアログが表示されます。

5. ドメインを選択して、**[次へ]** をクリックします。

   認証画面が表示されます。

6. 「ドメイン名¥ユーザー名」の形式でユーザー名を入力して、パスワードを入力します。

7. **[次へ]** をクリックします。

8. [Active Directory コンテナの選択] 画面で、インポートするドメイン名または Active Directory コンテナを選択します。

   ドメイン名を選択すると、すべての Active Directory がインポートされ、任意の Active Directory コンテナを選択すると、選択したコンテナのみがインポートされます。

9. **[終了]** ボタンをクリックします。

グループへのポリシーの設定

ポリシーは、組織内の様々なグループの様々なクライアント設定を含みます。

グループにポリシーを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. EPS コンソールで、グループを右クリックします。

   [グループの追加]、[グループの削除]、[グループ名の変更]、[Active Directory からインポート]、および [ポリシーの設定] などのオプションとともにサブメニューが表示されます。

4. **[ポリシーの設定]** オプションをクリックします。

   ポリシーのリストが表示されます。

5. 適用するポリシーを選択します。

   適用したポリシーが、エンドポイント名、グループ、その他の詳細とともに、右側のパネルに表示されます。

エンドポイントのグループの変更

この機能を使用して、組織でのポリシー変更のため、エンドポイントを特定のグループに入れるか、グループを変更する必要があるかを確認することができます。変更されている場合、新しいグループの保護ポリシーが適用されます。

エンドポイントのグループを変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. Endpoint Security コンソールで、グループを選択します。

   選択したグループのすべてのエンドポイントのリストが右側のパネルに表示されます。
4. エンドポイントを選択して、目的のグループにドラッグします。

   エンドポイントが新しいグループに追加されます。

グループとポリシーのエクスポート

この機能によって、グループとそこに割り当てたポリシーを、ひとつの Endpoint Security サーバーから別のサーバーにエクスポートできます。再インストール時、ある Endpoint Security サーバーから別のサーバーにグループを移動させる必要がある場合に便利です。データは .db ファイルにダウンロードされます。このファイルを別のサーバーにコピーして、インポートオプションを使用し、グループとそこに割り当てたポリシーをインポートする必要があります。

グループとそこに割り当てたポリシーをエクスポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. **[エクスポート]** をクリックします。

   次のメッセージが表示されます。「このファイルを保存または開きますか」
4. **[保存]** をクリックします。

   グループとそこに割り当てたポリシーを含むファイルが保存されます。

グループとポリシーのインポート

この機能によって、グループとそこに割り当てたポリシーをまとめて、ひとつの Endpoint Security サーバーから別のサーバーにインポートできます。グループをエクスポ

ートすると、グループのデータが .db ファイルにダウンロードされます。このファイルを別のサーバーにコピーして、グループのインポートオプションを使用する必要があります。

グループをインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[グループの管理]** を表示します。
3. **[インポート]** をクリックします。

   ファイルを選択するウィザードが表示されます。
4. 以前エクスポートされたファイルを選択します。

   グループとそこに割り当てたポリシーがインポートされ、次のメッセージが表示されます。**ファイルが正常にインポートされます。**

どのグループにも割り当てられていないポリシーは、[グループの管理] ページからエクスポートまたはインポートされません。これらのポリシーは [クライアント] > [ポリシーの管理] ページの [エクスポート] または [インポート] オプションを使用してエクスポートまたはインポートすることができます。

Chapter

8

ポリシーの管理

各組織は、その組織のユーザーを規制するポリシーの実施を望みます。Seqrite Endpoint Security により、管理者はグループに属するユーザーを集中的に制御、および管理できるポリシーを作成できます。

特定のウェブサイトのみの参照を許可するポリシーを作成したり、定期的にシステムをスキャンしたり、メール通信のポリシーを実装したりできます。特定のアプリケーションの使用、および USB デバイスの使用を制限することもできます。ポリシーの管理機能によって、新しいポリシーの作成、および既存のポリシーの修正や削除を柔軟に制御できます。異なる保護ポリシーを異なるグループに作成して制御しやすくします。

ポリシーには、異なるクライアント設定およびスキャンスケジュールが含まれることがあります。作成したポリシーは、簡単にグループに適用できます。グループまたはサブグループのユーザーは、同じポリシーを継承します。グループとは組織の部署のことです。ポリシー設定を作成する前に、グループを作成するべきです。各クライアントのポリシーステータス（適用、保留中、失敗など）を閲覧できます。このステータスは、CSV フォーマットでエクスポートできます。

グループの作成方法を理解するには、[グループの追加] を参照してください。

セキュリティポリシーシナリオの理解

以下の例で、異なるセキュリティポリシーを組織内の異なる部署に対して作成する方法を示します。例として、マーケティングと会計という 2 つの部署を使用します。

マーケティング部門および会計部門のポリシー設定比較表			
クライアント設定	ポリシー機能	マーケティング部門	会計部門
スキャン設定	スキャンモード	自動	高度なスキャン
	ウイルス対策設定	有効	有効
	疑わしいパックファイルのブロック	有効	有効
	自動偽装セキュリテ	有効	有効

	ィツールスキャン		
	感染したエンドポイントをネットワークから切断する	有効ではありません	有効
メール設定	メール保護	有効	有効
	信頼できるメールクライアントの保護	有効	有効
	スパム対策のレベル	低	高
外部ドライブ設定	外部ドライブのスキャン	有効	有効
	自動実行保護	有効	有効
	モバイルスキャン	有効ではありません	有効
不正侵入防御・検知システム（IDS/IPS）	不正侵入防御・検知システム（IDS/IPS）	有効	有効
	システムをネットワークから切断する(DDoS およびポートスキャン攻撃の場合のみ)	有効ではありません	有効
ファイアウォール	ファイアウォール	有効	有効
	レベル	低	高
ウェブセキュリティ	ブラウジング保護	有効	有効
	フィッシング対策	有効	有効
ウェブカテゴリ	ビジネス	許可	拒否
	ソーシャルネットワーキング	拒否	拒否
アプリケーションコントロール	CD/DVD アプリケーション	許可	無許可
	ゲーム	無許可	無許可
高度なデバイスコントロール	高度なデバイスコントロールを有効にする	有効	有効
	デバイスタイプ	有効なデバイスはありません	デバイスが選択され有効になりました
	例外	有効ではありません	有効で適切に追加されました

データ喪失防止	データ喪失防止を有効にする	有効	有効
	データ転送チャンネルを選択する	ネットワーク共有とクリップボードを監視する。プリントスクリーンを無効にする。	アプリケーション経由の転送とリムーバブルデバイスを監視する
	監視するデータを選択する	ファイルタイプ、機密データ、ユーザー定義辞書	ファイルタイプ、機密データ
	処置	ブロックとレポート	レポートのみ
ファイル活動モニター	ファイル活動モニターを有効にする	有効	有効
	リムーバブルドライブ	有効	有効
	ネットワークドライブ	有効	有効
	ローカルドライブ	有効ではありません	有効
アップデート設定	自動アップデート	有効	有効
	インターネットからダウンロードする	有効	有効ではありません
	Endpoint Security サーバーからダウンロードする	有効ではありません	有効
インターネット設定	プロキシ設定	有効	有効ではありません
パッチ管理	欠落しているパッチのスキャンとインストール	有効	有効
一般設定	クライアント設定へのアクセスを許可する	有効	有効

ポリシーの作成

ポリシーで、異なるグループのクライアント設定を管理できます。クライアント設定でポリシーを作成できるほか、スケジュール設定を作成し、異なるグループに適用することもできます。

新しいポリシーの作成

新しいポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. 新しいポリシーを作成するには、**[追加]** をクリックします。

   新しいポリシーの設定画面が表示されます。
4. [ポリシー名] テキストボックスに、ポリシー名を入力します。

   新しいポリシーに名前を付けた後、クライアント設定およびスケジュール設定を行う必要があります。
5. [説明] テキストボックスで、ポリシーの簡単な説明を入力します。
6. 設定を保存するには、**[ポリシーの保存]** をクリックします。

   新しいポリシーの作成時に、**[クライアントに自分で設定させる]** オプションを選択して、クライアントに独自の設定を許可できます。

このオプションを有効にすると、高度なデバイスコントロールとデータ喪失防止機能が無効になります。

ポリシーのコピー

ポリシーをコピーするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. コピーするポリシーを選択して、[**ポリシーのコピー**] アイコンをクリックします。

   選択したポリシーが設定と共に表示されます。
4. [ポリシー名] テキストボックスに、ポリシー名を入力します。

   ポリシー設定も変更できます。
5. 設定を保存するには、**[ポリシーの保存] をクリックします。**

ポリシー名の変更

ポリシー名を変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. 名前を変更するポリシーをクリックします。

   選択したポリシーが設定と共に表示されます。
4. [ポリシー名] テキストボックスで、ポリシー名を変更します。

   ポリシー設定も変更できます。
5. 設定を保存するには、**[ポリシーの保存] をクリックします。**

ポリシーの削除

ポリシーを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. 削除するポリシーを選択して、**[削除]** をクリックします。

   確認メッセージが表示されます。
4. 選択したポリシーを削除する場合は、**[はい]** をクリックします。

   選択したポリシーがグループに適用されていると、そのポリシーは削除できず、ポリシーの削除に失敗したことを示すメッセージが表示されます。

グループに適用されているポリシーを削除する場合は、異なるポリシーをそのグループに適用して削除対象のポリシーがどのグループにも適用されていない状態にすると、正常に削除できます。

ポリシーのインポートとエクスポート

この機能を使用して、Seqrite Endpoint Security のポリシーをインポートまたはエクスポートすることができます。再インストールが必要な場合や、複数のエンドポイントを同じ設定にしたい場合に、現在使用しているエンドポイントに設定された内容をエクスポートするだけで、対象のエンドポイントに簡単にインポートできます。初期設定とお客様の設定の両方をエクスポートできます。

設定は Seqrite Endpoint Security をアンインストールする前にエクスポートする必要があります。設定のインポートおよびエクスポートは、同じ方法で実行できます。

ポリシーのエクスポート

ポリシー設定をエクスポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. エクスポートするポリシーを選択して、**[エクスポート]** ボタンをクリックします。
4. ポリシーを保存するドライブとフォルダーを選択します。
5. **[保存]** をクリックします。
   ポリシー設定ファイルが、選択した場所にエクスポートされます。

ポリシーのインポート

ポリシー設定をインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[ポリシーの管理]** を表示します。
3. **[インポート]** ボタンをクリックします。
4. インポート設定ファイルを、保存した場所から選択します。
   新しいメッセージが表示され、インポートするポリシーを選択できます。
5. インポートするポリシーを選択して、**[インポート]** をクリックします。

Chapter

9

アセット

アセット機能を使用して、システム情報、ハードウェア情報、インストールされているソフトウェアを監視することができます。ネットワークのシステム構成に施されたハードウェア変更がある場合に確認することもできます。さらに、実際に変更が行われたエンドポイントリストを記録し、その情報を CSV 形式のファイルでエクスポートすることも可能です。

エンドポイントの詳細を確認する

すべてのエンドポイントの詳細を表示するには、次の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[クライアント]>[アセット]** を表示します。

   [アセット] ビューには、すべてのクライアントに関する以下の詳細が記載されています:

欄	説明
エンドポイント名	エンドポイントの名前を表示します。
グループ	選択したクライアントが属しているグループ名を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
IP アドレス	IP アドレスを表示します。
オペレーティングシステム	エンドポイントのオペレーティングシステムの名前を表示します。
システム製造元	システム製造元の名前を表示します。

特定のエンドポイントの詳細を表示するには、次の手順に従ってください:

1. 次のいずれかを実行してください:
   - [アセット] ページの [検索] テキストボックスでエンドポイント名/IP を入力して、[検索] アイコンをクリックします。

- 表示されたリストからエンドポイントを選択します。

2. **[詳細を表示]** をクリックします。

   [詳細を表示] 画面が表示されます。

   - [システム情報] タブにシステム情報の詳細が表示されます。Windows OS の PS プロダクトキーが表示されます。

     OS プロダクトキーは、Windows Vista 以降のオペレーティングシステムのクライアントのみが使用できます。

   - [ハードウェア情報] タブにハードウェア情報の詳細が表示されます。
   - [インストールされているソフトウェア] タブにシステムにインストールされているソフトウェアの詳細が表示されます。

     MS Office プロダクトキーは、MS オフィス 2010 以降のみで利用できます。

     この MS Office のプロダクトキーは、Mac オペレーティングシステムのクライアントでは使用できません。

     MS オフィスのライセンスステータスが表示されます。

     予想されるライセンスステータスと MS Office の詳細を以下の表に示します。

ライセンスのステータス	説明
ライセンス無し	この製品にはライセンスが供与されていません。
ライセンス有り	この製品にはライセンスが供与されています。
OOBGrace	MS Office のライセンスは猶予期間中です。
OOTGrace	MS Office のライセンスを最有効化する必要があります。
NonGenuineGrace	MS Office のライセンスはオンライン検証に失敗し、猶予期間中です。
ExtendedGrace	MS Office ライセンスの猶予期間が延長されます。
通知	MS Office のライセンスは猶予期間外にあるか、検証に失敗しています。

     エンドポイントの詳細を CSV 形式で保存できます。

アセット管理を有効にする

次の手順に従って［アセット管理レポート］を有効にできます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]>[クライアント]>[アセット管理]** を表示します。
3. アセット管理を有効にするには、**[アセット管理を有効にする]** チェックボックスを選択します。

4. **［適用］**をクリックします。

一部のソフトウェアの詳細が［アセット］に表示されない場合があります。

Chapter

10

設定

この機能により、管理者はデフォルトポリシーの設定を確認してカスタマイズできます。デフォルトポリシーは、システムに製品をインストールすると、すぐに使用可能になります。デフォルトポリシーには、クライアント設定とスケジュールスキャン設定が含まれており、グループに適用できる最適なセキュリティです。必要に応じて設定をカスタマイズできますが、名前は変更できません。デフォルトポリシーは、[ポリシーの管理] オプション（Seqrite Endpoint Security> [クライアント] > [ポリシーの管理] の順に選択）からも利用でき、設定をカスタマイズできます。

設定をカスタマイズして後でデフォルト設定に戻したい場合は、デフォルトボタンをクリックします。

クライアント設定

このセクションには、以下の項目が含まれています:

スキャン設定

この機能により、組織内のクライアントシステムのスキャン開始方法のポリシーを定義できます。ポリシーを改良することで、ウイルス対策または DNA スキャンを有効にしたり、疑わしいパックファイルをブロックしたり、その他の設定を行ったりできます。

次の表では、スキャン設定の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
自動スキャンモード	✓	✓	X
実行可能ファイルをスキャン	✓	✓	X
すべてのファイルをスキャン（時間がかかりま	✓	✓	X

す)			
パックファイルのスキャン	✓	X	X
受信ボックスのスキャン	✓	X	X
アーカイブファイルをスキャン	✓	✓	X

スキャン設定に対してポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[スキャン設定]** を表示します。
3. [スキャナ設定] で、スキャンモードを選択します。

   スキャンモードには、[自動] および [高度なスキャン] があります。

   [ウイルス対策]、[高度な DNA スキャン]、[疑わしいファイルのブロック]、[自動偽装セキュリティツールスキャン]、[感染したエンドポイントをネットワークから切断する]、[除外ファイルおよびフォルダ] を有効にして、さらにファイル拡張子によってファイルをスキャン対象から除外できます。
4. 設定を保存するには、**[ポリシーの保存] をクリックします。**

スキャナ設定

[スキャナ設定] で、以下のいずれかのスキャンオプションを選択できます:

- **自動***: これはデフォルトのスキャン設定で、クライアントに最適な保護を提供します。
- **高度なスキャン**: このオプションを選択すると、要求に応じてスキャンオプションの設定を詳細にカスタマイズする必要があります。このオプションを選択すると、以下に説明する他の機能が有効になります:

機能	説明
スキャンする項目の選択	以下のいずれかのスキャンオプションを選択します: 実行可能ファイルをスキャン:実行可能ファイルのみをスキャンします。 すべてのファイルをスキャン:すべてのファイルをスキャンしますが、スキャンに時間がかかります。
パックファイルのスキャン*	実行可能ファイルのパックファイルをスキャンします。
受信ボックスのスキャン*	受信ボックス内のメールをスキャンします。
アーカイブファイルの	他のファイルを含む ZIP および ARJ などの圧縮フ

スキャン*	ァイルをスキャンします。
アーカイブスキャンのレベル	アーカイブファイルでのスキャンレベルを設定できます。デフォルトでは、スキャンレベルは 2 に設定されています。デフォルトのスキャンレベルを上げることはできますが、スキャン速度に影響を及ぼすことがあります。
アーカイブファイルでウイルスが見つかったときに実行する処置を選択してください。	オンデマンドスキャン中にアーカイブファイルでウイルスが見つかったときに実行する処置を選択できます。処置を以下から 1 つ選択します: • 削除 - アーカイブ内で単一のファイルが感染している場合でも、アーカイブファイル全体を削除します。 • 隔離 - 感染したファイルを含むアーカイブを隔離します。 • スキップ - アーカイブファイル内でウイルスが見つかっても、処置を実行しません。
ウイルスが見つかったときに実行する処置を選択します。	手動スキャン中にウイルスが見つかったときに実行する処置を選択できます。処置を以下から 1 つ選択します: • 修復 - ウイルスに感染したすべてのファイルを自動的に修復します。修復不能なファイルは削除します。 • 削除 - ウイルスに感染したすべてのファイルを自動的に削除します。 • スキップ - ファイル内でウイルスが見つかっても、処置を実行しません。
アスタリスク (*) の付いた機能が適用されるクライアントについては、比較表をご覧ください。	

ウイルス対策設定

この機能により、メールの添付ファイル、インターネットからのダウンロード、ファイル転送、およびファイルの実行などから侵入する可能性があるウイルスに対してクライアントシステムを常時監視できます。システムを安全に保ち、脅威から守るために、ウイルス対策を常に有効にしておくことをお勧めします。

次の表では、ウイルス対策設定の機能の比較を示しています。これらの機能は様々な系統の Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
起動時にウイルス対策をロードする	✓	✓	✓
アラートメッセージを表示する	✓	✓	X
感染源をレポート	✓	X	X
ウイルスが見つかったときに実行する処置を選択する	✓	✓	X

ウイルス対策では、以下の機能を設定できます:

機能	説明
起動時にウイルス対策をロードする	リアルタイム保護を有効にして、システムが起動するたびにウイルス対策をロードします。
アラートメッセージを表示する	ウイルス対策により感染したファイルが検出されるたびに、ウイルス名およびファイル名が記載されたアラートメッセージを表示します。
感染源をレポート	ウイルスが検出されるシステムのソース IP アドレスを表示します。
ウイルスが見つかったときに実行する処置を選択する	手動スキャン中にウイルスが見つかったときに実行する処置を選択できます。処置を以下から 1 つ選択します: • 修復 - ウイルスに感染したすべてのファイルを自動的に修復します。修復不能なファイルは削除します。 • 削除 - ウイルスに感染したすべてのファイルを自動的に削除します。 • アクセス拒否 - 感染したファイルへのアクセスをブロックします。

高度な DNA スキャン設定

ウイルス定義データベースにシグネチャが存在しない新しい未知の悪意ある脅威に対してクライアントシステムを保護します。DNA スキャンは、システムに潜む悪意のある未知または不明な脅威を検出して除去する、Seqrite 独自のテクノロジーです。DNA スキャン技術は、きわめて低い誤検出率で疑わしいファイルを捕捉します。

高度な DNA スキャン設定には、以下の機能も含まれています:

機能	説明
DNA スキャンを有効にする	デジタルネットワークアーキテクチャ（DNA）パターンに基づいて、システムをスキャンします。
挙動検出システムを有効にする	ファイルおよびシステムの挙動に基づいて、それらをスキャンします。ファイルやシステムの挙動が疑わしく、また挙動が勝手に変化した場合は、疑わしいとみなされます。この検出は、ファイルまたはシステムの重大度レベル（低、中、高）に基づいて分類されます。疑わしいファイルがシステムに報告された頻度に基づいて、検出重大度レベルを選択できます。
疑わしいファイルの送信	疑わしいファイルを自動的に Seqrite リサーチラボに送信してさらに分析します。
ファイル送信時に通知を表示する	DNA が疑わしいファイルの送信時に、通知を表示します。

- 高度な DNA スキャン設定機能は、Windows オペレーティングシステムのクライアントのみで使用できます。
- 「挙動検出システム」スキャン設定は、Windows XP 64 ビットおよび Windows Server プラットフォームには適用されません。

疑わしいパックファイルのブロック

本機能によって、疑わしいパックファイルへのアクセスを発見してブロックできます。疑わしいパックファイルとは、様々な方法で圧縮またはパックされ、さらに暗号化されている悪意のあるプログラムです。これらのファイルが解凍されると、エンドポイントシステムに深刻な被害を及ぼす可能性があります。

クライアントが疑わしいファイルにアクセスしないようにして、感染を広げないようにするために、本オプションは常に有効にしておくことをお勧めします。

疑わしいパックファイルのブロック機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

自動偽装セキュリティツールスキャン設定

この機能は、偽装セキュリティツールや偽造アンチウイルスソフトウェアを自動的にスキャンして削除します。本機能を有効にすると、ファイル内に偽装セキュリティツールが潜んでいないかすべてのファイルをスキャンします。

自動偽装セキュリティツールスキャン機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

感染したエンドポイントをネットワークから切断する

感染したエンドポイントをネットワークから切断します。以下のオプションが使用できます:

- **修復不能なウイルスが見つかったとき**:修復不能なウイルスがメモリ内で実行されているのが見つかった場合、エンドポイントを切断します。
- **DNA スキャンによって疑わしいファイルが見つかったとき**:疑わしいファイルがメモリ内で実行されているのが見つかった場合、エンドポイントを切断します。

感染したエンドポイントをネットワークから切断する機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

除外ファイルおよびフォルダ

除外ファイルおよびフォルダ機能では、既知のウイルスのスキャン、高度な DNA スキャン、疑わしいパックファイルのスキャンから除外するファイルとフォルダを指定できます。特定のファイルとフォルダを信頼し、スキャンから除外するのに役立ちます。

次の表では、除外ファイルおよびフォルダの機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
除外:既知のウイルス検出	✓	✓	X
除外:DNA スキャン	✓	X	X
除外:疑わしいパックされたファイルのスキャン	✓	X	X
除外:挙動検出	✓	X	X

ファイルまたはフォルダを追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[スキャン設定]** を表示します。
3. [除外ファイルおよびフォルダ] で、**[追加]** をクリックします。
4. [項目の除外] 画面で、次のいずれかを選択します:
   - **フォルダの除外**:[フォルダの除外] を選択した場合、[フォルダーパスの入力] テキストボックスにフォルダパスを入力します。
     サブフォルダもスキャンから除外する場合は、[**サブフォルダも含める**] を選択します。

- **ファイルの除外**:[ファイルの除外] を選択した場合、[ファイルパスの入力] テキストボックスにファイルパスを入力します。

5. [除外] で、要件に応じて以下のいずれかを選択します:
   - 既知のウイルス検出
   - DNA スキャン
   - 疑わしいパックされたファイルのスキャン
   - 挙動検出
6. 設定を保存するには、[OK] をクリックします。

- [既知のウイルス検出] を選択すると、[DNA スキャン] および [疑わしいパックされたファイルのスキャン] も実行され、3 つのオプションすべてが選択されます。
- [DNA スキャン] を選択すると、[疑わしいパックされたファイルのスキャン] も実行され、両方のオプションが選択されます。
- ただし、[疑わしいパックされたファイルのスキャン] または [挙動検出] は単一のオプションとして選択できます。

拡張子を除外する

リアルタイムウイルス対策のスキャンから、ファイル拡張子によってファイルを除外できます。問題の原因になっている可能性のある特定のカテゴリのファイルを除外することによって、パフォーマンス関連の問題のトラブルシューティングに役立ちます。

スキャンからファイル拡張子を除外するには、以下の手順に従ってください:

- [拡張子を除外する] で、ファイル拡張子名テキストボックスに拡張子を入力し、[追加] をクリックします。

  ファイル拡張子は xml、html、zip（ドットなし）のいずれかの形式にしなければなりません。

拡張子を除外する機能は、Windows および Mac オペレーティングシステムのクライアントのみで使用できます。

メール設定

この機能により、様々なソースからのメール受信に対する対策規則をカスタマイズできます。スパム、フィッシング、およびウイルスに感染したメールをブロックする規則を設定できます。

次の表では、メール設定の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
メール保護を有効にする	✓	✓	X
信頼できるメールクライアントの保護を有効にする	✓	X	X

メール設定を行うには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[メール設定]** を表示します。
3. 有効にするオプションを選択します。

   メール設定オプションには次のものがあります:メール保護、信頼できるメールクライアントの保護、スパム対策、スパム対策のレベル、ホワイトリスト、およびブラックリスト。
4. 設定を保存するには、**[ポリシーの保存]** をクリックします。

メール保護

メール保護機能では、受信するすべてのメールに対する保護規則を適用できます。メールに添付された感染ファイル（マルウェア、スパム、ウイルス）もブロックできます。

メール保護をグループ内のユーザーに適用するには、[メール保護を有効にする] チェックボックスを選択します。この機能が有効になると、すべての受信メールが、受信ボックスに送られる前にスキャンされます。

