JAHIS

ＪＡＨＩＳ技術文書　２３－１０３

Japanese Association of Healthcare Information Systems Industry

ＪＡＨＩＳ
セキュアトークン実装
ガイド･機器認証編
Ver.1.1

２０２４年１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　セキュアトークン実装ガイド･機器認証編

ま　え　が　き

本ガイドは、医療機関等に設置された医療情報システムを構成する物理的個体識別可能なエンティティである端末や医療機器（以下、医療機器等と記す。）を、Wi-Fi によって施設内ネットワークに接続する目的で識別・認証するためのクレデンシャルを格納するセキュアトークの利用環境に対する機器及びセキュアトークンへの要求事項をまとめたものである。

情報技術発達によって、様々な機器を無線技術によって接続する例が増えてきている。医療機関等の施設内で利用する医療機器等においても、医療機器等の設置の容易性や可搬性を確保のために Wi-Fi によって施設内ネットワークに接続する例が見られるようになっている。「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)に述べられている通り、Wi-Fi を用いて施設内ネットワークを構築する場合には、不正なコンピュータ等の接続、DoS 攻撃、ネットワーク上のデータの傍受や改ざんを防がなければならない。本ガイドは、Wi-Fi によって医療機器を施設内ネットワークに接続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不正アクセス対策及び端末認証によって不正端末の接続を防止する対策並びにその実例を示すとともに、そこで利用されるセキュアトークンに関して、ユースケース、セキュアトークンの要件、運用上の要件、相互運用の要件を明らかにしている。

JAHIS は産業界の業界団体として、医療機関等のネットワークの安全性を図るためには医療機器等の識別・認証の基盤の普及、セキュアトークンの実装・相互運用性の確保を図ることが重要な役割であるとの判断から、JAHIS 会員各社の意見を集約し、「JAHIS セキュアトークン実装ガイド・機器認証編」を JAHIS 技術文書としてまとめたものである。本ガイドで扱う医療機器等の識別・認証を行う要件は、参照規格及び技術動向に合わせて変化する可能性がある。JAHIS としても継続的に本技術文書のメンテナンスを重ねてゆく所存であるが、本ガイドの利用者はこのことにも留意されたい。

本ガイドが、医療情報システムの安全な運用の促進に貢献できれば幸いである。

２０２４年１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　＞＞

本ガイドは関連団体の所属の有無に関わらず、ガイド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。ただし一部の改変を伴う場合は個々の責任において行い、本ガイドに準拠する旨を表現することは厳禁するものとします。

本ガイドならびに本ガイド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、本ガイド作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目　　次

1. 適用範囲

医療サービスを行う医療機関等に設置された医療情報システムを構成する物理的個体識別可能なエンティティである端末や医療機器（以下、医療機器等と記す。）を Wi-Fi によって施設内ネットワークに接続する目的で識別・認証するためのクレデンシャルを格納するセキュアトークンに関して、

- セキュアトークンを利用するユースケースを明らかにする。
- セキュアトークンの要件を明確にし、必要な機能を定める。
- セキュアトークンを利用する際に必要となる相互運用性を確保するための仕様を定める。
- セキュアトークンを利用する際に要求される運用上の要求事項を明らかにする。
- セキュアトークンを利用して医療機器等の管理を行う実例を示す。

識別及び認証に用いるクレデンシャルの内容は規定しない。

2. 引用規格・引用文献

厚生労働省　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 システム運用編, 令和 5 年 5 月

厚生労働省　「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」に関する Q&A、令和 5 年 5 月

IEEE Std 802.1X-2020 - *IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control*, Jan 2020

RFC 2315, PKCS #7: *Cryptographic Message Syntax Version 1.5*, March 1998

RFC 7292, PKCS #12: *Personal Information Exchange Syntax v1.1*, July 2014

RFC 2986, PKCS #10: *Certification Request Syntax Specification Version 1.7*, November 2000

保健医療福祉情報システム工業会　セキュアトークン実装ガイド　2015 年 2 月

総務省　「企業等が安心して無線 LAN を導入・運用するために」　平成 25 年 1 月

3. 用語の定義

エンティティ

情報システムを利用するクレデンシャルの対象となる主体。医療分野であれば、患者や医療従事者等の自然人の他、一定の権限をもった組織の代表者や医療機関等の組織、機能範囲によって決められる医療機器等のネットワークに接続される医療機器等が該当する。

クレデンシャル

認証においてエンティティの身元と関連する属性を識別するための情報オブジェクト。一般的なクレデンシャルの例としては、X.509 公開鍵身元識別情報証明書、X.509 属性証明書等がある。

トークン

クレデンシャルを格納するハードウェア。本ドキュメントにおいては、ソフトウェア技術によって仮想的にトークンを実現したソフトウェアトークンと呼ぶものも含む。

セキュアトークン

クレデンシャルを格納し一定の物理的耐タンパー性をもったデバイストークン。外部からの要求に従っ

てクレデンシャルへのアクセス、暗号演算等を行って結果を返すことによって、識別及び認証の機能の一部を構成する。

識別

情報システム内で、エンティティを一意に特定するための情報の有効性を検証するプロセス。

認証

電子的な手段によって利用者が情報システムに提示する利用者の身元識別情報に関する信用を確立するプロセス。

ノード

エンティティがネットワークに接続される点。

機器認証

ネットワークに接続された機器の認証。物理的な医療機器等のネットワーク接続の確認に対応する。

ノード認証

ネットワークに接続されたノードの認証。論理的なノードのネットワーク接続の確認に対応する。

4. 略語

このガイドでは、次の略語を用いる。

CA	認証局（Certification Authority）
IHE ITI-ATNA	IHE - IT インフラストラクチャ - 監査証跡とノード認証 (IHE - IT Infrastructure - Audit Trail and Node Authentication)
PKI	公開鍵基盤（Public Key Infrastructure）
Wi-Fi	略語ではない。Wi-Fi Alliance が命名した用語
AP	アクセスポイント(Access Point)
PSK	事前共有鍵（Pre-Shared Key）
RADIUS	Remote Authentication Dial-In User Service
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-PEAP	Extensible Authentication Protocol Protected EAP
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
AES	Advanced Encryption Standard

5. 概説（機器認証とノード認証）

5.1. 機器認証の必要性

医療情報システムにおいては、機微な情報を取り扱うために、安全の確保された機器、サービスの間で情報交換を行う必要がある。

安全性が確立されている組織内の機器やシステムが他の機器やシステムに接続する場合には、接続する相手が信頼できる組織内の機器やシステムであることを確認する必要がある。そのためには、接続元と接続する医療機器等やサービスの間で相互にクレデンシャルによって識別して信頼性を確認する機器認証が必須となる。特に機微な情報を取り扱う医療情報システムにおいては、接続を要求しているエンティティが組織の管理下にある信頼できる医療機器等であることを確認することが重要となる。

1）内部環境の認識

多様な機器が医療機関等の施設内ネットワークに接続されるようになってきている。医療情報システムやシステムを利用する端末だけでなく、計測機器、撮影機器、モニタ端末、各種サーバ等が接続されている。

また、有線による接続だけでなく、無線技術を使ったネットワーク接続も普及してきている。今後も病棟

で利用するタブレット端末だけでなく、ポータブル医療機器も Wi-Fi 等の無線によって施設内ネットワークに接続するケースが増えると予想される。

さらに、有線あるいは無線の接続の形態を問わず、ネットワークに接続した医療機器等の管理も求められるようになってきている。不正な端末の施設内ネットワーク接続による不正アクセスを防ぐことは、安全管理上の重要な課題の１つである。

２）外部環境の認識

標的型メール等、サイバー攻撃による内部情報流出が報道されている。重要なデータに対する不正アクセスを防止することは、機微な情報を取り扱う医療機関等においては重要なこととなっている。

不正アクセスの防止、不正機器の接続防止を行うためには機器の識別と確認が必要となる。そのためには医療機器等の識別・認証は有効な手段となる。安全管理ガイドラインは、１３．ネットワークに関する安全管理措置における遵守事項において、一般的なネットワークに対する安全措置として以下のように説明している。

> 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。採用する認証手段は、PKI による認証、 Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。

また無線 LAN（Wi-Fi）に関しては、遵守事項において以下のように説明している。

> 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。
> ー適切な利用者以外に無線 LAN を利用されないようにすること。例えば、 ANY 接続拒 否等の対策を実施すること。
> ー不正アクセス対策を実施すること。 例えば MAC アドレスによるアクセス制限 を実施すること。 ただし、MAC アドレスは詐称可能で あることや、最近のモバイル 端末においてはプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることから、MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。
> ー不正な情報の取得を防止するため、 WPA2 AES 、WPA2 TKIP 等により通信を暗号化す ること。
> ー利用する無線 LAN の 電波 特性を勘案して、通信を阻害しないものを利用すること 。

アクセス先の識別を確実に行って不正アクセスを防止すること、すなわち医療機関等が管理している機器であることを確認するためには、医療機関等が発行したクレデンシャルによる医療機器等の識別・認証が有効である。

5.2. 機器認証とノード認証

医療情報システムにおいては、機微な情報を取り扱うために、安全の確保された機器あるいはノード間で情報の交換を行う必要がある。ここで機器とは、ネットワークに接続され、ネットワークを介して通信を行うネットワーク構成要素（例：コンピュータ、ルータ、サーバ等）であるとともに、物理的な存在と１対１に対応付けられたものとする。ノードは同様にネットワークを介して通信を行うネットワーク構成要素であるが、論理的な存在であり、必ずしも物理的な存在と１対１に対応付けられるわけではない。

ネットワークに接続され物理的な存在が明らかである医療機器等において、接続先の医療機器等を接続に先立って識別・確認する場合には機器認証を用いることになる。安全性が確立されている組織内のエンティティが組織外のエンティティと接続する際に接続に先立って相手が信頼できる接続先であることを確認する

