クラウドサービス（SaaS）活用のための ネットワーク設計

2021 年 8 月

石塚健太郎[1]、中川あきら[1]、関谷勇司[1]、田丸健三郎[2]

要旨

オフィス業務用のツールやグループウェア、コミュニケーションツール等のソフトウェアの機能をクラウドサービスとして提供するソフトウェア・アズ・ア・サービス（SaaS）を活用することで、業務の効率化や円滑なコミュニケーションを実現できる。一方で、SaaS 利用にあたって多くのトラフィックがインターネットを含む組織外部のネットワーク帯域を消費する。このようなトラフィックを既存のネットワーク基盤が十分に処理できず、円滑な SaaS 利用が妨げられることがある。また、組織外にあるリモート端末から組織内のサーバや SaaS にアクセスする場合にも、トラフィックが適切に制御される必要がある。本ディスカッションペーパーでは、これらのトラフィックを扱うためのネットワーク構成上の注意点と、ネットワーク上のボトルネックを回避し SaaS の利用を円滑化する各種のトラフィック制御技術の比較及び適用領域を示すとともに、それらの技術を利用する際に考慮すべきセキュリティ上の注意点について述べる。

[1] 内閣官房政府 CIO 補佐官
[2] 内閣官房情報通信技術（IT）総合戦略室 プロジェクトマネージャー

目次

１　はじめに

１．１　背景と目的

政府では「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年 6 月 7 日各府省情報統括責任者（CIO）連絡会議決定）に基づき、「クラウド・バイ・デフォルト原則」、すなわち、政府情報システムを整備する際にクラウドサービスの利用を第一候補とする原則を導入し、政府情報システムにおける効率性・セキュリティ水準・技術革新対応力・柔軟性・可用性の向上を目指している。

クラウドサービスを活用することは、政府機関や行政機関にとっても、組織の内外問わず業務を実行できる環境を提供し、迅速なデータの共有やコラボレーションを促進し、最新の機能が適宜実装され、システム基盤の管理をクラウドサービス事業者に任せることができる等、多くの利点をもたらす。特に既存システムをインフラストラクチャ・アズ・ア・サービス（IaaS）に移行するのみならず、アプリケーションの機能をサービスとして利用するソフトウェア・アズ・ア・サービス（SaaS）を活用することで、業務や運用の効率化が期待できる。代表的な SaaS としては、Microsoft 365 や Google Workspace 等のグループウェア、Box や Dropbox 等のコンテンツ共有サービス、Cisco WebEx や Zoom 等のビデオ会議サービスなどが挙げられる。

アプリケーションの利用において SaaS は非常に便利である一方、政府機関のような多数の業務端末がネットワークに接続される環境では、SaaS 向けのトラフィックの特性に注意する必要がある。SaaS の導入により、メールやスケジュール共有、ファイル共有等の従来組織内に閉じていたトラフィックや、ビデオ会議等で新たに生じるトラフィックが組織外の SaaS に向かい、組織外向けのトラフィック量が増大する。加えて、グループウェアやビデオ会議などの SaaS はデータの同期・予定表の共有・チャット等のやりとりなどの機能を利用するために、通常の Web 閲覧等と比べて非常に多くの通信セッション（端末・SaaS 間通信で確立される通信の単位、TCP ではコネクションに相当）を常時利用するため、同時接続セッション数が増大する特性がある。これらの特性により、既存の政府機関等のネットワーク構成のまま SaaS の利用を始めると、既存のネットワーク基盤では通信のボトルネックが生じ、SaaS へのトラフィックを十分に処理できない。その結果、SaaS の円滑な利用が困難となるだけではなく、Web 閲覧を始めとする他のトラフィックへの影響が生じる。

本ディスカッションペーパーでは、SaaS の利用により生じるトラフィックの特性と、既存のネットワーク構成で生じる通信のボトルネックを回避し、SaaS の円滑な利用を実現するためのトラフィック制御技術について解説し、それぞれの適用領域について述べる。また、トラフィック制御以外のネットワーク構成の注意点や、トラフィック制御を行う場合のセキュリティ上の注意点についても述べる。

１．２　適用対象

本ディスカッションペーパーは、SaaS の活用を検討している政府機関や行政機関を対象としている。

１．３　位置付け

本ディスカッションペーパーは、SaaS を円滑に利用するためのネットワーク設計における要件定義や、クラウドサービス向けのトラフィック制御技術を選択するための標準ガイドライン群の一つとして位置付けられる。

１．４　用語

本ディスカッションペーパーにおいて使用する用語は、本ディスカッションペーパーに別段の定めがある場合を除き、標準ガイドライン群用語集の例による。その他専門的な用語については民間の用語定義を必要に応じて参照すること。

