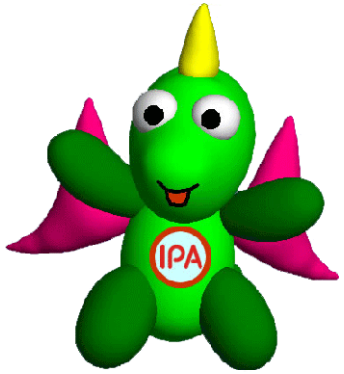
IPA Information-technology Promotion Agency, Japan

IPA重要インフラ情報セキュリティ
シンポジウム2012

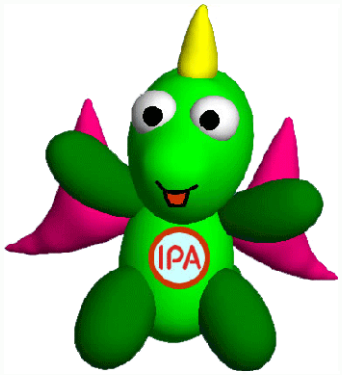
サイバー攻撃と
制御システムのセキュリティ対策(標準化)の
現状と課題について

パネルディスカッションへ

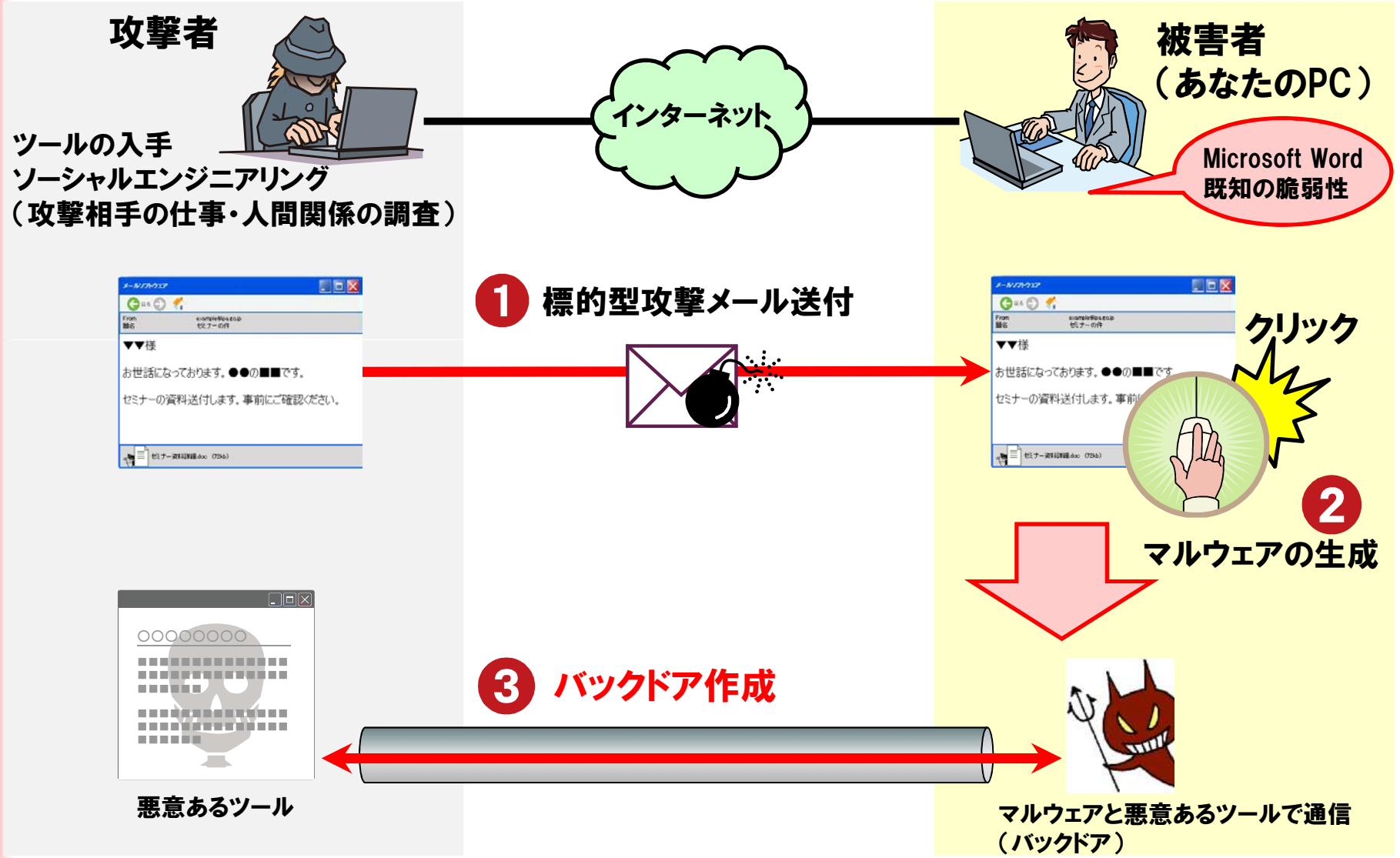


2012年2月23日
IPA技術本部　セキュリティセンター
情報セキュリティ技術ラボラトリー長
小林偉昭

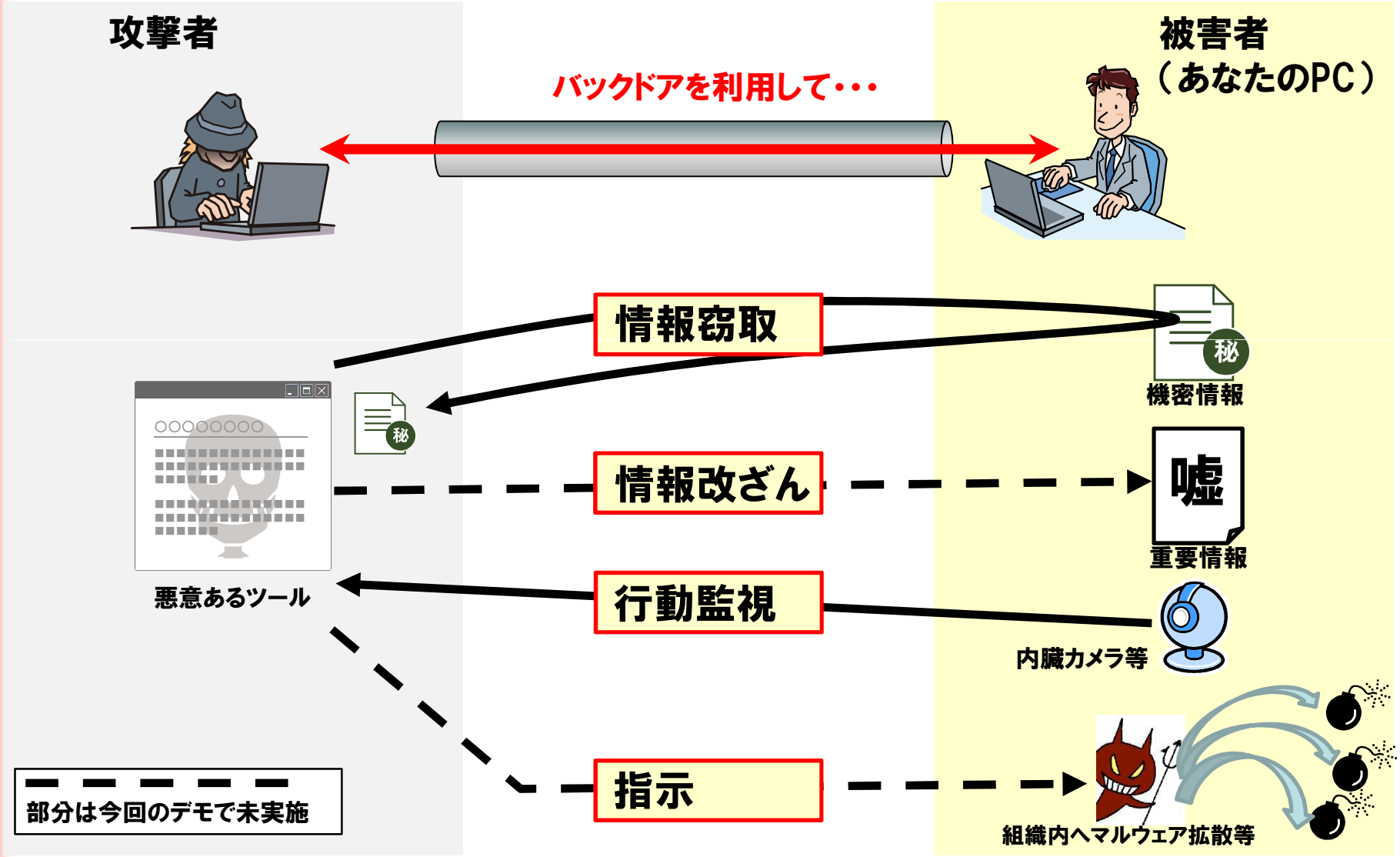
目次



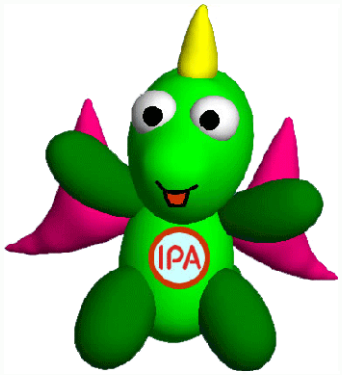
サイバー攻撃のデモ概要　その1



サイバー攻撃のデモ概要　その2



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）

