ユーティリティ制御システムのセキュリティへの対応

ICS Cybersecurity Incident Response and Troubleshooting Process

制御システムセキュリティカンファレンス2015,
JPCERT/CC, 2015/2/12

高野　正利
Masatoshi TAKANO
Toyota Motor Corporation, and
Technical Committee on Instrument and Control Networks,
Industrial Applications Division, SICE, Japan
masatoshi_takano　@　mail.toyota.co.jp

目次　Table of Contents

1. 本日の要旨

- 制御システムのトラブルシューティングにセキュリティのことも考える
  Improving ordinal troubleshooting with the awareness of cyber-related issues
  通常のトラブルシューティングとセキュリティハンドリングを
  分けて考えない
  Having a cybersecurity incident-handling installation, separate from the ordinal troubleshooting flow, makes the operations and troubleshooting capabilities more complex.
- 多層防御により，時間を稼ぐ
  Establishment of multilayered defense for buying time

2. ポイント　Priorities of ICS cybersecurity approaches

2.0　その機能は，本当に必要なのかを考える

- 本当に必要な機能なのか.
- その機能追加に伴うセキュリティリスクについても考える.

2.1　制御システムの情報セキュリティをユーザ視点で考える
Consideration of operator’s perspective

2.2　考慮すべき点
Consideration of today’s security defense of ICS

.1　脆弱性リスクの見積りは困難
Uncertainties of future risk estimation

.2　マネジメントシステムの視点
Management-system application to ICS cybersecurity

.3　制御システムセキュリティ対策の限界
ICS security limitations compared to IT system

2.1 ユーザ視点で考える

Consideration of operator's perspective

- 多くのオペレータはセキュリティ問題に遭遇していない

  Many plant-floor operators have few experience of the detection of possible cyber-incidents during ordinal troubleshooting.
  Most ICS troubleshooting is for non-cyber-related issues.

	Standalone controllers	Network based ICS	IT systems
System	Hard-wired relay, loop controllers, or PLCs without field networks	DCSs, PASs, SCADA, Industrial Ethernet/Field bus	Office system, Web, Internet, Intranet
Cyber incidents	Could not be found.	Recently, have reported.	Have many experiences.

2.1　ユーザ視点で考える（続き）

Consideration of operator’s perspective

- セキュリティ問題のアラームは上がらない可能性が高い
- オペレータはセキュリティ問題かどうかに気づけない場合が多い

→日々のプラント異常・故障への対応の中で，
セキュリティ問題を見分けられるかどうかが
大きな課題となる．

2.1　ユーザ視点で考える（続き）

Consideration of operator’s perspective

制御システムと情報システムのセキュリティ対応比較

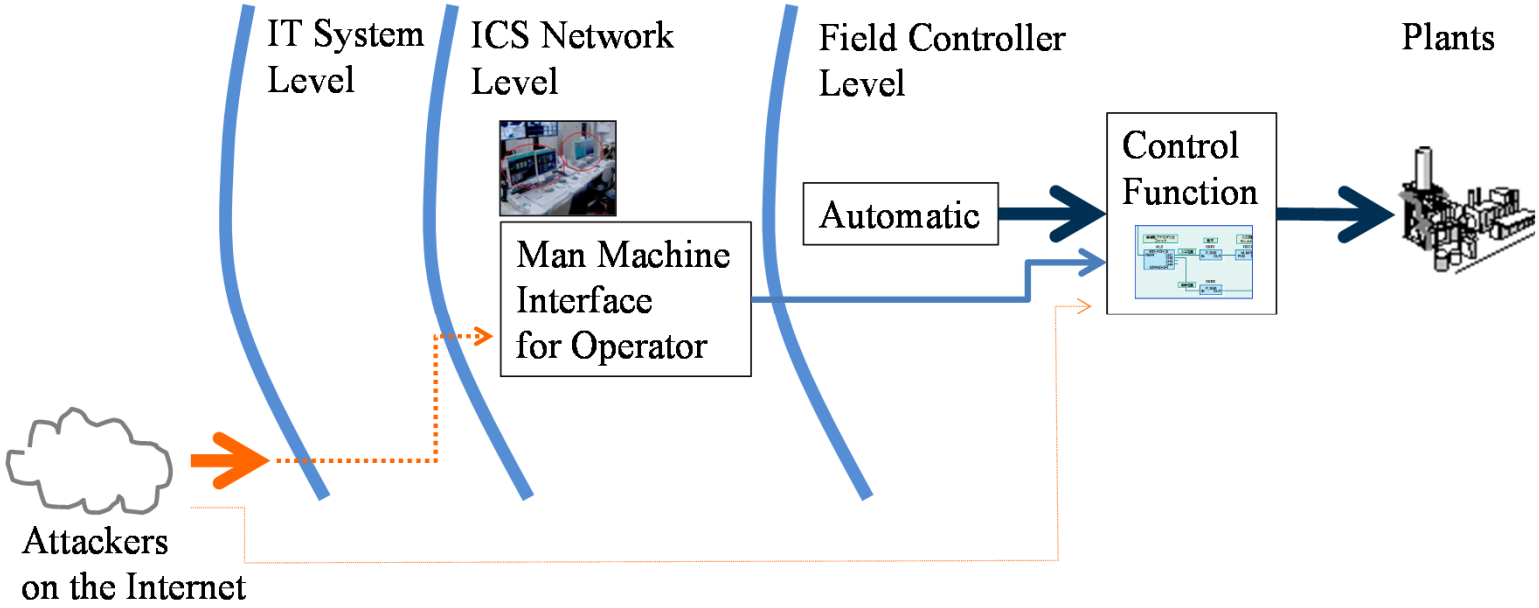
	IT システム	制御システム
サイバーセキュリティを認識できるか	多くのケースで念頭にある	通常故障などのトラブルシューティング過程で，ほぼ認識していない
脆弱情報への対応	アンチウィルスソフトウェア，パターンファイル等は通常，自動的にアップデート	・自社システムにその脆弱点があるかどうかの確認 →現状，これが困難 ・脆弱点があった場合に，今やるのか／次期改修時か／当面見合わせかの判断を実施したいが →現状，判断材料なし
脆弱性情報の扱い	ベンダーの製品から検索可能な情報	ユーザに認識できるように公開する必要あり（自社システム構成に使われているのか／いないのか）
サイバーセキュリティ脅威への対応	足し算（More with more） とにかくアップデート	引き算（More with less） 制御機能に絞ったシステム構成によるリスク低減

