ENDPOINT PROTECTOR

by CoSoSys

情報漏えい対策（DLP）と モバイルデバイス管理

あらゆるネットワーク規模とあらゆる業界に柔軟に対応

Windows、Mac、Linuxに対応するDLPソリューション

ネットワーク全体を保護

ジュピターテクノロジー

https://www.jtc-i.co.jp/
042-358-1250

ENDPOINT PROTECTOR

by CoSoSys

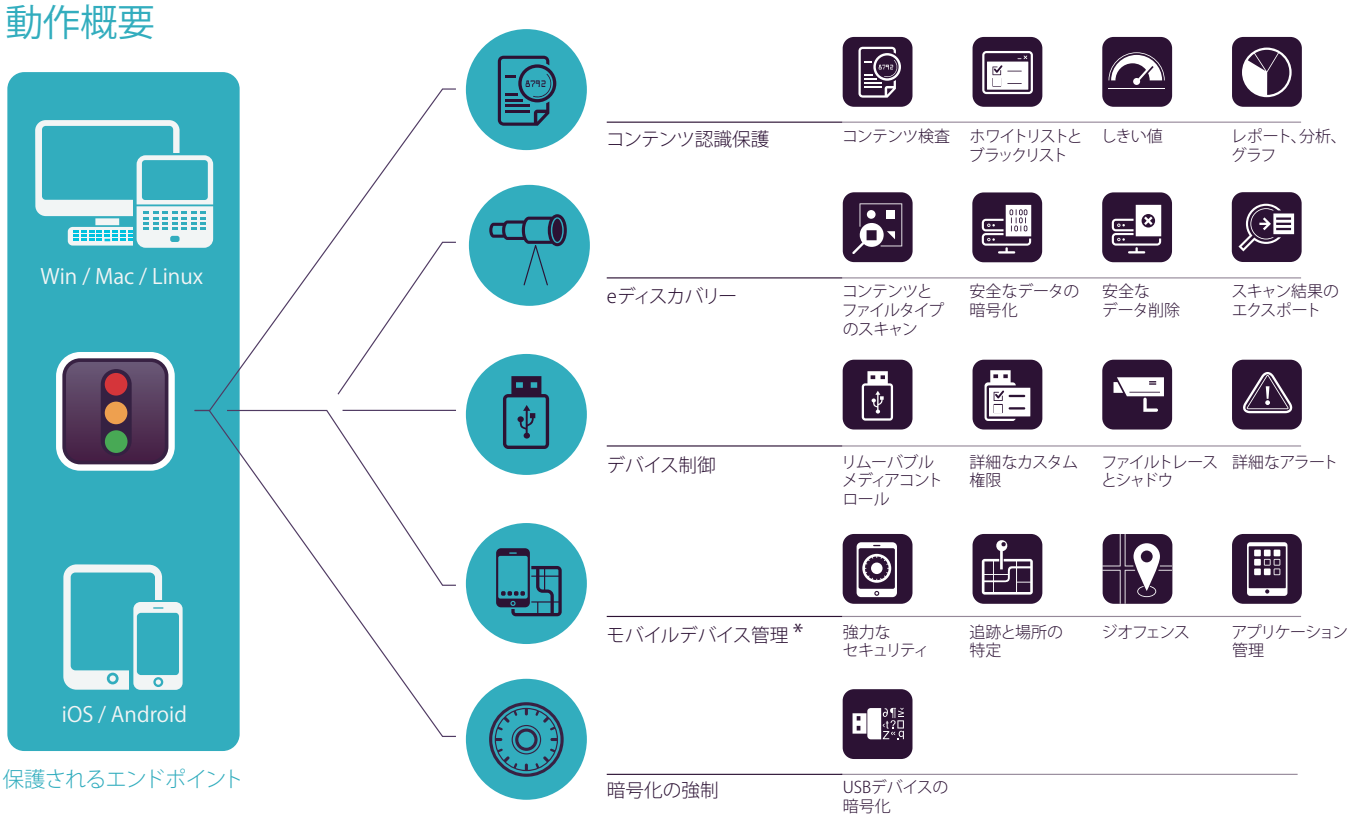
ポータブルストレージデバイス、クラウドサービス、モバイルデバイスによって引き起こされる脅威から機密データを保護するためのすぐに使えるソリューション

ポータブル、ライフスタイルデバイス、クラウドが仕事や生活の仕方を変えている世界で、Endpoint Protector は、生産性を維持しながら作業をより便利で安全に簡単に、内部脅威からデータを保護するよう設計されています。

