トピックス

クラウド時代のセキュリティ対策
―次世代セキュリティ「ゼロトラスト」の実装ポイント―

パブリッククラウドの活用が進み、企業の情報資産が社内だけでなくインターネット上にも存在するようになったことで、セキュリティ管理の範囲が広がっている。本稿では、境界防御を容易に突破できるサイバー攻撃や、内部の人間による重要情報の持ち出しのリスクへ対応する、セキュリティ強化のポイントを紹介する。

NRIセキュアテクノロジーズ コンサルティング事業本部
デジタルセキュリティコンサルティング部 上級セキュリティコンサルタント
鳥越（とりごえ） 真理子（まりこ）
専門はセキュリティ管理・ITガバナンスなどの支援およびコンサルティング

境界防御からの脱却

サイバー攻撃によって企業の情報セキュリティが侵害され、重要情報が窃取される事例が多数発生している。これに対して企業が以前から取り組んできたのが境界防御である。これは、社内ネットワークと外部との接点において重点的に対策を行うもので、その前提にあるのは、社内は安全だが外部（インターネットや他組織と接続しているネットワーク）は危険だという考え方である。データへのアクセス権限やアカウント管理も重要とされてはいるが、実際には、アクセス権限を持つストレージに保存されたデータに、どのユーザーがアクセスしたかを十分に管理できていない企業がほとんどである。

現在、境界防御はAPT攻撃（Advanced Persistent Threat。持続的標的型攻撃）によって簡単に破られている。その理由は、社内のシステムがぜい弱性を抱えていたこともあるが、上でも述べたように、データアクセスの認証・認可の仕組みを強化してこなかったことが大きい。また、アクセスログなどの検証が十分にできておらず、管理者にアラートを上げる仕組みが不十分なことも、被害拡大をもたらす要因となっている。

「ゼロトラスト」への転換

巧妙化する攻撃に対して情報セキュリティを確保するためには、接続元ネットワークがどこにあるかを問わない、新しいセキュリティモデルが求められる。「Trust but Verify（信ぜよ、しかし確かめよ）」から「Verify and Never Trust（確かめよ、決して信頼するな）」へ、すなわち「ゼロトラスト」という次世代セキュリティへの転換である。

この「ゼロトラスト」という概念は最近のものではなく、米国の調査会社Forrester Research社のJohn Kindervag氏が、2010年に初めて提唱したものである。

「ゼロトラスト」の要点は次の通りである。

①全てのユーザー、ネットワーク、デバイスを確認する。
②ネットワークの内部と外部を区別しない。
③どのネットワークからでも、セキュアなア

クセスを実現する。

④厳密な最小権限、Need to Knowコンセプト（知る必要がある最小限の人にのみ知らせるという考え方）に基づくアクセス管理を徹底する（ユーザーとエンドポイントデバイスの徹底管理）。

⑤全ての通信ログを監視する。

2016年の初めに、米国のGoogle社は自社の「ゼロトラスト」移行プロジェクトである「BeyondCorp」の詳細を開示した。その内容は、同社が2010年から「ゼロトラスト」への刷新を開始し、90％の社内システムをインターネットからアクセスできるようにしたというもので、セキュリティ業界を中心に「ゼロトラスト」がブームとなるきっかけをつくった。

「BeyondCorp」の目標は、「Google社の全従業員が、信頼できないネットワークを介して、VPN（仮想専用ネットワーク）を使用せずに働けるようにすること」であった。プロジェクトを開始した当時は、VPNの使用が前提で、サーバーデータへのアクセスの制御は不十分だったが、「BeyondCorp」ではアクセスするユーザーと利用するデバイスの2つを認証の主体とし、ユーザーがいる物理的な場所やネットワークに依存しない形になったという。

