クラウドサービス利用における安全・安心の確保

佐々木 大地

1. はじめに

2020年頃より世界中に拡大した新型コロナウイルス感染症（COVID-19）の影響により，私たちは在宅での仕事を余儀なくされ，テレワークの導入とともにクラウドサービスを利用する企業も急激に増えていった．Microsoft Azure®（以降，Azure）やAmazon Web Services®（以降，AWS），Google Cloud Platform®（以降，GCP）といったパブリッククラウドサービスや様々なSaaSサービスは，毎日出社せずともどんな場所からでも仕事ができる環境を私たちに与え，またシステム開発においてもオンプレミスと比較にならないスピードで柔軟性と拡張性のあるシステムを市場に提供できるようになった．その一方で，クラウドサービス利用者のセキュリティ対策の欠如によって，日々多くのセキュリティ事故が発生している．

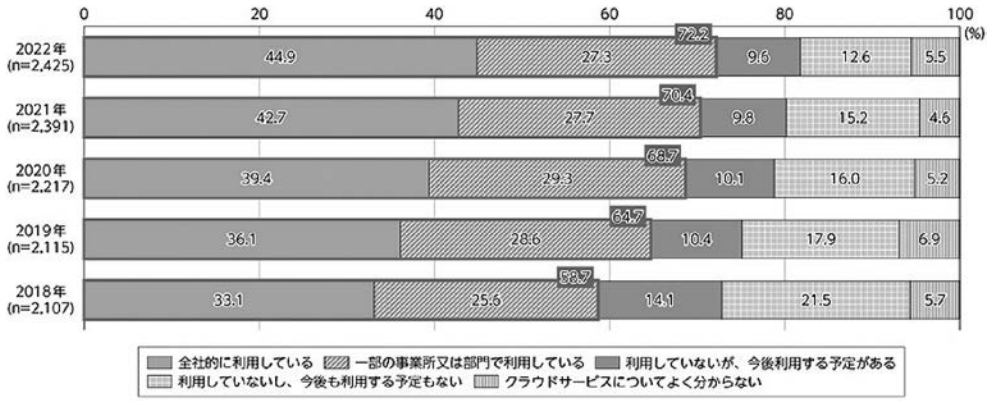
本稿では，クラウドサービスを利用者が安全・安心に利用するために考慮すべき点と対策について，具体的な方法やサービスを挙げながら説明する．2章でクラウドサービスの現在の普及状況とセキュリティ事故状況について統計データを踏まえて確認し，3章ではクラウドサービスを安全・安心に利用する上での考慮点について，様々な機関から公開されている有用な文書の内容を紹介しつつ説明する．4章では，ツールやサービスを用いた対策方法と，そのメリット・デメリットを述べる．

2. クラウドサービスの普及とセキュリティ事故

クラウドサービスが急激に広まり，社会経済活動を支えるICT基盤となった一方，利用する上でのセキュリティ対策の欠如により，事故も多く発生している．本章では統計データから現在の国内でのクラウドサービスの普及状況を確認し，またセキュリティ事故の具体例について述べる．

2.1 普及状況

図1は総務省の「情報通信白書令和5年版 データ集」[1]，図2は総務省の「令和4年通信利用動向調査報告書」[2]から引用したデータである．企業におけるクラウドサービスの利用状況（図1）を見ると，部分的にでもクラウドサービスを利用している企業は2022年時点で72.2%となっており，新型コロナウイルスの感染拡大前である2019年の64.7%と比較して7.5%増加している．次に，産業分類別に見ると，「利用している」の割合は，情報通信業（93.1%），および金融・保険業（91.7%）では90%を超えており，建設業（84.5%），および不動産業（83.6%）では80%以上となっている[*1]．



