News Release

国立研究開発法人新エネルギー・産業技術総合開発機構
株式会社日立製作所

2017.10.2

サイバー攻撃の脅威を早期に検知する新規アルゴリズムを開発、「Hitachi Anomaly Detector」として製品化へ
―重要インフラ分野におけるシステムのセキュリティ向上に貢献―

（株）日立製作所は、サイバー攻撃の脅威を早期に検知し、セキュリティ対策を施すことが困難な装置が混在する制御システムなどへの導入を可能とする自動学習・検知アルゴリズムの開発に成功しました。今後、開発成果の製品化に向けた検証を行い、本年12月をめどに新製品「Hitachi Anomaly Detector」として提供を開始し、体制、運用を含めたシステムのセキュリティ向上に貢献します。

NEDOは内閣府の指定を受け、内閣府事業「戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保」の管理法人を担っています。本事業は電力やガス、水道、鉄道、航空、金融など重要インフラ分野の制御システムのセキュリティの強化を目的としたものです。本件はその第一弾の成果となります。

1. 概要

近年、IoTの進展に伴い、ネットワークにつながる重要インフラに対するサイバー攻撃のリスクが高まっています。従来のセキュリティ対策は、セキュリティソフトウェアをシステムに導入して検知するエージェント型やあらかじめ顕現化しているリスク要因との比較により検知するシグネチャ型などが一般的ですが、攻撃手法そのものが日々高度化・巧妙化しているため、新型のサイバー攻撃を検知することが難しく、問題となっています。また、制御システムの場合、システム停止が容易でないことから、システム改修を伴うセキュリティ対策を頻繁に施すことが困難であるほか、セキュリティ対策を施せない装置が混在していることも、セキュリティ対策の足かせとなっています。

このような背景のもと、NEDOは内閣府の指定を受け、内閣府事業「戦略的イノベーション創造プログラム（SIP）[※1]」の課題の一つの「重要インフラ等におけるサイバーセキュリティの確保」の管理法人を担い、研究開発を推進しています。本事業を通じて、電力やガス、水道、鉄道、航空、金融など重要インフラ分野の制御システムのセキュリティ強化の実現をめざしています。

株式会社日立製作所は、重要インフラ分野の制御システムのセキュリティ強化とサービス安定運用の実現に向け、サイバー攻撃から制御システムを守るための制御・通信機器および制御ネットワークの動作監視・解析技術と防御技術に関する研究開発を行ってきました。今般、本プロジェクトにおいて、（株）日立製作所は、正常なシステム状態を定義し、現状と照合しながら異常を検知するアノマリ型[※2]自動学習・検知アルゴリズムを開発することに成功しました。

2. 今回の成果

今回研究開発したアルゴリズムは、システムを多角的な視点でホワイト化※3 しながら自動生成を繰り返す監査アルゴリズムを多層に積み重ねて構成し、システムの異変を検知するものです。これにより、サイバー攻撃の探索行為における予兆やなりすましにより検知をすり抜けようとするサイバー攻撃などの検知率を向上することが可能となります。

また、今回新たに研究開発した独自の機械学習エンジンにより、構成変更や機能追加によるシステムの差分を自動的に吸収するため、運用負荷を低減することが可能となります。加えて、汎用的に利用できるアルゴリズムのため、対象 OS やシステム構成に制約なく適用することが可能となり、様々な分野の様々なシステムに効率よく展開することが可能となります。

さらに、今回、本プロジェクト内で重要インフラ事業者との協働検討の体制を築き、システムに導入し易い形式での提供方法も合わせて検討しました。その結果、本技術を活用し、システムの外側に設置した装置により監視する構成とすることで、セキュリティ対策を施せない古い装置が混在する制御システムなどへの導入を可能としました。

これらの成果により、サイバー攻撃の予兆などを早期に発見し、安定したサービス提供に貢献します。

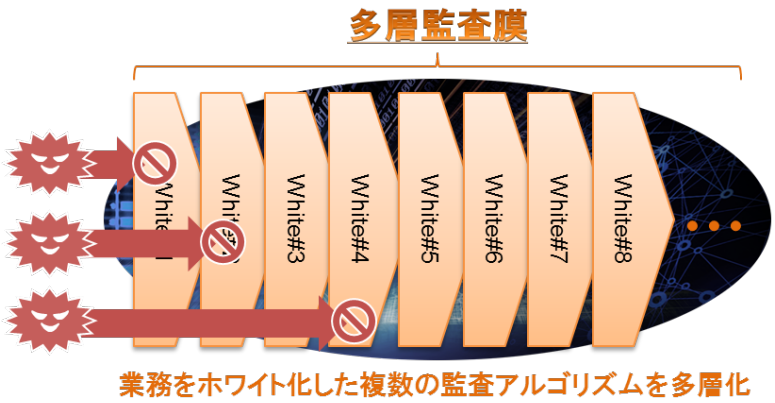

図　自動学習アルゴリズムの概念図

3. 今後の予定

（株）日立製作所は、2017 年 12 月をめどに今回開発した技術を実装した製品を提供開始する予定です。今後、重要インフラ分野をはじめとする制御システム・情報システムに本製品を提供するとともに、SOC※4 や情報共有基盤などと連携し、システムに対するセキュリティの向上だけでなく、体制、運用を含めたセキュリティの向上を進めていきます。

なお、本製品は、NEDO が 2017 年 10 月 13 日（金）にベルサール神田で開催する「SIP／重要インフラ等におけるサイバーセキュリティの確保　シンポジウム 2017」、および、（株）日立製作所が 2017 年 11 月 1 日（水）～2 日（木）に東京国際フォーラムで開催する「Hitachi Social Innovation Forum 2017 TOKYO」において、紹介します。

4. （株）日立製作所のHitachi Anomaly Detectorに関するウェブサイト

http://www.hitachi.co.jp/products/it/network/communimax/infra/had/index.html

【用語解説】

※1 戦略的イノベーション創造プログラム（SIP）

SIP は Cross-ministerial Strategic Innovation Promotion Program の略称で、内閣府の総合科学技術・イノベーション会議が自らの司令塔機能を発揮して、府省の枠や旧来の分野の枠を超えたマネジメントに主導的な役割を果たすことを通じて、科学技術イノベーションを実現するために新たに創設するプログラム。自動走行や防災分野など 11 の課題テーマに対し、府省・官民・分野の枠を越え、それぞれ基礎研究から実用化・事業化までを見据えた取り組みを推進している。

※2 アノマリ型

正常なシステム状態などを定義し、現状と照合することで異常を検知する手法。

※3 ホワイト化

入力された正常時のデータを分析し、正常と判断可能な要素の組合せおよび値や範囲を定義すること。

※4 SOC

SOC は Security Operation Center の略称で、サイバー攻撃や各種セキュリティインシデント等の監視や分析を行う組織のこと。

5. 問い合わせ先

（本ニュースリリースの内容についての問い合わせ先）

NEDO IoT 推進部 担当：藤野、小島、上野 TEL：044-520-5211

株式会社日立製作所 セキュリティ事業統括本部 マネジメント本部 事業管理部

http://www.hitachi.co.jp/Prod/comp/Secureplaza/inquiry.html

（その他NEDO事業についての一般的な問い合わせ先）

NEDO 広報部 担当：髙津佐、坂本、藤本 TEL：044-520-5151 E-mail：nedo_press@ml.nedo.go.jp