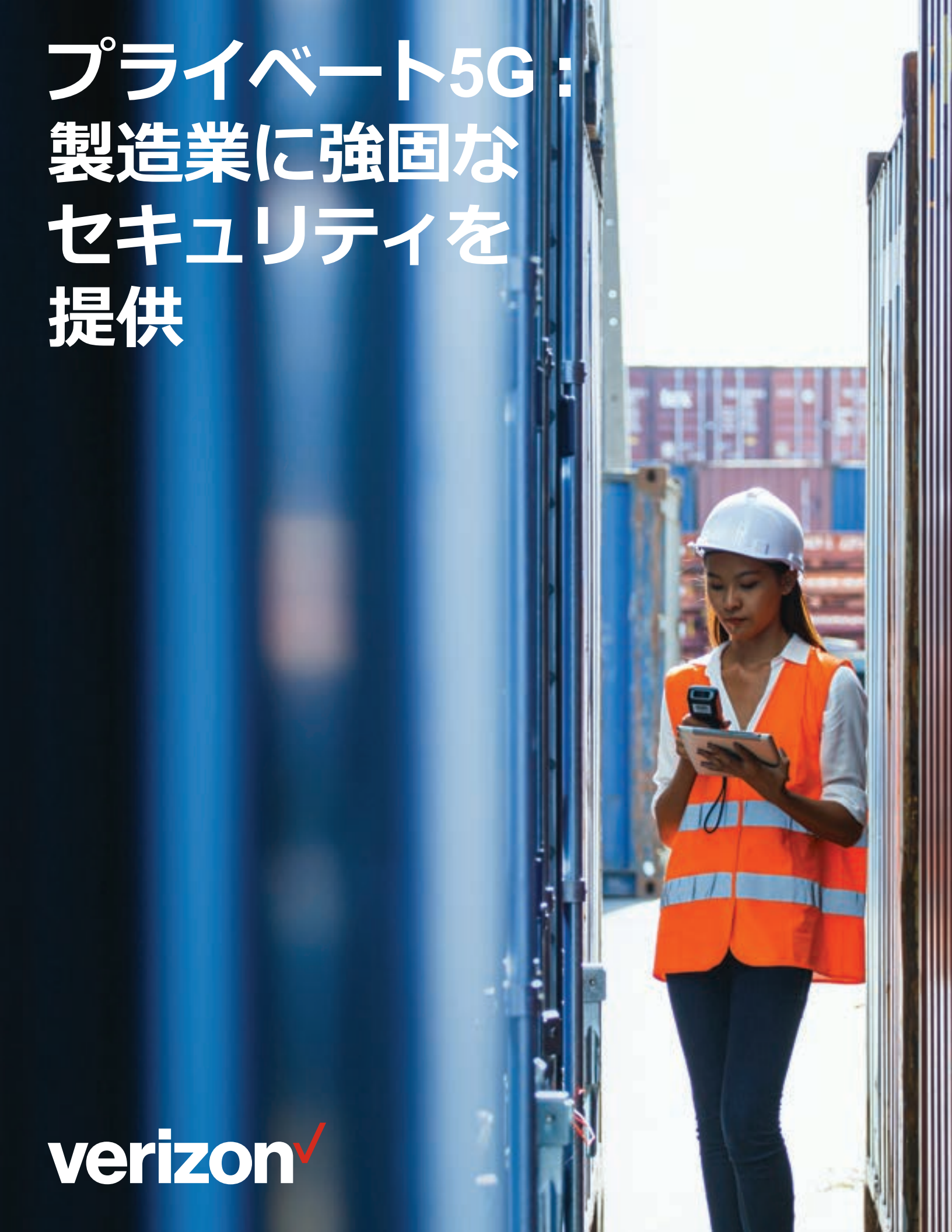
プライベート5G：製造業に強固なセキュリティを提供



verizon

目次

このホワイトペーパーでわかること	**03**
問題点：高度な接続性の選択肢が多すぎる	**04**
5GとWi-Fiの比較	**05**
5Gにおける選択肢：パブリックとプライベート	**06**
5Gと産業環境におけるセキュリティの主な検討事項	**07**
NIST CSF の項目	**09**
特定	09
防御	10
検知	11
対応	11
復旧	11
まとめ	12

