

# 制御システム・セキュリティ

## 2012年度の動きを振り返る

一般社団法人 JPCERTコーディネーションセンター  
理事 宮地 利雄

1. 制御システムのセキュリティ問題への取組が本格化
2. Stuxnetが口火のひとつとなったサイバー戦争の議論
3. 制御システム製品の脆弱性に関する動向
4. 制御システムのインシデントに関する動向
  - 注目されたインシデント
  - 標的型攻撃
  - マルウェア感染
  - インターネットに直結された制御システム
5. 制御システムのセキュリティ標準の動向
6. 制御システムの管理を巡る新しい思潮

- 経済産業省の「制御システム・セキュリティ・タスクフォース」が中間とりまとめを公表（6月1日）

[http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem\\_security/report01.htm](http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.htm)

- 2011年10月から官民により検討
- その後の対策の方向性を提示

## 制御システムセキュリティ対策の方向性

### 未然防止対策

	日本	北米	欧州
①国際標準化の推進	セキュリティ基準	欧米の体制、動向をにらみながら、戦略的な標準作成、及び、評価・認証スキームの立ち上げを推進。	業界主導、国支援
②テストベッドの構築	共通の検証設備（テストベッド）	業界と国の共同（一部重要インフラは国主導、政府機関におけるテストベッドにおいて蓄積された検証データ、知見、ノウハウ等が民間機関による評価認証と連携）	
③評価・認証スキームの構築	評価認証	欧米の制御システムの評価・認証は、民間単独事業だったものが、公的評価・認証や標準適合のためのテスト結果提供という形を取りながら公的性格を強めつつある。	

### 事後対策

#### ④インシデント対応体制の構築

・米国の工業用制御システムのレスポンスチーム（ICS-CERT）においては、インシデント現場への技術派遣を実施。我が国も要検討。  
 ・また、パッチ適用の動作試験や、注意喚起情報の公開可否の判断ルールを検討。

### 共通対策

#### ⑤人材育成、ユーザ企業への普及啓発の推進

ハイエンド人材等の育成、安全性確保に対するリスクとコスト意識醸成を含めたユーザ企業等への普及啓発

# 制御システム (ICS) のセキュリティ問題への取組が本格化

- 国内では、技術研究組合「制御システム・セキュリティ・センター」(CSSC) が発足

<http://www.css-center.or.jp/>

- 2012年3月6日に設立;理事長に新誠一教授(電気通信大学)
- 12組織の組合員(2012年10月現在)
- 宮城県多賀城市にテストベッドを構築中

- JPCERT/CCも体制を拡充し、ICS関連の脆弱性とインシデント対応にフォーカスして取組を強化

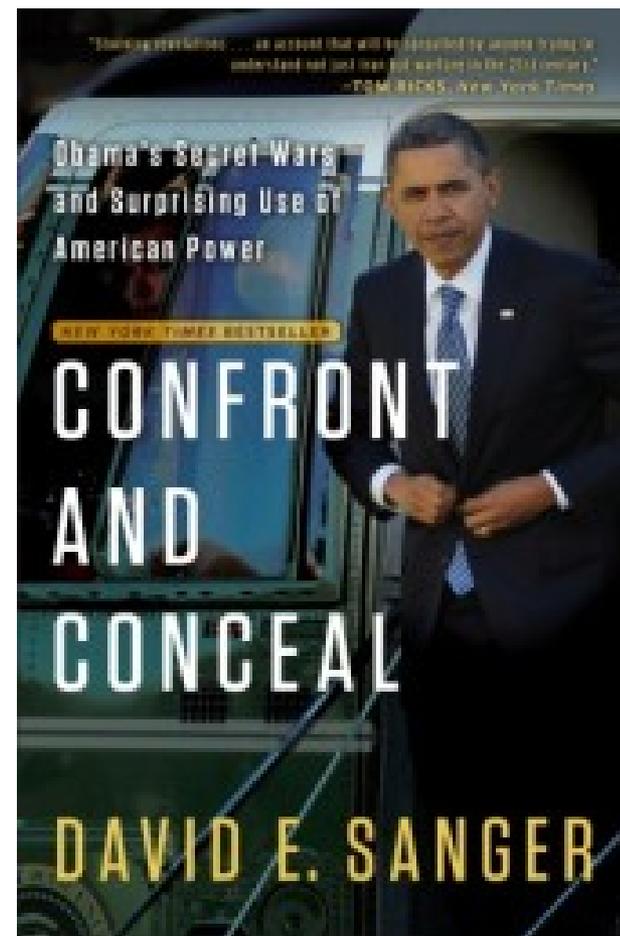
<http://www.jpCERT.or.jp/ics/>

- VECは第1回「VEC制御システムセキュリティ対策ソリューションカンファレンス」を開催(2012年11月28日)

