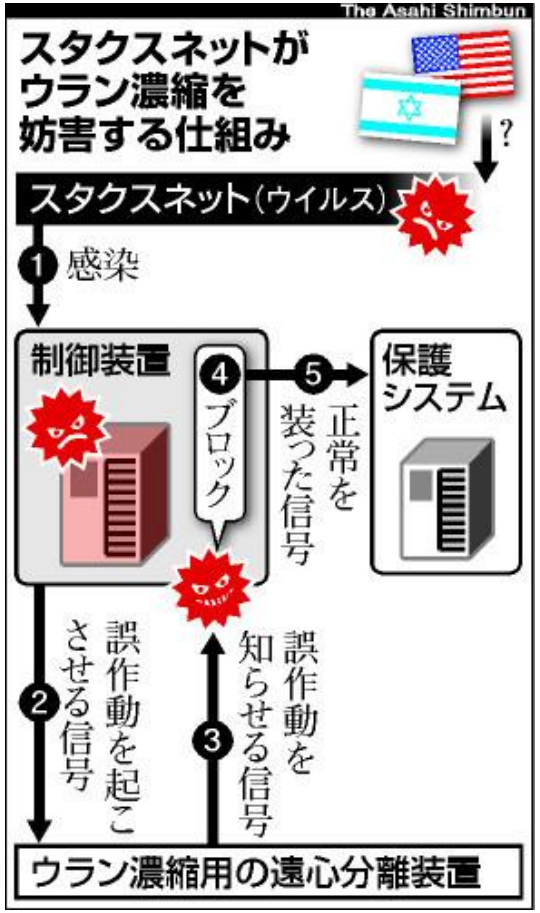
制御システムセキュリティ検討タスクフォースについて

新　誠一
電気通信大学

イラン核施設の妨害ウイルス イスラエルと米国が開発か



産業制御システムを乗っ取る新しいコンピューターウイルス「スタクスネット」が、国家が関与するサイバー攻撃の一環として開発された可能性が高まってきた。16日付の米紙ニューヨーク・タイムズは、イランのウラン濃縮を妨害する狙いで、イスラエルがスタクスネットの試験を行っていたと報じた。米国の核技術専門家らの証言などが根拠で、開発には米国も協力していたという。

http://www.asahi.com/international/update/0116/TKY201101160282.html

2011/1/17

STUXNET特徴

＜種類＞

- 亜種を含め4種類のバイナリが存在する
- サイズは、500～600KBぐらい
- 環境に応じて動作を変え、多様な形態をとって標的システムに展開する。

＜機能＞

- C&Cサーバ(Command and Control server)と通信して最新版にアップデート更新する
- Stuxnet同士でPeer to Peer通信してお互いのバージョンを確認し、古い方は新しい方からアップデート更新する機能がある。
- C&Cサーバからの指令をStuxnet同士で伝え合う。最新指令を伝達する機能がある。

PDF資料もご参考ください。

＜感染力＞

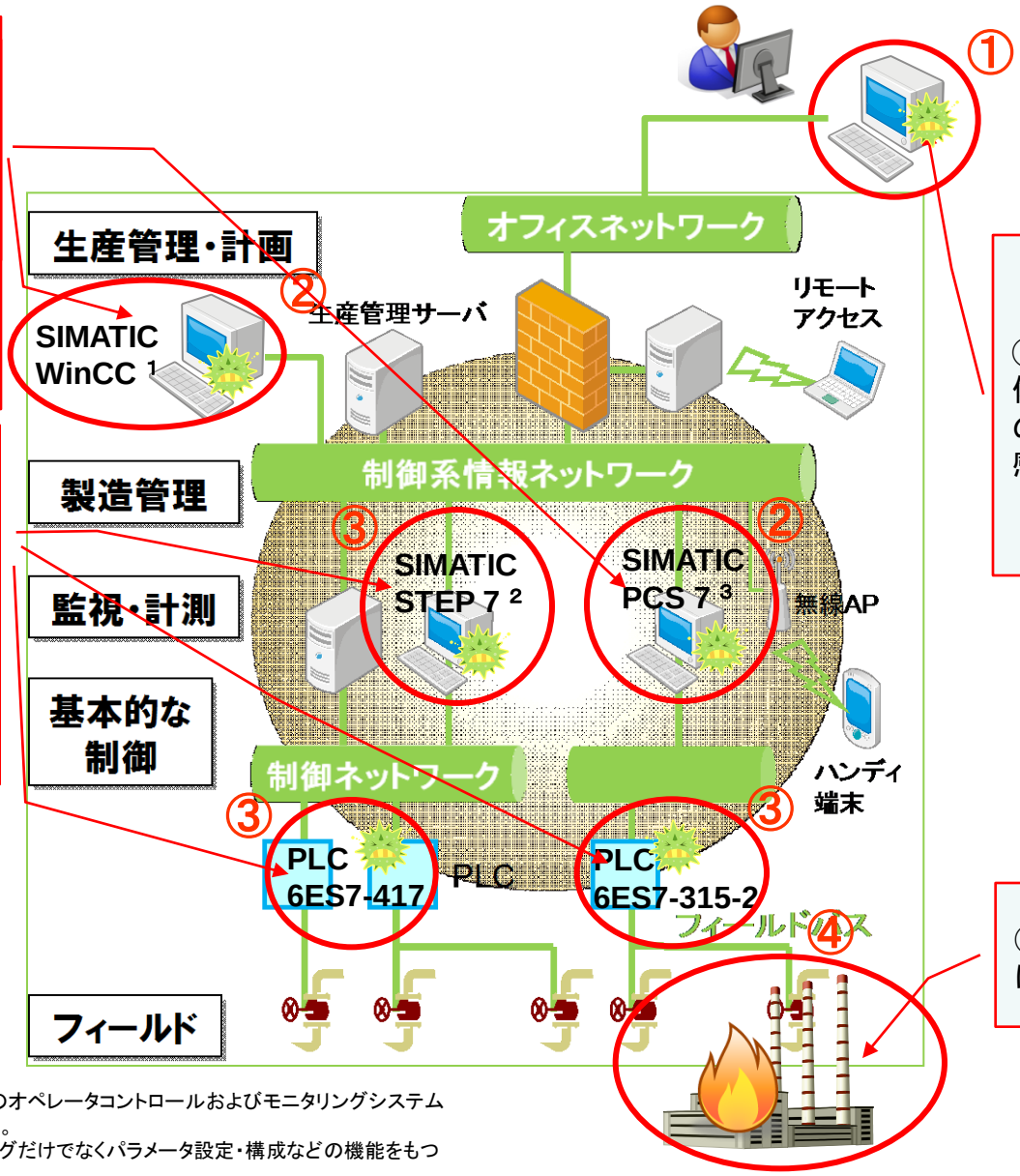
- Windowsの複数の脆弱性を利用して感染させる
  - Windowsシェルの脆弱性により、リモートでコードが実行される。(MS10-046)
  - 印刷スプーラーサービスの脆弱性により、リモートでコードが実行される(MS10-061)
  - Serverサービスの脆弱性により、リモートコードが実行される(MS08-067)
  - Windowsカーネルモードドライバの脆弱性により、特権が昇格される(MS10-073)
  - タスクスケジューラの脆弱性により、特権が昇格される(MS10-092)
- 転移方法は、インターネットだけでなく、USBメモリなどの媒体を経由しながら感染度は高い
- 感染PCの範囲は拡大している　Windows－2000、XP,2003,Vista、Server2007／2008

