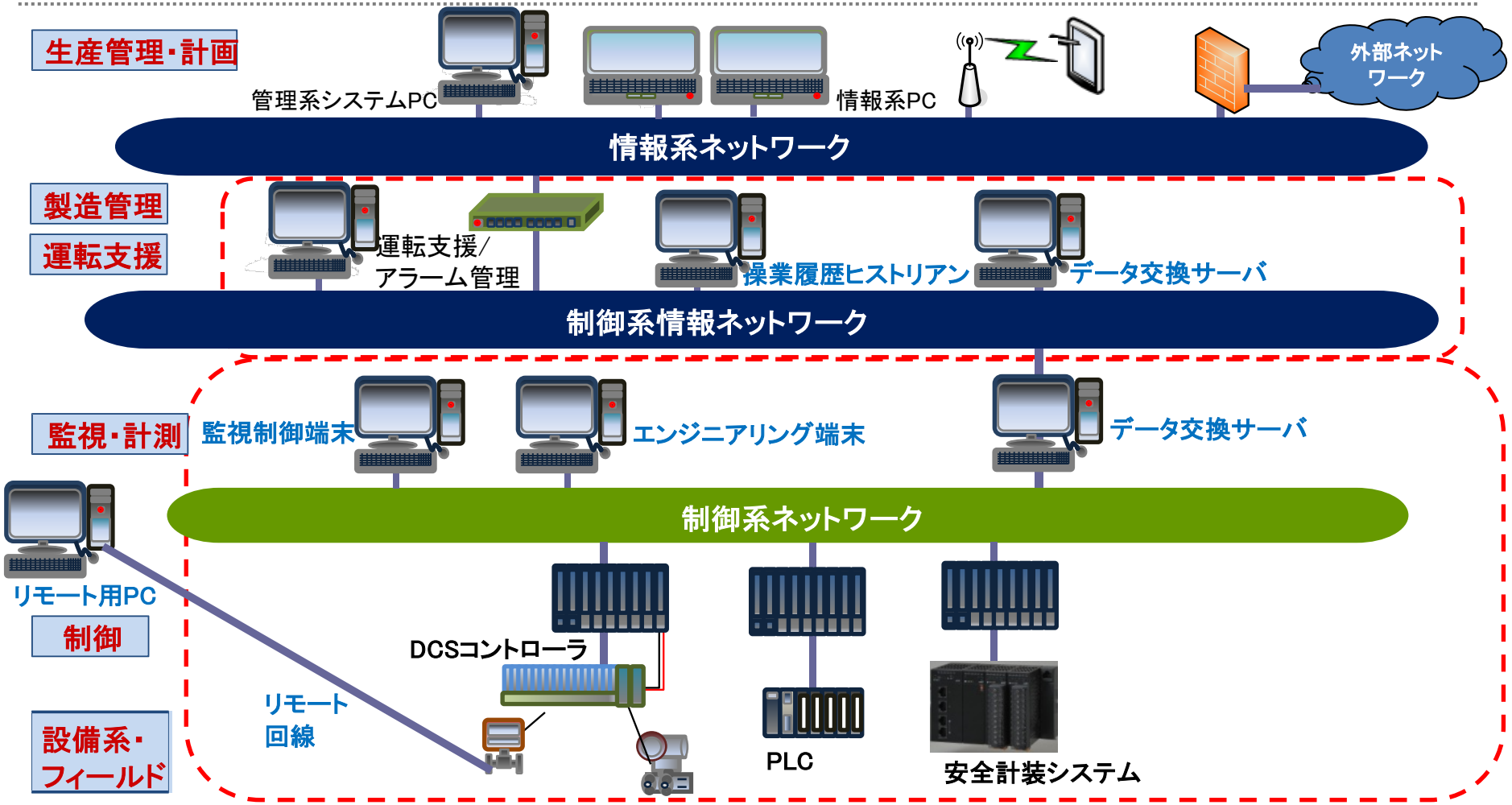
制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について

技術研究組合制御システムセキュリティセンター

制御システムネットワーク



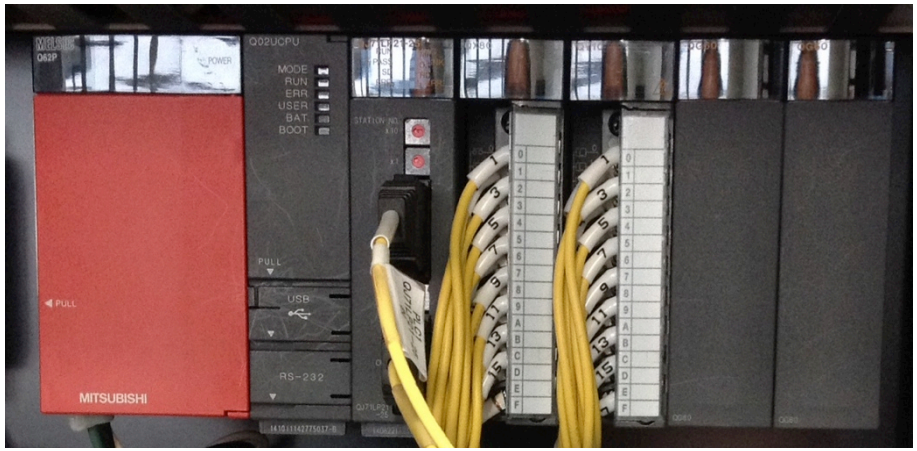
・制御情報ネットワークは、IP（Internet Protcol）化が進んでいる
・制御ネットワークは、必ずしもIP化されておらず、制御ネットワークは非IPであることもある
・リモートメンテナンス回線・リモート監視回線はIP化が進んでいる
・通信機器と端末・サーバは、汎用化が進んでいる

PLCとDCS

DCS

一般に、DCSは、オペレータ（運転員）が制御・監視を行うためのHMI（Human Machine Interface）と、フィールドネットワークに接続して、HMI とコントローラを接続する制御ネットワークの3つの構成要素からなる。化学やガスプラントで利用。

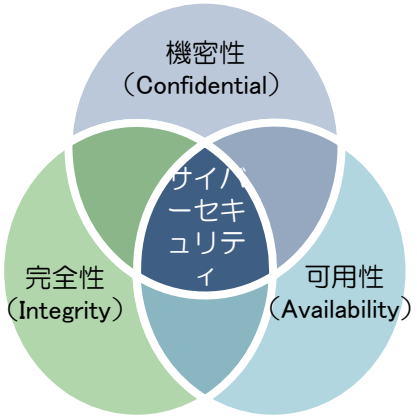
PLC



PLC は、パソコンと監視・制御ソフトウェアの組み合わせによりプロセスの制御・監視を実行するものである。組立プラントやビル制御等で利用。

制御セキュリティと情報セキュリティ

- セキュリティの3要素は、資産(情報や装置etc)の機密性・完全性・可用性である。これらはセキュリティの３要件とされ、英語の頭文字を取ってCIAと呼ばれる。いずれの要素についてもバランスよく維持することが重要である。
  - 機密性（Confidential）
    - 許可された者が許可された方法でのみ資産にアクセスできることを確実にすること。つまり、権限のないユーザーがアクセスできないようにすること。
  - 完全性（Integrity）
    - 資産の正確さ及び完全さを保護する特性
  - 可用性（Availability）
    - 許可された利用者が必要な時に適時にアクセス可能であり、確実に利用できる状態



・制御システムにおいても、情報システムにおいても、可用性・機密性・完全性のバランスを確保することが重要。

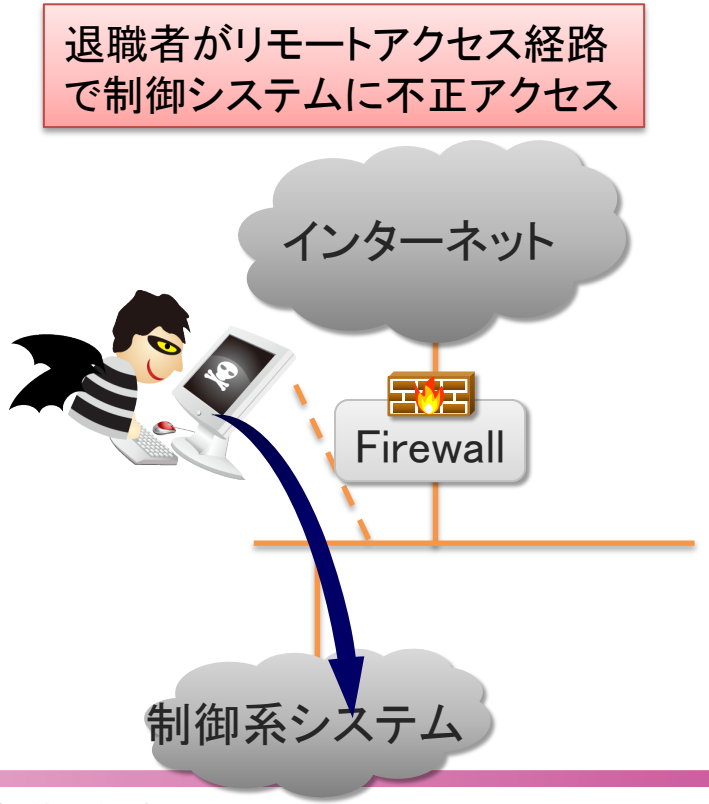
・可用性を阻害する技術、機密性を阻害する技術、完全性を阻害する技術はそれぞれ特徴がある

・制御システムにおけるセキュリティ対策の留意点は、セキュリティパッチを当てることが難しく、ブラックリスト型のウィルス対策ソフトウェアの利用は難しいことである

水道分野におけるセキュリティ事故事例

- 2001年にオーストラリアの下水処理施設が外部からリモートアクセス経由で不正に操作され、下水が海洋に流出した。結果、海洋系に多大な被害が出た。
- 解雇された元従業員による犯行。※その後、逮捕された。
- 在職時に利用していたリモートアクセス経路及びアカウントを利用して、外部から制御システムを不正操作するに至った。

Chesapeake Bay Program/CC BY 2.0　写真は参考画像です



鉄道分野のセキュリティ事故事例

- 2003年に米国では社内の情報システム経由でマルウェア（sobig）への感染が内部で蔓延し、信号システムが停止するに至った。
- 復旧するのに6時間を要し、その間列車の運航ができなかった。

CSX Train

Flowizm .../CC BY 2.0

Sobig解説

トロイの木馬型のマルウェアで、自分自身のコピーをメールの添付ファイルとして感染範囲を拡げる活動を行う。感染すると、Windowsのアドレス帳や特定の拡張子（txt、eml、html、htm、dbx、wab）のファイルからメールアドレスを収集し、取得できたアドレス宛に悪意を持った添付ファイルを付与したメールを送信することで感染を拡大させる。

石油化学分野のセキュリティ事故事例

- 2008年トルコで、石油パイプラインが爆発した。パイプラインに設置されている監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入した。不正に動作制御系にアクセスし、管内の圧力を異常に高めて爆発を引き起こした。
- 攻撃者はすべての警報装置（カメラやセンサ）の動作を止め、通信を遮断するなどの操作も実施した。

Oil pipeline

Will Russell/CC BY 2.0　写真は参考画像です

Oil pipeline(全体図)

