オープン化と制御システムセキュリティ対策
～国際規格と装置認証と安全とリモートサービス～

PLCopen Japan
OPC Foundation
NECA 制御システムセキュリティ研究会
制御システムセキュリティ関連団体合同委員会
VEC事務局
村上正志

Agenda

1. **制御装置や制御システムにとってのサイバー攻撃の脅威**
2. オープン化と制御システムセキュリティ対策

世界中で起きている制御システムを対象にしたサイバー攻撃事例

2012年5月米国ミシガン州の天然ガスパイプラインをターゲットに中国からサイバー攻撃された。8日米国土安全保障省当局者は8日、AFP通信に対し、米国の天然ガスパイプライン会社がサイバー攻撃の標的になっていると明らかにした。
2010年7月に発生の加エンブリッジの原油漏出事故原因は安全対策の機能停止

2003年1月、米オハイオ州にある原子力発電所の制御システムがウイルスに感染して、5～6時間にわたって安全管理システムが停止。

Stuxnetは、2010年6月に発見された。イランのウラン濃縮施設を標的につくられたマルウェア兵器。8400台中4600台を交換することになった。

複数の米軍高官は28日、北朝鮮のサイバー攻撃の能力は高まっているとの見方を明らかにするとともに、2012年は同国が軍事的挑発を仕掛ける機会が多くあると警戒感を示した。

イランの核施設に使用されていたシーメンス製の制御システムは、日本の水道施設でも100台以上使用されており、この一部がスタックスネットに感染していた。

米国の交通信号表示

豪州では水道運営会社に雇用を拒否された元契約社員の技術者が、腹いせに下水処理施設の制御システムを不正に操作してポンプを止め、100万キロリットルもの汚水が周辺に垂れ流されたという。

03年8月に米東部にある鉄道会社で、信号制御システムがウイルスに感染して列車のダイヤが乱れた。

11年2月には、ブラジルの発電所でも制御システムがウイルスに感染し、運用停止に追い込まれている。

2012年サウジアラビアの石油会社大手サウジアラムコが、8月中旬におよそ30,000台にのぼる同社のワークステーションがサイバー攻撃の被害を受けたと認める声明を出した。

2011年8月19日付け中国国営テレビで中国軍部のサイバー攻撃部隊の存在を放映

サイバー攻撃の遍歴

敵を知り

2006 2008 2010 2011 2012 2013

情報セキュリティ

バグ

コンピュータウィールス

Serverを攻撃

Dos攻撃／Bots

大量データを送りつける

Serverを乗っ取り

マルウェア／ワーム

Doqu

Flame

Gauss

DATAを破壊

機密情報を搾取

目的の情報ファイルを見つけたら、指定したサイトへアップ

あらゆる手段を使って目的の情報ファイルをマルウェア作成者へ届ける。

あらゆる手段を使って制御システム構成情報をマルウェア作成者へ届ける。

2006 2008 2010 2011 2012 2013

制御システムセキュリティ

Stuxnet

制御システムを操作

制御システムを破壊

Shamoon

装置を操作

装置を破壊

米国政府がイラン核開発妨害プロジェクト「オリンピックゲーム」開始：ニューヨークタイム紙による

イスラエルが参加で加速、イラン中部ナタンズにある各施設へサイバー攻撃：ニューヨークタイム紙による

イランの研究者のコンピュータを介してウィルスがインターネットに流出：ニューヨークタイム紙による

Stuxnetの特徴

敵を知り

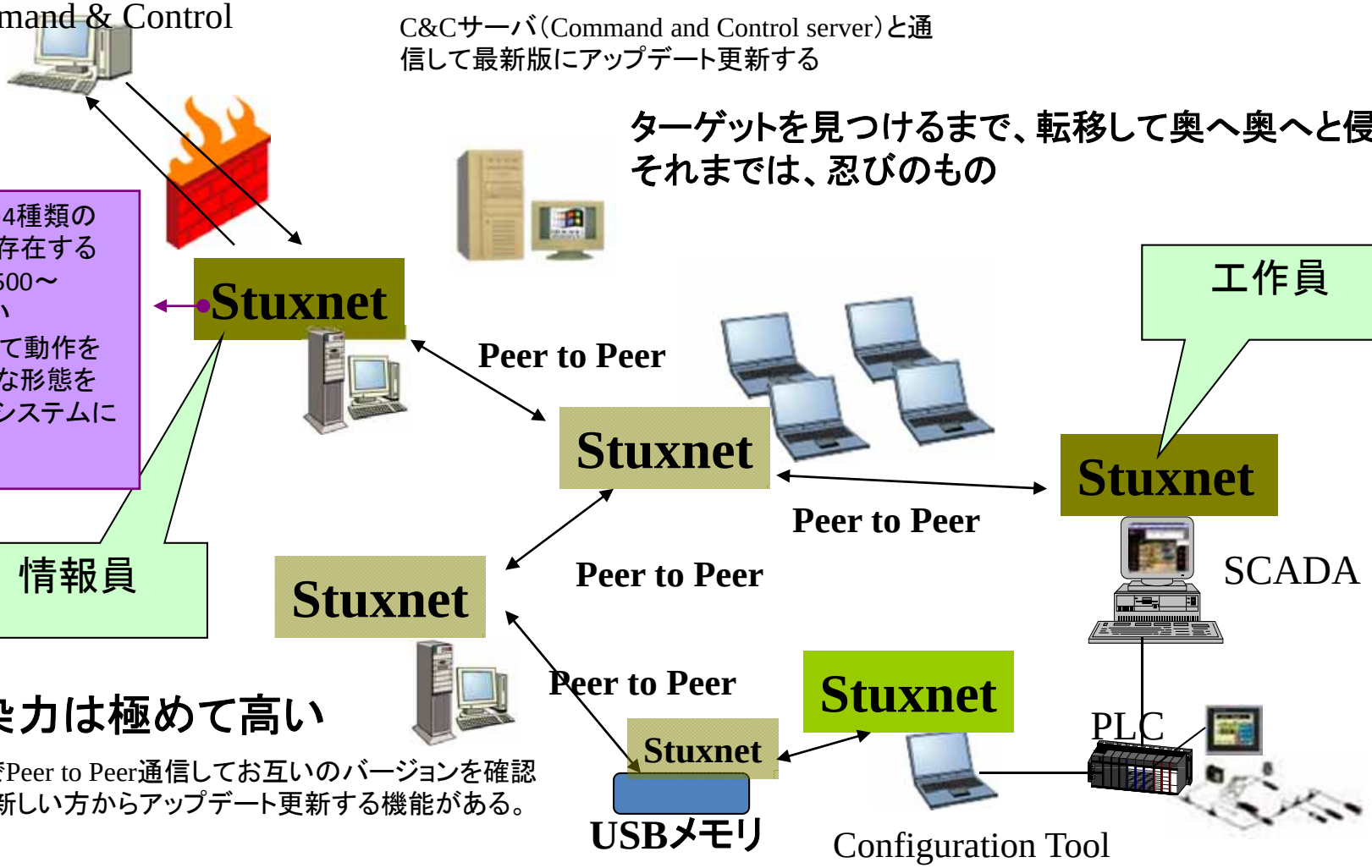
Stuxnetの司令部

C&C Server
Command & Control

C&Cサーバ（Command and Control server）と通信して最新版にアップデート更新する

ターゲットを見つけるまで、転移して奥へ奥へと侵入
それまでは、忍びのもの

亜種を含め4種類のバイナリが存在するサイズは、500～600KBぐらい
環境に応じて動作を変え、多様な形態をとって標的システムに展開する。



情報員

感染力は極めて高い

Stuxnet同士でPeer to Peer通信してお互いのバージョンを確認し、古い方は新しい方からアップデート更新する機能がある。

Peer to Peer通信で双方向の情報を最新に上げていくことでC＆C Serverの指令を伝達する方法
つまり、C&Cサーバからの指令をStuxnet同士で伝え合う。最新指令を伝達する機能がある。

