マルチクラウド時代の次世代ハイブリッド型ネットワークの実現

Realizing Next-generation Hybrid-type Network for Multicloud Era

● 高村　智幸　● 櫻井　秀志　● 山本　大　● 村上　雅彦
● 山崎　浩一　● 海野　由紀

あらまし

企業ではクラウドの利活用が活発になり，企業内ネットワークの形態は大きな転換期を迎えている。従来型のセンター集中型閉域ネットワークではなく，拠点から直接インターネット上のSaaS(Software as a Service)を活用できるハイブリッド型ネットワークへの移行を考えている企業もある。しかし，それを実現するためには，複雑化する多拠点のネットワーク運用や拠点内のセキュリティ対策の課題を解決しなければならない。富士通と富士通研究所は，SD-WAN(Software-Defined Wide Area Network)の考え方と，合理的なマルウェア対策の考え方を基にそれらの課題を解決するとともに，更に利便性と安全性を両立させたセキュリティ技術の研究開発を行っている。

本稿では，マルチクラウド環境に最適化されたハイブリッド型ネットワークを実現するための富士通の取り組みについて述べる。

Abstract

As businesses actively employ cloud technology, enterprise networks are coming to a major turning point. Some businesses wish to shift from a conventional closed and centralized enterprise network to a new, hybrid-type network that allows direct access to Software as a Service (SaaS) via the Internet even from branch office. However, to realize this hybrid-type network, challenges in terms of operability of increasingly complex multi-branch office networks and security measures inside branch offices must be solved. Fujitsu and Fujitsu Laboratories approach these challenges based on the concepts of Software-Defined Wide Area Network (SD-WAN) and reasonable malware security measures. We also pursue research and development of security technology that achieves both greater convenience and safety. This paper describes the efforts made at Fujitsu to realize a hybrid-type network optimized for multicloud environments.

ま え が き

近年，多くの企業はビジネスや組織の急速な変化への対応と，働き方改革に必要な業務環境の整備のために，業務システムのクラウドへの移行とオンデマンド型ソフトウェアサービス（SaaS：Software as a Service）の利用に取り組んでいる。その結果，業務用途やサービスレベルによってクラウドを使い分ける，マルチクラウド環境に必然的に移行しつつある。

一方，働き方改革の推進によってモバイルユーザーが増加し，マルウェアが企業内ネットワークに持ち込まれる機会が増えている。また工場では，IoT化を進める過程で様々な端末機器やセンサー機器がつながり始めている。その結果，設備メンテナンスの際に，外部から持ち込まれたメンテナンス用のパソコンやUSBメモリによってマルウェアが持ち込まれ，生産停止となる事故も発生している。このように，企業では今まで以上にセキュリティ対策が重要な課題になっている。

今，企業はマルチクラウド化とエンドポイントの多様化を踏まえ，将来的なネットワーク形態の方向性を考える必要に迫られている。これは，インターネット上のSaaS利用が増加することにより，センターとインターネットとの接続箇所が輻輳（ふくそう）し，ボトルネックとなる問題が生じるためである。具体的には，以下の二つの形態のいずれかを選択しなくてはならない（**図-1**）。

（1）従来型ネットワーク

これまでの本社・データセンター（以下，センター）集中型の閉域ネットワークを維持したまま，センターのネットワークインフラを強化し，マルチクラウド環境に移行する。

（2）ハイブリッド型ネットワーク

従来とは異なり，できる限りインターネットを活用し，センターの業務システムだけでなく，各拠点からインターネット上のSaaSにも直接アクセスできるネットワークに移行する。

（2）は，センターと各拠点との間の回線・設備コストを削減でき，かつそれがボトルネックになることを回避できるため，SaaS利用時のレスポンスが改善する点で極めて魅力的である。一方で，今まで不要であったネットワークポリシー（以下，ポリシー）の運用負荷の効率化と，各拠点におけるセキュリティ対策の見直しが大きな課題となる。

