IPA Better Life with IT

沖縄サイバーセキュリティネットワークセミナー
「IoT時代におけるセキュリティビジネスの創出に向けて」

IoTにおける脅威と対策
～「IoT開発におけるセキュリティ設計の手引き」～

2017年 3月23日（木曜日）

独立行政法人情報処理推進機構（IPA）
技術本部　セキュリティセンター
情報セキュリティ技術ラボラトリー
博士（工学）　　辻 宏郷

はじめに

「情報セキュリティ10大脅威」 個人・組織共に14位（2016年）→個人10位・組織8位（2017年）

情報セキュリティ

10 大脅威 2016

～個人と組織で異なる脅威、立場ごとに適切な対応を～

IPA 独立行政法人情報処理推進機構 セキュリティセンター 2016 年 3 月

個人 14 位　組織 14 位

17位 IoT に関連する機器の脆弱性の顕在化

～多種多様な機器が繋がる日常～

自動車、情報家電、医療機器、インフラ設備、流通用機器等、日常生活に関連する多種多様な機器がインターネットに繋がるようになってきた。従来インターネットに繋がることを想定していなかった機器が、インターネットに繋がることにより脆弱性への脅威が顕在化してきた。

＜脅威と影響＞

昨今、自動車や情報家電等 IoT に関連する機器が登場し、世の中に普及し始めている。一方、それらの機器は、今までインターネットに繋がることを想定しておらず、十分なセキュリティが考慮されていない状態でインターネットに繋がっているものもある。それにより、攻撃者がインターネット越しにその機器の脆弱性や設定不備等を突いて攻撃を行い、不正アクセスやウイルス感染等が行われる可能性がある。その後、データの改ざんや漏えい、機器操作をされる等が懸念される。

＜攻撃手口＞

- DoS/DDoS
- IoT に関連する機器の脆弱性を悪用
- 他機器からのウイルス感染

＜事例と傾向＞

- 米国の自動車がハッキング対策で 140 万台リコール

クライスラー製自動車の車載情報システムに脆弱性が存在し、外部からの攻撃により、車両を操作される可能性があった。[I]

- IoT 機器を標的とした攻撃とアクセスを観測

警察庁の発表によると、インターネットに接続された IoT 機器を標的とした攻撃を観測しており、この攻撃を受けた機器が、攻撃者の命令に基づいて動作する「ボット」になる事例を確認した。[II] また、産業制御システムで使用される PLC（Programmable Logic Controller）の脆弱性を標的としたアクセスも観測されている。[III]

＜対策/対応＞

組織（製品開発者）

- 脆弱性対策 等

詳細については、IPA が公開している SEC journal [IV] 参照して頂きたい。

組織（利用者）、個人

- 機器使用前に、説明書を確認
- 初期設定済みのパスワードの変更
- 不要な機能の無効化
- 機器のソフトウェアの更新
- 他の機器によるインターネットの接続制限（ルータ、ファイアウォール等）

参考資料

I. Chrysler、車の遠隔操作問題で140万台のリコール発表
http://www.itmedia.co.jp/enterprise/articles/1507/27/news038.html
II. IoT機器を標的とした攻撃の観測について 平成27年12月15日
https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf
III. 産業制御システムで使用されるPLCを標的としたアクセスの観測について（第2報）
https://www.npa.go.jp/cyberpolice/detect/pdf/20150605.pdf
IV. つながる世界における脅威と脆弱性対策のポイント（SEC Journal No.43）
https://www.ipa.go.jp/files/000049573.pdf

49

https://www.ipa.go.jp/security/vuln/10threats2016.html

IPA Better Life with IT

プレスリリース
2017 年 1 月 31 日
独立行政法人情報処理推進機構

「情報セキュリティ 10 大脅威 2017」を決定

～個人と組織で IoT 機器の脅威が初めてランクイン～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、情報セキュリティにおける脅威のうち、2016 年に社会的影響が大きかったトピックなどを「10 大脅威選考会」の投票によりトップ 10 を選出し、「情報セキュリティ 10 大脅威 2017」として順位を決定し、公表しました。
URL：https://www.ipa.go.jp/security/vuln/10threats2017.html

「情報セキュリティ 10 大脅威 2017」は、2016 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約 100 名のメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。(*1) 2017 年も昨年同様に「個人」と「組織」という異なる視点で 10 大脅威を選出しています。

■「情報セキュリティ 10 大脅威 2017」

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	7 位
3 位	スマートフォンやスマートフォンアプリを狙った攻撃	3 位	ウェブサービスからの個人情報の窃取	3 位
5 位	ウェブサービスへの不正ログイン	4 位	サービス妨害攻撃によるサービスの停止	4 位
4 位	ワンクリック請求などの不当請求	5 位	内部不正による情報漏えいとそれに伴う業務停止	2 位
7 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサイトの改ざん	5 位
6 位	匿名によるネット上の誹謗・中傷	7 位	ウェブサービスへの不正ログイン	9 位
8 位	情報モラル不足に伴う犯罪の低年齢化	8 位	IoT 機器の脆弱性の顕在化	ランク外
10 位	インターネット上のサービスを悪用した攻撃	9 位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT 機器の不適切管理	10 位	インターネットバンキングやクレジットカード情報の不正利用	8 位

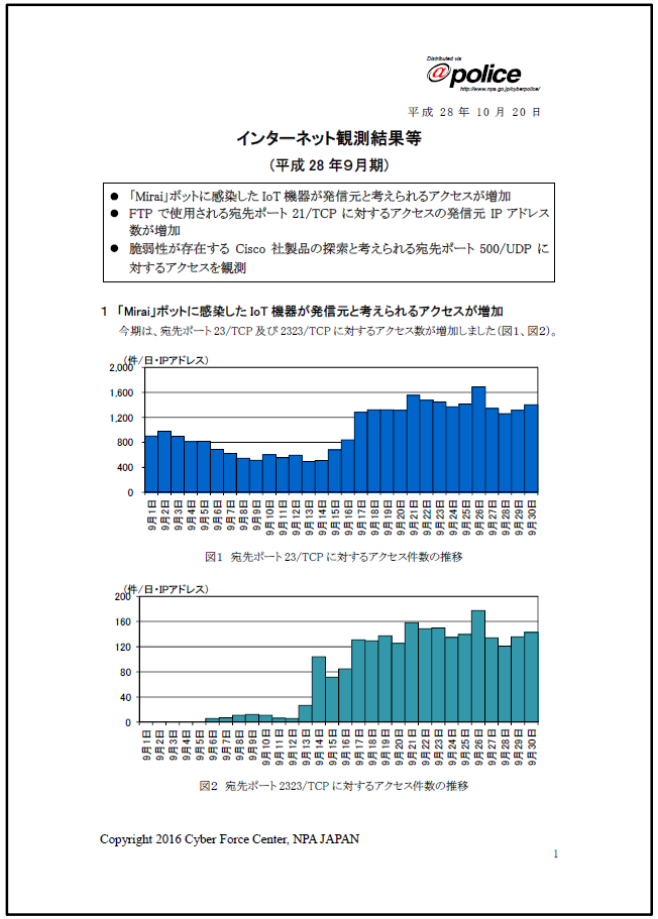
(*1) 予め IPA が 23 の候補を選定し、投票により 10 大脅威を選出。

