News Release
2019.11.29

国立研究開発法人新エネルギー・産業技術総合開発機構
富士通株式会社
大学共同利用機関法人 情報・システム研究機構 国立情報学研究所

20Gbps 高速大容量の通信環境において不審通信の検知に成功
—2020 年度に本技術を利用したサービスの実用化を目指す—

NEDOが管理法人を務める内閣府事業「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」において、富士通と国立情報学研究所（NII）は、20Gbps高速大容量のネットワークを対象に収集・蓄積・解析を組み合わせた技術の有用性を検証する実証実験を行い、従来技術では検知できなかった不審な通信を検知することに成功しました。

本実証実験にて有用性を検証した技術は、高速大容量の通信データを対象として通信の規則性や関係性に基づいた解析を行い、全体から乖離している通信挙動を特定することで、不審な通信を検知する技術を新たに富士通にて開発し、さらにネットワーク上の大量の通信データを収集・蓄積する技術などを組み合わせることで実現しました。

富士通は、今後、解析結果に基づきネットワーク管理者向けに対処方法を推奨する技術の開発を進め、2020年度に、今回開発した技術と組み合わせたサービスの実用化を目指します。また、NIIは、本事業の成果を発展させ、サイバー攻撃発生時の被害状況を推定しその影響範囲を極小化する手法の実現を目指します。

1. 概要

近年、高度化が進むサイバー攻撃は既存のセキュリティ対策を巧妙にすり抜けることが多いため、侵入を検知した際にはすでにサイバー攻撃の踏み台[※1]とされていることも少なくありません。このため、内在する脅威を、いかに素早く捕捉できるかが重要です。

近年開発が進む、攻撃シナリオのモデル化や人工知能（AI）技術を活用した最新の検知技術は、長期にわたる通信ログを攻撃手口と関連付けて解析することで、脅威情報の見逃しを削減しています。しかしながら、さまざまな形態で利用される高速大容量のネットワーク環境においては、解析処理に利用する内部データなどが膨大となり、これらの技術をそのまま適用することが困難です。

このような背景のもと、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）が管理法人を務める「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」において、富士通株式会社（以下、富士通）と大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（以下、NII）はネットワーク上の大量のデータを収集・蓄積・解析することで不審な通信を抽出し、そのデータの特長をもとに、ネットワークの監視や調査などを行う対応者へ、最適な対処法を推奨する技術の開発を推進しています。

今般、本事業において、富士通は、通信の規則性と関係性に着目することで、汎用サーバーにおいて高速大容量の通信データを対象とする解析を行い、ネットワーク上の大量データから正規の通信特性を逸脱する踏み台特有の通信を識別する技術を開発しました。この技術を用いて、NIIが構築した20Gbps高速大容量のネットワークを対象に収集・蓄積・解析を組み合わせた技術の有用性を検証する実証実験を行い、従来技術では検知できなかった不審な通信を検知することに成功しました。

