制御システムセキュリティセンター開設の経緯と目指すもの

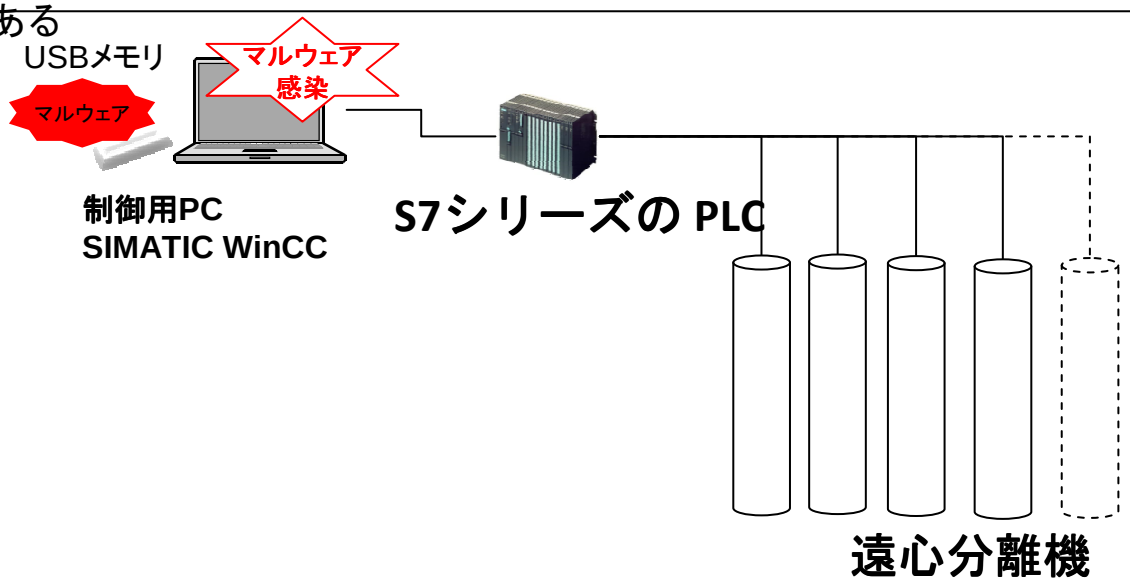
新　誠一
技術研究組合制御システムセキュリティセンター
理事長

Email: seiichi.shin@uec.ac.jp
http://www.css-center.or.jp/

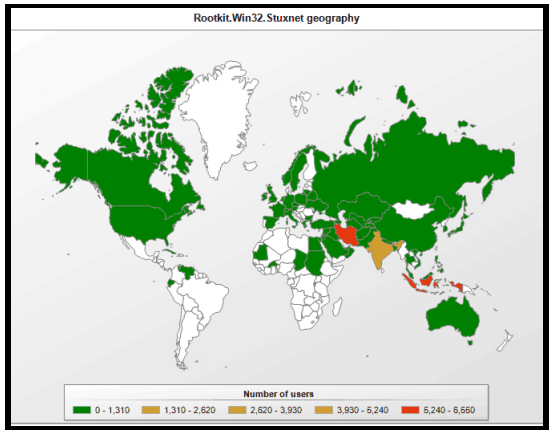
設立の背景

■Stuxnetの概要

・ 2010年9月に、イランのナタンズにある核燃料施設のウラン濃縮用遠心分離機を標的として、サイバー攻撃がなされた
・この攻撃は、4つの未知のWindowsの脆弱性を利用しており、PCの利用者がUSBメモリの内容をWindows Explorerで表示することにより感染する
・ウイルス開発費用は恐らく500万ドルから1000万ドルであり、核施設周辺を空爆するより安価であると言われている
・遠心分離機には過剰な負荷がかかり、20%が破壊されたと言われている
・一部では、Stuxnetは、イスラエルと米国が開発し攻撃を実行したと言われている
・イランの核開発計画は、Stuxnetにより大幅に遅れた（3年程度）との噂もある



シマンテック社が確認した感染数を各国別に示したもの



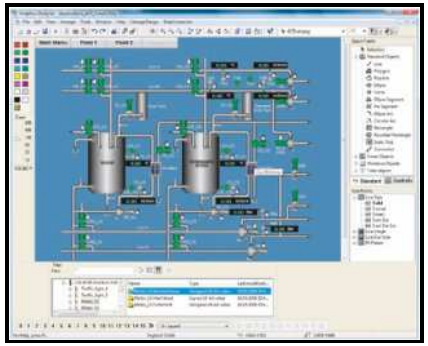
Source: http://ebiquity.umbc.edu/blogger/2010/09/23/is-stuxnet-a-cyb weapon-aimed-at-an-iranian-nuclear-site/

■Stuxnetの特徴

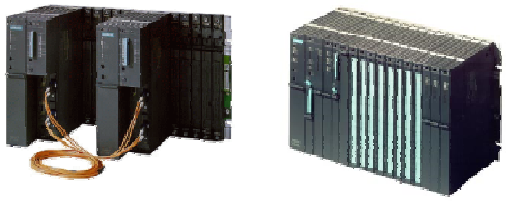
Stuxnet の標的は、「**独シーメンス社の SIMATIC WinCC とSIMATEC　PCS 7 制御されている制御システム**」である。

- **SIMATIC WinCC** とは、PLCの制御用PC向けのPCであり、シーメンス社製のPLC（Programmable Logic Controller）の S7 シリーズの制御PCに使用されることが多い。

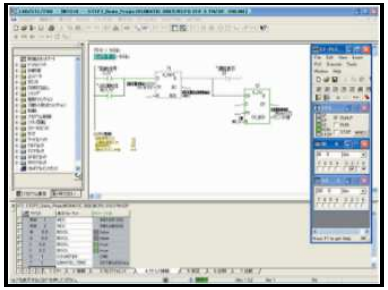
- **SIMATIC PCS 7**とは、SIMATEC WinCC の可視化ソフトウェア、STEP 7 設定ソフトウェアを統合ソリューションの総称である。



