2020 年 09 月 25 日

サービス＆セキュリティ株式会社 e-Gate センター

ゼロトラスト環境におけるセキュリティ監視について

1. 概要

近年、政府の働き方改革の一環としてテレワークが推進されておりましたが、コロナ禍の影響によりテレワーク導入が急激に加速しました。そのため社外から社内ネットワークにアクセスする機会が増え、これまでの「境界型」に変わる「ゼロトラスト」と呼ばれるセキュリティモデルが注目されています。今回はこの「ゼロトラスト」環境におけるセキュリティ監視についてご紹介いたします。

2. ゼロトラスト（Zero Trust）とは

企業、団体のシステムでは社内のシステム（内部）とインターネット（外部）の接続点がセキュリティの重点ポイントであり、これまで「境界型」の多層防御によるセキュリティ対策が一般的でした。「境界型」では内部ネットワークは信頼し、外部からの侵入に対して重点的に対策をするため、ラテラルムーブメント（内部間の横展開攻撃）には脆いという弱点がありました。

しかし、テレワークのように社外から社内へのアクセスやクラウドシステムを利用される等システム構成が変化し、これまでの「境界型」の考え方ではセキュリティ対策の範囲や条件が変わってしまい不十分となります。「ゼロトラスト」では、すべてが信頼できない対象としてリソースへのアクセス毎に信頼評価を実施し、信頼できるものだけを許可します。ここではアクセス毎に信頼評価を行うことよりも、どのように信頼評価しているかが重要となります。また評価結果を信用スコアとして記録します。

次の 3 要素により厳密な信頼評価を行います。

1. 信頼されたユーザからのアクセスであるか
2. 信頼されたネットワークからのアクセスであるか
3. 信頼された端末からアクセスであるか

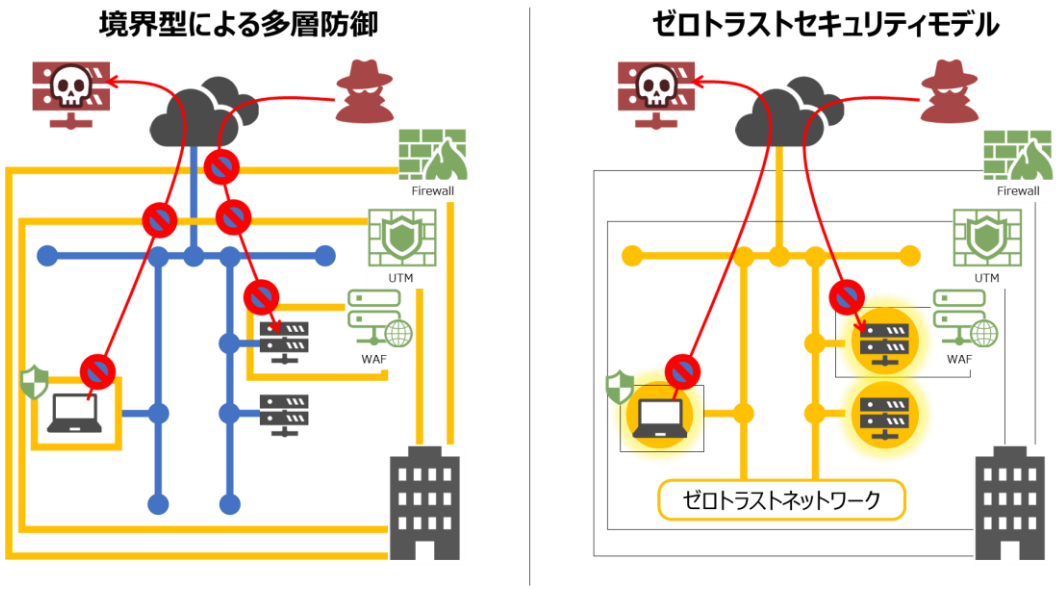

図 1 境界型とゼロトラストの違い

3. ゼロトラストの課題

ゼロトラストはアメリカの市場調査会社であるフォレスター・リサーチ社(Forrester Research, Inc)の John Kindervag 氏によって 2010 年に提唱されたセキュリティモデルの概念です。10 年が経過しながら十分に普及していない状況は、下記の実装上の課題があるためだと言えるでしょう。

■コスト面での課題

ゼロトラストは UTM のような製品を導入するだけで実現できるものではなく、EDR（Endpoint Detection and Response）や認証基盤、VPN 等様々なセキュリティ分野への初期投資が必要となります。またそれらを統合的に運用するためにエンジニアの確保や運用保守コストが必要になります。

■業務運用面での課題

ゼロトラストでは内部ネットワークをさらに細分化したマイクロセグメンテーションを構築し、各セグメントへのアクセスごとに認証が必要となります。ユーザはアクセス時に毎回パスワード入力をするとなると業務効率が著しく低下します。セキュリティは向上しますが利便性が低下するというトレードオフの課題が発生します。

■システム運用面での課題

これまでの説明の通り、ゼロトラストでは様々なセキュリティ分野を統合的に運用するモデルです。システムの運用にあたり、各分野に精通するエンジニアが求められます。各機器から出力されるログを分析しインシデントレスポンスに備える必要があります。 EDR を例に挙げると、各クライアント端末から膨大なログが出力されるため、これを人がひとつずつ分析することは不可能です。そこで SIEM（Security Information and Event Management）のような分析基盤を運用することになりますが、SIEM の導入や運用も莫大なコストが必要となります。

4. ゼロトラストの実現に向けて

クラウドの普及によりゼロトラストの課題は飛躍的に解決されつつあります。現在、大手クラウドベンダーでは IAM（Identity and Access Management）によりリソースへのきめ細かなアクセス制御を実現しています。また、サービス内容を細分化することでマイクロセグメンテーションも実現しています。更にシングルサインオン（SSO）を導入することで利便性も確保できます。このように従来はゼロトラストを自社で構築しようとすると機器の購入から構築、運用、保守まで莫大なコストが必要でしたが、クラウドサービスを利用することでコストコントロールが柔軟にできるようになってきています。

しかし、インシデントレスポンスに関しては従来通り自社で実施する必要があります。ゼロトラストではインシデントの検知に信用スコアを使用することが予想されます。検知した後は信用スコア変動の原因を分析し、分析結果に応じた対処が必要となります。これには専門家の知識、ノウハウが必要となるでしょう。

5. ゼロトラスト環境におけるセキュリティ監視について

上記の通り、ゼロトラスト環境でのセキュリティ監視は信用スコアを軸とした分析と検知を実施されることになります。具体的には、あるデバイスで起動すべきアプリケーションの起動時間が短い場合やあるユーザが普段アクセスしない時間帯にアクセスし、認証に成功した場合等、これらの信頼評価を蓄積しスコアとして管理します。この信用スコアを軸にインシデントを検知することは誤検知の低減、攻撃検出精度の大幅な向上に寄与し、今後のセキュリティ監視の指標として期待されています。

6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス「e-Gate」 e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp