Information-technology Promotion Agency, Japan

IPAグローバルシンポジウム2012

制御システムの今あるセキュリティ脅威と対策について

～制御システムは、セキュリティ脅威とは関係ないと思っていませんか～

2012年5月24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

1. **サイバー攻撃とは**
2. 近年のサイバー攻撃の分析
3. 制御システムの現状
4. 制御システムへのサイバー攻撃例と課題
5. 社会インフラを支える制御システムに向けて

サイバー攻撃の例

■ 2011年から2012年はサイバー攻撃の報道が目立つ

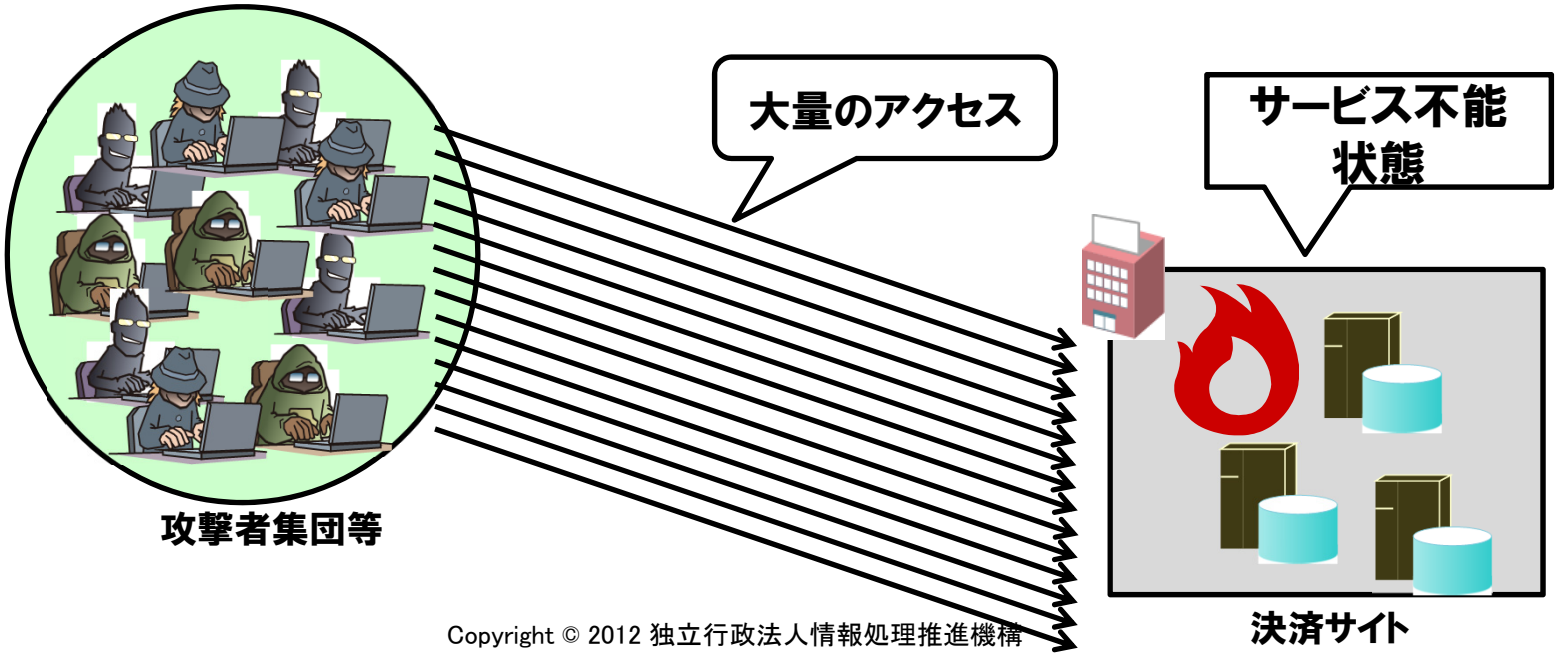
時期	報道
2011/2	中国から欧米エネルギー5社攻撃 （毎日新聞等）
2011/3	韓国で大規模ハッカー攻撃　大統領府や銀行など40機関 （朝日新聞等）
2011/3	仏財務省にサイバー攻撃、G20情報盗まれる （読売新聞等）
2011/4-5	ソニーにサイバー攻撃、個人情報流出1億件超 （朝日新聞等）
2011/5	韓国の農協でシステム障害 （読売新聞等）
2011/6	米グーグル：中国からサイバー攻撃　米韓政府関係者ら被害 （毎日新聞等）
2011/9	三菱重にサイバー攻撃、80台感染…防衛関連も （読売新聞等）
2011/9	IHIにもサイバー攻撃　日本の防衛・原発産業に狙いか （産経新聞等）
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）
2012/1	JAXA：職員のパソコン感染、無人補給機情報など流出か （毎日新聞等）
2012/2	農水省に標的型メール攻撃、情報流出狙う？ （読売新聞等）
2012/2	特許庁、トロイの木馬型感染…メール情報流出か （読売新聞等）
2012/3	国際協力銀行の顧客220社とのメール流出 （毎日新聞等）

サイバー攻撃の例：
～決済サイトへのDDoS攻撃～

IPA

■ 決済サイトへの攻撃

- 決済サイトが、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。
- 大手企業の運営する、攻撃者から地方自治体向けシステムが狙われ、そのシステムが一定期間サービスを提供できない状態になった。
- 韓国の主要サイトに対して、DDoS攻撃が行われた。ウェブサービスのプログラムをウイルスへと改ざんし、利用者に感染させてDDoS攻撃を行った。



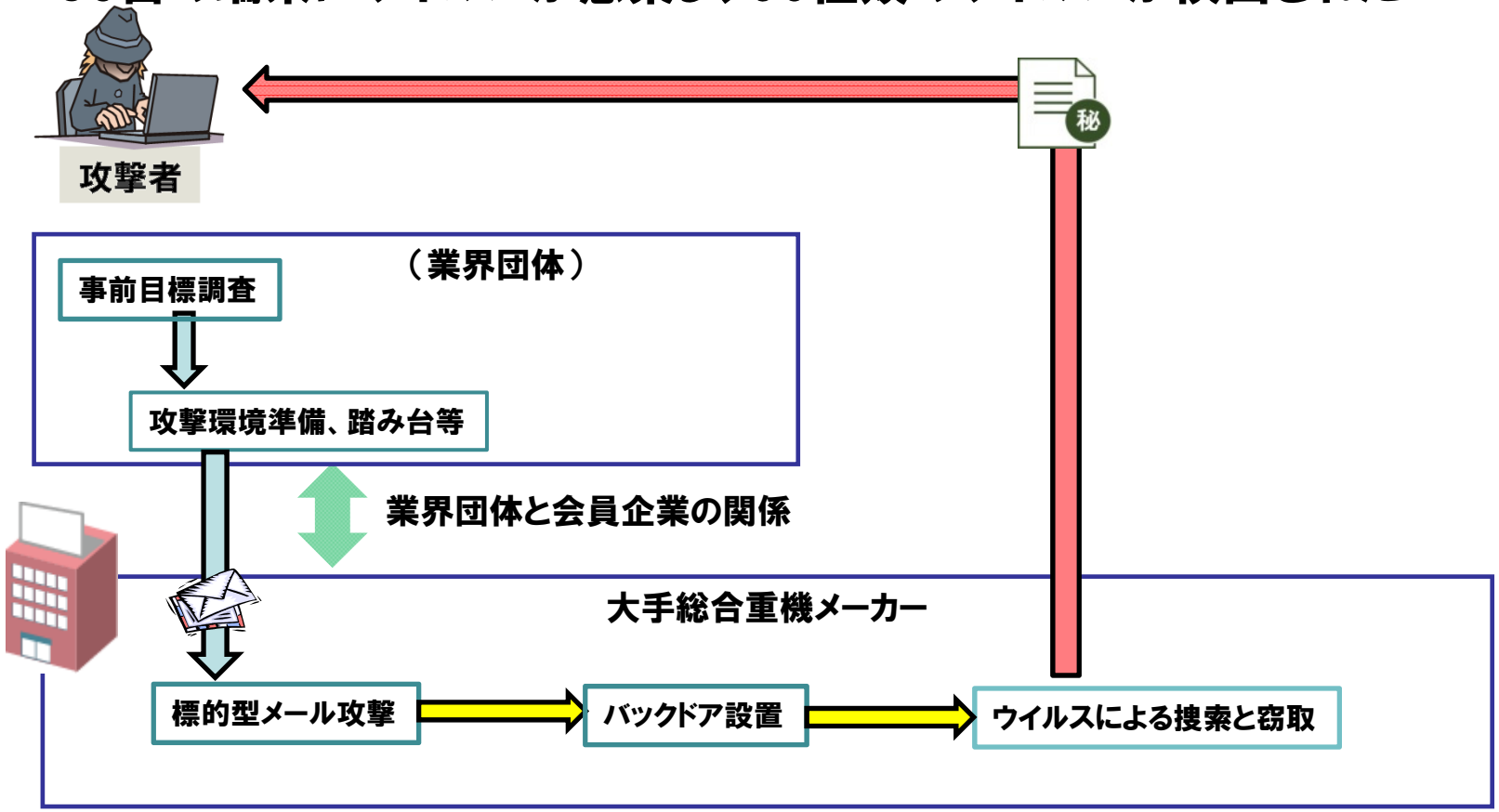
サイバー攻撃の例：

～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～

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

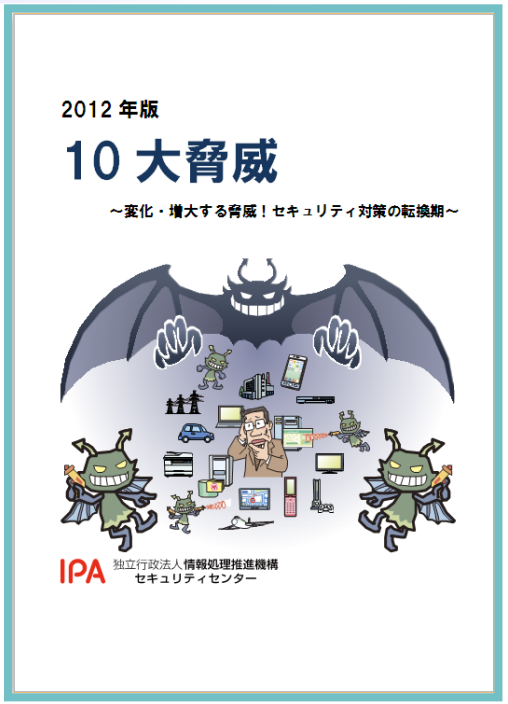


2012年版「10大脅威」
『変化・増大する脅威！セキュリティ対策の転換期』

2012年3月22日公開

http://www.ipa.go.jp/security/vuln/documents/10threats2012.pdf

2012年版10大脅威は、2011年に発生したセキュリティインシデントや攻撃情報などの一般報道を基にして、情報セキュリティ分野の研究者や実務担当者129人で構成する「10大脅威執筆者会」でまとめたもの。2005年から毎年公開しており、今年で8回目。下記のような構成で、情報セキュリティ分野の脅威に関する情報をまとめた資料。



第1章	・情報セキュリティを取巻く環境の変化
第2章	・10の脅威について概要と影響の解説
第3章	・今後対策が重要となる脅威

投票により順位付け

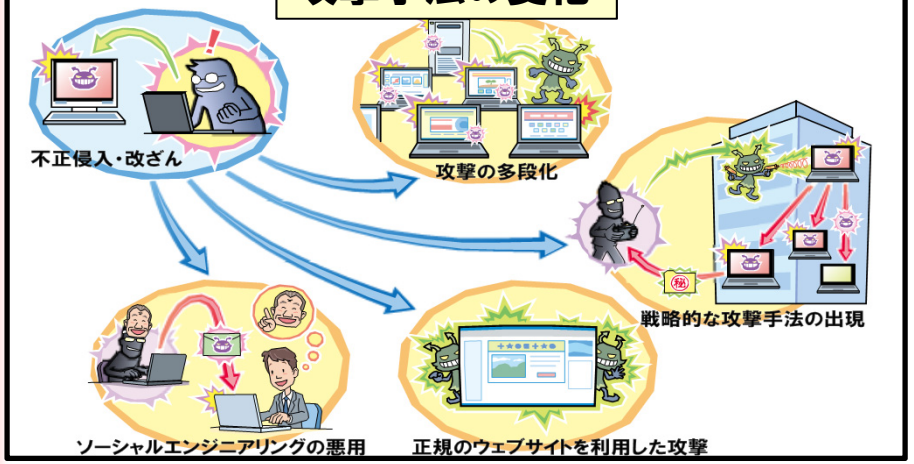
ダウンロード数：99,584
（3/22-31まで）

情報セキュリティを取り巻く状況の理解やセキュリティ対策の参考に、本書をご活用ください。

10大脅威　第1章
情報セキュリティを取り巻く環境の変化

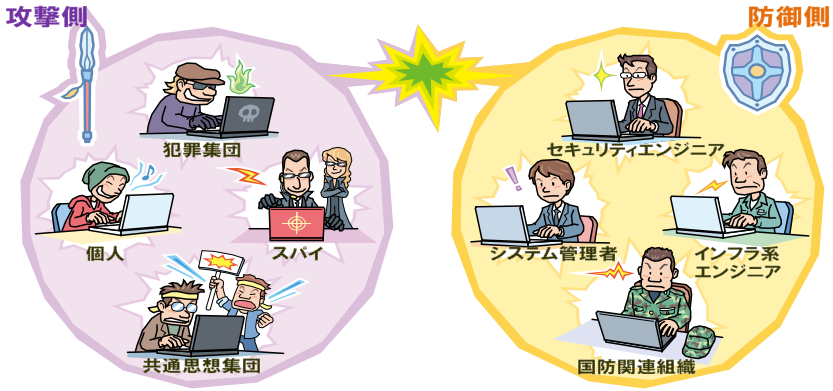
IPA

攻撃手法の変化

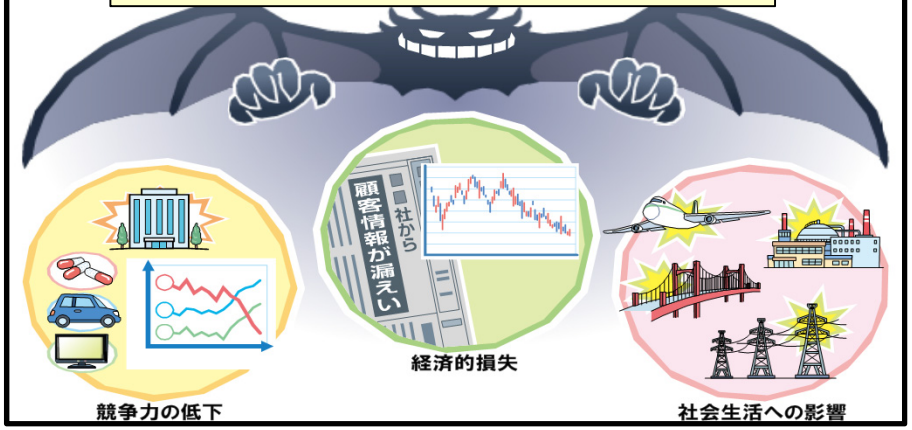


システム環境の変化

情報セキュリティを取り巻く構図の変化



攻撃を受けた際のインパクトの変化



制御システムも狙われる環境になりつつあり、
重要インフラ等が狙われた場合、社会生活に影響を及ぼす懸念も

10大脅威　第2章
2012年執筆者会が選んだ10大脅威

10大脅威執筆者会が選んだ 2012年情報セキュリティ10大脅威

はサイバー攻撃関連の脅威

1位	機密情報が盗まれる!?新しいタイプの攻撃 New
2位	予測不能の災害発生！引き起こされた業務停止 New
3位	特定できぬ、共通思想集団による攻撃 New
4位	今もどこかで…更新忘れのクライアントソフトを狙った攻撃
5位	止まらない！ウェブサイトを狙った攻撃
6位	続々発覚、スマートフォンやタブレットを狙った攻撃
7位	大丈夫!?電子証明書に思わぬ落し穴 New
8位	身近に潜む魔の手・・・あなたの職場は大丈夫？
9位	危ない！アカウントの使いまわしが被害を拡大！
10位	利用者情報の不適切な取扱いによる信用失墜 New

10大脅威　第2章
例:【3位】特定できぬ、共通思想集団による攻撃

- 脅威
  - 自分たちの主義・主張に反する政府機関や企業を攻撃する集団
  - ソーシャルメディアを活用することで手広く仲間を募り、攻撃を呼掛ける
  - 自らの主張を認めさせるために、攻撃を予告し、攻撃対象組織が主張を見直すように要求。要求が却下されれば、下記の攻撃を実施

    攻撃例:DDoS,機密情報の暴露、ウェブサイトの改竄

10大脅威　第2章
例:【3位】特定できぬ、共通思想集団による攻撃

- **対策1:インターネットへ公開しているウェブサーバなどの定期的なセキュリティ対策**
  - 公開サーバの脆弱性対策
  - 機密情報の取り扱いに関する見直し
  - 日ごろからのセキュリティ対策
- **対策2:利用者の意見に耳を傾ける**
  - 対立する問題に対して、適切に対応することにより、問題の発生を未然に防げる可能性がある
  - 対決姿勢を煽らない対応も重要である

