自己紹介　橋本芳宏

名古屋工業大学 社会工学科 経営システム分野　教授

（制御系セキュリティに関して）

2011年～2012年　経済産業省
　制御システムセキュリティ検討タスクフォース
　人材育成WG 委員
2012年～2014年　IPA（情報処理推進機構）
　制御システムワーキンググループ委員
2016年～　内閣府 戦略的イノベーション創造プログラム
　重要インフラ等におけるサイバーセキュリティの確保
　セキュリティ人材育成 委員
2017年～　IPA産業サイバーセキュリティセンター講師

名古屋工業大学制御システムセキュリティWS開催
　2015年3月19,20日　13社18名参加
　2015年8月26,27日　30社74名参加
　2016年3月29,30日　26社47名参加
　2017年9月12,13日　29社47名参加
　2018年3月6,7日　　15社21名参加
　研究室でのサイバー攻撃のデモにはのべ500名以上来訪

（プロセス制御に関して）

2010年～　計測自動制御学会 プロセス塾講師

（略歴）

1985年　京都大学化学工学専攻博士課程（単位取得退学）
1985年　名古屋工業大学 生産システム工学科 助手
2003年　名古屋工業大学 システムマネジメント学科 教授
　　学内組織再編を経て、現在にいたる

SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

事業年度：平成27年度～平成31年度

大学、企業、国立研究開発法人等

研究者　　研究者

SIP研究開発テーマ

(a) コア技術

- 制御・通信機器、IoT向けの真贋判定技術
- システムの動作監視・解析・防御技術

(b) 社会実装技術

- 適合性確認のあり方と仕組みの検討
- 情報共有・評価検証プラットフォーム技術
- 重要インフラセキュリティ人材の育成

マルウェア分析　内部統制
物理セキュリティ　入口出口対策
データセキュリティ
ファイアウォール

既存の認証制度（EDSA, JISEC, JCMVP, ・・・）
ICTや金融のISAC
IT人材

社会実装（重要インフラ）



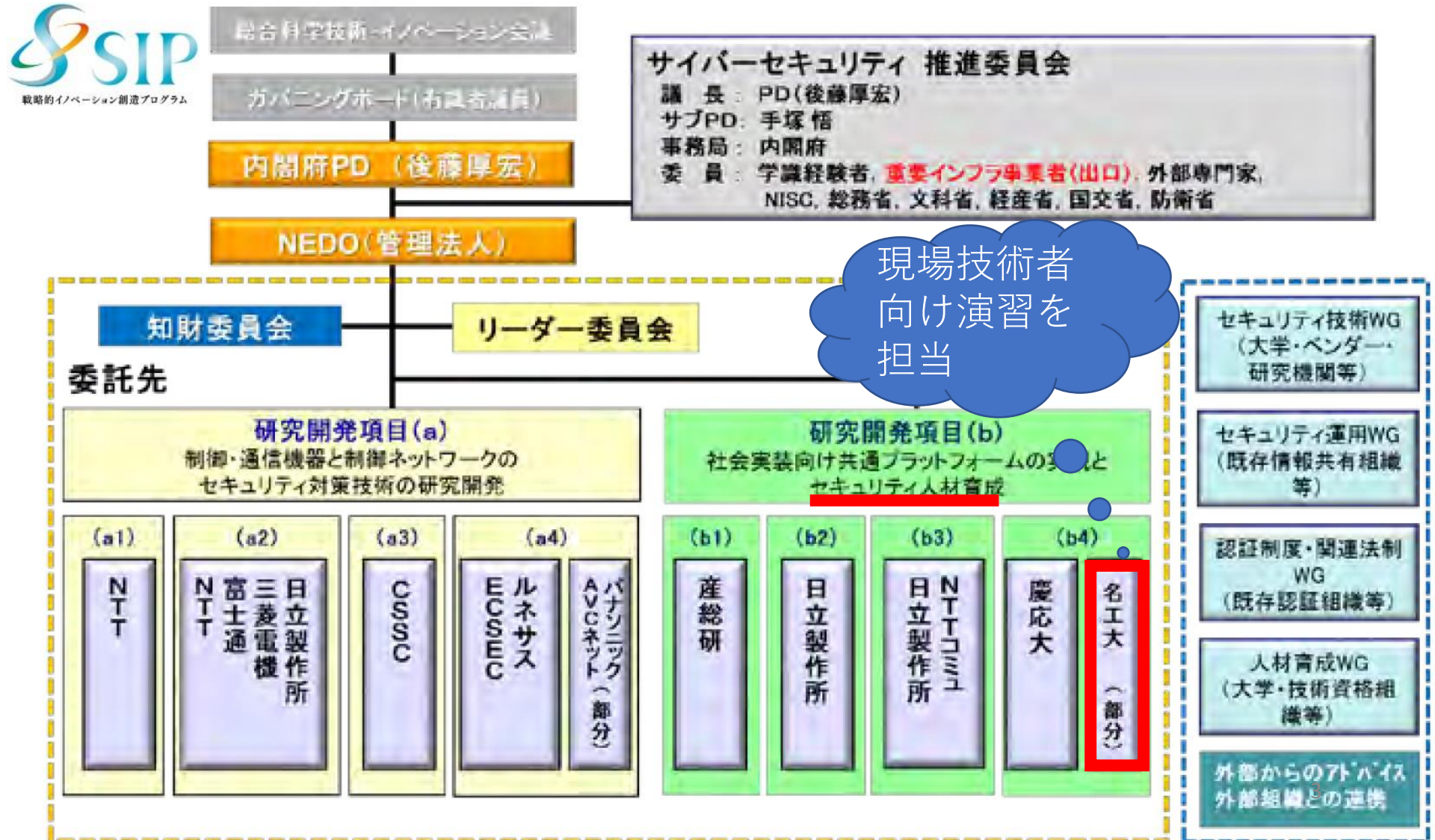

