



夢ある未来を、共に創る。



「RADIUS GUARD S」のご紹介

2020年 2月

SCSK株式会社
ITプロダクト&サービス事業本部
ネットワーク部

- ◆ **RADIUS GUARD Sについて**
- ◆ **特徴と機能**
 - ・認証
 - ・アカウント管理
 - ・CA (証明書発行・管理)
 - ・ユーザーツール
 - ・DHCP
 - ・冗長構成
- ◆ **主な実績**
- ◆ **Ver.6.15.00新機能**
- ◆ **導入にあたり**
- ◆ **参照資料**

RADIUS GUARD Sについて

RADIUS・CA(証明書発行)・DHCP

各種サービスが提供可能な認証基盤用サーバーアプライアンス

アプライアンス版



- ◆ 専用アプライアンス製品
- ◆ 1Uハーフサイズの省スペース
- ◆ 1Uサイズで冗長対応

バーチャルアプライアンス版



- ◆ VMware ESXi
- ◆ Nutanix AHV
20年5月対応

クラウド対応版

AWS **Microsoft Azure**
20年4月対応 20年7月対応

環境にあわせて3つのプラットフォームから選択

セキュリティ強化に必須な不正接続対策に

無線LAN/有線 接続認証

- PEAP/TLSの導入
- MAC認証の実現
- 持ち込みPC対策
- ゲストアカウント発行

VPN接続認証

- 二段階認証の導入
- 私用デバイス制限
- 証明書認証

各種証明書発行 プライベートCA

- 各種証明書発行
- 証明書配付フロー
- スマートデバイス対応

Radiusサーバー機能

- ◆ 認証処理

認証局 (CA) 機能

- ◆ 証明書発行

ユーザーツール機能

- ◆ 申請ワークフロー

外部AD/LDAP参照機能

- ◆ 既存ID情報の参照

DHCPサーバー機能

- ◆ IPアドレス配布



サーバー運用負担軽減

- ◆ 基盤OSのメンテや維持費用が不要
- ◆ ウィルス対策や各種アップデート作業は不要
- ◆ 国内開発のサポートと保守を提供



- ・ 認証台数や、登録数の追加は？
- ・ 追加費用がかかる機能はどれだっけ？
- ・ 設置場所やスペースはどうしよう？

◆ 200～200,000エン트리 までカバー

- 登録エン트리数が増えても同じハードウェアのままライセンス更新で対応

◆ Radiusクライアントの接続数は無制限 (登録数は最大10,000エン트리)

- 最大Radiusクライアントの登録数に制限はなし

◆ 追加費用の必要なオプション機能は

**DHCPオプション、内部LDAP登録連携、
Shibbolethオプション だけ**

- 2500ライセンス以上は外部LDAP/AD参照機能も標準対応

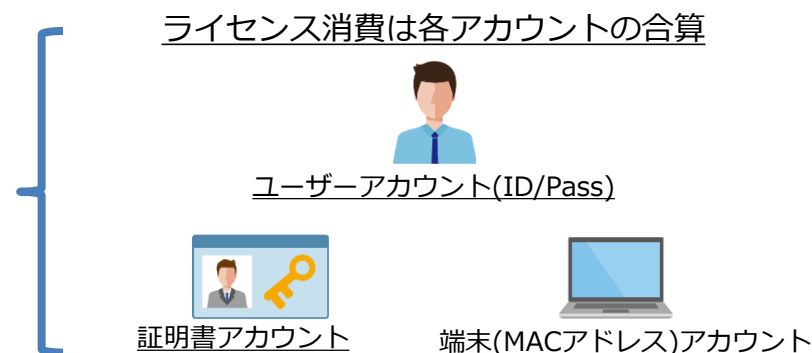
※200、500ライセンスはOption設定

- CA機能や各種ユーザーツールなどの管理機能は最小エン트리数から使用可能
- スマートデバイス向け対応も標準実装

◆ 本体＋標準ライセンスセット(初年度費用)

各プラットフォーム共通ライセンス体系

- RADIUS GUARD S 200ライセンス
- RADIUS GUARD S 500ライセンス
- RADIUS GUARD S 2,500ライセンス
- RADIUS GUARD S 5,000ライセンス
- RADIUS GUARD S 10,000ライセンス
- RADIUS GUARD S 50,000ライセンス
- RADIUS GUARD S 200,000ライセンス
- RADIUS GUARD S 300,000ライセンス (MAC認証用:提案時弊社要件確認必須)
- RADIUS GUARD S DHCPライセンス (認証ライセンスは別途追加可能)



◆ オプション

- 外部LDAP/AD参照オプション (200/500ライセンスのみ必要)
外部LDAP/ADを参照して認証する機能
- DHCPオプション
通常のRADIUS GUARD SにDHCP機能を追加
- 内部LDAP登録連携オプション
外部LDAPクライアントからRADIUS GUARD S 内部のアカウント情報を改廃 (参照のみはオプション不要)
- アドバンス連携オプション
クライアント証明書エクスポート機能、ADユーザー登録機能、認証ログアウト機能等
- 文教/学術向けオプション
 - Shibboleth SPオプション
 - UPKIクライアント証明書配付オプション

バーチャルアプライアンス (VA) 版



- ◆ VMware ESXi
- ◆ Nutanix AHV

- 機能はハードウェアアプライアンスと同等となります※1
- バックアップファイルは相互互換性があります
- 冗長構成はハードウェア版/クラウド対応版の**混在構成が可能です**

※1: USBメモリ、UPS連携等のハードウェア依存機能を除く

- VMware ESXi動作環境

VMware ESXi 6.0以上 (ハードウェアバージョン7)

※リリースバージョンにより動作確認済み環境が異なります

- Nutanix AHV動作環境

AHV + Prism Central環境

※リリースバージョンにより動作確認済み環境が異なります

ハードウェア仕様は

- 仮想CPU数: 4個
- メモリサイズ: 4GB
- 仮想HDD容量: 60GB
- NIC: eth0・eth1
- CD/DVDドライブ: 未使用

※各環境用の起動イメージの貸出は随時お受け付け中ですのでご相談ください。

クラウド対応版



◆ AWS

◆ Microsoft Azure

- 機能はハードウェアアプライアンスと同等となります※1
- バックアップファイルは相互互換性があります※2
- 冗長構成はハードウェア版/VA版と**混在構成が可能です**

※1: Eth0のみ、USBメモリ利用・UPS連携不可等の一部プラットフォーム依存機能を除く

※2: ネットワーク設定等の一部項目は反映されません

※3: 利用可能なサービス・機能はクラウドサービス側の仕様に依存します

■ AWS対応版動作環境

- インスタンスタイプ
- ストレージ
- ネットワークインターフェイス

※Amazon Elastic Compute Cloud上で動作

: t2.medium以上 (vCPU2コア、メモリ 4GB)

: 60GB 汎用SSD (gp2)

: eth0 (ルーティング設定等はVPCに依存)

AWS



Amazon EC2

■ Azure対応版動作環境

- アーキテクチャ
- 動作確認済みサイズ
- ストレージ
- ネットワークインターフェイス

※Microsoft Azureの仮想マシン上で動作

: x86_64

: Standard_B2s (2vpcpu、メモリ 4GiB)

: 60GB

: eth0 (ルーティング設定等はAzureに依存)

Microsoft
Azure

(Microsoft Azure Marketplace上から動作イメージは入手可能)

注意:

- ・クラウド対応版の機能はアプライアンス機と同等ですが、性能については、クラウド環境の影響を受けるため、アプライアンス機と同等の性能を保証するものではありません。
- ・クラウド対応版を利用するために必要なクラウド環境上での動作費用はお客様負担となります。
- ・Azure環境でDHCPサービスはクラウドサービス仕様として未サポートとなります。

RADIUS GUARD Utilityの紹介

■ RADIUS GUARD Utilityとは

- RADIUS GUARD S導入ユーザー限定の**無償ツール**
- ご利用者様の構築/運用を支援する補助ツールセット
- RADIUS GUARDシリーズの有効ライセンスをお持ちのユーザーに提供
- Windowsアプリ(非インストール型)として提供

■ RADIUS GUARD Utilityのできること



無線の利用状況やIPの払出状況
はどうなってるだろう？

その疑問に！

- 特定ユーザー/端末の認証状況をソートしたい
- 払出IP/MACアドレス別の払出状況を把握したい
- 特定メッセージの発生傾向を確認したい



RADIUS GUARD UTILITY
ログ可視化ツール

- RADIUS GUARD Sのログを取り込んで詳細検索
- 検索キーワードの日別/時間別カウント数表示
- 検索結果の出力(抽出ログ/カウント結果CSV)



認証サーバーの動作を確認するの
に無線APと端末の用意は大変。。。。

その負担に！

- 設定した通りの認証動作を簡単に確認したい
- RGSの動作確認をしたい
- 認証動作の結果を残したい
- アカウントの認証確認をしたい



RADIUS GUARD UTILITY
RADIUS試験ツール

- PCから各種認証パケットの簡易試験
(PAP/CHAP/MS-CHAPv2/EAP-PEAP・TLS)
- 標準属性(Attribute)の追加が可能
- 試験結果のテキスト出力
- 連続試験条件の設定

RADIUS GUARD S連携Syslogサーバー（ハードウェア/VA版による提供）

- アプライアンス型のため、導入が容易なSyslogサーバー
- 各種ログをWEB-GUIで可視化するログ管理アプライアンス
- 受信可能な情報はSyslog(UDP/TCP)とSNMPトラップ(v1・v2c)
- 受信ログ条件毎のテンプレートを元に特定アクションの実施が可能

LOG@Adapter



RADIUS GUARD S



【各種アクション】

- ・テンプレート作成によるアクション指定が可能
(カウント・メール送信・SNMPトラップ等)

【ログ解析機能】

- ・RADIUS GUARD Sの認証ログを解析対象ログとして即時解析・分割格納する機能を搭載
- ・認証ログを見やすく可視可することが可能

No.	選択	アクション	送信日時	受信日時	ホスト	ポートタイプ	ポート	ユーザー	MACアドレス	IPアドレス	VID	CLASSID	ESSID	その他	設置場所
1	☐	ログイン	2018/09/20 15:09:00	2018/09/20 15:04:08	192.168.1.100 (192.168.1.100)		3	test	ab:13:74:c2:5e:a7	192.168.1.100	1				
2	☐	認証成功	2018/09/20 15:08:59	2018/09/20 15:04:07	192.168.1.100 (192.168.1.100)			test						radius auth	
3	☐	ログイン失敗	2018/09/20 15:08:29	2018/09/20 15:03:37	192.168.1.100 (192.168.1.100)		3	test	ab:13:74:c2:5e:a7	192.168.1.100	1				
4	☐	認証失敗	2018/09/20 15:08:29	2018/09/20 15:03:37	192.168.1.100 (192.168.1.100)			test						radius auth	

どうなった

いつ

どのスイッチ・ポートから

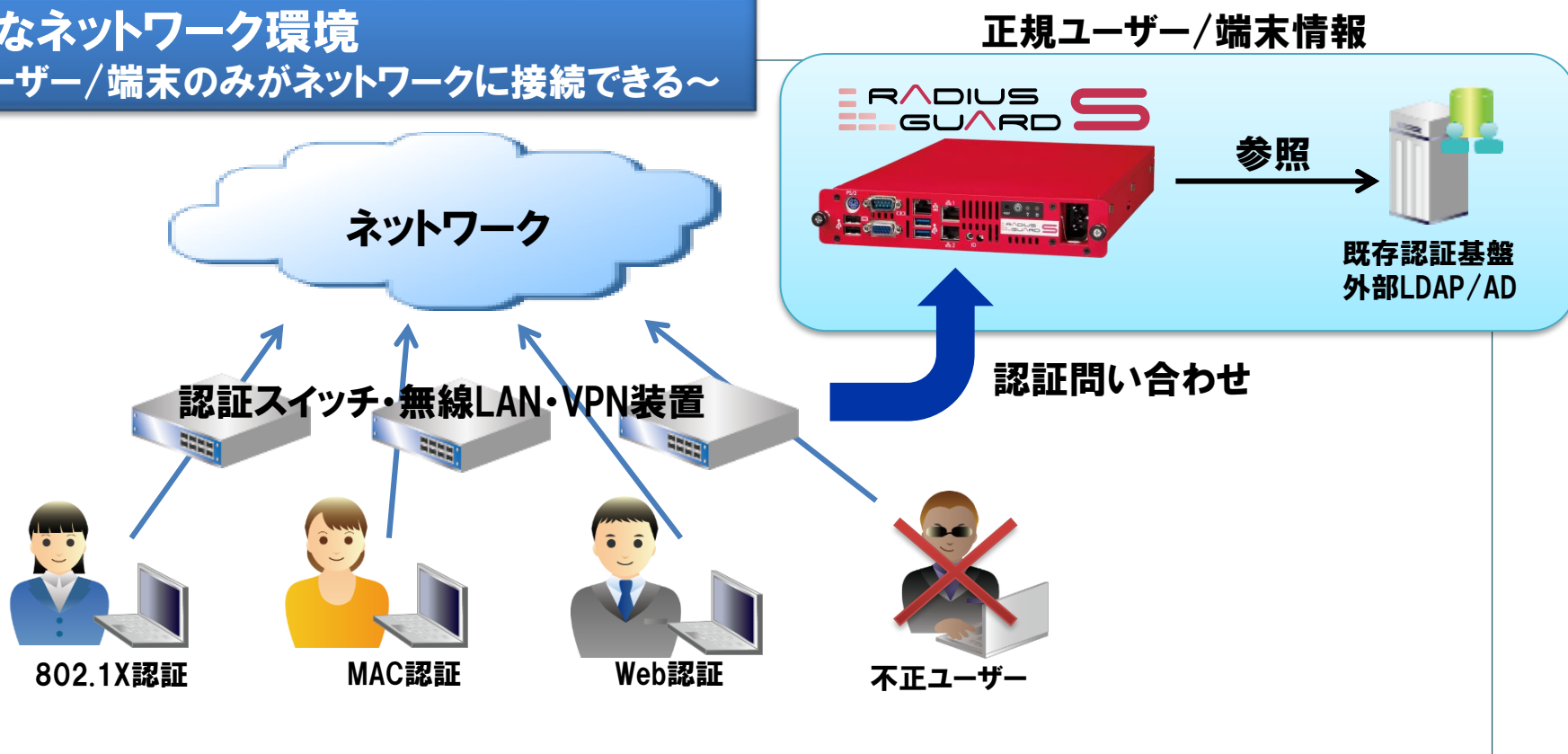
誰が・どのPCで

特長と機能：認証

- ・ 認証スイッチ、無線LAN、VPN装置などと連係してRADIUS認証
- ・ Web/MAC/802.1X (EAP-MD5/TLS/TTLS/PEAP) 認証に対応
- ・ RADIUSクライアントによらないライセンス体系
- ・ 外部LDAPやActive Directory を参照した認証も可能

