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 ２８ 年　 ５ 月 ３１ 日現在

機関番号：１３９０３
研究種目：基盤研究(B)（一般）
研究期間：2013～2015
課題番号：２５２８２１０１

研究課題名（和文）サイバー攻撃を考慮した制御系と緊急シャットダウンシステム構築法の開発

研究課題名（英文）Development of Controllers and Emergency Shutdown Systems Considering Cyber-Attacks

研究代表者
橋本　芳宏（Hashimoto, Yoshihiro）

名古屋工業大学・工学（系）研究科（研究院）・教授

研究者番号：９０１８０８４３

交付決定額（研究期間全体）：（直接経費）　　13,200,000円

研究成果の概要（和文）：本研究では、計装ネットワークへの侵入を完璧に防ぐのは不可能であるとの認識の下、全面的に攻略される前に検知して安全にシャットダウンさせることができるシステムの構築をめざした。安全を確保するための計装ネットワークの分割、隠ぺい工作を検出するための計装ネットワークの分割を設計するCADの開発を行った。さらに攻撃を回避するために、コントローラとハニーポットを動的に切り替えるシステムを開発した。またサイバー攻撃を検知したのちに、攻撃を防御し、復旧するまで、組織的に対応できるような演習を開発し、３回ワークショップを開催した。

研究成果の概要（英文）：In this study, the construction of the system, which can detect cyber-attacks, prevent the invasion to the whole instrumentation network and shut it down safety, were developed under the recognition that it was impossible to protect control systems perfectly from cyber-attacks. CADs to divide the instrumentation networks to ensure the safety and to detect concealment by cyber-attackers. A protection system to switch controllers and honeypots dynamically was developed. In addition, exercise for people beyond the organization from the detection of cyber-attacks to restoration was developed and workshops were held three times.

研究分野：プロセスシステム工学

キーワード：サイバーセキュリティ　プロセス制御　安全

１．研究開始当初の背景

2010 年にイランの核燃料施設の制御システムを標的にした Stuxnet が登場して以来, 制御システムへのサイバー攻撃は増え続けており, 2013 年の時点の日本でもすでに，1 か月以上の長期停止を余儀なくされた工場が発生していた．従来，ICS (Industrial Control Systems)は独自 OS の採用，ネットワークの独立性などの理由により，サイバー攻撃に対するセキュリティ面は問題視されていなかった．しかし，様々なシステムとのネットワーク接続，Windows や Ethernet など汎用システムによる構築化がなされることにより，その前提が覆されている．アンチウイルスソフトの導入やセキュリティパッチなどの一般的な脆弱性対策は，ICS の主機能であるリアルタイム制御に悪影響を与える恐れがあるため，容易には導入できないという事情がある．また，一般的な情報システムへのサイバー攻撃と異なり，ICS へのサイバー攻撃はプラントの爆発事故など甚大な事故を引き起こす危険性があるため，事故防止の観点から，安全に関する ICS 独自のセキュリティ強化を行う手法の開発が重要な課題となっている．

ISA99, IEC62443 という AICS (Automatic Industrial Control Systems)のサイバーセキュリティ対策に関する標準規格も議論されているが，そこでは，Zones and Conduits という多層防御と SAL (Security Assurance Levels)というセキュリティレベルの評価は提案されているものの制御系が攻略された際の安全性を関連付けた議論にはなっていない．

暗号化やユーザー認証などの情報セキュリティ技術を制御ネットワークに適用することで，セキュリティを高める提案になっているが, 現在の制御系では, 即時性を重要視して，セキュリティを高めるのには有効と理解していても適用していないのが実情であるし，情報セキュリティ対策では，新たな脆弱性の発見とその対策の開発の頻度が激しく，いたちごっこできりがないという面が否めない．

プロセス計装では，従来より安全を重大課題として，通常制御，警報を発生することによるオペレータのマニュアル操作，緊急遮断システムと多重防御層を設定することが提案されている．しかし，サイバーセキュリティを事故原因の一つとして想定された解析はなく，サイバー攻撃の場合，まず，通常制御が破綻し，次にアラームに頼ってもダメで，緊急遮断システムが安全を確保するという順番も成立するとは限らない．

２．研究の目的

本研究では，サイバー攻撃に対して，安全を担保するための制御ネットワークの構成方法と情報セキュリティ技術の適用方法を検討する．そして，サイバー攻撃を検知した場合に，安全を確保するとともに，いち早く復旧し，他のプラントへの攻撃も防ぐという組織的な対応を検討し，それを実現するための演習を企画することもめざす．