SIMATIC WinCC
の画面イメージ



S7シリーズの
PLC

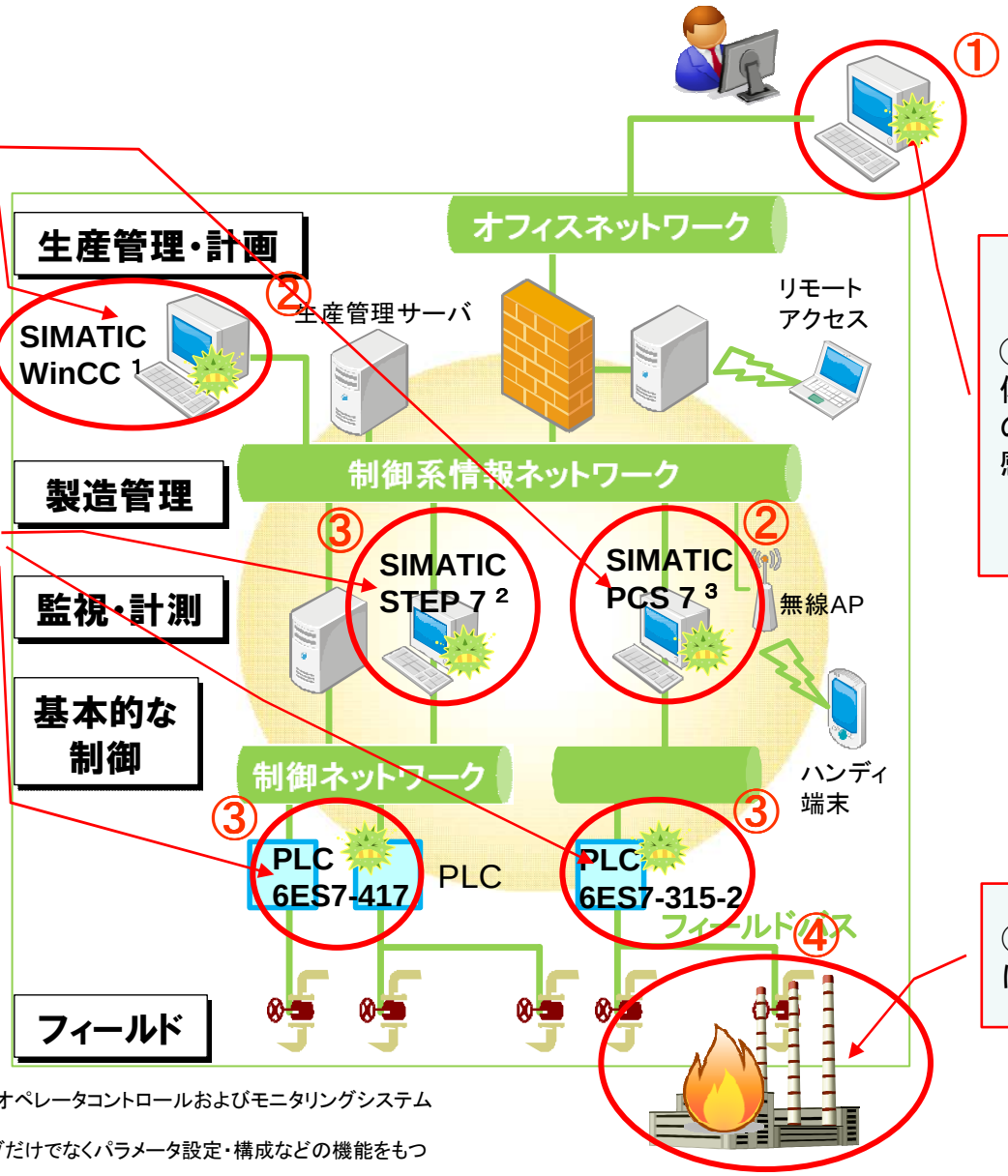


SIMATIC　STEP 7
の画面イメージ

■Stuxnetの攻撃手順

②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

③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



①USBメモリ等の外部記録媒体を経由して、スタックスネットのウィルスがウィンドウズOSに感染。

④制御システム上にある装置に対する攻撃の実行

1 SIMATIC WinCCは、PC ベースのオペレータコントロールおよびモニタリングシステムなどの機能をもつSCADAソフトウェア。
2 SIMATIC STEP 7は、プログラミングだけでなくパラメータ設定・構成などの機能をもつソフトウエア。
3 SIMATIC PCS7は、プロセス制御システム。

