広がるクラウド利用、潜伏するシャドーIT

マルチクラウド時代に適したセキュリティー対策「CASB」とは？

セキュリティーの専門家がクラウド利用を勧めるケースがあります。セキュリティー対策に十分な人材や予算をかけられない場合、自社でサーバーを運用するよりも、SaaSなどのクラウドサービスを利用した方が安全な場合があるためです。一方昨今では、一つの企業がいくつものクラウドサービスを導入・活用したり、部署ごとに異なるクラウドサービスを活用しています。しかし、異なるクラウドサービスのセキュリティーレベルを一定に保ち、管理することは困難であるとの指摘も挙がっています。そこで注目されているのが、複数のクラウドサービスの安全な運用を可能にするソリューション「CASB（Cloud Access Security Broker）」です。

クラウドサービスの混在によって高まるセキュリティーリスクへの対処は？

総務省が公表している「情報通信白書（平成28年度）」によると、クラウドサービスを利用している企業の割合は年々増えています。2015年末の時点で何らかのクラウドサービスを利用している企業は4割を超えて44.6%に達し、金融業界や大企業でもクラウドサービスの導入が進んでいるという傾向が読み取れます。

中でも注目すべきは、より広範囲な用途でクラウドサービスが浸透してきた点でしょう。主な利用サービスの上位には、電子メールやファイル共有・保管のサービスが挙げられるものの、サーバー利用が42.9%、社内情報共有・ポータルが36.8%に達しているように、これまでイントラネット上に構築していたシステムのクラウド化も進んでいます。

一方クラウド利用が広がるにつれて浮上したのが、セキュリティーへの懸念です。代表的な例は、機密ファイルや個人情報の入ったファイル、業務に関係ないファイルがクラウド上に保管されてしまう問題でしょう。

手軽さから利用が拡大しているストレージサービスなどのパブリッククラウドは、自由度が高く便利な故に、公開範囲や共有範囲の設定を誤るなど、ちょっとした操作ミスで公開してはいけないファイルが共有されてしまうこともあります。さらにマルウェアに感染したファイルをクラウドにアップロードしてしまい、社内、社外で共有などすれば、感染被害を広げてしまうことにつながります。

クラウドの活用においては、「シャドーIT」対策も必要です。シャドーITとは、情報システム部の関与しない形で勝手にIT機器やクラウドサービスが業務に利用されることで、ガバナンスやセキュリティーの面から問題視されています。

適切に管理されていない個人所有の端末で、会社のクラウドやパブリッククラウドサービスに業務利用で接続すれば、会社の情報などが個人端末に保存され、情報漏えいなどのリスクが高まります。しかし、BYOD（Bring Your Own Device：個人所有のデバイスを業務に利用すること）が注目されていたように、近年のワークスタイルの多様化を考えると一概に禁止しにくい面もあり、セキュリティーをどのように担保するかは大きな課題でした。

マルチクラウド時代に適したセキュリティー対策「CASB」とは？

さらにパソコン、スマートフォン、タブレットというように利用端末の台数や種類が増えれば、社員が使うクラウドサービスやアプリの管理が行き届かなくなりがちです。またいろいろな種類の端末からクラウドサービスを利用する状況になれば、クラウドサービスやアプリの管理の負担もそれだけ重くのしかかるでしょう。アプリ管理やデバイス管理のソリューションはありますが、ソフトウェア資産を把握できていないと、脆弱（ぜいじゃく）性の管理、インシデント発生時の対処、原因究明が困難になります。

なにより問題なのは、クラウドサービスやアプリごとに「セキュリティーレベル」や「サービスレベル」が一定ではないため、企業として統一したセキュリティーポリシーの徹底が難しい状況が生まれることです。

