IoT時代のセキュリティ

2015年12月14日（月）

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
センター長　頓宮　裕貴

本日の講演の流れ

- IPAのご紹介

1. IoTセキュリティが必要となる社会的背景
2. IoT社会の構成と脅威の分類
3. 最近の脅威事例
4. 外部からの攻撃だけとは限らない
5. まとめ

＜IPAが提供する対策コンテンツ＞

IPA（情報処理推進機構）のご紹介

（Information-technology Promotion Agency, Japan）

- 日本のIT国家戦略を技術面、人材面から支えるために設立された、経済産業省所管の独立行政法人。
- 誰もが安心してITのメリットを実感できる**“ 頼れるIT社会”**の実現を目指しています。

①情報セキュリティ

・ウイルス、不正アクセス等の届出機関。及び、調査研究、情報セキュリティの普及啓発活動。
・いち早く対策方法を広く国民に向けて発信

②情報処理システムの信頼性向上

・重要インフラを支える情報処理システムの信頼性向上に向けた取り組み

③IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成や発掘などの促進。また、若手人材の育成やIT人材に必要なスキルの明確化に向けた取り組み

IPA　検索

IPA/ISEC(セキュリティセンター)の使命と事業の柱

【使命】
経済活動、国民生活を支える情報システムの安全性を確保すること

企画

- セキュリティセンター業務の企画・調整
- 他事業部門、バックオフィスとの連携、調整
- 行政機関、関係機関等との連携、調整

ウイルス・不正アクセス及び脆弱性対策

- ウイルス・不正アクセスの届出・相談受付
- 脆弱性関連情報の届出受付・分析、提供
- 組込み機器（制御システム）等のセキュアな利用に向けた取組み
- 標的型サイバー攻撃の情報共有、相談受付

暗号技術

- 暗号アルゴリズムの安全性監視活動
- 暗号世代交代の普及促進

セキュリティの第三者認証

- ITセキュリティ評価・認証制度（コモンクライテリア）
- 暗号モジュール試験認証制度（JCMVP）

調査・分析

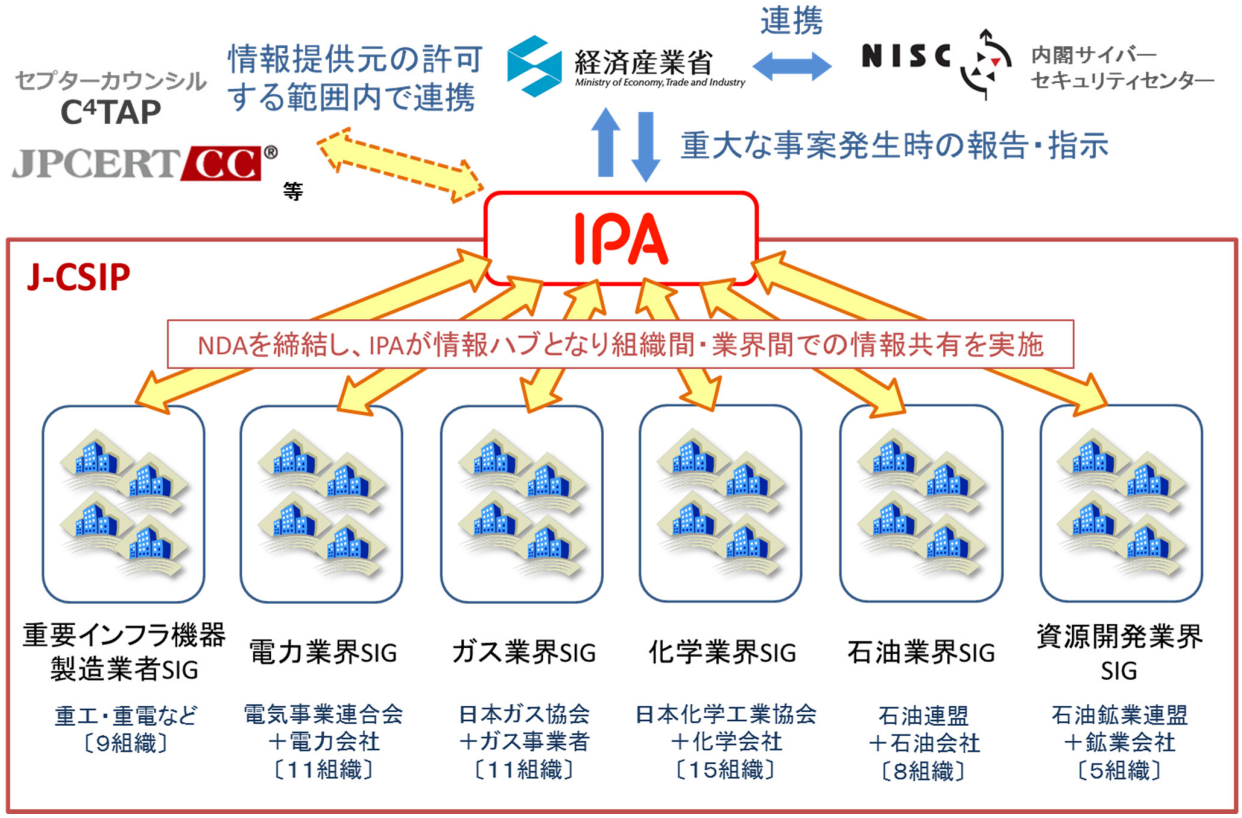
- 情報セキュリティ関連の社会経済的分析
- 情報セキュリティ白書
- 意識調査、被害実態調査

普及啓発・国際連携

- 世界の情報セキュリティ機関との連携
- 情報セキュリティの普及、啓発
- 中小企業のセキュリティ対策向上
- 情報セキュリティ対策ベンチマーク

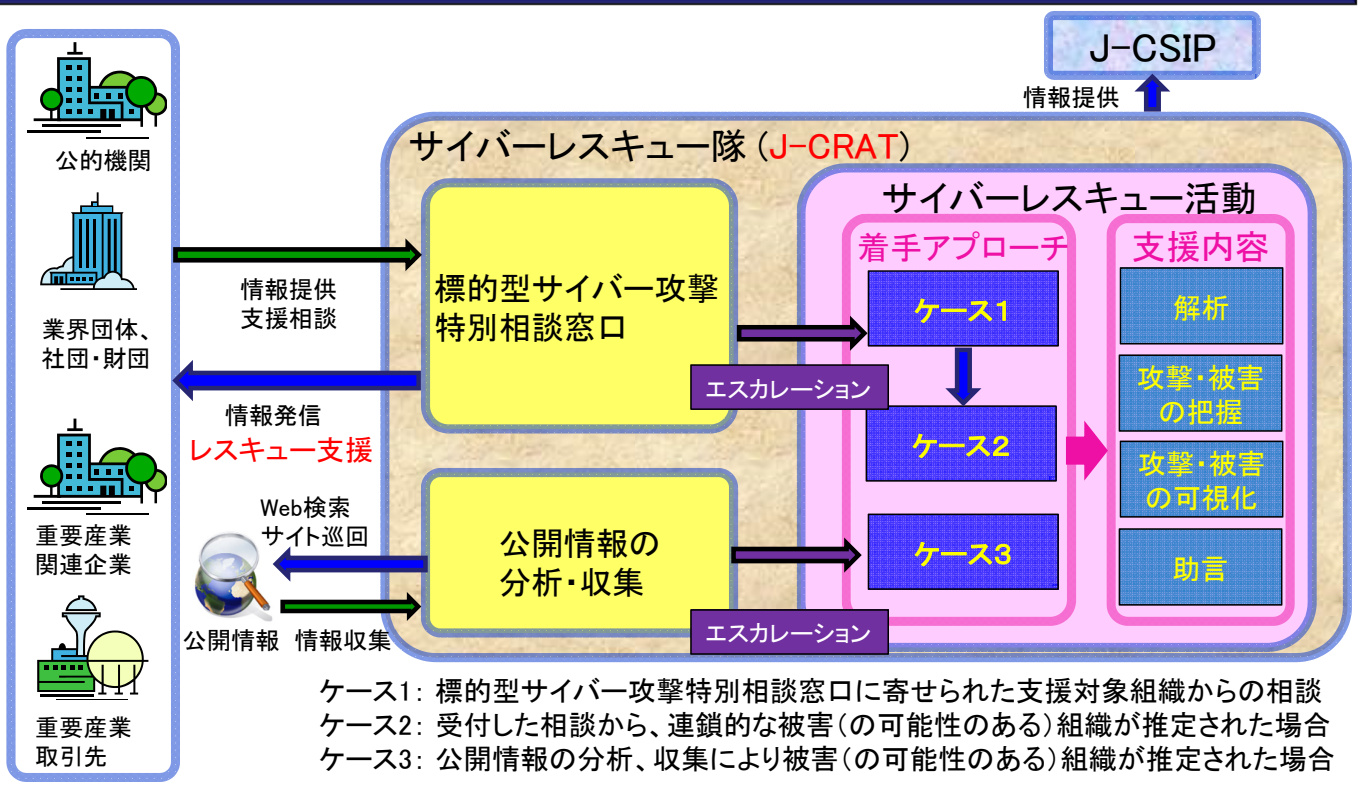
IPAの取り組み（標的型サイバー攻撃の情報共有）
サイバー情報共有イニシアティブ（J-CSIP）

