インフラの安心・安全な長期運用を支える制御システムセキュリティー技術

Cybersecurity Technologies Ensuring Safe, Secure, and Long-Term Operation of Control Systems for Infrastructure

春木　洋美 HARUKI Hiroyoshi　　小池　正修 KOIKE Masanobu　　内匠　真也 TAKUMI Shinya

近年，重要インフラの制御に用いられる制御システムは，ネットワーク化の進展により様々な脅威にさらされており，増大するサイバー攻撃に対する，制御システムの防御が課題になっている。長期運用を前提とした制御システムに対しては，設計・開発時だけでなく，運用開始後にもセキュリティー対策をすることが重要になる。

東芝グループは，運用時のセキュリティー対策として，あらかじめ登録された許可済みのアプリケーションの一覧を確認することにより，未知のマルウェアからシステムを守るホワイトリスト型の実行制御技術WhiteEgret™と，攻撃された場合にも影響範囲を局所化できるグループ鍵を効率的かつ安全に配布・更新するためのグループ鍵管理技術の研究開発に取り組んでいる。

In line with the ongoing progress of information networking, control systems for critical infrastructure are facing various types of security threats. In particular, demand has arisen for the protection of such systems against increasing cyberattacks. To realize stable long-term operation, it is necessary to continuously apply the latest countermeasures against cyberattacks after the commencement of commercial operation, as well as to implement security countermeasures in the product design and development phases.

The Toshiba Group has been promoting research and development of the following cybersecurity technologies for control systems in operation: (1) a whitelisting execution control technology called WhiteEgret™ that can protect the systems against unknown malwares by checking a list of allowed applications registered in advance , and (2) a group key management technology that can efficiently and securely provide and update a group key to localize the area targeted in a cyberattack.

1. まえがき

電力システムや化学プラントなどの重要インフラの制御に用いられる制御システムは，数多くの制御機器などで構成され，それらの機器は，ネットワークで接続されて連携動作する。一方で，近年，制御システムを対象としたサイバー攻撃が増大しており，例えば，核燃料施設を対象としたStuxnetや電力システムを対象としたBlackEnergyなどが，制御システムを対象としたマルウェアとして知られている[(1)]。このような攻撃では，インターネット経由だけでなく，USB（Universal Serial Bus）メモリーや，不正端末を制御システム内に接続するといった内部犯行などによる攻撃も起きている。そのため，インターネットに接続されていない場合でも，悪意のある攻撃者を想定した，制御システムへのセキュリティー対策が重要である。

制御システムへのセキュリティー対策の一例として，情報システムで利用されてきたセキュリティー対策技術の導入が考えられる。これは，多くの場合に有用であるが，20年を超える長期間の利用や，システムの停止・再起動時のコストの大きさなど，制御システムでの制約条件が情報システムとは異なり，別のセキュリティー対策が必要となる場合がある。そのため，制御システムの要件に基づいて情報システムのセキュリティー対策技術を導入するか，別の対策を行うかを決定しなければならない。

ここでは，制御システムのセキュリティー対策に求められる前提条件や要件を明確にするとともに，その課題を解決する制御システムセキュリティー技術について述べる。

2. 制御システムセキュリティーに求められる要件

一般に，制御システムは，20年以上使われることが多い（要件(A)）。このような長期間にわたって動作するシステムでは，設計・開発時にセキュリティー対策技術を適用するだけでは，適用したセキュリティー対策技術が危殆（きたい）化するおそれが高いなど，十分とは言えない。そのため，制御システムに対しては，設計・開発時だけでなく，運用時にも対応可能なセキュリティー対策が必要となる。

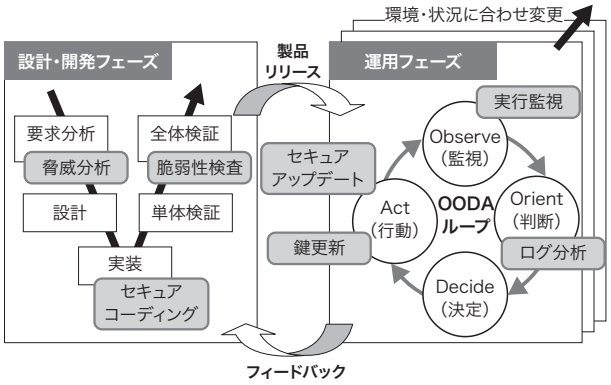

図1. セキュア運用のためのOODAループ

システム設計・開発時のV字モデルに合わせたセキュリティー対策技術の導入に加え，運用開始後には，OODAループを適用し，常時システムの監視・分析・対策を実施することが重要である。

