ローカル５Ｇセキュリティガイドライン

初版　2022年 3月

一般社団法人　ＩＣＴ－ＩＳＡＣ
５Ｇセキュリティ推進グループ

ローカル５Ｇセキュリティガイドラインの配布に当たって

ICT-ISAC理事長　齊藤忠夫

通信システムは伝統的には有線回線を通して情報を転送する方式として広がっておりました。しかし、近年では携帯通信が一般化し、端末機数でも有線通信の端末数を上回り、2020年以降の通信システムでは、無線方式を主としたシステムがさらに広がります。2020年から2030年までの5G方式では人口の数倍に達する端末を使う時代になるとされています。

21世紀に入って、端末数が増加する中、様々なマルウェアがはびこり、ユーザの円滑な情報処理を妨げる状況が発生しています。5Gの時代にはさらに多数の端末が展開されます。工場等では端末を接続するネットワークにも無線周波数が割り当てられ、ローカル無線網が幅広く展開し、そのための電波周波数も割り当てられます。5Gシステムを活用するにはこうしたローカル５Gネットワークのセキュリティを確保しなければなりません。ローカル無線網はそれが設置される場所で展開され、無線網のセキュリティもそれを活用する組織毎に確保しなければなりません。ローカル無線網の管理者がそれぞれのローカル5Gのセキュリティ確保の手法を適切に実現していただくことが重要になります。ここにおまとめしたガイドラインが皆様のお役に立つと期待しております。

前書き

本ガイドラインは、ローカル5Gを利用する組織、およびソリューションを提供する組織を対象として、ローカル5G利用時に検討すべきセキュリティについてまとめたものである。

5Gサービスの開始に続き、ローカル5Gのサービスも2020年から開始された。公衆ネットワークでは対応し切れない様々な潜在的ニーズに対応することが期待されており、自治体や民間企業などにおいてその利用が検討されている。これまで無線によるネットワーク構築には主にWi-Fiが用いられてきたが、通信範囲の狭さやセキュリティの確保にコストがかかることがデメリットであった。ローカル5Gはこのようなデメリットを解消したサービスであるだけでなく、5Gそのものの特徴（広帯域、低遅延など）も有していることから、今後の普及が見込まれている。

しかしながら、ローカル5Gは新しいサービスであるが故に、これまで検討することがなかった新たな観点でのセキュリティ対策が求められる。これら必要なセキュリティ対策は何であるかを明らかにするとともに、予め対処に向けて整理することは、ローカル5Gの普及及び安全な利活用において必須と考えられる。

ICT-ISACは、ISPを含む通信事業者、放送事業者、ソフトウェアベンダ、情報提供サービス事業者、情報関連機器製造事業者を含む幅広い分野の方々と協力し、これからのネットワークのセキュリティ確保を目指して活動している。新たな社会基盤としてスタートしたローカル5Gに対して、必要なセキュリティ対策の検討が必要と判断し、ICT-ISACは「5Gセキュリティ推進グループ」を2020年2月に発足させ会員企業とともに議論を重ねてきた。本ガイドラインは、5Gセキュリティ推進グループでの議論結果をまとめたものである。本ガイドラインが、ローカル5Gの導入・利活用・保守に関わる様々な方に参照いただき、少しでもローカル5Gの普及に貢献することが出来れば望外の喜びである。

改編履歴

版	更新日	内容
1.0	2022年3月31日	初版

目次

１．はじめに

1.1 ガイドラインの目的

5Gサービスがスタートして数年が経過した。移動通信は世代に伴って通信速度が格段に向上しており、5Gは従来の通信サービスと比較して、より一層通信速度が向上したサービスとなっている。加えて5Gは、「低遅延」「同時接続」の観点においてもこれまでのサービスと比較して大幅に向上しており、ヒトだけではなくあらゆるモノも繋ぐことが期待されている。よって5Gは、まったく新しいコミュニケーションツールと捉えることが出来、これまで想像もしなかった新しいサービスや世界を構築することが可能と考えられる。

ローカル5Gは、通信事業者によって提供される5Gサービス技術を活用し、自治体・民間企業などが独自にネットワークを構築できる仕組みである。ローカル5Gにおいては、広いエリアでのネットワーク構築を求められることはなく、たとえば敷地内などある特定のエリア内や、ビルなどの建物内といった、限定された範囲でのネットワークの構築が可能となっている。現状では、こういったニーズにはWi-Fiを用いたネットワーク構築が主であるが、5Gの利点である高速大容量、低遅延、SIMカード利用による必要時にのみ接続するといったセキュリティ機能を生かすことで、より安全で高度なネットワークを得ることができる。ローカル5Gの定義、および免許取得については[1][2][3]を参照されたい。

ところで、これまでのSI事案と同様、ローカル5Gを使ったサービス事案においてもセキュリティの確保は重要である。構築運用されるネットワークの規模が大きくなるに従い、複数の事業者による共同作業となるであろうし、また保守運用時における監視やインシデント対応といった手順を決めておかねばならない。このようにセキュリティに関する検討は必要であるが、ローカル5Gを利用した案件では、従来のネットワークセキュリティに加え、5Gの特性（高速大容量、低遅延）を逆手に取ったサイバー攻撃への対応も必要となってくる。

このような背景のもと、ICT-ISACでは2020年2月に「5Gセキュリティ推進グループ」を新たに立ち上げ、ローカル5Gを円滑に普及させるために必要なセキュリティについて検討を進めてきた。本ガイドラインは当グループに参加している有志により作成されたもので、ローカル5Gの導入・利活用・保守に関わる様々な方に参照いただくことで、ローカル5Gの普及に貢献することを目的としている。今後普及が期待されるローカル5G利用において、サービスを享受する「利用者」、およびサービスを提供する「事業者」のそれぞれの立場から、導入時や運用時で検討すべきセキュリティを提示している。

なお当グループでは、「利用者」および「事業者」が現時点でローカル5G利用にどのようなセキュリティ課題を有しているかを把握するため、2020年12月から2021年1月までの期間、アンケートを実施した[4]。アンケート結果は3.2節にも紹介しているが、より詳細な情報はICT-ISACのホームページに掲載されているので、興味のある方はご覧いただきたい。なお本ガイドラインは、このアンケート結果を参考にして作成したことを付記しておく。

1.2 本ガイドラインの読者層

本ガイドラインの想定する読者層は大きく分けて次の2者である：①ローカル5Gサービスを享受する「利用者」、および②ローカル5Gサービスを提供する「事業者」である。本ガイドラインでは、「利用者」「事業者」のキーワードを多用することに留意されたい。

「利用者」の例としては、地方自治体、工場、病院などが想定されるが、これに限らずローカル5Gサービスを利用し、自ら又はその先のお客様に向けて魅力的なサービスを提供する主体を指す。

「事業者」は、ローカル5G免許を取得しローカル5Gサービスを提供する事業者のことを指す。この事業者は、従来の電気通信事業者とは異なり、お客様（＝利用者）に対しローカル5Gネットワークの構築を提供する。多くの場合、その後のネットワーク保守・運用も手掛けることになると想定される。サービス提供においては、複数のビジネスパートナーと共に展開する場合もあるが、本ガイドラインの「事業者」は、その中でローカル5Gネットワークについて主体的に提供する事業者を想定している。

1.3 近年の動向

ローカル5Gの免許は、2020年3月に初めて交付された。その後、免許を取得した事業者は着実に増加しており、同年10月時点での免許取得事業者数は12者[5]であったが、翌2021年10月の段階では66者[6]となっている。引き続き事業者数は増加することであろう。

これら事業者は実際のビジネス展開の前段階として実証実験を積極的に展開しており、たとえば農作業の自動化や工場内の無線化、また防災分野への適用といった事例が報告されている[7]。今後、実証実験の結果を用いて、実サービスへ移行する事案もあると思われる。

1.4 用語の定義

用語	定義
5Gセキュリティ	これまでのネットワークセキュリティ要件に加え、5Gの利活用場面で特に意識が必要なセキュリティ要件を指す。広義に解釈し、5Gネットワークの普及にともないIoTデバイスや産業機器がネットワークに接続することが期待されることから、これらエンドポイントのセキュリティ要件も含める場合がある。
5G	第５世代通信システムのこと。国際電気通信連合(ITU)によって定められた規定「IMT-2020」を満足する、無線通信システム。要求要素として、高速大容量、低遅延、多数同時接続を定義している。
ローカル5G	地域や産業の個別ニーズに応じて地域の企業や自治体等の様々な主体が、自らの建物内や敷地内でスポット的に柔軟に構築可能な5Gシステム。[5]
LTE Advanced	第４世代通信システムのこと。国際電気通信連合(ITU)によって定められた規定「IMT-Advanced」を満足する無線通信システム。
ミリ波	5Gで利用される26GHz帯以上の高周波数帯を指す。 日本国内のローカル5Gでは28.2G～29.1GHz帯が制度化されている。
Sub6	5Gで利用される6GHz帯未満の周波数帯を指す。 日本国内のローカル5Gでは4.6G～4.9GHz帯が制度化されている。
NR	5G無線方式
eMBB	高速大容量通信
URLLC	超高信頼低遅延通信

mMTC	多数端末接続通信
Core Network(CN)	交換機、加入者情報管理装置などで構成されるネットワーク。[8]
RAN	コアネットワークと端末との間に位置する、無線レイヤの制御を行う基地局などで構成されるネットワーク。[8]
CSIRT	Computer Security Incident Response Teamの略。「コンピュータセキュリティインシデント」に関する報告を受け取るとともに、他のセキュリティ関連組織と連携して原因の調査、および復旧に向けた対応活動を行う組織体の名称。
SIMカード	電話番号を特定するための固有のID番号が記録された、携帯やスマートフォン等が通信するために必要なICカード。
STRIDEの分類法	脅威を洗い出すための手法。Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の六つの性質から脅威を洗い出す。
脅威	システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。
脆弱性	一つ以上の脅威によって付け込まれる可能性のある資産または管理策の弱点。
NF	5Gの実現方式として採用されたサービスベースアーキテクチャにおける、ネットワークに必要な個別機能群（Network Function）のこと。
C-Plane	5Gコアネットワークにおける、通信の確立などをするためにやり取りされる一連の制御処理（プロトコル）。
U-Plane	5Gコアネットワークにおける、ユーザデータの送受信処理（プロトコル）。
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードを指す。
IMEI	端末識別番号のこと。電話番号や回線契約とは関係なく、端末が持つ固有の番号である。「国際移動体装置識別番号（International Mobile Equipment Identifier）」の略。
IMSI	GSM方式、3G方式、LTE方式などの携帯電話等で用いる最大15桁の識別番号（ITU-T E.212規格準拠）。端末内やSIMカードに書き込まれ、携帯電話網はIMSIにより利用者の識別及び認証を行う。International Mobile Subscription Identity の略。
SIMスワッピング	SIMハイジャック、あるいはSIMスワップ詐欺とも呼ばれる、一種のアカウント乗っ取り詐欺。携帯電話番号を悪用した個人情報の盗難手法であり、携帯電話の番号を奪うことで電話やSMSメッセージを乗っ取る。

