IoT 時代の新しい制御システムセキュリティコンセプト「情報物理セキュリティ」とその具体例「MemWiper」の紹介

Physically Isolated Information Security (PIIS) and MemWiper: A New Security Concept for Control Systems in IoT Era and Its Embodiment

新井 貴之 *1　　仲矢 実 *1
Takayuki Arai　　Makoto Nakaya

IoT（Internet of Things）時代に増大が懸念される遠隔からの攻撃リスクを低減するための新しいセキュリティコンセプトとして，「情報物理セキュリティ」を提案する。「情報物理セキュリティ」コンセプトでは，遠隔から攻撃されづらい「情報物理セキュリティ施策」を用いてシステムを攻撃から保護する。「情報物理セキュリティ施策」の簡単な実装例として，USB メモリ消去装置「MemWiper」を試作した。「MemWiper」を用いることで，ウイルス感染という情報セキュリティ問題を物理的な操作で低減できる。本稿では，情報物理セキュリティの考え方とその具体例である「MemWiper」について紹介する。

Yokogawa proposes physically isolated information security (PIIS), a new security concept for reducing the risk of remote attacks on industrial control systems. PIIS can protect plants from remote attacks. As a simple implementation, Yokogawa has developed MemWiper, a prototype device that erases the memory of USB devices. MemWiper reduces the risk of virus infection through physical operation. This paper explains the PIIS concept and the MemWiper memory erasers.

1. はじめに

近年のセンシング技術，無線技術やマイクロデバイス技術の進展により，様々なモノがネットワークでつながり，遠隔での操作や制御を行う IoT（Internet of Things）の技術適用が着々と進行している。**図 1** に示すように，現実世界のプラントで計測されたデータを基に定量的に分析，学習，モデル化し，Cyber Physical System あるいは Digital Twin と呼ばれるサイバー空間に仮想プラントが構築される。プラントの挙動を模擬するサイバー空間上のモデルを活用し，実際の生産現場で生じる原燃料の多様化や生産量調整などの課題に，最適なオペレーション条件を提供するなど，IoT 技術は安全・安心な操業や効率的な生産に貢献している [(1)(2)]。

一方で，様々なモノがインターネットに接続されれば，インターネットを通じてウイルス感染や不正アクセスを許す機会が増える。もしソフトウェアに脆弱性が見つかれば，そこを目がけて攻撃される可能性が増大する。脆弱性が少ないといわれる標準ソフトウェアでも，脆弱性が必ずしもゼロではないため，放置された脆弱性が攻撃対象として狙われる可能性は高い。IoT によってもたらされる利便性や生産性向上とは裏腹に，IoT 時代を迎えるにあたっては，外部からの攻撃者に対するセキュリティを考えなければならない。

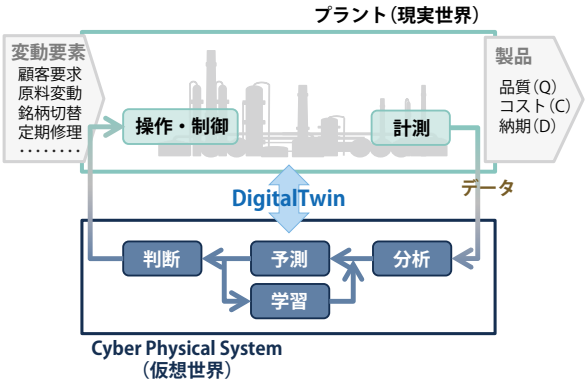

図 1　Cyber Physical System の活用による操業改善

プラントの制御システムのセキュリティは，単に情報システム技術（IT）をそのまま適用すべきではないと考えている。プラントの生産現場における制御システム（OT）には，プラント独自の特質がある。**表 1** に，IT と OT のセキュリティに関する項目の比較を示す。

*1 マーケティング本部 イノベーションセンター
インキュベーション部

表 1 情報システムと制御システムの比較

項目	情報システム（IT）	制御システム（OT）
セキュリティ最優先事項	データの流出を防ぐ **機密性**	生産性に影響を与えない **可用性**
セキュリティ事故での被害の大きさ	金銭的損失，プライバシー被害	人命損失，社会的甚大な被害
セキュリティの対象	情報	設備，装置，製品
攻撃者の進化に対する対策	防衛技術がすぐに陳腐化するため **スピード重視**	設備・装置が長期稼働するため **完全性重視**
システムの運用期間	5 年未満	20 年以上
セキュリティパッチの配布	随時，定期的	定修時に実施，不定期

