資料３－１

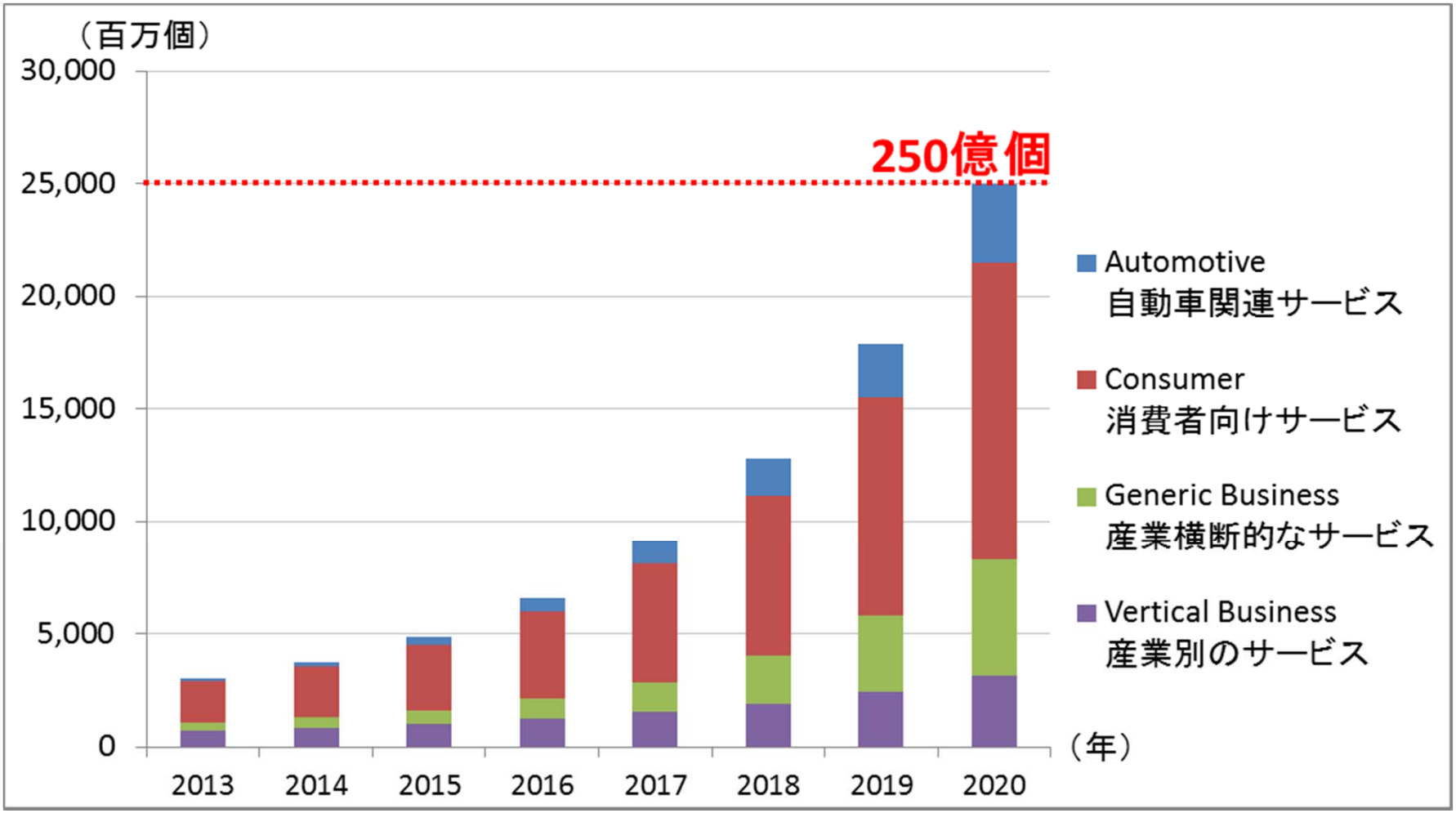
IoTセキュリティの動向について

平成２８年１月２１日

事務局

IoT機器の増加と普及分野

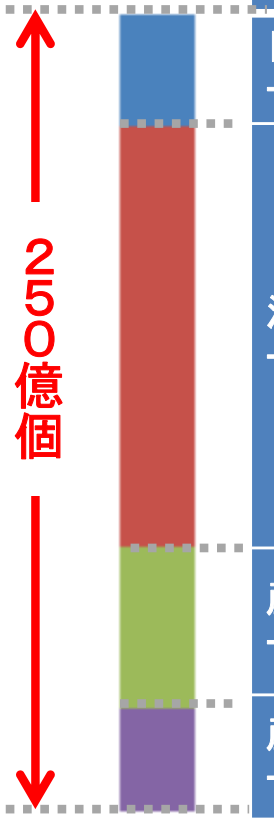
- 近年、コンピュータ以外のコンピュータ内蔵デバイスを、インターネット等のネットワークに接続して動作させることが一般化している。
- 250億個以上のIoT機器が、2020年にはネットワークサービスに活用される見込みである。



Gartner「Forecast Analysis: Internet of Things, Endpoints and Associated Services, Worldwide, 2014 Update」（2014年12月）を基に事務局にて作成

IoT機器の増加と普及分野

➢ IoT機器の増加及び普及分野に関する、2020年時点の予測においては、ホームエネルギーマネジメント（HEMS）を始めとする消費者向けサービスが52.7%と大半を占める。