公開サーバ(サービス)に対して、DDoS対策の負荷に耐えられるように設計したり、日頃からセキュリティ点検と対策を行ったりすることが重要

10大脅威　第3章
社会基盤である重要インフラへの攻撃

- **状況の変化**
  - 近年では利便性やコスト面のメリットから、VPN (Virtual Private Network) を利用したリモート監視や制御用端末にWindowsやUNIX系OSが採用されるようになっている
  - 情報系システム同様のシステム環境に近づきつつある

⇒ **情報系システム同様にサイバー攻撃の脅威が現実化**

- **想定される脅威**
  - 攻撃を受けた際の被害は**我々の生活にも密接に関ってくる**
  - 例）重要インフラが攻撃されると
    - 交通システムの場合：電車の運行停止やダイヤの乱れなど、交通機関が麻痺

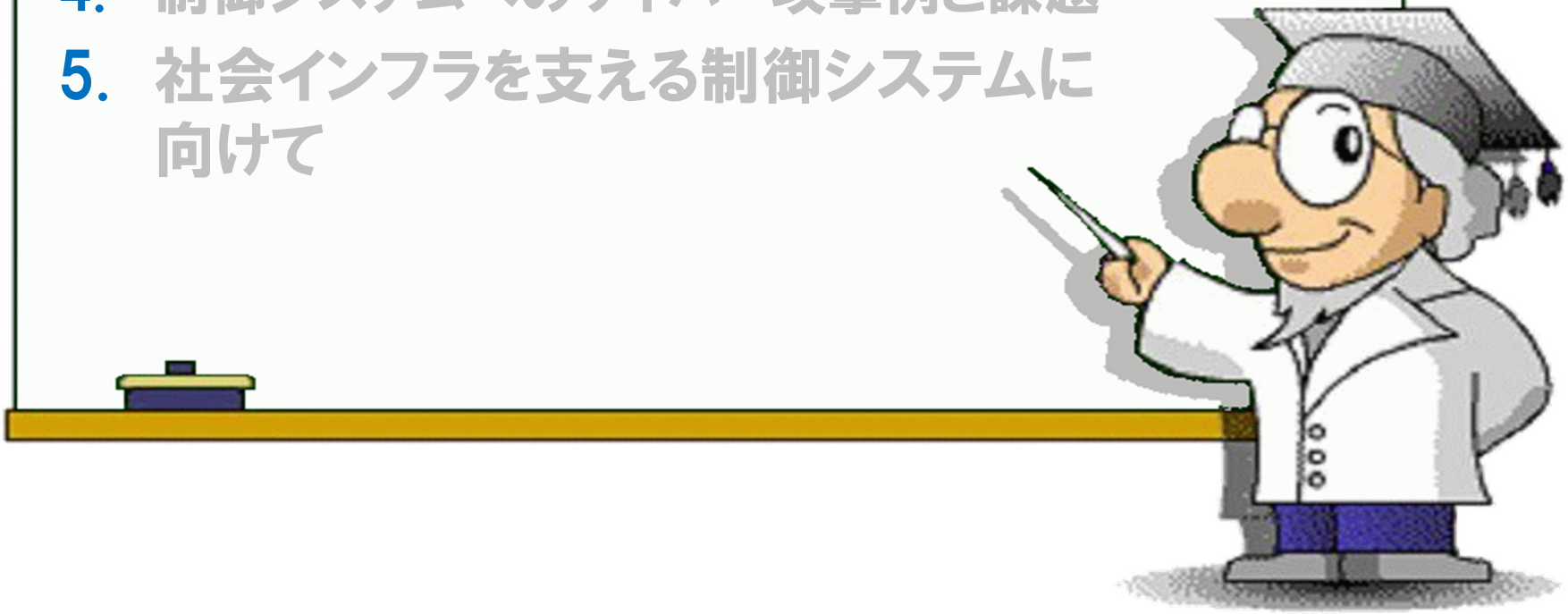
重要インフラへの攻撃は、社会の混乱を狙ったものであるため、攻撃が発生した際のインパクトが大きい

10大脅威　第3章
社会基盤である重要インフラへの攻撃

- **海外での事例**
  - 鉄道ダイヤ乱れ（2003年米国）
    - 米国東部の鉄道会社の信号管理システムがウイルスに感染
    - 周辺の3路線で列車の運行停止やダイヤ乱れが発生
  - 原子力システムへのウイルス感染（2003年米国）
    - 米国の原子力発電所でVPN接続を介して制御システムにウイルスが侵入
    - 5時間に渡ってシステムが停止してしまった
- **重要システムにおけるセキュリティ対策の難しさ**
  - 情報系システムとは異なり、「システムを止めない事」が重要視される傾向
  - 我々の生活に密接に絡んでいるため、24時間365日稼働することが求められる
  - 情報システムと異なり、パッチ適用のためにシステムを停止することが難しい。如何にシステムを止めずにセキュリティを確保するかが大きな課題
  - 故障（ハード障害・劣化やソフト不良）とサイバー攻撃の切り分けが困難

目次

1. サイバー攻撃とは
2. **近年のサイバー攻撃の分析**
3. 制御システムの現状
4. 制御システムへのサイバー攻撃例と課題
5. 社会インフラを支える制御システムに向けて



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？・Hacktivist・
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

今日の攻撃者像の分析

1.諜報活動をする者？

目的
情報窃取が主な目的
（情報破壊等もあり得る）

手法
標的型攻撃メール
組織内ネットワークへ侵入

事例
大手重工関連企業
衆議院・参議院

2.共通思想集団（Hacktivist）

目的
独自の主義主張

手法
サーバへのDDoS攻撃
サーバから情報窃取
SNSで勢力拡大

事例
Anonymous, Lulzsec
ゲーム会社への攻撃

3.詐欺集団（従来からの攻撃の1つ）

目的
金銭目的

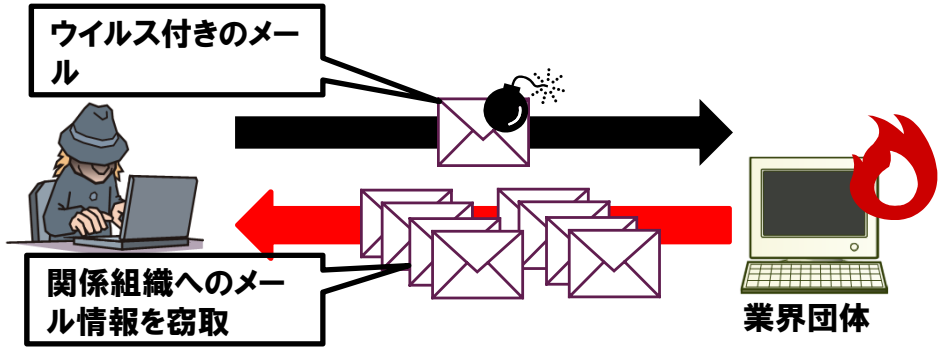
手法
フィッシング詐欺
マルウェア感染
（クレジットカード番号取得等）

事例
一般ユーザのウイルス感染
決済サイトへの攻撃
ショッピングサイトへの攻撃

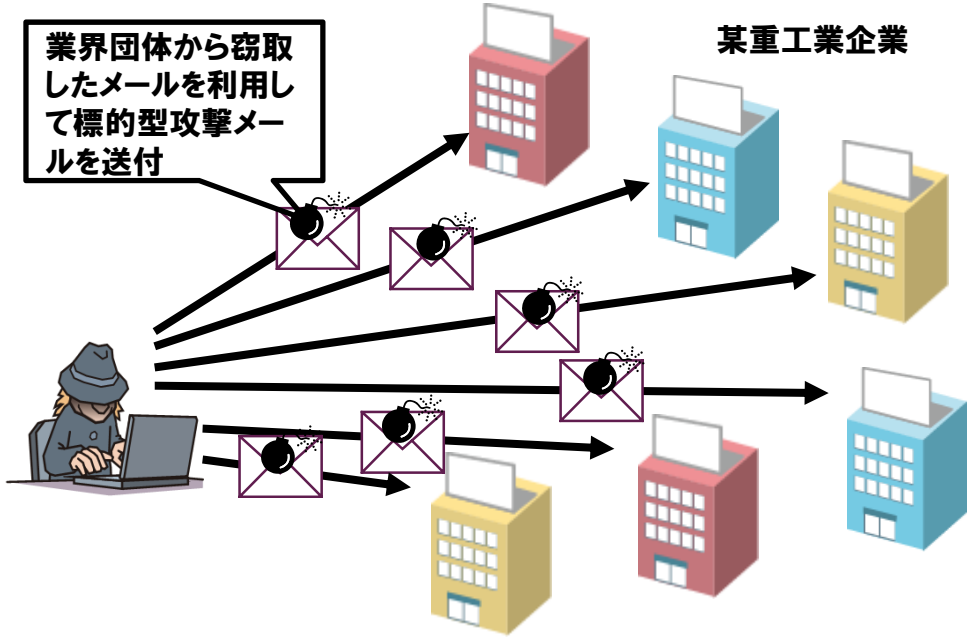
組織の機密情報を窃取する諜報活動を行うサイバー攻撃

攻撃の流れ

①
団体職員のPCがウイルスに感染し、
関係企業とやり取りしていたメール情報が盗まれた。



②
盗まれたメールを使用され、
関係企業に対して
標的型攻撃メールを送付された。

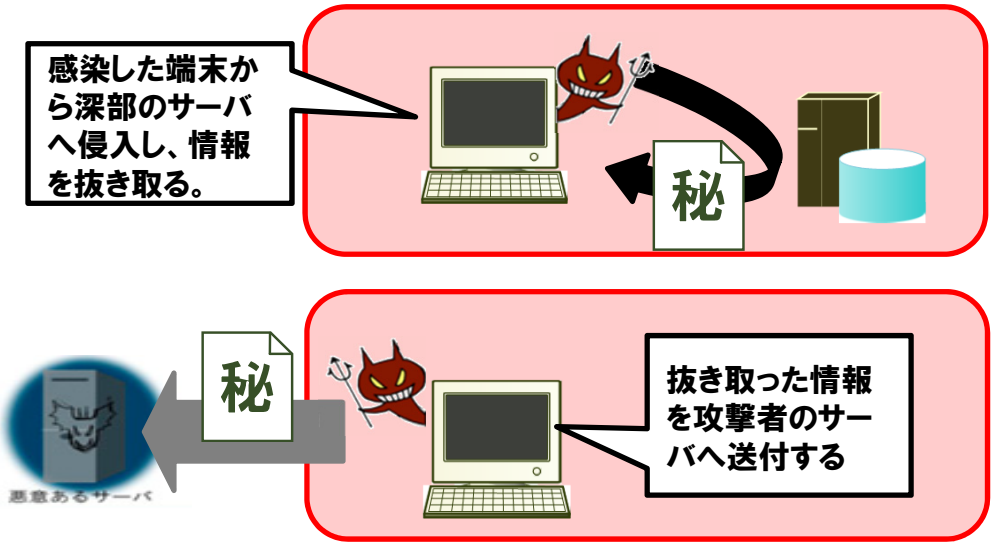


組織の機密情報を窃取する 諜報活動を行うサイバー攻撃

続き

事象：ウイルスは社内拡散

端末に感染したウイルスにより**内部サーバへ侵入され、一部の情報を抜き取られた可能性がある。**
抜き取られた情報を攻撃者のサーバへ送付される。



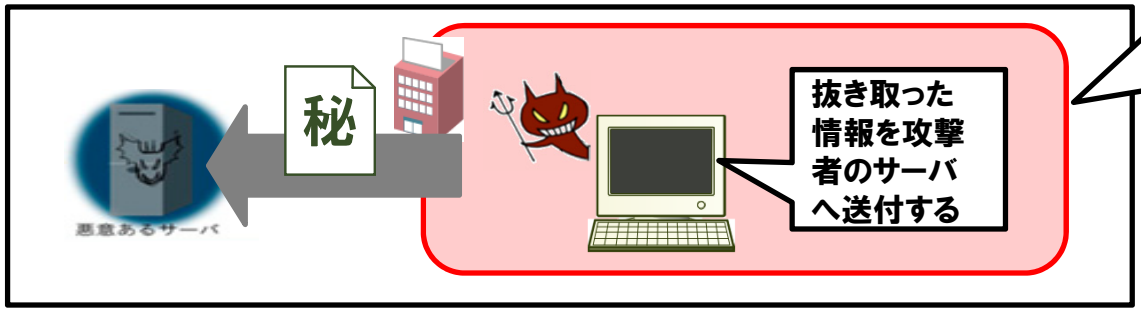
組織内に巧妙なルートで侵入され、
- 組織内拡散
- 組織内調査
- 重要サーバへの不正アクセス

による・・・
組織の重要情報（知的財産、顧客情報等）を狙われる事件が顕在化

現状のサイバー攻撃を行う攻撃者の目的

① 情報窃取

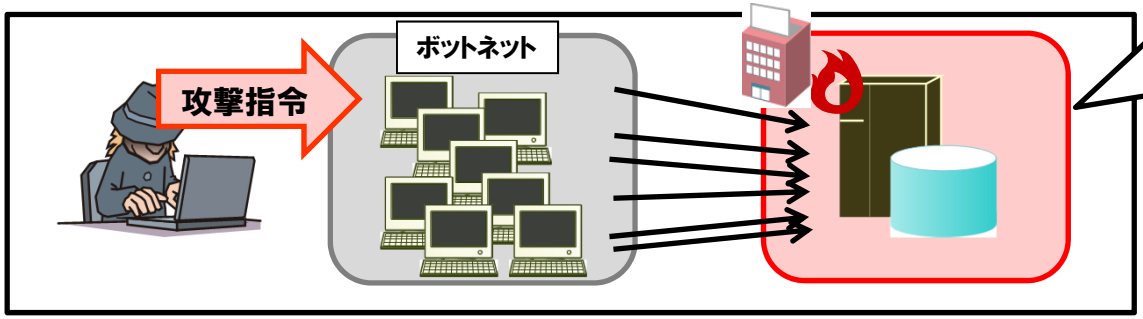
- 金銭に繋がるオンラインバンキング等のアカウント情報等
- 企業の知財や政府の機密等の重要情報



