



# 地方自治体の無線LAN整備に必須となる不正接続対策の提案

## RADIUS GUARD Sによる認証環境の実現

SCSK株式会社  
ネットワークセキュリティ事業本部  
セキュリティプロダクト第二部

2023/11

# CONTENTS

## 目次

1. 無線LANの活用と不正接続対策
2. RADIUS GUARD Sについて
3. 導入事例

# 1

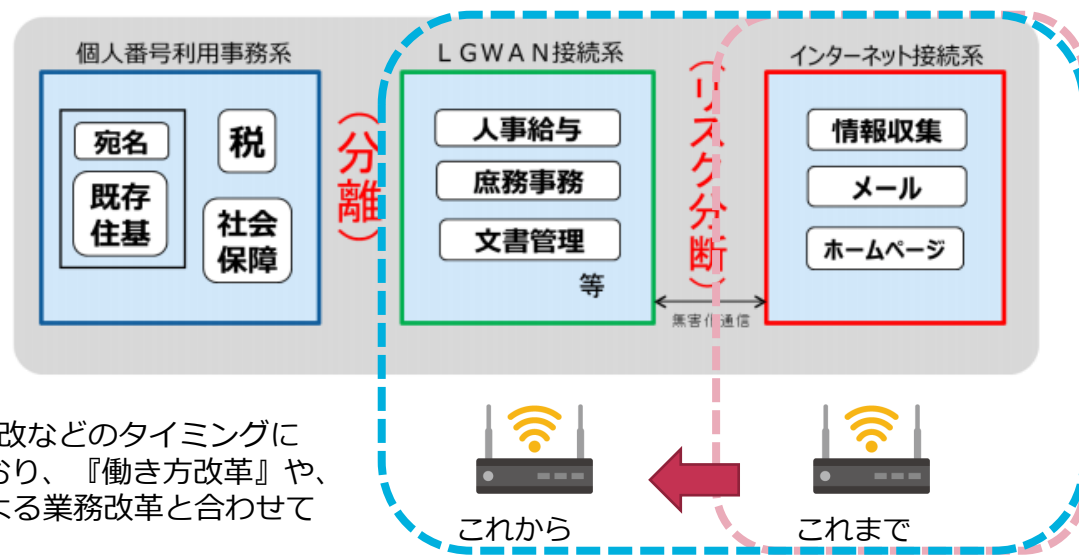
## 無線LANの活用と不正接続対策

---

# 無線LANの利用範囲の拡大

## ■ LGWAN接続系における庁内無線LANの利用

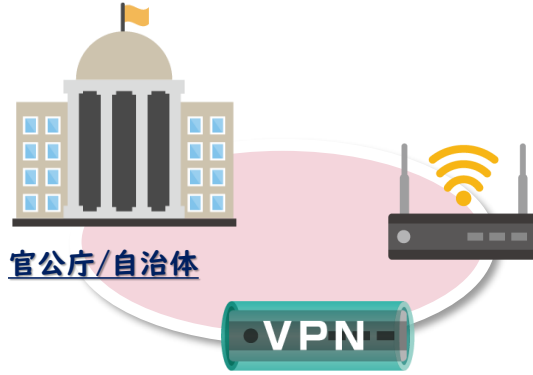
これまでインターネット接続系において許可されていた無線LANの利用が、新たにLGWAN接続系においても利用が可能となりました。今後、ますます無線LANの利用が拡大していくと想定されます。



■ 庁舎の立て替え・ネットワーク更改などのタイミングにおいて、無線LANの整備は広がっており、『働き方改革』や、『スマートデバイス』の導入などによる業務改革と合わせて無線LANの必要性が拡大しています。

## 無線LANは必須のネットワーク環境へ

# ガイドラインによる認証の明記



## 無線LANに認証技術の導入は必須

20年12月:総務省のセキュリティガイドラインが改定されセキュリティ要件について追記されました。

### 【ガイドライン抜粋】

(13) 無線 LAN 及びネットワークの盗聴対策 ①統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び**認証技術の使用を義務付けなければならない**。

### ■ ガイドラインのポイント

- 無線LANを利用する場合、不正アクセス対策を実施
- ネットワーク利用が許可されたものであることを確認
- 電子証明書による端末認証などの利用制限が必要

総務省：  
「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定について」より抜粋



# ネットワークインフラに対するセキュリティの必要性

## ■ 不正接続対策の重要性

働き方改革や、オフィス環境の変化、コロナ禍によるテレワーク環境の広がりなどネットワーク環境は急速に変化しています。このような変化の中で安全なネットワークに必要な対策が取られていないため、不正接続などのリスクが増大しています。



