Japanese

Association of

Healthcare

Information

Systems Industry

JAHIS

セキュリティ委員会報告書

JAHIS
医療情報システムにおける
無線通信技術利用ガイド

2025 年8月

一般社団法人

保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

セキュアトークン WG

JAHIS 医療情報システムにおける無線通信技術利用ガイド

ま え が き

（背景）医療施設においては、Wi-Fi や PHS を始めとする無線技術を利用した医療情報システムが稼働している。各医療施設は、無線通信技術を利用して医療情報システムを構築・運用する際にも、厚生労働省の発行した「医療情報システムの安全管理に関するガイドライン第 6.0 版」（以下安全管理ガイドラインと略す）の各種要件を満たす必要がある。

（この報告書の目的）JAHIS セキュリティ委員会としては、Wi-Fi を用いて医療施設内のネットワークを構築する場合に安全管理ガイドラインに記載されている最低限の対策及び実例を示している。しかしながら、今後は5G を始めとする他の無線通信技術も医療施設の医療情報システムの中で利用される場面も増えると想定している。そのため、本報告書は今後利用が想定される無線通信技術に関して、基本的な技術仕様、導入に際する注意点などをまとめて、導入する無線通信技術の参考情報として活用されることを目的としている。

（想定する読者）本書は医療施設に無線通信技術を適用することを計画している医療施設の管理者、医療施設のネットワーク構築に際して無線通信技術を適用したシステムを構築するネットワークサービス提供者等に対し、利用する無線通信技術を決定する際に参考とする情報を提供することを想定している。

（利用条件）本報告書は調査時点での公開情報を元に取りまとめたものであるので、利用にあたっては利用者の責任において最新情報を確認の上利用いただきたい。

2025 年8月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会
セキュアトークン WG

＜＜ 告知事項 ＞＞

本報告書は利用者が本工業会の会員であるか否かにかかわらず、報告書の引用を明示することで自由に使用することができるものとします。本報告書の部分実装や拡張を行う場合は、実装者の責任において行うこととし、その実装範囲や拡張範囲を関係者に提供、公開することを推奨します。

本報告書ならびに本報告書に基づいたシステムの導入・運用についてのあらゆる障害や損害について、本工業会はなんらの責任を負わないものとします。ただし、本工業会の会員は本報告書についての疑義を申し入れることができ、担当委員会はこれに誠意をもって対応するものとします。

目　次

1. はじめに

JAHIS セキュリティ委員会では、セキュアトークン WG を中心に JAHIS 内外の関係者の協力のもと、本報告書を作成した。

本書は現時点の各無線通信技術の状況について調査した結果を取りまとめたものであり、技術の進歩や普及によって情報が陳腐化する可能性があることからJAHIS標準類としてではなく、報告書として取りまとめた。

本書はあくまで調査時点での公開情報を基に取りまとめたものであるので、利用にあたっては利用者の責任において各無線通信技術の提供各社及びサービス提供の各社の最新情報を確認の上利用いただきたい。

また、本書はシステム実装について解説は行っていない。あくまで参考資料の位置づけであるので、不足する情報についてはシステム構築ベンダー等の他の公開資料などを参照いただきたい。

2. 概要

本書は、現在普及している無線通信技術及び今後普及の見込まれる無線通信技術について、技術的な特徴等、安全管理ガイドラインとの整合性確保の方策、導入・運用時に想定されるコスト等について調査した結果をとりまとめたものである。調査は、既に普及している PHS、LTE、及び Wi-Fi 並びに今後普及の見込まれる sXGP、Local 5G、及び Private 5G について実施し、技術的な特徴、主な用途、セキュリティ機能、導入コスト、運用の負荷、移行及び今後の発展等の状況を調査している。

3. 主な用語

5G-AKA: 5th Generation Authentication and Key Agreement の略。
ETSI TS 33.501: Security architecture and procedures for 5G system, 3GPP で規定される認証および鍵共有のプロトコル。

AKA: Authentication and Key Agreement の略。
認証と鍵合意の手順。SIM カードに格納された鍵と通信事業者側の鍵を使って認証を行い、暗号鍵を導出する。

ADPCM: Adaptive Differential Pulse Coded Modulation の略。
音声など信号をデジタルデータに変換する変調技術の一つ。PCM(Pulse Coded Modulation)方式よりデータ量を小さく圧縮できるため、多くの波形に適用可能。

CS-ID: Cell Station ID の略。
基地局を識別する番号。自営用のシステムでは、システム呼び出し符号(29 ビット)と付加 ID(13 ビット)の計 42 ビットで表現される。

EAP-AKA: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement の略。
RFC 4187 で規定される認証および鍵共有のプロトコル。

EAP-AKA': Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement の略。
RFC 5448 で規定される認証および鍵共有のプロトコル。

FDM: Frequency Division Multiplexing の略。
電気通信における多重化技術の一つ。利用可能な周波数帯域を異なる周波数チャネルに分割し、それぞれのチャネルに異なる信号を割り当てることによって 1 つの伝送路で同時に複数の伝送を可能とする。

IEEE 802.1x: 有線/無線を問わずネットワークに接続する端末を接続時に認証を行い、ネットワークへの接

続を許可するための規格。認証が未完了の通信を拒否することができるので、ネットワークへの不正アクセスを防止できる。

IMSI: International Mobile Subscriber Identity の略。
携帯電話の加入者を識別するための国際的な識別番号。最大 15 桁で構成される。

ISDN: Integrated Services Digital Network の略。音声信号をデジタル化して、デジタル化した電気信号として送受信するネットワーク。サービス総合デジタル網などとも呼ばれる。

LTE: Long Term Evolution の略。
詳細は 5.1.2.1 参照。

Local 5G: 自営の5G ネットワーク。詳細は 5.1.2.3 参照

MIMO: Multiple Input Multiple Output の略。
無線通信において、複数の送信アンテナと受信アンテナを使用してデータを同時に送受信する技術。空間多重化やビームフォーミングなどを活用することによって、通信速度の向上や伝送品質の改善を可能とする。

