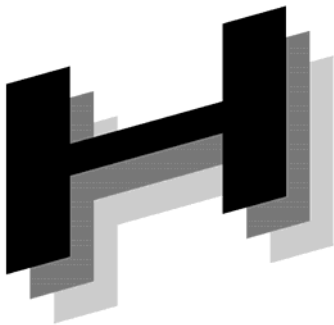




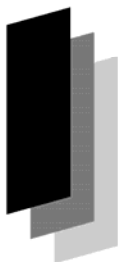
Japanese



Association of



Healthcare



Information



Systems Industry

J A H I S  
セキュアトークン実装  
ガイド・機器認証編  
Ver 1.0

2017年3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ン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4.4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の最低限のガイドライン（C項）及び推奨されるガイドライン（D項）を満たすための方法や例を示すとともに、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。

2017年3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 .....	1
2. 引用規格・引用文献 .....	1
3. 用語の定義 .....	1
4. 略語 .....	2
5. 概説（機器認証とノード認証） .....	2
5.1. 機器認証の必要性 .....	2
5.2. 機器認証とノード認証 .....	3
6. ユースケース .....	4
6.1. 前提となるモデル .....	4
6.2. 想定される脅威とその対策 .....	5
6.3. Wi-Fi で接続する機器 .....	7
7. 機器への要求 .....	8
7.1. はじめに .....	8
7.2. 基本構成 .....	8
7.3. 安全管理ガイドラインの要件（C 項）を満たす機能及び設定 .....	9
7.3.1. 前提条件 .....	9
7.3.2. 医療機器等の設定 .....	9
7.3.3. 運用及び留意事項 .....	9
7.4. 安全管理ガイドラインの推奨要件（D 項）を満たす機能及び設定 .....	10
7.4.1. IEEE802.1x の基本 .....	10
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 .....	11
7.4.3. EAP に対応した Wi-Fi AP .....	12
7.4.4. EAP-TLS,EAP-PEAP 等に対応した RADIUS サーバ .....	12
7.5. 機器のインタフェース要件 .....	12
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 .....	12
7.5.2. 信頼できる証明書の登録（必須） .....	12
7.5.3. クレデンシャルの格納（必須） .....	13
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） .....	13
7.6. 適切なログの作成と収集 .....	13
8. セキュアトークン .....	13
8.1. 機器認証とセキュアトークン .....	13
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 .....	16
8.3. セキュアトークンの具体例 .....	16
8.4. セキュアトークンに要求される機能 .....	17
9. 運用モデル .....	18

9.1. 安全管理ガイドラインの要件 (C 項) を満たす例 (MAC アドレスフィルタリングを行うモデル) .....	18
9.2. 安全管理ガイドラインの推奨要件 (D 項) を満たす例 (802.1x を EAP-PEAP で利用するモデル) .....	19
9.3. 安全管理ガイドラインの推奨要件 (D 項) を満たす例 (802.1x を EAP-TLS で利用するモデル) .....	21
附属書 A 運用モデルを実現する設定例 .....	23
A.1. 安全管理ガイドラインの要件 (C 項) を満たす設定例 (MAC アドレス フィルタリングを行うモデル) .....	23
A.1.1 Wi-Fi AP の設定例 .....	23
A.1.2 医療機器等の設定例 .....	24
A.2. 安全管理ガイドラインの推奨要件 (D 項) を満たす設定例 (802.1x を EAP-PEAP で利用するモデル) .....	27
A.2.1 Wi-Fi AP の設定例 .....	27
A.2.2 医療機器等の設定例 .....	28
A.3. 安全管理ガイドラインの推奨要件 (D 項) を満たす設定例 (802.1x を EAP-TLS で利用するモデル) .....	34
A.3.1 Wi-Fi AP の設定例 .....	34
A.3.2 医療機器等の設定例 .....	35
附属書 B CA の運用例 .....	44
B.1. 概要 .....	44
B.2. プライベート CA の構築 .....	44
B.3. RADIUS サーバ証明書の発行 .....	44
B.4. 医療機器等に対する機器認証用の証明書発行 .....	45
附属書 C 機器への組み込み例 .....	46
C.1. 概要 .....	46
C.2. PC 内蔵型 .....	46
C.3. 組み込み型 .....	46
付録一 1. 参考文献 .....	48
付録一 2. 作成者名簿 .....	49

## 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 4.4 版, 平成 29 年 3 月 (予定)

IEEE Std 802.1X-2010 - *IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control*, February 2010

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

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、無線 LAN (Wi-Fi) に関して以下のように説明している。

無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS : Denial of Service 等）を行ったり不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて PC を識別するが多いが、MAC アドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の窃視を防止するために、暗号化等による“情報漏えい”への対策も必要となる。

アクセス先の識別を確実に行ってなりすましを防止すること、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。

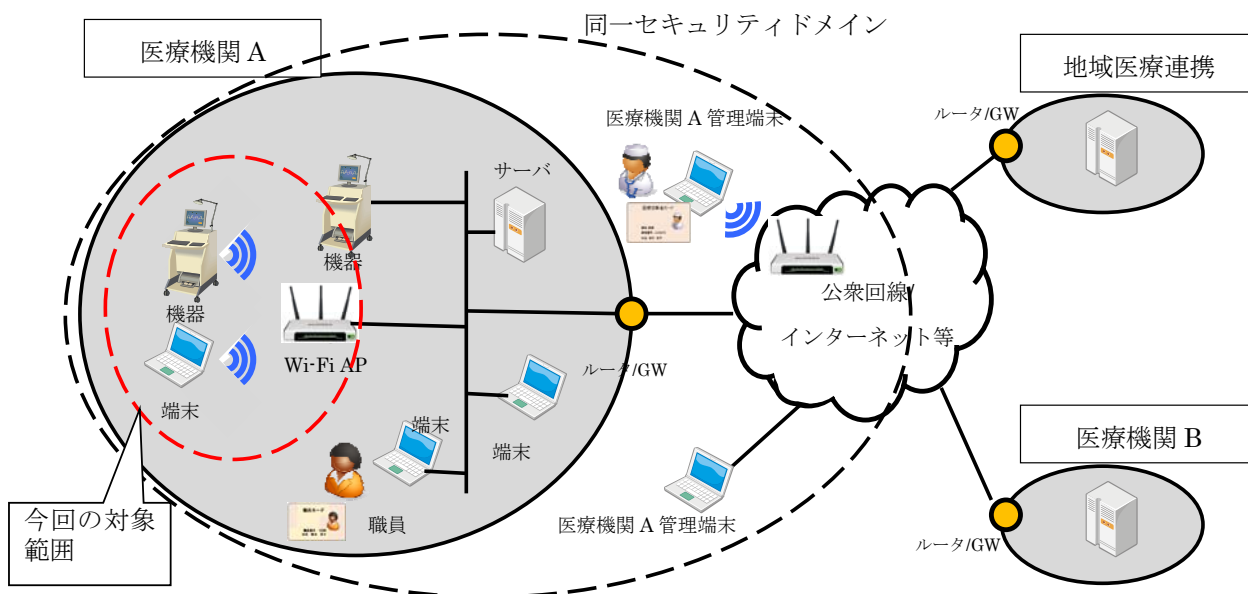


図1 ノード認証モデル

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、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。



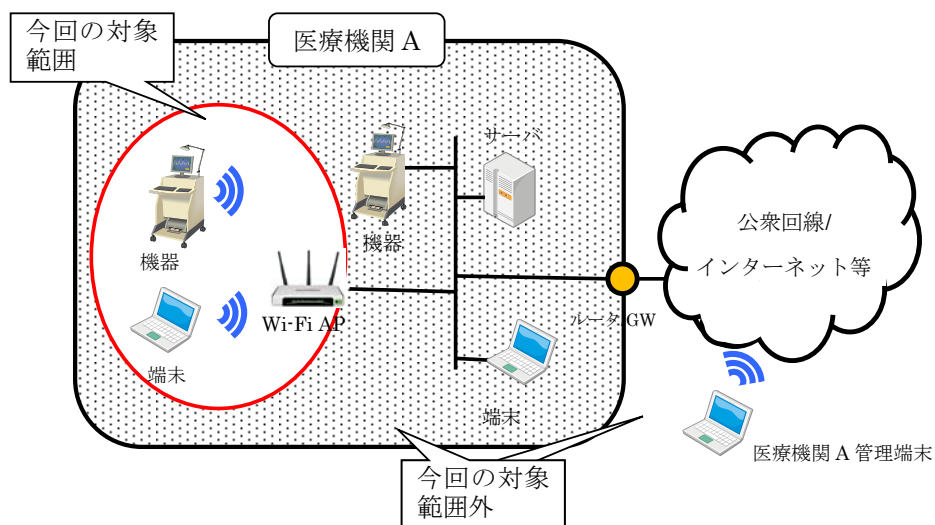


図2 前提となるモデル

## 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で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)

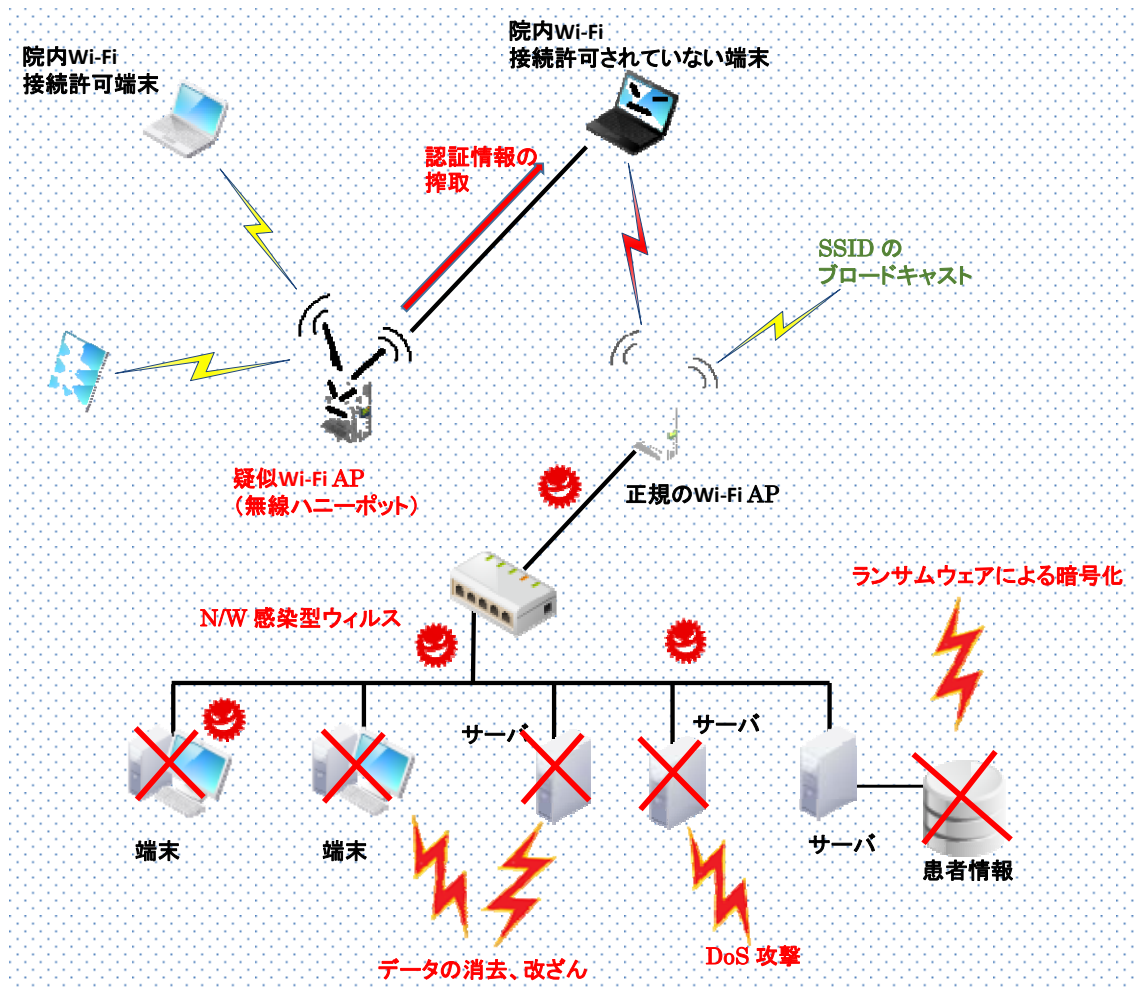


図3 脅威にさらされたWi-Fi環境

[対策]

基本的には安全管理ガイドライン 6.5 章の C 項を順守すれば対策は可能である。ただし、リスクをより減らすため C 項の遵守だけではなく、D 項についても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/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。

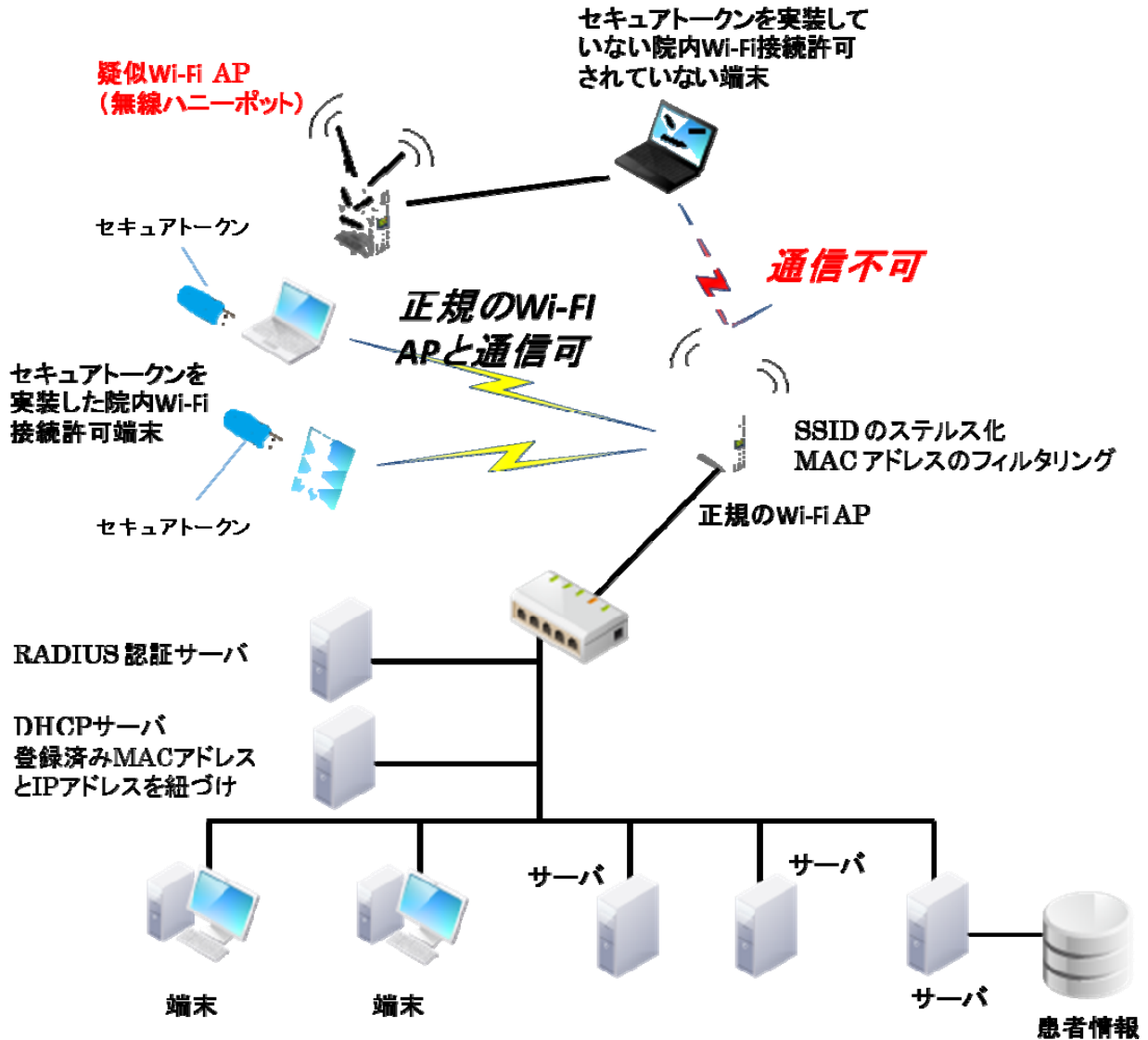


図4 セキュアなWi-Fi環境

### 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な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、医療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 IEEE 802.11ac/WPA2 等をサポートした医療機器等
  - (2) EAP(RFC 3748)及び IEEE 802.11ac/WPA2 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。

