IPA Information-technology Promotion Agency, Japan

平成24年電気学会全国大会

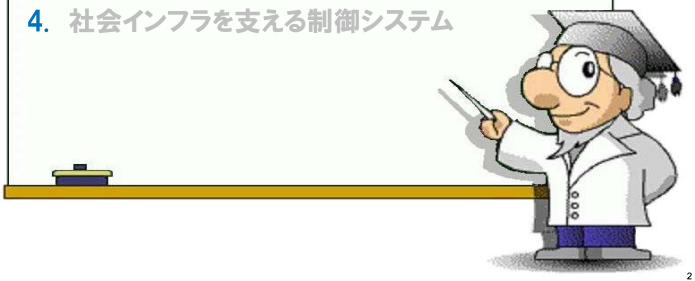
スマートシティと技術者倫理

制御機器へのサイバー攻撃の現状

2012年3月22日

独立行政法人 情報処理推進機構 IPA
技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー長
小林偉昭

目次



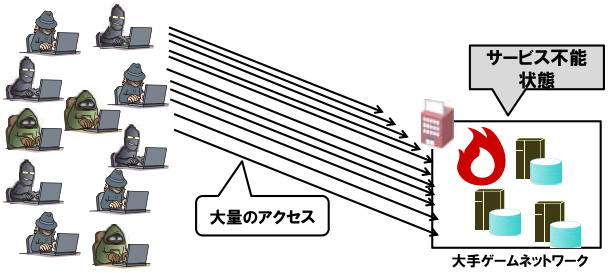
サイバー攻撃とは

■ 2011年にサイバー攻撃の報道が目立った

時期	報道
2011/2	中国から欧米エネルギー5社攻撃（毎日新聞等）
2011/3	韓国で大規模ハッカー攻撃 大統領府や銀行など40機関（朝日新聞等）
2011/3	仏財務省にサイバー攻撃、G20情報盗まれる（読売新聞等）
2011/4-5	ソニーにサイバー攻撃、個人情報流出1億件超（朝日新聞等）
2011/6	米グーグル：中国からサイバー攻撃 米韓政府関係者ら被害（毎日新聞等）
2011/9	三菱重にサイバー攻撃、80台感染…防衛関連も（読売新聞等）
2011/9	IHIにもサイバー攻撃 日本の防衛・原発産業に狙いか（産経新聞等）
2011/10	衆院にサイバー攻撃 議員のパスワード盗まれる（朝日新聞等）
2011/11	サイバー攻撃：参院会館のPC、ウイルス感染は数十台に（毎日新聞等）

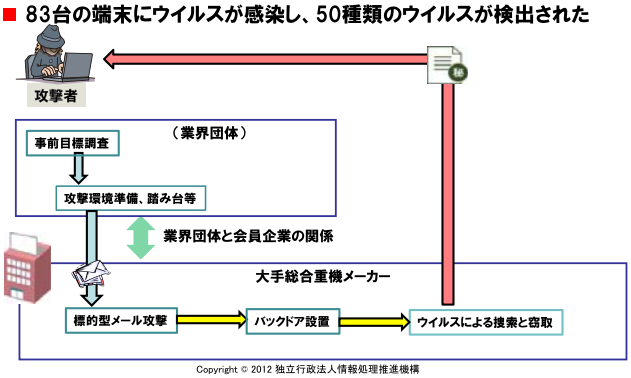
サイバー攻撃の例：
～ゲームネットワークへのDDoS攻撃～

■ 大手ゲームネットワークへの攻撃（2011年4月）
- 大手ゲームネットワークが、攻撃者集団（Anonymous）からDDoS攻撃<ネットワークやサービス等を使用できない状態にする攻撃の一つ>を受けたと報道されている
  - その後、同社および同社関連企業に対するサイバー攻撃によって最大規模の情報漏えいの事件が発生した



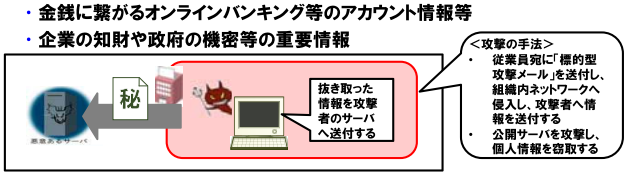
サイバー攻撃の例：
～日本、イスラエル、インド、米国の防衛産業企業に対する標的型攻撃～

■ 国内の大手総合重機メーカーへの攻撃（2011年9月）
- 国内大手総合重機メーカの軍需情報、原発情報の窃取を目的とした攻撃
- 大手総合機器メーカが加盟している団体を攻撃し、事前目標を定めた
- 83台の端末にウイルスが感染し、50種類のウイルスが検出された

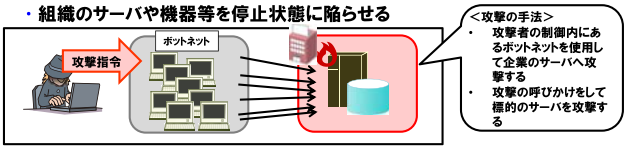


サイバー攻撃の目的

■ 現状のサイバー攻撃を行う攻撃者の目的
- 情報窃取
  - 金銭に繋がるオンラインバンキング等のアカウント情報等
  - 企業の知財や政府の機密等の重要情報



- サービス運用妨害（DoS）
  - 組織のサーバや機器等を停止状態に陥らせる



サイバー攻撃の変遷
～ 攻撃手法の巧妙化だけでなく攻撃者像にも変化 ～

■ 攻撃者の狙い

いたずら目的 顕示欲の誇示	金銭目的（犯罪） サービス妨害（嫌がらせ）	スパイ・諜報活動 機密情報の窃取

■ 攻撃者像

攻撃者1人 セキュリティ技術者	グループ 犯罪者	国家？ 犯罪プロ集団

■ 攻撃手法

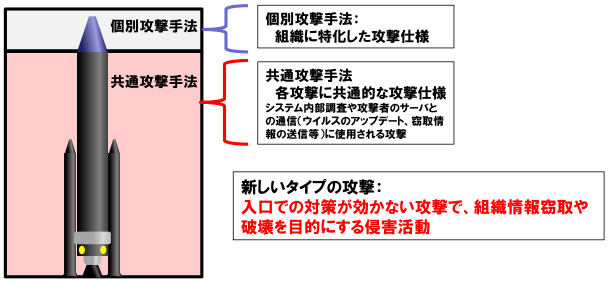
不正侵入	Botnet Spamメール	標的型・シーケンシャル マルウェア

※ソーシャルエンジニアリングによる、ウェブ、メール、USB等経由の攻撃へ

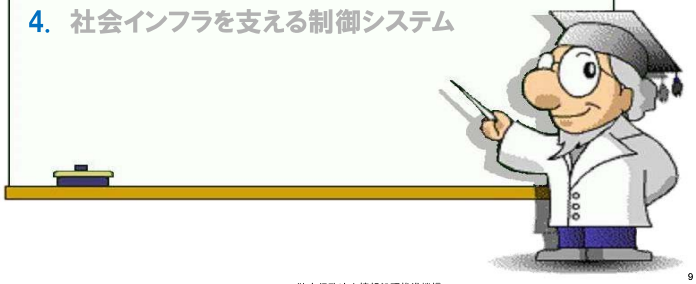
■ ビジネスインパクト
- 個人情報流出 ⇒ 企業の社会的責任
- 知的財産情報の窃取 ⇒ 企業の競争力低下、国家の危機管理問題へ
- 制御機器やシステム停止 ⇒ 企業の競争力低下、サプライチェーンの崩壊、社会インフラの混乱、国家の危機管理問題へ

サイバー攻撃のまとめ

■ サイバー攻撃のまとめ
- サイバー攻撃はウェブやメール、USBメモリ等を使い、組織の情報を窃取したり、サービスの運用妨害を行おうとしている。
- サイバー攻撃はソーシャルエンジニアリング等を使うようになったり、組織化されたりしており、年々巧妙になっている



目次

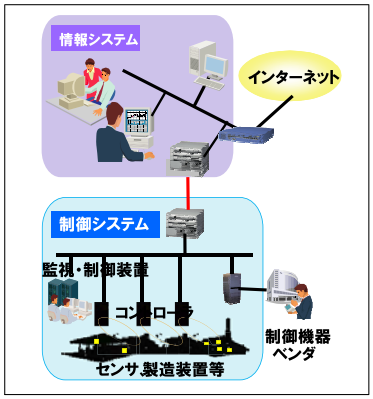


制御システムとは

■ 位置づけ
- センサやアクチュエータ等のフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群（システム）。
- 自動車等製造業の工場や電気・ガス等の重要インフラにおける管理・維持等で利用されている。

制御システムの状況

■ 制御システムの状況＜従来と最近＞

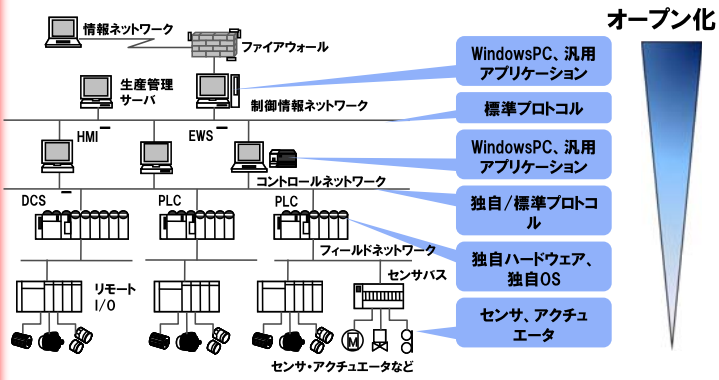


最近の背景：
情報システムとの接続や
他組織との連携（SCM）

1. ＜従来＞
情報システムと制御システムは繋がっていない
＜最近＞
ネットワークやUSBメモリ等で繋がるようになった
2. ＜従来＞
独自仕様のOSやアプリ
＜最近＞
汎用OSネットワークや標準プロトコルを使用

