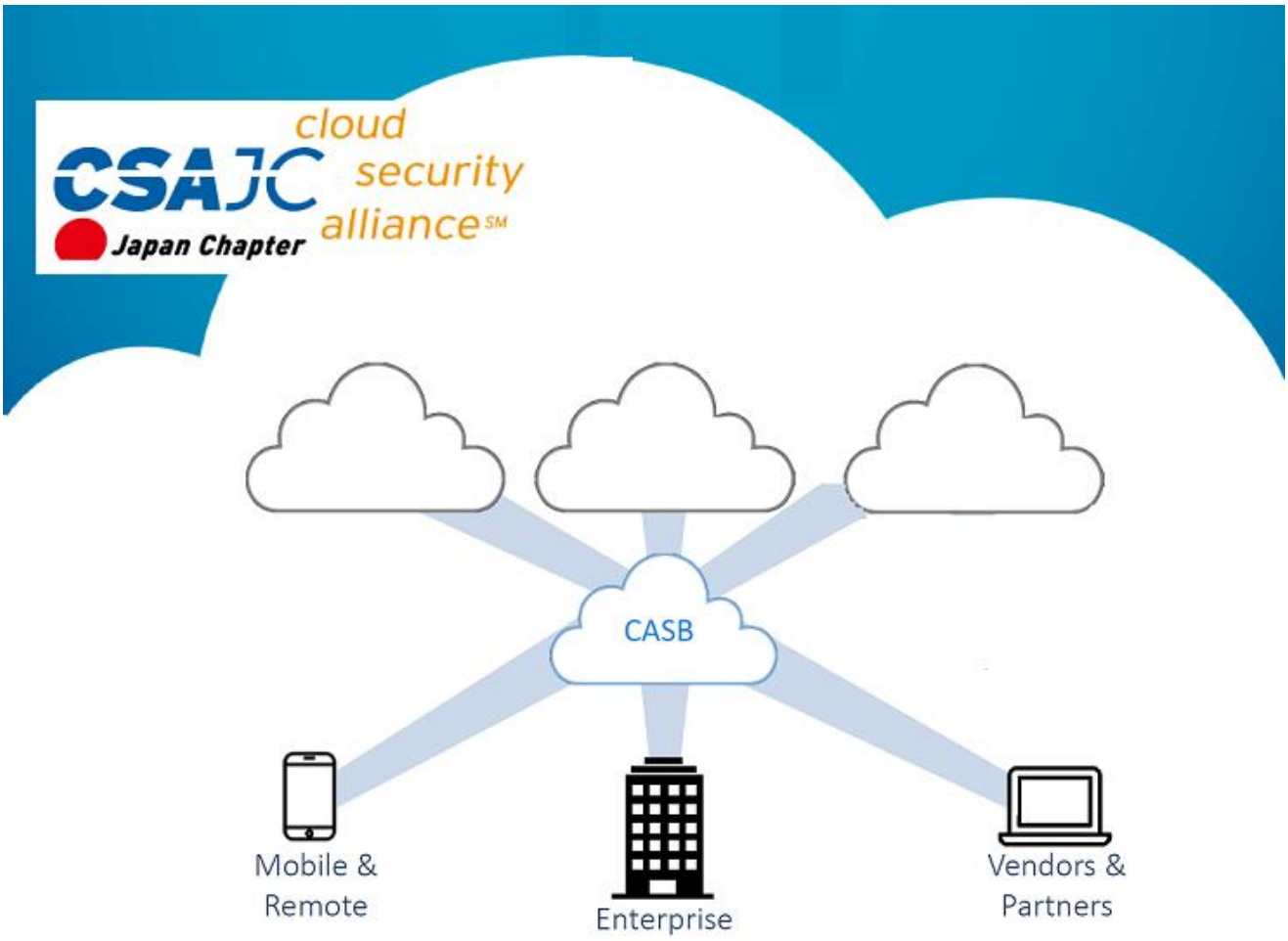


CASB (Cloud Access Security Broker)

～ クラウド利用におけるセキュリティギャップの解消と活用事例 ～

CASB ホワイトペーパー

日本クラウドセキュリティアライアンス

CASB ワーキンググループ

2017 年 3 月 2 日

はじめに

このたびは本書、CASB ホワイトペーパーをお手に取って下さり、誠にありがとうございます。

本書はクラウドセキュリティアライアンス日本支部の CASB ワーキンググループが、調査会社の発表資料や会員企業からの情報提供をもとに独自に編纂したものです。

CASB（Cloud Access Security Broker, クラウドアクセスセキュリティブローカー）は、調査会社によると IT セキュリティ分野で、この 3 年程度の近年での最大の注目テクノロジーとされています。
しかしながらこの分野が新しくまだまだ日本語による公開情報が不足しており、その実態がよく分からない状況となっています。

本書が CASB 理解への一助となり、ひいては読者の皆様のクラウド利用におけるセキュリティ向上施策検討へ何らかの貢献ができれば幸いです。

なお本書は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

2017 年 3 月

一般社団法人クラウドセキュリティアライアンス
CASB ワーキンググループ執筆メンバー
上田光一、高岡隆佳、小林岳夫、露木正樹、澁谷寿夫、渡辺慎太郎、諸角昌宏

変更履歴

日付	バージョン	変更内容
2017 年 3 月 2 日	バージョン 1.0	初版発行

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。

https://cloudsecurityalliance.jp

目次

1. 概要

1.1 クラウド利用に関するセキュリティ課題

クラウドファースト、クラウドネイティブといった言葉が一般に浸透し、多くの組織にとってクラウド利用は極めて自然でかつ妥当な選択肢となっています。一方でその組織にとってクラウド利用を選択しない理由として常に上位に挙げられるのが、セキュリティに関する懸念です。

