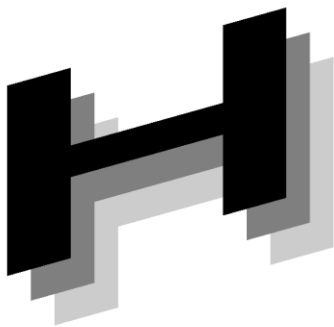




Japanese



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. 1.1 実装例

2024年4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 Ver.

## 1.1 実装例

### ま え が き

本書は、本編である「JAHIS セキュアトークン実装ガイド・機器認証編」で説明した Wi-Fi を用いて施設内ネットワークを構築する場合に「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の設定例を示したものである。利用に際しては、本編の内容を理解した上で利用することを前提としているので、本書の利用者はその点に留意されたい。

本書が、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4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 >>

本実装例は関連団体の所属の有無に関わらず、実装例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、本実装例に準拠する旨を表現することは厳禁するものとします。

本実装例ならびに本実装例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、本実装例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実装例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. 本書の構成 .....	1
2. 運用モデルを実現する設定 .....	1
概要.....	1
2.2. 最低限の不正アクセス対策の実現（MAC アドレスフィルタリングを行うモデル） .....	1
2.2.1. 概要.....	1
2.2.2. Wi-Fi AP の設定例.....	1
2.2.3. 医療機器等の設定例.....	3
2.3. 端末認証によって不正端末の接続を防止する設定例（802.1x を EAP-PEAP で利用するモデル） .....	6
2.3.1. 概要.....	6
2.3.2. Wi-Fi AP の設定例.....	6
2.3.3. 医療機器等の設定例.....	10
2.4. 端末認証によって不正端末の接続を防止する設定例（802.1x を EAP-TLS で利用するモデル） .....	20
2.4.1. 概要.....	20
2.4.2. Wi-Fi AP の設定例.....	20
2.4.3. 医療機器等の設定例.....	24
3. CA の運用例.....	37
3.1. 概要 .....	37
3.2. プライベート CA の構築.....	37
3.3. RADIUS サーバ証明書の発行.....	37
3.4. 医療機器等に対する機器認証用の証明書発行.....	38
4. 機器への組み込み例.....	39
4.1. 概要 .....	39
4.2. PC 内蔵型.....	39
4.3. 組み込み型 .....	39
5. WPA2 及び WPA3 が混在する場合の運用例.....	40
付録－1. 参考文献 .....	41
付録－2. 作成者名簿.....	42

# 1. 本書の構成

・本編である“セキュアトークンガイド・機器認証編”では、採用する技術・標準類とそれらを利用するモデルについて説明している。本書では、本編で説明した技術・標準類を用いた運用モデルを実現するための具体的な設定例等について説明する。

・用語および略語は、本編の規定に従う。

## 2. 運用モデルを実現する設定

### 2.1. 概要

本書**実装例**では、本編 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 の設定例として株式会社バッファロー WAPM-AX4R の設定画面例を、医療機器等の設定例として Microsoft 社 Windows 11 の設定画面例を示す<sup>1</sup>。

### 2.2. 最低限の不正アクセス対策の実現（MAC アドレスフィルタリングを行うモデル）

#### 2.2.1. 概要

本節では、本編 9.1 に説明した MAC アドレスフィルタリングによって最低限の不正アクセス対策を行う場合の設定例を示す。

#### 2.2.2. Wi-Fi AP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA3-Personal(AES)の設定

---

<sup>1</sup> 記載されている各社の商品名は、商標または登録商標です。

Wi-Fi	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	WAPM-AX4R-XXXX						
次の場合に有効にする	通常時と緊急時						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
ステアリング	無効						
優先制御	優先						
VLAN ID	<table border="1"> <thead> <tr> <th>VLANモード</th> <th>VLAN ID</th> <th>追加VLAN ID</th> </tr> </thead> <tbody> <tr> <td>Untagged Port</td> <td>1</td> <td></td> </tr> </tbody> </table>	VLANモード	VLAN ID	追加VLAN ID	Untagged Port	1	
VLANモード	VLAN ID	追加VLAN ID					
Untagged Port	1						
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	使用しない						
ロードバランス(同時接続台数制限)	<table border="1"> <thead> <tr> <th>2.4GHz</th> <th>5GHz</th> </tr> </thead> <tbody> <tr> <td>128 / 128</td> <td>128 / 128</td> </tr> </tbody> </table>	2.4GHz	5GHz	128 / 128	128 / 128		
2.4GHz	5GHz						
128 / 128	128 / 128						
Wi-Fiの認証	WPA3 Personal						
暗号化方式	AES						
キー更新間隔	60 分						
事前共有キー	XXXXXXXX						
Management Frame Protection	有効(Required)						
追加認証	MACアドレスリストによる制限						