- 1 -

https://www.ipa.go.jp/about/press/20170131.html

はじめに

2016年、IoTボットネットによる大規模DDoS攻撃の脅威が発生



平成 28 年 10 月 20 日

インターネット観測結果等

（平成 28 年9月期）

- 「Mirai」ボットに感染した IoT 機器が発信元と考えられるアクセスが増加
- FTP で使用される宛先ポート 21/TCP に対するアクセスの発信元 IP アドレス数が増加
- 脆弱性が存在する Cisco 社製品の探索と考えられる宛先ポート 500/UDP に対するアクセスを観測

1 「Mirai」ボットに感染した IoT 機器が発信元と考えられるアクセスが増加

今期は、宛先ポート 23/TCP 及び 2323/TCP に対するアクセス数が増加しました（図1、図2）。

図1 宛先ポート 23/TCP に対するアクセス件数の推移

図2 宛先ポート 2323/TCP に対するアクセス件数の推移

https://www.npa.go.jp/cyberpolice/detect/pdf/20161020.pdf

公開日：2016/11/04 最終更新日：2016/11/04

JVNTA#95530271
Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威

概要
近年、IoT 機器を使用した大規模なボットネットが構築され、分散型サービス運用妨害（DDoS）攻撃に使用されています。システムやネットワークの保護のために、IoT 機器および接続されているハードウェアを保護することが重要です。

影響を受けるシステム

- プリンタ、ルータ、ビデオカメラ、スマート TV など、インターネット経由でデータの送受信を行う IoT 機器

詳細情報
2016年9月20日、Krebs on Security が最大で 620Gbps を超える大規模な DDoS 攻撃を受けました。この DDoS 攻撃は、Mirai と呼ばれるマルウェアに感染した IoT 機器によって構築されたボットネットから行われました。Mirai は、脆弱な IoT 機器を定期的にスキャンして感染し、ボットネットに取り込みます。Mirai は初期設定で使われることの多いユーザ名・パスワードの組み合わせ 62組からなるリストを使用して、脆弱な機器をスキャンします。多くの IoT 機器は保護が全くされていない、または不十分なため、この短いリストでも数十万の機器へのアクセスが可能になります。Mirai の作者を名乗る人物によると、38万を超える IoT 機器が Mirai に感染し、Krebs on Security に対する攻撃に使用されたとのことです。

9月下旬には、フランスのウェブホスト OVH に対して、Mirai を使用した最大で 1.5Tbps にもなる DDoS 攻撃が行われました。

Mirai の影響を受けた IoT 機器は主に、家庭用ルータ、ネットワークカメラ、デジタルビデオレコーダでした。9月末には Mirai のソースコードが公開されたため、他の DDoS 攻撃に広く使用される可能性があります。

10月初旬、Krebs on Security は、IoT ボットネットによる攻撃を引き起こす、Mirai とは別系統のマルウェアについて言及しています。この別系統のマルウェアはまだソースコードが明らかになっていませんが、Bashlite と呼ばれています。Bashlite も Mirai 同

https://jvn.jp/ta/JVNTA95530271/index.html

情報セキュリティ

安心相談窓口だより

ネットワークカメラや家庭用ルータ等のIoT機器(※1)は利用前に
必ずパスワードの変更を

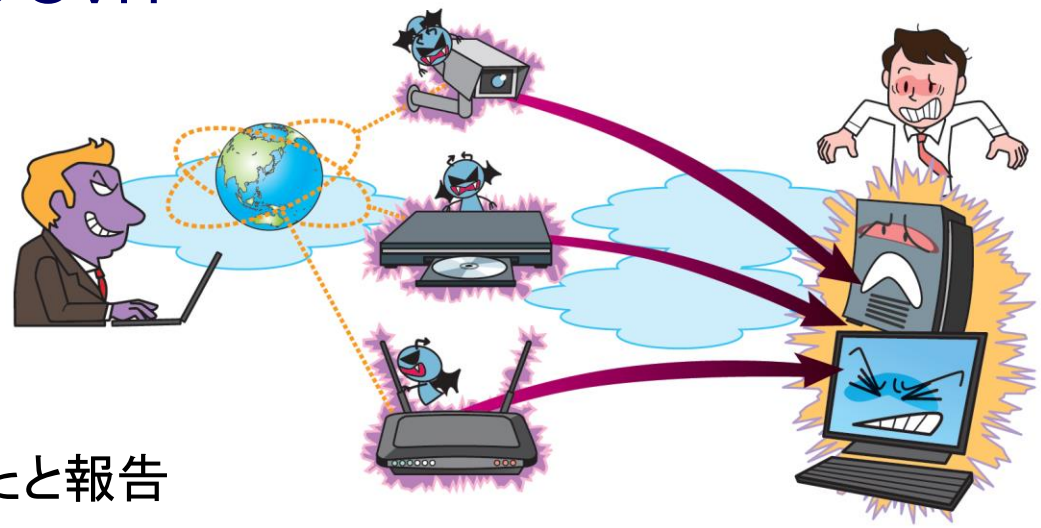
図1：ログイン情報が初期設定のままのIoT機器が狙われるイメージ

https://www.ipa.go.jp/security/anshin/mgdayori20161125.html

IoTにおける脅威の事例

IoTボットネットによって生じたDDoS攻撃の被害とは？

- 2016年9月： セキュリティ専門家ブログ “Krebs on Security”
  - マルウェア「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
  - Dyn社は1000万のIPアドレスが攻撃に参加していたと報告



- 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マルウェア感染攻撃（「Mirai」の亜種？）
  - 4～5%がクラッシュまたは制限状態となり、90万ユーザに影響

IoTにおける脅威の事例

IoT機器を狙うマルウェア「Mirai」の正体とは？

- 組込みLinuxおよび軽量UNIXコマンドツールBusyBoxの上に実装されたIoT機器を感染対象としている。
- ハードコーディングされた「ユーザ名とパスワード」を用いて、telnet（ポート番号23および2323）でログイン可能なIoT機器に感染する。
  - IoT機器の典型的な「ユーザ名とパスワード」の一覧表を内包
- 「Mirai」に感染したIoT機器は、同様に感染可能なIoT機器を探索して攻撃者に報告し、ボットネット構築に利用される。
- 「Mirai」に感染したIoT機器は、60秒毎にC&Cサーバと通信。また、C&Cサーバからの攻撃命令を受信して、指定された対象にDDoS攻撃を実施する。
- ソースコード公開により、異なる感染方法・攻撃方法を持つ「亜種」が出現している。

