様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月　 ８ 日現在

機関番号：１３９０３
研究種目：基盤研究(B)
研究期間：2012～2014
課題番号：２４３１０１１９

研究課題名（和文）セキュリティを含めたプラントの本質安全システム構築法の開発

研究課題名（英文）Development of Intrinsically Safe System for Cyber-secure Plants

研究代表者
越島　一郎（Ichiro, Koshijima）

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）　　14,500,000円

研究成果の概要（和文）：本研究では、オープン化された制御システム系ネットワークを含むプラント並びに制御システムを対象として、安全性確保に加えてサイバー攻撃からのセキュリティ防御を含めた独立防御階層（IPL）の設計・運転手法の確立を目指した。この結果、サイバー攻撃の特徴である同時多発性を想定して、①プラント運転者の視点に立った攻撃検知方法、②攻撃者の視点に立った、攻撃妨害方法、③攻撃に対して抵抗力のあるサイバーレジリエントな組織構築方法の開発を行うことで、既存のIPLを最大限活用する方策を開発した。なお、本研究の成果は、学術論文8報、国際学会発表12件、国内学会発表16件、特許申請2件に纏められている。

研究成果の概要（英文）：In this research, a new concept of IPL (Independent Protection Layer) for safety and cyber-security was discussed to protect computer controlled critical infrastructures from cyber-attacks. As the results, the development team proposed the new methodology that fully utilizes conventional IPL. The following three rational developments are included in this proposal; 1) Intrusion detection system from the viewpoint of plant operators, 2) Attach interference system from the viewpoint of attacker’s psychology, 3) Resilient organization against the cyber-attacks. These developments were presented through 8 journal papers, 12 international conferences, 18 domestic conferences and 2 patents.

研究分野：プロセスシステムズエンジニアリング，プロジェクトマネジメント

キーワード：プラント制御システム　サイバーセキュリティ　セーフティ

１．研究開始当初の背景

サイバーテロによる重要インフラへの攻撃は、2010 年 Stuxnet というワームの出現により、現実のものとなった。Stuxnet の攻撃対象はイランの核燃料濃縮施設の遠心分離機という非常に特定されたもので、そこに至るあらゆる経路を探るため、世界中に感染が広がり、本来孤立しているはずのシステムへの攻撃に成功した。現在、プラント計装のシステムは、Windows や OPC というオープンシステムで構築されるようになり、同じワームで多くの箇所を攻撃できる可能性がある。また、リアルタイム性が必要な計装システムは、セキュリティパッチの適用を控えるのが通常で、危弱性が高い。情報系のセキュリティの向上は、攻撃と防御のイタチゴッコであり、ファイアーウォール等の防御体制の充実はもちろん必要であるが、情報系での防御が破綻したとしても、プラントでの事故を防ぐことができるように、プラントの設計と運転の安全性を本質的に高める必要がある。

従来の安全設計は、トラブルが発生しても安全に停止することを目指していたが、テロの攻撃では、重要インフラを停止させることも目的のひとつであり、不必要に停止させられることは回避しなければならないし、これまでの安全設計では、複数故障の同時発生は確率が低いと扱っていたが、サイバーテロ対策では、複数トラブルの同時発生や隠蔽を想定しなければならない。このため、サイバーテロに対するプラントの本質安全を実現するためのプラント設計・計装設計・プラント運転の設計方法・評価方法の確立は急務であった。

２．研究の目的

本研究は、オープン化された制御システム系ネットワークを含むプラント並びに制御システムを対象とし、安全性の概念にセキュリティも含め、独立防護階層（IPL）の評価を改め、安全性を統一的に確保する設計・運転手法の確立を目指して、以下の３つを研究目的とした。

1) 解析対象構造（プラント構造並びに IT ネットワーク構造）のモデル化
本質的に動的な IT ネットワークを一体としてとらえるための構造モデルを検討する。
2) 解析対象の動的状態遷移（プラント制御、ネットワーク操作）の制動
異常伝播モデルを構築し、そのモデルを基にして伝播を抑制、分離、遮断する設計法を構築する。
3) SCADA、DCS 等の自動制御用ハードウエア・ソフトウエアが介在した装置間の故障波及解析
悪意によるこのようなアクセスが在り得るという観点で、フェールセーフ、フールプルーフを設計しなおす手法を開発する。また、擬似プラント・システムを用いたプラントオペレータのセキュリティ・リスク対応演習プログラムを提供することを目指すこととした。