- 平成 25 年総務省発表の情報通信白書によると、クラウドサービスを導入しない理由として第 1 位の「必要がない」に続き、第 2 位が「セキュリティに不安がある」というものでした。
  (http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc244140.html)
- 2014 年、メディア会社の調査(TechTarget ジャパン「パブリッククラウドサービス利用時のセキュリティに関する読者調査リポート（2014 年 6 月）)によると、クラウドサービスのセキュリティの課題として、第 1 位に挙げられたのが可用性の不安、続いて第 2 位はデータの秘匿性というものでした。
  (http://wp.techtarget.itmedia.co.jp/contents/?cid=14882)
- 昨年 2015 年のある民間企業の調査によると、パブリッククラウド導入への不安の第 1 位は「情報漏えい、セキュリティのリスク」というものでした。
  (http://prtimes.jp/main/html/rd/p/000000014.000009999.html)

これらの調査は主に利用者視点でまとめられていますが、一方さらに時期を遡りより社会的視点、あるいは事業者よりの視点でいえば、下記のような調査、分析結果も公開されています。

- ガートナー社レポート 「Assessing the Security Risks of Cloud Computing」
  調査への協力やスク軽減へのサポートなど事業者責任への言及がなされています（2008 年）
- Cloud Security Alliance 「Security Guidance for Critical Areas of Focus on Cloud Computing」
  総合的かつ体系的展開と詳細な項目を網羅したもので世界の参照指針の一つとなりました（2009 年）
- 経済産業省 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
  ISO/IEC27002 の管理策に加えクラウド特有の要素が加筆されました(2011 年)

ではクラウド利用者としては、こういった各種調査をもとにクラウド利用の指針を作成するなり、自組織の重要事項に基づいて評価や利活用の施策を検討実施していくことが望ましいのでしょうか？

現実的には、利用者が短期に実現することには様々に困難であり、時間がかかるプロセスとなるものと思われます。利用者視点では「セキュリティ」あるいは「情報漏えい」のような包括的な不安で表現される一方、ベストプラクティスでは管理項目が多岐に渡り、相当の作業量となります。これはクラウドの利点であるはずの「容易で迅速なサービス導入」という、クラウドに対する利用者側の期待値に反するものとなり、クラウドを利用したいがセキュリティ上の不安があるという上記調査結果につながる理由となっています。

1.2 具体的懸念とは

情報セキュリティの分野ではよく 3 要素として、以下の 3 つの性質が取り上げられます。

- 機密性（Confidentiality）
- 完全性（Integrity）
- 可用性（Availability）

機密性の観点では、事故・事件の双方の観点による組織外への情報漏えい、また組織内であっても所定の権限を越える情報資産へのアクセスなどが考えられます。完全性については、情報の不正な改ざんが考えられます。可用性については必要なときに必要な情報にアクセスできない、あるいは情報資産の毀損により永久にアクセスできないといったことも考えられます。

実際に日本国内で報道された事例としては、以下のようなことありました。

- ある国内クラウド事業者内部の操作ミスにより、ホスティングされていた情報がすべて削除されてしまい、復旧不能となった（可用性、完全性）
- ある海外事業者の大規模な連鎖不具合により、システムが数時間によりアクセス不能となった（可用性）
- クラウド事業者ではないが、預託された大量の個人情報が、業者の内部犯行により流出した（機密性）

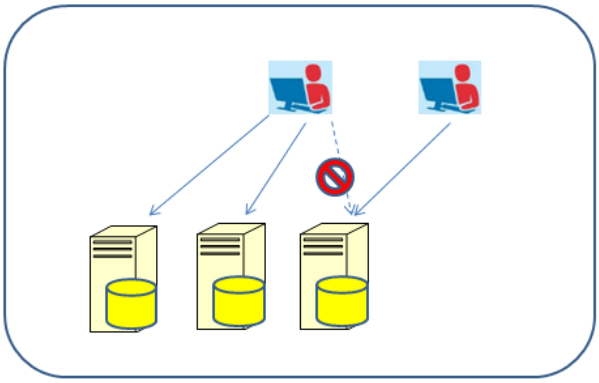
特に大きくは報道されていない事例としては以下のようなものもあります。

- 開発者向けクラウドにアップロードしたソースコード中に、他のクラウド利用のためのアクセスキーがハードコーディングされており、これが盗用、悪用され多大なクラウド利用料を請求された(機密性)

これらは実際に大小問わず報道されたものですので、氷山の一角と考えられます。
特に機密情報の漏えいについては、関係者以外に事例を公開することはまれですし、そもそも気が付いていない可能性すらあるからです。

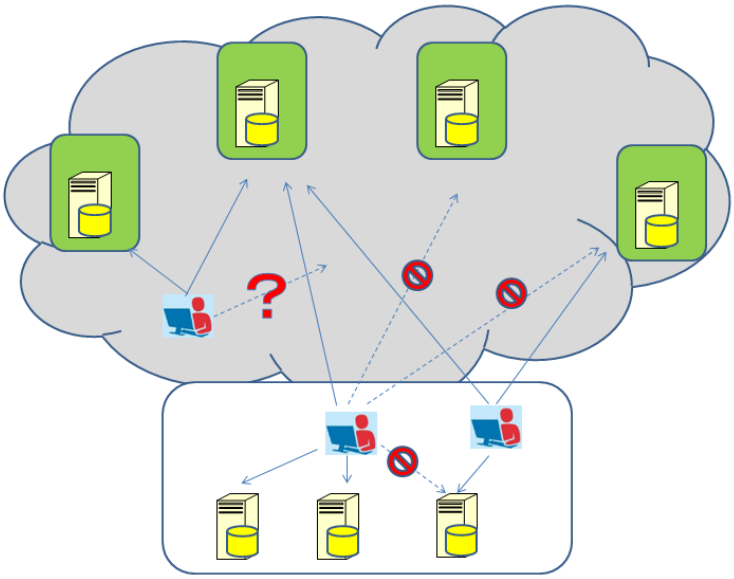
1.3 いったい何が起こっているのか

従来型の IT インフラでは情報資産はすべて組織内に存在しており、管理の所在がその組織にあることは明白でした。対象とするリスクが事故であれ事件であれ、その組織の意思で IT インフラの管理・統制・ガバナンスを効かせることが可能でした。