	集計企業数	比重調整後集計企業数	クラウドサービスの利用状況							
			利用している	全社的に利用している	一部の事業所又は部門で利用している	利用していない	利用していないが、今後利用する予定がある	利用していないし、今後も利用する予定もない	クラウドサービスについてよく分からない	無回答
全体	2,428	2,428	1,749	1,087	662	539	233	306	134	6
[産業分類]										
建設業	368	102	86	55	31	14	8	6	2	−
製造業	387	639	455	271	183	153	85	68	28	4
運輸業・郵便業	408	227	145	77	67	70	30	40	12	−
卸売・小売業	364	489	377	245	133	91	35	55	21	−
金融・保険業	165	29	27	21	6	2	1	1	0	−
不動産業	159	38	32	25	7	4	1	3	2	−
情報通信業	257	132	123	101	22	9	5	4	1	−
サービス業、その他	320	772	505	293	213	197	68	129	68	2

出典：情報通信白書令和5年版 データ集（総務省）[1]

図1　企業におけるクラウドサービスの利用状況

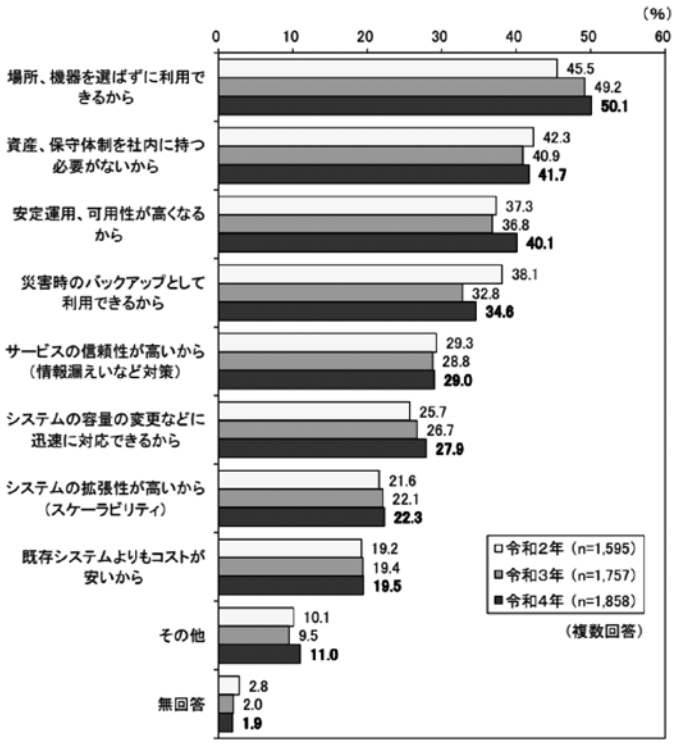
次に，クラウドサービスを利用している理由（図2）を見ると，「場所，機器を選ばずに利用できるから」が50.1%と最も高く，「資産，保守体制を社内に持つ必要がないから」が41.7%，「安定運用，可用性が高くなるから」が40.1%と続く．このように総務省のデータからも，クラウドサービスが情報通信業以外の業種にも広まり，利用率が高まっていることがわかる．

2.2　セキュリティ事故

セキュリティ事故の件数は年々増加しており，東京商工リサーチの調査によると，個人情報漏えい・紛失事故は2021年と2022年の2年連続で発生者数・件数ともに過去最多を記録[3]している．ここ数年での個人情報漏えい・紛失事故の発生者数・件数の増加は，近年のクラウドサービスの急激な広まりと無関係ではないだろう．本節では，具体的にどういった事故が発生しているかを述べる．

