



Japanese



Association of



Healthcare



Information



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

Systems Industry

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

ー般社団法人 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
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
2.2.2. Wi-Fi AP の設定例1
2.2.3. 医療機器等の設定例
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
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
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
3.1. 概要
3.2. プライベート CA の構築
3.3. RADIUS サーバ証明書の発行
 3.4. 医療機器等に対する機器認証用の証明書発行
4. 機器への組込み例
4.1 概要 39
4.2 PC 内蔵型 39
4.3. 組み込み型
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
□ 妳一Ⅰ· 罗勺ス\\\\\
付録-2. 作成者名簿

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)

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-FiAPの設定 SSID、WPA3-Personal(AES)の設定

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。
 © JAHIS 2024

Wi-Fi	● 有効 ○ 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	🗹 2.4GHz 🗹 5GHz
ステアリング	無効 ~
優先制御	優先 🗸
VLAN ID	VLANモード VLAN ID 追加VLAN I Untagged Port マ 1
ANY接続	✓ 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 5GHz 128 /128 128 /128
	MDA0 Dessent
¥1-+1の認証	WPA3 Personal V
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 V

追加認証

② Wi-FiAP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
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
検出されたサiー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-FiAPの設定

SSID、WPA3-Enterprise の設定

Wi-Fi	● 有効 ○ 毎効
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	🗹 2.4GHz 🗹 5GHz
ステアリング	無効 ~
優先制御	優先 ~
VLAN [D	VLANモード VLAN ID 追加VLAN ID [Untagged Portマ] 1
ANY接続	✓ 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 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 !	GHz ステアリング Wi-Fiの認証 暗号化				
1 有効 XXXX-\\PA31 〇	〇 無効 WPA3 Enterprise AES 編集 削除				
2 有効 XXXX-WPA21 〇	○ 無効 WPA2 Personal AES 修正中				
使用可能SSID	2. 4GHz 5GHz 14 /16 14 /16				
Wi-Fi	● 有効 ○ 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	✓ 2.4GHz ✓ 5GHz				
ステアリング	無効 ~				
優先制御	優先 ~				
VLAN ID	VLANモード VLAN ID 追加VLAN ID Untagged Port ~ 1				
ANY接続	☑ 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 5GHz 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				
DADTHS	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 無効 🔷

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		0	0	無効	WPA3 Enterprise AES	編集	削除
2	有効	XXXX-WPA2	1		0	0	無効	WPA2 Enterprise AES	編集	削除

新規追加

② Wi-FiAPの設定

RADIUS サーバの設定

RADIUS設定	RADIUS設定				
RADIUSサーバー					
プラ	イマリーRAD	DIUSサーバー			
サーバー	○内蔵 ●∮	外部			
サーバー名					
認証ポート	1812				
Accounting	🗹 使用する				
Accountingポート	1813				
Shared Secret					
Session-Timeout	3600	秒			
+2+	いがローPAF	LIII2 ++ 15			
サーバー	・ファウ Mill) ok ±R			
サーバー名					
認証ポート	1812				
Accounting	☑ 使用する				
Accountingポート	1813				
Shared Secret					
Session-Timeout	3600	秒			
Calling-Station-Id	""(区切りな)	し,小文字) 🗸			
Called-Station-Id	""(区切りな)	し,小文字)			
「設定」					
内蔵RADIUSサール	х —				
内蔵RADIUSサーバー		□ 使用する			
EAP内部認証		PEAP(MS-PEAP) V			
EAP証明書ファイル飛	鉽	PKCS#12(*.pfx / *.p12)			
EAP証明書ファイル		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・	バスワード				
Shared Secret					
Session-Timeout		3600 秒			
Termination-Action		 再認証を行う(RADIUS-Request) 再認証を行わない(Default) 送信しない 			
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

Х

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

0A	証明書	

全般 詳細 証明のパス								
◎ 証明書の情報								
この CA ルート証明書は信頼されていません。 信頼を有効にするにはこの証 明書を信頼されたルート証明機関のストアにインストールしてください。								
発行先:								
発行者:								
有効期間 2018/03/22 から 2023/03/22								
証明書のインストール(I) 発行者のステートメント(S)								
ОК								

