

<u>2025年4月1日</u> OP24-DE-702-01



RADIUS GUARD S V7

簡単スタートアップガイド (vol.2)

SCSK Corporation

修正履歴

改版番号	日付	区分	内容
第1版	2024/6/18	新規作成	初版作成
第2版	2025/4/1	変更	部署名の変更

目次

1	アカウント自動棚卸(自動削除)	5
	1-1 自動削除の設定	6
2	外部認証局登録とサーバー証明書	8
	2-1 外部認証局の登録	8
	2-2 外部認証サーバー証明書の登録	9
	2-2-1 CSR 情報の発行	9
	2-2-2 サーバー証明書の登録	. 11
	2-3 RADIUS サーバーの設定	. 12
	2-4 外部サーバー証明書発行	. 12
3	外部 Active Directory を参照した認証	.13
	3-1 事前設定	.13
	3-2 外部 AD サーバーの登録	. 14
	3-2-1 Active Directory ユーザーアカウントの DN 形式を確認する	. 17
	3-3 AD サーバーの接続確認	. 17
	3-4 AD サーバー側の確認	. 18
	3-5 複数の AD 接続について	. 19
4	冗長設定	. 21
	4-1 冗長構成について	. 21
	4-1-1 冗長機能の概要	. 21
	4-1-2 冗長機能の注意事項	. 21
	4-1-3 異なるプラットフォーム間での冗長化	. 21
	4-2 RADIUS 機能の冗長化	. 22
	4-2-1 動作概要	. 22
	4-2-2 RADIUS の冗長設定	. 23
	4-3 DHCP 機能の冗長化	. 26
	4-3-1 動作概要	. 26
	4-3-2 DHCP の冗長設定	. 27



1 アカウント自動棚卸(自動削除) Web MAC 802.1x VPN

アカウント自動棚卸(自動削除)を使用することで、一定期間認証されていないアカウントや、有効期限切れのアカウントの無効化および削除を自動で実施できます。アカウント自動棚卸(自動削除)では、以下の処理を自動で行えます。

- 最終認証日時から指定日数が経過したアカウントを無効化する
- 無効化してから指定日数が経過したアカウントを削除する
- アカウント有効期限から指定日数が経過したアカウントを削除する
- アカウント情報を登録した日から指定日数が経過したアカウントを削除する
- ユーザーアカウントの削除と連動して、そのアカウントが申請していたアカウント も削除する



アカウント自動棚卸(自動削除)では、ユーザーアカウント、端末アカウント、証明書ア カウントに対して、以下の処理を行えます。また、以下の処理のルールはディレクトリご とに適用が可能です。

表 1

	コーザーマカウント	詳士フォウント	証明書マカウヽ。ト
	ユーリードカウンド	「姉木プリソフト	証明音パカリント
ネットワーク利用無効	最終認証日から指定E	1数が経過したアカウン	トのネットワーク利用
	を無効化する		
アカウント削除	ネットワーク利用が無	対になってから指定日常	数が経過したアカウン
(ネットワーク利用無	トを削除する		
効)			
アカウント削除	アカウント有効期限が	切れてから指定日数が	クライアント証明書
(有効期限切れ)	経過したアカウントを	:削除する	の有効期限が過ぎて
			から指定日数が経過
			したアカウントを削
			除する
アカウント削除	最終更新日から指定日	数が経過したアカウント	~を削除する
(最終更新日)			



1-1 自動削除の設定

管理メニューで「アカウント操作(内部 DB)」をクリックし(a)、「自動削除設定」を選 択します(b)。「自動削除設定」画面が表示されます。

Tips 初期状態で設定されてい る「ルート設定」は、	アカウントー覧 環境設定 CA RADTUS アカウント操作(内部08)	自動削除 新規登録 該当するデ	C	 管理端末/証明 5ります。 	唐而辞。		
RADIUS GUARD S V7内 部に登録されている全	アカウント設定 ユーザーパスワード設定 定明インボート/エクスポート	No.		名称▲▼ ルート10字	対象ディレクトリ▲▼	アカウント自動術隊機能	H#
ティレクトリを対象とし た設定です。				<i>n</i> -1904	1.00	1011 (- 44 (-	6

Tips

登録できるディレクトリ 数に制限はありません。

特定のディレクトリに対して自動削除を設定する場合は「新規登録」ボタンをクリックし (c)、「自動削除設定登録」 画面を表示します。

展る

自動削除設定登録	
1 名称※ (32文字(JP)	
2 対象ディレクトリ※	欄訳 未選訳
3 アカウント自動剤除機能	◎使用する ●使用しない
<u>а-7-</u>	
4 ネットワーク利用無効(※1) (0~9999)	●使用する ●使用しない 最終認証日から 90 日以上経過したアカウント

```
のネットワーク利用を無効にする
5 アカウント剤除
(ネットワーク利用無効)
                   使用する 使用しない
                  ネットワーク利用が無効になってから90 日以上経過したアカウントを削除する
  (0~9999)
6 アカウント制除
                  使用する 使用しない
  (有効期限切れ)
                  アカウント有効期限日が過ぎてから90 日以上経過したアカウントを削除する
  (0~9999)
7 アカウント制除
                  使用する 使用しない
  (最終更新日)
                  最終更新日から90 日以上経過したアカウントを削除する
  (0~9999)
```

