2025 年 4 月 1 日
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

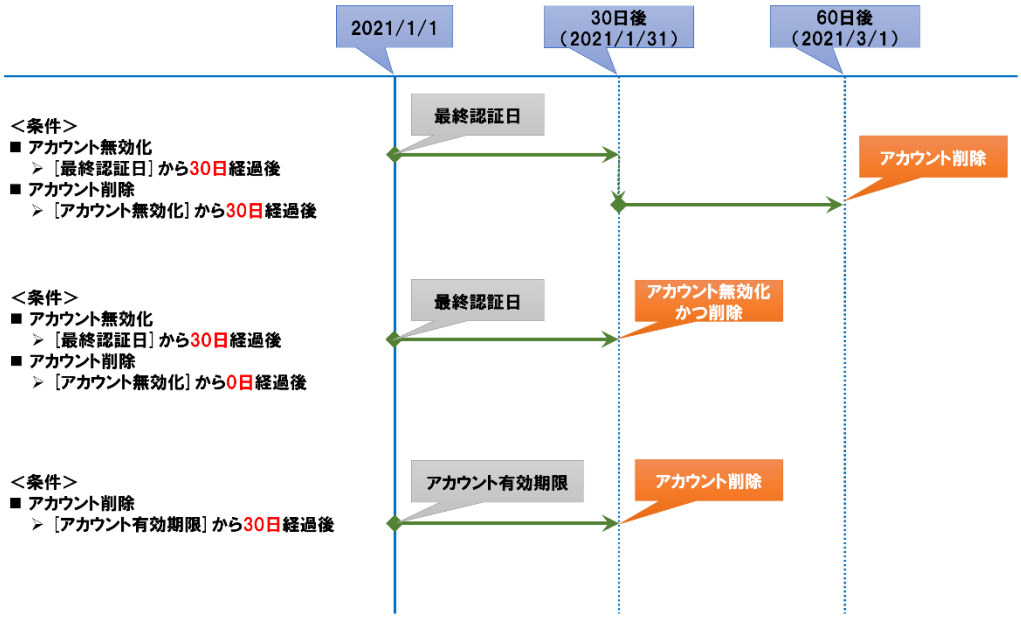
目次

1 アカウント自動棚卸（自動削除）

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

	ユーザーアカウント	端末アカウント	証明書アカウント
ネットワーク利用無効	最終認証日から指定日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（ネットワーク利用無効）	ネットワーク利用が無効になっ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（有効期限切れ）	アカウント有効期限が切れてから指定日数が経過したアカウントを削除する		クライアント証明書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）	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		

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、RADIUS GUARD S V7 内部に登録されている全ディレクトリを対象とした設定です。

