News Release

2016 年 9 月 16 日
SCSK株式会社

不正通信端末を自動排除、ブラックリスト機能で高セキュア環境を実現
「RADIUS GUARD® S」 最新ソフトウェア提供開始

SCSK株式会社（本社：東京都江東区、代表取締役社長：谷原　徹、以下SCSK）は、セキュリティを強化し、不正通信端末の自動排除を実現するブラックリスト機能をサポートした「RADIUS GUARD® S」（ラディウスガード　エス）の最新ソフトウェアの提供を9月16日から開始します。

1. 背景

現在の企業・組織では、IoTやビッグデータ、クラウドサービスの普及、企業のグローバル展開などにより、ネットワークを通じた情報資産の活用が進んでいます。しかし、サイバー攻撃や内部の不正通信などで企業の重要情報が漏えいする事件・事故は後を絶たず、昨今では標的型攻撃に代表されるマルウェア感染による情報漏えいの被害も増加しています。

これらの不正通信を遮断する製品や仕組みは多数存在しますが、多くの場合、ネットワークのゲートウェイ上で不正と検知した通信（シグネチャやふるまいなど）をトリガーに、一時的に通信を遮断するのみで、継続的な遮断の仕組みを実現することは難しく、特にゼロデイ攻撃といった新たな不正通信の試みによっては検知漏れが発生するなど、本当の意味での情報漏えい対策は厳しい状況でした。またゲートウェイを通らない内部ネットワークのみに限った不正通信は防御する仕組みは難しいことから、新たな課題も発生しています。

そのような中、「RADIUS GUARD® S」最新ソフトウェアでは、これらの課題を解決するために不正通信端末をブラックリスト化する機能を追加し、不正と判定された通信の特定に応じて、端末に紐付くアカウントまで自動で無効化して、不正通信を根本から排除する仕組みを実現しました。

2.「RADIUS GUARD® S」 最新ソフトウェア

「RADIUS GUARD® S」は、認証に必要な要素を網羅したスタンダードな認証アプライアンスです。オンプレミスからクラウドまで幅広くサポートする高精度な認証環境の提供と運用負荷の低減を実現することから、多くのお客様にご支持いただき、既に5,000台を超える導入実績があります。このたび新たに提供開始する「RADIUS GUARD® S」の最新ソフトウェアでは、以下の機能を強化しました。

（1）強化ポイント

① ブラックリスト機能

syslogサーバー（弊社推奨品）で受信したセキュリティログ※1を参照し、不正通信を行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する機能です。ブラックリストに登録されたアカウントは「RADIUS GUARD® S」の認証処理において、拒否を行いますので、付随する認証スイッチや無線アクセスポイントが接続を拒否することから、その後のネットワーク利用が不可能になり、セキュリティの強化が実現できます。

※1 セキュリティログは、IPSなどのsyslogに対応したセキュリティ機器から出力された情報を使用します。
（連携の実績などは適宜RADIUS GUARD® オフィシャルサイトをご覧ください。）

② アカウント登録時のMACアドレス自動取得、紐付け機能

利用者がアカウント申請を行った際、自動的に申請を行った機器のMACアドレスを収集し、申請において許可されたアカウントと自動的に紐付けて記録します。
この機能を利用することで、認証処理においてアカウントの申請を行った時点の端末かどうかも自動チェックを行って認証処理を行うので、アカウントの使い回し防止はもちろん、運用における利便性も向上します。