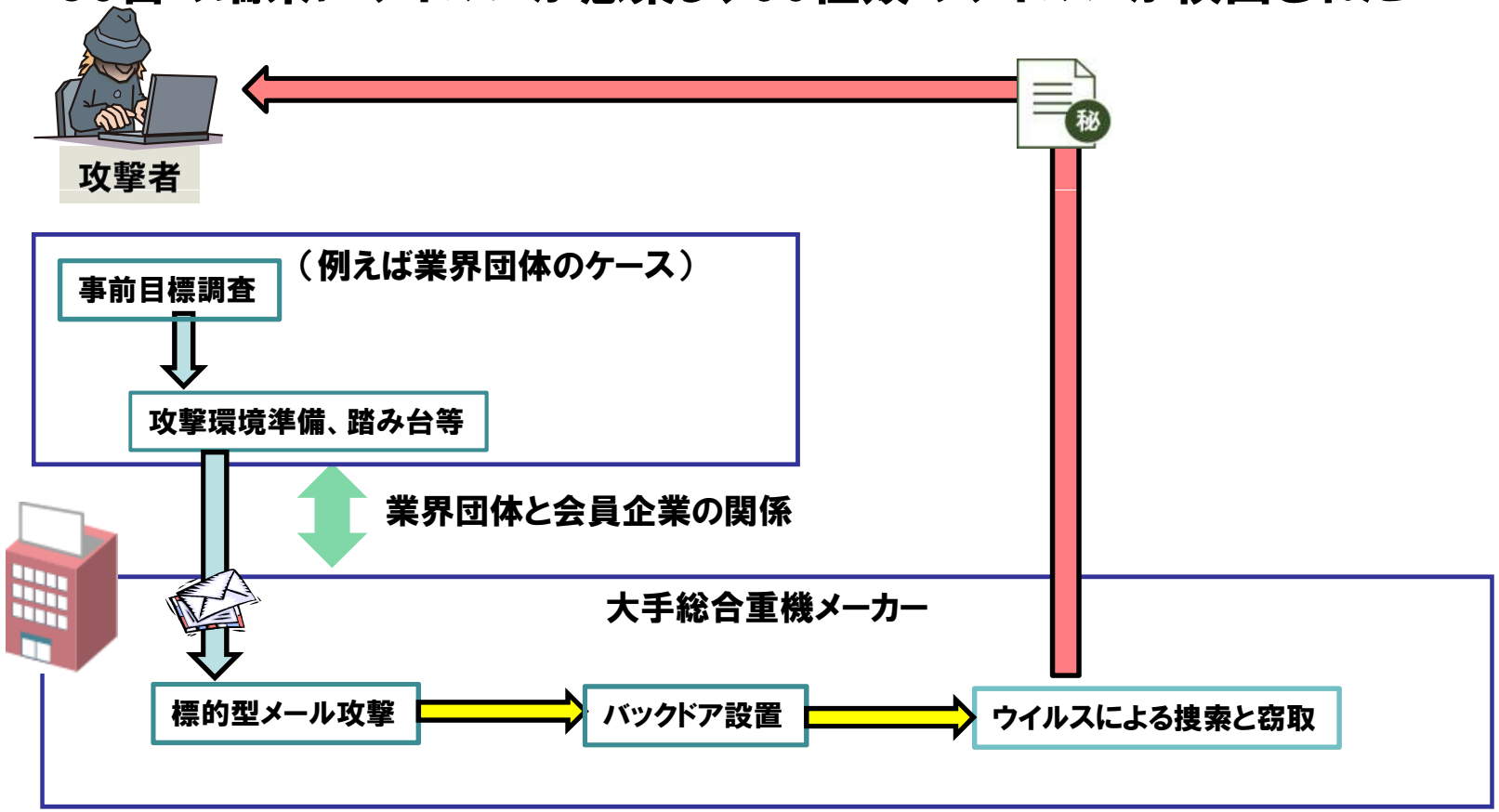
サイバー攻撃の例：

～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～

IPA

■ 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

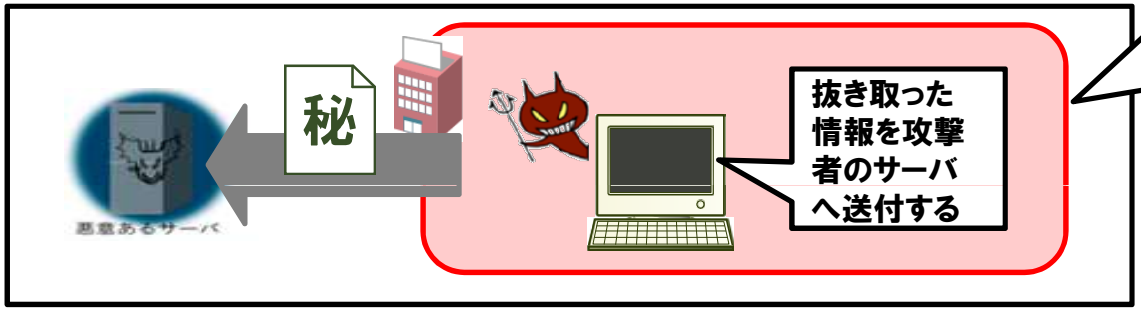


サイバー攻撃の目的

■ 現状のサイバー攻撃を行う攻撃者の目的

– 情報窃取

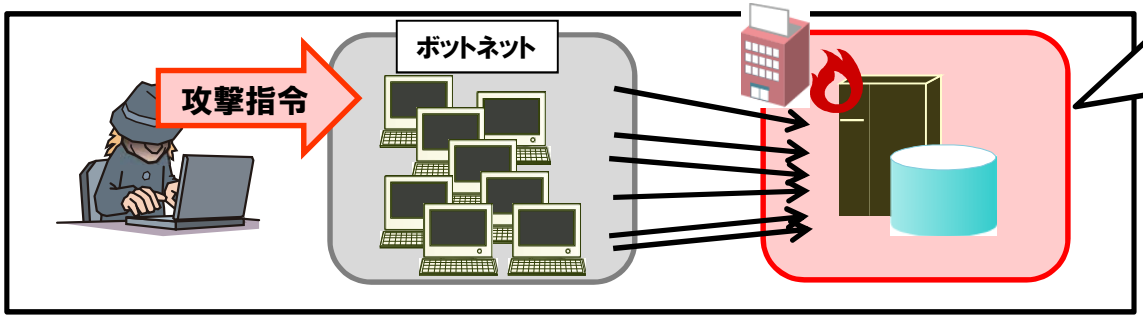
- 金銭に繋がるオンラインバンキング等のアカウント情報等
- 企業の知財や政府の機密等の重要情報



＜攻撃の手法＞
- 従業員宛に「標的型攻撃メール」を送付し、組織内ネットワークへ侵入し、攻撃者へ情報を送付する
- 公開サーバを攻撃し、個人情報を窃取する

– サービス運用妨害（DDoS）

- 組織のサーバや機器等を停止状態に陥らせる



