



Seqrite

# Endpoint Security Total エディション

企業向け統合エンドポイントセキュリティと管理コンソール

## 製品の特長

データ漏えいを防ぎ、資産やファイル転送を監視し、Webセキュリティとアンチウイルスの堅牢な機能を提供する革新的なエンドポイントセキュリティです。

- » マルウェア対策、Webの保護、ブラウザの保護、データの保護(DLP)がすべて1つのライセンスで利用可能
- » すべてのMicrosoftアプリケーションの脆弱性に対するパッチに関するニーズを満たす統合パッチ管理ソリューション
- » 優れた資産管理機能により、Windows、Mac、Linuxの各エンドポイントの包括的かつ累積的な情報を提供
- » 管理者はデバイス名と時間単位のアクセスを指定してUSBインターフェイスを完全に制御可能
- » 1つの管理コンソールからWindows、Mac、Linuxのエンドポイントを強力に保護
- » エンドポイントネットワーク全体のランサムウェアインシデントの報告

## 機能



### アプリケーションコントロール

従業員が使用するさまざまな外部デバイスを管理できます。組織は、WindowsプラットフォームとMacプラットフォームでさまざまなデバイスタイプを制御、設定し、それぞれにアクセスポリシーを定義できます。この機能を使用すると、IT管理者は以下を許可できます。

- » 特定のクライアントからデバイスへのアクセスを一定期間、一時的に許可
- » USB大容量ストレージデバイスへのモデル名による指定アクセス
- » 大容量ストレージと入力デバイスを除くすべてのUSBデバイスのUSBインターフェイスのブロック
- » すべてのファイルシステムの完全なデバイス暗号化

これらの拡張機能に加え、各外部ストレージデバイスに以下のアクセスタイプを設定できます。

- **許可**: デバイスとの間でデータを転送可能
- **ブロック**: デバイスとの間でデータを転送不可
- **読み取り専用**: デバイスからデータの読み取りのみ可能



## ランサムウェア対策

ランサムウェア対策機能は、プログラムの動作をリアルタイムで分析する、Seqriteの行動ベースの検出テクノロジーを使用します。このテクノロジーが、ランサムウェアなどの脅威の検出とブロックに役立ちます。また、追加の保護レイヤーとして、データが安全な場所にバックアップされるので、ランサムウェア攻撃を受けた場合にファイルをリストアできます。

**Seqriteのランサムウェア対策機能は、他のランサムウェア対策ツールよりも効果的かつ先進的。**

- » **シグネチャベースの検出:** 感染したEメール、USBドライブなどのメディア、ネットワーク内の感染したシステムを通じてシステムに侵入しようとする既知のランサムウェアを検出します。
- » **システムで新たなランサムウェア感染をプロアクティブに監視:** その一部がランサムウェア攻撃になりうるダウンロードファイルのアクティビティを監視します。
- » **行動ベースの検出エンジンで動作:** プログラムの動作をリアルタイムで分析するので、被害が及ぶ前にプログラムを停止できます。
- » **データのバックアップとリストアのツールを組み込み:** バックアップとリストアのツールが、重要なファイルをプロアクティブにバックアップし、安全な場所に保存します。ランサムウェア攻撃を受けた場合はこれらのファイルをリストアできます。



## Webフィルタリング

特定のカテゴリのWebサイト（例：ソーシャルネットワーキング、ゲームなど）や、個々のユーザーが指定するWebサイトをブロックすることで、Webアクセスを制限し、生産性を向上できます。

## アプリケーションコントロール

アプリケーションのカテゴリ別に、ネットワーク内での実行を許可または却下できます。この機能は、既存のブロックリストにカスタムアプリケーションを追加できる柔軟性も備えています。

- » アプリケーションのカテゴリ全体を許可または却下可能
- » 事前定義されたブロックリストにないカスタムアプリケーションを追加可能
- » ネットワーク内にインストールされているすべてのアプリケーションの概要（許可または却下）を表示

## アセットマネジメント

すべてのエンドポイントのハードウェアとソフトウェアの構成に関する包括的、累積的な情報を示します。管理者は、各システムに関連するハードウェア構成、システム情報、インストールされているアップデート、ハードウェア / ソフトウェアの変更点を容易に確認できます。任意のシステムでハードウェアまたはソフトウェアの変更があった場合は、設定されているEメールアドレスに通知が送られます。たとえば、RAMに変更があった場合、変更に関する詳細情報を示す通知が管理者に送信されます。

