プレスリリース

平成 27 年 9 月 16 日

国立研究開発法人情報通信研究機構
横 河 電 機 株 式 会 社
国 立 大 学 法 人 京 都 大 学

制御システムの健全性を確認するトラフィック分析・可視化技術を開発

～電力・ガス・水道などの重要インフラを支える制御システムのセキュリティインシデントを検知～

【ポイント】

- 重要インフラを支える制御システムのセキュリティインシデントを早期に検知・分析・可視化する技術
- 制御システムに求められる高い可用性を損なうことなくインシデントの検知が可能
- 社会の重要インフラを支える制御システムのセキュリティ向上に貢献

国立研究開発法人情報通信研究機構（NICT、理事長: 坂内 正夫）は、横河電機株式会社（YOKOGAWA、代表取締役社長: 西島 剛志）及び国立大学法人京都大学（京都大学、岡部 寿男教授、高倉 弘喜准教授（当時））と共同で、電力・ガス・水道などの重要インフラの制御システムのネットワーク健全性を確認するためのトラフィック分析・可視化技術を開発しました。本技術により、制御システムで流れるネットワークトラフィックを分析・可視化することで、マルウェア感染等のセキュリティインシデントを早期に発見することが可能になります。なお、本技術は、共同研究相手であるYOKOGAWAが発売した、可視化技術と回収・解析を組み合わせて制御システムネットワークの健全性を診断する業界初のサービス「ネットワーク健全性確認サービス」に用いられており、今後、重要インフラに係る制御システム等のセキュリティ向上に貢献することが期待されます。

【背景】

近年、電力・ガス・水道などの重要インフラの制御システム（以下「制御システム」）がサイバー攻撃の対象として狙われるようになり、制御システムのセキュリティ確保が大きな課題となっています。制御システムは、汎用OSや標準プロトコルを用いた、よりオープンなシステムに移行し続けており、それに応じた感染経路の多様化（USB メモリ経由での感染など）から、マルウェア感染のすべてを未然に防ぐことは困難になっています。そのため、実際にセキュリティインシデントが発生した際に早期に発見するための技術開発が急務となっています。また、制御システムは、10～20 年といった長期間にわたって使用されるため、その可用性（システムが安定して動作し続けること）を損なわない対策技術が求められています。

【今回の成果】

NICT、YOKOGAWA 及び京都大学は共同で、制御システムにおけるマルウェア感染等のセキュリティインシデントを早期に発見するためのネットワークトラフィック分析・可視化技術を開発しました。

我々が着目したのは、「制御システムのネットワークは、特定用途のために設計・運用されていることから、多様なトラフィックが流れる一般の情報システムとは異なり、システム内を流れるトラフィックの正常状態を把握しやすい」という点です。

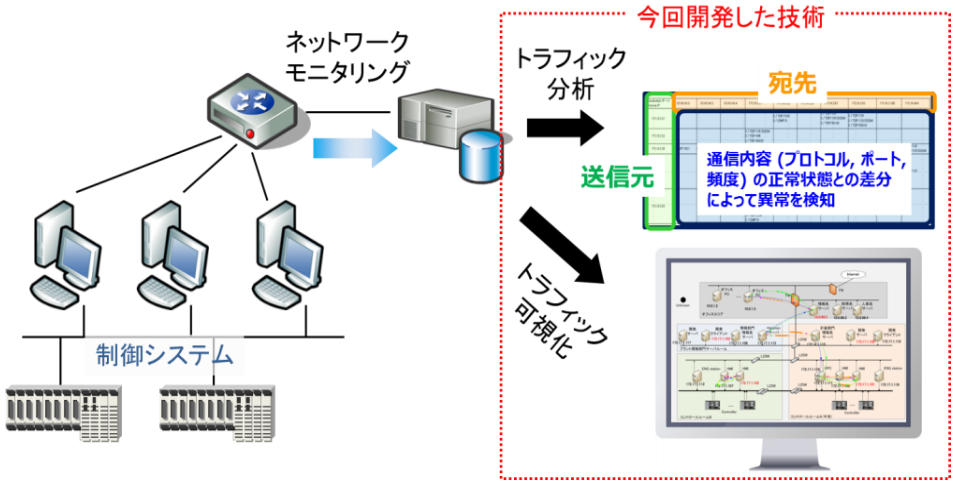


図 1　今回開発した技術の概要図

我々が開発した技術では、まず、制御システムのネットワークを流れる正常状態のトラフィックをホワイトリストとして保存します。このホワイトリストを基に、制御システムネットワークの挙動を時系列的に比較することで、マルウェア感染時のトラフィックの増加や不明な IP アドレスとの通信といった意図しない通信の発生を発見することができます。

