制御系システムと人間系システムの共存

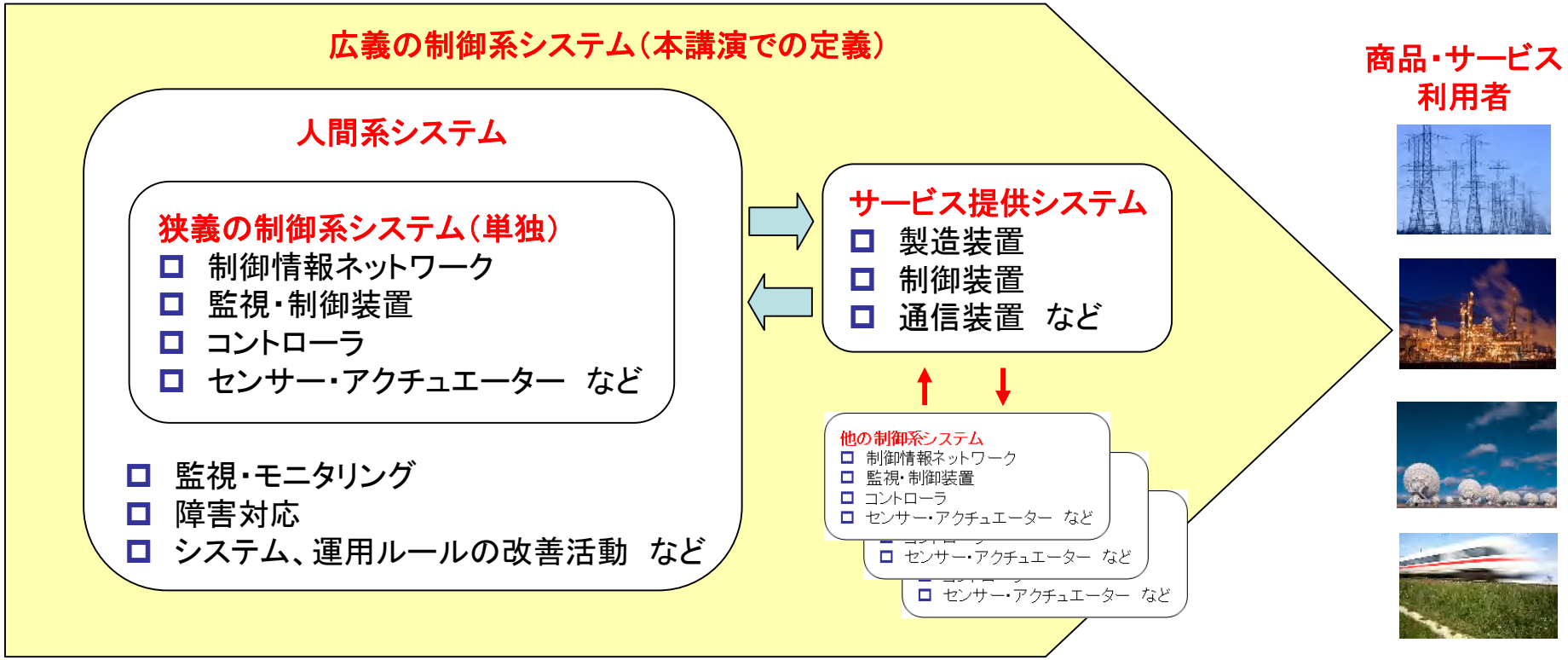
~ 今後の制御システムセキュリティのあり方に関する一考察 ~

2011年2月10日

渡辺研司
名古屋工業大学・大学院社会工学専攻

制御系システムとセキュリティ・マネジメントの範囲

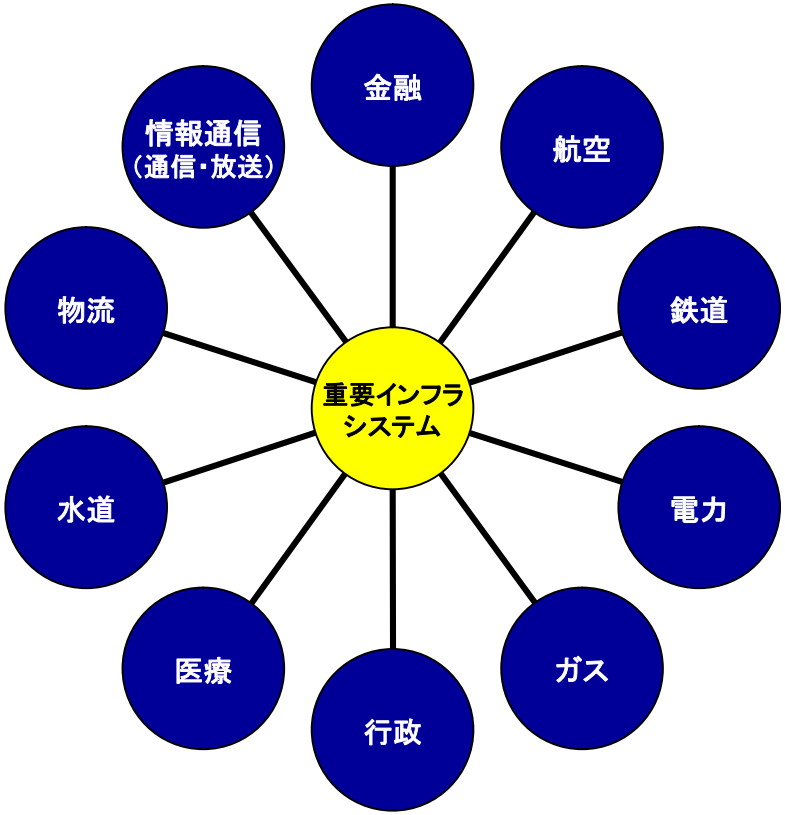
