Web 認証拡張機能簡易ドキュメント

センチュリー・システムズ(株)

1.　Web 認証機能(キャプティブポータル機能)について

Web 認証はパケットフィルタの一種で、認証を通ったユーザの IPv4 アドレスを送信元/宛先に持つ転送のみを通過させる機能です。Web 認証機能によるパケットの判定は、ユーザが設定した forward(in/out)フィルタ通過後に評価されます。

2.　Web 認証コマンド

2-1. 移行コマンド

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#web-authenticate
(config-webauth)#
```

2-2. 認証方式

対応している認証方式は、HTTP Basic 認証、および Post 認証です。

○ authenticate basic

＜説　　明＞ Basice 認証、または POST 認証を行うかどうかを設定します。

＜書　　式＞ authenticate basic (|redirect)
　　authenticate post-ext-html (|redirect)
　　authenticate post-ext-xml (|redirect)

＜　No　＞ no authenticate

＜初 期 値＞ no authenticate

＜備　　考＞

・redirect を指定した場合、Web 認証後に URL 転送を行うことができます。転送先の URL は、redirect-url コマンドで指定してください。

・Web 認証を有効にする場合は、HTTP サーバを起動してください。（global mode で、http-server enable を設定します。）

・post-ext-html または post-ext-xml を指定すると、外部 WEB サーバ連携機能（post でのアクセス）が有効になります。

2-3. 認証 URL

Basic 認証の URL は「http://本装置の IP address/login.cgi」です。たとえば、LAN 側 IP アドレスが 192.168.0.254 の場合、http://192.168.0.254/login.cgi にアクセスすると、Web 認証ダイアログが表示されます。

2-4. 強制認証

通常、外部に接続したいユーザは、認証 URL へのアクセスが必要となります。強制認証機能では、TCP80 番への接続を監視し、未認証のユーザからこの接続があった場合に、強制的に Web 認証を行います。Default では本機能は無効です。

○ monitor

＜書　　式＞ monitor port 80 (|redirect)
　　monitor port 80 443 (|redirect) （https enable の設定が必要です）

＜　No　＞ no monitor port

＜初 期 値＞ no monitor port

＜備　　考＞

・authenticate basic + monitor port 80 443
　未認証の PC から外部 Web に http/https アクセスすると、Web 認証ダイアログが表示されます。

・authenticate basic + monitor port 80 443 redirect
　未認証の PC から外部 Web に http/https アクセスすると、Web 認証後に redirect-url に転送されます。

・no authenticate + monitor port 80 443 redirect
　未認証の PC から外部 Web に http/https アクセスすると、Web 認証なしで redirect-url へ転送されます。

2-5. URL 転送

Web 認証後、任意の URL へ転送させることができます。Web 認証は行わず、外部へのアクセスがあった時に指定した URL へリダイレクトさせるように動作させることも可能です。

○ redirect-url

＜説　　明＞ 転送先の URL を指定します。

＜書　　式＞ redirect-url RedirectURL (cf. http://www.centurysys.co.jp)

＜　No　＞ no redirect-url

2-6. 接続許可時間

Web 認証後にユーザが通信可能な時間を、以下の 3 つから選択することができます。

○ close idle-timeout

＜説　　明＞ 許可されたユーザからの無通信状態が一定時間経過すると接続が遮断されます。
　　タイムアウトは 60-2592000 秒の間で任意の値を設定することができます。
　　Default は 1800 秒です。

＜書　　式＞ close idle-timeout <60-2592000>

＜　No　＞ no close

＜初 期 値＞ close idle-timeout 1800

○ close session-timeout

＜説　　明＞ 認証で許可された通信を強制的に切断するまでの時間を設定します。認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。
　　タイムアウトは 60-2592000 秒の間で任意の値を設定することができます。
　　Default は 1800 秒です。

＜書　　式＞ close session-timeout <60-2592000>

＜　No　＞ no close

＜初 期 値＞ close idle-timeout 1800

○ close idle-timeout XXXX session-timeout XXXX

＜説　　明＞ 無通信状態が一定時間経過するまたは認証で許可された通信を強制的に切断するまでの時間を