<http://www.vec-member.com/>

# Stuxnetから始まった中近東でのサイバー戦争？

- Sanger著「対決と潜伏 – オバマ大統領の秘密の戦争と米国の能力の驚くべき利用」の出版
  - Stuxnetでイランを攻撃する大統領命令
  - 米国政府からはコメント無し
- Stuxnetと類似した構造をもつとされる複数のマルウェアが見つかる
  - Duqu, Flame (Flamer), Gauss
  - 直接にはICSを狙わずスパイ活動
- マルウェア「Shamoon」
  - Windowsのシステム・ディスクを破壊
  - イランがサウジアラビアを攻撃？



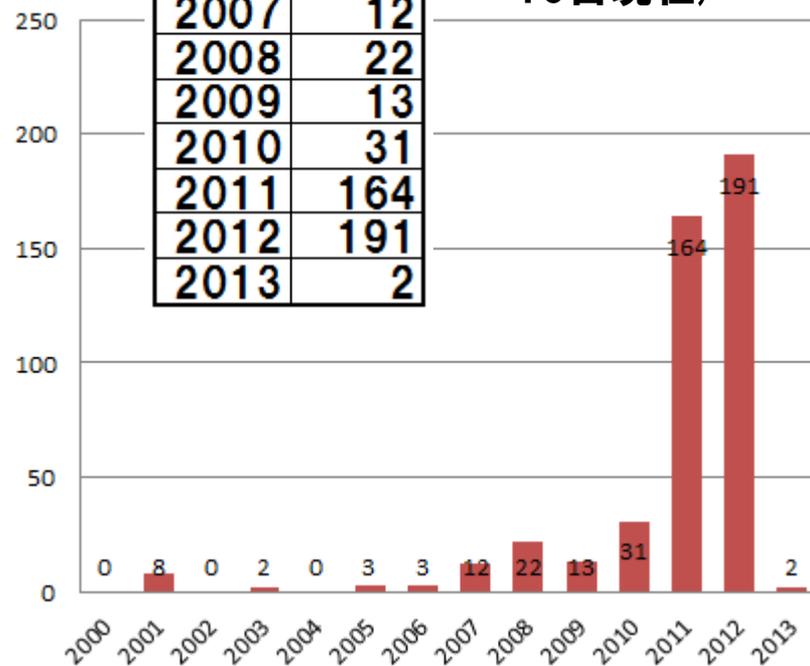
- 各国政府が「重要インフラへのサイバー攻撃は戦争行為」とみなす方向で検討や  
声明
  - － サイバー空間を陸海空とならぶ軍事戦略次元と位置づける
  
- 国家が背後で操るサイバー攻撃が米国の重要インフラに向けられ社会的な混乱を招く事態を米国は強く警戒
  - － 大統領令に基づく官民連携の強化をはかる
  - － 重要インフラ関連のICSを含むシステムの強化を急ぐ
  - － 重要インフラ関連事業者へのAPT的な攻撃によるICSを含むシステム情報の流出への対策
  - － 特に、エネルギー関連業界に注力
    - ガス・パイプライン業界、電力業界など

# 制御システム製品の脆弱性の報告件数

- 増加傾向が続く  
制御システム用製品の脆弱性の報告
- 米国ICS-CERTが脆弱性の取扱ポリシーを改訂
  - － いわゆる「45日ルール」を明示
- 米国ICSJWGのベンダーWGがベンダーのための脆弱性取扱ガイドラインを発行
  - － 脆弱性情報の開示に積極的な姿勢

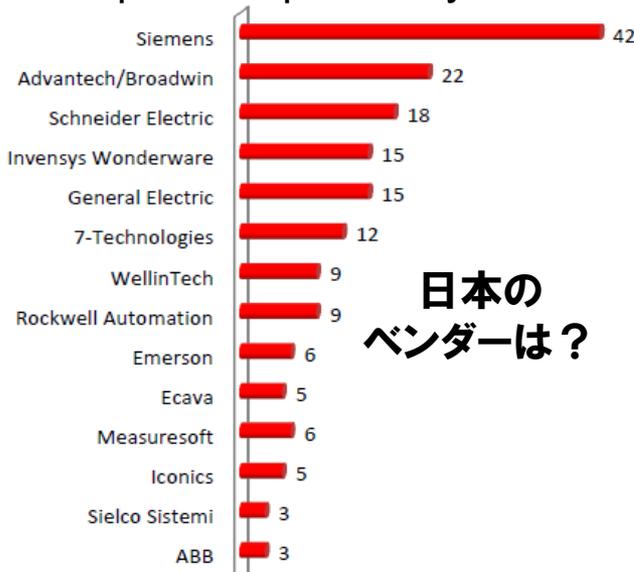
年	件数
2000	0
2001	8
2002	0
2003	2
2004	0
2005	3
2006	3
2007	12
2008	22
2009	13
2010	31
2011	164
2012	191
2013	2