【出典】http://www.iij.ad.jp/company/development/report/iir/033.html 等をもとに作成

IoTにおける脅威の事例

「Mirai」にハードコーディングされたユーザ名とパスワードの例

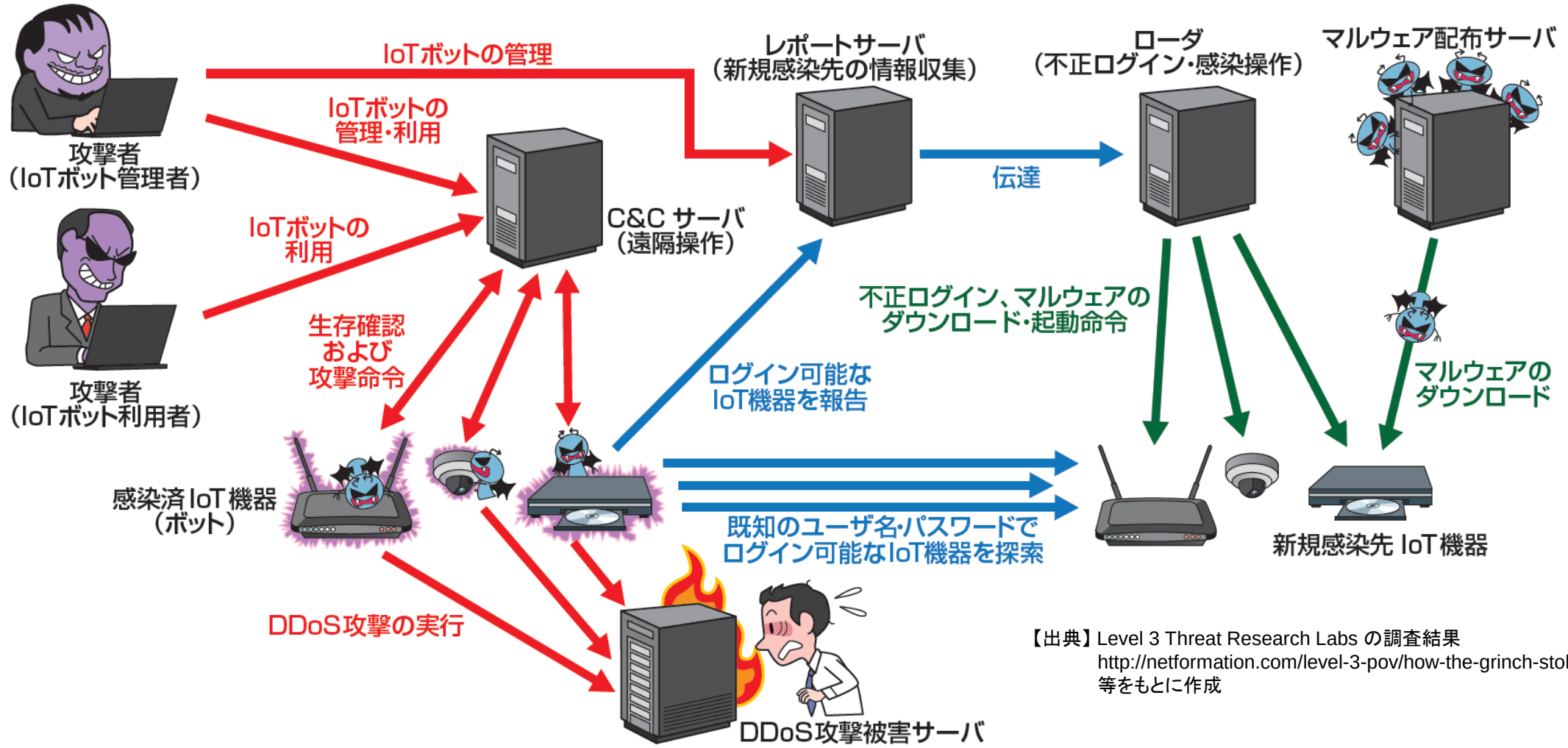
ユーザ名	パスワード	該当するIoT機器の例
root	xc3511	Shenzhen Ele Technology, DVR
root	vizxv	Zhejiang Dahua Technology, Camera
root	admin	IPX International, DDK Network Camera
admin	admin	
root	888888	Zhejiang Dahua Technology, DVR
root	xmhdipc	Shenzhen Anran Security Technology, Camera
root	default	
root	juantech	Guangzhou Juan Optical & Electronical Tech
root	123456	
root	54321	8x8, Packet8 VoIP Phone 等
support	support	
root	（未設定）	Vivotek, IP Camera
admin	password	
root	root	
user	user	
root	pass	Axis Communications, IP Camera 等
admin	smcadmin	SMC Networks, Routers
admin	1111	Xerox, Printers 等
root	666666	Zhejiang Dahua Technology, Camera
root	klv123	HiSilicon Technologies, IP Camera

ユーザ名	パスワード	該当するIoT機器の例
supervisor	supervisor	VideoIQ
666666	666666	Zhejiang Dahua Technology, IP Camera
ubnt	ubnt	Ubiquiti Networks, AirOS Router
root	klv1234	HiSilicon Technologies, IP Camera
root	Zte521	ZTE, Router
root	hi3518	HiSilicon Technologies, IP Camera
root	jvbzd	HiSilicon Technologies, IP Camera
root	anko	Shenzhen ANKO Tech, DVR
root	zlxx.	Electro-Voice, ZLX Two-way Speaker?
root	7ujMko0vizxv	Zhejiang Dahua Technology, IP Camera
root	7ujMko0admin	Zhejiang Dahua Technology, IP Camera
root	system	IQinVision (Vicon Industries), Camera 等
root	ikwb	Toshiba, Network Camera
root	dreambox	Dream Property GmbH, Dreambox Receiver
root	user	
root	realtek	RealTek Routers
root	00000000	Panasonic, Printer
admin	1111111	Samsung, IP Camera
admin	123456	ACTi, IP Camera
admin	meinsm	MOBITIX AG, Network Camera

【出典】http://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/ 等をもとに作成

IoTにおける脅威の事例

「Mirai」の主な挙動（感染・ボットネット構築・DDoS攻撃）とは？



【出典】Level 3 Threat Research Labs の調査結果
http://netformation.com/level-3-pov/how-the-grinch-stole-iot
等をもとに作成

IoTにおける脅威の事例

なぜIoT機器は「Mirai」に感染してしまったのか？

- 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の動作やポートのオープンは利用者に非公開の「バックドア」であった。
- 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。
  - 管理用パスワードがハードコーディングされており、ユーザが変更出来ないIoT機器も存在した。
  - 一部機器では「バックドア」状態で、ユーザ名やパスワードの存在が利用者に隠蔽されていた。