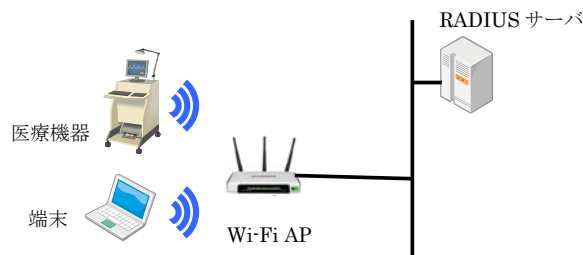


図5 Wi-Fi で接続する機器等の基本構成

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 接続する場合の要求事項を定めている。6.5 の技術的安全対策の中では、最低限度のガイドライン及び推奨されるガイドラインを定めている。以下に該当部分を示す。

#### C. 最低限のガイドライン

##### 11. 無線 LAN を利用する場合

システム管理者は以下の事項に留意すること。

- (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策を行うこと。
- (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。
- (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。
- (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。
- (5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考にすること。

#### D. 推奨されるガイドライン

7. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。

7.3 に最低限のガイドライン (C 項) を満たす場合の機能と設定を、7.4 に推奨されるガイドライン (D 項) を満たす場合の機能を示す。

## 7.3. 安全管理ガイドラインの要件 (C 項) を満たす機能及び設定

### 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/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. 安全管理ガイドラインの推奨要件（D項）を満たす機能及び設定

### 7.4.1. IEEE802.1xの基本

802.1xの基本的な仕組みを図6に示す。

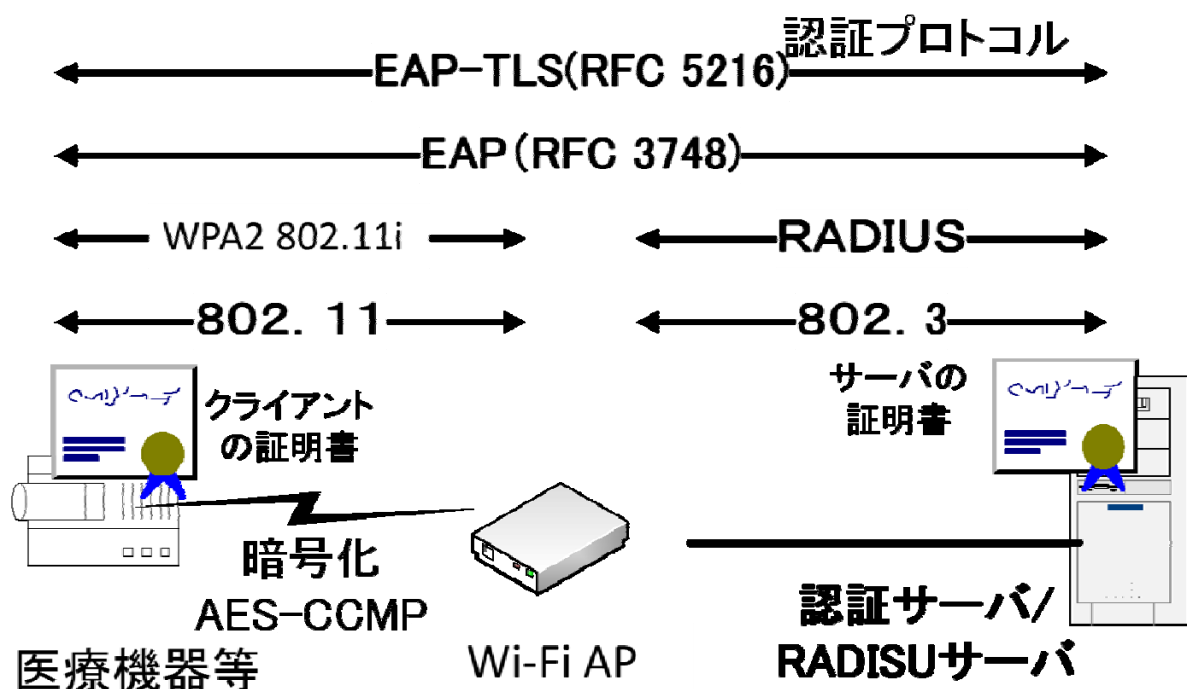


図6 802.1xの基本的な仕組み

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。

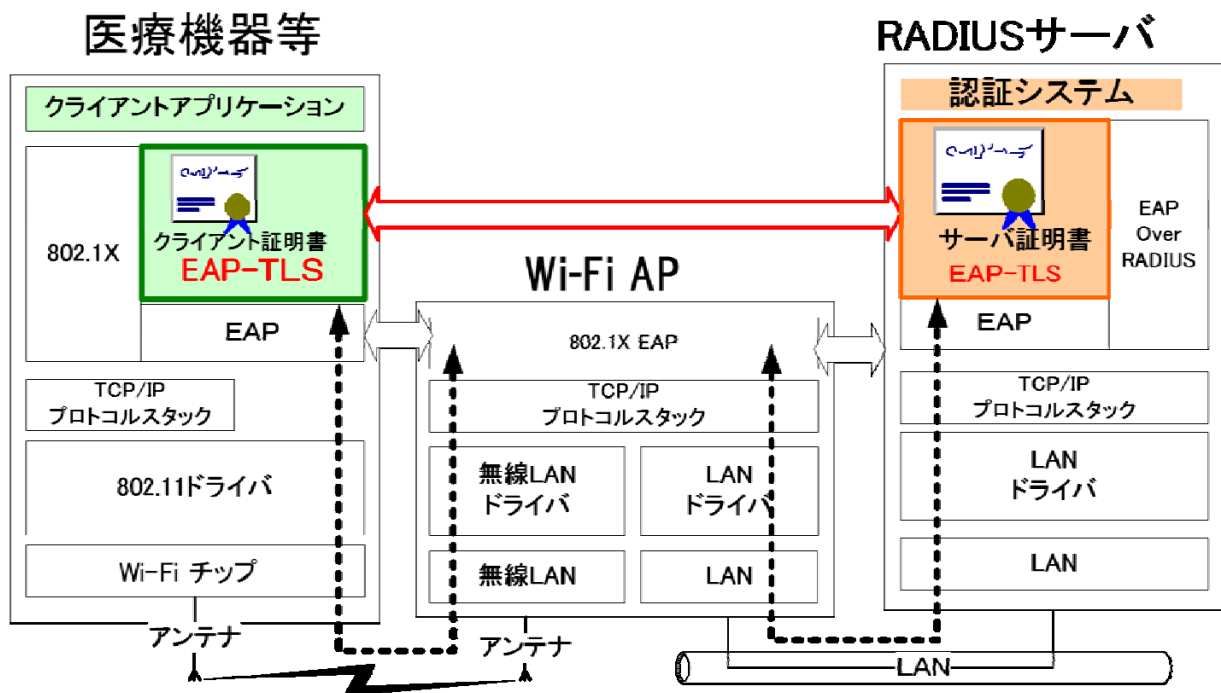


図7 802.1xの実装イメージ

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間には、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ヤル (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ヤ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ヤ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ヤ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。クレデンシヤ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ヤ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ヤ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ヤルを生成・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ヤ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ヤ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。証明書及び医療機器等のライフサイクルに合わせた証明書発行手順の一例は、附属書 B を参照のこと。

### 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技術的対策 (C項6) を満たすために、少なくともアクセス時間の把握に必要なログを残す必要がある。さらにD項においては、「IoT機器・システムが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すること」が求められている。ここで言う適正な接続とは、医療機関等が管理している医療機器等からの接続を確認することができ、その他の機器からの接続はされない事を指す。そのためには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しているとは言えず、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。

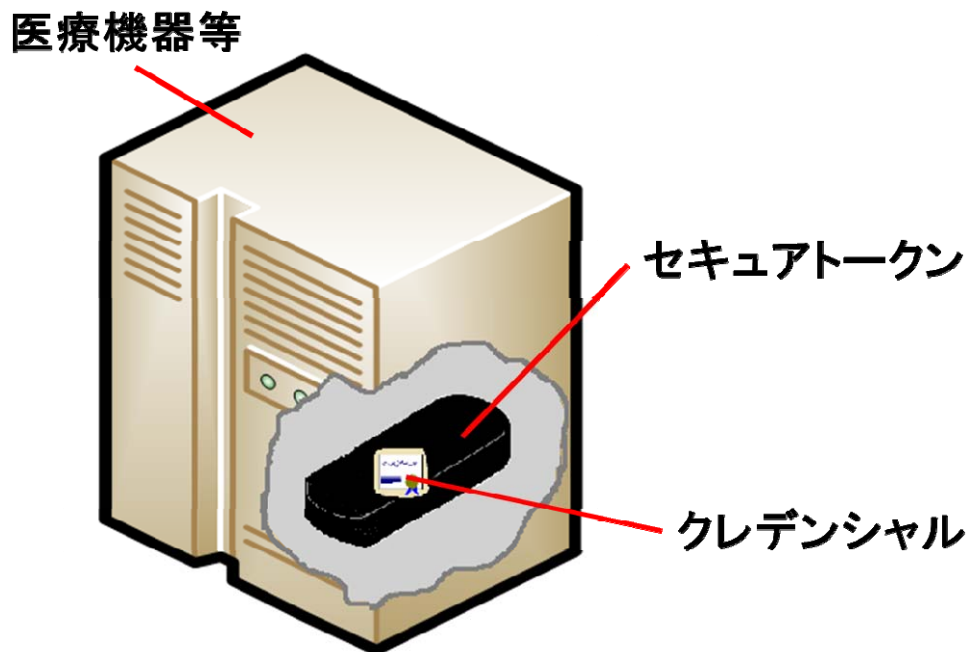


図8 クレデンシャル及びセキュアトークン：機器等の埋め込み型の場合

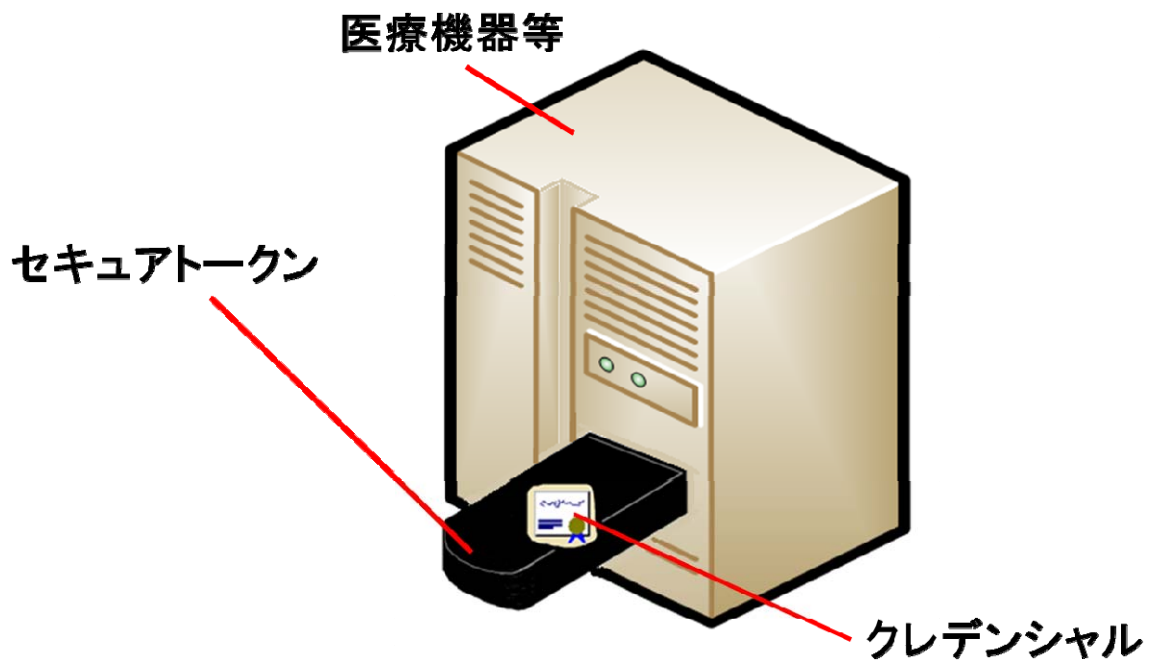


図9 クレデンシャル及びセキュアトークン：取り外し型の場合

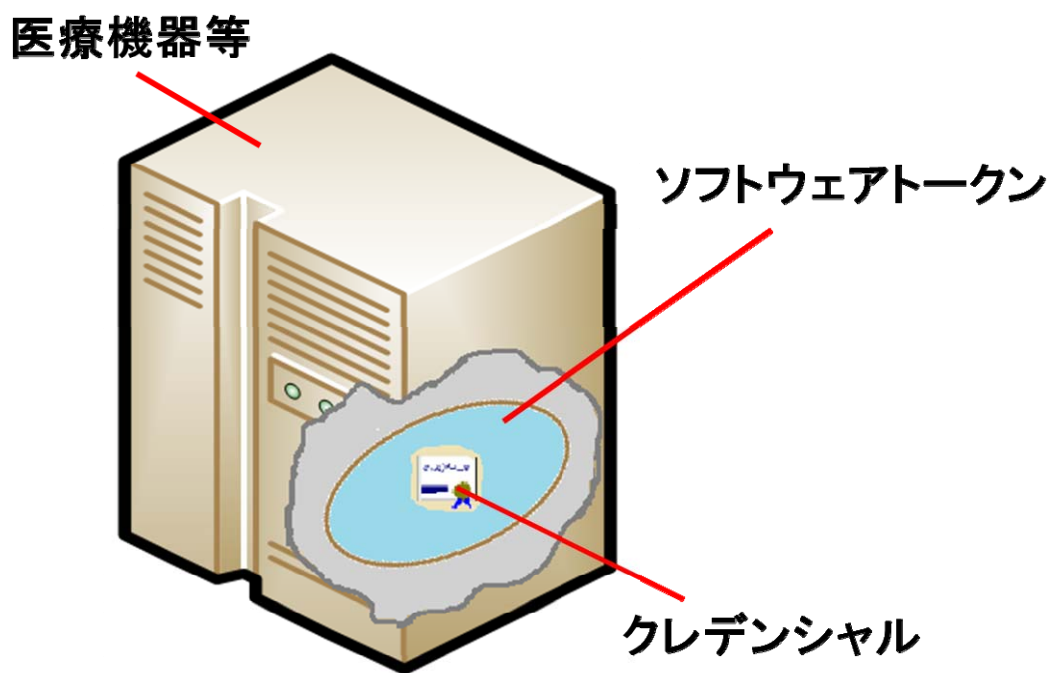


図10 クレデンシャル及びソフトウェアトークン

## 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	<ul style="list-style-type: none"> <li>・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</li> <li>・バックアップを作成することが可能</li> </ul>	<ul style="list-style-type: none"> <li>・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ため、コピーによって成りすまされる危険性がある</li> <li>・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</li> </ul>
------------	--	---