このホワイトペーパーでわかること

5G技術は、その期待からビジネスにおける実用化へと急速に進化し、企業の多くがすでにプライベート5Gのメリットを実感しています。5Gの導入に前向きな企業、特に工業や製造業の企業は、ここ数年、5Gのユースケースを開発し、業務を変革することを推進してきました。そして今、実際に工場内、研究所、そして現場で実現しつつあります。「第4次産業革命」で約束されていたことが現実のものとなりつつあります。

しかし、依然としてセキュリティには懸念が残ります。

5G技術は、機密データやシステムの保護を強化するためのセキュリティ管理機能を備えていますが、企業のセキュリティプログラムに根深く残る従来の課題が5Gによって自動的に解決されるわけではありません。クラウド、モバイル、産業分野向けモノのインターネット（IIoT）などの変革をもたらす技術を積極的に推進する事業部門に、企業のセキュリティチームの監視体制が従来から追いついていなかったとしたら、5Gの採用後もその課題を抱えることになります。

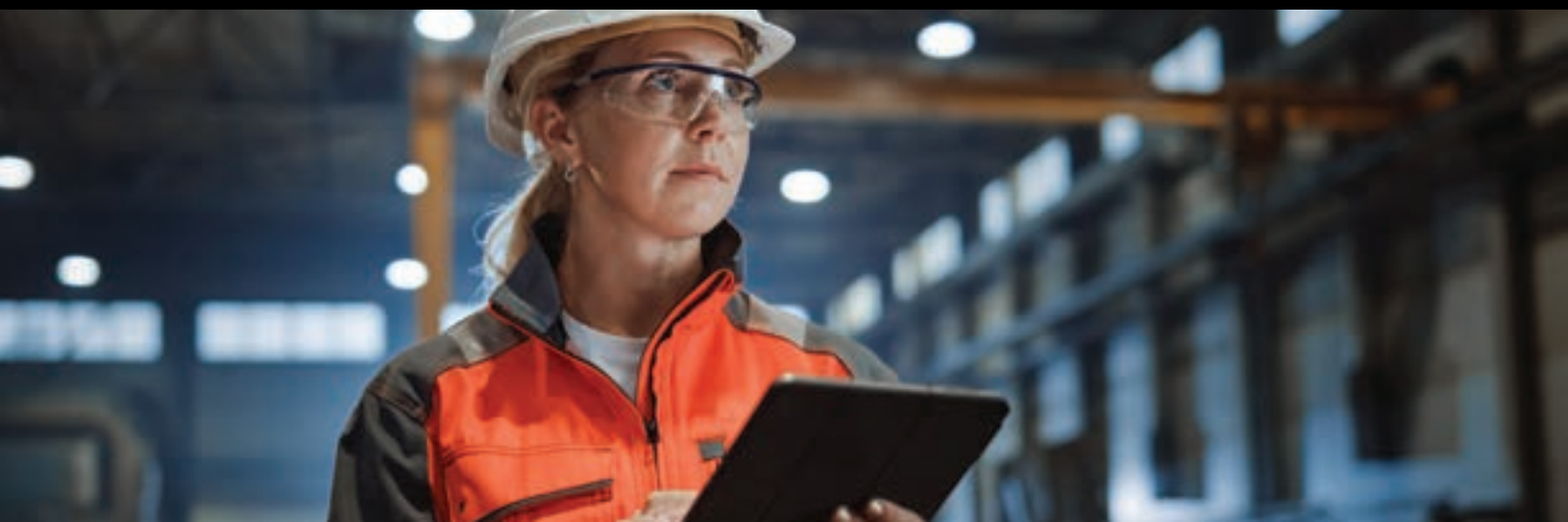
とはいえ、5Gによってビジネスの安全性を強化するための道筋はあります。

米国商務省のNIST CSF（National Institute of Standard and Technology Cybersecurity Framework/「重要インフラのサイバーセキュリティ対策を改善するためのフレームワーク」）は、企業のIT資産のセキュリティを向上させ、特定の5Gユースケースに内在するリスクを軽減するために必要なガイダンスを提供しています。このフレームワークは、ISO 27110などの他の規格も準拠している世界標準とみなされています。