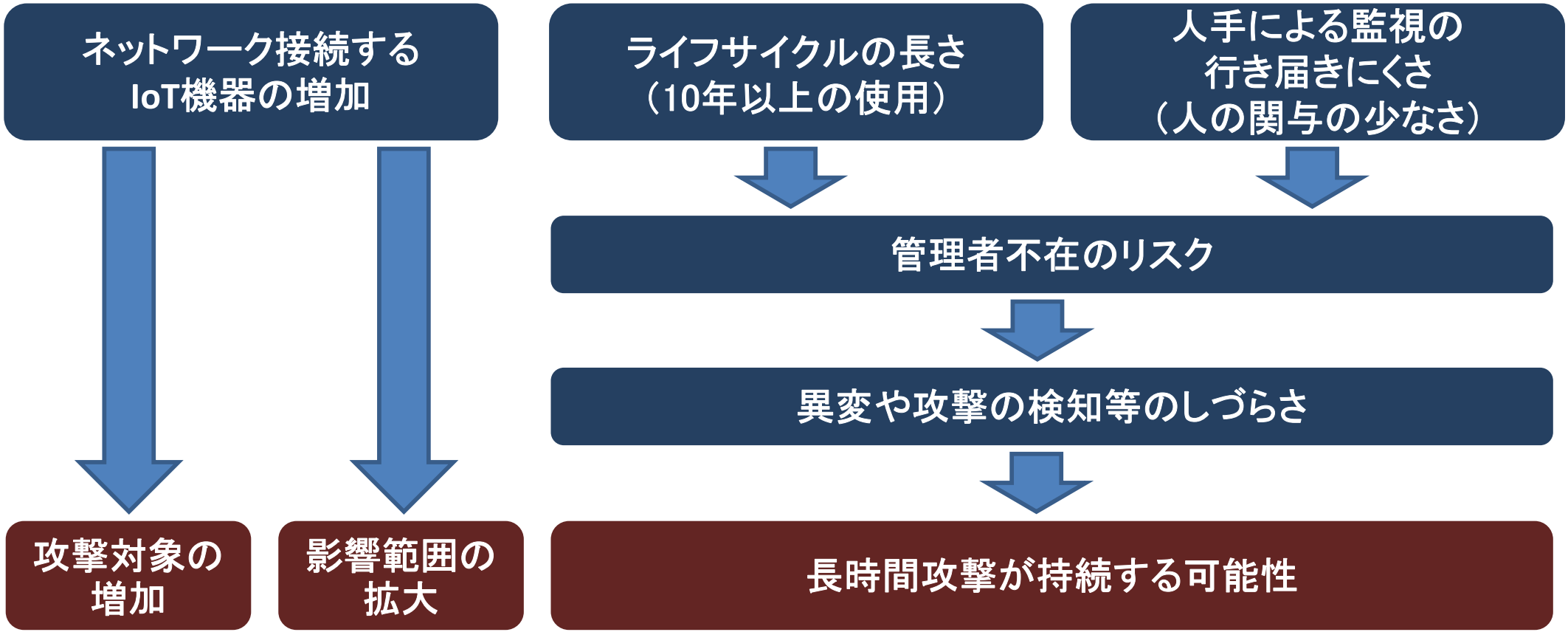


カテゴリー	サブカテゴリー	2020年 普及台数 予測（億個）	2020年 普及割合 予測
自動車関連 サービス	・コネクテッドカー ・サブシステム	35.1	14.0%
消費者向け サービス	・健康・フィットネス ・ホームオートメーション ・ホームエネルギーマネジメント（HEMS） ・ホームセキュリティ・ホームセーフティ ・情報提供・娯楽	131.7	52.7%
産業横断的な サービス	・自動化　・エネルギー　・情報提供 ・セーフティ　・セキュリティ	51.6	20.6%
産業別の サービス	・農業　・銀行・証券　・教育　・行政　・医療　・製造業 ・鉱業　・卸売・小売業　・輸送　・電気・ガス・水道等	31.6	12.7%

Gartner「Forecast Analysis: Internet of Things, Endpoints and Associated Services, Worldwide, 2014 Update」（2014年12月）を基に事務局にて作成

IoT時代の新たなセキュリティ上の脅威とセキュリティ対策の必要性①

- 「ネットワーク接続するIoT機器の増加」、「ライフサイクルの長さ（10年以上の使用）」、「人手による監視の行き届きにくさ（人の関与の少なさ）」等の、IoTシステム・サービスの動向及び特徴を踏まえた、セキュリティ対策が求められる。



IoT時代の新たなセキュリティ上の脅威とセキュリティ対策の必要性②

- IoTの進展がイノベーションを加速し、実世界に連動した新たな脅威へのセキュリティ対策が求められる。

IoTによる環境変化	IoT脅威	IoTセキュリティ対策
技術の変化 情報処理･通信 → モノの制御･接続	セーフティ、物理的な脅威の拡大	セーフティとセキュリティの統合的な対策
価値の生み出し方の変化 「製品」 → 「サービス」 → シェアリング・エコノミー → ゼロ・マージナルコスト社会	多様なユーザのセキュリティリテラシーの違い	開発フェーズのみならず、保守運用フェーズにおいてもセキュリティ対策
プロセス・イノベーション サプライチェーンの多様化	サプライチェーンリスクの拡大 （レイヤの多層化･部品調達）	サプライチェーンリスクマネジメント
プロダクト・イノベーション ドローン、自動運転、介護ロボットなど新たな機器の登場	セキュリティの配慮が不十分	提供者・利用者のセキュリティリテラシの高度化

