JPCERT CC®

制御システムセキュリティの現在と展望 2016

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

JPCERT/CC 20周年

全体概要

- 主なインシデント報告の概要
- 脆弱性の報告の推移

- インターネット接続と
  インターネット探索システムの進化
- 研究者の動向

- 標準化と認証の進展
- 対策に向けた動き

- まとめ

2015年に公表された
大きなICSセキュリティ・インシデント

大きな事故もなく2015年が過ぎると思いきや，年末になり…

- イランのハッカーが米国のダム制御システムに2013年に侵入
  12月20日にWall Street Journal紙が報道
- 外国人ハッカーが米国の電力網に複数回侵入
  12月21日にAP通信社が配信
- ウクライナ西部でサイバー攻撃によると見られる大規模停電
  12月24日にウクライナの民間放送局がニュース番組TSNで報道
  ―ICSへのサイバー攻撃による実害としてStuxnetに次ぐ

米国のダム制御システムへの侵入(2013年)

Wall Street Journal紙(2015年12月20日)によれば…

http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

- NSAの調査官が脆弱なICS探索活動(イラン?)を発見
  標的とされていたICSシステムのIPアドレスを特定
  DHSに通知
- IPアドレスから標的が「Bowman」ダムであると割り出した
  - 全米にBowmanを名称に含むダムが31あった
  - オレゴン州には「Arthur R. Bowmanダム」
    (高さ約75*m*；アース構造型)
  - 最終的には「Bowman Avenueダム」だった
    (ニューヨーク市近郊Rye村にあり
    高さ6*m*；コンクリート板製)
- 侵入されたものの不正な操作はなかった

写真：Wall Street Journal紙より

外国人ハッカーが米国の電力網に複数回侵入(2013年以降)

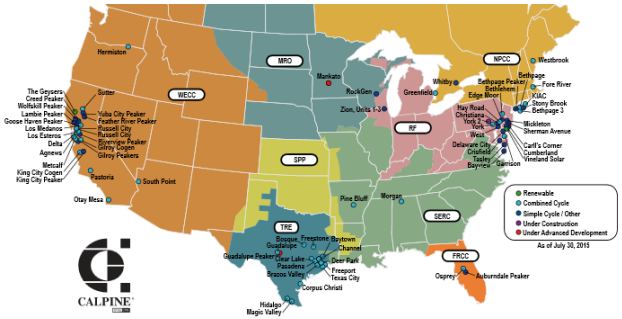
AP通信社の配信(12月21日)によれば…

http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks

- 送電用ICSに過去10年間に十数回外国人ハッカーが侵入
  (匿名の専門家)
- 2012～2013年にはロシア人ハッカーが電力会社などを
  マルウェアに感染させて情報収集 (DHS)

BlackEnergy2

- サイバー・スパイが重要インフラシステム情報を大量に収集；
  Calpnine社の71の発電所の詳細な技術情報が盗まれている
  (Cylance社の専門家)
- 関係企業から古い技術情報が盗まれていた；
  自社の技術情報が持ち出されていたことを
  Cylance社からの連絡で初めて知った
  (電力会社Calpine社)



ウクライナ西部でサイバー攻撃によると見られる大規模停電

ウクライナの民間放送局がニュース番組TSNで報道(12月24日)
http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

- 12月23日夕方にウクライナ西部の1州の半分と州都の一部で停電；復旧までに約6時間を要し40～70万人程度が影響を受けた
  - 遮断機が切れた経緯の詳細は不明
- ICSが使えず，復旧は手動により行われた；当該ICS網内でマルウェアBlackEnergy3が見つかった
- 同時に電話システムも攻撃され，電話機が鳴り続けた
- 同時に報道機関などへサイバー攻撃
- サイバー攻撃が引き起こした停電として関心
  - SANS https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
  - iSight http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/
  - SentinelOne https://www.sentinelone.com/blog/sentinelone-discovers-a-new-delivery-tactic-for-blackenergy-3/

ファイルを削除してシステムをダウンさせる

ウクライナ西部の大規模停電 (続き)

- 攻撃の経過 (限定的な情報に基づく暫定的な推定)
  1. 変電所を監視するSCADAシステムに侵入した
  2. ワークステーションやサーバを感染させた
  3. 監視機能を停止 (；変電所の遮断機を切断？)
  4. SCADAシステムのホストを破壊(ファイル消去)
  5. コールセンターに多量の架電をして顧客対応を邪魔した

- 複数の電力会社の複数の変電所を同時に切断
  - —Prykarpattyaoblenergo社(Ivano-Frankivsk地域で低圧配電)
    2,759MW，顧客数：50.9万
  - —Kyivoblenergo社(キエフ地域で低圧送配電)
    5,296MW，顧客数：81.9万
    - 遠隔操作の変電所を不正に切断されて8万顧客が3.5時間停電
      (11万V級7か所，3.5万V級23か所)

ウクライナ西部の大規模停電（残っている主な疑問点）

- 変電所の遮断機をどのように切断したのか？
  - マルウェアBlackEnergyにそのような機能は無さそう

- 攻撃したのは誰か？
  - 従来のBlackEnergyを使っていたのはロシア国内のグループ
  - ロシアvsウクライナの紛争を念頭にウクライナ政府によるでっちあげ説も

- 攻撃した目的は何か？
  - 発電所を狙った方が大きな打撃を与えられる(発電所を狙い，遮断機を自由に操作できれば，オーロラ脆弱性を利用して発電機を破壊できたはず)

- ウクライナ政府への警告？
- 秋にはクリミア半島への送電鉄塔が破壊される事件

(参考) Black Energy 2 (2014年)

- 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ェア感染
  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