このホワイトペーパーでは以下の内容を扱っています。

- パブリック5Gとプライベート5Gの違い
- 産業環境でのプライベート5Gの使用と、それに関連するサイバーセキュリティの検討事項へのとりくみ
- 5Gや「インダストリー4.0」を導入する際に、セキュリティを強化するためのNIST CSFの活用法

5G技術のメリットを完全かつ安全に実現するためには、セキュリティチーム、ITおよびネットワークチーム、IT部門以外のビジネスリーダーを含めたコラボレーションが鍵となります。そのコラボレーションを可能にするための共通フレームの参考資料として、このホワイトペーパーをご利用いただければ幸いです。



問題点：
高度な接続性の選択肢が多すぎる

製造業をはじめ、流通センター、鉱業、エネルギー生産など、多くの産業において、高度なネットワーク技術に基づいたユースケースがビジネスのあらゆる側面を変革しています。

マシン間通信（M2M）は長年標準とされてきた業務手順にとって代わり、IIoTが生成する膨大なデータはほぼリアルタイムで分析されることで積極的な活用が可能になります。また、ワイヤレス通信に基づくタイムセンシティブネットワーキング（TSN）やAGV（無人搬送車）などの新しいユースケース、あるいはビデオカメラの接続や拡張現実／仮想現実などの帯域幅を多く必要とするケースにおいても、強固なネットワーク基盤が求められます。

しかし、ビジネス特有の要件に最も適したネットワーク基盤技術はどれなのでしょうか？
プライベート5G？ パブリック5G？ Wi-Fi 5かWi-Fi 6？

また、それぞれのセキュリティについてはどうでしょうか？

5GとWi-Fiの比較

ビジネスに不可欠なネットワークに5G技術を使用することは、特に大規模産業の企業にとって、非セルラー技術（Wi-Fi 6など）よりも多くの利点があります。しかし、どちらの技術もインダストリー4.0の動向に触発された新たなユースケースや要件をサポートするために、大きな進歩を遂げています。

5Gは、スループットの向上、サービスの展開、レイテンシーの低減において、データの処理量、全体的な信頼性とともに、劇的な進歩を遂げています。この技術は、4Gのセルラー技術を進化・改良したもので、3GPP（第3世代パートナーシッププロジェクト）標準化団体がプロバイダー向けにセキュリティのベストプラクティスに関するガイダンスを提供しています。これは、5Gネットワークが安全に設計されていることを意味しており、ユーザが使用する機器の認証と認可、エンドツーエンドの暗号化、プライバシー強化機能、ゼロトラストアーキテクチャなどの機能が組み込まれています。5Gに本質的に備わったこれらの要素がネットワーク全体の通信を保護することで、セキュリティを向上させます。

さらに、5Gは認可された周波数帯を使用しているため、他の無線機器からの干渉問題を軽減し、ネットワークスライシングを可能にすることで、サービス品質を向上させます。また、5Gは、クラウドで使用されている多くの技術ソリューションを使用し、その中核に仮想化を採用しているため、サービスの展開に柔軟性があります。これは、5Gがモバイルエッジコンピューティングをサポートできることを意味し、特にレイテンシーの問題をコスト効率の高い方法で解決することができます。また、5Gは、ユビキタスアクセス、ロードマップの柔軟性、WANおよびLAN技術のサポートを提供します。

一方、Wi-Fi 6は認可不要の周波数スペクトルの帯域しか使用していないため、「ノイズの多い」環境では干渉を制御することが困難です。Wi-Fiは主に家庭やオフィスのLANで使用されているため、デバイスエコシステムがこれらの環境により焦点を当てたものになっています。一方、セルラー技術である5Gは、モバイル、固定、場所の移動、屋内、屋外での使用にも適しています。

Wi-Fiは、これらの欠点にもかかわらず、消費者やオフィスのLAN環境において重要な役割を果たし続けると思われます。特に、Wi-Fi 6がWi-Fi 5よりも改善されたことで、ピークデータレート、レイテンシー、密度、エネルギー効率などの性能が向上しています。

ユーザが使用する機器の認証と認可、エンドツーエンドの暗号化、プライバシー強化機能、ゼロトラストアーキテクチャなど、5Gに本質的に備わったこれらの要素がネットワーク全体の通信を保護することで、セキュリティを向上させます。