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。

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。

Tips
ネットワーク利用無効、アカウント削除は、ユーザー／端末／証明書のそれぞれで設定できます。

Tips
ネットワーク利用無効からアカウント削除までの日数を「0 日」にした場合、無効化と削除が同時に実施されます。

Tips
自動削除処理は、日時処理（0:30）で実施されます。

表 2

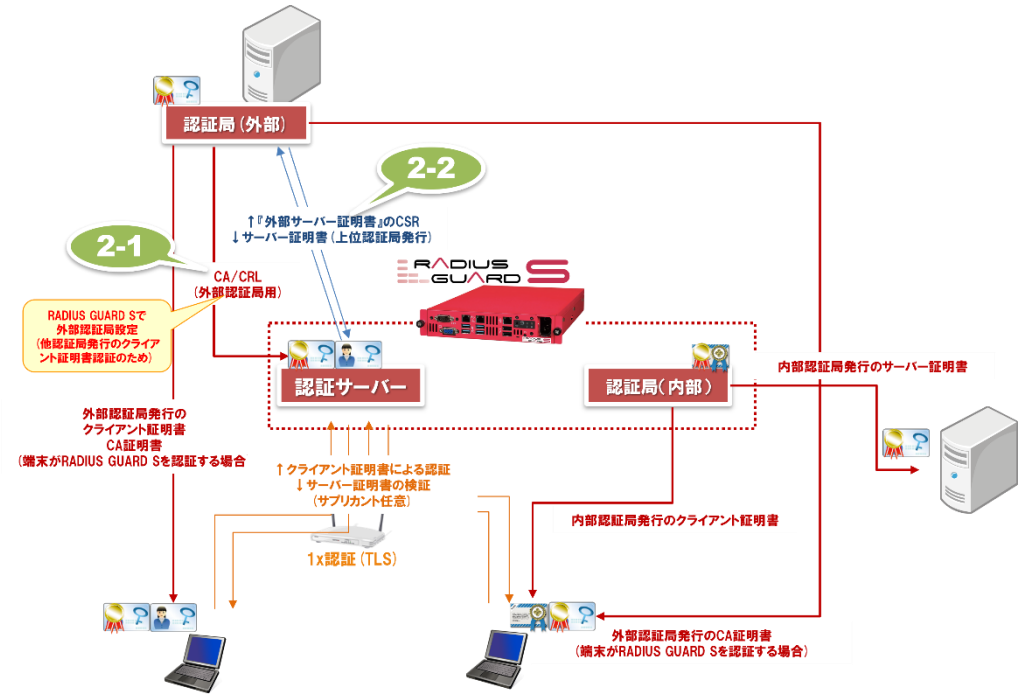
	項目名	初期値	内容
①	名称	空欄	設定の名称を入力
②	対象ディレクトリ	未選択	「**選択**」ボタンをクリックし、設定対象のディレクトリを選択
③	アカウント自動削除機能	使用しない	アカウント自動削除機能を使用するかどうかを設定
④	ネットワーク利用無効	使用しない	最終認証日から指定日数が経過したアカウントのネットワーク利用を無効にするかどうかを設定
⑤	アカウント削除（ネットワーク利用無効）	使用しない	ネットワーク利用が無効になった日から指定日数が経過したアカウントを削除するかどうかを設定
⑥	アカウント削除（有効期限切れ）	使用しない	アカウントの有効期限またはクライアント証明書の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かどうかを設定

	項目名	初期値	内容
⑦	アカウント削除（最終更新日）	使 用 しない	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かどうかを設定

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 GUARD S V7 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。

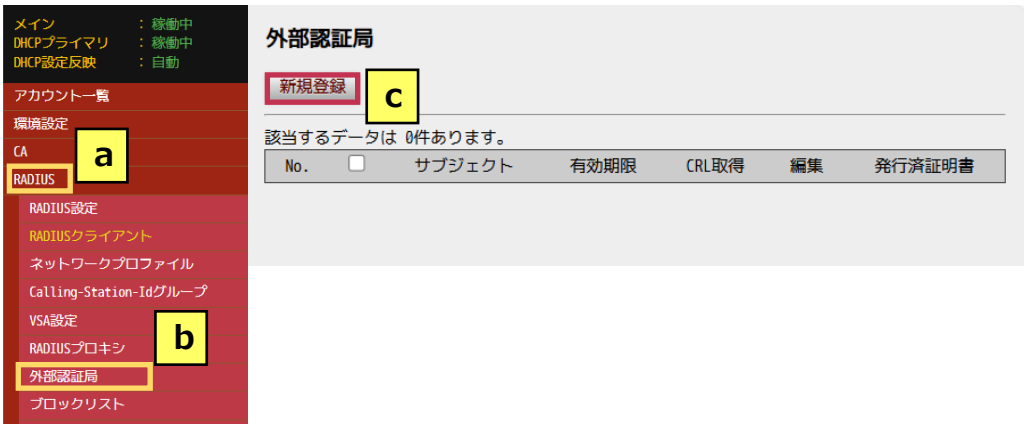


2-1 外部認証局の登録

Tips
外部認証局は５件まで登録できます。

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）。



Tips
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。

表 3

	項目名	初期値	内容
①	CA 証明書	指定なし	「**ファイルの選択**」ボタンをクリックして、既存の CA 証明書を選択
②	CRL	登録しない	「**登録する**」を選択したのち、「**自動登録**」を選択。「**手動登録**」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	取得先サーバー	空欄	CRL 取得先のサーバーの IP アドレス、ポート番号を入力
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
⑦	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 GUARD S V7 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。