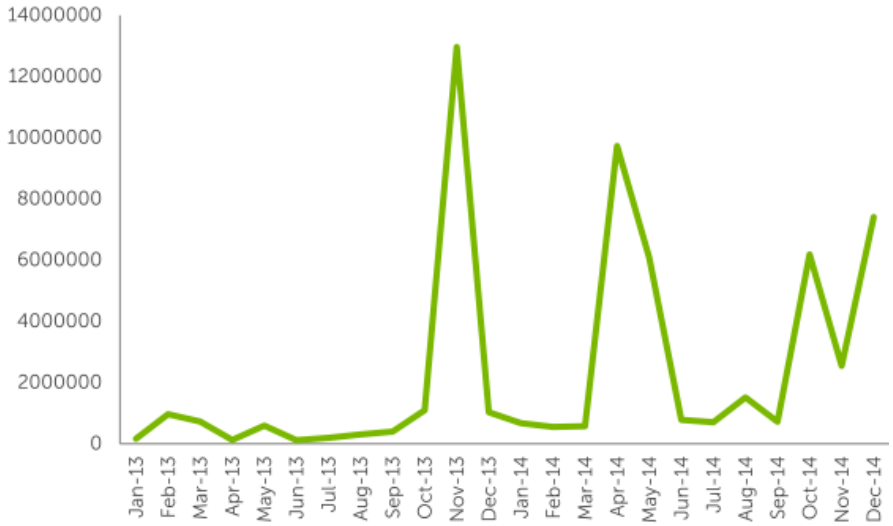
- 計測制御に対する影響は報告されていない
  - 本格攻撃に備えた情報収集？
  - モジュラー化された構造をもち感染後に動的に機能追加可能

制御システム用機器に対する攻撃的活動の活発化

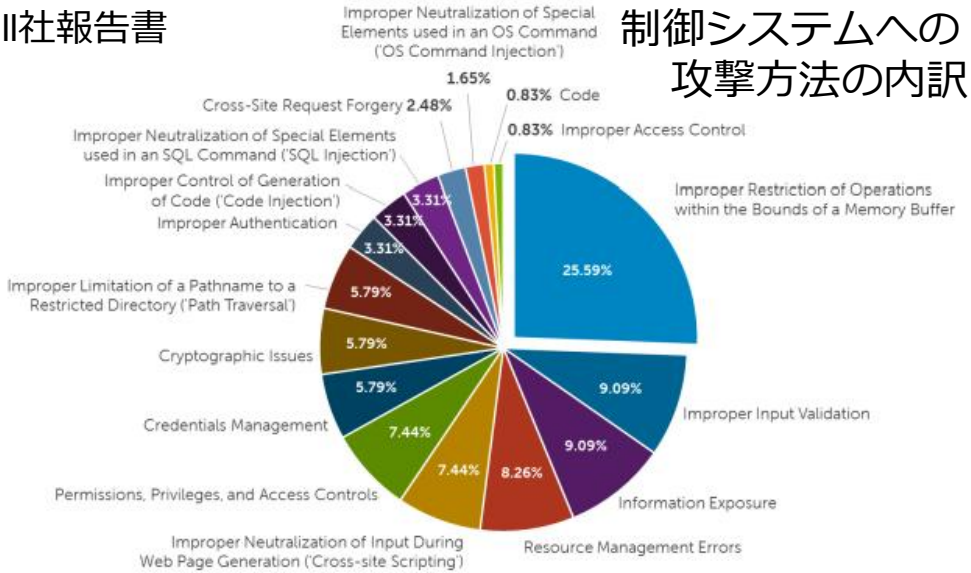
- 警察庁：産業制御システムで使用される PLC の脆弱性を標的としたアクセスの観測について (5月26日)
  https://www.npa.go.jp/cyberpolice/topics/?seq=16382
- Dell： 2015 Dell Security Annual Threat Report (9月)
  http://www.sonicwall.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf
  —SonicWallが検知した制御システムへの攻撃が1年間に倍増
  標的になっている主な地域はフィンランド，英国，米国

