IPA Better Life with IT

ET & IoT Technology 2018
IPA ブースプレゼンテーション

多様化するIoTのセキュリティ脅威とその対策

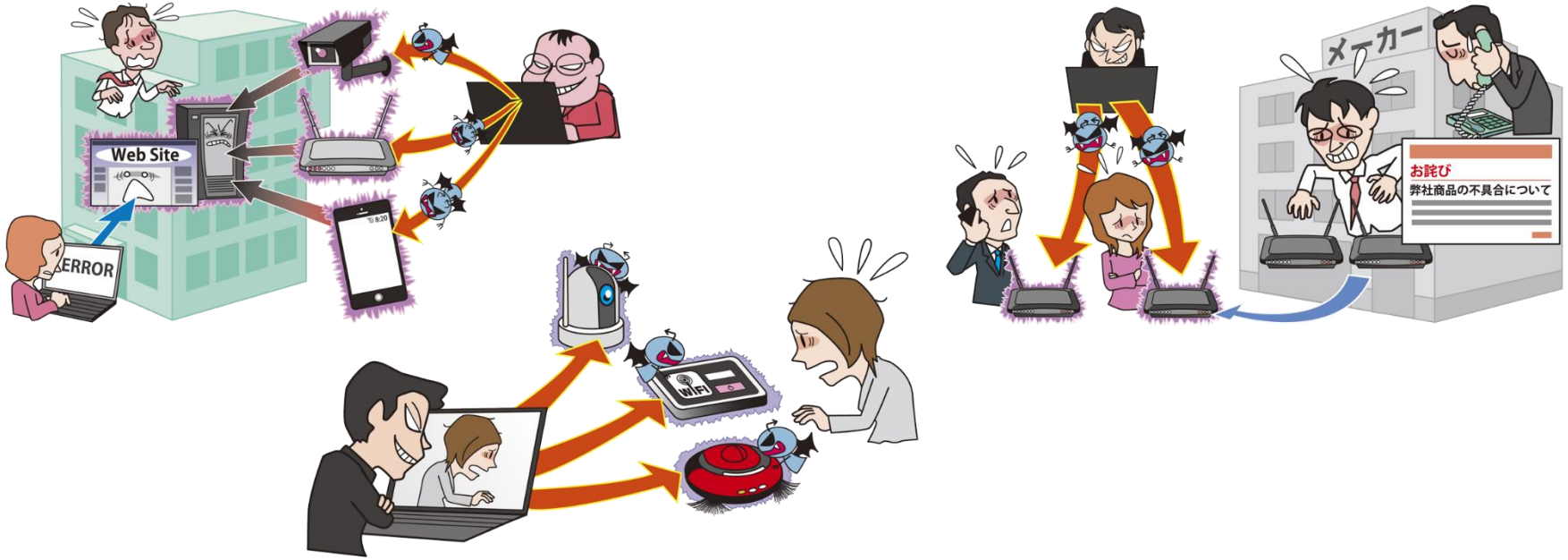
～セキュリティ・バイ・デザインと脆弱性対策の重要性～

2018年11月14日（水） 15:00-15:20
2018年11月16日（金） 15:30-15:50

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
セキュリティ対策推進部
博士（工学）　辻 宏郷

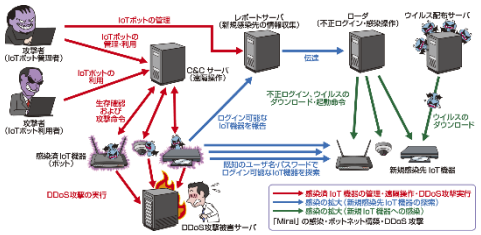
第一部　多様化するIoTのセキュリティ脅威

- 「Mirai」の出現
- IoT機器に感染するウイルスの多様化
- 脆弱性を有するIoT機器の散在、国内に広がる感染被害



多様化するIoTのセキュリティ脅威
「Mirai」の出現（1/2）大規模DDoS攻撃の脅威

- 2016年9月： セキュリティ専門家ブログ “Krebs on Security”
  - ウイルス「Mirai」に感染したIoT機器で構成されたボットネット
  - 約620GbpsのDDoS攻撃
- 2016年9月： フランスのホスティングサービス OVH
  - 14万5千台以上のIoT機器からDDoS攻撃
  - ピーク時に1Tbpsを超える攻撃トラフィックを観測
- 2016年9月末: 「Mirai」のソースコード公開
- 2016年10月： DNSサービス提供会社 Dyn
  - Twitter, SoundCloud, Spotify, Reddit 等に影響
- 2016年11月： ドイツのISP Deutsche Telekom
  - 顧客に配布したルータに対する感染攻撃（「Mirai」の亜種）
  - 4～5%が利用不能となり、90万ユーザに影響、被害総額：約200万€