３．研究の方法

安全対策では，フェールセーフ，フールプルーフという考え方が一般的に用いられる．サイバー攻撃によるプロセス制御の破綻は，ネットワークを通じて侵入して直接操作するか，マルウエアとして感染して操作するかのバリエーションはあるが，安全の破綻は，操作端を危険な状態が発生するように操作されるか，危険な状態を回避するために本来働くべき操作が動作できないようにされるかという「悪意の誤操作，悪意の誤動作」とみなせる．つまり，悪意に基づいているかどうかの違いはあるが，従来から検討されている誤操作，誤動作であるので，これまでの安全解析の手法が適用できるはずであると考えられる．

悪意に基づくと，従来の安全解析では，そこまで検討しなくてもよいであろうとされていた多重性，多層性が問題になってくるが，サイバー攻撃だからと言って，これまでには想定できなかった新たな事故が発生するようになるわけではない．

事故を確実に発生させようとすれば，どんどん困った状況に陥らせるように，悪意の誤操作を積み重ね，その状態を気づかせないように隠ぺいも行うことが考えられる．

このような操作を不可能にするように，情報セキュリティ技術を適用することも重要であるが，いたちごっこになりかねない情報セキュリティ対策だけでなく，制御対象の特徴を利用して，サイバー攻撃で発生してしまった物理的な変化が，不安全な状態に発展するまでに，検知し回避対策を実現できる制御ネットワーク構造を構築することも有効であると考える．

重大事故が考えられるプラントほど，不安全な状態は，一つの操作だけで発生することがないように，フェールセーフ，フールプルーフとなるように，プラント及びコントローラは設計される．重大事故は，複数個の不安全操作が重なることで初めて発生するのであれば，その一部の不安全操作を阻止できれば，一部のセキュリティ対策が破綻し，不安全な操作を実行されても，重大事故は防げるので，それらへのサイバー攻撃には，別の手段が必要になるように複数のゾーンに分割して，それぞれに異種のセキュリティ対策を配置することを考える．

この検討を行うために，安全解析の手法の一つである Fault Tree Analysis を利用する．この方法では，事故原因を And，Or で整理するので，同時に攻略されないように別のゾーンに分割管理すべきコントローラを洗い出すことができる．事故原因をサイバー攻撃とすると，FTA で洗い出す異常原因は，コントロ

ーラの異常，センサーの異常と限定することができる．プラントの場合，事故発生が想定される装置のコントローラではなく，上流や下流のコントローラの異常が引き金になる可能性があるので，大規模なプラントであると，Fault Tree の数が多くなるし，各 Fault Tree の構築もたいへんになる．

そのため，各装置のモジュールに，その装置の状態変化まで展開した Fault Tree のトップ部分を登録し，装置の接続関係をもとに，事故原因になるコントローラの異常まで展開する CAD を開発することにした．

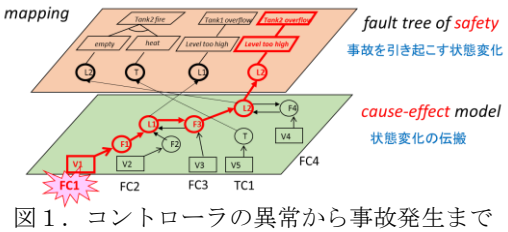

図１．コントローラの異常から事故発生まで

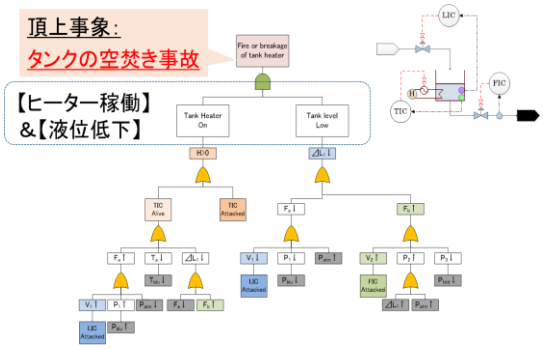

図２．サイバー攻撃の Fault Tree の例

また，事故の解析から，サイバー攻撃を受けた際の，異常の検知から，サイバー攻撃を受けているという判定，安全確保のための操作，被害拡大を阻止するための関係部署への連絡や，早期復旧のための対応までのシナリオを作成し，シナリオを下に，組織をまたがった対応力強化のための制御系サイバーセキュリティ演習を企画する．

４．研究成果

サイバー攻撃による事故を想定した FTA として，危険な状態を発生させるためのコントローラの操作を解析する Tree と危険な状態に気づかせないようにするためのコントローラの操作を解析する Tree からなる構成の Fault Tree を提案した [6,23]．

