マイナンバー

ISO/IEC 27001：2013

暗号化仮想ドライブIRM

S-WorkPoint

御社の機密情報はしっかり保護されていますか？

機密情報や個人情報の漏えい防止を目的とした仮想化ソリューション

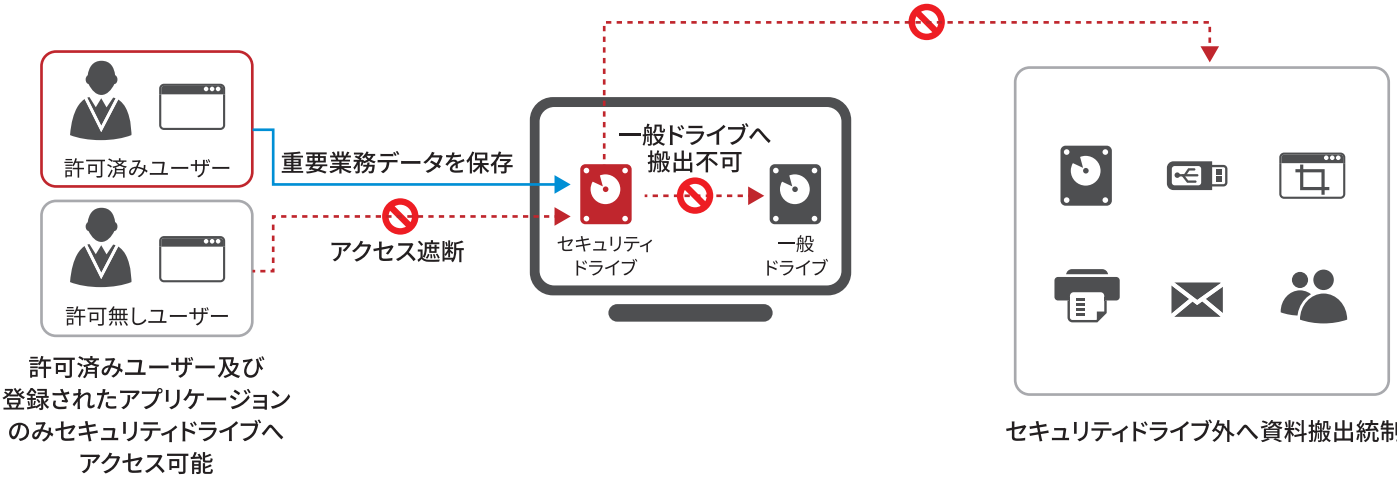
文書ファイル、設計図面、開発ソースなど機密情報や大量の個人情報 の流出を防ぐため、仮想化技術ベースに暗号化されたセキュリティドライブにのみデータを保存して制御する「暗号化仮想ドライブIRM」ソリューションです。

IT技術の発達により企業の存続をも左右する情報流出事件が発生し、被害規模も年々増加傾向にあります。
製造業や鉄鋼業で発生した機密情報の漏えい事件では1,000億円以上に上る損害が発生しており、個人情報では2014年に教育関連企業で3,500万件を超える情報漏洩事件が発生し、その対策として約1年分の利益(260億円以上)を費やす事態となりました。

企業の機密情報はMS OFFICE文書を初め、様々な形式がPCに保存されます。これらのデータは、自社だけでなく関係会社との共同作業を通じて作られる場合もあり、データ流出の危険性が大きいこともあります。これらに対してデータ保存に対する効率的な管理と強度の高いセキュリティ対策が要求されています。

S-WorkPoint

すべての業務データを暗号化された仮想領域内(セキュリティドライブ)に限定して保存します。
セキュリティドライブ間におけデータの共有を通じて円滑な作業をサポートするとともに、セキュリティドライブ外へのデータの持ち出しを禁止することで業務効率を維持しながらセキュリティ性を向上することができます。



SOFTCAMP

マイナンバー

ISO/IEC 27001：2013

暗号化仮想ドライブIRM

S-WorkPoint

01 導入対象

1. IT、自動車、病院、金融機関、造船、建設会社など情報流出の際、甚大な被害を引き起こす可能性のある分野の事業者
2. 外部の関連企業と頻繁にデータの共有を行い、作業終了時にはデータの破棄・回収が必要な事業者
3. オフィス文書、CAD図面、ソースコード等、大容量で重要なデータを扱い、セキュリティ対策を必要とする事業者
4. 個人情報保護法やISOなど情報セキュリティに関連する法律や制度に準拠するために、情報セキュリティを導入しなければならない事業者