システムの階層構造からみたIoTの脅威例

- IoTシステムの階層構造は、「機器」、「ネットワーク」、「プラットフォーム」、「サービス」の4階層に整理することができる。
- 想定される脅威および対策技術は以下のようなものが挙げられる。

階層構造	階層ごとの脅威の分類例	脅威の具体例	対策技術
サービス	・サービスへのなりすまし攻撃 ・サービスの脆弱性への攻撃 ・サービスへのDoS攻撃	相互利用サービスへのなりすましによる不正利用	・サービスへのアクセス制御 ・脆弱性対策
プラットフォーム	・プラットフォームのデータ改ざん ・プラットフォームからの情報漏えい ・プラットフォームへのDoS攻撃	プラットフォームのデータ改ざんによるサービス侵害	・プラットフォームへのアクセス制御 ・IoT機器のログ管理・監視 ・プラットフォームのデータ暗号化
ネットワーク	・ネットワーク経由での盗聴による情報漏えい	ネットワーク上の通信暗号化の欠如による情報漏えい	・通信データ暗号化 ・ネットワーク監視
機器	・機器へのなりすまし攻撃 ・機器内のデータ改ざん ・機器からの情報漏えい	マルウェア配布・感染による情報漏えい、機器の乗っ取り	・機器認証 ・ユーザ認証 ・機器内のデータ暗号化

分野別にみたIoTの脅威例

- セキュリティカンファレンスにおいて、ホームエネルギーマネジメント（HEMS）やコネクテッドカー等に関連するIoTの脅威例が発表されている。

カテゴリー	サブカテゴリー	発表年・会議	概要
自動車関連サービス	・コネクテッドカー ・サブシステム	2013年 CODE BLUE	自動車の不正操作のデモを紹介。コントローラエリアネットワーク（CAN）(*1)パケットを傍受・解析し、不正なパケットをCANに送信することにより、スピードメーターを不正な表示にしたり、ブレーキを無効化したりすることが可能。
消費者向けサービス	・ホームエネルギーマネジメント（HEMS）	2014年 Black Hat USA	セキュアでないホームオートメーション開発の危険性の一例を紹介。ホテルの部屋内機器の管理に利用されているKNX(*2)net/IPプロトコルをキャプチャ・解析し、機器を不正に遠隔操作が可能。
産業別のサービス	・銀行	2014年 Black Hat USA	デビットカードやクレジットカードの認証にチップとPINを用いるEMVプロトコルの脆弱性を紹介。有効なPINなしでもトランザクションを決済処理してしまう可能性を指摘。
	・医療	2012年 Breakpoint Security Conference	ペースメーカーの不正遠隔操作のデモを紹介。専用装置と植込み型ペースメーカー間の通信を傍受・解析し、ペースメーカーと不正な通信を行うことによって、830ボルトの電圧を発生させることが可能。

(*1)コントローラエリアネットワーク（CAN）：Robert Bosch社が1986年に公開した車載ネットワークプロトコル。1994年国際標準規格（ISO 11898)に認定。
(*2)KNX：欧州のKNX協会が2002年に公開したスマートハウスにおける通信プロトコル。2006年国際標準規格(ISO/IEC 14543-3)に認定。
出展：総務省「M2Mセキュリティ実証事業」調査結果から抜粋