「Mirai」の詳細については、2017年3月公開の「情報セキュリティ10大脅威 2017」3章をご覧ください。

https://www.ipa.go.jp/security/vuln/10threats2017.html

多様化するIoTのセキュリティ脅威
「Mirai」の出現（2/2）感染理由とその対策

- ポート番号23または2323でtelnetが動作していた。
  - IoT機器を利用している間、動作している必要があるか否か不明。
  - 無効化する管理インタフェースが存在しないIoT機器があった。
  - 一部機器では、telnetの動作は利用者に非公開の「バックドア」状態。

☞ 製品出荷後に不要となる管理機能は、無効化した上で出荷する。
製品出荷後も一部必要となる管理機能は、無効化手段を提供し、説明書等に明記して、利用者に周知徹底する。

- ユーザ名、パスワードが初期値のまま動作していた。
  - IoT機器の利用開始前に、ユーザが変更していなかった。
  - パスワードがハードコーディングされており、ユーザが変更不可の機器も。
  - 一部機器では、ユーザ名やパスワードの存在が利用者に隠蔽。

☞ 初期パスワードを変更可能とし、セキュアなパスワードに変更すべきであると説明書等に明記して、利用者に周知徹底する。

「Mirai」の詳細については、2017年3月公開の「情報セキュリティ10大脅威 2017」3章をご覧ください。

https://www.ipa.go.jp/security/vuln/10threats2017.html

多様化するIoTのセキュリティ脅威
IoTに感染するウイルスの多様化（1/5）

- IoT機器のMirai等の感染に対抗する「Hajime」
  - 2016年10月、Mirai解析用ハニーポットが初めて検出
  - 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - 感染後、ポート番号23, 5358, 5555, 7547の通信を遮断し、結果的に「Mirai」やその亜種の感染を防止
  - 攻撃の踏み台とせず、作成者の善意（?）の警告メッセージを表示
  - P2P通信を用いて遠隔操作
    （特定のC&Cサーバが存在しないため、ボットネットの解体困難）
  - 高度な隠密性（感染機器のファイルシステムから自身を削除、実行中プロセスリストからプロセス名を書き換えて自身の存在を隠蔽）
  - 2017年4月、感染手段の拡張（TR-064の脆弱性を悪用）
  - 2017年9月、感染手段の更なる拡張（ポート番号5358のtelnet）
  - 感染機器台数の増減はあるものの、依然としてボットネットを形成

多様化するIoTのセキュリティ脅威
IoTに感染するウイルスの多様化（2/5）

- IoT機器を破壊する「BrickerBot」
  - 第三者へのDDoS攻撃に悪用せず、IoT機器の利用者に直接被害を与えるウイルス
  - 2017年3月、ハニーポットが初めて検出
  - 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - 感染後、設定変更、インターネット接続妨害、動作速度低下、機器上のファイル消去等の致命的な改変を行い、最終的に使用不能に
    → 結果的に、「Mirai」やその亜種の感染を防止
  - 2017年4月、米国Sierra Telが顧客に配布したモデムを攻撃。インターネット接続機能や電話接続機能が失われ、修理・交換に
  - 2017年7月、インドBSNL社及びMTNL社が顧客に配布したモデムやルータを攻撃。BSNL社の6万台、全顧客の45%の接続に影響
  - 2017年12月、作者「Janit0r」は、「インターネット化学療法」プロジェクトの終了を宣言。1,000万台以上のIoT機器を攻撃してきたが、引退すると表明

多様化するIoTのセキュリティ脅威
IoTに感染するウイルスの多様化（3/5）

- 続々と登場する「Mirai」の亜種
  - 特定のIoT機器固有の脆弱性を突いて感染、初期パスワードから変更しても防御不能
  - PERSIRAI
    - 2017年4月発見
    - ポート番号81で管理画面にアクセス可能なOEM生産のIPカメラに感染
    - IPカメラ侵入後、3種類の既知の脆弱性（CVE-2017-5674他）を突いて、他のIPカメラを攻撃
  - Reaper (IoTroop, IoT reaper)
    - 2017年10月発見
    - 様々なカメラやルータ等が持つ、機種固有の脆弱性を突いて感染
  - Satori／Okiru
    - 2017年12月報告
    - ポート番号52869経由でネットワークコントローラチップ用SDKの脆弱性（CVE-2014-8361）、または、ポート番号37215経由でホームルータの未知の脆弱性（CVE-2017-17215）を突いて感染

