未来を拓くチカラと技術。

NTT AT

News Release

2019年4月24日
NTTアドバンステクノロジ株式会社

# マルウェア防止ソリューションで重要資産を防御

## ～特許技術ファーストパケット認証を採用したBlackRidgeTACソリューションの販売開始～

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：神奈川県川崎市、代表取締役社長：木村丈治）は、BlackRidge Technology, Inc（以下：BlackRidge、本部：ネバダ州、CEO：Bob Graham）のBlackRidge TAC（Transport Access Control）ソリューション（以下：本製品）販売において、BlackRidgeと代理店契約を締結し、2019年4月から販売を開始しました。

本製品は、ゼロ・トラストネットワーク時代におけるネットワークセキュリティの一つ、マイクロセグメンテーションを提供します。BlackRidge 特許技術のファーストパケット認証（後述）により信頼できない第三者からのアクセスを防ぎ、情報漏えいなどのセキュリティインシデントが発生する前に防御します。

NTT-AT は、セキュリティビジネスを重点分野の一つと位置づけており、さまざまなセキュリティ製品およびサービスを提供しています。今般、本製品をラインナップに追加することで、既存のセキュリティ商材と組み合わせたより高度なセキュアソリューションの提供が可能となります。

### １．背景

TCP/IPプロトコルは、「つながる」ことを目指す世界を実現し、多くのイノベーションが生まれました。同時に、攻撃者にとっても利用しやすいためセキュリティインシデントの温床になっており、増え続けるセキュリティ脅威への防御対策として、多種多様なセキュリティ製品・ソリューションが開発され世の中に提供されています。

しかし、昨今サイバー攻撃は巧妙化しており、従来のFW、IPS/IDSなどで守れている環境さえも、セキュリティ脅威にさらされています。実際に一度マルウェア攻撃などで内部ネットワークに侵入されると、横の端末、隣のセグメントへと瞬く間に侵食されていきます。そして、最終的には目的の情報資産にたどり着き、外部へ情報漏えいする事例も多く存在します。

NTT-AT はセグメントや端末毎に個別アクセス制御、セキュリティ対策を実施する「マイクロセグメンテーション」が上記脅威に対し、有効な防御策として考えています。守りたい情報資産に対して、アクセス可能ユーザや端末ルールを一元的に管理・設定することで、セキュリティと柔軟性を両立したネットワーク環境を提供します。これにより無尽蔵にセキュリティ対策を講じることなく、最適な運用管理やコスト設計が可能となります。

### ２．製品概要と特長

本製品は、米国国防総省との協定により軍事に利用するIP接続デバイスのクローキング技術に提供するために開発されたファーストパケット認証（特許技術：下記図1）を実装した製品です。

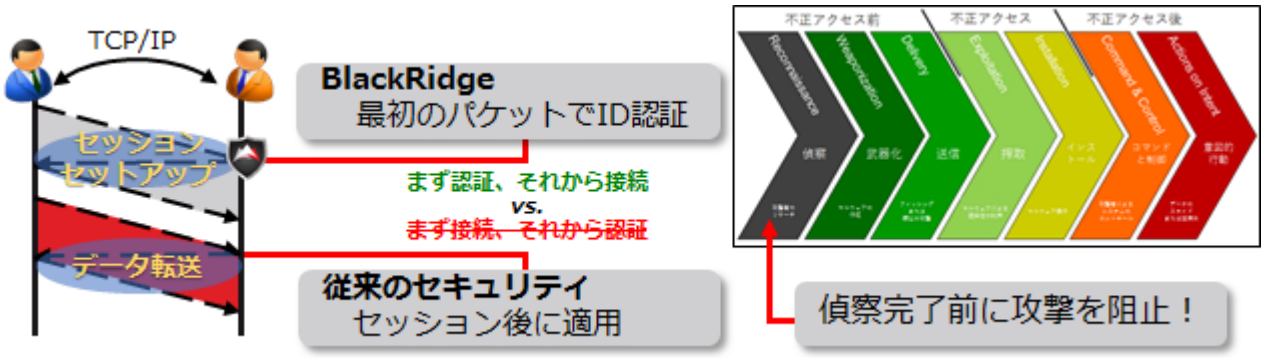


図１　特許技術ファーストパケット認証とは

TCP 通信の３ウェイハンドシェイク初パケット（SYN）に対して ID 認証を提供することで、本来アクセス権が無い攻撃者や第三者のアクセスから情報資産を守れます。TCP/IP の従来技術を応用しているので既存ネットワーク環境に特別な対応は一切必要ありません。本製品を情報資産の前とアクセスする側に設置するだけで実現可能です。低負荷で実装できるので、既存ネットワーク構成の根本から改革する必要があったマイクロセグメンテーションに比べ導入ハードルが格段に低くなります。

本製品は、TCP ヘッダのシーケンス番号フィールドにハッシュ関数で生成した独自 ID を埋め込み、通信を実施します。未導入のユーザに対しては通常の TCP ヘッダのように見えるため、特に影響なく既存通信を継続することができることが大きな特徴の一つです。

## ３．提供製品一覧（一部抜粋）

| オーケストレーション製品 | ゲートウェイ製品 | | クライアント製品 | |
|---|---|---|---|---|
| 管理サーバ | 物理製品 | 仮想製品 | 仮想製品 | 仮想クライアント |
| BR-BEM-VM3221-T | 販売予定なし<br>（2019/4 現在） | BR-2010<br>BR-2020<br>BR-3231-T<br>BR-3221-SR | TAC Endpoint | ID-Base<br>ID-500～ID-50k<br>ID-plus |

