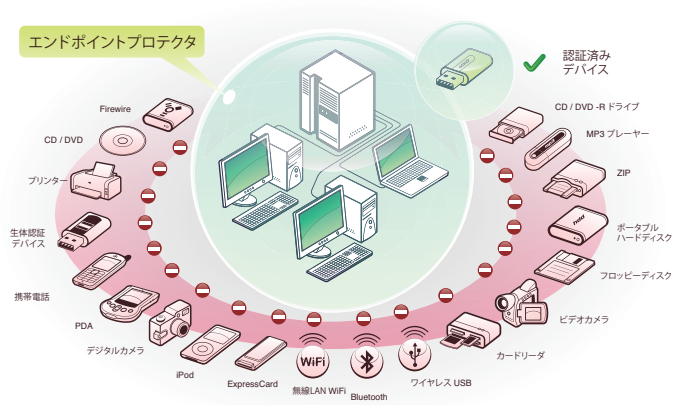
Endpoint Protector 2009™

Device Control and Data Loss Prevention for businesses

Windows XP/Vista/7 Client Version: 3.0.7.3
Windows 2003/2008 Server Version: 3.0.4.1
Mac OS X Version: 1.0.4.4
Linux Server Version: 3.0.4.1

エンドポイントも、データもこれで安全。



エンドポイントプロテクタ 2009 は、企業方針に沿ったエンドポイントでのポータブルデバイスの利用ルールを強化するためのアプローチを提供します。その上、PC と Mac のどちらもプロテクションできる唯一のソリューションです。エンドポイントプロテクタ 2009 は、世界のいたるところでワークスタイルやライフスタイルを変えているポータブルなライフスタイル・デバイスを、生産力を維持しつつ、仕事をより便利で、安全で楽しく利用できるように設計されています。

ホワイトリストベースのアプローチが、ある特定のデバイスに対して特定のユーザ／グループの使用を許可するので、どんなデバイスが使用されているか、そして、ユーザがどんなデータを移すことができるかなどの設定や制御をしている間も生産性は保たれます。

エンドポイントプロテクタ 2009 は内部からの脅威によってもたらされるデータの漏えいや、盗難、破損、あるいは何らかの信用を落とすような危険を劇的に減少させます。

制御可能なデバイスのタイプ:

- USB フラッシュドライブ (Normal USB Drives, U3, etc.)
- メモリーカード (SD, MMC, CF, etc.)
- CD/DVD-ドライブ (内蔵タイプ、外付けタイプ)
- 外付けハードディスク
- フロッピードライブ
- カードリーダー (内蔵タイプ、外付けタイプ)
- ZIP ドライブ
- デジタルカメラ
- スマートフォン／BlackBerry／PDA
- iPod／iPhone
- FireWire デバイス
- MP3 プレーヤ／メディアプレーヤ
- Biometric ドライブ
- Bluetooth デバイス
- プリンタ
- Express カード (SSD)
- ワイヤレス USB

Endpoint Protector 2009
PC と デバイスの間のファイヤーウォール

エンドポイントプロテクタで、デバイスの社内利用方針や、データセキュリティにおける規定や基準、データ不履行管理やIT基準の遵守が容易になります。

TrustedDevicesを使用することで搬送時のデータの暗号化を実施します。

ワークステーション、ノートブック、ネットブック用のエンドポイントセキュリティ

持ち運び可能なポータブルデバイスによってプロテクションに反する脅威が引き起こされます。 データの意図的、または偶然の漏えい、窃盗、損失、またはマルウェア感染を防止します。

デバイスの管理／デバイスの制御

ネットワーク上のデバイスへのユーザ、コンピュータからの権限を定義します。

Webベースの集中管理／ダッシュボード

持ち運び可能なポータブルデバイスの使用は集中管理されます。Web ベースの管理およびリポーティングインタフェースは、管理者や、IT セキュリティスタッフの需要を満たし、広範囲にわたる組織内のデバイスの制御とデータ転送活動のリアルタイムな情報を提供します。

ファイルトレーシング／ファイルシャドーイング

ファイルトレーシングはあらかじめ認証されたデバイスへのコピーおよび、コピー先のすべてのデータを記録します。 ファイルシャドーイングは制御デバイスで使用されたすべてのファイル（削除されたものでさえ）保存します。