Observe-orient-decide-act (OODA) loop for secure operation of control system

システムの設計・開発時から運用時までのセキュリティーライフサイクルを，**図1**に示す。設計・開発時には，一般的なシステム開発のV字モデルに合わせ，様々なセキュリティー対策技術を導入する。例えば，要求分析時にはセキュリティー対策が必要な部分を抽出し（脅威分析），実装時には抽出した対象のコーディングを適切に行い（セキュアコーディング），検証時にはシステムにセキュリティー上の問題がないかを確認すること（脆弱（ぜいじゃく）性検査）が考えられる。

一方，運用開始後には，OODA（Observe-Orient-Decide-Act）ループを適用し，常時システムの監視・分析・対策を実施する。例えば，セキュリティー上の問題が発生していないかを常時監視し（Observe），監視で得られた情報から状況を判断し（Orient），セキュリティー上の問題がある場合にどう対策するかを決定し（Decide），それを実行する（Act）といった一連の活動を繰り返し適用する。そのためには，常時監視するためのプログラム実行監視や，ネットワーク上のデータ監視，それらから得られた各種ログを分析してシステム内の状況を把握するためのログ分析などのセキュリティー技術による対策が考えられる。また，OODAループを長期間適用するために，環境や状況に合わせてこれらの方式を改善していくことも求められる。更に，OODAループで得られた知見を設計・開発にフィードバックすることで，将来システムのセキュリティー強化につなげることもできる。

制御システムでは，長期間利用という前述の要件(A)以外に，下記のような要件（特徴）を有する場合もあり，セキュリティー対策技術の適用には注意が必要である。

(B) リアルタイム処理の要求がある　　システムによっては，数百μsなどでのリアルタイム処理を要求される場合があるため，それを阻害するセキュリティー対策技術は利用できない。

(C) インターネットに接続できるとは限らない　　情報システムは，インターネットに常時接続されることが多いが，制御システムでは，運用に支障を来さないようにインターネット接続を制限する場合があるので，これを前提とするセキュリティー対策技術は利用できない。

(D) システムごとにアプリケーションやデータの種別が異なる　　情報システムでは，定番のアプリケーションやHTTP（Hypertext Transfer Protocol）などのデータ種別が利用されるが，制御システムでは，個別のアプリケーションや分野ごとに異なるデータ種別（BACnetやOPC-UA（OLE（Object Linking and Embedding）for Process Control-Unified Architecture）など）が利用される。そこで，特定のシステムやアーキテクチャーに依存せずに，システムに適合可能なセキュリティー対策技術が要求される。

(E) システム全体の再起動を極力しない　　全体の起動時間が数分から数時間を要する場合があることから，システム全体の再起動を要求するセキュリティー対策技術は利用できない。

(F) 運用開始後には変更される頻度が低い　　情報システムでは，様々なアプリケーションをインストールすることが多いが，制御システムでは，運用開始後にアプリケーションをインストールするなどの変更頻度は低い。

3. ホワイトリスト型実行制御技術 WhiteEgret™

悪意のプログラムを検出する方法としては，**図2**に示すように，ブラックリスト方式とホワイトリスト方式の二つの実行制御方式が知られている。ブラックリスト方式は，パターンファイルに基づいて悪意のあるプログラムを検出する方式であるが，パターンファイルと呼ばれるデータを定期的に更新しなければならないことや，定期的なチェックに相当な負荷が掛かることから，制御システムには適していない。一方で，ホワイトリスト方式は，あらかじめ実行許可するプログラムを登録する方式であり，2章で述べた制御システムの要件

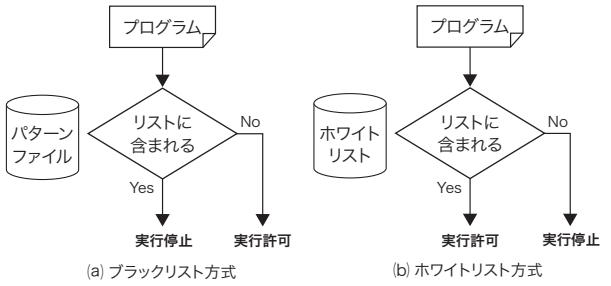

図2. マルウェアの検出方法

悪意のプログラム(マルウェア)を検出する方法には，ブラックリスト方式とホワイトリスト方式の2種類の実行制御方式がある。

Malware detection mechanisms in case of blacklisting and whitelisting software

(B)，(C)，(F)に適合している。

東芝グループは，Linux®搭載の制御システムが増えることを想定し，Linux®上で動作するホワイトリスト型実行制御技術WhiteEgret™を開発している[2]。WhiteEgret™は，制御システムの特徴に合わせて，以下の実装を行っている。

