資料４
科学技術・学術審議会
研究計画・評価分科会
核不拡散・核セキュリティ作業部会
(第22回)
R4.1.11

サイバーセキュリティ分野における人材育成

東北大学大学院工学研究科技術社会システム専攻

高橋　信

自己紹介

- 東北大学大学院工学研究科　教授
- 専門：原子力工学、認知工学、安全工学、ヒューマンファクタ、リスクコミュニケーション、脳科学

航空管制業務の安全性に関する研究

認知シミュレーションによる安全性評価

想定外事象への対応方策の研究

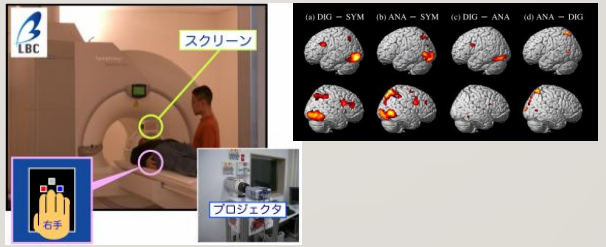
運転訓練・現場のルールの認知心理学的面からの再構築

原子力システムの安全性向上

制御システムのサイバーセキュリティ

先端診断技術のサイバー攻撃早期認識への応用

脳機能解析を用いたインタフェース評価

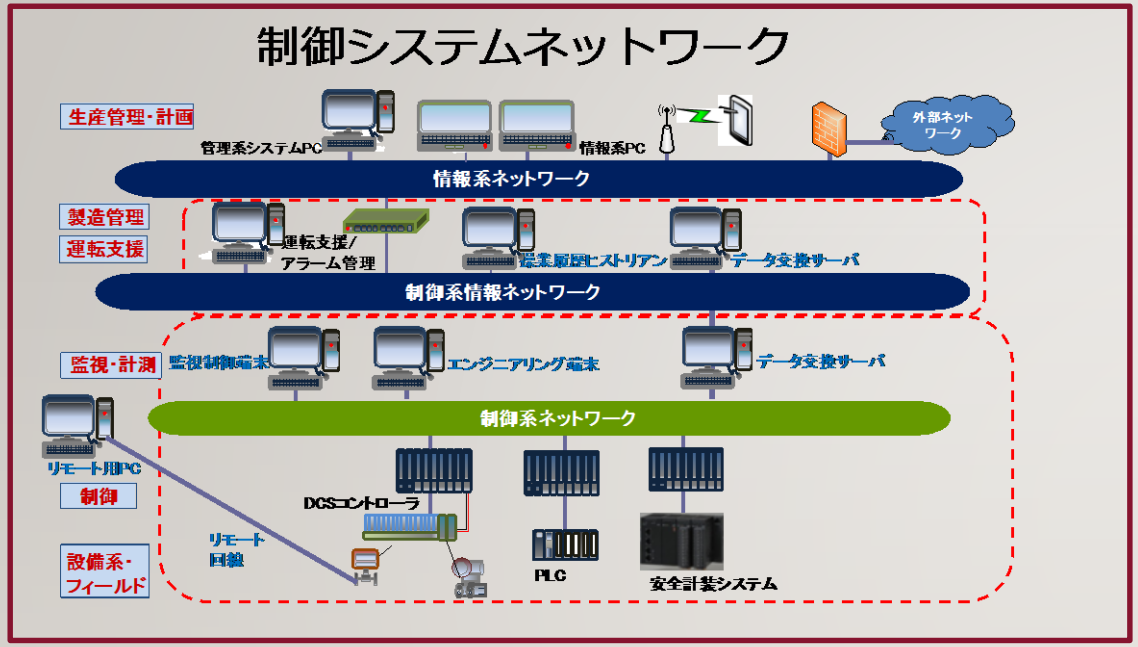


インタフェース評価への脳科学的知見の応用

本日の話題提供内容

- ✓ 制御システムセキュリティセンターにおける人材育成
- ✓ 東北大学におけるセキュリティ人材育成
- ✓ Security と Safety

制御システムセキュリティセンター
Control System Security Center: CSSC



- 制御情報ネットワークは*IP*（*Internet Protocol*）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

- 現代社会を支える多くのインフラが制御システムネットワークに依存
- 密結合で相互依存性の高い現代のシステムは脆弱性が高い
- サイバー攻撃による影響は重大になり得るため外部からの攻撃に対しての防御が必要
- 日本でも既に多くのインシデントが発生しており工場停止や業務停止の事例も
- IoTやDXを推進する上でサイバー攻撃に対するリスク認識が低いのが現状

制御システムセキュリティセンター
Control System Security Center: CSSC

CSSC（技術研究組合制御システムセキュリティセンター）＊とは？

- ベンダー、ユーザーが知見を共有し研究開発を行う拠点＊＊
- 世界水準の制御システムセキュリティ＊＊＊に関する知見
- 制御機器のセキュリティレベルに関する国際的な認証活動
- サイバー攻撃に関する事例に関する知見とそれに対する対策
- サイバーセキュリティに関する人材育成ための教育コンテンツ