３．研究の方法

「セキュリティを含めたプラント安全システムの構築法の開発」を行うため、安全性評価手法開発とテストベンチ開発の二つの研究グループを組織して取り組み、互いの成果を統一して、新たなプラント安全の確立に努めた。

安全評価手法開発グループ：
安全確保の網羅性を確保する手法である HAZOP を、悪意による操作介入の下でも、安全性を確保できる対策が確認できるまで、解析を展開するように、拡張するとともに、ネットワークセキュリティの防御層も整理し、セキュリティを含めたプラント安全を評価できる FTA、ETA の構築と評価方法を検討する。研究協力者にも、検討に参加してもらい、現状の脆弱性について整理する。

テストベンチ開発グループ：
セキュリティの観点での現在のシステムの脆弱性を実感し、多重の防御の必要性とその方法について学ぶためのテストベンチのプラントと教育プログラムを開発する。このテストベンチは、脆弱性とともに最新の剛健性を実現できるシステムでなければならず、研究協力者から、現状及び最新のセキュリティ情報を提供してもらい、プラントとして高いセキュリティが実現できるシステムを開発する。

また、セキュリティ教育プログラムの開発は、本研究の範囲としないが、技術研究組合制御システムセキュリティセンター(理事長：新 誠一 電気通信大学 教授)並びにオランダ ENCS(European Network for Cyber Security)と連携して実施した。

なお、研究方法は以下のとおりである。

1) プラント安全
- 因果ネットワークによる定性推論や意図を表現する知識ベースの構築の知見を生かして、悪意による多重異常の想定方法、記録方法について渕野を中心に検討する。
- 定性モデルによる異常の伝播に基づく異常診断と対策立案の研究成果から、セキュリティを考慮したアラームの設計方法を検討する。

2) ネットワークセキュリティ
- ディスクリート・イベント・シミュレーション（DeS）に FTA の確率統計の概念を加味することで、ネットワークセキュリティの防御層の整理と安全性評価を行う。
- 安全性評価として統合するための、異常時の対策立案(2008)の研究を基礎とし

て、セキュリティに関するリスクの評価方法について検討する。

3) 実証用テストベンチの構築

・ サイバーテロを再現し、従来の計装システムの危弱性をシミュレーションするためのテストベッドを構築する。

4) 安全性評価手法の開発

・ 平成 24 年度に開発した HAZOP,アラーム、ネットワークセキュリティ、FTA 評価の結果を統合

・ セキュリティを含めたプラント安全評価を可能にする手法を開発

5) 実証用テストベンチの構築

・ ミニプラントの計装、ビジネス系ソフト、ネットワークのハードウェア、ソフトウェアを完成させ、さまざまなセキュリティレベルで検討

・ 様々なセキュリティレベルでの演習が、現場オペレータ、エンジニア、業務系のシステムエンジニアと異なる立場の人間に対して行えるようにシステムを整備

6) テストベンチを用いて、実証試験を実施

・ 化学プラントｒ企業のオペレータなど、実際の現場の人も参加した実証試験の実施

４．研究成果

サイバー攻撃からのセキュリティ防御を含めた独立防御階層（IPL）の評価フレームワークを与えるとともに、設計・運転手法の確立を目指した結果、サイバー攻撃の特徴である同時多発性を想定して、以下の開発を行うことで、従来の単一故障を想定して安全を担保する既存の IPL を最大限活用する方策を開発した。

① プラント運転者の視点に立ち、プラント並びにその制御システムが持つ冗長性と整合性を活用した攻撃検知方法の開発

② 攻撃者の視点に立った、攻撃妨害方法の開発

③ 攻撃に対して抵抗力のあるサイバーレジリエントな組織の構築方法の開発

なお、本研究の成果は、学術論文 8 報、国際学会発表 12 件、国内学会発表 16 件、特許申請 2 件に纏められている。

また、本研究の成果を基に、平成 26 年 1 月 8,9 日には産業技術総合研究所セキュアシステム研究部門との共催で「サイバーセキュリティチュートリアル」を名古屋工業大学で開催し、約 80 名の参加者にサイバーセキュリティの現状、その問題点並びに行われている研究について紹介した。平成 27 年 3 月 18,19 日には、プラントオーナー、制御機器ベンダー、セキュリティ専門家を招いて、2 日間に亘り「制御系セキュリティ演習」ワークショップを開催した。内容は、以下のとおりである。

