ゼロトラスト

中山裕貴（(株)ボスコ・テクノロジーズ）
nakayama@bosco-tech.com

1. ゼロトラストとは

近年，一般的な企業におけるネットワーク環境はクラウドサービスの利用や，各種モバイル端末の普及，BYOD（Bring Your Own Device）の浸透，複数の内部ネットワークの構成，多数のリモートオフィスの運用など，多種多様な要素により構成されている．そのため，そのネットワーク構造は複雑化の一途をたどっており，従来の静的なネットワークベースの境界防御によるセキュリティ対策のみでは十分な対策を取ることが困難となっている．更に，図1に示すように，境界防御は一度攻撃者が境界を突破すると，水平移動の制限が困難であること，内部不正に対して有効な対策が取れないこと，攻撃の高度化に対応できないことなど，様々な課題を有している．これらの問題点を解決するために，近年ではゼロトラストという考え方に基づいた，ネットワークセキュリティの実現手法に関する研究や提案が多数行われている．

ゼロトラストとはネットワークやデバイスからのアクセスを暗黙的に信用せずに，常にアクセスの信頼性を検証することで，サービスや資産，リソースを保護することに焦点を当てたセキュリティの考え方である．ゼロトラストにおいて特に重要であるのは「暗黙的な信頼を前提とせず，資産や機能に対するリスクを継続的に分析・評価する」点である．これを実現するためには，従来の境界防御のようにファイヤウォールを一つ置けば完了するのではなく，様々な構成要素を組み合わせることが重要である．つまり，ゼロトラストの考え方に基づいたネットワークセキュリティを実現するためのたった一つの特効薬は存在しない．一方で，その構成要素は全てが真新しいものではなく，既存の技術の組合せで十分実現可能なものも多く存在する．

2. ゼロトラストの基本

ゼロトラストはリソースアクセスに際して，信頼は決して暗黙のうちに与えられるものではなく，継続的に評価されなければならないという前提に基づいている．図2にゼロトラストによるリソースへのアクセスの概念を示す．リソースへのアクセスは，ポリシー決定ポイントとポリシー実施ポイントを介して実施される．この図では境界防御におけるファイヤウォールがポリシー決定ポイントとポリシー実施ポイントに置き換わっただけのように見えるが，大きな違いとして，ネットワークという大きなゾーンで信頼している境界防御と異なり，可能な限り小さいゾーンで信頼するという点がある．

ポリシー決定ポイントはゼロトラストにおいて中核となる役割を担っており，信頼するか否かの判定をトラストアルゴリズムに基づいて行っている．トラストアルゴリズムがその判定を行うにあたり，ゼロトラストには七つの基本原則がある[(1)]．理想としては全ての原則が完全な形で実装されることが望ましいが，必ずしもその全てが純粋な形で実装されるとは限らないことに注意してほしい．

①全てのデータソースとコンピューティングサービスをリソースとみなす．

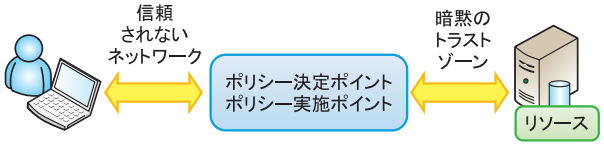

図2　ゼロトラストアクセスの概念

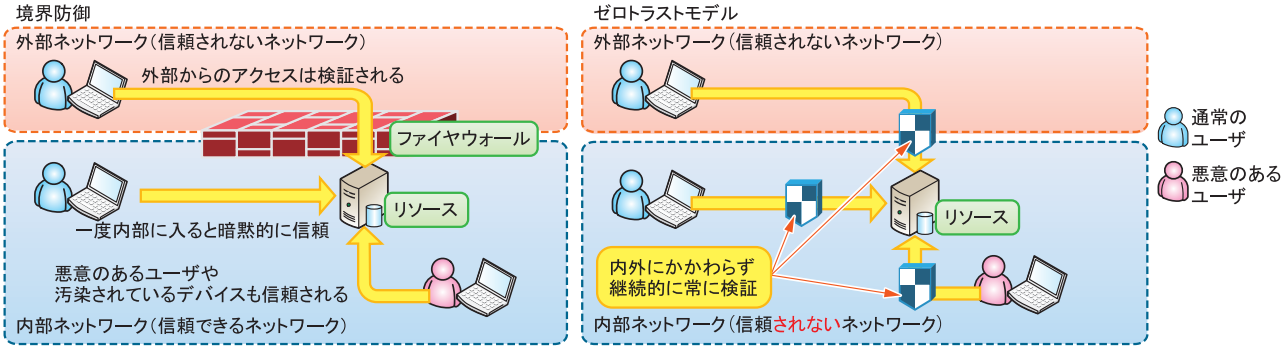

図1　境界防御とゼロトラストモデルの対比

本会ハンドブック「知識の森」
https://www.ieice-hbkb.org/portal/doc_index.html

②ネットワークの場所に関係なく，全ての通信を保護する．
③企業リソースへのアクセスはセッション単位で付与する．
④リソースへのアクセスは，クライアントアイデンティティ，アプリケーション／サービス，リクエストする資産の状態，その他の行動属性や環境属性を含めた動的ポリシーにより決定する．
⑤全ての資産の整合性とセキュリティ動作を監視し，測定する．
⑥全てのリソースの認証と認可を動的に行い，アクセスが許可される前に厳格に実施する．
⑦資産，ネットワークインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ態勢の改善に利用する．

