富士通のセキュリティエバンジェリストが語る！ これからのサイバーセキュリティのあり方とは

FUJITSU JOURNAL / 2018年8月28日

企業・組織を狙ったサイバー攻撃が後を絶ちません。ますます複雑化する攻撃に対して、私たちは重要な資産をどう守っていくべきなのでしょうか。サイバーセキュリティに関し、企業が取り組むべき課題はたくさんあります。富士通のセキュリティエバンジェリストである太田大州が、サイバーセキュリティを巡る国際ルールや独自の技術開発や人材育成などの最新動向を踏まえ、これからのセキュリティ対策のあり方について解説します。

デジタルが世界を動かす時代、重要なのは「サイバーセキュリティ」

AI（人工知能）やIoT（モノのインターネット）、ビッグデータなどの新しい技術が日常生活やビジネスに大きな変革をもたらそうとしています。2015年の国連総会で採択された「SDGs（Sustainable Development Goals）」の取り組みでも、デジタルは非常に大きな役割を果たすことになります。

私は「デジタルはインターネットによって覚醒した」と考えています。インターネットがあればこそ、あらゆるものがつながり、あらゆるデータの交換が瞬時にできるようになるからです。そこで重要となるのが「サイバーセキュリティ」です。

サイバーセキュリティを考えるうえでは、インターネットを理解する必要があります。インターネットは、米国が1959年に国家プロジェクトとして取り組んだ軍事用ネットワーク「ARPANET」がその始まりです。その後、1980年代に軍事用から学術用に切り離されます。民間の研究所や大学などが中核となり基盤を活用し始めます。それから1990年代後半以降、爆発的に普及が進んでいきます。

富士通では2001年をインターネット元年と位置付け、「Everything on the Internet」という事業戦略を掲げて、インターネットをビジネスに最大限活用できるようネットワーク社会の基盤づくりを推進してきました。

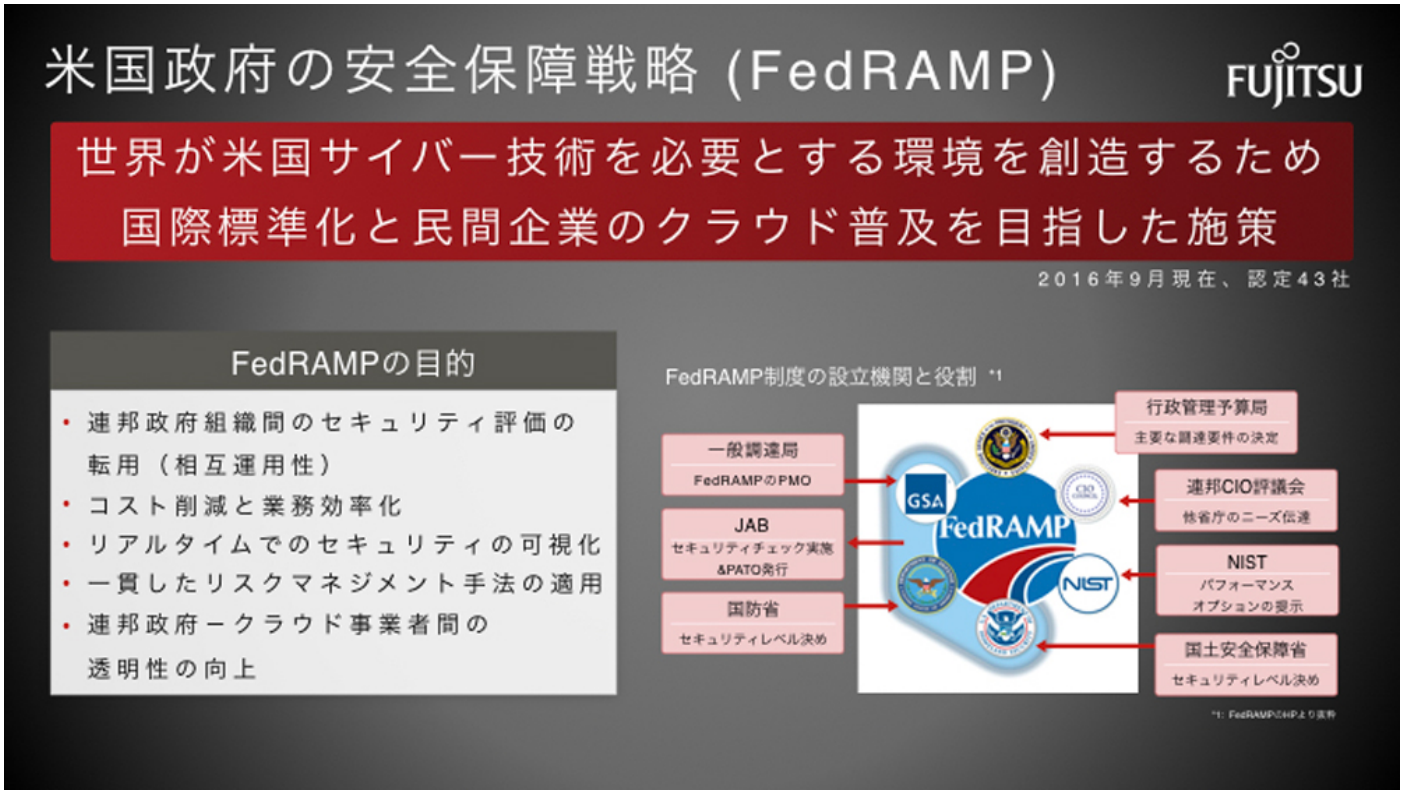
ところが、2001年9月11日に起きた米国同時多発テロでは、インターネットがテロ行為を実行する上で巧妙に悪用されました。この事件は以後のサイバーセキュリティに大きな変革をもたらすことになります。

米国がこの事件を調査した結果、テロ組織はインターネットを最大限活用してテロを実行したことが明らかになりました。それを受けて、米国をはじめ各国がサイバーセキュリティに関して様々な対策を開始しています。

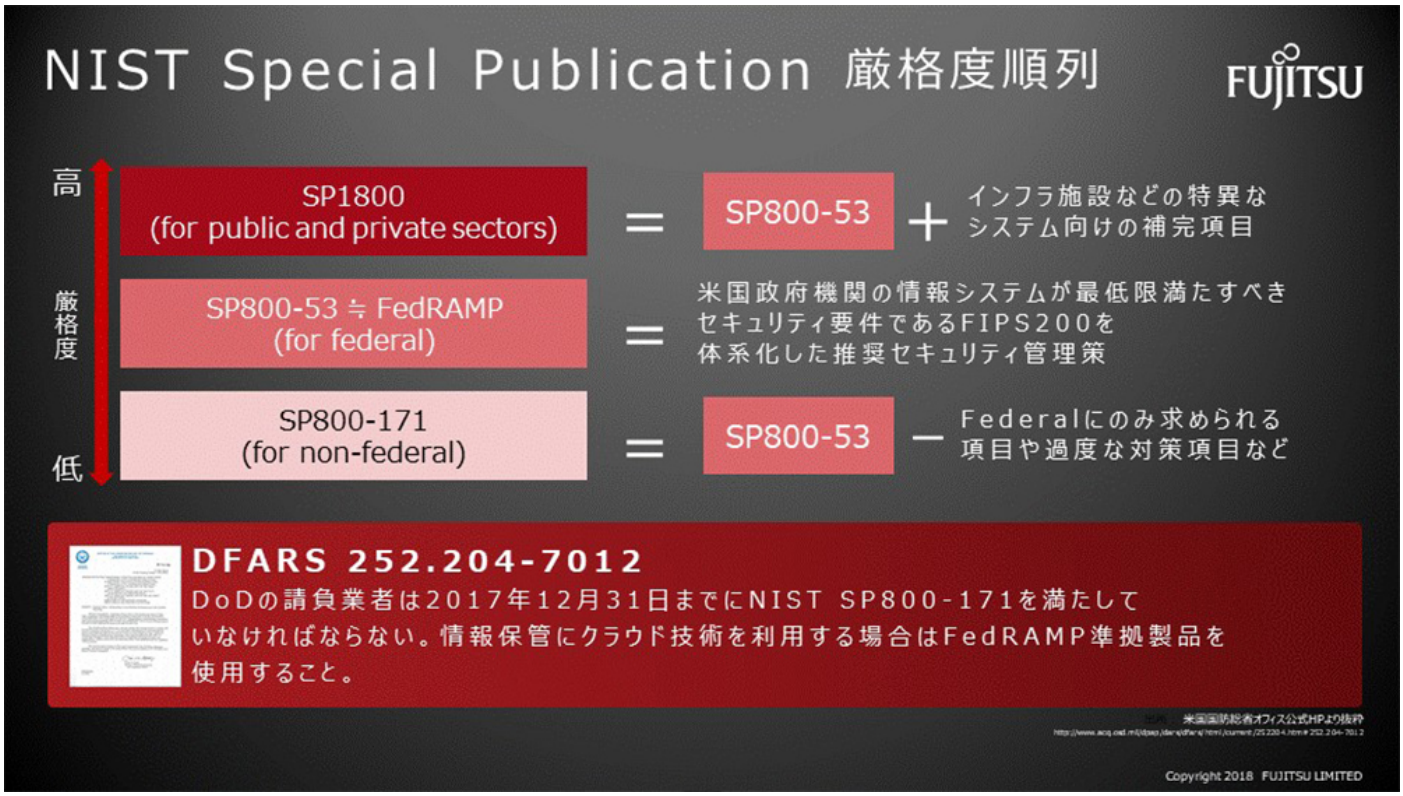
米国・欧州における国際ルール形成の最新動向

サイバーセキュリティの重要性が高まるなか、米国や欧州が主導となり国際ルールの形成が進んでいます。特に、米国では「サイバー空間の覇権は安全保障における絶対条件」として位置づけられています。

そして、2011年には、政府の安全保障戦略として「FedRAMP」という連邦政府共通のクラウドサービス調達のためのセキュリティ基準を制定しました。



また、NIST（米国立標準技術研究所）では「SP800シリーズ」というガイドラインを策定しました。特に民間の産業界を対象にしたセキュリティ対策基準「SP800-171」規約は、それを満たしていない限りサプライチェーンに参加できないという厳しい制約を設けています。



EUでは、2018年5月、欧州委員会によりネットワークと情報システムのセキュリティに関する指令「NIS Directive」、72時間以内の公開・通知義務や多大な罰金制度などの厳しい罰則を適用する「EU一般データ保護規則（GDPR）」がそれぞれ施行されています。

NIS Directiveでは、重要インフラ事業者に対して、最新のサイバーセキュリティ対策を講じることを要請しており、国際基準に準拠することを規定しています。GDPRでは、最大で企業のグループ年間売上高の4%、または2,000万ユーロの罰金を定めるなど、経営側での厳格なガバナンスを要請しています。

「No Security, No Digital」の時代に

このような状況の中、機密情報に関する経営へのインパクトは非常に大きくなっています。記憶に新しいところでは、2018年3月、米Facebook保有の個人情報が英コンサルティング会社に流用された事件が発生しました。個人情報の件数は、発表当初の5,000万人から、最大8,700万人規模になると発表され、Facebookの株価は20%急落し、時価総額で8兆円が消失しました。

サイバー攻撃から機密情報を守ることの重要性が極めて大きくなり、もはや「セキュリティなくして、デジタルなし（No Security, No Digital）」と言えます。

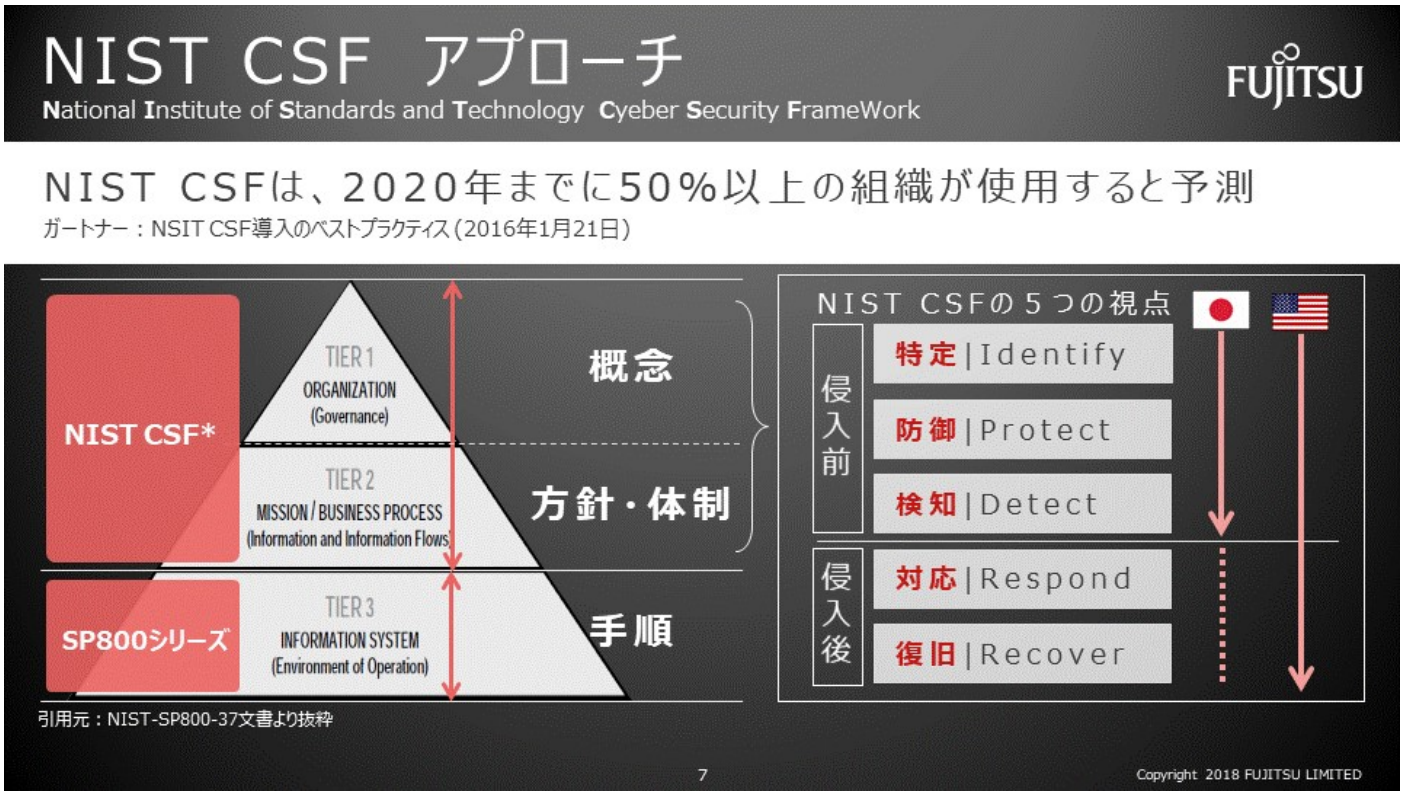
さらにIoTの台頭による新たな脅威は、企業のCSR（社会的責任）にも関わります。その影響範囲はサプライチェーン全体にも及びます。

サプライチェーンは単一企業の問題ではなく、社会全体の問題として捉える必要があります。そのため、サイバー攻撃への対応能力を高めることが求められます。また、各種セキュリティ基準を順守する能力が必要となります。サイバー攻撃を受けることを前提として、その対策に取り組む必要があるということです。

より少ない人材で効果的な対策を

それでは、サイバーセキュリティ対応能力を高めるために必要なこととは何でしょうか。
富士通では米NISTが策定した国際的なルールを正しく理解し、日本がどのように効率的・効果的に対応していくかが重要だと考えています。

NISTはサイバーセキュリティ対策の概念・方針、対策について「CSF（Cyber Security Framework）」アプローチを採用しています。CSFでは、マルウェアの侵入前後を「特定」「防御」「検知」「対応」「復旧」の5つの視点で捉えています。米国と比べて、日本は特に侵入後の対応・復旧の視点が不十分だとされています。



具体的には、標的型攻撃における攻撃者の行動を構造化したフレームワーク、いわゆる「サイバーキルチェーン（Cyber Kill Chain）」への対策です。

日本では多くの企業・組織が、国際的な情報セキュリティ規格群「ISO 27000シリーズ（ISMS）」に準拠する仕組みを確立していますが、CSFの5つの視点からするとサイバーキルチェーンの中には補完すべき領域も存在します。この補完領域を私たち富士通がサポートするべきだと考えています。

また、攻撃者の手法が多様化する中、重要資産を多層防御で守る必要があります。しかし、多層防御には多大なコストがかかり、またその製品の選定や導入に当たっては対応できる人材が必要になります。
ところがIPA（情報処理推進機構）の「IT人材白書2018」によると、IT人材の7割がITベンダーに所

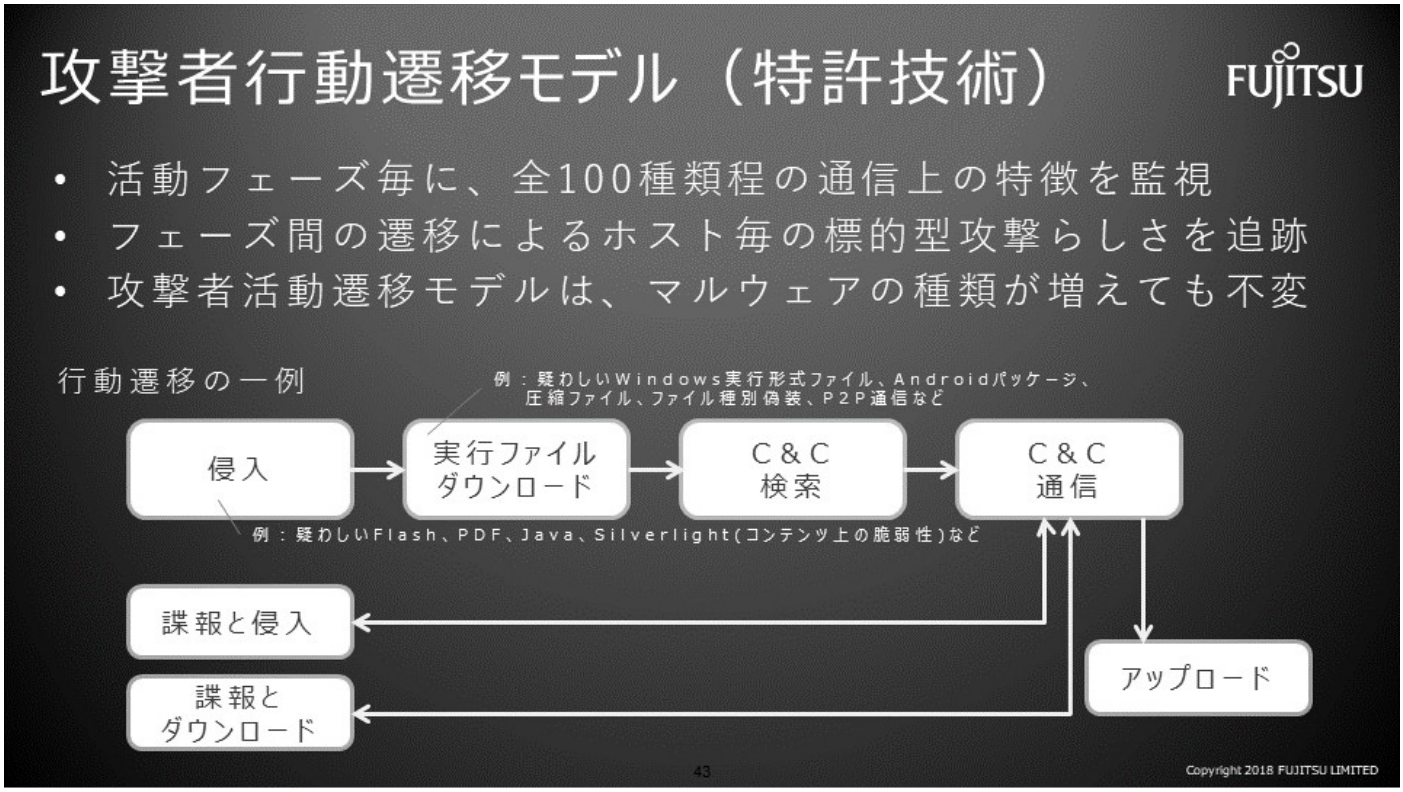
属し、ユーザー企業には残り3割程度しかいません。その比率が逆となっている米国と比べると、日本では人材不足が課題になっていると言えます。また、経済産業省の統計によると、2020年には情報セキュリティ人材が19万3,000人も不足するとも言われています。

こうした現状を受けて、私たちは「より少ない人材で効率的にインシデント対応ができる運用基盤」が必要だと考えました。

独自の着眼点で取り組む富士通の挑戦

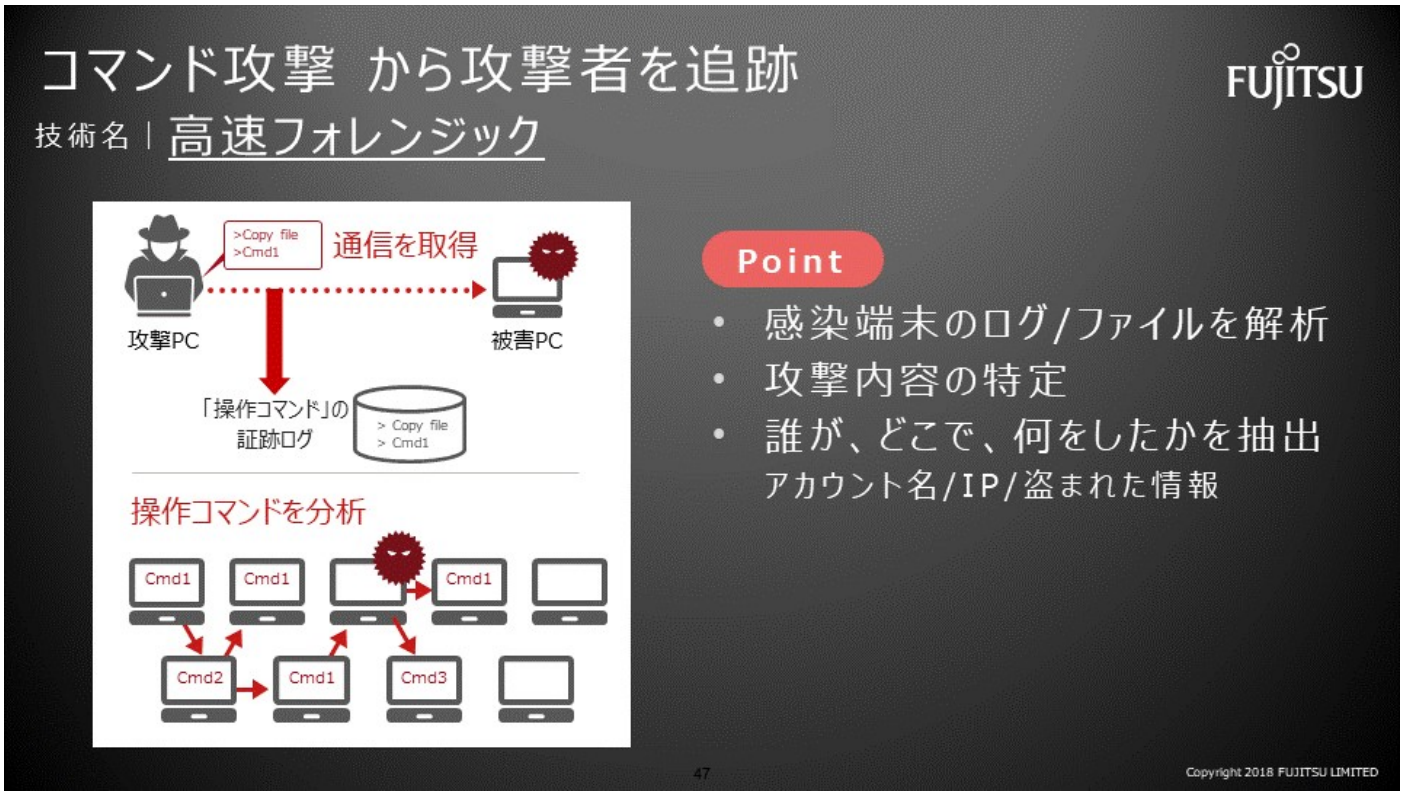
富士通は、これまでとは異なる新しい着眼点のもとで、独自のセキュリティ技術を開発しています。攻撃者が保有するツールや手法は無限に存在するので、探し続けるには多くの労力を要します。そこでマルウェアの振る舞いの分析に労力を費やすよりも、「攻撃者の行動の遷移」を捉え、怪しい行動を攻撃プロセスとして把握する技術を開発、製品化しています。

1つが「攻撃者行動遷移モデル」技術です。攻撃者は一定の行動要素を組み合わせて攻撃します。この技術では、100種類ほどの攻撃パターンの通信上の特徴を監視し、通信遷移から攻撃者を追跡し、時系列で可視化して攻撃の全容を追跡します。従来は高度技術者が行っていた分析がオペレータでも判断可能となるため、対応時間の短縮と人材不足の解消にも効果が期待できます。

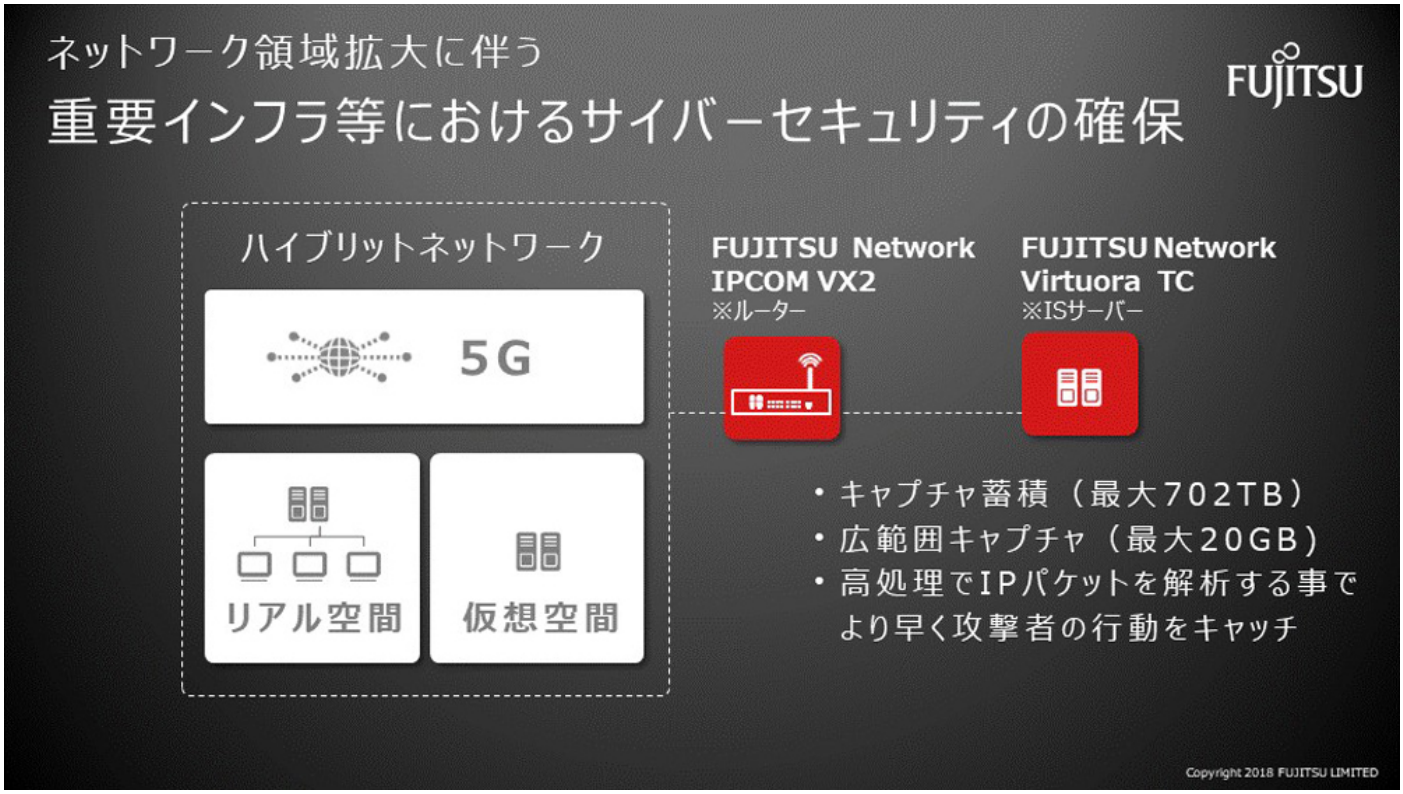


2つ目が「高速フォレンジック」技術です。全てのパケットをキャプチャして、その中から攻撃者が使うコマンドだけを抽出する技術を確立しました。攻撃コマンドを解析することで、その影響範囲を俯瞰して表示でき、攻撃全体を迅速に把握することが可能になりました。例えば、125万

件が流出された日本年金機構の事案でシミュレーションしたところ、実際には約3カ月間かかった調査時間をわずか1時間に短縮できました。



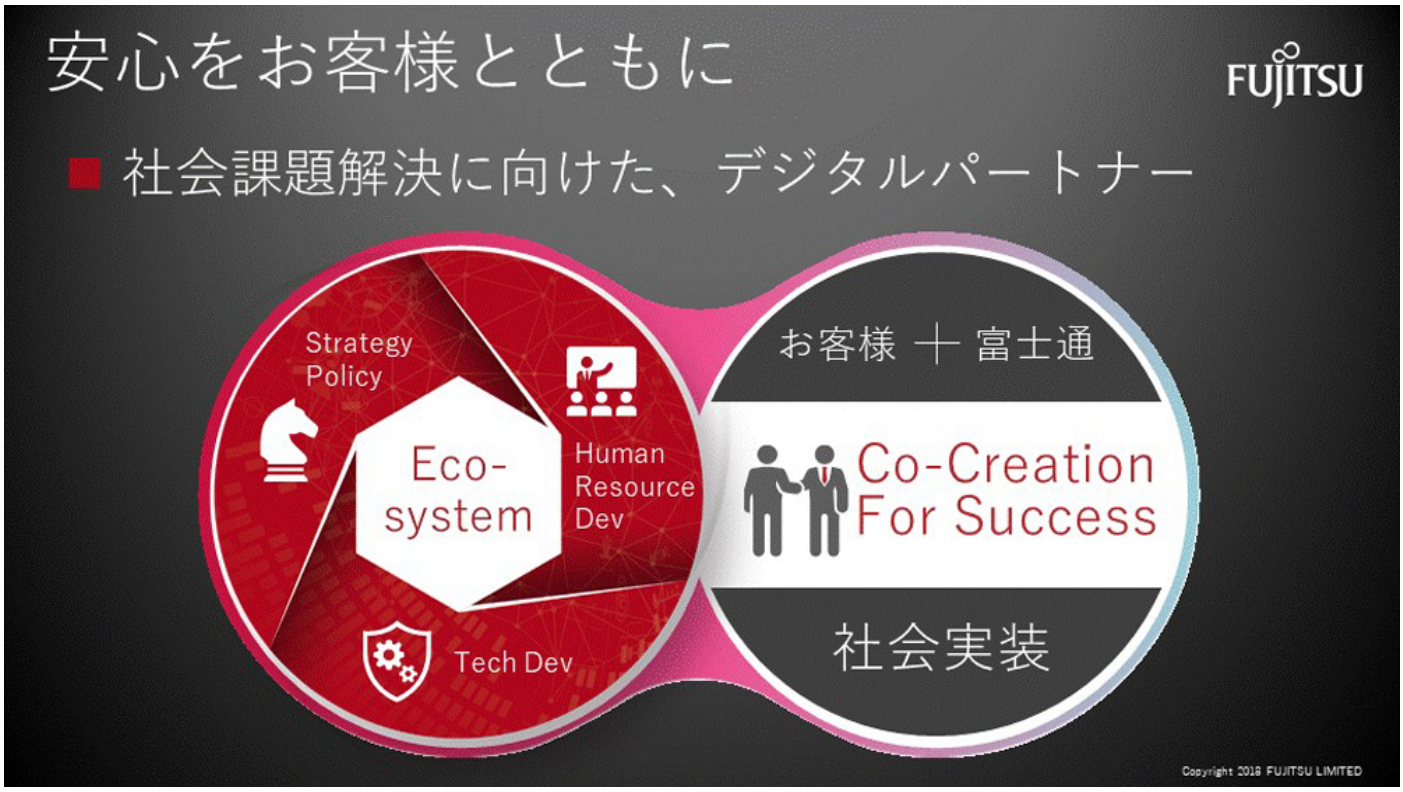
3つ目が「高速パケットキャプチャ」技術です。5G時代を迎える今後、パケットの量が現在の1000倍となり、混入される攻撃も膨大な量になることが予想されます。富士通は、内閣府の戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保（管理法人NEDO）に参画し、仮想空間に張られる仮想ネットワークも対象としたパケットキャプチャの研究に取り組んでいます。



セキュリティなくして「共創」はあり得ない

技術と人材は、産業を発展させるための大きな軸となります。富士通では技術に対する研究開発を進めると同時に、2014年に「セキュリティマイスター制度」を設立して人材育成にも注力しています。

ますます複雑化するサイバー攻撃に備えるためには、攻撃されることを前提と捉えて対策を行うことです。富士通では、セキュリティをビジネスとしてお客様に提供するのではなく、お客様のパートナーとなり、お客様が安心・安全を確保したビジネスを展開できるように支援するというものです。そのためには、セキュリティマイスター制度を通じて、「セキュリティ・バイ・デザイン」を実現できる人材の育成に今後も注力していきます。



私たち富士通は、今後もお客様のビジネスを支えるデジタル革新のパートナーであり続けることを目指します。それを支えるのがセキュリティです。共創（Co-cration）は、セキュリティなくして語ることはできません。これからも富士通は、セキュリティに関する独自技術の開発や人材の育成に取り組んでいきます。

太田 大州
富士通株式会社
サイバーセキュリティ事業戦略本部
シニアエバンジェリスト

FUJITSU JOURNAL / 2018年8月28日