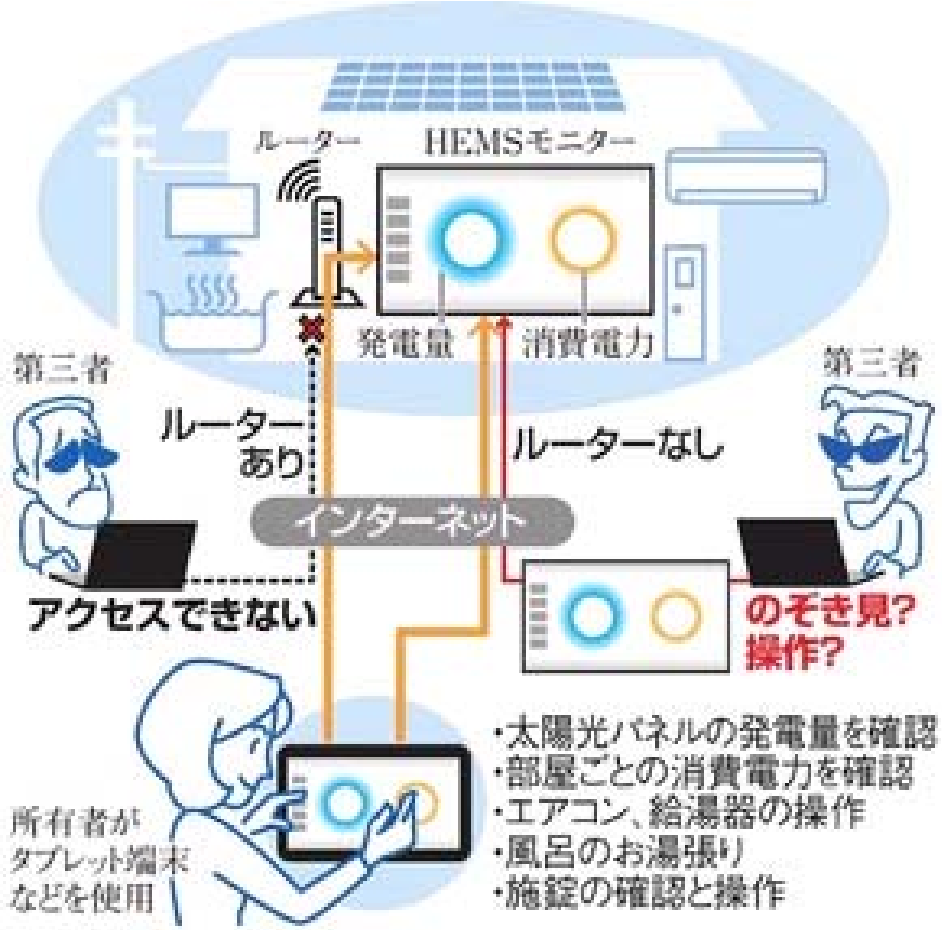
具体的事例①：自動車

- 2015年のBlack Hat国際会議での発表によると、2014年式の自動車において、インターネットから遠隔操作を可能とする脆弱性を著名なセキュリティ研究者が発見。自宅からインターネット経由で自動車の遠隔操作に成功した。
- 脆弱性への対応として、自動車会社は140万台のリコールを発表した。

出典：Black Hat USA（2015年8月）

具体的事例②：ホームエネルギーマネジメント（HEMS）

- HEMSの利用者が、外部からのアクセスを遮断できるルーターを介さずに、HEMSの確認及び操作用のパソコンをインターネットに接続しているケースでは、インターネット上の第三者がモニター画面を見ることができる状態になっており、勝手にエアコンを操作されたり鍵を開けられたりする可能性があることが分かった。

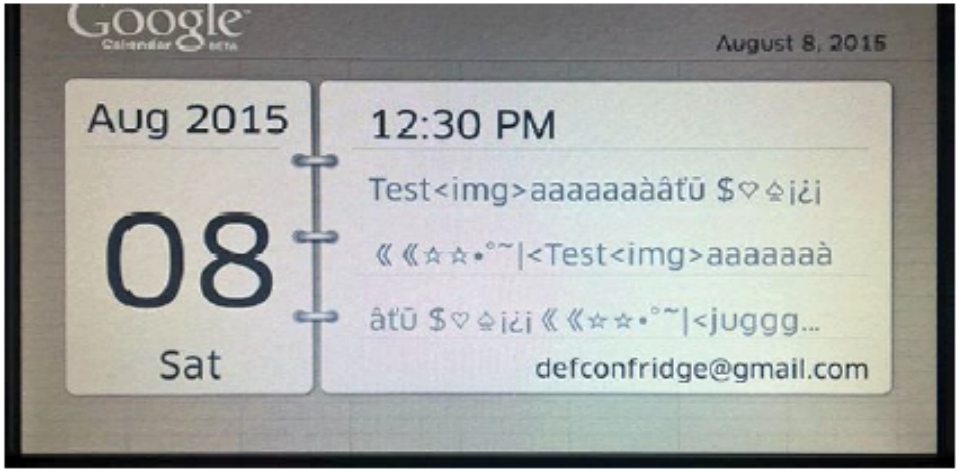


出典：朝日新聞デジタル（2015年5月）

具体的事例③：家電（冷蔵庫）

- 2015年、DEFCONのIoTハッキングコンテストで、スマート冷蔵庫の脆弱性が発見された。
- SSL証明書の検証が正しく行われておらず、Googleアカウントが窃取可能な状態になっていた。

DEFCONで開催されたIoTハッキングコンテストで、サムスン製のスマートホームアプライアンスシリーズのスマート冷蔵庫で脆弱性が発見される。
SSL証明書を正しく検証していないため、スクリーンに表示するためのGoogleカレンダーのアクセスを盗聴され、Googleのアカウント認証が窃取可能。
ファームウェアアップデートのためのサムスンのサイトへのアクセスは防御が掛っており、攻撃は失敗。



