

さらに、各クラウドサービスのセキュリティ設定も一括管理できます。サービスごとにセキュリティ設定を確認し、更新することは煩雑で管理負荷が高く、設定ミスや漏れの可能性も高くなります。「Bitglass」を活用することで、クラウド環境のセキュリティポリシー統一も実現できます。また、AIを使ったマルウェア対策として定評のあるCylance®のマルウェア検知機能を採用し、クラウドサービスへアップロードするデータ、またダウンロードするデータにマルウェアが含まれていないかを常に監視する機能も備えています。セキュリティを強化し、クラウドサービスの安全なビジネス活用の実現を支援します。

各デバイスにエージェントソフトをインストールすることなく使うことができるので、導入も容易です。

日立ソリューションズは日本初の「Bitglass」代理店です



Gartnerが発表した「Cloud Access Security BrokersについてのMagic Quadrant」\*2で、リーダーの一社として位置づけられている「Bitglass」。すでに米国では350社100万ユーザー\*3を持つこのサービスの日本初の販売パートナーとして取り扱いを始めたのが日立ソリューションズです。

日立ソリューションズでは、「Microsoft® Office 365™」や「Salesforce」をはじめとする、さまざまなクラウドサービスをお客様に提供してきました。これらのクラウドサービスをより安心してご利用いただけるよう、「Bitglass」をはじめ、さまざまな製品・サービスを組み合わせたクラウド環境をトータルで提供していきます。

クラウドサービス利用時のセキュリティにお悩みの方はもちろんのこと、これからクラウドサービスの導入を検討されている方は、日立ソリューションズにご相談ください。

\*2 出典:Gartner, Magic Quadrant for Cloud Access Security Brokers, Craig Lawson, Steve Riley, 29 October 2018

\*3 2018年10月時点



クラウドサービスの導入を検討されている方、  
クラウドサービス利用時のセキュリティにお悩みの方、  
日立ソリューションズにご相談ください。

クラウドサービスの利用ルール…守られていますか？

次世代CASB Bitglassは  
ユーザー・管理者に負担をかけず  
クラウドサービスの  
セキュアな利用を実現！

利用サービスの  
可視化



利用状況の把握・  
リアルタイム制御



エージェントレスで  
簡単導入



bitglass 日立 検索



www.hitachi-solutions.co.jp/bitglass/

※ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するように助言するものではありません。ガートナー・リサーチの発行物は、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。※BitglassはBitglass, Inc.の米国およびその他の国における商標、または登録商標です。※本資料にはCylance Inc.の著作物が含まれています。※CylanceはCylance Inc.の米国およびその他の国における商標、または登録商標です。※その他、本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記していません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本カタログ中の情報は、カタログ作成時点のものです。

株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp



本カタログ掲載商品・サービスの詳細情報

www.hitachi-solutions.co.jp/column/shion/vol18/

IT探偵 しおんが解決!  
企業潜入調査物語

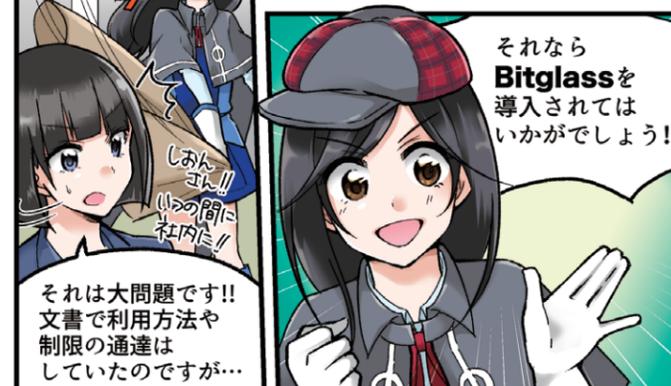
クラウドを安全にビジネス活用！次世代CASBでシャドーITを防げ！

プロローグ

都内某所に、ITを駆使して企業の悩みに解決するという、特別な探偵事務所がある。そこで働くエリートIT探偵の「伊野部しおん」は、企業が悩むセキュリティや業務効率化の課題を次々と調査・解決していく。

