ネットワーク事業者向けIoTセキュリティガイドライン

ネットワーク事業者向け IoT セキュリティ ガイドライン

バージョン 2.0

2017 年 10 月 31 日

本文書は GSMA の拘束力のない恒久参照文書です。

セキュリティ区分： 公開可能

本文書の入手および配布は、セキュリティ区分で認められた者に限られます。本文書は GSM の機密文書であり、著作権保護が適用されます。本文書はその提供目的のためにのみ使用されるものとし、本文書の全部もしくは一部の情報を、GSM の書面による事前の承認なくセキュリティ区分によって認められている者以外に開示する、またはそれ以外の方法で利用可能にすることを禁じます。

著作権表示

免責事項

GSM Association（GSMA）は、本文書に記載する情報の正確性、完全性または適時性について、（明示、黙示を問わず）一切の表明、保証または約束を行わないものとし、それらに対する責任を本免責事項によって放棄します。本文書の情報は予告なしに変更されることがあります。

反トラスト法上の通知

本文書の情報は、GSM Association の反トラスト法コンプライアンス方針を全面的に遵守しています。

目次

1 はじめに

1.1 概要

本文書では、IoT サービス提供者にサービスを提供して、システムのセキュリティおよびデータのプライバシーの確保を担うネットワーク事業者に向けたトップレベルのセキュリティガイドラインを提供します。推奨事項に関しては、今日展開されており、容易に利用できるシステムおよび技術に基づいています。

1.2 文書の構成

本文書は、ネットワーク事業者および IoT サービス提供者向けの文書です。本文書の読者は、下記に示す GSMA の IoT セキュリティ ガイドラインの文書群[11]にある他の文書を読むことに関心を寄せるかもしれません。

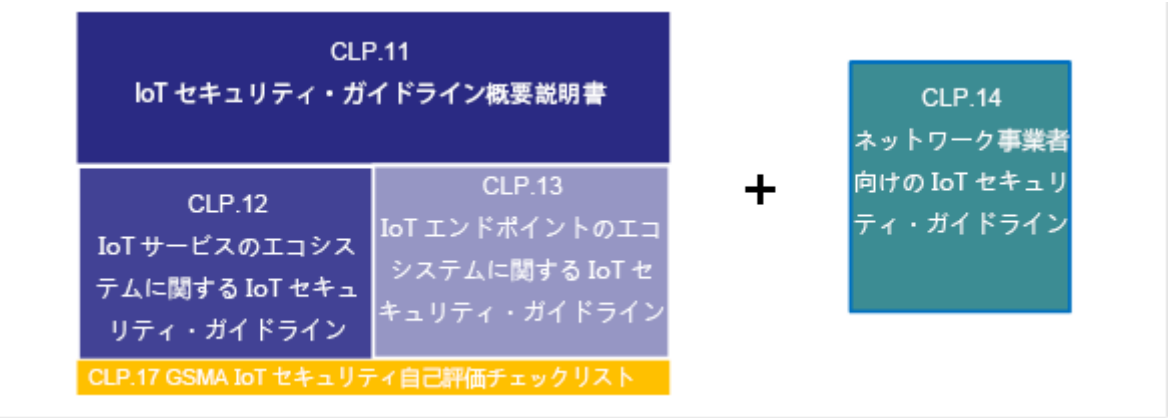


図1 - GSMA IoT セキュリティ ガイドライン文書群の構成

1.3 文書の目的および範囲

本文書は、IoT サービス提供者およびそのネットワーク事業者のパートナーとの間で交わすサプライヤー契約のチェックリストとして機能します。

本文書の範囲は次の内容に限定されています。

- IoT サービスに関連するセキュリティ ガイドライン。
- ネットワーク事業者が提供するセキュリティサービスに関する推奨事項。
- セルラーネットワーク技術。

本文書は、新たな IoT 仕様や標準の作成を意図したものではなく、現時点で利用可能なソリューション、標準、ベストプラクティスを示すものです。

本文書には、既存の IoT サービスの陳腐化を加速させる意図はありません。ネットワーク事業者の既存 IoT サービスとの下位互換性は、安全性が適切に保証されていると見なされる場合は維持する必要があります。

本文書は、IoT サービスプラットフォームがエンドユーザー（たとえば、スマートフォンや PC アプリケーションを介してエンドユーザーとデータを共有すること）やエコシステム内の他のエンティティとデータを共有するための IoT サービスプラットフォーム（または IoT コネクティビティ管理プラットフォーム）上に実装されているインターフェイスおよび API に関連するセキュリティ問題については取り扱いません。前述したインターフェイスおよび API は、「ベストプラクティス」のインターネットセキュリティ技術およびプロトコルを利用して保護される必要があります。

特定地域の国内法令および規則を遵守することによって、本文書のガイドラインが無効となる場合がありますのでご注意ください。

1.4 想定読者

本文書の主な対象読者は次の通りです。

- 第一に、IoT サービス提供者にサービスを提供したいと考えているネットワーク事業者。
- 第二に、固定回線ネットワークのセルラーを利用して新しい革新的な接続製品およびサービス（いわゆる「モノのインターネット」）の開発を目指している企業や組織。本文書では、これらの企業を「IoT サービス提供者」と呼びます。

1.5 用語の定義

用語	説明
デバイスホストによるレポートの識別	エンドポイントデバイスがネットワーク事業者にホスト情報を報告する機能。GSMA Connection Efficiency Guidelines[17]を参照してください。
Diameter（ダイアメーター）	Diameter（ダイアメーター）とは、コンピューターネットワークの認証、承認、および会計プロトコルです。IETF RFC 6733 [18]を参照してください。

用語	説明
エンドポイント	IoT エンドポイントとは、インターネット接続された製品やサービスの一部として機能またはタスクを実行する物理コンピューティングデバイスです。IoT デバイスの一般的な 3 つのクラスに関する説明、およびエンドポイントの各クラスの事例については、CLP.13 [29]のセクション 3 を参照してください。
ゲートウェイ	複雑なエンドポイントデバイスで、通常は軽量エンドポイントデバイス（ローカルネットワークを経由で接続）とワイドエリアネットワーク間をブリッジします。詳細については、CLP.13 [29]を参照。
モノのインターネット	モノのインターネットとは、複数のネットワークを通じてインターネットに接続された様々なマシン、デバイス、器具が連動して動作することを指します。これらのデバイスには、タブレットや家電製品などの日用品のほか、データの送受信ができる通信機能を備えた車両、モニター、センサーなどのマシンが含まれます。
IoT 接続管理プラットフォーム	通常はネットワーク事業者がホストするシステムで、IoT サービス提供者による IoT サブスクリプションと料金プランの自己管理を可能にします。
IoT サービス	サービスを実行するために IoT デバイスからのデータを利用するコンピュータープログラム。
IoT サービスプラットフォーム	IoT サービス提供者がホストするサービスプラットフォームで、エンドポイントに通信して IoT サービスを提供します。
IoT サービス提供者	新たに革新的な接続機能を備えた IoT 製品やサービスを開発しようとしている企業または組織。提供者がネットワーク事業者になる可能性があります。
軽量エンドポイント	通常は、制約されたデバイス（センサーやアクチュエータなど）で、ゲートウェイデバイスを経由して IoT サービスに接続します。
ネットワーク事業者	IoT エンドポイントデバイスを IoT サービスプラットフォームに接続する、通信回線のオペレーター。
UICC	ETSI TS 102 221（欧州電気通信標準化機構の技術仕様）に規定されている、暗号が異なるセキュリティドメインにおいて複数の標準化されたネットワークまたはサービスの認証アプリケーションをサポートすることができる、セキュアエレメントのプラットフォーム。ETSI TS 102 671 に規定されている埋め込み式要素に埋め込まれることがある。
ワイドエリアネットワーク	広範な地理的距離にわたって広がっている電気通信ネットワーク。

1.6 略語

用語	説明
3GPP	第 3 世代プロジェクト パートナーシップ
AKA	認証および鍵合意
APDU	アプリケーションプロトコルデータユニット
API	アプリケーションプログラミングインターフェイス
APN	アクセスポイント名
BGP	ボーダーゲートウェイプロトコル
CEIR	中央機器識別登録
CERT	コンピューター緊急対処チーム
DNS	ドメインネームシステム
DoS	サービス拒否
DPA	データ処理契約
EAB	拡張アクセス制限
EAP	拡張認証プロトコル
EID	eUICC 識別
ETSI	欧州電気通信標準化機構
EU	欧州連合
eUICC	埋め込み UICC
FASG	不正およびセキュリティグループ
GCF	グローバル認証フォーラム
GGSN	ゲートウェイ GPRS サポートノード
GPRS	汎用パケット無線サービス
GRX	GPRS ローミングエクスチェンジ
GSM	移動体通信用のグローバルシステム
GSMA	GSM Association
GTP	GPRS トンネリングプロトコル