セキュアなネットワーク環境

～正規ユーザー/端末のみがネットワークに接続できる～



さまざまなアクセス制御 その1

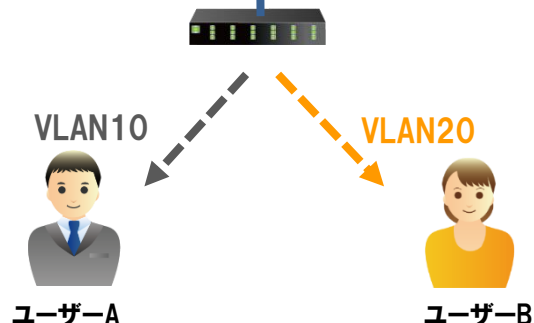
- ・ ユーザー・端末・証明書ごとに接続VLANを割り当てる
- ・ ユーザー・端末・証明書を所属させるディレクトリごとに接続VLANを割り当てる
(共通アトリビュート)

【運用例】 ユーザーごとに接続VLANを割り当てる

RADIUS GUARD S



ユーザー	VLAN
ユーザー A	10
ユーザー B	20

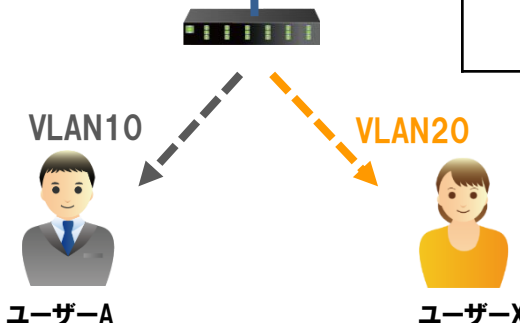


【運用例】 ディレクトリごとに接続VLANを割り当てる

RADIUS GUARD S



ディレクトリ	ユーザー	VLAN
営業	ユーザー A	10
	ユーザー B	
	ユーザー C	
技術	ユーザー X	20
	ユーザー Y	
	ユーザー Z	

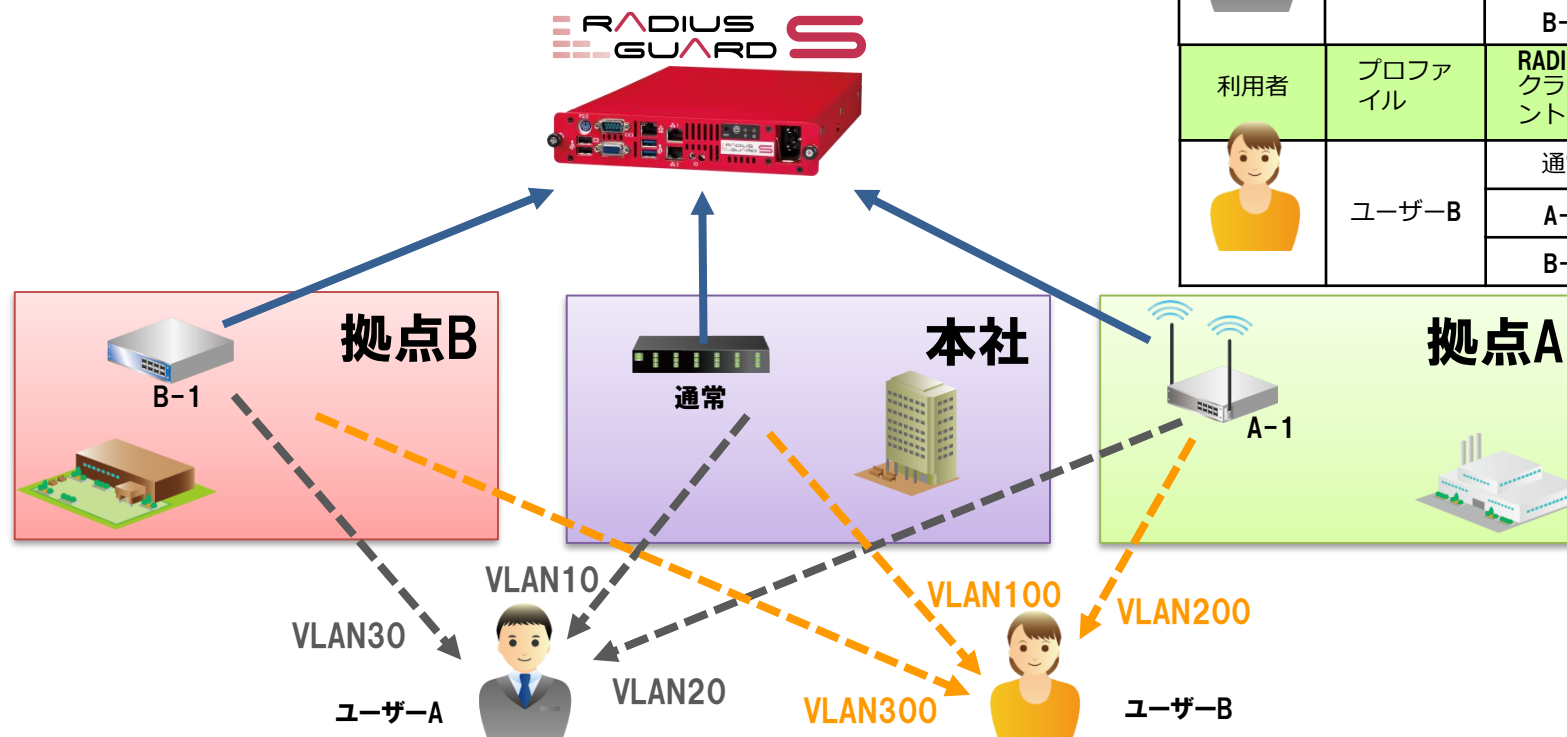


ユーザーを所属させる
ディレクトリごとに接続
VLANを管理できます！
営業=VLAN10
技術=VLAN20

さまざまなアクセス制御 その2

- ・ ユーザー・端末・証明書の接続VLANを、RADIUSクライアントグループごとに割り当てる
(ネットワークプロファイル&RADIUSクライアントグループ)

【運用例】
ユーザーの接続VLANを拠点ごとに割り当てる



RADIUS GUARD S 登録内容

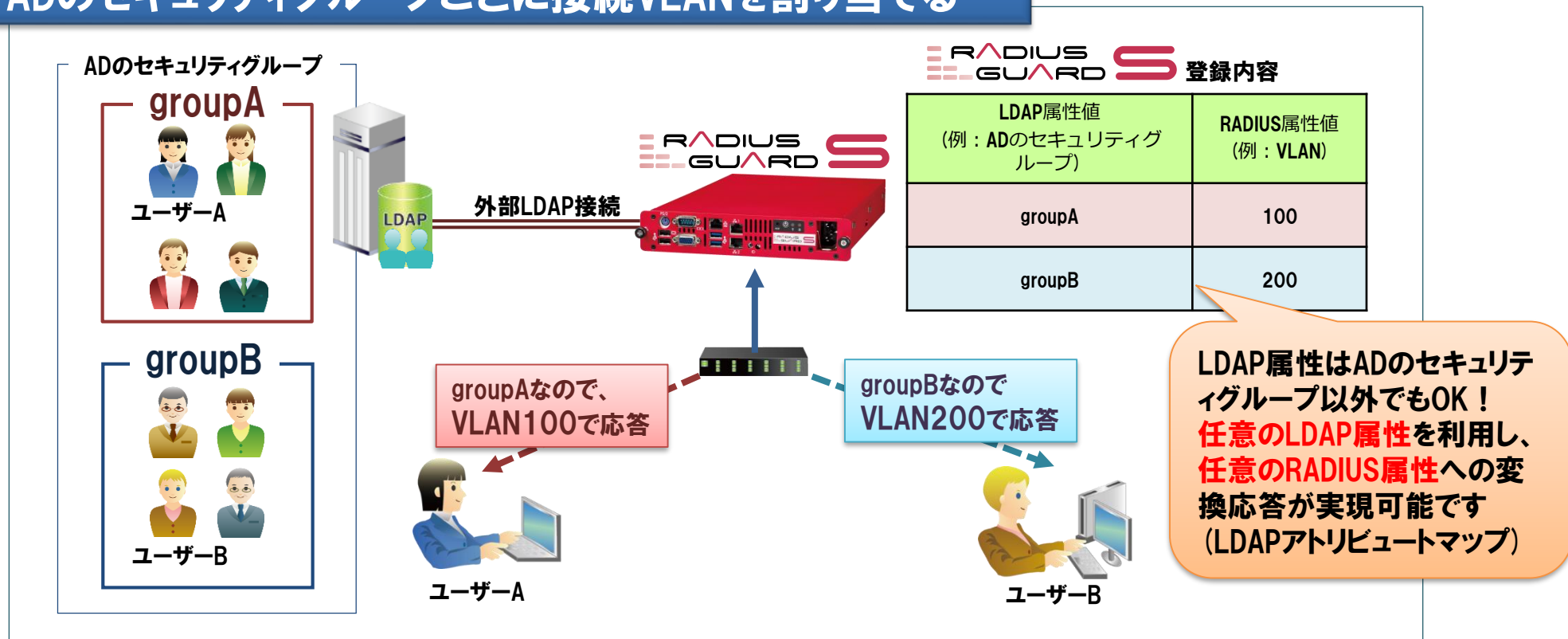
利用者	プロファイル	RADIUSクライアント	VLAN
	ユーザーA	通常	10
		A-1	20
		B-1	30
利用者	プロファイル	RADIUSクライアント	VLAN
	ユーザーB	通常	100
		A-1	200
		B-1	300

さまざまなアクセス制御 その3

- ・ 外部LDAPの属性値に応じて接続するVLANを割り当てる
(ネットワークプロファイルの外部LDAPアカウント適用)
(LDAPアトリビュートマップ…LDAP属性とRADIUS属性のマッピング機能)

【運用例】

ADのセキュリティグループごとに接続VLANを割り当てる



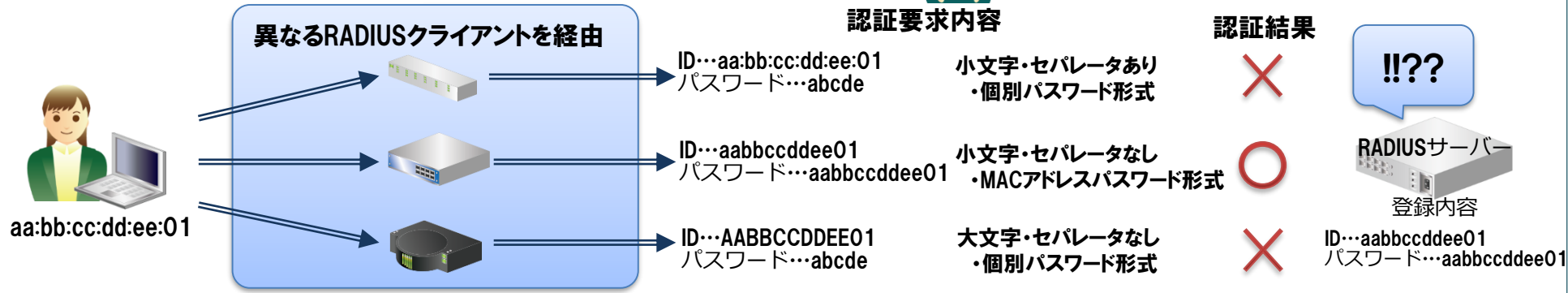
MACアドレス形式の混在環境に対応

差別化
ポイント！

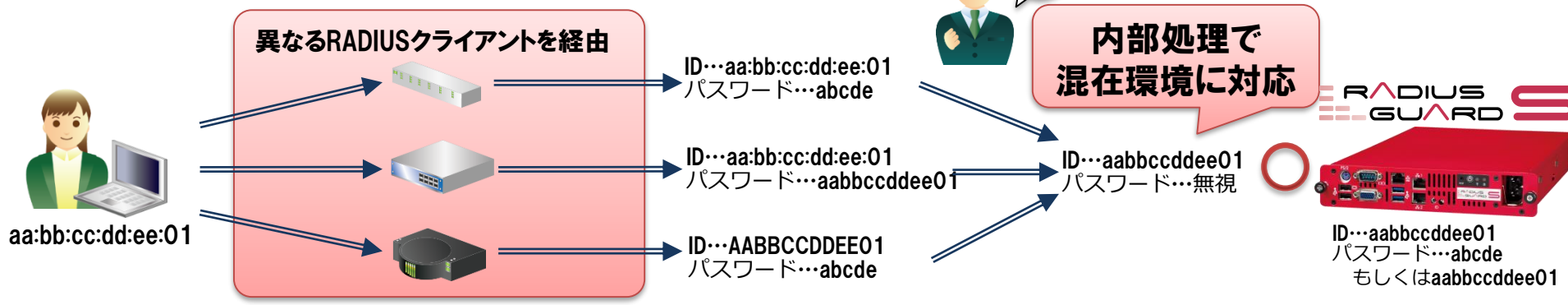
SCSK
夢ある未来を、共に創る。

- ・ 大文字小文字・セパレータ記号を無視して認証
- ・ MACパスワードは、共通文字列でもMACアドレスでもOK
- ・ MACパスワードを無視して認証することも可能

一般的RADIUSサーバー製品



RADIUS GUARD S だったら...