２　SaaS活用のためのネットワークの要件

２．１　既存の政府機関等のネットワーク構成

従来の政府機関等のネットワークでは、多くの場合、各拠点から通信事業者が提供する IP-VPN 等を利用した広域ネットワーク（WAN）を経由してデータセンタや中央庁舎等（以下「システム基盤」）に接続し、システム基盤の内部に配置されているメールサーバやスケジュール共有サーバ、ファイルサーバ、業務サーバ等にアクセスし業務を実施する（図 1）。このネットワーク構成では、業務端末を用いてインターネットを利用し調査や情報収集を行う際には、不正サイトへのアクセスや不正ファイルのダウンロードを防止しセキュリティを担保するためのプロキシサーバやファイアウォール、統合脅威管理（UTM）装置等を経由して接続する構成となっている。リモートワークなどで外部から府省内で利用する業務サーバ等にアクセスするためには、リモート端末から SSL-VPN や IPsec-VPN 等で通信を暗号化したリモートアクセス経由で、システム基盤のサーバに接続する。若しくは、仮想デスクトップインフラストラクチャ（VDI）環境がシステム基盤の内部に構築され、組織内外からリモート端末を VDI 環境に接続した上で業務サーバにアクセスする形態が採用されている。

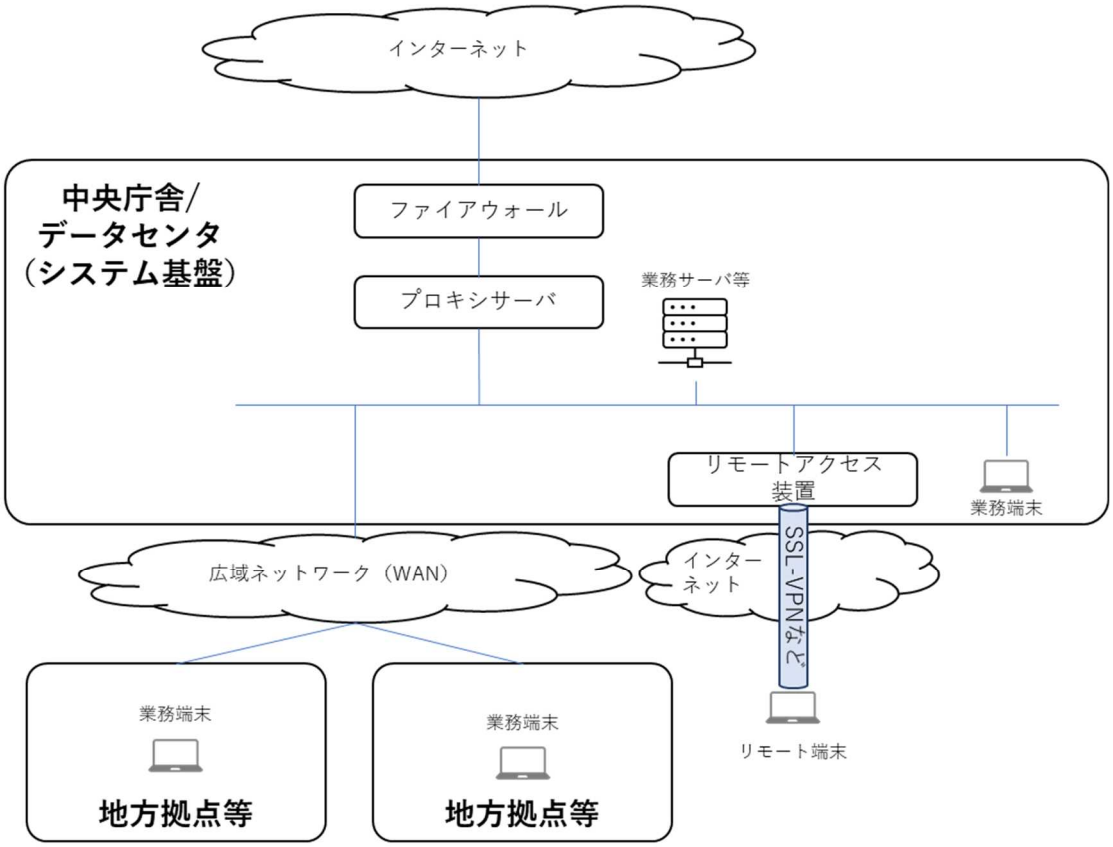

図 1　既存の政府機関等のネットワーク構成

２．２　SaaS 向けトラフィックの特性

SaaS では、メールサーバやスケジュール共有サーバ、ファイルサーバ、業務サーバ等に相当するものが組織外の SaaS から提供される形になる。そのため、これまで各拠点とシステム基盤の間に留まっていたこれらのトラフィックが全てインターネットに流れることになる。加えて、オフィススイート等端末側にインストールされるアプリケーションでは端末内部で完結していた処理も、SaaS との通信を必要とするようになる。さらに、ファイルの保存先をクラウドストレージ等に設定する利用形態では、SaaS への通信量は一層増大する。

SaaS として提供されるビデオ会議用のアプリケーション等のビデオコミュニケーションツールでは、トラフィックの増大に加え、それらが利用する通信プロトコルも考慮する必要がある。具体的には、プロキシサーバやファイアウォールで通過させていた HTTP/HTTPS に加え、これまでは遮断していた UDP 等も通過させなくてはならない。

さらに、SaaS 向けトラフィックの特性として、端末 1 台が利用する通信セッションの数が非常に多いことにも留意する必要がある。メールサービスやスケジュール調整といったグループウェアでも、1 端末あたり通常は 20～30 セッション、多い場合は 100 セッション