用語	説明
HLR	ホームロケーションレジスタ
HSS	ホーム加入者サーバー
ICCID	集積回路カード識別番号
IMEI	国際移動体装置識別番号（端末識別番号）
IMSI	国際移動体加入者識別番号
IoT	モノのインターネット
IP	インターネットプロトコル
IPSec	インターネットプロトコルセキュリティ
L2TP	レイヤ 2 トンネリングプロトコル
LBO	ローカルブレイクアウト
LPWAN	低電力ワイドエリアネットワーク
LTE	ロングタームエヴォリューション
M2M	マシンツーマシン
MAP	モバイルアプリケーションパート
MME	モビリティ管理エンティティ
OMA	Open Mobile Alliance
OSS	オペレーションサポートシステム
OTA	無線通信を経由して
PTCRB	当初は PCS Type Certification Review Board の頭文字を繋いだものですが、現在では適用されません。
RAN	無線アクセスネットワーク
SAS	セキュリティ認証制度
SGSN	サービス GPRS サポートノード
SIM	加入者識別モジュール
SMS	ショートメッセージサービス
SoR	ローミングのステアリング
SS7	信号システム No. 7

用語	説明
UMTS	ユニバーサル移動体通信サービス
USSD	非構造付加サービスデータ
VLR	ビジターロケーションレジスタ
VPN	バーチャルプライベートネットワーク
VoLTE	ボイスオーバーLTE
WAN	ワイドエリアネットワーク

1.7 参考文献

参照	文書番号	タイトル
[1]	ETSI TS 102 225	Secured packet structure for UICC based applications www.etsi.org
[2]	ETSI TS 102 226	Remote APDU structure for UICC based applications www.etsi.org
[3]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application www.3gpp.org
[4]	該当なし	Open Mobile API specification www.simalliance.org
[5]	OMA DM	OMA Device Management www.openmobilealliance.org
[6]	OMA FUMO	OMA Firmware Update Management Object www.openmobilealliance.org
[7]	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification www.gsma.com
[8]	ETSI TS 102 310	Extensible Authentication Protocol support in the UICC www.etsi.org

参照	文書番号	タイトル
[9]	3GPP TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode www.3gpp.org
[10]	NISTIR 7298	Glossary of Key Information Security Terms www.nist.gov
[11]	GSMA CLP.11	IoT Security Guidelines Overview Document https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[12]	該当なし	Introducing Mobile Connect – the new standard in digital authentication https://www.gsma.com/identity/mobile-connect
[13]	3GPP TS 34.xxx	3GPP 34 series specifications www.3gpp.org/DynaReport/34-series.htm
[14]	3GPP TS 37.xxx	3GPP 37 series specifications www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	3GPP 31 series specifications www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	Security Accreditation Scheme for UICC Production http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	IoT Device Connection Efficiency Guidelines https://www.gsma.com/iot/iot-device-connection-efficiency-guidelines/
[18]	IETF RFC 6733	Diameter Base Protocol www.ietf.org
[19]	ETSI TS 102 690	Machine-to-Machine communications (M2M); Functional architecture www.etsi.org
[20]	TR-069	CPE WAN Management Protocol www.broadband-forum.org

参照	文書番号	タイトル
[21]	該当なし	OpenID Connect openid.net/connect/
[22]	該当なし	FIDO (Fast IDentity Online) Alliance fidoalliance.org/
[23]	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface www.etsi.ord
[24]	該当なし	National Institute of Standards and Technology (NIST) www.nist.gov
[25]	該当なし	European Network of Excellence in Cryptology (ECRYPT) www.ecrypt.eu.org
[26]	GSMA CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[27]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) tools.ietf.org/html/rfc5448
[28]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) tools.ietf.org/html/rfc4186
[29]	GSMA CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[30]	該当なし	Wireless Security in LTE Networks www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	該当なし	oneM2M Specifications www.oneM2M.org
[32]	GSMA CLP.17	IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/

参照	文書番号	タイトル
[33]	該当なし	LPWA Technology Security Comparison. A White Paper from Franklin Heath Ltd https://goo.gl/JIOlr6
[34]	CLP.28	NB-IoT Deployment Guide www.gsma.com/iot
[35]	CLP.29	LTE-M Deployment Guide www.gsma.com/iot
[36]	3GPP TS33.163	Battery efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) www.3GPP.org

2 ネットワーク事業者が保護できる IoT サービス資産

IoT サービス資産を適切に保護する上で実装すべきセキュリティ機能は、各サービスに固有のものです。したがって、適切なリスクおよびプライバシーの影響評価プロセスを利用して、セキュリティに関する具体的なニーズを引き出すのは依然として、IoT サービス提供者の責任です。ネットワーク事業者および IoT サービス提供者は、同様のセキュリティ要件を共有して資産を保護することが多いため、重複した（冗長性のある）セキュリティインフラストラクチャを実装するのではなく、一般的なセキュリティソリューションを活用することは理にかなっています。さらに、多くの場合、ネットワーク事業者は IoT サービス提供者でもあります。

ネットワーク事業者が提供するセキュリティサービスは、IoT サービスを提供する際に利用する資産を保護する上で重要な役割を果たします。これらには次の内容が含まれます。

- IoT エンドポイントデバイスと IoT サービスプラットフォーム間で送信される IoT サービスデータ。これには、直接影響のあるプライバシーセンシティブなデータ（エンドユーザー関連のデータなど）と、プライバシーに関する二次的な影響も及ぼす可能性のある、商業的に利用できるデータ（アクチュエータ制御データなど）の両方が含まれます。
- エンドポイントデバイス（ゲートウェイデバイスを含む）内で利用されるセキュリティ資産（IMSI、キーセットなど）およびネットワーク構成設定（APN、タイマー値など）。
- 商標の評判、企業の責任下にある顧客やユーザーのデータ、戦略情報、財務データ、健康記録など、IoT サービス提供者の企業秘密情報。
- IoT サービス提供者のビジネスインフラストラクチャ、サービスプラットフォーム、企業ネットワークおよびその他プライベートネットワークの要素。
- ネットワーク事業者が提供し、IoT サービスで使用する公開用（つまり共有）データセンターのインフラストラクチャ。これには、公共サービス、ホストされた機能、仮想化インフラストラクチャ、クラウドの設備などが含まれます。
- 通信ネットワークインフラストラクチャには、無線アクセスネットワーク、コアネットワーク、バックボーンネットワーク、基本的なサービス機能（DNS、BGP など）、固定ネットワークおよびセルラーネットワークへのアクセスおよび集約などが含まれます。

3 ネットワークセキュリティの原則

適切かつ信頼性の高いセキュリティ機構は、ネットワーク事業者が自身のネットワーク内で実装する必要があります。

このセクションでは、ネットワークが IoT エコシステム内でどのように価値を提供できるかについて説明します。

通信ネットワークが提供する最も基本的なセキュリティ機構は次のとおりです。

- IoT サービスに関わるエンティティ（つまり、ゲートウェイ、エンドポイントデバイス、ホームネットワーク、ローミングネットワーク、サービスプラットフォーム）の識別および認証。
- IoT サービスを考案するために接続する必要のあるさまざまなエンティティへのアクセス制御。
- IoT サービスのネットワークが処理する情報のセキュリティ（機密性、整合性、可用性、信頼性）およびプライバシーを保証するためのデータ保護。
- ネットワークリソースの可用性を保証し、攻撃から保護するためのプロセスおよびメカニズム（たとえば、適切なファイアウォール、侵入防止およびデータフィルタリング技術など）

3.1 ユーザー、アプリケーション、エンドポイントデバイス、ネットワークおよびサービスプラットフォームにおける安全な識別。

識別は、IoT サービス内のエンティティに一意の識別子を提供し、これらの電子 ID を実世界の法的拘束力のある ID との関連付けから構成されます。

移動体通信に接続された IoT サービス内において、エンドポイントデバイスは IMSI および/または IMEI（EID は eUICC を備えたデバイスにも使用可能）を用いて識別されます。ネットワークは、ネットワークコードと国コードを用いて識別されます。ID を提供する各方法は、それに関連付けられている安全保証のレベルが異なります。

安全な認証はセキュリティで保護された ID に基づいてのみ実現できるため、ID は認証プロセスにおいて重要な役割を果たします。したがって、IoT サービス内で発行して使用される ID（たとえば、IMSI、IMEI または ICCID）が不正改造、偽装または盗難から安全に保護されることが不可欠です。

