

5 セキュリティ

# 安心・快適な XaaS 利用を可能にし、 ビジネス変革を支える “XaaS Access Security”

ビジネスの変革を目的にデジタルトランスフォーメーション（以下、DX）を推進する企業は、さまざまな XaaS（ザース：IaaS、PaaS、SaaS などの総称）を利用するようになる。これに伴う IT インフラの多様化に従来のセキュリティ対策だけで対応することは難しいため、NTTコミュニケーションズ（以下、NTT Com）は “XaaS Access Security” の提案を進めている。

## 多様な IT インフラに対応する セキュリティ対策が必要

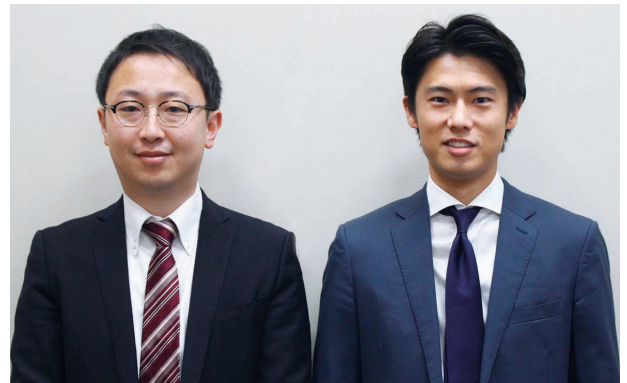
「迅速な市場参入」、「利益率の増加」、「働き方改革」といったビジネス変革に取り組む企業にとって、さまざまな XaaS が欠かせないものとなっている。それに伴い、アクセス元はオフィスに加えて外出先や自宅、アクセス経路はインターネットや MPLS、アクセス先はデータセンター（以下、DC）や XaaS といったように、IT インフラが多様化している。この状況に対応するセキュリティ対策が必要であるとして、大六氏は次のように語る。

「拠点と DC を MPLS で接続し、インターネットとの境界にファイアウォールを設置する、従来の『境界防御』型セキュリティ対策は、境界の『内』を保護するためのものです。外出先からのモバイル通信、自宅からインターネットを経由した XaaS 利用といった『外』の IT インフラは保護できません。安心して XaaS を利用するには『外』を保護する対策が必要ですし、IT インフラの変化に合わせてセキュリティ対策も常に進化する必要があります。これを可能にするのが、クラウド型プロキシと CASB（キャスビー：Cloud

Access Security Broker) を中心とする “XaaS Access Security” です。」

## クラウド型プロキシ (分散型インターネット ゲートウェイ)

インターネット接続を集約した DC にインターネットゲートウェイ（以下、IGW）を設置する従来の集約型に対し、クラウド型プロキシは、世界中のノードに設置した IGW を通じ、どこからでも安全に XaaS へアクセスできるようにし



NTTコミュニケーションズ株式会社 ICT コンサルティング本部  
(左) 井本 裕基氏 (右) 大六 隼人氏

た、分散型のプロキシサービスだ（図 1）。アクセス元の端末にプロキシのアドレス設定さえしておけば、利用者がある場所に応じて自動でノードを選択し、どこに居ても近

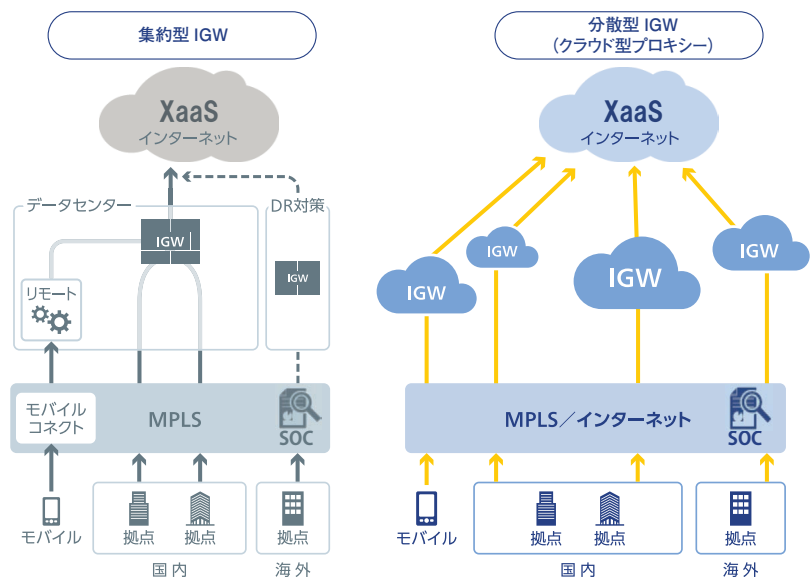


図 1 インターネットゲートウェイ構成イメージ

くにあるノードを自動選択する。アメリカにいるときにはアメリカのIGWを通じてXaaSにアクセスできる。クラウドサービスであるため、利用者の増加に対応するのも容易だ。

