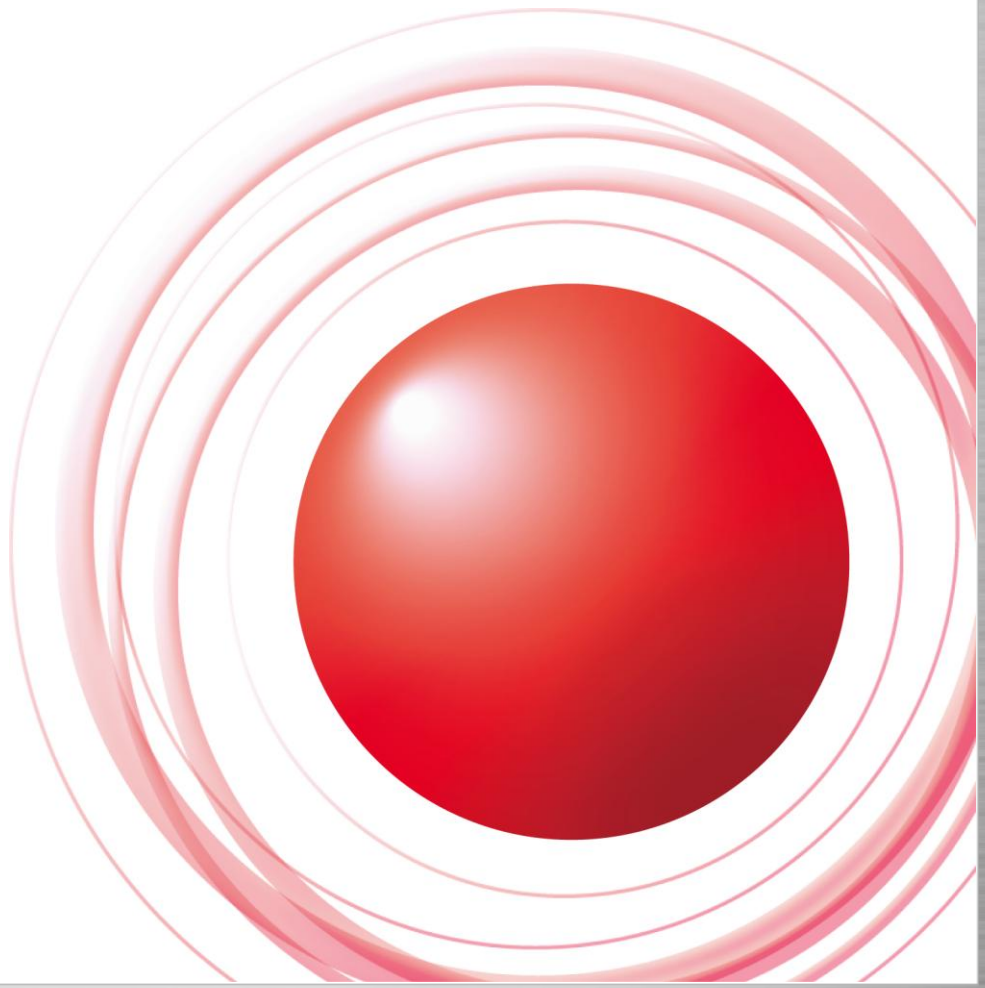
情報セキュリティ月間 キックオフ・シンポジウム

大切な情報をどう守るか― 情報セキュリティ最前線
パネルディスカッション資料

IIJ
Internet Initiative Japan



2013/02/01

株式会社インターネットイニシアティブ
サービスオペレーション本部セキュリティ情報統括室
齋藤衛

Ongoing Innovation

自己紹介

齋藤　衛（さいとう　まもる）

株式会社インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室 室長
1967年生まれ。1993年中央大学大学院 理工学研究科 管理工学専攻修了。

1995年株式会社インターネットイニシアティブに入社。法人向けファイアウォールサービスに従事の後、法人向けセキュリティサービスの 開発(マネージドセキュリティサービス、IDSサービス、DDoS対策サービスなど)、セキュリティサービス担当プロダクトマネージャを経て、現職。

