中小企業のクラウド利用

5つの
セキュリティリスクと
その対策

手軽な導入やスモールスタートが可能なITシステムの提供形態として、
クラウドサービスが脚光を集めています。特に中小企業では、
そのメリットをより活かしやすく、ビジネスへの大きな支えとなります。
一方で、クラウドサービスを利用するにあたっては、さまざまな
注意点があります。特にセキュリティに対する不備や認識不足は重大な
リスクを招くおそれがあるため、しっかり考慮した上で適切な対策を
施しておく必要があります。

いまや「事業継続」に欠かせないツールに

クラウドサービスが不可欠である理由

近年頻発する自然災害、また大規模な感染症による事業への影響は大きく、またそれはしばしば長期間に及びます。こうした不測の事態に備えるため、場所やデバイスを問わずに利用できるクラウドサービスは非常に効果的なツールとなります。

これまでクラウドサービスといえば、「社内にサーバーなどの設備を用意することなく導入できる」、「運用管理の手間がかからない」、「ユーザーの人数や利用頻度に応じた料金で利用できる」、「常に最新バージョンの機能を利用できる」など、どちらかといえば導入や運用の容易さなどのメリットが重視されてきました。しかし、いまやクラウドサービスは、企業の事業継続に欠かせない環境として注目されるようになっています。

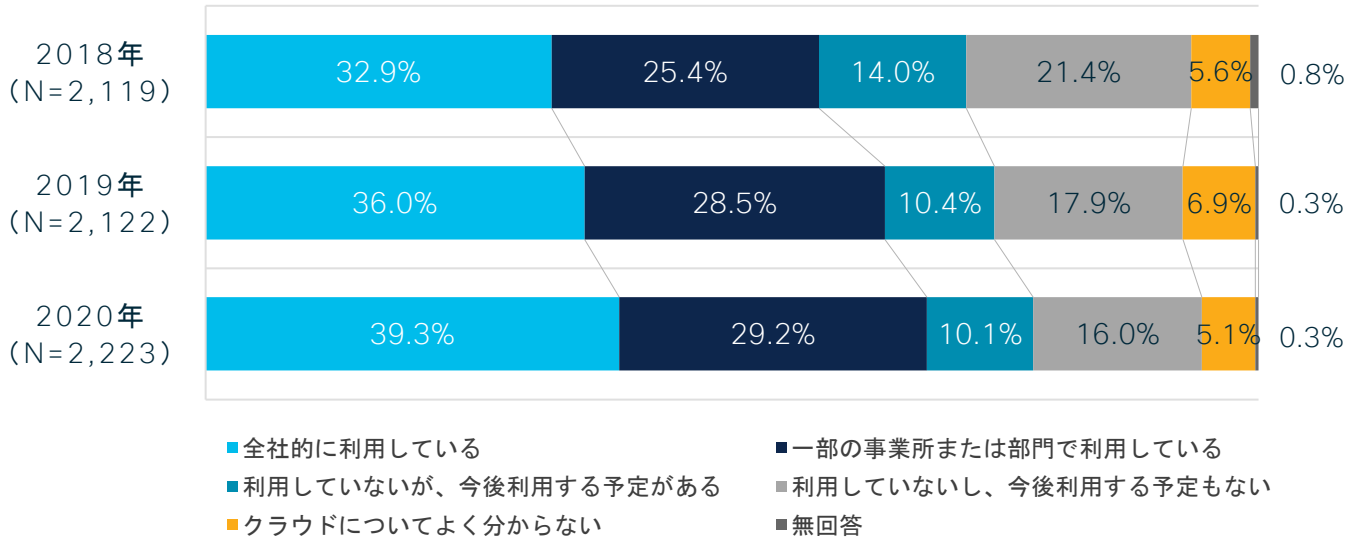
クラウドサービス利用は増加傾向

実際にどのようなクラウドサービスが利用されているのでしょうか。コミュニケーション系では、チャットツールやグループウェアのほか、在宅勤務の普及でWeb会議の利用が急拡大しました。バックオフィス系では会計や労務/勤怠管理ほか、電子契約の利用も拡大しつつあります。また営業系では、顧客管理（CRM）や営業支援（SFA）、名刺管理などが広く使われています。