http://www.vec-member.com/salon/111/salon111.htm

～想定外の攻撃発生　2010年Stuxnet攻撃例～

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

東日本で巨大地震
東北M8.8、国内最大
死者・不明多数、津波で街壊滅

11日午後2時46分、東北・三陸沖を震源とする国内観測史上最大のマグニチュード（M）8.8の極めて強い地震が起き、宮城県北部で震度7を観測した。

http://www.nikkei.com/paper/article/g=96959
99693819695E3E3E2EBE48DE3E3E2E1E0E2E3E
39F9FEAE2E2E2;b=20110312

2011/3/13

経済産業省
情報セキュリティ対策室

商務情報政策局

サイバーセキュリティと経済　研究会

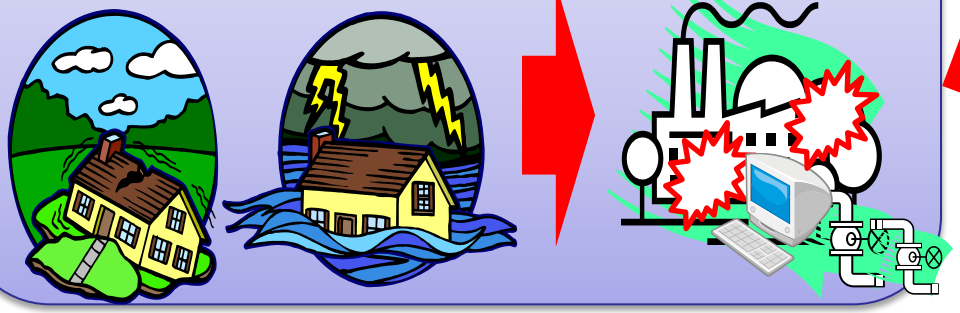
平成22年12月20日	第1回	第1回 議事要旨	第1回 配付資料
	第2回（非公開）		
平成23年3月3日	第3回	第3回 議事要旨	第3回 配付資料

http://www.meti.go.jp/committee/kenkyukai/k_8.html

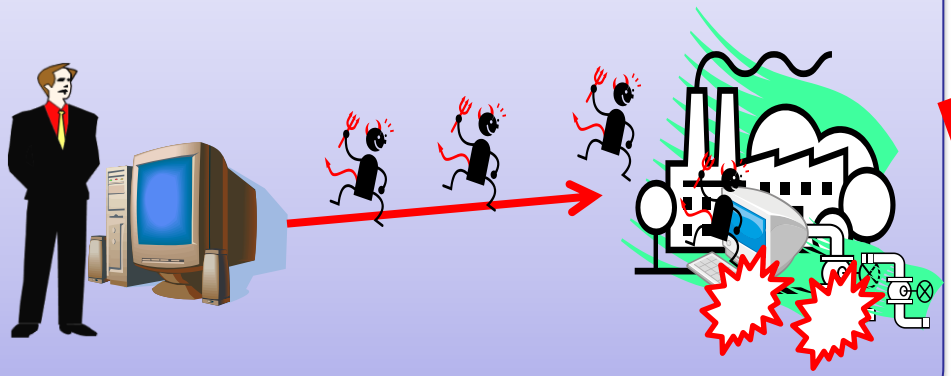
自然災害とサイバー攻撃

想定外の自然災害

地震　津波



想定外のサイバー攻撃



発生事象

・システムの停止

・製品の生産不可

・不良品の製造

・製造関連情報の消失

発生し得る事象は変わらない

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

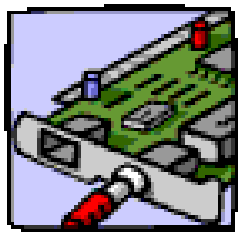
- クラウド，予備機によるシミュレーションの活用
- ソフトウェア，ハードウェアの新陳代謝化
- ハードも含んだシミュレーション

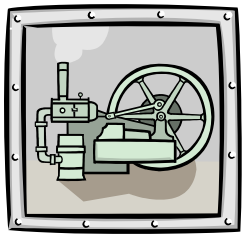
制御システム

- システムは要素の結合
- 要素は同一または異なる
- 要素は結合可能，交換可能


人


ソフト


エレキ


メカ


素材

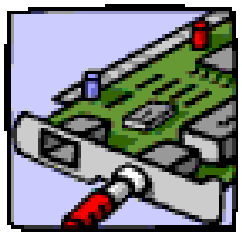
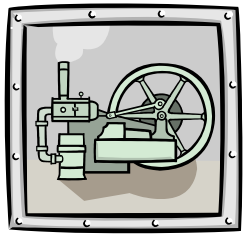

環境

IT

仮想

モデル

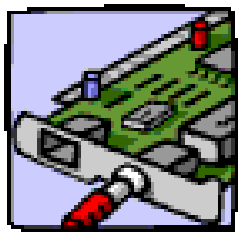
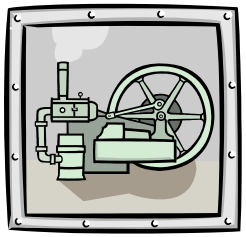