Miraiマルウェア	Linuxで動作するコンピュータをターゲットとし、感染端末を遠隔操作できるボットにするマルウェア。ネットワークカメラや家庭用ルーター等のIoTデバイスを主要なターゲットとする。2016年に発見され、非常に大規模なDDoS攻撃を引き起こしたことで有名。Windows をターゲットにする亜種も存在する。
C&Cサーバ	サイバー攻撃者がマルウェアをコントロールする際に用いる指令サーバのこと。
Cell-ID	基地局に割り当てられている番号。
ISO 27001	情報セキュリティマネジメントシステム（ISMS）に関する国際規格。
ICT-ISAC	ICTに関わるセキュリティの対策・対応レベルの向上に資する活動を行うために、社員間の幅広い相互連携を図り、安定した情報流通、情報伝達を維持することで、安全なICT社会の形成に寄与することを目的とした一般社団法人。

２．5Gネットワークの概要

2.1 5Gの特徴

5Gは、LTE Advancedの次の世代となる移動通信システムで、モバイルブロードバンドサービスを強化するための更なる高速・大容量通信の実現に加え、多接続、低遅延を実現し、製造、医療、交通など、さまざまな分野での応用が期待されている。5Gでは最大通信速度が4Gの20倍の20Gbpsとなり、高精細な画像や動画の配信が可能になることで、コンテンツ配信だけでなく、遠隔医療や遠隔監視の高度化などにも貢献することが期待されている。5Gでは、ミリ波・sub6、および、4G LTE周波数のNR化を組み合わせてエリア構築が行われ、ミリ波では28GHz帯の周波数と400MHzの帯域幅、sub6では3.7/4.5GHz帯の周波数と100MHzの帯域幅を利用した高速・大容量通信が可能となっている。また、4G LTE周波数のNR化により既存の基地局設備を活用した迅速な5Gエリア化が可能となっている。遅延に関しては、5Gでは無線区間の遅延が4Gの10分の1の1msとなり、エッジコンピューティングとの組み合わせによりエンドツーエンドの低遅延化が実現できる。エッジコンピューティングは、ユーザ端末に近いネットワークのエッジ側にサーバを配備することでサーバからの応答時間の短縮を図る仕組みで、無線区間の低遅延化とあわせて通信のリアルタイム性を向上させ、自動制御やVR/ARなどのユースケースでの活用が期待されている。5Gにおけるデバイスの同時接続数は100万デバイス/km2と4Gの10倍になっており、機器監視やスマートシティなどIoT分野での活用が期待されている。5Gでは、こうした様々な分野での活用に際して、サービス毎、用途毎に仮想的な専用ネットワークを提供するネットワークスライシング技術を導入し、各々のサービスの利用状況が他のサービスに影響を及ぼさない形で、多種多様な要求に応える複数のネットワークを同時提供することが可能になる。

5Gでは移動通信ネットワークが産業や医療など含むより広範な分野で活用されることになるため、セキュリティ対策の重要性も一層高まっている。過去、移動通信ネットワークでは、偽基地局による盗聴・改ざん、加入者のロケーショントラッキング、基地局への物理攻撃などの様々なセキュリティ脅威に対して、世代を重ねる毎に対策の強化が図られてきている。移動体通信がデジタル化された2Gから無線区間の暗号化やSIMを用いた強固な加入者認証が導入されており、3Gにおいては端末と基地局間の相互認証が導入され偽基地局の脅威に対応している。その他、より強固な暗号アルゴリズムへの変更、有線区間のセキュリティ対策、制御信号の改ざん検知など様々なセキュリティ強化が図られている。今後導入が進むスタンドアローンの5Gにおいては、加入者IDの秘匿の強化によるロケーショントラッキング対策や、ユーザ通信に対する改ざん検知の追加など、4Gにおける残存脅威への対策が図られており、利用者の立場では、より安心して利用できる移動通信サービスが実現されることが期待される。一方で、移動通信ネットワークを構築・提供する立場では、仮想化技術のより一層の活用が進み、エッジコンピューティングやネットワークスライシングなどの新しい仕組みが導入されることで、その構築・運用においてセキュリティ上考慮すべき事項は増えており、国内外で5Gインフラの安全・信頼性確保のための取り組みが進められている。

2.2 ローカル5Gの概要、および制度

この節では文献[2][9]を参考にして記述する。

ローカル5Gは、通信事業者以外の様々な主体（地域の企業や自治体等）が、自らの建物や敷地内において、スポット的に柔軟にネットワークを構築し5Gを利用可能とする新しい仕組みである。携帯電話事業者による全国向け5Gサービスとは異なり、自営の5Gネットワークとして活用が可能となる。想定される利用例としては、スポーツスタジアム運営事業者、遠隔医療を導

入するために医療機関、CATV事業者、事業主が導入するスマートファクトリー、自治体によるテレワーク環境や河川等の遠隔監視、農家が自動農場管理を進めるなど、様々な場面が考えられる。

ローカル5Gのメリットとしては、以下が挙げられる[10]：

- 地域や産業の個別のニーズに応じて柔軟に5Gシステムを構築できる
- 通信事業者ではカバーしづらい地域で独自に基地局を設けられる
- 他の場所の通信障害や災害などの影響も受けにくく、電波が混み合ってつながりにくくなることもほとんどない

ローカル5Gの利用に際しては、無線局免許の取得が必要となる。当面は「自己の建物内」または「自己の土地内」での利用を基本とされていることに注意されたい（例外あり）。申請は、管轄の総合通信局へ必要書類を提出することで行える。円滑に処理を進めるためには事前の相談などが必要な場合もあるので、総合通信局とは早めにコンタクトを取るのが望ましい。

３．ローカル5Gのセキュリティの課題および対策

従来のITシステムにおいて一定のセキュリティ対策が必要であることと同様、ローカル5Gを活用したシステムにおいてもセキュリティの確保は必要である。前章で述べたように、ローカル5Gはこれまで通信事業者のみが提供してきた5Gを用いていることから、システム全体として見たときのセキュリティ確保は従来のITシステムより検討すべき項目が増えるため複雑になることが考えられる。しかしながら、どのようなセキュリティ脅威を想定すればよいのか、その対策を実施する責任者は誰なのかなどについて、十分な情報があるとはいえない。

本章では、本ガイドラインの目的であるローカル5Gセキュリティについて述べる。まず3.1節では、十分な対策を講じないままローカル5Gを利用した場合にどのような不具合が生じ得るかを仮説のストーリーとして紹介する。次に、ローカル5Gのセキュリティについて現時点でどのような認識がなされているかを共有するべく、3.2節でICT-ISACにて実施したアンケート結果を紹介する。その後、3.3節でローカル5Gを活用したシステムで重要と考えられるセキュリティ脅威とその対策例を紹介する。

読者のみなさまは、ローカル5Gシステムを提供する「事業者」、またはシステムを利用する「利用者」のどちらかだと思われる。本章を読んでいただくことで、それぞれの立場で実施が必要な対策を認識し、優先度に応じて対策実施をしていただければ幸いである。

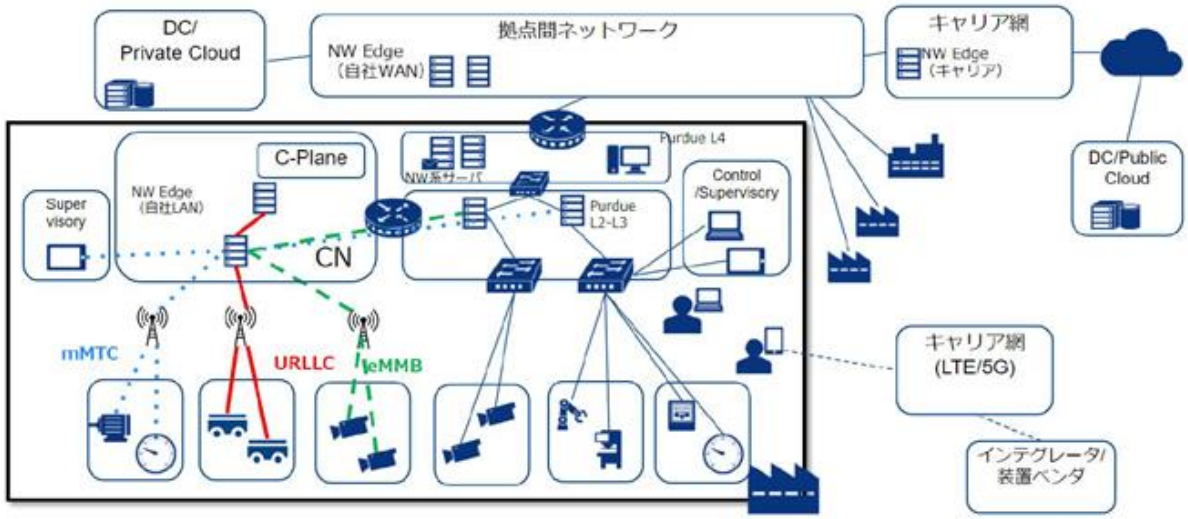
3.1 ローカル5G利用時に想定される脅威（ユースケースによる仮説）

この節では、ローカル5G利用時にセキュリティを適切に対処しなかった場合に起こり得る脅威の例について、仮説のストーリーを用いて紹介する。

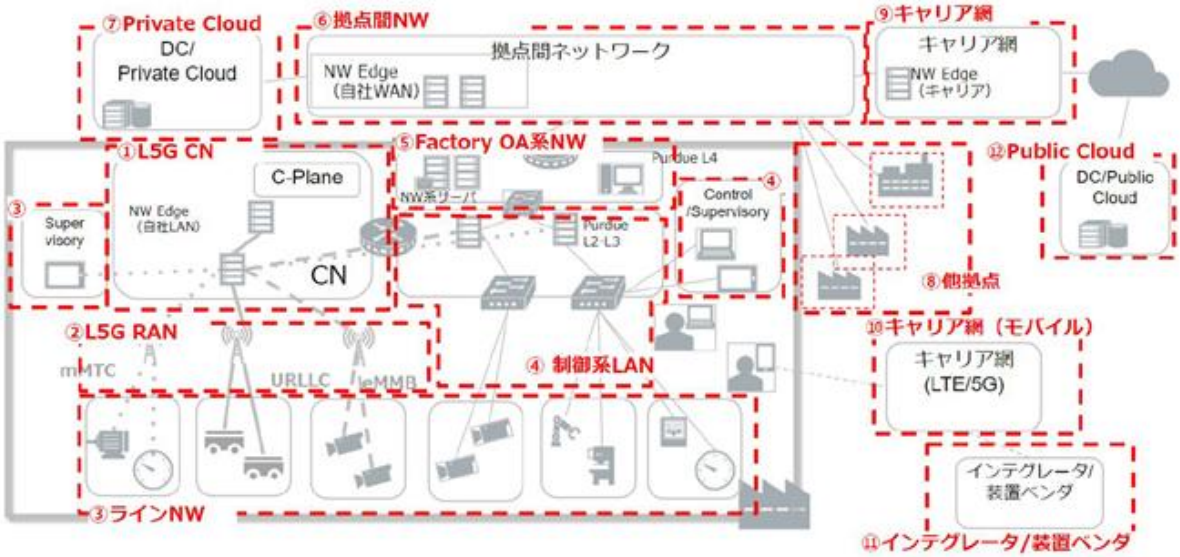
以下のストーリーを読んでいただければお分かりのように、これまでのITシステムでは想定・検討もしないようなインシデント原因が新たに浮上することが考えられる。また、インシデントの原因はありふれたものであったとしても、問題の切り分け時に新たな困難が生じる可能性がある。利用者、事業者の双方においては、関係するシステム・サービスでどのようなインシデントが起こり得るか否か、その検討が求められる。

