



Account@Adapter+ V7 認証設定例（KOKOMOクラウド）

HCNET エイチ・シー・ネットワークス株式会社

（2026/5/7 作成）

- ▶ 本資料では、エイチ・シー・ネットワークス株式会社(以下HCNET社)製RADIUS認証アプライアンス Account@Adapter+ V7のRADIUS/CA機能と、APRESIA Systems 株式会社(以下APRESIA社)が提供するKOKOMOクラウドを組み合わせ、以下のRADIUS認証を実施する方法について説明します。
 - ▶ Web認証
 - ▶ MACアドレス認証
 - ▶ 内部DBを利用したIEEE802.1X PEAP認証
 - ▶ 外部ADを利用したIEEE802.1X PEAP認証
 - ▶ IEEE802.1X EAP-TLS認証
 - ▶ 属性応答
- ▶ 設定例ではAPRESIA社製スイッチおよびアクセスポイント、Active Directoryサーバーの基本設定が完了していることを前提とし、Web認証、MACアドレス認証、IEEE802.1X PEAP認証およびEAP-TLS認証、属性応答に必要な設定のみを説明します。
- ▶ 本資料は、Account@Adapter+ V7 Ver.7.03.00の仕様に従って記述したものになります。
使用している画面等は、環境により表示される内容に若干の差異が発生する場合がありますのでご注意ください。
- ▶ 本資料は、HCNET社での検証に基づき、HCNET社製RADIUS認証アプライアンス Account@Adapter+ V7 およびAPRESIA社製KOKOMOクラウドの操作方法を記載したものです。
すべての環境での動作を保証するものではありませんのでご注意ください。

1. 設定例および動作確認環境

- 1-1.対象OS・認証方式一覧
- 1-2.使用機器
- 1-3.ネットワーク設定
- 1-4.構成図

2. KOKOMOクラウドの設定

- 2-1.KOKOMOクラウドへのアクセス
- 2-2.SSID設定
 - 2-2-1.SSIDの設定
 - 2-2-2.Web認証用 SSIDの設定
 - 2-2-3.MAC認証用 SSIDの設定
 - 2-2-4.EAP-PEAP認証用(内部DB) SSIDの設定
 - 2-2-5.EAP-PEAP認証用(外部AD) SSIDの設定
 - 2-2-6. EAP-TLS認証用 SSIDの設定(WPA2エンタープライズ/WPA3エンタープライズ)
 - 2-2-7.EAP-TLS認証用 SSIDの設定(WPA3-Enterprise 192bit mode)
 - 2-2-8.属性応答用 SSIDの設定

3. Account@Adapter+ V7 設定

- 3-1.管理画面へのアクセス
- 3-2.ネットワーク設定
- 3-3.CA設定
 - 3-3-1.CA設定
 - 3-3-2.内部サーバー証明書設定
 - 3-3-3.クライアント証明書ポリシー
- 3-4.RADIUS設定
 - 3-4-1.RADIUS設定
 - 3-4-2.RADIUSクライアント登録
 - 3-4-3.ネットワークプロファイルの設定
- 3-5. アカウント登録
 - 3-5-1. サブディレクトリ作成
 - 3-5-2. 端末共通パスワード設定
 - 3-5-3. Web認証・EAP-PEAP認証用 ユーザーアカウント登録
 - 3-5-4. MAC認証用 端末(MAC)アカウント登録
 - 3-5-5. EAP-TLS認証用 証明書アカウント登録
 - 3-5-6. EAP-TLS認証用 証明書発行
- 3-6. 外部LDAP/AD登録
 - 3-6-1. 外部AD登録

4. 検証

4-1. Web認証

4-2. MAC認証

4-3. EAP-PEAP認証(内部DB)

4-3-1. EAP-PEAP認証における事前準備

4-3-2. WindowsにおけるEAP-PEAP認証(内部DB)の実施

4-3-3. MacOSにおけるEAP-PEAP認証(内部DB)の実施

4-3-4. iOSにおけるEAP-PEAP認証(内部DB)の実施

4-3-5. AndroidにおけるEAP-PEAP認証(内部DB)の実施

4-4. EAP-PEAP認証(外部AD)

4-4-1. WindowsにおけるEAP-PEAP認証(外部AD)の実施

4-4-2. MacOSにおけるEAP-PEAP認証(外部AD)の実施

4-4-3. iOSにおけるEAP-PEAP認証(外部AD)の実施

4-4-4. AndroidにおけるEAP-PEAP認証(外部AD)の実施

4-5. EAP-TLS認証

4-5-1. EAP-TLS認証における事前準備

4-5-2. WindowsにおけるEAP-TLS認証の実施

4-5-3. MacOSにおけるEAP-TLS認証の実施

4-5-4. iOSにおけるEAP-TLS認証の実施

4-5-5. AndroidにおけるEAP-TLS認証の実施

4-6. 属性応答

4-6-1. 属性応答検証の実施

4-6-2. 認証後の確認(Account@Adapter+ V7)

4-6-3. 認証後の確認(KOKOMOクラウド)

【補足】認証成功ログ/検証結果

1. 設定例および動作確認環境

- 1-1. 対象OS・認証方式一覧
- 1-2. 使用機器
- 1-3. ネットワーク設定
- 1-4. 構成図



 Adapter

- ▶ HCNET社製RADIUS認証アプライアンス Account@Adapter+ V7 の RADIUS/CA機能 と、APRESIA社が提供する KOKOMOクラウドを組み合わせ、下記OS環境において Web認証、MACアドレス認証、IEEE 802.1X(PEAP)認証、EAP-TLS認証 の動作確認を実施しました。その結果を以下に示します。

検証認証方式	Web認証	MACアドレス認証	IEEE802.1X PEAP認証	IEEE802.1X EAP-TLS認証
Windows 11 pro	○	○	○	○
MacOS Sequoia15	○	○	○	○
iOS 26	○	○	○	○
Android 16	○	○	○	○

製品名	メーカー	役割	バージョン
Account@Adapter+ V7	HCNET	RADIUS/CAサーバー	Ver.7.03.00
KOKOMOクラウド	APRESIA	クラウド管理基盤	-
KOKOMO-S212GT-P	APRESIA	L2スイッチ	Ver.1.2.110
KOKOMO-W222BE-IS	APRESIA	無線AP(RADIUSクライアント)	Ver.1.8.102
Dell Pro 16	DELL	無線端末	Windows 11 pro
MacBook Air	Apple	無線端末	MacOS Sequoia15
iPhone (第11世代)	Apple	無線端末	iOS 26
Google Pixel(第6世代)	Google	無線端末	Android 16

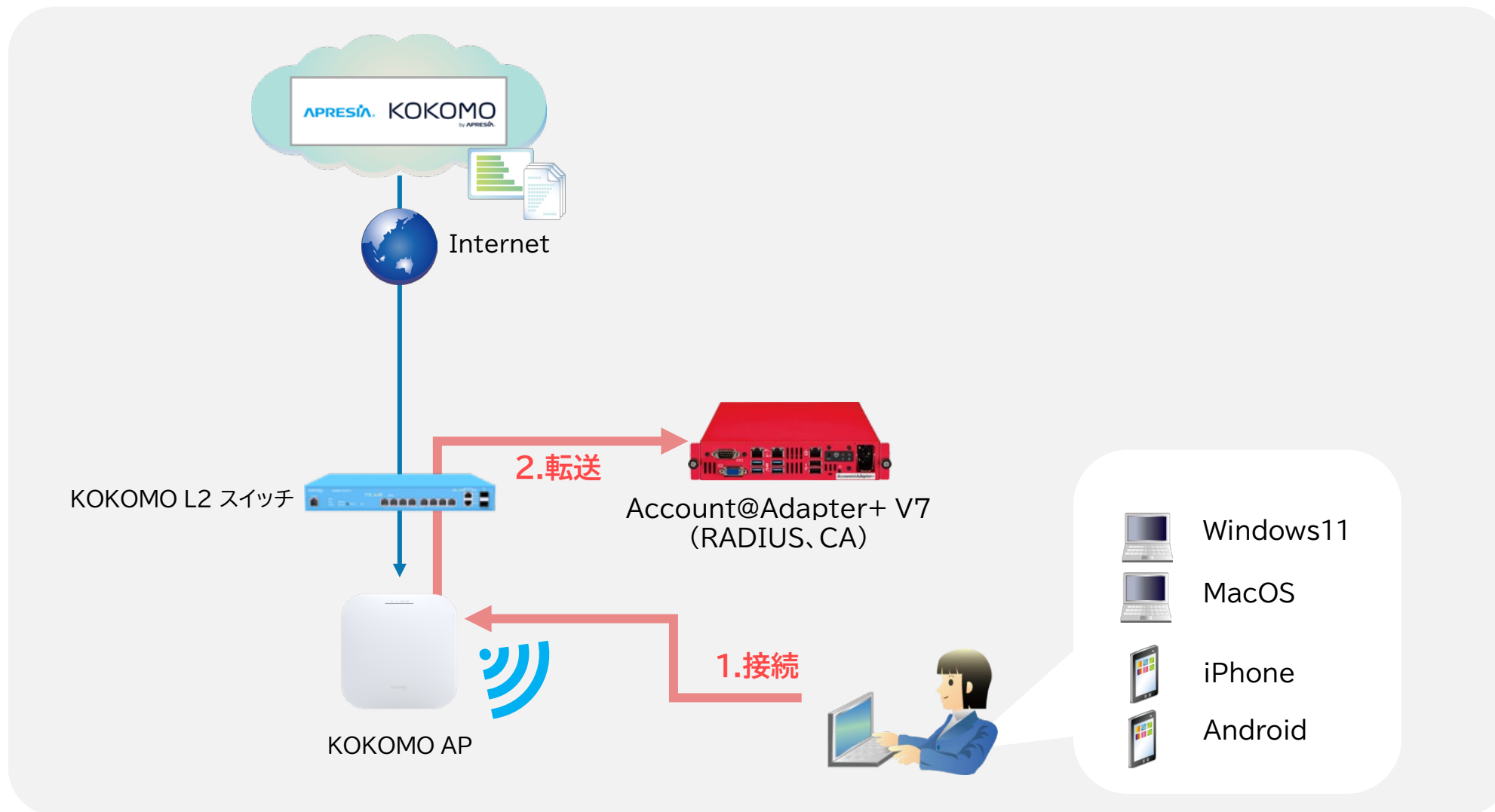
※動作検証を行った時点の製品やOSのバージョンを記載しています。

※製品やOSを実際にご利用いただく際には脆弱性などの問題が対策されたバージョンを選定いただくようにしてください。

1-3.ネットワーク設定

製品名	IPアドレス	RADIUSポート	シークレットキー
Account@Adapter+ V7	192.168.102.3	1812	kokomo
KOKOMO-S212GT-P	192.168.102.4	1812	kokomo
KOKOMO-W222BE-IS	192.168.102.5	1812	kokomo
Dell Pro 16	DHCP	-	-
MacBook Air	DHCP	-	-
iPhone (第11世代)	DHCP	-	-
Google Pixel(第6世代)	DHCP	-	-

1-4.構成図



2.KOKOMOクラウドの設定

実施する設定は次の通りです。

2-1.KOKOMOクラウドへのアクセス

2-2.SSID設定



2-1.KOKOMOクラウドへのアクセス

- ▶ KOKOMO機器の設定を行うため、KOKOMOクラウドにアクセスします
 - ▶ Microsoft Edgeを起動し、下記URLにアクセスします
 - ▶ <https://lan.kokomocloud.com/login>
- ▶ メールとパスワードを入力し、KOKOMOクラウドにログインします

アカウントをお持ちでない場合 [登録](#)

KOKOMO Cloudにサインインする

メール

パスワード [パスワードを忘れた場合](#)

[ログイン](#)

または

[G Google](#)

[利用規約](#) [プライバシーポリシー](#)