場合には、ノード認証を用いることとなる。実際の認証を行う手順や技術は同様のものを用いることになるが、単一のセキュリティドメインの中で物理的な存在が明らかな医療機器等と通信を行う場合には機器認証、異なるセキュリティドメイン間で通信を行う場合には物理的な存在を必ずしも確認することはできないので接続先のノードの信頼性をノード認証によって確認することになる。

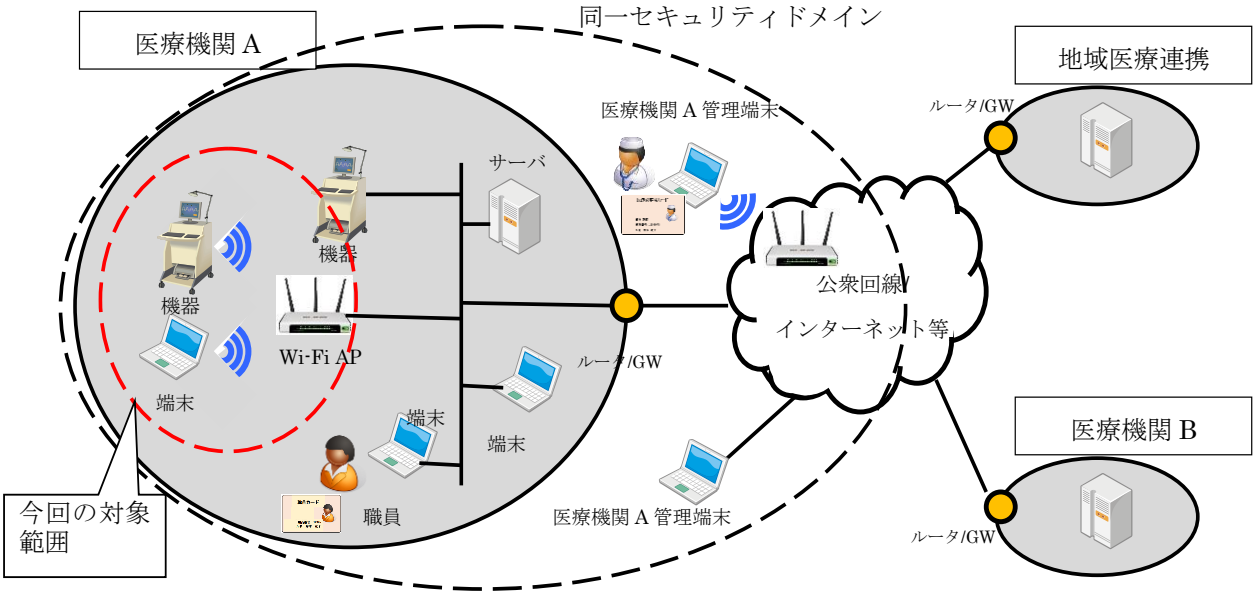

図１　ノード認証モデル

ノード認証に関しては、「セキュアトークン実装ガイド」で説明している。ノード認証によって接続するのは、組織の入り口になるルータや GW である。これはノードに対応する機器が故障などによって入れ替わったとしても同じ組織として認証される必要があるためで、ノード認証が求められる例となる。図１にその概要を示す。

6. ユースケース

6.1. 前提となるモデル

医療機関等では、さまざまな医療機器および端末などの医療機器等が Wi-Fi を使用している。医療機関等で使用されている医療機器等を Wi-Fi AP にアクセスするモデルを想定する。Wi-Fi でアクセスする全ての機器は、医療機関等で物理管理が適切に実施されていることを前提とする。図２に今回の前提となるモデルを示す。対象は Wi-Fi で医療機関内のネットワークに接続される医療機器等とし、有線にて医療機関 A 内のネットワークに接続される医療機器等は対象外である。また、医療機関 A からルータ/GW を経由して、公衆回線/インターネット等にも接続されることもあり、それら医療機関の外にある医療機器等も対象外である。

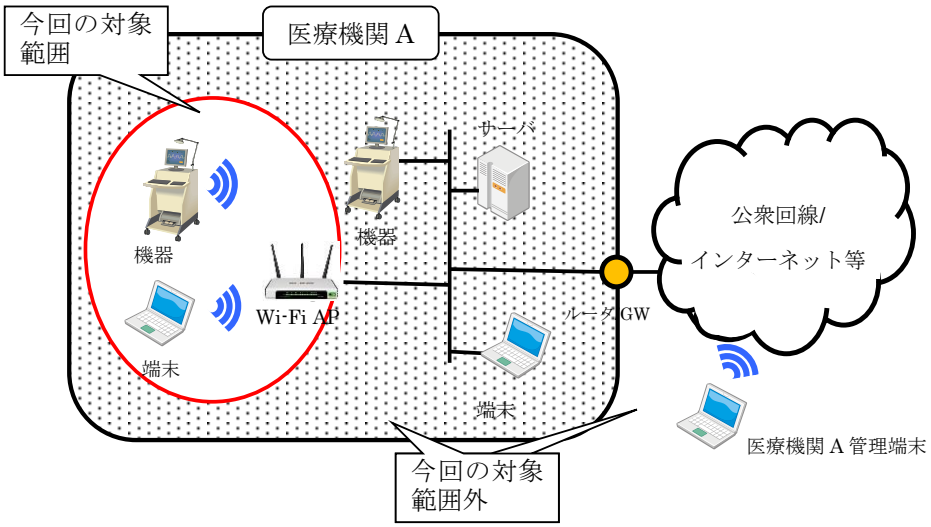

図２　前提となるモデル

6.2. 想定される脅威とその対策

[脅威]

十分なセキュリティ対策が施されていない Wi-Fi 環境では、医療機関等の管轄下にない端末が接続された場合、次のような脅威にさらされる（図３参照）。

- ネットワーク感染型のウイルスの拡散と医療機関等内の機器への感染
- サーバ上のデータの搾取、改ざん、消去が行われる。
- 医療業務の遂行に必要なデータを持つサーバ等にランサムウェアが感染する。
- ネットワーク機器、サーバに過負荷をかける攻撃を行い、業務を妨害する。
- （Wi-Fi 用の DoS 攻撃ツール）
- 疑似 AP（無線ハニーポット）に正規の端末を接続させ通信を傍受して院内のリソースに
- アクセスするための認証情報等を搾取する。（ノート PC による不正 AP が可能）
- AP のブロードキャストによる SSID の漏えい（収集）

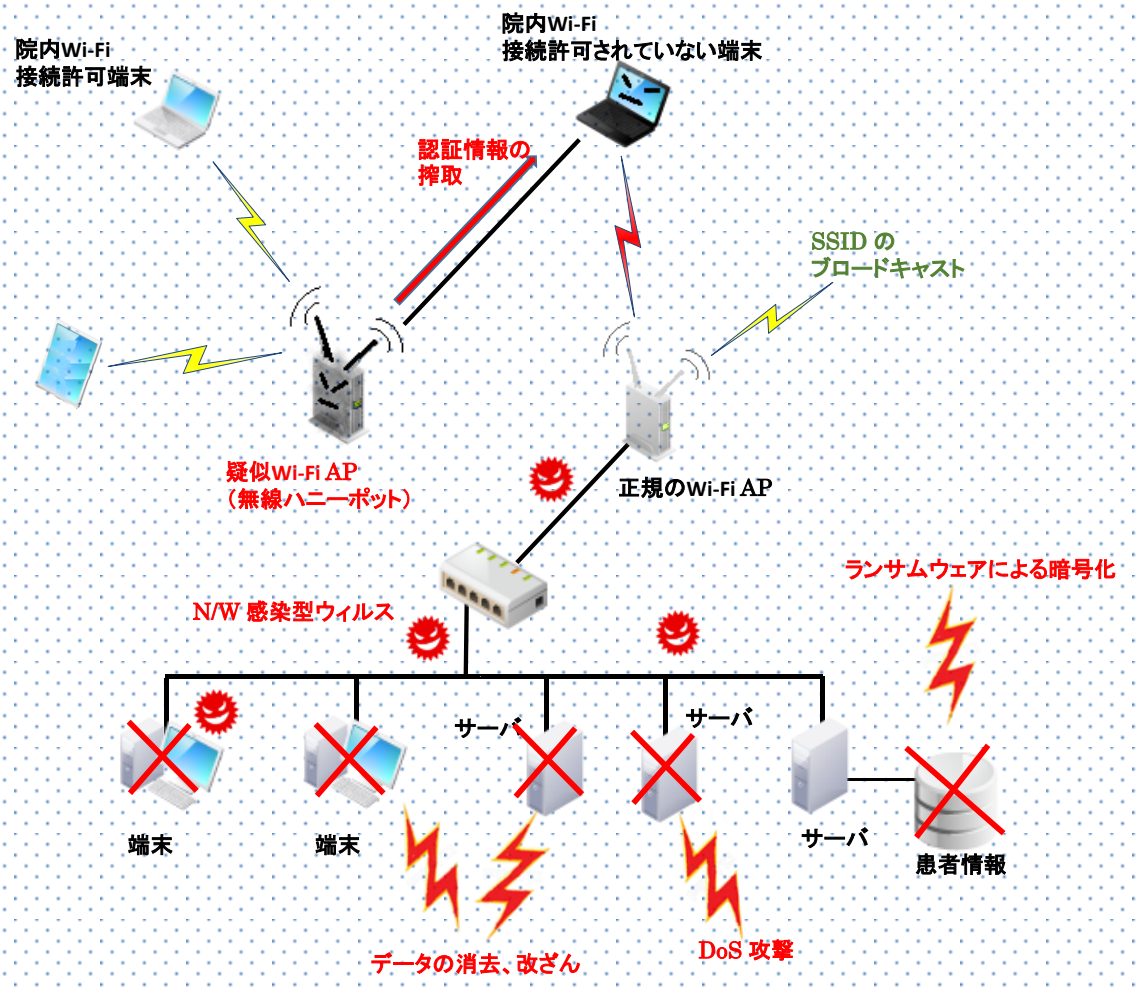

図３　脅威にさらされた Wi-Fi 環境

[対策]