Tips

新たに自動削除設定を登 録した場合、対象のディレ クトリは「ルート設定」で の設定内容の対象外にな ります。

名称、対象ディレクトリ、アカウント自動削除機能などを設定し、画面下部の「登録」ボ タンをクリックします。

表 2

Tinc				
		項目名	初期値	内容
イットワーク利用無効、ア カウント削除は、ユーザー	1	名称	空欄	設定の名称を入力
/端末/証明書のそれぞ	2	対象ディレク	未選択	「 <mark>選択</mark> 」ボタンをクリックし、設定対象のディレクト
れで設定できます。		トリ		リを選択
	3	アカウント自	使用し	アカウント自動削除機能を使用するかどうかを設定
Tips		動削除機能	ない	
▲→	4	ネットワーク	使用し	最終認証日から指定日数が経過したアカウントのネッ
らアカウント削除までの		利用無効	ない	トワーク利用を無効にするかどうかを設定
	5	アカウント削	使用し	ネットワーク利用が無効になった日から指定日数が経
無効化と削除か同時に実 施されます		除(ネット	ない	過したアカウントを削除するかどうかを設定
		ワーク利用無		
		効)		
Tips	6	アカウント削	使用し	アカウントの有効期限またはクライアント証明書の有
自動削除処理は、日時処理		除(有効期限	ない	効期限から指定日数が経過したアカウントを削除する
(0:30)で実施されます。		切れ)		かどうかを設定



	項目名	初期値	内容
\overline{O}	アカウント削	使用し	最終更新日から指定日数が経過したアカウントを削除
	除(最終更新	ない	するかどうかを設定
	日)		



2 外部認証局登録とサーバー証明書

802.1x VPN

外部認証局(CA局)のCA証明書およびCRLをRADIUS GUARDSV7に登録することで、内部認証局で発行したクライアント証明書に加えて外部認証局で発行されたクライアント証明書でも認証できるようになります。



2-1 外部認証局の登録

RADIUS GUARD S V7 以外の既存の外部認証局(CA 局)の CA 証明書および CRL ファ イルを用いて外部認証局を登録します。

管理メニューで「RADIUS」をクリックし(a)、「外部認証局」を選択します(b)。「外部認証局」タブで「新規登録」ボタンをクリックします(c)。

メイン : 稼働中 DHCPプライマリ : 稼働中 DHCP設定反映 : 自動	外部認証局
アカウント一覧	新規登録
環境設定	
RADIUS	No. 🗌 サブジェクト 有効期限 CRL取得 編集 発行済証明書
RADIUS設定	
RADIUSクライアント	
ネットワークプロファイル	
Calling-Station-Idグループ	
VSA設定	
RADIUSプロキシ D	
外部認証局	
ブロックリスト	

Tips

Tips

できます。

外部認証局は5件まで登録

外部認証局を登録した場 合、RADIUS 設定反映作業 が必要です。 →参照『簡単スタートアッ プガイド (vol.1)』の「5 RADIUS」

「外部認証局登録」画面が表示されます。外部認証局、CRL 設定、取得時刻などの情報を設定し、画面下部の「登録」ボタンをクリックすると、設定が登録されます。

外部認証局登録とサーバー証明書



外部認証局 サ	ーバー証明書	
外部認証局登録		
		ð
外部認証局	_	
① CA胚明書※	ファイルの選択 ファイルが選択されていません	
CRL設定		
	○登録する ®登録しない ◎ 自動登録 ○ 手動登録	
CRL更新日時		
自動登録設定		
3 取得時刻	◇時 ◇分	
4 取得間隔	24時間 🖌	
使用プロトコル	©FTP OHTTP OHTTPS OSFTP OSCP	
(5) 取得先サーバー	IPアドレス:ポート番号 : /	
6 ファイルパス (半角英数記号空白 25	6文字以内)	
取得先サーバー認証	○使用する ◎使用しない	
取得先サーバーユー (半角英数記号 64文字	ザーID (20月)	
取得先サーバーパス (半角英数記号 30文字	ワード ②変更する ◎変更しない 以内)	
	(確認用)	
リトライ機能	○使用する ◎使用しない	
手動登録設定		
CRLファイル	ファイルの違択ファイルが選択されていません	

表 3

	項目名	初期値	内容	
1	CA 証明書	指定な	「 ファイルの選択 」 ボタンをクリックして、 既存の CA	
		し	証明書を選択	
2	CRL	登録し	「 登録する 」を選択したのち、「 自動登録 」を選択。「手	
		ない	動登録」を選択した場合は、「CRL ファイル」で CRL	
			ファイルを選択	
3	取得時刻	未設定	CRL を定期取得する時刻を設定	
4	取得間隔	24 時間	CRL を定期取得する間隔を選択	
(5)	取得先サー	空欄	CRL 取得先のサーバーの IP アドレス、ポート番号を	
	バー		入力	
6	ファイルパス	空欄	外部サーバー上のファイルパス(ファイル名を含む)	
			を入力	
$\overline{\mathcal{O}}$	CRL ファイル	未選択	「CRL」で「 手動登録 」を選択した場合、「ファイルの	
			選択」ボタンをクリックして、CRL ファイルを選択	

Tips

CRLのチェックは、装置単位でオン/オフが可能ですが、認証局ごとに設定することはできません。

Tips

将来、既存のCA局が存在 しなくなり、RADIUS GUARDSV7のCA局を 有効にする場合は、既存の CA局で取得するCRLファ イルの有効期限は、既存の クライアント証明書の認 証期間を超える日付とな る設定で取得してください。