メール保護機能は、Microsoft Windows および Mac オペレーティングシステムのクライアントのみで使用できます。

信頼できるメールクライアントの保護

メールは最も広く使用されているコミュニケーション媒体なので、マルウェアやその他の脅威を運ぶために都合の良い手段として利用されます。ウイルス作成者たちは常に、代表的なメールクライアントの脆弱性を利用してウイルスコードを自動的に実行する新しい方法を探しています。また、ワームは独自の SMTP エンジンルーチンを使用して感染を広げます。

信頼できるメールクライアントの保護は、メールを送信する前にシステムのメール送信アプリケーションを認証する高度なオプションです。このオプションは、新しいワームのさらなる拡散を防ぎます。メールの送信が許可されたデフォルトのメールクライアントリストが含まれています。デフォルトリスト中のメールクライアントには、Microsoft Outlook Express、Microsoft Outlook、Eudora、および Netscape Navigator が含まれます。

信頼できるメールクライアントの保護は、Microsoft Outlook Express、Microsoft Outlook、Eudora、Netscape Navigator など、一般的に使用されているほとんどのメールクライアントをサポートしています。使用しているメールクライアントがこれらのものと異なる場合、信頼できるメールクライアントリストに追加できます。

信頼できるメールクライアントの保護機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

スパム対策

この機能では、問題のないメールと区別して、スパム、フィッシング、アダルトメール等の迷惑メールを除外できます。スパム対策機能を常に有効にしておくことをお勧めします。スパム対策を有効にすると、スパム対策のレベル、ホワイトリスト、およびブラックリストオプションも有効になります。

次の表では、スパム対策の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
スパム対策	✓	✓	X
スパム対策のレベル	✓	X	X
ホワイトリストを有効にする	✓	✓	X
ブラックリストを有効にする	✓	✓	X

スパム対策の設定

スパム対策を設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[メール設定]** を表示します。
3. **[スパム対策を有効にする]** を選択します。
4. [スパム対策のレベル] で、以下のいずれかの対策レベルを設定します:
   - **低**:低レベルのフィルタリングスパム対策ポリシーを適用します。
   - **中**:最適なフィルタリングを行います。中レベルのフィルタリングを有効にしておくことをお勧めします。本オプションはデフォルトで選択されています。
   - **高**:より厳格なフィルタリング基準を設けます。問題のないメールもブロックしてしまう可能性があるため理想的な対策レベルではありません。迷惑メールをあまりにも多く受信している場合にのみ、この対策レベルを選択してください。

5. ［ホワイトリストを有効にする］を選択して、ホワイトリストに含まれるメールに対して対策規則を実施します。
6. ［ブラックリストを有効にする］を選択して、ブラックリストに含まれるメールに対して対策規則を実施します。
7. 設定を保存するには、［ポリシーの保存］をクリックします。

アスタリスク（*）の付いた機能が適用されるクライアントについては、比較表をご覧ください。

ホワイトリストに関するスパム対策の設定

ホワイトリストは、信頼できるメールアドレスのリストです。ホワイトリストに含まれるメール ID から受信した内容はスパム対策のフィルタリングポリシーの対象外となり、「スパム」とタグ付けされません。

これは、問題のないメールアドレスがスパムとして検出される場合に便利です。あるいは、あるドメインをブラックリストに登録したものの、そのドメインの特定のメールアドレスからのメールを受け取りたい場合にも使用できます。

メールアドレスをホワイトリストに追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［設定］>［クライアント設定］>［メール設定］を表示します。
3. ［ホワイトリストを有効にする］チェックボックスを選択します。

   ［スパム対策］が有効になっているかをチェックします。［スパム対策］が有効になっている場合のみ、ホワイトリストオプションが有効になります。
4. ［メール ID］テキストボックスで、メールアドレスまたはドメインを入力して、［追加］をクリックします。

   ［インポート］ボタンを使用して、テキストファイルからメールまたはドメインをインポートできます。

- メールアドレスは、abc@abc.com の形式で入力してください。
- ドメイン名は次の形式で入力してください。*@mytest.com.
- 同一のメールアドレスを、ブラックリストおよびホワイトリストの両方に入力することはできません。

ブラックリストにおけるスパム対策規則の設定

ブラックリストのメールアドレスから届くメールはすべて、その内容に関わらずフィルタリングされます。このリストにあるアドレスからのメールにはすべて「[SPAM]」のタグが付けられます。

本機能は、お使いのサーバーがオープンメールリレーを使用している場合は特に有効です。オープンメールリレーは不明な送信者からのメールを送受信するために使用されます。このメーラーシステムがスパム業者に悪用されることがあります。ブラックリストを使用することで、受信する迷惑メールや不明な送信者からのメールをメール ID とドメインによってフィルタリングできます。

メールアドレスをブラックリストに追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[メール設定]** を表示します。
3. **[ブラックリストを有効にする]** チェックボックスを選択します。

   [スパム対策] が有効になっているかをチェックします。[スパム対策] が有効になっている場合のみ、ブラックリストオプションが有効になります。
4. [メール ID] テキストボックスで、メールアドレスまたはドメインを入力して、**[追加]** をクリックします。

   [インポート] ボタンを使用して、テキストファイルからメールまたはドメインをインポートできます。

- メールアドレスは、abc@abc.com の形式で入力してください。
- ドメイン名は次の形式で入力してください。*@mytest.com.
- 同一のメールアドレスを、ブラックリストおよびホワイトリストの両方に入力することはできません。

外部ドライブ設定

外部デバイスを接続すると、システムはそこからウイルスやマルウェアに侵入されるリスクにさらされます。CD、DVD、USB ドライブ等、外部デバイスに対する保護規則を設定できます。

次の表では、外部ドライブ設定の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
外部ドライブのスキャン	✓	X	✓
自動実行保護設定	✓	X	X
モバイルスキャン設定	✓	X	X

外部ドライブ設定を行うには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. [設定]>[クライアント設定]>[外部ドライブ設定] を表示します。
3. 有効にするオプションを選択します。

   外部ドライブ設定オプションには次のものがあります。外部ドライブ設定、自動実行保護設定、およびモバイルスキャン設定。
4. 設定を保存するには、[ポリシーの保存] をクリックします。

   外部ドライブ設定には、以下が含まれています:

外部ドライブ設定

外部ドライブ設定では、USB ドライブがお使いのシステムに接続されるとただちにスキャンを開始します。USB ドライブは、ウイルスやマルウェアをシステム間で転送するのに利用されるため、システムからアクセスする前に、これらのドライブにウイルススキャンを常に実行する必要があります。

自動実行保護設定

自動実行保護は、オペレーティングシステムの自動実行機能を使用して、USB ドライブや CD/DVD を介してシステムに侵入しようとする自動実行マルウェアからシステムを保護します。

モバイルスキャン設定

この機能は、携帯端末のウイルス、スパイウェア、その他のマルウェアをスキャンします。お使いの携帯端末をスキャンするには、次のいずれかの方法を使用してお使いの PC に接続する必要があります:

- USB ケーブル
- Bluetooth

モバイルスキャン機能は、サーバーオペレーティングシステムではサポートされていません。

不正侵入防御・検知システム（IDS/IPS）

多数のマシンを展開するネットワークを構築する場合、セキュリティは重要な問題になります。不正侵入防御・検知システム（IDS/IPS）を使用して、IDS/IPS、ポートスキャン攻撃、分散型サービス拒否（DDoS）などの様々なソースからの攻撃を検出することができます。この検出は、すべての通信にセキュリティ層を実装し、システムに対する望ましくない侵入または攻撃を遮断します。一定時間攻撃者をブロックする、感染したシステムをネットワークから切断する、管理者にアラートメッセージを送信する等の処置をとることもできます。

IDS/IPS 保護機能は、Microsoft Windows のクライアントのみで使用できます。

IDS/IPS 設定を変更して異なるポリシーを作成し、必要に応じて各グループに個別のポリシーを適用することができます。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[IDS/IPS]** を表示します。
3. チェックボックスを選択して以下のオプションの一つを有効にします:
   - 不正侵入防御・検知システム（IDS/IPS）を有効にする
   - ポートスキャン攻撃を検出する
     このチェックボックスを選択すると、[カスタマイズ] リンクが有効にされます。
   - DDoS 攻撃を検出する
     このチェックボックスを選択すると、[カスタマイズ] リンクが有効にされます。
4. 攻撃か検出された場合に実行する処置を、以下にオプションから選択します:
   - 攻撃者 IP を…分間ブロックする。
     点線部に時間を入力します。
   - エンドポイントをネットワークから切断する（DDoS およびポートスキャン攻撃の場合のみ）
   - 攻撃が検出されたときにアラートメッセージを表示します。
     攻撃が検出されたときに適切な処置をとることができます。
5. 設定を保存するには、**[ポリシーの保存]** をクリックします。

ポートスキャンのカスタマイズ

[ポートスキャン攻撃を検出する] および [DDoS 攻撃を検出する] のカスタマイズ方法は、以下の通りです:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[IDS/IPS]** を表示します。
3. **[ポートスキャン攻撃を検出する]** チェックボックスを選択します。
   カスタマイズされたリンクが有効にされます。
4. **[カスタマイズ]** リンクをクリックします。
   [設定 - ポートスキャン] ダイアログが表示されます。
5. 以下のレベルから 1 つ選択します:
   - **低**:多くのポートがスキャンされた場合に攻撃を検出します。
   - **正常**:複数のポートがスキャンされた場合に攻撃を検出します。
   - **高**:1 つのポートがスキャンされた場合でも攻撃を検出します。

- **カスタム**:[攻撃条件] と、[スキャンされたポート数が次の値を超えたとき] 欄をカスタマイズできます。

6. スキャンしない IP アドレスを除外するには、[除外される IP アドレス] セクションで、**[追加]** をクリックします。
7. [IP アドレスの追加] 画面で、IP アドレスまたは IP 範囲を入力して **[OK]** をクリックします。
8. スキャンしないポートを除外するには、[除外されるポート] セクションで、**[追加]** をクリックします。
9. [ポートの追加] 画面で、ポートまたはポート範囲を入力して **[OK]** をクリックします。

分散型サービス拒否 (DDoS) のカスタマイズ

DDoS 攻撃の設定のカスタマイズ方法は以下の通りです:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[IDS/IPS]** を表示します。
3. **[DDOS (分散型サービス拒否) 攻撃を追跡する]** チェックボックスを選択します。

   カスタマイズされたリンクが有効にされます。
4. **[カスタマイズ]** リンクをクリックします。

   [設定 - DOS] ダイアログが表示されます。

   以下のレベルから 1 つ選択します:
   - **低**:攻撃が多数発生した場合に検出します。
   - **正常**:攻撃が複数発生した場合に検出します。
   - **高**:1 つの攻撃が発生した場合でも攻撃を検出します。
   - **カスタム**:[攻撃条件] と、[攻撃元の数が次の数値を超えたとき] の数値をカスタマイズできます。
5. スキャンしない IP アドレスを除外するには、[除外される IP アドレス] セクションで、**[追加]** をクリックします。
6. [IP アドレスの追加] 画面で、IP アドレスまたは IP 範囲を入力して **[OK]** をクリックします。
7. スキャンしないポートを除外するには、[除外されるポート] セクションで、**[追加]** をクリックします。
8. [ポートの追加] 画面で、ポートまたはポート範囲を入力して **[OK]** をクリックします。

ファイアウォール

ファイアウォールは、インバウンドおよびアウトバウンドネットワークトラフィックを監視することでシステムを守ります。すべての受信トラフィックが安全で許可すべきかどうかを分析し、また、外部への通信がセキュリティポリシーに設定したコンプライアンスに従っているかどうかをチェックします。ファイアウォールは、バックグラウンドで目立たず動作し、悪意のあるネットワーク活動がないかを監視します。

必要に応じて、ファイアウォール保護を有効にしたり、例外ルールなどの設定を施したファイアウォールを適用したり、様々なグループ/部署ごとに異なるポリシーを作成したりできます。例えば、会計部門に対してセキュリティレベルを高にして適用し、追加のポリシー設定でポリシーを入力して例外ルールを適用できます。[ファイアウォール違反が発生したときにアラートメッセージを表示する] および [ファイアウォールレポートを有効にする] オプションを適用することもできます。マーケティング部門には、例外ルールを設定せずに低いセキュリティレベルでポリシーを作成し、[ファイアウォールレポートを有効にする] オプションを適用できます。

ファイアウォール機能は、Microsoft Windows のクライアントのみで使用できます。

ファイアウォール設定にポリシーを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[ファイアウォール]** を表示します。
3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. [レベル] オプションで、以下のいずれかを選択します:
   - すべてブロック
   - 高
   - 中
   - 低
5. デフォルトで **[Wi-Fi ネットワークのモニター]** チェックボックスを選択します。このオプションにより、安全対策が施されていない Wi-Fi ネットワークに接続したとき、および安全対策が施されていないクライアントの Wi-Fi（ホットスポット）へのアクセスが検出されたときに警告メッセージが表示されます。レポートはサーバーで生成されます。
6. ファイアウォール違反に関するアラートメッセージが必要な場合は、**[ファイアウォール違反が発生したときにアラートメッセージを表示する]** を選択します。
7. ブロックされたすべての接続をレポートする場合は、**[ファイアウォールレポートを有効にする]** チェックボックスを選択します。

8. ［例外］セクションにデフォルトの例外リストが表示されます。例外を追加または管理することができます。詳細については、例外の管理を参照してください。
9. 初期設定を復元するには、［**初期設定**］ボタンをクリックします。
10. 設定を保存するには、［**ポリシーの保存**］をクリックします。

ファイアウォールポリシーが［**すべてブロック**］に設定されている場合、ファイアウォールはすべての接続をブロックし、ネットワーク接続に影響を与える可能性のあるレポートを多数生成します。

セキュリティレベル

セキュリティレベル	説明
すべてブロック	例外なくすべてのインバウンドおよびアウトバウンドトラフィックをブロックします。これは最も厳格なセキュリティレベルです。
高	例外ルール付きで、インバウンドおよびアウトバウンドトラフィックをブロックします。例外ポリシーは、TCP、UDP、ICMP などの特定の通信プロトコル、IP アドレスを介したインバウンドまたはアウトバウンドトラフィックを許可または拒否するよう作成できます。
中	例外ルール付きで、すべてのインバウンドトラフィックをブロックし、すべてのアウトバウンドトラフィックを許可します。 例外ポリシーは、TCP、UDP、ICMP などの特定の通信プロトコル、IP アドレス、ポートを介したインバウンドまたはアウトバウンドトラフィックを許可または拒否するよう作成できます。例えば、特定の IP アドレスからの受信データを許可する場合、ユーザーはデータを受信できますが、その IP アドレスに送信することはできません。 このセキュリティレベルポリシーの特性を活かすには、インバウンドトラフィックの受信を許可し、アウトバウンドトラフィックをブロックすることをお勧めします。
低	すべてのインバウントとアウトバウンドトラフィックを許可します。 低いセキュリティレベルを適用する場合は、特定のプロトコル、IP アドレス、およびポートを使用して、特定のインバウンドおよびアウトバウンドデータを拒否する例外ルールを作成し、このセキュリティレベルポリシーの特性を活かすことをお勧めします。

例外ルールの管理

例外を使用すると、問題のないプログラムを許可して、高または中に設定されたファイアウォールレベルに関わらず通信を実行できます。例外によって、IP アドレスとポートを介したインバウンドとアウトバウンド通信をブロックまたは許可できます。

例外ルールの作成

例外ルールを持ったポリシーを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ファイアウォール]** を表示します。
3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. [例外] セクションで、**[追加]** をクリックします。
5. [例外の追加/編集] 画面で、[例外名] テキストボックスに名前を入力してプロトコルを選択します。

   プロトコルには次のものがあります:TCP、UDP、および ICMP。
6. **[次へ]** をクリックします。
7. [ローカル IP アドレス] で、IP アドレスまたは IP 範囲を入力して **[次へ]** をクリックします。

   [任意の IP アドレス] を選択した場合、IP アドレスを入力する必要はありません。
8. [TCP/UDP ポート] で、ポートまたはポート範囲を入力して **[次へ]** をクリックします。

   [すべてのポート] を選択すると、すべてのポートが選択されるため、ポートを入力する必要はありません。ローカル IP アドレス、IP 範囲、またはポートを指定する場合、この例外は着信に適用されます。
9. [リモート IP アドレス] で、IP アドレスまたは IP 範囲を入力して **[次へ]** をクリックします。

   [任意の IP アドレス] を選択すると、すべての IP アドレスがブロックされるため、IP アドレスを入力する必要はありません。リモート IP またはポートを指定した場合、例外は発信に適用されます。
10. [リモート TCP/UDP ポート] で、ポートまたはポート範囲を入力して**[次へ]** をクリックします。

    [すべてのポート] を選択すると、すべてのポートが選択されるため、ポートを入力する必要はありません。
11. [処置] で、**[許可]** または **[拒否]** のいずれかを選択します。

12. **[終了]** をクリックします。

    例外は、例外リストの上位に追加されます。例外の順序は例外ルールの優先順位により決まります。優先順位は降順です。[上へ] と [下へ] ボタンで例外ルールを移動できます。

13. **[ポリシーの保存]** をクリックします。

例外ルールの編集

必要な場合、自分で作成した例外ルールを編集することができます。例外ルールを編集するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ファイアウォール]** を表示します。
3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. [例外] セクションで、編集する例外を選択します。
5. [例外の追加/編集] 画面の [例外名] テキストボックスで名前を編集してプロトコルを編集します。

   プロトコルには次のものがあります:TCP、UDP、および ICMP。

6. **[次へ]** をクリックします。
7. 必要な場合、[ローカル IP アドレス] を編集してから、**[次へ]** をクリックします。
8. 必要な場合、[ローカル TCP/UDP ポート] を編集してから、**[次へ]** をクリックします。
9. 必要な場合、[リモート IP アドレス] を編集してから、**[次へ]** をクリックします。
10. 必要な場合、[リモート TCP/UDP ポート] を編集してから、**[次へ]** をクリックします。
11. [処置] で、**[許可]** または **[拒否]** のいずれかを選択します。
12. **[終了]** をクリックします。
13. **[ポリシーの保存]** をクリックします。

例外ルールの削除

作成した例外ルールを削除することができます。例外ルールを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ファイアウォール]** を表示します。

3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. [例外] セクションで、削除する例外を選択します。
5. **[削除]** をクリックします。

   選択した例外ルールが削除されます。
6. **[ポリシーの保存]** をクリックします。

例外ルールのエクスポート

作成した例外ルールをエクスポートすることができます。例外ルールをエクスポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ファイアウォール]** を表示します。
3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. [例外] セクションで、エクスポートしたい例外を選択します。
5. **[エクスポート]** をクリックします。

   [fwexcp.db を開く] ダイアログが表示されます。
6. **[ファイルに保存]** を選択します。
7. **[OK]** をクリックします。

   fwexcp.db データベースファイルをダウンロードします。

例外ルールのインポート

EPS の前のバージョンで作成された例外ルールをインポートすることができます。例外ルールをインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ファイアウォール]** を表示します。
3. ファイアウォールを有効にするには、**[ファイアウォールを有効にする]** チェックボックスを選択します。
4. **[インポート]** をクリックします。

   [ファイルアップロード] ダイアログが表示されます。
5. 「fwexcp.db」データベースファイルを選択します。
6. **[開く]** をクリックします。

   「fwexcp.db」データベースファイルをインポートします。

7. ［**ポリシーの保存**］をクリックします。

ウェブセキュリティ

この機能により、部署またはグループに対してセキュリティポリシーを作成し、ブラウザおよびフィッシング対策を有効にできます。悪意のあるウェブサイトまたはフィッシングウェブサイトをブロックします。必要に応じて、ウェブサイトへのアクセスを制限または許可することもできます。

次の表では、ウェブセキュリティの機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
ブラウジング保護	✓	✓	✓
フィッシング対策	✓	✓	✓
特定のカテゴリのウェブサイト（ウェブカテゴリ）へのアクセスを制限する	✓	✓	✓
特定のウェブサイトをブロックする	✓	✓	✓

ウェブセキュリティにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**設定**］>［**クライアント設定**］>［**ウェブセキュリティ**］を表示します。
3. ［ウェブセキュリティ］で、以下のいずれかまたは両方のチェックボックスを選択します:
   - ブラウジング保護
   - フィッシング対策
4. ユーザーがブロックされているウェブサイトにアクセスした場合に警告メッセージを表示するには、［**ウェブサイトがブロックされている時に警告メッセージを表示する**］チェックボックスを選択します。
5. ［ウェブカテゴリ］で、組織のセキュリティポリシーに応じて、カテゴリに基づいてウェブサイトへのアクセスを制限または許可します。カテゴリを有効にするには、［**ウェブサイトの特定のカテゴリへのアクセスを制限する**］チェックボックスを選択します。

   カテゴリをブロックすると、そのカテゴリに該当するすべてのウェブサイトがブロックされます。
6. ［指定されたウェブサイトをブロックする］セクションで、ブロックするウェブサイトを入力します。これにより、特定のウェブサイトが確実にブロックされます。こ

のセクションを有効にするには、**[特定のウェブサイトへのアクセスを制限する]** チェックボックスを選択します。

7. すべてのブロックされたウェブサイトのレポートを生成する場合は、**[ウェブセキュリティレポートを有効にする]** チェックボックスを選択します。

   このオプションを選択すると、ウェブの使用状況により、多数のレポートが生成されます。

8. 設定を保存するには、**[ポリシーの保存]** をクリックします。

ブラウジング保護設定

ユーザーが悪意のあるウェブサイトを閲覧すると、システムにファイルがインストールされることがあります。こうしたファイルがマルウェアを拡散したり、システムの処理速度を低下させたり、他のファイルを破壊したりします。このような攻撃は、システムに重大な被害を与える可能性があります。

グループのユーザーがインターネットにアクセスする際に、ブラウジング保護によって悪意のあるウェブサイトをブロックします。この機能を有効にすると、アクセスするサイトがスキャンされ、悪意があると判明した場合はブロックされます。

フィッシング対策設定

フィッシングは詐欺行為であり、通常はメールを通して、お客様の個人情報を盗もうとします。通常は、銀行、企業、サービスプロバイダ等、大手企業やよく知られたサイトからのメールを装ってメールを送信し、クレジットカード番号、社会保障番号、口座番号、パスワード等の個人情報を入手しようとします。

フィッシング対策により、管理者はユーザーがフィッシングや詐欺を行うウェブサイトにアクセスしないよう防ぐことができます。サイトにアクセスするとただちに、フィッシング行為が行われていないかスキャンします。フィッシング行為が発見された場合はブロックして、フィッシング行為を防止します。

ブラウジング保護およびフィッシング対策の除外

ブラウジング保護およびフィッシング対策の保護ポリシーに対して例外ルールを適用できます。問題がないにも関わらず、悪意のあるサイトやフィッシングサイトとして誤って検出されるサイトの URL を除外することができます。安全で問題のないことが確実な URL のみを除外することをお勧めします。

以下の方法で URL を除外できます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ウェブセキュリティ]** を表示します。
3. [ウェブセキュリティ] 画面で、**[除外]** ボタンをクリックします。

   [URL の除外] ダイアログが開きます。

4. [URL を入力してください] テキストボックスに URL を入力して、**[追加]** をクリックします。

   [誤って分類された URL の報告] ダイアログが開きます。悪意のあるサイトまたはフィッシングサイトとしてウェブサイトが検出されると、それらの誤って分類された URL について Seqrite ラボに報告できます。

5. 以下の理由から 1 つを選択します。
   - URL が有害として検出されている。
   - URL がフィッシングとして検出されている。
6. 誤った分類について報告する場合は、**[はい]** をクリックします。誤った分類について報告しない場合は、**[いいえ]** をクリックします。

   URL の除外リストに URL が追加されます。

7. 設定を保存するには、**[OK]** をクリックします。

設定	説明
追加	悪意のあるサイトまたはフィッシングサイトの検出から URL を除外できます。
削除	URL の除外リストから URL を削除できます。
レポート	URL が誤って分類された場合、報告します。

ウェブカテゴリ

多くの組織は、以下のような問題に直面する可能性があります:

- マルウェアによるシステムの感染
- 望ましくないウェブサイトを閲覧するユーザー
- 時間を無駄に過ごす従業員

これらの問題を回避するために、管理者はポリシーを定め、ユーザーと、ユーザーによるウェブサイトへのアクセスを管理する必要があります。

ウェブカテゴリ機能により、管理者はユーザーのインターネット閲覧行為を集中的に制御し管理できます。管理者は、グループの必要および優先度に基づいて、各グループに異なるセキュリティポリシーを作成できます。

ウェブカテゴリを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]**>**[ウェブセキュリティ]** を表示します。
3. ウェブカテゴリで、**[ウェブサイトの特定のカテゴリへのアクセスを制限する]** チェックボックスを選択します。

ウェブカテゴリが有効になり、各カテゴリへのアクセスを許可または拒否できます。

4. ［ステータス］欄で、［許可］または［拒否］のいずれかを選択します。

ウェブカテゴリの除外

ウェブカテゴリの保護ポリシーに対して例外ルールを適用できます。ウェブサイトカテゴリへのアクセスを制限したいが、制限カテゴリから特定のウェブサイトを許可したい場合に役立ちます。

そのようなウェブサイトを除外リストに登録するには、以下の方法に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［クライアント設定］>［ウェブセキュリティ］**を表示します。
3. ［ウェブカテゴリ］セクションで、**［ウェブサイトの特定のカテゴリへのアクセスを制限する］**チェックボックスを選択します。
4. **［除外］**ボタンをクリックします。