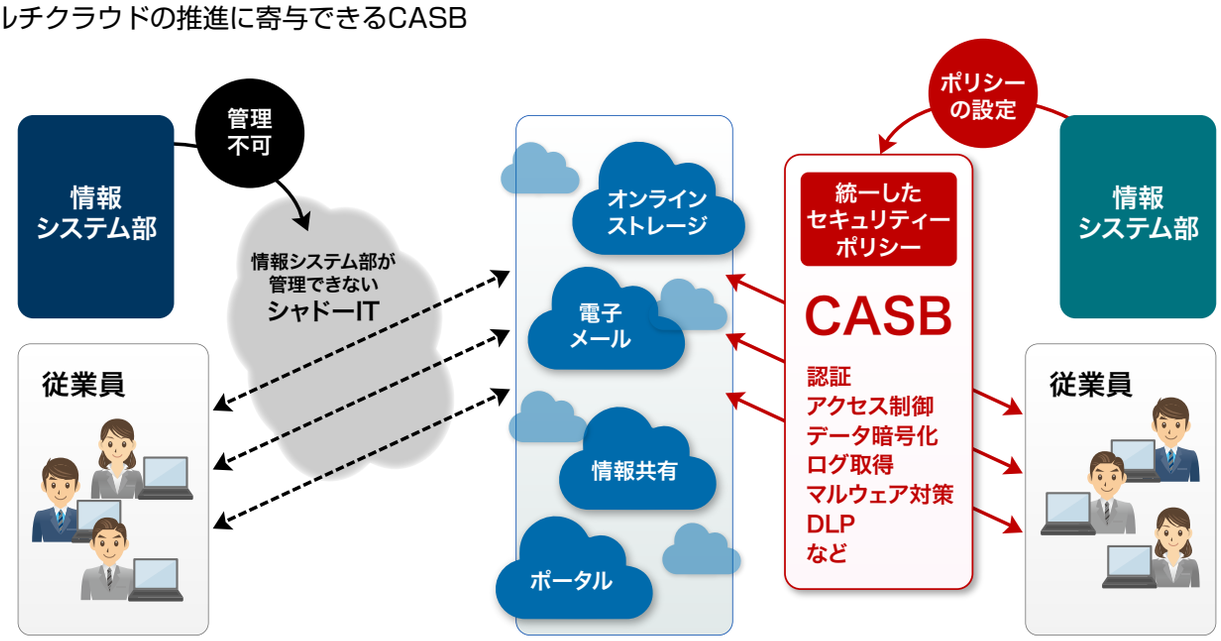
企業におけるクラウド利用において、ガバナンスと利便性の両立は最大の課題といえます。特に異なるセキュリティーポリシーのサービスが併用された場合、セキュリティーの強度はもっとも脆弱なポイントのレベルに押し下げられてしまいます。つまり、せっかくセキュリティー対策に投資をしても、安易なクラウド利用によって台無しにされてしまうかもしれないのです。

複数のクラウドサービスに統一したセキュリティーポリシーを適用できる「CASB」とは

クラウド利用に伴う課題において、主にマルチクラウドのセキュリティーポリシー対策、シャドーIT問題として注目されているのが「CASB（Cloud Access Security Broker）」です。複数のクラウドサービスに対して、一定のセキュリティーポリシーを適用できるソリューションで、ガートナーが2012年にその概念を提唱したことで、海外では広く知られるようになりました。

具体的には、企業が導入、活用している複数のクラウドサービスに対して、「認証／シングルサインオン」や「アクセス制御」、「データ暗号化」、「ログ取得」、「マルウェア対策」「DLP（Data Loss Prevention：情報漏えい対策）」など、自社が必要と考えるセキュリティーポリシーを一律に適用するサービス、ソリューションのことです。

図1：マルチクラウドの推進に寄与できるCASB



CASBを利用することで複数のクラウドサービスに対してセキュリティーポリシーを一律で適用できる
（図の右側はゲートウェイ型のCASBの一例）

CASBの提供形態は、クラウドサービスとユーザーの端末の間に入るゲートウェイサーバー（プロキシ型）、パブリッククラウドをAPI経由で管理するAPIサーバー（API型）、パソコンなどの端末にインストールするエージェント（エージェント型）などがあります。

CASBの考え方自体は新しいものではありませんが、ビジネスでのクラウド利用が一般化するにつれ、CASBへのニーズも高まり、2016年ごろから国内市場向けにCASBソリューションが投入されるニュースを目にするようになりました。2016年にはガートナーが「情報セキュリティ・テクノロジ トップ10」を発表していますが、そのなかでCASBは重要技術の筆頭に挙げられました。

グローバルにおけるCASB市場は急成長しており、欧米を中心にCASBへ参入するベンダーも増加しています。主だったセキュリティーベンダー、アプライアンスベンダーもCASBソリューションを用意しています。

従来は、会社でクラウドサービスを利用する際、セキュリティーポリシーに準拠した利用を実現するために新たなセキュリティー機能を追加したり、ポリシーに合わないサービスを排除したりするなど、システム側での対応を必要としていました。しかし、CASBを導入して、統一したセキュリティーポリシーを担保する方が現実的な対策ではないかという認識も徐々に広がっています。

特にシャドーITの問題は、ポリシーで禁止したとしても、強制することが難しいのが現状です。ポリシー違反をするユーザーがたとえ一部の例外であっても、そのわずかな見落としが重大なセキュリティーインシデントを引き起こすケースもあります。「わが社ではクラウド利用そのものを禁止しているから……」では、組織を守れない現実を認識すべきでしょう。