【図１．従来型セキュリティ】
守るべきデータ、システム、アクセス経路やそのコントロールはすべて、組織内で閉じている。

しかしクラウドでは、**データは社外**に存在します。そこへのアクセス方法や経路も多様であり、しかもこれが同時多発的に**複数**、それがしばしばシャドーIT（会社として許可されないクラウドサービス）といった形も含め組織の**管理者の意図とは別**に出現することになるのです。



【図２．クラウドセキュリティ】
守るべきデータ、システム、アクセス経路やそのコントロール組織の外側。

これでは従来型の境界型セキュリティのパラダイムでの解決は極めて困難です。

- エンドユーザ部門で調達されることが多いため、IT 部門の統制が効かず、十分なセキュリティを備えていない場合がある
- 機密データを社外に保存することになり、“見えない”箇所やリスクが発生する（リアルタイムな監査が提供されない）
- SaaS ベンダが提供するデータセキュリティは一様ではなく保証もされないため、ユーザ企業の責任となる
- SaaS ベンダが固有のセキュリティ向上策を採用する可能性はあるが、複数 SaaS を包括した“ユーザ中心”のセキュリティを提供することはできない
- オンプレミス側に投資したセキュリティ設備を、殆どの場合クラウドに適用・活用できない

調査会社のガートナー社は、こういった問題の調査結果をレポート（INF-15-10「注意すべき SaaS のセキュリティ・ギャップ」（G00263947)、2015/1/30）にまとめています。

1.4 セキュリティギャップの解消と CASB

ガートナー社の調査は、個々のセキュリティ侵害ではなくよりハイレベルな組織の GRC（ガバナンス・リスク・コンプライアンス）の観点にフォーカスしています。ガートナー社は、クラウド利用時の懸念を解消するテクノロジー、フレームワークとして、2012 年に初めて CASB（クラウド・アクセス・セキュリティ・ブローカ）を提唱しました。

組織の IT セキュリティ責任者（CISO）としては、クラウド利用を止めない限りはセキュリティギャップの解消に努める必要があります。これを実現するものが CASB です。

CASB は以下の 4 つの柱により構成されます。ガートナー社はセキュリティギャップを解消するにはこれらの機能が必要であり、それが単一点として提供されることにより組織のポリシー適用が可能になると主張しています。

- 可視性
- データセキュリティ（データ保護）
- コンプライアンス
- 脅威からの防御

「可視性」は、どのようなクラウドを誰が、いつ、どこから、どういったタイプのアクセスで利用しているか、についての理解を、組織の管理者に提供します。これはそのクラウドが「許可されたもの（サンクション IT）」「許可されていないもの（シャドーIT）」という観点や、そのクラウド業者がどういったセキュリティレベルにあるか、といった情報も含みます。

「データセキュリティ」は、クラウドに保存されるデータをよりよく保護するための機能を提供します。データアクセスに際し強固な認証を要求する、暗号化やトークン化の機能を備える、DLP の機能を備える、といったことを実現します。

「コンプライアンス」は、クラウド利用が組織内外の基準に照らして正当であることを保証する機能を備えます。利用者アクセスの監査ログやレポート、所定のコンプライアンス基準への適合性チェック、組織内監査システムとの統合などを実現します。

最後に「脅威からの防御」は、クラウド利用に関わる具体的な脅威に対策します。不正アクセスやその兆候の検出やその種のアクセス要求の排除が主たる提供機能になります。

これらを総合的に活用できる制御点として、オンプレミスに設置したウェブプロキシや CASB 機能を提供するクラウドサービスを利用することにより、SaaS 特有のセキュリティギャップを解消、すなわち複数の異なるクラウドサービスをオンプレシステムと同様、組織の求める基準に従った運用を実現できるようになります。

1.5 CASB をクラウド活用のイネーブラに

現代のように変化が極めて早い環境では、クラウドの活用は IT 利活用の中でも重要な位置を占め、組織へ好影響を与える施策のひとつと考えられます。一方セキュリティの課題があるため、クラウド利活用が進まないとするならば、組織にとっては大きな機会損失となり、生産性や競争力を下げる要因となります。

CASB によってクラウド利用のセキュリティが一定レベルで担保され、自組織のポリシーとの整合性が保てるならば、これはクラウド活用の促進要因すなわちイネーブラとして、間接的に組織の競争力強化に貢献できるものとなります。