## “共通パスワード・単純なIDによる接続”

ネットワーク環境の整備を優先するため、セキュリティ対策やリスク対策を置き去りにした無線LANやVPN環境には**不正接続対策**が必要です。

## 想定されるリスク



意図しない通信により帯域を圧迫/本来の業務に影響

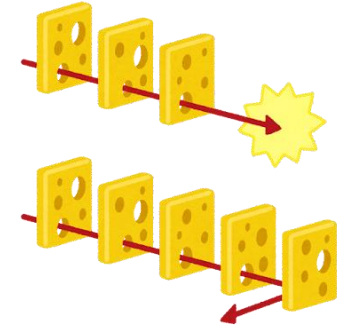
踏み台として利用され、いつのまにか加害者側

ネットワーク上の他のシステムに対する侵入経路

# 多層防御と適切な認証の導入

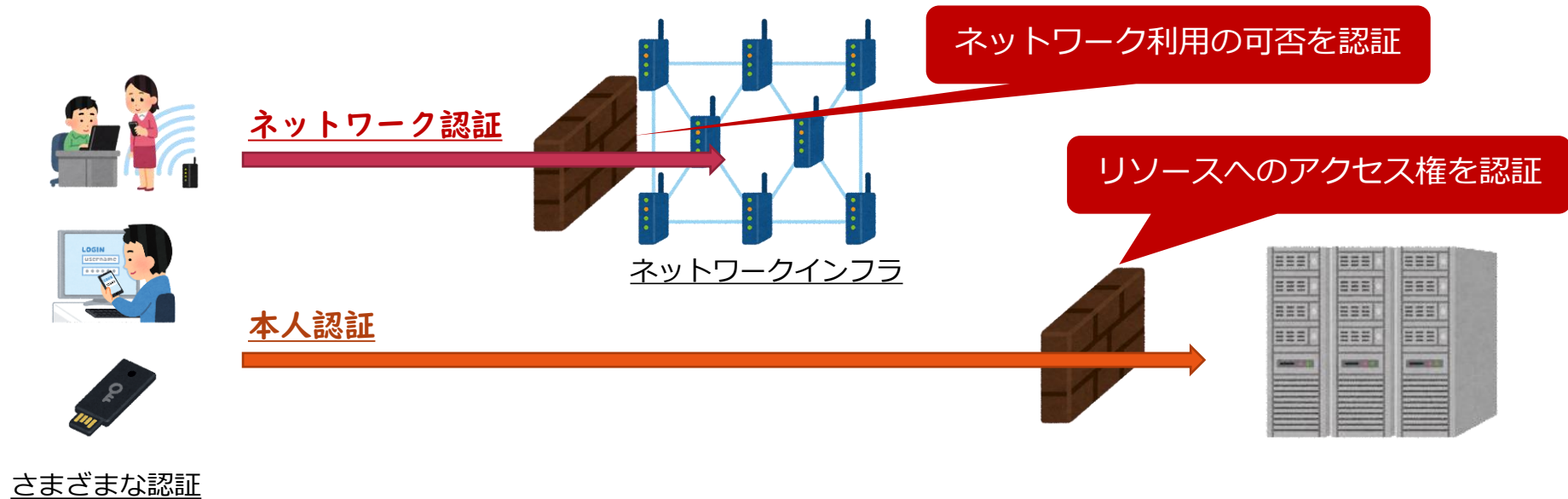
## ■ ゼロトラストだけでも、ネットワーク認証だけでも・・・

システムや情報資産の保護、利用者の安全なネットワークの活用に必要なセキュリティ対策にはさまざまな手法や技術の導入が必要となります。



## ■ 本人認証とネットワーク認証の違い

本人認証はWebアプリケーションやシステムの保護に欠かせない要素としてゼロトラストネットワークの中でも利用されています。ネットワークインフラで必要となる”ネットワーク認証”はネットワークを安全に利用するために欠かせないセキュリティ対策です。



# 拡大するランサムウェアの脅威に対する対策として

## ■ 被害経路は。。。

これまで・・・不正メール、不正サイト経由のファイルダウンロード  
現在・・・不正アクセスによる侵入、ターゲットとしての攻撃/拡散

## ばらまき型のターゲットから意図的な対象としてのターゲットへ

把握されている被害経路の半数近くが**VPN機器経由**であり、テレワーク環境の整備と合わせて対策は必須

## ■ 狙われにくいテレワーク環境へ

ID/Passwordのみの認証により運用されているテレワーク環境は、攻撃者から狙われやすい環境といえます。侵入対策を行い容易に攻撃されにくい環境を実現することは重要な予防策となります。

## ■ 侵入対策としての認証強化

アメリカの情報セキュリティを担う組織の一つであるCISAは2021年8月にリモートアクセス等の認証において単一要素認証だけを利用したシステムはセキュリティが低く、危険であるとの報告を行っています。

ご利用のテレワーク：VPN環境がID/Password認証のみの場合、直ちに侵入対策として認証手段の見直しを検討してください。



### ランサムウェアによる実害

- ・身代金による金銭被害
- ・暗号化によるサービス停止
- ・情報漏洩
- ・信頼性の喪失、復旧コスト



少しでも安全なテレワーク環境のために。。。



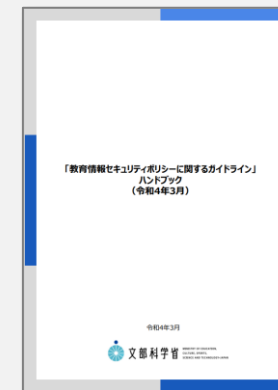


# 安全なネットワーク環境の実現に向けて

- ノートパソコンやスマートデバイスの普及により、端末のワイヤレス化が進みました。視覚化できない無線LANを利用するにあたり、端末やネットワークに対するセキュリティ確保の課題は避けて通れません。
- 各省庁からも、組織内でネットワークを利用するにあたってのガイドラインが策定されており、ネットワークセキュリティ確保においては**ネットワーク認証を導入し、不正接続を防止すべき**という指針が示されています。

## 主な省庁ガイドライン例

| 省庁名   | 指針名                                                                                                                                                                                                       | 記述                                                                                                              |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 総務省   | 地方公共団体における情報セキュリティポリシーに関するガイドライン(令和4年3月版)<br><a href="https://www.mhlw.go.jp/content/10808000/000936160.pdf">https://www.mhlw.go.jp/content/10808000/000936160.pdf</a>                                    | ネットワークに不正な機器の接続を防止するために、 <b>電子証明書による端末認証や、接続する機器のIPアドレス、MACアドレス等の認証情報を利用し制限</b> する必要がある。                        |
| 厚生労働省 | 医療情報システムの安全管理に関するガイドライン 第 5.2 版<br><a href="https://www.soumu.go.jp/main_content/000805453.pdf">https://www.soumu.go.jp/main_content/000805453.pdf</a>                                                    | 許可された者以外の無線 LAN の利用を防止するため、例えば <b>802.1xや電子証明書を組み合わせるなどして、無線LANのセキュリティを強化</b> すること。                             |
| 文部科学省 | 「教育情報セキュリティポリシーに関するガイドライン」ハンドブック(令和4年3月)<br><a href="https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_003.pdf">https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_003.pdf</a> | インターネット接続と同様に学校内の無線LANの可用性を確保することは、児童生徒の学習を止めないためにも必須事項です。 <b>無線LANの接続にはセキュリティの観点からクライアント証明書を用いることが推奨</b> されます。 |

