働き方改革時代の「ゼロトラスト」セキュリティ(5):

「ゼロトラストとは」で検索してもよく分からない？――米国政府による定義「SP 800-207」を読み解く

https://www.atmarkit.co.jp/ait/articles/2008/18/news014.html

デジタルトラストを実現するための新たな情報セキュリティの在り方についてお届けする連載。今回は、米国政府が考えるゼロトラストの定義と実践の姿について。

2020年08月18日 05時00分 更新

[仲上竜太, 株式会社ラック]

ベンダーによって言うことが違う「ゼロトラスト」

コロナ禍の影響で常態化しつつあるテレワーク／リモートワークの課題を解決するコンセプトとして、「ゼロトラストセキュリティ」「ゼロトラストアーキテクチャ」が注目されつつあります。しかし、その定義や内容は理解が容易ではなく、またベンダーによるゼロトラストの説明も微妙に異なるため、「一体何がゼロトラストなのか」とお考えの方も多いのではないかと思います。

デジタルトラストを実現するための新たな情報セキュリティの在り方についてお届けする連載『働き方改革時代の「ゼロトラスト」セキュリティ』。今回は、NIST(National Institute of Standards and Technology:米国立標準技術研究所)が発行したレポートである「SP 800-207 Zero Trust Architecture(2nd Draft)」に書かれた内容を基に、今後ゼロトラストを論じる上で軸となり得る、米国政府が考えるゼロトラストの定義と実践の姿について考えます。

影響力の大きな米国政府の定めるセキュリティ基準＝NIST SP 800シリーズ

サイバーセキュリティの取り組みやアプローチには、さまざまな方法や考え方が存在します。組織に合わせて方針を検討する際に、世界中で共通する指針としてさまざまな場面で参照されるレポートが、NISTの発行する「SP 800」シリーズです。

NISTは1900年代初頭に設立された米国の国立機関で、米国内の技術や産業の競争力を高めるため、標準となる技術規格の制定を行っています。産業の基盤となる計量に関する基準を定める機関として、「NIST-F1」と呼ばれる世界で最も正確な原子時計の運営や、AES(Advanced Encryption Standard)やSHA(Secure Hash Algorithm)といった世界中で一般的に使用されている暗号技術の標準化などでよく知られています。

サイバーセキュリティの構築や運用に関する指針が目的ごとにまとめられているSP 800シリーズは、NISTの中でも情報技術に関する研究を行うITL(Information Technology Laboratory)に所属するCSD(Computer Security Division)が発行しています。

このSP 800シリーズは、日本政府をはじめさまざまな機関で参照されています。防衛装備庁では令和元年度から、調達要件として「SP 800-171(連邦政府外のシステムと組織における管理された非格付け情報の保護)」と同程度の情報セキュリティ基準を採用しています。また、政府の推進する「サイバー・フィジカル・セキュリティ対策フレームワーク(CPFS)」でもNISTが発行している文書である「Cybersecurity Framework」やSP 800と対応した形で検討されています。

ゼロトラストの「具体的な」定義 - SP 800-207 Zero Trust Architectureを読み解く

世界のサイバーセキュリティ施策に大きな影響を与えているNIST SP 800シリーズですが、2019年に「SP 800-207 Zero Trust Architecture」としてゼロトラストに関するレポートが発表されました。

NISTによるゼロトラストの定義や実装方法についてまとめられたこのレポートは、今後米国政府での情報システムの調達基準などで参照される可能性が高く、これからゼロトラストに取り組む組織のセキュリティ担当者やネットワーク担当者にとって大変参考になる内容となっています。