   ［URL の除外］ダイアログが開きます。
5. ［URL を入力してください］テキストボックスに URL を入力して、**［追加］**をクリックします。

   URL の除外リストに URL が追加されます。
6. サブドメインを除外するには、［**サブドメインも除外する**］チェックボックスを選択します。
7. 設定を保存するには、［OK］をクリックします。

設定	説明
追加	URL がブロックカテゴリに属していても、制限から除外できます。
削除	URL の除外リストから URL を削除できます。

指定されたウェブサイトをブロックする

この機能は、特定のウェブサイトへのアクセス制限や、ウェブサイトが適切なカテゴリに分類されていない場合に役立ちます。また、カテゴリ全体をブロックするよりも制限したいウェブサイトのリストが限られている場合にも役立ちます。

ウェブサイトをブロックするには、次の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［クライアント設定］>［ウェブセキュリティ］**を表示します。
3. ［ウェブセキュリティ］画面の［特定のウェブサイトをブロック］セクションで、**［特定のウェブサイトへのアクセスを制限する］**チェックボックスを選択します。

［指定されたウェブサイトをブロックする］の機能（［追加］、［削除］、［すべて削除］）が有効になります。

4. ウェブサイトを追加するには、**［追加］**をクリックします。
5. ［URL の追加］画面で、［URL を入力してください］テキストボックスに URL を入力します。
6. サブドメインをブロックするには、［**サブドメインもブロックする**］を選択します。例えば、www.google.com をブロックして［サブドメインもブロックする］を選択すると、mail.google.com などすべてのサブドメインもブロックされます。
7. 設定を保存するには、**［OK］**をクリックします。

［サブドメインもブロックする］機能は、Mac オペレーティングシステムのクライアントでは使用できません。

アプリケーションコントロール

アプリケーションの使用中に、組織は通常、以下の問題に直面します:

- 違法または偽のアプリケーションが、クライアントシステムにインストールされていないか。
- 悪意のあるアプリケーションがシステムを感染させていないか。
- 不要なアプリケーションがシステムを妨害していないか。

この機能を使用して、管理者はユーザーが特定のアプリケーションへのアクセスや、それらで作業することを許可または拒否して、望ましくないアプリケーションにアクセスできないようにすることができます。無許可のアプリケーションにユーザーがアクセスしようとした場合に、アプリケーションにアクセスできない理由を通知することもできます。

管理者は、グループまたは組織の必要に基づいて、様々なポリシーを作成できます。例えば、マーケティング部門のユーザーに対して、ファイル共有アプリケーションやウェブブラウザへのアクセスを許可して、その他すべてのアプリケーションへのアクセスを制限できます。会計部門に対しては、アーカイブツールやウェブブラウザのみへのアクセスを許可できます。

アプリケーションコントロール機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

アプリケーションコントロールにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**設定**］>［**クライアント設定**］>［**アプリケーションコントロール**］を表示します。

3. アプリケーションへのアクセスをブロックするには、**[無許可のアプリケーションにアクセスしたらブロックする]** チェックボックスを選択します。
4. ブロックされたアプリケーションにアクセスしたときに通知を送信するには、**[無許可アプリケーションがブロックされたときにクライアントに通知する]** を選択します。
5. 必要場な愛、各アプリケーションカテゴリに対して［許可］または［無許可］のいずれかを選択します。

   アプリケーションカテゴリの設定は、［カスタマイズ］ボタンをクリックしてカスタマイズすることもできます。
6. 設定を保存するには、**[ポリシーの保存] をクリックします。**

カスタム

アプリケーションの設定をカスタマイズして、特定のアプリケーションやカテゴリを許可または無許可にできます。アプリケーションカテゴリを許可または無許可にすると、そのカテゴリにリストされたすべてのアプリケーションが許可またはブロックされます。

例えば、アプリケーションカテゴリの「メールクライアント」で、「Thunderbird」と「MailWasher」へのアクセスを無許可にして、他のすべてのアプリケーションへのアクセスを許可できます。同様に、アプリケーション「Thunderbird」のバージョンに対して、「Thunderbird 1」へのアクセスを無許可にして、それ以外の Thunderbird のバージョンへのアクセスを許可できます。

以下の方法でアプリケーションをカスタマイズできます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］**>**［クライアント設定］**>**［アプリケーションコントロール］** を表示します。
3. ［アプリケーションコントロール］で、アプリケーションカテゴリに対して［カスタム］をクリックします。

   ［無許可のアプリケーションがアクセスされたらブロックする］オプションが選択されていることを確認してから、［カスタマイズ］オプションをクリックします。

   選択したアプリケーションカテゴリのアプリケーションのリストが表示されます。
4. アプリケーションのリストで、無許可としてマークしたいすべてのアプリケーション名を選択します。
5. 設定を保存するには、**[ポリシーの保存] をクリックします。**

アプリケーションの追加

デフォルトのリストに新しいアプリケーションを追加できます。オペレーティングシステムまたはその他のシステム固有の動作に属するアプリケーションまたはファイルを追加して無許可にすると、システムが誤作動を起こす可能性があります。そのため、オペ

レーティングシステムまたはその他のシステム関連プログラムの一部ではないアプリケーションを追加することをお勧めします。

以下の通りにアプリケーションを追加できます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**設定**］>［**クライアント設定**］>［**アプリケーションコントロール**］を表示します。
3. ［アプリケーションの追加］セクションで、［**アプリケーションのカスタマイズ**］ボタンをクリックします。
4. ［カスタムアプリケーション］画面で、［**アプリケーションの追加**］をクリックします。
5. アプリケーションのパスを参照して指定します。
6. ［アプリケーション名］テキストボックスに、アプリケーション名を入力します。
7. ［アプリケーションカテゴリ］リストで、カテゴリを選択します。

   デフォルトのアプリケーションリストに新しいアプリケーションを追加する理由を記入することもできます。これにより Seqrite ソフトウェア製品の品質を向上できます。

   Seqrite ラボにアプリケーションメタデータを送信することもできます。
8. アプリケーションを追加するには、［**アプリケーションの追加**］をクリックします。

アプリケーションメタデータを Seqrite ラボに送信

このオプションを使用して、アプリケーションのメタデータを Seqrite ラボに送信して、アプリケーションカテゴリに含めることができます。メタデータには、名前、バージョン、会社名、および MD5 などのアプリケーションの情報が含まれています。アプリケーションを追加した理由を提供することもできます。この情報は、アプリケーションコントロールモジュールの改良に役立ちます。

アプリケーションカテゴリには、数千のアプリケーションがその機能に基づいて登録されています。カテゴリをブロックすると、そのカテゴリに該当するすべてのアプリケーションがブロックされます。

アプリケーションカテゴリを無許可にしてもブロックされないアプリケーションがある場合、そのアプリケーションを送信してください。Seqrite がそのアプリケーションを分析して、カテゴリに登録します。

- 無許可のアプリケーションのコピーまたは名前の変更を行う際、アプリケーションブロックの画面が表示されることがあります。
- ソフトウェアアップデートのためにアプリケーションの実行可能ファイルがアップデートされる場合、一部の無許可のアプリケーションが起動することがあります。このようなアプリケーションは、Seqrite Endpoint Security コンソールに追加して、Seqrite ラボにメタデータを送信す

ることをお勧めします。

高度なデバイスコントロール

CD/DVD や、ペンドライブなどの USB デバイスといったデータストレージデバイスを使用する際、組織では次のような点が問題となります:

- 自動実行機能が感染を引き起こさないか。
- 不要なデータまたはアプリケーションがシステムを妨害していないか。

この機能により、管理者は様々な権限のあるポリシーを作成できます。例えば、管理者はリムーバブルデバイスへのアクセスを完全にブロックし、読み取り権限のみを付与して、外部デバイスに何も書き込めないようにできます。また、管理者設定されたデバイスへのアクセスをカスタマイズすることもできます。グループにポリシーが適用されると、アクセス権も適用されます。例外リストを使用して、デバイスコントロールポリシーからデバイスを除外することができます。

Windows 2000 および Windows XP SP1 以降のオペレーティングシステム では、USB ストレージデバイス以外のデバイスをブロックすることはできません。

高度なデバイスコントロールポリシーの作成

高度なデバイスコントロールにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[高度なデバイスコントロール]** を表示します。
3. デバイスコントロールを有効にするには、**[高度なデバイスコントロールを有効にする]** チェックボックスを選択します。
4. [デバイスタイプのアクセスポリシーを選択する] で、以下のオプションからカテゴリを選択します:
   - ストレージデバイス
   - カードリーダー
   - ワイヤレス
   - モバイルとポータブルデバイス
   - インター
   - フェース
   - カメラ
   - その他
5. カテゴリ内の該当するデバイス用に以下のいずれかを選択します:

- 拒否
- 許可
- 読み取り専用

カテゴリのオプションが利用できるのは、そのメインカテゴリのチェックボックスを選択した場合のみです。

6. 設定を保存するには、**[ポリシーの保存] をクリックします。**

   このポリシーはリストで設定されたすべてのデバイスに適用されます。デバイスを追加しても、ポリシーをカスタマイズしない限り、同じポリシーが適用されます。

注意:

Windows クライアント

- NTFS のみ部分暗号をサポートしています。
- GUID パーティションテーブル (GPT) パーティションスタイルの USB ドライブは追加・認証できません。
- 認証済みの暗号化されたデバイスをフォーマットした場合、そのデバイスは無許可のデバイスとして扱われます。このため、管理者がデバイスコントロールで再度デバイスを追加し、ポリシーを設定する必要があります。
- SEPS 7.1 サーバーのネットワーク内システムに接続された USB デバイスは、**[管理者設定]**> **[サーバー]**>**[デバイスの管理]**> **[デバイスの追加]**>**[ネットワークデバイス]** リストには列挙されません。
- 一部のデバイス (Nokia 社製携帯電話、BlackBerry フォンなど) では、デバイスアクセス権を適用するためにシステムの再起動またはデバイスの再接続が必要な場合があります。
- 高度なデバイスコントロールから SATA コントローラをブロックする際、実際にはブロックが実行されていなくても、SATA コントローラがブロックされたことを示す画面が頻繁に表示されます。
- ウェブカムや Bluetooth でセッションが継続している場合、アクセス権を変更してブロックしても継続中のセッションは中断されません。アクセス権を適用するには、デバイスを再接続するかシステムの再起動が必要です。
- 外部 CD/DVD リーダーは **[管理者設定]**>**[サーバー]**>**[デバイスの管理]**>**[デバイスの追加]**>**[ネットワークデバイス]** リストに列挙されず、例外が生成されることもありません。

Mac クライアント

- SEPS の高度なデバイスコントロールで [読み取り専用] のオプションが選択されており、USB デバイスが接続されている場合、Finder の左フレームからしばらくデバイスにアクセスできないことがあります。

- USB デバイスがマシンに接続された状態で Mac クライアントをインストールすると、一瞬そのデバイスがマウント表示されなくなる場合があります。
- Mac クライアントのインストール時に NTFS USB デバイスがマシンに接続されていると、その USB デバイスが数秒間 2 つ見える場合があります。
- ターミナルコマンドを使用して USB デバイスをマウントまたはアンマウント表示すると、デバイスコントロールポリシーはそのデバイスに適用されません。
- FAT USB をマシンに取り付けた状態で Mac OSX 10.9 に Mac クライアントをインストールすると、デバイスはマウント表示されません。デバイスをマウント表示するには、取り外して再度取り付ける必要があります。
- iOS デバイス、内部カードリーダー、ウェブカム、CD/DVD、携帯電話および HFS 暗号化デバイスは、デバイスアクセス権を適用するためにデバイスの再接続が必要な場合があります。
- 例外機能は Bluetooth、Wi-Fi、ウェブカム、および外部 CD/DVD には対応していません。
- 「USB マスストレージ」モードで接続される iOS デバイス以外のすべての携帯電話は、「USB ストレージデバイス」カテゴリで検出されます。
- MTP モードで接続されている携帯電話は「Windows ポータブルデバイス」で検出されます。
- BlackBerry 携帯電話が「Sync Media」モードで Mac システムに接続されている場合、ブロッキング機能は動作しません。
- USB ストレージデバイスは Mac OS 拡張（ジャーナル、暗号化）ファイルフォーマットに変換されません。
- ブロック権限が iOS デバイスに設定されると、Mac システムに接続されている場合、iOS デバイスはブロックされません。この動作は Mac OS 10.12 のみに適用されます。

Linux クライアント

- UMS ベースの電話がサポートされている場合、MTP/PTP ベースの電話はサポートされません。
- EPS サーバーの内部 CD/DVD に設定された［読み取り専用］のオプションは、Linux クライアントではブロックされます。
- ワイヤレスアダプターはサポートされません。
- Bluetooth USB ドングルは、一部のオペレーティングシステムではサポートされません。
- サポートされるすべての Linux OS で、CD-DVD にブロックモードが設定されている場合、内部 CD-DVD トレイが複数回自動開閉することがあります。
- DC 設定で、読み取り専用モードが許可モードに変わると、USB ドライブも機能しなくなる場合があります。

- UMS 携帯電話番号は読み取り専用モードで機能しません。デバイスで利用可能なオプションでモードを変更すると、エンドポイントに接続されます。特定のモードでデバイスのプラグを抜くと、自動的にモードが変わりません。

デバイスコントロールリストに例外を追加する

許可された人物が使用するリムーバブルデバイスに例外を追加して、デバイスをポリシーから除外することができます。

例外リストにデバイスを追加するには、まずサーバーに追加してデバイスを許可する必要があります:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** >**[サーバー]**>**[デバイスを管理]** を表示します。
3. **[デバイスの追加]** をクリックします。
4. [ネットワークデバイス]、[USB デバイス] または [その他のデバイス] から選択します。

   USB デバイスを追加したい場合、[USB デバイス] を選択し、[デバイスの追加] ダイアログボックスにデバイス名を追加して [OK] をクリックします。

   ネットワークデバイスを追加したい場合、[ネットワークデバイス] を選択します。ネットワークで検出されたデバイスのリストが表示されます。デバイスを選択し、[OK] をクリックします。

   その他のデバイスを追加したい場合、[その他のデバイス] オプションを選択し、デバイスタイプを選択します。[デバイスの追加] ダイアログボックスに、デバイス名、デバイスベンダー ID、プロダクト ID、シリアル番号などの必要な情報を追加します。[OK] をクリックします。
5. **[設定]**>**[クライアント設定]**>**[高度なデバイスコントロール]** をクリックします。

   [高度なデバイスコントロールを有効にする] オプションが選択されていることを確認します。
6. **[例外]**をクリックします。
7. **[追加]** をクリックします。
8. 1 つ以上のデバイスを選択して、リストに表示されたデバイスから例外を追加します。
9. **[OK]** をクリックします。
10. [管理デバイス] 確認ダイアログボックスで **[はい]** をクリックします。
11. 必要に応じてアクセス権を設定します。
12. **[ポリシーの保存]** をクリックします。

同じデバイスを「モデル別 USB」オプションと「USB デバイス」オプションから追加し、「ブロック/許可/読み取り専用」アクセス権を両方のデバイスタイプに設定する場合、「モデル別 USB」のアクセス権セットが優先されます。

デバイスをサーバーに追加

デバイスをサーバーに追加する方法は、[デバイスの管理] をご覧ください。

データ喪失防止

SEPS 7.1 のデータ喪失防止（DLP）機能を使用して、機密企業データの不正な紛失、窃盗、漏えいを防ぐことができます。

エンドポイントで DLP を有効にする必要があります。DLP を有効にするには、DLP 機能の有効化を参照してください。

機密データの不正な漏えいを引き起こそうとしたユーザーについて、レポートを確認することもできます。データ喪失防のレポートを参照してください。

DLP 機能は、以下のチャンネルを通じて実行される、あらゆる不正な活動を防ぐことができます:

- プリントスクリーンオプションを使用してスクリーンショットを保存すること（Windows プラットフォームのみ対応）。このファイル/データは監視されません。
- リムーバブルデバイスを使用してデータをコピーすること（Windows プラットフォームのみ対応）。

  選択したファイルタイプに「リムーバブルデバイスをモニター」オプションが選択されている場合、リムーバブルデバイスは「読み取り専用」モードになります。
- UNC パスまたはマップしたネットワークドライブを使用して、アクセスしたネットワーク共有を使用すること（Windows プラットフォームのみ対応）。
- クリップボードを使用して、あるアプリケーションから別のアプリケーションに情報をペーストすること。
- プリンター活動を使用して、ローカルおよびネットワークプリンタから印刷すること。このファイル/データは監視されません。（Windows プラットフォームのみ対応）
- 第三者アプリケーション/サービスのオンラインサービスを使用して、メール、ファイル共有アプリ、クラウドサービス、ウェブブラウザ、ソーシャルメディアを利用するその他のアプリケーションなどのデータを送信すること。

モニターしたいデータのタイプを特定することもできます:

1. ファイルタイプ
   - グラフィックファイル（音声、動画、画像）
   - Office ファイル（MS Office、Open Office、Kingsoft Office）

- プログラミングファイル
- その他のファイルタイプ（圧縮ファイルなど）
- カスタム拡張ファイル

2. 機密データ
   - クレジット/デビットカードなどの機密データ
   - 社会保障番号（SSN）、メール ID、電話番号、運転免許番号、健康保険番号、パスポート番号、ID、インターナショナル・バンキング・アカウント・ナンバー（IBAN）、個人のマイナンバー、会社のマイナンバーなどの個人情報。
3. ユーザー定義辞書

   通信で使用する際にフラグが必要な単語/文字列を指定します。

   機密データとユーザー定義辞書データは、メール、インスタントメッセンジャー通信の件名やメッセージ本文に含まれている場合、モニターおよびブロックされません。

情報漏えいが試みられた際にメール通知で通知を受けるか、試みの実行を防ぐか、選択することができます。

- データ喪失防止機能は、Endpoint Security のビジネスおよびトータル系統ともに用意されていません。この機能を利用するには、DLP パックを別途購入する必要があります。
- データ喪失防止機能は EPS SME 系統ではサポートされていません。
- DLP 機能は Windows 2000 オペレーティングシステムでは使用できません。

データ漏えいの防止

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[クライアント設定]** >**[データ喪失防止]** を表示します。

   [データ喪失防止を有効にする] チェックボックスを選択します。データ漏えいが試みられるエンドポイントについて、アラートメッセージのオプションを選択することができます。
3. 次のオプションからモニターしたいチャンネルを選択します:
   - プリントスクリーン（Windows プラットフォームのみ対応）
   - リムーバブルデバイスをモニター（Windows プラットフォームのみ対応）
   - ネットワーク共有をモニター（Windows プラットフォームのみ対応）
   - クリップボードをモニター
   - プリンター活動（Windows プラットフォームのみ対応）

- アプリケーション/オンラインサービス経由のデータ転送をモニター

4. ［アプリケーション］ドロップダウンリストをクリックして、データ盗難の試みをモニターするアプリケーションを選択します。次のいずれかを実行してください:

   グループのアプリケーションをすべて選択できます。

   - グループキャレットを拡大して、アプリケーションをひとつずつ選択します。
   - Mac グループアイコンをクリックして、すべての Mac プラットフォームアプリケーションを選択します。
   - Windows アイコンをクリックして、すべての Windows アプリケーションを選択します。
   - グループキャレットを拡大して、ウェブブラウザをすべて、またはひとつずつ選択します。
   - グループキャレットを拡大して、メールアプリケーションをすべて、またはひとつずつ選択します。
   - グループキャレットを拡大して、インスタントメッセージアプリケーションをすべて、またはひとつずつ選択します。
   - グループキャレットを拡大して、ファイル共有アプリケーション/クラウドサービスをすべて、またはひとつずつ選択します。
   - グループキャレットを拡大して、ソーシャルメディア/その他アプリケーションをすべて、またはひとつずつ選択します。

5. ファイルタイプ、機密データ、およびユーザー定義辞書の設定を行います。
6. ［ブロックとレポート］や［レポートのみ］など、試みが実行された後に実施する処置を設定します。

   ［レポートのみ］の処置では、アラートプロンプトは表示されません。

7. ［設定例外］セクションで、以下を実行します:

   i. ［ドメイン］タブで、**［ドメイン例外を有効にする］**チェックボックスを選択します。
   ii. データ喪失防止から除外するドメインを選択します。
   iii. ［アプリケーション］タブで、**［アプリケーション例外を有効にする］**チェックボックスを選択します。
   iv. データ喪失防止から除外するアプリケーションを選択します。
   v. ［ネットワーク共有］タブで、**［ネットワーク共有例外を有効にする］**チェックボックスを選択します。
   vi. データ喪失防止から除外するネットワーク共有を選択します。

8. **［ポリシーの保存］**をクリックします。

Mac クライアントの場合:

- 機密およびユーザー辞書データは、メールまたはメッセンジャー通信の件名、メッセージ本文ではブロックされません。
- モニターされるファイルタイプがダウンロードされると、プロンプトとレポートが生成されます。
- Unicode データを含む特定のファイルタイプ（POT、PPT、PPTX、DOC、DOCx、XLS、XLSX、RTF）はブロックされません。

Seqrite は高度なスキャン機能であるデータ保存スキャンを提供します。この機能を使用して、特定のタイプのデータを様々なフォーマットで検索することができます。

ファイル活動モニター

この機能によって、お客様のコンピュータ、ネットワークドライブ、リムーバブルドライブ上の機密ファイルに関連する、あらゆる疑わしい活動をモニターすることができます。デフォルトのファイルセットの他、モニターしたいファイルタイプをカスタマイズおよび選択することができます。選択したファイルタイプに対するコピー、削除、名前の変更などの処置をモニターすることができます。[レポート] ページから、ファイル活動のレポートを生成できます。

ファイル活動モニター機能は、Windows および Mac オペレーティングシステムのクライアントで使用できます。

ファイル活動モニターを有効にする

ファイル活動モニターを有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[ファイル活動モニター]** を表示します。
3. **[ファイル活動モニターを有効にする]** を選択します。
4. [ドライブ内でモニターするファイルタイプとイベントを選択する] エリアで、ファイル活動をモニターしたいドライブにチェックマークを付けて選択します。

   イベントの選択は、リムーバブルドライブ、ネットワークドライブには対応していません。ローカルドライブには「削除」活動のみ選択してモニターできます。リムーバブルドライブには「すべてのファイル」をモニターするように選択可能です。

5. [ファイルタイプ] リストでは、すべてのドライブタイプでモニターしたいファイルタイプを選択するか、[すべてのファイルタイプ] チェックボックスを使用して、一覧表示されたすべてのファイルタイプを選択できます。
6. [カスタムファイル] では、除外したいファイルタイプを自分で追加することができます。プラスのっ記号 [+] をクリックして、モニターする新しいファイルタイプ拡

張子を追加することができます。削除アイコンを使用して、ファイルまたはフォルダタイプを削除します。

7. モニターから除外したいフォルダパスを入力します。例: C:¥JSmith.