＜攻撃の手法＞
- 攻撃者の制御内にあるボットネットを使用して企業のサーバへ攻撃する
- 攻撃の呼びかけをして標的のサーバを攻撃する

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 ～

IPA

■ 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

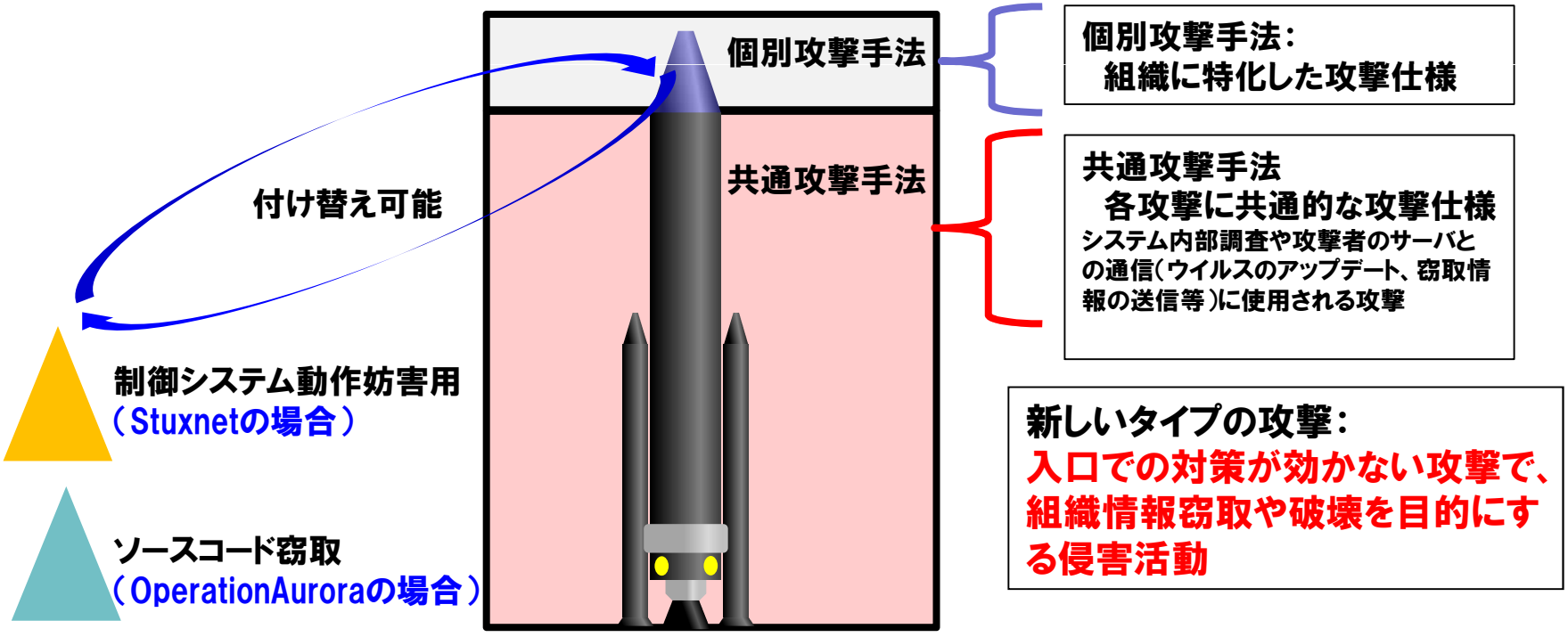
■知的財産情報の窃取 ⇒ 企業の競争力低下、国家の危機管理問題へ

■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

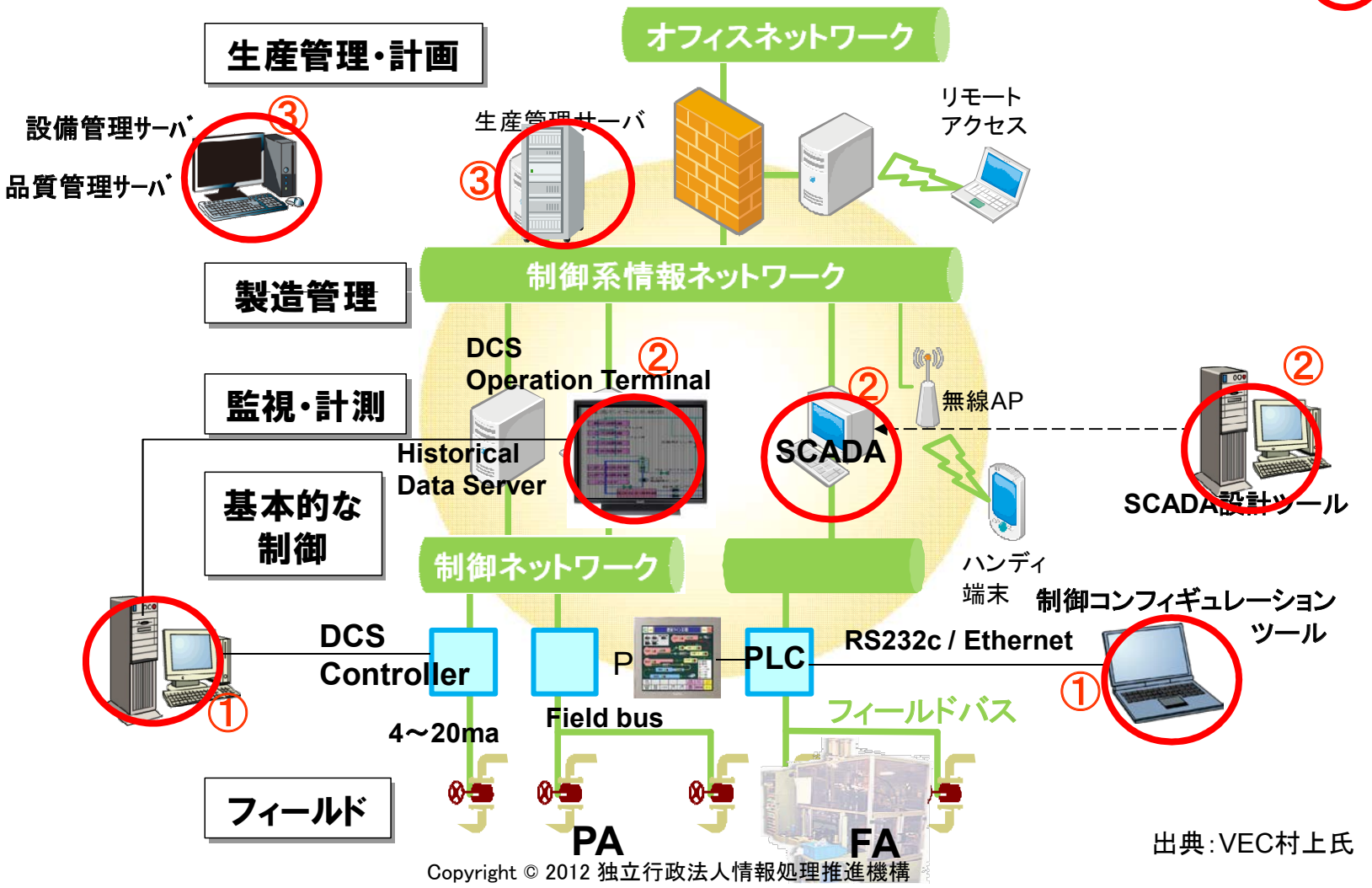
- サイバー攻撃はウェブやメール、USBメモリ等を使い、組織の情報を窃取したり、サービスの運用妨害を行おうとしている。
- サイバー攻撃はソーシャルエンジニアリング等を使うようになったり、組織化されたりしており、年々巧妙になっている