MLO: Multiple Link Operation の略。
Wi-Fi 7 で採用されている通信技術で、異なる周波数帯とチャネルでデータを同時に送受信できるようにする方式。2.4GHz，5GHz，6GHz 帯域に同時に接続することで、スループットや信頼性が向上し、遅延が減少する。

OFDM: Orthogonal Frequency-Division Multiplexing の略。
デジタル変調方式の一つ。互いに直交するサブキャリアを利用して複数の狭帯域信号を同時に送信することによって、帯域幅を効率的に活用することができる。

PHS: Personal Handy-phone System の略。
詳細は 4.1.1 参照。

PIAFS: PHS Internet Access Forum Standard の略。
業界団体(PIAF)が策定した伝送制御規格。

Private 5G: 特定ユーザー向けのみに提供する5G ネットワーク。詳細は 5.1.2.4 参照

PS-ID: Personal StationID の略。
子機や端末を識別するための番号。端末固有の 28 ビットの ID で、PS 内の ROM に書き込まれている。

QoS: Quality of Service の略。
ネットワーク上で流れるデータの優先順位を制御し、重要なデータの通信に遅延を発生させない技術。

SIM: Subscriber Identity Module の略。
契約者を識別するための識別番号、電話番号などが記録された IC モジュール等。

SUPI: Subscription Permanent Identifier の略。
5G における加入者識別番号。IMSI の代わりに使用され、プライバシー保護のために暗号化される。

sXGP: shared Xtended Global Platform の略。
TD-LTE（TDD 方式を適用した LTE)をベースとした自営通信専用のモバイル無線通信方式。詳細は 5.1.2.2 参照。

TDD: Time Division Duplex の略。
送受信の同一周波数を高速で切り替えて上り回線と下り回線を構成して通信を行う方式。

TDD-TDMA:Time Division Duplex Time Division Multiple Access の略。
PHS に使われている方式で、上り/下りの通信周波数が等しい TDD で TDMA を適用した通信方式。TDMA とは、通信に使用する 1 つの無線帯域の時間軸を複数に分割し、分割した複数の時間(タイムスロット)を複数のユーザーに割り当てることによって同時に複数のユーザーの通信を可能とする時分割多元接続による接続方法。VoLTE: Voice over LTE の略。

LTE方式で音声通話データをデータ通信によって提供する技術。

Wi-Fi: IEEE 802.11 シリーズで規定される無線通信技術。詳細は 4.2.1 参照。

WPA3: Wi-Fi Protected Access 3 の略。
Wi-Fi ネットワークのセキュリティを強化するための暗号化プロトコル。

基地局: 無線通信ネットワークにおいて、携帯電話やその他の無線デバイスと通信を行うための固定された送受信設備。基地局は、電波を送信し、受信することで、デバイス間の通信を中継する。

キャリアアグリゲーション :複数の周波数帯(キャリア)を同時に利用することで、データ通信速度を大幅に向上させる技術

通信事業者: 無線通信インフラストラクチャ(例えば、基地局、コアネットワーク、バックホールネットワークなど)を構築・運用し、音声通話、テキストメッセージ、データ通信などのサービスを提供する事業者。

ネットワークスライシング: 物理ネットワーク上に仮想的な論理ネットワークを形成し、異なるサービスやアプリケーションに対して最適なネットワークリソースを提供する技術。

4. 広く利用されている無線通信技術

4.1. PHS

4.1.1. 技術の特徴及び技術仕様

PHS は「Personal Handy-phone System」の略で、移動型無線通信システムの一つです。PHS は一般的な電話回線から専用アンテナを用いて狭い範囲に電波を届ける仕組みです。電波が届く範囲の目安は携帯電話が 2.5km～5km ほどなのに対して、PHS は 500m 程度と限定されており、半径 500m おきにアンテナを設置する必要があります。携帯電話端末をサービスとして提供するには電波法によって無線局免許状が必要ですが、PHS では無線局免許状が不要です。過去の携帯電話は周波数帯と高出力の影響によりペースメーカーをはじめとする医療機器に悪影響を与えるとされ、PHS を用いる医療機関が多かったのですが、近年の携帯電話は異なる周波数帯を用いるなど対策がされたのに加えて、無線 LAN を用いた IP 電話の普及などもあり、PHS の医療分野での優位性は失われつつあります。

スタンダードな PHS 方式においては、音声の符号化方式には 32kbps の ADPCM を使用します。周波数帯は 1.9GHz 帯を使用します。通話用帯域は、同帯域内において FDM です。1 つの通話用帯域上に、複信・多元接続方式として TDD-TDMA を採用します。1 フレームを 5ms とし、これを 625μs のスロット 8 つに分割します。TDD として、前半 4 つのスロットを下り（送信、基地局→端末）、後半 4 つを上り（受信、端末→基地局）、として独立して使用するため、多重数は 4 となります。また、8 スロットの内 2 スロットは制御スロットとして使用するため、1 つの周波数（1 つの通話用帯域）で同時に使用できるのは 3 通話となります。1 通話スロットあたりのトラフィックチャネル（通話チャネル）のデータレートは 32kbps であるため、64kbps のデータ通信を行う場合には、送受信スロットを 2 つずつ束ねて使用します。データを直接 PHS の通信チャネルに対し伝送する方式として PIAFS 仕様(ピアフ、Personal Handy-phone System Internet Access Forum Standard)が策定されました。利用上は、有線区間が固定電話回線に依拠するため、無線区間も含めて回線交換方式を基本とします。最新の規格は PIAFS2.2（ベストエフォート方式 32Kbps/64Kbps。PIAFS2.1 をベースに、PHS 端末間同士での 64Kbps 通信を可能にするために拡張されたもの）となっています。

4.1.2. セキュリティ上のポイント

PHS における基地局(CS)と端末(PS)の識別には基地局の CS-ID と端末の PS-ID が用いられます。PS-ID は PS 固有の符号であり出荷時に PS 内の ROM に書込まれます。CS-ID は自営用システムの場合はシステム呼出符号と付加 ID から構成されます。

子機間通話における識別符号は発呼する側 PS の PS-ID から構成され、着呼する側の識別符号は CS-ID のシステム呼出符号と着呼する PS の PS 呼出番号から構成されます。ここで PS 呼出番号は子機間通話モードでのみ有効な PS の論理番号です。子機間通話は同一親機に登録された複数の PS のように、同一のシステム呼出符号を共有している PS 間のみで有効です。