制御システムへの攻撃検知数

出典： Dell社報告書

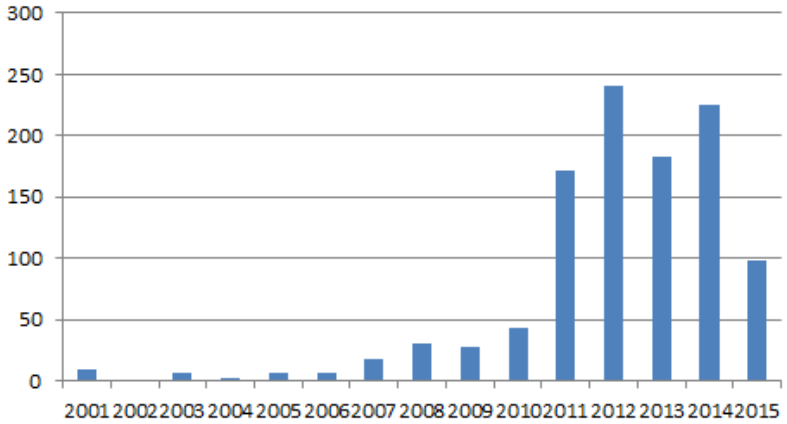


制御システムへの攻撃方法の内訳



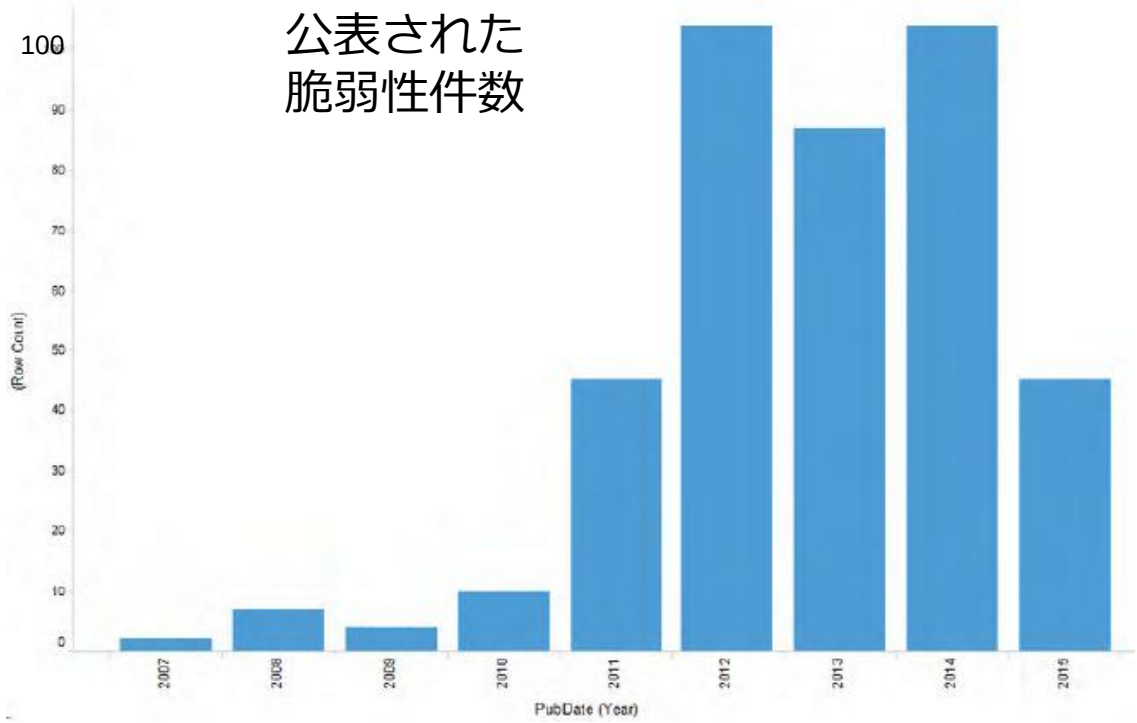
ICS製品の脆弱性報告数の推移

- 2011年以降の
  脆弱性報告件数は
  毎年200(100?)件前後の
  水準で推移

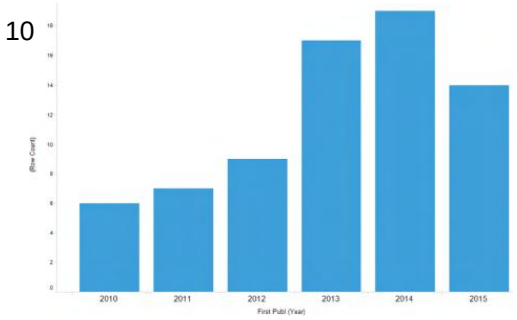


報告された脆弱性の件数(2015年は8月まで)
出典：OSVDB; 作図はJPCERT/CC

公表された
脆弱性件数



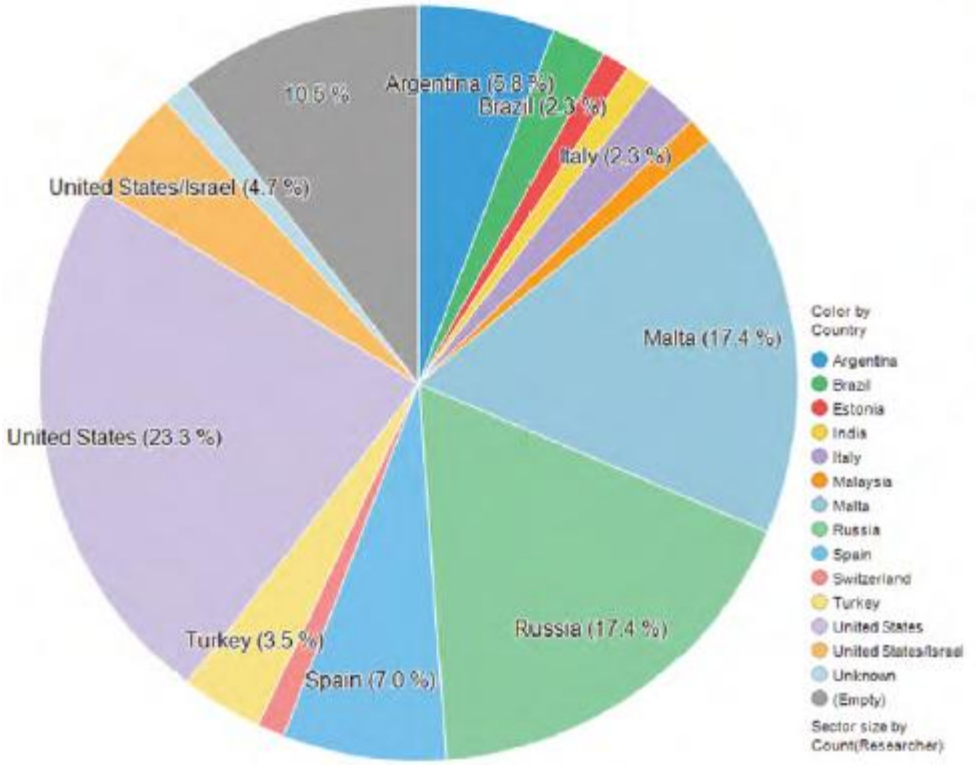
公表された攻撃コード数



出典：Up and to the Right
ICS/SCADA Vulnerabilities by the Numbers
Recorded Future社 (10月公表)

ICSセキュリティの研究者

- ICSセキュリティの研究者のほとんどが欧州と米国に
- 一部は闇市場に攻撃ツールや攻撃参考情報
  - 使い方が理解されず
    買い手探しが難航か？



脆弱性の発見者の国別内訳
出典：RecordedFuture社報告書

ICS製品の脆弱性をめぐる動向

- ICS製品には多数の脆弱性が今も潜在していると見られる
  - 機能仕様の設計でのセキュリティ不備も
- Metasploitのライブラリの蓄積・拡充

- 製品の脆弱性問題にして
  一部ICSベンダーでプロアクティブな取組みが始まる
  - 積極的な情報開示と調査
  - 汎用OSのセキュリティ・パッチに対する
    アプリケーション・ソフトウェアの動作検証