＜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

② 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

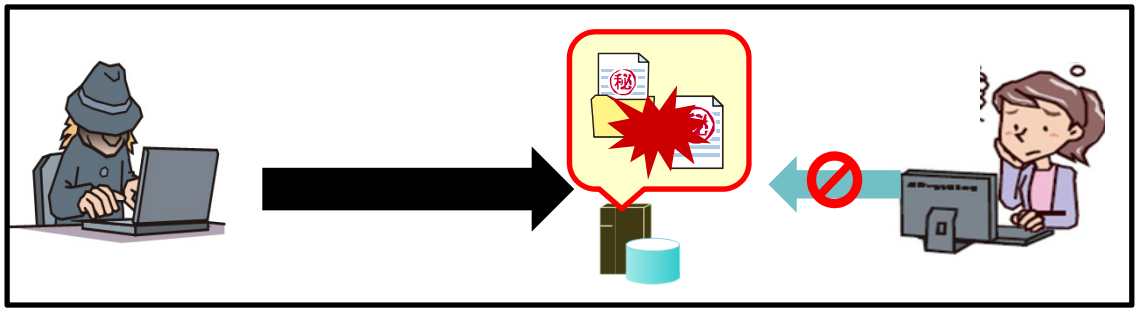


＜攻撃の手法＞
- 攻撃者の制御内にあるボットネットを使用して企業のサーバへ攻撃する
- 攻撃の呼びかけをして標的のサーバを攻撃する

現状のサイバー攻撃を行う攻撃者の目的

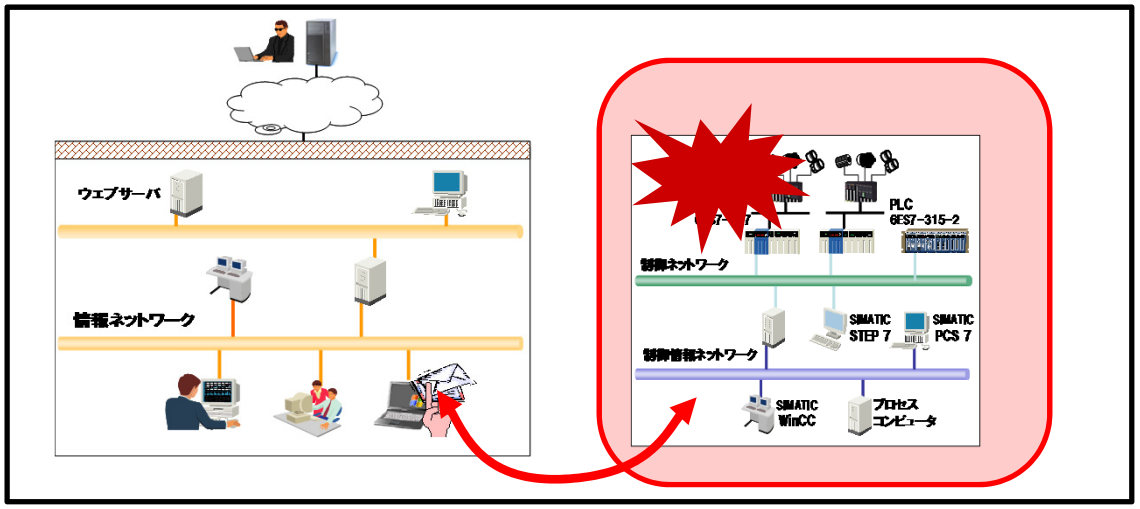
③ 情報破壊

- 組織の重要情報を破壊し運用不能に至らしめる



④ 物理的被害（特にクローズ制御系）

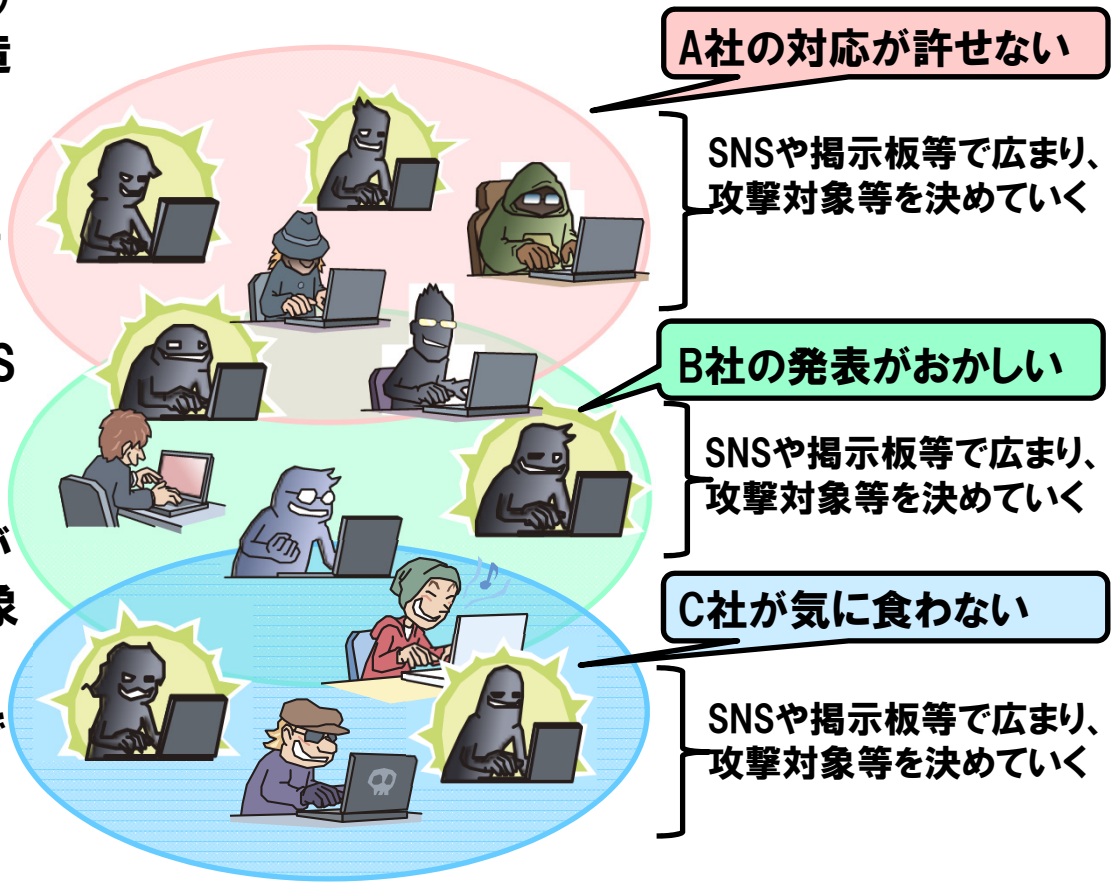
- 制御装置、駆動部等に誤作動を起こさせ装置自体を破壊。



共通思想集団(Hacktivist)による攻撃

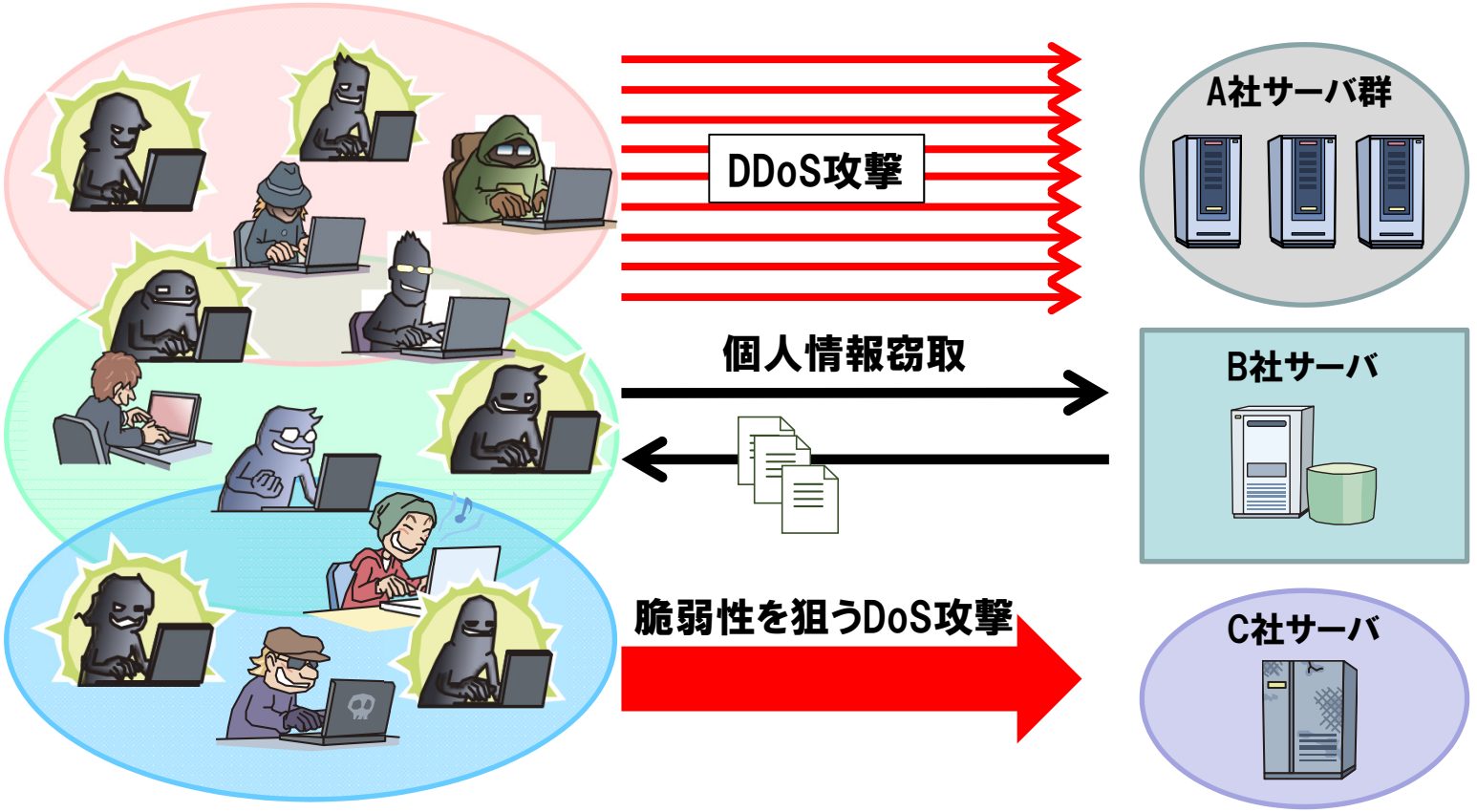
共通思想集団(Hacktivist)とは

- HacktivistはHacker(ハッカー)とActivist(活動家)を併せた造語
- 自分たちの主張を表明するため特定の企業や政府等のサーバへ攻撃を加える
- 同じ主張を持つ人たちが、SNSや掲示板等で扇動し、人数を広めていく
- また、SNS等でサーバに弱点があるなどが共有され、攻撃対象等が決まっていく
- 特定の人間が実施する攻撃ではなく、その主張を持ち、攻撃に賛同する不特定多数による攻撃



共通思想集団(Hacktivist)による攻撃

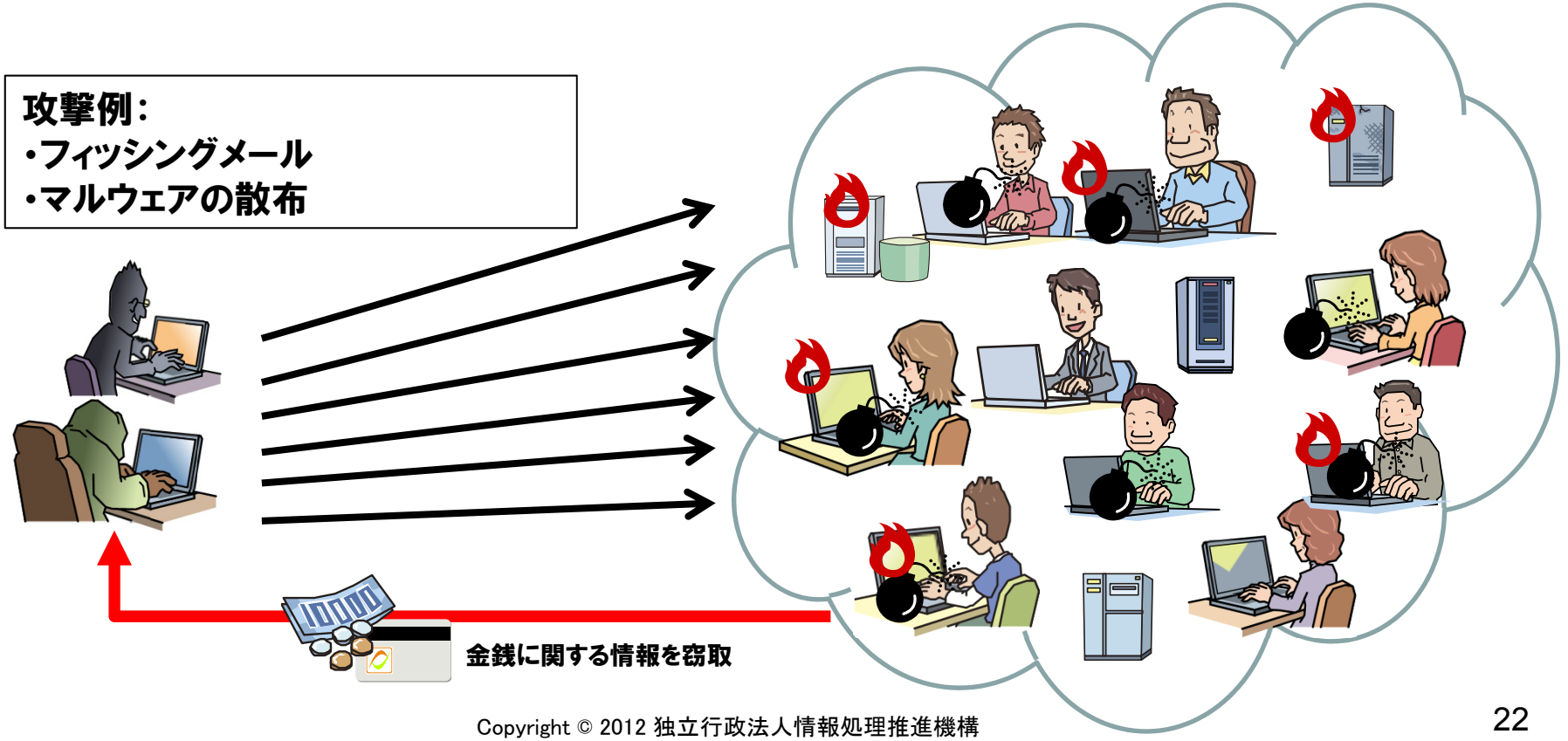
- **不特定多数から一斉に攻撃が行われる**
  - DDoS攻撃や個人情報窃取の攻撃が行われる
    - 脆弱性が残っているサーバに対する攻撃の場合、大量の個人情報漏えいが起こる場合も



詐欺集団による攻撃（従来からの攻撃の1つ）

■ 不特定多数に対して攻撃が行われる

- マルウェアの散布やフィッシングメールの送信など不特定多数に対して大量に攻撃を行い、引っかかってしまった利用者の金銭情報を窃取する。
- 利用者に対してだけではなく、サーバへの攻撃も行われる



攻撃者が使える環境について

- **攻撃ツール等が取引されている**
  - 攻撃ツール等が取引され、特別な知識や技術がなくても、攻撃を行うことが可能。
  - それほど高くない値段で取引が行われている場合もあると言われている。
- **フリーの攻撃ツールが公開されている**
  - フリーで攻撃ツールが公開されており、それを利用して攻撃を行うことで、それほど技術的に詳しくない攻撃者でも攻撃が可能である。
- **攻撃者は検査ツールも悪用している**
  - 検査ツールではあるが、実際の攻撃にも悪用できるような検査ツールも公開されている。（例：Metasploit）

攻撃者像まとめ

IPA

- **攻撃者は様々な目的があり様々な手法を使ってくる**
  - 諜報活動をする者：
    - 目的：情報窃取
    - 手法：標的型メール等
  - 共通思想集団（Hacktivist）：
    - 目的：独自の思想
    - 手法：DDoS等
  - 詐欺集団
    - 目的：金銭窃取
    - 手法：フィッシングメール・マルウェア散布、サーバへの攻撃
- **攻撃が行いやすい環境**
  - 知識がなくても、攻撃ツールを入手することが可能。
  - フリーで使える攻撃ツール・検査ツールもある。

⇨ **守る方もMetasploitやNessus等の検査ツールを使用して システムに弱点がないか検査することも重要。**

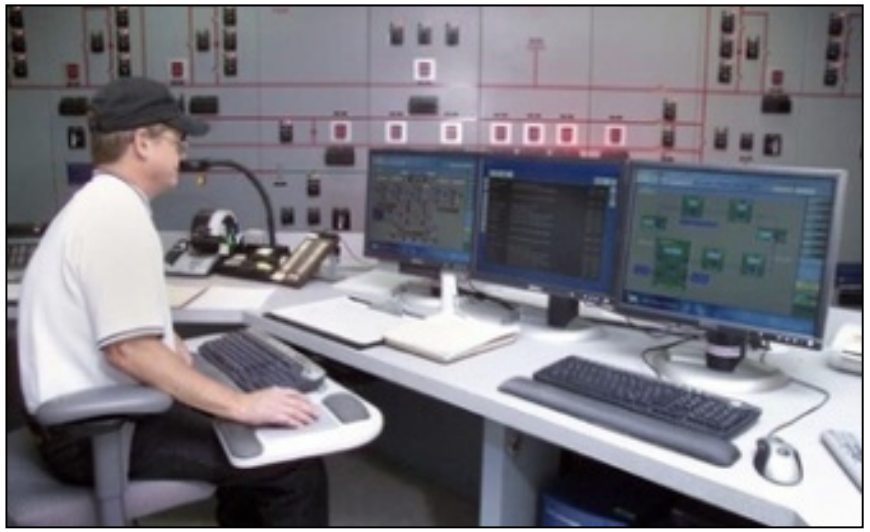
目次

1. サイバー攻撃とは
2. 近年のサイバー攻撃の分析
3. **制御システムの現状**
4. 制御システムへのサイバー攻撃例と課題
5. 社会インフラを支える制御システムに向けて