では次章にて、具体的な活用事例を見ていくことにしましょう。

2. 事例

2.1 事例① グローバル通信企業

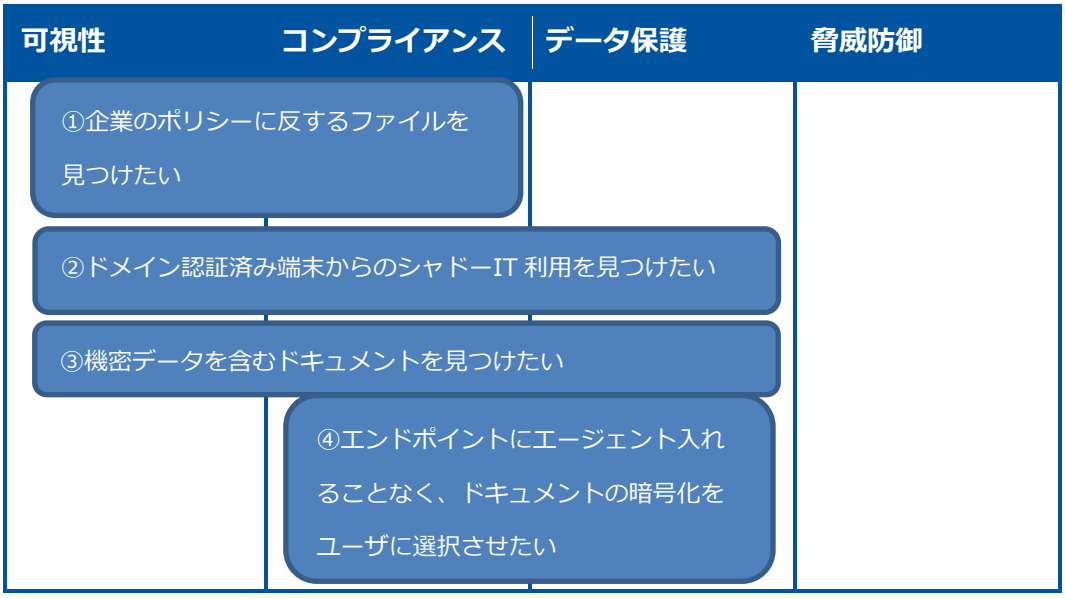
背景：

従業員 15,000 人の業務をクラウド（GoogleApps）に移すことを検討していたこの企業では、下記に挙げられる懸念事項をどう解決するか模索していました。

- ① 企業のポリシーに反するファイルを見つけたい
- ② ドメイン認証済み端末からのシャドーIT利用を見つけたい
- ③ 機密データを含むドキュメントを見つけたい
- ④ エンドポイントにエージェント入れることなく、ドキュメントの暗号化をユーザに選択させたい

要件の特定：

４つの懸念事項を詳細に検討していくと、これらがまさに CASB が解決しようとしている課題であることがわかります。CASB の４つの柱に照らし合わせると、下記のような対応になります。



CASB による解決：

本件での顧客企業要件を実現するためにはいくつか技術的な条件があります。

まず GoogleApps 企業アカウントとして発行されているユーザの挙動、ならびにそこで作成、共有されるデータをリアルタイムで精査し、制御する必要することが必要です。そのためには API ベースによる処理のリアルタイム性、制御のための処理ポイントの集約（ゲートウェイ）が必要となりました。

採用されたのが Symantec Elastica Securlets for GoogleApps および Audit 並びに Gateway です。すべての GoogleApps 企業アカウントは Symantec Elastica Gateway にて制御され、ここを通らない限り GoogleApps 上のデータにアクセスできません。また、Securlets により、GoogleApps 上で作成されるデータなどについては、ファイル単位での解析が行われその区分が行われます（要件①③）。（個人情報を含むか、怪しいコードを含むかなど）企業が定めたポリシーに従い、アクセスが許可されるユーザやそのデータ範囲などが制御されます。本来望ましくない機密情報が含まれるデータについては、辞書登録ワード検出にて特定され、適切なポリシーがそのデータに対して施行されます（要件③）。また必要に応じてユーザ側で選択したファイルを暗号化し、Google Apps とは別の場所（Elastica サービス内）で暗号鍵の制御と管理を提供します（要件④）。Audit 機能においては、各認証ユーザが利活用しているその他アプリケーションの信頼度を表示させ、管理者に対して適切なアプリケーションの利用のみ許可できるための指針となる情報を提供します（要件②）。

結果：

この CASB ソリューションによって、導入企業では下記のような価値が提供することができ、1 ユーザあたり年間 1600 円でクラウドにガバナンスを効かせることに成功しました。

- どのアプリケーションが業務生産性を下げ、またセキュリティ上のリスクとなるのかを特定可能に
- GoogleApps上のデータに対して自動的ないしは管理者側にて適切なポリシーを施行可能に
- ポリシー違反となるユーザの挙動についてリアルタイムで検出、ユーザへ適切な指導が可能に

