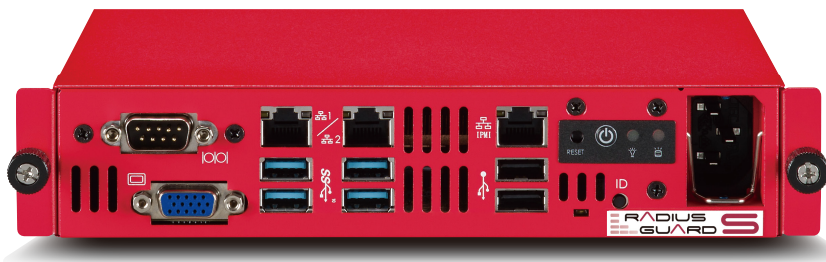


シリーズ累計

8,000^{*}台を突破!!

※2021年9月付 SCSK調べ

不正アクセス対策には 赤いRADIUS



RADIUS GUARD S

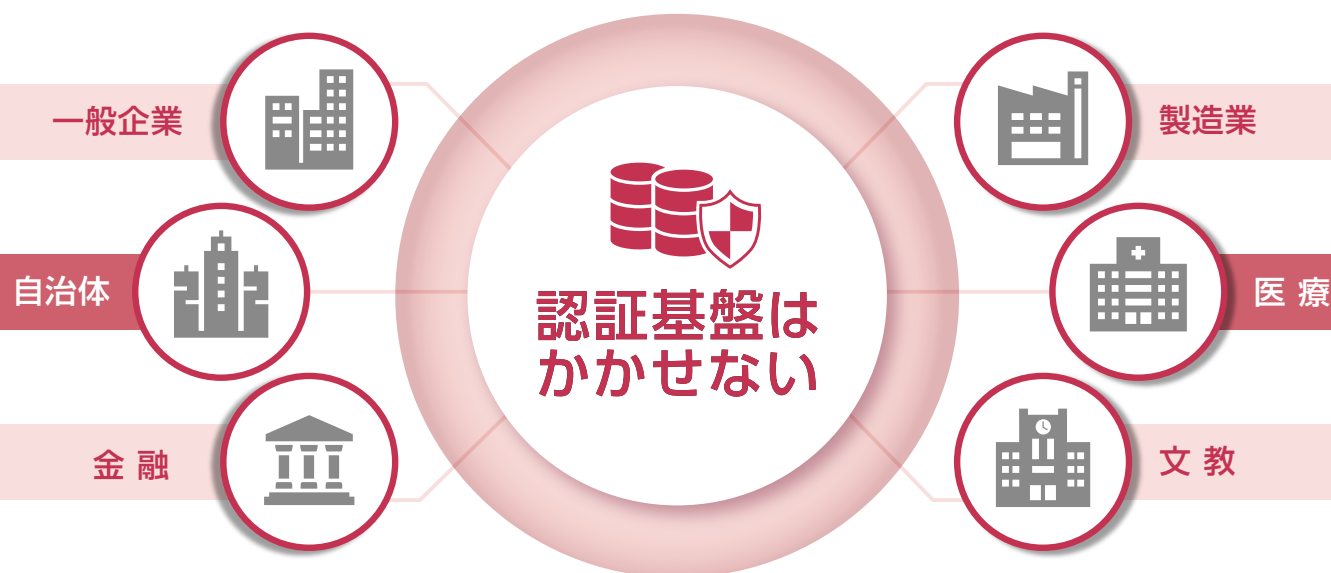
無線LAN・リモートアクセスのセキュリティ強化に必要な機能を提供する
RADIUS認証・CA(証明発行管理)・DHCPアプライアンスサーバー

無線LAN/VPNなどの認証の課題は RADIUS GUARD[®]Sが まとめて解決します



不正アクセス防止に向けたセキュリティ対策に必須の認証サーバー

無線LANの拡大や、VPN接続(リモートアクセス)の導入によるネットワーク環境の変化には不正な接続を防止するセキュリティ対策が必要です。RADIUS GUARD Sは様々なネットワーク環境で必要とされる認証機能をオールインワンで提供可能です



“不正接続防止”やユーザーアクセス制御に活躍!