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

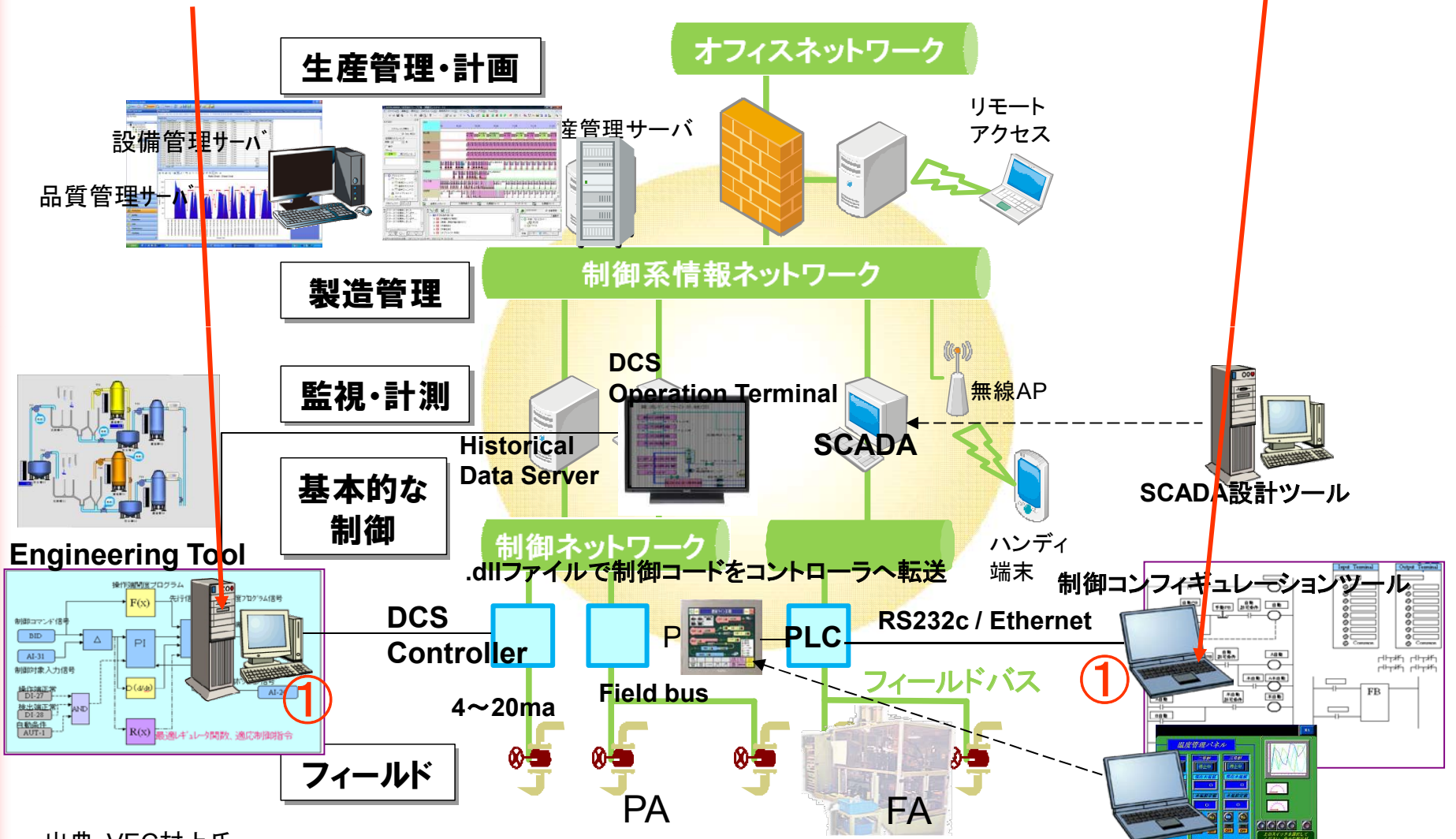
攻撃ターゲット⇒ ◯



出典:VEC村上氏

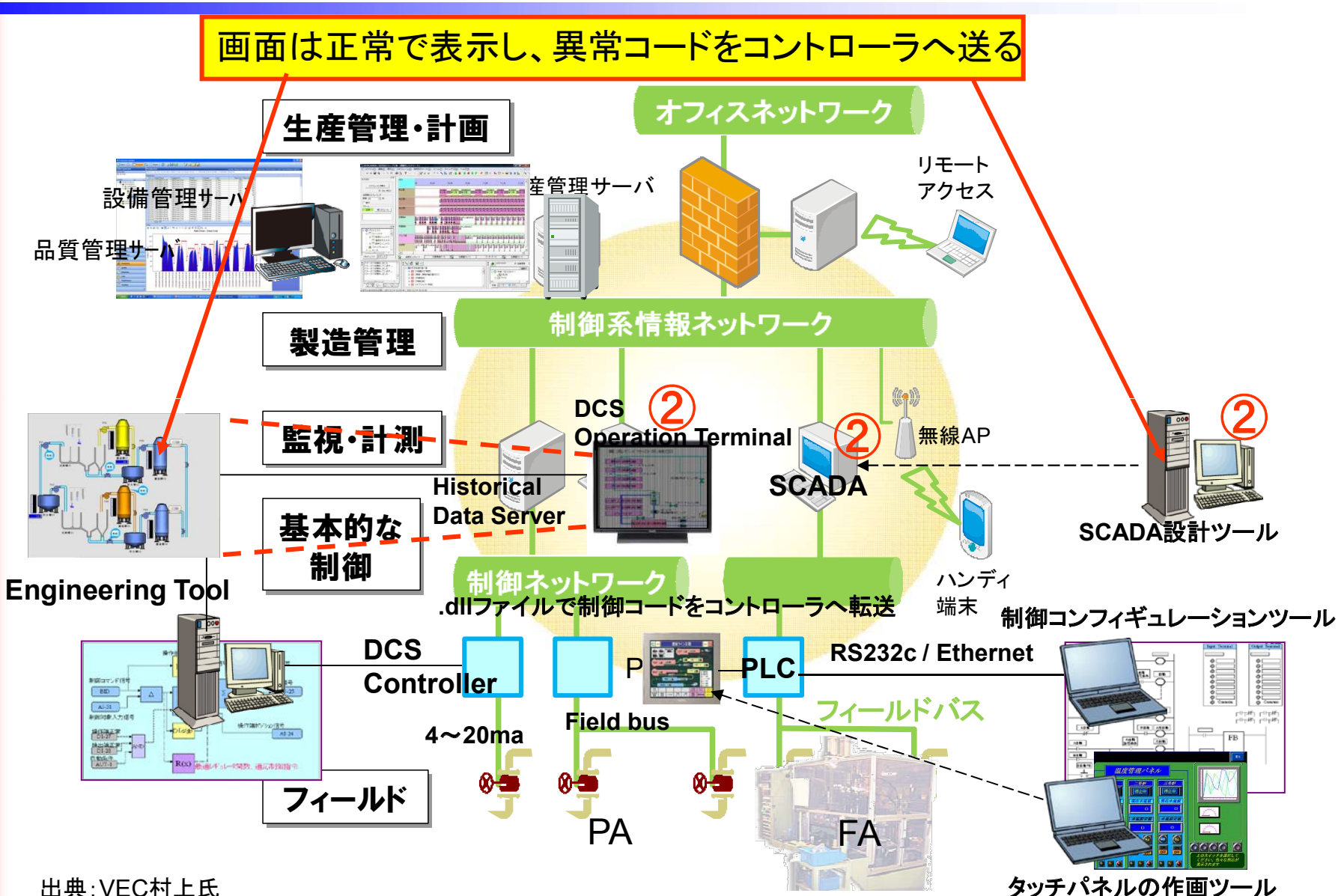
攻撃パターン例：データすり替え

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

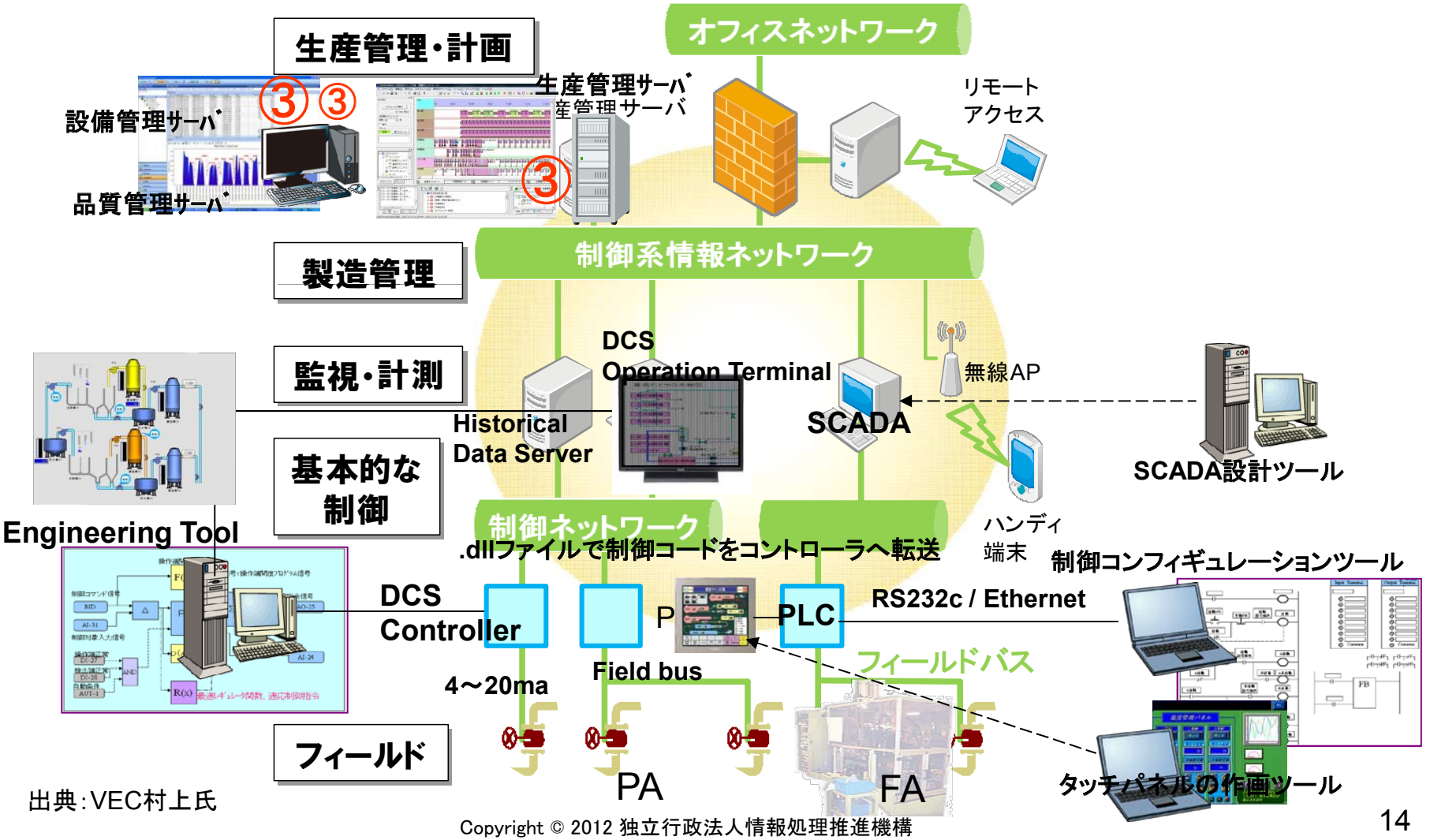
攻撃パターン例：異常コードをコントローラへ



出典：VEC村上氏

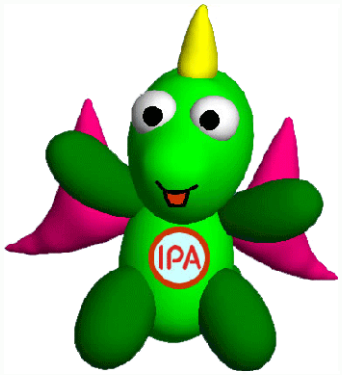
攻撃パターン例：生産管理・計画を異常に

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

目次



制御システムの課題・問題提起

① 脆弱性対策と標準・評価認証

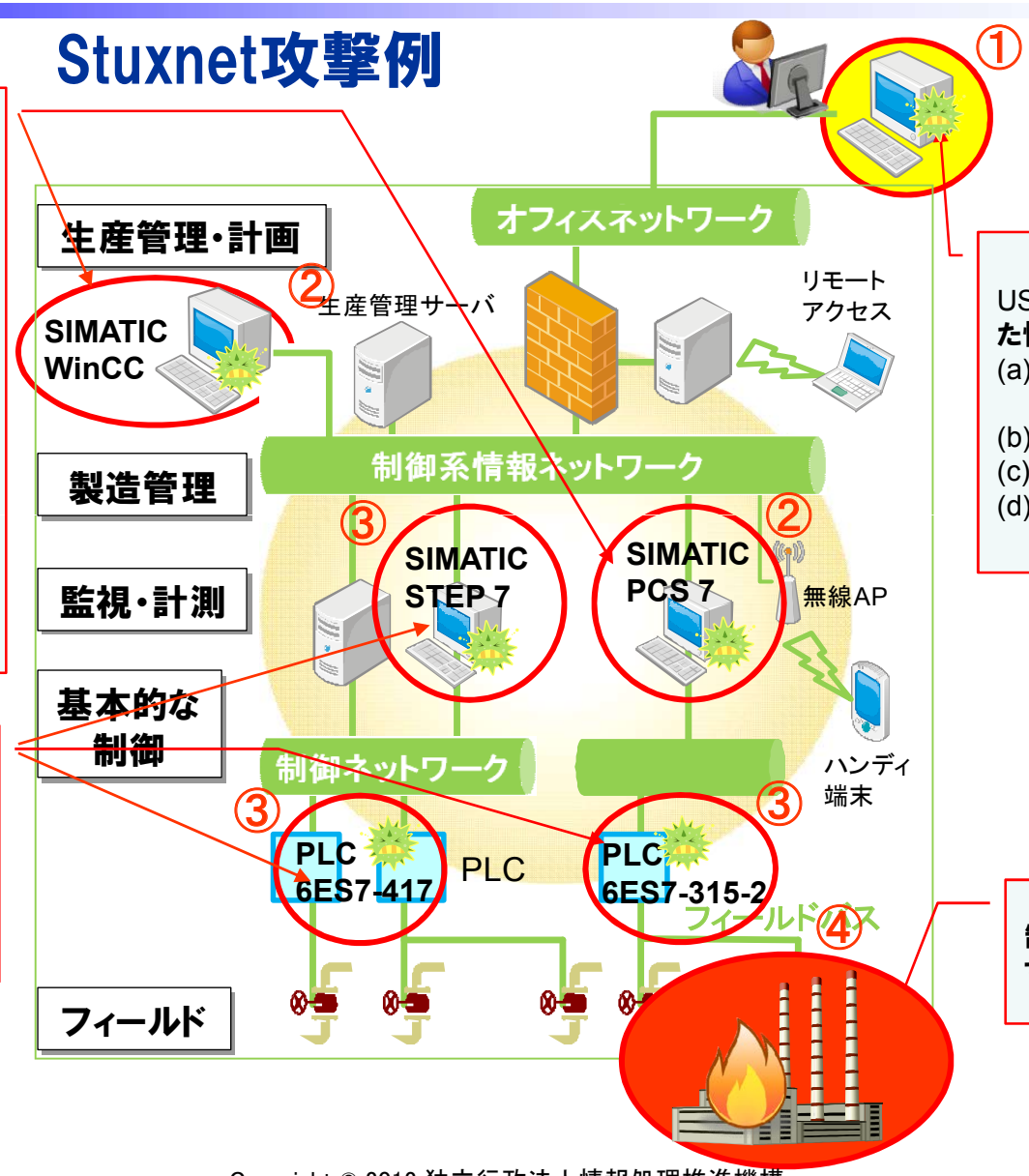
IPA

Stuxnet攻撃例

独シーメンス社製
遠隔監視ソフトウェア
（SIMATIC WinCC or
SIMATIC PCS 7）の
脆弱性を悪用し
て、SQL コマンド経由で
SIMATIC WinCC あるい
は、SIMATIC PCS 7 の
稼働する Windows シス
テムに感染

システムの脆弱性を利
用することにより、権限
昇格や、情報システム
環境内部でウイルスの
拡散などを実行

独シーメンス社製エンジ
ニアリングツール
(SIMATIC STEP 7) を
悪用して、PLC (プログ
ラマブルロジックコント
ローラ) に悪質なコード
の書き込み