多様化するIoTのセキュリティ脅威
IoTに感染するウイルスの多様化（4/5）

- 「Reaper」が感染拡大に悪用する脆弱性

	ベンダ名	脆弱性
1	D-Link	D-Link DIR-600/DIR-300(rev B)ルータにおける複数の脆弱性
2	GoAhead 及び各OEM	Wireless IP Camera (P2P) WIFICAMにおける複数の脆弱性 (CVE-2017-8225他)
3	NETGEAR	NETGEAR ReadyNASにおける非認証のリモートコマンド実行の脆弱性
4	VACRON	VACRON NVRにおけるリモートコマンド実行の脆弱性
5	D-Link	D-Link 850Lルータにおける複数の脆弱性
6	Linksys	Linksys E1500/E2500ルータにおける複数の脆弱性
7	NETGEAR	NETGEAR DGN1000/2200 v1ルータにおける非認証のコマンド実行の脆弱性
8	AVTECH	AVTECH IPカメラ・DVR・NVRにおける非認証の情報漏えい、認証バイパス等の脆弱性
9	各社	JAWS/1.0のHTTPサーバヘッダを返すカスタムWebサーバにおける非認証リモートコマンド実行の脆弱性

【出典】Radware Ltd. の調査結果
https://blog.radware.com/security/2017/10/iot_reaperbotnet/ をもとに作成

多様化するIoTのセキュリティ脅威
IoTに感染するウイルスの多様化（5/5）

	Miraiの脅威（2016年）	2017年以降に拡大した脅威 （左記に加えて）
攻撃手法	• 設定不備 ✓ 初期パスワードのまま ✓ 不要なプロセスの動作等	• 特定のIoT機器の脆弱性 ✓ 非認証のコマンド実行 ✓ 認証情報の漏えい等
攻撃対象	• 第三者	• IoT機器の利用者自身
被害	• DDoS攻撃によるサービス停止	• 機器設定の無断変更 ✓ 他のウイルス感染から保護 • 機器の使用不能、破壊 • 乗っ取り失敗による機能停止 • 不正操作 ✓ ネットワークカメラの覗き見等

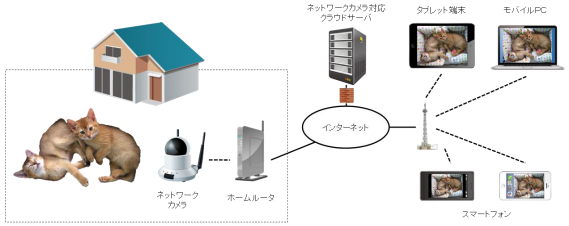
多様化するIoTのセキュリティ脅威
脆弱性を有するIoT機器の散在、国内に広がる感染被害

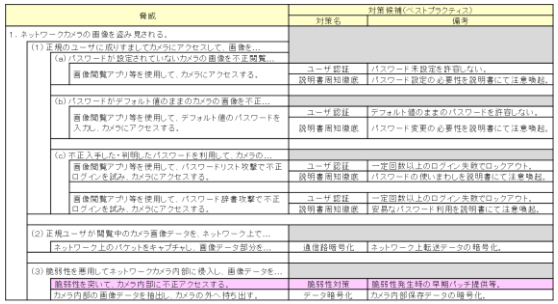
- 脆弱性やバックドアを有するIoT機器の国内での流通
  - 2017年1月、個人宅に設置したネットワークカメラの乗っ取り事件
  - 価格比較サイトで売れ筋ランキング及び注目ランキング1位のカメラの並行輸入品
  - 電子回路基板上プログラムに脆弱性（CVE-2017-8225）が存在し、パスワードを初期値から変更しても、第三者による不正操作が可能
  - 出荷時停止のtelnetを外部から起動可能（バックドア相当機能）

