IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

＜制御システムセキュリティ　課題と対策＞
「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」概要

～米国の活動調査から日本の課題を～

2009年2月20日
独立行政法人 情報処理推進機構（IPA） 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　hd-koba@ipa.go.jp

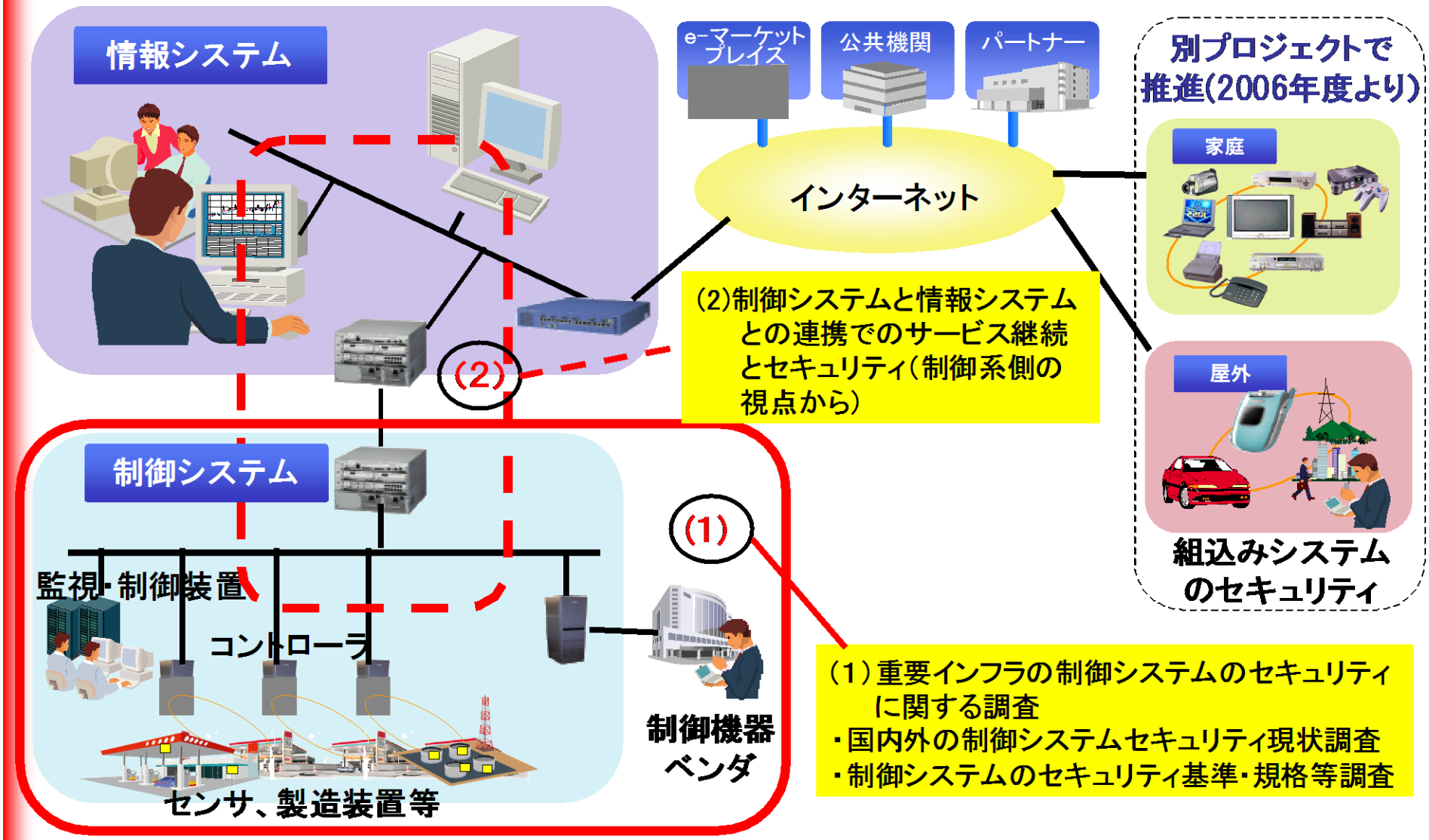
発表内容

- 調査の背景と目的
- 制御システムのオープン化状況、セキュリティ課題、セキュリティ基準・規格策定状況
- 米国のセキュリティ対策状況
- 日本と米国の現状の考察
- 今後のセキュリティ対策の方向性

