

先端技術キーワード解説

知っておきたい最新の動き

[ゼロトラストネットワーク]

2020年以降、新型コロナウイルス（Covid-19）感染拡大防止のため、リモートワークが拡大しました。そこで、急速に関心を集めたのがセキュリティです。それに対して、今、提唱されているのが「ゼロトラストネットワーク」です。どのようなものなのでしょうか。

1. ゼロトラストネットワークとは

(1) 限界となった「ペリメタモデル（従来型の境界防御モデル）」

「ペリメタモデル」とは、社内ネットワークのセキュリティを境界防御で保つものです。これは、サイバー攻撃等の脅威は境界外部にのみ存在するため、その脅威を境界内部に侵入させないというモデルです。

しかしながら、セキュリティの脅威は、日々、高度化、多様性が進み、境界防御だけで、脅威を全て防ぐことは難しくなってきました。

(2) ゼロトラストネットワークとは

「ゼロトラストネットワーク」とはコンピュータやネットワークの構成に依存しない新しいセキュリティ技術を指す言葉です。

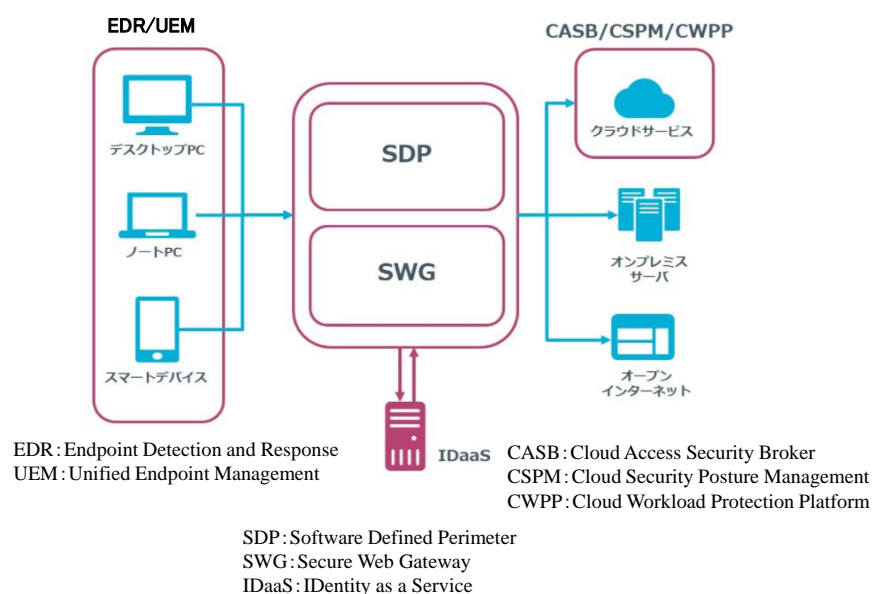
ゼロトラストネットワークでは、まず「全てを信頼しない」ことからスタートします。例えば、外部からのアクセスに対して、毎回セキュリティレベルをチェックして安全が確認できたデバイスのみアクセスを許可します。ゼロトラストネットワークの実装では、データの種類や用途に応じて、ネットワークを分割し、各ネットワークの境界においてセキュリティ対策を施します。

2. ゼロトラストの構成

一般的な構成は、右図です。

エンドポイント(デバイス等)では、EDR（マルウェアなどへの防御）や UEM（リモート管理、アプリケーション管理など）でセキュリティを担保します。

クラウド接続に関しては、CASB（非許可のアプリ等のアクセス制限など）、CSPM（管理者権限の付与の監視）、CWPP（コンテナや仮想マシンの情報漏洩を防止など）で、クラウドセキュリティを確保します。



ネットワークにおいては、SWG（オープンインターネット接続の保護など）、SDP（社外のデバイスから社内のリソースに対して安全な接続を提供など）でネットワークセキュリティを確保します。

それらのアクセスに関して、IDaaS において認証・認可されたユーザーのみがリソースへ接続するという仕組みになります。

そして、これらの情報は有機的に連携し、全体としてのセキュリティを保つことを可能とします。

[参考文献]

1) NRI Secure : テレワーク時代のセキュリティ | ペリメタモデルからゼロトラストモデルへ

<https://www.nri-secure.co.jp/blog/perimeter-to-zerotrust>

(注)

本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意ください。

無断転載、転用は固くお断りいたします。

Copyright (C) Satoru Haga 2022, All right reserved.

<p>技術・経営の戦略研究・トータルサポーター</p> <p>ティー・エム研究所</p>	<p>工学博士 中小企業診断士 社会保険労務士(登録予定) 代表 芳賀 知</p>
<p>E-Mail : info_tm-lab@mbn.nifty.com URL : http://tm-lab@a.la9.jp/</p>	