2-2 外部認証サーバー証明書の登録

外部認証局 (CA 局) にサーバー証明書の発行を依頼するための CSR 情報を作成し、サーバー証明書を登録します。

2-2-1 CSR 情報の発行

管理メニューで「RADIUS」をクリックし(a)、「RADIUS 設定」を選択します(b)。 「登録」ボタンをクリックし(c)、「外部サーバー証明書登録」画面を表示します。



メイン : 稼働中 DHCPプライマリ : 稼働中 DHCP設定反映 : 自動	RADIUS設定	
アカウントー覧 環境設定	RADIUSポート番号※ (半角数字 1~65535)	1812
	RADIUS Accounting※ (半角数字 1~65535)	○使用する ●使用しない ポート番号1813
RADIUS設定 RADIUSクライア b	接続状況 二重ログイン	◎記録する ○記録しない ◎許可する ○許可しない
ネットワークプロファイル	ログアウト	Framed-IP-Address属性を含まないAccounting-Stopを無 C
Calling-Station-Idグループ	認証サーバー証明書	○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
VSA設定		通知メール設定
RADIUSプロキシ	認証局	マ内部認証局の必要認証局
外部認証局	ODOLL/PJ	
ブロックリスト		

「作成」ボタンをクリックし(a)、「外部サーバー証明書登録 CSR 作成」画面を表示します。

外部サーバー証明書登録	
CSR情報	大作成 作成 名
サーバー証明 書※	未登録 ファイルの選択 ファイルが選択されていません
サーバー証明書秘密鍵	●登録したCSM情報の秘密鍵を使用する。 ○他のサーバーで登録したCSM情報の秘密鍵(パスフレーズ無し)を使用する。 ファイルの選択 ファイルの選択
※は必須項目です。	
	登 録

名前 (cn)、国 (c) などを設定し、画面下部の「登録」ボタンをクリックすると、CSR 情報が登録されます。

外部サーバー証明書登録 CSR作成				
入力規則 内部認証局設定をコピー 戻る				
CSR情報設定				
1名前(cn)※ (半角英数記号 64文字以内)				
2 国(c)	日本(JP) ~			
都道府県(st) (半角英数記号 128文字以内)				
市区町村(l) (半角革教記号 128文字以内)				

Tips

CSR 情報の入力規則を確 認するときには、「入力規 則」ボタンをクリックしま す。

	項目名	初期値	内容	
1	名前(cn)	空欄	認証局の名称を入力	
2	国(c)	日本	国名を選択	
(JP)				

表 4

CSR 情報の登録が完了すると、「外部認証局 CSR 設定を登録しました。」というメッセージが表示されるので「戻る」ボタンをクリックします(a)。



外部サーバー証明書登録 CSR作成				
入力規則 内部認証局設定をコピー 日本 夏る				
外部認証局CSR設定を登録しました。				
CSR情報設定				
名前(cn) <mark>※</mark> (半角英数記号 64文字以内)	ca.example.com			
国(c)	日本(JP) ~			

「外部サーバー証明書登録」画面の「CSR 情報」に、登録した cn の情報が表示されます。「DL」ボタンをクリックし(a)、CSR 情報ファイルをダウンロードします。

外部サーバー証明書登録		
CSR情報	ca.example.com 作成 表示 DL	Real
サーバー証明 書※	未登録 ファイルの選択 ファイルが選択されてい	いません
サーバー証明書秘密鍵	●登録したCSR情報の秘密鍵を使用する。 ○他のサーバーで登録したCSR情報の秘密鍵 □アイルの選択 □アイルが選択されてい	律(パスフレーズ無し)を使用する。 いません
※は必須項目です。		
Ĕ	」 除	登録

ダウンロードした CSR 情報ファイルを証明書発行依頼先に送付し、サーバー証明書の発行を受けます。

2-2-2 サーバー証明書の登録

発行されたサーバー証明書を登録します。

管理メニューで「RADIUS」をクリックし、「RADIUS 設定」を選択します。「登録」ボ タンをクリックし、「外部サーバー証明書登録」画面を表示します。

外部サーバー証明書登録	
	戻る
CSR情報	ca.example.com 作成 表示 DL
サーバー証明 書※	未登録 ファイルの選択 フ る が選択されていません
サーバー証明書秘密鍵	●登録したCSR情報の秘密鍵を使用する。 ○他のサーバーで登録したCSR情報の秘密鍵(パスフレーズ無し)を使用する。 ファイルの選択 ファイルが選択されていません
※は必須項目です。	
Ë	」除 登録 b

「ファイルの選択」ボタンをクリックし (a)、サーバー証明書を選択して画面下部の「登録」ボタンをクリック(b)します。



2-3 RADIUS サーバーの設定

外部認証局(CA局)で発行されたサーバー証明書やクライアント証明書を利用するよう に RADIUS GUARD S V7 を設定します。

管理メニューで「RADIUS」をクリックし(a)、「RADIUS 設定」を選択します(b)。

メイン : 稼働中 DHCPプライマリ : 稼働中 DHCP設定反映 : 自動	RADIUS設定	
アカウント一覧	RADIUSポート番号※ (米色物字 10:65535)	1812
	(平周数子 1~65535) RADIUS Accounting※ (半角数字 1~65535)	○使用する ◎使用しない ポート番号1813
RADIUS & Z	接続状況	◎記録する ○記録しない
ネットワークプロファイル	二重ログイン	●許可する ○許可しない C
Calling-Station-Idグループ	ログアウト	□Framed-IP-Address属性を含まないAccounting-Stopを無視する
VSA設定	認証サーバー証明書	○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
RADIUSプロキシ		通知メール設定
外部認証局	認証局	
プロックリスト	IEEE 802.1X認証	ZEAP-TLS ZPEAP ZEAP-TTLS ZEAP-MD5 ZEAP-MSCHAPv2