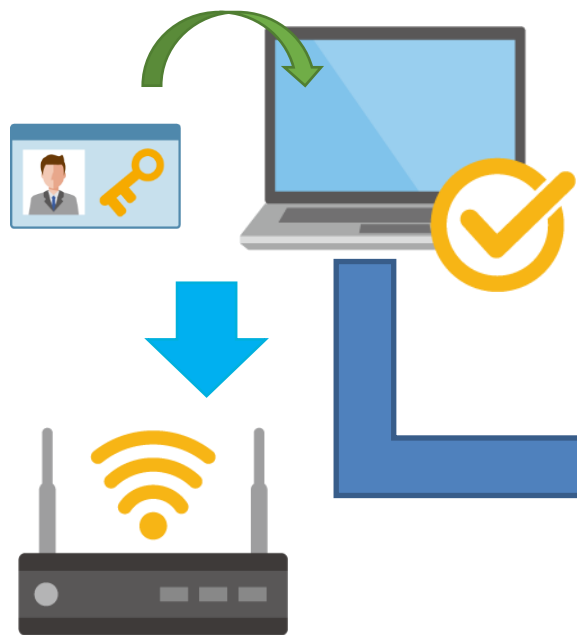


# 証明書によるデバイス認証の重要性

## ■ 無線LANで利用されている証明書認証(TLS認証)による不正接続対策

クライアント証明書を用いたデバイス認証は、主に無線LAN環境において組織から支給したデバイスであることを識別するために利用され、セキュリティ対策として広く活用されており、テレワーク:VPN環境にも導入可能です。

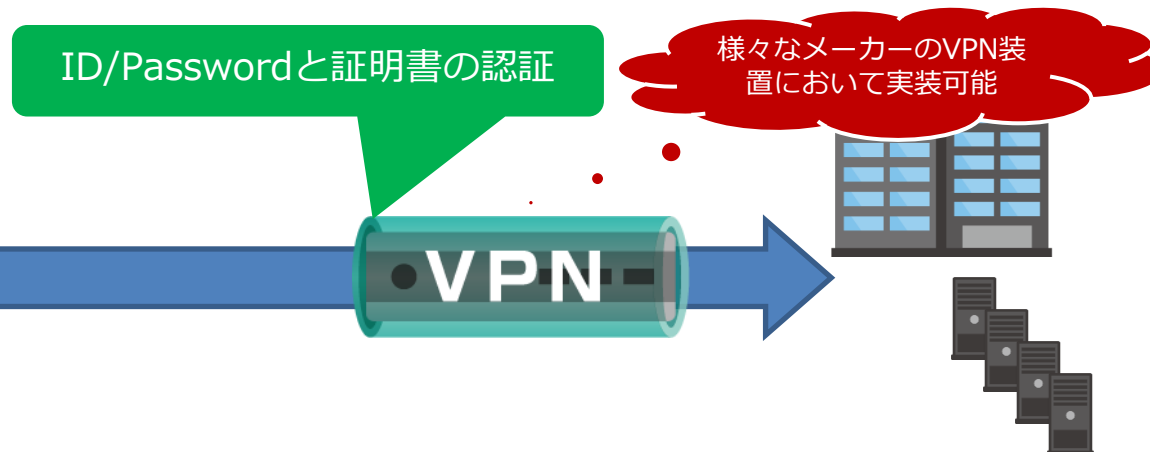
### 無線LANでは 証明書(TLS認証)利用が拡大



パソコン、タブレットなどOSを問わずに利用可能デバイス認証として利用できる仕組みの一つです。

### テレワーク：VPN接続において ID/Password + “クライアント証明書”

悪意のあるハッカーに利用・窃取されやすいID/Password情報だけでなく、端末自体が保持するクライアント証明書も認証することでVPN環境への侵入の難易度を高めることが可能です。



