【情報セキュリティ対策の主要ポイント】　　文責：河東岩夫　　作成日：平成 27 年 12 月 25 日

昨今、日本年金機構等での大規模な情報漏洩事件や IT の使用環境の著しい変化が生じているため、ベンダー各社が開催した４つの分野(標的型攻撃、組織内部者犯行、グラウド利用、BYOD 運用)の対策セミナーから“情報セキュリティ対策の主要ポイント”の知見を得たので以下のとおりに纏めた。

情報セキュリティリスクの状況	情報セキュリティ対策の事例
(1)標的型攻撃：標的型攻撃は、様々な手法で攻撃してくるため、侵入自体を完全に防ぐことは困難であるが、侵入を防ぐための対策はもちろん必要である。万が一侵入されても機密情報を窃取されないよう、右記のような対策を講じる必要がある。	①入口対策：次の事例等で多くの攻撃者の侵入を未然に防ぐ。 ・不正ソフトの社内ネットワークへの侵入を検知し、通信を遮断する。 ・入手ソフトをサンドボックス等で検証し、不正ソフトの社内への拡散を防止する。 ②内部対策：次の事例等で攻撃者の目的を阻む。 ・特権 ID(管理者権限)による機密情報や VLAN 等による部門間へのアクセスを制限する。 ・不正ソフトに感染した機器を社内ネットワークから即時に遮断する。 ③出口対策：次の事例等で機密情報の持ち出しを制御・困難にし、持ち出されても閲覧を困難にする。 ・機密情報の持ち出し制御(DLT)：機密情報をラベリングし、機密レベルに合わせた制御(例えば「社外秘」という文字列を含むファイルの USB やメール、Web 等への持ち出し禁止)を行う。 ・機密情報の閲覧制御：機密情報を暗号化することで、持ち出されても情報の流出を防ぐ。 ④ログ分析：攻撃を受けたシステムのログの分析を行うことで、標的型攻撃を検知し、迅速に対応する。
(2)組織内部者犯行：大規模な情報漏洩事件では内部者(委託先を含む)による犯行が多く起因しており、右記のような対策を強化する必要がある。	①業務内容や責任範囲に則したアクセス権の見直しを行い、アクセス範囲及び権限者を最小限にする。 ②IT 管理者や業務担当者の権限による不正行為を抑制するために、入退室記録、システムへのアクセスログ等の取得と記録の確認を定期的に行う。 ③組織内部での連絡・報告体制を明確にする。 ④仕事や役割に対する責任感、ルール違反を行った際に予想される結果等の教育を行う。 ⑤委託先での個人情報取扱いの状況確認、再委託等の状況把握、適切な委託先の監督を行う。 ⑥社内では常時監視の状況を従業員に意識させる等、内部不正行為に対する牽制を行う。 ⑦顧客情報等の重要な情報を持出した場合の罰則規定や契約条項を強化する。

情報セキュリティのリスク	情報セキュリティ対策の事例
(3)グラウド利用：グラウドサービスは利用者にとって情報システムの保守、運用、管理に関する負担が軽減される等での利点がある一方で、通信回線を利用、サービス提供者が管理するデータセンタにサーバを保管、サービス提供者に運用やデータ管理を依存する等の特性があるため、事業者が右記のような情報セキュリティ対策を適切に講じているかを確認し、選定する必要がある。	①データセンタの物理的な情報のセキュリティ(災害・侵入等)対策。 ②データのバックアップ(電子割符を含む)対策。 ③ハードウェア機器の障害対策 ④仮想サーバ等のホスト側の OS、ソフトウェア、アプリケーションでの脆弱性の判定と対策。 ⑤不正アクセスの防止対策。 ⑥アクセスログの管理対策。
(4)BYOD 運用：BYOD 端末の普及は業務の効率を向上させる点では大変に有効であるが、特に BYOD 端末の紛失時には個人情報の漏洩リスクがあるため、右記のような対策を講じる必要がある。	①IT 管理者は権限で MDM 等の機能により、BYOD 端末の紛失時の遠隔ロック、移動履歴の表示、アプリの配布・更新・削除、起動ブロック、不正対策ソフトのインストール、ユーザでのインストールの拒否等を行う。 ②業務領域をサーバ内の仮想 BYOD OS 内に設置し、端末内に設置しない。 ③端末認証とユーザ認証の多要素認証を使い、機密性の高いサーバを保護する。 ④VPN 等により、通信路のセキュリティを確保する。 ⑤盗難時の連絡体制、対応の手順を整備して社員へ周知する。 ⑥賠償責任を明記した従業者との誓約書や委託先との契約書を取り交わす。 ⑦原則、会社支給物と同等のセキュリティ対策を実装し運用する。