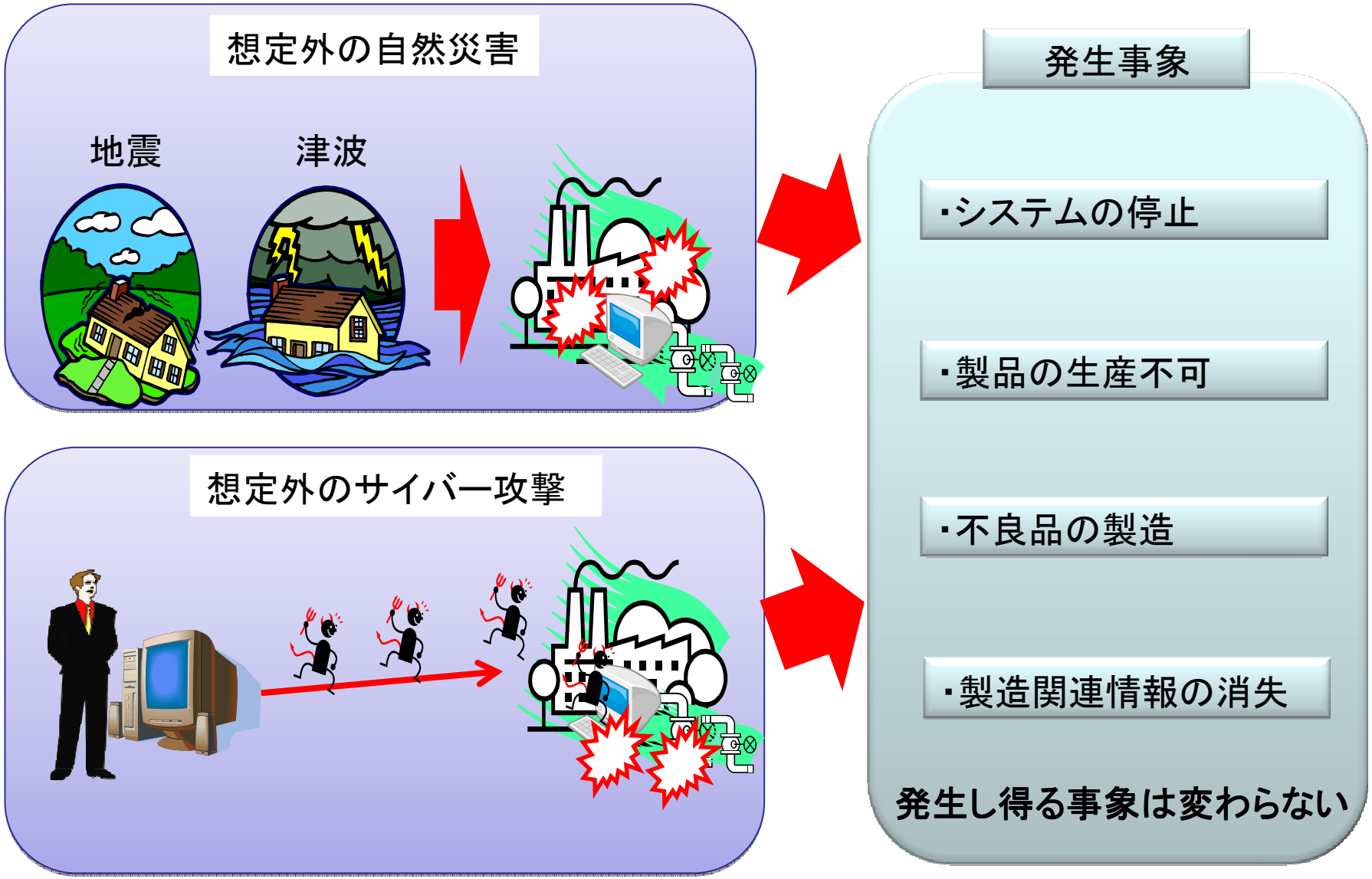
■神話の崩壊

- 非インターネット環境の神話崩壊
  USBおよびエンジニアリングツール経由の感染

- 非汎用OSは攻撃されないという神話崩壊
  特定OSを用いたコントローラを狙い撃ち

- 専門家善人神話崩壊
  エンジニアリングツールやコントローラの専門家の参加

自然災害とサイバー攻撃



経済産業省　サイバーセキュリティと経済研究会報告書より引用

制御系セキュリティ対策の難しさ

制御システムの特徴

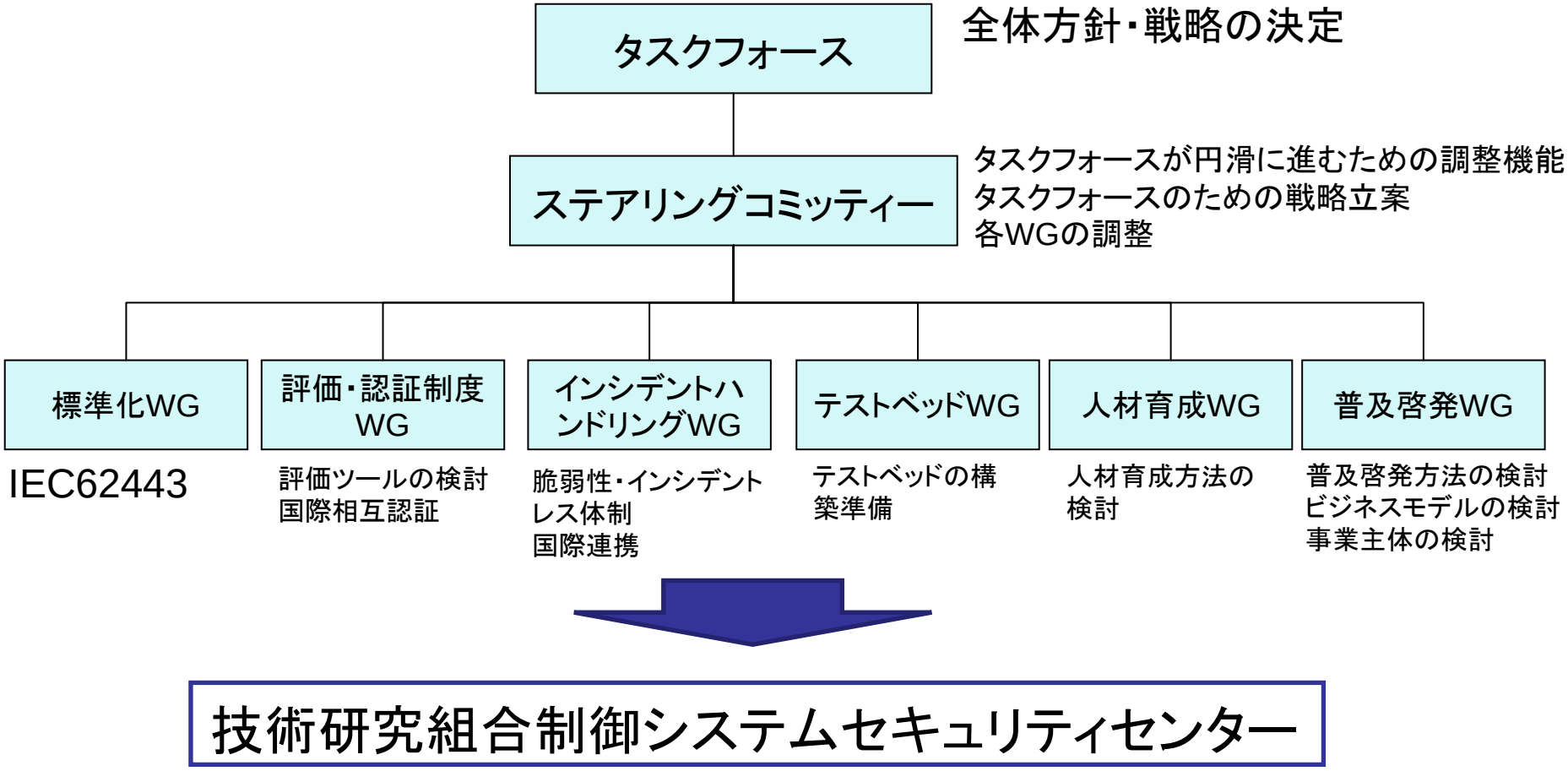
- 容易に止められない.
- 保有が長期.
  システムに実装されているソフトウェア、ハードウェアのアップグレード、入れ替え等が難しい。
- ソフトの暴走はメカの暴走

対　策

- クラウド，予備機によるシミュレーションの活用
- ソフトウェア，ハードウェアの新陳代謝化
- ハードも含んだシミュレーション