RADIUS GUARD Sは自動化や操作権限委譲などの機能を数多く標準実装し、日々のアカウント管理・証明書運用の負担を軽減できるため、様々な業界で導入が進んでいます

無線/有線
認証



証明書発行



VPN接続



企業事例

某放送局



DHCPも1台で提供可能な認証基盤として新規無線LANとともに導入。ゲスト向けのアカウント発行もワークフローで活用中。

製造業事例

某大手メーカー



無線LAN、VPN、Office365のアクセスにおいて証明書を利用したデバイス認証環境を構築。証明書配布に関わる負担を軽減。

官公庁事例

某県庁



庁舎の無線LAN更改に併せて個人情報保護のため証明書を利用した認証と、MAC認証の併用でセキュリティ強化。

文教事例

某私立大学



キャンパス無線LAN向けの認証基盤として導入。学生自身による利用申請登録が可能なワークフローを利用し運用負担を軽減。

※その他導入事例も多数、Webサイトで公開中

RADIUS GUARD S 四大機能



RADIUS サーバー

Web、MAC、802.1X 各認証に対応



認証局 (CA)

証明書発行/証明書管理 スマートデバイス対応



DHCP サーバー

統合管理機能を利用して、最大10,000IPアドレス x10セットの管理に対応



ワークフロー機能

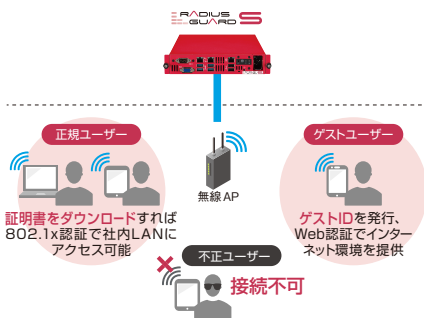
アカウントや証明書の申請から、承認処理、発行までワンストップ

CASE 1 無線LANに!

スマートデバイスと無線LAN環境の導入に

Point

- ▶許可されたPCやスマートデバイスだけを接続
- ▶端末やユーザーの識別を行いアクセス制御
- ▶オリジナルワークフローによる容易な申請と管理

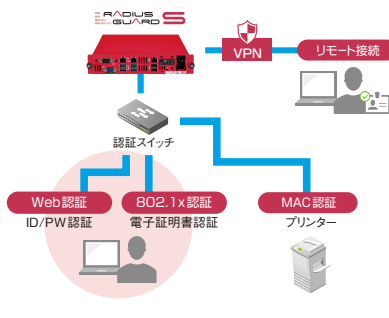


CASE 2 テレワーク環境に!

証明書を用いたデバイス認証基盤をVPN環境に

Point

- ▶VPNのデバイス認証をクライアント証明書で実現
- ▶有線環境で、認証スイッチに応じた様々な認証方式に対応
- ▶サーバー、ネットワーク機器などへのログイン認証にも

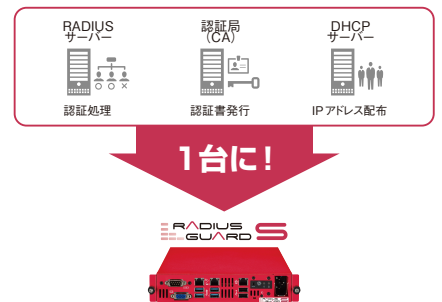


CASE 3 まとめて1台で!

ユーザー管理、端末管理に必要な複数のサーバーを1台に

Point

- ▶冗長機能とバックアップ情報で可用性もアップ
- ▶RADIUS、認証局 (CA)、LDAP、DHCPを1台で実現
- ▶アプライアンスによる保守運用負担とコストの低減



RADIUS GUARD S サポート機能

アカウント管理機能



200 ~ 200,000
ライセンス対応



未使用アカウント
検索機能



ディレクトリ・
アカウント管理



アカウント
自動削除機能



CSVによる一括登録
定期インポート機能



外部データベース連携

ユーザー認証



パスワード世代
管理機能



アカウントロック



Shibboleth SP対応

証明書機能



クライアント・サーバー
証明書の発行



外部発行された
証明書の認証



証明書配布が
可能なワークフロー

MAC 認証



MAC 認証パラメータ
処理機能



MAC アドレス区切り
文字自動修正



MAC アドレス
自動収集

管理者の負担軽減機能



運用負荷軽減
管理者権限のカスタマイズ



アカウント申請が可能な
ユーザーツール

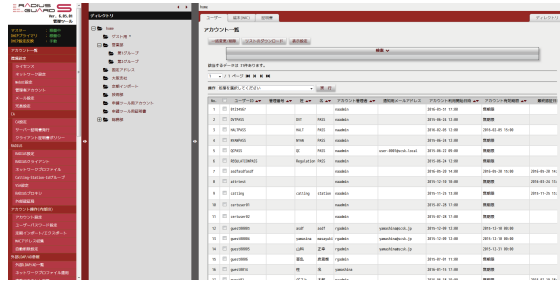


DHCPサーバー
機能強化

Point 1

導入後の運用負担を軽減する管理機能

登録情報は認証方式にあわせて3種類のアカウント「ユーザー・端末・証明書」として登録され、ディレクトリ単位の階層構造で管理。アカウントの一括登録に対応し、表示項目・検索項目のカスタマイズも可能です。
また、日々の運用業務を自動化する「自動削除機能・メール通知機能・定期インポート機能」などの利用により、管理者業務の負担を軽減し、認証基盤の運用を簡単に行うことができます。



▲ RADIUS GUARD S 管理画面

自動棚卸し機能

最終認証日時より、設定期間の利用がないアカウントは無効化や削除など、ディレクトリ毎の異なるルールで自動化することが可能です。

ディレクトリ管理者

各ディレクトリにアカウント改廃権限をもつ管理者を定義し、システム管理者の負担を分散します。

ディレクトリA(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	今日	1週間前	1週間前
ステータス	利用可能	無効	削除

ディレクトリB(証明書用)

最終認証から**3ヶ月後に削除**

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

Point 2

DHCPサーバー機能も1台で

1万IPアドレスの払い出しに対応したDHCPサーバー。認証サーバーとまとめることで、導入と維持コストを大幅に削減します。また、DHCPサーバーはMACアドレスをリース情報として保持しているため、認証情報のアカウント申請時に活用が可能。MACアドレス情報をあらかじめ入力する必要がなく、ユーザーは申請端末のMACアドレスを確認する作業、管理者は登録作業から解放されます。

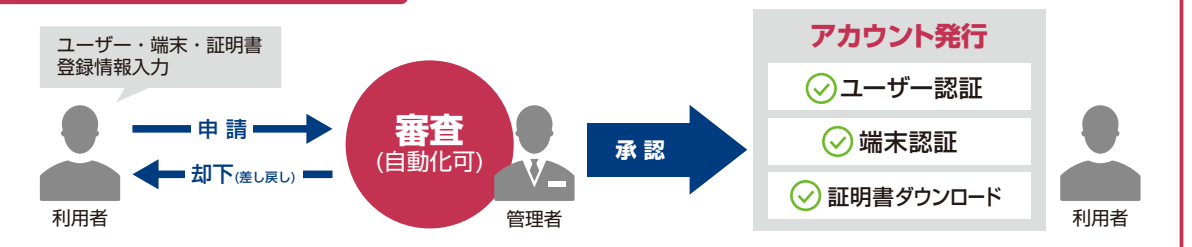


Point 3

申請ワークフローの実装

CSVファイルからの一括登録だけでなく、持ち込み端末の登録や、個別でのユーザー申請を紙ベースの申請処理の負担から管理者を解放する申請ワークフロー。ユーザーはWEB画面から申請することが可能となります。MACアドレスの申請や、ゲストアカウントの申請など、さまざまなシーンに対応した申請ワークフローを提供し、ユーザーによるクライアント証明書のダウンロードにも対応します。