(2)「RADIUS GUARD® S」の基本機能について

① ネットワーク認証に必要な五大機能※2(RADIUSサーバー、認証局(CA)、LDAPサーバー、DHCPサーバー、ワークフロー)をオールインワンで実現します。

② 全ての機能を1U(EIA規格)ラックのハーフサイズ筐体に凝縮し、省スペース設置を実現します。

※2 五大機能

・RADIUSサーバー
Web、MAC、802.1Xの各認証に対応

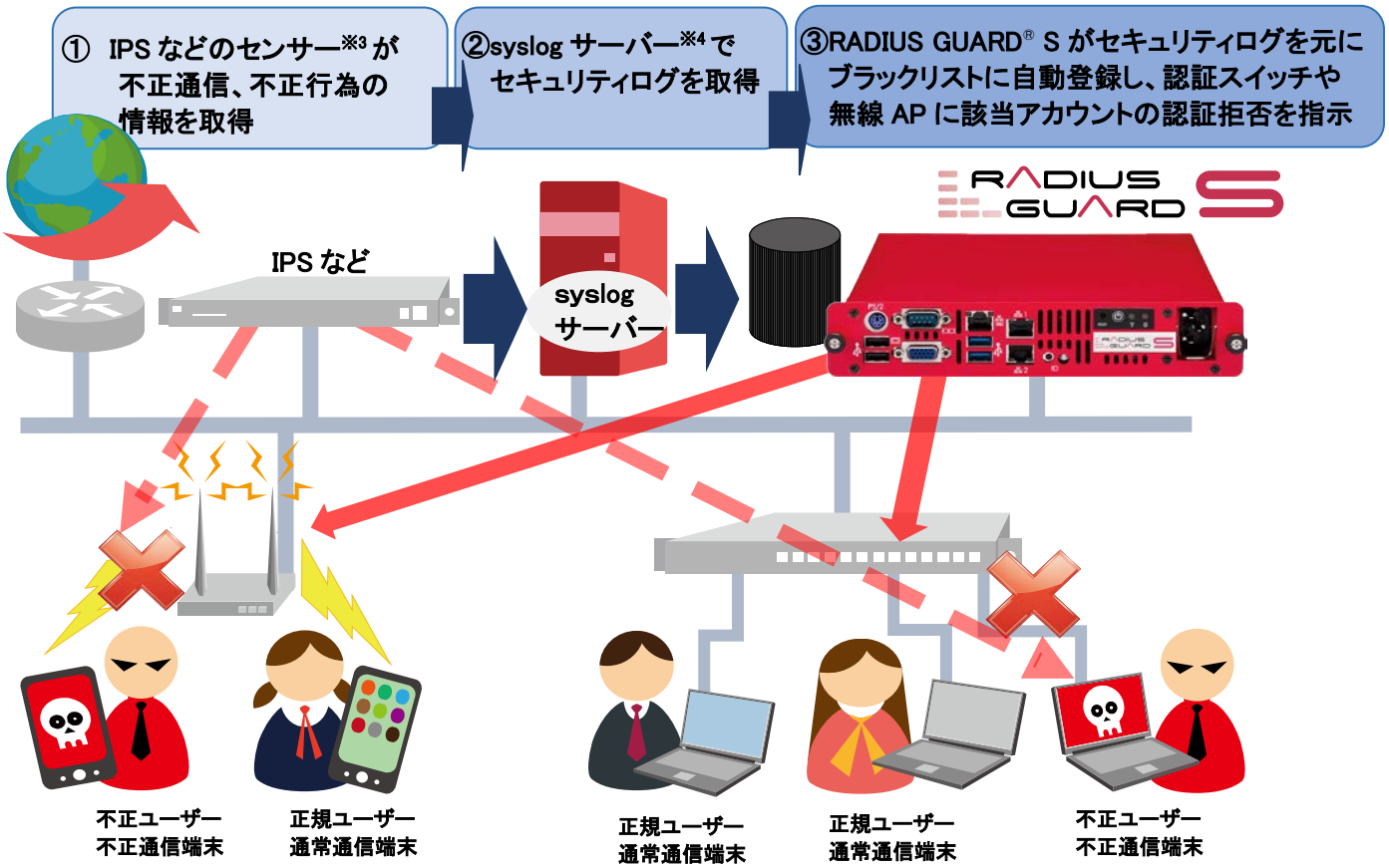
・認証局(CA)
証明書発行/証明書管理機能、PCはもちろんスマートデバイスにも対応

・LDAPサーバー
ユーザー管理、端末管理、認証情報管理機能

・ワークフロー
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で処理するワークフロー機能

・DHCPサーバー(オプションライセンス)※1サーバー1万IP払出し可能
統合マスタ管理機能により、最大IPアドレス5万IP払い出しと管理に対応

「RADIUS GUARD® S」 ブラックリスト機能動作イメージ



※3 syslog出力に対応するIPSなどのセンサー機器が必要です。

※4 「RADIUS GUARD® S」がブラックリスト連携するsyslogサーバーは、SCSK推奨品のみの対応です。
現在(2016年9月時点)はHC-NET製LOG@adapter(Ver5.02以降)が、SCSK推奨品となります。

「RADIUS GUARD® S VA」も同時サポート

最新ソフトウェアでサポートされる機能は、仮想サーバーで動作する仮想アプライアンス版「RADIUS GUARD® S VA」（ラディウスガード エス ブイエー）でも同様にサポートいたします。

「RADIUS GUARD® S」最新ソフトウェアバージョン表記について

ブラックリスト機能、MACアドレス自動取得、紐付け機能を追加した最新ソフトウェアを適用した場合のバージョン表記は6.05となります。
既に「RADIUS GUARD® S」、「RADIUS GUARD® S VA」をご利用いただきサポートのご契約をいただいているお客様には弊社サポート窓口より最新バージョンソフトウェア、および最新マニュアルをご提供いたします。

3. 「RADIUS GUARD® S」製品価格

「RADIUS GUARD® S」本体（200認証ライセンス搭載）・・・・・・・・・・・・・・・・・79万円（税抜）～

※上記金額に、初年度のサポート費用が別途必要です。（24時間365日保守など、さまざまなメニューを用意）
サポート契約を締結いただいているお客様は本件ソフトウェアを含め、常に最新ソフトウェアを提供いたします。
※「RADIUS GUARD® S VA」の価格はお問い合わせください。
※SCSKでは導入設置サービス/設計サービスも用意しています。費用はお問い合わせください。

4. 販売目標

2018年3月期までに、売上8億円 （ソフトウェア保守、各種導入サービスも含む）を目指します。
通信事業者、データセンター事業者、電子商取引（EC）事業者、銀行、証券、保険などの金融事業者、大学をはじめとする文教ネットワーク、機械、電子などの製造業、商社、小売などの流通事業者などを中心に、製品の販売をすすめてまいります。

本件に関するお問い合わせ先

【製品に関するお問い合わせ先】
SCSK株式会社
IT エンジニアリング事業本部 ネットワーク部
電話：03-5859-3034
E-mail：RG-info@ml.scsk.jp
RADIUS GUARD® S 製品サイト：http://www.scsk.jp/product/common/radius/

【報道関係お問い合わせ先】
SCSK株式会社
広報部 西広
電話：03-5166-1150