様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １４ 日現在

機関番号：１３９０３
研究種目：基盤研究(A)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０１８３７

研究課題名（和文）サイバー攻撃早期警戒による、被害分離・遮断用サイバー・タグアウト手法の開発

研究課題名（英文）Development of a cyber tag-out system for network isolation and damage mitigation with an early warning function

研究代表者

越島　一郎（Koshijima, Ichiro）

名古屋工業大学・工学（系）研究科（研究院）・教授

研究者番号：３０３０６３９４

交付決定額（研究期間全体）：（直接経費）　　32,100,000円

研究成果の概要（和文）：ICS (Industrial Control System)に対する外部からのサイバー攻撃に対応するには、４つの機能（F1: 攻撃の予兆を早期に発見する機能、F2: 不具合が発生するのを防ぐ機能、F3: 発生した不具合が悪化するのを防ぐ機能、並びにF4: 不具合から回復する機能）の構築が不可欠である。
このため、本研究ではF1への対応としてICS 専用の早期警戒機能を構築し、F2に対してプラント運転状況に合わせて不要な通信をタグアウト（遮断）する機能を開発した。この２つ機能は、F3およびF4への対応として不具合発生箇所をICS ネットワークから速やかに切り離すことにも有効である。

研究成果の学術的意義や社会的意義
これまで空間的、特に時間的にネットワークを孤立化させる論理的な方法論は報告されていない。また、その方法論をサポートするハードウエアの提供もなされていない。本研究の主眼点は、①攻撃者の行動特性を利用した早期警戒網で攻撃を検知・防御すると共に、②プラント運転状況に応じて制御に必要不可欠な機器を選択的にネットワークに接続する２点にある。このため、本研究によって開発された上記①，②に対応したタグアウトシステムは、サイバー攻撃者に容易に運転システムと運転状態を取得・改変させない仕組みで現場への導入も比較的容易のため、重要インフラの安全性向上に貢献し、社会的波及効果は極めて高いと考える。

研究成果の概要（英文）：The following four functions are essential to respond to external cyber attacks on ICS (Industrial Control System). F1: functions to detect early signals of cyber attacks, F2: function to mitigate the failure from cyber attacks, F3: function to prevent a propagation of the failure, and F4: recovery function from the failure.
In this research, we built an early warning function dedicated to ICS as a response to F1, and developed a function to tag out (block) unnecessary communication to F2 according to the plant operating condition. These two functions are also effective for quickly disconnecting the fault from the ICS network as a response to F3 and F4.

研究分野：制御システムセキュリティ

キーワード：サイバー・タグアウト装置　早期警戒システム　ゾーン設定・切替　制御ネットワーク用SDN　ハニーポッド　アクティブデセプション

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

【制御システムにおける安全対策の状況】

失われた 20 年と引き続く低成長経済下でプラントに対して行われたコスト削減策は、少人数化・自動化である。この核となった IT 技術は、サイバーセキュリティ問題をプラントに持ち込み、外部からの操作・運転情報の隠蔽の可能性を排除できない事態となっている。しかし現場では、ビジネス系の下層に製造系ネットワークが位置するため、「(サイバー攻撃が発生したときに) IT 部門がどのようなプロセスで対応しているのかまったく分からないし、どのように情報が下りてくるか分からない」状況にあり、企業全体で見ても、予算や人員の要求ができる部署や責任者が曖昧な状況にある。

【学術界・業界の状況】

本研究の背景を纏めると、以下のとおりである。

(1) プロセス系、制御系の学術界：情報技術・制御技術・プロセス設計技術・ヒューマンファクターが関わるこの複合領域に対して、積極的に関わることはなされていない。

(2) 重要インフラ、特に石油・石油化学業界：サイバー攻撃が現実のものと受け取られている。しかし、資金的に実際に事故が起こっている安全対応で手一杯であって、未だ自社実例がない（又は確認出来ていない）制御システム・セキュリティへの投資には消極的である。

(3) 製造系の現場：現場ではサイバー攻撃と認めることが困難で、更に認知したとしても少人数化によってプラントの安全を担保する時間的余裕は見込めない状況にある。

【状況の打開】

上記(1)から(3) に対する打開策として、以下が考えられる。

(1) プロセス系、制御系の学術界：申請者らにとって、自由に使用できるテストベッドの構築が後述する研究成果達成に大きく寄与している。このため研究者が共有できるテストベッドの構築し、公開することが必要である。

