情報セキュリティ白書 10大脅威

2013年度

- 1位「クライアントソフトの脆弱性を突いた攻撃」
  - 更新忘れのクライアントソフトが狙われている
    - Adobe Reader, Adobe Flash Player, Oracle Java(JRE)
  - ユーザの対策意識を高めることが重要
    - Mac OSを狙うFlashbackマルウェア（Adobe Flash Playerのアップデートを装う）
  - 脆弱性対策に加え、被害の出にくいシステム設計を行う
    - 個々のPCにファイアウォール(ハード)を設置
- 2位「標的型諜報活動の脅威」
  - 知らない間にスパイがあなたの情報を盗んでいる
    - 金銭目的のサイバー空間上での諜報活動
  - 攻撃者によるウイルスを使ったリモートハッキング
    - 標的型メール攻撃…URLへ誘導→PCハッキング
  - 外部からだけではなく、内部からの攻撃を想定した対策を
    - インターネットはパブリック・ネットワーク
- 3位「スマートデバイスを狙った悪意あるアプリの横行」
  - あなたの個人情報が狙われている
    - 金銭目的
  - 悪意あるアプリが情報を根こそぎ持って行く
    - 個人情報が多く保存されているスマートデバイス
  - 信頼できるアプリやサービスの利用を心がける
    - スマートデバイス用のウイルス対策ソフト
- 4位「ウイルスを使った遠隔操作」
  - 知らない間に濡れ衣を着せられることに！
    - 被害者ではなく加害者へ
  - 知らない間にウイルスによって遠隔操作される
    - 自分のPCがDDoS攻撃への加担（ボット化）
  - 日頃からPCを安全な状態に
    - 脆弱性対策(アップデート)、ウイルス対策
- 5位「金銭窃取を目的としたウイルスの横行」
  - 日本でもインターネットバンキングが狙われている
    - 海外の猛威が日本のユーザを標的に
  - 認証情報を取られると他人の口座に送金される
    - SpyEyeウイルス対策
  - PCを健全にし、自衛に努める
    - 脆弱性対策(アップデート)、ウイルス対策
- 6位「予期せぬ業務停止」
  - 自然災害やハードウェア障害、人的ミスが思わぬ事態を引き起こす
    - 日頃の堅実な運用・監視
  - 自然災害や障害は突然やってくる
    - 可用性対策！
  - 自然災害や障害を想定したシステムと運用を
    - システム設計・監視、アカウント／権限管理
- 7位「ウェブサイトを狙った攻撃」
  - 断続的に続くウェブサイトを狙った攻撃
    - 脆弱性大：ウェブサイトはさまざまなアプリケーションで構成
  - さまざまな意図により狙われるウェブサイト
    - 情報の窃取、ウイルス配布、改ざん(主義・主張)
  - 開発から運用・監視まで幅広い対策を
    - システム設計・監視、アカウント／権限管理、脆弱性対策
- 8位「パスワード流出の脅威」
  - 知らぬ間にパスワードが盗まれていませんか？
    - パスワードからパスフレーズへ、3か月(四季)毎の更新
  - オンラインサービス増加に伴うパスワード使い回しの現状
    - サービス毎に別のパスワード・パスフレーズ
  - 安全なパスワードの運用・管理が重要
    - アカウント／権限管理、パスワード更新設定
- 9位「内部犯行」
  - あなたの職場は大丈夫？内部に潜む犯行者
    - 元雇用員、非正規雇用員
  - 金銭目的での内部犯行が多発
    - 2012年度統計：内部犯行の動機の32%が金銭目的 ← 組織への不満、転職目的が26%
  - 不正を起こしづらい状況を創出
    - アカウント／権限管理、ポリシー／ルール
- 10位「フィッシング詐欺」
  - あなたの口座から預金が無くなっていませんか？
    - インターネットユーザをターゲットにしたフィッシング詐欺が横行
  - メールとウェブサイトを使った詐欺行為
    - 大手銀行を装ったフィッシング詐欺
  - 注意深い対応・対処を心がけること
    - 教育／啓蒙、アカウント／権限管理

2012年度

- 4位「今もどこかで…更新忘れのクライアントソフトを狙った攻撃」
  - 標的型攻撃にも悪用されるクライアントソフトの脆弱性
  - 資料
    - ➜ いまー番危ない脆弱性は何だ? ～2011年版～
    - ➜ 2011年度 情報セキュリティの脅威に対する意識調査
- 1位「機密情報が盗まれる！？ 新しいタイプの攻撃」
  - 情報窃取を目的とする標的型の諜報攻撃(APT)
    - APT(Advanced Persistent Threat)：先進的で執拗な脅威
    - =CE(Cyber Espionage)：サーバー空間における諜報活動
  - 事例
    - 2011/7：全衆議院議員ID流出
    - 2011/9：三菱重エウイルス
- 6位「続々発覚、スマートフォンやタブレットを狙った攻撃」
  - 狙われる小さなパソコン-スマートデバイス
  - 資料
    - ➜ スマートフォン市場規模の推移・予測（12年3月）
    - ➜ McAfee脅威レポート：2012年第1四半期
- 2位「予測不能の災害発生！引き起こされた業務停止」
  - 自然災害や人為的災害によるITシステムの故障、業務データの消失
  - 資料
    - ➜ 読者調査で分かった、計画停電後に企業が実施している電源対策
    - ➜ みずほ銀行　システム障害特別調査委員会の調査報告書
    - ➜ 新日鉄ソリューションズ　通信障害
- 3位「特定できぬ、共通思想集団による攻撃」
  - 社会変革をめざす共通的な思想を持つ集団による暴露・妨害攻撃
  - 資料
    - ➜ アノニマス サイバー攻撃
    - ➜ 対アノニマス？ サイバー攻撃対策機動チーム「CYMAT」発足
- 5位「止まらない！ウェブサイトを狙った攻撃」
  - 狙われ続けるウェブサイトの脆弱性
  - 資料
    - ➜ 通称「LizaMoon（ライザムーン）」によるウェブサイトの改ざん被害が拡大
    - ➜ 大規模なIFRAMEインジェクション攻撃
- 7位「大丈夫！？電子証明書に思わぬ落し穴」
  - 電子証明書の管理不備により、引き起こされた問題
  - 資料
    - ➜ 政府機関から盗まれた証明書、マルウェアに利用される
    - ➜ DigiNotarの不正証明書問題
- 8位「身近に潜む魔の手・・・あなたの職場は大丈夫？」
  - 組織内部・関係者による業務妨害や情報漏えい
  - 資料
    - ➜ セディナ　お客様情報の不正売却
    - ➜ SB モバイルの大規模障害
- 9位「危ない！アカウントの使いまわしが被害を拡大！」
  - アカウント情報の管理不備が原因で発生するなりすまし被害
  - 資料
    - ➜ Facebook、新しい管理ツール提供へ　ログイン乗っ取りは「毎日60万件」
    - ➜ ソニー　ユーザアカウントへの第三者のなりすまし
- 10位「利用者情報の不適切な取扱いによる信用失墜」
  - 利用者との結びつきが強い情報(利用者情報)の取り扱いに関する問題
  - チェック項目
    - 必要以上に利用者情報を収集していませんか？
    - 利用者にきちんと使用目的を伝えていますか？
  - 資料
    - ➜ ソニー　オフィシャルサイトをご利用中のお客様へ
    - ➜ コネクトフリー　お客様情報の不正取得