制御システムとは

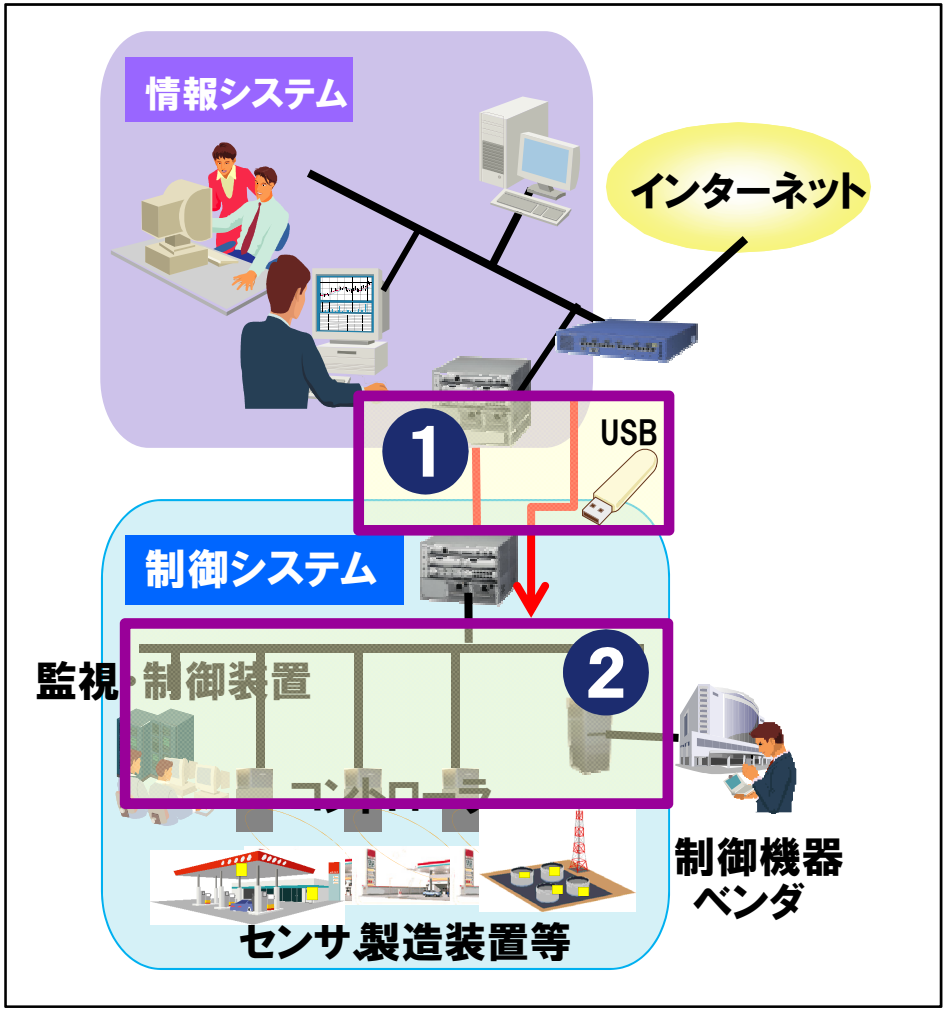
位置づけ

- 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

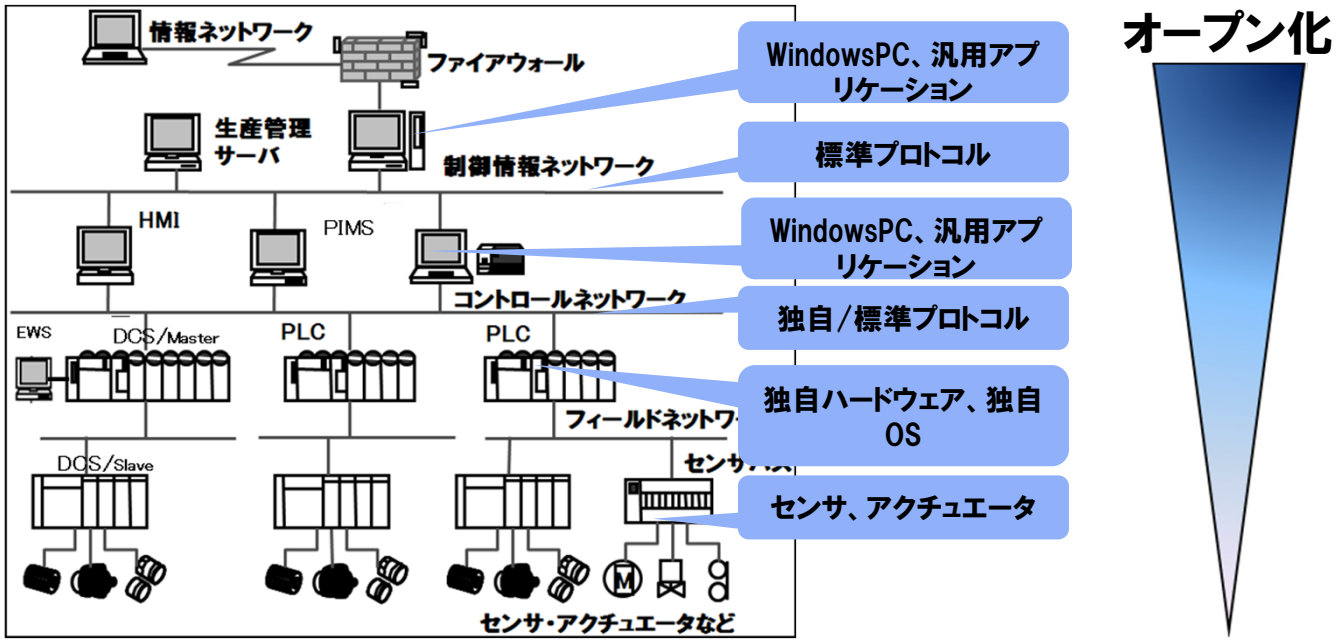
＜最近＞
ネットワークやUSBメモリ等で
繋がるようになった

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



- 例：プラント設備（生産ライン制御等）におけるオープン化の割合
  - 外部ネットワークとの接続　36.8%
  - 設備内のOSの利用状況　Windows：88.9% UNIX系：13.7%

経済産業省　サイバーセキュリティと経済　研究会　中間とりまとめ（案）：
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/report01.html

制御機器はインターネットに公開されていない？

- **制御機器がインターネットに公開される場合がある**
  - リモート管理の需要
    - 機器の状態監視
    - 処理の実行状況監視
    - など
- **インターネットに公開されている制御機器の確認**
  - SHODAN（ショーダン） http://www.shodanhq.com/

インターネットに公開されている機器検索を対象とした検索エンジン。
ウェブサーバ以外も検索対象としているため、インターネットに公開されていれば制御機器も検索結果に表示される。

知らぬ間に制御機器が公開状態になっている可能性も

SHODAN

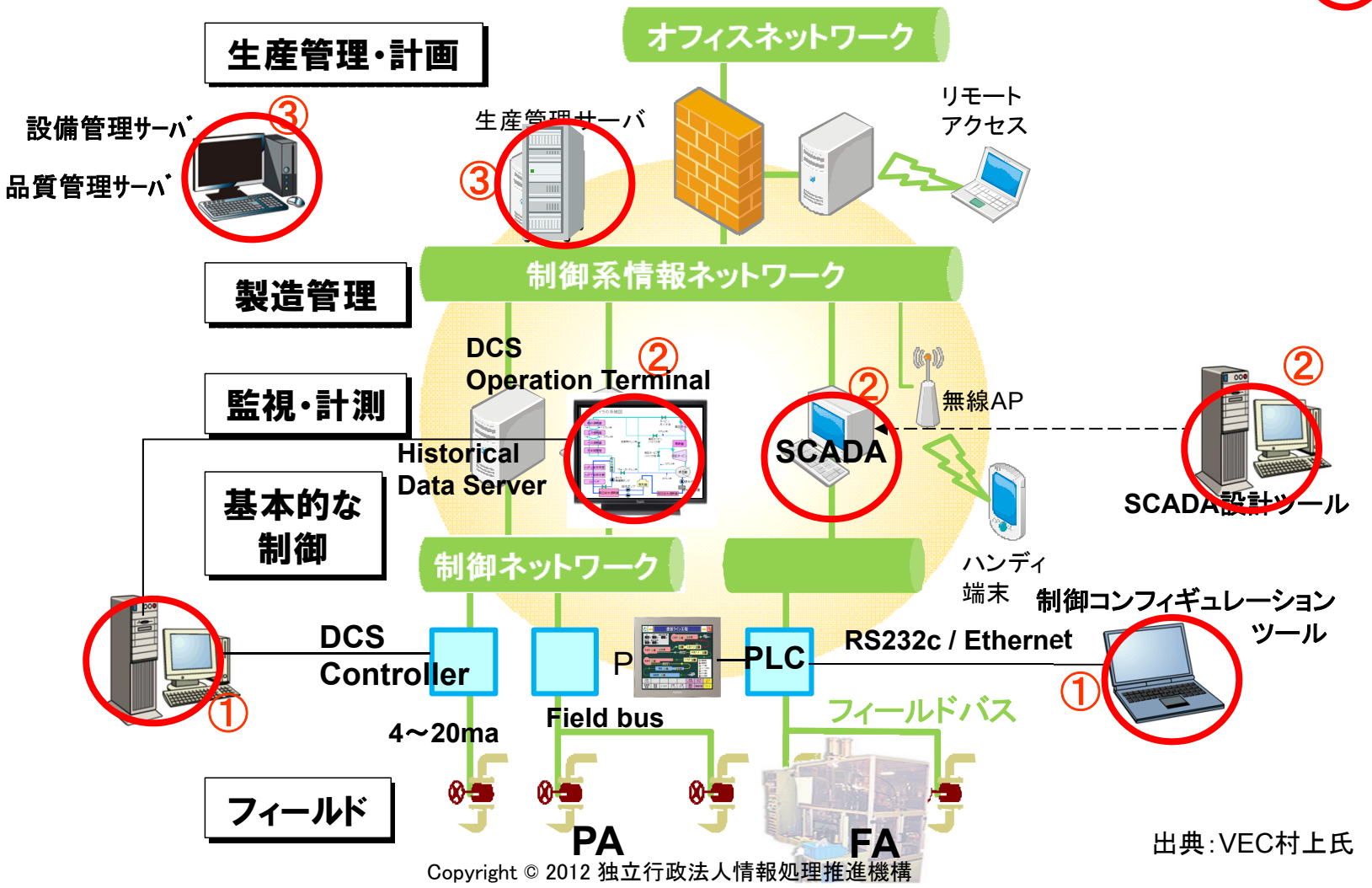
目次

1. サイバー攻撃とは
2. 近年のサイバー攻撃の分析
3. 制御システムの現状
4. **制御システムへのサイバー攻撃例と課題**
5. 社会インフラを支える制御システムに向けて

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

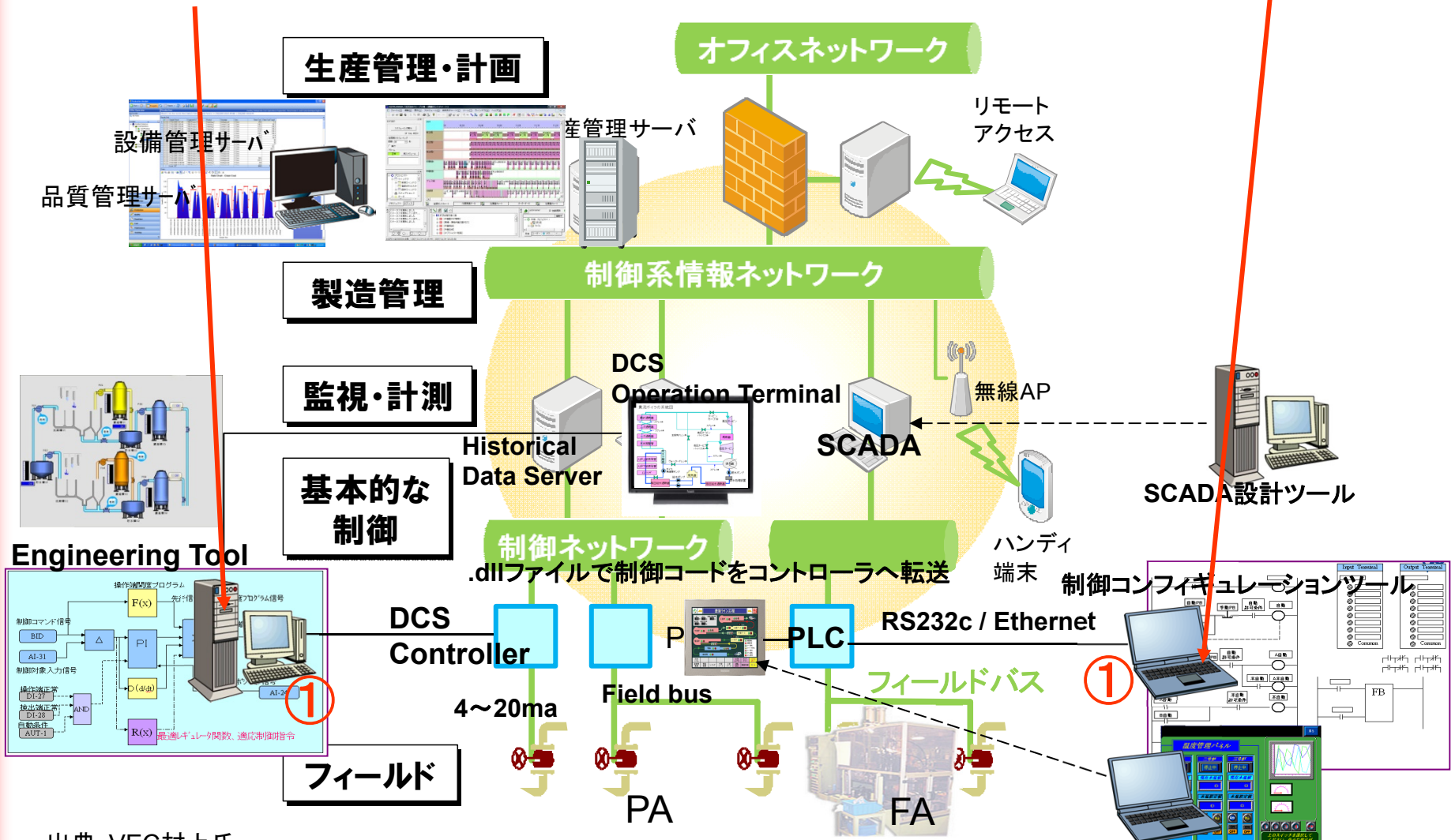
攻撃ターゲット⇒ ○



出典:VEC村上氏

攻撃パターン例：データすり替え

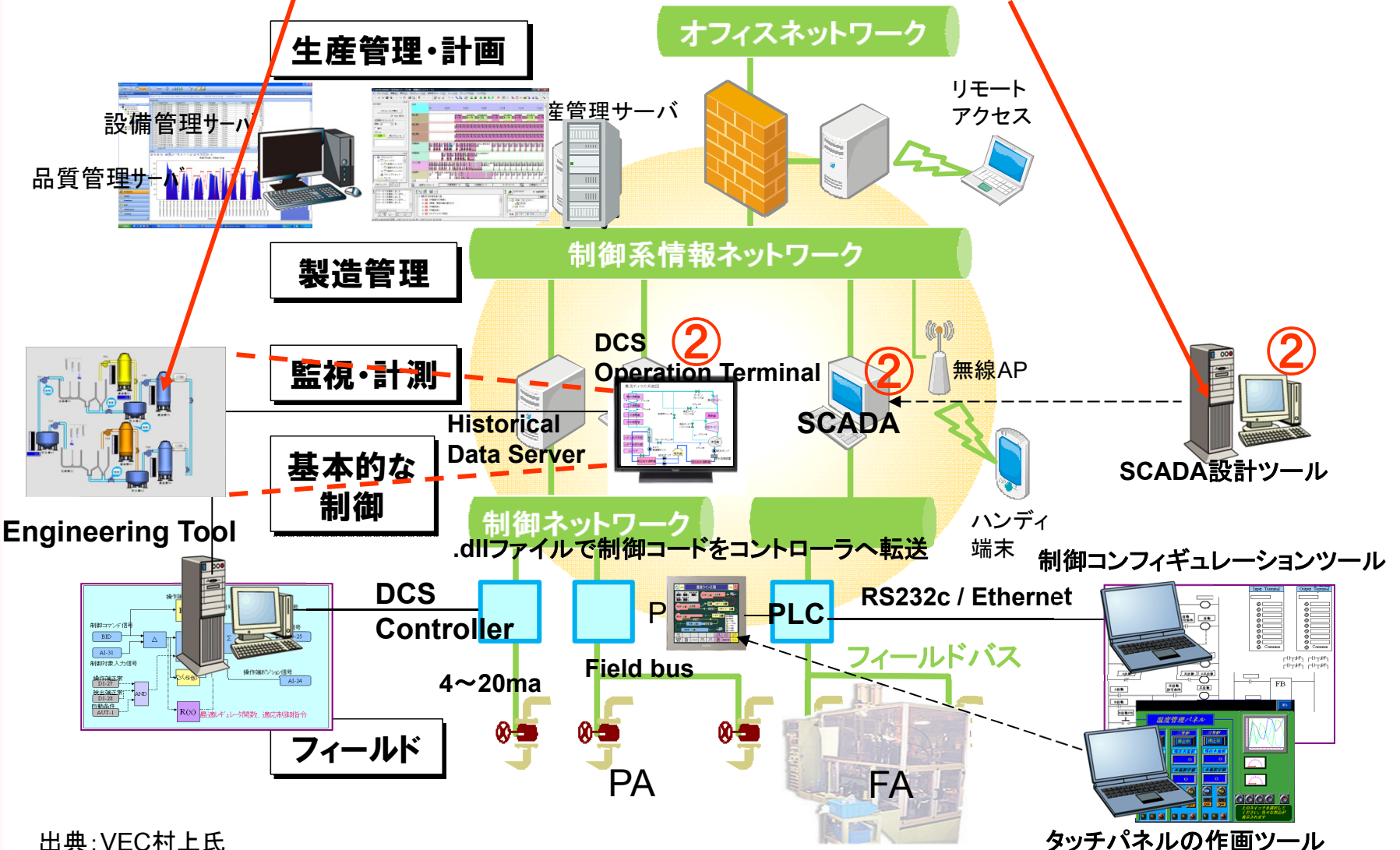
ファンクションブロックのパラメータやシーケンスロジック条件を書き換えたものとすり替える。



