クラウド時代に必要となるセキュリティ対策

Security Measures Required in the Cloud Era

三　池　聖　史

要　約　「クラウドファースト」「働き方改革」が社会に浸透するに連れて，クラウドサービスの需要はますます高まっている．このようなクラウドサービスを取り巻く環境変化から発生する課題に対応するために，クラウドサービス事業者にはクラウドサービスを安全に利用するための情報セキュリティ対策が不可欠である．一方，利用者も，クラウドサービスにオンプレミスのシステムと同等レベルの情報セキュリティ対策を求めるようになってきた．クラウドサービスを安全に活用するためには，クラウドサービス事業者と利用者の両方の立場から，どのような情報セキュリティ対策が必要か考えなければならない．

Abstract　As the social situation such as “cloud first” and “work style revolution” traverse the society, the demand for cloud services increase more and more. Information security measures are indispensable to cloud service providers for safe use of cloud services, and in order to deal with the challenges arising from such environmental changes surrounding the cloud services. Meanwhile, users begun to demand the level of information security measures to be the same level of on-premises systems. In order to utilize the cloud service safely, it is necessary to consider what kind of information security measures are required from the standpoint of both the cloud service provider and the user.

1. は　じ　め　に

企業の ICT への依存が高まる中で，情報システム構築の迅速化，管理・運用費用の低減化を実現する有効な手段としてクラウドサービスの利用が拡大し，クラウドファーストと呼ばれるほど，企業を支える重要な ICT 基盤となっている．一方，サービス形態，管理水準，サービスレベル等が異なる多様なクラウドサービスが提供され，企業のクラウド利用の選択肢が増えているにもかかわらず，情報セキュリティポリシーを満足できるクラウドサービスを企業が適切に選択できていない場合が多い．例えば企業がクラウドストレージを利用する場合，データがクラウド上で管理され，インターネットを通じて利用することになるため，常に第三者による不正アクセスや盗聴などの攻撃により，情報漏えいやデータ改ざん等に直面しやすくなる．

本稿では，クラウドを取り巻く環境から発生するこのような課題に対応し，クラウドサービスを安全に利用するための情報セキュリティ対策について述べる．2 章でクラウドサービス事業者が考慮すべき情報セキュリティ対策を述べ，3 章でクラウドサービス利用者が CASB（Cloud Access Security Broker：キャスビー）を使用することで，どのような情報セキュリティ対策が実現できるかについて述べる．

2.　クラウドサービス事業者のセキュリティ対策

本章では，クラウドサービス事業者がクラウドサービスを提供する際に考慮すべき情報セ

キュリティ対策について，総務省が公開している「クラウドサービス提供における情報セキュリティ対策ガイドライン」[1]を参考に「組織・運用に係る対策」「技術的対策」「物理的対策」の側面から整理する．

2.1　組織・運用に係る対策

本節では，クラウドサービス事業者の経営陣，情報資産の管理責任者，雇用予定・雇用中・雇用終了後の従業員を対象とした情報セキュリティへの取り組みについて述べる．

2.1.1　情報セキュリティへの組織的取り組み

経営陣は，情報セキュリティに関する組織的取り組みについての基本的な方針を定めた情報セキュリティポリシー，従業員に対する秘密保持または守秘義務についての要求，情報セキュリティ対策における具体的な実施基準や手順等を明確にした文書を作成する．これらの指針やルール，手続きや手順などに従って，経営陣主導の下，情報セキュリティ向上の実現に組織全体で取り組む．作成した文書類は，定期的またはクラウドサービスの提供に係る組織環境や業務環境，法的環境，技術的環境等の重大な変更が発生した場合に見直しを行う．特にクラウドサービスの提供にあたっては，外部組織の関与が多岐に渡るため，外部組織における情報資産に対する不正アクセス，情報資産の盗難や不正変更，情報処理設備の悪用や破壊等のリスクを識別し，情報資産に対する外部組織からのアクセスを管理・制限する方針と方法を定める．また，連携クラウド事業者が提供するクラウドサービスを利用する場合は，事業者間で合意された情報セキュリティ対策およびサービスレベルが，連携クラウド事業者によって確実に実施されるように契約や SLA を締結し，クラウドサービスの運用に関する報告および記録を常に確認し，定期的に監査を実施する．