ビル分野のセキュリティ事故事例

警備員による病院のHVACシステムのハッキング


W.B. Carrell Memorial Clinic

日時	2009年4月～6月
攻撃対象	米国テキサス州ダラス W.B. Carrell Memorial Clinic
侵入経路	病院のHVACシステム、患者情報のコンピュータ等の不正アクセス
被害	システムへの侵入、システム画面のオンライン上での公開、未遂だがDDoS攻撃の計画あり

TimeLine	経緯・概要
（背景）	同病院の夜勤の契約警備員（当時25）は、オンライン上で“Ghost Exodus”という名前で活動し、ハッカーグループ“Electronik Tribulation Army” のリーダも務めていた。
攻撃 2009.4-6	警備員は同病院のHVACシステムや顧客情報のコンピュータに侵入し、HVACシステムのHMI画面のスクリーンショットをオンラインで公開。公開された画面（次頁参照）では、手術室のポンプや冷却装置を含め、病院の様々な機能のメニューが確認できる。さらに、病院内のPCにマルウエアをインストールする（後述のDDoS攻撃のため、PCをボットネット化したものとみられる）様子なども動画に撮り公開している。
―	一方、病院の職員はアラーム設定が停止されたことで、HVACシステムのアラームがプログラムどおりに機能せず、不思議に思っていたが、内部から発覚することはなかった。
発覚・逮捕 2009.6	SCADAセキュリティの専門家がハッカーの知り合いからの情報を得て調査し、FBI及びテキサス州検察局に報告したことで発覚し、2009年6月26日警備員は逮捕された。（連邦刑務所への9年の禁固刑を受ける。）
攻撃計画（未遂） 2009.7	逮捕により未遂に終わったものの、警備員は、乗っ取られた病院のシステムを使って2009年7月4日（独立記念日）に大規模なDDoS攻撃を仕掛ける計画を立てており、インターネット上で協力してくれるハッカー仲間を募っていた。また、既に攻撃予定日の前日に辞職する旨を所属する警備会社に伝えていた。

出典：DOJプレスリリース (http://www.justice.gov/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html)

WannaCryの制御システムへの影響

- Windows をターゲットとしたランサムウェア
- ランサムウェアとは、感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラム
- Windows内のファイルを暗号化し、Bitcoinによる支払を要求
- 全感染PCのうち97%がWindows7
- MS17-010 の適用を適用すれば感染しない
- Windows 10では感染しない（改造版のPetyaでは感染する）
- メール添付ではなく、ポート445が開いており、MS17-010が適用されていないパソコンに感染
- 感染後特定のサイトに接続を試み、接続可能な場合は停止
- 日立製作所では、ドイツにおける自動車部品製造拠点において、電子顕微鏡を制御する装置への感染が発生
- ホンダでは、狭山工場の生産ラインを制御するPC複数台がWannaCryに感染したため、6月19日-6月20日の間、自動車の生産を停止した。
- 上記、日立製作所・ホンダ等制御システムにあるように制御システムにも影響を及ぼした

- 日本では日立製作所、川崎市上下水道局、JR東日本高崎支社など600か所・2000端末以上が感染した（件数はJPCERT／CCによる）
- 全世界では150か国にも及び、30万件以上の被害が出ていると推測されている
- 5月19日11時現在、3つの口座の総額は約8万8千ドル（約1000万円）