OSVDBに登録された制御システム製品の脆弱性件数  
(2013年1月10日現在)

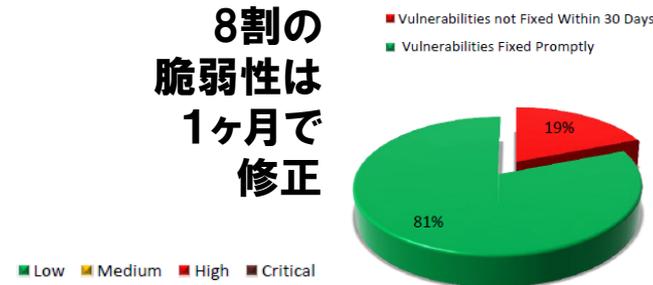


# 制御システム製品の脆弱性の傾向 ～ Positive Technologies社による調査報告から ～

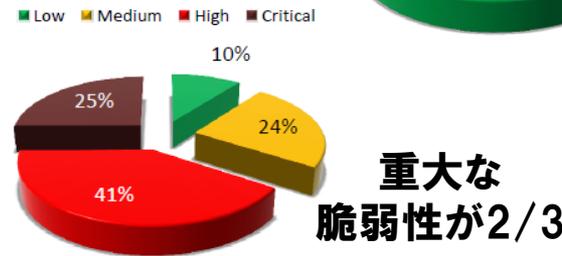
[http://www.ptsecurity.com/download/SCADA\\_analytics\\_english.pdf](http://www.ptsecurity.com/download/SCADA_analytics_english.pdf)



日本のベンダーは？

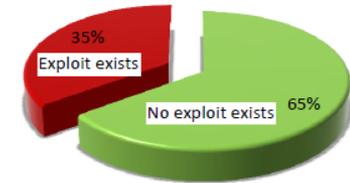


8割の脆弱性は1ヶ月で修正

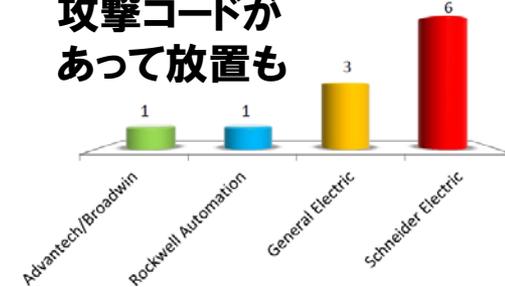


重大な脆弱性が2/3

35%に攻撃コード

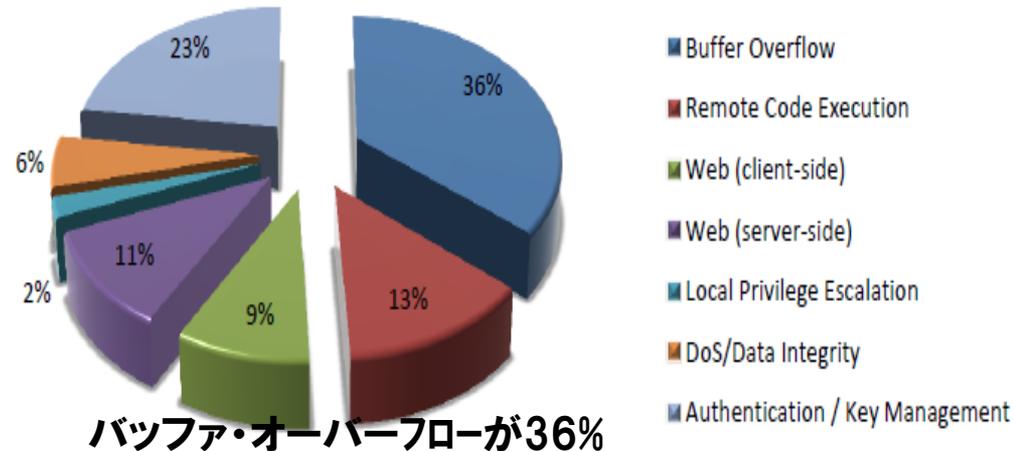
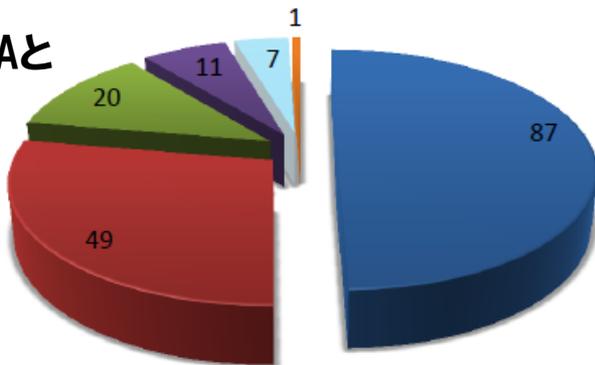


