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　３ 年　 ６ 月 ２２ 日現在

機関番号：１３９０３
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０１６６６

研究課題名（和文）サイバー攻撃下でもコントロールサービスを継続するための制御ネットワーク構造の開発

研究課題名（英文）Development of control network structure for continuing control service even under cyber attack

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）：サイバー攻撃者に操作されると、物理的な事故が発生してしまうコントローラに外部からアクセスできないようにして、事業所内のネットワークを仮想化し、クラウドに移行されたレベル３以上のネットワークにセキュアに接続するというレベル２のネットワークの新たな構造をフォグとして提案した。
フォグを実現する技術として、SDN技術で、攻撃の可能性を検知した時に、単に遮断するのではなく、コントローラを隔離し、サンドボックスに導き、安全性を確保するとともに攻撃者の情報を獲得する手段、検知された異常の危険性を脆弱性情報と組み合わせて評価する手段、暗号化されているコントローラへの通信内容を監視する手段などを開発した。

研究成果の学術的意義や社会的意義
サイバー攻撃は、工場設備にも及んでおり、甚大な事故が発生する可能性もある。サイバー攻撃の高度化は著しく、各社、各事業所で、セキュリティ対策の人員体制の確保はますます困難になっている。オフィス環境もクラウドに移行しているが、操業現場もクラウド、仮想環境などを駆使した新たな操業体制が望まれる。そこでの事業所のネットワークの構造のあるべき姿と防御方法について提案した。
ここでの提案は、現在世界で進行しているIndustrie4.0やOpen Process Automationにも適合する概念であるとともに、ネットワーク構造や監視、対応に対する具体的で新規な技術を示すものである。

研究成果の概要（英文）：We proposed a new structure for Level 2 networks as "fog", which is to prevent external access to the controllers, which would cause a physical accident if manipulated by a cyber attacker, and to virtualize the network in the plant site and securely connect it to a Level 3 or higher network that has been moved to "cloud".
We developed the technologies to realize "fog". One is SDN technology that, when it detects a possible attack, does not simply block it, but isolates the controller and leads it to a sandbox to ensure safety and acquire information on the attacker. Second is a risk assessment system to evaluate the risk of observed abnormality considering vulnerabilities in "fog". We propose to apply encrypted OPC-UA communication in "fog". Encryption makes communication secure, but it does not prevent the transmission of dangerous commands to the controller, so we developed a system to monitor the communication contents in encrypted communication.

研究分野：プロセスシステム

キーワード：サイバーセキュリティ　制御系ネットワーク　クラウド・フォグ　仮想環境　切り替え　リスク評価　暗号通信監視

１．研究開始当初の背景

プロセスオートメーションは、古くは、人を単純労働から解放し、その後、コンピュータの利用で、人にはできない高精度、高速、高品質、高効率な製造を実現させ、収益性向上に貢献してきた。安全で安定な操業を維持するために、信頼性を高める努力も続けられてきた。しかし、これまでの信頼性は、腐食や摩耗などによる劣化や、設計や施工の不良、人間の過誤による誤操作によるトラブルが対象であったが、悪意の攻撃も考慮しなければならない時代になっている。

すでに、重要インフラでのサイバー攻撃は増えてきており、2015 年 12 月にはウクライナで、BlackEnergy3 というマルウェアで 30 か所の変電所が同時に攻撃され、コールセンターも襲われたので、大規模の停電が長時間発生するという事件が発生した。2017 年には WannaCry というマルウェアで、世界中で病院やインフラに被害が出ているし、日本のセキュリティ先端企業でさえ被害にあった。

サイバーセキュリティの研究としては、認証や暗号化のように、鍵を頑丈にする技術や、ネットワークの防犯カメラに相当するパケットやログの監視・解析技術など、学術的な研究は多く存在するが、サイバー攻撃による制御系の操作で安全が破綻することを防御することを対象にした学術的研究は少ない。また、安全に対する研究も多いが、故障や、意図しない誤操作を対象にしたものがほとんどであり、サイバー攻撃のような悪意を前提にしたものはない。

