

中小企業向けゼロトラスト型セキュリティプラットフォームの提供を開始 ～サイバーセキュリティ・メッシュに必要な機能をオールインワンで提供～

NTT コミュニケーションズ株式会社（以下 NTT Com）は、ゼロトラスト型セキュリティプラットフォーム「WAN だふる[®] VxGPlatform（ワンダフル ブイエックスジープラットフォーム）」（以下 本ソリューション）を、2022 年 3 月 1 日より提供開始します。本ソリューションは、中小企業にも導入しやすいセキュリティプラットフォームで、サイバーセキュリティ・メッシュ^{*1}の概念にもとづきゼロトラスト^{*2}を中心とした機能を導入から保守まで一元的に提供します。セキュリティのプロフェッショナルが不在の場合でも導入から運用までを NTT Com にお任せいただけます。

1. 背景

セキュリティの脅威が世界中で拡大する中、大企業だけでなくサプライチェーンを構成する中小企業を狙った攻撃が増加しており、取引先企業への標的型攻撃の足掛かりとされる懸念が指摘されています。

また、IoT やコネクティッドカーなどインターネットへの接続を前提とした新たなサービスの普及によりさまざまな業界においてセキュリティ指針の策定と実装が急務になっており、企業規模を問わずゼロトラスト型のセキュリティ対策ニーズが増大しています。

一方で、サプライチェーンを構成する中小企業では予算や人材不足により十分なセキュリティ対策が講じにくいという課題があります。このような課題に対応するため、価格や運用面などにおいて中小企業でも導入しやすいセキュリティプラットフォームを提供します。

2. 概要と特長

本ソリューションはセキュリティ機器の導入から保守運用までを一元的にご提供するセキュリティプラットフォームです。基本メニューは標準モデルと BDAP[™]^{*3}モデルの 2 種類から選択でき、さらにオプションで必要な機能を組み合わせてご利用いただけます。主な特長は以下の通りです。

（1）必要なセキュリティ機能を導入から保守まで一元的に利用可能

サイバーセキュリティ・メッシュに必要なファイアウォール・UTM^{*4}・Web プロキシ^{*5}を中心としたセキュリティ機能と、リモートアクセス機能が標準でご利用いただけます。中小企業などにおいて、セキュリティのプロフェッショナルが不在の場合でも本ソリューションをご契約いただければ必要なセキュリティ機能がご利用でき、運用もお任せいただけます。

（2）脅威への多層防御（BDAP[™]モデルのみ対応）

標準モデルの UTM 機能に加え、NTT グループ独自のリアルタイムで更新される高精度なブロックリストによる多層防御を提供し、お客さまが C&C サーバー^{*6}やフィッシング

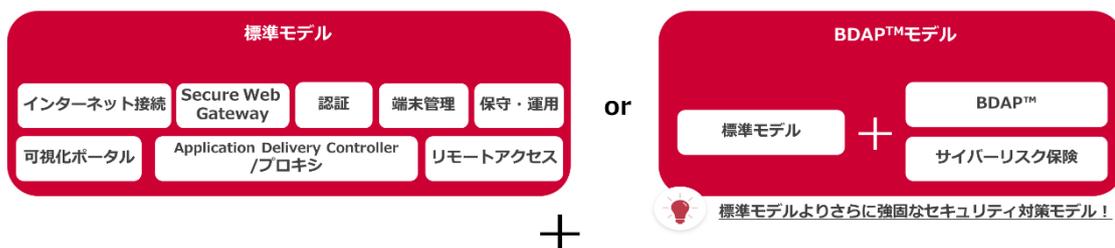
サイトへ接続するリスクを低減します。

(3) サイバーリスク保険の付帯（BDAP™モデルのみ対応）

サイバーリスク保険^{※7}が付帯されており、万が一不正アクセスなどによる情報漏えいが発生した場合の原因調査費用や損害賠償費用、弁護士やコンサルティング会社への相談費用などを補償します。

VxGPlatform 構成

基本メニュー



オプションメニュー（任意で選択）



3. 提供開始日

2022年3月1日

4. 提供価格

「本件に関するお問い合わせ先」もしくは営業担当までお問い合わせください。

5. 今後について

2022年度中を目標にEDR（Endpoint Detection and Response）の機能追加および5Gなどモバイル通信のセキュリティ強化を行います。また、新ドコモグループとして中小企業を含む全国の法人のお客さまへの展開をめざします。

NTTドコモ、NTT Com、NTTコムウェアは、新ドコモグループとして法人事業を統合し、新たなブランド「ドコモビジネス」を展開しています。「モバイル・クラウドファースト」で社会・産業にイノベーションを起こし、すべての法人のお客さま・パートナーと「あなたと世界を変えていく。」に挑戦します。



<https://www.nttdocomo.co.jp/biz/special/docomobusiness/>

NTT Com は、事業ビジョン「Re-connect X[®]」にもとづき、お客さまやパートナーとの共創によって、With/After コロナにおける新たな価値を定義し、社会・産業を移動・固定融合サービスやソリューションで「つなぎなおし」、サステナブルな未来の実現に貢献していきます。

Re-connect X

<https://www.ntt.com/about-us/re-connectx.html>

- ※1:サイバーセキュリティ・メッシュは、情報機器（PC やサーバーなど）がさまざまな場所に分散化された現代において、すべての情報機器に対しメッシュ状にセキュリティを張り巡らせることで、脅威に対してより強固な対策を行うという考え方です。
- ※2:ゼロトラストは、「信頼（Trust）を何に対しても与えない（Zero）」という前提に立ったセキュリティ対策の考え方で、社内外問わずすべてのアクセスに対して認証と許可を厳密におこないます。
- ※3:BDAP[™]（Blocklist Distribution Automatic and Protection）は、NTT Com の商標（出願中）で世界中のセキュリティ情報から脅威情報を収集し、本ソリューションが提供する UTM 装置へリアルタイムにブロックリスト登録することで最新の脅威からブロックするシステムです。BDAP[™] モデルでは標準モデルの機能に加え BDAP[™] との連携により自動防御でセキュリティリスクをさらに低減します。
- ※4: UTM（Unified Threat Management）は、複数のセキュリティ機能を一元化させた統合脅威管理機能です。
- ※5: WEB プロキシは、Web サイトへのアクセスを代理で行うサーバーです。悪意あるサイトにアクセスしてしまった際もアクセス元の情報流出を避けることができます。
- ※6: C&C サーバー（Command and Control Server）は、外部から侵入して乗っ取ったコンピューターを利用したサイバー攻撃で、踏み台のコンピューターの制御や指令を担うサーバーをさします。
- ※7: サイバーリスク保険は、東京海上日動火災保険株式会社と NTT Com の提携（協業施策）にもとづき、東京海上日動火災保険株式会社より提供します。