慶応大学がメインで、名工大も人材育成に参加

2020年までに、現場の技術者を対象に1000人規模の育成を目標

オリンピックの安心・安全に貢献

戦略的イノベーション創造プログラム(SIP)
重要インフラ等におけるサイバーセキュリティの確保

- 事業年度：平成27年度～平成31年度、平成28年度予算：25億円



IPA 産業系サイバーセキュリティ推進センターの設立
企業等でセキュリティ対策の中核を担う人材の育成

商務情報政策局 サイバーセキュリティ課
03-3501-1253

産業系サイバーセキュリティ推進事業
平成28年度第2次補正予算案額 25.0億円

事業の内容

事業目的・概要

- 情報システムに留まらず、社会システム全体を標的としたサイバー攻撃のリスクが高まっています。国家として、安全・安心な社会を築くために、特に、重要インフラや我が国経済・社会の基盤を支える産業における、サイバー攻撃に対する防護力の強化は必須です。
- そのため、独立行政法人情報処理推進機構（IPA）に産業系サイバーセキュリティ推進センター（仮称）を設置し、官民が共同してサイバーセキュリティ対策の中核となる人材を育成します。
- 具体的には、企業等から派遣された研修員が、ホワイトハッカーや研究者とともに、情報系システムから制御系システムまで全体を想定した模擬プラントを用いた演習や対策立案を行うため、模擬プラントの整備や攻撃用ツールの購入にかかる費用、調査費用等を支援します。

成果目標

- 模擬プラント等を活用し、重要インフラ事業者等において、サイバーセキュリティの総合的な戦略立案を担う人材を毎年100人程度育成します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → （独）情報処理推進機構

事業イメージ

産業系サイバーセキュリティ推進センター

- 情報系システムから制御系システムまで、システム全体を想定した**模擬プラントを設置**し、企業等でセキュリティ対策の中核を担う人材がホワイトハッカーや研究者と共に**システムの検証や演習**を実施。
- 自社のシステムのリスクを認識しつつ必要なセキュリティ対策を判断できる人材を育成。