基地局とデジタル網間のインタフェースは ISDN の加入者線インタフェース(DSS1：I インタフェース)をベースに移動サービスの PHS に固有な機能を追加した I インタフェースが採用されているため、セキュリティ上は ISDN と同様と考えられます。

4.1.3. 導入・運用に係る事項

電波法による無線基地局免許状が不要なため、設置についてはハードルが低い技術です。基地局からの有効エリアが 500m 程度となるため、多数の基地局を施設内に設置してエリアをカバーする必要があります。

4.1.4. 今後の見込み

070番号を持つ公衆網としての PHS サービスは 2021年1月 31 日に終了し、現在は構内 PHS が利用されているのみです。そのため今後は技術や製品のアップデートが行われることは期待できません。代替手段への切り

替えが推奨されます。

4.2. Wi-Fi

4.2.1. 技術の特徴及び技術仕様

【特徴】

Wi-Fiは近距離での無線通信を可能にする技術であり、この技術はWi-Fiの技術仕様や動作基準を定めた標準規格である IEEE 802.11 シリーズで規定されています。一方、Wi-Fi 製品の認証を行う団体である Wi-Fi Alliance によって認証された製品は、相互接続性、セキュリティ、プロトコルなどの標準規格に準拠していることが保証されます。

Wi-Fiの主な用途は自宅、企業、公共施設などでのネットワーク接続であり、2.4GHz、5GHz 帯および6GHz 帯(Wi-Fi6E)の周波数を使用することで広範囲のデバイスが高速でインターネットに接続できるようになっています。具体的な技術仕様として、5GHz 帯の最大通信速度は Wi-Fi 4(11n)で 600Mbps、Wi-Fi 5(11ac)で 6.9Gbps、Wi-Fi 6E(11ax)では 9.6Gbps に達します。また、通信距離は一般的に 2～30m 程度で、周波数が高くなると、通信速度は向上しますが、障害物やノイズの影響を受けやすくなり、通信距離は短くなります。2.4GHz 帯は広範囲に届きやすく、5GHz 帯は高速だが距離は短め、6GHz 帯はさらに高速だが最も距離が短くなります。また、最新の Wi-Fi 7 は、Wi-Fi 6E に比べて変調方式、最大ストリーム数、最大帯域幅が改善され、最大通信速度が約 36Gbps に増加します。さらに、MLO(Multi-Link Operation)などの新機能により、通信遅延や安定性が向上する見込みです。

4.2.2. セキュリティ上のポイント

Wi-Fiのセキュリティは、識別・認証とチャネル・セキュリティの 2 つの要素で成り立っています。識別・認証については、WPA3 などの強力な暗号化プロトコルを使ってデータの安全性を確保し、IEEE 802.1x を利用して端末を認証します。また、EAP-AKA や EAP-AKA'による Wi-Fi SIM 認証もあり、これによりネットワークに接続するデバイスが正当であることを確認し、不正アクセスを防ぎます。チャネル・セキュリティについても暗号化が重要であり、Wi-Fi 通信は無線で行われるため電波を傍受されるリスクがあるため、通信データを暗号化することで第三者によるデータの盗聴や改ざんを防ぎます。これらのセキュリティ対策により、Wi-Fiネットワークは安全性を高め、信頼性のある通信環境を提供し、特に WPA3 の導入や IEEE 802.1x は多様なデバイスやアプリケーションに対応するために不可欠であり、これによりネットワーク利用がより安全かつ効率的に行えるようになります。

導入・運用に係る事項

Wi-Fi の導入には、アクセスポイントやルータなどのハードウェアの購入、設置、設定にかかる設備投資が必要です。これらの費用はネットワークの規模やカバー範囲に応じて変動します。一方、Wi-Fi の運用負荷は比較的小さく、専門的な知識がなくても簡単に設定・管理が可能です。既存のスマートフォンやタブレットなどが対応しているため、特別な端末を用意する必要もありません。これにより、導入後の管理やメンテナンスも容易に行えます。

4.2.3. 今後の見込み

Wi-Fi 6/6E の普及により、通信速度の向上、接続の安定性、同時接続デバイス数の増加が期待されます。機器の増加に対応しやすくなります。さらに、Wi-Fi 7 の開発も進んでおり、より高速なデータ転送速度、低遅延、多数のデバイス同時接続が可能になります。これにより、高解像度ストリーミングなどの高帯域幅アプリケーションにも対応でき、Wi-Fiは引き続き重要な技術として位置づけられることが見込まれます。

5. 携帯電話網で使われる無線通信技術

5.1.　技術の特徴及び技術仕様

5.1.1. 基本的な特徴及び技術仕様

携帯電話網で使用される無線通信技術は、広範囲での安定した通信、高いセキュリティ、特定の用途に応じた高性能な通信を提供します。これらの技術は、広いカバレッジエリアを持ち、移動中でも安定した通信が可能です。また、SIM 認証を用いた高いセキュリティを提供し、エンドツーエンドの暗号化やユーザー認証が行われます。

LTE（Long Term Evolution）は、4G ネットワークの基盤を形成し、高速・大容量・低遅延なデータ通信を提供します。LTE は広範囲にわたるカバレッジを持ち、移動中でも安定した通信が可能です。sXGP は、LTE の一部である TD-LTE を利用した自営通信方式で、電波干渉が少なく、安定した通信が可能で、工場や物流センターなどでの IoT 化や DX 推進に活用されます。