２．研究の目的

本研究では、これまで研究が進んでいないセキュリティとセーフティの共通部分であるサイバー攻撃による安全の破綻を防止するための制御システムの構築と管理方法を研究する。本研究の特徴は、サイバー攻撃の手口に注目するのではなく、守るべきものを基準にセキュリティ対策を検討する点である。サイバー攻撃は、情報システムを利用して行われるため、物理的な変化を引き起こそうとすると、コントローラを誤動作させてアクチュエータを操作するか、センサーの値を改竄して、オペレータの誤操作を誘引するかしかない。そのため、本研究では、悪意による同時多重の誤動作・誤操作に対しても安全を確保できる多重多層の Fail-Safe, Fool-Proof の構築を、制御システムと情報ネットワークに対して検討する。

３．研究の方法

重要インフラのサイバーセキュリティ対策について、米国標準技術研究所からサイバーセキュリティ対策のフレームワークという取り組みの基本、共通用語なるものが提案されている。そこでは、Identify, Protect, Detect, Respond, Recovery という５つのコアの観点が示されている。自分の状況を認識し、防護策を考えるまでは、これまで取り組まれている面があるが、それも、一部の取り組みでやっている気になっている面がある。本研究では、脆弱性に注目した Identify の方法、事故が発生するプラントから水際へと意識を広げていく多重な Protect の設計に加えて、まだ、ほとんど普及していない制御ネットワークでの Detect と検知された後の Respond、そして、早期復旧に必要なバックアップや再発防止のために不可欠なログの確保という観点での Recovery と総合的に対策を検討する。

４．研究成果

(1) Identify

組織のリスクを識別する Identify に必要な脆弱性管理に、CVE(Common Vulnerabilities and Exposures)を

利用することを考え、制御ネットワークに存在するサーバーや PC の OS やアプリケーションに存在するモジュールを分析し、データベースに管理し、CVE データベースを監視することで、制御ネットワーク内の脆弱性をリアルタイムに把握できるシステムを構築した。ただし、システム内のモジュールの解析には、市販のツールを利用した。

(2) Protect

セキュリティパッチを即座に適用できるように、仮想環境を多重に用意し、仮想環境上にサーバーや PC を設定し、バックアップ側でパッチを適用し、即座に切り替えられる構造での制御システムネットワークの構築を提案した。さらに、制御ネットワーク内の通信は、セキュリティを考慮して開発された標準プロトコル OPC-UA に統一することを提案し、従来のシステムを利用しつづける場合にも OPC-UA ラッパーを利用することを提案した。

(3) Detect

上記の仮想環境内に、仮想の攻撃対象であるハニーポットを設置するとともに、システムログや通信パケットを監視することを提案した。ここで特に、重視したのは、コントローラに危険なコマンドが届くと、物理的な事故が発生してしまうリスクで、たとえ、通信が暗号化されていても、コントローラへの指示内容は監視したいという点である。暗号化された通信は傍受しても内容を把握できないのであるが、ここでは傍受ではなく、コントローラへの通信をこの機器を介さないと行えない構造にして、その機器に監視とログの安全な保存機能を持たせることにした。さらに、物理的な事故のリスクが検知されたときには、ネットワーク監視をしている SOC(Security Operation Center)だけでなく、プラント監視している SCADA 画面にも通知し、操業状態の変更という現場の体制につながりうるインターフェイスも提案した。図 1 に示しているのがその一例で、ここでは、どの箇所の通信を遮断して、操業を継続する、あるいは、安全のためにプラントを停止するなどの判断の支援になるように、異常が検知されているネットワーク内の箇所とその危険性を、ネットワーク内の脆弱性の存在とともに表示することを意識している。

(4) Respond

異常が検知されたときに、取りうる対応は、一部の通信遮断と代替通信経路を利用した操業継続、あるいは、一部のプラント停止、全面停止などの対応が必要になる。通信の遮断を検知すると自爆して証拠隠滅を図るマルウェアも少なくない。そのため、マルウェアを検知した時、プラント側への通信経路は遮断し、サンドボックスに切り替え、上部への通信は遮断するのではなく、ネットワークの他の部分からは隔離しながらも、外部との通信は維持するというネットワーク構造の変化を実現する SDN(Software Defined Network)を提案した。図 2 にその構造変化を示す。これは、敵の手口を探るとともに、再発防止のための情報確保にも重要で、次の Recover にも有用である。

