資料５－４

IoT機器のセキュリティ対策について

2017年12月11日

一般社団法人 情報通信ネットワーク産業協会
通信ネットワーク機器セキュリティ分科会

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。

主要会員　沖電気工業(株)　日本電気(株)　富士通(株)
三菱電機(株)　(株)日立製作所　(株)東芝

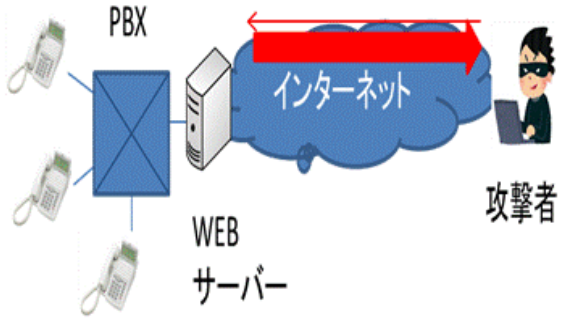
会長　　川崎　秀一（沖電気工業㈱代表取締役会長）

正会員:101社　　フォーラム会員:45社　　賛助会員:54社
（2017年8月現在）

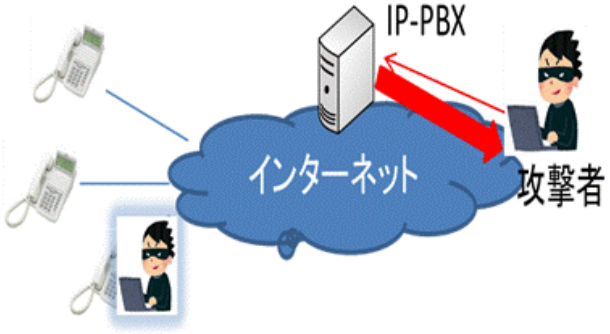
事例1: VoIPシステムにおけるセキュリティ脅威

- 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。

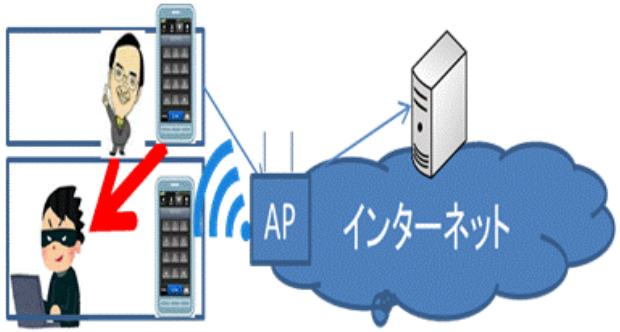
＊事案例：2015年6月12日総務省発表「第三者によるIP電話等の不正利用に関する注意喚起」にて事例報告あり。