以上を同時利用し、かつ継続的に接続する。そのため、コンテンツへのアクセス時のみに通信セッションを利用するこれまでの Web 閲覧の利用とは桁違いに多くの同時接続通信セッションを考慮する必要がある。同時接続通信セッションが多くなると、プロキシサーバやファイアウォール等のネットワークセキュリティ機器が処理可能なセッション上限数を越え、通信帯域に余裕があってもそれ以上の通信ができなくなるといったボトルネックが発生し、サービスの利用に支障が発生する場合がある。

ビデオコミュニケーションツール等のリアルタイム性を必要とするアプリケーションについては、端末から SaaS までのネットワーク遅延を抑える必要があるものもある。例えば、端末と SaaS 間の通信遅延（ラウンドトリップタイム）が一定以下、たとえば 100ms 以下、を要件とするものがある。各拠点や外部から SSL-VPN 等で接続した端末のインターネット通信では、VPN を経由することで SaaS までの通信距離が大きくなり通信遅延が生じることがある。また、ネットワーク内に多数のファイアウォールやプロキシサーバ等のセキュリティ機器が配置される場合には、それらの機器による通信遅延が大きくなりサービスが必要とする遅延要件を満たせないこともある。この遅延要件を満たせなくなると、ビデオ会議時に映像が表示されないなどの問題が生じる。このため、SaaS によっては遅延要件を満たすためプロキシサーバ等の利用を推奨していないものも多い。付け加えると、遅延要件の制約はリアルタイムコミュニケーションサービスに限らない。遅延が大きくなると、例えば予定表の表示に大幅な時間を要するなど、グループウェアの対話的な操作性の劣化につながる。

SaaS では基本的に接続先をドメイン名で規定しており、新機能の導入やサーバの変更等でドメイン名に紐づいた IP アドレスは頻繁に変動するという特性がある。また、コンテンツ配信やレスポンスの高速化のためにコンテンツ配信ネットワーク（CDN）等を活用しており、ドメイン名がコンテンツ配信事業者の IP アドレスに紐づくことも多い。ルータ等の従来の通信機器では IP アドレスに基づいてトラフィック制御を行うため、SaaS 向けの通信を判別して制御することが困難となる。一方、SaaS に用いられるドメイン名の変更は稀であり、SaaS へのトラフィック制御を効率的に行うには、ドメイン名に基づいたトラフィック制御が必要となる。ただし、SaaS の新サービスの追加や旧サービスの廃止に伴ってドメイン名の変更は起こりうるため、運用上はドメイン名の変動も考慮しておく必要がある。

上記の SaaS のトラフィックの特性から、従来のネットワーク構成で生じる問題を図 2 にまとめて示す。SaaS を利用するにあたっては、このようなトラフィックの特性に対応するために、これまで Web サイトの閲覧だけを考えて構成されていたネットワーク構成を変更する必要がある。

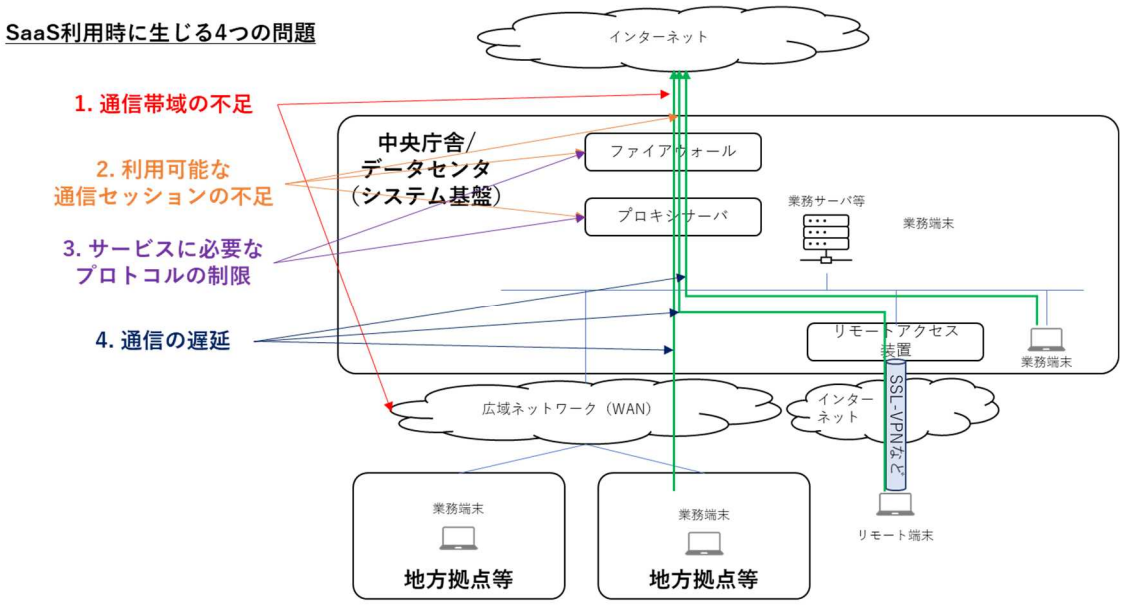

図 2　SaaS 利用時に生じるネットワーク上の問題

２．３　SaaS 利用時に考慮すべきネットワーク設計上の注意点

図 2 に示した SaaS 利用時に生じるネットワーク上の問題に対処するため、ネットワークの設計時に以下の 4 点に注意して要件を定める必要がある。

1. 十分な通信帯域の確保

グループウェア等の SaaS 利用では端末あたり、最大 2Mbps 程度の SaaS 向け通信が新たに生じる。また、ビデオコミュニケーションツールではさらに端末あたり最大数 Mbps を必要とする。端末あたりの通信量は内容によって異なるが、オーディオ通信のみで最大 80kbps、端末の画面共有も行うと最大 150kbps、顔画像等を出してのビデオ通話では画質により 600kbps～3Mbps を必要とする。これらのアプリケーション利用では、端末の台数が多くなると組織全体としての SaaS 向けの通信量が非常に大きくなる。そのため、インターネット回線等の SaaS 向け通信回線の帯域が十分でない場合は、SaaS 向け回線の十分な帯域の確保、若しくは回線の増設を行わなくてはならない。ここで必要な SaaS 向けの通信帯域はピーク時の端末数と端末 1 台当たりに必要な通信帯域を掛け合わせることで概算できる。例えば、ピーク時に 1,000 台の端末が同時にグループウェア（約 2Mbps）と顔画像等を出してのビデオ会議（600kbps 以上）を利用する想定では、少なくとも端末 1 台当たり約 2.6Mbps（2Mbps+600kbps）×1,000 台＝約 2.6Gbps の通信量を想定すべきである。

2. 大量の通信セッションへの対応

２．２節に示した通り、SaaS 向けの通信セッションは、Web 閲覧で生じるものとは異なり常時接続されるものが多く、大量の通信セッションを同時に扱う必要がある。セキュリティ機器、すなわちプロキシサーバやファイアウォール等では処理できる同時セッション数に制限があるため、宛先が明確で十分なセキュリティを担保できる SaaS 向けの通信に関しては、それらの機器をバイパスするトラフィックの制御を行う等、セキュリティ機器が処理するセッション数を機器要件に見合ったセッション数に抑える必要がある。

また、大量の通信セッションによって、組織外への NAT アクセスに利用するグローバル IP アドレスの送信元ポート番号が枯渇する場合がある。この場合には、仮に通信帯域が十分にあったとしても、ポート番号不足によって SaaS や Web へのアクセスが出来なくなる。そのため、組織内の端末数に見合った数の、NAT アクセス用のグローバル IP アドレスを確保しなくてはならない。1 グローバル IP アドレスあたり、約 60,000 ポートが送信元ポートとして利用できるため、これを 1 端末あたりの平均同時セッション数で割ることによって、グローバル IP アドレス１つあたりの端末の収容数の概算が可能となる。例えば、1 端末あたり平均 30 同時セッションを利用する場合、2,000 端末ごとに、1 グローバル IP アドレスを用意しなければならない。

3. 必要な通信プロトコルの利用許可

コラボレーションやビデオコミュニケーションを目的とする SaaS では、音声や映像を利用するリアルタイム通信を扱うために従来の HTTP/HTTPS ではなく UDP や QUIC を利用することが多い。従来のネットワーク構成では、プロキシサーバやファイアウォールによってインターネット向けの通信に HTTP と HTTPS 通信のみを許可している場合もあり、円滑な SaaS の利用には、それらに加え、UDP や QUIC 等を許可する必要がある。許可すべきプロトコルとポート番号等は各 SaaS 事業者より情報が提供されているため、それらに基づいたアクセス許可を実施する。

4. 通信遅延の抑制

SaaS を十分に活用するためには、端末からサービスまでの通信遅延がより少ないネットワーク構成としなければならない。具体的には、ネットワーク構成の階層をより少なくする、SaaS 向けの通信に関してはセキュリティ機器をバイパスする、帯域保証型の回線やより通信遅延の少ない回線を SaaS 向けに利用するといった、通信遅延を抑える対策を検討する必要がある。

また、同一の通信回線を利用して通常の Web アクセスと複数の SaaS を利用する場合には、それらの干渉を避けなければならない。この干渉には一部のトラフィックのバーストによる他のトラフィックへの影響が含まれる。このような影響を軽減し、より安定した SaaS の利用を実現するためには、帯域制御装置等を導入してサービスごとのトラフィックの最大利用帯域や最小利用帯域を制御する必要がある。

２．４　通信のボトルネックを回避するためのトラフィック制御

２．２節に示した通り、既存のネットワーク構成での SaaS 利用では、インターネット接続や WAN 回線、セキュリティ機器やリモートアクセス回線など、ネットワーク上の様々な箇所で通信ボトルネックが生じる可能性がある。ネットワーク基盤にボトルネックが生じると、SaaS の十分な活用ができないだけでなく、他のトラフィックにも影響を与える。これらのボトルネックを回避するためには、以下のような手段で SaaS 向けのトラフィックを制御する必要がある（図 3)。

