セキュリティ

ファイル暗号化サービス（ActSecure クラウドセキュアファイルサービス）

Microsoft 365やEMSに含まれる「Azure Information Protection」を活用し、
さまざまな場所にあるさまざまなファイルを自動暗号化
ファイルが流出しても読まれない安心な経営基盤を実現

1 ファイルが流出する「脅威」は「標的型攻撃による情報流出」「内部不正による情報流出」

IPA（独立行政法人 情報処理推進機構）が発行した「情報セキュリティ10大脅威 2019」では、前年に引き続き、1位と5位に情報漏えいに関する脅威がランクインしており、組織として情報漏えいに対応する必要性が示されています。業務が停止するほか情報漏えいによる社会的影響も拡大しています。

1位の「標的型攻撃による情報流出」については、企業や民間団体、官公庁など、特定の組織に対して、メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させ、そのPCを遠隔操作して、別のPCに感染を拡大し、最終的に個人情報や業務上の重要情報を窃取する標的型攻撃による被害が引き続き発生しています。

5位の「内部不正による情報漏えい」については、昨年に比べて順位は下がったものの、組織内部の職員や元職員による、情報の不正な持ち出しなどの不正行為は後を絶ちません。不正に持ち出した情報の紛失により情報漏えいにつながるケースは多々発生しています。

内部不正を防ぐには、制約や罰則を設けるといった管理的な対策に加えて、適切なアクセス権限の設定やログの収集・管理などの技術的な対策を取り、不正行為を防止するとともに、検知と追求が可能な環境であることを関係者に周知する必要もあります。

順位	「組織」の10大脅威	前年（2018年）の順位
1位	標的型攻撃による情報流出	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	ランク外
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	1 2位

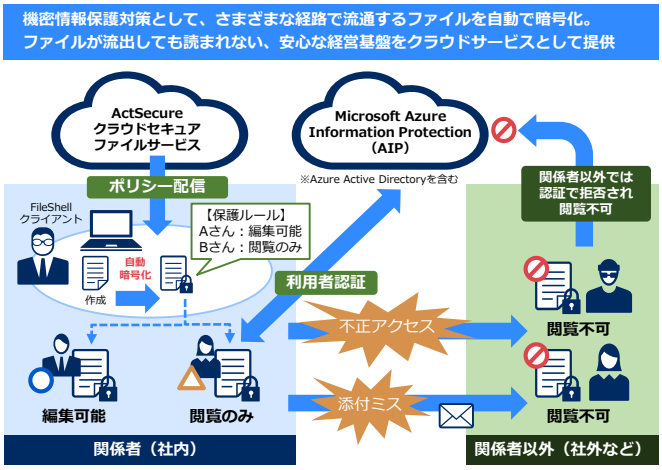
出典：情報セキュリティ10大脅威（https://www.ipa.go.jp/security/vuln/10threats2019.html）

情報セキュリティ10大脅威 2019 より

2 ファイルが流出することを前提にあらかじめファイルを暗号化

ファイル自身にセキュリティ情報を持たせ、ファイルがどこに存在しても、常にアクセスとアプリケーションの操作を制限することで、万が一、ファイルが漏えいしたとしても中身は漏えいしない安心できる環境を実現できます。

その環境を実現するために、ファイル自身にセキュリティ情報を持たせ保護（暗号化＋利用者認証）する基盤としてAzure Information Protectionを活用し、ActSecureクラウドセキュアファイルサービスでさまざまな場所や形式のファイルを自動で暗号化する仕組みをクラウドサービスとして提供しています。



クラウドセキュアファイルサービス とは

3 導入効果

経営観点のメリット

情報漏えい事故が発生すると、「取引先からの取引停止」「顧客からの信用失墜」「ブランドイメージの低下」による収益悪化と「被害者への賠償」「再発防止対策費用の投入」のためのコスト増が発生します。

特に、被害者への賠償として、個人情報漏えいに対する平均損害賠償額は1件あたり6億3767万円（NPO法人 JNSA発表 2019/6）との試算もあり、経営に深刻なダメージを負うことになります。

これらのリスクに対応するため、万が一ファイルが流出しても中身は漏えいしない対策で、セキュアな経営基盤を確立しておくことが重要です。

システム運用管理面のメリット

ファイル自身にセキュリティ情報を持たせ、通常時から保護（暗号化＋利用者認証）されたファイルを利用することで、万が一、ファイルが外部に流出したとしても、ファイルの中身を閲覧できないため、「情報セキュリティ10大脅威 2019」にもあげられる、標的型攻撃、内部不正などによる情報漏えいを防ぐことが可能です。