特長と機能：アカウント管理

アカウント管理機能の概要

- ・ ローカルデータベースで、ユーザー・端末・証明書の管理
- ・ 200～200,000アカウントの管理が可能
- ・ ディレクトリ単位での管理
- ・ 柔軟な管理者設定 (ディレクトリ管理者/承認のみ/DHCP管理) 分かりやすい
- ・ 表示項目のカスタマイズ

The screenshot shows the RADIUS GUARD S management tool interface. On the left is a sidebar menu, in the center is a directory tree, and on the right is the main account management area. Red boxes and arrows highlight specific features, with yellow boxes labeling parts of the interface.

設定メニュー (Setting Menu): Points to the left sidebar menu.

ディレクトリツリー (Directory Tree): Points to the central directory tree showing 'home', 'ゲスト用', '営業部', and sub-groups.

設定画面 (Setting Screen): Points to the top tabs 'ユーザー' (User), '端末 (MAC)' (Terminal (MAC)), and '証明書' (Certificate).

3ペインでアカウント管理がより分かりやすくなりました (Account management is easier with 3 panes): A general annotation for the three-pane layout.

ディレクトリごとにユーザー・端末・証明書各アカウントをタブ分けして個別管理 (Tab management by directory): Points to the tabs in the top right.

表示項目列は必要なものだけをカスタマイズ可能 (Customizable display columns): Points to the column headers of the account list table.

No.	☐	ユーザーID ▲▼	姓 ▲▼	名 ▲▼	アカウント管理者 ▲▼	アカウント有効期限
1	☐	guest01			naadmin	無期限
	☐	guest02			naadmin	無期限
	☐	sales-user01			naadmin	
	☐	sales-user02			naadmin	
5	☐	user01	user	01	naadmin	
6	☐	user02	user	02	naadmin	

- ・ 管理者による一括/個別登録、ユーザーによる申請登録が可能
- ・ アカウント**定期一括インポート**(追加・更新・削除) / エクスポート
- ・ 表示項目のカスタマイズ
 - 利用内容に合わせた項目設定が柔軟に設定できる！

ユーザー 端末(MAC) 証明書

アカウント登録

登録用サンプルファイル ダウンロード

一括登録 ▼

ディレクトリ home > 利用者

ユーザーID ※ (半角英数記号 64文字以内) user01

姓 (256文字以内) user

名 (256文字以内) 01

連絡先電話番号 (半角数字記号32文字以内) 03-XXXX-XXXX

通知用メールアドレス (半角英数字記号256文字以内) user01@aaauser.com

パスワード ※ (半角英数字記号256文字以内)

説明 担当課長

ユーザー登録画面

ユーザー 端末(MAC) 証明書

アカウント登録

登録用サンプルファイル ダウンロード

一括登録 ▼

ディレクトリ home > 利用者

MACアドレス ※ (半角英数記号 64文字以内) aabbcc445566

OS (256文字以内) windows

コンピューター名 (256文字以内) computer01

端末ユーザー名 (256文字以内) user01

ドメイン (256文字以内) aaauser.com

〇〇事業所利用端末 x

利用開始日時 (HH) 2015-05-06 00:00

端末登録画面

アカウント種別に応じて
登録項目設定を自由に
カスタマイズ可能

アカウント棚卸機能

差別化
ポイント！

SCSK
夢ある未来を、共に創る。

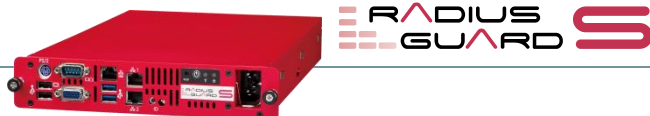
- こんなことに困ったこと、ありませんか…？
 - 登録したアカウントの利用状況を知りたい
 - 長期間使われていないアカウントを棚卸したい
 - 有効期限が過ぎたアカウントを棚卸したい



自動削除ではなく、
管理者が利用状況
を確認してからの手動
削除も可能！



認証ログを追わなくても、アカウントが最後に認証した日が一目でわかります。
さらに、長期末使用のアカウントを洗い出し、自動無効 & 削除までお任せ！



RADIUS
GUARD S

ディレクトリA (端末用)

最終認証から半年後に無効化・1年後に削除

最終認証日	ステータス
今日	利用可能
半年前	無効
1年前	削除

ディレクトリB (ゲスト用)

最終認証から1週間後に無効化 & 削除

最終認証日	ステータス
今日	利用可能
1週間前	無効
1週間前	削除

ディレクトリC (証明書用)

最終認証から3か月後に削除

最終認証日	ステータス
今日	利用可能
1か月前	利用可能
3か月前	削除 (失効)

アカウント棚卸機能～外部LDAPとの連動～

差別化
ポイント！

SCSK
夢ある未来を、共に創る。

・ 外部LDAPアカウント連動削除機能

- 外部LDAPからアカウントが削除された際に、ひも付け内部アカウント（端末／証明書）を連動削除
- 外部LDAPの属性値に応じて、ひも付け内部アカウント（端末／証明書）を削除

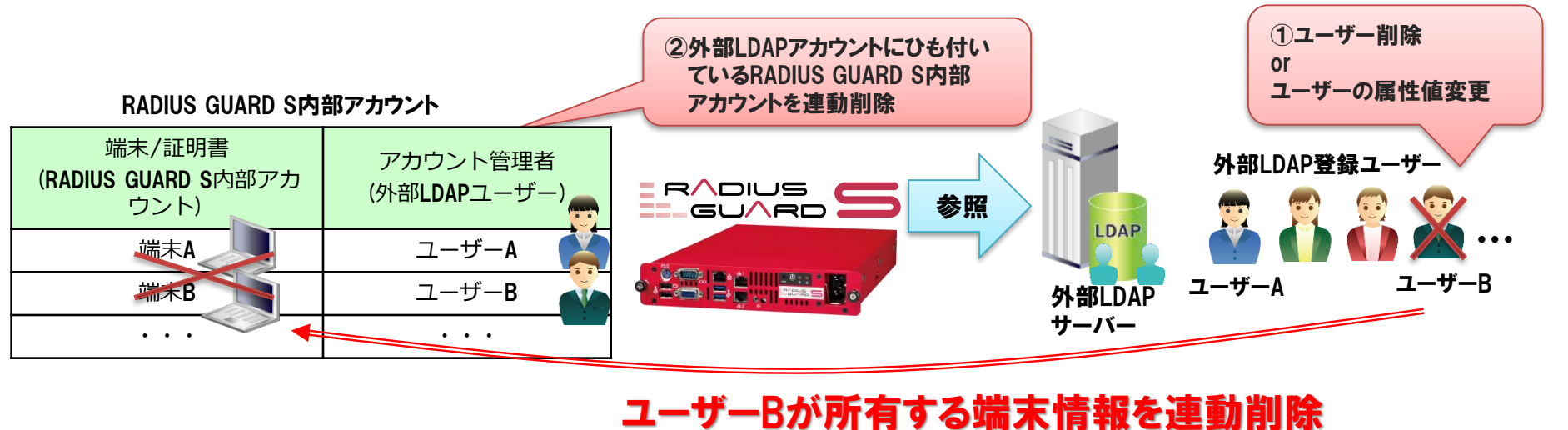
※連動削除機能で削除可能な内部アカウントは端末アカウントと証明書アカウントが対象です。

※ここが特長！ ひも付け内部アカウントとは・・・

RADIUS GUARD Sでは、内部アカウントを登録する際に、そのアカウントを管理所有するひも付けユーザー「アカウント管理者」を登録することができます。

「アカウント管理者」を外部LDAPアカウントとすることで、外部LDAP連動削除機能が利用できます。

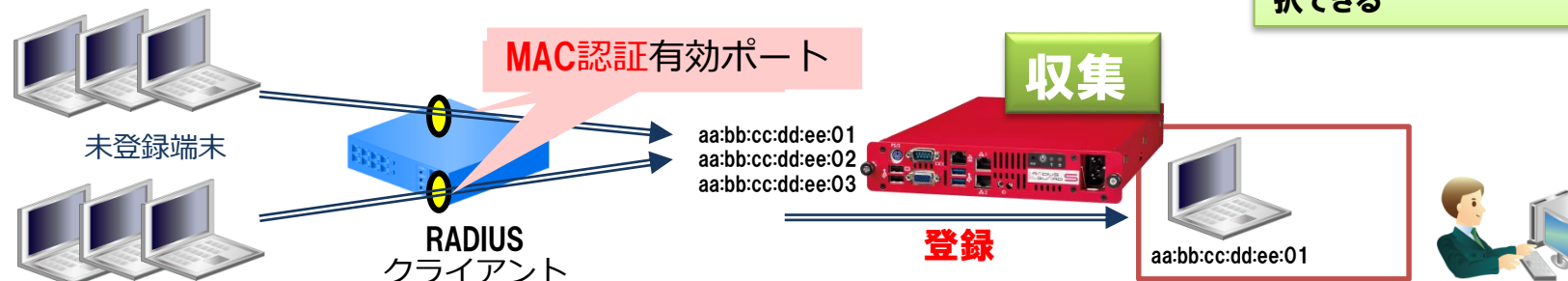
ユーザーツールを利用したアカウント申請時には、申請者がアカウント管理者として自動でひも付くのでとても便利です。この場合、「アカウント申請者＝アカウント管理者」と言い換えることもできます。



■ MACアドレス認証端末の自動収集・登録

□ 未登録端末のMACアドレスを収集してリスト化 & 自動登録

登録候補リストからの選択
登録、および自動登録が選
択できる



こんな便利な使い方！～自動収集時には属性適用も可能～

- ・特定のRADIUSクライアント配下のみ自動収集エリアとする
- ・自動収集した端末は特定VLANに隔離して利用させる、特定ロールに割り当てる

■ Web認証端末の自動登録

□ Web認証に成功した端末のMACアドレスを収集して自動登録

□ 認証ユーザーとMACアドレスのひも付け登録が可能

Web認証ユーザーと
端末のMACアドレスが
ひも付けで登録される



特長と機能：CA（証明書発行・管理）

- ・ クライアント/サーバー証明書の発行・管理、失効リスト管理
- ・ 管理者による一括/個別発行、ユーザーによる発行申請が可能
- ・ 複数のCAの運用で、証明書の移行もスムーズ
- ・ スマートフォンへの発行実績も豊富

CA設定

入力規則 名前(cn)・都道府県(st)を入力して登録

認証局 ☒ 自己認証局 ☐ 下位認証局

自己認証局情報設定

名前(cn)※ (半角英数字記号 64文字以内)

国(c)

都道府県(st)※ (半角英数字記号 128文字以内)

市区町村(t) (半角英数字記号 128文字以内)

組織名(o) (半角英数字記号 57文字以内)

部署(ou) (半角英数字記号 64文字以内)

メールアドレス(e-mail) (半角英数字記号 128文字以内)

有効期限

フレンドリー名 (半角英数字記号 64文字以内)

暗号アルゴリズム

署名アルゴリズム

鍵長

【CA設定画面】

home > 利用者

ユーザー 端末(MAC) 証明書 ディレクトリ

証明書タブを選択

アカウント一覧

アカウント登録 アカウント一括ダウンロード 表示設定

検索

該当するデータは 4件あります。

1 / 1 ページ

操作 処理を選択してください 実行

一括処理操作メニューより
処理を選択して実行

処理を選択してください

- 選択したアカウントを削除する
- 選択したアカウントを移動する
- 選択したアカウントのネットワーク利用を有効にする
- 選択したアカウントのネットワーク利用を無効にする
- 選択したアカウントの証明書を発行する
- 選択したアカウントの証明書1を発行する
- 選択したアカウントの証明書2を発行する
- 選択したアカウントの証明書を失効する
- 選択したアカウントの証明書1を失効する
- 選択したアカウントの証明書2を失効する
- 選択したアカウントの証明書をダウンロードする
- 選択したアカウントの証明書1をダウンロードする
- 選択したアカウントの証明書2をダウンロードする