Shamoon　敵を知り

サウジアラビアの企業を攻撃するために、イランが造ったと思われる。

持っている機能
1. Dropper：PCに感染し、必要となるソフトを仕掛ける機能
2. Wiper：破壊工作機能モジュール
3. Reporter：情報搾取モジュール（攻撃者に目標の情報を送信）

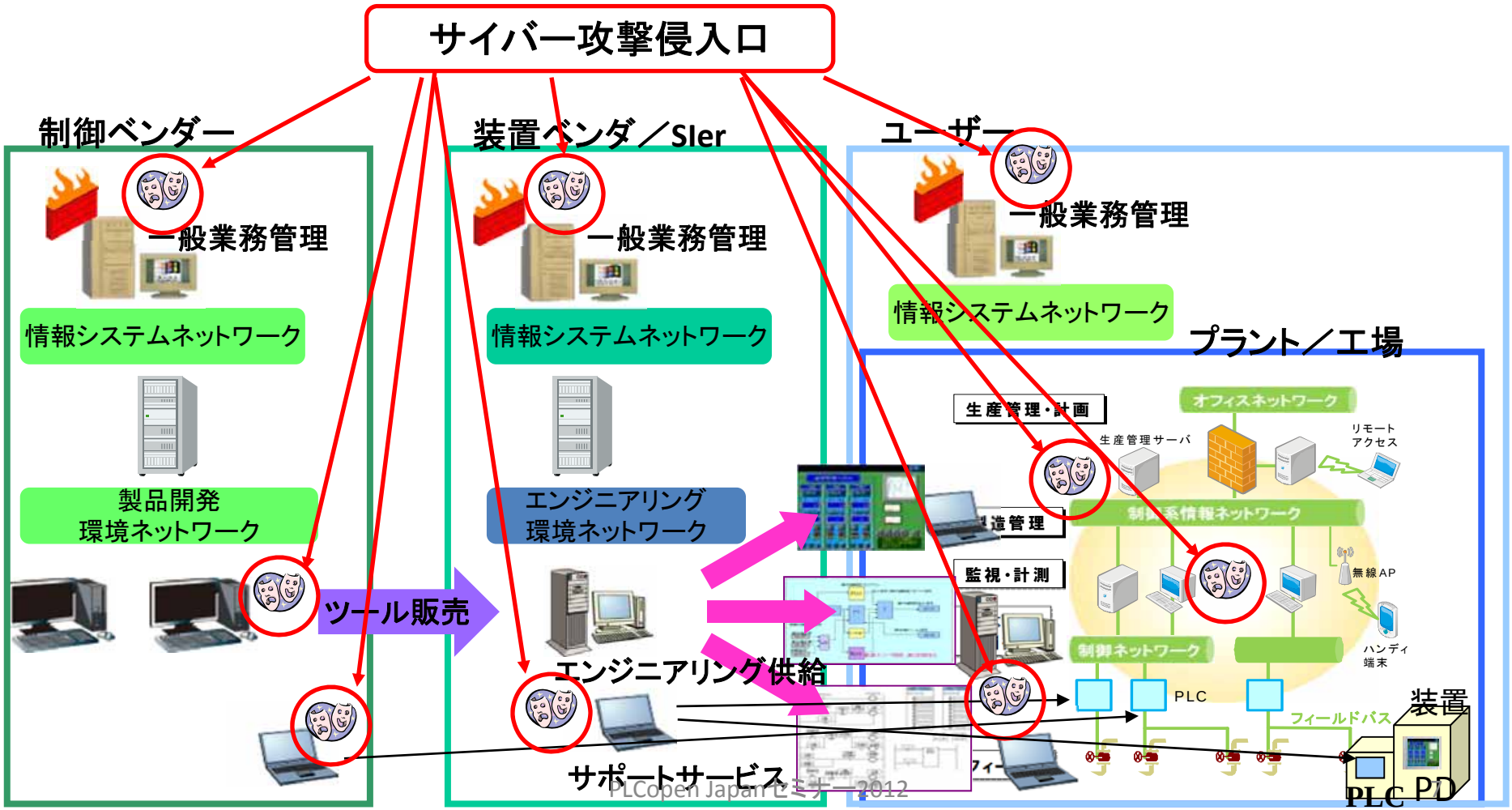
影響
Wiperモジュールの高いシステム破壊機能により、感染した組織は知的財産（IP）の窃盗、重要システムの停止など、運用上の影響を受ける可能性がある。感染したシステムの種類や数によって、実際の影響度は異なる。

マスターブートレコードの構造

アドレス		内容		サイズ（バイト）
Hex	Dec			
0000	0	ブートストラップローダ		446
01BE	446	第1パーティション	パーティションテーブル（各16バイト）	64
01CE	462	第2パーティション		
01DE	478	第3パーティション		
01EE	494	第4パーティション		
01FE	510	55h	ブートシグニチャ; 0xAA55	2
01FF	511	AAh		
MBRサイズ				512

サイバー攻撃の侵入口

- 制御ベンダの製品開発環境から、装置ベンダの開発環境、SIerエンジニアリング環境、ユーザーの現場環境と、サイバー攻撃の侵入口は、存在する。



我々にとって何が脅威か？

- **インターネットに国境は無い**
  - Stuxnetのターゲット⇒イランのウラン濃縮施設の遠心分離機制御システム⇒フィンランドのウラン濃縮施設の遠心分離機制御システムも同じ構成
  - **巻き添えになる脅威**
- **サイバー戦争が本格的になっている**
  - イラン⇒イスラエルの軍事施設、米国の石油・化学の施設（シェル、モービルなど）、サウジアラビアの公共施設⇒米国制御ベンダの制御製品エマーソン（、ハネウェルなど）⇒それらと同じ制御システム構成の施設
  - 中国⇒米国の原子力発電所の制御システムに関する情報入手
- **サイバー兵器**
  - 情報収集ツール：Duqu、Flame、Gauss
  - 攻撃ツール：Stuxnet、Shamoon
- **サイバーテロ集団が増えている**
  - アノニマス、ラルズセック
- **競合企業の攻撃**
- **標的攻撃される場合**
  - **緻密な攻撃方法**
    - 企業機密情報搾取：Duqu／Flameタイプ
    - 制御システム攻撃：Stuxnetタイプ
- **工場操業停止・出荷できない**
  - 直接的損害／間接的損害
  - FDAオーディットで認定停止（**再稼動しても出荷できない**）

製造関連情報の消失

制御システムの停止
製品の生産不可

不良品の製造・出荷
顧客の信頼喪失

爆発・火災
産業廃棄物垂流し

認可取り消し

ICS-CERT Report June 28 2012

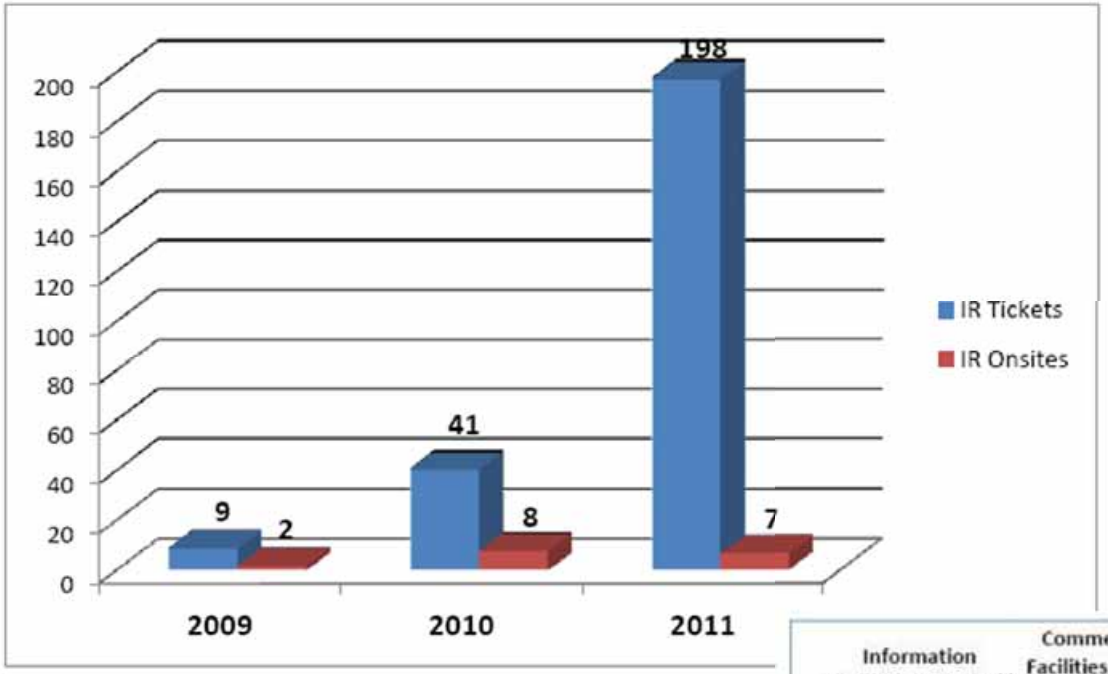


Figure 1. ICS-CERT incident response trends data.