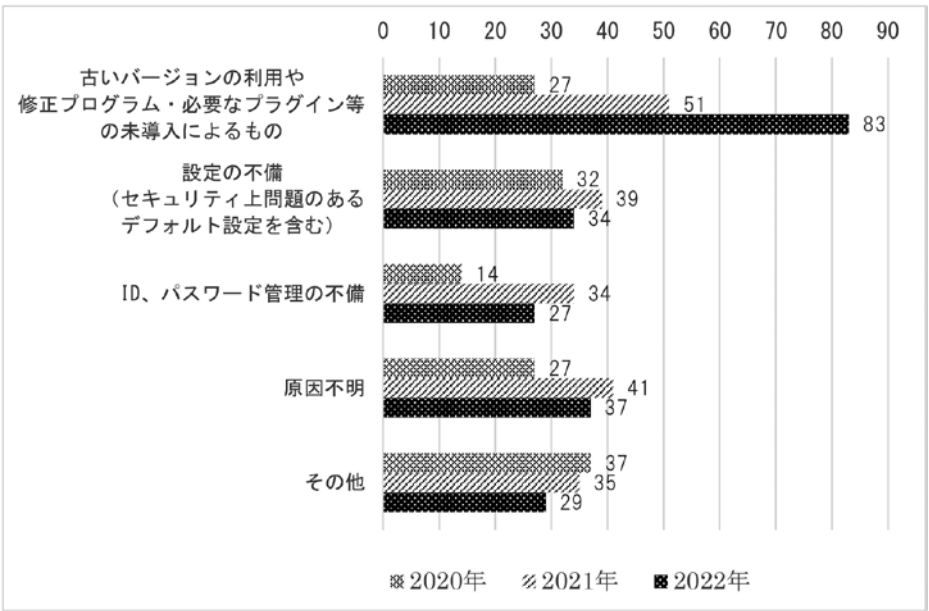
2.2.1　設定不備

クラウドサービス利用者の設定不備により，顧客の機密情報の流失のおそれに至る事案が増加している．図3は独立行政法人情報処理推進機構（以降，IPA）の「コンピュータ



出典：令和 4 年通信利用動向調査報告書（総務省）[2]

図 2　クラウドサービスを利用している理由



コンピュータウイルス・不正アクセスの届出状況［2022 年（1 月～ 12 月）］（IPA）[4]の図 2-6 を基に加工

図 3　不正アクセス原因別件数の推移（2020 ～ 2022 年）

ウイルス・不正アクセスの届出状況［2022年（1月～12月）］[4]」から引用してグラフを加工したものである．不正アクセスの原因別比率では，「設定の不備」が原因別比率で第2位となり，セキュリティ事故を起こす大きな要因となっている．

設定不備により発生した事故の具体例を挙げると，2020年頃にSalesforce® で問題となった事例がある．セールスフォース・ドットコム社で提供しているSalesforceが機能変更を行ったことに起因して，当該SaaSのユーザーアクセスに関する設定で，結果的にデフォルト値のセキュリティレベルが下がった．この機能変更について認識せずに，多くの利用者が低いセキュリティレベルのまま利用したことで，利用者の機密情報が流出した．

他には，パブリッククラウドサービスのストレージを公開設定にしていたことにより，長期間機密情報が公開され続けていた事例や，従業員が個人的に利用していたSaaSサービスが誤って公開設定になっていたことにより機密情報が流出した事例もある．

2.2.2　サイバー攻撃やアカウント情報の管理不備

サイバー攻撃やアカウント情報の管理不足による流出などによって，部外者がクラウドサービスに不正アクセスして情報が盗み出される事故が発生している．サイバー攻撃の例では，Office 365® に対するサイバー攻撃の事例がある．サイバー攻撃者がパスワードスプレー攻撃[*2]といった手法を使って，Office 365に不正にログインし，機密情報を窃取する事故が多く発生した．アカウント情報の管理不足の例では，パブリッククラウドサービスのアクセスキー漏洩による事例がある．これは，アクセスキーが書かれたソースコードを誤ってGitHub® にアップロードした等が原因で発生する事故である．近年頻出している事故であり，著名な企業でも2020年にはサイバーエージェント[*3]で，2022年にはトヨタ自動車[*4]で発生している．