Google Apps上のファイルの自動判別と可視化

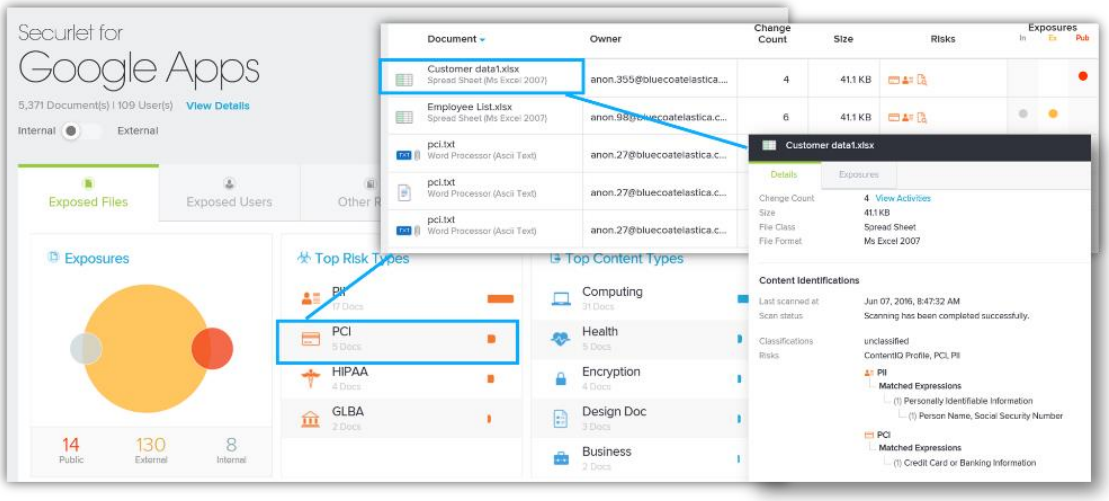


図 1-1.　Symantec Elastica Securlet

2.2 事例② 大手電力会社

背景：

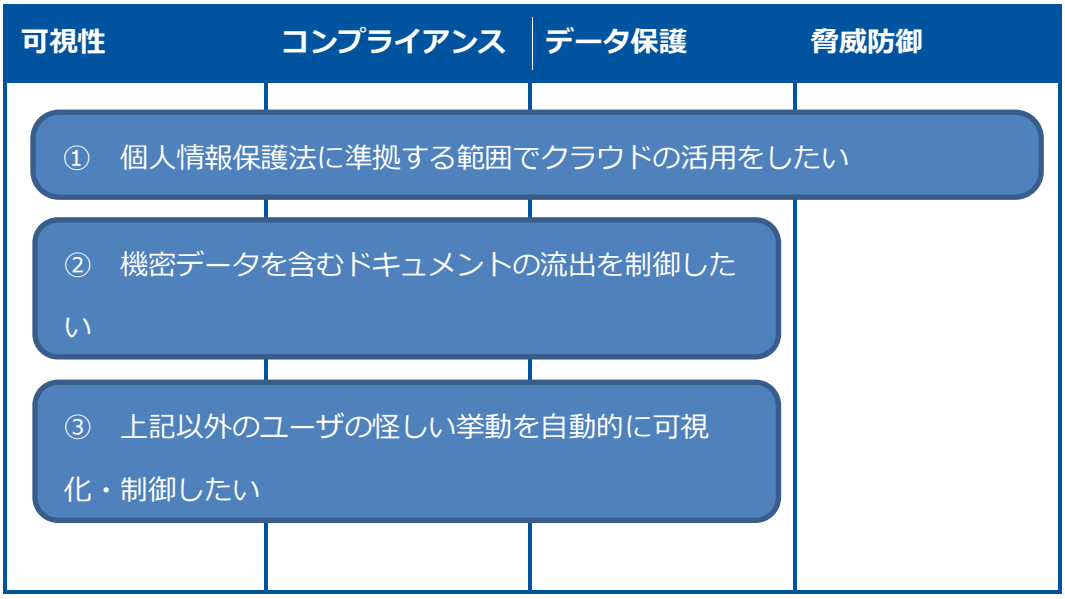
従業員 7,500 人の業務系 SaaS として Salesforce, O365, Dropbox に移すことを検討していたこの企業では、下記に挙げられる懸念事項をどう解決するか模索していました。

- ① 個人情報保護法に準拠する範囲でクラウドの活用をしたい
- ② 機密データを含むドキュメントの流出を制御したい
- ③ 上記以外のユーザの怪しい挙動を自動的に可視化・制御したい

要件の特定：

４つの懸念事項を詳細に検討していくと、これらがまさに CASB が解決しようとしている課題であることがわかります。

CASB の４つの柱に照らし合わせると、下記のような対応になります。



CASB による解決：

こちらのケースでは、クラウドへ移行するにあたって、国による強い個人情報保護法に対応するための施策が必要でした。

コストを下げるために 3 つの異なる業務系 SaaS への移行を検討した際に、サービスレベルの異なる SaaS に対し企業でガバナンスを効かせるには CASB が必要不可欠でした。とりわけ個人情報保護の観点から、機密情報を含むファイルに対し流出を未然に防ぐ仕組みを SFDC, O365, Dropbox に適用すると同時に、個人情報保護法に準拠する範囲でこれらの SaaS を活用する必要がありました。特に法律に対し違反と見なされた流出が発生した場合、大きな罰金（想定額 1.8 億円）も課せられることも CASB へ投資する一つのモチベーションとなりました。

そこでこの企業ではまず上記 3 つのアプリケーションに対し API ベースでリアルタイムにデータを認識・制御可能な Symantec Elastica Securlets および Gateway を採用しました。企業アカウントとして払い出され接続するユーザの上記業務系 SaaS のデータは Symantec Elastica Gateway/Securlets にて制御され、機械分析エンジンを搭載した DLP 機能により各ファイルやデータは企業の定める機密情報に該当するかしないか、リアルタイムに判定され、コンプライアンス上違反となるデータについてはアップロードまたは共有自体がブロックされます（要件①②）。特にこの企業が Elastica の持っている機能の中で高く評価したのが「ユーザのふるまい」を機械分析して個々のユーザに対するリスク値を算出する仕組みになります。ユーザがアプリケーションをどのように、どれだけ利用しているのかについて機械学習し、ポリシー違反やそれに近しい怪しげなふるまいをしているユーザをリスク値に従って適切なポリシーを自動的に適用することが可能になり、本機能により要件③を満たすことが可能となりました。また Gateway で提供する各ユーザのアクセスログは、CASB を通じて個人情報保護を準拠できている揺るがない証拠として監査に利用しています。（要件①）

結果：

このCASBソリューションによって、導入企業では下記のような価値が提供することができ、1ユーザあたり年間2600円でクラウドにガバナンスを効かせることに成功しました。

- 要求される法規制に対応するためのガバナンス（機密情報管理、監査）をオンプレで提供可能に
- 機密情報に該当するファイルを自動的に検知、適切なポリシーを施行可能に
- ポリシー違反となるユーザの挙動についてリアルタイムで検出、ユーザへ適切な指導が可能に