平成 27 年 3 月 18 日	
コマ	項目
	ウェルカムセッション
1	イントロダクション 概論
2	サイバー攻撃デモンストレーション １．攻撃デモ （対策なし 20 分、対策あり 10 分） ２．考察（グループディスカッション 30 分）
3	対策ツール紹介 １．製品紹介 （McAfee 様、ダイレックス様） ２．越島研究室研究成果 ３．既存セキュリティツール
4	現場インシデント対応セッション １．ディスカッション 30 分 ２．発表 5 分*4 チーム=計 20 分 ３．総合議論 10 分 ４．インシデントレスポンス （短期、現場寄り）
5	セキュリティ対策評価立案手法
6	セキュリティ対策提案セッション １．ディスカッション 40 分 ２．発表 10 分*4 チーム=計 40 分 ３．インシデントレスポンス （短期、現場寄り） （安全を確保するまでのシナリオ）
平成 27 年 3 月 19 日	
7	BCM と IT-BCP の概要
8	復旧までのシナリオづくりを含めた BCM 立案 １．ディスカッション （昼食・休憩は各グループで適宜） ２．インシデントレスポンス（長期） （復旧するまでのシナリオ）
9	各グループ BCM 発表セッション 発表 10 分*4 チーム=計 40 分 （余裕分）総合議論 20 分
１０	レジリエンス向上のための組織づくり
１１	これまでの世界の制御系セキュリティ演習と今回提案の演習の比較と解説
１２	総合討論 今後のセキュリティ対策の検討に求められるもの

重要インフラ（電力、ガス、上下水道、石油・石油化学プラント等）ばかりでなく現代のシステム（公共交通、高層ビル等）の多くは自動制御システムを用いて運用されている。本研究で構築した実証用テストベンチを用いたサイバー攻撃デモの見学者が 200 名を越えたことは、関係各位の関心の高さを表すものである。更に、これらのシステムに対す

るネットワークを通したサイバー攻撃の脅威は、2020 年に開催される東京オリンピックの妨害も含めて年々増大している。本研究によって、これらのシステムの３要素（人的資源（ソフト）、施設（ハード）、制御（ソフト））を最大限活用して、ハード・ソフトの両面からレジリエントな体制を構築することに貢献できたと考える。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　８件）

[1] 濱田佑希, 小野斎里, Ngo Hoai Duc, 越島一郎, P2M のためのリスクマネジメント手法に関する基礎的研究, 国際プロジェクト・プログラムマネジメント学会誌, Vol.7, No.2, pp.53-74, 20130200 (査読有)

[2] Yoshihiro Hashimoto, Takeshi Toyoshima, Shuichi Yogo, Masato Koike, Takashi Hamaguchi, Sun Jing, Ichiro Koshijima, Safety Securing Approach against Cyber-Attacks for Process Control System, Computers & Chemical Engineering, Vol.57, No.15, pp.181-186, 20131000 (査読有)

[3] 濱田佑希, 越島一郎, 渡辺研司, P2M フレームワークに基づく事業ライフサイクル BCMP に関する研究, 国際プロジェクト・プログラムマネジメント学会誌, Vol.8, No.2, pp.135-153, 20140200 (査読有)

[4] 橋本芳宏, 越島一郎, プロセス制御系のサイバーセキュリティ対策の立案と評価, ヒューマンファクターズ, Vol.19, No.1, pp.18-25, 20140800 (査読有)

[5] 青山友美, 越島一郎, 関　康平, 松田成史, 大規模サイバーセキュリティ演習から学ぶレジリエントなインシデントマネジメント, 信学技報, Vol.114, No.340, pp.19-23, 20141100

[6] 松田成史, 小池正人, 待井　航, 青山友美, 成岡秀真, 越島一郎, 橋本芳宏, 通信プロファイルを用いた制御システムネットワーク監視システム, 信学技報, Vol.114, No.340, pp.13-18, 20141100

[7] 待井　航, 加藤勇夫, 小池正人, 松田成史, 青山友美, 越島一郎, 橋本芳宏, 制御系システムのセキュリティ向上のための動的ゾーニング, 信学技報, Vol.114, No.340, pp.7-12, 20141100

[8] 濱田佑希, 青山智春, 越島一郎, 渡辺研司, 永里賢治, 状況マネジメントのための動的対応シナリオ生成手法に関する基礎的研究, 国際プロジェクト・プログラムマネジメント学会誌, Vol.9, No.2, pp.237-254, 20150312 (査読有)

