産業制御システムのネットワークログを対象としたインシデント分析手法の開発

石黒正揮*1　松本尭*1　松崎和賢*2　澤部直太*1　井上信吾*1　高橋茂*1　村瀬一郎*1

清水良昭*2　木内誠*3　平川博宣*3　久保智*4

*1 株式会社三菱総合研究所

100-8141 東京都千代田区永田町二丁目 10 番 3 号

*2 技術研究組合 制御システムセキュリティセンター 東京研究センター(TRC)

〒135-0064 東京都江東区青海 2-4-7

*3 アズビル株式会社

*4 富士電機株式会社

あらまし 電力プラント等の制御システムにおけるネットワークログを分析することにより、セキュリティ・インシデントの原因分析のための手法を示す。従来、制御システムにおいては、ネットワーク上の制御機器と Windows などの情報機器のイベントの関係を統合的に分析することが十分に分析することができなかった。Stuxnet 等の制御システムを対象としたインシデントの発生により、制御ネットワークにおいてもセキュリティ・イベントの分析に対する要求が高まっている。本研究では、制御機器と情報機器のイベントの相関を分析することにより、プロセスアラーム等の原因分析などを行うための手法および開発成果を示し、その特徴や課題についてまとめる。

キーワード インシデント分析、制御システム、イベント相関分析、異常検知、ウィルス、マルウェア

Development of An Incident Analysis Method for Network Logs of Industrial Control System

Masaki Ishiguro*1　Kazutaka Matsuzaki*2　Takashi Matsumoto*1　Murase Ichiro*1

Naota Sawabe*1　Shigeru Takahashi*1　Yoshiaki Shimizu　Makoto Kiuchi*3
Hironobu Hirakawa*3　Satoshi Kubo*4

*1Mitsubishi Research Institute, Inc. Information Technologies Research Dept.

10-3 Nagatacho 2-Chome, Chiyoda-ward, Tokyo 100-8141, Japan

*2Control System Security Center (CSSC), Tokyo Research Center (TRC)