本稿では，企業がハイブリッド型ネットワーク

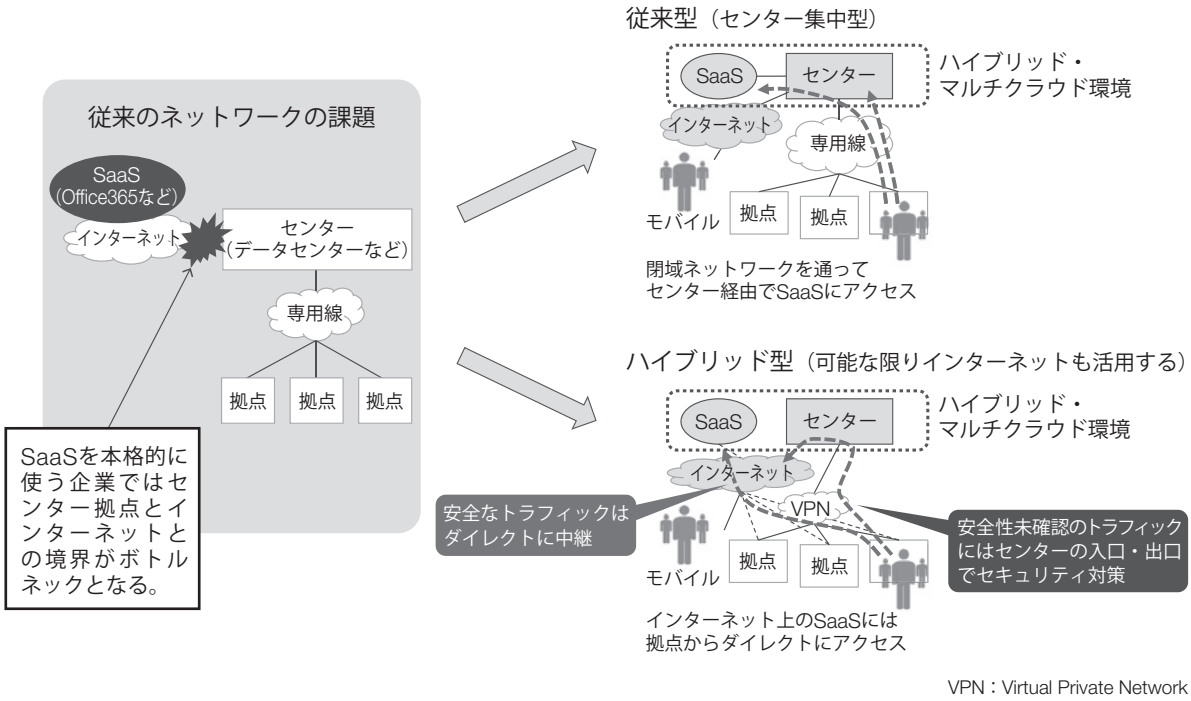


図-1　従来型とハイブリッド型ネットワークの比較

に移行する際の課題と，その解決に向けた富士通と富士通研究所（本稿では「富士通」に統一）の取り組みについて述べる。

ハイブリッド型ネットワークへの移行に向けた課題

ハイブリッド型ネットワークへの移行に向けて，以下の二つの課題がある。

● 多拠点のポリシー運用

ハイブリッド型ネットワーク構成では，各拠点からインターネット上のSaaSに直接アクセスする。そのため，どのトラフィックをインターネット経由で中継し，どのトラフィックをVPN（Virtual Private Network）経由でセンター向けに中継するかといったポリシーが必要になる。すなわち，ポリシーを適用する全ての拠点に対して，トラフィックごとにインターネット向け，VPN接続によるイントラネット向けの設定が必要である。その結果，拠点数に応じて多くの運用作業が発生する。

ポリシーの運用作業は二つの場面で必要とされる。一つ目は，新たにSaaSの利用を開始する際に，全ての拠点に対して設定を追加する場面である。二つ目は，新たに拠点を立ち上げる際に，ほかの拠点に倣って設定を追加しポリシーを適用する場面である。後者は，仮設オフィスが必要な業種や店舗の増減が激しい流通業界，M&Aが頻繁に行われる企業において，運用負荷を考える上で重要なポイントになる。

以上のことから，拠点ごとにポリシーをシンプルに管理し，ポリシー運用時の負担を軽減することと，ポリシーを適用するネットワーク拠点の増加時に少ない負担でポリシーを適用できることが求められる。