電力系統 

ガスプラント 

化学プラント 

ビルシステム 

実際に現場で使われている機器と同じDSC,PLCを使ったテストベッド

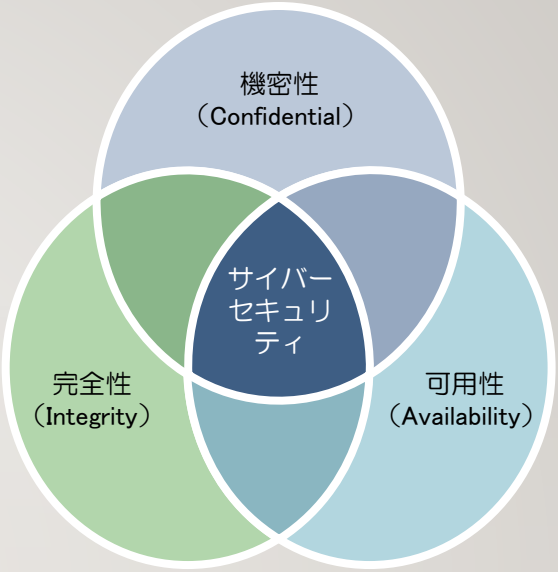
項番	制御システムへの典型的な攻撃シナリオ（ 全16シナリオの一部）
1	マルウェアや外部持込PCからのウィルス感染
2	超小型PCからの攻撃
3	情報系システムを介した攻撃
4	リモート接続端末を用いた攻撃
5	制御系ネットワークにおける不正操作
6	無線LANに係わる攻撃
7	機器に対する電磁波攻撃
8	計測機器への攻撃
9	外部のインフラからの供給途絶による機能不全
10	サプライチェーンリスク
11	建屋への物理攻撃による機能不全

⇔

項番	大項目	チェック項目（全400項目の一部）
1-1	USBメモリ等外部記憶媒体による既知ウィルス感染	管理された外部記憶媒体のみとする利用可能とするルールを整備すること
		許可されたUSBポート以外は原則利用禁止とするルールを整備すること
		USBポートを物理的に塞ぐこと
		USBポートの無効化を行うこと
		ウィルスチェックの確認を持込者の申請によるものとすること（ソフトと定義ファイル、実施日の明記を必須とする）
		外部記憶媒体等の隔離環境における最新ソフトによるウィルスチェックを事業者が行うこと
		複数ウィルス対策ソフトによるウィルスチェックを行うこと
		米国系および欧州系ウィルス対策ソフトによるウィルスチェックを行うこと
		端末とサーバにおけるホワイトリスト導入を行うこと

制御セキュリティと情報セキュリティ

- サイバーセキュリティとは、情報資産の機密性・完全性・可用性を維持することである。これらはサイバーセキュリティの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情報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