2.2.3　内部不正

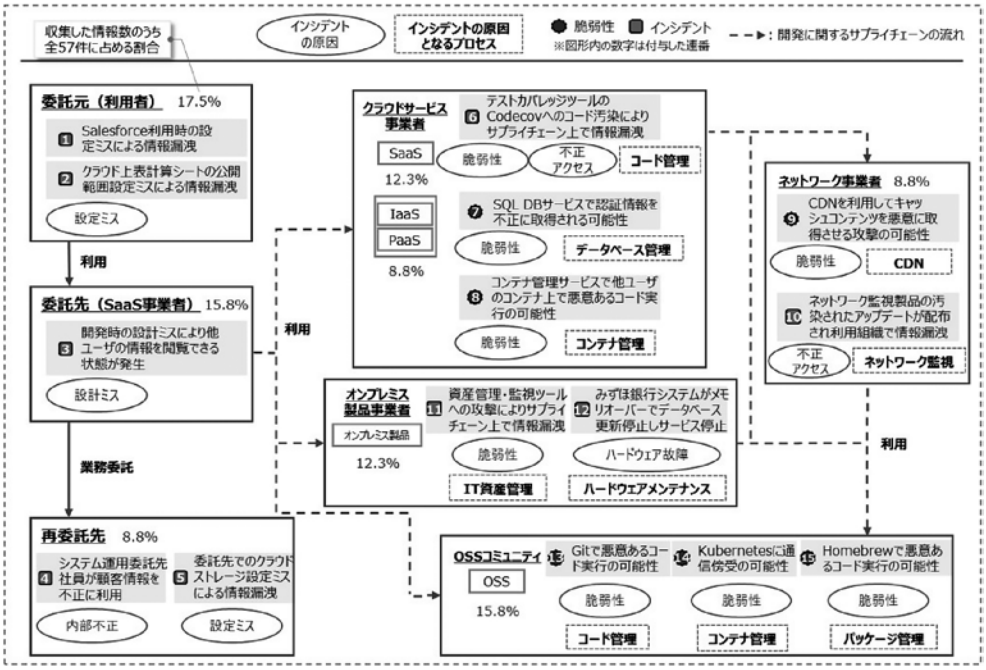
事業者の社員が顧客の情報を盗み悪用または情報流出（内部不正）させて事故が発生するケースもあり，こちらも頻出している．インターネットに繋がってさえいれば，どこからでもアクセスできるというクラウドサービスの性質上，内部不正を起こさないようにするためには，最小特権の原則[*5]を意識したアクセス権限や，退職者等の不要なアカウントを直ちに削除するといったアカウント管理を適切に行うことが重要である．

3.　クラウドサービスを安全・安心に利用する上での考慮点

本章では実際の統計データやガイドラインを参考に，クラウドサービスを安全・安心に利用するうえで考慮すべきポイントを述べる．

図4はIPAによる「クラウドサービスのサプライチェーンリスクマネジメント調査」の「SaaSに係るITサプライチェーン上のリスク所在のイメージ」[5]から引用したデータである．これは，SaaSに係るITサプライチェーンの図の中にIPAが収集したインシデントの原因や，原因となるプロセスを埋め込んだもので，SaaSに係るITサプライチェーン上でどのような箇所がリスクとなりやすいかを明らかにするために整理した図である．

割合を見ると「委託元（利用者）」が原因となっているものが17.5%と最も高く，そのインシデントの原因は「設定ミス」である．また他の「委託先（SaaS事業者）」，「再委託先」といったクラウドサービスを利用する組織のインシデントの原因を見るとこちらも「設定（設計）ミス」が原因としてある．一方，利用される側の原因をみると「脆弱性」「不正アクセス」が大半を占めている．これはクラウドサービス利用者の立場で見ると，提供者側が適切なセキュリティ対策や管理によって「脆弱性」「不正アクセス」等のインシデントに対処していることを確認した上で利用することが賢明であると解釈できる．