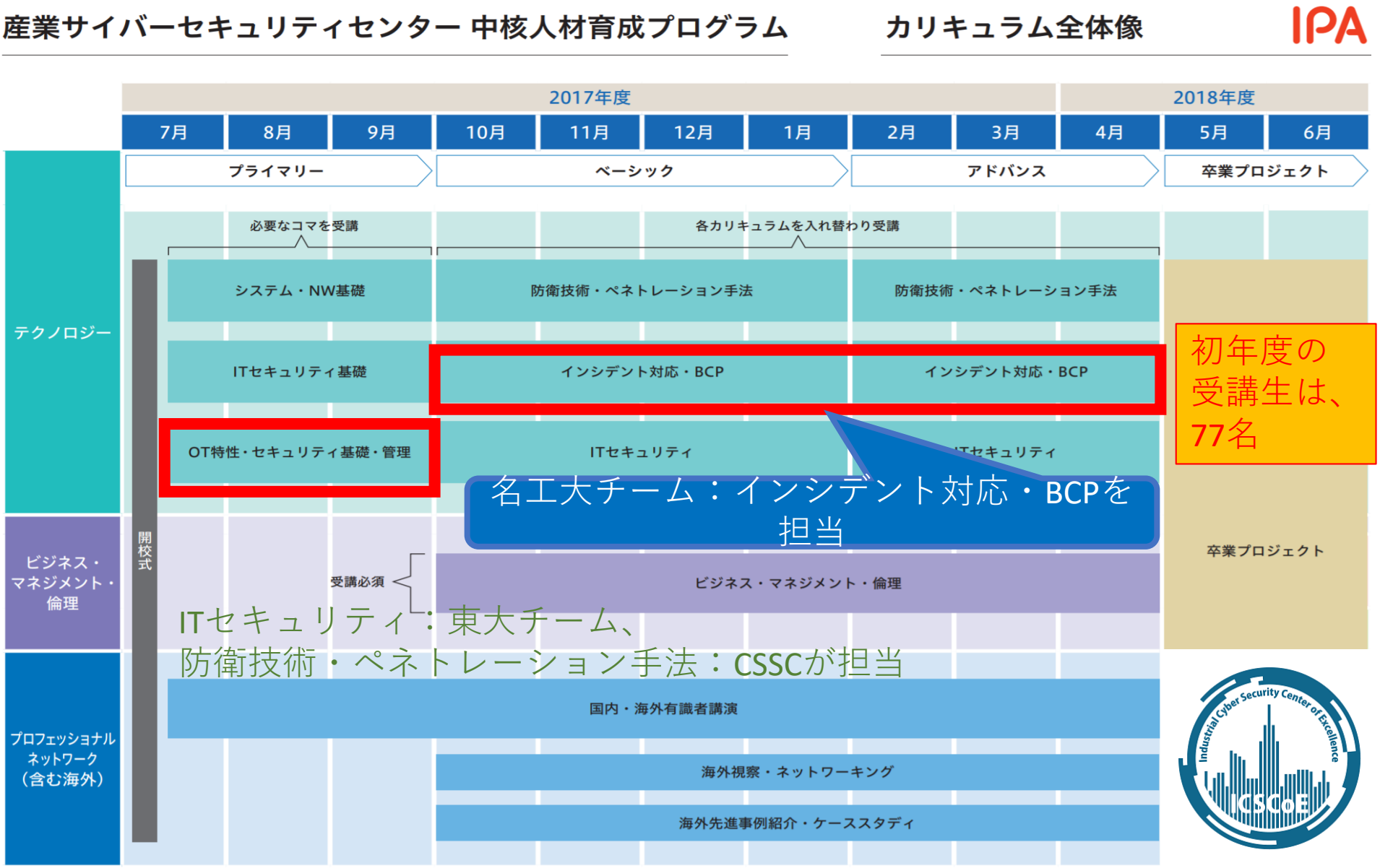
演習のイメージ

①セキュリティ、ネットワーク、制御システムの基礎ネットワークやシステム構築の演習
↓
②多様な攻撃パターンへの対応訓練
↓
③講師が作成したシナリオに基づく演習
↓
④演習シナリオを研修員自らが作成、実践

サイバーセキュリティ対策の中核人材育成による重要インフラ・産業のサイバーセキュリティ強化

各企業で、自社の演習を企画作成推進できる人材を毎年100人程度育成

IPA ICSCoE(Industrial Control Security-Center of Excellence)