（http://www.yomiuri.co.jp/science/goshinjyutsu/20170519-OYT8T50016.html より引用）

我が国の制御システムでの脅威

USBポート

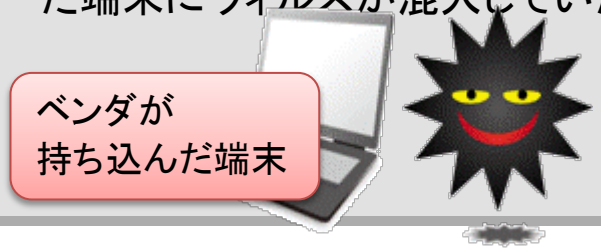
- USBメモリからのウィルス感染事例は頻繁に発生している

リモートメンテナンス回線

- 某社は米国の中央監視室からリモートメンテナンス回線によりタービンをリアルタイム監視
- リモートメンテナンス回線の先の端末からの不正アクセス・マルウェア混入

操作端末の入れ替え

- 日本の自動車会社では、ベンダが入れ替えた端末にウィルスが混入していた事例あり



物理的侵入

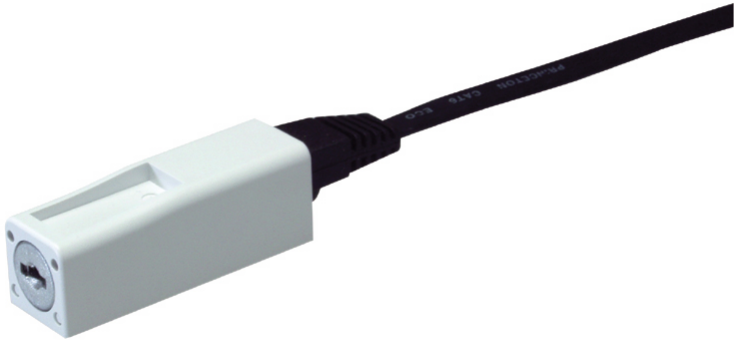
- 監視端末のパスワードが無い
- IDやパスワードは共通化、壁に張出し

その他過去の事例：
・日本のインフラ企業の操作員が、端末をインターネットに接続してゲームを行っていたところウィルスに感染

USBメモリ等接続する機器のコントロール対策の例

●未使用のUSBポートのロック

●未使用のLANケーブルの使用ロック



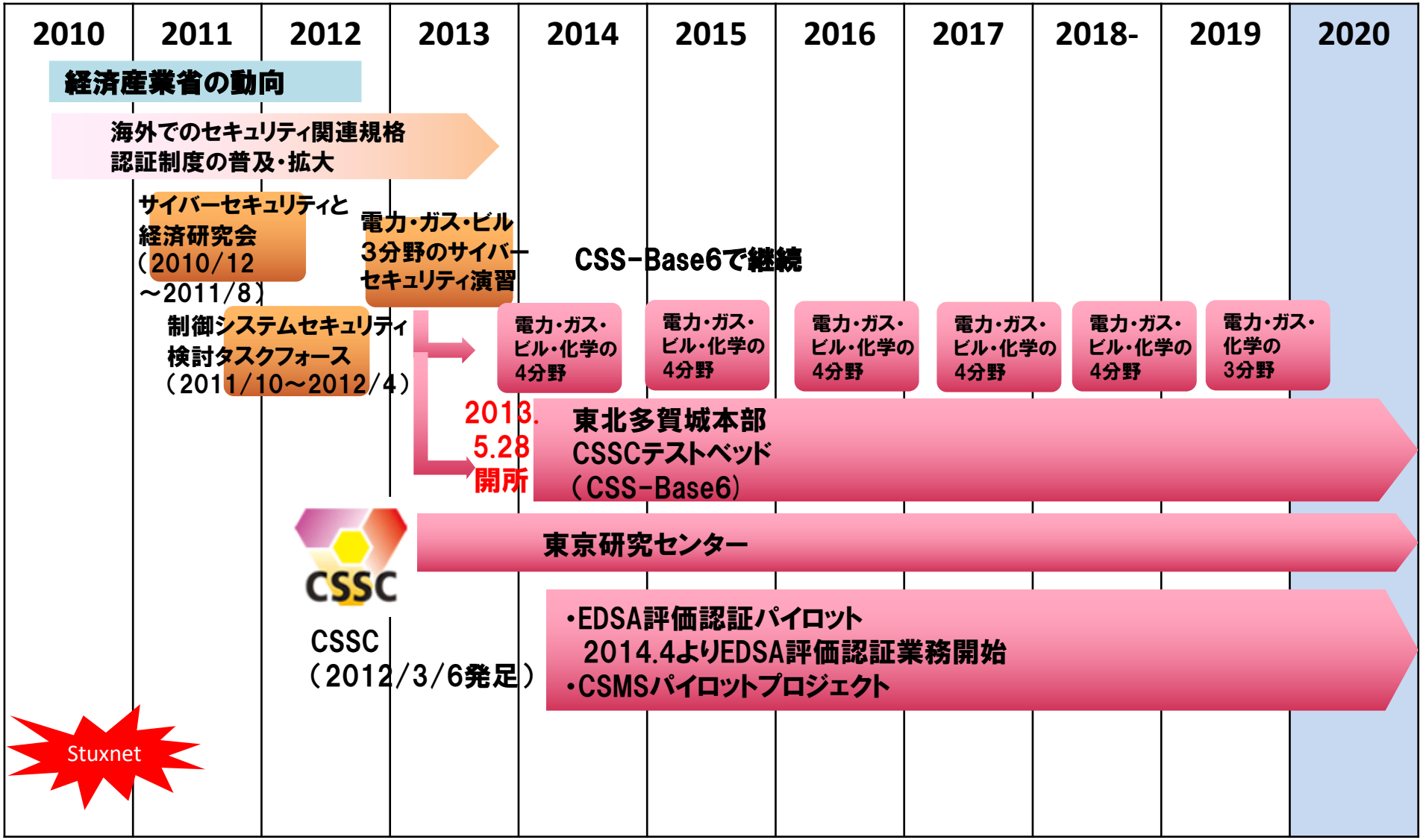
●HUBの未使用ポートのロック

●LANケーブルの抜き差しロック

その他の対策の方向性

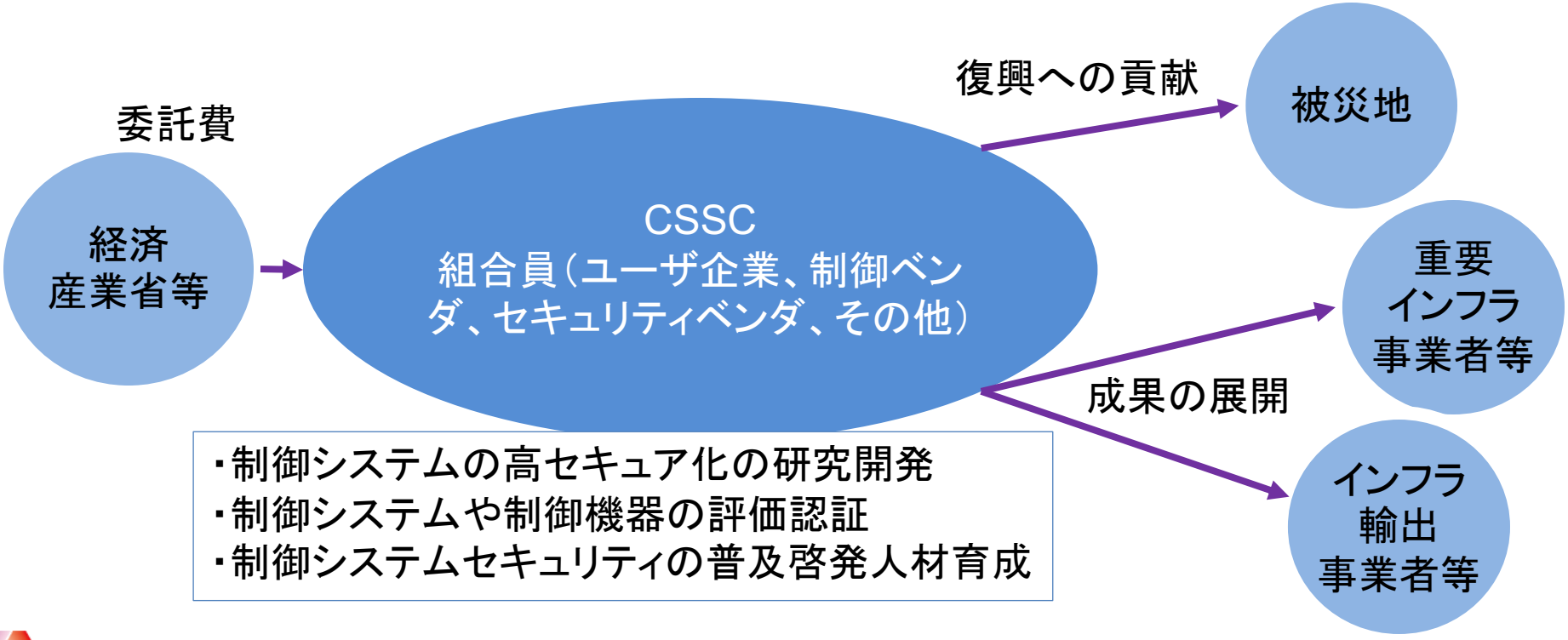
項番	我が国における脅威	対策の方向性
1	リモートメンテナンス回線	・リモートメンテナンス回線に接続されている端末の認証を行う（証明書を配布する等） ・端末におけるセキュリティ監査を実施する。
2	端末の入れ替え	・入れ替え時にスタンドアロンでマルウェアチェックを行う
3	その他	・物理的セキュリティ対策（鍵や入退室リストの管理、生体認証の導入、監視カメラの設置、持ち物や体重検査等）を徹底する

CSSCの歩み


2010
2011
2012
2013
2014
2015
2016
2017
2018-
2019
2020
経済産業省の動向
海外でのセキュリティ関連規格
認証制度の普及・拡大
サイバーセキュリティと
経済研究会
（2010/12
～2011/8）
制御システムセキュリティ
検討タスクフォース
（2011/10～2012/4）
電力・ガス・ビル
3分野のサイバー
セキュリティ演習
CSS-Base6で継続
電力・ガス・
ビル・化学の
4分野
電力・ガス・
ビル・化学の
4分野
電力・ガス・
ビル・化学の
4分野
電力・ガス・
ビル・化学の
4分野
電力・ガス・
ビル・化学の
4分野
電力・ガス・
化学の
3分野
2013.
5.28
開所
東北多賀城本部
CSSCテストベッド
（CSS-Base6）
CSSC
東京研究センター
CSSC
（2012/3/6発足）
・EDSA評価認証パイロット
2014.4よりEDSA評価認証業務開始
・CSMSパイロットプロジェクト
Stuxnet

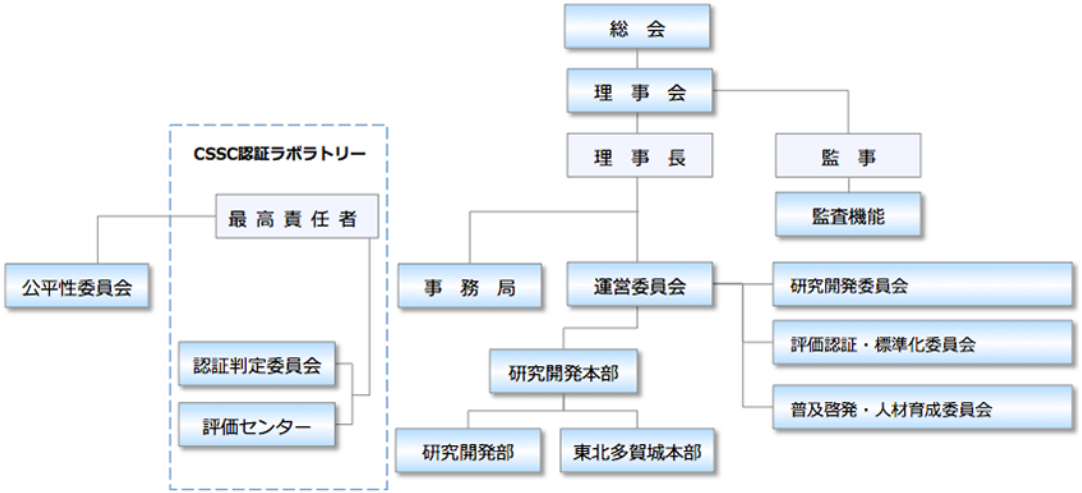
CSSCの活動目的と活動スキーム

1. 重要インフラを中心とする制御システムセキュリティの確保
2. 制御システムのセキュリティ確保に伴う輸出競争力強化
3. 被災地の復興への貢献



CSSCの組織体制

理事長　新誠一
（電気通信大学 教授）



東北多賀城本部長　高橋信
（東北大学 教授）

役職	氏名	所属等
理事長	新　誠一	国立大学法人電気通信大学 元教授
理事	伊東　忠義	アズビル株式会社　執行役員常務 アドバンスオートメーションカンパニー ソリューション・サービス事業統括長
理事	渡部　宗一	イーヒルズ株式会社　取締役
理事	石井　秀明	株式会社東芝 執行役常務
理事	宮尾　健	株式会社日立製作所 セキュリティ事業統括本部 副統括本部長
理事	関口　智嗣	国立研究法人産業技術総合研究所 情報・人間工学領域　領域長
理事	小野塚　正紀	三菱重工業株式会社　シニアフェロー ICTソリューション本部長
理事	藤田　正弘	三菱電機株式会社 常務執行役　開発本部長
理事	森　浩生	森ビル株式会社 取締役　副社長執行役員
理事	浦　直樹	株式会社オメガシミュレーション 代表取締役社長
顧問	高橋　信	東北多賀城本部長 東北大学　教授
顧問	渡辺　研司	名古屋工業大学　教授
顧問	澤田　賢治	国立大学法人電気通信大学　准教授
顧問	小林　和真	慶應義塾大学大学院　特任教授
監事	稲垣　隆一	弁護士
事務局長	村瀬　一郎	技術研究組合制御システムセキュリティセンター

CSSCの概要（2020年8月20日時点）

名称	**技術研究組合 制御システムセキュリティセンター** （英文名）Control System Security Center （略称）　CSSC ※経済産業大臣認可法人	**組合員** (50音順)	全26組織　*：創設時メンバー8社 株式会社IHI、アズビル株式会社*、アライドテレシス株式会社、アラクサラネットワークス株式会社、オムロン株式会社、国立研究開発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、ソニー株式会社、通研電気工業株式会社、国立大学法人電気通信大学、株式会社東芝*、東北インフォメーション・システムズ株式会社、国立大学法人東北大学、日本電気株式会社、一般財団法人日本品質保証機構、パナソニック株式会社、株式会社日立製作所*、富士通株式会社、富士電機株式会社、株式会社マクニカ、三菱重工業株式会社*、株式会社三菱総合研究所*、三菱電機株式会社、株式会社明電舎、森ビル株式会社*、横河電機株式会社*
設立日	2012年3月6日（登録完了日）		
所在地	【東北多賀城本部(TTHQ)】 宮城県多賀城市桜木3-4-1 （みやぎ復興パーク　F-21棟 6階） 【東京研究センター(TRC)】 東京都調布市小島町1-1-1 　UECアライアンスセンター505号		
賛助会員	株式会社OTSL、株式会社アイユート、日本原子力防護システム株式会社、株式会社原子力エンジニアリング、KPMGコンサルティング株式会社、千代田計装株式会社、日本ダイレックス株式会社、株式会社インフォセック、三菱スペース・ソフトウエア株式会社、国立研究開発法人理化学研究所、株式会社インフォメーション・ディベロプメント、株式会社テリロジー		
特別賛助会員	宮城県、多賀城市、株式会社アイシーエス、株式会社イーアールアイ、株式会社サイバーソリューションズ、株式会社システムロード、株式会社高山、テクノ・マインド株式会社、東杜シーテック株式会社、株式会社戸崎通信工業、トライポッドワークス株式会社、株式会社東日本計算センター、株式会社福島情報処理センター	**連携団体**	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、一般社団法人日本計装工業会、一般社団法人日本電気計測器工業会、一般財団法人製造科学技術センター、電気事業連合会、一般社団法人日本化学工業協会、一般社団法人東北経済連合会、一般社団法人宮城県情報サービス産業協会、多賀城・七ヶ浜商工会、一般社団法人ビルディング・オートメーション協会、一般社団法人日本ガス協会

CSSCにおける研究開発の概要

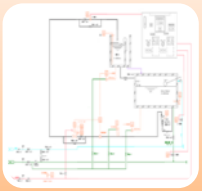
1

[製品]

コントローラ等を対象にして、現状の確認・対策、

およびセキュアな製品開発についての研究開発

2



[システム]

(IT)システムを中心とした現状のシステムの確認・対策、

およびセキュアなシステムを作るための研究開発

3

[プラント]

現状のプラントの確認・対策、

およびセキュアなプラントを作るための研究開発

4

[テストベッド]

製品・システム・プラントについて、模擬プラント等による

確認・対策を実施できる環境そのものに関する研究開発

CSSCにおける研究開発

1. [製品]

1

[製品]　コントローラ等を対象にして、現状の確認・対策、

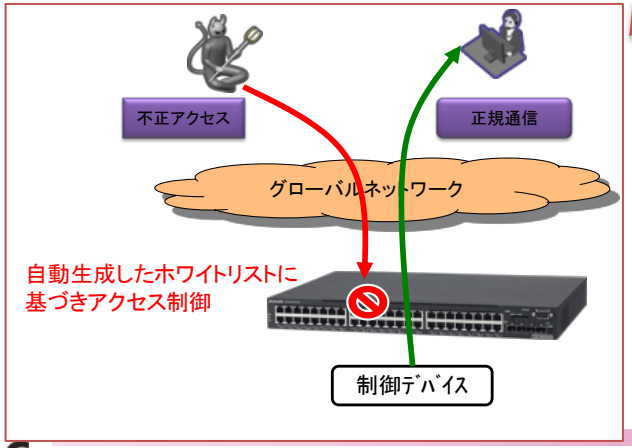
およびセキュアな製品開発についての研究開発

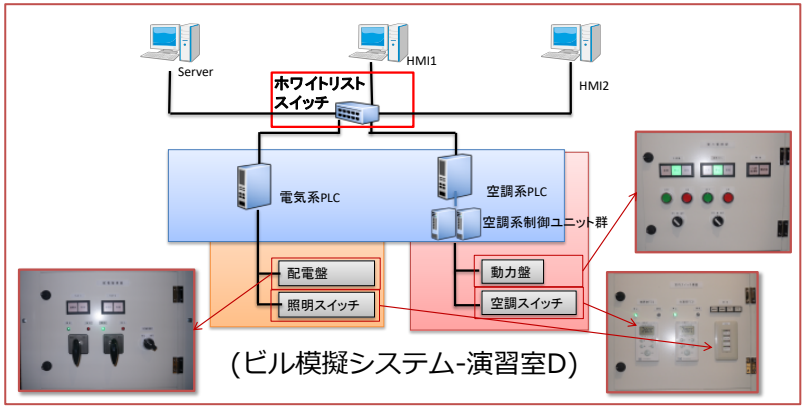
現状製品の検証技術

- ISCI/EDSA準拠のための検証技術
- CSSC独自の検証項目策定

セキュアな製品に向けた技術開発

- ホワイトリストスイッチ
- ホワイトリスト（端末・サーバ向け）
- セキュリティバリアデバイス(SBD)