   除外からフォルダパスを削除するには、リスト項目をクリックすると表示される削除アイコンをクリックします。削除アイコンをクリックすると、削除処置を確認するメッセージボックスが表示されます。

8. **[ポリシーの保存]** をクリックします。

アップデート設定

作業環境に多数のシステムがインストールされている場合、管理者にとって、すべてのエンドポイントのセキュリティパッチをアップデートする方法が課題となります。

この機能により、エンドポイントのアップデートを自動的に取得するポリシーを作成できます。異なるクライアントが異なるソースからアップデートを取得するポリシーを作成できます。異なるソースからアップデートを取得することで、単一サーバーの負荷を軽減します。

次の表では、アップデート設定の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
自動アップデートを有効にする	✓	✓	✓
アップデート通知ウィンドウを表示する	✓	✓	X
周波数	✓	✓	X
アップデートモード	✓	✓	✓

[アップデート設定] にポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[アップデート設定]** を表示します。
3. アップデートを自動的に取得するには、**[自動アップデートを有効にする]** を選択します。
4. アップデートを取得したときに通知ウィンドウを表示するには、[**アップデート通知ウィンドウを表示する**] を選択します。
5. [頻度] で、アップデートを取得するスケジュールを設定します。

- 自動
- スケジュールに従って

  [スケジュールに従って] を選択すると、[毎日の開始時刻] と [繰り返す] が有効になり、必要に応じて設定できます。

6. [アップデートモード] で、EPS がプライベート IP（プライベート IP からパブリック IP への変換）にインストールされると、以下のアップデート設定を設定することができます:

   ローカルクライアントの場合

   - インターネットからダウンロードする
   - Endpoint Security サーバーからダウンロードする
   - 指定されたアップデートサーバーからダウンロードする

   リモートクライアントの場合

   - インターネットからダウンロードする
   - 指定されたアップデートサーバーからダウンロードする

   異なるポリシーを作成するために、[アップデートモード] に異なるオプションを選択できます。

   [指定されたアップデートサーバーからダウンロードする] を選択すると、リストにアップデートサーバーの場所を入力する必要があります。

7. 設定を保存するには、**[ポリシーの保存]** をクリックします。

- [指定されたアップデートサーバーからダウンロードする] を選択すると、Linux クライアントは Endpoint Security サーバーからアップデートをダウンロードします。
- クライアントが（システムトレイの [ウィルス保護] アイコンを右クリックして）[インターネットからアップデート] を有効にしている場合、クライアントは Endpoint Security サーバーからアップデートを先に取得します。サーバーにアクセスできない場合、アップデートはインターネットセンターから自動的に取得されます。
- [インターネットからアップデート] は、Microsoft Windows と MAC オペレーティングシステムのクライアントのみで使用できます。
- アスタリスク（*）の付いた機能が適用されるクライアントについては、比較表をご覧ください。

アップデートサーバーの場所の入力

[指定されたアップデートサーバーからダウンロードする] オプションを選択する場合、アップデートを取得するアップデートサーバーの場所を入力してください。大規模なネットワークの場合、複数のアップデートマネージャを展開することもできます。エンドポイントが異なるサーバーから更新を取得できるため、負荷分散ができます。ネットワークに複数のアップデートマネージャを設定している場合、それらの URL をこのセク

ションに指定します。クライアント設定で、これらの場所からアップデートするようにクライアントを設定できます。

サーバーの場所を入力するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ダッシュボードで［**ホーム**］をクリックします。
2. ホームページで、製品名とバージョンの詳細の横にある［**アップデートマネージャ**］リンクをクリックします。
3. ［アップデートマネージャ］画面で、［**代替アップデートマネージャ**］をクリックします。
4. ［アップデートマネージャの URL を入力してください］テキストボックスに、URL を入力して、［**追加**］をクリックします。

   優先度に合わせて URL を配置できます。追加した URL は［アップデート設定］のアップデートサーバーの場所リストで使用できます。

インターネット設定

この機能により、管理者はインターネット接続を有効にする必要があるクライアントモジュールに対するポリシー作成の選択の幅が広がります。サーバーおよびポートに異なる設定を行い、クイックアップデート、スパム対策、ウェブセキュリティ、およびメッセンジャーなどのクライアントモジュールがインターネットに接続できるようにします。これは、デフォルトでインターネット接続が許可されていない安全な作業環境でクライアントモジュールを機能させるのに非常に役立ちます。

インターネット設定にポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**設定**］>［**クライアント設定**］>［**インターネット設定**］を表示します。
3. インターネットのプロキシ設定を行うには、［**プロキシ設定を有効にする**］を選択します。

   プロキシ設定の詳細が有効になります。
4. ［プロキシサーバー］にサーバー名を入力します。
5. ［ポート］にポート番号を入力します。

   ファイアウォールまたはプロキシサーバーを使用する場合、認証ルールも入力できます。この場合、［認証］にユーザー名とパスワードを入力します。
6. 設定を保存するには、［**ポリシーの保存**］**をクリックします。**

インターネット設定機能は、Microsoft Windows、Mac、および Linux オペレーティングシステムのクライアントで使用できます。

パッチサーバー

この機能を使用して、欠落しているパッチの確認とインストールするためにパッチサーバーを設定することができます。

パッチサーバー設定にポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定] > [クライアント設定] > [パッチサーバー]** を表示します。
3. **[パッチサーバーを有効にする]** チェックボックスを選択します。
4. 欠落しているパッチの確認やインストールのためにエンドポイントで使用されるリストからパッチサーバーを選択します。
5. **[エンドポイントのローミングに Microsoft パッチサーバーを使用して欠落しているパッチをスキャンしてインストールする]** チェックボックスを選択します。
6. 設定を保存するには、**[ポリシーの保存] をクリックします。**

Microsoft Windows OS のクライアントのみがパッチサーバー機能を利用できますが、Mac と Linux オペレーティングシステムのクライアントにはサポートされません。

一般設定

この機能により、クライアントがクライアント設定にアクセスしてパスワードを変更することを許可するポリシーを作成し、セーフモードプロテクション、セルフプロテクション、およびニュースアラートを有効または無効にできます。

次の表では、一般設定の機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
クライアント設定へのアクセスを許可する	✓	✓	✓
セーフモードプロテクションを有効にする	✓	✓	X
セルフプロテクションを有効にする	✓	✓	X
ニュースアラートを有効にする	✓	X	X

一般設定にポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. **[設定]>[クライアント設定]>[一般設定]** を表示します。
3. クライアントの設定にアクセスできるようにするには、**[クライアント設定へのアクセスを許可する]*** をクリックします。

   パスワード設定が有効になります。
4. [パスワードの入力] に、パスワードを入力して [パスワードの再入力] に再度同じパスワードを入力します。

   クライアントはこれらのパスワードをクライアント設定へのアクセスに使用します。
5. セーフモードプロテクションを有効にするには、**[セーフモードプロテクションを有効にする]*** を選択します。
6. セルフプロテクションを有効にするには、**[セルフプロテクションを有効にする]*** を選択します。
7. 様々なインシデントに関するニュースアラートを取得するには、**[ニュースアラートを有効にする]*** を選択します。
8. 設定を保存するには、**[ポリシーの保存] をクリックします。**

アスタリスク（*）の付いた機能が適用されるクライアントについては、比較表をご覧ください。

スケジュール設定

スキャンを定期的に実行すると、システムがクリーンで安全に保たれます。大規模な組織では、物理的に分離した環境にクライアントシステムがインストールされている場合があります。

すべてのシステムのスキャンをいつどのように開始するかを集中的に管理するために、管理者はポリシーを作成する必要があります。この機能により、クライアントシステムに対するスキャンスケジュールのポリシーを作成できます。

以下のスキャンをスケジュール設定できます:

クライアントスキャン

この機能により、都合の良い時刻に自動的にクライアントのスキャンを開始するポリシーを作成できます。スキャンを日次または週次で実行するかを定義し、スキャンモード（クイックスキャン、システム全体のスキャン）を選択できます。スキャン時にアンチマルウェアも有効にできます。これは他の自動保護機能を補完するもので、クライアントシステムがマルウェアから保護された状態を保ちます。

次の表では、クライアントスキャンの機能の比較を示しています。これらの機能は異なるオペレーティングシステム上の異なる Seqrite Endpoint Security クライアントに適用可能です:

機能	クライアント		
	Windows	Mac	Linux
クライアントスケジュールスキャン	✓	✓	✓
アンチマルウェアスキャン設定	✓	X	X

クライアントスキャンにスキャンスケジュールポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[スケジュール設定]>[クライアントスキャン]** を表示します。
3. 次の設定を行います。[クライアントスケジュールスキャン]、[スキャナ 設定]、および [アンチマルウェアスキャン設定]。
4. 設定を保存するには、**[ポリシーの保存]** をクリックします。

[デフォルト] ボタンをクリックしていつでもデフォルト設定に戻すことができます。

クライアントスケジュールスキャン

この機能により、特定の頻度でクライアントのスキャンスケジュールを定義できます。

クライアントスケジュールスキャンを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[スケジュール設定]>[クライアントスキャン]** を表示します。
3. [クライアントスケジュールスキャン] で、**[スケジュールスキャンを有効にする]** を選択します。
4. [頻度] で、[毎日] または [毎週] オプションを選択します。
5. [開始時刻] で、時刻を時間と分で設定します。
6. クライアントのスキャンを繰り返す場合は、**[スキャンを繰り返す]** を選択して、スキャンを繰り返す間隔を設定します。
7. クライアントがオフラインの場合に通知を取得するには、**[クライアントがオフラインの場合に通知する]** を選択します。

スキャナ設定

この機能により、クライアントのスキャンに適用するスキャンモードまたはスキャンする項目を定義できます。

スキャナ設定を行うには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[スケジュール設定]**>**[クライアントスキャン]** を表示します。
3. [スキャナ設定] セクションの [スキャン方法] で、以下のスキャンモードを選択します。
   - **クイックスキャン**（オペレーティングシステムがインストールされているドライブをスキャン）
   - **システム全体のスキャン**（すべての固定ドライブをスキャン）
4. 最適な設定を行うには、**[自動]** オプションを選択します。
5. 高度な設定を行うには、**[高度なスキャン]** オプションを選択します。

   [高度なスキャン] オプションを選択すると、スキャン項目およびスキャンタイプなどの詳細な設定を行うことができます。
6. [スキャンする項目の選択] で、次のいずれかを選択します:
   - 実行可能ファイルをスキャン
   - すべてのファイルをスキャン（時間がかかります）
   - パックファイルのスキャン
   - 受信ボックスのスキャン
   - アーカイブファイルをスキャン
7. [アーカイブファイルをスキャン] オプションを選択すると、次のオプションも設定できます:
   - アーカイブスキャンのレベル:レベル 5 まで設定できます。
   - アーカイブファイルでウイルスが見つかったときに実行する処置を選択してください。ウイルスが検出された場合の対処を、[削除]、[隔離]、[スキップ] から 1 つ選択します。
8. [ウイルスが見つかったときに実行する処置を選択してください] で、次のいずれかの処置を選択します:修復、削除、スキップ。

アンチマルウェアスキャン設定

この機能により、マルウェアをスキャンできます。

アンチマルウェアスキャン設定を行うには、以下の手順に従ってください:

1. マルウェアのスキャンを有効にするには、**[アンチマルウェアスキャンを実行する]** チェックボックスを選択します。
2. [マルウェアが見つかったときに実行する処置を選択する] で、次のいずれかの処置を選択します。[クリーニング] および [スキップ]。

パックファイルのスキャン、受信ボックスのスキャン、およびアンチマルウェアスキャン設定は、Windows オペレーティングシステムのクライアントのみで使用できます。

アプリケーションコントロール

この機能を使用して、都合の良い時刻に自動的にクライアントにインストールされるアプリケーションのスキャンを開始するポリシーを作成することができます。クライアントに存在する許可または無許可のアプリケーションをスキャンすることもできます。

アプリケーションのスキャンにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[アプリケーションコントロール]** を表示します。
3. 次の設定を行います。[アプリケーション 1 コントロール]、[スケジュールスキャン]、および [スキャンとレポート]。
4. 設定を保存するには、**[ポリシーの保存] をクリックします。**

[デフォルト] ボタンをクリックしていつでもデフォルト設定に戻すことができます。

アプリケーションコントロールスケジュールスキャン機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

アプリケーションコントロールスケジュールスキャン

この機能により、スケジュールを定義して、都合に合わせて、または指定した頻度でアプリケーションをスキャンできます。

アプリケーションコントロールスケジュールスキャンを設定するには、以下の手順に従ってください:

1. [スケジュールスキャンのチューンアップ] で、**[スケジュールスキャンを有効にする]** を選択します。
2. [頻度] で、[毎日] または [毎週] オプションを選択します。
3. [開始時刻] で、時刻を時間と分で設定します。
4. アプリケーションのスキャンを繰り返す場合は、[スキャンを繰り返す] を選択して、スキャンを繰り返す間隔を設定します。
5. クライアントがオフラインの場合に通知を取得するには、**[クライアントがオフラインの場合に通知する]** を選択します。

スキャンとレポート

この機能では、様々な方法でアプリケーションのスキャンを開始できます。

［スキャンとレポート］で、以下のいずれかのオプションを選択します:

- 無許可アプリケーション
- 無許可および許可アプリケーション
- インストール済みのすべてのアプリケーション

チューンアップ

この機能を使用すると、ポリシーを作成して、都合の良い時間や間隔でクライアントを自動的にチューンアップすることができます。

チューンアップのポリシーを作成するには、以下の手順に従ってください:

1. 次の設定を行います。［チューンアップスケジュールスキャン］および［チューンアップ設定］。
2. 設定を保存するには、**［ポリシーの保存］をクリックします。**

注意:［デフォルト］ボタンをクリックしていつでもデフォルト設定に戻すことができます。

チューンアップスケジュールスキャン機能は、Windows デスクトップオペレーティングシステムのクライアントのみで使用できます。

チューンアップスケジュールスキャン

この機能を使用すると、スケジュールを定義して、希望する頻度でクライアントをチューンアップできます。

チューンアップスケジュールスキャンを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［スケジュール設定］>［チューンアップ］**を表示します。
3. ［チューンアップスケジュールスキャン］で、**［スケジュールスキャンを有効にする］**チェックボックスを選択します。
4. ［曜日］で曜日を選択します。
5. ［開始時刻］で、時刻を時間と分で設定します。
6. スキャンを繰り返す場合は、［スキャンを繰り返す］を選択して、スキャンを繰り返す間隔を設定します。
7. クライアントがオフラインの場合に通知を取得するには、**［クライアントがオフラインの場合に通知する］**を選択します。

チューンアップ設定

この機能を使用して、チューンアッププロセスの実行方法とクリーニング対象を定義できます。以下のいずれか、またはすべてのオプションを選択します:

- ディスクのクリーンアップ
- レジストリのクリーンアップ
- 次回起動時にデフラグ

脆弱性スキャン

この機能を使用して、クライアントの脆弱性スキャンのスケジュールを設定し、クライアントの潜在的な脆弱性をスキャンすることができます。

脆弱性スキャンのポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[スケジュール設定]**>**[脆弱性スキャン]** を表示します。
3. 次の設定を行います。[脆弱性スキャン] および [スキャンとレポート]。
4. 設定を保存するには、**[ポリシーの保存] をクリックします。**

   [デフォルト] ボタンをクリックしていつでもデフォルト設定に戻すことができます。

脆弱性スキャン機能は、Windows オペレーティングシステムのクライアントのみで使用できます。

脆弱性スキャンのスケジュール

この機能により、都合に合わせてクライアントの脆弱性スキャンのスケジュールを定義できます。

脆弱性スキャンをスケジュールにするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]**>**[スケジュール設定]**>**[脆弱性スキャン]** を表示します。
3. [脆弱性スキャン] で、**[スケジュールスキャンを有効にする]** チェックボックスを選択します。
4. [曜日] で曜日を選択します。
5. [開始時刻] で、時刻を時間と分で設定します。
6. スキャンを繰り返す場合は、**[スキャンを繰り返す]** を選択して、スキャンを繰り返す間隔を設定します。
7. クライアントがオフラインの場合に通知を取得するには、**[クライアントがオフラインの場合に通知する]** を選択します。

スキャンとレポート

［スキャンとレポート］で、以下のいずれかを選択します:

- Microsoft アプリケーションおよびその他のベンダーのアプリケーション
- Microsoft アプリケーションのみ
- その他のベンダーのアプリケーションのみ

保存データスキャン

この機能を使用して、様々なフォーマットの特定のデータタイプの検索、およびエンドポイントやリムーバブルデバイスにある機密情報の検出を行うことができます。詳細については、保存データスキャンを参照してください。

保存データスキャンを実施するには、エンドポイントで DLP を有効にしなければなりません。DLP を有効にするには、DLP 機能の有効化を参照してください。

保存データスキャンにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［スケジュール設定］>［保存データスキャン］**を表示します。
3. ［スケジュールスキャンを有効にする］を選択して、スキャンの頻度と時間を設定します。

   クライアントがオフラインの場合、［スキャンを繰り返して通知する］を選択できます。
4. 設定を保存するには、**［ポリシーの保存］をクリックします。**

パッチスキャン

パッチスキャンはインストールされた製品やクライアントマシンのオペレーティングシステム（OS）で欠落しているパッチを確認します。確認が終了した後、結果が生成されます。

パッチスキャンにポリシーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［スケジュール設定］>［パッチスキャン］**を表示します。
3. **［自動パッチスキャンを有効にする］**チェックボックスを選択して、スキャンの頻度と時間を設定します。

   ［クライアントがオフラインの場合通知する］を選択することもできます。

4. ［パッチインストール設定］セクションで［**重大度レベルが同等かそれ以上で欠けているソフトウェアパッチの自動インストール**］チェックボックスを選択してリストから重大度レベルを選択します。
5. ［**システムの自動再起動を許可する**］チェックボックスを選択します。
6. パッチのインストールでエンドポイントを除外するには、［**ここをクリック**］リンクをクリックします。

   ［パッチインストールの除外］ダイアログが表示されます。

   i. 必要に応じて、［EPS ネットワークでサーバー OS のあるエンドポイントを除外する］チェックボックスを選択します。
   ii. ［**以下のエンドポイントを除外する**］チェックボックスを選択します。
   iii. エンドポイント名または IP を入力します。
   iv. ［**追加**］をクリックします。エンドポイントの詳細が表示されます。エンドポイントを削除することができます。削除するには、リストでエンドポイントを選択し、［**削除**］をクリックします。
   v. ［**適用**］をクリックします。
7. 設定を保存するには、［**ポリシーの保存**］**をクリックします。**

Chapter

11

レポート

このメニューは、クライアントの最新情報を提供し、ウイルスインシデント、ポリシーおよびアップデートに関する総合的なログを保持します。接続しているすべてのオンラインクライアントの最新ステータス、およびオフラインクライアントの前回のアップデートレポートを提供します。これらのログを使用して、組織のウイルス対策ポリシーを査定して、感染のリスクが高いクライアントを特定します。また、これらのログによって、クライアントが最新のアップデートを取得しているかどうかを検証できます。

クライアント

この機能により、すべてのオンラインおよびオフラインクライアントのレポートを確認できます。クライアントのレポートは次のモジュールで利用できます:ウイルススキャン、アンチマルウェアスキャン、ウェブセキュリティ、チューンアップ、デバイスコントロール、アプリケーションコントロール、不正侵入防御・検知システム（IDS/IPS)、ファイアウォール、脆弱性スキャン、ファイル活動モニター、アセット管理。

ウイルススキャンのレポートの表示

この機能により、ウイルス対策、スキャナスケジューラ、メモリスキャン、およびメール保護モジュールによるクライアントのスキャン後に、ウイルスが見つかったかどうかに関するレポートを生成できます。

ウイルススキャンのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[ウィルススキャン]** を表示します。
3. ［全般レポート］ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストフィールドにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。

5. **レポートのタイプ**を選択します。

   レポートは、チャートおよび表形式で表示されます。

6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

[生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、[パラメータを変更] をクリックします。

チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ファイル名	ウイルスに感染したファイルの名前を表示します。
ウイルス名	ファイルを感染させたウイルスの名前を表示します。
実行した処置	ウイルスに対して実行した処置を表示します。
詳細を表示	レポートの詳細を表示します。詳細を表示するには、[詳細を表示] リンクをクリックします。

アンチマルウェアスキャンのレポートの表示

この機能により、スケジュールスキャンモジュールおよびオンデマンドスキャンモジュール（[クライアント] > [クライアントアクション] > [スキャン]）によるクライアントのスキャン後に、マルウェアが見つかったかどうかに関するレポートを生成できます。

アンチマルウェアスキャンのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[アンチマルウェアスキャン]** を表示します。
3. [全般レポート] ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストボックスにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。

5. **レポートのタイプ**を選択します。

レポートは、チャートおよび表形式で表示されます。

6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

[生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、[パラメータを変更] をクリックします。

チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
マルウェアの名前	マルウェアの名前を表示します。
マルウェアのタイプ	マルウェアのタイプを表示します。
実行した処置	マルウェア攻撃に対して実行した処置を表示します。

ウェブセキュリティのレポートの表示

この機能を使用して、ブラウジング保護、フィッシング対策、またはブロックウェブサイトモジュール（[設定] > [クライアント設定] > [ウェブセキュリティ]）によりウェブサイトがブロックされたかどうかに関するレポートを生成できます。

ウェブセキュリティのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[ウェブセキュリティ]** を表示します。
3. [全般レポート] ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストボックスにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。
5. **レポートのタイプ**を選択します。

   レポートは、チャートおよび表形式で表示されます。

6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

   [生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、**[パラメータを変更]** をクリックします。

   チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

注意:SME 系の Seqrite Endpoint Security の場合、表形式のレポートのみがウェブセキュリティで使用できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ブロックされたウェブサイト	ブロックされたウェブサイトを表示します。
カテゴリ	ブロックされたウェブサイトが属すカテゴリを表示します。

チューンアップのレポートの表示

この機能により、チューンアップされたクライアントの数およびチューンアップされていないクライアントの数に関するレポートを生成できます（[クライアント] > [クライアントアクション] > [チューンアップ]）。

チューンアップレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[チューンアップ]** を表示します。

   レポートがチャート形式で表示されます。
3. グループのレポートを生成するには、グループ名を選択します。
4. **レポートのタイプ**を選択します。

   レポートは、チャートおよび表形式で表示されます。
5. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

[生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、**[パラメータを変更]** をクリックします。

チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを印刷または CSV 形式または PDF 形式で保存できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	チューンアップ実行日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
チューンアップステータス	クライアントがチューンアップされたかどうかを表示します。
前回実行日	最後にチューンアップを実行した日付を表示します。

高度なデバイスコントロールのレポートの表示

この機能を使用して、リムーバブルデバイスがブロックされたかどうか、無許可のデバイスに対してどのような処置が実行されたかなど、デバイスコントロールのポリシーに関するレポートを生成できます（[設定] > [クライアント設定] > [高度な デバイスコントロール])。

高度なデバイスコントロールのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**レポート**]>[**クライアント**]>[**高度な**デバイスコントロール] を表示します。
3. [全般レポート] ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストボックスにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。
5. **レポートのタイプ**を選択します。

   レポートは、チャートおよび表形式で表示されます。
6. 選択したパラメータのレポートを生成するには、[**生成**] をクリックします。

[生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、[パラメータを変更] をクリックします。

チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

デバイスコントロールのプロンプトとレポートは「ネットワーク共有」に生成されません。

この高度なデバイスコントロールレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ユーザー名	ドメインに属しているユーザー名を表示します。
デバイス名	ポリシーに違反したデバイス名を表示します。
デバイスタイプ	デバイスのタイプを表示します。
シリアル番号	デバイスのシリアル番号を表示します。
実行した処置	デバイスコントロールポリシーに違反した処置を表示します。

データ喪失防止（DLP）のレポートの表示

この機能を使用して、無許可でデータを窃盗あるいはコピーしようとする試みについてのレポートを生成、確認できます。このレポートはユーザー、試みが実行されたエンドポイント、操作の時刻とチャンネルを特定します。

アクセス時スキャン

アクセス時スキャンのヘルプで特定の時間にデータを受信するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]**>**[クライアント]**> **[データ喪失防止]**>**[アクセス時スキャン]** を表示します。
3. データが必要な期間の開始日と終了日を入力します。
4. [グループ名] を選択します。
5. [エンドポイント名] を入力します。
6. 棒グラフ形式や表形式など、レポートのタイプを選択します。
7. 疑わしい活動が実行されている可能性があるチャンネルを選択します。

8. **［生成］**をクリックします。

   ［生成］ボタンをクリックすると、サマリーが表示されます。パラメータを変更したい場合、**［パラメータを変更］**をクリックします。

表形式のレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポートの開始日を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	ドメイン名を表示します。
ユーザー名	ユーザー名を表示します。
IP アドレス	エンドポイントの IP アドレスを表示します。
送信元	データがコピーまたはアクセスされたファイルのパスを表示します。
コンテンツタイプ	アクセスされたコンテンツタイプを表示します。
一致したアイテム	アクセスされたコンテンツのサブタイプを表示します。
ファイルパス	データがコピーまたはアクセスされたファイルのパスを表示します。
チャンネル	疑わしい活動が実行されている可能性があるチャンネルを表示します。
チャンネル詳細	疑わしい活動が実行されている可能性があるチャンネルの詳細を表示します。
送信者	送信者のメール ID を表示します。
受信者	受信者のメール ID を表示します。
件名	メールの件名を表示します。
実行した処置	疑わしい活動を監視するための処置を表示します。

オンデマンド/スケジュールスキャン

このスキャンを実行すると、機密情報レポートが生成、表示されるほか、選択したエンドポイントにユーザー定義辞書が生成、表示されます。このレポートでは、スキャン中に検出された検索条件に合ったテキストも表示されます。スキャン方法に関する詳細については、保存データスキャン を参照してください。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［レポート］>[クライアント]>[データ喪失防止］> ［オンデマンド/スケジュールスキャン］**を表示します。

3. データが必要な期間の開始日と終了日を入力します。
4. グループ名を選択してエンドポイント名を入力します。
5. 棒グラフ形式や表形式など、レポートのタイプを選択します。
6. スキャンするコンテンツのタイプを選択します。
7. **[生成]** をクリックします。

レポートは、CSV または PDF フォーマットで印刷またはエクスポートできます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	ドメイン名を表示します。
ユーザー名	ユーザー名を表示します。
スキャンタイプ	オンデマンドまたはスケジュールスキャンのいずれかのスキャンタイプを表示します。
機密データインシデント	スキャン時の機密データ合計数を表示します。
データ辞書インシデント	スキャン時のユーザー定義辞書データの合計数を表示します。
詳細	保存データスキャンの詳細を表示します。

アプリケーションコントロールのレポートの表示

この機能を使用して、アクセスまたはインストールされたアプリケーションの数、またそれらが許可されたアプリケーションなのか無許可のものかに関するレポートを生成できます。

アプリケーションコントロールのレポートは、アクセス時スキャン、およびインストールされたアプリケーションに対して個別に生成できます。

アクセス時スキャン

アクセス時スキャンのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]**>**[クライアント]**>**[アプリケーションコントロール]** を表示します。
3. [全般レポート] ページで、**[アクセス時スキャン]** タブをクリックしてアクセスされたアプリケーションに関するレポートを生成します。
4. レポートの開始日および終了日を選択します。

5. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストフィールドにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。

6. レポートのタイプを選択します。

   レポートは、チャートおよび表形式で表示されます。

7. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

   [生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。さらに、パラメータを変更したい場合、[パラメータを変更] ボタンを使用することで実行できます。

   チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ユーザー名	ドメインに属しているユーザー名を表示します。
ブロックされたアプリケーション	ブロックされたアプリケーションを表示します。
アプリケーションのバージョン	ブロックされたアプリケーションのバージョンを表示します。
アプリケーションのカテゴリ	ブロックされたアプリケーションのカテゴリを表示します。
アプリケーションのパス	ブロックされたアプリケーションのインストールパスを表示します。