現実

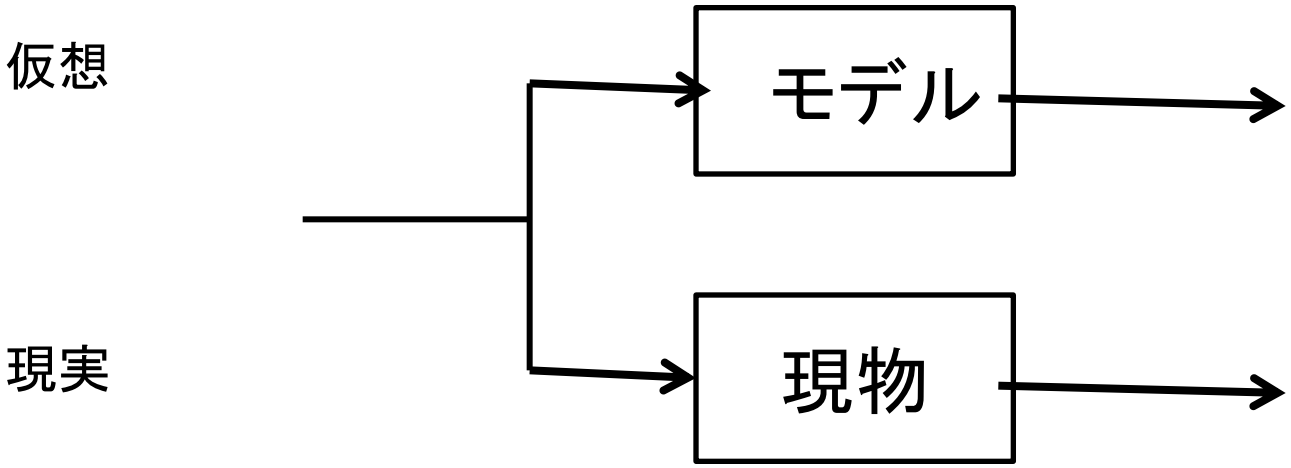
現物



人　ソフト　エレキ　メカ　素材　環境

対策1：振る舞い監視

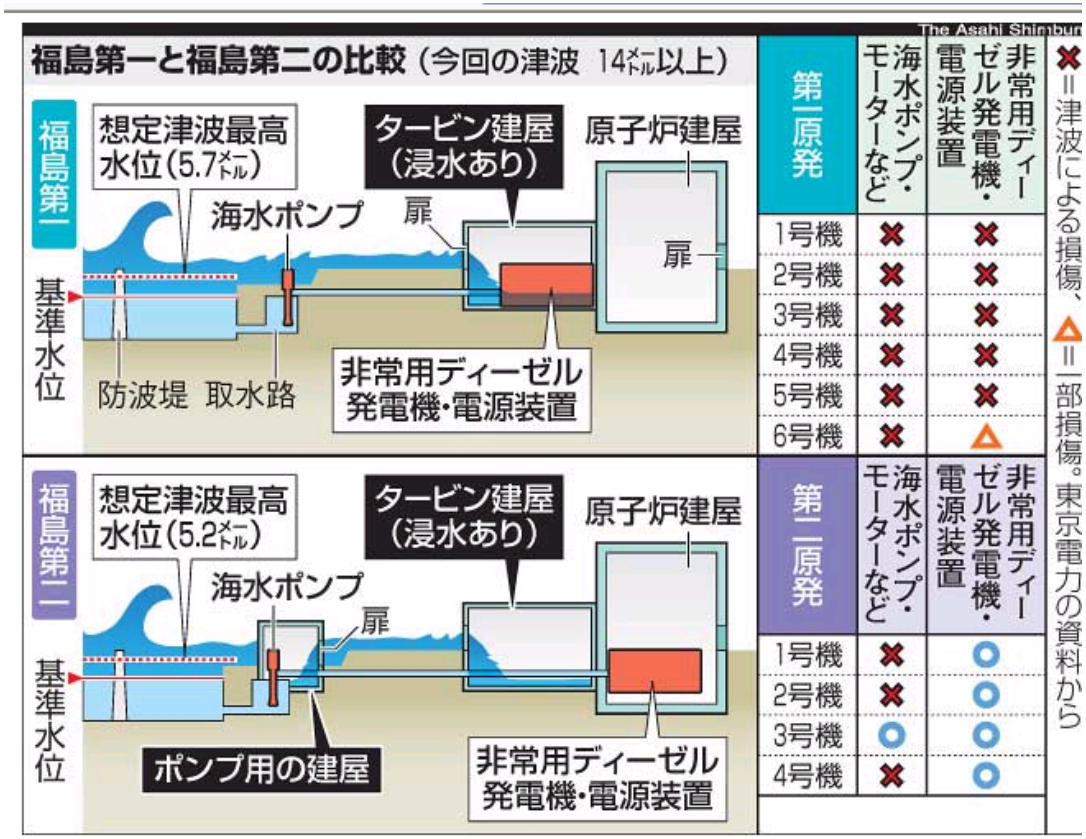


- モデル上での検証
- 現物とモデルの一致性検証

- モデル群の振る舞いと現物群の振る舞いの一致性検証

身元保証から振る舞い監視へ

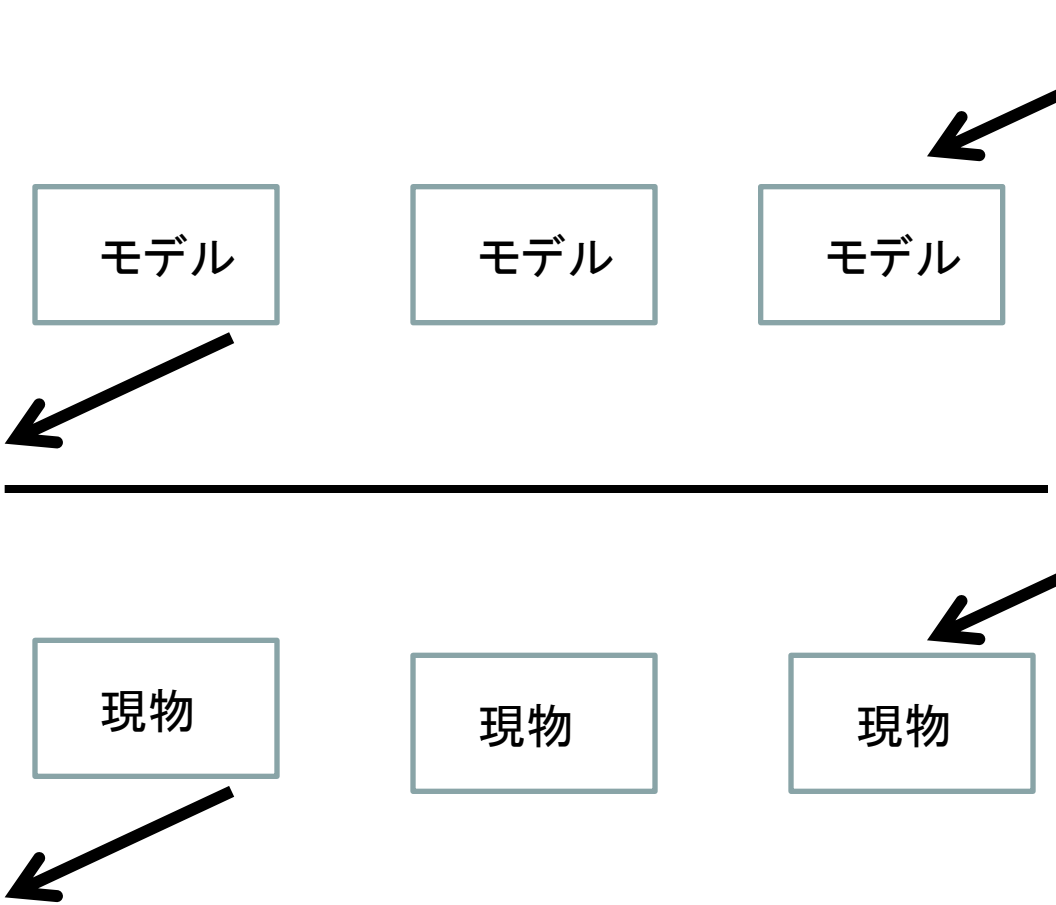
福島第1，第2原発の比較



http://www.asahi.com/photonews/gallery/infographics3/110406jiko01.html

2011/4/9

対策2:開発ツールのオンライン利用



Processor In the Loop Simulation
(プロセッサーまでも仮想化したシミュレーション)

Software In the Loop Simulation
（全て仮想世界におけるシミュレーション）

Hardware In the Loop Simulation
(現物も含んだシミュレーション)

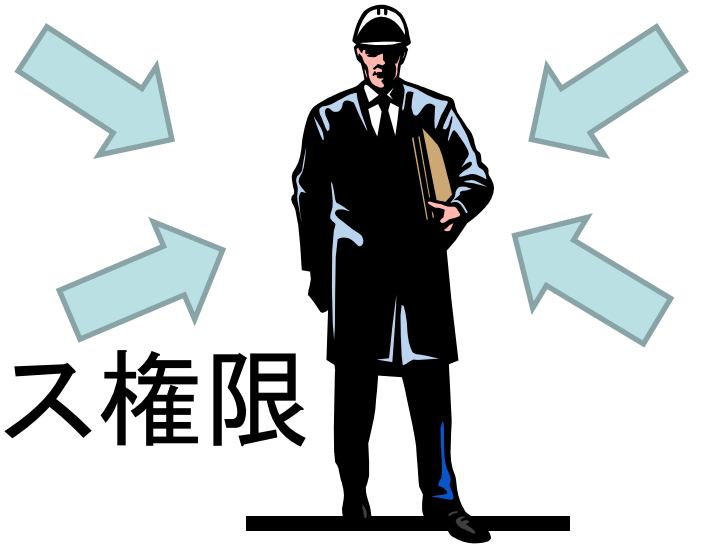
マルチベンダーによる複数コントローラの動作検証

国際標準化の必要性

対策3：専門家集団養成

インシデント情報

セキュリティツール



アクセス権限

十分な待遇

基礎力
（情報，制御，ドメイン）

「制御システムセキュリティセンター（CSSC）（仮称）」

1. 背景

制御システムに対するサイバー攻撃への対処は、国家の安全保障、危機管理上重要な課題である。セキュリティが確保されない場合、制御システムの停止、エネルギー使用状況等の機密情報漏洩等が発生する可能性が顕在化する。

海外では、制御システムセキュリティに対する国際規格の整備が進み、またこれに基づく認証制度が確立されてきており、インフラシステム輸出に対する貿易障壁となる可能性がでてきている。