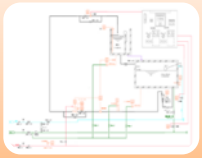




CSSCにおける研究開発

2. [システム]

2



[システム] (IT)システムを中心とした現状のシステムの確認・対策、

およびセキュアなシステムを作るための研究開発

現状システムの検証技術

- ISCI/SSA準拠のための検証技術
- CSSC独自の検証項目策定

セキュアなシステムに向けた技術開発

- セキュアな制御システム構築ガイド(IEC 62443)
- 制御システムにおけるセキュアなログ集約技術
- 制御システムにおける横断的なログ分析技術
- 制御システムの資産管理共通化技術(SCAP)
- CSSC独自の検証ツール

(化学模擬プラント
-システム評価室)

(FA模擬プラント-
模擬プラント室)

CSSCにおける研究開発

3. [プラント]

3

[プラント] 現状のプラントの確認・対策、

およびセキュアなプラントを作るための研究開発

オンライン情報(1)

オンライン情報(2)

オフライン情報

サイバー攻撃を含む異常仮説の絞り込み

- オンライン情報(1):リアルタイムで常にモニターしている情報
- オンライン情報(2):必要に応じてオンラインで獲得する情報
- オフライン情報：現場情報を獲得し人間がシステムに入力する情報

現状のプラント運転の検証技術

- ケイパビリティモデルに基づくシステムリスク管理態勢成熟度評価
- CSMS演習コンテンツ

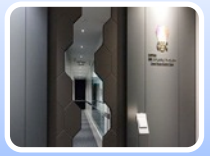
セキュアなプラントに向けた技術開発

- サイバー攻撃の早期認識技術
- モデルベース制御に基づくセキュリティ技術
- ヒューマンファクター対策

CSSCにおける研究開発

4. [テストベッド]

4



[テストベッド] 製品・システム・プラントについて、模擬プラント等による確認・対策を実施できる環境そのものに関する研究開発

全模擬プラント、
接続機器を対象

テストベッドの構築

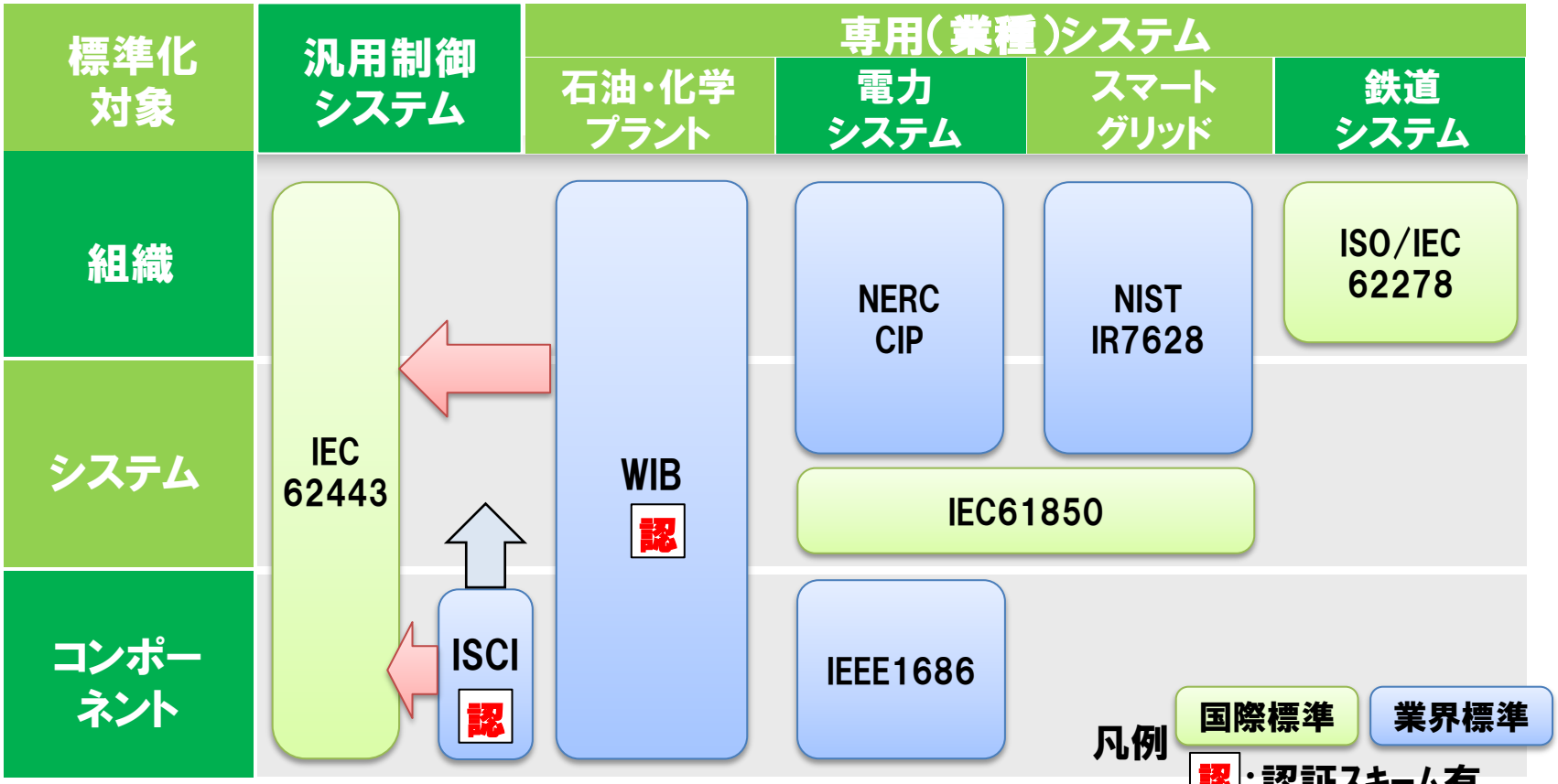
- 9つの模擬プラントの構築
- OPCによる相互接続環境の構築
- マルウェアの動作を再現する機能の構築
- 対応策の構築

テストベッドへの検証環境の構築

- 遠隔検証環境の構築
- 疑似攻撃環境の構築

評価認証手法の開発
（１）制御システム分野での標準化に関する技術動向

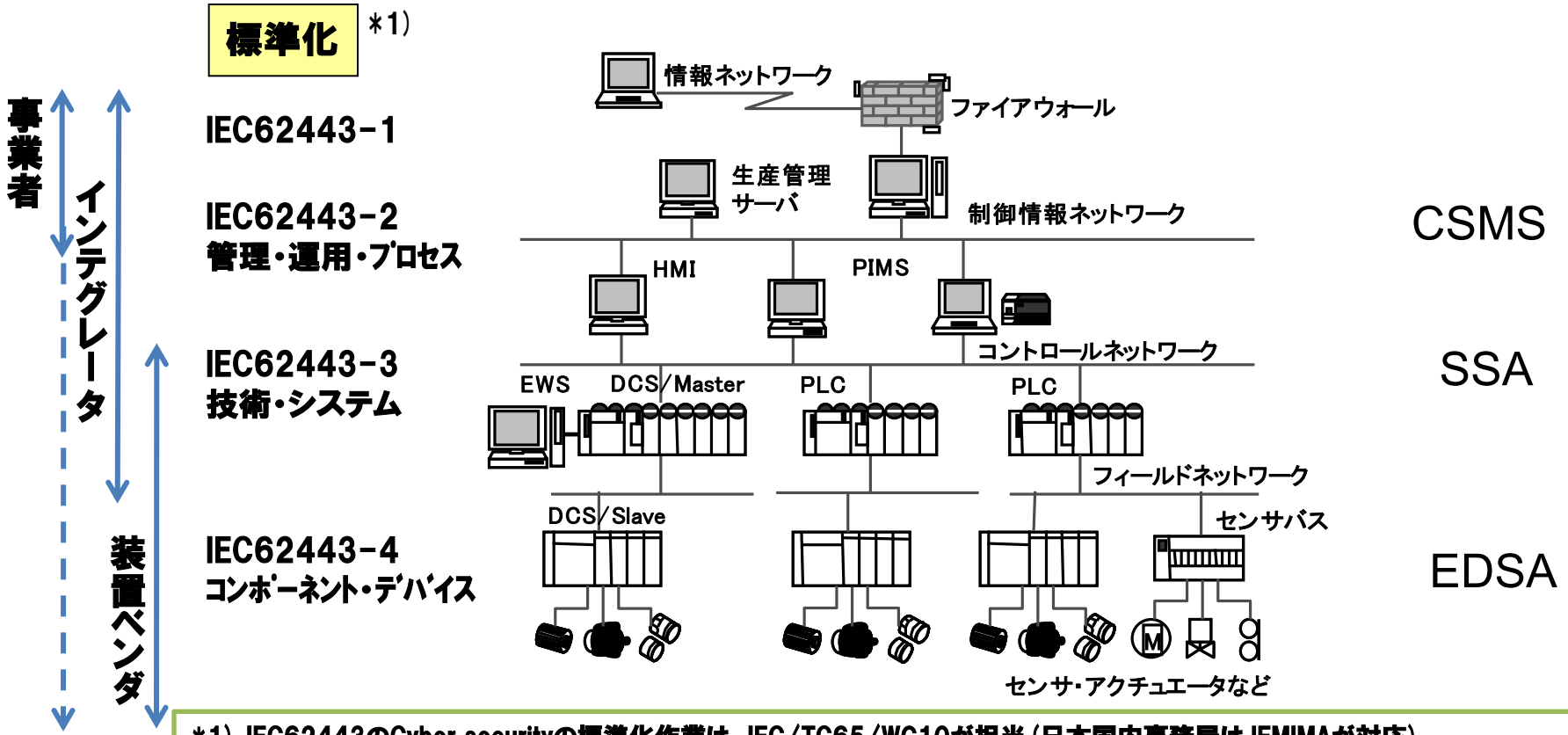
■制御システムのセキュリティの標準・基準には、組織やシステムのレイヤに対応したもの、業種や業界に対応したものなど、**様々な標準・基準が提案**されている。
■こうした中で、**汎用的な標準・基準として、IEC62443が注目**されてきており、**一部事業者の調達要件**に挙がってきている。
■業界で評価認証が先行しているISCIやWIBの基準が、IEC62443のシリーズに統合される動きとなっている。



ISCI: ISA Security Compliance Institute　WIB: International Instrument User's Association