Tips

「認証サーバーの証明書」 の「外部サーバー証明書」 は、サーバー証明書を登録 していると選択可能にな ります。

Tips

「認証局」の「外部認証局」 は、CA 局発行の CA 証明 書を登録していると選択 可能になります。

Tips

RADIUS 設定を変更した 場合、RADIUS 設定反映作 業が必要です。 →参照『簡単スタートアッ プガイド (vol.1)』の「5 RADIUS」

「RADIUS 設定」画面が表示されます。

CA 局で発行されたサーバー証明書を利用する場合は、「認証サーバー証明書」で「外部 サーバー証明書」を選択します(c)。

外部 CA 局で発行されたクライアント証明書を利用する場合は、「認証局」で「**外部認証** 局」にチェックを付けます(d)。

画面下部の「登録」ボタンをクリックすると、設定が登録されます。

2-4 外部サーバー証明書発行

外部機器の CSR を取り込んで、外部機器向けのサーバー証明書の発行を行うことができます。



3 外部 Active Directory を参照した認証 Web 802.1x

RADIUS GUARD S V7 に Active Directory などの外部 LDAP サーバーの情報を登録す ることで、外部 LDAP サーバーに登録されているアカウント情報を使用してネットワー ク認証することもできます。



Active Directory を外部 LDAP サーバーとして PEAP 認証を行うには、RADIUS GUARD S V7 を AD ドメインに参加させる必要があります。

3-1 事前設定

管理メニューで「**環境設定**」をクリックし (a)、「**ネットワーク設定**」を選択します (b)。 メンテナンスツールメニューに切り替わるので、「**ネットワーク設定**」をクリックします (c)。



「ネットワーク設定」画面が表示されます。画面下部に移動し、ホスト名、DNS 設定、 時刻設定を設定して「登録」ボタンをクリックします。

Tips

RADIUS GUARD S V7 を ドメインに参加させる場 合、ホスト名、DNS サー バー、NTP サーバーの設定 が必要です。DNS サーバー については、参加するドメ インの LDAP サービスの SRV レコードが取得可能 である必要があります。



ホスト名設定	
 ホスト名※ (半角英数記号 63文字以内) (ドメインを含む場合は 半角英数記号 255文字以内) DNS設定 	master081.hcnet2008R2.com
 2 DNSサーバー (XXX.XXX.XXX.XXXX) (1行1IPアドレス 最大3行) 	192.168.4.3 [入力例] 192.168.1.1 192.168.1.2 192.168.1.3
タイムアウト (0~30) 時刻設定	
 ③ NTPサーバー (XXX.XXX.XXX.XXXX) (1行1IPアドレス 最大3行) 	●使用する(NTPサーバーを指定) ○使用しない 下記時刻を設定 2015 年 9 月 1 日 16 時 16 分 18 秒 210.173.160.27 210.173.160.57 210.173.160.87 (入力例) 192.168.1.1 192.168.1.2 192.168.1.3

表 5

Tips RADIUS GUARD S V7の 時刻をドメインコント ローラーと合わせる必要 があるため、NTP サーバー にはドメインコントロー ラーと同一の NTP サー バーの IP アドレスを指定 します。

	項目名	初期値	内容
1	ホスト名	localho	RADIUS GUARD S V7 のホスト名を FQDN で入力
		st.	
		localdo	
		main	
2	DNS サーバー	空欄	Active Directory または SRV レコードを参照できる
			DNS サーバーの IP アドレスを入力
3	NTP サーバー		「 使用する 」を選択し、ドメインコントローラーと同
			一の NTP サーバーの IP アドレスを入力

3-2 外部 AD サーバーの登録

管理メニューで「**外部 LDAP/AD 参照**」をクリックし(a)、「**外部 LDAP/AD 一覧**」を 選択します(b)。「外部 LDAP/AD 一覧」画面が表示されます。

外部 Active Directory を参照した認証



CA	外部LDAP/AD一覧							
RADIUS	新規登録							
アカウント操作(内部)	該当するデータ	\$.						
外部LDAP/AD参照	削除優先职	1.更新						
外部LDAP/AD一覧	ID 🗆	優先順位	区分	接続先	名称	状態	備考	編集
ネットワークプロファ・ D	DB -	0		127.0.0.1	内部DE	有効	内部登録アカウント	8
連動アカウント削除/無効化								
最終認証日時								
ユーザーツール								
DHCP								

「新規登録」ボタンをクリックし(c)、「外部 LDAP/AD 登録」画面を表示します。

ቃ	h部LDAP/AD登録	
	優先順位 (半角数字0~999)	0
	名称 ※ (32文字以内)	
	種別 ※ ①	●LDAP ○Active Directory
	2	ドメイン (半角英数記号 252文字以内)
3	IPアドレスまたはFQDN ※ (半角英数記号 64文字以内)	
4	検索フィルタ ※ (半角英数記号 1024文字以内)	 ●標準設定 ○任意設定
5	LDAP属性マップ ※	 ●標準設定 □ファイルを登録 □ファイルの選択 □アイルが選択されていません □ 1行目を無視して登録する
6	匿名bind※	◉使用しない ○使用する
7	bindDN <mark>※</mark> (1024文字以内)	
8	bindDN/ペスワード ※ (半角英数記号 128文字以内)	(確認用)
9	BaseDN ※ (1024文字以内)	

種別、ドメイン、IP アドレスなどを設定し、画面下部の「登録」ボタンをクリックしま す。

表 6

	項目名	初期値	内容
1	種別		「Active Directory」を選択
2	ドメイン		RADIUS GUARD S V7 を参加させる Active Directory
			のドメイン名を入力
3	IP アドレスま		Active Directory の IP アドレスまたはホスト名を入
	たは FQDN		カ
(4)	検索フィルタ		「 標準設定 」を選択
(5)	LDAP 属 性		「 <mark>標準設定</mark> 」を選択
	マップ		
6	匿名 bind		「 使用しない 」を選択
\bigcirc	bindDN		Active Directory に LDAP bind して検索するアカウ
			ントを DN 形式で入力

Tips

「検索フィルタ」で「標準 設定」を選択すると、 「(|(sAMAccountName= %U)(sAMAccountName =%{mschap:User-Name})(servicePrincipal Name=%u))」が検索フィ ルタとなります。

Tips

「bindDN」に入力するア カウントは、Active Directoryのアカウントの CN 属性(bindDNの最初 の「CN=○○」部分)と sAMAccountName 属性 の値が一致している必要 があります。

Tips

RADIUS 設定を変更した 場合、RADIUS 設定反映作 業が必要です。 →参照『簡単スタートアッ プガイド (vol.1)』の「5 RADIUS」



	項目名	初期値	内容
8	bindDN パス		LDAP bind するアカウントのパスワードを入力
	ワード		
9	BaseDN		アカウント検索するディレクトリの開始位置を DN 形
			式で入力

外部LDAP/AD一覧



削除 優先順位更新

ID		優先順位	区分	接統先	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	-

「ドメイン設定」をクリックし(a)、「ドメイン設定」画面を表示します。

ドメイン設定

	戻	5
1 このドメインに参加する※	Active Directory: newbiz4.local 🗸	
 NetBIOSドメイン名 (半角英数記号 15文字以内) 	NEWBIZ4	
- ※は必須項目です。 NetBIOSドメイン名に使用可能な記 登録した情報を反映させるには設定	号は の3種類です。 2反映操作が必要です。	
	登録	_

必要項目を設定し、画面下部の「登録」ボタンをクリックします。

表 7

	項目名	初期値	内容
1	このドメイン		外部 LDAP/AD 登録にて登録した AD サーバーを選択
	に参加する		
2	NetBIOS ドメ		AD サーバーの NetBIOS ドメイン名を入力
	イン名		



3-2-1 Active Directory ユーザーアカウントの DN 形式を確認する

DN (Distinguished Name) は、LDAP の相対識別名です。Active Directory ユーザーア カウントの DN 形式を確認する場合、「Active Directory ユーザーとコンピュータ」画面 でユーザーアカウントを右クリックして「Active Directory のプロパティ」を表示しま す。「属性エディター」タブをクリックし(a)、「distinguishedName」属性の値を確認 します(b)。

Tips 「属性エディター」タブ は、「表示」メニューをク リックして「拡張機能」を 有効にすることで表示さ れます。

📴 Active Directory 그~	げーとコンピューター	_ __
ファイル(F) 操作(A) 表示	モ(V) ヘルプ(H)	
🗢 🔿 🖄 🔂 🖬	X 🗈 Q 😹 🖬 🖬	🔧 🕱 🗊 🗾 🕱
Active Directory ユ 全部の 全部の 全部の 合称で 合称で 合称で 合称で した の に の の の の の の の の の の の の の	前 Administrator Allowed RODC Password Replic	種類 説 ▲ ユーザー コン cation Group セキュリティ グルこ0
🗉 adusers 🛛 🔮	Cer Administratorのフロパティ Der	<u> </u>
Computers Domain Con Series LostAndFour Managed Ser	Dnx 所属するグループ パスワークの Dnx セッション リ Dni 全般 住所 アカウン Doi 金般 住所 アカウン Doi 個人用仮想デスクトップ	ードレブリケーション ダイヤルイン オブジェクト セキュリティ 環境 リモート制御 リモート デスクトップ サービスの コーティイル ト プロファイル 電話 所属されている組織 ム a た証明書 ク COM+ 属性エディター のガナ
	Doi 属性(B): Doi 属性	l (de la
● Program Dat ● ● System	Ent displayNamePrintable Ent distinguishedName	<未設定> CN=Administrator,CN=Users,DC=example,DC=local
TDS Quota	Grc dVISION Grc dSASignature Gut dSCorePropagationD krb dynamicLDAPServer RA employeeID Re: employeeNumber	<未設定> <未設定> 2012/08/06 15:56:01 韓国 (標準時); 2012/08/06 15:5 <未設定> <未設定> <未設定> <未設定> <ま設定> <ま設定>
لتترانت مستعاد	extensionName facsimileTelephoneN	<本訳定/ <未設定/ 、<未設定/

3-3 AD サーバーの接続確認

登録した外部 LDAP/AD との接続確認を行います。外部 LDAP/AD 一覧から、該当する機器の 「状態」の有効ボタンをクリックする(a)と、機器の接続状態を確認することができます。