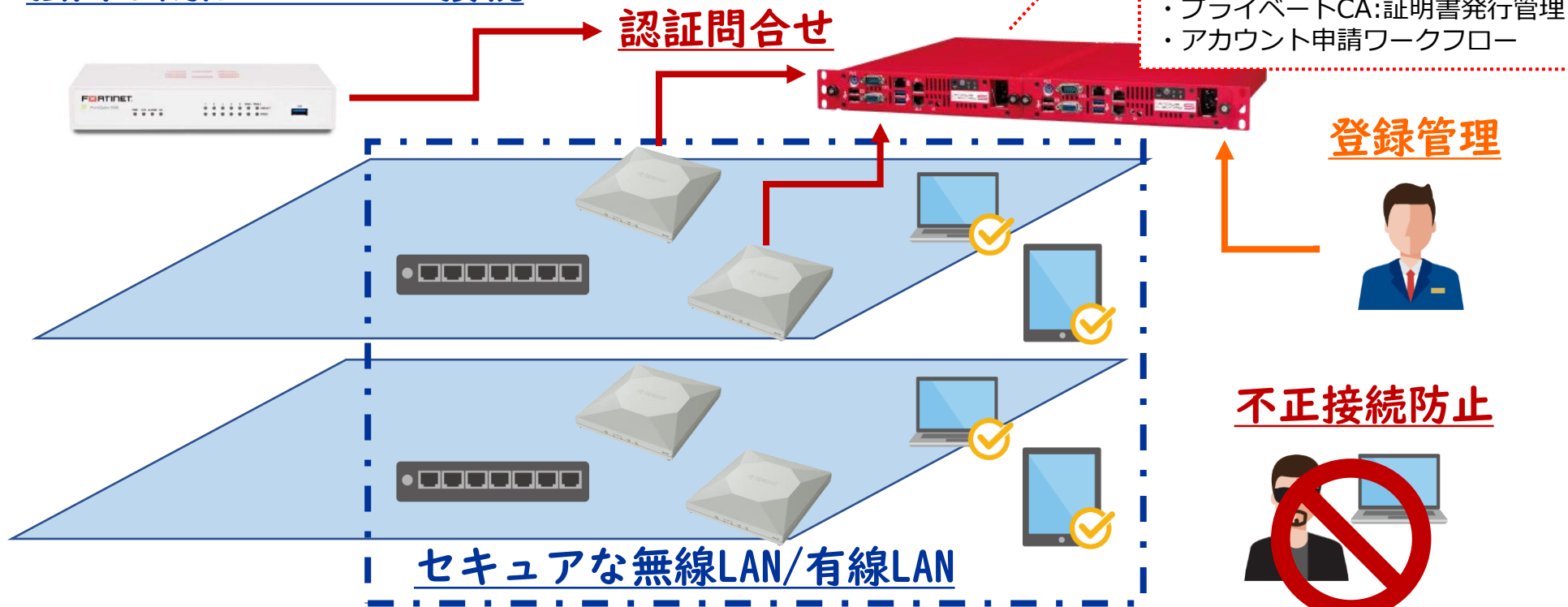
証明書認証により、テレワーク/  
無線LAN環境をより安全な認証環境へ

# 認証基盤の動作概要

## ■ 認証基盤で実現するセキュアな無線LAN・リモートアクセス

このような無線LANやリモートアクセス(VPN)環境の不正アクセス対策を実現する機能が**認証基盤**となります。専用の認証アプライアンスは認証基盤の導入・日々の運用負担を大幅に軽減し安全なネットワーク環境を実現します。

### 強固な認証によるVPN接続



# 2

## RADIUS GUARD Sとは

製品概要と主な特徴について

---

# RADIUS GUARD Sとは



## **RADIUS・CA(証明書発行)・DHCP**

国内  
開発

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

### クラウド

- Amazon AWS
- Microsoft Azure

### アプライアンス



- 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

### 仮想アプライアンス



- VMware ESXi
- Nutanix AHV
- Hyper-V

### 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

- Web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



# RADIUS GUARD Sの特徴

## ■ RADIUS GUARD S導入の特徴とメリットについて

RADIUS GUARD Sは認証基盤のサーバーとして、様々なメーカーの無線APやVPNルーターと連携し強固な認証環境を提供します。三点で他の認証基盤製品と差別化を行っています。

オールインワン

拡張性

運用負荷軽減

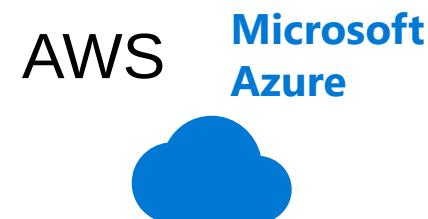
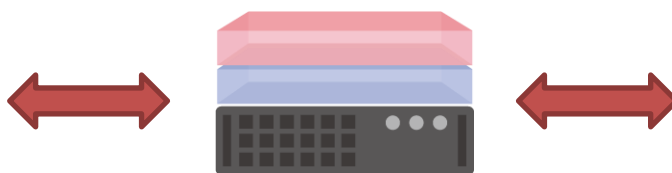
# 特徴:オールインワン/拡張性

## ■ オールインワン

- 認証基盤に必要な機能をまとめて1筐体で実現:認証(RADIUS)・証明書(CA)・DHCP
- アカウント管理に必要な様々な機能は追加オプションなく利用可能
- DHCPライセンスは初期オプション費用のみで最大1万IPアドレスの払出が可能
- ユーザー申請やキッティング環境の構築に利用可能なワークフロー機能も標準提供
- 2500ライセンス以上のモデルは外部LDAP/AD参照は標準実装(LDAPSにも対応)

## ■ 拡張性

- 最小200アカウントでスモールスタート可能。差分のみでライセンス拡張が可能
- 最大200,000アカウントまで拡張に伴うハードウェアの追加購入が不要
- RADIUSクライアントの接続数が無制限で大規模環境にも導入可能
- ユーザー環境にあわせた導入形態が選択可能(アプライアンス版/仮想版/クラウド版)
- Intuneとの連携機能による証明書自動配付(SCEP)の実現(要オプション)



## 特徴:運用負荷軽減

### ■ 運用負荷の軽減

- ディレクトリ構造によるアカウント管理で日々のアカウント改廃業務の権限委譲が可能
- ユーザーによる申請フローの実現でアカウント登録業務の簡略可
- アカウントの自動削除機能により棚卸し業務の削減
- アカウントの定期インポート(CSV)機能により登録作業を自動化
- 支援ツール:RADIUS GUARD Utilityの提供



