ローカル5Gセキュリティガイドラインの概要

5Gセキュリティ推進グループ

ICT-ISAC

2022.3.31

ガイドラインの背景と目的

背景

- 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。
- 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。

目的

- 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。
- 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。
- 本ガイドラインが、ローカル5Gの普及・導入・利活用・保守に係る様々な方に参照いただき、少しでも貢献することが出来れば望外の喜びである。

読者層、利用方法

想定する読者層

- 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。
- 「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。

本ガイドラインの利用方法

- ローカル5G利用において重要と思われるセキュリティリスクを記載。
- リスク毎に、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説明している。
- また、それぞれのリスクに対処すべきは「事業者」か「利用者」のどちらかを明示している（双方で対処するべきリスクも存在する）。
- 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。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。

リスク一覧（1）

項番	脅威	誰が対処すべきか		リスク内容
		事業者	利用者	
3.3.1	なりすましによる不正ログイン	○		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
3.3.2	なりすましによる不正ログイン	○	○	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
3.3.3	データの改ざん	○		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)
3.3.4	特定の脆弱性によるDoS	○		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
3.3.5	特定の脆弱性によるDoS	○		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
3.3.6	外部要因による通信品質劣化	○	○	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

リスク一覧（2）

項番	脅威	誰が対処すべきか		リスク内容
		事業者	利用者	
3.3.7	盗難	○		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
3.3.8	盗難	○		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
3.3.9	盗難	○	○	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
3.3.10	その他（ログの削除）	○	○	ログが削除され、不正侵入に気づかない
3.3.11	その他（マルウェア感染。踏み台）	○	○	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
3.3.12	その他	○	○	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
3.3.13	その他	○		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

ローカル5Gセキュリティ対策の普及に向けて・・・

本ガイドラインにつきまして
ご質問、ご要望などございましたら、以下の連絡先までお送りください。

ICT-ISAC 事務局
担当：上原、引地
https://www.ict-isac.jp/contact/