5G は第 5 世代移動体通信システムを指し、国際電気通信連合無線通信部門（ITU-R）が策定してきたモバイルシステムの規格です。1 世代前の4G と比較して約 20 倍の超高速の伝送速度、10 倍の多数同時接続、10 分の 1 となった超低遅延通信が実現可能です。ただし 3 つの特徴を同時に実現することはできないため、ニーズに応じて取捨選択を行い、5G ネットワークを個別に構築することが必要です。利用可能な周波数帯としては、ミリ波と呼ばれる 28GHz 帯（27.0～29.5GHz）と、Sub6 と呼ばれる 3.7GHz 帯（3.6～4.2GHz）、4.5GHz 帯（4.4～4.9GHz）、既存の設備を利用するために 4G 周波数帯を転用しているものがあります。ミリ波の特徴としては、周波数が高いため、超高速な通信が可能となりますが、電波が遠くまで飛ばず、障害物に弱いという特徴があります。一方Sub6 はミリ波と比べると周波数がミリ波程高くないため、長距離をカバーでき障害物にも強いですが、ミリ波のような超高速な通信はできないという特徴があります。4G 周波数帯を転用した場合は、ミリ波や Sub6 と比較するとスピードは遅くなりますが、5G の技術を使うため、4G/LTE よりは速くなります。また、既存設備を使用するため、エリア展開がスピーディーという特徴があります。

医療機関においては、Wi-Fi は設置や運用が簡単でコストが低い一方、電波干渉や通信距離の制約があります。携帯電話網の技術は、広範囲での安定した通信と高いセキュリティを提供し、大規模なエリアや高密度な環境での利用に適しています。特に、Local 5G や Private 5G は、医療機関内での高密度なデバイス接続や低遅延が求められる環境において有効です。用途や環境に応じて、これらの技術を適切に選択・組み合わせることで、効率的で信頼性の高い通信環境を構築することが可能です。

5.1.2.　　世代等による特徴

5.1.2.1 LTE

LTE は、4G の技術標準の一つであり、4G は、3G に続く高速データ通信を実現するための規格で、LTE はその中でも特に広く採用されています。LTE は、データ通信速度の向上、低遅延、効率的なスペクトル利用を特徴とし、理論上の最大ダウンロード速度は 100Mbps 以上であり、OFDM（直交周波数分割多重）技術を採用し、効率的なデータ伝送を実現しています。ただし、初期の LTE は、ITU が定めた 4G の基準を完全には満たしていなかったため、LTE は「3.9G」と呼ばれることがあります。後に登場した LTE-Advanced は、ITU の 4G 基準を満たし、さらに高速な通信速度と効率を提供しました。LTE-Advanced は、キャリアアグリゲーション、MIMO（多入力多出力）技術などを利用し、理論上の最大ダウンロード速度は 1Gbps 以上に達します。

5.1.2.2 sXGP

sXGP はプライベート LTE とも呼ばれ、2023 年 3 月にサービスが終了した公衆 PHS が使用していた 1.9GHz 帯を使用する TD-LTE をベースとした自営通信のための無線通信方式です。自営 PHS の後継サービスとして、PHS のコンセプトを踏襲しつつもモバイルルーターやスマートフォンなどで使われている 4G（LTE）方式をベースに機能を拡張しています。無線局の免許不要で使用することができ、周波数はほぼ専用であるため、電波干渉が少ないという特徴があります。スマートフォンを端末として利用でき、スマートフォンが

デュアル SIM に対応していれば、公衆ネットワークと自営ネットワークの両方を使用することも可能です。また、アクセスポイントを切り替えるハンドオーバーの切り替え時間が非常に短いことも特徴です。音声通話は VoLTE を使用し、QoS 保証がされるため高品質です。

周波数は 1.9GHz 帯（Band 39）を使用し、帯域幅として 1.4MHz、5MHz、10MHz を使用可能です。最大通信速度は上り 4Mbps/下り 12Mbps（5MHz）、上り 8Mbps/下り 28Mbps（10MHz）です。通信距離は半径 100m です。sXGP は、ネットワークの中心となるコアネットワーク装置にバックホールネットワークを通じてアクセスポイントが接続されます。コアネットワーク装置は、オンプレミスに設置される場合もあれば、クラウド上に構築される場合もあります。コアネットワークはインターネットゲートウェイを通じてインターネットと接続され、外部との通信を実現します。

5.1.2.3 Local 5G

Local 5G は、5G の通信方式を用いて自営の5G システムとすることができます。Local 5G により一般企業・自治体等が独自に 5G ネットワークを構築でき、屋内・屋外を対象とした独自に構築したエリアに対して、5G ネットワークを提供することが可能となります。

Local 5G の構築には基地局の免許が必要で、システム導入の手間がかかり、運用管理も必要ですが、他のエリアでの通信トラブルや災害の影響を受けにくいというメリットがあります。利用する周波数帯については 4.6-4.9GHz 及び 28.2-29.1GHz となっており、免許に基づいた無線周波数を安定して利用することが可能となります。

Local 5G は独自の基地局を運営する自営通信方式のため、5G の特徴である超高速・超低遅延・多数同時接続の中から、目的やニーズに応じて必要となる性能を取捨選択し、サービス設計した5G ネットワークを構築することが可能です。

Local 5G によるネットワークの構築の際は、ネットワークスライシング技術等を利用することで、システム、サービス毎にトラヒック分離が可能となり、柔軟で自由なシステムとすることができます。そのため、通信を止めることが重大な影響を及ぼすことになるミッションクリティカルな領域でも活用可能となり、工場やキャンパス、イベント会場などでの通信や IoT デバイスの連携等に利用することができます。

5.1.2.4 Private 5G

Private 5G は、通信事業者の通信網の一部を利用した特定ユーザー向けのみに提供する 5G ネットワークです。Local 5G では利用者自ら無線免許を取得する必要が有りますが、Private 5G の場合、通信事業者が企業や自治体の敷地内に基地局を設置し、利用者の個別要件に応じた5G ネットワークを構築・運用するため、構築の手間が軽減されます。ただし、システム、サービス設計の自由度については、通信事業者が提供するサービスに従うため、Local 5G と比較すると制限があります。

Private 5G は、既存の通信事業者の設備を使い、物理ネットワーク上に仮想的な論理ネットワークを形成するネットワークスライシングの技術による論理的な分離したネットワークを提供する方式（共有型）と、医療機関等の敷地内に通信事業者の設備を個別設置して提供する方式（専有型）があります。利用する周波数帯は、選択する通信事業者によって異なりますが、ミリ波、Sub6 を割り当てられているため、選択した通信事業者が提供するサービスに従うこととなります。