接続先の種類によって以下のように表示が異なります。AD サーバーに接続し、ドメイン参加している場合の例は下記となります。失敗表示がある場合、項目にそって設定内容を見直してください。



外部LDAP/AD一覧
新規登録 NetBIOSドメイン名対応表 NTLM認証設定
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)
該当するデータは3件あります。 削除 優先順位更新

3-4 AD サーバー側の確認

Active Directory の Computer コンテナに RADIUS GUARD S V7 のホスト名が登録されていることを確認します。

「Active Directory ユーザーとコンピュータ」画面を表示し、「Computers」コンテナ を選択します(a)。

	Active Directory ユーザーとコンピューター	
ファイル(F) 操作(A) 表示(V) へ	ルプ(H) Q 🔜 🛛 📷 🧏 🗽 🛍 🐨 🗖 🗽 🔽	1
 Active Directory ユーザーとコンと ▶ ○ 保存されたクエリ 	名前 種類 説明 Image: Second Content of the	
 Domain Controllers ForeignSecurityPrincip 		
CostAndFound Managed Service Acco Service Acco		
Program Data		

「Computers」コンテナに RADIUS GUARD S V7 のホスト名が存在していることを確認します(b)。



3-5 複数の AD 接続について

複数の Active Directory による構成では、以下の注意が必要です。

単一ドメイン



RADIUS GUARD S V7の RADIUS 認証では、Authorize→Authenticate という 2 段階 の認証処理が行われます。Active Directory 向けの PEAP 認証では、Authorize で LDAP 問い合わせ、Authenticate で NTLM 認証が行われます。

LDAP 問い合わせは、外部 LDAP として登録しているすべての Active Directory に対す る属性応答になります。このため、LDAP 問い合わせの対象となるすべての Active Directory を外部 LDAP として登録しておく必要があります。

NTLM 認証は、RADIUS GUARD S V7 が所属するドメインの Active Directory のうち 1 台以上が登録されていれば認証は成功します。NTLM 認証は DNS の SRV レコードの 応答によって決まります。

LDAP問い合わせによるAuthorize処理には失敗したが、NTLM 認証によるAuthenticate 処理には成功した際に、認証が成功したかどうかは選択可能です。ただし、属性応答が必要な場合にはAuthorize 処理に成功する必要があります。



複数ドメイン



異なるドメインに対して Active Directory 向け PEAP 認証を行う場合、RADIUS GUARD S V7 が所属するドメインと、その他のドメインを同一フォレストで構成するか、信頼関係を結ぶ必要があります。

NTLM 認証は、RADIUS GUARD S V7 が所属するドメインのいずれかの AD サーバーに 対して行われ、さらにその AD サーバーを介して、信頼するドメインのいずれかの AD サーバーに対しても行われます。

LDAP 問い合わせは、外部 LDAP 登録したすべての AD サーバーに対して行われます。 属性応答を行う場合は、異なるドメインの AD サーバーを含め、すべての AD サーバーを 外部 LDAP として登録しておきます。



4 冗長設定

4-1 冗長構成について

4-1-1 冗長機能の概要

RADIUS GUARD S V7 の RADIUS/LDAP 機能では、1 台のメインに対して最大 19 台の レプリカによる冗長構成が可能です。このとき、メインとなる 1 台を明示的に指定する 必要があります。また、IP アドレスでネットワーク到達性が確保できる場合、WAN 越え での冗長構成も可能です。

また、RADIUS GUARD S V7 の DHCP 機能では、プライマリ 1 台に対してセカンダリ 1 台の冗長構成が可能です。最大 20 台のサーバーまで統合して管理できます。

RADIUS/LDAP 機能の設定は、メインでのみ行い、レプリカはメインから同期される設定情報を保持します。

認証機能を含めて、すべての動作には RADIUS GUARD S V7 が持つ実 IP アドレスが使用されます。サービスはすべての装置で Active として動作するため、正常時は負荷分散も可能です。ただし、RADIUS クライアント側の設定も必要となります。

メインで障害が発生した場合、RADIUS クライアントがレプリカ側に RADIUS 問い合わ せを行うことでサービスが継続されます。

4-1-2 冗長機能の注意事項

RADIUS GUARD S V7 で冗長構成を設定する場合、以下の点に注意する必要があります。

- メインおよびレプリカとなる RADIUS GUARD S V7 のライセンスは、同一のライ センスモデルであり、異なるサーバー番号で登録します。
- メインサーバーとレプリカサーバー間のネットワーク帯域幅は 10Mbps 以上が推 奨されます。

また、DHCP サーバーとして動作する RADIUS GUARD S V7 を冗長構成する場合、冗 長構成に組み込まれるまで初回の IP アドレス払い出しは行われません。

4-1-3 異なるプラットフォーム間での冗長化

仮想アプライアンス版およびクラウドサービス版は、アプライアンス版と同様にメイン /レプリカ構成による冗長化が可能です。仮想環境の構成により、仮想サーバーは多様な 配置が可能です。

アプライアンス版、仮想アプライアンス版、クラウドサービス版のそれぞれをメイン/レ プリカとして混在した冗長構成を構築することが可能です。この場合、eth0 に設定する IP アドレス同士のネットワークの到達性を確保する必要があるため、安定した常時接続 される WAN 回線等を確保してください(10Mbps 以上を推奨)。



