

NetAttest EPS

認証連携設定例

【連携機器】 ラッカスネットワークス ICX 7150 シリーズ

【Case】 IEEE802.1X EAP-PEAP(MS-CHAP V2)/

EAP-TLS/EAP-TLS+ダイナミック VLAN

Rev1.0



株式会社ソリトンシステムズ

はじめに

本書について

本書はオールインワン認証アプライアンス NetAttest EPS と、ラッカスネットワークス社製 L2/L3 スイッチ ICX 7150 シリーズの IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN 環境での接続について設定例を示したものです。設定例は管理者アカウントでログインし、設定可能な状態になっていることを前提として記述します。

アイコンについて

アイコン	説明
	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び ICX 7150-24P 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。

NetAttest は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

目次

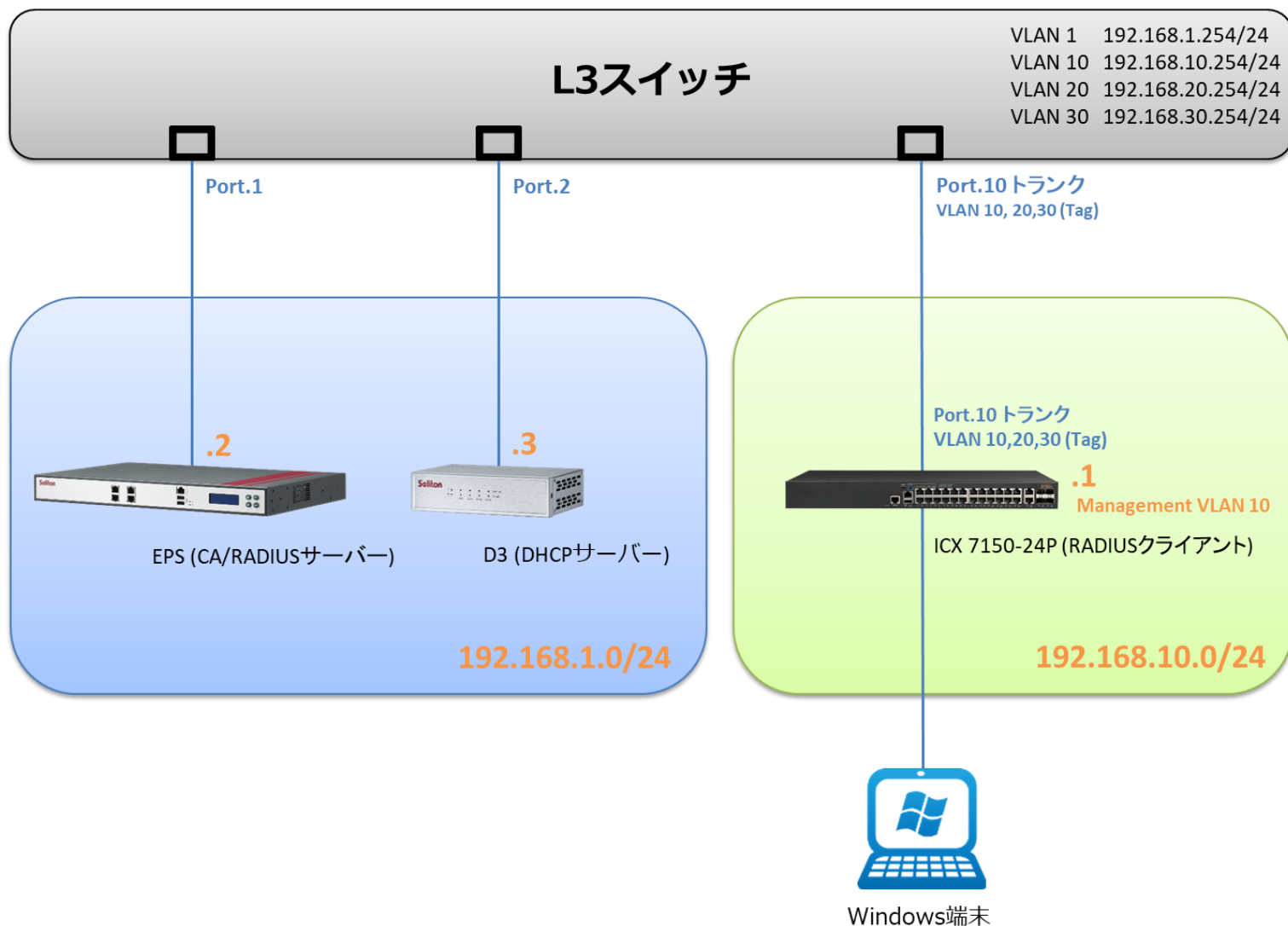
1. 構成	1
1-1 構成図	1
1-2 環境	2
1-2-1 機器	2
1-2-2 認証方式	2
1-2-3 ネットワーク設定	2
2. NetAttest EPS の設定	3
2-1 初期設定ウィザードの実行	3
2-2 システム初期設定ウィザードの実行	4
2-3 サービス初期設定ウィザードの実行	5
2-4 ユーザーの登録	6
2-5 ユーザーのリプライアイテムの設定	7
2-6 クライアント証明書の発行	8
3. ICX 7150 シリーズの設定	9
3-1 Ruckus ICX 7150 シリーズ 設定の流れ	9
3-2 Ruckus ICX 7150 スイッチ設定項目	9
3-2-1 Radius サーバーの登録	9
3-2-2 IEEE802.1x の設定	10
3-2-3 IronWare 08.0.90 以降のファームウェアご使用時の注意事項	11
4. Windows 10 のクライアント設定	12
4-1 EAP-PEAP 認証	12
4-2 EAP-TLS 認証	13
4-2-1 クライアント証明書のインポート	13
4-2-2 サプリカント設定	15
5. 動作確認結果	16
5-1 EAP-PEAP 認証	16
5-2 EAP-TLS 認証	17
5-3 EAP-TLS+ダイナミック VLAN 認証	18
付録 L3 スイッチ、Ruckus ICX 7150-24P の設定	19
ポート設定、DHCP リレー設定	19
Ruckus ICX 7150-24P の設定	20

