2013 年 10 月 18 日

独立行政法人情報処理推進機構（IPA）

制御システムのセキュリティインシデントから学ぶ

本概要は、欧州ネット・情報セキュリティ機関（ENISA：European Network Information Security Agency）が発行する、“Can we learn from SCADA security incidents?”の概訳となります。

内容の詳細につきましては、原文をご参照ください。

URL：

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

制御システムの汎用化が進むにつれて、制御システムのセキュリティに対する懸念が指摘されている。近年の制御システムのセキュリティインシデントを鑑みても、制御インフラのガバナンス、とりわけ組織として、深刻なインシデントに適切に対処し、分析を行った上で、その経験から学ぶことが重要となる。

欧州連合（EU）では、重要インフラシステムおよびネットワークのセキュリティ向上のためのサイバーセキュリティ戦略を掲げている。このホワイトペーパーはその一環として、重要インフラ事業者が制御システムのインシデントの事後分析を実施・活用する環境を整備するにあたっての考慮事項を纏めたものである。

インシデントの事後分析

事後分析はデジタルフォレンジックの第一歩ではあるが、両者を混同するべきではない。デジタルフォレンジックは警察などの当局を交え、裁判で認められる裁判証拠を収集することを目的とするが、事後分析は、情報として「何が狙われたのか」「攻撃の意図」「攻撃に使われた（システム・組織の）脆弱性」「盗まれた情報の追跡調査による犯人（像）」の特定を目的とする。

インシデントの事後分析の主な意図は、必要な情報を収集し、何が起こったのかインシデントの詳細を綿密に把握すること、また、その結果学んだことを、レジリエンスの高いシステムにするための改善に生かすことである。

制御システムはその多様性他の特性から、単一的な方法では情報の収集や対応が困難なことも多い。以降に、制御システムのインシデントレスポンスおよび事後分析にあたっての考慮点として、体制と役割割分担、収集情報、および課題と推奨策を示す。

体制と役割分担

調査を含むインシデントレスポンスの流れは、「1．インシデント検知」「2．対応開始」「3．データ収集」「4．復旧作業／データ分析」「対応終了／報告」の 5 段階となる。

制御システムの特有性から、対応チームには従来必要とされる要員の他、制御システム側の対応を取り纏める「制御システムインシデント統括者（CSIM）」、制御システムのセキュリティ専門家である「制御システムセキュリティスペシャリスト（CSSS）」、制御システムの構築・運用等の専門家である「制御システムエンジニア（CSES）」を有するべきである。

以下に、制御システムインシデントへの対応および事後分析における、従来要員・制御システム要員の役割分担を示す。

表 1. 制御システムのインシデントレスポンスおよび事後分析における役割分担

レスポンス活動	ハンドリングチーム	制御側とのレスポンスコーディネータ	インシデント連絡窓口（POC）	全体レスポンス統括者	制御側レスポンス統括者	制御セキュリティ専門家	制御構築・運用専門家	制御機器ベンダコーディネータ
インシデント検知								
検知	主	副	主					
報告・記録	主	主	主					
レスポンス開始								
分類	主		主	副	主			
エスカレーション			主	主	主	副		
緊急対策	主		主	主		副	副	主
データ収集								
出動	副	主	副	主	主	副	副	副
調査	副	主	主	副	主	主	副	副
隔離・抑制	主	主	副	副	主	主	主	副
復旧作業／データ分析								
復旧方法検討		副	副	副	主	主	主	主／副
復旧		副	副	副	主	主	主	副
システムアップグレード		副	副	副	主	主	主	副
レスポンス終了／報告								
インシデント概要報告		主	副	副	副	主	副	
軽減対策			主	主	主	主	副	副
システムアップグレード	主		主	主	主	主	副	

【凡例】 主： 主担当　　副： 副担当

収集情報

制御システムは、その性質上、1000 分の 1 秒レベルでの処理が要求されることや、データの変動が激しいことから、事後分析に必要なデータの収集にあたっては、時計の正確性が非常に重要となる。調査中のタイムスタンプや記録の実施にあたっては、この点に十分気をつけねばならない。

制御システムでは、様々な機器から様々な情報を収集することが可能である。以下に、制御システムの構成機器から収集可能なデータの種類、および留意事項を示す。

表 2. SCADA/ICS システムの構成機器から収集可能なデータの種類

	コントロールセンタ	フィールド機器
近代的／汎用 制御システム技術	・ネットワークトラフィックのキャプチャ ・OSやHMIが改変されている場合は、システム管理者に要相談	・ネットワークログ ・コントロールセンタで確認できるフィールド機器に関するログ - 機器の電源がオフ: 何か証拠が残ってないか、機器を検証 - 機器の電源オン: 日付、時間、現状上がっているプロセス、および 動いているプロセスを確認
近代的／独自 制御システム技術	・事後分析ツールが使用できる可能性あり ・ネットワークトラフィックのキャプチャ ・ベンダとのコミュニケーション必須	・ネットワークログ ・コントロールセンタで確認できるフィールド機器に関するログ ・ベンダの間でのコミュニケーション必須 ・組み込みのベンダ固有のセキュリティ機能に関係る可能性あり
レガシー／独自 制御システム技術	・事後分析ツールの使用は不可 ・ロギング機能なし ・ベンダのサポートなし（サポート切れ） ・機器の所有者が、何かしら情報を持っている可能性あり ・シリアルベースの通信、ネットワークトラフィックのキャプチャ不可	・シリアルベースの通信、ネットワークトラフィックのキャプチャ不可 ・サンプリングおよびデータ上書きの速度が速い ・ベンダとのコミュニケーション必須 ・経験豊かな制御システムエンジニアの支援が必須

課題と推奨策

データの変動性の高さ、非常に限られたロギング機能など、制御システムの特徴が、技術的観点・運用的観点の双方から、データの収集および分析を困難にする可能性もある。

以下に、制御システムの事後分析において直面しうる課題と推奨策を示す。

- データ収集における課題
  - 不十分なログ機能（元々セキュリティでなくプロセス監視目的のため）による、収集可能なデータの制限
  - 高いデータの変動性による、収集可能なデータの制限
  - カスタム仕様のカーネルの使用による、収集ツール等との互換性喪失
  - 低い処理能力のため、機能の追加・改善不可

- データ分析における課題
  - 扱うデータやプロトコルが異なることによる、事後分析ツールの流用不可（改善が必要）
  - データに意味を見出すための相関分析の手間

- 運用における課題
  - 情報システムの運用（機密性・完全性・可用性重視）と制御システムの運用（可用性・信頼性・安全性重視）の間の文化の壁
  - セキュリティアーキテクチャに対する低い受容性（保守的姿勢）
  - 従来の制御システム（レガシーシステム）を保守できる人員・スキルの不足
  - 情報システムと比べて長いライフサイクル（数年 vs 数十年）

- 推奨策
  - 既存の仕組みにおける、レポーティングおよび分析力の向上：有用なデータをどこで入手できる

か、許容可能なオーバーヘッド等を見極め、ロギング機能を強化する

- 最低限、システム共通のイベントに関するログの取得を実現：必要に応じて、ロギング機能をもつ適切なセキュリティ対策（ファイアウォールや侵入検知など）を導入する
- 人員の役割とスキルを見直し：事後分析に際し、自組織の運用員が保有するスキル（保有しないスキル）を明確にする
- 組織・国家間の情報共有促進：官民、組織間、国家間で経験や知見を共有し、生かす

以上