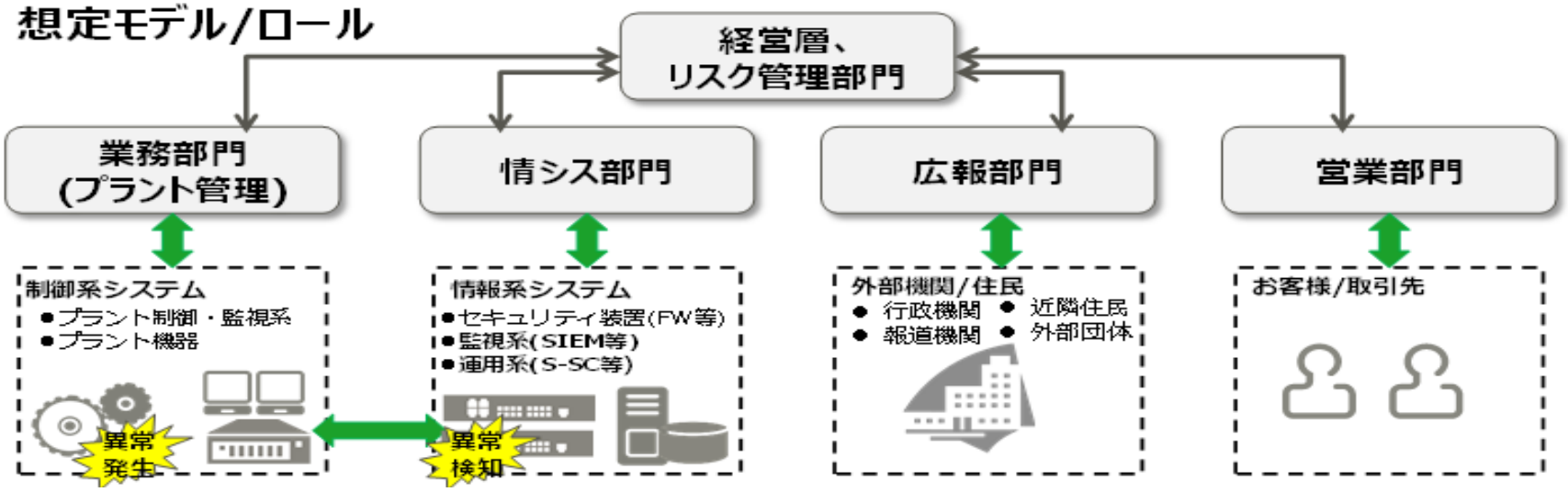
名工大制御系サイバーセキュリティWS

（第1回）2015年3月19,20日 13社18名参加
（第2回）2015年8月26,27日 30社74名参加
（第3回）2015年3月29,30日 26社47名参加
（第4回）2016年9月27日 32社54名参加
（第5回）2017年9月12,13日 29社47名参加



現場のインシデント対応だけでなく、多くの部門の連動の演習

■ 想定モデル/ロール



VECの制御システムセキュリティ研究分科会の“つるまいプロジェクト”参加企業

BSIグループジャパン株式会社
株式会社ICS研究所
株式会社MHPSコントロールシステムズ
NTTコミュニケーションズ株式会社
アズビル株式会社／
アズビルセキュリティフライデー株式会社
アドソル日進株式会社
株式会社カスペルスキー
シュナイダーエレクトリック株式会社
株式会社立花エレテック
トレンドマイクロ株式会社
千代田システムテクノロジーズ株式会社
日本シノプシス合同会社
日本ダイレックス株式会社
日本電気株式会社
株式会社ベルチャイルド
マカフィー株式会社
横河電機株式会社

2017年4月24日（月）
ペネトレーションテスト
トライアル開始記念撮影

名古屋工業大学にて
前列は、当日参加VEC会員
後列は、名工大メンバー

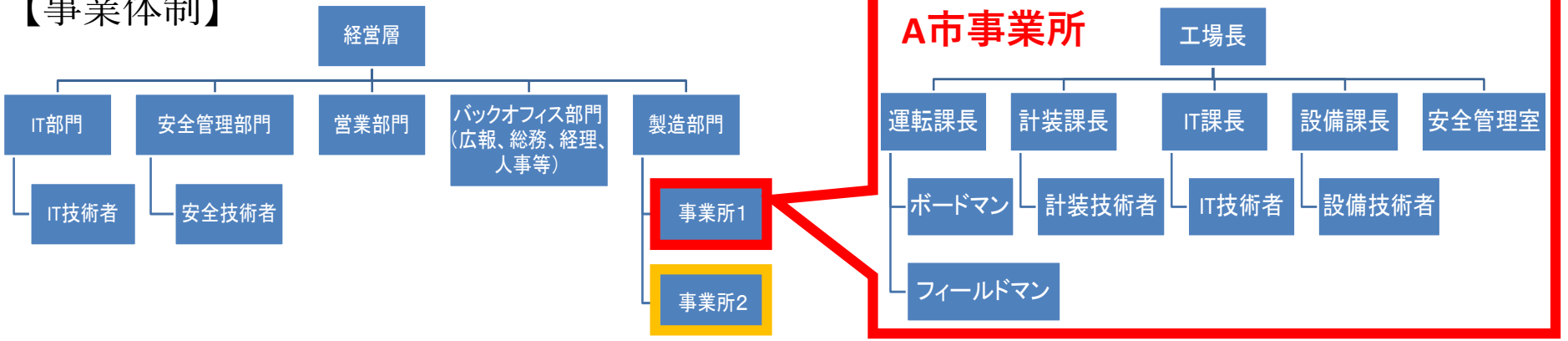
計装配線、PLCプログラム
仮想環境整備、OPC-UA
SCADA作成、監視ツール
導入など、学生が担当