基本的には安全管理ガイドライン 13 章の遵守事項⑬を順守すれば最低限の対策は可能である。ただし、リスクをより減らすためには総務省発行の「企業等が安心して無線 LAN を導入・運用するために」に書かれている通り、利用者グループ及び利用する資産の範囲の性質に応じて、無線ＬＡＮに採用する認証方法、暗号化方式等を含めた情報セキュリティ対策を実施することが望ましい。

具体的には下記のようなセキュリティ対策が施されていると不正に Wi-Fi 接続しようとする端末があっても排除され、セキュアな環境を保つことができる（図４参照）。

- SSID を非表示にする。（ステルス ID）
- ANY 接続を拒否する。
- MAC アドレスによるフィルタリングを行う。
- WPA2/WPA3-Personal(AES)等十分な強度を持った暗号化を適用する。
- Wi-Fi 接続の認証にセキュアトークンを使用する。（RADIUS 認証）
- DHCP サーバで MAC アドレスと IP アドレスの紐づけを行う。

詳細については 7 章、運用モデルについては 9 章を参照のこと。

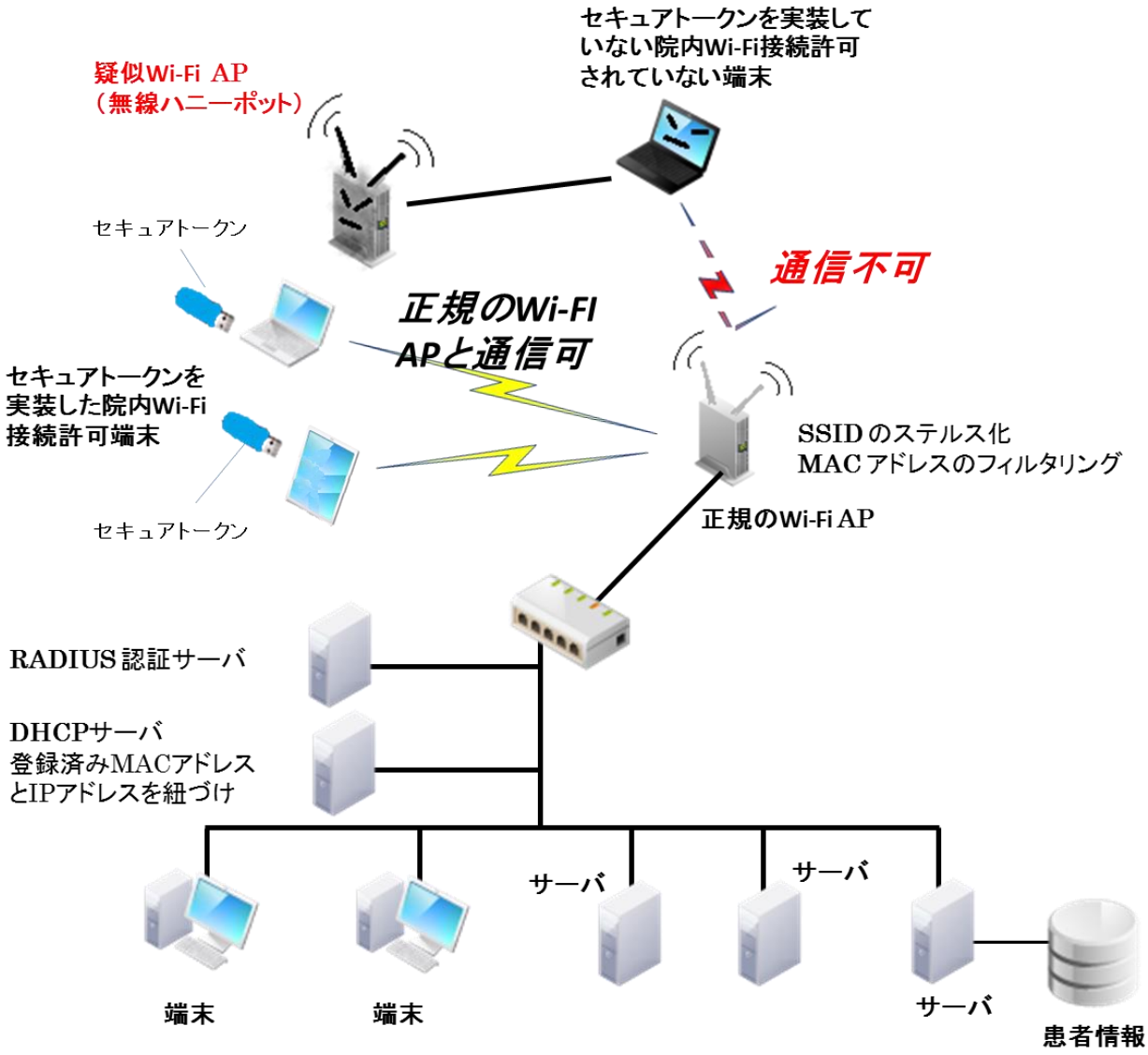

図４　セキュアなWi-Fi環境

6.3. Wi-Fiで接続する機器

医療機関等においてWi-Fiを利用する具体的な例としては、以下のものが挙げられる。

- 病棟などにおけるノートPCやタブレット端末の利用
  看護師等がベッドサイドにてケア等をする際にノートPCやタブレット端末をWi-Fi接続して医療情報システムにアクセスし、患者情報を参照したり、ケアの結果を入力したりするなどのニーズがある、
- ポータブルな計測機器等の利用
  持ち運び可能な心電計等から Wi-Fi を用いて計測データ等を医療情報システムに伝送するなどのニーズがある
- 患者と一緒に移動する各種計測機器の遠隔監視（テレメータ等）
  心拍数や呼吸数などをモニタリングする医療用テレメータ等を Wi-Fi を用いて集中管理システムと連携させることにより適切なケアを可能にするニーズがある
- 配線が難しいエリアでの通信の利用

・　手術室など配線が難しいエリアにおいて Wi-Fi を用いた医療情報システムの参照や入力、医療機器等のネットワーク接続などのニーズがある

7. 機器への要求

7.1. はじめに

Wi-Fi に対応した機器は、Wi-Fi Alliance の定める相互接続性認証試験を受けて Wi-Fi 認定を取得しており、試験に含まれる方式（IEEE802.1n, WPS2.0 等）での Wi-Fi の相互接続性は保証される。つまりセキュリティ設定を始めとする接続のパラメータ等を正しく設定すれば、確実に目的とする AP に接続することが可能となる。本章では、まず想定する基本構成を説明し、Wi-Fi を用いて医療機器等をネットワークに接続する際に最低限必要となる設定、確実な機器認証を行うために必要となる設定、そしてクレデンシャルの管理に必要となる共通のインタフェースについて説明する。

医療機関等において Wi-Fi を通じて医療機器等を利用する場合には、これらを念頭に環境を設定すると共に、対応した医療機器等を導入する必要がある。また、Wi-Fi によって接続する医療機器等はこれらの仕様に対応する必要がある。

7.2. 基本構成

医療機器等を、Wi-Fi を用いて医療機関等の施設内のネットワークに接続するためには、医機機器等の認証を行う必要がある。多くの Wi-Fi 対応機器で採用されている機器認証のためのプロトコルは IEEE 802.1x(以降 802.1x と)である。802.1x を利用するには、以下のような 3 つのコンポーネントが必要になる。

(1) EAP-TLS(RFC 5216), EAP-PEAP 等の認証プロトコル及び WPA2/WPA3 等をサポートした医療機器等
(2) EAP(RFC 3748)及び WPA2/WPA3 等をサポートした Wi-Fi AP
(3) EAP-TLS, EAP-PEAP 等の認証プロトコルをサポートした RADIUS サーバ

図 5 にその概要を示す。

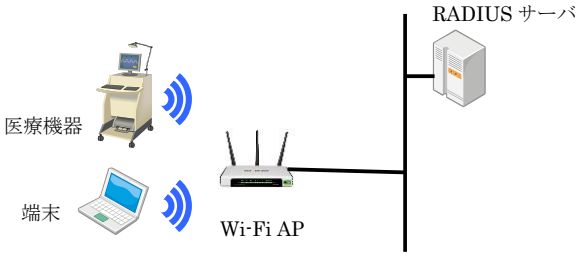

図 5　Wi-Fi で接続する機器等の基本構成

医療機関等の施設内ネットワークに Wi-Fi によって接続する医療機器等は、例えば PC、モバイルデバイス、医療機器が考えられるが、ここでは、医療機器を中心に説明する。

安全管理ガイドラインにおいては、Wi-Fi 接続する場合の遵守事項として次の対策を行うよう求めている。

－適切な利用者以外に無線 LAN を利用されないようにすること。例えば、 ANY 接続拒 否等の対策を実施すること。

－不正アクセス対策を実施すること。 例えば MAC アドレスによるアクセス制限 を実施すること。 ただし、 MAC アドレスは詐称可能で あることや 、最近のモバイル 端末においてはプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることから、 MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。

－不正な情報の取得を防止するため、 WPA2 AES 、 WPA2 TKIP 等により通信を暗号化すること。
－利用する無線 LAN の 電波 特性を勘案して、通信を阻害しないものを利用すること 。

不正アクセス対策として最低限度の要求としては、MAC アドレスによるアクセス制限が求められている。7.3 では、その条件を満たす場合の機能と設定を説明する。留意事項に対処するためには、総務省・「企業等が安心して無線 LAN を導入・運用するために」に書かれている通り、利用者グループ及び利用する資産の範囲の性質に応じて、無線ＬＡＮに採用する認証方法、暗号化方式等を含めた情報セキュリティ対策を実施する必要がある。7.4 では、そのセキュリティ対策を実現する場合の機能と設定を示す。

7.3. 最低限の不正アクセス対策を実現する機能及び設定

7.3.1. 前提条件

比較的小規模の医療機関等であって、Wi-Fi AP の数が限定されていて接続される医療機器等の数もそれほど多くなく、医療機器等及び Wi-Fi AP それぞれに対して個別の設定管理可能である環境を想定する。

