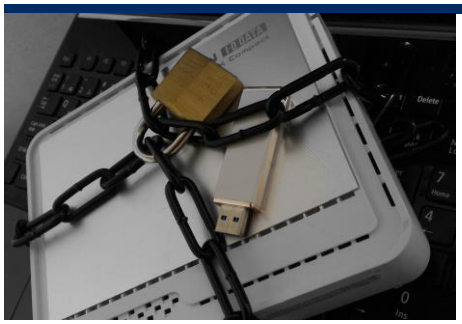
外部記憶メディアの利用制御と暗号化

Check Point Endpoint Security Media Encryption



外部記憶メディアの不正利用、紛失・盗難による情報漏えいを、メディアの利用制御と暗号化で防止します。

正規の利用者にはセキュアでスムーズなデータ受け渡しを許可しながら、私物のUSBメモリなどによる悪意ある情報持ち出しをブロックします。また、外部記憶メディアへ保存したデータを暗号化で強力に守ります。（AES-256bit暗号）

外部記憶メディア経由でやりとりされる企業情報の保護

■外部記憶メディアの暗号化

メディアの紛失・盗難に備え、AES-256bit暗号でデータを強力に保護。Media Encryptionで暗号化したメディアは、Media Encryptionが導入されていないPCでもパスワード入力でデータの復号・暗号ができます。

従来製品/一般的なメディア暗号製品

外部記憶メディア内のファイルを、「ファイル単位」で暗号化

ファイル単位で暗号化

Media Encryption

外部記憶メディア「本体」を暗号化します。データを保存する際、強制的に暗号化領域へ格納します。

暗号化領域

外部記憶メディア「本体」を丸ごと暗号化しているため、「ファイル名」すら見られることがありません。

■外部記憶メディアの利用制御による情報流出の未然防止

メディアに対する「読み取り」「書き込み」操作をきめ細かく制御。部門ごとに異なるポリシー設定・管理を行えます。

▲ポリシー設定例：特定の暗号化メディアのみ利用可能

USBメモリなど、未許可の私物メディアを接続した場合は、アクセスが拒否され、データの読み取りもできません。

PCと暗号メディア間のデータ移動および暗号メディアに対する操作ログを一元管理

■ファイル名でも検索可能。重要ファイルの持ち出しチェックに！

蓄積された操作ログから、ファイル名やデバイス名でフィルタをかけ、必要なログをすぐに確認。Media Encryptionがインストールされたの操作ログ、暗号化メディアの操作ログを取得することが可能です。

▼ログを取得できる情報

No	説明
1	使用可能デバイスにアクセスした場合
2	未許可デバイスへアクセスした場合
3	未許可リムーバブルメディアを接続した場合
4	ウィルススキャンによってリムーバブルメディアの使用が許可された場合
5	未許可リムーバブルメディア内のウィルススキャンに失敗した場合
6	リムーバブルメディアを暗号化した場合
7	暗号化メディアの暗号化を解除した場合

■社外へ持ち出されたメディアの操作も追跡可能

Media Encryptionで暗号化を行った外部記憶メディアは、外部のPC（ME非導入PC）でも利用でき、さらにメディアに対する操作ログが暗号メディア内へ格納されます。ログは、社内ネットワークへの再接続の際、自動的に管理サーバへ送信されます。

▼ログを取得できる情報 ※一部抜粋

No	説明
1	イベントが発生した年/月/日
2	イベントが発生した時間
3	ログのID番号（昇順）
4	イベントの種類
5	ユーザ
6	PC名/IPアドレス
7	フルコンピュータ名
8	リムーバブルメディア上で行われた操作の種類
9	操作を行ったファイル
10	操作を行ったプロセスなど