「グローバル企業にとってのメリットが特に大きいと言えます。機能追加や変更も全世界同時に行うことができます。また十分な機能を備えているため、オンプレミスのプロキシもクラウド型プロキシに置き

換え、IT資産を削減することも可能です。さらに、各IGWのプロキシログをNTT ComのSOC(Security Operation Center)に送り通信状況を分析することもできます。これは日本でNTT Comだけが提供しているサービスメニューです。」(大六氏)

### CASB：シャドーITや不適切な操作、不正アクセスを防止

多様なXaaSの登場に伴い、企業側が把握していないITサービスを社員が勝手に使う、いわゆるシャドーITが増加しており、情報漏洩やサービス停止によるデータ紛失などのリスクが懸念されている。「把握していないサービスが10はある」と想定してシャドーITの実態を調査したところ、100を超えるサービスが使われていた、といった事例も珍しくないという。

企業が把握している安全なXaaSであっても、機密情報を暗号化せずにアップロードする、アップロードしたファイルの閲覧権限が不適切、

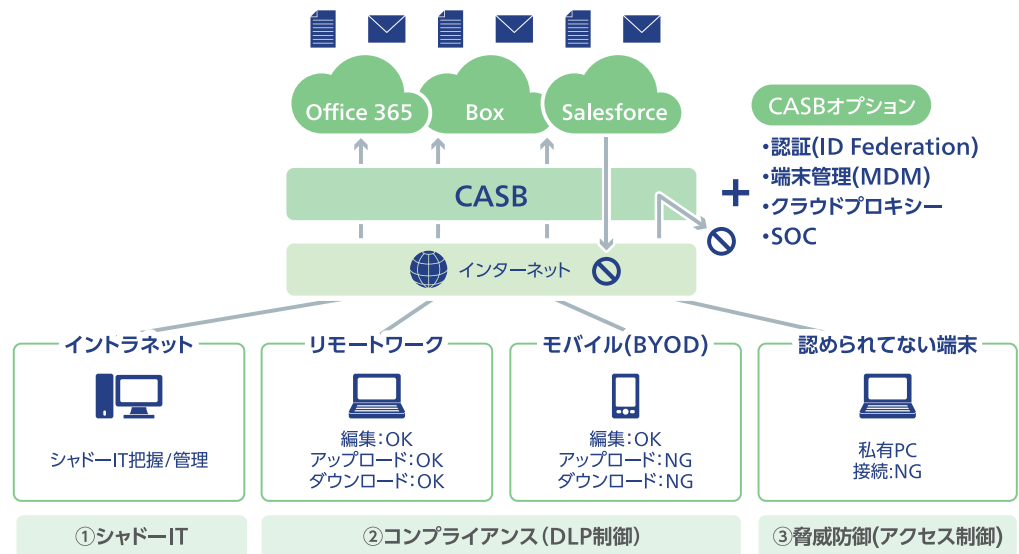


図2 クラウドセキュリティソリューション (CASB)

といった利用者の操作に起因する情報漏洩の可能性がある。こうした問題の防止に役立つのがCASBだ。

「CASBはXaaS利用に伴うトラフィックを一括して監視するクラウドサービスです。『どのサービスが安全か』というリストを持っているため、シャドーITを制限するだけでなく、『企業側で把握していなくても、安全なサービスならそのまま利用させる』という運用が可能です。また許可されているサービスでも、個人アカウントでのアクセスは制限することができます。さらに、ファイルをアップロードする際には強制的に暗号化させる、個人情報が含まれるデータには制限をかける、といったことに加え、データ共有する相手が適切な権限を持った相手かを判断することも可能です。」(井本氏)

このほか「普段は日本からアクセスしているアカウントが数分後に突然アメリカからアクセスした」、「普段は行わない大量のデータダウンロードや外部へのコピーが行われ

た」といったように、利用者の振る舞いから異常を検知し、アクセスを制限するといった制御を行う機能も備えている。

### 各種技術を組み合わせた複合的なソリューション提供

NW、DC、クラウドまでフルスタックで提供するケイパビリティ、マルチベンダー対応といったNTT Comの特長を活かすソリューションについて、井本氏は次のように述べている。

「エンドポイントで脅威の検知や対応を行うEDR(Endpoint Detection and Response)、SD-WAN (Software Defined WAN) など、各種技術を組み合わせた複合的なソリューションとしてXaaS Access Securityを提供します。また、セキュリティ対策の計画立案からソリューションの導入・運用サポート、さらには効果分析や改善に向けたコンサルティングまで、トータルで対応できる強みを活かしていく考えです。」