平成22年度
内閣官房情報セキュリティセンター委託調査

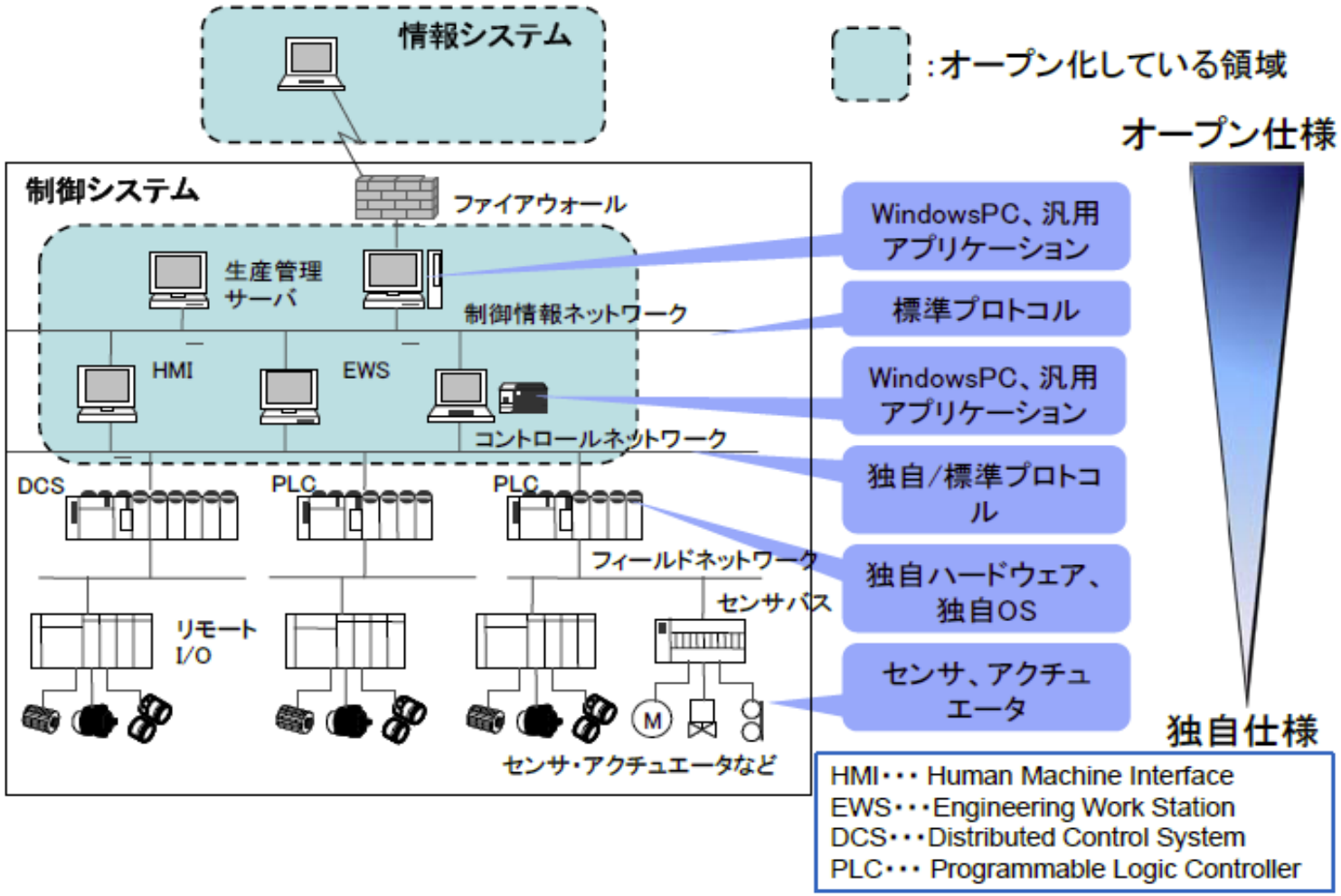
制御システムのオープン化が重要インフラのセキュリティに与える影響の調査

平成23年3月

（財）未来工学研究所

1. 制御システムのオープン化の概要

汎用製品の採用及び標準プロトコルの採用の両方を含めて、
「制御システムのオープン化」と呼ぶ（IPA)



2. 制御システムのオープン化に係る最近の動向と将来予測①
情報システムVS制御システム

IPAが指摘する情報システムVS制御システム

	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
システム更新	10-20 年	3-5 年
稼働時間	24 時間 365 日連続	通常業務時間内
運用管理	現場技術部門	情報システム部門