USBメモリやインターネットを通じた情報システムへのウイルス感染
(a)USB などのリムーバブル
メディア経由
(b)ネットワーク経由
(c)ファイル共有経由
(d)感染 PC において権限昇格

制御システム上にある装置に対する攻撃の実行

出典：VEC村上氏

制御システムの課題・問題提起

① 脆弱性対策と標準・評価認証

脆弱性対策(パッチ対策)の確実・タイムリーな実施

＊パソコン/サーバ：適宜パッチ実施可能

しかし、制御システムは、止められない！！

⇒ パッチのできる環境整備

⇒ セキュリティを作り込んだ製品の選択

制御システム向けの共通的なセキュリティ標準とその評価・認証

制御システムのセキュリティ規格(IEC62443)
対応製品・システムの採用と管理システム(CSMS)**の構築**

CSMS (Cyber Security Management System)**は、**
ISMS (Information Security Management System)**をベースに制御システム向けに特化・強化**

制御システムの課題・問題提起

② サイバー攻撃によるインシデントへの対応

IPA

迅速・適切なサイバーインシデントへの対応

＊パソコン/サーバ：人が関与している場合がほとんど。
通常の動作とは違うなと気付く可能性が大きい

しかし、制御システムは、人が関与する場面が少ない！監視盤はあるが。
ハードの劣化等の障害かも知れない。切り分けはどうするの？？

⇨ 切り分け手順へサイバー攻撃での異常可能性も追加
(ガイド等の整備）

⇨ サイバーインシデント発生時の連携体制
事業者・ベンダ・専門家等のタイムリー・緊密な連携

米国では、ICS-CERTが活動中
日本は、どのような形態がよいのか、議論中

ICS-CERT : Industrial Control Systems – Cyber Emergency Response Team

制御システムの課題・問題提起

③ 官民連携PPPによる情報共有　PPP：Public Private Partnership

制御システムは、社会のインフラを支えている

サイバー攻撃を成功させないためには

＊情報システムに比べると、自社だけの被害という認識よりも
社会のインフラ全体へ影響を与えてしまうという認識が強い

＊地震・台風などの自然災害時の対応体制が参考になるか。
3.11では、自助・共助・公助の連携したBCPが必要になった。

⇨ **自助・共助・公助の連携でのサイバー攻撃への対応**
（連携ガイド等の整備）

⇨ **具体的な事例**

米国：DHSによる制御システム向けCSSPのICSJWGが活動中
欧州：ENISAのPPPガイド(36の勧告）
日本：重工・防衛産業9社とIPAでのJ-CSIP準備中
(3月末正式開始)

DHS : Department of Homeland Security　CSSP : Control Systems Security Program　http://www.us-cert.gov/control_systems/
ICSJWG : Industrial Control Systems Joint Working Group
ENISA : European Network and Information Security Agency
Good Practice Guide on Cooperative Models for Effective Public Private Partnerships (PPPs)
http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps

官民連携によるサイバー攻撃への対応

サイバー情報共有イニシアティブ J-CSIP

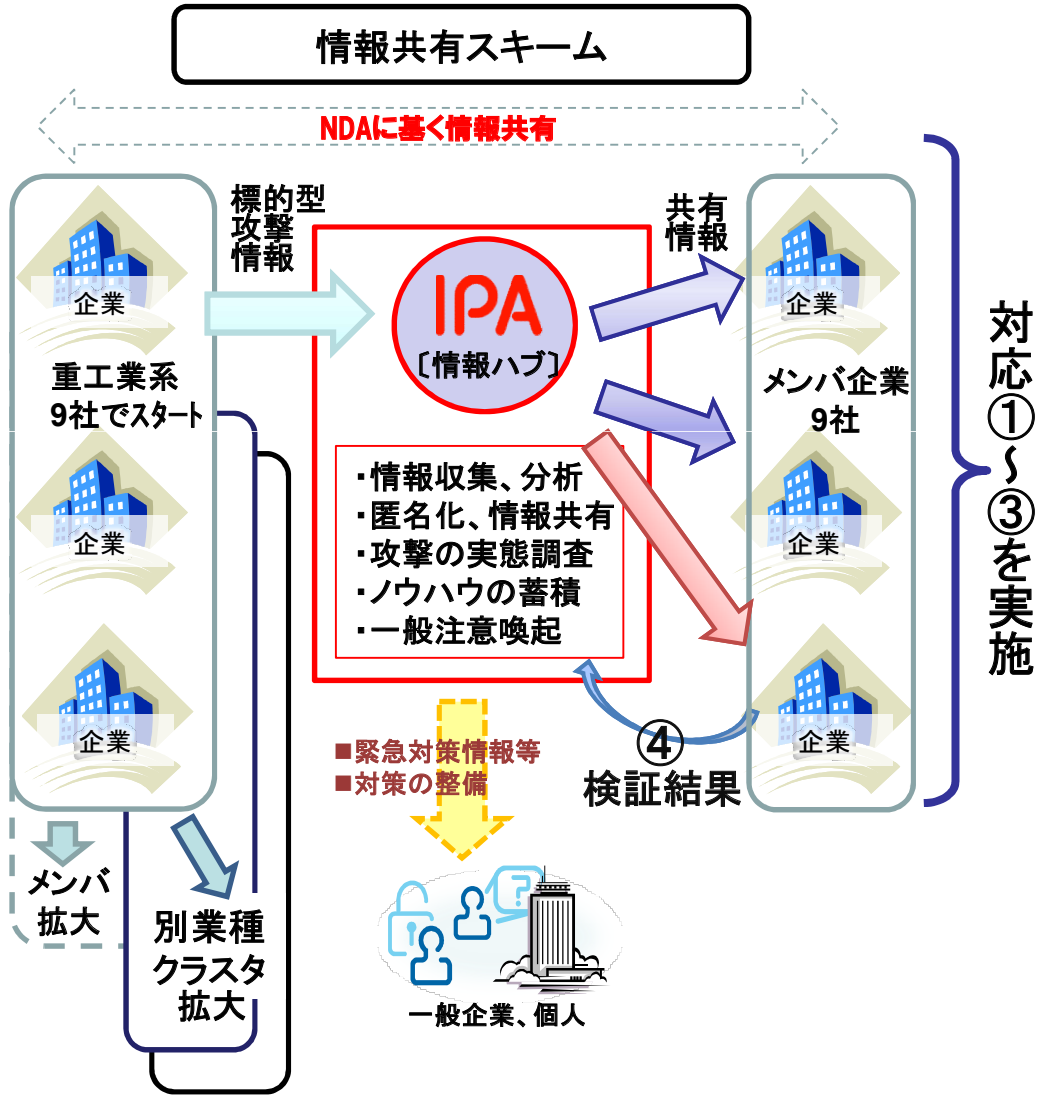
J-CSIPメンバ企業実施項目

① 組織内への注意喚起
⇒ メール開封を回避
②メールサーバのアーカイブの検証
⇒ 攻撃痕跡検証
③防御対策
⇒メールフィルタのチューニング、
FWパラメータ設定等

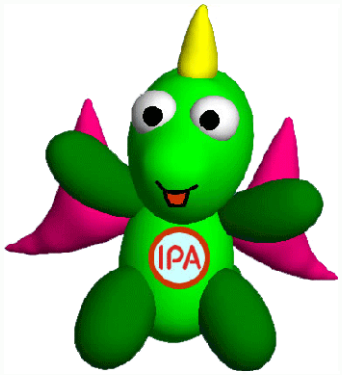
④ 検証結果のフィードバック ⇒ 再度の情報共有
- ✔ 該当メール、類似メールの検出有無
- ✔ 開封の有無
- ✔ 被害の有無

標的型攻撃メールからスタート

J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan



目次



パネルディスカッション

テーマ ： 安全な社会インフラの持続に向けて

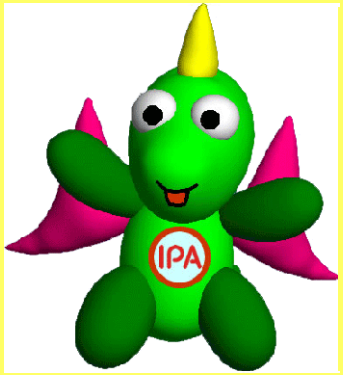
① 官民連携PPPによる情報共有

② サイバー攻撃によるインシデントへの対応

③ 脆弱性対策、標準・評価認証

④ 人材育成

⑤ 会場から



参考資料　：　標準・評価・認証

制御システム分野における標準と認証･評価の位置づけ

標準化 *1)

事業者

インテグレータ

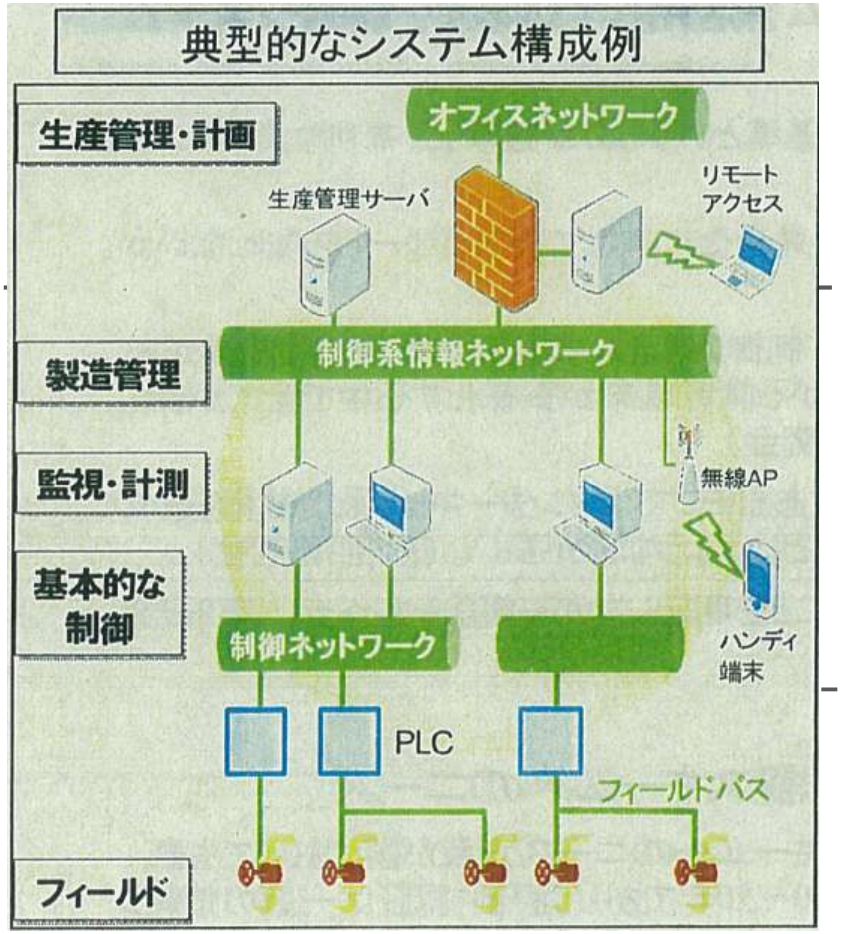
装置ベンダ

IEC62443-1

IEC62443-2
管理･運用･ﾌﾟﾛｾｽ

IEC62443-3
技術･システム

IEC62443-4
ｺﾝﾎﾟｰﾈﾝﾄ･ﾃﾞﾊﾞｲｽ



認証･評価

･WIB*2)
＜Wurldtec＞

＜評価事業者＞
･ISCI:ISASecure*3)
＜exida＞
･Wurldtec Achilles*4)
＜Wurldtec＞

*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（ﾍﾟﾈﾄﾚｰｼｮﾝ、ﾌｧｼﾞﾝｸﾞﾃｽﾄ）。調達要件に指定されている。