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

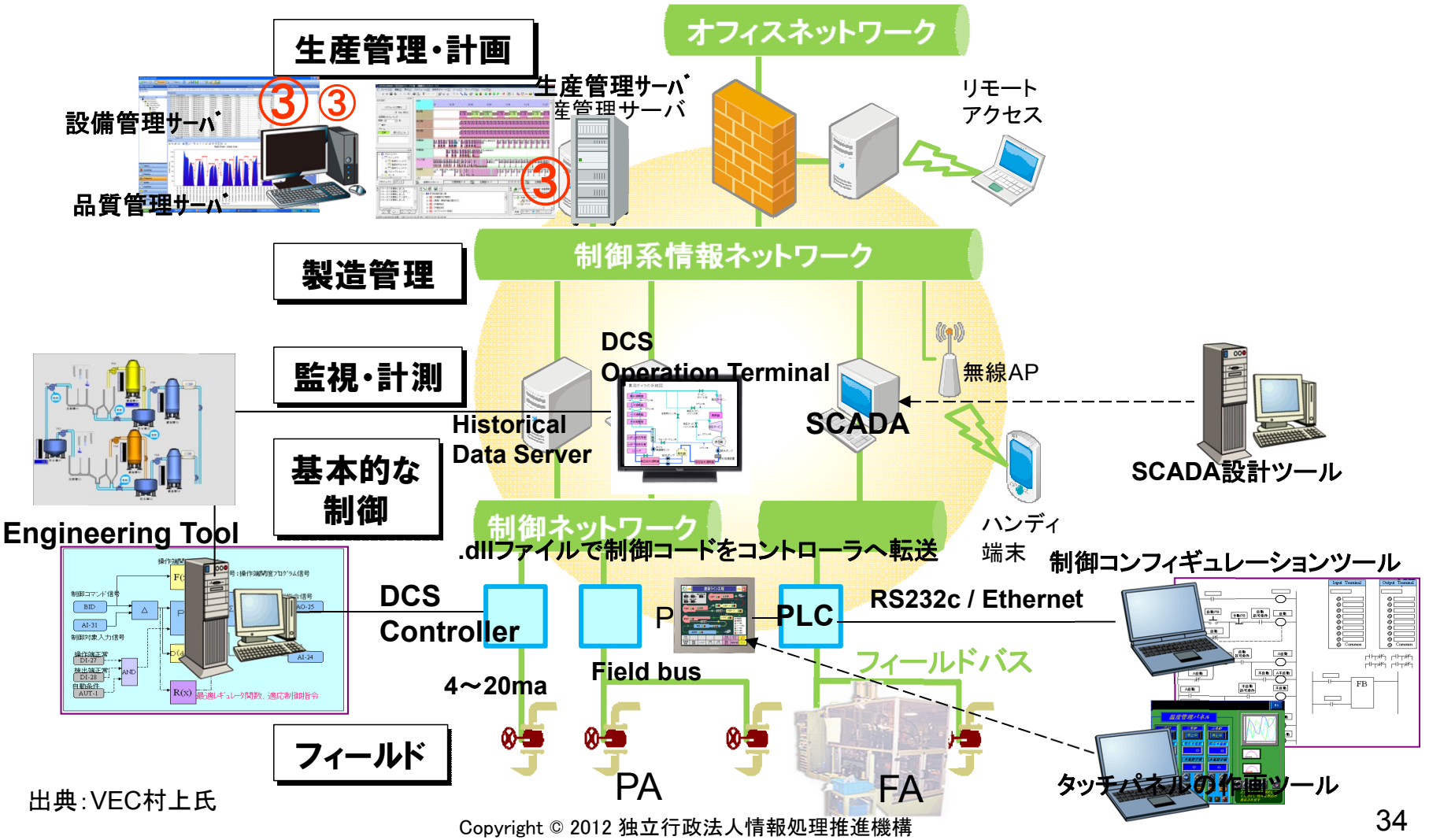
画面は正常で表示し、異常コードをコントローラへ送る



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。



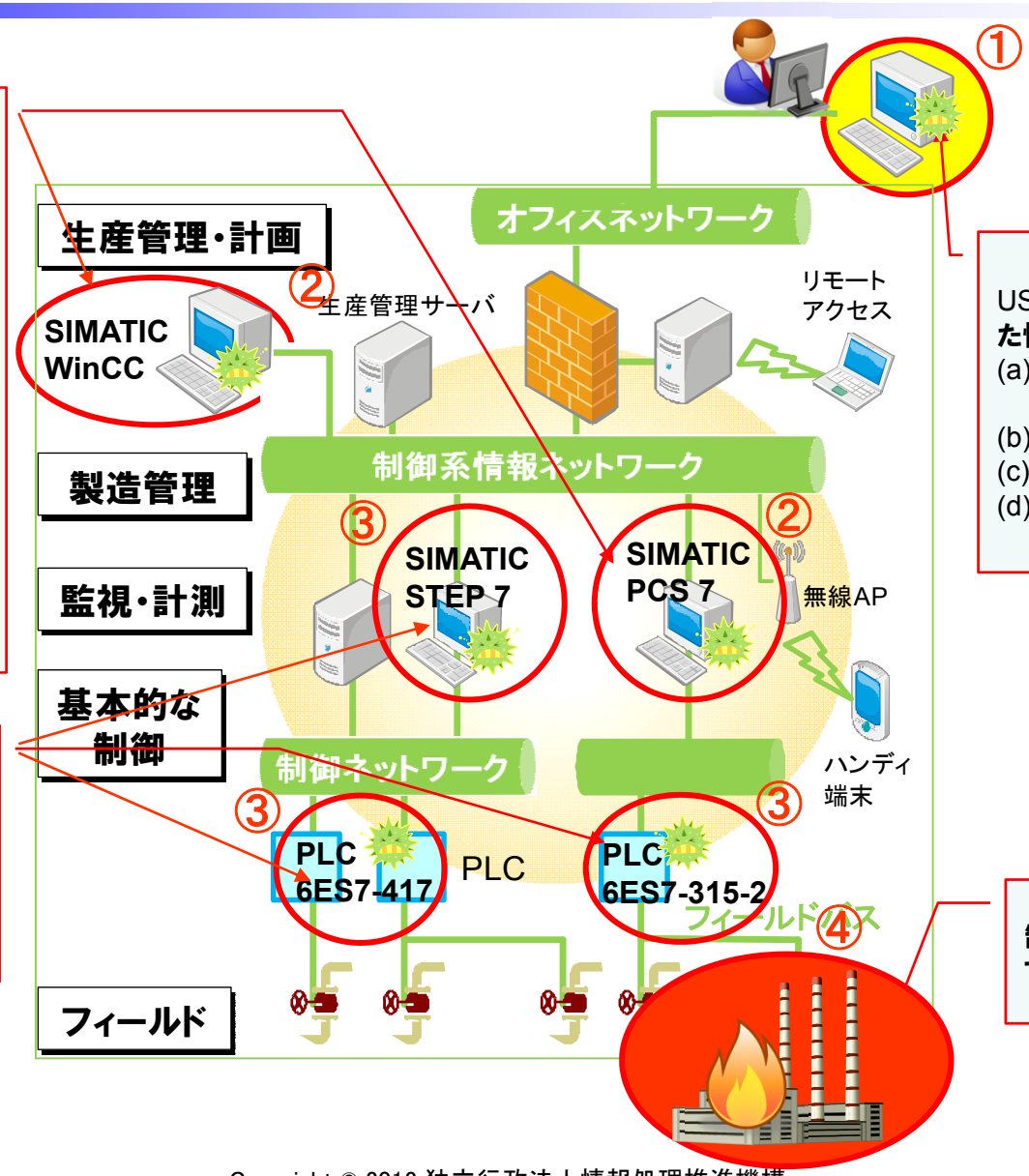
出典：VEC村上氏

Stuxnet攻撃例

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。

【課題４：攻撃者の関心が増大】

社会混乱を目的とした攻撃が顕在化しつつある。

	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

1. サイバー攻撃とは
2. 近年のサイバー攻撃の分析
3. 制御システムの現状
4. 制御システムへのサイバー攻撃例と課題
5. **社会インフラを支える制御システムに向けて**

制御システムのセキュリティ事件の例

契約警備員による内部犯行

- 発生した国
  - ◇米国
- 業種
  - ◇ビル管理
- 原因
  - ◇内部者によるシステム侵入
- 想定被害
  - ◇ビルの空調を止める
  - ◇患者の個人情報を窃取

2009年夏、米国のダラスにある病院Carrell Clinicの契約警備員が病院内のPCにマルウェアを仕込み、病院にある患者の情報や暖房、換気、空調(HVAC)システム等の情報をインターネット上にアップロードしていた。また、HVACシステムのアラームが停止状態になっていた。更に、DDoS攻撃を呼びかけていた。

Source: http://scan.netsecurity.ne.jp/article/2009/08/04/24098.html

制御システムのセキュリティ事件の例

信号機に対するハッキング

- 発生した国
  - ◇米国
- 業種
  - ◇道路管理
- 原因
  - ◇システムが脆弱な状態
- 想定被害
  - ◇道路状況の混乱

写真：The Telegraph
http://www.telegraph.co.uk/

2009年1月、米国の複数の州における信号機（交通メッセージ表示）が「ゾンビ注意（ZOMBIES AHEAD）」に変更された。この例はいたずらだが、原因はシステムにおけるパスワードをデフォルトのままにしていたり、本来ロックしておかなければならない機能をロックしていなかったりシステムが脆弱な状態にあったため、いたずらに利用された。

Source: Los Angels Times
http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html

制御システムのセキュリティ事件の例

線路のトラックポイントに対するハッキング

- 発生した国
  - ◇ポーランド
- 業種
  - ◇鉄道
- 被害
  - ◇12人のけが人

2008年、14歳の少年がテレビのコントローラを改造し、ポーランドの鉄道のトラックポイントに対してハッキングを行い、4つの車両を脱線させた。その結果、12人のけが人を出した。
鉄道のシステムに対しては、鉄道会社へハッキングを行い、そのシステムを勉強していた。

The Register
http://www.theregister.co.uk/2008/01/11/tram_hack/

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

➢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

「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
- **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＞

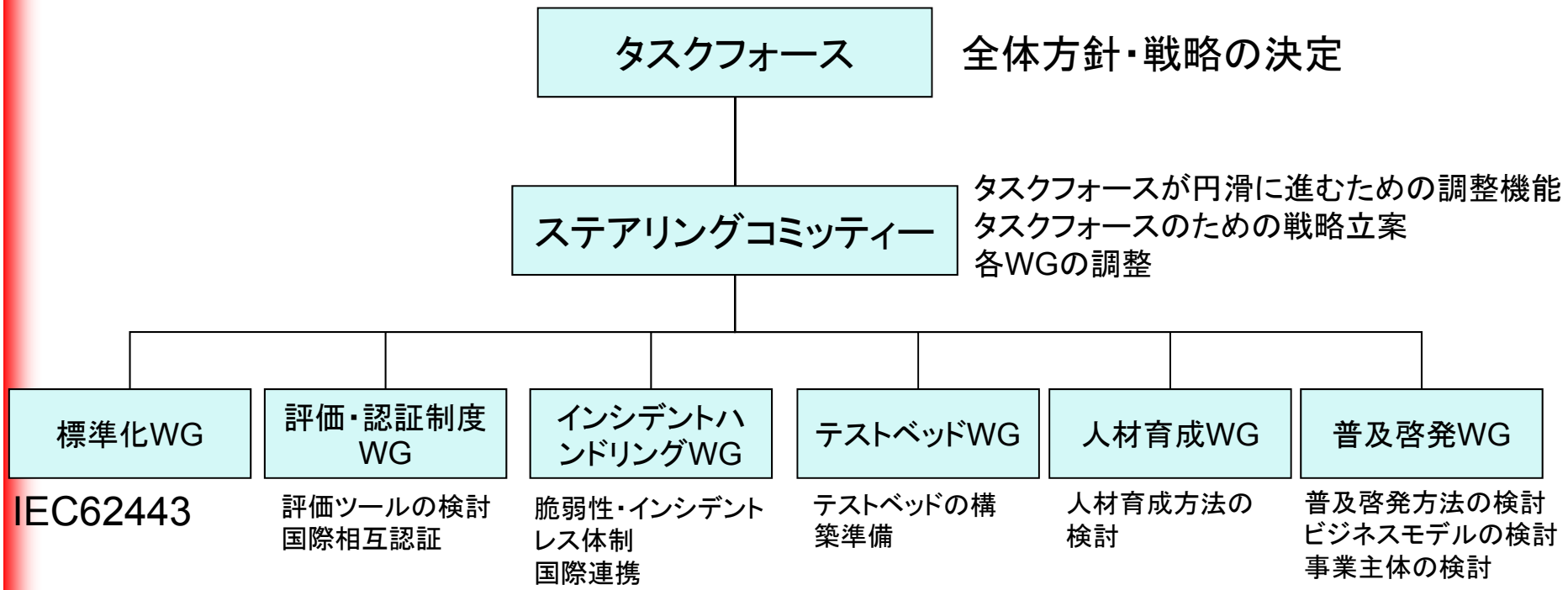
- 標準化WG (IPA)
- 評価・認証制度WG (IPA)
- インシデントハンドリングWG
- テストベッドWG
- 人材育成WG
- 普及啓発WG

ICS：Industrial Control Systems

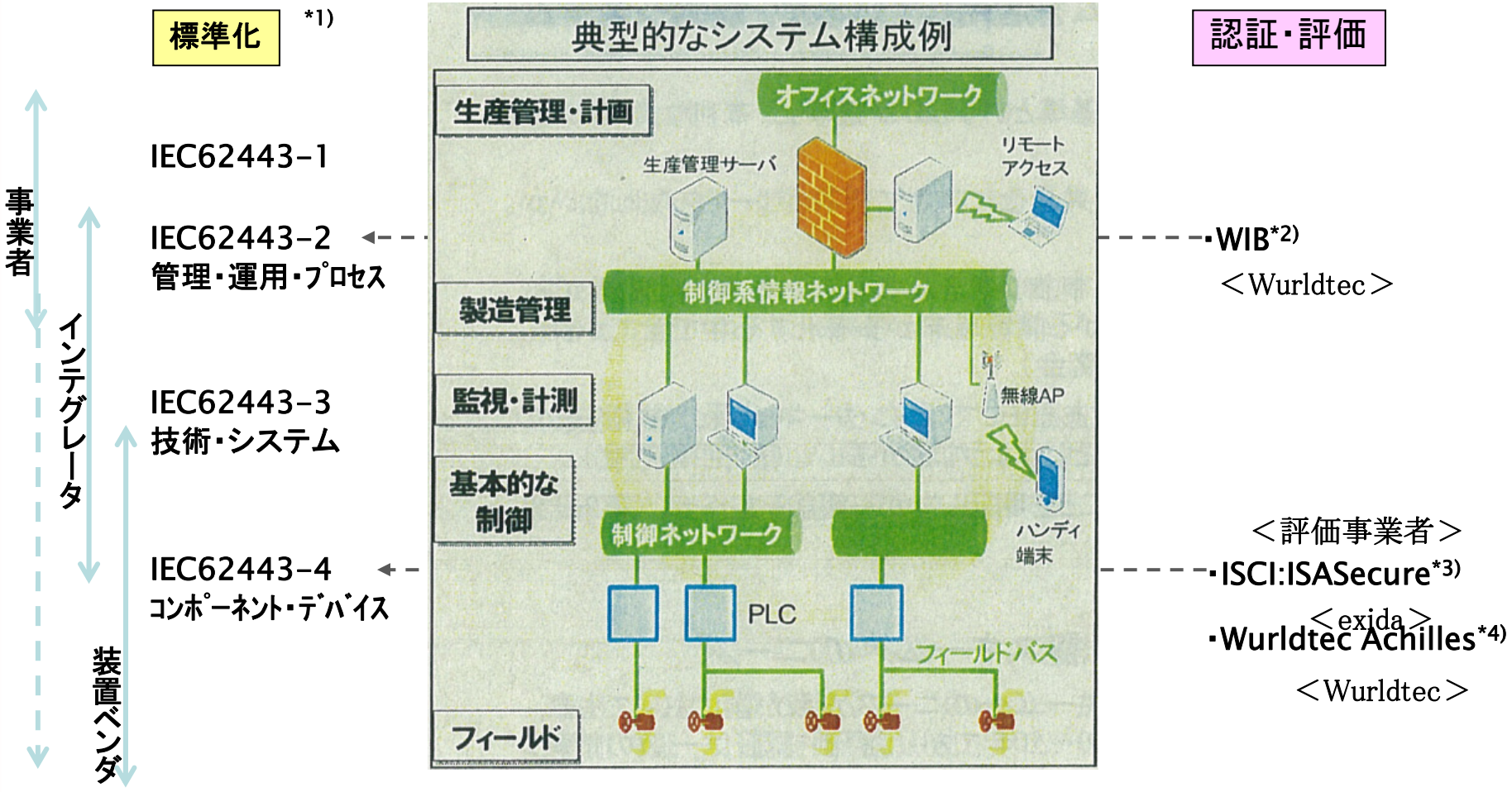
制御システムセキュリティ検討タスクフォース

IPA

- ステアリングコミッティが全体戦略の策定、各WGの調整作業に専念。
- 標準化、評価・認証制度、テストベッド、人材育成、普及啓発については別途WGにて検討。

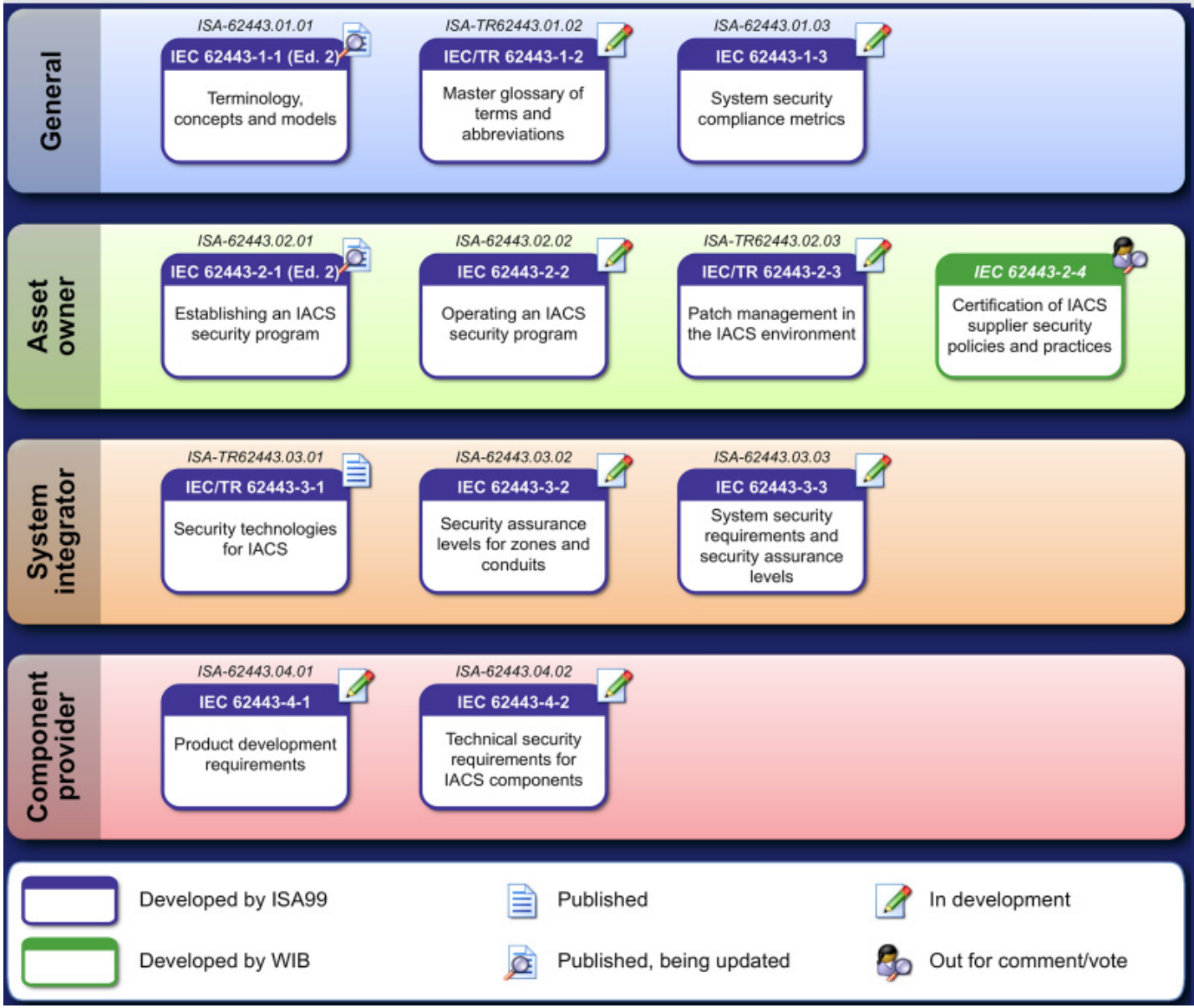


制御システム分野における標準と認証･評価の位置づけ



*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（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。

IEC 62443, Security for industrial automation and control systems – Network and system security



The IEC 62443 standards form four sub-series, aligned with the three previously identified classes of users.