1.1 調査の背景と目的

- 重要インフラの制御システムへの標準プロトコル（IPネットワーク）や汎用製品の導入、情報システムとの接続や連携が進展
- 今後、制御システムにおける情報セキュリティ上の課題が顕在化する可能性あり
- 制御システムの情報セキュリティに関する国内外の動向と、障害発生時におけるサービス継続への現状の把握が必要

1.2 調査の内容



1.3 調査の進め方

ICSセキュリティ＆サービス継続検討会委員名簿（五十音順、敬称略）

【委員長】	渡辺　研司	長岡技術科学大学
【副委員長】	越島　一郎	名古屋工業大学
【委員】	梅田　裕二	株式会社 東芝
	大谷　純一	三菱電機 株式会社
	小川　永志樹	横河電機 株式会社
	小美野　明弘	株式会社 日立ハイテクコントロールシステムズ
	小島　一浩	独立行政法人 産業技術総合研究所
	杉野　隆	国士舘大学
	高木　淳一	株式会社 山武
	高橋　郁夫	IT法律事務所
	中野　利彦	株式会社　日立製作所
	深堀　道子	独立行政法人 情報通信研究機構
	宮地　利雄	有限責任中間法人JPCERT コーディネーションセンター
	山口　英	奈良先端科学技術大学院大学
【アドバイザ】	門田　浩	独立行政法人 情報処理推進機構　ソフトウェア・エンジニアリング・センター
	山田　安秀	独立行政法人 情報処理推進機構　セキュリティセンター
【オブザーバ】	井土　和志	経済産業省 商務情報政策局 情報セキュリティ政策室
	井上　信吾	有限責任中間法人JPCERT コーディネーションセンター
【事務局】	小林　偉昭	独立行政法人 情報処理推進機構　セキュリティセンター
	中野　学	同上
	織茂　昌之	株式会社　日立製作所
	相羽　律子	同上

1.4 調査の対象

（1）国内調査

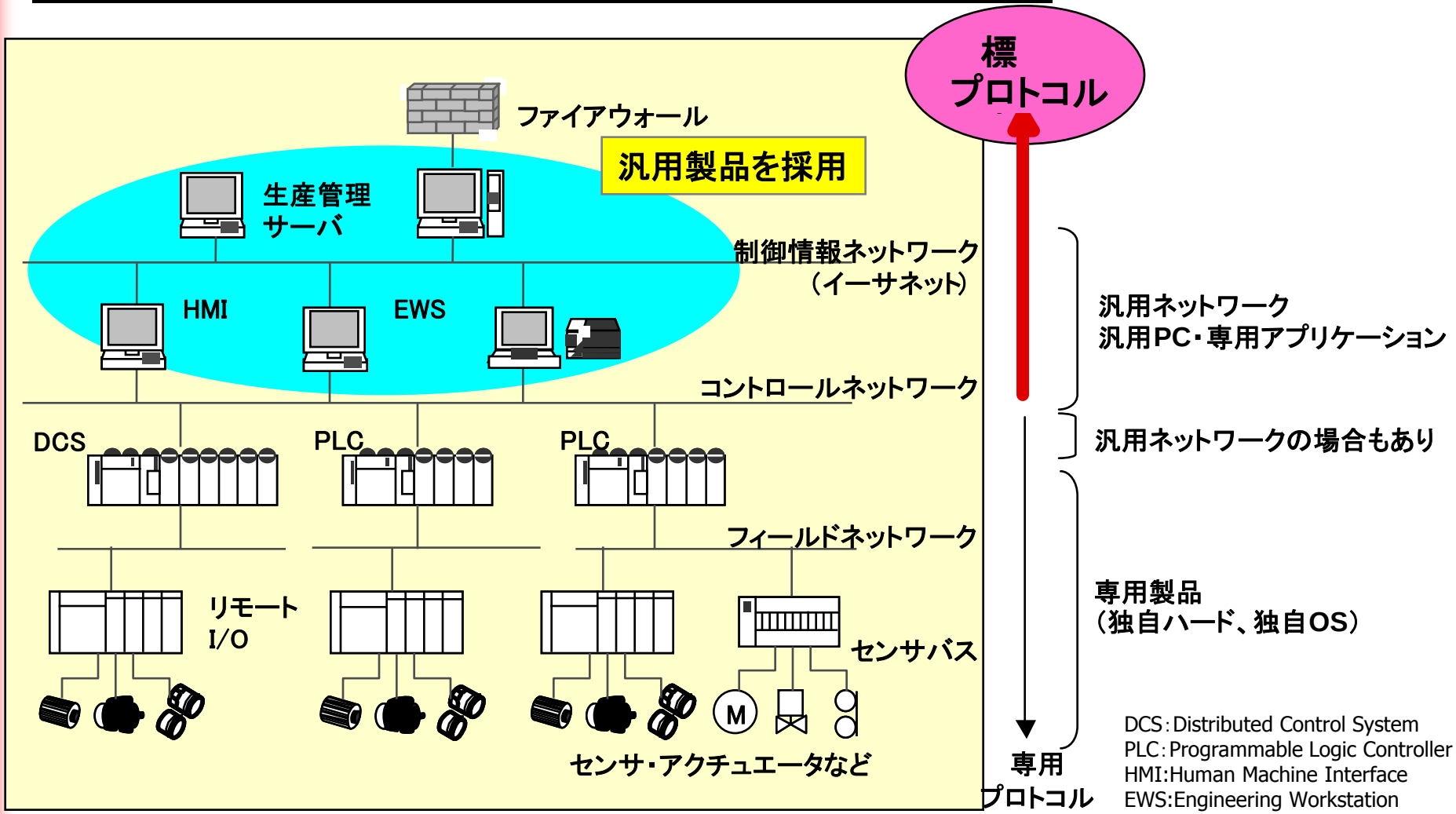
- 国内制御機器ベンダへのヒアリング：国内制御システムベンダ6社
- 大学のヒアリング：長岡技術科学大学、名古屋工業大学、
  国士舘大学、奈良先端科学技術大学院大学
- 業界団体との意見交換：
  （社）日本電気計測器工業会 PA・FA計測制御委員会
  セキュリティ調査研究WG

