IIJ. news

IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan.
Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry.
The history of IIJ is indeed the history of the Internet in Japan.

October 2020
VOL. 160

特集 Zero Trust Architecture ゼロトラスト

IIJ. news
October 2020
VOL. 160

ぷろろーぐ

働き方

株式会社インターネットイニシアティブ
代表取締役会長
鈴木 幸一

子供の頃から、学校が決めたルールに従わず、宿題をやってこないに始まって、生徒であれば当たり前になすべきことをせず、怠惰ゆえの余計な抵抗をしては、廊下に立たされる、黒板消しで頭を叩かれるなど、教師から無駄に叱責されていた。およそ物事を杓子定規に決めることに馴染まない性格だったようだ。例えば、夏休みの宿題をさぼることで、二学期の最初の一日、二日は、教師の厳しい怒りを買うのだが、その代償として、より自由で重石（おもし）のない、解放された夏休みの時間を得ていた。大人になっても、その性格は変わらないが、一方で、普通の人があまり気にならないことについては、古臭いというか、保守的な反応をするようだ。

最近、呆れられているのが、新型コロナウイルスの感染に対処するために実施されている在宅勤務に対する反応である。三〇年も前から繰り返し書き、話をしているのだが、インターネットの普及によって時間と空間のコンセプトそのものが変わり、わが社の社員も七〇パーセント近くが在宅勤務となって、逆に将来が心配になってきたのだ。オフィスに出勤しなくとも、クラウド化・高速化するネットによって、過不足なく仕事をこなすことができる。確かに、過不足なく業務に対応できることは指摘されるまでもなく、なにより、自ら推進してきたことでもあるので、言われるまでもないのだが、業務を回すだけで、若い人の能力が弾けるのか心配である。人が育って、化けてくれない限り、企業の発展はないのだと、ぶつくさ呟くのである。

オフィスまで往復する時間を考えると、在宅勤務によって浮いた時間を利用して、毎日、二時間以上は勉強できる。オフィスの空間も節約でき、コスト削減につながる……等々、あっという間にその利点を箇条書きできるのだが、そのようなメリットだけでは、将来の企業の成功を支えることにはならないのだ。そして、メリット・デメリットを議論しているうちに、面倒になって打ち切ってしまう。

毎朝、混んだ電車に揺られて、オフィスにたどり着き、夜遅く、疲れた身体を一時間以上もかけて自宅まで運んでいく労力を考えるなら、できる限り在宅の割合を増すことで、働き方改革になり、生活の質そのものが豊かになるのだと言われると、いち早くネットの商用化を手掛けた私は、そこで逡巡するのだ。

朝の通勤電車が駅のホームに停まると、すでに満員の車両から人があふれ出てくるので、そこを押し返して、ぎゅうぎゅうの車両に乗り込む。ドアを閉めるために、バイトさんが乗客を押し込んで、やっとドアが閉まり、発車する。そんな働き方が良かったとは、口が裂けても言えないが、それが奇跡の経済成長を続けていた時代の働き方であり、いかにも時代を象徴しているようなものだった。形が内実を決めてしまうというのはよくあることで、ネットの利用による在宅勤務という働き方は、今の日本の若者の内実に似合っているのかもしれない。

昔、といっては言い過ぎだが、一九九〇年代、シリコンバレーに行くと、「今週はほとんど眠ってないし、家にも帰っていない。土曜日には家に戻らないと、女房に逃げられてしまう」――コーラの大きなペットボトルを抱えた若者と、長い時間、話し込んだものだった。あの働き方とシリコンバレーの空気が、私には居心地のいいものだった。

イラスト／末房志野

TOPICS

Zero Trust Architecture
ゼロトラスト

「ゼロトラスト」、つまり「全て信頼できない」ことを前提にする
セキュリティモデルが注目を集めている。
本特集では、この新しい考え方が生まれた背景から、
ゼロトラストを正しく理解するためのポイント、
企業ネットワークでゼロトラストを実現するためのアプローチまでを徹底解説する。

特集イラスト／高橋 庸平

新しい働き方に対応したセキュリティモデル
ゼロトラスト

クラウドシフトが進むことで情報資産が分散配置され、利用形態も多様化している。
そこで登場したのが、従来の境界防御型のセキュリティモデルを見直し、
新しい働き方に対応したセキュリティモデル「ゼロトラスト」である。

IIJ プロフェッショナルサービス第一本部
プロフェッショナルサービス３部 部長
井本 直樹

ワークスタイルの変化

新型コロナウイルス感染症が拡大するなか、二〇二〇年四月七日の緊急事態宣言を受けて、企業のテレワーク活用は一気に拡大しました。感染症の終息時期は誰にも予測できない状況ではありますが、今回の経験を踏まえて「仕事＝オフィス」という前提を捉え直し、テレワークは今後、恒久的な業務手段として定着する見通しとなっています。テレワークは、平時での利用であれば生産性を上げる有効な手段であると言われており、国際的に見ると労働生産性が低く、労働者人口の減少による人手不足がいっそう深刻化するであろう日本においては、新しい働き方の選択肢としてその活用が強く求められています。

デジタルワークプレース

今後、五～一〇年で企業内の業務システムは、DX（デジタル・トランスフォーメーション）の流れもあり、「クラウドシフト」が加速すると考えられます。それにともないこれまで企業内にあった業務システムがクラウドサービス上で稼働することになるため、従来のネットワークセキュリティの考え方や対策を見直していく必要が出てきます。

SaaSなどのクラウドサービスは、機能・利便性が企業にとって魅力的である反面、利用サービスのコネクション・トラフィックの増大による負荷がかかるため、利用時に従業員がストレスなく仕事に集中できるITインフラ整備が不可欠となります。また、いつ・どこでも仕事ができるようになると、オフィス外で利用するデバイスの紛失やウイルス感染などによる情報漏えい対策も必要になります。さらには、「働き方改革」によるテレワークの活用やクラウドシフトを通して生産性向上に資する手段が充実していく一方、情報システム部門は、システム管理者・従業員それぞれの目線で、どのように運用・管理していくのかを検討しなければなりません。

こうした背景から、デジタル技術を最大限に活用して、「あらゆる場所・時間・デバイスから仕事ができる環境」を実現する「デジタルワークプレース」による課題解決が注目されています。

恒久的なテレワークに向けて

テレワークが急速に広がったことで、ITシステム部門がどのような課題に直面し、どのようなIT投資計画を考えているのか？――これらに関して、IIJはアンケート調査を実施しました。

アフターコロナ時代のIT投資の方向性として、再び同じような状況が発生した際に現在のITシステムで乗り越えられそうかという問いに対しては、「まったく問題ない」「問題ない」を合わせた回答は三割程度にとどまっています。また、今後IT投資を強化したい要素としては、テレワーク環境に関するものが上位を占めました。（アンケート調査の詳細は、16・17頁「IIJ Research　となりの情シス」参照）

こうした現状は、「緊急措置としてテレワークに踏み切ったが、セキュリティレベルをこれまで通り維持したい」「オフィス一極集中を避け、どこからでも安

界防御型」のアプローチだけでは限界があります。そこで、これを解決する手段として「ゼロトラスト」というセキュリティモデルが登場しました。

ゼロトラストとは

ゼロトラストは、アメリカの調査会社 Forrester Research が二〇一〇年に提唱した考え方です。従来の境界防御型は、保護すべき情報資産が境界内ネットワークにあり、アクセスは境界内ネットワークからに限られ、脅威を内部に侵入させないというセキュリティモデルでした。しかし、アメリカの大手通信会社で当時発生した大規模な情報漏えい事件では、境界内ネットワークに属する内部ユーザの権限を悪用することで、組織の情報資産が剽窃されました。

これを機に、境界内ネットワークは安全であるという前提のもと境界で防御するセキュリティ対策には限界があり、境界の内外を問わず全ての動きを検証し、リソースの安全を確保するために常にアクセスコントロールを行なう、言い換えると「全て信頼できない」ことを前提とするセキュリティモデルが生まれました。

ゼロトラストは技術規格の標準化を支援するアメリカ国立標準技術研究所（NIST）が発行している「SP 800-207」のなかで提唱されています。そして、さまざまな議論を経てアップデートされ、二〇二〇年八月に最終版が公開されました。

そこでは、実装手段そのものを定義するのではなく、「実現にはさまざまな実装形態がある」と記述されており、ポイントは左記の通りです。

●全てを信頼しないという前提に立った時、どのようにアクセス元を信頼すべきか。
●ポリシーの定義ポイント・実行ポイントを一箇所に決める。
●アクセス許可ポリシーは、周辺システムから得られるさまざまな情報を用いて、動的に定義・実行する。

ゼロトラストの現状

最近、海外メーカを中心に「ゼロトラスト」をキーワードとした製品やソリューションが出ています。そこでは、各社が得意とする領域（IDaaS、EDR／MDM、CASB、仮想ブラウザ、FW／UTMやWEBプロキシなど）をベースに「これがゼロトラストである」とバズワード的に使用される傾向があり、情報システム部門はどういった対策をとるべきかわからず、誤解を招いている状況が見られます。そこで重要になるのは、どの目線でゼロトラストに対応しているか？　という本質を見抜くことです。

他方、従来の境界防御型を否定するようなメッセージも散見されますが、「SP 800-207」では、境界防御型がなくなるわけではないとされています。例えば、テレワークの活用が加速する一方、業務継続に与える影響などを懸念して、テレワークの適用割合を一定レベルに留めている企業も依然として多くあります。この場合、テレワークでの業務とオフィスでの業務が共存するかたちとなり、オフィス中心の業務においては、これまで通り、境界防御型によるセキュリティ対策も有効となります。当面は新型コロナウイルス感染症による影響レベルの見方が不確実であり、テレワークの適用割合を変化させるといったコントロールを行なう企業が多いと想定されます。

「あらゆる場所・時間・デバイスから仕事ができる環境」を実現するデジタルワークプレースの利活用が進むなか、境界防御型も活かしながら、ゼロトラストを従業員の働き方に合わせてうまく取り込んでいけるITインフラの整備が求められているのです。

こうしたゼロトラストの現状を踏まえ、本特集では技術的な解説やIIJが実現するゼロトラストについて紹介します。

まず「NIST」が提唱するゼロトラスト」では、NISTが示しているゼロトラストの技術面を解説します。次に「ゼロトラストのポイント」では、セキュリティサービスを提供する立場としてIIJが目指すゼロトラストの技術面にフォーカスします。続く「デジタルワークプレースで実現するゼロトラスト」では、IIJがこれまでに培ってきた豊富なマネージドサービスの提供実績などをもとに、ゼロトラストの課題を解決するデジタルワークプレースについて述べます。またコラムでは、混乱しがちなSASEとゼロトラストの違いと、工場IoT領域などでゼロトラストとしてIIJが提供するFSEGに触れます。