(2) 重要インフラ、特に石油・石油化学業界：プラントの安全強化が同時にセキュリティ強化につながるソリューションの開発が不可欠である。

(3) 製造系の現場：現場においてプラント機器とオペレータが持つ能力を最大限活用するには、サイバーセキュリティ問題を局所化するサイバー・タグアウトシステム（タグアウトシステムは、米国連邦労働安全衛生局によって義務付けられた安全管理システム）が必要である。

２．研究の目的

これまで申請者らのこれまでの研究から、以下が重要である事が判明した。

(1) 攻撃の早期警戒によって、攻撃側にフリータイム（攻撃側がシステムに潜伏していることに、防御側が気付いていない状態）を与えないこと
異常な通信を検知したら攻撃者（又は標的型攻撃で用いられる情報収集型のマルウエア）の情報収集時間を引き延ばすことで、“フリータイムを無駄に消費したくない”攻撃者の心理を逆手に取った、「攻撃者に攻撃を断念させる防御方法」を開発する。

(2) 攻撃側にフリータイムを許したとしても、重要インフラの各構成要素間で行われるやり取りを系統的に把握させないこと
本件の解決方策として、a)通信の孤立化と b)通信の暗号化が考えられる。最新の制御機器の CPU パワーが向上している事から暗号化は大変有効であるが、既存の重要インフラでも低コストで有効な対応策として、a)通信の孤立化を選択とする。通信の孤立化には、以下の２種類が考えられる。
① 空間的孤立化：ハードウエア間の情報的・物理的なつながりをブロック
② 時間的孤立化：ハードウエアが制御される時間流れの中で、特定な時間をブロック

本研究では、双方の孤立化を同時に実現しすることで、「セキュリティ確保すると共に外部からの侵入による不安全行為を阻止するための方法論(サイバー・タグアウトと称す)」の開発と実証を研究目的とした。

３．研究の方法

攻撃者の行動特性を利用した早期警戒網で攻撃を検知・防御すると共に、プラント運転状況に応じて制御に必要不可欠な機器を選択的にネットワークに接続・切断することで、制御システムのセキュリティを高める目的を達成するために、２つのグループ A) 攻撃者に攻撃を断念させる防御方法の開発、B) プラントの運転状態に合わせて通信をサイバー・タグアウトするための方法論の開発に分けて研究を実施した。更に、研究協力者と共に C) 機能実証用システムの開発を行った。

A)から C)の詳細は以下の通りである。

A． 攻撃者に攻撃を断念させる防御方法の開発

A1． ICS ネットワークに設置可能な「低対話型ハニーポッド」機能：ICS ネットワーク内で、制御機器の存在しないアドレスへ擬似制御機器として設置することで、ここへの通信を異常通信として判定し、設置しても通信障害を発生させないハニーポッド機能である。

A2． ICS ネットワークの構成を動的に変化させる機能：異常通信を検知すると、ハニーポッ

ドの擬似制御機器としてのプロフィールとアドレスを変更して、収集した情報に基づいた攻撃を意味の無いものとする機能である。

A3. ハニーポッドを分散配置した早期警戒機能：複数のハニーポッドを分散配置することで、情報の集約を図り、網を構成することで特に同時多発するマルウエア攻撃の予兆を捉える。

B. プラントの運転状態に合わせて通信をサイバー・タグアウトするための方法論の開発
本研究の主体であり、以下の機能を有する必要がある。

B1. 動的ゾーニング機能：現場機器から得られた情報から、プラントの運転状態に合わせて現場機器（制御機器（DCS、PLC や SCADA）とそれによって制御されるプラント機器）をゾーン分けし、サイバー攻撃を分離・遮断する機能ある。

B2. 通信経路を決定する機能：B1.で決定したゾーン毎に経路を限定した通信を行う機能であり、攻撃者によるネットワーク構造の把握、通信の傍受並びにネットワークへの侵入を抑制する。

B3. 通信経路を指示する機能：B2.によって決まった通信経路に合わせて、通信ネットワークの接続・切断を管制する。

C. 機能実証用システムの開発

C1. 早期警戒システム並びにサイバー・タグアウトシステムのプロトタイプ

C2. 機能試験と学術研究に共用するテストベッド

C3. 分散配置する早期警戒網

４．研究成果

各年度ごとの、「研究の方法」A1 から C3 に対応した研究成果は以下の通りである。

平成２８年度

A1. 「低対話型ハニーポッド」機能の開発: ICS ネットワークにサイバー攻撃によって出現する通信パターン特性を利用し、攻撃検知を行う低対話型ハニーポッドを実装した。