〔学会発表〕（計２８件）

[1] 濱田佑希, Ngo Hoai Duc, 越島一郎, プロジェクトトラブルの発生構造と管理に関する基本的考察, 国際プロジェクト・プログラムマネジメント学会 2012 年度春季研究発表大会, 東京農工大学小金井キャンパス, 20120421

[2] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, S. Jing and I. Koshijima, Conceptual Framework for Security Hazard Management in Critical Infrastructures, The 11th International Symposium on Process Systems Engineering, Singapore, 2012 (査読有)

[3] T. Hamaguchi, K. Takeda, M. Noda, N. Kimura, A Method of Designing Plant Alarm Systems with Hierarchical Cause-Effect Model, The 11th International Symposium on Process Systems Engineering, Singapore, 2012 (査読有)

[4] 濱田佑希, 小野斎里, 越島一郎, P2M のためのリスクマネジメント手法に関する基礎的研究, 国際プロジェクト・プログラムマネジメント学会 2012 年度秋季研究発表大会,東京農工大学小金井キャンパス, 2012

[5] 橋本芳宏, 与語修一, 森田貴仁, 孫晶, 越島一郎, 設備管理とサイバーセキュリティ, 日本設備管理学会平成 24 年度秋季研究発表大会,名城大学, 20121117

[6] 松田成史, 越島一郎, 制御系ネットワーク監視プローブの開発, 日本設備管理学会東海支部平成 24 年度学生研究発表会, 名古屋工業大学, 20130301

[7] Tomomi Aoyama, Ichiro Koshijima, A Unified Framework for Safety and Security Assessment in Critical Infrastructure, 日本設備管理学会東海支部平成 24 年度学生研究発表会, 名古屋工業大, 20130301

[8] 森田貴仁, 与語修一, 孫晶, 越島一郎, 橋本芳宏, 制御系セキュリティ向上のためのゾーン設計, 第 13 回適応学習制御合同シンポジウム, アクロス福岡, 20130305

[9] 濵田佑希, 中島朗, 川口均, 渡辺研司, 越島一郎, P2M を用いた企業間 BCP の統合化に関する基礎的研究, 国際プロジェクト・プログラムマネジメント学会 2013 年度春季研究発表大会, 東京工業大学田町キャンパスイノベーションセンター, 20130420

[10] Tomomi Aoyama, Masato Koike, Ichiro Koshijima, Yoshihiro Hashimoto, A Unified Framework for Safety and Security Assessment in Critical Infrastructures, Safety and Security Engineering V, pp.67-77, Rome, Italy, 20130900 (査読有)

[11] Takahito Morita, Shuichi Yogo, Masato Koike, Takashi Hamaguchi, Sun Jing, Ichiro Koshijima, Yoshihiro Hashimoto, Detection of Cyber-Attacks with Zone Dividing and PCA, 17th International Conference in

Knowledge Based and Intelligent Information and Engineering Systems, Vol.22, pp.727-736, Kitakyushu, Japan, 20130909 (査読有)

[12] 予語修一, 橋本芳宏, 越島一郎, 孫晶, 浜口孝司, 小池正人, サイバー攻撃リスクの評価方法, 化学工学会 第 44 回秋季大会, 東北大学, 20130919

[13] 濱田佑希, 越島一郎, 渡辺研司, P2M フレームワークに基づく事業ライフサイクル BCP に関する研究, 国際プロジェクト・プログラムマネジメント学会 2013 年度秋季研究発表大会, 東京農工大学小金井キャンパス, 20131005

[14] 関康平, 越島一郎, 安藤敬亮, チームプロジェクトにおけるリーダー選出手法に関する研究, 日本経営工学会平成 25 年度秋季大会, 日本工業大学宮代キャンパス, 20131116

[15] Jing Sun, Yoshihiro Hashimoto, Shuichi Yogo, Takahito Morita, Hiroki Moritani, Ichiro Koshijima, A Process Alarm Design of Quantitative Value with Zone Dividing for Control System Security, 2013 Asian Conference of Management Science & Applications, pp.372-377, 20131200 (査読有)

[16] 関康平, 越島一郎, 濱田佑希, 緊急時における迅速なリーダー選出手法に関する研究, 平成 25 年度経営工学会中部支部研究発表会, 名古屋工業大学, 20140227

[17] 濱田佑希, 青山智春, 越島一郎, 渡辺研司, 永里賢治, 状況マネジメントのための動的シナリオ生成手法に関する基礎的研究, 国際プロジェクト・プログラムマネジメント学会 2014 年度春季研究発表大会, 東京工業大学田町キャンパスイノベーションセンター, 20140419