現在は2020年2月に発行された2nd Draftが最新となっています。

- SP 800-207 (Draft), Zero Trust Architecture | CSRC

ドキュメントは7つのセクションで構成されており、第1セクションから第3セクションにかけてゼロトラストが生まれたいきさつやゼロトラストの基本、構成する各コンポーネントの説明がなされておりゼロトラストのコンセプトを学ぶことができます。第4セクション以降は、ゼロトラストの実装シナリオやユースケース、ゼロトラストにおける脅威、既存の連邦政府規約との関係、そしてゼロトラストへの移行方法といった、ゼロトラストの考え方を取り入れる上での方法論に続きます。

ゼロトラスト（ZT）とゼロトラストアーキテクチャ（ZTA）

これまでの連載でも解説したように、組織のネットワークを境界で防御することが難しい時代になってきました。クラウドの活用によるデータの分散や、リモートオフィスやモバイルなど組織におけるネットワークは複雑かつ広範に広がっています。境界による防御では、一度境界を突破したサイバー攻撃者のネットワーク内部での展開を防ぐことができません。

ゼロトラストは、このような現実的な課題を踏まえたサイバーセキュリティの原則でありネットワークセキュリティの新しいモデルです。企業が所有しているネットワークは、所有していないネットワークと変わらない、もしくはそれ以上に信頼できないと仮定します。ネットワークが信頼できないため、データへのアクセスを必要とするユーザーや資産のみに限定し、常に身元とセキュリティ状態を認証し承認する必要があります。

NIST SP 800-207では、これらの操作を正確に行う際の不確実性を最小化するよう設計されたコンセプトとアイデアの集まりが「ゼロトラスト（ZT）」として定義されています。

不確実性を軽減するための方法として、データやアプリケーションなどのリソースの粒度を可能な限り細かくすることによる、認証や認可、暗黙の信頼ゾーンの縮小に焦点を当てています。

下図のように、信頼されていないゾーン（例えばインターネット）にいる利用者が、あるポリシーに従ってデータにアクセスする場合を考えます。リソースにアクセスを希望する利用者は、ポリシー定義点、ポリシー施行点で認証され、暗黙的な信頼ゾーンを通してリソースへのアクセスが許可されます。

ゼロトラストアクセス（筆者がSP 800-207掲載の図を翻訳）

SP 800-207では、このモデルを空港のセキュリティと乗客の関係に例えて説明しています。全ての乗客はセキュリティチェック（PDP/PEP）を通過し、ターミナルエリアを通して搭乗ゲートへアクセスします。ターミナルエリア内では自由に動き回ることができます。

従来の境界型モデルで構築されたネットワークでは、利用者はVPNを通して組織内ネットワークに接続し、データへアクセスします。この場合、VPNさえ通ってしまえば、正規の利用者として他のデータにもアクセスできてしまいます。

空港の例では、乗客がターミナルエリアを通して目的外の飛行機の搭乗ゲートにもアクセスできるのと同様です。これではサイバー攻撃者による内部侵入後の横展開による被害拡大を防ぐことができません。

ゼロトラストでは、このPDP/PEPとリソースの間を可能な限り近づけ、暗黙的な信頼ゾーンを最小化するための原則とコンセプトを提供しています。

さらにSP800-207では、このようなゼロトラスト（ZT）の原則に基づいたネットワーク設計のアプローチと、企業におけるサイバーセキュリティ戦略そのものを「ゼロトラストアーキテクチャ（ZTA）」として定義しています。

次回も引き続きSP800-207から、ゼロトラストの考え方と実践を読み解く

今回はNISTの発行するSP800-207からゼロトラスト、そしてゼロトラストアーキテクチャの定義を紹介しました。次回も引き続きSP800-207から、ゼロトラストの考え方と実践を読み解きます。

筆者紹介

仲上竜太

株式会社ラック

セキュリティプロフェッショナルサービス統括部 デジタルペンテストサービス部長

兼 サイバー・グリッド・ジャパン シニアリサーチャー

進化するデジタルテクノロジーをこよなく愛し、サイバーセキュリティの観点で新たな技術の使い道の研究を行うデジタルトラスナビゲーター。家ではビール片手に夜な夜なVRの世界に没入する日々。