制御系システムの範囲とセキュリティマネジメントの対象範囲（概念例示）

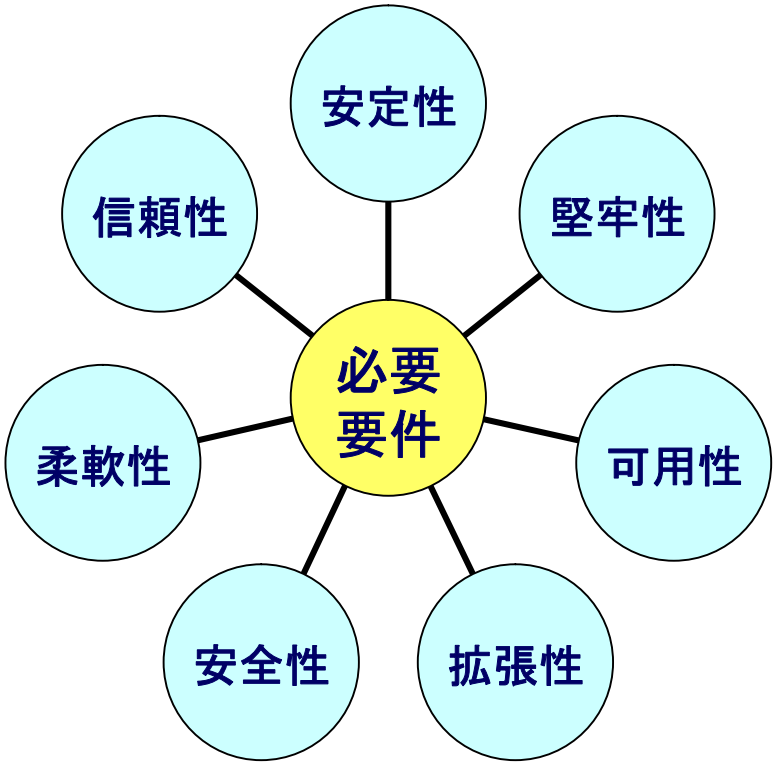


- 実際の制御は制御系システムと人間系システムの組合せで行われる
- 人間系システムとは監視、障害対応、システムや運用ルールの改善活動など
- セキュリティ・マネジメントには実際のサービス・機能への影響度分析が必要
- 広域・複合的なサービス・機能提供には複数の制御系システムが接続される