SASEとゼロトラストは、どう違うのか？

IIJプロダクト本部 SDN開発部 シニアプロダクトマネジャー
水野 正和

SASEとは

SASEはSecure Access Service Edgeの略で、そもそもは、2019年8月のGartner社のレポート「The Future of Network Security Is in the Cloud」*で登場した用語です。さまざまなセキュリティ機能やネットワーク機能を融合し、包括的にクラウドサービスとして提供することを目指しています。その背景には、企業のクラウド活用の拡大があります。クラウド活用が進むと、守るべき情報資産が社内だけでなく社外にも多く存在することになり、資産へのアクセスもさまざまな場所から行なわれます。SASEは、このような変化に対応しようとするものです。

ゼロトラストとは

ゼロトラストは「決して信頼せず、常に検証する」というセキュリティの考え方・概念です。詳細は、本特集の各論をご一読ください。

SASEとゼロトラストの違い

SASEもゼロトラスト同様に、守るべき資産が社内だけでなく社外にも多く存在する環境において、いかに重要資産を守るか、について論じています。では、解決したい状況が同じSASEとゼロトラストの違いは、どこにあるのでしょうか？

結論から述べますと、ゼロトラストはSASEの中心となる考え方です。企業などの組織がゼロトラストを実現していくための方法論がSASEです。

本特集の記事にもある通り、例えば、NISTの「SP 800-207」は、ゼロトラストの原則や論理コンポーネント、機能モデルの説明が中心で、セキュリティの特定分野に焦点をあててはいません。一方、上述したGartner社のレポートには、「SASEが提供する機能は、IDやリアルタイムコンテキスト、企業のセキュリティポリシー、そして継続的な評価にもとづいたサービスとして提供される」と記されており（これはゼロトラストの考え方と同じです）、さらにSASEのキーテクノロジーとしてSD-WAN、SWG、CASB、FWaaS、ZTNAなどのネットワーク機能やセキュリティ機能が挙げられています。さらに、SASE提供ベンダの例も記載されているなど、導入を検討しているユーザにとって、より具体的な記述となっています（ただし、SASEの範囲は広く、全てをカバーする製品やサービスは現時点ではまだありません）。

余談になりますが、SASEのキーテクノロジーの1つとしてZTNA（Zero Trust Network Access）が挙げられており、同じ「Zero Trust」という言葉があるため、SASEとゼロトラストの関係を理解するのが少々ややこしくなっているかもしれません（もしかしたら、ゼロトラストはSASEの一部であるかのように思われている方もいらっしゃるかもしれません）。ZTNAは、ゼロトラストの世界を実現するための技術の1つであり、ベンダや取り上げられる文章によってはSoftware-Defined Perimeter（SDP）として表されることもあります。認証済みのユーザ、デバイス、アプリケーションのみを、組織内の他のユーザ、デバイス、アプリケーションへアクセス許可する、というセキュリティ機能です。

＊ Gartner, The Future of Network Security Is in the Cloud, 30 August 2019, Neil MacDonald, Lawrence Orans, Joe Skorupa

NISTが提唱するゼロトラスト

最近「ゼロトラスト」という言葉を耳にする機会が増えてきたのではないだろうか？本稿では、NISTの文書をもとに「ゼロトラストの考え方」を解説する。

IIJ ネットワーククラウド本部 アプリケーションサービス部
運用技術課
古賀 勇

NISTとゼロトラスト

「ゼロトラスト」は、NIST（アメリカ国立標準技術研究所）が提唱しているセキュリティモデルの一つです[*1]。

NISTは、統一基準を発布して米国政府の各省庁への対応を主導的に求めたり、ガイドラインを発行して政府の調達基準を定めている組織で、IT分野ではコンピュータセキュリティや暗号化技術に関する先駆的存在です。

NISTと聞いても、あまりピンとこない方もいるかもしれませんが、二〇一七年に従来の認証管理のあり方を翻し、「パスワードの定期変更をユーザに強制すべきでない」（SP 800-63 B）というガイドラインを発行したことを機に、日本の内閣サイバーセキュリティセンター（NISC）や総務省のガイドラインが改訂され、メディアでも「パスワードの定期変更は不要」と大きく報道されたことが、記憶に新しいところです[*2]。

世の中の情勢と将来を見据えた標準化で産業や技術を支え、アメリカの技術革新と産業競争力を強化することがNISTのミッションであり[*3]、IT分野における貴重な技術文書が数多く公開されています。

ゼロトラストが注目される背景

多くの企業でマイクロソフト社のOffice 365やグーグル社のGoogle Workspace（旧G suite）に代表されるクラウドサービスの利活用が進むと同時に、モバイルデバイスの普及により、場所を問わず業務データにアクセスできるようになりました。それに加え、新型コロナウイルス感染症の影響で、自宅やオフィス外の場所から業務を行なうテレワークが急速に広がっています。

これまではインターネットと社内ネットワークの境界をファイアウォールで分断して内側に安全地帯をつくり、情報漏えいや外部の攻撃から守る「境界防御型」のセキュリティモデルが一般的でした。しかし、昨今のクラウドシフトにともない、従来型のセキュリティモデルが通用しなくなり、守るべきセキュリティの境界が曖昧になっています。さらに、従来型のセキュリティモデルは「内部犯行に対して脆弱である」という致命的な弱点を抱えていました。

こうした課題を踏まえ、全ての通信をフラットに扱い、常に検証し続けることで、最終的に「企業データを守ること」を目的としたのが、ゼロトラストアーキテクチャ（ZTA：Zero Trust Architecture／SP 800-207）です。

ゼロトラストの基本原則

ゼロトラストを理解するうえで、念頭に置くべき三つのポイントがあります。

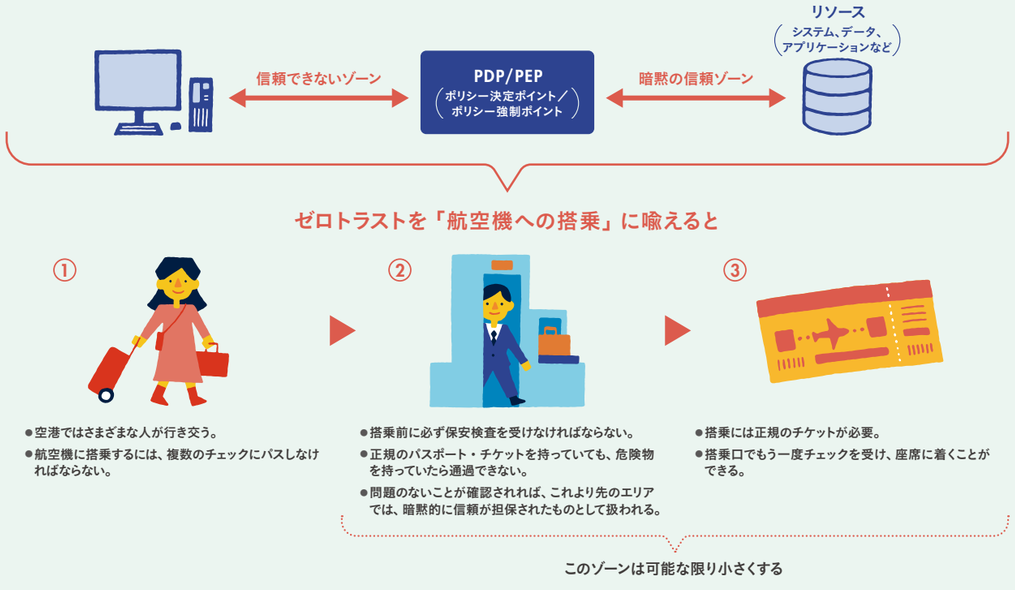
①ゼロトラストは、ネットワークを守るのではなく、データを守るためのアプローチである[*4]。

②ゼロトラストでは、ネットワーク的な位置や単一の認証（Authenticate＝誰であるかを識別すること）のみによって、認可（Authorize＝アクセスを許可）されることはなく、必ず複数の観点から総合的に判定され、最終的な決定が下される。

③ゼロトラストは、RFCや要求仕様ではなく、「目指すべき方向性」「指針」「BCP（Best Current Practice：現時点での最善事例）をまとめた「信条」「概念」である。

これらの前提をよく理解しておくことが重要であり、特に③は、ゼロトラストへ舵を切る際に、極めて重要な考え方になります。

市場に出回っている製品やサービスのなかには「ゼロトラスト」を謳ったものが少なくありませんが、「ゼロトラスト製品」「ゼロトラスト対応サービス」といった訴求の仕方をしている製品に関しては、その本質を見極め、自社の方針に合致するか否かを判断する必要があります。



ゼロトラストを理解するための基本知識

先に説明したように、ゼロトラストは目指すべき方向性を示した信条・概念であり、それを実現する手段はさまざまです。

では、どのようにしてデータを守るのか、例示したいと思います。上図は、データへアクセスするまでのプロセスを、空港で航空機に搭乗して座席に着くまでの手続きに喩えたものです[*5]。

①空港ではさまざまな人々が行き交います。そして、航空機に搭乗するには、複数のチェックにパスしなければなりません。

②搭乗前には、セキュリティチェックポイントを通過する必要があります。ここで身分の証明、保安検査官によるチェックが行なわれます。正規のチケットを持ち、身分が正しいことを証明できても、危険物を持っていたら通過できません。問題ないことが確認されれば、これより先のエリアでは、暗黙的に信頼が担保されたものとして扱われます。

③最終的に搭乗するには、正規の搭乗券を持っていなければなりません（データへのアクセスを許可されている）。搭乗口で改めてチェックを受け、ようやく座席に着くことができます（データにアクセスできる）。

ここで重要なポイントは②です。ゼロトラストの文書では、これに該当する部分を「PDP（Policy Decision Point＝ポリシー決定ポイント）」「PEP（Policy Enforcement Point＝ポリシー強制ポイント）」と表現しています。

空港の例では、PDPは保安検査官による振る舞いチェック、金属探知機によるチェック、手荷物検査にあたります。またゼロトラストでは、そのときの脅威情報（Threat Intelligence）を外部参照し、ポリシーの決定に関与することについても言及しています。空港の例では、指名手配犯の情報やニュースなどがそれにあたります。

PEPは、保安検査を実施するセキュリティチェックポイントそのものに該当します。

このように複数の観点や振る舞いから動的にポリシーを決定するゼロトラストの手法は、空港で実際に行なわれている保安検査とよく似ています。

繰り返しになりますが、ゼロトラストは信条・概念であり、常に追い求めなければならないものでもあります。グーグル社は、自社のネットワーク設計をゼロトラストアーキテクチャに置き換えるまでに、八年の歳月を要したと発表しています[*6]。とても長い道のりですが、「千里の道も一歩から」と言えるでしょう。

次稿では、このゼロトラストの考え方をもとに、もう少しディープな側面に触れてみたいと思います。

*1 ゼロトラストの文書は、2020年8月に最終版が公開されました。この全文はNISTのWEBサイトでどなたでも読むことができます。
https://csrc.nist.gov/publications/detail/sp/800-207/final

*2 SP 800-63Bを読むと、厳密には「パスワードの変更タイミングを強制しないのが望ましい」となっており、「パスワードの定期変更は不要**ではない**」ことに注意が必要です。