- Flashpoint社の調査によると、この条件を満たすIoT機器が世界中に51万5千台以上発見されている。
  - ベトナム 80,499台、ブラジル 62,359台、トルコ 39,736台、台湾 28,624台、中国 22,528台、ロシア 21,814台、韓国 21,059台、タイ 15,744台、インド 14,789台、英国 14,081台

【出典】https://www.shodan.io/report/aE9jvAXo をもとに作成

IoTにおける脅威の事例

IoT機器のベンダおよびユーザはどうすれば良いのか？

- IoT機器ベンダの対策例
  - 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。
  - 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。
  - 初期パスワードは変更必須、セキュアでないパスワードは設定不可とすることが望ましい。
- IoT機器ユーザの対策例
  - 製品の説明書を熟読し、注意事項に従って利用する。
  - 常時動作不要な管理機能が実装されている場合、不要である間は機能を無効化する。
  - 動作上問題なければ、ルータ経由でネットワークに接続し、ルータにて不正通知をブロックする。
  - ネットワーク接続前、初期パスワードをセキュアなものに変更する。

IoTにおける脅威の事例
その他のインシデント事例

- 2015年3月および5月、WebカメラやHEMS（住宅用エネルギー管理システム）が、設定不備等により外部からアクセス可能な旨が指摘される。
  - 店舗や住宅内に設置されたWebカメラの映像・音声を第三者が見聞き可能。
  - スマートハウスが管理する情報を見られたり、家庭内機器を遠隔操作される可能性。
- 2016年1月、大学や高等専門学校等の複合機やプリンターの設定不備が指摘される。

- 2015年4月ホスピーラ社の薬剤ライブラリや輸液ポンプの設定等を管理するサーバソフトの脆弱性が報告される。
  - インターネット越しにサーバ上の投与する薬や投薬量を改ざんする事が可能。
- 2016年10月、Animas社のインスリンポンプに脆弱性、治療情報漏えいや不正操作・妨害の恐れ。
- 2017年1月、St. Jude Medical社の心臓ペースメーカーに脆弱性、不正な遠隔操作の恐れ。

- 2015年8月Black Hat及びDEF CONにおいて、Jeep Cherokeeの脆弱性を攻撃し、遠隔操作を成功させた事例が報告される。
  - ファームウェアを改竄した車に対して攻撃コードを送りこむことで、ブレーキ、ステアリング、エアコン等への干渉が可能。
- 2016年2月、国内電気自動車の専用スマートフォン用アプリに脆弱性、不正な遠隔操作の恐れ。

IoTにおけるセキュリティ対策の重要性

IoTの現状と課題

- 家電、自動車、玩具、産業機器など多種多様な「モノ」がネットワークを介してつながるIoT（モノのインターネット）では、「つながること」で発生する脅威に対するセキュリティ対策の不十分さや、責任分界点の曖昧さなど、様々な課題がある

  - ネットにつながる脅威を意識していない、セキュリティ対策が不十分な「モノ」の接続
  - コストの観点からセキュリティ対策が意図的に割愛される可能性
  - 医療機器など、生命に関わる「モノ」の接続
  - ゲーム機や自動車など、「モノ」同士の無線等による自律的な接続
  - ネットを介して「モノ」から収集される情報の用途は「モノ」側では制御が困難であり、システムやクラウドサービスなどバックエンド側での管理が必要
  - つながる世界を広げていくためには、「モノ」同士の技術的（通信プロトコル、暗号、認証等）、ビジネス的な約束事の確立が不可欠

IoTにおけるセキュリティ対策の重要性
「IoT開発におけるセキュリティ設計の手引き」

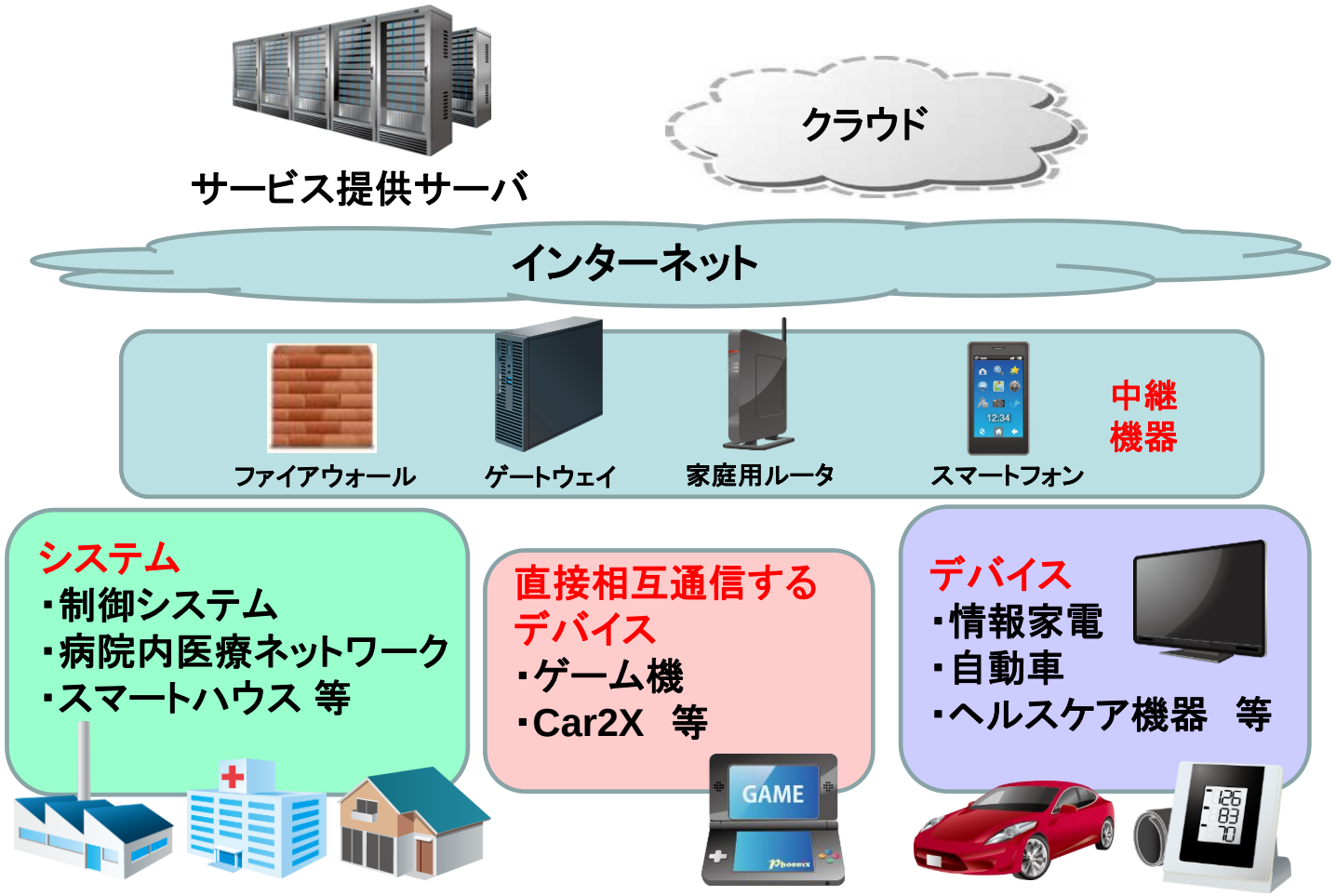
2016年5月12日、IPAウェブサイトにて公開
https://www.ipa.go.jp/security/iot/iotguide.html