(1) Linux®標準機能だけを利用　Intel®製のCPUだけでなく，様々なアーキテクチャーでの利用を想定し，LSM(Linux Security Modules)を利用(要件(D))

(2) 多くの機能をユーザー空間で実現　カーネル空間への実装では，変更時にシステムの再起動を要することから，ホワイトリスト管理などの処理をユーザー空間で実装(要件(E))

WhiteEgret™が導入された制御機器の動作イメージを，**図3**に示す。WhiteEgret™では，プログラムのパス名と，プログラムの改変を検出するためのハッシュ値を利用する。この制御機器は，実行の制御を行うWhiteEgret™ for Kernel，制御プログラム，及び事前に準備したホワイトリスト(動作を許可するプログラムのパス名とハッシュ値の一覧)で構成される。実行ファイルの起動要求から，カーネル空間のシステムコール処理を呼び出すと，WhiteEgret™ for Kernelがその処理をフックし，制御プログラムに確認要求を行う。制御プログラムは，確認要求されたプログラムのハッシュ値を算出し，ホワイトリストに格納されたハッシュ値と一致するかを確認し，確認結果を通知する。WhiteEgret™ for Kernelは，通知された結果に基づいて，プログラムの起動可否を決定する。具体的には，パス名，ハッシュ値が一致した場合には起動を許可し，それ以外の場合には起動を不可とする。

制御システムの要件(A)を満たしているかを確認するため，Intel®製CPU及びARM®製CPUで簡易プログラムを10回

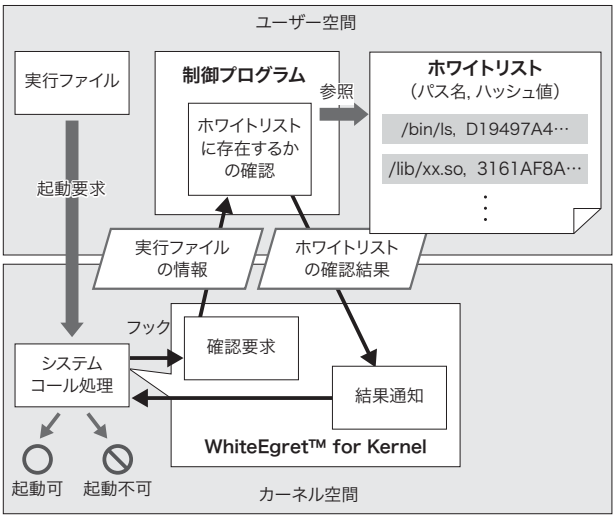

図3. WhiteEgret™が実装された制御機器の動作イメージ

WhiteEgret™ for Kernelが処理をフックし，制御プログラムがホワイトリスト内を確認することで，実行プログラム起動の可否を決定する。

Outline of implementation of WhiteEgret™

起動し，各実行時間により，開発技術によるアプリケーション実行への影響を評価した。その結果，WhiteEgret™を利用した場合は，初回起動時にハッシュ計算処理によって数ms以上の負荷が掛かるが，2回目以降は，通常実行した場合とほぼ同等の1 ms以下の負荷にとどまることを確認した。

また，これらの機能だけでなく，Java®などのスクリプトファイルの実行制御を行うための，ファイル読み込み制御機能の開発や，制御プログラムのセキュリティー強化のための取り組みなども進めている。更に，制御機器や組み込み機器などへの幅広い活用を期待し，Linux®カーネルへの標準搭載を目指した活動も実施している。

4. グループ鍵管理技術

制御システムでは，複数の機器に同一の情報を渡すために，マルチキャスト通信と呼ばれる通信方式が利用される。一方，制御システムの要件(A)(長期間の安全稼働)に対しては，攻撃者に侵入された場合にも影響範囲を局所化することが求められる。その対策としては，侵入された機器をほかの機器から切り離す方法が考えられる。その手法の一つとして，複数の機器で同一の鍵であるグループ鍵を共有し，ある機器が侵入された場合にはグループ鍵を更新することで安全性を維持する，グループ鍵管理方式がある。