A2. ICS ネットワークの構成を動的に変化させる機能の開発: A1.のハニーポッドにアクセスがある毎にネットワークの構成を変更する機能を実装した。また、エンドユーザ支援協力企業 Y 社の製品に組み込み、FACTORY2017 の同社ブースにて実演展示を実施した。

A3. ハニーボッドを分散配置した早期警戒機能の開発： ICS ネットワーク内では、ハニーボッドは Zone と Conduit に合わせて配置する必要がある。このため、分担者の橋本が VISIO で開発している Zone 設計支援ツールを拡張した。

B1. 動的ゾーニング機能の開発: 非定常運転モード(スタートアップ、シャットダウン等)に合わせて Zone 構造を予め設定し、通信経路を切り替える Software Defined Network を OpenFlow を用いて構築した。

B2. 通信経路を決定する機能： 制御機器に対する通信経路は制御機器自身と OPC サーバで管理されている。このため、予め取得した通信経路情報から B1.で決定された Zone を通る経路を抽出する機能を Zone 設計支援ツールに組み込んだ。

C2. 共用テストベッドの開発: プロセス機器は固定だが、制御機器の構成や接続方法を実験者が柔軟に変更可能とするテストベッドを構築した。(図１参照)

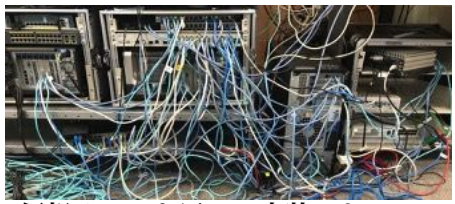
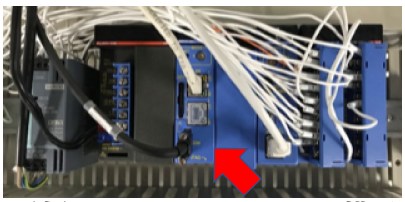


図１仮想サーバを用いて実装したテストベッド
（VEC「つるまいプロジェクト」でのペネトレーションテストのため、複数のセキュリティ・アプライアンスをインストールした上で仮想企業の ICS ネットワークを模擬した状態）

平成２９年度：

A1. 「低対話型ハニーボッド(HP)」の実環境での試験運用：開発支援協力企業 P 社が有する事業所ネットワーク監視システムに接続して実地試験を行なった。この試行で月平均 100 ギガ（最大 400 ギガ）のログを収集し、ランサムウエアによる攻撃の検出にも成功した。

A2. PLC への HP の組み込み：平成 28 年度に A1.にて Raspberry Pi 上に実装した HP を、制御機器メーカーの協力を得て市販 PLC に実装し、現場への導入を可能とした。(図２参照)



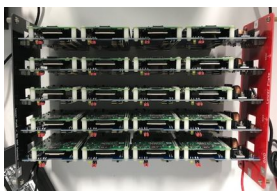


図２（左）HoneyPod Industry（横河電機 e-RT3 Plus への実装 矢印のユニット）
（右）HoneyNet（Raspberry PI 20 台で構成 分散配置用）

B3．動的ゾーニング用 Open vSwitch の開発:平成 28 年度開発した B1．B2.を、SDN 技術を用いてハードウエア（８ポート Hub の形状）として実装した。(図３参照)

図３動的ゾーニング用 Open vSwitch （タグアウトシステム）

C1．サイバー・タグアウトシステムのプロトタイプ: B3.と攻撃パターン学習結果を組み合わせることで攻撃手法と対象を推定し、攻撃を受けた箇所を切り離すシステムのプロトタイプを開発した。

C2．機能試験と学術研究に共用するテストベッドの構築: NTT コミュニケーション、マカフィー、カスペルスキー、トレンドマイクロの協力を得て、サイバー攻撃テストベッドを構築し、ホワイトハッカー東大 M 准教授のペネトレーションテストによって、 制御システム向けセキュリティ対策の試験環境として有用であることが確認された。

C3．クラウドへの情報集約:分散配置した HP が収集した攻撃情報をクラウドに集約し、モニタリンクするシステムのプロトタイプを、PTC 社のクラウド ThingWorks 上に構築した。

平成３０年度：

A3．ハニーポッドを分散配置した早期警戒機能：「つるまいプロジェクト」（制御システムを標的にしたサイバー攻撃の産学共同研究）における攻撃実験において、「低対話型ハニーポッド」(HP)を複数分散配置して攻撃の予兆を捉える実験を実施し、有効性を確認した。これをもって、当初計画した「攻撃者に攻撃を断念させる防御方法の開発」は完了した。