4-2 RADIUS 機能の冗長化

4-2-1 動作概要

冗長構成時の認証動作

RADIUS GUARD S V7 の設定情報は、メインからレプリカにリアルタイムで同期されます。



Tips

RADIUS 問い合わせ先の 切替動作は、RADIUS クラ イアントでの設定に依存 します。

> 障害などによってメイン機が利用不可になった場合、メインからレプリカに同期された 設定情報を元にレプリカによってサービスが継続して提供されます。



負荷分散

メイン/レプリカを 1:N 冗長構成とすることで、RADIUS クライアントからの問い合わ せ負荷を分散できます。

- 1. メイン/レプリカを 1:N 冗長構成にし、メインの設定情報をレプリカに同期
- 2. 各レプリカを RADIUS クライアントの問い合わせ先のプライマリとして登録



冗長設定



4-2-2 RADIUS の冗長設定

メインサーバーの設定

メインとする RADIUS GUARD S V7 を設定します。

管理メニューで「**環境設定**」をクリックし(a)、「**ライセンス**」を選択します(b)。メン テナンスツールの「ライセンス」画面に移行します。

メイン : 稼働中 DHCPプライマリ : ****中 DHCP設定反映 つ	ライセンス	
アカウント一覧	バージョン	7.00.01
環境設定	現在の登録アカウント数	13 / 200000
ライセンス	DBデータサイズ	約 1.1GB
ネットワーク設定		
WebUI設定	RADIUS GUARD S V7	
管理者アカウント		
オペレーションボード設定	 ライセンス 	
ダッシュボード設定	2 役割	□このサーバーの役割を変更する
メール設定	Č	◎メインサーバー ○レプリカサーバー
UPS設定		
冗長設定		類登

ライセンスおよび役割を設定し、画面下部の「登録」ボタンをクリックします。

表 8

	項目名	初期値	内容
1	ライセンス	空欄	ライセンスを入力
2	役割		「 メインサーバー 」を選択

管理メニューで「環境設定」をクリックし(a)、「冗長設定」を選択します(b)。「冗長設定」画面が表示されます。





「共通鍵登録」ボタンをクリックし(c)、「共通鍵」を表示します。

冗長設定		
共通鍵 半角英数記号 32文字以内	●変更する ◎変更しない	
		(確認用)
	登録	

Tips 「(確認用)」にも共通鍵を 入力します。

> 「変更する」が選択されていることを確認してテキストボックスに共通鍵を入力し(d)、 画面下部の「登録」ボタンをクリックします。

レプリカサーバーの設定

レプリカとする RADIUS GUARD S V7 を設定します。

管理メニューで「<mark>環境設定</mark>」をクリックし(a)、「**ライセンス**」を選択します(b)。メン テナンスツールの「ライセンス」画面に移行します。

イン : 稼働中 HCPプライマリ : 稼働中 HCP設定反映	ライセンス	
_{アカウントー第}	バージョン	7.00.01
	現在の登録アカウント数	13 / 200000
ライセンス D ネットワーク設定	DBデータサイズ	約 1.1GB
WebUI設定	RADIUS GUARD S V7	
管理者アカウント 1)	
オペレーションボード設定	9 51222	
ダッシュボード設定 2	役割	□このサーバーの役割を変更する
メール設定		◎メインサーバー ○レプリカサーバー
UPS設定		
冗長設定		「 え 登 」 「 」

ライセンスおよび役割を設定し、画面下部の「登録」ボタンをクリックします。

表 9

	項目名	初期値	内容
1	ライセンス	空欄	ライセンスを入力
2	役割		「 レプリカサーバー 」を選択

管理メニューで「**環境設定**」をクリックし(a)、「**冗長設定**」を選択します(b)。メンテ ナンスツールの「冗長設定」画面に移行します。

Tips

メインサーバーとレプリ カサーバーのライセンス 数は同一にしてください。 異なるライセンス数では 冗長構成はできません。



冗長設定

メイン : 稼動中 DHCPラテイマリ : 稼動中 DHCP設定反映 : 自動 アカウントー% a 振焼設定 1 IPアドレス (xxx, xxx, xxx, xxx)
アカウントー系 a ① IPアドレス (XX, XX, XX, XXX)
アカウントー第
ライセンス ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
ネットワーク設定 半角英数記号 32文字以内
WebUT設定
管理者アカウント 登録
オペレーションボード設定
ダッシュポード設定
メール設定
UPSigit D

IP アドレスおよび共通鍵を設定し、画面下部の「登録」ボタンをクリックします。

表 10

	項目名	初期値	内容
1	IP アドレス	空欄	メインサーバーの IP アドレスを入力
2	共通鍵	空欄	メインサーバーに登録した共通鍵を入力

Tips メインサーバーは、共通鍵 が確認されたレブリカ サーバーを自動的に登録 し、データをリアルタイム で同期します。

冗長設定の確認

メインとした RADIUS GUARD S V7 で、冗長構成の内容を確認します。

管理メニューで「環境設定」をクリックし(a)、「冗長設定」を選択します(b)。「冗長設定」画面が表示されます。

メイン ・稼働中	冗長設定				
DHCP設定反映	共通鍵登録				
Phone a	該当するデータは	1件あります。			
環境設定	SHAFE OLDER TO ME SHE	してください	• # 6		
ライセンス	DRTP ADAENC ARDIV	UCC (CCU			C
ネットワーク設定	No.		サーバー番号	IPアドレス	同期状態
WebUI設定	1	02		192.168.102.101	有効
管理者アカウント					
オペレーションボード設定					
ダッシュボード設定					
メール設定					
UPS設定 冗長設定					