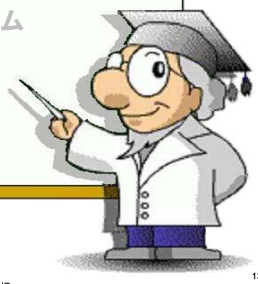
制御システムの状況

「オープン化」：汎用製品＋標準プロトコル



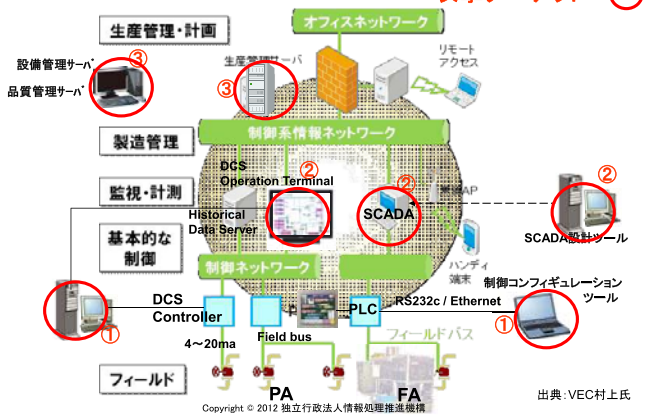
目次

1. サイバー攻撃とは
2. 制御システムの現状
3. **制御システムへのサイバー攻撃例と課題**
4. 社会インフラを支える制御システム



制御システムにおける攻撃対象例

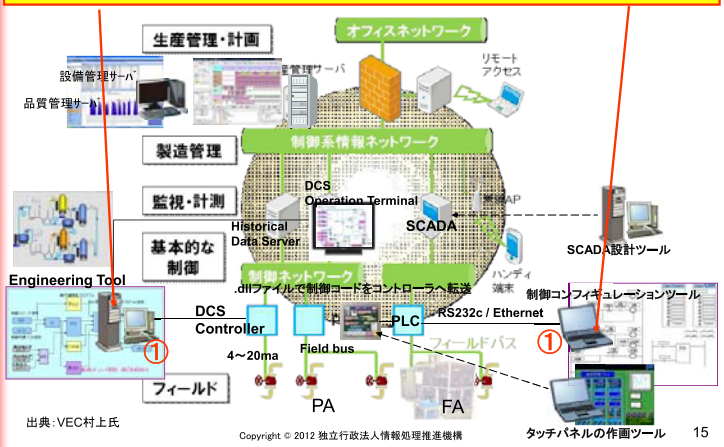
攻撃目的:装置や設備の破壊、悪品質製品生産や生産の暴走、装置ベンダの信頼失墜等　攻撃ターゲット⇒◯



出典:VEC村上氏

攻撃パターン例:データすり替え

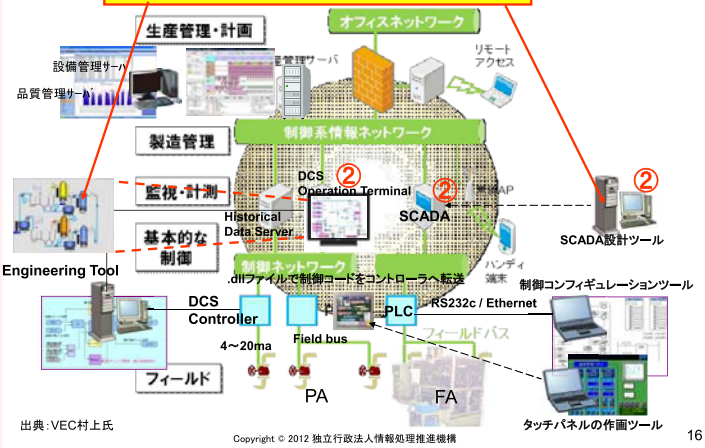
ファンクションブロックのパラメータやシーケンスロジック条件を書き換えたものとすり替える。