素材やエネルギーを生産するプラントにおいては，プラントを停止し生産に影響を与えてはいけないため，可用性が重視される。また，プラントライフサイクルが 20 年以上と長いため，IT のように防衛技術がすぐに陳腐化することを前提とした対策は取れない。OT においては，セキュリティ対策は長期にわたって強固であることが求められる。

本稿では，制御システムに最適なセキュリティコンセプト「情報物理セキュリティ」について説明し，このコンセプトを具現化した持ち込み USB デバイスに対するセキュリティ対策として，「MemWiper」を紹介する。

2. 制御システムの 3 層モデルとセキュリティ施策

制御システムの典型的な構成例として，3 層モデルがある（**図 2**）。3 層モデルのシステムは，フィールドネットワーク・制御ネットワーク・制御情報ネットワークの 3 層のネットワークで構成され，制御情報ネットワーク上のルータを介して外部ネットワークと接続される。

外部の攻撃者からの制御システムへの攻撃経路として

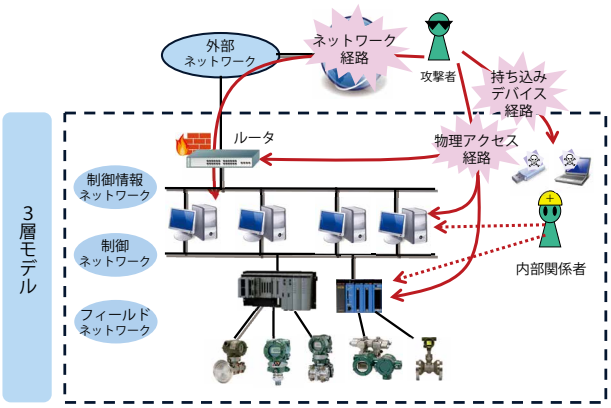

図 2 制御システムの 3 層モデルと主な攻撃経路

は，ネットワーク経路，持ち込みデバイス経路，物理アクセス経路の 3 つがある。ネットワーク経路は，外部のネットワークから制御システムに侵入する経路である。外部ネットワークと接続されていない制御システムでは，この経路は存在しない。持ち込みデバイス経路は，外部から制御システムに持ち込まれる USB メモリや PC などのデバイスを介して，制御システムに侵入する経路である。物理アクセス経路は，外部から制御システムの設置場所に物理的に侵入する経路である。

ネットワーク経路，持ち込みデバイス経路に対するセキュリティ施策としては，ネットワークセキュリティ施策やエンドポイントセキュリティ施策などの情報セキュリティ施策が用いられる。また，物理侵入経路攻撃へのセキュリティ施策としては，物理セキュリティ施策が用いられる（**図 3**）。