1. 構成

1-1 構成図

以下の環境を構成します。

- ・ L3 スイッチには VLAN1、VLAN 10、VLAN 20、VLAN 30 の 4 つの VLAN を作成する
- ・ 接続するクライアント PC の IP アドレスは、NetAttest D3-SX15 の DHCP サーバーから払い出す
- ・ 各 VLAN の設計および用途は以下とする。
 - VLAN 1 : 192.168.1.0/24 (EPS、D3)
 - VLAN 10 : 192.168.10.0/24 (ICX 7150-24P、デフォルト VLAN/user01 用)
 - VLAN 20 : 192.168.20.0/24 (ダイナミック VLAN/user02 用)
 - VLAN 30 : 192.168.30.0/24 (ダイナミック VLAN/user03 用)



1-2 環境

1-2-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST05	ソリトンシステムズ	RADIUS/CA サーバー	4.10.4
ICX 7150-24P	ラッカスネットワークス	RADIUS クライアント (L2/L3 スイッチ)	ver. 08.0.80d
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブライアント
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.17

1-2-2 認証方式

IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST05	192.168.1.2/24	UDP 1812	secret
ICX 7150-24P	192.168.10.1/24		secret
Client PC	DHCP	-	-

2. NetAttest EPS の設定

2-1 初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「<http://192.168.2.1:2181/>」にアクセスしてください。

下記のような流れでセットアップを行います。

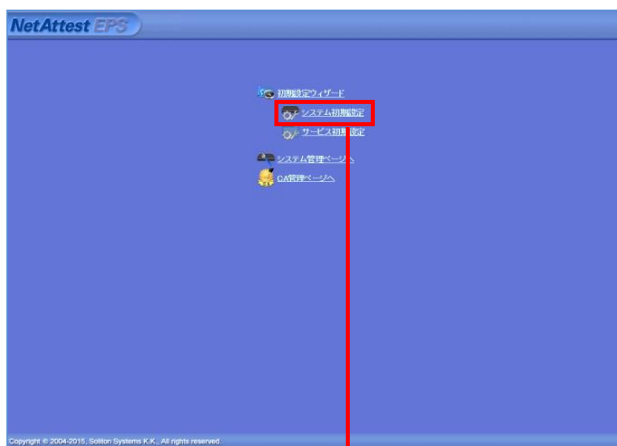
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