２．目的

本技術研究組合は、制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証にいたるまで一貫して業務を遂行する。

・制御システムにおけるセキュリティ確保の第３者検証手法の確立。

・検証手法に基づく制御システムセキュリティの検証実施。

・制御システムを高セキュア化するための構成および技術に関する研究開発。

・国際規格に基づく認証のための環境整備。

・制御システムセキュリティのインシデント対応、人材育成・啓発推進。

3. 事業内容

	項目	概要
1	システムセキュリティ検証	検証手法確立、実システム、コンポーネントの評価実施、
2	高セキュア化構成・技術の確立	制御システム向けセキュア構成および技術の確立
3	セキュリティ国際規格	戦略的な国際標準化活動と国内展開
4	国際規格準拠認証	国際規格準拠の認証ツール開発と、基準整備
5	インシデントサポート	インシデント情報の収集、管理、対策サポート
6	人材育成	制御エンジニア向けセキュリティスキル教育
7	普及啓発	セキュリティアラート体験、ガイドライン提供

4. 経緯

2010/12 → 2011/8 「サイバーセキュリティと経済」研究会
座長：村井　純（慶応）

2011/10 → 2012/3(予) 「制御システムセキュリティ検討タスクフォース」（TF）
座長：新　誠一（電気通信大）

WG事務局体制
ステコミ
標準化WG
評価認証WG
ｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞWG
ﾃｽﾄﾍﾞｯﾄﾞWG
人材教育WG
普及啓発 WG

施策実施環境の検討

現状	課題
①サイバー攻撃による影響が把握できない。 ②対策レベルを検証できない。 ③コンポーネント/デバイスの組み合わせた相互接続性の検証は出来ない。	①テストベッド要求仕様の策定。 ②テストベッド構想、環境の策定。 ③運営主体の策定 ➢ 継続的にサポート運営していく体制。 ④国際連携

