資料4－6

情報通信環境の変化と
情報セキュリティの脅威・課題について

総務省 情報通信政策局
情報セキュリティ対策室
2008年1月31日

2010年-11年頃の情報通信環境とは？

- **ユビキタスネット社会の実現**

  いつでも、どこでも、何でも、誰でもネットワークに簡単につながり、利用できる社会

  - **情報通信ネットワーク技術の高度化**
    - ・電気通信網のIP化（NGN）の普及とインターネットとの並存
    - ・IPv6の利用促進（IPv4との共存）
    - ・次世代無線システム等無線アクセスの多様化
    - ・第4世代移動通信システムの実現
    - ・家電のネットワーク化（情報家電）・高機能なロボットの普及
    - ・FMC、FMBC（固定通信、移動通信、放送の融合）サービスの台頭
    - ・P2P等、オーバーレイネットワークの利用拡大、等

  - **スマートフォン等、携帯電話の高機能化によるモバイル利用環境の進展**
    - ・ OS、アプリケーションのオープン化、APIの公開
    - ・携帯端末等を利用して、ホームネットワークに繋がった情報家電を制御
    - ・携帯端末による認証・電子決済、等

- NWを流通するデータ量、NWと接続するデバイス数の爆発的増加
  - ・インターネット利用者数の増加
  - ・携帯電話端末、PDA、ゲーム端末等、non-PCによるインターネット利用の増加
  - ・Blog、SNSなどのCGM（インターネットを通じて消費者が情報を生成し発信していくメディア）の増加
  - ・大容量マルチメディアコンテンツの流通拡大
  - ・情報家電、RFIDの利用拡大（運輸、卸売・小売、医療・福祉、製造、等）、等

- 消費活動等の変化
  - ・非接触ICカードの普及による電子マネーの利用拡大（携帯機能の高度化）
  - ・こだわり型の消費活動の増大（口コミ情報や価格比較の利用、書込み）
  - ・RFIDによるリアルタイムの商品管理
  - ・商品情報・顧客情報の増大と営業戦略の変化、等

- 中小企業でのICT利用による生産性向上
  - ・ASP・SaaS、SOA、等

ICTサービスの状況予測（3年から5年後）

サービス提供者

金融・保険業
・顧客の個人情報を利用した金融商品の提供・販売*1
・バイオメトリックスなどの高度認証技術により店舗へ行かず 高額決済を実現*1
・株券の電子化*9

情報通信業
・個人向け情報配信（コンテンツの適切な配信）
・通信、放送関連法の一本化*8
・地上波デジタルへの移行*8
・ワンセグのサイマル放送開始*10

電気・ガス・熱供給・水道業
・自動検針、課金
・自動事故検知
・機器稼働状況確認
・センサー等と連動した省エネ制御

公務
・電子申請（転居や納税(e-TAX)などの手続をワンストップサービス、事業者向け行政サービス）*3
・電子投票
・国勢調査のInternet対応
・社会保障カードの実用化（年金・健康保険・介護保険の一元管理）*3
・防災情報の共有（速報・予測）*3

医療・福祉業
・人と薬品の統合管理（RFIDによる、投薬確認など）
・バイタルサイン利用による遠隔予防医療*2
・レセプトのオンライン化*3
・個人健康情報の一元管理と個人活用（電子私書箱）*3
・センサーなどによる、自律移動支援環境の実現*3
・GPSやセンサーを利用した徘徊検知・診察や治療の遠隔医療
・介護ロボット

複合サービス事業業
・電子郵便局
・電子切手

教育・学習支援業
・小中高等学校への高速インターネット接続の実現*3
・試験の電子化
・生涯学習の充実（博物館などのコンテンツの充実）*3

運輸業
・無線タグによるトレーサビリティの実現（配送の効率化、配送主・先へ状況通知、国際流通基盤の確立など）*3
・電子航空券（携帯＋2次元バーコード）の国際標準化*5
・GPS情報やセンサーを利用した、安全運転支援防止システム*3
・パスポートのIC化

製造業
・廃棄物の電子管理による徹底（電子マニフェスト）*3
・業務用ソフト基盤の共通化*6
・家電の稼働確認
・家電の省エネ制御
・ソフトウェアの自動更新
・環境に配慮したグリーン調達の普及*10
・国内市場の低迷により海外進出が本格化*10
・生産ロボットの高機能化

卸売・小売業
・生鮮食品のトレーサビリティ（RFIDを利用することで、品質保持期限を管理など）*3
・電子商取引におけるメーカーから卸・小売業までの共通基盤の整備*3
・ネットスーパー（個配）
・国内市場の低迷により海外進出が本格化*10