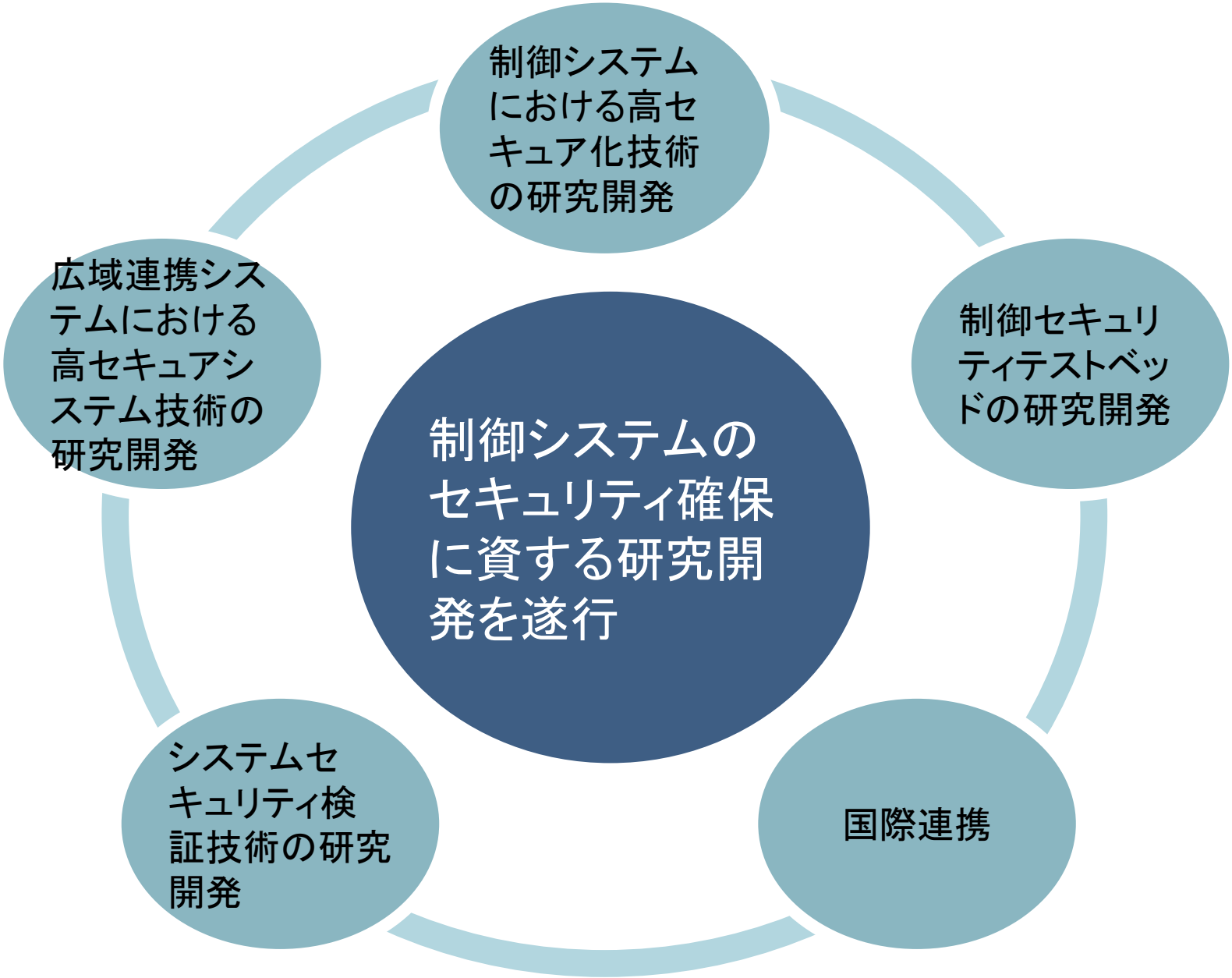
制御システムセキュリティ検討タスクフォース

- 経済産業省が主催。
- 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。



組合の概要

活動目的とアクティビティ



組織概要

設立日

2012年3月6日（登記完了日）

住所等

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

組合員

- 組合員（2012年6月13日現在）

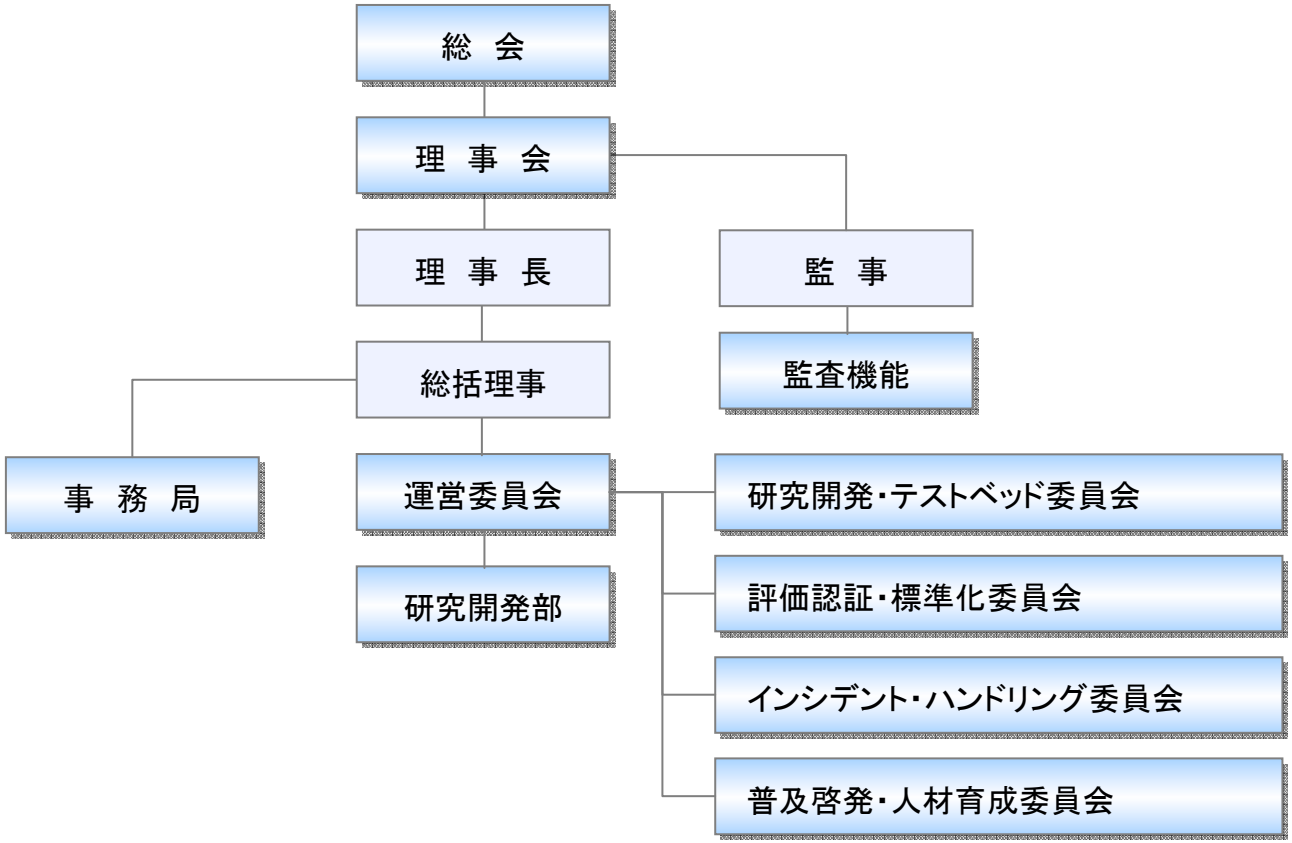
  独立行政法人産業技術総合研究所、独立行政法人情報処理推進機構、
  アズビル株式会社、NRIセキュアテクノロジーズ株式会社、株式会社東芝、
  富士電機株式会社、株式会社日立製作所、三菱重工業株式会社、
  株式会社三菱総合研究所、森ビル株式会社、横河電機株式会社、
- その他連携予定