評価認証手法の開発
（２）EDSA認証の全体像

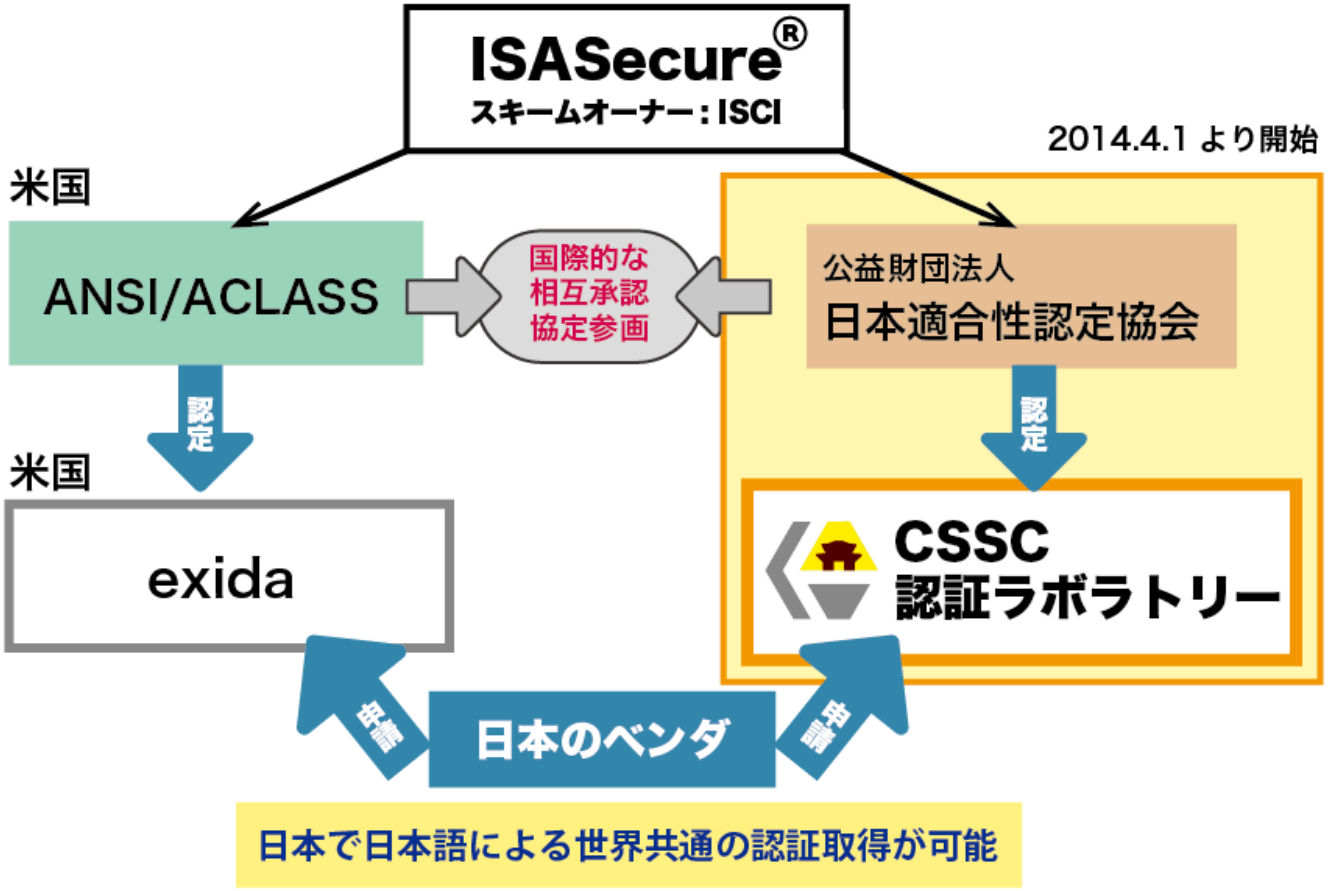
■IEC62443は制御システムセキュリティの全レイヤ/プレイヤーをカバーした規格
■先行する評価認証の規格（EDSA認証、WIB認証等）がIEC62443に採用される方向



*1) IEC62443のCyber securityの標準化作業は、IEC/TC65/WG10が担当（日本国内事務局はJEMIMAが対応）
*2) EDSA:Embedded Device Security Assurance:制御機器（コンポーネント）の認証プログラム→IEC62443-4に提案されている
*3) WIB: International Instrument User's Association →IEC62443-2-4に提案されている

DCS: Distributed Control System PLC: Programmable Logic Controller PIMS: Process Information Management System

評価認証手法の開発
（３）EDSA認証スキームへの日本での展開



成果展開：　平成25年度のパイロット認証を通して、
平成26年度より評価認証事業を開始

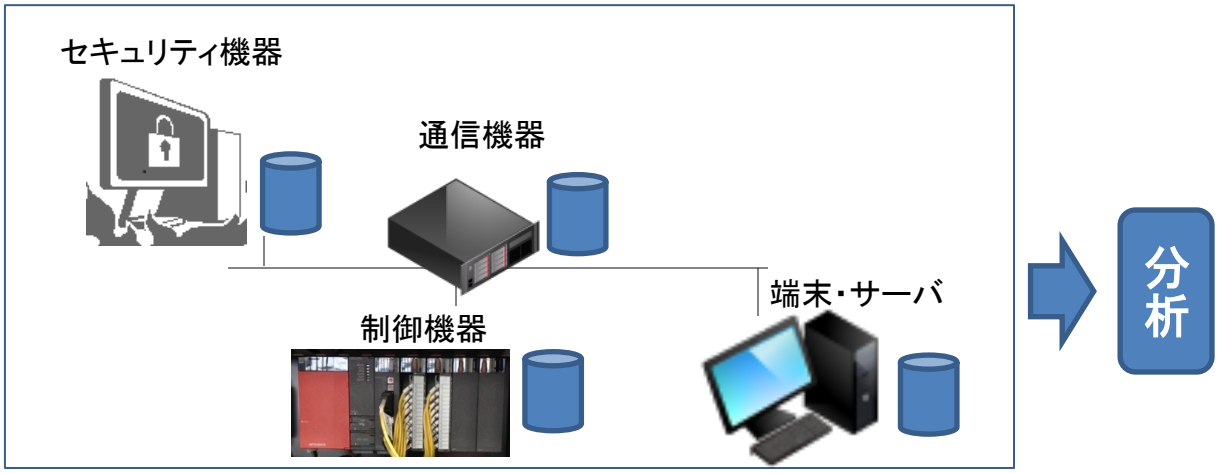
インシデント分析技術の開発

概要：

1. **通信機器、セキュリティ機器、端末・サーバ（パソコン）、制御機器のセキュアなログの蓄積技術**
2. **通信機器、セキュリティ機器、端末・サーバ（パソコン）、制御機器のログの横断的な分析技術**

ログの分析技術

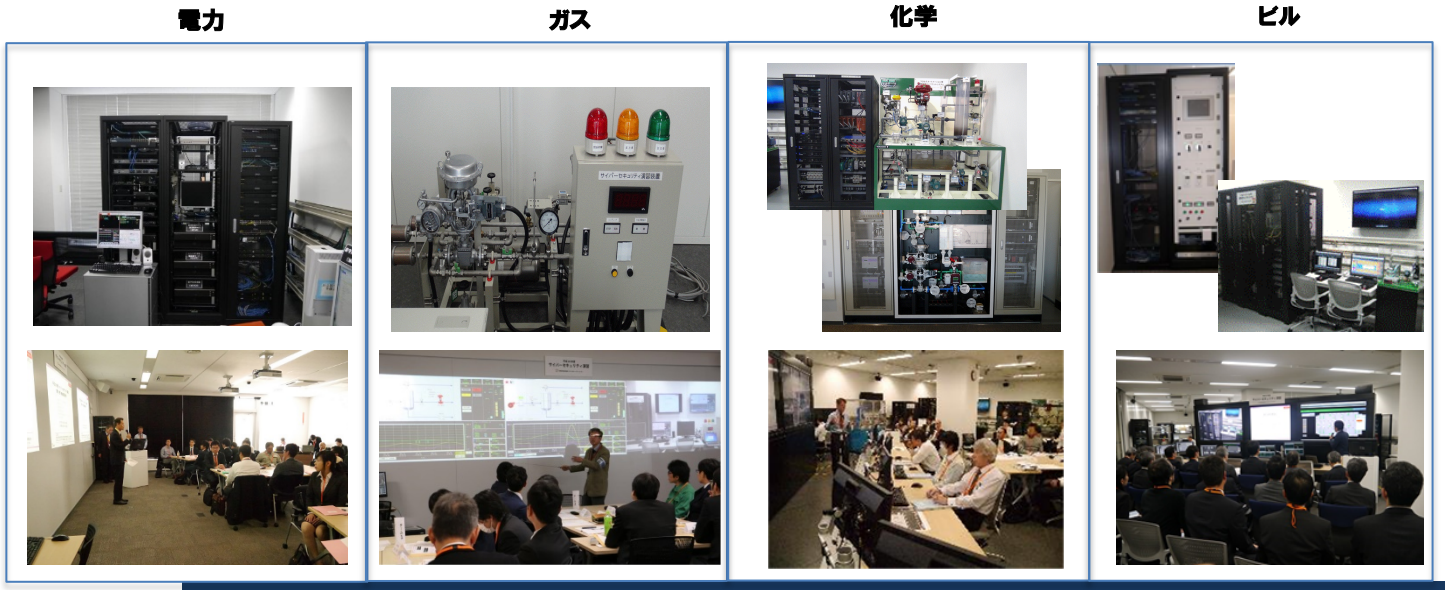
制御機器、通信機器、セキュリティ機器、パソコン等の多様なログを横断的に分析し、セキュリティインシデントの原因を推定



成果展開：　平成26年度はビル・化学・ガス模擬プラントにて検証
平成27年度以後重要インフラ事業者に展開

人材育成プログラムの開発
サイバーセキュリティ演習の実施概要

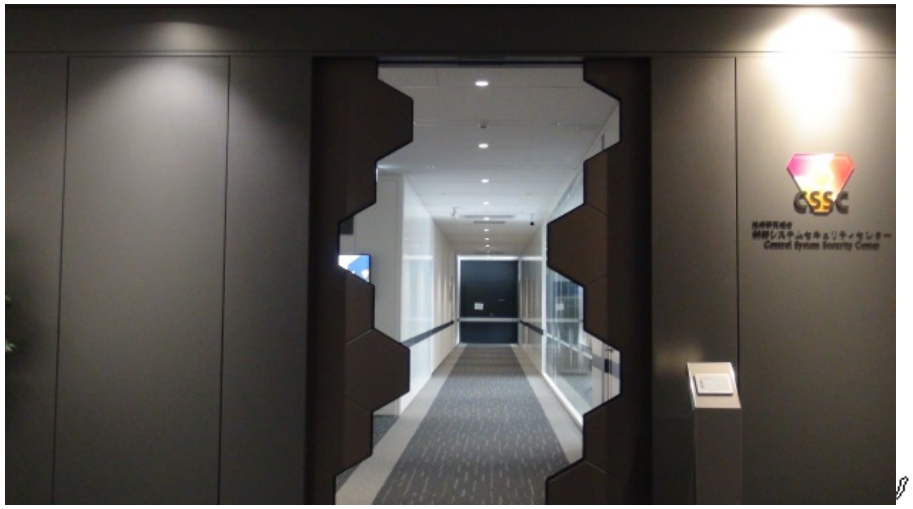
目的	・電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等の関係者が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性を検証する。 ・各分野の参加者、関係者における制御システムセキュリティ対策を中心とした知見の獲得を促すことで、演習の成果を関係機関におけるセキュリティ向上につなげる。
参加者	業界団体、事業者、有識者、所管省庁など。