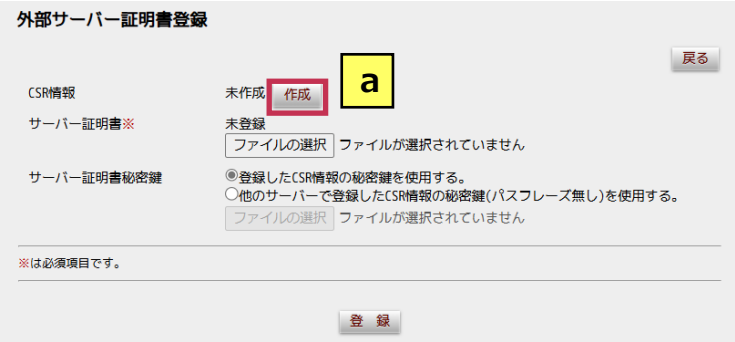
2-2 外部認証サーバー証明書の登録

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。

「**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。



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。

Tips

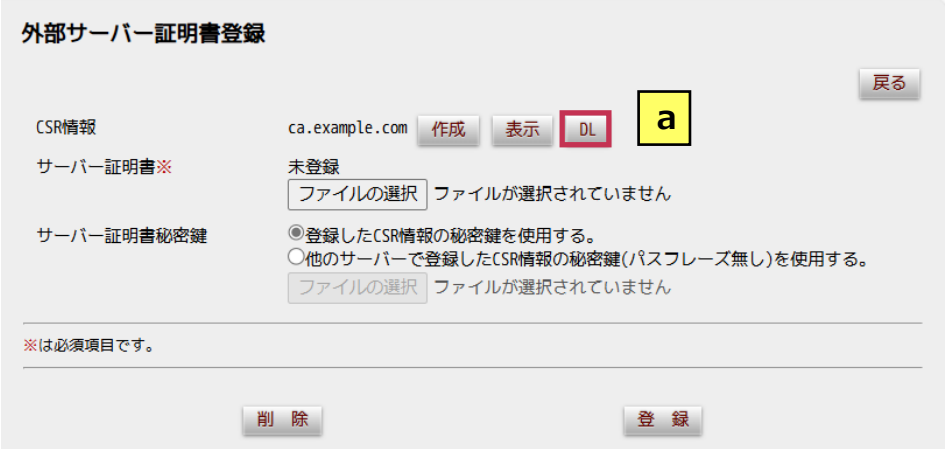
CSR 情報の入力規則を確認するときには、「入力規則」ボタンをクリックします。

表 4

	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（JP）	国名を選択

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」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。

