トピックス

安全かつ積極的なクラウド利用に向けて
―CASBによるクラウド利用の可視化と統制―

クラウドサービスの利用は年々拡大している。一方で、クラウドサービスの不適切な利用により、業務データの流出などが懸念される事態も起きている。安全にクラウドサービスを利用するには、適切な統制が必要となる。そうした統制に有効なものの1つとして、クラウドサービスの利用を可視化、制御するツール「CASB」を紹介する。

NRIセキュアテクノロジーズ DXセキュリティ事業本部
セキュリティインテグレーション一部 セキュリティエンジニア
下山（しもやま） 洋一（よういち）
専門はサイバーセキュリティソリューションの導入・保守・運用

クラウドサービス利用の拡大

総務省の平成30年度版情報通信白書によると、社内で一部でもクラウドサービスを利用している企業の割合は2017年に56.9％となっており、すでに企業の過半数がクラウドサービスを利用している。この割合は2013年の33.1％、2016年の46.9％から大幅に増加しており、今後もクラウドサービスの利用は拡大が予想される。

クラウドサービスが提供され始めた頃は、運用におけるセキュリティに不安を感じる企業も多く、積極的に利用する企業は少なかった。また、情報を守る観点から、社内からのアクセスができないように、URLフィルタリングによるアクセス遮断なども行われていた。

しかし、クラウドサービスの利便性や安全性が認められたことで、社内の一部や取引先が業務で利用することが増え始めた。それにより、利用を禁止していては業務に支障をきたす場面が多くなり、アクセスを許可する企業が増えてきている。

既存のセキュリティツールでのアクセス管理の難しさ

ここで課題となったのが、クラウドサービスへのアクセス管理である。利用を許可するサービスと、禁止するサービスに分けてアクセスを管理しようにも、従来のURLフィルタリングだけではアクセス制御が困難であるため、必要なサービスまで遮断してしまうなど、制御しきれていないケースである。また、情報システム担当者が把握していないクラウドサービスを業務に利用する「シャドーIT」も発生している。このシャドーITは、これまでは社内で利用の統制ができていた業務データが、クラウドサービスを通じて外部へ流出する可能性があり、情報システムの管理やコンプライアンスの点からも好ましくない。

従来行われていた、URLフィルタリングによるクラウド利用制御では、URLベースでWebサイトやクラウドサービスを識別している。この方法では、多くの場合、「Webメール」や「クラウドストレージサービス」

といったカテゴリごとにアクセス制御を行っている。そのため、例えば「Webメール」カテゴリの中のMicrosoft Exchange Onlineのみ許可し、他のWebメールは遮断するといったことができないケースが多い。回避策として、クラウドサービスのURLを個別にホワイトリストへ登録する方法もあるが、クラウドサービスは、その性質上、ドメインやURLが予告なく頻繁に変化する。そのため、ホワイトリストの更新を間に合わせるのは容易ではなく、URLフィルタリングでの運用は、事実上困難である。

加えて、同一のクラウドサービスを法人でも個人でも利用できる場合、URLベースでは利用者を区別できないことが多い。例えばクラウドのストレージサービスを法人として契約している場合、社内から法人アカウントではログインさせるが、個人アカウントではログインできないようにしたいといった場合がある。しかし、URLベースでは、個人アカウントによるログインを、法人アカウントによるログインと区別して遮断することができない。こうしたケースでは、誤って別のアカウントでログインしてしまったり、個人アカウントによって業務データが持ち出されたりといったリスクを避けられない。

またアクセス制御設定のミスなどで、ユーザーが意図せず、クラウド上のデータに第三者がアクセス可能な状態にしてしまうこともある。そのため、情報漏えいにつながるインシデントも、多数発生している。

また他にも、社内のユーザーから利用申請があったクラウドサービスについて、そのサービスを許可してよいかどうかの調査や判断を行うことは非常に難しい。利用許可の判断を行うにあたって、それがどのようなサービスであるかだけではなく、サービス提供者が信頼できるか、通信やデータは暗号化されているか、適切な運用がされているかなどを調査することが望ましいが、これには非常に時間と手間がかかる上、詳細は非開示であるとして必要な情報が入手できないこともある。

クラウド時代のセキュリティ対策

こうした問題に対処するには、これまでのセキュリティ対策では不十分である。そこで必要とされるのは、以下の3つの機能である。

①ユーザーによるクラウドサービスの利用状況を、詳細に把握できる機能
②ユーザーによるクラウドサービスの利用を、細かく制御できる機能
③クラウドサービス自体の設定を、適切に制御できる機能

これらの要件を、既存のセキュリティ対策製品は満たしていない。そこで、米国の調査会社であるGartner社が提唱したのが、CASB（Cloud Access Security Broker）という考え方である。

CASBの考え方にのっとったセキュリティ製品では、ユーザーとクラウドサービスの間に単一のコントロールポイントを設け、認証やサインオン、アクセス制御といった管理を行う。また、利用するサービスごとに異なるセキュリティポリシーの適用や、ログの取得によって、クラウドサービス利用の可視化、

