制御システムセキュリティに求められる人材
Human resources
for cyber security of Industrial control system

アズビル株式会社　環境・標準化推進部標準化推進グループ
岡本　秀樹
制御システムセキュリティセンター　評価認証・標準化委員会委員
h.okamoto.fi@azbil.com

2012-08-30
画像電子学会　第10回国際標準化教育研究会

Contents

1. 急浮上した制御システムセキュリティ

- 制御システムはどこで使われているのか
- STUXNETの出現
- 神話の崩壊
- 我々も例外ではない。誰が守ってくれるのか
- そしてCSSCが設立！

1. 急浮上した制御システムセキュリティ

- 制御システムはどこで使われているのか

結構重要な施設で使われている

- 原子力発電所の冷却制御
- LNGのパイプライン監視
- 石油コンビナートの運転制御
- 鉄鋼炉の燃焼制御
- 半導体工場のクリーンルームの空調
- ビルの空調制御
- 微生物実験施設の空調

1. 急浮上した制御システムセキュリティ

- 制御システムはどこで使われているのか

これら施設で事故が起きると・・・

- 原子力発電所の冷却制御　⇒　放射能汚染
- LNGのパイプライン監視　⇒　爆発，火災
- 石油コンビナートの運転制御　⇒　火災，爆発
- 鉄鋼炉の燃焼制御　⇒　火災
- 半導体工場のクリーンルームの空調　⇒　有毒ガス漏洩
- ビルの空調制御　⇒　ボイラーの爆発，施設の稼働停止
- 微生物実験施設の空調　⇒　病原菌の拡散

1. 急浮上した制御システムセキュリティ

- STUXNET（スタックスネット）の出現

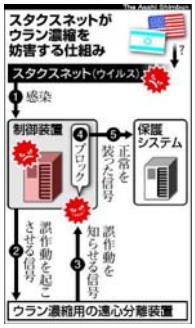
2010年秋：イラン原子力施設へのサイバー攻撃

STUXNETというマルウエアにより，ウラン濃縮用遠心分離機が稼働できなくなったとされる

出所：http://www.familysecuritymatters.org

1. 急浮上した制御システムセキュリティ

●STUXNETの出現



- USBが接続されたPCから感染し、ネットワーク内に侵入。
- 行動範囲を広げながら、PLCを制御するコンピュータに感染。
- PLCのプログラムを書換え，遠心分離機のモーターを異常高速回転。
- 遠心分離機を故障させた。

PLC
Programmable Logic Controller
工場などの自動機械の制御に使われていたリレー回路の代替装置として開発された制御装置

http://www.asahi.com/international/update/0116/TKY201101160282.html

1. 急浮上した制御システムセキュリティ

●制御システムのセキュリティへの警鐘

制御システムはサイバー攻撃を受けない（はず，だろう）根拠

- 専用プログラム言語やOSを使っており一般に知られていない
- 専用の通信プロトコルが使われており，多種にわたる
- OA系情報システムやインターネットと分離されているから感染しない
- 内部の者から攻撃されることはない

実際に攻撃され，これらの根拠は気休めでしかないことが分かった。
制御システム専門家にも，そして，サイバー攻撃者にも。

1. 急浮上した制御システムセキュリティ

●我々も例外ではない。誰が守ってくれるのか

世界各地でサイバー攻撃が増えつつある。

米国では、原子力発電所から化学工場、水道施設がサイバー攻撃されている。

日本においても被害が発生している。

- 石油プラントの生産情報管理系サーバーがマルウェアに汚染され、10日間ほど生産停止。
- 半導体工場で生産監視制御系ネットワークのPCがマルウェアに汚染され、復旧作業に1ヶ月間ほど要した。
- 企業の生産機密情報が海外のサイトに出ていた。