成果展開：　各分野にて制御セキュリティの脅威と対策の必要性が認識されつつあるところ

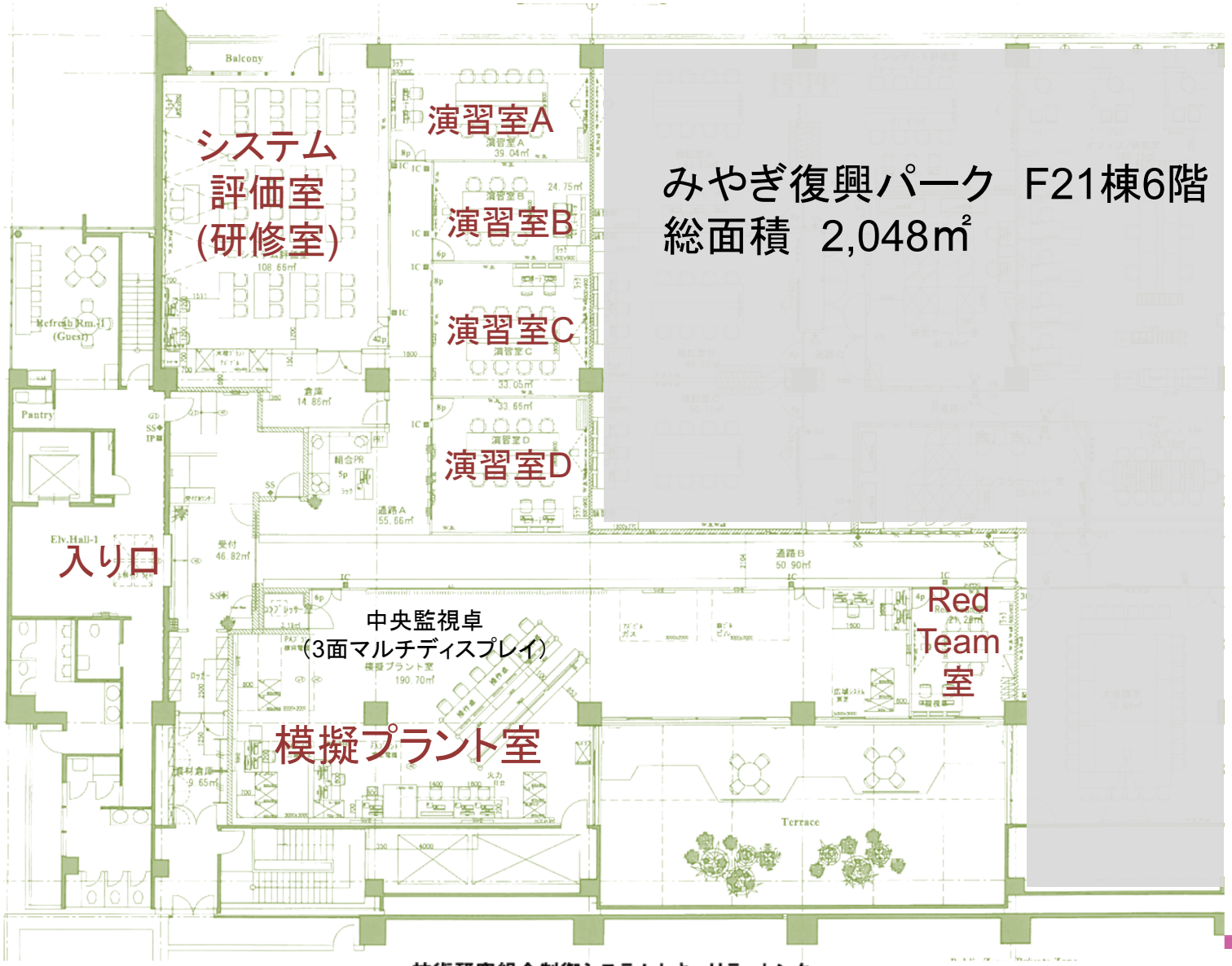
テストベッド（CSS-Base6）概要

東北多賀城本部(TTHQ)



http://www.css-center.or.jp/

東北多賀城本部（テストベッド：CSS-Base6）



テストベッド：所在地

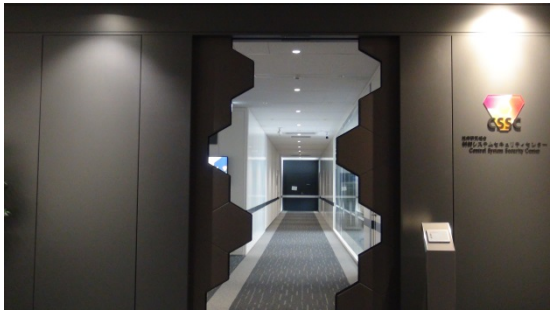
【所在地】 〒985-0842
宮城県多賀城市桜木3-4-1　みやぎ復興パーク　F21 6階

【電話】 022-353-6751

電車ご利用の場合のアクセス

●JR仙石線／
「多賀城駅」より徒歩13分
またはタクシー5分

テストベッド：入り口と模擬中央監視卓



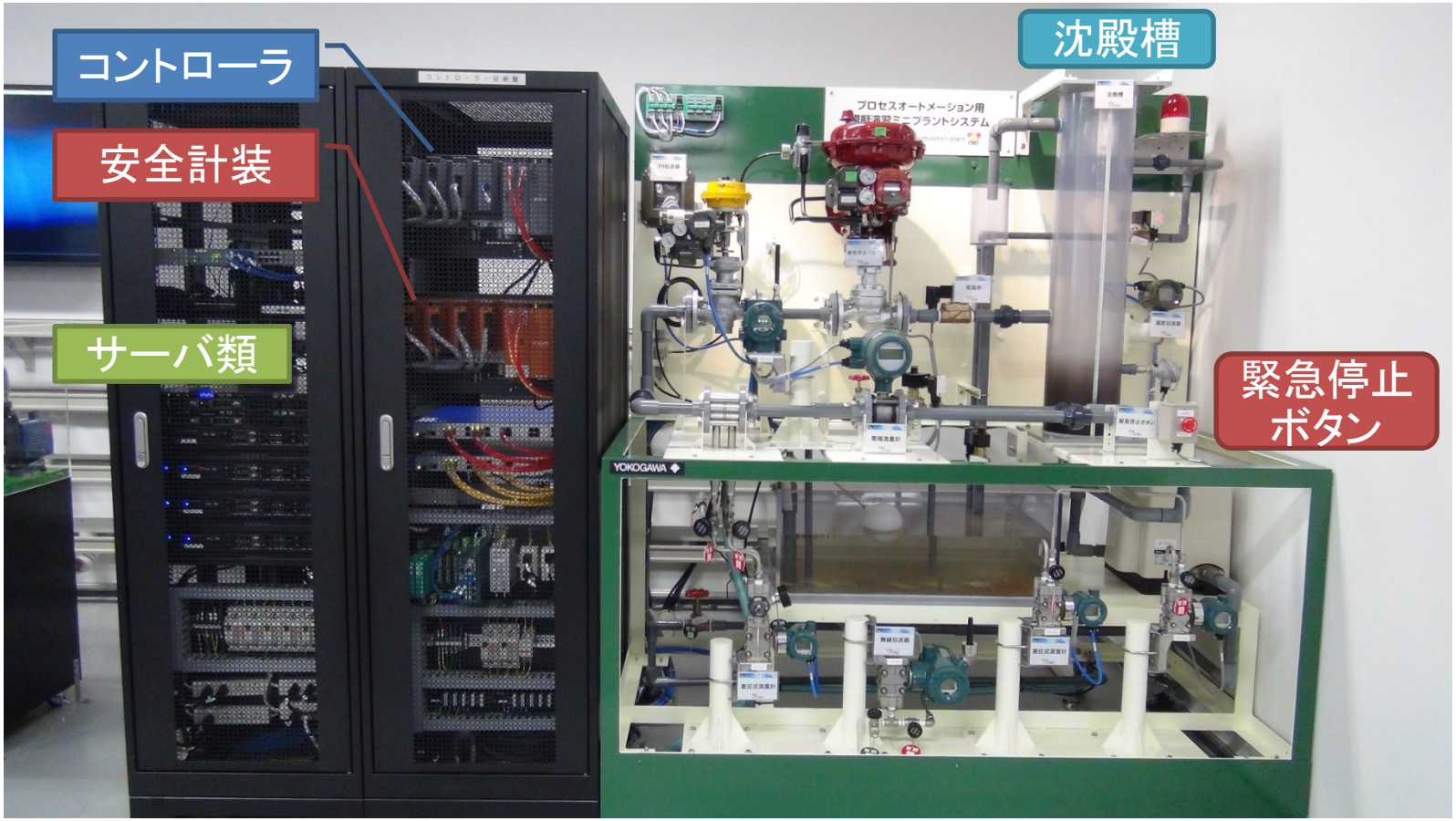
模擬システム

■ **制御システムの特徴的な機能を切り出し、デモンストレーションとサイバー演習が実施可能な模擬システムを構築した。**

■ **2020年8月時点では、下記の９種類の模擬システムが稼働中。**

（１）排水・下水プラント
（２）ビル制御システム
（３）組立プラント
（４）火力発電所訓練シミュレータ
（５）ガスプラント
（６）広域制御（スマートシティ）
（７）化学プラント
（８）組み立てプラント２
（９）ビル制御システム２

