制御システム・セキュリティ 2010年度 動向報告

JPCERTコーディネーションセンター

宮地利雄

2010年度の動向概要

1. 事故・事件
2. 政策・制度の動向
3. 標準化の動向
4. ガイドライン・教科書の動向
5. 米国ICS-CERTの動向
6. JPCERT/CCの活動

2010年前半の事件・事故

- 割賦販売された自動車を遠隔停止
  - 参考： Hacker Disables More Than 100 Cars Remotely (Wired, 2010-03-17; http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+%28Wired:+Index+3+%28Top+Stories+2%29%29)

- 米国テキサス州の電力会社に中国からサイバー攻撃
  - 攻撃は阻止され被害なし
  - 参考：‘Cyber Attack’ Aimed At Texas Electricity Provider (Click2Houston.com, 2010-04-03; http://www.click2houston.com/news/23046216/detail.html)

2010年後半の事件・事故

- 制御システムを狙ったマルウェアStuxnetが報告された
  - ☞ 詳しくは本日の小熊の講演でご紹介します
- 2年前のスペインSpanair航空 5022便墜落事故の原因が中央制御コンピュータのマルウェア感染だったと判明

  参考： Malware implicated in fatal Spanair plane crash (MSNBC, 2010-08-20; http://www.msnbc.msn.com/id/38790670/ns/technology_and_science-security/)

- 制御システム関連製品の脆弱性情報が多数公表された

  参考：JPCERT/CC制御システム関連製品の脆弱性情報; http://www.jpcert.or.jp/ics/vul.html

2010年度の政策・制度の動向

- 電力網に対してより強い規制権限を米国大統領に付与（電力網ならびにインフラ保護法が成立）

  参考： FierceGouvernment, 2010-06-13;
  http://www.fiercegovernmentit.com/story/house-approves-grid-act/2010-06-13

- 米国NSAが重要インフラ（民間保有を含む)へのサイバー攻撃探知システム「Perfect Citizen」の導入を検討との報道

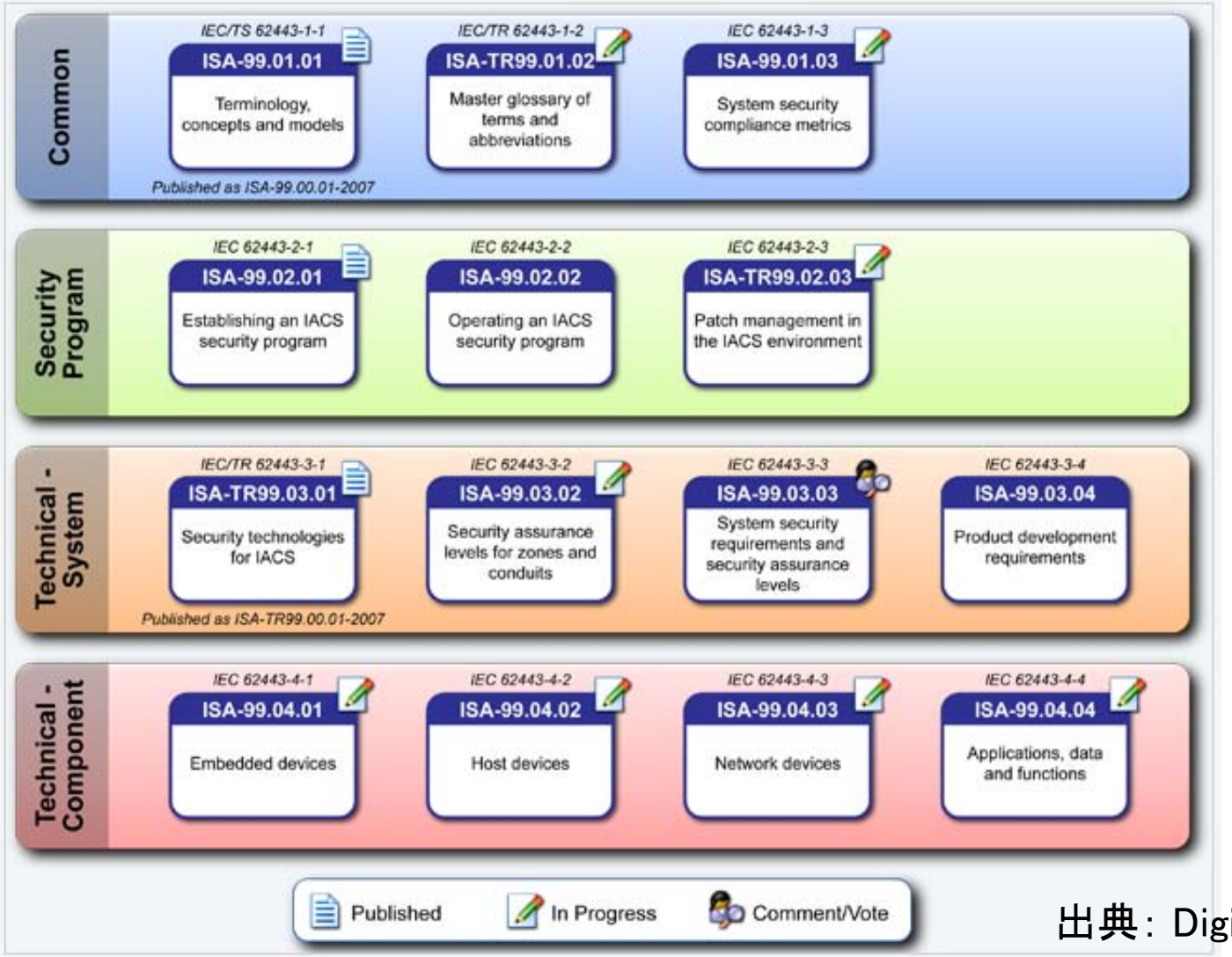
  参考： Cnet, 2010-07-12; http://japan.cnet.com/news/society/story/0,3800104748,20416639,00.htm