サービス業
【情報家電等】
・ホームコントロール*7
－個人により、空調・照明を自動制御
－屋外先から家電コントロール*2
－帰宅を感知し、自動で空調などを制御
・ホームセキュリティ*7
－屋外から室内を監視
－キーレスエントリー
－自動点灯等
・生活支援*7
－遠隔存在検知
－利用頻度による自動メンテナンス
－在庫情報とECショッピングの連携*2
・エンターテイメント*7
－個人向け情報配信（行動履歴利用。例：amazon）
－個人向けコミュニケーションサイト（例：SNS）
－屋外からの録画予約、視聴
－データ保存領域の共有
・ネットワークゲーム

コンシューマー
・どこででも業務環境が利用可能（テレワーク）*3
・SNSなどを利用した、地域にとらわれないコミュニケーションの実現と活性化
・メタバース（例：SecondLife）でのマルチライフの到来*10
・消費者主導の市場へ*1
・子供から、高齢者まで必要なサービスを利用できる（入力の簡易化）
・RFIDやGPSを利用した、子供の見守りシステムの普及
・ビジネス視点でIT活用するﾊﾟﾜｰﾕｰｻﾞの出現
・産消逆転現象
・サービスモデリング化現象
・店舗購買ｽﾀｲﾙの激変(ｾﾙﾌﾚｼﾞetc.)

端末

PC/PDA
・PCとAV機器の一体化
・携帯との融合
・連携型セマンティックWeb
・豊かでやさしいﾘｯﾁｸﾗｲｱﾝﾄ

情報家電（Internet家電）
・半導体の省電力化
・センサー家電のNW化
・センタ監視サービス進化

OS/ミドルウェア
・利用者が意識しないﾐﾄﾞﾙﾍﾞﾙでの端末監視・制御の実現
・端末仮想化の普及
・SOA／ASP・SaaS

携帯電話/スマートフォン
・携帯電話のSIMロック解除
・PCと変らない機能・性能の実現

非接触ICカード
・ホームセキュリティとの連携
・企業通貨の電子マネー化

RFID
・UHF帯の実用化
・RFID利用シーン多様化
・小売、流通ｼｽﾃﾑとの連携
・購買情報分析への流用化

ネットワーク

internet
・IPv6の普及（携帯電話、車載ITS、IT家電）
・膨大なNW機器管理

NGN
・2010年NGNの本格商用化
・1G光サービスの多様化
・連携型ID管理サービス
・知的IT処理システム出現
・IT処理システムの連携PF化
・ﾌﾟﾛﾋﾞｼﾞｮﾆﾝｸﾞ自動化

無線アクセス
・WiMAXの商用本格化
・第4世代移動通信システムの実現
・どこででもPCが無線LANにつながる（FONなど）
・ソフトウェア無線化

出典：
*1：NRI HPより
*2：u-Japan HPより
*3：首相官邸 IT戦略本部 重点計画2007より
*4：文部科学省 HPより
*5：NIKKEI NET HPより
*6：YOMIURI ONLINE より
*7：経産省 HPより
*8：総務省 HPより
*9：金融庁HPより
*10：「2008 日本はこうなる」三菱UFJリサーチ&コンサルティング（2007/11）