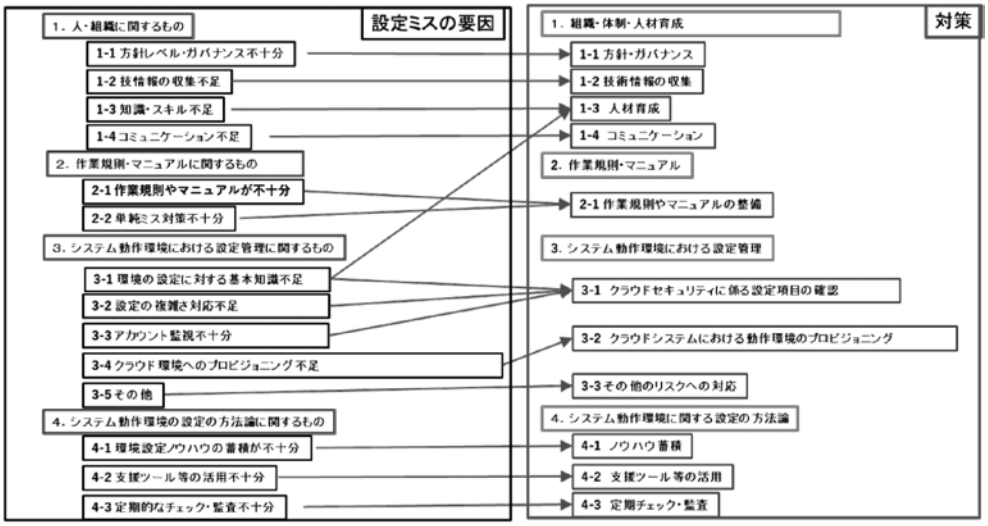
出典：クラウドサービスのサプライチェーンリスクマネジメント調査（IPA）[5]

図4　SaaSに係るITサプライチェーン上のリスク所在のイメージ

3.1　クラウドサービスの設定不備

クラウドサービス利用者のインシデントの原因としてクラウドサービスの設定不備が大きな原因の一つとなっていることが分かった．本節では具体的にどう防げばよいのかを見ていく．総務省が公開している「クラウドサービス利用・提供における適切な設定のためのガイドライン」では，安全・安心なクラウドサービスの利用・提供に資することを目的として，利用者・事業者双方において共通的に認識しておくべき事項及び具体的な対策を整理し，取りまとめている[6]．このガイドラインでは，クラウドサービス利用者に対してヒアリング調査を行った結果から「設定ミスの要因」についてまとめられており，利用者側の対策を導出したものがある（図5）．

各対策についての詳細とベストプラクティスについては，同ガイドラインを参照いただきたい．本節では同ガイドラインの「3−1 クラウドセキュリティに係る設定項目の確認」



出典：クラウドサービス利用・提供における適切な設定のためのガイドライン（総務省）[6]

図5　クラウドサービス利用側の要因と対策の関係

に焦点を当てる．そこにはセキュリティ設定項目の類型とその対策が表1のようにまとめられており，具体的にどういった項目に対して設定不備の対策を実施するかを検討するうえで大変参考になる．

表1　クラウドにおけるセキュリティ設定項目の類型と対策

No.	セキュリティ設定項目の類型	類型項目における推奨設定の概要
1	IDとアクセス管理（IAM）	IDとアクセス管理とは，「誰が」「どのリソースに対し」「どのような操作ができるか」を定義し，アクセス制御を実現するために提供されているサービスである． 管理者はクラウド全体のセキュリティに関与するため，管理者アカウントとユーザアカウントを分離し，管理者アカウントには多要素認証を必須にする等の設定を確実に行うほか，組織の要件に応じてユーザアカウントのIPアドレス制限など各種設定を確実に行う必要がある．特にゲストユーザーについては，不要な情報公開を避けるため，必要最小限の権限とする．また，暗号化キーは統合管理サービスで集中管理することを推奨する．なお，管理者がIDとアカウントを網羅的に把握する仕組み（申請ベースで中央での払い出し，CASBによる新規アカウントの個別発行不可等）を設ける必要がある．
2	ロギングとモニタリング	ロギングは，クラウドにおける挙動やアラート発報の基本となるものである．デフォルトでは，アクティブになっていないサービスもあるので，適切にロギング設定を行い，アラートや監査を行えるようにしておく必要がある．
3	オブジェクトストレージ	クラウド利用におけるオブジェクトストレージのセキュリティでは，データの外部漏えいに備えて暗号化等が基本となるが，暗号化キーの管理方法なども重要となる．また，オブジェクトストレージの公開設定などデフォルト値も確認しておく必要がある．
4	インフラ管理	

