ひとつのソフトウェアで
あらゆる情報漏洩リスクに対抗する

SecureCore DSE

Data Security Expert

こんな失敗が起きていませんか…？

- 大事な顧客名簿を暗号化し忘れて、部外者からも見えてしまった
- データが委託先で不正利用され、情報漏洩事件となってしまった
- 仕入れ価格の入った書類をうっかり顧客にメールしてしまった
- 派遣社員／外注社員が、私物のUSBメモリに機密データをコピーして持ち帰ってしまった
- 飲み会のあと、製品の設計図が入ったパソコンを電車に忘れてしまった
- 端末がなりすましメールに感染し、知らぬ間に個人情報を外部に送信されてしまった

取り返しのつかない事態になる前に！
SecureCore DSE があれば、その心配から解放されます！

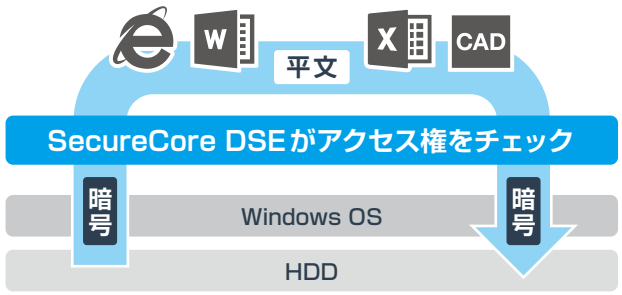
ファイル暗号化 | ユーザ管理 | 端末管理 | 申請承認フロー管理 | アプリホワイトリスト管理 | 外部媒体個体管理
ポート制御 | オフライン制御 | 外部媒体制御 | アプリケーション制御 | 配布制御 | 端末監視 | アクセス証跡記録

SecureCore DSE 3つのPOINT

POINT1 ファイル単位で暗号化+アクセス制御！

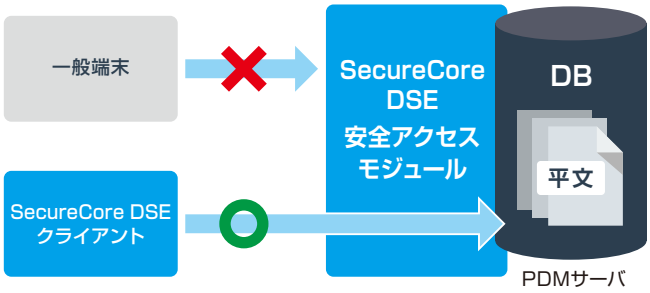
内部不正　標的型攻撃　盗難・紛失・置き忘れ　管理ミス・誤操作

SecureCore DSEの「透過式暗号化技術」



権限を持っているユーザーはSecureCore DSEの存在を意識することなくデータを閲覧・編集できますが、権限を持たないユーザやハッキング、マルウェアに対してはデータを復号できないので文書を開いても文字化け状態となります。

PDM・ERPサーバをセキュリティモジュールで保護



SecureCore DSEクライアントが入っている端末からのアクセスのみ許可
サーバ内のデータは暗号化していないのでサーバ機能は従来通り機能

※PDM=Product Data Management「製品データ管理」「設計技術情報管理」

アプリケーション制御

- アプリケーションをホワイトリスト、ブラックリストに登録することで、不正アプリケーションのアクセスをブロック
- アプリケーションの外部通信を制御することで、機密データが社外ネットワークに送信されることをブロック

申請承認フロー管理

- 暗号化データを平文に変換したい時、申請承認フローでうっかりミスと内部不正を防ぐ

POINT2 外部媒体や通信デバイスを制御！

内部不正　盗難・紛失・置き忘れ　管理ミス・誤操作

企業の情報インフラは社内と社外の境界を超えて拡大しています。SecureCore DSEの外部媒体・ハードウェア制御なら、スマートフォンやUSBメモリなどデバイスの利用や接続先ネットワークなどを細かく制御。機密情報が社外へ漏洩することを阻止できます。

USBポートを制御

USBメモリ　外付HDD　外付CD、DVDなど

禁止　読取専用　書込専用　許可

禁止　許可

ハードウェアを制御

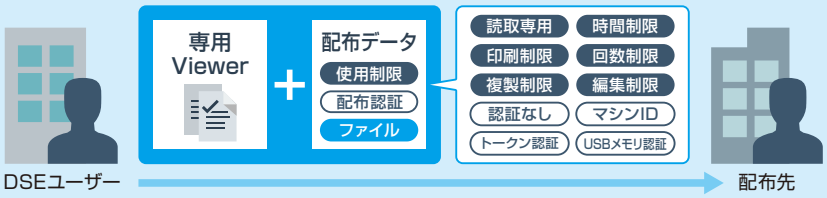
ストレージデバイス
フロッピーディスク、タイプデバイス、PCMCIAカード、プリンター、1394デバイス、ポータブルデバイスなど

ネットワーク装置
無線LAN、Bluetooth、赤外線デバイス、モデム・3Gカード、COMポート／LPTポートなど

POINT3 他企業とやりとりするファイルもコントロール可能！

二次流出　内部不正　管理ミス・誤操作

企業間での情報共有は現代のビジネスには必須事項ですが、その分情報がリスクに晒される場面も増えています。SecureCore DSEは、配布ファイルを専用Viewerと一緒に配布することで配布先マシンをIDで制御可能。相手先に渡した機密情報の不正利用や二次流出による情報の拡散を防ぐことができます。



さまざまなOSに対応

Windows　Mac　Linux　Android　iOS

※Windows以外のOSでは、一部機能制限される場合があります。

使えるセキュリティをお客様へ

【提供元】飛天ジャパン株式会社
〒103-0016 東京都中央区日本橋小網町 9-3 CANAL TOWER 4F／7F
TEL 03-3668-6668(代)／FAX 03-3668-6667
https://ftsafe.co.jp/
sales@ftsafe.co.jp

※記載されている製品仕様、名称などは改良のため予告無く変更する場合があります。