## 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との認証機能：「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ワード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 C 項の要件を満たす例である。9.2 及び 9.3 は推奨される D 項の要件を満たす例である（設定例については、附属書 A を参照）。

### 9.1. 安全管理ガイドラインの要件（C 項）を満たす例（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 に示した安全管理ガイドラインの要件（C 項）を満たす実装例に相当する。図 11 に構成例を示す。

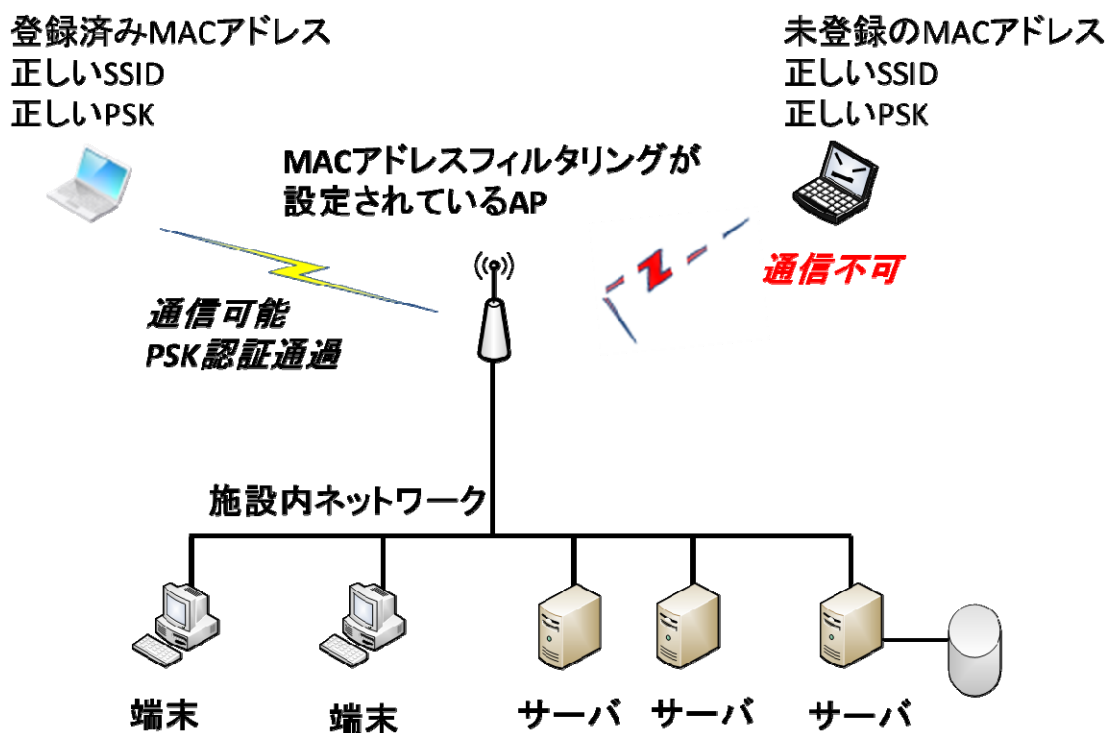


図 11 安全管理ガイドラインの要件（C 項）を満たす場合の構成例

#### 【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-PSK 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<sup>1</sup>。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. 安全管理ガイドラインの推奨要件 (D 項) を満たす例 (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 に示した安全管理ガイドラインの推奨要件 (D 項) 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。

---

<sup>1</sup> 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 IPA の情報等を参照のこと  
<http://www.ipa.go.jp/security/ciadr/wirelesslan.html>

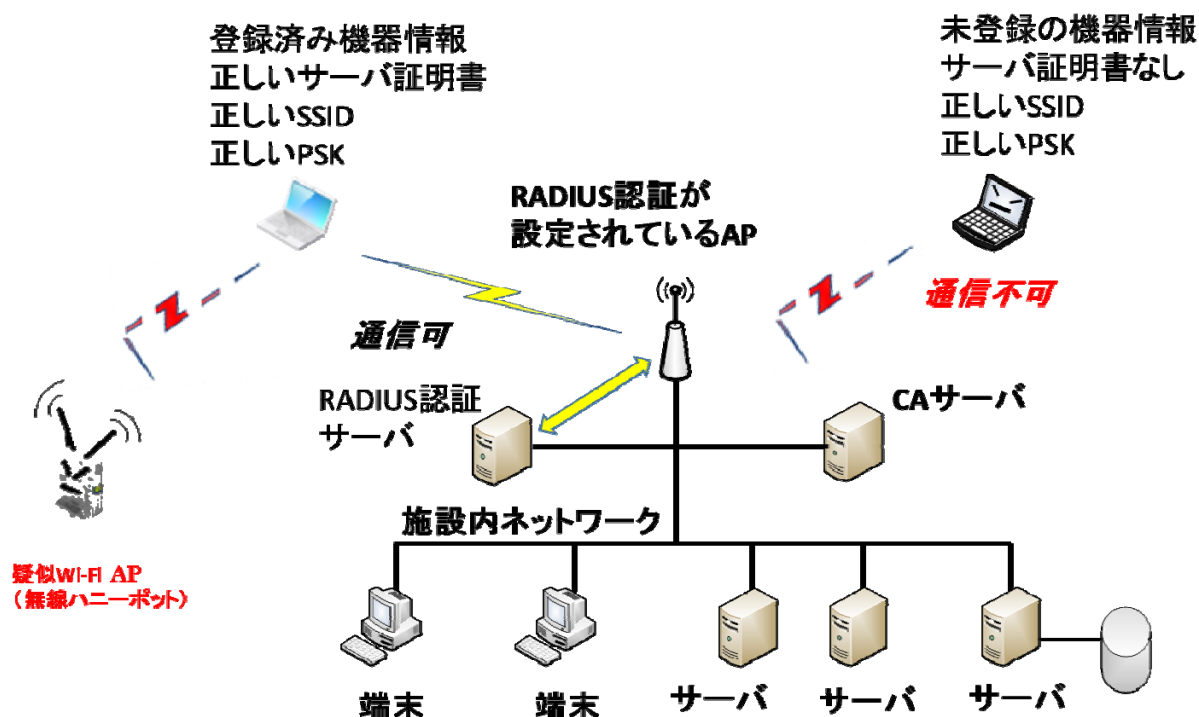


図 12 802.1x を適応する場合 (EAP-PEAP) の構成例

#### 【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-PSK)
  - ・ SSID ステルス設定 (ANY 接続拒否・有効)
  - ・ WPA2-PSK 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-PSK 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り。



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。（附属書 B 参照）

### 9.3. 安全管理ガイドラインの推奨要件（D 項）を満たす例（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 に示した安全管理ガイドラインの推奨要件（D 項）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。

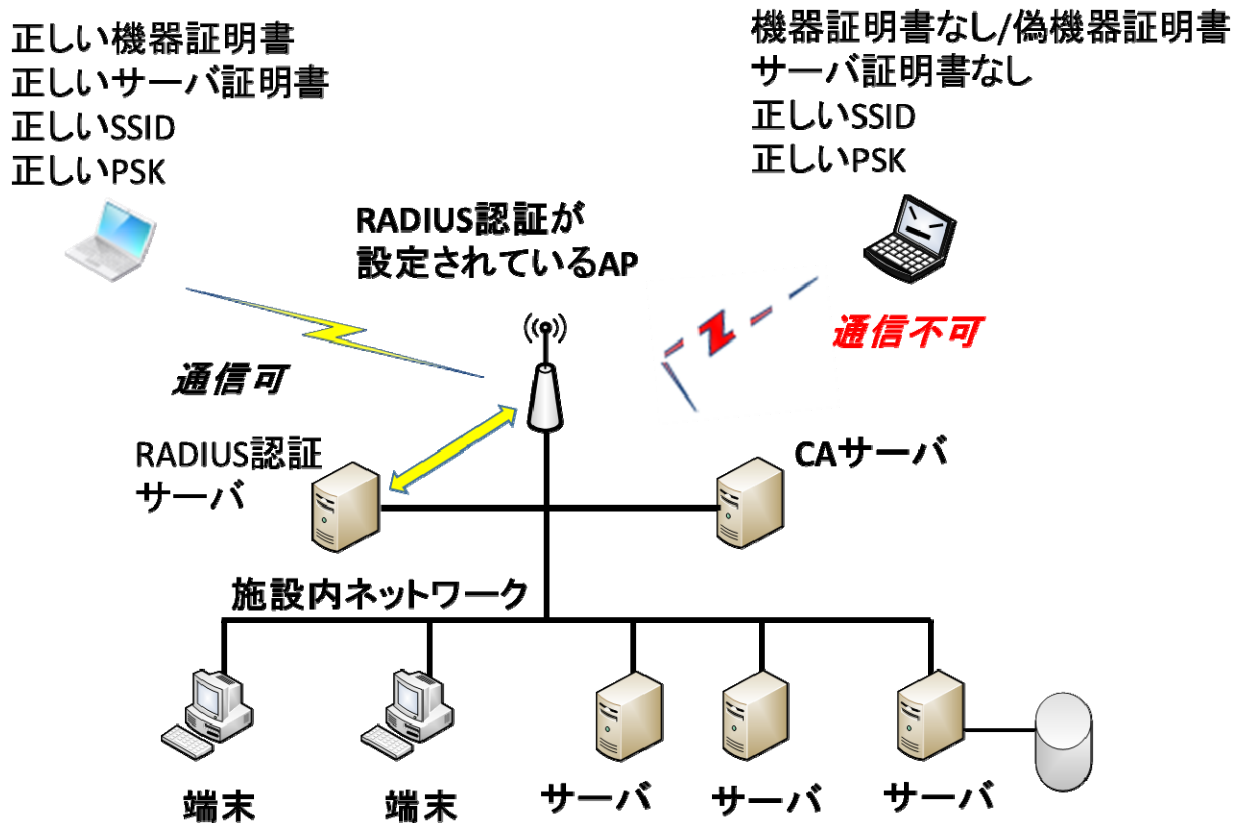


図 13 802.1x を適応する場合（EAP-TLS）の構成例

【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-PSK）
  - ・ SSID ステータス設定（ANY 接続拒否・有効）

- ・ WPA2-PSK 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。(附属書 B 参照)

## 附属書A 運用モデルを実現する設定例

本附属書では、9.1、9.2 及び 9.3 に示した運用モデルを実現するための設定例を示す。ここで示す例は一例であって、実際の設定の際には利用する環境によって差異が生じる可能性がある。Wi-Fi AP の設定例としてアイコム株式会社 AP-90M の設定画面例を、医療機器等の設定例として Microsoft 社 Windows7 の設定画面例を示す。

### A.1. 安全管理ガイドラインの要件（C 項）を満たす設定例（MAC アドレスフィルタリングを行うモデル）

9.1 に説明した運用例を実現するための設定例を次に示す。

#### A.1.1 Wi-Fi AP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA2-PSK の設定

The screenshot shows a web-based configuration interface for a wireless AP. On the left is a navigation menu with options like 'TOP', '情報表示', 'ネットワーク設定', and '無線設定'. The main area is titled '無線1 仮想AP' and contains two sections: '仮想AP設定' and '暗号化設定'. In the '仮想AP設定' section, the 'SSID' field is highlighted with an orange box and contains masked characters. In the '暗号化設定' section, the 'ネットワーク認証' is set to 'WPA2-PSK', the '暗号化方式' is 'AES', and the 'PSK (Pre-Shared Key)' field is also highlighted with an orange box and contains masked characters. Other settings include 'インターフェース: ath0', '仮想AP: 有効', 'VLAN ID: 0', '接続端末制限: 63', and 'MAC認証: 有効'.

## ② Wi-Fi AP の設定

接続を許可する機器・端末の MAC アドレス登録

TOP

▼情報表示

▼ネットワーク設定

LAN側P

DHCPサーバー

ルーティング

パケットフィルター

▼Web認証

▼無線設定

▼無線1

無線LAN

仮想AP

認証サーバー

MACアドレスフィルタリング

ネットワーク監視

AP間通信 (WDS)

WMM詳細

### 無線1 MACアドレスフィルタリング

MACアドレスフィルタリング設定

インターフェース:

MACアドレスフィルタリング:  無効  有効

フィルタリングポリシー:  許可リスト  拒否リスト

---

端末MACアドレスリスト

MACアドレス:

---

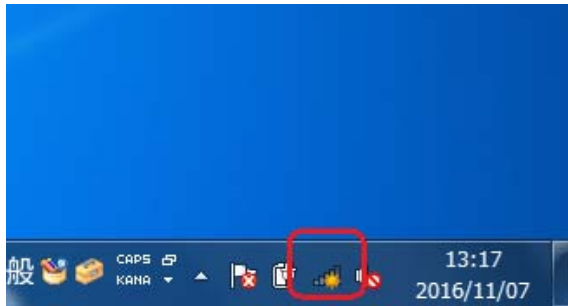
MACアドレスフィルタリング設定一覧

登録済みの端末	受信中の端末	通信状況	
	00-1D-XX-XX-XX-XX	通信不許可	<input type="button" value="追加"/>
	00-1D-XX-XX-XX-XX	通信不許可	<input type="button" value="追加"/>
	00-1D-XX-XX-XX-XX	通信不許可	<input type="button" value="追加"/>
?			
	00-1D-XX-XX-XX-XX	通信不許可	<input type="button" value="追加"/>
78-3A-XX-XX-XX-XX		登録済	<input type="button" value="削除"/>
24-A0-XX-XX-XX-XX		登録済	<input type="button" value="削除"/>
24-A0-XX-XX-XX-XX		登録済	<input type="button" value="削除"/>
6C-88-XX-XX-XX-XX		登録済	<input type="button" value="削除"/>
60-67-XX-XX-XX-XX		登録済	<input type="button" value="削除"/>

### A.1.2 医療機器等の設定例

SSID、WPA2-PSK 等の設定 (Windows 7 の場合)

- i. 無線 LAN のアイコンをクリック



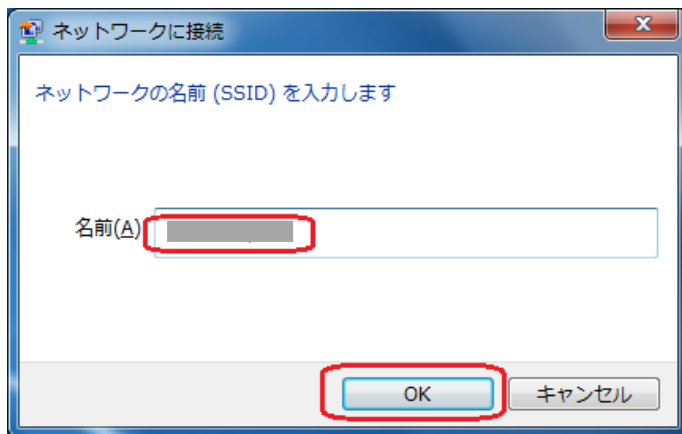
ii. 「他のネットワーク」をクリック



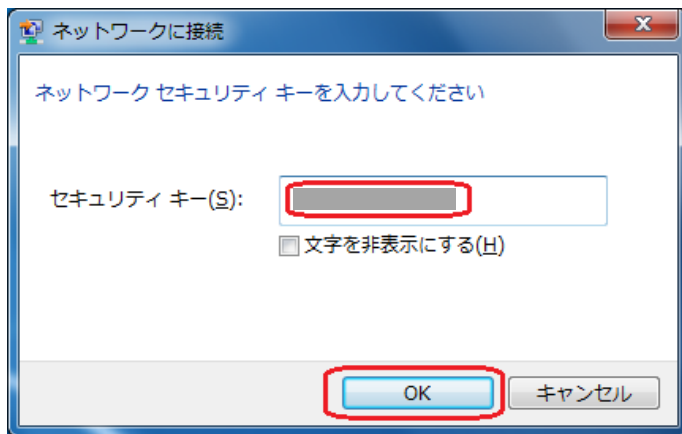
iii. 「接続」をクリック



- iv. SSID を入力して、「次へ」をクリック



- v. PSK を入力し、「次へ」をクリック



## A.2. 安全管理ガイドラインの推奨要件（D 項）を満たす設定例（802.1x を EAP-PEAP で利用するモデル）

9.2 に説明した運用例を実現するための設定例を次に示す。

### A.2.1 Wi-Fi AP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA2-PSK の設定

無線1 仮想AP

仮想AP設定

インターフェース: ath0

仮想AP:  無効  有効

SSID: ※※※※※※※※※※

VLAN ID: 0

ANY接続拒否:  無効  有効

接続端末制限: 63

アカウントテイング:  無効  有効

MAC認証:  無効  有効

暗号化設定

ネットワーク認証: WPA2-PSK

暗号化方式: AES

PSK (Pre-Shared Key): ※※※※※※※※※※

WPAキー更新間隔: 120 分

- ② Wi-Fi AP の設定  
RADIUS サーバの設定

無線1 認証サーバー

RADIUS設定

アドレス:

ポート:

シークレット:

セカンダリー:

アカウントテイング設定

アドレス:

ポート:

シークレット:

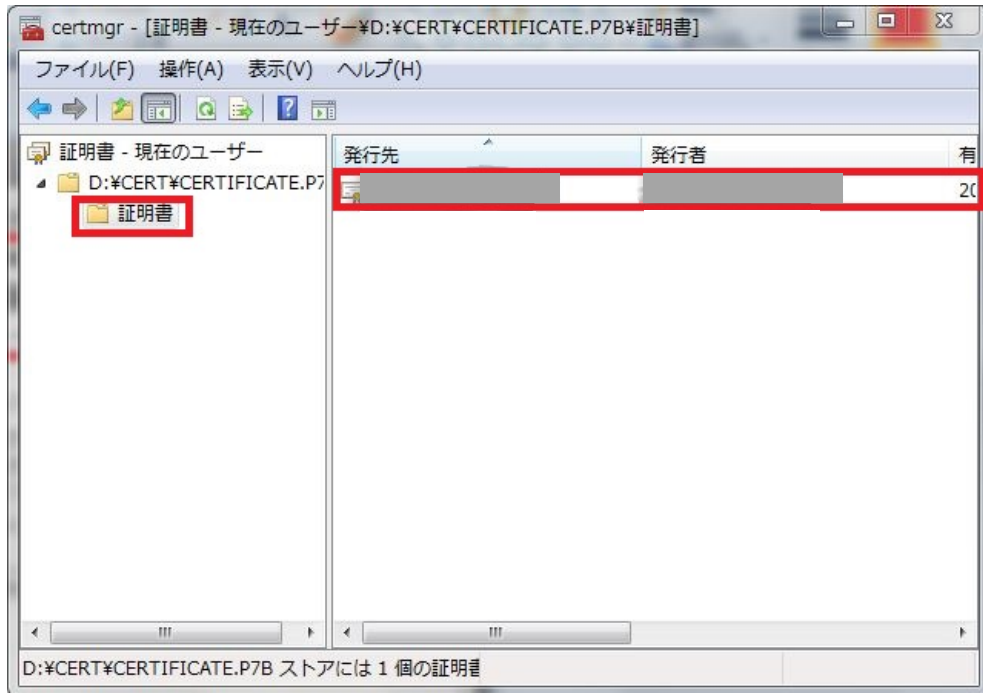
セカンダリー:

登録 取消

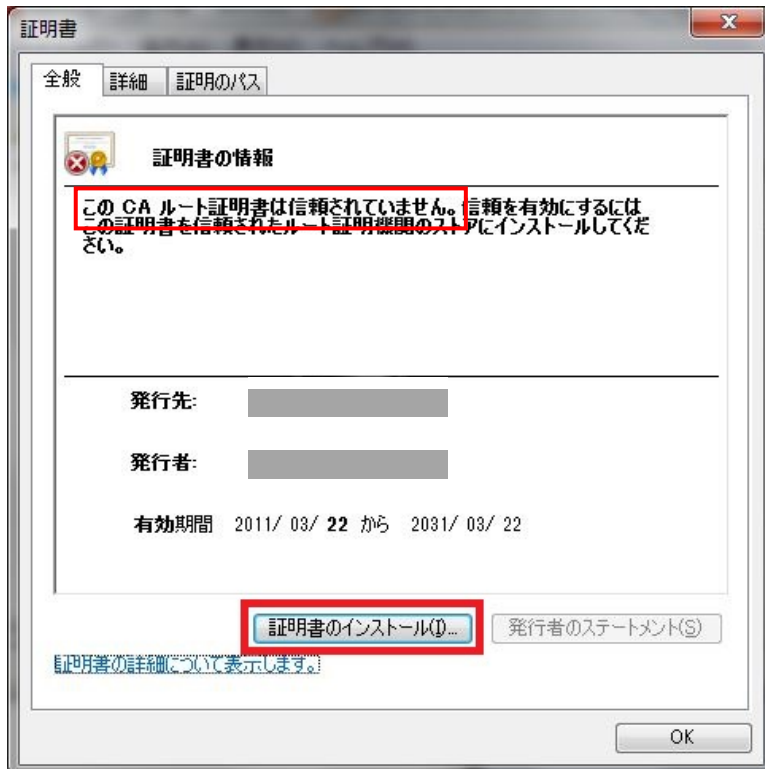
## A.2.2 医療機器等の設定例

### 1) ルート証明書のインポート

- i. 設定する証明書ファイルをダブルクリックする。CERTMGR が起動するので、証明書をクリックするとインポート対象の証明書のリストが表示される。

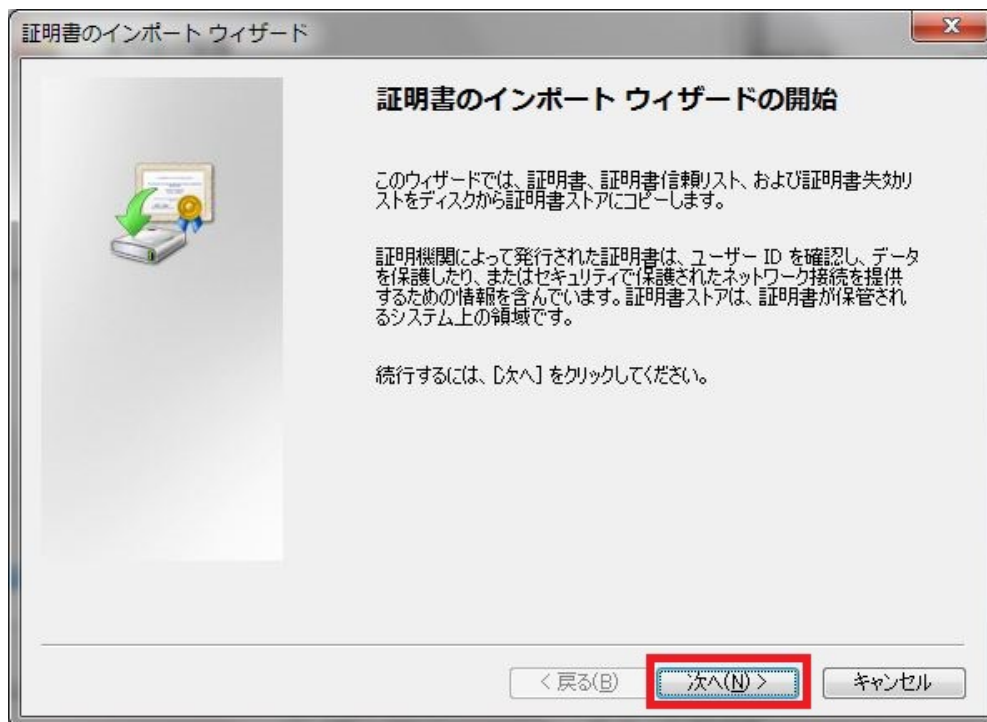


- ii. インポートする証明書の内容が表示されるので、間違いなければ“証明書のインストール” ボタンを押す。インポートする際には、医療機関等のポリシーに適合する証明書であることを確認すること。

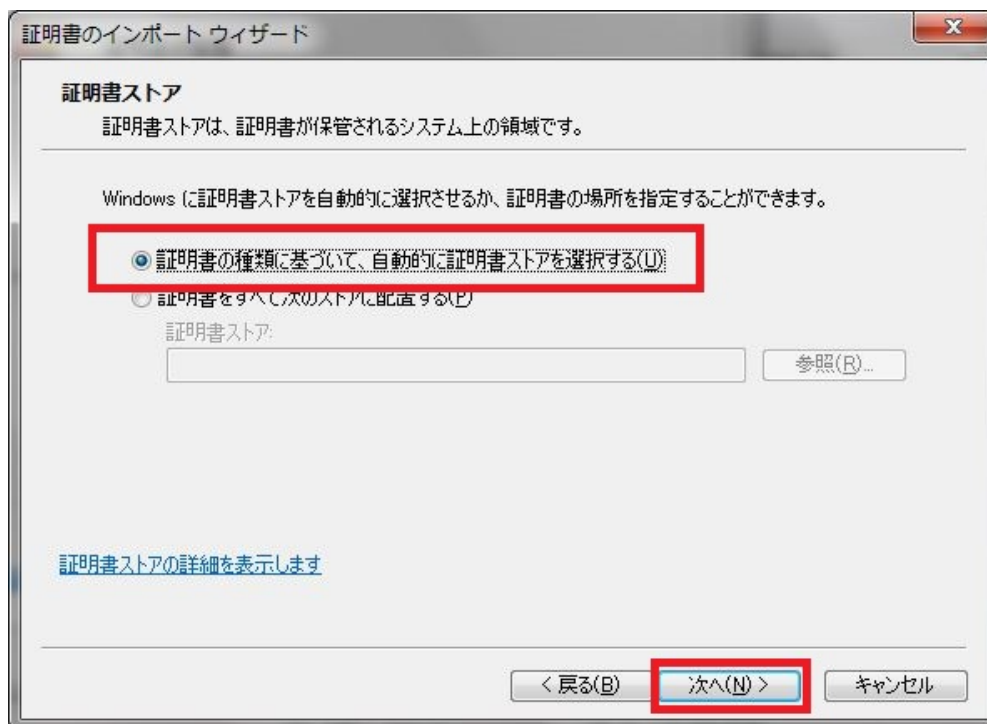




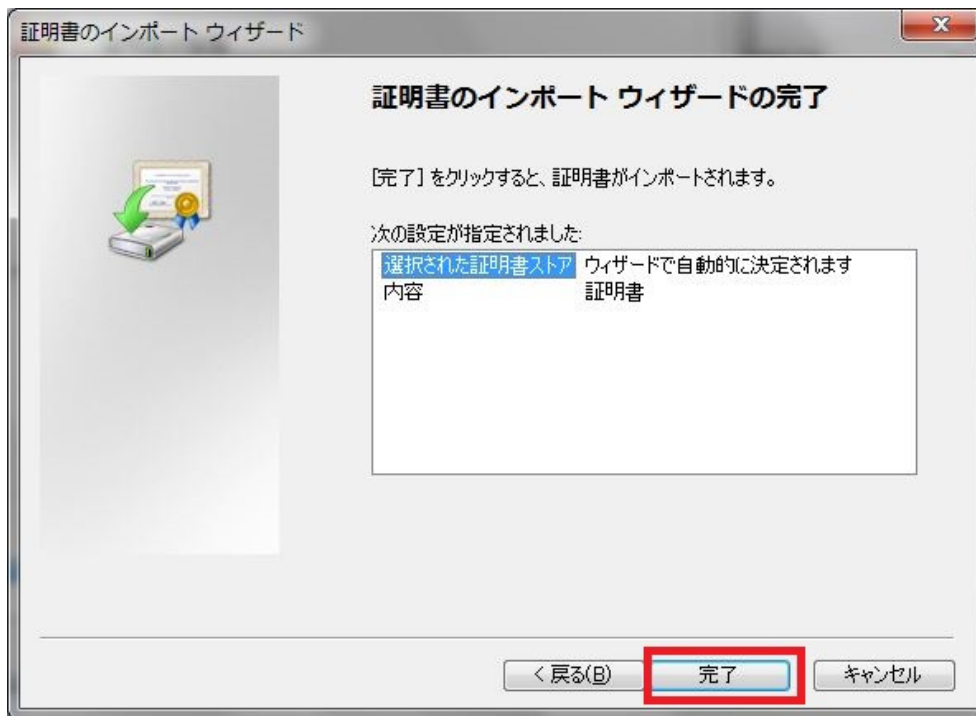
- iii. 証明書のインポートウィザードが始まるので、“次へ” ボタンを押す。