5.2. セキュリティ上のポイント

携帯電話回線のセキュリティは、端末と基地局間の無線通信部分のセキュリティ、基地局以降のセキュリティに大別することができます。本報告の対象となる前者では、セキュリティで重要となる端末の識別、認証、無線通信の暗号化のための仕様が次のように定められています。

1）端末の識別

LTE においては、最大 15 桁の IMSI（International Mobile Subscriber Identity）によって、端末を識別しています。IMSI は以下の MCC,NMC,NSIN から構成されています（表5. 2. 1参照）。

表5. 2. 1 IMSI の構成

名称	内容
MCC (Mobile Country Code)	3 桁の国番号。日本は 440 と441。
NMC(Mobile Network Code)	2-3 桁の事業者番号。
SN(Subscriber Number)	9-10 桁の加入者識別番号

IMSI は SIM カードが製造されるときに書き込まれます。MMC と NMC を合わせた PLNM(Public Land Mobile Network)は ITU-T E.212 に従った登録が必要となっており、日本では総務省が管理しています。IMSI は、5G では 15 桁の SUPI(Subscription Permanent Identifier)と呼ばれています。LTE では IMSI が保護されずに送信されるので追跡可能となる等プライバシー上の問題が指摘されていましたが、5G ではMMCとNMCを除いた部分であるSUPIを公開鍵で暗号化することでプライバシー保護に配慮しています。

2） SIM 認証

USIM(Universal Subscriber Identity Module：いわゆる SIM)に格納されている鍵と通信事業者側の鍵を使って AKA(Authentication and Key Agreement：認証と鍵合意)の手順に従って認証を行い、AV(Authentication Vector)と呼ばれる認証に用いるデータを用いて暗号鍵が導出されます。5G の場合には、暗号に用いる鍵に加えて完全性検証に利用される鍵が導出されます。

具体的な AKA の手順としては、LTE では RFC 4187 で規定される EAP-AKA、RFC 5448 および RFC 9408 で規定される EAP-AKA'が利用され、5G では、5G-AKA または、EAP-AKA '‘が利用されています。

3） 通信の暗号化

端末と基地局の間の無線通信は、AKA で導出された暗号鍵を用いて暗号化されます。暗号化には 128 ビットの「AES」、「SNOW 3G」、「ZUC」等の暗号アルゴリズムが用いられています。5G においては256ビットの鍵が使えるように拡張が計画されています。

暗号鍵はセッションごとに異なるものが使用されており、セッション間でのセキュリティが強化されています。主な鍵は次の通りです。

◆KASME(Key Access Security Management Entity)： 認証後に生成される鍵。

◆KeNB(Key eNodeB)： eNodeB(基地局)で使用される鍵

◆KRRC(Key Radio Resource Control)： RRC 層で使用される鍵

5.3. 導入・運用に係る事項

5.3.1. LTE

LTE の導入にはインフラ整備が必要で、基地局の適切な配置が求められます。医療機関内では、建物の構造やレイアウトに応じて最適な配置を検討することが重要となります。また、基地局の設置には電波の干渉を避けるための周波数管理が求められます。LTE は 1.9GHz 帯などの周波数を使用しており、これらの周波数の管理を適切に行う必要があります。

また、LTE の導入コストは、既存の Wi-Fi と比較して高くなることがあります。基地局の設置や運用にかかる費用、SIM カードの発行・管理費用などが含まれます。しかし、既に普及している技術であるため、機器やサービスの価格は比較的安価となります。また、電波利用料が不要なため、運用コストを抑えることができます。

運用面では、運用管理には専門的な知識を持った管理者が必要となります。無線従事者資格取得者が 2 名以上必要となる場合もあり、通信品質の維持やトラブルの早期発見・対応のために、基地局の設置やメンテナンス、ネットワークの監視・管理が求められます。

スケーラビリティの面でも LTE は医療機関全体を一つのネットワークでカバーすることが可能であり、これにより、複数のアクセスポイントを設置する必要がなく、運用管理が簡素化されます。また、コアネットワーク装置はオ

ンプレミスでの設置のほか、クラウド上に構築することもできます。これにより、アクセスポイントの増設や移動などにも柔軟に対応できます。

以上のように、LTE の導入・運用にはコストや専門知識が必要ですが、高い通信品質とセキュリティを提供するため、医療機関においては有効な選択肢となります。

5.3.2. sXGP

sXGP は免許不要局として構成できるため、無線従事者の設置および電波利用料が不要です。導入にあたっては、コアネットワーク装置およびアクセスポイントを設置する必要があります。また、sXGP で使用する端末および sXGP で使用する SIM の導入も必要です。

アクセスポイントの同時接続数は製品によって異なりますが、同じ周波数帯を使用する PHS よりも多いため、設置するアクセスポイントの数を減らすことが可能です。

端末は一般に市販されている携帯電話やスマートフォンを利用できるため、専用の端末を準備する必要はありません。デュアル SIM に対応した端末を使用すれば、1 台の端末で sXGP と公衆回線を併用することも可能です。

5.3.3. Local 5G

Local 5G の導入運用を検討する際は、サービス開始時期を見据えた事前準備が必要となり、導入検討・設計として、免許申請の 2 ヶ月前までには総合通信局等に頭出しが必要となるため、そのための導入目的、導入機器の検討を行った上で、エリア設計、干渉調整を行い、免許申請を基地局、端末に対して行う必要があります。その後、構築として基地局の設置、アンテナ工事、ネットワーク工事、技術基準適合証明等を受けていない新設機器の場合は、予備免許を取得した上で新設検査を行います。本免許が交付されたらサービス開始となり、無線従事者選任届の提出、エリア確認、電波利用料の納付や、申請、サービスの内容によっては開設無線局数届出書の提出、定期検査等が必要になります。

免許の申請にあたっては、事務的な申請だけでなく、電波状況の確認・証明、無線設備の性能確認、電波干渉の確認等で基準を満たす必要があります。

導入コストについては、利用する周波数帯域(ミリ波帯、Sub6 帯)、システムの構成(LTE 設備との連携)、規模によって大きくコストが異なります。また利用する周波数帯や実現形態によって価格は異なるが、基地局や陸上移動局毎に電波利用料が必要となります。