インストールされたアプリケーション

インストールされたアプリケーションのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]**>**[クライアント]**>**[アプリケーションコントロール]** を表示します。

3. ［全般レポート］ページで、**［インストールされたアプリケーション］**をクリックしてレポートを生成します。
4. レポートの開始日および終了日を選択します。
5. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストボックスにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。
6. 選択したパラメータのレポートを生成するには、**［生成］**をクリックします。

   ［生成］ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。さらに、パラメータを変更したい場合、［パラメータを変更］ボタンを使用することで実行できます。

   生成したレポートは印刷するか、［CSV］または［PDF］ボタンを使用して CSV または PDF 形式で保存できます。

レポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
グループ名	選択したクライアントが属しているグループ名を表示します。
モジュール名	アプリケーションをスキャンしたモジュール名を表示します。
サマリー	インストールされたアプリケーションの要約を表示します。
詳細を表示	インストールされたアプリケーションの詳細を表示します。詳細を表示するには、［詳細を表示］リンクをクリックします。 クライアントマシンに存在する許可および無許可のアプリケーションに関する情報も含まれています。

不正侵入防御・検知システム（IDS/IPS）のレポートの表示

この機能により、ポートスキャン攻撃、DDoS（分散型サービス拒否）攻撃、または侵入の試みがあったかどうか、どのような処置が実行されたかに関するレポートを生成できます。

IDS/IPS のレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［設定］>［クライアント設定］>［IDS/IPS］**を表示します。

3. ［全般レポート］ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、テキストボックスにエンドポイント名を入力します。入力したエンドポイント名のレポートが生成されます。
5. ［レポート対象］で、レポートを生成する攻撃のタイプを選択します。

   レポートは次のモジュールに対して生成されます:侵入防止、ポートスキャン、および DDoS 攻撃。
6. 選択したパラメータのレポートを生成するには、**［生成］**をクリックします。

   ［生成］ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。さらに、パラメータを変更したい場合、［パラメータを変更］ボタンを使用することで実行できます。

   生成したレポートは印刷するか、［CSV］または［PDF］ボタンを使用して CSV または PDF 形式で保存できます。

侵入防止のこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
検出された脆弱性	クライアントで検出された脆弱性を表示します。
実行した処置	攻撃に対して実行した処置を表示します。
詳細を表示	インストールされたアプリケーションの詳細を表示します。詳細を表示するには、［詳細を表示］リンクをクリックします。

ポートスキャンのこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
攻撃者 IP	攻撃者の IP アドレスを表示します。

攻撃者の MAC アドレス	攻撃者の MAC アドレスを表示します。
スキャンされたポート	スキャンされたポートを表示します。
実行した処置	攻撃に対して実行した処置を表示します。

DDOS のこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
攻撃者 IP	攻撃者の IP アドレスを表示します。
攻撃者の MAC アドレス	攻撃者の MAC アドレスを表示します。
実行した処置	攻撃に対して実行した処置を表示します。

ファイアウォールのレポートの表示

この機能により、ブロックされた通信トラフィック（インバウンドまたはアウトバウンド)、およびファイアウォールのセキュリティレベル（[設定] > [クライアント設定] > [ファイアウォール]）などのファイアウォールの保護ポリシーに関するレポートを生成できます。

ファイアウォールのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[ファイアウォール]** を表示します。
3. [全般レポート] ページで、**[ファイアウォール]** タブをクリックしてレポートを生成します。
4. レポートの開始日および終了日を選択します。
5. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、グループ名を選択してエンドポイント名を入力します。選択したグループに属すエンドポイントの名前のレポートが生成されます。
6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

［生成］ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。さらに、パラメータを変更したい場合、［パラメータを変更］ボタンを使用することで実行できます。

チャート形式でレポートを生成する場合は、［印刷］オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

ファイアウォールのこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ローカル IP	ローカル IP アドレスを表示します。
リモート IP	リモート IP アドレスを表示します。
プロトコル	プロトコル名を表示します。
方向	ブロックされた通信トラフィックの方向を表示します。
ファイアウォールのレベル	ファイアウォールのセキュリティポリシーのレベルを表示します。
詳細を表示	インストールされたアプリケーションの詳細を表示します。詳細を表示するには、［詳細を表示］リンクをクリックします。

Wi-Fi レポートの表示

この機能を使用して、Wi-Fi 接続に関するレポートを生成することができます。このレポートは、安全ではない Wi-Fi に接続された時にエンドポイントの詳細を提示します。

Wi-Fi レポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［レポート］>［クライアント］>［ファイアウォール］** を表示します。
3. ［全般レポート］ページで、**［Wi-Fi］** タブをクリックしてレポートを生成します。
4. レポートの開始日および終了日を選択します。
5. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、グループ名を選択してエンドポイント名を入力します。選択したグループに属すエンドポイントの名前のレポートが生成されます。

6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

   折りたたみ可能なサマリー画面が表示されます。また、**[パラメーターを変更]** ボタンでパラメーターを変更することもできます。

   チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

Wi-Fi のこのレポートページには、クライアントに関する以下の詳細が記載されています。

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
Wi-Fi 名	Wi-Fi 接続名を表示します。
物理アドレス	エンドポイントの物理的なアドレスを表示します。
イベント	安全ではない Wi-Fi に接続された時のイベントを表示します。 例:安全ではない Wi-Fi への接続が検出されました。

脆弱性スキャンのレポートの表示

この機能により、ネットワーク内のエンドポイントに存在する脆弱性に関するレポートを生成できます。レポートは以下のいずれかのカテゴリに基づいてフィルタリングされます:

- すべての脆弱性
- 重大度
- ベンダー
- 主な脆弱性

脆弱性スキャンのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[脆弱性スキャン]** を表示します。
3. [レポートの生成] ページで、レポートの開始日および終了日を選択します。
4. グループ名およびエンドポイント名を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、グループ名を選択してエンドポイント名を入力します。選択したグループに属すエンドポイントの名前のレポートが生成されます。

5. ［レポートのタイプ］で、生成するレポートのタイプを選択します。
6. 選択したパラメータのレポートを生成するには、**［生成］**をクリックします。

   ［生成］ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。さらに、パラメータを変更したい場合、［パラメータを変更］ボタンを使用することで実行できます。

   チャート形式でレポートを生成する場合は、［印刷］オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

脆弱性スキャンのこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
脆弱性 ID	脆弱性インシデントの一意の CVE-ID を表示します。
脆弱性タイトル	脆弱性インシデントの説明を表示します。
重大度	脆弱性インシデントの重大度を表示します。
ベンダー	脆弱性がレポートされたベンダーの名前を表示します。
詳細を表示	脆弱性の詳細を表示します。詳細を表示するには、［詳細を表示］リンクをクリックします。

ファイル活動モニターレポートの表示

設定に合わせて、疑わしいファイル活動のレポートを表示します。以下のパラメータを使用してレポートを生成することができます:

- 開始日
- 終了日
- 場所
- グループ名
- エンドポイント名
- イベント

レポートは表形式または円グラフ形式で取得できます。このレポートには、あらゆるローカル、ネットワーク、またはリムーバブルデバイスに対して実行された試み、ユーザー名、エンドポイント名、インシデントの数についての情報も表示されます。チャートの上のリンクをクリックして、場所に分割したファイルタイプを閲覧できます。ファイ

ルの削除など、特定ファイルタイプに対する活動の概要を閲覧することもできます。個人のファイル活動を閲覧することができます。

ファイル活動のレポートの表示

ファイル活動レポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[設定]>[クライアント設定]>[ファイル活動モニター]** を表示します。
3. [レポートの生成] セクションで、ファイル活動をモニターしたい期間の開始日と終了日を入力します。
4. モニターしたい場所、グループ名、エンドポイント名、イベントのタイプを選択します。
5. **[生成]** をクリックします。レポートが生成され、画面に表示されます。表形式と円グラフ形式による表示を切り替えることができます。

   [生成] ボタンをクリックすると、折りたたみ可能なサマリー画面が表示されます。パラメータを変更したい場合、[パラメータを変更] をクリックします。

   チャート形式でレポートを生成する場合は、[印刷] オプションをクリックしてレポートを印刷できます。表形式でレポートを生成する場合は、レポートを CSV 形式または PDF 形式で保存できます。

ファイル活動モニターのこのレポートページには、クライアントに関する以下の詳細が記載されています:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	エンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
ファイル名	モニターされているファイル名を表示します。
場所	ドライブのタイプを表示します。
ユーザー名	ドメインに属しているユーザー名を表示します。
詳細	イベントの詳細を表示します。

アセット管理レポートの表示

[レポート] ページの [アセット管理] タブで、エンドポイントのアセットに関連するレポートを生成することができます。このレポートは、特定の期間、グループ、あるいは特定のエンドポイントに対して生成することができます。レポートは棒グラフ形式またはチャート形式で取得できます。ハードウェア変更レポートやソフトウェア変更レポートなど、必要なレポートのカテゴリを選択することもできます。必要に応じてレポートを印刷することができます。

アセット管理のレポートの表示

アセットインシデント

アセットインシデントレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[アセット管理]** を表示します。
3. **[アセット**インシデント] タブを選択します。
4. [レポートの生成] エリアで、必要なレポートの条件を入力または選択します。特定の期間のレポートを生成したり、必要なレポートのタイプを選択したり、該当欄にエンドポイント名を入力して特定エンドポイントのレポートを調べたりできます。
5. 棒グラフ形式か表形式か、レポートのタイプを選択します。
6. **[生成]** をクリックします。画面にレポートが表示されます。レポートを印刷したい場合、印刷アイコンを使用します。

現在のアセット

現在のアセットレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]>[クライアント]>[アセット管理]** を表示します。
3. [現在のアセット] タブを選択します。
4. [レポートの生成] エリアで、必要なレポートの条件を入力または選択します。オペレーティングシステム、システム製造元、プロセッサ、前回のシャットダウン、RAM またはアプリケーション名を選択します。

   [生成] をクリックします。画面にレポートが表示されます。レポートを印刷したい場合、印刷アイコンを使用します。レポートは、CSV または PDF フォーマットで保存できます。

パッチ管理レポートの表示

この機能を使用して、パッチに関するレポートを生成することができます。このレポートでは、ネットワークのエンドポイントにインストールされているパッチの詳細が表示されます。

以下のパラメータを使用してレポートを生成することができます:

- 開始日
- 終了日
- グループ名
- エンドポイント名
- レポートのタイプ

- 重大度
- パッチステータス

レポートは表形式でクライアントまたはパッチごとに利用できます。このレポートには、ドメイン、パッチ名、アプリケーション名、ターゲットにされた脆弱性、スキャンタイプ、およびパッチステータスに関する情報も表示されます。パッチの詳細も確認することができます。

パッチのレポートを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[レポート]**>**[クライアント]**>**[パッチ管理]** を表示します。
3. レポートの開始日および終了日を選択します。
4. [グループ名] を選択します。

   グループのレポートを生成する場合は、エンドポイント名テキストボックスを空白にしておきます。エンドポイント名のレポートを生成する場合は、グループ名を選択してエンドポイント名を入力します。選択したグループに属すエンドポイントの名前のレポートが生成されます。
5. **レポートのタイプ、重大度、**および**パッチステータス**を選択します。
6. 選択したパラメータのレポートを生成するには、**[生成]** をクリックします。

   概要レポートが表示されます。また、**[パラメーターを変更]** ボタンでパラメーターを変更することもできます。

   [印刷] オプションをクリックしてレポートを印刷できます。レポートは、CSV または PDF フォーマットで保存できます。
7. パッチの詳細を表示するには、[**パッチタイトル**] リンクをクリックします。

   [パッチの詳細] ダイアログが表示されます。**[印刷]** オプションをクリックしてパッチの詳細を印刷できます。パッチの詳細は、CSV または PDF フォーマットで保存できます。
8. **[閉じる]** をクリックします。

パッチ管理の [レポート] ページで以下のパッチ詳細が表示されます:

欄	説明
日時	レポート生成日時を表示します。
エンドポイント名	レポートが生成されるエンドポイントの名前を表示します。
ドメイン	選択したクライアントがログインするドメインを表示します。
パッチタイトル	パッチの名前をハイパーリンク形式で表示します。名前をクリックしてパッチの詳細を表示することができます。

重大度	欠落しているパッチの重大度を表示します。
カテゴリ	インストールされているパッチのカテゴリを表示します。
アプリケーション	アプリケーションの名前を表示します。例: Windows 8
ターゲットにされた脆弱性	クライアントでターゲットにされた脆弱性を表示します。
スキャンタイプ	スキャンのタイプを表示します。
パッチステータス	パッチのステータスを表示します。

サーバー

この機能を使用して、サーバーで発生したすべてのインシデントのイベントログを確認できます。一次デバイスアクセス用の OTP 生成ログも表示されます。

サーバーのイベントログを表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**レポート**］>［**サーバー**］を表示します。
3. レポートの開始日および終了日を選択します。
4. ［イベントログ］ページで、レポートのカテゴリを選択します。

   レポートは印刷するか、[CSV] または [PDF] ボタンを使用して CSV または PDF 形式で保存できます。必要に応じて、イベントログを削除することもできます。

欄	説明
削除	イベントログを削除します。
印刷	イベントログを印刷します。
CSV	CSV 形式でレポートを保存できます。
PDF	PDF 形式でレポートを保存します。

管理

この機能により、サーバーおよびクライアントで生成されたレポートを管理できます。レポートをいつ自動的に削除するかを設定できます。レポートを手動でエクスポートして削除できます。

設定の管理

以下の方法で、いつ自動的にレポートを削除するかを設定できます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. ［**レポート**］>［**管理**］>［**設定**］を表示します。
3. ［設定］ページで、以下のように設定します:
   - ［レポートを自動的に削除する日数］で、自動的にレポートを削除する日数を設定します。
   - ［過去…日間のレポートを次の受信者に自動的にメール送信］で、レポートを必要とする日数を設定します。
   - ［メールアドレス］テキストボックスに、メールアドレスを入力します。
     複数のメール ID を入力する場合は、カンマで区切ります。
4. ［メール送信の頻度］で、レポートを送信する頻度と時刻を設定します。
5. ［メール送信するレポートの選択］で、メール送信するレポートのタイプを設定します。
6. 設定を保存するには、**[保存]** をクリックします。

注意:モジュールに 1000 を超えるレコードが含まれる場合、最新のレコード 1000 のみがメールされます。

エクスポートの管理

以下の方法で、レポートを PDF 形式でエクスポートできます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**レポート**］>［**管理**］>［**エクスポート**］を表示します。
3. ［選択条件］で、エクスポートするレポートを以下から選択します:
   - すべてのレポートをエクスポートするには、［すべてのレポート］を選択します。
   - ［以下の条件に従って］で、開始日および終了日などの選択条件を設定し、グループ名を選択してエンドポイント名を入力します。
4. ［レポートの選択］で、レポートをエクスポートするモジュールを選択します。
   使用している Seqrite Endpoint Security に関連するモジュールが表示されます。
5. すべての選択条件を設定してから、**[エクスポート]** をクリックしてレポートを PDF 形式で出力します。

レポートの削除の管理

以下の方法でレポートを手動で削除できます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**レポート**］>［**管理**］>［**レポートの削除**］を表示します。
3. ［レポートの手動削除］で、以下のいずれかのオプションを選択します:

- レポートを削除する日数: 日数を選択して、指定した日数を経過したレポートを削除します。
- すべてのレポートを削除: これまで生成されたすべてのレポートを削除する場合に、このオプションを選択します。

4. ［レポートの選択］で、削除するレポートのタイプを以下の中から選択します:
   - クライアントレポート
   - サーバーレポート
5. 選択条件を設定してから、［**削除**］をクリックしてレポートを削除します。

Chapter

12

管理者設定

[管理者設定] セクションには、以下の項目があります:

サーバー

この機能により、サーバーに関連した様々な設定を行えます。設定には、通知の送信方法と通知の理由の設定、SMTP 設定、アクセスを許可するデバイスの追加、緊急時のサーバーのリダイレクト、およびユーザーの管理などがあります。

パスワードの変更

無許可のユーザーが設定を変更したり、エンドポイントから Seqrite クライアントを削除したりするのを防ぐために、Seqrite Endpoint Security をパスワード保護することをお勧めします。Seqrite Endpoint Security にコンソールパスワードを指定する必要があります。このパスワードは Seqrite Endpoint Security で変更できます。

コンソールパスワードを変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**管理者設定**] > [**サーバー**] > [**パスワードの変更**] を開きます。
3. [古いパスワード] テキストボックスに、現在のスーパー管理者パスワードを入力します。
4. [新しいパスワード] テキストボックスに新しいパスワードを入力し、[パスワードの再入力] テキストボックスに新しいパスワードを再度入力します。
5. [**適用**] をクリックします。

メールアドレスを変更する

登録したメールアドレスが表示されます。必要に応じて、メールアドレスを変更することができます。

メールアドレスを変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. ［**管理者設定**］> ［**サーバー**］>［**メールアドレスを変更**］を開きます。
3. ［メールアドレス］テキストボックスで、メールアドレスを編集します。
4. **［適用］**をクリックします。

通知

ウイルスが検出された、メモリ内でウイルスがアクティブになった、ウイルスが発生したなどの様々なイベントに関する通知を送信できます。無許可のデバイスやアプリケーションへのアクセスが行われた、またはウイルス定義が最新ではなくなった場合、侵入検知に対する通知が送信されます。通知には、Active Directory との同期の失敗に関するアラートやライセンス関連情報なども含まれています。ネットワーク全体で発生したインシデントが報告されるため、適切な処置を実行してミスを防ぐことができます。

通知には以下のものがあります:

- 様々なインシデントに関するメールおよび SMS 通知。
- SMS 送信用のメール ID や携帯電話番号のリストを作成するためのイベント通知用メール & SMS の設定。
- 国コードなしの携帯電話番号を設定しなければなりません。

メールおよび SMS 通知

メールおよび SMS 通知を設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］> ［**サーバー**］>［**通知**］を表示します。
3. 送信する通知を有効にするには、［メールおよび SMS 通知］で、**［通知を送信するイベントを選択してください］**オプションを選択します。

   ［送信される通知］の他のすべてのオプションが有効になります。
4. ［ウイルス感染とウイルスアウトブレイク］で、以下のインシデントに関する通知を取得するメディアを選択します:
   - エンドポイントでウイルスが検出されました
   - エンドポイントでウイルスがアクティブです
   - ネットワークのウイルスアウトブレイク

   通知はメール、SMS、またはその両方で取得できます。ただし、エンドポイントでウイルスが検出された通知に関しては、メールのみで取得できます。

   ［ネットワークのウイルスアウトブレイク］オプションを選択すると、通知が必要な場合の設定をさらにカスタマイズできます。これは、ウイルスアウトブレイクを警告します。

   ネットワークのウイルスアウトブレイクをカスタマイズするには、以下の手順に従ってください:

- ［ネットワークのウイルスアウトブレイク］の横にある［**カスタマイズ**］をクリックします。
- ［ウイルスアウトブレイクの詳細］画面が表示されます。
- ［ウイルスインシデントの合計数が超えました］で、インシデント数およびウイルスアウトブレイクが起きているシステムの数を設定します。
- ［および時間範囲］で、通知をトリガーする頻度の時間幅を設定します。
- 設定を保存するには、［**保存**］をクリックします。

5. IDS/IPS で、通知を取得するイベントを選択します:
   - エンドポイントで侵入が検知されました
   - エンドポイントでポートスキャンインシデントが検出されました
   - エンドポイントで DDoS 攻撃が検出されました

   注意:侵入防止の通知はメールのみで送信できます。
6. ［高度なデバイスコントロール］で、通知を取得するイベントを選択します:
   - デバイスコントロールポリシー違反の試み

   注意:デバイスコントロールの通知はメールのみで送信できます。
7. ［アプリケーションコントロール］で、通知を取得するイベントを選択します:
   - 無許可のアプリケーションにアクセスする試み

   注意:アプリケーションコントロールの通知はメールのみで送信できます。
8. ［アップデート］で、以下のインシデントに関する通知を取得するメディアを選択します:
   - サービスパックが使用可能です
   - エンドポイントは最新のウイルス定義にアップデートされていません
   - アップデートマネージャーのウィルス定義が最新ではありません

   注意:エンドポイントがアップデートされていないことを知らせる通知は、メールのみで送信できます。
9. ［Active Directory 経由でインストールする］で、以下のインシデントに関する通知を取得するメディアを選択します:
   - Active Directory と同期できませんでした
10. ［切断されたエンドポイント］で、通知を取得するイベントを選択します:
    - 感染のため、エンドポイントはネットワークから切断されました
    - DDoS 攻撃のため、エンドポイントはネットワークから切断されました
    - ポートスキャンのため、エンドポイントはネットワークから切断されました

    注意:すべてのインシデントの通知はメールのみで送信できます。

11. [ライセンス関連] で、以下のインシデントに関する通知を取得するメディアを選択します:
    - ライセンスが失効しました
    - ライセンスの有効期限が近づいています
    - ライセンスの上限を超えています
12. [データ喪失防止] で、イベントの通知を有効にします:
    - データ喪失防止ポリシー違反の試み
13. [アセット管理] で、イベントの通知を有効にします。
    - エンドポイントで行われたハードウェア変更
14. 設定を保存するには、**[適用]** をクリックします。

イベント通知用メールとSMSの設定

[メールおよび SMS 通知] を設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**管理者設定**] > [**サーバー**] > [**通知**] を表示します。
3. [イベント通知用メールおよび SMS の設定] で、**[設定]** をクリックします。
   [メールおよび SMS の通知] プロンプトが表示されます。
4. [メール ID のリスト] にメールアドレスを入力して、**[追加]** をクリックします。
   複数のメールアドレスを入力できます。
5. [携帯電話番号のリスト] に携帯電話の番号を入力して、**[追加]** をクリックします。
6. メールアドレスと携帯電話の番号を保存するには、**[適用]** をクリックします。
7. 設定を保存するには、**[適用]** 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。

- 現時点では SMS を用いた通知機能はインドと UAE に在住のお客様のみご利用いただけます。
- 一部のイベントは SMS 通知に対応していません。
- National Do Not Call Registry (DND) にリストされた携帯電話番号は、インド政府のその時点での電話規制政策により、通知を受信ができる場合とできない場合があります。

今すぐ購入

この機能で、通知を送信するための Seqrite Endpoint Security SMS バンドルを購入できます。

[SMS の残数] セクションでは、SMS 通知を送信できる数が表示されます。通知を送ると、残数に反映されます。通知を続けて送信するには、SMS バンドルを購入して SMS 制限を増やす必要があります。

以下のいずれかの方法で SMS バンドルを購入できます:

- [今すぐ購入] リンクをクリックして以下を行います。このリンクをクリックすると、通知に使用する Seqrite Endpoint Security SMS バンドルのポータルに転送され、そこで SMS バンドルを購入できます。
- 直接オンラインポータルを開き、以下を行います。直接オンラインポータルを開いて SMS バンドルを購入します。SMS バンドルの URL は、http://www.seqrite.com/psmsです。

ショッピングポータルで、SMS バンドルの購入方法に関する指示に従ってください。

SMS バンドルを購入するとすぐに、SMS の残数オプションの限度が有効期限と共にアップデートされます。限度に反映されない場合、[ライセンス情報のアップデート] ボタンをクリックしてアップデートすることができます。

以下の方法でラインセンス情報を更新し、SMS バンドルの限度を更新することができます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**ホーム**] > [**ライセンスの表示**] リンクを表示します。
3. [ライセンスマネージャー] で [**ステータス**] ボタンをクリックします。
4. [ライセンスステータス] 画面で [**ライセンス情報の更新**] ボタンをクリックします。

   ライセンスが更新され、最新の残数が表示されます。

SMTP 設定

この機能により、SMTP ホストの詳細を設定できます。Seqrite Endpoint Security からのすべてのメール（通知メール、レポートメールなど）は、SMTP サーバーに送信されてルーティングされます。

SMTP 設定を行うには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**管理者設定**] > [**サーバー**]>[**SMTP 設定**] を表示します。
3. [SMTP サーバー] テキストボックスに、SMTP サーバーの IP アドレスまたはドメイン名を入力します。
4. [ポート] テキストボックスに、ポート番号を入力します。
5. [メールアドレスから通知] テキストボックスに、メールアドレスを入力します。

Endpoint Security サーバーから送信されるすべてのメールには、差出人アドレスとしてこのメールアドレスが表示されます。

6. ユーザー認証のために、[ユーザー名] テキストボックスにユーザー名を入力します。

   [ユーザー名] フィールドは使用している SMTP サーバーによって異なります。ユーザー名またはメール ID を指定するよう求められます。

7. [パスワード] テキストボックスにパスワードを入力します。
8. [ユーザー認証の方法] に、以下のいずれかを選択します:
   - なし:このオプションを選択すると、HTTP プロトコルを通じてメール通知を送信します。
   - SSL:このオプションを選択すると、SSL (Secure Sockets Layer) プロトコルを通じてメール通知を送信します。
   - TLS:このオプションを選択すると、TLS (Transport Layer Security) プロトコルを通じてメール通知を送信します。
9. Seqrite は、SMTP ホストの詳細が正しいことを確認するために SMTP 設定をテストすることを推奨します。SMTP 設定をテストするには、**[適用]** をクリックしてから **[SMTP 設定をテストする]** をクリックします。
10. [テストメール] ダイアログの **[メールの送り先]** テキストボックスにユーザーのメール ID を入力します。
11. **[メールを送信]** をクリックします。