5Gにおける選択肢：パブリックとプライベート

セルラー技術の特徴は、パブリックかプライベートかを選べる点です。パブリックネットワークとは異なり、プライベートネットワークでは、一般消費者向けのモバイルサービスよりも要件の厳しい、ローカルエリアのカバレッジに特化した非常に特殊なユースケースに対応する状況が多くなっています。例としては、生産ライン管理やAGVなどが挙げられます。

プライベート5Gは同じ技術を使用していますが、顧客専用のネットワークを提供し、企業が必要とする帯域に特化しています。これにより、データとネットワークの管理が強化され、外部へのデータの共有をブロックしています。その結果、センサーやカメラなどのIoTデバイスの使用が顧客の構内に制限され、ローミングする必要がないユースケースでは、プライベート5Gが有力な選択肢となります。

また、プライベート5Gは、セキュリティを重視する企業にとってもメリットがあります。サイバー脅威の種類は変わりませんが、ネットワークが組織によって物理的に管理され、セキュリティが確保されたエリアでのみ使用されるという事実は、保護レベルがさらに高くなることを意味します。たとえば、信号の妨害が可能な距離まで近づくには、物理的にその場にいる必要がありますが、これは物理的なセキュリティを突破し、しかも検知されないようにしなければならないことを意味します。物理的なセキュリティ対策と論理的なセキュリティ対策を組み合わせた多層防御を覚えておきましょう。

5Gネットワークの種類 - 主な特徴

パブリック

- モバイルネットワーク事業者の専門知識、ソリューションおよび数多くのスペクトルを使用
- 公共ネットワークからの完全な提供と公共ネットワークとの相互運用性
- 重要なデバイスやアプリケーションに優先順位をつけるためのサービス品質の向上
- 低レイテンシーとローカルに置かれたデータストレージと処理を提供するオンサイトゲートウェイのオプションを備えた、パブリックネットワーク内のエッジコンピューティングが可能

プライベート

- 高度に強化されたセキュリティとプライバシーを可能にする専用ネットワーク
- パブリックモバイルネットワークに接続しない独立したネットワーク
- 設計、導入スケジュール、運用を完全に管理
- SLAを完全制御
- 低レイテンシーで局所的なデータストレージと処理を提供するエッジコンピューティング
- ネットワークの設計や管理の一部またはすべてをアウトソーシング
- スペクトルへのアクセスと使用に対する直接的な責任

出典（部分的に改変）：https://www.gsma.com/iot/wp-content/uploads/2020/10/2020-10-GSMA-5G-IoT-Private-and-Dedicated-Networks-for-Industry-4.0.pd

5Gと産業環境におけるセキュリティの主な検討事項

産業用制御システム（ICS）や運用技術（OT）に大きく依存している複雑で重要な環境では、プライベート5Gの利用が最適と思われます。たとえば、込み入った工場のフロアや広大な港湾施設のような環境で実行される接続では、物理的な構造物や他の無線信号による信号干渉の可能性が非常に高くなります。プライベート5Gは、安定した信頼性の高い速度と低レイテンシーを実現し、接続中断のリスクを最小限に抑えることができるため、このような環境で特に効果を発揮します。

セキュリティ担当者ならご存知の通り、可用性は、システムやデータの完全性、機密情報の保護と並んで、サイバーセキュリティの要の1つです。

5Gで大規模なIoTを展開するには、デバイスのセキュリティを確保し、脆弱性を管理し、分析プラットフォームへのデータの安全な転送を確保するための拡張性を備えたセキュリティプログラムが必要です。IoTデバイスへの攻撃を監視し、これらのデバイスへの攻撃を迅速に検知して対応できるセキュリティ能力を持つことが重要です。最近話題になったいくつかの攻撃では、侵害されたIoTデバイスが大規模なDDoS攻撃に悪用されました。マルウェアやランサムウェア攻撃など、5Gを搭載したアプリケーションへのサイバー攻撃は、製造プロセスに大きな混乱をもたらし、顧客サービスや収益の確保を妨げるだけでなく、契約上の責任、規制への不適合、風評被害などを引き起こす可能性があります。また、データ転送時のセキュリティが不十分だと、機密情報や顧客の個人情報が盗まれる可能性があります。

