情報漏えい対策ソリューション『秘文』

①紛失・盗難対策

フルディスク暗号化

OS領域も含めハードディスクを丸ごと暗号化する事で、紛失・盗難時の情報漏えいを防止します。ハードディスクを抜き取られ、別PCで情報を読み取ろうとしても、暗号化されているため中身を参照できません。
また、OS起動前に秘文独自の認証を設け、多段の認証にする事もできます。

【対応製品】 FDE

ハードディスク(ドライブ)・メディア・ファイル暗号化

ハードディスクだけでなく、メディアも暗号化する事で、紛失・盗難時の情報漏えいのリスクをより軽減します。復号できるのは、秘文クライアントがインストールされ、なおかつ鍵が一致するPCのみなので、第三者が中身を参照することは出来ません。
※ProgramFilesやWindows配下等は暗号化対象外

【対応製品】 IC ODE

※ODEはCD/DVD/BDに暗号化持ち出しする場合に必要

②外部デバイス不正利用対策

外部デバイス持ち出し制御

USBメモリ、外付けHDDなどの外部媒体への持ち出しを制御する事で、外部への情報漏えいを防止します。また、全ての持ち出しを禁止するのではなく、許可したUSBメモリであれば持ち出し可能など、柔軟な制御ができます。
更に、iPhone、iPadなど、新たに登場したデバイスへの書き出しを禁止する事もできます。

【対応製品】 Basic IF IF Plus

※IF Plusはデスクトップにアラートを表示させる場合に必要

また、申請・承認ワークフロー製品と連携し、承認されたファイルのみ持ち出しを許可する事も可能です。

【対応製品】 Extension IF Plus

③ファイルサーバ保護対策

ファイルサーバ暗号化

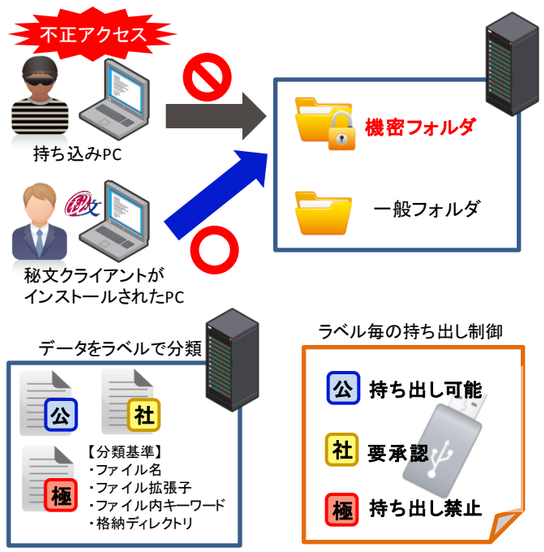
ファイルサーバのデータを暗号化することで、情報漏えいを防止します。ファイルサーバに対してアクセスできるのは、秘文クライアントが導入されているPCのみなので、自宅から勝手に持ち込んだPCでアクセスをしても、データにアクセスができません。

【対応製品】 Basic FSV
IC または IF

ファイルサーバデータの機密分類

ファイルサーバのデータにラベルをつけることで、データの重要度が一目で分かるようになります。更にデータの重要度に応じて外部媒体への持ち出しを制御する事もできます。

【対応製品】 Extension IF Plus



④無線LAN対策

NEW

アクセスポイント制御・VPN利用の強制

無線LAN使用時、社内では許可したアクセスポイントのみ接続可とし、危険なアクセスポイントへの接続を禁止する事が可能です。
社外では、公衆の無線LANスポット等を使用しつつ、必ず社内のVPNサーバ経由させることで、社外にいても社内と同様のセキュリティポリシを適用することが出来ます。

【対応製品】 APC

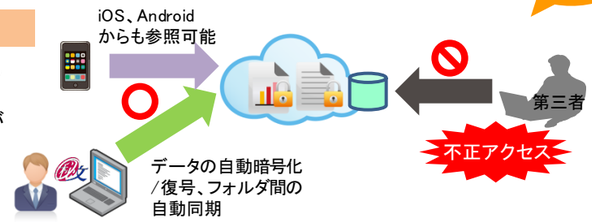
⑤クラウドストレージ対策

NEW

クラウドストレージデータ暗号化

クラウドストレージと同期するデータを自動的に暗号化することで、クラウドストレージ上のデータを守ります。秘文がインストールされたPCでなければデータは復号できないため、クラウドストレージのアカウントが漏えいしても、第三者はデータを参照する事ができません。

【対応製品】 CP



⑥メール誤送信対策

メール添付ファイル自動暗号化

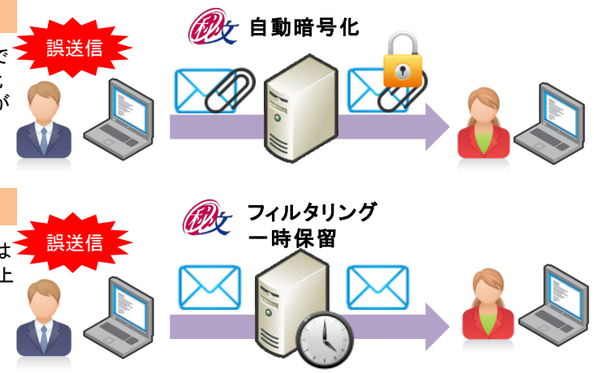
添付ファイルを自動的に暗号化することが可能です。パスワードは固定で指定する他に、ランダムに自動生成することもできます。暗号化を自動化することで、セキュリティレベルをあげつつ、ユーザ負荷の低減にもつながります。