CASBの中核をなす四つの機能

製品やサービスごとに機能は異なりますが、CASBを構成する機能の主な柱は「可視化」「コンプライアンス」「データセキュリティー」「脅威防御」の四つとされています。

図2：CASBを構成する機能

可視化	CASBを介したアクセスのログ、既存システムのログを管理することで、誰がどのようなクラウドサービスを使ったのか、扱ったデータは何か、といったトラッキングを行います。SaaS型クラウドサービスのAPIを使ってトラッキングを行う製品もあれば、ファイアウォール、ゲートウェイやプロキシサーバーのログなどを活用する製品もあります。
コンプライアンス	セキュリティーポリシーの運用基準を満たすようにアクセスを制御したり、不正な運用、コンプライアンス違反を検知、防止したりします。保存するファイルのコンプライアンス適合性、ユーザーや管理者の監査、利用しているクラウドサービスそのもののセキュリティー要件のチェック、リスク評価なども行います。
データセキュリティー	アクセス制御技術、暗号化技術、認証技術によりデータを保護します。アカウントやグループベースの制御のほか、データやファイルの種類による制御、デバイスや接続ネットワークなどにより制御します。アクセス制御では、2段階認証のような認証、データの暗号化やトークン化（情報マスキング）を行える製品もあります。
脅威防御	一般にクラウドサービス側では、「データ」や「操作」が危険を伴うかの判断ができません。例えば、機密データを含むファイルがアップロードされても、クラウドサービス側で「これは機密データである」という判断はできません。しかしCASBを利用することで、重要データの流出防止のほか、マルウェアの検出、振る舞い分析などの実行、不審な操作の制御、ログ機能と連動した脅威分析機能を利用できます。

CASBはサービスやソリューションによって機能に差がありますが、「従業員がどのようなクラウドサービスを利用し、どのようなデータを預けようとしているのか」、さらに「どのような操作を行い、その中に不正なファイルがないか」「暗号化などの対策は万全か」といった状況の把握、管理が可能となります。サービスやセキュリティーのレベル、機能に差があるクラウドサービスを、一定のポリシーのもと、統合的に管理できる点も特徴の一つといえるでしょう。

セキュリティー管理者、CIOから見ても、サービスやデバイスごとに細かい設定をしたり、運用ルールを実施させることに頭を悩ませず、複数のクラウドサービスをまとめて管理できるメリットがあります。管理しきれずに、やむなく使用禁止としていたクラウドサービスの利用が可能になれば、従業員による勝手な利用、個人アカウントで契約しているクラウドサービスを業務に利用する「野良アカウント」の防止にもつながります。

マルチクラウドが広がる国内企業。セキュリティーを担保するCASBは大きな選択肢に

国内企業でも業務に「Dropbox」「OneDrive」「iCloud」などを利用するところが増えています。「Office 365」「G Suite」などのSaaS型グループウェアも一般的となりつつあります。また電子メールは、フィッシングや標的型攻撃メールといった問題から、そもそもビジネス環境での利用を見直す企業も現れはじめました。重要データはメールを使わず、ビジネス向けのファイル転送サービスやセキュアな共有ストレージを利用するという運用です。従業員間のコミュニケーションには、メールからビジネスチャットへとシフトする動きも活発化しています。

スマートフォンやタブレットもビジネスの現場に徐々に浸透しはじめています。しかしデバイス側のリソース（ストレージ容量やCPUパワー）が貧弱、かつセキュリティーを担保するため、クラウドサービス利用を前提としているといってもよいでしょう。クラウド上でデータを扱えば、余分なデータはモバイルデバイス上に残さないで済みます。

以上のような状況を踏まえると、企業において複数のクラウドサービスを利用するマルチクラウドが本格化するのは避けられそうにありません。一定のセキュリティーレベルを保ちつつ、業務をこなすことが難しくなります。

情報システム部やセキュリティー担当者が、さまざまなクラウドサービスを把握し、自社ポリシーに合致したサービスやアプリを選定し、正しい設定を徹底させるには限界があります。ガバナンス、コンプライアンスの統合管理、そして従業員の業務効率を整合させてマルチクラウド環境を利用するため、CASBに対するニーズはますます増加しそうです。

CASBを検討する際は、利用したいクラウドサービスに対応しているか、制御できる範囲が自社ポリシーをカバーできるか、必要なログも保管しているか、といったポイントを抑えておくとよいでしょう。

もちろん、現場からのニーズがあっても、セキュリティーポリシーを維持できなければ、利用を禁止、制限せざる得ないクラウドサービスが出てくる可能性もあります。その場合は、全体の利便性と安全性について従業員など現場とのコミュニケーションが大切となります。

今後利用が増大する企業のクラウド活用。安全かつ効率的に利用するため、ぜひCASBに注目してみてください。

【 制作／コンテンツブレイン 】

NTTコムウェア株式会社
URL：http://www.nttcom.co.jp/

WEB 掲載：2017.4