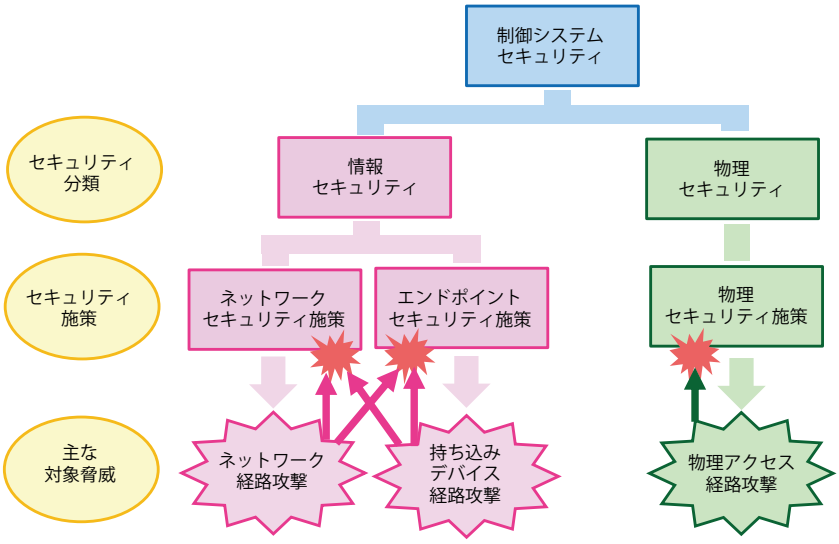

図 3 セキュリティ施策の分類と対象脅威

ネットワークセキュリティ施策は，保護対象ネットワーク（制御情報ネットワークなど）内に設置した装置によって，攻撃者による通信を検知･排除する施策であり，ファイアウォール・IDS（Intrusion Detection System）・IPS（Intrusion Protection System）などの装置が用いられる。エンドポイントセキュリティ施策は，保護対象装置（PC など）内のソフトウェアによって攻撃者によるアクセスを検知･排除する仕組みであり，ウイルス検知ソフト・ホストベースファイアウォール・ホワイトリスティングなどの施策がある。物理セキュリティ施策は，攻撃者による物理的な侵入を検知・排除する仕組みであり，入退出管理・施錠管理・物理侵入検知などの施策がある。

これらの施策の他にも，セキュリティポリシの策定や人的セキュリティ施策（セキュリティ担当者の配置，関係者に対する教育）などの管理施策なども行われている。

3. 現状のセキュリティ施策の問題点

前章で述べたネットワークセキュリティ施策やエンドポイントセキュリティ施策などの情報セキュリティ施策については，遠隔からの攻撃によってセキュリティ施策が無効化されるリスクが常に残存する問題がある [3]。

情報セキュリティ施策は，次の攻撃手段によって遠隔の攻撃者から無効化される恐れがある。

(1) 情報セキュリティ施策の脆弱性への攻撃
情報セキュリティ施策のために使用されるソフトウェア・ファームウェアなど（例えば，PC 上のウイルス対策ソフトや，ファイアウォール上のファームウェアなど）に脆弱性が発見された場合，遠隔からの攻撃によって情報セキュリティ施策が無効化される恐れがある。

(2) 管理インタフェースへの攻撃
情報セキュリティ施策の管理インタフェース・設定ファイル・アップデートファイルなどに脆弱性が発見された場合や，管理インタフェースの認証情報などが漏洩した場合，遠隔からの攻撃によって情報セキュリティ施策が無効化される恐れがある。

(3) 関連ソフトウェアの脆弱性への攻撃
情報セキュリティ施策自体に脆弱性が発見されなくても，情報セキュリティ施策と同時に使用している OS・ライブラリ・通信プロトコルなどに脆弱性が発見されれば，遠隔からの攻撃によって情報セキュリティ施策が無効化される恐れがある。

これらを悪用した遠隔からの攻撃リスクを低減するためのセキュリティ対策としては，多層防衛と即時パッチ適用などのセキュリティ強化施策が一般に行われている。

多層防衛は，複数種類のセキュリティ施策を多層に配置する施策である。多層防衛によって，攻撃リスクの低減が期待できるが，システムの構成要素が増えることにより，管理コストや脆弱性などのリスク要素が増えてしまう恐れがある。

即時パッチ適用は，脆弱性を修正するパッチが発行された場合に，可能な限り短時間に適用する施策である。即時パッチにより既知の脆弱性を標的にした攻撃への耐性向上が期待できるが，未知の脆弱性を悪用したゼロデイ攻撃への効果は期待できない。また，パッチ適用に際しては，システムを停止する必要が発生する場合もあるため，可用性が求められるシステムでは実施が困難な場合もある。

このように，現状のセキュリティ対策では，ネットワーク経路や持ち込みデバイス経路などを経由した遠隔攻撃からシステムを保護する一方で，セキュリティ対策自体が遠隔から攻撃を受けるリスク要因になるという問題がある。

また，遠隔からの攻撃を困難にする手段として，外部ネットワークからの隔離（Air gapping）が行われることもある。この手段は，遠隔からの攻撃経路を断つ強力な施策であるが，ネットワーク接続による利便性が犠牲になる。IoT 時代にはつながるリスクがある中，IoT によるメリットを安全に享受するためには，遠隔から攻撃できないセキュリティ施策の開発が望まれる。

4. 制御システムの新しいセキュリティコンセプト「情報物理セキュリティ」

情報セキュリティ施策が遠隔からの攻撃によって無効化される問題への対策として，セキュリティ施策の管理インタフェースを遠隔の攻撃者から物理的に隔離する「情報物理セキュリティ」コンセプトを提案する [4]。「情報物理セキュリティ」では，遠隔の攻撃者から操作・監視できない構造とした「情報物理セキュリティ施策」を用いて制御システムを保護する。