4.1	仮想マシン（VM，VPS）	物理サーバを論理的に分離する仮想マシンを利用する際，仮想マシンのディスク暗号化，エンドポイント保護などの設定を確実に行う必要がある．また，ホスト OS，ゲスト OS 等の最新パッチ，ウイルス対策（AV，EDR 等）の設定及びその監視・運用（MDR，SOC 等）についても留意する必要がある．
4.2	ネットワーク	クラウド利用は，インターネット経由となるため，外部ネットワークとのアクセスに関する基本的なセキュリティ設定，仮想プライベートクラウドのセキュリティ設定，Firewall/IPS/IDS や WAF などによる境界防護および境界内防護等に関する設定を確実に行う必要がある．加えて，重要情報を扱うシステムでは，信頼できる VPN による通信の暗号化などのネットワークセキュリティ対策を検討する．
5	セキュリティ等の集中管理	IaaS/PaaS が提供するセキュリティ集中管理機能，キーマネジメントサービス，運用管理コンソール，監査ツール，コスト管理サービスなど，構成管理を横断的に集中管理可能なツールやサービスを積極的に利用することを推奨する．これらはデフォルトでは有効化されていない場合があるため，有効化のための設定確認を推奨する．
6	IaaS/PaaS が提供する，その他のサービスや機能 ※短期間に新たなサービスや機能が追加されることがあるため，下記の項目以外にも追加された時点で，設定値についても確認を行う必要がある．	
6.1	鍵管理	鍵管理は安全に秘密鍵を管理・作成・制御する方法を提供する．暗号化鍵の管理に係る設定については，ID とアクセス管理，ロギングとモニタリング等とも関連し，集中管理するサービスを提供するクラウドもある．使用するクラウドに応じた適切な設定がある．
6.2	PaaS が提供するアプリケーション	クラウドで提供されるアプリケーションには様々なものがあるが，個々の事業者から提示されるアクセス許可などの設定やデフォルトの公開範囲等の設定を確実に行う必要がある．
6.3	データベース	クラウドで使用するデータベースの保護，監査，暗号化などの設定及びデフォルト設定値の確認を確実に行う必要がある．
6.4	コンテナ	コンテナとは，ホスト OS 上で「コンテナエンジン」と呼ばれるシステムを動作させ，「コンテナ」と呼ばれる実行環境を複数構築する技術である．コンテナを利用する際は，コンテナエンジンに係るセキュリティ関連の設定を確実に行う必要がある．
7	その他の設定項目	上記以外のクラウドサービス事業者が提供する統合資産管理，モバイルデバイス管理等のサービスについては，個々の事業者から提示されるセキュリティ設定を確実に行う必要がある．また，これらはデフォルトでは起動していないことが多いので，起動のための設定値を確認することを推奨する．

出典：クラウドサービス利用・提供における適切な設定のためのガイドライン（総務省）[6]

また，特に重要な設定項目として，以下の 4 項目を挙げている．いずれも「ID とアクセス管理」に関わるものであり，優先度を高くして対策することが肝要である．

- ユーザアカウントの管理においては，パスワード設定の厳格化や多要素認証の設定を行う．
- 管理者や特権アカウントの管理においては，①多要素認証，②複数人でのチェック体制をとる．
- 管理者や特権アカウントについては，認証，アクセスログ及び設定変更等のログ監視を行う．