*3 日本貿易振興機構の調査レポート
「米国NISTの標準策定プロセス」（2019年1月）。
https://www.jetro.go.jp/world/reports/2019/02/339d3d579a99af87.html

*4 説明をシンプルにするために「データ」としていますが、実際には「リソース」です。例えば、業務アプリケーションの実行やインフラに対する利用権限も含まれます。

*5 この例はNISTの原文（5ページ目）にも出てきます。

*6 https://cloud.google.com/beyondcorp

ゼロトラストのポイント

本稿では、ゼロトラストのポイントとして「認可」「信用スコア」「運用」の3点にフォーカスして解説します。

IIJセキュリティ本部
吉川 弘晃

え方を実現するアプローチも多岐にわたっています。ここでは、ゼロトラストを実現するための一助となるポイントを紹介します。

ゼロトラストの原則

ゼロトラストとは、そもそもどういったものなのでしょうか？　ゼロトラストはリソースの保護に焦点をあてた考え方であることがNIST（アメリカ国立標準技術研究所）の文書「SP 800-207」でも示されていますが、具体的にどのような考えなのか、同文書の基本理念として掲げられているものを見ていきたいと思います。

〈ゼロトラストの基本理念〉

- 全てのデータソースとコンピューティングサービスはリソースとして見なされる。
- ネットワークの場所に関係なく、全ての通信が保護される。
- 組織リソースへのアクセスは、セッション毎に認可される。
- 所有および関連する全ての資産の完全性とセキュリティ体制を監視・測定する。
- 全てのリソース認証と認可は動的であり、アクセスを許可する前に厳密に実施される。
- ネットワークインフラストラクチャ、通信の状態など、できるだけ多くの情報を収集し、セキュリティ態勢を改善する。

基本的には〝信用を与えない状態（アクセスを拒絶する状態）〟を標準とし、それを〝信用を与える状態（アクセスを許可する状態）〟に持っていくためにはどのように考えれば良いのか、ということが書かれています。これを「ゼロトラストのために実現すべきこと」と捉えると、少々乱暴ですが「アクセス毎に認証・認可をする」「資産の完全性を保つ」「多くの情報を収集し、セキュリティ改善を行なう」の三点が挙げられ、後者の二点は「アクセス毎に認証・認可をする」ために継続して行なうべきこと、すなわち「運用」です。

要点として「認証・認可」と「運用」の二点にまで単純化をしました。では「認証・認可」のうち、より複雑な「認可」とその方法論である「信用スコア」について順番に見ていき、最後に「運用」について解説します。

認可

リソースへのアクセスはどのような情報にもとづいて判断されるべきでしょうか？　次に示すのはリソースへのアクセスを分類する一つのかたちですが、アクセス時に決定する項目だけでなく、あらかじめ分類・登録しておかなければならないものも含んでいることに注意が必要です。

〈アクセスの分類〉

- どのような情報にアクセスしようとしているのか？
  そのアクセスで操作対象となっているリソースはどういった情報なのか、リソースの機密度などを分類したもので、アセットデータベースから抽出できます。
- アクセスしようとしているのは、どのような人物なのか？
  認証されたユーザの名前、所属グループなどの情報で、認証時に抽出できます。
- どのような操作を行なおうとしているのか？
  操作の種類と、その操作が持つ危険度です。

- どのようなシステムからアクセスしようとしているのか？
  アクセス元のシステムの分類です。デバイスメーカ、OS種別、バージョン、パッチの適用状況などで、アセットデータベースから抽出できます。
- どのような場所からアクセスしようとしているのか？
  デバイスの位置情報や無線LANの暗号強度などアクセス場所にかかわる情報です。

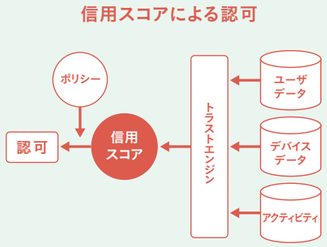
認可を判断する際は、これらの要素に対して判定していくことになります。例えば、脆弱性を持つ状態ではアクセスを許可しないというポリシーなのであれば、アクセス元システムの情報と脆弱性情報を突き合わせて判定することになります。また、機密度の高い情報へは、社内からのアクセスで、かつ一定以上の暗号強度を持っているネットワークに接続している場合に参照を許可するということであれば、アクセス先情報の機密度とアクセスしてきている場所および接続ネットワークの情報が使われます。活用の様態はいろいろ考えられますが、先にも述べたように事前にアクセス先となるリソースを分類しておくこと、アクセス元となる端末の情報を分類しておくこと、それを継続的に更新すること、すなわち「運用」ですが、認可判断にはそこで使う情報が常に更新され最新状態であることが重要で、こういった運用抜きに動的な判定をすることはできないでしょう。

信用スコア

前項ではアクセスに含む要素を分類することで認可判断に生かすかたちを紹介しましたが、これ以外にもそのアクセスが信用できるかを、ユーザの情報／デバイスの情報／過去のアクティビティから信用スコアとして算出して、認可に生かすこともできます。

信用スコアによる認可は、アクセスが持つ要素に対して直接ポリシーでの検査を行なうのではなく、リクエストとリクエストを発行したユーザのデータから計算された信用スコアをあいだに挟み、リソース毎に定められた信用スコアを持つ場合にリソースへのアクセスを許可するというものです。ゼロトラストの考え方ではポリシーは膨大なものとなり、その維持に大きなコストが発生してしまいますが、信用スコアは、これを緩和する助けとなります。

この時、信用の計算に用いるデータは継続的に収集される必要があり、スコアは常に更新されるべきものであることに注意してください。また過去から現在までの一定期間の行動履歴から信用スコアを計算する場合には、入社したばかりの社員はデータ不足により信用スコアが計算できず、結果として、その業務で必要なリソースにアクセスできないといったことも考えられます。業務は望ましいことではないため、想定されるケースのリストアップと対処を定めておくことも重要です。



運用

認可の項でも少々触れましたが、ゼロトラストを実現するためには「運用」が重要になります。繰り返しになりますが、ゼロトラストはソリューションを導入するだけで完結し、あとは何もしなくて良いというものではありません。例えば、アクセス先となるリソースはたいてい増え続けますので、資産として分類・登録し続けなければなりませんし、登録済みのリソースであっても、重要度などが変わることもあり、その対処も必要です。パッチが適用されていることをアクセス要件とするのであれば、「パッチが適用されていない＝業務が行なえない」という状況を避けるためにも、それをユーザ任せにするのではなく、きちんとコントロールしなければなりません。また、マルウェアに感染してリソースへのアクセス要件を満たさなくなった端末は、速やかに感染状態から回復し、再度アクセス可能な状態にする必要があるでしょう。そのほかにも、信用スコアによる認可を行なうのであれば、信用スコア不足でアクセスできなかった場合の原因調査と対応が必要です。

ここでは簡単に思いつくものだけを紹介しましたが、ゼロトラストの世界では、正常系を維持するための運用と、正常系から外れた場合の対処としての運用を継続して行なうことが今まで以上に重要な要素になると言えるでしょう。

以上、ゼロトラストのポイントとして――

- 認可
- 信用スコア
- 運用

これら三点について解説しました。「ゼロトラストとは何か？」や「何をすればゼロトラストを実現したと言えるのか？」ということに対する明快な解ではありませんが、皆さまの会社のゼロトラストの実装を考える際の契機になるのではないでしょうか。本稿が今後のセキュリティ計画の一助となれば幸いです。

デジタルワークプレースで実現するゼロトラスト

IIJが企業のネットワークにおいてゼロトラストを実現し、その業務をサポートするうえでの具体的なサービスおよび利用シーンを紹介する。

IIJ ネットワーククラウド本部
エンタープライズサービス部 部長
吉川 義弘

本稿では、NISTの文書「SP 800-207」で定義しているゼロトラストの重要なポイントを紹介しながら、IIJがゼロトラストを実現するためにどのようなアプローチをとっているのか、デジタルワークプレースとの関連について、詳しく述べていきます。

ゼロトラストの七つの基本的な信条

ゼロトラストでは、企業の持つIT資産（ITリソース）が、自社データセンター内だけでなく、クラウドをはじめとしたさまざまなネットワーク上に分散して存在する一方、それらにアクセスする人やデバイスも、社内ネットワークだけでなく、さまざまな場所からアクセスするような状況下において、どのような人やデバイスでも暗黙的にアクセスを許可するべきではなく、その都度、可否を確認すべきである、という考え方が前提になっています。つまりデフォルトでは、全てを信頼せず、必要なアクセスのみを確認したうえで許可する、というポリシーがベースになります。

この場合、どのようにアクセスもとを認可していくのかについて「SP 800-207」では、基本的な信条というかたちで定義しています。（右表参照）

ゼロトラストの7つの基本的な信条

① 対象とするITリソースは「全て」
アクセスする対象のITリソースは、SaaSやクラウド上に存在するもの含めて「全て」である。

② ネットワーク的なロケーションを信用しない
「社内であれば安全」といったネットワーク的なロケーションは、そもそも信用してはならない。

③ 認可確認は「セッション毎に」行なう
例えば、ログイン認証時に許可されたとしても、リソースのアクセス時には再度、許可を受けなければならない。

④ リソースへのアクセスポリシーは動的に決める
アクセスポリシーは、アクセスしようとしているユーザやデバイスの状態によって可変的かつ動的なものでなければならない。

⑤ 企業のデバイスは常にセキュアな状態に保つ
デバイスの状態が適切に維持・管理され、それがモニタリングされていなければならない。

⑥ 確実で強固な認証と認可確認の仕組み
多要素認証などを備えた、強固な認証・認可システムが必要である。

⑦ 常にネットワークの情報収集を行ない、ポリシー策定に反映させる
ネットワークのトラフィックとアクセスに関する情報収集と分析を常に行ない、それを新たなポリシー策定と実行のための改善に活かす。

ゼロトラスト実装のための論理コンポーネント

これら七つの信条を実装していくための方法として、「SP 800-207」では、通信を制御し、認可する役割であるPDP（ポリシー決定ポイント）やPEP（ポリシー強制ポイント）のほかに、デバイスの管理やセキュリティ維持を含んだ継続的な診断、リスク軽減、認証、脅威情報といった複数の論理コンポーネントを組み合わせて実現するモデルを提示しています。

これらを用いることで、ゼロトラストで求められる「全てをデフォルト拒否」としたうえで、時間や場所（社内／社外）などの条件やデバイスの状況など、さまざまな動的コンテキストを考慮して、アプリケーション単位で必要な通信のみを許可するポリシーを設定・実行します。

ここでもう一つの通信制御の考え方を紹介します。これまで説明してきた手法は、デバイスにエージェントをインストールするものでした。これは、会社で管理されたデバイスであることが前提となっていますが、仕事の形態によっては、必ずしも会社でデバイスを管理できるとは限りません。こういったケースでは、利用するPCのセキュリティパッチや脆弱性などがない状態になっているかといったことはわかりませんし、資産管理ソフトやウイルス対策ソフトなどが入っているとも限りません。