東芝グループは，**図4**に示すように，膨大な数の制御機器に対しても，効率的かつ安全にグループ鍵の配布・更新

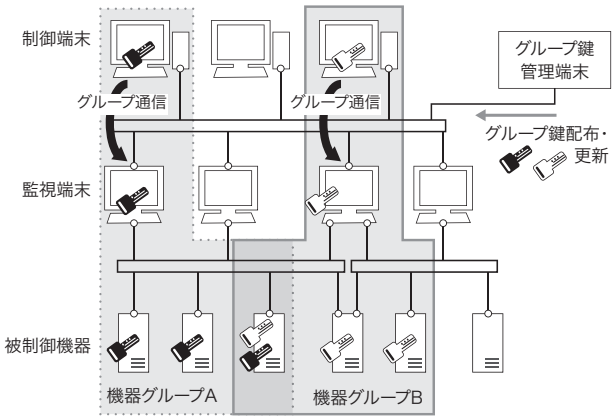

図4. グループ鍵管理技術を適用した制御システム
グループ鍵管理技術を適用することで，任意の機器グループが構成できるとともに，グループ鍵の配布に要する平均通信量を削減できる。

Control system operating in conjunction with multiple devices applying group key management

を行うグループ鍵管理技術を開発している。この技術の特長は，著作権保護などで用いられる技術を適用することによって，通常は機器数に比例した数のグループ鍵を配布・更新する際に必要なシステムへの負荷を軽減できる，鍵管理方式を採用している点にある[3]。

この方式では，各ノードにノード鍵が割り当てられた完全二分木を用いる。また，各制御機器にある葉ノードから根ノードまでの経路上のノードに，割り当てられた全てのノード鍵を持たせる。このとき，各制御機器が一部重複して持つノード鍵を利用してグループ鍵を配布することで，任意の機器グループの構成を実現しながらも，配布に要する平均通信量を削減できる。また，ある制御機器からノード鍵が漏えいしても，漏えいしたノード鍵を用いずに，各グループのグループ鍵を再配布して更新することで，システムを安全に保つことができる。

更に，異なるベンダーが製造する制御機器の相互接続性を確保するために，IEEE® 802委員会（電気電子技術者協会 802委員会）やエコーネットコンソーシアムにおいて，標準化活動に積極的に取り組んでいる。東芝グループが開発したグループ鍵管理技術は，マルチキャスト通信のセキュリティー規格を定めたIEEE 802.21-2017や，HEMS（Home Energy Management System）などの特定ユースケース専用機能を定めたIEEE 802.21.1-2017に採用された。現在，IEEE 802.21-2017と関連規格のISO/IEC JTC1/SC6（国際標準化機構／国際電気標準会議 第一合同技術委員会／サブコミッティー 6）における規格化を進めている。

5. あとがき

増大する制御システムを，サイバー攻撃から守るための制御システムセキュリティー技術について述べた。

制御システムの前提条件である長期間利用に対応するには，運用前のセキュリティー対策に加え，運用開始後のセキュリティー対応が重要である。今後も，ここで述べたホワイトリスト型実行制御技術や，グループ鍵管理技術，機器から得られるログデータの分析技術など，OODAループを実現するための取り組みを進めていく。

文　献

(1) 宮地利雄．“制御システム・セキュリティの現在と展望 ～ この1年間を振り返って ～”．制御システムセキュリティカンファレンス 2018．東京，2018-02，JPCERTコーディネーションセンター．2018．
(2) 小池正修，ほか．“Linux上でのホワイトリスト型実行制御機能WhiteEgretの開発”．コンピュータセキュリティシンポジウム（CSS）2017．山形，2017-10，情報処理学会 コンピュータセキュリティ研究会．2017，3D3-4．
(3) 花谷嘉一，ほか．M2M通信システム向けグループ鍵管理技術．東芝レビュー．2014，69，1，p.14–17．

春木　洋美　HARUKI Hiroyoshi
研究開発本部 研究開発センター
研究企画部
情報処理学会会員
Research Planning Dept.

小池　正修　KOIKE Masanobu, Ph.D.
東芝デジタルソリューションズ（株）
インダストリアル ICT セキュリティセンター セキュリティ運用推進部
博士（工学）　情報処理学会会員
Toshiba Digital Solutions Corp.

内匠　真也　TAKUMI Shinya
研究開発本部 研究開発センター
コンピュータアーキテクチャ・セキュリティラボラトリー
OS研究会・情報処理学会会員
Computer Architecture & Security Systems Lab.