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

### MACアクセス制限設定 - 登録リストの編集

編集を終了して前の画面へ戻る

#### 登録リストの新規追加

登録するMACアドレス

新規追加

#### 登録リスト

MACアドレス	操作
MACアドレスが登録されていません	

全てのMACアドレスを消去

#### 検出されたWi-Fi内蔵パソコン一覧

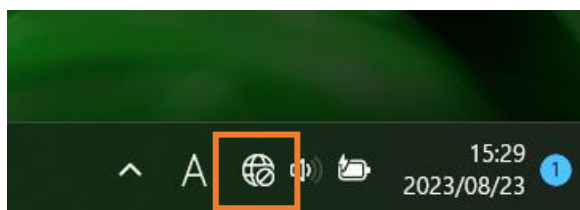
MACアドレス	操作
Wi-Fi内蔵パソコンは検出されていません	

現在の状態を表示

2.2.3. 医療機器等の設定例

SSID、WPA2/WPA3-PSK 等の設定 (Windows 11 の場合)

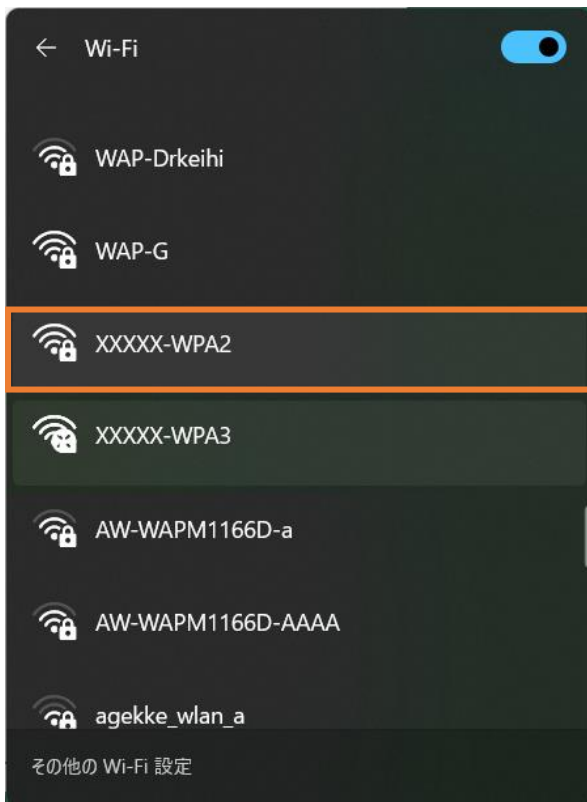
- i. 無線 LAN のアイコンをクリック



- ii. アンテナマーク横の「>」をクリック



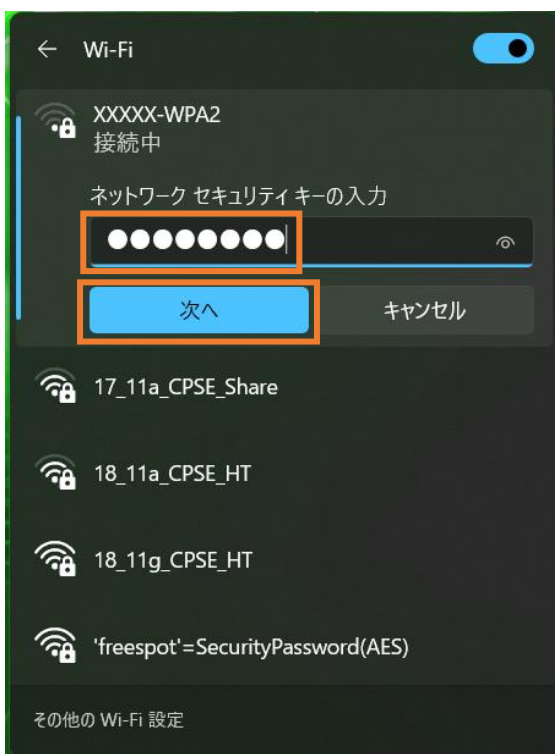
- iii. SSID をクリック



- iv. 「自動的に接続」にチェックが入っていることを確認し「接続」をクリック



- v. 「事前共有キー」PSKを入力し「次へ」をクリック





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

### 2.3.1. 概要

本設では、本編 9.2 に説明した 802.1x を EAP-PEAP による端末認証によって不正端末の接続を防止する場合の設定例を示す。

### 2.3.2. Wi-Fi AP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA3-Enterprise の設定

Wi-Fi	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	WAPM-AX4R-XXXX
次の場合に有効にする	通常時と緊急時
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
ステアリング	無効
優先制御	優先
VLAN ID	VLANモード: Untagged Port, VLAN ID: 1, 追加VLAN ID:
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	使用しない
ロードバランス(同時接続台数制限)	2.4GHz: 128 /128, 5GHz: 128 /128
Wi-Fiの認証	WPA3 Enterprise
暗号化方式	AES
キー更新間隔	60 分
Management Frame Protection	有効(Required)
追加認証	追加認証を行わない
RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する

## SSID、WPA2-Enterprise の設定

### SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	Wi-Fiの認証	暗号化		
1	有効	XXXXX-WPA3 1		<input type="radio"/>	<input type="radio"/>	無効	WPA3 Enterprise AES		編集	削除
2	有効	XXXXX-WPA2 1		<input type="radio"/>	<input type="radio"/>	無効	WPA2 Personal AES		修正中	

使用可能SSID	2.4GHz	5GHz
	14 /16	14 /16

Wi-Fi	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	XXXXX-WPA2
次の場合に有効にする	通常時と緊急時
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
ステアリング	無効
優先制御	優先
VLAN ID	VLANモード: Untagged Port, VLAN ID: 1, 追加VLAN ID:
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	使用しない
ロードバランス(同時接続台数制限)	2.4GHz: 128 /128, 5GHz: 128 /128