▶ 2-2-1.SSIDの設定①

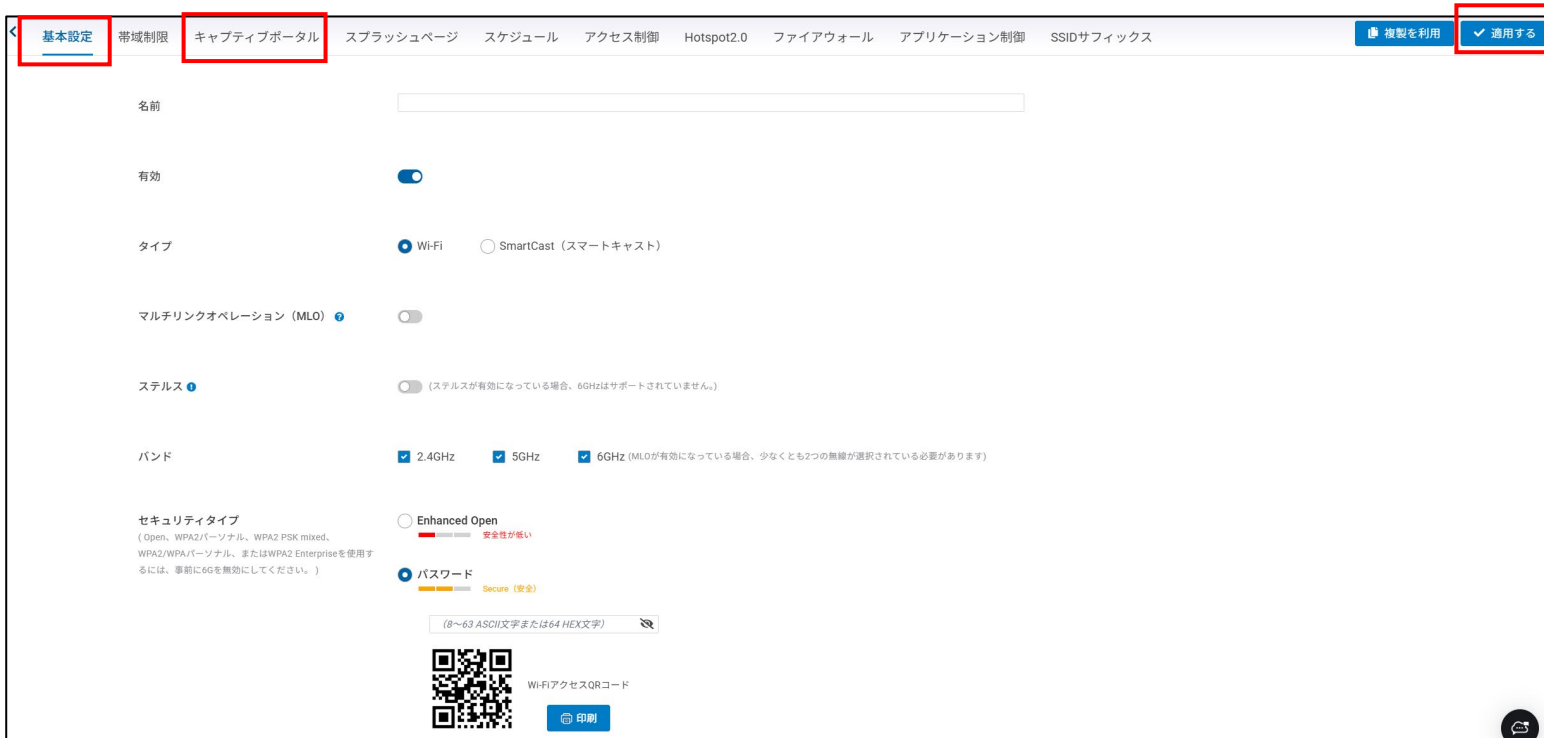
▶ 設定[アクセスポイント]-[SSID]に遷移します



▶ 画面右上の[SSIDの追加] をクリックします

1-7/7 削除 + SSIDの追加 緊急Wi-Fiを有効にする								
☐	SSID	バンド	有効	ステルス	セキュリティ	キャプティブポータル	スプラッシュページ	帯域制限
☐	A@A_PEAP_Internal	2.4G 5G	はい	いいえ	WPA3エンタープライズ	なし	ローカル	無効
☐	A@A_MAC	2.4G 5G	はい	いいえ	WPA3パーソナル	カスタムRADIUS	ローカル	無効
☐	A@A_PEAP_AD	2.4G 5G	はい	いいえ	WPA3エンタープライズ	なし	ローカル	無効
☐	A@A_TLS	2.4G 5G	はい	いいえ	WPA3エンタープライズ	なし	ローカル	無効
☐	A@A_Web	2.4G 5G	はい	いいえ	WPA2パーソナル	カスタムRADIUS	ローカル	無効
☐	A@A_DVLAN	2.4G 5G	はい	いいえ	WPA2エンタープライズ	なし	ローカル	無効
☐	A@A_DVLAN_Web	5G	はい	いいえ	WPA2パーソナル	カスタムRADIUS	ローカル	無効

- ▶ 2-2-1.SSIDの設定②
 - ▶ [基本設定]タブ内を入力し、画面右上の[適用する]をクリックします
 - ▶ Web認証用/MAC認証用/EAP-PEAP認証用(内部DB)/EAP-PEAP認証用(外部AD)/EAP-TLS認証用/属性応答用に分けてSSIDを作成します
 - ▶ Web認証用/MAC認証用については[基本設定]タブおよび[キャプティブポータル]タブ内も入力します



▶ 2-2-2.Web認証用 SSIDの設定

- ▶ SSID「 A@A_Web」を作成します
- ▶ セキュリティタイプはWPA2パーソナルで認証しております

■ Web認証用 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	パスワード
③パスワード	(任意パスワード)
④WPAタイプ	WPA2パーソナル

■ Web認証用 キャプティブポータル設定

設定項目	設定値
⑤有効	有効オン(トグル右)
⑥認証タイプ	カスタムRADIUS
⑦サーバー1 IPアドレス	192.168.102.3
⑧サーバー1 Secret	kokomo




2-2.SSID設定

- ▶ 2-2-3.MAC認証用 SSIDの設定
 - ▶ SSID「A@A_MAC」を作成します
 - ▶ セキュリティタイプはWPA3パーソナルで認証しております

■ MAC認証用 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	パスワード
③パスワード	(任意パスワード)
④WPAタイプ	WPA3パーソナル

■ MAC認証用 キャプティブポータル設定

設定項目	設定値
⑤有効	有効オン(トグル右)
⑥認証タイプ	カスタムRADIUS
⑦サーバー1 IPアドレス	192.168.102.3
⑧サーバー1 Secret	kokomo
⑨RADIUS MAC-Auth	有効オン(トグル右)

The screenshot shows the SSID configuration page with the following settings and annotations:

- 名前:** A@A_MAC
- 有効:** ☒
- タイプ:** ☒ Wi-Fi ☐ SmartCast (スマートキャスト)
- マルチリンクオペレーション (MLO):** ☐
- ステルス:** ☐ (ステルスが無効になっている場合、6GHzはサポートされていません)
- バンド:** ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが無効になっている場合、少なくとも2つの無線が選択されている必要があります)
- セキュリティタイプ:**
 - ☐ Open
 - ☐ Enhanced Open
 - ☒ パスワード
- パスワード:** [Redacted]
- QRコード:** [QR Code]
- Wi-Fiアクセスコード:** [Redacted]
- WPAタイプ:** WPA3パーソナル
- 有効:** ☒
- 認証タイプ:**
 - ☐ クリックスルー
 - ☐ KOKOMO Cloud RADIUS
 - ☒ カスタムRADIUS
- カスタムRADIUS認証タイプ:** CHAP
- サーバー1:** IPアドレス: 192.168.102.3, ポート: 1812, Secret: kokomo
- サーバー2:** [Redacted]
- サーバー3:** [Redacted]
- Accounting負荷分散:** ☒ PRO AP
- CoA (認証情報更新):** ☐
- RADIUSによる帯域幅制限:** ☐
- RADIUS MAC-Auth:** ☒

- ▶ 2-2-4.EAP-PEAP認証用(内部DB) SSIDの設定
 - ▶ SSID「A@A_PEAP_Internal」を作成します
 - ▶ セキュリティタイプはWPA2エンタープライズ/WPA3エンタープライズで認証を実施しております
 - ▶ 各自セキュリティタイプを変更して認証を実施しております。その他の設定値は共通となります

名前: A@A_PEAP_Internal

有効: ☒

タイプ: ☒ Wi-Fi ☐ SmartCast (スマートキャスト)

マルチリンクオペレーション (MLO): ☐

ステルス: ☐ (ステルスが有効になっている場合、6GHzはサポートされていません)

バンド: ① ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが有効になっている場合、少なくとも2つの無線が選択されている必要があります)

セキュリティタイプ: ☐ Open (安全性が低い) ☐ Enhanced Open (安全性が低い) ☐ パスワード (Secure (安全)) ☐ WPA2エンタープライズ (より安全) ② ☒ WPA3エンタープライズ (より安全) (2.4G 5G 6G)

認証方法: ③ カスタムRADIUS

SuiteB 192ビット: ☐

	IPアドレス	ポート	Secret	RadSec
④⑤ サーバー1	192.168.102.3	1812		☐
サーバー2				☐

■ EAP-PEAP認証用(内部DB) 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	WPA2エンタープライズ /WPA3エンタープライズ
③認証方法	カスタムRADIUS
④サーバー1 IPアドレス	192.168.102.3
⑤サーバー1 Secret	kokomo

- ▶ 2-2-5.EAP-PEAP認証用(外部AD) SSIDの設定
 - ▶ SSID「A@A_PEAP_AD」を作成します
 - ▶ セキュリティタイプはWPA3エンタープライズで認証を実施しております

名前: A@A_PEAP_AD

有効: ☒

タイプ: ☒ Wi-Fi ☐ SmartCast (スマートキャスト)

マルチリンクオペレーション (MLO) ☐

ステルス ☐ (ステルスが有効になっている場合、6GHzはサポートされていません)

バンド: ① ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが有効になっている場合、少なくとも2つの無線が選択されている必要があります)

セキュリティタイプ: ☐ Open (安全性が低い) ☐ Enhanced Open (安全性が低い) ☐ パスワード (Secure (安全)) ☐ WPA2エンタープライズ (より安全) ② ☒ WPA3エンタープライズ (2.4G 5G 6G) (より安全)

③ 認証方法: カスタムRADIUS

SuiteB 192ビット ☐

④ ⑤

	IPアドレス	ポート	Secret	RadSec
サーバー1	192.168.102.3	1812		☐ テスト
サーバー2				☐ テスト

■ EAP-PEAP認証用(外部AD) 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	WPA3エンタープライズ
③認証方法	カスタムRADIUS
④サーバー1 IPアドレス	192.168.102.3
⑤サーバー1 Secret	kokomo

- ▶ 2-2-6.EAP-TLS認証用 SSIDの設定(WPA2エンタープライズ/WPA3エンタープライズ)
 - ▶ SSID「A@A_TLS」を作成します
 - ▶ セキュリティタイプはWPA2エンタープライズ/WPA3エンタープライズ/ WPA3-Enterprise 192bit modeで認証を実施しております
 - ▶ 各自セキュリティタイプを変更して認証を実施しております。その他の設定値は共通となります
 - ▶ WPA3-Enterprise 192bit modeでの認証については別途設定が必要となります。次項に記載しております

名前: A@A_TLS

有効: ☒

タイプ: ☒ Wi-Fi ☐ SmartCast (スマートキャスト)

マルチリンクオペレーション (MLO): ☐

ステルス: ☐ (ステルスが有効になっている場合、6GHzはサポートされていません)

バンド: ① ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが有効になっている場合、少なくとも2つの無線が選択されている必要があります)

セキュリティタイプ: ☐ Open (安全性が低い) ☐ Enhanced Open (安全性が低い) ☐ パスワード (Secure (安全)) ☐ WPA2エンタープライズ (より安全) ② ☒ WPA3エンタープライズ (より安全)

認証方法: ③ カスタムRADIUS

SuiteB 192ビット: ☐

IPアドレス: ④⑤ 192.168.102.3 ポート: 1812 Secret: RadSec: ☒

サーバー1: 192.168.102.3 1812 テスト

■ EAP-TLS認証用 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	WPA2エンタープライズ /WPA3エンタープライズ
③認証方法	カスタムRADIUS
④サーバー1 IPアドレス	192.168.102.3
⑤サーバー1 Secret	kokomo

- ▶ 2-2-7.EAP-TLS認証用 SSIDの設定(WPA3-Enterprise 192bit mode)
- ▶ KOKOMOクラウド側での設定は以下のみとなりますが、Account@Adapter+ V7側での設定が別途必要となります
- ▶ 詳細は24～26スライドをご参照ください

名前: A@A_TLS

有効: ☒

タイプ: ☒ Wi-Fi ☐ SmartCast (スマートキャスト)

マルチリンクオペレーション (MLO) ☐

ステルス ☐ (ステルスが有効になっている場合、6GHzはサポートされていません)

バンド: ① ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが有効になっている場合、少なくとも2つの無線が選択されている必要があります)

セキュリティタイプ: ☐ Open (安全性が低い) ☐ Enhanced Open (安全性が低い) ☐ パスワード (Secure (安全)) ☐ WPA2エンタープライズ (より安全) ② ☒ WPA3エンタープライズ (2.4G 5G 6G) (より安全)

③ 認証方法: カスタムRADIUS

④ SuiteB 192ビット: ☒

⑤ ⑥ サーバー1: IPアドレス: 192.168.102.3 ポート: 1812 Secret: *****

■ EAP-TLS認証用 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	WPA3エンタープライズ
③認証方法	カスタムRADIUS
④SuiteB 192ビット	有効(トグル右)
⑤サーバー1 IPアドレス	192.168.102.3
⑥サーバー1 Secret	kokomo