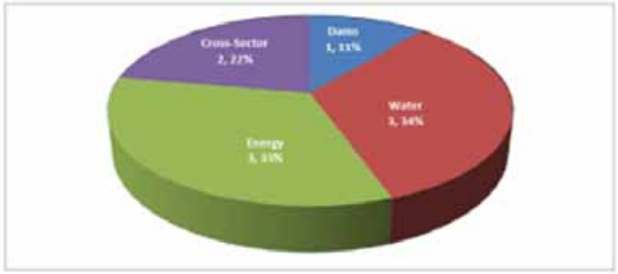


Figure 2. Incident reports by sector (2009).

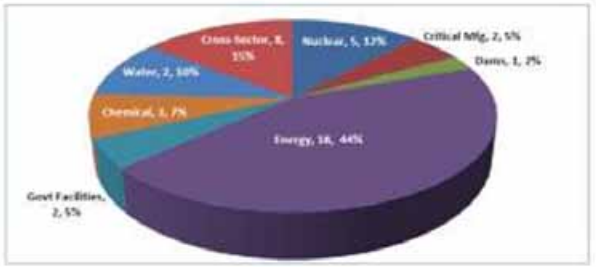


Figure 3. Incident reports by sector (2010).

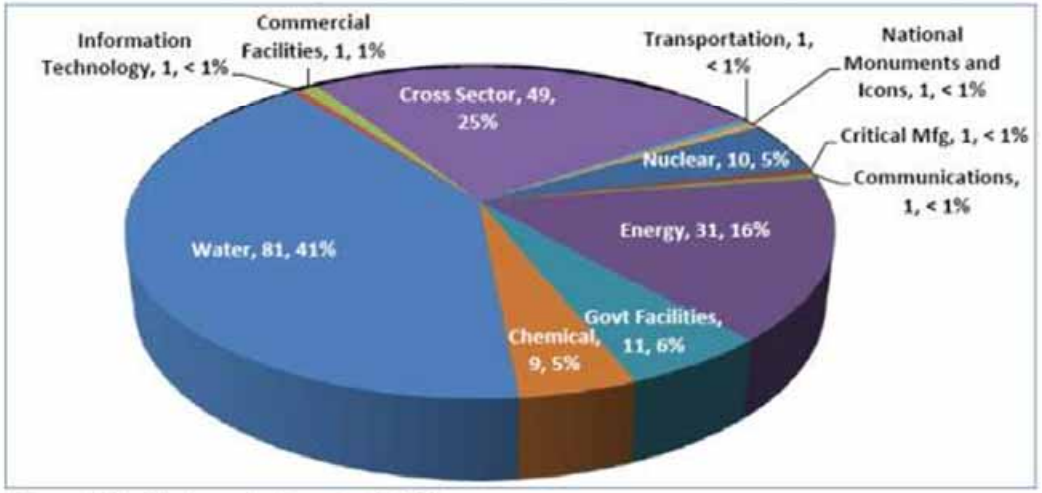
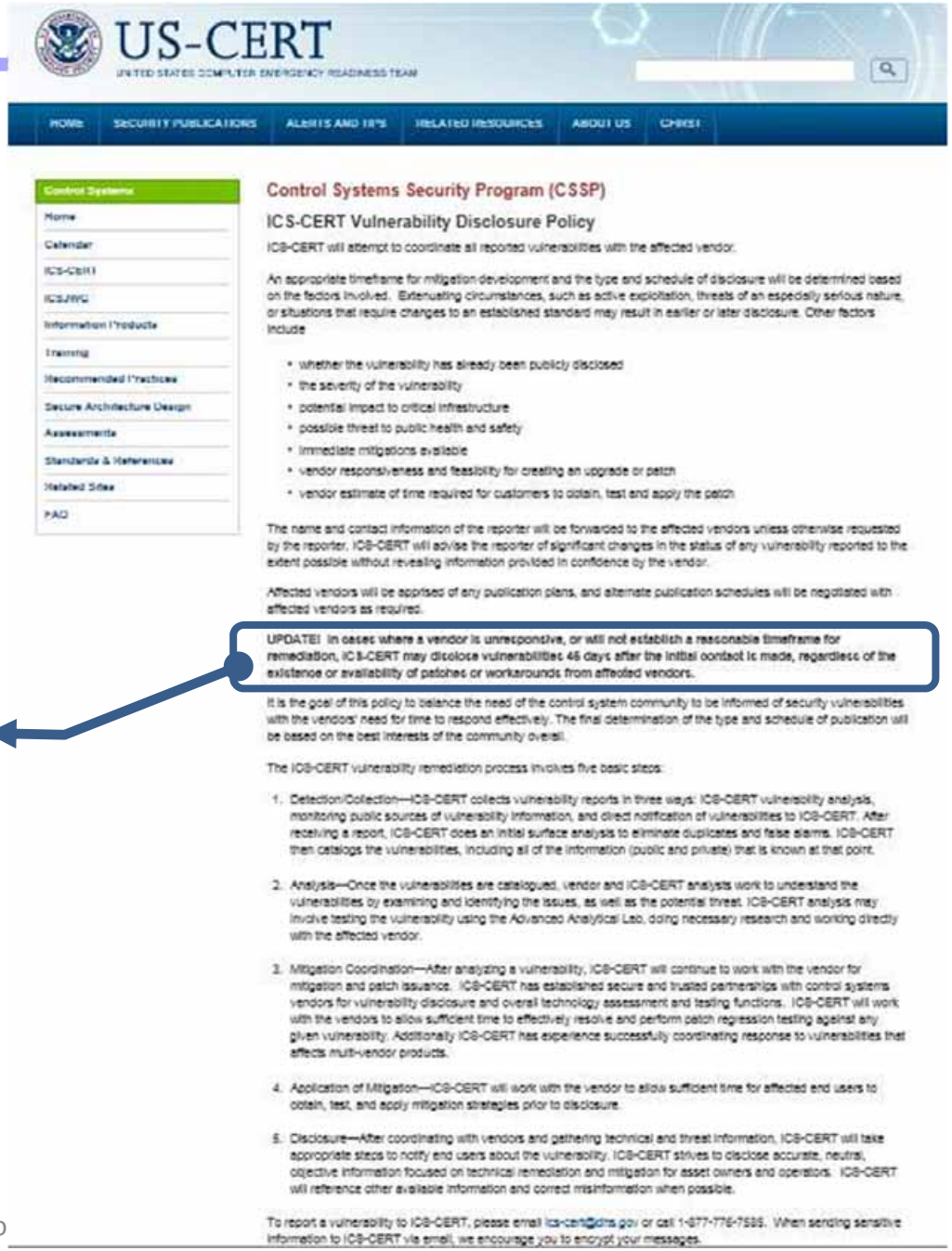


Figure 4. Incident reports by sector (2011).

http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

ICS-CERTが、脆弱性情報の取り扱いポリシーについて一部変更

【今回更新】ベンダの対応が鈍い場合、または、ベンダが提示するパッチの準備に必要なタイムスケジュールが妥当ではないと思われる場合、ICS-CERTはベンダに脆弱性発見の通知をした日から45日後以降に、パッチや回避策の在る無しに関わらず、脆弱性情報を公開することがあります。



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | SECURITY PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | ABOUT US | CONTACT

Control Systems
Home
Calendar
ICS-CERT
ICSJWG
Information Products
Training
Recommended Practices
Secure Architecture Design
Assessments
Standards & References
Related Sites
FAQ

Control Systems Security Program (CSSP)

ICS-CERT Vulnerability Disclosure Policy

ICS-CERT will attempt to coordinate all reported vulnerabilities with the affected vendor.