ファイルホワイトリスティング

認証されたファイルだけが認証されたデバイスに移すことができます。 その他のすべてのファイルはブロックされ、試みられた転送は報告されます。

デバイス稼動ログ – Audit Trail（監査証跡）

デバイスの稼動ログはすべてのクライアントと接続されたデバイスに保存され、監査と詳細分析のためのデバイス、PC および、ユーザーの履歴を提供します。

リポートと分析

稼動状況の精査を簡単にする強力なレポート、グラフィックスと分析ツール。

セキュリティポリシーを簡単に施行 (Active Directory)

定義済みのユーザグループ (Active Directory GPO) 向けのカスタマイズ可能なテンプレートによる単純化されたデバイス管理ポリシーはネットワーク間でのセキュリティポリシーの施行と管理を容易にします。

仮のオフラインパスワード／ネットワーク「オフライン」モード

保護された PC がネットワークから切り離されてもセキュリティは保たれます。オフライン仮パスワード機能により、生産性を損なうことなく、移動先でもデバイスの使用を暫定的に許されることができます。

Endpoint Protector クライアントセルフディフェンス

ユーザが管理権限を持っている PC であっても、保護を提供します。

エンドポイントのセキュリティポリシーを施行し、データがどのように、誰によって転送されるのかを制御します。

システム条件

クライアント

- *Windows 7 (32/64bit)*
- *Windows Vista (32/64bit)*
- *Windows XP (SP2) (32/64bit)*
- *Windows 2003/2008 (32/64bit)*
- *Mac OS X 10.4+*
- *.Net 2.0 Framework*
- 最小で *32 MB* のディスク空き容量

サーバ

サポート可能なOS:

- *Windows 2003 Server*
- *Windows 2008 Server*
- *Debian (*Ubuntu), Red Hat (Fedora, CentOS), Suse*

サポート可能な Web サーバ:

- *IIS 6.0 / 7.0 or*
- *Apache (Version 5 or newer)*

サポート可能なデータベース:

- *Microsoft SQL 2005/2008 (Exp.)*
- *or MySQL (Version 5 or newer)*

追加のサーバ条件:

- *PHP (Version 5) with SOAP support*
- *OpenSSL Version 0.9.8*

ディレクトリサービス

- *Active Directory*

MSI 配布メカニズムを通して設定する簡単なセットアップ。

エンドポイントプロテクタサーバは、異なるプラットフォームのサーバとの互換性があるので、既存のインフラストラクチャに対して素早く、費用対効果の高いインテグレーションを可能にします。

直感的な *Web* ベースのインタフェースで、効率の良い管理を可能にします。

Endpoint Protector 2009 ダッシュボード
リポート／管理ツール

Endpoint Protector 2009 は３つのパートのセキュリティで構成されています。
予防 – モニタリング – 暗号化と施行

Endpoint Protector はポータブルストレージとエンドポイントデバイスを利用する作業環境に**安心**と**安全**を提供します。ネットワークのエンドポイントセキュリティポリシーが実施されている間、保護されている PC でも認可されたデバイスは継続して使用できるので、ユーザの効率は制限されません。

強制暗号化 - EasyLock TrustedDevice 技術によって機密データデータの搬送を保護します

TrustedDevice 技術は保護された環境で、エンドポイントソフトウェアとセキュリティーポリシーを通じてすべてのエンドポイントデバイスの認可、制御をするだけでなく、搬送時における取り扱いに注意の必要な機密データを保証し、信用できるよう保護することを証明するように設計されています。格納されたすべてのデータが暗号化されているのでデバイスが盗まれたり、なくしてしまった場合に、第三者によってアクセスされることはありません。

詳しい情報、フリートライアルはこちら： www.EndpointProtector.com

CoSoSys Ltd.
E-Mail: sales@cososys.com
Phone: +40-264-593110
Fax: +40-264-593113

アップタウン株式会社
info-office@uptown.jp
(048)711-2731 Fax: (048)711-2730
〒330-0071 埼玉県さいたま市浦和区上木崎1-15-5
アップタウン株式会社
http://uptown.jp/