No.	☐	cn	発行済み証明書1サブジェクト	発行済み証明書1有効期限	証明書1	証明書2	編集
1	☐	user01	ou=user,dc=home	2025-04-26 00:00:00	失効 DL	-	
2	☐	user02	ou=user,dc=home	2025-04-26 00:00:00	失効 DL	-	
3	☐	user03			発行	-	
4	☐	user04			発行	-	

発行済み証明書の有効期限がリスト表示される

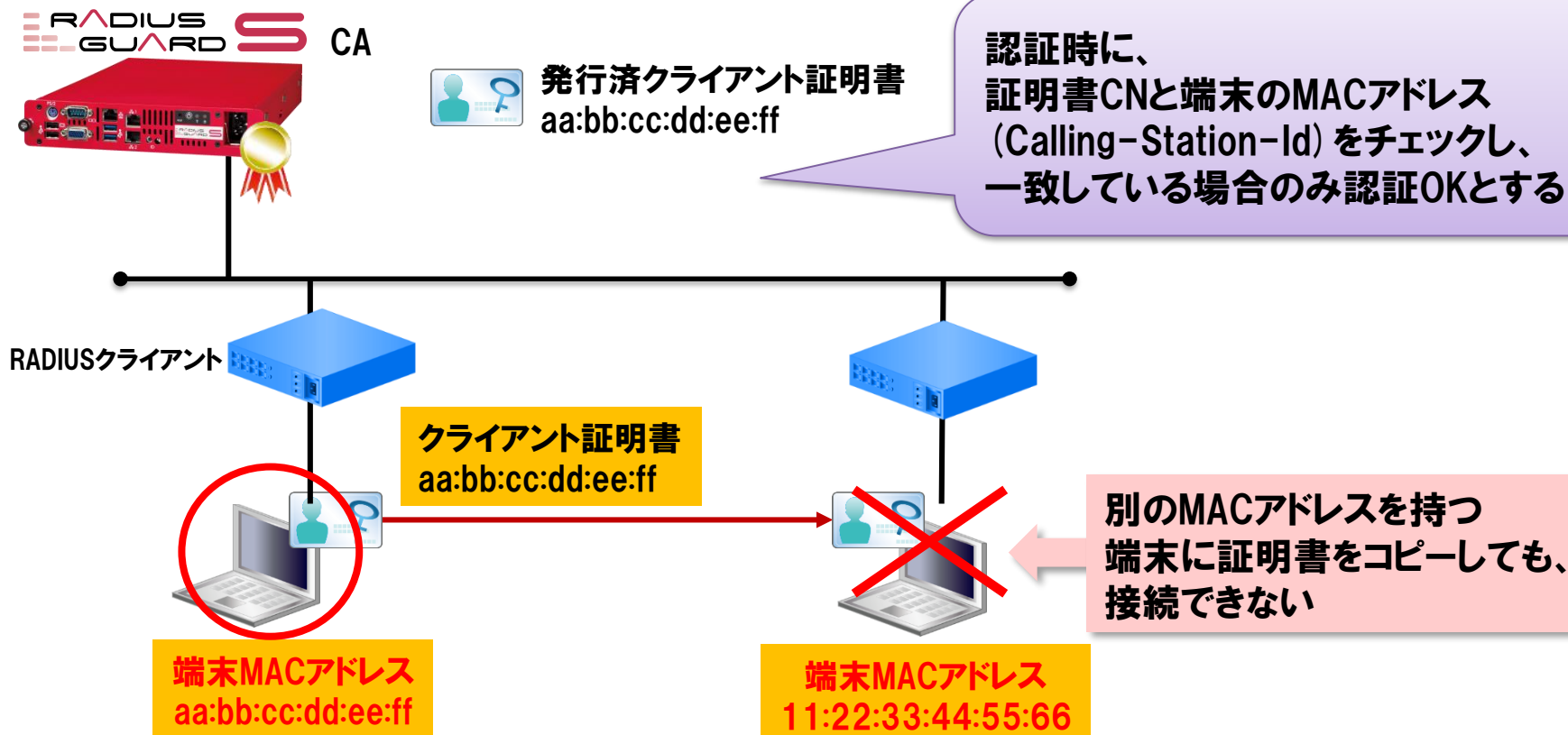
処理をしたいアカウントを選択

各アカウント個別に処理したい場合は、
アカウント個別の処理ボタンで発行・失効を実施

【証明書アカウント管理画面(証明書発行例)】

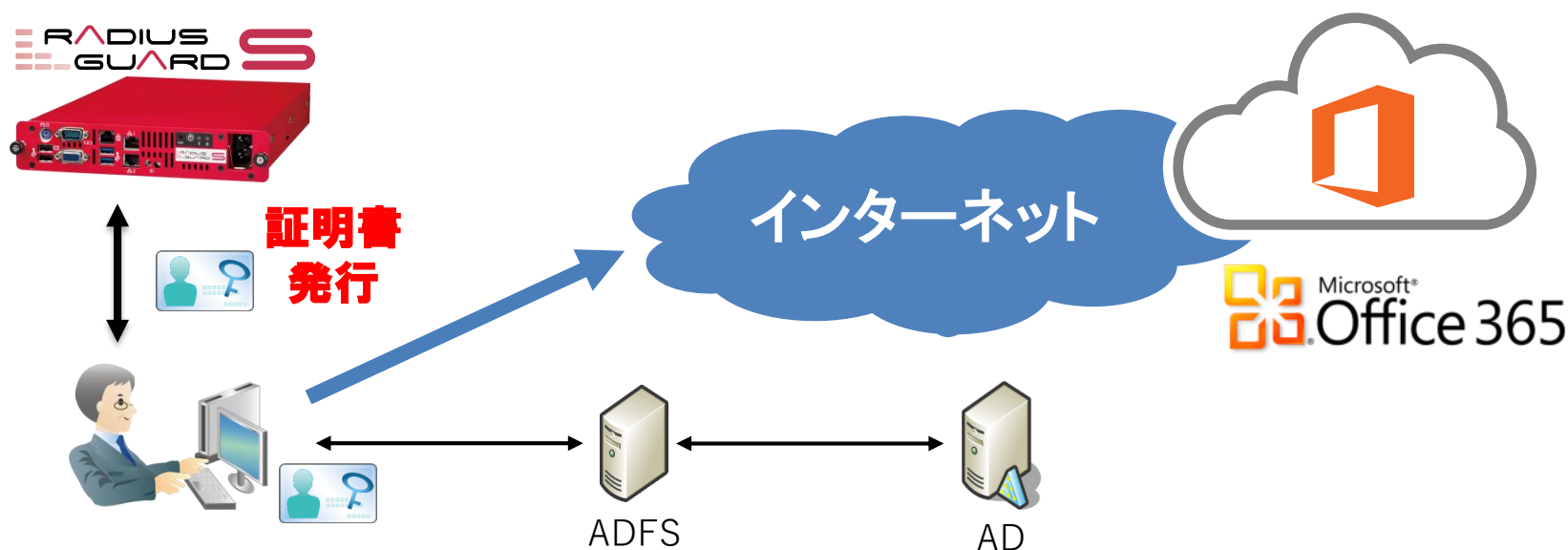
- ・ 証明書CNと端末のMACアドレス(Calling-Station-Id)との不一致チェック
- ・ 証明書と端末の1対1ひも付けが可能

しくみ



- ・ ADFS環境のデバイス認証に利用可能なクライアント証明書が発行に対応
- ・ クラウドサービスよりも安価にクライアント証明書の維持管理が可能

しくみ



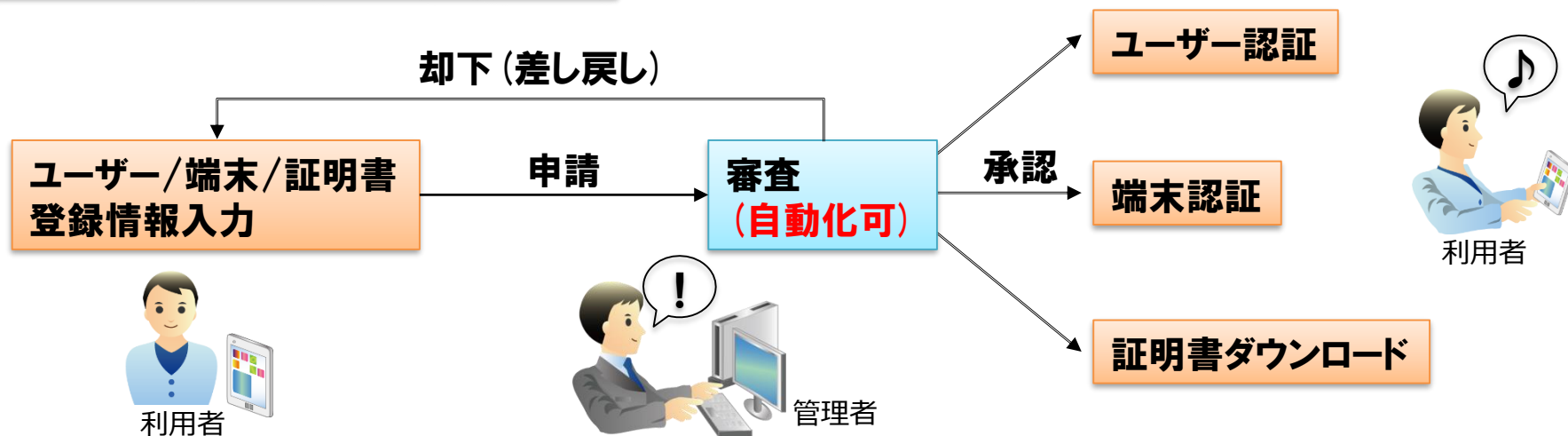
証明書認証による認証ルールを追加し信頼された証明機関から発行された証明書を有するデバイスからの認証要求のみを認可するように設定することで、クライアント証明書を持つ端末からのアクセスに制限可能

特長と機能：ユーザーツール

ユーザーに任せて管理者負荷を軽減しませんか
紙ベースでの申請、もうやめませんか

- ・ ユーザーツールとは、利用者向けのWebインタフェース
 - 利用者によるユーザー/端末/証明書の申請
 - 管理者による審査履歴管理
 - 証明書のダウンロードや更新
 - パスワード有効期限通知 & 変更 & 再登録

申請・承認ワークフローの概要



柔軟な申請ポータル#1

- ・ 3種（ユーザー/端末/証明書）の申請を最大**256**ポリシーの作成が可能
 - 異なる立場の利用者に対し、それぞれの申請方式を提供できる（社員、外注、ゲスト…）
 - 申請ポリシーごとに異なるポータルURLで提供することも可能

Ver. 6.00.00
管理ツール

マスター : 稼働中
DHCPプライマリ : 稼働中

アカウント一覧
環境設定
CA
RADIUS
アカウント操作(内部DB)
外部LDAP/AD参照
ユーザーツール
申請ポリシー
申請審査
審査結果
表示設定
オプション設定
DHCP
Shibboleth
外部システム連携
ログ参照
メンテナンス
ログアウト

申請ポリシー編集

①アカウント種別（ユーザー・端末・証明書）を選択

表示順 (半角数字 0~999) 0

名称※ (256文字以内) ユーザ申請

英語名 (256文字以内) ユーザ申請

表示設定※ ユーザーツール表示設定 ▼

ログインアカウント

②申請ポリシー設定

☐ 申請用アカウント
ID

☐ 変更する・変更しない
PW

☐ 内部アカウント 選択 未選択

☒ 外部LDAP/ADアカウント colorsAD ▼

検索BaseDN

☒ 認証用と共通
dc=colors,dc=scs,dc=co,dc=jp

☐ 指定する

検索filter

☒ 認証用と共通
(|(sAMAccountName=%U)(servicePrincipalName=%U))

☐ 指定する

※事前に外部LDAP/AD参照＞外部LDAP/AD登録の設定を行ってください

☐ 認証不要

【申請ポリシー作成画面】

スマートデバイス対応ページも！

e | English

RADIUS GUARD S

ID

パスワード

☒ ユーザ申請
☐ MAC申請
☐ 証明書申請

ログイン

③反映

【ユーザーツール申請ポータル】

柔軟な申請ポータル#2

・ 申請画面イメージ

- ユーザー/端末/証明書の申請に必要な基本入力フォーマットを提供
- 入力項目を自在にカスタマイズ可能 (必須/任意/表示のみ/非表示の選択)

ユーザー申請

ID/PW自動発行対応

ユーザー申請

申請者ID user01
ユーザーID ※ ユーザーID自動割り当て
(半角英数記号 64文字以内)
ディレクトリ
姓 (256文字以内)
名 (256文字以内)
アカウント管理者 user01
アカウント利用開始日時 (yyyy/MM/dd HH) 2015-05-13 19:00:00
メールアドレス (半角英数記号 256文字以内)
通知用メールアドレス (半角英数記号 256文字以内)
1行1アドレス 最大 5 件

端末申請

端末申請

申請者ID user01
端末情報
MACアドレス ※ aabbcc112233
(半角英数記号 64文字以内)
OS Windows
(256文字以内)
ディレクトリ
端末名 (256文字以内)

証明書申請

クライアント証明書申請

申請者ID user01
cn ※ user01-cert
(半角英数記号 64文字以内)
ディレクトリ
証明書アカウント名 (256文字以内)
アカウント管理者 user01
通知用メールアドレス (半角英数記号 256文字以内)
1行1アドレス 最大 5 件
30文字以内 (確認用)

項目	表示名(日本語)	表示名(英語)	申請画面	編集画面	非表示
ディレクトリ	日)ディレクトリ 英)Directory		表示のみ	表示のみ	
ユーザーID	日)ユーザーID 英)User ID		必須	表示のみ	
管理番号	日)管理番号 英)Management Number		非表示	非表示	
姓	日)姓 英)Last Name		任意	任意	✓
名	日)名 英)First Name		任意	任意	✓

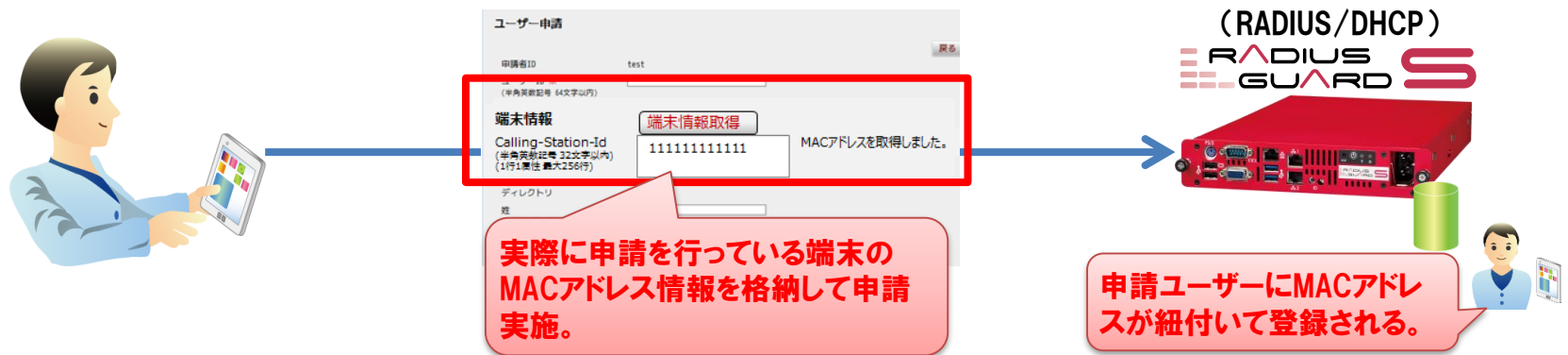
表示設定

申請方式ごとに入力フォーマットを
自在にカスタマイズ可能！

ユーザーアカウントへのMACアドレス自動登録機能

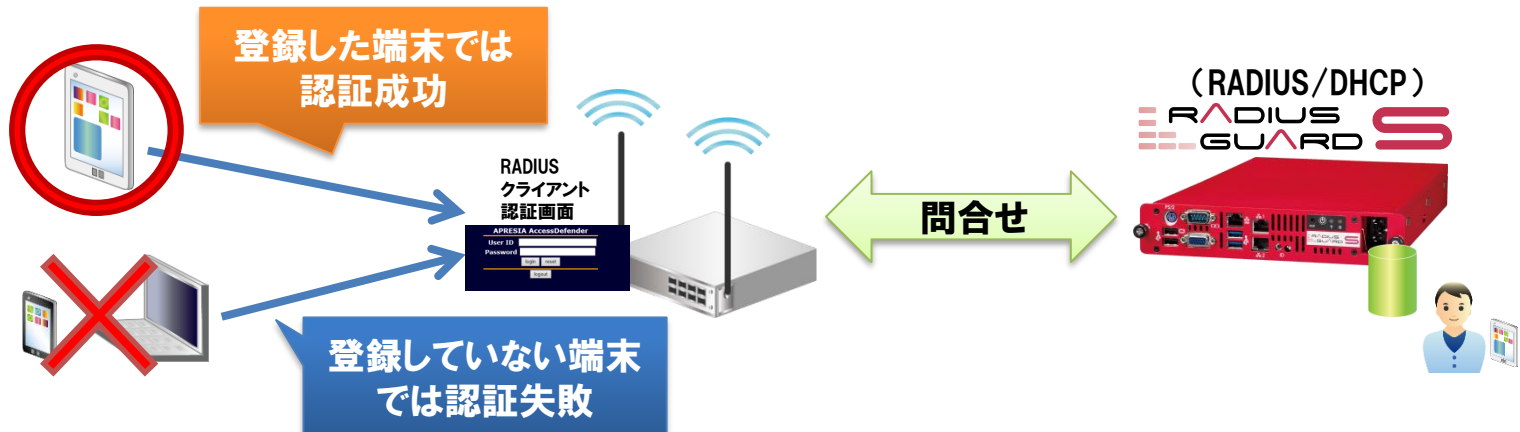
- ・ ユーザーアカウント申請を行う際に、申請端末のMACアドレス情報を自動取得してCalling-Station-ID属性へ自動格納
- ・ 発行されたユーザーアカウントは、申請した端末のみでネットワーク接続が可能
- ・ 申請者、発行されたアカウント、使用端末の紐づけ管理に

申請



認証

同じユーザーアカウントで
認証を行っても…



※DHCPオプションが必要な機能となります。

アカウント申請管理の悩みを解決

差別化
ポイント！

SCSK
夢ある未来を、共に創る。

・利用シーン

- 企業内の来客・ゲスト用ネットワークや入院患者向けのインターネット接続の提供
- 学校や公共スペース、観光地など、不特定多数へのネットワーク提供
- 企業内の個別調達PCや学生向けのMAC認証環境における申請ワークフローとして

・アカウント申請ワークフローを利用すると

- 各利用者に個々のアカウントを利用させることで、**証跡管理や利用状況を把握**
- **棚卸機能を併用し**、有効期限後の自動削除を行うことも可能

・端末登録にユーザーはクリックのみ

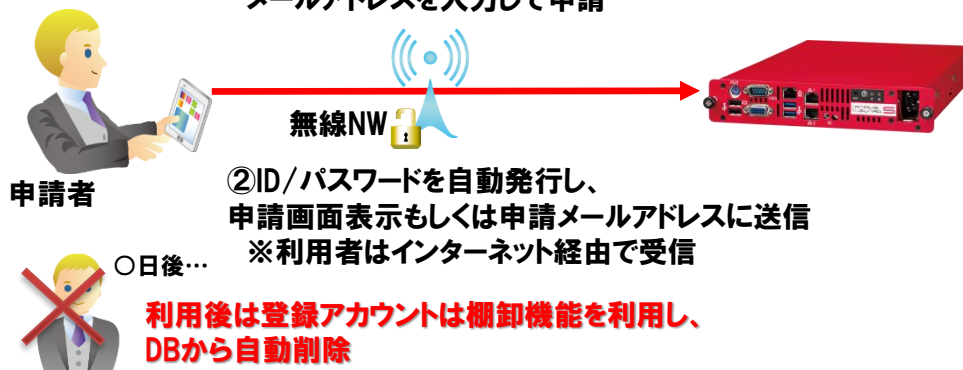
- **MACアドレス、OS、端末ユーザー名、コンピュータ名、ドメイン名を自動取得**して登録
- 端末登録時には申請者情報をひも付け登録（外部LDAPアカウントも利用可）



紙ベース申請や、認証DBと連動しない手間のかかるアカウント申請から解放！

一次利用アカウントの簡単申請

- ① 申請用ネットワーク経由で、RADIUS GUARD Sのアカウント申請画面にアクセスし、メールアドレスを入力して申請



MAC認証の端末の簡単申請

- ① 申請用ネットワーク経由で、RADIUS GUARD Sのアカウント申請画面にアクセス



証明書の運用の悩みを解決

差別化
ポイント！

SCSK
夢ある未来を、共に創る。

・ 申請ユーザー情報で証明書を自動発行

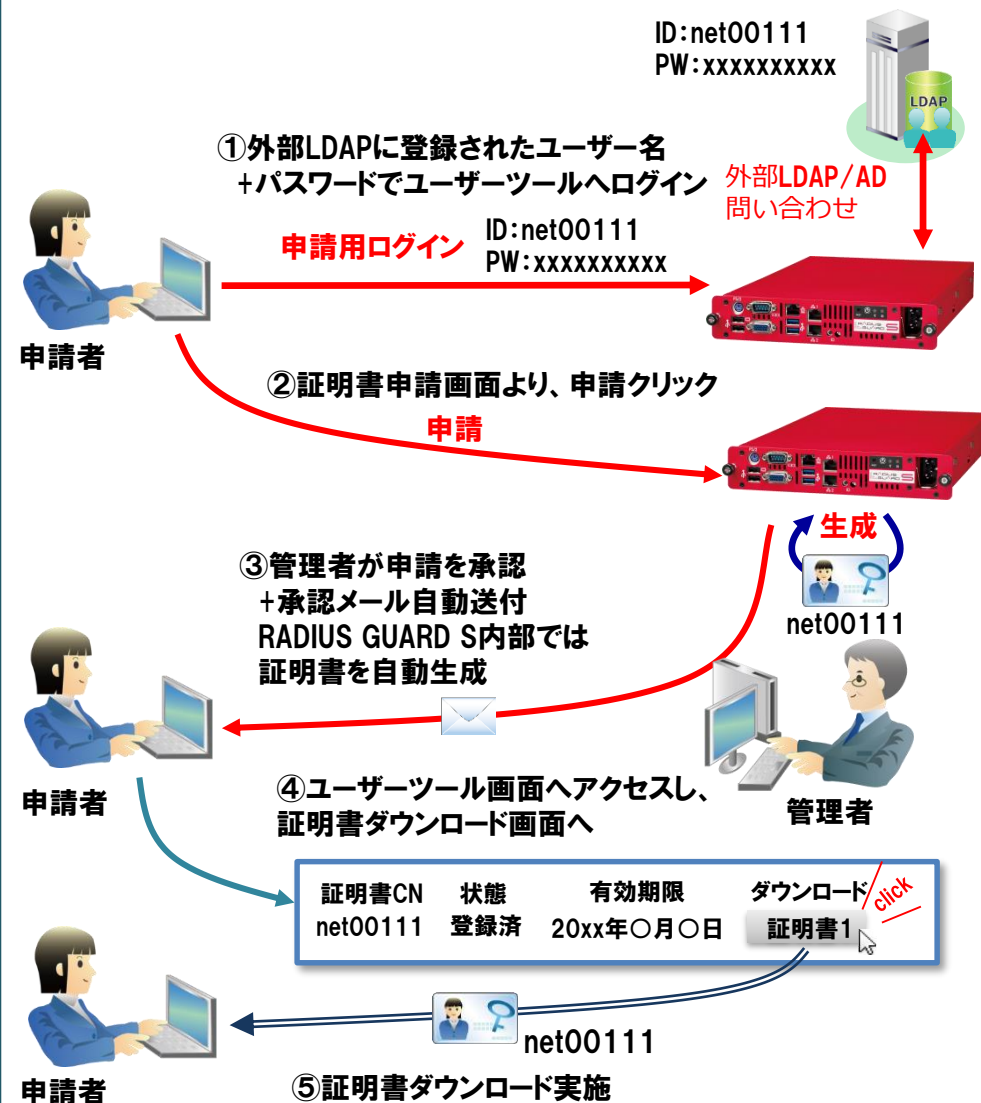
- 申請画面にログインすると、自分の名前の証明書がダウンロードできる
- 申請者のログインIDを証明書CNに自動引用してクライアント証明書を発行するしくみ=>管理者による証明書の事前作成が不要！
- 申請者のログインIDに外部LDAP/ADアカウントを利用することで、外部LDAP/ADのアカウント名の証明書が発行できる

・ 証明書の更新

- 有効期限が切れた証明書をユーザーが更新するしくみ
- 有効期限切れ警告メール通知
→証明書を再発行→ダウンロード

事前に証明書を作成しておかなくても、簡単にユーザーベースの証明書が発行できるのが便利！

申請ユーザー情報で証明書を自動発行



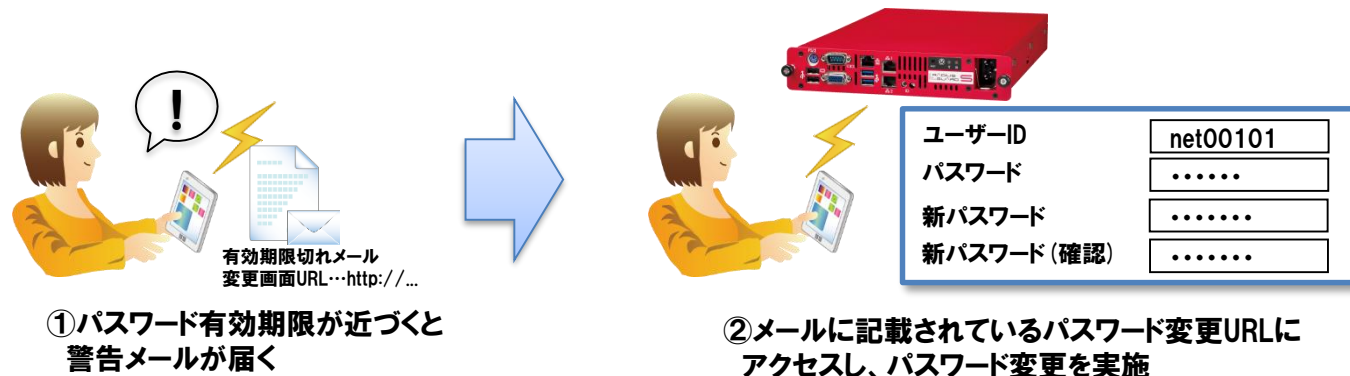
パスワードの運用の悩みを解決

差別化
ポイント!