- ▶ 2-2-8.属性応答用 SSIDの設定
- ▶ SSID「A@A_DVLAN」を作成します
 - ▶ セキュリティタイプはWPA2エンタープライズで認証を実施しております
 - ▶ KOKOMOクラウド側での設定は以下のみとなりますが、Account@Adapter+ V7側での設定が別途必要となります
 - ▶ 詳細はスライド28～29をご参照ください

名前: A@A_DVLAN

有効: ☒

タイプ: ☒ Wi-Fi ☐ SmartCast (スマートキャスト)

マルチリンクオペレーション (MLO): ☐

ステルス: ☐ (ステルスが有効になっている場合、6GHzはサポートされていません)

バンド: ☒ 2.4GHz ☒ 5GHz ☐ 6GHz (MLOが有効になっている場合、少なくとも2つの無線が選択されている必要があります)

セキュリティタイプ: ☐ Open ☐ Enhanced Open ☒ WPA2エンタープライズ

認証方法: カスタムRADIUS

④⑤

サーバー1: IPアドレス 192.168.102.3, ポート 1812, Secret *****

サーバー2: (空欄)

☐ NAS ID

☐ NAS IP: 0.0.0.0

☐ NASポート: 20

⑥ ☒ RADIUSによるVLAN

■ 属性応答用 基本設定

設定項目	設定値
①バンド	2.4GHz 5GHz
②セキュリティタイプ	WPA2エンタープライズ
③認証方法	カスタムRADIUS
④サーバー1 IPアドレス	192.168.102.3
⑤サーバー1 Secret	kokomo
⑥RADIUSによるVLAN	チェック有

3.Account@Adapter+ V7 設定

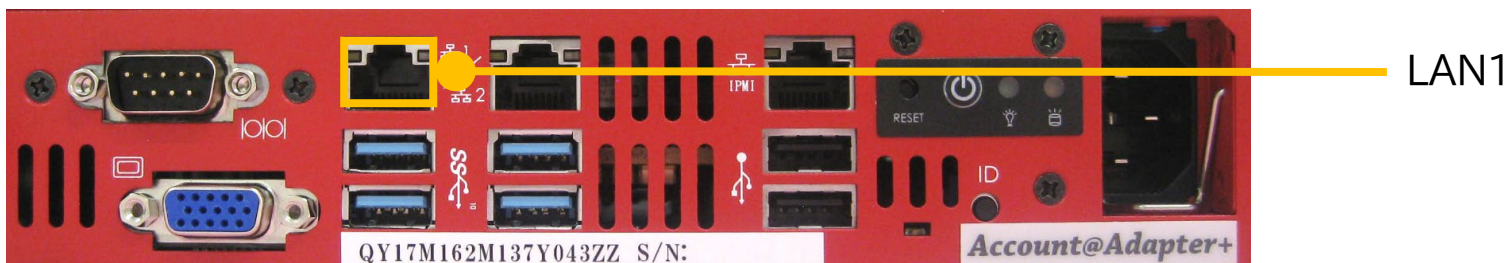
実施する設定は次の通りです。

- 3-1.管理画面へのアクセス
- 3-2.ネットワーク設定
- 3-3.CA設定
- 3-4.RADIUS設定
- 3-5.アカウント登録
- 3-6.外部LDAP/AD登録



3-1. 管理画面へのアクセス

- ▶ Account@Adapter+ V7の設定を行うため、管理画面にアクセスします
 - ▶ Account@Adapter+ V7の初期IPアドレスは「192.168.0.1/24」となります
設定を行う際は、クライアント端末のIPアドレスを同じセグメントに設定の上実施願います
 - ▶ クライアント端末とAccount@Adapter+ V7のLAN1(左側)をLANケーブルで直接接続します



- ▶ Microsoft Edgeを起動し、下記URLにアクセスします
 - ▶ <http://192.168.0.1:8080/manager/>
- ▶ 管理者IDとパスワードを入力し、管理画面にログインします
 - ▶ ログインID: naadmin
 - ▶ パスワード: naadmin

The screenshot shows the login interface for the Account@Adapter+ V7 maintenance tool. The title is 'Account@Adapter+ Ver. 7.03.00' with the subtitle 'メンテナンスツール'. There are two input fields: 'ログインID' (Login ID) and 'パスワード' (Password), both highlighted with a red border. Below the fields is a 'ログイン' (Login) button.

- ▶ 管理ツール [環境設定]－[ネットワーク設定]－《メンテナンスメニュー》に遷移します

ネットワーク設定

ネットワーク設定

eth0

IPアドレス※ ① 192.168.102.3
(XXX.XXX.XXX.XXX)

ネットマスク※ ② 255.255.255.0
(XXX.XXX.XXX.XXX)

eth1

IPアドレス
(XXX.XXX.XXX.XXX)

ネットマスク
(XXX.XXX.XXX.XXX)

デフォルトゲートウェイ※ ③ 192.168.102.1
(XXX.XXX.XXX.XXX)

DNS設定

DNSサーバー ④ 192.168.4.3
(XXX.XXX.XXX.XXX)
(1行1IPアドレス 最大3行)

【入力例】
192.168.1.1
192.168.1.2
192.168.1.3

タイムアウト
(0～30) 秒

■ ネットワーク設定

設定項目	設定値
①IPアドレス	192.168.102.3
②ネットマスク	255.255.255.0
③デフォルトゲートウェイ	192.168.102.1
④DNSサーバー	192.168.4.3

Active Directoryアカウントで認証を行うには、Account@Adapter+ V7がドメインに参加し、対象ドメインのLDAPサービスのSRVレコードを取得できるようDNSが適切に設定されている必要があります。

- ▶ 設定後、画面下部の[登録]をクリックします

▶ 3-3-1.CA設定

- ▶ 管理ツール [CA]－[CA設定]を開き、CAの[設定]をクリックします

CA設定

入力規則

認証局 ① ☒ 自己認証局 ☐ 下位認証局

自己認証局情報設定

名前(cn)※ ②
(半角英数記号 64文字以内)

国(c) ③

都道府県(st)※ ④
(半角英数記号 128文字以内)

市区町村(L)
(半角英数記号 128文字以内)

組織名(o)
(半角英数記号 57文字以内)

部署(ou)
(半角英数記号 64文字以内)

メールアドレス(E-mail)
(半角英数記号 128文字以内)

有効期限

フレンドリー名
(半角英数記号 64文字以内)

Basic Constraints ☒ non-critical ☐ critical

使用目的 ☒ 付与しない ☐ 付与する
☒ non-critical ☐ critical
☐ digitalSignature(0)
☐ KeyCertSign(5)
☐ CRLSign(6)

CRL配布ポイント ⑤ ☐ 使用する ☒ 使用しない
(半角英数記号 1024文字以内)

OCSP URI ⑥ ☐ 使用する ☒ 使用しない
(半角英数記号 1024文字以内)

■ 自己認証局情報設定

設定項目	設定値
①認証局	自己認証局
②名前(cn)	ca_kokomo
③国(c)	日本(JP)
④都道府県(st)	Tokyo
⑤CRL配付ポイント	使用しない
⑥OCSP URI	使用しない

・CRL配付ポイント、OCSP URIはデフォルトで「使用する」になっているので「使用しない」を選択し、登録します。必要な場合は「使用する」を選択し、値を入力して登録してください。

・CA設定登録後、同じCNの内部サーバー証明書が自動で生成されます

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

▶ 3-3-2.内部サーバー証明書設定

- ▶ 管理ツール [CA]－[CA設定]を開き、内部サーバー証明書の[設定]をクリックします

内部サーバー証明書設定

入力規則

サーバー証明書情報

名前(cn)※ ① ☒ 自己認証局と同じcnとする
(半角英数記号 64文字以内) ☐ 任意 ca_kokomo

国(c) ②

都道府県(st)※ ③
(半角英数記号 128文字以内)

市区町村(l)
(半角英数記号 128文字以内)

組織名(o)
(半角英数記号 64文字以内)

部署(ou)
(半角英数記号 64文字以内)

メールアドレス(E-mail)
(半角英数記号 128文字以内)

使用目的
☒ 付与しない ☐ 付与する
☒ non-critical ☐ critical
☐ digitalSignature(0)
☐ keyEncipherment(2)

CRL配布ポイント ④ ☐ 使用する ☒ 使用しない
(半角英数記号 1024文字以内)

OCSP URI ⑤ ☐ 使用する ☒ 使用しない
(半角英数記号 1024文字以内)

SANs dnsName ⑥
(半角英数記号 255文字以内)
(1行1設定 最大10行)

有効期限

■ 内部サーバー証明書設定

設定項目	設定値
①名前(cn)	自己認証局と同じcnとする
②国(c)	日本(JP)
③都道府県(st)	Tokyo
④CRL配付ポイント	使用しない
⑤OCSP URI	使用しない
⑥SANs dnsName	dnsskokomo

・CRL配付ポイント、OCSP URIはデフォルトで「使用する」になっているので「使用しない」を選択し、登録します。必要な場合は「使用する」を選択し、値を入力して登録してください。

・Android端末でEAP-TLS認証する場合、ドメインを入力する必要があります。「SANs dnsName」で設定した値がドメインとなります。

※WPA3-Enterprise 192-bit modeで認証する場合、設定項目「鍵長」の設定値を「4096bit」以上にする必要があります。

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

▶ 3-3-3.クライアント証明書ポリシー

▶ ※EAP-TLS WPA3 192-bit モードで認証する場合、当該設定が必要です。

▶ 管理ツール [CA]－[クライアント証明書ポリシー]をクリックします

クライアント証明書ポリシー

通知メール設定

クライアント証明書有効期限 ☒ 全体に設定する(以降に発行する証明書に適用)

☒ CA証明書の有効期限に準ずる(2036年04月07日)

☐ 日付指定

証明書1

証明書2

☐ 発行日からの有効期間を指定

証明書1 年

証明書2 年

☐ アカウントごとに設定する(初期値)

☒ CA証明書の有効期限に準ずる(2036年04月07日)

☐ 日付指定

証明書1

証明書2

☐ 発行日からの有効期間を指定

証明書1 年

証明書2 年

署名アルゴリズム

鍵長 ①

■ クライアント証明書ポリシー

設定項目	設定値
①鍵長	4096bit

▶ 設定後、画面下部の[登録]をクリックします

▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

▶ 3-4-1.RADIUS設定

▶ 管理ツール [RADIUS]－[RADIUS設定]を開きます

RADIUS設定

RADIUSポート番号※
(半角数字 1～65535) ① 1812

RADIUS Accounting※
(半角数字 1～65535) ② ☐使用する ☒使用しない
ポート番号 1813

接続状況 ☒記録する ☐記録しない

二重ログイン ☒許可する ☐許可しない

ログアウト ☐Framed-IP-Address属性を含まないAccounting-Stopを無視する

認証サーバー証明書 ③ ☐使用しない ☒内部サーバー証明書 ☐外部サーバー証明書 登録
通知メール設定

認証局 ④ ☒内部認証局 ☐外部認証局

IEEE 802.1X認証 ⑤ ☒EAP-TLS ☒PEAP ☐EAP-TTLS ☐EAP-MD5 ☐EAP-MSCHAPv2
PEAPの対応inner-tunnel認証方式:EAP-MSCHAPv2, EAP-TLS
TTLSの対応inner-tunnel認証方式:PAP, CHAP, MSCHAPv2, EAP-MSCHAPv2, EAP-TLS
☐outer-tunnel認証のAccess-AcceptにReply-Message属性を含める

内部アカウント ☒使用する ☐使用しない

認証失敗アカウントロック ☐使用する ☒使用しない
認証連続失敗回数 5
通知メール設定

最終認証日時記録 ☒内部アカウント ☐外部LDAP/ADアカウント

▶ 設定後、画面下部の[登録]をクリックします

▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

■ RADIUS設定

設定項目	設定値
①RADIUSポート番号	1812
②RADIUS Accounting	使用しない
③認証サーバー証明書	内部サーバー証明書
④認証局	内部認証局
⑤IEEE 802.1X認証	EAP-TLS/PEAP

・認証サーバー証明書:内部サーバー証明書
(サーバー証明書検証の際にCA設定で設定した内部サーバー証明書を使います。)

・認証局:内部認証局
(本製品を認証局として指定するための設定となります。)

※WPA3-Enterprise 192-bit modeで認証する場合、設定項目「Cipher Suites」の設定値を「任意設定:ECDHE-RSA-AES256-GCM-SHA384」にする必要があります。

- ▶ 3-4-2.RADIUSクライアント登録
 - ▶ 管理ツール [RADIUS]－[RADIUSクライアント]を開きます
 - ▶ 画面上部の[新規登録]をクリックします

RADIUSクライアント登録

登録用ファイルサンプル

ヘルプ

戻る

ファイルから一括登録 ▼

クライアントID※ ① kokomo-ap
(半角英数記号 32文字以内)