クラウドサービスを利用する企業の割合は年々増加しており、総務省の「令和2年通信利用動向調査報告書（企業編）」によると、「全社的に利用している」企業の割合は39.3%、「一部の事業所または部門で利用している」は 29.2%となっています。つまり60%近くの企業がクラウドサービスを利用していることがわかります。

これら2つの回答項目は、以下の図が示すようにいずれも2018年から増加の傾向を示しており、クラウドサービス利用に対する意欲は確実に高まっているといえるでしょう。

クラウドサービスの利用状況



出典：総務省「令和2年通信利用動向調査報告書（企業編）」

クラウドサービス利用の課題

利用実態の把握や不正アクセスのリスクに注意

クラウドサービスはメリットばかりではありません。その裏側にあるデメリットを確実に理解した上で利用することが肝要です。
特に次の3点について注意が必要です。

1. 利用実態を把握できない

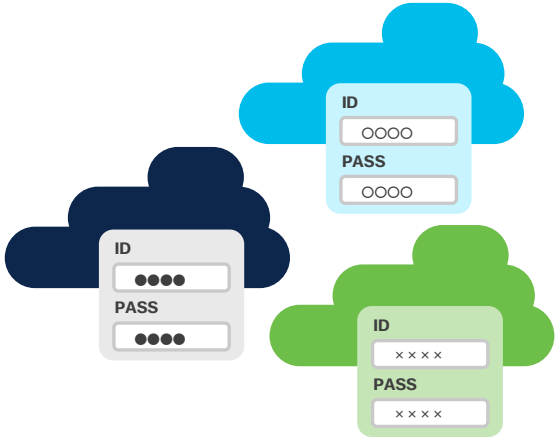
クラウドサービスは、個人所有のパソコンやスマートフォンを含めたさまざまなデバイス、家庭内や公共のインターネット回線を使って、どこからでも利用できるだけに、管理者がその実態を把握することが困難になります。

目の届かないところで従業員が勝手に判断し、ファイル共有サービスなどのクラウドサービスを業務利用するといったシャドーITが蔓延する場合もあります。こうした状態を放置しておくとガバナンスの低下につながり、企業全体の大きなリスクとなります。

2. アカウントやパスワードの管理が煩雑

クラウドサービスは一般的にアカウントIDとパスワードがあればどこでも使えるようになります。逆に言えばそれらが外部に流出してしまえば、簡単になりすましされてしまいます。

アカウントIDとパスワードは契約しているクラウドサービスごとに必要となるため、利用するクラウドサービスの数が増えれば増えるほど管理が煩雑になります。従業員も自分のアカウントとパスワードを覚えきれず管理がずさんになりやすい問題が起こります。



3. IT資産管理ソフトで管理しきれない

多くの企業は、社内に存在するIT資産の管理のためにすでに「IT資産管理ソフト」を利用しています。従業員のPCやそこにインストールされているソフトウェアを把握し、不正なソフトインストールや不正なデータの持ち出しなどへの監視を行っていました。

しかし、クラウドサービスそのものやクラウドサービス内に保存されるデータは、そうした従来型の仕組みによる管理は通用しなくなり、専用の対策が必要となります。

クラウドサービス利用で生じるセキュリティインシデント

わずかな管理ミスから重大な情報漏えいに

国内企業で相次ぐ情報漏えい事件

クラウドサービスを利用する上で最も注意しなければならないのが情報漏えいです。実際に日本企業においても数多くの情報漏えい事件が起こっています。

最近の例としてある企業では、グループ内の十数万人規模の従業員が利用しているクラウドサービスが不正ログインされ、大量の取引先情報や個人情報が流出しました。

そのほかの企業でも、利用中の営業管理用クラウドサービスが不正アクセスを受け、保管していた最大百数十万件におよぶ個人情報などが流出しました。こちらはクラウドサービスのセキュリティ設定にミスがあったことが原因と見られています。