http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

出典：Pen Test Partners（2015年8月）

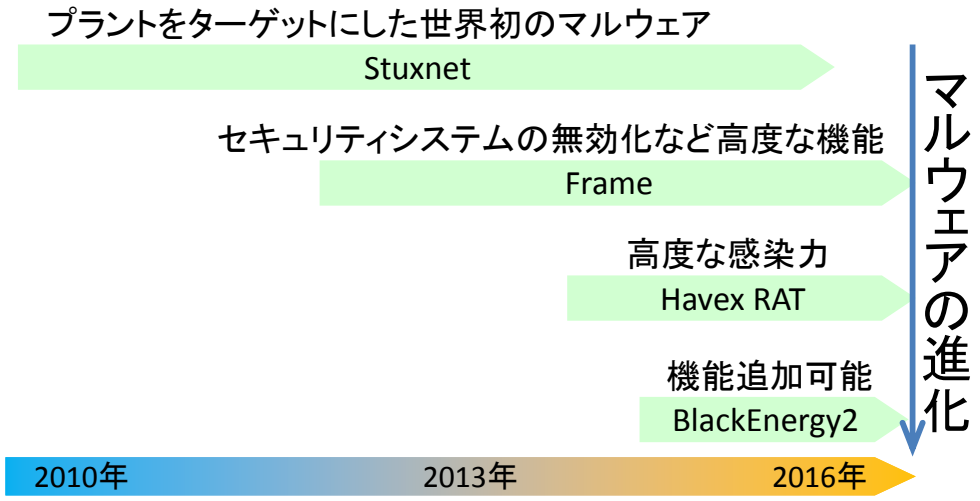
具体的事例④：プラントをターゲットにした脅威の拡大

- **プラントをターゲットとしたマルウェアStuxnetの出現後も、高度なマルウェアが出現し、インシデントは増加傾向**
- **セキュリティ対策なしにインターネットに直結されたプラントが多数存在し、脅威の原因となっている。**

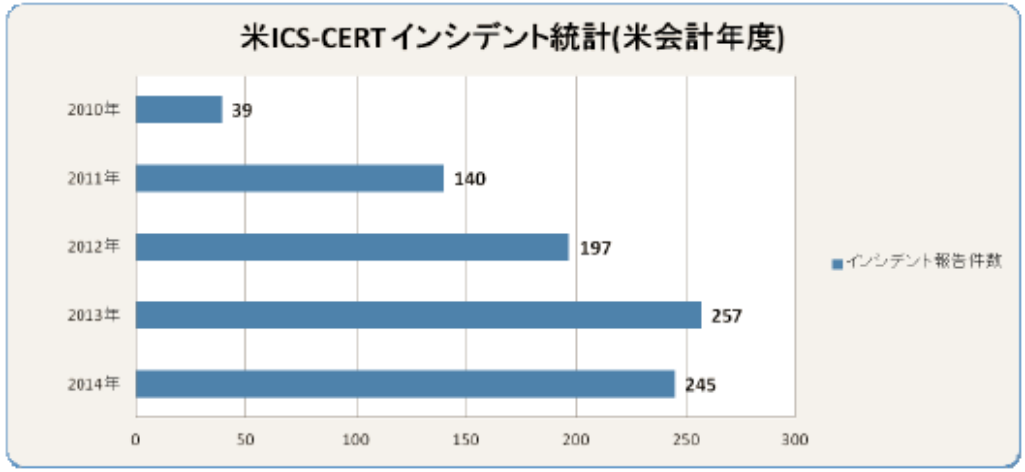
■ Havex RAT (2014年6月)
- 欧米のエネルギー企業等のプラントを狙ったマルウェア
- 遠隔操作用のマルウェアで、プラグインにより機器の情報を収集。
- 計測制御に対する影響は報告されていない。(JPCERT/CC)

■ BlackEnergy 2（2014年10月）
- プラントに侵入する高度なマルウェア
- 米国の複数の企業の制御系コンピュータがマルウェアに感染
- 感染コンピュータは、インターネット接続される制御装置

■ 高度なマルウェアの出現時期



（出所：三菱総合研究所作成）



米ICS-CERTによるインシデント（セキュリティ事故）統計推移

プロトコル/機器	ポート番号	台数
HVAC/BACNe		13,475
Serial-to-Ethernet gateway		204,416
Siemens SIMATIC/ICCP	102	3,477
MODBUS/TCP	502	16,066
DNP3	20000	625
Ethernet/IP	44818	4,522
BACNet	47808	11,553
Total		2,186,971

インターネットに直結されたプラント用機器
（出所：制御システムセキュリティの現在と展望2015, JPCERT/CC）

IoTの脅威例　参考①：JNSA「IoTの脅威　Top10」

No.	分類	脅威
1	Webインタフェース	認証の既定値、認証の平文通信の盗聴、アカウントリスト攻撃によるデータ漏洩、破壊、規約準拠の欠如、サービス停止、機器の乗っ取り
2	認証と認可	弱いパスワード、脆弱なパスワード復旧機能、弱い認証、アクセス制御の欠如によるデータ漏洩、破壊、規約準拠の欠如、サービス停止、機器の乗っ取り
3	ネットワークサービス	ネットワークサービスの脆弱性を利用しデバイス自身またはバウンスを利用した攻撃によるデータ漏洩、破壊、サービス停止、他の機器への攻撃
4	通信の暗号化の欠如	ネットワーク上の通信の暗号化の欠如により、通信データを覗き見されることによるデータ漏洩、ユーザアカウント情報の漏洩
5	プライバシー	不十分な認証、弱い暗号化通信、ネットワークの脆弱性、機器の設定ミス等によるパーソナルデータ漏洩
6	クラウドインタフェース	クラウドのWebサイトに関する不十分な認証、弱い暗号化通信、ネットワークの脆弱性、機器の設定ミス等によるユーザデータ漏洩、機器の乗っ取り
7	モバイルインタフェース	モバイルアプリケーションに関する不十分な認証、弱い暗号化通信、アカウントリスト等によるユーザデータ漏洩、機器の乗っ取り
8	セキュリティ設定	アクセス権設定、暗号設定、パスワードオプション等の不備によるユーザデータ漏洩、機器の乗っ取り
9	ファームウェア	悪意のあるダウンロードファイルの配布によるユーザデータ漏洩、機器の乗っ取り、他の機器への拡散
10	物理的セキュリティ	USB、SDカード等の記憶装置を介したOSへのアクセスによるユーザデータ漏洩、機器の乗っ取り、他の機器への拡散