申請・承認ワークフローの概要



Point 4

オリジナル支援ツール“RADIUS GUARD Utility”

日々の設定変更・運用などの負担を軽減する支援ツールを提供。

- ・ログ可視化ツール: RADIUS GUARD Sのログを取り込み、キーワードの発生状況を視覚的に確認可能
- ・RADIUS試験ツール: 無線APや端末を用意しなくても、PC上からRADIUSの認証試験が可能なツール。PAP/CHAP/MS-CHAPv2/EAP-PEAP・TLSに対応



サポート機能

日々の煩雑な運用業務をサポートし、
管理者の負担を軽減するさまざまな機能が実装されています。

定期バックアップ機能

設定情報や、アカウント情報などを含んだバックアップイメージが機器の障害などに備え自動的に保存され、保守作業時もスムーズに復旧させることが可能です。

冗長機能

RADIUSサーバーの冗長構成は1:1や、1:Nの大規模環境にも対応。遠隔地構成や、異なるプラットフォーム間(例:HW版-AWS版)の冗長構成にも対応するため柔軟な導入が可能です。(DHCPサーバーの冗長構成は、1:1)

診断情報取得機能

サポート窓口とのやりとりに必要な情報がまとめて取得できる診断情報取得機能により、エスカレーション時の負担を大幅に軽減できます。

RADIUSクライアント登録数は最大10,000エントリー

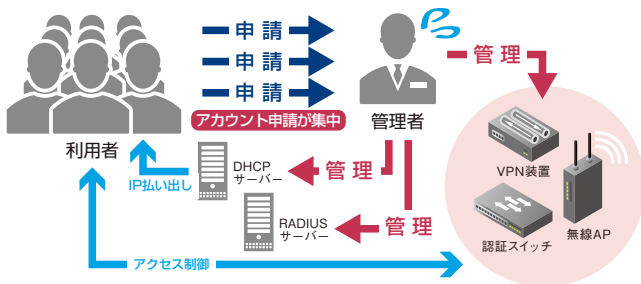
ネットワーク機器などのログイン認証に利用する場合など、登録されるアカウント数よりもRADIUSクライアントの登録数が求められる場面でも、RADIUS GUARD Sは10,000エントリーまで、最小ライセンスから対応します。

効果的な導入ケース

RADIUS GUARD Sの導入で、管理者負担の大幅軽減

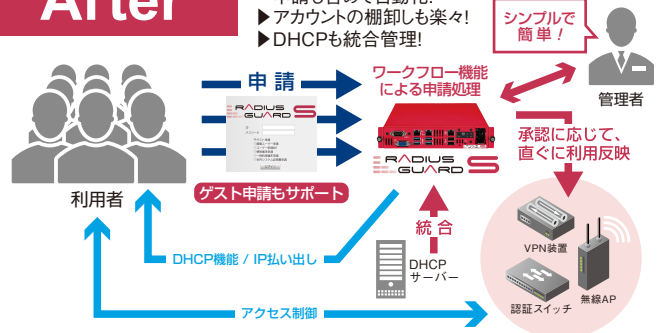
Before

- ▶管理者が手作業でアカウントを設定。
- ▶期初や期末は、膨大な作業量。
- ▶アカウントのステータス管理も大変!



After

- ▶ワークフロー機能でアカウント処理、申請も含めて自動化!
- ▶アカウントの棚卸しも楽々!
- ▶DHCPも統合管理!



連携製品 動作実績

無線LAN製品

メーカー名	確認済み製品名
ICOM	APシリーズ
アライドテレシス	NWS APシリーズ TQシリーズ
アルカテルルーセント	OmniAccessWLANシリーズ
エアロハイネットワークス	Aerohiveシリーズ
HPE	Arubaシリーズ MSMシリーズ
NECプラットフォームズ	NAシリーズ
キーエンス	BTシリーズ
シスコシステムズ	Merakiシリーズ Aironetシリーズ ワイヤレスコントローラシリーズ
日本電気	UNIVERGE QXシリーズ
D-link	DWLシリーズ
バッファロー	AirStationシリーズ
フォーティネット	FortiAPシリーズ
富士通	SR-Mシリーズ
フルノシステムズ	ACERAシリーズ
メルネットワークス	MCシリーズ
ヤマハ	WLXシリーズ
ラックスワイヤレス	ZoneFlexシリーズ ZoneDirectorコントローラシリーズ
リバーベッド	Xirus Wi-Fiシリーズ