7.3.2. 医療機器等の設定

1）Wi-Fi AP の設定

医療機器等及び Wi-Fi AP は、Wi-Fi 認定を受けている製品であって、以下の設定ができることが必要になる。

- SSID を非表示にする。
- ANY 接続を拒否する。
- WPA2/WPA3-Personal(AES)等十分な強度を持った暗号化を適用する。
- SSID あるいは Wi-Fi によって接続する医療機器等の MAC アドレスによるアクセス制限を行う。

2）医療機器等の設定

Wi-Fi 認定を受けている医療機器等は、最低限必要となる機能はすべて備わっている。そのため、以下の設定を正しく行う必要がある。

- Wi-Fi AP に設定した SSID を適応する。
- WPA2/AES 等 Wi-Fi AP に設定した暗号化を適用する。

7.3.3. 運用及び留意事項

7.3.2 で説明した設定は、第三者のデバイスが無条件に接続されることを防ぐ、あるいは関係者の未登録デバイスが不正接続されるのを防ぐなど、比較的軽微なリスクに備えるセキュリティレベルと理解すべきである。MAC アドレスの本来の役割はネットワーク上で機器を特定するために設定されている識別子であって、ネットワーク通信に用いるための識別子の情報は暗号化の対象にならず、パケットキャプチャを実行すれば接続が許可されている通信可能な端末の MAC アドレスを容易に知ることができる。また MAC アドレスをソフトウェアによって変更することも比較的容易であるため、なりすましの対策にはならない。悪意ある攻撃者からの侵入に対抗する方策にはならないので、悪意ある攻撃を防ぐためには採用すべきでない。

それでもなお利用する場合には、医療機器等の導入及び廃棄に応じて Wi-Fi AP に登録されている MAC アドレスの棚卸、具体的には使わなくなったアドレスの削除等の運用対策を合わせて実施する必要がある。

7.4. 端末認証によって不正端末の接続を防止するための機能及び設定

7.4.1. IEEE802.1x の基本

総務省・「企業等が安心して無線 LAN を導入・運用するために」においては、許可されていない端末が無線 LAN に接続されることを防止する対策として、端末認証が行える IEEE802.1X 認証を利用することが適

当であると説明されている。

802.1x の基本的な仕組みを図６に示す。

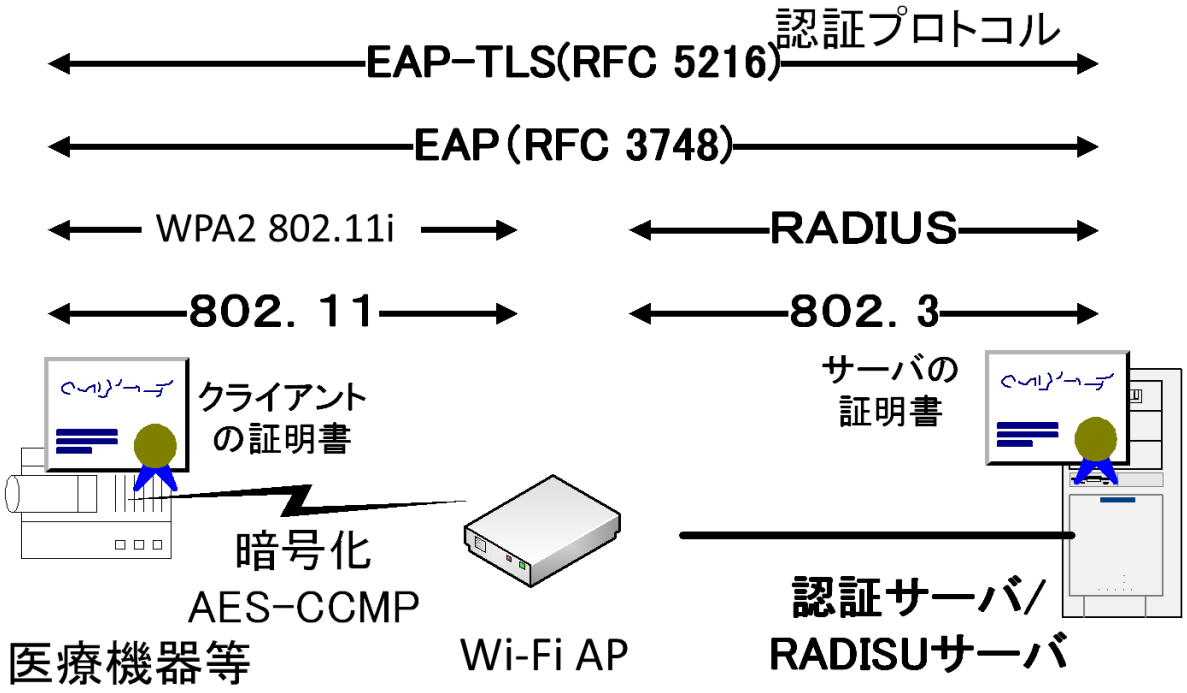

図６　802.1x の基本的な仕組み

図６において医療機器等は、Wi-Fi AP 経由により医療機関等の施設内ネットワークに IP 接続することになるが、この際、医療機器等の識別・認証が行われる必要がある。

この医療機器等の認証には、802.1x のフレームワークが利用されるが、この 802.1x における認証では、医療機器等の認証を Wi-Fi AP が直接行う訳ではない。医療機器等の認証は、医療機関等の施設内ネットワークに設置されている認証を行う RADIUS サーバと医療機器等の間において EAP-TLS などの認証プロトコルにより行われる。

RADIUS サーバは、医療機器等の認証結果を Wi-Fi AP への通知し、その認証結果により Wi-Fi AP は、医療機器等による医療機関等の施設内ネットワークへの IP 接続を許可する。

RADIUS サーバは、EAP-TLS,EAP-PEAP 等の認証プロトコルをサポートが必要になるが、こうした RADIUS サーバは、多くの製品が存在する。

次に、認証プロトコルとして EAP-TLS をサポートした 802.1x の実装のイメージを図７に示す。

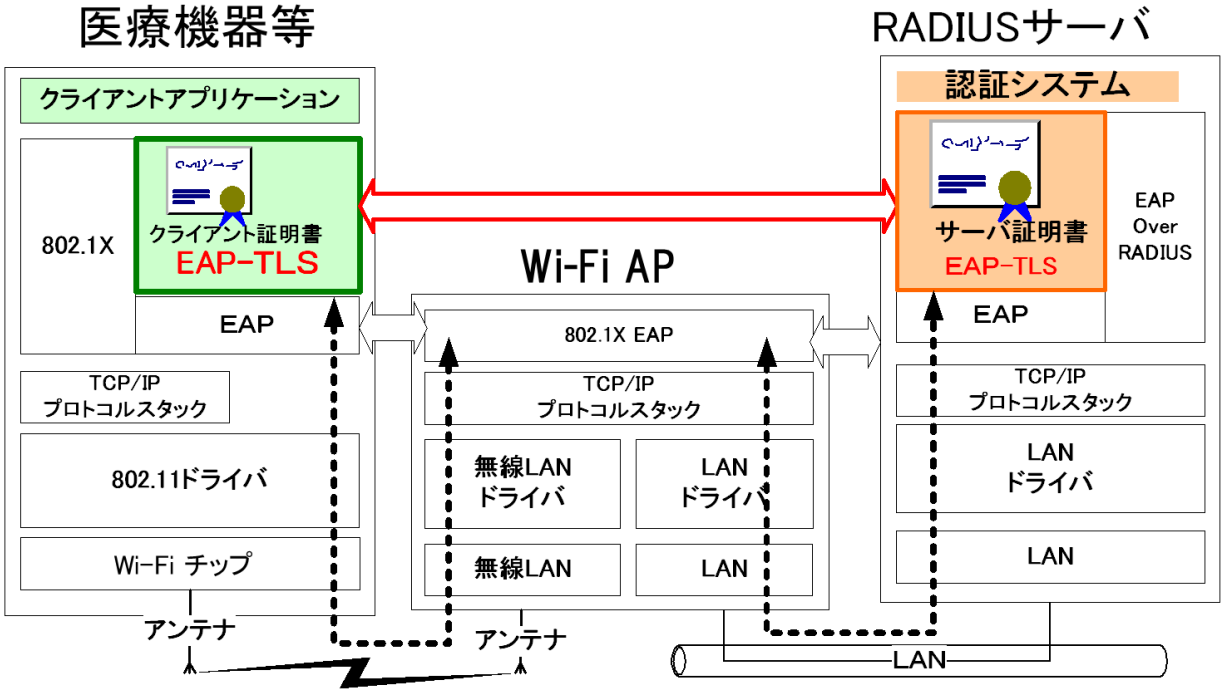

図７　802. 1x の実装イメージ

認証プロトコルに EAP-TLS を使う場合、医療機器等は、クレデンシャル（クライアント証明書及び秘密鍵）を扱える必要があり、また、このクレデンシャルを使った認証プロトコル（EAP-TLS）が実装される必要がある。

7.4.2.　EAP-TLS,EAP-PEAP 等をサポートし Wi-Fi AP に接続する医療機器等

802.1x を利用して医療機関等の施設内ネットワークに接続する医療機器等は、EAP（RFC 3748 Extensible Authentication Protocol）をサポートする必要があり、また、EAP 上における認証プロトコルである EAP-TLS(RFC 5216), EAP-PEAP 等をサポートする必要がある。

EAP-TLS, EAP-PEAP 等の認証プロトコルを利用する場合、医療機器等は RADIUS サーバの認証を行う必要があり、そのため RADIUS サーバ証明書の検証を行う。RADIUS サーバの認証は、実質的に Wi-Fi AP の認証になるが、これは Wi-Fi AP のなりすまし防止の対応になる。医療機器等は、この RADIUS サーバの認証を行うためには、RADIUS サーバ証明書を発行した CA のルート証明書を医療機器等の内部に持つ必要がある。医療機器等はこのルート証明書を信頼点として RADIUS サーバの認証を行う。

認証プロトコルとして EAP-TLS を利用する場合は、この医療機器等においてクレデンシャル（機器証明書及び秘密鍵）を扱う必要がある。一般的には、RADIUS サーバ証明書を発行した CA からこの医療機器等への機器証明書を発行することになる。

医療機器等と Wi-Fi AP 間は、暗号化がサポートされるべきであるが、これには、医療機器等において 802.11i/WPA2/WPA3 のサポートが推奨される。

EAP-TLS では、動作環境により、利用する暗号アルゴリズムを切り替えることができるが、医療機器等の実装においては、RSA2048bit、SHA-256 といった十分な暗号強度を持った暗号アルゴリズムをサポートする必要がある。

7.4.3.　EAP に対応した Wi-Fi AP

Wi-Fi AP は、802.1x/EAP をサポートしたものを利用する必要がある。Wi-Fi AP は、一般的には、

EAP-TLS,EAP-PEAP 等の認証プロトコルを直接扱うわけではない。Wi-Fi AP と RADIUS サーバ間は、認証、暗号化などが必要になるが、これには RADIUS プロトコルが利用される。
医療機器等と Wi-Fi AP 間は、暗号化がサポートされるべきであるが、これには、Wi-Fi AP において 802.11i/WPA2/WPA3 のサポートが推奨される。

7.4.4. EAP-TLS,EAP-PEAP 等に対応した RADIUS サーバ

802.1x を利用する場合、EAP 及び EAP-TLS,EAP-PEAP 等の認証プロトコルをサポートした RADIUS サーバが必要になる。

EAP-TLS, EAP-PEAP 等の認証プロトコルをサポートするためには、RADIUS サーバのためのクレデンシャル（RADIUS サーバ証明書及び秘密鍵）のサポートが必要になる。

認証プロトコルとして EAP-TLS を利用する場合は、この医療機器等の機器証明書の検証を行う必要がある。そのため機器証明書を発行した CA のルート証明書を RADIUS サーバ内に格納する必要がある。

7.5. 機器のインタフェース要件

7.5.1. セキュアトークンとクレデンシャルのインタフェース

Wi-Fi に関連するインタフェースに関しては、Wi-Fi 認定を取得することで満たされるため、本節では、セキュリティを確保するために必要となるインタフェースの説明を行う。

7.4 で説明した医療機器等の確実な認証を行うためには、各医療機器等が識別・認証を行うためのクレデンシャルを保持する必要がある。医療機器等の内部に保持するクレデンシャルを安全に管理するためには、セキュアトークンが必要となる。クレデンシャルは外部で生成され、機器内のセキュアトークンに格納されるため、セキュアトークンとのインタフェースが重要となる。医療機器等の確実な認証を行う際に考慮すべきクレデンシャルの種類は次の通りとなる

- ルート証明書
- 医療機器等の証明書。認証鍵と証明書を外部で生成して設定する場合と、鍵は医療機器等の内部で生成し、証明書を外部で生成する方法がある。

医療機器等にクレデンシャルを設定するインタフェースは、オンラインで CA と通信を確立してクレデンシャルを生成・格納する方法と、USB 等の媒体を通じて CA が生成したクレデンシャルを医療機器等に格納する方法の 2 種類存在する。オンラインによる設定を行うのか、オフラインによって設定を行うのかはシステムの構築や運用によって異なるので、本書においてはオンライン/オフライン共通となるクレデンシャルのフォーマットについて説明する。

RADIUS サーバ及び医療機器等に対する証明書の発行過程、及び CA の運用等は本書の範囲外とする。

7.5.2. 信頼できる証明書の登録（必須）

本節では、RADIUS サーバを確認するための証明書の設定のインタフェースを説明する。802.1x で接続するサーバの認証を行う際に、接続先のサーバの信頼性を検証するサーバの証明書、及びそのルート証明書が必要となる。

証明書のフォーマットは PKCS#7（RFC 2315）に従う必要がある。単体の証明書を取り扱う場合には、DER encoded binary X.509 あるいは Base 64 encoded binary X.509 フォーマットに従う必要がある。

設定するルート証明書は、前記フォーマットに従った証明書を電子ファイルで受け取り、医療機器等に設定することになる。そのため、ファイル名に使用する文字コード及び範囲、入力方法に配慮する必要がある。

7.5.3. クレデンシャルの格納（必須）

本節では医療機器等に対して CA が発行した秘密鍵及び公開鍵証明書を含むクレデンシャルを格納するためのインタフェースを説明する。

クレデンシャルのフォーマットは、PKCS#12（RFC7292）に従うものとする。CA から発行される医療

機器等のクレデンシャルはPKCS#12に従ったファイルとして受け渡されるので、ファイル名に使用する文字コード及び範囲、入力方法に配慮する必要がある。また、PKCS#12 に従ったファイルはパスワードによって保護されているので、パスワードに使用する文字コード及び範囲、入力方法に配慮する必要がある。

7.5.4. 機器で鍵を生成する場合の証明書要求（オプション）

医療機器等が生成した公開鍵に対して CA で公開鍵証明書を発行し、機器に公開鍵を設定するためのインタフェースを説明する。

鍵ペアを医療機器等の内部で生成し、公開鍵の生成を CA に PKCS#10（RFC2986）に従った証明書要求を送る。要求には医療機器等を識別する情報と選択した公開鍵が含まれる。要求が成功すると、CA が医療機器等に公開鍵証明書を送りかえす。医療機器等は CA より証明書を受け取り、医療機器等の内部に取り込む。

7.6. 適切なログの作成と収集

適正な接続が確保されているかを検証するためには、適切なログを作成していることが重要である。安全管理ガイドラインQ＆Aにおいては、シス８章第⑥条への質問「シQ－21 IoT 機器を含む医療情報システムの接続状況や異常発生を把握するためにはどのような方法あるか。」に対して、「A IoT 機器・医療情報システムそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録してください。」と回答されている。また総務省の「企業等が安心して無線LANを導入・運用するために」においても、運用で実施すべき事項として「ログの収集・保存・分析」が挙げられている。適切なログを残すためには、接続されたIoT機器を含む個々の機器を確実に識別し、医療機関等にて管理している医療機器等であることを確認すること必要である。

Wi-FiはAPなど有線LANとは異なる機器を使用するが、それらの機器に含まれる情報を識別情報として使用することが考えられる。しかし、詐称等の問題から機器の識別を確実に行っているとは言えず、医療機関等にて管理している識別用の管理IDを利用することが対策となる。厳密な管理が必要とされる環境では、機器認証時に使用されるクレデンシャルの情報を識別用の管理IDとして用いるとより、確実な識別が可能となる。

この識別用の管理IDがログに記載されることで、適正な接続が確保されていることが確認できる。ログは、障害対応といった従来のシステムの稼働に関する目的に加えて、不正アクセスや情報漏えいといったセキュリティの問題に関する目的でも必要とされてきている。信頼に足るログは監査対応でも使用でき、適正な運用がされていることを立証する際の基本（根幹）となる。

今回のモデルではクレデンシャルとして電子証明書を使用し、AP 経由で RADIUS サーバに接続し認証されるため、AP と RADIUS サーバ双方でのログ取得が必要となる。AP ではアクセス日時、ユーザ ID、AP の IP アドレスや MAC アドレス、RADIUS サーバでは認証に使用した電子証明書のサブジェクト等に含まれている情報（Common Name や Serial Number 等）などがログに記載されるべき情報となる。

8. セキュアトークン

8.1. 機器認証とセキュアトークン

機器の識別及び認証を適切に行うためには、機器に発行されたクレデンシャルで行うのが確実である。各医療機関等の管理責任で機器を唯一に識別するためのクレデンシャルを発行し、機器と結びつける。IHE ITI TF-1では、双方向の証明書に基づいた機器認証を各ノード間の接続のために使用することが要求されている。

トークンは、組織、人、機器等の各エンティティに対して発行されたクレデンシャルを格納し、識別・認証の際に利用可能にするものである。信頼のおける認証を行うためには、信頼できるクレデンシャルを利用するとともに、安全性の確保されたトークンを利用する必要がある。

図８は、医療機器等に埋め込まれたトークンの例である。識別・認証の際には、機器内に IC チップ等の形態で組み込まれたトークンに格納されたクレデンシャルによって機器認証を行う。図９は、トークンが機器から取り外し可能なトークンの例である。医療従事者等の自然人がノードとなる場合には、人に対して発行されたクレデンシャルを例えば IC カードに格納して端末に挿す（結びつける）ことによってクレデンシャルを利用する。機器の場合には、機器に対して発行されたクレデンシャルを、例えば USB トークンに格納して機器に挿す（結びつける）ことによってクレデンシャルを利用する。図 10 はハードウェアを使わず、暗号やアクセス制御などソフトウェアの技術によってクレデンシャルを保護する例である。標準的な OS では、クレデンシャルを保護する機能が組み込まれているのが普通となっている。