**GOOD!!**

| RGS機能               | 工数想定                                      | 導入前工数想定                    | 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<br>場合=>約1.5人日の圧縮 |
| ユーザーツール<br>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<br>申請/承認/登録作業        | 1アカウント当たり<br>15+5+15=35min | 15min<br>(ユーザー=>承認のみ) | 1/2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<br>申請/承認/登録作業        | 1アカウント当たり<br>5+5+5=15min   | 5min<br>(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アカウント当たり<br>5+5=10min     | 2min<br>(ユーザー作業)      | 1/5工数へ圧縮                       |
| MACアドレス自動登録         | MACアドレス認証用の端末登録作業、端末<br>のMACアドレス確認作業と登録業務 | 1端末あたり<br>15~20min         | 1min<br>(登録用NWに接続)    | 1/15工数へ圧縮<br>(半自動)             |
| DHCP<br>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<br>ための登録作業           | 1端末当たり<br>10~15min         | 0min(自動化)             | 100アカウント*年2回の<br>場合=>約1.5人日の圧縮 |

# RADIUS GUARD S共通ラインナップ※24年2月～

16

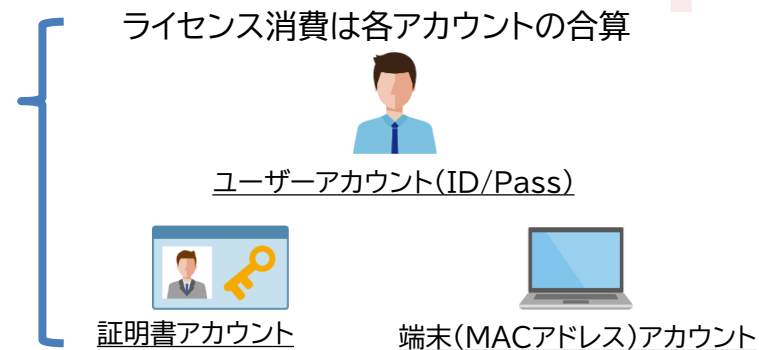
## ■ ライセンス体系一覧(希望小売価格は下記)

- 200/500ライセンス (外部LDAP/AD参照オプション無し)
- 2,500/5,000/10,000/50,000/200,000ライセンス
- DHCP専用ライセンス

## ■ オプションライセンス一覧

- 外部LDAP/AD参照オプション 60万円  
(200/500ライセンスのみ必要。2,500ライセンス以上はバンドル)  
外部LDAP/ADを参照して認証する機能
- DHCPサーバーオプション 60万円  
通常のRADIUS GUARD SにDHCP機能を追加
- API/内部LDAP登録連携オプション 60万円  
API利用、外部のLDAPクライアントから内部アカウント情報を改廃 (参照のみはオプション不要)
- アドバンスド連携オプション 60万円  
Active DirectoryにRADIUS GUARD S内部のアカウント情報を登録、Intune連携機能他
- SAML/Shibboleth SPオプション 60万円  
Shibboleth認証のサービスプロバイダ(SP)として、ネットワーク認証(WEB認証)に対応
- UPKIクライアント証明書配付オプション 60万円  
「UPKI電子証明書発行サービス」発行クライアント証明書の取り込み+配付機能

## ■ ハードウェア保守提供:ハードウェア版は最大5年のハードウェア保守(本体ライセンスと同一期間)※24年2月～



### 必要なライセンス数の目安は

- 認証するユーザー数
- 発行したいクライアント証明書数

などの合計がおおよその必要ライセンスとなります。このため、組織の人数やデバイス数と認証方式で検討

| ライセンス数  | 200       | 500         | 2,500       | 5,000       | 10,000      | 50,000      | 200,000     | DHCP専用      |
|---------|-----------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| アプライアンス | ¥ 800,000 | ¥ 1,200,000 | ¥ 1,800,000 | ¥ 2,300,000 | ¥ 2,900,000 | ¥ 3,500,000 | ¥ 5,000,000 | ¥ 1,100,000 |
| VA・クラウド | ¥ 600,000 | ¥ 1,000,000 | ¥ 1,600,000 | ¥ 2,100,000 | ¥ 2,700,000 | ¥ 3,300,000 | ¥ 4,800,000 | ¥ 900,000   |

同一筐体のまま、差額でアップグレード可能

希望小売価格表(初年度サポート込)

# 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

大好評  
負担軽減！



## ■ 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**  
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)



その負担に！

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。。。。

- ・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**  
RADIUS試験ツール

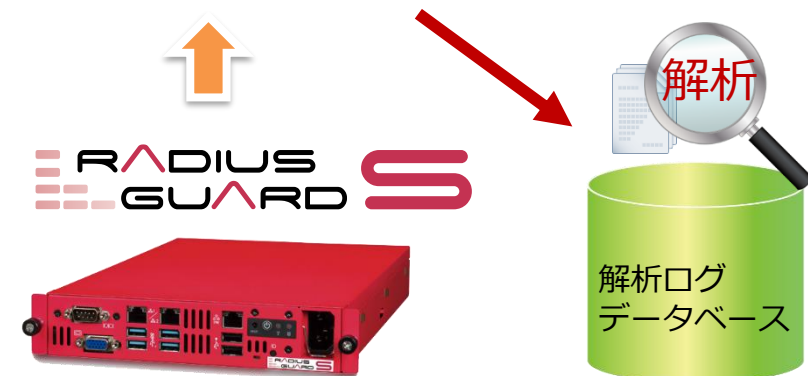
- ・PCから各種認証パケットの簡易試験(PAP/CHAP/MS-CHAPv2/EAP-PEAP・TLS)
- ・標準属性(Attribute)の追加が可能
- ・試験結果のテキスト出力
- ・連続試験条件の設定