- IEC/TR 62443-2-3
  (IACS環境におけるパッチ管理)発行
  - ICS利用組織向け
  - ICS製品ベンダー向けの内容も含む

インターネットからアクセス可能な制御システム

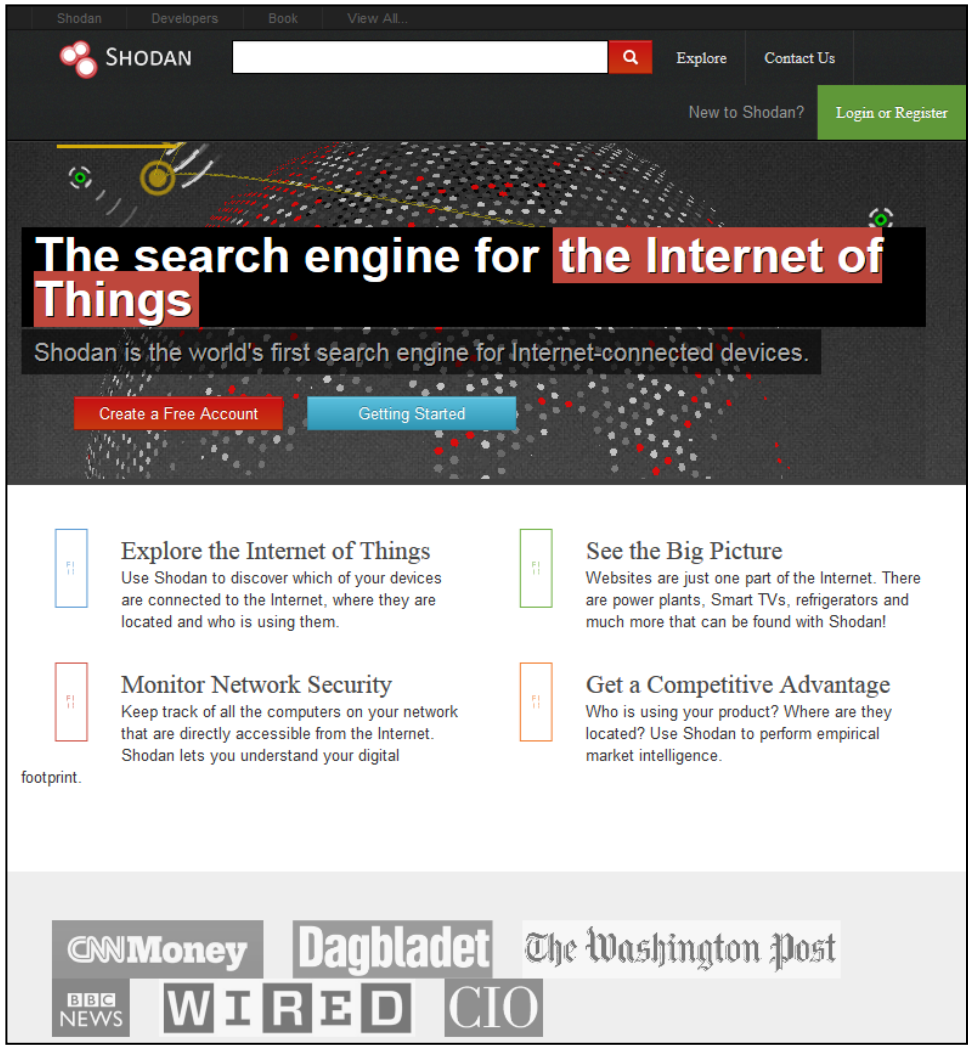
インターネット上の機器を検索する技術が向上

- SHODAN
  - 制御システムが見つかりやすくなるような機能強化
    例) ICS用プロトコル
  - FBIも注意喚起
- 他にも類似の検索システム

インターネットとの接続性を要求する機器の増加

- VPN機器
- 複合機(プリンタ)
- タンクの計量計
- ビル管理システム
  (空調や警備システム等)

インターネット上の機器検索サービス



SHODAN (2009～)

ICSfind (2015～)

ICSセキュリティ 「2.0」 (ステップ・アップ)

守備側

- セキュリティ認証取得
- 一部の業界における課題認識向上への取組み
- ICS用セキュリティ機器やサービスの登場
- 標準規格の整備

攻撃側

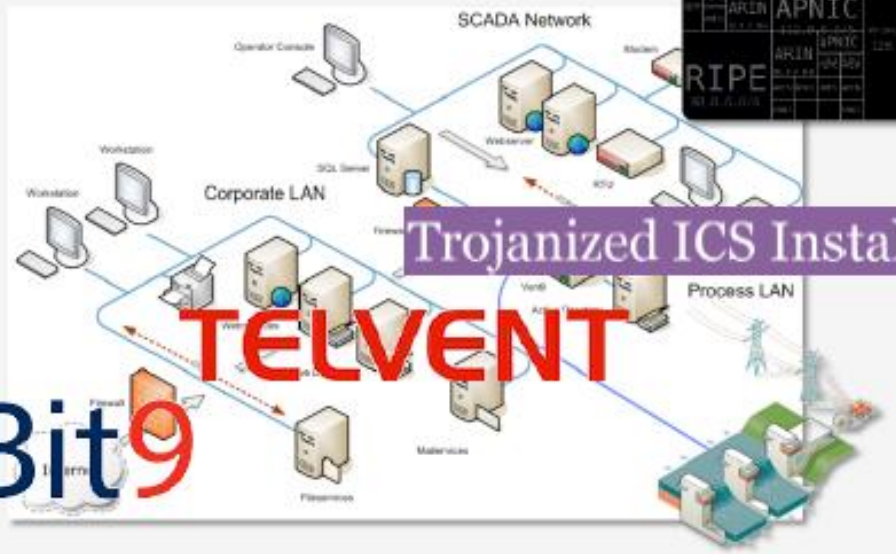
- ICSに関する情報の蓄積
- ICSのより高度なシステム的弱点を研究
- 国際紛争とサイバー攻撃(テロ行為，軍事行為)