## 脆弱性スキャン

この機能は、ネットワーク内にインストールされているアプリケーションとオペレーティングシステムの既知の脆弱性をリアルタイムでスキャンします。既知の脆弱性に対するセキュリティ対策を確立し、脅威エージェントによるセキュリティ侵害を防止できます。

- » Adobe、Safari、Mozilla、Oracleなどのアプリケーションの脆弱性をスキャン
- » ネットワーク内のコンピュータで利用されていてパッチが適用されていないオペレーティングシステムに関する通知を送信



## パッチマネージメント

一元的なパッチ管理戦略により、セキュリティの脆弱性に効果的に対処できます。IT管理者は、エンドポイントにインストールされているMicrosoftアプリケーションに未適用のパッチを確認し、インストールできます。一元化されたシンプルなアプローチで、必要なパッチをすべて確実に展開することで、セキュリティのリスクを軽減し、ネットワークの生産性を向上できます。



## 情報漏えい対策 (DLP)

リムーバブルデバイス、ネットワーク共有、Webアプリ、オンラインサービス、スクリーンショット、システムクリップボードなどのデータ転送手段を制御することで、組織内外での情報漏えいを防止できます。DLPには、エンドポイントやリムーバブルデバイスの保存データをスキャンする機能もあります。DLPでは、以下のものを制御できます。

- » Officeファイル、グラフィックファイル、プログラミングファイルなど
- » クレジットカード / デビットカード情報、個人ファイルなどの機密情報
- » ユーザー定義のカスタム辞書の実装、データ漏えいに関する即時のアラートや累積的レポートの入手が可能



## ファイルアクティビティモニター

機密ファイルを監査し、ファイルのコピー、名前変更、削除などの不審な操作を監視します。この方法で、内外の脅威をブロックし、機密データの漏えいを監視できます。ローカルドライブ、リムーバブルドライブ、ネットワークドライブに転送されるファイルもすべて監視できます。

ファイルのアクティビティの監視ツールは、ネットワーク内外に移動するすべてのファイルを監査できると同時に、組織内にあるあらゆる形式の機密ファイルに対する操作を大局的に把握できる、重要な機能です。管理者は、この機能による監視から除外するフォルダのパスを指定できます。



## IDS/IPS

高度な防御により、ポートスキャン攻撃、DDoS (Distributed Denial of Service) など、さまざまな攻撃を検出できます。この検出機能は、すべての通信にセキュリティレイヤーを実装して、不正な侵入や攻撃からシステムを守ります

- » **不正侵入防御:** アプリケーションのソフトウェア脆弱性の悪用を試みる不正なネットワークアクティビティをブロックします。
- » **ポートスキャン攻撃の防止:** 基本的に、ポートスキャン攻撃は、ネットワーク内の各ポートに順番にメッセージを送信します。攻撃元は、受け取る応答に応じて、ポートが使用されているかどうか、さらに脆弱性を探せるかどうかを判断します。この機能は、ネットワーク内で開いているポートを攻撃しようとする侵入者をブロックします。
- » **DDoS攻撃の防止:** DDoS (Distributed Denial of Service) は、DoS攻撃の一種であり、通常はマルウェアに感染した複数のシステムを使用して、単一のシステムを標的としてサービス拒否攻撃を仕掛けます。Seqrite Endpoint Securityは、ネットワーク内のあらゆるシステムに対するあらゆるDDoS攻撃の開始を適切にブロックします。



## グループポリシー管理

ネットワーク内に異なるユーザグループを定義付けし、それぞれのグループごとに柔軟にポリシーを設定できます。



## スパム対策

エンドポイントの受信トレイで、ネットワークの防御をくぐり抜けたスパム、フィッシング攻撃、迷惑メールをスキャンします。



## サードパーティのアンチウイルスの削除

EPSクライアントのインストール時に別のアンチウイルスソリューションが検出された場合は、そのアンインストーラが起動するか、ソリューションが自動的にアンインストールされます。既存のアンチウイルスソリューションがシステムから削除されるまで、Seqrite EPSのインストールは実行されません。



## ブラウジングの保護

ネットワーク内からアクセスされた不正なWebサイトによる攻撃からエンドポイントクライアントを保護できます。



## フィッシング対策

インターネット上の不正なコードによるフィッシング攻撃は、ネットワークに侵入し、拡散する前に阻止されます。



## ファイアウォール保護

企業ネットワークに対する不正アクセスをブロックします。観測されたネットワークトラフィックに基づいて、カスタマイズルールを低、中、高、またはすべてブロックに設定できます。管理者は、特定のIPアドレスやポートを許可またはブロックする例外も設定できます。3つのファイアウォールカスタマイズレベルは以下のとおりです。