Wi-Fiの認証	WPA2 Enterprise
暗号化方式	AES
キー更新間隔	60 分
Management Frame Protection	無効
Fast Transition (802.11r)	無効, Mobility Domain ID:
追加認証	追加認証を行わない
RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する

修正保存

編集を終了して前の画面へ戻る

WPA3 と WPA2 の SSID が作成されていることを確認する

## SSID設定 - SSIDの編集

### ステアリング ポリシー設定

ステアリング ポリシー

### SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	Wi-Fiの認証	暗号化		
1	有効	XXXXX-WPA3	1	<input type="radio"/>	<input type="radio"/>	無効	WPA3 Enterprise AES		<input type="button" value="編集"/>	<input type="button" value="削除"/>
2	有効	XXXXX-WPA2	1	<input type="radio"/>	<input type="radio"/>	無効	WPA2 Enterprise AES		<input type="button" value="編集"/>	<input type="button" value="削除"/>

- ② Wi-Fi AP の設定  
RADIUS サーバの設定

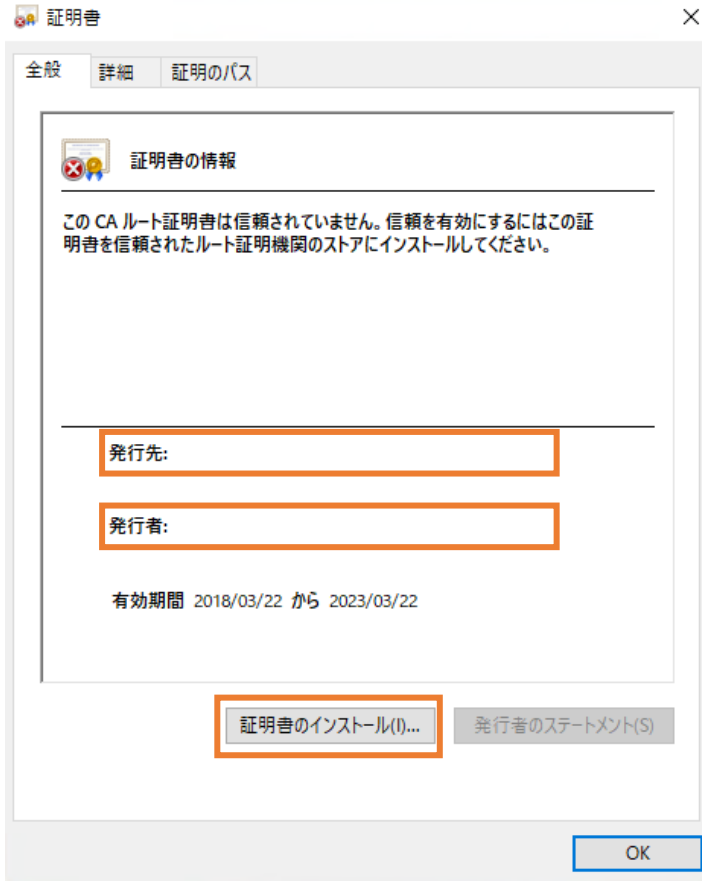
RADIUS設定	
<b>RADIUSサーバー</b>	
プライマリー-RADIUSサーバー	
サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	<input type="text"/>
認証ポート	<input type="text" value="1812"/>
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	<input type="text" value="1813"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
セカンダリー-RADIUSサーバー	
サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	<input type="text"/>
認証ポート	<input type="text" value="1812"/>
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	<input type="text" value="1813"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
Calling-Station-Id	""(区切りなし, 小文字) ▼
Called-Station-Id	""(区切りなし, 小文字) ▼
<input type="button" value="設定"/>	
<b>内蔵RADIUSサーバー</b>	
内蔵RADIUSサーバー	<input type="checkbox"/> 使用する
EAP内部認証	PEAP(MS-PEAP) ▼
EAP証明書ファイル形式	PKCS#12(*.pfx / *.p12)
EAP証明書ファイル	<input type="button" value="ファイルの選択"/> ファイルが選択されていません
EAP証明書ファイル・パスワード	<input type="text"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
Termination-Action	<input checked="" type="radio"/> 再認証を行う (RADIUS-Request) <input type="radio"/> 再認証を行わない(Default) <input type="radio"/> 送信しない
<input type="button" value="設定"/>	

### 2.3.3. 医療機器等の設定例

#### 1) ルート証明書のインポート

- i. ルート証明書ファイルをダブルクリックすると、下記ダイアログが表示される。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




- ii. 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



iii. 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



“完了” ボタンを押すと証明書がインポートされる

←  証明書のインポート ウィザード

### 証明書のインポート ウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:


ユーザーが選択した証明書ストア	ウィザードで自動的に決定されます
内容	証明書

完了(F)





