JPCERT CC®

制御システムセキュリティの現在と展望 2015

～この1年間を振り返って～

一般社団法人
JPCERTコーディネーションセンター
顧問　宮地　利雄

概要： Stuxnetの報告から今年で5年に

- ICSに対するサイバー攻撃はまだ希少
  - —ICS堅牢化は緒に就いたが課題も山積
  - —ICS攻撃で儲けるシナリオが見つかっていない

- これまではStuxnetがICSを狙った唯一のマルウエアだったが、ICSを狙った2種類のマルウエアが新たに登場
  - —Havex
  - —Black Energy 2

幸いにも実害の報告はない

- Stuxnet以降初の重大な物理的被害を伴うサイバー攻撃の報告
  - —ドイツの製鉄所にサイバー攻撃

概要： ICSセキュリティ

コミュニティの動向

- IPAとJPCERT/CCが調整する脆弱性取扱制度でICS関連製品も明示的に取扱を開始
- CSSCがICS製品認証を開始
- JIPDECがCSMS認証を開始
- 標準化の動向

研究者の動向と話題になったニュース

- ICSの基本的なコンポーネントに対するセキュリティ検証
- オーロラ脆弱性の関連情報をDHSが開示
- 中小規模のビル管理システム
- SHODANとSHINEプロジェクト
- 意図的でないがICS障害に起因する事故

概要： ICSを取り巻く外部環境の変化

- マイクロソフト社製Windows XPのサポートが終了
- 米国NISTが重要インフラ・サイバー・セキュリティ強化の枠組み
- サイバーセキュリティ基本法が成立

- ✓ ICSを狙ったサイバー攻撃
- ✓ ICSのサイバー・インシデント事例

STUXNETの報告から今年で5年に

Stuxnetに続くマルウエア

- Flame、Duqu、Shamoon： Stuxnetの直後に中東で報告
  - 事務用システムからの情報窃取ないしシステムの破壊
  - StuxnetのようなICS用の機能をもつマルウエアではなかった

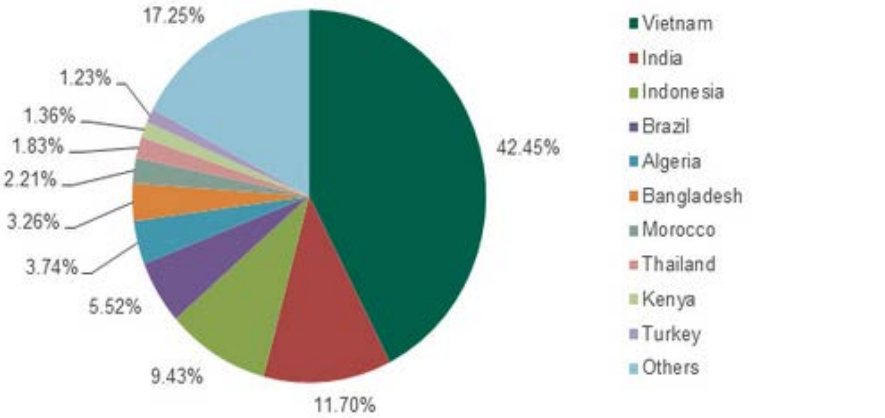
- Havex RAT (2014年6月) (RAT: Remote Access Trojan)
  - ICS-CERTアドバイザリ (ICSA-14-178-01)
    「ICSを狙ったマルウエア」 (2014年6月30日；7月1日)
  - 攻撃集団： ロシア Energetic Bear *(CrowdStrike)*

    別称Dragonfly *(Symantec)*、 Crouching Yeti *(Kaspersky)*

- BlackEnergy2 (2014年10月)
  - ICS-CERTアラート (ICS-ALERT-14-281-01B)
    「ICSに侵入する高度のマルウエアによる攻撃が進行中」
    (2014年10月29日；12月10日)
  - 攻撃集団： ロシア Sandworm *(Kaspersky)*

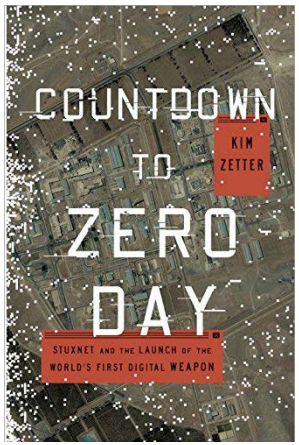
Stuxnet — 今なお

- CVE-2010-2568：
  最近まで攻撃されていた
  Stuxnet**が利用した**
  Windows**のゼロディ脆弱性**
  （Kaspersky**社調査**）
  - **細工した、**LNK**や**.PIF**ファイルにより管理者権限を奪取可能**



CVE-2010-2568 detections, country distribution Nov 2013 - June 2014

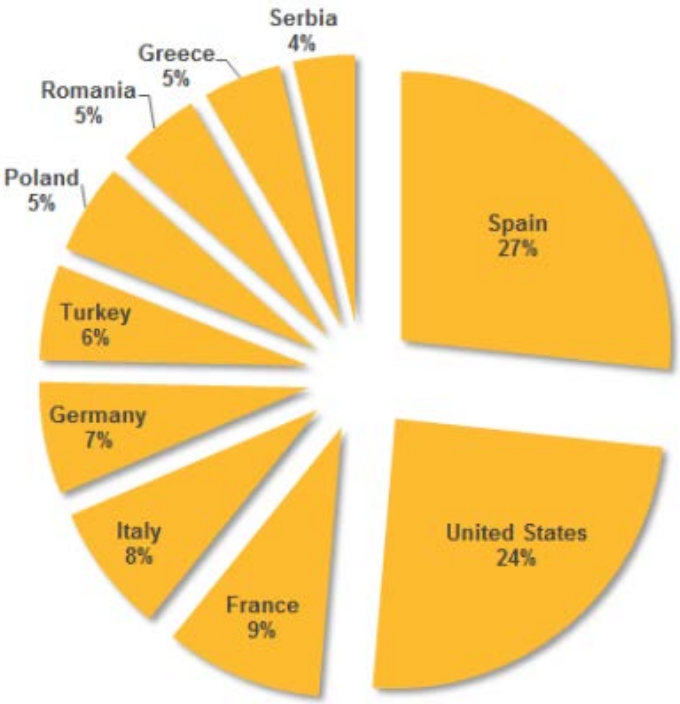
- **イランの核施設を**Stuxnet**に感染させる経路となった5社のベンダーが明らかに**
  - Kaspersky**社**
    http://securelist.com/analysis/publications/67483/stuxnet-zero-victims/
  - Symantec**社**
    http://www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz



Kim Zetter's
"Countdown to Zero Day"

Havex RAT

- 欧米の企業を狙っているとされる
  - エネルギー関連企業？
    http://blog.f-secure.jp/archives/50730250.html
  - 製薬関連企業？
    http://info.belden.com/a-cyber-security-dragonfly-bc-lp
- 水飲み場攻撃やスパムから感染
- 遠隔操作用のマルウエアで様々なプラグインがある
  - 一部のプラグインがOPC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
  - 本格攻撃に備えた情報収集？
  - プラグインが進化中



攻撃によってコンピュータから情報が盗み取られた被害の多い上位 10 カ国

出典：シマンテック セキュリティ レスポンス ブログ
Dragonfly: 妨害工作の危機にさらされる欧米のエネルギー業界
http://www.symantec.com/connect/ja/blogs/dragonfly-0

Black Energy 2

- ICS-CERTによれば
  米国の複数の企業のHMI搭載コンピュータがマルウエア感染
  ICS-CERT Alert (ICS-ALERT-14-281-01B)
  - 元々のBlack EnergyはDDoS攻撃に使われるボット
  - 亜種(Black Energy 2)が出現しICS製品を攻撃

- 感染コンピューターはインターネット接続性があるHMI
  - 複数のベンダー製のHMIを狙い
    ICS製品の脆弱性を悪用
    GE社製Cimplicity、 Advantech/Broadwin社製WebAccess、 Siemens社製WinCC

- 計測制御に対する影響は報告されていない
  - 本格攻撃に備えた情報収集？
  - モジュラー化された構造をもち感染後に動的に機能追加可能

ドイツの製鉄所がサイバー攻撃を受けて甚大な被害

- ドイツ政府(BSI：連邦情報セキュリティ室)が12月に公表した「ドイツのITセキュリティ2014年」の中に記載 (p.31 3.3.1)
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
  — 被害企業の実名や発生時期は不詳

- 標的型サイバー攻撃
  — 高度のフィッシングとソーシャル・エンジニアリングで事務用ネットワークに侵入してから工場ネットワークに到達
- 大きな被害
  — まずコンポーネントおよび工場レベルで頻繁な障害が発生
  — 最終的にはシステムで溶鉱炉を制御できない状態に
- スキルがある攻撃者
  — ITセキュリティとICSの双方の知識を持ち合わせていた模様

- ✓ 脆弱性の取扱い
- ✓ EDSA認証 — CSSCによる認証開始
- ✓ JIPDECによるCSMS認証開始

ICSセキュリティ・コミュニティの動向

国内の脆弱性取扱制度
(情報セキュリティ早期警戒パートナーシップ)

- 明示的に制御システム用製品も取り扱うことに
  - ―ガイドラインを改定 (2014年5月30日)
    https://www.jpcert.or.jp/vh/PR20140530-vulPSG.pdf
    https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
    https://www.jpcert.or.jp/vh/vul-guideline2014.pdf
  - ― 製品ベンダーからの脆弱性情報の提供ルールを弾力化

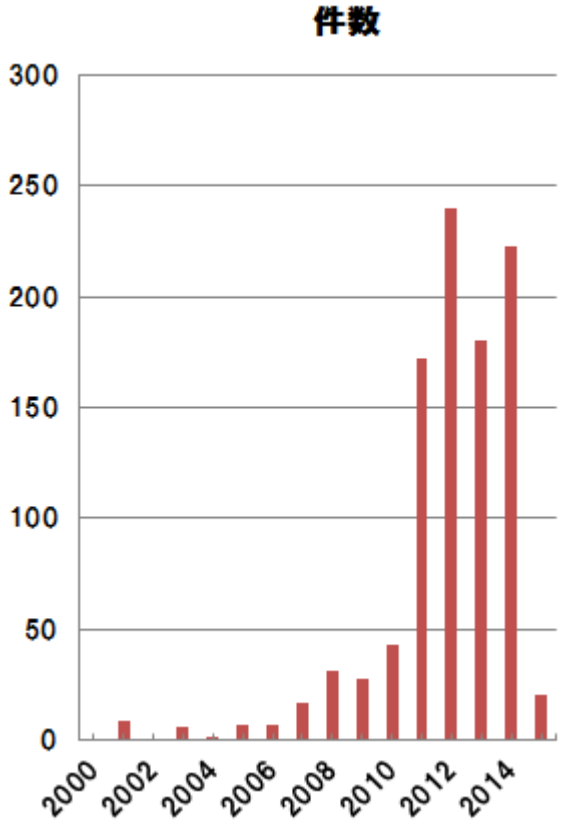
- 制御システム用製品のベンダーの社内体制整備へ
  - ― 自社製品に関する脆弱性の報告に迅速かつ適切に対応できるような社内体制と手順の準備

ICS製品に関連して注目された脆弱性の動向

- 2011年以降の脆弱性報告件数は毎年200件前後の水準で推移

- 多数の製品に影響した深刻な脆弱性
  - HeartBleed (OpenSSLの脆弱性)
  - ShellShock (GNU bashの脆弱性)
  - ICS関連製品の一部にも影響

- サプライ・チェーン問題の顕在化
  - 共通ライブラリに由来する脆弱性が多数の製品に影響
  - CodeSys、CodeWright社製DTM



脆弱性の報告件数推移
OSVDBの情報から作図

PLCにおける脆弱性のサプライ・チェーン問題

典型的なPLCの内部構造

- 他のベンダーなどから導入されたOSカーネルや各種のランタイム・モジュールを利用して実現
  - 通信に関連した機能は外部から素性が見える
- 脆弱性も継承される
- サプライ・チェーンの上流ベンダーの認識が甘く適切な脆弱性対応をしない場合も

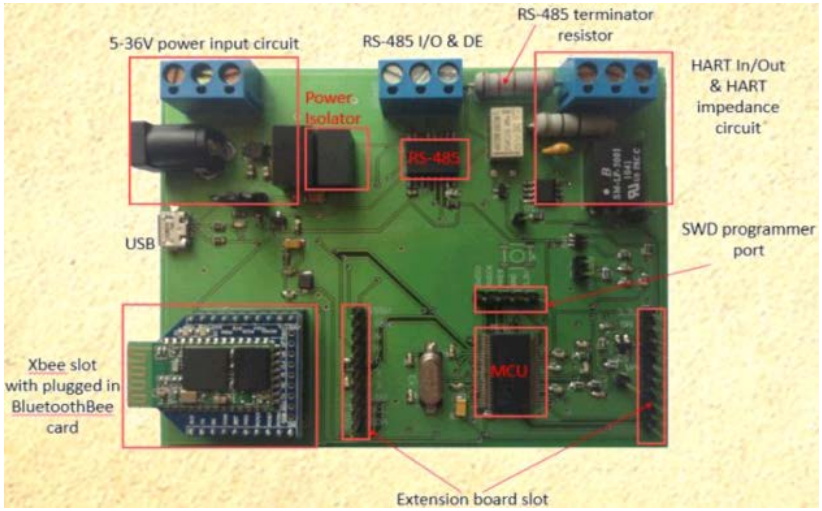
ICSプロトコルに対するファジング・ツールの開発拡充

- AEGIS社から
  DNP3ファザーやModbus TCPファザー (2014年3月;有償製品)
  http://www.automatak.com/aegis/
  http://www.automatak.com/robus/index.html
  - DNP3は米国や豪州などの電力や水道で利用されている ICS用プロトコル
  - ICS-CERTを通じて約30件の脆弱性情報が公表済み

- Digital Security社(ロシア)がインタフェース装置を開発し
  HARTプロトコル(20mA電流ループ)経由で
  FDT/DTM (Field Device Tool/Device Type Manager)に対するファジング
  http://www.securityweek.com/dtm-component-vulnerabilities-expose-critical-control-systems-cyberattacks
  - 無防備なICS用レガシー・プロトコル
  - レガシー技術と近代的技術の接点でしばしば現れる脆弱性

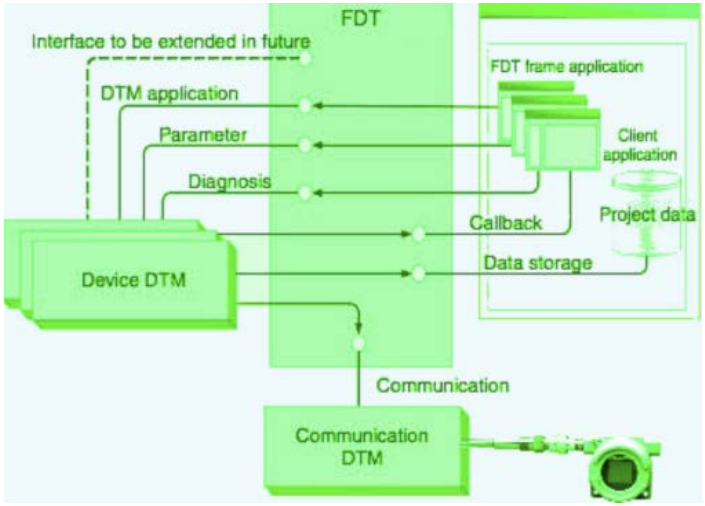
Digital Security社によるHARTとFDT/DTMに対する攻撃実験

- 特製インターフェース・ボード経由でHARTプロトコルに対する攻撃
  - パケットの盗聴
  - 通信のジャミング
  - スレーブのポーリングIDの変更
  - スレーブへの成りすまし
  - マスターをスリープ・モードに移行



HART(20mA電流ループ)用特製モデム

- FDT/DTMに対するファジング
  - 14ベンダーの501種の機器に対応するコンポーネントに29件の脆弱性
  - ICS-CERTアドバイザリ(ICSA-15-012) CodeWrights社製HART DTMの脆弱性



ISA Secure EDSA (Embedded Device Security Assurance)認証

- ISCI （ISA Security Compliance Institute)が認証
  - CSSCによる認証も開始 (2014年4月)
  - IEC 62443-4-1を基礎に

国内ベンダー製品

- ICS用製品のセキュリティを認証

認証機関	ISCI	CSSC	合計
直近1年間の認証件数	1	3	4
総件数	6	3	9

- FFRI社製RavenがCRTツールとして承認された (7月)

EDSA認証製品一覧

ベンダー名	製品タイプ	モデル名
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001
RTP Corporation	Safety manager	RTP 3000
Honeywell Process Solutions	DCS Controller	Experion C300
Honeywell Process Solutions	Fieldbus Controller	Experion FIM
横河電機 (Yokogawa)	Safety Manager	SCP451/461-11 : Vnet/IP
横河電機 (Yokogawa) ★CSSC	DCS Controller	CENTUM VP
日立(Hitachi) ★CSSC	DCS Controller	HISEC 04/R900E
アズビル(Azbil) ★CSSC	DCS Controller	Harmonas/Industrial-DEO/Harmonas-DEO system Process Controller DOPCⅣ (Redundant type)
Schneider Electric	Field Control Processor	Field Control Processor 280 (FCP280)

Achilles認証の後塵を拝しているEDSA認証

表示年時点での認証製品の総数
(新たな認証製品だけではない)

製品認証	2010年	2014年	2015年
Achilles Communications Certification	22	135	216 (GE社が買収)
MuDynamics	3	(Spirent社が買収)	
ISA ISCI (EDSA)	0	5	9
Exida	1		

2010年時点の認証製品数はRagnar Schierholz氏らによる”Security Certification – A critical review”に依る

ISCIが新たな認証制度を発表 (2014年2月)

- ISA Secure SSA (System Security Assurance)
  - ターンキー・システム型の制御システム(製品)のセキュリティを認証
  - IEC 62443-3-3に基づく

- SDLA （System Development Life Cycle Assurance)
  - ICS製品ベンダーの開発工程のセキュリティを認証

- いずれも認証の付与実績はまだ発表がない

JIPDECがCSMS適合性評価制度を開始

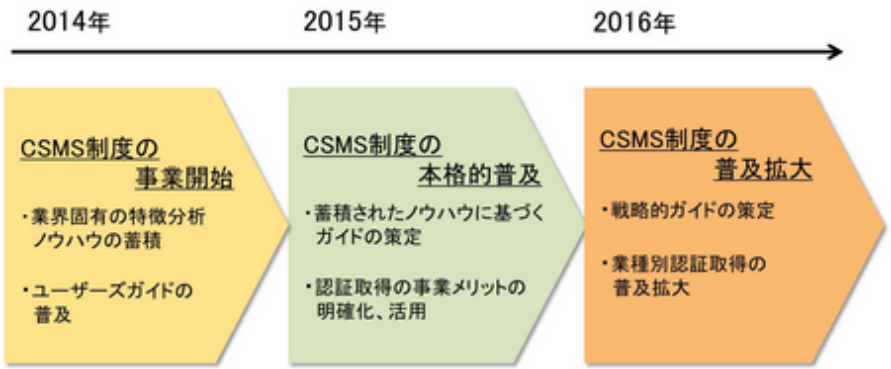
- ICSを対象としたサイバー・セキュリティ・マネジメント・システム(CSMS)に対する第三者認証制度

- JIPDECが世界に先駆けて認証制度を開始

  http://www.isms.jipdec.or.jp/csms.html

  — IEC 62443-2-1に基づく

  — 組織を認証

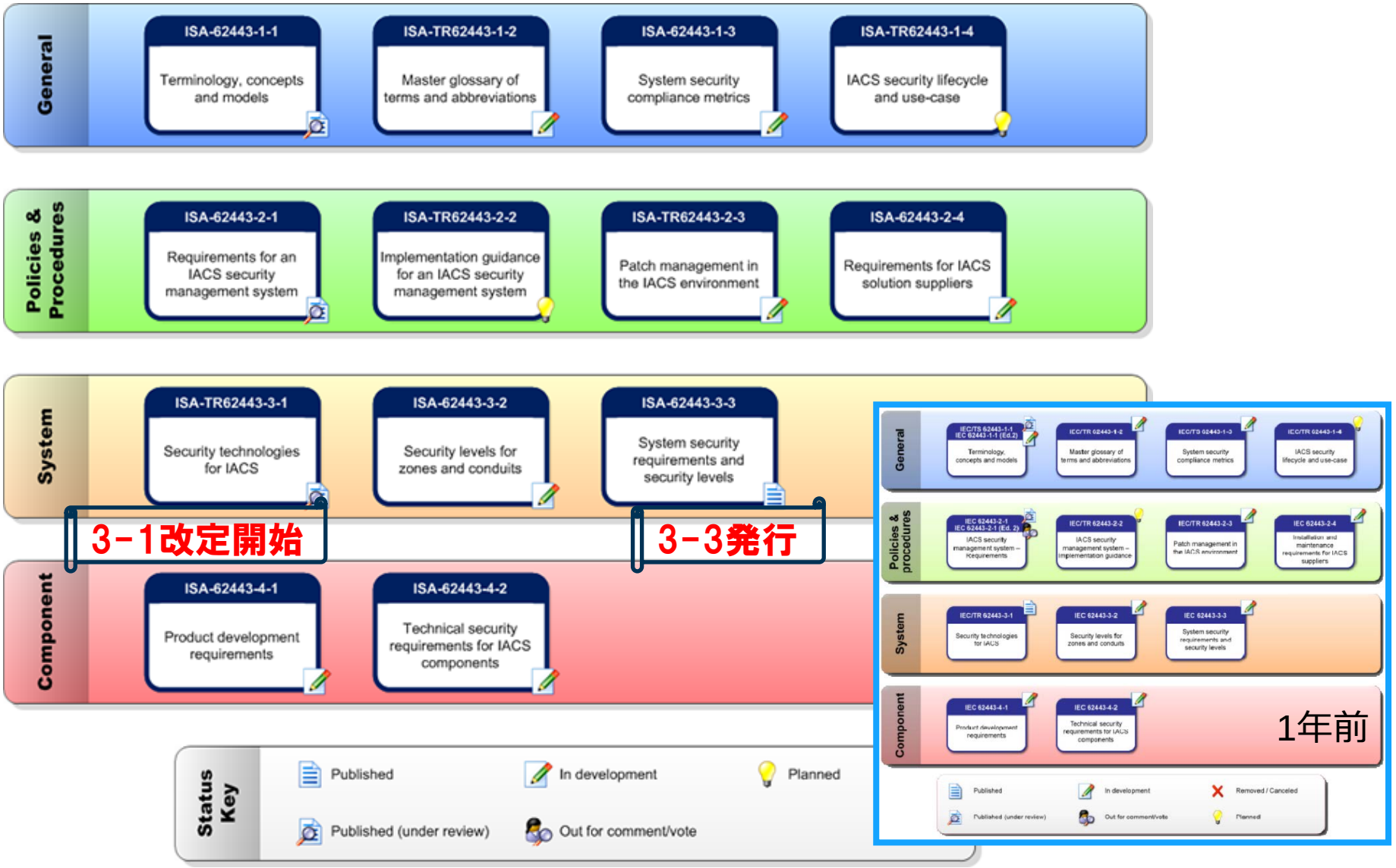


- 認証された組織

  — 三菱化学エンジニアリング(株)

  — 横河ソリューションサービス(株)

ISA/IEC 62443シリーズ標準の動き

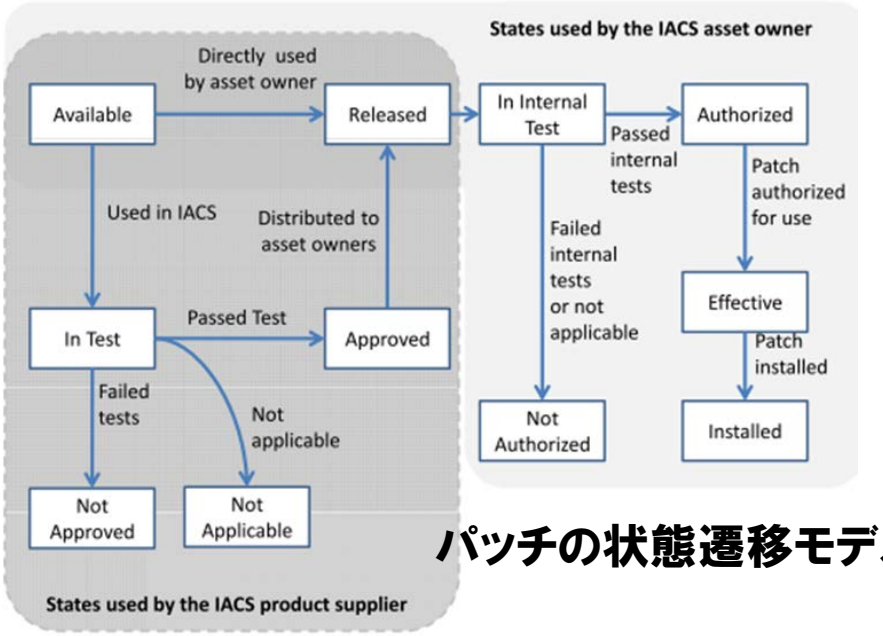


ISA/IEC 62443-2-3 (パッチ管理)

標準が規定しているのは：

- 複数のベンダーから
  パッチ情報を入手するための
  情報交換モデル
- ICS保有/利用者が
  強固なパッチ管理プロセスを
  構築し維持するための
  ガイダンス
- ICSのパッチ管理における
  製品提供ベンダーの役割

- パッチ管理プロセス
  1. 情報収集
  2. 監視と評価
  3. パッチの試験
  4. パッチの展開
  5. 検証と報告



パッチの状態遷移モデル

ISA-99委員会はレビューのため草案を公表
http://isa99.isa.org/Documents/Forms/AllItems.aspx (Drafts)

- ✓ オーロラ脆弱性の関連情報をDHSが開示
- ✓ 中小規模のビル管理システム
- ✓ SHODANとSHINEプロジェクト
- ✓ 意図的ではないがICS障害に起因する事故

ICSセキュリティ研究者の動向と話題になったニュース

オーロラ脆弱性の関連情報をDHSが開示

- (誤って?)米国DHSが他のオーロラの関連文書を大量に開示(7月)
  http://threatpost.com/dhs-releases-hundreds-of-documents-on-wrong-aurora-project/107107

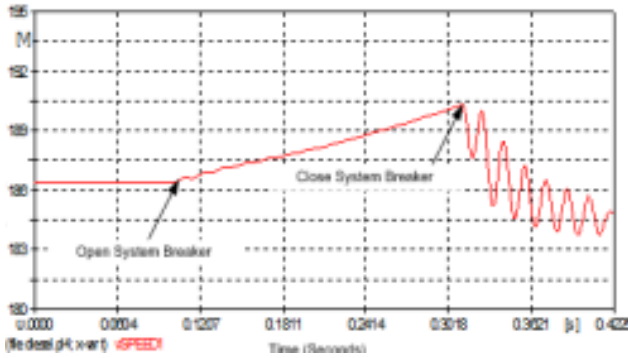
2つのオーロラ	オーロラ脆弱性	オーロラ作戦
概要	発電機の基幹網への接続タイミングで異常なトルクが発生して設備破壊を引き起こす脆弱性	2010年1月にGoogle社などの米国企業が受けたAPT攻撃；中国が攻撃元とされている
経緯	2007年3月に公開実験 詳細情報は公表されなかった	

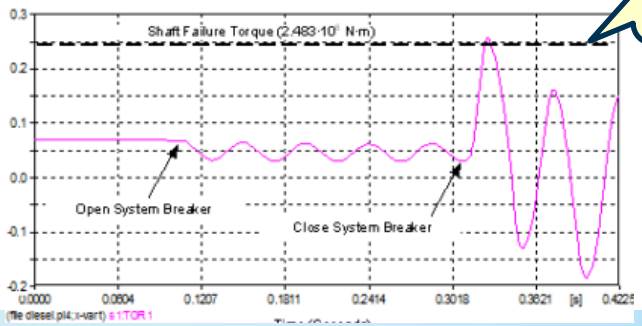
情報公開請求者の意図はオーロラ作戦？

- 既存の保護機構ではAurora脆弱性を悪用した攻撃に対抗できない
- 影響を軽減するためのハードウェア(2製品)の導入が現実的な解だがあまり導入されていない

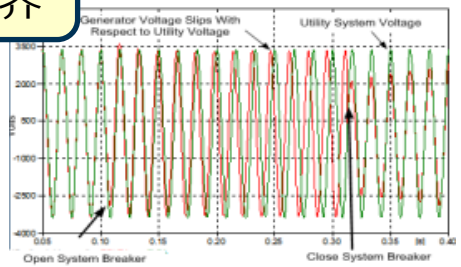
オーロラ脆弱性

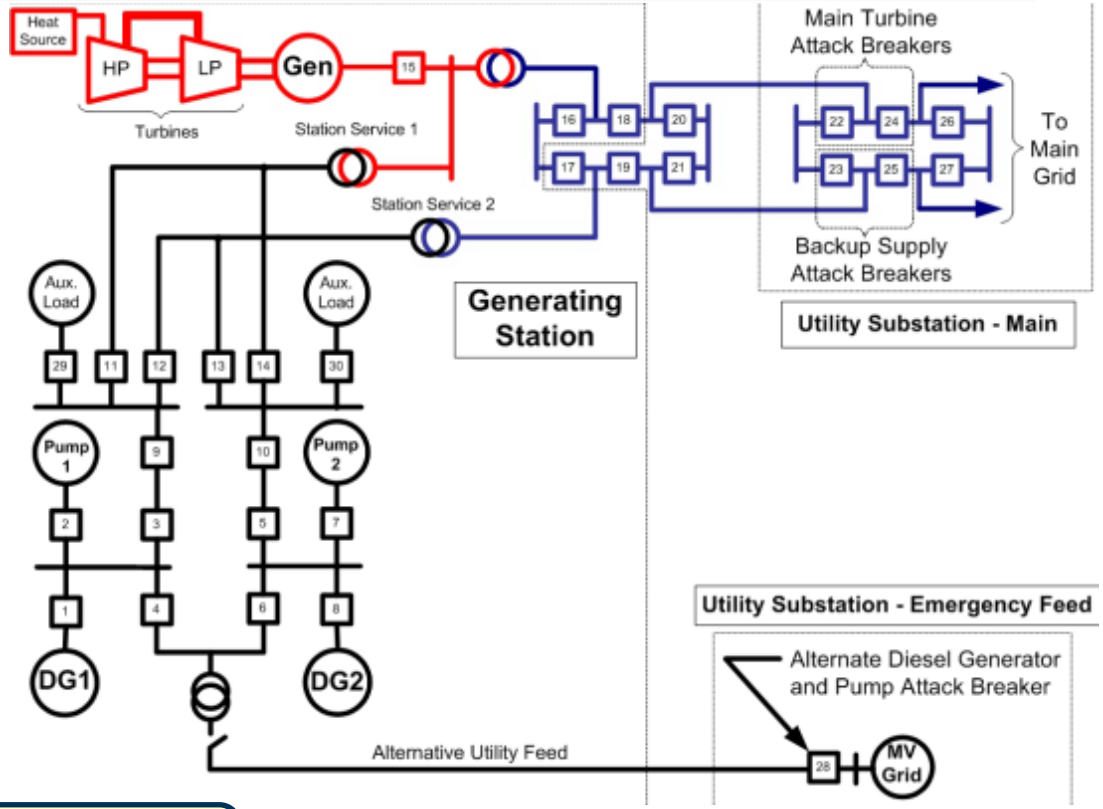
- 攻撃ブレーカーを
  オフにすると
  加速し位相がずれる
- 攻撃ブレーカーを
  オンにすると
  大きな電流とトルクの
  パルスが発生する





許容できる
トルク限界





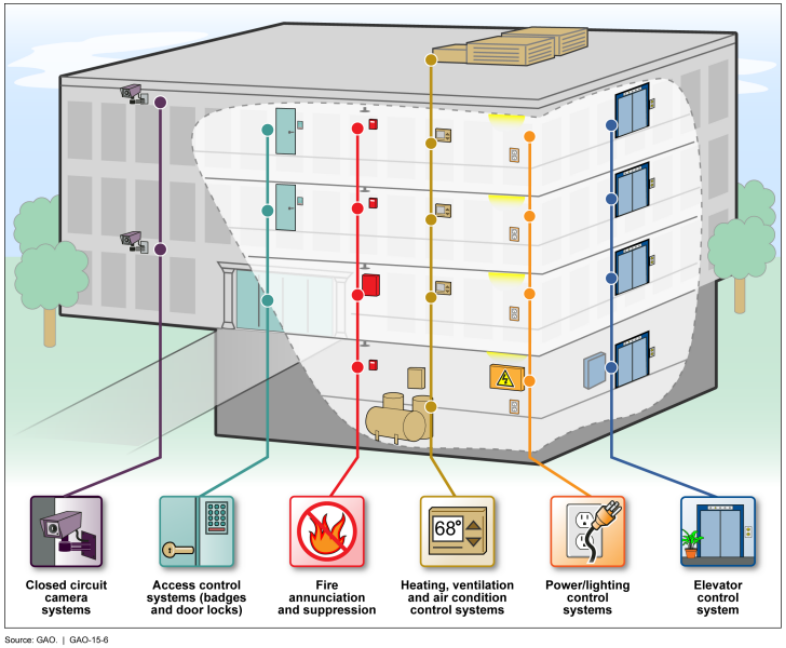
交流発電機を
網に接続する
には位相同期
が必要

米国GAOが連邦施設のビル制御システムについて勧告 (12月)

- 連邦施設のサイバー・セキュリティ
  DHSとGSAはビル制御システムのサイバー・リスクに対処すべし
  http://www.gao.gov/assets/670/667512.pdf
  - 連邦施設の物理的な保安とサイバー・セキュリティの合同評価がなされてきたが、ビル制御システムのサイバー・リスクについては対応戦略も実際の対処も不十分

- ビル管理システムの多くは
  ベンダーによる遠隔保守機能を搭載
  - パスワード管理もベンダー任せ？

- アセット・オーナーの担当者不在
- 施設数が多く個別対処に手間暇

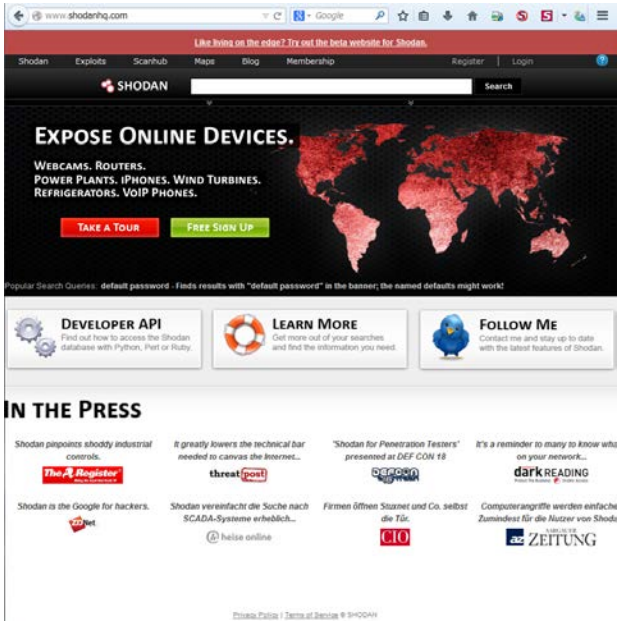


SHODANの ICS探索能力が向上

- SHODANはインターネットに接続されたノード(サーバ等の機器)を検索するサービス
  - John Matherly氏が個人的な興味から構築しサービス提供
  - クローリング周期は比較的ながく運用の不安定さも
  - 人手による少量の検索は無料

- 検索結果の地図上表示を追加

- ICS関連プロトコルの処理コードや製品固有のシグニチャ―等の提供を受けてICS関連の探索能力が向上
  - BACnet
  - 大手ベンダーのSCADAやPLC



http://www.shodanhq.com/

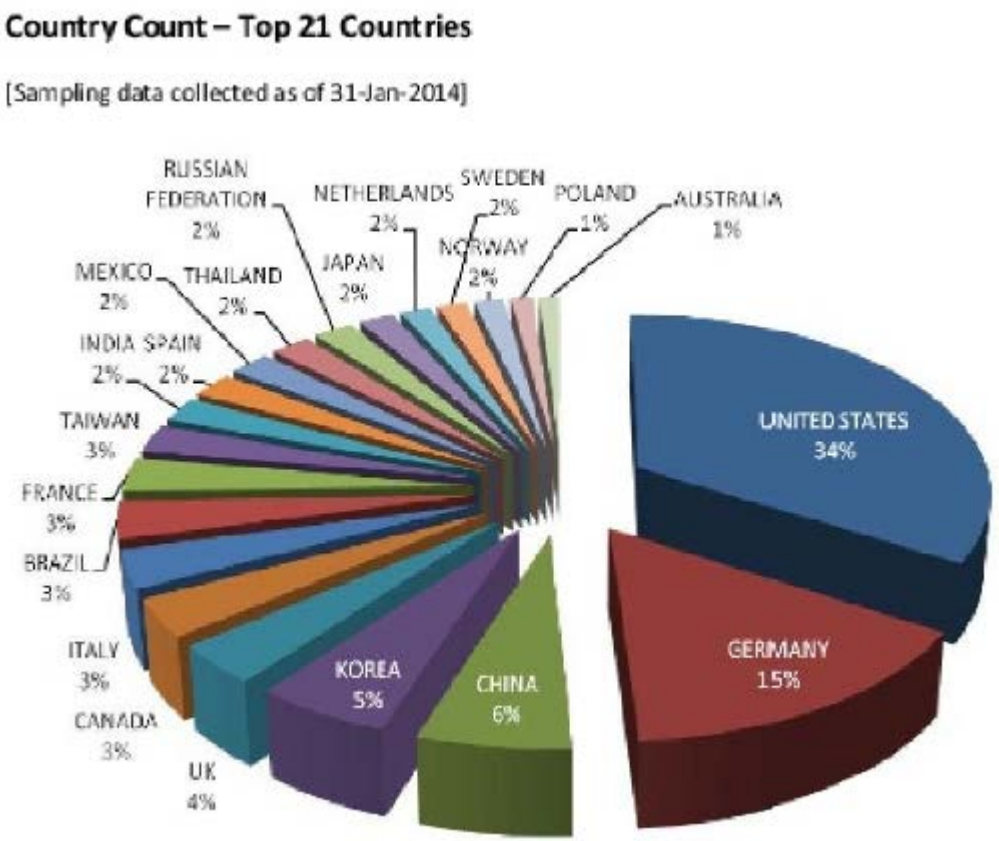
SHINE (Shodan INtelligence Extraction) プロジェクトが報告書

http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

- 突然にプロジェクトを中止(2014年1月)
  約2年間の調査結果をまとめた報告書を公表（10月）
- インターネットに直結されたICS用機器を
  SHODANを利用して 調査

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

SHINEプロジェクト報告書 — 上位21か国の内訳



出典: SHINEプロジェクト報告書

国名	台数	%
米国	616,994	33.8
ドイツ	280,248	15.3
中国	112,114	6.1
韓国	99,856	5.5
英国	66,234	3.6
カナダ	62,712	3.4
ブラジル	62,376	3.4
イタリア	62,266	3.4
フランス	56,827	3.1
台湾	46,836	2.6
インド	41,309	2.3
スペイン	40,911	2.2
メキシコ	39,904	2.2
タイ	39,027	2.1

米国PG&E社のSan Bruno市ガス・パイプライン爆発事故の裁判

- 2010年9月にSan Bruno市の住宅街でPG&E社の天然ガス・パイプラインが爆発
  - 甚大な被害
    死者：8名、負傷者：66名
    被害家屋： 38軒
  - 制御システムの不具合で異常事態の発生を見逃す
    (意図的な攻撃ではない)

- PG&E社に対して複数の訴訟
  - 被害者から400件の民事訴訟
    (うち350件は係争中； 賠償金総額は1.55億ドル以上の見込み)
  - 28項目の刑事訴訟 (14億ドルの罰金； 2014年9月)
  - 株主から民事訴訟

- ✓ マイクロソフト社製Windows XPのサポートが終了
- ✓ NISTが重要インフラ・サイバー・セキュリティ強化の枠組み
- ✓ サイバー・セキュリティ基本法が成立

ICSを取り巻く外部環境の変化

Windows XPのサポート終了

- 2014年4月8日でWindows XPの「拡張サポート」が終了
  - ICS環境でもHMIなどで多用された
  - 新OSに移行した利用組織も大手を中心に相当数か
    - 組織の情報セキュリティ・ポリシーをICS環境にも適用
    - HMIの買換え需要が見られた
    - ICSでもソフトウェア・ライフサイクル管理の文化醸成の契機に
  - 使い続ける場合には
    ホワイト・リスティングやゾーニングによる保護でリスクを低減