ブラックリストとホワイトリストに基づいたアプローチは、ポリシーを作成することで柔軟性のある権限を与えることができます。組織は特定の PII（個人識別情報）をスキャンし、業務を中断させることなく、特定のコンピューター / ユーザー / グループの特定の URL とドメイン名への転送を許可しますが、特定のリムーバブルデバイスの使用やクラウド共有アプリケーション、その他のオンラインサービスへのデータ転送を拒否する選択肢があります。

Endpoint Protector は、ハードウェアまたは仮想アプライアンスとして提供され、数分でセットアップできます。さらに、レスポンシブ管理インターフェイスにより、デスクトップからタブレットまで、あらゆるデバイスからのポリシーの管理とレポートの参照が可能です。
Endpoint Protector は、漏えい、盗難、他の侵害によりデータが漏えいする可能性のある内部脅威の発生リスクを大幅に削減します。さらに、さまざまなルールや規制にも準拠できます。

動作概要



コンテンツ認識保護（Windows、macOS、Linux）	操作中のデータを監視および制御して、さまざまな出口ポイントを経由して機密ファイルを持ち出すことができるかどうかを判断します。フィルターは、ファイルタイプ、アプリケーション、定義済みおよびカスタムコンテンツ、正規表現などを設定できます。
eディスカバリー（Windows、macOS、Linux）	ネットワークのエンドポイントに保存されているデータをスキャンし、機密データが承認されていないコンピューターで検出された場合、暗号化や削除などの対応処理を適用します。
デバイス制御（Windows、macOS、Linux）	USB と周辺機器ポートの監視と制御。デバイス、ユーザー、コンピューター、グループ、グローバル権限を設定します。
モバイルデバイス管理 *（Android、iOS、macOS）	スマートフォンやタブレットのセキュリティレベルを管理、制御、調整します。プッシュセキュリティ設定、ネットワーク設定、アプリケーションなど
暗号化の強制（Windows、macOS）	USB ストレージデバイスにコピーされたデータを AES 256 ビット暗号化で自動的に保護します。クロスプラットフォーム対応、パスワードベースで使いやすく、非常に効果的です。

* 販売準備中の機能です。

ジュピターテクノロジー
https://www.jtc-i.co.jp/
042-358-1250

コンテンツ認識保護
（Windows、macOS、Linux）

メールクライアント：Outlook / Thunderbird / Lotus Notes
Webブラウザ：Internet Explorer / Firefox / Chrome / Safari
インスタントメッセージ：Skype / Microsoft Communicator / Yahoo Messenger
クラウドサービスとファイル共有：Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa
その他 アプリケーション：iTunes / Samsung Kies / Windows DVDメーカー / Total Commander / Team Viewer など

定義済みコンテンツフィルター
フィルターは、クレジットカード番号、社会保障番号など、事前に定義されたコンテンツに基づいて作成することができます。

カスタムコンテンツフィルター
フィルターは、キーワードや式などのカスタムコンテンツに基づいて作成することもできます。さまざまなブラックリスト辞書を作成できます。

正規表現フィルター
詳細なカスタムフィルターを作成して、保護されたネットワーク間で転送されるデータの一定の反復を見つけることができます。

ファイルタイプフィルター
ファイルタイプフィルターは、ユーザーが手動で修正した場合でも、その拡張子に基づいて特定の文書をブロックするために使用できます。

ファイルホワイトリスト
他のすべてのファイル転送はブロックされますが、冗長性を回避し生産性を高めるためにホワイトリストを作成することができます。

ドメインと URL のホワイトリスト
会社のポリシーを厳守しますが、従業員は仕事をする上で必要な柔軟性を得ることができます。会社のポータルまたはメールアドレスをホワイトリストに登録します。

プリントスクリーンの無効化
画面キャプチャ機能を無効にし、画面に表示される貴重なデータが保護されたネットワークから流出しないようにします。

クリップボードの監視
コピー & ペースト / カット & ペーストにより機密コンテンツの情報漏えいをなくし、データセキュリティポリシーをさらに強化します。

レポートと分析
強力なレポートおよび分析ツールを使用して、ファイル転送に関連するアクティビティを監視します。ログとレポートは SIEM ソリューションにエクスポートすることもできます。

ダッシュボードとグラフィックス
最も重要なイベントや統計情報をすばやく視覚的に確認するために、グラフや図を利用できます。

Active Directory
AD などのツールを活用して、大規模環境での展開をより容易にします。すべてのグループと監視対象をインポートして同期できます。

フィルターのグローバルおよび通常のしきい値
ファイル転送が許可される違反回数を定義します。これは、各コンテンツタイプまたはすべての違反の合計に適用されます。

ファイルトレース
さまざまなオンラインアプリケーションやクラウドサービスへのすべてのファイル転送や試行を記録し、ユーザーの行動を明確に表示します。

ファイルシャドウ
制御されたデバイスに転送されるか、または、メール、クラウドストレージ、その他のアプリケーションを使って転送されるファイルのコピーを保存します。

オフライン一時パスワード
一時的に、ネットワークから切断されたコンピューターへのファイル転送を許可します。セキュリティと生産性を確保できます。

メールアラートの作成
機密ファイル転送に関連する最も重要なイベントに関する情報を提供するために、定義済みメールアラートとカスタムメールアラートを設定することができます。

プリンターの DLP
ローカルプリンターとネットワークプリンターの機密文書の印刷をブロックし、情報漏えいやデータ盗難を防止するためのポリシーを設定できます。

HIPAA コンテンツ認識ポリシー
PHI 情報、FDA 承認医薬品、ICD-9 コードなどの転送が行われる前に、文書を詳細にスキャンすることができます。

シンクライアントの DLP
ターミナルサーバーのデータを保護し、他の種類のネットワークと同様にシンクライアント環境での情報漏えいを保護します。

その他の機能
他の多くの機能も利用できます。
https://www.jtc-i.co.jp/contact/

ジュピターテクノロジー
https://www.jtc-i.co.jp/
042-358-1250

eディスカバリー
（Windows、macOS、Linux）

ファイルタイプ：画像ファイル / Officeファイル / アーカイブファイル / プログラムファイル /メディアファイルなど
定義済みコンテンツ：クレジットカード / 個人識別情報 / 住所 / 社会保障番号 / ID /パスポート / 電話番号 / 納税者番号 / 健康保険番号など
カスタムコンテンツ / ファイル名 / 正規表現 / HIPAA

コンテンツとファイルタイプスキャン
ファイルタイプ、定義済みコンテンツ、カスタムコンテンツ、ファイル名、正規表現、HIPAAで保護されたコンテンツに応じて、組織にとって重要なコンテンツを定義するカスタムeディスカバリーポリシーを作成します。選択したコンテンツに従って機密データをスキャンします。

データの暗号化
機密データが見つかると、AES 256 の強力な暗号化ソリューションで暗号化するオプションを使用でき、不正な従業員のアクセスを防ぎ、情報漏えいの可能性を回避できます。

データの削除
企業ポリシーに違反すると、機密情報を即座に削除することにより、データを保護し、業界規制のコンプライアンス準拠を保証します。

スキャン結果のエクスポート
スキャン結果は、Excel、PDF、CSV ファイルにエクスポートでき、管理用のレポートまたは監査文書として使用できます。スキャン結果には、機密データが検出されたコンピューター、機密データの内容、パス、検出時刻、暗号化 / 削除 / レポートされたか、その他の重要な情報などの詳細が表示されます。.

ファイルタイプブラックリスト
ファイルタイプブラックリストは、ネットワークのエンドポイントに保存される特定のドキュメント（画像ファイル、Office ファイル、アーカイブファイル、プログラムファイルなど）を検出するために使用できます。

定義済みコンテンツブラックリスト
クレジットカード番号、社会保障番号、個人識別情報、その他のデータなどの事前定義されたコンテンツのブラックリスト情報を追加し、保存場所と企業ポリシーに違反しているかを検出します。このブラックリストは、PCI DSS、HIPAA などの規制へのコンプライアンス準拠を保証するのに役立ちます。

カスタムコンテンツブラックリスト
キーワードや式などのカスタムコンテンツに基づいてブラックリストを作成します。さまざまなブラックリスト辞書は、コピー / ペースト、手入力、インポートによって作成できます。

ファイル名ブラックリスト
名前に基づいて特定のファイルを検索し、その場所を追跡します。発見されたファイルの一覧と削除、暗号化、復号化などの実行されたアクションがeディスカバリースキャン結果に表示されます。

正規表現ブラックリスト
高度なカスタムブラックリストを作成して、保護されたネットワークに保存されたデータの特定の再発を見つけることができます。

HIPAA 保護データ
PHI 情報、FDA 承認医薬品、ICD-10 および ICD-9 コードなどのエンドポイントの詳細なスキャンを可能にします。HIPAA に準拠し、機密ヘルスケア情報の所在を検出し、必要に応じて対応措置を適用します。

しきい値
しきい値オプションを使って冗長スキャンを回避できます。特定の違反件数に応じて検査を停止する時間や、最小ファイルサイズに基づいてスキャンするファイルを指定することができます。