原因は不正アクセスだけでなく「管理側のミス」も

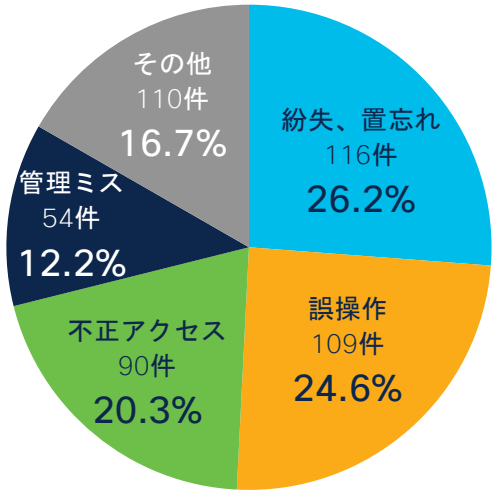
クラウドサービスそのものはITの高度な運用ノウハウをもつ事業者によって厳重に管理されているため、一般的に高い安全性が担保されています。

ただし実際に安全かどうかは、利用者側の管理体制に大きく左右されてしまうことになります。特定非営利活動法人日本ネットワークセキュリティ協会（JNSA)の2018年度の調査によると、実際に情報漏えいは不正アクセスだけではなく、紛失、誤操作、管理ミスなど管理する側の原因によるところが多いことにも注意が必要です。一般的に多くのクラウドサービスは、初期設定状態ではIDとパスワードでアクセスできてしまうため、わずかな管理漏れや設定ミスが重大なセキュリティインシデントにつながります。

たとえばクラウドサービスごとにアクセス権の設定方法やデフォルト設定が異なっているにもかかわらず、その違いを認識しないまま運用を開始すると、誰でも簡単にアクセス可能な状態になってしまう場合があります。

また、システム管理担当者がクラウドサービスは自分たちの責任範囲外という意識をもってしまうと、複雑かつ変化の激しいサイバー攻撃やクラウド特有のリスクへの対応がおろそかになり、セキュリティ上の脆弱性を見逃しがちです。

情報漏えいの原因は、不正アクセスだけでなく、人的ミスによるものも多い



●その他の内訳

盗難	17件	3.8%
設定ミス	16件	3.6%
内部犯罪・内部不正行為	13件	2.9%
不正な情報持ち出し	10件	2.3%
バグ・セキュリティホール	8件	1.8%
目的外使用	3件	0.7%
ワーム・ウイルス	1件	0.2%
その他	6件	1.4%

脆弱な個人端末は「強固な認証」で安全に

無防備な個人端末に要注意

多くのクラウドサービスはデバイスを選ばず利用できますが、前章で触れたように不正アクセスには細心の注意が必要です。特に注意を要するのが、従業員の私物の端末からクラウドサービスへのアクセスを認めている、あるいは見逃しているケースです。プライベート利用を兼ねている個人端末は紛失してしまうリスクもあれば、第三者に触られたり見られたりする可能性もあります。

個人端末には会社支給のPCと同等のセキュリティ対策が施されていないケースもあります。ID・パスワード情報が記憶されてすぐにアクセスしやすい状態になっていたり、ID・パスワード情報がわかりやすいところにメモされていたりすることもしばしば見られます。

多要素認証で本人認証を強化

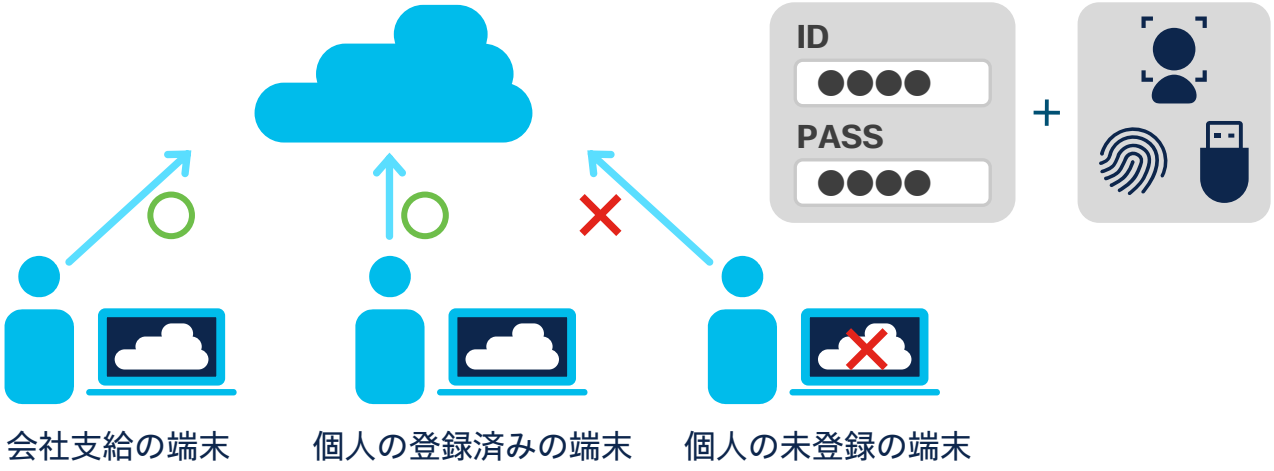
個人端末はもちろん、会社支給の端末を利用している場合であっても、他人によるなりすましを防ぐ最良の方法は、クラウドサービスを利用しようとしているユーザーが「本人」であることをその都度確認し、制御することです。