2011/11/22 三次補正 → 2012/1 補正予算執行開始

「産学官連携ｻｲﾊﾞｰｾｷｭﾘﾃｨ ｺﾝｿｰｼｱﾑ（技術研究組合）」

５．発起人　６．費用負担

５．設立準備会の発起人

・代表　　：　電気通信大学　新　誠一　教授

・事務局　　：　（社）日本能率協会内

ものつくり支援事業ユニット

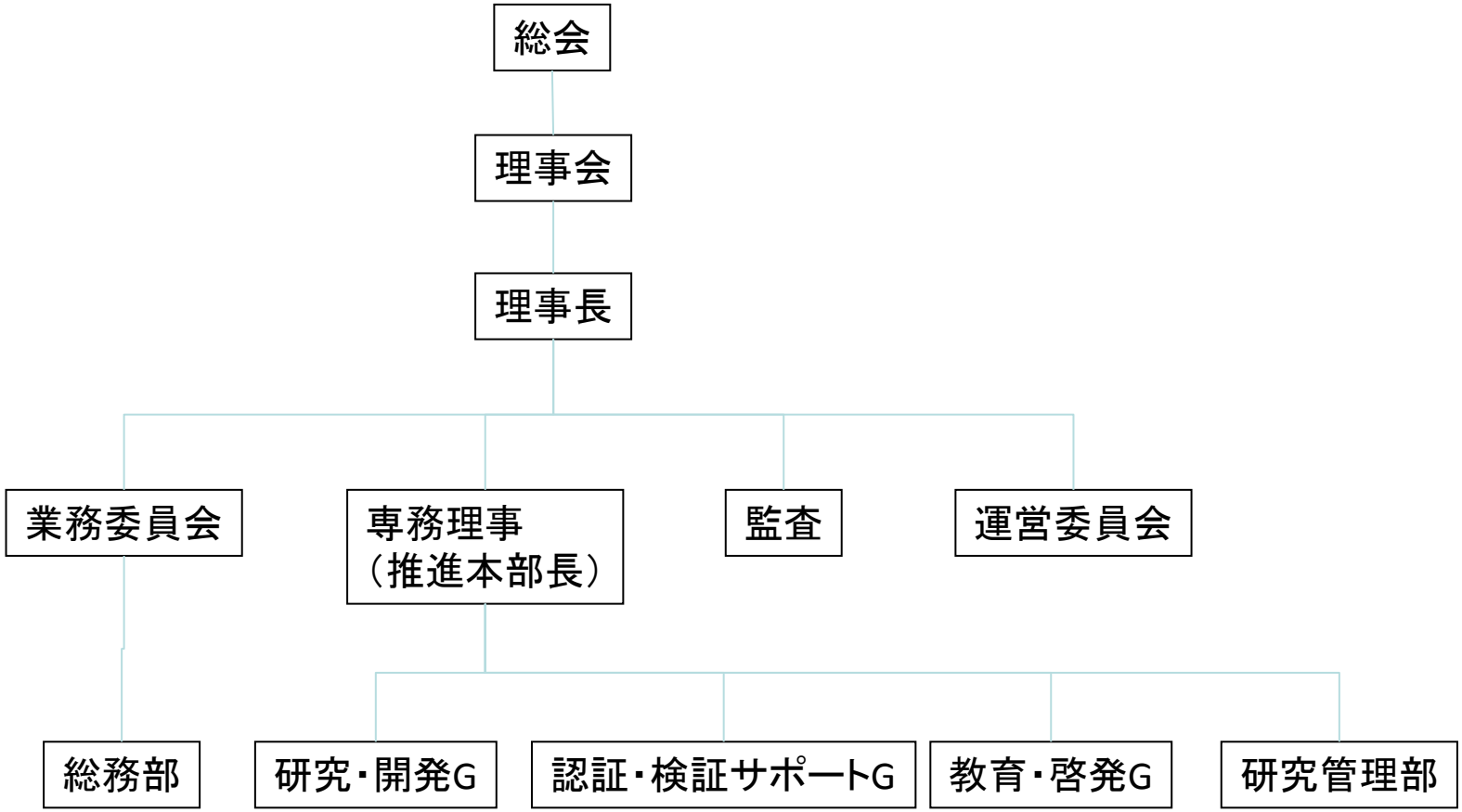
吉野　生也　氏　、　中澤　清　氏

６．費用負担方法（仮）

・経済産業省からの研究委託事業公募への応募と受託

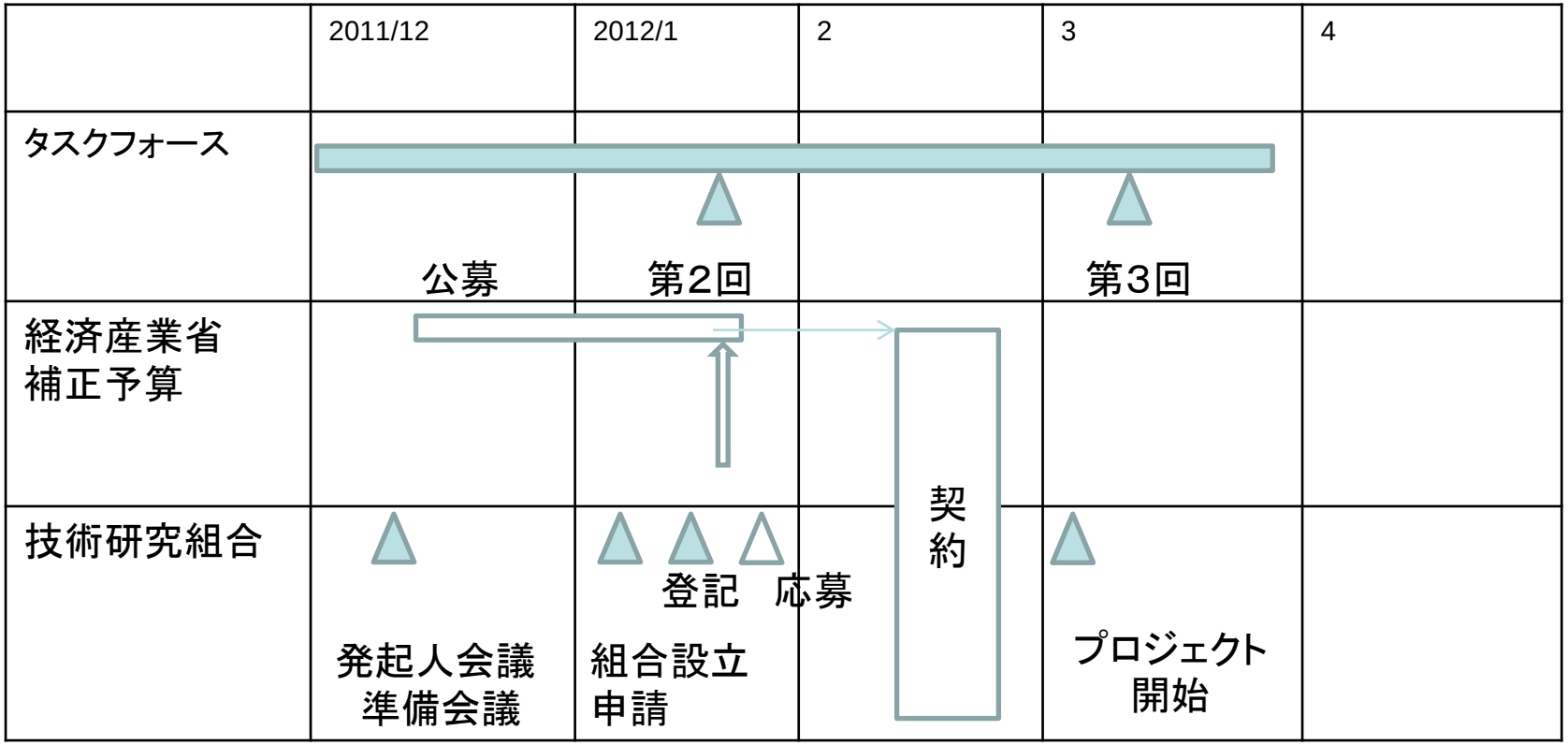
・各組員からの賦課金

「7．技術研究組合体制(仮)