越島エナジー（地域冷暖房サービス）

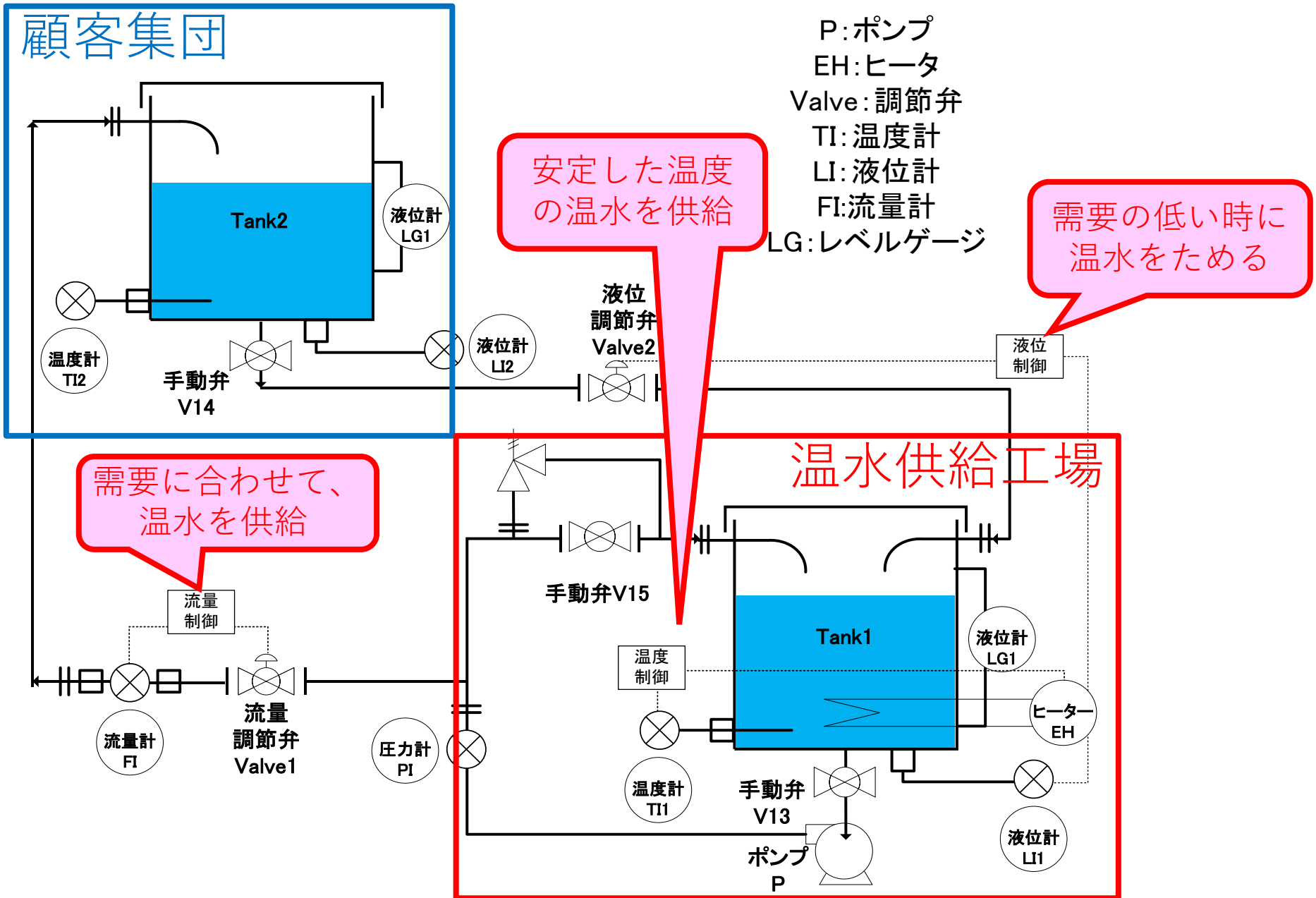
街、オフィス、商店、病院、データセンター
などに安定した熱源をお届けし、
地域の安全・安心な生活をささえます。