2010年-11年頃の情報通信環境における情報セキュリティの脅威・課題

➢情報通信ネットワーク技術の高度化

◆ 電気通信網のIP化（NGN）の普及とインターネットとの並存

•サーバー等の攻撃ではなく、ネットワークに接続した携帯電話や情報家電等の機器が直接的な攻撃の対象となる。

•利用者関連の情報が集約するサービス・ストラタムが攻撃の対象となる。

•NGNの伝送プロトコルに関連する脅威が発生する可能性がある。（回線の乗っ取り、不正転送、盗聴、タダ掛けなど。実装レベルでの不具合。）

•NNI・UNI・SNI等を通じて複数の電気通信事業者やアプリケーションサービス、利用者端末（利用者自身）が連携する際に、成りすまし等が発生する可能性がある。

•NGNになっても、現状発生しているインターネット上のセキュリティ問題（スピア攻撃やウイルス感染等）が減少、消滅せず、脅威は継続・高度化していく。

•NGNにおけるサービスのオープン化・水平連携型の促進による関係事業者の増加により、インシデント対応が複雑化する。

◆ IPv6の利用促進（IPv4との共存）

- IPv6化によりNAT／プロキシがなくなることで、内部ネットワークや端末・アプリケーションが直接攻撃にさらされる可能性がある。
- グローバルIPアドレスが固定化されるため、行動分析が容易になると共に、特定アドレスへの継続的な攻撃が可能になる。
- IPv4上でIPv6のトンネルリングの利用や、不正にIPSecが利用されることで、FW、IDS等が機能せず、適切な管理が出来ない状況の下で、ウイルス感染等が進む可能性がある。
- IPv6対応ルータの自動アドレッシング、ルータ発見機能により、任意のルータを新設することにより、既設ルータのアドレス設定やルーティングが強制的に変更させられる恐れがある。
- マルチキャスト通信を介した無差別攻撃の可能性がある。
- 現在でも生じているTCP/IPの脆弱性に関連する攻撃事象が、IPv6でも継続して生じる場合がある。（SYN Flood攻撃、ICMP Echoリクエスト等）
- IDS等のセキュリティ機器のIPv6対応への遅れが懸念される。
- IPv4とIPv6の混在するネットワークが利用されることにより、運用管理上の負担が増加する

◆ 次世代無線システム等無線アクセスの多様化

◆ 第4世代移動通信システムの実現

- 利用者数・端末数の増加により、利用者への攻撃が増加する。
- OSやアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する。
- 携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報をターゲットにした盗聴、不正アクセス、改ざんなどの攻撃の増加する可能性が高い。
- 無線通信技術の脆弱性をつく攻撃、端末の盗難・紛失等による被害が拡大する。
- 無線基地局やアンテナへの物理的な盗聴や不正アクセス、破壊などの脅威が増加する。
- 携帯端末等に対して、PC端末と同等のセキュリティ対策が実装できるか、課題。

◆家電のネットワーク化（情報家電）・高機能なロボットの普及

- 様々な情報家電機器やサービスが普及することで、ITの知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者をターゲットにしたソーシャルエンジニアリング攻撃が増加する。
- OSやアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する。
- 情報家電等を通じて流通する個人情報や機密情報の量が増えると想定され、当該情報をターゲットにした盗聴、不正アクセス、改ざんなどの攻撃が増加する可能性が高い。
- サイバー攻撃の踏み台化や、家電製品を誤動作させることにより人命に影響を及ぼすような攻撃に発展する可能性がある。
- 家電製品のライフサイクルに対応した情報セキュリティ対策が確立されていない。（売切り、長期間利用、転売・破棄）

◆ FMC、FMBC（固定通信、移動通信、放送の融合）サービスの台頭

•携帯電話・固定電話の複数端末を跨って、個人情報や機密情報が流通するケースが増大し、当該情報の盗聴、不正アクセス、改ざんなどの攻撃が増加する。

•ウイルスが埋め込まれた不正なコンテンツがブロードキャストされる可能性や、放送局への成りすましによる偽造コンテンツの送信等が発生する可能性が生じる。

◆ P2P等、オーバーレイネットワークの利用拡大

•一定の利用者やサービスなどで閉じた仮想ネットワークを構成することで、ビジネス上の利点がある一方、嗜好が近く、ソーシャルエンジニアリングによる攻撃がし易くなる可能性や、管理者不在の有害ネットワークとして、構成される可能性がある。

◆ 暗号技術の危殆化

•危殆化した暗号を利用したシステムやサービスにより、盗聴、不正アクセス、改ざんなどの攻撃が生じる可能性がある。

➢スマートフォン等、携帯電話の高機能化によるモバイル利用環境の進展

- ◆ OS、アプリケーションのオープン化、APIの公開
- ◆ 携帯端末等を利用して、ホームネットワークに繋がった情報家電を制御
- ◆ 携帯端末による認証・電子決済
- ◆ GPSの標準搭載により、位置情報利用の拡大

•利用者数・端末数の増加により、利用者への攻撃が増加する。

•OSやアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する。

•携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報をターゲットにした盗聴、不正アクセス、改ざんなどの攻撃の増加する可能性が高い。

•サイバー攻撃の踏み台化や、家電製品を誤動作させることにより人命に影響を及ぼすような攻撃に発展する可能性がある。

•様々な情報家電機器やサービスが普及することで、ITの知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者をターゲットにしたソーシャルエンジニアリング攻撃が増加する。

•携帯端末に対して、PC端末と同等のセキュリティ対策が実装できるか、課題。

➢ネットワークを流通するデータ量、ネットワークと接続するデバイス数の爆発的増加

◆ インターネット利用者数の増加

•様々な情報家電機器やサービスが普及することで、ITの知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者をターゲットにしたソーシャルエンジニアリング攻撃が増加する。

