12の「オフィスセキュリティソリューション」で中堅・中小企業においても万全なセキュリティ対策を

ITの普及と活用の進化は、ビジネスに利便性とさらなる拡大の機会をもたらす一方、さまざまなセキュリティリスクを抱えることにも繋がっています。当社は、企業の身近に迫るセキュリティリスクの中でも、近年、多く発生している「情報流出・紛失」「改ざん・破壊」「侵入・感染」の3つの危機に対して、12の対策をまとめた「オフィスセキュリティソリューション」を提供しています。

セキュリティ事故の傾向と企業における対策状況

情報システムやインターネットの活用によりICTの利便性は大幅に向上している一方、情報漏えい問題やサイバー攻撃などのニュースは日々絶えることがありません。JPCERT/CC「インシデント報告対応レポート」とIPA「情報セキュリティ白書2014」によると、2013年度に発生したセキュリティ事件・事故は29,191件と前年と比べて46%も増加し、その内訳は「情報流出・紛失」が81.3%、ホームページやサーバーなどの「改ざん・破壊」が10%、企業の情報ネットワークへの「侵入・ウイルス感染」が6.4%となっています。

攻撃は、従来のパソコンやサーバーをウイルスに感染させる「愉快犯」から、改ざんやフィッシング詐欺などの「金銭目的」に変わっています。攻撃の手口も高度な技術を使い、複数の手口を組み合わせ、長期間に渡って攻撃をし続けるなど、高度化、かつ悪質化しています。

また、スマートフォンやタブレットなどのモバイル端末がビジネスシーンで活用されることが多くなり、攻撃対象がパソコンやサーバーからモバイル端末に広がったこともセキュリティ事故を増大させる要因になっていると考えられます。

このように、年々増加するセキュリティ事故に備え、企業においては、セキュリティ事故に対する対策を進めていますが、中堅・中小企業は大企業とは異なり、セキュリティ対策に長けた専門技術者がいなかったり、対策のために十分なコストがかけられなかったりといった現状があります。

しかし、2005年より施行された個人情報保護法により、大企業の委託先がセキュリティ事故を起こした場合でも委託元の大企業が社会的責任を負い、損害を補償することが社会通例となりつつあることから、中堅・中小企業においても、しっかりとしたセキュリティ対策を行わないと、自社のセキュリティリスクを脅かすだけでなく、取引にまで影響する時代になっていると言えます。

「内部の悪意」と「間接漏えい」による情報流失をどう防ぐか

セキュリティリスクの中でも2013年度のセキュリティ事故の81.3%を占める「情報流出・紛失」について、実際に起こった事故の実例を見ながら効果的な対策を紹介します。

(1)情報流出事件

●ケース1:退職者による情報流出(悪意ある内部による漏えい)

某ソフトウェア開発会社で、「退職者」により次期製品の設計情報が他社に流出する事件が起こりました。この会社では、全社員へ情報管理の教育を定期的に行い、またルールや手順を定めるなどの対策を行っていましたが、悪意を持った社員による情報流出を防ぐことはできませんでした。悪意を持った内部による情報流出は防ぐことが難しいと言える一例になります。

●ケース2:取引先による間接漏えい(間接漏えい)

某設備工事会社では、顧客から工事を請け負い、工事の一部を委託先に依頼しており、工事にあたり個人情報や工事図面などの重要情報を委託先に渡していました。しかし、委託先では、重要情報が入ったパソコンを車内に放置するなど、重要情報の取り扱いや管理の意識が低く、顧客からクレームと改善指示を受ける事態となりました。委託先を含めた自社のセキュリティ対策が取引にまで影響する一例になります。

(2)悪意ある内部と間接漏えいへの対策

上記事件のように、悪意を持った内部(社員)や取引先での情報流出は、社員教育やルールの徹底、また従来型の情報を受け渡す時だけのパスワードによる暗号では、情報の流出を防ぐことはできません。当社では、この「悪意を持った内部(社員)」と「取引先」による情報流出対策として、「電子ファイル暗号・追跡サービス」を提供しています。

本サービスは、2つの予防対策と1つの事後対策により、重要情報が流出する

ことも想定した対策が行えることが特長です(図-1)。

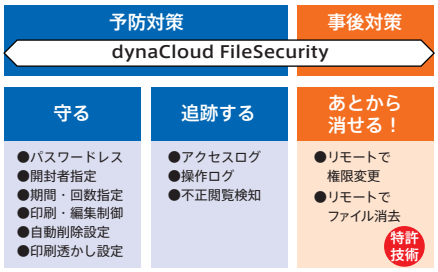

図-1　電子ファイル暗号・追跡サービス
(dynaCloud FileSecurityの概要)

●守る(予防対策)

DRM暗号技術を使い、パスワードによる暗号ではなく、メールアドレスを用いて個人を特定する暗号で重要情報を保護します。また、「いつまで」「何回まで」「印刷可否」などの権限情報を付与して重要情報へのアクセスを制限します。権限を満たさない場合は、重要情報を見せないことに加え、権限を破ってアクセスした場合は自動で重要情報を物理的に消す仕組みを提供しています。