さらに、NICT で開発し、既に技術移転をしているリアルタイムトラフィック可視化ツール NIRVANA[*1] を基に、制御システム独自の通信プロトコルに対応させるなどの改良を行い、異常が発見された際のトラフィック状況の把握が容易になりました。（図 2-正常時、図 3-インシデント発生時）

本技術は、制御システムの各サーバに検出用のソフトウエアをインストールする必要がなく、導入が容易であり、制御システムに求められる高い可用性に影響を与えることなく、インシデント検知が可能です。

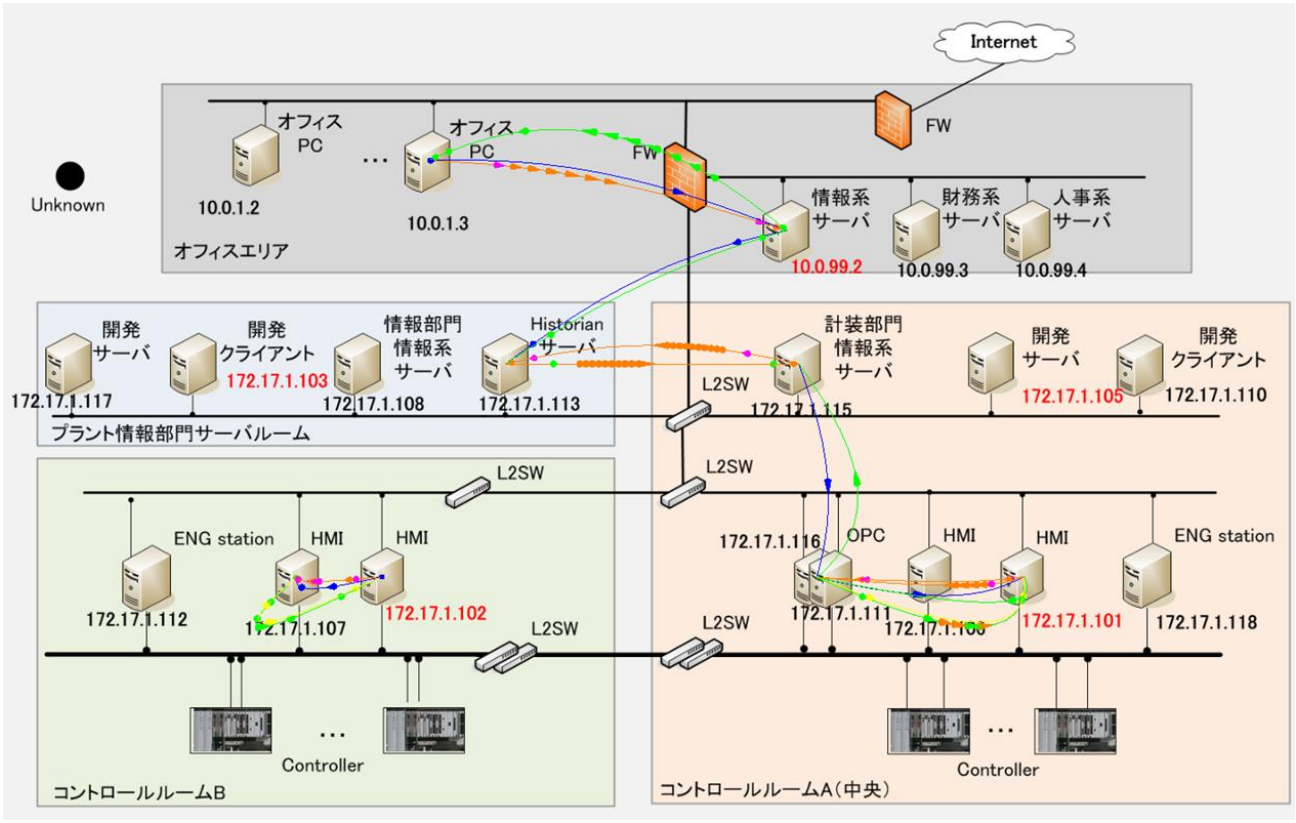


図 2　制御システムのネットワーク可視化例（**正常時**）

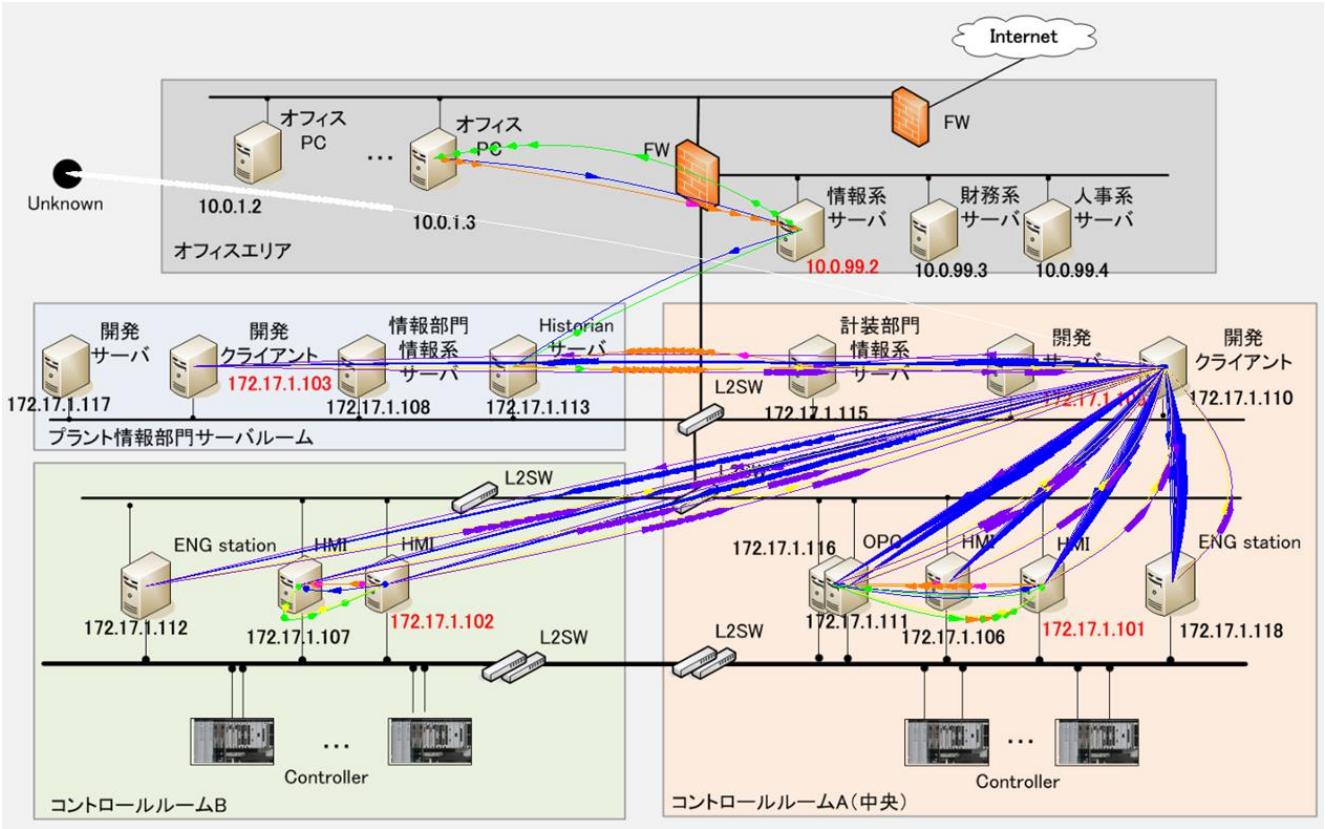


図 3　制御システムのネットワーク可視化例（**インシデント発生時**）

（ここでは、中央右側のコントロールルーム A 内の 1 クライアントサーバーがマルウェアに感染し、ネットワーク内に攻撃のための大量のトラフィックを送信している様子が可視化されている。）