・総務　・財務　・資材　・保安

９．スケジュール（予定）

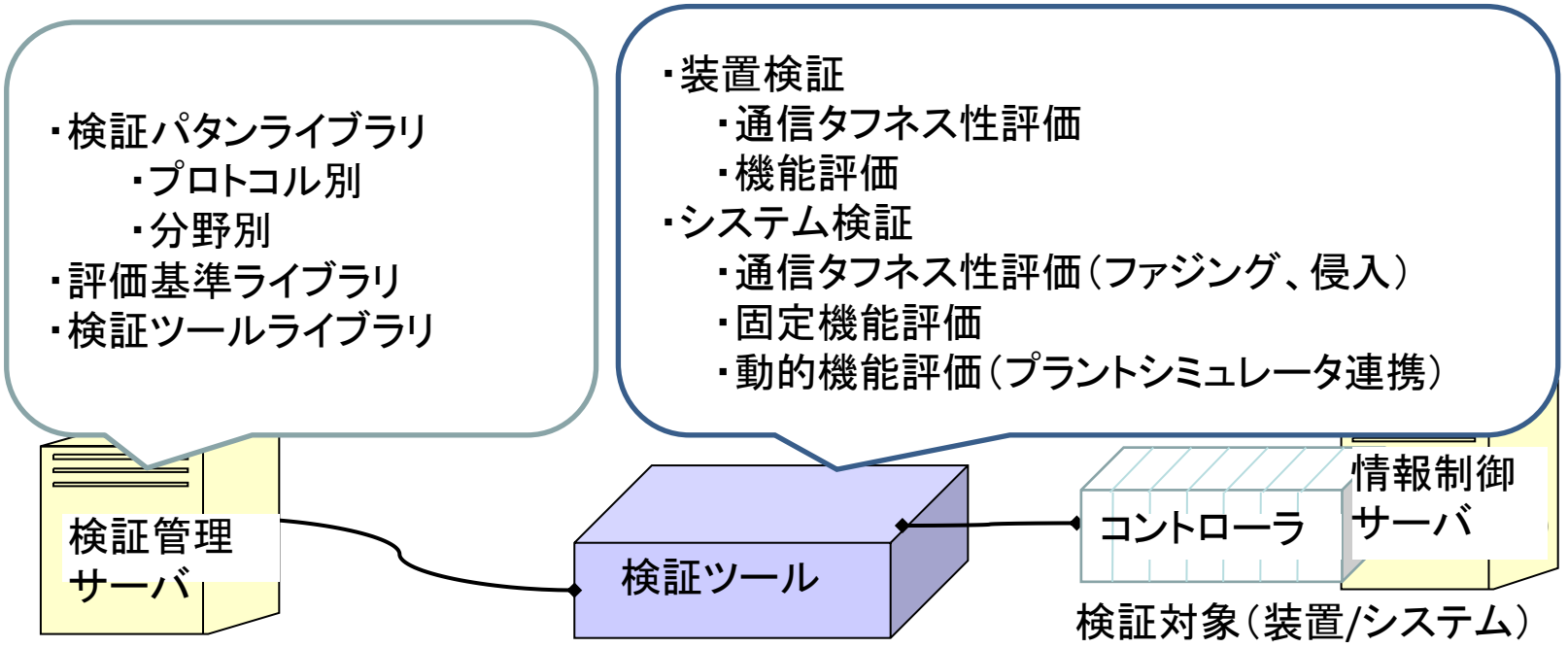

2011/12
2012/1
2
3
4
タスクフォース
公募
第2回
第3回
経済産業省
補正予算
契約
技術研究組合
登記　応募
発起人会議
準備会議
組合設立
申請
プロジェクト
開始