出典：JNSA「IoTのセキュリティ脅威と今後の動向」（2015年）

IoTの脅威例　参考②：CSA「IoTネットワークサービスへの主な脅威候補」

No.	分類	脅威
1	サービスの妨害、停止	デバイスがその動作に必須の情報をサービスから得ている場合のサービス停止、レスポンス低下による不具合の発生（さらに、大量のデバイスにほぼ同時に発生することによる社会的な混乱）
2	誤った情報の流布	デバイスが受け取る情報をサーバ側で改ざんすることで、攻撃者が意図した情報を様々な形で流布
3	不正なデータによる機器の乗っ取りや妨害	デバイスがサーバから受け取ったデータによりその動作を決定する場合のサーバ側でのデータ改ざんによるデバイスの動作妨害、意図的な特定動作の実行
4	収集された様々な情報の漏洩や悪用	デバイスから収集された大量のデータがサーバに格納されている場合のユーザ情報もしくは匿名情報の情報漏洩、悪用
5	スクリプト、アプリケーションコードの改ざん	多くのデバイスがサーバ側から受け取るアプリケーションやスクリプトコードをサーバ側で変更することによる、デバイスへの任意の動作の実行
6	デバイスに配布するシステムソフトウエア（ファームウエア）改ざん	デバイスのシステムソフトウエア（ファームウエア）の自動更新機能を利用した改ざんコードのデバイスへの配布、およびデバイス制御の奪取と様々な用途への使用
7	不正なデバイスもしくは個別に乗っ取られたデバイスからのサーバ侵害	サービスのデバイス認証が不完全な場合や回避手段がある場合、もしくは正規のデバイスがなんらかの方法で乗っ取られた場合のサービスに対する有効な攻撃、およびこの攻撃が成功した場合のNo.１～6に述べたすべての脅威をもたらす可能性
8	他サービスとのデータ授受インターフェイスに対する侵害	様々なサービス間でのデータ相互利用における、他サービスや他事業者とのインターフェイスの不正利用、攻撃によるサービス侵害

出典：CSA「IoT（M2M もしくはスマート家電を含む）ネットワークサービスへの主な脅威候補」（2014年）

IoT技術・標準化動向

- IoTシステムの各階層の技術仕様や、階層間のインターフェースを規定する技術仕様に関し、さまざまな標準化団体等により技術標準化が取り組まれている。
- 通信・Internet系においては、「oneM2M」、「3GPP(*1)」、「GSMA(*2)」、「ITU- T(*3)」が、IoT技術の標準化に取り組んでいる。
- 「oneM2M」は、通信系の標準化の流れを統合して2015年2月にいち早く技術仕様を標準化（リリース1として発行）し、「ITU-T」は、2015年6月にIoT関連の研究グループを再編・統合して「SG20」を新設した。なお、IoTのセキュリティについては、セキュリティに関する研究グループ「SG17」と連携して取り組む。

■ 通信・Internet系の主な標準化団体

oneM2M	3GPP（概念：「MTC(*4)」）	GSMA（概念：「eSIM(*5)」）	ITU-T（研究グループ：「SG17・SG20(*6)」）

日経エレクトロニクス「乱立するIoT/M2M標準化　注目株を見極める」（2015年9月）を基に事務局にて作成

(*1)3GPP：3rd Generation Partnership Project
(*2)GSMA：GSM Association
(*3)ITU- T：International Telecommunication Union-Telecommunication Standardization Sector
(*4)MTC：Machine Type Communication
(*5)eSIM：Embedded Subscriber Identity Module
(*6)SG17・SG20： Study Group 17・Study Group 20