● 拠点内のセキュリティ対策

今や，企業内ネットワークにマルウェアが侵入し，常に様々な攻撃の標的となる危険にさらされていると認識する必要がある。

ハイブリッド型ネットワークに移行する際のセキュリティ対策としては，まず安全とみなせるトラフィックのみをポリシーに従って分離して，インターネットへ直接中継する。一方で，安全性未確認のトラフィックはVPN経由として，企業内ネットワークの入口と出口におけるセキュリティ対策を実施することが基本的な考え方となる。

マルウェアがネットワーク内に侵入した場合は，感染端末からほかの端末に感染が広がり情報漏えいルートが増加することに留意する必要がある。したがって，感染端末をこれまで以上に早くネットワークから切り離すことが重要である。以上のことから，運用管理者には端末の所在を探索してネットワークから切り離す手段が必要となる。また，拠点内のネットワークにおいて，マルウェア感染を検知できることと，マルウェアの感染が拡大しにくいネットワーク構成であることが求められる。

課題解決に向けた富士通の取り組み

本章では，ハイブリッド型ネットワークへ移行する際に，前章で述べた課題解決に向けた富士通の取り組みを紹介する。

● 拠点数増加時の運用負担軽減

ポリシーを適用するネットワーク拠点数が増えても効率的な運用管理を実現するためには，いわゆるSD-WAN（Software-Defined Wide Area Network）の考え方が解となる。運用管理ポータル上で各拠点の回線状態やルータ，LANスイッチなどのネットワーク機器（以下，機器）の状態を可視化し，一元的に管理する（**図-2**）。新たに拠点を立ち上げる際には，雛型となるポリシーを適用する。そして，拠点数が多いネットワーク構成でも，マルウェア感染端末の所在を即座に把握し対処できることが重要である。

更に，ネットワークに機器を接続した際には，

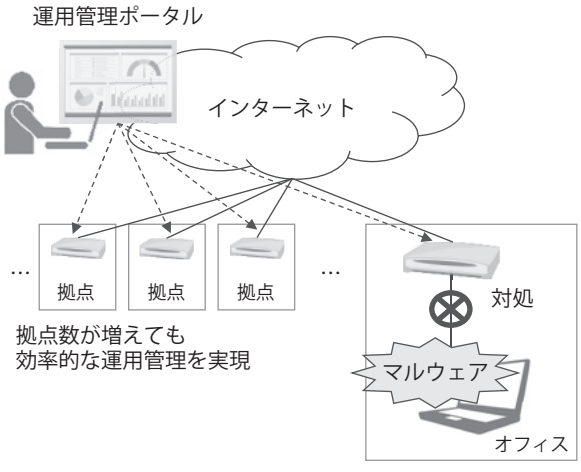


図-2　課題解決のポイント

そのコンフィギュレーションも自動的に行う（ゼロタッチコンフィグ）。富士通は，10年以上の実績があるゼロタッチコンフィグ機能を実現する技術を保有している。海外ベンダーのゼロタッチコンフィグ機能は，グローバル市場で大勢を占めるDHCP（Dynamic Host Configuration Protocol）をベースにしているため，国内のNGN（Next Generation Network）環境との親和性が低く，実際にはゼロタッチにならないケースが多い。それに対して，富士通はPPPoE（Point-to-Point Protocol over Ethernet）またはIPoE（Internet Protocol over Ethernet）をベースとする国内のネットワーク環境に適した，ゼロタッチコンフィグ機能を実現している。

● 拠点内のセキュリティ対策

次に，拠点内ネットワークに必要なセキュリティ対策として，マルウェアの感染防止・検知・対処について述べる。マルウェアに対しては，ハイブリッド型ネットワーク全体を俯瞰した施策（技術）が必要である（**図-3**）。インターネットと拠点内ネットワークの境界となるDMZ（DeMilitarized Zone）では，前述した入口･出口対策を極めていく。また，最新技術を利用した高度なマルウェア検知対策を適用する。一方，拠点内ネットワークでは以下の施策を行う。

- 脆弱な端末を接続させない，もしくは隔離するといった手法で感染リスクを低減する。
- ネットワーク上の振る舞いからマルウェア感染端末を検知する。
- マルウェア感染端末を検知した際に，直ちにネットワークから切り離す。

各施策について，以下に詳述する。

(1) マルウェア感染の防止

情報システム部門の管理下にない端末の接続や，脆弱性のある端末の接続を制限する。富士通は，これらに対応した持ち込み端末対策ソリューションとネットワーク検疫ソリューションを提供している。また，マルウェア感染の拡大を防ぐために，適切なセグメンテーション（ネットワークの論理的な分離）および外部ネットワークとの通信制限を行う。セグメンテーションは安全性を高めるために必要である半面，運用負荷が増大するデメリットもある。このため，富士通は利便性と安全性を両立させたセグメンテーション技術の開発に取り組んでいる。

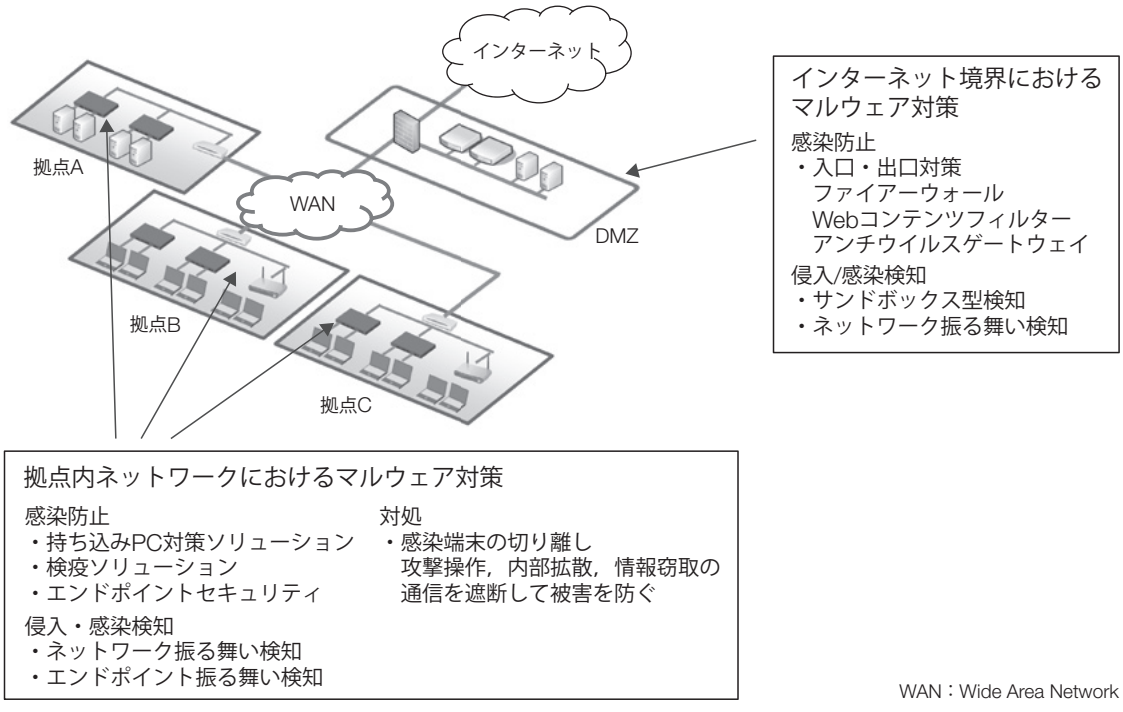


図-3　ハイブリッド型ネットワーク全体を俯瞰したセキュリティ対策

(2) マルウェア侵入・感染の検知

拠点内ネットワークでは，ネットワーク上の振る舞いに基づいてマルウェアを検知する。マルウェアの検知は，インターネットと拠点内ネットワークの境界，クラウド内，エンドポイント，そして拠点内ネットワークなど，様々な場所でそれぞれに適した技術を駆使して行う必要がある。富士通は，マルウェアの進化に合わせて新たなソリューションを提供するとともに，新たな検知技術の研究開発にも取り組んでいる。

(3) マルウェア感染の対処

マルウェアに感染した場合，それを検知した場所によらず，感染端末を特定してネットワークから切り離すことが重要である。マルウェア感染の検知・対処の流れを**図-4**に示す。マルウェアの感染を検知したら，まずネットワーク内の感染端末の所在を特定する。そして，感染端末にできるだけ近い機器からその端末を切り離して隔離することで，感染活動と情報漏えいを防ぐ。この際，業務に対しては局所的な影響にとどめられるように対処することが求められる。

一般的な企業では，マルウェア感染端末が見つかった場合，端末の接続状態の可視化が不十分なため，端末の所在を特定することは難しい。また，端末の切り離し作業には，ネットワークの専門技術者が必要とされるため，迅速な対応ができていない。富士通は，これらの問題を解決するために，端末の所在を特定し，簡単なオペレーション，または自動的に当該端末をネットワークから切り離すソリューションを提供している。

以上述べてきたとおり，ハイブリッド型ネットワーク移行に関する二つの課題に対して，富士通は運用管理者の業務負担低減を図りつつ，安心・安全なネットワーク環境を実現できる。

実現に向けた要素技術

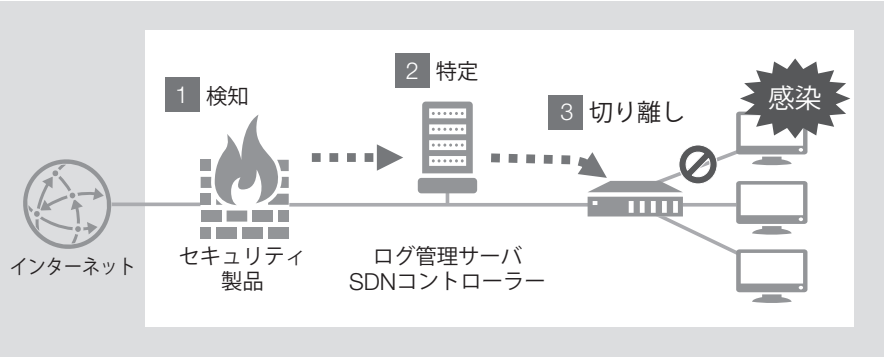
本章では，安心・安全なハイブリッド型ネットワークにおいて，利便性と安全性を両立させたセキュリティの要素技術として，三つの富士通独自技術を概説する。

● セキュアプロビジョニング技術

ハイブリッド型ネットワークの効率的かつ安全な運用を可能にするためには，SD-WANの考え方が必要である。各拠点の立ち上げ時には，ゼロタッチコンフィグによって自動的に機器をコンフィギュレーションする。

しかし，コンフィギュレーション対象となる機器の正当性を確認する従来の手法には，課題があった。ゼロタッチコンフィグでは，どの拠点にどのシリアル番号の機器を設置したのかという「ひも付け情報」をリモートサーバに伝える必要がある。機器のコンフィギュレーションには，センターと拠点との間のVPN接続といったセキュリティ関連設定も含まれる。もしひも付け情報に誤りがあると，所望のコンフィギュレーションが意図した拠点の機器に正しく配備されず，運用時のセキュリティリスクにつながる。このため，これまでは専門知識を持った拠点のエンジニアなどが，注意深くひも付け作業を行う必要があった。

そこで，富士通は機器の設置やひも付けを行う



SDN：Software-Defined Network

図-4　マルウェア感染端末の切り離し

人によらず，機器の取り違え，誤った拠点への設置などのリスクを低減するセキュアプロビジョニング技術を開発した（**図-5**）。本技術では，リモートサーバと通信可能な管理端末（タブレットなど）を用いて，機器の設置・ひも付けを行う。管理端末を介して，リモートサーバが機器の認証を行うことで，機器の取り違えを防ぐ。更に，あらかじめ拠点に送付されたQRコードによるワンタイムパスワードを管理端末で読み込むことで，機器と拠点との確実なひも付けを実現する。本技術によって，セキュリティリスクを低減し，信頼性の高いゼロタッチコンフィグを実現できる。

● **スマートセグメンテーション技術**

マルウェアの感染拡大を防ぐためには，適切なネットワークセグメンテーションを行うことが効果的である。具体的には，拠点内ネットワークを組織や業務内容などに合わせて小さな論理ネットワークに分離し，セグメント化する。これによって，マルウェアが侵入したとしてもセグメンテーションを行わない場合に比べて，小さなセグメント内に被害を局所化できる。

しかし，セグメンテーションを行うことはネットワーク接続の柔軟性を損ない，運用負荷が増大するおそれがある。このため，セグメント化されたネットワークでは，分離したセグメント同士を業務内容などに合わせて安全に，かつ短時間につなぎ替えることが必要となる。

富士通では，ネットワーク管理者が簡単なポリシーを設定するだけで，セグメントを安全に，かつ短時間につなぎ替えるスマートセグメンテーション技術を開発している（**図-6**）。本技術では，ポリシーを基に，業務に必要な情報だけをセグメント間で送受信できるように，機器の設定情報を変更する。これにより，運用管理者の負担を最小化し，安全なネットワークの構築・運用が可能となる。

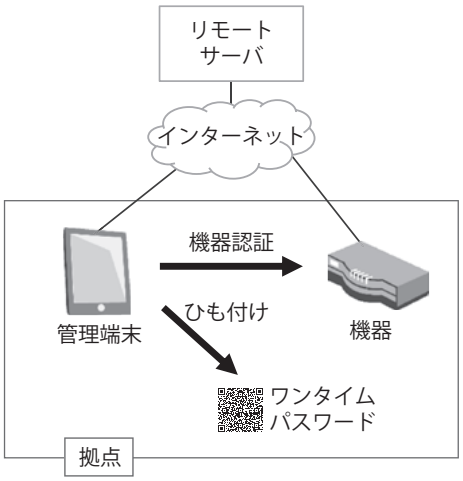


図-5　セキュアプロビジョニング技術

● **標的型攻撃検知技術**

富士通では，ネットワーク上の振る舞いを基にマルウェアを検知する技術の開発に取り組んでいる。こうした技術は既にいくつか知られているが，マルウェアが進化する中，検知技術も進化し続ける必要がある。

拠点内ネットワークに侵入したマルウェア

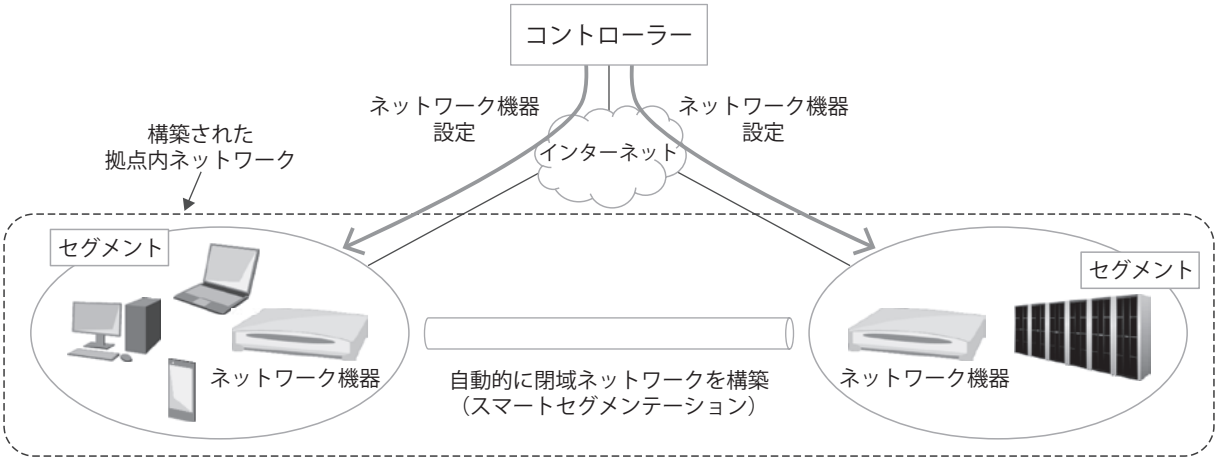


図-6　スマートセグメンテーション技術

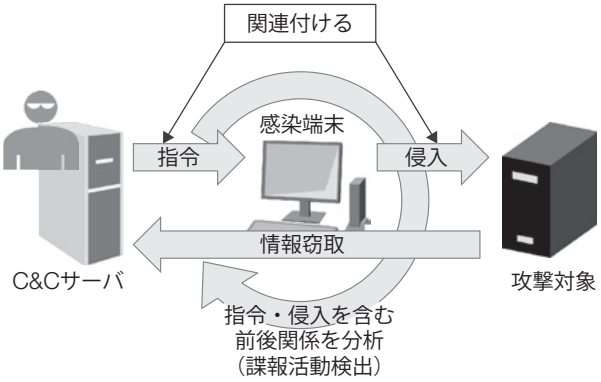


図-7　拠点ネットワーク内通信の解析による諜報活動の検出

は，RAT（Remote Access Trojan/Remote Administration Tool）と呼ばれる。RATが外部ネットワークに置かれた攻撃者のC&C（Command & Control）サーバに接続することで，攻撃者は感染ホストへのリモートアクセスが可能になる。攻撃者は，最初に侵入したホストから次の標的に侵入し，情報を窃取するといった諜報活動を繰り返す。この諜報活動は，通常の業務で利用されているSMB（Server Message Block）プロトコルが使われているため，通信ログを見ても通常の業務と攻撃を区別することは難しい。そこで，富士通ではこれらの通信を区別し，RATによる諜報活動を早期に検知する技術を開発した。(1)

本技術では，まず拠点内ネットワークの通信を収集・分析する。そして，RAT感染端末に指令を送るためのリモート通信と，感染端末から別の端末（攻撃対象）に侵入してコマンドやプログラムを実行する内部攻撃通信を，それぞれの特徴から抽出する。次に，これら二つの通信をひも付けることで，攻撃者の諜報活動を検知する（**図-7**）。

異なる相手との通信を関連付けて解析したり，通信の時系列的な流れを解析したりすることで，個々の通信の単一の振る舞いとしては正常であっても，システム全体としては矛盾や異常が見えてくるようになる。更に，複数の監視点からの情報を収集・統合する連携技術を組み合わせることで，リモート通信と内部攻撃通信が異なる監視点で観測されるような諜報活動であっても，検知できる。(2)

本技術により，RATによる諜報活動を，マルウェアのシグネチャ（マルウェアが持つ特徴的なデータパターン）や動作定義に依存することなく迅速に検知し，攻撃者からの情報窃取の防止が期待できる。

む　す　び

本稿では，企業内ネットワークを対象とした次世代のハイブリッド型ネットワークソリューションと，その実現に向けた富士通の取り組みについて述べた。

企業内ネットワークは，クラウドの利活用，事業形態，エンドユーザーの働き方などに合わせて最適化されていく。また，IoTの普及，新たなセキュリティ脅威への対応，5G（第5世代移動通信システム）の普及，AI（人工知能）を使った先端テクノロジーの登場など，今後の環境の変化と関連技術の進化に合わせてネットワーク技術も変化し続ける。富士通は，これらの変化に対応し，お客様起点のソリューションの開発と提供に取り組んでいく。

本研究の一部は，総務省委託研究「サイバー攻撃解析・検知に関する研究開発」により実施したものである。

参考文献

(1) 鳥居 悟ほか：特定の企業や個人を対象にしたサイバー攻撃対策技術. FUJITSU, Vol.64, No.5, p.516-522 (2013).
http://img.jp.fujitsu.com/downloads/jp/jmag/vol64-5/paper09.pdf
(2) 山田正弘ほか：組織内ネットワークにおける標的型攻撃の振る舞い検知に向けた複数センサ連携手法．暗号と情報セキュリティシンポジウム（SCIS），2015.

著者紹介

高村　智幸（たかむら　ともゆき）
富士通（株）
ネットワークサービス事業本部
エンタープライズ向けネットワークビジネスの企画・戦略策定に従事。

櫻井　秀志（さくらい　ひでし）
富士通（株）
ネットワークサービス事業本部
エンタープライズ向けネットワークソリューション・インテグレーションの技術支援に従事。

山本　大（やまもと　だい）
（株）富士通研究所
セキュリティ研究所
サイバーセキュリティ，暗号実装に関する研究開発に従事。

村上　雅彦（むらかみ　まさひこ）
（株）富士通研究所
セキュリティ研究所
ネットワークサービス技術に関する研究開発に従事。

山崎　浩一（やまさき　こういち）
（株）富士通研究所
セキュリティ研究所
スマートセグメンテーション技術に関する研究開発に従事。

海野　由紀（うんの　ゆき）
（株）富士通研究所
セキュリティ研究所
ネットワークセキュリティ，サイバーセキュリティに関する研究開発に従事。