SCSK
夢ある未来を、共に創る。

■ パスワード変更(パスワード有効期限切れ)

□ 有効期限切れメール通知→パスワード変更画面→ID＋現パスワード＋新パスワード入力



■ パスワード再登録(パスワード忘れ)

□ パスワード再登録画面→ID＋登録済メールアドレス入力→パスコードをメール通知→パスコード＋新パスワード入力



特長と機能：DHCPサービス (要オプション)

DHCP機能 基本概要と特長

差別化
ポイント！

SCSK
夢ある未来を、共に創る。

・ 払い出し性能・制御

- 1筐体 (1グループ) の払い出しIPアドレス数は、**最大1万IP**までOK
払い出し性能は最大100IP/毎秒
- スコープ (サブネット) 数は1筐体で**2,048**の登録が可能
- 払い出し制御対象MACアドレスの登録管理 (**最大20万件**) が可能

・ 複数台運用時の統合管理機能

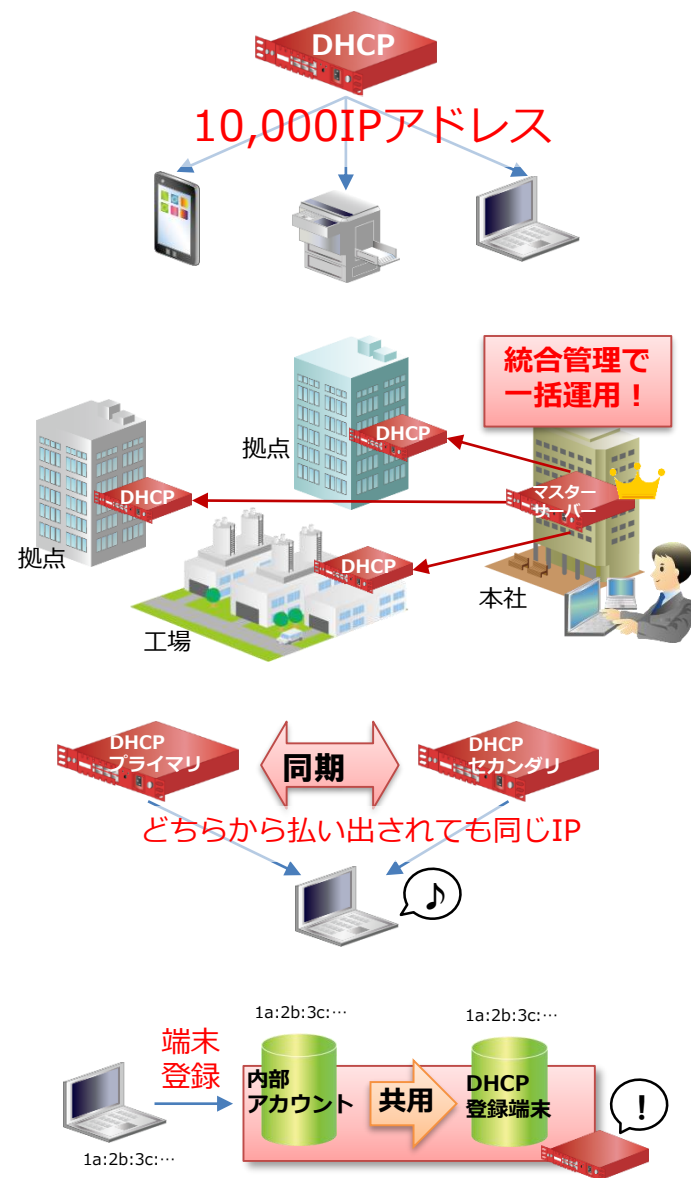
- 更に大規模環境の場合は、**複数のRADIUS GUARD SのDHCP設定情報を統合管理**する運用が可能
- 最大20台で構成

・ 筐体間の1対1冗長に対応

- DHCPプライマリ:セカンダリ間でリース情報リアルタイム同期
- 障害時も**同一の払い出しIP情報を引き継ぎつつ、新規払い出しIPの重複を防ぎます**

・ 認証用MACアドレスの転用(DHCP専用では不可)

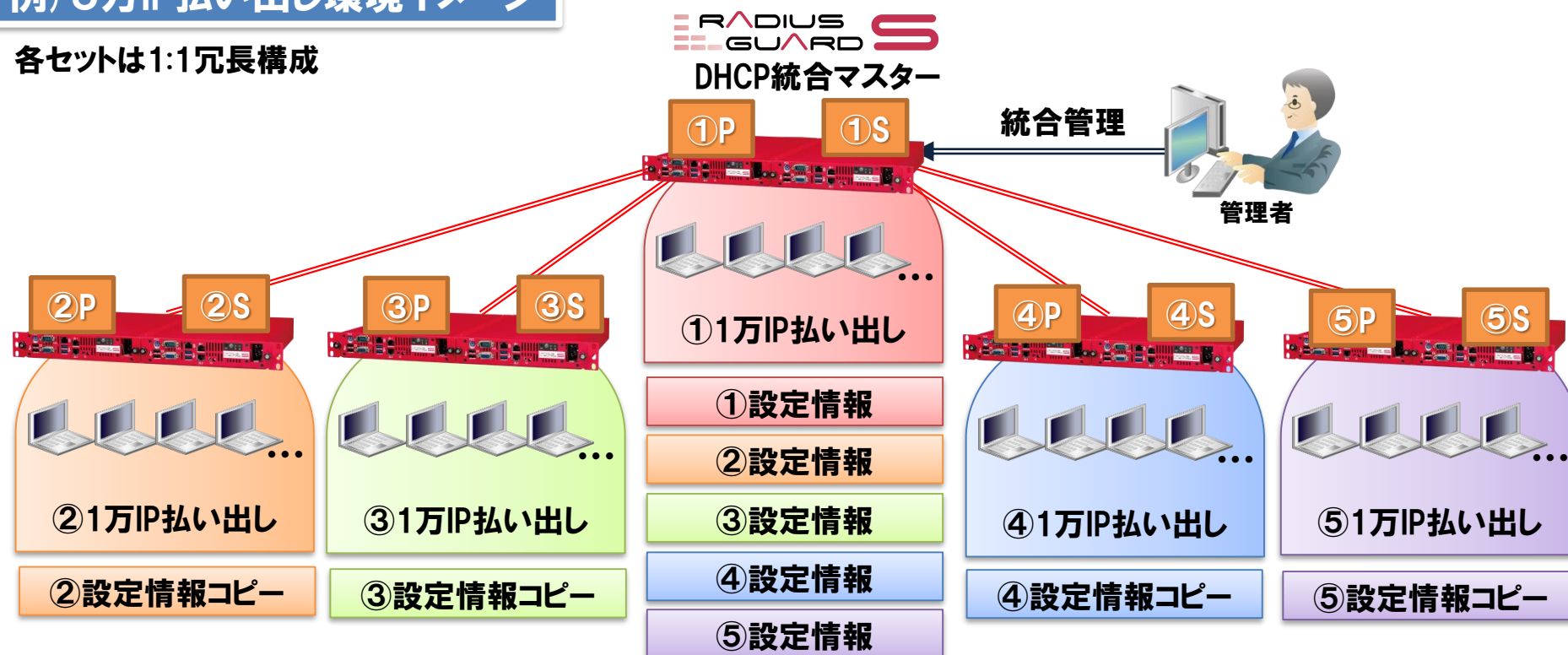
- **認証用MACアドレスを、DHCP払い出し情報に利用可能**
- ネットワーク認証性能に影響を与えない



- ・ 複数セットで多IP払い出し環境を構成可
 - プライマリ(P) : セカンダリ(S) の1セットで2048セグメント、1万IP払い出し
 - 統合マスターでは、最大20台の設定情報を統合管理
- ・ プライマリ(P) : セカンダリ(S) 間で、リース情報のリアルタイム同期
- ・ 各種DHCPオプションに対応

例) 5万IP払い出し環境イメージ

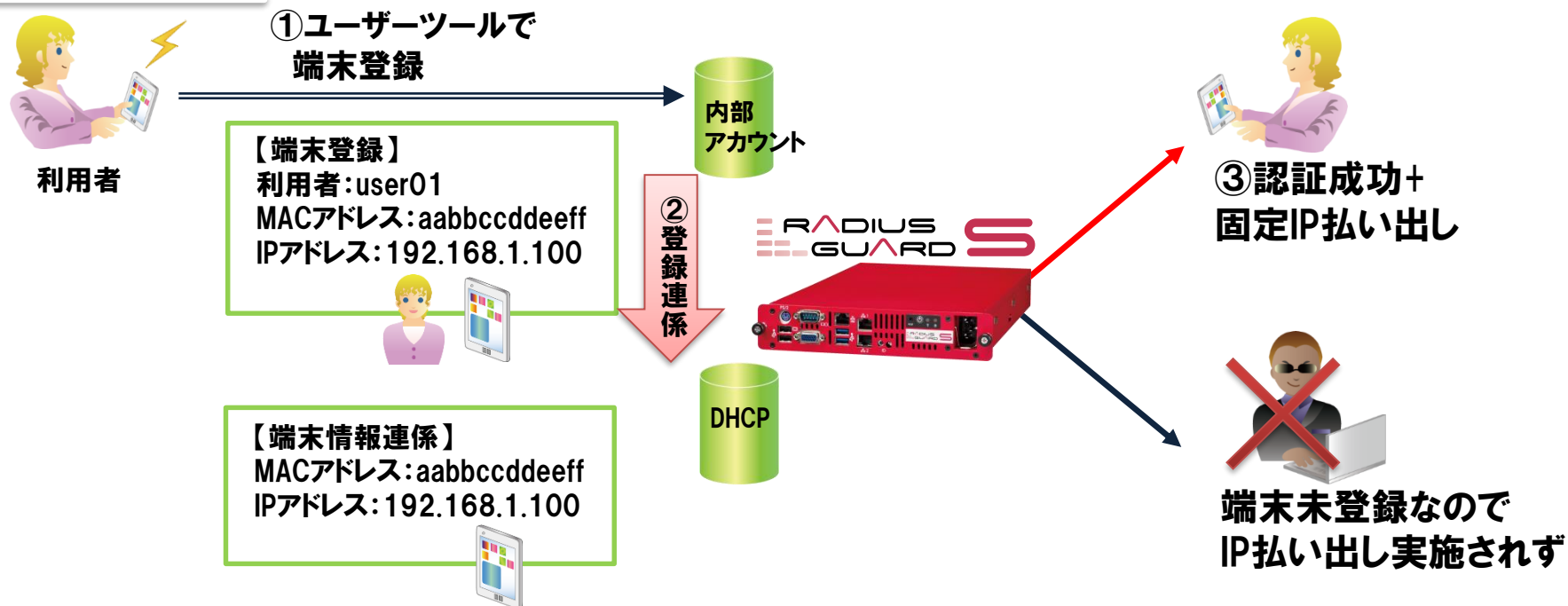
各セットは1:1冗長構成



- ・ 認証用に内部アカウントとして管理している端末情報を、DHCP払い出し端末に連携可能
 - 登録端末のみIPを払い出す(サブネット指定も可)
 - 登録端末に固定IPアドレスを払い出す
- ・ 各種属性を活用することで、端末のひも付け管理が可能に

利用者(ユーザー) --- 端末(MACアドレス) --- IPアドレス --- ホスト名 etc.

DHCP連携イメージ



特長と機能：冗長構成

・冗長構成

マスター⇒スレーブへ設定情報レプリケート (リアルタイム)

