RADIUS GUARD S　SPECIAL INTERVIEW　SCSK

急増するVPNや無線LAN、不正アクセスは大丈夫？簡単にセキュリティを向上するには

「当たり前」になったVPNや無線LANの認証セキュリティを見直せ

テレワークやモバイルデバイスの利用が拡大する今、「VPN」や「無線LAN」は業務に必要不可欠となっている。だが普及が進むにつれ、従来のID・パスワードなどによる認証方式だけでは、不正アクセスの被害を受ける危険性が高まっている。認証要素を増やせばセキュリティは強化されるものの、利便性は損なわれ、運用管理の負担が増える可能性もある。安全なアクセスと利便性、運用管理の負荷軽減を実現する手段はあるのだろうか。

SCSK株式会社
プロダクト・サービス事業グループ
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　営業第一課
マネージャ
泉水 正則 氏

SCSK株式会社
プロダクト・サービス事業グループ
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　営業第一課
プロフェッショナル プロダクトスペシャリスト
尾崎 一平 氏

VPNや無線LANの利用拡大で浮上したセキュリティの脅威

近年、働き方改革の一環でテレワークの普及が進み、業務でモバイルデバイスを活用する機会が急増した。社員1人につきノートPC、タブレットなど複数のデバイスを支給する企業も珍しくない。

接続デバイスの多様化により、社内システムにアクセスする手段も有線から無線LANへと変化した。柔軟な働き方を支援するために社内をフリーアドレス制にする例も増えており、どこからでもアクセスできる無線LANは、今や「通信インフラの主役」と言っても過言ではない。

しかし、無線LANの利便性の高さは、見方を変えれば「意図しない人やデバイスが社内システムに簡単にアクセスできる危険にさらされた状態」とも言える。ファイアウォールで外部からの不正アクセスやデバイスの情報漏えい、デバイスのウイルス感染の脅威を対策しても、その中間となるネットワーク接続のセキュリティを意識できていない企業も少なくない。

最近のインシデントとしては、コロナ禍でテレワークを行う国内企業38社がVPN（仮想専用線）で社内ネットワークにアクセスする際のID・パスワードが流出し、不正接続の被害を受けたというニュースが記憶に新しい。まさにネットワーク接続時のセキュリティが重要であることを示す例だ。

年々、巧妙化するサイバー攻撃から機密情報を守り、ネットワークの適正利用を確保するには、現状のネットワークに合わせたセキュリティ対策を施すことが急務である。従来のID・パスワードや証明書など複数の要素を掛け合わせた多段認証でいまこそVPNや無線LANを含むネットワーク接続の認証基盤を強化すべきだ。

だが、認証要素を増やせば強固なセキュリティが実現するものの、ユーザーの利便性が損なわれたり管理者の負担が増大したりする懸念がある。いかにしてそのバランスを実現すれば良いのだろうか。

管理者の負荷をかけずに認証の運用管理を可能に

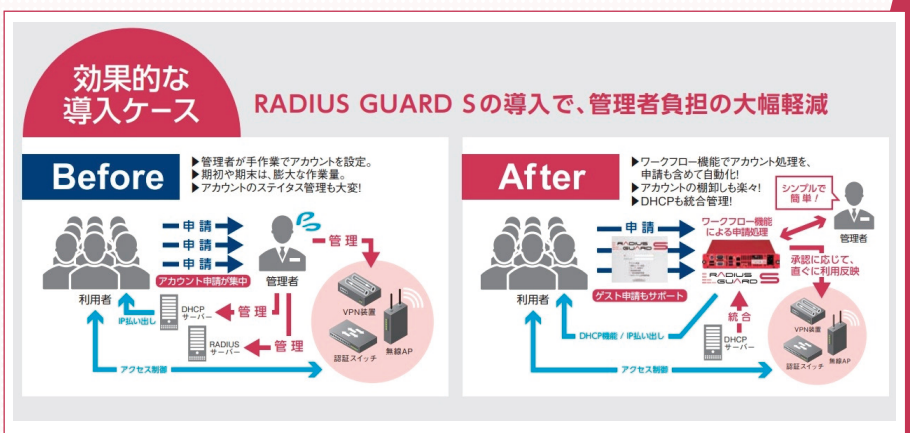
もちろん、認証の仕組みを新たに設ければ、その分、認証情報の管理が増加し、IT管理者の負担は確実に増加する。それを抑止するのが、SCSKの「RADIUS GUARD S（ラディウスガードS）」が提供するワークフローの仕組みだ。これについてSCSK プロダクト・サービス事業グループの尾崎 一平氏は次のように話す。

「ユーザーがブラウザーの申請画面に直接アクセスし、メールアドレスやIDなど申請に必要な任意の項目を登録します。管理者の作業は、ユーザーの申請情報を確認して内容に問題なければ承認ボタンを押すだけです。RADIUS GUARD Sの認証データベースに申請内容に沿ったユーザー情報や自動取得されたデバイス情報等が登録され、ユーザーは電子証明書のダウンロードが可能となります」（尾崎氏）