【対応製品】 MG

コンテンツフィルタリング・一時保留

添付ファイルの中身をチェックし、特定のキーワードが含まれている場合は保留する等のコンテンツフィルタリングができます。また、メールをサーバ上で一時的に保留することで誤送信時にキャンセルできます。他にも、添付ファイルの自動的暗号化、上長CCチェック(または自動追加)、ウイルスチェック、スパムチェック機能が備わっています。

【対応製品】 EMG



⑦Webアクセス対策

ファイルアップロード制御・URLフィルタリング

ファイルの中身をチェックし、特定のキーワードが含まれている場合はアップロードを禁止する等のコンテンツフィルタリングができます。他にも、URLフィルタリング、ウイルスチェック、スパイウェアチェック機能が備わっています。

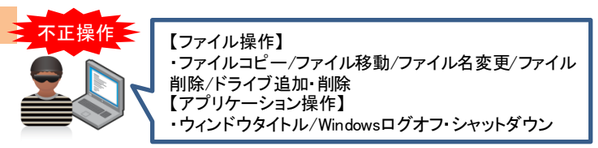
【対応製品】 WBG

⑧ログ対策

操作ログの取得

ユーザのファイル操作ログおよびウィンドウタイトルログを取得できます。ユーザの不正操作抑止や、事後のログ検索等に有効です。

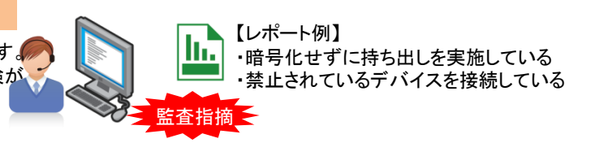
【対応製品】 Basic OM



ログの点検

秘文製品が取得するログを集約し、様々な条件でレポートが作成できます。結果をメールで通知することも可能で、容易に不正操作の有無等の点検ができます。

【対応製品】 Basic



秘文概要

秘文は、様々な場面における情報漏えいリスクから企業を守るセキュリティ・ソフトウェアです。情報を暗号化し、不正な利用を防止する「紛失・盗難対策」を始め、メール添付ファイル、Webアップロードなどによる情報の持ち出しを制御し、「持ち出しのコントロール」を実現します。更に、Windows 8リリースに伴い最近ニーズが多くなっている無線LANやクラウドストレージデータへの対策等、クライアント端末から情報漏えいとなる様々な出口を防ぐ事ができます。

秘文の強み

ラインナップの豊富さ

「秘文」という1つの製品で、情報漏えいの出口となるあらゆる部分の対策をトータルで行うことができます。
そのため、対策や脅威毎に別シリーズの製品を購入する必要がありませんし、同じメーカで開発された製品ですので、共存した際の動作についても安心です。

運用・管理の容易性

“企業の情報漏えいをトータルに対策する”というコンセプトに基づき、管理者にとって容易な運用・管理を実現します。
豊富な機能が1つのパッケージにまとめられていることにより、強固な情報漏えい対策は勿論、製品の展開、運用、アップデートにおける管理者、及び、ユーザに対する負荷の軽減、また、段階的な情報漏えい対策の実現が可能です。

導入実績

「秘文」は、**6900社、720万ライセンス**の導入実績*があります。
富士キメラ総研「2014ネットワークセキュリティビジネス調査総覧<上巻：市場編>」では、ファイル暗号化分野（シェア48.3%）、および持ち出し制御分野（シェア58.9%）において、**市場における秘文の金額シェアはNo.1**となっています。
都市銀行、地方銀行、官公庁・自治体、製造業、流通業と業種業態、規模の大小に関係なく、導入されています。

＊2014年3月末時点

アシスト+秘文の強み

アシストの支援体制

2002年6月に秘文の販売を開始し、販売社数は延べ**1000社以上**を数えます。
アシストには秘文の専任技術者が約20名在籍し、全国拠点でお客様の構築支援を実施し、数クライアントから数万クライアントまで多数の実績があります。

アシストの保守体制

専任スタッフによる**自社のサポートセンター**を設置し、メール、Webだけでなく、電話でも受付・対応しています。サポートに対するお客様の満足度は毎年**90%**以上です。また、FAQや技術情報をご参照いただける技術情報サイトを開設し、定期的に技術情報メール配信もお送りしています。

メーカとの連携体勢

開発元（日立ソリューションズ）のサポート部隊＆設計部隊と綿密な連携を取り、問題の**早期回答/修正モジュールの迅速な提供**を実現します。
機能拡張、提供ドキュメントの整備など「使いやすさ」の向上を目的として活発に交流。月に2回定例ミーティングも開催し、良好な関係を築いています。