有線LAN製品

メーカー名	確認済み製品名
アプレシアシステムズ	Apresiaシリーズ ApresiaLightシリーズ
アライドテレシス	CentreCOMシリーズ
アラクサラネットワークス	AXシリーズ
アルカテルルーセント	OmniSwitchシリーズ
HPE	Arubaシリーズ ProCurveシリーズ
H3C	Sシリーズ
シスコシステムズ	Merakiシリーズ Catalystシリーズ
日本電気	IXシリーズ IP8800シリーズ UNIVERGE QXシリーズ
バッファロー	インテリジェントスイッチシリーズ
パナソニックネットワークス	ZEQUOシリーズ
富士通	SR-Sシリーズ
ヤマハ	SWXシリーズ

VPN製品

メーカー名	確認済み製品名
F5ネットワークス	APMシリーズ
シスコシステムズ	ASAシリーズ
シトリックス	NetScalerシリーズ
ジュンパーネットワークス	SSGシリーズ
ソニックウォール	Aventailシリーズ SonicWall SRAシリーズ
バルスセキュア	PSAシリーズ MAGシリーズ
パロアルトネットワークス	PAシリーズ
フォーティネット	FortiGateシリーズ
富士通	IPCOMシリーズ

その他製品

メーカー名	確認済み製品名
A10 Networks	Thunderシリーズ
マイクロソフト	Office365 ADFS向け

※記載の情報は、2021年3月現在の情報です。(五十音順)

※その他、実績は多数となりますが全ての環境において動作を保証するものではありません。

最新の情報はHPでご確認ください

<https://www.scsk.jp/product/common/radius/>



製品仕様 / 機能一覧

RADIUS GUARD S 製品仕様 (アプライアンス版、仮想アプライアンス版、クラウド対応版共に、製品機能は共通です。)

機能名	機能説明
管理可能アカウント数	200 / 500 / 2,500 / 5,000 / 10,000 / 50,000 / 200,000 (同一筐体のまま、最大200,000アカウントまで拡張可能) ※MAC認証のみ300,000アカウント可: 事前要件確認必須・拡張導入不可
RADIUSクライアント登録数	最大10,000 エントリ (ネットワークアドレスによる登録可)
ユーザー/端末/証明書アカウント管理機能	ユーザー/端末/証明書アカウントを管理する機能 (作成、編集、一括インポート/エクスポート/証明書ダウンロード、MACアドレス自動取得、ユーザー/端末/証明書アカウント自動削除、パスワード有効切れフォロー通知メール)
認証機能 (RADIUS)	認証クライアント(無線AP等)からの認証要求に対して、認証結果を応答する機能 (ネットワーク属性管理、RADIUSプロキシ、外部参照含む) 802.1x・Web・MAC認証に対応(PAP/CHAP/MS-CHAPv1/MS-CHAPv2/EAP-MD5/EAP-MSCHAPv2/EAP-TLS /EAP-TTLS/PEAP)
自己認証局機能 (CA)	証明書を管理する機能 (CA証明書ダウンロード、自己サーバー証明書発行、外部サーバー証明書発行、外部認証局証明書インポート、証明書発行/失効ログ出力、失効リスト公開、下位認証局)
ユーザーツール	ユーザー/端末/証明書アカウント登録申請・編集・削除ワークフロー、証明更新、端末情報自動収集、ゲストID自動発行、パスワード期限切れ通知、パスワード自動生成
冗長化機能	ユーザー/端末/証明書アカウント情報や認証機能を冗長化し、可用性を向上させる機能
外部LDAP/AD参照機能 ※1	外部のLDAPやActive Directory® のアカウント情報を参照して認証する機能
内部LDAP登録連携機能 ※2	外部のサーバーからLDAPプロトコルで内部アカウントの情報を改廃する機能 (LDAPバインド)
AD登録連携機能 ※3	内部アカウントをActive Directory® へ登録する機能
DHCPサーバー機能 ※4	DHCPサーバーの設定とIPアドレス払い出しを管理する機能 (IPアドレス払い出し、サブネット管理、端末管理、DHCPオプション管理、DHCP冗長化)
DHCP最大IP払い出し数	最大10,000 IPアドレス
DHCP統合管理機能	最大10セットまで可能 (10,000 IPアドレスx10セットまで拡張可能)
ブラックリスト機能	syslogサーバー(弊社推奨品 ※5)で受信したセキュリティログを参照し、不正通信を行なった端末のアカウントをブラックリストに自動的に登録して、認証処理において拒否を行なうセキュリティ強化機能
Shibboleth SP機能 ※6	RADIUS GUARD SをShibboleth認証のスイッチ認証SPとして使用する機能 ユーザーツールのログインをShibboleth認証に対応する機能
UPKIクライアント証明書配付機能 ※7	国立情報学研究所(NII) [UPKI電子証明書発行サービス] 発行のクライアント証明書を、RADIUS GUARD Sに取り込み、利用者ごとのダウンロードが実施可能となる機能