- 2015年7月14日にはWindowsサーバ2003の「拡張サポート」が終了予定

米国NISTが重要インフラのサイバー・セキュリティ強化の枠組み

Framework for Improving Critical Infrastructure Cybersecurity

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

- 約1年間の公開論議を経て2014年2月12日に第1版を公表

オバマ大統領からの指令を受けてNISTが策定

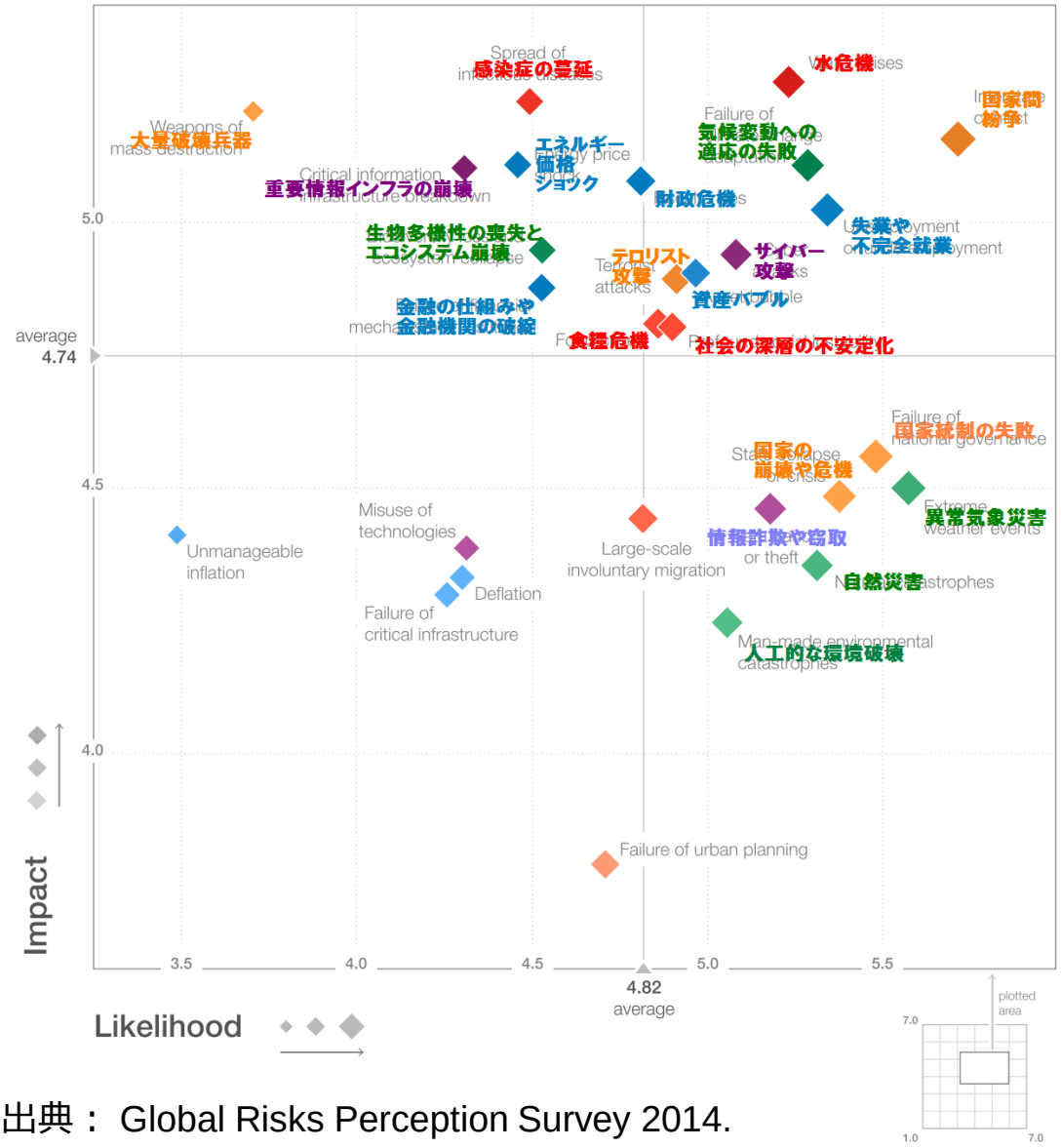
- 構成
  - コア + 実現層 + プロファイル
- 経営陣にも理解されやすいセキュリティ管理の枠組みを整理した文書
  - 技術文書ではない
- 業界はおおむね歓迎
  - 不安視されていた規制色が皆無
- 各省庁が呼応した各分野別のガイド類を順次発行

サイバーセキュリティ基本法が成立 (11月)

- 概要
  - 我が国のサイバーセキュリティに関する施策の基本理念
  - 国及び地方公共団体の責務等
  - サイバーセキュリティ戦略の策定等の施策の基本事項
  - 内閣にサイバーセキュリティ戦略本部を設置

- 内閣サイバーセキュリティセンター(NISC)が発足　（2015年1月）
  - 内閣官房の「情報セキュリティセンター」を改組・拡充
  - 我が国のサイバーセキュリティの司令塔機能を担う

まとめ



出典： Global Risks Perception Survey 2014.

- サイバー攻撃は世界的な重要課題
  - 国際関係のきしみ
- ICSの場合には物理的な被害を伴う可能性がある
- 他山の石のうちに対策を！

JPCERT/CCが提供するICSセキュリティ関連サービス

- インシデントの報告受付と支援依頼
- 脆弱性情報の調整
  (製品開発者登録が望ましい)
- 月刊ニュース・レター配布
  (登録が必要)
- 情報ベースConPaS
  (登録が必要)
- 参考情報
- 制御システムセキュリティコンファレンス
- 情報共有会・報告会

https://www.jpcert.or.jp/ics/ics-form.html

迅速に脆弱性情報を受け取るため
https://www.jpcert.or.jp/vh/regist.html

https://www.jpcert.or.jp/ics/ics-community.html

https://www.jpcert.or.jp/ics/conpas/index.html

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：icsr@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/ics/

インシデント報告

- Email：ics-ir@jpcert.or.jp
- Web: https://www.jpcert.or.jp/ics/ics-form.html

ご清聴ありがとうございました。