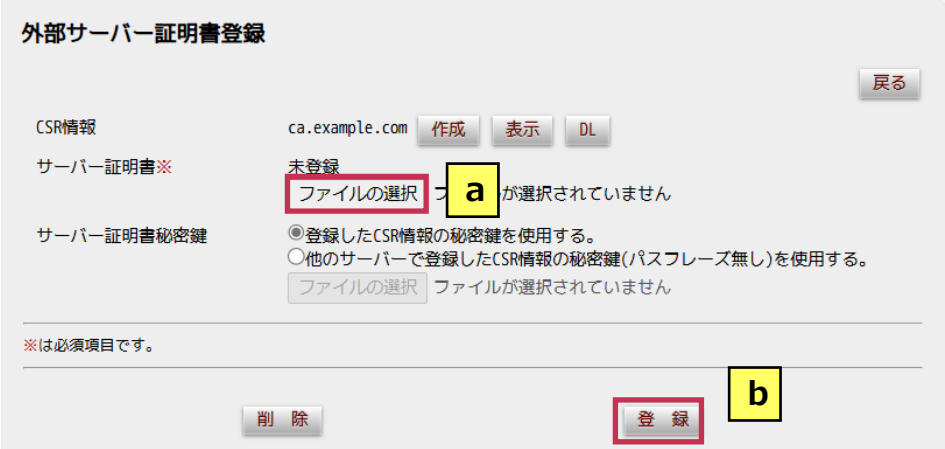


ダウンロードした CSR 情報ファイルを証明書発行依頼先に送付し、サーバー証明書の発行を受けます。

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。



「**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）。

「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。

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

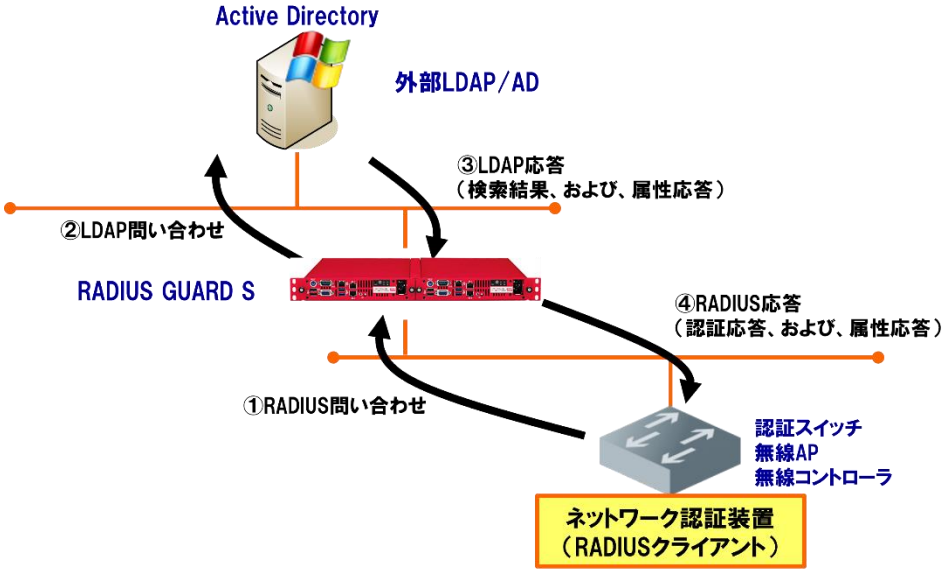
RADIUS 設定を変更した場合、RADIUS 設定反映作業が必要です。
→参照『簡単スタートアップガイド（vol.1）』の「5 RADIUS」