重要システムと求められる要件

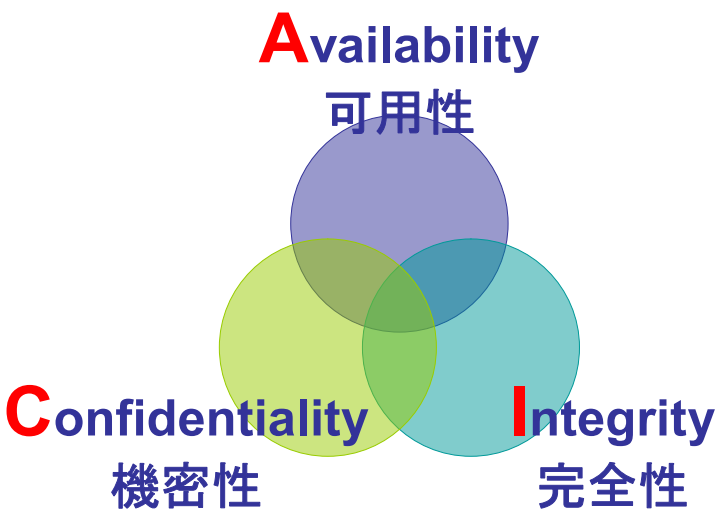
重要インフラシステムの要件





制御系システムのセキュリティ・マネジメント

セキュリティ・マネジメントのアプローチ

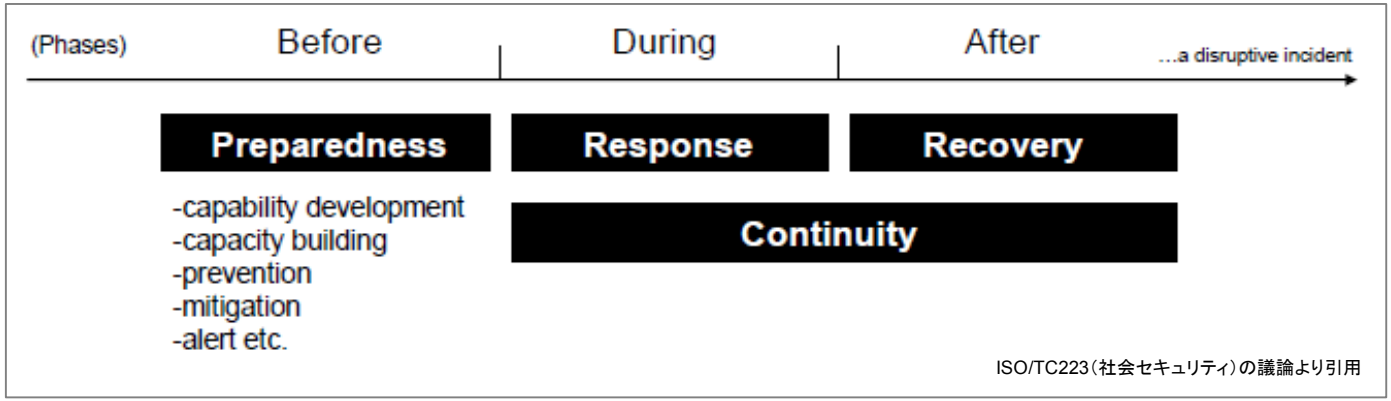


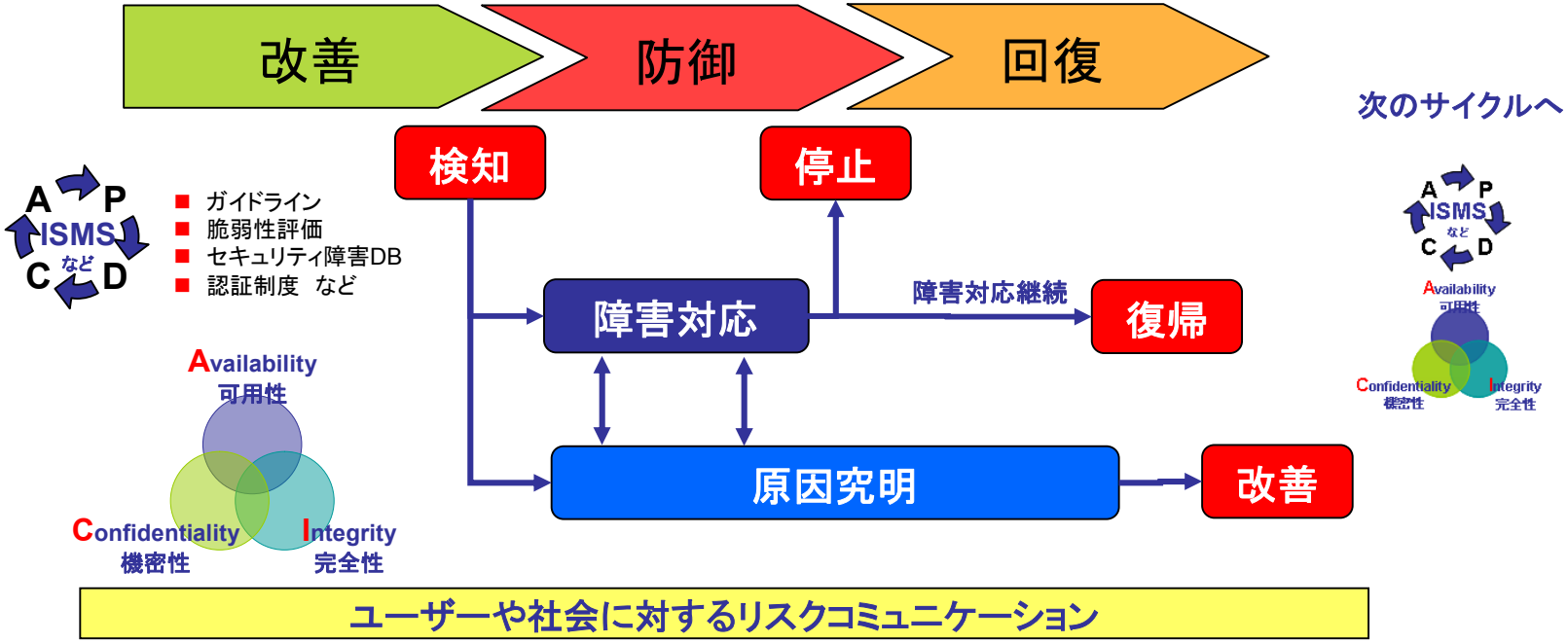
Dynamic Security Management
（動的セキュリティ・マネジメント）

- 情報システム全般にはC．I．Aの順で重点がおかれるが、制御系システムにはA．I．Cの順番をベースにフェーズに応じた可変的な運用が求められる
- 「新しいタイプの攻撃」の出現は今後も続くが、対症療法であってはならない
- 脆弱性の事前検知・意図的攻撃からの防護以外も含めた柔軟性が必要
- 原因事象もさることながら結果事象に着目することも必要
- 事前対策や水際作戦には限界
- 事故前提のレジリエンス（柔軟性のある回復力）を制御系（狭義）と人間系、更には商品・サービスの提供に関わるシステム全体で構築することが肝要
- 特に人間系システムにおける監視・検知、および障害対応における専門人材育成の強化と国内外の人的ネットワークの構築着手が急がれる