3.1.1 仮説ストーリー1：自動車工場でローカル5G利用

サイバー自動車は、ローカル5G開始に伴い、工場における既存通信インフラの刷新や工場運用における人的コストの削減を目的に、既存の通信網からローカル5G通信網への換装を実施した。換装後のシステム・ネットワーク構成の概要図については、下図のとおりである。また、各工場内のシステム・ネットワーク構成については、下図と同様の構成で設置されているため、工場A・工場B、又はその他工場についても同じ構成である。



さらに、サイバー自動車は、下図に示す運用形態でローカル5Gを導入している。



■シナリオ１「繋がらないローカル5G」

サイバー自動車は、工場のローカル5G導入に際して、ローカル5G構築支援をサイバー通信株式会社に委託した。サイバー通信は、ローカル5GにおけるCoreNetwork(CN)及びRANに関する構築支援を実施している。また、遠隔によるCN,RANの運用・保守について担任しており、導入から半年間異常なく運用していた。

ある日、サイバー自動車の工場Aにおいて、ローカル5Gに乗せ換えた装置（IoTデバイス）が一斉に応答しなくなるという事態が発生した。この問題が工場A CSIRTから本社CSIRTに送られ、事態発生の１週間前に実施された装置ベンダによるリモート定期点検で装置自体の異常がないことを確認していたため、ローカル5G通信網（CN、RAN）の異常、又はローカル5G網に対するサイバー攻撃の可能性があるとの結論に至り、サイバー通信へ調査を依頼した。

サイバー通信が調査を実施したところ、担任する範囲において異常は見られなかった。そのため、工場Aは、事態を招いた原因が不明な状態での運用は危険であるとの見解から、ローカル5Gに乗せ換えた通信網、装置について運用を、原因が判明するまでの期間停止する決断をした。

数日後、本社CSIRTの調査により、ローカル5Gに乗せ換えた装置（IoTデバイス）に含まれるルート証明書が失効していることが原因であることが判明した。

工場Aは元来、2つの装置ベンダに対して、IoTデバイスを発注しており、その保守整備についても各装備ベンダに委託していたため、サイバー自動車及びサイバー通信による監視・調査における盲点となっていた。また本事案は、工場Aの従来のネットワーク構成下で証明書の自動更新について設定を完了していたが、ローカル5G換装時に設定の見直しをしていなかったことに起因しているとの結論に至った。

■シナリオ２「ローカル5Gにおける情報共有」

サイバー自動車は、ロシアのサンクトペテルブルクに工場Bを運営しており、日本国内にある工場Aと同様の設計で建設されている。工場Bの設計は、Level One Roboticsという下請け業者に委託している。Level One Roboticsは、ローカル5G換装に伴う施設・設備の設計変更について、サイバー通信のロシア支店と、運用前の最終調整段階であった。

ある日、サイバー自動車の自動車製造事業部長宛に、「お金を振り込まないと、日本の工場を停止させる。」といったカタコトの日本語で脅迫電話が入った。役員会議では、本件が重視され、サイバー自動車は調査・対策委員会を設置することとなった。

調査委員会は、Level One Roboticsが、提携している各企業が有する工場の設計図に関するバックアップデータを漏洩させてしまったとの情報を入手した。この事実に基づき、調査委員会は、ローカル5G換装後の設計図に関するバックアップデータが解析されている可能性が大きく、サイバー攻撃による工場の運用停止が予期される旨を対策委員会に報告した。

対策委員会は、調査委員会の報告を受け、同様の設計で建設されている全工場に関連する事案であり、最優先で対処すべき課題であることを認識し、ローカル5G換装に関わった全てのステークホルダーを招集し、リモート会議で対策を検討することとなった。

仮説ストーリー1における教訓：

どちらのシナリオも、ローカル5Gによりシステム構築や運用を手掛けるプレイヤー（＝事業者）が増えたことで、原因がどこであるかの切り分けが問題となっている。マルチベンダによるシステムに対する問題切り分けの困難さは今に始まったことではないが、ローカル5Gを利用するシステムでは、接続される機器の種類や構成を必ずしも十分把握していないローカル5G事業者と、ローカル5G基地局の仕様に精通していない現場のシステム運用担当者の連携が必要になることから、これまでのシステムと比較して問題切り分けがより複雑になり時間がかかるのは自明である。いざというときに原因の切り分けを迅速に行うためには、平常時から、ローカル5G事業者と現場のシステム運用担当者との間で接続機器の構成やネットワークに関する情報を共有しておき、リスクアセスメントを共同で行って、トラブルが発生した場合の原因切り分け手順をルール化しておく等の工夫が必要である。こういった知見を事業者がどの程度有しているかは、ローカル5Gシステムのインシデントに対して迅速に対応できるか否かを左右する、重要なファクターと考えられる。

3.1.2 仮説ストーリー2：ローカル5Gを利用した防災での出来事

近年、異常気象に伴う自然災害が多数発生していることから、X市では市内の河川沿いや山間部にセンサーやカメラを設置。ネットワークにはローカル5Gを利用してセンサーやカメラ映像からの情報や映像を市役所内の災害対策室へ集約、リアルタイムで監視することで河川の氾濫や土砂崩れといった自然災害をいち早く察知する体制を構築した。災害対策、デジタル化、セキュリティ対策の基盤整備を進めるために、システム構築には、大手ITベンダのZ社の提案を採用し、Z社がセンサー、監視カメラ、ローカル5G用アンテナ、そしてネットワークなどを設置した。

■シナリオ１：SIMカードの盗難

監視カメラ群は、建物の屋上や、X市が所有する土地などに設置されていた。河川敷近くに設置されたカメラはフェンスで囲われていたものの、不審者の侵入を強固に防御するには必ずしも十分ではなかった。

ある日の夜、攻撃者が河川敷近くの敷地内にフェンスをよじ登って侵入。監視カメラからローカル5Gアクセスに必要なSIMカードを盗んだ。当該カメラからの映像は途絶えたが、市役所内の災害対策室のメンバーはカメラの機械的故障と判断。Z社に連絡するも業務時間外ということで担当者を捕まえることが出来ず、翌日にベンダZ社へ連絡することとした。

攻撃者は盗んだSIMカードを早速悪用し、タブレットを用いてX市のローカル5Gネットワークに接続。ツールを使い、サーバ等のIPアドレスを確認した攻撃者は災害対策室のサーバに対してログインを試みた。可能性のあるIDのいくつかについてPWを推測して攻撃を仕掛けたところ、ID:saitai、PW:saitaiでログインに成功。サーバを乗っ取った攻撃者は、サーバから重要な情報をネットワーク経由で抜き取るとともにディスク内のファイルを次々に暗号化。サーバは動作を停止し、監視カメラやセンサーからの情報を得ることが不可能になったX市は、その後に台風の直撃を受けたが、河川や山間部の状況を把握することが出来ず、当初想定していた災害対応が後手後手に回ってしまった。

■シナリオ２：建築物等による通信障害

山間部に設置されたセンサーや監視カメラは、土砂崩れの予兆検知や、発生した災害の規模を把握する目的で、専門家から提案を受けた地点に多数設置されている。地形は複雑であることから、ローカル5Gアンテナは見通しの良い場所に設置され、それぞれのセンサーや監視カメラとの接続を良好に保っていた。

ところが、ある時から一部のセンサーや監視カメラの接続が不安定になった。不安定になる機材が設置されている場所はほぼ特定されていたが、不安定になる時間帯は一定しなかった。ベンダのZ社に調査を依頼したものの、ローカル5Gアンテナに不具合はなく、またセンサーや監視カメラ側の機材にも不具合はなかった。念のため機材を新品に入れ替えたものの、接続の不安定は解消されず、Z社としてもお手上げの状況であった。仕方なく、原因が分からないまま不安定な利用を続けざるを得なかった。

原因は、山中の土地所有者が建設したコンクリート建造物であった。この建築物がアンテナとセンサーの間に建てられたため、5G電波が届きづらくなって接続が不安定になっていたことが判明したのは、事象が発生してから相当時間が経過してからのことであった。

仮説ストーリー2における教訓：

シナリオ1では、センサーや監視カメラの物理的セキュリティが十分でないことが問題であった。ローカル5GではSIMカードの有無で接続可否がコントロールされるため、一般には無線LANよりセキュリティが高いと考えられている。しかしながら本シナリオのようにSIMカードが万が一盗まれた場合は、攻撃者によるネットワーク侵入の可能性がある。

次に、物理的なセキュリティ確保に加え、ローカル5Gで構築されるネットワークにおいても最低限のセキュリティ対処は必要である。シナリオにあるような容易に想像できるID/PWの設定を避けることに加え、端末の脆弱性対策も必要である。

なお、市役所とZ社は保守運用契約を締結していると思われるが、シナリオ1のような場合も想定されているか精査が必要である。自治体の防災システムにおいて、担当者に連絡が取れないことが果たして許容されるのかは、検討の余地がある。

シナリオ2では、Z社の原因究明において機材の故障や設定ミスが原因と思いこみ、それらの確認をしたものの、周辺の状況変化までは気づくことが出来なかった。ローカル5Gは5GというITベンダでは取り扱ってこなかった通信を活用している。よって、さまざまな通信障害に対して適切な問題切り分けが出来るよう、ITベンダは準備をする必要がある。場合によっては、メジャーな通信事業者との連携も有効な手段である。

3.2 アンケートの実施とその結果

本ガイドラインの執筆時点(2022年3月)では、ローカル5Gのビジネスはまだ立ち上がったばかりといえる。ビジネス事例が少ないこともあり、ローカル5G事業を進める側にとって具体的に何に気をつけなければならないか、またサービスを受ける側においても事前に自ら検討すべき点は何か、といった情報は必ずしも多くない。特にセキュリティの観点では、「ローカル5Gセキュリティは重要」との指摘がされているものの、具体的に何を実践すれば良いのかといった情報は少ないと思われる。

そこでICT-ISACでは、ローカル5Gサービスを提供する事業者と、ローカル5Gサービスを利用すると思われる利用者の双方に対し、ローカル5Gサービスの提供・利用に際してどういった課題があるかを明らかにすることを目的としたアンケートを実施した。アンケート結果の概要はICT-ISACホームページに掲載されている[4]。興味のある方はご覧いただきたい。

アンケートの基本情報は次の通りである。

【目的】

ローカル5Gのセキュリティガイドライン策定のため、ローカル5Gセキュリティに対する世の中のニーズを把握すること

【実施期間】

2020年12月14日～2021年2月1日

【アンケート依頼先】

- ICT-ISAC会員企業
- ローカル5G免許事業者
- 5Gセキュリティ推進グループ参加メンバーより、関係社、関係団体に依頼
- 国内他業種ISAC（金融ISAC、電力ISAC、交通ISAC、ソフトウェアISAC、J-AUTO-ISAC、貿易会ISAC）

3.2.1 事業者

ローカル5G関連事業を展開するにあたって、回答企業のうち80%は何らかの検討を実施、あるいは実施中である（図1）。これより、多くの事業者が何らかのセキュリティ対策の必要性を認識していることがわかる。