MIME タイプホワイトリスト
MIME タイプをスキャンから除外し、ホワイトリストに追加して冗長性を回避し、生産性を向上させます。eディスカバリーポリシーを効率的に管理します。

許可ファイルホワイトリスト
eディスカバリーで定義したスキャンポリシーの例外としてホワイトリストにファイルをアップロードします。ポリシーがファイルタイプ、定義済みコンテンツ、カスタムコンテンツなどに基づいている場合でも、ホワイトリストに登録されたファイルはスキャン対象から除外されます。

その他の機能
他の多くの機能も利用できます。
https://www.jtc-i.co.jp/contact/

デバイス制御
（Windows、macOS、Linux）

USBドライブ / プリンター / Bluetoothデバイス / MP3プレーヤー / 外付けHDD / Teensyボード / デジタルカメラ / Webカメラ / Thunderbolt / PDA / ネットワーク共有 / FireWire / iPhone / iPad / iPods / ZIPドライブ / シリアルポート / PCMCIAストレージデバイス / 生態認証デバイス/その他

グローバル権限の設定
既定では、デバイス権限はネットワークを通じてグローバルに適用されます。しかし、このモジュールは詳細に設定することもできます。

グループ権限の設定
グループに基づいてデバイス権限を詳細に設定できるため、さまざまな部門に異なるアクセス権が適用できます。

コンピューター権限の設定
コンピューターごとにデバイス権限を設定できます。コンピューターが組織内で独自の役割を果たしている場合に役立ちます。

ユーザー権限の設定
その役割と業務に基づいて、ユーザーごとに、会社のポリシーに従って異なるデバイスアクセス権を与えることができます。

デバイス権限の設定
詳細な権限は、ベンダー ID、プロダクト ID、シリアル番号に基づいてデバイスレベルまでドリルダウンできます。

カスタムクラス
同じベンダーの製品の管理を容易にするためデバイスクラスに基づいて、権限を作成することができます。

信頼できるデバイス
暗号化デバイスの場合、暗号化のレベル（ソフトウェア、ハードウェアなど）に基づいて異なるアクセス権を設定できます。

ファイルトレース
さまざまな USB ストレージデバイスへのすべてのファイル転送や試行を記録し、ユーザー操作を明確に表示します。

ファイルシャドウ
後で監査目的で使用できる制御されたデバイスに転送されたファイルのコピーを保存します。

オフライン一時パスワード
一時的に、ネットワークから切断されたコンピューターへのデバイスアクセスを許可します。セキュリティと生産性を確保します。

メールアラートの作成
あらかじめ定義されたメールアラートとカスタムメールアラートは、デバイスの使用に関連する最も重要なイベント情報を提供するように設定できます。

ダッシュボードとグラフ
最も重要なイベントや統計情報をすばやく視覚的に確認するために、グラフと図を利用できます。

レポートと分析
強力なレポートと分析ツールを使用して、デバイス使用に関連するすべてのアクティビティを監視します。ログとレポートをエクスポートすることもできます。

その他の機能
他の多くの機能も利用できます。
https://www.jtc-i.co.jp/contact/

暗号化の強制
（Windows、macOS）

USB の暗号化の強制
暗号化された USB デバイスのみを認証し、リムーバブルストレージデバイスにコピーされるすべてのデータが自動的に保護されるようにします。

強力なセキュリティ技術
政府は、アプリケーションの完全性を保証するために、256 ビット AES 暗号化、パスワード保護、改ざん防止技術を承認しました。

マスターパスワード
マスターパスワードを作成すると、ユーザーパスワードをリセットするなどのさまざまな状況で操作の継続性が提供されます。

その他の機能
暗号化は、クラウドストレージ、ローカルフォルダー、CD/DVD でも利用できます。
https://www.jtc-i.co.jp/contact/

モバイルデバイス管理
（Android、iOS、macOS）

iOS と Android のリモート登録
デバイスは、SMS、メール、URL リンク、QR コードを使ってリモートで登録することができます。ネットワークで最も便利な方法を選択できます。

一括登録
効率的な導入プロセスのために、最大 500 台までのスマートフォンとタブレットを同時に登録することができます。

リモートロック
関連するインシデントが発生した場合にモバイルデバイスを即座にリモートでロックできます。デバイスの紛失や誤配置による情報漏えいを回避します。

追跡と場所の特定
会社のモバイルデバイスを密接に監視し、企業の機密データの場所を常に把握します。

組み込み機能の無効化
カメラなどの内蔵機能の許可を制御し、情報漏えいや機密データの損失を回避します。

紛失したデバイスを見つけるためにサウンドを再生する
デバイスが見つかるまで大音量の着信音を鳴らして、誤って配置されたモバイルデバイスを見つけます（Android のみサポート）。

モバイルアプリケーション管理
組織のセキュリティポリシーに従ってアプリケーションを管理します。無料および有料のアプリを、登録されたモバイルデバイスに即座にプッシュできます。

ネットワーク設定のプッシュ
Bluetooth、着信音モードを含む、メール、Wi-Fi、VPN 設定や無効化などのネットワーク設定をプッシュします。

アラート
拡張事前定義システムアラート、およびカスタムシステムアラートを設定するオプションが利用できます。

レポートと分析
強力なレポートと分析ツールを使用して、デバイス使用に関連するすべてのユーザーアクティビティを監視します。ログとレポートをエクスポートすることもできます。

Samsung KNOX のキオスクモード
モバイルデバイスを特定のアプリにロックまたは格納します。モバイルデバイスのセキュリティをリモートで強制し、専用デバイスに変えることができます。

macOS 管理
DLP 機能を拡張するために、追加の管理オプションを利用して Mac を MDM モジュールに登録することもできます。

パスワードの強制
強力なパスワードポリシーを強制して、モバイルデバイスに保存される企業の機密データを保護します。

リモートワイプ
情報漏えいを回避する唯一の方法がデバイスをワイプするという重大な状況で、簡単にリモートで実行できます。

ジオフェンス
地理的領域に仮想境界を定義し、特定の領域でのみ適用される MDM ポリシーを詳細に制御します。

iOS の制限
業務関連の使用のみが可能であることを確実にします。企業ポリシーに準拠していない場合は、iCloud、Safari、App Store などを無効にします。

Android に vCard をプッシュ
Android モバイルデバイスに連絡先を追加プッシュし、モバイルの使用者が適切な人とすばやく連絡できるようにします。

アプリの監視
従業員がモバイルデバイスにダウンロードしているアプリケーションを把握して、仕事と個人使用の境界線を維持します。

資産管理
デバイス名、タイプ、モデル、容量、OS バージョン、キャリア、IMEI、MAC などのモバイルデバイスの内部情報を取得します。

メールアラートの作成
モバイルデバイス使用に関連する最も重要なイベント情報を提供するため、メールアラートを設定することができます。

ダッシュボードとグラフ
最も重要なイベントや統計情報をすばやく視覚的に確認するために、グラフと図を利用できます。

その他の機能
他の多くの機能も利用できます。
https://www.jtc-i.co.jp/contact/

100%展開の柔軟性

Endpoint Protector は、あらゆる規模のネットワークに柔軟に対応でき、大企業、中小企業、さらには家庭のユーザーによって使用されます。クライアント / サーバーアーキテクチャでは、Web ベースのインターフェイスから簡単に展開し、集中管理できます。ハードウェアアプライアンス、仮想アプライアンス、アマゾン ウェブ サービスのインスタンス、クラウド版に加えて、スタンドアロン版でも基本機能が提供されています。

Endpoint Protector

コンテンツ認識保護、eディスカバリー、デバイス制御、暗号化は、Windows、MacOS、Linux のバージョンおよびディストリビューションが動作するコンピューターで使用できます。モバイルデバイス管理とモバイルアプリケーション管理は、iOS および Android モバイルデバイスでも利用できます。

My Endpoint Protector

コンテンツ認識保護、デバイス制御、暗号化は、Windows と Mac で動作するコンピューターで使用できます。モバイルデバイス管理とモバイルアプリケーション管理は、iOS および Android モバイルデバイスで利用できます。

画像はBlueVault EPP5アプライアンス モデルH2

Hardware Appliance

BlueVault EPP5アプライアンス、
BlueVault io デバイスコントロール

Virtual Appliance

Amazon Instance

Cloud Solution

モジュール

		保護されるエンドポイント		コンテンツ認識保護	eディスカバリー	デバイス制御	暗号化の強制	モバイルデバイス管理
Windows		Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
		Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
		Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
macOS		macOS 10.6	Snow Leopard	●	●	●	●	
		macOS 10.7	Lion	●	●	●	●	
		macOS 10.8	Mountain Lion	●	●	●	●	
		macOS 10.9	Mavericks	●	●	●	●	
		macOS 10.10	Yosemite	●	●	●	●	
		macOS 10.11	El Capitan	●	●	●	●	
		macOS 10.12	Sierra	●	●	●	●	
Linux		Ubuntu		●	●	●	n/a	
		OpenSUSE		●	●	●	n/a	
		CentOS / RedHat		●	●	●	n/a	
		*endpointprotector.com/linux でサポートされているバージョンとディストリビューションの詳細を確認してください						
iOS		iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10						●
Android		Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+)						●