Vol.2017-DPS-170 No.35
Vol.2017-CSEC-76 No.35
2017/3/3

# 管理端末に感染したマルウェアによる制御プログラムの改ざん検知について

岩崎亜衣子[†1]　榊原裕之[†1]　河内清人[†1]

**概要**：近年，制御システムへのサイバー攻撃が増加し問題となっている．イラン核開発設備に対して行われたサイバー攻撃であるスタックスネットでは，制御プログラムを改ざんすることで制御システムをダウンさせ，稼動停止に陥らせたと言われている．本稿では，マルウェアによる不正な改ざんで，制御プログラムが不正な挙動をするように機能を追加される，または必要な機能が削除されるといった変更が行われると仮定し，管理端末に感染したマルウェアによる更新プログラムの改ざんを，更新プログラムの変更内容の異常度合いに基づき検知する方法について検討を行った．

**キーワード**：スタックスネット，サイバー攻撃

# Detection of control program tampering by a malware infected on a management terminal

AIKO IWASAKI[†1]　HIROYUKI SAKAKIBARA[†1]
KIYOTO KAWAUCHI[†1]

***Abstract***: In recent years, cyber attacks on control systems have increased and become a problem. In the Stuxnet which is a cyber attack against the Iran nuclear development facility, it is said that the control system was downed by tampering with the control program and caused the operation to stop. In this paper, we assume that the on a control program mal-functions are added or some functions are deleted or modified to make illegal behaviors by malware, we propose a method of detecting tampering with a control program update based on the degree of abnormality of an update contents.

***Keywords***: Stuxnet, Cyber Attack

## 1. はじめに

近年，発電プラントなどの制御システムへのサイバー攻撃によって機能不全のリスクが高まっており，制御システムへのサイバー攻撃の対策技術が注目されている．イラン核開発設備に対して行われたサイバー攻撃であるスタックスネットでは，遠心分離機の制御を行う制御機器の更新プログラムを改ざんすることで遠心分離機の回転数異常をおこし，制御システムをダウンさせ稼動停止に陥らせたと言われている．従来の制御システムに対する攻撃対策技術の，感染経路となりうる通信を制限したり，マルウェアの実行を制限したりする対策では，一度端末がマルウェアに感染してしまうと，その後の活動を検知できない．ホワイトリストスイッチのように，ホワイトリストを用いて制御ネットワーク内の通信を監視するネットワークスイッチでは，感染後の活動を検知できるが，ホワイトリストの精度に依存する特徴があり，また，例えば保守作業など正常と定めた作業範囲でマルウェアが活動を行うと，検知できない．

本稿では，スタックスネットのようなマルウェアが，保守作業中に活動し制御機器の更新プログラムを不正に書き換えた場合に検知する方法を示す．本方式では，制御機器の更新プログラムが，マルウェアによる不正な改ざんにより，不正な動作をする機能を追加される，または必要な機能が削除されるといった変更が行われことで，多くのプログラムコードが書き換えられるという仮定を置く．この仮定に基づき，制御機器の管理端末に感染したマルウェアによる更新プログラムの改ざんを，プログラムの変更量や範囲の異常度合いをランク付けすることで検知する．本稿は以下の構成である．2 章では，背景となる制御システムへのサイバー攻撃と，その対策について概説する．3 章では，従来の対策技術の課題と，不正改ざんの検知について触れる．4 章では，従来技術の課題への対策として検討した不正な改ざんの検知方法について概説する．5 章でその効果について考察し，6 章でまとめる．

## 2. 制御システムへのサイバー攻撃と対策

従来の制御システムは，高信頼性やリアルタイム性，耐環境性などの観点から，オフィスなどで用いられる情報システムとは異なり，独自仕様のハードウェア，ネットワー

†1 三菱電機株式会社,神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501 Japan

Vol.2017-DPS-170 No.35
Vol.2017-CSEC-76 No.35
2017/3/3

クで運用され，外部ネットワークに接続しない閉鎖的な環境下にあった．しかし近年では，利便性の向上や生産性の効率化のために，汎用 OS や標準プロトコルが使用されるようになった．情報システムと物理的に隔離されている場合でも，制御システムと情報システム間のデータ交換に USB 媒体などを利用することがあるため，USB 媒体を経由してマルウェアが感染し，窃取したデータからさらに強力な攻撃を行う事例が発生しており，制御システムも情報システムと同様にサイバー攻撃による脅威に晒され，機能不全となるリスクが高まっている．