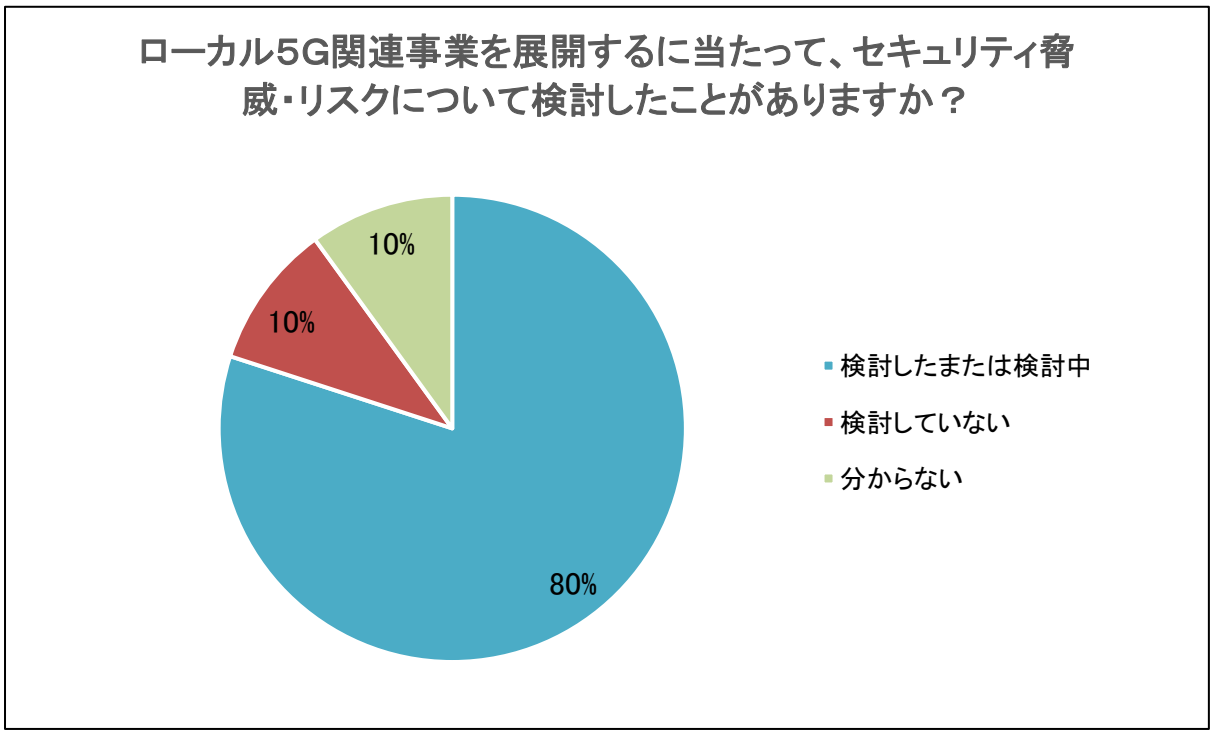


図１

具体的な検討方法については、自社で独自に検討している事業者が一番多い（図2）。しかしながら「何が問題になるかわからない、どうすればセキュリティが守れるか分からない」と感じている事業者が多く、ローカル5Gのセキュリティに関する適当な外部ドキュメントがないことから、手探りでの検討になっている状況がわかった（図3）。

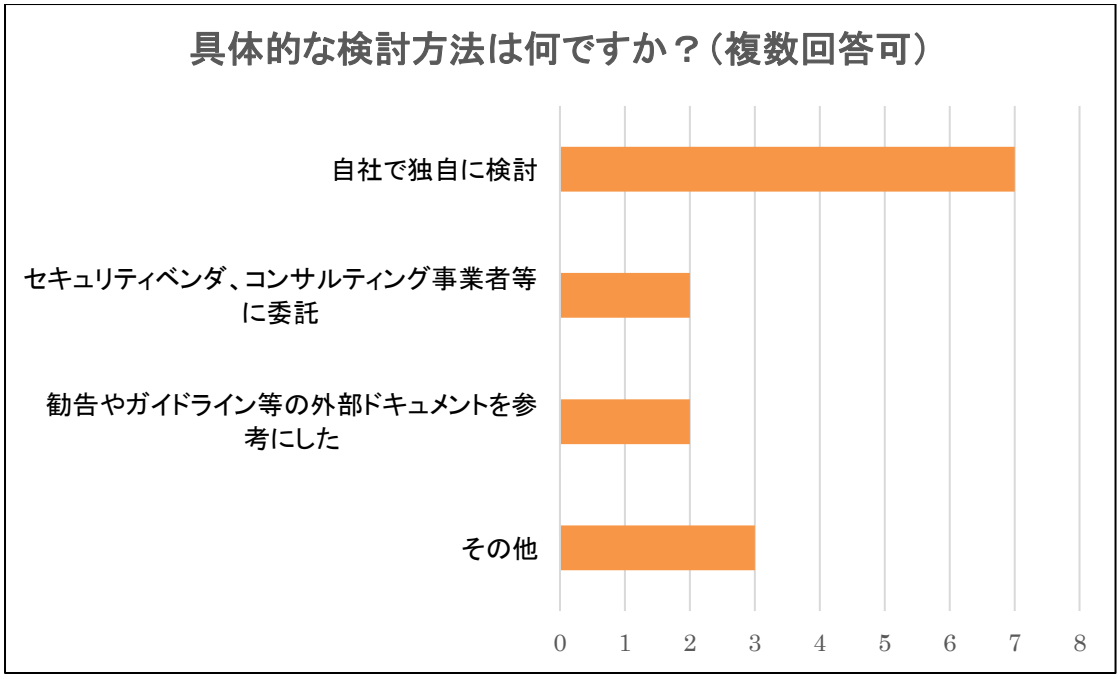


図２

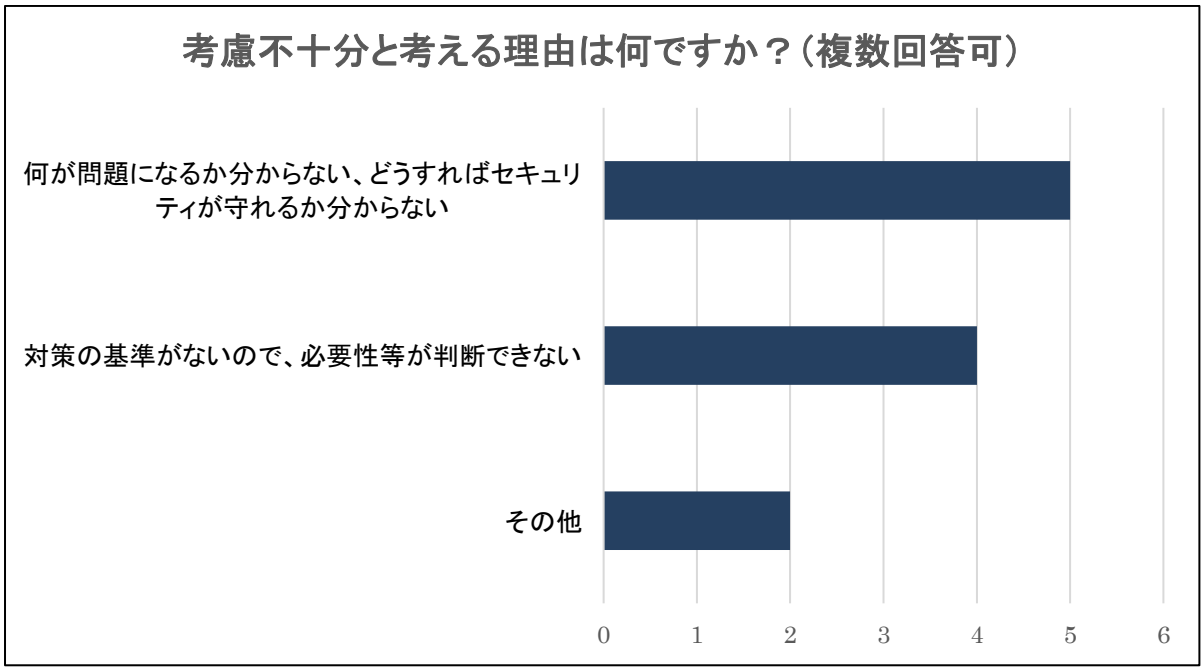


図３

また、セキュリティ対策として定めるべき要件については、特に5Gネットワーク特有の対策に対するニーズが大きいことから（図4, 図5）、既存のICTセキュリティ対策と5G特有の対策を明確にしたガイドラインを策定することで、ガイドライン利用者の理解度が高まると想定される。