The 1st sub-series provides general information relevant to the other three subseries.

※International Electrotechnical Commission

＜制御システムセキュリティ＞
IEC62443のご紹介

IEC62443規格化の状況

(2012年2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	ー 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	ー 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

IEC62443-2-1の概要
Establishing an IACS* security program

- 概要
  ◇CSMS(Cyber Security Management System)と呼称
  　ISMS(ISO27001)のIACS版と考えられ、ほぼ同様の要求事項。
- CSMSの要件:全127要件
  ◇リスク分析 (Risk analysis)
  　・リスクの識別、分類、評価等の要件
  ◇リスク対応 (Addressing risk with the CSMS)
  　・セキュリティ基本方針、組織、対策、実装に関する要件
  ◇モニタリングと改善 (Monitoring and improving the CSMS)
  　・適合性 (監査実施)、監査結果評価による改善・維持等の要件

*IACS: Industrial Automation and Control Systems

リスク分析 (Risk analysis)

- Risk identification, classification and assessment

◇リスク識別、分類、及び評価

- リスク評価方法を選択
- IACSの識別
- IACSの全ライフサイクルでリスク評価
- リスク評価の文書化
- 脆弱性評価記録の維持

リスク対応
（Addressing risk with the CSMS ）

- Security policy, organization, and awareness
  ◇CSMSの対象範囲の定義
  ◇管理層を含むセキュリティ組織の確立・責任の定義
  ◇スタッフのトレーニングとセキュリティ認識
  ◇Business continuity plan（回復対象、チーム等）
  ◇セキュリティポリシーと手順
- Selected security countermeasures
  ◇要員や物理的環境的セキュリティ、アカウント制御
- Implementation
  ◇リスク管理と実行、システム開発とメンテナンス
- ◇情報・文書管理、インシデント対応計画

モニタリングと改善
(Monitoring and improving the CSMS)

- 適合性評価(Conformance)
  - ・監査プロセスの規定
  - ・定期的なIACS監査を実施
  - ・適合性測定法を確立
  - ・不適合時の罰則の定義
  - ・監査人の能力を保証
- CSMSのレビュー・維持改善
  - ・CSMSの管理、実行組織の割り当て
  - ・定期的なCSMS評価
  - ・業界のCSMS戦略を監視、評価

ISMSとCSMSの主な相違点

項　目		ISMS	CSMS
要員のトレーニング	トレーニング計画策定	○	○
	トレーニングの実施	○	○
	トレーニング結果の維持	○	○
	計画の妥当性の証明	△	○
	トレーニング計画の改善	△	○
内部監査	監査プロセスの規定	○	○
	監査人の能力保証	○	○
	不適合時の罰則	△	○

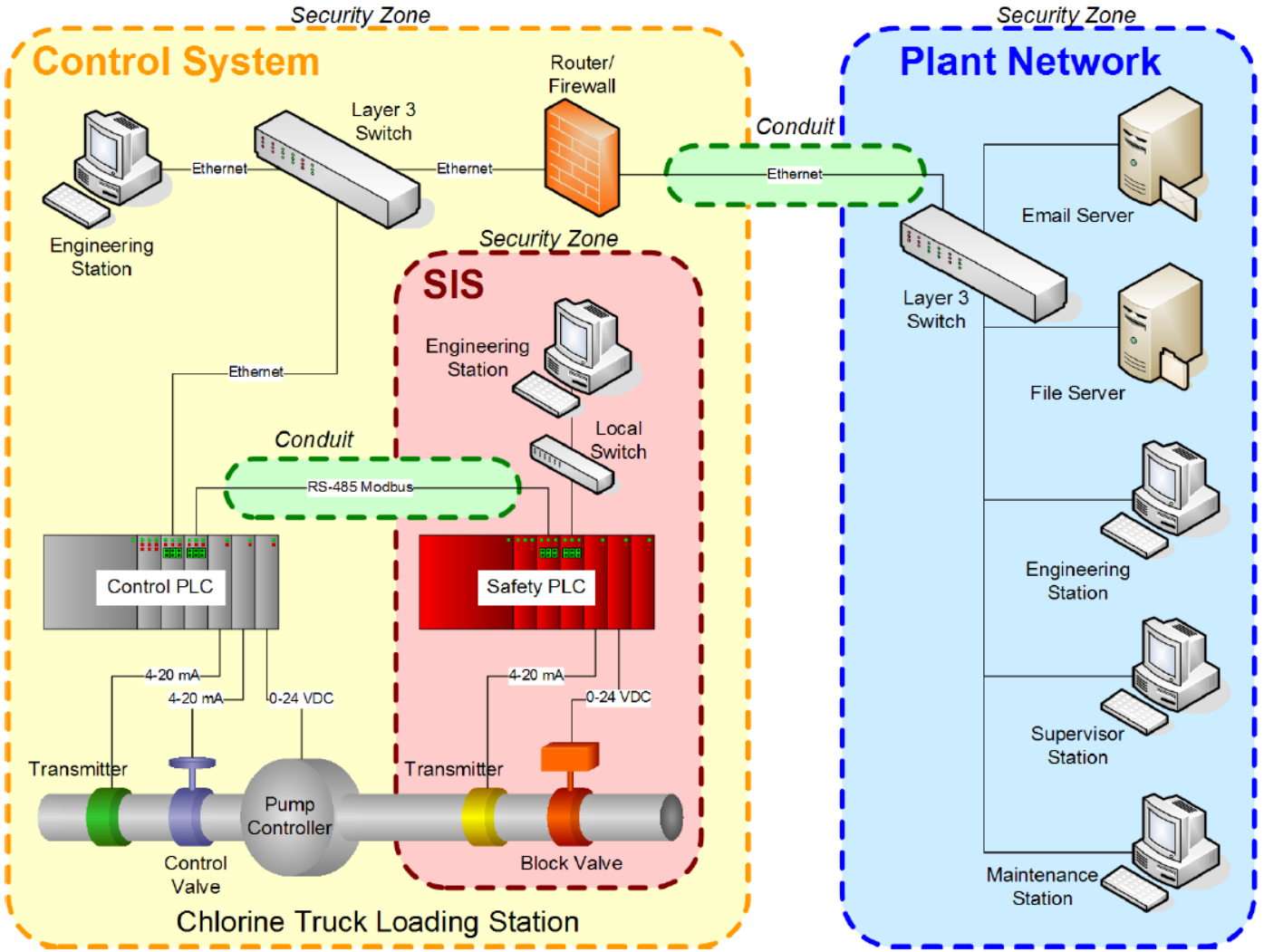
○：shall、△：should

IEC62443-3-3 (案) の概要
System security requirements and security ssurance levels

IPA

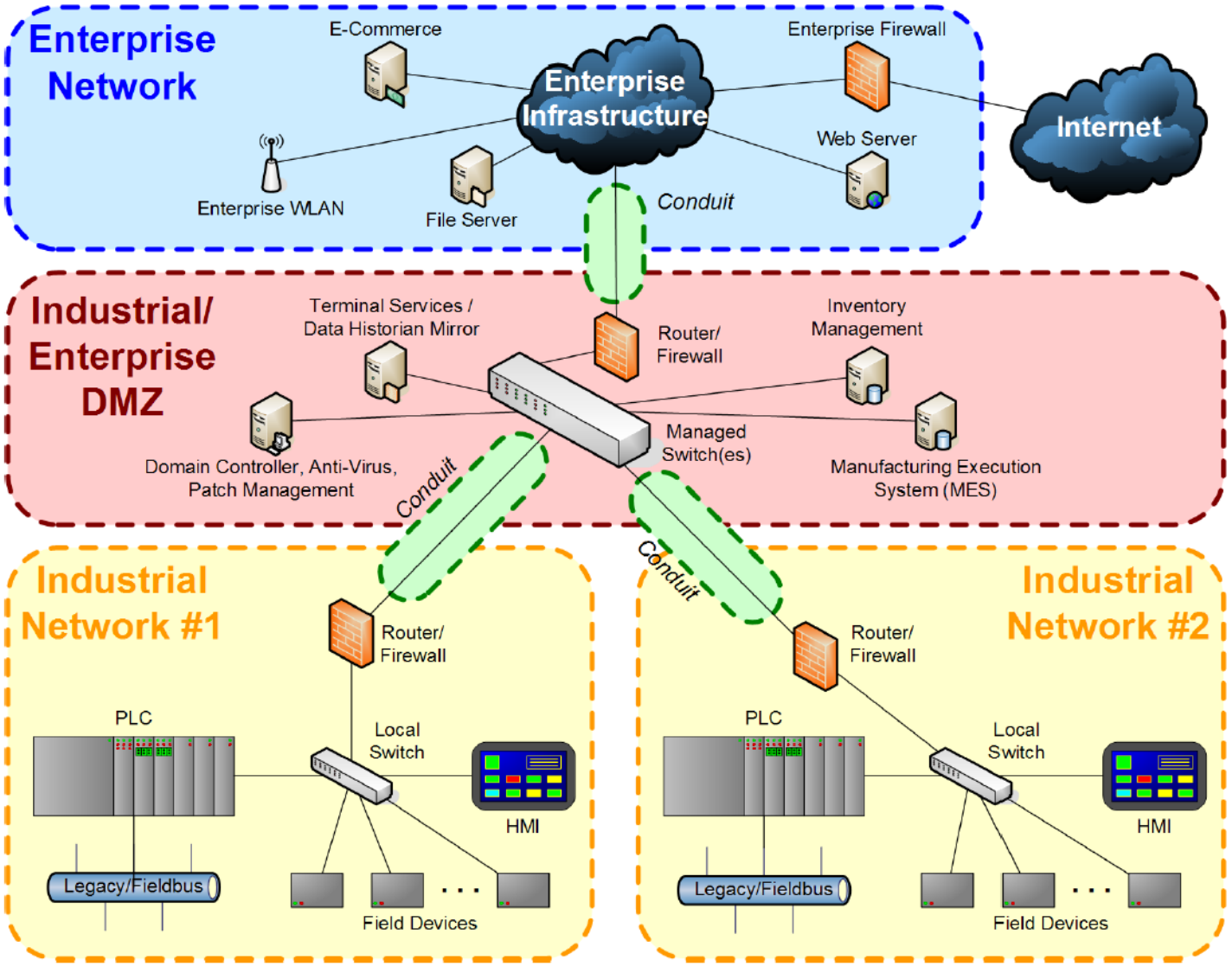
- 概要
  - ◇扱う人、プロセス、デバイスの識別・認証、
    及びそれらのアクセス制御 (証跡記録) の要件を規定。
    扱うデータの完全性・機密性、資源の可用性等の要件も含む。
  - ◇7種の要件に4段階のセキュリティ保証レベルSAL (Security assurance levels) を規程。
- システムセキュリティ要件について：全94要件 (7種の大項目)
  - ◇識別及び認証 (Identification and authentication control)
    - ・人、プロセス、デバイスの認証、パスワード強度等の要件
  - ◇利用制御 (Use control)
    - ・適切な権限付与、証跡記録、ワイヤレスアクセス制御
  - ◇データの完全性・機密性、資源の可用性要件
    - ・通信完全性、暗号の利用、DoS対策やバックアップ等の要件

産業システムの構成例(１)



産業システムの構成例(２)

階層的な製造システム



識別及び認証
(Identification and authentication control)

- 人、プロセス、デバイスの認証
- アカウント管理
- パスワード認証の強度
- 公開鍵認証の強度
- デバイス認証

利用制御
(Use control)

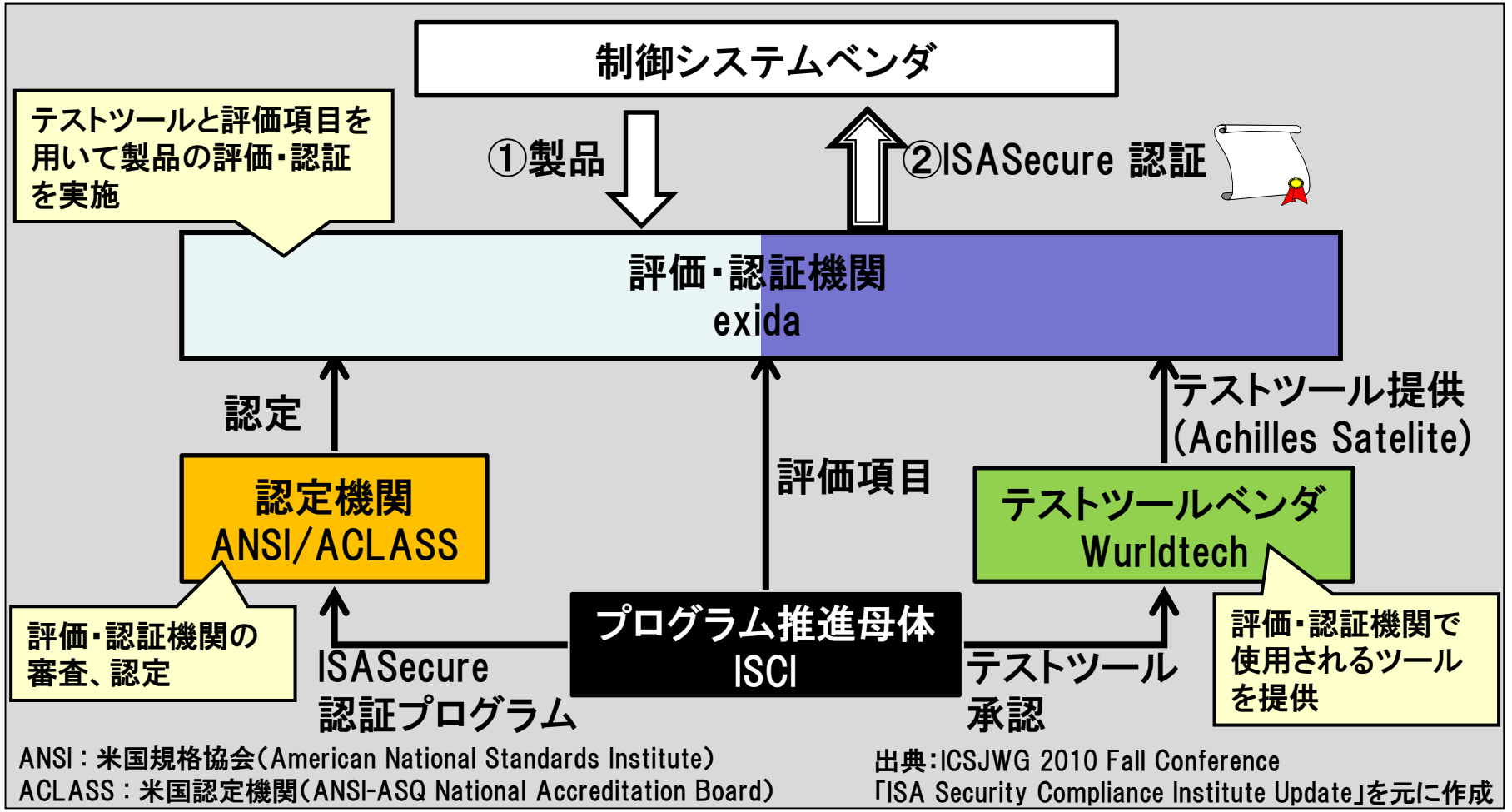
- 適切な権限付与
- ワイヤレスアクセス制限
- 監査可能なイベント
- タイムスタンプ
- 監査情報の保護
- 否認防止

