某市役所

導入製品
InterSafe FileProtection

完全自動暗号化でヒューマンエラーを補完。運用のことがよく考えられていると思いました。

総務部情報システム課 導入担当者

InterSafe ILP、InterSafe FileProtectionについて

InterSafe ILPは、機密データの漏洩防止や、データの安全な持ち出し、データ流出後に備えた4つの製品で構成されるオールインワンの情報漏洩対策群です。デバイス制御ソフトとデータ持出し申請・承認ソフト、自動暗号化ソフトやセキュリティUSBメモリ作成ソフトを、目的や業務にあわせて導入でき、組織内外のデータを多層的に防御します。
ファイル自動暗号化ソフトInterSafe FileProtectionは、すべてのファイルを保存時に自動で暗号化し、データの持ち出し時や万一のデータ流出時に備える有効な対策です。

「データの流出後の対策としてファイル暗号化は最適です。」

首都圏の某市役所では、大規模情報漏洩事件の報道をきっかけに、データ流出後の情報管理体制強化のためInterSafe ILP（InterSafe FileProtection）を導入しました。体制強化策の検討開始から運用開始まで、およそ1か月半とスピーディに展開されています。
導入担当者にお話しを伺いました。
※某市役所では、InterSafe FileProtectionをご利用になっています。
※本事例はお客様の許可を得たうえで、導入元が特定できないよう弊社で作成したイメージ事例です。

年金情報の大量漏洩事件をきっかけに、「漏洩後の対策強化」を急ぎ検討

－ 今回暗号化ソフトを検討するきっかけとなったのはどのようなことですか？

昨年機密情報管理体制強化の一環として、監視ツールを導入しました。その結果、アンチウイルスソフトでは検知されないウイルスの侵入が定期的に発見されるようになりました。何らかの対策が必要ということを課題として認識し、情報収集をしていたところに、日本年金機構での個人情報漏洩事件が起きました。上層部から情報管理体制を強化するよう指示があり、急ピッチで対策を検討することとなりました。

－ 具体的にはどのようなセキュリティ対策を実施していたのですか。

ファイヤウォールやアンチウイルスといった基本的なセキュリティ対策に加え、資産管理やWebフィルタリング、メールフィルタリング、監視ツールを順次追加導入して運用してきました。しかし、情報が流出した後の対策はできていませんでした。

ヒューマンエラーは無くならないだからシステムでの補完が不可欠

－ 年金情報の漏洩は、メールからのウイルス感染が原因と報道されていました。

怪しいメールは開かない、添付ファイルに気を付ける、ということは、セキュリティの基本と言われており、事実その通りです。しかし、実際の攻撃は非常に巧妙です。一見して「怪しい」と思わせないように工夫されていますから、個人のITスキルやリテラシに依存するルール運用では、到底防ぐことはできません。このようなヒューマンエラーは起こる、という考えのもとでシステムを強化しようと考えました。

－ 具体的にはどのような対策を検討したのですか？

機密情報が含まれるファイルがネットワーク外に出ていく、ということを前提に検討を開始しました。ウイルスによるデータの流出だけでなく、部署によっては機密データを業務委託先などとやり取りする場合もあるからです。

システム関連を委託している事業者に相談した結果、いくつかの提案がありました。まずは、ハードディスクの暗号化製品です。しかし、ハードディスク外にデータを出した時点で暗号解除され平文化されるため、流出後の対策にはなりません。次に、サンドボックス型のふるまい検知製品も提案されましたが、根本対策にはならず、さらに価格が大変高価なことから今回は見送りました。組織内からは、導入済のメールフィルターで十分ではないか、という意見もありましたが、メール送受信時には有効なものの、それ以外の保存データは保護されません。結局、データ流出後の対策としてもっとも適していると判断したのがファイル単位の暗号化でした。

違和感無く、完全自動暗号化 お試しクラウドで導入テスト

ー ファイル暗号化製品の比較検討において、重視したことはどのようなことですか？

まず、既存のファイル運用ルールが変わらないこと、操作時に違和感が無いことが重要です。職員の中には、ITスキルが高いとはいえない者も多くいます。例えば、暗号化によってファイルのアイコンや拡張子が変わってしまう製品では、慣れるまでには相当の混乱が想像できます。

