漏洩を前提にした先進的な情報漏洩対策ソリューション「Secure Protection」

情報漏洩のニュースは、民間企業、公的機関を問わず、後を絶ちません。現に、情報漏洩の事件・事故はセキュリティ事件・事故の8割を超えるほど多数発生し続けているのが現状です。この背景を踏まえ、当社では、「情報漏洩は防ぎきれない」ことを前提にした先進的な情報漏洩対策ソリューションを2016年1月より販売開始、民間企業や官公庁・自治体などで活用いただいています。

情報漏洩は防ぎきれない

情報セキュリティ対策を進めている情報処理推進機構（IPA）の情報セキュリティ白書によると、2013年度に発生したセキュリティ事件・事故のうち、情報流出や紛失などのいわゆる情報漏洩は、81.3%を占めています。多くの企業では、ウイルスやマルウェアへの対策、従業員への教育、USB利用禁止、ネットワークセキュリティ強化などの対策を行っていますが、過去からの推移を見てもいまだ減少していません。これは、情報漏洩の経路が、(1) ウイルスやマルウェアなどの外部からの攻撃、(2) メール誤送信等の人為的なミス、(3) 社員による不正持ち出し、(4) 委託先などからの間接的な漏洩と、多岐に渡ることに起因しています**(図-1)**。

また、メールに添付されているファイルを開いた場合やインターネットからファイルをダウンロードした場合は、パソコンの一時保存領域に保存されますが、これらのファイルはパソコン操作者（社員）が把握することができないため、パソコン操作者（社員）が認知していない重要・機密ファイルがパソコンに存在するケースも発生し得ます。

この背景を踏まえ、当社では、「情報漏洩は防ぎきれない」ことを前提にした対策が必要と考え、万が一、情報漏洩が発生しても重要・機密な情報は漏洩させない新たなソリューションの開発を行いました。それが、先進的なソリューション「Secure Protection」です**(図-2)**。

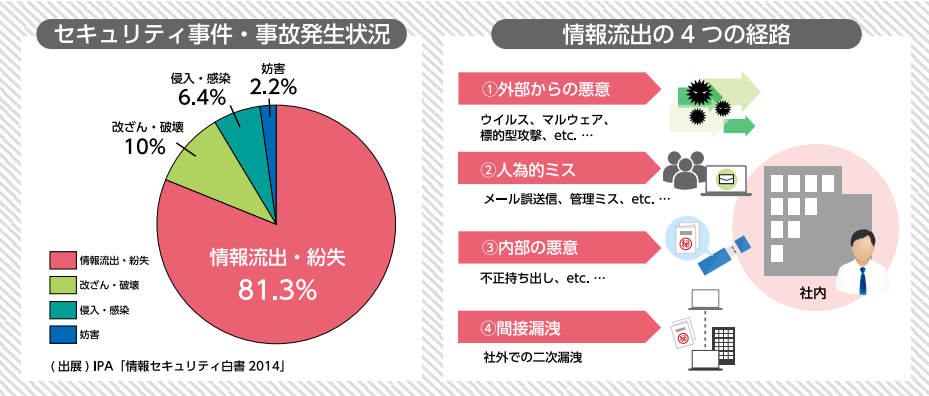

図-1　セキュリティ事件・事故発生状況と情報流出の４つの経路

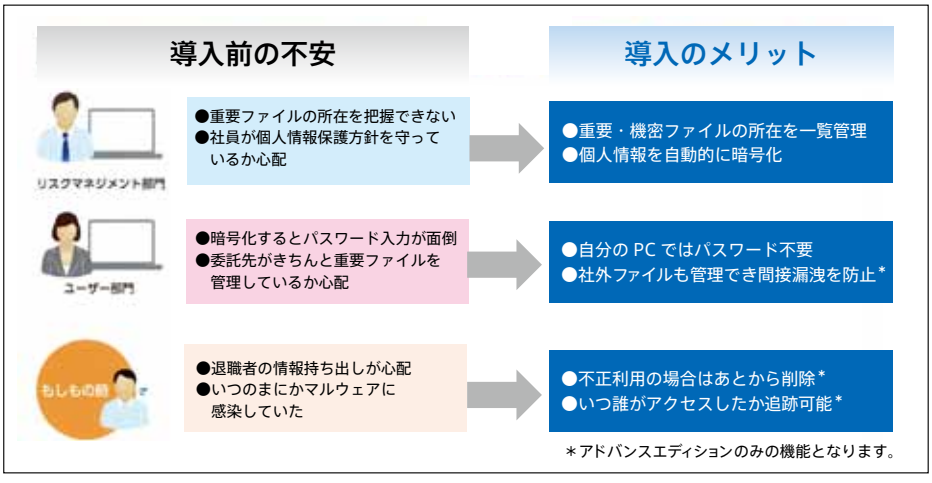

図-2　Secure Protectionの導入メリット

重要・機密ファイルを自動で探して暗号化、追跡する

「Secure Protection」は、社員のパソコンに保存されているファイルを定期的に探索する「自動で探す」、探索した結果、発見した重要・機密情報ファイルを暗号化する「自動で守る」、暗号化したファイルに対するアクセス履歴の管理を行う「管理して追跡する」、万が一、情報ファイルが漏洩した場合には「あとから消す」の４つの機能を提供しています。