IPAは、標的型サイバー攻撃の情報共有と早期対応の場として、J-CSIPを発足。



IPAの取り組み（標的型サイバー攻撃特別相談窓口）
サイバーレスキュー隊（J－CRAT）

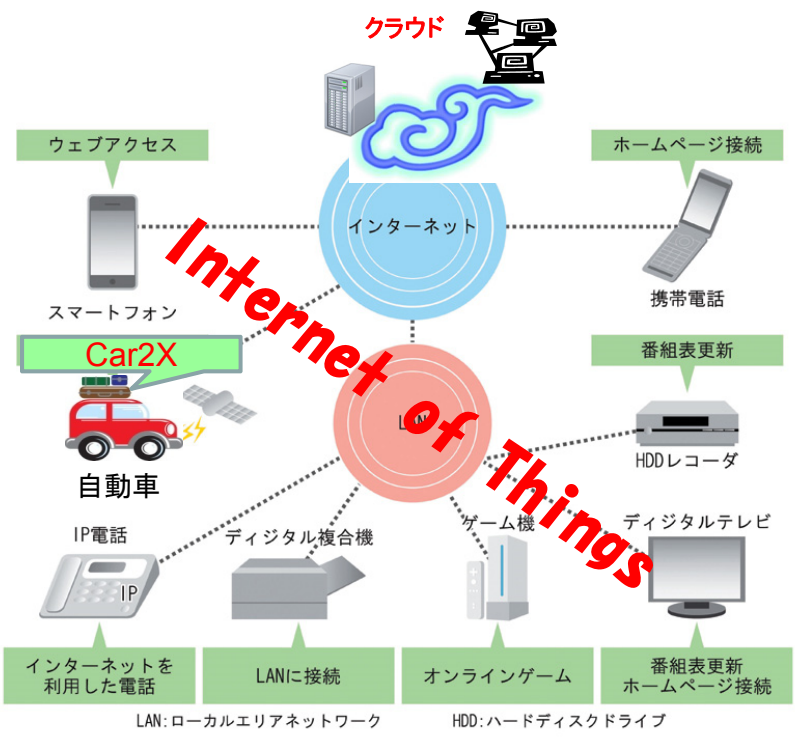
特別相談窓口へ寄せられた相談や関連で見つかった連鎖的な被害、公開情報を契機として支援



ケース1：標的型サイバー攻撃特別相談窓口に寄せられた支援対象組織からの相談
ケース2：受付した相談から、連鎖的な被害（の可能性のある）組織が推定された場合
ケース3：公開情報の分析、収集により被害（の可能性のある）組織が推定された場合

1. IoTセキュリティが必要となる社会的背景
～情報セキュリティの昔・今・これから～

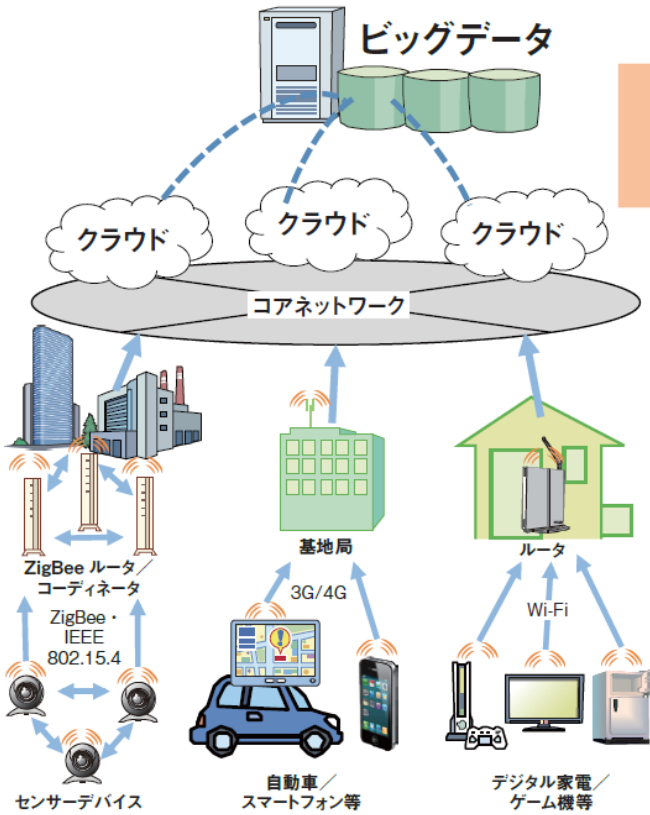
組込み機器の今昔
～繋がるモノ～



・これまでの組込みシステム
■スタンドアロンで動作
■機械的な制御

・これからのIoTシステム
■インターネットを含めた様々なネットワークと接続して動作
■クラウドの活用
■ソフトウェア制御
■個人情報や操作情報のような機微な情報を含めた様々な情報を扱う

ビッグデータの時代へ
～IoTとビッグデータが実現する様々なサービスと脅威～



IoT とビッグデータが実現する
- ◆スマート農業
- ◆スマートヘルスケア・医療
- ◆スマートハウス
- ◆自動車の自動運転
- ◆次世代交通システム…

＜IoTシステムの脅威＞

「情報」と「機器」の操作

ビッグデータへ情報が集約・蓄積
機器同士の連携

＜脅威＞
- ・情報漏えいや改ざん
- ・利用者が意図しない機器の動作

出展：IPA情報セキュリティ白書2015

三つの進化と、それに伴うセキュリティ課題

新しいサービスの発達

新しい技術や機器の発展に伴って、様々な新しいサービスが創出される。これにより、組込み業界に様々なプレイヤーが係わり、多様な情報が扱われるようになる。

情報の価値や重要度に応じたセキュリティや情報の取扱いを利用者が理解・選択出来るような仕組みが必要となる。また、新しいサービスの出現に伴って、それに適したセキュリティを検討する必要がある。

ネットワークへの接続

通信機能の搭載が容易・必須になり インターネットを含めた公共回線の利用が当然となる。これによって様々なモノが繋がる世界になる。

これまでネットワーク経由の攻撃が考慮されてこなかった製品群が、今後は攻撃の対象となるため、製品のセキュリティはもちろん、利用者の教育についても検討する必要がある。

汎用プロトコル等の利用

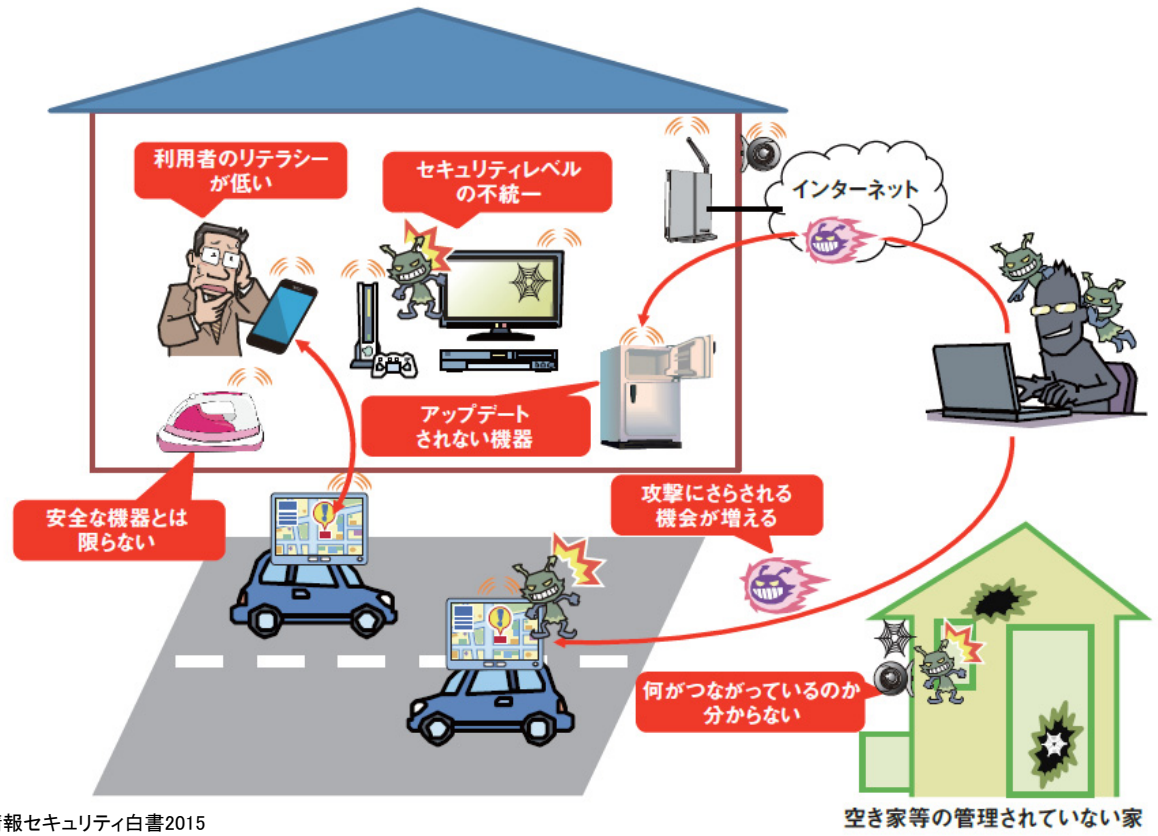
多種多様な機器を接続するためや、機器のコスト競争等から、例えばTCP/IPなどの汎用プロトコルが利用されるようになる。

これまで利用されてきた独自プロトコルが標準化され、一般的なPCでも利用される汎用プロトコル等が利用されることで、PCと同様の脅威が発生する可能性がある。

IoTのこれから

- 新しいサービスの発達
  - 車載センサの情報を活用したサービス（自動車）
  - 健康促進に向けた身体情報の活用（ヘルスケア）
  - 一般家庭における高度医療の実現（医療）
- ネットワークへの接続
  - 自動車とスマートフォンの連携（自動車）
  - 組織LANと外部ネットワークの接続（制御システム・医療）
- 汎用プロトコル等の利用
  - 様々なシステムへのオープンソース等の汎用プロトコル利用
  - 業界を超えたソフトウェアメーカ等の参入

想定されるIoT のセキュリティ上の問題点

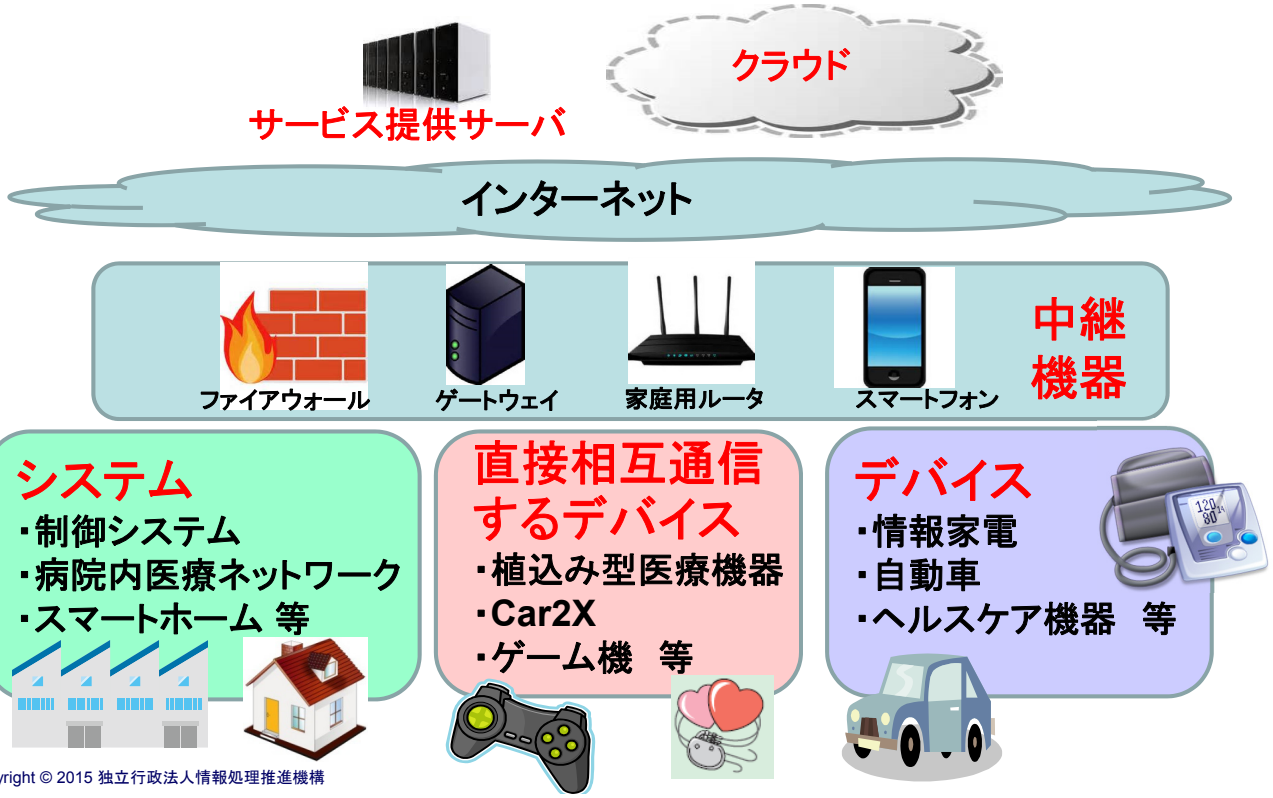


出展：IPA情報セキュリティ白書2015

2. IoT社会の構成と脅威の分類
～IoTと関連する様々な機器やシステム～

IoTの全体像

■ 脅威を整理するために、IoTの全体像のモデルを作成



IoTの全体像

サービス提供サーバ・クラウドでの脅威の事例と対策

【脅威の事例】

■ サービス提供サーバの情報漏えいの事例（2015年7月）

- シャトレーゼ　→SQLインジェクション攻撃／約21万人分の会員情報流出
- タミヤ　→Webサーバへの不正アクセス／ユーザー情報流出
- 新日本プロレスリング→サーバへの不正アクセス／ファンクラブ会員情報流出

■ クラウドでの脅威事例

- 2009年3月　Google社“オンライン・オフィス・アプリケーション「Google Docs」”
  →意図しない相手へのドキュメント共有
- 2014年9月　Apple社“iCloud”→アカウント乗っ取り、多数の画像が流出

重要情報を狙った標的型攻撃、サービス提供サーバ・クラウドへの不正アクセスが脅威となっている。

また、内部不正による情報漏えいが大きな問題になっている。

【対策】

脆弱性対策や認証・ログイン方法の見直し・内部不正対策

IoTの全体像

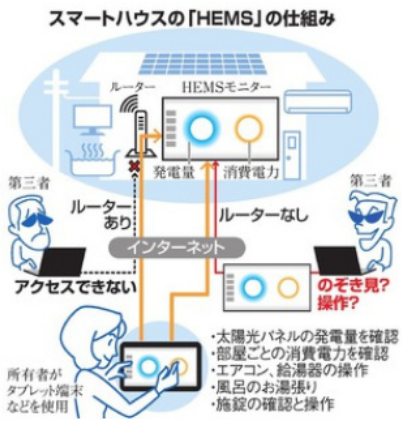
中継機器での脅威の事例と対策

【脅威の事例】

■スマートハウスが管理する情報を不正アクセスされる可能性

2015年5月に朝日新聞でネットワーク接続方法の誤りが指摘される

次世代省エネ住宅「スマートハウス」の情報を一元管理する「HEMS: Home Energy Management System」をルータを介せずネットワークに繋げた場合、第三者に情報を見られたり、家庭内機器を遠隔操作されたりする可能性がある。

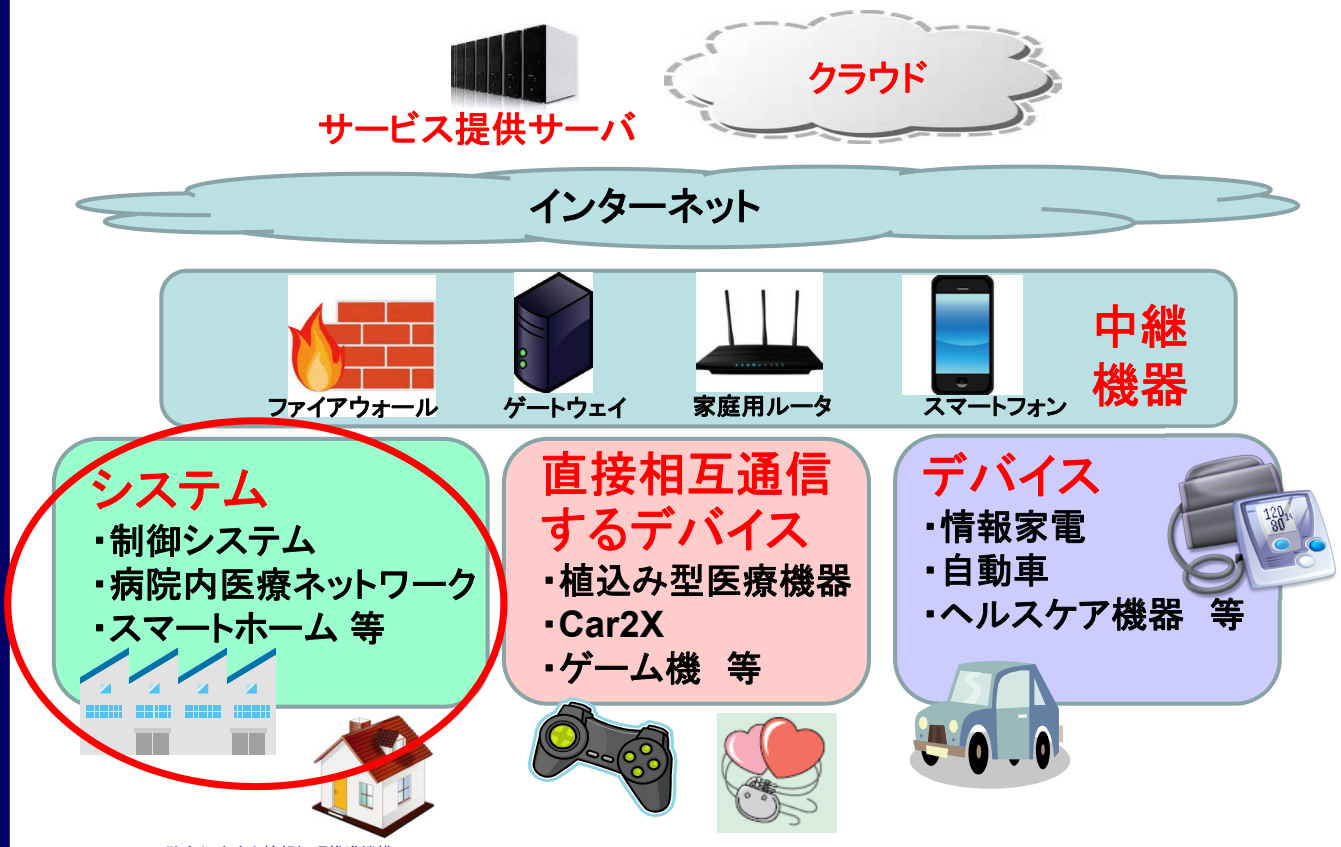


（出展）朝日新聞（2015年5月11日）「鍵開け・のぞき見…スマートハウスご注意　他人操作恐れ」
http://www.asahi.com/articles/ASH525J2JH52PTIL00H.html

【対策】

様々な形態でネットワークが繋がる環境下でサービス事業者や機器開発者だけでは無くシステム構築を行うSIerやユーザに対して利用上の注意を明確することが必要

IoTの全体像



システムでの脅威の事例と対策

【脅威の事例】

- 鉄道のトラックポイントに対するハッキング（2008年ポーランド）
  14歳の少年がテレビのコントローラを改造→ハッキングを行い脱線事故
- 核施設に対するマルウェア（Stuxnet）感染（2010年イラン）
  入念に準備されたマルウェアで複数のゼロデイ脆弱性を狙う
  →核施設における遠心分離機を破壊
- 鉄鋼工場のサイバー攻撃被害（2014年ドイツ）
  溶鉱炉が正常にシャットダウンできず操業及び装置に被害

【対策】

- 対策マネージメント組織の構築
- 現状の対策状況の確認
- 事業継続計画（BCP）で想定する主要なリスクと捉え、
  関連会社を含むサプライチェーン全体のセキュリティを検討

IoTの全体像

デバイスでの脅威と対策

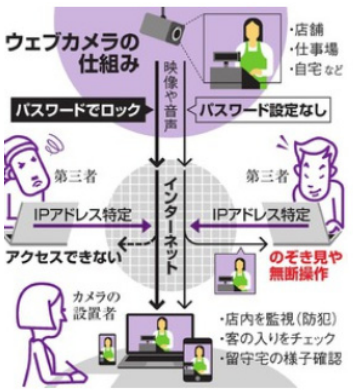
【脅威の事例】

■ Webカメラの画像を意図しない相手が見ることが可能な事例

2015年3月に朝日新聞でWebカメラの利用の不備が指摘される

- IPアドレス等から2,163台のWebカメラを検出、内769台でパスワードが未設定
- 非公開の試作品や店舗や工場の様子が確認できた
- カメラによっては場所を特定できるケースもあり
- カメラの向き等を第三者が操作できた可能性も指摘される

出展：朝日新聞（2015年3月16日）「ウェブカメラ、ネットで丸見え3割　パスワード設定せず」
http://www.asahi.com/articles/ASH3654C1H36PTIL00W.html



【対策】

- デフォルトパスワードなどの基本的な運用の見直し
- 脆弱性の発見時に速やかなアップデート等が出来るような体制・機能を整備

IoTの全体像

相互通信するデバイスでの脅威の事例と対策

【脅威の事例】

■ 植込み型医療機器の脆弱性

- 2011年、無線通信を行う植込み型のインスリンポンプやペースメーカに脆弱性が発見され、健康被害に繋がる攻撃が実施される可能性が指摘された。

■ ゲームデータを不正に改ざんする行為に関する注意喚起

- 「無線通信を行うゲーム機が改ざんされたゲームデータを受け取り実行することで、ゲームが正常にプレイできなくなる可能性」に関する注意喚起

【対策】

- デバイス機器の脆弱性や外部の通信機器による誤作動等に備えた対策

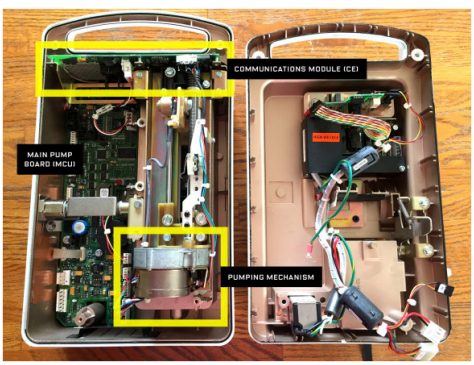
3. 最近の脅威事例
～2015年に報告された事例から～

情報家電・医療機器のセキュリティ事例

■ 2015年8月DEF CONにおいて、サムソン電子社のスマート冷蔵庫「RF28HMELBSR」に脆弱性が発見される。

- 冷蔵庫のインターネット通信機能におけるSSL証明書の検証処理に不備があり、中間者攻撃（MITM＝man-in-the-middle attack）が可能
- 冷蔵庫の扉の液晶パネルに搭載されたGmail Calendarの通信時、Googleサービスへのログイン情報が窃取される可能性

出展：PEN TEST PARTNERS LLP「スマート冷蔵庫と液晶パネル」
https://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/



■ 2015年4月セキュリティ研究者のBilly Rios氏が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を報告

※薬剤投与の人為的ミスを防ぐため、投与する薬や投薬量の設定が可能なシステム

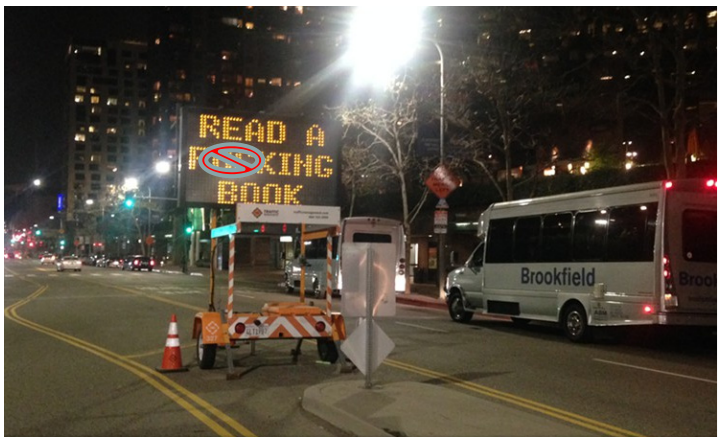
- 脆弱性を利用することで、インターネット越しにサーバ上の投与する薬や投薬量を改ざんする事が可能
- 認証機能が無いため、サーバから更にポンプ等へ不正アクセスが可能

（出展）WIRED「輸液ポンプ例」
http://www.wired.com/2015/04/drug-pumps-security-flaw-lets-hackers-raise-dose-limits/

電光掲示板セキュリティの事例

2015年1月ロサンゼルスのダウンタウンで交通情報を表示する電光掲示板がハッキングされたと報道される。

- Traffic Management Incorporated社（掲示板の所有者）の発表では、手口は不明だが、装置のある場所に侵入して書き換えたか、または、WiFi通信タイプためリモートから書き換えられた可能性もあり、原因不明



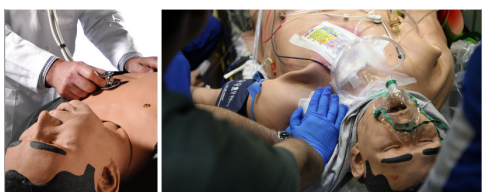
（出展）LA WEEKLY
http://www.laweekly.com/news/read-a-f-ing-book-street-sign-was-likely-a-hack-photos-5332229

その他のセキュリティ事例

■ 2015年9月 医療従事者の演習用に利用される人体シュミレータであるマネキン「iStan」に脆弱性が発見される。

※iStanは様々なシュミレータやデバイス、演習用シナリオを含み、ワイヤレスでコントロールできる医療用ロボット

- 総当り攻撃やDoS攻撃によって、シュミレータ内のペースメーカを停止させ、「死亡」状態とすることに成功



（出展）iStan「」CAE Healthcare
http://caehealthcare.com//images/uploads/brochures/iStan.pdf

■ 2015年8月BlackhatにおいてTrackingPoint社のスマート“ライフル”に脆弱性が発見される。

※ライフルのスコープにLinuxベースのコンピュータを利用し、Wi-Fi接続でスマホ等のアプリと連携させることで、風速や気温を入力し命中率を向上させる機能を持つ。

- 認証回避、暗号化の不具合等を利用して内部の情報の書き換えが可能。
- Tracking Point社はこの報告を受けホームページで、「Wifi機能を利用する際は100フィート（約30m）にハッカーが居ないことを確認すること」と表示（9月下旬現在は表示は消えている）

（出展）Tracking Point社のスマートライフル
http://tracking-point.com/precision-guided-firearms/precision-guided-semi-auto-556

4. 外部からの攻撃だけとは限らない

～ビッグデータへ情報が集約・蓄積されるIoT時代 内部からの攻撃に備えるセキュリティ対策～

自動車の情報セキュリティに関連する事例

【脅威の事例】

■解雇された従業員が遠隔イモビライザーを不正操作

→100台以上の自動車が使用不能（2010年3月米国テキサス州）

自動車販売店に解雇された従業員が別の従業員のIDとパスワードを使用し、Webサーバから遠隔イモビライザーを装着した自動車を使用不能にさせた事件

《使用不能の自動車の状態》

・自動車のエンジンがかからない

・警告ホーンが鳴り続け止められなくなる

※遠隔イモビライザー：電子キーを利用した自動車盗難防止機能を遠隔から操作できるシステム

自動車販売店は、ローン返済が滞った場合に遠隔イモビライザーを利用して自動車の使用を不能にさせるために装着していた。

遠隔イモビライザーによって使用不能になった自動車は、管理者が解除するまで使用不能な状態を解除することができない。

【対策】

・IDとパスワードの管理徹底

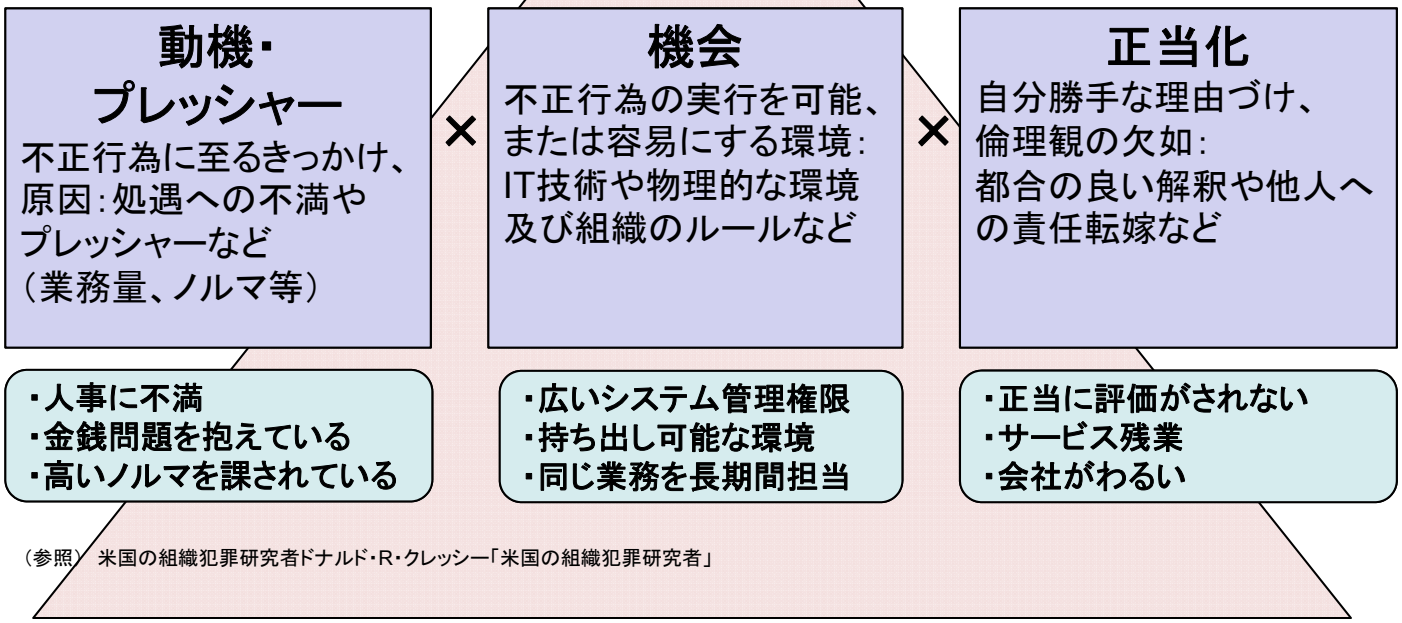
・内部者（退職者等）の管理

・職場環境の整備

今後、新しいサービスが発展してくることで、これまで想定していなかった脅威が発生する。

不正のトライアングル

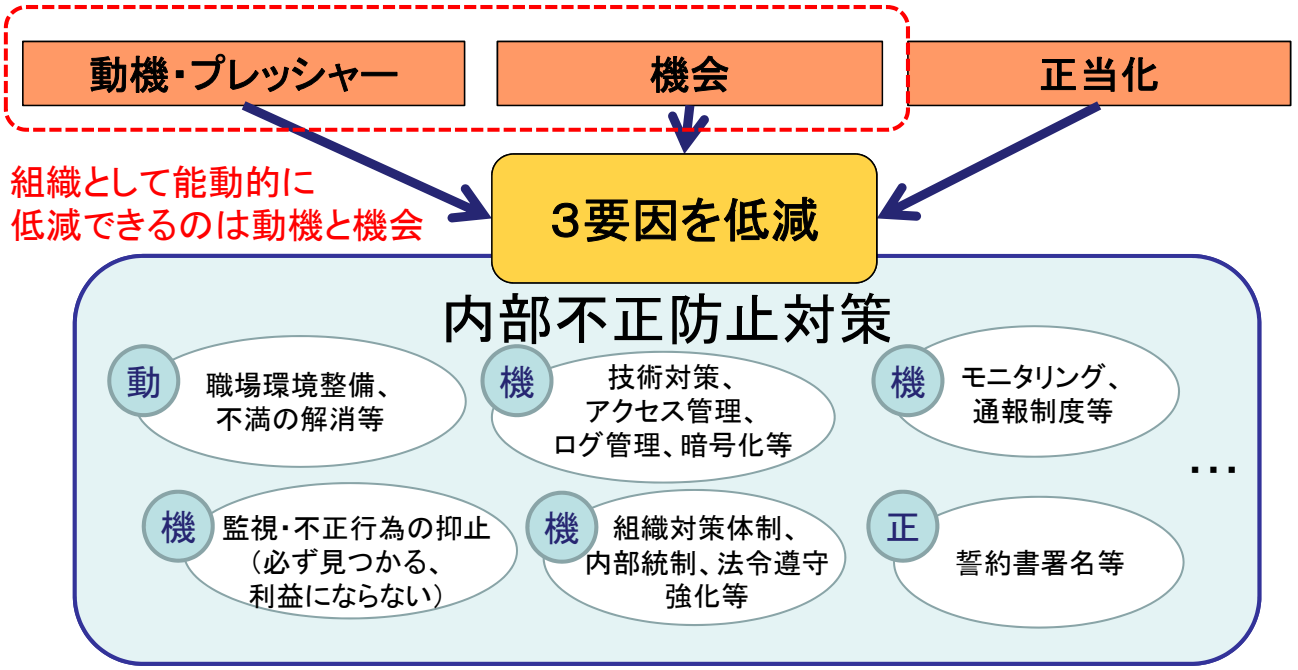
- 内部不正は「動機・プレッシャー」「機会」「正当化」の3要因が揃った時に発生する



（参照） 米国の組織犯罪研究者ドナルド・R・クレッシー「米国の組織犯罪研究者」

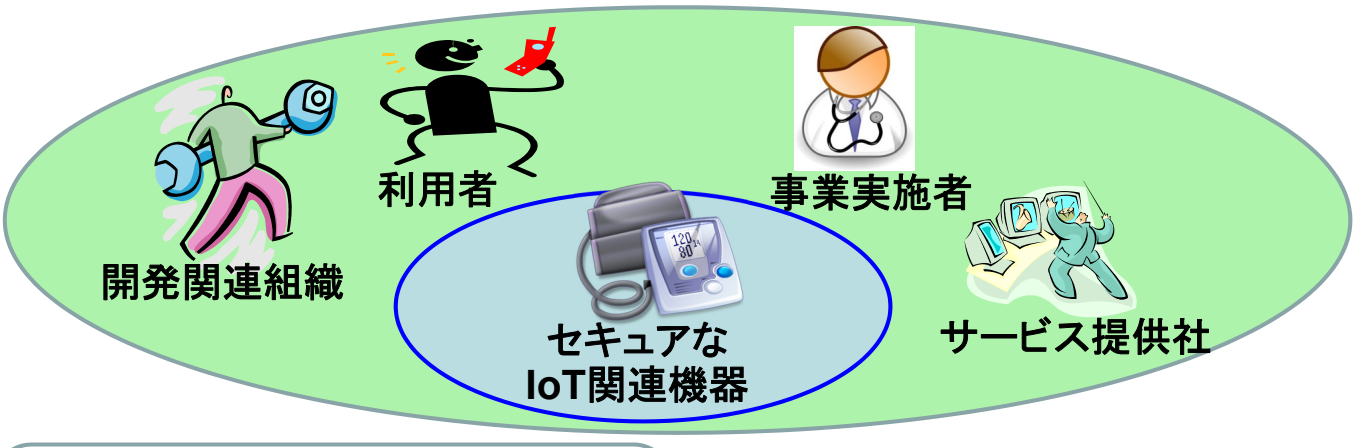
内部不正防止対策は３要因の低減

- 組織対策として重要なこと＝
  「動機・プレッシャー」と「機会」の低減



5. まとめ
～IoTセキュリティのこれから～

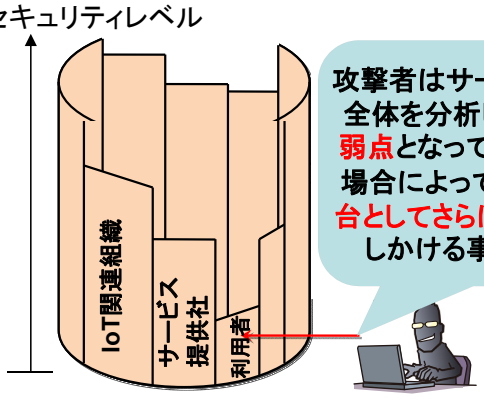
総合的＆継続的なセキュリティ対策を



樽の理論

何本もの樽材で組み合わせ、タガを締めた樽には、一番短い樽材の位置までしか水は入らない。それより長い樽材をどれほど高級なものにしたとしても、この結果は変わらない。

効果的なセキュリティ対策を実施するためには、組込み機器の開発関連組織のみならず、それに関わる組織・人の連携が必要



攻撃者はサービス・システム全体を分析した上で、**一番弱点**となっている所を狙う。場合によってはそれを**踏み台としてさらに内部に攻撃**をしかける事もあり得る。

＜IPAが提供する対策コンテンツ＞
～これまでのIPAの調査と開発成果から～

安全なシステム開発推進に向けたIPAの取組み

セキュリティ対策

- 調査、動向把握、開発方針・体制整備（ﾋﾞｼﾞﾈｽｲﾝﾊﾟｸﾄ分析含む）
- セキュアなシステムの設計
- セキュアプログラミング
- ソースコード診断
- テスト（ファジング等）
- 脆弱性診断（ﾍﾟﾈﾄﾚｰｼｮﾝ）
- 運用時対策
- 脆弱性対策

システムライフサイクル

1. 企画 → 2. 設計 → 3. 開発 → 4. 製造 → 5. 運用／利用 → 6. 廃棄

脅威、動向 ／ 脆弱性 ／ 攻撃

IPAの成果物

- ■制御システム利用者のための脆弱性対応ガイド
- ■自動車の情報セキュリティへの取組みガイド
- ■医療機器における情報セキュリティに関する調査
- ■情報家電向けガイド
- ■組込みシステム向けガイド
- ■生体認証導入、運用ガイド
- ■情報セキュリティ白書2015
- ■10大脅威
- ■内部不正防止ガイドライン
- ■開発者向け脆弱性実習ツール AppGoat
- ■ファジング活用の手引き
- ■「高度標的型攻撃」対策に向けたシステム設計ガイド
- ■安全なウェブサイトの作り方
- ■安全なSQLの呼び出し方
- ■セキュアプログラミング講座
- ■JVN、JVN iPedia、MyJVN
- ■ウェブ攻撃検出ツールiLogScanner
- ■WAF読本
- ■安全なウェブサイト運営入門
- ■ウェブ健康診断仕様
- ■5分でできる！情報ｾｷｭﾘﾃｨﾎﾟｲﾝﾄ学習

※下線が入っているIPAの成果物は、開発関連組織やサービス提供社だけでなく、事業実施者や利用者の方々にも参照していただきたい資料となります。

情報システムにおける セキュリティ対策コンテンツ(1/3)

対象:システムライフサイクル
2. 設計 3. 開発 4. 製造

- セキュリティ上の弱点(脆弱性)を作りこまないための教育
  - 学習によって脆弱性に対する理解を深める
  - サンプルアプリで実際に手を動かして脆弱性を知る
  - 「よくある脆弱性」に対するチェックを行う

学習の流れ

学習テーマ選択後の流れ

脆弱性原理解説 ▷ 演習 ▷ 影響解説 ▷ 対策方法解説 ▷ 脆弱性修正 ▷ 解答・修正例確認

ウェブアプリの脆弱性体験学習ツール
AppGoat

AppGoat ～突いてみますか？脆弱性！～

Androidアプリの脆弱性体験学習ツール
AnCole

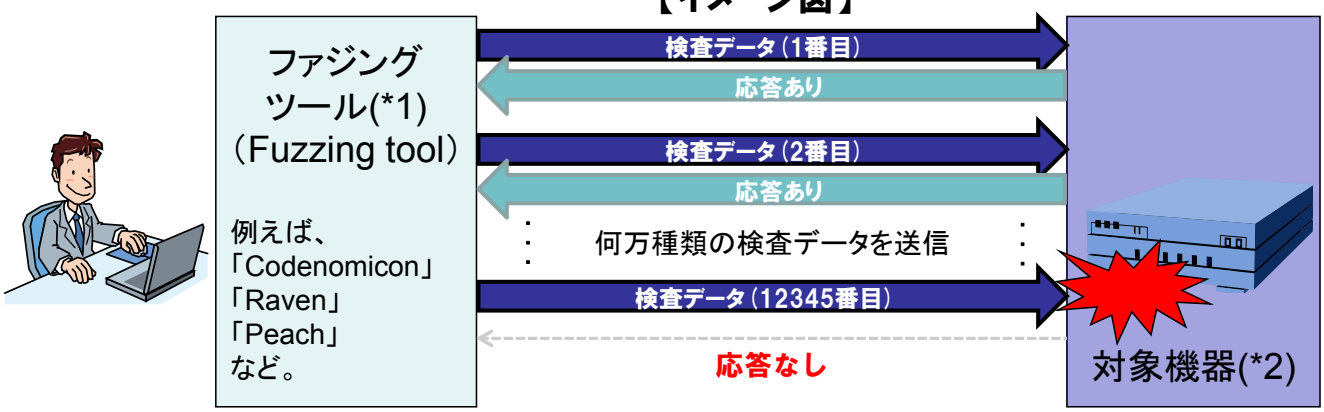
AnCole アンコール!
Android Secure Code Learning Tool

情報システムにおける セキュリティ対策コンテンツ(2/3)

対象:システムライフサイクル
2. 設計 3. 開発 4. 製造

- ファジング(英名:Fuzzing)活用の手引き
  - 何万種類もの問題を起こしそうなデータ(例:極端に長い文字列)を送り込み、対象製品の動作状態(例:製品が異常終了する)から脆弱性を発見する技術

【イメージ図】



IPAが実施したファジングでは、ルータの脆弱性を発見。他の組込み機器に対しても調査中。
IPAではこの調査結果や、ファジングの利用ガイド等も随時公開。

(*1): ファジングツールは、商用製品だけではなく、オープンソースソフトウェア、フリーソフトウェアも存在します。
(*2): この図では組込み機器を示していますが、ソフトウェア製品でも同様です。

情報システムにおける セキュリティ対策コンテンツ(3/3)

対象:システムライフサイクル
5. 運用／利用

■ 脆弱性情報データベース JVN iPedia

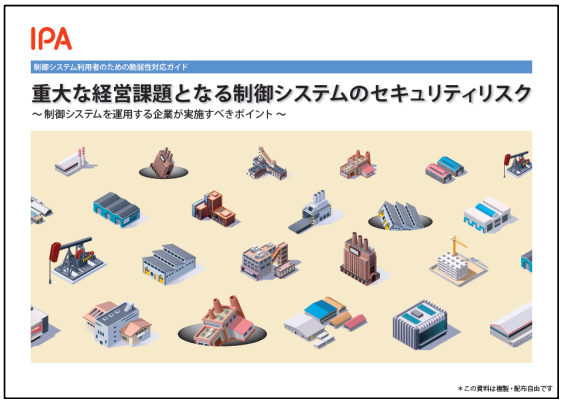
URL:http://jvndb.jvn.jp/
国内外の脆弱性対策情報を収集したディクショナリデータベース

- IPAが運営するサイト
- 国内ベンダーと連携をし、脆弱性対策情報を公開
- 海外の脆弱性DB(NVD)の情報を日本語翻訳して公開
- 約54,700件の脆弱性対策情報を登録

制御システム利用者 のための脆弱性対応ガイド

対象:システムライフサイクル
1. 企画

- 制御システムを利用されている企業の皆様が、制御システムを使い続けていくうえで、今後検討が必須となるセキュリティリスクと対策の考え方を掲載



A5サイズ、全30ページ

【想定読者】
- 制御システムを運用されている企業の**経営者**の皆様 / **経営企画**、リスク管理部門等の**リスク管理担当**の皆様
- 制御システムの**導入**及び**調達**を**担当**する皆様
- 制御システムの**運用・管理**に携わる**管理者**の皆様

【構成】
- 制御システムのリスク
- 制御システムに関して経営者がすべきこと
- 制御システムのセキュリティ対策のポイント

資料はIPAのホームページでご確認いただけます。(PDFデータ提供中)
→ https://www.ipa.go.jp/files/000044733.pdf

自動車の情報セキュリティへの取組みガイド

対象：システムライフサイクル
1. 企画

本ガイドは、自動車セキュリティの確保に向けた自社の取組みを把握すると共に、情報セキュリティへの取組みを強化する為の指針を示しています。

本ガイドは自動車のライフサイクル（企画・開発・運用・廃棄）に沿って検討すべき情報セキュリティへの15項目の取組みについて、具体的にどのようなことに取り組むべきかという事項と、自社がどの程度まで取り組めているかチェックするための「取組みレベル」をそれぞれ整理

ライフサイクル	セキュリティへの取組み
マネジメント（全体）	設計、実装時のセキュリティ対策、セキュリティ評価・デバッグ、利用者等への情報提供用コンテンツ等の準備
企画フェーズ	セキュリティに配慮した要件定義の策定、セキュリティ関連予算の確保、開発外部委託におけるセキュリティへの配慮、新技術に関連する脅威への対応
開発フェーズ	設計、実装時のセキュリティ対策、セキュリティ評価・デバッグ、利用者等への情報提供用コンテンツ等の準備
運用フェーズ	セキュリティ上の問題への対処、利用者や自動車関係者への情報提供、ぜい（脆）弱性関連情報の活用
廃棄フェーズ	廃棄方針の策定と周知

資料はIPAのホームページでご確認いただけます。（PDFデータ提供中）
http://www.ipa.go.jp/security/fy24/reports/emb_car/

医療機器における情報セキュリティに関する調査

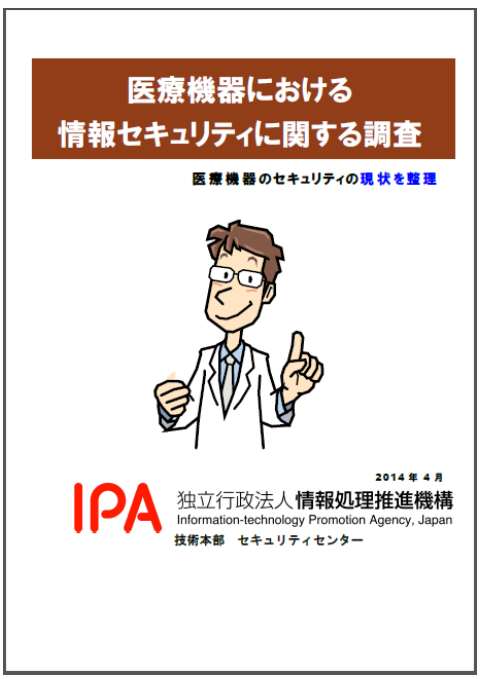
対象：システムライフサイクル
1. 企画

医療機器のセキュリティへの現状を整理

海外では2008年頃から情報セキュリティ上の脅威が顕在化しており、本調査では、事例として内外の脅威、医療機器における情報セキュリティへの取組みを収集

【調査方法】
(1) 医療機器セキュリティに関する脅威事例の調査
(2) 国内外の医療機器セキュリティに対する取り組みの調査

【国内外の医療機器セキュリティに対する取り組みの調査】
- 米国・欧州における医療機器のセキュリティに対する取り組みや関連する組織
- 医療機器のセキュリティに関する国際標準の動向
- 国内の医療機器のセキュリティに対する取り組みや関連する組織



資料はIPAのホームページでご確認いただけます。（PDFデータ提供中）
https://www.ipa.go.jp/security/fy25/reports/medi_sec/

情報セキュリティ白書2015

対象：システムライフサイクル
1. 企画

情報セキュリティ全般に関する状況をまとめた参考資料

本白書は、企業・組織のシステム開発者や運用者を対象に、情報セキュリティインシデントや攻撃の手口に関する現状、及び対策に役立つ情報を提供すること、また、パソコンやスマートフォンを使用する一般の利用者に対しても、身近にある情報セキュリティ上の脅威への認識を促すことを目的に制作しています。

第Ⅰ部　情報セキュリティの概要と分析
- 序章　2014年度の情報セキュリティの概況～10の主な出来事～
- 第1章　情報セキュリティインシデント・脆弱性の現状と対策
- 第2章　情報セキュリティを支える基盤の動向
- 第3章　個別テーマ

第Ⅱ部　情報セキュリティ10大脅威2015

付録　資料・ツール

「情報セキュリティ白書 2015」の印刷書籍版・電子書籍版は、以下のURLよりご確認ください。
https://www.ipa.go.jp/security/publications/hakusyo/2015.html

内部不正防止ガイドラインの参考資料
ソリューションガイドを活用した具体策の検討

対象：システムライフサイクル
1. 企画

①対策の指針、ポイントを理解する
リスクに対する具体的な対策を立案するためのヒントとする

組織における内部不正防止ガイドライン

（付録）「内部不正チェックシート」

資料はIPAのホームページでご確認いただけます。
→https://www.ipa.go.jp/security/fy24/reports/insider/

②具体的な実施策を立案する
製品・ソリューションの利用等を検討

JNSA※内部不正対策ソリューションガイド

※JNSA：特定非営利活動法人日本ネットワークセキュリティ協会

資料はJNSAのホームページでご確認いただけます。
→http://www.jnsa.org/result/2013/surv_acci/index.html

『高度標的型攻撃』対策に向けたシステム設計ガイド

対象：システムライフサイクル
2. 設計 → 3. 開発 → 4. 製造

企業等の組織においては、基本的なセキュリティ対策以外にも情報が外部に流出しないための対応を施す必要がある

入口突破されても攻略されない内部対策を施す

「高度標的型攻撃」対策に向けたシステム設計ガイド

内容1	・高度標的型攻撃の全容と対策導出アプローチ
内容2	・脅威の全体イメージ
内容3	・システム設計対策セット
内容4	・その他の活用場面

資料はIPAのホームページでご確認いただけます。（PDFデータ提供中）
→ http://www.ipa.go.jp/security/vuln/newattack.html

システム開発や管理業務、関連部署との相互調整を行う手引書(ガイドブック)として、本書をご活用ください

安全なウェブサイトの作り方

対象：システムライフサイクル
2. 設計 → 3. 開発 → 4. 製造

脆弱性対策を盛込んだ設計を

- **失敗から学ぶ**
  - IPAに届出られた脆弱性関連情報をもとに、対策をまとめたガイド
  - 脆弱性ごとに解説と「根本的解決」「保険的対策」を記載（11種類）
  - 「ウェブサイトの安全性向上のための取り組み」を記載（7項目）
  - 「失敗例」として解説と修正例について記載（6種類）
  - ウェブセキュリティの実装状況のチェックリストつき

2015/03/12 に新しくなりました

資料はIPAのホームページでご確認いただけます。（PDFデータ提供中）
→ https://www.ipa.go.jp/security/vuln/websecurity.html

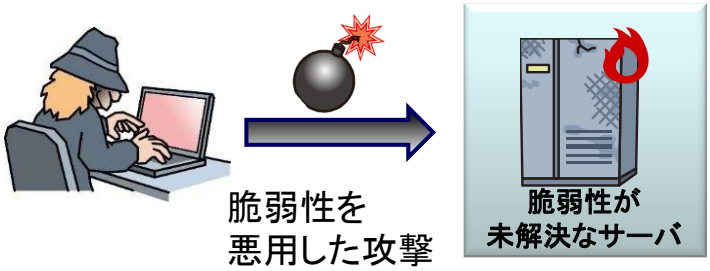
Windows Server 2003のサポート終了に伴う注意喚起

Windows Server 2003のサポートが2015年7月15日に終了しました。

サポート終了後は修正プログラムが提供されなくなり、脆弱性を悪用した攻撃が成功する可能性が高まります。

周辺ソフトウェアもサポートが順次終了していくため、あわせて対策が必要です。

サポートが継続しているOSへの移行検討とOS移行に伴う周辺ソフトウェアの影響調査や改修等について迅速な対応をお願いします。



- 業務システム・サービスの停止・破壊
- 重要な情報の漏えい
- データ消去
- ホームページの改ざん
- 他のシステムへの攻撃に悪用

会社の事業に悪影響を及ぼす被害を受ける可能性があります

詳しくは　IPA　win2003　検索

なおWindowsXPを利用されている方はサポートが継続しているOSへの移行検討をお願いします

情報セキュリティに関する新たな国家試験！

情報セキュリティマネジメント試験

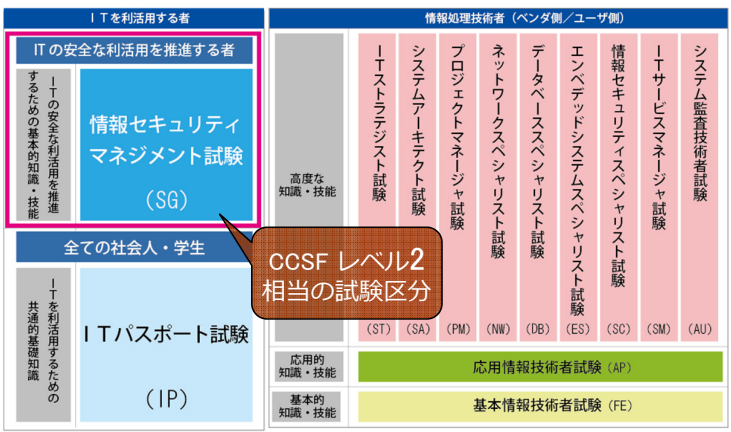
IPA

情報セキュリティマネジメント試験とは

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的スキルを認定する試験

試験の位置づけ

経済産業省所管の国家試験である**「情報処理技術者試験」の新たな試験区分として創設。**



試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	90分	多肢選択式 （四肢択一）	50問 50問	60点 （100点満点）
午後	90分	多肢選択式	3問 3問	60点 （100点満点）

実施時期（予定）

- 開始：**H28年度春期**
  （申込受付：2016年1月中旬開始予定）
- 春期・秋期の**年2回**
  （春期：4月第3日曜、秋期：10月第3日曜）

更に詳しく知りたい方へ

新試験がわかるパンフレット

職場の情報セキュリティ管理者育成に！

職場の情報セキュリティ管理者のための**スキルアップガイド**

情報セキュリティ**スキルアップハンドブック**

新試験の対象者像を踏まえ作成

ITパスポート試験

あなたのＩＴ力を証明する国家試験

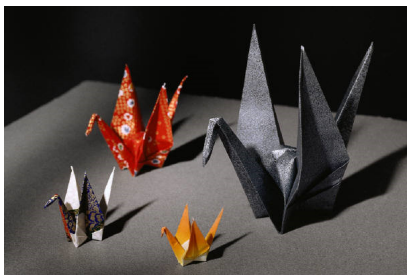
ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「iパス」は、ITを利活用するすべての社会人・学生が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。

ご清聴ありがとうございました！

本成果はIPAのWebサイトでダウンロードする事ができます。
https://www.ipa.go.jp/security/index.html



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