設定します。
タイムアウトは 60-2592000 秒の間で任意の値を設定することができます。
session-timeout は idle-timeout より大きい値を設定する必要があります。
＜書　　式＞ close session-timeout <60-2592000> session-timeout <60-2592000>
＜　No　＞ no close

○ close browser-close
＜説　　明＞ 認証を受けた Web ブラウザのウィンドウを閉じるまで接続が有効です。
Web 認証時の HTML により、ブラウザから 60 秒毎にリフレッシュが行われます。
リフレッシュがなくなると接続を遮断します。
＜書　　式＞ close browser-close
＜　No　＞ no close
＜初　期　値＞ close idle-timeout 1800

2-7. アカウント管理
Basic 認証におけるユーザ名、パスワードを本装置上で管理/ 認証する方法(ローカル認証)と、外部の RADIUS サーバに対して本装置から認証する方法(RADIUS 認証)があります。また、RADIUS 認証に失敗した場合にローカル認証を行うこともできます。
＜書　　式＞ account authenticate (local|radius|radius-and-local)
＜　No　＞ no account authenticate
＜初　期　値＞ account authenticate local

2-8. ローカル認証
ローカル認証用のユーザ名、パスワードを最大 64 組まで設定することができます。
＜書　　式＞ account username USERNAME password (|hidden) PASSWORD
＜　No　＞ no account username USERNAME

2-9. RADUIS 認証
RADIUS 認証は PAP 認証によって行われます。RADIUS サーバへの認証要求は、タイムアウトが 5 秒で、最大 3 回までリトライします。
○ RADUIS サーバ設定
アカウント認証を行う RADIUS サーバの IP アドレス、UDP ポート番号、秘密鍵(secret)を設定することができます。UDP ポート番号の Default は 1645 番です。また RADIUS サーバは 2 つまで設定することができます。
＜書　　式＞
radius A.B.C.D password (|hidden) PASSWORD (|auth-port <1645|1812|<1024-65535>)
radius A.B.C.D auth-port (1645|1812|<1024-65535>)
＜　No　＞ no radius A.B.C.D (設定を削除します)
no radius A.B.C.D auth-port (auth-port のみを初期値に戻します)
＜初　期　値＞ radius A.B.C.D auth-port 1645

○ Attribute 設定
RADIUS サーバに通知するアトリビュートのうち、以下のアトリビュートについて任意の値を設定することができます。
＜書　　式＞ radius attribute nas-ip-address A.B.C.D
radius attribute nas-identifier WORD

＜　　No　　＞ no radius attribute (nas-ip-address|nas-identifier)

＜備　　考＞ RADIUS 認証を使用する場合は、どちらかのアトリビュートを設定する必要があります。

NAS-IP-Address: 通常は本装置の IP アドレスを設定します。

NAS-Identifier: 任意の文字列を設定します。半角英数字が使用できます。

○Idle timeout で使用する Attribute の指定

接続許可時間に idle timeout を指定している場合は、RADIUS サーバからの応答アトリビュートの値をタイムアウトとして使うことができます。

＜書　　式＞ radius idle-timeout attribute

(ascend-idle-limit|ascend-idle-limit-vsa|idle-limit)

＜　　No　　＞ no radius idle-timeout attribute

＜備　　考＞

・ascend-idle-limit Ascend-Idle-Limit(Attribute Type=244)

・ascend-idle-limit-vsa Ascend-Idle-Limit(Attribute Type=244、VSA Type=26、Vendor-ID=529)

・idle-limit Idle-Timeout (Attribute Type=28)

○ Session timeout で使用する Attribute の指定

接続許可時間に session timeout を指定している場合は、RADIUS サーバからの応答アトリビュートの値をタイムアウトとして使うことができます。以下のアトリビュートから選択してください。

＜書　　式＞ radius session-timeout attribute

(ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)

＜　　No　　＞ no radius session-timeout attribute

＜備　　考＞

・session-timeout Session-Timeout (Attribute Type=27)

・ascend-maximum-time Ascend-Maximum-Time(Attribute Type=194)