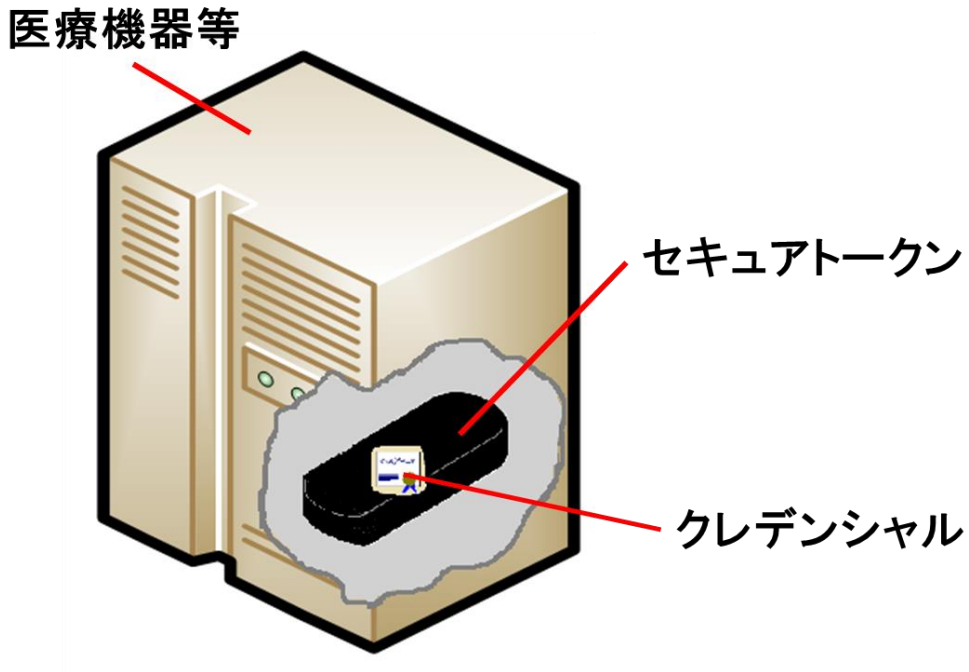

図８　クレデンシャル及びセキュアトークン：機器等の埋め込み型の場合

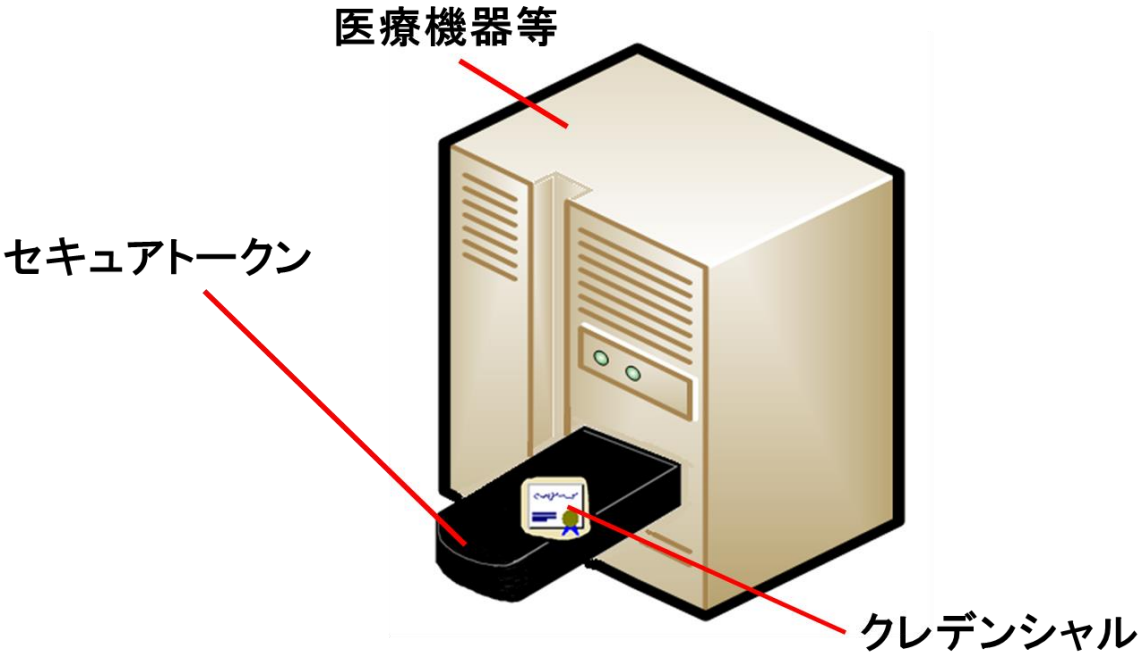

図９　クレデンシャル及びセキュアトークン：取り外し型の場合

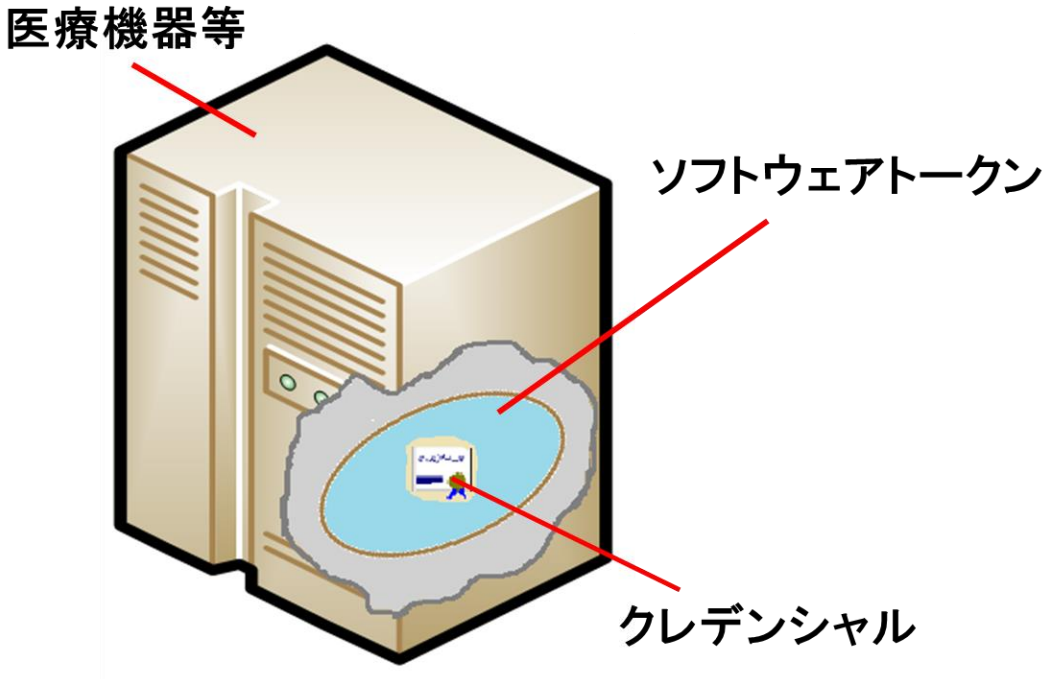

図 10　クレデンシャル及びソフトウェアトークン

8.2. 機器管理に要求されるクレデンシャル及びトークン

本ガイドが対象とする医療機関等の管理する医療機器等は同一セキュリティドメインに属するので、そのドメイン内での安全性を確保するために、次の要件を満たす必要がある。

要件１：適切な発行管理が行われたクレデンシャルの利用

組織内で医療機器等を唯一に特定できるように発行管理されたクレデンシャルを発行できる仕組みが必要となる。PKI を用いたとしても、必ずしも第三者が運営する信頼できる CA の証明書を使わなければならないということではない。組織内で運営する CA によって証明書を発行する運用も可能である。PKI を用いた場合には、証明書の有効期限に合わせた証明書の更新や医療機器等の廃棄に従った証明書の失効等の運用が求められる。

要件２：クレデンシャルと医療機器等への格納

発行されたクレデンシャルは、対象となる医療機器等に格納されなければならない。そのため、機器管理者は、発行されたクレデンシャルを対応する医療機器等に適切に格納する必要がある。機器管理者には、医療機器等を導入した際の適切なクレデンシャルの格納、更新が発生する場合の適切なクレデンシャルの更新、医療機器等を廃棄する場合のクレデンシャルの消去等の運用が求められる。

要件３：トークンによるクレデンシャルの保護

医療機器等に設定されたクレデンシャルは、適切に保護することによって、複製による成りすましやクレデンシャルの改ざん・破壊を防がなければならない。そのため、選択したクレデンシャルによる効果、リスク、コストを考慮の上、セキュアトークンの利用等安全性を確保できる方法でクレデンシャルを保護する必要がある。

8.3. セキュアトークンの具体例

セキュアトークンの具体的な例としては次が挙げられる。

a) USB タイプトークン
b) IC カード
c) SD カードタイプトークン
d) 埋め込み型
e) ソフトウェアトークン

それぞれのセキュアトークンのメリット及びデメリットを表１に示す

表１　セキュアトークンの形態とそのメリット及びデメリット

	メリット	デメリット
機器埋め込み型	・設置環境の物理的セキュリティを極端に高める必要はない	・機器の故障が生じると、クレデンシャルは再発行する必要があり、機器の入替と再発行・登録が完了するまで運用が停止する可能性がある
取り外し型	・ハードウェアが故障してもトークンを差換えるだけで済むので、運用停止が最小限で済む可能性がある	・紛失や持ち去られる危険性もあるので、管理に配慮する必要がある

ソフトウェアトークン	・特別なハードウェアを必要としないので、安価で実現することができる ・バックアップを作成することが可能	・物理的な保護がなく、クレデンシャルの複製が作成されてしまう可能性があるので、コピーによって成りすまされる危険性がある ・ハードウェアよりも悪意あるソフトウェアによって攻撃される恐れが高い

8.4. セキュアトークンに要求される機能

医療機器等で利用するセキュアトークンは以下の機能を持つ。セキュアトークンを利用する際のインタフェースは製品やOS等に依存する。Mandatoryは必須、Conditionalは条件付き、Optionalは任意を表す。

a) クレデンシャル保管機能：「Mandatory」

医療機器等の正当性を保証するためのクレデンシャル（電子証明書）を、耐タンパー性を持つ不揮発性メモリ等に暴露しないよう正確性及び機密性を担保して格納する。そのため、格納されたクレデンシャルは、セキュアトークン外に取り出せないよう保持する必要がある。この機能によって、クレデンシャルが不正にコピーされることを防止する。

b) セキュアトークンとセキュアトークンを接続あるいは搭載する医療機器等の間の認証機能：「Mandatory」

セキュアトークンとセキュアトークンを接続あるいは搭載する医療機器等は、互いに正当であることを確認する。医療機器等及びセキュアトークンは、お互いに正当な相手が保有しているべき暗号鍵やパスフレーズを相手側が保有していることを、メッセージのやり取りによって確認する。セキュアトークン内のデータの読み出し、書込み、演算等の前に実行する。本機能によって、取り外し可能な形態のセキュアトークンの場合に、他の許可されていない医療機器等でセキュアトークンが利用されることを防止する。

c) セキュアトークンに秘密鍵の演算を行わせる機能：「Conditional」

本機能は、医療機器等がPKIによって認証される場合に必須となる。医療機器等がセキュアトークンに対してセキュアトークンが保持する秘密鍵での演算を要求する機能である。例えばIHE ITI-ATNAでは、機器と対向ノードはTLSを用いて相互に認証する。そのため、医療機器等は下記手順で認証する。