1. 急浮上した制御システムセキュリティ

●我々も例外ではない。誰が守ってくれるのか

アズビル株式会社


ビルディング
オートメーション事業
ビルの空調制御


アドバンスト
オートメーション事業
プラントの制御・監視


ライフ
オートメーション事業
高齢者の見守りシステム

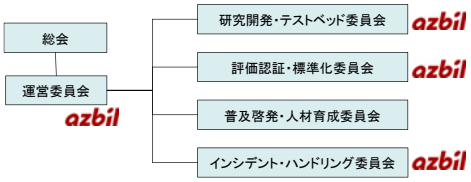
どうサイバー攻撃から守ってくれるのか
どうサイバー攻撃を防げばいいのか
お客様

1. 急浮上した制御システムセキュリティ

●そしてCSSCが設立！

重要インフラへのサーバー攻撃の被害は自然災害に匹敵する。
制御システムをサイバー攻撃からきちんと守れるようにしよう！

経済産業省が技術研究組合制度を利用して
制御システムセキュリティセンター設立　2012-03-06
（CSSC：Control System Security Center）



1. 急浮上した制御システムセキュリティ

●そしてCSSCが設立！

研究開発・テストベッド委員会
- 制御システムの要件を満足するセキュアな構成・技術の開発
- 最新セキュリティ検証ツールの開発／提供

評価認証・標準化委員会
- 国際標準への積極的な提案と利用ガイドラインの作成
- 国内における国際認証体制の確立

インシデント・ハンドリング委員会
- インシデント対応マニュアルの提供，対策のサポート

普及啓発・人材育成委員会
- セキュリティ教育のカリキュラム作成・実施
- セキュリティ対策効果の体験

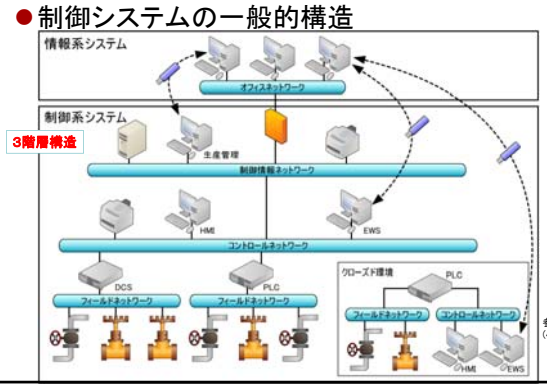
2. 制御システムの構造と脆弱性

- 制御システムの一般的構造
- 一般の情報システムとの違い
- 脆弱性：どこが弱いのか

 13

2. 制御システムの構造と脆弱性

- 制御システムの一般的構造



参考文献 (4)

14

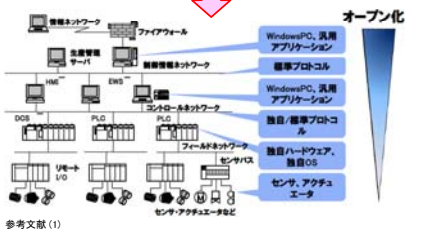
2. 制御システムの構造と脆弱性

- 制御システムの一般的構造

プラント設備（生産ライン制御等）におけるオープン化の割合

- **外部ネットワークとの接続　36.8%**
- **設備内のOSの利用状況　Windows：88.9%　UNIX系：13.7%**

実は意外とオープン化が進行



参考文献 (1)

「Windows」は、米国 Microsoft Corporation の米国およびその他の国における登録商標です

 15

2. 制御システムの構造と脆弱性

- 一般の情報システムとの違い

制御システムの特徴

- 可用性が最重要
- 長期運用が前提
- リアルタイム制御
- 現場の技術部門が管理

 16

2. 制御システムの構造と脆弱性

- 一般の情報システムとの違い

セキュリティ情報	情報システム	制御システム
ウイルス対策／モバイルコード	一般的，広く使用	効果的な配備は一般的でない／不可能
サポート技術の寿命	2～3年，多様なベンダ	最大20年，単一ベンダ
外部委託	一般的，広く利用	運用は外部委託されることもあるが，サービス提供者は多くない
パッチの適用	定期的，計画的	まれ，非計画的，ベンダ固有
変更管理	定期的，計画的	厳格に管理され複雑
時間に厳しい処理	一般に遅延を許容	遅延は許されない
可用性	一般に遅延を許容	24時間365日（連続稼働）
セキュリティ意識	民間部門でも公共部門でも中程度／情報システム部門	物理的セキュリティ以外は貧弱／現場の技術部門
セキュリティテスト／監査	優れたセキュリティプログラムに含まれる	停電に備えたテストを時折実施
物理セキュリティ	安全（サーバ室など）	遠隔／無人，安全

