資料36－5

IoT機器のセキュリティ対策について

2018年3月6日

一般社団法人 情報通信ネットワーク産業協会

2017年度 CIAJの概要

情報通信技術(ICT)活用の一層の促進により、情報通信ネットワークに係る産業の健全な発展をはかるとともに、情報利用の拡大・高度化に寄与することによって、社会的、経済的、文化的に豊かな国民生活の実現および国際社会の実現に貢献することを活動の目的としています。

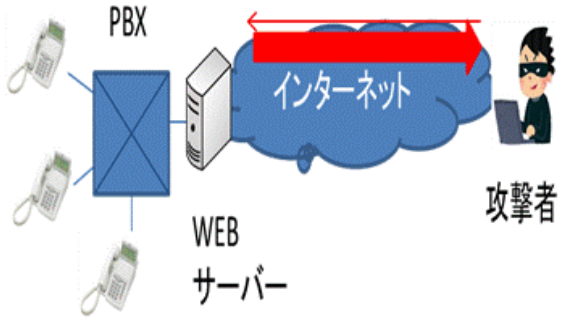
通信ネットワーク・端末機器等の供給事業者が正会員として、通信事業者やサービス・プロバイダー、ユーザー企業等がフォーラム会員として加盟し、ICT産業の活性化につながる政策提言・意見発信、ICT利活用の推進による新たなビジネス創出の推進、グローバルビジネスの推進、業界共通諸課題の解決に取り組んでいます。

正会員:101社　フォーラム会員:44社　賛助会員:54社
(2018年2月現在)

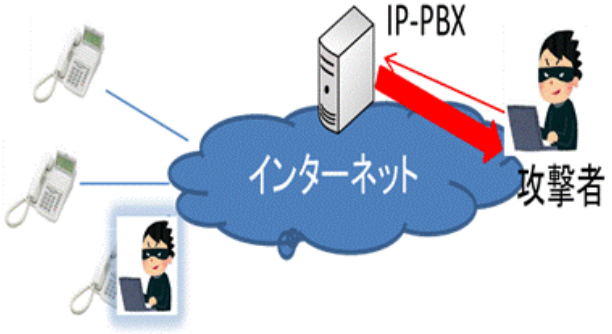
事例1: VoIPシステムにおけるセキュリティ脅威

- パスワードなど「端末情報の漏洩」により、通信内容が「盗聴」されたり、利用者の端末が「なりすまし」を受けて不正に利用され、多額の通信費が請求されるなどが発生。
- VoIPサーバーを「乗っ取り」、正しい利用者が使用できないようにするなどの脅威もあり。

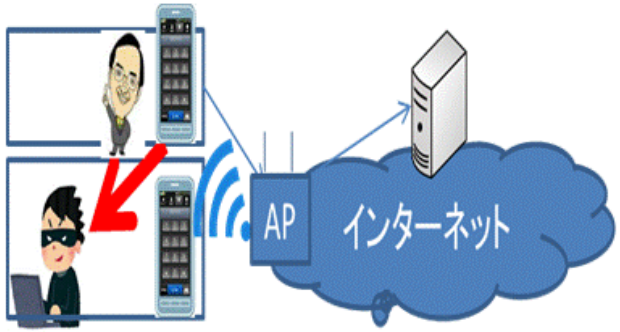
＊事案例：2015年6月12日総務省発表「第三者によるIP電話等の不正利用に関する注意喚起」にて事例報告あり。