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。

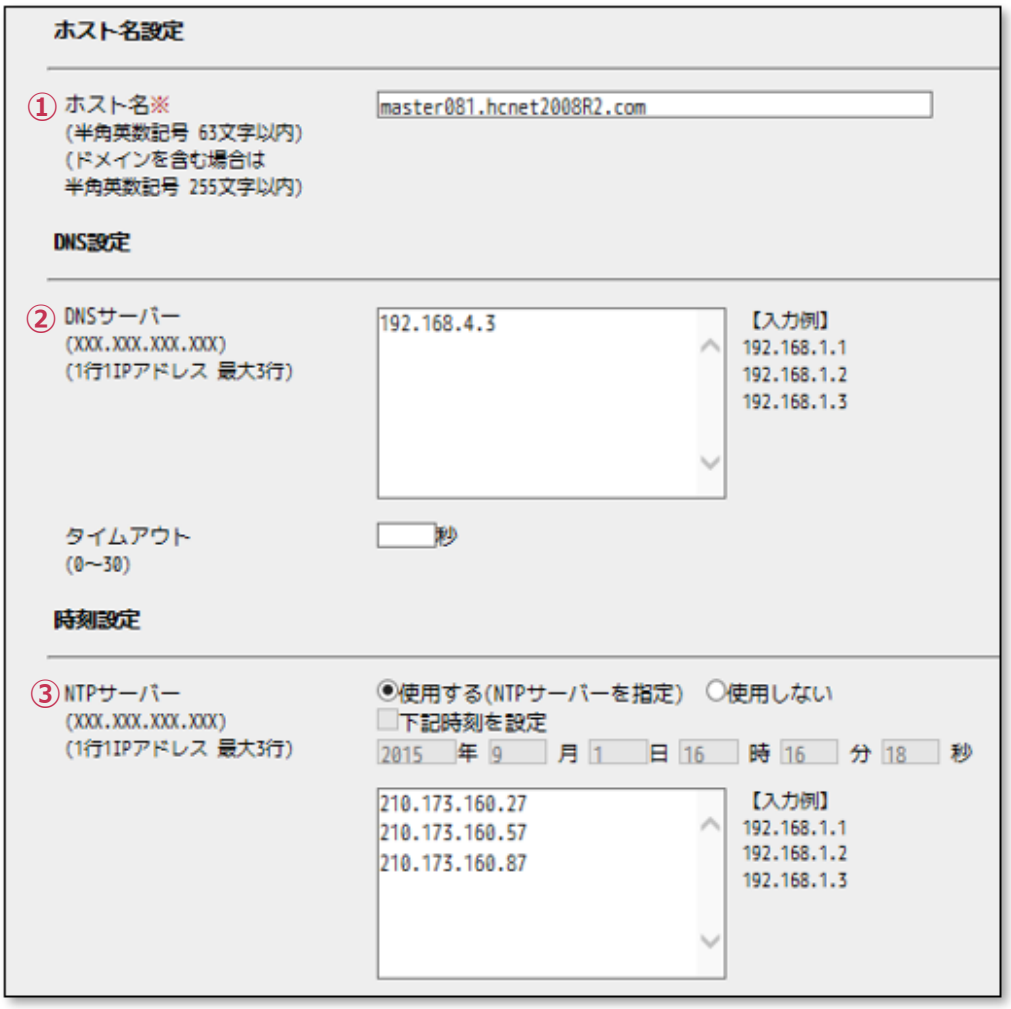


表 5

	項目名	初期値	内容
①	ホスト名	localhost.localdomain	RADIUS GUARD S V7 のホスト名を FQDN で入力
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

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。

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。

「**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。

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 アドレスまたは FQDN		Active Directory の IP アドレスまたはホスト名を入力
④	検索フィルタ		「**標準設定**」を選択
⑤	LDAP 属性マップ		「**標準設定**」を選択
⑥	匿名 bind		「**使用しない**」を選択
⑦	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})(servicePrincipalName=%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 パスワード		LDAP bind するアカウントのパスワードを入力
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