*C（Confidentiality：:機密性）、I（Integrity：完全性）、A（Availability：可用性）

NISTが指摘する情報システムVS制御システム

	情報技術	制御技術
性能要求の違い	非リアルタイム	リアルタイム
	応答の信頼性	応答はタイムクリティカル
	高いスループットが要求される	相応のスループットでよい
	遅れや揺れが許容される	遅れや揺れは重大な問題
信頼性要求の違い	スケジュール化された運用	連続的運用
	時々の不具合に寛容	停止は致命的
	フィールドでのベータテスト可	完全なテストが期待される
リスク管理要求の違い デリバリ対セイフティ	データの統合性が絶対的必要	人間の安全性が絶対的必要
	リスクの影響はデータの喪失とビジネス運用の喪失	リスクの影響は人命、設備、製品の喪失と環境へのダメージ
	リブートによるリカバリが可能	フォールトトレランスが必須

2. 制御システムのオープン化に係る最近の動向と将来予測②
オープン化によって浮上した制御システムのリスク

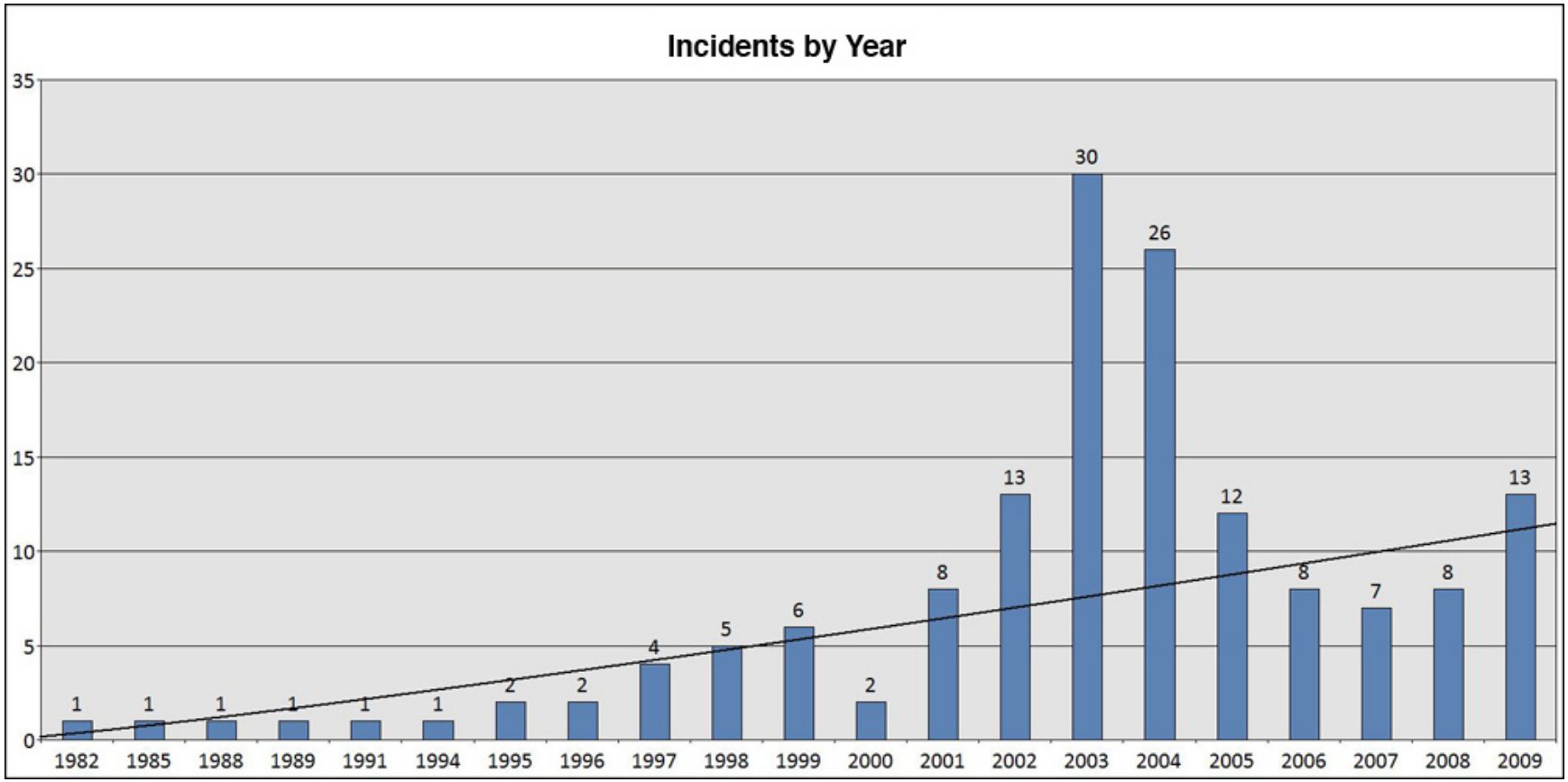
IPAの指摘する制御システムのリスク

①オープン化に伴う脆弱性リスクの混入
・汎用製品の採用に伴う汎用製品が有するハードウェア・ソフトウェアの脆弱性の継承
・標準プロトコルを採用することによるウィルスの侵入や機密情報漏えいの可能性
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
・制御システムの長いライフサイクル（ 10年～20年）による陳腐化（情報系は5年程度）
③可用性（Availability）重視によるセキュリティ機能の絞込み
・制御システムでは可用性を重視しウィルス監視プログラムの自動更新などは行われない
・その結果制御システムのセキュリティレベルは情報システムと比べて大幅に遅れている