2-4-7 Aomi, Koto-ku, Tokyo 135-0064, Japan

*3Fuji Electric　*4Azbil Corporation

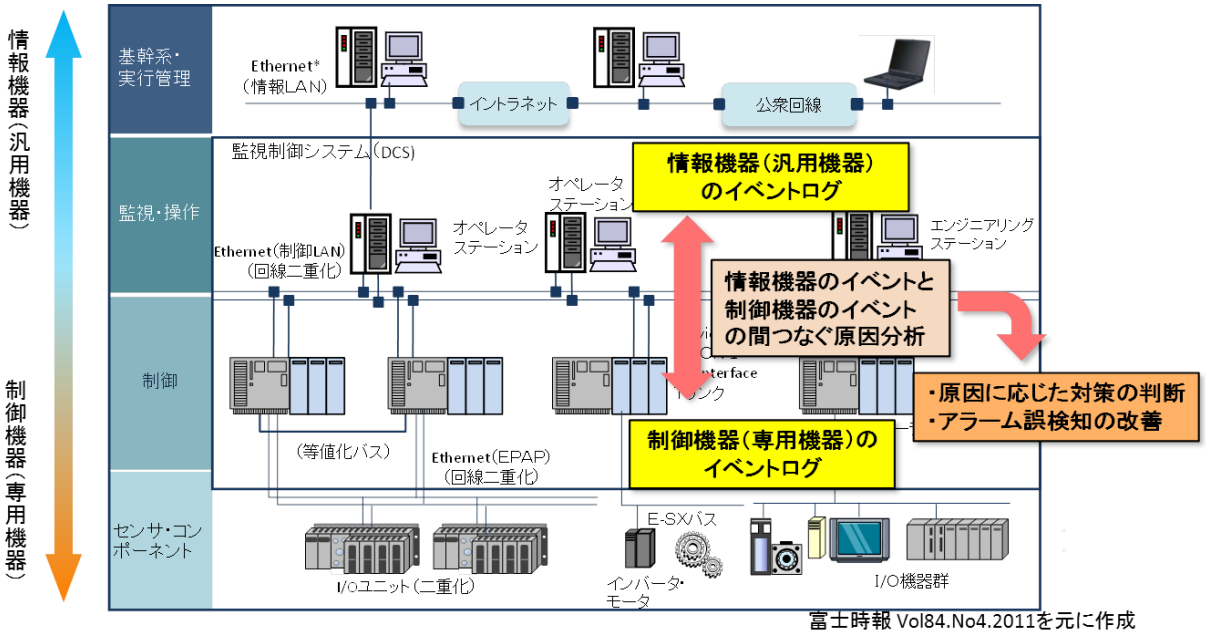
1　はじめに

制御システムはインターネットからは隔離された専用機器から構成されるシステムが中心であったため、ネットワーク攻撃などのセキュリティ脅威への対策はあまり考慮されていなかった。

近年、プラント制御、ビル・オートメーション等の産業制御システムにおいて Windows、UNIX 等の汎用製品やTCP/IP 通信プロトコルの導入、企業情報ネットワークとの接続が進み、それらの汎用システムにおいてみられる攻撃手法が、制御システムにおいても発生するリスクが高まっている。実際、Stuxnet 等のウィルスがイランの核施設における制御システムに感染し、制御システムの異常動作を引き起こすインシデントが発生したことにより、制御システムにおいてもセキュリティ上の脅威に対する認識が高まっている。本研究では、産業制御システムを標的としたウィルス等による攻撃に対して、制御システムネットワーク上の機器などのイベントログや通信ログを分析することにより、インシデントの原因分析等を行う手法について検討を行う。

2. 産業制御システムにおけるインシデント分析に関するニーズ

制御システムネットワークは、図 1に示すとおりSCADA や HMI など人の操作が介在する制御機器を中心に構成されるネットワークや、PLC や DCS など自動制御・リアルタイム制御を中心とするネットワークなどの複数のゾーンから構成される。前者は Windows 系/UNIX 系などの汎用機器の導入が進み、Stuxnet 等のウィルスによる攻撃対象となるリスクが高まっている。制御システム分野では、これまでは制御システムネットワーク上のイベントログから産業プロセスに関する異常状態を検知するプロセスアラームの分析および管理を目的としたシステムが利用されてきたが、セキュリティ・イベントについては焦点が当てられていなかった。近年、Windows 系の導入が進むにつれて、セキュリティ・インシデントに対する分析のニーズが高まっている



富士時報 Vol84.No4.2011を元に作成

図 1 制御ネットワークシステムの構成とインシデント分析の必要性

情報系ネットワークの分野では、IDS や異常検知システムなどのセキュリティ・イベントを対象とした一定レベルの検知技術は確立されているが、これらの技術を制御システムに適用する場合、セキュリティ・イベントと産業プロセスアラームを統合的に分析することが困難である[1,4,8]。

以上のような状況から、制御システム分野においては、セキュリティ・イベントやプロセスアラームに対してネットワークゾーン横断的に分析することにより、セキュリティ・イベントに起因するプロセスアラームの識別やプロセスアラームの原因を統合的に分析することで、対策の優先度が高いプロセスアラームの選別を行うことなどがニーズとして挙がっている。本研究では、このようなセキュリティ・イベントとプロセスアラームのイベント相関分析によりゾーン横断的なアラームの原因分析を行うための手法を提案し、その特徴

3. 関連研究

制御システムに対する IDS および攻撃検知技術については、ネットワーク侵入検知システム snort を用いた DigitalBond 社による攻撃検知ルールに基づく手法が挙げられる[5]。この手法では、SCADA、HMI、PLC 等で利用される制御システム専用プロトコルの DNP3 や Modbus 等に対応して攻撃の特徴を定義したルールに基づき、バッファオーバーフローやスキャンなどの攻撃を検知することができる。この手法では、特定の機器間の通信に対するトラフィックを分析対象としており、多数の機器が関わる一連のイベント系列全体を追跡することができない点が本研究とは異なる。

SRI の DATE プロジェクト[3]では、DigitalBond の攻撃検知ルールやベイズ推定をもとに検知したイベントに対する相関分析から攻撃検知を行う手法を提案しているが、相互に関連する一連のイベントから構成されるパス全体を分析していない点が本研究とは異なる。

このほか、イベント相関分析に基づくセキュリティ・インシデントの検知手法についてはいくつか報告されている[5]が、ネットワークゾーンを跨ぐ一連のイベントパス全体を対象に分析を行う手法は見られない。

一方、ネットワーク上のトラフィックに関する特徴量をもとにニューラルネットや統計的手法を適用し異常検知を行う手法はあるが、情報系または制御機器に関するイベントのいずれかを対象としたものであり、双方のイベント群を統合的に分析する手法は見られない[6,7]。

4. セキュリティ脅威

制御システムに対する攻撃は、イランの核施設で発生した Stuxnet ウィルスによるインシデントが代表的である。制御システムはゾーンに分割されたネットワークの多段構成をとるものが一般的になり、それらに対応して Stuxnet は、攻撃ステップの順を追ってネットワークの深層に侵入する。Stuxnet は、ステップごとに多数の攻撃手法を網羅的にパッケージ化し、攻撃対象の環境に応じてそれらの攻撃手法を選択的に適用する[2]。

以下に Stuxnet 等の攻撃手法をもとに、制御システムへの実際の攻撃要素をまとめる。

制御システムへの攻撃ステップと攻撃要素の実例

(1) Windows 系に感染
- Windows 系の脆弱性に対するゼロデイ攻撃(Windows Shell, 印刷スプーラ、Server NetPathCanonicalize サービス、Windows カーネルモードドライバ、タスクスケジューラ等の脆弱性等)
- USB デバイス接続による感染(autorun.inf. .LNK 脆弱性)。
- LoadLibrary コールなどを監視する IPS を迂回。
- 他のプロセスに DLL を inject して感染する。

(2) 痕跡隠蔽
- Rootkit インストール
- セキュリティ関連プロセスの不正停止(Mcshield.exe, avguard.exe 等の停止)

(3) 自己更新

- 外部 C&C サーバに接続(windowsupdate.com、msn.com 等の DNS 検索)
- 自身の更新のダウンロードと適用

(4) 標的に感染
- SIMATEC WinCC クライアントにデフォルトアカウント・パスワードでログイン
- WinCC サーバに感染(WinCC の SQL データベースのハードコードされた認証を利用し、データベースにコードを inject する。)
- WinCC の PLC の通信機能に隠蔽を施す。
- HMI に対する送信情報を改ざんし、自身を隠蔽する。
- 盗んだ鍵で作成された正当な証明書で署名をする。

(5) 本攻撃
- WinCC/PCS7(Siemens 製 DCS)配下の PLC に送られる STL 書換え(STL は、PLC のコードやデータを書き換える言語)
- PLC にラダーロジックを inject する。
- モーターの回転周波数を変更する。
- ターゲット装置のセンサーが出すアラームを停止して誤動作に気づかせない。

5. インシデント分析手法

5.1 分析アプローチ

制御システムネットワーク上の通信や機器のアラームなどのイベントログを対象にしたインシデント分析について示す。Stuxnet を代表とするウィルスは、痕跡隠蔽や潜伏化の技術を高めている。したがってこのような攻撃に対するインシデント分析を行うためには、膨大なイベントログの中で散発的に発生する限られた数のログから攻撃を検知することが求められる。また、4 章に示すような段階的に進展する攻撃に対して一連のイベント系列を追跡することがインシデント分析に有効である。そこで本研究では、制御システムへの攻撃全体を構成する個々の要素攻撃手法については、既存の IDS や、制御システム分野における産業プロセスアラーム管理システムをベースとし、機器間の通信イベントに基づき相互に関連する可能性のあるイベント系列を抽出することで、情報系のネットワークゾーンにおけるセキュリティアラートと物理系ネットワーク上の産業プロセスアラームのイベント相関分析を行うことに主眼を置く。これにより、ゾーン横断的なアラートの原因分析やセキュリティアラートに起因する産業プロセスアラームの識別など、優先度の高いアラームの選別を支援するシステムを実現する。