ここで一般的に用いられるのが、多要素認証という方法です。従来からのアカウントIDとパスワード（記憶情報）に加え、スマートフォンなどのデバイス、専用のハードウェアトークンを用いた「所有物」による認証や、指紋や顔などを用いた「生体認証」など、複数の要素を組み合わせて本人であることを認証することで、自分自身以外からの不正なアクセスを防ぐことができます。

接続デバイスの正当性を確かめる

さらにクラウドサービスにアクセスする端末の検疫も重要です。その端末が会社で認められたものであるか確認するとともに、OS やブラウザのバージョン、アンチウイルスのインストール状況などもチェックし、安全性が確認できない端末に対してはアクセスをブロックします。このように「本人」と「端末」の両面から対策を施すことで、クラウドサービスを利用する際の安全性を高めることができます。

「端末」と「本人」の両面から認証を強化



クラウドのリスクと対策②：IT部門管理外のクラウド利用

信頼できないクラウド利用は必ず可視化

まん延するシャドーITをどう防ぐか

会社が正式に契約したクラウドサービスだけでなく、個人が勝手な判断でクラウドサービスを業務で利用しているケースが散見されます。許可されていないIT利用は一般的に「シャドーIT」と呼ばれており、上司や同僚の目が行き届かないテレワーク環境では、このリスクがより高まっているともいえるでしょう。

こうしたシャドーITとして使われているクラウドサービスの中には、セキュリティ対策が不十分であったり、運用が不安定であったり、会社のセキュリティポリシーにそぐわないものも少なくないだけに注意が必要です。