SMTP 設定がパブリックメールサーバー (例: Gmail) を使用して設定されている場合、および安全性の低いアプリを許可する設定がパブリックメールサーバーで無効にされている場合、EPS はメールを送信することができません。

デバイスを管理

この機能を使用してすべての USB デバイスとシステム内部デバイス (例:Bluetooth、Webcam) を認証することができます。ポリシーに従って設定された場合、認証されたデバイスを EPS クライアントシステムで許可またはブロックすることができます。EPS 環境でデバイスを管理するには、すべての USB ストレージデバイスでこの認証を実行しなければなりません。

USB デバイスのクリーニング

デバイスコントロールツール (dcconfig tool) にデバイスを追加する前に、ディスクをクリーニングします。

ディスクをクリーニングするには、以下の手順に従ってください:

1. デバイスを接続します。
2. コマンドプロンプトで、以下のコマンドを一つずつ入力します。

```
diskpart
list disk
Select disk <#>
clean
convert mbr
```

3. クリーンアップ後、ディスクにパーティションを作成します。

   これで、ディスクを追加する準備が完了しました。

EPS クライアントがインストールされている/されていないデバイスの追加

EPS クライアントがインストールされている/されていないデバイスを追加するには、以下の手順に従ってください:

1. ウェブコンソールにログオンします。
2. クリーンデバイスを接続します。
3. **[管理者設定]** >**[サーバー]**>**[デバイスを管理]** を表示します。
4. **[デバイスを追加]** > [USB デバイス] を選択します。[デバイスダイアログを追加] ダイアログが表示されます。
5. **[ここをクリック]** リンクをクリックして、デバイスコントロールパッケージをダウンロードします。
6. DEVCTRL.7Z ジップファイルを展開します。
7. devctrl フォルダーで dcconfig.exe ファイルをダブルクリックします。
8. デバイスの詳細が [デバイスコントロール] ダイアログに表示されます。**[デバイス名]** ボックスでデバイス名を入力します。
9. デバイスを認証するには、以下の一つを実行します:
   - EPS クライアントがインストールされているシステムを使用している場合、利用可能なオプションは以下の通りです。
     - 暗号化なし
     - 部分暗号化
     - 完全暗号化
   - EPS クライアントがインストールされていないシステムを使用している場合、利用可能なオプションは以下の通りです:
     - 暗号化なし

    - 部分暗号化
- 暗号を適用する場合、以下の表を参照します:

暗号化	処置
いいえ	• ［**このデバイスを社内ネットワーク内でのみアクセス可能にする**］チェックボックスのチェックを外します。この設定はデフォルトで選択されています。 • ［**このデバイスを暗号化する**］チェックボックスのチェックを外します。
部分	• ［**このデバイスを社内ネットワーク内でのみアクセス可能にする**］チェックボックスを選択します。この設定はデフォルトで選択されています。 • ［**このデバイスを暗号化する**］チェックボックスのチェックを外します。
完全	• ［**このデバイスを社内ネットワーク内でのみアクセス可能にする**］チェックボックスを選択します。この設定はデフォルトで選択されています。 • ［**このデバイスを暗号化する**］チェックボックスを選択します。 • 完全暗号化を適用すると、［フォーマット］ウィンドウが表示されます。デバイスのフォーマットを行います。

10. ［**ファイルに保存**］をクリックします。dcinfo.dat ファイルが作成されます。
11. dcinfo.dat ファイルが devctrl フォルダに保存されます。
12. ［**管理者設定**］>［**サーバー**］>［**デバイスを管理**］を表示します。
13. ［**デバイスを追加**］>［USB デバイス］を選択します。［デバイスダイアログを追加］ダイアログが表示されます。
14. ［**参照**］をクリックして dcinfo.dat ファイルをアップロードします。
15. ［**適用**］をクリックします。

    デバイスがデバイス例外に追加され、リストに表示されます。

管理者フォルダーから dcconfig ツールにデバイスを追加

管理者フォルダーから dcconfig ツールにデバイスを追加する場合

1. クリーンデバイスを接続します。
2. Seqrite Endpoint Security サーバーで、「<installation directory>¥Seqrite¥Endpoint Security 7.1¥Admin」フォルダを参照します。

3. dcconfig.exe ファイルをダブルクリックします。[デバイスコントロール] ダイアログが表示されます。
4. [**検索**] ボタンをクリックして、添付されているデバイスの詳細を表示します。
5. デバイスの詳細が [デバイスコントロール] ダイアログに表示されます。[**デバイス名**] ボックスでデバイス名を入力します。
6. デバイスを許可する場合、利用可能な暗号化オプションは以下の通りです:
    - 暗号化なし
    - 部分暗号化
    - 完全暗号化

    暗号を適用する場合、以下の表を参照します:

暗号化	**処置**
いいえ	• [このデバイスを社内ネットワーク内でのみアクセス可能にする] チェックボックスのチェックを外します。この設定はデフォルトで選択されています。 • [**このデバイスを暗号化する**] チェックボックスのチェックを外します。
部分	• [このデバイスを社内ネットワーク内でのみアクセス可能にする] チェックボックスを選択します。この設定はデフォルトで選択されています。 • [**このデバイスを暗号化する**] チェックボックスのチェックを外します。
完全	• [このデバイスを社内ネットワーク内でのみアクセス可能にする] チェックボックスを選択します。この設定はデフォルトで選択されています。 • [このデバイスを暗号化する] チェックボックスを選択します。 • 完全暗号化を適用すると、[フォーマット] ウィンドウが表示されます。デバイスのフォーマットを行います。

7. [**追加**] をクリックします。

部分暗号化は NTFS のみサポートします。暗号化なしと完全暗号化は、すべてのファイルシステムでサポートされます。

デバイスコントロールポリシーへの例外の追加

許可された人物が使用するリムーバブルデバイスに例外を追加して、デバイスをポリシーから除外することができます。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. [**管理者設定**] >[**サーバー**]>[**デバイスを管理**] を表示します。
3. 表示される [**デバイスの追加**] ドロップダウンリストで、適切なデバイスカテゴリをクリックします。以下のデバイスカテゴリが表示されます:
   - **ネットワークデバイス**:ネットワークに接続されたデバイスのリストが自動的に表示されます。管理したいデバイスを選択します。[**OK**] をクリックします。
   - **USB デバイス**:ネットワークデバイスリストに記載されず、接続されていない USB デバイスを追加したい場合、このオプションを使用します。詳細については、EPS サーバがインストールされているまたは EPS クライアントがインストールされている/されていないデバイスの追加を参照してください。
   - **モデル別 USB**:このオプションを使用します。組織が同じメーカーの同じモデルの USB ストレージデバイスを多数所有している場合。モデル名別に USB を追加できます。[モデル名別にデバイスを追加] ダイアログボックスが表示されます。**デバイス名**を入力します。[**モデル名を追加**] リストボックスからモードを選択します。以下のモードが表示されます:
     - **自動**:USB マスストレージデバイスが Windows オペレーティングシステムに接続されている場合、デバイスモデル名は自動的に表示されます。

       モデル名の自動取得は Mac オペレーティングシステムでサポートされていません。
     - **リストから**:事前に指定されたデバイスモデル名のリストが表示されます。リストからモデル名を選択します。
     - **手動**:**モデル名**を入力します。ダイアログボックスに表示される手順に従います。

       同じ USB ストレージデバイスが USB デバイスおよびモデル別 USB として認証される場合、モデル名が優先されます。
   - **その他のデバイス**:接続されておらず、リストに存在しないデバイスを追加したい場合、このオプションを使用します。デバイスタイプを選択して該当情報を入力します。
4. 表示されたリストから管理したいデバイスを選択して、[**OK**] をクリックします。

   リストにデバイスが表示されたら、必要に応じて [**許可**] の下にあるボタンを [はい] または [いいえ] に切り替えます。表示される [編集] アイコンを使用して表示されるデバイス名を変更したり、[ゴミ箱] アイコンを使用してリストからデバイスを削除したりすることもできます。

   注意:デバイスの許可アクセス権を [いいえ] に設定している場合、例外リストに追加することはできません。
5. デバイスを例外リストに追加するには、[設定] > [クライアント設定] > [高度なデバイスコントロール] を表示します。
6. [**例外**]をクリックします。

7. ［追加］をクリックします。［管理デバイス］ダイアログボックスに、許可したデバイスのリストが表示されます。
8. デバイスの［例外に追加］ ボタンを切り替えます。
9. ［OK］をクリックします。
10. ［管理デバイス］確認ダイアログボックスで［はい］をクリックします。デバイスが例外リストに追加されます。

    デバイスを削除するには、デバイスを選択してから、表示されるゴミ箱アイコンをクリックします。
11. 必要に応じてアクセス権を設定します。
12. ［ポリシーの保存］をクリックします。

- Windows Vista のウェブコンソールにアクセスする場合は、Internet Explorer の［保護モード］オプションを OFF にしてください。
- ウェブコンソール経由でデバイスを追加できない場合は、デバイスコントロールツールを使用して USB ストレージデバイスを追加することもできます。このツールは、EPS サーバーの次の場所にあります:<Installation folder>¥Admin¥dcconfig.exe
- デバイス機能の追加は、Windows 10 オペレーティングシステムの Edge ブラウザと Google Chrome 44 以降のバージョンで動作しません。

データ喪失防止

データ喪失を防止するために、以下の機能に対しグローバルな設定を行うことができます:

- ユーザー定義辞書
- ドメイン例外
- カスタム拡張子
- アプリケーション例外
- ネットワーク共有例外

ユーザー定義辞書

ユーザー定義辞書の機密情報を含む可能性のある、または参照するための特定のキーワードやフレーズを追加できます。エンドポイントの文書にユーザー定義辞書に追加したテキストやフレーズが含まれる場合、保存データスキャンまたはデータ喪失防止機能により、そうした文書のパスや場所が表示されます。

このセクションで、ユーザー定義辞書を作成または管理することができます。ユーザー定義辞書はデータ喪失防止設定からモニターされます。

辞書の追加

辞書を追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[ユーザー定義辞書]** を表示します。
3. **[辞書を追加]** をクリックします。
4. 名前、説明、追加する用語などの詳細を入力します。
5. **[追加]** をクリックします。

   複数の用語を辞書に追加できます。

   特定の用語を選択し、**[削除]** をクリックすることで用語を削除することができます。
6. **[OK]** をクリックします。

辞書のインポート

使用したい辞書をインポートすることも可能です。

辞書をインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[ユーザー定義辞書]** を表示します。
3. **[インポート]** をクリックします。
4. [辞書をインポート] ダイアログで **[参照]** をクリックします。

   [ファイルアップロード] ダイアログが表示されます。
5. 有効なエクスポートされた辞書データベースファイル（例:expdict.db）を選択します。
6. **[開く]** をクリックします。

   データベースファイルをインポートします。

辞書のエクスポート

作成した辞書をエクスポートすることができます。

辞書をエクスポートするには、以下の手順に従ってください。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[ユーザー定義辞書]** を表示します。

3. ［ユーザー定義辞書］ページで、エクスポートしたい辞書を選択します。
4. ［アクション］欄で［**エクスポート**］アイコンをクリックします。

   データベースファイルをダウンロードします。データベースファイルのデフォルト名は expdict.db です。必要に応じて、ファイル名を変更することができます。

辞書でのアクション

提供されるリストから辞書を選択し、［アクション］欄で必要なアクションを実施して、追加した辞書を編集、削除またはエクスポートすることができます。

ドメイン例外

このセクションで、データ喪失保護から除外したいドメイン名を追加することができます。

ドメイン例外は Windows プラットフォーム上の Outlook と Thunderbird メールクライアントのみサポートします。

ドメイン名の追加

データ喪失保護から除外したいドメイン名を追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**サーバー**］>［**データ喪失保護**］>［**ドメイン例外**］に移動します。
3. テキストボックスにドメイン名を入力します。
4. ［**追加**］をクリックします。

ドメイン名の削除

- 個々のドメイン名を削除するには、ドメイン名の隣にある［**削除**］アイコンをクリックします。
- 複数のドメイン名を削除するには、削除したいドメイン名のチェックボックスを選択してから［**削除**］をクリックします。

ドメイン名のインポート

使用したいドメイン名をインポートすることができます。

ドメイン名をインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**サーバー**］>［**データ喪失保護**］>［**ドメイン例外**］に移動します。
3. ［ドメイン例外］ページで、［**インポート**］をクリックします。

   ［ファイルアップロード］ダイアログが表示されます。

4. 有効なエクスポートされたドメインデータベースファイルexdomain.db）を選択します。
5. ［開く］をクリックします。

   データベースファイルをインポートします。

ドメイン名のエクスポート

作成したドメイン名をエクスポートすることができます。

ドメイン名をエクスポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［管理者設定］>［サーバー］>［データ喪失保護］>［ドメイン例外］に移動します。
3. ［ドメイン例外］ページで、エクスポートしたいドメイン名を選択します。
4. ［エクスポート］をクリックします。

   データベースファイルをダウンロードします。データベースファイルのデフォルト名は exdomain.db です。必要に応じて、ファイル名を変更することができます。

ドメイン名でのアクション

提供されるリストからドメイン名を選択し、［アクション］欄で必要なアクションを実施して、追加したドメイン名を編集または削除することもできます。

カスタム拡張子

ファイルのデフォルト拡張子のほかに、必要に応じてその他の拡張子をモニターすることができます。追加の拡張子はカスタム拡張子と呼ばれます。

このセクションで、データ喪失保護からモニターするカスタム拡張子を追加することができます。

カスタム拡張子は Windows プラットフォームでのみサポートされます。

カスタム拡張子の追加

カスタム拡張子を追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［管理者設定］>［サーバー］>［データ喪失保護］>［カスタム拡張子］に移動します。
3. カスタム拡張子を入力します。
4. ［追加］をクリックします。

カスタム拡張子の削除

- 個々のカスタム拡張子を削除するには、カスタム拡張子の隣にある［**削除**］アイコンをクリックします。
- 複数のカスタム拡張子を削除するには、削除したいカスタム拡張子のチェックボックスを選択してから［**削除**］をクリックします。

カスタム拡張子のインポート

使用したいカスタム拡張子をインポートすることができます。

カスタム拡張子ファイルをインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**サーバー**］>［**データ喪失保護**］>［**カスタム拡張子**］に移動します。
3. ［カスタム拡張子］ページで、［インポート］をクリックします。

   ［ファイルアップロード］ダイアログが表示されます。
4. 有効なエクスポートされたカスタム拡張子データベースファイル（例:expfiles.db）を選択します。
5. ［**開く**］をクリックします。

   データベースファイルをインポートします。

カスタム拡張子のエクスポート

作成したカスタム拡張子をエクスポートすることができます。

カスタム拡張子ファイルをエクスポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**サーバー**］>［**データ喪失保護**］>［**カスタム拡張子**］に移動します。
3. ［カスタム拡張子］ページで、エクスポートしたいカスタム拡張子を選択します。
4. ［**エクスポート**］をクリックします。

   データベースファイルをダウンロードします。データベースファイルのデフォルト名は expfiles.db です。必要に応じて、ファイル名を変更することができます。

カスタム拡張子でのアクション

提供されるリストからカスタム拡張子を選択し、［アクション］欄で必要なアクションを実施して、追加したカスタム拡張子を編集または削除することもできます。

アプリケーション例外

このセクションで、データ喪失保護から除外するアプリケーションを追加することができます。データ喪失保護でモニターされるアプリケーションのみ追加します。

アプリケーション例外は Windows プラットフォームでのみサポートされます。

アプリケーション例外の追加

アプリケーション例外を追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[アプリケーション例外]** に移動します。
3. アプリケーションを追加するには、**[参照]** をクリックして、アプリケーションの完全なパスを指定してください。
4. [アプリケーション名] を入力します。
5. **[追加]** をクリックします。

X64 ビット OS で「**system32**」フォルダからアプリケーションを追加している場合、アプリケーションを「**system32**」フォルダから他の場所にコピーします。次に、その場所からアプリケーションを追加します。

アプリケーション例外の削除

- 個々のアプリケーション例外を削除するには、アプリケーション例外の隣にある **[削除]** アイコンをクリックします。
- 複数のアプリケーション例外を削除するには、削除したいアプリケーション例外のチェックボックスを選択してから **[削除]** をクリックします。

アプリケーション例外のインポート

使用したいアプリケーション例外をインポートすることができます。

アプリケーション例外をインポートするには、以下の手順に従ってください。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[アプリケーション例外]** に移動します。
3. [アプリケーション例外] ページで、**[インポート]** をクリックします。

   [ファイルアップロード] ダイアログが表示されます。

4. 有効なエクスポートされたアプリケーションデータベースファイル（例:expapps.db）を選択します。
5. **［開く］**をクリックします。

   データベースファイルをインポートします。

アプリケーション例外のエクスポート

作成したアプリケーション例外をエクスポートすることができます。

アプリケーション例外をエクスポートするには、以下の手順に従ってください:

1. ［アプリケーション例外］ページで、エクスポートしたいアプリケーションを選択します。
2. **［エクスポート］**をクリックします。

   データベースファイルをダウンロードします。データベースファイルのデフォルト名は expapps.db です。必要に応じて、ファイル名を変更することができます。

アプリケーション例外でのアクション

提供されるリストからアプリケーション例外を選択し、［アクション］欄で必要なアクションを実施して、追加したアプリケーション例外を編集または削除することもできます。

ネットワーク共有例外

このセクションで、データ喪失保護から除外する UNC フォーマットのネットワーク共有パスを追加することができます。

ネットワーク共有例外の追加

ネットワーク共有例外を追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［管理者設定］**>**［サーバー］**>**［データ喪失保護］**>**［ネットワーク共有例外］**に移動します。
3. ネットワーク共有例外を入力します。
4. **［追加］**をクリックします。

ネットワーク共有例外の削除

- 個々のネットワーク共有例外を削除するには、ネットワーク共有例外の隣にある［**削除**］アイコンをクリックします。
- 複数のネットワーク共有例外を削除するには、削除したいネットワーク共有例外のチェックボックスを選択してから［**削除**］をクリックします。

ネットワーク共有例外のインポート

使用したいネットワーク共有例外をインポートすることができます。

ネットワーク共有例外をインポートするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[サーバー]** > **[データ喪失保護]** > **[ネットワーク共有例外]** に移動します。
3. [ネットワーク共有例外] ページで、**[インポート]** をクリックします。

   [ファイルアップロード] ダイアログが表示されます。
4. 有効なエクスポートされたネットワーク共有データベースファイル（例: expnetsh.db）を選択します。
5. **[開く]** をクリックします。

   データベースファイルをインポートします。

ネットワーク共有例外のエクスポート

作成したいネットワーク共有例外をエクスポートすることができます。

ネットワーク共有例外をエクスポートするには、以下の手順に従ってください:

1. [ネットワーク共有例外] ページで、エクスポートしたいアプリケーションを選択します。
2. **[エクスポート]** をクリックします。

   データベースファイルをダウンロードします。データベースファイルのデフォルト名は expnetsh.db です。必要に応じて、ファイル名を変更することができます。

ネットワーク共有例外でのアクション

提供されるリストからネットワーク共有例外を選択し、[アクション] 欄で必要なアクションを実施して、追加したネットワーク共有例外を編集または削除することもできます。

リダイレクト

この機能により、Endpoint Security サーバーを変更して、Endpoint Security を新しいバージョンにアップグレードできます。既存のクライアントを新しい EPS サーバーにリダイレクトすることで、新しい EPS サーバーを使用して通信できるようになります。クライアントを選択、またはすべてのクライアントを設定して、新しいサーバーにリダイレクトします。この機能は、クライアントが低帯域幅回線で接続されている大きなネットワークの場合、特に便利です。この機能を使って、グループのクライアントを選択して新しいサーバーへ移動させることができ、お客様の都合に合わせた段階的なリダイレクトが可能になります。

ソフトウェアのバージョンアップグレードの場合は、前のバージョンの Endpoint Security クライアントがアンインストールされ新しいバージョンがインストールされます。

サポートされているリダイレクトケースを以下の表に示します。

以前のバージョンの EPS サーバー	新しいバージョンの EPS サーバー
ローカル/プライベート IP にインストール	ローカル/プライベート IP にインストール
ローカル/プライベート IP にインストール	ローカル/プライベートドメインにインストール
ローカル IP にインストール（パブリックに変換）	ローカル IP にインストール（パブリックに変換）
パブリック IP にインストール	パブリック IP にインストール
パブリック IP にインストール	FQDN にインストール（完全修飾ドメイン名）

- リダイレクトプロセスが実行されている場合、前にインストールされた EPS はアンインストールされません。リダイレクトプロセスコマンドがすべてのクライアントに配信される前に、前の EPS をアンインストールする場合、そのコマンドを受信できなかったクライアントは前の EPS と新しい EPS の両方と通信することができません。
- リダイレクトは Linux オペレーティングシステムにインストールされているクライアントには適用できません。
- グループの復活:クライアントのリダイレクト後に前のクライアントグループポリシー構成を維持するために、管理者は［グループを管理］から古いクライアントグループポリシー構成のエクスポート、および新しい EPS サーバーへのインポートを実行できます。リダイレクト後、古いクライアントは新しい EPS サーバーで前と同じグループに置かれます。

同じ名前のグループがリダイレクトサーバーに存在する場合、新しくインポートされたグループ名の最後に「_1」が付けられます。

- グループの復活は MAC と Windows クライアントのみに適用できます。

リダイレクトを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［管理者設定］>[サーバー]>[リダイレクト］**を表示します。
3. ［サーバー名/IP］テキストボックスで、新しい EPS サーバーのサーバー名または IP アドレスを入力します。
4. ［ポート］テキストボックスに、ポート番号を入力します。

5. 以下の手順に従ってください:

   i. [**このチェックボックスを選択してパブリック IP アドレス/ホスト名を追加する**] チェックボックスを選択します。

   ii. リモートクライアントの場合のみ、[**サーバー名/IP**] テキストボックスで新しい EPS サーバーのサーバー名またはパブリック/変換された IP アドレスを入力します。

   EPS がパブリックモードでインストールされた場合、上記の 2 つの欄は表示されません。

6. **リダイレクトタイプ**リストでオプションを一つ選択します:

   - すべてのクライアントをリダイレクト:リダイレクトされるすべてのクライアントを選択する場合。
   - すべてのクライントのリダイレクトと自動再起動:アップグレードプロセスですべてのクライアントをリダイレクトし、自動再起動する場合。このオプションを有効にすると、ユーザーに再起動まで15 分を示すカウントダウンがプロンプト表示され、15 分後に強制的に再起動されます。クライアントの再起動後、クライアントの新しいバージョンが（静かに）にインストールされ、 リダイレクトプロセスが完了します。
   - 選択されたクライアントのリダイレクト:このオプションを選択すると特定のクライアントを、リダイレクトプロセスに選択することができます。このオプションを選択すると、[クライアントを選択] のリンクが表示されます。[**クライアントを選択**] をクリックします。[クライアントを選択] ダイアログボックスで、リダイレクトするクライアントを選択して [**OK**] をクリックします。右上の [エンドポイント名/IP] 検索ボックスを使用して、名前または IP アドレスでエンドポイントを選択します。

7. スキャン設定を適用するには、[**適用**] をクリックします。

リダイレクトプロセスが同じ EPS バージョンに対して実行されると、[すべてのクライアントをリダイレクトして再起動する] オプションが設定されているとしても、クライアントシステムは自動的に再起動されません。

ユーザーの管理

この機能を使用して、管理者レベルとレポート閲覧レベルのユーザーリストを作成、編集、無効、削除することができます。ユーザーのタイプには、以下のものがあります:

スーパー管理者

スーパー管理者ユーザーには、Seqrite Endpoint Security のすべての機能へのアクセス権があります。スーパー管理者は、管理者ユーザーを作成または変更できます。スーパー管理者のみが Seqrite Endpoint Security をアンインストールする権限があります。

1 人のユーザーのみにスーパー管理者権限が付与されます。スーパー管理者のデフォルトユーザー名は、「administrator」です。

管理者

管理者権限を持つユーザーは、以下の 2 つの点を除き、スーパー管理者と同じ権限を持ちます:

1. 管理者権限を持つユーザーは、管理者権限のある別のユーザーを作成できません。
2. 管理者権限を持つユーザーは Seqrite Endpoint Security をアンインストールできません。

レポートビューア

レポートビューア権限を持つユーザーは、レポートおよび機能のステータスを確認できます。それ以外の権限はありません。ただし、このタイプのユーザーは、自分のパスワードを変更できます。

新しいユーザーの作成

新しいユーザーを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** >**[サーバー]**>**[ユーザーの管理]** を表示します。
3. [ユーザーの管理] ページで、**[ユーザーの追加]** をクリックします。

   [ユーザーの追加/編集] ダイアログが開きます。
4. [ユーザー名] テキストボックスに、ユーザー名を入力します。
5. [**新しいパスワード**] テキストボックスに新しいパスワードを入力します。
6. [**新しいパスワードの再入力**] テキストボックスに新しいパスワードを再度入力します。
7. **メール ID** テキストボックスに、ユーザーのメール ID を入力します。
8. [タイプ] リストで、ユーザータイプを選択します。

   ユーザータイプには次のものがあります。管理者およびレポートビューア。
9. [ユーザーステータス] リストからユーザーの有効または無効を選択します。
10. 設定を保存するには、**[保存]** をクリックします。

既存のユーザーの変更

既存のユーザーを変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. ［**管理者設定**］>[**サーバー**]>[**ユーザーの管理**］を表示します。