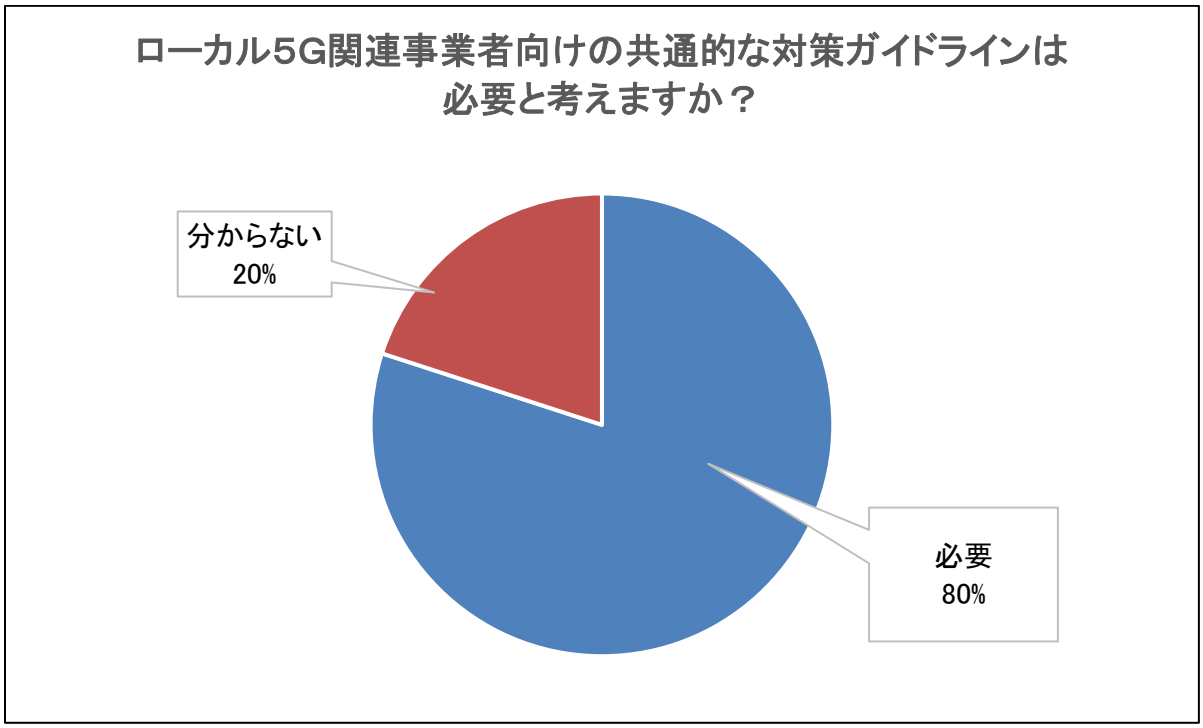

ローカル5G関連事業者向けの共通的な対策ガイドラインは
必要と考えますか？
分からない
20%
必要
80%

図４

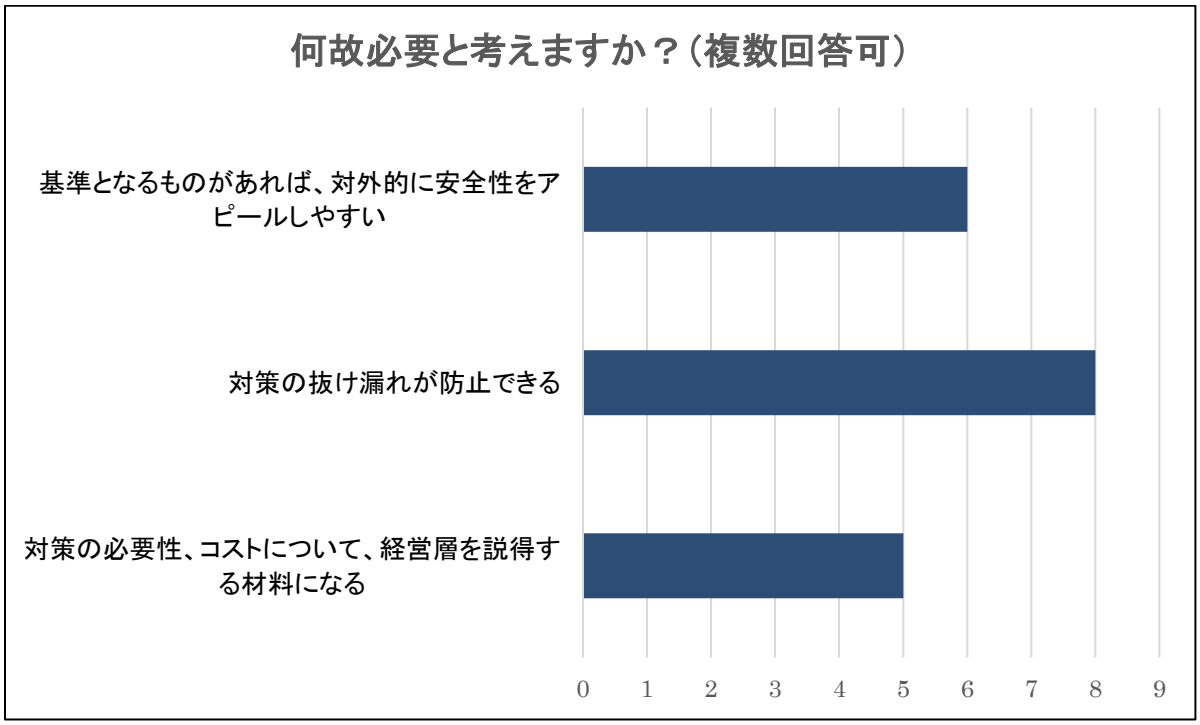

何故必要と考えますか？（複数回答可）
基準となるものがあれば、対外的に安全性をアピールしやすい
対策の抜け漏れが防止できる
対策の必要性、コストについて、経営層を説得する材料になる
0
1
2
3
4
5
6
7
8
9

図５

3.2.2 利用者

ローカル5Gの導入・利用を検討している企業は半数弱ではあるが、現状を考慮すると一定数がローカル5Gに興味は持っているものと考えられる。しかしながら、具体的な導入まで検討は進んでいないところが大半で、セキュリティの検討も進んでいない状況がうかがえる（図6）。

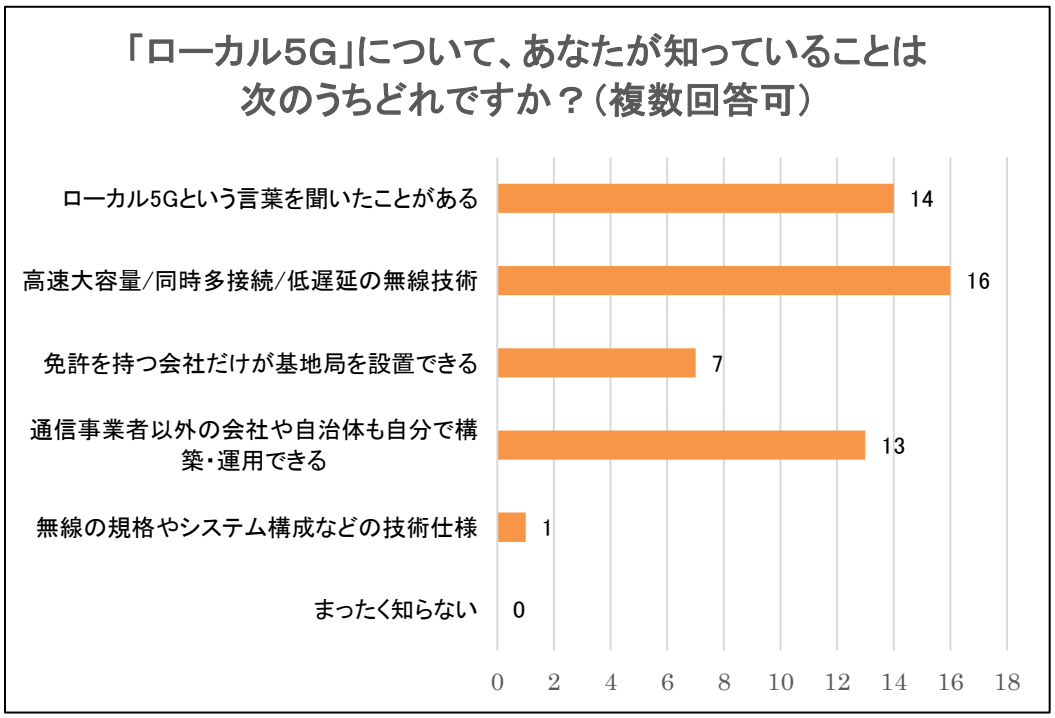


図６

しかし、ローカル5Gのセキュリティ対策を社外に任せるのではなく、社内のシステム部門で責任をもち検討・対策しようとしており、セキュリティに対する意識は高いことが分かる（図7）。

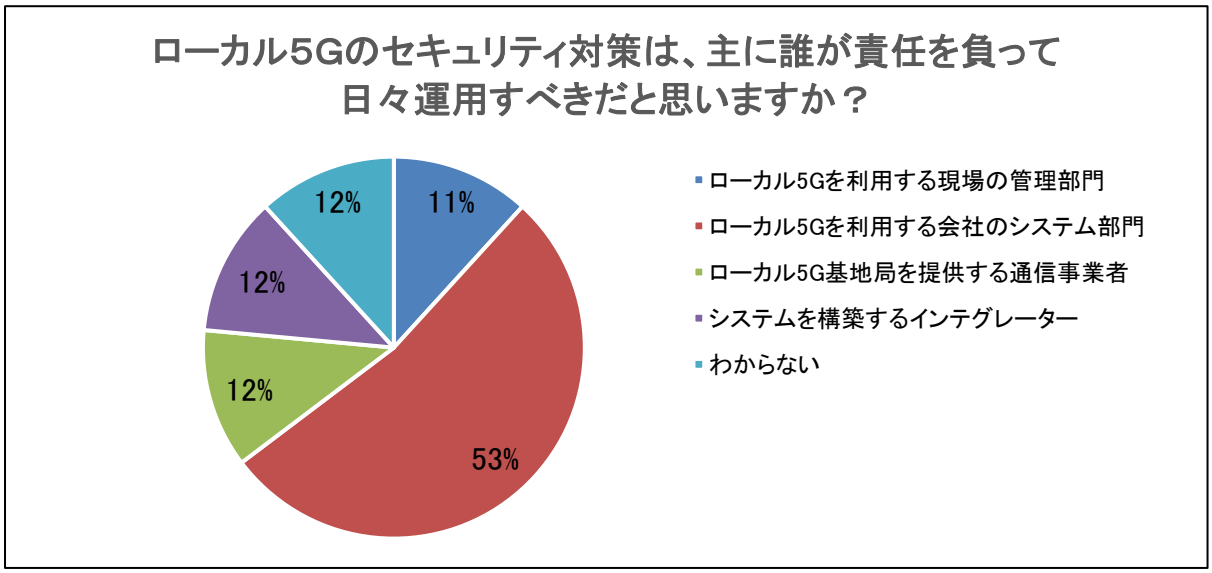


図７

現在のLAN等のセキュリティに対しては、外部企業を活用するなどセキュリティ対策を検討している。またセキュリティ対策には各種ガイドラインを活用している割合が高い（図8）。

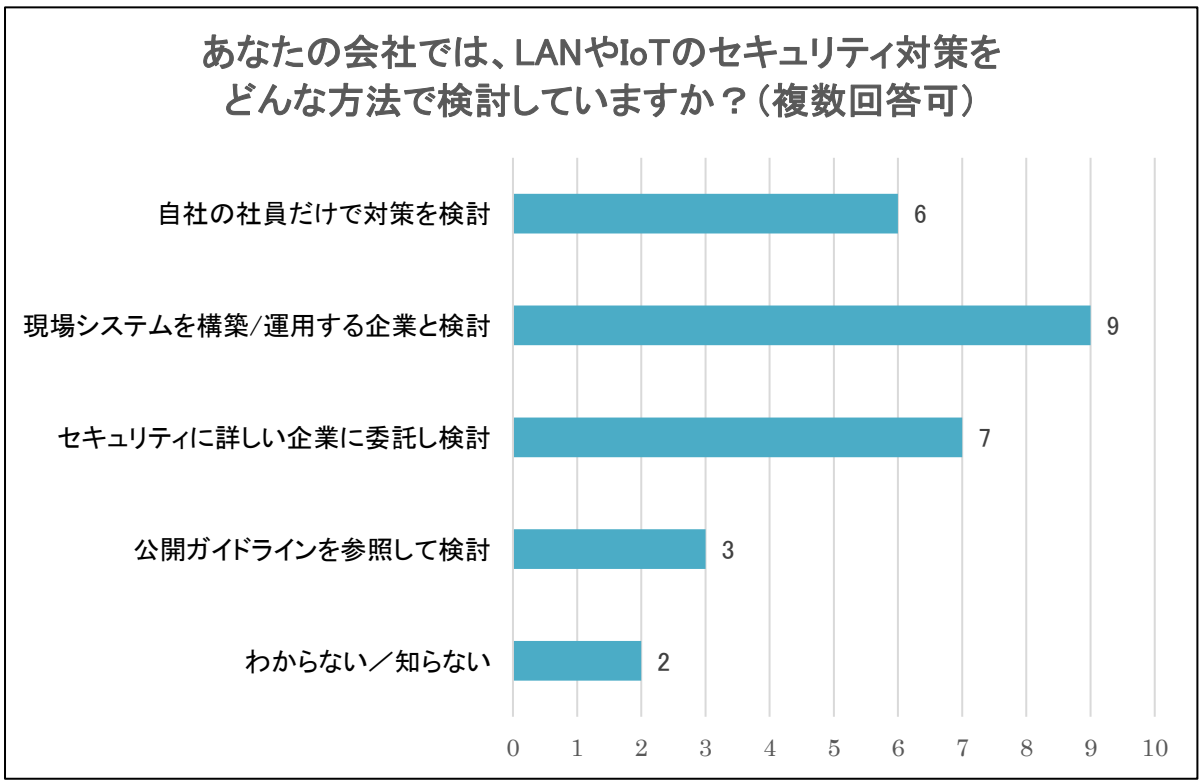


図８

このため、ローカル5Gに対しても、参照できるガイドライン、特に業界別のガイドラインが求められていると考えられる。

ICT-ISAC「5Gセキュリティ推進グループ」では、これらのアンケート結果から事業者・利用者それぞれのニーズを把握するとともに、メンバーによるローカル5Gサービスにおけるセキュリティ課題を検討して本ガイドラインを作成した。残念ながら、本ガイドラインの執筆時点(2022年3月)ではローカル5Gの普及は十分でなく、さまざまな業種業界での利用例に乏しいため、業界別のガイドラインの作成は今後検討することとし、現時点での知見に基づいた共通的なローカル5Gセキュリティガイドラインを目標としている。