図 2-1.　Symantec Elastica ユーザのリスク評価画面

2.3 事例③ 大手製造業会社

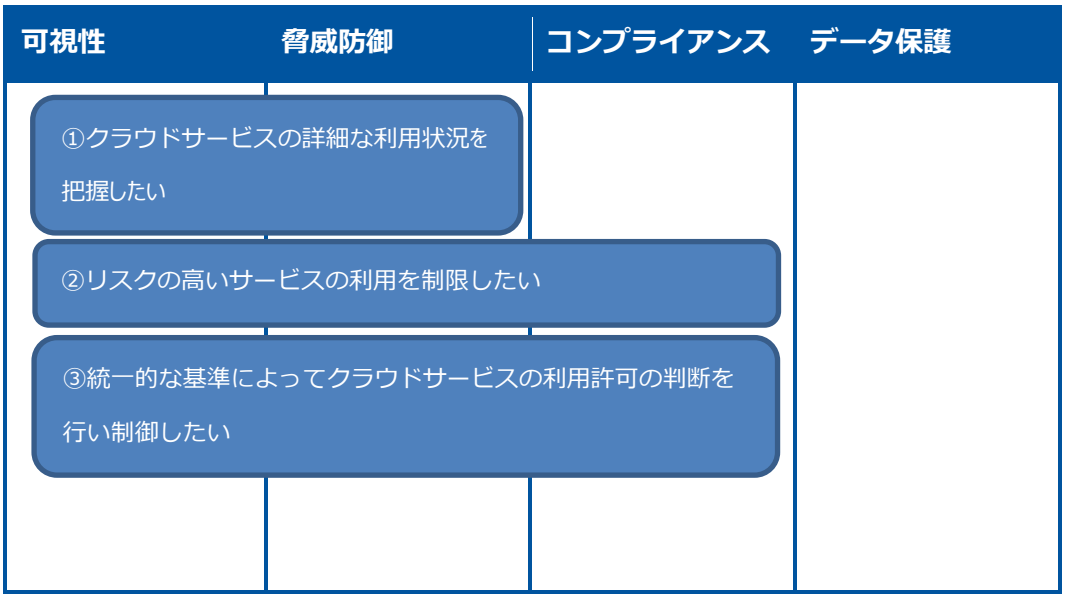
背景：

従業員 50,000 人のクラウド利用状況の把握と IT システム部へ依頼されるクラウドサービスの利用許可の判断の効率化を検討していたこの企業では、下記に挙げられる懸念事項をどう解決するか模索していました。

- ① クラウドサービスの詳細な利用状況を把握したい
- ② リスクの高いサービスの利用を制限したい
- ③ 統一的な基準によってクラウドサービスの利用許可の判断を行い制御したい

要件の特定：

3 つの懸念事項を詳細に検討していくと、これらがまさに CASB が解決しようとしている課題であることがわかります。CASB の 4 つの柱に照らし合わせると、下記のような対応になります。



CASB による解決：

こちらのケースでは、社内で利用されているクラウドサービスの把握が急務でした。また、IT システム部へ日々依頼されるクラウドサービスへのアクセス可否判断の調査ために数日かかっており、統一的な判断基準が必要と感じていました。

そこでこの企業は Skyhigh for Shadow IT を導入することにより、国内に配備されている 6 台のプロキシサーバのアクセスログを元にクラウドサービスの可視化を実現しました。その際の懸念点は以下の 2 つです。

- 機密情報(クライアント IP アドレス, ユーザ名)のアップロード
- トラフィックの増大

プロキシのアクセスログに含まれるクライアント IP およびユーザ認証情報は企業固有の情報のため、そのままの形では外部へ送ることが許可されませんでした。アクセスログからクラウドサービスへのアクセスを解析する Skyhigh の Enterprise Connector は、それらの機密情報をクラウドにアップロードする際に一方向の暗号化でトークナイズすることにより、難読化を実現しています。また、アップロードされるデータは、アクセスログからクラウドサービスへのアクセスのみを抽出するため、生ログファイルのサイズのおおよそ 1%程度となるため、懸念事項であった業務に影響するトラッフィクの増大にはなりませんでした。上記により 2 つの懸念事項は解決され導入に至りました。(要件①)

可視化されたクラウドサービスの利用状況から企業で利用が不適切と考えられるサービスを容易に把握することが可能となりました。このケースでは、一番目としてクラウドサービスのうち匿名で利用できるもの(Anonymous Use = Yes)をフィルタリング機能により抽出し、それらのサービスのドメイン名などをプロキシのブラックリストに登録することによりリスクの高いサービスを止めることに成功しました。(要件②)

日々の運用として、社内からクラウドサービスの利用許可の要望が IT システム部へ届きます。Skyhigh 導入前は、それらのサービスがどのようなサービスであり情報漏えいのリスクがあるかなど、数日かけて調査する必要がありました。Skyhigh 導入後は、Cloud Registry に登録されているリスク情報を元に判断することが可能となりました。上記例のように予め匿名で利用できるサービスであれば許可しないといったことが可能となります。(要件③)

結果：

この CASB ソリューションによって、企業内で懸念されていた Shadow IT の詳細を把握することができ、今後のクラウドサービス決定のための情報を知ることができました。また、今まで時間のかかっていたクラウドサービスのリスク判定を Global Registry を利用することにより短期間での判断が可能となりました。

