安全な暮らしを支える セキュリティ技術の研究開発

サイバー攻撃が日々激化、巧妙化を続け、企業システムの安全が脅かされています。一方で、様々な機器がネットワークに接続される IoT時代をむかえ、パーソナル情報をはじめとする様々な機器からの情報を安全に利活用することが望まれています。これらの課題の解決のために、富士通研究所では、最先端の技術開発に取り組んでいます。本報告書では、最近猛威を振るっている標的型攻撃を早期に検知する技術と、IoT機器同士の軽量かつ高セキュアな相互認証技術をご紹介します。

≫ 標的型サイバー攻撃の新しい検知技術

巧妙化するサイバー攻撃

近年、特定組織や個人を標的として情報窃取を行うことを目的とした標的型攻撃が急増しており、その攻撃の方法は、より巧妙になってきています。標的型攻撃では、マルウェアと呼ばれる悪意あるプログラムが用いられます。

最新のマルウェアは、通常の業務で発生するメール送受信やウェブアクセスなどの通信に紛れて、攻撃者が組織外から内部の感染パソコンを遠隔操作し、内部情報を取集するRAT（Remote Access Trojan）というタイプが主流になってきています。RATが攻撃する際の通信内容にはマルウェア自体が含まれず、遠隔操作の通信自体も暗号化されていることがほとんどで、従来のアンチウイルスソフトウェアや不正侵入検知システムなどの対策では発見が困難でした。

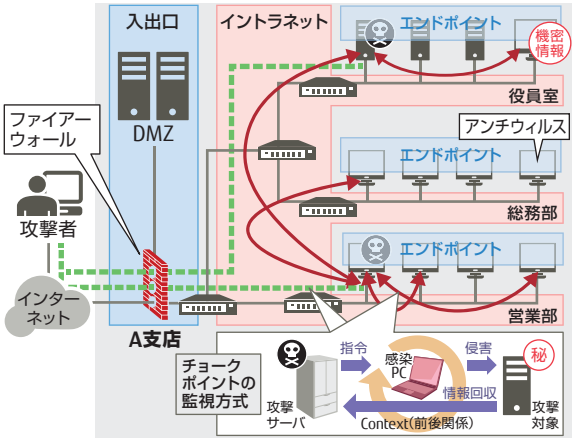
組織内に侵入したマルウェアの新しい検知技術

今回、RATの社内潜伏活動をイントラネットで検知する技術を開発しました。

1. チョークポイントの監視方式

多様な攻撃の手口に共通する通信の特徴的なパターンをチョークポイントと呼びます。この通信パターンに着目し、イントラネットを流れている通信の種類と、関連する通信の前後関係を解析することで、RATによる社内潜伏活動を検知します。通信の種類と前後関係のみを見るので、通信にマルウェアが含まれていなかったり、暗号化されていたりしても高い検出率を実現します。

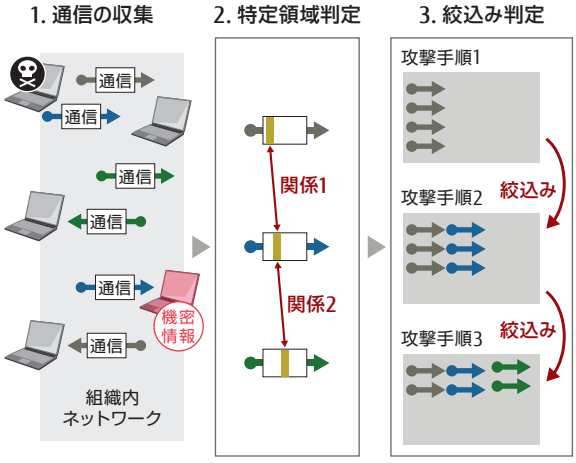
チョークポイントの監視方式のイメージ



2. RATの通信パターンの効率的な判定技術

チョークポイントの監視方式において、攻撃通信の判定を、二つの技術で効率的に行います。一つは、一般に通信内容の詳細解析が必要な攻撃通信の判定を、複数通信の特定領域の情報と通信順序の関係のみを使用し、検知精度を下げることなく解析処理量を削減しながら攻撃通信を判定する「特定領域判定」技術です。もう一つは、大量の通信の中から複数通信で構成された攻撃を抽出する時間がかかる処理を、攻撃手順の段階ごとに解析すべき通信情報の候補を狭めて管理することで、効率的に複数の不審な通信を判定する「絞込み判定」技術です。

RATの通信パターンの効率的な判定技術の概要



開発技術を、2,000台規模の端末が接続された大量の業務通信が流れているギガビットのネットワーク環境で、RATの潜伏活動を再現しながら実証評価し、全通信パケット量の0.0001%に当たるRATの攻撃通信をすべて検知すると共に、業務通信を攻撃通信と誤検知しないことを確認しています。

新しい検知技術の効果

本技術を搭載したネットワーク装置を組織内ネットワークへ配備することにより、組織内のイントラネットを流れる不正な通信を監視することができます。ファイアーウォールやアンチウイルスソフトウェアでは検知困難な標的型攻撃のマルウェアを、情報漏えい前に検出することに効果を発揮します。今後は、攻撃検知後の対処技術の研究開発も目指して行きます。

