NTTグループの最新ソリューションガイド

NTTアドバンステクノロジ　マイクロセグメンテーション・ソリューション

既存のNWの中で、IoT機器・重要資産を安全に隔離するのは簡単ではない！

- スマートファクトリ：事務棟（PC、サーバ）と工場棟（PLC、ロボット、工作機械）を、つなぎたくても、つなげられない。
- 社会インフラ：長年使っている医療機器・制御機器はセキュリティ対策が十分ではないが、安全に使い続けたい。
- 発電所：原子炉等の監視映像を既設 LAN 回線に相乗りさせたいが、部外者には絶対見せたくない。
- 自動車・重工業：新車、航空機（機密情報）の設計・製造を工場外からアクセスして業務を効率化したい。
- 学校：校務系と学習系そしてインターネット接続を伴う校務外部系の３つの NW の分離を簡単で使い易く実現したい。
- IoT 機器：現在の NW が複雑であり、既存の物理 NW を変えずに、アクセス権限をキレイに整理整頓したい。

「BlackRidge TAC ソリューション」が、これらの課題を簡単に解決します！

★米国国防総省との協定により開発された特許技術“ファーストパケット認証”を採用。

★TCP SYN パケットに認証用の独自 ID を埋込むことで、通信開始前に認証するため、特定のユーザ～重要資産の安全かつクローズドな接続を簡単に実現。

★従来の多数のルータ・ファイアウォールでのアクセス権限管理に比べ、一元管理により作業が大幅に削減可能。

特許技術“ファーストパケット認証”採用のBlackRidge TACソリューションで重要資産を防御します。

NTTアドバンステクノロジ（以下：NTT-AT）が本年4月より販売を開始している米国BlackRidge Technology, Inc（以下、BlackRidge）が開発したTAC（Transport Access Control）ソリューションは、TCP/IPのファーストパケット（SYNパケット）に対しセキュリティポリシーを実施する特許技術“ファーストパケット認証”を用いたセキュリティ製品です。TCP/IPのSYNパケットそのものを認証し、不正アクセスをシャットアウト。これによりすべてのサイバー攻撃で悪用されるTCP/IPの脆弱性を遮断できます。BlackRidgeのTACソリューションは、信頼しないことを前提としたゼロ・トラストネットワーク時代のネットワークセキュリティに有効な「マイクロセグメンテーション」対応を容易かつ低コストで実現します。

ゼロ・トラストネットワーク時代に相応しいアクセス制御の「マイクロセグメンテーション化」が不可欠に

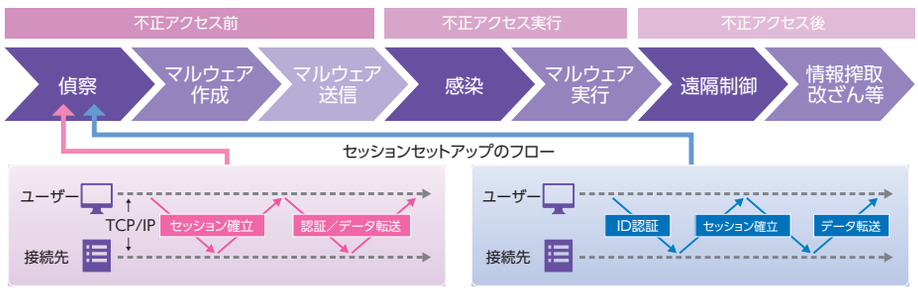
ますます高度化・巧妙化するサイバー攻撃に加え、端末の接続環境も多様化している現在、攻撃者を境界の内側に侵入させない境界防御型セキュリティではなく、信頼しないことを前提としたゼロ・トラスト対応のネットワークセキュリティが必要とされてきています。従来のファイアウォール、IPS/IDS（不正侵入検知・防御システム）などで守れている環境さえも、セキュリティ脅威にさらされています。実際に一度マルウェア攻撃などで内部ネットワークに侵入されると、横の端末、隣のセグメントへと瞬く間に侵食されていきます。そして、最終的には目的の重要資産にたどり着き、外部へ情報漏えいする事例も多く存在します。

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」が前述のような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ー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実現します。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簡単に実現できます。

TCP/IPの脆弱性を遮断する特許技術“ファーストパケット認証”を実装した革新的セキュリティ製品

NTT-ATが2019年4月より販売を開始した「BlackRidge TACソリューション」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（存在を隠蔽する技術）に提供するために開発された特許技術“ファーストパケット認証”を実装した革新的なソリューションです。