（2）海外調査（米国）

- 政府機関のヒアリング：NIST（National Institute of Standards and Technology）
- 研究機関、大学へのヒアリング：INL（Idaho National Laboratory）、
  Dartmouth大学、I3P（Institute for Information Infrastructure Protection）
- セキュリティ関連ベンダへのヒアリング：MITRE Corporation、Digital Bond
- カンファレンスでの情報収集：
  Process Control Systems Industry Conference 2008

2.1 制御システムのオープン化状況

「オープン化」：汎用製品＋標準プロトコル



DCS：Distributed Control System
PLC：Programmable Logic Controller
HMI:Human Machine Interface
EWS:Engineering Workstation

2.2 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

【課題２：製品長期利用に伴うセキュリティ対策陳腐化】

・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

【課題３：可用性重視に伴うセキュリティ機能絞込み】

・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せず

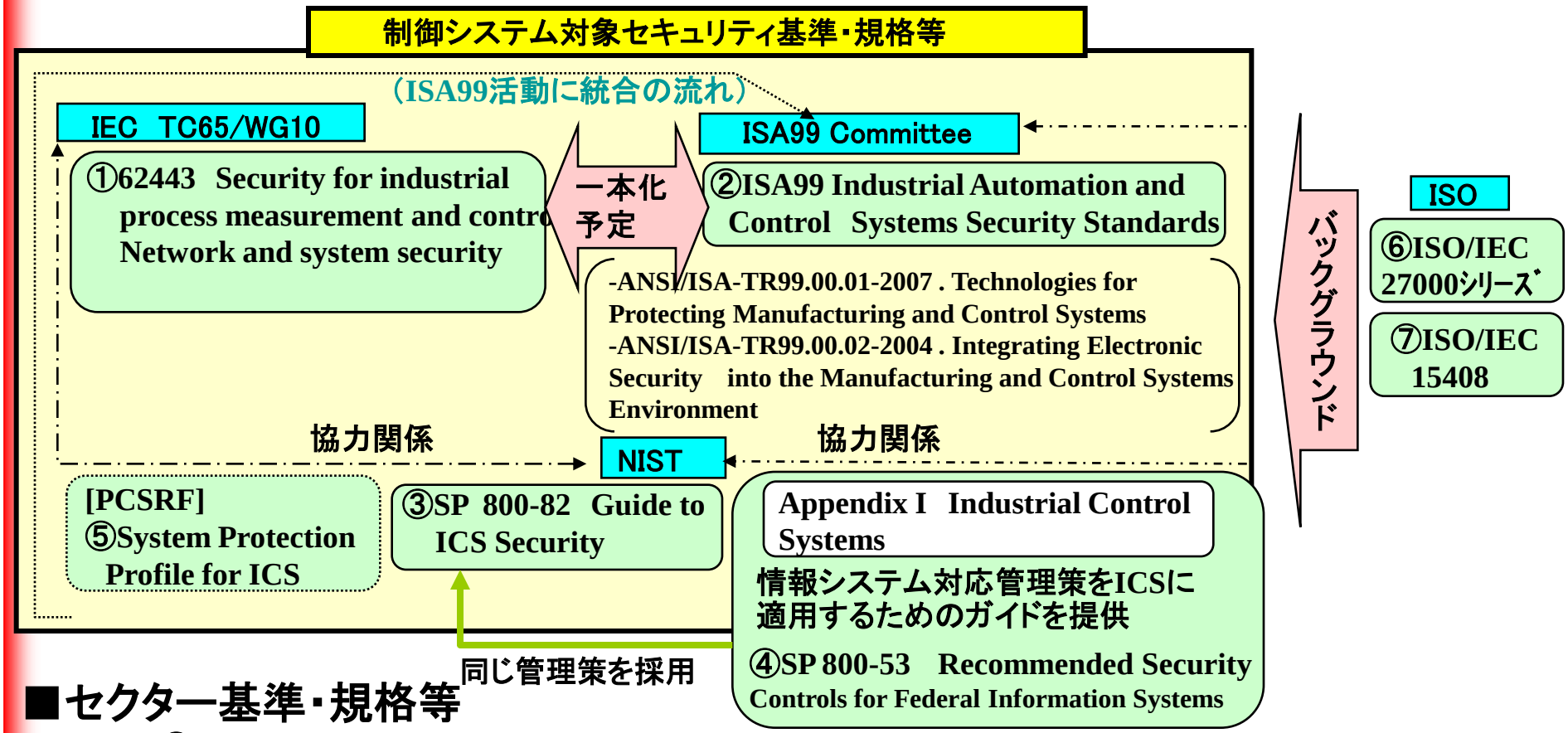
	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報

2.3 セキュリティ対策における背景の違い

セキュリティ上 必要となる要件	情報システム	制御システム
技術のサポート期間	3-5年	20年以上
パッチ提供サイクル	頻繁・定期的	ベンダごとに不定期、長期間間隔で実施（公表値なし）
システム上流れるデータの処理速度	データ受け取り遅延が致命的な被害となるケースは少ない	システム／機器制御にはリアルタイムのデータ受け取り処理が不可欠
可用性 （Availability）	再起動は許容可能	24時間365日の安定稼動が不可欠（再起動は許されない）
セキュリティに関する意識	民間企業、公的機関とも意識が行き渡り、定義されている	発展途上にあり未成熟。情報システム技術の適用で対応するケースもある
被害の結果	金銭的損失、プライバシー被害	人命損失の可能性