2.1.2　情報資産の管理

情報資産，すなわちクラウドサービスの提供に必要なハードウェア，ソフトウェア，通信機器・回線などの構成要素およびそれらを介する情報について，管理責任者を定めるとともに，利用可能者，利用目的，利用方法，返却方法などを明確にし，情報資産の目録を作成する．また，情報資産の価値や個人情報保護などの法的要求に基づき，取り扱いの慎重さの度合いや重要性の観点から情報資産をレベル分けし，レベルごとに安全な処理・保存・伝達・秘密解除・破棄などの手順を定める．特にクラウド利用者から預託された情報については，利用者がクラウドサービスの利用を終了する場合，預託された情報を利用者が取扱うことができる形で返却し，クラウドサービスの情報処理施設などから二度と取り出せないように破棄する．

2.1.3　情報セキュリティポリシーの遵守，点検および監査

各情報資産の管理責任者は，自分の責任範囲内の全ての情報セキュリティ対策が情報セキュリティポリシーに則り正しく確実に実施されるよう，定期的にレビューと見直しを行う．また，クラウドサービスの提供に用いる情報システムが情報セキュリティポリシー上の要求を遵守していることを確認するため，定期的に点検・監査する．

2.1.4　従業員に係る情報セキュリティ

雇用予定の従業員に対して，機密性・完全性・可用性に係る情報セキュリティ上の要求と責任の分界点を示して説明し，雇用契約を締結する際はこの要求などに対する明確な同意を得る．雇用期間中は，従業員に対して情報セキュリティポリシーの意識向上のため適切な教育・訓練を実施する．また，従業員が情報セキュリティポリシーまたはクラウドサービス提供上の契約に違反した場合の対応手続きを明確にする．

従業員の雇用が終了または変更となった場合の，アクセス権の削除や支給した情報資産の返却など，実施すべき事項や手続き，確認項目などを明確にする．

2.1.5　情報セキュリティインシデントの管理

サービス停止，情報漏えい・改ざん・破壊・紛失，ウイルス感染などの（疑いを含む）情報セキュリティインシデントや情報システムのぜい弱性を発見した場合，できるだけ速やかに管理責任者に報告できるように手続きを定め，全従業員に周知徹底する．また，報告を受けた後に迅速に対応ができるよう，責任体制および手順を確立する．

2.1.6　法令と規則の遵守

個人情報，機密情報，知的財産など，法令や契約上適切な管理が求められている情報については，該当する法令や契約を特定した上で，その要求に基づき適切な情報セキュリティ対策を実施する．関連する法規には個人情報保護法，不正競争防止法，著作権法，e-文書法などがある．

クラウドサービスの提供を続ける上で重要な会計記録，データベース記録，取引ログ，監査ログ，運用手順等については，法令・契約および情報セキュリティポリシーなどの要求事項に従って適切に管理する．

利用者に対して，利用しようとしている情報システムや情報処理施設がクラウド事業者の所有であり，認可されていないアクセスは許可されないことを，警告文の画面表示などによって警告する．

2.2　技術的対策

本節では，クラウドサービスの提供に用いるアプリケーション，プラットフォーム，サーバ・ストレージ，通信機器などへの技術的対策をまとめる．

2.2.1　稼働・障害・パフォーマンス監視

応答確認などの稼働監視，サービスの正常動作を確認する障害監視，サービスのレスポンス時間などのパフォーマンス監視の実施基準や手順などを定め，サービス稼働状態を監視する．稼働停止や障害，パフォーマンス低下を検知した場合は，利用者に速報とフォローアップ報告を通知する．また，監視結果の定期報告書を作成して利用者と管理責任者に報告する．