一部隠ぺいされても，一部生き残れば，隠ぺい工作を見破れるという性能を確保するための制御ネットワークの分割を提案する CAD[6,23]と，一部攻略されても，一部生き残れば，不安全な状態を回避できるという性能を確保するための制御ネットワークの分割を提案する CAD[7]を開発した．

さらに，実験装置に工業計装を取り付け，異なるゾーンで守る制御系ネットワークの実装方法を示し，その計装を実際にサイバー攻撃して，防御策がないと危険な状態になりかねない現状を示すとともに，異なるゾーンを設定する防御法の有効性を示すデモンストレーションを開発した．このデモンストレーションには，2016 年 4 月時点で，のべ 400 名近くの来訪者を得ている．

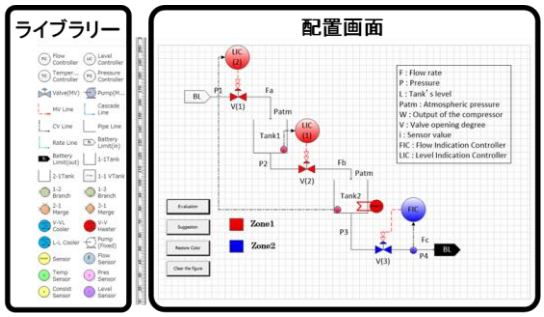

図３．ゾーン分割提案 CAD の画面例

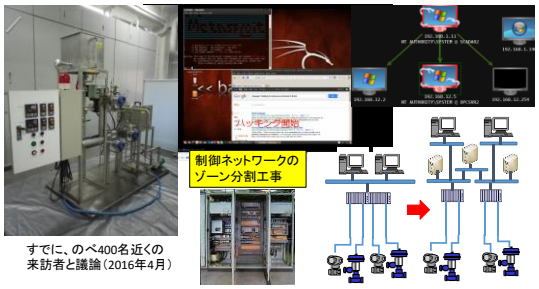

図 4. サイバー攻撃のデモンスレーション装置

さらに，プラントの異常検知から，サイバー攻撃と判断し，安全対策し，復旧するまでの対応を，ビデオ画像で設定を確認しながら，グループで検討する演習を 3 回開催した．2015 年 3 月 29，30 日には 13 社 18 名，2015 年 8 月 26，27 日には 30 社 74 名，2016 年 3 月 29，30 日には 26 社 47 名の参加を得た．

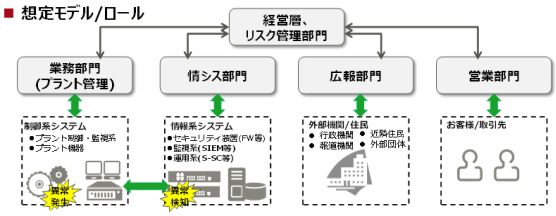

図 5. 演習で対象とする社内組織の例

図 6. 演習で用いる想定ビデオの画面の例

図 7. 演習のグループディスカッションの風景

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　6 件）

1) Industrial Control System Monitoring Based on Communication Profile, Masafumi Matta, Masato Koike, Wataru Machii, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, Journal of Chemical Engineering of Japan, 査読有, Vol.48, No. 8, pp.609-618 (2015-08)
2) Optimal Personnel Reallocation based on the Skills and Knowledge in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of the Institute of Industrial Applications Engineers, 査読有, Vol.3, No.3, pp.126–133 (2015-07)
3) Organizational Structure on the Resilience of Production Processes based on Artificial Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of the Institute of Industrial Applications Engineers, 査読有, Vol.3, No.3, pp.141–147 (2015-07)
4) Business Process Model Approach for Management of Plant Alarm System, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda: J. of Chemical Engineering of Japan, 査読有, 48(8), pp.641-645 (2015)
5) 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，橋本芳宏，越島一郎，ヒューマンファクターズ，査読有，Vol.19(1), pp.18-25 (2014-08)
6) Safety Securing Approach against Cyber-Attacks for Process Control System, Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, I. Koshijima, Computers & Chemical Engineering, 査読有，Vol.57, pp.181-186 (2013)

〔学会発表〕（計　20 件）

7) 制御系のサイバーセキュリティ対策のための安全解析ツールの開発，森谷　祥貴，浜口孝司，越島一郎，橋本芳宏，計測自動制御学会第 3 回制御部門マルチシンポジウム (2016)
8) Strategic Security Protection for Industrial Control System, H.Takagi, T.Morita, M.Matta, H.Moritani, T.Hamaguchi, S.Jing, I.Koshijima, Y.Hashimoto, Proc. SICE Annual Confernce, 査読有，pp.1215-1221 (2015)
9) Dynamic Zoning Based on Situational Activitie for ICS Security, Wataru Machii, Isao Kato, Masahito Koike, Masafumi Matta, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, the 10th Asian Control Conference 2015 (ASCC 2015), 査読有, pp.1242-1246 (2015-05)
10) Studying Resilient Cyber Incident Management from Large-scale Cyber Security Training, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Wataru Machii and Kohei Seki, the 10th Asian Control Conference 2015 (ASCC 2015), 査読有, pp.2890-2893 (2015-05)
11) Impact of an Organizational Structure on the Resilience of Production Processes Based on Artificial Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, The 3rd International Conference on Industrial Application Engineering 2015 (ICIAE2015), 査読有, GS3-4 (2015-03)