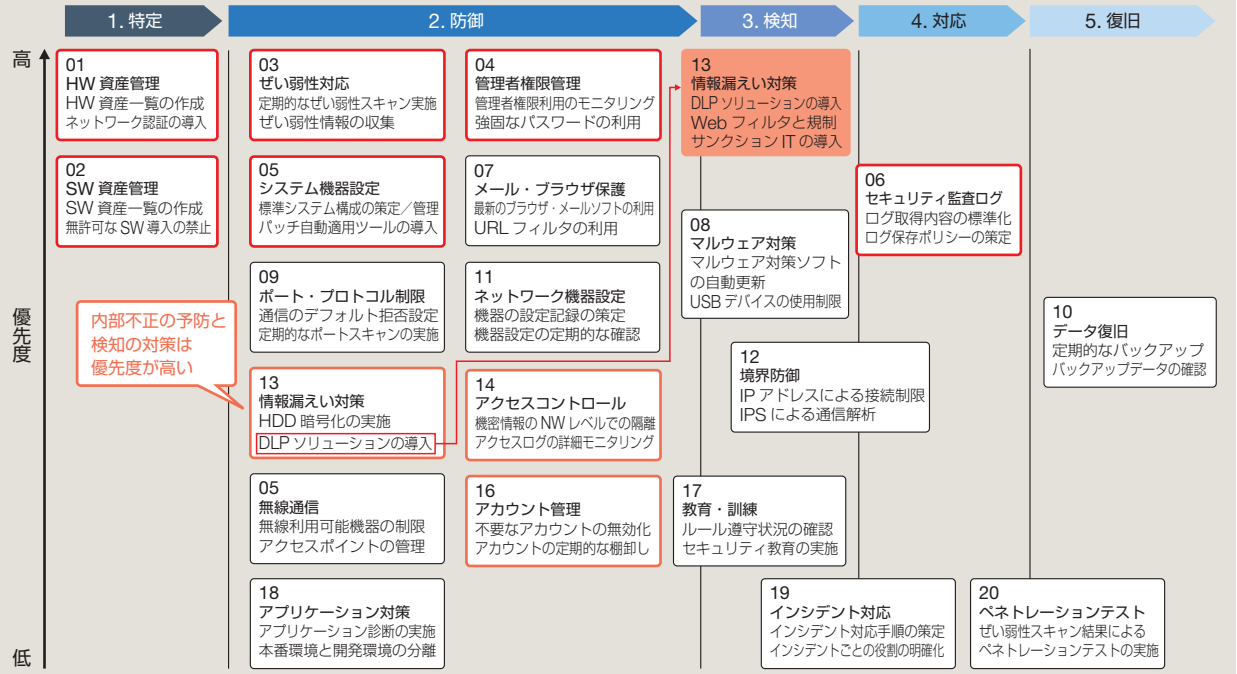
今、パブリッククラウドが目覚ましい発展を遂げるなかで、「ゼロトラスト」という次世代セキュリティを志向したアーキテクチャーを実装する企業が増えてきている。その方法としては、例えば、社内端末をGoogle Chromebookに、オフィスアプリケーションをG Suite（Google社がWebサービスとして提供している企業向けのソフトウェア群）に一本化するものがある。あるいは、Windows10への移行の機会に、これまで個別に導入していた資産管理、ぜい弱性管理、ウイルス対策やEDR（Endpoint Detection and Response。エンドポイントでの検出と対応）の機能を、Microsoft Defender ATP（ATPはAdvanced Threat Protectionの略）やWindows10のセキュリティサービスを活用して、Microsoft Azureポータルのセキュリティセンターで管理するやり方もある。

Webアプリのシステムが主流となり、アプリ連携が進むなか、サービスの一貫したセキュリティを確保したい場合は、強化されたデバイス管理と認証・認可の技術活用に比重を移さざるを得ない状況がある。「ゼロトラスト」を実現する中核的な技術は、従来よりも強固なアイデンティティ管理・アクセス管理である。これは、データへのアクセスがあった際に、ユーザーIDや役職といったユーザー属性だけでなく、利用されているデバイスの情報（最新のセキュリティパッチが適用されているか、ウイルスチェックは行われているかなど）もチェックし、アクセスの可否を判断する技術をいう。

アーキテクチャー設計の要点

「ゼロトラスト」は、境界防御に依存することなく、データアクセスを100％確認することが重要で、データへのアクセスが本人のものかを全て検証する形になっている。また、業務アプリケーションの通信をHTTPS（暗号化された通信手順）に統一し、詳細か

図1 「ゼロトラスト」のアーキテクチャー設計



出所：CIS Controls の資料を元に、NRI セキュアテクノロジーズ作成

つデバイスに依存しないアクセス分析が行えることが必須条件となる。その上で、「ゼロトラスト」のアーキテクチャーは、主に次の2つのセキュリティ上の課題を解決する必要がある。