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

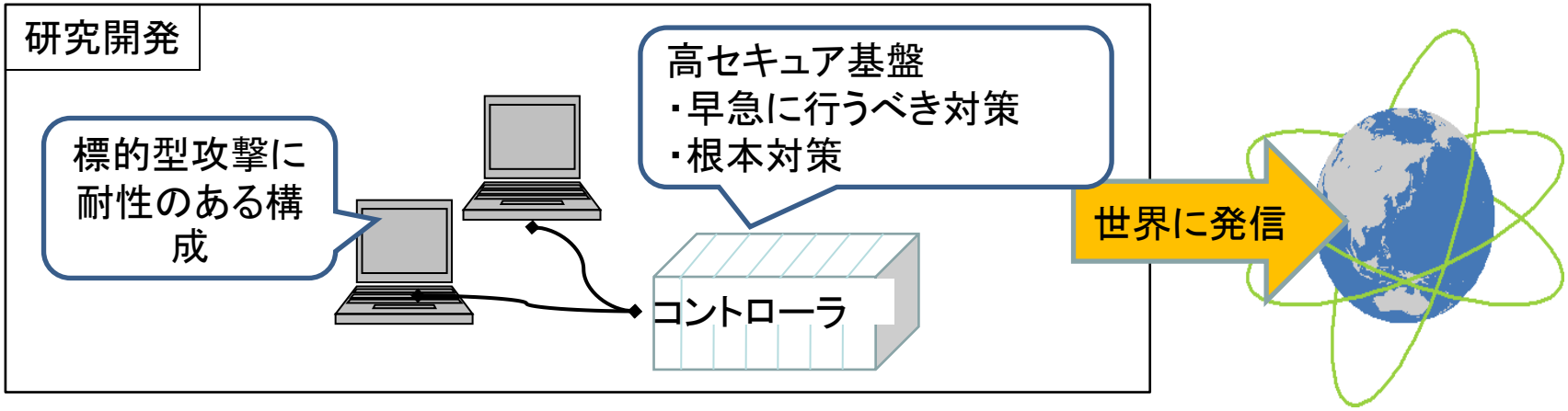


2. 高セキュア化構成・技術の研究開発

■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

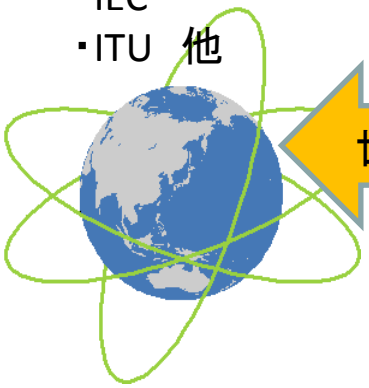
■狙う効果

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

国際規格委員会

- ・IEC
- ・ITU　他



世界に提案

国際規格整備/提案

国際標準IEC62443規格
＋欧米主要セキュリティ規格

NERC：北米電力業界
NIST：米国標準技術局
ISA：国際自動制御学会
WIB：国際計装ユーザ協会
CPNI：英国インフラ保護センタ

整備提供

ガイドライン
・共通
・分野

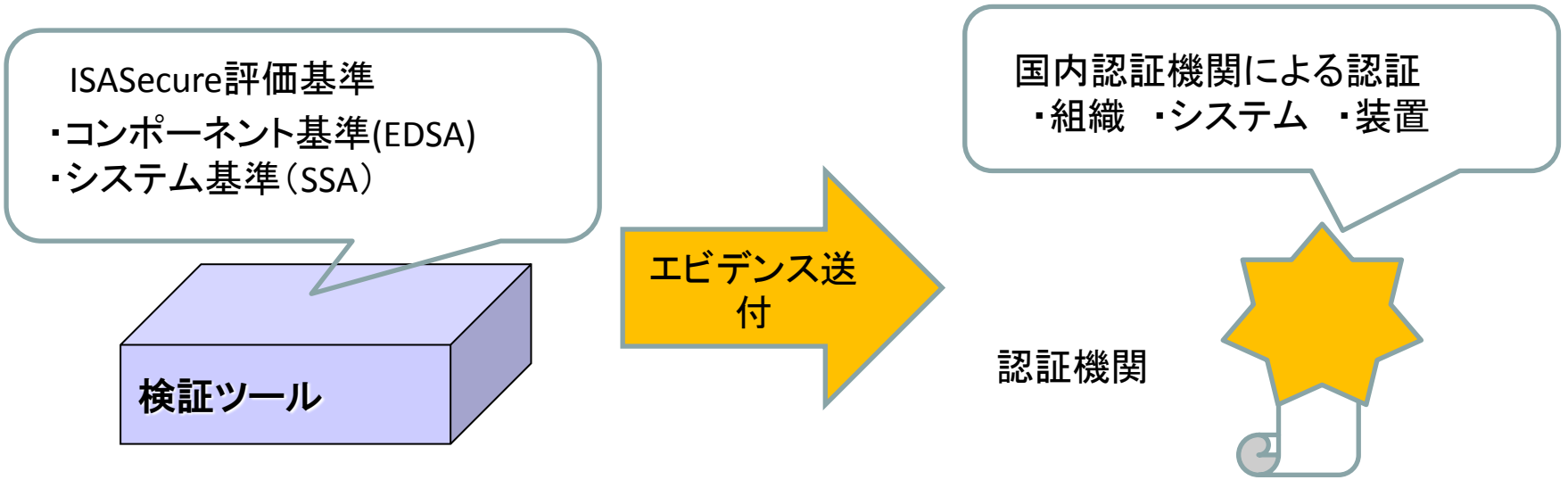
4. 国際規格準拠認証

■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

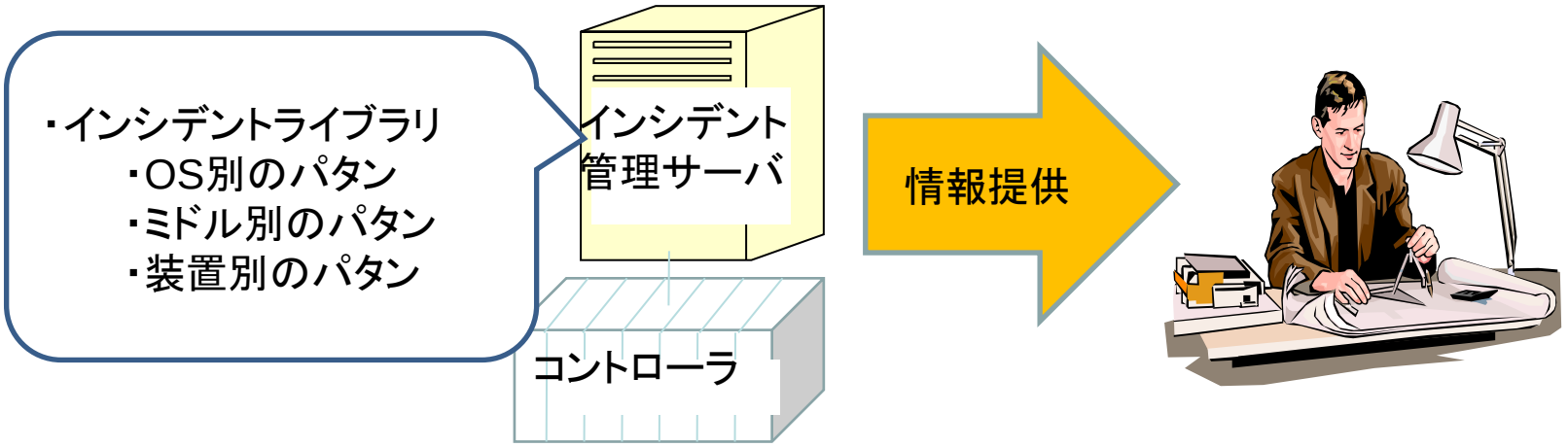


5. インシデントサポート

■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）



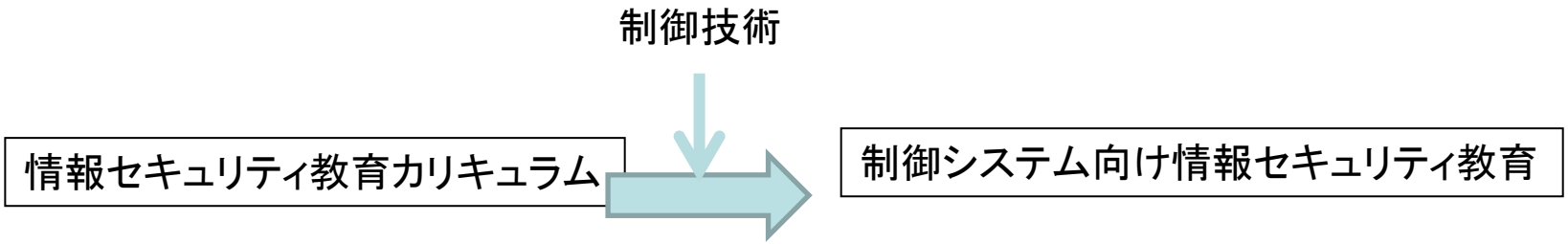
６．人材育成

■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

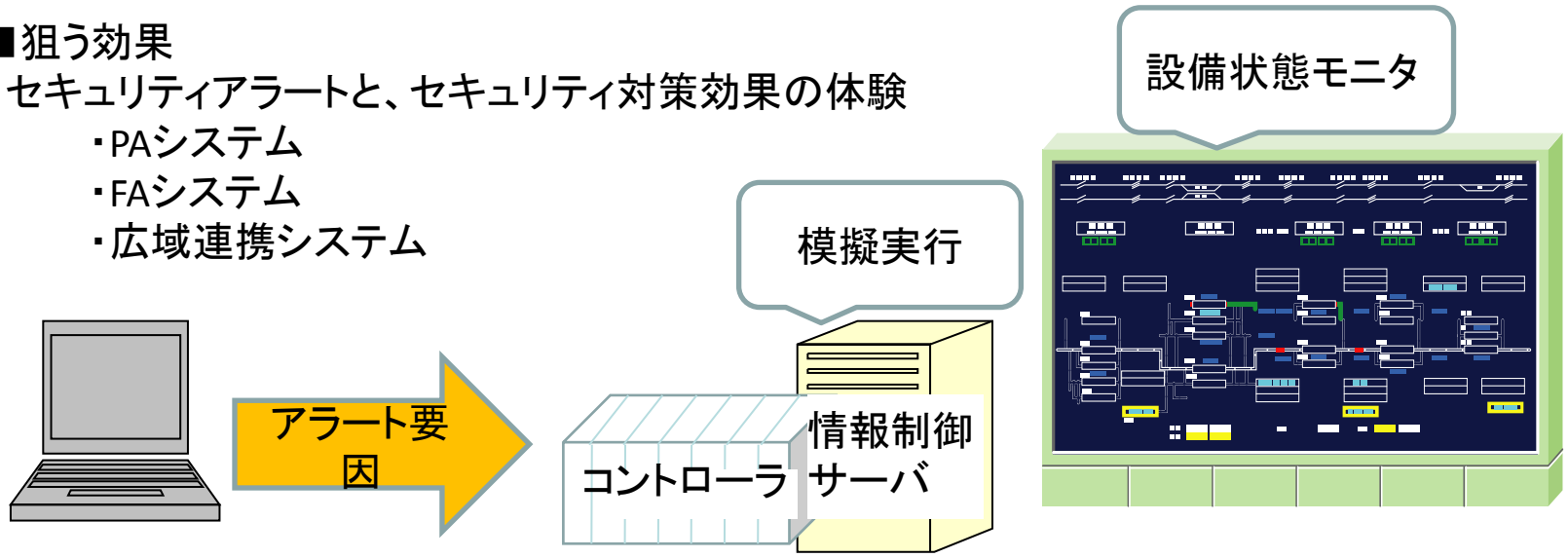


7. 普及啓発

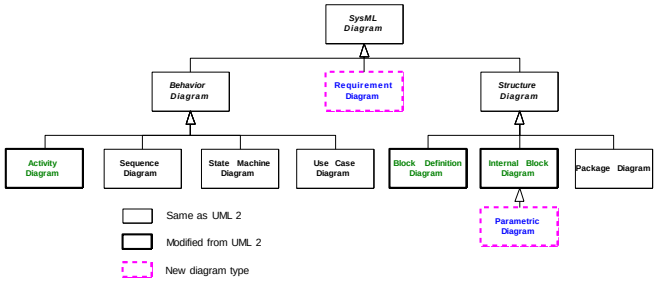
■狙う効果

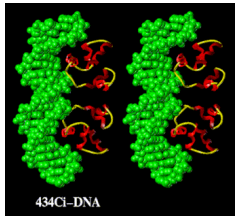