  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

理事および監事等

理事長	新　誠一	国立大学法人電気通信大学　教授
総括理事	松井　俊浩	独立行政法人産業技術総合研究所 セキュアシステム研究部門長
理事	岩崎　雅人	アズビル株式会社　執行役員 アドバンスオートメーションカンパニー社長
理事	小西　信彰	横河電機株式会社　執行役員 IAプラットフォーム事業本部　システム事業部長
理事	齊藤　裕	株式会社日立製作所　執行役専務 インフラシステムグループ長　兼　インフラシステム社　社長
理事	平本　康治	三菱重工業株式会社　執行役員 エンジニアリング本部副本部長 兼　原動機事業本部副事業本部長
理事	竹中　章二	株式会社　東芝 執行役常務待遇 スマートコミュニティ事業統括部　首席技監
理事	森　浩生	森ビル株式会社　　専務執行役員
監事	稲垣　隆一	弁護士
顧問	小林　和真	倉敷芸術科学大学　教授
顧問	渡辺　研治	名古屋工業大学　教授
事務局長	村瀬　一郎	株式会社三菱総合研究所　情報通信政策研究本部　副本部長

組織体制



7/13現在　出向者5名

お台場本部

所在地:
東京都江東区青海2丁目4番7号
独立行政法人産業技術総合研究所
臨海副都心研究センター　別館8F

http://unit.aist.go.jp/waterfront/

多賀城拠点