1. SaaS 用の回線を敷設し、SaaS 向けのトラフィックを特定の回線に向けることにより、帯域不足を解消する。別回線を敷設することで既存のトラフィックへの影響を与えないようにできる。インターネット回線そのものの増速で通信帯域の不足に対応することもできる。
2. SaaS 向けのトラフィックを識別し、プロキシサーバやファイアウォール等のセキュリティ機器をバイパスする。
3. 各拠点に SaaS 向け回線を別途敷設し SaaS 向け通信を特定の回線に振り分ける。別回線の敷設により既存のトラフィックへの影響を与えないようにできる。インターネット回線と同様に WAN 回線の増速で対応することもできる。
4. リモート端末に通信振り分けを行うアプリケーションをインストールし、SaaS 向けの通信がリモートアクセス回線を利用しないように振り分ける。

いずれの場合においても、SaaS 向けのトラフィックを適切に振り分けるトラフィック制御技術を利用しなくてはならない。３章ではこのような SaaS 向けのトラフィック制御技術について詳説し、それぞれの適用領域について述べる。

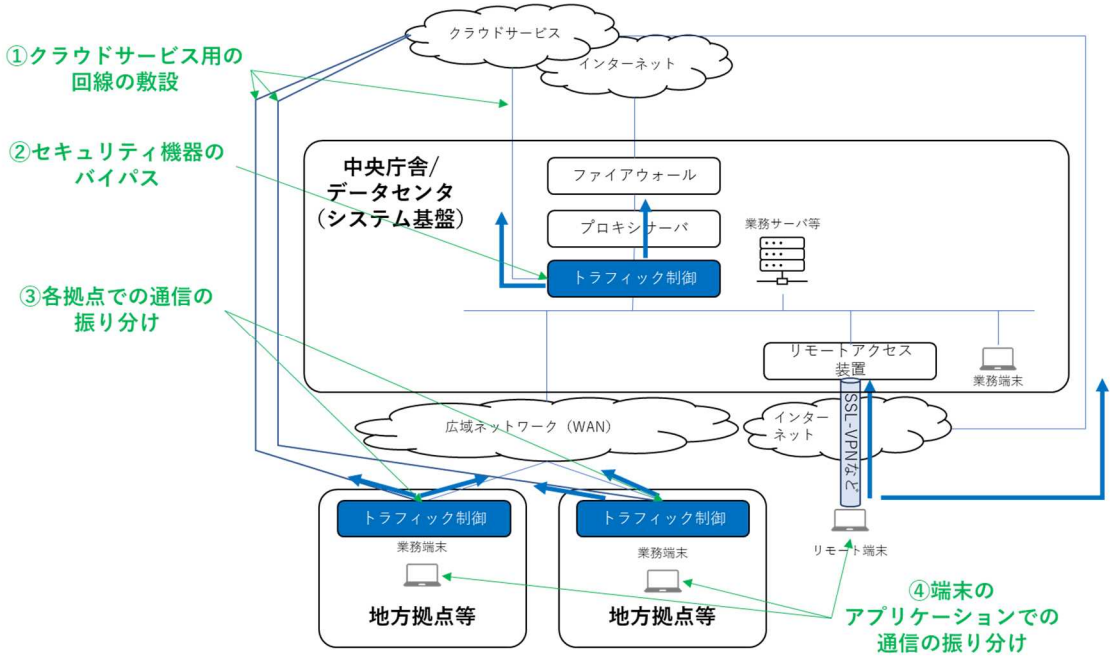

図 3　SaaS 活用のためのトラフィック制御

3　SaaS向けトラフィックの制御技術と適用領域

SaaS 向けのトラフィックの制御は、ネットワーク機器や端末にインストールするアプリケーションで行うことが可能だが、それぞれのトラフィック制御で利用している方法に違いがあることに留意する必要がある。このため、満たすべき要件に合わせた技術を選択する必要がある。SaaS 向けトラフィックの制御には、大別すると以下の 3 つの方法がある。

- IP アドレスに基づくトラフィック制御：SaaS が利用している IP アドレスを識別してトラフィックを制御する方法。
- ドメイン名に基づくトラフィック制御：SaaS が利用するドメイン名を識別してトラフィックを制御する方法。
- アプリケーション識別に基づくトラフィック制御：トラフィックの内容を識別して SaaS を識別し、トラフィックを制御する方法。

本章では、それぞれの方法の特徴と適用可能な領域について述べる。

3．1　IP アドレスに基づくトラフィック制御

主にルータやファイアウォール、UTM で SaaS 向けトラフィック制御を行う場合には、SaaS 事業者が公開している IP アドレス範囲や通信プロトコル、ポート番号の情報等を用いて、トラフィックの送信先/送信元の IP アドレスを識別することでトラフィック制御を行うことができる。また、UTM の製品によっては SaaS ごとの IP アドレスのリストを自動収集し、そのデータベースを配信することでトラフィック制御をしやすくする仕組みを提供してい

るものもある。これらを利用することで、ルータやファイアウォール、UTM により該当する IP アドレス向けの通信を制御して異なる通信経路に向ける等の動作が可能になる。

その一方で、２．２節で示した通り SaaS の多くが CDN を利用しており、また、サービスそのものの IP アドレスが頻繁に変わることから、IP アドレス範囲の変更に注意しなくてはならない。ベンダー提供の自動配信される IP アドレスのリストも、リアルタイムの完全な追随が保証されているわけではない。そのため、自動配信される IP アドレスのリストをファイアウォールのルール等に適用し SaaS へのアクセス可否等で利用してはならない。これは、リストから漏れた SaaS へのアクセスが阻害され、アプリケーション利用が阻害されるためである。したがって、この方法によるトラフィックの制御は、トラフィックを IP アドレスで識別可能な範囲で特定の回線に振り分ける場合に適しており、トラフィックの振り分け先の双方が SaaS に疎通している環境でのみ利用すべきである。