【事業体制】

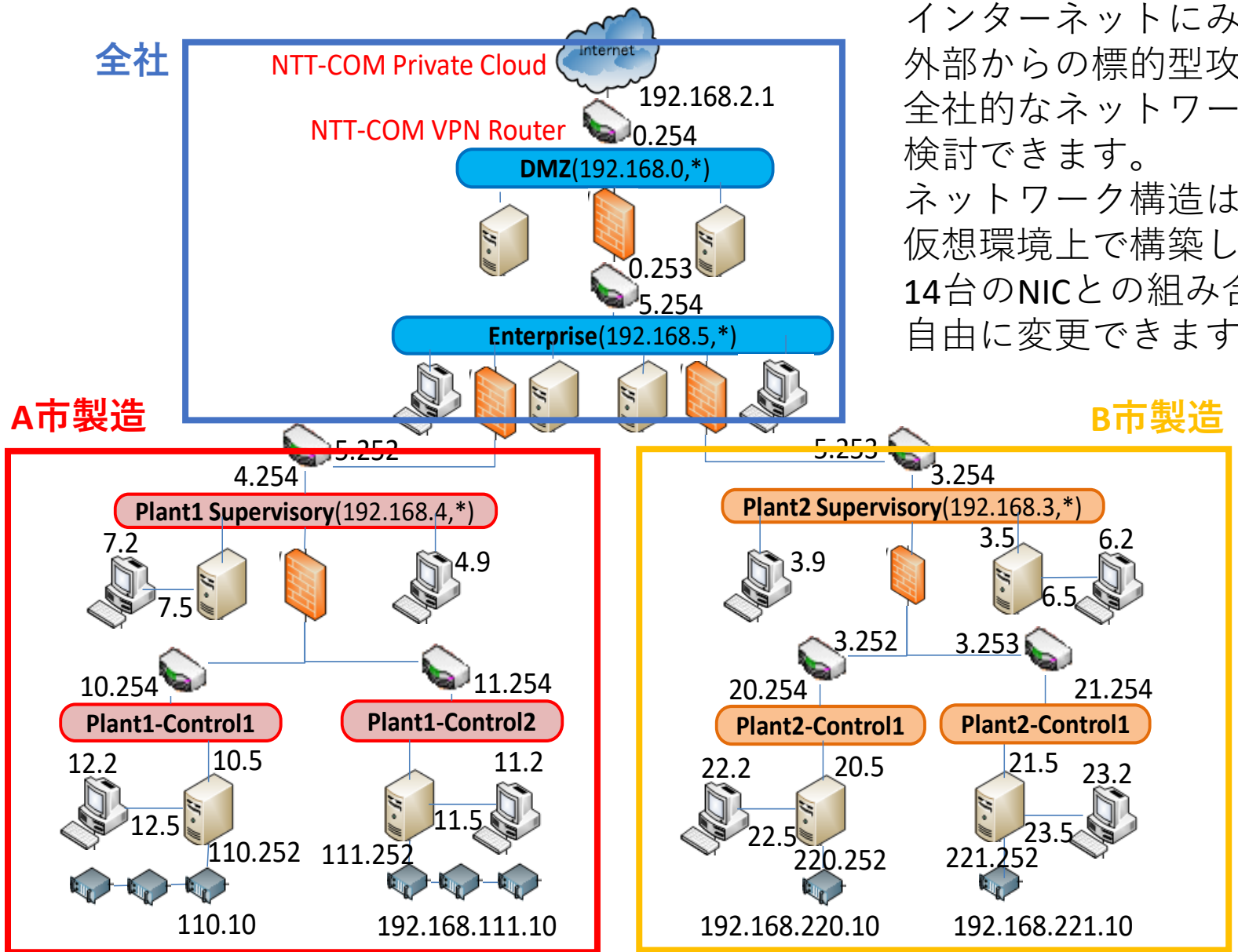


地域暖房サービスのシステム構成

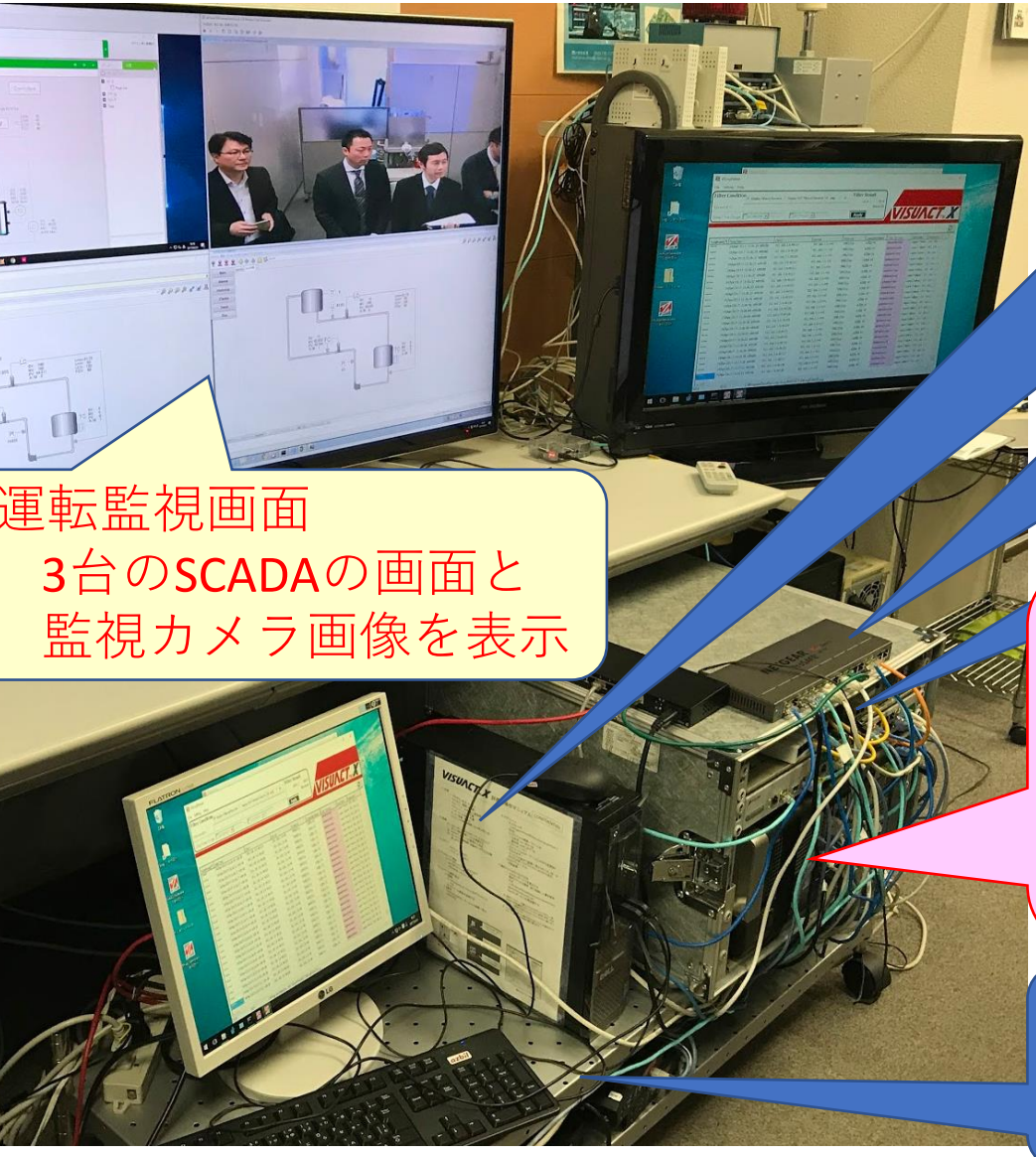


越島エナジーネットワーク構成

NTT-COMのプライベートクラウドを
インターネットにみなして、
外部からの標的型攻撃にも、
全社的なネットワークを模試して
検討できます。
ネットワーク構造は、Vmwareの
仮想環境上で構築しているので、
14台のNICとの組み合わせで、
自由に変更できます。