Organizational Structure on the Resilience of Production Processes based on Human Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of Engineering Science and Technology Special Issue on SOMCHE 2014 & RSCE 2014 Conference, 査読有, pp.30-40 (2015-01)

12) A Method for Generation and Check of Alarm Configurations Using Cause-Effect Matrices for Plant Alarm System Design, T.Hamaguchi, B.Mondori, K.Takeda, N.Kimura, M.Noda, Proc. 17th International Conference on Human-Computer Interaction, 査読有, pp.549-556 (2015)
13) Modelling of a Business Process for Alarm Management Lifecycle in Chemical Industries, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Proc. 17th International Conference on Human-Computer Interaction, 査読有, pp.579-587 (2015)
14) 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，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，待井　航，青山友美，越島一郎，橋本芳宏，信学技報，査読無, Vol.114(340), pp.7-12 (2014-11)
15) 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，青山友美，越島一郎，関康平，松田成史，信学技報，査読無，Vol.114(340), pp.19-23 (2014-11)
16) Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security, H. Moritani, S. Yogo, T. Morita, M. Kojima, K. Watanabe, J. Sun, I. Koshijima, Y. Hashimoto, ICCAS 2014, 査読有，Oct. 22-25, Korea (2014-10)
17) Industrial Control System Monitoring based on Communication Profile,

Masafumi Matta, Masato Koike, Wataru Machii, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, Okayama, Japan, 査読有, Paper No. 1092435, (2014-06)
18) Dynamic Zoning of the Industrial Control System for Security Improvement, Wataru Machii, Tomomi Aoyama, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, Okayama, Japan, 査読有, Paper No. 1065756 (2014-06)
19) BPM Approach for Describing Plant Alarm System Design Process, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Proc. WCOGI 2014, PS-3, 査読有(2014-06)
20) Framework for Life Cycle Security and Safety for Critical Infrastructures, Tomomi Aoyama, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, 査読有, Paper No. 1092680 (2014-06)
21) A Process Alarm Design of Quantitative Value with Zone Dividing for Control System Security, J. Sun, Y. Hashimoto, S. Yogo, T. Morita, H. Moritani, I. Koshijima, 2013 Asian Conference of Management Science & Applications, 査読有, pp.372-377 (2013)
22) Detection of Cyber-Attacks with Zone Dividing and PCA, T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, I. Koshijima, Y. Hashimoto, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems, 査読有, Vol.22, pp.727-736 (2013)
23) A Unified Framework for Safety and Security Assessment in Critical Infrastructures, T. Aoyama, M. Koike, I. Koshijima, Y. Hashimoto, Proc. of Safety and Security Engineering V, 査読有, pp.67-77 (2013)
24) Generating Alternative Modules for a Plant Alarm System Based on First-Out Alarm Alternative Signals, T.Hamaguchi, B.Mondori, K.Takeda, N.Kimura, M.Noda, Procedia Computer Science, 査読有, 22, pp. 937-944 (2013)
25) A Method of Designing Plant Alarm System based on First Alarm Alternative Signals for Each Assumed Plant Malfunction, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Proc. PSE Asia 2013, 査読有, pp. 245-250 (2013)
26) Determination of Alarm Setpoint for Alarm System Rationalization using Performance Evaluation, N.Kimura, T.Hamaguchi, K.Takeda, M.Noda, LNCS 8017, 査読有, pp. 507-514 (2013)

〔図書〕（計　1 件）

27) プラント制御システムのセキュリティ対策,橋本芳宏, 4 章 19 節,化学工場・研究所の事故対策と安全管理,技術情報協会 (2015)

〔産業財産権〕

○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
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

橋本芳宏（名古屋工業大学工学研究科・教授）
研究者番号：90180843

(2)研究分担者

越島一郎（名古屋工業大学工学研究科・教授）
研究者番号：30306394

渡辺研司（名古屋工業大学工学研究科・教授）
研究者番号：90361930

浜口孝司（名古屋工業大学工学研究科・助教）
研究者番号：80314079

(3)連携研究者

（　　）
研究者番号：