IoT サービス提供者が直面する可能性のある実務上の問題の 1 つは、IoT サービスが多くの IoT サービスプラットフォームとの通信を必要とする可能性があり、それぞれが個別の一意な識別を必要とする可能性があることです。各 IoT サービスプラットフォームへの通信リンクを確立する上で使用される各 ID は、IoT サービスが安全にプロビジョニングして、格納し、管理する必要があります。

IoT サービスに対して適切な場合、ネットワーク事業者は、エンドポイントデバイスを安全に識別する UICC ベースのメカニズムを使用することを推奨します。ネットワーク事業者は、UICC が提供する安全なストレージ機能を IoT サービス提供者に拡張して、追加した IoT サービスに関連する ID を UICC 上に格納させることもできます。この手法は、移動体通信のエンドポイントデバイスおよび移動体通信以外のエンドポイントデバイス（EAP-AKA [27]など）の両方に適用できます。

ネットワーク事業者は「シングルサインオン」サービスも提供でき、エンドポイントデバイスが ID を一旦確立して証明し、その後、不便さを感じることなく、いくつかの IoT サービスにプラットフォームに接続できます。このようなサービスを利用する上でのセキュリティに関するトレードオフやリスクは、複数のプラットフォームにわたって考慮する必要があります。

3.2 ユーザー、アプリケーション、エンドポイントデバイス、ネットワークおよびサービスプラットフォームにおける安全な認証。

NIST [10]によると、「認証」とは多くの場合、「情報システムのリソースへのアクセスを許可する前提条件として、ユーザー、プロセス、またはエンドポイントデバイスの ID を検証する」ことです。

ネットワーク事業者は、IoT サービスに関連付けされたユーザー、アプリケーション、エンドポイントデバイス、ネットワークおよびサービスプラットフォームが確実に認証されるようにサービスを提供できます。

認証には関連する否認不可のプロパティがあります。NIST [10]による否認不可の定義は次のとおりです。「情報の送信者に配信証明が提供され、受領者に送信者の身元証明が提供されているので、いずれも後で情報の処理を拒否できないことを保証すること。」否認不可は、トランザクションやメッセージのソースを特定する際に、信頼性が侵害されていないことをアサートすることに依存します。

3.3 安全な通信チャネルの提供

ネットワーク事業者は、広域の移動体通信ネットワークおよび固定ネットワーク向けの通信セキュリティメカニズムを提供して、「クラス最高の」通信の整合性、機密性および信頼性を再保証します。ネットワーク事業者は、必要に応じて仮想プライベートネットワーク（VPN）と暗号化されたインターネット接続を用いて企業ネットワークに安全な接続を提供して管理することができます。

安全な通信チャネルの目的は、チャネルを経由して送信されるデータが、データ主体の知識や同意なしに処理、使用、または送信されないことを保証することです。暗号化技術は、機密性、整合性および信頼性の特性を保証することにより、安全なデータ送信で重要な役割を果たします。暗号化は、軽量エンドポイン

ト、ネットワークの側面（衛星バックホールの制約など）、および提供されるサービスを考慮して設計および展開されるシステムに対して適切でなければなりません。

ネットワーク事業者は、IoT サービス提供者にデータ暗号化サービスを提供して、通信の整合性とネットワークの回復性を確保することができます。

従来、ネットワーク事業者は公衆通信のインフラストラクチャまたはパブリックまたはプライベートネットワークインフラストラクチャを混合したものを提供しています。多くのネットワーク事業者は、パブリックネットワークインフラストラクチャを通過する顧客/ユーザーデータが、パブリックネットワークインフラストラクチャに入るポイントとネットワークから離れるポイントとの間で暗号化されるようにすることができます。必要に応じて、ネットワーク事業者は IoT サービス提供者を支援して独自の暗号化資格情報を展開または抽出して、ネットワーク事業者のインフラストラクチャ経由での通過中に IoT データの機密性を保証することもできます。

ネットワーク事業者は、顧客に単一顧客向けの専用通信チャネルを提供するプライベートネットワークを提供でき、インターネットなどのパブリックネットワークを通過するデータがないことを保証できます。このようなプライベートネットワークは次の方法で作成することができます。

1. レイヤ 2 トンネリングプロトコル（L2TP）などのトンネリングプロトコルを使用し、インターネットプロトコルセキュリティ（IPsec）などのプロトコルを使用してセキュリティを保護する方法。または
2. たとえば BEST [36]を用いて UE とアプリケーションサーバー間のエンドツーエンドのセキュリティを顧客に提供する方法。または
3. 下記に示す例のように、共有無線ネットワークでコアネットワークの個別インスタンスを展開することで、IoT サービス専用のネットワークを作成する方法。

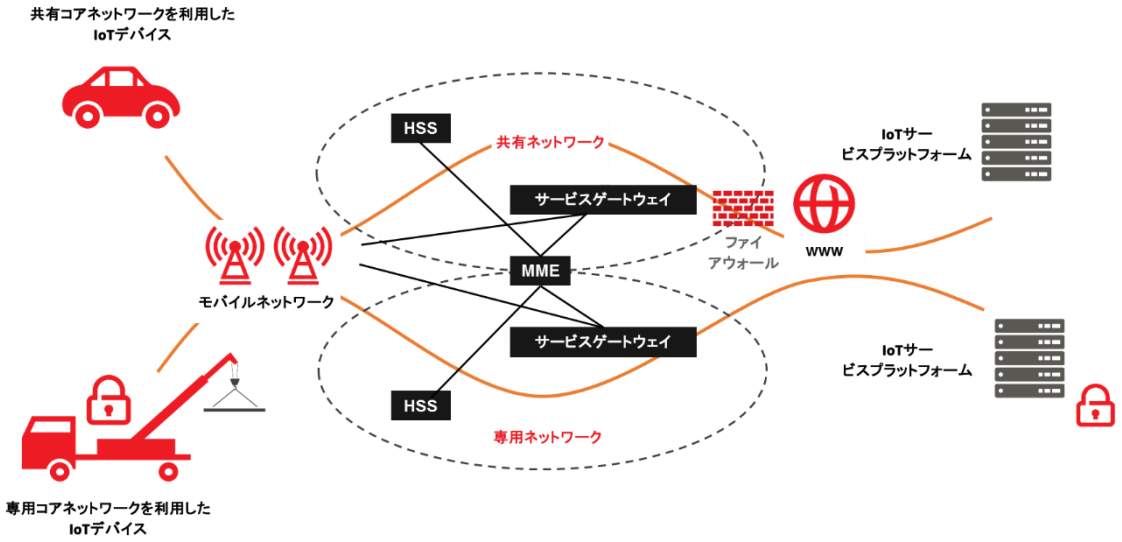


図2 - プライベートネットワーク構成の例

3.4 通信チャネルの可用性確保

NIST [10]による「可用性」とは、承認されたエンティティの要求に応じてアクセスでき、使用可能であるという特性です。

ネットワーク事業者は、利用可能なネットワークを IoT サービス提供者に提供することができます。ネットワークの可用性を実現する上で、ネットワーク事業者が提供する最も基本的なメカニズムは次のとおりです。

3.4.1 認可されたスペクトルの使用

GSMA ネットワーク事業者のメンバーは、各国の規制当局が発行したライセンスの条項に基づいて認可された専用のスペクトルを用いてネットワークを運用します。このスペクトルを不正に使用すると起訴の対象となりますが、認可されたスペクトルを使用することにより、他の無線技術からの干渉を最小限に抑えます。ネットワーク事業者は国内の規制当局とともに、無許可の干渉源を探し出して、ネットワークの可用性に影響を与えないようにします。

許可されたスペクトルを使用することにより、ネットワークを運用するための専用無線帯域をネットワーク事業者に提供し、ネットワーク事業者はネットワークのサービスエリアと容量の計画立案を慎重に行い、顧客に対するネットワークの可用性を最大限に確保できるようにします。

3.4.2 実績のある標準ネットワーク技術の実装

GSMA のネットワーク事業者メンバーは、3GPP などの標準化団体が規定する GSM、UMTS、LTE などの標準ネットワーク技術を実装しています。標準化された技術を使用することにより、ネットワーク事業者間の

相互運用性が保証されるだけでなく、標準化がその技術の堅牢性を確保するために、その作成中に最大限の精査の対象になることも保証します。

3.4.3 テスト済みの認定ネットワーク技術の実装

ネットワーク事業者が保有するネットワーク部品の多くは、国際的な試験規格に従ってテストが行われ、認定されます。複雑なエンドポイントデバイスおよびそれに含まれる通信モジュールは、GCF、PTCRB、およびネットワーク事業者の承認テストを通じて、3GPP の検査規格[13]の対象となります。無線アクセスネットワーク（RAN）は、ネットワーク事業者の承認テストを通じて、3GPP の検査規格[14]の対象となります。UICC は、ネットワーク事業者の承認テストを通じて 3GPP の検査規格[15]の対象となり、さらに GSMA SAS 認定[16]の対象となることがあります。