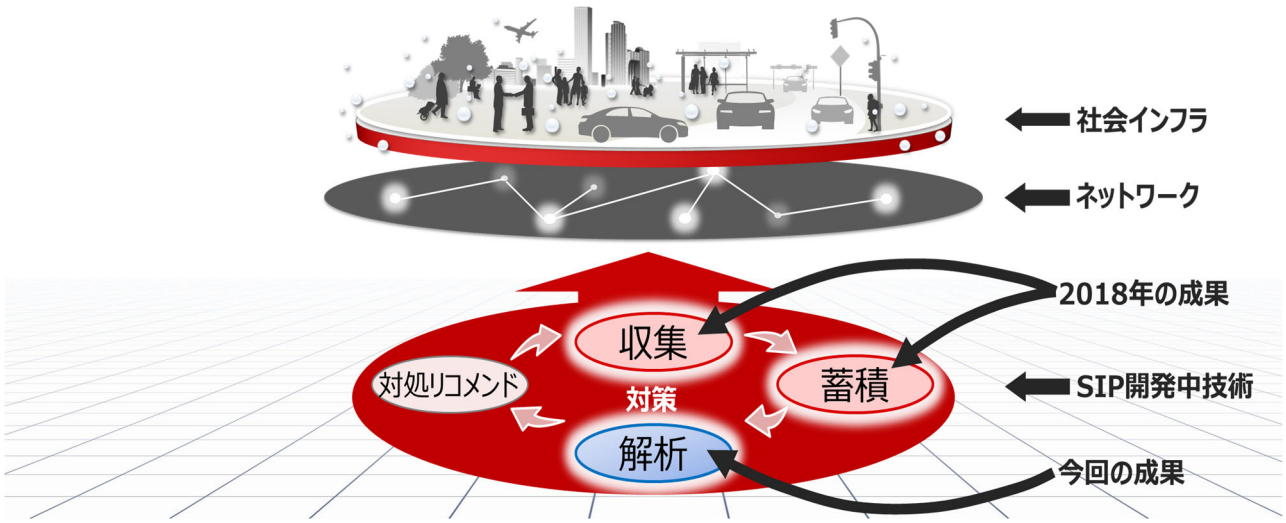

図　本事業の概要図

2. 今回の開発技術・成果

(1)多種多様な大量の通信データを解析し、踏み台特有の通信を検知する技術を開発

外部からのサイバー攻撃においては、機密情報の探索や侵入経路の拡大など遠隔操作の踏み台として、組織内ネットワークの機器が悪用されています。この踏み台となった機器は、正規業務の通信と攻撃操作の通信を同時に行っていることになります。

本技術の特徴は、踏み台と外部の攻撃サーバー間で定期的に発生する通信の周期性に着目し、攻撃サーバーによる通信の特徴を捉えることで、正規利用の通信特性から逸脱する通信を検知します。この技術では、通信の特徴を示す通信パターンを数値化し、富士通独自の数理モデルを用いて判別することで、汎用サーバーにおいても大量の通信データの解析を可能としています。また、規則的な通信を行う正規業務の通信に対しては、通信データの送受信相手や他機器への通信状況を指標化することで踏み台特有の通信と区別し、作業の漏れや解析の誤りを抑止することが可能です。

(2)NIIの実証実験ネットワーク環境において従来検知が困難な踏み台特有の通信を検知

技術の有効性を確認するため、今回の開発技術と仮想ネットワークの通信性能を向上させる分析技術※2、およびネットワークの通信データを欠損なく収集・蓄積する技術※3を実装した汎用サーバーを、NIIの高速大容量のネットワーク環境に設置し、2018年10月から実証実験を実施しました。実証実験の結果、20Gbpsの大容量通信を行うネットワークにおいて、通信データを欠損することなく、踏み台特有の不審な通信を検知することに成功しました。検知した通信は、正規業務の通信と同一の通信ポートを悪用したもので、大容量通信を行うネットワーク上では、従来のセキュリティ装置で検知されないものでした。

3. 今後の予定

富士通は、本事業において、解析結果に基づきネットワーク管理者に対する対処方法の推奨を行う技術の開発を進め、2020年度に、今回開発した技術と組み合わせたサービス化を目指します。また、NIIは、本事業の成果を発展させ、サイバー攻撃発生時の被害状況を推定しその影響範囲を極小化する手法の実現を目指します。

【注釈】

※1 踏み台

マルウェアに感染したサーバーなどの通信機器。

※2 仮想ネットワークの通信性能を向上させる分析技術

仮想ネットワークの通信パケットを低負荷でキャプチャ―し、通信ボトルネックの分析、解消する推奨設定を提示する技術。

株式会社富士通研究所 2016年11月16日発表

https://pr.fujitsu.com/jp/news/2016/11/16-1.html

※3 ネットワークの通信データを欠損なく収集・蓄積する技術

仮想ネットワークの通信データを高速に欠損なく収集し、仮想・物理ネットワーク双方から収集した通信データをリアルタイムに蓄積する技術。

NEDO、富士通 2018年1月10日発表

https://www.nedo.go.jp/news/press/AA5_100893.html

4. 問い合わせ先

（本ニュースリリース内容についての問い合わせ先）

NEDO IoT推進部 担当：山形、千代延 TEL：044-520-5211

富士通株式会社

（1）お客様からの問い合わせ先：ネットワークソリューション事業本部 TEL：044-280-9861

（2）報道関係者からの問い合わせ先：広報IR室 TEL：03-6252-2174

NII 総務部企画課 広報チーム TEL：03-4212-2164 E-mail：media@nii.ac.jp

（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：佐藤、坂本、中里 TEL：044-520-5151 E-mail：nedo_press@ml.nedo.go.jp