- iv. 証明書ストアを“自動的に選択させる”を選択し、“次へ” ボタンを押す

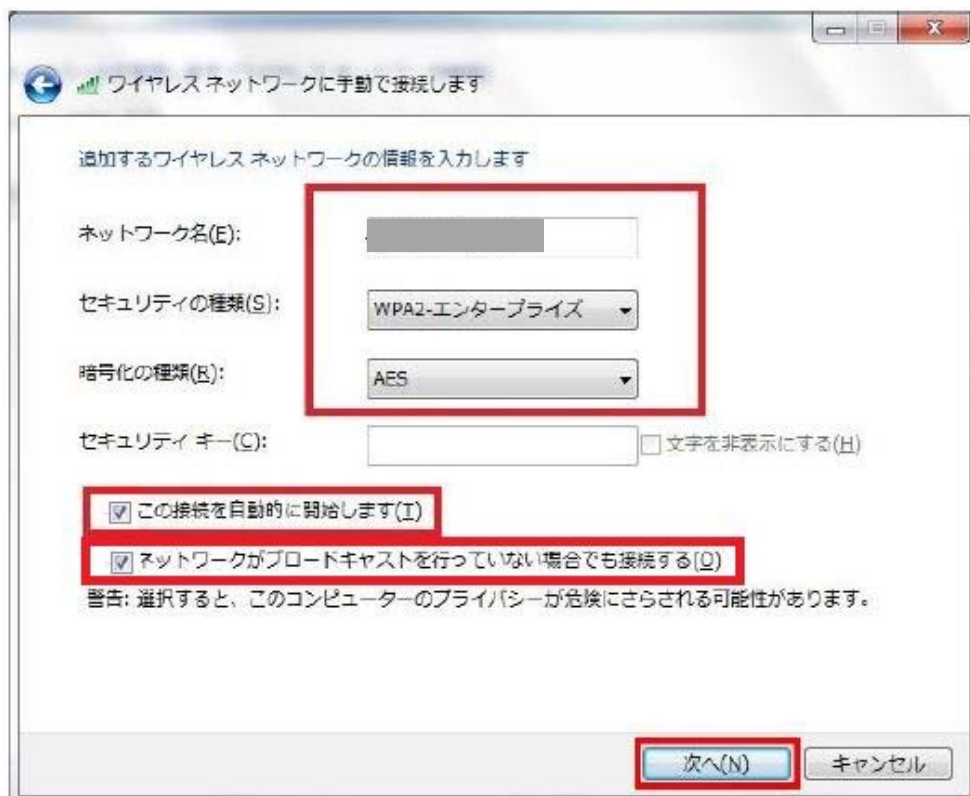


- v. “完了” ボタンを押すと証明書がインポートされる



## 2) Wi-Fi の接続を設定する

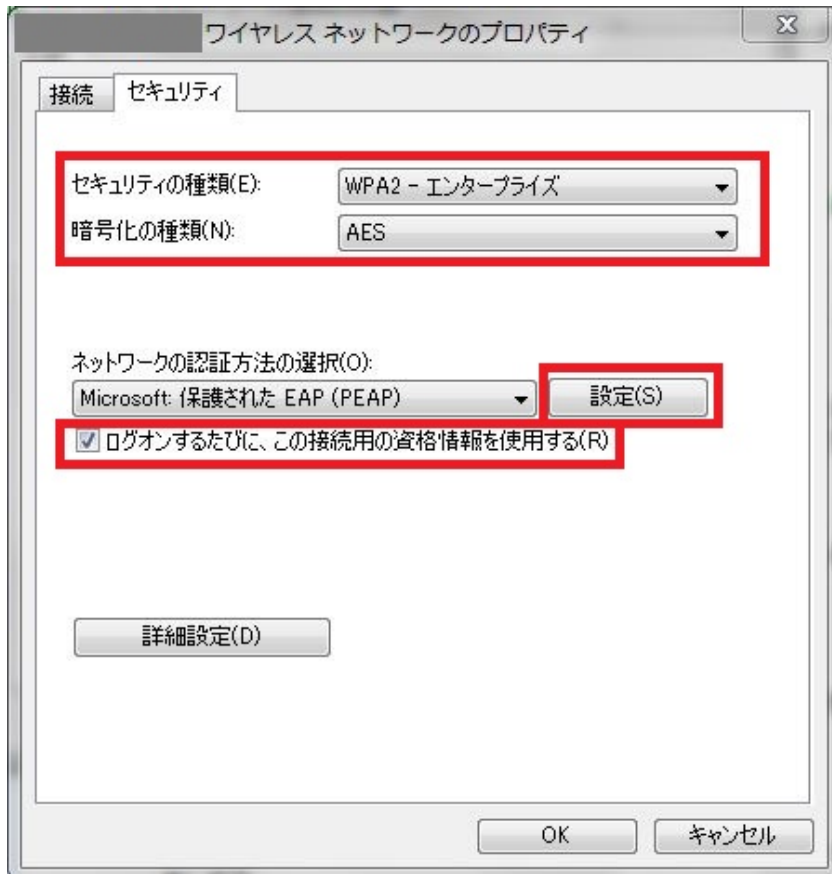
ネットワークの情報で、SSID、セキュリティの種類に「WPA2-エンタープライズ」、暗号化で「AES」を選択。セキュリティキーは空欄のままとして、“この接続を自動的に開始” 及び“ネットワークがブロードキャストを行っていない場合でも接続する” のチェックを入れて、“次へ” ボタンを押す。



3) 「接続の設定を変更します」をクリック。

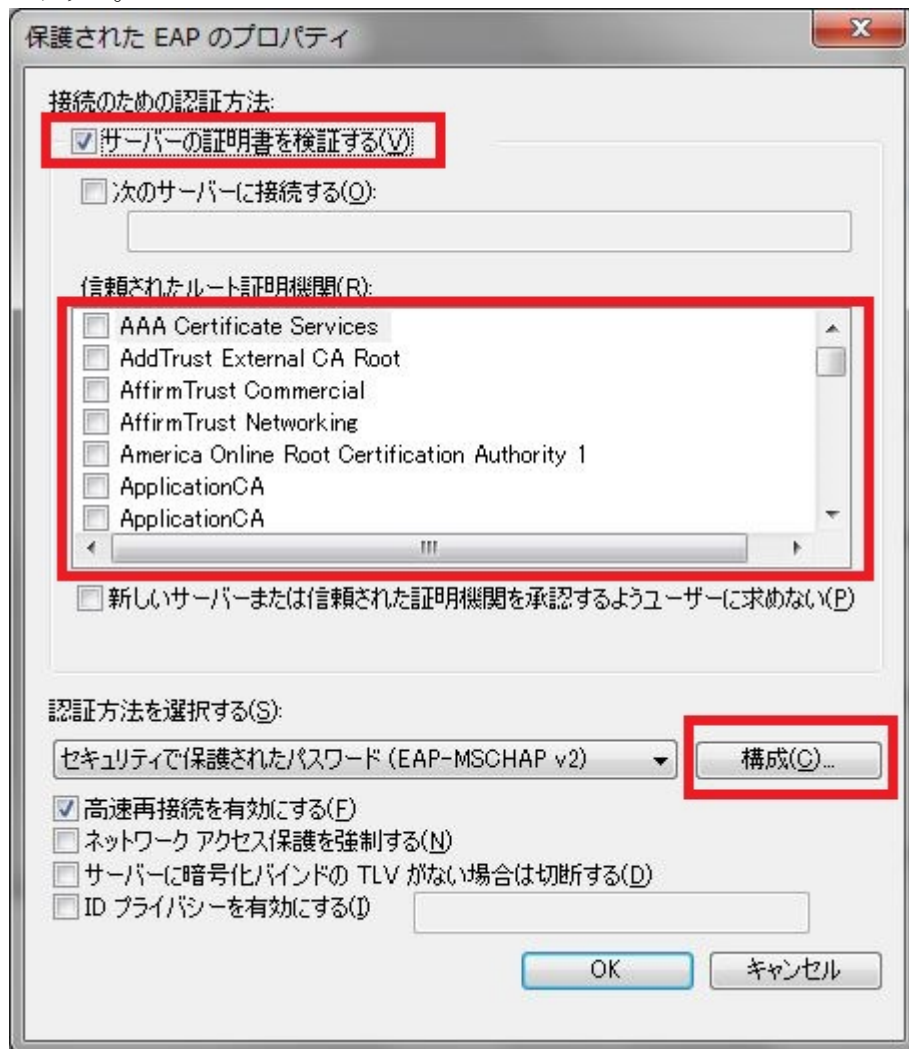


4) セキュリティタブで、ネットワーク認証方法の選択を「Microsoft 保護された EAP(PEAP)」を選択、「ログオンするたびに、この接続用の資格情報を使用する」をチェックし、「設定」をクリック。

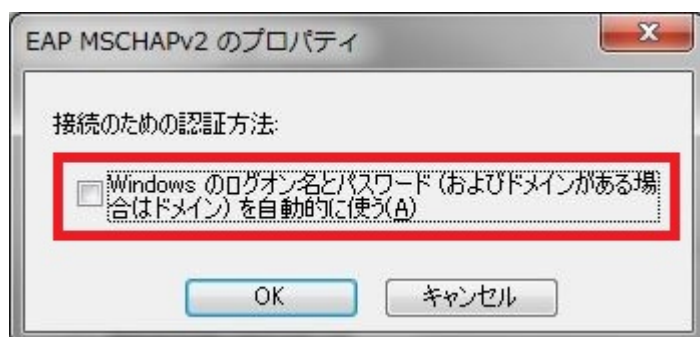


5) “サーバの証明書を検証する” にチェックがあることを確認し、インポートした CA 証明書にチェックを入れる。

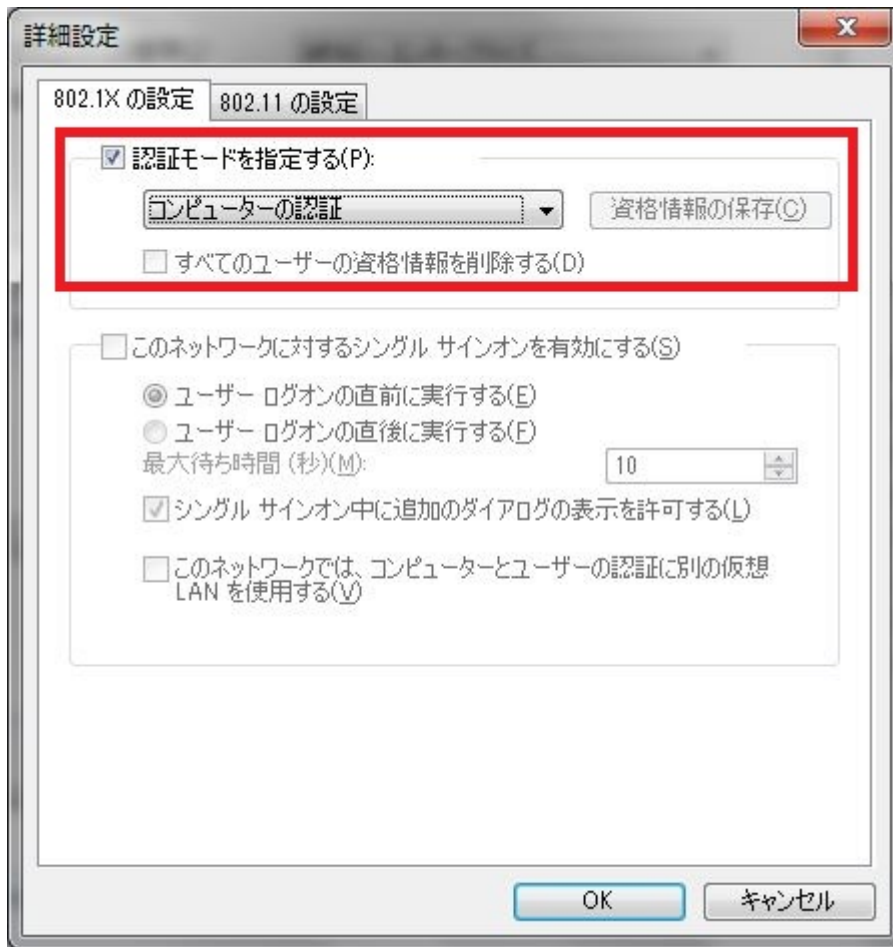
認証方法を選択するで “セキュリティで保護されたパスワード (EAP-MSCHAP v2)” を選択し、“構成” をクリック。



6) 接続のための認証情報から、「Windows のログオン名とパスワードを自動的に使う」のチェックを外す



7) ワイヤレスネットワークのプロパティまで戻り、「詳細設定」をクリックする。  
802.1x の認証モードの指定で、ユーザ認証を選択する。



## A.3. 安全管理ガイドラインの推奨要件（D 項）を満たす設定例（802.1x を EAP-TLS で利用するモデル）

9.3 に説明した運用例を実現するための設定例を次に示す。

### A.3.1 Wi-FiAP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA2-PSK の設定

The screenshot shows the configuration page for '無線1 仮想AP' (Wireless 1 Virtual AP). The left sidebar contains a navigation menu with '無線設定' (Wireless Settings) expanded to '仮想AP' (Virtual AP). The main content area is divided into two sections:

- 仮想AP設定 (Virtual AP Settings):**
  - インターフェース: ath0
  - 仮想AP:  無効  有効
  - SSID: ※※※※※※※※※※ (highlighted with a red box)
  - VLAN ID: 0
  - ANY接続拒否:  無効  有効
  - 接続端末制限: 63
  - アカウントテイング:  無効  有効
  - MAC認証:  無効  有効
- 暗号化設定 (Encryption Settings):**
  - ネットワーク認証: WPA2-PSK
  - 暗号化方式: AES
  - PSK (Pre-Shared Key): ※※※※※※※※※※ (highlighted with a red box)
  - WPAキー更新間隔: 120 分

- ② Wi-Fi AP の設定  
RADIUS サーバの設定

The screenshot shows the configuration page for '無線1 認証サーバー' (Wireless 1 Authentication Server). The left sidebar contains a navigation menu with '無線設定' (Wireless Settings) expanded to '認証サーバー' (Authentication Server). The main content area is divided into two sections:

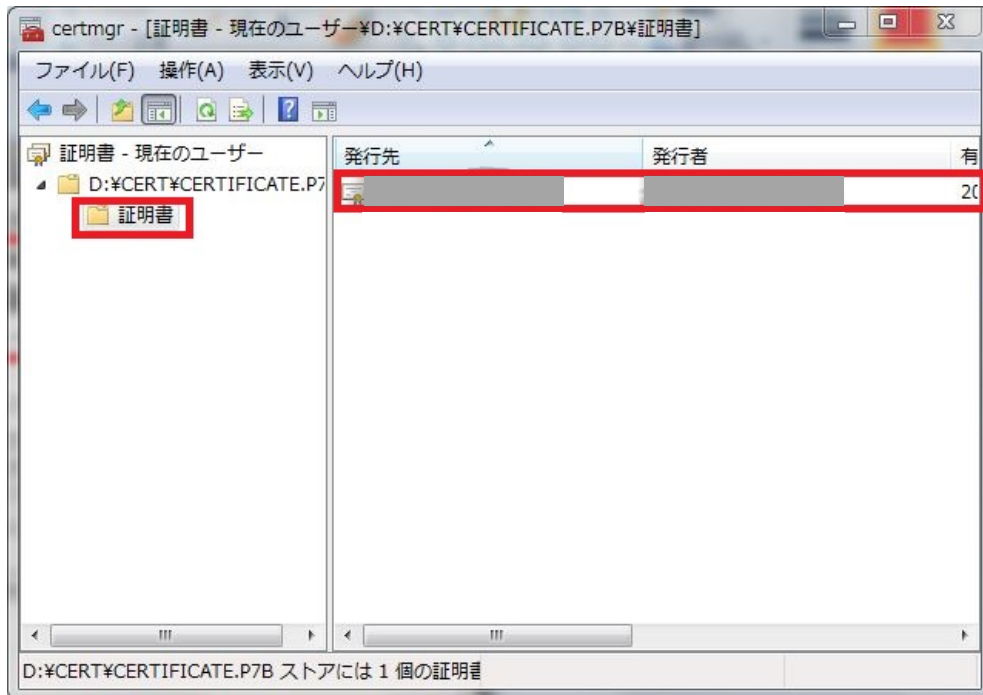
- RADIUS設定 (RADIUS Settings):**
  - アドレス: XXX.XXX.XXX.XXX (highlighted with a red box)
  - ポート: 1812
  - シークレット: XXXXXXXXXXXX
  - セカンダリー: 1812
  - secret
- アカウントテイング設定 (Accounting Settings):**
  - アドレス: XXX.XXX.XXX.XXX (highlighted with a red box)
  - ポート: 1813
  - シークレット: XXXXXXXXXXXX
  - セカンダリー: 1813
  - secret

Buttons for '登録' (Register) and '取消' (Cancel) are visible at the bottom right.