3.4.4 回復性のあるネットワークトポロジおよび構成

ネットワーク事業者は、必要な地理的冗長性と分離を実装、構築する回復性のあるネットワークを提供して、最小限に抑えたダウンタイムで最大限の可用性を確保します。厳格なサービス品質とサービスレベル契約が確実に満たされるように、すべてのネットワーク要素は慎重に構成され、監視されます。

3.4.5 ネットワークリソースのリアルタイム監視および管理

ネットワーク事業者は、ネットワークトラフィックを管理し、ネットワークの需要に対応し、障害を修正するために、ネットワークの性能を 24 時間 365 日、リアルタイムで監視する最先端のネットワーク運用センターを実装しています。追加情報は、セクション 4.10 をご覧ください。

3.4.6 脅威管理および情報共有

GSMA の不正およびセキュリティグループ（FASG）は、すべてのネットワーク事業者が詐欺やセキュリティインテリジェンス、およびインシデントの詳細をタイムリーかつ責任が取れる方法で共有できる、オープンで受容力があり、信頼できる環境を提供しています。グループは、グローバルな詐欺やセキュリティの脅威に関する状況を評価し、ネットワーク事業者とその顧客に関連するリスクを分析し、適切に緩和させるアクションを定義して優先順位を付けます。

3.4.7 ローミングサービス

標準ネットワーク、エンドポイントデバイス技術、相互接続サービスを使用することにより、ネットワーク事業者はネットワークローミングサービスを提供し、顧客に向けて、ネットワークのサービスエリアと可用性をさらに向上させることができます。

3.4.8 エンドポイントデバイスの性能監視および管理

ネットワーク事業者は、ネットワークに接続するエンドポイントデバイスの性能を測定して、過度の無線干渉（国内規制に準拠していないなど）を生み出すエンドポイントデバイスや、ネットワーク信号トラフィック（GSMA Connection Efficiency Guidelines [17]に準拠していないなど）で同様にネットワーク全体の性能を低下させる可能性のあるエンドポイントデバイスを隔離することができます。したがって、異常な動作が検出されると、エンドポイントデバイスを監視したり、切断したり、ファームウェアを更新したりすることができます。

4 プライバシーの検証

IoT が提供する機会を実現するには、IoT サービスを提供してデータを収集している IoT サービス提供者を消費者が信頼することが重要です。GSMA とそのメンバーは、ユーザーが自分のプライバシーが適切に尊重され保護されていると思う場合にのみ、消費者の自信と信頼が完全に達成されると信じています。

世界中ですでに確立したデータ保護およびプライバシー法があり、ネットワーク事業者に適用され、遵守されています。事業者は、IoT サービスおよび技術という観点から、プライバシーに関するニーズに対処するために、既存のデータ保護規制および原則を適用することは可能であると考えています。

しかし、IoT サービスは通常、IoT サービス提供者のパートナーと一緒に作業する事業者を対象としています。IoT サービスに関する規制の明確性と法律の確実性が存在すること、そしてプライバシーとデータ保護に関する規制がサービスと技術に中立な方法ですべての IoT サービス提供者に一貫して適用されることが重要です。

ネットワーク事業者は、何らかの方法でデータを処理する場合、IoT サービス提供者と「データ処理契約（DPA）」を締結する必要があることを認識する必要があります。特定の IoT サービス向けに策定するデータ保護およびセキュリティプラクティスには、個人のプライバシーに対する全体的なリスクと、その個人に関するデータが収集、配布および使用されるという状況を反映する必要があります。規制上の介入は、認識したリスクが現れ、そのリスクに対処するには既存の措置が不十分である領域に限定するべきです。たとえば、（TS-0003 [31]経由）oneM2M では、オペレーターはサービス提供者に代わり、プライバシーマネージャーの役割を果たすことができます。

ネットワーク事業者は、プライバシーとセキュリティに関する問題に取り組んだ豊富な経験を引き出して、IoT サービス提供者と協力して作業し、IoT 技術と消費者経験全体にプライバシーとセキュリティを組み込むことができます。このように協力することにより、IoT サービス提供者は提供するサービスに照らして、関連する消費者のプライバシーリスクを特定して緩和することができるようになります。

詳細については、「GSMA Mobile Privacy Principles」を参照してください。
http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 ネットワーク事業者が提供するサービス

ネットワーク事業者は、IoT サービス提供者に安全な移動体通信および固定のワイドエリアネットワーク（WAN）を提供することができます。

このセクションでは、IoT サービスをワイドエリアネットワークに接続する際のベストプラクティスな推奨事項について説明します。必要に応じて、推奨事項は使用する技術とは独立しますが、移動体通信やその他のネットワークタイプのベストプラクティスにも使用できます。

5.1 安全なサブスクリプション管理の手順

このセクションでは、ネットワーク事業者が IoT サービス提供者のサブスクリプションをどのように管理すべきかに関する推奨事項を説明します。

- ネットワーク事業者または IoT サービス提供者は、現在だけでなく将来でも IoT サービス（音声、データ、SMS など）を有効にするために必要とされるネットワークサービスの評価を実施する必要があります。
- ネットワーク事業者はこの評価を踏まえて、「最小特権の原則」に従って運用し、特定の IoT サービスに必要なサービスのみを IoT サービス提供者のサブスクリプションに設定する必要があります。
  例：
    - データベアラのみを使用する IoT サービスには、音声と SMS サービスをプロビジョニングべきではありません。
    - エンドポイントデバイスが既知の IoT サービスプラットフォームにのみ接続する場合、デバイスに関連付けられたサブスクリプションでは、IP アドレスの範囲（またはドメイン）で知られているホワイトリストへの接続のみを許可する必要があります。
    - IoT サービスが音声または SMS を使用する場合は、予め構成された固定ダイヤルリストの使用を検討する必要があります。

- ネットワーク事業者は、重要な IoT サービス（重要な医療サービスに関連するサブスクリプションなど）を有効にする IoT サブスクリプションに対して、安全なサブスクリプション管理のプロセスを実装する必要があります。これらのサービスを任意に切断すべきではありません。
- ネットワーク事業者は、従来のサービスを提供するために使用する従来の UICC から IoT サービス用の UICC を特定し、IoT サービス提供者が必要とする場合、これらを適切に分離する必要があります。
    - IoT サービスに使用する UICC が従来の「ハンドセット」用の UICC から分離されている場合、他の方法の場合よりもネットワーク事業者による関連するサブスクリプションの安全かつ効率的な管理に向けた基礎が提供されます。たとえば、ネットワーク事業者は、

寿命を延長させて、これらの UICC をかなり長時間（つまり長年）サポートするようにより良く構成されたエンドポイントデバイスに対して、個別の HLR/HSS を使用することを検討することができます。

5.1.1 UICC の供給および管理

5.1.1.1 UICC（OTA、無線通信を経由して）のリモート管理

一部のシナリオにおいて、IoT エンドポイントデバイスは物理的にアクセスできません。UICC への変更をリモートで実行できるようにするには、ネットワーク事業者が UICC OTA の管理をサポートする必要があります。UICC OTA のセキュリティメカニズムでは、最新の ETSI [1] [2]および 3GPP [3]の仕様に従って、IoT サービスに最も適しているレベルのセキュリティを使用する必要があります。

IoT エンドポイントデバイスは、UICC OTA コマンドの実行が確実に成功するために、UICC が認識する必要な APDU コマンドをサポートする必要があります。

5.1.1.2 取り外しができない UICC

ネットワーク事業者は、IoT エンドポイントデバイスが物理的な改ざんに対して脆弱である可能性があるとサービス脅威モデルが示唆している場合、IoT サービスに対して取り外しができない UICC（つまり、マシンフォームファクタ）を提供する必要があります。このような脅威を検出して対応できるようにするためには、追加のセキュリティ対策を適用する必要があります。

5.1.1.3 組み込み型 UICC（eUICC）のリモート管理

ネットワーク事業者は、エンドポイントデバイスを遠隔地またはたどり着くのが難しい場所に配置する必要がある IoT サービス用の取り外しができない UICC（つまり eUICC）の安全なリモート管理を提供する必要があります。

たとえば、IoT サービス提供者が所有者ではなく、容易にアクセスできないエンドポイントデバイス（たとえば自動車）に組み込まれた多くの eUICC を管理する必要のある IoT サービス提供者の場合など。

通常、事業者は IoT コネクティビティ管理プラットフォームを使用して、（e）UICC によって IoT デバイスに提供される通信サービスを監視および制御します。

ネットワーク事業者は、GSMA の「Remote Provisioning Architecture for Embedded UICC Technical Specification [7]」をサポートする必要があります。

5.1.1.4 UICC ベースのサービス

ネットワーク事業者は、IoT サービス提供者に UICC ベースのサービスを提供することができます。これにより、IoT サービス提供者は、IoT サービス用に安全で耐タンパー性のあるプラットフォームとして UICC を使用することができます。このような UICC ベースのサービスは通常、JavaCard™ で開発され、JavaCard™ に準拠したすべての UICC カード間で相互に運用することができます。IoT エンドポイントデバイス用のアプリケーションに関する例は、ネットワーク品質の監視および報告となることがあります。UICC プラットフォームが提供する耐タンパー性のある機能は、攻撃者が物理的にアクセスできる IoT エンドポイントデバイスにとって極めて重要です。すべての関係者にとって共通の安全な要素として UICC を活用することにより、安全な IoT エンドポイントデバイスをよりコスト効率のよいものにすることもできます。

UICC は、IoT サービス提供者が管理するセキュリティキーを含め、IoT サービス用機密データの耐タンパーストレージ用としても使用することができます。ETSI TS 102 225 [1]では、Global Platform Card Specification の Confidential Card Content Management を活用して、IoT サービス提供者が UICC 上で独自のセキュリティドメインを管理できるようにしています。

IoT サービス提供者またはネットワーク事業者は、UICC 内にこのようなセキュリティドメインを作成するよう、UICC サプライヤーに依頼することができます。UICC の発行者は適切なセキュリティキーで保護されていることを確認し、IoT エンドポイントデバイスはアクセスに必要な APDU コマンドを実行することができます。

さらに、UICC を用いて（安全に格納されているキーを用いて）暗号化して、IoT サービスに機密性の高い内容を送信したり、Open Mobile API [4]や oneM2M TS-0003 [31]などのサービスを経由してエンドポイントデバイスベースのアプリケーションにセキュリティサービスを提供したりすることもできます。

5.1.1.5 安全な UICC の製造およびプロビジョニング

ネットワーク事業者は、製造プロセスおよびプロビジョニングプロセスが GSMA の Security Accreditation Scheme (SAS) [16]に従っていると認定されている製造業者から UICC を調達する必要があります。

5.2 ネットワーク認証および暗号化アルゴリズム

このセクションでは、多様なワイドエリアネットワークのネットワーク認証およびリンク暗号化に関する推奨事項およびベストプラクティスについて説明します。

ネットワーク事業者は、IoT サービス提供者のエンドポイントデバイスが求める寿命を満たすネットワーク認証のアルゴリズムを実装する必要があります。

ネットワーク事業者は、USSD、SMS および IP データ接続など、IoT サービスが使用できる通信サービスを数種類提供します。本文書では、IP データ接続が IoT サービスで使用される通信サービスの中で最も利用されている形式なので、IP データ接続のみを説明します。

存在する多くの IoT サービスで USSD および SMS が使用されているため、USSD および SMS には、IP データ接続と比較して、セキュリティサポート機能が制限されていることを強調する価値があります。一般的に、USSD および SMS のトラフィックは、ネットワーク事業者と暗号化保護メカニズムが暗号で保護したデフォルトの「エンドツーエンド」ではないため、SMS メッセージに対して機密性と整合性は確保できません。USDD または SMS を通信に使用する IoT サービス提供者は、USDD および SMS に関連する脆弱性を認識し、可能であれば、サービス層で追加の暗号化を実装する必要があります。

5.2.1 GSM/GPRS（2G）システムのセキュリティ

GSM/GPRS ネットワークを提供するネットワーク事業者は次の内容を行う必要があります。

- 最低限 128 ビットの A5/3 ストリーム暗号を使用して、IoT エンドポイントデバイスとベースステーション間のリンクを保護します。可能であれば、ネットワーク事業者は A5/1 および A5/2、または暗号化されていないリンクの使用を避けてください。
- MILENAGE 認証アルゴリズムを使用します。ネットワーク事業者は COMP128-1 および COMP128-2 を避ける必要があります。ネットワーク事業者は、TUAK 認証アルゴリズムのサポートを考慮する必要があります
- 不正なベースステーションの攻撃に対処して緩和するために適切な措置を取ります。

GSM/GPRS システムでは、ネットワークはエンドポイントデバイスによって認証されず、デバイスのみがネットワークによって認証されます。したがって、GSM/GPRS システムを使用する場合は、サービス層でのエンドツーエンドの暗号化が推奨されます。IoT サービスとして提供されるソリューションでは、実際の処理、エンドポイントデバイスの制限、ネットワークの帯域幅の制約を考慮する必要があります。

GSM/GPRS システムでは、GRX ネットワーク上で作成される SGSN および GGSN 間の GTP トンネルは暗号化されません。ネットワーク事業者は、GRX ネットワークがプライベートネットワークとして管理されていることを保証することで、このリンクのセキュリティを確保する必要があります。

5.2.2 UMTS（3G）システムのセキュリティ

UMTS ネットワークでは相互認証が可能で、エンドポイントデバイスがネットワークによって認証されるだけでなく、ネットワークもデバイスによって認証されます。

UMTS ネットワークを提供するネットワーク事業者は、MILENAGE 認証およびキー生成アルゴリズムをサポートしなければなりません。ネットワーク事業者は、Kasumi の機密性と整合性の暗号化アルゴリズムをサポートする必要があります。

ネットワーク事業者は、TUAK 認証アルゴリズムのサポートを考慮する必要があります

5.2.3 LTE（4G）システムのセキュリティ

LTE ネットワークを提供するネットワーク事業者は、MILENAGE 認証アルゴリズムをサポートしなければなりません。ネットワーク事業者は、LTE EEA1、EEA2 または EEA3 の暗号化アルゴリズムをサポートする必要があります。

ネットワーク事業者は、TUAK 認証アルゴリズムのサポートを考慮する必要があります。

ネットワーク事業者は、GSMA ホワイトペーパー「Wireless Security in LTE Networks」[30]を見直すことを推奨します。

5.2.4 低電力ワイドエリアネットワークのセキュリティ

いくつかの低電力ワイドエリア（LPWA）ネットワーク技術は、さまざまなネットワーク事業者によって展開されています。LPWA ネットワーク展開状況の完全かつ最新の一覧は、GSMA のウェブサイトにあります。
www.gsma.com/iot

NB-IoT [34]および LTE-M [35]の展開ガイドは GSMA のウェブサイトにあり、ネットワークとデバイスの両方の観点からこれらの技術を一貫して確実に展開する上で役立ちます。

2017 年 5 月、情報セキュリティアナリストの Franklin Heath 氏が「LPWA Technology Security Comparison」[33]というタイトルで独立した報告書を発表し、その報告書では、スマート農業、スマート街灯、煙探知器、水道メーター、スマートメーターなど、一般的ないくつかの IoT のユースケースに関して、5 種類の低電力ワイド エリア（LPWA）ネットワーク技術のセキュリティ機能を比較・対比しています。認可されたスペクトル、LTE-M、NB-IoT および EC-GSM-IoT で動作する 3GPP 標準化モバイル IoT 技術のセキュリ

ティ機能はもちろんのこと、認可されていないスペクトル技術 LoRaWAN および Sigfox のセキュリティ機能も評価します。この報告書は次の URL からダウンロードできます。https://goo.gl/JIOlr6 [33]

この報告書では、LPWA ソリューションを検討する際に、コスト、長いバッテリ寿命、ネットワークのサービスエリアなどの他の考慮事項に加えて、必要なセキュリティレベルを策定する必要があると述べています。IoT のセキュリティニーズが主にプライバシーと安全性への懸念によってどのように左右されるか、そして LPWA 技術を用いた展開は、GSMA IoT Security Assessment [32]などのツールを使用したセキュリティリスク評価の対象となることを強調しています。