【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

IoTの定義と全体像の整理
IoTの定義と全体像

■ 脅威と対策を検討するために、IoTの全体像のモデルを作成



IoTの定義と全体像の整理
IoTの構成要素（1）

- サービス提供サーバ、クラウド
  - ネットワークに接続され、IoTに対応するサービスを提供するサーバやクラウド
  - IoTによって様々な価値の高い情報を収集
    → 攻撃者によって魅力的な攻撃対象に！
  - 従来からの対策の強化が必要
    - 確実な脆弱性対策
    - 認証・ログイン方法の見直し

IoTの定義と全体像の整理
IoTの構成要素（2）

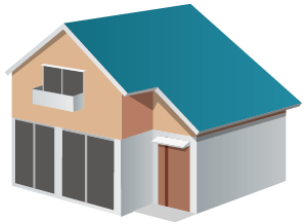
- 中継機器
  - IoT機器やシステムをネットワークへ接続
  - 例：　ファイアウォール、ゲートウェイ、ルータ
    スマートフォンが有力な中継機器に
  - デバイスのセキュリティ対策を補完
    - 不正通信をブロックし、デバイスと通信させない等



IoTの定義と全体像の整理
IoTの構成要素（3）

- システム
  - 複数の機器で構成、中継機器経由でネットワークに接続されるシステム（広義のIoT機器）
  - 例：　制御システム、病院内医療ネットワーク、スマートホーム
  - パッチ適用困難な場合やレガシーOS利用中等、対策が困難な場合も



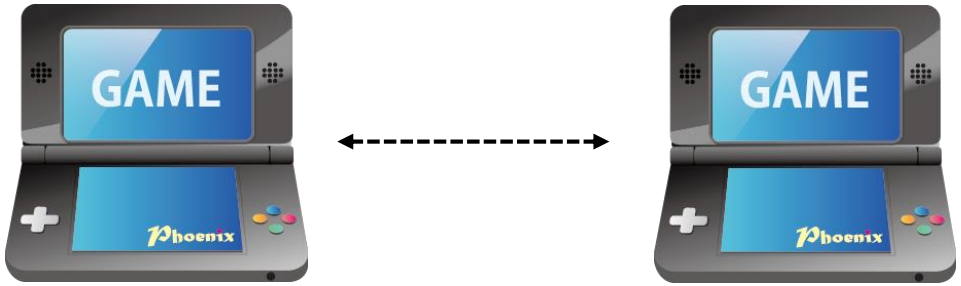


IoTの定義と全体像の整理
IoTの構成要素（4）

- デバイス
  - 中継機器を介してインターネット上のサーバやクラウド、他の機器と接続
  - 例：　情報家電、ヘルスケア機器、自動車
  - 非力なデバイス＝大きさや性能上の制約から、セキュリティ対策の一部を「中継機器」に代行してもらう場合も
  - 高機能デバイス＝「中継機器」機能を内蔵


IoTの定義と全体像の整理
IoTの構成要素（5）

- 直接相互通信するデバイス
  - 中継機器経由のインターネット接続に加えて、
    デバイス同士で直接通信
  - 例：　ポータブルゲーム機器、
    車々間通信Car2X対応自動車
  - 中継機器による補完対策が出来ないため、
    不正に改変・改造されたデバイスとの接続対策を実装要



IoTのセキュリティ設計
セキュリティ設計の手順

- セキュリティ設計の手順
  1. 対象システム／サービスの全体構成の明確化
  2. 保護すべき情報・機能・資産の明確化

【脅威分析】

  3. 保護すべき情報・機能・資産に対して、想定される脅威の明確化

【対策検討】

  4. 脅威に対抗する対策の候補の明確化
  5. 脅威レベル、被害レベル、コスト等を考慮して、
     実装すべき対策を選定

IoTのセキュリティ設計
脅威分析（1） アプローチ

- **一般的なアプローチ**

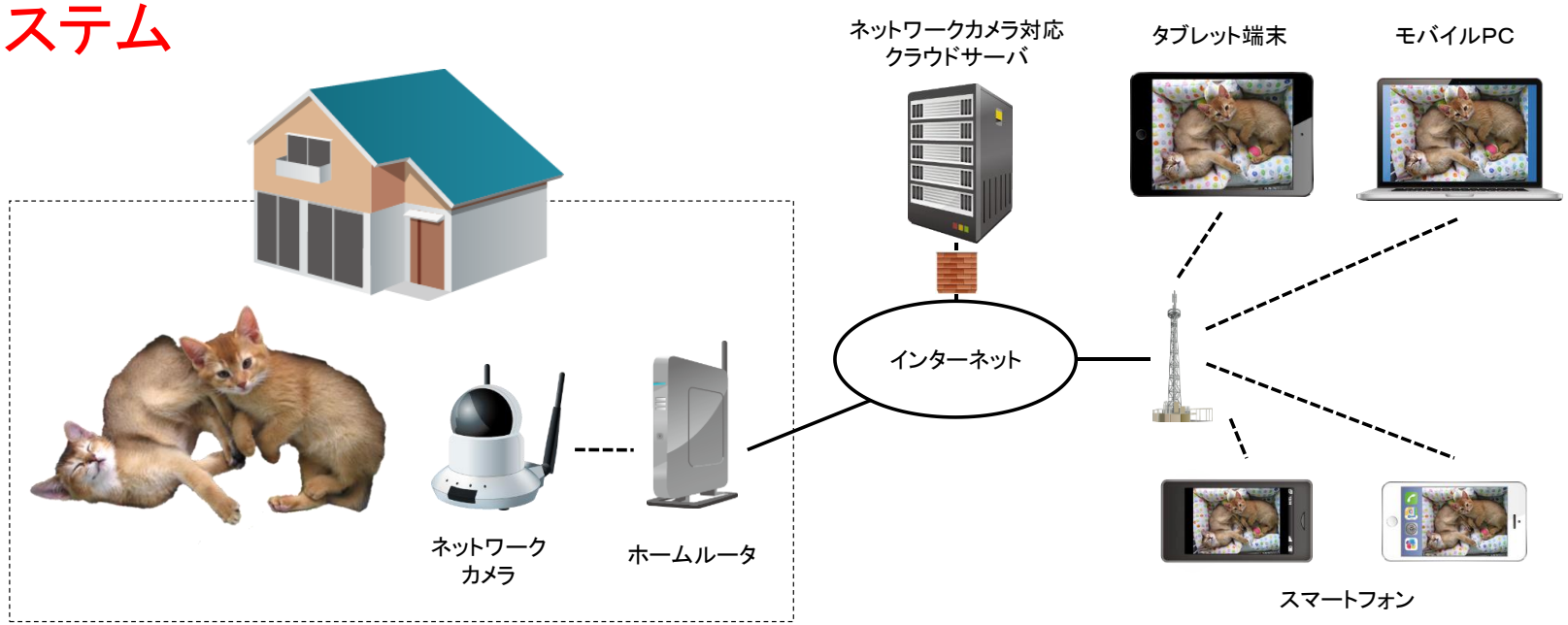
  想定される脅威および脆弱性を洗い出し、攻撃される可能性、攻撃された場合の想定被害からリスクを評価し、リスクの高い箇所にこれを抑止するための対策を検討する。