お客様導入事例

JFEテクノリサーチ株式会社

技術情報を商品として扱う会社故に高いセキュリティ意識を企業風土とする同社では、商品である技術データを受け渡す媒体である外部メディアの暗号化対策を決断。複数製品を検討した結果、「秘文」のコストパフォーマンスの高さを評価し、全社セキュリティ標準の1つに選定した。

郵船情報開発株式会社

日本郵船（NYK）グループの情報システム構築を担う同社では、グループにおけるセキュリティ・レベルの向上とコンプライアンス徹底のため、IT資産配布管理ソフトウェアとして「JP1/NETMシリーズ」データ保護ソフトウェアとして暗号化機能に加えて、外部へのデータ持ちだし制御やログの取得を備えた「秘文」を選定した。

税理士法人AKJパートナーズ

企業の成長・発展をサポートする会計・税務の専門家集団である同社では、金融機関との取引開始を機に、ISO 27001取得が必須となり、機能だけでなく、実績による安心感、コストパフォーマンスなど、様々な観点で比較検討した結果、「秘文」を選定。
ISO 27001取得プロジェクトを予定通り完遂し、金融機関のみならず、既存顧客からも「よりいっそう安心できる」との評価をいただている。

秘文製品ラインナップ

アイコンの見方：□・・・サーバ製品 ○・・・クライアント製品

	製品名	機能概要	価格
FDE	秘文AE Full Disk Encryption（FDE）	ハードディスクフル暗号化	16,000円（クライアント1台あたり）
IC	秘文AE Information Cypher（IC）	ハードディスク（ドライブ）暗号化、リムーバブルメディア暗号化、ファイル暗号化	10,000円（クライアント1台あたり）
ODE	秘文AE Optical Disc Encryption（ODE）	CD/DVD暗号化 CD/DVD書き込みログ取得	4,000円（クライアント1台あたり）
Basic	秘文Server Basic	ユーザ管理、持ち出し制御ポリシー管理、 USBメモリ情報管理、ログ収集	1,000,000円（1システムあたり）
Extension	秘文Server Extension	申請・承認ワークフロー、機密ファイルのラベル付け	2,800,000円（1システムあたり）
IF	秘文AE Information Fortress（IF）	外部デバイス持ち出し制御、読み込み制御、許可USBメモリ管理 デバイス使用可否制御、ファイル持ち出しログ取得	10,000円（クライアント1台あたり）
IF Plus	秘文AE IF Plus	承認ファイル持ち出し制御、デスクトップアラート表示、機密レベル表示	6,000円（クライアント1台あたり）

	製品名	機能概要	価格
FSV	秘文AE File Server（FSV）	ファイルサーバ暗号化	100,000円（ファイルサーバ1台あたり）
APC	秘文AE Access Point Control（APC）	Wi-Fi制御、VPN接続強制	3,000円（デバイス1台あたり）
CP	秘文Cloud Data Protection（CP）	クラウドストレージデータの暗号化 （OneDrive、Dropbox、box、Googleドライブ）	300円（月額/1ユーザあたり）
MG	秘文AE Mail Guard（MG）	メール添付ファイル自動暗号化 メール送信制御	500,000円（100アカウントあたり）
EMG	秘文AE Email Gateway（EMG）	メールフィルタリング（コンテンツフィルタリング） 添付ファイル暗号化、一時保留、上長CC付加	550,000円（100アカウント/初年度） 275,000円（2年目以降）
WBG	秘文AE Web Gateway（WBG）	URLフィルタリング、アップロード制御、ウイルス対策、スパイウェア対策	850,000円（100アカウント/初年度） 425,000円（2年目以降）
OM	秘文ME Operation Monitor（OM）	ファイル操作ログ取得	5,000円（クライアント1台あたり）

※表示価格は税抜きです　※保守費用はライセンス価格の15%です（秘文CP、秘文EMG、秘文WBGを除く）。

セキュリティ最新トピック　～Wi-Fiに潜むカメレオン！？の正体～

アクセスポイントに潜み、風邪のように感染を広げるウイルスがイギリスの研究者により開発されました。その名もChameleon（カメレオン）。
Chameleonはアクセスポイント自身の機能には影響を与えずに、そのWi-Fiに接続するすべてのユーザの情報を盗むことができるだけでなく、セキュリティレベルが低い他の感染可能なWi-Fiアクセスポイントを探し、ウイルス検出機能をすり抜けて感染を広げていくそうです。大都市では、1つのアクセスポイントにわずか数人から数千人もが接続するため、攻撃者は膨大な重要データへのアクセスを取得できてしまう恐れがあります。カフェや駅、空港などの無料のWi-Fiは便利な反面、いつどこで情報が窃取されてもおかしくありません。Wi-Fi利用時は適切なセキュリティ対策が必要不可欠です。

問い合わせ先

アシスト
東京都千代田区九段北4-2-1 市ヶ谷東急ビル
システムソフトウェア事業部
TEL：03-5276-3475

アシスト　秘文　検索