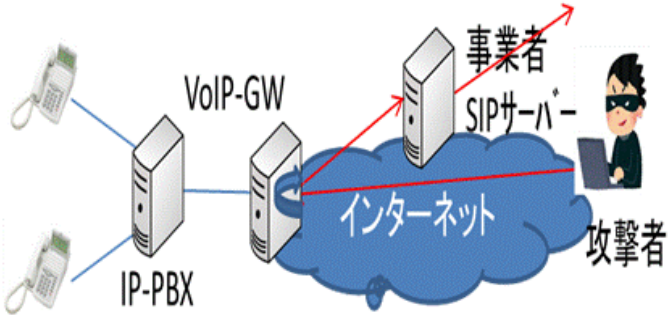
端末情報の漏洩



なりすまし



盗聴



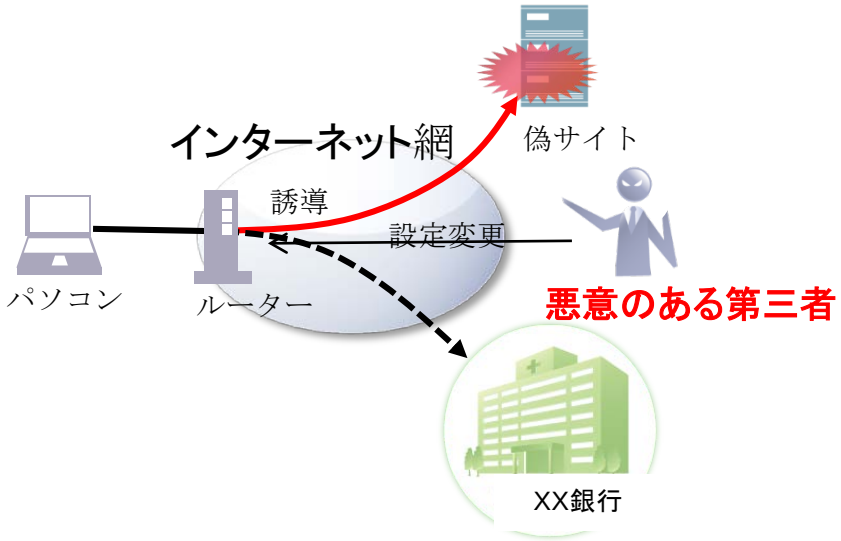
乗っ取り

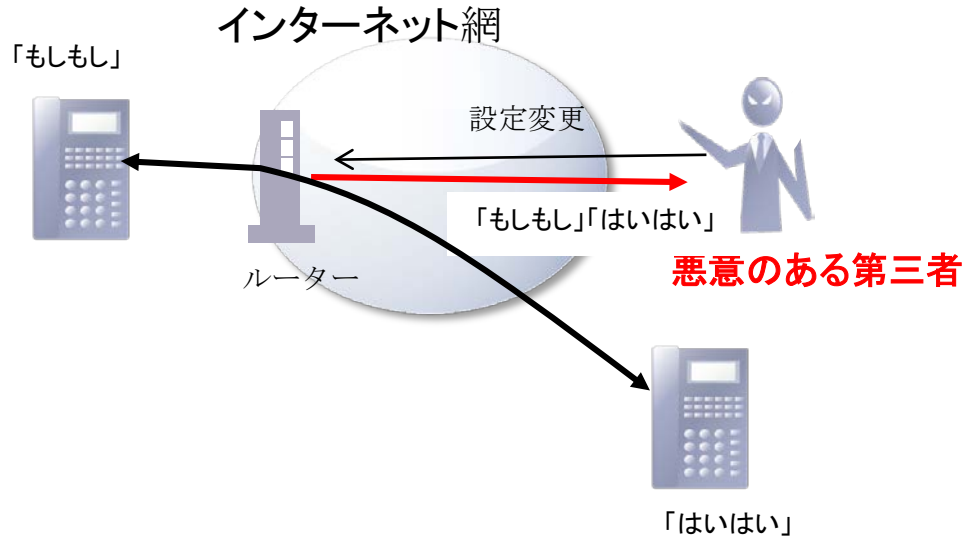
事例2: ルーターにおけるセキュリティ脅威

外部からの不正アクセスによる悪意のルーター設定変更により、下記のようなセキュリティ事故が発生。

- ◆ 偽ウェブサイトへの誘導（IDやパスワード、個人情報等の搾取）。
- ◆ インターネットとの通信内容の傍受、改竄等

＊事案例：2015年6月12日総務省発表「無線LANルータの不正利用に関する注意喚起」にて事例報告あり。





IoT機器に関するサイバーセキュリティ上の課題

事例3: IPカメラにおけるセキュリティ脅威

- ◆ 不適切なパスワード設定やセキュリティ脆弱性のあるIPカメラが、不正アクセスにより乗っ取られ、外部から不正な操作をされたり、映像情報がインターネット上で公開されてしまう事例が発生している。
- ◆ 後述ボットウィルスに感染させられ、DDoS攻撃の足場にされる事例も発生している。

＊事案例：2014年頃より、海外サイトにて、不正アクセスされた多数のIPカメラ映像が公開されている事例が発生。