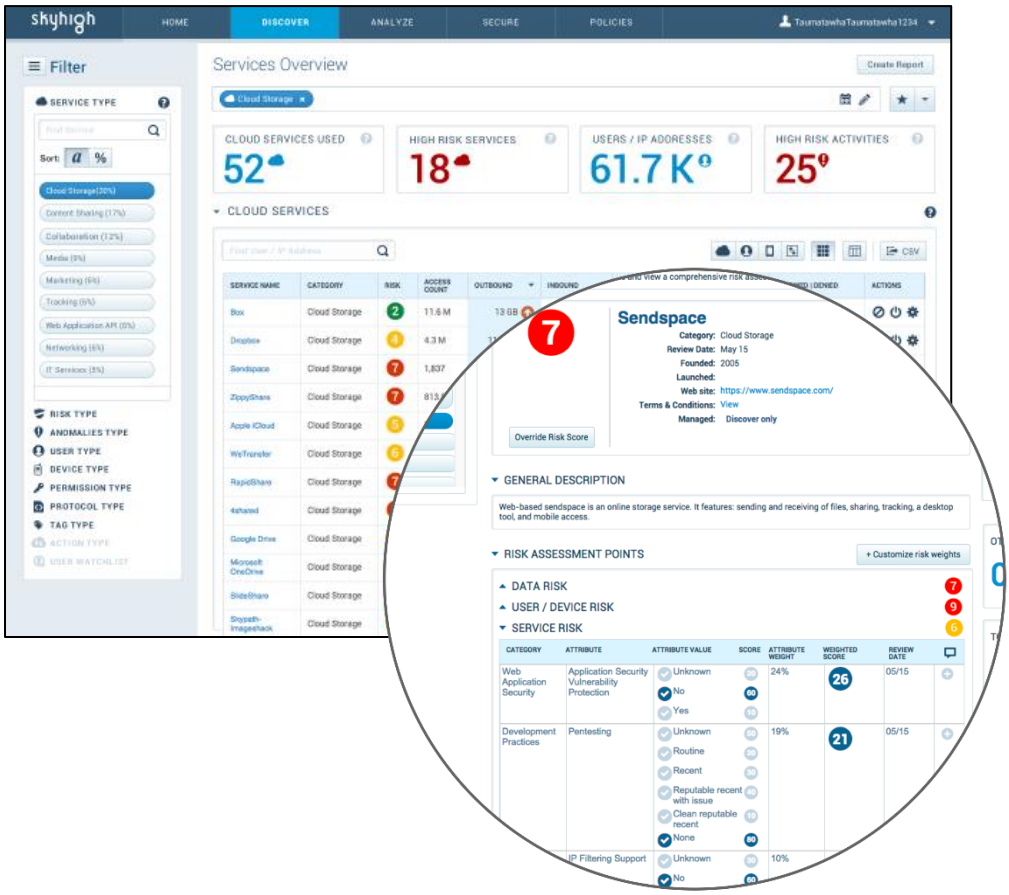


図 2-3 Skyhigh Networks のダッシュボード(サービス一覧と Global Registry)

2.4 事例④ 金融サービス会社

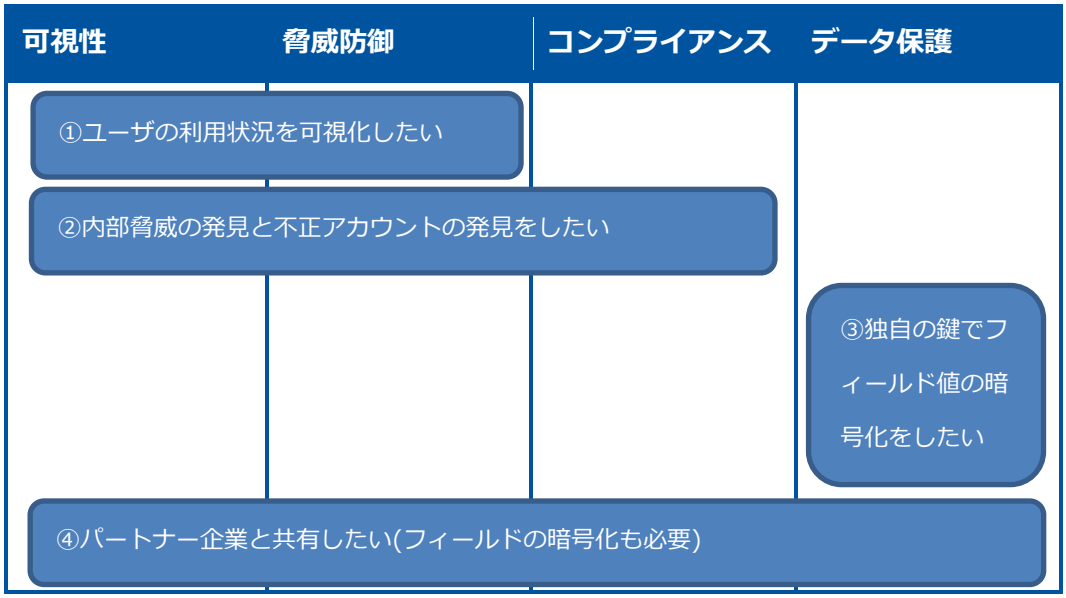
背景：

世界中に従業員 10,000 人の業務系 SaaS として Salesforce の利用をしていた企業では、下記に挙げられる懸念事項をどう解決するか模索していました。

- ① ユーザの利用状況を可視化したい
- ② 内部脅威の発見と不正アカウントの発見をしたい
- ③ 独自の鍵でフィールド値の暗号化をしたい
- ④ パートナー企業と共有したい(フィールドの暗号化も必要)

要件の特定：

4 つの懸念事項を詳細に検討していくと、これらがまさに CASB が解決しようとしている課題であることがわかります。CASB の 4 つの柱に照らし合わせると、下記のような対応になります。



CASB による解決：
こちらのケースでは、Salesforce の詳細な利用状況の可視化と同時に、内部脅威と不正アカウントでのアクセスを発見することが第一の目標でした。また Salesforce の鍵ではなく社内にある独自の鍵で暗号化する必要がありました。

そこでこの企業は、Skyhigh for Salesforce を導入することにより上記 4 つの要件を満たすことが可能でした。

まず、Salesforce に対して API ベースでのアクセス状況の取得を行いダッシュボード上に可視化します。それにより、いつ、どこで、誰が、どのデータにアクセスしたかを知ることが可能となります。(要件①)

それらのアクティビティを元に機械学習による行動解析を行い、不適切な特権アクセス、過度なアクセスおよびデータ漏洩による内部脅威を検知することが可能となります。また、コンプライアンスおよび調査のためのすべてのユーザと管理者の操作の証跡が保存されており、確認することができます。(要件②)

よりセキュアにデータを Salesforce に保存するため、機密情報(顧客名、電話番号など)を社内にある鍵管理サーバを利用して暗号化する必要がありました。Skyhigh for Salesforce のリバースプロキシと社内にインストールした Key Agent Server を利用することにより社内の鍵管理サーバと連携し独自の鍵を利用してフィールドの暗号化を行うことが可能となります。また、Skyhigh では暗号化されたフィールドに対してもアプリケーションの機能(ソート、検索など)をそのまま利用することが可能です。(要件③)

暗号化のために社内のゲートウェイに暗号化装置を設置する方法では、社内からのアクセスには対応が可能でしたが、社外からのリモートアクセスやパートナー企業からのアクセスに対応することが容易ではありませんでした。また、パートナー企業の対応のためにすべてのパートナー企業に同様の暗号化装置を設置することも難しく、どこからアクセスした場合でも暗号化に対応する必要がありました。
Skyhigh for Salesforce のリバースプロキシを利用し、Salesforce へのアクセスをリバースプロキシ経由にすることにより、社外からのアクセスおよびパートナー企業からのアクセスにおいても暗号化に対応することが可能となりました。 (要件④)