制御を行う。これらの機能を有するツールや製品群が、CASBと呼ばれている。

安全なクラウドサービスの利用に寄与するCASB製品の機能

CASB製品が持つ、クラウドサービスを安全に利用するための機能を紹介する。

(1) ログ解析

主にWebプロキシやファイアウオール（FW）のログを解析し、クラウドサービスの利用状況を可視化する。従来型のURLフィルタリングでは、カテゴリごとに識別していたが、CASBではクラウドサービスごとに識別することが可能である。これにより、クラウドサービスごとの利用状況を詳細に把握できる。また、アクセスが検知されたクラウドサービスについて、その種類や、利用における潜在的なリスクについての調査結果を提供している。これにより、不適切なシャドーITの利用がないかどうか、容易に確認することができる。

また、社内のユーザーから利用申請があったクラウドサービスについても、許可しても問題がないかを適切に判断することが容易となる。

(2) プロキシ連携によるアクセス制御

クラウドサービスへのアクセス経路にWebプロキシとして介在し、クラウドサービスの利用をリアルタイムで制御できる。未契約のクラウドサービスや、API（Application Programming Interface）を提供していないクラウドサービスに対しても制御できるため、自社での利用を許可していないクラウドサービスへのアクセスもコントロールできる。

また、従来のURL フィルタリングや次世代ファイアウオールと異なり、クラウドサービスごとに利用可否の設定や、同じクラウドサービスでも自社の企業ID のみログインを許可するといったログインIDによる制御が可能となる。加えて、特定の端末からのみアクセスを許可する、ダウンロードのみ許可するなど、操作やデータなどによる細かな設定で利用を制御できる。

これにより、ログ解析で検知した不適切なシャドーIT へのアクセスを遮断することが可能となる。前述のクラウドサービスに関する情報と連携し、一定基準以下のクラウドサービスへのアクセスを遮断することもできる。また、利用を許可しているクラウドサービスであっても、誰がどのような操作を行ったかのログを残せるので、情報漏えいにつながるような不適切な利用もチェックでき、ガバナンスを効かせることができる。（表1参照）

この機能を利用して、リモートワークなど、社外からの利用においても、クラウドサービスの利用を監査し、セキュリティを担保できる。

(3) API連携機能

クラウドサービスが提供するAPIを利用し、クラウドサービス上の設定やデータを制御できる。複数のクラウドサービスに対し、統一の利用ポリシーをCASBで定義し、ポリシーに違反している設定がないかどうか、複数のクラウドサービスに対して横断的にチェックできる。これにより、利用しているクラウド

サービスのセキュリティ設定レベルを、自動的に一定以上に保つことができる。利用を許可したクラウドサービスであっても、サービスごとの詳細な設定は利用申請したユーザーが実施するケースもあるが、誤って第三者にクラウドサービス上のデータ公開してしまうようなインシデントを防げる。また、マイナンバーやクレジットカード番号など機密情報を含むデータや、マルウェアに感染しているファイルを、クラウドサービス上で横断的に検索し、隔離したり削除したりすることで、情報漏えいのリスクを軽減することもできる。プロキシ連携によるアクセス制御と異なり、すでにクラウドサービス上にアップロードされているファイルやデータに対しても、あとから新しい検査ルールを作成することで対応が可能だ。

表1　従来製品とCASBの制御可能範囲の違い

制御可能範囲	URLフィルタ	次世代FW	CASB
URL	○	○	△
サービス	–	○	○
ID	–	–	○
操作	–	–	○
データ	–	–	○

CASBは従来のギャップを制御可能

CASB製品導入の流れ

CASB製品の利用にあたっては、利用する機能によっていくつかの導入パターンがある。最も一般的な流れとしては、まずはログ解析機能を利用して自社のクラウドサービス利用状況を把握し、その上で制御ポリシーを決めてからプロキシ連携によるアクセス制御を実施する。

また、利用許可している特定のクラウドサービスに対しての制御がメインであれば、そのクラウドサービスだけ制御するよう設定して利用を開始し、それ以外についてはログを取得しておくことで、後からシャドーITに対する制御を行うことができる。また、ログが取得されていることから、例えば利用していたクラウドサービスでインシデントがあった場合であっても、その利用状況を速やかに把握し、影響の度合いを判断することも可能である。

クラウド時代の情報セキュリティに必須のCASB製品

CASB製品の導入により、セキュリティを保ちながら、クラウドサービスを利用できるようになる。情報システム担当者は、複数のクラウドサービスを一括管理できることで、ユーザーからの利用申請に対してもスピーディーな対応が可能になる。

今後、企業におけるクラウドサービスの利用はますます増加していくだろう。積極的なクラウドサービスの利用は、新たなサービスやプロダクトの提供に寄与する。しかし、セキュリティや安全性が犠牲になることがあってはならない。安全性を確保しながらクラウドサービスのメリットを享受するためには、CASB製品は欠かせないものといえる。これからのクラウド時代に必要な情報セキュリティ対策として、導入の検討を強く勧めたい。■