・ascend-maximum-time-vsa Ascend-Maximum-Time(Attribute Type=194, VSA Type=26, Vendor-ID=529)

○ 全ての radius 設定を一括削除

全ての radius 設定を一括削除することができます。

＜書　　式＞ no radius

2-10.　MAC アクセスリスト

Web 認証機能を有効にすると、外部との通信には認証が必要となりますが、mac access-list で指定した MAC アドレスを持つ端末については、認証を必要とせずに通信を許可または拒否することができます。

＜書　　式＞ mac access-list (permit|deny) HH:HH:HH:HH:HH:HH (|IFNAME)

＜　　No　　＞ no mac access-list (permit|deny) HH:HH:HH:HH:HH:HH

2-11.　Web 認証フィルタ

Web 認証フィルタを設定すると、ある特定のホストやネットワーク、インタフェースについて Web 認証せずに通信が可能となります。Web 認証フィルタの設定条件については、global mode の ip web-auth access-list を参照してください。Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。

2-12.　認証ログの出力

認証ログ（login success ログ）をシスログに出力します。

＜書　　式＞ log enable

＜　No　＞ no log enable

＜初　期　値＞ no log enable

＜備　　考＞

・有効（log enable）時、TCP80 監視による認証ログ（login success ログ）をシスログに出力します。

・有効（log enable）時、login.cgi 接続による認証ログ（login success ログ）をシスログに出力します。

2-13.　証明書

○ cert certificate

＜説　　明＞ 証明書を設定します。

＜書　　式＞ cert certificate NAME WORD (|source A.B.C.D|X:X::X:X)

＜　No　＞ no cert certificate NAME

＜備　　考＞ 証明書は、以下のように設定します。

cert certificate disk0:/certs/newcert.pem

cert certificate test ssh://user@192.168.0.10/certs/newcert.pem

○ cert chain-certificate

＜説　　明＞ 中間証明書を設定します。

＜書　　式＞ cert chain-certificate NAME WORD (|source A.B.C.D|X:X::X:X)

＜　No　＞ no cert chain-certificate NAME

＜備　　考＞ 中間証明書は、以下のように設定します。

cert chain-certificate test disk0:/certs/subcert.pem

○ cert private-key key

＜説　　明＞ 本装置の秘密鍵を設定します。

＜書　　式＞ cert private-key NAME key WORD (|source A.B.C.D|X:X::X:X)

＜　No　＞ no cert private-key NAME key

＜備　　考＞ 秘密鍵は、以下のように設定します。

cert private-key test key ssh://user@192.168.0.10/certs/newkey.pem

○ cert private-key key

＜説　　明＞ パスフレーズを設定します。

＜書　　式＞ cert private-key NAME password (|hidden) WORD

＜　No　＞ no cert private-key NAME password

＜備　　考＞ パスフレーズは、以下のように設定します。

cert private-key test password abcdefgh

2-14.　その他

○ https enable

＜説　　明＞ https 動作を有効にします。

＜書　　式＞ https enable

＜　No　＞ no https enable

＜初　期　値＞ no https enable

＜備　　考＞

・https 動作を有効にするには証明書の設定が必要です（証明書設定が無い場合、初期証明書を使用します）。設定できる証明書は、中間証明書、証明書、秘密鍵です。

・証明書の設定は、CLI から以下のような形式で設定します。

cert chain-certificate test ssh://user@192.168.0.1/certs/subcert.pem

cert certificate test ssh://user@192.168.0.1/certs3/newcert.pem

cert private-key test key ssh://user@192.168.0.1/certs3/newkey.pem

cert private-key test password abcdefgh

・https 有効時には証明書関連の設定が正しくない場合、restart http-server しても、HTTP サービスが起動しない場合があります（show service で確認するようにしてください）。

・monitor port 80 443 設定で、port 80 と 443 の監視を有効にすることができます。https enable 設定時は片側のみ（80 のみ、443 のみ）の監視設定は出来ません。

