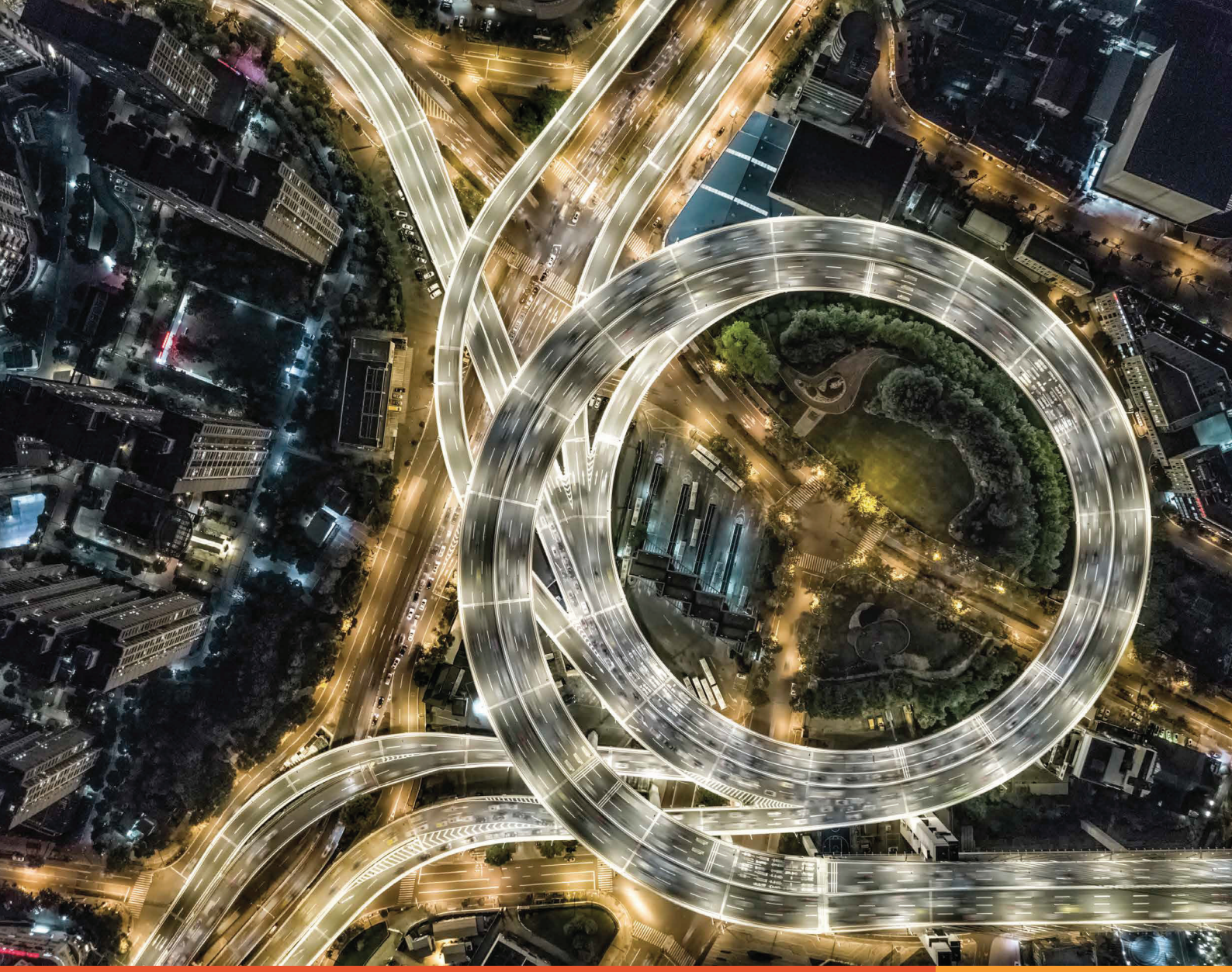


未来の安全な5Gのために

5Gネットワークの可能性をフルに実現するために
サイバーセキュリティが最重要である理由

pwc

www.pwc.com/jp

目次

概要

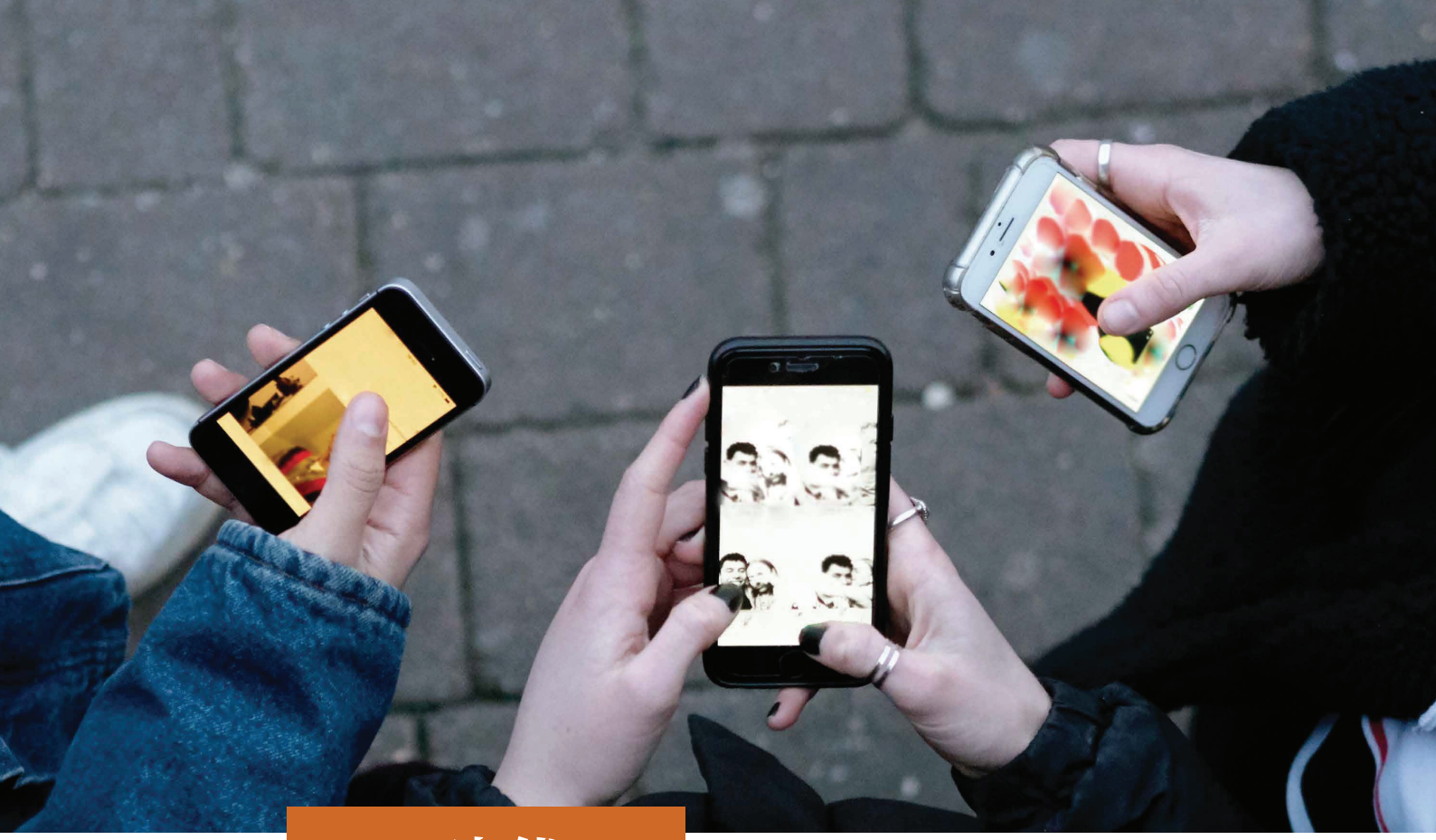
5G世界の可能性とセキュリティを結び合わせる

世界各地で人々の生活や仕事は互いに接続されたデバイスで変わりつつある。デバイスをつなぎ、コミュニケーションを可能とする通信ネットワークはこの革命に不可欠である。この意味で、高速・高帯域の5Gネットワークの実現は大きな前進である。ただし、これは全体像の中で見る必要があろう。さまざまなことが喧伝されてはいるものの、実のところ、5Gで可能となるサービスの多くは、5Gの前身である4Gや各種LPWAN（低消費電力広域通信）ですでに提供されている。

とはいえ、5Gの根底にある技術は、通信ネットワークの再概念化など、根本的に従来技術と異なる点がある。第1世代～第4世代のモバイル技術は全て物理的アーキテクチャを基礎としていた。5Gは新たなハードウェアを含んでいるとはいえ、何よりもまず仮想ネットワークである点が重要であり、これにより、ネットワークと無線通信の収束が実現した。この飛躍的進歩は、相次ぐ技術革新を生み出すだろうが、最も影響が感じられるものは無線技術の新たな、または強化された利用法であろう。第4次産業革命（4IR）インフラストラクチャー、スマートシティ、自動運転車、遠隔手術、進化し強化された人工知能（AI）システムなどが考えられる。