NISTSP800-82の指摘する制御システムの4つのリスクファクター

①標準化されたプロトコルと技術の採用、
②汎用プロトコルによる接続の増加、
③安全でない虚偽的な接続、
④インターネットを介した公共的接続。

2. 制御システムのオープン化に係る最近の動向と将来予測③
増加する制御システムのセキュリティインシデント数



2010年は10件（2011年３月時点）

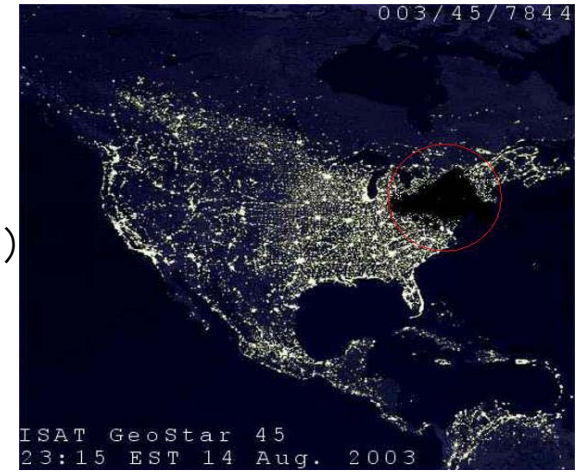
出典：Repository of Industrial Security Incidents (RISI)

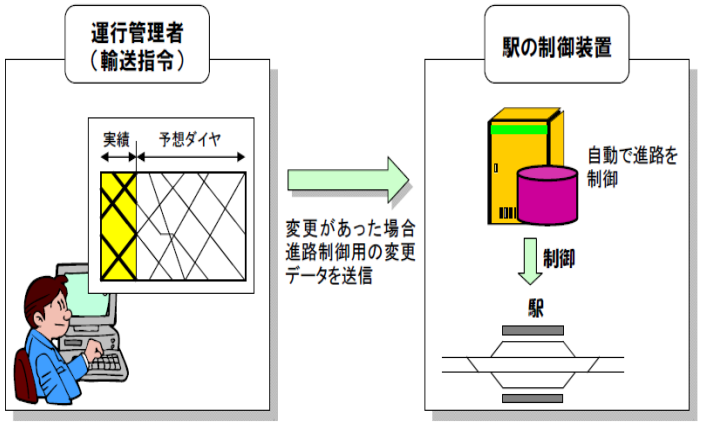
2. 制御ステムのオープン化に係る最近の動向と将来予測④
米欧日の最近の事例

米国
①米国東海岸の大停電（2003年8月）
②トランスアラスカ・パイプライン漏洩（2010年5月25日）
③ワシントンDCの地下鉄事故（2009年6月22日）
④ジョージア州ハッチ原子力発電所の停止（2008年3月7日）
⑤オーロラ発電機試験の実施

欧州
①ロンドン地下鉄の誤進路への侵入（2010年9月8日）
②エアフランス447便の大西洋での墜落（2009年6月１日）
③ダブリン港トンネルの閉鎖（2008年2月27日）

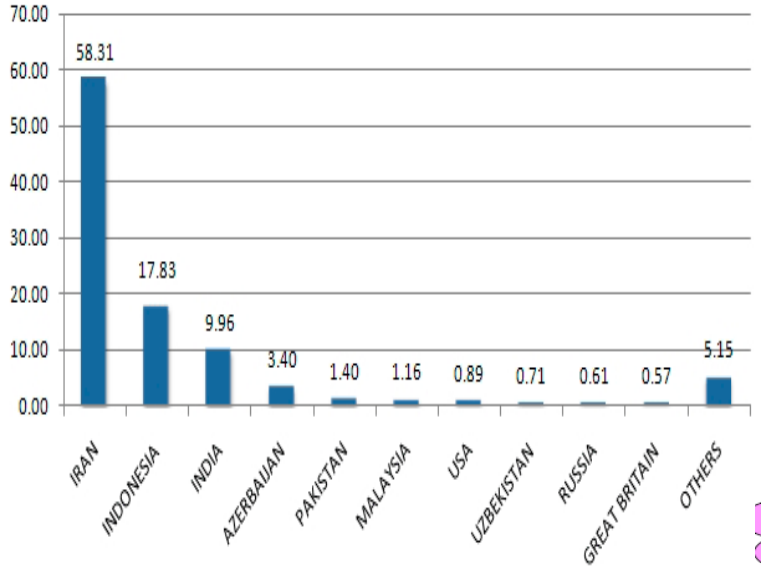
日本
①JR東日本新幹線の全線停止（2011年１月17日）
②みずほ銀行のシステム障害（2002年4月、2011年３月）