2-2 システム初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

その後、システム初期設定ウィザードを使用し、以下の項目を設定します。

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- メインネームサーバーの設定



初期設定ウィザード - 設定項目の確認

設定内容を確認して下さい。
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

ネットワーク時刻	
NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効

EPSライセンス	
最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

戻る 再起動

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

項目	値
優先順位	EAP 認証タイプ
1	TLS
2	PEAP

項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.10.1
シークレット	secret

2-4 ユーザーの登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

[ユーザー] - [ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

The screenshot shows the NetAttest EPS user management interface. The 'ユーザー一覧' (User List) table contains one entry: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An arrow points to the 'ユーザー設定' (User Settings) form, which is pre-filled with 'user01' for the name and ID, and 'password' for the password. The 'OK' button is also highlighted with a red box.

項目	値
姓	user01 user02 user03
ユーザーID	user01 user02 user03
パスワード	password password password

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test		発行	変更 削除
user01	user01		発行	変更 削除

2-5 ユーザーのリプライアイテムの設定

ダイナミック VLAN で接続先を制御したいユーザーにリプライアイテムを設定します。
対象のユーザーの「変更」ボタンよりユーザー設定画面に進み、「リプライアイテム」タブにて「VLAN ID」と「タグ」を指定します。

NetAttest EPS 管理画面の「ユーザー一覧」画面。ユーザーリストの「変更」ボタンが赤い枠で囲われ、赤い矢印が下の画面へと指している。

名前	ユーザーID	最終認証成功日時	ロック状態	証明書	タスク
test user	test			証明書	変更 削除
user01	user01			発行	変更 削除
user02	user02			発行	変更 削除
user03	user03			発行	変更 削除

NetAttest EPS 管理画面の「ユーザー設定」画面。編集対象が user02。タブは「リプライアイテム」に切り替えられている。標準のリプライアイテム設定で、VLAN ID が 20、タグが 0 と設定されている。

項目	値		
ユーザーID	user01	user02	user03
VLAN ID	-	20	30
タグ	-	0	0

2-6 クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

[ユーザー] - [ユーザー一覧]から、該当するユーザーのクライアント証明書を発行します。

(クライアント証明書は、user01.p12 という名前で保存)

項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の . . .	チェック有

3. ICX 7150 シリーズの設定

3-1 Ruckus ICX 7150 シリーズ 設定の流れ

ラッカスネットワークス社製有線 LAN スイッチ ICX 7150 シリーズを設定するためには CLI を用います。本書では代表して ICX 7150-24P を使用し、CLI を用いて各種設定を実施する方法を紹介します。

3-2 Ruckus ICX 7150-24P スイッチ設定項目

3-2-1 RADIUS サーバーの登録

ICX 7150-24P に VLAN 10、VLAN 10 の IP アドレスおよびデフォルトゲートウェイを設定し、RADIUS サーバーとして NetAttest EPS を登録します。

[入力値]

```
ICX7150-24P Router>enable
```

```
ICX7150-24P Router#configure terminal
```

```
ICX7150-24P Router(config)#vlan 10
```

```
ICX7150-24P Router(config-vlan-10)#tagged ethernet 1/1/12
```

```
ICX7150-24P Router(config-vlan-10)#router-interface ve 10
```

```
ICX7150-24P Router(config-vlan-10)#int ve 10
```

```
ICX7150-24P Router(config-vif-10)#ip address 192.168.10.1/24
```

```
ICX7150-24P Router(config-vif-10)#exit
```

```
ICX7150-24P Router(config)# ip route 0.0.0.0/0 192.168.10.254
```

```
ICX7150-24P Router(config)#radius-server host 192.168.1.2 auth-port 1812 acct-port 1813 default  
key secret dot1x mac-auth no-login
```

VLAN 20、VLAN 30 についても同様に VLAN のみを設定します。

3-2-2 IEEE802.1x の設定

Flex Authentication を有効にして IEEE802.1x 認証の設定および eth 1/1/1 から eth 1/1/6 ま
でを認証ポートとして設定します。