- **攻撃シナリオベースのアプローチ**

  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。

IoTのセキュリティ設計
脅威分析（2） 攻撃シナリオベースの実施例

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（3） 攻撃シナリオベースの実施例

攻撃シナリオ例：【被害1】ネットワークカメラの画像を盗み見される。

- 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、画像を不正閲覧する。
    - （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する。
      - 画像閲覧アプリ等を使用して、カメラにアクセスする。
    - （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閲覧する。
      - 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。
    - （c）不正入手・判明したパスワードを利用して、カメラの画像を不正閲覧する。
      - 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。
      - 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。
  - （2）正規ユーザが閲覧中のカメラ画像データを、ネットワーク上で盗聴する。
    - ネットワーク上のパケットをキャプチャし、画像データ部分を抽出する。
  - （3）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを窃取する。
    - 脆弱性を突いて、カメラ内部に不正アクセスする。
    - 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。

IoTのセキュリティ設計
対策検討（1）

- 脅威分析の結果に基づき、必要な対策を検討する。
  - 対象機器のリソース（CPUの処理能力やメモリ容量等）、コスト、インシデント発生時の影響度等を十分に考慮する

対策候補一覧（1/2）

対策名	機能・目的	対応する脅威の例
脆弱性対策	開発段階での脆弱性混入を防止する。運用段階で検出された脆弱性を解消する。	ウイルス感染、不正アクセス
セキュア開発	実装時にセキュアプログラミングを実施する。また、セキュリティテストを実施したことを確認の上で出荷する。	ウイルス感染
サーバセキュリティ	サーバのセキュリティ（設定情報を含む）を定期的に確認し、問題があれば修正する。	不正アクセス
FW機能	接続先をIPアドレス・ポート番号で制限する。	不正アクセス、DoS攻撃
サーバ認証	クライアントがサーバを認証することにより、サーバへの成りすましを防止する。	成りすまし、情報漏えい
フィルタリング	信頼できないウェブサイトへのアクセスを禁止する。また、信頼できないアドレスからのメール受信を拒否する。	ウイルス感染、SPAMメール
IDS/IPS	入出力データを監視し、不正アクセスの検知、抑止を行う。	不正アクセス、DoS攻撃
DoS対策	DoS（DDoS）攻撃を遮断するための対策を実施する。	DoS攻撃
アンチウイルス	ウイルスを検知・除去して、ウイルス感染を防止する。	ウイルス感染
仮想パッチ	ソフトウェア更新等が実施できず、脆弱性を完全に除去できない場合、脆弱性を突いた攻撃を前段にてブロックする。	ウイルス感染
ユーザ認証	利用者を認証することにより、利用者の成りすましによる脅威を防止する。可能であれば、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。	不正利用、不正アクセス、情報漏えい

IoTのセキュリティ設計
対策検討（2）

対策候補一覧（2/2）

対策名	機能・目的	対応する脅威の例
メッセージ認証	通信相手から送信されたメッセージを認証することにより、通信相手への成りすましによる偽メッセージ送信や、メッセージの改ざんを防止する。	成りすまし、データ改ざん、不正コマンド
通信路暗号化	データの通信路を暗号化し、通信路上のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。また、通信路上でのデータの改ざんを検知する。	盗聴・改ざん
データ暗号化	データ自体を暗号化し、仮に蓄積時または通信時のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。	情報漏えい
データ二次利用禁止	データの目的外利用を禁止し、二次利用先からの漏えいを防止する。	情報漏えい
ホワイトリスト制御	予め許可したプログラム以外の動作を禁止し、ウイルス感染を防止する。	ウイルス感染
ソフトウェア署名	署名されたソフトウェアの動作のみ許可し、ウイルス感染したソフトウェアや不正改造されたソフトウェアの動作を防止する。	ウイルス感染、不正改造
出荷時状態リセット	IoT機器を出荷時状態にリセットして、データや出荷後の設定を全て削除する。	情報漏えい
セキュア消去	記録していた場所から復元不可能な様にした上で、データを消去する。	情報漏えい
耐タンパーH/W	筐体開封を検知して内部情報を自動消去する等、ハードウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
耐タンパーS/W	プログラムやデータ構造の難読化等、ソフトウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
遠隔ロック	遠隔操作によりIoT機器の機能をロックし、第三者による不正利用を防止する。	不正利用
遠隔消去	遠隔操作によりIoT機器内のデータを消去し、情報漏えいを防止する。	情報漏えい
ログ分析	各種ログを分析することで、不正アクセスを検知し、何が行われたかを突き止める。	不正アクセス
説明書周知徹底	使用上の注意事項を説明書に明記し、使用開始前の利用者の一読を周知徹底する。	（設定誤り・操作誤りに起因する各種脅威）

IoTのセキュリティ設計
対策検討（3） 攻撃シナリオへの対策候補記入

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
脆弱性対応（1） 開発段階

- 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

IoTのセキュリティ設計
脆弱性対応（2） 運用段階

- 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） IPAが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64,000件（2016年12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
- 脆弱性届出制度
  - 発見された脆弱性の届出受付
  - JPCERT/CC経由で開発者に対応依頼
  - 用意された対策情報の周知

具体的な脅威分析・対策検討の実施例
4分野における分析・検討を実施

- 4分野における実施例

  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

- 各実施例における記載項目
  - 対象分野の概要　・・・　当該分野の説明、背景
  - 動向　・・・　脅威、インシデント事例
  - 分野の特徴　・・・　IoT化によるセキュリティ上の影響
  - 全体構成図（および解説）
  - セキュリティ対策上の留意事項
  - 脅威と対策表