実際に会社に無断で使用していたある大容量ファイル送信サービスが不正アクセスされ、大量の個人情報が流出するという事件が起こったこともあります。

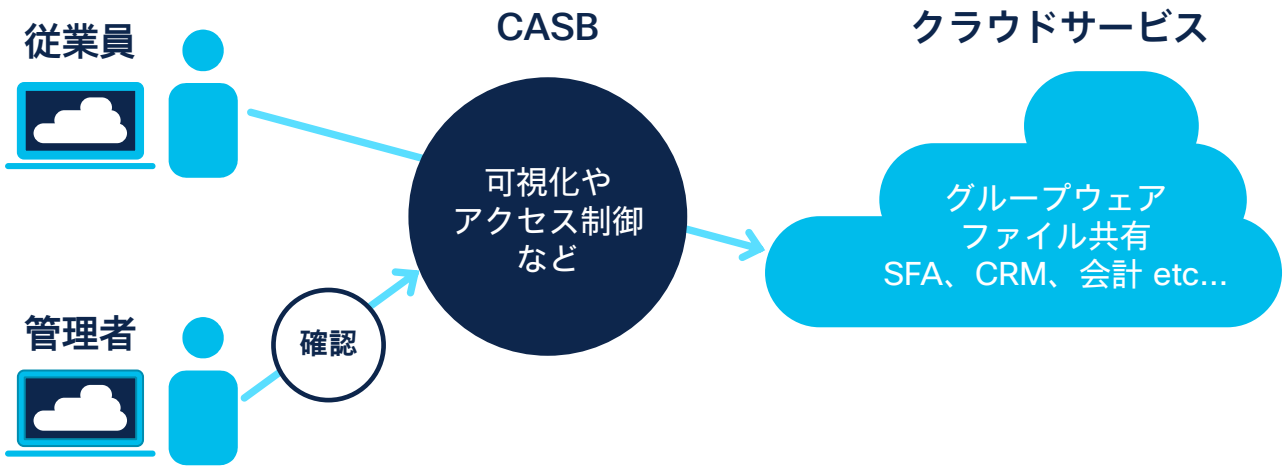
クラウドサービスの利用状況を可視化して制御

シャドーITによるクラウド利用の対策は、あらゆるユーザーのクラウドアクセスを可視化し、認可外のクラウドサービスへのアクセスを管理者へ通知したり、もしくは自動できに制御したりできる仕組みが理想的です。とはいえ多様なクラウドサービスにアクセスするすべてのトラフィックをモニタリングすることは非常に困難で、これまで対策は思うように進んでいませんでした。

そうした中で注目されているのが、CASB（Cloud Access Security Broker）と呼ばれるITツールです。インターネット上に設置されたゲートウェイを通過するトラフィックの中身を分析して集計することで、クラウドサービスの利用状況を効果的に可視化します。

また、発見されたシャドーITを遮断するだけでなく、許可されたクラウドサービスについても、たとえばファイルのアップロードを制限したり、外部への情報公開を禁止したりするなど、きめ細かいポリシー制御を行えるようになります。

従業員のクラウドアクセスを可視化して制御



クラウド上のゲートウェイでアクセスを遮断

不審なサイトによるマルウェアやフィッシングの被害

クラウドサービスに限らず、業務ではさまざまなWebサイトにアクセスする必要があります。中には業務と関係ないサイトへのアクセスするケースもあり、それに伴って故意か否かを問わず不審なサイトへアクセスしてしまうリスクが発生します。

また、フィッシング攻撃と呼ばれるサイバー脅威の手口では、攻撃者が信頼できる企業や組織を装い、メールやインスタント・メッセージを通じて偽装サイトへ誘導します。こうした悪意を持ったWebサイトにアクセスすると、クレジットカード番号やアカウント情報など重要な情報を盗まれるほか、マルウェアを送り込まれる恐れがあります。

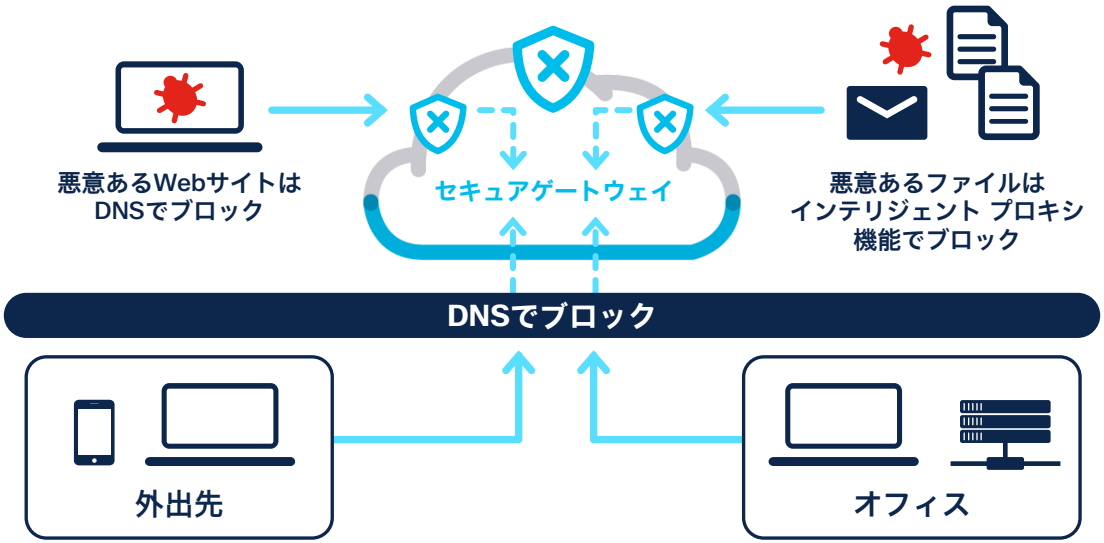
クラウド上の「ゲートウェイ」でアクセスを遮断

不審なWebサイトへのアクセスを防ぐための代表的な手段として、URLフィルタリングによってあらかじめ業務に関係ない不適切なサイトや不審なサイトへアクセスしないように制御する方法があります。この種の機能は企業内に一般的に設置されているファイアウォールやUTMでも備わっていますが、社外の端末から直接インターネットにアクセスするユーザーを保護することはできません。