2.4 セキュリティ基準・規格策定状況

■標準化団体策定基準・規格等



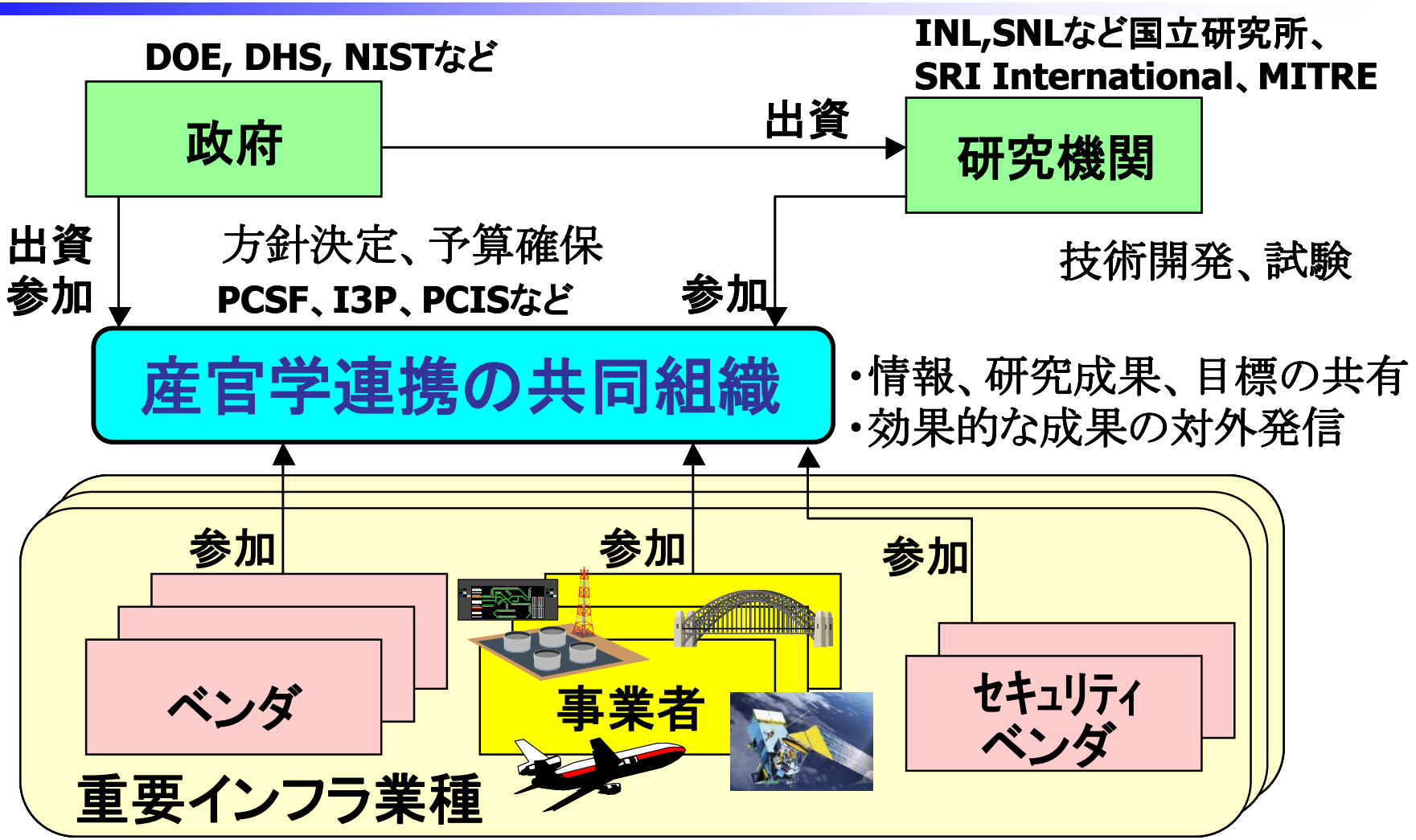
■セクター基準・規格等

電力　⑧NERC Cyber Security Standards CIP-002 ～CIP-009

ガス　⑨American Gas Association (AGA) Standard 12, "Cryptographic Protection of SCADA Communications"

石油　⑩American Petroleum Institute (API) Standard 1164, "Pipeline SCADA Security"

3.1 米国における取り組み概要



PCSF Process Control Systems Forum
PCIS Partnership for Critical Infrastructure Security
I3P Institute for Information Infrastructure Protection

3.2 米国のセキュリティ対策状況（1/2）

- **CSSP（Control Systems Security Program）**

ーDHSがイニシアチブをとって、官民連携にて推進

ー制御システムにおける脆弱性リスクの削減、および脅威への対応に必要な対応能力の獲得を目的に活動

（成果物：セキュリティカタログ、自己評価ツール、要求仕様書、研修の提供など）

- **NSTB（National SCADA Test Bed Program）**

ーCSSPの一環で、DOEやOEがイニシアチブをとって、官民連携にて推進。エネルギー関連事業者にフォーカス

ー研究施設での実運用環境に近い条件で脆弱性検証試験や、オンサイトでのセキュリティテストサービスを提供

DHS	Department of Homeland Security
DOE	Department of Energy
OE	Office of Electricity Delivery and Energy Reliability