スレーブを複数持つことで**1:N (最大19) 構成にも対応**

冗長時切替動作は、RADIUSクライアント側の設定に依存

実IP管理、拠点間を介した構成も可能

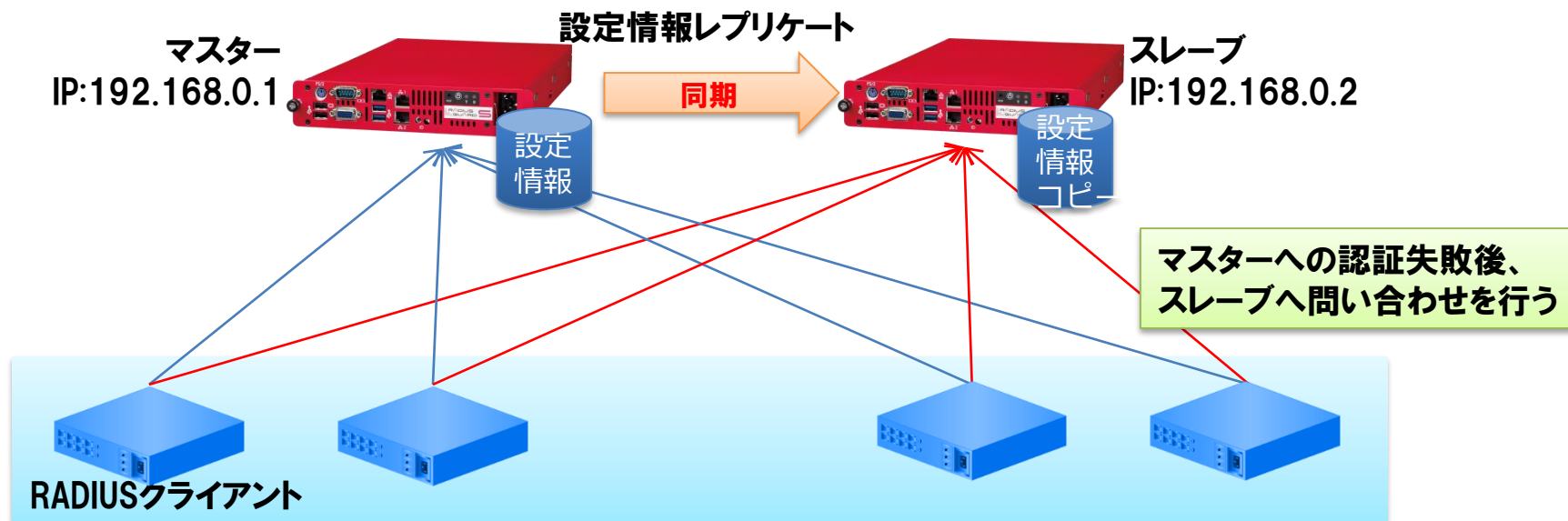
設定情報の改廃はマスターのみで、設定情報の統合管理が可能

サービスはマスター/スレーブ=Active/Activeのため負荷分散構成も可能

マスター障害時は、スレーブ機をマスター昇格させることで設定改廃可能

遠隔地に設置する
冗長構成にも対応

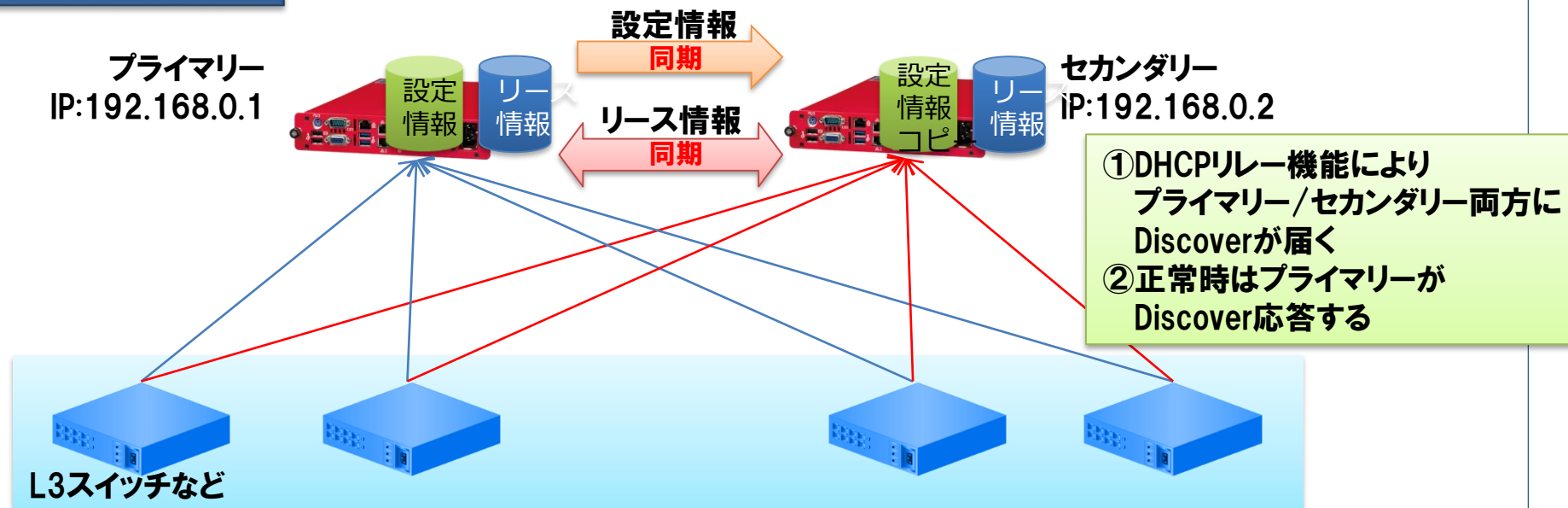
1:1冗長構成イメージ



・ 1:1冗長構成

- プライマリー=>セカンダリーの設定情報レプリケート (リアルタイム)
- プライマリー<=>セカンダリーのリース情報レプリケート (リアルタイム)
- 障害時にも同じIPアドレスを引き継げる
- プライマリー/セカンダリー両方にDiscoverが届くように構成する
- 正常時のDiscover応答はプライマリーが優先して行う
- 設定情報の改廃はプライマリーのみ

1:1冗長構成イメージ





- ・ バックアップ情報って？
- ・ 機能追加やバージョンアップの手間は？
- ・ 問い合わせ時の情報取得は？

◆ USBメモリに定期バックアップ

- 標準実装のUSBメモリに世代管理(1週間・日次処理)も可能な自動バックアップ
- 保存先はローカルディスク、FTP転送にも対応

◆ UPS連携機能も実装(SNMPトラップでのネットワーク経由シャットダウン対応)

◆ 障害情報等を含めたワンクリック一括診断情報収集

◆ CLI対応(特定コマンド実行可能)

◆ カスタムロゴ登録機能

◆ 認証・システム・DHCPログのほかに認証デバックログ機能

◆ syslog転送に対応。ローカル保存は最大500万件(1か月分)

主な実績

・さまざまなメーカーの無線アクセスポイント、認証スイッチ、VPN装置とRADIUS関係可能

無線LAN製品

シスコシステムズ

HP/アルバネットワークス

ラッカスワイヤレス

メルーネットワークス

ヤマハ

フルノシステムズ

アイコム

バッファロー

Aerohive NETWORKS

リバーベツド

アライドテレシス

フォーティネット

Office365向け

ADFSのデバイス認証で利用可能

有線LAN製品

シスコシステムズ

アラクサラネットワークス

HP/アルバネットワークス

APRESIA Systems

アライドテレシス

富士通

NEC

パナソニックLSネットワークス

ヤマハ

VPN製品

シスコシステムズ

ジュニパーネットワークス

デル(ソニックウォール)

フォーティネット

F5ネットワークス

パロアルトネットワークス

※その他、実績については製品サイト参照

※すべての環境において動作を保証するものではありません

RADIUS GUARDシリーズ 出荷実績:累計6,000台超

主な導入ユーザー(順不同)

企業

株式会社リコー様

朝日放送グループホールディングス株式会社様

株式会社島津製作所様

株式会社日比谷花壇様

株式会社メイテツコム様

株式会社アクセス国際ネットワーク様

株式会社東京システムリサーチ様

神姫バス株式会社様

株式会社アトリウム様

セーフィー株式会社様

日置電機株式会社様

住友三井オートサービス株式会社様

株式会社グリオグループ様 (AWS対応版)

キャノンシステムアンドサポート株式会社様

HRソリューションズ株式会社様 (AWS対応版)

文教

国際基督教大学様

慶應義塾大学様

浅野学園様

沼津情報・ビジネス専門学校様

恵泉女学園様

辻調理師専門学校様

福岡工業大学様

京都橘中学校・高等学校様

公共

東京都東久留米市様

京都府南丹市様

国立研究開発法人理化学研究所様

病院

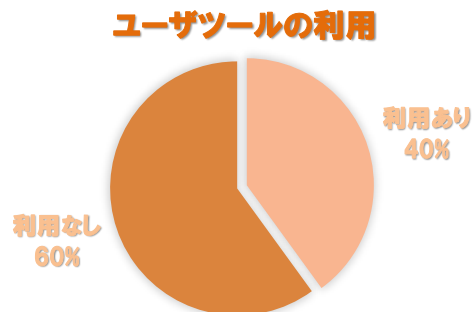
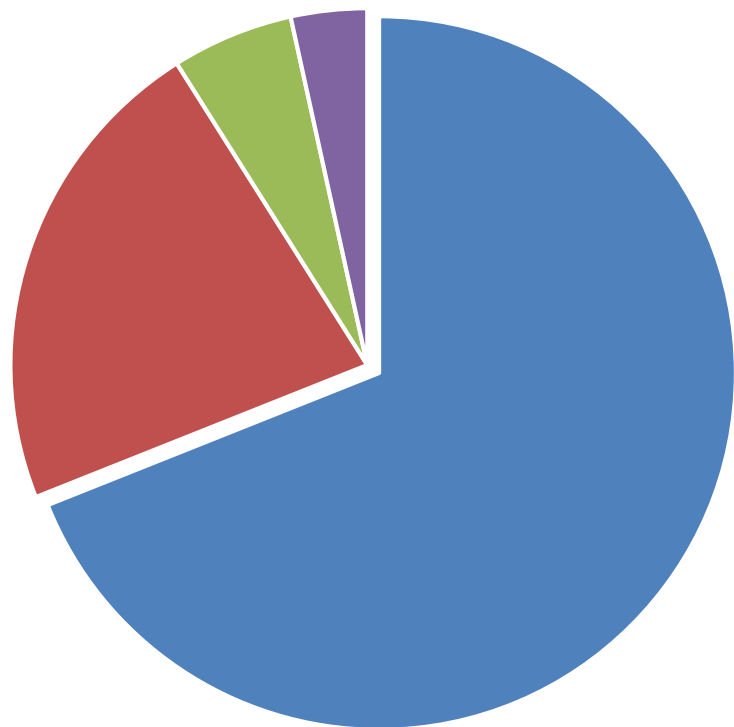
京都岡本記念病院様

某県庁、市役所などのセキュリティ強靱化として導入実績や、キャリア企業、金融系企業などでの実績も多数
RADIUS認証、CA、DHCPサービスが必要な場面で業種を問わず多数の導入実績

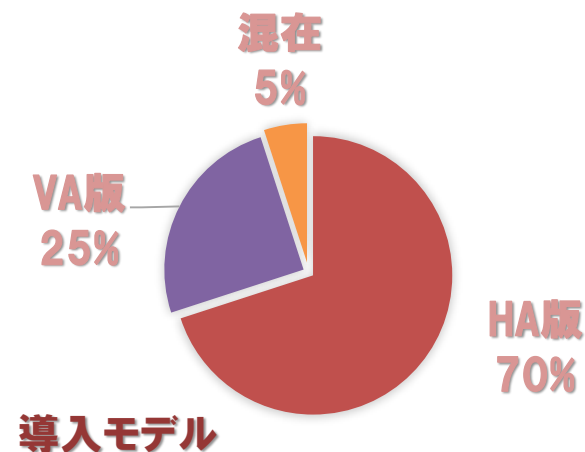
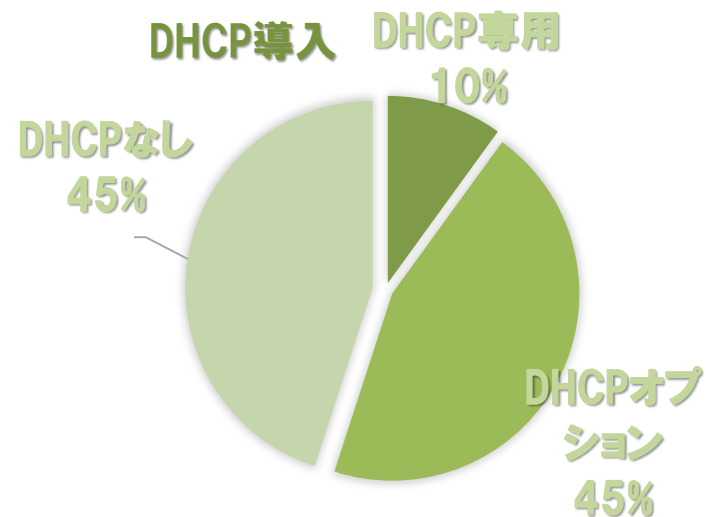
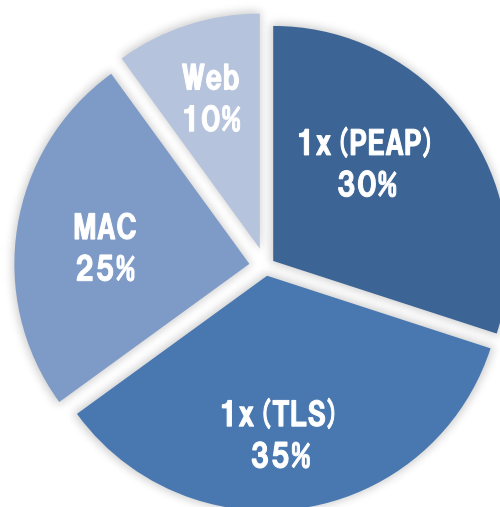
20年度:GIGAスクール構想における教育委員会様向けに県・市町村の各自治体様で導入多数 (提案ご相談ください)