今日、こうした動きは新型コロナウイルス感染症の世界的流行下で起きている。世界各国で何らかの「ステイ・アット・ホーム」令が発出され、在宅で勤務する者も多数に上り、その際使用される通信回線は5Gネットワークに基づくものが急速に増えつつある。デジタル変革で先行する企業は今回のコロナ禍に対応するにあたって、技術やサイバーセキュリティ、レジリエンス確保にこれまで行ってきた投資が結実したことを物語っている。

こうした変容がサイバーセキュリティを厳しく精査することにもなった。一部の評論家は、5Gネットワークが従来技術以上の数のデバイスに接続可能で、「エッジ（ユーザーに近い場所）」にあるデバイスの処理能力も用いて分散処理を行うことから、サイバー攻撃が多面的になるのではないか、との懸念を表明している。しかし、5Gに予想される脆弱性は、その多くが5Gエコシステムの要素に起因しており、典型的なものは端末デバイス自体のセキュリティである。ただし、5Gネットワークにおけるサイバーセキュリティ問題は克服可能であり、世界規模の取り組みにより5Gの可能性をフルに引き出すイノベーションの確固たる基礎を提供しうるという明るい見通しもある。



5G時代へ

現在、世界は膨大な数の5G対応機器がつながるマッシブIoTでサポートされ、互いにつながる時代に入ろうとしている。この世界で、5Gはスマートシティや第4次産業革命のオペレーティング・モデル、スマートホーム、スマート交通、スマート医療、その他無数の可能性を秘めた利用例の根幹となっている。PwCが先ごろ世界経済フォーラム（WEF）と共に発表したレポート「The Impact of 5G: Creating New Value across Industries and Society」では、すでにビジネス環境を変貌させつつある5Gの利用例を幅広く概説している。