クライアント名
(50文字以内)

IPアドレス※ ② 192.168.102.5
(XXX.XXX.XXX.XXXまたは
XXX.XXX.XXX/XX)

シークレットキー※ ③
(半角英数記号 128文字以内) (確認用)

■ RADIUSクライアント登録

設定項目	設定値
①クライアントID	kokomo-ap
②IPアドレス	192.168.102.5
③シークレットキー	kokomo

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

▶ 3-4-3.ネットワークプロファイルの設定

- ▶ 管理ツール [RADIUS]－[ネットワークプロファイル]を開きます
- ▶ [ネットワーク属性]タブを選択し、画面上部の[新規登録]をクリックします

ネットワーク属性編集

ネットワーク接続 ① ☒ 許可する ☐ 拒否する

名称※ (32文字以内) ② VLAN10用

備考 (256文字以内)

Account@Adapter+ V7定義済み属性

NA-Vlan-Id (半角数字 10文字以内) Reply ☐ 個別設定する

Access-Defender-Class (半角数字 10文字以内) Reply ☐ 個別設定する

Filter-Id (半角英数字 253文字以内) Reply ☐ 個別設定する

Callback-Number (半角英数字 253文字以内) Check ☐ 個別設定する

Tunnel-Type ③ Reply 13 ☐ 個別設定する

Tunnel-Medium-Type ④ Reply 6 ☐ 個別設定する

Tunnel-Private-Group-Id ⑤ Reply 10 ☐ 個別設定する

☒ このネットワーク属性を標準ネットワーク属性としたネットワークプロファイルを作成する。

名称※ (32文字以内) ⑥ Profile-VLAN10

備考 (256文字以内)

■ ネットワーク属性登録

設定項目	設定値①
①ネットワーク接続	許可する
②名称	VLAN10用
③Tunnel-Type	13
④Tunnel-Medium-Type	6
⑤Tunnel-Private-Group-Id	10
⑥名称	Profile-VLAN10

・②名称はネットワーク属性名になります。⑥名称はネットワークプロファイル名になります。

・「このネットワーク属性を標準ネットワーク属性としたネットワークプロファイルを作成する。」にチェックし、名称を入力して登録することで、ネットワークプロファイルを同時に作成することができます。

・作成したネットワークプロファイルは[ネットワークプロファイル]タブを選択し[編集]を押すことで編集をすることができます。RADIUSクライアントの指定などの細かい制御が可能です。

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

- ▶ 3-5-1.サブディレクトリ作成
 - ▶ ディレクトリペインの[home]を開きます
 - ▶ [ディレクトリ] タブを選択し、画面上部の[新規登録]をクリックします

ディレクトリ作成

親ディレクトリ home

ディレクトリ名※ ① dir-a

LDAPディレクトリ名

ユーザー登録数 ☒ 無制限 ☐ 制限する 件

端末登録数 ☒ 無制限 ☐ 制限する 件

証明書登録数 ☒ 無制限 ☐ 制限する 件

IPプール

IPプール設定 未指定 ▼

端末共通パスワード

端末共通パスワード ☒ 上位と同じ設定で作成 ☐ 全端末共通パスワードを設定 ☐ 任意の値を設定

共通アトリビュート

共通アトリビュート ② ☐ 作成しない ☐ 上位と同じ設定で作成 ☒ 個別に作成

ネットワークプロファイル ③ Profile-VLAN10 ▼

■ ディレクトリ作成

設定項目	設定値①
①ディレクトリ名	dir-a
②共通アトリビュート	個別に作成
③ネットワークプロファイル	Profile-VLAN10

・共通アトリビュート:ディレクトリ内のすべてのアカウントに対して、共通のネットワーク関連属性を一括設定する機能。

・前項で作成したネットワークプロファイル「Profile-VLAN10」をディレクトリ「dir-a」の共通アトリビュートに設定することで、dir-aに登録されたアカウントにはそのネットワークプロファイルが適用されます。

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ 3-5-2.端末共通パスワード設定
 - ▶ ディレクトリペインの[dir-a]を開きます
 - ▶ 右ペイン上部の [ディレクトリ]をクリックします

端末共通パスワード

端末共通パスワード

① ☒ 変更する ☐ 変更しない

☐ 全端末共通パスワードを設定

☐ 任意の値を設定

(確認用)

② ☒ MAC アドレスを設定

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ ポップアップウィンドーが出てくるので、[OK]をクリックします

■ 端末共通パスワード

設定項目	設定値①
①端末共通パスワード	変更する
②端末共通パスワード種別	MACアドレスを指定

・端末共通パスワード:MAC認証時にRADIUSクライアントとRADIUSサーバー間でやり取りされるパスワードのこと。

・RADIUS認証においては、MAC認証の場合も、RADIUSクライアント-RADIUSサーバー間ではuser-nameとpassword属性を用いた通信が行われます。

・RADIUSクライアントの設定や仕様に合わせた設定を行ってください。

・「MACアドレスを設定」に設定することで、区切りなし小文字MACアドレスをパスワードとして利用します。

- ▶ 3-5-3.Web認証・EAP-PEAP認証用 ユーザーアカウント登録
 - ▶ ディレクトリペインの[dir-a]ディレクトリー[ユーザー]タブを開きます
 - ▶ [新規登録]をクリックします

ディレクトリ home > dir-a

ユーザーID ※ ① user01
(半角英数記号 64文字以内)

姓
(256文字以内)

名
(256文字以内)

アカウント管理者 naadmin
(半角英数記号空白 64文字以内)

通知用メールアドレス
(半角英数記号 254文字以内)
(1行1属性 最大5行)

パスワード ※ ② (確認用)
(半角英数記号 64文字以内)

説明
(256文字以内)

アカウント利用開始日時 2026-04-09 00:00
(YYYY-MM-DD hh:00)

アカウント有効期限 ※ ③ ●無期限
(YYYY-MM-DD hh:00) ○期限あり

ネットワーク利用 ●有効 ○無効

アカウント利用 ●有効 ○無効 ○一時停止

■ ユーザーアカウント登録

設定項目	設定値①
①ユーザーID	user01
②パスワード	kokomo
③アカウント有効 期限	無期限

・dir-aにuser01を作成

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ 3-5-4.MAC認証用 端末(MAC)アカウント登録
 - ▶ ディレクトリペインの[dir-a]ディレクトリー[端末(MAC)]タブを開きます
 - ▶ [新規登録]をクリックします

ディレクトリ home > dir-a

MACアドレス ※ ①

(例: 00:00:00:00:00:00)

端末名
(256文字以内)

アカウント管理者
(半角英数記号空白 64文字以内) naadmin

通知用メールアドレス
(半角英数記号 254文字以内)
(1行1属性 最大5行)

説明
(256文字以内)

アカウント利用開始日時
(YYYY-MM-DD hh:00) 2026-04-09 00:00

アカウント有効期限 ※ ② ☒ 無期限
☐ 期限あり

(YYYY-MM-DD hh:00)

ネットワーク利用 ☒ 有効 ☐ 無効

アカウント利用 ☒ 有効 ☐ 無効

最終認証日時

■ 端末(MAC)アカウント登録

設定項目	設定値①	設定値②	設定値③	設定値④
①MACアドレス	(Windows端末のMACアドレス)	(MacOS端末のMACアドレス)	(iOS端末のMACアドレス)	(Android端末のMACアドレス)
②アカウント有効期限	無期限	無期限	無期限	無期限

- ・dir-aに4つの端末(MAC)アカウントを作成
- ・各種、クライアント端末のMACアドレスを入力し登録

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ 3-5-5.EAP-TLS認証用 証明書アカウント登録
 - ▶ ディレクトリペインの[dir-a]ディレクトリー[証明書]タブを開きます
 - ▶ [新規登録]をクリックします

ディレクトリ

home > dir-a

cn ※
(半角英数記号 64文字以内)

① cert01

証明書アカウント名
(256文字以内)

アカウント管理者
(半角英数記号空白 64文字以内)

naadmin

通知用メールアドレス
(半角英数記号 254文字以内)
(1行1属性 最大5行)

説明
(256文字以内)

アカウント利用開始日時
(YYYY-MM-DD hh:mm)

2026-04-09 00:00

発行済み証明書1利用開始日時

発行済み証明書1有効期限

次回発行する証明書有効期限
※

CA証明書の有効期限に準ずる：2036-04-11

ネットワーク利用

☒有効 ☐無効

アカウント利用

☒有効 ☐無効

■ 証明書アカウント登録

設定項目	設定値①	設定値②	設定値③	設定値④
①cn	cert01	cert02	cert03	cert04

- ・dir-aに4つの証明書アカウントを作成
- ・cert01をWindows用、cert02をMacOS用、cert03をiOS用、cert04をAndroid用に想定して作成

- ▶ 設定後、画面下部の[登録]をクリックします

- ▶ 3-5-6.EAP-TLS認証用 証明書発行①
 - ▶ ディレクトリペインの[dir-a]ディレクトリー[証明書]タブを開きます
 - ▶ 証明書アカウントの証明書1欄にある[発行]をクリックします

No.	☐	cn ▲▼	証明書アカウント名 ▲▼	発行済み証明書1有効期限	最終認証日時 ▲▼	アカウント管理者 ▲▼	証明書1	証明書2	編集
1	☐	cert01				naadmin	発行	-	

- ▶ ポップアップウィンドーが起動するので、[OK]をクリックします

192.168.102.3:8080 の内容

証明書を発行します。
よろしいですか？

OK

キャンセル

- ▶ 発行完了となります。
- ▶ 証明書のダウンロードは[DL未]を、証明書の停止は[一時停止]を、失効は[失効]をそれぞれ押すことで可能です

No.	☐	cn ▲▼	証明書アカウント名 ▲▼	発行済み証明書1有効期限	最終認証日時 ▲▼	アカウント管理者 ▲▼	証明書1	証明書2	編集
1	☐	cert01		2036-04-11 00:00:00		naadmin	失効 DL未 New 一時停止	-	

▶ 3-6-1.外部AD登録①

- ▶ 管理ツール [外部LDAP/AD参照]-[外部LDAP/AD一覧]-[新規登録]をクリックします

外部LDAP/AD登録

優先順位
(半角数字0~999) 0

名称 ※ ① AD(4.3)
(32文字以内)

種別 ※ ② ☒ LDAP
☒ Active Directory
ドメイン
(半角英数記号 252文字以内) ③ adapter-demo.com

IPアドレスまたはFQDN ※ ④ 192.168.4.3
(半角英数記号 64文字以内)

検索フィルタ ※ ☒ 標準設定
(半角英数記号 1024文字以内) ☐ 任意設定

LDAP属性マップ ※ ☒ 標準設定 DL
☐ ファイルを登録
ファイルの選択 ファイルが選択されていません
☐ 1行目を無視して登録する

匿名bind※ ☒ 使用しない ☐ 使用する

bindDN ※ ⑤ CN=adapter_admin,CN=Users,DC=adapt
(1024文字以内)

bindDNパスワード ※ ⑥ (確認用)
(半角英数記号 128文字以内)

BaseDN ※ ⑦ DC=adapter-demo,DC=com
(1024文字以内)

- ▶ 設定後、画面下部の[登録]をクリックします
- ▶ [登録]をクリック後、画面左上の[RADIUS設定反映]をクリックします

■ 外部AD登録

設定項目	設定値
①名称	AD(4.3)
②種別	Active Directory
③ドメイン	adapter-demo.com
④IPアドレスまたはFQDN	192.168.4.3
⑤bindDN	CN=adapter_admin,CN=Users,DC=adapter-demo,DC=com
⑥bindDNパスワード	(bindDNパスワード)
⑦BaseDN	DC=adapter-demo,DC=com

■ AD登録ユーザー情報

設定項目	設定値
①ID	hcnet01
②パスワード	hcnet01

▶ 3-6-1.外部AD登録②

- ▶ 外部LDAP/AD参照一覧から、登録したADを確認できます
- ▶ [ドメイン設定]をクリックします

外部LDAP/AD一覧 ヘルプ

新規登録 ドメイン設定 NetBIOSドメイン名対応表 NTLM認証設定

該当するデータは2件あります。

削除 優先順位更新

ID	☐	優先順位	区分	接続先	名称	状態	備考	編集
DB	☐	0	-	127.0.0.1	内部DB	有効	内部登録アカウント	-
LDAP3	☐	0	AD *	192.168.4.3	AD(4.3)	有効		

- ▶ [このドメインに参加する]項目に、前項で設定した「ADサーバーの名称:ドメイン名」を選択する
- ▶ 設定後、画面下部の[登録]をクリックします

ドメイン設定

このドメインに参加する※ AD(4.3) : adapter-demo.com ▼

NetBIOSドメイン名
(半角英数記号 15文字以内)