そこで今後必要となるのが、どの場所からどんな端末でも、インターネットにアクセスする前に、クラウド上にある「セキュアWebゲートウェイ」を経由させて安全を確保する仕組みです。このゲートウェイには、DNSによる名前解決の仕組みを用いてWebサイトの危険度を判定し、より幅広い保護を可能にした「セキュアインターネットゲートウェイ」と呼ばれるものもあります。

もちろん、不審なサイトだけではなく、自社独自のポリシーでアクセスを許可したくないサイトもあるでしょう。そのため多くの製品では、Webサイトのドメインやサイトのコンテンツカテゴリ、特定のWebアプリケーションのアクセスなどさまざまな制御が可能です。

クラウド上の「セキュアゲートウェイ」で不正なサイトを遮断



多要素認証とID管理でなりすましを防止

不正アクセスによる金銭的被害も増大

多くのクラウドサービスは、初期状態ではアカウントIDとパスワードが知られてしまえば、本人以外からの不正アクセスが簡単に行われてしまいます。こうしたなりすましによる不正アクセスは、すぐには発覚しづらいという問題もあります。

ある家電量販店は不正ログインされ、数十万円分のポイントが不正利用されました。また、ある流通業は1000人近いアカウントに不正ログインが発生し、数千万円にも及ぶスマートフォン決済の被害を受けました。同様のなりすましによる不正アクセスは、クラウドサービスでも多発しているのです。

多くのインターネットユーザーはサイト間でパスワードを使いまわすことが多く、サイバー犯罪者は、その性質を利用して、不正に入手したID＆パスワードリストを用いて別のサービスへのログインに使えないかを総当り的に試します。これはいわゆる「パスワードリスト攻撃」と呼ばれています。

「ID&パスワード管理」依存をなくす

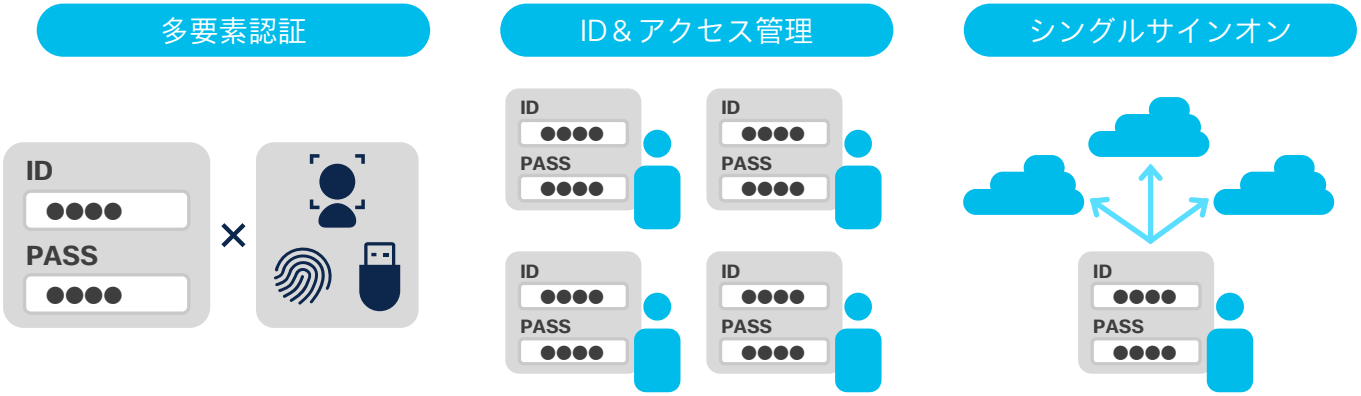
なりすましによる不正アクセスを防ぐ最も効果的な手段の1つが、先にも紹介した多要素認証によるユーザーの本人確認です。ID＆パスワードの組み合わせが外部に流出してしまったとしても、手元のスマートフォンへの認証や生体認証などを組み合わせれば、不正アクセスを防ぐことができます。