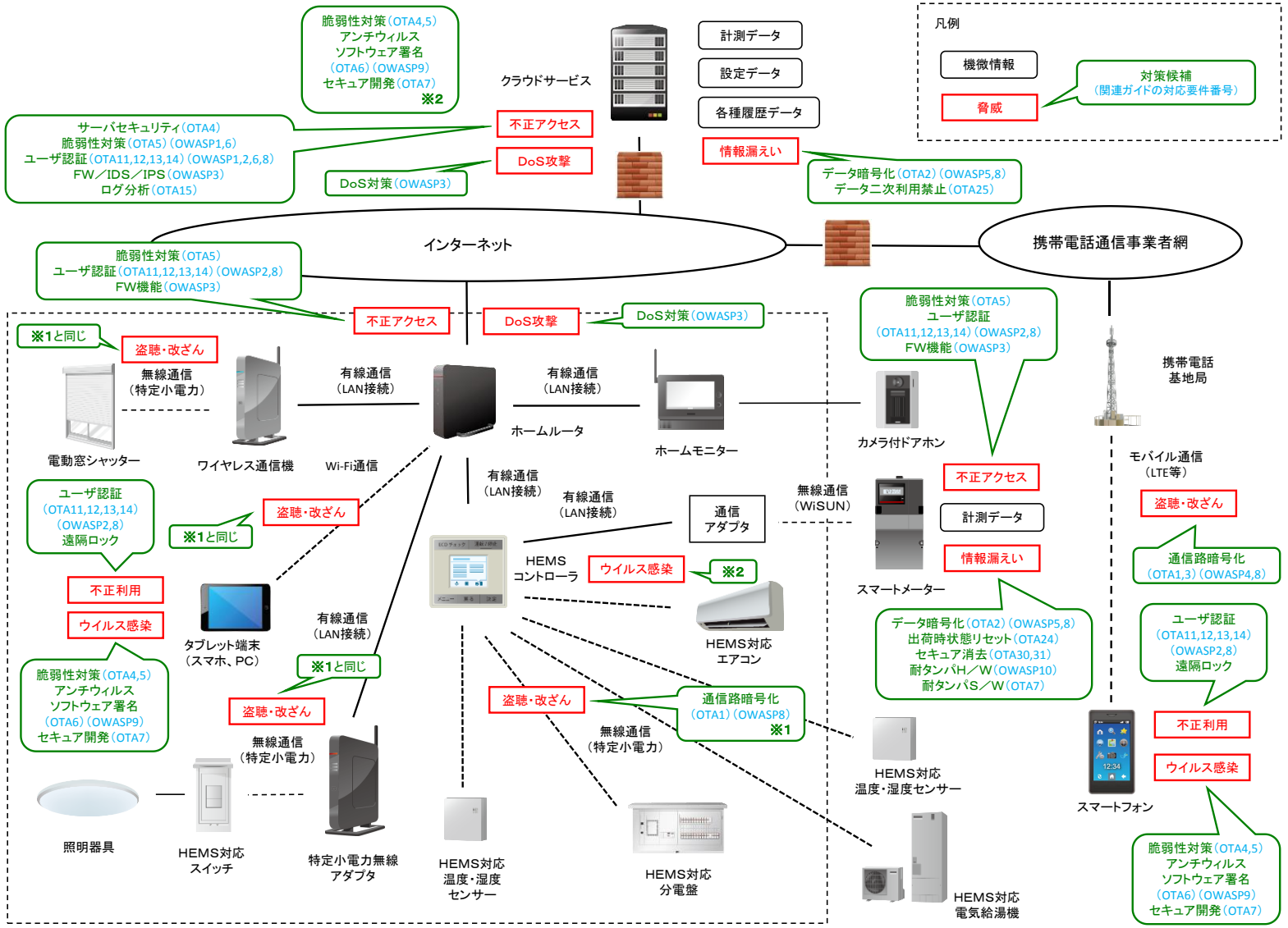
具体的な脅威分析・対策検討の実施例
実施例　スマートハウス（1）

- 対象分野の概要
  - HEMSを中心とした宅内機器の一元管理
- 動向
  - 2015年5月、HEMS不正アクセスの恐れ
  - 2016年3月、ガス機器の遠隔操作サービス
- 分野の特徴
  - 在宅状況確認（データの不正取得）から施錠解除（遠隔操作）を経て家屋への侵入、火災や宅内冠水といった金銭的・物理的被害につながる恐れ

具体的な脅威分析・対策検討の実施例

実施例　スマートハウス（2）

全体構成図



具体的な脅威分析・対策検討の実施例
実施例　スマートハウス（3）

- 全体構成図から想定される脅威
  - スマートハウス内の設置機器に保存されたデータの漏えい
  - 通信路上のデータの盗聴・改ざん
  - クラウドサービスやホームルータへの不正アクセス
    （不正ログイン、許可なき遠隔操作）
  - クラウドサービスやホームルータへのDoS攻撃
  - クラウドサービス上に保存されたデータの漏えい

具体的な脅威分析・対策検討の実施例
実施例　スマートハウス（4）

- セキュリティ対策上の留意事項

  情報漏えい対策に加えて、適切に遠隔操作が行われるための対策の実装が重要

  - 第三者による家庭内機器の許可なき遠隔操作を防止するための対策（不正アクセス対策）
  - 正規の利用者による正当な遠隔操作の妨害を受けないための対策（DoS対策）

具体的な脅威分析・対策検討の実施例
実施例　スマートハウス（5）

- 有効と考えられる対策
  - 機器、クラウドサービス上のデータ暗号化
  - 屋外に設置する機器の分解対策（耐タンパー）、データのセキュアな消去
  - 通信路の暗号化
  - クラウドサービスやホームルータにおける不正アクセス対策（脆弱性対策、認証強化等）
  - クラウドサービスやホームルータにおけるDoS対策

具体的な脅威分析・対策検討の実施例
実施例　スマートハウス（6）

脅威と対策表（抜粋）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
スマートハウス（屋内）	HEMS コントローラ	ウイルス感染	脆弱性対策	OTA4, OTA5	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA7	
	ホームルータ	不正アクセス	脆弱性対策	OTA5	
			ユーザ認証	OTA11, OTA12, OTA13, OTA14	OWASP2, OWASP8
			FW機能		OWASP3
		DoS攻撃	DoS対策		OWASP3
	無線通信（特定小電力、WiSUN、Wi-Fi）	盗聴・改ざん	通信路暗号化	OTA1	OWASP8
	タブレット端末	不正利用	ユーザ認証	OTA11, OTA12, OTA13, OTA14	OWASP2, OWASP8
			遠隔ロック		
		ウイルス感染	脆弱性対策	OTA4, OTA5	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA7	
ユーザ（外出先）	スマートフォン	不正利用	ユーザ認証	OTA11, OTA12, OTA13, OTA14	OWASP2, OWASP8
			遠隔ロック		
		ウイルス感染	脆弱性対策	OTA4, OTA5	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA7	