こうしたケースでは、利用するデバイスの状態によってアプリケーションの利用を許可／拒否するとできることが重要です。誰に（WHO）は、適用対象となるデバイスやユーザ、どのような状態（HOW）は、通信先などになります。さらに、これらをセッション毎に確認していくことが求められます。

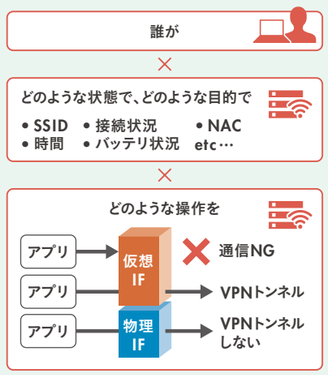
「ポリシー管理」「ネットワークアクセス制御」といった機能で実現できます。同サービスは、デバイスにソフトウェアをインストールするエージェント型のVPNサービスであり、サーバ側で設定したポリシーはデバイス上で動作するため、デバイス上で通信が行なわれるたびにリアルタイムでチェックすることが可能です。

誰に（WHO）については、適用対象とするデバイス、ユーザ、Active Directoryのグループやデバイスのグループなどを指定できます。

どのような状態（HOW）については、IPアドレスやDNSサーバのアドレスといったシンプルなIPアドレスベースの状態に加えて、SSID／BSSIDといったWi-Fiを用いたロケーションの状態、時間帯などのスケジュールに関する状態、ネットワークインタフェースの状態、接続状況、バッテリ状況といったデバイス環境に関する状態を指定できます。さらに、ネットワークアクセス制御機能を利用することで、クライアントOSのバージョン、Windows Updateの状態、アンチスパイウェアソフトのインストール有無、製品、定義ファイルの状況なども細かく指定できます。

何を許可する（WHAT）については、アプリケーション・宛先単位で、VPNトンネルを通じてトラフィックを許可する、VPNトンネルを通さずに通信させる、拒否するなどを設定できます。

IIJ フレックスモビリティサービスの「ポリシー管理」と「ネットワークアクセス制御」



通信、アプリケーションの制御

次に、ゼロトラストのなかで主軸となっているPDP／PEPで実現する、通信、アプリケーションの制御、認可について、二つのIIJサービス（IIJフレックスモビリティサービス、IIJ仮想デスクトップサービス）の実装例をもとに説明していきます。

通信を制御するポリシーには、どういった要素が必要でしょうか？　まず、誰に（WHO）、どのような状態（HOW）、何を許可する（WHAT）を設定でき

ゼロトラストを実現するIIJのサービスコンポーネント

- **IIJ セキュアエンドポイントサービス**
  デバイスのセキュリティ、資産管理
- **IIJ フレックスモビリティサービス**
  通信、アプリケーションの制御
- **IIJ 仮想デスクトップサービス**
  通信、アプリケーションの制御
- **IIJ クラウドプロキシサービス**
  通信、アプリケーションの制御
- **IIJ ディレクトリサービス for Microsoft**
  認証
- **IIJ ID サービス**
  認証

デジタルワークプレースで実現するゼロトラストモデル

IIJでは、複数のサービスコンポーネントを組み合わせてゼロトラストを実現するアプローチを採用しています。左表は、デジタルワークプレースのサービスコンポーネントを組み合わせる一例です。

す。これは、オンプレミスのシステムで実現しても、クラウドサービスで実現しても良い、理想的なモデルとして提示されているものです。

いうアプローチではなく、あらかじめ利用する人やグループなどの条件をもとに許可されたアプリケーションを、サーバ側から配布するというアプローチをとることで解決します。この場合、ユーザに配布するアプリケーションは、デバイスからは完全に分離・仮想化された状況で利用する方式を採用します。

これは、IIJ仮想デスクトップサービスにより実現します。ここでは、利用者の状況に応じて配信するアプリケーション（場合によってはデスクトップ）を決めておき、認証時にサーバから配信します。加えて、ローカルのデバイスからファイルをアップロードすることも、配信されたアプリケーション側からローカルのデバイスにダウンロードすることも禁止させるというポリシーを設定することで、デバイスからの分離を実現します。ユーザのデバイスからは、画面転送のプロトコルのみが許可されます。さらに、リモートからの認証時にIIJ IDサービスを利用して、多要素認証を組み合わせることで、認証強度をさらに強固にできます。

想定されるユースケース

最後に、リモートワークにおける典型的なユースケースを挙げてみましょう。

現在、正社員と契約社員が混在している企業は数多くあると思われます。この際、正社員は会社配布のデバイスを利用して通常業務を行なう一方、一時的な契約社員が特定の業務を担う場合は、会社支給のデバイスを配布できないといったケースがあるかと思います。

そこで、正社員は会社支給のPCでウイルスチェックソフト、資産管理ソフト、IIJフレックスモビリティサービスのエージェントをインストールしたPCからリモートワークを行ない、契約社員は私用のPCから業務を行なうというケースを想定すると、次のようなポリシーを考えることができます。

- 正社員が業務に利用するアプリケーションは、勤怠システム用のクライアントアプリケーションと、営業管理用のクライアントアプリケーション、コミュニケーション用のMicrosoft Teams、ブラウザ（Google Chrome）のみに限定する。
- 業務を行なう時間帯は「九時～一七時半」とする。
- デバイスは会社支給のPCであり、ウイルス検知ソフトのバージョンを指定する。
- ログイン時に、強制的にVPNトンネルを張り、上記以外の私用PCなどの利用は許可しない。
- 契約社員は、ローカルから分離された仮想デスクトップ上のブラウザ、Microsoft Teamsからのみ業務を行なう。ログイン時は二要素認証を必須とする。

こうしたポリシーを適用することで、リモートワークにおいても、社内で業務するのと変わりないセキュリティレベルを保つことができます。

コロナ禍をキッカケに、リモートワークが急速に進むと同時に課題も見えてきました。これを踏まえて、全ての仕事をデジタル化し、ネットワーク上で行なうことを前提とした時代へと急速に向かうと予想されます。そうしたなか、セキュリティは最重要項目として考える必要があり、そのためには、ゼロトラストを実現していくことが非常に重要になってきます。

IIJのデジタルワークプレースは、使いやすく、働きやすい環境を提供するのみならず、その前提となるゼロトラストをネットワーク上で実現するサービスプラットフォームです。今後もさらなる機能拡充を目指して進化していきますので、どうぞご期待ください。

ゼロトラスト対応のFSEG

IIJプロダクト本部 SDN開発部 シニアプロダクトマネジャー
水野 正和

FSEG（エフセグ）は、IIJで初めてゼロトラストモデルに対応したネットワークセキュリティ・ソフトウェアです。ネットワーク管理者が規定するセキュリティポリシーを、FSEGがネットワーク全体に自動的に適用します。市場を見ると、「マイクロセグメンテーション」あるいは「アイデンティティベースのアクセス制御」への対応をもってゼロトラスト対応とアピールしている製品・ソリューションが多いようですが、FSEGはどちらも実装しています。ゼロトラストということで、未認証のデバイス・ユーザをFSEG管理下の資産に接続させないことは当然ですが、FSEGはほかにもさまざまなことを「信じていません」。

「デバイス」を信じていません

デバイスが適切なセキュリティ対策を行なっていることをFSEGは期待していません。例えば、搭載ソフトウェアが更新されていないPC、セキュリティ機能を追加・更新できない組み込み機器・IoT機器。また、いったん接続が許可されたデバイスでも、その後もずっと問題がないとはFSEGは考えません。デバイスが稼働中に何らかの脅威に感染することもあるからです。FSEG管理下では、さまざまなセキュリティ機能をFSEGが管理するネットワーク側で実装しており、デバイスからのトラフィックを常にチェックします。この機能はFSEG側で適切に更新されます。ネットワークがさまざまなデバイスを常時監視するのです。デバイスにエージェントソフトなどをインストールする必要はありません。

「隣人」を信じていません

社内の同じネットワークにつながっているデバイスだからといって、そのデバイスとの通信を許可してしまって良いでしょうか？FSEGは「相互通信を許可するデバイス・ユーザの集まり」を定めます。同じグループに属していれば通信を許可し、異なるグループ間は（たとえ同じVLANにつながっていても）FSEGでは通信を許可しません。このグループ化技術がFSEGでのマイクロセグメンテーションを実現します。デバイスやユーザは、認証結果に応じたグループに配置されます。このグループを適切に定めれば、脅威の侵入後の水平拡散を最小限に抑えることができます。さらに、グループ内のデバイスも疑いながら常時監視していることは先述した通りです。FSEGのグループ化は、いわゆる許可リストによる通信制限とは異なる手法です。また、FSEGでのグループの実装技術は、従来のようにネットワーク機器の設定によるもの（VLAN設定など）とは異なり、仮想的に作成しますので、ネットワーク機器の構成に縛られることなく、非常に柔軟に対応できます。標準技術を用いているため、ベンダロックインの懸念もありません。

「確認」を多重化できます

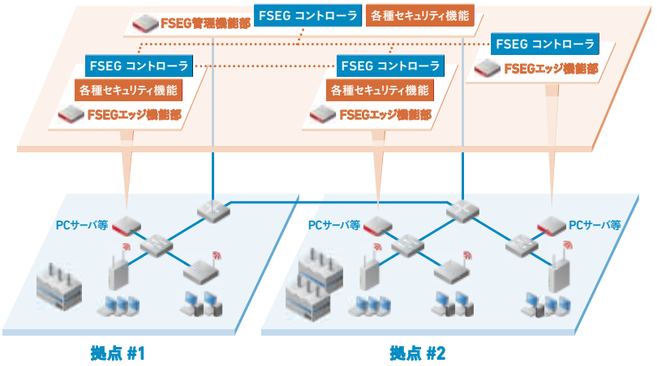
FSEGがネットワーク側で実装するセキュリティ製品は、さまざまなセキュリティ機能（IPS、振る舞い検知、デバイス識別、URLフィルタリングなど）を用いることができ、特定のセキュリティベンダに依存していません。さらに、複数のセキュリティベンダの製品を組み合わせて、多段階のチェック機能を構築できます。あるセキュリティ機能で脅威が検知された場合、その検知が妥当かどうかを別の機能で追加検証できるのです。また、グループ毎に適用するセキュリティ機能を設定できます。例えば、オフィス機器／工場内FA機器といったグループ分けを行なうことで、守りたいものに応じた（各グループに応じた）適切なセキュリティ機能を利用できます。

「まだ大丈夫」を信じていません

あるグループのあるデバイスが脅威に感染したことが検知された時、FSEGは「同じグループの他のデバイスではまだ検知されていないから問題ないだろう」とは考えず、「同じグループに属しているのだから（相互通信が可能なのだから）すでに感染している可能性が高い」と考えます。そして、グループ毎に「監視強化」「隔離」などさまざまな処置を「予防」として実施できます。

FSEGは「さまざまなユーザ、デバイスがつながる環境」に適しています。例えば、IT（Information Technology）とOT（Operation Technology）の融合により新しい価値を創出しようとしている製造業、働き方改革やオフィス効率化を目指してIoT導入を進めている企業、ICT化を進めている学校などです。世界的な新型コロナウィルス禍により、産業界も教育界も変革を迫られていますが、その場しのぎの対応では意味がありません。そうならないよう、ゼロトラスト対応FSEGの導入をご検討いただければと思います。