3.2 米国のセキュリティ対策状況(2/2)

- **Roadmap to Secure Control Systems**

ー官民連携で、制御システムにおけるセキュリティ対策の進め方を示すロードマップを作成。エネルギー分野で先行。水も。

- 2006年スタート、2015年までの10年をかけてセキュリティを強化した制御システム環境への移行を目指す

- **I3Pによるプロジェクト**(Institute for Information Infrastructure Protection)

ーI3Pメンバが政府資金などを活用し、リスクマップ(脆弱性予見ツール)をはじめとした、セキュリティ対策ツールを開発

- **民間における認証プログラム**

ー民間企業による独自のセキュリティ認証プログラムも存在

Wurldtech社:ACHILLES、Mu Technologies社:MUSIC

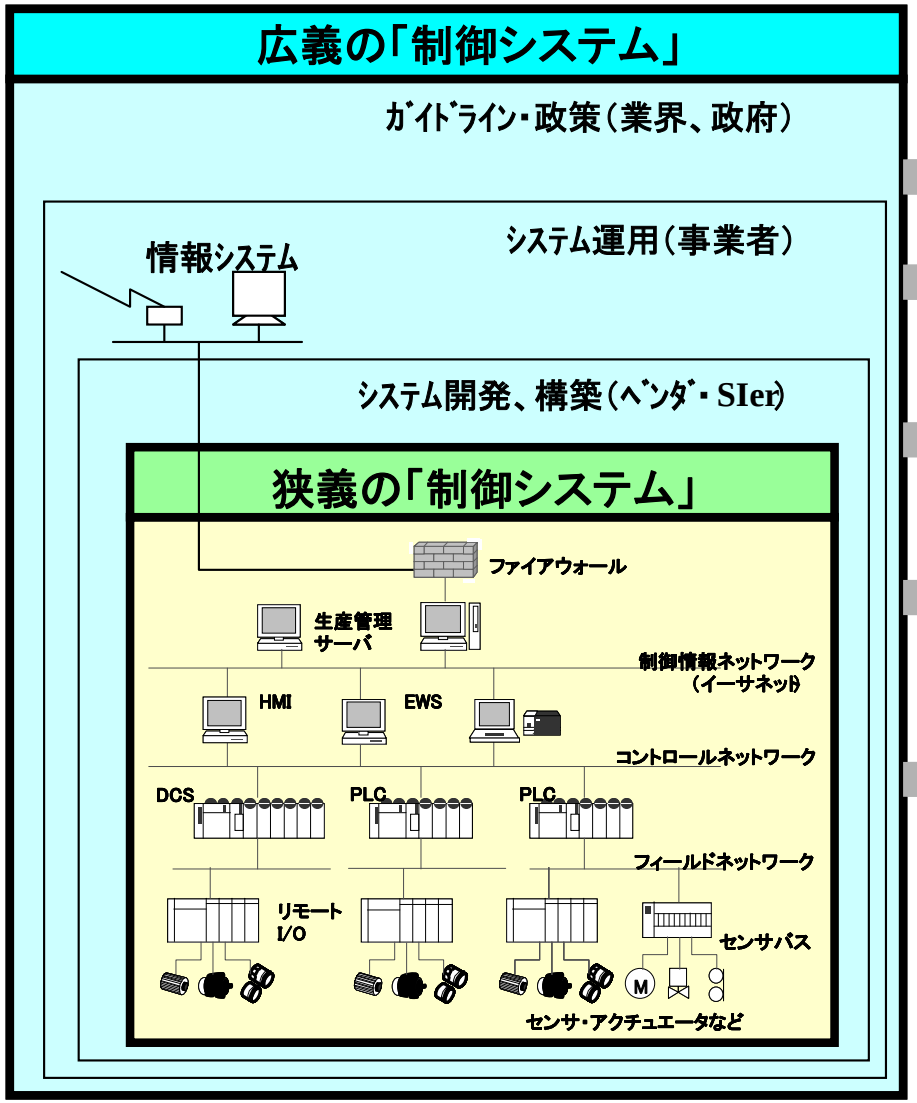
4.1 日本と米国の現状の考察(1/2)