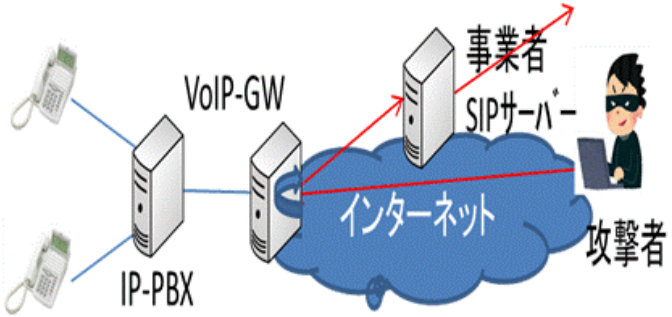
端末情報の漏洩



なりすまし



盗聴



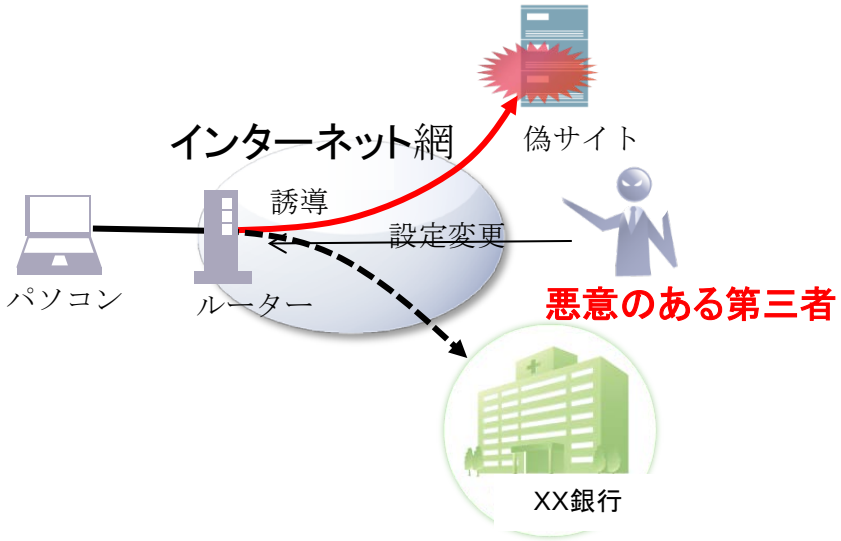
乗っ取り

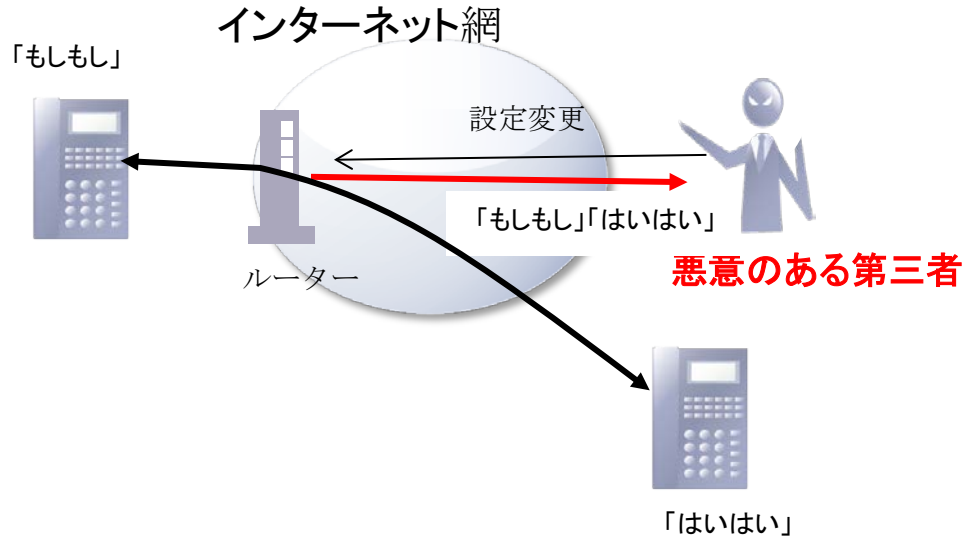
事例2: ルーターにおけるセキュリティ脅威

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: 複合機におけるセキュリティ脅威

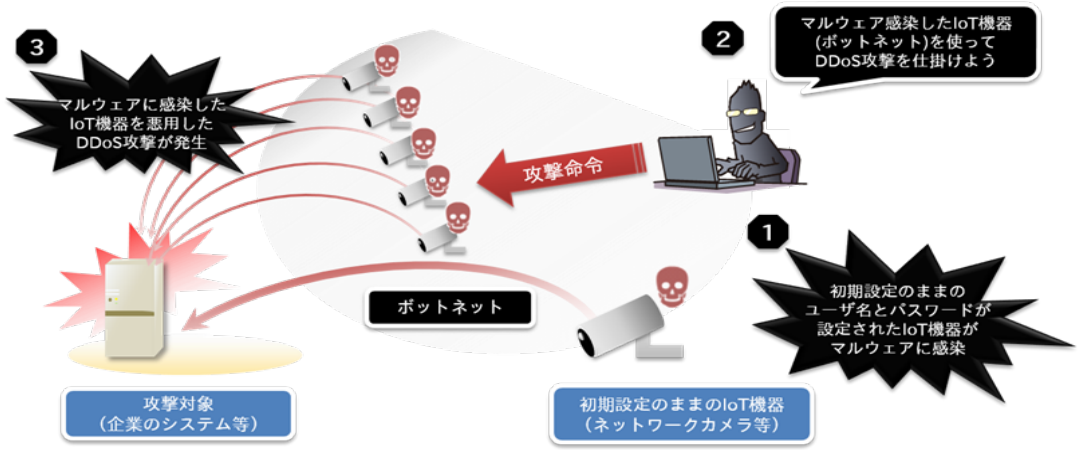
- 遠隔からの管理・保守等を実施可能とするために、簡易なWebサーバ機能を搭載している複合機などが外部から直接アクセス可能なネットワークに接続されていた場合に、外部からの不正なアクセスにより、機密情報を読み取られる等の被害が発生する場合あり。
- 複合機以外にも、Webカメラ、テレビ会議システム、IP電話機などの機器に同様のリスクあり。