FSEG 概略図



新連載

IIJ Research
となりの情シス

徹底調査で見えてきた、コロナ禍が浮き彫りにしたITシステムの課題

～情シス 269人にIIJが独自アンケートを実施

社会・経済活動に大打撃をもたらした新型コロナウイルスの感染拡大を受け、
企業のITシステム部門はワークスタイルの変革を余儀なくされている。
コロナ禍を乗り切る一手法として、テレワーク環境の急速な整備はその象徴と言えるが、
目下、ITシステム部門はどのような課題に直面し、どのようなIT投資計画を立てているのか？
IIJが実施したアンケート調査の結果を紐解いてみたい。

コロナ禍が浮き彫りにしたITシステムの課題

IIJではIIJメールマガジン配信読者のITシステム部門担当者を対象に「新型コロナウイルス対応におけるITシステムの課題」と「今後のIT投資の方針」に関するアンケート調査を実施しました（実施期間：2020年6月23～29日／有効回答数：269件）。その結果、新型コロナウイルスへの対応におけるITシステム面の課題として、以下が上位に挙げられました。

- **WEB会議ツールの使い勝手や使い方の周知**
- **VPNの遅延や接続待ちの発生**
- **端末をすぐに支給できなかった**
- **在宅時のネットワーク環境を用意できなかった（モバイルルータなど）**
- **WEB会議ツールの遅延や切断の発生**

Q1. **新型コロナウイルスへの対応において、ITシステム面で課題だと感じたことを全て選択してください。**

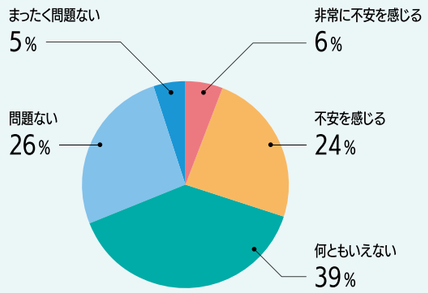
回答を見ると「テレワーク環境の整備」と「テレワークでの円滑な業務実施」が課題であると言えます。質問の選択肢には、セキュリティ、人的リソース、コストに関する課題なども含まれていましたが、それよりもテレワーク環境を用意し、円滑に業務を実行していくという部分を課題として強く感じていたことがうかがわれます。

こうした結果の要因としては「対応までのスピード感が求められたこと」が考えられます。例えば、東京オリンピック・パラリンピックに向けたテレワーク環境の整備は、対応期限が明確だったため、予定を立てて準備を進めることが可能でした。しかし、今回のコロナ禍は急速に感染が拡大し、瞬く間に状況が一変しました。緊急事態宣言の発令まで時間的猶予がなく、流されるように対応に追われた面は否めないでしょう。何よりもまず「業務を継続するための環境整備」が、多くの企業で最優先事項であったことが見てとれます。

アフターコロナ時代のIT投資の方向性

緊急事態宣言への対応を経て、企業は一定の“経験値”を積んだはずです。では、今後をどのように考えているのでしょうか？

Q2. **今後、同様の状況が発生した際に現在のITシステムで乗り越えられそうですか？**



調査の結果を見ると、「まったく問題ない」「問題ない」をあわせた回答が3割程度にとどまっており、多くの企業が現状のITシステムに不安を抱いていることが明らかになりました。

そこで、今回の対応を踏まえて、強化したいIT投資について尋ねたところ、以下のような回答が上位を占めました。

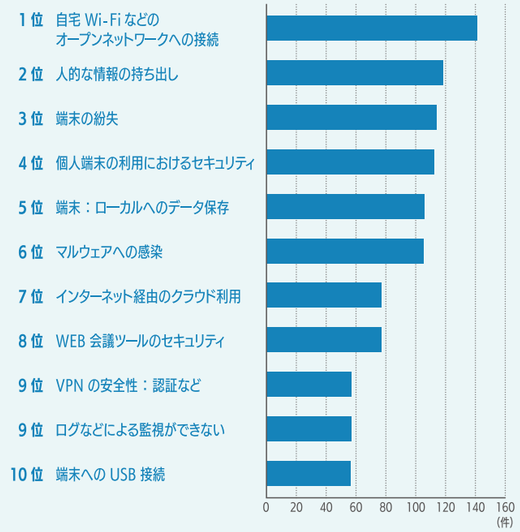
- **テレワーク環境のセキュリティ強化**
- **VPNの速度や安定性を向上させたい**
- **テレワーク環境の利用者の利便性を向上させたい**
- **テレワーク拡大にともなうネットワークの負荷対策**
- **端末の状況を可視化したい**

Q3. **今回の対応を踏まえ、今後、IT投資を強化したい要素を全て選択してください。**

回答の傾向としては「テレワーク環境の強化」に関連したものが上位に、新たなテレワーク関連システムの整備に関するものが下位にきています。このことから、多くの企業でテレワーク環境はすでに整備されており、今後の感染拡大に備え、既存のテレワーク環境のセキュリティ、安定性、利便性の向上などに投資の方向性が向いていると推察されます。

ここで、第1位の「テレワーク環境におけるセキュリティ強化」を深堀してみましょう。「セキュリティ」とひと言でいっても多様な要素がありますが、本調査ではおもにテレワーク時におけるセキュリティリスクについて尋ねてみました。

Q4. **テレワーク時におけるセキュリティが懸念されていますが、リスクと感じられる項目を全て選択してください。**



テレワーク時におけるセキュリティリスクとして第1位に挙がったのが「自宅Wi-Fiなどのオープンネットワークへの接続」です。自宅のネットワークは、ルータの脆弱性が放置されている可能性があり、そうしたネットワークへの接続はリスクと捉えられているということです。次に多かったのが「人的な情報の持ち出し」と「端末の紛失」です。ここからは、情報漏えいに対して強い危機感があることがわかります。

テレワーク実施時は、PCを社外に持ち出したり、社外から社内ネットワークにアクセスしたりします。ITシステム部門の管理が行き届かない社外では、運用ルールやセキュリティポリシーの徹底がむずかしいため、利用者のIT環境や行動など「利用者に依存する要素」が重大なリスクと考えられているのです。

特設サイト「法人IT調査レポート」開設！

IIJでは、情報システム部門の方々を対象にアンケート調査を定期的に行ない、その内容を特設サイト「法人IT調査レポート」で公開しています。今回のテーマについてより詳しく知りたい方は、こちらのサイトも併せてチェックしてください。
https://www.iij.ad.jp/svcsol/survey/

本連載では、今後も「法人IT調査レポート」のダイジェスト版を紹介していきますので、ご期待ください！

人と空気とインターネット

転換の発想

―一般社団法人イノベーションインスティテュート
取締役
浅羽 登志也

異常気象や世界規模の感染症など、
我々の生活を一変させる
事象が起こっている。
今回は、そうした危機を
チャンスに転換する
発想について考えてみたい。

今年の夏は……

今年も無事お米の収穫を終えました。残念なことに、七月に雨の日が異常に多く、そのせいで日照時間が短く、気温も低かったため、昨年に比べると収穫量が落ちてしまいました。そのかわり八月がとても暑かったので、八月中に米の生育が追いついたようで、収穫時期は昨年よりも一週間ほど早まりました。私のような素人ではない、プロ農家さんたちはこの変化にちゃんと対応できたのか、特に収量を落とすこともなかったようです。なんとも悔しい限りです。

一方、面白いことに気がつきました。それは米を脱穀したあとの藁（わら）が、例年に比べると長くてしっかりしていることです。つまり、私の田んぼの稲たちは、田んぼから吸収したり、光合成で作った養分を、稲藁のもとになる茎の成長に、より多く使ってしまったようなのです。

植物の成長にはざっくり二段階あり、栄養成長と生殖成長に分けることができます。栄養成長は植物の身体にあたる茎や葉を成長させる段階で、生殖成長は花を咲かせ、実を育てる段階です。稲の場合、この切り替わりのタイミングは、積算温度の影響を受けます。つまり、ある程度の気温（水温）がある日数以上続くと、花芽が形成されて、実をつける準備をするのです。今年は七月の低温で積算温度があまり上がらず、栄養成長の期間が長かったので、そちらに養分をとられてしまったのでしょう。私はできるだけ人為的に与える肥料を少なくしたい派なので、通常は四月に一回、有機肥料を撒くだけにしているのですが、普通の農家は七月ごろに追肥するのが一般的です。私も七月に追肥しておけば、収量に影響が出なかったのかもしれません。まぁ、量は減りましたが、できたお米は例年通りの美味しいお米ですし、立派に育った藁を何か別のことに活用すればいいので、良しとしようと思います。

今年はもう一つ例年と違うことがありました。なんと、九月に軽井沢で桜が咲いたのです。たくさん咲いたわけではなく、駅前のコンビニの横に生えている木だけなのですが、テレビのニュースで取り上げられたのを見て、それは珍しいとわざわざ見に行き、写真も撮ってしまいました。原因は、おそらく私の米の収量が減ったのと同様に七月の低温だと思います。七月に低温が続いたのち、八月に急に暑くなったので、冬から春になったと勘違いしてしまったのでしょう。そんなことが起こるなんて思ってもみなかったので、かなり驚きました。

私の米の収量が多少落ちたり、軽井沢の一本の桜の木が九月に咲いたりするくらいなら大した話ではないのですが、最近は台風の振る舞いもだいぶ変化してきています。近年は毎年のように観測史上最大の台風をむかえる羽目になり、大きな被害につながることも増えてきました。規模だけでなく進路についても、九州の西側をかすめて朝鮮半島から中国にまっすぐ北上したかと思えば、九州の南あたりで直角に曲がって東に向かってみたりと、今まであまり見たことのない変わった進路を辿るようにもなりました。これはおそらく地球温暖化が進んだために起こった異常気象の一環なのだろうと、感じている人も多いのではないでしょうか。

新しい時代を切り拓く

新型コロナウイルス感染症の影響により、多くの国で都市封鎖が行なわれ、経済が大きく減速した反面、温室効果ガスの排出量が減るというプラスの側面も生じたのではないかと思い、ネットを検索してみました。すると「四月初旬までの一日あたりのCO₂の排出量が、二〇一九年の平均値と比べて、最大一七パーセント減少した」とする論文が五月一九日付で『Nature Climate Change』に発表された、という『WIRED』の記事が見つかりました。「一七パーセント減」をどう捉えるかはむずかしいところですが、論文によると、一七パーセント減少しても二〇〇六年の水準に戻ったにすぎないということです。逆に、この一四年間でいかに急速に増えてきたのかという事実を改めて思い知らされました。