3.3 主なリスクとその対策例

この節では、ローカル5Gを利用・提供するにあたって検討すべきセキュリティ課題のうち、特に検討が必要と考えられる課題を記載している。ご承知の通り、セキュリティ課題は多数存在し、一つでも多く対策を打つことに越したことはない。しかしながら、多く対応すればするほどリソースがかかることから、サービスそのもののリスクや機密情報がどこに保管されているか、などを考慮し費用対効果やスケジュールも加味しながら検討すべきである。なお、全ての項目がローカル5G特有のセキュリティ脅威ではないことに注意されたい。これまでのITシステム・ソリューションで求められているような、既に知られている課題・対策も含まれているが、そのような項目は数多くあるセキュリティ対策の中でも普遍的なものであり、本ガイドライン執筆陣としてもぜひ対策を検討してもらいたい項目と認識いただきたい。

以下では、リスクの内容、対策を打たなかった場合にどのような被害が予想されるか、そしてどのような対策を打てばよいかを、リスクごとに記載している。一般的には、サービスを提供する事業者側がセキュリティ対策を検討することになるが、だからといって利用者側は何もしなくていいわけではないことに注意されたい。最終的にローカル5Gを活用したシステムを利用するのは利用者側であり、もしこのシステムで何等かのセキュリティ事故・事件が発生した場合にもっとも被害を受けるのは利用者自身である。もちろん、利用者側にセキュリティの専門家がおらず、何をすればいいのか見当もつかない、ということは十分にあり得る。本項ではローカル5G利用において重要と思われるセキュリティ課題を記載しているので、ぜひこれらの情報を活用し、自らのシステムではこれらの課題がどうなっているかの確認をしていただきたい。

以下の項では、リスク内容と共に「脅威」「脆弱性」「NWのどの部分で発生するか」「誰が対処すべきか」を記載している。「脅威」「脆弱性」は、STRIDEの分類法をベースに一部修正して作成している。詳細はAppendixを参照してほしい。その後に、当該リスクの詳細な説明と対処策について述べる。読者はそれぞれの項目を活用し、読者自身にとって重要と思われる項目から読むことをお勧めする。

主なリスク	リスクに対する脅威と対策例
デバイスのなりすまし	3.3.1 脆弱なIoTデバイスへのなりすまし不正ログイン
	3.3.2 SIMカードの不正利用によるなりすまし不正ログイン
基地局間中継機器のなりすまし	3.3.3 バッテリードレイン攻撃によるデータの改ざん
機器へのDoS攻撃	3.3.4 5Gコアへの不正メッセージ攻撃
	3.3.5 IoTデバイスからの大量シグナリングメッセージ攻撃
外部要因による通信品質劣化	3.3.6 障害物による電波妨害
盗難・盗聴によるデバイスの悪用	3.3.7 デバイスのアクセス制限管理不備による盗難
	3.3.8 未暗号によるデータ盗聴
	3.3.9 デバイスの設置管理不備
物理的な脆弱性	3.3.10 侵入者による証跡ログの削除
	3.3.11 IoTデバイスの踏み台化による内部感染
	3.3.12 出入り業者によるIoT機器の持込や設備構成変更
	3.3.13 リモート管理の誤操作・誤設定による不具合やセキュリティホール

3.3.1 脆弱なIoTデバイスへのなりすまし不正ログイン

項目	項目の定義・説明
リスク内容	脆弱なIoTデバイスにマルウェアが仕込まれ、共有リソースへのアクセスID、パスワードを搾取し共有リソース上の機密情報が漏洩する
脅威	なりすましによる不正ログイン
脆弱性	人的・環境的脆弱性、共有リソースの不正な使用
NWのどこの箇所か	エッジデバイス（IoT機器、タブレット、スマホ等）
誰が対処すべきか	事業者
リスク概要	ローカル5Gネットワークに接続されるIoTデバイスのセキュリティ対策が脆弱である場合、機密情報の入手を目的としたサイバー攻撃の不正ログインの踏み台となりマルウェアが仕込まれ、共有リソース上の機密情報漏洩の原因となる可能性がある。 IoTデバイスのセキュリティ対策が脆弱な例としては、①IoTデバイス自身に類推されやすいパスワードや強度の低いパスワードが設定されている場合、②IoTデバイスのOSやソフトウェアに実装上の脆弱性がある場合、が挙げられる。
対処策	事業者はIoTデバイスに設定するパスワードについて、容易に類推されないようパスワード設定ルールを規定し運用する必要がある。 また、IoTデバイスの脆弱性を定期的に検査し、検査に合格したデバイスのみを利用することが望ましい。具体的な脆弱性の検査手法としては脆弱性検査スキャナーや、ペネトレーションテスト（侵入テスト）ツールがある。 さらに、不正ログインやマルウェア感染を100%防ぐことは困難であることから、マルウェアの検知と削除が実施できるセキュリティ対策ツールを運用し、マルウェアに感染した場合でも被害を食い止めるよう対処することが望ましい。

3.3.2 SIMカードの不正利用によるなりすまし不正ログイン

項目	項目の定義・説明
リスク内容	悪意者がIoTデバイスのSIMカードを窃取し、不正デバイスに当SIMカードが使われシステムへログイン、システム内へマルウェアが仕込まれ、システムがサイバー攻撃を受ける
脅威	なりすましによる不正ログイン
脆弱性	不正デバイスの接続
NWのどこの箇所か	エンドポイント
誰が対処すべきか	事業者、利用者
リスク概要	ローカル5Gシステムに対するセキュリティ脅威は、外部からの脅威侵入と内部からの脅威侵入との2つに大別することができる。特にローカル5Gを含むモバイルネットワークにおいては内部からの脅威侵入が懸念点となる。モバイルネットワークで使用されるデバイスは、有線ネットワークのデバイスに比べ設置場所が厳密に固定されず、第三者による接触が容易な場合が多い。また、節電のために不使用時にデータ通信を停止したり、休止状態に移行するモバイルデバイスも存在し、デバイスの状態変化が頻繁に発生するためにセキュリティ状態も変化しやすい。 特徴的な内部脅威の一例としてSIMカードの不正利用によるなりすましによる不正ログインがある。SIMカードは、セルラーモバイルネットワークでは接続デバイスの識別子として機能し、その内部に格納された暗号鍵を基にネットワーク接続の可否を判断する認証に使用される。SIMカードは高レベルな耐タンパ性が特長で、基本的に外部からSIMカード内への侵入・内部データの改ざんは不可能といわれている。そのためこのSIMカードを基にしたデバイス認証は非常に強力であり、モバイルネットワークの高セキュリティ性を支えている。一方で認証がこのSIMカードに依存しているがゆえに、SIMカードさえ正しければどんなデバイスでもモバイルネットワークにつながってしまう危険が発生する。 本脅威はSIMカードを正規デバイスから不正に窃取し、許可されていないデバイスに差し込んで使用するSIMスワッピングと呼ばれる不正行為として知られており、ローカル5G環境においても発生が懸念される。
対処策	ローカル5Gは、DX化の進展に伴い、今後より多種多様のデバイスの使用やBYODの積極活用が想定され、これらの新たな利用デバイスに対するセキュリティ対策も求められる。なりすましによる不正ログインの対策は、他のセキュリティ脅威・リスクにつながる最初の入り口となるため、特に対策の中でも重要なポイントとなる。 ローカル5Gシステムは、自営での運用のため、利用者がローカル5Gシステムに接続されるすべてのデバイスとそのセキュリティ状態を一元的に管理・監視するための対策が望ましい。SIMスワッピングの対策は、ローカル5Gシステムに接続されるデバイスの真正性(正しいデバイスであること)を常に保証することが求められる。例えば、デバイス識別番号のIMEI、SIM識別番号のIMSIを組み合わせることで、SIMスワッピングされた異なるIMEIの不正デバイスからの接続時に真正性チェックを行うことができ、当該リスクの対策が可能と考える。

3.3.3 バッテリードレイン攻撃によるデータの改ざん

項目	項目の定義・説明
リスク内容	悪意ある攻撃者がIoTデバイスと基地局の間に設置した中継機器によりIoTデバイスの省電力モード機能を無効にして、本来長寿命であるIoTデバイスのバッテリを消耗させる(バッテリードレイン攻撃)
脅威	データの改ざん
脆弱性	システム脆弱性
NWのどこの箇所か	ローカル5G基地局、エッジデバイス（IoT機器、タブレット、スマホ等）
誰が対処すべきか	事業者
リスク概要	悪意ある攻撃者がIoTデバイスと基地局の間に偽の基地局になりすました中継機器を設置した場合、偽の基地局はIoTデバイスに対してローカル5Gネットワークへの再接続要求を送信することが可能となる。再接続要求を受信したIoTデバイスは一旦ネットワークとの接続を解放し、省電力モードからIdleモードに移行したのち再接続を試みる。 この再接続が頻繁に実行されると、短い周期でIoTデバイスからネットワークへのシグナリング通信が発生するため、IoTデバイスのバッテリが急激に消耗する可能性がある。これにより、本来長期間バッテリ交換を行わないことを想定するIoTデバイスの運用に影響を及ぼす可能性がある。
対処策	事業者はIoTデバイスと基地局の間のネットワークにおいて、管理外の中継機器が物理的に設置されていないかどうかを適切に管理する必要がある。また、IoTデバイスのベンダと協力してデバイスの消費電力や省電力モードの状態を定期的に監視し、異常状態が発生した場合に即座にネットワーク管理者に通知する仕組みを構築しておくことが望ましい。

