ホワイトペーパー

Trust-Enhanced Networking

サイバー・リアルを繋ぐネットワークによるトラスト

（概要）メタバースや Web3 の普及とともに、企業や社会の活動がサイバー空間へシフトしていく中で、様々なステークホルダとの関係を構築していくには、サイバー空間上での信頼性の根拠となる情報を新たに確立していく必要があります。本ホワイトペーパーは、サイバー空間とリアル空間を繋ぐのに必要不可欠なネットワークの新たに担うべき役割として、リアル空間におけるフィジカル情報の裏付けによってサイバー空間にトラストをもたらす"Trust-Enhanced Networking"というコンセプトを示します。

1. はじめに

現代社会の情報インフラはネットワークに深く依存し、様々な情報がデジタル化され、インターネットを介して流通するようになりました。また、スマートフォンの急速な普及と、SNS (Social Network Service) や EC (Electronic Commerce) を始めとするオンラインサービスの発展によって、人々は常にインターネットに繋がる状況になっています。今後、更なる IoT (Internet of Things) や AI (Artificial Intelligence) の進展、それらを活用したサービスによって、人々のあらゆる活動がサイバー上で行われる「サイバー社会」に向かっていくと考えられます。

このサイバー社会を安全に、かつ安定的に実現していくために、インターネットの機能や構造は日々変化しています。その変化の中で筆者らは、２つの変化に着目しています。

１つ目の変化は、企業・組織におけるデータの保管場所が、企業・組織自身の機器で構成される「オンプレミス」から、クラウド事業者が提供する「クラウド」へ移行していることです。クラウドサービスは今日の市場に十分に浸透し、企業や組織の多くのデータは複数のクラウド上に点在・混在しています。データの所有者である企業・組織は、クラウド事業者やその背後にある法制度への信頼を元に、クラウドサービス上に自身のデータを保管しています。

２ つ目の変化は、メタバースに代表される仮想空間上で展開される企業・社会活動の顕在化です。オンライン会議ツールや電子契約は、既に私たちの生活に浸透していますが、数年後には同様にメタバース上でのビジネス活動が浸透するでしょう。そのとき、実世界における様々なビジネスは、仮想空間上で実行されます。仮想空間上では、実世界における国や地域を飛び越し、グローバルを跨いだ多様なステークホルダとの関係を構築し、新しいビジネスを創造していくと考えられます。

一方、これらの変化に関連して、世界情勢の変化とそれに対応した法制度にも着目する必要があります。2018 年に欧州で運用が始まった「EU 一般データ保護規則（General Data Protection Regulation：GDPR）」や、経済安全保障のデータ保護の観点から、実世界における地理を意識したデータのガバナンスについての重要性が増しています。

「クラウド」や「仮想空間」を中心としたサイバー社会において、企業・組織が安心して活動を行うには、データの越境移転問題や相手の地理的位置といった実世界に関わる懸念も考えていく必要があります。そこで、著者らは、これまでのサイバー空間のトラストだけではなく、実世界との接点であるネットワークの視点からの新たなトラストが必要になると考えます。

富士通は、社会的責務として IDYX 技術 [1]、CDL 技術 [2]および透過的トラスト技術 [3]といったデジタルトラストの研究に取り組んでいます。本ホワイトペーパーは、今後の社会変化に伴って発生する課題に対して、将来のネットワークがどのような役割を果たしてサイバー社会におけるトラストを支えていくかについてまとめたものです。

2.サイバー社会におけるトラスト

2.1.フィジカルを含むトラストについて

データが本物であること・改ざんされていないこと、及びデータが（データの所有者、正当なユーザの）意図しない状態におかれていないこと・使われ方が意図通りであること、「デジタルトラスト」はこれらを保証します。

クラウドや仮想空間の利用が進んだサイバー社会では、アクセス認証や暗号化といったセキュリティ技術・手段に加えて、実世界におけるフィジカルな部分を含む考え方がデジタルトラストにおいて重要になると考えます。例えば、オンライン上でデータが国や地域を跨って送受信される際に、送信者・受信者の国や地域の法制度にそぐわないケースが出てくる可能性があります。また、オンライン会議ツール等の仮想空間上において

商談相手として話している人物が実際にはその相手が居るはずのない国や地域に住んでいる無関係な人物で、商談相手に送ったはずの重要な情報を悪意のある人物に盗み取られるという可能性もあります。

このように、サイバー空間上のデータや商談相手の「地理的な問題」はサイバー社会が進展した場合においても重要になると考えられます。サイバー社会のデジタルトラストの実現には、データにアクセスする相手やデータを格納するクラウド事業者のデータセンターの地理的な位置や、データが通過するネットワークの信頼性を考慮して議論する必要があります。