また、IP アドレスによるトラフィック制御を行う際に、端末にプロキシサーバの宛先が指定されている場合には、トラフィックの宛先 IP アドレスがプロキシサーバのものとなるため、宛先が SaaS であるかどうか識別ができなくなり、結果として全ての通信がプロキシサーバを通ることになる。この場合は、端末側に PAC ファイル等を配布して、振り分け対象の SaaS 向けの通信に関してはプロキシサーバをバイパスして、IP アドレスによるトラフィック制御を適用しなくてはならない。この場合には、PAC ファイルを常に最新に維持することも運用要件に含めなくてはならない。

加えて、IP アドレスに基づくトラフィック制御では、同一の宛先 IP アドレスで複数のサービスが稼働している場合の区別はつかない。例えば、ドメイン名 www.office.com が対応するグローバル IP アドレス（13.107.6.156）は、このドメイン名以外にも 22 のドメイン名と対応している（例えば rooptekno.com 等）[3]。IP アドレスに基づいて通信の振り分けを行っている場合、どちらのドメインでアクセスした場合も同じ通信経路に振り分けられてしまう。したがって、同じ IP アドレスを持つ異なるサービスのトラフィックの振り分けを行う場合は、IP アドレス以外の方法でのトラフィック制御を行わなくてはならない。

３．２　ドメイン名に基づくトラフィック制御

Web アプリケーションサーバーの負荷分散などを行う際に利用されるネットワーク機器であるアプリケーションデリバリコントローラ（ADC）では宛先のドメイン名に基づいたトラフィック制御を行うことができる。この方式では端末からの通信を一度 ADC で受信し、ADC が宛先に対する名前解決（ドメイン名と IP アドレスの変換）を行い、宛先との通信を確立する。SaaS のドメイン名は公開されており、トラフィック制御を行いたいドメイン名をリストとして ADC に登録しておき、ADC がトラフィックに含まれるドメイン名をリストと照合することでトラフィックの制御を行う。そのため、SaaS の IP アドレスの変更に対処

[3] 2021 年 6 月時点

しやすい利点がある。ドメイン名に基づくトラフィック制御では、IP アドレスに基づくものに比べてより確実な制御を可能とし、かつリストを更新する頻度も少ない。例外的に、ドメイン名が頻繁に変更される一部の SaaS については、自動更新サービスも提供されている。３．１節で述べたような同一の宛先 IP アドレスで複数のドメイン名でのサービスが提供されている場合にトラフィックを適切に制御したい場合には、ADC を利用してサービスのドメイン名に基づいて通信経路の振り分けや通信可否の決定を行わなくてはならない。

SaaS 向けのトラフィック以外の Web 閲覧などの通信を既存のセキュリティポリシーに従ったプロキシサーバなどで制御をしたい場合には、ADC をプロキシサーバとして動作させることで、既存のプロキシサーバと多段プロキシの構成を組むことも可能である。端末側では、ADC のみをプロキシサーバとして指定し、ADC で既存のプロキシサーバのバイパスの要不要を判断させることが可能になる。ADC は一般的なプロキシサーバと比較して非常に多くの同時セッションを高速に処理することができるため、SaaS 向けの通信で増大する通信量、セッション数に見合ったプロキシサーバを増設するよりも、ADC を併用する方が少ない機器数でトラフィックを処理できる。

一方で、ドメイン名に基づくトラフィック制御が有効なプロトコルは、通信データにドメイン名が含まれる HTTP 及び HTTPS のみとなる。UDP トラフィック等の制御を行う場合は、３．１節で述べた IP アドレスに基づく制御を ADC で行わなくてはならない。ドメイン名でトラフィック制御をおこなう際には、名前解決に利用する DNS に基づいてトラフィックを転送するため、４．２節で述べる DNS サーバの信頼性（名前解決後の IP アドレス情報の改ざんを防ぐための仕組みの導入等）を確保しなくてはならない。

UTM 等でも ADC と同様宛先のドメイン名の名前解決を行って通信を転送する仕組みを持つものもあるが、以下の点には注意が必要である。これらの通信機器では宛先ドメイン名を名前解決した後の IP アドレスをルーティングテーブルに保持し、この IP アドレスに基づいて通信経路を振り分ける実装としているものがある。この実装では、異なる宛先ドメイン名でも同じ宛先 IP アドレスであれば IP アドレスに基づく通信経路の振り分けがおこなわれるため、ドメイン名に基づいたトラフィック制御にこのような機器を利用してはならない。

３．３　アプリケーション識別に基づくトラフィック制御

アプリケーションの特徴を表すシグネチャ等に基づき SaaS 向けのトラフィックを識別する方式も利用されている。この方式は、ソフトウェア定義型 WAN（SD-WAN）装置や次世代ファイアウォール、端末にインストールするアプリケーションで利用されている。アプリケーションのシグネチャはベンダーが自動更新する形で提供されることが多く、利用者はアプリケーションを選択するだけで、自動的に SaaS 向けのトラフィックの制御を行うことができる。３．１節や３．２節で述べた IP アドレスやドメイン名の情報に加え、アプリケーション固有のトラフィックの特徴を利用してアプリケーション識別を行っており、HTTP や HTTPS

