覚えておきたいクラウド&データのキホン（第14回）

クラウドプロキシとは？メリット・デメリットを比較

2022.03.31

クラウドサービスの台頭により、企業のIT環境は「所有」から「利用」へと大きく変化しています。

それによって、社内のネットワークからインターネットに接続するためのプロキシ（プロキシサーバー）も、クラウドサービスとして提供されるようになっています。オンプレミスのプロキシとクラウドプロキシは、何が違うのでしょうか。本記事では、クラウドプロキシの仕組み、機能、メリット・デメリットなどを紹介します。

クラウドプロキシの概要

プロキシ（Proxy）は「代理」という意味を持つ言葉です。企業の内部ネットワークとインターネットの境界で、Webブラウザーなどの代理としてインターネットに接続するのがプロキシの役割となります。

一般的にプロキシは、企業で情報セキュリティ対策のために導入されます。プロキシを代理として利用することで、アクセス先のIPアドレスをサイバー攻撃者に追跡されることを防いだり、悪意あるWebサイトへのアクセスを制限したりできます。

このプロキシをクラウド上に構築したものが「クラウドプロキシ」です。オンプレミス環境に置かれたプロキシ（以下、従来型のプロキシ）とクラウドプロキシの役割は同じで、置かれている場所が異なります。

クラウドプロキシの仕組み

クラウドプロキシが登場した背景には、SaaS（Software as a Service）の普及が関係しています。テレワークなどで従業員が社外から社内のサーバーにアクセスする機会が増えたことで便利になった半面、機密情報の漏えいリスクなどが生じているためです。

社内から社外のWebサーバーへアクセスする際は、従来型プロキシを使うことで、ある程度の情報セキュリティが担保できます。一方、テレワークなどで社外からインターネットや社内サーバーにアクセスする際は従来型のプロキシをそのまま使えないため、クラウドプロキシが必要になったというわけです。

従来型のプロキシを経由して社外から社外のWebサーバーにアクセスすることもできますが、そのためにはVPN（Virtual Private Network）で社内のネットワークに接続しなければなりません。

対してクラウドプロキシは、クラウド上にあるプロキシサーバーが通信をコントロールします。Webサーバーへアクセスする際、クラウドプロキシを経由すれば、情報セキュリティを担保しながら、直接Webサーバーへアクセスできます。

クラウドプロキシの機能

クラウドプロキシは、従来型のプロキシと同様にWebブラウザーなどの代理としてWebサーバーと通信する役割のほかに、外部とのセキュリティゲートウェイとしても機能します。以下3つに分けて紹介します。

複数の情報セキュリティ機能

クラウドプロキシは、アンチウイルスやURLフィルタリング、サンドボックスなど、複数の情報セキュリティ機能を用意しています。最近では、クラウドサービスの通信を監視するCASB（Cloud Access Security Broker）の機能を有するクラウドプロキシもあります。これらを活用することで、従業員がクラウドサービスを使う際の情報漏えいリスクを低減させることができます。

通信負荷の分散

SaaSなどのサービスを導入すると、従業員のアクセスが集中して社内ネットワークに負荷がかかり、通信が不安定になることがあります。クラウドプロキシを通してネットワークへの負荷を分散させることで、通信のパフォーマンス低下を抑えることができます。

マルチデバイスへの対応

テレワークでは、PCのほかスマートフォンやタブレット端末など、さまざまなデバイスからインターネットにアクセスすることが想定されます。しかし、デバイスごとに情報セキュリティ対策をするのは、管理側に多大な労力が伴います。すべてのデバイスからのアクセスをクラウドプロキシ経由にすれば、情報セキュリティポリシーを統一しやすくなります。

クラウドプロキシのメリット・デメリット

メリット1：社内ネットワークの負荷軽減

従来型のプロキシは、社外から直接アクセスできません。VPNを利用して社内ネットワークにアクセスする必要がありますが、アクセスが集中した際は社内ネットワークに負荷がかかり、通信のパフォーマンスが低下するケースがあります。

クラウドプロキシは社外から直接アクセスできるため、社内ネットワークのパフォーマンスに影響を及ぼしません。

メリット2：運用コスト削減

従来型のプロキシは、自社でサーバーを管理する必要がありました。加えて、トラフィックが増加した場合、都度サーバーやネットワーク機器を増設しなければなりませんでした。サーバーを管理する人材の確保や費用も必要です。

クラウドプロキシの場合、サーバーはクラウド事業者が管理します。サーバーやネットワーク機器を購入する必要がなく、ハードウエアの管理も必要ないため、従来型のプロキシと比べコストを削減できる可能性があります。

デメリット1：業務をサービスに合わせる必要がある

クラウドプロキシは、クラウド事業者によってサービスの更新が行われます。更新によって管理画面や各種設定の手順が変更された場合、業務もそれに合わせて変更する必要があります。アップデートの内容が周知された段階で、修正点や変更点を事前に確認しておくことが求められます。

デメリット2：障害発生時に自社で対応できない

クラウドプロキシは、クラウド事業者が運営しています。例えば、クラウド事業者がサイバー攻撃に遭い、サービスが停止する可能性もゼロではありません。もしそうなった場合、自社では対応できないので復旧まで待つ必要があります。

まとめ

クラウドプロキシは、クラウドサービスの利用において、ネットワークの最適化や情報セキュリティ対策、コスト削減につながる有効な手段の1つです。もしクラウドプロキシの導入を検討されている場合、NTT西日本の「セキュリティおまかせプラン・セキュリティおまかせプラン プライム」をお薦めします。同サービスは不正アクセスなどの外部脅威と、従業員によるデータ紛失といった内部脅威の双方に対応したサービスです。「セキュリティおまかせプラン」であれば有償オプション、「セキュリティおまかせプラン プライム」であれば基本サービスとしてクラウドプロキシが利用でき、悪意のあるWebサイトへのアクセスの検知・遮断を実施します。不正通信や異常検知があった場合はセキュリティサポートセンターから連絡が届いたり、毎月運用監視レポートが送られたりとサポート体制も充実しているので、情報セキュリティ担当者の負担軽減も期待できるでしょう。