2.2.2　時刻同期

責任分界の観点からログによる証拠保全が重要であるため，時刻同期の方法を規定し実施する．また，定期的に時刻同期の状況を確認する．

2.2.3　パッチ適用

OS，その他ソフトウェアの技術的ぜい弱性に関するパッチ発行等の情報を定期的に収集し，随時パッチを適用する．

2.2.4　稼働率

クラウドサービスを利用者に提供する時間帯（サービス時間帯）を定め，その時間帯におけるクラウドサービスの稼働率を規定する．また，定期保守時間を規定する．

2.2.5　容量・能力

要求されたサービス性能を確実に満たすために，利用者の利用状況の予測に基づいて設計した容量や能力などの要求事項を記録した文書を作成する．

2.2.6　ログの記録

利用者の利用状況や，例外処理と情報セキュリティ事象のログを取得し，保管する期間や保管方法，監査方法などを明確にする．また，システムの実務管理者や運用担当者の作業を記録し，定期的にレビューする．

2.2.7　ぜい弱性診断とウイルス対策

ぜい弱性やウイルスに対し，診断方法や時期などの計画を明確にして定期的に診断し，その結果に基づいて対策を講じる．

2.2.8　データの暗号化とバックアップ

データベースに格納された個人情報や機密情報などのデータを暗号化するとともに，利用者のサービスデータ，アプリケーションやサーバ・ストレージなどの管理情報およびシステム構成情報の定期的なバックアップを実施する．また，バックアップされた情報が正常に記録され，正しく復号化し読み出すことができるかどうか定期的に確認する．

2.2.9　外部ネットワークからの不正アクセス防止

ネットワーク構成図を作成する．また，アクセス制御方針とそれに基づいてアクセス制御を許可または無効とするための正式な手順を策定する．利用者の接続回線も含めてサービスを提供する場合はその回線も含めてアクセス制御の責任を負う．

アクセス制御方針に則り，情報システム管理者やネットワーク管理者にアクセス権限の割当や制限を施す．利用者および情報システム管理者，ネットワーク管理者などのアクセスを管理するための適切な認証方法，特定の場所および装置からの接続を認証する方法などにより，アクセス制御となりすまし対策を行う．また運用管理規定を作成し，ID・パスワードを用いる場合はその運用管理方法とパスワードの有効期限を規定に含める．

外部および内部からの不正アクセスを防止するファイアウォールやリバースプロキシを導入するとともに，IDS/IPS の導入などで不正な通過パケットを自動的に発見，遮断する措置を講じる．

2. 2. 10　外部ネットワークにおける情報セキュリティ対策

外部ネットワークを利用した情報交換において，情報を盗聴，改ざん，誤った経路での通信，破壊などから保護するため，情報交換の実施基準や手順などを作成し，通信の暗号化を行う．第三者が当該事業者のサーバになりすますフィッシングなどを防止するため，サーバ証明書の取得などの必要な対策を実施する．

利用する全ての外部ネットワーク接続について，情報セキュリティ特性，サービスレベル（特に，通信容量とトラフィック変動が重要）および管理上の要求事項を特定する．また，外部ネットワークの障害を監視し，障害を検知した場合は管理責任者に通報する．

2. 3　物理的対策

本節では，クラウドサービスの提供に用いるサーバ・ストレージ，情報セキュリティ対策機器などの情報システムが設置されている施設への物理的対策について述べる．

2. 3. 1　災害対策と電源・空調の維持，システム防護

地震や水害に備え，停電や電力障害が生じた場合の電源を確保しておく．また，設置されている機器による発熱を抑えるのに十分な容量の空調を提供する．サーバルームには，火災検知・通報システムおよび消火設備を備え，放水などの消火設備の使用に伴う汚損の対策，雷が直撃した場合の対策，静電気の対策を講じる．

2. 3. 2　建物の情報セキュリティ対策

カード制御による出入口や有人の受付など重要な物理的セキュリティ境界に対し，個人認証システムを用いて従業員および出入りを許可された外部組織の入退室記録を作成し，適切な期間保存する．また監視カメラを設置し，その稼働時間と監視範囲を定めて監視を行い，監視カメラの映像を適切な期間保存する．