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

☞ 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開始
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。
保存場所
○現在のユーザー(C)
○ ローカル コンピューター(L)
続行するには、【次へ】 をクリックしてください。
次へ(N) キャンセノ

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
÷	≫ 証明書のインポート ウィザード
	証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
	Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ● 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
	 ・ 証明書をすべて次のストアに配置する(P) 証明書ストア:
	参照(R)
	次へ(N) キャンセル

"完了"ボタンを押すと証明書がインポートされる

← 🛛 夢 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 内容	ウィザードで自動的に決定されます 証明書

完了(<u>F</u>)	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

_	\times	

← 💐 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 プ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。	
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■	
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

- 😰 🤈	イヤレスネットワークに手動で	き接続します			
追加	コするワイヤレス ネット	フ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	示(こする(H)	
ای eta	2 この接続を自動的に開始 2 ネットワークがブロードキャス :: 選択すると、このコンピュー?	します(T) トを行っていない場合でも接続する ターのプライバシーが危険にさらされる	(O) 可能性があります。		
			-		b. s. 1. 0

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

				—		\times
←	🔮 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	6(H)	
	☑□の接続を自動的に開始し	ます(T)				
	マ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	0		
			次へ(V)	キャンセ	μ

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	トワークのブロバティ		×
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過	選択(O):		
Microsoft: 保護された E/	AP (PEAP) 🛛 🗸	設定(S))
			_
🔽 ログオンするたびに、この)接続用の資格 <mark>情報を</mark>	使用する(R)	
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)	
■ 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)	
■ 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)	
■ 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)	
ビログオンするたびに、この 詳細設定(D))接続用の資格情報を	使用する(R)	
■ 「「「「」」「「」」「「」」「」」「」」「「」」「」」「「」」「」」「」」「」)接続用の資格情報を	使用する(R)	
■ D グオンするたびに、この 詳細設定(D))接続用の資格情報を	使用する(R)	
・ビログオンするたびに、この 詳細設定(D))接続用の資格情報を	使用する(R)	
■グオンするたびに、この 詳細設定(D)	D接続用の資格情報を	使用する(R)	

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 \times 接続のための認証方法: ○ 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 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): サーバーの ID を確認できない場合にユーザーに通知する \sim 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) □ サーバー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

EAP MSCHAPv2 のプロパティ	×
接続のための認証方法:	
Windows のログオン名と	とパスワード (およびドメインがあ
┗━━■◎場合は下X12)を自動	がいに(史つ(A)
ОК	キャンセル

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

詳細設定	\times
802.1Xの設定 802.11の設定	
☑認証モードを指定する(P):	
ユ−ザ−認証 ′ 資格情報の保存(C)	
□ すべてのユーザーの資格情報を削除する(D)	
このネットワークに対するシングル サインオンを有効にする(S)	
○ ユーザー ログオンの直前に実行する(E)	
○ ユーザー ログオンの直後に実行する(F)	
最大待5時間(秒)(M): 10 ▲	
 シングル サインオン中に追加のダイアログの表示を許可する (L) 	
 このネットワークでは、コンピューターとユーザーの認証に別の仮想 想 LAN を使用する(V) 	
OK キャンセノ	L

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-FiAPの設定

SSID、WPA3-Enterprise の設定

Wi-Fi	● 有劾 ○ 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	🗹 2.4GHz 🗹 5GHz
ステアリング	無効 ~
優先制御	優先 🗸
VLAN [D	VLANモード VLAN ID 追加VLAN ID Untagged Port マ 1
ANY接続	子 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 5GHz 128 /128 128
11 F: A 21 4	NIDAQ Entermine
第1-F102認証	VPA3 Enterprise V
暗号化方式	AES V
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