○ access-path

＜説　　明＞ access-path を指定します。

＜書　　式＞ access-path WORD

＜　No　＞ no access-path

＜備　　考＞

・access-path test と設定した場合、http://A.B.C.D/test へのアクセスは、http://A.B.C.D/login.cgi へのアクセスと同等の動作になります。

・設定がディレクトリ指定（例：access-path test/）の場合、そのディレクトリ以降は任意の文字列として処理します。http://A.B.C.D/test/も、http://A.B.C.D/test/abcd も、login.cgi へのアクセスとして動作します。

・login.cgi 自体へのパスを無効にすることはできません。

・最大設定数は 1 個です。最大文字数は、128 文字です。

○ wispr-success-url

＜説　　明＞ 指定 URL への認証前アクセスに対して、HTTP 200 OK を返します。

＜書　　式＞ wispr-success-url URL

＜　No　＞ no wispr-success-url URL

＜備　　考＞

・設定がディレクトリ指定（設定値の終わりが'/'）の場合、そのディレクトリ以降は任意の文字列として処理します。

・最大設定数は 16 個です。最大文字数は、250 文字です。

3. Web 認証拡張コマンド

web-authenticate mode で、authenticate post-ext-html を設定することで、外部 WEB サーバ連携機能（post でのアクセス）が有効になります。

3-1. 移行コマンド

#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

(config)#web-auth-extension <1-16>

(config-webauth-ext)#

3-2. ネットワーク設定

○ network

＜説　　明＞ post 認証を行う端末のネットワークアドレス範囲を指定します。
＜書　　式＞ network A.B.C.D/M
＜　No　＞ no network
＜備　　考＞
・外部サーバ連携機能の有効時は、端末からのアクセスに対して、web-auth-extension <1-16> の番号順にネットワーク設定(network A.B.C.D/M)を検索し、該当する web-auth-extension の設定で動作します。
・該当するネットワーク設定が存在しない場合、認証エラーのリザルト画面が表示されます。
・該当するネットワーク設定が複数存在する場合は、web-auth-extension の番号の小さい設定で動作します。

3-3. RADUIS 認証

○ account authenticate
＜説　　明＞ RADIUS 認証を行う場合に設定します。
＜書　　式＞ account authenticate (none|radius|disable)
＜　No　＞ no account authenticate
＜初　期　値＞ account authenticate none
＜備　　考＞
・radius を指定すると、post アクセスで渡されるユーザ ID とパスワードのデータを元に、該当ネットワークの RADIUS サーバにアクセスして認証を行います。
・none を指定すると、認証を行いません（認証 OK として動作します）。また POST データ（ユーザ ID、パスワード）に関するチェックも行いません。
・web-authenticate mode で、log enable を設定すると、認証時のログをシスログに出力します。

○ radius server
＜説　　明＞ RADIUS サーバの設定を行います。
＜書　　式＞
radius A.B.C.D password (|hidden) PASSWORD)　(|auth-port <1645|1812|<1024-65535>)
radius A.B.C.D auth-port (1645|1812|<1024-65535>)
＜　No　＞ no radius A.B.C.D （RADIUS サーバを削除します）
no radius A.B.C.D auth-port（認証ポートの設定を初期値に戻します）
＜初　期　値＞ radius A.B.C.D auth-port 1645
＜備　　考＞
・RADIUS サーバは、2 つまで設定することができます。
・RADIUS サーバへのアクセスタイムアウトは 5 秒で、リトライは 2 回行います（タイムアウト値およびリトライ回数を変更することはできません）。

○ radius attribute
＜説　　明＞ 送信アトリビュートの設定を行います。
＜書　　式＞ radius attribute nas-identifier WORD
radius attribute nas-ip-address A.B.C.D
radius attribute chap-password
＜　No　＞ no radius-attribute
＜備　　考＞
・RADIUS サーバへの送信アトリビュートは、上記アトリビュート（NAS-IP-Address, NAS-Identifier）および User-Name, User-Password, Login-IP-Host(端末の IP アドレス)、Message-Authenticator です。
・chap-password を設定した場合は、User-Password の代わりに、CHAP-Password を使用します。

○ radius idle-timeout attribute