新技術全般に言えることであるが、5Gの導入にあたってはサイバーセキュリティに対するアプローチを見直す必要がある。政府、地方自治体、企業をはじめとする多くの団体がすでに5G革命に取り組んでその可能性を追求しようとしており、見直しはこの意気込みをくじくような形とならないように配慮しなければならない。実際、5G特有のリスクを理解し、対策を講じれば、従来以上のレジリエンスを実現し、企業の収益や社会的利益を生み出す強力な武器として5Gを使うことができるだろう。このことは、今回のパンデミックが人々の生活と働き方をかつてないやり方で変容させる中、これまで以上に絶対的な条件となっている。

5Gが従来と異なる理由については数字が物語っている。5Gの技術特性を組み合わせると（技術特性については5ページの「5Gの技術特性」を参照のこと）5Gは4Gよりも100倍程度速いスピードを達成可能で、対応可能な接続数も大幅に多い。こうしたメリットは超低レイテンシーでさらに高まる（レイテンシーとはリクエストに対するレスポンスを受け取るのに要する時間を指す）。

消費者は、超高解像度（UHD）の映画を秒単位でダウンロードできるようになることを期待しているものの、5Gの真価は、幅広い革新的なアプリケーションを実現可能にする技術特性を有していることであろう。エンターテインメントの楽しみ方はもちろん、働く場所や働き方、交通手段、健康維持の方法なども変貌させる可能性がある。AIを用いてパーソナライズした5Gアプリケーションは人のさまざまな活動をサポートする役割を今以上に担うようになるであろう。

5Gではネットワークがソフトウェアで実現され、分散デジタルルーター経由で転送され、末端から近い端末に処理を移転することで処理速度やパワーを最適化しており、喧伝されているさまざまな可能性が実現できる理由もそこにある。この点が、ハブ・アンド・スポーク方式を採用した過去世代のモバイルテクノロジーと異なっている。

「ゼロトラスト」アプローチ

5Gネットワークの潜在的メリットを消費者や企業、社会全体に向けてフルに提供し、かつエンドユーザーの安全を保証するためには、ネットワーク自体を安全に保つことが非常に重要である。コロナ危機によりテレワークを採用する企業が増加し、遠隔医療が用いられる場面も増える中、セキュリティの重要性はなおいっそう高まっている。例えば、スタッフがオフィス外で働いている場合、企業のITシステムには大きな負荷がかかり、サイバーセキュリティ攻撃に対する脆弱性が高まってしまう。また、患者がタブレットやPC、携帯電話などを通じて医師から診察を受ける場合、機密性の高い医療情報が安全に保たれる必要がある。

5Gも含め、ネットワークをサイバー攻撃から守るために不可欠な第一歩は、脆弱性が発生する可能性のある箇所を理解することである。これは主として接続点であり、リスクがネットワークの一要素から別の要素へと転移する箇所である。4Gでもそうであったが、5Gの場合もこのリスク転移の両サイドには別々の企業が関与していることが多い。つまり、エンド・ツー・エンドのセキュリティを有効にするためには協調的アプローチが不可欠なのである。テクノロジーツールは急速に進歩し、企業のみならずサイバー犯罪者も自分の利益のために進歩したツールを使おうとしているため、協調的アプローチには迅速性も求められる。

5Gエコシステムにはモバイル通信会社、ネットワークベンダー、システムインテグレーター、エンドユーザー企業など多数の関係者がいる。コンポーネントをネットワークに接続する場合、全てのコンポーネントに関してその安全性を確認し、プロファイリングし、評価し、必要であればその評価に基づいて5Gサービスへのアクセスを制限する必要があり、関係者全てがこれに同意することが望ましい。これは以下の要素を基礎とする戦略によって達成可能である。

1. ゼロトラストアプローチ：デバイスやソフトウェア全てを対象とするエンド・ツー・エンドの堅固なセキュリティ体制は、5Gエコシステム全体がさらされるリスクを減少させる。ネットワークやリソースへの接続に先立ってデバイスのセキュリティ水準を評価し、そのニーズとセキュリティ水準に応じたリソースアクセスを許可する。また、ソフトウェアはコアソフトウェアからIoTデバイス用ソフトウェアまで、また、ファームウェアからクラウドまで、全て慎重にチェッ

5Gの技術特性

5Gは、コアシステムや管理システム、また無線からアプリケーションに至るプロトコルレイヤー全般など、ネットワークの特徴の多くを変化させる。その技術特性には以下のようなものが含まれる。

- ネットワークスライシング。これにより、サービスプロバイダーはサービスとしてのネットワーク（NaaS）を特定の契約者グループに提供することができる。NaaSでは、契約者グループはニーズに応じてデバイスやサービスを自身で管理できるなどの柔軟性を得ることができる。
- 強化されたモバイルブロードバンド（1～20Gbps）。4Kや8Kの高解像度3Dビデオ通信やオンラインゲームなどをサポート。
- 超低レイテンシー（1ms未満）。拡張現実や仮想現実、遠隔医療、高度交通システム、製造業におけるオートメーション化など、ミッションクリティカルなサービスに重要。
- 大量のデバイスを扱える接続性。自動車、モバイル通信契約者、企業、IoTなど向け。
- 高い可用性と高密度。何十億人もの契約者に無制限の接続を提供可能。
- 低電力消費。マシン・ツー・マシン通信では最長10年の電池寿命。