私を含め、多くの人々はコロナ禍のもと、かなり活動を抑えていたはずですが、これだけやっても一四年前に戻すのがやっとなのです。グレタさん（一七歳のスウェーデンの環境活動家）に罵倒されるまでもなく、もうシステム自体を変えないとダメなんじゃないかと、目先の利益しか考えない無責任な大人の一員である私も身に染みて理解できた気がします。そう思うと、このコロナ禍を一つのチャンスと捉えて、仮に今回の感染症を押さえ込むことができたとしても、以前の状態に戻ることを考えるべきではなく、新たな生活様式、経済様式、社会様式への転換を推し進めていくべきなのでしょう。その時はインターネットをベースとしたICTが大事なツールとなるはずです。

ただしその際に重要なのは、何かの活動をICTによって別のものに〝転換〟する発想だと私は考えています。CO₂の削減というとちょっと面倒なので、わかりやすく「エネルギー消費を減らす」とすれば、例えば、リモートワークを推進すると、ネットやPCなどのデバイスの活用頻度が増え、その分のエネルギー消費が増えるでしょうから、どこか別のところでそれ以上のエネルギー消費を削減しないと意味がないことになります。するとその分は、人の移動で消費されていたエネルギーを削減してまかなうと同時に、オフィスなどはさっさと解約して、通勤や出張という概念をなくしてしまうくらいの大胆な転換が必要なのではないかと思うのです。

私の大学の後輩で、いい意味でヘンな奴がおりまして、今はAI翻訳ベンチャーの社長を務め、数年前にIPO（株式公開）もし、順調に事業を拡大して注目されていました。そんな彼は、コロナ禍で在宅勤務になった時、「もうオフィスはいらない。バーチャル空間に移転してVRでいいじゃん」と、開発から本社機能まで全部バーチャルオフィスでできるようにして、今は自宅で大きなゴーグルをはめて仕事をしているそうです。さらに、本社の登記もバーチャル空間に移そうとしたら、それはできないとお役所に言われて、オフィスは少し残さざるを得なかったと憤慨していました。

また、直接の面識はないのですが、ベストセラー『シン・ニホン』の著者・安宅和人さんは、国土の七割を占める森をもっと活用すべきと、全国に「風の谷」を作るプロジェクトを始めたそうです。スマートシティなどとは全く異なる発想で、私はとても共感しました。このように、すでに転換を大真面目に進めている人たちがいるのは心強い限りです。

もうハンコをなくすくらいでガタガタ言っている場合ではないでしょう。これまで当たり前だった何をやめて、何に転換すれば、変化を乗り越え、新しい時代を切り拓けるのか。ここからがインターネット革命の本番なのかもしれません。

Technical Now

東京都 大田区

クラウドで「自治体情報システム強靭性向上モデル」を実現 インターネット接続系をIIJサービスで刷新

東京都大田区は「自治体情報システム強靭性向上モデル」に準拠したインターネット接続システムを、クラウドサービスで刷新した。最適なサービスの提供に加え、IIJのプロジェクトマネージメントにより、多岐にわたる要件のシステム刷新を“超短期間”で実現。職員の業務利便性とセキュリティの向上を両立した。アセットレスのクラウドサービスの活用により、運用管理の負荷も大幅に軽減された。

[導入前の課題] セキュリティを担保しつつ、業務利便性を向上させたい

羽田空港を擁する自治体として、都市間交流を進めながら「来て良し、住んで良し」のまちづくりを推進する大田区。文化・産業・観光施策や住民サービスの向上を目指し、積極的にITを活用している。

そのIT環境は、総務省より示された「自治体情報システム強靭性向上モデル」に対応し、マイナンバー情報を扱う「個人番号利用事務系」、自治体間を結ぶLGWAN（Local Government Wide Area Network：総合行政ネットワーク）につながる「内部情報系」、外部インターネットにつながる「インターネット接続系」にネットワークを3分割し、厳格な通信制御により、強固な情報セキュリティを実現している。

LGWAN接続系端末は約3500台。仮想環境上からLGWANやインターネットにアクセス可能だ。ただし、これは閲覧のみ。マルウェア感染や情報漏えいを防ぐため、メールの送受信や必要な資料を入手したい場合は、ファイル無害化システムを経由しなければならない。「このファイル無害化システムを搭載した専用端末が各課に1～2台配備されているのですが、順番待ちが発生していました」と大田区の佐藤明弘氏は振り返る。

「ペーパーレス化などを推進するため、大田区ではタブレット端末も導入しましたが、タブレット端末や自席PCでは、メールの添付ファイルや業務で使うファイルのダウンロードなどを制限していました」と大田区の鈴木弘晃氏は振り返る。職員からこれをできるようにしてほしいという要望が数多く寄せられていたという。またタブレット端末には、庁内ネットワークを経由しないタブレット用のインターネット接続システムを構築。2系統のインターネット接続システムを運用することも大きな負担になっていたという。

そうしたなか、利用していたメールサービスが2020年3月末でサービス終了を表明。タブレットのリース期間も2019年12月で満了となる予定だった。「これを機に、利便性とセキュリティを両立できる新たなインターネット接続システムの実現を目指しました」と佐藤氏は語る。

[選定の決め手] 充実したクラウドサービスと技術力・コストを総合評価

自治体の情報システムは、従来、オンプレミスが基本であったが、政府が示した「クラウド・バイ・デフォルト原則」に沿って、クラウド利用が前提になりつつある。大田区も新たなインターネット接続システムはクラウドをベースに考え、生産性とセキュリティ向上、そしてTCO（Total Cost of Ownership：総保有コスト）の削減を目指した。この実現に向け、パートナーに選定した1社がIIJである。「クラウドサービスを数多く提供しており、クラウド／ネットワーク／セキュリティ関連の技術力が高い。コストも含めた総合力を評価しました」と佐藤氏は選定の理由を述べる。

プロジェクトに参加したベンダは10社近くにのぼる。そのなかでIIJは、PCおよびタブレットのインターネット接続システムとそのセキュリティ対策のクラウド化を担当。クラウド型ネットワークサービス「IIJ Omnibusサービス」、クラウド型メールセキュリティ「IIJセキュアMXサービス」、セキュリティ監視・運用サービス「IIJ C-SOCサービス」、WEB閲覧・無害化時の利便性の高いインターネット分離ソリューション「SCVX」、さらには、約600台のタブレットの調達・キッティングなどを提供した。

プロジェクトの推進にあたり、IIJでは専任のPM担当者を配置し、他ベンダとの調整や交渉もこのPM担当者が窓口になって対応した。「例えば、ファイル無害化システムを実装した仮想環境は別のベンダが担当しましたが、これをベースにセキュアなインターネット接続を実現する環境構築や各種設定もIIJのサポートのおかげでスムーズに進みました」と佐藤氏は評価する。

[導入後の効果] 超短期間でシステムを刷新。自席でファイル取得も可能に

環境構築は2019年10月にスタートし、同年11月にはメールおよび仮想環境をリリース。同年12月にタブレットを納品し、新たなインターネット接続システムの本格稼働を開始した。「要件が多岐にわたるプロジェクトを実質2カ月ほどの“超短期間”でカットオーバーできました。プロジェクトのなかでIIJが果たしてくれた役割は大きい」（佐藤氏）。

現在はPC用、タブレット用に分かれていたインターネット接続環境をIIJサービスで一本化。自席のPCやタブレットでファイル無害化システムも利用できるようになった。「自席でメールの送受信やファイルダウンロードを行なえ、順番待ちせずにすむので、非常に好評です」と鈴木氏は満足感を示す。異なるネットワーク間でファイルを移動するために使用していたUSBメモリも必要なくなり、紛失などによるリスクもなくなった。

「セキュリティインシデントの対応や各種の設定変更などもIIJがサポートしてくれます。サポートセンターの回答も的確でレスポンスも速い。以前と比べて運用負荷も大幅に軽減されています」（鈴木氏）。

インターネット接続システムのクラウド化を実現し、業務の利便性とセキュリティ向上を両立した大田区。この仕組みをベースに、自治体業務のさらなる生産性向上を目指す考えだ。

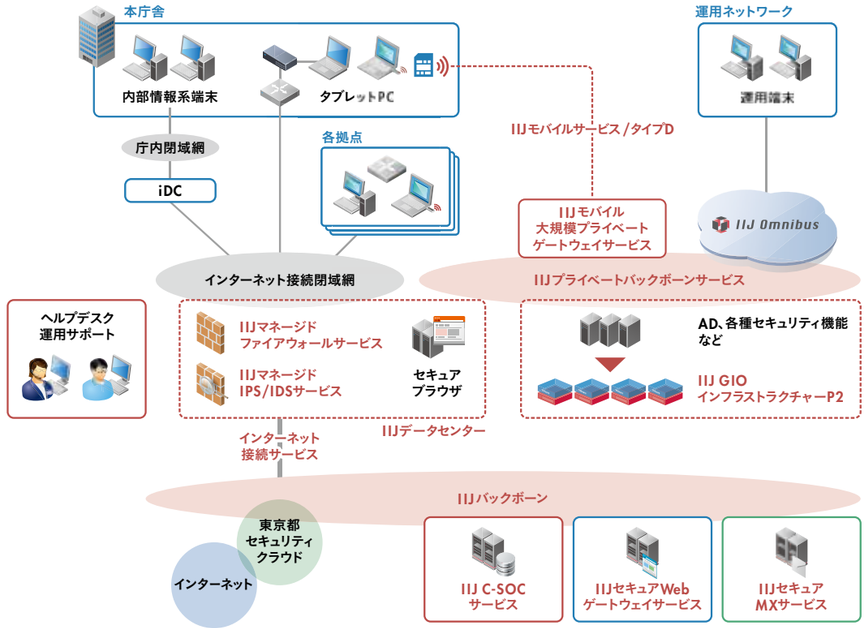
※ 本記事は2020年2月に取材した内容をもとに構成しています。
記事内のデータ、組織名、役職などは取材時のものです。

大田区
企画経営部 情報システム課
NW担当係長
佐藤 明弘 氏

大田区
企画経営部 情報システム課
NW担当係長
鈴木 弘晃 氏

大田区役所
所在地：東京都大田区蒲田五丁目13番14号
設立：1947年3月
区内人口：738,128人
（2020年4月1日現在）

羽田空港跡地の再開発をはじめとする都市機能の更新や沿線のまちづくりを進め、地域力を結集した「国際都市おおた」の実現を目指す。防犯・防災、福祉、子育て、教育、産業、環境など、さまざまな施策を通じ、きめ細かでより質の高い行政サービスの提供にも努めている。



Technical Now

大和リゾート株式会社

Office 365へダイレクト接続する最新サービスで大規模テレワーク導入のセキュリティポリシーを担保

Office 365 が提供する Microsoft Teams は、テレワークを実現するうえで不可欠なツールだ。
大和リゾートは 2020 年 4 月からテレワークを本格導入することを決定。
グループのセキュリティポリシー上、Office 365 へダイレクト接続が可能なサービスを探していた。
そこで、IIJ から提案を受けた Office 365 にダイレクト接続できる新サービス
「IIJ クラウドエクスチェンジサービス for Microsoft Azure Peering Service」を他社に先駆けて導入した。