3.　クラウドサービス利用者のセキュリティ対策

クラウドサービス事業者が 2 章で述べたような情報セキュリティ対策を講じてクラウドサービスを提供しているとは限らない．従って，クラウドサービスを利用する企業側でも，企業内でどのようなクラウドサービスが利用されているか，利用しているクラウドサービスの情報セキュリティ対策は十分か把握した上で，安全なクラウドサービスを利用するべきである．

本章では，クラウドサービス利用時の情報セキュリティ課題について述べ，それらの課題を解決する，CASB を利用した利用者の情報セキュリティ対策を紹介する．

3. 1　クラウドサービス利用時のセキュリティ課題

企業の情報セキュリティ対策は従来，社内のオンプレミスシステムをイントラネット経由で利用することを前提にしてきた．ところが，クラウドサービスの利用が本格化し，「働き方改革」の推進によってモバイルの活用が広がり始めた現在では，クラウドサービスにアクセスする際にセンター拠点（社内データセンターや本社等）のファイアウォールや UTM，プロキシ等を経由させるという従来型の「境界セキュリティ」の枠組みのなかで情報セキュリティを担保するのが困難になっている．本節では，クラウドサービスの利用時の課題について述べる．

課題 1)：クラウドへのダイレクトアクセス

業務効率を上げるために，各拠点や外出先から直接インターネット経由でクラウドを利用することを認めると，既存の情報セキュリティの仕組みを迂回するので，情報セキュリティポリシーの適用や利用状況の把握が困難になる．

課題 2)：シャドー IT の増加

社員あるいはユーザー部門単位で勝手にクラウドサービスを利用するケースである．情報セキュリティ対策が十分でないオンラインストレージやチャットを，業務データの保管や共有に利用する例も少なくない．これも課題 1) と同様，情報セキュリティポリシーの適用と利用状況の把握は難しい．

課題 3)：正式に契約しているクラウドの不正利用

企業として正式に契約した「正規のクラウド」を利用している社員は安全かと言えば，そうとも言い切れない．利用するクラウドの数が増えれば，社員がルールに則って正しく使っているかを管理して情報セキュリティポリシーを徹底させるのが困難になる．

図 1 に上記三つのクラウドサービス利用時のセキュリティ課題をまとめる．クラウド環境では，社員の行動や業務データの移動が見えない．企業のこうした課題を解決するためのツールの一つが CASB（Cloud Access Security Broker：キャスビー）である．CASB を活用することで，リスクの高いクラウドサービスの利用を可視化し制御することができる．

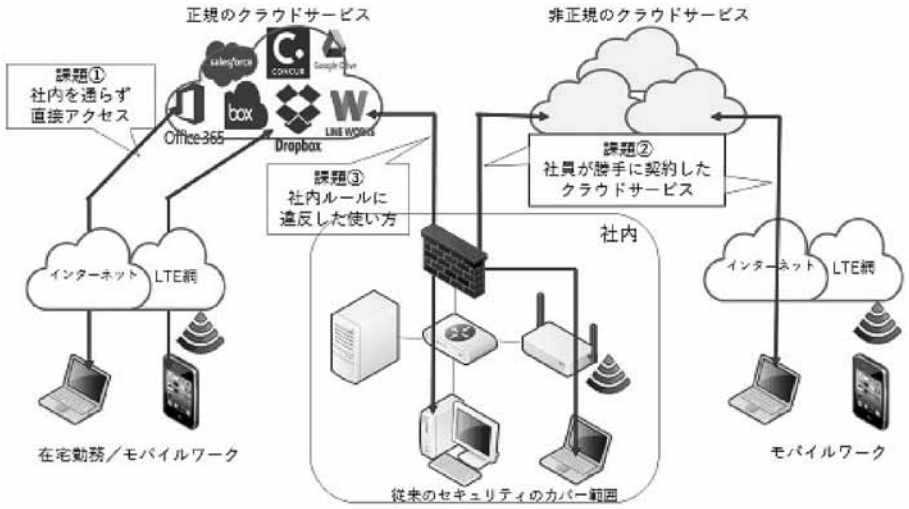

図 1　クラウドサービス利用時のセキュリティ課題

3. 2　CASB

CASB は米国ガートナー社が 2012 年に提唱した考え方で，企業が利用するクラウドサービスの可視化，データ保護，アクセス制御を実現するサービス/製品を指す．具体的には，クラウドサービスの利用者とクラウド事業者の間に CASB を配置し，利用者のクラウドサービスの利用状況の把握，アクセス制御，データ暗号化，ログ取得といったクラウドサービスへのアクセスに関する情報セキュリティ対策を提供する．CASB の構成を図 2 に示す．