こうした能力を実現するために、5Gは異種アクセスネットワークをサポートし、可変帯域に対応する新しい無線インターフェースを備えている。パケット・コア・ネットワーク更新も実装作業が進行中であり、従来のモバイルサービスと5Gモバイルサービスでインフラストラクチャーを共有するなど、サービス提供や業務効率の向上を図っている。

クする必要があり、ソフトウェアの開発や実装に先立って、リソースハブやコードベースはマルウェアが含まれていないことを確認しなければならない。アプリケーション・プログラミング・インターフェース（API）はリスクのレベルごとに区分けし、アクセスを制御する必要がある。

2. ユニバーサル暗号化：データ窃盗やデータ破壊リスクを抑えるために、通信会社をはじめとする5G関係者はエンドポイントとサービス間の通信セキュリティを確保するために強力な暗号化方式を採用しなければならない。採用する暗号化方式は柔軟なものでなければならず、時の経過とともに基準やリスクが高度化した場合、これに伴って強化可能でなければならない。また、主要な管理プロセスを集中型にすれば、いわゆる中間者攻撃（互いに正しい相手とやりとりしていると信じているネット参加者2名の間にハッカーが割って入り、両者のやりとりを傍受する攻撃）のリスク軽減に有用であろう。

3. AIによる制御：機械学習（ML：マシンラーニング）やAIは、超高密度のマシン間通信や超低レイテンシーの各種アプリケーションなどを対象にセキュリティ方針の徹底を図るために必要な高速かつ正確なインサイトおよびインテリジェンスを提供し、攻撃パターンが変異しやすいサイバーリスクの識別、軽減に大きな役割を果たす。AIや機械学習技術は能力が高く、トラフィック分析、ディープ・パケット・インスペクション、脅威識別、感染隔離など、5Gアーキテクチャ全般のセキュリティ制御に用いられよう。

AI――5Gネットワークやアプリケーション、デバイスの中核における強力なツール

通信会社は5G設置に乗り出しているが、ネットワークのかつてない複雑さへの対応が課題となっている。その主な原因としては、5Gが高密度分散ネットワークであること、大規模アンテナアレイが必要でその設定が難しいこと、ネットワークインフラストラクチャー全般の更新が求められること、などが挙げられる。IoTや関連のスマートシステムからは、予想されるものも予想外のものも含めてさまざまなニーズが生じると思われ、このようなニーズに対するソリューションの開発を継続的に行っていくための体制づくりも必要であろう。ネットワークを今以上に迅速かつ適切に管理することが求められる。

AIはネットワークの品質管理に動的に関与することにより、現在可能な手法よりも迅速にネットワークの問題を検知、修正することができると考えられ、こうした課題に対処するために必須のものとなろう。ネットワークスライシングに関しても、オペレーターのスライシング戦略を最適化してスライスアロケーションを迅速に評価、診断、決定するなど、その可能性をフルに引き出すために必要とされよう。

ネットワークから離れるが、過日のPwCのレポートにおいて、AIと5Gを組み合わせたコネクテッドデバイスが相次いで実現し、「スマート」という言葉の意味が2つの点で変貌するであろうということが強調された。第1は、ユーザーインターフェースがタッチ式からタッチ・音声併用、あるいは音声のみへと急速に変化していくことである。第2は、こうしたデバイスがユーザーの求める作業には個別のアプリを用い、AI駆動のアルゴリズムでユーザーのニーズを予想、求められる前に自動的にニーズを満たすであろうという点である。

このような進歩を通じて、AIと5Gはエンドユーザーに大きな影響をもたらすであろう。第1に、5G上で送られる大量なデータにより自動化やカスタマイズが現在よりも進んだ製品やサービスが生まれ、パーソナライゼーションが進む。第2に、AIが人の能力を拡張し、人とマシンの関係性をより強固なものとするなど、人々のデジタル体験が進化して親近感を覚えやすく人間性を感じるものとなる。この2点が合わさると、第3の影響が生じる。すなわち生産性の大幅向上および仕事と私生活における心の余裕によって、人々が本当に興味のある活動を追求する余暇が増える。

5Gの世界において、AIはサイバーセキュリティでも活用される。悪意ある攻撃者の用いるツールは高度化を続けているが、AIと機械学習は企業にとってこうした攻撃者からシステムを守る強力な新ツールとなるであろう。AIを用いてデータをチェックし、疑わしいデータはフラグを立てて人間が分析、その結果をAIにフィードバックすることでAIの予測精度向上を図る。PwCでは、このサイクルが最も効果的な防御であり、最重要システムの防御に最適であろうと考えている。このようにして、あらゆる用途で5Gのメリットをフルに発揮させるイノベーションのための堅固で安全な基盤が形成されるのである。

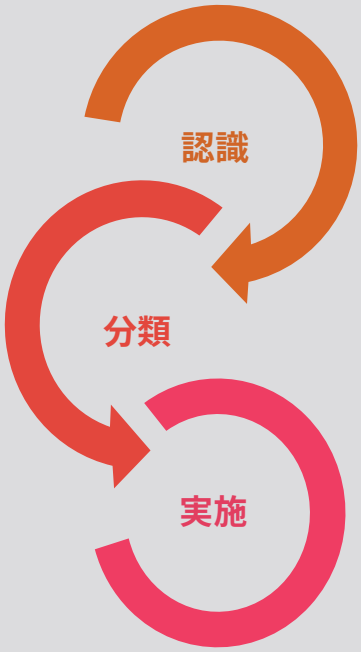
5Gも含め、ネットワークをサイバー攻撃から守るために大変重要な第一歩は、脆弱性の発生する可能性のある箇所を理解することである。

