ADD VNTR.

5Gへと向かうお客様に安心を提供し、確かな成功へ

MACNICA

10年以上にわたり培ってきた テレコムセキュリティの知見を５Gに生かす

背景と課題

真の 5G と呼ばれる 5G SA（スタンドアロン）サービスが本格的に稼働を開始するに伴い、スマートファクトリーや遠隔医療など社会課題を解決に導くユースケースが普及すると想定されます。ただし、そうした中で必ず担保しておかなければならないのがセキュリティです。2022 年 1 月現在では、16 ヵ国 20 オペレータが 5G SA 商用ネットワークを開始しており※、稼働実績が徐々に蓄積され始めている状況です。今後はさまざまなセキュリティリスクが顕在化し、攻撃事例が増加するものと予想されています。

※出典：GSA

マクニカの特徴

マクニカは、国内外の通信キャリア業界に特化したセキュリティ対策を数多く支援しています。一般的なセキュリティベンダーが扱う「リスク診断」「侵入試験」「セキュリティ対策ソリューション」の提案だけでなく、セキュリティ機器導入から運用支援、セキュリティサービス、通信キャリアにおけるセキュリティ 運用組織（SOC/CSIRT）立上げや、モバイルネットワークに適合するファイアウォール /IDS の導入検討など、業界固有のリスクや実運用を考慮した伴走型支援を提供します。

マクニカを選ぶメリット

マクニカはお客様と寄り添い、5G にまつわるリスクをいかに恒常的にコントロールするかというゴールを共に描き、お客様と共に伴走します。自環境におけるセキュリティ要件に対し、規格 / 業界ベストプラクティスとのギャップを評価 / 分析するセキュリティ総点検や、外部に露出している脆弱性から内部への侵入を許すリスク別に設けたペネトレーションテストを経て、セキュリティ定期監査の自動化まで実現することが主なシナリオです。

なぜ5Gセキュリティが必要なのか？

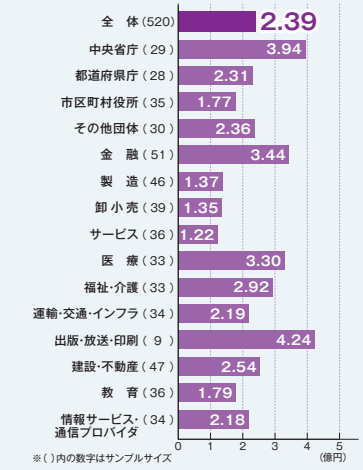
高速大容量、高信頼・低遅延、多数同時接続といった特徴を持つ5G。
真の5Gと呼ばれる5G SA（スタンドアロン）の展開も近づいており、
ますます期待が高まっています。
5G SAの世界では、多種多彩なITサービスが、動的なスライス上の
仮想アプライアンスによって提供されることになります。
これに伴い5Gとオープンなネットワークやシステムとの“つながり”が
さらに拡大します。