http://www.sonycid.jp/profile/d_office.html

所在地:
宮城県多賀城市桜木3丁目4番1号
ソニー(株)仙台テクノロジーセンター敷地内
みやぎ復興パーク内

みやぎ復興パークとは
東日本大震災により被害を受けた東北地域のものづくり産業の復興及び新たな産業の創出・発展を図るための拠点

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

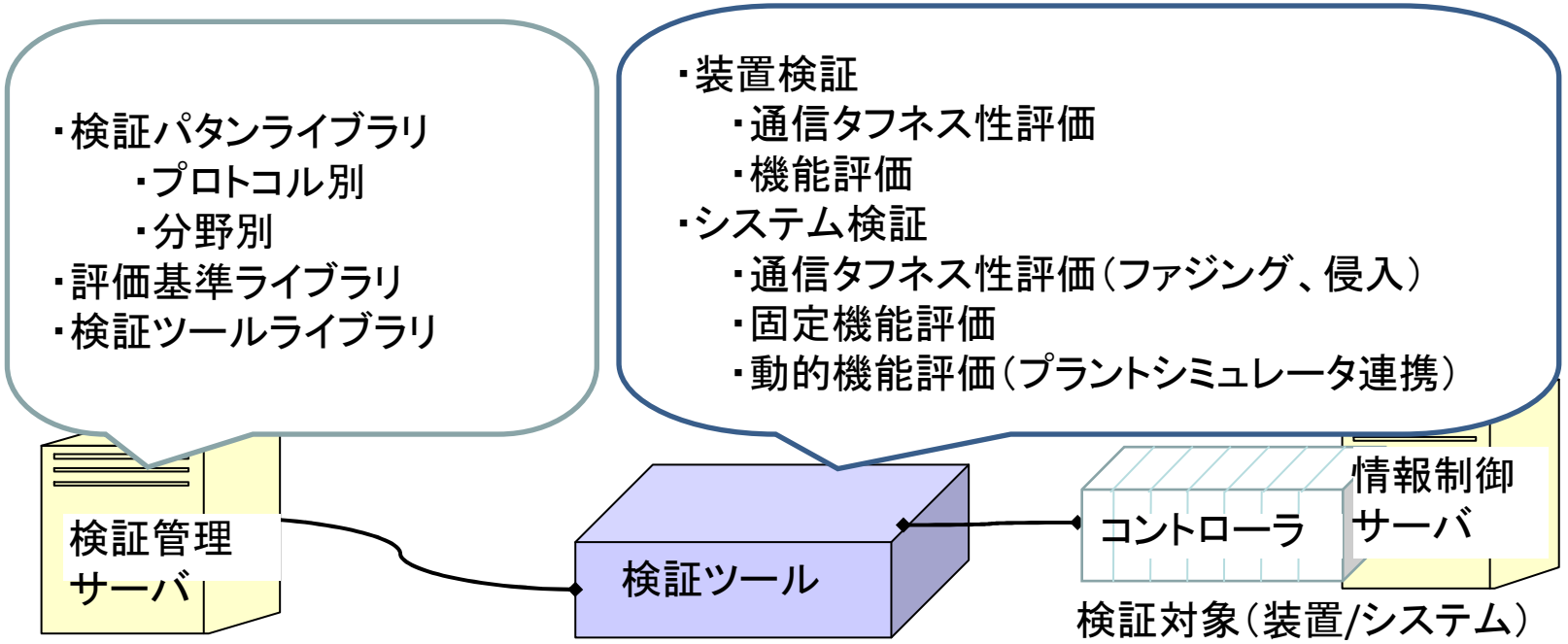
■狙う効果

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

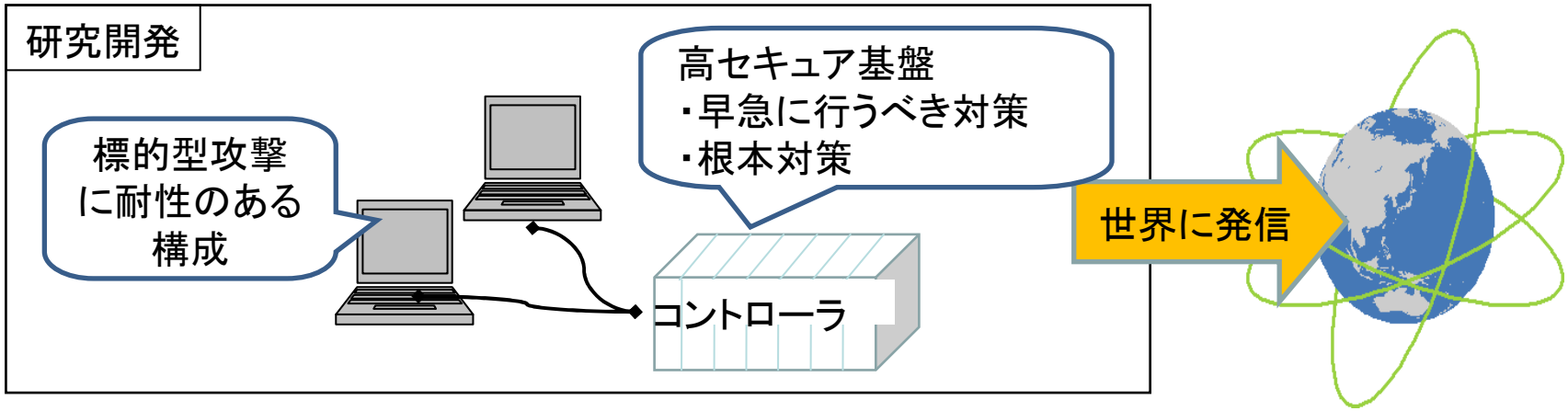


2. 高セキュア化構成・技術の研究開発

■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

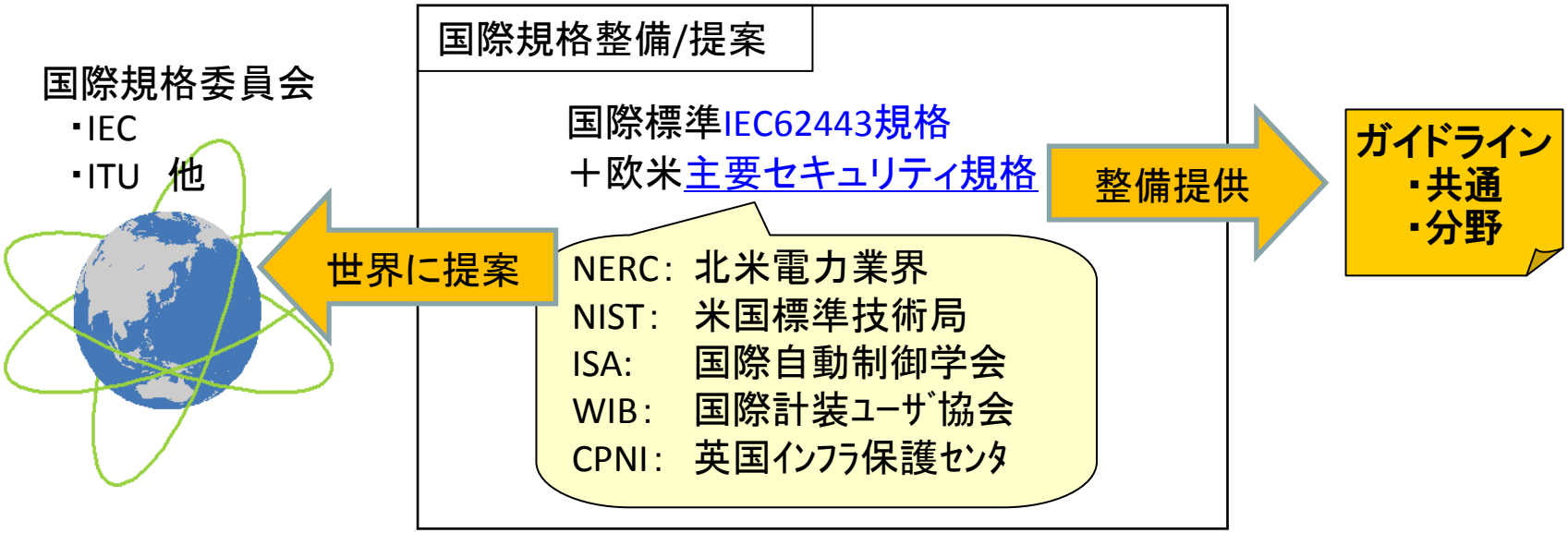


3. セキュリティ国際規格

■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



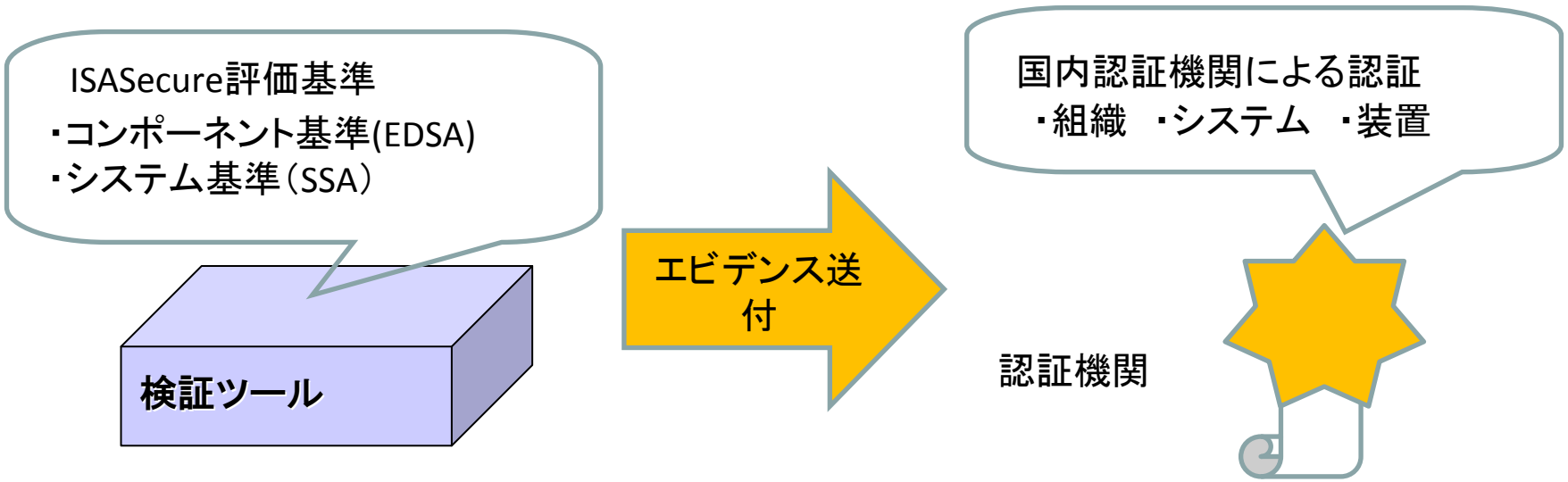
4. 国際規格準拠認証