この戦略では、5Gエコシステムに参加している各企業が集団で5G環境を守る。このことは、企業がクライアントにサービスを提供したり提携先と業務を遂行したりする能力に過度の影響はないだろう。この戦略を運用する方法に、ゼロトラストアーキテクチャ（ZTA）と称するID駆動型モデルを採用する方法があり、実績もある。これは、重要なデータやインフラ資産にアクセスされている場合に、「誰が、何を、どこで、なぜ、どのように」アクセスしたかを特定する総合情報インフラストラクチャー・セキュリティ・モデルである。

ZTAでは、セキュリティ機能を用いてポリシーを実施し、場所や接続方法を問わず全ユーザー、デバイス、アプリケーション、データリソース、およびその間の通信トラフィックを保護する。図表1に示すACEモデル（認識（Awareness）、分類（Classification）、施行（Enforcement））はZTA実装を考える企業にとって参考になろう。

図表1：5G向けゼロトラスト方針の採用

総合情報インフラストラクチャー・セキュリティ・アプローチでは、重要データやインフラストラクチャー資産へのアクセスにあたり、誰が、何を、どこで、なぜ、どのようにアクセスするかを調べなければならない。このID駆動型アプローチは一般にゼロトラストアーキテクチャ（ZTA）と呼ばれ、セキュリティ機能を用いてポリシー順守を求め、ACEモデルを用いて場所や接続方法を問わず全ユーザー、デバイス、アプリケーション、データリソース、およびその間の通信トラフィックを保護する。



プロファイリング：ネットワーク上のエンドポイントやアプリケーションは全て特定し、プロファイリングを行う。
評価：デバイスのセキュリティ状況を確認する。
特定：どのユーザーやデバイスがどのように接続されているかを知る。
学習：モニタリングとログ記録でデバイスやユーザーの挙動を継続評価する。

重み付け：保護対象の資産、データ、アプリケーションの価値や重要性を評価する。
リスクスコア：セキュリティエクスポージャーの影響に応じてリスクスコアを割り当てる。
グループ割り当て：データ、ユーザー、エンドポイントをデータ分類バケットやデータ分類グループにマッピングする。
アプリケーションの優先順位付け：業務権限、データ分類バケット、該当するリスクスコアを用いて優先順位を示すセキュリティ方針を生成する。

制限：セキュリティ方針に基づき、アクセス適格性とアクセス限界を定める。
隔離：セキュリティ侵害やセキュリティ違反の検知、抑制、隔離方法を定める。
通知：セキュリティ侵害やセキュリティ違反の通知メカニズムを用意する。
区分：アプリケーション、エンドポイント、ユーザーをID駆動型で区分けするフレームワークを定める。
施行：定めたセキュリティ方針に基づき、アクセス限界において、IDベースの制御を実施する。

出所：PwCによる分析

設計されたレジリエンス

ゼロトラストアプローチとこれに基づくアーキテクチャを採用済みの企業は、5G時代にサイバーレジリエンスを開発し、組み込むための好ポジションを占めている。これらを達成するための貴重なガイダンスとして、PwCは世界各国の企業3,500社以上を対象とした調査に基づく最新レポート「Global Digital Trust Insights Survey 2021」を提供している。

この調査によれば、高い水準のレジリエンスを有する企業は、レジリエンスの開発戦略に関する3つの分野で上位25%に入っていることが判明した。基本的に「設計されたレジリエンス」を重視しており、他社を大きくリードし、結果として以下のようなことが可能となっている。

- **データ資産の可視性向上：**レジリエンスの高い企業は、データ資産や既存プロセスが業務の中核にどのような影響を与えているかを常にモニターしている。デジタル・トラスト・インサイト・レポートでは、高いレジリエンスをもつ企業の91%が正確な資産一覧を作成、常に最新の状態を保っているが、その他の企業でこれができているのは47%にすぎない。特に多数のベンダーと協働している企業の場合は、この一覧にサードパーティーとの共同作業を含める必要があり、5Gの世界ではまず間違いなく共同作業をすることになるだろう。

  レジリエンスに劣る企業は先行企業に追い付くための行動を取るべきであろう。自動でリアルタイムの資産一覧やネットワーク全体で実行中のプロセスを正確に把握するためのマッピングなどができれば、レジリエンスで劣る企業も自社の抱える脆弱性を認識し、その対策に着手することができよう。

- **耐性テストを行う：**レジリエンスに優れた企業は大局的観点に立ち、リスクの高い状況に対処するために耐性水準を知ろうとする。調査では、サイバー攻撃を受けて基幹業務が影響を受けた場合、衝撃許容度、つまり、運用が中断された際の許容範囲内で防衛できた企業は3分の1に満たないことが判明している。大多数の企業は、調査対象中で最も規模の大きい企業も含め、こうした事態が発生した場合、重要業務サービスへの障害発生に対処できていなかった。