表1　提供製品一覧

## ４．ソリューション概要

オフィス情報資産（業務アプリケーション等）環境をマイクロセグメンテーション化した例を図 2 で示します。昨今 FW、IDS/IPS、WAF 等で多層防御してあるネットワークでもマルウェア添付メールは侵入し、端末感染から被害を拡大しています（左図）。

本製品毎に設定したアクセスポリシーにて情報資産のアクセス可否を設定でき、未導入であればアクセスすらできなくなります。これにより部署毎、端末毎、ユーザ毎にセグメントを分離し、万が一感染端末が発生した際も他情報資産に影響を与えない環境を実現します。

また、インターネットなどの外部へのアクセスは本製品を導入していても可能です。既存のユーザビリティを確保できることも特徴の一つです。

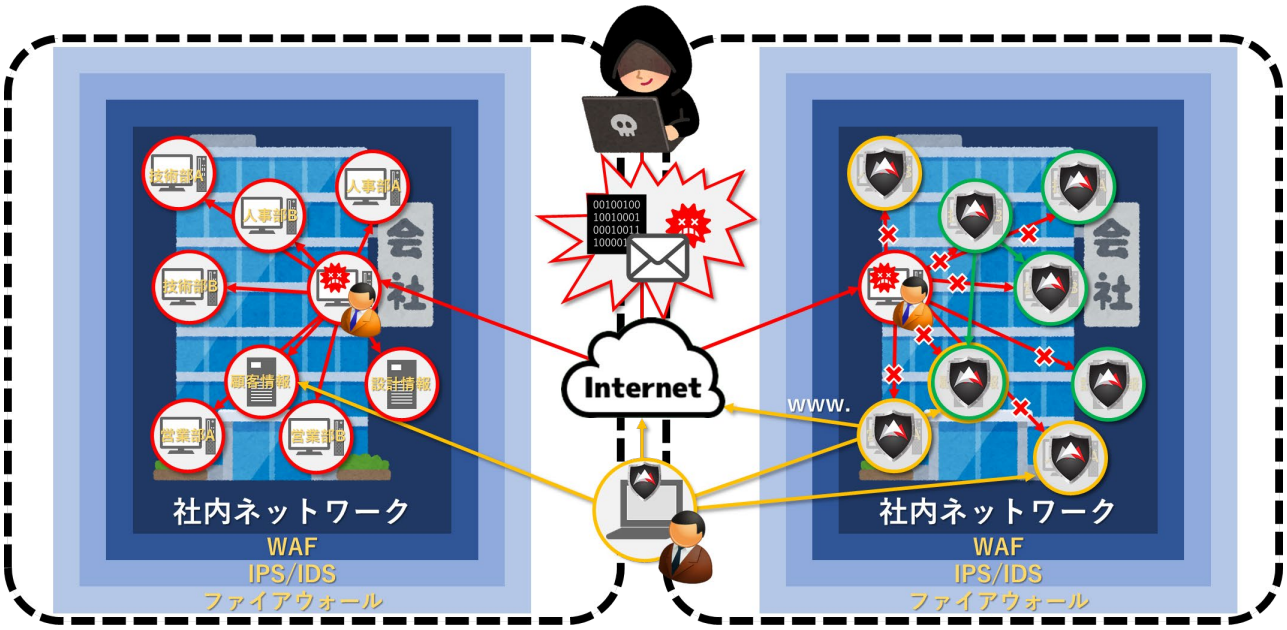


図 2　重要アセットのマイクロセグメンテーションイメージ（左図：導入前、右図：導入後）

## ５．販売開始

2019 年 4 月から

## ６．販売価格

お客様のネットワーク環境や導入端末数などに合わせて最適な製品／サービスをご提案します。提案価格はその都度お見積りさせていただきます。

## ７．今後の展開

本製品は、既に米国国防総省や世界的な IT 企業、クラウド事業者、医療等の分野に利用されています。NTT-AT では、国内において同様のニーズが潜在している現状を踏まえ、一般のエンタープライズに加え、工場、公共、交通、金融、医療、学校、IoT 分野など、サイバー攻撃を遮断しなければならない多くのシーンに、本製品を販売していく予定です。

## ■BlackRidge Technology, Inc について

BlackRidge Technology, Inc は、2010 年に米国国防総省の出資を受けて設立された会社で、主なパートナーは Ciena、Cisco、IBM です。活動内容は次世代サイバーセキュリティソリューション製品の開発、販売、サポートを行っており、ネットワークやサーバ資産やクラウドシステム等をサイバー攻撃から安全に保護することが出来ます。行政機関や企業内 LAN や IoT、クラウドサービスなどに活用されています。

＊1： マルウェア(Malware)
⇒ 「malicious software（悪意があるソフトウェア）」の略語。不具合を起こす意図で作られているソフトやプログラムの総称。
ウイルス・ワーム・トロイの木馬・ランサムウェア等があります。

＊2： ゼロ・トラストネットワーク(Zero Trust Network)
⇒ もともと Forrester Research が 2010 年に提唱した考え方。
「信頼しないことを前提とし、全てのトラフィックを検査、ログ取得を行う」という性悪説のアプローチモデル。

＊3： 3 ウェイハンドシェイク(three-way handshaking)
⇒ IP ネットワーク上で TCP による接続(コネクション)を確立するための手順。パケットの送受信を 3 回行うことからこのように呼ばれる。



**本件に関するお問い合わせ**

NTTアドバンステクノロジ株式会社
セキュリティ事業本部 IP プロダクツビジネスユニット
BlackRidge 製品担当
ＴＥＬ：044-589-6928
https://www.ntt-at.co.jp/product/blackridge/