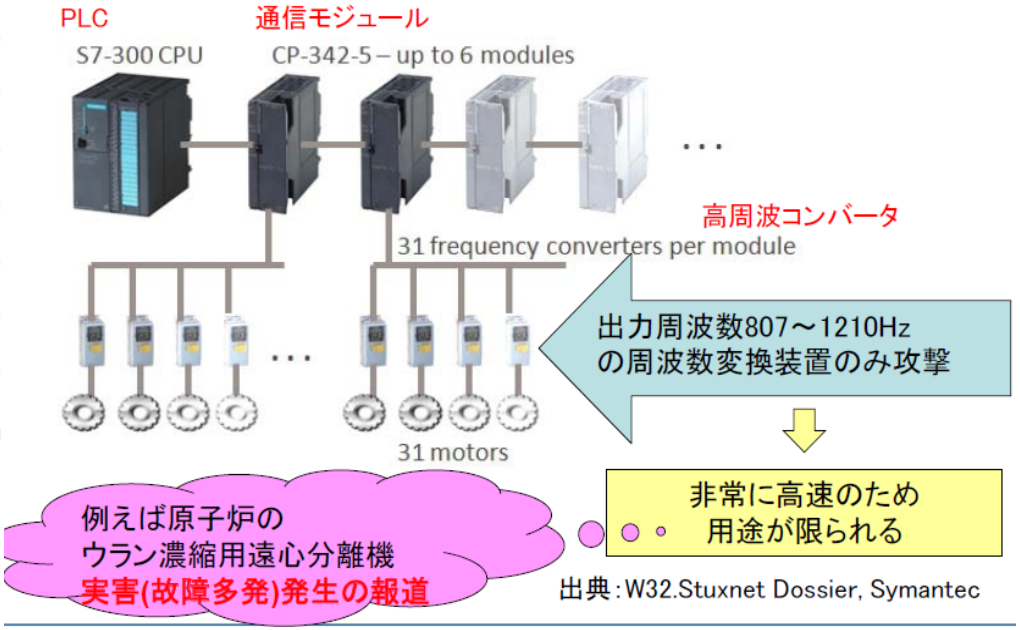


2. 制御ステムのオープン化に係る最近の動向と将来予測⑤
新しいタイプの脅威—STUXNET①

Stuxnetの国別感染ホスト分布



標的となった周波数変換ドライブへの攻撃



制御システムがサイバー攻撃の本格的対象になった。
情報システムから侵入して制御システムをダウンさせた。

2. 制御ステムのオープン化に係る最近の動向と将来予測⑥ 新しいタイプの脅威—STUXNET②

打ち砕かれた制御システムの安全性神話

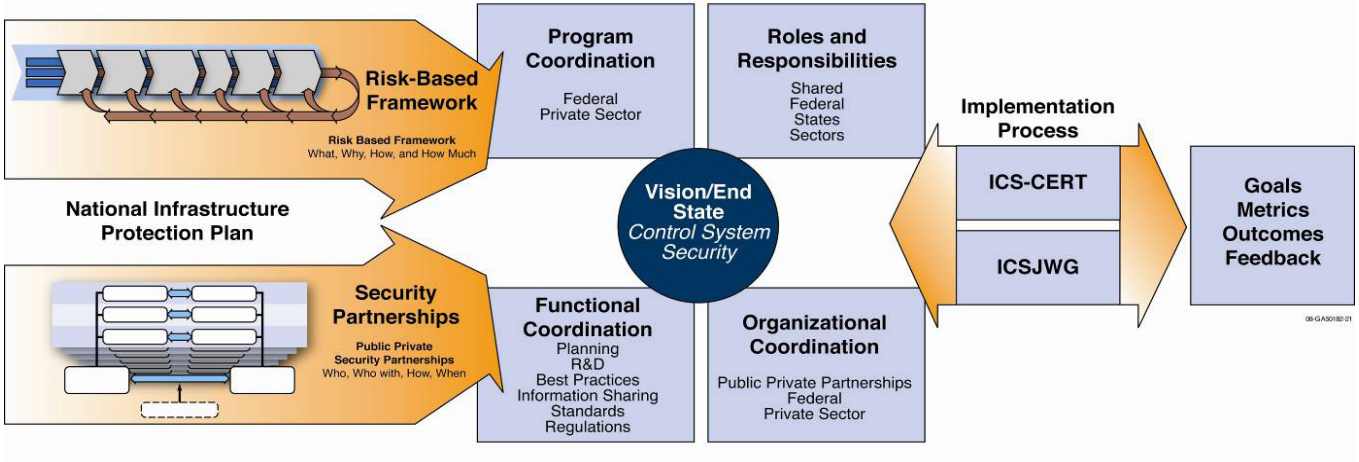
①制御システムはサイバー攻撃と無縁だ。
②制御システムをインターネットと切り離しておけば100%安全だ。
③特殊なシステム構成だから外部にいる攻撃者に分かるはずがない。
④新品のUSBメモリだけ使っていれば安全だ
⑤マルウェアに感染するとコンピュータ自体の動きが異常になる(制御システムは異常停止しない限り稼働させ続ければよい)。