もう1つ重要なのが「ID＆アクセス管理」の仕組みを導入することです。適切なアカウントが発行されているか、正しいパスワード設定があらかじめなされているかどうかの確認を行い、不正アクセスの原因をあらかじめ潰しておくことも重要なポイントです。

なお、アカウントやパスワードが外部に漏れてしまう背景には、複数のクラウドサービスを利用するユーザーに煩雑なパスワード管理を任せている（責任を押し付けている）ことも一因となっています。

この課題を解消するのが、1つのID＆パスワードで、どのサービスにもアクセスできる「シングルサインオン」です。従業員のパスワード管理の負担を解消し、ずさんなパスワード管理に陥ることもないため、不正アクセスリスクを大きく低減することができます。

不正アクセスやパスワード管理リスクを防ぐ工夫



信頼できるクラウドサービスかを確認

クラウドサービスごとに安全性・信頼性のレベルに差異がある

主要なクラウドサービスは高い安全性・信頼性を備えていると言われます。オンプレミスでシステムを運用する場合、セキュリティ対策に加え、システムの死活監視やトラフィックの監視、各種ログの管理と保管、サーバールームの入退室管理、さらには建物自体の災害対策や停電対策（UPSや非常用電源）などもすべて自力で行わなければなりません。クラウドサービスを利用すれば、こうしたコストと手間のかかる対策を事業者に任せることができます。

ただし、これはあくまでも総体的な観点からであって、クラウドサービスごとに安全性・信頼性のレベルには差異があることを認識しておく必要があります。

クラウドサービスを評価する第三者認証制度

クラウドサービスを利用する際には、自社のセキュリティポリシーやコンプライアンス要件にあったサービスを選定することが基本となります。

例えばクラウドインフラ側でどんなセキュリティ対策が行われているのか、データを保存するデータセンターはどこにあるのか、データ保護やバックアップはどんな形で行われるのか、ISOやSOCなどの第三者認証を取得しているかどうかは、クラウドサービスごとの差異を見極める特に重要なポイントです。

国としても政府機関などが安全性・信頼性の高いクラウドサービスを導入できるよう、「政府情報システムのためのセキュリティ評価制度」（通称：ISMAP）を立ち上げています。国際標準などを踏まえて策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経てクラウドサービスを登録する制度で、このリストに掲載されている事業者かどうかも今後の大きな判断基準となります。

クラウドサービスに関連したセキュリティ基準や第三者評価制度の例

第三者認証	概要
ISO27017	クラウドサービスの提供や利用に対して適用されるセキュリティの第三者認証
SOC1／SOC2	システム受託会社（クラウドサービス事業者）の内部統制を証明するための制度。SOC1は財務報告に係る内部統制、SOC2はセキュリティ・可用性・処理のインテグリティ・機密保持・プライバシーに関する内部統制を証明する。
CSマーク	日本の特定非営利活動法人日本セキュリティ検査協会(JASA)による情報セキュリティ監査制度。対象は日本に限られる。
CSA STAR	米国の非営利団体Cloud Security Allianceによるセキュリティ成熟度を評価する制度。対象は米国を含む全世界
ISMAP	日本政府によるクラウドシステム調達で一定のセキュリティ基準を満たしたものを認定する制度

中小企業のセキュリティ強化を支援

安全なクラウド利用を支えるシスコのソリューション

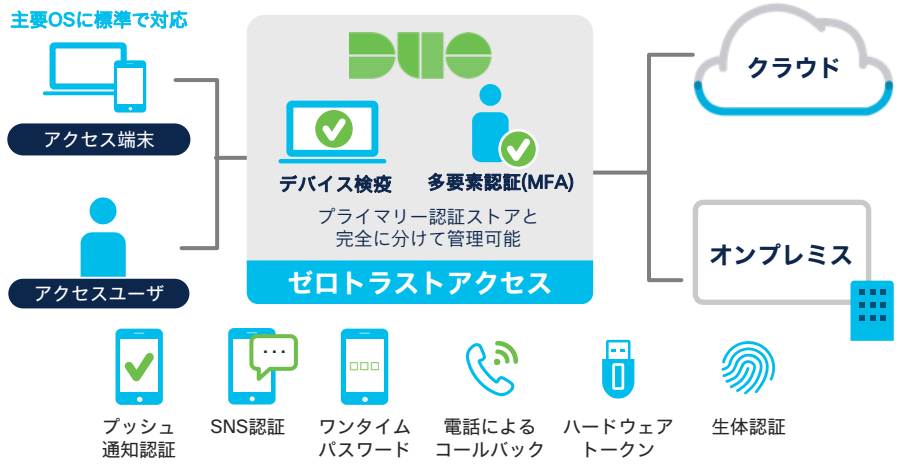
シスコでは、中小規模の企業の皆様が、より安全に多彩なクラウドサービスを利用できるようにするためのセキュリティソリューションを提供しています。