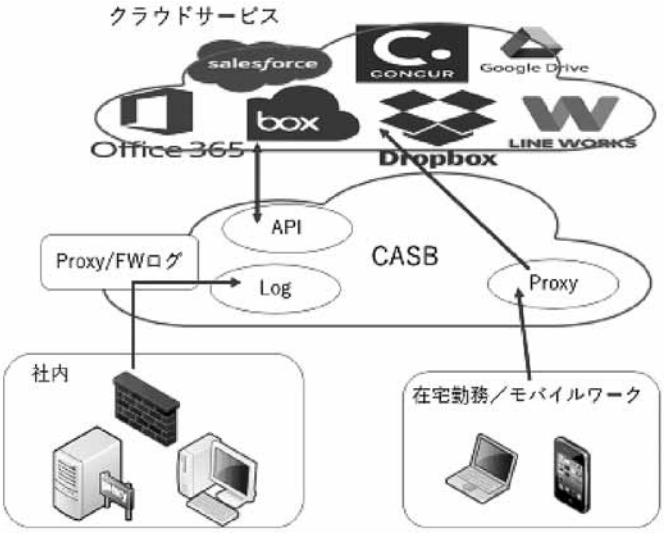

図 2　CASB の構成

CASB で提供される機能は「可視化」「データセキュリティ」「コンプライアンス」「脅威防御」の四つに大別される．

「可視化」は CASB の基本機能で，誰がどのクラウドサービスを使っているのか，その頻度などの利用状況を分析し，リスクの高い挙動を発見した場合には，ダッシュボード画面に強調表示したり，管理者に通知することで対処を促す（図 3）．また，各種のクラウドサービスの安全性を継続的に分析しレーティングする機能も備える．

図 3　クラウドサービス利用状況の表示例

クラウドサービスの利用状況を「可視化」した上で，リスクをコントロールするのが残り三つの機能である．

「データセキュリティ」機能はアクセス制御によって未許可端末/ユーザーのアクセスを禁止したり，データの暗号化で情報流出を防止する．

「コンプライアンス」機能は業界標準や法規制，社内コンプライアンスに基づいたデータ運用が行われているかを監査しレポーティングする．

「脅威防御」機能はクラウドサービスを通じて社外に出るデータを監視し，特にインサイダーや特権ユーザーによる不正な利用を防ぐ．またマルウェアの検知・感染防止機能を実装するCASB もある．

図 4 に「可視化」「データセキュリティ」「コンプライアンス」「脅威防御」の四つの機能を示す．これらの機能を活用することで，オンプレミスシステムと同じように，クラウドサービスに対しても情報セキュリティポリシーを適用し，社員の行動を可視化・制御することが可能となり，3.1 節の課題を解決することができる．