＜説　　明＞ 受信時に適応するタイムアウト値のアトリビュート指定を行います。
＜書　　式＞ radius idle-timeout attribute
　　(ascend-idle-limit|ascend-idle-limit-vsa|idle-limit)
＜　No　＞ no radius idle-timeout attribute
＜備　　考＞ web-authenticate mode で、close 設定を行ってください。

○ radius idle-timeout attribute
＜説　　明＞ session-timeout 値に使用するアトリビュートの設定を行います。
＜書　　式＞ radius session-timeout attribute
　　(ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)
＜　No　＞ no radius session-timeout attribute

○ no radius
＜説　　明＞ すべての RADIUS 設定を削除します。
＜書　　式＞ no radius

3-4. 受信オプション
○ receive-option idle-timeout
＜説　　明＞ XML の idle_timeout キーを指定します。
＜書　　式＞ receive-option idle-timeout
＜　No　＞ no receive-option idle-timeout

○ receive-option session-timeout
＜説　　明＞ XML の session_timeout キーを指定します。
＜書　　式＞ receive-option session-timeout
＜　No　＞ no receive-option session-timeout

○ receive-option permit
＜説　　明＞ XML の source_address キーを設定します。
＜書　　式＞ receive-option permit source A.B.C.D/M
＜　No　＞ no receive-option permit source

○ receive-option password-key
＜説　　明＞ XML の password_key キーを設定します。
＜書　　式＞ receive-option password-key (|hidden) PASSWORD)
＜　No　＞ no receive-option idle-timeout

3-5. その他
○ access-url
＜説　　明＞ 指定ネットワーク内に対して、転送先 URL を指定します。
＜書　　式＞ access-url URL
＜　No　＞ no access-url
＜初　期　値＞ no access-url

＜備　　考＞

・URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。

・access-url は、Web 認証が未認証の端末でもアクセス可能な URL を指定します。

・access-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

○ redirect-url

＜説　　明＞ 指定ネットワーク内に対して、認証 OK の場合の転送先 URL を指定します。

＜書　　式＞ redirect-url URL

＜　No　＞ no redirect-url

＜初 期 値＞ no redirect-url

＜備　　考＞

・URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。

・redirect-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

○ failure-url

＜説　　明＞ 指定ネットワーク内に対して、認証エラーの場合の転送先 URL を指定します。

＜書　　式＞ failure-url URL

＜　No　＞ no failure-url

＜初 期 値＞ no failure-url

＜備　　考＞

・URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。

・failure-url は、Web 認証が未認証の端末でもアクセス可能な URL を指定します。

・failure-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

4. 表示および実行コマンド

4-1. 情報表示

○ show web-authenticate timer

＜説　　明＞ Web 認証で認証した端末のタイマー情報を表示します

＜書　　式＞ show web-authenticate timer

○ show web-authenticate cert

＜説　　明＞ Web 認証で設定した証明書ファイルを表示します。

＜書　　式＞ show web-authenticate cert (chain-certificate|certificate|private-key)

4-2. 実行

○ clear web-authenticate timer

＜説　　明＞ Web 認証で認証した端末を削除します。

＜書　　式＞ clear web-authenticate timer (A.B.C.D|all)

5. Web 認証機能設定例

Web 認証機能の設定例は弊社ホームページで公開しております。

https://www.centurysys.co.jp/futurenet-tech-wiki/setting/fnw_nf_authentication/