では、サイバー社会においてデジタルトラストを確保するために、どのような実世界のフィジカル情報が必要でしょうか？一つには、サーバやルータ、端末などネットワークを構成する各々の装置が置かれた地理的な位置を示す「位置情報」があります。サイバー空間上における商談相手が使用している端末の正しい位置を把握できれば、商談相手になりすました「悪意ある人物」に重要な資料を送ってしまう可能性は格段に減るでしょう。また、装置の設置場所を把握できれば、データの保管・送受信においてユーザが信頼するネットワークを指定する、ということができるようになるでしょう。

著者らは複雑に進化するサイバー社会を支えるデジタルトラストを実現する手段として、ネットワークや複数のクラウドに分散する装置、ユーザ資産であるデータが格納されているサーバ・ストレージの地理的位置の正しい把握と活用が不可欠であると考えています。

2.2.ネットワークにおける課題

一般にネットワークにおける位置情報というと、GPS (Global Positioning System) や携帯端末が接続している基地局に基づく情報がすぐに思い浮かびます。これらは、地図や天気などのアプリケーションで広く使用されています。また、アプリケーションだけでなく、サーバ・ルータなどネットワークを構成する装置の位置情報は、トラフィックの経路最適化などネットワークの運用管理・制御にも利用されています。それらには、IP アドレスとそれを有する装置の位置情報のペアを提供する IP Geolocation と呼ばれるデータベースサービスが使われています。

しかし、その位置情報は信頼できるものでしょうか？例えば、IP Geolocation のサービスで得られる位置情報は、運用者や接続するネットワークプロバイダ、VPN（Virtual Private Network）などのリモート接続サービスの利用有無などで容易に変わってしまいます。携帯端末で広く使用されている GPS についても、端末上で位置を偽装するツールがすぐに見つかります。著者らは、既存の位置情報では、「信頼性の根拠」として利用することは難しいと考えています。

通信経路についてはどうでしょうか？ 現在のネットワークでは、利用者が送ったデータがどのような経路を通って相手に到達したかを利用者自身が確認することは困難です。さらに、悪意を持った攻撃者もしくはオペレーションミス等によって誤った通信経路がインターネットに広告されることで、データが本来あるべき経路を通らないといった問題が発生します。

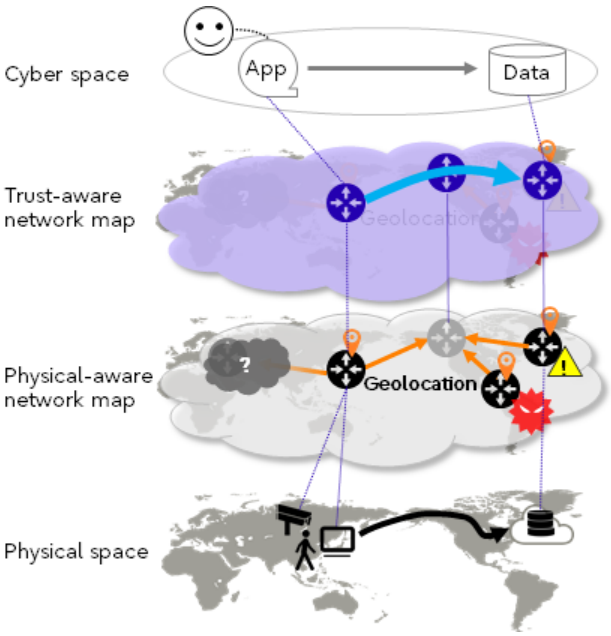

図 1 Concept of Trust-Enhanced Networking

サイバー社会におけるデジタルトラストの実現には、通信経路の安全性・信頼性情報を収集し、ユーザである個人・企業に提供することで上記のような問題を解決する必要があります。

3. Trust-Enhanced Networking

著者らは、今後のサイバー社会のデジタルトラストの強化に向けて、ネットワークが新たに担うべき役割として、フィジカル空間の裏付けによってサイバー空間での活動にトラストをもたらす "Trust-Enhanced Networking"というコンセプトを提唱します。

ネットワークは、多数のネットワークプロバイダとの接続関係や SDN (Software Defined Networking), NFV (Network Functions Virtualization) といった仮想化技術の適用により、柔軟で効率的なデータの送受信が可能になった一方、サイバー空間から見てブラックボックスで不透明なものとなってきました。提唱する"Trust-Enhanced Networking"では、可能な範囲でネットワークの地理的な要素を信頼できる情報としてサイバー空間で活用できるようにするとともに、ネットワーク自身をユーザにとってトラスタブルにすることを目指します。例えば、フィジカル空間の携帯端末等のエンドデバイス、通信を中継するルータ等のネットワークデバイス、データを管理するストレージなどの位置情報を検証できる形でサイバー空間に提供することや、これらの地理的な位置も考慮した新しいトラスタブルな経路制御を行うことなどを想定します。