キャンセル

## 2) Wi-Fi の接続を設定する

「接続またはネットワークのセットアップ」で「ワイヤレスネットワークに手動で接続します」をクリック

←  接続またはネットワークのセットアップ

### 接続オプションを選択します

-  **インターネットに接続します**  
ブロードバンドまたはダイヤルアップによるインターネットへの接続を設定します。
-  **新しいネットワークをセットアップする**  
新しいルーターまたはアクセス ポイントをセットアップします。
-  **ワイヤレス ネットワークに手動で接続します**  
非公開のネットワークに接続するか、または新しいワイヤレス プロファイルを作成します。
-  **職場に接続します**  
職場へのダイヤルアップまたは VPN 接続をセットアップします。

次へ(N)

キャンセル



### WPA3-Enterprise の場合

「ネットワーク名」に SSID を入力、「セキュリティの種類」で” WPA3-エンタープライズ」を選択、「この接続を自動的に開始します」と「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」にチェックを入れる

The screenshot shows a Windows dialog box titled "ワイヤレス ネットワークに手動で接続します" (Manually connect to wireless network). The main heading is "追加するワイヤレス ネットワークの情報を入力します" (Enter information for the wireless network to add). The fields are as follows:

- ネットワーク名(E): XXXXX-WPA3
- セキュリティの種類(S): WPA3-エンタープライズ
- 暗号化の種類(R): AES
- セキュリティキー(C): [Empty field]  文字を非表示にする(H)

Below the fields, there are two checked checkboxes:

- この接続を自動的に開始します(T)
- 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(O)

A warning message follows: "警告: 選択すると、このコンピューターのプライバシーが危険にさらされる可能性があります。" (Warning: Selecting this option may put the privacy of this computer at risk.)

At the bottom right, there are two buttons: "次へ(N)" (Next) and "キャンセル" (Cancel).

### WPA2-Enterprise の場合

「ネットワーク名」に SSID を入力、「セキュリティの種類」で” WPA2-エンタープライズ」を選択、「この接続を自動的に開始します」と「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」にチェックを入れる

← ワイヤレス ネットワークに手動で接続します

追加するワイヤレス ネットワークの情報を入力します

ネットワーク名(E): XXXXX-WPA2

セキュリティの種類(S): WPA2-エンタープライズ

暗号化の種類(R): AES

セキュリティキー(C):   文字を非表示にする(H)


この接続を自動的に開始します(T)

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(O)

警告: 選択すると、このコンピューターのプライバシーが危険にさらされる可能性があります。

次へ(N) キャンセル

3) 「接続の設定を変更します」をクリック

←  ワイヤレス ネットワークに手動で接続します

正常に XXXXX-WPA2 を追加しました

→ [接続の設定を変更します\(H\)](#)  
接続のプロパティを開き、設定を変更します。

閉じる

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

XXXXX-WPA2 ワイヤレス ネットワークのプロパティ

接続 セキュリティ

セキュリティの種類(E): WPA2 - エンタープライズ

暗号化の種類(N): AES

ネットワークの認証方法の選択(O):  
Microsoft: 保護された EAP (PEAP) 設定(S)

ログオンするたびに、この接続用の資格情報を使用する(R)

詳細設定(D)

OK キャンセル

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

保護された EAP のプロパティ

接続のための認証方法:

証明書を検証してサーバの ID を検証する(V)

次のサーバに接続する (例: srv1、srv2、.\*¥.srv3¥.com)(O):

信頼されたルート証明機関(R):

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3

接続前の通知(T):

サーバの ID を確認できない場合にユーザーに通知する

認証方法を選択する(S):

セキュリティで保護されたパスワード (EAP-MSCHAP v2) 構成(C)...

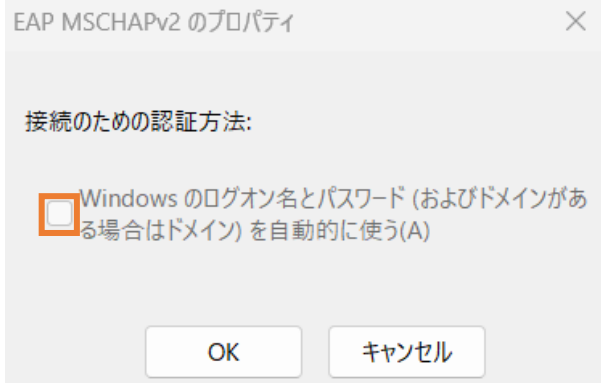
高速再接続を有効にする(F)

サーバに暗号化バインドの TLV がない場合は切断する(D)

ID プライバシーを有効にする(I)

OK キャンセル

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



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

### 2.4.1. 概要

本設では、本編 9.3 に説明した 802.1x を EAP-TLS による端末認証によって不正接続を防止する場合の設定例を示す。

### 2.4.2. Wi-Fi AP の設定例

- ① Wi-Fi AP の設定  
SSID、WPA3-Enterprise の設定

Wi-Fi	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	WAPM-AX4R-XXXX						
次の場合に有効にする	通常時と緊急時						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
ステアリング	無効						
優先制御	優先						
VLAN ID	<table border="1"><thead><tr><th>VLAN モード</th><th>VLAN ID</th><th>追加VLAN ID</th></tr></thead><tbody><tr><td>Untagged Port</td><td>1</td><td></td></tr></tbody></table>	VLAN モード	VLAN ID	追加VLAN ID	Untagged Port	1	
VLAN モード	VLAN ID	追加VLAN ID					
Untagged Port	1						
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	使用しない						
ロードバランス(同時接続台数制限)	<table border="1"><thead><tr><th>2.4GHz</th><th>5GHz</th></tr></thead><tbody><tr><td>128 / 128</td><td>128 / 128</td></tr></tbody></table>	2.4GHz	5GHz	128 / 128	128 / 128		
2.4GHz	5GHz						
128 / 128	128 / 128						
Wi-Fiの認証	WPA3 Enterprise						
暗号化方式	AES						
キー更新間隔	60 分						
Management Frame Protection	有効(Required)						
追加認証	追加認証を行わない						
RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する						