An appropriate timeframe for mitigation development and the type and schedule of disclosure will be determined based on the factors involved. Extenuating circumstances, such as active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure. Other factors include

- whether the vulnerability has already been publicly disclosed
- the severity of the vulnerability
- potential impact to critical infrastructure
- possible threat to public health and safety
- immediate mitigations available
- vendor responsiveness and feasibility for creating an upgrade or patch
- vendor estimate of time required for customers to obtain, test and apply the patch

The name and contact information of the reporter will be forwarded to the affected vendors unless otherwise requested by the reporter. ICS-CERT will advise the reporter of significant changes in the status of any vulnerability reported to the extent possible without revealing information provided in confidence by the vendor.

Affected vendors will be apprised of any publication plans, and alternate publication schedules will be negotiated with affected vendors as required.

UPDATE! In cases where a vendor is unresponsive, or will not establish a reasonable timeframe for remediation, ICS-CERT may disclose vulnerabilities 45 days after the initial contact is made, regardless of the existence or availability of patches or workarounds from affected vendors.

It is the goal of this policy to balance the need of the control system community to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of the type and schedule of publication will be based on the best interests of the community overall.

The ICS-CERT vulnerability remediation process involves five basic steps:

1. Detection/Collection—ICS-CERT collects vulnerability reports in three ways: ICS-CERT vulnerability analysis, monitoring public sources of vulnerability information, and direct notification of vulnerabilities to ICS-CERT. After receiving a report, ICS-CERT does an initial surface analysis to eliminate duplicates and false alarms. ICS-CERT then catalogs the vulnerabilities, including all of the information (public and private) that is known at that point.

2. Analysis—Once the vulnerabilities are catalogued, vendor and ICS-CERT analysts work to understand the vulnerabilities by examining and identifying the issues, as well as the potential threat. ICS-CERT analysis may involve testing the vulnerability using the Advanced Analytical Lab, doing necessary research and working directly with the affected vendor.

3. Mitigation Coordination—After analyzing a vulnerability, ICS-CERT will continue to work with the vendor for mitigation and patch issuance. ICS-CERT has established secure and trusted partnerships with control systems vendors for vulnerability disclosure and overall technology assessment and testing functions. ICS-CERT will work with the vendors to allow sufficient time to effectively resolve and perform patch regression testing against any given vulnerability. Additionally ICS-CERT has experience successfully coordinating response to vulnerabilities that affects multi-vendor products.

4. Application of Mitigation—ICS-CERT will work with the vendor to allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to disclosure.

5. Disclosure—After coordinating with vendors and gathering technical and threat information, ICS-CERT will take appropriate steps to notify end users about the vulnerability. ICS-CERT strives to disclose accurate, neutral, objective information focused on technical remediation and mitigation for asset owners and operators. ICS-CERT will reference other available information and correct misinformation when possible.

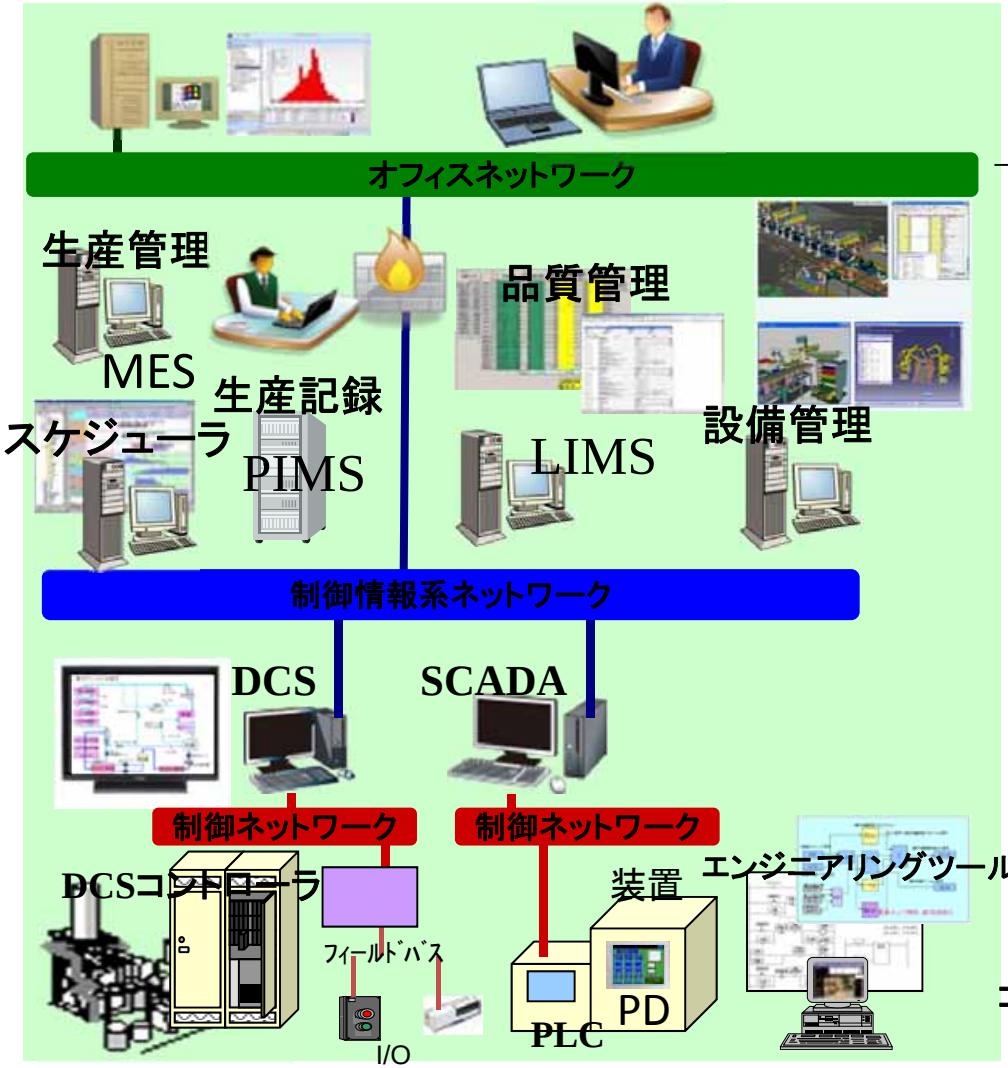
To report a vulnerability to ICS-CERT, please email ics-cert@dhs.gov or call 1-877-776-7585. When sending sensitive information to ICS-CERT via email, we encourage you to encrypt your messages.