2001年よりIIJグループの緊急対応チーム IIJ-SECTの活動を行う(IIJ-SECTは2002年にFIRSTに加盟)。テレコムアイザックジャパン 、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、テレコム・セプターなど複数の団体の運営委員。総務省「スマートフォンとクラウドセキュリティ研究会」構成員など複数の場で活動を行う。共訳書として「ファイアウォール構築 第二版」(オライリー・ジャパン) 。IIJ-SECTの活動は平成21年度「経済産業省商務情報政策局長表彰（情報セキュリティ促進部門）」を受賞。

スマートフォンの利活用とセキュリティ対策

スマートフォン利用の利点

- 個人利用者にとって
  - 高速な複数の接続手法でどこでも使える。
  - ネットワーク上の多くのサービスを利用でき、多様な形式の情報を取扱い・参照・表示できる。
  - 個人の活動を簡単に電子化、保存、転送、公開できるツール（写真、つぶやき、位置情報など）。
- 企業などにとって
  - 利用者が利点を駆使して知的活動を行うことで、仕事をする機会の増加、速度の向上が期待できる。
  - 利用者自身の端末を仕事に使ってくれることによるコスト削減が期待できる。

スマートフォンの利活用とセキュリティ対策

スマートフォン利用上の問題

- 実際に発生した事件などから
  - 盗難、紛失、覗き込みなどの携帯端末としての問題
  - 公衆無線LAN利用に関連する問題
  - 脆弱性対応手法、速度、手作業によるアップデート
  - マルウェア感染による被害
  - パーミッションによる情報へのアクセス許可
  - セキュリティ対策アプリに対する制限
  - 非公式マーケットなどからのアプリの入手経路
  - 情報窃取目的などの悪意のあるアプリ
  - 正当なアプリによる利用者情報の過剰な取得と取り扱い
  - アプリと連携するクラウド上などのネットワークサービスのセキュリティの問題
  - 国外のOSベンダ、アプリ開発者、サービス事業者などは、国内の規制を受けない

⇒携帯電話のセキュリティ対策手法およびPCのセキュリティ対策手法両方で保護する必要がある。ただし、それだけでは十分ではない可能性がある。

スマートフォンの利活用とセキュリティ対策

PCとスマートフォンの違い

IIJ Internet Infrastructure Review(定期発行技術レポート) Vol. 17より
http://www.iij.ad.jp/development/iir/

	PC	スマートフォン	利用者が注意する点	改善の方向性
OS	・脆弱性の緊急対応についてはタイムリーなアップデートがある。 ・アップデートでOSに問題が出ることは比較的少ない。 ・月次で自動的にアップデート。	・脆弱性への対応がPCに比べて遅い。 ・アップデートされたOSの品質に問題。 ・アップデートは利用者による操作が必要。 ・JailBreak、Root化の問題がある。	・OSの更新を行う。 ・セキュリティについて考慮された端末を利用する。	プラットフォーム事業者によりOS仕様が厳密に管理されている場合はプラットフォーム事業者の努力による。オープンなOSでは端末メーカによって独自の対策が行われていることもある。
アプリ	・アンチウィルスソフトが高い権限で動作している。 ・主要なアプリケーションは自動アップデートされる。 ・アプリケーションの安全性の評価が比較的容易。	・アンチウイルスソフトが一般ユーザ権限で動作している。 ・アップデートはアプリ開発者や利用者に任せられている。 ・非公式マーケット、非公式アプリが存在し、安全性の検証が困難。	・アプリケーションの入手に注意する。 ・アプリケーションがアクセスするデータを確認する。 ・利用しているアプリの評判を確認する。 ・不必要な情報の取得があれば、利用をやめる。 ・利用するネットワークサービスの評判を確認する。	公式マーケットによるチェックの強化や、キャリア等による独自の安全性検証が徐々に強化されつつある。
利用者情報	・利用者情報とアプリケーションの関連性が低い。 ・利用者自身による保護対策の選択が可能である。	・アプリケーションと利用者情報が密接に結合している。 ・アプリ利用権限の粒度が荒く、いったん許可した権限は以後変更されない。	・GPSなどの個人データが付与される機能は、不必要であればオフにする。 ・利用するネットワークサービスの認証情報を適切に扱う。 ・作成したバックアップやネットワークサービスにアップロードされたデータは暗号化する。	監督官庁の研究会や業界団体等でよりよい利用者情報の扱い方について検討が行われている。
無線LAN	・意識的に接続が必要。	・不正なアクセスポイントが横行している。 ・アクセス先がわからない/わかりづらい。	・無線LAN利用時のアクセスポイントに注意する。 ・無線LAN利用時には暗号化通信を行う。	総務省スマートフォンクラウド研究会での問題提起があり、今後の検討課題となっている。
端末管理と利用の状況	・基本的には利用場所、利用シーンが限定される。物理的な固定を前提としてセキュリティワイヤー利用等が可能。	・利用場所や利用シーンが多岐にわたり、可搬性が非常に高い。 ・携帯電話と同様の感覚で利用されている。	・利用時の周りの状況に注意する。適時、仕事をしてよい状況かどうか判断する。 ・覗き込まれるような公共の場所では利用しない。 ・紛失、盗難対策を行う。特に喫茶店などで机の上におかない。	会社利用を前提として、MDM等の利用で被害状況の軽減が可能である。また、従来通り、プライバシフィルタ等の対策も有効である。