   すべてのユーザーのリストが表示されます。

3. 編集するユーザーの横にある［**編集**］ボタンをクリックします。
4. 割り当てられた権限に応じて、設定を変更できます。

   ［ユーザーの追加/編集］ダイアログが開きます。

5. ［新しいパスワード］テキストボックスに新しいパスワードを入力します。
6. ［新しいパスワードの再入力］テキストボックスに新しいパスワードを再度入力します。
7. 必要な場合は、［タイプ］リストで新しいタイプを選択します。
8. ［ユーザーステータス］ドロップダウンメニューからユーザーの有効または無効を選択します。
9. 設定を保存するには、[**保存**］をクリックします。

ユーザーの削除

既存のユーザーを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>[**サーバー**]>[**ユーザーの管理**］を表示します。

   すべてのユーザーのリストが表示されます。

3. 削除するユーザーの横にある［**削除**］をクリックします。

   ユーザーを削除する適切な権限がある場合、ユーザーが削除されます。

   確認メッセージが表示されます。

4. ユーザーを削除するには、[**はい**］をクリックします。

インターネット設定

この機能を使用して、管理者は、インターネット接続を有効にするために必要なサーバーモジュールのプロキシ設定を使用できます。クラウド接続、ライセンスの同期、ライセンス履歴の表示、メールの送信 & SMS の通知、メッセンジャーなどのサーバーモジュールのインターネット設定を行えます。これは、デフォルトでインターネット接続が許可されていない安全な作業環境でクライアントモジュールを機能させるのに非常に役立ちます。

インターネット接続を行うには、以下のステップを実施してください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**]>[**サーバー**]>[**インターネット設定**］を表示します。

3. インターネットのプロキシ設定を行うには、**[プロキシ設定を有効にする]** を選択します。

   プロキシ設定の詳細が有効になります。

4. [プロキシサーバー] にサーバー名を入力します。

5. [ポート] にポート番号を入力します。

   ファイアウォールまたはプロキシサーバーを使用する場合、認証ルールも入力できます。この場合、[認証] にユーザー名とパスワードを入力します。

6. スキャン設定を適用するには、**[適用]** をクリックします。

[管理者設定] のインターネット設定は、[アップデートマネージャの接続設定] に反映されます。

バックアップのスケジュール

EPS ポリシー、グループ、および Seqrite Cloud のユーザーの一覧のバックアップを、リクエストした定期的な間隔でスケジュールできます。

バックアップをスケジュールするには、以下の手順に従ってください:

1. **[バックアップのスケジュールを有効にする]** チェックボックスを選択します。
2. バックアップを取る頻度（毎月、毎週、毎日、指定日）を設定します。
3. バックアップ時間のスケジュールを組みます。
4. **[保存]** をクリックします。

スケジュールされた日時に自動的にバックアップが行われます。

オンデマンドバックアップ:

このオプションで、現在の設定をバックアップすることができます。そうすることで、スケジュールされた時間まで待つことなく現在の変更を保存することができます。

[今すぐバックアップ] をクリックして、現在の EPS サーバーの設定をバックアップします。

復元

このオプションを使用して、設定（ポリシー、グループ、ユーザーなど）を Cloud に保存されているバックアップファイルから復元することができます。このオプションは、EPS サーバーを再インストールした場合、または前の状態に設定を戻さなければならない場合に役立ちます。

復元を行うには、以下の手順に従ってください:

1. **[バックアップの詳細を表示]** をクリックします。

2. 復元するバックアップを選択し、[**復元**] をクリックします。
3. バックアップをダウンロード後、[**次へ**] をクリックします。
4. 復元する設定を選択します。
5. [**次へ**] をクリックします。

   バックアップが正常に復元されます。

Seqrite Cloud は別製品であり、追加で購入されたユーザーのみが利用できます。

パッチ管理

パッチ管理で、ネットワークでインストールされたアプリケーションに対し、欠落しているパッチの確認やインストールを集中管理できます。パッチ管理で、欠落しているパッチを自動的に確認やインストールすることもできます。

Microsoft Windows OS のクライアントのみがパッチ管理機能を利用できますが、Mac と Linux オペレーティングシステムのクライアントにはサポートされません。

パッチサーバーのインストール

パッチサーバーをインストールするには、以下の手順に従ってください:

1. 32 ビット版 Windows OS の場合、 以下のリンクの一つからセットアップをダウンロードします:

   - http://dlupdate.quickheal.com/builds/seqrite/71/jap/pmsetup32.msi
   - http://download.quickheal.com/builds/seqrite/71/jap/pmsetup32.msi

   64 ビット版 Windows OS の場合、 以下のリンクの一つからセットアップをダウンロードします:

   - http://dlupdate.quickheal.com/builds/seqrite/71/jap/pmsetup64.msi
   - http://download.quickheal.com/builds/seqrite/71/jap/pmsetup64.msi

2. Seqrite パッチサーバーをインストールしたいネットワークのシステムでセットアップを起動します。
3. インストールの終了後、EPS コンソールから Seqrite パッチサーバーを追加すると利用可能になります。

新しいパッチサーバーの追加

新しいパッチサーバーを追加するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。

2. [**管理者設定**] > [**サーバー**] > [**パッチ管理**] を表示します。
3. [パッチ管理] ページで **[新しいパッチサーバーを追加]** タブをクリックします。
4. [新しいパッチサーバーを追加] セクションでサーバー名を入力します。
5. パッチサーバーがローカルクライアントに展開される場合、以下の手順に従います:
   i. **[サーバー IP/ホスト名]** テキストボックスで、パッチサーバーのプライベート IP アドレスまたはホスト名を入力します。
   ii. **[ポート]** にポート番号を入力します。デフォルトポート HTTP は 3698 SSL:6201 です。
   iii. **[SSL を使用]** チェックボックスが選択されていることを確認します (SSL が選択されている場合、パッチサーバーが SSL をサポートしていることを確認します)。このチェックボックスはデフォルトで選択されています。
   iv. [EPS 詳細] セクションの **[EPS IP/ホスト名]** テキストボックスで、EPS サーバーのプライベートまたはパブリック IP/ホスト名を指定します。Seqrite はプライベート IP/ホスト名を指定することを推奨します。

   パッチサーバーがリモートクライアントのネットワークに展開される場合、以下の手順に従います。
   i. **[サーバー IP/ホスト名]** テキストボックスで、パッチサーバーのパブリック IP アドレスまたはホスト名を入力します。
   ii. **[ポート]** にポート番号を入力します。デフォルトポート HTTP は 3698 SSL:6201 です。
   iii. **[SSL を使用]** チェックボックスが選択されていることを確認します (SSL が選択されている場合、パッチサーバーが SSL をサポートしていることを確認します)。このチェックボックスはデフォルトで選択されています。
   iv. [EPS 詳細] セクションの **[EPS IP/ホスト名]** テキストボックスで、EPS サーバーのパブリック IP/ホスト名を指定します。
6. **[追加]** をクリックします。

パッチサーバーの削除

パッチサーバーを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. [**管理者設定**] > [**サーバー**] > [**パッチ管理**] を表示します。
3. [パッチ管理] ページで **[新しいパッチサーバーを追加]** タブをクリックします。

   既存のパッチサーバーステータスが表示されます。ステータスオプションは以下の通りです:

ステータス	説明
オンライン	パッチサーバーはオンラインです。
オフライン	パッチサーバーはオフラインです。
アンインストールされました	パッチサーバーがアンインストールされています。
無効	パッチサーバーは EPS コンソールに追加されます。次に、同じパッチサーバーが別の EPS コンソールに追加されます。この場合、最初の EPS のパッチサーバーステータスは無効として表示されます。

4. ポリシーに適用されている場合、パッチサーバーを削除することはできません。削除したいパッチサーバーを選択して、その隣の［**削除**］リンクをクリックします。

   確認メッセージが表示されます。

5. ［**はい**］をクリックして、パッチサーバーを削除します。

パッチサーバーの設定

EPS サーバーとエンドポイントが通信する Seqrite パッチサーバー用のポートを設定します。

パッチサーバーを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**サーバー**］>［**パッチ管理**］を表示します。
3. ［パッチ管理］ページで［**パッチサーバーを設定**］タブをクリックします。
4. リストからパッチサーバーを選択します。設定セクションが表示されます。
5. ［**設定**］タブを選択して以下を実行します:
   i. パッチサーバーのポート番号が表示されます。ポート番号は変更できます。
   ii. ［**SSL を使用します（パッチサーバーが SSL で設定される場合このチェックボックスを選択します)**］チェックボックスを選択します。
   iii. 自動ダウンロードセクションで、［**重大度が同等またはそれより高い場合、検出された欠落しているパッチを自動的にダウンロードする**］を選択します。チェックボックスを選択します。
   iv. リストから重大度を選択します。重大度のオプションは以下の通りです:

重大度	説明
致命的	脆弱性によりユーザーインタラクションなしにコードが実行されます。

重要	脆弱性により、ユーザーデータの機密性、完全性、または利用可能性が侵害される恐れがあります。プロンプトの起源や品質、ユーザビリティに関わらず、警告やプロンプトがクライアントに表示されます。
中	脆弱性の影響は、認証要件や非デフォルト設定のみへの適用といった要素により、かなり軽減されます。
低	脆弱性の影響は、影響を受けたコンポーネントの性質により全面的に軽減されます。
指定されていない	脆弱性は偶発的な不具合となる可能性があります。

6. **[インターネット設定]** タブを選択して、以下を実行します:

   プロキシサーバーの詳細が表示されます。デフォルトで **[プロキシ設定を有効にする]** チェックボックスを選択します。プロキシ設定を無効にするチェックボックスのチェックを外します。

   i. **[プロキシサーバー]** テキストボックスに、プロキシサーバーの IP アドレスが表示されます。必要な場合、IP アドレスを編集します。

   ii. **[ポート]** テキストボックスに、プロキシサーバーのポート番号を入力します。必要な場合ポート番号を編集します。

   iii. **[認証を有効にする（該当する場合)]** チェックボックスを選択して認証を有効にします。

   iv. **[ユーザー名]** と **[パスワード]** 欄に、サーバー認証を入力します。

7. **[パッチ同期]** タブを選択して以下を実行します:

   i. 前のパッチ同期ステータスと最後に正常にパッチが同期された日が表示されます。

   ii. [アップストリームパッチサーバーを設定] セクションで、以下のオプションからアップストリームパッチサーバーを選択します。

アップストリームパッチサーバー	説明
Microsoft パッチサーバー	使用されているアップストリームパッチサーバーは Microsoft パッチサーバーです。本オプションはデフォルトで選択されています。
組織のパッチサーバー（WSUS）	使用されるアップストリームパッチサーバーは組織のパッチサーバー（WSUS - Windows サーバーアップデートサービス）です。 このオプションを選択した場合、WSUS サーバー URL を

	入力します。
Seqrite パッチサーバー	使用されるアップストリームパッチサーバーとして Seqrite パッチサーバーが設定されます。 このオプションを選択した場合、リストからパッチサーバーを選択します。

iii. [パッチ同期を設定] セクションで、**[パッチ同期のスケジュールを有効にする]** チェックボックスを選択します。

iv. パッチ同期の**頻度**として、毎週または毎月のいずれかを選択します。

v. リストから**平日**を選択してパッチ同期を実行します。

vi. **[開始時間]** リストで時間と分を選択してパッチ同期を実行する時間を選択します。

vii. **[フィルター..]** をクリックして、パッチ同期用のフィルターを指定します。[Windows パッチ同期設定] ダイアログが表示されます。

a. **[製品]** タブで、パッチを受け取りたい Microsoft 製品を選択します。展開するフォルダーを選択します。

b. **[カテゴリ]** タブを選択します。同期させるパッチタイプを選択します。

c. **[言語]** タブを選択します。以下のオプションの一つを選択してパッチの言語を選択します:

- すべての言語でパッチをダウンロードする
- 以下で選択した言語でパッチをダウンロードする

d. **[適用]** をクリックして、パッチ同期用のフィルターを適用します。初期設定を復元するには、**[初期設定]** をクリックします。

viii. **[開始]** をクリックしてパッチ同期をすぐに実行します。

ix. パッチ同期が実行されている場合、**[停止]** をクリックしてパッチ同期を停止します。通知がパッチ管理サーバーに送信されます。

8. **[適用]** をクリックして構成設定を適用します。

一般事項

この機能を使用して、実行中のセッションのタイムアウト時間を設定できます。現在のセッションが指定した時間無効になると、実行中のセッションはタイムアウトします。

一般機能を設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** >**[サーバー]**>**[一般事項]** を表示します。

3. ［セッションタイムアウト時間］リストで、時間を設定します。

   20 分、30 分、または 60 分のいずれかを選択できます。

4. **［適用］**をクリックします。

マルチサーバー移行期間

マルチサーバー移行期間機能により、一定期間以前のバージョンをアンインストールすることなく EPSのより新しいバージョンをインストールすることができます。この機能を使用すると、既存のクライアントをより新しいバージョンに簡単に移行させることができます。スケジュールに合わせて、30 ～ 90 日の範囲で移行期間を選べます。本機能を使用するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **［管理者設定］**>**[サーバー]**>**[一般事項]** を表示します。
3. マルチサーバー継続期間リストで日数を選びます。
4. **［適用］**をクリックします。

- 複数のサーバーが設置されている場合、このオプションはインストールされているバージョンよりも新しいバージョンでのみ利用できます。
- デフォルトで、継続期間は 60 日が選択されています。

クライアント

このセクションには、以下の項目が含まれています。

クライアントインストール

この機能を使用して、クライアントをインストールする場所のパスを指定できます。デフォルトで設定されているパスは、必要に応じて変更できます。

Seqrite クライアントのインストールパスを変更するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**クライアント**］>［**クライアントのインストール**］を表示します。

   ［クライアントインストール］ページが表示されます。

3. クライアントインストールパスを設定するには、［**クライアントのインストール先パスを指定してください**］テキストボックスにインストールパスを入力します。
4. SEPS がインストールされた時にスキャンを開始するために、［スキャンとレポート］セクションで以下のオプションを選択できます:

- 脆弱性:クライアントエンドポイントの脆弱性スキャンを設定し、SEPS が正常にインストールされた後に SEPS サーバーにレポートを送信する場合、このチェックボックスを選択できます。
- インストール済みのすべてのアプリケーション:SEPS が正常にインストールされた後にクライアントエンドポイントでインストールされたすべてのアプリケーションのスキャンを設定する場合、このチェックボックスを選択できます。スキャンレポートが SEPS サーバーへ送信されます。本オプションはデフォルトで選択されています。

5. 設定を適用するには、**[適用]** をクリックします。

- この機能は、Mac および Linux オペレーティングシステムのクライアントでは使用できません。

非アクティブクライアント設定

エンドポイントから Seqrite クライアントをアンインストールすると、プログラムにより自動的にサーバーに通知されます。サーバーはこの通知を受信すると、コンピュータツリーのクライアントアイコンを削除します。

ただし、クライアントが他の方法で削除されると（コンピュータのハードドライブの再フォーマット、または手動によるクライアントファイルの削除など)、Seqrite Endpoint Security はクライアントを非アクティブとして表示します。ユーザーがクライアントを長時間アンロードまたは無効にした場合も、サーバーはクライアントを非アクティブとして表示します。

アクティブなクライアントの表示を保護するために、Seqrite Endpoint Security が非アクティブなクライアントをコンピュータ保護リストから削除するように設定できます。

非アクティブクライアント設定機能は、Microsoft Windows、Mac、および Linux オペレーティングシステムのクライアントのみで使用できます。

非アクティブクライアントを削除するには、以下の手順を実施してください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]**>**[クライアント]** を開きます。

   [クライアントインストール] ページが表示されます。
3. [非アクティブクライアント設定] で、**[非アクティブクライアントの自動削除を有効にする]** を選択します。
4. [非アクティブの場合にクライアントを削除] リストで、Seqrite Endpoint Security がクライアントを非アクティブとして認識してからの日数を選択します。
5. 設定を適用するには、**[適用]** をクリックします。

アセット管理

この機能を使用して、システム情報、ハードウェア情報、インストールされているソフトウェアやアップデートなどエンドポイントに関する様々な情報を収集することができます。

次の手順に従って［アセット管理レポート］を有効にできます。

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**クライアント**］を開きます。
3. **［アセット管理を有効にする］**チェックボックスを選択します。
4. **［適用］**をクリックします。

クライアントのローミング

ローミングサービスにより、組織のネットワーク外にいるクライアントが、Seqrite クラウドを経由して EPS サーバーに接続できます。この機能を使用して、管理者はポリシーの適用、チューンアップの初期化、アプリケーションコントロールスキャンなどのスキャン、脆弱性スキャン、EPS サーバーから遠隔操作でウィルススキャンを実施できます。

クライアントは、ステータスのアップデート（クライアントがローミングを実施すると、最新のステータスがクライアントステータスタブとダッシュボードでローミングとして表示されます)、最新設定のダウンロード、クライアントレポートの送信が行えます。

EPS は［インターネット設定］タブで設定されるプロキシ設定を使用してクラウドベースのローミングサービスと通信します。プロキシ設定が利用できない場合、EPS は直接通信します。

以下の手順でローミングサービスを有効にできます:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**クライアント**］>［**ローミングクライアント**］を表示します。
3. **［クラウドプラットフォームに接続］**をクリックします。

   ［接続処理の完了］ページが表示されます。
4. **［OK］**をクリックします。
5. **［ローミングサービスを有効にする］**チェックボックスを選択します。
6. クライアントに以下のいずれかのローミングモードを選択します:
   - 自動

     このモードでは、クライアントが組織のネットワーク外にいる場合、すべての EPS クライアントがローミングサービスに自動で接続されます。
   - マニュアル

このモードでは、選択されたクライアントのみがローミングサービスに接続できます。このモードを選択した場合、以下の方法で特定のクライアントを選択できます:

a. **[クライアントの選択]** をクリックします。

b. このサービスを使用するには、ネットワークのクライアントを選択して有効にします。

c. **[OK]** をクリックします。

7. **[適用]** をクリックします。

再インストール

同じプロダクトキーを再インストールする場合、以下に従い、クライアントのローミングを有効にする必要があります:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. **[管理者設定]** > **[クライアント]** > **[ローミングクライアント]** を表示します。
3. **[クラウドプラットフォームに接続]** をクリックします。

   [接続処理の完了] ページが表示されます。
4. [OK] をクリックします。
5. OTP を受信するメールアドレスを選択します。
6. **[次へ]** をクリックします。
7. 選択したメールアドレスを確認し、**[確認]** をクリックして OTP を受信します。
8. メールで受信した OTP を入力します。
9. メールが届かない場合、**[OTP の再生成]** をクリックして再度生成します。

   接続処理が完了します。
10. **[OK]** をクリックして続行します。
11. **[ローミングサービスを有効にする]** と **[ローミングモード]** を選択します。

- クライアントのローミング機能は、Windows と Mac のオペレーティングシステムでのみサポートされます。
- インターネット接続では、このサービスを使用しなければなりません。

データ喪失防止 (DLP)

このセクションで、購入した DLP ライセンスの数と使用した DLP ライセンスの数を確認できます。また、エンドポイントの DLP パックを有効または無効にできます。

このページには以下の情報が表示されます。

- 資格のある（購入した）DLP ライセンスの合計数
- 使用した DLP ライセンスの数

DLP 機能の有効化

DLP 機能を有効にするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ［**管理者設定**］>［**クライアント**］>［**データ喪失保護**］を表示します。

   DLP 機能が有効にされるすべてのエンドポイントが一覧表示にされます。
3. ［**追加**］をクリックします。

   すべてのグループを表示したウィンドウが開きます。各グループには、そのグループに属しているエンドポイントの名前が含まれています。
4. Endpoint Security コンソールで、グループを選択します。

   右側のフレームに、関連するグループのすべてのエンドポイントが表示されます。
5. エンドポイントを選択して、[OK] をクリックします。

   DLP 機能が選択したエンドポイントに対して有効にされます。
   必要に応じて、エンドポイントを削除することもできます。

欄	説明
検索	名前でエンドポイントを検索できます。
CSV	CSV 形式でリストを保存します。
追加	DLP を有効にするエンドポイントを追加できます。
削除	エンドポイントを削除できます。

EPS クライアントがクライアントリストから削除されると、DLP 有効リストからも削除されます。

Chapter

13

アップデートマネージャ

アップデートマネージャは Seqrite Endpoint Security に統合されたツールです。Seqrite Endpoint Security のアップデートのダウンロードおよび管理に使用します。この機能は柔軟性があり、アップデートを単一のマシンにダウンロードできます。すべての Seqrite Endpoint Security クライアントはアップデートをこの集中管理された場所から取り込みます。機能強化またはバグ修正のために Seqrite Endpoint Security の自動アップデート機能も提供します。Seqrite Endpoint Security と統合したアップデートマネージャには、アップデートマネージャアプリケーションで使用できるすべての機能が含まれています。ここでの設定変更はすべて、アップデートマネージャアプリケーションに反映されます。

アップデートマネージャのステータスの表示

この機能を使用して、アップデートマネージャでダウンロードされたすべてのアップデートの情報を表示します。コンソールには、バージョン、サービスパック、関連するウイルスデータベースの日付が表示されます。

コンソールでは以下の詳細情報も提供されます:

欄	説明
エンドポイント名	アップデートマネージャをインストールしたエンドポイントの名前が表示されます。
IP アドレス	アップデートマネージャをインストールしたエンドポイントの IP アドレスが表示されます。
ステータス	アップデートマネージャの情報（オンラインかまたはオフラインかどうか）が表示されます。
アップデートマネージャ URL	アップデートをダウンロードするためのアップデートマネージャ URL を提供します。代替アップデートマネージャ、クライアント、およびその他の EPS アップデートマネージャがこの URL を使用できます。

[アップデートマネージャのステータス] の下に、以下の 2 つのボタンがあります:

ボタン	説明
今すぐ更新	このボタンをクリックして、アップデートのダウンロードを開始する通知を Seqrite Endpoint Security から代替アップデートマネージャに送信します。この処理はバックグラウンドで行われるため、ユーザーには見えません。**[戻る]** をクリックして、[ステータス] ページに戻ります。
ロールバック	このボタンをクリックして、アップデートマネージャを前回のアップデート状態に戻します。 注意:この機能は、アップデートマネージャの設定で［**新しいアップデートをダウンロードする前に常にバックアップを作成する**］オプションが選択されている場合のみ使用できます。ロールバックを実行する手順は以下の通りです。 • **[ロールバック]** ボタンをクリックします。ポップアップウィンドウが開きます。ロールバックによって影響を受ける Seqrite 製品のアップデートが表示されます。 • ロールバックプロセスを開始するには、**[ロールバック]** をクリックします。

アップデートマネージャの設定

[アップデートマネージャの設定] で、使用できる機能は以下の通りです:

機能	説明
自動アップデートを有効にする	このボックスを選択して、Seqrite Endpoint Security の自動アップデートを有効にします。本機能はデフォルトで有効になっています。この機能を無効にしないことをお勧めします。
新しいアップデートをダウンロードする前に常にバックアップを作成する	このチェックボックスを選択して、既存のアップデートのバックアップを作成してから、新しいアップデートをダウンロードします。このバックアップは、前回のアップデートへのロールバックが必要な場合に使用します。本機能はデフォルトで有効になっています。
レポートを削除するまでの日数	このボックスを選択すると、指定した日数の経過後にレポートが自動的に削除されます。本機能はデフォルトで有効になっており、日数は 10 日が設定されています。
Seqrite Endpoint Security サービスパックをダウンロードする	Seqrite Endpoint Security サービスパックのアップデートを取得するには、[**Endpoint Security サービスパックをダウンロードする**] チェックボックスを選択します。本機能はデフォルトで有効になっています。
ダウンロードするア	SEPS 製品リストが表示されます。デフォルトで、すべての

ップデートを選択する	製品が選択されます。どのアップデートを Endpoint セキュリティにダウンロードするかを検証します。
ダウンロード速度を制限する（Kbps）	アップデートのダウンロード速度を制限したい場合は、[**ダウンロード速度を制限する（キロビット毎秒）**] チェックボックスを選択します。テキストボックスに速度を入力します。 64 ～ 8192 キロビット毎秒の範囲で速度制限を入力できます。

設定を保存するには、[**適用**] ボタンをクリックします。

アップデートマネージャースケジュール

この機能を使用して、特定の頻度でアップデートマネージャのアップデートスケジュールを定義できます。

アップデートマネージャスケジュールを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる [**アップデートマネージャ**] リンクをクリックします。
3. [アップデートマネージャ] ページで、[**アップデートマネージャ設定**] タブをクリックします。
4. [自動アップデートを有効にする] の横の [**設定**] ボタンをクリックします。

   [アップデートマネージャスケジューラ] ダイアログが表示されます。
5. **カスタム**オプションを選択して以下のオプションを設定します:
   i. [**頻度**] で、[毎日] または [毎週] オプションを選択します。
   毎週オプションを選択した場合、リストから平日を選択します。
   ii. [**開始時刻**] で、時刻を時間と分で設定します。
   iii. アップデートマネージャのアップデートを繰り返したい場合、[**アップデートを繰り返す**] チェックボックスを選択して、アップデートを繰り返す日にちを設定します。
6. [**適用**] をクリックします。

代替アップデートマネージャ

大規模なネットワークの場合、複数のアップデートマネージャを異なるサーバーに展開することができます。これにより、負荷分散が図られ、クライアント設定でクライアントを設定し、これらの場所からアップデートを取得させることができます。代替アップデートマネージャの詳細、追加、編集、または削除を確認できます。

推奨事項

リモートクライアントの場合、リモートクライアントが展開されるネットワークで代替アップデートマネージャをインストールします。

新しい代替アップデートマネージャの追加

EPS サーバーで新しい代替アップデートマネージャを追加するには、以下の手順に従わなければなりません:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる［**アップデートマネージャ**］リンクをクリックします。
3. ［アップデートマネージャ］ページで、［**代替アップデートマネージャ**］タブをクリックします。

   すべてのアップデートマネージャのリストが表示されます。
4. ［**追加**］をクリックして、新しい代替アップデートマネージャを作成します。
5. EPS クライアントで代替アップデートマネージャがインストールされるエンドポイントのリストが表示されます。

   リストでエンドポイントを選択して、そのエンドポイントで代替アップデートマネージャを作成します。
6. ［**アップデートマネージャ名**］テキストボックスに名前を入力します。
7. ［**アップデートマネージャサイト**］テキストボックスに代替アップデートマネージャの URL を入力します。
8. 設定を保存するには、［**追加**］をクリックします。

代替アップデートマネージャの詳細の表示

EPS クライアントにインストールされた代替アップデートマネージャの詳細を表示するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる［**アップデートマネージャ**］リンクをクリックします。
3. ［アップデートマネージャ］ページで、［**代替アップデートマネージャ**］タブをクリックします。

   すべてのアップデートマネージャのリストが表示されます。
4. 代替アップデートマネージャの横にある［**設定**］リンクをクリックして、代替アップデートマネージャのステータスと設定を表示します。

5. ［代替アップデートマネージャの詳細］画面が表示されます。**［ステータス］**タブをクリックして、以下の詳細が示されたステータスを表示します:

欄	説明
アップデートマネージャー名	代替アップデートマネージャの名前が表示されます。
エンドポイント名	代替アップデートマネージャをインストールしたエンドポイントの名前が表示されます。
IP アドレス	代替アップデートマネージャをインストールしたエンドポイントの IP アドレスが表示されます。
ステータス	代替アップデートマネージャの情報（オンラインかまたはオフラインかどうか）が表示されます。
アップデートマネージャ URL	アップデートをダウンロードするためのアップデートマネージャ URL を提供します。この URL を使用できるのは、EPS アップデートマネージャ、クライアント、およびその他の代替アップデートマネージャです。

詳細（製品名、バージョン、サービスパック、ウィルスデータベースの日にち）が示されたインストール製品のリストも表示されます。［アップデートマネージャのステータス］の下に、以下の 2 つのボタンがあります:

ボタン	説明
今すぐ更新	このボタンをクリックして、アップデートのダウンロードを開始する通知を Seqrite Endpoint Security から代替アップデートマネージャに送信します。この処理はバックグラウンドで行われるため、ユーザーには見えません。**［戻る］**をクリックして、［ステータス］ページに戻ります。
ロールバック	このボタンをクリックして、代替アップデートマネージャを前回のアップデート状態に戻します。 注意:この機能は、代替アップデートマネージャの設定で［**新しいアップデートをダウンロードする前に常にバックアップを作成する**］オプションが選択されている場合のみ使用できます。ロールバックを実行する手順は以下の通りです: • **［ロールバック］**ボタンをクリックします。ポップアップウィンドウが開きます。ロールバックによって影響を受ける Seqrite 製品のアップデートが表示されます。 • ロールバックプロセスを開始するには、**［ロールバック］**をクリックします。

6. **［設定］**タブをクリックして、以下の詳細が示されたステータスを表示します

［代替アップデートマネージャの設定］で、使用できる機能は以下の通りです:

機能	説明
自動アップデートを有効にする	このボックスを選択して、Seqrite Endpoint Security の自動アップデートを有効にします。本機能はデフォルトで有効になっています。この機能を無効にしないことをお勧めします。
新しいアップデートをダウンロードする前に常にバックアップを作成する	このチェックボックスを選択して、既存のアップデートのバックアップを作成してから、新しいアップデートをダウンロードします。このバックアップは、前回のアップデートへのロールバックが必要な場合に使用します。本機能はデフォルトで有効になっています。
レポートを削除するまでの日数	このチェックボックスを選択すると、指定した日数が経過した後にレポートが自動的に削除されます。本機能はデフォルトで有効になっており、日数は 10 日が設定されています。
Seqrite Endpoint Security サービスパックをダウンロードする	Seqrite Endpoint Security サービスパックのアップデートを取得するには、[**Endpoint Security サービスパックをダウンロードする**］チェックボックスを選択します。本機能はデフォルトで有効になっています。
ダウンロードするアップデートを選択する	SEPS 製品リストが表示されます。デフォルトで、すべての製品が選択されます。どのアップデートを Endpoint セキュリティにダウンロードするかを検証します。
ダウンロード速度を制限する (Kbps)	アップデートのダウンロード速度を制限したい場合は、［**ダウンロード速度を制限する（キロビット毎秒)**］チェックボックスを選択します。テキストボックスに速度を入力します。 64 ～ 8192 キロビット毎秒の範囲で速度制限を入力できます。

7. 設定を保存するには、**［適用］**ボタンをクリックします。

既存代替アップデートマネージャの詳細の修正

既存の代替アップデートマネージャの詳細を修正するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる**［アップデートマネージャ］**リンクをクリックします。

3. ［アップデートマネージャ］ページで、**［代替アップデートマネージャ］**タブをクリックします。

   すべてのアップデートマネージャのリストが表示されます。

4. 代替アップデートマネージャの横にある**［編集］**リンクをクリックします。

   ［代替アップデートマネージャの編集］ダイアログが表示されます。

5. **［アップデートマネージャ名］**と**［アップデートマネージャサイト］**またはそのいずれかを修正します。

   抱いたアップデートマネージャが EPS クライアントにインストールされている場合、アップデートマネージャサイトを編集できません。

6. 設定を保存するには、**［アップデート］**をクリックします。

代替アップデートマネージャスケジュール

この機能により、特定の頻度で代替アップデートマネージャのアップデートスケジュールを定義できます。

代替アップデートマネージャスケジュールを設定するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる**［アップデートマネージャ］**リンクをクリックします。
3. ［アップデートマネージャ］ページで、**［代替アップデートマネージャ］**タブをクリックします。

   すべてのアップデートマネージャのリストが表示されます。

4. 代替アップデートマネージャの横にある**［設定］**リンクをクリックして、代替アップデートマネージャのステータスと設定を表示します。

   ［代替アップデートマネージャの詳細］画面が表示されます。

5. **［設定］**タブをクリックします。
6. ［自動アップデートを有効にする］の横の［設定］ボタンをクリックします。

   ［アップデートマネージャスケジューラ］ダイアログが表示されます。

7. **カスタム**オプションを選択して以下のオプションを設定します:

   i. **［頻度］**で、［毎日］または［毎週］オプションを選択します。
   毎週オプションを選択した場合、リストから毎日を選択します。

   ii. **［開始時刻］**で、時刻を時間と分で設定します。

iii. アップデートマネージャのアップデートを繰り返したい場合、[**アップデートを繰り返す**]チェックボックスを選択して、スキャンを繰り返す日にちを設定します。

8. [**適用**]をクリックします。

代替アップデートマネージャの削除

既存の代替アップデートマネージャを削除するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる[**アップデートマネージャ**]リンクをクリックします。
3. [アップデートマネージャ]ページで、[**代替アップデートマネージャ**]タブをクリックします。

   すべてのアップデートマネージャのリストが表示されます。
4. 削除するものを選択してから、[**削除**]をクリックして選択した代替アップデートマネージャを削除します。

   確認メッセージが表示されます。アップデートマネージャを削除する場合
5. 代替アップデートマネージャを削除するには、[**はい**]をクリックします。

Chapter

14

ライセンスマネージャ

この機能を使用して Seqrite Endpoint Security ライセンスを管理できます。Seqrite Endpoint Security ライセンスのステータスを確認して、ライセンス情報をアップデートできます。ライセンス更新、既存セットアップへの新規ライセンス追加、追加機能パック購入を申し込むことができます。

ステータス

この機能を使用して、ライセンス情報の現在のステータスを確認できます。ライセンスのステータスを確認するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、製品名および詳細と並んでいる［**ライセンスを表示**］リンクをクリックします。
3. ［ライセンスマネージャ］ページで、［**ステータス**］タブをクリックします。

   ライセンス情報には以下の詳細情報があります:

見出し	説明
会社名	Seqrite Endpoint Security を登録する会社名を表示します。
製品名	製品名を表示します。例:Endpoint Security - 合計
プロダクトキー	Seqrite Endpoint Security のプロダクトキーを表示します。
製品タイプ	製品タイプを表示します。例:通常。
インストール番号	インストール番号を表示します。
ライセンス有効期限	Seqrite Endpoint Security ライセンスの有効期限を表示します。
使用したライセンスの数	有効期限までに使用したライセンスの数を表示します。
残りのライセンスの	残りのライセンスの数を表示します。

数	
権限付与されているライセンスの最大数	購入したライセンスの総数を表示します。
権限付与されているDLP ライセンスの最大数	権限付与されている DLP ライセンスの総数を表示します。DLP 機能を契約している場合のみ表示されます。

ライセンス情報のアップデート

この機能は、既存のライセンス情報を Seqrite 有効化サーバーと同期する際に有用です。ライセンス情報は、必要に応じてアップデートできます。

以下のライセンス情報をアップデートできます:

- ライセンスの有効期限:ライセンスを更新したにもかかわらず有効期限が更新されない、または前の有効期限が表示されている場合。
- SMS の残数:通知用に SMS バンドルを購入したものの、上限が更新されていない場合。
- メール ID:有効化を行った際に提供されたメール ID が変更されたものの、アカウントに反映されていない場合。
- 機能変更またはエディション変更はアクティベーションサーバーと同期されます。

現在購入済みのライセンスを更新したいけれどもその方法がわからない、または更新時に問題が発生している場合は、お手元のプロダクトキーを Seqrite サポートチームにお電話でお伝えください。

ライセンス履歴の表示

[ライセンス履歴] ボタンをクリックすると、ライセンス購入履歴の詳細を確認できます。[ライセンス履歴] ページに製品詳細が表示されます。以下の情報も表示されます:

- 日時:取引が行われた日付と時刻です。
- 活動:ライセンス有効化、パック追加、ライセンス更新、ライセンス追加、ライセンスの再有効化といった購入のタイプです。
- 問題の詳細:タイプ、追加されたライセンスの数、追加または削除された機能パックのタイプ、購入済みライセンスの有効期限など、取引に関連する詳細です。

ライセンス注文フォーム

この機能を使用して、追加ライセンス、既存のライセンスの更新、またはエディションのアップグレードのライセンス注文フォームを作成できます。これはオフラインで行うもので、ライセンス注文フォームを作成するためのものです。

注文フォームを作成したら印刷して、ベンダーまたはディーラーに連絡して郵送します。注文フォームは、メールに添付して Seqrite セールスチームに送信することもできます。セールスチームより購入手続きについてご連絡いたします。

ライセンス注文フォームを作成するには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. ホームページで、[**ライセンスを表示**] タブをクリックします。
3. [ライセンスマネージャ] ページで、[**ライセンス注文フォーム**] タブをクリックします。
4. ライセンス注文フォームを作成するには、以下のいずれかを選択します:
   - ライセンスを更新する:現在のライセンスを更新できます。
   - 新しいエンドポイントにライセンスを追加する:追加ライセンスを購入できます。
   - エディションのアップグレード/追加機能の購入:以下の表に従って、エディションのアップグレードや追加機能の購入を行うことができます。

EPS エディション	アップグレードパック
SME	ビジネス/合計
ビジネス	トータル

5. [**注文する**] をクリックします。

   注文が作成され、自動メールが Seqrite 部門販売担当に送信され、注文が処理されます。

ライセンスを更新する

[ライセンスを更新する] オプションを選択した場合、Seqrite のオンラインポータルにリダイレクトされ、そこでライセンス更新を注文できます。ポータルにアクセスすると、ライセンスの詳細が表示されます。

Seqrite オンラインポータルで、以下の手順に従ってください:

1. [**製品の詳細**] セクションで、お使いの製品ライセンスの詳細を確認します。必要な場合、会社のメールアドレス、管理者メールアドレス、および電話番号を変更できます。
2. [注文の更新] セクションで、更新の**間隔**を選択します。
3. システムで更新する**エンドポイントの数**（ライセンス）を選択します。
4. DLP パックを追加するには、[DLP パック] チェックボックスを選択します。すでに DLP パックに登録している場合、その DLP パックのエンドポイント番号を割り当てることができます。
5. DLP パックに割り当てるエンドポイントの番号を選択します。

6. [次へ] をクリックします。

   ライセンス更新注文の概要が表示されます。注文がご希望どおりに処理されるよう、よく確認してください。注文内容を変更する場合は、[戻る] ボタンをクリックして前のページに戻り、必要な変更を行います。

7. 注文の送り先のメール ID を入力します。

8. [要求する] をクリックします。

   ライセンス更新要求番号が生成されます。この番号はライセンス更新に関連するやり取りで必要になるので保存してください。

新しいエンドポイントにライセンスを追加する

[新しいエンドポイントにライセンスを追加する] オプションを選択した場合、Seqrite のオンラインポータルにリダイレクトされ、そこでエンドポイントの追加ライセンスを注文できます。ポータルにアクセスすると、ライセンスの詳細が表示されます。

Seqrite オンラインポータルで、以下の手順に従ってください:

1. [製品の詳細] セクションで、お使いの製品ライセンスの詳細を確認します。必要な場合、会社のメールアドレス、管理者メールアドレス、および電話番号を変更できます。

2. 追加ライセンスが必要なエンドポイント（ライセンス）の番号を選択します。

3. すでに DLP パックに登録している場合、その DLP パックのエンドポイント番号を割り当てることができます。

4. [次へ] をクリックします。

   追加ライセンス注文の概要が表示されます。注文がご希望どおりに処理されるよう、よく確認してください。注文内容を変更する場合は、戻るボタンをクリックして前のページに戻り、必要な変更を行います。

5. 注文の送り先のメール ID を入力します。

6. [要求する] をクリックします。

   ライセンス追加要求番号が生成されます。この番号は追加ライセンスの注文に関連するやり取りで必要になるので保存してください。

追加機能を購入する

[追加機能を購入する] オプションを選択した場合、Seqrite のオンラインポータルに転送され、そこで追加機能のライセンスを注文できます。ポータルにアクセスすると、ライセンスの詳細が表示されます。

Seqrite オンラインポータルで、以下の手順に従ってください:

1. **[製品の詳細]** セクションで、お使いの製品ライセンスの詳細を確認します。必要な場合、会社のメールアドレス、管理者メールアドレス、および電話番号を変更できます。
2. **[以下からアップグレードパックを選択する]** セクションで、次のうちの一つを選択します:
   - ビジネス
   - トータル
3. **[DLP パック]**（データ喪失防止を含む）チェックボックスを選択します。
4. DLP パックに割り当てるエンドポイントの番号を選択します。
5. **[次へ]** をクリックします。

   機能パックの注文の概要が表示されます。注文がご希望どおりに処理されるよう、よく確認してください。注文内容を変更する場合は、戻るボタンをクリックして前のページに戻り、必要な変更を行います。
6. 注文の送り先のメール ID を入力します。
7. **[要求する]** をクリックします。

   新しい機能パックのライセンス要求番号が生成されます。この番号は新しい機能パックに関連するやり取りで必要になるので保存してください。

エディションのアップグレード

[ライセンスをアップグレード] オプションを選択した場合、Seqrite のオンラインポータルに転送され、そこでエディションのアップグレードを注文できます。ポータルにアクセスすると、ライセンスの詳細が表示されます。

Seqrite オンラインポータルで、以下の手順に従ってください:

1. [製品の詳細] セクションで、お使いの製品ライセンスの詳細を確認します。必要な場合、会社のメールアドレス、管理者メールアドレス、および電話番号を変更できます。
2. **[以下からアップグレードパックを選択する]** セクションで、次のうちの一つを選択します:
   - ビジネス
   - トータル
3. アドオン機能パックを選択することもできます。**[DLP パック]** チェックボックスを選択します。
4. DLP パックに割り当てるエンドポイントの番号を選択します。
5. **[次へ]** をクリックします。

アップグレードパックの注文の概要が表示されます。注文がご希望どおりに処理されるよう、よく確認してください。注文内容を変更する場合は、戻るボタンをクリックして前のページに戻り、必要な変更を行います。

6. 注文の送り先のメール ID を確認します。
7. **[要求する]** をクリックします。

   新しいアップグレードパックのライセンス要求番号が生成されます。この番号は新しいアップグレードパックに関連するやり取りで必要になるので保存してください。

Chapter

15

パッチ管理

パッチ管理（PM）で、ネットワークでインストールされたアプリケーションに対し、欠落しているパッチの確認やインストールを集中管理できます。パッチ管理で、欠落しているパッチを自動的に確認したりインストールしたりすることもできます。

パッチ管理のワークフロー

1. パッチ管理サーバーをインストールする
2. パッチ管理サーバーを追加する
3. パッチ管理サーバーを設定する
4. 欠落しているパッチをスキャンする
5. 欠落しているパッチを選択してインストールする
6. インストールされた欠落しているパッチのレポートを生成する

   インストールの手順は以下の通りです。パッチ管理の他の手順はコンソールの存在に応じて記載されます。

パッチ管理サーバーのシステム要件

パッチ管理サーバーのシステム要件は Seqrite Endpoint Security サーバーのシステム要件と同じです。詳細は、SEPS サーバーのシステム要件をご覧ください。

- クライアントが 25 以上ある場合、Seqrite は Windows サーバーオペレーティングシステムでパッチ管理サーバーをインストールされることを推奨します。
- パッチ管理サーバーのインストールは Microsoft Windows XP（32 ビット）システムでサポートされません。
- PM クライアントは Microsoft Windows XP（32 ビット）システムでサポートされます。

パッチ管理サーバーのインストール

パッチ管理サーバーのインストールを開始するには、以下の手順に従ってください:

1. 32 ビット版 Windows OS の場合、 以下のリンクの一つからセットアップをダウンロードします:

   - http://dlupdate.quickheal.com/builds/seqrite/71/jap/pmsetup32.msi
   - http://download.quickheal.com/builds/seqrite/71/jap/pmsetup32.msi

   64 ビット版 Windows OS の場合、 以下のリンクの一つからセットアップをダウンロードします:

   - http://dlupdate.quickheal.com/builds/seqrite/71/jap/pmsetup64.msi
   - http://download.quickheal.com/builds/seqrite/71/jap/pmsetup64.msi

2. Seqrite パッチサーバーをインストールするネットワークのマシンでセットアップを起動します。
3. パッチ管理サーバーセットアップウィザードで［**次へ**］をクリックします。

   使用許諾契約書が表示されます。使用許諾契約書はよくお読みください。
4. ［**同意する**］チェックボックスを選択して使用許諾契約書に同意し、［**次へ**］をクリックします。
5. 別の場所にパッチ管理サーバーをインストールしたい場合は、［**参照**］をクリックします。デフォルトパスでインストールを続行する場合は、［**次へ**］をクリックします。
6. ［パッチデータベース設定］画面が表示されます。パッチコンテンツストレージフォルダーパスが表示されます。パッチコンテンツストレージパスを変更したい場合、［**参照**］をクリックします。
7. デフォルトの場所を変更したい場合、［**パッチサーバーデータのインポート**］チェックボックスを選択します。［**参照**］をクリックしてパスを指定します。

   EPS 7.0 パッチサーバーデータベースのバックアップがすでにエクスポートされている場合、EPS 7.1 パッチサーバーのデータベースにインポートすることができます。
8. ［**次へ**］をクリックします。
9. プロキシ設定を有効化および設定するには、以下を実行します:

   - ［**プロキシ設定を有効にする**］チェックボックスを選択します。

- [**プロキシサーバー**] テキストボックスに、プロキシサーバーの IP アドレスまたはドメイン名を入力します（例えば、proxy.yourcompany.com など)。
- [**ポート**] テキストボックスに、プロキシサーバーのポート番号(例: 80) を入力します。
- [**認証を有効にする（該当する場合)**] チェックボックスを選択します。
- [**ユーザー名**] と [**パスワード**] 欄に、サーバー認証を入力します。
- [**次へ**] をクリックします。

10. [アップストリームパッチサーバー] 画面で、次のうちの 1 つを選択します:
    - **Microsoft:**使用されているアップストリームパッチサーバーは Microsoft パッチサーバーです。本オプションはデフォルトで選択されています。
    - **組織のパッチサーバー (WSUS):**使用されるアップストリームパッチサーバーは組織のパッチサーバー（WSUS - Windows サーバーアップデートサービス）です。このオプションを選択した場合、WSUS サーバー URL を入力します。
11. [**次へ**] をクリックします。
12. [ウェブサイト設定] ページで、以下を実行します:
    - [サーバー設定] セクションで、次のうちの 1 つを選択します。
      - **完全なコンピュータ名**:ウェブサイトを設定するコンピューター名を指定します。
      - **IP アドレス**:ターゲットサーバーの IP アドレスを指定します。ただし、システムが DHCP で設定されている場合は、IP アドレスを選択しないことをお勧めします。
    - [**HTTP ポート**] テキストボックスで、サーバーのリスニングポートとして使用するポート番号を入力します。
    - [**Secure Socket Layer を有効にする**] チェックボックスがデフォルトで選択されています。SSL ポート番号を入力します。このポート番号はサーバーのリスニングポートとして機能します。
    - [**次へ**] をクリックします。
13. 確認のプロンプトが表示されたら [**はい**] をクリックします。
14. インストール概要画面が表示されます。必要な場合、[**戻る**] をクリックして、設定を変更することができます。

    [**インストール**]をクリックします。インストールが開始されます。
15. インストールを完了するには、[**終了**] をクリックします。

インストール/アンインストールに失敗すると、[**インストールログの表示**] チェックボックスのみが表示されます。ログを表示するには、[**インストールログ**

の表示］チェックボックスを選択します。

16. インストールの終了後、EPS コンソールから Seqrite パッチサーバーを追加すると利用可能になります。

Microsoft Windows OS のクライアントのみがパッチ管理機能を利用できますが、Mac と Linux オペレーティングシステムのクライアントにはサポートされません。

リモートクライアントに対する推奨事項

リモートクライアントの場合、リモートクライアントが展開されるネットワークでパッチサーバーをインストールします。パッチサーバーのプライベート IP はパブリック IP に変換しなければなりません。

パッチサーバーデータのバックアップ

パッチサーバーのパッチデータベースとパッチコンテンツをバックアップします。

パッチサーバーデータをバックアップするには、以下の手順に従ってください:

1. <installation directory>/Seqrite パッチ管理/パッチサーバー/コンテンツフォルダにあるすべてのファイルとフォルダーを手動でバックアップします。
2. ［**スタート**］>［**プログラム** ］>［**Seqrite パッチサーバーデータのバックアップ**］の順に選択します。バックアップウィザードが起動します。
3. ［**参照**］をクリックして、パッチデータベースをバックアップするパスを指定します。
4. ［**バックアップ**］をクリックします。

   「pmdb.exp」データベースファイルが生成されます。このファイルはパッチサーバーデータベースを復元するために使用できます。

パッチサーバーのアンインストール

パッチサーバーをアンインストールするには、以下の手順に従ってください:

1. ［**スタート**］>［**プログラム**］>［**パッチサーバーのアンインストール**］を表示します。

   アンインストールウィザードが起動します。
2. ウィザードが完了すると、パッチサーバーがアンインストールされます。

Chapter

16

技術サポート

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。

サポートオプションには、よくある質問に対する回答を FAQ で見つける、質問を送信する、メールで質問を送信する、直接電話で問い合わせるなどがあります。

サポートオプションにアクセスするには、以下の手順に従ってください:

1. Seqrite Endpoint Security ウェブコンソールにログオンします。
2. Seqrite Endpoint Security ダッシュボードの右上の［**サポート**］ボタンをクリックします。

サポートには以下のオプションがあります:

ウェブサポート:FAQ を見る（よくある質問）と**フォーラムに参加する**という 2 つのサービスを提供しています。これらのサポートサービスから質問をメールで送り、適切な回答を得ることができます。

メールサポート:当社のサポートウェブページに転送される**チケットを送信する**サポートを提供しています。サポートウェブページで、よくある質問とその回答を読むことができます。問題の回答を見つけられない場合は、チケットを送信します。

ライブチャットサポート:このオプションを使用して、当社のサポート担当者とチャットすることができます。

リモートサポート:このサポートモジュールでは、遠隔操作でお客様のコンピュータシステムに接続して技術的な問題を解決するお手伝いをします。

電話サポート:

電話サポートのご希望の場合は製品ご購入元販売代理店までお問い合わせください。

その他お問い合わせ先 :

techsupport@quickheal.co.jp

その他のサポートソース

その他のサポートソースについては、以下のサイトをご覧ください:

http://www.seqrite.com/seqrite-support-center

プロダクトキーを紛失した場合

プロダクトキーはお客様の Seqrite Endpoint Security 製品の ID の役割を果たしています。プロダクトキーを紛失した場合は、再発行しますので Seqrite 技術サポートまでご連絡ください。プロダクトキーの再発行には、若干の手数料が発生します。

本社問合せ先

Quick Heal Technologies Limited

(旧 Quick Heal Technologies Pvt. Ltd.)

Reg. Office:Marvel Edge, Office No.7010 C & D, 7th Floor,

Viman Nagar, Pune 411014, Maharashtra, India.

公式ウェブサイト:http://www.seqrite.com.

メール:support@seqrite.com