[18] Tomomi Aoyama, Isao Kato, Ichiro Koshijima, Masahito Koike, Framework for Life Cycle Security and Safety for Critical Infrastructures, The 5th World Conference of Safety of Oil and Gas Industry, Paper No. 1092680, Okayama, Japan, 20140608 (査読有)

[19] Masafumi Matta, Masato Koike, Wataru Machii, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, Industrial Control System Monitoring based on Communication Profile, The 5th World Conference of Safety of Oil and Gas Industry, Paper No. 1092435, Okayama, Japan, 20140608 (査読有)

[20] Wataru Machii, Isao Kato, Masahito Koike, Masafumi Matta, Tomomi Aoyama, Ichiro Koshijima, Yoshihiro Hashimoto, Dynamic Zoning of the Industrial Control System for Security Improvement, The 5th World Conference of Safety of Oil and Gas Industry, Paper No. 1065756, Okayama, Japan, 20140608 (査読有)

[21] 青山友美, 越島一郎, 重要インフラにおけるサイバーレジリエンスマネジメント, 日本プラント・ヒューマンファクター学会 2014 年大会, 日本大学生産工学部, 20140912

[22] 林 拓哉, 渡辺 研司, 越島 一郎, 防災情報・災害情報の提供方法及び統合化に関するフレームワークの検討, 日本経営工学会平成 26 年度秋季大会, 東京理科大学 野田キャンパス, 20141108

[23] 青山友美, 越島一郎, 関　康平, 松田成史, 大規模サイバーセキュリティ演習から学ぶレジリエントなインシデントマネジメント, 電子情報通信学会第 28 回情報通信システムセキュリティ研究会, 東北学院大学　多賀城キャンパス, 20141127

[24] 待井　航, 加藤勇夫, 小池正人, 松田成史, 青山友美, 越島一郎, 橋本芳弘, 制御系システムのセキュリティ向上のための動的ゾーニング, 電子情報通信学会第 28 回情報通信システムセキュリティ研究会, 東北学院大学 多賀城キャンパス, 20141127

[25] 松田成史, 小池正人, 待井　航, 青山友美, 成岡秀真, 越島一郎, 橋本芳宏, 通信プロファイルを用いた制御システムネットワーク監視システム, 電子情報通信学会第 28 回情報通信システムセキュリティ研究会, 東北学院大学 多賀城キャンパス, 20141127

[26] Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Ichiro Koshijima, Optimal job routine assignment for the improvement of operational resilience based on skills and knowledge of production staff in the chemical industry, SCIS & ISIS 2014, pp.861-866, Kitakyushu, Japan, 20141203 (査読有)

[27] Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Ichiro Koshijima, Optimal Personnel Reallocation in Production Processes Based on the Skills and Knowledge in the Chemical Industry, The 3rd International Conference on Industrial Application Engineering 2015 (ICIAE2015), Kitakyushu, Japan, Paper GS3-3, 20150328 (査読有)

[28] Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Impact of an Organizational Structure on the Resilience of Production Processes Based on Artificial Factors in the Chemical Industry, The 3rd International Conference on Industrial Application Engineering 2015 (ICIAE2015), Kitakyushu, Japan, Paper GS3-4, 20150328 (査読有)

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　２件）

名称：災害・避難情報蓄積配信システム
発明者：越島一郎、渡辺研司、小池正人、林拓哉
権利者：国立大学法人名古屋工業大学
種類：特許
番号：2014-192275
出願年月日：2014 年 9 月 22 日
国内外の別：国内

名称：動的ゾーニングプラントシステム
発明者：越島一郎、待井航、小池正人、青山友美、内田拓郎
権利者：国立大学法人名古屋工業大学
種類：特許
番号：2015-036148
出願年月日：2015 年 2 月 26 日
国内外の別：国内

○取得状況（計　０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
越島　一郎（名古屋工業大学工学研究科・教授）
　研究者番号：３０３０６３９４

(2)研究分担者
橋本　芳宏（名古屋工業大学工学研究科・教授）
　研究者番号：９０１８０８４３
渕野　哲郎（東京工業大学工学研究科・准教授）
　研究者番号：３０２１９０７６
濱口　孝司（名古屋工業大学工学研究科・所教）
　研究者番号：８０３１４０７９

(3)連携研究者
（　　）

　研究者番号：