紙やメールの申請処理は不要であり、誤った申請内容のユーザーへの修正依頼や認証データベースへの登録など煩雑な作業も不要だ。無線LAN接続への認証要素を追加してもユーザーの利便性を損なうことなく、セキュアなアクセスが実現できるのである。

なおRADIUS GUARD Sは、外部のLDAPやActive Directory のアカウント情報を参照した認証も可能である。Active Directoryに登録済みのユーザーであれば、管理者の承認なしで、ゲストにアクセス権限を付与できるようなワークフローも実現可能だ。

その他にも、接続したいデバイスから申請すればMACアドレスの自動取得機能（DHCPオプション併用）もあるため、デバイスによる認証方式を採用する企業では、デバイス情報を元にしたアカウント登録のワークフローもスムーズに実行可能だ。



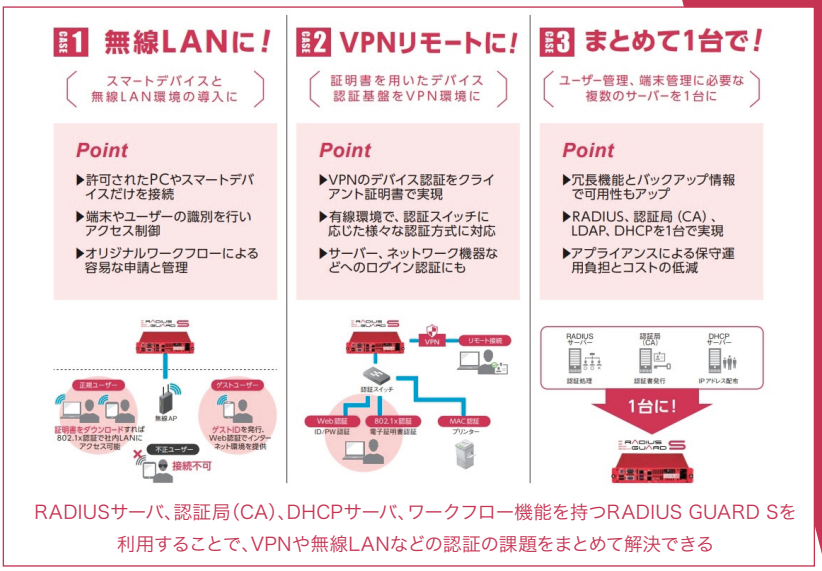
RADIUS GUARD Sの導入は管理者の負担を減らすことにもつながる

アプライアンス1台で不正なネットワーク接続を抑止

無線LANの利用やVPNによるネットワーク接続が拡大する中、脅威の侵入を防ぐ1つの手段として挙げられるのが、接続時の認証セキュリティ対策だ。すなわち許可した適切なデバイスだけを接続し、それ以外を遮断するというアプローチである。

これを実現する製品の1つがRADIUS GUARD Sである。尾崎氏は次のように説明する。

「RADIUS GUARD Sは、有線、無線LANとVPN接続への不正接続防止に必要な認証機能が搭載されたアプライアンス製品です。RADIUS認証、プライベート認証局(CA)などによる認証基盤機能から、DHCPサーバとしての機能、認証情報の申請・承認を行うワークフローまでが1台の筐体(きょうたい)に含まれています。個別に認証用のサーバを構築するのに比べて無線LAN接続の認証強化を短期間で実現し、セキュリティ対策にかかる費用や人的リソースを大幅に軽減できます」(尾崎氏)



RADIUSサーバ、認証局(CA)、DHCPサーバ、ワークフロー機能を持つRADIUS GUARD Sを利用することで、VPNや無線LANなどの認証の課題をまとめて解決できる

複数要素による多段認証の実現には、「人」や「デバイス」など異なる属性を識別できる仕組みの構築が必要不可欠だ。たとえば、ID・パスワードのように人が記憶する情報だけでは、意図しないデバイスの利用や、ID情報の漏洩で容易に社内システムにアクセスできてしまう。そこで、デバイスの識別に必要な要素であるMACアドレスと電子証明書を組み合わせることでセキュリティ確保する多段認証環境が実現する。

ディレクトリ単位のアカウント管理で運用の自動化を実現

ネットワークに接続するセキュリティポリシーは、役員や一般社員、ゲスト、デバイス毎でそれぞれ異なるケースも多いはずだ。RADIUS GUARD Sでは、任意のセキュリティポリシー別にディレクトリを作成しアカウントを登録することでディレクトリ単位の管理ができる。システム管理者とは別にディレクトリの管理者権限を持つアカウントを自由に作成できるため、管理者の日々の業務が分散され、アカウント管理の省力化、さらには自動化も実現できる。