「冗長設定」画面にレプリカサーバーが表示されていることを確認します(c)。



4-3 DHCP 機能の冗長化

4-3-1 動作概要

RADIUS GUARD S V7 を DHCP サーバーとして動作させた場合、プライマリ1台に対してセカンダリ1台の冗長構成が可能です。IP アドレスの最大払出数は、最大5万件となります。IP アドレスには、それぞれの RADIUS GUARD S V7 の実 IP アドレスが使用され、仮想 IP アドレスは設定しません。

サービスはプライマリ/セカンダリが Active/Standby で動作します。

L3 スイッチやルーターなどでリレー先をプライマリ/セカンダリに設定することで冗長 構成が成立します。



プライマリ/セカンダリを 1 つのセットとして、最大 20 台を束ねた統合管理が可能となります。ただし、リース情報の同期は冗長構成のペア間でのみになります。

プライマリ/セカンダリ間では、設定情報およびリース情報など以下の情報がリアルタ イムで同期されます。

- DHCP サブネット情報(スコープ/リース範囲)
- 登録端末情報(登録端末のみへの IP アドレスの払い出し、特定端末への固定 IP アドレスの払い出し)
- DHCP リース情報

プライマリで障害が発生した場合、クライアント、L3 スイッチ、ルーターがセカンダリ 側に DHCP 要求を行うことでサービスが継続します。このとき、正常時にプライマリ側 で払い出した IP アドレスはセカンダリ側が重複して払い出しません。

WAN 回線障害や eth0 の同期通信障害など、冗長構成でプライマリサーバーとセカンダ リサーバー間の通信のみが停止した場合、プライマリサーバーとセカンダリサーバーで それぞれ同じ IP アドレスを払い出し、端末が IP アドレス重複で通信できなくなる可能 性があります。

4-3-2 DHCP の冗長設定

DHC サーバーとして RADIUS GUARD S V7 を動作させる場合、プライマリ/セカンダ リともに DHCP サーバーグループに登録する必要があります。DHCP サーバーグループ の登録については、『簡単スタートアップガイド (vol.1)』の「7 DHCP」を参照してくだ さい。

同一の DHCP サーバークループに登録した DHCP サーバーをプライマリ/セカンダリとして冗長設定します。

プライマリサーバーの設定

プライマリサーバーとする RADIUS GUARD S V7 の管理メニューで「DHCP」をクリックし (a)、「サーバーグループ」を選択します (b)。「サーバーグループ」画面が表示されます。

アカウント一覧	サーバーク	ブループ				
環境設定	#-15-1		コン-任容得			
CA	5 11 5	JU J XZ KA	11 75 KK			
RADIUS	該当するテー	タは0件あります。				
アカウント操作(内部DB)	Nc. 🗆	グループ名▲▼	フライマリIPアドレスAマ セカンダリIPアドレスAマ	プライマリネットマスク	設定反映	編集
外部LDAP/AD参照			C.555 5 11 7 1 5 1 4	200000000000		
ユーザー						
рнср а						
サーバーグループ						
スコープ設定						
登録端末一覧						
オプション定義						
全体設定						
Shibboleth						
外部システム連係						
ログ参照						
メンテナンス						
ログアウト						

「**サーバーグループ登録**」ボタンをクリックし(c)、「サーバーグループ登録」画面を表示します。

◎する ●しない
T
255.255.255.0 [/24] 🔻
60
180

冗長構成、セカンダリサーバー番号、セカンダリ IP アドレス、セカンダリネットマスクの情報を設定し、画面下部の「登録」ボタンをクリックします。

	項目名	初期値	内容
1	冗長構成		「 する 」を選択
2	セカンダリ		セカンダリサーバーとするサーバーを指定
	サーバー番号		

表 11



Tips

DHCPサーバーを冗長構成 で登録するためには、異な るライセンスの RADIUS GUARD S V7 が必要です。

Tips

DHCPサーバーを冗長構成 で登録する前には、プライ マリ/セカンダリの機器 で「冗長設定」画面による 設定を実施しておく必要 があります。



	項目名	初期値	内容
3	セカンダリ IP		セカンダリサーバーの IP アドレスを指定
	アドレス		
4	セカンダリ	255.255.255.0	セカンダリサーバーのネットマスクを選択
	ネットマスク	[/24]	



SCSK株式会社 セキュリティ事業本部 セキュリティプロダクト第二部 〒135-8110 東京都江東区豊洲 3-2-20 豊洲フロント TEL:03-5859-3037 E-mail:rg-staff@scsk.jp 製品 URL:https://www.scsk.jp/sp/radius/

- RADIUS GUARD S および、RADIUS GUARD S ロゴは、SCSK 株式会社の登録商標です。
- 本書記載の製品名および会社名は各社の商標または登録商標です。
- 記載の内容(定価、仕様など)は、改良のため予告なしに変更する場合があります。
- 記載の内容は 2025 年 4 月現在、ファームウェアバージョン Ver7.xx のものです。

RADIUS GUARD S V7 簡単スタートアップガイド(vol.2)

Copyright(c) 2024 SCSK Corporation. 2025 年 4 月 第 2 版

> SCSK 株式会社 東京都江東区豊洲 3-2-20 豊洲フロント