・無線環境を中心に、VPN向けCAやDHCP運用としても導入実績多数

主なご利用割合（弊社提案における）



無線認証方式



■ 無線/有線認証 ■ VPN認証 ■ Login認証 ■ Office365,etc

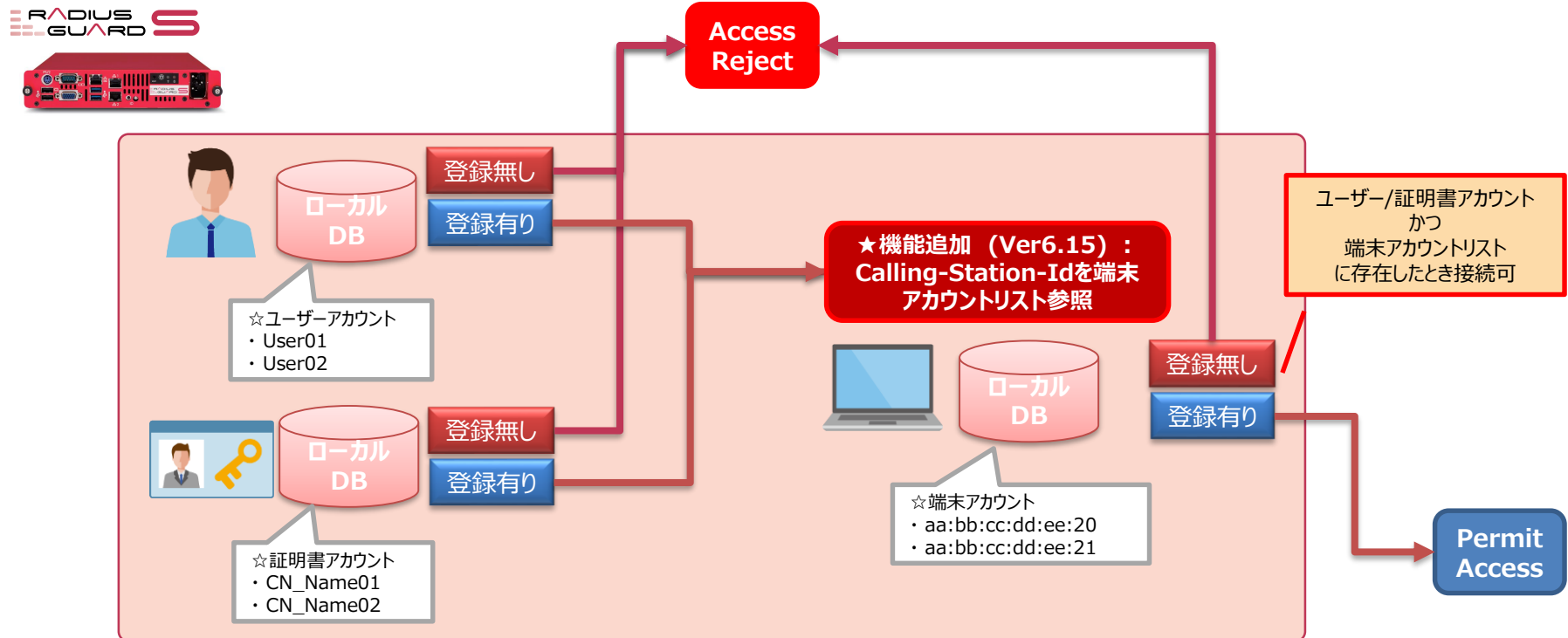
Ver.6.15.00新機能

(最新バージョンについては製品サイトを参照ください)

- アカウント情報の暗号化機能
 - 内部DBのアカウント情報を暗号化する
 - 暗号化する/しないは管理者が選択可能
- 認証時の内部DBアカウントとのCalling-Station-Id一致チェック
 - ネットワークプロファイルに以下設定を追加し、認証時に複数の要素をクロスチェック可能とする
 - ・ Calling-Station-Idが内部DBの端末アカウントと一致しない場合、認証拒否
 - ・ ユーザーが内部DBのユーザーアカウントと一致しない場合、認証拒否
 - 上記ネットワークプロファイルの適用先は外部AD、内部アカウントどちらも選択可能
- 申請期間によるメッセージ表示制御
 - ユーザーツールでアカウントを申請する際、アカウントの有効期限を初期値より長く申請した場合に注意喚起のメッセージを表示する
- ディレクトリ毎の登録アカウント制限
 - ディレクトリ毎にアカウントの登録数制限をかける
 - アカウント数制限の設定はスーパーユーザのみ可能とし第一階層ディレクトリに制限をかけた場合、第二、第三階層以下のディレクトリのアカウント数は第一階層ディレクトリに設定した制限数を超えないようにする
 - 各ディレクトリの編集画面から「ユーザー」「端末」「証明書」の種別毎に個別で設定可能

- 管理者アカウントのカスタム化
 - 管理者権限の一つ「ディレクトリ管理者」が管理外のディレクトリを参照できるようにする
※現仕様ではディレクトリ管理者が管理外ディレクトリを参照するためには
もう一つ管理者アカウントを作成しログインしなおす必要があるため
- 証明書アカウントの証明書を管理画面からDL時の「DL済」
 - ユーザーツールからダウンロードした場合、「DL未」から「DL済」の表示に変更される(既存と同じ)。
 - ユーザーツールから証明書をダウンロードしていなくても、管理ツールからダウンロードした場合、「DL未」から「DL済」の表示に変更する(新規動作)
 - 既存の動作と同じ様に、ユーザーツールからダウンロードしない限り、管理ツールからダウンロードしても、「DL未」の表示から変更されないようにすることも可能とする
- パスワード変更時のパスワードの外部AD参照
 - ユーザーがパスワード変更する際のログインID,PWを外部AD参照可能とする。
 - ADユーザー登録機能を利用し、変更後の新PWはRGS⇒ADへ同期する
(アドバンス連携オプションが前提)
- CA証明書の有効期限通知
 - 日次処理で以下証明書の有効期限を監視し、メールを送信する。
 - ・ CA証明書(自己認証局/下位認証局)
 - ・ https接続時に使用する証明書(内部サーバー証明書、または外部サーバー証明書)
 - ・ RADIUS認証サーバー証明書(内部サーバー証明書、または外部サーバー証明書)
 - メール送信先は、それぞれの証明書ごとに5件指定可能にする
 - メール送信先が、設定されていない場合、メールを送信しない

• Calling-Station-Id判定の参照先を端末アカウントリストへ拡張



Calling-Station-Idによる判定が拡張されるとデバイス接続制限の運用に容易に。

- PEAP認証時にN:NのID/Pass※+MACアドレス判定による二段階認証が可能
- TLS認証時の証明書使い回しでも、MACアドレス判定によるデバイス制限が可能
- MACアドレス管理は検索、一括・定期インポートなど柔軟な運用が可能

※外部AD/LDAP参照時にも、RADIUS GUARD SのローカルDBの端末アカウントを参照可能

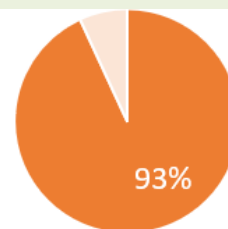
ご提案・導入にあたり

国産ならではの 優れた品質と手厚いサポート

ソフトウェア、ハードウェア共に**日本国内生産**されており、高い品質とお客さま環境に合わせたサポートを提供します。

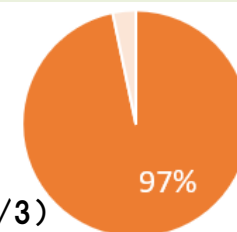
複雑なシステム環境を理解しているエンジニアが、
お客さまのご要望に応えます。

対応スピードに満足



サポートセンター
満足度調査
(2018/7~2019/3)

サポート内容に満足



ネットワークインテグレータ による開発

ネットワーク設計、構築、運用サポートの経験を生かし、システム全体で活用できる最適な設計。
進化していくお客さまのシステム環境を考慮し、開発しています。

アプライアンス&わかりやすい管理画面で 素早い導入

OSのインストールやメンテナンスに手間取らないアプライアンス製品。わかりやすい管理画面。
素早く導入できるRADIUS GUARD Sが、お客さまの導入&運用コストを削減します。

運用に必要な機能も 1台に集約

定期バックアップ、GUIバージョンアップ、障害解析情報の収集なども可能です。
運用に必要な機能もトータルでそろっているので便利です。

RADIUS GUARD Sには、既存の作業を自動化、もしくは権限委譲により、担当者の負担を軽減するアカウント管理機能が多く実装されています。



RGS機能	工数想定	導入前工数	導入後工数	効果
自動削除 (自動棚卸し)	年2回のアカウント棚卸し精査	2Day*2回	0min (自動化)	4人日の圧縮
定期インポート	アカウントの定期的な追加作業	1アカウント*10min	0min (自動化)	100アカウント*年2回の場合=>約1.5人日の圧縮
ユーザーツール アカウント登録	ユーザー・承認者・情シス担当の各工程での申請/承認/登録作業	1アカウント 15+5+15min=45min	15min (ユーザー=>承認のみ)	1/3工数へ圧縮
アカウント改廃	ユーザー・承認者・情シス担当の各工程での申請/承認/登録作業	1アカウント 5+5+5min=15min	5min (ユーザー=>承認のみ)	1/3工数へ圧縮
パスワード変更	ユーザー申請=>承認作業	1アカウント 5+5min=10min	1min (ユーザー作業)	1/10工数へ圧縮
MAC自動登録	MAC認証用の端末登録作業。端末のMACアドレス確認から登録申請	1端末 15~20min	1min (登録用NWに接続のみ)	1/15工数へ圧縮
DHCP MACアドレス自動取得	MACアドレスを利用したアカウント制御のための登録作業 (Calling-Station-ID等)	1端末 10~15min	0min (自動化)	100アカウント*年2回の場合=>約1.5人日の圧縮

DHCPサーバ機能 (オプション) を平行して利用することで更にコスト削減！！

- ◆ ハードウェアアプライアンス本体＋フルオプションパック
- ◆ 各VA版＋フルオプションパック
- ◆ 各クラウド対応版

動作確認や、相互接続検証などにご使用いただける検証機器のお貸し出しを実施しております

- ハードウェアアプライアンス = 標準 2週間（冗長構成は別途ご相談）
- VA版はDVD-ROMでお貸し出し
- AWS対応版は共有インスタンスのご案内/Azure対応版はVHDファイルのご案内
- 貸出時にご要望に応じてハンズオンセミナーの実施
- ◆ 検証目的用 専用パッケージ販売
パートナー様向けに、検証用途向けの専用パッケージをご用意しております
- ◆ 設計支援ツールとして、設定シートのご提供
- ◆ 最新ファームウェア情報や導入事例の更新は製品サイトをご覧ください
<http://www.scsk.jp/product/common/radius/index.html>

・ RADIUS GUARD Sを初めてご利用いただく方に

- 連携実績のある機器の設定例まで含んだガイド資料を多数ご用意

◆ RADIUS GUARD S_スタートアップガイド.pdf

◆ 基本設定ガイド

- ・ RADIUS GUARD S_設定ガイド(Web、MAC認証編).pdf
- ・ RADIUS GUARD S_設定ガイド(IEEE802.1X編).pdf
- ・ RADIUS GUARD S_設定ガイド(外部LDAP・AD関係編).pdf

◆ 応用設定ガイド

- ・ RADIUS GUARD S_設計ガイド(ユーザー申請).pdf
- ・ RADIUS GUARD S_設計ガイド(端末申請).pdf
- ・ RADIUS GUARD S_設計ガイド(証明書申請).pdf
- ・ RADIUS GUARD S_設計ガイド(eduroam)
- ・ RADIUS GUARD S_設計ガイド(ネットワークプロファイル).pdf
- ・ RADIUS GUARD S_設計ガイド(アカウント自動棚卸).pdf
- ・ RADIUS GUARD S_設計ガイド(RADIUSサーバーと認証局の移行).pdf
- ・ RADIUS GUARD S_設計ガイド(UPKIクライアント証明書配送).pdf

◆ 端末設定ガイド

- ・ RADIUS GUARD S_証明書インストール(iOS編).pdf
- ・ RADIUS GUARD S_証明書と無線設定(Windows10編).pdf
- ・ RADIUS GUARD S_証明書と無線設定(Android編).pdf

・ その他のお役立ち資料として

- 提出物や要件打ち合わせに活用可能な Excelベースの【設定シート】
- 提案において利用可能な製品縛り資料

弊社担当にご相談ください

◆ 他メーカー連携設定ガイド

- ・ RADIUS GUARD S_設定ガイド(Apresia編).pdf
- ・ RADIUS GUARD S_設定ガイド(Apresia(動的VLAN)編).pdf
- ・ RADIUS GUARD S_設定ガイド(Alaxala編).pdf
- ・ RADIUS GUARD S_設定ガイド(Alaxala(動的VLAN)編).pdf
- ・ RADIUS GUARD S_設定ガイド(Cisco WLC編).pdf
- ・ RADIUS GUARD S_設定ガイド(Cisco WLC(動的VLAN)編).pdf
- ・ RADIUS GUARD S_設定ガイド(YAMAHA WLX(1x認証)編).pdf
- ・ RADIUS GUARD S_設定ガイド(YAMAHA WLX(MAC認証)編).pdf
- ・ RADIUS GUARD S_設定ガイド(Aruba_PCAP-TLS認証編).pdf
- ・ RADIUS GUARD S_設定ガイド(Aruba_MAC認証編).pdf
- ・ RADIUS GUARD S_設定ガイド(Riverbed Xirrus編).pdf
- ・ RADIUS GUARD S_設定ガイド(Aerohive編).pdf
- ・ RADIUS GUARD S_設定ガイド(Ruckus_ZD編).pdf
- ・ RADIUS GUARD S_設定ガイド(Ruckus_SZ編).pdf
- ・ RADIUS GUARD S_設定ガイド(Ruckus_Unleashed編).pdf
- ・ RADIUS GUARD S_設定ガイド(Fortigate_SSL-VPN編).pdf
- ・ RADIUS GUARD S_設定ガイド(NEC_QX編).pdf
- ・ RADIUS GUARD S_設定ガイド(Allied_SW編).pdf
- ・ RADIUS GUARD S_設定ガイド(Allied_AP編).pdf

【お問い合わせ先】
SCSK株式会社
ITプロダクト&サービス事業本部 ネットワーク部
TEL:03-5859-3034
RG-info@ml.scsk.jp