## SSID、WPA2-Enterprise の設定

### SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	Wi-Fiの認証	暗号化	
1	有効	XXXXX-WPA3 1		<input type="radio"/>	<input type="radio"/>	無効	WPA3 Enterprise AES		編集 削除
2	有効	XXXXX-WPA2 1		<input type="radio"/>	<input type="radio"/>	無効	WPA2 Personal AES		修正中

使用可能SSID	2.4GHz	5GHz
	14 / 16	14 / 16

Wi-Fi	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	XXXXXX-WPA2						
次の場合に有効にする	通常時と緊急時						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
ステアリング	無効						
優先制御	優先						
VLAN ID	<table border="1"><thead><tr><th>VLANモード</th><th>VLAN ID</th><th>追加VLAN ID</th></tr></thead><tbody><tr><td>Untagged Port</td><td>1</td><td></td></tr></tbody></table>	VLANモード	VLAN ID	追加VLAN ID	Untagged Port	1	
VLANモード	VLAN ID	追加VLAN ID					
Untagged Port	1						
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	使用しない						
ロードバランス (同時接続台数制限)	<table border="1"><thead><tr><th>2.4GHz</th><th>5GHz</th></tr></thead><tbody><tr><td>128 / 128</td><td>128 / 128</td></tr></tbody></table>	2.4GHz	5GHz	128 / 128	128 / 128		
2.4GHz	5GHz						
128 / 128	128 / 128						
Wi-Fiの認証	WPA2 Enterprise						
暗号化方式	AES						
キー更新間隔	60 分						
Management Frame Protection	無効						
Fast Transition (802.11r)	無効 Mobility Domain ID						
追加認証	追加認証を行わない						
RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する						

修正保存

編集を終了して前の画面へ戻る



WPA3 と WPA2 の SSID が作成されていることを確認する

## SSID設定 - SSIDの編集

### ステアリング ポリシー設定

ステアリング ポリシー

設定

### SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	Wi-Fiの認証	暗号化		
1	有効	XXXXX-WPA3	1	<input type="radio"/>	<input type="radio"/>	無効	WPA3 Enterprise AES		編集	削除
2	有効	XXXXX-WPA2	1	<input type="radio"/>	<input type="radio"/>	無効	WPA2 Enterprise AES		編集	削除

新規追加

- ② Wi-Fi AP の設定  
RADIUS サーバの設定

RADIUS設定	
<b>RADIUSサーバー</b>	
プライマリ-RADIUSサーバー	
サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	<input type="text"/>
認証ポート	<input type="text" value="1812"/>
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	<input type="text" value="1813"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
セカンダリ-RADIUSサーバー	
サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	<input type="text"/>
認証ポート	<input type="text" value="1812"/>
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	<input type="text" value="1813"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
Calling-Station-Id	""(区切りなし, 小文字) ▼
Called-Station-Id	""(区切りなし, 小文字) ▼
<input type="button" value="設定"/>	
<b>内蔵RADIUSサーバー</b>	
内蔵RADIUSサーバー	<input type="checkbox"/> 使用する
EAP内部認証	PEAP(MS-PEAP) ▼
EAP証明書ファイル形式	PKCS#12(*.pfx / *.p12)
EAP証明書ファイル	<input type="button" value="ファイルの選択"/> ファイルが選択されていません
EAP証明書ファイル・パスワード	<input type="text"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> 秒
Termination-Action	<input checked="" type="radio"/> 再認証を行う (RADIUS-Request) <input type="radio"/> 再認証を行わない(Default) <input type="radio"/> 送信しない
<input type="button" value="設定"/>	

### 2.4.3. 医療機器等の設定例

#### 1) 機器証明書のインポート

- i. PKCS#12形式の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

← 証明書インポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):

※ [Redacted File Name] 参照(R)...

注意: 次の形式を使うと1つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

次へ(N) キャンセル

- 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

×

← 証明書のインポートウィザード

秘密キーの保護  
セキュリティを維持するために、秘密キーはパスワードで保護されています。

---

秘密キーのパスワードを入力してください。

パスワード(P):

パスワードの表示(D)

インポートオプション(I):

秘密キーの保護を強力にする(E)  
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)  
キーのバックアップやトランスポートを可能にします。

仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)

すべての拡張プロパティを含める(A)