# Log@Adapter+のご紹介

## 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



### 【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. | <input type="checkbox"/> 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   | <input type="checkbox"/>    | ログイン   | 2018/09/20<br>15:09:00 | 2018/09/20<br>15:04:08 | 192.168.1.100<br>(192.168.1.100) |        | 3   | test | aa:bb:cc:dd:ee:ff | 192.168.1.100 | 1   |         |       |             |      |
| 2   | <input type="checkbox"/>    | 認証成功   | 2018/09/20<br>15:08:59 | 2018/09/20<br>15:04:07 | 192.168.1.100<br>(192.168.1.100) |        |     | test |                   |               |     |         |       | radius auth |      |
| 3   | <input type="checkbox"/>    | ログイン失敗 | 2018/09/20<br>15:08:29 | 2018/09/20<br>15:03:37 | 192.168.1.100<br>(192.168.1.100) |        | 3   | test | aa:bb:cc:dd:ee:ff | 192.168.1.100 | 1   |         |       |             |      |
| 4   | <input type="checkbox"/>    | 認証失敗   | 2018/09/20<br>15:08:29 | 2018/09/20<br>15:03:37 | 192.168.1.100<br>(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



# OneID@Adapterのご紹介

## オンプレミスタイプのSSOアプライアンスサーバー（ハードウェア/VA版による提供）

### ■OneID@Adapter Webポータルへの一度のログインで、複数のサービスにシングルサインオン

- シングルサインオン標準規格であるSAML(Security Assertion Markup Language)に対応
- SAML非対応Webサービスを対象とした認証には、ブラウザ拡張機能※を使用した代理認証を併用可
- OneID@Adapter登録アカウントごとに、Webサービス利用可否を設定可能
- 証明書やワンタイムパスワードを利用した多要素認証に対応

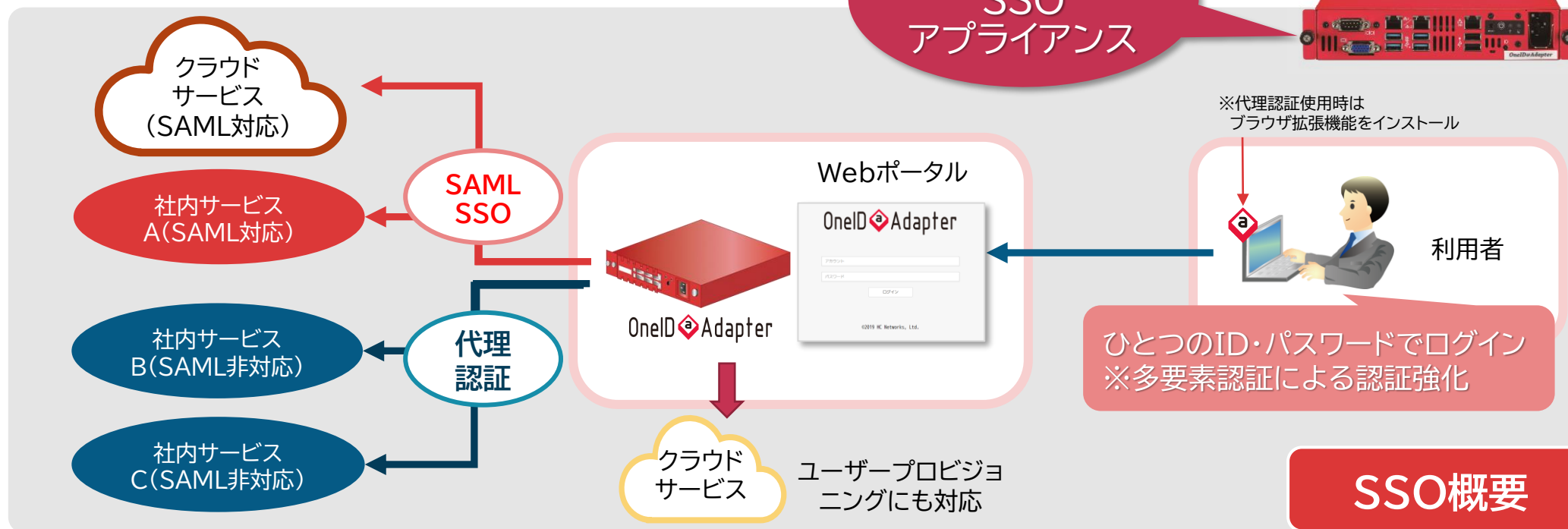
外部接続ができない閉域NWや、環境において  
IdP機能を外部サービスに依存しないSSOを提供