2.2 考慮すべき点
Consideration of today's ICS security defense

.1 脆弱性リスクの見積りは困難
Uncertainties of future risk estimation

.2 マネジメントシステムの視点
Management-system application to ICS cybersecurity

.3 制御システムセキュリティ対策の限界
ICS security limitations compared to IT system



2.2.1 脆弱性リスクの見積りは困難

Uncertainties of future risk estimation

情報系システムのセキュリティ対応

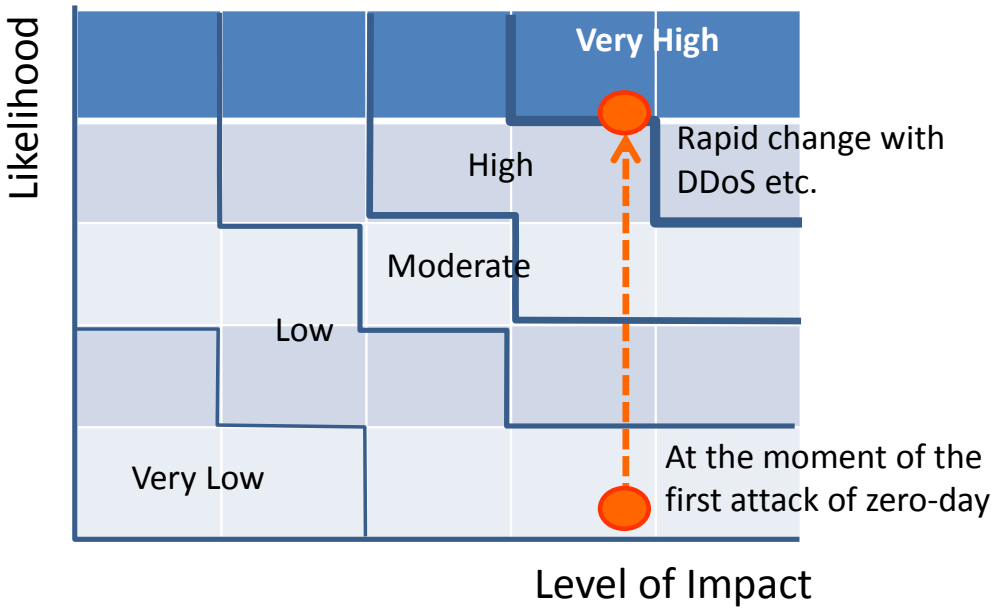
- 既知の脆弱性→アンチウィルスソフトなどにより検知し防御する仕組み
- 未知の脆弱性をついたもの（Zero-day-attack）→現時点で容易ではない.