IoT の特徴とセキュリティ上の課題

性 質	セキュリティ上の課題	5Gセキュリティとの関連項目
脅威の影響範囲が大きい	HEMSやコネクテッドカー等のIoT機器はインターネット等のネットワークに接続していることから、ひとたび攻撃を受けると、ネットワークを介して関連するIoTシステム・IoTサービス全体へその影響が波及する可能性が高く、IoT機器が急増していることによりその影響範囲はさらに拡大してきている。	○
脅威の影響度合いが大きい	自動車分野、医療分野等において、IoT機器の制御（アクチュエーション）にまで攻撃の影響が及んだ場合、生命が危険にさらされる場面さえも想定される。さらに、IoT機器やシステムには重要な情報（例えば個人の生活データ、工場のデバイスから得た生産情報等）が保存されている場合もあり、こうしたデータの漏えいも想定される。	○
IoT機器のライフサイクルが長い	自動車の平均使用年数は12～13年程度と言われていたり、工場の制御機器等の物理的安定使用期間は10年～20年程度のものが多く存在するなど、IoT機器として想定されるモノには10年以上の長期にわたって使用されるものも多く、構築・接続時に適用したセキュリティ対策が時間の経過とともに危殆化することによって、セキュリティ対策が不十分になった機器がネットワークに接続されつづけることが想定される。	-
IoT機器に対する監視が行き届きにくい	IoT機器の多くは、パソコンやスマートフォン等のような画面がないことなどから、人目による監視が行き届きにくいことが想定される。こうした場合、利用者にはIoT機器に問題が発生していることがわかりづらく、管理されていないモノが勝手にネットワークにつながり、マルウェアに感染することなども想定される。	-
IoT機器側とネットワーク側の環境や特性の相互理解が不十分	IoT機器側とネットワーク側それぞれが有する業態の環境や特性が、相互間で十分に理解されておらず、IoT機器がネットワークに接続することによって、所要の安全や性能を満たすことができなくなる可能性がある。特に、接続するネットワーク環境は、IoT機器側のセキュリティ要件を変化させる可能性があることに注意をすべきである。	○
IoT機器の機能・性能が限られている	センサー等のリソースが限られたIoT機器では、暗号等のセキュリティ対策を適用できない場合がある。	-
開発者が想定していなかった接続が行われる可能性がある	IoTではあらゆるものが通信機能を持ち、これまで外部につながっていなかったモノがネットワークに接続され、IoT機器メーカやシステム、サービスの開発者が当初想定していなかった影響が発生する可能性がある。	-

総務省「令和２年　情報通信白書」より

セキュリティインシデントによる年間平均被害総額



※（）内の数字はサンプルサイズ

総務省「令和２年　情報通信白書」より

拡大するサイバー脅威の侵入ポイント

従来のモバイル通信は完全にクローズドな世界（閉域網）で運用されていたため、サイバー攻撃の侵入はきわめて困難でしたが、つながりが拡大するに伴いIoT機器やインターネットなど侵入のための入口も拡大していきます。また、動的なスライス上の仮想アプライアンスによって展開されるサービスにはオープンソースや汎用プロトコルが利用されており、そこにもさまざまな脆弱性が潜在しています。

サイバー脅威がもたらす被害の深刻化

DXでは必然的に、工場や機器を外部のクラウドなどと接続することになります。それと比例して高まるのがセキュリティリスクです。現に、ある製造業では外部からのサイバー攻撃を受け、生産を一時停止せざるを得ない事態に陥ったインシデントもメディアで報道されています。DXはセキュリティ対策と両輪で進めることが重要です。特に製造業の場合、提供する製品の脆弱性がお客様に被害を及ぼし、自社が加害者になってしまう恐れもあるため、セキュリティの取り組みは不可欠です。

5G活用へのアプローチ

マクニカでは、テレコムの根幹部分におけるセキュリティ対策で実績を重ねてきました。そうした中で培ってきたインテリジェンスに基づくリスクアセスメントにより、お客様が直面する可能性が高い5Gセキュリティの全体課題を整理し、あるべき対策を策定しつつ、共に未来のVisionを描いていきます。

歴史的な脆弱性とその対策を理解

5Gだけを捉えて的確なセキュリティ対策ができるわけではありません。5Gは3G時代からの連綿と積み重ねてきた技術によって実現されているため、その歴史を紐解いて脆弱性およびその対策を理解する必要があります。たとえば現在サービス提供されているNSA（ノンスタンドアロン）方式の5Gは、コアネットワークに4Gの設備や技術を流用しているため、4Gのセキュリティに関する知識も必須となります。

新しいユースケースに対応したセキュリティを検討

5G SAによってユースケースが拡大するに伴って、セキュリティの観点もどんどん変化していきます。ユーザーの権限や監視体制も見直していかなければなりません。将来を見据えつつ、政府や公的機関から公開されるガイドラインに対応するのは当然のこと、通信キャリアや企業自身が主体的に策定していかなければならない部分も増えていきます。