本章では，近年の制御システムへのサイバー攻撃の事例や，攻撃に使われたマルウェアについて述べる．

### 2.1 制御システムへのサイバー攻撃

近年，制御システムへのサイバー攻撃が増加している．攻撃の影響が大きい発電所などが標的とされることが多く，2010 年のイラン核処理施設に対する攻撃では，核施設における遠心分離機が，スタックスネットと呼ばれるマルウェアによって回転数異常になり破壊され，施設が一部停止した．2015 年にはサイバー攻撃によってウクライナで大規模な停電が発生した．また 2005 年にはアメリカで，13 の自動車工場への攻撃によって 50 分間操業停止となり，被害総額は約 1400 万ドルとなった事例もある．

制御システムを狙ったサイバー攻撃で用いられたマルウェアを以下に紹介する．

(1) Stuxnet（スタックスネット）

スタックスネットは，制御システムを標的とした初のマルウェアだと言われており，2010 年にイラン核開発設備に対して行われたサイバー攻撃によってその存在が明らかになった[1] [2]．複数の Windows と SCADA[1]ソフトウエアの脆弱性を利用してサーバを乗っ取り，遠心分離機を操作する PLC[2]のラダープログラムを書き換え，遠心分離機の周波数を仕様で規定している以上に設定したり，急激に変動させたりすることで遠心分離機を破壊した．この攻撃では，まず USB などの外部媒体を経由して保守ツールに感染し，保守員のプログラム書き換え操作をフックして不正な更新プログラムに差し替える．この時，保守ツールに対しては正常な制御プログラムを書き込んだかのように偽装する．

(2) DragonFly

DragonFly は，水飲み場攻撃や標的型メール，制御系ソフトウエアのアップデートにウイルスを混入して感染する[3]．OPS[3]の情報を収集する機能や，OPC[4]/SCADA S/W と関係するポートを開いているホストをスキャンする機能で主にエネルギー業界のスパイ活動を行っている．この攻撃では，まず情報ネットワークを経由して監視制御装置にマルウェアを感染させる．感染したマルウェアは各種情報を取得し，外部の不正者に送信する．

(3) Black Energy

Black Energy は，2007 年に確認されて以降進化を重ねているウイルスで，標的型攻撃によって感染する[4][5]．監視制御に使われる HMI[5] 製品を標的としており，インターネットにアクセスできる構成や運用の組織が狙われている．マクロ付ドキュメントを用いての攻撃が行われた．

(4) Flame

スタックスネットと同様の技術を使ってコンピュータに感染し，インターネット上でスパイ活動を行う[6][7]．端末に表示された内容から，標的に関する様々な情報を窃取する．

### 2.2 攻撃検知技術

制御システムへのサイバー攻撃の増加を背景に，攻撃検知・対策技術が研究開発され，導入され始めている．本節では，制御システムへのサイバー攻撃対策の例について述べる．

- データダイオード
  データダイオードは，外部ネットワークからの侵入を，通信を一方向のみに物理的に制限することで防ぐ装置である[8]．外部ネットワークからのマルウェアの侵入を防ぐことはできるが，USB などの媒体を利用した感染は防ぐことができない．
- アンチウイルス
  アンチウイルスは，あらかじめ定義したウイルスのルールによってマルウェアを検知・除去する．計算機にインストールしてマルウェアの実行を防止するプログラムである．定義されていないマルウェアを検知することはできない．
- ロックダウン
  ロックダウンは，あらかじめ定義したプログラム以外のプログラム実行を抑制する．計算機にインストールしてマルウェアの実行を防止するプログラムである[9]．既知，未知問わず攻撃を検知できる．
- ホワイトリストスイッチ
  ホワイトリストスイッチは，制御ネットワーク内の通信を監視するネットワークスイッチである[10]．通信

1 Supervisory Control And Data Acquisition　産業用制御システムの 1 つであり，計算機によりシステム監視とプロセス制御を行う．
2 Programmable Logic Controller　工場などの自動機械の制御に使われる制御装置
3 OPerators Station　運転操作用端末．
4 OLE for Process Control プロセス制御において，異なる製造元の各種制御機器間においてリアルタイムでデータ通信を行うための標準規格．
5 Human Machine Interface　人間と機械が情報をやり取りするための手段や，そのための装置やソフトウエアなどの総称

Vol.2017-DPS-170 No.35
Vol.2017-CSEC-76 No.35
2017/3/3

する装置の IP アドレス・ポート番号をあらかじめ定義し，それ以外の通信が発生したらアラートを出力する．感染後のマルウェアによるポートスキャンなどの活動を検知できる．