Cyber security defense of ICS is unable to identify the risk of cyber-related incident exploitation, including new architecture of attacks, or is unable to predict the risk of what will be exploited next.

2.2.2 マネジメントシステムの視点

Management-system application to ICS

・Zero-day attackは当然のことながら予測が出来ず，
頻度の大小に関わらず影響度が高いものは，
リスク低減が必要になると考えたほうが良い．



- Organization cannot identify and recognize whether the rapid transition of the risk level would have occurred.
- Thus, ordinal risk assessment could not be applicable to cybersecurity risk assessment for the management system.

2.2.3　制御システムセキュリティ対策の限界

ICS security limitations compared to IT system

・制御システムは，リアルタイム性の確保や，運用期間が長いことによるプアな（5～10年単位で見れば）コンピュータ資源などの制約がある.

・リアルタイムでのアンチウィルスソフト等の更新は難しいため，必要な制御機能を絞り込み，ソフトウェアの最少化が重要.

- IT system employs online, real time update mechanisms of security software such as security patches or virus pattern files.
- In contrast to the IT security, an ICS platform may not run the cyber security software, or may require processes to discover whether new versions of antivirus software or pattern files work correctly. It is difficult to implement the security software into ICS.

2.2.3+ 制御システムセキュリティ対策

Different views of ICS security considerations

・機密性
  ・ アクセス制御（識別と認証），暗号化
・正確性
  ・ **TCP**によるバーチャルサーキット（例えば）
・可用性
  ・ 安定稼動 → システム資源・動作の保証
  ・ 障害対応
  ・ 応答性
  （リアルタイム性）
  ・ ウィルス対応他

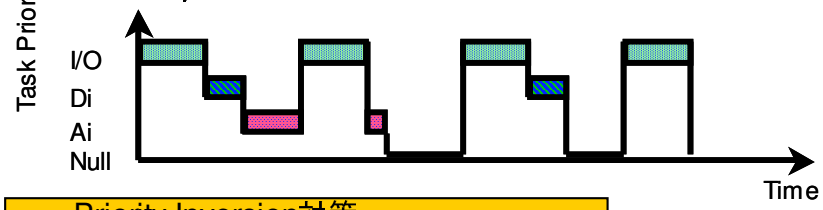
The definition of "realtime" by IEEE-POSIX is to provide a required level of service in a bounded response time.

・周期タスクのデッドラインの保証
・非周期タスクの要求時間内での応答

Schedulability
Rate Monotonic Theory

$$\sum_{i=1}^{n} \frac{C_i}{T_i} \leq n\left(2^{\frac{1}{n}} - 1\right)$$

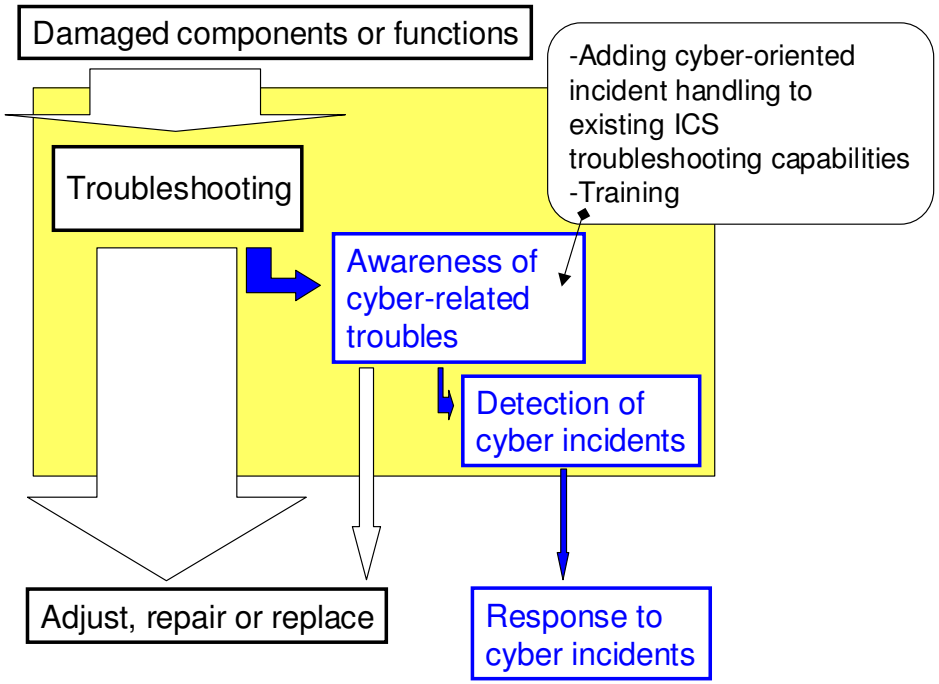
Ci＝独立した周期タスクの最悪実行時間
Ti＝周期
n＝タスク数



・Priority Inversion対策
・Dead Lock対策

3. 制御システムのトラブルシューティングにセキュリティ問題への少しの意識

ICS troubleshooting with awareness of cybersecurity



- An acute awareness of the potential for cyber-related, together with the main stream of the troubleshooting, supports the response to cyber-incidents.
- Maintenance organizations should add cyber-oriented incident handling to existing ICS troubleshooting trees.

可能性の高いものからトラブルシューティングし，並行してセキュリティ問題の可能性を確認

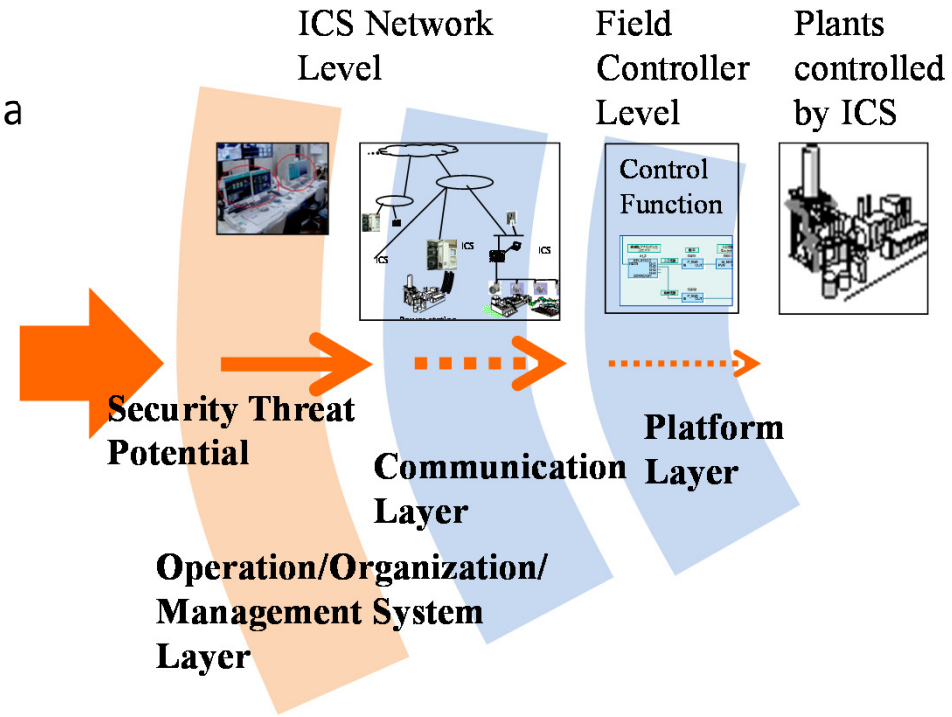
・制御システムのトラブルシューティングにおいては，
セキュリティ起因であっても，通常の設備故障であっても，
トラブルとなっている機器や制御機能のトラブルシューティングから入るべきである．