B3．サイバー・タグアウト装置のプロトタイプ製作：開発支援協力企業 P 社にてデモ展示をおこない、実務環境での有用性の確認を頂いた。これをもって、当初計画した「プラントの運転状態に合わせて通信をサイバー・タグアウトするための方法論の開発」を完了した。

C2．学術研究に共用するテストベッド：これまで協力いただいた関係企業に対して、早期警戒網と ICS 用 SDN を用いたタグアウトシステムのデモ展示を実施した。

C3．分散配置する早期警戒網：早期警戒網プロトタイプを、通期に渡り製造企業（組立加工系１社）の現場に設置して実データ収集にあたった。この結果は、当初考慮していなかった、次の２点の開発に繋がった。

C3-1.通常時（非異常時）の通信パターンを機械学習アルゴリズムによって学習することで、サイバー攻撃の予兆を検知する方法

C3-2.多量のログ（400Gb/月）を対象とした Near Real Time Monitoring (nRTM)を行う方法

これをもって、当初計画した「機能実証用システムの開発」は完了した。

５．主な発表論文等

〔雑誌論文〕（計　９件）

1) 加藤 勇夫，太田 結隆，越島 一郎，リーン＆アジャイルプログラムマネジメントに関する基礎的考察 － イノベータ育成のためのイノベーションプロセスの再考 －，国際 P2M 学会誌，査読有，Vol.13(2)，2019，pp.60-80

2) Tsuchiya Akihiro、Fraile Francisco、Koshijima Ichiro、Ortiz Angel、Poler Raul, Software defined networking firewall for industry 4.0 manufacturing systems, Journal of Industrial Engineering and Management，査読有，Vol.11(2)，2018，pp.318-333

3) Ota Yuitaka、Aoyama Tomomi、Nyambayar Davaaadorj、Koshijima Ichiro, Cyber incident exercise for safety protection in critical infrastructure, International Journal of Safety and Security Engineering，査読有,Vol.8，2018，pp.246-257

4) T. Hamaguchi, H. Sakashita, H. Moritani, K. Takeda, N. Kimura, M. Noda, Method for Designing Alarm System Using DAEs, CE Matrices and Preference Indices, Journal of Chemical Engineering of Japan，査読有，Vol.50，2017，pp.439-444

5) Hideyuki Shintani, Tomomi Aoyama, Ichiro Koshijima, Study on High Resilient Structures for IoT Systems to Detect Accidents, Journal of Disaster Research，査読有，Vol.12，2017，pp.1073-1080

6) Tomomi Aoyama, Toshihiko Nakano, Ichiro Koshijima, Yoshihiro Hashimoto, Kenji Watanabe, On the Complexity of Cybersecurity Exercises Proportional to Preparedness, Journal of Disaster Research，査読有，Vol.12，2017，pp.1081-1090

7) 孫晶，高木ひとみ，伊藤一馬，越島一郎，橋本芳宏，制御系ネットワークのセキュリティ対策立案のアプローチ，横幹連合会誌「横幹」，査読有，Vol.10，2016，pp.107-115

8) 孫晶，高木ひとみ，越島一郎，橋本芳宏，ICS セキュリティ対策の立案手法，日本設備管理学会誌，査読有，Vol.28，2016，pp.119-125

9) Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Ichiro Koshijima, A Metric for Quantitative

Estimation of Production Process Resilience based on the Production Support System in the Chemical Industry, Journal of Chemical Engineering of Japan, 査読有, Vol.49, 2016, pp.673-679