攻撃コードがあっても放置も



■ SCADA ■ HMI ■ PLC ■ Hardware ■ Software ■ Interface/Protocol

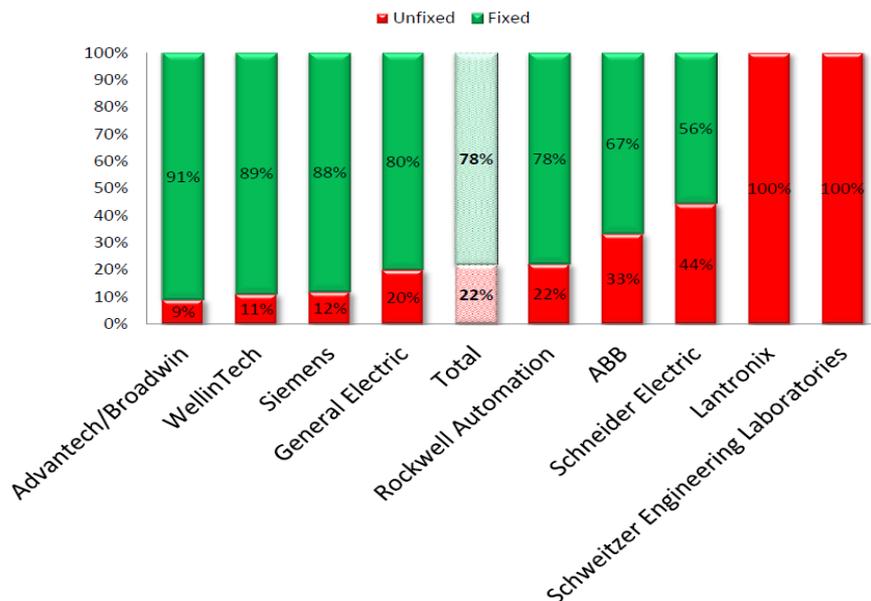
SCADAとHMIで3/4



バッファ・オーバーフローが36%

■ 海外の一部ベンダーではセキュリティ対応の社内体制を整備して脆弱性への対応と積極的な情報開示を開始

■ ベンダーにより対応姿勢が二極化



> Home > Technology Areas > IT-Security > Siemens CERT

### To raise the bar against hackers

Siemens IT Security is protecting internal IT infrastructure and supporting secure product development. It is established as an independent and trustworthy partner to develop preventive security measures, assess information security and respond to security incidents. With these activities, it helps its customers worldwide to achieve the necessary security level for effective protection against hacker attacks.



### Assess - Prevent - Respond

IT Security serves as the central point of contact for secure IT infrastructure, secure Siemens products and CERT services. It supports in developing systems securely, assessing information security and responding to security incidents.

### Global Networking and Competence as Success Factors

Siemens IT Security has been a leader in establishing communities and sharing best practice principles due to its longstanding project experience within the Siemens group. Moreover, the knowledge exchange is enhanced by active cooperation with technical communities and collaboration with leading industry and university partners.

Highly qualified experts for subjects such as secure architectures, application security, forensics or secure software development offer flexible and tailored consulting services for the Siemens group and its customers. The research activities proactively investigate future technological challenges and develop practical solutions.