また、5Gに対応したユースケースの設計と実行にセキュリティが組み込まれていなければ、人命や身体が危険にさらされます。よく言われる例は、5G対応の自律走行車にまつわる最悪のシナリオです。サイバー攻撃から適切に保護されていない自動運転車の後部座席に乗りたいと思う者はいません。

また、発電所や水処理施設などの産業組織への攻撃は大惨事につながる可能性があります。実際、この種の攻撃はすでに発生しており、これが非常に現実的なリスクであることを示しています。2014年には、ドイツの製鉄所がサイバー攻撃の結果、大きな被害を受けました[1]。また、2021年初頭には、フロリダ州で、ハッカーが水道施設の産業制御システムに侵入して公共の水道を汚染しようとしました[2]。

NIST CSFがプライベート5Gネットワークのセキュリティに役立つ理由

NIST CSFがサイバーセキュリティプログラムの設計に対し指針として提唱するフレームワークを、プライベート5Gネットワークとそれを実現するアプリケーションに適用することで、リスクを大幅に低減できることが実証されています。NIST CSFは、以下の5つの柱となる重要な機能を組織が開発する必要性を強調しています。

特定
自社の資産と組織に対する社内外の脅威を知る。

防御
クラウドやモバイル、IoTなど、あらゆる場所の重要なインフラ、資産、データを安全に保護する。

検知
システムやデータの侵害を検知する能力を強化・促進する。

対応
セキュリティインシデントを迅速かつ効果的に管理するための計画を策定・維持する。

復旧
システムの連続稼働時間を最大限伸ばし、コストのかかる業務中断を最小限に抑えるための回復力を付けるための計画を立てる。

[1] https://www.bbc.com/news/technology-30575104 [2] https://www.bbc.com/news/world-us-canada-55989843

業界全体のフレームワークを構成する3要素：

フレームワークコア | 実装の成熟度段階 | プロファイル

コアの3つの項目：

機能 | カテゴリー | サブカテゴリー

構成の上位項目となる5つの機能：

特定 | 防御 | 検知 | 対応 | 復旧

この5つの機能の下に23のカテゴリーが階層化されています（以下を参照）。

機能	カテゴリー
特定	資産管理 ビジネス環境 ガバナンス リスクアセスメント リスクマネージメント戦略 サプライチェーンリスク管理
防御	ID管理およびアクセス制御 意識向上およびトレーニング データセキュリティ 情報保護、プロセス、および手順 保守 保護技術
検知	異常とイベント セキュリティの継続的な監視 検知プロセス
対応	対応計画 コミュニケーション 軽減 改善
復旧	復旧計画 改善 コミュニケーション

NIST CSFの詳細

特定

セキュリティプログラムを開発する際の重要な出発点は、組織のネットワーク上にどのような資産のデバイスがあり、各資産にどのようなデータが存在するのかを特定することです。基本的に、認識できないものを保護することはできません。この作業の一環として、企業は「王冠の玉石」、すなわち侵害されたり利用不能になったりすると、組織の運営能力に根本的な影響を与える重要な資産を特定する必要があります。

最終的には、企業は自社の運用環境の全体像を把握する必要があります。プライベート5Gネットワークを既存のネットワークに追加することの影響を考える際には、何が追加されるのかを正確に理解することが重要です。追加されるのは、プライベート5Gネットワークや導入されるハードウェアやソフトウェアの要素だけではなく、ユースケースをサポートし、この技術を活用するさまざまなコンポーネントも含まれます。

さらに、収集されたデータがどこで処理され、後でアクセスできるように保存されるのかを理解することも重要です。 また、さまざまなユースケースについて、ビジネスの成功に果たす役割や、それを実現するために必要な技術とデータの組み合わせの観点から、優先順位をつける必要があります。

この段階でのもう1つの重要な要素は、企業が自身のリスクプロファイルを特定し、理解することです。今日の企業には、業務のやり方が異なるさまざまな部門や、事業分野が異なる子会社がある場合があります。そのため、セキュリティプログラムの設定が複雑になり、さまざまなネットワークのリスクプロファイルを判断するためには、データを収集して文脈ごとに分類する必要があります。

プライベート5Gに関して、特に産業分野でのリスクに関する検討事項については、すでに述べたとおりです。独自の技術で構築され、ITやOT（運用技術）を専門とするプロバイダーが提供する産業用のオペレーションについても、組織のリスクプロファイルに織り込み、復旧のしやすさにどのような影響があるかを考慮する必要があります。