制御システム・セキュリティのフェーズ

改善・防御・回復の位置づけ整理





高度に自動化され接続されたシステム群の障害

2010年5月6日米国NY株式市場で見られたフラッシュ・クラッシュ

■ 2010年5月6日、ニューヨーク株式市場ダウ平均指数は14:30分には10,600ドル前後だったが、14:47には9,870ドルと一挙に**前日比9.2%とブラックマンデー以来の大暴落**を記録。15:00には10,410ドルまで回復。

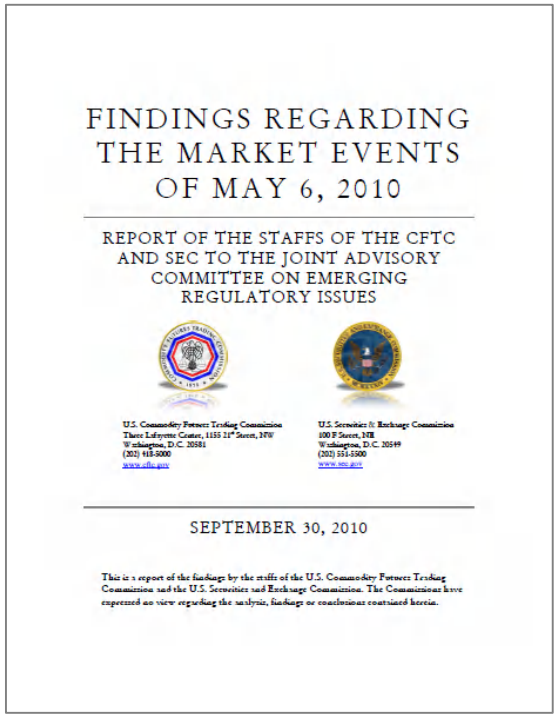
■ **原因究明は長期化**したが、その間、**①証券会社の誤発注**、**②プログラム・ミス**などが原因として報道された。いずれにしても何らかの理由で売買の需給バランスが瞬間的に崩れたことが引き金となり、**HFT（高頻度プログラム取引）**や、個別銘柄の**ボラティリティを制御する仕組み**が機能しなくなり、更に、同一銘柄が複数の市場で取引される**市場構造から、問題を増幅した**といえる。

【障害発生の背景】

- ミリ秒単位のHFT（High Frequency Trade：高頻度プログラム売買取引）の台頭
- 小口取引の急増（今回の直接的原因となったe-mini取引など）に伴う取引件数激増
- 指数取引の構成銘柄の複雑性の増加（組み入れ銘柄の多様化）
- 同じ銘柄に対して複数の取引市場が存在する証券市場の構造