出典:VEC村上氏

攻撃パターン例:異常コードをコントローラへ

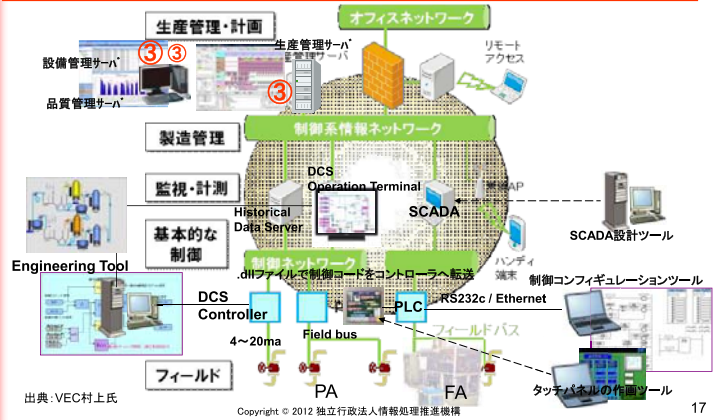
画面は正常で表示し、異常コードをコントローラへ送る



出典:VEC村上氏

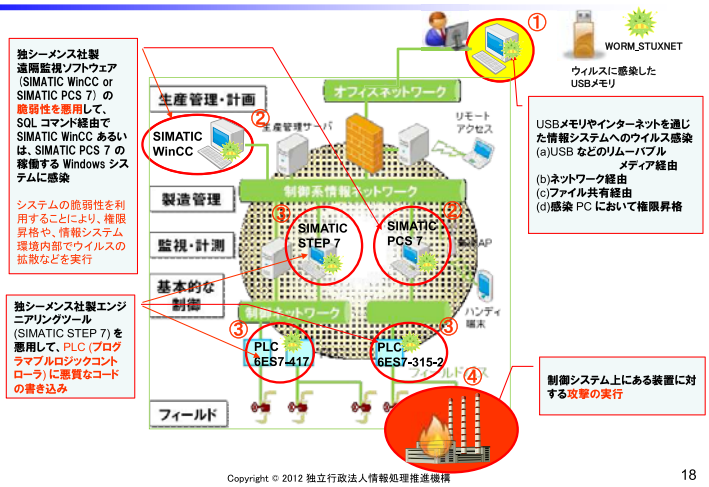
攻撃パターン例:生産管理・計画を異常に

生産スケジュールの製品成分レシピなどを悪品質にすり換える。生産数量指示を変える。コントローラへの直接指示コードを送って装置や設備にストレスを加える。



出典:VEC村上氏

Stuxnet攻撃例



制御システムへのセキュリティ課題

制御システムのセキュリティ課題

【課題1：オープン化に伴う脆弱性リスクの混入】

汎用製品、標準プロトコルネットワーク採用により、脆弱性リスク、ワームなどのウイルスの侵入や、機密情報漏えいのおそれがある。

【課題2：製品の長期利用に伴うセキュリティ対策技術の陳腐化】

制御システムは通常10～20年使用。セキュリティ対策も最新ではない可能性がある。

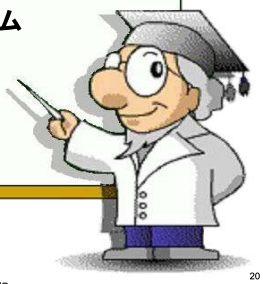
【課題3：可用性重視に伴うセキュリティ機能の絞込み】

可用性重視の観点から、一般的に、システム上の負荷となるウイルス監視やチェックプログラムの自動更新がない、または間隔が長い。

	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報

資料：IPA「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」より抜粋

目次



社会インフラを守る：サイバー空間で制御システムはますます大切に

原子力設備、電力、銀行、鉄道、航空、水道、医療等の重要インフラ分野の90%は民間

重要インフラの制御システムの事故の例

➢原子力発電所の制御システムへのワーム侵入

- 発生した原因
  - ◇VPN接続による内部感染
  - ◇対象パッチの未更新
- 事件の影響
  - ◇6時間の運用停止

2003 年1 月、オハイオ州Davis Besse 原子力発電所でマイクロソフトのSQL サーバを狙ったSlammer（読み方：スラマー）ワームがVPN（Virtual Private Network）接続を介して侵入・感染し、SCADA システムを約5 時間にわたって停止させた。同施設のプロセス・コンピュータも停止し、再運用までに約6 時間を費やしたほか、他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。感染したSlammer ワームに対するパッチは、その時点で公開されていたが、発電所のシステムには該当パッチがあてられていなかった。

Davis Besse 原子力発電所

重要インフラの制御システムの事故の例

アンチウイルスソフトがシステムの安全停止を妨害

- 発生した原因
  - ◇不正操作（過失）
- 業種
  - ◇石油

TÜVが認証済のボイラー安全保護システムはPCワークステーション上で動作するMicroSoft Excelを使用していた。また、このワークステーションはノートン社製のアンチウイルスソフトを導入していた。このアンチウイルスソフトはPCと保護システムとの間の固有通信を妨害し、安全停止が実行されなかった。

© 2009 Security Incidents Organization

重要インフラの制御システムの事故の例

セキュリティ監査時にPLCが故障

- 発生した国
  - ◇米国
- 業種
  - ◇食品会社
- 事故原因
  - ◇内部者（過失）
- 想定被害
  - ◇$1M以上の損失

セキュリティコンサルタント は食品会社の事業とネットワークの脆弱性を監査した。一時的に妨害を行なうパケットを Ethernetでコントロールネットワークに流したため、複数のPLCに深刻な欠損が生じた。このパケットは4か、それ以上のICMPエコー要求を含むものであった。

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

「サイバーセキュリティと経済研究会」での検討と制御システムセキュリティ検討タスクフォースの設置

サイバーセキュリティと経済研究会
（経済産業省）

＜概要＞

サイバー攻撃により、知的財産やライフラインを狙った事案や企業等の機密漏えいが多発している状況から、ITの安全確保によって守るべき対象が経済活動や国民生活に直接関わる分野へ質的に変化していることを鑑み、経済の成長・安全保障の観点から、必要な情報セキュリティ政策を検討。

◇主な検討項目

- ・標的型サイバー攻撃への対応
- ・制御システムの安全性確保
- ・情報セキュリティ人材の育成

制御システムセキュリティ検討タスクフォース
（経済産業省）

＜概要＞

左記研究会の検討に基づき、主に以下の2点における制御システムセキュリティについての施策の実施検討。

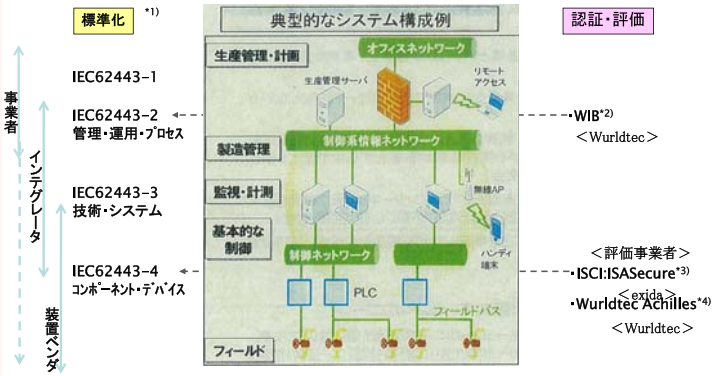
◇日本国内のICSセキュリティ確保
◇ICSの海外輸出のための評価認証

＜タスクフォースに配置するWG＞

- ・標準化WG (IPA)
- ・評価・認証制度WG (IPA)
- ・インシデントハンドリングWG
- ・テストベッドWG
- ・人材育成WG
- ・普及啓発WG

ICS：Industrial Control Systems

制御システム分野における標準と認証・評価の位置づけ



*1) IEC62443のCyber securityの標準化作業は、IEC/TC65/WG10が担当。日本では、JEMIMAが対応（幹事：Yokogawa）。
*2) International Instrument User's Associations, 認証はWurldtech Achilles認証。IEC62443-2-4に取り込み。
*3) EDSA(Embedded Device Security Assurance) certification。ISA99標準仕様。IEC62443-4-1に相当。
*4) ネットワーク接続装置（コントローラ等）の信頼性認証（ペネトレーション、ファジングテスト）。調達要件に指定されている。