データの完全性・機密性、資源の可用性要件

- データの完全性
  - ◇通信完全性
  - ◇セキュリティ機能の検証
  - ◇入力正当化
  - ◇セッション完全性
- データの機密性
  - ◇情報永続性
  - ◇情報機密性
  - ◇暗号の使用
- 資源の可用性
  - ◇サービス妨害攻撃からの保護
  - ◇バックアップ
  - ◇回復と再構成

ISASecure認証プログラム

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



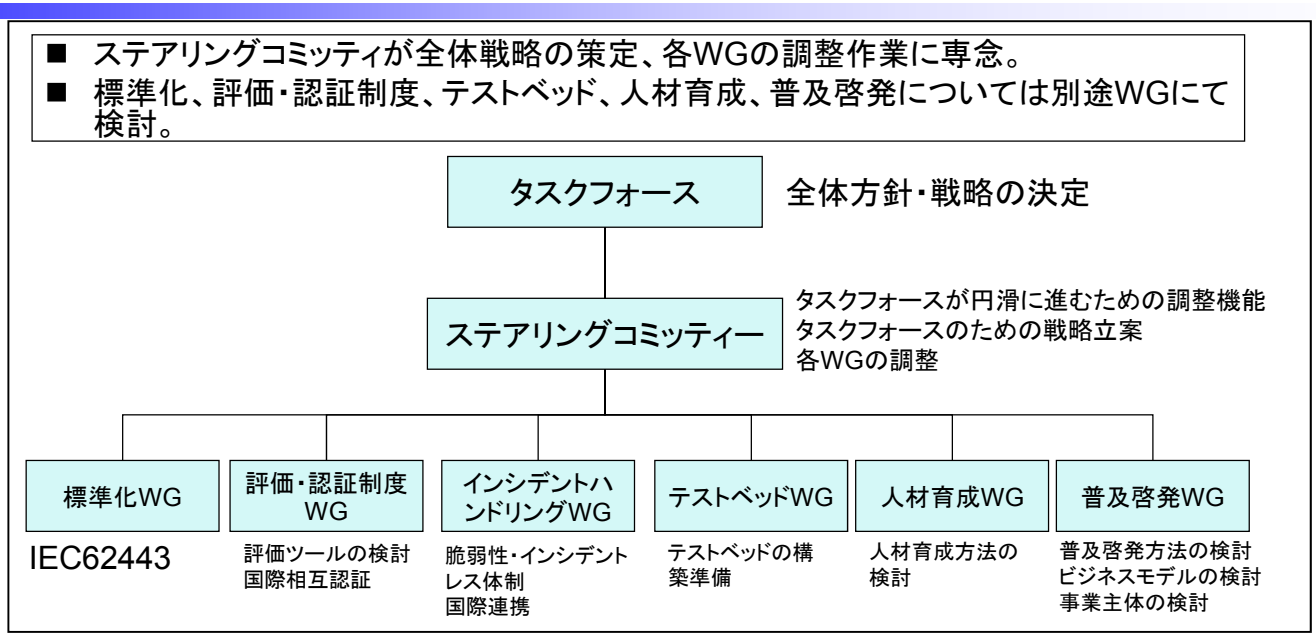
ANSI：米国規格協会(American National Standards Institute)
ACLASS：米国認定機関(ANSI-ASQ National Accreditation Board)

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

制御システムセキュリティ検討タスクフォース

IPA

■ ステアリングコミッティが全体戦略の策定、各WGの調整作業に専念。
■ 標準化、評価・認証制度、テストベッド、人材育成、普及啓発については別途WGにて検討。

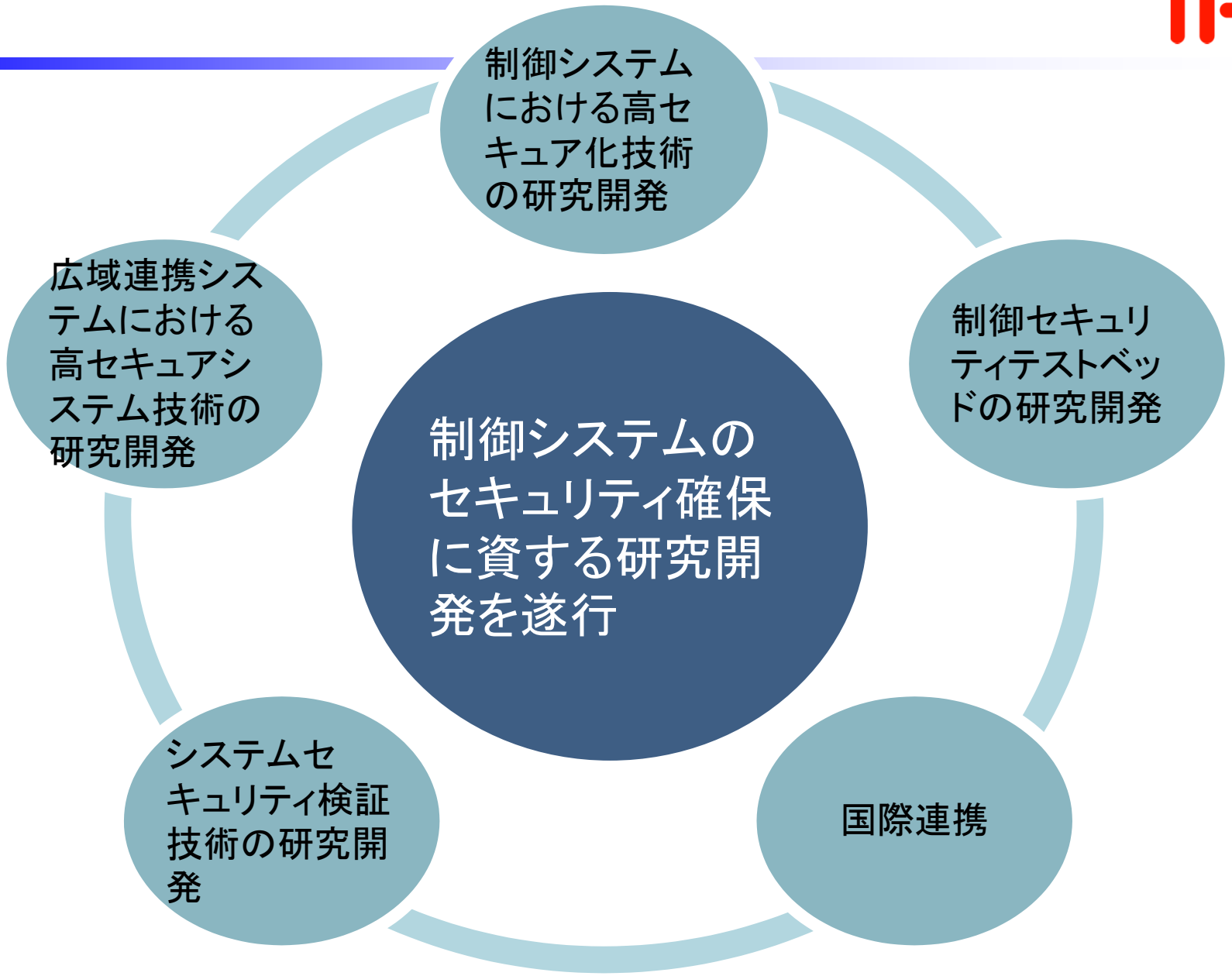


技術研究組合制御システムセキュリティセンター

技術研究組合
制御システムセキュリティセンター
－ CSSC －

組合の概要

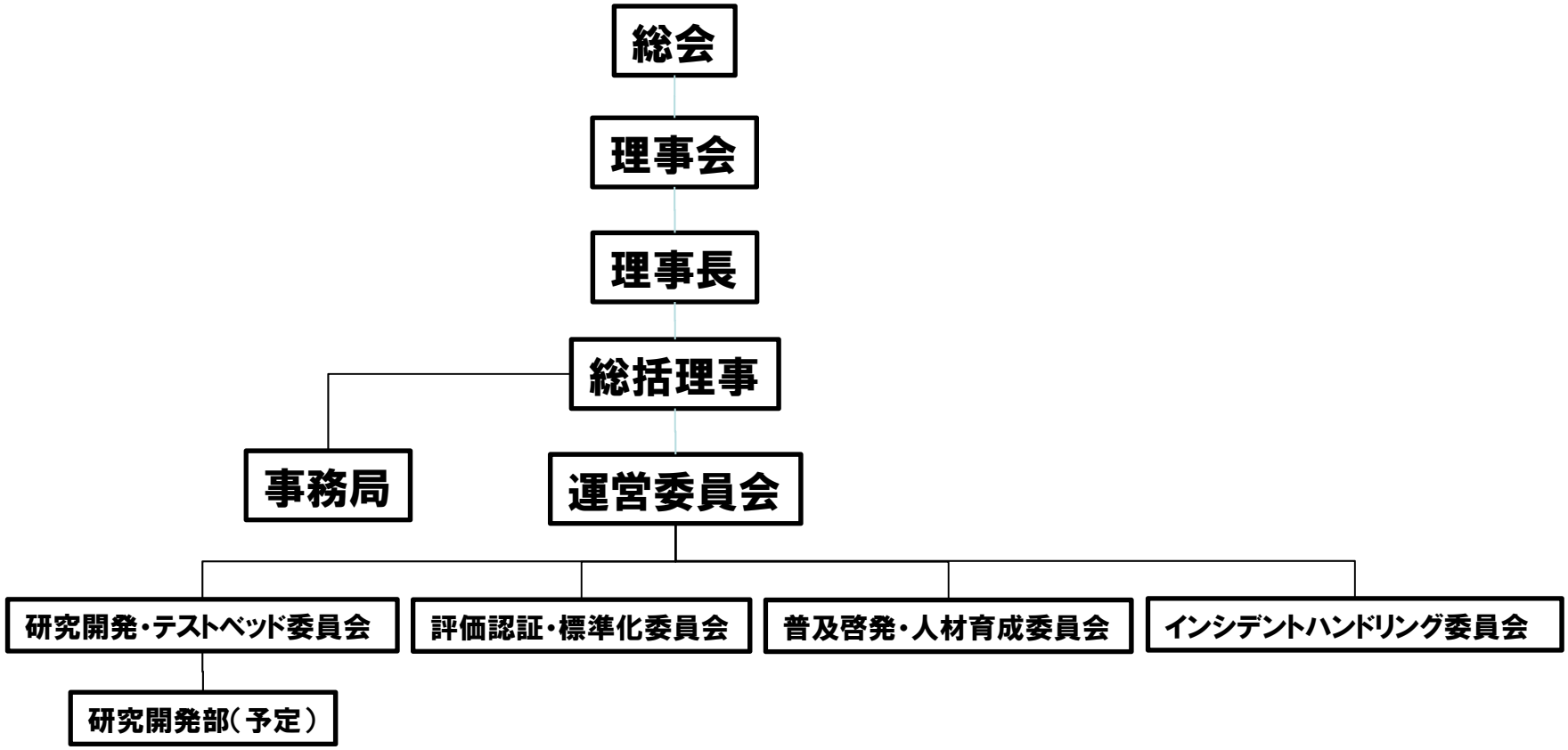
活動目的とアクティビティ



組織と組合員

- 住所
  - 本部：
    東京都江東区青海二丁目3番26号　独立行政法人産業技術総研究所臨海副都心センター内
  - テストベッド構築予定地：
    宮城県多賀城市桜木三丁目4番1号　みやぎ復興パーク内
- 設立時組合員
  独立行政法人産業技術総合研究所、株式会社東芝、株式会社日立製作所、
  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、
  株式会社山武、横河電機株式会社
- 設立後の組合員
  独立行政法人情報処理推進機構、富士電機株式会社
- その他連携予定
  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、石油連盟　他