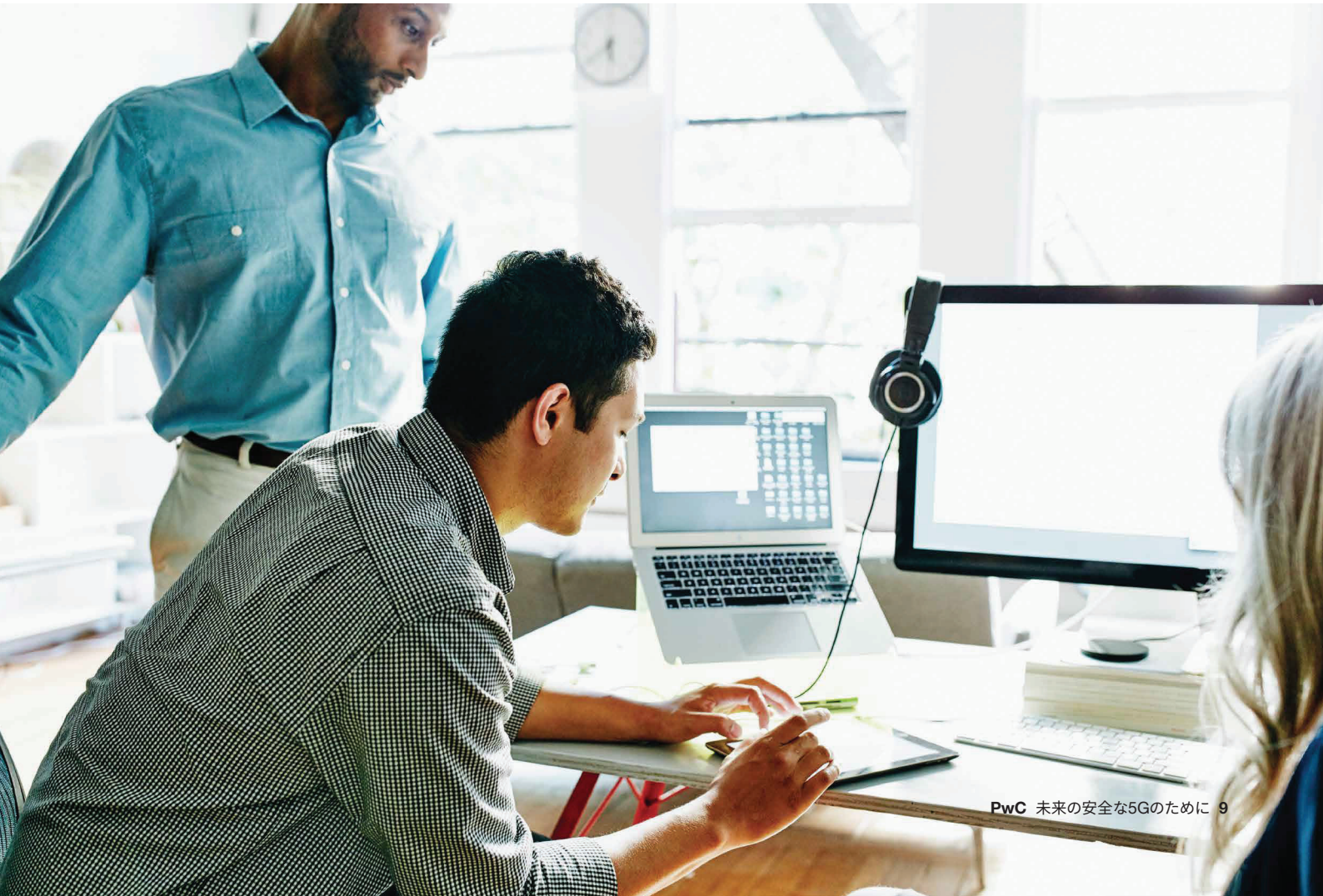
  重要業務サービスを特定し、基準を定めて衝撃許容度を明確にし、衝撃許容度をテストして業務サービスにマッピングすれば、企業は来るべき脅威への備えを万全にすることができる。

- **適応し、改良する：**レジリエンスに優れた企業は業務戦略を継続的に進化させる。データ資産の可視性を向上させ、許容度水準をテストすれば、企業は高レジリエンスリーグ入りを果たすことができる。しかし、技術が急速に進歩する場合、変化に適応できる企業は、高レジリエンス企業の中でも34%にすぎないことが判明した。

  全方位からの防御を鉄壁なものとするために、高レジリエンス企業の3分の1は新規技術採用に伴ってレジリエンスの改良を図っている。こうした企業は中核資産のパフォーマンスやIT依存度をモニターする専任チームを設けているところが多く、サイバー問題に起因する業務混乱が発生した場合には教訓を学び、業務サービスを迅速かつ着実に改善していくことができる。企業は自動化や制御を活用した先進の脅威ハンティング機能を対策の一環として採用することが望ましい。

上記3分野を合わせて実践すると、企業は伝統的な「災害復旧・業務継続モデル」型企業から「設計されたレジリエンスモデル」型企業へと移行するが、これはコロナ禍からの復興期を乗り切るために多くの企業が必要とすることであろう。「設計されたレジリエンス」を用いれば企業や業務、システムはサイバー攻撃から保護されることが実証されており、これはもちろん5G環境でも重要かつ有効である。

レジリエンスに劣る企業は先行企業に追い付くための行動を取るべきであろう。自動でリアルタイムの資産一覧やネットワーク全体で実行中のプロセスを正確に把握するためのマッピングなどができれば、レジリエンスで劣る企業も自社の抱える脆弱性を認識し、その対策に着手することができる。