### Extract from Siemens CERT portfolio:

- CERT services
- Security assessments and information security reviews
- Development of secure architectures
- Secure coding and security lifecycle support
- Security measure plans
- Secure coding
- Embedded systems security
- Incident handling and security monitoring

Corporate Technology  
The Siemens Think Tank

Text Size

- > Siemens CERT
- > ProductCERT Security Advisories
- > Siemens Vulnerability Handling

### Related Links

- > Corporate CERT Services (Intranet)
- > Industrial Security Website
- > German CERT Association (in German)
- > Forum of Incident Response and Security Teams
- > International Information Integrity Institute

### Downloads

- Reliable IT security for energy automation

### Contact

- johann.fichtner@siemens.com

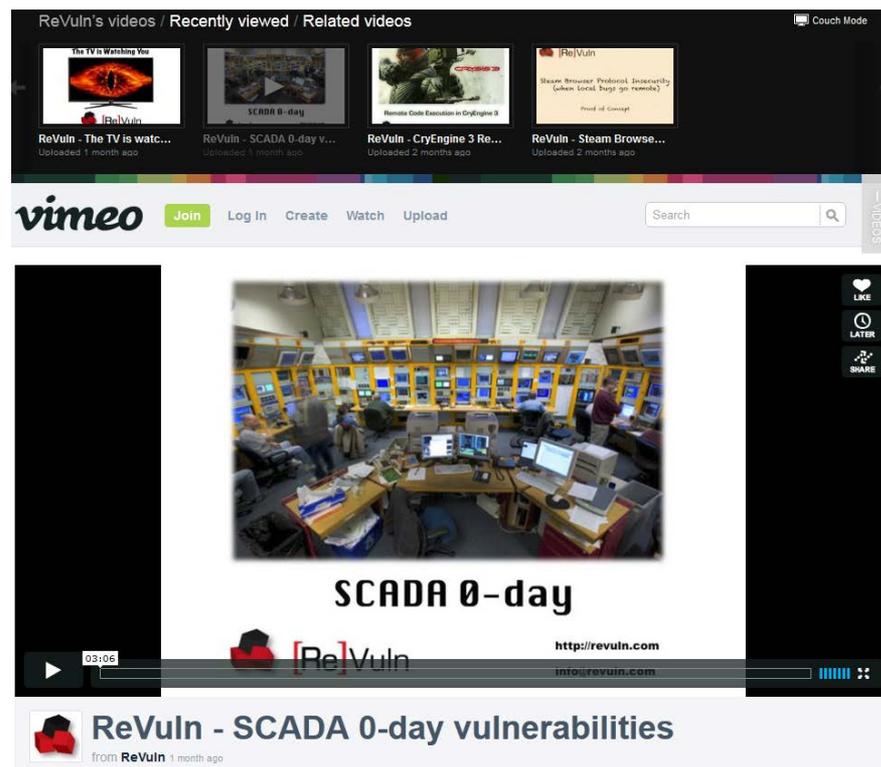
# ICS製品の脆弱性情報を 販売する会社までが現れる

■ 対策のない新しい脆弱性の  
情報を製品利用企業向けに  
購読契約ベースで販売

■ 製品開発ベンダーや  
CERT機関には売らない

■ 事業的な成否は未知数：  
— 対策のない脆弱性情報を  
ICS利用企業が買って  
どれだけ価値があるのか？

■ IT関連製品に関しては、製品ベンダーやIDS/IPSベンダーの一部が新しく発  
見された脆弱性情報を買い取っている



ReVuln's videos / Recently viewed / Related videos

ReVuln - The TV is watc...  
Uploaded 1 month ago

ReVuln - SCADA 0-day V...  
Uploaded 1 month ago

ReVuln - CryEngine 3 Re...  
Uploaded 2 months ago

ReVuln - Steam Browse...  
Uploaded 2 months ago

vimeo Join Log In Create Watch Upload Search