・特権アカウント利用者や特権昇格可能なアカウントは，最小限とすることが望ましい．

より具体的なクラウドサービスの推奨設定を確認する方法として，総務省が表1の作成時に参考にした，CIS[*6]（Center for Internet Security）が発行している CIS Benchmarks というベストプラクティス集が有効である．このベストプラクティス集では Azure，AWS，GCP といったパブリッククラウドや Microsoft 365® といった SaaS サービス等，各クラウドサービスに沿ったセキュリティ設定の推奨策がまとめられている[*7]．

3.2　クラウドサービスの信頼性

本節では，クラウドサービス提供者がセキュリティ対策や管理を適切に実施しているかどうか，取り扱うデータに適したコンプライアンスを満たしているかどうかを，利用者が確認する方法について述べる．そのひとつに，クラウドサービス提供者が取得している認証を確認する方法がある．例えば，個人情報保護の管理策を確認する場合は，P マークや ISMS 認証がある．さらにクラウドサービス固有の管理策（ISO/IEC 27017）が適切に導入，実施されていることを認証する場合は，ISMS クラウドセキュリティ認証の取得状況を確認するとよい．また政府が活用するクラウドサービスのセキュリティを評価する制度として ISMAP があり，ここに登録されているクラウドサービスは，政府機関が要求するレベルの情報セキュリティ対策が実施されていると判断できる．国際的には，「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」の指標の内部統制を評価する SOC2 や米国政府機関のクラウドセキュリティ認証制度である FedRAMP がある．

企業によってはクラウドサービスを利用するにあたって，自社のセキュリティポリシーを遵守できるかどうか確認するため，企業独自のセキュリティチェックシートをクラウドサービス提供者側に記入してもらう運用を行っている．このチェックシートを作成する際の参考になる文書として，総務省の「クラウドサービスの安全・信頼性に係る情報開示指針」や，経済産業省の「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」がある．また国際的にはクラウドセキュリティアライアンス（CSA）が「CCM/CAIQ」というチェックシートを公開して，利用されている．ただし，このようなチェックシートは確認項目が多く，利用する企業側もクラウドサービス提供側も作業負荷が高くなることが多い．同様に，チェックシートの更新も作業負荷が高くなるため，最新のセキュリティや関連法を取り入れられずに古いまま使い続けることも想定される．

チェックシートで確認したクラウドサービス導入後の継続的な評価をどうするかといった課題もある．そのため，各クラウドサービスのリスク評価を代替して行い，データベース化してクラウドサービス利用者にセキュリティ情報を開示するサービスが市場に出始めている（4章で説明）．

4.　クラウドサービスを利用する上でのセキュリティ対策

3章ではクラウドサービスを利用する上での考慮点をあげたが，これらの対策を利用者側ですべて対処することは，リソースの関係上，難しい場合が多い．そのため，ツールや

サービス等を使って，より効率的に対処することが現実的である．本章では，具体的にどういったツールやサービスがあり，それぞれどのようなメリット・デメリットがあるのかについて述べる．

4.1　パブリッククラウド

パブリッククラウドサービスを利用する際のセキュリティ対策として，三つの方法がある．一つ目は，パブリッククラウドサービス自体に備わっている機能を利用する方法である．主要なパブリッククラウドサービスには，現在の設定に不備がないか，また様々なコンプライアンスに適合しているかを，それ自体で確認する機能が存在している．例えば，AWS では「AWS Security Hub」，Azure では「Microsoft Defender for Cloud」，GCP では「Security Command Center」が該当する．これらのサービスは安価であることが多く，ポータル上の操作だけで簡単に利用を開始できる利点がある．またサービスを利用している限りは継続的にセキュリティ状況を確認することができる．ただし，UI や機能等が頻繁に更新され，時にはサービス名称まで変更となることがあるため，利用者は常に最新の情報を追って仕様を把握しておかなければならない．そのため，利用しているパブリッククラウドサービスをある程度使いこなし，熟知していることが求められる．