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



“次へ” ボタンを押すと、ルート証明書のインストールが始まる

## 2) 警告ダイアログの表示

- i. 「セキュリティ警告」ダイアログが表示されるが、「はい」をクリックし、「正しくインポートされました」と表示されれば完了



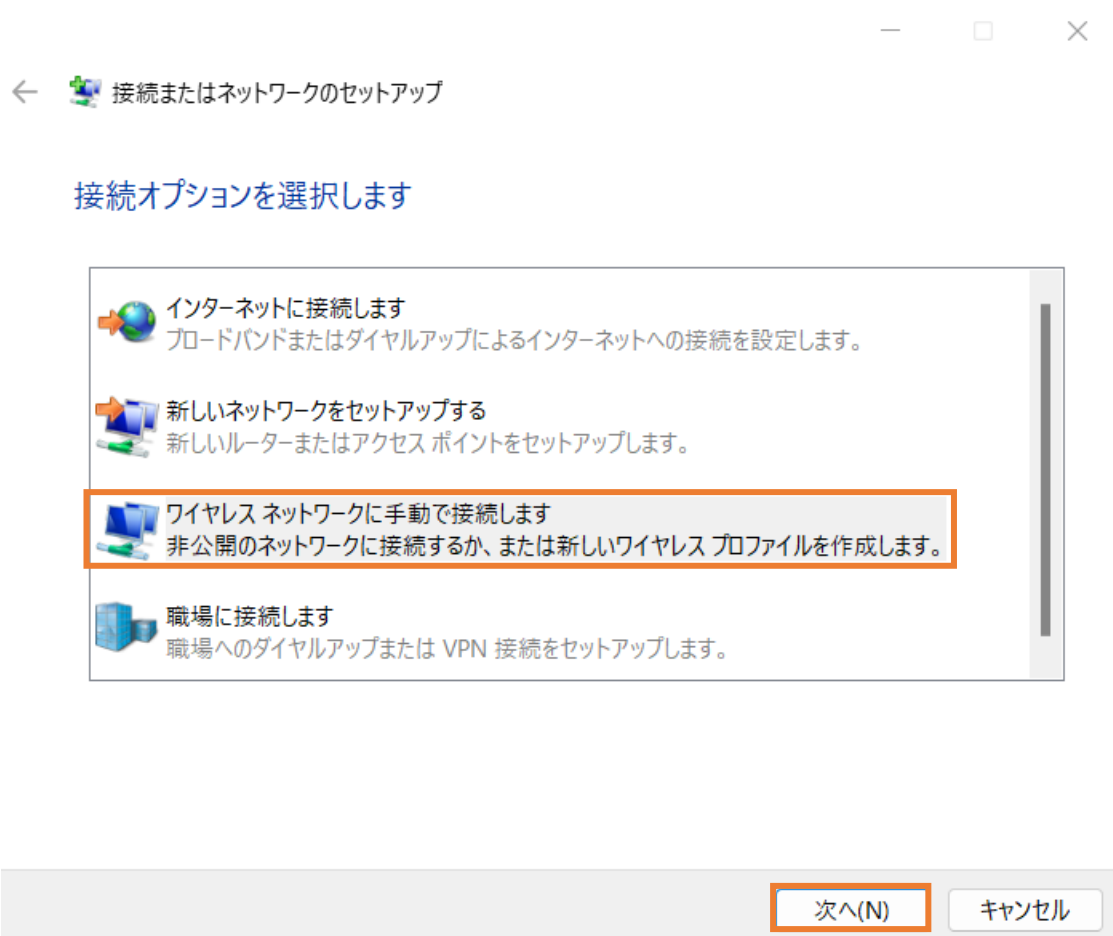
- ii. 「証明書のインポートウィザードの完了」が表示されたら完了





### 3) Wi-Fi の接続を設定する

「接続またはネットワークのセットアップ」で「ワイヤレスネットワークに手動で接続します」をクリック



#### 4) SSID 他の設定

##### WPA3-Enterprise の場合

「ネットワーク名」に SSID を入力、「セキュリティの種類」で” WPA3-エンタープライズ」を選択、「この接続を自動的に開始します」と「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」にチェックを入れる

← ワイヤレス ネットワークに手動で接続します

追加するワイヤレス ネットワークの情報を入力します

ネットワーク名(E): XXXXX-WPA3

セキュリティの種類(S): WPA3-エンタープライズ

暗号化の種類(R): AES

セキュリティキー(C):   文字を非表示にする(H)

この接続を自動的に開始します(T)

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(O)

警告: 選択すると、このコンピューターのプライバシーが危険にさらされる可能性があります。

次へ(N) キャンセル

## WPA2-Enterprise の場合

「ネットワーク名」に SSID を入力、「セキュリティの種類」で” WPA2-エンタープライズ」を選択、「この接続を自動的に開始します」と「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」にチェックを入れる



←  ワイヤレス ネットワークに手動で接続します

追加するワイヤレス ネットワークの情報を入力します

ネットワーク名(E):

セキュリティの種類(S):

暗号化の種類(R):