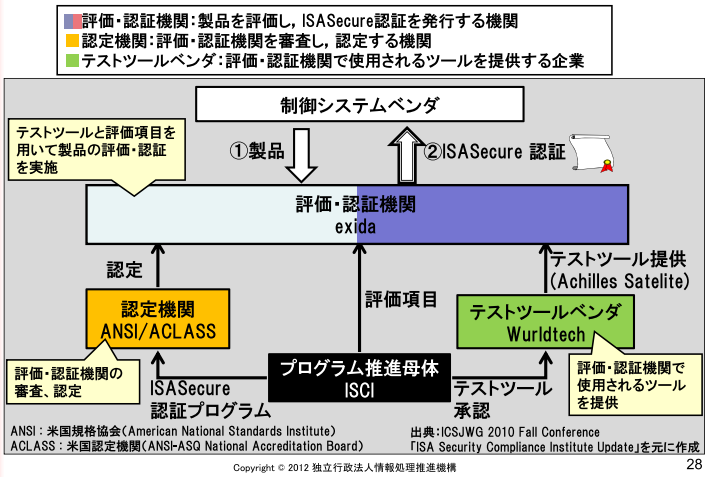
IEC62443規格化の状況

（2011年11月現在）

区分	主対象者	IEC	基本名及び概要	現状のステータス：ドキュメントの状況、ドラフトの現状	現状のステータス：投票フェーズ	リリース予定：発行済み、DTR、Edition2など	詳細	評価認証機関：規格を利用した認証者
共通	全体	62443-1-1	Terminology, concepts and models <セキュリティ概念、Scadaモデル一般論、本標準の用語統一と導入部分で認証に関わらない。>	発行済み、アップデート中/RR作成中	(済)	2009.07 Ed.2：1CDは2101104	・セキュリティ概念（目的、基本要件、体系、13ドメイン分析、ポリシー、組織、ゾーニング、セキュリティレベル、ライフサイクル） ・参照モデル（3階層）、資産モデル（参照アーキテクチャ、ゾーン&経路モデル	認証対象外
		62443-1-2	master glossary of terms and abbreviations	テクニカルレポートとしてレビュー中	○	1DC：2012Q1 DTR：2012Q3		
		62443-1-3	System security compliance metrics	ドラフト執筆中	○	1DC：2011Q4 DTR：2013.02		
セキュリティプログラム	事業・運用者	62443-2-1	Establishing an IACS security program <事業者自体のセキュリティマネージメントシステム構築>	発行済み、アップデート中、RR作成中	(済)	2010.10 Ed.2：CDVは2012Q4	CSMS（Cyber Security Management System）、ISMS（ISO27001）ICS版 ・リスク解析、リスク対応（ネットワーク、組織、対策、実装）、モニタリングと改善 ・127要件（ISO17799：128、ISO27001：133） ・本文（38P）、補足資料（121p）、ISO27001との対応表 ISMSと類似の認証は可能だが、ISMS認証の普及は日本が主。	
		62443-2-2	Operating an IACS security program	ドラフト執筆中	○	1DC：2012Q2 CDV：2013Q1		
		62443-2-3	Patch management in the IACS environment	ドラフト執筆中	○	1DC：2012Q4 DTR：2112Q3		
		62443-2-4	Certification of IACS supplier security policies and practices <事業者が制御システムのコンポーネントやシステムを調達する際のセキュリティ要件集>		(ほぼ済)	CD：2011.04 CDV：2011.10 <目途> ・2012.5 最終版CD予定	要件レベルが3段階（全、部、個）で構成。 製品のセキュリティ要件を、下記4種で明示的に規定 ・製品組織要件（3分類、10項目） ・セキュリティ機能要件（12分類、44項目） ・受入テスト要件（10分類、40項目） ・メンテ／保守要件（10分類、36項目） ・ISO/IEC 27002をベースとしているとの記載有。	(WIB：Wurldtech、exida)
技術・システム	Sier	62443-3-1	Security technologies for IACS <セキュリティ技術解説書で認証対象でない>	発行済み、RR作成中	(済)	2009.07	認証、フィルタリング／ブロッキング／アクセス制御（FW、IDS、VLAN）、 暗号／データ保護、管理・監査・記録、ソフト管理（脆弱性対応含）、 物理セキュリティ、人的セキュリティ	認証対象外
		62443-3-2	Security assurance levels for zones and conduits	ドラフト執筆中	○	1DC：2012Q2 CDV：2013.02		
		62443-3-3	System security requirements and security assurance levels	ドラフトが75%完成済み	(ほぼ済)	1DC：2011.10 CDV：2012Q1		
部品	ベンダ	62443-4-1	product development requirements	ドラフト執筆中	○	1DC：2012Q2 CDV：2013Q1	セキュアなコンポーネントを開発するための方法を規定。 ISASecureのEDSA（SDSA）をベースにしている。	(EDSA:exida) Wurldtech
		62443-4-2	technical security requirements for IACS components	ドラフト執筆中	○	1DC：2012Q1 CDV：2013Q1	デバイス、システムに搭載されるセキュリティ機能を規定。 ISASecureのEDSA（FSA）をベースにしている。	(EDSA:exida) Wurldtech

IEC: International Electrotechnical Commission CD: Committee Draft , CDV: Committee Draft for Vote , DC: Document for Comments ISA: International Society of Automation
IACS: industrial Automation and Control Systems DTR: Draft Technical Report , NP: New Work Item Proposal , RR:Review Report WIB: international instrument User's Associations

ISASecure認証プログラム



ご清聴ありがとうございました！

本発表の中に引用した報告書はIPAのWebサイトでダウンロードする事ができますので、ご活用下さい。
http://www.ipa.go.jp/security/index.html

Contact：
IPA（独立行政法人 情報処理推進機構）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
TEL 03（5978）7527
FAX 03（5978）7518
電子メール vuln-inq@ipa.go.jp