産業・制御システムセキュリティの理想と現実のギャップに目を向けよう

東京電機大学　教授
奈良先端科学技術大学院大学　客員教授

猪俣敦夫

本日の話題：仮題？と過大？と課題？

- 情報漏洩の脅威？「個人」情報と「システム」情報の違いを見直そう
- 「**仮題**」産業・制御システムとIoT、ごっちゃになっていない、同じセキュリティ対策が必要なの？
- 「**過大**」とても信頼できる第３者によるお墨付きは安心だけど、そんなにコスト（お金）も時間もかけられるの？
- 「**課題**」結論、何がハッピーなんだろうか？（セキュリティ投資は大切かもしれないけれど生み出される価値・利益は？）
- というあたりを今日の話題にしたいと思います。正直、私自身もまだ答えがないところもありますので、皆様と一緒に議論できれば幸いですm(_ _)m

自己紹介（猪俣敦夫）

- (一社)　JPCERTコーディネーションセンター　理事
- (一社)　公衆無線LAN認証管理機構　代表理事
- 京都女子大学、同志社女子大学（関西）非常勤講師
- 経済産業省　IoTセキュリティWG 座長
- ベネッセHD株式会社　情報セキュリティ監視委員
- (公財)　日本適合性認定協会(JAB) ISO/IEC17065 技術審査員
- 東京都足立区　情報公開・個人情報保護審議会委員
- IPAセキュリティキャンプ全国大会　講師
- NICT CYDER, SECHACK365委員
- 奈良県警察　サイバーセキュリティ対策アドバイザー
- 情報処理安全確保支援士（登録セキスペ申請中(笑)

。。。等諸々

- 専門分野：暗号（公開鍵暗号、楕円曲線）、情報セキュリティ人材育成
  - 関西では文部科学省の支援をいただき10年ほど情報セキュリティ人材育成を行ってきました。
- 奈良市在住（毎週、関西と東京を痛勤しています）

記憶から消えてしまった漏洩事件と消えない漏洩事件の違い？

- ベネッセ事件をはじめとして、個人情報漏洩は今や企業・組織の破綻を引き起こす大きなトリガ
  - 「子ども」の情報
  - 家庭内の「機微情報」
- 大学などの教育機関
  - 学生の個人情報は
    - 成績や家庭のことなど機微情報
  - 研究に関わる秘匿情報
    - 遺伝子ゲノム、特許案件
- 何もやっていなかった
  - では済まされない時代
  - クレーム？何も言い返せない
- 普段からの教育・啓蒙
  - 意識付けが大切
  - じゃぁ誰がやるの?
  - いつやるの?


ベネッセ情報流出、高裁に審理差し戻し　損害賠償訴訟

岡本玄　2017年10月23日22時49分

シェア　ツイート　ブックマーク　メール　印刷

0　list　0

情報
TTL

通信教育 大手ベネッセコーポレーション（岡山市）の顧客情報流出事件で、関西の男性が「自分や家族の個人情報がもれた」として損害賠償を求めた訴訟の 上告審 判決が２３日、 最高裁 第二小法廷であった。小貫芳信裁判長はプライバシー侵害を認めた上で、「審理が尽くされていない」と指摘。男性敗訴とした二審・大阪高裁 判決を破棄し、高裁に審理を差し戻した。

同社の情報流出をめぐっては、ほかに１万人以上が原告となる集団訴訟も係争中で、 最高裁 判決は影響を与えそうだ。

小貫裁判長は、男性やその子どもの氏名、住所などの個人情報は法的保護の対象で、流出はプライバシーの侵害にあたると指摘。「ベネッセの過失や男性の精神的損害の有無、程度などをさらに審理する必要がある」と結論づけた。

ベネッセの情報流出は、業務委託先の社員が約３５００万件の顧客情報を持ち出し、名簿業者に売却。ベネッセは対象者におわびの品として５００円分の金券を送った。一方、この社員は 不正競争防止法 違反で起訴され、 東京高裁 で実刑判決を受けた。 控訴審 判決ではベネッセ側の不備も認められた。

https://www.asahi.com/articles/ASKBR5J92KBRUTIL03N.html

たかが名前にメアド、されど個人情報

- 個人情報漏えいは、今や組織の存続すら危ぶまれる事態を招く脅威
  - 謝れば済むものではない。時間は何も解決してくれない
- 自分は注意しているから問題ない！
  - と思って油断している時をずっと攻撃者は見ている
- 何故、個人情報漏えいが発生するのか？
  - 「カネ」になる
    - クレジットカード（CVC/CVVコード, 有効期限) 5-30$/1 accout
    - 誕生日、旧姓、出生地
    - 医療、健康情報 その10倍以上-->保険詐欺、なりすまし
  - アカウントの連鎖
    - SNSアカウント-->フィッシング、スパム配信
    - 航空会社等のマイレージ→現金化
    - Webカメラ → 盗撮（今家ほとんどのラップトップPCにはカメラが標準搭載）
    - 同じIDやパスワード、誕生日などのデータ等・・・
- さて産業・制御システムのセキュリティも同じ脅威を考えるべきなのだろうか

私たちを取り巻く生活に必須の「何か」

- いわゆる重要インフラ、今や巨大なお化けのようなネットワーク
  - 電気・ガス・水道
  - 鉄道、バス、交通機関
  - テレビ、ラジオ、電話（固定・携帯・WiFi網）
  - そしてインターネット
- それぞれの領域にて、監視用のセンサや制御されるアクチュエータ等が厳密に管理され、連携して動作
- 大災害をはじめとした非常時以外に止まることはほとんどない
  - 二重化、冗長化、バックアップ
  - 特に「可用性」
- いわゆる産業・制御システムの世界

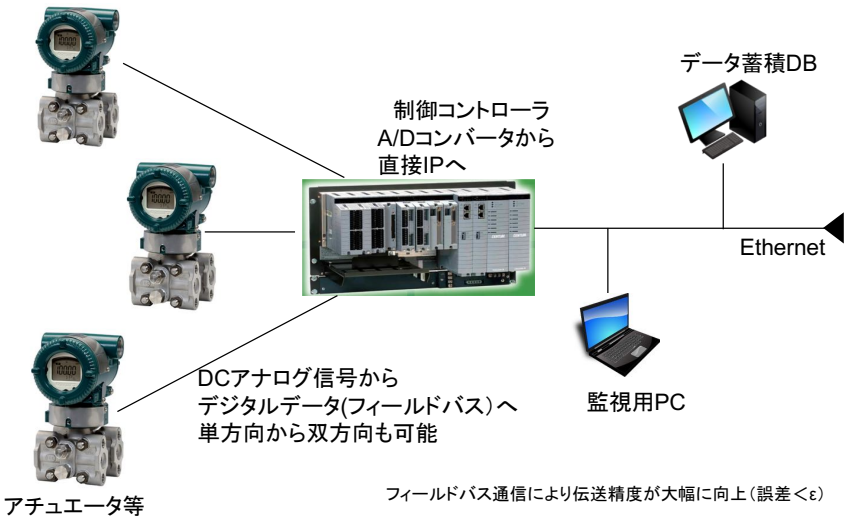
産業・制御システムの世界？

- 今や私たちの生活を下支えする重要インフラと切っても切り離せない
  - いわゆるパソコンではない。Raspberry Piでもない
- 事例
  - アクチュエータ制御（水道、ガス等）

横河電機様
差圧電送器(流量や圧力等)
出力信号　4-20mA DC

横河電機様
FCS(Field Control System)
通信は、Ethernet
IP, TCP, UDPなど当然喋れる
有線だけでなく無線も可能

アナログ伝送からフィールドバス通信へ



フィールドバス通信により伝送精度が大幅に向上（誤差<ε）

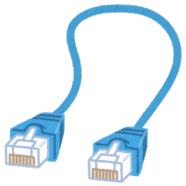
例：流量の二乗に比例してオリフィスで発生する差圧を差圧伝送器で計測し、4-20mA信号に変換後、制御システムに伝送

制御システムの分散化

- PLC(Programmable Logic Controller)だけでなくDCS（Distributed Control System)制御が当たり前、いわゆる分散コンピューティングと同じ世界
  - 送電網（電力グリッド）
  - 化学プラント、石油精製プラント
  - 信号機、環境センサ
- 制御コントローラ
  - 高性能PCサーバとほぼ同様
    - 高速CPU
    - 大容量メモリ
    - Linuxベース
  - Web(httpサーバ）I/F
    - いわゆるL7 C/Sモデルに近い
- Gigabit Ethernet
  - IP, TCP/UDP
- 冗長化
- レガシーな通信I/Fにも対応
  - Tリンク（シリアル、半二重等）
  - レガシー対応は重要な要素

富士電機様
制御コントロールステーション

DCSとPLC、実は微妙に違う



- DCS（Distributed Control System）
  - 計装分野が主（複雑なPIDをはじめとして詳細な制御が可）
  - 制御速度は1-2(sec)
  - 高額
- PLC（Programmable Logic Controller）いわゆるシーケンサ
  - 多方面で活用が可（いわゆるリレースイッチのお化け、ロジック制御、シーケンス制御、サーボ、監視等）
  - 安価
  - 制御速度は1-50(msec)と比較して高速
- しかし、ゲートウェイを介してみると外から見れば攻撃者にとっては何も変わらない。だから閉域ネットワークで構築するのが当たり前
  - L2/Ethernet
  - L3/IP
  - L4/TCP,UDP
  - L7/FTP, HTTP, etc...

クローズドならば安心だよね?

- 過去のレガシーな通信プロトコルだけでなく、普通にIPも喋る「普通」のサーバと同じ＝インターネットに対する脅威
- まさかインターネットに繋げるわけないじゃない、もちろんクローズドなネットワークだからうちは平気だよ
- 侵入ルート初期はまさか？？

HVAC
(Heating, Ventilation, and Air Conditioning)

05 Target Hackers Broke in Via HVAC Company

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

Target spokeswoman **Molly Snyder** said the company had no additional information to share, citing a "very active and ongoing investigation."

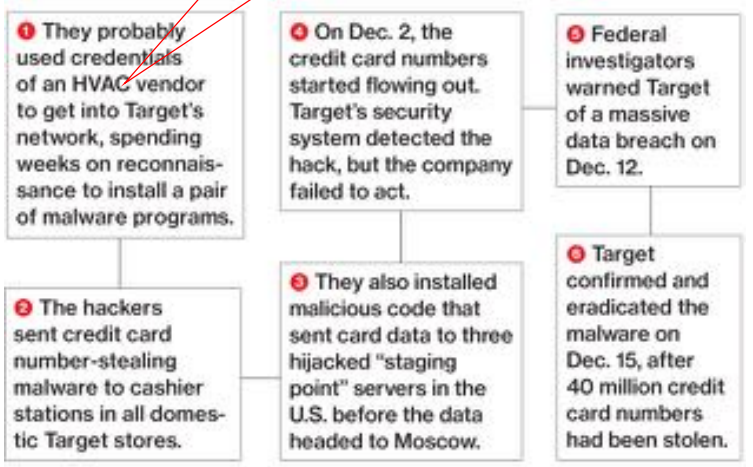
It's not immediately clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target's payment system network. But according to a cybersecurity expert at a large retailer who asked not to be named because he did not have permission to speak on the record, it is common for large retail operations to have a team that routinely monitors energy consumption and temperatures in stores to save on costs (particularly at night) and to alert store managers if temperatures in the stores fluctuate outside of an acceptable range that could prevent customers from shopping at the store.

"To support this solution, vendors need to be able to remote into the system in order to do maintenance (updates, patches, etc.) or to troubleshoot glitches and connectivity issues with the software," the source said. "This feeds into the topic of cost savings, with so many solutions in a given organization. And to save on head count, it is sometimes beneficial to [illegible] vendor to support versus train or hire extra people."

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

For Target via HVAC

本来、顧客情報システムと管理システムのネットワークは分離されるべきだが。。。



引用元 http://ivebeenmugged.typepad.com/my_weblog/2014/03/target-questions.html

研究・教育という金言の下

- 実験サーバを公開するのでグローバルアドレス下さい
  - 研究を遂行することは重要、問題なし。
- ポートは（使うか分からないけど）80だけじゃなくて22, 443, ・・・、面倒だからwell-knownじゃないポートたくさん、あとTCP/UDP全て通るようにしておいて下さいね
  - あとで面倒だし全部空けておいた方が楽。
- 管理者はよく触る学生のXX君にしておこう
  - （最近の）システムよく知らんし、教育的見地から学生に任せることは良い、ドヤ顔
- テレビ会議システム使うからたくさんポート空けてね。これ重要な会議に使うから必須ね
  - あの先生に関わると厄介だし、責任は我々じゃないし空けとこか。まぁ売り物システムだし問題ないよ（謎の自信

- 今日いらしている某ひら先生。どうすればいいの？

起こるべくして起きる…

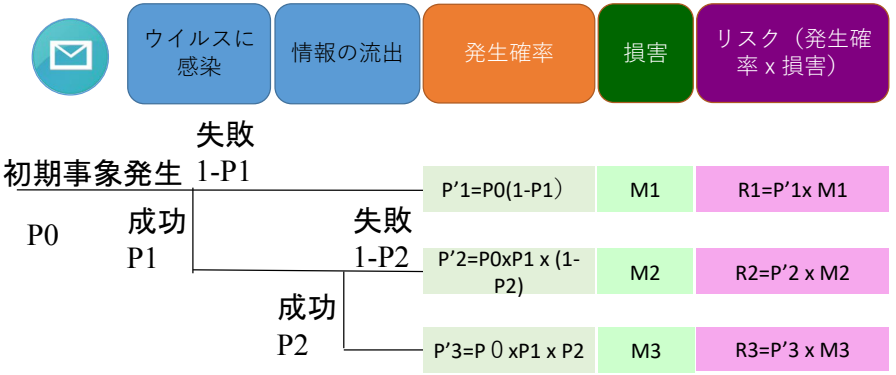
- 大学ならではの自由でオープンなネットワーク環境
  - FWで全てを囲むことは研究活動の大きな障壁
    - 教育・研究に必要とあればグローバルIPアドレスは提供して当然
    - DMZに設置しる!なんて面倒なこと言わない
  - 構築した人以外分からない多くの謎鯖（kernel改変、まるでbotな謎サーバ、アプリなんでもあり・・・）
- セキュリティリテラシを学んでいない教員が多いことはもはや当たり前
  - 上原哲〇郎先生の叫びが常に聞こえる・・・
    - インシデント発生の対応の遅さ
    - 状況の深刻さの認識不足
    - 他人任せ、学生任せのWebサーバ、脆弱性のあるCMS導入
    - 忘れ去られ放置された研究用サーバ、山盛りラズパイなどなど

そんな私達のために IPA制御システムセキュリティリスク分析ガイド

1. セキュリティ対策におけるリスク分析の位置付け
2. リスク分析の全体像と作業手順
3. リスク分析のための準備作業
4. リスク分析の実施
   1. 資産ベースのリスク分析
   2. 事業被害ベースのリスク分析
5. リスク分析結果の解釈と活用法
6. セキュリティテスト
7. 特定セキュリティ対策に対する追加基準

Whats? イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

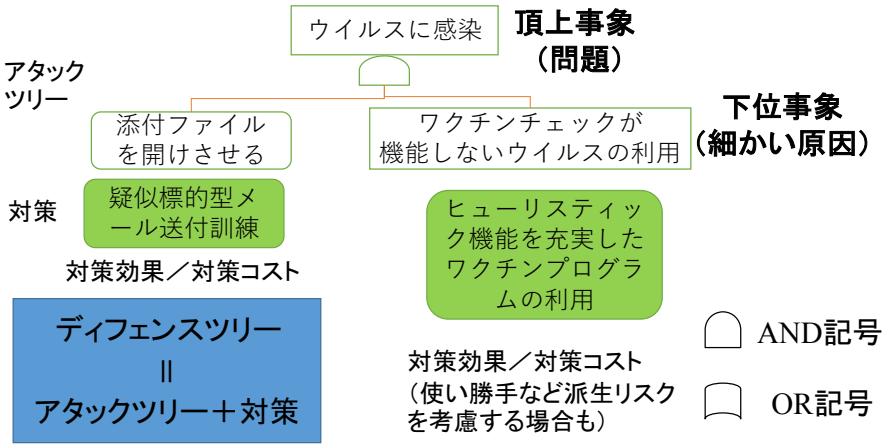


RT=R1+R2+R3

佐々木良一先生：講義資料より引用

Whats? ディフェンスツリー分析

- 攻撃に対しトップダウンにその要因を分析するアタックツリー分析に対策を加えたもの



佐々木良一先生：講義資料より引用

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）
1	ポーランドの鉄道におけるトラックポイントの不正操作	鉄道	ポーランド	2008 年 1 月	路面電車システムがハッキングされ、4 両の車両が脱線し、12 人の負傷者を出した。	14 歳の少年が、テレビのリモコンを改造したコントローラを用いて、路面電車システムに対してハッキングを行い、ポイント切替機を不正に操作した。
2	スマートメーターを対象としたサイバー攻撃	電力	米自治領プエルトリコ	2009 年	攻撃を受けた会社のスマートメーターを配置した地域内で、電力消費記録設定が改ざんされた。	攻撃者はインターネット上で見つかったツールを利用し、メータ管理を模取りし、プログラムを変更することでデータを改ざんした。
3	ウラン濃縮施設の遠心分離機における Stuxnet 感染	電力	イラン	2010 年 11 月	ウラン濃縮施設の遠心分離機がマルウェアに感染し、約 8,400 台の遠心分離機が停止した。	USB メモリを介して、マルウェア（ワーム）Stuxnet に感染。Stuxnet は、周波数変換装置を制御する PLC に侵入し、周波数を変え回転速度を通常よりも上げたり下げたりすることで、最終的に遠心分離機を破壊した。
4	ロンドンオリンピックの電力系統への DoS 攻撃	電力	英国	2012 年 7 月	オリンピック開会式（2012 年 7 月 27 日）の際に、照明システム（電力系統）への DoS 攻撃を受けたが、実際の被害には及ばなかった。	照明システム（電力系統）への DoS 攻撃が 40 分間続き、北米や欧州の 90 の IP アドレスから 1,000 万のアクセスがあった。
5	世界的大手の石油企業におけるワークステーションへの攻撃	石油	サウジアラビア	2012 年 8 月	世界的大手の石油企業の約 30,000 台のワークステーションがマルウェアに感染し、コンピュータ上のファイルが消去され、1 週間以上にわたって社内ネットワークを停止させられた。幸いにも、石油生産はネットワークが独立したシステムになっていたため影響を受けなかった。	ハッカーグループによる Shamoon と呼ばれるマルウェアを用いた攻撃によるものであった。
6	尖閣諸島問題等と関連したとみられるサイバー攻撃	政府・行政機関等	日本	2012 年 9 月	総務省統計局、政府インターネットテレビ等、少なくとも 11 のウェブサイトが一定の間、閲覧困難となった。また、裁判所や東北大学病院等、少なくとも 8 のウェブサイトが、中国の国旗等の画像や尖閣諸島は中国のものである旨の文章等が表示するよう改ざんされた。	中国のハッカー集団「紅客連盟」の掲示板等において、攻撃対象として日本の行政機関や重要インフラ事業者等が掲示されたほか、中国の大手チャットサイト「YY チャット」等では、最大 4 千人が参加し、攻撃予告や攻撃ツール等に関する書き込みがなされた。

IPA制御システムセキュリテ

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）
18	ドイツの原子力発電所におけるマルウェア感染	電力	ドイツ	2016 年 4 月	原子力発電所で、検査料棒を操作しているコンピュータがマルウェアに感染しているのが発見された。マルウェアが発見されたコンピュータは、インターネットに接続していなかったため、マルウェアが活動を始めることはなく、発電所の運転に影響はなかった。	3 基の原子炉のうち、稼働中の B 号機のコンピュータから、PC を遠隔操作できる W32.Ramnit と、PC 内部のファイルを盗み取る Conficker という 2 種類のマルウェアが、発電所の技師により発見された。また、原子炉の操作システムを管理している場所から離れた別のオフィスでは、マルウェアに感染した USB メモリ 18 本が見つかった。なお、Conficker と W32.Ramnit は、どちらも USB メモリ経由で拡散する。
19	サウジアラビアの空港、政府機関への攻撃	航空	サウジアラビア	2016 年 11 月	民間航空総局の事務管理システムの PC 数千台が破壊される被害が発生、業務が数日間停止した。 運航や空港業務、航空システムには影響は出ていない。 少なくとも 8 つの政府系組織で被害が確認された。	マルウェア Shamoon の新型が攻撃に使われた。Shamoon は、起動時に読み込まれるマスターブートレコードを消去し、コンピュータを機能不全にする。
20	サンフランシスコの交通システムにおけるランサムウェア感染	交通	米国	2016 年 11 月	サンフランシスコの交通公社で、最大 2,112 台のコンピュータがランサムウェアに感染し、料金徴収が不能になった。電車やバスの運行自体には影響なく、市営鉄道の改札を開放して対応し、3 日後に完全復旧した。	コンピュータがランサムウェアに感染し、ハッカーらは復号鍵と引換えに 100 ビットコインを要求し、支払わなければ盗んだ 30GB のデータを公開するとも脅迫したが、内部調査の結果データ窃取はハッカーのハッタリと判断し、脅しを無視した。感染経路は従業員によるメールの添付ファイル／ポップアップ／リンクのクリックと見られる。
21	米国最大の病院における ランサムウェア感染	医療	米国	2017 年 4 月	米国で最大規模の病院グループで、IT 障害のため 136 件の手術と数百件のがん患者の化学療法の予約をキャンセルする事態が発生した。抗がん剤を処方するシステムや医用画像情報システムが使用不能になったほか、血液検査等も不能になった。遠隔で画像を確認することもできなくなった。	WannaCry（ランサムウェア）の感染が原因であった。なお、同病院では、セキュリティに問題がある Windows XP が現役で使われていた。
22	日本国内の自動車の生産システムにおけるランサムウェア感染	製造（自動車）	日本	2017 年 6 月	自動車の生産工場でコンピュータが WannaCry に感染しているのが発見され、1 日操業を停止した。他工場への影響はなく、同工場も翌日には操業を再開した。	生産ラインを制御するシステムが WannaCry に感染した。 5 月に世界中で WannaCry 感染が報告されたのを受けて対策を図めていたが、完全に防ぐのは難しいことが改めて示された。
23	オーストラリア ヴィクトリア州の交通関連のカメラにおけるランサムウェア感染	交通	オーストラリア	2017 年 6 月	ヴィクトリア州で、159 台のスピード違反取り締まりカメラと交差点監視カメラが、WannaCry に感染した。感染により断続的に再起動を繰り返す状態が発生した。7,500 件の違反切符について一旦取り消すと発表した。	保守作業用に持ち込まれた USB メモリによって WannaCry に感染した。
24	世界的物流会社の子会社におけるマルウェア感染	物流	オランダ	2017 年 6 月	世界的物流会社の子会社のグローバルな業務システムがサイバー攻撃を受け、業務と通信が大きな影響を受け、顧客へのサービスと請求で広範な遅れが発生した。更に、取引高の減少によって売り上げが減少した。	Petya（マルウェア、NotPya と呼ばれている）がウクライナの税務ソフトウェアソリューションに仕込まれた後、同社がウクライナで営業しているほか、被害に遭ったソフトウェアを使用しているため、Petya がグローバルネットワーク全体に侵入し、データを暗号化した。

IPA制御システムセキュリティ分析ガイドより引用

ムムム、気を取り直し…

- 情報システム（いわゆるIT）と制御システムで考えるべきセキュリティって何が違うんだろう？

- という解を見つけるためにお約束のドキュメントそれがNIST SP
- NISTのSP（Special Publication)かFIPS（Federal Information Processing Standard）

- NIST SP800-82
  - Guide to Industrial Control Systems (ICS) Security
    - SCADA (Supervisory Control and Data Acquisition) 計装、レガシー
    - DCS (Distributed control systems)
    - Other control system configuration such as PLC
- NIST SP800-53
  - Recommended Security Controls for Federal Information Systems
    - Management controls
    - Operational controls
    - Technical controls

SP800-52
Guide to Industrial Control Systems (ICS) Security

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
性能要件	リアルタイム不要 応答は一貫していること ハイスループット必須 大きな遅延とジッターは許容 重要な緊急相互作用が少ないこと セキュリティに必要な程度に厳格なアクセス制限を実装できること	リアルタイム 応答は緊急を要する 中程度のスループットで可 大きな遅延やジッターは不可 人その他の緊急相互作用への応答が重要 ICS へのアクセスは厳重に制限されるが、マンマシンインタフェースを阻害・干渉しない
可用性（信頼性）用件	リブート等の応答は可 可用性の欠点はシステムの運用要件に応じて許容されることが多い	プロセスの可用性要件によりリブート等の応答は不可 可用性要件から冗長システムが必要となる場合あり 停止は数日又は数週間前にあらかじめ計画・予定 高可用性要件により徹底的な展開前試験が必要
リスク管理要件	データを管理 データの機密性と保全が肝要 フォールトトレランスはさほど重要でない（瞬時のダウンタイムは重大リスクでない） 重大なリスク影響は業務の遅延	物理世界の制御 人の安全が肝要、プロセスの保護はその次 フォールトトレランスが不可欠、瞬時のダウンタイムも不可 重大なリスク影響は法令不履行、環境への影響、人命・装備品・生産喪失
システム運用	システムは一般的 OS 上で使用 アップグレードは自動展開ツールを利用するので容易	まちまちで専用の OS を使用する場合あり、セキュリティ機能はないことが多い 専用制御アルゴリズムと修正済みハードウエア/ソフトウエアが関係するため、ソフトウエア変更は慎重を要し、通常ベンダーが担当
リソースの制約	システムはセキュリティソリューション等の追加サードパーティアプリケーションに対応する十分なリソースを運用	システムは所期の産業プロセスに対応するようにできており、追加セキュリティ機能に対応する十分なメモリや演算リソースはない

NIST SP800-52(JPCERT翻訳版) https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf

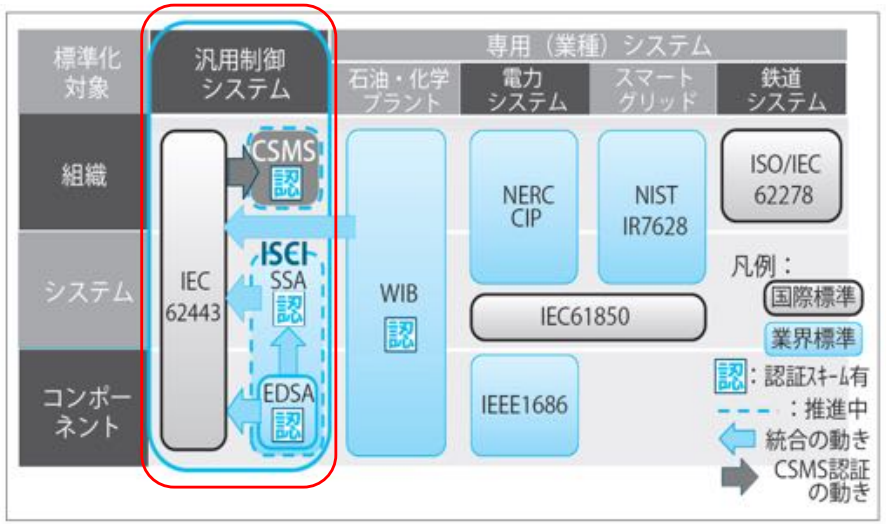
ここでもTime To Liveは大きな意味が？

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
通信	標準通信プロトコル プライマリ有線ネットワークで局所的に無線機能あり 一般的 IT ネットワーク規範	多数の専用・標準通信プロトコル 専用有線・無線（無線及びサテライト）を含む数種の通信メディアを利用 ネットワークは複雑で、制御エンジニアの専門知識を必要とすることあり
管理変更	ソフトウエア変更は良好なセキュリティポリシー・手順に従いタイムリーに実施。手順は自動化されていることが多い。	ソフトウエア変更は、システム全体を通じて徹底的に試験・展開し、制御システムが保全されるようにする。ICS 停止の多くは、数日又は数週間前にあらかじめ計画・予定が必要。サポートが終了した OS を使用している場合あり
管理サポート	多様なサポートスタイルあり	サービスサポートは通常 1 業者のみ
コンポーネントの寿命	3 年～5 年	10 年～15 年
コンポーネントの所在場所	通常ローカル所在で、アクセスが容易	コンポーネントは隔絶された遠隔地にあり、アクセスにはかなりの物理的労力が必要

NIST SP800-52(JPCERT翻訳版) https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf

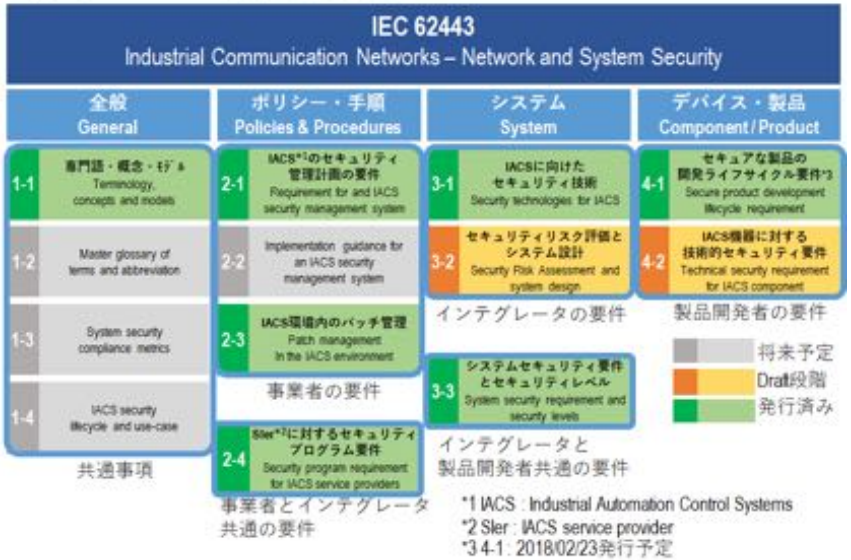
- あれ？（よく聞く）IoTデバイスってすぐ捨てるよね、捨てちゃうよね。

制御システム分野の標準化動向



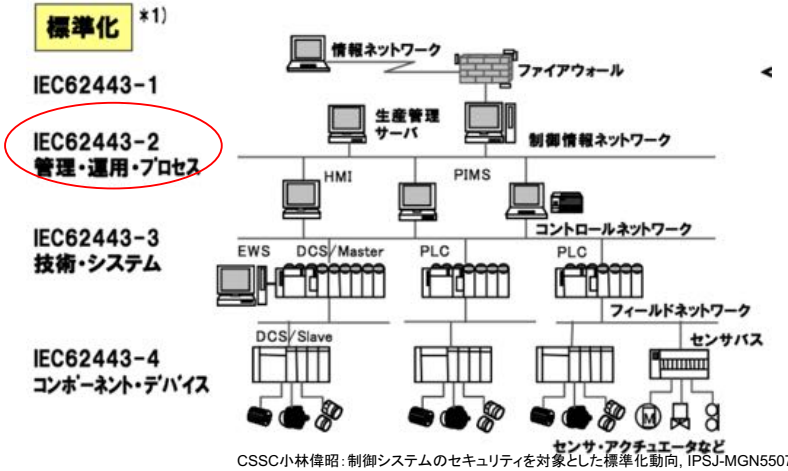
小林偉昭：制御システムのセキュリティを対象とした標準化動向, IPSJ-MGN550709

IEC62443: 構成と発行状況



http://controlsystemlab.com/index.php/iacs_security_002/

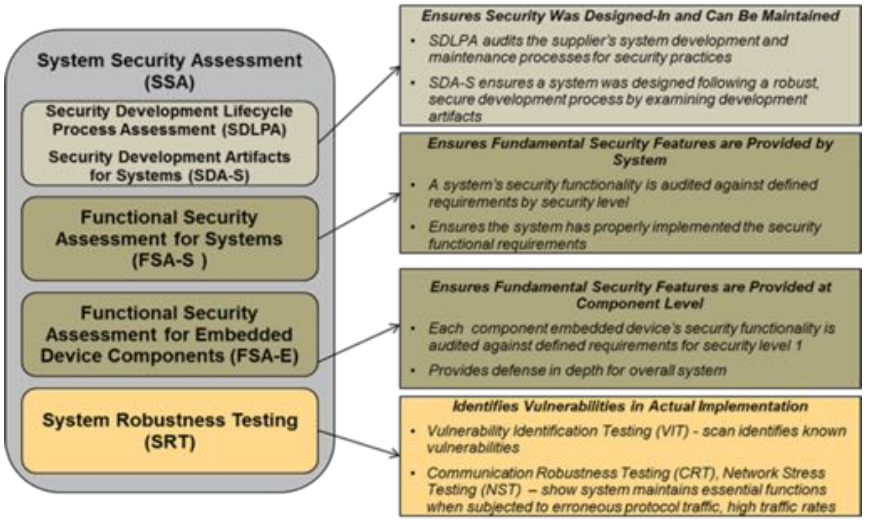
ISMSに対して
CSMS(Cyber Security Management System)
ISA-62443-2



CSSC小林偉昭：制御システムのセキュリティを対象とした標準化動向, IPSJ-MGN550709

いわゆるISMS(情報セキュリティマネジメントシステム)の考え方を制御システムにも導入
産業・制御システムにも実は適切な運用・管理・プロセスが重要

SSA(System Security Assessment)
ISA-62443-3-3, 4-1, 4-2
意外と結構細かい規定が山ほどある…



ISA Secureより

事例：CSSC-CL（制御システムセキュリティセンター認証ラボラトリ）

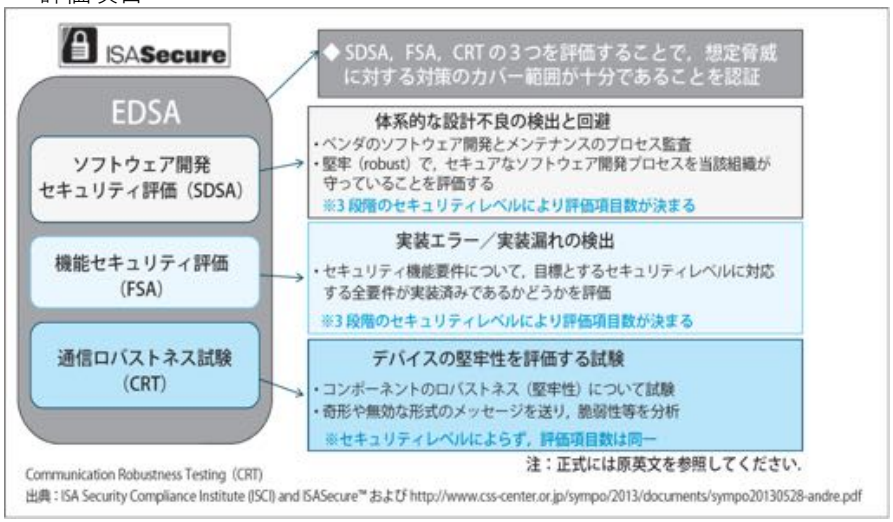
制御システムセキュリティセンター認証ラボラトリ http://www.cssc-cl.org/jp/aboutus/index.html

ISO/IEC 17065 プロセスが大切

- 適合性評価-製品、プロセス及びサービスの認証を行う機関に対する要求事項」
  - その能力は、対象製品の評価(試験、検査、関連システム審査等)並びに評価結果に基づく認証業務に従事している個々の要員の職務遂行能力、個々の評価設備の能力及び各評価遂行能力(適切な評価方法の選択等)
- 第三者として製品を認証する能力があると認められることから、第一者(製品を供給する人)や第二者(製品を購入する人)から信頼され、かつ社会的にも信頼される
  - そのような認定された製品認証機関から認証された製品は、認証の基準を満足する製品であることが保証され、消費者は安心してその製品を購入できる

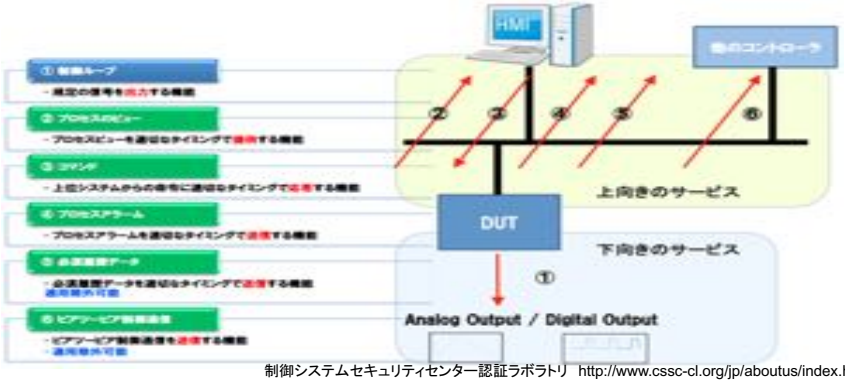
EDSA認証

- 制御機器のセキュリティ保証（スキームオーナはISCI）
  - ISO/IEC62443標準フレームワークに基づきISASecure® EDSA認証の仕様を開発
- 評価項目



評価試験はどんなことを？

IEEE 802.3(Ethernet)
ARP
IPv4
ICMPv4
UDP
TCP



制御システムセキュリティセンター認証ラボラトリ　http://www.cssc-cl.org/jp/aboutus/index.html

どのような試験が行われるのか？

- いわゆるfuzzing（ファジング）テスト

表 16 - IPv4.T08：無効な送信元 IP アドレスを持つ NPDU の拒否

テスト ID	IPv4.T08
テスト名	無効な送信元 IP アドレスを持つ NPDU の拒否
テストの説明	第 4.2.4.5.2 項の M9 又は M10 に照らして無効である送信元 IP アドレスを持つ ICMPv4 PDU を送信する。
参照要求事項	第 4.2.4.5.2 項，M9 又は M10
テストタイプ	基本的なロバストネス：PDU の内容の意味規則違反
テストステータス	必須
DUT に期待される動作	無効な送信元 IP アドレスを指定した NPDU を受信した DUT は，それを無視し，通知をせずに破棄する。また，送信元を DUT とした NPDU を DUT が送信していない場合に，受信した NPDU で指定されている送信元 IP アドレスが DUT のものである場合も，同様の処理を実行する。
テストの目的	受信した NPDU の送信元 IP アドレスが明らかに無効である状況で DUT の保護手段が示すロバストネスを精査する。
テスト構成	IPv4 アドレッシング又は IPv6 アドレッシングのいずれかを使用する。スイッチを設けた基本のネットワークで TD と DUT を接続する（[CRT.Test_configuration_1] で規定）。すべての仲介ファイアウォールで，DUT による ICMP エラーレポート機能を有効にすることが望ましい。
テスト手順	第 4.2.4.5.2 項の M9 又は M10 に照らして無効である送信元 IP アドレスを持つ IPv4 NPDU を TD から送信し，任意の送信先 IP アドレスに宛てた DUT からの応答 NPDU をリッスンする。TD は，DUT からのあらゆる応答を監視できる。
DUT に期待される応答	DUT が必須サービスを適切に維持し続ける。
結果	合格又は不合格
備考	

表 17 - IPv4.T09：未定義のプロトコルタイプ又は未実装と考えられるプロトコルタイプを参照する NPDU の処理

テスト ID	IPv4.T09
テスト名	未定義のプロトコルタイプ又は未実装と考えられるプロトコルタイプを参照する NPDU の処理
テストの説明	プロトコルタイプのフィールド値が DUT では未定義であるか又は未実装と考えられる ICMPv4 PDU を送信する。
参照要求事項	
テストタイプ	基本的なロバストネス：PDU の内容の意味規則違反
テストステータス	必須
DUT に期待される動作	DUT が，無効なプロトコルタイプ又は未実装のプロトコルタイプを指定した NPDU を受信して応答する。この応答では，送信先到達不能の理由コードの値を 0x02（プロトコル到達不能）とした ICMPv4 送信先到達不能 PDU を伝達する NPDU を使用する。ただし，DUT はこのような受信 NPDU を無視し，通知なしで破棄してもよい。
テストの目的	受信した NPDU のプロトコルタイプ値が DUT で無視されることが想定できる状況で，DUT の保護手段が示すロバストネスを精査する。

ISA Secureより引用　http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification-(In-Japanese)

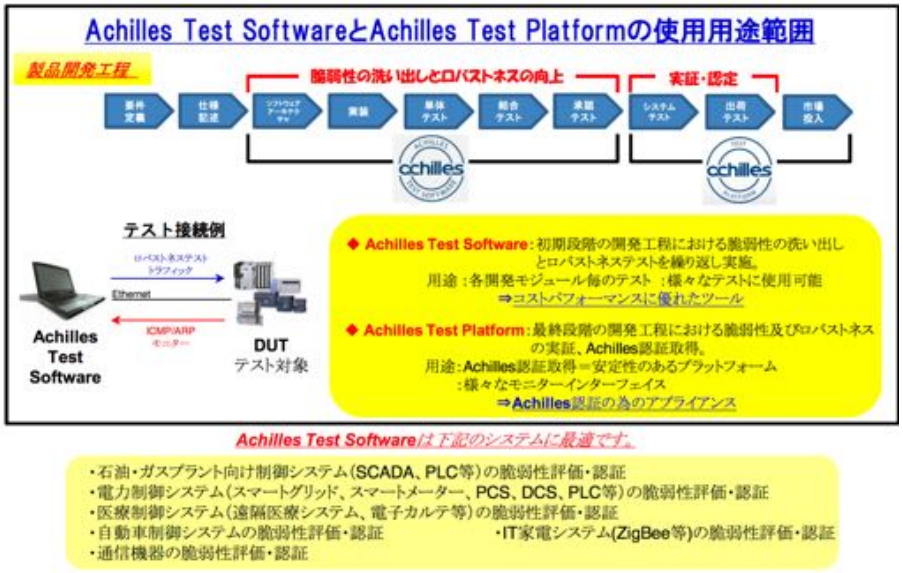
制御システムはIPv6が当たり前の世界

表 24 - TCP.T18：高負荷の下でのサービスの維持：初期 SYN フラッディング

テスト ID	TCP.T18
テスト名	高負荷の下でのサービスの維持：初期 SYN フラッディング
テストの説明	有効と思われる多数の TCP TPDU を DUT に送信する。この TCP TPDU は，TCP 接続を開始した後，その接続の確立（完全な 3 ウェイ TCP ハンドシェイク）に失敗する。これにより，DUT の接続状態ストレージリソースで障害を引き起こすことを試みる。TPDU フラッディング速度は，飽和テストではなく，高負荷テストになるように選択する。追加の要求事項については，[CRT.Rate_limiting] を参照。
参照要求事項	要求事項 TCP.R18
テストタイプ	負荷ストレス
テストステータス	必須
DUT に期待される動作	DUT は，受信した TCP TPDU のフラッディングから自身を保護する。この TCP TPDU は，接続のネゴシエーションを開始し，3 段階の接続ネゴシエーション処理をハングしたままにして，完了を待機する状態に置く。
テストの目的	一時的で大量の TCP 接続を受信し，これに耐えて，この状態から回復する DUT の能力を評価する。この TCP 接続は，SYN フラッディング攻撃と呼ばれる攻撃によって，半オープン状態になっているものである。
テスト構成	IPv4 アドレッシング又は IPv6 アドレッシングのいずれかを使用する，スイッチを設けた基本のネットワークで TD と DUT を接続する（[CRT.Test_configuration_1] で規定）。DUT ベンダは，保護機能の起動を想定していない速度の上限値を指定しなければならない。
テスト手順	DUT の TCP ポートに宛て，現在未使用になっている IP 送信元アドレスと TCP 送信元ポートの対を設定した多数の有効な TPDU を TD から送信する。この TPDU では SYN フラグを設定する。この送信によって発生する，SYN と ACK の両方を設定した TCP TPDU に TD は応答しない。IP 送信元アドレスの 1 つとして，ブロードキャスト IP アドレスを使用しなければならない。
DUT に期待される応答	DUT が必須サービスを適切に維持し続ける。
結果	合格又は不合格
備考	このフラッディング中，DUT の動作を調査するために，TD は他の TCP 接続の確立と使用を試みることができる。これらの調査用 TCP 接続には，NULL ではないトラフィックを配置する。

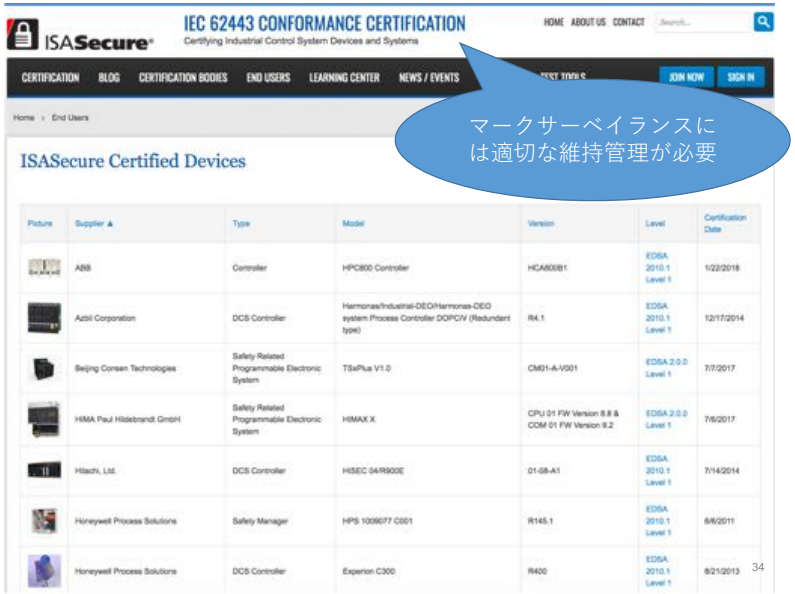
ISA Secureより引用　http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification-(In-Japanese)

有名なテスト環境の1つ（H/WもS/Wもある）



Achilles Test Software(ATS) https://www.direx.com/assets/achilles_ats_revd.pdf

頑張ればきちんとしたお墨付きがもらえる



認証取得は信頼の証？

- 産業・制御システムは、これまで見てきたように私たちの生活に直結したものであることが多い、あるいは製品そのものの価値を高めるためには厳格に管理された認証取得プロセスを経ていることは大変重要
  - 認証取得はコストも、そして時間もものすごくかかる根気の要る作業
- 根気 vs お金 vs 仁義
- 生活に密着？→いわゆるIoTの世界はどうなのだろう
- 世の中の動向はどうなのだろうか

JNSA2017セキュリティ10大ニュース

【第１位】10月4日　総務省が「IoTセキュリティ総合対策」を発表
～ 攻撃者が嬉々とするIoT機器の危機的な状況 ～

【第２位】5月14日　IPAがランサムウェア「WannaCry」に関する注意喚起を発表
～ 侮るなかれ、セキュリティ対策の基本の基本 ～

【第３位】8月25日　米国の一私企業のミスで日本の通信インフラが混乱
～ 巨人の喉一つでゆらぐインターネット ～

【第４位】10月16日　世界が狂騒したWPA2の脆弱性は狂想だった
～ SNSでの不確かな憶測情報が不安を助長した ～

【第５位】12月20日　米国、サイバー攻撃に北朝鮮関与を断定
～ 国家によるサイバー攻撃の常態化 ～

【第６位】12月5日　長野県の高校生が不正アクセス容疑で逮捕される
～ 目立つサイバー犯罪の低年齢化 ～

【第７位】5月30日　改正個人情報保護法が全面施行に
～ 個人情報の保護と利活用の両立に効果を発揮するか ～

【第８位】9月7日　米国消費者信用情報会社Equifaxで大量の個人情報が流出
～ 止まらぬ大規模情報漏洩事件 ～

【第９位】10月2日　IPA「情報処理安全確保支援士」累計で約7,000名に！
～ 2020年までに3万人は達成できるのか ～

【第10位】10月31日　セキュリティ会社員がウイルス保管容疑で逮捕
～ セキュリティ企業が時代の要請に応えるべきか ～

http://www.jnsa.org/active/news10/

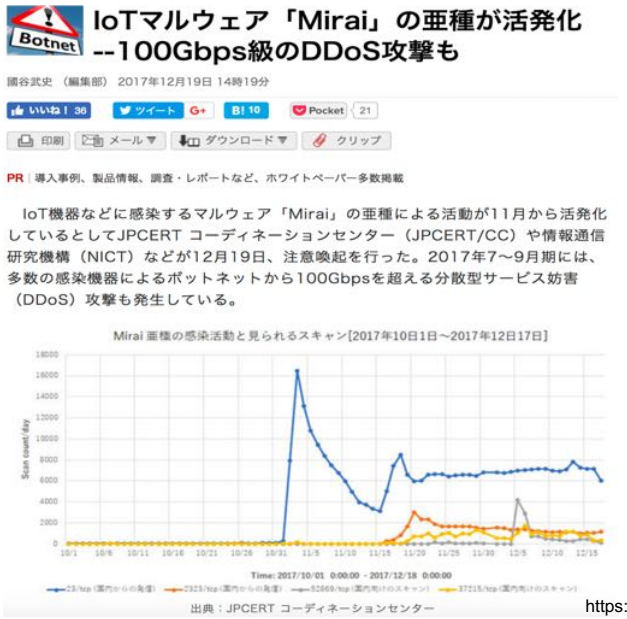
IPA情報セキュリティ10大脅威2018より

■「情報セキュリティ 10 大脅威 2018」　　NEW：初めてランクインした脅威

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	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
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の可能性	4 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化（アンダーグラウンドサービス）	9 位

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

ところでIoTセキュリティ？



IoTマルウェア「Mirai」の亜種が活発化 --100Gbps級のDDoS攻撃も

國谷武史（編集部） 2017年12月19日 14時19分

いいね！ 36　ツイート　G+　B! 10　Pocket 21

印刷　メール　ダウンロード　クリップ

PR｜導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載

IoT機器などに感染するマルウェア「Mirai」の亜種による活動が11月から活発化しているとしてJPCERT コーディネーションセンター（JPCERT/CC）や情報通信研究機構（NICT）などが12月19日、注意喚起を行った。2017年7～9月期には、多数の感染機器によるボットネットから100Gbpsを超える分散型サービス妨害（DDoS）攻撃も発生している。

Mirai 亜種の感染活動と見られるスキャン[2017年10月1日～2017年12月17日]

出典：JPCERT コーディネーションセンター

まさかの「いらすとや」様でもモノのインターネットのデザイン
そんな時代…

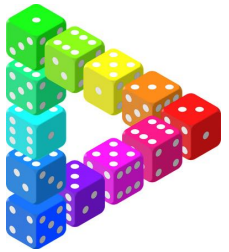
https://japan.zdnet.com/article/35112184/

試験にも必ず出る(笑)
情報セキュリティ3大要素CIA

- Confidentiality（機密性）
  - 許可のある人だけが情報へアクセスできること
    - アクセス制御、暗号化、ID/パスワード認証
- Integrity（完全性）
  - 情報そのものに正確性が保証されていること
    - 電子署名、改ざん検知
- Availability（可用性）
  - 情報そのものに必要な時はいつでもアクセスできること
    - システム/ネットワークの二重化・冗長化、（クラウド）

- OECDの情報セキュリティガイドラインにて定義
  - ISO/IEC27001(JIS Q 27001)にて規定
    - ISMS(情報セキュリティマネジメントシステム）を構築する際にも重要

最近ではCIA3+3=6大要素



- Reliability（信頼性）
  - システムやプロセスが矛盾なく動作すること
    - データ、動作の突き合わせ、頑健なシステム・OS等
- Accountability（責任追跡性）
  - 利用者やサービスの振る舞い、責任が説明できること
    - ログ調査（デジタルフォレンジック）、否認防止(Non-Repudiation)
- Authenticity（真正性）
  - 故意または過失による虚偽や改ざん等を防止すること。第３者から見て作成の責任の所在が明確であること
    - 改ざん検知、電子署名

- 新たにISO/IEC TR13335にて規定

Webカメラの現実（何か問題ある？）

Amazon.co.jpにてWebカメラ　無線LANとして検索してみた結果

制御システムと言うと?

Amazon.co.jpにて制御システムとして検索してみた結果

視点：プライバシー問題

- EVITA[1]では、V2Xのセキュリティを検討するため、リスク分析として深刻度クラスを定義
  - 安全性、プライバシ、財務、運用に関する深刻度を0～4に分類

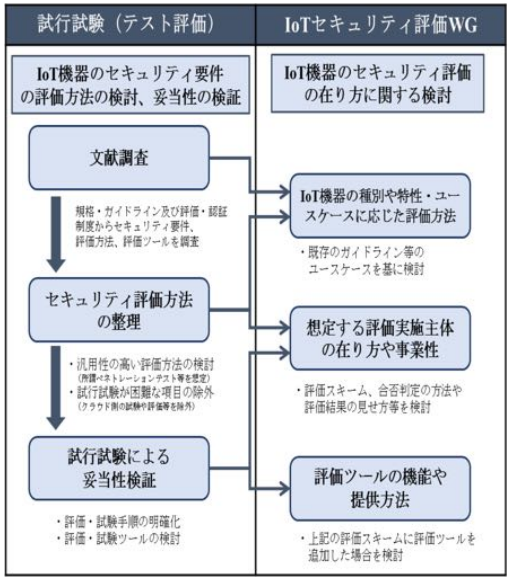
EVITAの深刻度クラス	セキュリティ脅威のアスペクト			
	安全性: Ss	プライバシ: Sp	財務: Sf	運用: So
0	ケガなし	プライバシの侵害なし	財務的な被害なし	支障なし
1	軽傷	匿名情報のみ ※個人や場所が特定できない	低い損失	運行継続可能
2	重症	個人の特定 （一度きり/その瞬間の）	中程度の損失	短時間の運行停止
3	生命にかかわる	個人の追跡可能	多額の損失	長時間の運行停止
4	複数の生命にかかわる	複数の個人を追跡可能	–	運行不可能（長期間）

[1] E-safety Vehicle Intrusion proTected Applications：欧州においてITS関連の中でも特に車載ネットワーク、セキュリティチップ設計（ハードウェア）等をテーマとしたセキュリティ開発プロジェクト

IoT機器セキュリティ調査by METI

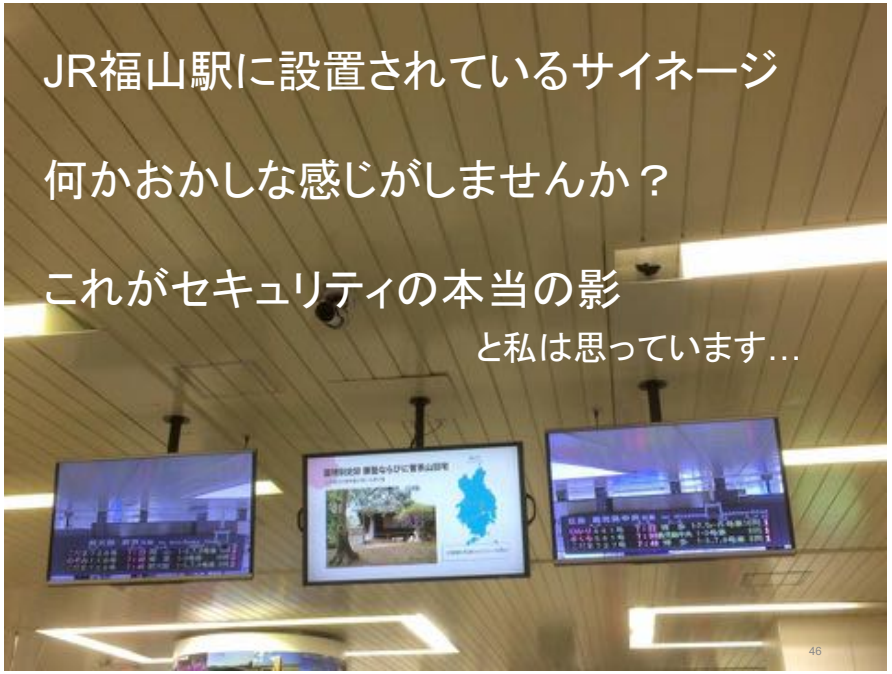
平成28年度IoT推進のための新産業モデル創出基盤整備事業
(IoT機器のセキュリティ評価調査)

- ネットワークに接続される脅威を考慮していない機器の接続やセキュリティにコストをかけられない機器の接続等、機器におけるセキュリティ課題が生じることが懸念
  - 多くのIoT機器の製造企業は独自のセキュリティ検証・評価を進めている状況であり、IoT機器の利用者（サービスプロバイダやエンドユーザ）、IoT環境に関わる事業者等がIoT機器のセキュリティを客観的に評価することが困難
- IoT機器のセキュリティ要件や評価方法を整理するとともに、第三者評価の在り方について検討を実施



総括：仮題？と過大？と課題？

- 情報漏洩の脅威？「個人」情報と「システム」情報の違いを見直そう
- 「**仮題**」産業・制御システムとIoT、ごっちゃになっていない、同じセキュリティ対策が必要なの？
- 「**過大**」とても信頼できる第３者によるお墨付きは安心だけど、そんなにコスト（お金）も時間もかけられるの？
- 「**課題**」結論、何がハッピーなんだろうか？（セキュリティ投資は大切かもしれないけれど生み出される価値・利益は？）
- 脅威ばかりに目がいってしまい、本来投資すべきところを見誤る可能性がある。セキュリティが生み出す価値は最大が「０」である



最後に（あくまでも自論ですが）

- とかく情報セキュリティは「寝た子を起こすな」ではいけない
  - 「脅威」をきちんと知ることも大事
  - じゃぁ危ないから「使うな」ではなく、職場、家族などの場における「対面」でのコミュニケーションで、きちんと話して、実際に触ってみて、使っていきましょうという意識が大切
  - 問題を起こしたことを隠す、のではなく、即座に伝える職場の雰囲気に。
- 上司、管理者、そして業界はきっとあなたの良き解決者になってくれるはず（＾-＾）