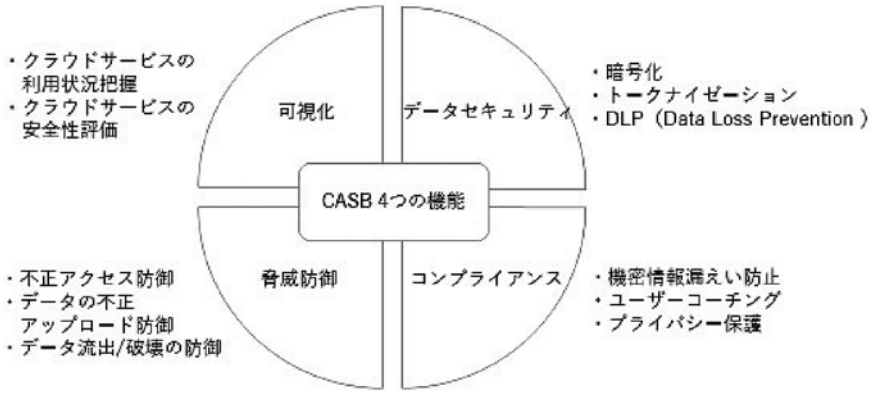

図 4　CASB の四つの機能

3. 3　CASB を利用したクラウドサービスのセキュリティ対策

2 章でクラウドサービス事業者が実施すべき情報セキュリティ対策をまとめたが，クラウドサービスの利用者にとっては，利用するクラウドサービスのセキュリティ対策が十分かどうかを判断することは困難である．

そこでCASB を使って，利用するクラウドサービスが安全か，企業のセキュリティポリシーに違反したクラウドサービスを利用していないかなどをモニタリングし，分析・評価するとともに，企業のクラウドセキュリティポリシーを策定，または見直す．さらに，安全ではないクラウドサービスは利用を制限するなどの対策を講じなければならない．

ユニアデックス株式会社（以降，ユニアデックス）では，「McAfee Skyhigh Security Cloud（以降，Skyhigh）」の販売を 2018 年 4 月から開始した．Skyhigh は米国ガートナー社の評価でCASB のマーケットリーダに位置付けられ，国内で最も導入実績が多く，日本のクラウドサービスに最も多く対応している．ユニアデックスは Skyhigh の可視化機能を利用し，顧客が安全なクラウドサービスを利用するための付加価値サービスを提供している．本節では，その事例を紹介する．

1）クラウドサービス利用状況の可視化と分析・評価

定期的にクラウドサービスの利用状況をレポートし，許可していないクラウドサービスを利用していないか，リスクが高いサービスを利用していないかを分析・評価する（図 5）．すべての利用状況を可視化することで，3.1 節の三つの課題である「社外からのダイレクトアクセス」「シャドー IT（未契約クラウド）」「正規契約クラウドの不正使用」の現状を把握することができる．

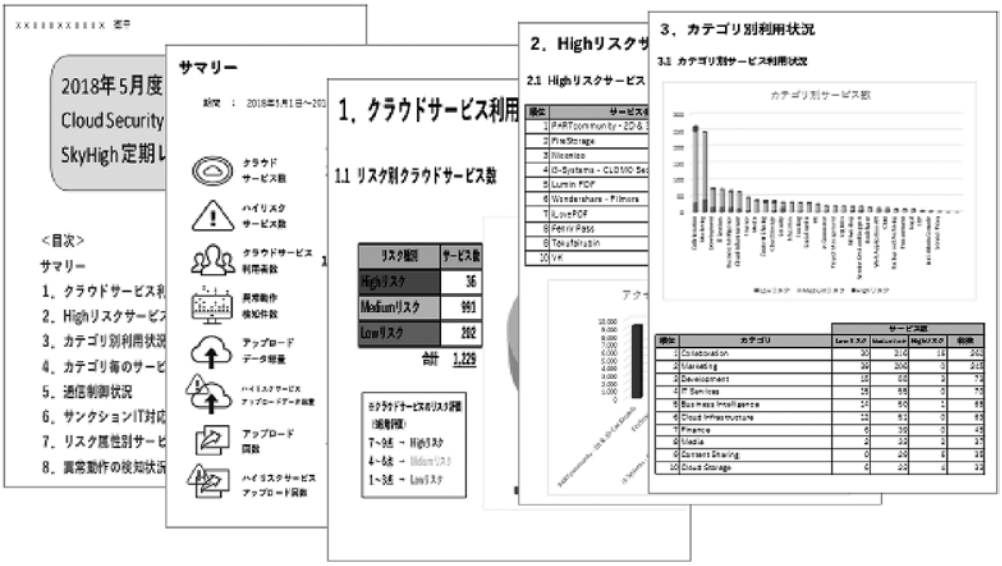

図 5　CASB 定期レポート

2）クラウドサービスのグルーピング

利用状況から，クラウドサービスを以下のように企業全体で利用を許可するサービス，利用者を一部の社員に限定したサービス，利用を認めないサービスに分類し，クラウドサービスの利用を制限する．図 6 にクラウドサービスのグルーピング例を示す．