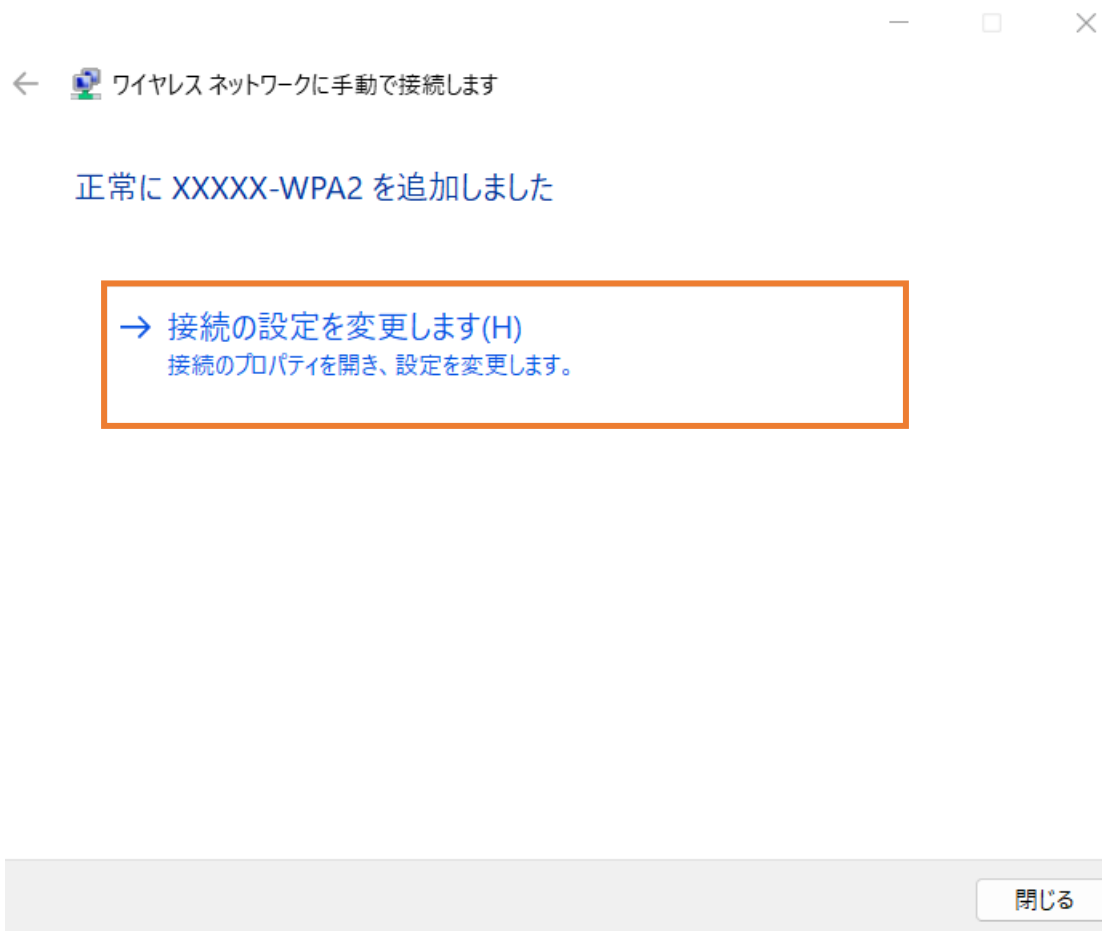
セキュリティキー(C):   文字を非表示にする(H)

この接続を自動的に開始します(T)

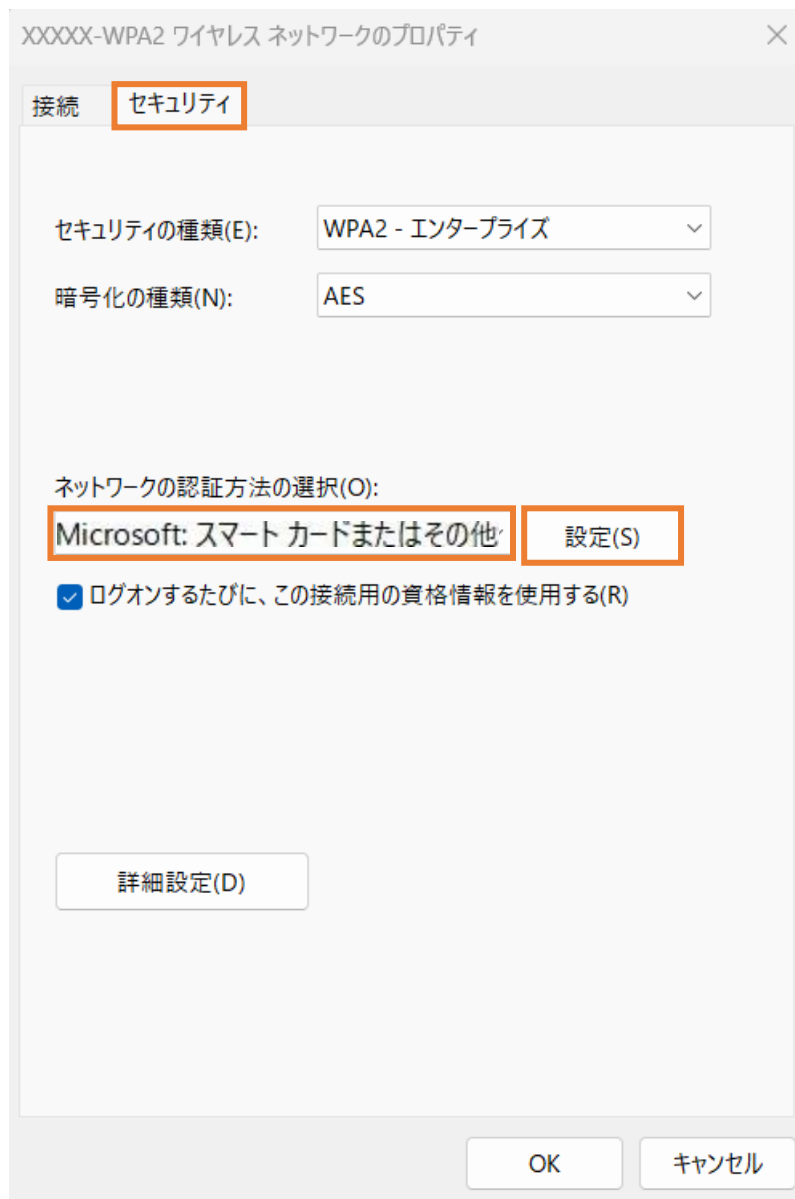
ネットワークがブロードキャストを行っていない場合でも接続する(O)