- ▶ 3-6-1.外部AD登録③
 - ▶ 外部LDAP/AD参照一覧を開きます
 - ▶ [有効]をクリックします

ID	☐	優先順位	区分	接続先	名称	状態	備考	編集
DB	-	0	-	127.0.0.1	内部DB	有効	内部登録アカウント	-
LDAP3	☐	0	AD*	192.168.4.3	AD(4.3)	有効		

- ▶ 以下の確認結果メッセージが出れば、AD連携成功です
- ▶ 失敗する場合は、各種パラメータを見直してください

LDAP検索が成功しました。
ADへの接続情報の確認が成功しました。(0)
ADへのcomputerアカウントの参加状態の確認が成功しました。(0)
NTLM認証の確認が成功しました。(0)

4. 検証

4-1.Web認証

4-2.MAC認証

4-3.EAP-PEAP認証(内部DB)

4-4.EAP-PEAP認証(外部AD)

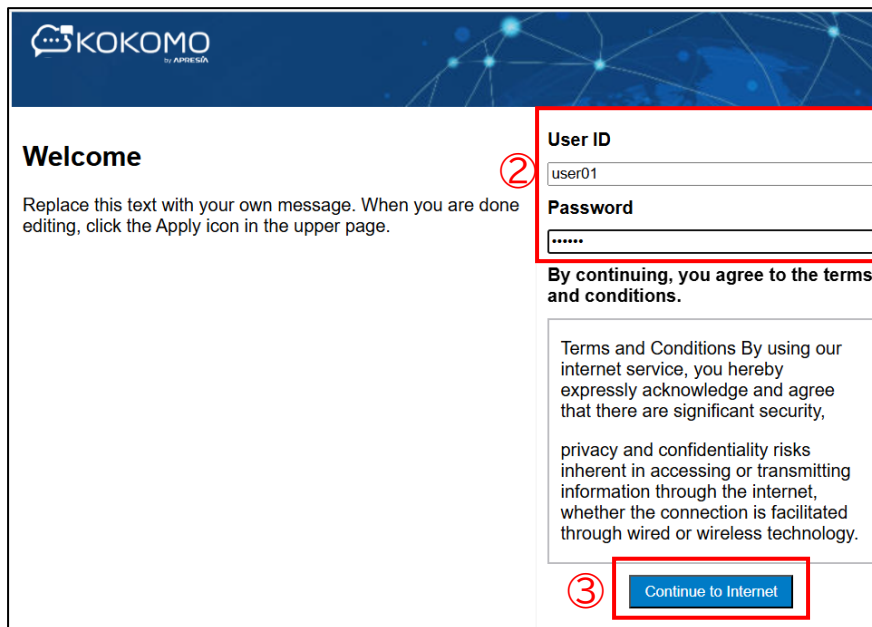
4-5.EAP-TLS認証

4-6.属性応答

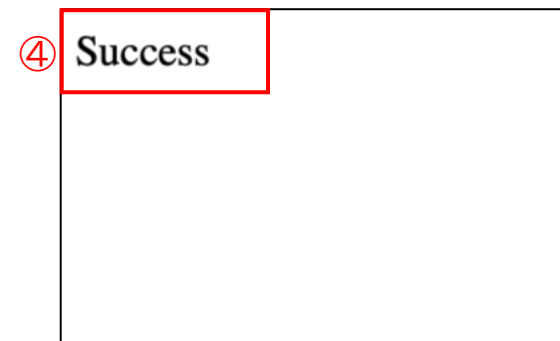


 Adapter

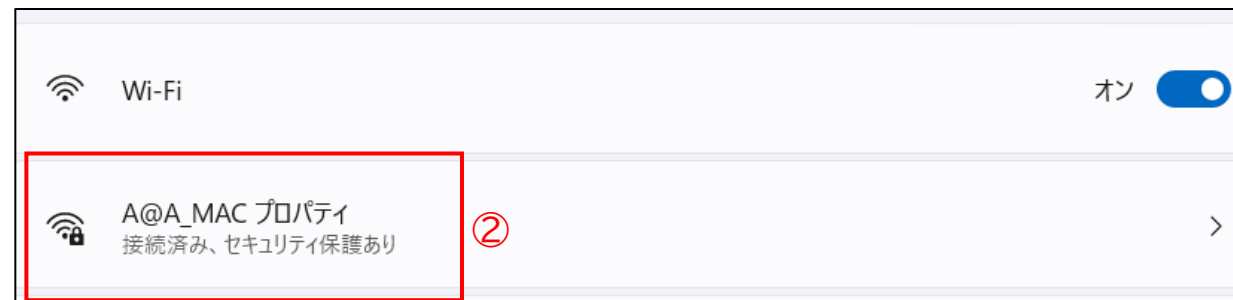
- ▶ Windows /MacOS /iOS/Android におけるWeb認証の実施
- ▶ Web認証の手順は各OSで共通のため、代表例としてWindows端末での認証手順を掲載しています
- ▶ ① SSID「A@A_Web」の[接続]をクリックします
 - ▶ 自動的にブラウザが起動しキャプティブポータルに遷移します
- ▶ ② User ID:user01 Password: kokomo を入力します
- ▶ ③ [Continue to Internet]をクリックします
- ▶ ④ 認証成功すると「Success」と表示されます



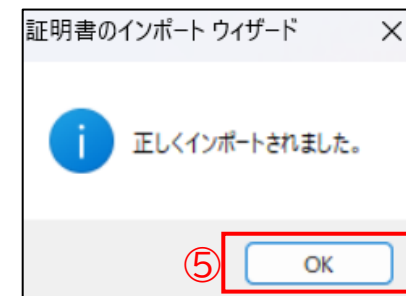
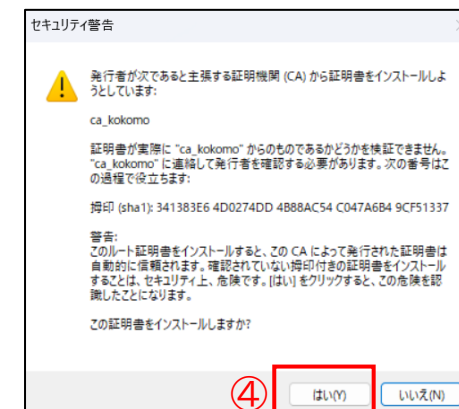
The screenshot shows the 'KOKOMO' captive portal login page. The page has a blue header with the 'KOKOMO' logo. Below the header, there is a 'Welcome' section with a message: 'Replace this text with your own message. When you are done editing, click the Apply icon in the upper page.' To the right of the welcome message, there are two input fields: 'User ID' (containing 'user01') and 'Password' (containing '*****'). These fields are highlighted with a red box and a circled '2'. Below the password field, there is a checkbox labeled 'By continuing, you agree to the terms and conditions.' and a text box containing the terms and conditions. At the bottom right, there is a blue button labeled 'Continue to Internet', which is highlighted with a red box and a circled '3'.



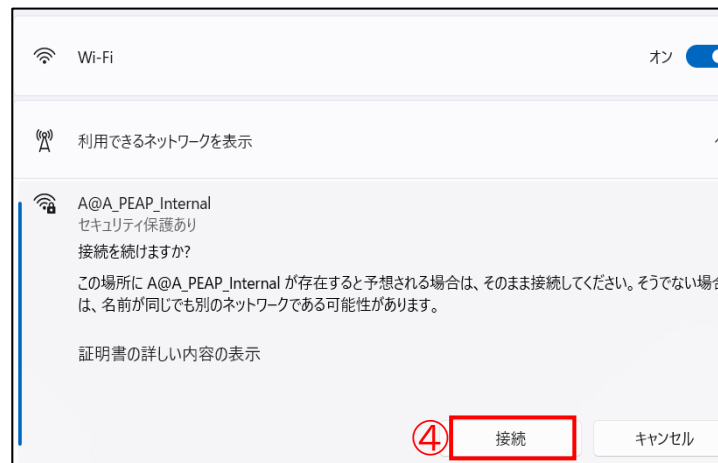
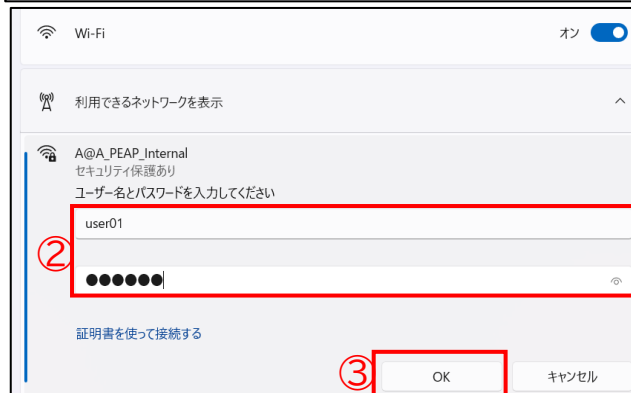
- ▶ Windows /MacOS /iOS/Android におけるMAC認証の実施
- ▶ MAC認証の手順は各OSで共通のため、代表例としてWindows端末での認証手順を掲載しています
 - ▶ ① SSID「A@A_MAC」の[接続]をクリックします
 - ▶ ② 認証成功すると「接続済み」もしくはSSID名にチェックが表示されます



- ▶ 4-3-1.EAP-PEAP認証における事前準備
 - ▶ 事前準備:クライアント端末にCA証明書をインポートしておきます
- ▶ 代表例としてWindows端末でのインポート手順を掲載しています。
 - ▶ ① 管理ツール [CA]－[CA設定]を開き、CAの[p12]をクリックします
 - ▶ ② ダウンロードファイルをクリックします(警告画面が出た場合、[許可する]を選択してください)
 - ▶ ③ 起動した『証明書のインポートウィザード』をすべてデフォルトのまま[次へ]をクリックします
 - ▶ ④ セキュリティ警告ダイアログが出るので[はい]をクリックします
 - ▶ ⑤ [正しくインポートされました]と表示されたら完了です



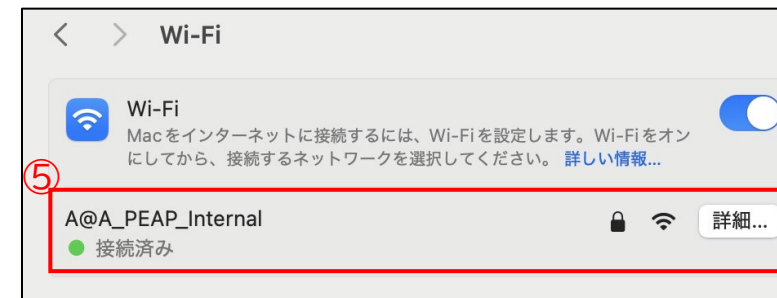
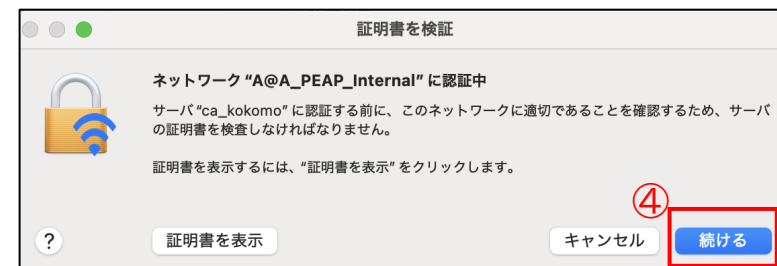
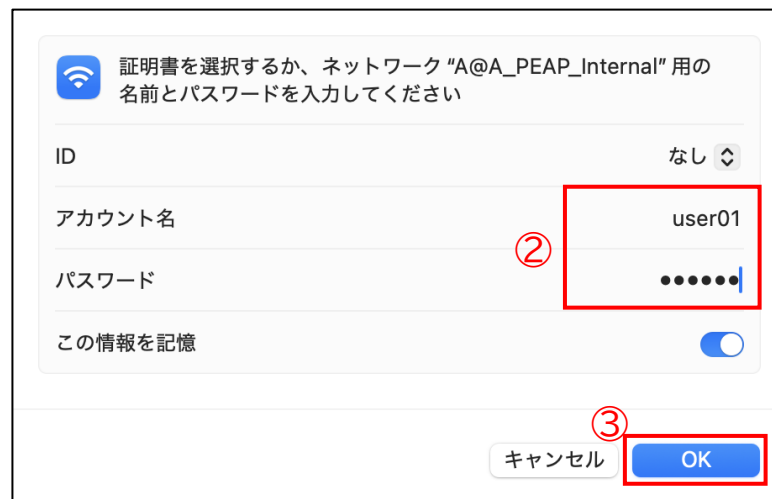
- ▶ 4-3-2.Windows におけるEAP-PEAP認証(内部DB)の実施
 - ▶ ① SSID「A@A_PEAP_Internal」の[接続]をクリックします
 - ▶ ② ユーザー名:user01 パスワード:kokomo を入力します
 - ▶ ③ [OK]をクリックします
 - ▶ ④ [接続]をクリックします
 - ▶ ⑤ 認証成功すると「接続済み」と表示されます