•利用者の増加に伴い、各種サービスの入り口となるWebブラウザの脆弱性をつく攻撃の影響範囲が拡大する可能性がある。

◆ 携帯電話端末、PDA、ゲーム端末等、non-PCによるインターネット利用の増加

•利用者数・端末数の増加により、利用者への攻撃が増加する。

•OSやアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する。

•携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報をターゲットにした盗聴、不正アクセス、改ざんなどの攻撃の増加する可能性が高い。

•携帯端末等に対して、PC端末と同等のセキュリティ対策が実装できるか、課題。

◆ Blog、SNSなどのCGM（Consumer Generated Media）の増加

•インターネットの利用形態や消費活動への影響が大きい反面、情報セキュリティ意識が必ずしも高くない情報発信者の増加による意図しない個人情報の漏えいが増加する。

•事故を装った意図的な個人情報の漏えい・プライバシーの侵害が発生する可能性がある。

◆ 大容量マルチメディアコンテンツの流通拡大

•情報セキュリティ意識が必ずしも高くない情報発信者の増加による意図しない個人情報の漏えいが増加する。

•（一部の利用者により）大量のメディアコンテンツが流通することにより、ネットワーク設備への影響が懸念される。

◆ 情報家電、RFIDの利用拡大（運輸、卸売・小売、医療・福祉、製造、等）

•情報家電、RFID等で利用される個人情報、機密情報の流通量が増えると想定され、当該情報をターゲットにした情報漏えい、改ざんなどの攻撃の増加する可能性が高い。

•ICカード、読み取り装置との間での通信データの盗聴・改ざんなどが発生する可能性がある。

➢消費活動等の変化

- ◆ 非接触ICカードの普及による電子マネーの利用拡大（携帯機能の高度化）
- ◆ こだわり型の消費活動の増大（口コミ情報や価格比較の利用、書込み）
- ◆ RFIDによるリアルタイムの商品管理
- ◆ 商品情報・顧客情報の増大と営業戦略の変化

•流通する個人情報や機密情報の量が増えると想定され、当該情報をターゲットにした情報漏えい、改ざんなどの攻撃の増加する可能性が高い。

•様々なネットワーク機器やサービスが普及することで、ITの知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者をターゲットにしたソーシャルエンジニアリング攻撃が増加する。

◆仮想世界の普及

•仮想世界の通貨等をターゲットにした情報漏えい、改ざんなどの攻撃が増加する可能性が高い。

➢中小企業でのICT利用による生産性向上

•ネットワークを介して提供される設備やサービスを利用する場合などでは、当該サービスの提供者の設備に障害が発生した場合に被害の範囲が広範になることから、こうした設備等を意図的に攻撃する可能性が高くなる。

•外部に集約される企業情報等をターゲットにした情報漏えいや改ざん等の攻撃が増加する可能性がある。

環境変化により、今後顕在化が予想される情報セキュリティの主な脅威と課題（まとめ）（案）

2010年-11年頃の、いつでも、どこでも、何でも、誰でもネットワークに簡単につながり、利用できる「ユビキタスネット社会」における情報セキュリティの主な脅威と課題は、次の項目にまとめられるのではないか。

- 脅威の対象となる範囲の拡大（物、人）
  - ネットワークに接続される機器・デバイスが爆発的に増大し、脅威の対象範囲が拡大
  - OS、ｱﾌﾟﾘｹｰｼｮﾝの共通化により、１つの脆弱性が及ぼす対象範囲が拡大
  - インターネット利用の進展により、情報セキュリティに関する意識や知識が必ずしも高くない利用者が増加
  - 情報の保持、管理する場所・主体の変化

- 脅威の対象となる情報の増加
  - ビジネスモデルや利用形態の変化に伴い、決済情報、認証情報、位置情報等の個人情報や企業情報が、ネットワークを流通する機会が増大
  - 仮想世界の通貨等、新しい価値ある情報の流通が増加

- 対策の困難性の拡大
  - 情報通信技術の進展や、利用形態・ビジネスモデルの恒常的な変化により、将来の脅威予測が非常に難しい
  - ネットワークに接続される端末・デバイスや情報量の爆発的な増大、利用する個人の増加、及び業界を越えて機器製造業者、電気通信事業者、サービス提供事業者等の多くの関係者が複雑に関連し合うと想定される環境において、情報セキュリティを検討するに当たっての参照モデルが確立されていない
  - ソーシャルエンジニアリングを駆使した対象範囲を絞った攻撃が進行するなど、ウイルス感染や意図的に情報漏えいを引き起こす手法が高度化・潜行化してきている
  - 情報セキュリティ対策の主体、責任範囲が不明確
  - 情報セキュリティに関する事案が発生した場合に、迅速かつ効果的な対策を実施するための（国内外の情報共有・連携を含む）体制が確立されていない