より高度な攻撃法の研究(1/2)

Marina Krotofil氏のHITB(2015年10月14日)講演資料より

より高度な攻撃法の研究(2/2)

- Select a vulnerability from the list of ICS-CERT advisories
- Scan Internet to locate vulnerable devices
- Exploit



Trojanized ICS Installers

TELVENT

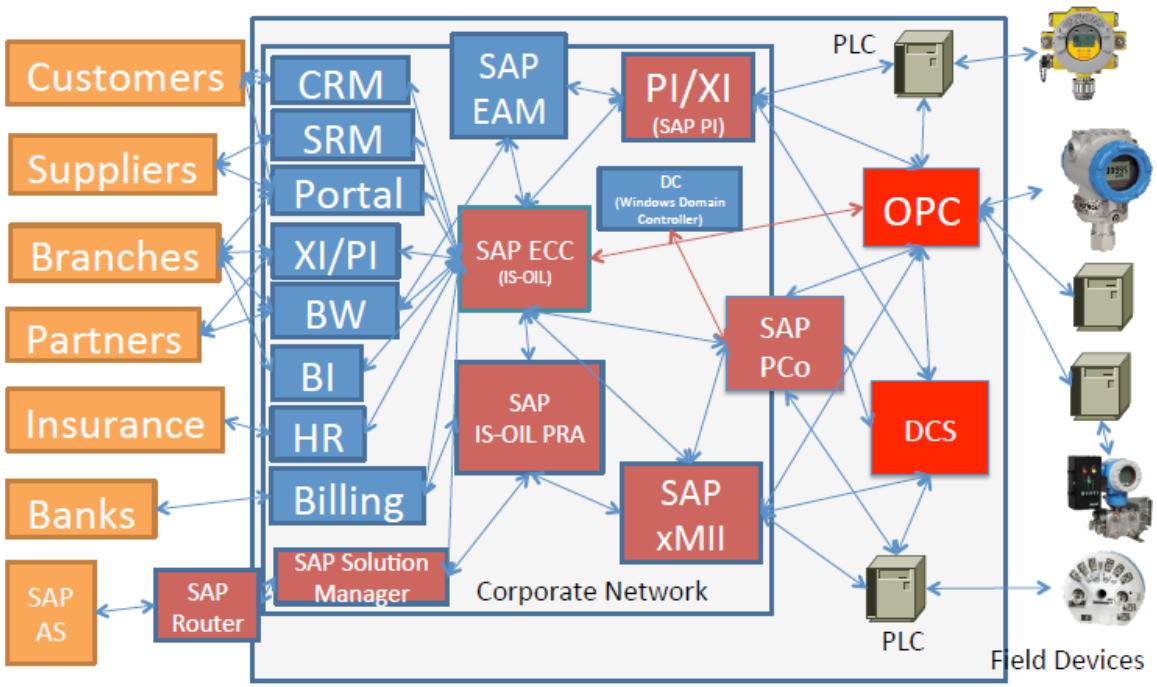
Bit9

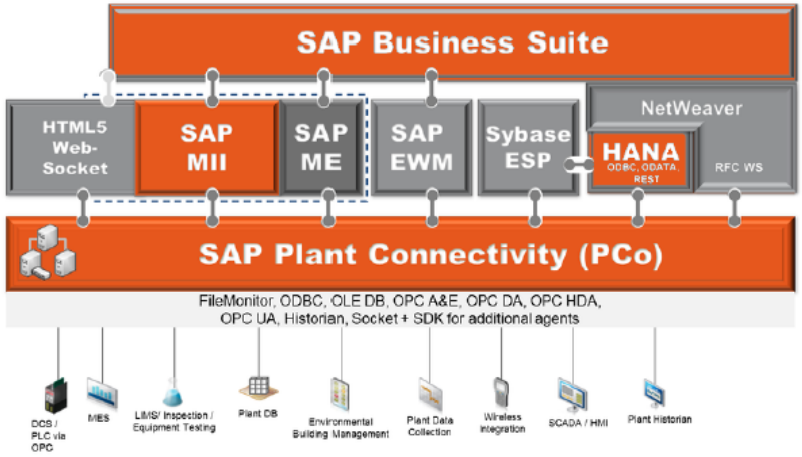
- E. Leverett, R. Wightman. Vulnerability Inheritance in Programmable Logic Controllers (GreHack'13)