JPCERT/CCが示すStuxnetの教訓

Stuxnetにおける事実	Stuxnetに耐えるために求められるもの
脆弱性を衝いて侵入された	• 脆弱性を作り込まない**技術力** • 事前に脆弱性を除去しておく**組織力** • 部分的に多少の脆弱性があっても耐えられる(多層防御)ようにシステムを構成しておく**技術力**
開発者は標的の制御システムを知り尽くしていたと見られる	• システム構成に関する情報が攻撃者に知られても耐えられる防衛ラインを作り込む**技術力**
特定の環境でのみ攻撃動作	• 異常を検知する**眼力(人)**
異常をHMIで表示されないよう隠蔽	• 制御システムの異常も疑ってみて総合的に判断する**眼力(人)**
今でもStuxnetを知らない制御システム運用者も少なくない	• **情報収集**のための**組織力**
ゼロデイ脆弱性が悪用されているので，普通の復旧では再び侵入される	• すみやかなシステム**復旧**と業務継続のための戦略

3. 制御システムのオープン化が情報セキュリティに与える影響① 米国①

米国DHSの示す制御システムセキュリティの協調体制

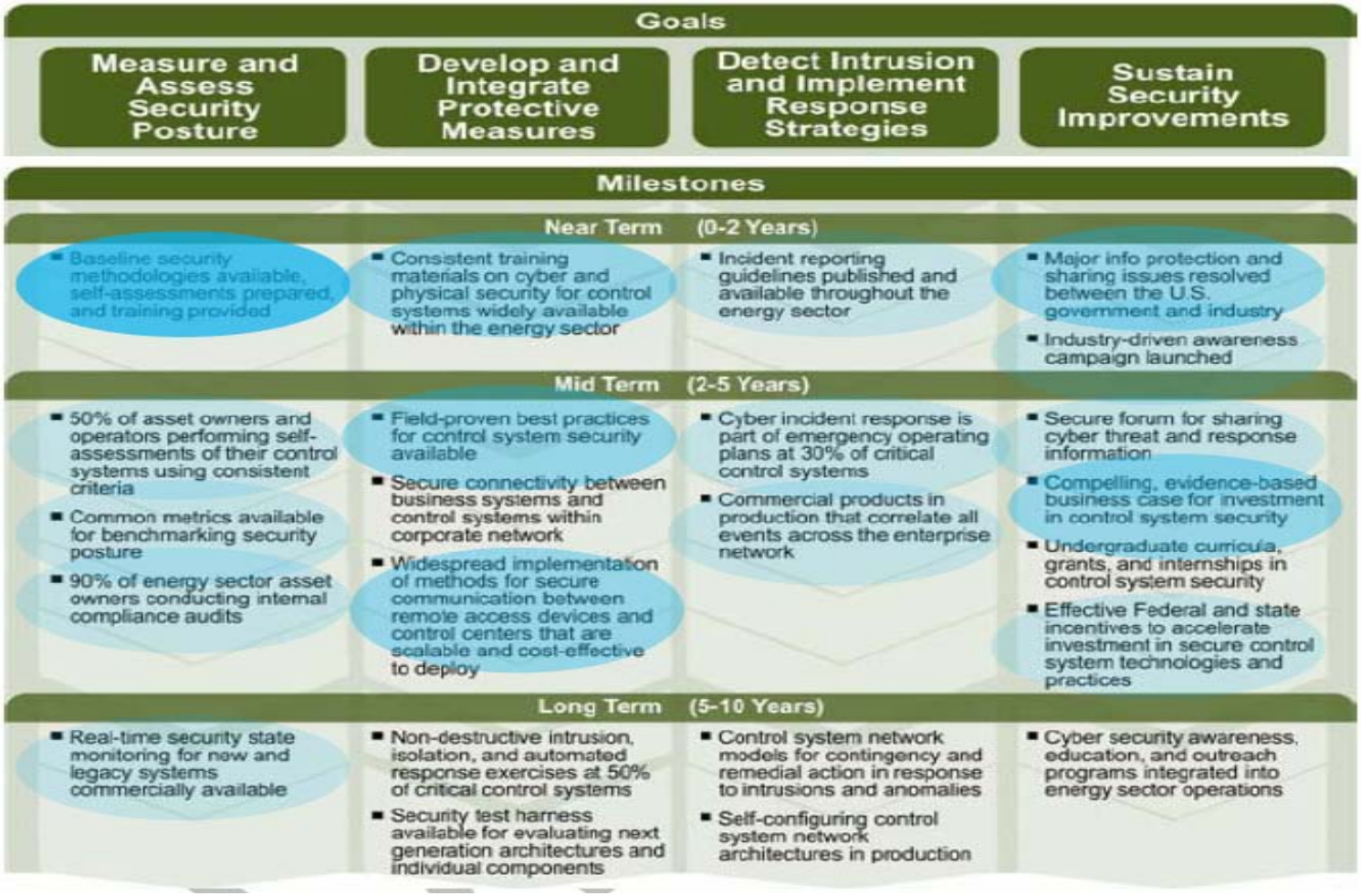


ICSJWG(ICS Joint Working Group)の６つサブグループ

①情報共有サブグループ
②国際協力サブグループ
③研究開発サブグループ
④安全な制御システムへのロードマップサブグループ
⑤ベンダサブグループ
⑥人材開発サブグループ

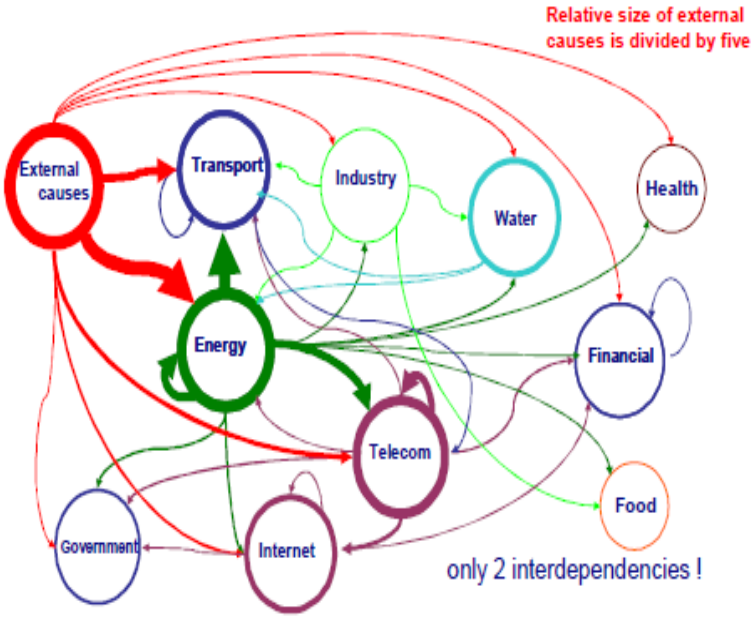
3. 制御システムのオープン化が情報セキュリティに与える影響②
米国②
エネルギー制御システムの技術開発ロードマップ