上記基本原則に基づき，トラストアルゴリズムでは図3に示すとおり，様々な情報をトラストアルゴリズムの入力として扱う．特に基本原則における④，⑤，⑦が入力に該当する．

3. ゼロトラストの構成要素

先述のとおり，ゼロトラストなネットワークは複数の論理コンポーネントにより構成されているが，基本的には図4に示すとおり，ポリシー決定ポイント，ポリシー実施ポイント，外部ソース群の三つから構成される．また，ポリシー決定ポイントはポリシーエンジンとポリシーアドミニストレータにより構成される．これらのコンポーネントは，オンプレミスまたはクラウドベースのサービスを介して運用される．それぞれの論理コンポーネントは下記のとおりの役割を持つ．

- ポリシーエンジン：指定されたリソースへのアクセスを許可するための最終的な決定を行う．ポリシーエンジンは，トラストアルゴリズムを使用して，リソースへのアクセスを許可したり，拒否したり，取り消したりの判定を行い，ポリシーアドミニストレータはその決定を実行する．
- ポリシーアドミニストレータ：クライアントとリソース間の通信経路の確立や遮断を行う．具体的にはクライアントとリソースにアクセスするために使用するセッション固有の認証トークンやクレデンシャルを生成する．
- ポリシー実施ポイント：クライアントとリソース間の接続を有効にし，監視し，最終的に接続を終了する役割を担う．ポリシー実施ポイントはポリシーアドミニストレータと通信し，リクエストを転送する．
- 外部ソース群：トラストアルゴリズムの入力となる様々なデータやポリシールールを提供する．具体的にはCDM（Continuous Diagnostics and Mitigation）システムやSIEM（Security Information and Event Management）システム，ID管理システムなどが挙げられる．

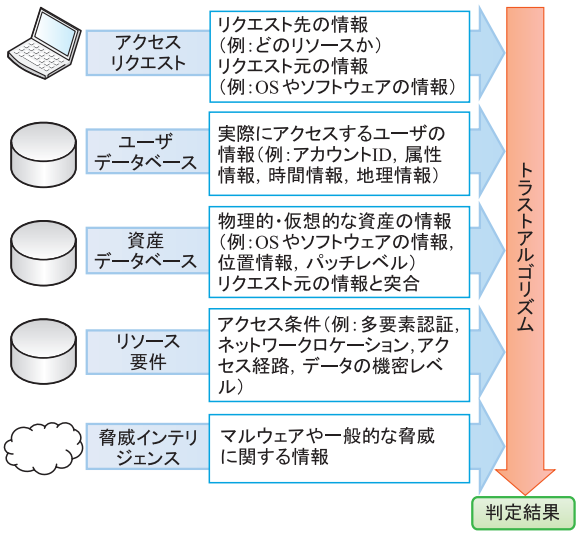

図3　トラストアルゴリズム

4. ゼロトラストの実現

ここまでゼロトラストの考え方やその構成要素を記したが，単一の仕組みを取り入れることで完全なゼロトラストが実現できるわけではない．一方で，多数のコンポーネントから構成されているからこそ，既にゼロトラストのコンポーネントとなる要素を持ち合わせている組織や企業も珍しくないであろう．更に，SIEMやアクティビティログ，ID管理システム，コンプライアンス管理システム，ポリシー実施ポイントなど，ゼロトラストの構成要素の中にはOSS（Open Source Software）を組み合わせることで簡単に実現可能なものも多い．そのため，ゼロトラストだからと難しく考えることなく，まずはネットワークの状況を見える化したり，各種アクセス権限の見直しから始めたりすることで，ゼロトラスト導入への第一歩を踏み出すことができる．

文　献

（1） V. A. Stafford, “Zero trust architecture,” NIST special publication, 2020, 800 : 207.

（2024年4月15日受付）

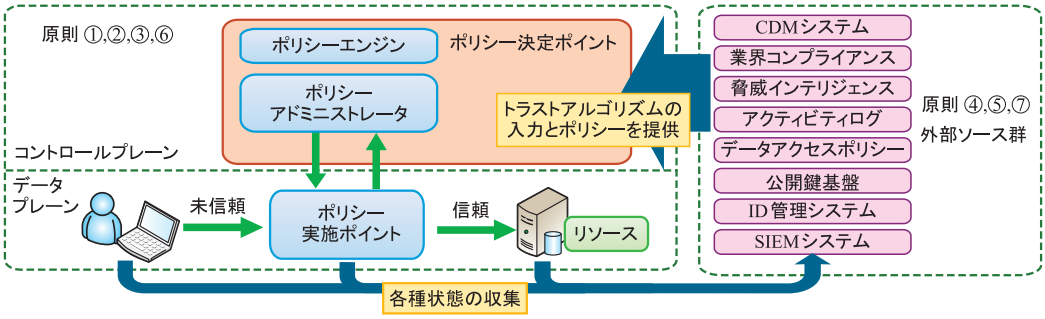

図4　ゼロトラストにおける論理コンポーネント