Marina Krotofil氏のHITB(2015年10月14日)講演資料より

ICS～業務基幹システム連携に弱点が潜在か

- 多くのICSは業務基幹システムと連携
- SAP社やOracle社製品ないしその周辺が脆弱





Alexander Plyakov氏の
BlackHatEuropeにおける
講演資料より

国際紛争とサイバー攻撃

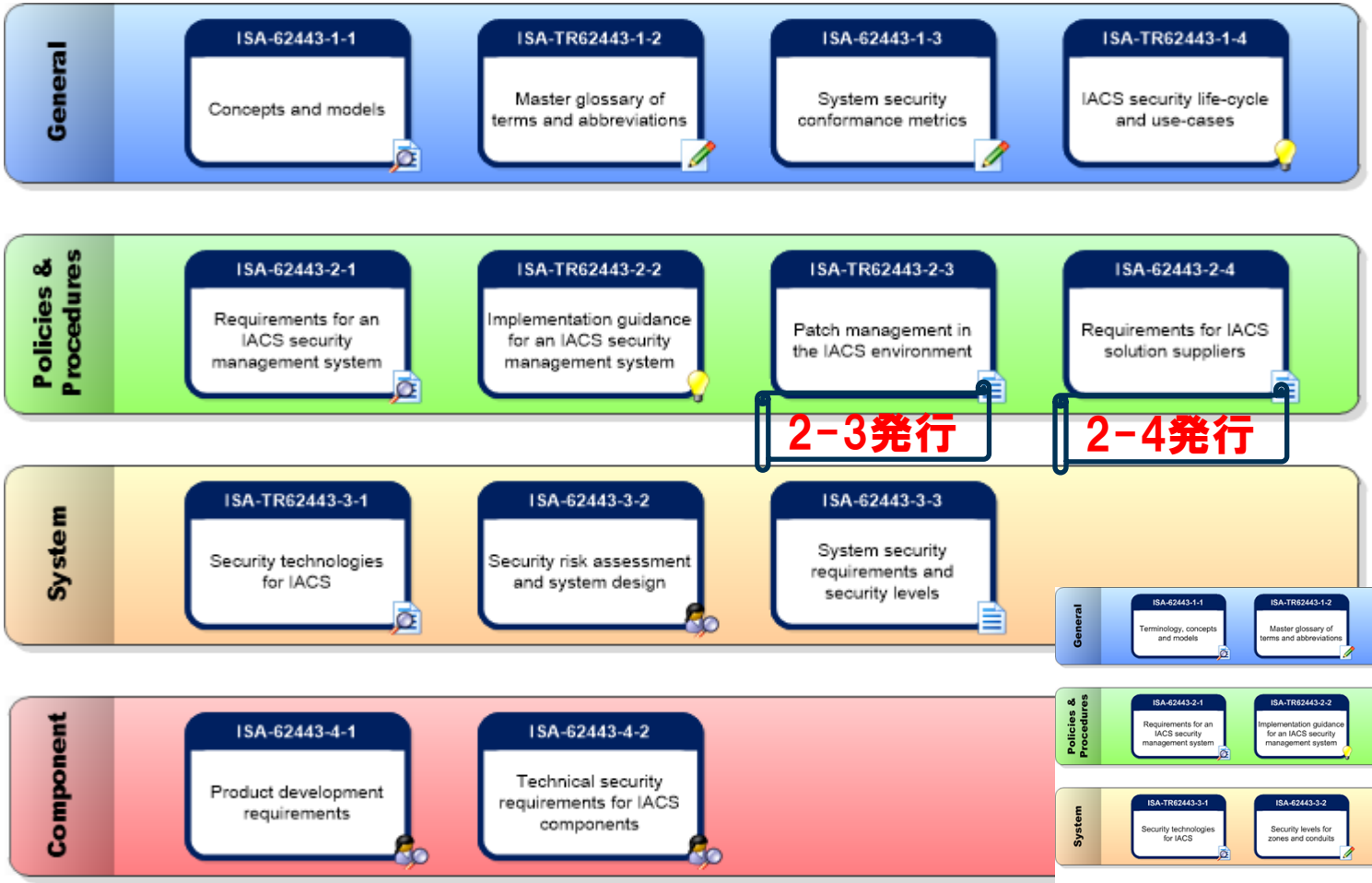
- 米国が警戒する
  中国のサイバー攻撃団
  UgryGorilla
  - 米国の重要インフラを狙う
  - 人民解放軍の関連組織か？

米国が人民解放軍関係者を
サイバー攻撃犯として指名手配

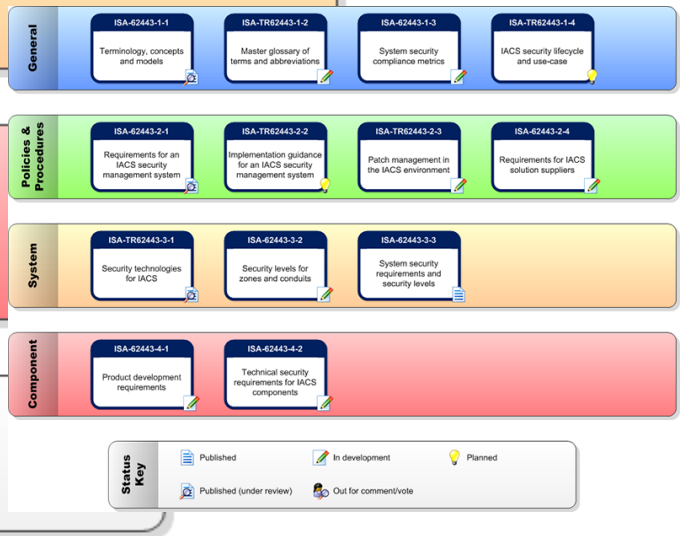
- 中近東地域の活動家
  - イラン
  - IS

- ロシア → ウクライナ (?)
- 北朝鮮 → 韓国 (?)

ISA/IEC 62443シリーズ標準の動き



1年前



http://isa99.isa.org/Public/Forms/AllItems.aspx (→Documents)

ISA Secure EDSA (Embedded Device Security Assurance)認証

- **EDSA (Embedded Device Security Assurance)**
  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	1	2
総件数	7	4	11

- **SDLA (Security Development Lifecycle Assurance)**
  セキュアな**ICS**製品の開発組織を認証
  - **Schneider**社の**3**拠点

10月からドイツの
DAkkSも認証機関に

ISASecure® CSSC DAkkS Deutsche Akkreditierungsstelle

伸びるAchilles認証と奮起が期待されるEDSA認証

表示年時点での認証製品の総数
(その年の新たな認証製品ではない)

製品認証	2010年	2014年	2015年	2016年
Achilles Communications Certification	22	135	216 (GE社が買収)	329
MuDynamics	3	(Spirent社が買収)		
ISA ISCI (EDSA)	0	5	9	11
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

JIPDECはCSMS適合性評価制度(2014年)

- 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)

ISO/IEC 27000シリーズ (ISMS)

- 27000:2014　→ 2015年改訂版発行予定
  Information security management systems - Overview and vocabulary

- 27001 : 2013
  Information security management systems — Requirements

- 27002 : 2013
  Code of practice for information security controls

- 27009 (発行目標2016年)
  Sector-specific application of ISO/IEC 27001 — Requirements

- TR 27019 : 2013
  Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

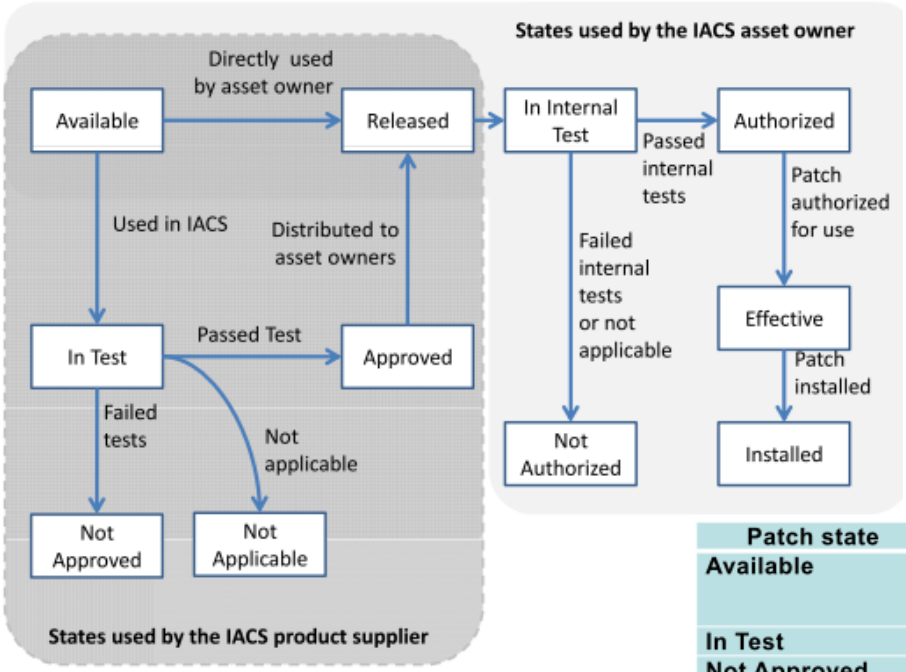
ISA/IEC TR62443-2-3 (パッチ管理)

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

ISA/IEC TR62443-2-3 (パッチ管理)



- パッチの作成から適用までの状態遷移モデルと各状態の定義

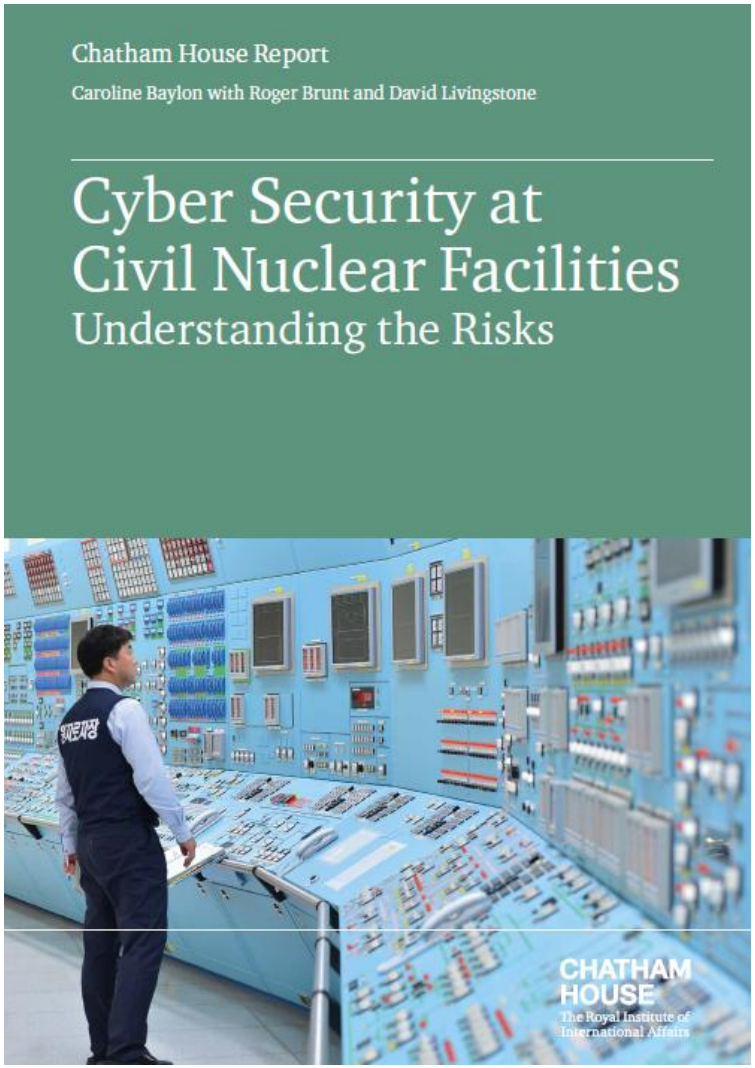
パッチの状態遷移モデル

Patch state	Patch state definition	Managed by
Available	The patch has been provided by a third party or a IACS supplier but has not been tested.	*Asset owner* *Product supplier*
In Test	The patch is being tested by a IACS supplier	*Product supplier*
Not Approved	The patch has failed the testing of the IACS supplier and should not be used until.	*Product supplier*
Not Applicable	The patch has been tested and is not considered related to IACS use.	*Product supplier*
Approved	The patch has passed testing by the IACS supplier.	*Product supplier*
Released	The patch is released for use by the IACS supplier or third party, or the patch may be directly applicable by the asset owner for their internally developed systems.	*Asset owner* *Product supplier*
In Internal Test	The patch is being tested by the asset owner testing team.	*Asset owner*
Not Authorized	The patch has failed internal testing or may not be applicable.	*Asset owner*
Authorized	The patch is released by the asset owner and meets company standards for updatable devices or by inspection did not need testing.	*Asset owner*
Effective	The patch is posted by the assist owner for use.	*Asset owner*
Installed	The patch is installed on the system	*Asset owner*