セキュリティアラートと、セキュリティ対策効果の体験

- ・PAシステム
- ・FAシステム
- ・広域連携システム



新陳代謝





毎日5千億個の細胞が生まれ

毎日5千億個／日の細胞が出ていく

免疫系，ホルモン系

ISOにおける標準化

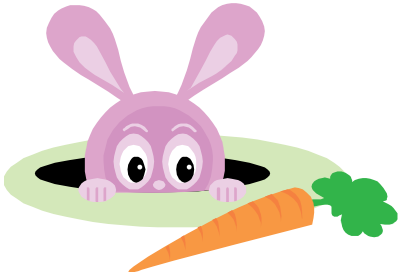
ISO15745　Part 4 ADS-net, FL-net

60兆個の細胞が同一の遺伝子を持つ

OMGにおける標準化

Super Distributed Object→Robot Technology Component→Security, Safety, and Save

制御システムセキュリティ



2011/11/20

イランの核科学者、爆弾で死亡

【テヘラン＝共同】イランのファルス通信によると、同国の首都テヘラン北部で11日朝、車に取り付けられた爆弾が爆発し、同国の核科学者で大学教授のムスタファ・アハマディロウシャン氏（32）ら2人が死亡、1人が負傷した。イランのラヒミ第1副大統領は「（イスラエルなど）イランと敵対的関係にある国が関わったテロ」と非難。同通信によると、テヘラン州の治安当局者も過去に核科学者らが殺害された手口と似ていることなどから、イスラエルのテロリストによる犯行だと話した。アハマディロウシャン氏は中部ナタンズにあるウラン濃縮施設での作業に関わっていたという。

http://www.nikkei.com/paper/article/g=9695
99969381959FE3E3E2E5EA8DE3E3E2E3
E0E2E3E09494E0E2E2E2;b=20120112

2012/1/12

まとめ

- 実世界から仮想世界へのモデリング
- 仮想世界から実世界への実装
- 仮想世界での振る舞いチェック
- 実世界でのモデルを用いた振る舞いチェック
- Multi Physics, Multi Vender, Multi User
- 制御系セイフティ，制御系セキュリティ