機密情報の流出を自動で「探して」「守る」情報漏えい対策ソリューション

当社は、個人情報などの重要・機密情報ファイルを見つけて自動で暗号化するソリューション「Secure Protection（セキュアプロテクション）」を販売しています。釧路市では、自治体情報システムのセキュリティ対策強化に本製品を導入し、職員の負担がほとんどない運用で情報流出・紛失への対策を実現しています。

「情報は流出すること」を前提としたソリューション

多くの企業では、ウイルス対策はもとより、重要・機密ファイルの持ち出し制限、USBメモリなどの持ち込み・使用の禁止、従業員のセキュリティ教育、機密保持誓約書など、さまざまな対策を講じてきました。にもかかわらず、情報流出事件・事故は毎日のように起きており、従来の「流出・漏えいを未然に防ぐ」ツールの導入だけでは、情報流出は防ぎ切れないのが実情です。そうであれば、「情報は流出する」ことを前提とした対策を講じるほかありません。

当社が販売している「Secure Protection」は、まさに「情報が流出しても漏えいはしない」ことをコンセプトにした製品です。守るべき情報を探し、暗号化し、管理・追跡し、万一の流出の際にはファイルをあとから消去する、という一連の動作を自動的に実行することで、あらゆる経路での情報流出や紛失を抑止するものです**（図-1）**。

(1) 自動で「検索」「暗号化」

あらかじめ指定したルールで社員のパソコンを定期的に検索、独自アルゴリズムで個人情報を含む重要・機密ファイルを高精度で検出します。マイナンバー、住所、氏名、電話番号、メールアドレス、口座番号、クレジットカード番号、免許証番号、保険証番号などを含むファイルの検索を行うほか、重要、極秘、文書番号などあらかじめ設定したキーワードによる検索も可能です。

また、検索により検出されたファイルは、自動的に暗号化されます。

(2)「管理・追跡」と「あとから消す」

暗号化した重要・機密情報ファイルは、リアルタイムでファイルへのアクセス・操作ログを確認でき、いつ誰がアクセスしたかが追跡できます。万一、ファイルが流出した場合でも、「あとから消す」仕組みにより、情報漏えいを防ぎます。検索・暗号化したファイルの閲覧制限は管理サーバー上で一元管理され、閲覧制限の変更が可能です。

釧路市が2,000ライセンスを導入

釧路市では、2016年2月にこのSecure Protectionを全職員の端末に導入し、情報セキュリティ対策の強化に成功しています。

導入当初は、マイナンバー制度の運用開始を控え、全国の自治体情報システムのセキュリティ強化が求められました。同市では早くから、USBメモリなど外付けデバイスの制限や使用状況のログを残す仕組みの導入、さらには業務システムのインターネットからの分離、メールの無害化などに取り組んできました。個人情報を含むファイルについても、各職員のPCには個人情報は残さずサーバー上に保管するということも徹底してきましたが、消去忘れなどヒューマンエラーによる情報流出のリスクは残されていました。