「情報物理セキュリティ施策」は，次のアプローチで実現する。

(1) ソフトウェアの隔離
セキュリティ施策として使用されているソフトウェア・ファームウェアへの攻撃対策として，遠隔の攻撃者からソフトウェアや設定が変更されることを防ぐ必要がある。そのため，セキュリティ施策のソフトウェアやセキュリティ設定の変更には設定対象機器への物理アクセスが必要な構造にする（例えば，ファームウェアの書き換えを許可・禁止する電気的なスイッチを設置するなど）。

(2) 管理インタフェースの隔離
セキュリティ施策として使用されている管理インタフェースへの攻撃対策として，遠隔の攻撃者からソフトウェアや設定が変更されることを防ぐ必要がある。そのため，セキュリティ施策のソフトウェアや設定の変更には，設定対象機器への物理アクセスが必要なインタフェース構造にする（例えば，無線 LAN の有効／無効を管理する際に，無線 LAN アダプタの電源を

制御する電気的なスイッチで有効／無効にするインタフェースを設置するなど)。

(3) 物理機構の使用

遠隔からの攻撃への対策として，セキュリティ施策の設定・操作には，ソフトウェアから操作できない物理的な仕組みや操作を組み合わせた構造にする（例えば，PC 内蔵カメラを有効／無効化する際に，カメラ前に物理的な覆いを設置するなど)。

これらのアプローチにより，「情報物理セキュリティ施策」のソフトウェアや設定を変更するためには物理アクセスが必要な状況になり，遠隔からの攻撃が困難になる。「情報物理セキュリティ施策」を遠隔からの攻撃経路であるネットワーク経路・持ち込みデバイス経路に適用することで，低い被攻撃リスク（物理攻撃経路）で高い攻撃リスク（ネットワーク経路・持ち込みデバイス経路）への対策が行える（**図 4**)。

このような「情報物理セキュリティ」のコンセプトを制御システムの製品・システム・サービス・運用の設計に取り入れることで，制御システムの情報セキュリティ問題を扱いやすい物理セキュリティ問題に転嫁して対策できる。

「情報物理セキュリティ施策」を外部からの攻撃経路に実装することで，遠隔からの攻撃に強い制御システムを実現し，IoT 時代のつながるシステムの安全の確保が期待できる。

5. 情報物理セキュリティ施策例 「MemWiper」

5.1「MemWiper」の背景と概要

「情報物理セキュリティ」の簡単な施策例として，USB メモリ消去装置「MemWiper」を試作した。制御システムの運用現場では，制御システム内の PC から日報データなどのファイルを持ち出したいという需要がある。このとき，USB メモリを用いると便利であるが，USB メモリがコンピュータウイルスなどのマルウェアに感染していると，接続先の PC に感染が拡大するリスクがある。

USB メモリから PC へのウイルス感染の対策としては，主にウイルス対策ソフトウェアが用いられている。ウイルス対策ソフトウェアでは，既知のウイルスの検知・除去は期待できるが，未知のウイルスへの感染リスクは除去できない。そのため，ウイルス感染を許容できないシステムでは，USB メモリの使用を禁止したり，USB メモリの代わりに CD-R などの記録型光学メディアを使用したりするなどの運用が行われている。これらの対策により，外部から PC へのウイルス感染リスクの除去が期待できるが，USB メモリを使用した場合と比較すると，利便性・所要時間などに難点がある。

USB メモリを用いた安全なデータ持ち出しを実現する手段として，「情報物理セキュリティ」コンセプトに基づいた対策装置「MemWiper」（**図 5**）を試作した。「MemWiper」は，USB メモリと PC の間に設置する小型の装置であり，USB メモリの内容を消去してから PC に接続することで，USB メモリから PC へのウイルス感染リスクを除去する（**図 6**)。