## 3. 従来技術の課題と目的

### 3.1 従来方式の課題

従来の制御システムへの攻撃検知技術は，感染の経路となりうる通信を制限したり，マルウェアの実行を制限したりする対策が多い．しかし，一度感染を許してしまうと，それ以降の対策が困難である．ホワイトリストスイッチでは，ポートスキャン等の単純な探索活動を検知可能な場合もある．しかし，あらかじめ定義した正常状態のパターンからの逸脱で攻撃を検知するホワイトリスト方式は，ホワイトリストが適切でない場合，誤検知が多くなってしまう課題がある．また，正常と定めた範囲で攻撃が成立してしまう場合は，検知できない．例えばスタックスネット攻撃のように，管理端末などにマルウェアが感染し，管理端末を従業員が操作している間に更新プログラムなどの改ざんが行う場合，正規の操作に成りすましての不正な更新であるため，正規の操作と区別がつかず攻撃として検知できない．また，保守の活動をホワイトリストでは無く，ログ分析などを用いることで検知する場合でも，保守の作業として制御プログラムの更新処理を行っている最中にマルウェアが介入し，活動することがあるため，正規の操作と区別がつかず検知できない．

### 3.2 不正改ざん検知

このような保守活動中の，不正な書き換えを行う攻撃への対策として，いくつかの方法が考えられる．

① プログラムの比較

管理端末上に存在する，保守員が制御機器へ書き込んだ更新プログラムと，実際に制御機器上の書き込まれた更新プログラムを比較する方法が考えられる．比較して一致しなければ，マルウェアによって更新プログラムが改ざんされたと判断できる．しかし，管理端末自体がマルウェアに感染していた場合，管理端末上に存在する更新プログラムが制御機器に対する更新前に既に書き換えられている可能性がある．この場合，管理端末上と制御機器上の両方の更新プログラムが改ざんされているため，比較しても一致してしまい，不正な書き換えを検知できない．

これに対し，更新プログラムを管理端末とは別の端末に保持しておき，比較する手法も考えられる．この場合，管理端末がマルウェアに感染していても，別の端末が感染していなければ更新プログラムが改ざんされることは無いため，不正な書き換えを検知できる．しかし，更新のたびに別端末にも保存する必要があり，またこの別端末への保存を安全に行う必要がある．

② 仮想制御システムでの実行

制御ネットワーク内に仮想の制御システムを構築し，更新プログラムが書き込まれる前に，仮想の制御システムで更新を実行し，正しく動作するか確認する方法が考えられる．しかし，この方法では，大規模な制御システムを対象とする場合，仮想の制御システムを構築することが難しく，また，構成の変更などの保守や工事の作業を仮想の制御システムにも反映させる必要があり，手間がかかる．

## 4. 提案方式

そこで本稿では，以上のような背景を踏まえ，管理端末がマルウェアに感染していても，また，制御システムの構成の変更に大きく影響されずに，マルウェアによる更新プログラムの不正な書き換えを検知する方式を提案する．本章では，管理端末等がマルウェアに感染し，更新プログラムがマルウェアによって書き換えられたことを検知する方式について述べる．本方式は，更新プログラムがマルウェアによって書き換えられた場合，更新プログラムの差し替えや不正な挙動を起こすための機能の追加，または正常な動作ができなくなるような機能の削除などにより，多くのプログラムコードが書き換えられている可能性を仮定している．

### 4.1 方式の概要

不正な書き換えを検知する処理は制御システム内の図 1 のような環境で行われる．本提案方式の処理は，制御システムの保守ネットワーク上にあるパケットキャプチャ等の機器から通信データを収集し，収集した通信データから更新プログラムを抽出し，ネットワーク上を流れてきた更新プログラムと，現在制御に用いられている現行プログラムとの差分をとり，その差分（変更）の範囲が正常かどうかを判定する．