これに関連して、産業環境で活動する多くの企業は、これまで隔離されたプライベートネットワーク内で独自の技術を使用し、一定のセキュリティ層を形成してきました。プライベート5Gがサポートするユースケースのタイプには、パブリッククラウド環境へのアクセスをたびたび必要とします。

このようなネットワークアーキテクチャの変更は組織のリスクプロファイルに影響を及ぼすため、これもリスクプロファイルに織り込む必要があります。その上で、どのようなセキュリティ技術、人材、プロセスが導入されているか、不足しているものがないかを特定し、定期的に評価する必要があります。一般的に、これは年1回独立したアセスメントを行うことによって達成されます。これらすべての基礎となるのは、組織が達成しようとしているセキュリティの成果であり、これにはリスクの軽減、コンプライアンス、プライバシーのレベルが含まれます。

防御

セキュリティプログラムの基盤となるのは、防御を形成する技術です。これらの防御技術の構築も防衛境界を固定する従来のアプローチから変わる必要があります。というのは、企業のIT環境が仮想化されたコンポーネント、ネットワーク要素（オンプレミスとクラウド）、サービスとしてのソフトウェア（SaaS）、増加するリモートワーカーを含むハイブリッドネットワーク環境へと移行しているためです。

このような新しいモデルを反映した防御のしくみが必要となります。プライベート5Gネットワークのセキュリティのコアとなる高レベルの防御には、暗号化が使用され、ゼロトラスト原則が取り入れられています。したがって、プライベート5Gネットワークがサポートするユースケースのさまざまな要素を保護することに重点を置く必要があります。

これには、さまざまな種類の技術が考えられます。たとえば、ネットワークスライシングは、ユースケースやデータの種類によってネットワークのキャパシティを分割し、ネットワーク上を移動する他のデータから分離することで、さらに高いレベルの防御を実現します。

エンドポイントレベルでの防御も重要な検討事項です。ラップトップやモバイル機器などのエンドポイントデバイスは、セキュリティのためのセンサーを組み込むことできますが、IoTデバイスには、そのサイズや容量を反映した専用のエンドポイント技術が必要になります。

エンドポイントだけでなく、プライベート5Gのユースケースに必要なアプリケーションやデータ処理も防御が必要なのです。しかし、それをどのように、どのレベルまで行うかは、使用する技術の種類や組み込まれている防御機能の能力、パブリッククラウドを使用するかどうか、そしてそれがもたらす関連リスクなどよって異なります。攻撃の巧妙さと様々なタイプの攻撃者が絶え間なく増加し、企業の重要な資産を保護する必要性が依然として存在するため、ゼロトラストは、NIST CSFの「防御」の柱にふさわしいアプローチを開発するための基盤であり続けています。

最後に、企業のセキュリティプログラムの最前線である従業員への依存度が高まる中、脅威、技術、プロセスの変化を従業員のトレーニングや意識向上活動に確実に反映させることが重要です。

検知

サイバーセキュリティに関する一般的な考え方は、「侵害されるかどうかではなく、いつ侵害されるか」というものです。侵害された場合には、その検知の速さが重要です。ベライゾンの『2021年度データ漏洩/侵害調査報告書』で報告されているように、データ漏洩/侵害の約20%が数ヶ月以上発見されないままになっています。

すでに述べたビジネスに対するリスクの種類、特に人命への脅威を考えると、検知の速さは非常に重要です。したがって、検知はあらゆるセキュリティプログラムの重要な部分です。そのため、プライベート5Gや関連するユースケースの導入を始める企業は、ネットワーク、アプリケーション、データストレージに変更を加えることも含め、現状の検知技術にどのようなアップデートが求められるかを検討する必要があります。

特に高度な産業環境を持つ企業にとって課題になりそうなのは、独自のフォーマットを持つことが多いログデータを現状の検知技術で取り込むことができるかどうかです。このような場合、企業は既存の検知技術がこれらのデータタイプを取り込み、有効に処理できることを確認する必要があります。また、ネットワークトラフィックを調べることができるネットワーク分析技術を活用し、それを使ってデータ漏洩/侵害の証拠を含む不審な活動を探すことも検討する必要があるかと思います。