Cisco Secure Access by Duo

ゼロトラストの考え方に基づき、さまざまなクラウドサービスを利用するユーザーとデバイスの信頼性を評価し、安全なアクセスのみを許可するセキュリティサービスです。なりすましによる不正アクセスを防止する多要素認証、従業員が使用している端末のセキュリティ状態を検証するデバイス管理などの機能を提供しています。

例えば、ある企業では、Google Workspace や Box、Salesforceといったクラウドサービスにアクセスする手段としてDuoを活用。これらのクラウドサービスに一括してログインおよび認証を行えるようになったことで、高い安全性のほか、パスワードを忘れてログインができなくなるという業務上の不要なトラブルがなくなっています。

多要素認証とデバイス認証を提供するDuo Security

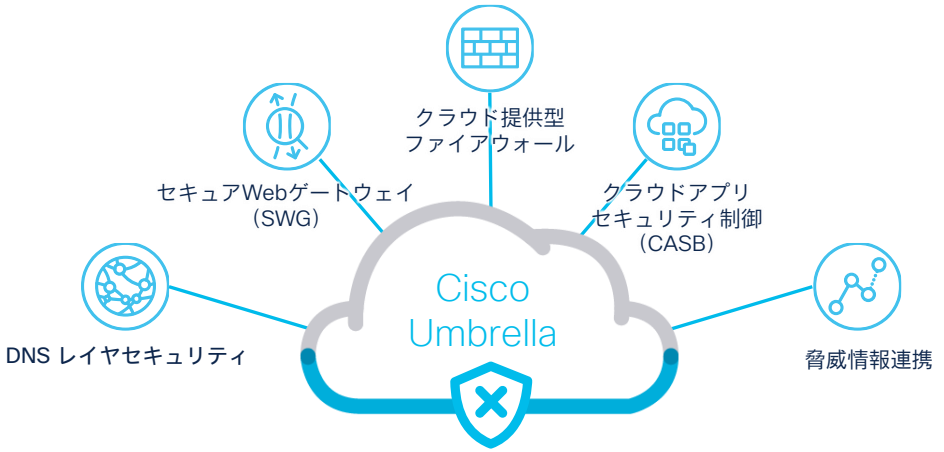


Cisco Umbrella

安全でセキュアなインターネットアクセスを実現するセキュリティソリューションです。クラウドで提供されるため、既存のシステム構成に大きな影響を与えず導入できます。DNS セキュリティ、セキュア Web ゲートウェイ、クラウド提供型ファイアウォール、CASB、サンドボックスなど、幅広いセキュリティ機能を提供します。

例えば、ある自治体の教育委員会は、文部科学省のGIGAスクール構想に基づいた「1人1台端末」「児童生徒の自宅学習環境整備」の実現に向けて配備計画を進める中で、Cisco Umbrellaを採用し、家庭からでも安心してインターネットを利用可能としつつ、危険なサイトや不適切なサイトへの接続をブロックする環境を実現しました。

DNSセキュリティを中心に安全なWebアクセスに必要な対策を網羅



中小企業向けセキュリティはこちらをご覧ください

cisco.com/c/ja_jp/solutions/small-business/cloud/security.html

無料デモ・トライアル・お問い合わせはこちら

cisco.com/c/ja_jp/solutions/small-business/contact.html

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。

製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ

平日10:00-12:00, 13:00-17:00

0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback

©2022 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は2021年12月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

http://www.cisco.com/jp

2289-2112-000-X