項目	差異および特徴的な傾向	
	米国	日本
(1)制御システムのオープン化状況	(A)標準仕様に準拠した制御システム(SCADA) が普及 (B)ワイヤレスネットワークの導入の検討が進展	(a)社会インフラ系の制御システムにおいては事業者ごとの独自仕様が中心 (b)事業者間の連携やコスト削減圧力が少なくオープン化が進んでいない
(2)制御システムセキュリティの課題	(A)情報システムとの接続により自動化されたワームなどの脅威が顕在化(情報システムは外部ネットワークと接続している)	(a)セキュリティ対策不十分による被害がなく、セキュリティ対策の優先順位は低い (b)重要インフラへの攻撃事例が少ない
(3)セキュリティ対策状況	(A)SCADAテストベッドを開設し、セキュリティ技術の開発、検証を実施 (B)ツールや、第三者機関によるセキュリティテストなどを利用可能 (C)製品認証機関による認証製品利用可能	(a)事業者またはベンダ内で共通的に利用可能なセキュリティテスト環境等はない
(4)脆弱性関連情報の公開	(A)US-CERTは制御システムの脆弱性のデータベースを持つが15～20件と少数 (B)ベンダのユーザグループ内で解決	(a)情報開示による事業者のメリットはなく、積極的な情報共有および活用は困難 (b)JPCERT/CCでは制御システムの脆弱性情報の収集・公開を実施。件数は少ない
(5)推進体制	(A)国家安全保障の観点から政府が主導し、産官学連携の対策体制を構築 (B)国立研究所が技術的なバックボーンを担当	(a)事業者またはベンダによる独自の対策が行われている (b)NISC他による調査・情報共有の機会が増えつつあるが、まだ少ない

4.1 日本と米国の現状の考察(2/2)

項目	差異および特徴的な傾向	
	米国	日本
(6)利用者側の認識	(A)エネルギーセクタ、水セクタでは制御システムセキュリティのロードマップ作成 (B)一般の製造業における認識は依然低い状況	(a)全般的に制御システムのセキュリティに対する認識は低い (b)電中研などの取り組みにあるように電力などの一部セクタでは認識されている
(7)標準化、規格化	(A)NISTでは制御システムに関する政府機関向けの標準(SP800-82)を作成 (B)連邦政府向けセキュリティ対策要件(SP800-53)にも制御システムへの適用を記述 (C)ISA99、IEC62443など策定中	(a)標準品や業界デファクト品が明確な要求仕様として示されることは少ない (b)米国向けにおいては、規格対応が応札条件となるケースがあり、認証取得が進展中 (c)事業者またはベンダ(JEMIMA含む)独自の標準化対応・検証活動に留まる
(8)情報システムと制御システムの連携	(A)表示やモニタリングのためにデータを引き出す目的で統合が進展 (B)制御システムと情報システムとをつなげることにより業務フローを適切に評価しフィードバックが可能	(a)制御システムと情報システムとの接続は増加傾向 (b)保守用を含み、外部ネットワークとの直接接続は実施せず (c)情報システムと制御システムの運用管理は、独立した体制、規定で実施

5.1 今後のセキュリティ対策の方向性



セキュリティ対策の方向性

- 法、ガイドライン等の策定
- 共通研究、技術開発の推進

- 事業者運用ポリシーの遵守
- 教育、物理セキュリティ等の併用

- コンポーネントシステム単位での検証
- 事業者、業界団体仕様への対応

- ファイアウォール、ルータ等による
  ネットワークセグメント分割

可用性と両立する形での
情報系セキュリティ技術適用を検討

- 不正侵入検知システム
- 不正侵入防御システム
- アンチウィルスソフト
- Windows 等へのセキュリティパッチ

5.2 今後のセキュリティ対策の方向性

●制御システムセキュリティのガイドライン確立

－米国では政府主導で進展。日本でもガイドライン確立は有効

●制御機器ベンダおよび事業者に対する啓発

－課題や対策の必要性に対する認識の向上が必要

●セキュリティ検証環境の整備

－対策を支援、実行するためのツール開発、テスト環境の提供

●国際協調の必要性

－国際標準化含め、グローバル化への対応が必要

ご清聴ありがとうございました。

「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」報告書

2009年3月　IPAウエブサイトで公開予定

IPA　セキュリティセンター