対応

この機能の柱にとって重要な部分は計画を立てることであり、セキュリティオペレーションを成功させるために非常に重要です。これは、定期的にテスト運用を実施し、さまざまな脅威への対応を検討することを意味します。また、セキュリティ体制を第三者に評価してもらうことも強く推奨します。

企業は産業に特化した方法で計画を立てる必要があります。対応の方法も業界によって異なります。そのため、技術パートナーも産業環境を理解した上で、この計画を支援する必要があります。

企業がプライベート5G技術とそれに関連するユースケースを使い始め、保護プログラムや検知プログラムを調整する際には、対応計画も調整し、それが強化されているかどうか、堅牢性を維持しているかどうかをテストする必要があります。

また、侵害が発生した場合のバックアップとして、追加のリソースを用意しておくことも重要です。ほとんどの組織は、侵害の発生に備えた専任の要員を確保するためにリソースを無駄にすることはできません。侵害が発生する可能性はあるとしても、すぐには起きないかもしれません。つまり、その従業員は暇を持て余していることになります。したがって、産業組織では、侵害が発生したときの対応を兼務するスタッフを配置するか、すぐに対応できる第三者のパートナーを持つか、あるいはその両方を組み合わせる必要があります。

復旧

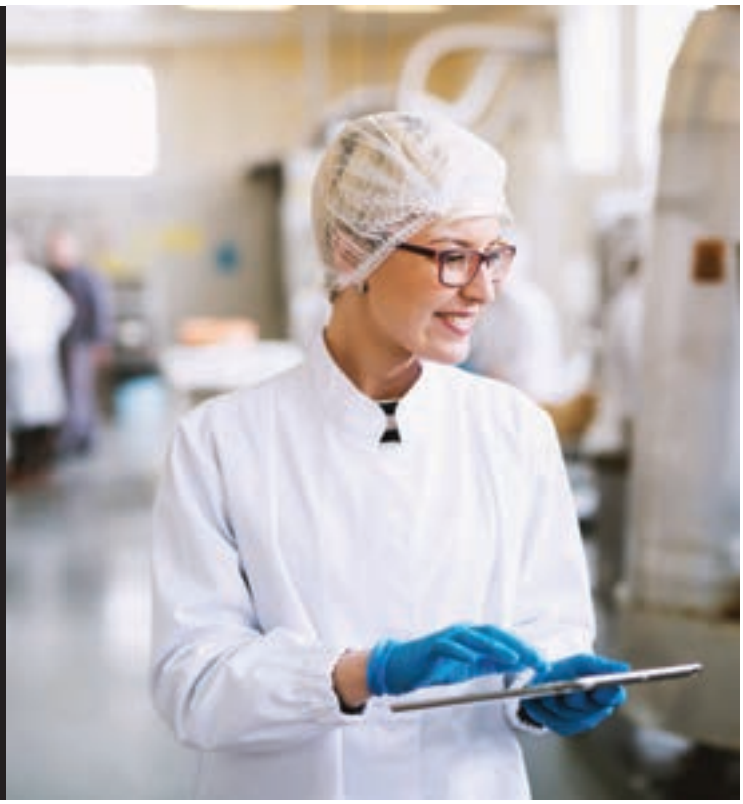
この機能の柱を検討する際には、ビジネスへの影響を最小限に抑えるために、ビジネスの特定のニーズや影響を受けるエンドポイントについての再検討をする必要があります。

プライベート5Gネットワークでは、企業は新しい技術ベンダーを導入することになるため、復旧プロセスの一環としてベンダーからどのような支援が必要になるかを理解し、それを復旧計画に組み込む必要があります。

まとめ

5Gによるビジネスの未来が到来しています。プライベート5Gは、産業を変革するための次世代のネットワーク基盤となります。第4次産業革命の恩恵を受け、そのリスクを管理するためには、賢明なビジネスリーダーとITやセキュリティの担当者が、これまで以上に協力し合う必要があります。

NIST CSFとともに5Gに本質的に備わっているセキュリティ管理機能を活用することで、組織は無限のイノベーションへの道筋を確実に描くことができます。



ベライゾンの5Gサービスが産業をどのように変革できるかについての詳細は、verizon.com/business/ja-jp/solutions/5g/をご覧ください。