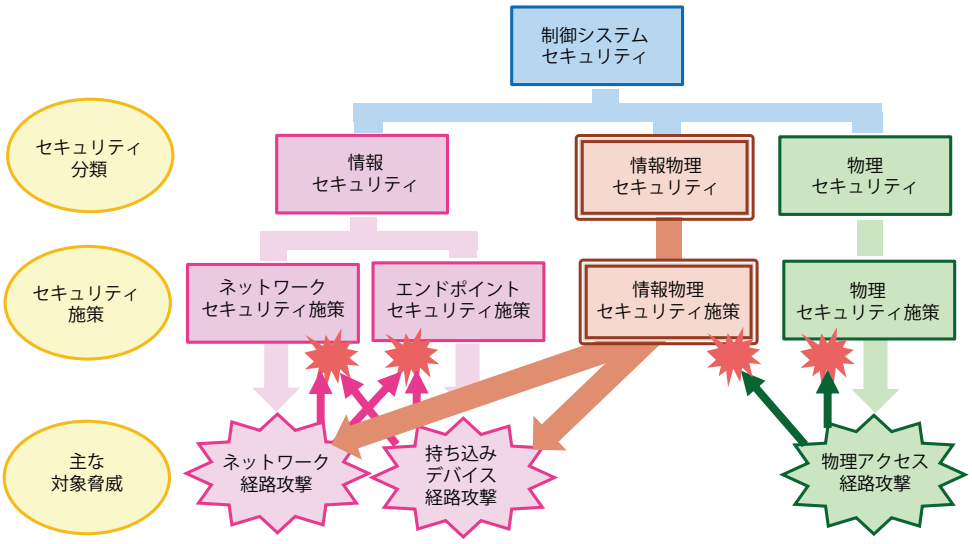

図 4 セキュリティ施策の分類と「情報物理セキュリティ」

図 5 USB メモリ消去装置「MemWiper」外観

5.2「MemWiper」の使用方法と動作

「MemWiper」は，「接続してボタンを押せば，内容が消去されて PC に接続される」という動作を行い，簡単に使用できる。具体的には，次の手順で使用する。

(1) 接続

ユーザは，「MemWiper」の「USB 差込口」に USB メモリを接続し，「MemWiper」の「USB プラグ」を PC に接続する。

すると，PC から「MemWiper」に電源が供給され，「MemWiper」内の「USB スイッチ IC」によって，USB メモリが「MemWiper」内の「消去用マイコン」に接続される。「消去用マイコン」は，USB メモリが正常であるかを確認し，正常であれば「状態表示ランプ」を点滅させて「ERASE ボタン」操作待ちの状態になる。

(2)「ERASE ボタン」操作

ユーザが「ERASE ボタン」を押すと，「消去用マイコン」によって USB メモリの内容が消去される。「消去用マイコン」は USB メモリの内容が消去されたかどうかを確認し，消去されていれば「USB スイッチ IC」によって USB メモリを PC に接続し，「状態表示ランプ」を連続点灯させる。PC は，USB メモリの接続を検知し，未フォーマットのデバイスとして認識する。

(3) フォーマット操作

ユーザは，PC 上で USB メモリのフォーマット操作を行う。

Windows などの OS では，標準機能によってフォーマットツールが自動的に起動するので，それを用いてフォーマット操作を行う。USB メモリのフォーマットは数秒で完了する。フォーマット後は，通常の USB メモリと同様にファイルの書き込みが可能になる。

(4) ファイルコピー

ユーザは PC を操作して，必要なファイルを USB メモリにコピーする。

(5) 取り外し

ユーザは PC 上で USB メモリの取り外し操作を行う。「MemWiper」の「状態表示ランプ」が消灯し，安全に取り外せる状態になる。

ユーザは「MemWiper」を PC から取り外し，USB メモリを「MemWiper」から取り外す。

5.3「MemWiper」と「情報物理セキュリティ」

「MemWiper」の設計にあたっては，「情報物理セキュリティ」のコンセプトに基づいて次の工夫を行った。

(1)「MemWiper」のソフトウェアは，内蔵マイコン内のファームウェアとして読み取りや変更ができない形で内蔵した。これにより，遠隔からのソフトウェアに対する攻撃を困難とした。