 17

2. 制御システムの構造と脆弱性

- 脆弱性：どこが弱いのか

攻撃目的：装置や設備の破壊、悪品質製品生産や生産の暴走、装置ベンダの信頼失墜等　攻撃ターゲット⇒

参考文献 (1)

「Ethernet」は、富士ゼロックス株式会社の商標です。

 18

2. 制御システムの構造と脆弱性

azbil

● 脆弱性：どこが弱いのか

攻撃されたときの現象

① 知らないうちに製造製品の機密情報が外部のWebに公開される。
② 生産情報が書き換えられる
　・生産数量，品質レシピ，品質検査基準値
③ 制御システムを操作
　・制御システムが暴走，停止
　・制御施設が破壊される爆発火災
④ リフレッシュ作業でのリスク
　・危険な作業を伴う
　・その間，生産操業ができない

参考文献 (2)

2. 制御システムの構造と脆弱性

azbil

● 脆弱性：どこが弱いのか

たとえばスマートメータ

- 電気メーターをデジタル化
- 検針作業を効率化
- 電力消費量をグラフ化
- 供給計画の効率化
- 遠隔で操作

＜脆弱性＞
- 暗号化されていない通信
- 認証のないデータアクセス
- 電力消費量分析によるプライバシー問題
- 何秒ごとにデータを送るか
- メーターの数値を書き換える
- 耐タンパー性
- ICMPのハンドリング

参考文献 (3)

3. 標準化の動き

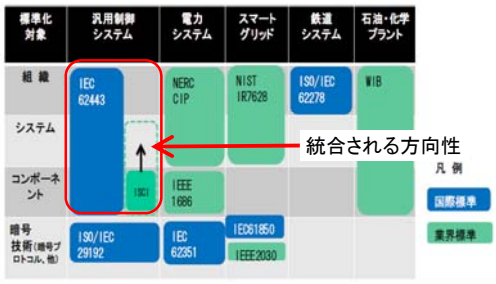
azbil

- 欧米の動き
- 国際標準の概観
- IEC62443シリーズ
- 認証
- CSSCの動き

3. 標準化の動き

azbil

● 国際標準の概観　汎用分野の標準化が進んでいる



参考文献 (5)

3. 標準化の動き

azbil

● 欧米の動き

・ガイド・ツール
セキュリティ基準の策定、推奨プラクティス集の公開、自己評価ツールの配布を実施
・評価・検証
テストベッドの開設によるセキュリティ検証を実施
データベース
制御システムのインシデント情報のデータベース構築・公開を開始
・認証
民間主導によるセキュリティ監査・認証サービスが行われており、ISA ISCIによる標準化が進展中
・普及
制御システムセキュリティ強化に向けた認識向上や関係者間の信頼関係構築により施策の普及を促進させるための、情報共有コミュニティを設置し運用

3. 標準化の動き

azbil

● IEC62443シリーズ　発行されているものは3本だけ

IEC62443-1-x
概要，コンセプト，用語

IEC62443-2-x
管理，運用プロセス

IEC62443-3-x
技術，システム

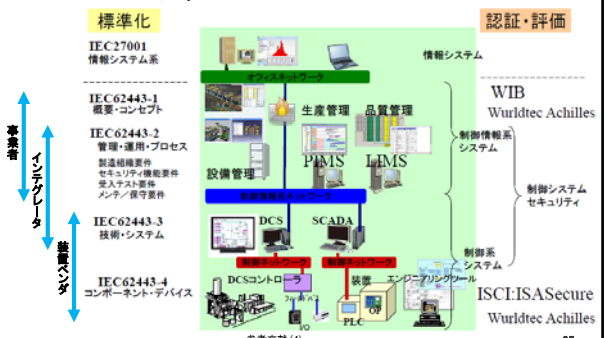
IEC62443-4-x
コンポーネント，デバイス

参考文献 (4)