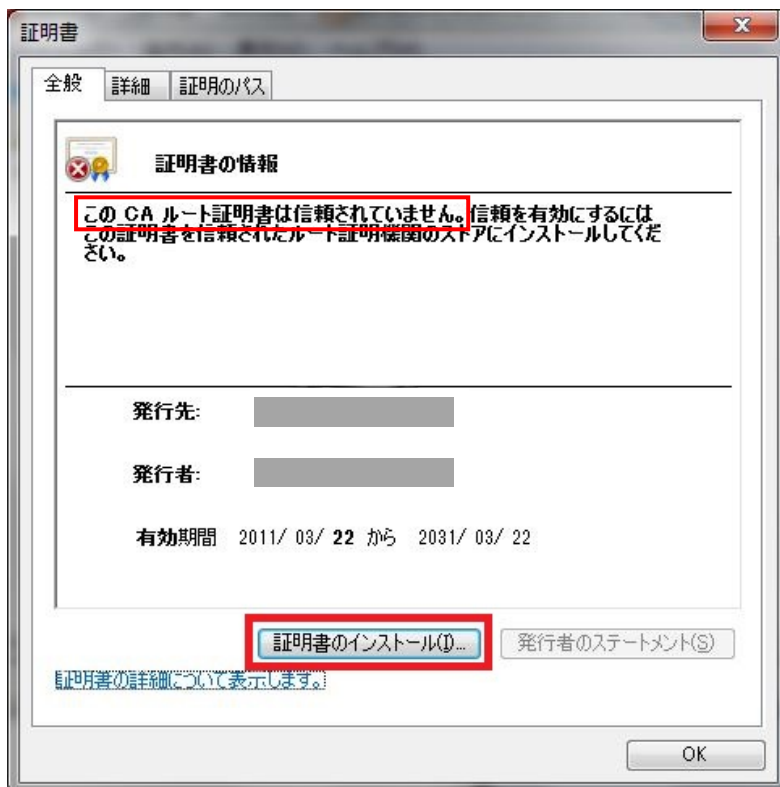
### A.3.2 医療機器等の設定例

#### 1) ルート証明書のインポート

- i. 設定する証明書ファイルをダブルクリックする。CERTMGR が起動するので、証明書をクリックするとインストール対象の証明書のリストが表示される。

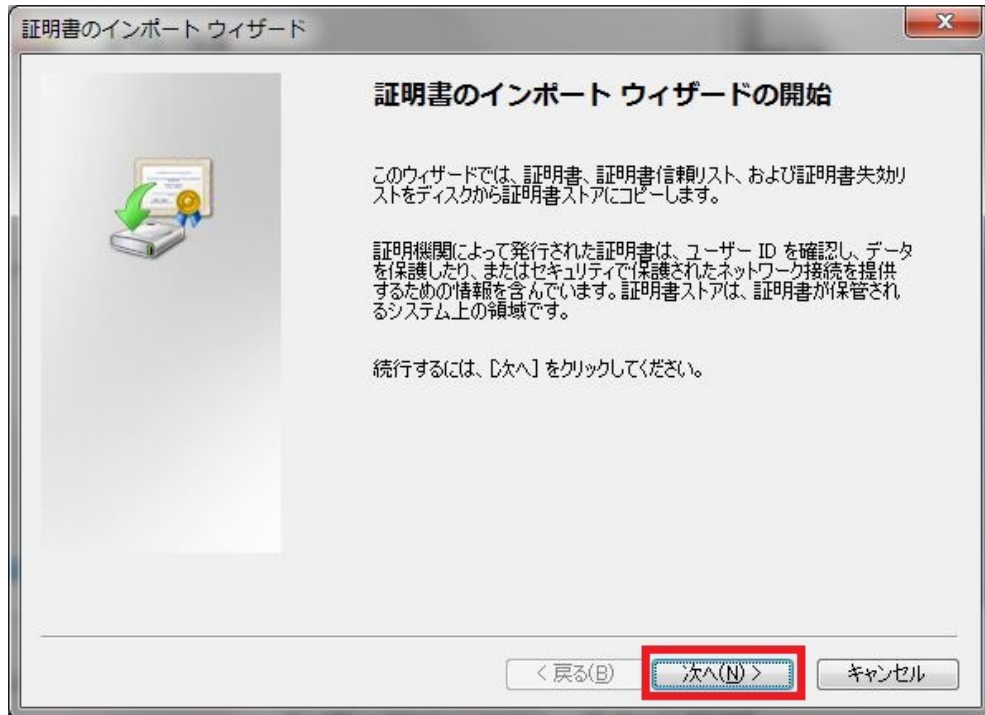


- ii. インポートする証明書の内容が表示されるので、間違いなければ“証明書のインストール”ボタンを押す。インポートする際には、医療機関等のポリシーに適合する証明書であることを確認すること。

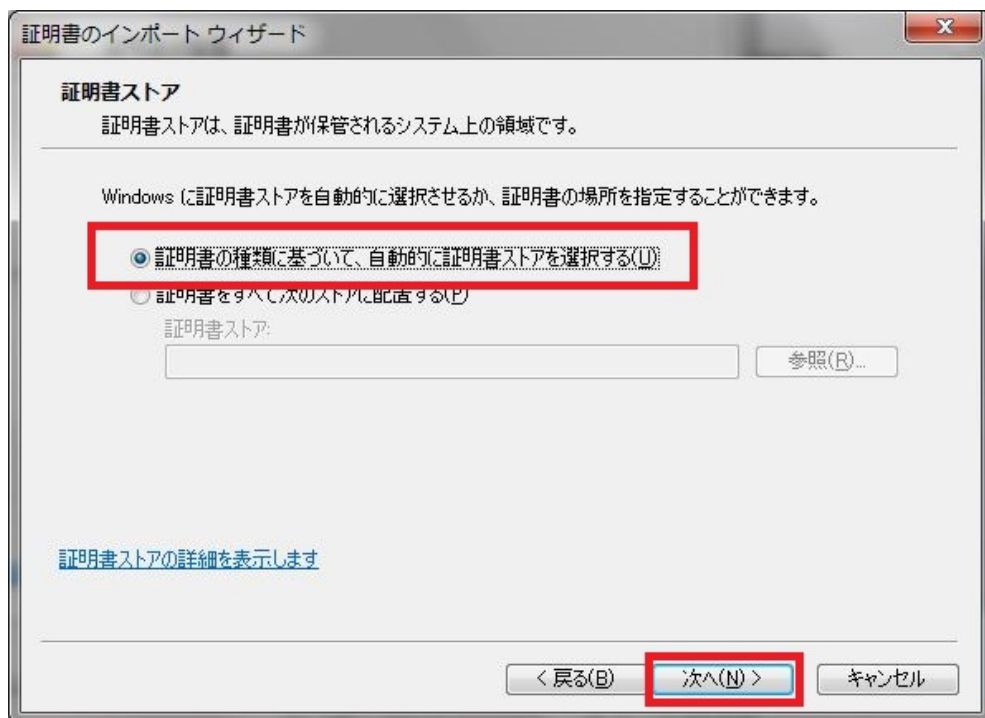




iii. 証明書のインポートウィザードが始まるので、“次へ” ボタンを押す。

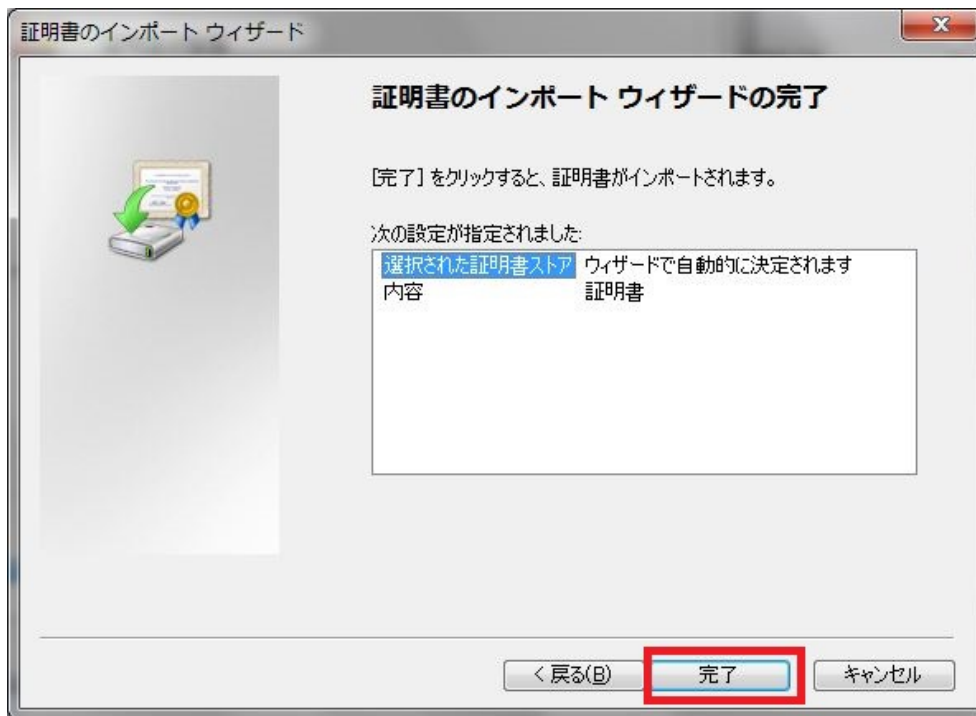


iv. 証明書ストアを“自動的に選択させる”を選択し、“次へ” ボタンを押す



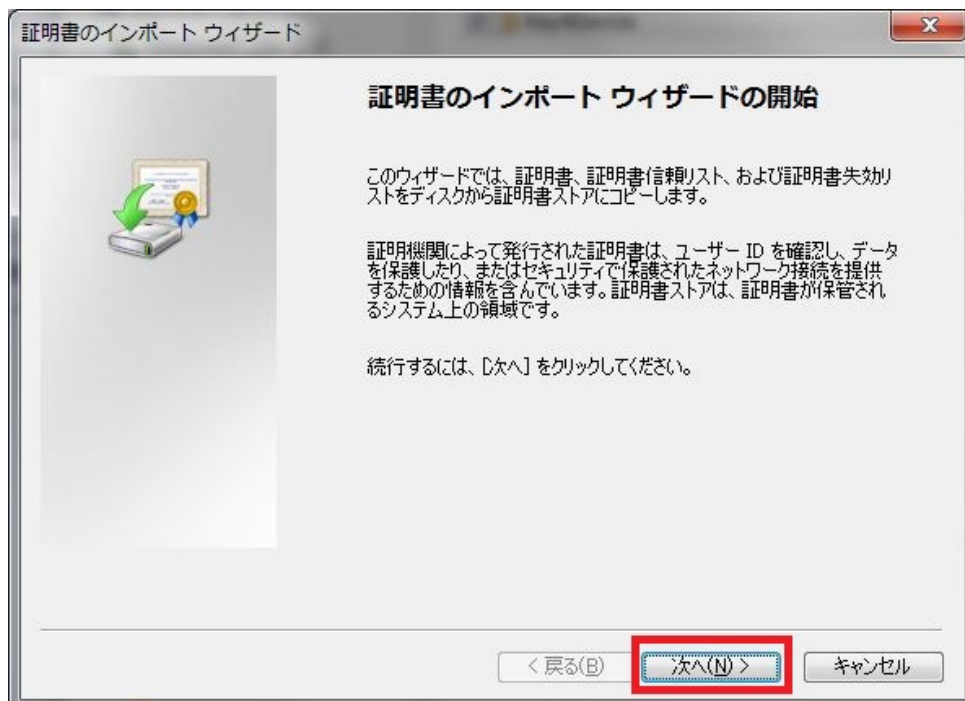


- v. “完了” ボタンを押すと証明書がインストールされる

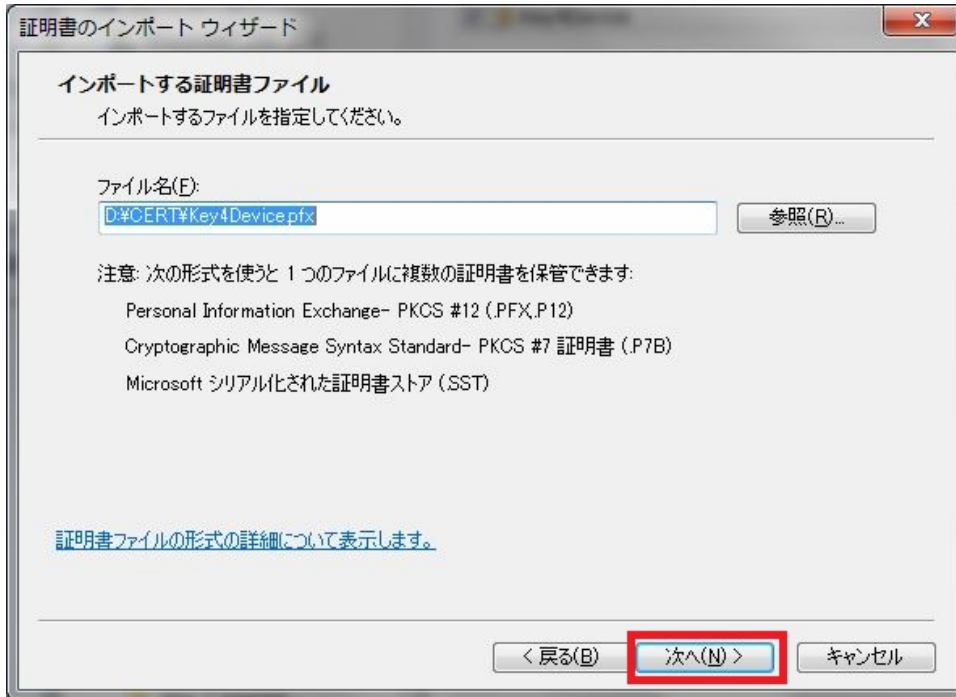


2) 機器証明書のインポート

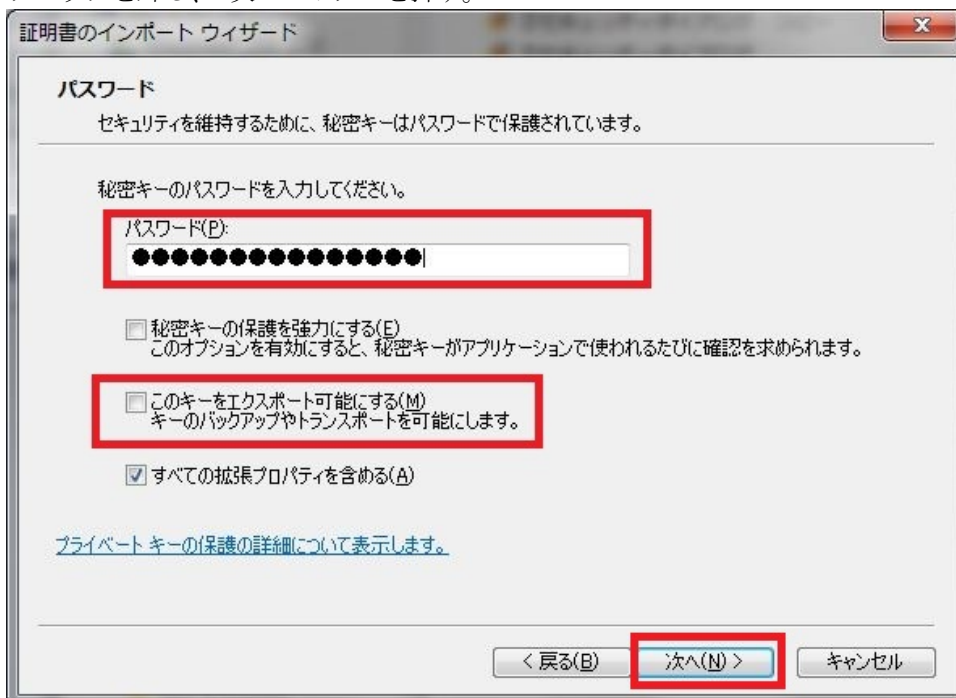
- i. 証明書ファイルをダブルクリックする。証明書のインポートウィザードが始まるので、“次へ” ボタンを押す。