提案手法は、セキュリティアラート、プロセスアラームのみならず、ネットワークイベント、操作イベント・動作イベント等に拡張したイベント相関分析にも応用が可能である。

提案する手法における主な処理ステップは以下のようになる。

(1) イベント相関分析
- イベントパスの抽出
  通信関係をもとに関連する可能性のあるイベント系列をすべて抽出する。
- イベントパスの発生率評価
  イベントパスごとに発生率を推定する。

(2) 原因分析
- イベントパスの危険度評価
  危険パターンとの類似性からイベントパスの危険度を評価する。

以下の節では、各ステップの基本的な実現方式を示す。

5.2 イベント相関分析

本手法では、制御システムネットワーク上のイベントについて、機器間の通信に基づき、関連性を持つ可能性のあるイベント系列をすべて抽出し、抽出されたイベント系列の発生率を評価することにより、ゾーン横断的なイベント相関分析を行う。

具体的には、制御システムネットワークに接続される機器上のイベントログや機器間の通信ログに対して、機器間の通信を辿り時間軸上で、相互に関係を持ちうるイベント系列(イベントパスと呼ぶ)をすべて抽出する。

一方、一定時間の観測ウィンドウにおいて、同時に発生するイベント対（共起イベント）の発生率をすべてのイベントの対について計算し、上記で得られたイベントパス上の連続するイベント対の発生率の積を求めることで、イベントパス全体の尤度（発生する可能性の高さ）を求める。以上によりゾーン横断的なイベント相関を求める。

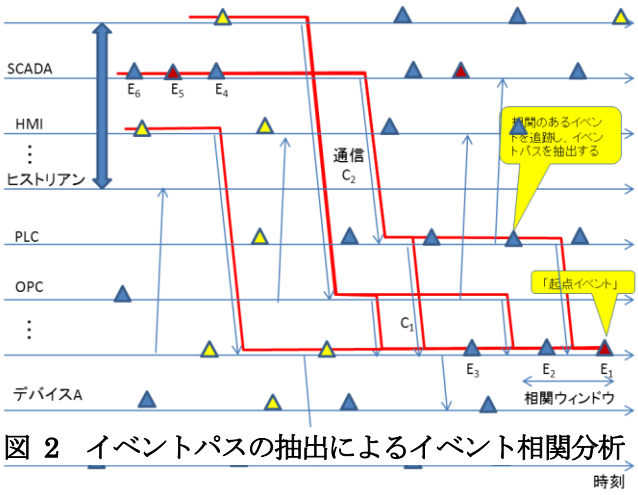


図 2　イベントパスの抽出によるイベント相関分析

5.3 原因分析手法

Stuxnet 等の攻撃ステップ等をもとに危険なイベントの発生順序などを危険パターンとして登録し、イベント相関分析によって得られたイベントパスと危険パターンとのイベント列の類似度を評価することによりイベントパスの危険度を評価する。イベント列の類似度は、DPマッチングや隠れマルコフモデル(HMM)などにより求めることが可能である。これにより着目するイベントを起点にして、時間をさかのぼり関連性をもつイベントパスに対して危険度に基づくランキングを行い特に危険度の高いイベントパスの原因イベントを特定することが可能になる。

実装

以上に示した手法の基本部分を実装した。データ管理部は、セキュリティイベント管理システム(SIEM)の splunk を利用し、ユーザインタフェースは、WEB ベースで実現した。また、分析エンジンは、Hadoop 上で並列実行な実現方式とした。