スマートフォン利用の対策

- スマートフォンはまだ発展途上である
  - 端末メーカ、OSベンダ、アプリ開発者、サービス事業者、法律やガイドラインの整備、国際協調連携などは、それぞれの企業や組織が対応を進めている。
- 個人ユーザにとって
  - 総務省スマートフォン情報セキュリティ三カ条などを実践する。
    (基本ソフトを更新する、ウイルス対策ソフトを利用する、アプリケーションの入手方法に気を付ける)
  - 利用中のアプリのセキュリティ情報に気を付ける。
  - 紛失対策（遠隔消去など）、バックアップを実施する。
  - 日々の利用において、仕事をしてよい場所かどうかを判断する。
- 企業などにとって
  - 仕事利用時の対策手法を提供し、利用方法をガイドライン化する。
    - 仕事の通信に対する暗号化など安全な通信路の提供
    - 安全なバックアップ手法と管理の提供
    - スマートフォンアプリに直接仕事の情報を扱わせない利用形態の提供(リモートデスクトップなど)

企業等におけるサイバー攻撃対策

企業等におけるサイバー攻撃対策

企業等におけるサイバー攻撃と対策の現状

- 攻撃状況
  - 諜報活動(標的型攻撃含む)
  - 内部犯行
    - The CERT Insider Threat Center (http://www.cert.org/insider_threat/index.html)
    - 財団法人 社会安全研究財団 情報セキュリティにおける人的脅威対策に関する調査研究会、「情報セキュリティにおける人的脅威対策に関する調査研究報告書」（http://www.syaanken.or.jp/02_goannai/08_cyber/cyber2203_01/pdf/cyber2203_01.pdf）。

- 既存のセキュリティ対策手法
  - 外部からの攻撃に対する境界防御(ファイアウォール、侵入防御システムなど)
  - 個別攻撃手法に対する対症療法(脆弱性対策、Webアプリケーションファイアウォール、アンチウイルス、迷惑メール対策など)
  - ユーザ認証、記録、異常の即時検出と報告

企業等におけるサイバー攻撃対策

企業等におけるサイバー攻撃対策の課題

- 既存の対策に対する不信
- 知の結集のむずかしさ
  - 標的型攻撃を扱う複数の対策プロジェクト
    - サイバーインテリジェンス対策のための不正通信防止協議会、サイバー情報共有イニシアティブ、テレコムアイザック官民連携会合、サイバー攻撃解析協議会、CEPTOAR Council 情報共有WG、日本セキュリティオペレーション事業者協議会 WG5など
  - 情報提供、情報共有、情報公開の必要性とむずかしさ(法律上、契約上の制約など)
- 不慮の事態への対応

企業等におけるサイバー攻撃対策

企業等におけるサイバー攻撃対策の強化

- 既存対策手法の機能と限界の再認識
- 標的型攻撃や内部犯行を想定した対策
  - 組織内ネットワークにおける複数の境界の設定、および認証、通信記録、操作記録の保全と結合など
  - 重要な情報資産の（再）定義
- 緊急対応の仕組み(CSIRTなど)の構築
- 情報提供、情報共有、情報公開の準備

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation