# 深刻化するサイバー攻撃の脅威、AIやブロックチェーン技術で創る「信頼」とは

## データ・システム・人の3つの視点で対策を考える

FUJITSU JOURNAL / 2019年1月30日

日々、深刻度を増すサイバー攻撃の脅威。今、セキュリティ対策技術だけではなく、取り扱う「データ」「システム」、そして「人」が正しいことをいかに確保するかが急務の課題です。2018年12月4日に開催した、セキュリティをテーマとした「Fujitsu Insight 2018」では、デジタル時代の信頼・創造を実現する、最先端のセキュリティ技術を紹介しました。

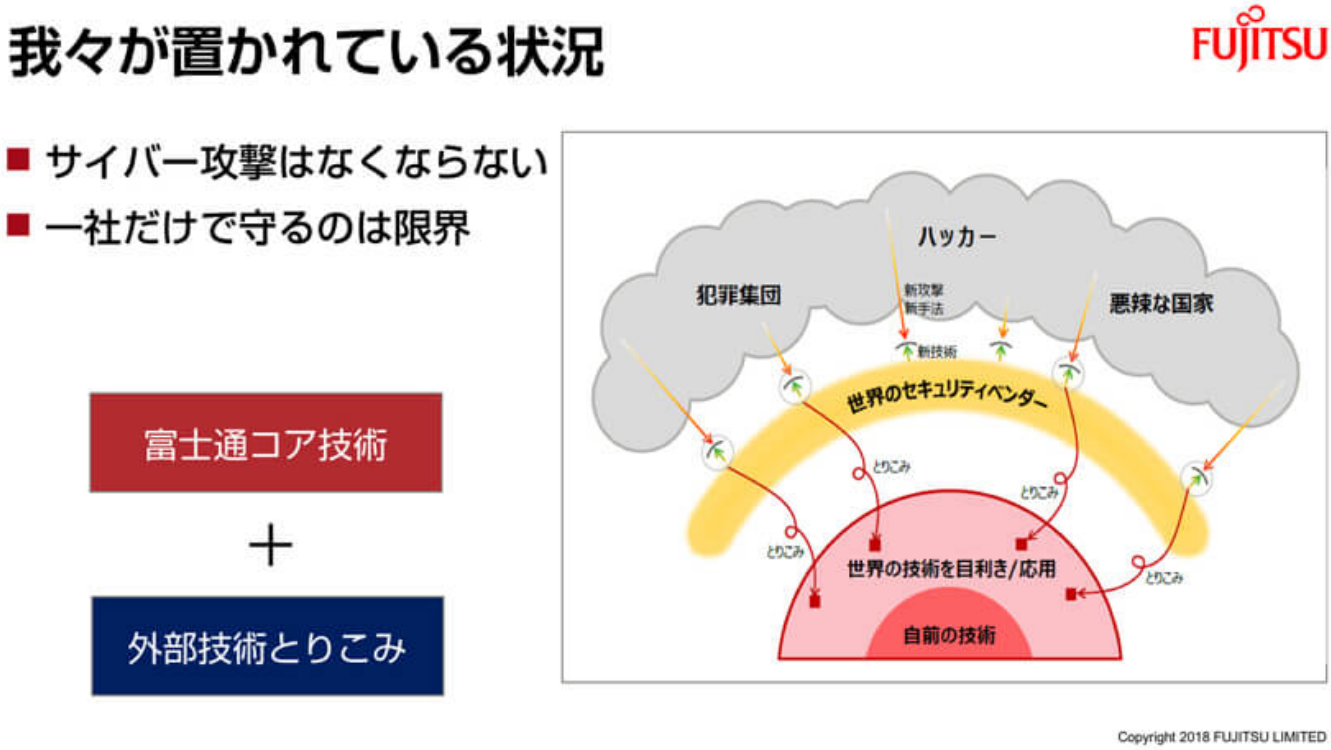
【Fujitsu Insight 2018「セキュリティ」 セミナーレポート】

## デジタル時代のサイバーセキュリティ対策技術最前線、富士通の取り組み

セミナーの冒頭では、富士通の飯島淳一がサイバーセキュリティ対策に関する富士通の取り組みを紹介しました。

富士通株式会社
サイバーセキュリティ事業戦略本部 本部長
飯島 淳一

世界のGDPは約8000兆円で、世界中の企業の純利益は、約400兆円。これに対してサイバー被害は約60兆円で、今や人類の最大の被害がサイバー攻撃と言われています。日々、新たな攻撃が開発され、1社だけの力で守るのはかなり難しい状況です。富士通では、セキュリティーベンダーなど外部技術を取り込みつつ、富士通のコア技術と融合させて、企業や人々が活動するこのデジタル社会を守る取り組みを進めています。




セキュリティ専門の機関や企業との共創が求められている

サイバーセキュリティ事業戦略本部とセキュリティ研究所は、富士通グループ内において一体として運営しています。具体的には両部門のトップが参加して、四半期ごとに戦略協調会議を実施し、戦略やお互いに委託する業務内容について合意し、運営しています。

また、両部門の人材交流も進めています。そして、研究所で開発した技術を富士通のセキュリティサービスに組み込んで提供しています。単なる技術開発にとどまらず、人を育てるための技術を追求していきます。

## デジタル時代の鍵を握る「信頼と創造」

続いて、富士通グループが研究開発しているセキュリティ技術について、富士通研究所の津田宏が説明しました。

株式会社富士通研究所
セキュリティ研究所長
津田 宏

本日のキーワードは「信頼（トラスト）」です。デジタル時代において、信頼がどのような形に変わっていくのか。そして信頼に対して、「データ」や「システム」、「人」の3つの観点で、世の中がどのように変わっていくのか、その研究についても説明します。

富士通は、1976年に「信頼と創造の富士通」というキャッチフレーズを掲げました。当時の信頼は英語ではリライアビリティと表現され、例えば、システムが止まらないといった製品の信頼性や正確性のことでした。

デジタルの時代になって、信頼はリライアビリティだけではなく、トラスト、つまり他社や自社の関係性における信頼へと変わってきました。サイバー攻撃が日々発生している中、製品だけではなく、データやシステム、人も含めての信頼が重視されています。

もう1つのキーワードは、創造、つまりクリエイティビティです。デジタル時代に、ありとあらゆる人、モノがデータとして繋がり、利活用される時代になると、1社ではなく、「Co-Creation」、つまり、お客様と一緒に創造する取り組みが大切になります。こうした考えのもと、セキュリティは「信頼」と「創造」を支える重要なテクノロジーと言えます。

トラスト（信頼）には、3段階があると考えています。トラスト1.0は、人と人とのローカルな信頼です。お金に例えると、物々交換時代に貨幣の役割を果たし始めた貝殻といえるでしょう。トラスト2.0は、組織の制度や契約などによる信頼です。お金で考えると、国が発行する通貨です。トラスト3.0は、例えばブロックチェーンをもとに生み出されたビットコインなどの仮想通貨といえます。国家に依存せず、テクノロジーだけで作った信頼です。これからのデジタルビジネスにおいて、実はセキュリティの技術というのは、このトラストを作り上げる上で非常に重要です。

## データのトラストの重要性、「データテロ」が早晩起きる

富士通研究所では、「人のトラスト」「データのトラスト」「システムのトラスト」をどう守り、保護し、保証するかを考えて取り組んでいます。その中で、データ、システム、人の順番で1つ1つ事例を紹介します。

まずデータのトラストです。考えておかなければいけないポイントは、パーソナルデータや機密データというように、守るべきデータの種類がガイドラインや法律で確実に決まりつつあるということです。サイバー攻撃対策でも、守るべきものだけをちゃんと守るという時代になってきました。

また、AI（人工知能）とセキュリティについても考える必要があります。AIは、学習データが間違ってしまうと、導かれる回答も間違ってしまいます。このAIの性質を狙った「データテロ」は確実に起きるでしょう。AIに学習させるデータをどう守るのか、これがこれからの新しいテーマです。同様に金融から非金融へと応用範囲が拡大しているブロックチェーンのセキュリティも重要な問題です。

データの中でもパーソナルデータは、「21世紀のオイル」と言われています。2011年の世界経済フォーラムでの示された考え方で、オイルとは様々な産業のもとになるという意味です。パーソナルデータを例えば、石油と考えると、国から国への移動、持ち出しなどには制限がかかります。それがEUのGDPR（EU一般データ保護規則）であり、中国のサイバー法です。日本もようやく欧米並みに、データ管理の法整備が進められているところです。

## データトラスト、ブロックチェーン技術でデータの来歴を管理

今後、データのトラストをどのように考えていかなくてはならないのか。富士通は、AIやデータを利活用したい企業が、例えばAIに学習されるデータがどのように作られたのかを確認できる技術を開発しました。これが2018年9月に発表した「Chain Data Lineage（チェーンデータリネージュ）」という技術です。

動画：【ブロックチェーン】業種・業界を超えたデータ流通の信頼性を向上する「Chain Data Lineage」

その際に非常に気になるのが、データの来歴です。データも「原料となるデータ」があって、それに対してまた別のデータが加えられ加工され、あたかもサプライチェーンのようにデータが商品になっていく時代になるでしょう。この流れを全部見せていくとその時にデータを誰がどういじったかというような情報を全てこの改ざんできないブロックチェーンの中に管理していく発想です。

また、データの中にはパーソナルデータのように、本人の同意が必要なデータもあります。こうしたデータについては自動的に判別して、本人の同意がなければ提供できない仕組みも考えました。

## システムのトラスト、 攻撃のログを短時間で解析

システムのトラストの実現については、「高速フォレンジック」という技術があります。フォレンジックスというのは、ハードディスクのログなどを確認し、「どのように犯罪が行われたか」を分析する技術です。


サイバー攻撃、特に標的型攻撃では、マルウェアを送って、感染させてから外部から侵入し、社内を探しまわって重要なデータを盗み出します。高速フォレンジックでは、証跡ログをとり、さらに操作コマンドを分析することで、攻撃がなされたことの証拠や、その攻撃者が何をやったのか、攻撃の手口を明らかにすることができます。これらを高速で実行できるのが特長で、従来ではサーバのログを解析するなどに3カ月くらいかかっていましたが、そういった調査や分析をほぼ1時間でできることを実証しました。これは、総務省の情報通信研究機構との共同研究、共創の事例でもあります。

また、攻撃者の活動を「グラフデータ」として表現して学習するAI技術も適用しています。「Deep Tensor®（ディープテンソル）」という富士通のAI技術を使ったマルウェア分析です。これまでのAIでは苦手とされていた、人が判断に利用していた「グラフ」データを、Deep Tensor®で学習させることで、高精度な分析と検知が可能になりました。オープンデータを活用した事例で

は、精度97%という高さを実現しています。将来的には、この技術も組み合わせてインシデントの管理を可能な限り自動化していこうと考えています。

## 人のトラスト、高まるアイデンティティ管理の重要性

最後のトピックこれは、「人」です。本人の認証など、アイデンティティの管理が重要になります。日本もキャッシュレスの時代になりますが、そういった時代にこそ、本人認証が重視されます。

ただし、スマートフォンやパソコンでのログインに使用する生体認証は、その機器を持っている人が本物かどうかをチェックするだけの認証です。それがこれからの時代には、何万人という人の中から本人であることを判定してくれる生体認証技術が求められます。

富士通の手のひら認証技術や指紋認証技術でも、1万人くらいの人の中から本人を特定することができますが、これを増やすにはどうしたらいいか。生体認証もマルチの時代になります。普段は顔だけども、必要な場合は例えば指紋や静脈などを使うという選択です。そこで、顔認証と静脈認証を組み合わせました。この二つの技術を融合させることにより、100万人規模の「手ぶら決済」などを実現できるようになりました。

動画：顔認証と手のひら静脈認証で「手ぶらで簡単決済」

## サイバー空間における「信頼の輪」を広げる

サイバーセキュリティにおけるリスクをマネージメントするためには、事象を把握して、データを収集し、これを可視化することが大前提になります。こうしたマネジメントサイクルを支える三つの要素が、「正しいデータ」「健全なITインフラ（システム）」、そして「適切な範囲の共有（人）」です。富士通グループは、健全なサイバー空間の利用環境の維持について、お客様、パートナー様との信頼の輪を広げて、守っていきたいと考えています。

## 登壇者

富士通株式会社
サイバーセキュリティ事業戦略本部
本部長
**飯島 淳一**

株式会社富士通研究所
セキュリティ研究所長
**津田 宏**