3. 標準化の動き

azbil

●IEC62443シリーズ　標準と認証

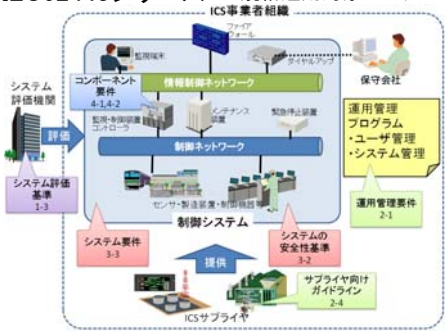


参考文献 (4)

3. 標準化の動き

azbil

●IEC62443シリーズ　規格適用対象のマッピング



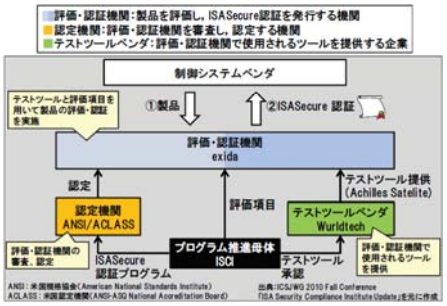
参考文献 (1)

3. 標準化の動き

azbil

●認証　今はまだ機器に対する認証しかない

通信レベル，セキュリティ機能，ソフト開発プロセスの3つの側面で評価



参考文献 (5)

3. 標準化の動き

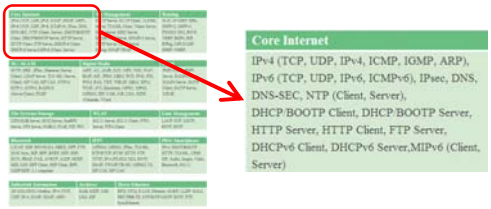
azbil

●認証

テストの一部　通信レベルの評価

例：テストツール（Codenomicon）が対象とするプロトコル

制御システムの中で利用される通信プロトコルは、極めて種類が多い



http://www.toyo.co.jp/it/codenomicon/cod_seihin3.html

3. 標準化の動き

azbil

●CSSCの動き

研究開発の成果を踏まえ，審議中の規格に対して積極的な提案を行っていく

参考文献 (4)

4. セキュリティの特質と対応

azbil

- ●サイバー攻撃の事件簿
- ●サイバーセキュリティの特質
- ●運用に求められる対応
- ●プロトコルに求められる対応
- ●機器に求められる対応

4. セキュリティの特質と対応

azbil

● サイバー攻撃の事件簿

参考文献 (4)

4. セキュリティの特質と対応

azbil

● サイバーセキュリティの特質

たとえば次のような特質

- 攻撃者の目的はさまざまであり対応もさまざま
- 日々攻撃手法が進化する
- 制御システムの防御は最適化しきれない
- 故障や異常をサーバー攻撃の影響と判断しきれない

4. セキュリティの特質と対応

azbil

● サイバーセキュリティの特質

攻撃者の目的はさまざまであり対応もさまざま

動機

うらみ，いやがらせ
力の誇示，いたずら
脅迫
利益目的（株価操作など）

攻撃目的

企業秘密（製造方法，レシピ，生産情報など）の奪取
システム障害による業務妨害
有害物質の排出，爆発・火災など社会的損害の発生

4. セキュリティの特質と対応

azbil

● サイバーセキュリティの特質

日々攻撃手法が進化する

Stuxnet 2009, 2010 ⇒ Duqu 2011 ⇒ Flame 2012.5 ⇒ Gauss 2012.6 ⇒ H?

THEY WILL NOT WAIT !