伊野部 しおん

IT探偵事務所に勤めるエリート探偵。3年前までは某企業のスーパーエンジニアだったらしい。依頼先の関係者に変装をして、ITの課題を探し出して解決していく変装調査型の仕事を得意とする。



登場人物

うつつた みらい  
宇津下 未来

情報システム部のホープとして1年前に入社。セキュリティ意識が高く知識・技術ともに部長を上回るとの噂。自立心が強いせいか恋愛関係も年下と付き合うことが多い。



そりゅう よしお  
曾柳 好男

IT探偵事務所所長兼取締役を務める社長。さまざまな企業に監査などの内部調査を依頼され、しおんを送り込んで企業課題を解決させている。





### IT探偵しおんが解決!

働き方改革の推進や、運用管理コストの最適化が求められる今、さまざまな業務システムにおいて、SaaSをはじめとするクラウドサービスの活用が広がりつつあります。クラウドサービスは導入が容易にできる一方で、従業員が会社で管理・契約していないIT機器やサービスを勝手に利用する「シャドーIT」が新たなセキュリティリスクとなっています。日立ソリューションズが提供する、次世代CASB（キャスビー：Cloud Access Security Broker）「Bitglass」は、このようなシャドーITを見える化、さらにクラウドサービス利用状況の可視化やリアルタイムでの制御を行うことで、安全なクラウドサービス活用の実現を支援します。

## 「シャドーIT」が会社の新たなセキュリティリスクに

クラウドサービスは場所を問わず利用できることもあり、在宅勤務や社外での空き時間を活用したテレワークなど、働き方改革を推進するインフラとして活用が広がりつつあります。また、社内にサーバーを設置する必要がなくなるので、運用管理の面からメリットを感じて導入する企業も少なくありません。

一方、このようなクラウドサービスは、部門や個人が簡単に使い始めることができるため、「シャドーIT」が増える原因にもなっています。

一般的に、クラウドサービスはセキュリティにも配慮された設計になっていますが、ユーザーの使い方によっては、情報漏洩が発生してしまうこともあります。例えばクラウドストレージサービスは社外にファイル共有する手段としてよく使われますが、適切なアクセス設定をしないと、意図せず社内情報が誰でもアクセスできる状態になってしまい、その結果、事業に大きな影響が出てしまった、ということも起こり始めています。

また、許可されていない私物デバイスから会社で契約しているクラウドサービスを利用することにより、私物デバイスへの重要情報持ち出しができてしまいます。万が一、その私物デバイスがマルウェアに感染していたりすると、情報が漏洩してしまうという危険性もあります。

クラウドサービスの普及とともに、「シャドーIT」は新しいセキュリティリスクとして見過ごせない状況になりつつあります。



## 見えなかった「シャドーIT」を可視化する「CASB（キャスビー）」

見えにくいシャドーITを可視化するのが「CASB（キャスビー）」です。CASBはファイアウォールのログなどから、ネットワーク上を流れるクラウドサービスの通信を抽出、どのようなクラウドサービスがどう使われているかを可視化することで、無断で使われているクラウドサービスを検知します。

このようにCASBは、これまで困難とされていたクラウドサービス利用の監視を強化し、管理の強化やセキュリティリスクの低減を実現できます。

クラウドサービスの可視化という点では大きな力を発揮するCASBですが、詳細な利用状況の把握や、クラウドサービスの制御を行うことができないものも多々あります。また、制御ができて、CASB単体ではなく、他のシステムと組み合わせることで実現するという形であり、特にリアルタイムでの制御は課題となっています。



## 次世代CASB「Bitglass」でクラウドサービスの管理をさらに強化

そこで、シャドーITの可視化、クラウドサービスの利用状況把握・リアルタイムでの制御を1つのサービスで実現する次世代CASBとして登場したのが「Bitglass」です。

「Bitglass」は爆発的に数を増やすクラウドサービスに対応するため、AIを新サービスの検知に活用。収集したクラウドサービスの情報を機械学習によって日々学習し、判別できるクラウドサービスの数は約67万\*1にものぼります。

また、会社で契約しているクラウドサービスを誰がどのように利用しているかなどの利用状況の把握や、クラウドサービスの利用を社内ネットワークのみに限定するなど利用時の制御を行うことも可能です。

\*1 2019年4月時点