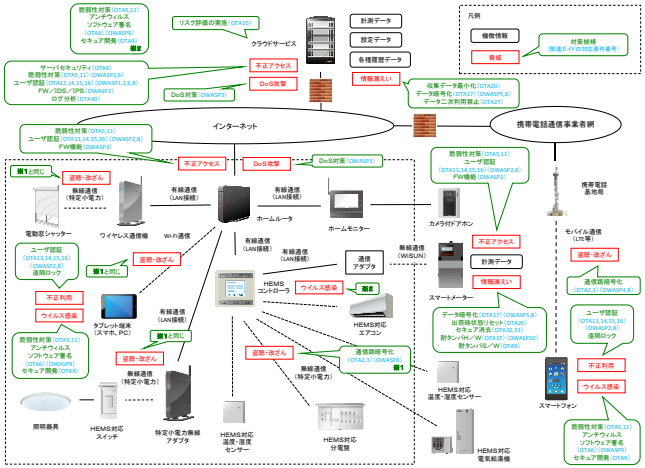
- 国内におけるIoT機器のウイルス感染の急増
  - 2017年11月、Miraiの亜種によるスキャン通信の観測急増
  - 2017年12月、警察庁・NICT・JPCERT/CCから注意喚起
  - Miraiの亜種「Satori／Okiru」の感染拡大と推測
  - 感染機器の多くは、脆弱性（CVE-2014-8361）を有する国内製品の無線LANブロードバンドルータ（2013年6月以降更新F/W提供済）

第二部　IoT製品／サービスの開発者・製造者・提供者の対策
「IoT開発におけるセキュリティ設計の手引き」を題材に

- セキュリティ・バイ・デザイン（設計段階からセキュリティを考慮）
- 脆弱性対策（セキュリティ対策の継続的サポート）







IoT製品／サービスの開発者・製造者・提供者の対策
「IoT開発におけるセキュリティ設計の手引き」を題材に

【セキュリティ・バイ・デザイン】

設計段階からセキュリティを考慮

- システムの全体構成の明確化
- 保護すべき情報・機能・資産の明確化
- 「脅威分析」 保護対象に対する想定脅威の明確化
- 「対策検討」 対策候補の洗い出し、
  脅威・被害・コスト等を考慮した選定

【脆弱性対策】

セキュリティ対策の継続的サポート

- 脆弱性対応
- ソフトウェア更新

「IoT開発におけるセキュリティ設計の手引き」
開発者向けのIoTセキュリティ対策ガイド

【手引きの内容】

- IoTの定義と全体像の整理
- IoTのセキュリティ設計
  - 脅威分析
  - 対策の検討
  - 脆弱性への対応
- 関連セキュリティガイドの紹介
- 具体的な脅威分析・対策検討の実施例
  ①デジタルテレビ、②ヘルスケア機器とクラウドサービス、
  ③スマートハウス、④コネクテッドカー
- IoTセキュリティの根幹を支える暗号技術
- 「つながる世界の開発指針」との対応


IPA Better Life with IT

プレスリリース
2016 年 5 月 12 日
独立行政法人情報処理推進機構

「IoT 開発におけるセキュリティ設計の手引き」を公開
～4 分野の IoT の脅威分析と対策検討の実施例を掲載～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）セキュリティセンターは、今後の IoT の普及に備えて、IoT 機器および、その使用環境で想定されるセキュリティ上の脅威に対し、事業者（開発者）の読んだ参考書であると考え、「IoT 開発におけるセキュリティ設計の手引き」を作成し、本日公開しました。
URL：https://www.ipa.go.jp/security/iot/iotguide.html

近年、IoT [*1] が多くの注目を集めています。現在では IoT と分類されるようになった、組込み機器の情報セキュリティについて、IPA は 2006 年から脅威と対策に関する調査を実施してきました。現在 IoT と呼ばれる機器には、高額から IoT を想定し開発されたものの他に、今後での動作を前提としていた機器に、ネットワーク接続機能が後付けされたものが多く存在すると考えられます。そのため、IoT の企画と利用者の安全な利用のために、ネットワークで接続やサービスが繋がることで生じうる様々な脅威、それらが原因のリスクや被害を予め踏まえておく必要があります。

そこで、IPA では IoT の全体について「サービス提供サーバ・クラウド」「中継機器」「システム」「デバイス」「直接相互通信するデバイス」と 5 つの構成要素に分類し、IPA の IoT モデルを設定しました。その上で、各々の構成要素における課題の抽出・整理を行いました。

図 1　IPA の IoT モデルの全体像

また、今まで蓄積してきた知見を基に、「デジタルテレビ」「ヘルスケア機器とクラウドサービス」「スマートハウス」「コネクテッドカー」の 4 分野を具体的な IoT システムの事例として、脅威分析と対策検討の実施例を掲載しています。この資料では、脅威が想定される箇所と、設計や初号化など