模擬システム：（１）排水・下水処理プラント

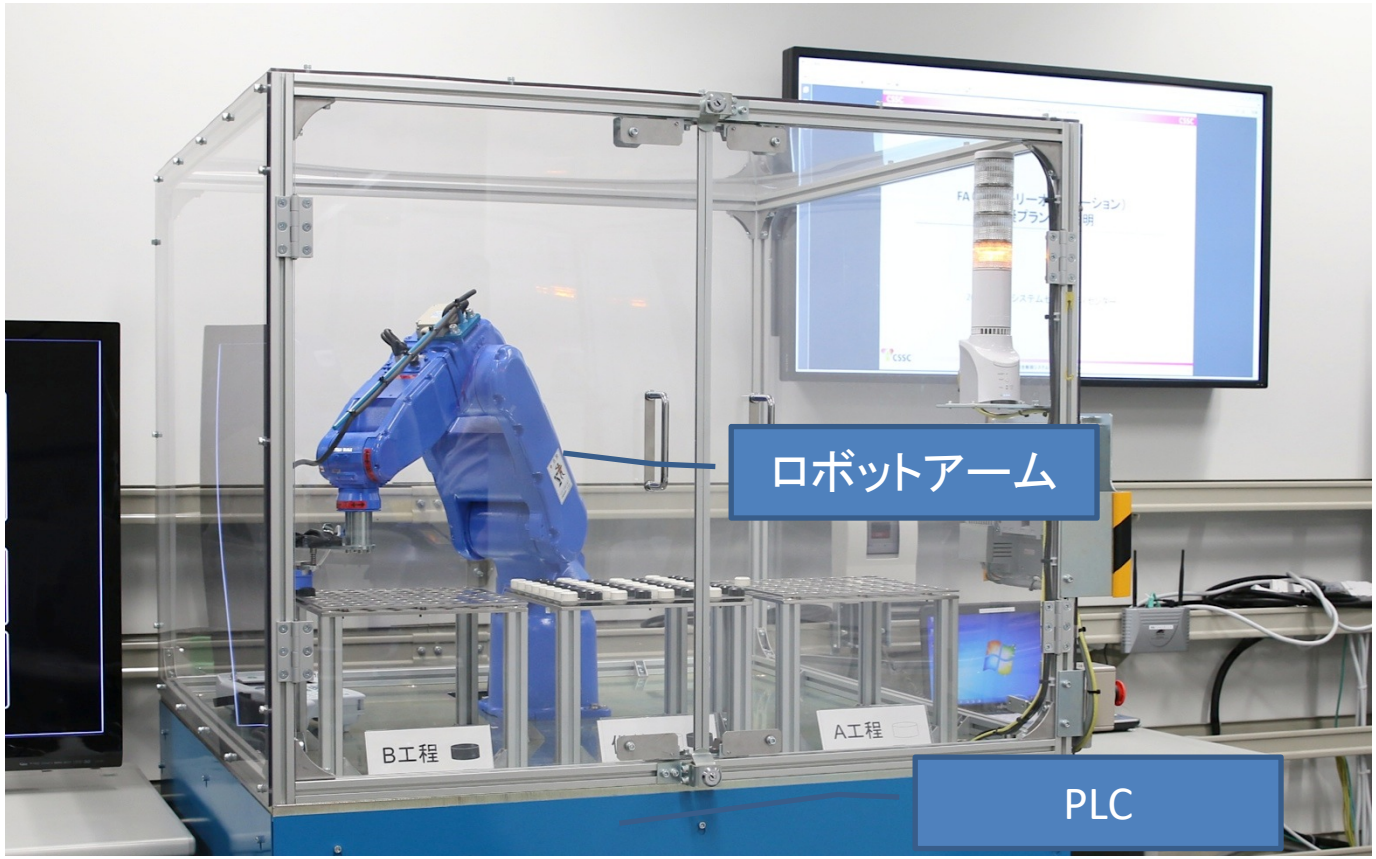


下水処理で多く用いられている汚泥と水の分離を行う沈殿槽の一部を模擬している
コントローラは流入水量が一定となるように制御している

模擬システム：（２）ビル制御システム

模擬プラント室の照明及びエアコン(模擬装置)の制御を行っている

模擬システム：（３）組立プラント

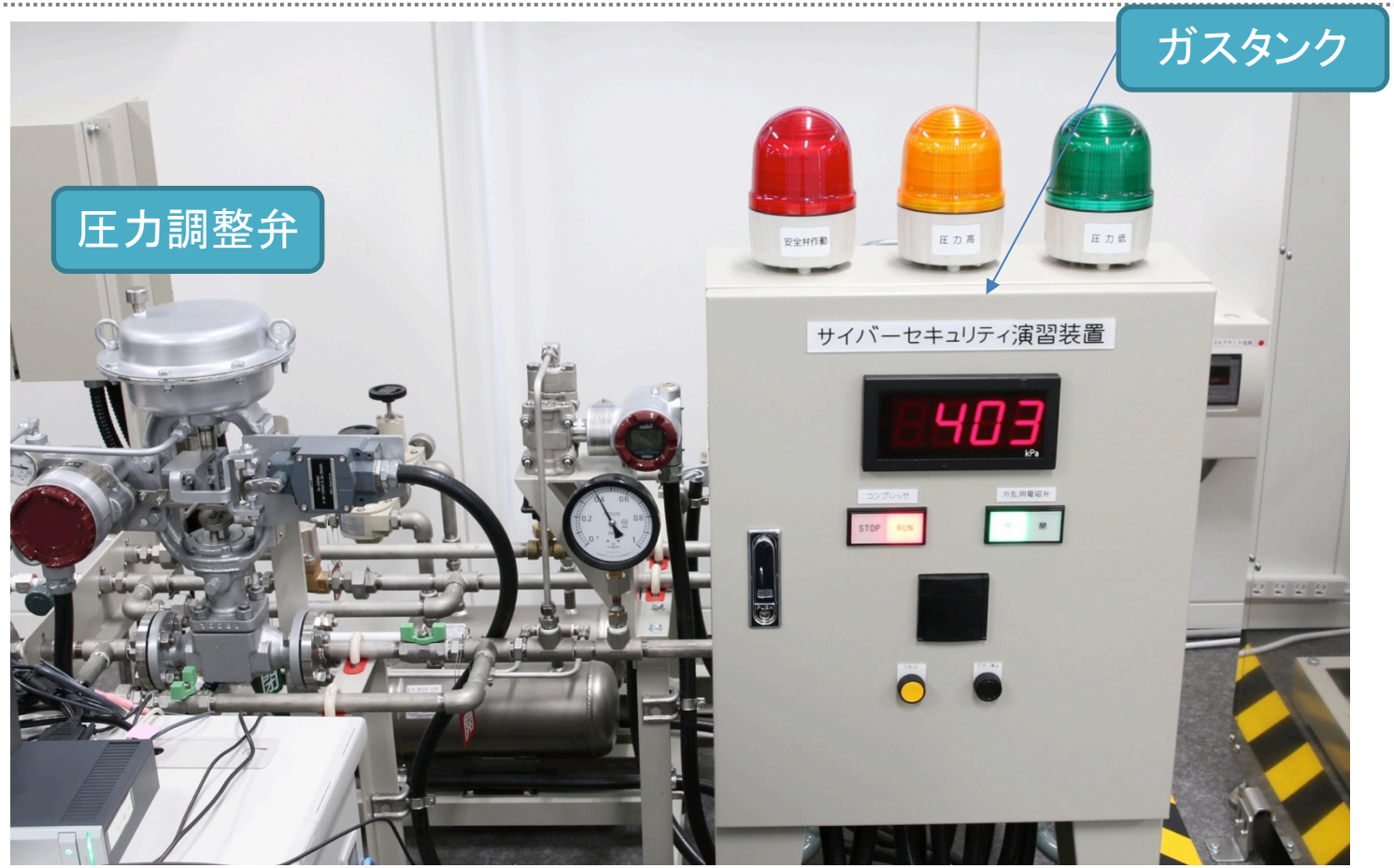


自動車組み立て工場の一部のロボット(部品のより分け)を模擬している
中央の部品を白い部品をA工程、黒い部品をB工程に配置する

模擬システム：（４）火力発電所訓練シミュレータ

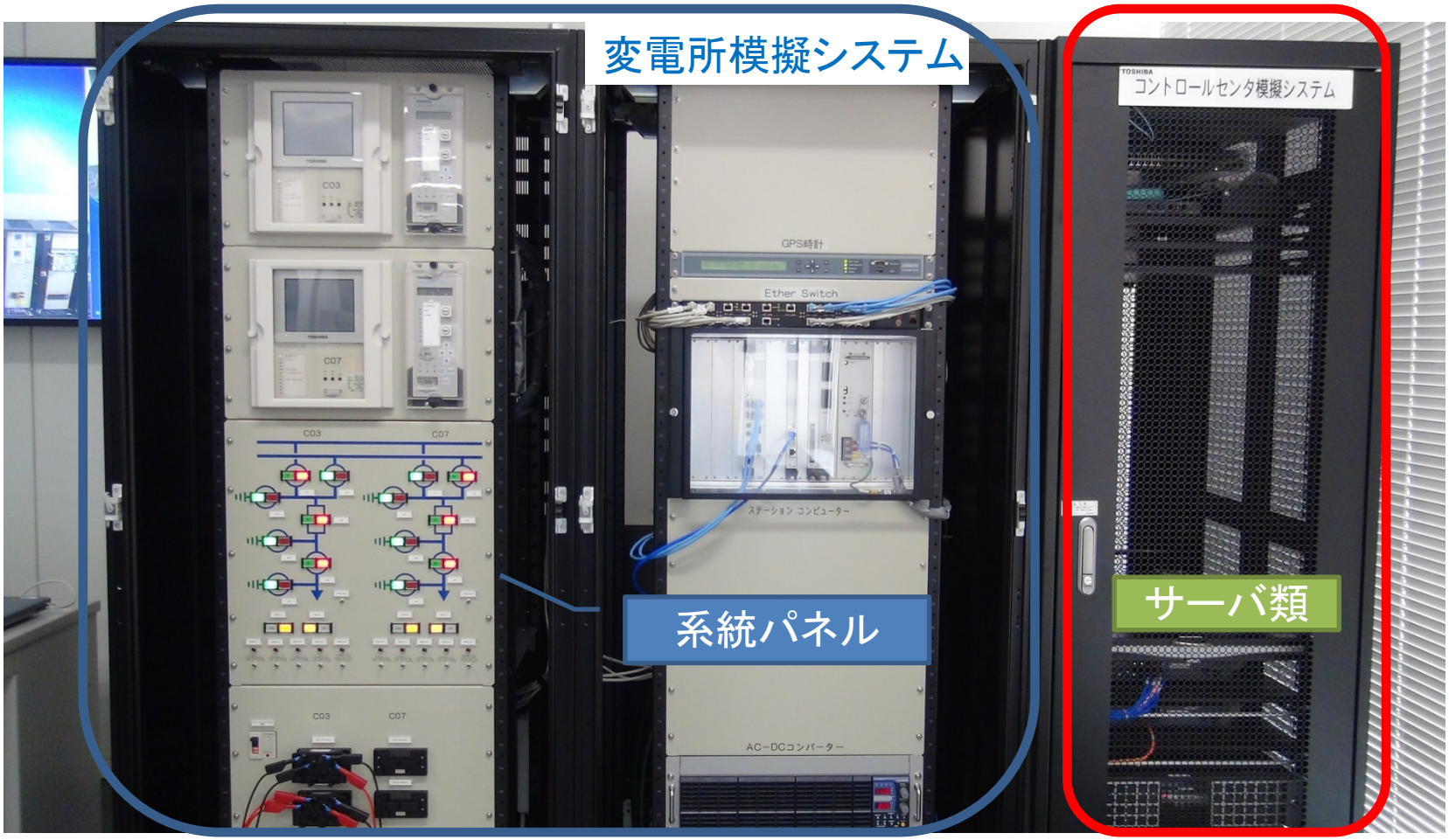
火力発電所に設置されている訓練シミュレータ装置
運転監視員が日常の訓練で使用しているシミュレータ(主に機器の故障などを想定)に
サイバーインシデントが発生したときの挙動を実装