Roadmap to Secure Energy Control System

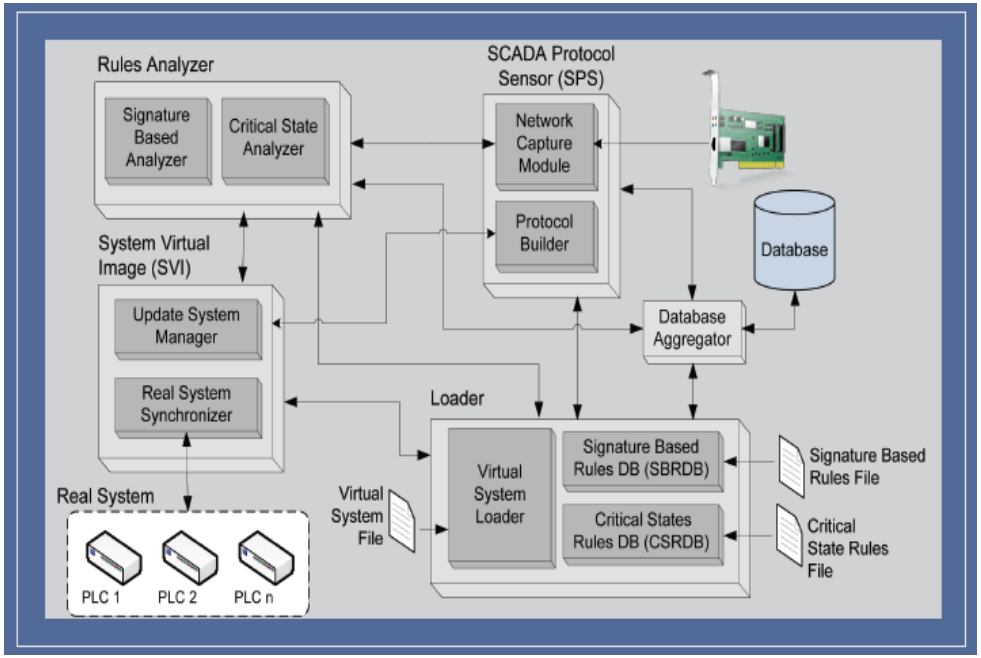


3. 制御システムのオープン化が情報セキュリティに与える影響③
欧州①
カスケード波及研究とARCADEシステム研究

オランダTNOによる重要インフラ間のカスケード波及研究



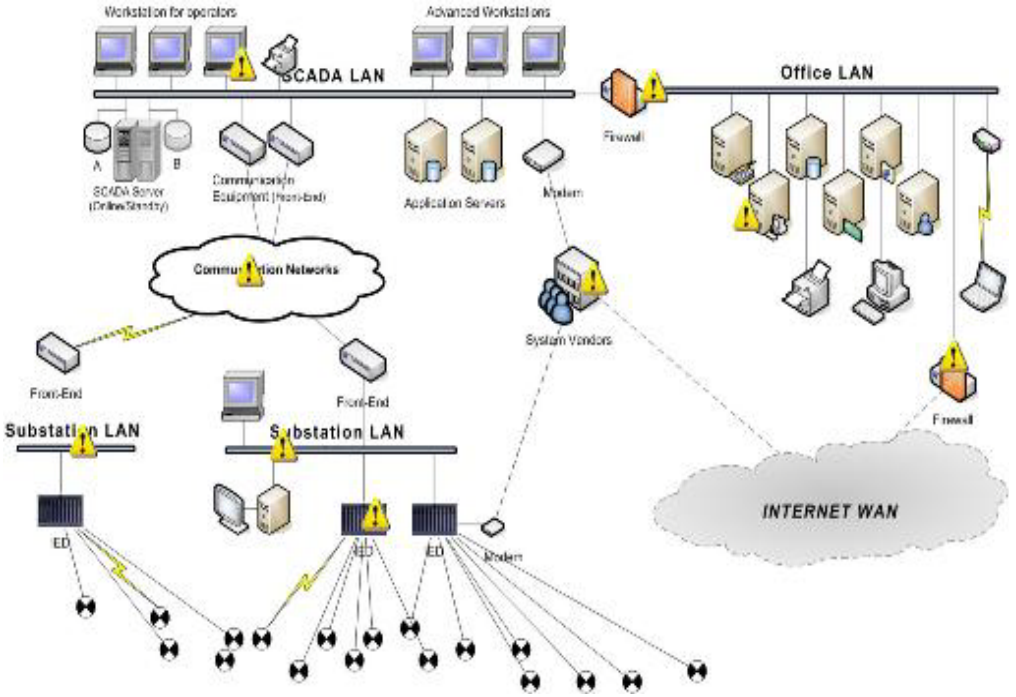
Institute for Protection and Security for Citizens のCIP（Critical Infrastructures Protection）によるARCADEシステムの研究