1 有効 X0XXX-WPA31 ● 無効 WPA3 Enterprise AES 福集 副除 2 有効 X0XXX-WPA21 ● 無効 WPA2 Personal AES 修正中 使用可能SSID 2.4GHz 5GHz 5GHz 6000000000000000000000000000000000000	Index 状態 SSID VLAN ID 2.4GHz 5GH;	z ステアリング Wi-Fiの認証 暗号化
2 有効 X00000-WPA21 ● 無効 WPA2 Personal AES 修正中 使用可能SSID 2.4GHz 5GHz 14 /16 14 /16 Wi-Fi ● 有効 ● 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 ② 2.4GHz ② 5GHz ステアリング 一方の ● 無効 ● 優先制御 優先 > VLAN ID Untagged Port > 1 ANY接続 ② 許可する ブ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 5GHz 128 YiLFiの認証 WPA2 Enterprise 年一更新間隔 60 Management Frame Protection 無効 >	1 有効 XXXX-WPA31 〇 〇	無効 WPA3 Enterprise AES 編集 削除
使用可能SSID 2.4GHz 5GHz 14 /16 14 /16 Wi-Fi ● 有効 ○ 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 ② 2.4GHz ② 5GHz ステアリング 無効 > 優先制御 一億先 > VLAN ID 10 Utanged Port > 1 ANY接続 ● 許可する ブライバシーセパレーター 使用しない > Pードバランス(同時接続台数制限) 2.4GHz 5GHz Wi-Fiの認証 WPA2 Enterprise Wi-Fiの認証 WPA2 Enterprise 年一更新間隔 60 外 Management Frame Protection 無効 > ●	2 有効 XXXX-WPA21 〇 〇	無効 WPA2 Personal AES 修正中
Wi-Fi ●有効 ●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 2 2.40Hz ≤ 50Hz ステアリング 無効 > 優先制御 優先 > VLAN ID ULAN TO UNtagged Port > 1 ANY接続 学 許可する ブライバシーセバレーター 使用しない > ロードバランス(同時接続台数制限) 2.40Hz 50Hz 128 VI-Fiの認証 WPA2 Enterprise 第号化方式 AES > キー更新間隔 60 グ 無効 >	使用可能SSID	2. 4GHz 5GHz 14 /16 14 /16
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 2.4GHz ステアリング 無効、 優先制御 優先、 VLAN ID ULAN ID Utagged Port、1 道加VLAN ID ANY接続 評可する 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 5GHz /128 Wi-Fiの認証 WPA2 Enterprise Wi-Fiの認証 WPA2 Enterprise キー更新間隔 60 分 Management Frame Protection 無効、 無効、	Wi-Fi	● 有効 ○ 無効
次の場合に有効にする 通常時と緊急時~ 使用デバイス 2.4GHz ステアリング 無効~ 優先制御 優先~ VLAN ID 追加VLAN ID ULANモード VLAN ID Untagged Port~ 1 ANY接続 ご 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 5GHz 128 Vi-Fiの認証 WPA2 Enterprise 第号化方式 AES~ キー更新間隔 60 分 無効 ~ Management Frame Protection 無効 ~	SSID	XXXXX-WPA2
使用デバイス 2.40Hz 5GHz ステアリング 無効 > 優先制御 優先 > VLAN ID 値加VLAN ID VLAN ID Untagged Port > 1 ANY接続 ゴ 許可する プライバシーセパレーター 使用しない レードバランス(同時接続台数制限) 2.4GHz 5GHz 128 Wi-Fiの認証 WPA2 Enterprise レー更新間隔 60 分 Management Frame Protection 無効 >	次の場合に有効にする	通常時と緊急時 🗸
ステアリング 無効 ~ 優先制御 優先 ~ VLAN ID VLAN TD Untagged Port ~ 1 ANY接続 ご許可する 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 5GHz 128 Wi-Fiの認証 WPA2 Enterprise 暗号化方式 AES ~ キー更新間隔 60 第効 ~ 無効 ~	使用デバイス	🗹 2.4GHz 🗹 5GHz
優先~ VLAN ID UNAN ID Untagged Port > 1 ANY接続 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 5GHz 128 /128 Wi-Fiの認証 WPA2 Enterprise 年一更新間隔 60 分 Management Frame Protection 無効 >	ステアリング	無効 ~
VLAN ID 追加VLAN ID 追加VLAN ID Untagged Port > 1 1 ANY接続 ご 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 5GHz 128 128 128 Wi-Fiの認証 WPA2 Enterprise 暗号化方式 AES > キー更新間隔 60 Management Frame Protection 無効 >	優先制御	優先 ∨
ANY接続 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 5GHz 128 /128 /128 /128 /128 /128 /128 /128	VLAN ID	VLANモード VLAN ID 追加VLAN ID Untagged Port ~ 1
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 5GHz 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	ANY接続	☑ 許可する
ロードバランス(同時接続台数制限) 2.4GHz 5GHz 128 /128 128 Wi-Fiの認証 WPA2 Enterprise ~ 暗号化方式 AES ~ キー更新間隔 60 Management Frame Protection 無効 無効	プライバシーセパレーター	使用しない
Wi-Fiの認証 WPA2 Enterprise 暗号化方式 AES キー更新間隔 60 Management Frame Protection 無効 無効	ロードバランス(同時接続台数制限)	2. 4GHz 5GHz 128 /128 128
暗号化方式 AES ~ キー更新間隔 60 Management Frame Protection 無効 ~ 無効 ~	Wi-Fiの認証	WPA2 Enterprise
キー更新間隔 60 分 Management Frame Protection 無効 、	暗号化方式	AES ~
Management Frame Protection 無効 < 無効	キー更新間隔	60 分
無効 >	Management Frame Protection	無効 ~
Fast Transition (802.11r) Mobility Domain ID	Fast Transition (802.11r)	無効~ Mobility Domain ID
追加認証を行わない	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 >	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