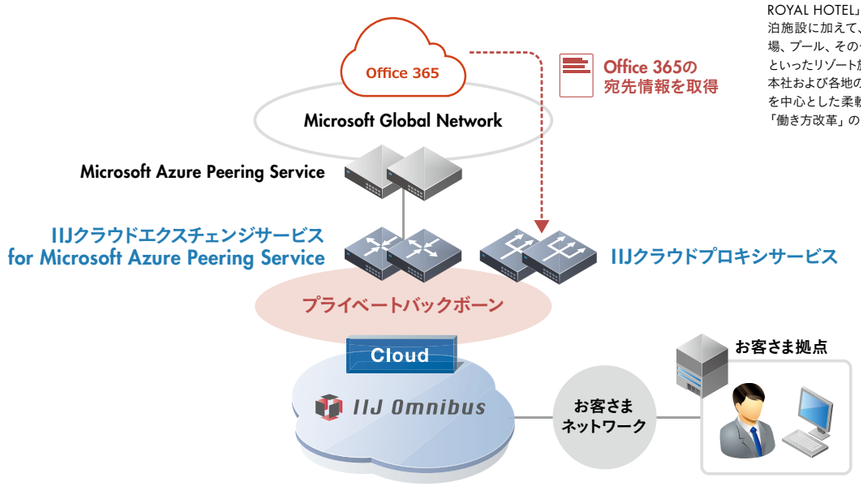
大和リゾート株式会社
管理本部CS部
システム管理グループ
（西日本支社駐在）
グループ長
高田 真次 氏

大和リゾート株式会社
管理本部CS部
システム管理グループ
（西日本支社駐在）
次長
近藤 章 氏

大和リゾート株式会社

大和リゾート株式会社
本社：東京都江東区有明三丁目7番18号 有明セントラルタワー 10階
設立：1973年
連結売上高：466 億 9,800 万円（2018 年 3 月期）
従業員数：2,011人

大和ハウスグループの企業で、ホテル「DAIWA ROYAL HOTEL」の運営管理を手がける。宿泊施設に加えて、レストラン、宴会場、ゴルフ場、プール、その他のスポーツ施設、遊戯施設といったリゾート施設全般の運営管理を行なう。本社および各地の事業所を縮小し、テレワークを中心とした柔軟な働き方への移行を目指す「働き方改革」の先進企業でもある。



[導入前の課題] テレワークへの完全移行を計画 セキュリティポリシーの壁に直面

大和ハウスグループの一員で「DAIWA ROYAL HOTEL」の運営などリゾート事業を手がける大和リゾートは、2020年に大きな執務スタイルの転換を目指していた。急速に広まりつつあるテレワークを、一部の従業員が利用するのではなく、全社の基本にしてしまおうという大胆な計画だ。将来的には東京の有明地区にある本社、大阪の西日本支社などの事業所を必要最低限の規模に縮小し、基本的な業務をテレワークで行なおうという一大プロジェクトである。

大和リゾートの高田真次氏は「本社のある有明地区は2020年夏の世界的スポーツイベントの会場予定地となっており、その時期の通勤問題が1つのキッカケとなり、2020年4月からテレワークを実施するということで検討が始まりました」と振り返る。

マイクロソフトがOffice 365で提供するコミュニケーションプラットフォーム「Microsoft Teams」（以下、Teams）をテレワークの基盤に採用。Teamsは、チャットなどの文字のコミュニケーションだけでなく、通話やテレビ会議、資料などを共有した共同作業などもできるツールで、テレワークの基盤としての機能が備わっている。すでに大和ハウスグループではOffice 365を使っていたことも、この採用を後押しした。

ただし、課題もあった。それは社内ネットワークからOffice 365に接続する回線の問題で、大和ハウスグループのセキュリティポリシーではダイレクト接続が必須だった。従来は大和ハウスグループのプロキシサーバを介して外部クラウドサービスとダイレクト接続していたが、帯域が潤沢とは言えなかった。さらにOffice 365では1人あたり30～40といった多くのセッションと通信帯域を使うため、大和リゾートの2000人規模の従業員がテレワークに移行すると、グループ他社の通信に影響を与える懸念もあった。

大和リゾートの近藤章氏は、次のように説明する。「以前は回線とプロキシサーバがボトルネックになり、非常に遅かったのが現実です。そこでOffice 365とダイレクト接続できる回線の解決策を探し、グループの情報システム会社であるメディアテックに相談したところ、IIJを紹介されました」。

[選定の決め手] Office 365とダイレクト接続が可能なIIJの新サービス

自社のネットワークからOffice 365にダイレクト接続が可能で、テレワークに耐え得るネットワーク構成を求めて、大和リゾートはIIJに相談を持ちかけた。IIJは2019年11月、Office 365を含むMicrosoft Azureとのダイレクト接続を提供する「IIJクラウドエクスチェンジサービス for Microsoft Azure Peering Service」のリリースを控えており、これがちょうど要件にマッチするとして大和リゾートに提案した。この新サービスの提供開始は2020年4月で、大和リゾートのテレワーク実施と同時期であり、その前にPreview期間として事前のテレワーク試行にも対応可能であることがわかった。

大和リゾートはIIJを含む数社に提案を求めたが、要件を満たしたのはIIJだけだった。テレワークプロジェクトが始動した2019年9月と言えば、テレワーク実施までに残された時間は半年しかない。「迷っている暇はありませんでした。良いと判断したIIJの新サービスで前に進めて、うまくいかなかったら改めて別のソリューションを探せばいいと考えていました」（近藤氏）。

ネットワーク構成の中心は、IIJクラウドエクスチェンジサービス for Microsoft Azure Peering Serviceを使ったマイクロソフトのクラウドサービスとのダイレクト接続。Office 365のTeamsを活用するため、大和ハウスグループのセキュリティポリシーに抵触することなく、信頼性と必要な帯域を確保できるようにした。

同時に「IIJクラウドプロキシサービス」を利用し、Office 365で大量に発生するセッション情報を管理するためのプロキシサーバをクラウド化。これにより、プロキシサーバの運用工数とプロキシサーバ自体にかかる負荷を削減した。

[導入後の効果] 社内 LAN 接続と変わらないテレワーク環境を実現

今回IIJからは、ネットワークだけでなく、Office 365利用に必要なライセンスや認証サービスも含めて提供。先述の構成で2020年4月のテレワーク実施を安心して迎えられるはずだったが、2020年初頭からの新型コロナウイルスへの対応で、テレワーク開始が前倒しとなった。大和リゾートのシステム管理グループでは、パソコンのセットアップを順次進めると同時に、IIJのサービスを利用したネットワークのカットオーバーを急いだ。

3月上旬、新しいネットワークのPreview利用と、約200台のテレワーク用パソコンの準備が整い、Teamsを利用したコミュニケーション基盤が前倒しで本番利用可能になった。高田氏は「カットオーバーの時点では大きな混乱もなく、Teamsを利用したテレワーク環境が実際に動き出しました」と胸をなでおろす。

実は、大和リゾートではTeams利用時のもう1つの課題への対応も進めている。外線電話の取り扱いだ。「働き方改革を推進していくと、会社宛の外線電話をテレワーク中の従業員でも受けられる仕組みが必要になります」（近藤氏）。

IIJに相談すると、ソフトバンクが提供しているクラウドPBXを利用したTeams向けの音声通話サービス「UniTalk」の情報が得られた。Teamsの通話機能で固定電話番号による発着信が可能になる国内初のサービスで、大和リゾートではテレワークに必須の機能として導入に向けた検証を行なっている。

テレワーク用のノートPCとTeams活用によるテレワーク環境整備で、「どこにいても99パーセント以上は社内LANのデスクトップと同じ業務ができます。IIJの提案で構築したネットワークにより、セキュリティポリシーに合致したうえで利用者に快適なインフラが整備できたと感じています」と高田氏は満足感を示す。事業所を縮小する狙いでスタートした大和リゾートの本格的なテレワークを、IIJの最新サービスが見えないところで支えている。

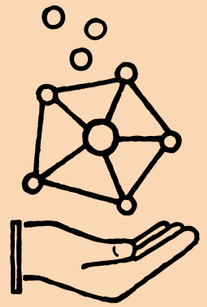
※ 本記事は2020年3月に取材した内容をもとに構成しています。
記事内のデータ、組織名、役職などは取材時のものです。

Internet Trivia

インターネット・トリビア

携帯電話のエリアの広さと人口カバー率

IIJ MVNO 事業部 事業統括部
シニアエンジニア
堂前 清隆



スマートフォンを利用するうえで、携帯電話の電波が届く範囲「サービスエリア」の広さはとても重要で、各社はエリアの拡大に力を入れています。エリアが広い・狭いということを公平に比較するための指標の一つに「人口カバー率」があります。これは、携帯電話の電波が届いている範囲に、日本の人口のうちどれだけの割合が住んでいるかを表しています。といっても、一人ひとりの住まいを訪問して調査をすることは現実的ではありませんので、あくまで机上で計算した推計となります。

かつて、この推計は市町村単位で行なわれていました。市町村の代表地点（役所・役場の所在地）に電波が届いていれば、その市町村の人口分を全てカバーしたとして計算されていたのです。しかし、この方法はあまりに大雑把で、利用者の体感とのズレも大きいと言われていました。そこで、2014年に推計方法が改められ、全国を500メートル毎に区切った範囲（メッシュ）を定め、そのメッシュの半分以上の場所に電波が届いていれば、メッシュ内に居住する人口をカバーしたと判定することになりました。これは、総務省が携帯電話会社に新しい電波を割り当てる際の審査基準として定められたもので、より実態に近い推計が可能になります。

本稿の執筆時点では、NTTドコモ、KDDI（au）、ソフトバンクの三社とも、メッシュ方式における人口カバー率は99パーセントを超えていると発表しています。また、2019年に新規参入した楽天モバイルも、2021年夏をメドに人口カバー率96パーセントを目指すと発表しています。

ですが、人口カバー率だけで「スマートフォンが使えるエリア」を表せるわけではありません。利用者が特に実感するのは、マンションやオフィスビルなどの建物内でしょう。

一般的に、携帯電話の基地局はビルの屋上や鉄塔など屋外に設置されます。そのため、屋外には比較的電波が届きやすいのですが、コンクリートや鉄骨に囲まれた屋内には電波が届きにくくなります。また、基地局の多くは高所からやや斜め下向けに設置されているため、建物の上層階には電波が届きにくくなります。つまり、建物の一階、窓際には電波が届いていても、上層階や建物中心部には電波が十分に届かないということが起こります。

この問題を解決するため、大手三社は利用者の多いビルには、各フロアに基地局（アンテナ）を設置するという対策を行なっています。日本の携帯電話市場では人口カバー率が高いのは当たり前で、こうした対策をどれだけ上積みできるかが、利便性を左右するキーになっていると言えるでしょう。

ところで、2019年より新しい携帯電話システムである5Gの利用が始まっています。5Gはこれまでの3G・4Gとは異なる基地局設備が必要になるため、各社ともゼロスタートで各地に基地局の建設を進めています。