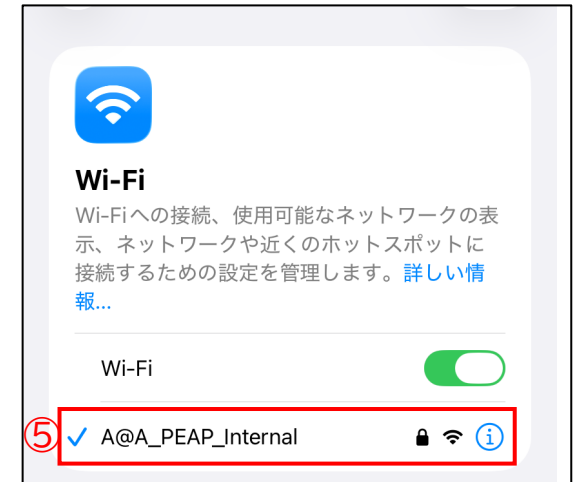
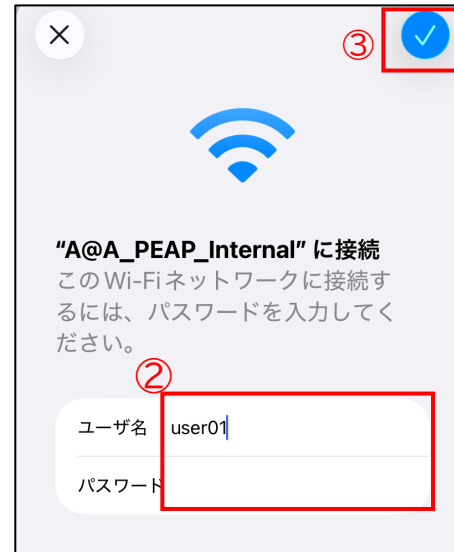
4-3.EAP-PEAP認証(内部DB)

▶ 4-3-3.MacOS におけるEAP-PEAP認証(内部DB)の実施

- ▶ ① SSID「A@A_PEAP_Internal」をクリックします
- ▶ ② アカウント名:user01 パスワード:kokomo を入力します
- ▶ ③ [OK]をクリックします
- ▶ ④ [続ける]をクリックします
- ▶ ⑤ 認証成功すると「接続済み」と表示されます



- ▶ 4-3-4.iOS におけるEAP-PEAP認証(内部DB)の実施
 - ▶ ① SSID「A@A_PEAP_Internal」をクリックします
 - ▶ ② ユーザー名:user01 パスワード:kokomo を入力します
 - ▶ ③ [信頼]をクリックします
 - ▶ ④ 認証成功するとSSID名にチェックが表示されます



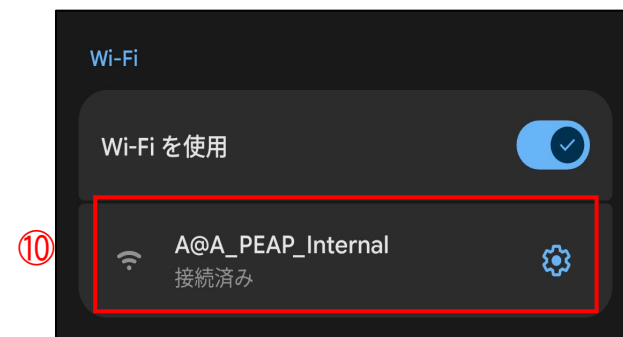
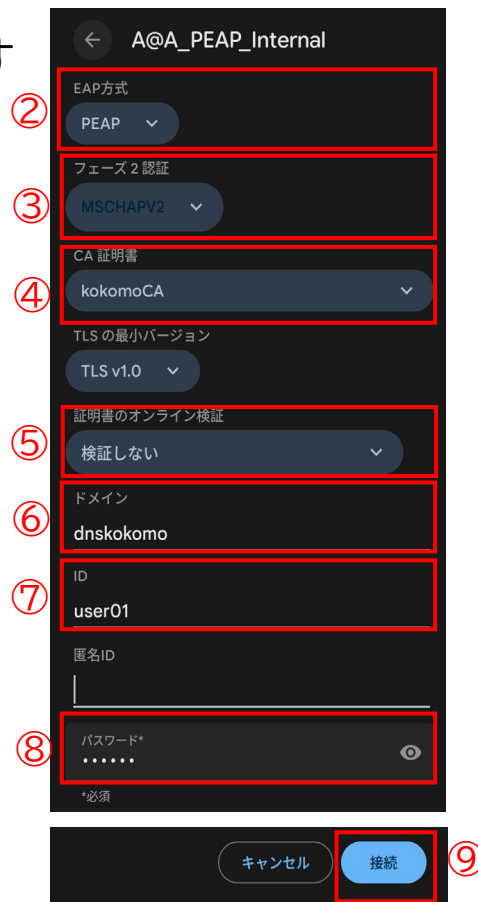
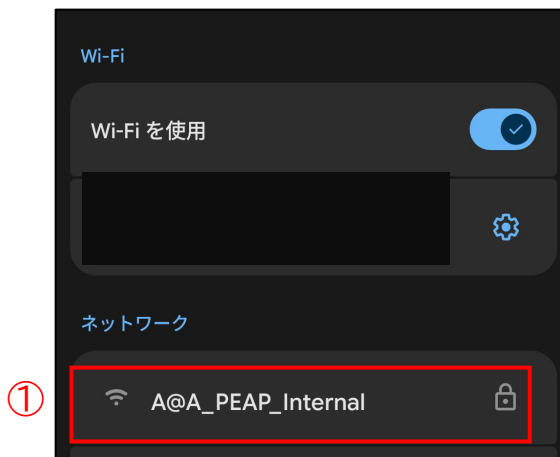
4-3.EAP-PEAP認証(内部DB)

▶ 4-3-5.AndroidにおけるEAP-PEAP認証(内部DB)の実施

- ▶ ① SSID「A@A_PEAP_Internal」をクリックします
- ▶ ②～⑧表に記載の値を入力/選択します
- ▶ ⑨ [接続]をクリックします
- ▶ ⑩ 認証成功すると「接続済み」と表示されます

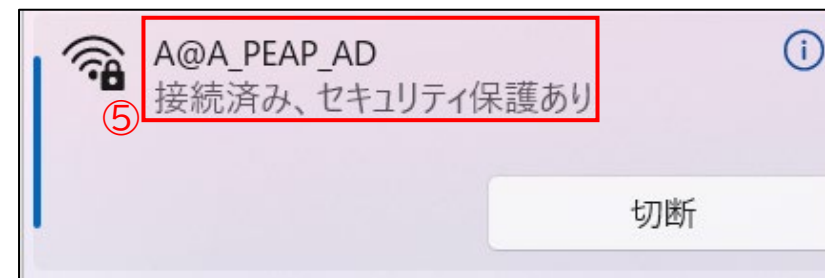
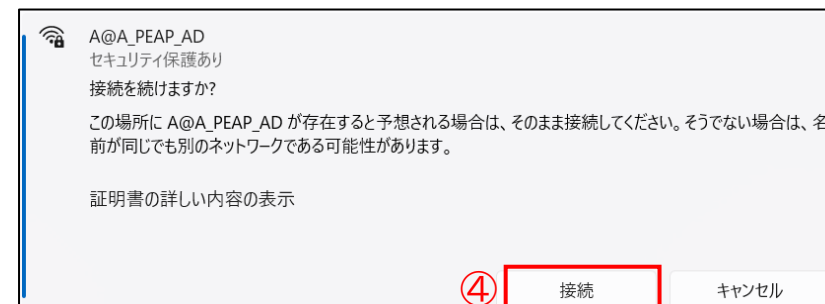
■ 認証設定

設定項目	設定値
②EAP方式	PEAP
③フェーズ2認証	MSCHAPV2
④CA証明書	kokomoCA
⑤オンライン認証ステータス	検証しない
⑥ドメイン	dnskokomo
⑦ID	user01
⑧パスワード	kokomo

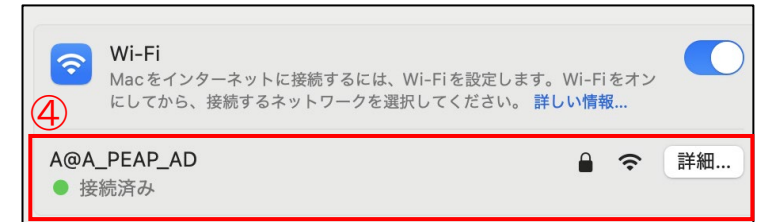
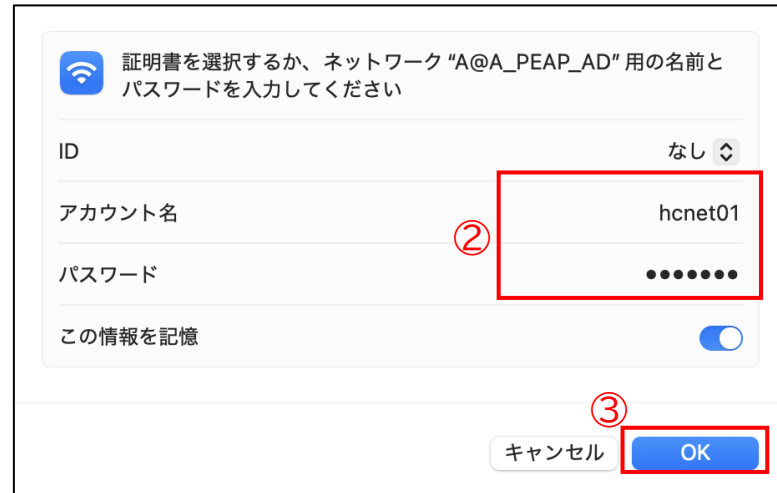
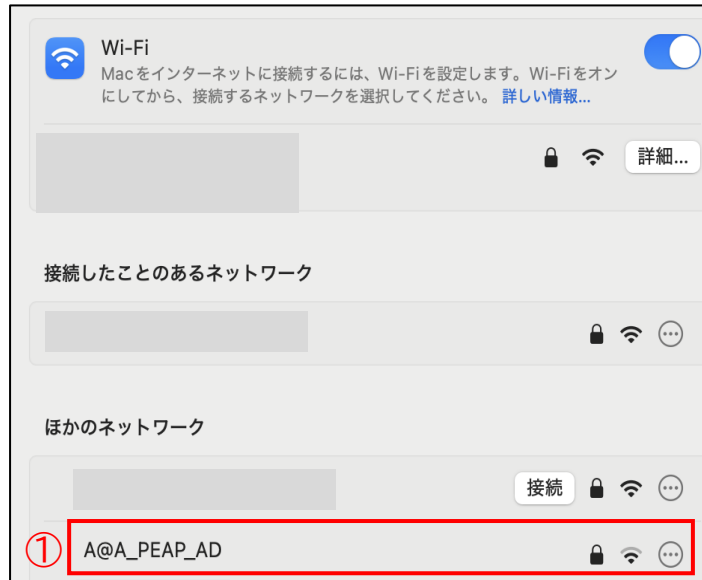


4-4.EAP-PEAP認証(外部AD)

- ▶ 4-4-1.Windows におけるEAP-PEAP認証(外部AD)の実施
 - ▶ ① SSID「A@A_PEAP_AD」の[接続]をクリックします
 - ▶ ② ユーザー名:hcnet01 パスワード:hcnet01 を入力します
 - ▶ ③ [OK]をクリックします
 - ▶ ④ [接続]をクリックします
 - ▶ ⑤ 認証成功すると「接続済み」と表示されます