IEC 62443-2-1:2010公表

- IEC 62443-2-1:2010(E)が2010年11月に制定され公表された
- 制御システム(IACS: industrial automation and control systems)のためのサイバー・セキュリティ管理システム(CSMS: cyber security management system)の確立に必要な要素(ポリシー，手続，実施手順，要員)を定義し，それら要素を策定するためのガイダンスを提供.
- ANSI/ISA 99.02-2009と同じ内容
- 以前のIEC 62443-2/Ed.1に相当する

- ISAの組織が弱体化しており今後の標準化活動が停滞する可能性も懸念されている

ISAの標準化活動



出典：DigitalBond社

2010年度の新しいガイドラインや教科書

- 米国NISTが「スマートグリッド相互運用性標準のための枠組みとロードマップ 1.0版 」(SP-1108)を公表

  参考：NIST, 2010-01; http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

  - GAOはFERCに規制権限が無いなど多くの課題も残っていると指摘

    参考： 2011-01-12; http://www.gao.gov/new.items/d11117.pdf

- AIM-SECタスクフォースがスマート・メータに関するセキュリティ・ガイドを公表

  参考： 2010-06-22; http://www.smartgridipedia.org/images/9/90/AMI_Security_Profile_-_v2_0.pdf

- ISAから教科書「制御網セキュリティ(Industrial Network Security)第2版」

2010年度の新しい報告書

- サイバー戦争時代の重要インフラ
  - ICS担当の 76%が他のIP網ないしインターネットとの接続を認める

  参考：米国マカフィー，2010-05；http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf

ICS-CERTとは

- 米国DHS(国土保安省)で制御システム・セキュリティを担当する
  - 重要インフラの運用の中核を占めている制御システムのセキュリティ強化を技術面から推進する
  - 国土保安に関する大統領令7号(HSPD-7；2003年12月)に基づく「制御システム・セキュリティ・プログラム」(CSSP)の二本柱の一つ
  - **官民連携**による制御システム・セキュリティ合同WG(ICSJWGと相互補完関係