①新サービスが次々と登場し、インターネット上で扱う情報やシステム開発の手順が増たことによる課題

②勤務場所を限定しない働き方が広がることによる課題

インターネット上で情報の保存、作成、共有に関する各種のサービスが利用できることは、内部の人間が不正に企業の情報資産を管理外の領域に持ち出すことを容易にする。その結果、不正の機会は増大することになり、実際に内部不正は後を断たない状況である。そのため、「ゼロトラスト」には、外部の脅威としてのサイバー攻撃、内部の脅威としての内部不正と過失について、リスク対応を厳格に行うことが求められる。

従来、セキュリティアーキテクチャーの設計や評価には、CIS（Center for Internet Security。米国のインターネットセキュリティの標準化組織）によって定義されたフレームワーク「CIS Controls」を参照することが多かった。「ゼロトラスト」ではこれらに準拠するだけでなく、内部不正への対応としてDLP（Data Loss Prevention。機密データの漏えいを阻止する）ソリューションを導入したり、アクセスコントロールやアカウント管理の優先度を上げてギャップ分析（理想と現実との差の分析）を行い、不足するセキュリティ対策を導入したりする必要がある（図1参照）。

なお、「CIS Controls」の基礎項目01～06は効果が大きい（標的型攻撃の85％以上を

阻止または軽減できるといわれる）ので、最優先で対策すべきである。また、内部不正の予防と検知に特化したDLPソリューションは、抑止効果を持つとともに、被害の把握にも役立つ。

「ゼロトラスト」の実装

「ゼロトラスト」の実装は、境界防御に偏ったセキュリティの在り方を見直して、デバイスのセキュリティ、認証・認可、SOAR（Security Orchestration and Automation Response。さまざまなツールを連携させてセキュリティ業務の運用を自動化すること）を特に意識して進める必要がある。

一方、「ゼロトラスト」の実装に当たって、従来の環境を残そうとすると余計に費用がかかることがあり、単純に適用するだけではリスクが残ることがある。また他の課題が見つかることも多い。

以下では、筆者のコンサルティングの経験に基づいて、「ゼロトラスト」実装におけるポイント、課題や対策を紹介したい。発展途上の技術も多いが、クラウド技術を適切に活用して、利便性とコストメリットを多くの企業が享受できることを願っている。

①情報資産の集中管理なくして実現は不可能

「ゼロトラスト」を実装するには、そもそも情報資産が集中管理されている必要がある。情報資産の定義と管理が徹底されていなければ、守るべき情報を特定することができない。まずは、サーバー側でデータアクセスのログを取得・分析する仕組みを構築することが課題として挙げられる。

②内部不正のログ監視は難易度が高い

全てのログを監視できたとしても、技術的な限界もあるため、内部の人間の不正アクセスを完璧に検知するのは難しい。従って、CASB（Cloud Access Security Broker。従業員のクラウド利用を管理するサービス）を利用するなどして、アクセスさせたくないクラウドサービスは組織のポリシーとして禁止しておくといった対策が重要になる。

③統合プラットフォームサービスの利用

SOARを実現するためには、エンドポイントセキュリティ、ネットワークセキュリティ、認証・認可の各サービスを統合するプラットフォームが別途必要になる。その際に、信頼できる脅威情報が利用されているかどうかが重要なポイントになる。また、資産管理情報、ぜい弱性情報、脅威検知のアラート情報などの管理情報を1つのサーバーやサービスに集約することは、技術的なポイントであるとともに、コスト削減にもつながる。

④アジリティやコストメリットを享受する

情報セキュリティ対策を「ゼロトラスト」に転換することで得られるメリットは、リスク低減だけではない。「ゼロトラスト」は、原則的にネットワークの形態には依存しないため、よりセキュアな回線を実現するのにかかっていた費用を見直すことも可能だ。また、ITリソースの導入時にセキュリティを取り込むことで情報セキュリティ対策単体のコストを削減でき、アーキテクチャーを最適化することで重複する機能を提供しているソリューションを停止できる。実装にかかる時間を短縮できるのも、「ゼロトラスト」の無視できない効果である。 ■