製品コンセプトは、TCPシーケンスフィールドの最初のパケット（SYNパケット）に認証用にハッシュ関数で生成した独自IDを埋め込んでおくことで、パケットを送信したユーザーやデバイスをネットワーク接続が確立する前に認証します。これにより、本来アクセス権のない攻撃者や第三者のアクセスから重要資産を守ることができます。従来のように、ネットワーク接続が確立した後で、ID認証を行うのでは遅すぎます。図1に示すように従来と比べ、「ID認証してから接続させる」ことにより、アクセス権限のない端末・デバイスからのアク



従来は「接続してから認証させる」>リスク高　BlackRidgeは「ID認証してから接続させる」>リスク低

図1　特許技術“ファーストパケット認証”の概要

セスをシャットアウトできます。これにより、TCP による各種セキュリティ攻撃から重要資産を守ることが可能になります。

「BlackRidge TAC ソリューション」は、隠蔽したい情報資産の手前に設置する BlackRidge ゲートウェイ（仮想アプライアンス）、アクセス元のクライアント用 BlackRidge エージェント、管理サーバにより構成されます。

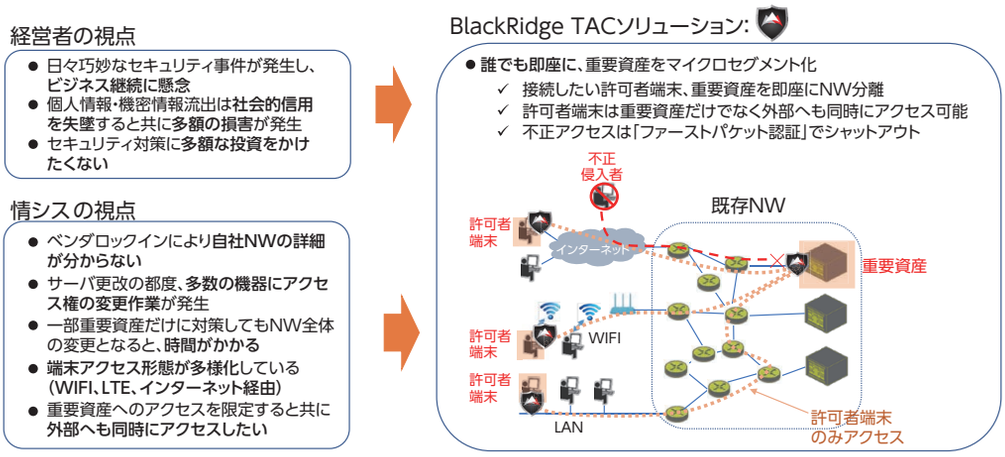


図２　BlackRidge TAC ソリューションによるマイクロセグメンテーション

「BlackRidge TAC ソリューション」の主な特長

BlackRidge TAC ソリューションは、主な特長として以下の３点があげられます。

①セキュリティ対策コストや運用リソースを大幅削減

「入口」を守ることで、これまで PC ウイルスソフトからファイアウォールに至るまでの膨大なセキュリティ対策コストや運用の手間を大幅に低減することが可能です。

②既存システムに手を加えず、多彩なプラットフォームに対応

シンプルな ID 認証方式のため、既存の機器類はそのまま利用可能です。PC から仮想環境・クラウドまでさまざまなプラットフォームに導入できます。

③米国国防総省に採用された信頼の実績

BlackRidge TAC ソリューションは、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。例えば、パブリック／ハイブリッドクラウドへのアプリケーション移行（クラウド環境のクローキング）事例では、BlackRidge クラウドゲートウェイが信頼できる ID によるアクセスをホワイトリスト化し、認定された ID のみがクラウドリソースと通信可能な環境を実現。これにより、高価で複雑な VPN、ネットワーク認証およびファイアウォールを必要とせずに信頼できない ID による不正アクセスのリスクを排除しています。

図２は、既存システムの NW を変更せずに、重要資産をマイクロセグメント化するイメージを示しています。守らなければならない重要資産は、社内の個人情報・機密情報に限らず、製造工場・病院の IoT 機器、社会インフラの野外設備など多種多様です。

今後 NTT-AT では、一般企業に加え、製造、公共、金融、医療、IoT 分野など、多くのシーンに本製品を販売し、セキュリティ問題の解決に貢献していく予定です。

NTT アドバンステクノロジ

BlackRidge 製品担当スタッフ

「セキュリティ専門技術」と「製品毎の技術サポート」で、
高い競争力のトータルサービスを提供いたします。
お客様の課題解決のお手伝いをさせていただきますので、
是非、お気軽にご相談ください。

お問い合わせ先
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
E-mail：blackridge@ml.ntt-at.co.jp　URL：https://www.ntt-at.co.jp/product/blackridge/