- » **低:** 低に設定されたファイアウォールでは、追加の例外を除き、送受信するトラフィックがすべてアクセス許可されます。
- » **中:** 追加の例外を除き、送信するトラフィックはすべて許可されますが、受信するトラフィックはブロックされます。
- » **高:** 追加の例外を除き、送受信するトラフィックがすべてブロックされます。
- » **すべてブロック:** 送受信するトラフィックがすべてブロックされます。

この機能では、ファイアウォールルールに例外を設定することもできます。たとえば、ファイアウォール設定を「高」に設定した場合、特定のIPアドレスまたはポートの接続をすべて許可する例外を追加できます。



## チューンアップ

この機能は、ジャンクファイルを消去し、レジストリ / ディスクの無効なエントリを削除することで、ネットワーク内のコンピュータシステムのパフォーマンスを向上させます。

- » チューンアップは、Endpoint Security Serverからすべてのエンドポイントに対して実行できます。
- » 特定の日時にメンテナンスのスケジュールを設定することもできます。





## ローミングプラットフォーム

Seqriteローミングプラットフォームは、企業がエンドポイントへの接続を維持し、エンドポイントを管理できるクラウドベースのソリューションです。エンドポイントはローカルの企業ネットワークに接続していなくてもかまいません。この機能により、ネットワーク管理者は、エンドポイントの最新状況を確認し、ネットワークに接続していないエンドポイントに対して以下の操作を容易に行うことができます。

- » コンプライアンス状況を確認する
- » セキュリティポリシーを適用する
- » セキュリティ上の脅威をスキャンする
- » チューンアップを実行してパフォーマンスを向上させる
- » ローミングクライアントをリダイレクトする
- » サービスパックを適用する
- » レポートと通知を確認する



## EメールとSMSの通知

この機能は、事前設定されたEメールアドレスや電話番号に通知を送ります。

- » ネットワーク管理者は、ウイルスの検出、ウイルスの大量発生、許可されていないデバイスへのアクセス、ライセンス期限などの重大なネットワークイベントに関する通知を受け取ることができます。



## 複数のアップデートマネージャ

この機能では、複数のアップデートマネージャをネットワーク全体に展開できます。これは、ロードバランシングと、アップデートマネージャが1つである場合によく見られる、ネットワーク輻輳の防止に役立ちます。

## その他

SeqriteのWindowsクライアントのビルドや機能もEndpoint Securityに統合されています。Windowsクライアントの以下の設定をEPS Serverから設定することもできます。

- » **行動検出システムの設定**: これらの設定は、ヒューリスティックなスキャンング手法でアプリケーションを調べることで、未知のウイルス、マルウェア、その他の脅威をリアルタイムで検出します。
- » **セーフモード保護の設定**: これらの設定により、セーフモードになっているコンピュータへの不正アクセスを防止できます。

## Product Comparison

Features	Business	Total	Enterprise Suite
アンチウイルス	✓	✓	✓
Eメール保護	✓	✓	✓
IDS / IPS	✓	✓	✓
ファイアウォール保護	✓	✓	✓
フィッシング対策	✓	✓	✓
ブラウジングの保護	✓	✓	✓
SMS 通知	✓	✓	✓
脆弱性スキャン	✓	✓	✓
ローミングプラットフォーム	✓	✓	✓
アセットマネージメント	✓	✓	✓
スパム対策	✓	✓	✓
Web フィルタリング	✓	✓	✓
アドバンスドデバイスコントロール	✓	✓	✓
アプリケーションコントロール		✓	✓
チューンアップ		✓	✓
ファイルアクティビティモニター		✓	✓
パッチマネージメント		✓	✓
情報漏えい対策 (DLP)			✓

# システム要件

---

## EPSサーバ オペレーティングシステム

- 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 / Home Premium / Professional / Enterprise / Ultimate (32ビット/64ビット)
- Microsoft Windows Vista Home Basic / 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 and SP2 / Professional Edition (32ビット/64ビット)
- Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / 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)

### Note:

- 25クライアント以上の場合、Windows Server OSにEPSサーバとパッチマネージメントサーバをインストールすることを推奨します

- 500クライアント以上の場合、専用Webサーバ(IIS)を立てることを推奨します

### 最少推奨要件(コンソールシステム)

- プロセッサ:
  - 最少: 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
- メモリ:
  - 最少: 2 GB
  - 推奨: 4 GB 以上
- 空きハードディスク容量:
  - 最少: 4.8 GBの空きハードディスク容量
  - 推奨: 10 GB の空きハードディスク容量
- Internet Explorer 7 以上
- 256色モードで、解像度1024 x 768をサポートするモニタ