1) クレデンシャル（公開鍵証明書）を対向ノードに送信する。
2) 対向ノードから送られてきたチャレンジ（乱数）をトークンに格納されたクレデンシャル内の公開鍵と対になる秘密鍵を用いて暗号化（演算）して対向ノードへ返信する。

本機能によって、保護された環境で秘密鍵に直接触れることなく秘密鍵を用いた暗号演算を実行することを保証する。

d) クレデンシャルの書込み・更新機能：「Mandatory」

クレデンシャルを書込み・更新する。医療機器等が外部から受け取ったクレデンシャルをセキュアトークン内の耐タンパー性を持つメモリ等暴露しないメモリ上に書き込む。手動で実行する場合と、オンラインで実行する場合がある。本機能によって、許可された管理者等のエンティティのみがセキュアトークンにクレデンシャルを格納できることを保証する。

e) 鍵生成機能：「Optional」

クレデンシャルの書込み･更新する際に、トークン内にてクレデンシャルを構成する鍵ペア(公開鍵及び、秘密鍵)を生成する。秘密鍵はトークン外に取り出せないよう保持する。本機能によって、秘密鍵の安全性を担保する。

f) オンライン更新機能：「Optional」

クレデンシャルの書込み･更新する際に、CA等とオンラインに接続して実行する。組織外のCA等を用いる場合には、通信の安全性を確保する必要がある。本機能によって、許可されたエンティティ（CA等）のみがセキュアトークンにクレデンシャルを格納できることを保証する。

9. 運用モデル

安全管理ガイドラインの要件を満たした上で、Wi-Fi を用いて機器を医療機関等の施設内ネットワークに接続する場合の設定例を示す。9.1 は最低限の不正アクセス対策を実現する例である。9.2 及び 9.3 は端末認証によって不正端末の接続を防止する例である。

9.1. 最低限の不正アクセス対策を実現する例（MAC アドレスフィルタリングを行うモデル）

【構成例】

小規模な医療機関等が Wi-Fi AP にて MAC アドレスフィルタリングを行う例で、7.3 に示した最低限の不正アクセス対策を実現する実装例に相当する。図 11 に構成例を示す。

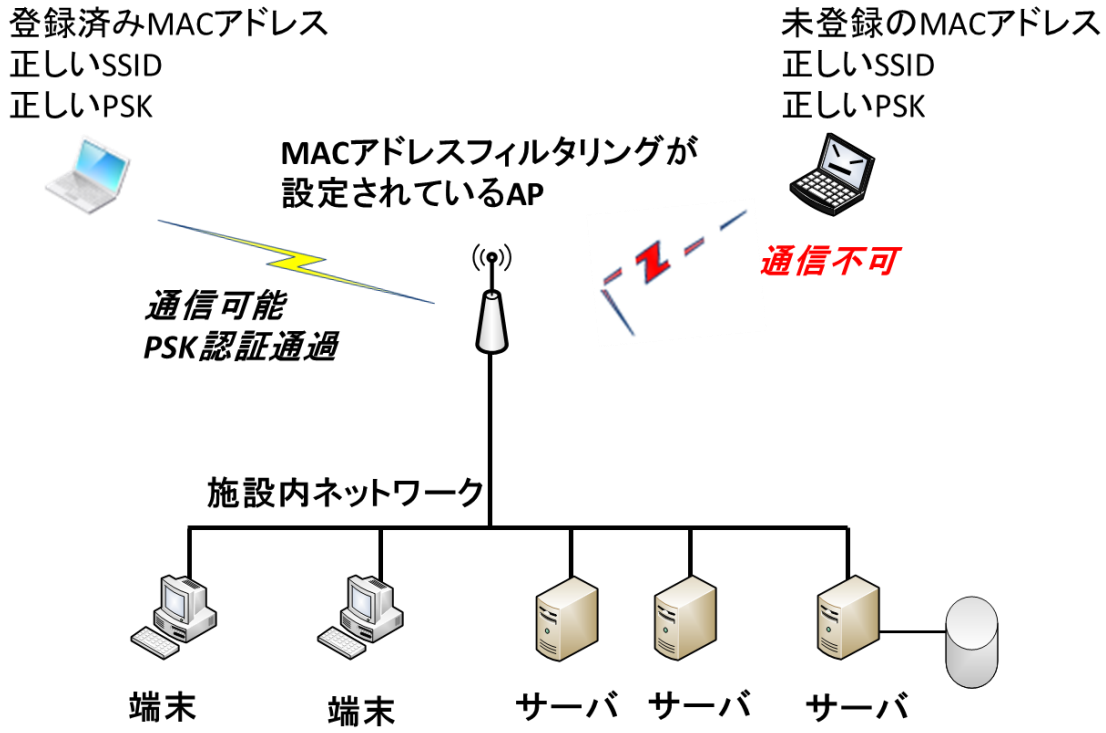

図 11　安全管理ガイドラインの要件（C 項）を満たす場合の構成例

【設定内容】

Wi-Fi AP と接続する医療機器等に以下の設定が必要となる。

① Wi-Fi AP の設定
- SSID ステルス設定（ANY 接続拒否・有効）
- WPA2/WPA3-Personal(AES)に暗号化設定
- MAC アドレスフィルタリング（医療機器等の MAC アドレス登録・設定）

② 医療機器等の設定
- SSID 及び PSK パスフレーズ設定

【安全に利用するための運用上の注意点】

PSK のパスフレーズは、医療機関名や診療科名等、類推されやすい文字列にすると悪意を持った攻撃者の対象になりやすいため、半角英数字＋記号を用い最低でも 20 文字の文字数が良い[1]。また、医療機関等の名称を連想させる SSID は攻撃者の興味を引く場合があるので注意する必要がある。

PSK 認証方式のパスフレーズは各機器・端末共通であり、PSK が判明すれば、無線 LAN 接続が可能になる。設定した端末によっては、容易に再表示して確認することができる。そのためパスフレーズは、定期的な変更等の運用が必要であり、パスフレーズの漏えい事故や、その恐れがある場合は直ちに変更する必要がある。

【運用管理】

医療機器等の導入、廃棄に従って、Wi-Fi AP に登録した医療機器等の MAC アドレス設定を追加・削除する必要がある。また廃棄する医療機器等や、Wi-Fi への接続が不要となった機器から PSK が漏えいしないよう、無線プロファイルの設定を削除する必要がある。

9.2. 端末認証によって不正端末の接続を防止する例（802.1x を EAP-PEAP で利用するモデル）

【構成例】

管理する機器台数が多い場合の構成で、7.4 に示した総務省・「企業等が安心して無線 LAN を導入・運用するために」を満たす実装例に相当する。 802.1x を利用するが、接続する医療機器等の認証は医療機関等で医療機器等を識別・管理する機器識別子（機器 ID）/パスワード、サーバ側認証をデジタル署名で行う。RADIUS サーバには機器 ID/パスワードを登録することによってアクセスを許可する医療機器等を登録し、その情報により認証及びアクセス制限を実現する。医療機器等は RADIUS サーバの証明書を検証することによって、正当性を確認する。

[1] Wi-Fi で設定する PSK のパスフレーズの文字数等については総務省の情報等を参照のこと
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/j_enduser/ippan06.htm

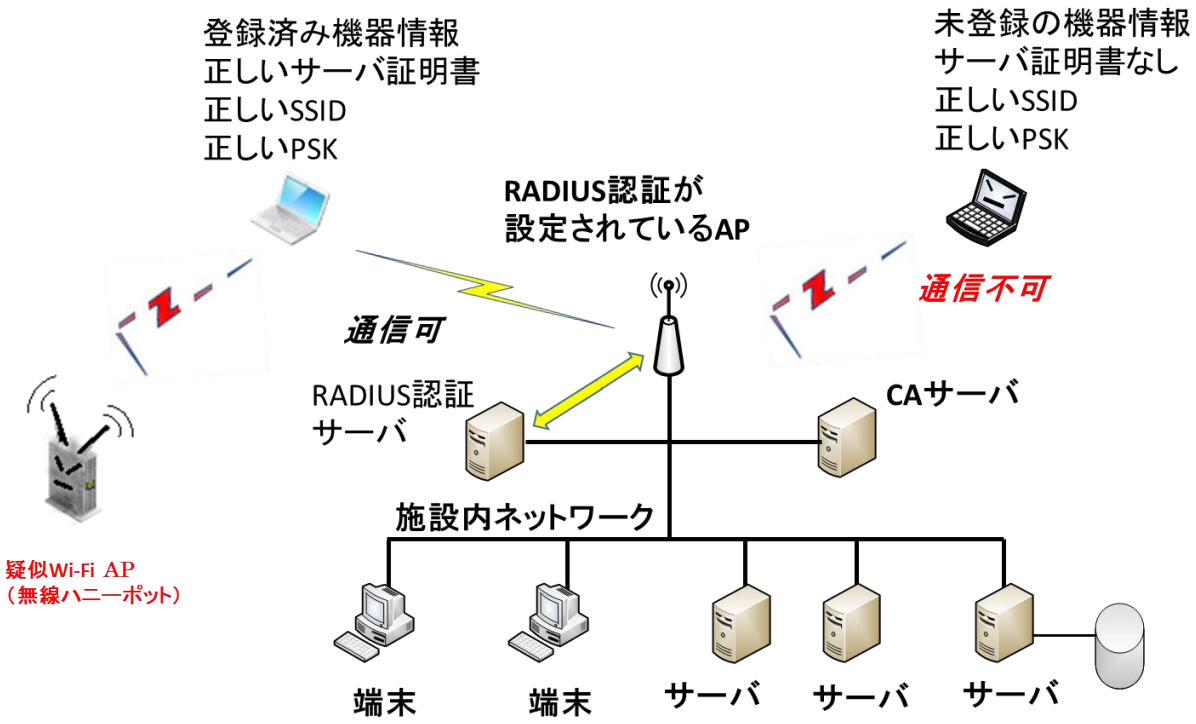

図 12　802.1x を適応する場合（EAP-PEAP）の構成例

【設定例】

Wi-Fi AP、RADIUS サーバ、接続する医療機器等に以下の設定が必要となる。

① Wi-Fi AP の無線設定（SSID、WPA2/WPA3）
- SSID ステルス設定（ANY 接続拒否・有効）
- WPA2/WPA3-Personal(AES)に暗号化設定