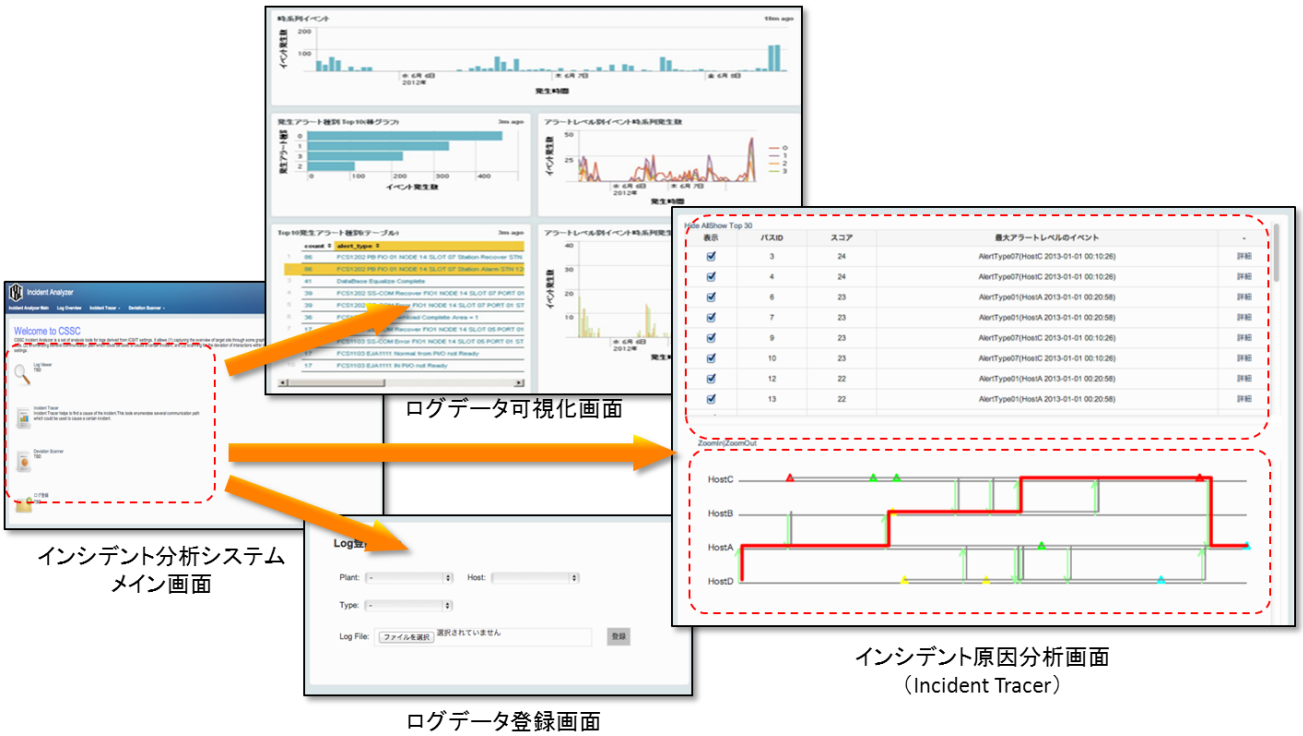


図 3　実装システムの機能画面概観

6. 提案手法の特徴および課題

提案する手法は、特定の機器間のイベントのみならず、多数の機器上で連鎖的進展する一連の攻撃などに対して、イベント系列全体のゾーン横断的な相関分析を行うことができる点が特徴である。

入力するイベントログとして、産業プロセスに関する既存のプロセスアラーム管理システムにおけるプロセスアラームと情報系ネットワークにおける IDS によるセキュリティアラートを用いることにより、セキュリティアラートに起因するプロセスアラームの識別や原因分析などが可能となる。