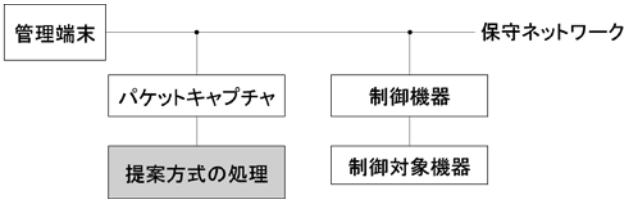


図 1　提案方式の処理環境

Vol.2017-DPS-170 No.35
Vol.2017-CSEC-76 No.35
2017/3/3

### 4.2 処理の構成

次に本検知方式を構成する処理について述べる．処理のフローを図 2 に示す．

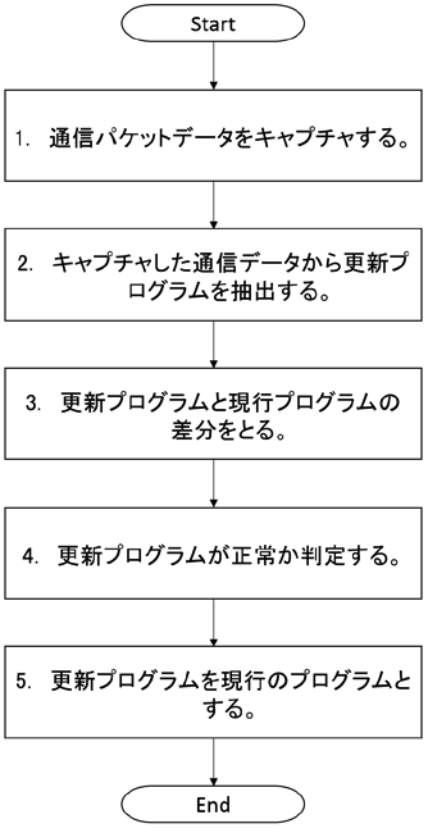


図 2　処理のフロー図

1. 管理端末から制御機器へと送られる通信パケットデータを，パケットキャプチャ等で収集する．
2. 1 で収集したデータを受信し，通信データに更新プログラムが含まれている場合，通信データから更新プログラムを抽出する．
3. 現在制御に使用している現行のプログラムと 2 で抽出した更新プログラムを比較し，差分を取る．
4. 3 で求めた差分が正常の範囲かを，あらかじめ定めた閾値によってランク付けし，更新プログラムが正常かを求める．
5. 4 の結果が正常だった場合，2 で構築された更新プログラムを現行プログラムとする．

### 4.3 判定方式

図 2 の 3，4 番目の処理にあたる，正常の範囲かどうかの判定例を図 3 を用いて説明する．

① 現行プログラムと，抽出した更新プログラムとの差分を取る．

② 差分から，更新プログラムによってどの程度変更が加えられるかを求める．例えば，差分を取ったときに，削除されている行数を a，追加されている行数を b，パラメータが変更されている行数を c とすると，それらの合計が現行プログラムコードの総行数の何割にあたるか（(a+b+c) /現行プログラム行数）を計算する．

③ パラメータが変更されている箇所においては，そのパラメータ値の変化についても差分を取り，どの程度変更が加えられるかを求める．例えば，パラメータ値が X から Y に Δ=Y-X 増加していたとき，その Δ は設定可能なパラメータ値の最大値（MAX）と最小値（MIN）の範囲の何割にあたるか（|Δ|/|MAX-MIN|）を計算する．

④ ②, ③で求めた割合を，閾値を元にランク付けを行い，不正な書き換えか，正常な書き換えかを判定する．例えば総プログラムコード行数の 9 割を超えた変更がなされていれば改ざんされた可能性が極めて高い，などである．表 1 に簡単なランク付けの例を示す．このランク（ここでは正常度：高低で示している）が判定結果となり，出力される．

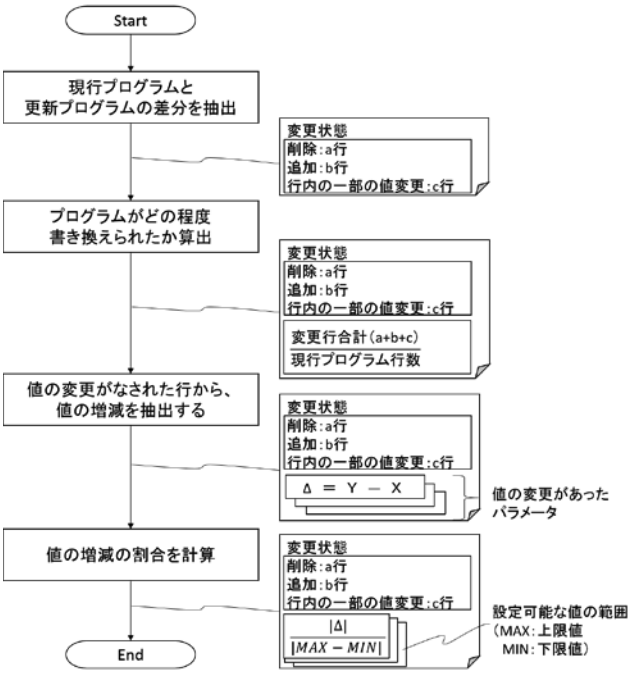


図 3　判定方式③

表 1　ランク付け例

| | 変更行：少 | 変更行：多 |
|---|---|---|
| 値の変更：小 | 正常度：高 | 正常度：低 |
| 値の変更：大 | 正常度：低 | |