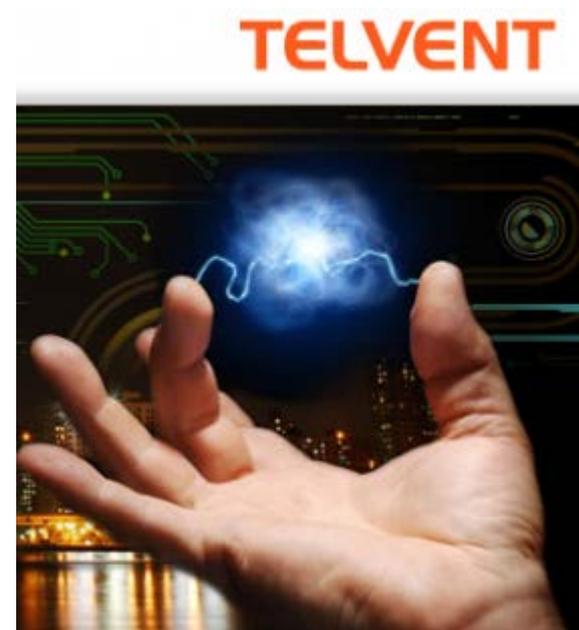
SCADA 0-day

ReVuln  
http://revuln.com  
info@revuln.com

ReVuln - SCADA 0-day vulnerabilities  
from ReVuln 1 month ago

- **利用者を震撼させた  
制御システム・ベンダーのシステムへの中国人ハッカーの侵入**
- **米国ICS-CERTは、標的型の攻撃の中で、制御システムが標的とされることを警戒**
  - 包括的なAPT (Advanced Persistent Threat) 対策の一環としての制御システム・セキュリティ対策を進める
- **マルウェアによる制御システムの異常も散発**
  - アジア太平洋地域にある刑務所の監視用CCTVがConfikerに感染してダウン (Symantec社)
- **インターネットに直結された制御システムが増加？**

- Telventカナダ社が「中国人ハッカーに侵入された」と顧客に通知
  - 米国やカナダ, スペインに事業展開
  - マルウェアをインストールされ,  
中核製品の一つのプロジェクト・ファイルが盗まれた
- Telventカナダ社では客先に設置された制御システムの遠隔監視サービスも提供
  - 顧客の多くは電力会社



# 米国における重要インフラ事業者への 標的型サイバー攻撃が活発化

## ■ 米国ICS-CERTが重要インフラ事業者への標的型サイバー攻撃に 注目

- サイバー攻撃がICSに及んだ事例は極めて少ないが、社内情報システム内でICS関連情報を探し回った形跡
- 標的になっているのは、天然ガス・パイプライン事業者や電力事業者

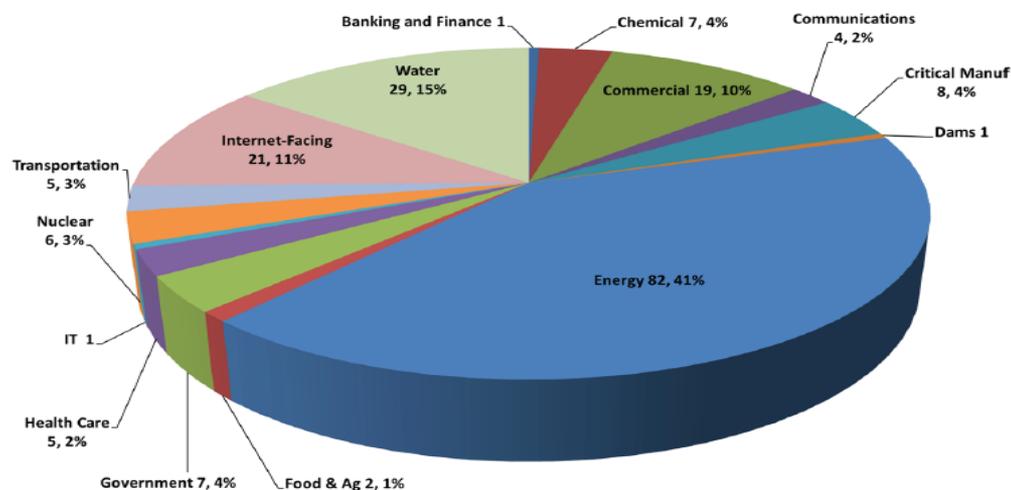


Figure 4. Incidents by Sector – Fiscal Year 2012

\*Fiscal year 2012 represents the time period of October 1, 2011–September 30, 2012



(頻発していると見られますが、以下は公表された事例です)

- **アジア太平洋地域にある刑務所の監視用CCTVがConfikerに感染 (Symantec社による情報)**
  - Windowsマシンがダウンして監視が不能に
  
- **タービン制御システムの約10台のコンピュータがウィルス感染したと電力会社が米国ICS-CERTに相談**
  - 定期保守期間中にソフトウェア更新用のUSBメモリ経由で感染
  - 運転の再開が予定よりも3週間遅れることに
  - 別の電力会社でも類似のマルウェア感染事例

## ■ コンピュータ (インターネット・サーバ) 検索エンジン Shodan

<http://www.shodanhq.com/>

## ■ SHINEプロジェクト

- Shodanを利用して  
制御システム製品を検索
- 数十万台規模の製品を発見
- 日本の事例は少数
- 攻撃されて大問題を起こしそうな  
制御システムは多くはなさそう
- 4割は脆弱との報告も