ネットワーク構築環境とその監視システム



運転監視画面
3台のSCADAの画面と
監視カメラ画像を表示

Azbilの監視システム
VISUACT-X

4チャンネルのミラー出力を行う
インテリジェントハブNET GEAR

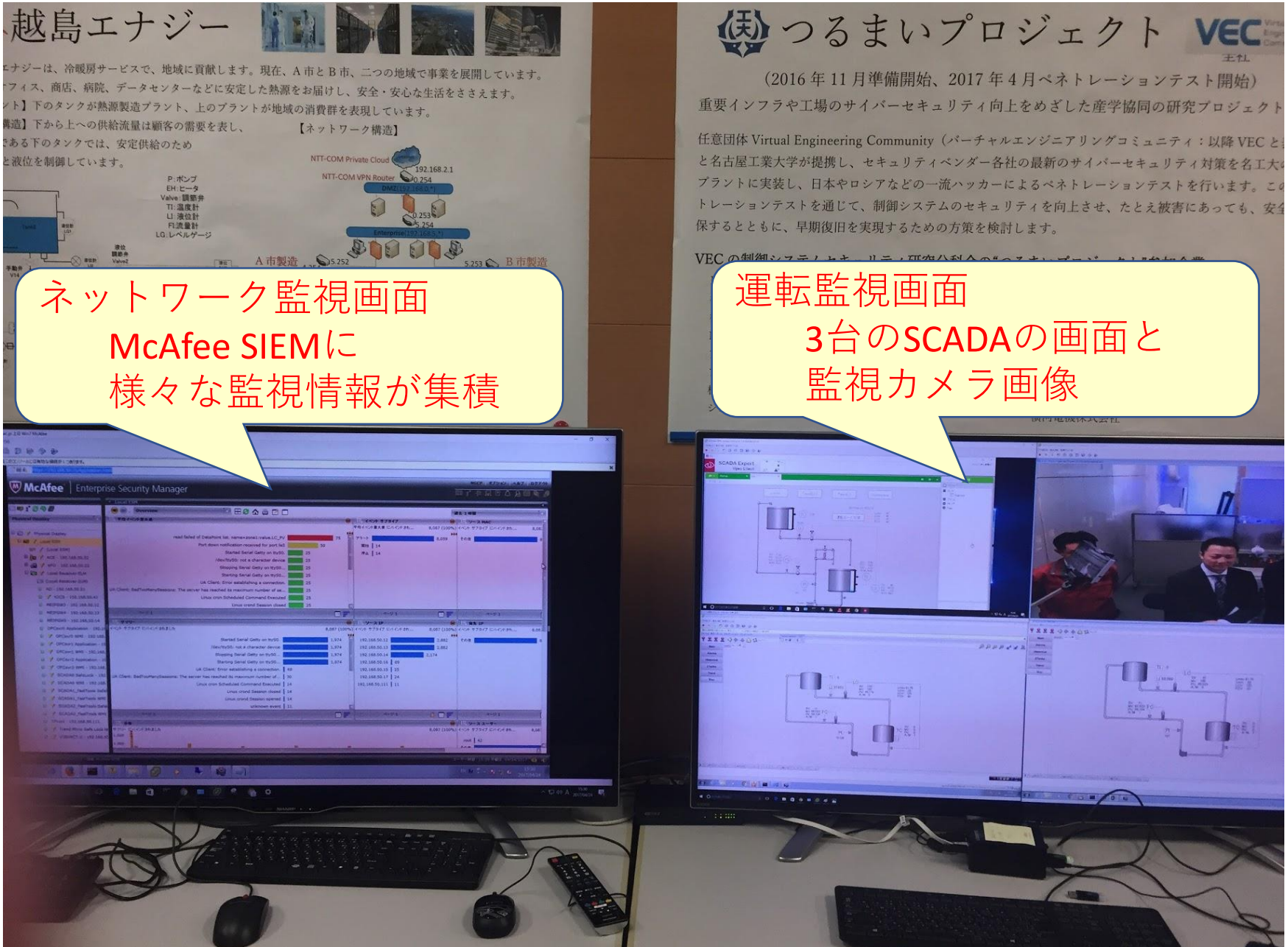
8チャンネルの監視と遮断を行う
インテリジェントハブTiFront

すべてのネットワーク環境を構築し、
14のNICをもつVmwareサーバー

Trendmicroのホワイトリストや
KasperskyのKICSなど
様々な最新ツールを実装

すべての監視環境を集約し、
ルールベースでの監視結果を出力する
McAfee SIEMを実装した小型PC

つるまいプロジェクト 監視画面



トライアル中の模様

監視画面をのぞきながら、現在の攻撃状況を推論