海外動向（先行するガイドライン等について）

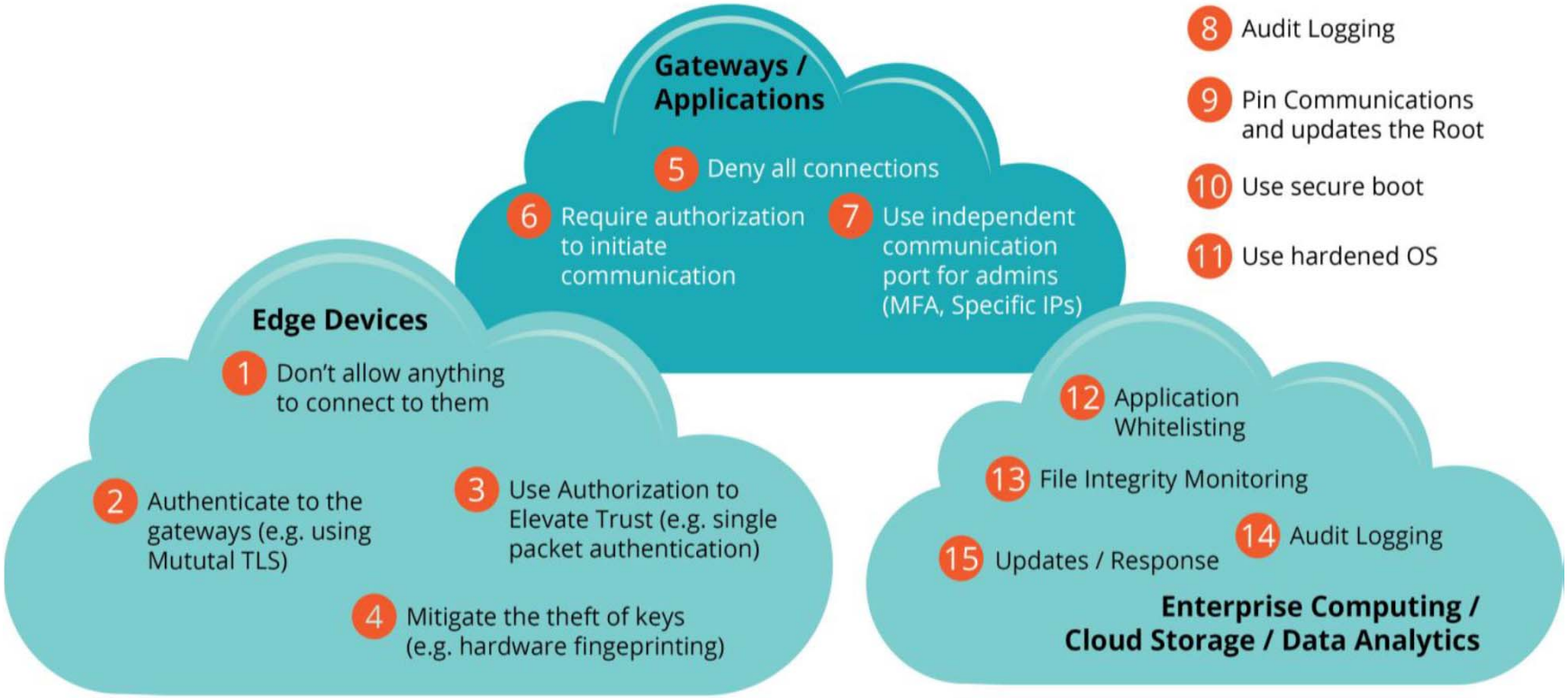
- 欧米においても、IoTに関するセキュリティガイドラインは整備段階である。
- 各ガイドラインにおいて守備範囲が異なり、分野横断的なガイドラインは未整備である。

国または地域	区分	団体	ガイドライン名（上段）／概要（下段）
米国	民間	CSA(*1)	Security Guidance for Early Adopters of the Internet of Things(IoT)
			・IoT早期導入者向けのセキュリティの手引き書 ・ITU-T Y.2060の用語を基に、IoTシステムのセキュアな実装を目的としたセキュリティ対策などを推奨
欧州	政府系	ENISA(*2)	Security and Resilience of Smart Home Environments: Good practices and recommendations
			・スマートホームに限定したセキュリティの実践方法と勧告文書 ・異なるタイプの低性能な機器やサービスを統合したスマートホーム環境における、新たなリモート攻撃の可能性と全体的なセキュリティへの取り組みの必要性を提唱

(*1)CSA：Cloud Security Alliance（クラウドセキュリティアライアンス）
(*2)ENISA：European Network and Information Security Agency（欧州ネットワーク情報セキュリティ庁）