• ICS-CERTとしての活動開始は2009年秋ころから
• 従来からエネルギー省の資金でこの分野の研究に取り組んできたアイダホ国立研究所が技術的母体

- 役割
  - 制御システムが関連するインシデントへの対応 (事後対応)
  - 制御システム製品の脆弱性の分析と取扱の調整 (リスク除去軽減)
  - 制御システム・セキュリティに関連する各種情報の提供 (予防対策)

ICS-CERTの組織と活動予算

JPCERT CC®

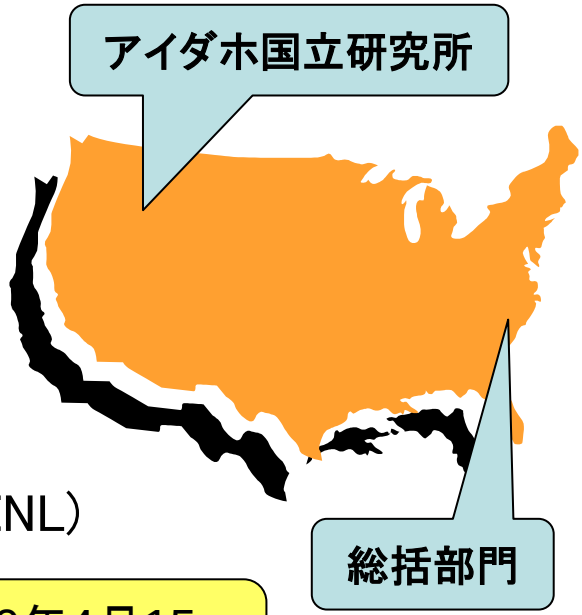
2011年予算：23.6億ドル，常勤職員:2,969名

- 国土保安省(DHS)
  - 国家防護計画(NP&P)：物理攻撃を含むテロ対策計画
    - 重要インフラ防護

2011年予算：8.66億ドル，常勤職員:1,162名

      - 国家サイバー・セキュリティ部(NCSD)
        - 制御システム・セキュリティ計画(CSSP)
          - ICS-CERT

2011年予算：
2730万ドル
(大部分はICS-CERTの予算か？)



- ICS-CERT
  - 統括部門：約10名，ワシントンDC近郊
  - 技術部門：50～60名，アイダホ国立研究所(INL)

予算額などの出典は2010年4月15日にDHSが行った議会証言記録等

ICS-CERTの主な活動

JPCERT CC®

- 注意喚起情報の提供
  - 一般公開情報＋限定公開情報；CIA等からの諜報も含む
- 制御システム関連製品の脆弱性の調査と修正のための調整
  - インシデント対応で見つかる脆弱性
  - ICS-CERTによる独自の脆弱性探索
  - 製品ベンダーとの共同による脆弱性探索
- 国内官民および国際間での連携活動
  - ガイドラインの提供

    JPCERT/CCで
    邦訳公開も多数
  - 教育コースの提供

Stuxnetが攻撃したSiemens社製PCS 7の脆弱性も共同調査がなされていた

国際セミナーの様子
(2009年4月撮影)

ICS-CERTの主な活動

JPCERT CC®

インシデント対応

- 事業者の依頼に応じたインシデント発生時の技術支援活動
- 重大な影響があると判断したインシデントではICS-CERTから要員を現地派遣
  - ✓ フォレンジック技術などによる原因分析，再発防止対策助言
  - ✓ 平均して毎月1回程度の派遣実績
  - ✓ 例えば，上水道のための制御システム・インシデント事例では，給水地域が砂漠地帯で，断水が住民の死活にかかわるため出動
- インシデント対応を通じて見つかる制御システム製品の脆弱性も

ICS-CERTの動きなど

参考: http://www.us-cert.gov/control_systems/

- 提供情報(ウェブ)の拡充
- セキュリティ評価ツールCSATを改版（最新：第3版）
- 制御システム・セキュリティ教育コースの提供
  - 各種のコースが用意されているが，メインは3.5日の技術コース
  - 国際パートナー向けのコースや特別コースの設定も可能