ネットワークセキュリティの重要な要因の一部は、次のような評価の一部として考慮する必要があるとこの報告書で強調されています。

- 最大ダウンリンクデータレートおよびアップリンクデータレートを含む帯域幅。これにより、LPWA ネットワークでサポートされるか、アプリケーションレイヤーで実装されるセキュリティ機能が制限される場合があります。
- 毎日のダウンリンクおよびアップリンクのスループット。LPWA デバイスは通常、無線通信を経由するセキュリティアップデートなどのセキュリティ機能に影響を与える可能性があるデータを常に送受信しません。
- 認証。デバイス、加入者およびネットワーク。安全なネットワーク接続には、デバイス、加入者、ネットワークプロバイダーなど、相互に認証する上で多様な当事者を必要とします。この技術は悪意あるアクターがこの当事者の「なりすまし」になることから保護する必要があります。
- データの機密性。暗号化は通常、攻撃者がデータを傍受するのを防止するために使用されます。これに対する信頼は、アプリケーションレイヤーでエンドツーエンドのセキュリティを確立することで向上させることができます。
- キーのプロビジョニング。認証、機密性および整合性に対する暗号技術はすべて、当事者間で安全に共有される暗号キーに依存します。
- 認定機器。多くの市場では、無線伝送を備えたデバイスが販売される前に承認または認定を受けるための法的要件があります。これはセキュリティ機能が検証される良い機会です。
- IP ネットワーク。IP を使用するとデバイスに対するインターネットからの攻撃の可能性が広がるので、セキュリティ機能を考慮する必要があります。

この報告書では、LPWA 技術にある潜在的に重要ないくつかのセキュリティ機能は、ネットワーク事業者が直接有効にするか、ネットワーク事業者が実施する他の選択肢に依存するという点で、ある程度の選択肢

があると結論付けています。ネットワーク事業者は、ネットワーク構成で実施する選択肢におけるセキュリティ上の影響を認識し、これら選択肢の状態を顧客へ明確に伝達するようにする必要があります。一部の選択性はデバイス製造元の管理下にあり（取り外しができない eUICC などの固定された安全な要素を含めるかどうかなど）、顧客に対してこのセキュリティ上の影響を伝達するのと同じ義務が適用されます。

LPWA 技術を使用する際のセキュリティに関する具体的な考慮事項は次のとおりです。

すべての LPWA ネットワーク技術の場合：

- IP ネットワーク層がリンク層上に実装されているかどうか。
- セキュアエレメントが存在するかどうか。存在する場合、それが取り外し可能かどうか。
- データの整合性がどの程度保証されているか。
- 技術でサポートされるアルゴリズムまたはキーの長さがブラックリストになっているかどうか、または非推奨かどうか（GPRS の 64 ビット暗号キーなど）。

3GPP LPWA ネットワーク技術（つまり、NB-IoT および LTE-M）の場合：

- リモート SIM プロビジョニング（RSP）がサポートされているかどうか。
- どの整合性アルゴリズム（EIAx/GIAx）と機密性アルゴリズム（EEAx/GEAx）が実装されて許可されているか。

LoRaWAN の場合：

- ABP（Activation By Personalization）または OTAA（Over-The-Air Activation）が実装されているかどうか、OTAA の場合、AppKey がデバイス間で共有されるのかどうか。

SigFox の場合：

- SigFox ネットワークを使用する場合、ペイロードの暗号化はオプションですが、利用可能であることを考慮する必要があります。したがって、Sigfox 認定の暗号チップを使用して、AES 128 暗号化を有効にして、無線通信を経由してデータを機密扱いとして維持する必要があります。

すべての LPWA デバイスの場合：

- どのような形態のセキュリティ証明書が実施されたか（ある場合）。

5.3 固定ネットワークのセキュリティ

ネットワーク事業者または IoT サービス提供者の管理下にある Wi-Fi ネットワークのデフォルト構成に関する推奨事項には、EAP-SIM [28]または EAP-AKA [27]の認証が含まれており、ETSI TS 102 310 [8]の UICC EAP フレームワークに依存する場合があります。

5.4 トラフィックの優先順位付け

ネットワーク事業者は、提供される IoT サービスに対して適切な「サービス品質（QoS）」レベルを提供することができます。

5.5 バックホールセキュリティ

GSM、UMTS および LTE を規定する 3GPP 規格では、暗号化されたブラックホールリンクの使用を義務付けていません。さらに、異なるネットワーク事業者間で RAN とバックホールを共有することにより、セキュリティ上のさらなる脆弱性をもたらす可能性があります。

ネットワーク事業者は、エンドユーザーのデータはもちろんのこと、シグナリングプレーンのデータトラフィックにも GSM、UMTS および LTE ネットワークのブラックホール暗号化を実装する必要があります。

5.6 ローミング

ネットワーク事業者は、ローミングサービスを利用して IoT サービス提供者に国際的なモバイルフットプリントを提供することができます。

ローミングネットワークは、ホームネットワークとローミングネットワークを接続するために使用される SS7/ダイアメーターインターワーキング機能の相対的な開放性により、セキュリティ侵害に対して脆弱になる可能性があります。これは、ローミングネットワークに常駐する IoT エンドポイントデバイスの割合が高い可能性があるため、IoT サービスと特に関連性があります。ローミングエンドポイントデバイスの割合が高い理由はいくつかあります。まず、多くのエンドポイントデバイスは 1 か所で製造され、グローバルに流通します。したがって、多くの場合、UICC を交換することは実用的ではなく、組み込み型の UICC の場合では不可能です。次に、多くの場合、いくつかのローミングネットワークが複数のサービスエリアを網羅する可能性があるため、ローミング状態はローカル接続よりも好ましいです。グローバルな UICC と専用 IoT ローミング契約でグローバルアライアンスを形成することにより、現地の法律が許可している恒久的なローミング状況が促進されます。

ネットワーク事業者は、サービス拒否の攻撃（意図的でない DoS 攻撃を含む）、不正な発信元からの要求、および「ローミングのステアリング」サービスの悪用から HLR および VLR を保護する方法を検討する必要があります。

ローミングは、主要なコアモバイルネットワークエンティティ間で交換されるネットワーク事業者間の信号プロトコルによって促進されます。

1. ローミング（訪問先）ネットワークの VLR または SGSN と、ホームネットワークの HLR 間の MAP（モバイルアプリケーションパート）プロトコル（CDMA ネットワークの場合、IS41 は MAP に似ています）。
2. LTE ローミングネットワークの MME とホーム LTE ネットワークの HSS 間のダイアメーター（S6a などの一定の変数）プロトコル。
3. 訪問先ネットワークの SGSN/S-GW と、ホームネットワークの GGSN/P-GW 間での GTP（GPRS トンネリングプロトコル）を用いたローミングデータ転送。

このセクションでは、IoT サービスに関するローミングセキュリティの問題に焦点を当てます。一般的なローミングセキュリティの問題は、GSMA FASG（不正およびセキュリティグループ）とそのサブグループで取り扱っています。そのため、異なる国にある 2 つの異なる VLR から受信したローミングにおける二重登録（標準的なローミング詐欺のシナリオ）などの問題は、本書の範囲外となります。

5.6.1 ローミングのシグナリングストーム/攻撃

IoT には、エンドポイントデバイスの性質が異なり、サービスの重要度レベルが非常に高い可能性があるため、モバイルネットワークから追加のセキュリティ要件があります。多数のエンドポイントデバイスにサービスを提供している間、モバイルネットワークはシグナリングストームにさらされています。意図的に悪意のある DoS 攻撃は、このようなストームの原因の 1 つにすぎません。モバイルネットワークを供給している特定のエリアにおける停電、自然災害、またはサービスエリアの問題は多くの国々で共通しているため、このような問題が発生します。そのエリアにあるすべてのローミングスマートメーターおよびその他のエンドポイントデバイスは、同時に別のローミングネットワークへローミングを試みます。前述のシナリオはシグナリングストームを生み出し、ホーム HLR/HSS に重大なリスクを与えます。3GPP TS 23.122 [9]では、このようなシナリオに対処すべく、拡張アクセス制限（EAB）のサービスを定義しています。ネットワーク事業者は、共通したドメイン固有のアクセス制限メカニズムに加えて、EAB 用に構成されたエンドポイントデバイスに対し、ネットワークアクセスを制限できます。EAB の構成は UICC またはエンドポイントデバイス自体で実行できます。ネットワークセキュリティのゲートウェイは、意図的な DoS 攻撃を「シンクホール」するように構成する必要があります。

優先度の低いエンドポイントデバイスと重要なエンドポイントデバイスを区別するために、ホームネットワークの事業者（IoT サービス提供者とともに）が必要となる場合もあります。たとえば、医療機器がシグナリングストームやサービス拒否攻撃の下でサービスを維持し続けることが必要な場合があります。ネットワークは、シグナリングストーム状態の下で「優先度の低い」エンドポイントデバイスのローミング登録を拒否する必要がありますが、「優先度の高い」エンドポイントデバイスを登録できるようにする必要があります。実装される拒否メカニズムは、シグナリングストームの後に行う登録の再試行でエンドポイントデバイスを支援するバックオフタイマーを伴う場合があります。