結果：

この CASB ソリューションによって、より安全に Salesforce を利用するために下記の価値を提供することができました。

- リバースプロキシを利用することにより、社内外、パートナー企業へ暗号化を提供
- アクティビティの可視化と行動監視により不正なアクセスなどの内部脅威を検知
- 独自の鍵サーバにより暗号化が可能

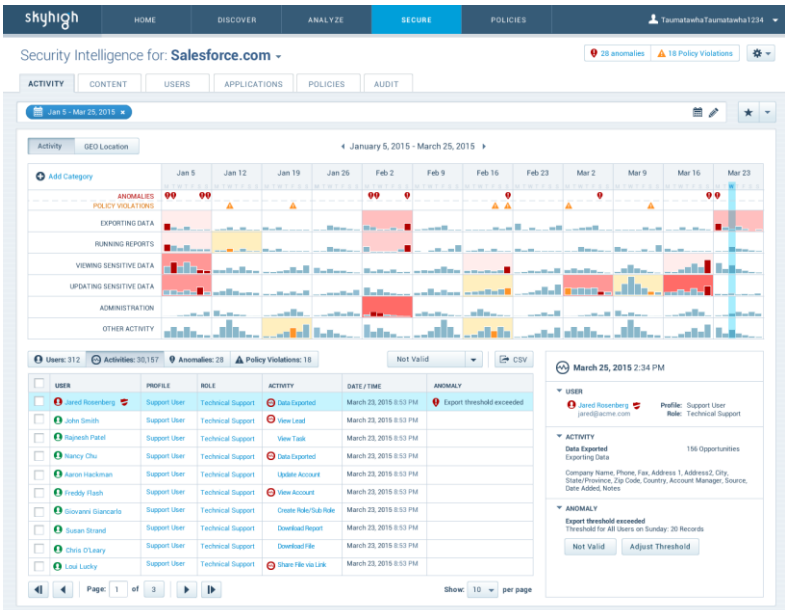


図 2-4 Skyhigh Networks のダッシュボード(アクティビティモニタ)

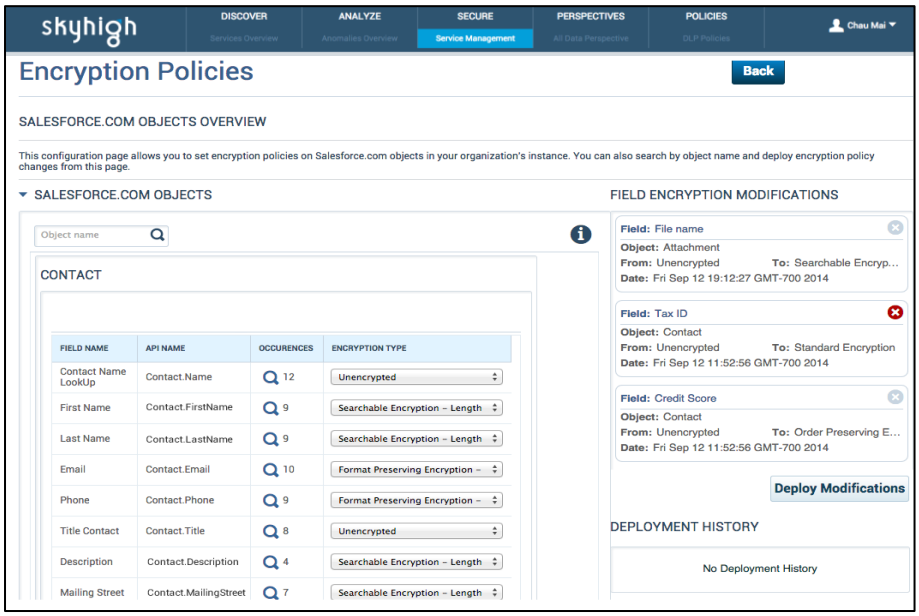


図 2-5 Skyhigh Networks のダッシュボード(暗号化設定画面)

3. おわりに

2015 年より、クラウドセキュリティアライアンス（CSA）ジャパンでは、CASB-WG 活動を開始しました。これは CSA グローバルとは独立した、ジャパン独自の活動となります。

CASB 自体は市場認知のまだ浅いコンセプトであること、CASB ベンダの動向にもある程度左右されること、また CASB ベンダーの買収が活発でありまだまだ変化のある業界、テクノロジーと考えられ、固定的な共有認識が確立するまで時間がかかるかも知れません。しかしながら基本のコンセプトはガートナー社の主張する SaaS のセキュリティギャップ解消にあることは間違いなく、CSA ジャパンの CASB-WG ではこういった状況も踏まえなるべく中立的な観点で、日本国内での CASB 関連情報の発信に努めて参ります。

CASB-WG 活動にご興味のある方は CSA ジャパン（info@cloudsecurityalliance.jp）までお問い合わせください。

4. 参考文献

ガートナー発行レポート：

Mind the SaaS Security Gaps (ID: G00263947, 2014/10/3)

Emerging Technology Analysis: Cloud Access Security Brokers (ID: G00264199, 2014/9/25)

注意すべき SaaS のセキュリティ・ギャップ (INF-15-10, 2015/1/30)

Technology Overview for Cloud Access Security Broker (ID: G00269985, 2015/5/19)

クラウド・アクセス・セキュリティ・ブローカのテクノロジ概要 (INF-15-107, 2015/1/17)

Select the Right CASB Deployment for Your SaaS Security Strategy (ID: G00270559, 2015/3/12)

Budgeting for the SaaS Security Gap (ID: G00271282, 2015/1/28)

How to Evaluate and Operate a Cloud Access Security Broker (ID: G00292468, 2015/12/8)

Market Guide for Cloud Access Security Brokers (ID: G00274053, 2015/10/22)

Market Guide for Cloud Access Security Brokers (ID: G00293664, 2016/10/24)

ITU ジャーナル：

Vol.45 No.1 (2015, 1) 特集 クラウドセキュリティ<1>

p12-17. クラウドのセキュリティ課題 CSA 及び所説に基づく整理