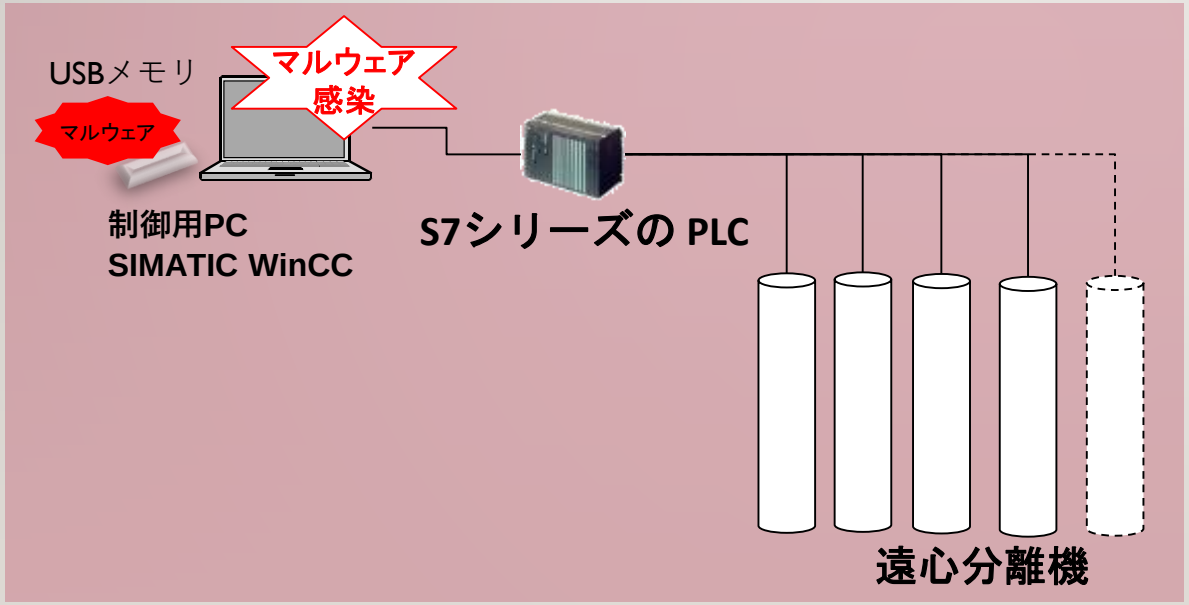


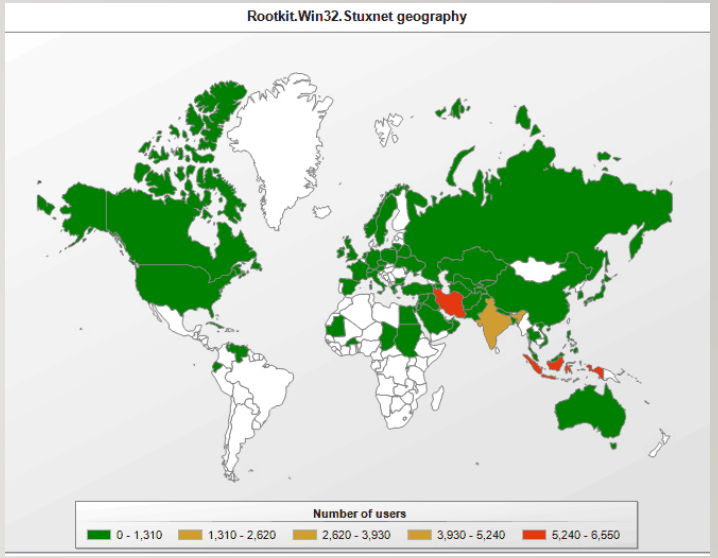
●制御セキュリティ
可用性　＞　完全性　＞　機密性

●情報セキュリティ
機密性　＞　完全性　＞　可用性

制御システムに対する最も有名なサイバー攻撃　STUXNET

- 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
- 四個の未知の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各国別感染数

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

東北大学におけるCSSCとの連携によるセキュリティ人材育成

”東北大学VISION2030”の重点戦略

- 情報環境の最適化と情報セキュリティ強化
  - 最先端のセキュリティ技術と知見を有するCSSCとの連携を通じて、他の大学とは一線を画する高いレベルでのセキュリティが実現
- コネクティッドユニバーシティ戦略の実現の条件となるセキュリティの確保
  - オンラインのセキュアな研究・教育フレームワークの実現
  - リモート制御・実験環境に関する　先端的知見の活用

東北大学におけるセキュリティ人材育成 原子力規制からの補助事業による規制人材育成

「連携教育研究プログラムによる俯瞰的知識を有する原子力規制人材育成」

代表：東北大学大学院工学研究科（量子エネルギー工学専攻）教授　橋爪秀利

＜補助事業の目的＞

本専攻における従来からの主要教育課題である原子力工学を理解するための各種物理学及び保全、バックエンド、生活環境復旧、原子力安全と規制に関する理解に加え、他専攻・他研究科の活断層、地震・津波・火山等の自然科学、耐震・建築等に関わる工学とサイバーセキュリティの基礎的素養と知識を身につけ、他分野の知見を俯瞰的に適用でき、将来の原子力分野における設計・建設、保守・運転、規制そして研究・開発の中核となりうる人材を継続的に輩出するための教育体制を構築することを本補助事業の目的とする。

Ⅰ.サイバーセキュリティ教育の実施

- Ⅰ-1) 大学における制御システムセキュリティ教育のカリキュラム構築
- Ⅰ-2) テストベッドの大学生教育に向けた改良（遠隔での実施の実現）
- Ⅰ-3) サイバーセキュリティ教育の実施

まとめ

- **サイバーセキュリティは「核セキュリティ」の一部に過ぎない**
  - 但し、「セキュリティ意識」という面では共通した側面も
  - 「核セキュリティ文化」？？？
- **サイバーセキュリティの技術的な面での教育は重要であるが、そこで得た知識は「攻撃」にも利用可能**
  - ホワイトハッカー的人材の育成は重要であるが諸刃の剣
- **サイバー攻撃に関する手法、技術は速い速度でアップデートされている**
  - 対策側も常にアップデートが必要
- **第一にサイバー攻撃のリスクを的確に認識することが必要**
  - 一般社会におけるサイバーリスクに関する認識は極めて低い
- **情報セキュリティと制御システムセキュリティの差異を認識することが必要**
  - 情報セキュリティ　→情報漏洩の阻止
  - 制御システムセキュリティ　→システムの安全の確保
- **「核セキュリティ」の目的を明確にすることが必要**
  - 原子力発電所の「安全」の確保？
  - 核物質の外部への持ち出しの阻止？
  - 核開発関係の情報の漏洩の防止？
  - インシデント発生時のフォレンジック

  ⎫ 人材育成という観点からは異なる資質が求められる