# OneID@Adapter

オンプレミス型  
SSO  
アプライアンス



※代理認証使用時は  
ブラウザ拡張機能をインストール



# 3

## 主な実績

---

# RADIUS GUARD Sの導入実績

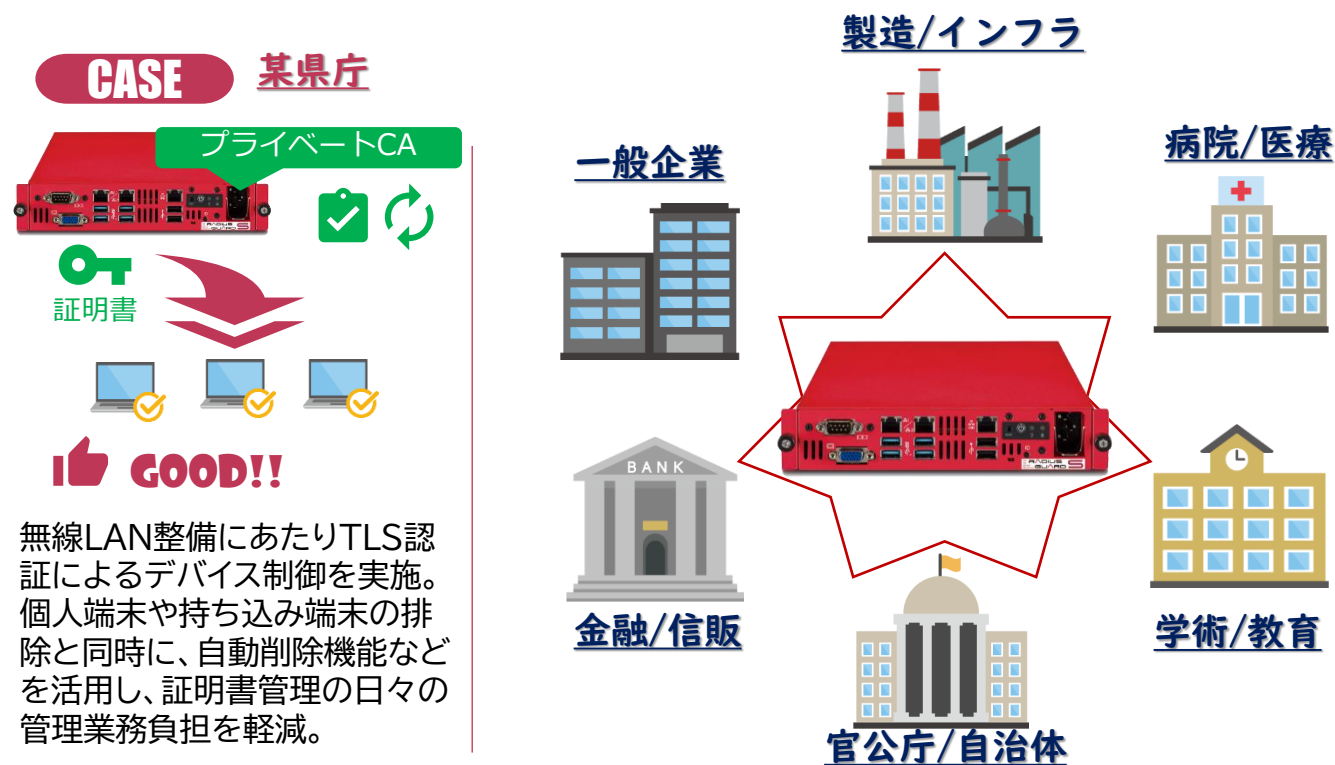
## ■ 豊富な導入実績と事例

シリーズ累計の出荷台数は**9000台以上**。

某県庁、市役所などのセキュリティ強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

無線LAN構築、テレワーク環境整備などのRADIUS認証、CA、DHCPサービス向けに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