2016年頃より、特定メーカ製品で家庭内設置IPカメラの不正操作事例が多数発生

事例4: 複合機におけるセキュリティ脅威

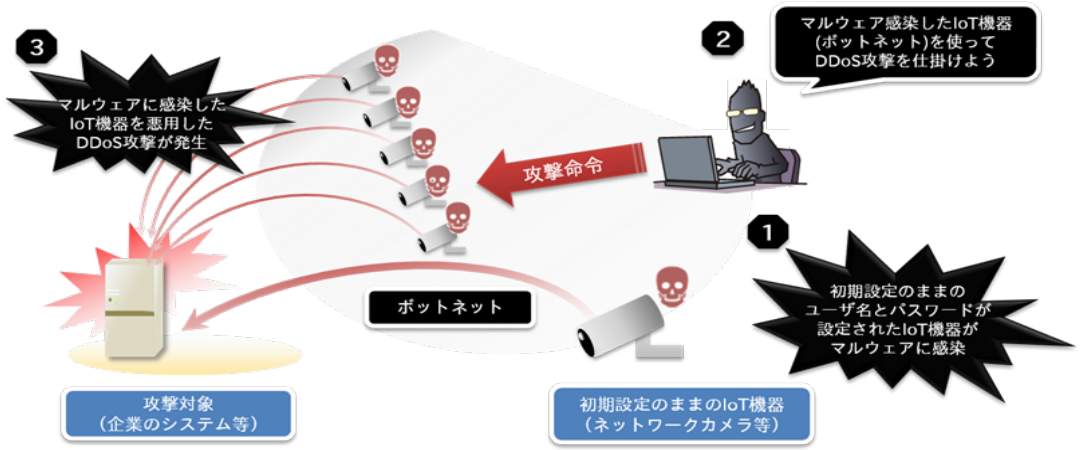
- ◆ 遠隔からの管理や操作を実施可能とするために、簡易なWebサーバ機能を搭載している複合機などが、適切なセキュリティ設定がなされていない状態で、外部から直接アクセス可能なネットワークに接続されたため、機器内に保管されている機密情報が外部から読み取られる等の被害が発生。
- ◆ 複合機以外にも、テレビ会議システム、IP電話機などの機器に同様のリスクあり。

＊事案例：2013年11月頃、複数の大学等で、複合機で読み取った情報がインターネット上で閲覧できる状態になっていたことが判明。

事例5: ボットウイルスによるIoT機器のセキュリティ脅威

- IPカメラやDVRなどのIoT機器については、適切なパスワード設定などのセキュリティ対策が不十分になり勝ち。知らないうちにボットウイルスに感染させられている機器が多数存在。
- ボットウイルスに感染した機器は、外部からの操作が可能となり、ある時、特定サイトに対するDDoS攻撃等実施する踏み台（攻撃元）に使用される等、攻撃側に加担してしまうケースあり。