＊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4: ボットウイルスによるIoT機器のセキュリティ脅威

- Web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）

IoT機器が採るべきセキュリティ対策

以下では、今後、各種IoT機器が採るべきセキュリティ対策について記述します。

考え方

- まず、何を守るのか、どのような脅威があるのかを分析・定義する。

  例）企業や官公庁　　機密情報、提供サービス
  個人　　プライバシー、財産
  通信事業者　　**機器の大量感染による影響、予期せぬ伝送帯域の占有**

- 上記の具体的対策/手段を国際標準の規程に沿って、実装する。

  参考となる国際標準の例

  ISO/IEC15408：

  - セキュリティ製品（ハード/ソフトウェア）およびシステムの開発や製造、運用などに関する国際標準であり、情報セキュリティ評価基準として、1999年6月に採択された。ITSEC（Information Technology Security Evaluation Criteria）やCC（Common Criteria）とも呼ばれる。
  - CCでは、様々なセキュリティ機能要件が規定されており、保護資産と脅威に応じて機能要件の選択を行う（プロテクションプロファイル）。
  - ただし、CCは認証を受けるための手続きが煩雑であること、また、プロテクションプロファイルによっては必要なリソース量も多く、Webカメラ等、比較的簡易なIoT機器については、必ずしも適さない。早期に、適切な国際標準の策定が必要。

IoT機器が採るべきセキュリティ対策

国際標準化を目指した活動

(1) IoT高信頼化要件

IoT高信頼化要件		IoT高信頼化を実現するための機能要件	対応IoT高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	初期設定が適切に行われ、その確認ができる	1、2
		サービスを利用する時に許可されていることを確認できる	3、4
予防	稼働中の異常発生を未然に防止できる	異常の予兆を把握できる	5、6、7、8、9
		守るべき機能・資産を保護できる	4、5、6、10
		異常発生に備えて事前に対処できる	11
検知	稼働中の異常発生を早期に検知できる	異常発生を監視・通知できる	12、13
		異常の原因を特定するためのログが取得できる	5、6
回復	異常が発生しても稼働の維持や早期の復旧ができる	構成の把握ができる	14
		異常が発生しても稼働の維持ができる	8、15、16、17
		異常から早期復旧ができる	11、18、19、20
終了	利用の終了やシステム・サービス終了後も安全安心が確保できる	自律的な終了や一時的な利用禁止ができる	18、21、22
		データ消去ができる	23

(2) IoT高信頼化機能

IoT高信頼化機能					
1	初期設定機能	9	ウイルス対策機能	17	冗長構成機能
2	設定情報確認機能	10	暗号化機能	18	停止機能
3	認証機能	11	リモートアップデート機能	19	復旧機能
4	アクセス制御機能	12	監視機能	20	障害情報管理機能
5	ログ収集機能	13	状態可視化機能	21	操作保護機能
6	時刻同期機能	14	構成情報管理機能	22	寿命管理機能
7	予兆機能	15	隔離機能	23	消去機能
8	診断機能	16	縮退機能		

出典：IPA「つながる世界の開発指針」の実践に向けた手引き [IoT高信頼化機能編]より

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防御機能として何らかの基準を設けることは、粗悪な製品を排除する意味から有効と考える。

- しかしながら、その際、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、以下の点につき、注意が必要。

  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ベンダによる自主規制、自己適合宣言による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。