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 無効 ~

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		0	0	無効	WPA3 Enterprise	AES	編集	削除
2	有効	XXXX-WPA2	1		0	0	無効	WPA2 Enterprise	AES	編集	削除

新規追加

② Wi-FiAPの設定

RADIUS サーバの設定

RADIUS設定		
RADIUSサーバー		
プラ	・ イマリーRAE	DIUSサーバー
サーバー	○内蔵 ●タ	汁音 β
サーバー名		
認証ポート	1812	
Accounting	🗹 使用する	
Accountingポート	1813	
Shared Secret		
Session-Timeout	3600	秒
+7+	い。	DTU2++
サーバー)ノンツリーRAL 〇 内帯 ①	1105 ツーハー (A本R
サーバー名		
認証ポート	1812	
Accounting	■ 使用する	
Account ingポート	1813	
Shared Secret		
Session-Timeout	3600	
Calling-Station-Id	""(区切りな)	(/小文字) ✔
Called-Station-Id	""(区切りな)	し,小文字) ✓
設定		
内蔵RADIUSサーノ	х —	
内蔵RADIUSサーバー		□ 使用する
EAP内部認証		PEAP(MS-PEAP) V
EAP証明書ファイル刑	鉽	PKCS#12(*.pfx / *.p12)
EAP証明書ファイル		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・	バスワード	
Shared Secret		
Session-Timeout		3600 秒
Termination-Action		 再認証を行う(RADIUS-Request) 再認証を行わない(Default) 送信しない
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

証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
保存場所	
◎ 現在のユーザー(C)	
○ ローカル コンピューター(L)	
続行するには、 [次へ] をクリックしてください。	

ii. ファイル名を確認して "次へ" ボタンを押す

デーレオスな明ティーノル			
/ホード9 回転明書 ノアイル	(m) 7/+/+1.		
インホートするノアイルを描	にとしてくたさい。		
ファイル名(F):			
×			参照(R)
		10 m + 10 m + 4 + 4	
注意:次の形式を使うと	1つのノアイルに復数の証	労苦を保管(さます:	
Personal Information	on Exchange- PKCS #12	(.PFX,.P12)	
Cryptographic Mes	sage Syntax Standard-	PKCS #7 証明書 (.P7B)	
Microsoft シリアル化	とされた証明書ストア (.SST)	

- 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
 - ✓ ✓ ✓ ✓ 取得者のかめやのかが
 ✓ ✓ ✓ 取得者のかめやのかが
 ✓ むれるは物なから、必要キロがつかで保護されています。
 ✓ かっのたったものれていてきか。
 パロク・「やあっ」()
 パロク・「のまっ」()
 パロク・「のを思っ」()
 パロのであっ」()
 パロのであっ」()</li

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

証明書が保管されるシステム上の領域です。 習書ストアを自動的に選択させるか、証明書の場所を指定することができます。 種類に基づいて、自動的に証明書ストアを選択する(U) すべて次のストアに配置する(P) トア: 参照(R)
3音ストアを自動的に選択させるか、証明音の場所を指定することができます。 重頻に基づいて、自動的に証明音ストアを選択する(U) すべて次のストアに配置する(P) トア: 参照(R)
重類に基づいて、自動的に証明書ストアを選択する(U) すべて次のストアに配置する(P) トア: 参照(R)
すべて次のストアに配置する(P) トア: 参照(R)
トア: 参照(R)
参照(R)

"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

セキュリテ	/ 晉告 ×
Δ	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:
	証明書が実際に "TEST V5 CA" からのものであるかどうかを検証できません。"TEST V5 CA" に連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます:
	揖印 (sha1); CFF90AF0 DFD22FD4 C4E1C8F3 DFAD0D60 4488CE24
	答告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない拇印付きの証明書をインストール することは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認 険したことになります。
	この証明書をインストールしますか?
	HUAD LUNGAR

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

← 🐉	証明書のインポートウィザー	ž.		>
	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	こ ウノザードで自動的に決定されます		
	内容	PFX		
	ファイル名	C:¥Users		
	-			
			完了(F)	キャンセル

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

- 🗆 🗙

← 💐 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。	- 1
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。	
「「「「「「」」「「」」「「」」「「」」「「」」「「」」「「」」「「」」「「	- 1
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

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

追加するフィアレス不少	トリークの消報を入力します	
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)	
マネットワークがブロードキ	ヤストを行っていない場合でも接続する	
音古: 選択 9 つと、このコノヒ.	1-ダーのノフ1ハンーか厄映にさらされる	2月能性があります。

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

4	🔊 ワイヤレス ネットワークに毛動で	亲続 .ます		_		\times
	追加9 る)1 (レス イット)	- 2011 南報を入力しま9				
	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	表示にする	5(H)	
	■この接続を自動的に開始しま	ます(T)				
	✓ ネットワークがブロードキャスト 警告・選択すると、このコンピュータ-	を行っていない場合でも接続する(O) -のプライバシーがた険にさらされる可	能性があります			
		WYYTTY INERCOULD'S	881273 00 7 8 9	0		
			次へ(N)	キャンセ	ᆀ

5)「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

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

XXXXX-WPA2 ワイヤレス ネッ	トワークのプロパティ		\times
接続 セキュリティ			
セキュリティの種類(F):	WPA2 - エンタープライ	ば	~
	450		
増亏12の種類(N):	AES		~
ネットワークの認証方法の運	【択(O):		_
Microsoft: スマート カ	ードまたはその他	設定(S)	
🚽 ログオンするたびに、この	接続用の資格情報を	吏用する(R)	
詳細設定(D)			

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

○ 白公のフマート カードを使う(S)	
 ロカの人(ートカートを使う(C) ロカンピューターの証明書を使う(C) 	詳細設定(A)
●「単純な証明者の違抗を使う(推奨)(M)	
□ 証明書を検証してサーバーの ID を検証する(V)	
	-2XX(O)-
次のサーハーに接続する(例: srv1、srv2、, *+,srv	/3#.com)(O):
13 現されたルート証明機関(K):	
AAA Certificate Services Raltimore CuberTruct Root	<u>^</u>
Class 3 Public Primary Certification Author	itu
	ny .
DigiCert Global Boot CA	
DigiCert Global Root G2	
	Ŷ
<	>
	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	とするようユーザーに求めない(P)
THICK I MICHAEL THERE THE PLACE	
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

「詳細設定」	\times			
802.1Xの設定 802.11の設定				
✓ 認証モードを指定する(P):				
コンピュータ認証 ~ 資格情報の保存(C)				
□ すべてのユーザーの資格情報を削除する(D)				
□ このネットワークに対するシングル サインオンを有効にする(S)				
○ ユーザー ログオンの直前に実行する(E)				
○ ユーザー ログオンの直後に実行する(F)				
最大待ち時間 (秒)(M): 10				
シングル サインオン中に追加のダイアログの表示を許可する (L)				
 このネットワークでは、コンピューターとユーザーの認証に別の仮想 想 LAN を使用する(V) 				
OK キャンセル	L			

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

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。



医療機器等

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。

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

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。

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。

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

© JAHIS 2024

めにディスプレイ等の表示機能とキーボート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²。 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 を実現するサプリカント、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。

² 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㈱
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)