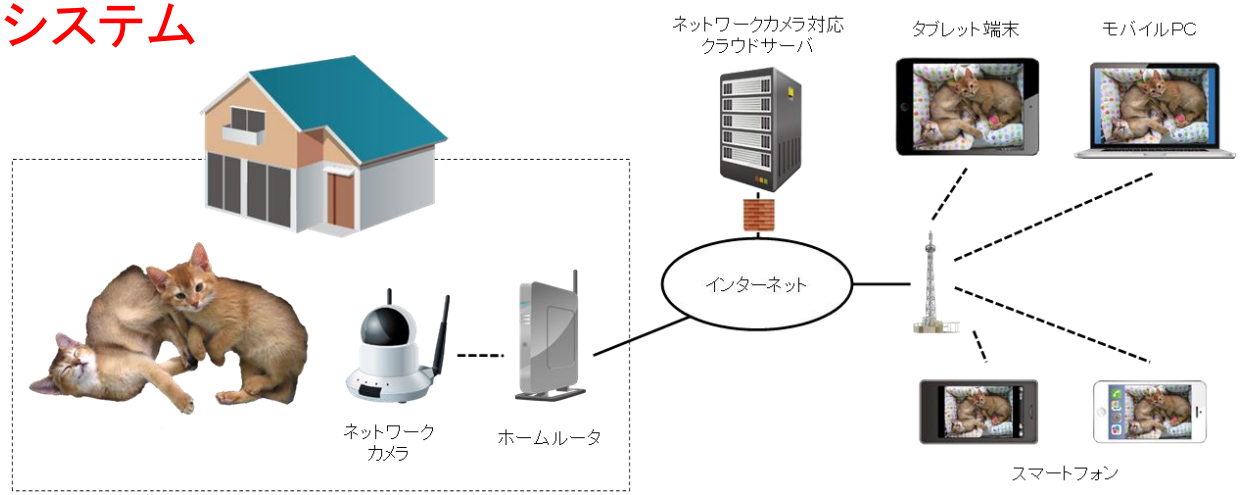
[*1] Internet of Things：モノのインターネット

https://www.ipa.go.jp/security/iot/iotguide.html

IoTのセキュリティ設計
脅威分析と対策検討の実施例（1/2）

防止したい被害を列挙し、それらの被害を生じさせる攻撃シナリオを洗い出し、そのような攻撃を抑止するための対策を検討する。

例：ネットワークカメラシステム



- 防止したい被害の例
  1. ネットワークカメラの画像を盗み見される
  2. ネットワークカメラからの画像を改ざんされる
  3. ネットワークカメラの画像を閲覧できなくなる

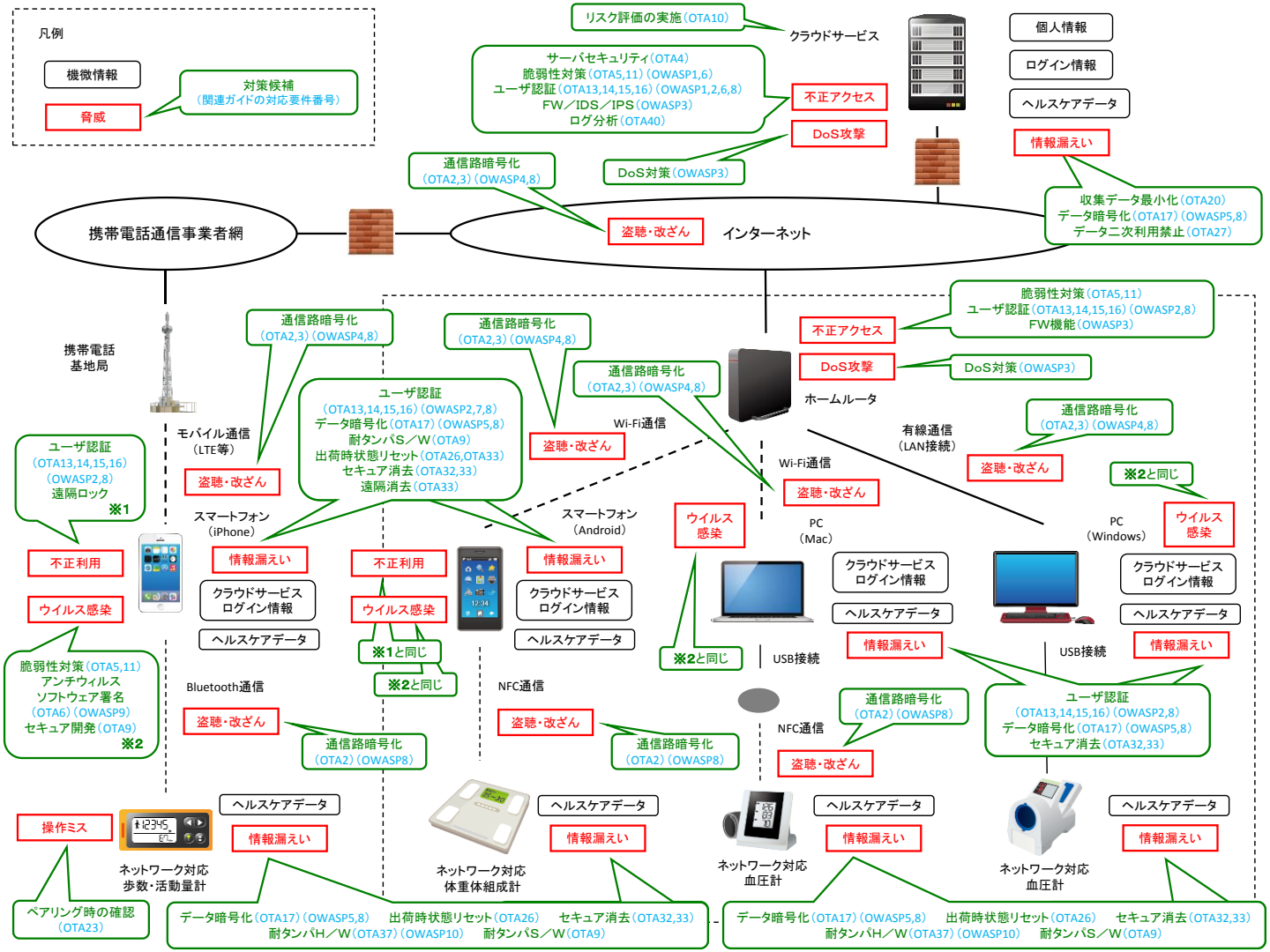
（注）ネットワークカメラとしての機能は正常動作させつつ、第三者への攻撃の踏み台に悪用する攻撃の対策も考慮要。