今後の制御系システム・セキュリティへの示唆

本事例から得られる示唆



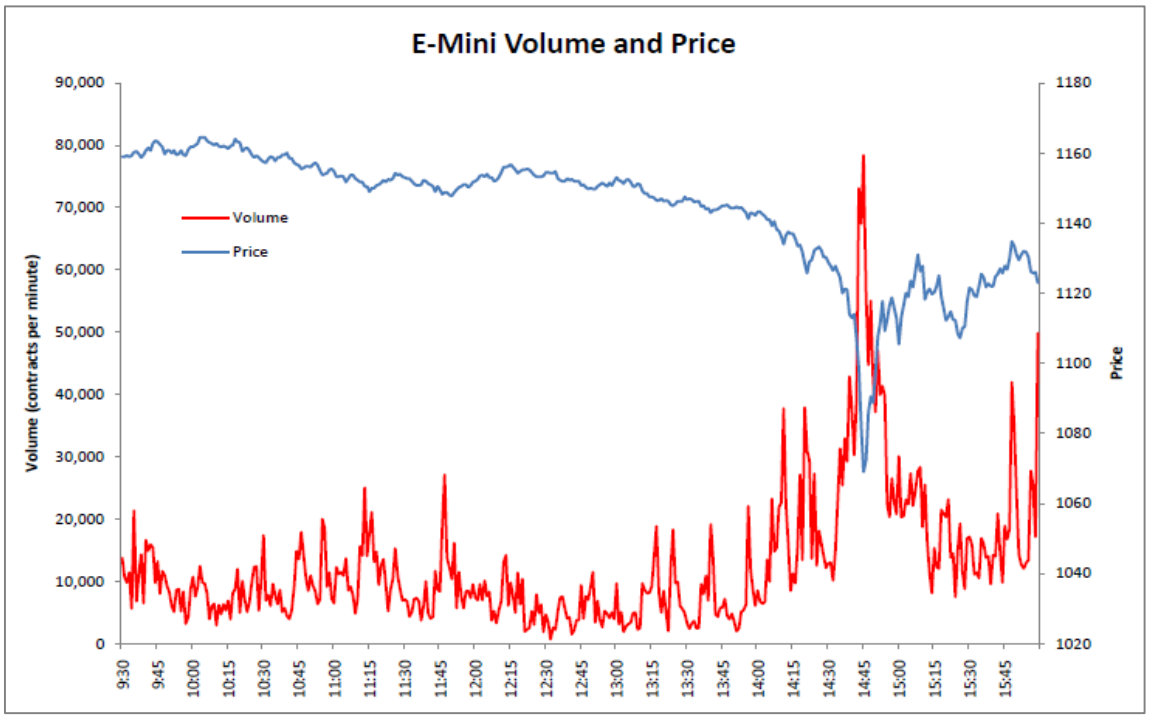
FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010

REPORT OF THE STAFFS OF THE CFTC AND SEC TO THE JOINT ADVISORY COMMITTEE ON EMERGING REGULATORY ISSUES

SEPTEMBER 30, 2010

This is a report of the findings by the staffs of the U.S. Commodity Futures Trading Commission and the U.S. Securities and Exchange Commission. The Commissions have expressed no view regarding the analysis, findings or conclusions contained herein.

http://sec.gov/news/studies/2010/marketevents-report.pdf



- 高度に自動化・高速化された株式売買システム（双方向高速データの膨張）
- 微小なゆらぎが大量データの連鎖増幅を短時間に呼び起こし、多数の制御系システムが接続された全体システムが大きくブレる結果となる（バタフライ効果・システミック・リスク）
- 制御系システムの個別最適化の集合体が全体システムの最適化には必ずしも直結しない
- サーキット・ブレイカー（異常時緊急停止）に関する運用ルール制定の重要性

自動化の落とし穴

Lisanne Bainbridge（英国・エンジニアリング心理学者）の定義

- 人間の仕事の容易な部分をとってしまい、難しい部分をさらに難しくしている。
- システム設計者は人間を信頼できない、非能率的なものとみている一方で、自動化できない仕事を人間に負わせている。
- 高度に自動化されたシステムにおける人間の仕事は、自動装置が設計どおりに動いていることを確認するだけ。モチベーションの低下が発生したり、極めて稀にしか起こらない異常を見つけることが難しくなる。
- めったに故障することのない自動化システムの、緊急時に必要なスキルを人間が実践する機会を奪っている。
- 最終的に、人間の訓練に膨大な費用がかかる仕事だけを残す。

→ **飛行機の航行管理・制御システムのモード選択（知覚/注意の失敗）**

技術リスクと高度技術社会への対応

制御系システム・セキュリティには技術的な部分のみならず人間系システムの強化が重要

- 20世紀に誕生した技術は、人類が快適で豊かな生活を得るために、利益機会としてのリスクをとってきた果実であるが、損失機会としてのリスクも生み出してきた。
- 高度技術に支えられた巨大技術システムを中心とした、社会インフラを支える重要システム群は、自動化の大幅な採用により、人間の役割を分散型の肉体労働から集約型の頭脳労働に変えるとともに、事故の特徴をも変えた。
- 技術のリスクはその使い方に依存するものであり、ITリスクについては予防管理への偏重から、事後対応の充実に重点が移りつつある。

ご清聴ありがとうございました

渡辺研司
watanabe.kenji@nitech.ac.jp