Vol.2017-DPS-170 No.35
Vol.2017-CSEC-76 No.35
2017/3/3

## 5. 考察

4.3 で示した方式について，効果を考察する．

### 5.1 効果の考察

本方式を用いることで，保守員が保守の作業として制御プログラムの更新を行っている最中であっても，マルウェアによって更新プログラムの多くの行または大幅にパラメータを不正に書き換えられた場合に検知できる．当方式により検知した場合は，速やかに保守員に連絡することで，不正な更新プログラムにより制御が行われことを防止できる．また，端末上からデータを収集するのではなく，ネットワーク上を流れる通信データから更新プログラムを抽出し，比較することにより，管理端末が侵害されていてもその影響を直接受けることは無い．また，既存のパケットキャプチャ等を活用することで通信データを収集できるため，制御システムの構成を変更する必要がない．

### 5.2 今後の課題

一方で，以下の項目についても検討を行い，適切に判定できるように決める必要がある．これらの決定方法については，実際の運用環境などを参考に決定する必要がある．

- プログラムコードの変更量，範囲（割合）の閾値
- 値の変更量，範囲（割合）の閾値
- ランク付けのための閾値

また，攻撃者が対象となる制御システムに精通していた場合に少ない変更で改ざんを行うこともあるため，閾値を決める際に考慮する必要がある．

## 6. まとめ

本稿では，マルウェアよって更新プログラムを書き換えられ，制御システムが不正な挙動を起こすことを防ぐために，マルウェアによる不正な更新プログラムの書き換えを，そのプログラムコードの変更量によって判定する方式について考察を行った．本方式を用いることで，管理端末が感染し，更新のための作業中であっても，不正な書き換えを検知できると考える．実際に検知を行うためには，プログラムコードの変更範囲の判定や，ランクの付け方を適切に決める必要があり，実際の運用環境に関するデータによって，決定する必要がある．また，その際，攻撃者が対象となる制御システムに精通していた場合少ない変更で改ざんを行うことも考慮して検討する必要がある．

## 参考文献

[1] トレンドマイクロ．“「STUXNET」ファミリが SCADA システムを狙う！” (オンライン) (引用日: 2017 年 1 月 27 日.) http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=STUXNET+Malware+Targets+SCADA+Systems.

[2] Symantec. “W32.Stuxnet Dossier Version 1.4.” (オンライン) (引用日: 2017 年 1 月 27 日.) https://www.symantec.com/content/en/

[3] シマンテック．“Dragonfly: エネルギー業界のサイバースパイ” (オンライン) (引用日: 2017 年 1 月 27 日.) https://www.symantec.com/ja/jp/outbreak/?id=dragonfly.

[4] カスペルスキー．“APT グループ「BlackEnergy」の新たなスピア型フィッシング攻撃を確認 ～ウクライナの組織が標的に” (オンライン) (引用日: 2017 年 1 月 27 日.) https://blog.kaspersky.co.jp/black-energy/10363/

[5] カスペルスキー．“破壊活動集団「BlackEnergy」が攻撃を拡大” (オンライン) (引用日: 2017 年 1 月 27 日.) https://www.kaspersky.co.jp/about/news/virus/2016/vir22022016

[6] カスペルスキー．“Flame” (オンライン) (引用日: 2017 年 1 月 27 日.) http://www.kaspersky.co.jp/flame

[7] Naked Security. “Flame malware – more details of targeted cyber attack in Middle East“ (オンライン) (引用日: 2017 年 1 月 27 日.) https://nakedsecurity.sophos.com/2012/05/28/flame-malware-cyber-attack/

[8] 株式会社 東芝．“データダイオード Waterfall 一方向セキュリティゲートウェイ” (オンライン) (引用日: 2017 年 1 月 30 日.) https://www.toshiba.co.jp/cl/pfsol/gateway/index_j.htm

[9] MONOist. “制御システム防御に最適なロックダウン型ウイルス対策ソフトの運用性が向上“(オンライン) (引用日: 2017 年 1 月 30 日.) http://monoist.atmarkit.co.jp/mn/articles/1501/07/news108.html

[10] CSSC. “制御システムセキュリティの対策技術紹介 ～ホワイトリストスイッチ，サイバー攻撃早期認識支援技術～” https://www.jpcert.or.jp/present/2016/20160217_CSC-CSSC.pdf