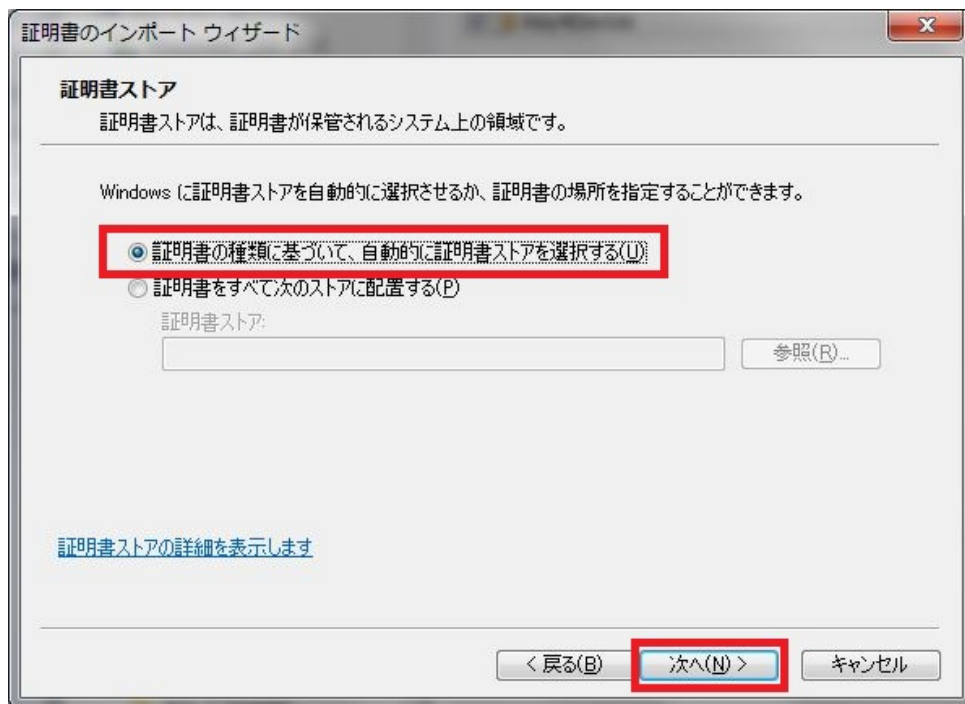
- ii. ファイル名を確認して“次へ”ボタンを押す。



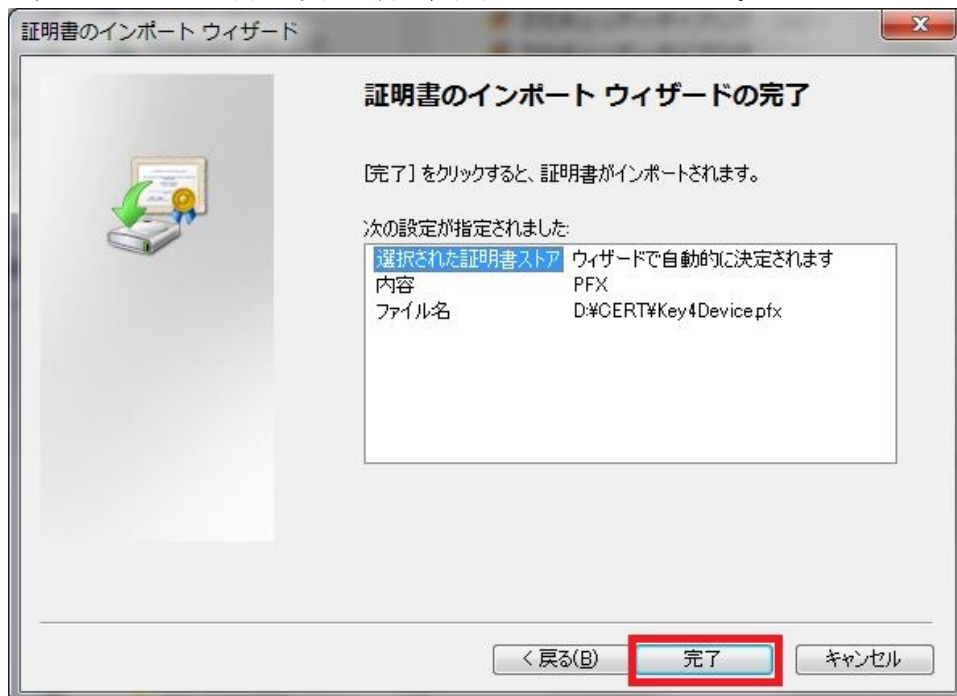
- iii. ファイル(PKCS#12)に設定されたパスワードを入力する。“このキーをエクスポート可能にする”のチェックを外し、“次へ”ボタンを押す。



- iv. 証明書ストアは自動選択を設定して“次へ”ボタンを押す

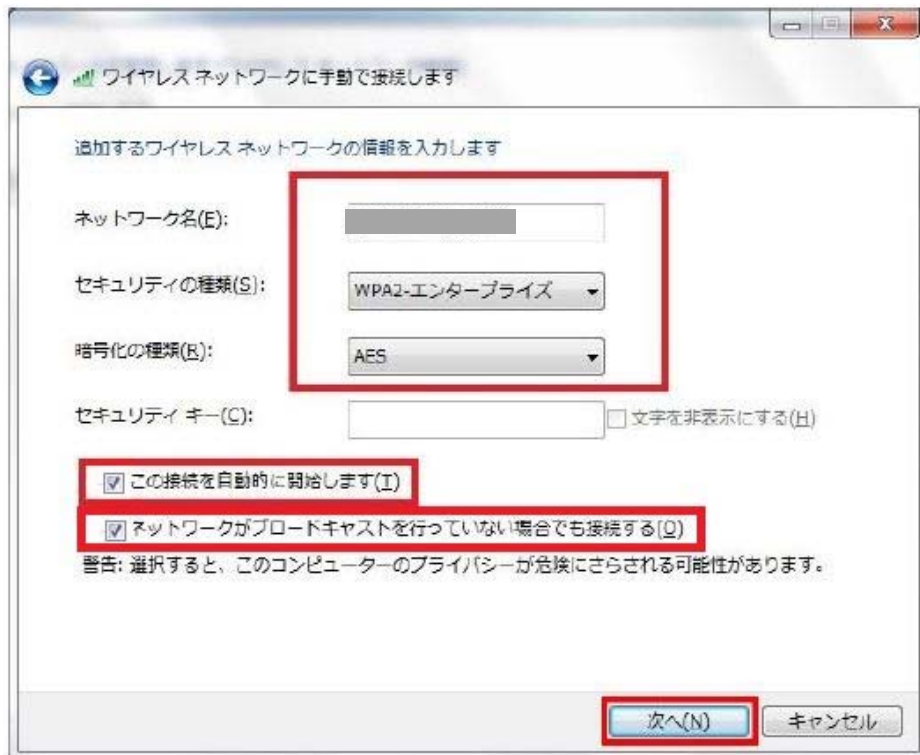


- v. “完了” ボタンを押すと、証明書と秘密鍵がインポートされる。

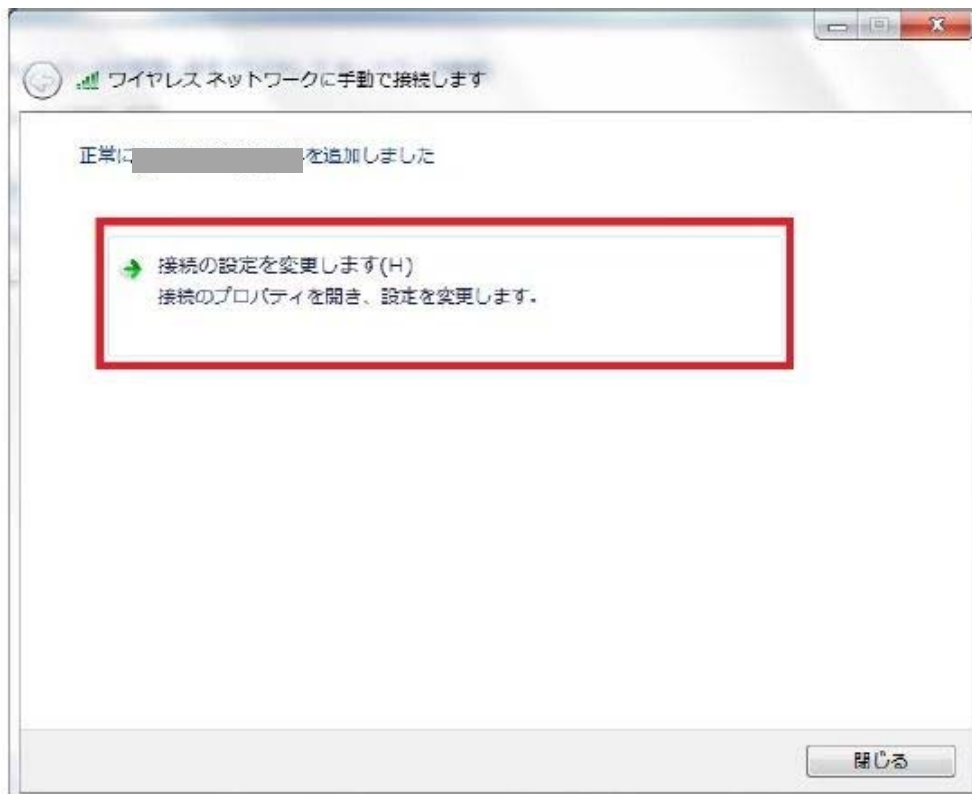


### 3) Wi-Fi の接続を設定する

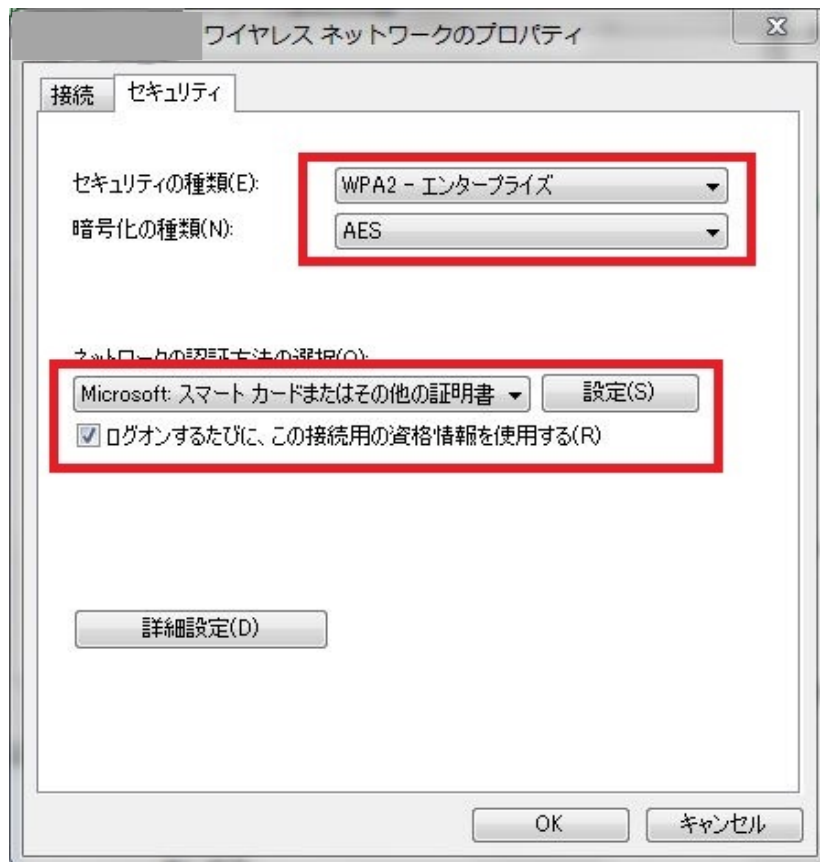
ネットワークの情報で、SSID、セキュリティの種類に「WPA2-エンタープライズ」、暗号化で「AES」を選択。セキュリティキーは空欄のままとして、“この接続を自動的に開始”及び“ネットワークがブロードキャストを行っていない場合でも接続する”のチェックを入れて、“次へ”ボタンを押す。