組織体制



活動の方向性

0. サイバーセキュリティテストベッド

平成24年度中に、宮城県多賀城市（宮城復興パーク）とお台場（産総研臨海副都心センター）を接続して構築

1．システムセキュリティ検証

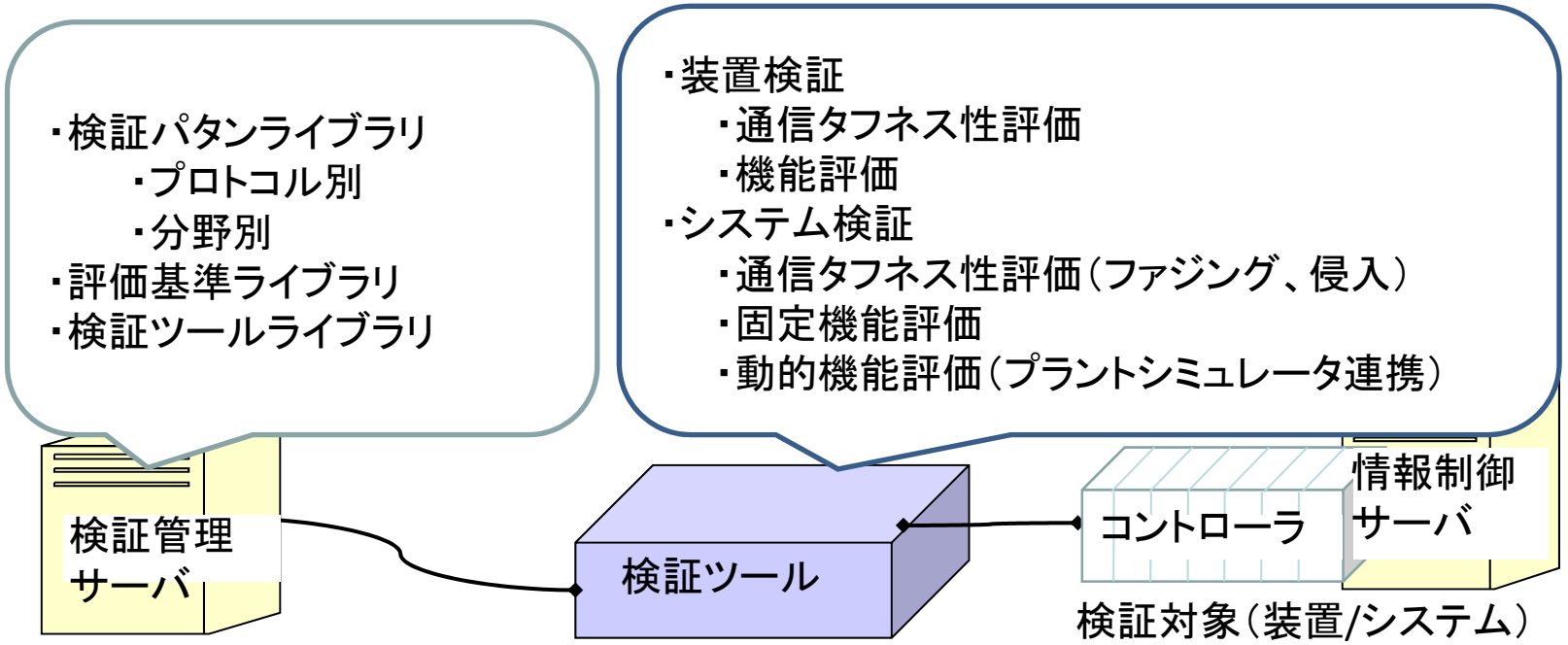
■狙う効果

システム・コンポーネントに対する最新セキュリティ検証ツールの提供

・コンポーネント、システムのセキュリティ検証ツール開発/共通利用

・セキュリティ検証パタンの蓄積と共有

・相互接続の検証

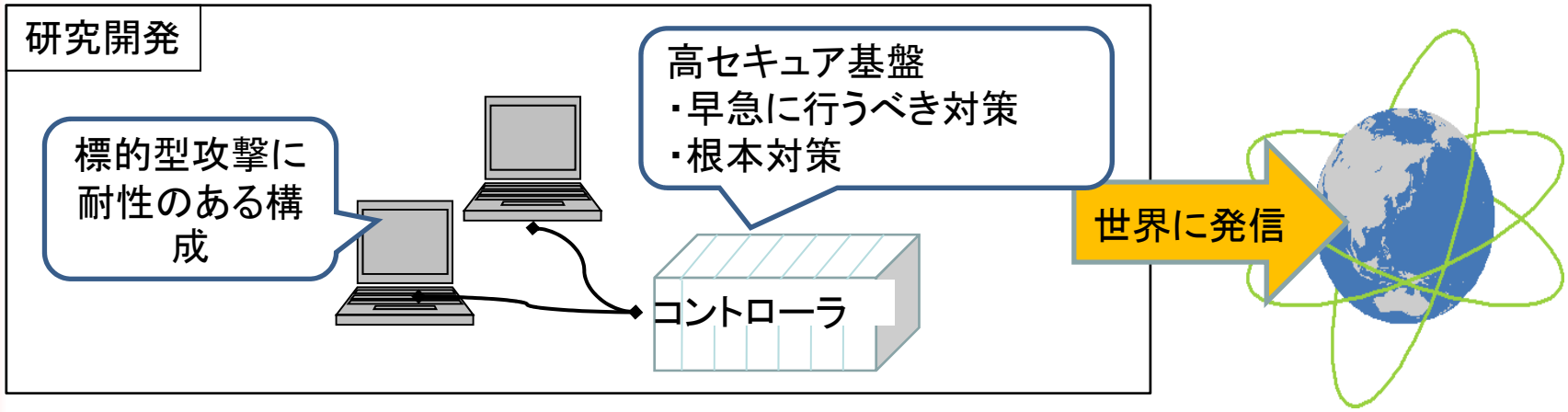


2. 高セキュア化構成・技術の研究開発

■狙う成果

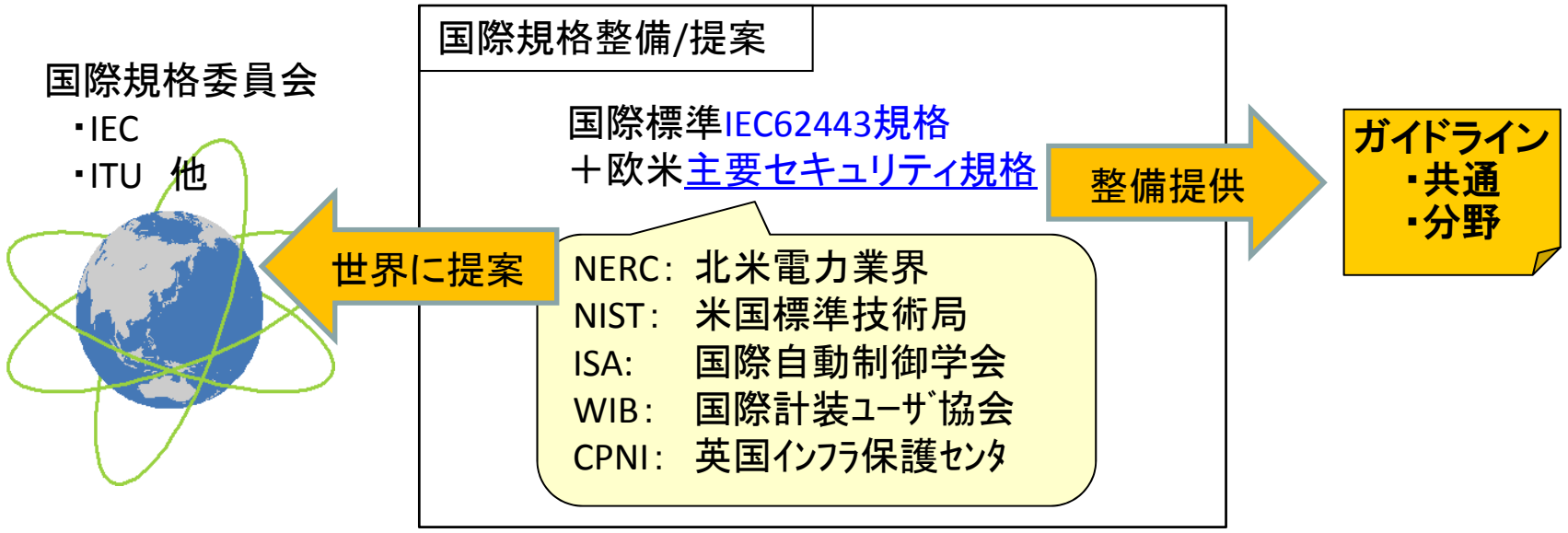
制御システムの要件（性能、安定稼動、長期保守、既存システム/標準との相性など）を満足する日本発のセキュア構成・技術

- ・制御システムおよびスマートシティ（オープンネットワーク）での広域連携制御向けセキュア構成・技術（暗号/認証/鍵管理、安全稼動、仕様記述、検証、多重化など）
- ・制御システム稼動状況と連動した問題箇所解析技術
- ・セキュリティ対策効果の検証



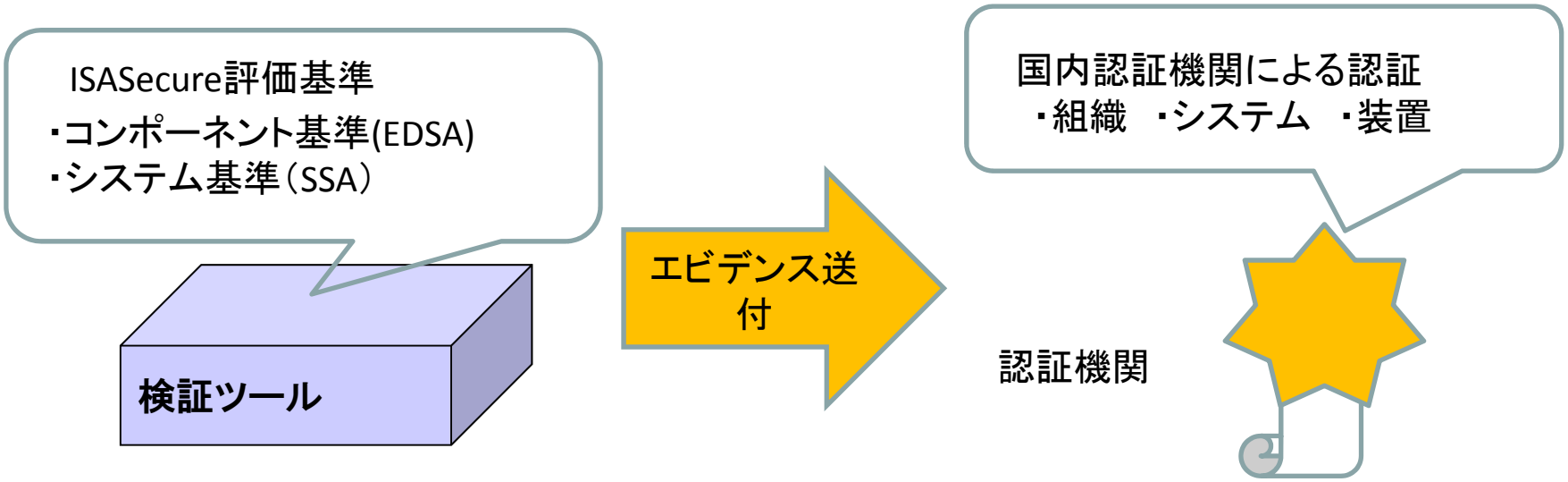
3. セキュリティ国際規格

■狙う効果
セキュリティ国際規格に対するイニシャティブ確保
・国際規格案の早期入手
・国際規格策定への先手提案（開発技術にもとづく提案）
・セキュリティ関連規格群からの標準ガイドライン構築



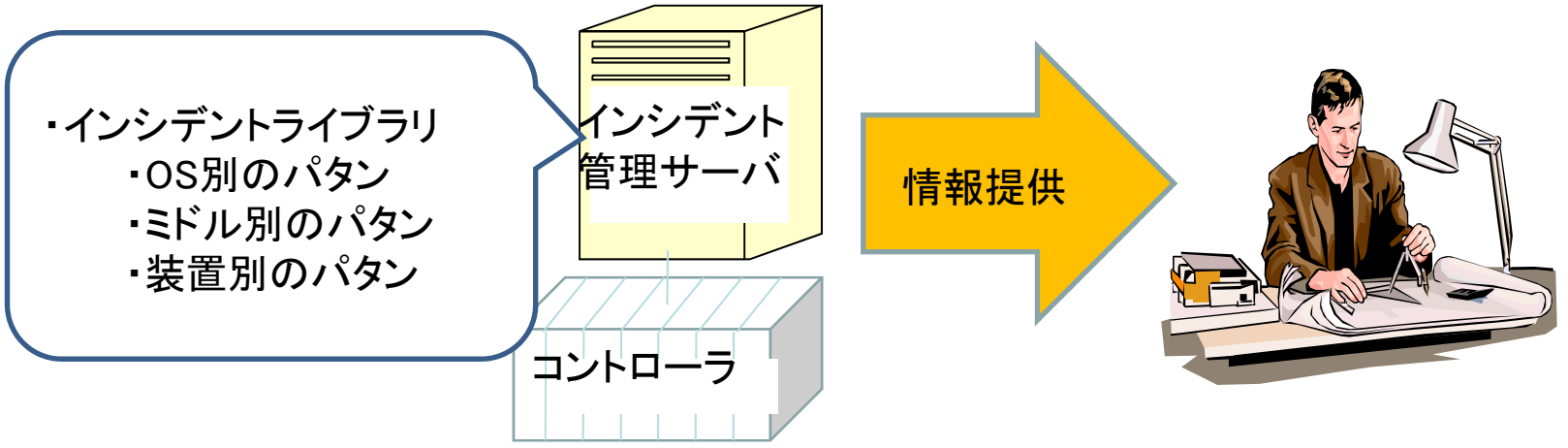
4. 国際規格準拠認証

■狙う効果
第3者による客観的な評価基準に基づく国際認証の早期取得
・検証ツールと連携した認証
・国内認証機関と連携した短期間（低コスト）認証



5. インシデントサポート

■狙う効果
制御システムにおけるインシデントサポート
- インシデント対応マニュアルの提供
- インシデントライブラリの整備と利用環境の提供
- インシデント対策サポート（オンサイトも含む）



JPCERT/CC殿と連携して実施

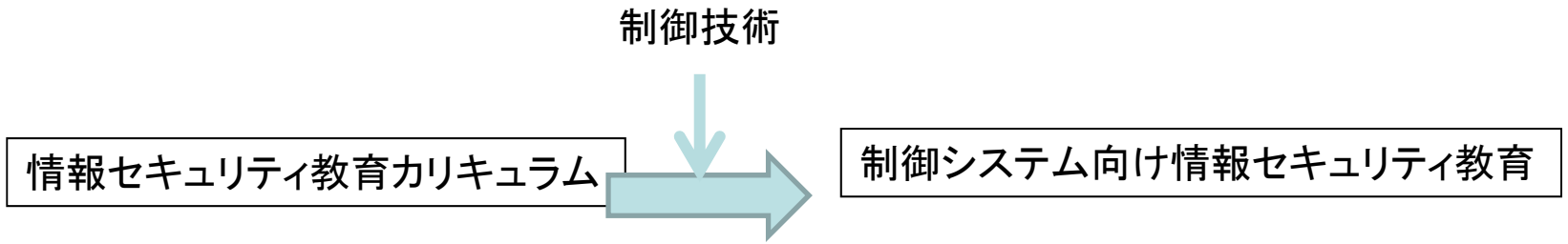
6. 人材育成

■狙う効果

制御システムエンジニアをターゲットにした疑似体験を含めたセキュリティ教育実施

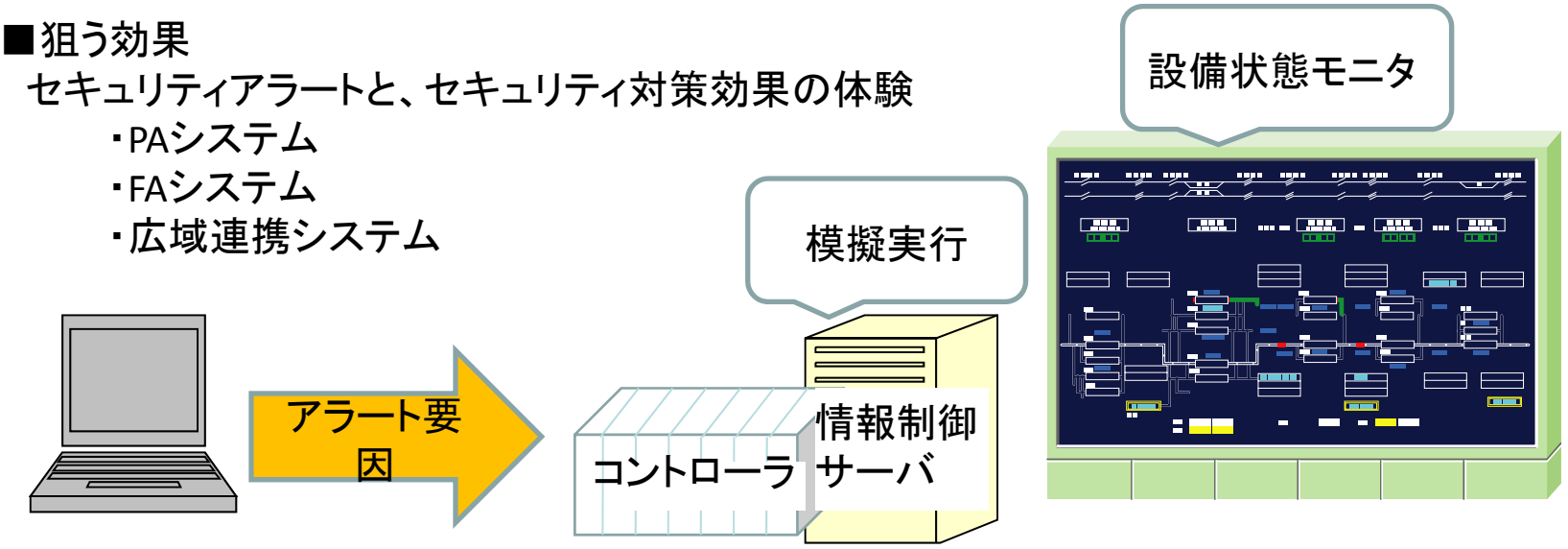
・制御システムを前提としたセキュリティ構築教育

・制御システムを前提とした障害切り分け教育

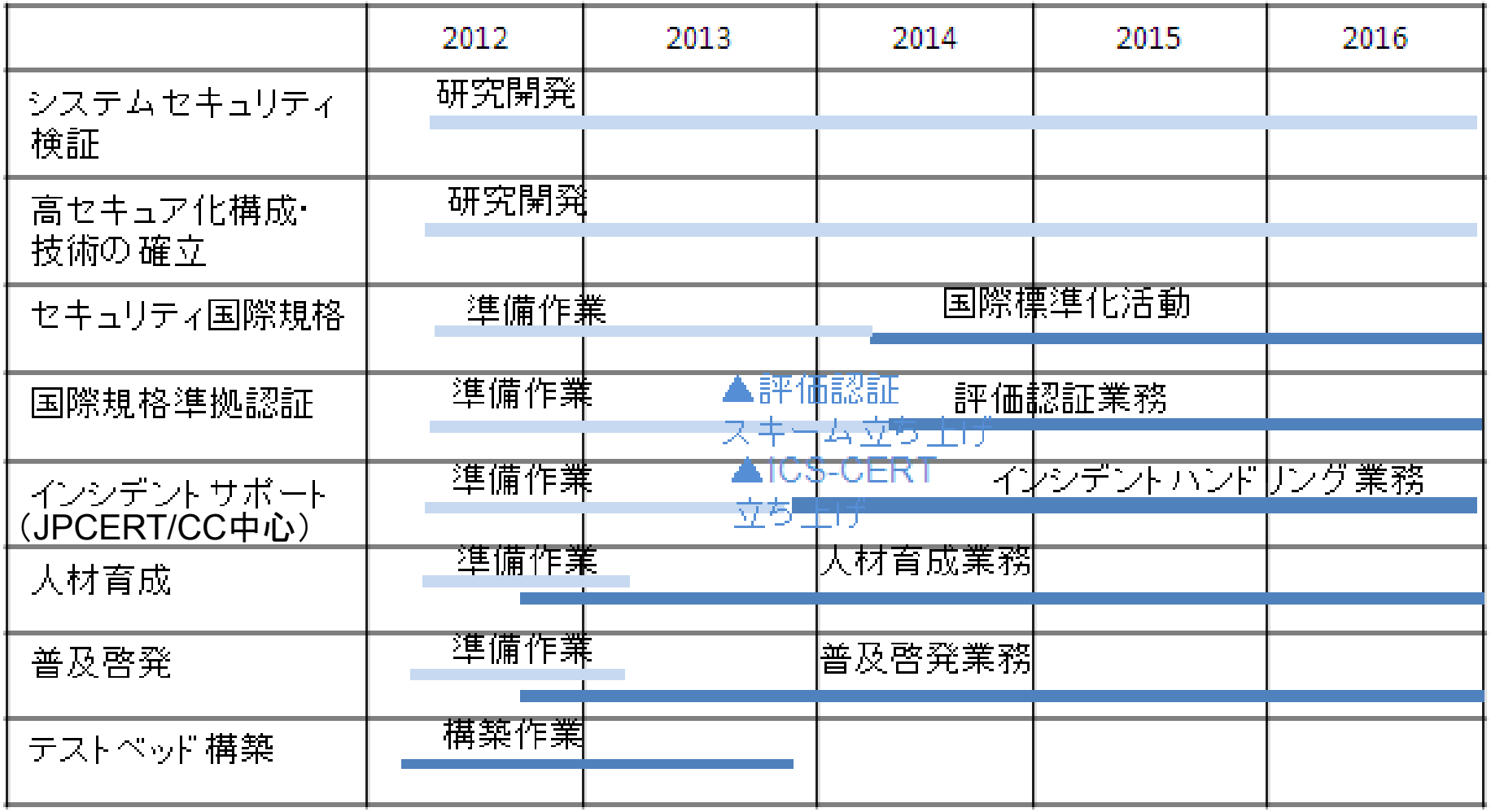


7. 普及啓発

■狙う効果
セキュリティアラートと、セキュリティ対策効果の体験
・PAシステム
・FAシステム
・広域連携システム



マイルストン



まとめ

1. 技術研究組合制御システムセキュリティセンターは、制御システムのセキュリティ確保を目指します。

2. 検証、研究開発、インシデントサポート、認定認証スキーム、国際国際連携、人材育成・普及啓発、そしてテストベッド構築を行います。

3. 平成24年度中は、次世代の制御セキュリティ確保のためのインフラとなるテストベッド構築を行います。

4. テストベッドを用いて、検証、研究開発、認定認証その他の業務を行い、日本発の制御システムセキュリティ技術を確立し、システムや機器の輸出の起爆剤となることを目指します。

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