3.3.4 5Gコアへの不正メッセージ攻撃

項目	項目の定義・説明
リスク内容	5Gコアが異常なフォーマットもしくは異常なパラメータを含むメッセージを外部から受信し、検証や破棄の処理が不十分である場合に、ソフトウェアの不具合によりシステムのパフォーマンスが著しく低下、もしくは停止する
脅威	特定の脆弱性によるDoS
脆弱性	システム脆弱性
NWのどこの箇所か	5Gコア
誰が対処すべきか	事業者
リスク概要	5Gコアが外部のNWから想定しないフォーマットやパラメータのパケットを受信し、正しく検証や妥当性の確認が行われない場合、ソフトウェアの処理に異常をきたし主に可用性に影響を与える可能性がある。 具体的には5GコアのNF上でパケット処理がスタックし、トランザクション処理性能が低下する事象や、ファームウェアや内在するモジュールの再起動が発生し、処理中のコネクションが切断される事象が発生する。 一時的な影響に留まる脆弱性でも、継続的に不正パケットを受信する場合、さらに影響が拡大する可能性があり、利用者側への影響としては、通信品質の低下、あるいは接続や通信不可に至る。
対処策	事業者は、5Gコアが運用上想定されるパケットのみ処理するようパケットの検証とエラー処理が妥当であるか確認する必要がある。 具体的な対策としては、5Gコアの開発時に既知の脆弱性を発見するシステムセキュリティテストに加え、製品固有の脆弱性を発見するファジングテストを実施する事が望ましい。外部のベンダに5Gコアのシステム開発を依頼する場合にはこれらセキュリティテストの実施結果を開示可能であるか確認しておくことが望ましい。 利用者も事業者が提供する5Gシステムのセキュリティ対策を評価する上で、どのようなセキュリティテストを実施しているか情報提供可能であるか確認する事が望ましい。 持続的なセキュリティ対策として、システムセキュリティテストおよびファジングテストはソフトウェアのアップデートやシステムの更改のタイミング、特に外部ネットワークとの接続点が増加するタイミングで実施する事が望ましい。 ファジングテスト実施例 ・診断対象メッセージ 外部から到達する可能性のあるリクエストメッセージ、レスポンスメッセージ。運用上受信する想定がされていないメッセージタイプやAPIパラメータも含める。 ・想定する攻撃シナリオ 5GコアにNW接続する事が想定されている他組織の設備から設定ミスやソフトウェアバグで意図しない不正なフォーマットやパラメータを持つパケットが送信される。 5Gコアに接続されることが想定されていない悪意ある第三者が、隣接する設備を踏み台に、もしくは直接5Gコアに対して意図的に不正なフォーマットやパラメータを持つパケットを送信する。 ・フォーマットのファジング（例） パラメータの順序を入れ替える、同じパラメータを繰り返す、Mandatoryパラメータを削除する、パラメータのメタ値をランダムデータにする。 ・パラメータのファジング（例） 規程外のパラメータデータを入力する（ランダムなデータを含む）、長大なデータを入力する、Null値を入力する。

3.3.5 IoTデバイスからの大量シグナリングメッセージ攻撃

項目	項目の定義・説明
リスク内容	マルウェアにより不正に制御されたIoTデバイスからシステムの容量を超える大量のシグナリングが送信され、システムを停止させる
脅威	特定の脆弱性によるDoS
脆弱性	システム脆弱性
NWのどこの箇所か	エッジデバイス（IoT機器、タブレット、スマホ等）、ローカル5G基地局、5Gコア
誰が対処すべきか	事業者
リスク概要	ローカル5Gネットワークに接続されるIoTデバイスのセキュリティ対策が脆弱な場合、悪意のある攻撃者が仕込んだマルウェアによりデバイスの制御を不正に乗っ取り、大量のデバイスを同時に再起動させることが可能となる。これにより各デバイスからネットワークへ再接続要求のための大量のシグナリングが送信され、基地局やコアネットワークを過負荷状態に陥らせてシステムの性能劣化や停止につながるおそれがある。
対処策	事業者は、3.3.3節の対処策で述べたIoTデバイスに対する不正アクセス対策を確実に実施する必要がある。 また、事業者は基地局ならびに5Gコアのベンダと協力し、これらの装置において処理可能なシグナリング量のしきい値を適切に設定し、しきい値を超える大量のシグナリングが発生した場合は再接続要求を拒否して正常なIoTデバイスの接続を保護できるよう、システム停止に陥らない対策を取ることが望ましい。

3.3.6 障害物による電波妨害

項目	項目の定義・説明
リスク内容	非管理者によるエリア内に通信妨害物・遮蔽物が設置され通信遅延が発生する
脅威	外部要因による通信品質劣化
脆弱性	人的・環境的脆弱性
NWのどこの箇所か	5Gエッジ
誰が対処すべきか	事業者、利用者
リスク概要	ローカル5Gの周波数の1つである、28.2GHz～28.3GHz帯は直線的な電波を持つ周波数帯であるため、障害物に弱いという性質を持つ。そのため障害物の多い環境では、通信できる距離が短くなりカバーエリアが狭くなってしまう。 例えば工作機器やロボット、クレーン等が常に稼働するような工場環境においては、これらが動く障害物となることでローカル5Gの電波伝搬に影響を及ぼし、思わぬ形で通信遅延やスループット低下を招くリスクがある。 そのためローカル5Gネットワークの構築後、カバーエリアを意識せずに工場内部で工作機器の増設やレイアウト変更を実施した場合、電波伝搬環境が変動し通信品質劣化に陥るリスクも考えられる。
対処策	事業者はローカル5Gネットワークの構築前に、電波伝搬に影響を与える障害物を考慮したエリア設計を実施する必要がある。具体的には、設計段階における電波伝搬シミュレーションツールによる机上のエリアプランニングの実施に加え、実環境におけるスペクトラムアナライザ等による電波環境調査の実施が望ましい。これにより、工場環境での工作機器のような動的な障害物が電波伝搬に与える影響を考慮したエリア設計が可能となる。 さらに事業者は、ローカル5Gネットワーク構築後にカバーエリアが損なわれないよう、予め利用者との間で機器増設やレイアウト変更等に関する指針を取り決めておくことが望ましい。加えて、事業者が定期的に電波環境調査を実施し、当初設計通りのカバーエリアが維持されているかどうかをチェックしておくことも有効な対処策となる。

3.3.7 デバイスのアクセス制限管理不備による盗難

項目	項目の定義・説明
リスク内容	ローカル5G構成機器のファームウェア、設定情報、ログ等へのアクセス権限管理が十分でなく、悪意ある者によって機器から盗み出される
脅威	盗難
脆弱性	システム脆弱性
NWのどこの箇所か	5Gコア
誰が対処すべきか	事業者
リスク概要	ローカル5Gを利用する際には、当然ながらローカル5Gを提供するための構成機器が必要である。これらの機器の設定は、サービス仕様に沿って事業者が実施する。事業者は、サービス開始後の保守運用も視野に入れてアクセス権限を設定すると思われるが、作業者の単純なミス・運用途中での設定変更の引継ぎ漏れ、などの理由で、あるべき設定内容になっていない場合が考えられる。 アクセス権限の設定は非常に重要であり、管理が十分でない場合、本来はアクセスできないはずのユーザによるデータの読み込みが発生し得る。構成機器内の設定情報や、ID/PWといった情報が洩れ、更なるサイバーインシデントにつながり被害が拡大する恐れがある。
対処策	事業者は、サービス仕様に基づいたアクセス権限設定を決定し、利用者とも合意を取っておくことが望ましい。また、保守運用中にアクセス権限の変更を行う場合には、その変更履歴を確実に記録するとともに、保守運用のチーム内で共有しておくことが望ましい。これらの情報は、保守運用のメンバーが人事異動などで交代する際、引継ぎ事項の一つとしておくことが望ましい。 事業者は、定期的（一年に一度、など）にアクセス権限の設定項目を調査し、本来のサービス仕様に沿った設定になっているか確認をとることが望ましい。利用者は、可能ならば事業者から定期的に報告を受けた方が良い。利用者は、可能ならば事業者との保守運用契約に、その旨を記載した方が良い。

3.3.8 未暗号によるデータ盗聴

項目	項目の定義・説明
リスク内容	C-Plane/U-Planeを流れるデータが設定不備による未暗号によりデータが盗聴される
脅威	盗難
脆弱性	システム脆弱性/人的・環境的脆弱性
NWのどこの箇所か	5Gコア／RAN
誰が対処すべきか	事業者
リスク概要	弱い暗号アルゴリズムの使用や暗号処理の省略を許容する不適切な設定が行われていた場合に、制御プレーンやユーザプレーンを流れるデータが盗聴される恐れがある。
対処策	ローカル5Gシステムで使用する暗号アルゴリズムや暗号鍵の鍵長に関するポリシーを定め、5Gの各コンポーネントにおいてポリシーに従った安全な暗号アルゴリズムが使われていることを保証すること。また、ユーザ端末とのセキュリティネゴシエーションの際に、ユーザ端末から不正な構成パラメータを提示されたとしてもそれを受け入れないことを検証すること。

3.3.9 デバイスの設置管理不備

項目	項目の定義・説明
リスク内容	誰でもアクセスできる場所にあるローカル5G構成機器を悪意ある者に盗み出される
脅威	盗難
脆弱性	物理的脆弱性
NWのどこの箇所か	エンドポイント(エッジデバイス)
誰が対処すべきか	事業者、利用者
リスク概要	ローカル5Gはデバイスを無線技術によってネットワーク接続するため、従来の有線接続に比べ設置場所やデバイス位置変更に対して柔軟性が高い。そのため、屋外での利用や、ラインレイアウト変更が頻繁に発生する工場内、自動搬送車に代表される移動体等で利用が期待される。その一方、屋外等のオープンなエリアにデバイスが設置された場合には不特定な人物による物理的接触を許す可能性があり、また運用時にデバイスが管理者の有視界範囲にない場合にはデバイスの位置が変わってもすぐには気づきにくい問題があり、悪意のある者によってデバイスが盗難にあうリスクが存在する。また、一旦奪取されたデバイスに不正な変更が加えられたり、マルウェア等を組み込まれ、再度ネットワークに接続された後に不正行為の足掛かりとされるリスクもある。
対処策	デバイスを屋外に固定設置する場合には、第三者が不用意に接触したり取り外したりできないように、デバイス設置場所への接近を制限したり、デバイスをしっかりと固定する等の物理的な対処を施す必要がある。これらの対処は屋内においても内部不正行為を防ぐために考慮する必要がある。 また、運用管理の中でデバイスのネットワーク接続状態を常に監視し、予定外の接続状態変更に対してアラームが上がる仕組みを用意しておくことも重要である。Cell-IDやデバイスに搭載されたGPS機能でデバイスの位置を常時確認・トラッキングできる仕組みを用意できれば、万が一のデバイス盗難時の調査・対処に役立つ。 さらに、デバイスが意図せずネットワーク接続が切断されたのち、再び接続要求があった場合には、そのまま通常接続に戻さず、通信先や利用サービスが限定される検疫ネットワークに一旦接続、デバイスの正常性を確認の上で通常接続に戻す等の対策が有効である。

3.3.10 侵入者による証跡ログの削除

項目	項目の定義・説明
リスク内容	ログが削除され、不正侵入に気づかない
脅威	その他（ログの削除）
脆弱性	物理的脆弱性
NWのどこの箇所か	ローカル5Gコア、システム、NOC/SOC
誰が対処すべきか	事業者、利用者
リスク概要	通常、システムでは操作ログ、システムログなど多くのログが記録される。これらログが適切に管理、運用されておらず不正侵入に気づかないリスクがある。例えば、そもそもログが管理されてない場合や、侵入者が不正アクセスの痕跡を削除する場合が考えられる。 ローカル5G環境においては、利用者はITシステムのログに加えて、ローカル5Gシステムのログを管理することとなり、ITとローカル5Gシステムのログをもとにセキュリティ対応を考える必要があり、ログ統合などの運用が煩雑化する懸念がある。
対処策	ログを複数個所で記録またはバックアップを取得することを検討する。不正侵入により痕跡を削除された場合は、削除されたログの時間帯や周辺の関連ログを相互参照することでログの追跡が可能となる。