IoTセキュリティの根幹を支える暗号技術
暗号技術の適切な実装・運用

- 保護すべき情報に対する不正アクセス、盗聴、改ざん・偽造、成りすまし等の脅威への対策として、暗号技術を用いた認証、暗号化、電子署名の導入

- 暗号技術の実装・運用に不備が存在した場合、対策の効果を無効化する攻撃が成立する恐れ
  - 2014年、スペインの電力会社が採用したスマートメーターの脆弱性（全てのメーターで同一の暗号鍵を使用）
  - 2010年、インターネット接続機能を有する家庭用ゲーム機において、公開鍵暗号アルゴリズムの秘密鍵「ルートキー」が漏えいした問題（鍵生成する際のランダムであるべき値が同一値）

IoTセキュリティの根幹を支える暗号技術
IoTにおける暗号技術利用チェックリスト

- IoTで採用した暗号技術の利用・運用方針を明確化し、安全性の評価を支援するチェックリスト
  - 39項目に対する必須要件および推奨要件
  - 暗号技術の設計・運用条件を明確化
  - 第三者による客観的な評価を支援

暗号技術の詳細項目とセキュリティ要件 （◎必須要件　〇推奨要件）		参照[38][39][40][41][42][43][44]
暗号アルゴリズムと鍵長		
1	【暗号化アルゴリズム（共通鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC暗号リストの「電子政府推奨暗号リスト」に掲載された共通鍵暗号を採用することが望ましい。 〇共通鍵暗号としてブロック暗号を採用する場合、CRYPTREC暗号リストに掲載された暗号利用モードを採用することが望ましい。 ◎鍵長128ビット以上の暗号鍵を選択すること。	・FIPS SP800-57 Part 1: 4.2.2, 5.6 ・FIPS SP800-131A: 2 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC暗号リスト

「つながる世界の開発指針」との対応

- 本手引きは、「つながる世界の開発指針」（2016年3月24日公開）に対し、具体的なセキュリティ設計と実装を実現するためのガイド。
- 「つながる世界～」の17の開発指針と本手引きの記載事項との対応を付録に掲載。

「つながる世界の開発指針」			本書（「IoT開発におけるセキュリティ設計の手引き」）の対応箇所	
分析	指針4	守るべきものを特定する	5.1.～5.4.	実施例として、システム構成を整理し、図5-1～図5-4にて各構成要素や機微な情報の所在を明確化。
	指針5	つながることによるリスクを想定する	3.1.	実施方法の例として、接続があると判明した箇所に対する脅威分析を説明。
			3.2.	実施方法の例として、接続点において発生すると考えられる脅威に対する対策検討を説明。
			5.1.～5.4.	実施例として、システム構成を整理し、図5-1～図5-4にて接続の有無を明確化。
			5.1.～5.4.	実施例として、図5-1～5-4、表5-1～表5-12にて接続点において発生する脅威と対策を明確化。
	指針6	つながりで波及するリスクを想定する	（同上）	指針5と同一（接続する機器が攻撃の入口・脅威の糸口となるか否か、分析・検討する）。
	指針7	物理的なリスクを認識する	3.1.	脅威分析において、物理的なリスクも検討対象とする。但し、3.1.では物理的リスクに該当する例はない。
			3.2.	物理的リスクによって生じると考えらえる脅威に対して、対策を検討する。
			5.1.～5.4.	実施例として、図5-1～5-4、表5-1～表5-12にて物理的リスクに起因する脅威と対策を明確化。
設計	指針8	個々でも全体でも守れる設計をする	2.	IoT構成要素の定義・説明（2.5.）にて、機器によっては他の機器と連携して防御する可能性について示唆。
			3.2.	実施方法の例として、①外部インタフェース経由および③物理的接触によるリスクによって生じる脅威に対する対策検討を説明。
			3.3.	実施方法の例として、②内包リスクによって生じる脅威に対する対策検討（脆弱性対策）を説明。
			5.1.～5.4.	実施例として、図5-1～5-4、表5-1～表5-12にて各リスクに起因する脅威と対策を明確化。
			付録C.	セキュリティ対策の根幹となる暗号技術の安全性を確認するチェックリストを提供。

おわりに

- IoTにおける脅威
  - IoTボットネットによる大規模DDoS攻撃の脅威
  - マルウェア「Mirai」の感染・ボットネット構築・DDoS攻撃
  - その他のインシデント事例

- セキュリティ対策の重要性

  「IoT開発におけるセキュリティ設計の手引き」を題材に
  - 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・対策検討・脆弱性対応）
  - 具体的な脅威分析と対策検討の実施例
  - IoTセキュリティの根幹となる暗号技術利用チェックリスト

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　テクニカルウォッチ
「増加するインターネット接続機器の不適切な情報公開とその対策」

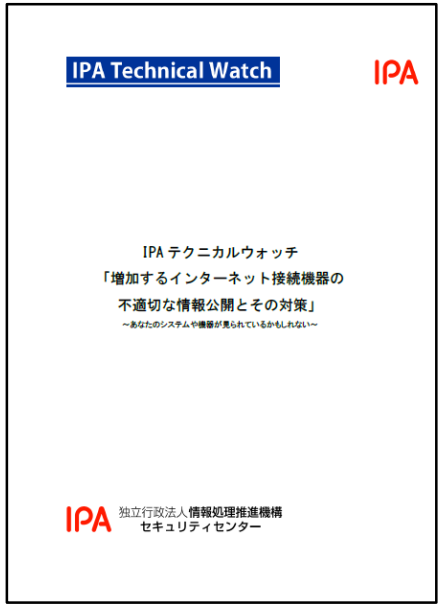
- インターネットに接続されている機器を検索するサービス（SHODANとCensys）の活用方法を紹介
- インターネットに接続されている機器のIPアドレス、ポート番号、OS、バナー情報などを検索可能

  ⇒ IoT機器がどのように見えているか確認できる

  ⇒ 問題点の早期発見、対策実施等、IoTシステムのセキュリティ向上に活用できる

本レポートは、IPAのWebサイトからダウンロードできます。

https://www.ipa.go.jp/security/technicalwatch/20160531.html



参考情報③「情報セキュリティ10大脅威 2017」

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」約100名の投票により、情報システムを取巻く脅威を順位付けして解説

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

- 2017年版は？
  - 1月31日に順位を発表
    - 個人10位「IoT機器の不適切管理」
    - 法人8位「IoT機器の脆弱性の顕在化」
  - 3月末に詳しい解説を公開予定
    - 3章　注目すべき脅威や懸念
      「IoTにおけるセキュリティ脅威の顕在化」

ご清聴ありがとうございました！

本手引きは、IPAのWebサイトからダウンロードできます。
https://www.ipa.go.jp/security/iot/iotguide.html

Contact：
IPA（独立行政法人 情報処理推進機構）
技術本部　セキュリティセンター
情報セキュリティ技術ラボラトリー
TEL：03（5978）7527
FAX：03（5978）7552
電子メール：　vuln-inq@ipa.go.jp