IEC62443規格化の状況

(2012年1月現在)

区分	主対象者	IEC	原本名及び概要	現状のステータス ドキュメントの状況，ドラフトの現状	2012のTC65's Plenary meetingにDC提示予想	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 <本標準での用語の統一と、一般論の導入部分で、認証自体には関わらない。>	発行済み，アップデート中 RR作成中	(済)	2009.07 Ed.2：1CDは21011Q4	・セキュリティ概念（目的、基本要件、体系、リスク分析、ポリシー、経路、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（5階層）、資産モデル（参照アーキテクチャ）、ゾーン＆経路モデル	― 認証の対象外
		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）のICS版： ・リスク解析、リスク対応（ポリシー、組織、対策、実装）、モニタリングと改善 ・127要件（ISO17799：128、ISO27001：132） ・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認証が普及しているのは日本が主。	
		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>	・CD：7/21時点、55%の賛成でプロジェクト存続。 ・9/19-22： IEC/TC65/ WG10：現CDへのコメント（1,112件）を受け、改訂案を議論、2012.2全体調整予定。 <評価・適合性に関しては全部削除し、スコープ外とし、他のドキュメントとの整合性をとる>	(ほぼ済)	CD：2011.04 CDV：2011.10 <目標> ・2012.5 最終版CD予定	要件レベルが3段階（金、銀、銅）で構成。 製品に対するセキュリティ要件を、下記の4レイアで明示的に既定している： ・製造組織要件（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記載有	(WIB：Wurldtech、exida)
技術・システム	構築事業者・SI	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・証跡、ソフト管理（脆弱性対応含む）、物理セキュリティ、人的セキュリティ	― 認証の対象外
		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	prodauct 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) *) CRTはWurldtechもエントリ中

IEC: International Electrotechnical Commision
IACS: industrial Automation and Control

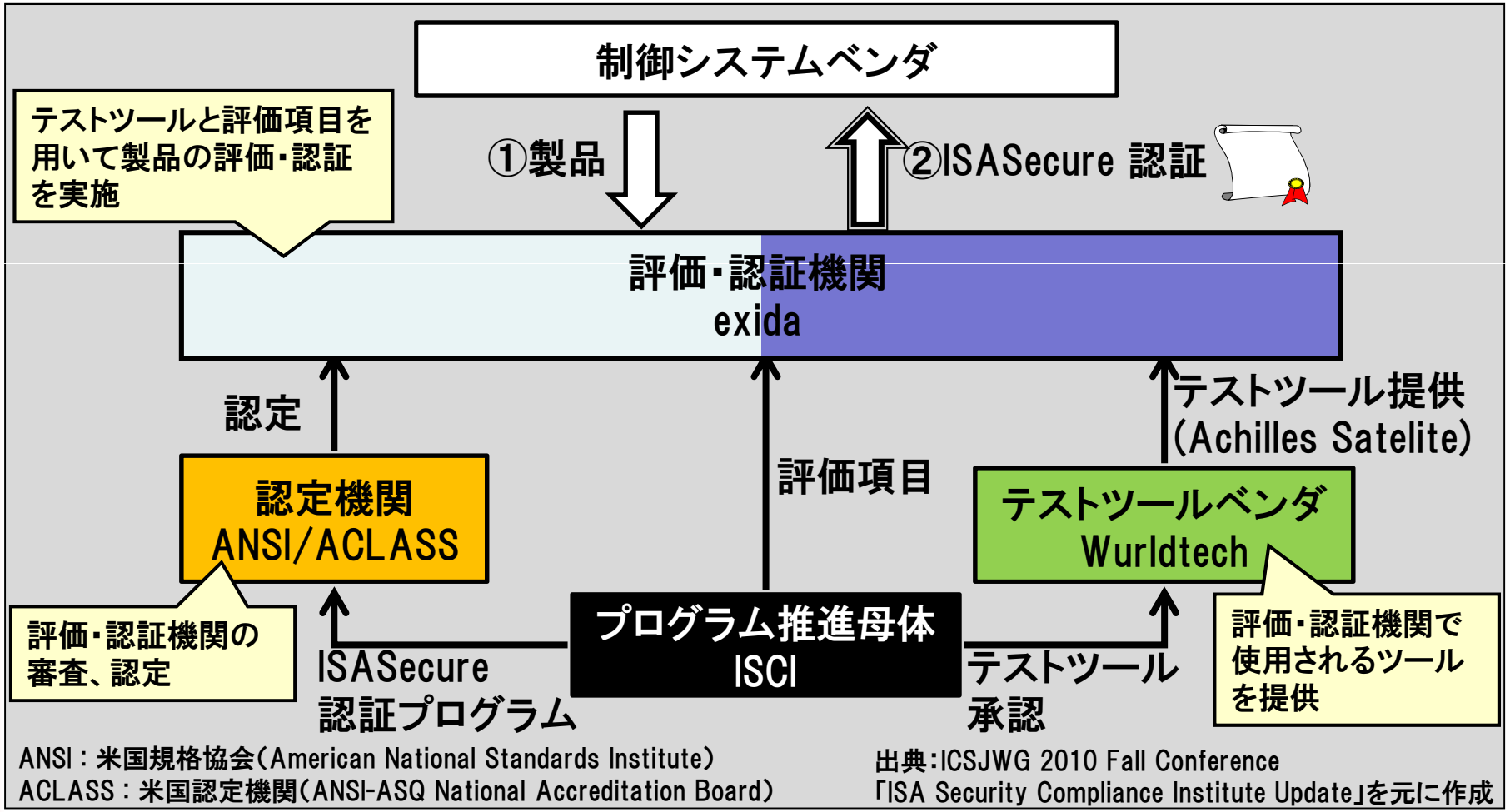
CD：Committee Draft 、CDV：Committee Draft for Vote、DC：Document for Comments
DTR: Draft Technical Report 、NP：New Work Item Proposal 、RR:Review Report

ISA: International Society of Automation
WIB: international instrument User's Associations

ISASecure認証プログラム

IPA

評価・認証機関：製品を評価し，ISASecure認証を発行する機関
認定機関：評価・認証機関を審査し，認定する機関
テストツールベンダ：評価・認証機関で使用されるツールを提供する企業



ANSI：米国規格協会(American National Standards Institute)
ACLASS：米国認定機関(ANSI-ASQ National Accreditation Board)

出典:ICSJWG 2010 Fall Conference
「ISA Security Compliance Institute Update」を元に作成

ご清聴ありがとうございました！

本発表の中に引用した資料等は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/

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