■利用許可サービス：全社で使用しているクラウドサービス
- 会社で契約しているサービス
- 申請・承認プロセスなし，利用者限定なし
- Skyhigh のリスク評価でローリスクと判断されたサービス

■利用限定サービス：社員からの要望により使用を承認したクラウドサービス
- 自社のクラウドセキュリティポリシーに合致したサービス
- 申請・承認プロセスあり，利用者限定あり
- 厳格なデータセキュリティ対策による制御を実施

■利用不可サービス：完全に使用を認めないクラウドサービス
- Skyhigh のリスク評価でハイリスクと判断されたサービス
- データ暗号化未対応，マルチテナント未対応，匿名ユーザーの利用可能など
  自社のクラウドセキュリティポリシーの基準に満たない

■上記の分類に当てはまらないサービス

・その他，判断や分類が困難なクラウドサービスなど

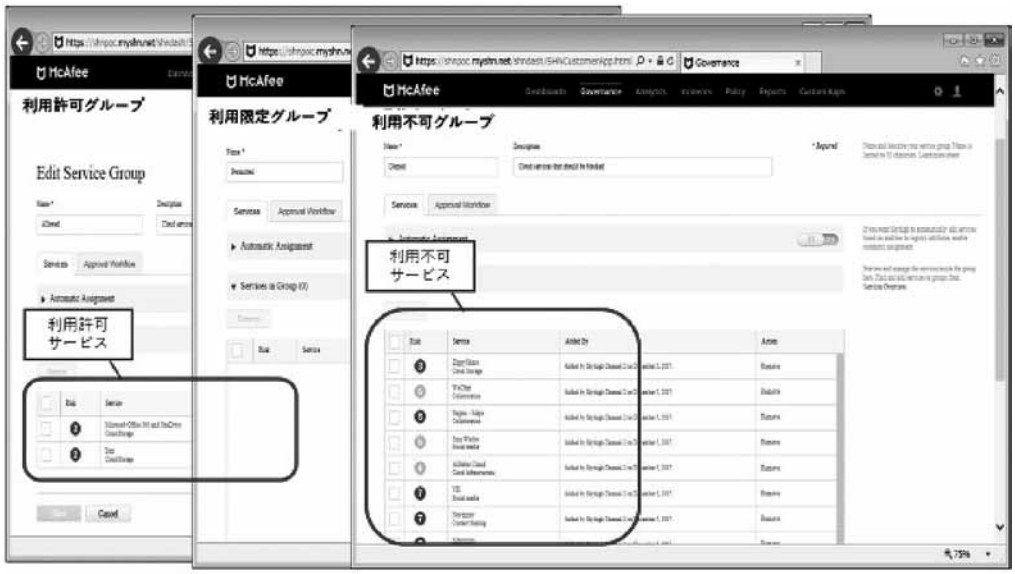

図 6　クラウドサービスのグルーピング例

3）クラウドセキュリティポリシーの策定

Skyhigh には，クラウドサービスを分析するための約 50 のリスク評価項目（リスク属性）がある．この項目を基にクラウドサービス利用基準（クラウドセキュリティポリシー）を策定する．