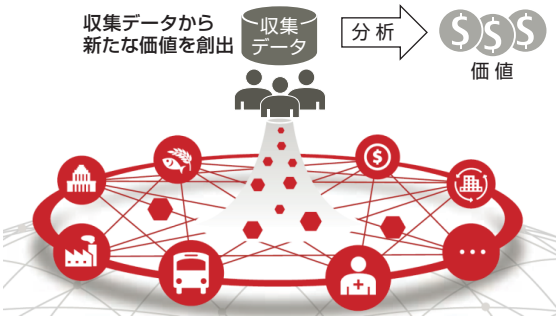
» IoT時代の機器間相互認証技術

IoTのセキュリティ確保のために

汎用PCに加えて、エアコン、照明、自動車など、多様な機器がインターネットに接続されるIoT時代をむかえ、機器が得た情報を収集し、その分析結果を利活用する新たなビジネスに注目が集まっています。こうした用途では、収集した情報が正しいか、機器が不正に操作されていないかを保証するセキュリティ技術が必須となります。一方で、2020年には接続されるデバイスが約500億個になると予想されており、そこで使用されるセキュリティ技術にも高い効率性が求められます。富士通研究所では、IoTの世界で効率的に機器同士の相互認証が可能な技術の研究開発を行っています。

現在のインターネットでは、TLS（Transport Layer Security）と呼ばれる認証・暗号通信技術が広く利用されています。TLSでは、通信相手が正しいことを認証するために、公開鍵暗号を利用します。一般に公開鍵暗号では、ユーザーや機器と使用する鍵との紐付けを保証する証明書が必要です。通信相手の認証には、証明書を互いに送信し、証明書検証などの負荷の高い暗号処理が必要となります。それを機器数の膨大なIoTの世界で行うと、全機器に証明書を準備・管理する膨大な手間がかかること、また、証明書検証のための暗号処理と通信量の爆発的増加が課題となります。そこで、富士通研究所では、証明書を利用しない相互認証技術を開発しました。

↓IoT利用イメージ



機微情報も通信されるためセキュリティ確保は必須

開発した技術

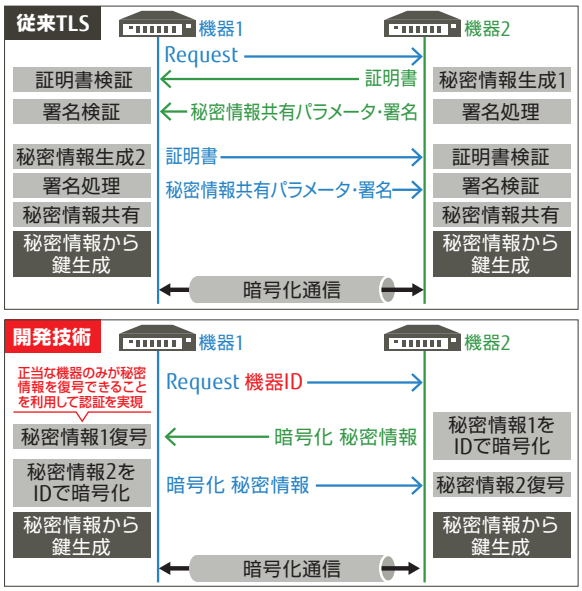
開発技術では、IDベース暗号と呼ばれる、IDを鍵に使える公開鍵暗号を活用しています。TLSで使われている公開鍵暗号、RSA暗号や楕円曲線暗号では、ユーザーとは無関係の乱数を鍵に使います。そのため、暗号化を行うには、事前に通信相手の証明書を入手し、その鍵（乱数）の正当性を検証する必要がありました。これに対し、IDベース暗号では、相手のIDが鍵のため、証明書の事前入手や、証明書を使った鍵の確認をすることなく、暗号化を行うことが可能です。

開発した相互認証技術では、この性質を利用して、相手の機器IDで暗号化した秘密の情報を互いに送りあいます。次に、入手した暗号化秘密情報を復号し、その秘密情報から暗号通信用の一時鍵を生成します。暗号化に使用したIDに対応する正当な機器のみが秘密情報を復号可能なため、この一時鍵でその後の通信を行うことで、相互認証と暗号通信を同時に実現できます。

また、TLSを拡張して、開発した相互認証方式の適用技術を開発しました。適用技術では、既存のTLSプロトコルに適合するように、IDベース暗号による秘密情報の交換を整形・最適化しました。特にこれまでのTLSでは、証明書の交換なしには、機器IDとしてIPアドレスやドメイン名などしか利用できない制約があったのですが、送信者の情報を通信開始時に効率的に伝達する拡張を行うことで、任意の情報を機器IDとして利用可能となりました。

この適用技術により、従来のTLS利用と同等の簡便さで、機器IDによる相互認証技術の利用が可能となります。

↓従来TLSと開発技術との比較



[開発技術の効果]

開発技術を小型のワンボードマイコンに実装したところ、TLSと比較して通信量を1/4、処理性能を2.5倍にすることに成功しました。開発技術により、軽量に機器間の相互認証が可能となり、膨大な機器が接続されるIoTの世界におけるセキュリティ確保を効率的に実現できます。

[相互接続性確保に向けた取り組み]

本研究で開発している認証は、IoTの基盤部分で利用される技術です。今後、数百億個の機器がネットワークでつながるIoTの世界で相互接続性を確保するためには、独自ではなく、他社との協力も重要となります。そのため現在、東大グリーンICTプロジェクトと共同でBEMS（Building Energy Management System）向け通信規格IEEE1888への適用開発を進めています。今後は、本プロジェクトでのIEEE標準化を目指しています。