「**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。

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。

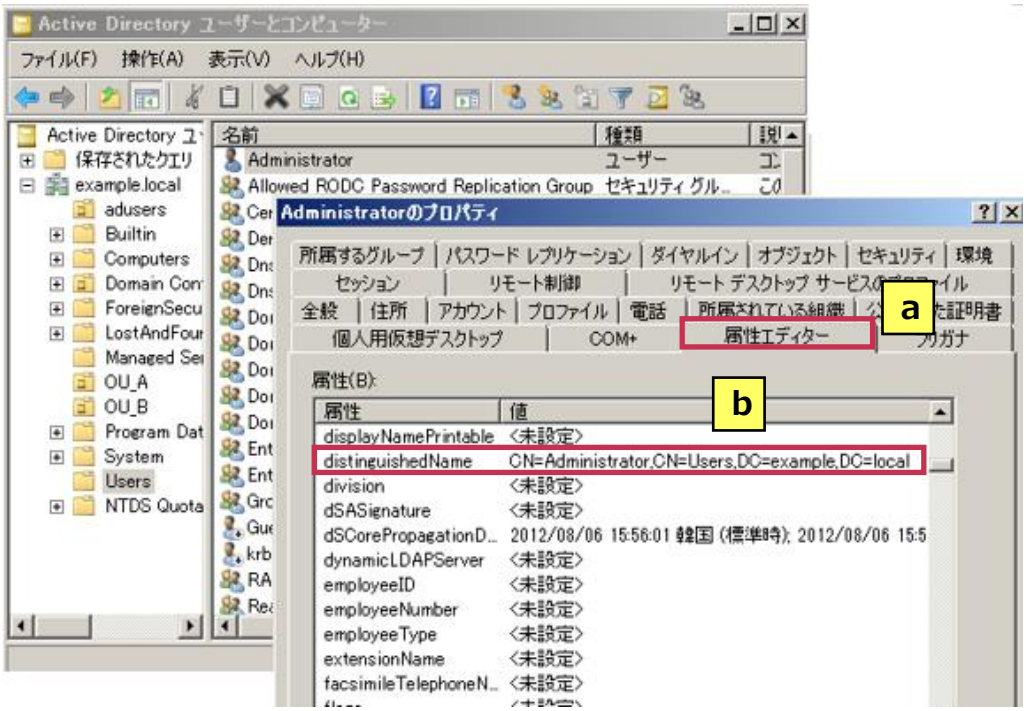
表 7

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

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。



3-3 AD サーバーの接続確認

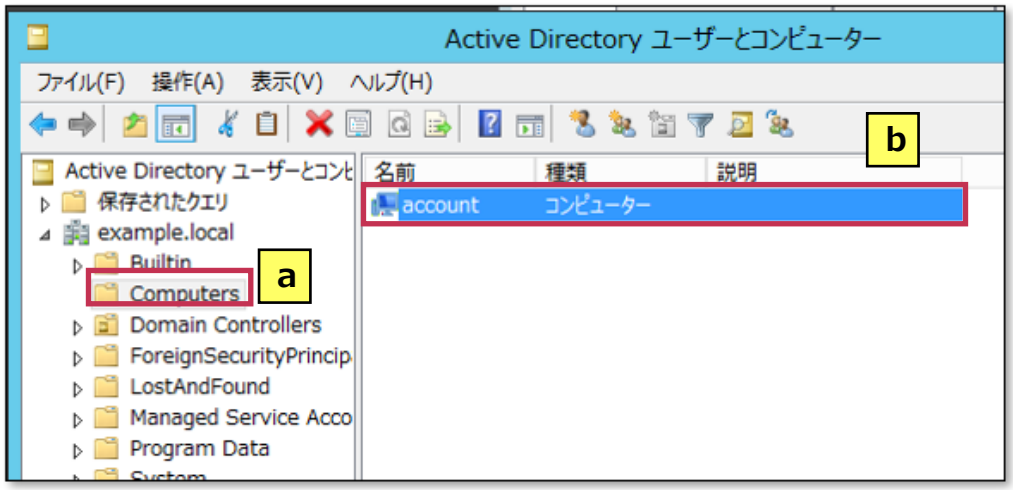
登録した外部 LDAP/AD との接続確認を行います。外部 LDAP/AD 一覧から、該当する機器の「**状態**」の有効ボタンをクリックする(a)と、機器の接続状態を確認することができます。

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。

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）。

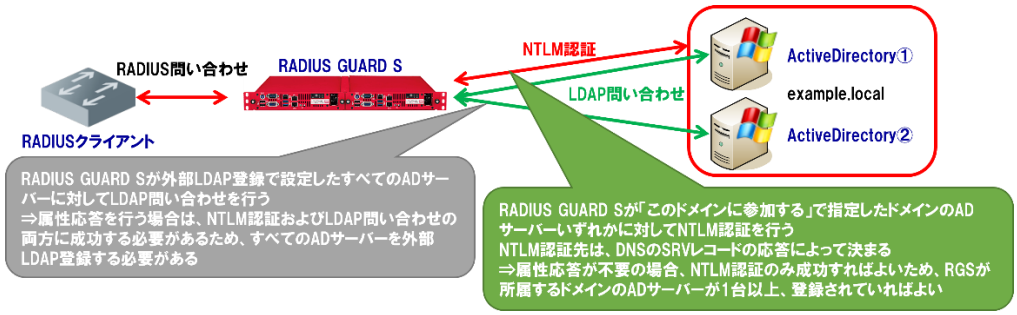


「**Computers**」コンテナに RADIUS GUARD S V7 のホスト名が存在していることを確認します（b）。

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

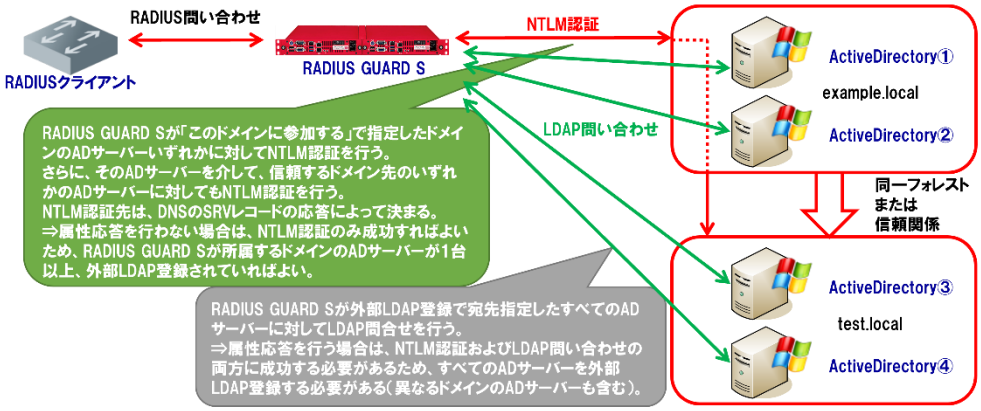


RADIUS GUARD S V7 の RADIUS 認証では、Authorize→Authenticate という 2 段階の認証処理が行われます。Active Directory 向けの PEAP 認証では、Authorize で LDAP 問い合わせ、Authenticate で NTLM 認証が行われます。