5.3.4. Private 5G

Private 5G では、通信事業者の5G のユーザーと設備を共有する設備共有形と、Private 5G の契約者のみが専用のアクセスを行う設備専用型の大きく２つの方式があり、通信事業者のサービス提供形態によって異なります。これは、近隣に通信事業者の5G基地局があるか、屋内の場合は電波が十分に浸透している必要があるため、場合によっては、設備専有型として新たな設備導入が必要になることがあります。運用自体は通信事業者に任せることができるため、Local 5Gと比べてハードルは低くなります。Private 5G では設備共有形、設備専用型でそれぞれ特殊な機能によってパケット伝送や、接続可否を判断しているため、対応できる端末が、限られることになります。

導入コストについては、既設の 5G 環境が利用できるか、設備を共有するかによって初期投資額が異なってきます。また、Private 5G では利用者が免許を取得する必要がなく、電波利用料を負担することはありませんが、通信事業者が通信料等を設定しているため、通信事業者に依存した形でコストが上下します。

5.4. 今後の見込み

5.4.1. LTE

今後、LTE ネットワークは 5G ネットワークへのスムーズな移行が期待され、既存の LTE インフラは、5G の導入に向けた基盤として重要な役割を果たしています。LTE（3.9G）のサービスは徐々に終了し、LTE-Advanced(LTE-A)も 5G へと移行していく見込みです。なお、LTE は 5G の補完的な技術としても引き続き利用され、特に 5G のカバレッジがまだ十分でない地域では重要な役割を担っています。

5.4.2. sXGP

通信速度が低速であるものの、比較的安価にネットワークを構築できること、既存のスマートフォンを利用でき、多数の機器が sXGP への対応を始めていること等から、製造業、物流、医療等さまざまな分野で利用されています。また病院では、PHS と同じ周波数を利用し、PHS 同様に低出力（送信電力: PHS 19.0; sXGP 20.0 (dBm)）の sXGP は導入が容易であると考えられます。

5.4.3. Local 5G

Local 5G に関しては、2025 年以降に普及期が来ると考えられており、中小企業や小規模案件に適用できることが重要であるとされています。デバイスの機能拡張や低廉化、通信品質の改善、業界特化ソリューションの蓄積/横展開などのボトルネックが存在しているため、事業者同士の共創が必要とされています。

5.4.4. Private 5G

Private 5G は Local 5G の導入に課題がある事業者が、投資、運用負担が少ないため、様々なユースケースに対応できる方式として考えられています。

6. 厚労省安全管理ガイドライン適用のポイント

6.1. 安全管理ガイドラインに規定されるネットワークに関する安全管理措置への対応

6.1.1. ネットワークに関する安全措置と採用技術の関連

安全管理ガイドライン・システム運用編には「13 ネットワークに関する安全管理措置」にネットワークシステムの遵守事項が定められています。採用する無線通信技術に依存する事項もあるため、技術の採用に当たっては対応方法を確認する必要があります。表 6.1-1 に各安全管理措置と各無線技術で必要となる対応方針を示します。

表6.1-1 ネットワークに関する安全管理措置

安全管理ガイドラインでの記載される遵守事項	対応方針
① ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。	共通。構築の際に事業者との間で合意が必要。 特に外部の中継施設を経由する場合に、各端末から施設の入り口となる接続点までの責任の所在は明確にしておく必要がある。
② セッション乗っ取り、 IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアな ネットワークを利用すること。	共通。無線通信技術によらない対応。
③ オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。	採用する技術による追加対策が必要となる。特に外部の中継施設を経由する場合に、各端末と医療施設の入り口となる接続点の間の確認が必要となる。
④オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じ て、必要な単位で、 互いに 確認し、採用する通信方式や、採用する認証手段を決めること。	共通。無線通信技術によらない対応。
⑤ ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェア の混入が生じないよう、セキュリティ対策を実施すること。	共通。接続点の問題。実施方法は採用する無線通信技術によって異なる可能性がある。
⑥オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、 TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。	共通。アプリケーション層での問題。

⑦ 利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。	共通。アプリケーション層での問題。
⑧ 医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。	共通。採用する無線通信技術で安全性が確保されていることを確認する。
⑨ ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。	共通。採用する無線通信技術で安全性が確保されていることを確認する。
⑩ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。	共通。採用する無線通信技術で安全性が確保されていることを確認する。
⑪ 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。	共通
⑫ 医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。	共通
⑬ 医療情報システムにおいて無線 LAN を利用する場合、次に掲げる対策を実施すること。	Wi-Fi のみ該当。対応方法等については、JAHIS セキュアトークン実装ガイド・機器認証編を参照のこと

6.1.2. 各無線技術を応用する際の注意点

① ネットワークの責任分解及び責任の所在

携帯電話回線を利用する際には外部の中継施設を経由するので、各端末から施設の入り口となる接続点までの責任の所在を明確にする必要があります。通信事業者にある設備を通じて通信を行う場合は通信事業者が運用管理責任を負います。特に施設との接続点となる機器の責任の所在が通信事業者側にあるのか、医療機関側にあるのかを明確にしておく必要があります。医療機関と通信事業者との契約において運用管理実施責任が通信事業者側にある場合においても、医療機関側が最終的な管理責任を負います。医療機関が運用責任を負う設備を通じて通信を行う場合には、すべての管理責任は運営主体である療施設側が負うこととなります。

② チャネル・セキュリティの確保範囲

携帯電話回線を利用する際には外部の中継施設を経由するので、各端末から施設の入り口となる接続点までのチャネル・セキュリティの確保を確認する必要があります。

③ 接続点の機器の安全性

運用管理を行う通信事業者あるいは医療機関が、責任をもって安全性を保つよう運用する必要があります。

6.2. 安全管理ガイドラインに規定されるネットワークに対する安全管理への対

応

安全管理ガイドライン・システム運用編 13.1 には、医療情報システムで求めらる「セキュアなネットワーク」が求められおり、13. 1には構築・運用に関する遵守事項がまとめられています。無線通信技術を使って構築されるネットワークにおいても遵守する必要があるので、対応方法を確認する必要があります。表 6.1-2 に、安全管理ガイドライン 13 章の銃事項と表 6.1-1 の安全措置の対応を示します。