模擬システム：（５）ガスプラント



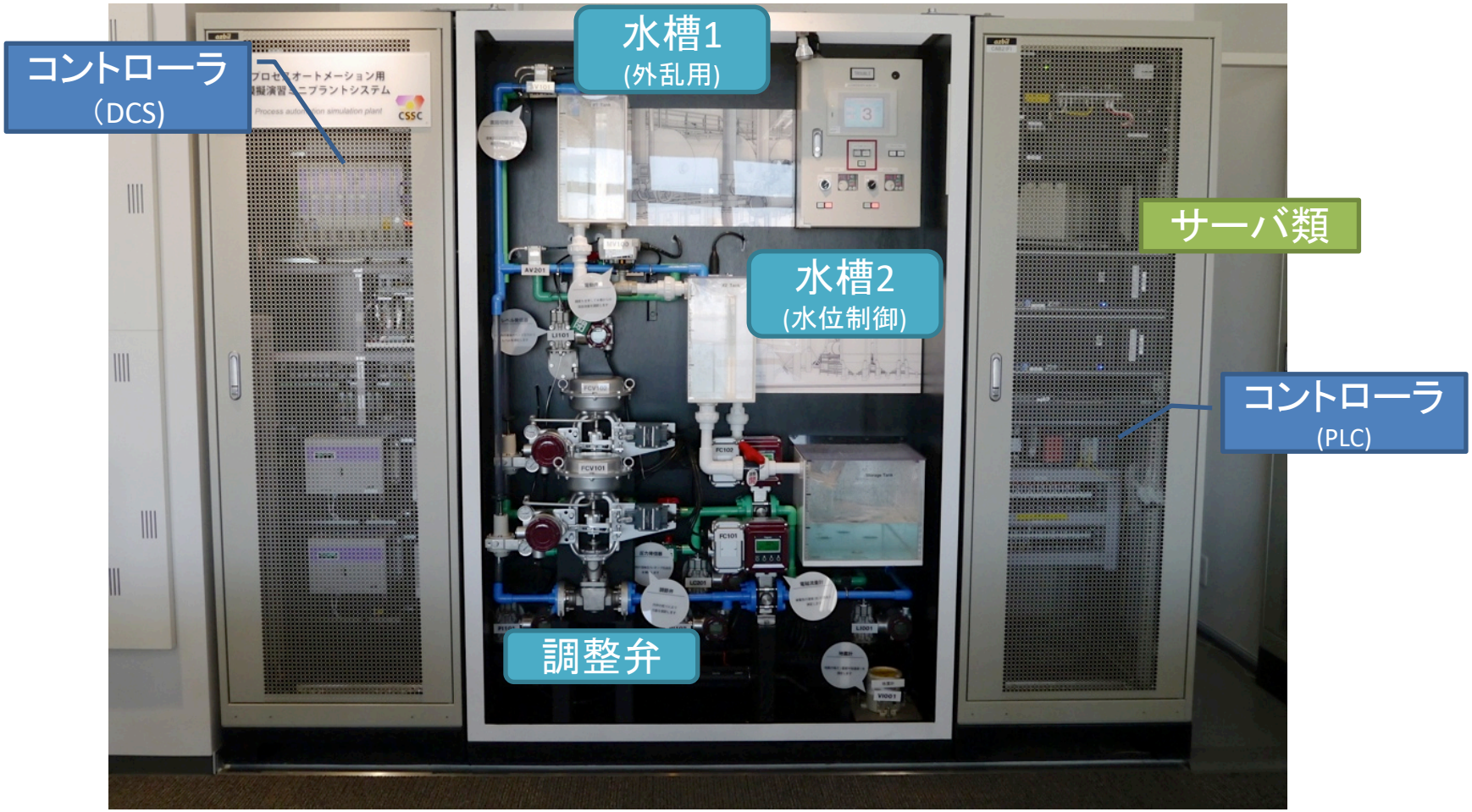
表示盤の背面に設置している、ガスタンクの圧力を一定とする制御を行っている

模擬システム：（６）広域制御（スマートシティ）



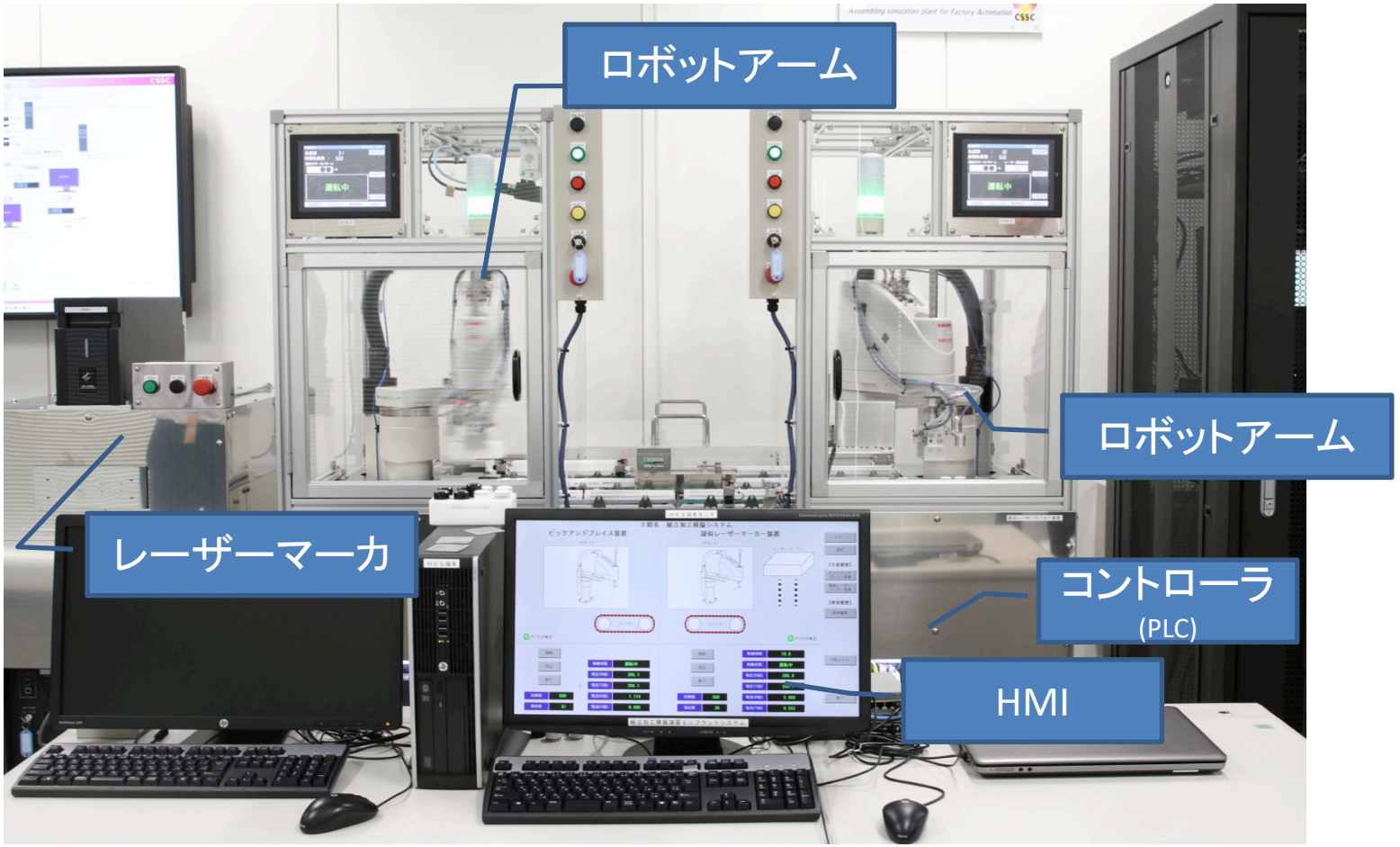
スマートシティを構成するコントロールセンタ及び変電所の模擬システム
送電系統などをコントロールセンタから集中操作可能

模擬システム：（７）化学プラント



中央に設置されている水槽2の水位一定制御を行っている
上段に設置されている水槽1は水槽2の水位を変化させる外乱要素となる

模擬システム：（８）組み立てプラント２



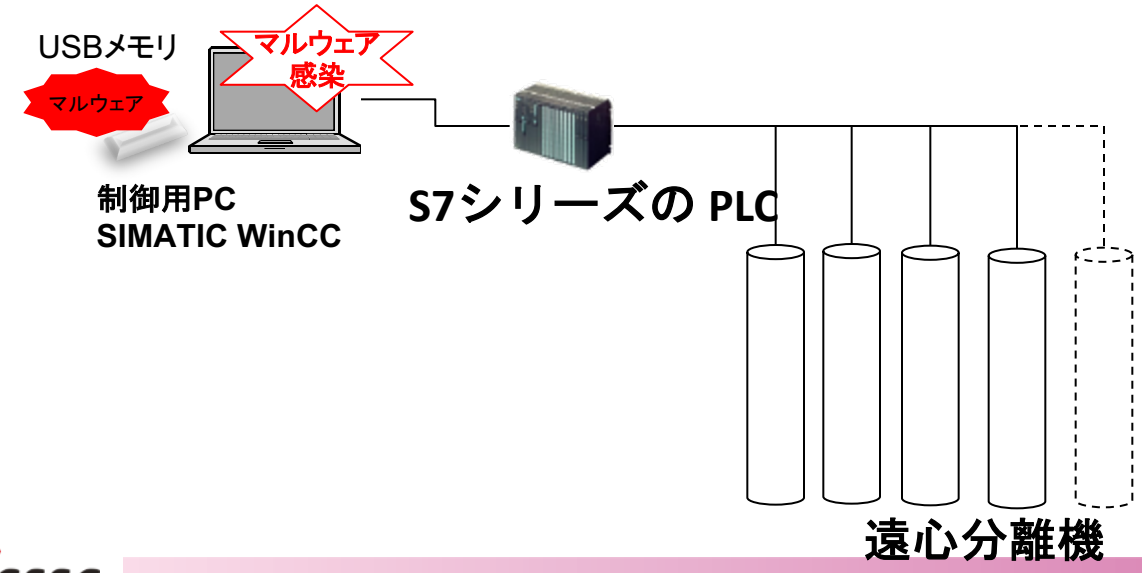
自動車組み立て工場の一部のロボット(部品のより分け)を模擬しており、
ロボットアームで部品を台座に載せ、レーザでマーキングを施す。

模擬システム：（９）ビル制御システム２

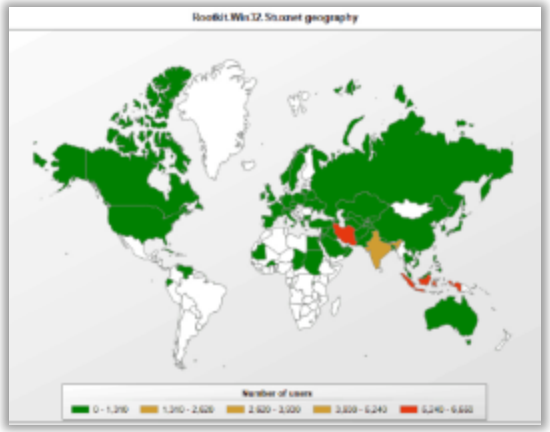
空調と照明の制御を行うビル制御システム。

付録： Stuxnetの概要

- 2010年9月に、イラン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
- 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
- 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
- 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-cyber-weapon-aimed-at-an-iranian-nuclear-site/