●追跡する(予防対策)

重要情報に対して、いつ・誰がアクセスしたのかといったすべてのログをクラウドサーバーに保存しています。これにより、自身が管理する重要情報に対して、いつ・誰がアクセスしたのかを追跡することができます。また、許可していない人が重要情報にアクセスしている場合には、「守る」仕組みで付与した権限情報を変更して、許可していない人に渡った重要情報を見せない、物理的に消す仕組みを提供しています。

●あとから消す(事後対策)

万が一、重要情報が流出してしまった場合、重要情報への権限情報を変えることで、流出した重要情報をあとから物理的に消す仕組みを提供しています。

本サービスはクラウドサービスとして提供していますので、初期コストや、ハードウェア・ソフトウェア・サーバー管理者などのリソースが不要です。自社で対策が急務となった場合でも、最短1週間ですぐに導入することが可能となっています。

身近な脅威と対策を12のソリューションで提供

先の「電子ファイル暗号・追跡サービス」を含め、当社では特に事故や被害が多い「情報流出・紛失」「改ざん・破壊」「侵入・感染」に焦点を当てた、身近に迫るセキュリティリスクに対応する12のソリューションを提供しています。導入しやすいクラウドサービスを多数取り揃え、自社に見合ったセキュリティ対策が行えるよう、さまざまなサービスを提供しています(表-1)。

表-1　オフィスセキュリティソリューション

リスク・脅威		サービス・ソリューション名	サービス概要
情報流出・紛失	不正持ち出し、流出、紛失から重要情報を守る	電子ファイル暗号・追跡サービス クラウドサービス	DRM※1暗号技術より、重要情報を「守る」「追跡する」「後から消す」仕組み
	誤送信や改ざんから電子メールを守る	メールセキュリティサービス クラウドサービス	ウイルス対策、本文・添付ファイル暗号、誤送信対策により電子メールを守る仕組み
	紛失や盗難からモバイル端末を守る	モバイルデバイス管理サービス クラウドサービス	モバイル端末を一元管理、ワイプ機能によりモバイル端末を初期化する仕組み
	紛失や盗難からパソコンを守る	東芝VDI対応シンクライアントソリューション	東芝独自技術により、端末に一切の情報を残さないシンクライアントパソコン
	悪意ある内部犯行から重要情報を守る	特権ID/アクセス管理ソリューション	ID管理とアクセス管理機構により、不正アクセスから重要情報を守る仕組み
改ざん・破壊	改ざんや乗っ取りからWebサイトを守る	改ざん検知・変更管理サービス クラウドサービス	常時監視、変更管理、セキュリティ監査評価機構により、Webサイトを守る仕組み
侵入・感染	脆弱性を突いた侵入、感染からパソコンやモバイル端末を守る	マルチデバイス管理サービス クラウドサービス	マルチネットワーク・マルチデバイス対応により国内外に点在するIT資産を一元管理、自動セキュリティ診断でIT資産を守る仕組み
	セキュリティホールを突いた侵入、感染からパソコンを守る	情報漏えい防止・監視アプライアンス	OSや各種ソフトウェアのパッチ情報を一括管理、自動適用でIT資産を守る仕組み
	不審者の不正入室から守る	出入管理ソリューション	防犯センサと連動した小型軽量の出入管理により、機密場所を守る仕組み
	不審者の不正入室、不正行動から守る	ネットワークカメラモニタリングサービス クラウドサービス	クラウドを用いた監視カメラにより、いつでもどこからでも機密場所を守る仕組み
	不正な無線LANの脅威から守る	無線IPS(不正侵入防止)ソリューション	不正な無線LAN、デザリングを経由した情報搾取、情報持ち出しから守る仕組み
	検疫機構により、社内ネットワークを守る	資産管理・ネットワーク検疫ソリューション クラウドサービス	IT資産を一元的に管理、セキュリティポリシーに満たないIT資産を検疫することにより不正接続からネットワークを守る仕組み

※1　DRM……Digital Rights Management

自社に見合ったセキュリティ対策

セキュリティ対策を行うことは、自社のセキュリティを守るだけでなく、企業存続の危機から守ることにも繋がっています。しかし、すべてのセキュリティリスクの対策を行うには、青天井のコストと多大なリソースが必要になることから、特に中堅・中小企業では現実的な取り組みとは言えません。

当社では、米国CSCで定義された情報セキュリティフレームワーク(図-2)を使い、セキュリティリスクに対する優先度や網羅性を見極めながら対策の適用範囲を決めていくとともに、企業の身近に潜むセキュリティリスクに対応する12のソリューションにより、中堅・中小企業に見合ったセキュリティ対策を提供していきます。

(SIソリューション事業部　野瀬 克紀)

図-2　情報セキュリティフレームワーク(出典：Critical Security Controls)