通信だけでなく UDP トラフィック等の識別や、同一 IP アドレスで提供されるサービスの差異の認識も期待される。

一方で、アプリケーションの識別方式の詳細は多くが非公開となっており、識別精度は100%ではない。特に通信序盤のトラフィックの識別精度が十分でない場合があることから、IP アドレスによるトラフィック制御と同様に、トラフィックをアプリケーション識別が可能な限り特定の回線に振り分ける場合に適しており、SaaS の利用を阻害しないためにはトラフィックの振り分け先の双方が SaaS に疎通していなくてはならない。アプリケーション識別の結果をファイアウォールのルール等に適用し SaaS へのアクセス可否等で利用すると、サービスへの到達性が阻害される場合があり、このような利用方法は避けるべきである。

また、IP アドレスによるトラフィック制御と同様に、端末にプロキシサーバの宛先が指定されている場合は、トラフィックの宛先 IP アドレスがプロキシサーバのものとなる。すなわち、アプリケーション識別に成功してもトラフィック制御ができず、結果として全ての通信がプロキシサーバに向かう。この場合は、IP アドレスによるトラフィック制御と同様に、端末側に PAC ファイル等を配布して、振り分けを行いたい SaaS 向けの通信に関してはプロキシサーバをバイパスしなくてはならない。この場合は、３．１節に示した通り、PAC ファイルに対するメンテナンスの運用を要件に含めなくてはならない。

４　トラフィック制御を行う際に留意すべきセキュリティ

本章では、SaaS 向けのトラフィック制御を行う際に考慮すべきセキュリティについて概説する。各セキュリティ技術の詳細は別のガイドライン等を参照すること。

４．１　既存の境界型ネットワークセキュリティに依存しないセキュリティ

２．４節に示した通り、SaaS を円滑に利用するために、既存の境界型ネットワークセキュリティで利用されているプロキシサーバやファイアウォール等のセキュリティ機器をバイパスする等、端末から SaaS に対して直接アクセスする場合がある。そのため、SaaS を活用した業務効率の向上を実現するには、従来の境界型ネットワークセキュリティに依存しないセキュリティについて考慮すべきである。

多くの SaaS は自身でセキュリティ機能を持っている。具体的には、アクセス制御、アクセスログの取得、ユーザの振る舞いの取得、SaaS 上のデータに含まれる不正の検知などがあげられ、サービス利用にあたってこれらの機能を積極的に利用すべきである。これらは統合セキュリティ管理サービスとの連携も可能であり、SaaS 利用に関わる不正な行動やデータの検知等を効率的におこなうこともできる。

境界型ネットワークセキュリティに依存しないアーキテクチャとして、ゼロトラストアーキテクチャの実現についても検討すべきである。この実現には、ユーザや端末等の組織内のリソースに対して適切な統合 ID 管理を行い、SaaS や組織内のサービス及びリソースへのアクセスに対して適切な認証と認可を行わなければならない。多くの SaaS は統合 ID 管理

基盤と連携して適切な認証・認可を行う機能を提供しており、これによりゼロトラストアーキテクチャを実現し、境界型ネットワークセキュリティ機器をバイパスしてもセキュリティを担保できる場合がある。ユーザや端末の振る舞いに応じた動的な認証・認可を行うために、端末の信頼性（インストールされている OS やアプリケーションが適切かどうか）や振る舞いの監視、複数端末に渡るネットワーク上での振る舞い監視、アクセス先のリソースやアプリケーションの信頼性を検証する仕組みを導入しても良い。

また、組織外部のリモート端末から直接 SaaS やインターネットにアクセスする場合の通信に対して、組織内のネットワークからインターネットにアクセスする際と同等の境界型セキュリティを適用する必要がある場合は、クラウドサービス型のプロキシ等を利用しても良い。SaaS 向けの通信の制御やクラウドサービス型のプロキシまでの通信の暗号化を行う場合は、リモート端末にインストールするアプリケーションと併せて利用することが望ましい。また、組織内にある業務サーバ等へのリモートアクセスを行う場合は、リバースプロキシ機能を提供しているクラウドサービスを利用しても良い。

４．２　ドメイン名の解決に関わるセキュリティ

２．２節で述べた通り、SaaS は基本的にドメイン名で宛先が規定されていることから、ドメイン名の情報改ざんを阻止する仕組みを導入すべきである。とくに組織の外部にあるリモート端末から SaaS を利用する場合には、適切な DNS サーバを利用する仕組みを導入すべきである。オープンな Wi-Fi 環境で提供される DNS サーバを利用した場合には特に情報の改ざんの可能性が高く、信頼できる DNS サーバを利用できる仕組みを導入することが望ましい。