	重要なファイルを「自動で探す」	重要なファイルを「自動で守る」	重要なファイルを「管理して追跡する」	重要なファイルを「あとから消す」	ポイント
スタンダードエディション	○	○	×	×	●自己復号形式の暗号 ●自分のPCではパスワードレス
アドバンスエディション	○	○	○	○	●パスワードレスで暗号・復号 ●閲覧制限（回数・期間）指定可能 ●リモートで閲覧条件を変更可能 ●あとからファイル削除が可能

図-3　Secure Protectionエディション

また、リスクマネジメント部門や情報システム部門などの管理者に対して、社員のパソコンに保存されている重要・機密ファイルを管理する管理者向け機能を提供しています。

「Secure Protection」は、導入形態に合わせてスタンダードとアドバンスの2つのエディションを提供しています。スタンダードエディションでは「自動で探す」と「自動で守る」の２つの機能と管理者向け機能を提供、アドバンスエディションでは「自動で探す」「自動で守る」「管理して追跡する」「あとから消す」の４つの機能と管理者向け機能を提供しています**(図-3)**。

（1）重要・機密ファイルを「自動で探す」 スタンダード アドバンス

パソコン起動時や定時刻に「Secure Protection」が起動し、パソコンの全てのディスクを探索して、あらかじめ指定した条件に合致する重要・機密情報ファイルを探索します。

ファイル探索の条件は、「マイナンバー」「氏名」「住所」「電話番号」「メールアドレス」「口座番号」のほか、「取扱注意」や「社外秘」といった固定文字を指定することが可能です。

（2）重要・機密ファイルを「自動で守る」 スタンダード アドバンス

スタンダードエディションでは一般的な暗号アルゴリズムであるパスワード付AES暗号、アドバンスエディションでは閲覧制限（閲覧者や閲覧期間、回数、印刷可否など）を付与したDRM暗号によりファイルを暗号化します。

一般的には、暗号化されたファイルを開く際には指定されたパスワードを入力する必要がありますが、「Secure Protection」では自己認証方式の採用により、正当なファイル所有者であればパスワードレスで暗号化されたファイルを開くことができます。このため、ファイル暗号化による業務の手間が増えることはありません。

（3）守った重要・機密ファイルを「管理して追跡する」 アドバンス

暗号化した重要・機密ファイルに対するアクセスログが自動で取得され、暗号化した重要・機密ファイルのアクセス履歴と不正アクセス有無を管理する機能を提供するほか、暗号化した重要・機密ファイルの閲覧制限（閲覧者や閲覧期間、回数、印刷可否など）を設定・変更する機能を提供します。

（4）守った重要・機密ファイルを「あとから消す」 アドバンス

暗号化した重要・機密ファイルに不正なアクセスが発生した場合や、万が一、重要・機密ファイルが漏洩した場合には漏洩したファイルを物理的にあとから消す仕組みを提供します。

（5）管理者向け機能

スタンダード アドバンス

探索・暗号化の結果をサーバに集約管理します。リスクマネジメント部門や情報システム部門などの管理者に対し、社員の「どのパソコン」の「どこ（ファイルパス）」に「どんな（探索条件）」重要・機密ファイルが「いくつ（何件）」保存されているのかを一元的に管理する機能を提供します。

統合的な情報漏洩対策ソリューションへ

マイナンバー制度では情報漏洩に対する罰則も規定されるなど、政府主導で情報セキュリティ対策が推し進められており、情報漏洩の対策は重要度が一段と高まっています。

このような背景の中、「Secure Protection」は官公庁や自治体、業種を問わず多くの企業から問合せをいただいています。

今年春に、重要・機密ファイルが保存されたパソコンでは、印刷やファイルのコピー、外部デバイスの使用を制限するオプションサービスの提供を開始しました。また、資産管理ツールと連動した統合的管理が行える機能バージョンアップのほか、情報セキュリティ対策のためのITO・BPOサービスを順次、提供していく計画です。

「マルウェア感染で保険者情報流出」、「社員が個人情報を売却」などの情報漏洩に関するニュースは後を絶ちません。情報漏洩に関するセキュリティ事件・事故が起こらない安全な社会の実現に向け、当社では今後も「Secure Protection」をはじめ、多くのセキュリティ対策商品やサービス、ICT全般にわたるサービス、ソリューションを提供していきます。

（SIソリューション事業部　野瀬 克紀）

導入を決定したある自治体様のコメント

公務で取り扱う個人情報、及び特定個人情報を含む情報資産の適切なセキュリティ対策強化を進めています。従来は、個人情報ファイルに暗号やパスワードを設定して作業終了後に消去する運用を行っていましたが、暗号忘れや消去忘れなどのリスクから、職員のPCに保存している重要・機密情報ファイルを自動で探し暗号化する「Secure Protection」を導入しました。