■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

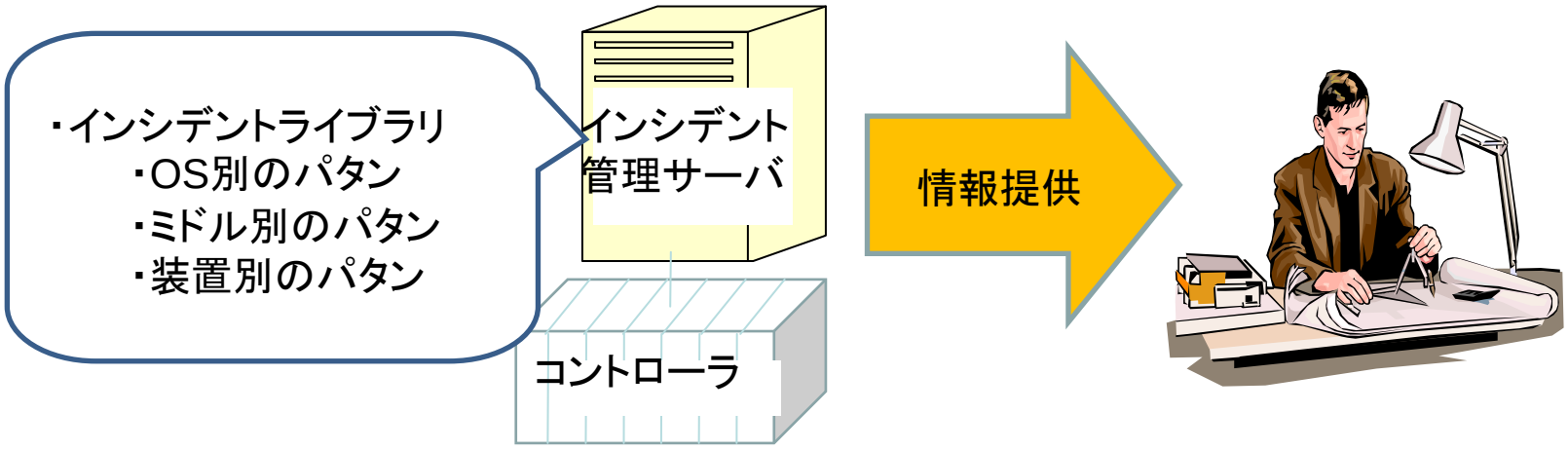


5. インシデントサポート

■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

情報セキュリティ教育カリキュラム

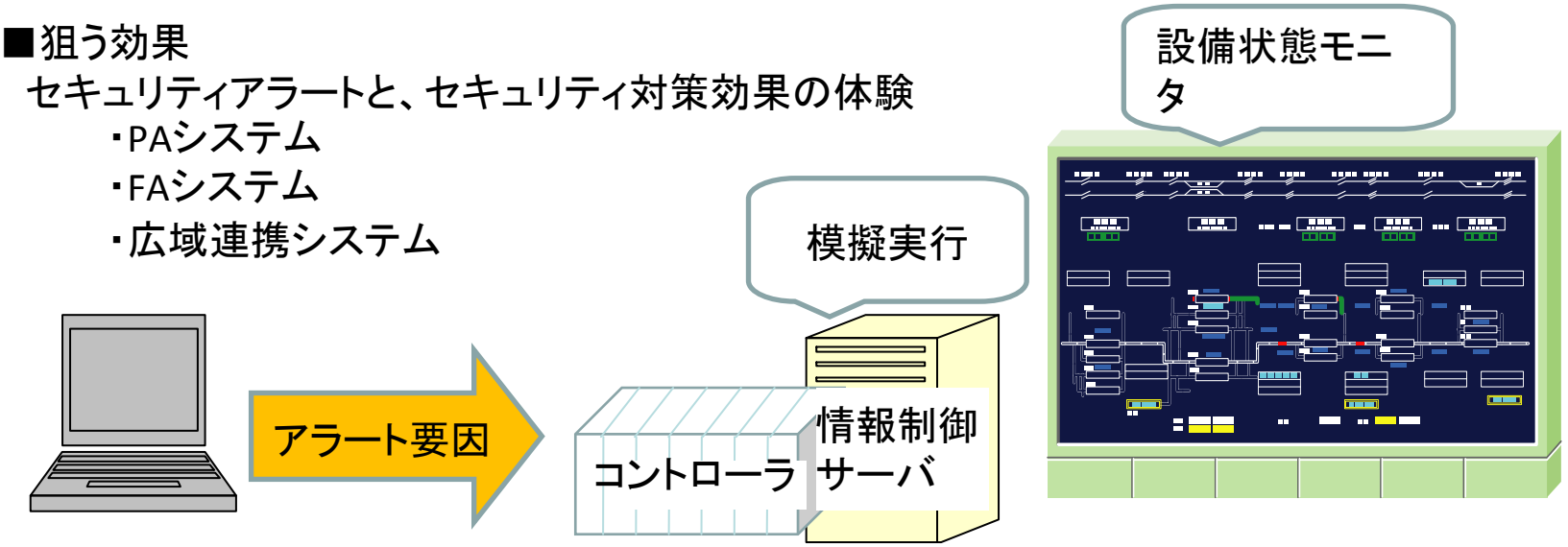
制御システム向け情報セキュリティ教育

7. 普及啓発

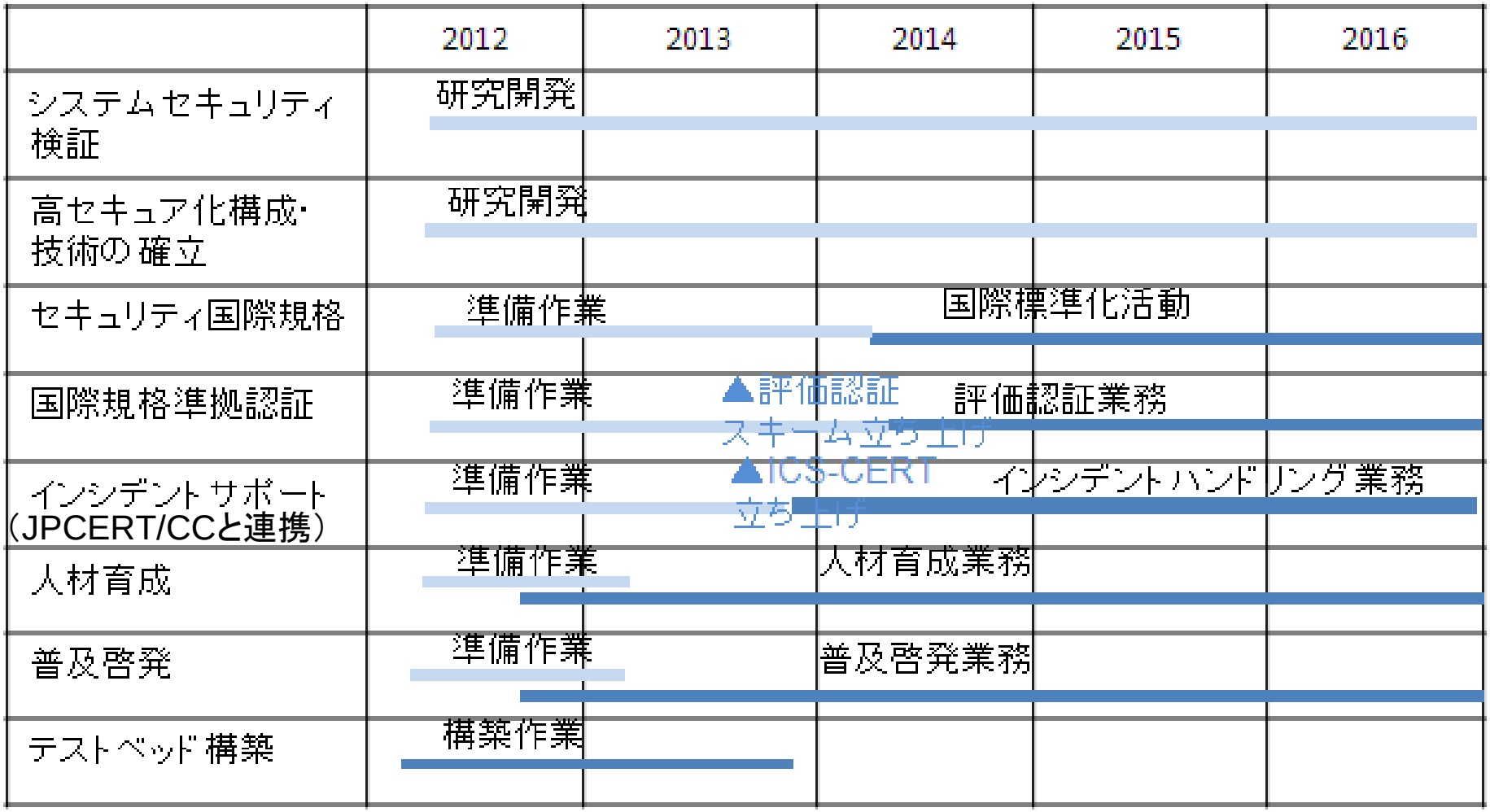
■狙う効果

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



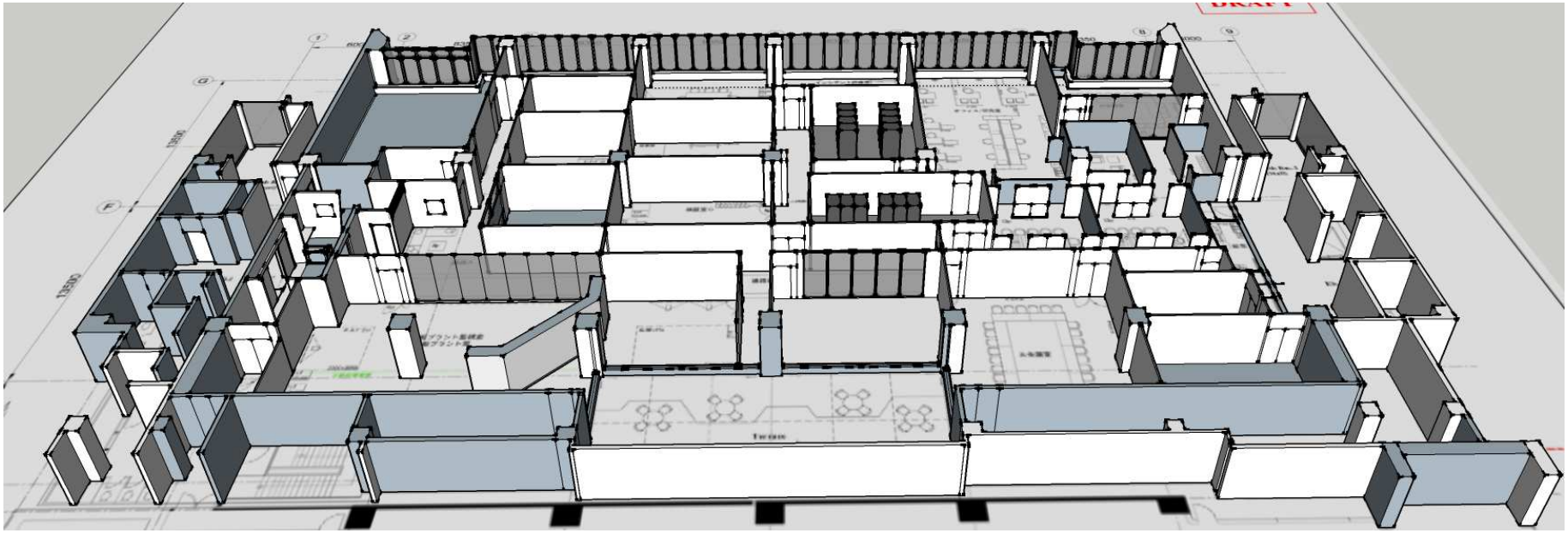
マイルストン


2012
2013
2014
2015
2016
システムセキュリティ検証
研究開発
高セキュア化構成・技術の確立
研究開発
セキュリティ国際規格
準備作業
国際標準化活動
国際規格準拠認証
準備作業
▲評価認証スキーム立ち上げ
評価認証業務
インシデントサポート（JPCERT/CCと連携）
準備作業
▲ICS-CERT立ち上げ
インシデントハンドリング業務
人材育成
準備作業
人材育成業務
普及啓発
準備作業
普及啓発業務
テストベッド構築
構築作業