開催地:
アイダホ・フォール
参加費: 無料

- ICSJWG (ICS Joint Working Group): 官民連携
  - 複数のサブグループ活動
    - 国際サブグループには米国外組織も参加が可能
      情報ベースへのアクセス権は保留（米国内利用者の意向を確認中）
  - 年に2回のコンファレンス
    - 4月にサンアントニオ，10月にシアトルで開催された
    - 次回は5月2～5日（ダラス）

2010年度のJPCERT/CCの活動

- **制御システムセキュリティ情報共有タスクフォース**
  - 定期的(隔月)にニュースレターを配付
  - 制御システム利用組織にも利用いただけるよう枠組みを見直し中

- **JEITA・JEMIMA・SICE合同セキュリティ研究部会と合同で セキュリティ対策評価ツールSSATの日本語化とチューニング**
  - SSATは英国CPNIが開発した MS/Excelベースのセキュリティ対策評価ツール
  - ☞ 詳しくは本日の新井様の講演で紹介いただきます

- **制御システムのセキュリティ実態調査**
  - リスク実態と今後の課題を掌握すべく，1～2月に実施中
  - 調査へのご協力に感謝します

2010年度のJPCERT/CCからの公開文書

- 制御システムのサイバーセキュリティ：多層防御戦略
  （米国DHS/INL資料の邦訳；3月公開）
- 人的セキュリティ・ガイドライン
  （米国DHS/INL資料の邦訳；3月公開）
- 推奨プラクティス：工業用制御システムにおけるサイバー・セキュリティ・インシデント対応能力の開発
  （米国DHS資料の邦訳；3月公開）
- 制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用
  （米国DHS/INL資料の邦訳；5月公開）
- グッド・プラクティス・ガイド　パッチ管理
  （英国NISCC(現在のCPNI)資料の邦訳；5月公開）

URL：　http://www.jpcert.or.jp/ics/information02.html

[参考] IPAから公表されている制御システム関連の調査報告書

年度	報告書名	URL
2010	制御システムの情報セキュリティ動向に関する調査報告書（仮題）	TBD
2009	制御システムセキュリティの推進施策に関する調査報告書	http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html
	水道・ガス・電力等の重要インフラ制御システムのセキュリティ向上に関する報告書	http://www.ipa.go.jp/security/fy21/reports/scada/index.html
2008	重要インフラの制御システムセキュリティとITサービス継続に関する調査報告書	http://www.ipa.go.jp/security/fy20/reports/ics-sec/index.html
2003	電力重要インフラ防護演習に関する調査	http://www.ipa.go.jp/security/fy15/reports/infra/index.html
2000	重要インフラセキュリティ対策事業成果	http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/cyber/index_psec.html
1999	「重要インフラにおけるセキュリティ対策の事例調査」調査報告書	http://www.ipa.go.jp/security/fy11/report/contents/intrusion/infrasec_pts/infrasec_pj.pdf
	米国重要インフラにおけるセキュリティ動向調査	http://www.ipa.go.jp/security/fy11/report/contents/intrusion/infrasec_sri/index.html

[参考] JPCERT/CC連絡先

- 一般受付
  - Email: office@jpcert.or.jp
  - 電話: 03-3518-4600 (Fax: +81-3-3518-4602)
  - URL: http://www.jpcert.or.jp/english/
  - Email: cs-security-staff@jpcert.or.jp
- インシデント報告
  - Email: info@jpcert.or.jp
- 脆弱性情報の調整
  - Email: vultures@jpcert.or.jp
- 情報セキュリティ早期警戒情報提供
  - Email: ww-info@jpcert.or.jp

[参考] JPCERT/CCのご紹介

- 1996年に正式発足した非営利の一般社団法人です
- 主要活動のほぼすべてを
  経済産業省からの委託事業として遂行しています
- 国際的なインシデント対応および脆弱性取扱における
  日本を代表する調整機関（National POC (Point of contact) CSIRT in Japan)
- 1998年よりFIRST (Forum of Incident Response and Security Team)の会員
- APCERT (Asia Pacific Computer Emergency Response Team) の運営委員
  ならびに事務局