DNS に登録された情報のセキュリティを保つためには、DNSSEC 等を利用して DNS サーバ間を転送される情報のセキュリティを保つとともに、端末から DNS に対するアクセスに DNS over TLS や DNS over HTTPS を利用して通信を暗号化することで、よりセキュリティを強化すべきである。また、DNS の名前解決の結果得られる IP アドレスが改ざんされていた場合に対応するために、IP アドレスレピュテーション等の脅威インテリジェンスを利用することが望ましい。これにより、通信経路上のトラフィック制御機器やセキュリティ機器においても、端末からの不正なサイトへのアクセスを防ぐことができる。

５　まとめ

SaaS を活用する際には、SaaS 向けのトラフィックの特性に対応したネットワーク基盤を構成する必要がある。SaaS 活用に適したネットワーク基盤の設計においては、以下の 4 点が必須要件となる。

1. インターネット向け回線（SaaS 向け回線）における十分な通信帯域の確保：1 台の端末あたり、SaaS 向けに平均数 Mbps のトラフィックの増加を見込んで通信帯域を確保しなくてはならない。インターネット回線の増速又は SaaS 向けの回線を別途導入して十分な

通信帯域を確保すべきである。

2. 大規模な通信セッションへの対応：1 台の端末当たり、少なくとも 20～30 の同時接続セッション数を追加で必要とする。端末の台数が多いとファイアウォールやプロキシサーバのようなネットワークセキュリティ機器が処理できる同時セッション数を上回るため、これらが通信のボトルネックとならないように、通信を制御する技術を用いて SaaS 向けトラフィックを適切にバイパスする等の対応をすべきである。さらに、NAT を利用する環境では組織全体として SaaS の接続に必要な送信元ポートが多数必要となるため、収容する端末数に応じて十分な数のグローバル IP アドレスを NAT に割り当てなくてはならない。
3. 必要な通信プロトコルの利用許可：ビデオ会議サービスのような SaaS では Web ブラウジングで利用する HTTP/HTTPS だけでなく UDP 等の通信を用いるため、端末と SaaS 間で必要となるプロトコルと宛先ポート番号を指定して通信を許可しなくてはならない。
4. 通信遅延の抑制：特にビデオ会議サービスのような SaaS では、通信遅延が 100ms 以下でないと映像が届かないなどの体感品質が劣化するものもあり、多くの SaaS がプロキシサーバの利用を推奨していない。これに対応するため、階層構造の少ないネットワーク設計やネットワークセキュリティ機器を通過するトラフィックのバイパスを行い、SaaS 向け通信の遅延を抑制しなくてはならない。

SaaS 向けトラフィックをバイパスする等適切な通信回線への振り分けを行う場合には、SaaS 向けのトラフィック制御技術を導入する必要があり、必要な振り分けの精度に応じて技術選択を行わなくてはならない。またセキュリティ面においては、SaaS の持つセキュリティ機能の活用や、統合 ID 基盤と連携した適切なアクセス制御等の従来の境界型セキュリティに依存しないセキュリティの導入、ドメイン名に対する情報改ざんを抑止できるような DNS 向けのセキュリティの導入が望ましい。

6　参考情報

(1) 政府情報システムにおけるクラウドサービスの利用に係る基本方針,
政府 CIO ポータル 標準ガイドライン群,
https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf
(2) Office 365 のネットワークトラブル撲滅法, 日経 XTECH,
https://active.nikkeibp.co.jp/atclact/active/17/062200310/
(3) クラウドサービスのトラフィック最適化, TechTarget ジャパン,
https://techtarget.itmedia.co.jp/tt/news/2001/17/news05.html
(4) Office 365 の NAT サポート, Microsoft 社ドキュメント,
https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/nat-support-with-microsoft-365?view=o365-worldwide
(5) Office 365 のネットワークと移行の計画, Microsoft 社ドキュメント,

https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/network-and-migration-planning?view=o365-worldwide

(6) Office 365 IP アドレスと URL の Web サービス, Microsoft 社ドキュメント, https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/microsoft-365-ip-web-service?view=o365-worldwide

(7) Office 365 URL 及び IP アドレス範囲, Microsoft 社ドキュメント, https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

(8) Microsoft Teams 用に組織のネットワークを準備する, Microsoft 社ドキュメント, https://docs.microsoft.com/ja-jp/microsoftteams/prepare-network

(9) Bandwidth Planning in your Cisco Webex Meetings Environment White Paper, Cisco 社ドキュメント, https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meetings/white_paper_c11-691351.html

(10) System requirements for Windows, macOS, and Linux, Zoom 社ドキュメント, https://support.zoom.us/hc/en-us/articles/201362023-System-requirements-for-Windows-macOS-and-Linux

(11) Meet のネットワーク、音声、動画に関する問題のトラブルシューティング, Google 社ドキュメント, https://support.google.com/a/answer/7582554?hl=ja#zippy=

(12) 政府情報システムにおけるゼロトラスト適用に向けた考え方, 政府 CIO ポータル ディスカッションペーパー, https://cio.go.jp/dp2020_03

(13) Zero Trust Architecture, NIST SP800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final

(14) DNS Security Introduction and Requirements, IETF RFC 4033, https://tools.ietf.org/html/rfc4033

(15) Specification for DNS over Transport Layer Security (TLS), IETF RFC 7858, https://tools.ietf.org/html/rfc7858

(16) DNS Queries over HTTPS (DoH), IETF RFC 8484, https://tools.ietf.org/html/rfc8484