※1 200および500ライセンスは外部LDAP/AD参照オプションが必要(2500ライセンス以上はバンドル) ※2 内部LDAP登録連携オプションが必要
 ※3 アドバンスド連携オプションが必要 ※4 DHCPオプションが必要 ※5 推奨製品 エイチ・シー・ネットワークス製 Log@Adapter+ (2019年11月時点)
 ※6 Shibboleth SPオプションが必要 ※7 UPKIクライアント証明書配付オプションが必要

RADIUS GUARD S 機器仕様 ※記載の情報は、RADIUS GUARD S 単体の情報です。



項目	詳細
外形寸法(W x D x H)	200 x 350 x 42.4mm (突起物含まず)
電源仕様	100~240V (50/60Hz) 付属する電源ケーブルは、国内AC100 V仕様
最大消費電力	114W
重量	2.8kg (付属物含まず)
インターフェース	10/100/1000 BASE-T x 2
付属品	外部USBメモリ x 1、1台設置用ラックマウント金具
EMI規格	VCCI Class A

RADIUS GUARD S クラウド対応版 動作環境 ※RADIUS GUARD SのリリースバージョンはVer6.13.00以降

aws	Amazon Elastic Compute Cloud(以下Amazon EC2)上で動作
Microsoft Azure	Microsoft Azureの仮想マシン上で動作 ※DHCP機能を除く

RADIUS GUARD S VA (仮想アプライアンス版) 動作環境 ※最新の動作環境については要確認願います。

	仮想環境	VMware ESXi 6.0以上/NutanixAHV+Prism Central環境/Microsoft Hyper-V環境
	CPU	仮想CPUをRADIUS GUARD S に4個割り当て可能
	RAM	4GB
	HDD	60GB

RADIUS GUARD S 価格

本体 & ライセンス	基本200ライセンスモデル ■79万円(税抜)~ (ライセンス=内部登録アカウント数) DHCPサーバー専用ライセンス(10,000 IP払い出し)モデル ■79万円(税抜) (認証ライセンス追加可能) ※上記金額に、初年度ハードウェア保守費用が必要です。 RADIUS GAURD S (仮想アプライアンス版・クラウド対応版) の価格: 基本200ライセンスモデル ■59万円 (税抜) ~
------------	---

※ハードウェアアプライアンスの最大保守期限は初年度開始日より5年間です。

導入検討に!

- 検証機の貸し出し受付中
- 設定方法が簡単にわかる
スタートアップガイドを配布中



HPはこちら

製品及びご購入に関するお問い合わせ

- RADIUS GUARDおよび、RADIUS GUARDロゴは、SCSK株式会社の登録商標です。
- 本カタログに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。
- その他、記載されている会社名、製品名は、各社の商標または登録商標です。
- 記載内容(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2021年9月現在のものです。