制御システムの防御は最適化しきれない

古いシステムがあり更新が困難（古すぎてパッチがあてられない）
新しい機器と古い機器が混在（セキュリティレベルが異なる）
不用意なシステム変更（潜在的な“穴”が出現）

4. セキュリティの特質と対応

azbil

● サイバーセキュリティの特質

故障や異常をサーバー攻撃の影響と判断しきれない

下記からサイバー攻撃だと“すぐに”判別することができる？

– 制御動作が時々遅くなる。
– 通信エラーが出るようになった。
– 制御データが抜けている。
– 制御動作変化しているべき制御データが変化していない。
– 制御信号が突然変化する。（突変現象）
– 壊れるはずの無い部分が壊れている。おかしなストレスがかかったと思われる。
– 制御機器のメンテナンスチェックが終了しない。
– 閉まっていなければならない操作端が開いている。また、その逆。
– 再起動してしばらくは正常動作していたが、また、同じ異常になった。
– ソフトウェア更新をしたら、異常になった。
– USBで作業をしたら、異常が出るようになった。
– 外部サポートを受けた後に、異常が出るようになった。
– 制御異常現象は出ていないがインシデント発生

参考文献 (2)

4. セキュリティの特質と対応

azbil

● 制御システムの特質

制御システムは，生産状況に合わせて改変される。
ウイルスなども日々新たなものが作られている。

⇒ ライフサイクルを通してセキュアな状態を維持する必要がある

参考文献 (5)

4. セキュリティの特質と対応

azbil

● 運用に求められる対応

◆セキュリテイ認識を持った対応能力
SSATで評価し改善

◆現場防衛力アップにつながるもの

現場の実践的防衛力アップツール：
必要な取組みがまとめられたもの
それを身につけさせてくれる
内容を理解したかどうか確認できる

SSAT（管理認識評価）
- 事業リスクの理解
- 継続した管理
- 防御体制の質
- マルウェア対策認識
- 内部からの脅威認識
- セキュリティ管理レベル
- バックアップと回復のシナリオ
- 物理的セキュリティ管理
- 対応能力の確立
- サードパーティ・リスク管理
- 調達

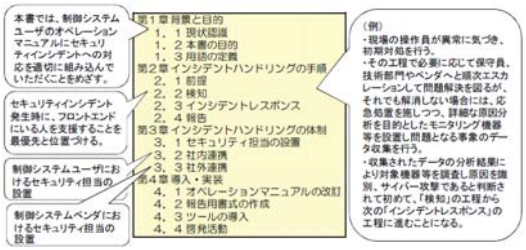
参考文献（2）

4. セキュリティの特質と対応

azbil

● 運用に求められる対応

現場の実践的防衛力アップにつながるツールの例：
インシデントハンドリングの対処手順ガイドライン



参考文献（5）

4. セキュリティの特質と対応

azbil

● 計装エンジニアに求められる対応

制御システムエンジニアリングの実践的防衛力アップにつながる技術を身につけること

- 現場の制御システムの実践的防衛力アップ
- 健全なエンジニアリング環境の確保⇒整備⇒管理
- 実践的インシデント対応技術とその対応作業のための制御システム設計手法

制御システムを評価し，制御システムを改善していく

4. セキュリティの特質と対応

azbil

● 機器ベンダに求められる対応

◆サイバー攻撃に対処できる制御製品開発

- クリーンな制御製品開発環境の整備
- サイバー攻撃を想定した品質検査
- 高度セキュア化技術の制御製品応用

◆インシデント対応の情報公開対応

セキュリティ対応を強化した制御製品を開発するとともに，Sierやユーザへの取り扱いガイドラインを出して，正しい製品管理を公表していく。

5. 求められる人材とその育成

azbil

● 求められる人材

● 育成の継続的課題

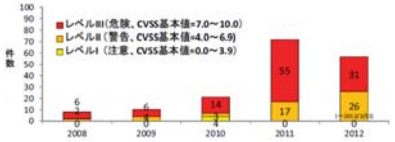


図 2-6. 産業用制御システムに関するソフトウェアの脆弱性件数と深刻度割合の年別推移
（出典）脆弱性対策情報データベース JVN iPedia®の登録状況
［2012 年第 1 四半期（1 月～3 月）］