〔学会発表〕（計１２件）

1) ニャムバヤル ダワードルジ，太田 隆、越島一郎，P2M における重要インフラのためのセーフティとセキュリティマネジメント・フレー ムワークに関する研究，国際 P2M 学会 2018 年度 秋季研究発表大会，2018，pp.293-299
2) S. Kondo, H. Sakashita, S. Sato, T. Hamaguchi, Y. Hashimoto, An application of STAMP to safety and cyber security for ICS, 13th International Symposium on Process Systems Engineering, 2018, pp.2335-2340
3) Haruna Asai, Tomomi Aoyama, Ichiro Koshijima, Design and Operation Framework for Industrial Control System Security Exercise, AHFE 2018, 2018, pp.171-183
4) Asuka Terai, Tatsuya Chiba, Hideyuki Shintani, Shoya Kojima, Shingo Abe, Ichiro Koshijima, WIT Transactions on Engineering Sciences, Risk 18, Vol.121, 2018, pp.197-208
5) 千葉達也，寺井あすか，新谷英介，小島将耶，越島一郎，異スペクトル変換を利用した産業用制御システムにおける異常検知システム，電子情報通信学会 2018 年総合大会，2018，pp.125
6) Davaadorj Nyambayar, Ichiro Koshijima, Safety and Security Integration for Production Industry Under Resilience Matrix, Safety and Security Engineering VII, 2017, pp.203-211
7) Hidekazu Hirai, Tomomi Aoyama, Davaadorj Nyambayar, Ichiro Koshijima, Framework for Cyber Incident Response Training, Safety and Security Engineering VII, 2017, pp.273-283
8) Asuka Terai, Shingo Abe, Shoya Kojima, Yuta Takano, Ichiro Koshijima, Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine based on Communication Profile, 2nd IEEE European Symposium on Security and Privacy,2017, pp.132-138
9) Tomomi Aoyama, Kenji Watanabe, Ichiro Koshijima, Yoshihiro Hashimoto, Developing a Cyber Incident Communication Management Exercise for CI Stakeholders, 11th International Conference on Critical Information Infrastructures Security, 2016,Paper 51
10) Wataru Machii, Akihiro Tsuchiya, Tomomi Aoyama, Takashi Hamaguchi, Yoshihiro Hashimoto, Ichiro Koshijima, Zoning Management of Secured Industrial Control System, The 7th International Symposium on Design, Operation and Control of Chemical Processes, 2016, Paper B131
11) H. Moritani, T. Yamamoto, S. Yamamoto, K. Ito, J. Sun, T. Hamaguchi, I. Koshijima, Y. Hashimoto, Generation of Fault Trees for ICS Safety and Security, The 7th International Symposium on Design, Operation and Control of Chemical Processes, 2016, Paper P102
12) Shinya Yamamoto, Takashi Hamaguchi, Sun Jing, Ichiro Koshijima, Yoshihiro Hashimoto, 12. A Hot-Backup System for Backup and Restore of ICS to Recover from Cyber-Attack, Advances in Human Factors, Software, and Systems Engineering, Advances in Intelligent Systems and Computing, Vol.492, 2016, pp.45-53

〔産業財産権〕

○出願状況（計　２件）

名称：通信装置
発明者：越島一郎，橋本芳宏，高野雄太，新谷英之，小島将也
権利者：越島一郎，橋本芳宏，高野雄太，新谷英之，小島将也
種類：特許
番号：特願 2017-196360
出願年：2017
国内外の別： 国外

名称：通信装置
発明者：越島一郎，橋本芳宏，高野雄太，新谷英之，小島将也
権利者：越島一郎，橋本芳宏，高野雄太，新谷英之，小島将也
種類：特許
番号：特願 2016-210845
出願年：2016
国内外の別： 国内

６．研究組織
(1)研究分担者
研究分担者氏名：橋本　芳宏
ローマ字氏名：HASHIMOTO Yoshihiro
所属研究機関名：名古屋工業大学
部局名：工学研究科
職名：教授
研究者番号（8桁）：90180843
研究分担者氏名：渡辺　研司
ローマ字氏名：WATANABE Kenji
所属研究機関名：名古屋工業大学
部局名：工学研究科
職名：教授
研究者番号（8桁）：90361930
研究分担者氏名：濱口　孝司
ローマ字氏名：HAMAGUCHI Takashi
所属研究機関名：名古屋工業大学
部局名：工学研究科
職名：准教授
研究者番号（8桁）：80314079
研究分担者氏名：青山　友美
ローマ字氏名：AOYAMA Tomomi
所属研究機関名：名古屋工業大学
部局名：工学研究科
職名：助教
研究者番号（8桁）：60770055
研究分担者氏名：寺井 あすか
ローマ字氏名：TERAI Asuka
所属研究機関名：公立はこだて未来大学
部局名：システム情報科学部
職名：准教授
研究者番号（8桁）：70422540

(2)研究協力者
研究協力者氏名：孫晶
ローマ字氏名：SUN Jing
研究協力者氏名：太田 結隆
ローマ字氏名：OTA Yuitaka
研究協力者氏名：ダワードルジ ニャムバヤル
ローマ字氏名：DAVAADORJ Nyambayar
研究協力者氏名：江口 元
ローマ字氏名：EGUCHI Hajime
研究協力者氏名：加藤 勇夫
ローマ字氏名：KATO Isao
研究協力者氏名：待井 航
ローマ字氏名：MACHII Wataru