また、このような仕組みをクラウド上のサービスで提供していることから、情報システム部門管理によるサーバー構築が不要です。

全体導入といった大規模から、早急に部分導入といった小規模まで、さまざまな導入計画を立てることが可能です。運用についてもサービスで一元管理し、「情報システム部門」の負担とならない運用性を実現しています。

利用者のメリット

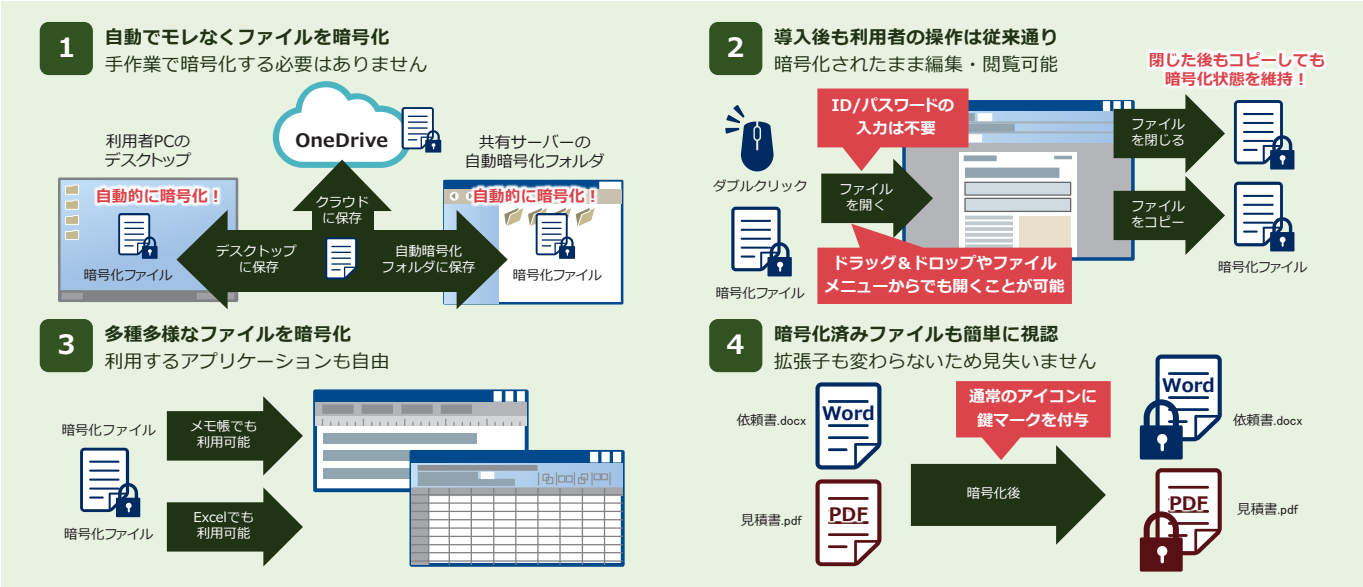
ファイル自身にセキュリティ情報を持たせる仕組みを導入しても利用者の操作性は変わらず、セキュリティと利便性の両立を実現する4つの仕組みを提供しています。

1 自動でモレなく暗号化　利用者のスキルやモラルに関係なく自動でファイルを暗号化できます。

2 導入後も利用者の操作は従来通り　利用者の認証も自動化、ファイルの利用を許された利用者のみファイルを開くことが可能です。またファイルを開いている間も、ファイル自身は暗号化されたままで、常にファイルを保護しています。

3 多種多様なファイルを暗号化　利用者が今まで利用しているアプリケーションのまま暗号化したファイルを利用することができます。

4 暗号化済みファイルも簡単に視認　暗号化した後、通常のファイルアイコンの上に鍵マークを付与し、暗号化状態を視認できます。拡張子は変わらないため、今まで通りの運用が可能です。



4 ファイル暗号化サービスで安心感を提供

ActSecureクラウドセキュアファイルサービスでは、NECグループで利用している機密情報保護ソフトウェア「InfoCage FileShell」をサービス化しています。「InfoCage FileShell」の総出荷数は70万クライアント以上で、140社／団体以上のお客さまにご利用いただいています。

「InfoCage FileShell」を導入いただいたお客さまが抱えていた代表的な課題は以下の3つです。

1. 標的型攻撃やうっかりミスによるファイル流出を完全に防ぐことは困難と感じている
2. 従業員や職員のITスキルに関係なくファイルを守りたい
3. なるべく従業員や職員の利便性を損ないたくない

これらの課題を「ファイル暗号化サービス」で解決し、ファイルが流出しても中身は漏えいしない安心な経営基盤を提供します。