また、暗号化するときに、右クリックや専用フォルダへの移動など、特別な操作が必要な場合、暗号化を忘れたままで保存されるファイルが多くなるでしょう。ヒューマンエラーを補完するためのシステムが、ヒューマンエラーの原因になっては本末転倒です。これらの条件をすべて満たすのが、InterSafe FileProtectionでした。

ー テストを実施したうえで、導入を決定されましたね。

検討開始から製品選定までスピーディに進めてきましたが、テストには相当時間がかかると踏んでいました。しかし、InterSafe FileProtectionでは、ALSIが提供する「ILPお試しクラウド」上でテストができます。そのため、テスト環境の準備はALSIに任せることができ、ほんの数日でテストが始められたのでとてもありがたかったです。

オフライン利用、 ファイル権限自動付与を高く評価 情シスの欲しいものがそろっている

ー 導入の決め手になったのはどのような点でしたか？

製品選定時の重視項目に加えて、オフライン時にも暗号化が有効で、かつファイルが利用できる、ということが大きなポイント加算になりました。万一サーバがダウンした時にも、業務が進められるというのは市役所にとって特に大きなベネフィットです。
また、ファイルの利用権限の自動付与により、機密ファイルへのアクセス管理ができること高評価でした。

ー 実際の庁舎内導入は、どのように進められたのですか？

急ぎ対策を進める必要があった為、優先度の高い機密情報を扱う部門から部分的導入を開始しました。実際の導入は、システム委託先に依頼しました。利用端末へのクライアントプログラムの展開は、ログオンスクリプトやプログラム配布のツールを利用することができ、作業負荷はあまりかかりませんでした。導入から運用まで、情報システム部門のかゆいところに手が届く、きめ細かな設定が準備されていて、よく考えられているなと改めて感心しています。

ー 実際にご利用になって、導入部門の方からはどのような反響がありましたか？

事前に導入説明会を実施していたため、操作の面で特別な質問を受けるようなことはありませんでした。ファイルを暗号化するための特別な操作が必要ないこと、また暗号化したファイルの拡張子やアイコンの見た目が変わらないことから、職員にも抵抗なく受け入れてもらっています。業務に混乱をきたすようなことは今のところ起きていません。ただ、外部とのデータやり取りの際に、暗号化ファイルをメールで送ってしまい、先方からデータが見られない、という連絡を受けることもあるようですが運用に慣れるうちに徐々に減っていくことと思います。

ー 今後の展開予定について教えてください。

部分導入での運用を始めたばかりですので、今後は順番に組織全体への展開を進めています。また、ネットワーク外の出先機関で業務を行っている部門があります。この部門に対して、スタンドアロン管理オプションを使ってInterSafe FileProtectionを導入したいと考えています。またSDKにより文書管理ソフトとの連携についてもすでに検討を開始しました。

今回は、データ流出後の対策を優先して導入しましたが、今後は情報を外に出さないための対策も強化が必要です。ALSIでInterSafe ILPとして提供しているデバイス制御やデータ書出しの原本管理なども追加して、多層的に根本的な情報漏洩対策体制を構築していきたいと考えています。

「ファイル操作に違和感がないことが導入の決め手でした」

スタンドアロン管理オプションとは

スタンドアロン管理オプションとは
InterSafe FileProtectionでは、取引先や拠点の事務所など、ネットワークが分断された環境でも、ポリシー適用やログ収集の一元管理が出来ます。
一般的な情報漏洩対策製品では、ネットワークから独立した環境では情報共有ができないため、個別にセキュリティ対策を施さねばなりません。
※スタンドアロン管理オプションは有償オプションです。

InterSafe FileProtection ご利用イメージ

開発・販売元

アルプス システム インテグレーション株式会社
〒145-0067　東京都大田区雪谷大塚町1-7
TEL 03-5499-8045　FAX 03-5499-0357
●詳しい情報は　https://www.alsi.co.jp/

■お問い合わせ先