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。

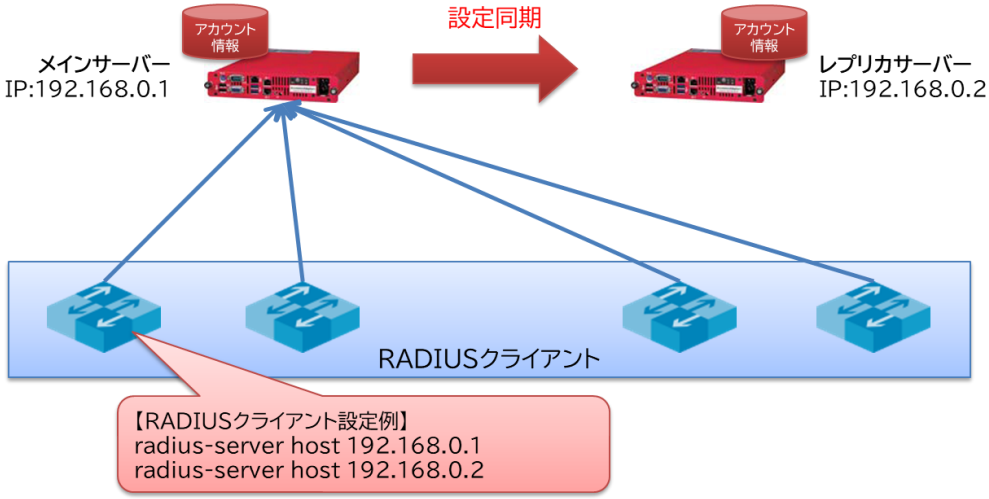
アプライアンス版、仮想アプライアンス版、クラウドサービス版のそれぞれをメイン／レプリカとして混在した冗長構成を構築することが可能です。この場合、eth0 に設定する IP アドレス同士のネットワークの到達性を確保する必要があるため、安定した常時接続される WAN 回線等を確保してください（10Mbps 以上を推奨）。

4-2 RADIUS 機能の冗長化

4-2-1 動作概要

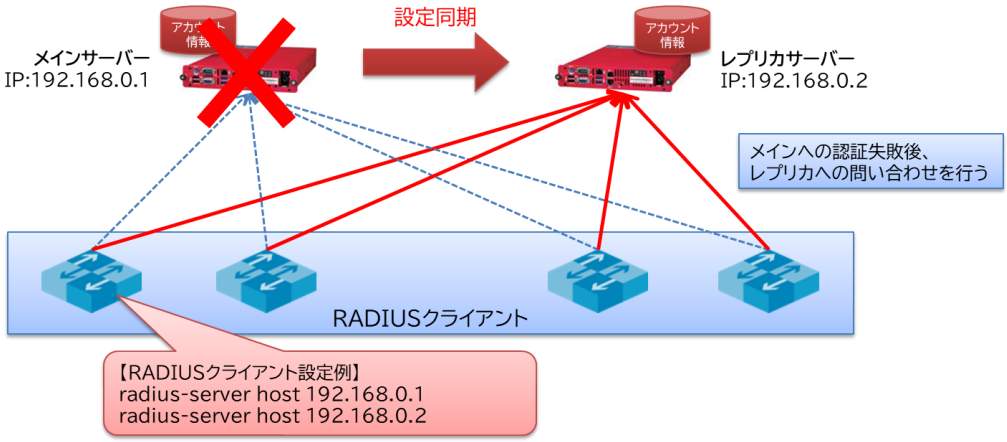
冗長構成時の認証動作

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。

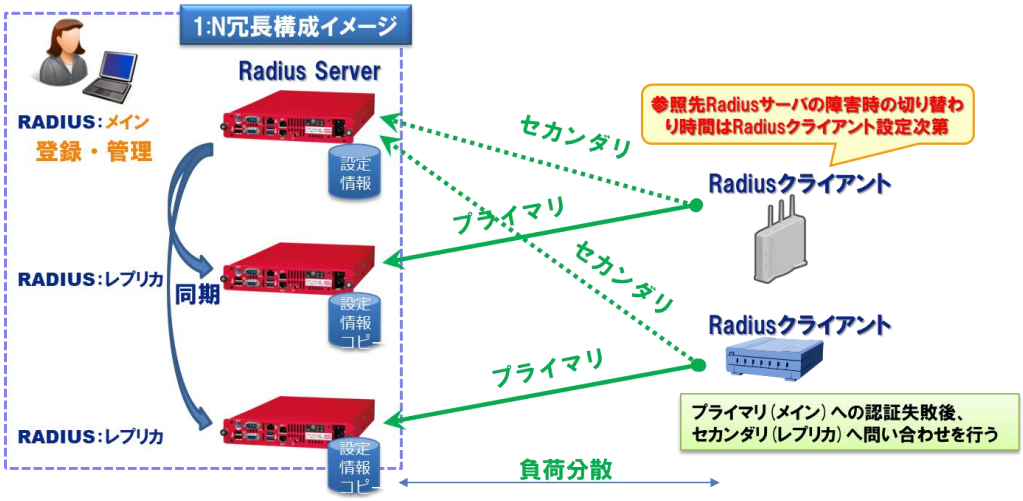
障害などによってメイン機が利用不可になった場合、メインからレプリカに同期された設定情報を元にレプリカによってサービスが継続して提供されます。