[入力値]

```
ICX7150-24P Router(config)# aaa authentication dot1x default radius
```

```
ICX7150-24P Router(config)# authentication
```

```
ICX7150-24P Router(config-authen)# auth-default-vlan 10
```

```
ICX7150-24P Router(config-authen)# dot1x enable
```

```
ICX7150-24P Router(config-authen)# dot1x enable ethernet 1/1/1 to 1/1/6
```

```
ICX7150-24P Router(config-authen)# dot1x port-control auto e 1/1/1 to 1/1/6
```

設定終了後に、コンフィグ(Running-Configuration)を Startup-Configuration に保存します。

[入力値]

```
ICX7150-24P Router(config)# write memory
```

Ruckus ICX 7150-24P の設定については、巻末の(付録)をご参照下さい。

3-2-3 IronWare 08.0.90 以降のファームウェアご使用時の注意事項

Ruckus IronWare 08.0.90 以降のファームウェアでは、デフォルトでは以下のユーザー名、パスワードが設定されています。以下のユーザーでログイン後、パスワードの再設定が必要となります。

- ユーザー名 : super
- パスワード : sp-admin

[IronWare 08.0.90 以降のログイン時画面]

Press Enter key to login

User Access Verification

Please Enter Login Name: super

Please Enter Password:

← デフォルトパスワード "sp-admin"設定

User login successful.

User 'super' login successful with default password. Please change the password.

Enter the new password for user super :

← 新規パスワード設定

Enter the reconfirm password for user super:

← パスワード再確認

Password modified successfully for user super

Authentication is enabled in the device for Console/WEB/SSH.

ICX7150-24P Router>enable

ICX7150-24P Router#

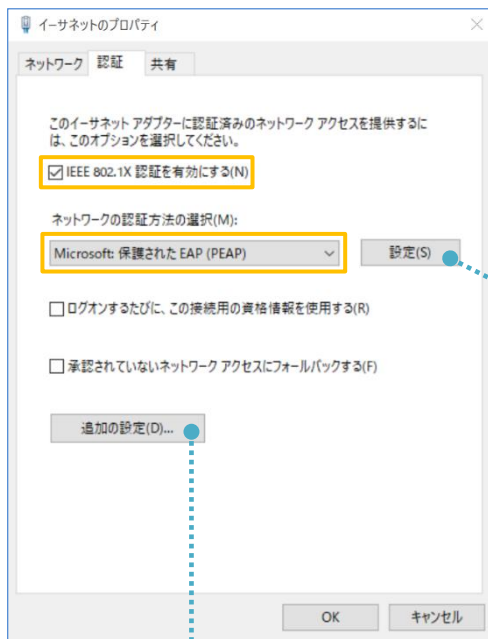
4. Windows 10 のクライアント設定

4-1 EAP-PEAP 認証

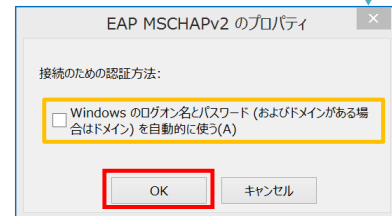
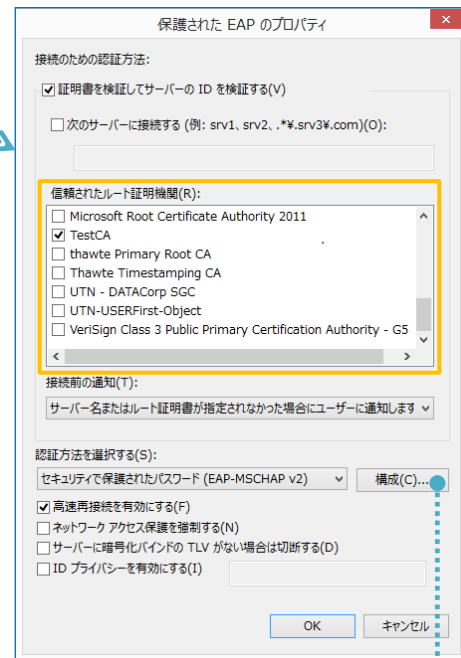
Windows 標準サブリカントで PEAP の設定を行います。