IoTのセキュリティ設計
脅威分析と対策検討の実施例（2/2）

脅威	対策候補（ベストプラクティス）	
	対策名	備考
1．ネットワークカメラの画像を盗み見される。		
（1）正規のユーザに成りすましてカメラにアクセスして、画像を…		
（a）パスワードが設定されていないカメラの画像を不正閲覧…		
画像閲覧アプリ等を使用して、カメラにアクセスする。	ユーザ認証	パスワード未設定を許容しない。
	説明書周知徹底	パスワード設定の必要性を説明書にて注意喚起。
（b）パスワードがデフォルト値のままのカメラの画像を不正…		
画像閲覧アプリ等を使用して、デフォルト値のパスワードを入力し、カメラにアクセスする。	ユーザ認証	デフォルト値のままのパスワードを許容しない。
	説明書周知徹底	パスワード変更の必要性を説明書にて注意喚起。
（c）不正入手した・判明したパスワードを利用して、カメラの…		
画像閲覧アプリ等を使用して、パスワードリスト攻撃で不正ログインを試み、カメラにアクセスする。	ユーザ認証	一定回数以上のログイン失敗でロックアウト。
	説明書周知徹底	パスワードの使いまわしを説明書にて注意喚起。
画像閲覧アプリ等を使用して、パスワード辞書攻撃で不正ログインを試み、カメラにアクセスする。	ユーザ認証	一定回数以上のログイン失敗でロックアウト。
	説明書周知徹底	安易なパスワード利用を説明書にて注意喚起。
（2）正規ユーザが閲覧中のカメラ画像データを、ネットワーク上で…		
ネットワーク上のパケットをキャプチャし、画像データ部分を…	通信路暗号化	ネットワーク上転送データの暗号化。
（3）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを…		
脆弱性を突いて、カメラ内部に不正アクセスする。	脆弱性対策	脆弱性発生時の早期パッチ提供等。
カメラ内部の画像データを抽出し、カメラの外へ持ち出す。	データ暗号化	カメラ内部保存データの暗号化。