スマートシティ――都市環境の未来を切り拓く

都市部の人口は急増を続けており、既存のインフラストラクチャーへの負荷も増加の一途である。世界各国において既存の都市をスマートシティへと変貌させることは今や急務であろう。英国規格協会（BSI）はスマートシティを「持続的・包括的かつ繁栄を続ける未来を市民に提供するため、物理的、デジタル的、人的システムが効果的に統合されている都市」と定義している。これはスマートシティがサイバー・フィジカル・システムの創造に物理システムとデジタルシステムを統合させる点を強調しており、まさに適切な定義と言えよう。

市民のニーズをより効果的に満たすことを目的に、デジタル化で数多くの都市システムを増強することができる。輸送システムやビル施設管理などがまず目に付くが、エネルギー、上下水道、公衆安全、廃棄物管理、公害防止などのシステムにも当てはまる。コロナ禍などの公衆衛生上の緊急事態にも対策のサポートに用いることができ、感染症のモデル化、検知、予測などや、政府に意思決定プロセスに必要なリアルタイムのデータを提供することができる。5Gは超高速、低レイテンシーのプラットフォームでこうしたサービスの基盤となり、スマートシティコンセプトの可能性をフルに実現するサポート役となるであろう。

スマートシティのシステムを安全に保つことは、インフラストラクチャー運用と市民の個人データ保護の2点で大変重要なことは明らかである。この安全はスマートシティシステムと接続するもの全ての開発にあたってゼロトラストアプローチを採用し、セキュリティを最重点に一から設計、評価、調整することで達成できる。

結論—信頼、レジリエンス、実現可能性を通して5Gの時流を掴め

5Gが世界を変える、とはよく耳にする言葉であるが、この誇張表現に流されてはいけない。確かに世界は変わりつつあるが、接続するスマートデバイスがほぼどこでも入手できるという事実がこの変化を推進しているのである。こうしたデバイスはネットワークを経由して接続され、ネットワークが重要な役割を果たしているのも事実であるが、あくまでこの新環境の一部分にすぎない。

とはいえ、5Gの到来がサイバーセキュリティ状況の変化を意味することは疑いようもない。明日の重要産業や社会活動のネットワークに、互いに接続された自動化コンポーネントが組み込まれる、5Gはその作業の流れや意思決定の連鎖の媒体となるであろう。デバイスは数百万台もあってさらに増え続けているが、特に自動運転車など低レイテンシーかつ高速な接続が必須の用途向けの場合、5G無しでは事実上使い物にならないであろう。スマートデバイスは多数が接続されているが、5Gはその中で最も接続されているコンポーネントであり、この点は決して誇張ではない。

こうした背景を考えれば、5Gエコシステム全般に効果の高いサイバーセキュリティが必須であることを疑う者はいないであろう。しかし、一般に5Gセキュリティ上の脆弱性とされるものは、その多くが5G技術に特有のものというわけではない。5Gネットワークに接続されるデバイスや暗号化アルゴリズム、AIエンジンなどに不正侵入やセキュリティ違反があった場合、5Gオペレーターやユーザーにとっては問題である。しかし、これは5Gに限った問題とは言えない。5Gの世界におけるセキュリティを有効なものとするためには、バリューチェーンに含まれる者全員がそれぞれの役割をしっかりと果たす必要がある。設置される全ての5Gネットワークの中心にサイバーセキュリティを据え、「設計されたレジリエンス」に裏打ちされたゼロトラストアプローチを取るよう、PwCが推奨するゆえんである。

そのために、企業経営者はセキュリティの根幹をなす三本柱に注力する必要がある。ここで三本柱とは（サイバーセキュリティ措置の採用を促進するための）信頼、（サイバー攻撃を防ぎ、乗り切り、復旧するための）レジリエンス、（既存の脅威や新たな脅威を克服するために迅速に対応するための）実現可能性である。この三本柱は健全なサイバー戦略の基礎であり、これにより企業は5Gを迅速かつ安全に実行することが可能となり、個人や企業、そして社会全体が確信をもってこの新しい強力なツールを安全に使用し、その能力を享受することができるようになろう。

お問い合わせ先

To find out more about how PwC can support your journey to a 5G-enabled future, please contact us.

Technology, Media and Telecommunications

Wilson Chow
Global Technology, Media and Telecommunications Leader
Partner, PwC China
+86 755 8261 8886
wilson.wy.chow@cn.pwc.com

Kirolous Zikry
Senior Manager, PwC UK
+44 77 2563 3388
kirolous.s.zikry@pwc.com

Cybersecurity & Privacy

Richard Horne
Partner, PwC UK
+44 77 7555 3373
richard.horne@pwc.com

Marin Ivezic
Industrial and IoT Cybersecurity
Partner, PwC Canada
+1 416 687 8672
m.ivezic@pwc.com

Peter Durojaiye
EMEA Cyber Impact Center
Director, PwC Hungary
+36 70 685 0360
peter.a.durojaiye@pwc.com

Grant Waterfall
EMEA Cybersecurity and Privacy Leader
Partner, PwC UK
+44 77 1144 5396
grant.r.waterfall@pwc.com