Agenda

1. 制御装置や制御システムにとってのサイバー攻撃の脅威
2. **オープン化と制御システムセキュリティ対策**

情報システムと制御システムの区分図

経営業務用情報端末



IEC27001
情報システム系
セキュリティ規格

情報システム

IEC62443-1
概要・コンセプト

IEC62443-2
管理・運用・プロセス

製造組織要件
セキュリティ機能要件
受入テスト要件
メンテ／保守要件

制御情報系ネットワーク（生産システム）

IEC62443-3
技術・システム

制御系ネットワーク

IEC62443-4
コンポーネント・デバイス

制御システム

IEC62443

ISA Reference	Draft	IEC Reference	Title	Owner	Status	Comments
ISA-TR62443-0-3	Link		Gap assessment of ANSI/ISA-99.02.01-2009	WG5	Approved	
ISA-62443-1-1	Link	IEC/TS 62443-1-1	Terminology, concepts and models	WG3	Published, Under Revision	Current edition published as ANSI/ISA-99.00.01-2007
ISA-TR62443-1-2	Link	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	WG3	Proposed	Content is under development on the Wiki
ISA-62443-1-3	Link	IEC 62443-1-3	System security compliance metrics	WG4	Under Development	
isa-62443-1-4	N/A	IEC/TR 62443-1-4	IACS security life cycle and use case	TBD	Proposed	
ISA-62443-2-1	Link	IEC 62443-2-1	IACS security management system - Requirements	WG2	Published, Under Revision	Current edition published as ANSI/ISA-99.02.01-2009
ISA-62443-2-2	Link	IEC 62443-2-2	IACS security management system - Implementation guidance	WG2	Proposed	
ISA-TR62443-2-3	Link	IEC/TR 62443-2-3	Patch management in the IACS environment	WG6	Proposed	
ISA-62443-2-4	N/A	IEC 62443-2-4	Certification of IACS supplier security policies and practices	IEC TC65/WG10	Proposed	Proposed as a national modification to the IEC standard.
ISA-TR62443-3-1	Link	IEC/TR 62443-3-1	Security technologies for IACS	WG1	Published	Current edition published as ANSI/ISA-TR99.00.01-2007
ISA-62443-3-2	Link	IEC 62443-3-2	Security assurance levels for zones and conduits	WG4	Under Development	
ISA-62443-3-3	Link	IEC 62443-3-3	System security requirements and security assurance levels	WG4	Approved	Previously numbered ISA-99.01.03
ISA-62443-4-1	Link	IEC 62443-4-1	Product Development Requirements	WG4	Under Development	
ISA-62443-4-2	Link	IEC 62443-4-2	Technical security requirements for IACS components	WG4	Under Development	

N/A - These work products are not yet available.

http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

SAL:Security assurance levels

- **SAL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation systems**

SAL1ーゾーンとパイプ（インテリジェントなルータもしくはファイヤーウォール）分割で何気ないか偶然の一致による妨害から制御システムを護ってください。

- **SAL 2 – Prevent the intended circumvention of zone and conduit segmentation systems by entities using simple means with low resources, generic skills and low motivation**

SAL2ー低資源、一般的な技術と低い動機づけで単純な手段を使用している実機能を有する実物によって、ゾーンとパイプ（インテリジェントなルータもしくはファイヤーウォール）分割で意図された妨害から制御システムを護ってください。

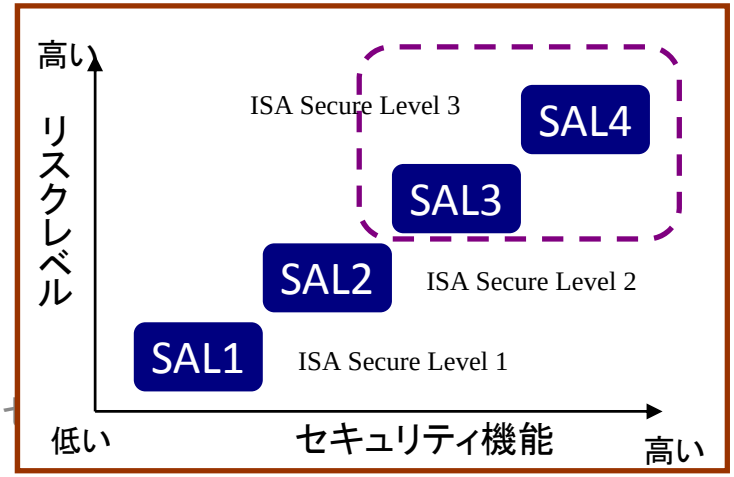
- **SAL 3 – Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means with moderate resources, system specific skills and moderate motivation.**

SAL3ー穏やかな資源、システムに特有の技術と穏やかな動機づけで高度な手段を使用している実機能を有する実物によって、ゾーンとパイプ（インテリジェントなルータもしくはファイヤーウォール）分割で意図された妨害から制御システムを護ってください。

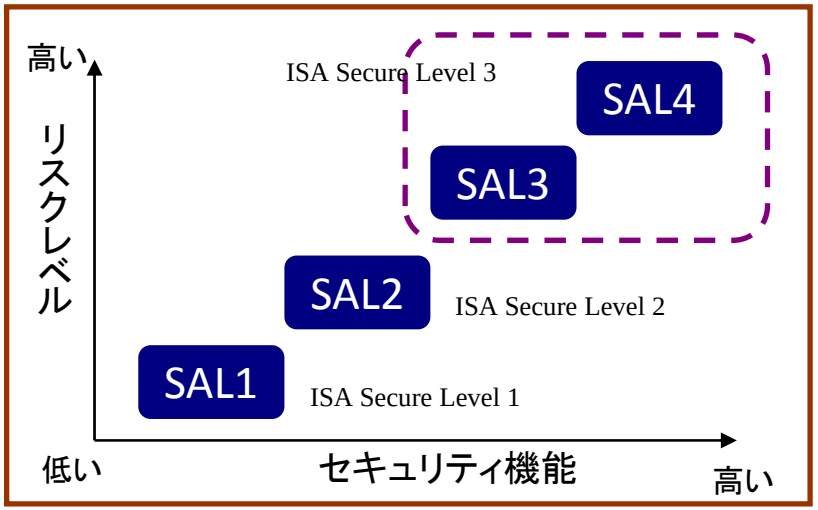
- **SAL 4 – Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means with extended resources, system specific skills and high motivation.**

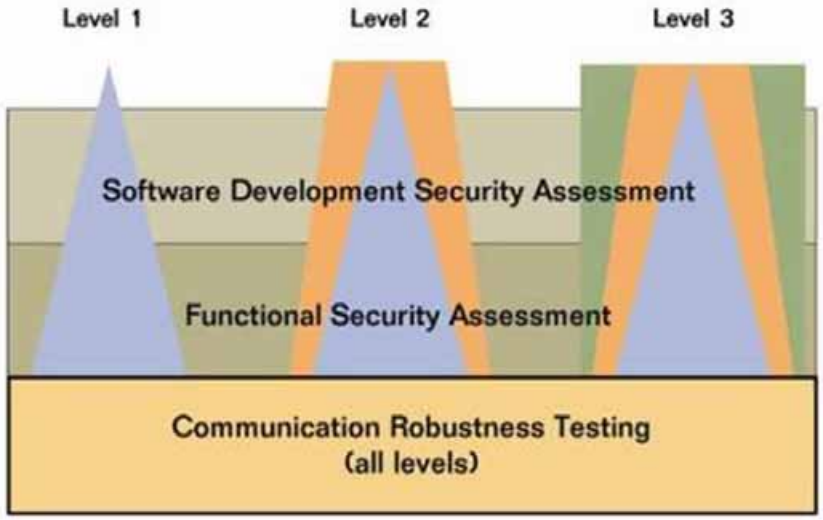
SAL4ー拡張資源、システムに特有の技術と高い動機づけで高度な手段を使用している実機能を有する実物によって、ゾーンとパイプ（インテリジェントなルータもしくはファイヤーウォール）分割で意図された妨害から制御システムを護ってください。

SAL／SLは、制御システムの常識になっています。



SAL: Security assurance levelsと ISA Secure EDSA：
Embedded Device Security Assurance





ISASecure EDSA Conformance Scheme Definition Documents

http://isasecure.org/Certification-Program/ISASecure-Program-Description.aspx

SAL／SLは、制御システムでも常識になっています。

ISASecure Level	内容
1	最も基本的な対策としてユーザ認証手段をサポート
2	ユーザ認証手段やその他の基本的な手段（OS設定等）を用いて装置やデータの安全性、機密性、可用性の保護をサポート
3	ユーザ認証手段やその他の高度な手段（暗号等）を用いて装置やデータの安全性、機密性、可用性の保護をサポート

制御装置や制御システムに関係する認証の考え

- ISO/IEC 15408 CC(Common Criteria)は、製品に関するセキュリティ仕様
- IEC62443は、製品を開発し提供するベンダの組織、製造、保守の3つのプロセスについて評価する規格
- ISA-SP99に基づいた制御システムのセキュリティ標準に準拠したかを評価するISASecure Embedded Device Security Assurance(EDSA)