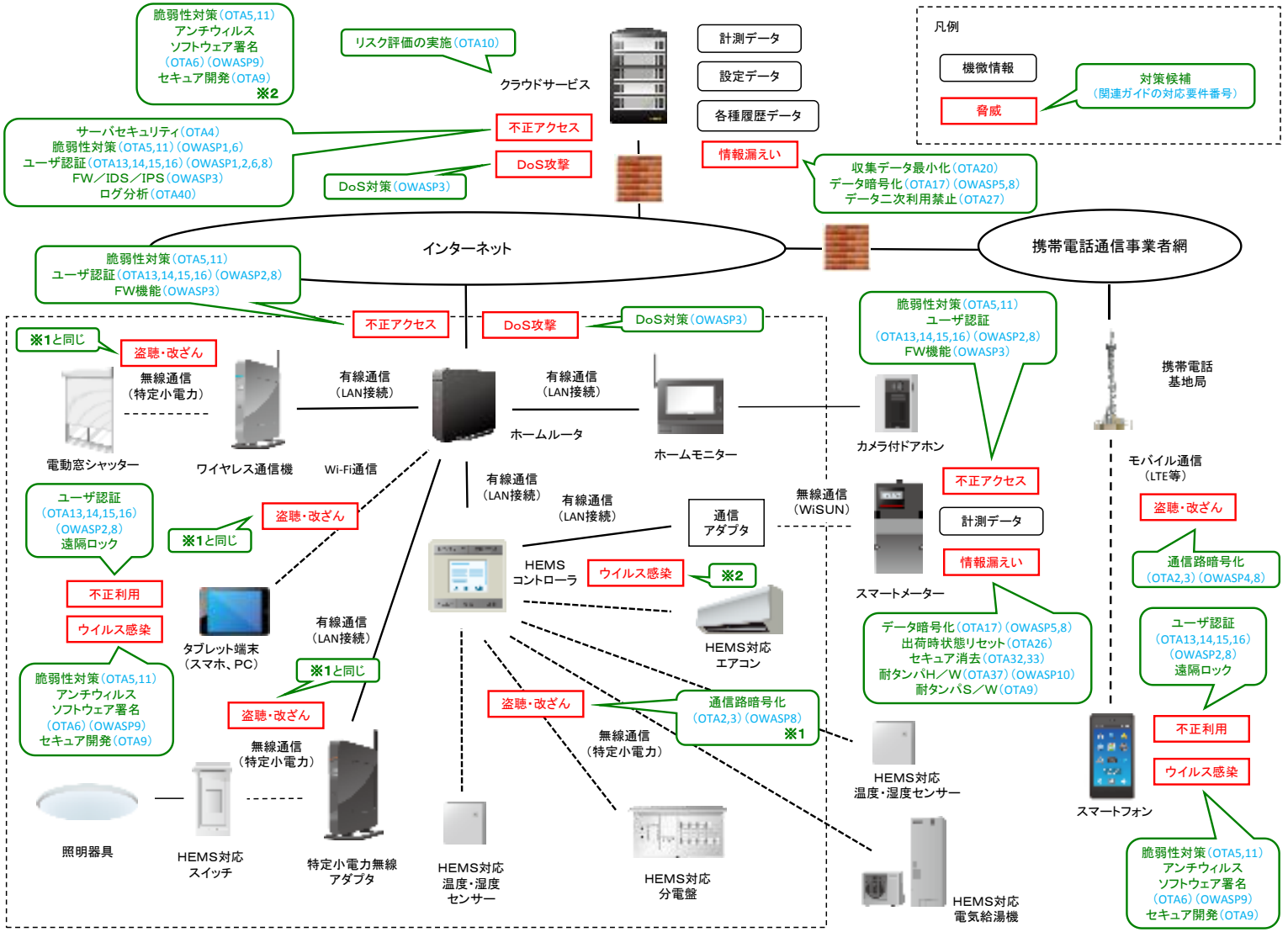
IoTのセキュリティ設計

具体的分析・検討実施例（1/2）ヘルスケア機器とクラウドサービス



IoTのセキュリティ設計

具体的分析・検討実施例（2/2）スマートハウス



IoTのセキュリティ設計
脆弱性対応（1/4）開発段階での対応

- 開発段階での対応
  - 新たな脆弱性を作り込まない
    - セキュアプログラミング技術の適用、コーディング規約、ハードウェアのセキュリティ
  - 既知の脆弱性を解消する
    - 外部のソフトウェア部品、サンプルコード
  - 残留している脆弱性を検出・解消する
    - 既知の脆弱性検査、ソースコード検査、ファジング（※）等
  - 製品出荷後の新たな脆弱性の発見に備える
    - ソフトウェアの更新機能の実装