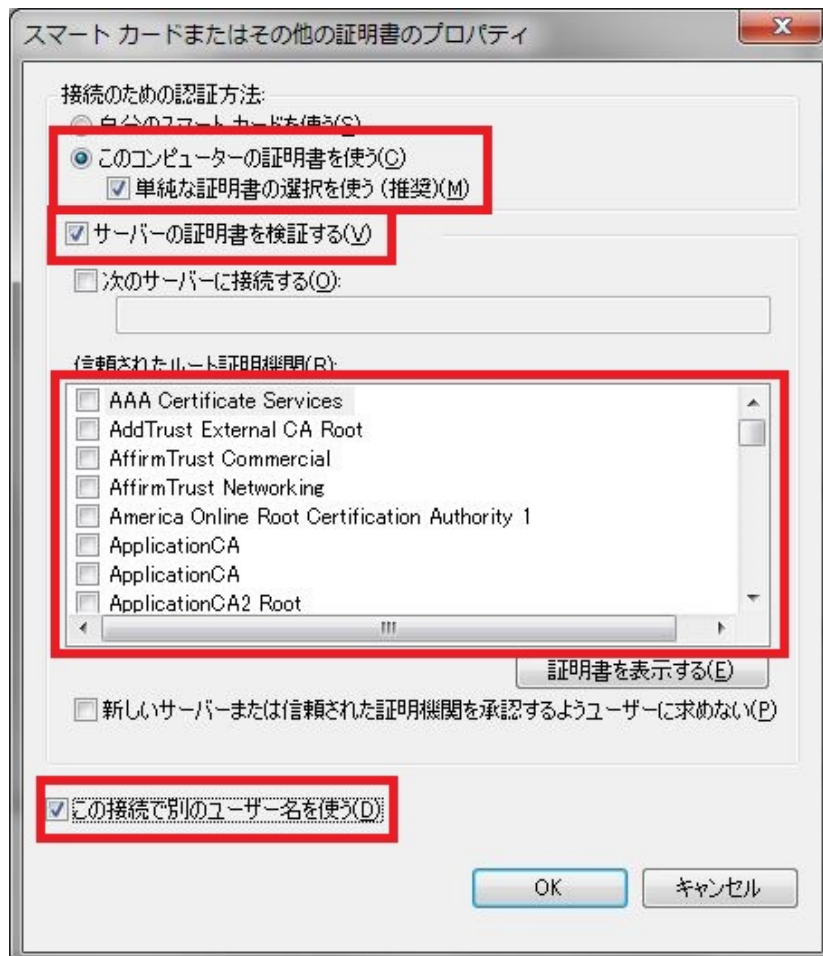
### 4) 「接続の設定を変更します」をクリック。



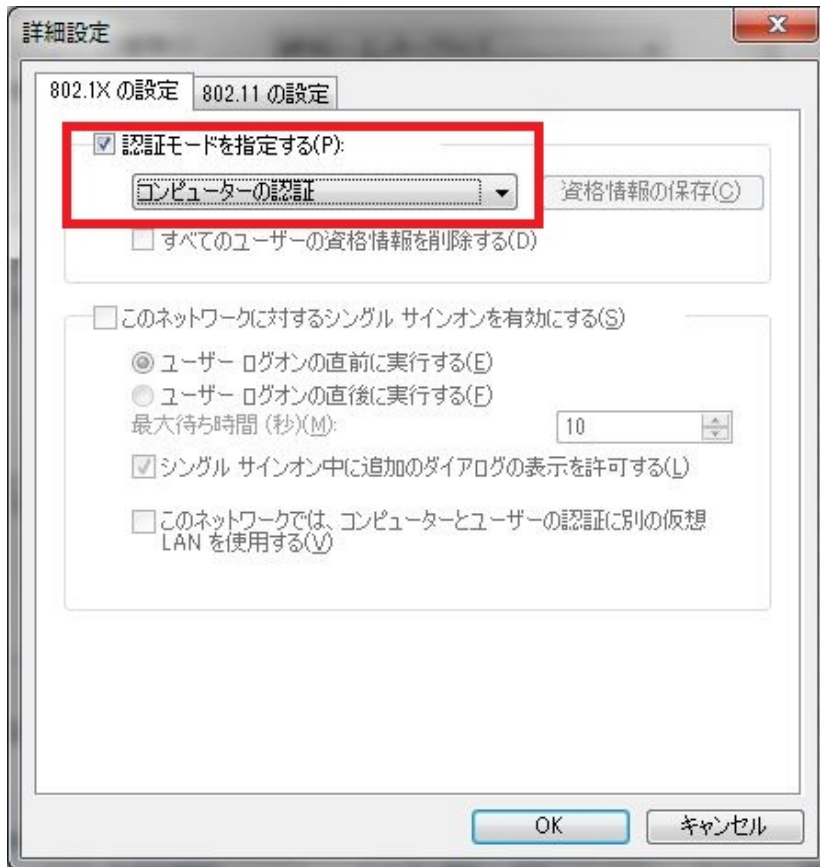
5) セキュリティタブで、ネットワーク認証方法の選択を“Microsoft スマートカードまたはその他の証明書”を選択、“ログオンするたびに、この接続用の資格情報を使用する”をチェックし、“設定”をクリック。



5) “サーバの証明書を検証する” にチェックがあることを確認し、インポートした CA 証明書にチェックを入れる。接続のための認証方法で “このコンピュータの証明書を使う” を選択し、“単純な証明書の選択を使う” にチェックを入れる。“この接続で別のユーザ名を使う” をチェックし、“OK” ボタンを押す。



6) ワイヤレスネットワークのプロパティまで戻り、「詳細設定」をクリックする。  
認証モードの指定で、コンピュータ認証を選択する。



7) SSID を選択して接続を開始すると証明書の選択画面が出るので、インストールした機器証明書を選択する。

## 附属書B CAの運用例

### B.1. 概要

本附属書では、RADIUS サーバ及び医療機器等に発行する証明書管理において注意すべき点を証明書のライフサイクル、医療機器等のライフサイクルの観点で説明する。証明書の発行は、第三者が運用する信頼できる CA から発行を受ける場合と、医療機関等が運営する CA を利用する場合がある。本附属書では、後者の場合の一例を説明する。図 B.1 に示す通り、ルートとなるプライベート CA によって RADIUS サーバ及び医療機器等への機器証明書を発行する。

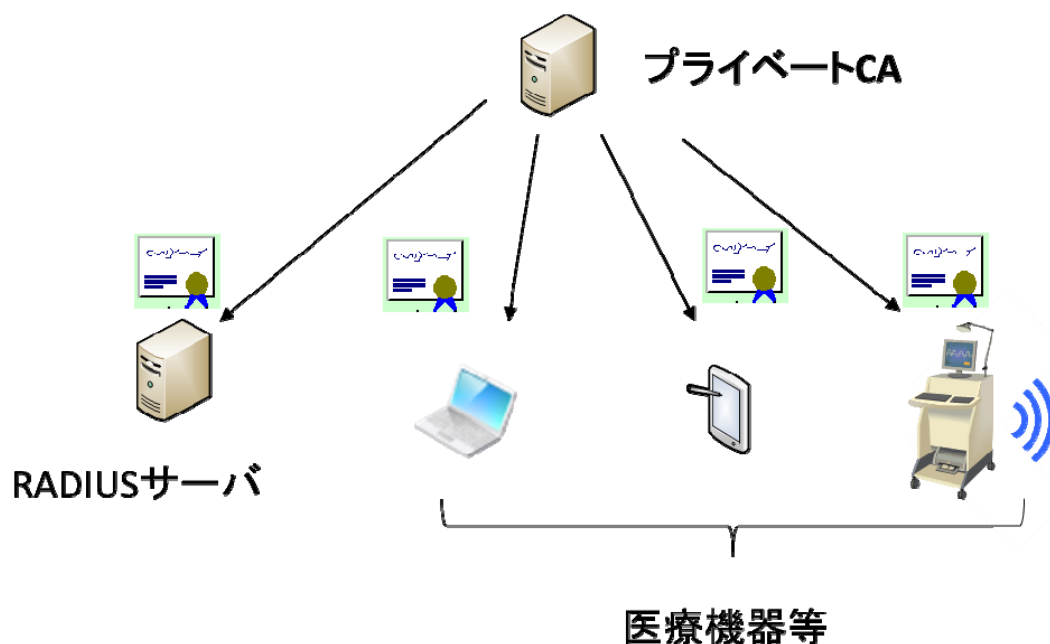


図 B.1 プライベート CA による証明書発行

### B.2. プライベート CA の構築

- ① CA の構築  
医療機関等で機器管理を行うためのプライベート CA を構築及び運用する。適応するのはその医療機関等が管理する医療機器等に限定し、医療機関等が信頼できる範囲となる。
- ② CA の運用  
医療機関等は適切な CA の管理を行わなくてはならない
- ③ 失効リスト(CRL)  
CRL は RADIUS サーバに反映すること。

### B.3. RADIUS サーバ証明書の発行

- ① 証明書の RADIUS サーバへのインポート  
一般的には RADIUS サーバ内で鍵ペアを生成し、公開鍵への証明書発行を CA に依頼する。発行を受けた証明書は RADIUS サーバ内に格納する。秘密鍵と対応する証明書はセキュアトークンで管理することが必



要となる。

② 証明書の更新

証明書は有効期限があるため、有効期限が切れる前に証明書の更新を行う必要がある。更新する証明書は、CA から発行を受ける。①と同様に RADIUS サーバにインストールする。

③ RADIUS サーバの更新

RADIUS サーバを運用する機器の耐用年数等によって、ハードウェアを更新するケースも想定される。その場合には、①の手順で新たな証明書の発行を受けて導入した RADIUS サーバにインポートする。新たな RADIUS サーバの運用が開始された後、旧 RADIUS サーバの証明書の失効管理を行う必要がある。

## B.4. 医療機器等に対する機器認証用の証明書発行

① 証明書の発行

証明書の発行は、第三者が運用する信頼できる CA から発行を受ける場合と、医療機関等が運営する CA を利用する場合がある。後者の場合には、証明書を利用する範囲は当該医療機関等に限定した運用をする必要がある。

② 証明書の医療機器等へのインポート

証明書の発行は、オンラインの場合とオフラインの場合がある。CA から発行を受けた証明書は医療機器等のセキュアトークンで管理することが必要となる。

③ 証明書の更新

証明書は有効期限があるため、有効期限が切れる前に証明書の更新を行う必要がある。更新する証明書は、①と同様に CA から発行を受け、②と同様に医療機器等にインポートする。

④ 医療機器等の廃棄

機器の管理者は CA にどの機器が廃棄されたのかを伝え、CA に証明書の失効を依頼する。CA は適切な失効管理を行う。

## 附属書 C 機器への組み込み例

### C.1. 概要

医療機器等に Wi-Fi 機能を組み込む際には、PC など既に Wi-Fi 接続に必要なハードウェア及びソフトウェアを搭載したコンポーネントを利用する場合と、機器に必要なハードウェア及びソフトウェアを組み込む場合の2つの実装方法が存在する。それぞれの実装に関してその方法の概要を示す。必要に応じて、本文及びその PC 等の説明書を参考に実施すること。

### C.2. PC 内蔵型

ここでは、市販されている Windows OS を搭載した PC を例にして説明する。セキュアトークンによるクレデンシャルの保護が必要で OS が備えている保護領域(ソフトウェアトークン)を利用する方法と、USB 型のトークンなどのハードウェアを利用する方法がある。

クレデンシャルの管理の際にはファイル名やパスワードの入力にキーボードなどの入力デバイスが必要になる。

必要となる機器等例

- PC
- OS(Windows)： サプリカント、暗号ライブラリ、証明書ストア(ソフトウェアトークンの場合) 通常の Windows OS には含まれている。ただし、Embedded 版ではそのモジュールを含まれない場合もあるので、含めるようにすること
- Key Board
- Wi-Fi I/F： Wi-Fi 認定されたもの
- USB 型トークン等(ソフトウェアトークンでない場合)。下記、証明書がストアされている。
- 証明書(医療機関等が管理しているもの。発行は医療機関等のポリシーに依存)

必要となる設定例

#### 1) (ソフトウェアトークンの場合)

証明書ストアに CA から発行されたクレデンシャルをインストールする方法 (インタフェース) が必要となる。例えば、証明書をネットワーク経由で入手可能である場合、その証明書をダブルクリックすることにより証明書をインストールするウィザードが起動し、インストールできる。可搬媒体を通じてファイルとして入手可能である場合、その媒体からインストールする。クレデンシャルを含むファイルをダブルクリックすることによりクレデンシャルをインストールするウィザードが起動し、インストールできる。認証に用いる鍵及び証明書は取り出せない形でインストールする必要がある。

(ハードウェアトークンの場合)

ハードウェアトークンを接続する I/F が必要 (例えば USB)。

ハードウェアトークンに証明書をインストールするためには別な装置を利用してクレデンシャルをインストールするか、あるいは機器にインストールする手段が必要

- #### 2) 無線 LAN の設定において、その証明書を利用する旨の設定が必要。不正アクセス防止のためパスワード等を設定すること。
- #### 3) RADIUS サーバ設置の場合は、RADIUS サーバの証明書をインストールする。RADIUS サーバには、本装置の機器 ID 及び証明書を設定することも必要になる。

### C.3. 組み込み型

組み込み型の場合には、Wi-Fi に対応したハードウェアの組み込みと、ハードウェアを動作させるソフトウェアが必要となる。また、クレデンシャルの管理を行う際には、ファイル名やパスワードの入力を行うた

めにディスプレイ等の表示機能とキーボード等の入力機能が必要となる。

接続の互換性を保証するためには、Wi-Fi 認定の取得が必要となる。少なくとも Standard IEEE、WPA、WPA2、EAP 等の確認が必要となる。詳細は Wi-Fi Alliance の情報を確認のこと<sup>2</sup>。

Wi-Fi の機能を実現するためには、IEEE 802.11n 等の無線仕様に適合するハードウェア、無線の動作を実現するサブリカント、セキュリティを確保するための暗号ライブラリ等のソフトウェアが必要となる。秘密情報（暗号鍵や機器 ID/パスワード）やクレデンシャルの管理には、セキュアトークンを用いるなどの保護が必要となる。

---

<sup>2</sup> Wi-Fi Alliance に関しては、<http://www.wi-fi.org/> を参照  
© JAHIS 2017

## 付録— 1. 参考文献

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

NIST SP800-120 *Recommendation for EAP Methods Used in Wireless Network Access Authentication*

NIST SPECIAL PUBLICATION 1800-1b (DRAFT), *ECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES, Approach, Architecture, and Security Characteristics*

ITU-T X.509 *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, 10/2016

RFC 3748 *Extensible Authentication Protocol(EAP)*, June 2004

RFC 5216, *The EAP-TLS Authentication Protocol*, March 2008

PEAP V0

Microsoft's PEAP version 0 (Implementation in Windows XP SP1), October 2002

<https://tools.ietf.org/html/draft-kamath-pppext-peapv0-00>

PEAP V1

Protecting EAP with TLS (EAP-TLS-EAP), August 2001

<https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-00>

PEAP V2

Protected EAP Protocol (PEAP), March 2003

<https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06>

## 付録—2. 作成者名簿

作成者（社名五十音順）

下野 兼揮	(株)グッドマン
松本 泰	セコム(株)
半田 富己男	大日本印刷(株)
浅野 之治	凸版印刷(株)
遠藤 方洋	凸版印刷(株)
平田 泰三	(一社)日本画像医療システム工業会(J I R A)
小出 一希	日本光電工業(株)
藤咲 喜丈	日本光電工業(株)
別府 嗣信	日本光電工業(株)
梶山 孝治	(株)日立製作所
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(株)
谷内田 益義	(株)リコー

改定履歴		
日付	バージョン	内容
2017/03/31	Ver. 1.0	初版

(JAHIS技術文書 16-103)

2017年3月発行

JAHIS セキュアトークン実装ガイド・機器認証編

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

(無断複写・転載を禁ず)