海外動向（米国CSA「IoTの早期導入者のためのセキュリティガイドライン」）

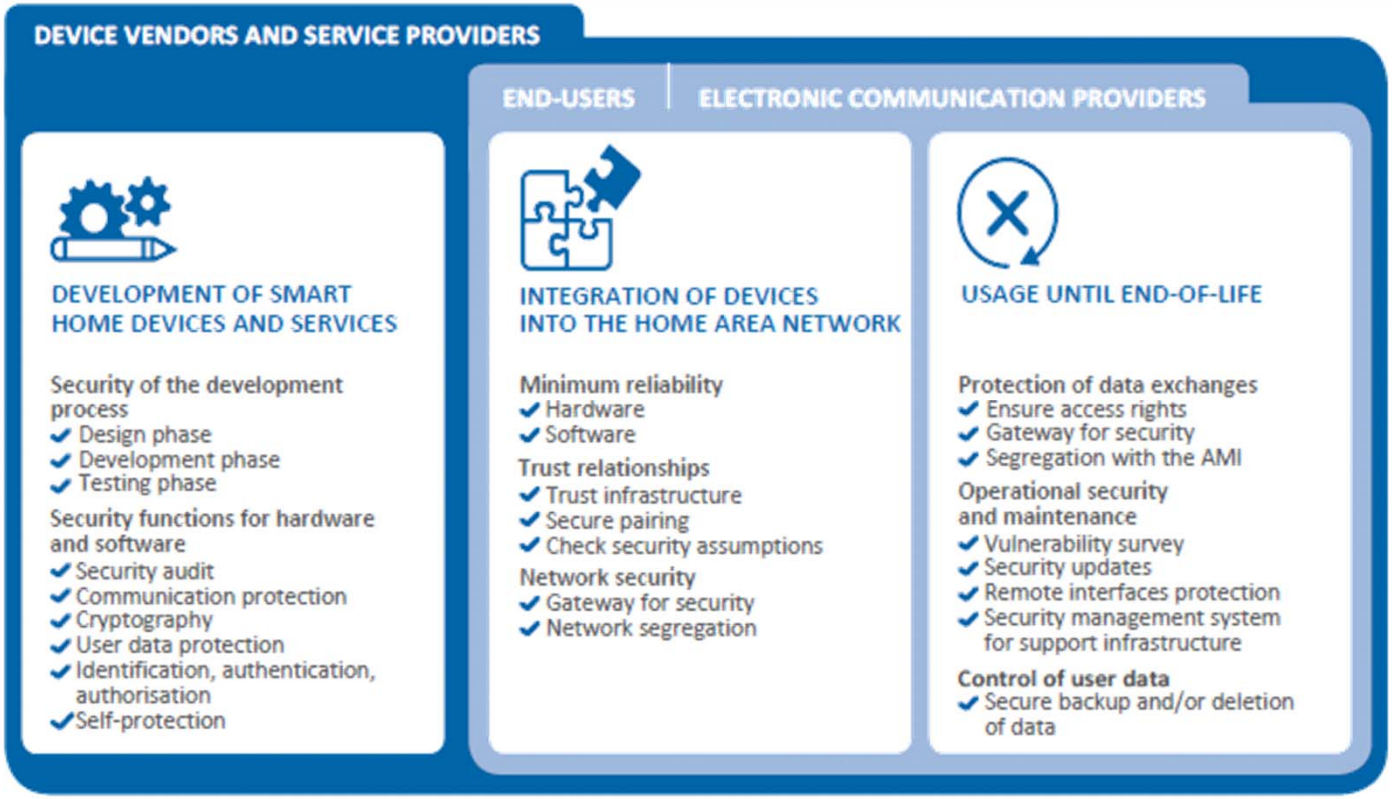
- 米国CSAは、IoT早期導入者向けのセキュリティの手引き書の中で、ITU-T Y.2060の用語を基に、IoTシステムのセキュアな実装を目的としたセキュリティ対策などを推奨している。
- 「IoTのためのセキュリティ保護アーキテクチャの構成要素」を「端末」、「ゲートウェイ/アプリケーション」、「エンタープライズ・コンピューティング/クラウド/データ分析」の大きく3つに分類している。



出典：CSA「Security Guidance for Early Adopters of the Internet of Things (IoT)」（2015年4月）における「IoTのためのセキュリティ保護アーキテクチャの構成要素」

海外動向（欧州ENISA「スマートホーム環境におけるセキュリティと強靭化）

- 欧州ENISAは、スマートホームに限定したセキュリティの実践方法と勧告文書の中で、新たなリモート攻撃の可能性と全体的なセキュリティへの取り組みの必要性を提唱している。
- 機器やサービスのライフサイクルを3つのフェーズに整理し、フェーズごとにセキュリティの実践方法を示している。
  1. スマートホーム機器とサービスの開発
  2. ホームエリアネットワークにおける機器の構築
  3. 廃棄に至るまでの機器とサービスの利用



出典：ENISA「Security and Resilience of Smart Home Environments: Good practices and recommendations」

【参考】(FTC「Internet of Things: Privacy & Security in a Connected World」)

- 2013年11月19日にFTCは「IoT：つながる世界におけるプライバシーとセキュリティ」と題したワークショップを開催しており、ワークショップの要約と企業に向けた勧告を提供している。
- FTCの使命である商業分野での消費者保護を目的とし、「消費者へ販売された」もしくは「消費者が使用している」IoT機器に議論を限定し、IoTの利点やリスクを述べている。

■ワークショップでの主な議題

・「セキュリティ」、「データの最小化」、「通知」、「選択」の4つの情報管理原則

■IoTの利点例

・ヘルスケア　　：患者の病状をかかりつけ医へ連携

・スマートホーム：電力事業者による消費者の電力利用分析、機器の問題特定
　　利用者の電力利用への関心向上

・自動車　　：自動車のセンサーに基づく運転手への道路状況通知
　　販売店へ行かずに無線でソフトウェアのアップデートを実施

■IoTのリスク例

・利用者の悪意に基づくリスク（認証されていないアクセスを可能とした上での個人情報の悪用等）

・個人情報や習慣、居場所、健康状態を長期間収集することから発生するプライバシーリスク

出典：FTC「Internet of Things: Privacy & Security in a Connected World」

【参考】(FBI「Internet of Things Poses Opportunities for Cyber Crime」)

- FBIは、企業や一般消費者向けにIoTの脆弱性に関する警告を続けており、また、サイバー犯罪の脅威を軽減するためのヒントを提言している。
- 内容は、IoT機器やIoTリスクについて説明し、インシデントの具体例を踏まえて、消費者保護のための提言を行っている。

■消費者保護のための提言

・保護されたネットワーク上にIoT機器を隔離する
・ルータ上でユニバーサルプラグアンドプレイプロトコルを使用不可とする
・IoT機器が意図された目的通りの状態となっているか検討する
・安全な機器を供給した実績のある製造業者からIoT機器を購入する
・IoT機器にセキュリティパッチを当てる
・家庭やビジネスで使用されている機器や家電の能力に気づく
・IoT機器を無線ネットワークへ接続したりリモートでIoT機器へ接続する時に、その時点の最良な方法を活用する
・家庭で使用する医療機器の能力を知っておく
・デフォルトパスワードからのパスワード変更を確実に行う

出典：FBI「Internet of Things Poses Opportunities for Cyber Crime」