■自社のクラウドサービス利用基準（クラウドセキュリティポリシー）策定

・ポリシーの例：匿名利用＝使用不可
　　マルチテナント未対応＝使用不可
　　データ暗号化未対応＝使用不可
　　リスク評価ハイリスクのサービス＝使用不可

■クラウド属性プロファイルの作成

・策定したクラウドセキュリティポリシーに基づいて Skyhigh リスク属性による
　クラウド属性プロファイルを作成（図 7）

■クラウドサービスのグループの作成

・作成したクラウド属性プロファイルを 2）で作成した各グループに対応づける

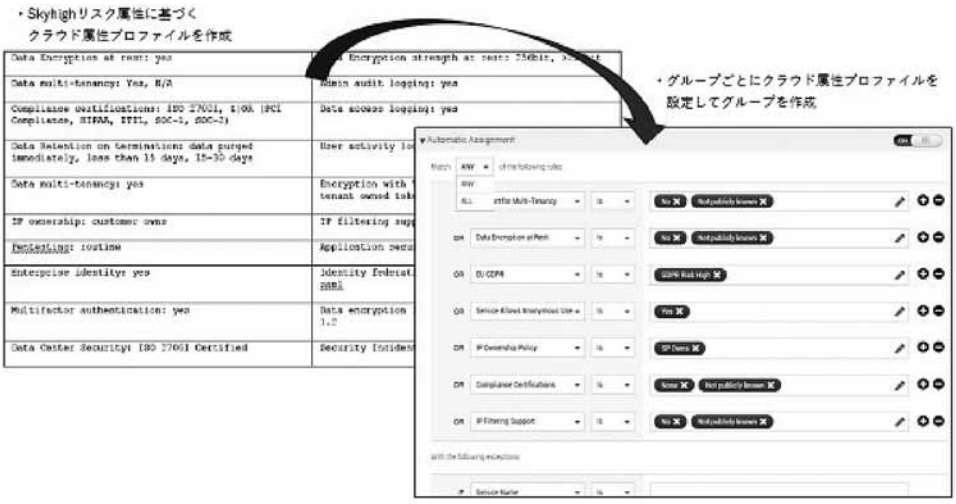

図 7　クラウド属性プロファイル例

4）クラウドサービスのアクセス制御

2）で作成した利用不可サービスグループの URL リストを抽出し，それをファイアウォールやプロキシなどに適用してアクセス制御を実施する．

上記，1）～ 4）を繰り返すことにより，クラウドサービスの利用を継続的に制御でき，3.1 節の三つの課題である「社外からのダイレクトアクセス」「シャドー IT（未契約クラウド）」「正規契約クラウドの不正使用」を抑止できる．

4. お　わ　り　に

安全なクラウドサービスを提供するには，クラウドサービス事業者がガイドライン[1]などにならってセキュリティ対策を講じる他に「ISMS クラウドセキュリティ認証（ISO/IEC 27017）」「CSA（Cloud Security Alliance）STAR 認証」などのクラウドセキュリティ認証を取得することも対策のひとつである．

一方，安全なクラウドサービスの利用を考えている企業からは，セキュリティ対策が十分でこれらの認証も取得している事業者のクラウドサービスを選択したい，CASB を利用してクラウドサービスの安全性を評価し利用を制御したいという要求が増えてくるだろう．

ユニアデックスが提供する CASB 製品とそれを利用した付加価値サービスが顧客の要求に寄与できれば幸いである．

最後に，本稿執筆にあたりご協力・ご指導頂いたすべての皆様に深く感謝し，御礼申し上げます．

参考文献　［1］ クラウドサービス提供における情報セキュリティ対策ガイドライン，総務省，2014年4月
［2］「CASB」を基礎から徹底解説（前編）―クラウドのリスクを可視化・制御，business network.jp，2017年9月26日，https://businessnetwork.jp/tabid/65/artid/5659/page/1/Default.aspx
［3］ 大元隆志，クラウドシフトに欠かせないCASBとは？，EnterpriseZine，2018年1月29日，https://enterprisezine.jp/article/detail/10308
［4］ CASBとは？シャドーITも把握するクラウド時代のセキュリティ対策，マカフィー公式ブログ，2018年3月14日，https://blogs.mcafee.jp/whatis-casb-characteristics

※上記参考文献に含まれるURLのリンク先は2018年8月28日時点での存在を確認.

執筆者紹介　三　池　聖　史（Seisih Miike）
1988年日本ユニシス(株)入社．2004年ユニアデックス(株)転籍．ユニアデックス転籍後は，セキュリティコンサルやセキュリティ製品の主管業務に従事．現在は，ITO戦略推進部に所属し，セキュリティ関連サービスの企画を担当．