ディレクトリ単位のアカウント管理による運用自動化の具体例を尾崎氏はこう説明する。

「大学を例に挙げると、頻繁にデバイスを交換する学生のディレクトリは、たとえば『最終接続日から1カ月以上アクセスを確認できないアカウントを認証データベースから自動的に削除する』というルールを設けて運用管理を効率化することもできます。一方、任期の定めがない教授のディレクトリは接続の有効期限を設けないなど、学生のディレクトリとは異なるルールを設けることも可能です」(尾崎氏)

また、既存の資産管理ソフトから払い出された情報とRADIUS GUARD Sを連携させれば、MACアドレスの更新・削除などのデバイス管理を手動で行う必要もなくなる。

マルチプラットフォーム下の冗長構成でBCP対策にも有効

RADIUS GUARD Sは拡張性にも優れた製品で、1台の筐体で200ユーザーから20万ユーザーまでカバーしている。他の認証アプライアンス製品の場合、たとえば導入当初はID・パスワードによる認証方式しか設定していない企業が、MACアドレスや電子証明書など認証要素の追加を検討すると、ライセンス数不足で筐体を交換せざるを得ない場合もある。最大20万ライセンスまで追加できるRADIUS GUARD Sであれば、導入後に認証要素を増やしても、ライセンスの拡張で対応できるため、筐体の追加購入は不要だ。

近年、IT基盤のクラウド移行が進むことで、オンプレミスの仮想化基盤やマルチクラウドとハイブリッド環境で業務システムを運用する動きが活発化している。こうしたニーズに応えてRADIUS GUARD Sは、VMwareやNutanixAHVで稼働する仮想アプライアンス版と、AWSやAzureなどのパブリッククラウド上で稼働するクラウド版も用意している。マルチプラットフォームに対応する強みを、尾崎氏は次のように話す。

「大企業の多くは、仮想化基盤やクラウドなど複数のプラットフォームに分散して業務システムを運用しはじめています。たとえば、本番環境を本社のオンプレミスのハードウェア、DR(ディザスタリカバリ)環境にクラウドを採用するなどの形もみられます。RADIUS GUARD Sであれば導入企業の多様なシステム構成に合わせて、冗長構成も組め、BCP対策でも利用できる点が強みです」(尾崎氏)

これは何も一般企業に限ったことではない。SCSKのプロダクト・サービス事業グループ 泉水 正則氏は、自治体でのニーズの高まりを次のように説明する。

「2020年5月に総務省が発表した『自治体情報セキュリティ対策の見直し』の中でも、自治体内部環境からパブリッククラウドへの接続による業務効率向上が明記されるなど、多くの場面でクラウドサービスの利用が見込まれ、複数のプラットフォーム対応は必須となっています」(泉水氏)

リコーや朝日放送テレビなど幅広い業種のネットワークセキュリティに貢献

煩雑な複数要素による多段認証の運用管理を軽減できるメリットや拡張性の高さからRADIUS GUARD Sはさまざまな業界で利用されている。国内で複写機・複合機のトップシェアを誇るリコーもその1社だ。

「リコーさまは、国内約280拠点と関連会社12社などグループ全体で共通の無線LAN環境再構築のため、RADIUS GUARD Sを導入されました。導入事例としては最大規模の約5万ユーザー、約10万デバイスのアクセス制御を電子証明書で徹底することで、無線LANのセキュリティ強化と運用管理の統一化を実現しています」(泉水氏)

朝日放送テレビではRADIUS GURAD Sの機能をフルに活用し、社内インフラにアクセスするユーザーやデバイスの可視化、ゲストユーザーと外部デバイスの認証フローの簡素化や不正アクセス防止などを実現している。

近年では、文部科学省が打ち出した「GIGAスクール構想」で、小中学生に支給するデバイスのセキュリティ対策に全国各地の教育委員会向けの問い合わせもあり導入が増えているという。

また、コロナ禍の影響で急ぎテレワークの対応に迫られ、多くの企業が無線LAN、VPN接続環境の最適なセキュリティ対策を模索している状況だ。この課題に対し、「無線LAN、VPN接続環境のセキュリティリスクを減らすには、ID・パスワードだけに依存しない多層防御が欠かせません」と泉水氏は指摘する。

最後に尾崎氏は、無線LANやVPN接続のセキュリティ対策に課題を抱える企業に対しこう締めくくった。

「さまざまな業態業種の企業にRADIUS GUARD Sを導入した経験から、SCSKでは無線LANやVPN接続のセキュリティ対策や、最適な認証の組み合わせ方・連携機器実績など豊富なノウハウがあります。これからの時代に適した働き方の実現を見据え、ネットワーク接続のセキュリティを強化したい企業はぜひお気軽にご相談ください」(尾崎氏)

SCSK株式会社
プロダクト・サービス事業グループ
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
東京都江東区豊洲3-2-20 豊洲フロント
TEL : 03-5859-3037　E-mail : rg-info@scsk.jp
https://www.scsk.jp/sp/radius/