※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認ください。

[イーサネットのプロパティ] の [認証] タブから以下の設定を行います。



項目	値
IEEE 802.1X 認証を・・・	有効
ネットワークの認証・・・	Microsoft: 保護された EAP



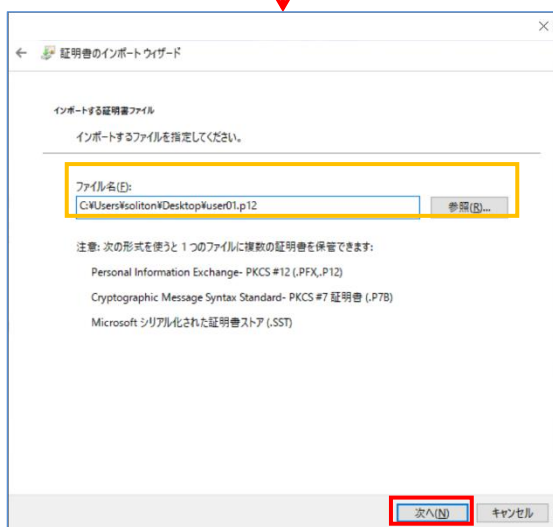
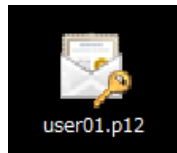
項目	値
認証モードを指定する	ユーザー認証

項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA
- Windows のログオン名と・・・	Off

4-2 EAP-TLS 認証

4-2-1 クライアント証明書のインポート

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01.p12) をダブルクリックすると、証明書インポートウィザードが実行されます。



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(O):

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。

すべての拡張プロパティをコピーする(A)

次へ(N) > キャンセル

【パスワード】

NetAttest EPS で証明書を発行した際に
設定したパスワードを入力

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(L)
 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

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:

選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Desktop\User01.p12

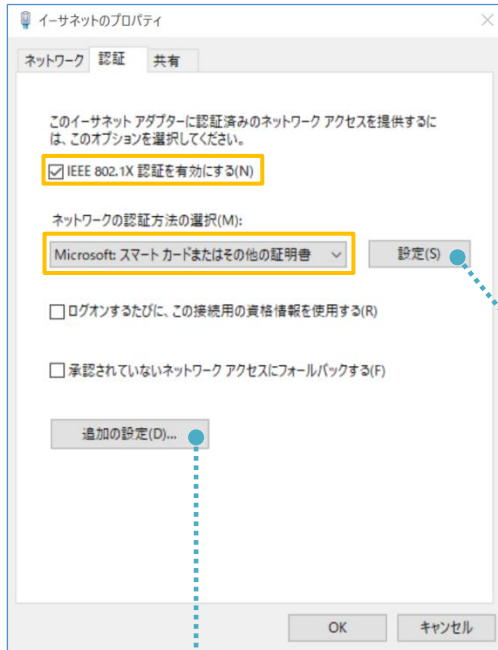
完了(F) キャンセル

4-2-2 サプリカント設定

Windows 標準サプリカントで TLS の設定を行います。

※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認下さい。

[イーサネットのプロパティ] の [認証] タブから以下の設定を行います。



項目	値
IEEE 802.1X 認証を有効にする	有効
ネットワークの認証方式の選択	Microsoft:スマートカードまたはその他の証明書



項目	値
接続のための認証方法	
- このコンピュータの証明書を使う	On
- 単純な証明書の選択を使う (推奨)	On
証明書を検証してサーバーの ID を検証する	On
信頼されたルート証明機関	TestCA

項目	値
認証モードを指定する	ユーザー認証

5. 動作確認結果

5-1 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)

EAP-PEAP 認証が成功した場合の ICX 7150-24P の “show authentication sessions all” による認証結果の表示例。ICX 7150-24P に設定された “auth-default-vlan 10” により、認証後 VLAN 10 が割り当てられます。

ICX7150-24P Router# show authentication sessions all

```
-----  
Port   MAC           IP(v4/v6)  User  VLAN  Auth  Auth  ACL  Session  Age  PAE  
      Addr           Addr      Name           Method  State           Time           State  
-----  
1/1/1  cc30.8032.8baf  N/A       user01  10    802.1X  Permit  None  12      Ena  AUTHENTICATED
```

5-2 EAP-TLS 認証

EAP-TLS 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)