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



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。

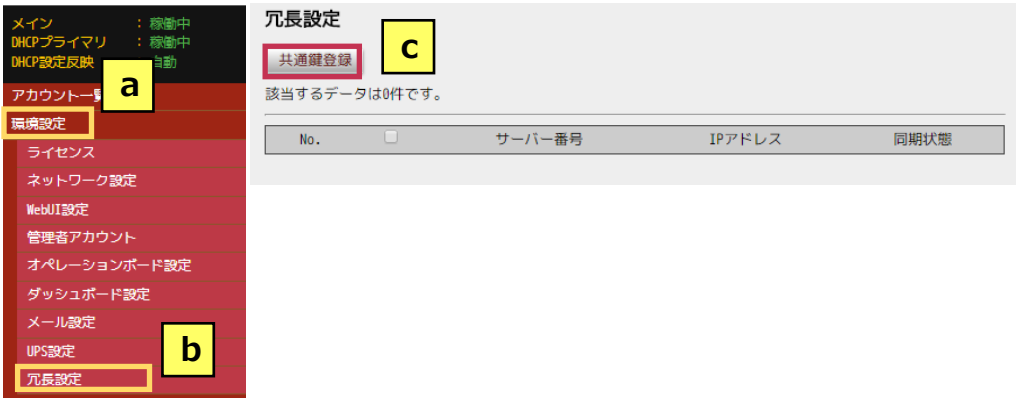
管理メニューで「**環境設定**」をクリックし（a)、「**ライセンス**」を選択します（b)。メンテナンスツールの「ライセンス」画面に移行します。

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。

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「**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。

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。

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。

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プ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。

「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)。

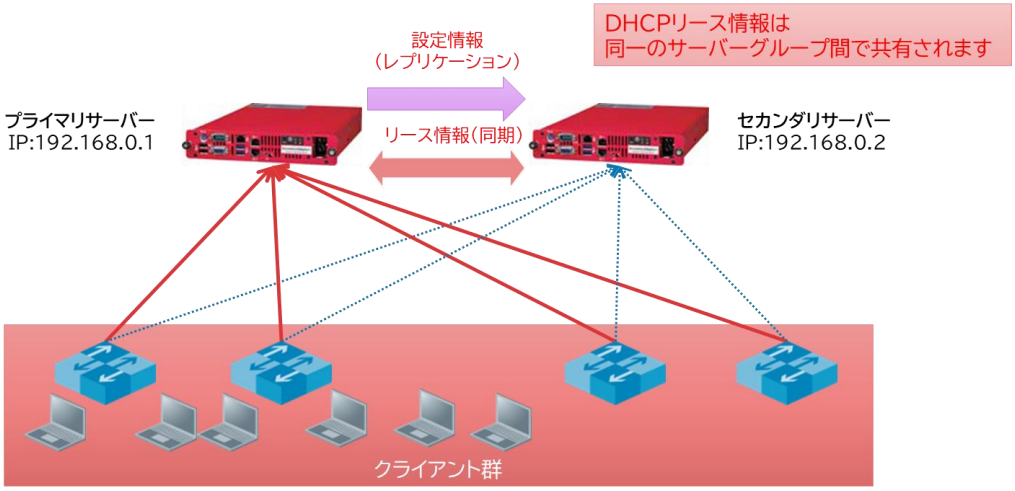
4-3 DHCP 機能の冗長化

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。

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。

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

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。

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。

「**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。

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。

表 11

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

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

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 V7
簡単スタートアップガイド（vol.2）

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