そのために"Trust-Enhanced Networking"では、図 1 に示すように、フィジカル空間とサイバー空間を繋ぐネットワークにおいて段階的なマッピングを行います。最初のマッピングにお

ける"Physical-aware network map"では、エンドデバイスやネットワークデバイス、それらをつなぐリンクの地理的位置の検証を試みます。次の"Trust-aware network map"では、"Physical-aware network map"にて検証されたネットワークに対し、サイバー空間のユーザからのトラストへの要求に基づき、地理的な位置も考慮したネットワーク制御を実行します。

以下に、それぞれのマッピングについて説明します。

3.1 ネットワークの位置検証

サイバー空間におけるトラストの判断材料としてネットワークを活用するために、地理的位置やデバイスの真正性など客観的な信頼性の観点でネットワークデバイスを評価し、"Physical-aware network map"を構成します。そのためには、エンドデバイスの位置情報、またネットワーク中のルータなどネットワークデバイスの位置情報の検証ができることが必要です。

しかし、現状、あらゆるデバイスの位置情報を検証できるわけではありません。信頼できるネットワークプロバイダ等のソースの裏付けから地理位置を確認できる場合もあれば、地理的位置の推定により、ある程度の位置を絞り込める場合もあります。一方で、地理的位置のヒントがまったく取得できない場合もあれば、悪意ある攻撃に晒され検証が困難なデバイスなどもあります。

このように、ネットワークデバイス自体の真正性に関する信頼性の度合いに濃淡があるだけでなく、ネットワークデバイスの地理的位置に関する確度にも濃淡があります。提唱する"Trust-Enhanced Networking"の試みの一部分は、技術的に位置検証の可能な対象範囲を広げること、そして、その位置検証の確度を高めることです。

3.2.トラスト指向のネットワーキング

経路制御やフロー制御といったネットワーキングにおいて、著者らは QoS (Quality of Service), QoE (Quality of Experience) に次ぐ新しい概念として、QoT(Quality of Trust) を導入します。

QoT は、個人・企業などのユーザやサービス・アプリケーション、転送されるデータごとのネットワーキングの要素に対して定義され得る指標です。例えば、ネットワークデバイスやそれらをつなぐリンク、データを保持するストレージに対する QoT を設定したとき、それぞれはユーザが主観的にそれらをどの程度信頼できそうかを定量的に表現したものです。前述の"Physical-aware network map"からの情報や、ユーザからのネットワーキングのトラストに関する主観的な要件などを入力として QoT を算出することで、トラスト指向の"Trust-aware network map"を導出することができます。これはユーザやサービスごとの主観により異なり得るものです。

そして、"Trust-aware network map"に基づいてトラスト指向のネットワーキングを実現します。例えば、ユーザにとってトラスタブルなネットワークデバイス、安心できる地域のみを経由する経路選択などが考えられます。

4.まとめ

今後進展するサイバー社会における企業や社会活動において、デジタルトラストは益々重要となってきます。これまでのネットワークは、フィジカル空間でデータを運ぶ役割でしたが、今後のネットワークは、サイバー空間の状況や要求に応じて、実世界におけるフィジカルの裏付けを提供し、デジタルトラストを強化する重要な役割になると考えています。その役割を担うためには、３章で示したような新しいネットワークの実現が必要です。また、サイバー空間でのトラストをより強固にするには、ネットワークだけでなく、サイバー空間上のデータへの裏付け等の付加情報を管理・提供することで、データの確からしさを検証可能な Trustable Internet [4]をはじめとするトラスト基盤や技術との連携も重要になってきます。筆者らは、これらの推進に向けて、様々な企業や大学と協調しながら、今後の社会に必要となるデジタルトラストの技術開発を進めてまいります。

参考文献

[1] IDYX：IDentitY eXchange の略。複数の企業などに分散している個人のアイデンティティ（ID や属性情報など）を、安全に企業・個人間で流通する当社技術。
https://pr.fujitsu.com/jp/news/2019/07/4.html

[2] CDL：Chain Data Lineage の略。データやモノの流通過程や加工処理を起源にまで遡り追跡できる当社技術。
https://pr.fujitsu.com/jp/news/2018/09/20-1.html

[3] 透過的トラスト技術：企業や政府省庁の間でやり取りを行うビジネスデータの作成・承認における改ざんを防ぎ、その真正性を保証する当社技術。
https://pr.fujitsu.com/jp/news/2020/10/6.html

[4] Trustable Internet：インターネット上のデータの確からしさを汎用的かつ容易に確認可能とする技術のコンセプト。
https://pr.fujitsu.com/jp/news/2022/10/13.html

お問い合わせ先

富士通株式会社

データ&セキュリティ研究所

contact-nwt@cs.jp.fujitsu.com