（※） IPAのWebサイト「脆弱性対策：ファジング」
https://www.ipa.go.jp/security/vuln/fuzzing.html

IoTのセキュリティ設計
脆弱性対応（2/4）運用段階での対応

- 運用段階での対応
  - 継続的に脆弱性対策情報を収集する
    - 出荷した製品、開発に利用した外部のソフトウェア部品
  - 脆弱性検出時、脆弱性対策情報を作成する
    - 脆弱性の概要、深刻度、影響を受ける範囲、想定される影響、対策等
  - 脆弱性対策情報をユーザに周知する
    - 速やかに、確実に通知 （例：脆弱性届出制度の活用）
  - 更新ソフトウェア（脆弱性修正版）を製品に適用する
    - 速やかに、確実に適用してもらう仕組み
    - ユーザによる適用が困難な場合は、リコールも考慮

IoTのセキュリティ設計
脆弱性対応（3/4）IPAの提供するコンテンツの活用

- 脆弱性対策情報データベース JVN iPedia
  - 約90,000件（2018年11月時点）の国内外のソフトウェアの脆弱性対策情報を蓄積
    - 既知の脆弱性解消（開発段階）、継続的な脆弱性対策情報の収集（運用段階）に活用可能

http://jvndb.jvn.jp/

- 『IoT製品・サービス脆弱性対応ガイド』
  - 2018年3月22日公開
    - IoT製品・サービスを開発・提供している企業の経営者・管理者向けガイド
    - セキュリティ対応に対する企業の責任の考え方や脆弱性対策の必要理由を解説

IoTのセキュリティ設計

脆弱性対応（4/4）IPAの提供するコンテンツの活用

JVNDB-2017-000229
ホームユニット KX-HJB1000 における複数の脆弱性

http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-000229.html

JVNDB-2017-000217
Wi-Fi STATION L-02F にバックドアの問題

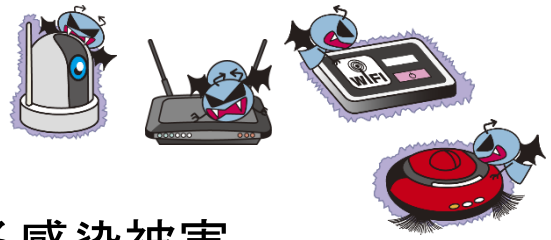
http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-000217.html

JVNDB-2017-000141
アイ・オー・データ製の複数のネットワークカメラ製品における
クロスサイトリクエストフォージェリの脆弱性

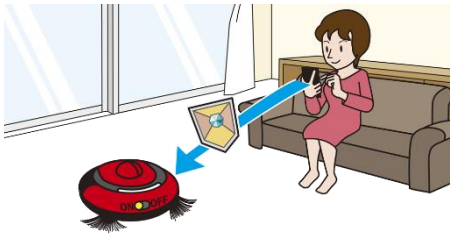
http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-000141.html

おわりに

- 多様化するIoTのセキュリティ脅威
  - 「Mirai」の出現
  - IoT機器に感染するウイルスの多様化
  - 脆弱性を有するIoT機器の散在、国内に広がる感染被害



- IoT製品／サービスの開発・製造者／提供者の対策
  「IoT開発におけるセキュリティ設計の手引き」を題材に
  - セキュリティ・バイ・デザイン（設計段階からセキュリティを考慮）
    - 脅威分析
    - 対策検討
  - 脆弱性対策（セキュリティ対策の継続的サポート）
    - 脆弱性対応
    - ソフトウェア更新



参考情報①
IPAのWebサイト「IoTのセキュリティ」

- IPAのWebサイトにおいて、「IoTのセキュリティ」のページを公開中
- IoTのセキュリティに関するIPAの取組み、参考となる資料等を紹介
  - 組込みシステム全般
  - 情報家電／オフィス機器
  - 自動車
  - 医療機器
  - 制御システム

https://www.ipa.go.jp/security/iot/index.html

参考情報②
「情報セキュリティ10大脅威 2018」解説資料

- 1章：情報セキュリティ対策の基本　IoT機器（情報家電）編
  - 一般家庭において普及の進むIoT機器（情報家電、スマート家電）の情報セキュリティ対策の基本について解説

IoT機器の購入前	IoT機器の利用時		IoT機器の廃棄時
	ネットワーク接続前	ネットワーク接続後	
・事前調査	・マニュアルの熟読 ・パスワードの変更 ・設定の見直し	・アップデートの実施 ・使用しないときは電源オフ	・廃棄・譲渡前の初期化

・IoT機器対応セキュリティ機器の導入検討
・既存のIoT機器の見直し

- 2章：情報セキュリティ10大脅威 2018
  - 個人9位 「IoT機器の不適切管理」（2017年10位）
  - 法人7位 「IoT機器の脆弱性の顕在化」（2017年8位）

https://www.ipa.go.jp/security/vuln/10threats2018.html