警告: 選択すると、このコンピューターのプライバシーが危険にさらされる可能性があります。

5) 「接続の設定を変更します」をクリック



6) “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



7) 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。“証明書を検証してサーバーの ID 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。“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

スマート カードまたはその他の証明書のプロパティ ✕

接続のための認証方法:

自分のスマートカードを使う(S) 詳細設定(A)

このコンピュータの証明書を使う(C)

単純な証明書の選択を使う (推奨)(M)

証明書を検証してサーバーの ID を検証する(V)

次のサーバーに接続する (例: srv1、srv2、.\*\$.srv3\$.com)(O):

信頼されたルート証明機関(R):

- AAA Certificate Services
- Baltimore CyberTrust Root
- Certum CA
- Certum Trusted Network CA
- Class 3 Public Primary Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3

証明書を表示する(E)

新しいサーバーまたは信頼された証明機関を承認するようユーザーに求めない(P)

この接続で別のユーザー名を使う(D)

8) 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



SSID を選択して接続を開始すると証明書を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

## 3. CA の運用例

### 3.1. 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。

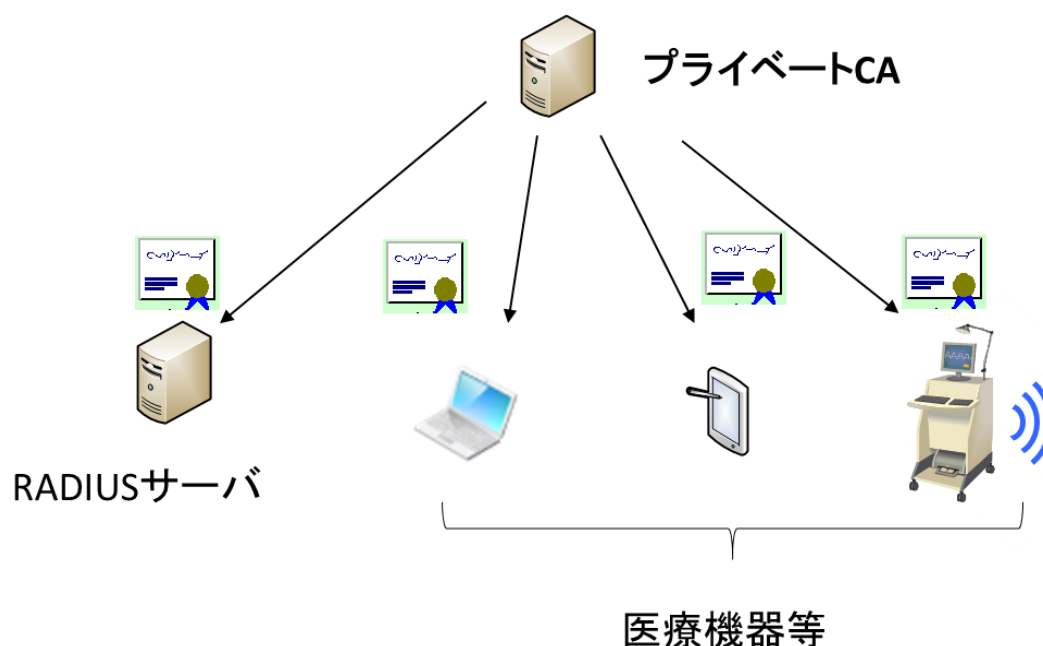


図 B.1 プライベート CA による証明書発行

### 3.2. 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。

### 3.3. 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。

### 3.4. 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。

## 4. 機器への組み込み例

### 4.1. 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。

### 4.2. 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。

### 4.3. 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、WPA3、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/ac/ax 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。

## 5. WPA2 及び WPA3 が混在する場合の運用例

Wi-Fi AP が WPA3 を実装する場合、あらかじめ WPA3 と WPA2 それぞれで SSID を作成し、Wi-Fi を用いて接続する医療機器等が実装している認証方式に合わせて接続させることが望ましい。

---

<sup>2</sup> Wi-Fi Alliance に関しては、<https://www.wi-fi.org/> を参照  
© JAHIS 2024

## 付録— 1. 参考文献

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

改定履歴		
日付	バージョン	内容
2024/01/12	Ver. 1.1	初版（ガイドより分離）

2024年4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 実装例

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)