＊事案例：2016年9月頃から急激に観測され始めたボットウイルス「Mirai」による被害が多数発生。



（出展：IPA 安心相談窓口だより第16-13-359号）

課題整理

【背景】

- IoTの進展により、ネットワークに接続される機器は多様化しており、従来のPC/サーバに比し、セキュリティ脆弱性のある機器が増加している。これにより、下記のようなセキュリティ脅威が拡大。
  - 不正アクセスによる情報漏洩、不正操作
  - ボット感染により、DDoS攻撃の足場とされる

【課題】

セキュリティ脆弱性のあるIoT機器を使用させないための対策が必要

【解決策骨子】

以下のような機能の実装が考えられる。

① 不正アクセスを防ぐ認証機能の実装
② セキュリティホール検出時の対処機能の実装

※ 上述の機器仕様による対策に加えて、運用時における対策（適切なパスワードの使用促進等）も重要。

機器仕様としてのセキュリティ脆弱性対策

以下に、IoT機器のセキュリティ脆弱性対策機能例を示します。
（CIAJ会員企業の製品すべてにおいて実装できている確認が取れている訳ではありません。）

(1) IP-PBX、ボタン電話

・設定管理インターフェースへのアクセスに対するID・パスワードの設定・変更機能
・ファームウェアのアップデートが可能
・デバッグ用ポートは閉じる
・「ログ」、「通話履歴」情報の提供

(2) ルータ

・設定管理インターフェースへのアクセスに対するID・パスワードの設定・変更機能
・ファームウェアのアップデートが可能
・「ログ」情報の提供

（特に、家庭向けルータの場合）
・工場出荷時パスワードの強制変更 あるいは ユニークな工場出荷時パスワード
・ファームウェアの自動アップデートが可能（ユーザー設定による）

機器仕様としてのセキュリティ脆弱性対策（続き）

(3) IPカメラ

・設定管理インターフェースへのアクセスに対するID・パスワードの設定・変更機能
・デバッグ用ポートは閉じる

(4) FAX、コピー複合機

・設定管理インターフェースへのアクセスに対するID・パスワードの設定・変更機能
・デバッグ用ポートは閉じる
・「ログ」情報の提供

＊尚、Office向け複合機では、一般にCC認証[*1]を取得している。

*CC認証：Common Criteria認証（ISO/IEC 15408）

＊補足コメント

- ID・パスワードによるアクセス認証機能としては、初期値からの設定変更強制（変更しなければ動作しない）機能や、パスワード桁数・使用文字種等の制約条件を課す機能等も考えられる（実装例もあり）が、パスワード強度等に関する国際的なコンセンサス/基準は未確立。
- セキュリティホール検出時に備えて、ファームウェアをアップデートする機能を有する機器も多いが、本機能自身がセキュリティホールになる可能性も指摘されている。

今後の取組みについて（意見・要望）

- IoT機器に関するセキュリティ対策機能として何らかの機能仕様の基準を設けることは、粗悪な製品が使用されないようにする意味から有効と考える。

- しかしながら、IoT機器市場の健全な発展の阻害要因とならないよう、費用対効果最大化を含む産業の国際競争力強化の観点から、下記の点に留意する必要がある。

  ① IoT機器ベンダにとって、グローバル市場への展開、競争力確保が重要。国内向け、海外向け製品の仕様を統一できるようグローバル市場で認められる国際標準への準拠を目指すべき。

  ② 機能仕様の基準を設けることと、第三者による認証要否は別次元の話と考える。専門の第三者による仕様確認/評価を必要とする機能以外は、コスト増に繋がる第三者認証はその必要性を十分吟味すべき。

  ③ 特に、準拠すべき国際標準が定まっていない状況下においては、将来、国際標準準拠に移行できるよう、指針/ガイドラインに沿った自主規制、ベンダによる自己適合宣言のユーザ周知を基本とすることが望ましい。

- 何らかの基準を設ける場合、類似の機能を有する他種の機器仕様にも広く影響がおよぶものと考える。関連各分野の意見を十分に聴取し、協議・検討を進めるべき。