参考文献（5）

5. 求められる人材とその育成

azbil

● 求められる人材

制御システムセキュリティの現場で必要となる人材

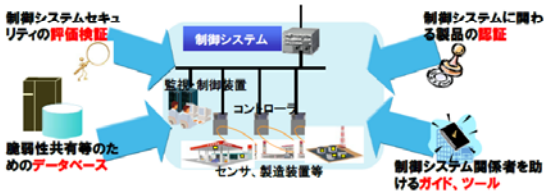
- ユーザ企業の現場
  ⇒ 一定の能力を持ったセキュリティアセッサ
- 制御製品やシステムの認証
  ⇒ ニュートラルな立場の査察官，監査官
- インシデントサポート ⇒ プロフェッショナルエンジニア
  対象となる制御製品をテストするプロ
  業種別の現場を熟知した企業サポートのプロ
- セキュリティリスク管理の認識度向上を展開できる人

5. 求められる人材とその育成

azbil

● 求められる人材

制御システムセキュリティは，大きく分けて次の4つのポイントで行うことが必要であり，これらを標準化する人材が求められる。



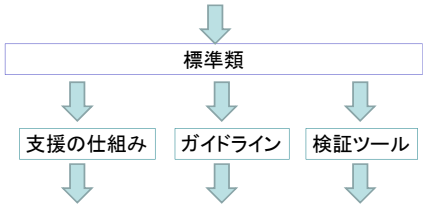
参考文献（1）

5. 求められる人材とその育成

azbil

● 求められる人材

制御システムセキュリティの現場で必要な標準を供給する人材



制御システムセキュリティの現場で必要となる人材

5. 求められる人材とその育成

azbil

● 育成の継続的課題

他の標準化分野に比べて流動性が高く，変化も速い

- 現場関係者の継続的教育
  個々のセキュリティ意識やビジネスインパクトの認識は一様ではない。
- 現場システムの改変
  設備の改変改・造や機器の入れ替えがある。ベンダーの追加・変更もある。
- サイバー攻撃者の進化
  いくらセキュリティ技術が進んでも，それを破る技術が開発される。
- マルウエアの蔓延
  管理された制御システムの外側には新旧のマルウエアが入り乱れて存在する。

5. 求められる人材とその育成

azbil

● 育成の継続的課題

サイバー環境が変動する中，現場で発生したインシデントやその対策情報を収集・把握して，標準化する者にフィードバックすることは，なかなか大変である。

現場作業者の継続的教育
現場システムの改変
サイバー攻撃者の進化
マルウエアの蔓延

現場と標準化エキスパートとの距離を縮め，コミュニケーションを良くしていく仕組みの構築が，継続的対応が求められる制御システムセキュリティにとって，重要な課題である。

5. 求められる人材とその育成

azbil

● さいごに

制御システムセキュリティ対策は一種の医療

現場エキスパートは，医者として患者の面倒をみる。

患者が訴える不定愁訴に潜む重大原因の推定
病原の特定と処方および経過観察
新たに出現した病原菌に対する治療薬・治療方法の学習
日和見菌により発症しないよう患者の健康をチェック・管理

標準化エキスパートは，現場エキスパートや病院経営者のためのガイドライン作成，新薬／新治療法の認可や，感染情報の提供を行う厚生労働省やWHOのようなもの。

参考資料

azbil

(1)「制御システムセキュリティ 国際標準の現状と日本の取り組み」 小林 偉昭（IPA）
計測展2011 TOKYOテクニカルセミナー資料
(2)「制御ベンダ／装置ベンダ／Sierに求められるセキュリティ対策についての提言」 村上正志（VEC）
制御システムセキュリティカンファレンス 2012資料
(3)「制御システムセキュリティの現実」 福森大喜（サイバーディフェンス研究所）
制御システムセキュリティカンファレンス 2012資料
(4)「制御システムの今あるセキュリティ脅威と対策について」小林 偉昭（IPA）
IPAグローバルシンポジウム2012資料
(5)「制御システムセキュリティ検討タスクフォース報告書 中間取りまとめ」 経済産業省（2012-06）