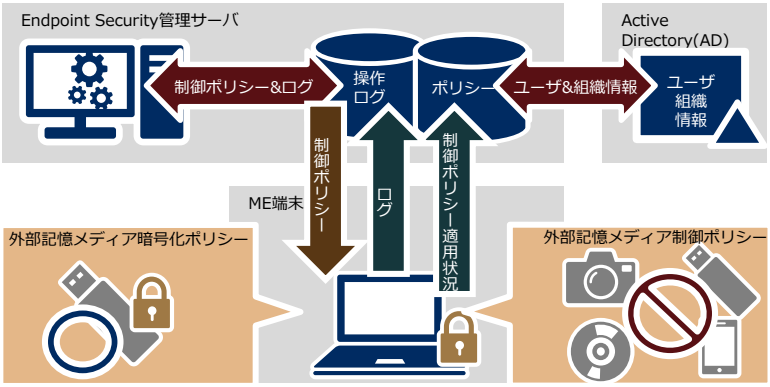
Media Encryption 導入イメージ

■管理サーバが、外部記憶メディア「接続制御ポリシー」の集中管理を実現

管理サーバで設定および変更されたポリシーは任意のタイミングでクライアントPCへ配信することが可能。ポリシーのアップデートに際し、エンドユーザ側での作業は一切不要です。

■Active Directoryとの連携で組織別のポリシー管理を実現

Active Directory(AD)に登録されているユーザや部門構成ごとに異なるポリシーの設定が可能。ADのない環境の場合、ユーザを仮想グループ化することで、複数ポリシーの適用ができます。



Endpoint Security 管理サーバでは、Media Encryption以外のEndpoint Securityシリーズ製品Full Disk Encryptionでも単一コンソールで管理可能です。

■暗号化対象外部記憶メディア

- 特殊な機能が付属していない一般的な外付けハードディスク
- 特殊な機能が付属していない一般的なUSBメモリ
- ブランクのCD/DVD

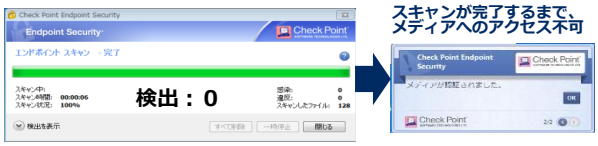
ポリシーで利用制御できるデバイス（抜粋）

フロッピー・ディスク・ドライブ、PDA イメージング・デバイス、デジタル音楽プレーヤー(iPod など)、各種スマートフォン(iPhone、Windows Mobile、BlackBerry) 無線ネットワーク・インタフェース・カード、Bluetoothネットワーク・アクセス・デバイス(モデムなど)、プリンタ、キーボード、スマート・カード・リーダー、USB フラッシュ・ドライブ、CD/DVD ドライブ、外付けハードディスク、USB接続のマスストレージ

クライアントPC内のアンチウィルスソフトとの連携も可能

■ウィルスファイルの社内持込をブロック

外部記憶メディア内のウィルススキャンが完了しなければ、メディアを利用できない設定も可能です。



動作環境

■管理サーバ

対応OS	Windows Server 2008 (32bit/64bit) Windows Server 2008 R2 (64bit) Windows Server 2012 (64bit) Windows Server 2012 R2 (64bit)
CPU	Intel Pentium プロセッサ E2140 もしくは 2GHz以上相当のプロセッサ
メモリ容量	2GB以上 (4GB以上を推奨)
HDD 空き容量	10GB以上(100GB以上を推奨)

■管理コンソール

対応OS	Windows Server 2008 (32bit/64bit) Windows Server 2008 R2 (64bit) Windows Server 2012 (64bit) Windows Server 2012 R2 (64bit) Windows 7 (32bit/64bit) Windows 8.1 (32bit/64bit) Windows 10 (32bit/64bit) ※管理サーバ・クライアントの動作条件に準じます。

■クライアント

対応OS	Windows 7 (32bit/64bit)	Professional Enterprise
	Windows 8.1 (32bit/64bit)	Pro Enterprise
	Windows 10 (32bit/64bit)	
CPU	OSの動作要件に準じる	
メモリ容量	2GB以上	
HDD 空き容量	2GB以上	

※システム要件はOSのサポート終了やメーカーの製品改良などの理由により、予告なく変更される場合があります。
導入検討いただく際には、必ず事前にご確認いただきますようお願い致します。

NEC　パートナーズプラットフォーム事業部　ソフトウェアお問い合せ
〒108-8424　東京都港区芝五丁目３３番８号（第一田町ビル）
TEL:03(3798)7177
受付時間：9:00～12:00、13:00～17:00
月曜日～金曜日（祝日・NEC所定の休日を除く）

日本電気株式会社　〒108-8001　東京都港区芝五丁目7-1（NEC本社ビル）