**RADIUS GUARD S**

さまざまな業種業態において主に無線LANやリモートアクセス環境でのセキュリティ強化のための認証基盤として導入いただいております。

他製品にない独自の機能とコストパフォーマンスで不正接続対策をサポート。

実際の導入/適用可否のご相談等もお受け付けしておりますのでお気軽に製品サイトからお問い合わせください。

# 自治体導入実績のピックアップ

22

## ■ 京都府様



京都府 様 **NEW!!**

802.1×認証

CA（証明書管理）

DHCP

柔軟なオフィス構成と組織変更に対するスピーディな対応が可能な無線LANの整備とともに不正接続対策も実現。DHCP運用と合わせた認証基盤を導入



詳細を見る



PDFをダウンロード

## ■ 茨城県大子町様



茨城県大子町 様 **NEW!!**

802.1×認証

CA（証明書管理）

DHCP

新庁舎の移転に合わせてLGWAN系及びインターネット系向けの無線LAN用のTLS認証によるセキュリティ確保のため、オールインワン認証基盤として導入。

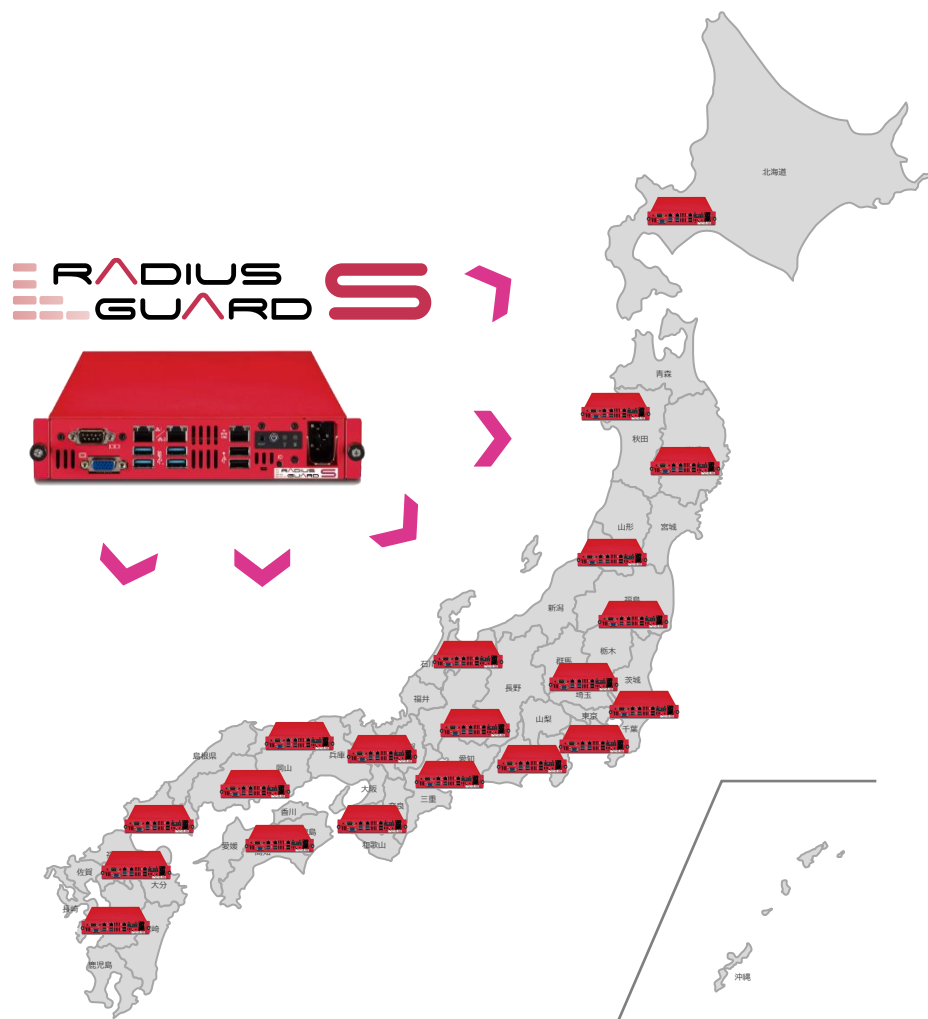


詳細を見る



PDFをダウンロード

# 全国公共/自治体での導入事例増加中



## ■ 無線LANの拡大とともに導入事例増加

各県庁、市町村における新庁舎や移転、ネットワーク更改のタイミングでTLS認証の導入時にご選択いただいております。LGWAN/Internet系の無線LAN利用に欠かせない認証基盤となっております。

20年度はGIGAスクール構想に伴い、教育委員会向けの導入が大幅に増加しました。センター集約型による導入で、一括管理による運用負荷軽減をご支援しています。

| エリア | 主な公共実績                 |
|-----|------------------------|
| 北海道 | 公共施設及び大学病院等            |
| 東北  | 県庁、教育委員会等              |
| 北陸  | 市町村、教育委員会等             |
| 関東  | 県庁、市町村、教育委員会、大学病院等     |
| 中部  | 県庁、市町村、教育委員会等          |
| 関西  | 県庁、市町村、教育委員会等          |
| 中国  | 県、市町村、教育委員会、大学病院等      |
| 四国  | 公立大学等                  |
| 九州  | 公立大学、大学病院等             |
| その他 | 官公庁、社団法人、公益法人、外部団体、警察等 |



# 豊富な導入実績

## ■ RADIUS GUARDシリーズ 出荷実績：累計9,000台以上

### 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

朝日放送テレビ株式会社様

株式会社メイテツコム様

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

日本工営株式会社様

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)

静岡ガス株式会社様 (AWS対応版)

株式会社日阪製作所様

株式会社電算システム様

#### 文教

国際基督教大学様

慶應義塾大学様

浅野学園様

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

秋田県大仙市教育委員会様

茨城県大子町様

京都府庁様

#### 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)



# 6

## 提案・導入のご支援について

---

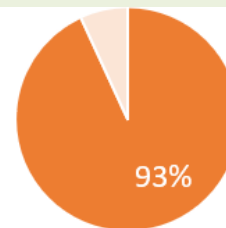
# RADIUS GUARD のサポートポイント

26

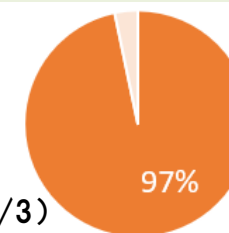
## 国産ならではの 優れた品質と手厚いサポート

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



### サポート内容に満足



サポートセンター  
満足度調査  
(2018/7~2019/3)

## 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のお貸し出し等

27

## ■ サービス概要

- RADIUS GUARD Sを安心してご利用頂くために、動作確認や相互接続検証にご利用頂ける無償検証機貸出サービスを行っております。

## ■ 貸出内容

- ハードウェアアプライアンス本体＋フルオプション : 一か月
- 各VA版(DVDもしくはDL提供)＋フルオプション : 三か月
- 各クラウド版(提供形態は下記)＋フルオプション : 三か月
  - AWS対応版…共有AMI
  - Azure対応版…Azure Marketplace

## ■ 貸出条件

- 貸出のご相談・貸出後のお問い合わせにつきましては、弊社営業までご連絡ください。
- 検証機在庫状況によりましては、貸出時期がご希望に添えない場合がございます。
- 貸出に関わる送料負担は双方元払いとなります。※VA版につきましては返却不要です。
- AWS対応版は、AWSアカウントIDのご教示をお願いいたします。

## ■ 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

## ■ 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

#### ■ 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
- ・ RADIUS GUARD S\_設定ガイド(冗長構築).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付).pdf
- ・ RADIUS GUARD S\_設定ガイド(Intune連携).pdf
- ・ RADIUS GUARD S\_設計ガイド(時短バージョンアップ作業).pdf
- ・ RADIUS GUARD S\_設計ガイド(MACアドレス自動収集).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

### ■ 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 Meraki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 PEAP-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
- ・ RADIUS GUARD S\_設定ガイド(FURUNO SYSTEMS ACERA編).pdf
- ・ RADIUS GUARD S\_設定ガイド(Juniper Mist編)
- ・ RADIUS GUARD S\_設定ガイド(Panasonic AIRRECT編)
- ・ RADIUS GUARD S\_設定ガイド(LOG@Adapter+)

## その他のご支援について

---

### ■ 其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

### ■ プライベートハンズオン対応

外販取扱検討や導入検討時に、RADIUS GUARD Sの操作方法や認証基盤に関するご相談などに対応可能なハンズオンを無償で対応させていただいております。ご希望の場合は別途、弊社担当営業までご相談ください。



## 著作権及び免責事項

- RADIUS GUARDおよび、RADIUS GUARDロゴは、SCSK株式会社の登録商標です。
- 本書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。
- 本書に記載されている製品仕様及び事柄は、将来予告なしに変更することがあります。
- 本書を用いた場合におけるいかなる事象、結果においてSCSKは一切責任を負いかねます。
- 記載の内容は2023年11月現在のものです。

## Contact us

SCSK株式会社

ネットワーク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

<https://www.scsk.jp/sp/radius/>

製品に関するお見積・個別案件のご相談や製品説明・デモ・ハンズオンのご依頼先について

[rg-staff@scsk.jp](mailto:rg-staff@scsk.jp) までお問い合わせください。