(5) Recovery

安全を確保するだけでなく、操業の復旧も重要である。バックアップを常にとり、即座に切り替えられる構造とともに、バックアップも攻撃されてしまうリスクも軽減するために、多重の仮想環境を利用する構造を検討した。コントローラやプラント運転員からは、どのサーバーにアクセスしているかはわからないがサービスは提供し続けてくれるという点でクラウドと同じであるが、プラントのコントローラと直結する事業所内に存在するシステムという意味でフォグと位置づけ、その必要な機能を整理した。

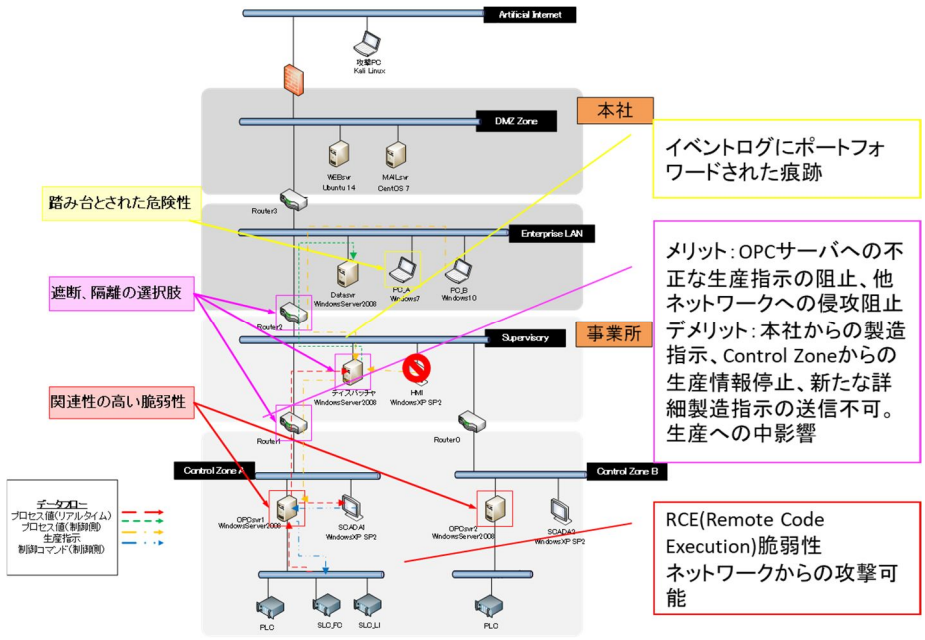

図 1. 異常検知時の状況表示と意思決定支援

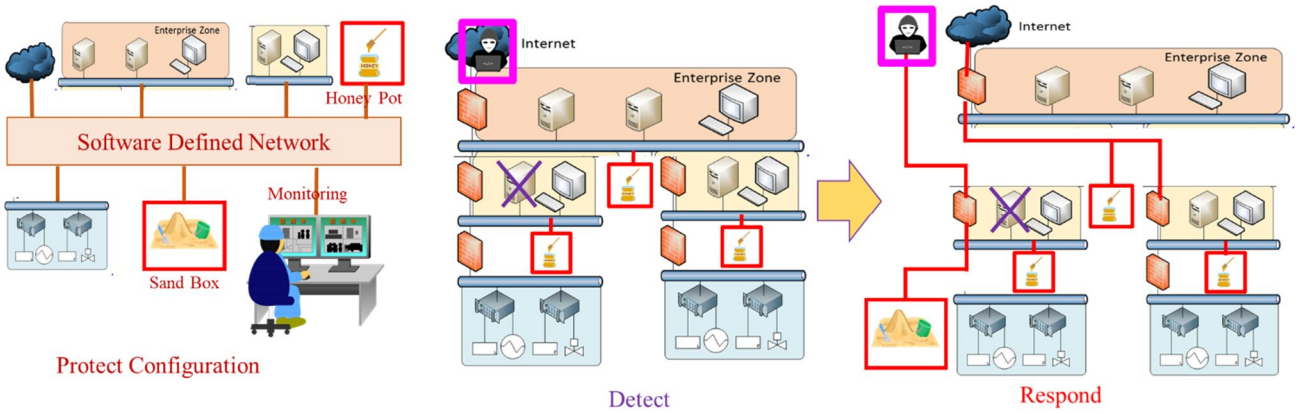

図 2. SDN によるネットワーク構造の変更

＜引用文献＞

① .National Institute of Standards and Technology(NIST), IPA 独立行政法人情報処理推進機構翻訳監修 Framework for Improving Critical Infrastructure Cybersecurity, 重要インフラのサイバーセキュリティを改善するためのフレームワーク, Version l.1, April l6,2018. https://www.ipa.go.jp/files/000071204.pdf

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Tsuchiya Akihiro、Fraile Francisco、Koshijima Ichiro、Ortiz Angel、Poler Raul	４．巻 11
２．論文標題 Software defined networking firewall for industry 4.0 manufacturing systems	５．発行年 2018年
３．雑誌名 Journal of Industrial Engineering and Management	６．最初と最後の頁 318,328
掲載論文のDOI（デジタルオブジェクト識別子） 10.3926/jiem.2534	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 M.Sumi, K.Iitaka, T.Hamaguchi and Y.Hashimoto
２．発表標題 Development of Plant Operator Support Tool based on Vulnerability and Network Monitoring Against Cyberattack
３．学会等名 18th Asian Pacific Confederation of Chemical Enginnering Congress (APCChE2019)（国際学会）
４．発表年 2019年

１．発表者名 Shun Kondo, Hiroto Sakashita, Souta Sato, Takashi Hamaguchi, Yoshihiro Hashimoto
２．発表標題 An application of STAMP to safety and cyber security for ICS