5Gのエリアを表す指標の一つとして、これまでの人口カバー率ではなく「5G基盤展開率」という数値が登場しました。総務省が電波を割り当てる際の審査にも、この基盤展開率が用いられています。5G基盤展開率も全国をメッシュに区切って評価するのは同じですが、ここに人口という要素を含めないのが特徴です。

人口カバー率では、そのメッシュに住んでいる人口が多いほど比重が大きくなります。つまり都市部が重視される計算方法でした。それに対し5G基盤展開率は、メッシュの数、すなわち面積だけで評価しているため、都市部でも地方でも同じ重みで扱う計算方法だと言えます。

4Gまでは、あくまで携帯電話・スマートフォンという直接、人が使う用途を想定していたため、人口密集地が重視されました。一方5Gは、スマートフォンに加え、IoTに代表される「モノ」が通信を行なうためのインフラでもあります。そのため、人口が密集している場所だけでなく、それ以外の場所についても電波を届ける必要があるとされ、それが審査基準にも現れているのです。携帯電話網の用途の拡大は、こんなところにも影響をおよぼしています。

イラスト／末房志野（P24,25）

Grobal Trends

グローバル・トレンド

データ覇権をめぐる世界の対立と日本の役割

IIJビジネスリスクコンサルティング本部
副本部長
鎌田 博貴

人権vs安全保障の対立軸

七月一六日、欧州司法裁判所が、EUから米国への自由な個人データ移転を認めるEUの決定は無効とする判決（シュレムスII判決）を下しました。米国の諜報機関が適切な事前審査がないまま外国人の個人データにアクセスする場合があり、事後的な司法救済の方法もなく、EU基本権憲章が保障するプライバシー・個人データ保護レベルを満たしていないことが判決の理由とされました。EUと米国とのあいだで、人権保障か、それとも国際テロから国と国民を守ることを優先するのか、各々がもっとも重視する基本価値の対立が表面化したわけですが、その底流にはデータ覇権をめぐる世界の対立軸が見えます。

データ主権確保の動き

この判決の背景となったソーシャルメディアの分野では、米国が世界市場を支配しています。これを苦々しい思いで見てきたEU諸国・企業がこの判決に対して、EUの価値観が米国のデータ覇権に一矢報いたと溜飲を下げていることは想像に難くありません。中国はもっとストレートに、自国のソーシャルメディア市場を囲い込んでいます。一方、人工知能、自動運転、自律制御など、世界を変えるIT新技術を成功させるためには、いかに多くのデータを囲い込むかが重要なポイントの一つになります。すでに中国、ロシア、インド、ベトナム、トルコなどいくつかの国々では、データの国外持出しを制限する「データローカライゼーション規制」を強化し、データ主権を先進国に握られることを阻止しようとしています。

多国間ルールの危機と日本の役割

EUvs米国、米国vs中国、先進国vs新興国など、データ覇権をめぐる複数の対立軸が顕在化する環境でデータ・プライバシーのコンサルティングという仕事に携わる筆者は、世界で事業展開しているお客さまから、各国規制対応に苦慮している実態をうかがうことが増えました。こうしたなか、昨年のG20大阪サミットで、安倍総理（当時）が、各国の規制を尊重しつつ、信頼にもとづく自由なデータ流通（Data Free Flow with Trust）を実現する多国間の枠組みを確立していくことを目指す「大阪トラック」を提唱しました。日本は多国間貿易ルールのなかで経済の繁栄を築いてきましたが、日本が国際データ流通における多国間ルールの確立に貢献し、データ覇権をめぐる世界の対立を緩和できることを期待しています。

株式会社 インターネットイニシアティブ

本社　東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-4466

関西支社　大阪府大阪市中央区北浜 4-7-28 住友ビルディング第二号館 5F
〒541-0041　TEL:06-7638-1400

名古屋支社　愛知県名古屋市中村区名駅南 1-24-30 名古屋三井ビルディング本館 4F
〒450-0003　TEL:052-589-5011

九州支社　福岡県福岡市博多区冷泉町 2-1 博多祇園 M-SQUARE 3F
〒812-0039　TEL:092-263-8080

札幌支店　北海道札幌市中央区北四条西 4-1 伊藤・加藤ビル 5 階
〒060-0004　TEL:011-218-3311

東北支店　宮城県仙台市青葉区花京院 1-1-20 花京院スクエアビル15F
〒980-0013　TEL:022-216-5650

横浜支店　神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-470-3461

北信越支店　富山県富山市牛島新町 5-5 タワー 111 10F
〒930-0856　TEL:076-443-2605

中四国支店　広島県広島市中区銀山町 3-1 ひろしまハイビル 21 5F
〒730-0022　TEL:082-543-6581

新潟営業所　新潟県新潟市中央区東大通 1-3-1 帝石ビル 4F
〒950-0087　TEL:025-244-8060

豊田営業所　愛知県豊田市西町 4-25-13 フジカケ鐵鋼ビル 5F
〒471-0025　TEL:0565-36-4985

沖縄営業所　沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル 8F
〒900-0015　TEL:098-941-0033

IIJグループ／連結子会社

株式会社 IIJグローバルソリューションズ
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-6777-5700

株式会社 IIJエンジニアリング
東京都千代田区神田須田町 1-23-1 住友不動産神田ビル2号館 7F
〒101-0041　TEL:03-5205-4000

ネットチャート株式会社
神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-476-1411

株式会社 IIJイノベーションインスティテュート
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6501

株式会社 IIJプロテック
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6766

IIJ America Inc.
55 East 59th Street, Suite 18C, New York, NY 10022, USA
TEL：+1-212-440-8080

IIJ Europe Limited
1st Floor 80 Cheapside London EC2V 6EE, U.K.
TEL：+44-0-20-7072-2700

株式会社トラストネットワークス
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6490

発行／株式会社インターネットイニシアティブ 広報部
お問い合わせ／株式会社インターネットイニシアティブ 広報部内「IIJ.news」編集室
〒102-0071 東京都千代田区富士見2-10-2 飯田橋グラン・ブルーム
TEL: 03-5205-6310　E-mail: iijnews-info@iij.ad.jp

編集／村田茉莉、鈴木健二、小河文乃、風穴江
編集協力／合同会社 Passacaglia
表紙イラスト／末房志野
デザイン／榊原健祐 (Iroha Design)
印刷／株式会社興陽館 印刷事業部

表紙の言葉「急カーブ」

学生時代、部活の合宿で山道をランニングしました。急なカーブを曲がる時は、早く走りたい気持ちが先走り、何度も転びました。スピードを緩めたり、姿勢や視線の先をどこにおくかで、カーブを上手く曲がりきれるかが変ってきます。今は、人生でも同じことが言えるのかもしれない、などと思います。

末房志野

◎IIJ.news表紙のデザインを壁紙としてダウンロードいただけます。ぜひご利用ください。
URL: https://www.iij.ad.jp/news/iijnews/wp/
◎IIJ.newsのバックナンバーをご覧いただけます。URL: https://www.iij.ad.jp/iijnews/

編集後記

近頃、オフィス付近でアカトンボをよく見かけます。前にしか飛ばず、退くことを知らないトンボを、戦国時代の武将たちは「勝虫」と好み、兜や着物のモチーフとしてとりいれました。ところで、トンボは変温動物なので、止まる場所を工夫しながら体温調整をしているそうです。さらに、飛びつつその場にとどまる高度な技（ホバリング）もできます。静止する場の状況を見極めようとするトンボの在り方、前にしか飛べないこと以上に「勝虫」っぽくありませんか？（A）／今年の夏に電子書籍リーダー「Kindle Paperwhite」を買って読書の仕方が少し変わりました。読書時間は、通勤電車の往復60分と寝る前の30分。以前は重いのが嫌で通勤中はもっぱら文庫本。重いハードカバーの単行本を敬遠していました。それがKindleを買ってからは、単行本で気になったものも手軽に楽しめるようになりました。今は、最近出た『三体』（劉 慈欣著・早川書房）の続編を通勤電車で快適に読んでいます。途中で飽きたら別の本を読んだり、人に聞いたお薦めの本は週末に本屋に行かずともその場ですぐに購入して読むことができたり――重さわずか200gの中に100冊以上入れられるKindleのおかげで本の選び方が変わり、本がより身近なものになったような気がします。そろそろ読書の秋ですね。（M）／先日、東京都の立川市と昭島市にまたがる昭和記念公園に行ってきました。園内には、水鳥の池や日本庭園、バーベキューガーデンなど様々な施設があるのですが、私のお目当ては、広大な原っぱの一角を埋め尽くすコスモスで、この時期になると毎年のように、観賞のために訪れます。赤や白、紫色の花びらが視界いっぱいに咲き乱れている光景は圧巻です。「秋桜」と書くコスモスは、春の桜ほど花見に混雑がなく、落ち着いて眺めることができるのも好きなところです。（K）／駅の自動改札機のフラッパーゲート。人が近づくと閉じるのは「強行突破しないように通せんぼ」しているのだと思ってましたが、友人の「向こう側から人が入って来ないように守ってくれてる」説を聞いて、目から鱗が落ちました。ゼロトラストも、最初は「何もかも信用しない」なんて、何て世知辛い……と思いましたが、実は、手間暇惜しまず細かく確認、認証することで、いつでも、どこでも、安心して利用できるようにしてくれているということですよね。そう考えると、言葉から受けていた物々しいイメージから、何だか頼もしい相棒に思えてくるから不思議。（風）

Information

1 オンラインイベント「IIJ デジタルワークプレース（DWP）Day」2021年のデジタルワークプレース ～情報システムが叶えるワクワクする働き方～

「デジタルワークプレース」とは、デジタル時代の働き方を支える快適な仕事空間であり、企業価値を向上させる成長戦略の1つであり、2021年のIT戦略の要となる、重要なキーワードです。本イベントでは、デジタルワークプレースに対する理解を深めるとともに、情報システムでワクワクする働き方を叶えるためのヒントをご紹介します。

開催日時　2020年11月5日（木）　14:00～17:20
参加費　無料（事前登録制）
参加方法　お申し込み完了後、メールにてご案内します
イベント詳細・申込　https://event.iij.jp/dwp/

2 IIJ ビジネスリスクマネジメントポータル（BizRis）リニューアル

世界のプライバシー保護法制およびIT対応を支援する会員制ポータル「IIJビジネスリスクマネジメントポータル（BizRis）」が、10月9日にリニューアルいたしました。

●注目のコンテンツ：グローバル・オーバービュー

世界のプライバシー保護規制の最新動向について、

a. プライバシー保護規制のグローバルマップ
b. 各国のプライバシー保護規制比較一覧表
c. 31カ国・地域毎の個別レポート

の3部形式で紹介する資料です。日本企業から問い合せの多い17調査項目（クッキー規制を含む）を対象に、法律事務所の協力も得て、四半期毎に内容を更新します。

●その他

・コンプライアンス対応に役立つニュース、解説
・実務に役立つ各種テンプレート、対応の手引き
・専門家のアドバイザリーサービス

も掲載しています。

ポータル詳細、会員登録　https://portal.bizrisk.iij.jp/


IIJ
Internet Initiative Japan