【今後の展望】

今回開発した技術は、共同研究相手である YOKOGAWA が発売した制御システム向けサイバーセキュリティ対策支援サービスである「ネットワーク健全性確認サービス」(※)に活用されるなど、今後の制御システムのセキュリティ向上に役立てられることが期待されます。

我々は、今後も制御システムにおけるサイバーセキュリティ対策技術に関する研究開発を推進し、安心安全な社会の実現に貢献してまいります。

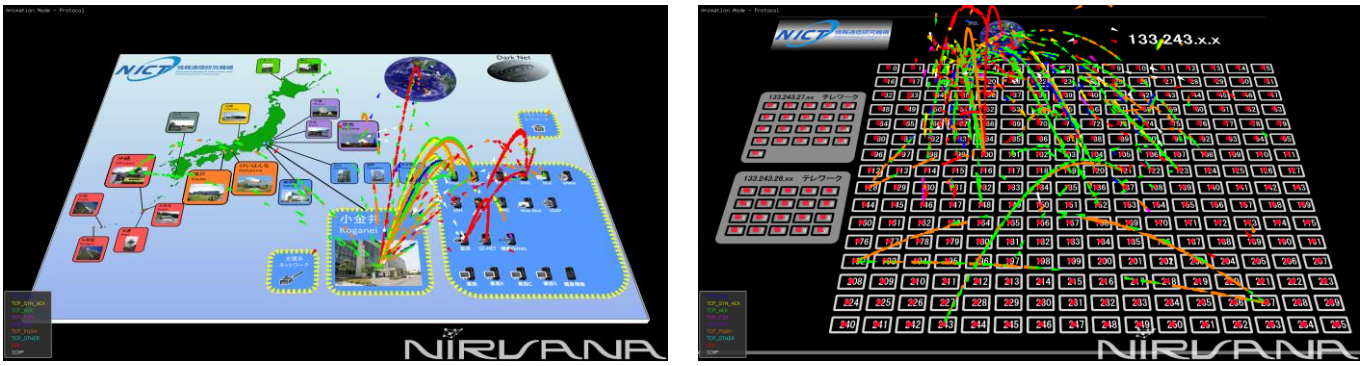
(※) 参考 URL: http://www.yokogawa.co.jp/sv/solution/eps/srv-netck-jp.htm

---

＜用語解説＞

***1 NIRVANA（ニルヴァーナ: NICTER Real-network Visual ANAlyzer）**

NICT が開発したトラフィックをリアルタイムに可視化・分析するシステム。NIRVANA は、大規模化・複雑化するネットワーク管理の負荷を、トラフィックの「見える化」によって軽減し、障害発生時に迅速な対応が可能になります。NIRVANA は技術移転が可能です。



NIRVANA による表示画面 （左: パケットモード、右: アドレスブロック表示）

＜ 本件に関する問い合わせ先 ＞

NICT
ネットワークセキュリティ研究所
サイバーセキュリティ研究室
笠間 貴弘、衛藤 将史、井上 大介
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

横河電機株式会社
IAPF システム事業部 PA システム企画部
江曽 賢一、鈴木 和也、星野 浩志
Tel: 0422-52-0212
E-mail: security-pr@ml.jp.yokogawa.com

京都大学
学術情報メディアセンター
ネットワーク研究部門高機能ネットワーク研究分野
岡部 寿男
Tel: 075-753-7458
E-mail: okabe@media.kyoto-u.ac.jp

＜ 広報 ＞

NICT
広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

横河電機株式会社
コーポレート・コミュニケーション室
久保 裕資
Tel: 0422-52-5530
E-mail: Yokogawa-pr@ml.jp.yokogawa.com

京都大学
企画・情報部 広報課
進藤 健司
Tel: 075-753-2071
E-mail: kohho52@mail2.adm.kyoto-u.ac.jp