### Java Runtime Environment (JRE) 要件

ウェブページからインストールまたはメールインストールを実行したり、デバイスの機能を追加する場合には、以下が要件となります:

- 32ビットWindows OS時
  - » JRE7またはJRE8のインストール
- 64ビットWindows OS時
  - » 32ビットブラウザから実行する場合、32ビットJRE7またはJRE8のインストール
  - » 64ビットブラウザから実行する場合、64ビットJRE7またはJRE8のインストール

## コンソールシステム追加ソフトウェア要件

Seqrite EPS サーバには、コンピュータシステム上にMicrosoft .NET Framework 4.0 と同様に、Microsoft IIS Web Serverが必要です。Microsoft IISのバージョンについては、以下を参照してください。

- IIS Version 10 (Windows 10)
- IIS Version 8.5 (Windows 8.1, Windows Server 2012 R2)
- IIS Version 8.0 (Windows 8, Windows Server 2012)
- IIS Version 7.5 (Windows 7, Windows Server 2008 R2)
- IIS Version 7.0 (Windows Vista, Windows Server 2008)
- IIS Version 6.0 (Windows Server 2003)
- IIS Version 5.1 (Windows XP SP3)

IISのインストール方法については、[ここをクリック](#)。

- 以下のIISコンポーネントの設定を確認ください:
- IIS Management Console
- Default Document
- Static Content
- CGI
- ASP.NET 4.0または以降のバージョン

## EPSクライアント

### Windows ワークステーション環境

- 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)

- Seqrite EPS のウェブサイトを見る場合は、Google Chrome ver.45, 46, 47 または、Mozilla Firefox ver.38, 39, 40を推奨します。

## For Windows

ウェブページからインストールまたはメールインストールを実行したり、デバイスの機能を追加する場合には、以下が要件となります:

- プロセッサ:
- 最少: 1 GHz 32ビット (x86) または 64ビット (x64) プロセッサ (Windows Vista)
- 推奨: 2 GHz 32ビット (x86) または 64ビット (x64) プロセッサ(Windows Vista以降)
- メモリ:
- 最少: 1 GB
- 推奨: 2 GB以上
- ハードディスクの空き容量:
- 最少: 3.2 GB の空きハードディスク容量

## For Mac

- Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12
- インテルまたはインテル互換性プロセッサ
- メモリ:
- 最少: 512 MB
- 推奨: 2 GB以上
- 1.2 GBの空きハードディスク容量

## For Linux

- 300 MHz 以上のインテルまたはインテル互換性プロセッサ
- メモリ:

- 最少: 512 MB
- 推奨: 2 GB以上
- 1.2 GB の空きハードディスク容量

## 32ビット

- RHEL 6.1, 6.2, 6.3, 6.4, 6.6, 6.7, 6.8
- BOSS 6
- Fedora 14, 18, 19, 20, 21, 25
- openSUSE 11.4, 12.2, 12.3, 13.2, 42.2
- Linux Mint 13, 14, 15, 16, 17.3, 18
- Ubuntu 10.10, 11.4, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.10
- CentOS 6.3, 6.4, 6.5

## 64ビット

- RHEL 6.1, 6.2, 6.3, 6.4, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3
- Fedora 14, 18, 19, 20, 21
- openSUSE 11.4, 12.2, 12.2
- Linux Mint 13, 14, 15, 16, 17.3, 18
- Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.10
- CentOS 6.3, 6.4, 6.5, 7.0
- SUSE Linux 11.00, 12.00, 12.2



EPSクライアントは、上記環境をサポートします。また、以下の要件に合致する場合、他のバージョンもサポート対象となります。

32ビットOS時: GNU C Library 2.11以降

上記LinuxOS以外のクライアントの場合、本番環境への実装前に、テスト環境でのクライアント検証をされることを推奨します。

システム要件とより詳細な情報が必要な場合、product manualを参照願います。



クイックヒール テクノロジーズ ジャパン株式会社

〒104-0033 東京都中央区新川 1-2-8 第5 山京ビル 10F

Phone : 03-6228-3983 | Fax : 03-6228-3984

Email (sales) : sales@quickheal.co.jp | www.quickheal.co.jp または www.seqrite.jp