- パッチ間の同時適用可能性を記述するXMLスキーマも定義

業界ごとに進み始めた課題認識向上への取組み

- 経団連：サイバーセキュリティ対策の強化に向けた提言 (2015年2月17日)
  …情報システムに加えて、組織内に閉じた形で利用されることが多い制御システムも攻撃対象となる。
- サイバーテロ防衛最前線 化学産業の取組み (化学工業日報)
- IAEA： International Conference on Computer Security in a Nuclear World (2015年6月１～5日)



Chatham House報告書

原子力業界のケース

- 第1回原子力業界におけるコンピュータ・セキュリティ国際コンファレンスをIAEAが開催 (6月)
  http://blog.lifars.com/2015/06/03/un-watchdog-nuclear-facilities-vulnerable-to-cyber-attacks/
  - 92か国から650名が参加
  - 天野事務局長：
    世界中の原子力施設は脆弱； サイバー攻撃が日常化
- Chatham House報告書：Cyber Security at Civil Nuclear Facilities
  https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf
  - 物理的なリスクに終始しサイバー・リスクへの配慮が足りなかった
- 米国NRCがサイバー・セキュリティ事故報告規程を発表 (10月)
- Nuclear Threat Initiative：NTI原子力安全インデックス (1月)
  http://www.nti.org/media/pdfs/NTI_2016_Index_FINAL.pdf
  - 日本のサイバー・セキュリティ対策(規制や要件の整備)は75点

その他の動き

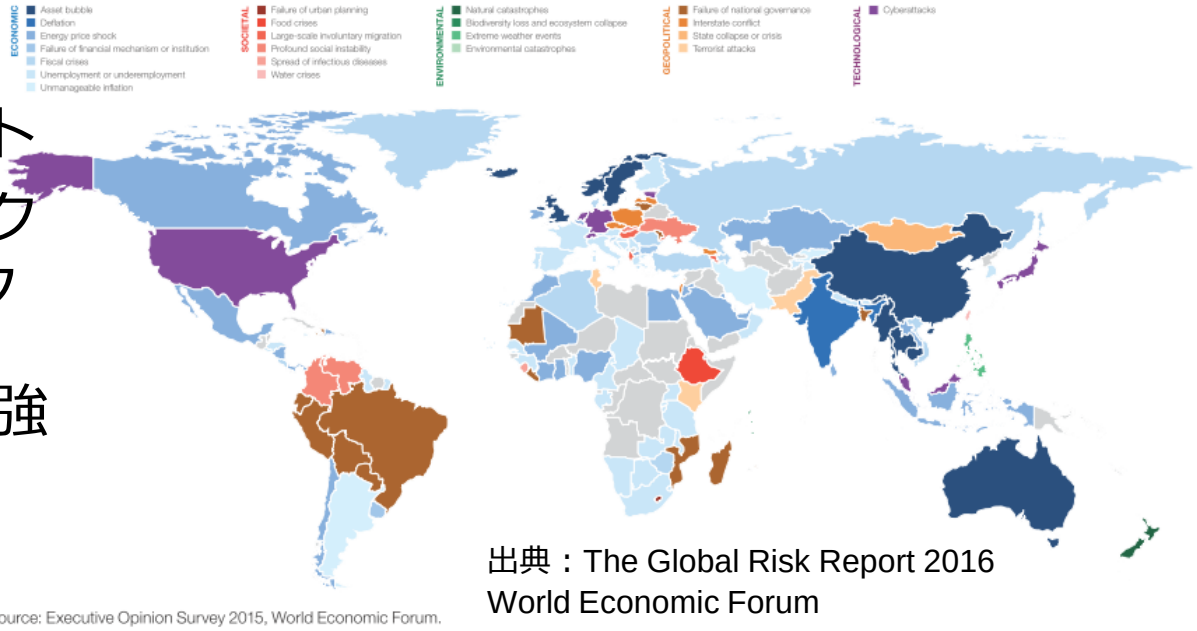
- ドイツで新しいITセキュリティ法が成立し発効 (7月)
  - 重要インフラ事業者に指定された約2,000組織と連邦機関に適用
  - BSIへのインシデント報告とサイバー・セキュリティ標準への準拠とを義務化； 違反組織に最高で10万ユーロの罰金
  - 対象業界ごとに順次規定を策定中 (2016年内の予定)

- Microsoft Windows XP Embeded拡張サポート終了 (2016年1月12日)

情報システムを含めたサイバー・リスクの動向

- ダボス会議でのアンケートによれば
  日本，米国，ドイツ，オランダ，スイス，エストニア，マレーシアでは
  サイバー攻撃が企業にとって最も懸念されるリスク
- 深刻化するサイバー攻撃
  - 高度サイバー(APT)攻撃，ランサムウェア等を用いた脅迫
- 国際的に注目される行事開催
  - 伊勢志摩サミット
  - 東京オリンピック&パラリンピック
- 一層のセキュリティ強化が求められている

企業にとって最も懸念される国別ごとのリスク



出典：The Global Risk Report 2016
World Economic Forum

まとめ

- 当面は高まる一方のサイバー・リスクと考えられます
- 改善に向けた動きが始まってはいるが
  入手できる断片的なツールを組み合わせて
  システム的な強化をはかる努力をするしかありません
- 攻撃者の動向についても情報収集と注意を！

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-form.html

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

今後ともよろしくお願いします

お問合せ、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：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

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