02 製品機能

仮想化技術基盤の暗号化されたセキュリティ領域
仮想ドライブを暗号化したセキュリティドライブを生成し許可されたアプリケーションだけがアクセス可能

データ持ち出し遮断
セキュリティドライブにのみ保存でき、セキュリティドライブの外へデータの持ち出しを遮断

オフラインログイン機能
サーバーに接続が不可能な外出先でもオフラインログインでセキュアな業務環境を利用可能

ファイルサーバーとの連携
ファイルサーバとの連携により、ローカルPCのセキュリティドライブ同様、権限によるデータの保存/持ち出しを制御

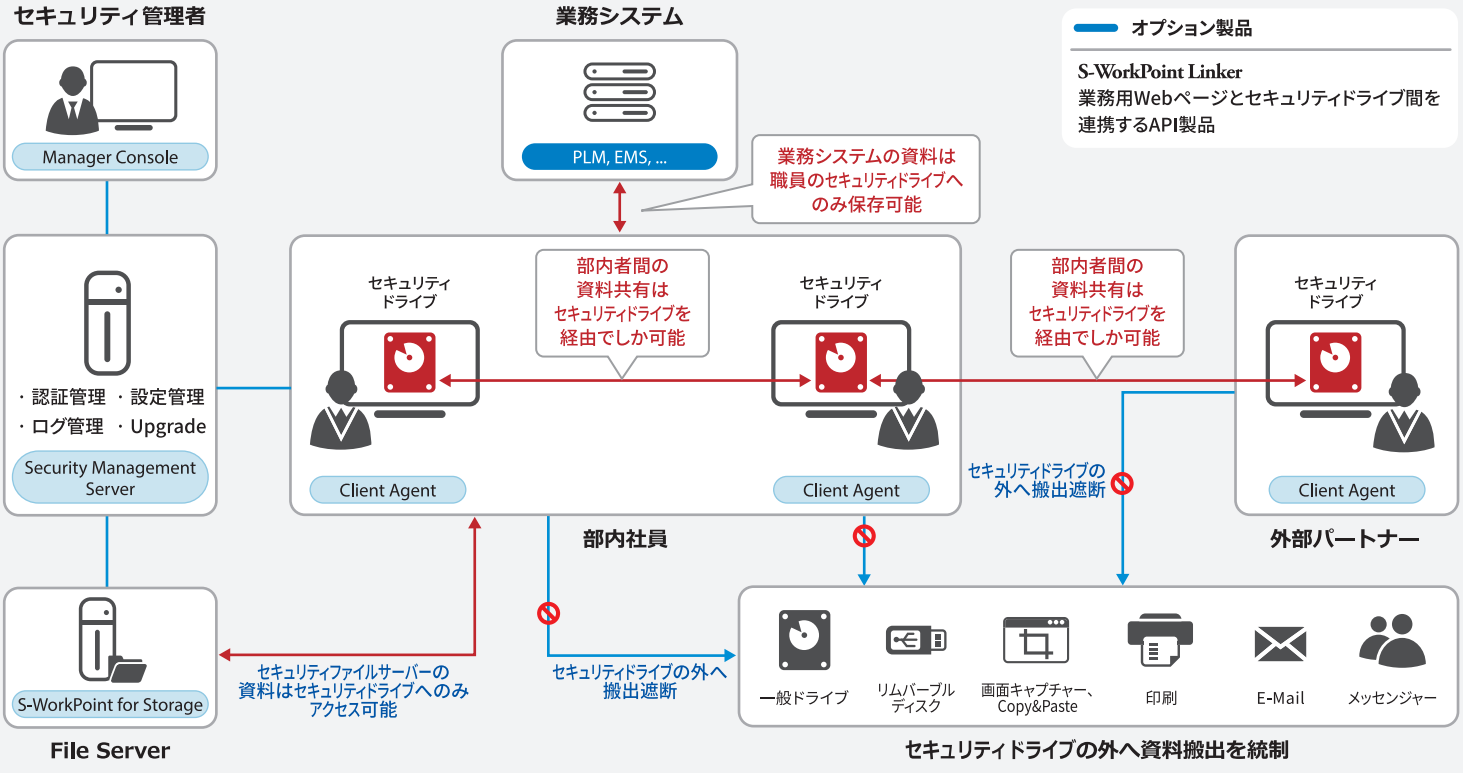
プロセス単位でプログラムを制御
独自に開発されたエンジンを通じて簡単にアプリケーションを登録・制御が可能

キャプチャ、コピー/ペースト制御
プリントスクリーン、画面キャプチャツールを遮断しデータ流出を防止

業務システムとの連携
グループウェア、承認/決裁システム、KMS、ERPなど基幹系業務システムとの連携により従来の業務プロセスを維持

効率的な管理機能
ユーザーと管理者の行動をすべてログで収集
中間管理者と下位管理者の設定で効率的な管理機能を提供

03 システム構成



SOFTCAMP