・既存のトラブルシューティングマニュアルなどに追記して，セキュリティ問題へ少し意識を持てるようにすることが，とりこぼしなくトラブルに対応できる方法と考える．

4. ガイドライン Practical guideline

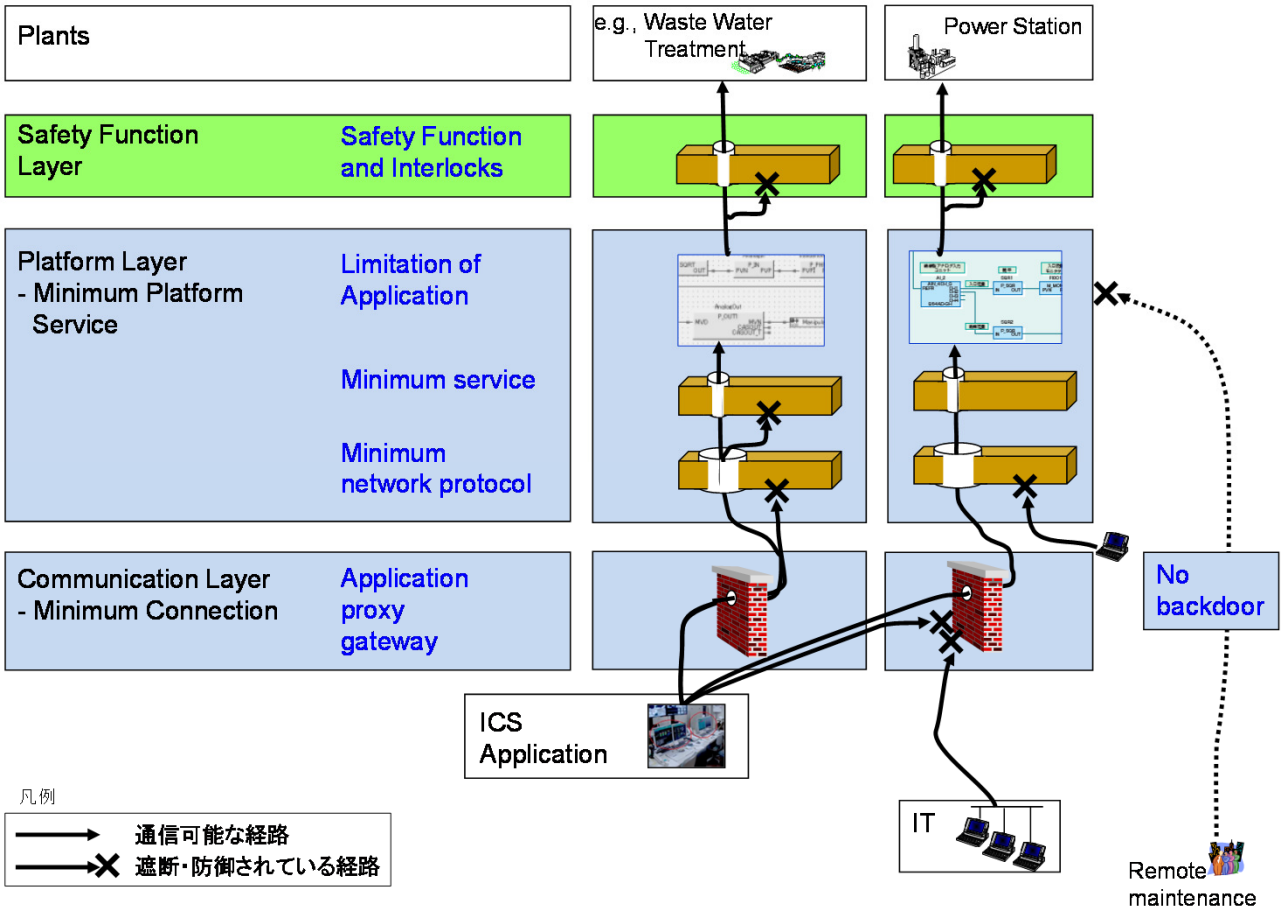
一般的な多層防御の制御システム例

- We describe a practical guideline to retard zero-day exploitation.
- Figure shows one of general defense-in-depth strategies including a platform layer and a communication layer.



4. ガイドライン（続き） Practical guideline

プラットフォームレイヤ： OSや通信プロトコルなどソフトウェアの必要最少化
コミュニケーションレイヤ： 必要な通信に制限するアプリケーションプロキシゲートウェイ等
→必要な制御機能以外の通信経路の遮断・防御を，
プラットフォームレイヤとコミュニケーションレイヤで直列に多層化することにより，
ひとつの脆弱性だけでセキュリティトラブルとなるリスクを低減する．



5. まとめ　Conclusions and discussion

プラントシステムのトラブルシューティングの中で,

セキュリティ問題をバランスしてとらえることの重要性

・プラントトラブルシューティング手順に

　セキュリティ問題をチェックできる枝葉を追加しておく

・制御システム独自の制約やITと共通する不確実性への対応として,

　より詳細なシリーズでの多層防御が有効な可能性がある.

This study considered ICS cyber-incident response and its protection from the viewpoint of operators' circumstances and limitations of today's security defense.

- Improving ordinal troubleshooting with the awareness of cyber is responsive to indefinite responses to trouble;
- Improving layered defense with a safety function is responsive to unpredictable attack and to unexpected changes of risk

本資料で使用している図表及び一部本文は，
下記参考文献からの引用です．

参考文献

1. 高野正利，ユーティリティ監視制御システムの情報技術と情報セキュリティ，計測と制御，第53巻第10号，2014/10.
2. Masatoshi Takano, “ICS Cybersecurity Incident Response and the Troubleshooting Process”, SICE Annual Conference 2014.
3. 高野正利，ユーティリティ制御システムのセキュリティ，情報セキュリティEXPO専門セミナー2010, 2010/5/12.
4. Masatoshi Takano, “Sustainable Cyber Security for Utility Facilities Control System based on Defense-in-Depth Concept”, SICE Annual Conference 2007.