ネットワーク事業者がホームネットワークやローミングパートナーから受信するすべてのローミングメッセージをスクリーニングすることが一般的に推奨されています。不正なホームネットワークや偽装したホームネットワークからのメッセージをブロック化することに加えて、エンドポイントデバイスの優先順位に従ってメッセージをフィルタリングする必要があります。シグナリングストームや DoS 攻撃の下では、優先度の高いエンドポイントデバイスや重要なエンドポイントデバイスからのメッセージを許可するか、重要でないエンドポイントデバイスからのメッセージを拒否する必要があります。一定期間、登録の試行や他のアクティビティを延期するには、拒否方法が必要です。

5.6.2 セキュリティベースのローミングのステアリング（SoR）

ネットワーク事業者が実行できるもう 1 つのセキュリティユースケースは、セキュリティ目的での IoT エンドポイントデバイスのローミングのステアリング（SoR）です。バックオフタイマーなしで「更新位置」を拒否すると、エンドポイントデバイスは再試行し、最終的には別のローミング（訪問先）ネットワークからの登録を試みます。SoR の別の方法は、UICC ローミング優先リストと UICC に格納されている他のパラメータを使用して、OTA を経由する方法です。UICC の OTA 更新機能により、ホームネットワークは優先ローミングリストを更新することができ、ローミングネットワークの選択プロセス中にネットワークの優先順位を決定します。ホームネットワークは、新しいリストでエンドポイントデバイスのメモリを最新の情報に更新することもでき、エンドポイントデバイスに新しいネットワークを即時に検索させることもできます。

特定の訪問先ネットワークでセキュリティリスクが検出された場合、ホームネットワークは SoR メカニズムを用いて、アウトバウンドローミングのエンドポイントデバイスを別の訪問先ネットワークに転送することを決定する場合があります。このようなエンドポイントデバイスのアクティブな転送は、エンドポイントデバイスが次に登録を試行する際か、SIM OTA サービスを利用するアドホックで行うことができます。特定の訪問先ネットワークに関連するセキュリティリスクは、そのネットワーク上をローミングしている比較的多数のエンドポイントデバイス、または他の入力で受信した情報によって問題が報告された場合に検出されます。

5.6.3 データローミングによるサービス拒否

DoS 攻撃は、モビリティシグナリングの空間に限定されず、データローミングもシグナリングストームの可能性のあるフィードになります。今日現在では、ローミングデータの大半は、訪問先ネットワーク SGSN（LTE の場合は S-GW）からホームネットワーク GGSN（LTE の場合は P-GW）にルーティングされます。データが訪問先ネットワークからインターネットへ直接ルーティングされる LBO（ローカルブレークアウト）のケースはめったに実装されません。2014 年 7 月以降、LBO サービスを有効にした EU 規制、LTE、特にローミングネットワークで行われる音声通話が国内の P-GW（訪問先ネットワークで行われる通常の回線切替音声通話を使用した今日のケースなど）で処理されることがある VoLTE（ボイスオーバーLTE）などの規制により、将来の状況は変わる可能性があります。

シグナリングストームは、ホーム GGSN/P-GW に新しいデータセッションの要求が殺到している場合に発生することがあります。GPRS プロトコルは、エンドポイントデバイスと GGSN との間に安全なトンネルを作成し、新しいセッション（PDP コンテキストの生成）の要求により、トンネルを設定し、IP アドレスをエンドポイントデバイスに割り当てます。IoT エンドポイントデバイスがカスタマイズした方法で動作しない場合、前述したように新しいデータセッションに対する要求のバーストを生成することができます。DoS 攻撃は比較的少数のエンドポイントデバイスで生成され、並行して新しいデータセッションの要求が複数作成されます。GGSN/P-GW サーバーの容量は限られており、このようなストームから保護する必要があります。

シグナリングストームを防止するには、ネットワーク事業者がセキュリティポリシーに基づいて、影響を受けるデバイスの通信プロファイルを変更するか、ネットワークのパケットコア内にセキュリティポリシーを成立させることによって、特定のデバイスがネットワークに接続するのを防止します。

重要なエンドポイントデバイスは、DoS 攻撃の下でもサービスを受ける必要がありますが、優先度の低いエンドポイントデバイスからの要求は一定の遅延期間、延期されます。

5.7 エンドポイントおよびゲートウェイデバイスの管理

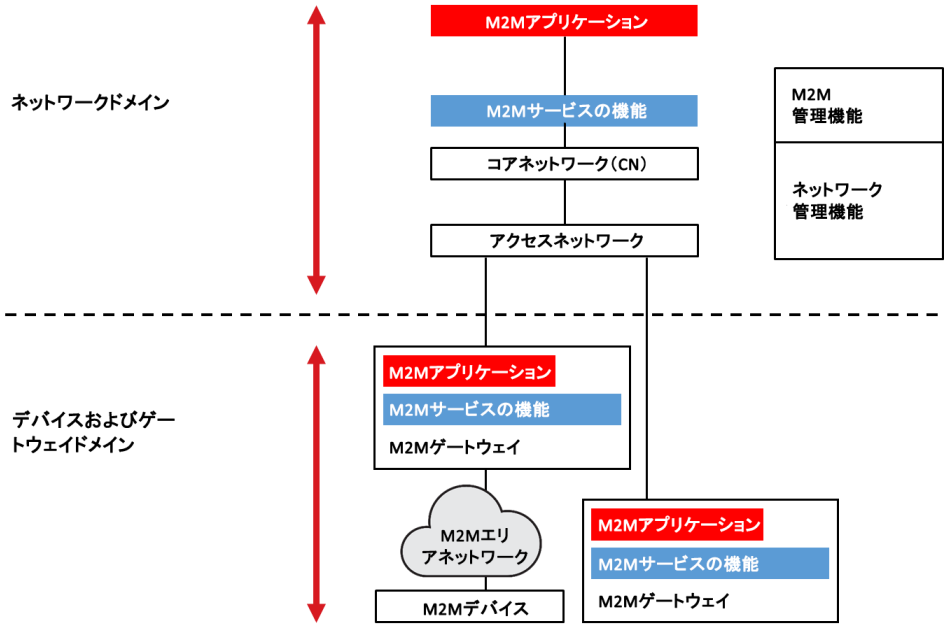
エンドポイントデバイスおよびゲートウェイデバイスのローカル構成管理コンソールを含め、ハードウェアおよびソフトウェアのセキュリティ対策は、本文書の範囲を超えていることに注意する必要があります。このセクションでは、ネットワーク関連の側面について説明します。エンドポイントデバイス関連のセキュリティガイドラインについては、GSMA の文書「CLP.11 IoT Security Guidelines Overview（IoT セキュリティ・ガイドライン概要説明書）」[11]を参照してください。

5.7.1 エンドポイントデバイスの管理

ネットワーク事業者は、IoT サービス提供者に「従来の」モバイルデバイス管理向けに開発された原則と技術の一部を採用して、エンドポイントデバイスとサブスクリプションを安全に構成および管理する基本機能を提供することができます。UICC を使用して移動体通信ネットワークに登録して接続する IoT エンドポイントデバイスは、今日存在する接続管理プラットフォーム、デバイス管理プラットフォーム、および UICC 管理プラットフォームを使用して管理することができます。

IoT サービスプラットフォームによって、この基本的なエンドポイントデバイス管理機能の上に、より複雑で具体的なエンドポイントデバイス管理機能を提供することができます。

典型的なエンドポイントデバイス管理アーキテクチャの例を下記に示します。これは ETSI M2M の通信原則[19]から抜粋しています。



a) - M2M デバイス管理向けの ETSI 高レベルアーキテクチャ

青色のブロックは、ネットワーク事業者の既存デバイス管理プラットフォームで従来管理されているものを示し、赤色のブロックは、IoT サービスプラットフォームで管理されるサービスコンポーネントを示しています。

ネットワーク事業者は、IoT サービス提供者の要求に応じて、赤色で示しているデバイス管理機能の一部を請け負うことができます。

5.7.2 ゲートウェイデバイスの管理

ゲートウェイデバイスを使用すると、IoT サービス提供者にとってデバイス管理がもう一段階複雑になる可能性があります。場合によっては、IoT ゲートウェイデバイスが移動体通信ネットワークに接続する UICC ベースのデバイスになることがあり、別の場合では、固定回線が使用されます。

ゲートウェイは管理対象のオブジェクトである必要がありますが、必要に応じて新しいファームウェアまたはソフトウェアで監視および更新することができます。ゲートウェイのネットワークバックボーンへの相互接続を保護する上で、安全なファームウェアとソフトウェアの更新、および安全なソフトウェアとシステムの統合メカニズムを提供するためのプロトコルを使用する必要があります。