対策に関する各国の機関と法規制状況

アジア　中国

- 製造設備などに関する国家標準規格としてはGB(Guo jia Biao zhun:国家標準）がある。GBは国家の強制規格であり、GB/Tは国家の勧奨規格である。またGB/Zは国家の指導的技術的な標準である。
- 制御システムの情報セキュリティに関しては、現在中国の強制的な規格であるGBは制定されていない。

Stuxnet⇒「超級工廠病毒」と書くその意味は「めったにない超級クラスの工業関連のワーム」

新華社通信では中国では業務に関係する600万台以上の個人コンピュータ、約1,000社の企業内コンピュータにStuxnetの感染が見られたと報告

制御システム⇒「工業控制系統」

- 「工業網路安全形勢分析」(2011年1月11日）にレポート
  - 2003年1月のスラマーワームの多量汚染事件、2005年8月のダイムラー・クライスラー13工場のワーム汚染による操業停止事件、2006年10月のペンシルバニア州ハリスバーグの浄水場コンピュータシステム侵入事案などを引用しつつ、中国が直面する問題を指摘している。

- 中国新五か年計画：グローバルに戦える企業を育てる
- IEC62443とISA SP99⇒中国版IEC62443

制御ベンダの企業方針とグローバルベンダの動向

反応しない経営者の言
●サイバー攻撃される製品の立ち位置にない。
●これで儲けようとしている者の企み
●実際に問題になってからで良い。
●サイバー攻撃なんて雲の上の話。それより、利益を上げろ。

Innovate and Demonstrate thought Leadership
業界のリーダー的存在の責務を果たす

Include in All Lifecycle Processes
製品のライフサイクルに対策を施す

Include in Development Processes
製品開発プロセスに対策を施す

Test and Fix at End of Development
認証の為に、製品開発の最後にテストを実施する

Fix,After Incident
インシデントが起きたらやる

Ignore Issues
言われてもやらない

General/Industrial/Commercial
必要最低限をやるベンダ

Critical Infrastructure
積極的に取り組むベンダ

SIEMENS
ABB
Schneider Electric
GE
EMERSON
Rockwell Automation
Honeywell

対策に関する各国の機関と法規制状況

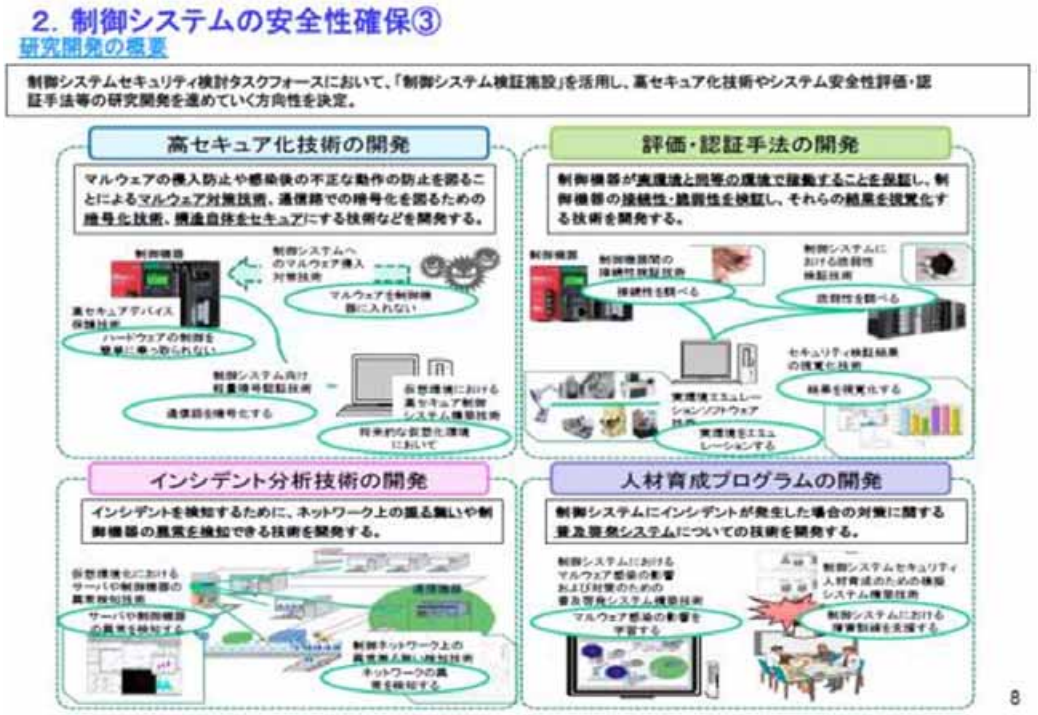
日本

５月技術組合制御システムセキュリティセンターを設立

サイバーセキュリティと経済研究会のフォローアップ会議が8月31日に開催された。

情報セキュリティに関する経済産業省の施策方針を明らかにした。

http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/007_haifu.html



対策に関する各国の機関と法規制状況

日本

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

技術研究組合
制御システムセキュリティセンター

理事長：
新　誠一（電気通信大学　教授）

組合員：
全１１社（2012年5月16日現在）
アズビル株式会社（旧：株式会社山武）
NRIセキュアテクノロジーズ株式会社
(独)産業技術総合研究所
(独)情報処理推進機構
株式会社東芝
株式会社日立製作所
富士電機株式会社
三菱重工業株式会社
株式会社三菱総合研究所
森ビル株式会社
横河電機株式会社

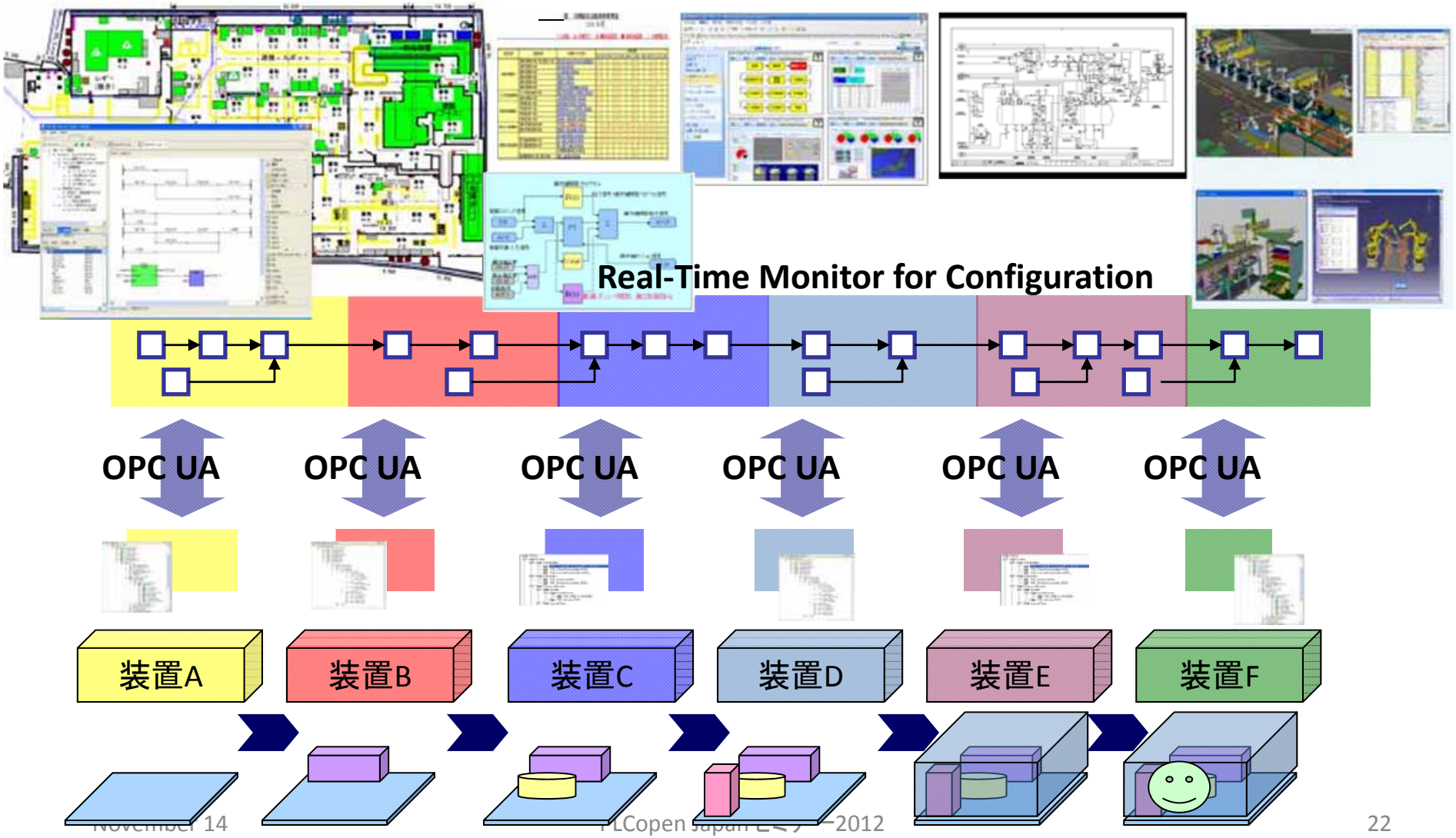
その他連携予定団体：
オムロン株式会社、三菱電機株式会社、
一般社団法人JPCERTコーディネーションセンター、一般社団法人日本電機工業会、
公益社団法人 計測自動制御学会、
一般社団法人電子技術情報産業協会、
社団法人日本電気計測器工業会、
社団法人製造科学技術センター、
電気事業連合会、一般社団法人日本ガス協会、
一般社団法人日本化学工業協会、 他
http://www.css-center.or.jp/index.html