## ■ 制御システムの操作や監視を インターネット経由の携帯機器で 実現するよう求める顧客も

The image shows a screenshot of the Shodan website. The top navigation bar includes links for Main, Exploits, Research, Videos, Anniversary Promotion, Register, and Login. The main content area features a search bar and the headline "EXPOSE ONLINE DEVICES." Below this, it lists various device types: WEBCAMS, ROUTERS, POWER PLANTS, IPHONES, WIND TURBINES, REFRIGERATORS, and VOIP PHONES. There are two buttons: "TAKE A TOUR" and "FREE SIGN UP". A world map is visible in the background, with some areas highlighted in red. Below the main content, there are three sections: "DEVELOPER API" (Find out how to access the Shodan database with Python, Perl or Ruby), "LEARN MORE" (Get more out of your searches and find the information you need), and "FOLLOW ME" (Contact me and stay up to date with the latest features of Shodan). At the bottom, there is a section titled "IN THE PRESS" with a map of North America showing numerous red location markers. Text snippets from news articles are visible, such as "Shodan pinpoints shoddy industrial controls." and "Shodan is the Google for...".

## ■ IEC 62443: 策定作業が続いている

### – セキュリティ管理に関する標準の動き

#### ■ 2-1: 改訂作業中

– ISO27000シリーズとの整合性を高める方向

– Stuxnetに対抗できるには1/3の管理策の見直しが必要とISA-99のWGが報告書

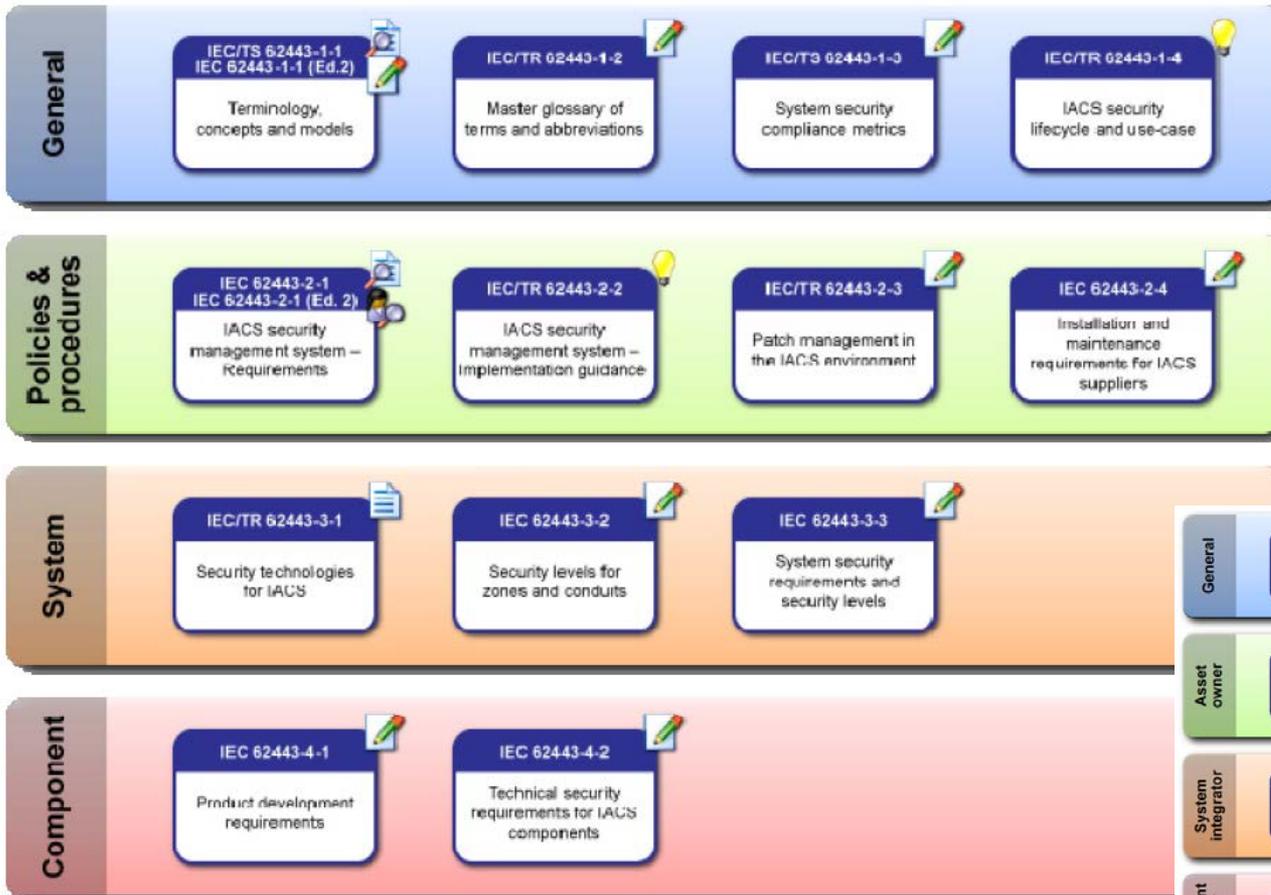
#### ■ 2-2: 策定を中止; 別の標準を2-2として新規追加

## ■ 米国NARCの電力業界向けセキュリティ標準CIPの改訂

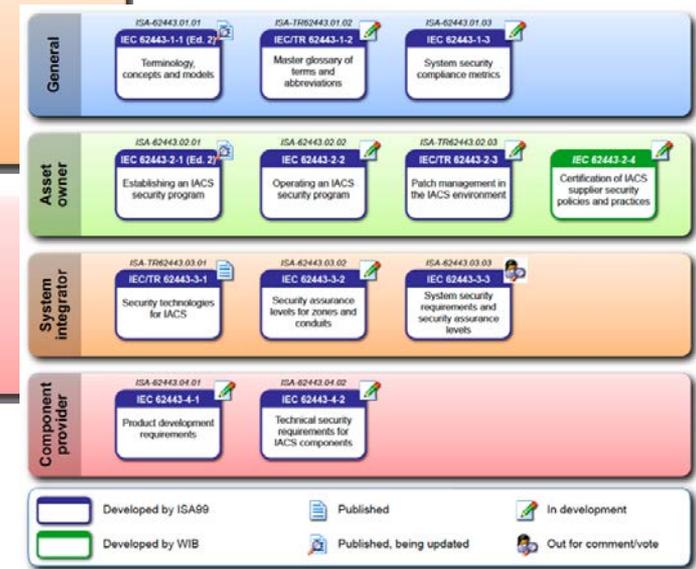
– 第5版を策定中

– FERC (連邦電力規制委員会) は第4版のCIPを承認して適用

# IEC 62443シリーズ

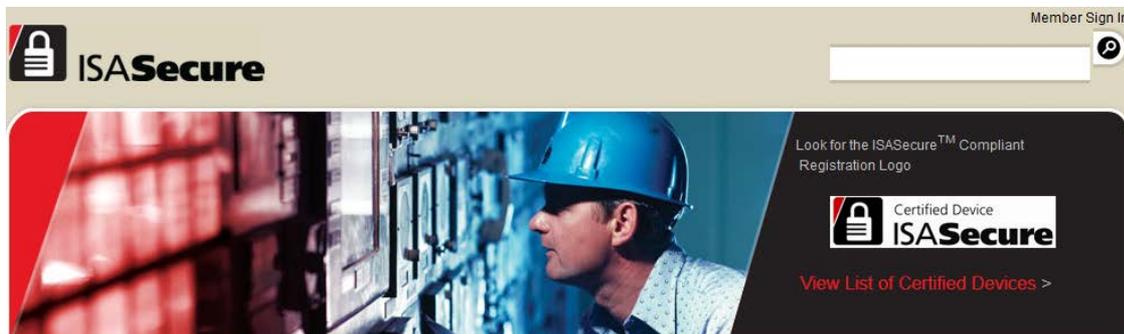


- ライフ・サイクルと利用事例を追加 (1-4)
- セキュリティ管理の運用を中止し、実現ガイドに置換 (2-2)
- ISAのWGがStuxnet対策として2-1は不十分との報告書



## ■ ISASecureの認定機器

- まだ4製品のみ
- 仕様上のセキュリティ不備は認定審査対象外



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

## ■ IPA～ISCI (ISA Secure Compliance Institute) の連携

- IPAが認証仕様の邦訳を作成

- **制御システムとコンピュータ・システムとの本質的な違いは何か？**
  - 物理的な設備や施設を基軸としたシステム
  - 情報システムとは無関係に導入し運用されてきた
  - 情報システム技術を次々と取り込み  
構造的には情報システムと大きくは違わなくなりつつある
  
- **IT (Information Technology) vs  
OT (Operational Technology)**
  
- **情報システム部門がOT領域もカバーする方向へ (?)**
  - ベンダーは顧客の情報システム部門とも接点

御静聴ありがとうございました

**2013年を  
日本の制御システム・  
セキュリティが  
実質的に向上する年に！**