マクニカの 5G セキュリティ支援アプローチ

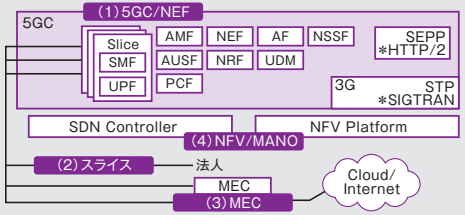
アセスメント

標準仕様／ガイドラインに基づく、
対策状況の可視化と脆弱性評価

総務省　3GPP　GSMA

アタックサーフェス毎の課題抽出と優先順位付け

●NEF ●スライス ●NFV/MANO ●MEC



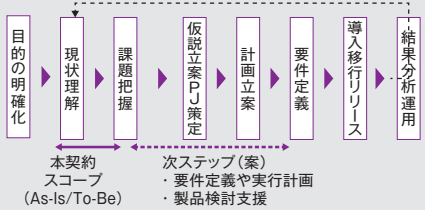
プロジェクト建付け

貴社の目指すポリシーの策定
ビジネス拡大とセキュリティのバランス

パートナー/
顧客の拡大による
ビジネスの最大化

NW機能の公開範囲の
拡大による
新たな脆弱性の可能性

5Gセキュリティ対策の内容・方向性
合意に向けたPJ計画書・体制整備



新たなセキュリティ運用の実現

新たなガイドラインの策定

外部事業者接続ガイドラインの策定

- 法人向けNW機能公開
- MVNO接続
- Private 5G

新たな対策の実装

- 認証基盤に基づくアクセス制御
- NW内の振舞いの異常検知
- オープンソフト時代に対応した脆弱性管理

全商用NWのセキュリティ監視運用体制の一元化

通信キャリアからマクニカが選ばれる理由

1 3G 時代から培った知見

マクニカは3G時代から10年以上にわたって通信キャリア業界に特化した
支援を数多く行ってきた実績があります。

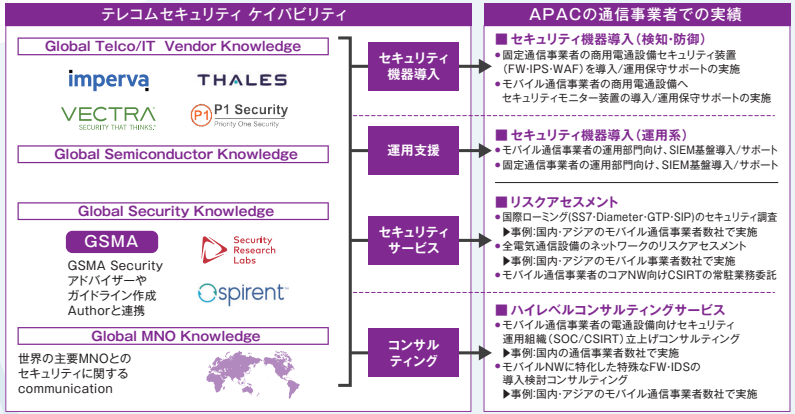
2 経験豊富なエキスパートによるコンサルティング

通信キャリアにおいてセキュリティを先導してきたエキスパートが、5Gセキュリティにまつわる専門知識を交えて、課題の棚卸から実運用までをサポートします。

3 5Gを利用する企業を支援

製造業などではローカル5Gを活用した工場のIoT化、スマート化などのニーズも高まっています。そうした中で考慮すべきセキュリティもトータルにサポートしていきます。

テレコムセキュリティサービスを 2014 年から提供



Beyond 5G（6G）時代へのさらなる前進

Society 5.0 に向けたガイドライン支援

Beyond 5G（いわゆる6G）は、サイバー空間を現実世界と一体化させ、Society5.0 のバックボーンとして中核的な機能を担うインフラとなることが期待されています。そこに向けたセキュリティのあるべき姿をマクニカは提言していきます。