本研究では、情報系および制御系の既存の IDS やプロセスアラームシステムをベースとして、それらのアラートを横断的に分析することにより、セキュリティイベントに起因したプロセスアラームの特定などを行う分析システムを開発した。本手法では、既存のシステムが発するアラートやイベントの危険度を前提とした分析を行っている。今後は、このような事前の知識に依存しない、イベント系列からの乖離度等に基づく分析手法によりスマートリスト方式の分析手法を開発することにより、適応性の高い汎用的な新たな分析手法を開発することが求められる。たとえば、正常時のログデータから、制御パラメータ書換えなどの危険な操作に至る正常なイベント系列の発生分布を抽出し、それらの動的に生成されたイベント系列から乖離度の高いイベント系列を検出する手法などが考えられる。

また、抽出されるイベントの危険度を評価する際に、危険パターンを知識として与える必要がある点である。危険パターンは、一般には、イベント発生順序に関する様々な組み合わせとなるため、幅広く網羅するために適切なパターンを与えることが問題となる。危険パターンとの類似度の代わりに、安全なイベントパターンとの距離や過去の正常時のパターンとの距離をもとに異常検知する方法などが考えられる。

また、提案手法は、入力として既存システムのアラートを前提とし、それらのイベント間の相関分析を行うことを主眼としているため、入力のアラートの精度に依存することとなる。

一方で、制御システムは動作のリアルタイム性に対する要求が極めて高いため、新たなセキュリティ機能の追加に対するシステムへの影響や安全性に対する検証が求められる。現在、ドラフトの検討が進められている国際標準 ISA-62443-3-3 においては、リソースの可用性やイベントへの迅速な対応について、基本要件が議論されている。このような上位の要件に対応して、具体的な検査項目を示していくことが重要である。

提案手法は、技術研究組合 制御システムセキュリティセンターにおいて構築を進めている制御システムテストベッド上での実験評価を予定している。

7 まとめ

本稿では、産業プロセスに関するアラームと情報系の IDS 等で検知されるセキュリティアラートについて、連鎖する一連のイベント系列全体に関するイベント相関分析を行うことで、セキュリティアラートに起因するプロセスアラートの識別や原因分析を行うための手法について提案し、その実装結果を示した。

謝辞

本研究は、経済産業省「平成 23 年度新規産業創造技術開発費補助金(IT 融合による新産業創出のための研究開発事業(サイバーセキュリティテストベッドの構築))」の下で実施される技術研究組合制御システムセキュリティセンターの委託研究の一環として実施しています。

参考文献

[1] Masaki Ishiguro, Hironobu Suzuki, Yoichi Shinoda, Ichiro Murase, Shigeki Goto, An Internet Threat Evaluation Method based on Access Graph of Malicious Packets, 19th Annual FIRST Security Conference, 2007

[2] W32.Stuxnet Dossier Version 1.4 (February 2011), Symantec Security Response, Nicolas Falliere, Liam O Murchu, and Eric Chien
[3] Linda Briesemeister, Steven Cheung, Ulf Lindqvist, Alfonso Valdes, Detection, Correlation, and Visualization of Attacks Against Critical, Eighth Annual Conference on Privacy, Security and Trust, PST 2010
[4] Digital Bond SCADA IDS Quickdraw SCADA IDS
[5] Security Event Processing with Simple Event Correlator, http://simple-evcorr.sourceforge.net/
[6] Communication Pattern Anomaly Detection in Process Control System, Steven Cheung ,Alfonso Valdes,2009 IEEE International Conference on Technologies for Homeland Security.
[7] Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine, Linda, O. 2011 4th International Symposium on Resilient Control Systems (ISRCS).
[8] 石黒 正揮、鈴木 裕信、村瀬 一郎、篠田陽一, インターネット上の脅威分析を支援する空間および時間的な特徴量に基づく分析手法, 情報処理学会論文誌 Vol.48, Number 9, pp.3148-3162, Sep. 2007