３．学会等名 International Symposium on Process Systems Engineering; PSE 2018（国際学会）
４．発表年 2018年

１．発表者名 A.Tsuchiya, U.Ota, Y.Takayama, T.Aoyama, T.Hamaguchi, Y.Hashimoto, and I.Koshijima:
２．発表標題 Cyber-Incident Exercise Admitting Inter-Organization for Critical Infrastructure Companies
３．学会等名 International Symposium on Process Systems Engineering; PSE 2018（国際学会）
４．発表年 2018年

１．発表者名 Hidekazu Hirai, Yuma Takayama, Tomomi Aoyama, Yoshihiro Hashimoto, Ichiro Koshijima
２．発表標題 Development of the Cyber Exercise for Critical Infrastructures Focusing on Inter-Organization Communication
３．学会等名 International Symposium on Process Systems Engineering; PSE 2018（国際学会）
４．発表年 2018年

〔図書〕　計1件

１．著者名 橋本芳宏	４．発行年 2020年
２．出版社 技術情報協会	５．総ページ数 770うち12
３．書名 工場･研究所における災害・事故および各種リスクの可視化と対策 第5章 第6節プラント制御システムのセキュリティ対策 12ページ	

〔出願〕　計2件

産業財産権の名称 制御ネットワークにおける通信監視システム	発明者 橋本芳宏、越島一郎、本田寿明、平石力哉	権利者 同左
産業財産権の種類、番号 特許、特願2020-001713	出願年 2020年	国内・外国の別 国内

産業財産権の名称 ネットワーク管理装置	発明者 越島一郎、橋本芳宏、尾川友規、西田稜	権利者 同左
産業財産権の種類、番号 特許、特願2020-001712	出願年 2020年	国内・外国の別 国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	濱口　孝司 (Hamaguchi Takashi) (80314079)	名古屋工業大学・工学（系）研究科（研究院）・准教授 (13903)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	青山　友美 (Aoyama Tomomi) (60770055)	名古屋工業大学・工学（系）研究科（研究院）・助教 (13903)	
研究分担者	越島　一郎 (Koshijima Ichiro) (30306394)	名古屋工業大学・工学（系）研究科（研究院）・教授 (13903)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関