EAP-TLS 認証が成功した場合の ICX 7150-24P の "show authentication sessions all"による認証結果の表示例。

```
ICX7150-24P Router# show authentication sessions all
```

```
-----  
Port  MAC          IP(v4/v6)  User  VLAN  Auth  Auth  ACL  Session  Age  PAE  
      Addr          Addr      Name  Method State  Time  State  
-----  
1/1/1  cc30.8032.8baf  N/A       user01  10    802.1X  Permit  None  12     Ena  AUTHENTICATED
```

5-3 EAP-TLS+ダイナミック VLAN 認証

■ EAP-TLS 認証+ダイナミック VLAN(VLAN 20)が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user02] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)

EAP-TLS 認証が成功した場合の ICX 7150-24P の "show authentication sessions all"による認証結果および VLAN 20 割当状態の表示例

```
ICX7150-24P Router# show authentication sessions all
```

```
-----
Port   MAC           IP(v4/v6)  User   VLAN  Auth   Auth   ACL   Session  Age  PAE
      Addr           Addr      Name           Method State           Time           State
-----
1/1/1  cc30.8032.8baf N/A        user02  20    802.1X Permit None    8      Ena   AUTHENTICATED
```

■ EAP-TLS 認証+ダイナミック VLAN(VLAN 30)が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	Login OK: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)

EAP-TLS 認証が成功した場合の ICX 7150-24P の "show authentication sessions all"による認証結果および VLAN 30 割当状態の表示例

```
ICX7150-24P Router# show authentication sessions all
```

```
-----
Port   MAC           IP(v4/v6)  User   VLAN  Auth   Auth   ACL   Session  Age  PAE
      Addr           Addr      Name           Method State           Time           State
-----
1/1/1  cc30.8032.8baf N/A        user03  30    802.1X Permit None    6      Ena   AUTHENTICATED
```

付録 L3 スイッチ、Ruckus ICX 7150-24P の設定

ポート設定、DHCP リレー設定

下記のようにポートの設定をします。

ポート	VLAN ID	ネットワーク	スイッチ IP アドレス	備考
1-5	1	192.168.1.0/255.255.255.0	192.168.1.254	
6-9	10	192.168.10.0/255.255.255.0	192.168.10.254	
10	10,20,30			VLAN 10,20,30 の トランクポート
11-14	20	192.168.20.0/255.255.255.0	192.168.20.254	
17-20	30	192.168.30.0/255.255.255.0	192.168.30.254	

DHCP リレー設定にて、「192.168.1.3」を指定します。

Ruckus ICX 7150-24P の設定

Ruckus ICX 7150-24P の設定完了後の設定イメージを以下に示します。RADIUS アカウンティングを有効にし、eth 1/1/1 から eth 1/1/6 まで 802.1x 認証の設定をします。RADIUS サーバー間との共有シークレット等は、暗号化されて表示されます。

なお、eth 1/1/7 から eth 1/1/12 までには MAC アドレス認証の設定を行っています。

```
ICX7150-24P Router#show running-config
Current configuration:
!
ver 08.0.80dT213
!
stack unit 1
module 1 icx7150-24p-poe-port-management-module
module 2 icx7150-2-copper-port-2g-module
module 3 icx7150-4-sfp-plus-port-40g-module
!
~略~
!
vlan 1 name DEFAULT-VLAN by port
no untagged ethe 1/1/1 to 1/1/12
!
vlan 10 by port
tagged ethe 1/1/24
router-interface ve 10
!
vlan 20 by port
tagged ethe 1/1/24
!
vlan 30 by port
tagged ethe 1/1/24
!
~略~
!
```



```
authentication
  auth-default-vlan 10
  max-sessions 1024
  re-authentication
  dot1x enable
  dot1x enable ethe 1/1/1 to 1/1/6
  dot1x port-control auto ethe 1/1/1 to 1/1/6
  mac-authentication enable
  mac-authentication enable ethe 1/1/7 to 1/1/12
!
!
aaa authentication dot1x default radius
aaa accounting dot1x default start-stop radius
aaa accounting mac-auth default start-stop radius
ip route 0.0.0.0/0 192.168.10.254
!
radius-server host 192.168.1.2 auth-port 1812 acct-port 1813 default key 2 $LW5kVW5v dot1x
mac-auth no-login
!
~略~
!
interface ve 10
  ip address 192.168.10.1 255.255.255.0
!
~略~
!
end
```