表6.1-2 セキュアなネットワークに対応する遵守事項

安全管理ガイドラインでの記載される遵守事項	表 6.1-1 安全措置との関連
13.1.1 セキュアなネットワークの構築	①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬
13.1.2 選択すべきネットワークのセキュリティ	共通。②③④⑤⑥⑦⑧⑨⑩⑪⑫
13.2 不正な通信の検知や遮断、監視	⑧⑨⑪
13.3.1　ネットワーク回線の暗号化	⑦⑩
13.3.2　情報に対する暗号化	⑦⑩
13.3.3　盗聴防止等	⑦⑩
13.4 無線 LAN の利用における対策	⑬

7. 新しい無線通信技術を利用するための方策

7.1. 無線技術を利用するための方策(概要)

本章では、4 章及び 5 章で説明した今後普及が見込まれる各無線通信技術のメリット、デメリット、導入・運用の注意点についてまとめます。すべてに勝る万能な無線通信技術はないので、利用範囲、メリット、デメリット、投入コスト、運用コスト等を比較し、各組織に適した方式を選定する必要があります。

7.2. 各無線技術の利用に関する方策

7.2.1. PHS

PHS は新製品の提供も終了しており、他の技術に移行する必要があります。

7.2.2. Wi-Fi

すでに Wi-Fi を導入している医療施設は多いと思われるので、導入への障壁は低いと考えられます。医療分野に限らず広く普及している技術のため、多くの端末や機器で利用可能です。そのほか必要となるアクセスポイント等の装置も、比較的安価に導入・運用することができます。他の無線技術よりも通信距離が短いため、多くのアクセスポイントが必要となる可能性が高く、電波干渉の影響を受ける可能性もあります。

最新の技術では、高速な通信が確保できるため、音声情報だけでなく、画像や映像を含む医療情報の伝送に利用できます。

医療機関の責任で導入することになるため、安全管理ガイドラインに従う技術対策を導入する医療機関側で検討した上で導入する必要があります。JAHIS セキュアトークン実装ガイド・機器認証編を参照して、適切な運営を設置した医療機関の責任で行う必要があります。構築に際しては、WPA3 等セキュリティの観点で安全性の高い技術を採用する必要があります。

7.2.3. LTE

実績のある技術であり、多くの端末が利用可能です。5Gに比べると容易に導入できるものと考えられます。ただし通信スピードは5Gに劣るため、大きな画像や映像の送受信には適さない場合があります。将来的には5Gへの移行が見込まれるため、移行を前提とした利用と割り切る必要があります。公衆回線を使うことにためので、安全性には特に配慮する必要があるセキュリティ対策を徹底し、データの暗号化や認証プロトコルの導入などを行うことで、安全な通信環境を確保することが重要です。

7.2.4. sXGP

PHS と同じ周波数帯の無線技術を用いているため、基地局の配置等を含めて PHS からの移行が比較的スムーズに行えるものと推測されます。

実効通信スピードはWi－Fi、LTE や5G には劣るので、画像や映像などの大領量のデータの送受信には向かない可能性が高いと考えられます。音声データと画像以外のデータの利用などに限定し、画像の利用は高速な通信技術を組み合わせるなど全体としての利用方法を検討したうえで導入する必要があります。

独自の通信システムなので、災害などの発生で公衆回線網がダウンした場合でも機能させることができます。

7.2.5. Local 5G

自前の無線設備等を持つこととなるため、導入の際のコストが課題となります。また、設置には基地局の免許が必要であり、運用に際しても知識を持った無線従事者取得者が必要となる等、他の技術にはないハードルが存在します。

5G の特性を活かして医療施設で使うサービス毎に使うデータの特性に合わせた最適な通信設定ができる可能性があるので、柔軟性は高く適切なデータ利用を加速する可能性があります。

LTE から移行する際には、周波数帯が異なるために通信距離が短くなるので、基地局・アンテナの再配置などの追加検討が必要となります。

7.2.6. Private 5G

通信事業者の設備を使い、運用も通信事業者が行うため、Local 5Gに比べて導入、運用のハードルは低いと考えられます。5Gの技術で高速な通信が可能ですが、通信事業者の設備を使うため、Local 5Gのようにアプリケーション毎に柔軟な通信設定をすることができるか否かは提供するキャリアに依存する形となります。

独自の通信システムではないので、災害の発生などで公衆回線網がダウンした場合には利用できなくなる恐れが高いと考えられます。

付録―1. 比較表

表 付 1-1 比較表

	PHS	LTE	Wi-Fi	sXGP	Local 5G	Private 5G
概要・特徴	・小型の携帯端末と基地局を利用 一般的なサービスは 2021 年 1 月に終了。テレメタリングサービスも 2023 年 3 月に終了。通信事業者とは独立の構内 PHS は当面運用可能	・(3G に比較して)高速・大容量・低遅延なデータ通信を提供 ・LTE と 4G は厳密には異なる。当初は 3G と 4G の間に LTE が生まれた。LTE の後継規格である LTE-Advanced と WiMAX2 が ITU で 4G として承認されているが、現在は LTE も4G に含まれる。	・近距離対応の無線技術を使用。IEEE 802.11 シリーズで規定され、Wi-Fi Alliance が準拠製品の認証を行っている。	・4GLTE の一部 DT-LTE を使った自営通信方式(専用) ・既存のスマートフォンが対応可能。工場や物流センターに設置したセンサーの利用等で IoT 化や DX 推進に活用することも可能 ・Wi-Fi に比べて電波干渉が少ない。 ・PHS の後継サービスとして期待されている。	・地域の企業や自治体等の主体が、自らの建物や知基地内で 5Gネットワークを構築(自営・専用) ・他のエリアで通信トラブルが発生しても影響を受けにくい。 ・5G の特徴である超高速、超低遅延、多数同時接続が利用可能	・通信事業者の通信網を利用したプライベートな5G ネットワーク(専用)。一般の 5Gとプライベート 5G の中間に位置する。 ・通信事業者が企業や自治体等の主体の敷地内に基地局の設備を設置して、ネットワークを構築し、運用する。 ・既存の事業者の設備を使い、ネットワークスライシングによる論理的な分離による提供(共有型)と主体者の敷地内に事業者の設備を設置する提供(専有型)がある。
主な用途	個人用通信、災害時の緊急通信	一般的なモバイル通信、携帯電話やモバ	自宅、企業、公共施設などのネットワーク接続	公共施設、商業施設、住宅地域などの密集	・工場、キャンパス、イベント会場などの	Local 5G と同じだが、通信事業者に提

		イルデバイスを対象とした通信		地域での通信インフラストラクチャ（内線電話の利用の他、IoT の無線通信インフラとしての利用を見込んでいる）	地理的領域内での通信、IoT デバイスの連携 ・超高速・大容量の特性を活かした映像系のアプリケーション ・超低遅延・多数同時接続の特性を活かした遠隔制御やコネクテッドカー、ロボット等の IoT	供するサービスに依存する。
周波数	1.9GHz 帯	700MHz, 800MHz, 900MHz, 1.5GHz，1.7GHz, 2GHz，　3.5GHz 帯	2.4GHz/5GHz/6GHz 帯	1.9GHz 帯（Band 39）	4 .6-4.9 GHz 帯（Sub 6） 28.2-29.1 GHz 帯（ミリ波）	3.7 GHz 帯(3.6-4.2 GHz) 4.5 GHz 帯（4.4-4.9 GHz） 28 GHz 帯（27.0-29.5GHz）
通信速度	最大 64Kbps	LTE 下り最大 326.4Mbps 上り最大 86.4Mbps 遅延時間 10ms LTE-A(4G) 下り最大 1Gbps 上り最大 100Mbps 遅延時間 1ms	5GHz 帯最大通信速度（論理値） Wi-Fi 4(11n): 600Mbps Wi-Fi 5(11ac): 6.9Gpbs Wi-Fi 6(11ax): 9.6Gbps	最大通信速度：上り 4Mbps/下り 12Mbps 10MHz 幅で上り 8Mbps/下り 28Mbps	28.3-29.1GHz 下り：5.2Gbps 程度 上り：1.9Gbps 程度 4.6-4.9GHz 下り：1.6Gbps 程度 上り：500Mbps 程度	Local 5G と同じだが、通信事業者に提供するサービスに依存する。
通信距離	基地局の出力 100-	数百 m 程度	一般には 2-30m 程度。	半径 100m	室内アンテナ：数十	Local 5G と同じだ

	200mW で、100-200m 、 出 力 500mW で 500m 程度		周波数が高くなると通信速度は向上するが、障害物やノイズの影響を受け安くなり通信距離は短くなる。		m 屋外アンテナ：数百 m	が、通信事業者に提供するサービスに依存する。
セキュリティ上のポイント	・データの暗号化 ・ユーザー認証	・エンドツーエンドの暗号化 ・SIM認証	・データの暗号化 ・WPA3 などの強力な暗号化プロトコルの使用	・エンドツーエンドの暗号化 ・SIM 認証	・エンドツーエンドの暗号化 ・SIM 認証 ・アクセス制御 ・データの隔離 ・増加する端末の管理・運用	Local 5G と同じだが、通信事業者に提供するサービスに依存する。
端末認証	・端末認証(確認済)	SIM 認証（RFC 4187 で規定される EAP-AKA 、RFC 5448 で規定される EAP-AKA’）	・IEEE 802.1x 等 ・ EAP-AKA, EAP-AKA’ による Wi-Fi SIM 認証もある	・SIM 認証	・SIM 認証 ・識別:IMS 番号 15 桁(MMC＋MNC＋MSIN)によって、どのネットワークに接続するかが決まる	Local 5G と同じだが、通信事業者に提供するサービスに依存する。
コスト	設備投資必要	設備投資不要	設備投資必要	設備投資必要 既に普及したLTEのため安価 電波利用料不要	設備投資必要 普及途上のため比較的高価 電波利用料が必要 資格を持った管理者が必要	設備投資不要（利用料に含まれる） 通信料が必要
運用負荷	中	小	小	中	大	小
メリット			・高速なので、音声だけでなく画像・映像の伝送にも使える。	・無線局の免許不要 ・既存の PHS の設置情報が使える可能性あり	・高速なので、音声だけでなく画像・映像の伝送にも使えそう。	・基地局の免許不要 ・運用管理は通信事業者が行う

デメリット	新たな導入はできない	将来5G に移行する前提の導入となる	・移動で切れやすい ・電波干渉による通信不安定性あり（特に2.4GHz 帯）	・通信速度がそれほどでもないので、画像の利用は難しそう ・対応した端末の種類が少ない	・基地局の免許必要。 ・運用管理が必要 ・障害物に弱い	・利用エリア制限がある ・障害物に弱い

付録―2. 参考情報

パーソナルハンディホンシステムの技術 渡辺文夫
https://www.jstage.jst.go.jp/article/itej1978/50/2/50_2_207/_pdf

sXGP とは
https://www.xgpforum.com/new_XGP/ja/007/sxgp.html

ローカル 5G 事業参入ハンドブック
https://www.ciaj.or.jp/ciaj-wp/wp-content/uploads/2023/01/handbook20230119.pdf

付録―3. 作成者名簿

作成者（社名／氏名 五十音順）

有馬　一閣	㈱NTTデータ
太田　英憲	三菱電機デジタルイノベーション㈱
梶山　孝治	富士フイルム㈱
喜多　紘一	（一社）保健医療福祉情報安全管理適合性評価協会（HISPRO）
酒巻　一紀	三菱電機デジタルイノベーション㈱
茗原　秀幸	三菱電機デジタルイノベーション㈱
谷内田　益義	特別委員

改定履歴		
日付	バージョン	内容
2025/07/31	Ver. 1.0	初版

（JAHISセキュリティ委員会報告書）
2025 年8月発行

JAHIS 医療情報システムにおける無線通信技術利用ガイド

発行元 一般社団法人 保健医療福祉情報システム工業会
〒105－0004 東京都港区新橋2丁目5番5号
（新橋2丁目MTビル5階）

電話 03-3506-8010 FAX 03-3506-8070