同市では、万一ファイルが外部に流出したとしても、そのファイルが開けなければ事故には結びつかないと

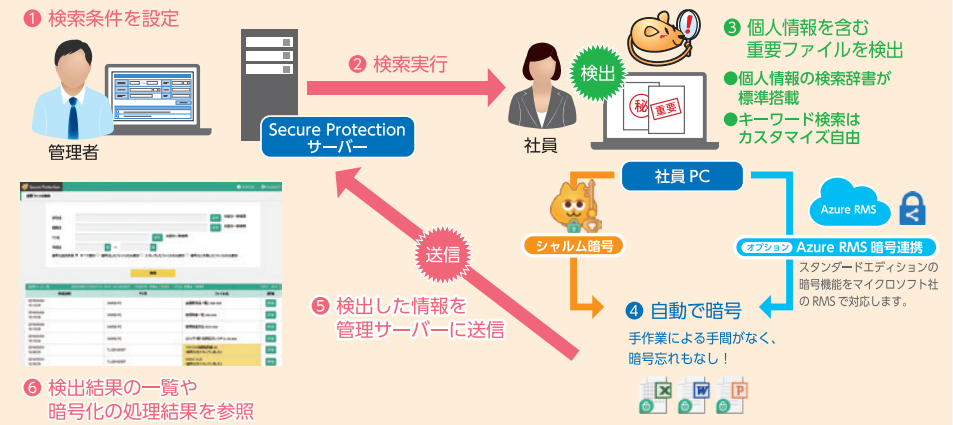

図-1　Secure Protectionの概要

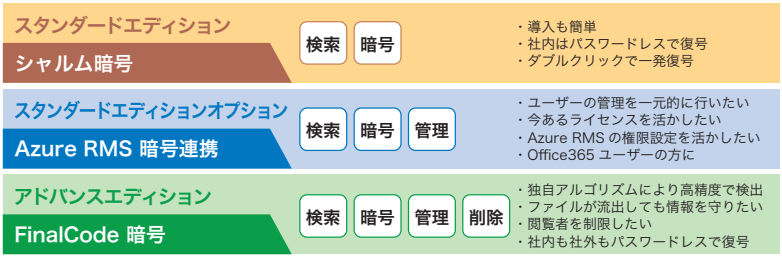

図-2　選べる暗号化方式

いう対策を講じるほうが合理的・現実的だと考え、職員の負担が極力少なくファイルを暗号化するツールの検討を始めました。

選定のポイントとなったのは、以下の3点です。

1) 職員が特別の操作をしなくても暗号化できること

2) 暗号化するファイルの選定条件を自由に設定できること

3) 適正な費用で導入できること

以上のポイントから、最終的にSecure Protectionを選定し、 2,000ライセンスを導入しました。

一般競争入札からSecure Protectionの運用開始まではわずか3カ月。百数十の部署から各部門のセキュリティの担当者が参加、わずか2時間の説明で導入準備は完了したのです。

Secure Protectionは自動的に暗号化できる点が最大の特長で、ユーザーが意識することなく暗号化されるため、従来と使い勝手はほとんど変わらず、職員の負担が少ないツールを検討したいという同市のニーズに応えることができました。

運用開始直後は、すべてのファイルに対して検索を行い、対象ファイルを暗号化するため、釧路市ではPCに負荷がかかるのではないかという不安もあったようです。そこで、初回のみ、職員が業務を行わない夜間にファイル検索を行うことで対応、2回目以降は差分検査を行うため、業務に支障が出るような負荷はありませんでした。現在は、昼休みの時間帯を利用してファイル検査・暗号化を実行しています。これにより、守られているという安心感を持っていただきました。

Secure Protectionは、名字、住所、生年月日、マイナンバー、口座番号などの個人情報の検索辞書を搭載しており、ファイルの検出レベルをお客様側のニーズに合わせた形で調整可能です。当社は、ファイルを暗号化する基準をさらに厳しくしたいという同市の要望にも対応しています。

「Microsoft Azure RMS」を追加サポート

2017年4月、Secure Protectionに新たな暗号化方式を追加しました。従来のシャルム暗号(スタンダードエディション)とFinalCode暗号(アドバンスエディション)に加え、Microsoft Azureのクラウド用オプションとして「Azure RMS暗号連携（スタンダードエディションオプション)」を提供しています(**図-2**)。

Office 365 環境でも情報漏えい対策を強化したいといったニーズに対応した機能で、新たに暗号化環境を用意することなく、Secure Protectionによる情報漏えい対策を導入できます。Secure Protection で検索した電子ファイルは Microsoft Azure RMS で暗号化され、情報漏えい対策の強化を図ることができます。本機能は、スタンダードエディションにわずかなオプション費用で利用できます。

このほか、「デバイス制御オプション」も新たに用意、基本機能に加えて、ファイルの不要な持ち出し、標的型攻撃などによる流出などのインシデントに対する対策を強化することができます(**図-3**)。各種デバイスへの機密情報ファイルの移動やコピーを禁止する「デバイス制御機能」や、ファイル操作ログ、メール送信ログ、印刷ログを取得して管理する「ログ管理機能」を搭載しています。

Secure Protectionは、金融から建築までさまざまな業種のお客様に導入いただいています。当社のWebサイトにも、さまざまな業種や規模の企業から問い合わせをいただいています。個人情報は守りたいが、人間が介在する以上、守り切れない、万一流出しても漏えいはしない、しかも情報システム部門や利用者が従来の仕組みを変えないで実現できる、という点で多くの企業が関心を示しています。

文部科学省では2017年秋に「教育情報セキュリティポリシーに関するガイドライン」を策定し、今後は、学校や教育機関などでもセキュリティ対策強化が求められてくるものと考えられます。こうした文教市場も含め、少しでも多くのお客様に製品のメリットを訴求していきます。

(デジタルエンジニアリング第３事業部　山本 崇史)

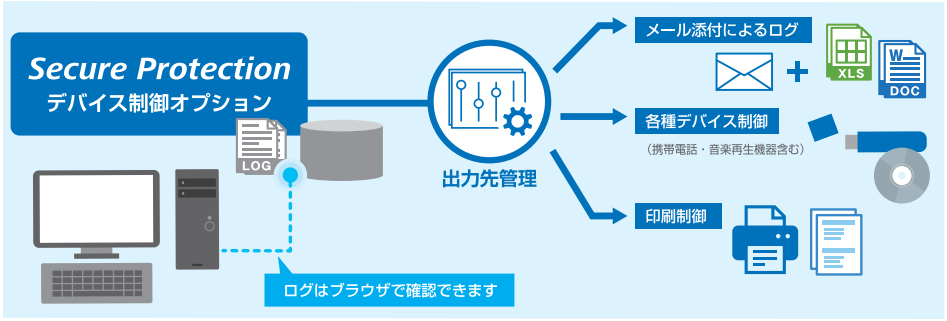

図-3　デバイス制御オプション