制御システムセキュリティ関連団体合同委員会

- JEMIMA
- JEMA
- NECA
- JEITA
- JARA
- SICE
- MSTC
- JPCERT/CC
- VEC

統一されたコンフィギュレーション環境が可能となれば

IEC61131-3への期待



世界に通用する生産／制御システム
その1：情報モデル利用

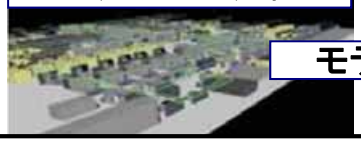
ERP
SCM
データベース
生産システム効率指標ISO22400
KPI
生産管理
KPI
品質管理
KPI
エネルギー管理
KPI
設備管理
情報処理演算
④利便性を確保した
サイバーセキュリティ対応
入力情報
OPC UA
①上位ITシステムと各Industry Ethernet
とのイントラネット接続
OPC UA　IEC-62541
デバイスのアドレス構造
情報を共有するモデル
操作／制御
制御演算
検出端
操作端
素材
メカニック
製品

ERP、PLM、SCM、CRMとの連携

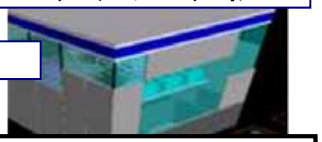
ISO22400
MESのKPIの標準化に対応

効率指標　品質の指標　能力インデックス
環境指標　目録管理指標　メンテナンス指標

生産システムの
3Dシミュレーション



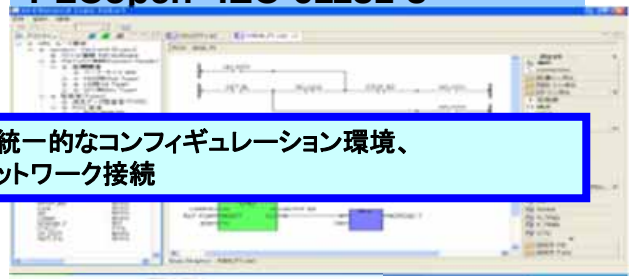
装置の
3Dシミュレーション



モデル

・ユーザーニーズの実現に必要なアプリケーションを制御コントローラが違っていても、装置単位で、生産ライン単位で、工場単位で扱えるようにするには、IEC-61131-3とIEC-62541を組み合わせることで作業のスピードアップとより、生産能力のアップの実現が容易になる。