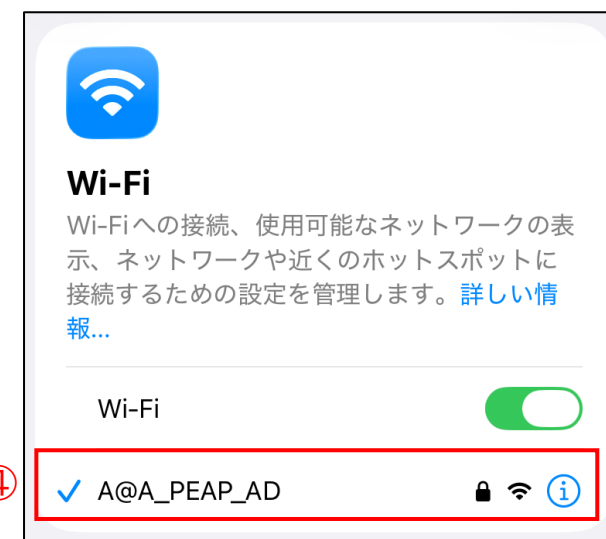
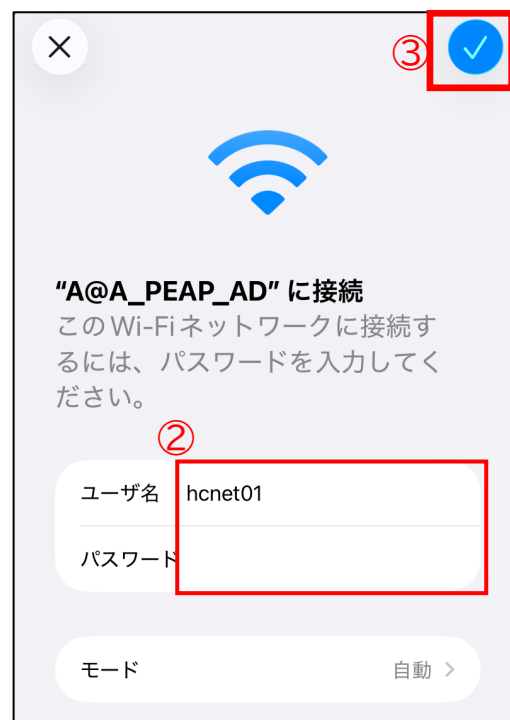
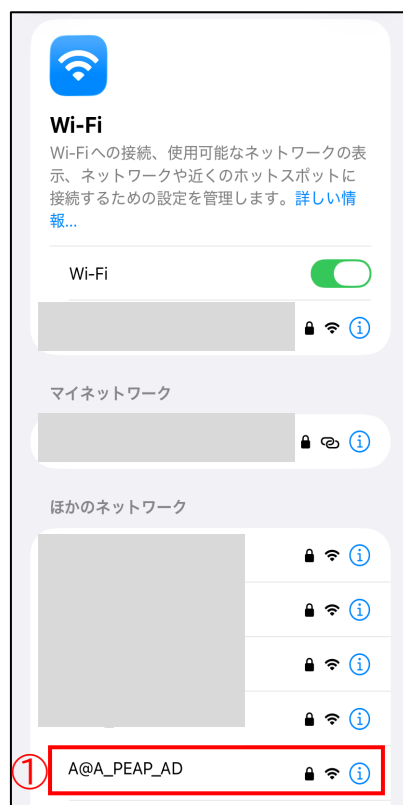


- ▶ 4-4-2.MacOS におけるEAP-PEAP認証(外部AD)の実施
 - ▶ ① SSID「A@A_PEAP_AD」をクリックします
 - ▶ ② アカウント名:hcnet01 パスワード:hcnet01 を入力します
 - ▶ ③ [OK]をクリックします
 - ▶ ④ 認証成功すると「接続済み」と表示されます



4-4.EAP-PEAP認証(外部AD)

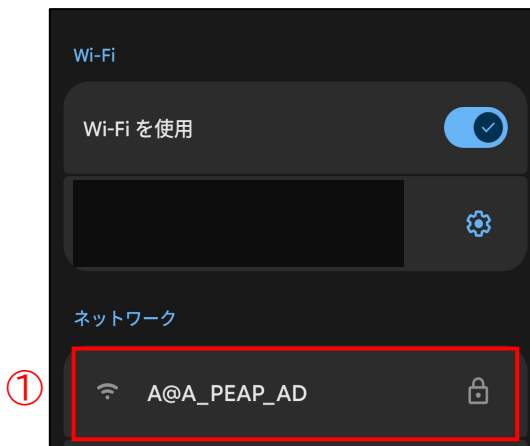
- ▶ 4-4-3.iOS におけるEAP-PEAP認証(外部AD)の実施
 - ▶ ① SSID「A@A_PEAP_AD」をクリックします
 - ▶ ② ユーザー名:hcnet01 パスワード:hcnet01 を入力します
 - ▶ ③ [チェックマーク]をクリックします
 - ▶ ④ 認証成功するとSSID名にチェックが表示されます



4-4.EAP-PEAP認証(外部AD)

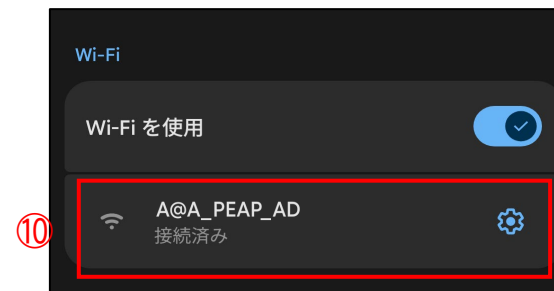
▶ 4-4-4.AndroidにおけるEAP-PEAP認証(外部AD)の実施

- ▶ ① SSID「A@A_PEAP_AD」をクリックします。
- ▶ ②～⑧表に記載の値を入力/選択します
- ▶ ⑨ [接続]をクリックします
- ▶ ⑩ 認証成功すると「接続済み」と表示されます



■ 認証設定

設定項目	設定値
②EAP方式	PEAP
③フェーズ2認証	MSCHAPV2
④CA証明書	kokomoCA
⑤オンライン認証ステータス	検証しない
⑥ドメイン	dnskokomo
⑦ID	hcnet01
⑧パスワード	hcnet01



▶ 4-5-1.EAP-TLS認証における事前準備

▶ 事前準備:クライアント端末にCA証明書およびクライアント証明書をインポートしておきます。

▶ CA証明書のインポート手順はスライド41をご参照ください

▶ 代表例としてWindows端末でのインポート手順を掲載しています。

▶ ① 管理ツールのディレクトリペイン[dir-a] – [証明書]タブを開き、「証明書1」列の[DL未]をクリックします

▶ ② [インポートパスワード]に任意の値を入力し、[実行]をクリックします

▶ ③ ダウンロードファイルをクリックします(警告画面が出た場合、[許可する]を選択してください)

▶ ④ 起動した『証明書のインポートウィザード』をすべてデフォルトのまま[次へ]をクリックします

▶ ⑤ パスワードは②で設定した値を入力して[次へ]をクリックします

▶ ⑥ [正しくインポートされました]と表示されたら完了です

No.	cn	証明書アカウント名	発行済み証明書1有効期限	最終認証日時	アカウント管理者	証明書1
1		cert01	2036-04-11 00:00:00		naadmin	失効 DL未 new 一時停止 ①

インポートパスワード入力

インポートパスワード ※ ② (半角英数記号 30文字以内)

..... (確認用)

実行 キャンセル

▼ 今日

cert01_1 ③

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。

④ 次へ(N) キャンセル

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。

⑤ パスワード(P):
☐ パスワードの表示(O)

インポートオプション(O):
☐ 秘密キーの保護を強制的にする(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)

次へ(N) キャンセル

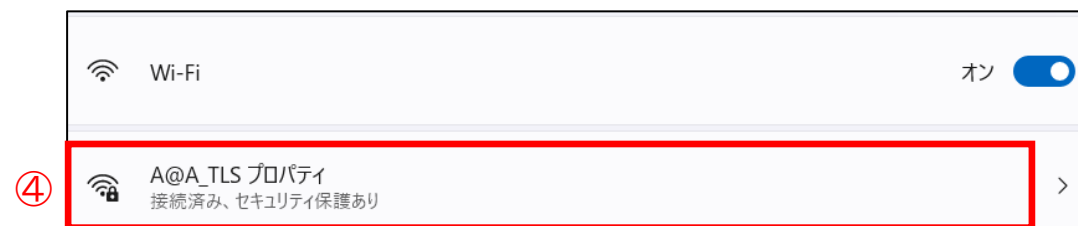
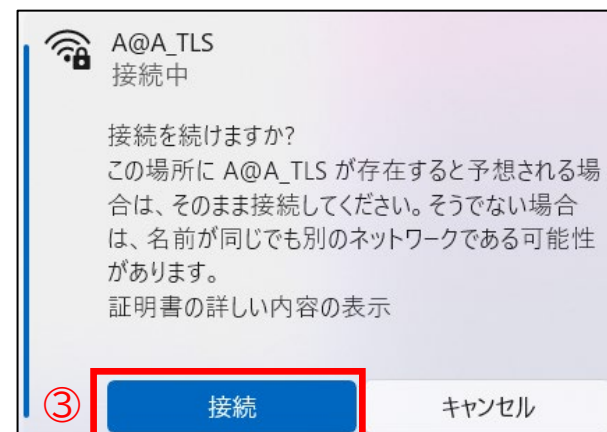
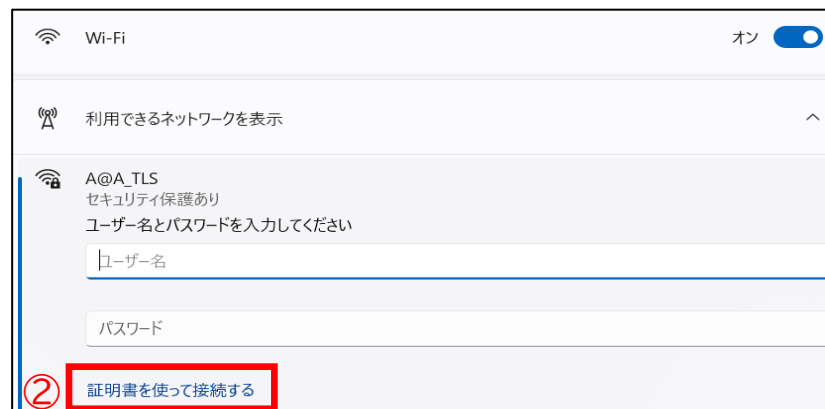
証明書のインポートウィザード

正しくインポートされました。

⑥ OK

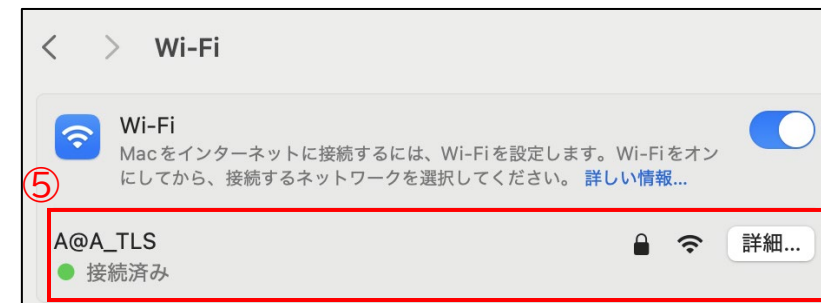
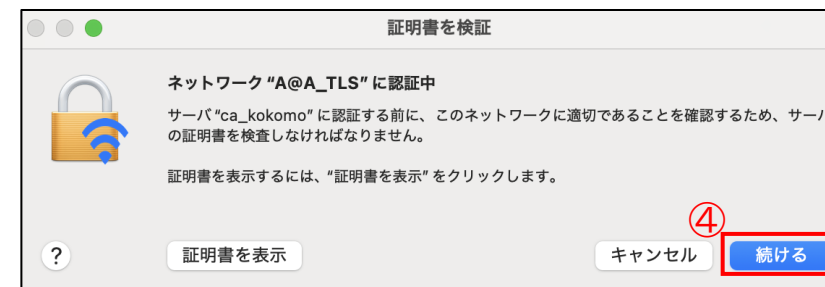
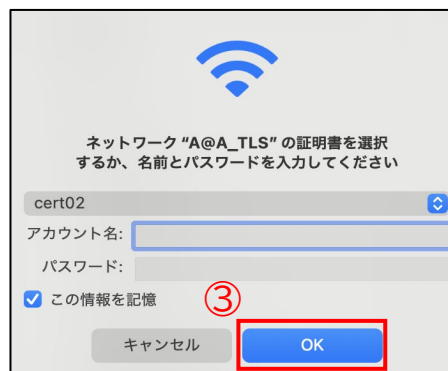
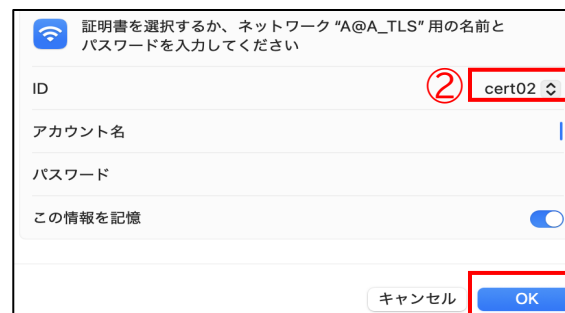
▶ 4-5-2.Windows における EAP-TLS認証の実施

- ▶ ① SSID「A@A_TLS」の[接続]をクリックします
- ▶ ② [証明書を使って接続する]をクリックします
- ▶ ③ [接続]をクリックします
- ▶ ④ 認証成功すると「接続済み」と表示されます