② Wi-Fi AP の RADIUS サーバ設定（RADIUS サーバ設定）
- 802.1x 認証を有効に設定
- RADIUS サーバの指定

③ RADIUS サーバ側の設定例
- CA による公開鍵発行と、RADIUS サーバへの設定。
- 医療機器等の登録（機器 ID およびパスワード）

④ 医療機器等の設定例（SSID、WPA2/WPA3 等の設定）
- SSID 及び PSK パスフレーズ設定
- 医療機器等の識別情報設定（機器 ID およびパスワード）
- 802.1x の設定
- RADIUS サーバの公開鍵証明書の設定

【安全に利用するための運用上の注意点】

PSK のパスフレーズは、医療機関名や診療科名等、類推されやすい文字列にすると悪意を持った攻撃者の対象になりやすいため、半角英数字＋記号を用い最低でも 20 文字の文字数が良い。また、医療機関等の名称を連想させる SSID は攻撃者の興味を引く場合があるので注意する必要がある。

機器 ID/パスワードは各機器固有の認証情報であるため、該当機器管理者以外に知られないようにする必要がある。

医療機器等は、接続する RADIUS サーバの証明書の正当性を検証する必要がある。

【運用管理】

CA によって RADIUS サーバの証明書を発行する必要がある。医療機器等の導入、廃棄に従って、RADIUS サーバに登録する医療機関等の組織内で医療機器等を識別する機器の識別子（機器 ID）/パスワードを登録・削除する必要がある。CA のルート証明書を設定する必要がある。

9.3. 端末認証によって不正端末の接続を防止する例（802.1x を EAP-TLS で利用するモデル）

【構成例】

管理する機器の台数が多い場合の構成で、7.4 に示した総務省・「企業等が安心して無線 LAN を導入・運用するために」を満たす実装例に相当する。802.1x を利用し、接続する医療機器等の認証は CA が発行した機器の証明書に基づくデジタル署名で行い、サーバ側認証をデジタル署名で行う。RADIUS サーバは、医療機器等に発行された証明書によって機器の正当性を確認する。医療機器等はサーバの証明書を検証することで、RADIUS サーバ側の正当性を確認する。図 13 にその構成例を示す。

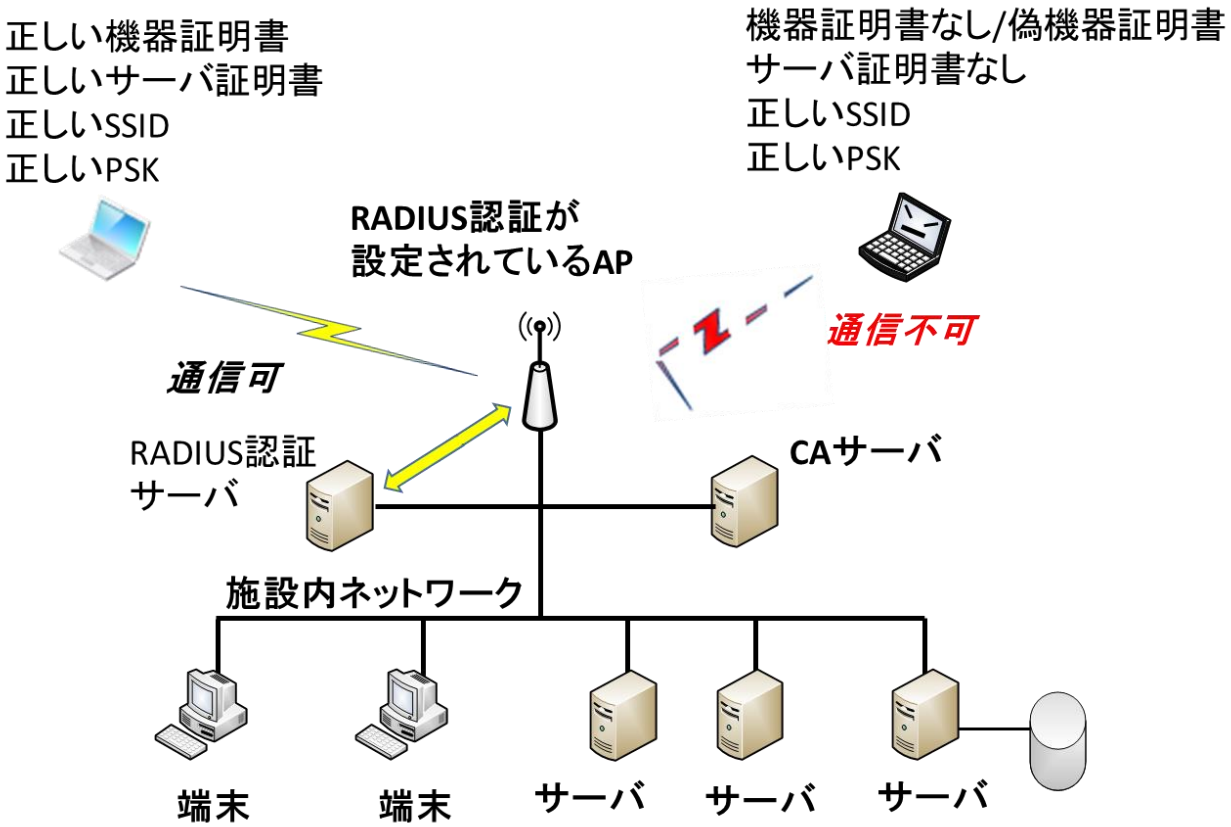

図 13　802.1x を適応する場合（EAP-TLS）の構成例

【設定例】

Wi-Fi AP、RADIUS サーバ、接続する医療機器等に以下の設定が必要となる。

① Wi-Fi AP の無線設定例（SSID、WPA2/WPA3）
SSID ステルス設定（ANY 接続拒否・有効）

WPA2/WPA3-Personal(AES)に暗号化設定

② Wi-Fi AP の RADIUS サーバ設定例（RADIUS サーバ設定）
- 802.1x 認証を有効に設定
- RADIUS サーバの指定

③ RADIUS サーバ側の設定例
- CA による証明書発行と、RADIUS サーバへの設定。

④ 医療機器等の設定例（SSID、WPA2-PSK 等の設定）
- SSID を指定してパスフレーズ入力
- 802.1x の設定
- ルート証明書の設定
- CA による機器証明書の発行
- 医療機器等に発行されたクレデンシャルの格納

【安全に利用するための運用上の注意点】

PSK のパスフレーズは、医療機関名や診療科名等、類推されやすい文字列にすると悪意を持った攻撃者の対象になりやすいため、半角英数字＋記号を用い最低でも 20 文字の文字数が良い。また、医療機関等の名称を連想させる SSID は攻撃者の興味を引く場合があるので注意する必要がある。
証明書のライフサイクル管理、接続する医療機器等のライフサイクル管理を適切に行う必要がある。

【運用管理】

医療機器等の導入、廃棄及び証明書の更新に従って、CA は医療機器等に対する証明書の発行及び失効の管理を適切に行わなければならない。導入の際には、医療機器等に対する証明書の発行、医療機器等へのクレデンシャル格納及びルート証明書の設定が必要となる。医療機器等に対する証明書を発行する CA の運用が必要となる。医療機器等に対して発行される証明書のライフサイクルに合わせた更新（証明書の再発行と医療機器等への設定）が必要となる。

付録―１．参考文献

NIST SP800-97　*Establishing Wireless Robust Security Networks:　A Guide to IEEE 802.11i,* February 2007

NIST SPECIAL PUBLICATION 1800-1, *SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES,* July 2018

ITU-T X.509 *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, 2019-10-14

RFC 8940 *Extensible Authentication Protocol(EAP) Session-Id Derivation for EAP Subscriber Identity Module (EAP-SIM), EAP Authentication and Key Agreement (EAP-AKA), and Protected EAP (PEAP),* October 2020

RFC 9190, *EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3,* February 2022

総務省　Wi-Fi 提供者向けセキュリティ対策の手引き、令和２年５月

付録―２．作成者名簿

作成者（社名五十音順）

梅野　智靖	アライドテレシス㈱
DUCH JAKUB	アライドテレシス㈱
有馬　一閣	㈱NTT データ
宇都宮　博	㈱バッファロー
梶山　孝治	富士フイルムヘルスケア㈱
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)
茗原　秀幸	三菱電機㈱
太田　英憲	三菱電機インフォメーションシステムズ㈱
酒巻　一紀	三菱電機インフォメーションシステムズ㈱
谷内田　益義	㈱リコー

改定履歴		
日付	バージョン	内容
2017/03/31	Ver. 1.0	初版
2024/01/11	Ver 1.1	・付属書の分離 ・厚労省ガイドライン 6.0 版改定に合わせた改定。

（ＪＡＨＩＳ技術文書　２３－ｘｘｘ）
２０２４年1月発行

ＪＡＨＩＳ　セキュアトークン実装ガイド・機器認証編 Ver. 1.1

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