ネットワーク事業者は、IoT サービス提供者に代わって安全なゲートウェイを提供して管理することができ、それにより、エンドポイントデバイスはネットワーク事業者のワイドエリアネットワークのセキュリティメカニズムと最適に統合する方法で安全に接続できます。

固定ネットワーク接続を用いて接続するゲートウェイは、Broadband Forum TR-069 CPE（カスタマ構内設備）ワイドエリアネットワーク（WAN）管理プロトコル[20]を使用してリモートで管理できます。

移動体通信ネットワーク接続を用いて接続するゲートウェイは、OMA デバイス管理（DM）および Firmware Update Management Object（FUMO）プロトコル[5] [6]を使用してリモートで管理できます。

5.7.3 IoT エンドポイントデバイスのブラックリスト

ネットワーク事業者は、IoT エンドポイントデバイスのブラックリストと GSMA Central Equipment Identity Register（CEIR）データベースへの接続を実装する必要があります。CEIR は GSMA によって管理される中央データベースであり、紛失したり盗まれたりしたエンドポイントデバイスに関連する IMEI、およびネットワークアクセスを許可する必要のないデバイスが入っています。IMEI が CEIR に入力されると、IMEI を含むエンドポイントデバイスは、そのデータを取得して、機器識別登録簿（EIR）の使用に基づいてローカルのブラックリストを実装するすべてのネットワーク事業者によってブラックリストに登録されます。

ネットワーク事業者は、ローカライズされたデバイスの「グレーリスト」を実装して「疑わしい」デバイスを一時的に停止させている間に、ブラックリストに登録する前に該当するデバイスの性質を調査することもできます。医療などの重要なサービスの場合、IMEI をブロックすることは望ましくないか、可能ではない場合があることに注意してください。エンドポイントデバイスの正しいアプリケーション（またはホスト）が識別できる限りにおいて、ネットワーク事業者が接続したエンドポイントデバイスの詳細を明確に理解しておくことが重要です。通信

モジュールベンダーに対して発行した IMEI を活用するエンドポイントデバイスは、エンドポイントデバイスがネットワーク事業者に対してホスト情報を報告できるようにする機能であるデバイスホスト ID レポートをサポートする必要があります。デバイスホスト ID レポートは、GSMA の Connection Efficiency Guidelines [17]で説明されています。

5.8 その他セキュリティ関連のサービス

5.8.1 クラウドサービス/データ管理

ネットワーク事業者は、IoT サービスを実装するためにホストされたクラウド IoT サービスプラットフォームを顧客に提供することができ、このようなサービスによって生成されたデータを格納および管理するサービスも提供することができます。

ネットワーク事業者は、IoT サービス提供者の要件に応じて、プライベートクラウドまたは共有クラウドインフラストラクチャのいずれかを提供することができます。

5.8.2 アナリティクスベースのセキュリティ

ネットワーク事業者は、IoT サービスによって生成されたデータにおける脅威と異常を識別するために、データ分析とディープパケットインスペクションサービスを提供できます。たとえば、ネットワーク事業者が社会保障番号や GPS 座標などの特定な文字列に対してディープパケットインスペクションを定期的に実行して、その情報が適切に保護されていないことを示唆したり、情報が漏洩する可能性があることを IoT サービス提供者の担当に警告したりする場合があります。

これは、軽量エンドポイントデバイスとサービス自体がこの機能を提供できないため、IoT にとって有利です。ネットワーク事業者は、IoT サービス提供者に可視性のあるセキュリティステータス、特定した脅威および攻撃、ならびに全体的なセキュリティヘルスチェックを提供できます。これらのイントロスペクションサービスは、特にデータサービスが暗号化されている場合、脅威が「パイプ内に」浸透しないようにするために不可欠です。提供されるサービスには次のものがあります。

- 異常検出と機械学習の使用による問題点の発見
- 侵入保護システムをリアルタイムエンドポイントデバイス診断に構築。
- ダッシュボードを提供して可視化し、異常を容易に特定。
- 自動化手段を提供して、疑わしい接続にフラグを立ててブロックする。
- クラウドベースの脅威分析サービスの提供。

5.8.3 セキュリティで保護されたネットワーク管理

ネットワーク事業者は、安全に管理、維持されているネットワークを提供することができます。

- 物理的または論理的なリンク障害が発生した場合のバックアップチャネル
- 可能性のあるセキュリティ侵害の証拠としてのリンク障害の特定
- セキュリティと整合性に影響を及ぼすローミングポリシーの実装
- UICC/SIM の管理
- 安全な情報の管理
- CERT のメンバーシップと脅威情報の共有に参加して将来発生する攻撃の軽減と予防。
- サービス拒否攻撃からの保護
- 定期的なセキュリティスキャンおよび脆弱性評価の実施
- ネットワークセキュリティ関連の規制要件の管理と処理
- 特定の IoT サービスに対して厳密に必要な最小限の通信オプションを制限

5.8.4 安全な IoT コネクティビティ管理プラットフォーム

ネットワーク事業者は、効率的かつスケーラブルな方法で IoT サブスクリプションと料金プランを管理する専用のコアネットワークと OSS インフラストラクチャをますます活用しています。このようなインフラストラクチャへのアクセスは、事業者の取引顧客（つまり、IoT サービス提供者）に公開されることが多いので、自身のサブスクリプション（個別または一括によるサービスのアクティブ化、停止など）を自身で管理することができます。

CLP 12「IoT Security Guidelines for IoT Service Ecosystem」[26]で提供しているサービスプラットフォームに関するガイドラインでは、IoT コネクティビティ管理プラットフォームをサポートするネットワーク事業者にとって有益なガイダンスを提供しています。これらのガイドラインには次の推奨事項が含まれています。

- ネットワーク事業者は、自身の IoT コネクティビティ管理プラットフォームのウェブポータルへのアクセスを確実にする必要があります。これはネットワーク事業者またはクラウドがホストされていることがあり、NIST [24]や ECRYPT2 [25]などの組織から最近公開された業界のガイダンスに従った「クラス最高の」暗号化を使用しています。
- ネットワーク事業者は、IoT コネクティビティ管理プラットフォームのウェブポータルにアクセスして、パスワードの作成、更新、リセットが標準的な「ベストプラクティス」の手順を利用していることを確認する必要があります。

5.8.5 証明書管理

ネットワーク事業者は、X.509 証明書管理サービスを提供することができます。

5.8.6 マルチファクタ認証

マルチファクタ認証サービスは通常、ユーザーがユーザー名とパスワードに加えて、電子トークンを使用して自分自身を認証するよう要求します。このように、マルチファクタ認証は権限のないユーザーからの IoT サービスへのアクセスに対してさらなる保護を提供することができます。

GSMA の Mobile Connect initiative [12]は、OpenID Connect [21]、FIDO [22]、ETSI MSS [23]とともに、IoT サービス提供者がエンドユーザーから追加の認証と情報を取得できるようにするマルチファクタ認証イネーブラの例となります。この状況におけるエンドユーザーは、異なるレベルの保証を提供する IoT サービスプラットフォームに情報を提供できる人間であり、例には PIN の入力やバイオメトリック署名の提供が挙げられます。

マルチファクタ認証ソリューションの大半は現在、従来の「スマートフォン」サービスを有効にするために使用されていますが、このような技術はネットワーク接続操作、ソフトウェア更新、ハードリセットの実行などの特定のタスクに対して人間の承認を保証する必要のある IoT サービスに適用することができます。

たとえば、マルチファクタ認証を使用すると、接続された自動車内にあるゲートウェイデバイスに加えて、モバイル ID を使用することができます。このユースケースでは、マルチファクタ認証のインフラストラクチャは、自動車内に提供されたインフォテインメントサービスおよび決済サービスにアクセスする自動車の乗員に対する追加の承認層として機能することができます。

付録A 文書管理

A.1 文書の履歴

バージョン	日付	変更事項の簡記	承認者	編集者/会社名
1.0	2016 年 2 月 8 日	New PRD CLP.14	PSMC	Ian Smith GSMA
1.1	2016 年 11 月 17 日	GSMA IoT セキュリティ評価スキームの参考資料の追加。 軽微な修正。	PSMC	Ian Smith GSMA
2.0	2017 年 9 月 30 日	LPWA の参考文献を追加するための大改正	IoT Security Group	Rob Childs GSMA

A.2 その他の情報

種類	説明
文書の所有者	GSMA IoT プログラム
連絡先	Rob Childs – GSMA

GSMA は、お客様に高品質の情報をお届けしたいと考えています。誤記や記載漏れなど、お気づきの点がございましたら、ご意見をお寄せください。お問い合わせ先：prd@gsma.com

ご意見、ご提案、ご質問をお待ちしております。