ファイアウォール、侵入検出、危機状態モニターを組み合わせたSCADAセキュリティシステム

3. 制御システムのオープン化が情報セキュリティに与える影響④
欧州②
VIKINGプロジェクト

VIKINGプロジェクトの研究対象の概略



VIKINGプロジェクトの目的

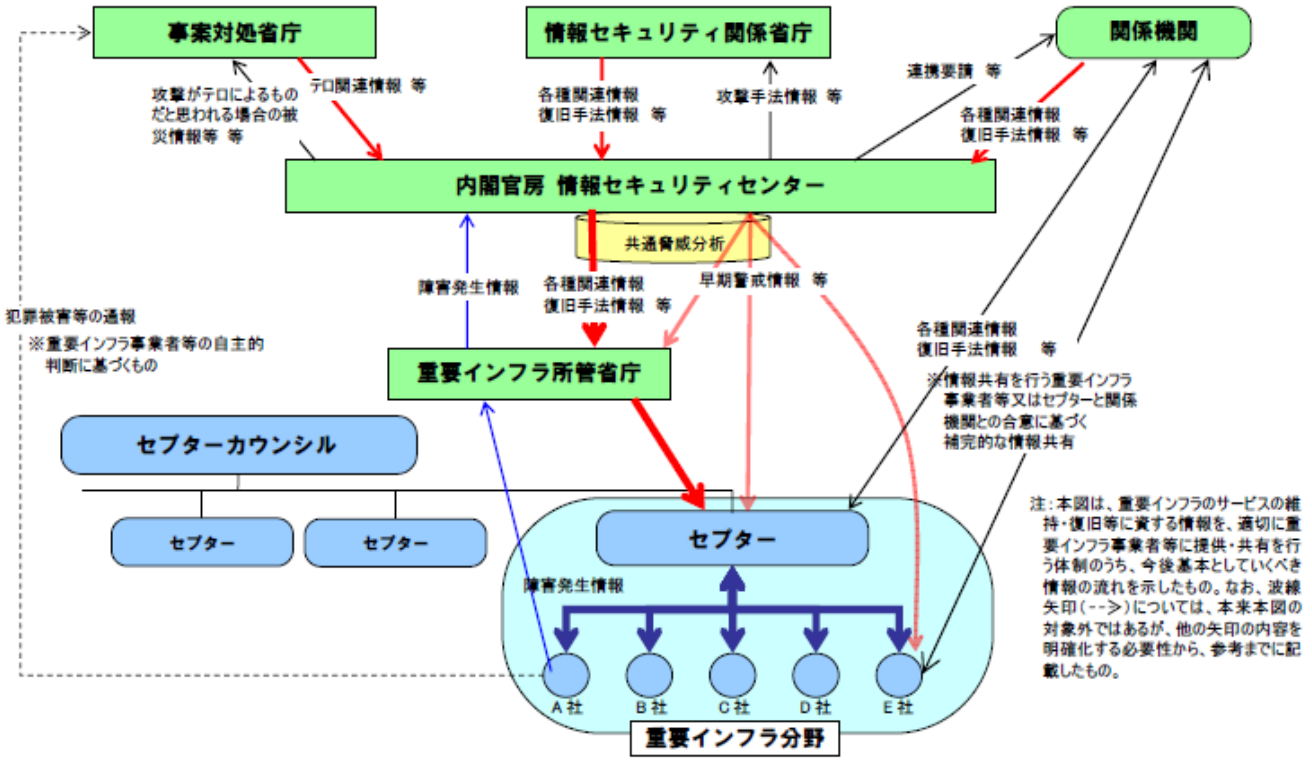
①SCADAシステムの脆弱性と
その社会的コストの解明
②これらの脆弱性を緩和する
戦略と技術の提案・試験
③重要インフラとその防護の
重要性の周知の向上

VIKINGプロジェクトの参加者

・ABB（ドイツのベンダ）、
・E.ON（ドイツの電力会社）、
・MML（スウェーデン企業）、
・Astron Informatics（ハンガリーの
SCADA開発企業）
・ETH大（スイス）
・KTH大（スウェーデン）、
・メリーランド大（アメリカ）
が参加

3. 制御システムのオープン化が情報セキュリティに与える影響⑤ 我が国

我が国における重要インフラセキュリティ情報分析と情報共有



・NISCを中心とした関係政府機関と重要インフラの各セプターとセプターカウンシルによる情報分析・共有体制が確立しつつある。
・IPAとJPCERT/CCが独自のアプローチで制御システムのセキュリティに関する分析や対策に取り組んでいる。

3. 制御システムのオープン化が情報セキュリティに与える影響⑥ 標準・規格化などの動向

情報系と制御系のセキュリティ、
システム運用者とコンポーネント視点から見た
標準・規格化などの動向

	管理運用視点 ・セキュリティ管理システム仕様 ・推奨実施例	コンポーネント視点 ・セキュリティ機能要件定義 ・評価・認証の枠組み
情報系セキュリティ	・ISO/IEC 27000シリーズ（27001：情報セキュリティ管理システム（ISMS）要求事項，27002：ISMS 実践のための規範，27005：情報システムのリスク管理，27006：認証/登録プロセスの要求仕様） ・NIST SP800-53他	・ISO/IEC 15408 （Common Criteria；CCと称される。製品がセキュリティに配慮すべき事項）
制御系セキュリティ	・ISA-99 （生産制御システムセキュリティ） ・ISO/IEC 62443（予定） （Industrial Process Measurement and Control – Net & System Security） ・NIST SP800-82	・PCSRF SPP-ICS （System Protection Profile - Industrial Control System）

・2010年10月にIEC 62443-2-1 Ed. 1.0が正式に成立した。
・NIST SP800-82は制御システムのセキュリティに関する標準となっている。

4. 我が国の重要インフラ関係者への提言

①制御システムの情報セキュリティ課題の重要性認識と、セキュリティ対策の積極的取組み

②情報共有体制の積極的整備

③制御システムの情報セキュリティに関する研究開発の積極的推進

④重要インフラの途絶の他インフラへのカスケード的波及に関する追跡調査の実施