PLCopen　IEC-61131-3



③統一的なコンフィギュレーション環境、
ネットワーク接続

②情報連携による異機種
Industry Ethernetをまたがる制御

世界に通用する生産／制御システム
その2：クラウド利用

業務用情報端末

C#

リスクの見える化

Cloud

SCM

ERP

CRM

リスクの見える化

サプライチェーンの見える化

安定操業を支える

業務ネットワーク

生産システムの環境評価：ISO20140

生産システム効率指標：ISO22400

アプリケーション

データベース

KPI

生産実績

生産管理

KPI

品質管理

工場の見える化

情報処理演算

KPI

エネルギー管理

安全の見える化

KPI

設備管理

セイフティ
制御システムセキュリティ対策

指令（動脈）

情報（静脈）

状況分析・診断ツール

OPC UA

OPC UA

情報モデル

M2M

Cloud
Server

OPC UA　IEC-62541

サポートサービス

C,C++、C#

制御演算

制御用
リアル
データ

検出端

操作端

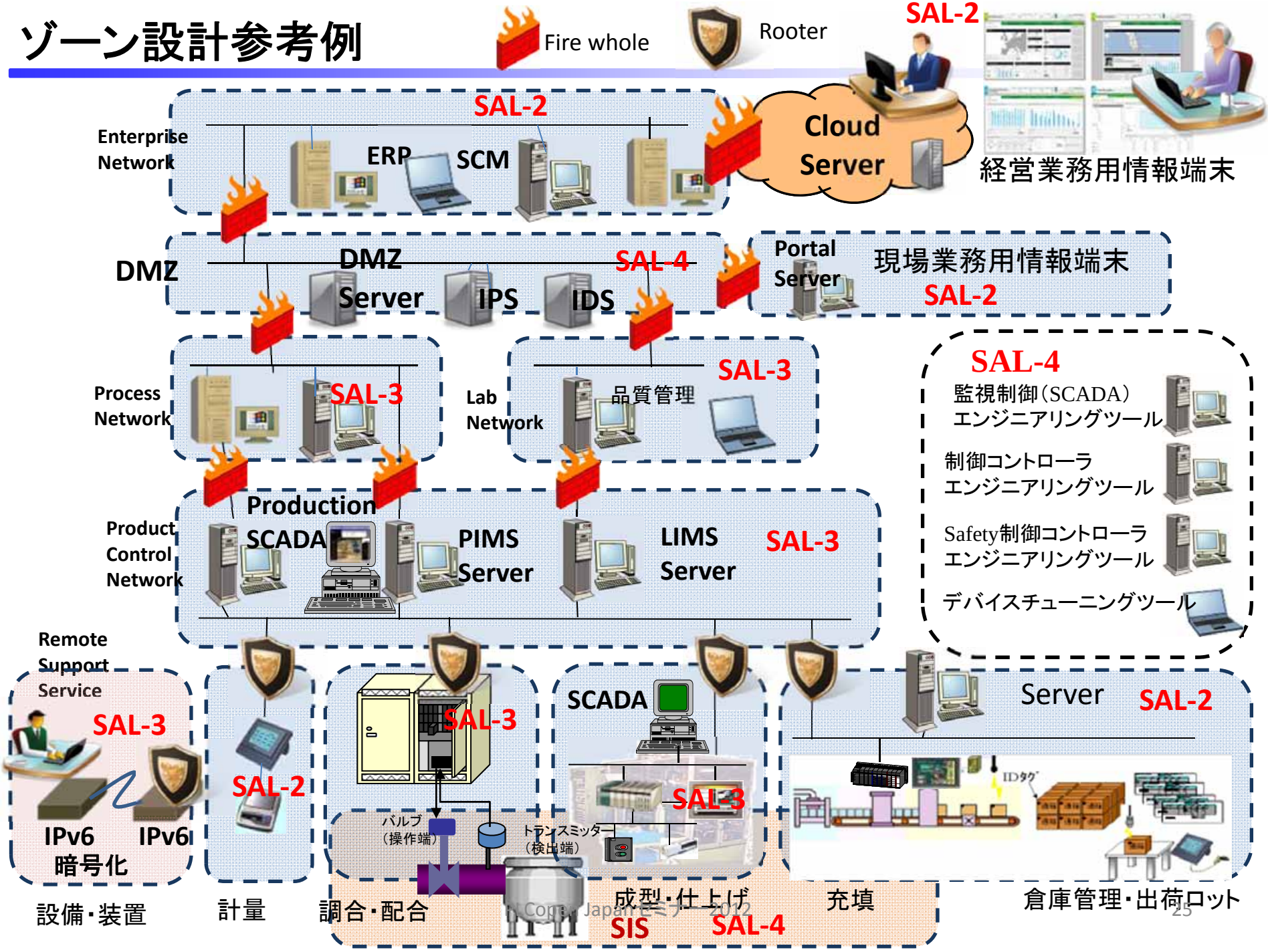
情報モデル

素材

メカニック

製品

ゾーン設計参考例

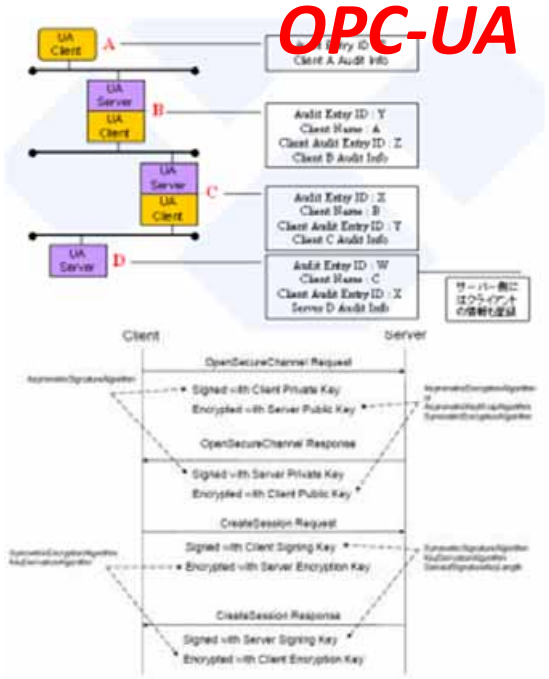

Fire whole
Rooter
SAL-2
Cloud Server
経営業務用情報端末
Enterprise Network
SAL-2
ERP
SCM
DMZ
DMZ Server
SAL-4
IPS
IDS
Portal Server
現場業務用情報端末
SAL-2
Process Network
SAL-3
Lab Network
品質管理
SAL-3
SAL-4
監視制御（SCADA）エンジニアリングツール
制御コントローラ エンジニアリングツール
Safety制御コントローラ エンジニアリングツール
デバイスチューニングツール
Product Control Network
Production SCADA
PIMS Server
LIMS Server
SAL-3
Remote Support Service
SAL-3
IPv6
IPv6
暗号化
SAL-2
SAL-3
バルブ（操作端）
トランスミッター（検出端）
SCADA
SAL-3
Server
SAL-2
IDタグ
設備・装置
計量
調合・配合
成型・仕上げ
充填
倉庫管理・出荷ロット
SIS
SAL-4

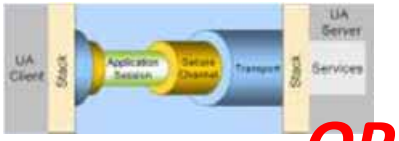
制御ベンダ／装置ベンダの対応例

- セキュリティプロダクト／サービスのオーナーをおく
  - 制御製品のセキュリティにおける企画から保守に至るまで全責任を取る
  - 社内セキュア管理の知識と実践の教育システム
- 社会インフラ、ライフライン、基幹産業の現場を支える制御製品であるか？　:セキュア製品に関するマーケティングの重要性
  - IEC62443対象制御製品にあたる
    - ユーザー指定の制御システムセキュリティ試験で合格し、安心を提供
      - 試験を受けるのにコストがかかる。 ⇒　セキュア対策製品の価格が上がる
      - ユーザーは、サイバー攻撃で被災し、工場操業停止する損害と比較検討して妥当な金額であるかを見る。
    - サイバー攻撃に強い制御製品
    - インシデント対応の情報公開対応
      - 顧客に対する供給者責任　⇒　信頼、安心
  - IEC624432対象制御製品にあたらない
    - 今までと変わらない
      - PL法、業界法規制、RoHS、
- ユーザー向けに
  - 「セキュリティ対策の制御製品取り扱いガイドライン」
  - 脆弱性対応

制御製品開発に求められるセキュリティ対応

- サイバー攻撃に強い制御製品に求めること
  - 制御製品企画の段階から、セキュリティ対策検討を加える
    - IEC62443対象の製品とするか否か
    - OSの選択、ネットワークの仕様、通信プロトコルの選択、ログ機能の検討
  - 制御製品における高度セキュア化技術研究
    - モジュール構造による製品設計
  - セキュア知識を持ってプログラム開発をする
    - OSによってコードの脆弱性レベルが変わる
  - 製品によっては、製品内に
    - タスク通信のログ機能
    - 監査機能
  - 製品によっては、ネットワーク通信に
    - ログ機能　⇒　監査機能
    - 通信プロトコルは、
      - オーディット機能
      - セキュリティ設定機能
        - » 署名
        - » 暗号化
        - » 通信スタック





OPC-UA

- 重要インフラの制御システムに使用される制御製品に求められることとは？
  - オンラインでのパッチあて作業ができ、オンラインで切り替えられる機能
    ⇒ オンラインでのソフトウェアバージョン管理システム

チェックできる環境整備

- **環境整備計画**
  - 対象製品の選定
    - 製品の重要性と事業性
  - 規模計画
    - 投資金額設定
    - 費用回収
    - 運営方法
- **環境整備**
  - 自社製品以外の環境構築
  - 3Dシミュレーションの活用
  - エミュレータ
  - **必要とされるツール類**
    - **Fuzz（評価）ツール**
    - **Robustness（評価）ツール**
    - **Scanning（追跡・監視）ツール**
    - **Exploit（影響確認）ツール**

制御製品開発環境の健全性

- 制御製品開発環境の健全性確保
  - 制御製品開発用ネットワークの隔離
    - ファイヤーウォール設置
    - ネットワーク・ケーブル
      - インターネット接続可能なケーブル
      - インターネット接続不可能なケーブル
  - セキュリティ確保、情報漏洩防止できる開発環境
- サーバーとPCネットワークのセキュリティチェック管理責任者をおく
  - ファイヤーウォールのDMZ (De-Militarized Zone):
  - IDS:侵入検知システム (Intrusion Detection System)
  - IPS:侵入防止システム(IPS: Intrusion Prevention System)
  - SAL-3/4対象

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

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

業界のキーパーソンにVECならではの切り口で役立つ情報とソリューションを提案する。

開催日：2012年11月28日

主婦会館　B2　クラルテ　スクール形式で110名

開催日時：2012年11月28日
開催場所：主婦会館　B2　クラルテ

プログラム
10:00～10:10　　開催挨拶
基調講演
制御システムターゲットのサイバー攻撃最新情報
海外企業の取り組み動向
ユーザーが現場ですぐできる対策
制御ベンダの役割り
　脆弱性対応について
装置ベンダの役割り
エンジニアリング会社の役割り
制御システムセキュリティ・ゾーン設計上の注意点とそこで使われる技術について
　作業エリアのゾーン区分
　ネットワーク設計でのゾーン区分
　無線通信設計でのゾーン区分
　人の権限を設計するゾーン区分
　データや情報モデル構造設計の対策
HMI作画設計上のセキュリティ対策
制御装置のリモートサービスでのセキュリティ対策ソリューション
インシデントフローチャート作成時の注意事項
VEC会員のソリューションご紹介