3.3.11 IoTデバイスの踏み台化による内部感染

項目	項目の定義・説明
リスク内容	Miraiなどのマルウェアに感染したIoTデバイスがローカル5Gに接続され、内部の機器が同様に感染する。また、C&Cサーバからの遠隔操作により、感染機器が攻撃の踏み台として利用される。
脅威	その他（マルウェア感染。踏み台）
脆弱性	不正デバイスの接続
NWのどこの箇所か	エンドポイント
誰が対処すべきか	事業者、利用者
リスク概要	すでにマルウェアに感染した機器が、ローカル5Gネットワークに接続することで、内部の機器が同様にマルウェア感染する可能性がある。 また、外部のC&Cサーバに接続できる経路が存在する場合には、感染した機器が遠隔操作される可能性が高くなることで、情報漏洩につながったり、DDoSの攻撃元（踏み台）となるリスクがある。
対処策	内部感染等のリスクについては、機器の認証等により不正な機器が接続されないようにする。ローカル5Gネットワーク内において、不正な通信の検知（IPS/IDS）ができる装置の設置検討が望ましい。各機器での感染防止として、不要なアプリの停止、ポートを閉じる。最新のセキュリティパッチの適用を行う。 さらに、可能であれば、機器上でマルウェア対策あるいはホワイトリスト型によるマルウェアの実行防止等を実装する。 C&Cサーバへのアクセスについては、レピュテーション機能を持つ通信装置などを置くことにより、C&Cサーバへのアクセスを防止することで、それ以上の被害を防ぐことを検討する。

3.3.12 出入り業者によるIoT機器の持込や設備構成変更

項目	項目の定義・説明
リスク内容	出入り業者によるIoT機器の持込や設備構成変更により、予期せぬ通信の挙動や障害が発生する
脅威	その他
脆弱性	物理的脆弱性
NWのどこの箇所か	エンドポイント(エッジデバイス)
誰が対処すべきか	事業者、利用者
リスク概要	ローカル5Gが導入される工場、プラント、ビル、スタジアム等には、そこに設置されている装置や機械のメーカー、設置事業者、運用事業者、点検事業者、保守事業者等が日々出入りしている。それらの事業者が、装置・機械の通信の設定や設置場所を変更したり、装置・機械の監視のためにローカル5Gのネットワークを利用したり、予兆保全のために無線通信機能を持つIoT通信機器を設置したりすることも想定される。 そのような作業が行われることがローカル5Gサービスの運用管理者や利用者に知らされていないと、現場で通信が途絶したり不正使用されたりしていると誤認され、セキュリティインシデントが発生しているかどうかを調査するためにシステム停止可否の検討を行う必要が生じるなど、混乱を招く恐れがある。 また、マルウェアに感染した機器が持ち込まれて、ローカル5Gにつながる機器や装置に無線や有線で接続されると、ローカル5Gを利用している他の機器・装置・機械にマルウェアが感染する恐れもある。
対処策	ローカル5Gサービスが提供されるエリアへの機器の持ち込みや無線通信の利用ルールを、ローカル5Gサービスの事業者、運用者、利用者の間で予め取り決めておき、そのルールが守られているかどうかをチェックする必要がある。 具体的には、現場に機器を持ち込む場合には事前に運用管理者に届け出を行うこと、PCやタブレットなどを持ち込む場合はサイバーセキュリティ検査を受けること、通信機器の設定内容や設置場所を変更する場合は事前に運用管理者の承認を得ること、といったルールを定めて全ての従業員やパートナー企業に周知し、ルールが守られているかどうかを定期的に検査する、といった取り組みが有効である。

3.3.13 リモート管理の誤操作・誤設定による不具合やセキュリティホール

項目	項目の定義・説明
リスク内容	ローカル5Gの基地局やGWをリモート管理する機器の誤操作・誤設定により、不具合やセキュリティホールが発生し得る
脅威	その他
脆弱性	物理的脆弱性
NWのどこの箇所か	ローカル5G基地局
誰が対処すべきか	事業者
リスク概要	ローカル5Gの基地局を管理する事業者は、その設定状態や動作状態の確認や変更を迅速に行うために、ローカル5G基地局にリモートアクセスするための通信機器を設置して遠隔監視・遠隔保守をすることが想定される。 そのリモートアクセス用の通信機器についてセキュリティ脆弱性や設定誤り、誤操作が存在した場合、外部からの不正アクセスやマルウェア感染等により、ローカル5G基地局の安全や安定的な運用が脅かされるリスクがある。
対処策	ローカル5Gでつながる基地局やゲートウェイや端末機器をリモートで監視・保守する必要がある場合は、リスクアセスメントを適正に行い、リモート監視用の通信機器やネットワーク、業務運用プロセスに適切なセキュリティ管理策を導入する必要がある。 具体的には、IDパスワードだけでなく多要素の認証を用いたり、インターネットではなく閉域ネットワークで接続するようにしたり、セキュリティインシデントを早期に検知できるツールを導入したりする方法が考えられる。

４．ローカル5Gのセキュリティ強化に向けた提言、さらなる課題

これまでに紹介したように、ローカル5Gは新たなサービスやソリューションを生み出す強力なツールとして期待されているが、その利用においては適切なセキュリティ対策が同時に求められる。3章に述べたセキュリティ脅威とその対策は、ローカル5Gを利用するにあたってリソースの許す範囲内で適用を検討することを強く推奨する。

もちろん、予算やセキュリティ人材の有無など種々の制限により、必要なセキュリティ対策が実施出来ない可能性がある。その場合は、利用者および事業者の双方が「残存リスク」としてしっかりと認識し、万が一インシデントが発生した際には速やかに問題切り分け・対応が出来るよう、平素より体制を構築するべきである。

いっぽう、サービス・システムの内容から検討がそもそも不要なセキュリティ脅威があることも考えられる。無駄な投資を回避するためにも、利用者・事業者が協力して必要なセキュリティ対策は何であるかを企画段階・設計段階から十分に議論することは重要である。システムのリスクを洗い出す方法としてはISO 27001など長年に渡って利用されているスキームがあるので活用されたい。言うまでもなく、システム・ソリューションにはローカル5G以外の要素も組み込まれており、それら要素におけるセキュリティ脅威の洗い出し・対策も必要であることを付記しておく。

なお、本ガイドラインを作成したICT-ISAC「5Gセキュリティ推進グループ」では、3章に示したセキュリティ脅威の他にも、様々なセキュリティ脅威をリストアップしている。今後、本ガイドラインを充実化するにあたり脅威および対策を追加していく予定である。

５．結言

本ガイドラインは、今後普及が見込まれるローカル5Gが安心して利用できるよう、重要と考えられるセキュリティ脅威とその対策について述べた。ローカル5Gは、これまでのITシステムをより高度にすることで社会に新たな価値を与える、有望な技術である。しかしながら同時に新たなセキュリティ脅威をも引き起こしかねない。これらセキュリティ脅威を適切に事前対処することにより、ローカル5Gを活用した様々なサービスが安全に提供され、そして社会がもっと豊かに、かつ便利になることであろう。本ガイドラインがその一助になれば幸いである。

謝辞：

本ガイドラインの作成にあたり、3.2節で紹介したアンケートを実施しました。なによりも先ず、アンケートにご回答いただいた全ての方々に感謝申し上げます。年末年始の多忙な時期にもかかわらず詳細にご回答いただけたことで、私どもはタイムリーに事情を知ることができました。

また、アンケート実施において様々な企業に声がけをしていただいた方々につきましても感謝申し上げます。多くのアンケート結果を得ることが出来たのは、みなさまのおかげです。

3.1.1節の仮説ストーリーに用いた情報は、奈良先端科学技術大学院大学先端科学技術研究科の門林雄基教授から使用を許可いただきました。厚く御礼申し上げます。

そして、本ガイドラインの草稿段階からコメントをしていただいた全てのみなさま、本当にありがとうございました。

Appendix：脅威、および脆弱性の分類

3.3節「利用において検討すべき点」では、それぞれのリスクの脅威および脆弱性について分類した。本ガイドラインにおいてはSTRIDEの分類法をベースに一部修正して作成している。具体的には、以下の通りである：

脅威

なりすましによる不正ログイン

データの改ざん

特定の脆弱性によるDoS

外部要因による通信品質劣化

脆弱性による特権昇格

盗聴

盗難

情報漏洩

その他（遠隔保守からの不正侵入）

脆弱性

物理的脆弱性

システム脆弱性

人的・環境的脆弱性

執筆者一覧：

敬称略、五十音順

植田　広樹（主査）	NTT
上原　道宏	ICT-ISAC
榎　佳紀	トレンドマイクロ
小野寺　充	東陽テクニカ
窪田　歩（副主査）	KDDI総合研究所
境野　哲	NTTコミュニケーションズ
篠原　一人	東陽テクニカ
善宝　弾	KDDIデジタルセキュリティ
津金　英行	トレンドマイクロ
名和　利男	サイバーディフェンス研究所
西川　寛一	トレンドマイクロ
原　聖樹	トレンドマイクロ
引地　信寛	ICT-ISAC
増田　浩代	富士通
山路　洋史	東陽テクニカ
横田　孝弘	KDDI

参考文献：

[1]「ローカル5G免許申請支援マニュアル 2.02版」、第5世代モバイル推進フォーラム地域利用推進委員会、2021年5月10日、https://5gmf.jp/case/4484/
[2]「ローカル５Ｇ導入に関するガイドライン」、総務省、2022年3月改定、https://www.soumu.go.jp/main_content/000804382.pdf
[3]「新たな周波数のローカル5G用の無線局免許申請受付開始」、総務省、2019年12月、https://www.soumu.go.jp/soutsu/kanto/press/2020/1218r1.html
[4]「ローカル5Gセキュリティ対策に関するアンケート結果(概要版)の公開について」、ICT-ISAC、2020年3月15日、https://www.ict-isac.jp/news/news20210315.html
[5]「５Ｇ・ローカル５Ｇの普及・高度化に向けた取組」、総務省 総合通信基盤局 電波部 移動通信課　新世代移動通信システム推進室、2020年10月、
https://www.soumu.go.jp/main_content/000716749.pdf
[6]「ローカル５Ｇの申請者及び免許人一覧 事業者」、総務省 GO!5Gサイト、https://go5g.go.jp/about5g/
[7]「ローカル5G開発実証成果報告書」、総務省 GO!5Gサイト、https://go5g.go.jp/carrier/l5g/
[8]「NTTドコモ　テクニカル・ジャーナル VOL.25 NO.3」、NTTドコモ、https://www.nttdocomo.co.jp/binary/pdf/corporate/technology/rd/technical_journal/bn/vol25_3/vol25_3_003jp.pdf
[9]「総務省におけるローカル５Ｇ等の推進」、総務省、https://www.soumu.go.jp/main_content/000739007.pdf
[10]「ローカル５Ｇの概要について」、総務省、https://www.soumu.go.jp/main_content/000644668.pdf