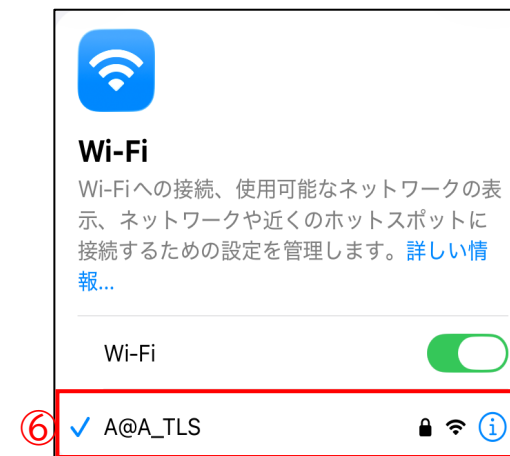
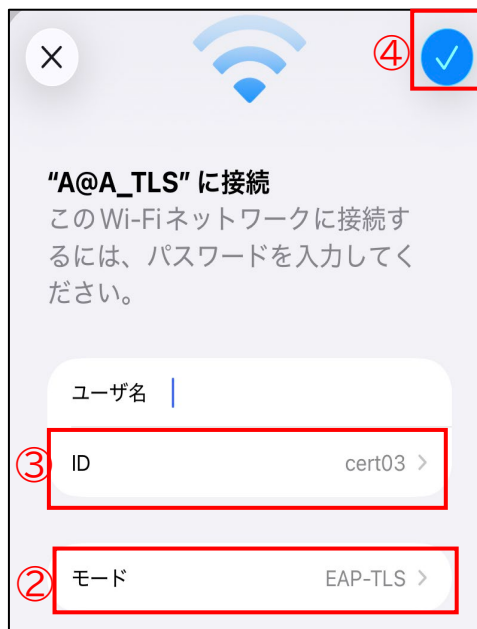


▶ 4-5-3.MacOS におけるEAP-TLS認証の実施

- ▶ ① SSID「A@A_TLS」をクリックします
- ▶ ② プルダウンから[cert02]を選択し[OK]をクリックします
- ▶ ③ 何も記入せず[OK]をクリックします
- ▶ ④ [続ける]をクリックします
- ▶ ⑤ 認証成功すると「接続済み」と表示されます



- ▶ 4-5-4.iOS におけるEAP-TLS認証の実施
 - ▶ ① SSID「A@A_TLS」をクリックします
 - ▶ ② [モード]をクリックし、[EAP-TLS]を選択します
 - ▶ ③ [ID]をクリックし、[cert03]を選択します
 - ▶ ④ [チェックマーク]をクリックします
 - ▶ ⑤ [信頼]をクリックします
 - ▶ ⑥ 認証成功するとSSID名にチェックが表示されます



▶ 4-5-5.Android におけるEAP-TLS認証の実施

- ▶ ① SSID「A@A_TLS」をクリックします
- ▶ ②～⑦表に記載の値を入力/選択します
- ▶ ⑧ [接続]をクリックします
- ▶ ⑨ 認証成功すると「接続済み」と表示されます



A screenshot of the EAP-TLS configuration screen for the SSID 'A@A_TLS'. The screen shows various settings with red boxes and circled numbers 2 through 7 indicating the steps for configuration: 2. EAP方式 (EAP method) set to TLS; 3. CA証明書 (CA certificate) set to kokomoCA; 4. 証明書のオンライン検証 (Online certificate verification) set to 検証しない (Do not verify); 5. ドメイン (Domain) set to dnskokomo; 6. ユーザー証明書 (User certificate) set to kokomo; 7. ID set to cert04. At the bottom, the '接続' (Connect) button is highlighted with a red box and a circled number 8.

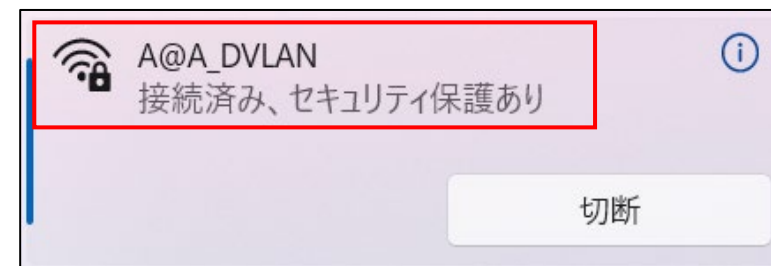
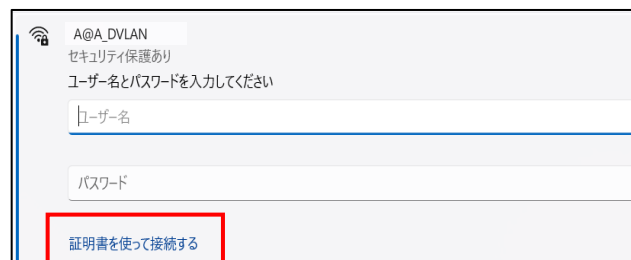
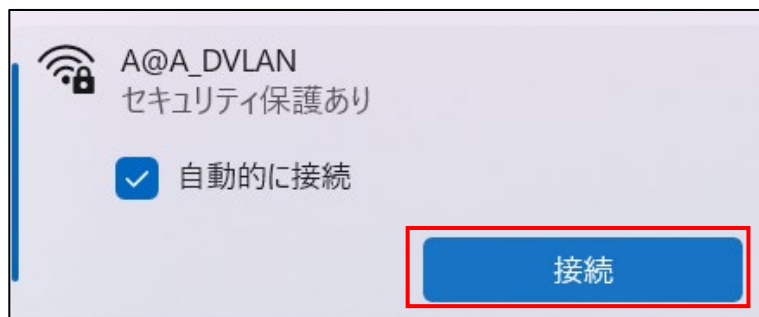
■ 認証設定

設定項目	設定値
②EAP方式	TLS
③CA証明書	kokomoCA
④オンライン認証ステータス	検証しない
⑤ドメイン	dnskokomo
⑥ユーザー証明書	kokomo
⑦ID	cert04



▶ 4-6-1.属性応答検証の実施

- ▶ 認証方式はEAP-TLS認証です。証明書アカウント(cert01~04)を利用し、各クライアント端末からSSID「A@A_DVLAN」へ接続し、認証成功後にVLAN10が割り当てられることを確認しました
- ▶ 属性応答によるVLAN割り当ては、認証方式に依存せず適用可能です
- ▶ 本ドキュメントの29~30スライドより、ディレクトリ[dir-a]配下に登録されているアカウントは認証後、VLAN10が割り当てられる設定となっています
- ▶ 代表例としてWindows端末(cert01)での認証結果を掲載しています



▶ 4-6-2.認証後の確認(Account@Adapter+ V7)①

- ▶ 検証時に返却属性や認証処理の詳細を確認するためのものです。通常運用で必須の設定ではありません
- ▶ Account@Adapter+ V7管理画面から[ログ参照]-[認証ログ]-[認証ログ詳細出力]タブをクリックします
- ▶ [RADIUS詳細ログ]を[出力する]に選択し、[対象アカウント]を[cert01]と入力し[登録]をクリックします

認証ログ 認証ログ詳細出力

ヘルプ

認証ログ詳細出力設定

RADIUS詳細ログ

☒ 出力する ☐ 出力しない

対象アカウント cert01

(半角英数記号空白 253文字以内)

登録

- ▶ [認証ログ]タブをクリックし、[検索]をクリックします

認証ログ 認証ログ詳細出力

ヘルプ

認証ログ

検索

priority ☒ debug ☒ info ☒ notice ☒ warn ☒ error ☒ crit ☒ alert ☒ emerg

フリーワード AND条件

OR条件

表示件数 新着順で最大 5000 件

検索

- ▶ 4-6-2.認証後の確認(Account@Adapter+ V7)②
 - ▶ 共通アトリビュートで設定した値がRADIUSクライアントに応答できていることが確認できます

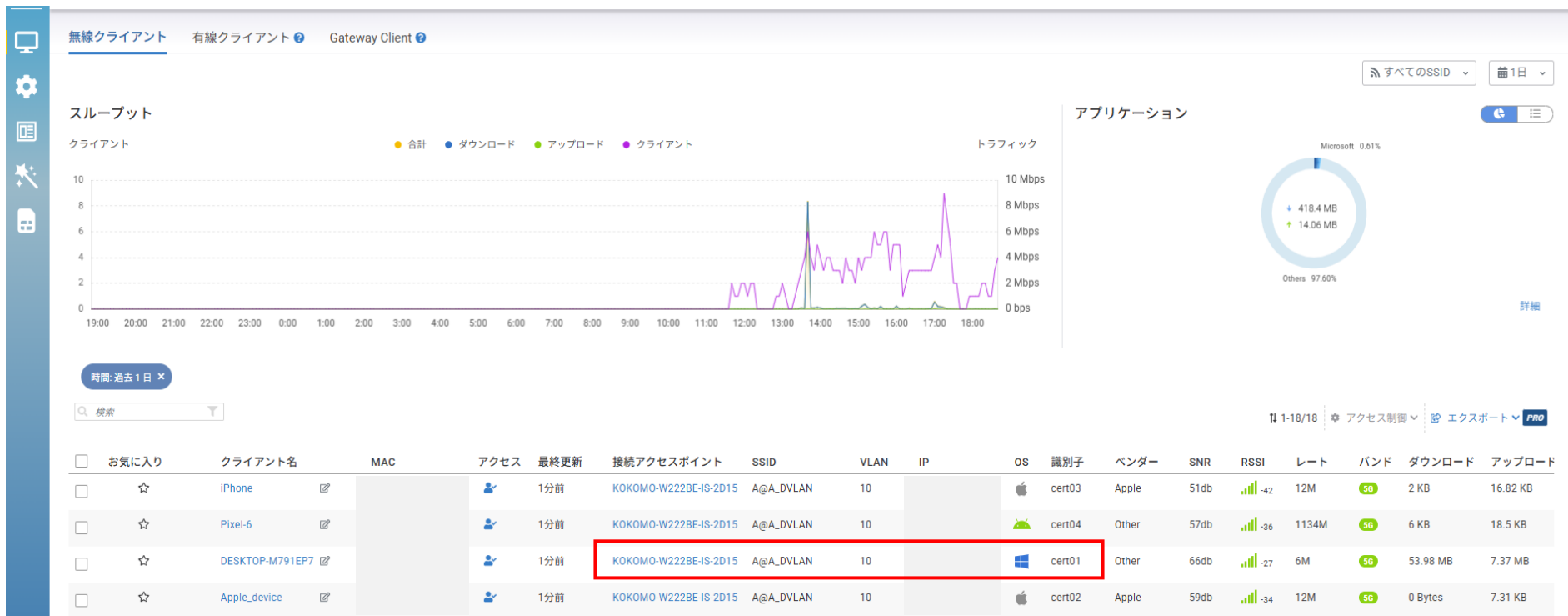
No.	ログ
1	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) User-Name = "cert01"
2	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) Message-Authenticator = 0x00000000000000000000000000000000
3	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) EAP-Message = 0x030a0004
4	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) MS-MPPE-Send-Key = 0x24792cedcf446b98a3976e7849b7723a384922a006587797cb74046db2e6512f
5	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) MS-MPPE-Recv-Key = 0x0a2ecb3f5b5eafad8b5d006706541abbe069aeb7551afe233735650c3b07d03f
6	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) Tunnel-Type := VLAN
7	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) Tunnel-Private-Group-Id := "10"
8	2026-04-10 18:21:49 local0 debug radiusd[46875]: (25) Tunnel-Medium-Type := IEEE-802

※VLAN-Idにあたる

※共通アトリビュート設定では[6]と設定

※共通アトリビュート設定では[13]と設定

- ▶ 4-6-3.認証後の確認(KOKOMOクラウド)
 - ▶ KOKOMOクラウドの管理画面から、管理[クライアント]に遷移します
 - ▶ RADIUSクライアント(KOKOMO-W222BE-IS-2D15)からもVLAN10を割り当てたことが確認できます



【補足】認証成功ログ/検証結果



Account@Adapter+ V7のWeb認証・MAC認証、PEAP・TLS認証のフォーマットになります。

・Web認証時のログ

Login OK: [user01] (from client kokomo-ap[192.168.102.5] port 0 cli 00-11-22-AA-BB-CC)

認証成功したユーザーアカウント

認証要求を送信したRADIUSクライアント

・MAC認証時のログ

Login OK: [00-11-22-AA-BB-CC] (from client kokomo-ap[192.168.102.5] port 0 cli 00-11-22-AA-BB-CC)

認証成功した端末(MAC)アカウント

認証要求を送信したRADIUSクライアント

RADIUSクライアントにCalling-station-id
が格納される場合は該当の端末のMACアドレ
スを格納(機器の仕様に依存します)

・PEAP/TLS認証時のログ

Login OK: [cert01] (from client kokomo-ap[192.168.102.5] port 0 cli 00-11-22-AA-BB-CC)

認証成功したユーザー/証明書アカウント

認証要求を送信したRADIUSクライアント

Login OK: [cert01] (from client kokomo-ap[192.168.102.5] port 0 cli 00-11-22-AA-BB-CC) via TLS Tunnel

TLS/PEAP認証の際に認証成功ログのほか、via TLS Tunnelと記載されたログが出力されます。