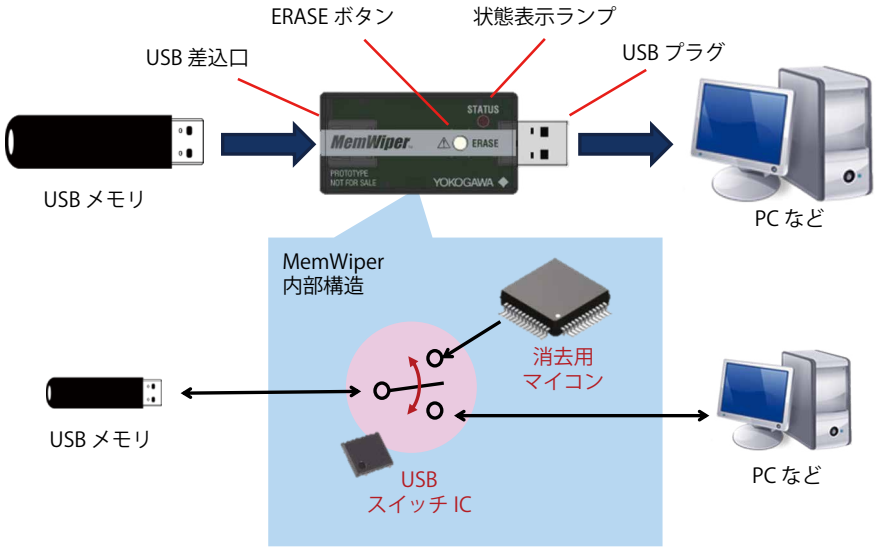

図 6「MemWiper」の内部構造と使用法

(2)「MemWiper」の動作は，物理的な接続と ERASE ボタンスイッチで管理する構造とした。これにより，遠隔からの操作を困難とした。
(3)「MemWiper」は，保護対象の PC から操作できない独立したハードウェアとして実装した。これにより，保護対象 PC 経由での遠隔攻撃を困難にした。

これらの工夫によって，「MemWiper」に対する遠隔からの攻撃が困難となり，攻撃のためには物理アクセスが必要になる。このような情報物理セキュリティ施策により，ウイルス感染対策という情報セキュリティの課題を，攻撃には物理アクセスが必要となる「MemWiper」という装置で対策できる。

5.4「MemWiper」についてのユーザからの意見

「MemWiper」の試作品について，制御システムユーザと制御システムセキュリティ関係者に対するヒアリングを実施し，次のような意見をいただいた。

- 単純で簡単に操作できる点が評価できる。
- 動作が明快でセキュリティ向上の効果が期待できる。
- MemWiper を外部からの作業者にも使わせたい。
- MemWiper を作業者全員に配布して使用することで，職場のセキュリティリテラシーの向上が期待できる。
- 新たな攻撃手法が発見されても，陳腐化しづらそうな点が良い。

これらの意見を見ると，情報物理セキュリティ施策の一例である MemWiper が，制御システムセキュリティ対策として有効であることが期待できる。

6. おわりに

IoT によるつながる利便性を安全に享受するためには，つながるリスクへのセキュリティ対策が必要不可欠である。

つながることにより，セキュリティ対策自体についても遠隔からの攻撃リスクが高まる。既存のセキュリティ施策は遠隔から攻撃される恐れのある管理インタフェースやアップデートなどの仕組みを持つものもあり，セキュリティ対策そのものが新しいリスク要素になる恐れもある。つながるシステムの安全を確保するためには，遠隔から攻撃されづらいセキュリティ施策の開発が望まれる。

本稿では，IoT 時代のセキュリティ対策として，「情報物理セキュリティ」コンセプトを紹介した。「情報物理セキュリティ」では，遠隔の攻撃者から攻撃しづらいように工夫した「情報物理セキュリティ施策」を用いることで，つながるシステムを遠隔攻撃から保護する。

「情報物理セキュリティ施策」の例として，USB メモリ消去装置「MemWiper」を試作した。「MemWiper」は遠隔から攻撃できないように工夫して設計された装置であり，「MemWiper」を用いることで，PC から USB メモリを用いて安全にファイルを持ち出すことができる。

「MemWiper」は現在商品化に向けて評価を行っている。試作品を広い分野のお客様に配布させていただき，様々な用途で評価していただきたいと考えている。評価にご参加いただける方はぜひご連絡いただきたい。

今後は，「情報物理セキュリティ」コンセプトに基づいた低価格で効果的な製品・サービスを開発・提供することで，IoT 時代の安心・安全を確保し，積極的なデータ活用による業務効率化の推進に寄与していきたい。

参考文献

(1) 仲矢実，“ サイバーフィジカルシステムのプラント操業への活用紹介と今後の展望 ”，分離技術，Vol. 48，No. 2，2018，p. 1-6
(2) 仲矢実，“ 製造プロセスにおける IoT，ICT 技術の活用 ”，技術情報協会，“ ミラープラントの予測技術によるオペレーション変革 ”，第 2 章 5 節
(3) Feng Xue, “Attacking Antivirus,” Black Hat 2008, http://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Whitepaper/bh-eu-08-xue-WP.pdf
(4) 新井貴之，“「情報物理セキュリティ」の考え方と対策ツール ”，計装，Vol. 61，No. 6，2018，p. 40-43