5G時代に発揮されるマクニカの強み

1 テレコムセキュリティのパイオニア

マクニカが技術商社として、通信機器メーカーに向けてテレコム設備に関するさまざまな商材の提供を開始したのは、2Gから3Gの黎明期に至る 1999年のことです。このビジネスはその後、国際基準（SS7）に基づく国際ローミングのセキュリティ対策という形で発展。日本の国内仕様に合わせたこの技術のカスタマイズやテクニカルサポートを通じて、通信キャリアとのパートナーシップを築いてきました。そうした中でマクニカが業界で初めて打ち出したのがテレコムセキュリティの概念です。

2 国内・海外 5G セキュリティガイドラインの深い知見

マクニカは国内はもとより、米国、中国、韓国、欧州など5G SA先進国において国家プロジェクトに参画している各地域の通信キャリアへのサポートを通じて、国内外の5Gセキュリティガイドラインに関する深い知見を蓄積。5G SAの展開に向けたセキュリティリスクの洗い出しおよび実装すべき対策を導き出します。

3 3G、4G、5Gネットワークの診断経験

5Gは3G時代から連綿と積み重ねてきた技術によって実現されたものです。そのため、3G、4G、5Gの全ての技術を熟知していなければセキュリティリスクのアセスメントを行うことはできません。マクニカは3Gおよび4Gの時代から通信キャリアのコアネットワークから基地局側のアクセス回線まで、数多くのネットワークを診断してきました。この経験とノウハウが5Gネットワークの診断にも活かされています。

4 世界からも認められる最先端セキュリティ技術の知見

世界で最も技術的かつ影響力のある情報セキュリティカンファレンスとして知られるBlack Hatには、世界トップクラスのセキュリティの専門家や技術者が一堂に会し、ブリーフィング（講演）やトレーニング、アーセナル（討議、質疑応答）を行っています。マクニカはこのBlack Hatの登壇者をはじめ、セキュリティ分野におけるキーマンと共にさまざまなプロジェクトを推進しています。

5 テレコムだけではない最先端 IT セキュリティへの知見

5Gによって、あらゆる人やモノがつながる世界が実現します。そうした中で拡大していくのがテレコムとITのシームレスな融合であり、双方の分野にまたがるITセキュリティの知見が求められます。マクニカはインターネットの黎明期からIT領域におけるネットワークセキュリティ対策のソリューションを提供し、ノウハウを培ってきました。また、テレコム系とIT系の双方において、豊富な実績をもつ海外パートナーと連携しています。

6 最先端セキュリティ技術の導入支援実績経験

マクニカではネットワークスライシングを導入した5G SA向け仮想基盤におけるセキュリティを確立すべく、独自の検証環境を構築。スライスを考慮したアクセス制御、スライス間でのリソース共有のケア、スライスを利用するテナント間での境界セキュリティ、スライスのライフサイクルに対応したセキュリティなどをテーマに、課題検証支援を行いました。また、この検証結果を業界全体に向けた提言にまとめていく予定です。

アイデアの整理から
お客様と向き合うDXコンサルティング

ADD VNTR.

ビジネスにおける課題の棚卸しからコンサルタントが伴走

マクニカのDXコンサルティングは、①マネジメント・経営、②製造DX、③サイバーフィジカルセキュリティ、④AI、⑤モビリティ、⑥モノづくりの6つの側面からお客様のデジタル変革を支援します。そしてこの取り組みの中核に位置するのが、あらゆる人とモノをつなぎ、新たなサービスの価値を創出していく5Gネットワークです。ただしこの技術は無限の可能性を持つと同時に、セキュリティに関する未知の脅威が潜在しているのも事実です。マクニカのコンサルタントは常にお客様と共に、笑顔あふれる豊かな未来に向けて、終わりなき成功へと寄り添い、伴走します。

コンサルタント紹介

株式会社マクニカ
DXコンサルティング室
マネージャー
黒澤　俊洋

株式会社マクニカ
DXコンサルティング室
マネージャー
日野　克也

株式会社マクニカ
DXコンサルティング室
シニアコンサルタント
塚田　晴史

まずはお気軽にご相談ください

フォームでのお問い合わせ

メールからお問い合わせはこちら
add-venture@macnica.co.jp