委員会における活動内容

テストベッド・研究開発委員会

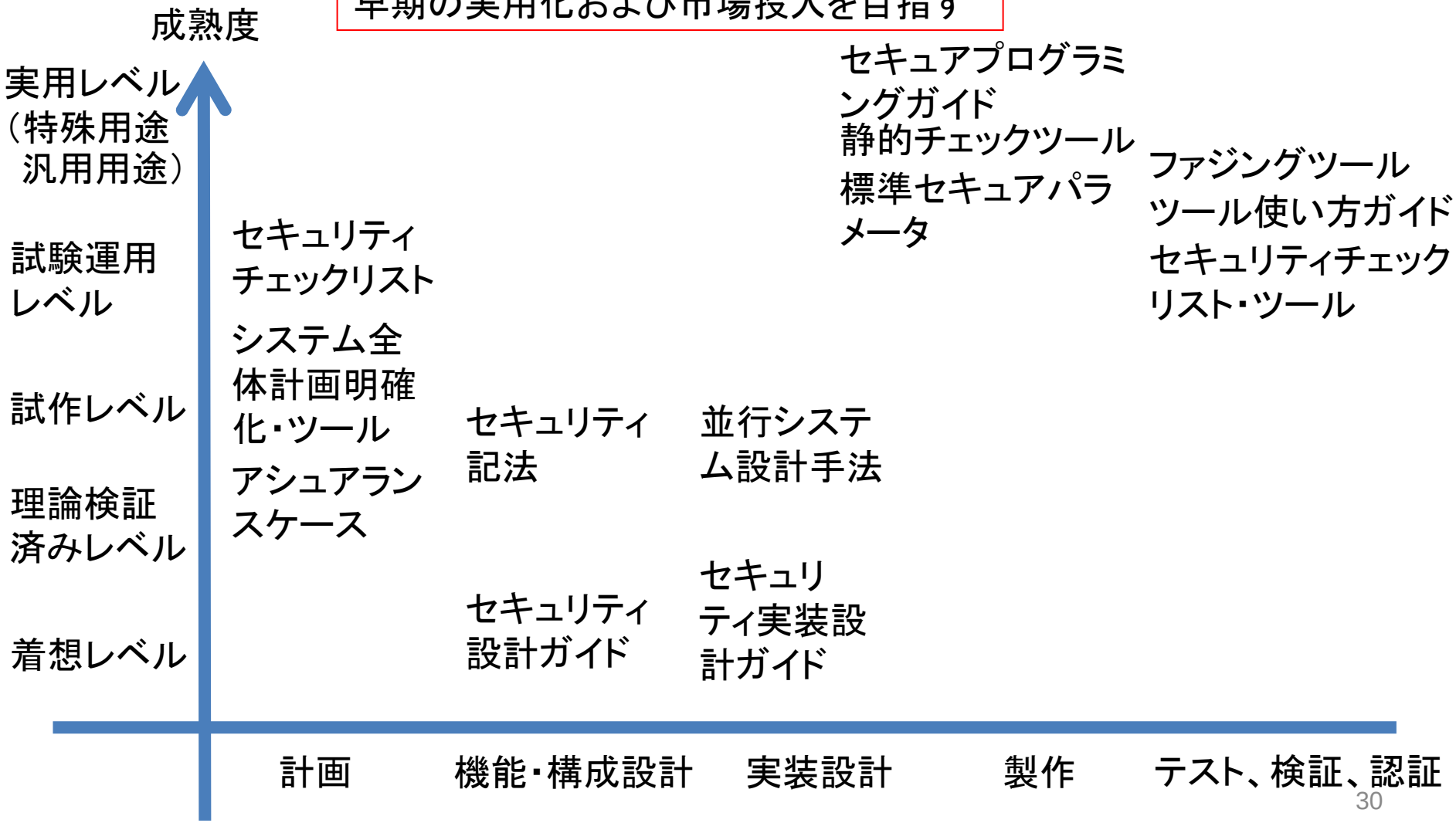
サイバーセキュリティテストベッドの設計



テストベッド・研究開発委員会

現在検討中の研究開発項目（開発プロセス）

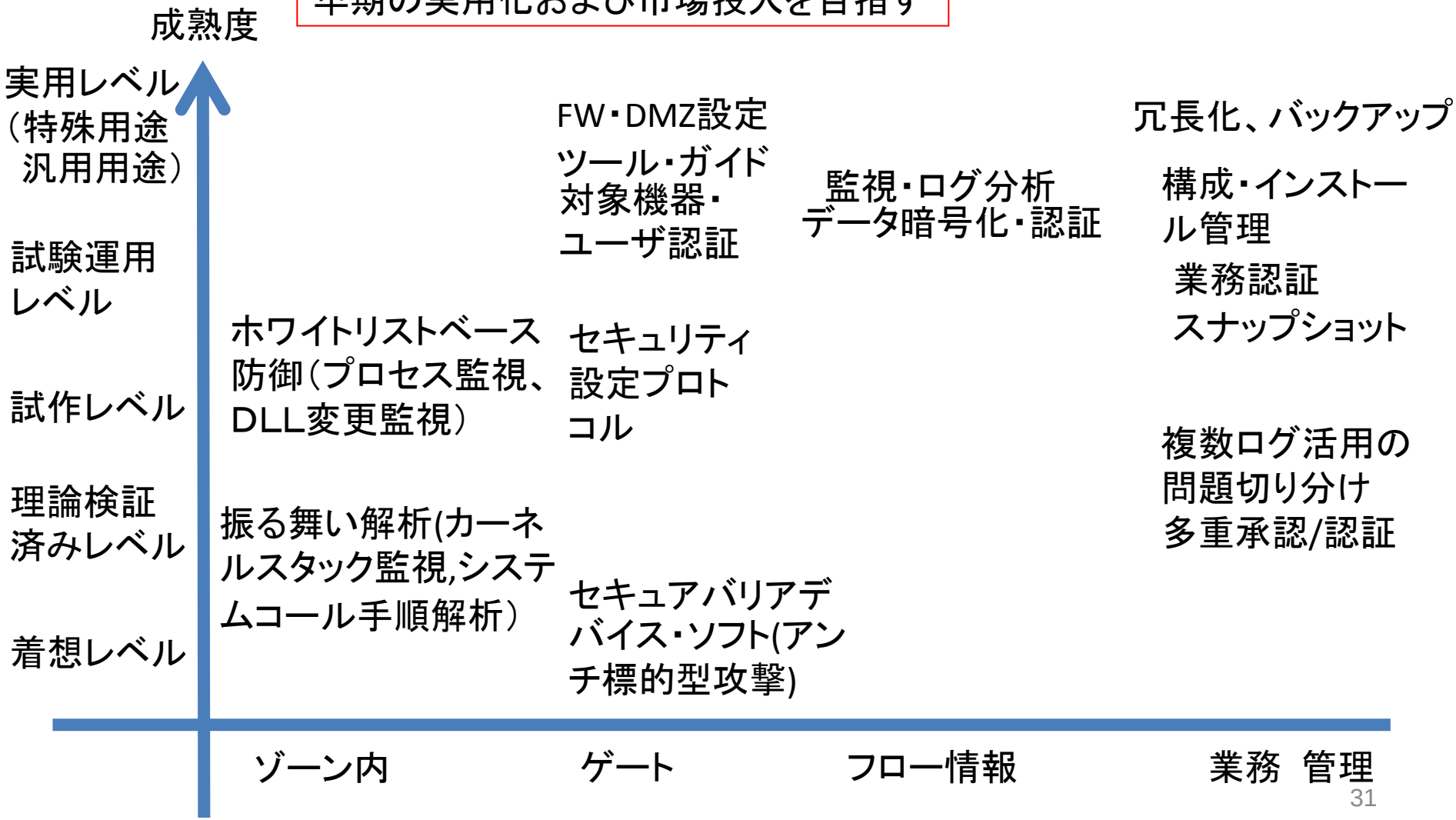
研究開発により対策技術成熟度を高め
早期の実用化および市場投入を目指す



テストベッド・研究開発委員会

現在検討中の研究開発項目（運用技術）

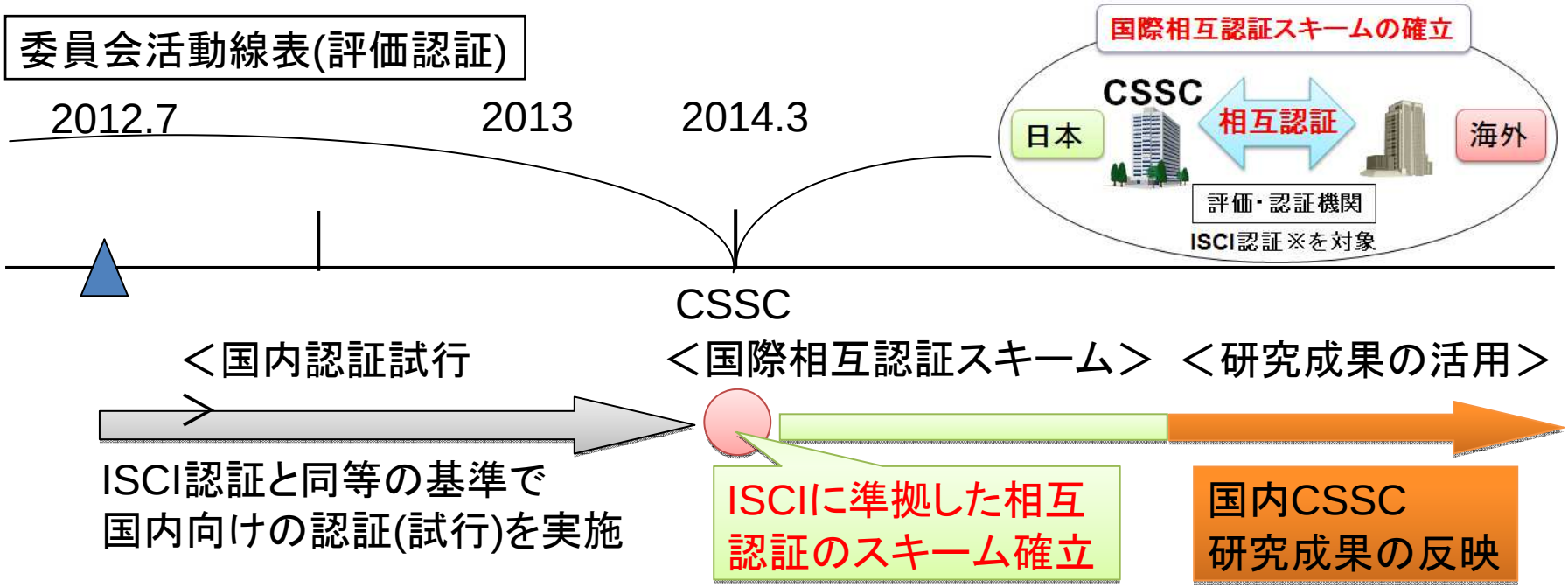
研究開発により対策技術成熟度を高め
早期の実用化および市場投入を目指す



評価認証・標準化委員会

主たる担当機関：アズビル、NRIセキュア、東芝、東芝ソリューション、日立、富士電機、横河、電通大、倉敷芸術科学大、AIST、IPA、(事務局)MRI
目標：制御システムのセキュリティに関する評価認証の国際相互認証のスキーム確立、及び標準化活動の実施
今後の取組みについては下記の線表を予定。

委員会活動線表(評価認証)



委員会活動線表(標準化)　CSSCウェブサイト抜粋

事業	2012年	2013年	2014年	2015年	2016年	2017年
セキュリティ国際規格	準備作業		国際標準化活動			

CSSC 普及啓発・人材育成委員会

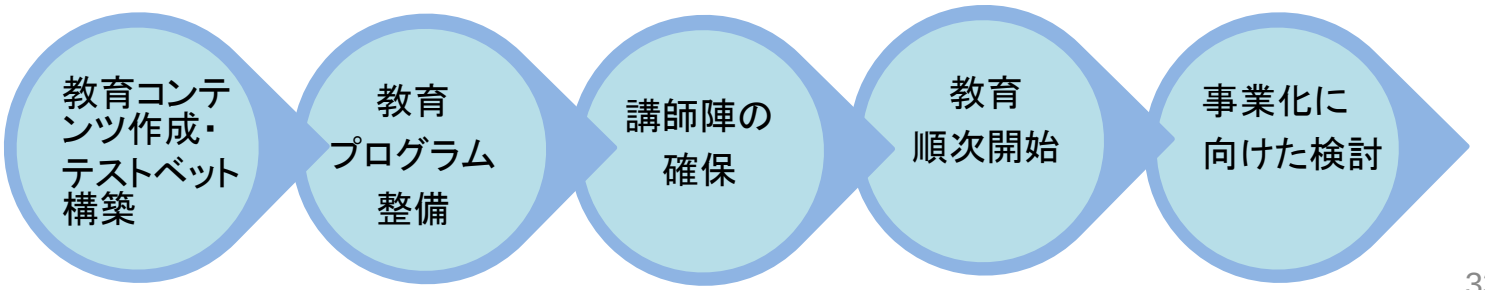
目　標　制御システム関係者の意識向上、スキルアップにより制御システムにおける情報セキュリティを確保し、安定した制御システムの操業に資する。

現場層向け(主にユーザー企業、ベンダー企業、Sier企業の責任者・エンジニア向け)
日々レベルアップするサイバー攻撃に対応できる現場のスペシャリストを育成する。

経営者層向け
経営者層が実際の被害や国際規格レベルでの技術向上を認識し、適切な経営資源の配分を行えるように啓発活動をおこなう。

具体的活動
1普及啓発・教育用コンテンツ・ルールの開発・実施
2テストベットを活用した実践的教育プログラムの整備・実施
3組合を運用していく上での人材育成

今後のマイルストン



CSSC インデントハンドリング委員会

主たる担当機関
アズビル セキュリティフライデー、NRIセキュア、東芝、日立製作所、富士電機、三菱重工業、横河電機、AIST、IPA

委員長
名古屋工業大学大学院 渡辺 研司 教授

目　標　技術研究組合制御システムセキュリティセンターにおいて、制御システムにおけるセキュリティインシデントハンドリングを行う場合に必要な技術を検討することを通して、関連の研究を推進する。

具体的活動
1.インシデントハンドリングに必要な技術の研究開発
① モニタリング技術の研究開発
② 改ざん防止技術の研究開発
③ 異常検知技術の研究開発
2.ICS-CERT との連携内容に係わる検討

事業	2012年	2013年	2014年	2015年	2016年	2017年
インシデントハンドリング技術の検討	研究開発					
		インシデント分析技術とインシデント分析設備の提供				

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、認証スキーム、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。