ゼロトラスト・アーキテクチャ実現支援サービス

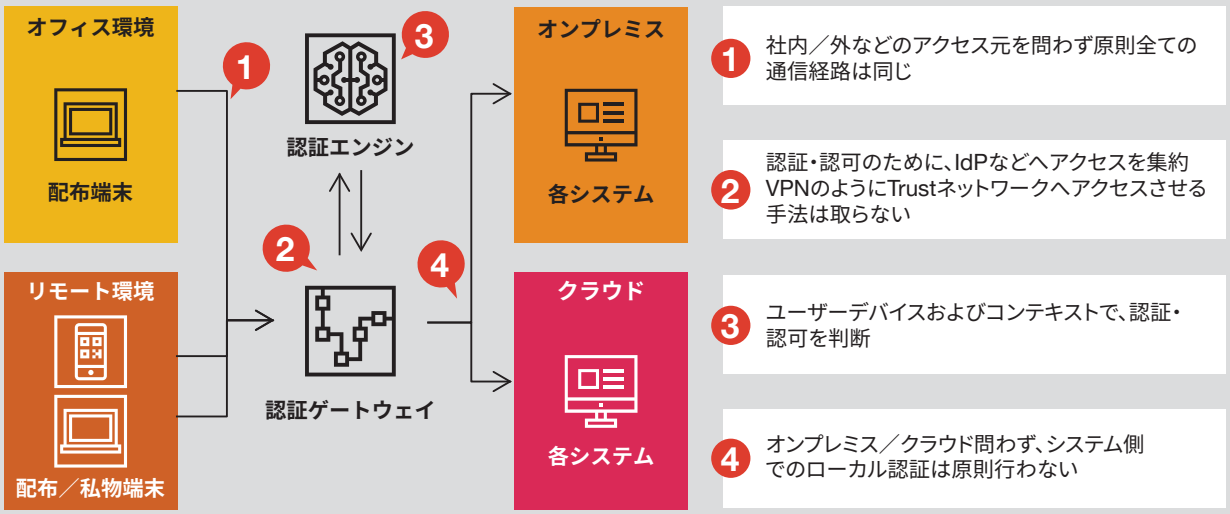
PwCコンサルティング合同会社では、リモートワークに代表される働き方の“ニューノーマル”に適応するための概念として注目されているゼロトラスト・アーキテクチャの実現支援サービスを行っています。

本サービスでは、ゼロトラスト・アーキテクチャの導入を検討する企業に対して、実現した場合のイメージを可視化し、ゼロトラスト・アーキテクチャがそもそも当該企業の課題を解決しうる打ち手であるかを評価・判断することから支援します。ゼロトラストかを推進することが有効であると判断した場合には、その達成に向けたポイントと主要なタスクを明確にします。

図表2：ゼロトラスト・アーキテクチャ実現支援サービスのアプローチ

アプローチ	実施事項
Step1 BxT	新しい働き方の創造 BxT（Business eXperienceTechnology）とは、技術、モノ、ルールや制約などを起点とした従来のビジネスの発想ではなく、「人間」を起点としてビジネスの在り方を考えるPwC独自のアプローチです。 ユーザーである社員を主役に新しい働き方について考え、リモートワークに求められるテクノロジーを当社コンサルタントワークショップ形式で検討します。
Step2 Assess	改善事項の抽出 現在のIT環境に対して、ゼロトラスト・アーキテクチャに基づく新しい働き方を実現するにあたり、障壁となるポイント、追加すべき機能を洗い出します。 貴社IT環境：設計書／構成図／通信フロー ⇔ pwc PwCナレッジ
Step3 Visualize	新たなITインフラの可視化 貴社の新しいビジネス基盤のBlueprint（概要設計）を資料化します。また、これらの実現に向けた主要なアクションを一覧化し、おおよそのコストについて報告を行います。 ※タスクやコスト（新規投資／削減可能な維持費）の詳細分析・報告は、オプションとなります（標準では簡易分析による報告を含みます）。

図表3：ゼロトラスト・アーキテクチャの概要



日本のお問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

PwCコンサルティング合同会社

■執筆者

藤島 太郎
マネージャー
携帯通信会社で米国でのMVNO事業の立ち上げなどを経て、PwCコンサルティング入社。
ハイテク、メディア&エンターテイメント、通信業界のクライアントを中心に幅広く支援を行っている。
特に、デザインコンサルティング手法を用いたコンセプトの設計、サービスデザイン、施策立案等、カスタマーエクスペリエンスの高度化・新規事業開発を得意とする。
PwC Japanグループがすすめる5G関連プロジェクトの推進リーダー。

坂口 博哉
マネージャー
大手外資系コンサルティングファームを経て現職に至る。
ハイテク産業、製造業、通信業界を中心に事業戦略立案～バリューチェーン改革～新業務／システム構想策定（PMO支援を含む）までを一気通貫で支援した経験を多数保有。
特にカーブアウトに伴うスタンドアローン企業の再編、トランスフォーメーションについて数多の実績を有し、複数のプロジェクトにおいて、プロジェクト責任者を複数担当。スタンドアローンイシュー全般に対して即効性のある改革をテーマに多数リード。
近年はコーポレート全体のDX化についても支援多数。

■執筆協力者

福永 新一
シニアアソシエイト

www.pwc.com

本報告書は、PwCメンバーファームが2020年2月に発行した『securing 5G's future』を翻訳し、日本企業への示唆を追加したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/gx/en/industries/technology/publications/securing-5g.html
日本語版発刊年月：2021年2月　管理番号：I202012-07