二つ目は，パブリッククラウドサービスの設定不備がないかツールで確認する方法である．この方法の利点はパブリッククラウドサービスのアカウント（サブスクリプション）を所有していなくても，ツールとパブリッククラウドサービスのユーザを連携して，そのパブリッククラウドサービスの API 等を活用することで確認できる点である．これにより，パブリッククラウドサービスを管理する者とツールを実行する者とで役割分担がしやすくなる．例えばクラウドセキュリティを管轄する部署が，企業内でそれぞれ管理されているクラウドサービスを，ツールを通して一元管理することができる．他にも確認結果のレポートを出力できる．具体的には「Nessus®」や「Prisma® Cloud」等がある．

三つ目は，企業が提供しているサービスを利用して，パブリッククラウドサービスの設定状況を確認する方法である．こちらの利点は，具体的な対処方法や脅威等がまとめられた報告書を得ることができ，不明な点はサービスの実施担当者に問い合わせることができる点である．パブリッククラウドのサービスやツールを自社内で使いこなすことが難しい場合はこのようなサービスを利用すると対処しやすいだろう．BIPROGY 株式会社（以降，弊社）でも「iSECURE® 脆弱性診断サービス」として「クラウド診断サービス」を提供している[7]．

4.2　SaaS サービス

SaaS サービスについてもパブリッククラウドと同様，それ自体に確認するサービスがついており，そのサービスを使って確認する方法，ツールで確認する方法，企業が提供しているサービスで確認する方法がある．ただし SaaS サービスは数多くの種類があり，CIS Benchmarks のように，セキュアな設定の基準となるベストプラクティスが公開されている SaaS サービスは，世界的に広く使われており設定不備があった場合にリスクが大

きいSaaSサービス（Microsoft 365やSalesforceなど）に限られる．そのため，ツールやサービスの対象もそういったベストプラクティスのあるSaaSサービスが対象となることが多い．具体的なベストプラクティスがないSaaSサービスの設定不備を確認する場合は，3.1節のガイドライン等を参考に設定を確認するか，企業が提供しているサービスを利用することになる．企業が提供しているサービスには，対象SaaSサービスのラインナップになくても，他クラウドサービスの設定確認のノウハウを活かして設定状況を確認できる場合があるため，活用するとよい．

4.3　設定不備への対策（まとめ）

ここまで，クラウドサービスの設定不備を確認するための効率的な対策について三つの方法を紹介してきた．それぞれの対策についてメリット・デメリットを表2にまとめた．利用しているクラウドサービスをある程度使いこなしており，サービス自体に設定を確認する機能が備わっていれば，まずはその機能の利用を検討してみるとよい．あまり使いこなせていない，サービス自体に機能が備わっていない，または確認後に手厚いサポートが欲しい場合は，企業が提供しているサービスの利用を検討してみるとよい．さまざまなクラウドサービスを一元管理したい，クラウドサービスを管理している部隊とは別の要員が確認したい場合は，ツールの利用を検討してみるとよい．

表2　パブリッククラウド・SaaSサービスの設定不備を確認する効率的な対策についてのメリット・デメリット

設定不備への対策	メリット	デメリット
クラウドサービス自体に備わっている機能を利用	・ポータル上の操作のみで簡単に利用できる． ・利用している限りは継続的に確認できる． ・他の対策と比較して安価になることが多い．	・サービスの仕様変更も多く，使いこなすにはそのクラウドサービスをある程度熟知しておかなければならない． ・機能が備わっていないクラウドサービスも多い．
ツールを利用	・アカウント（サブスクリプション）を所有していなくても，クラウドサービスとユーザ等を連携することで確認ができるため，作業の役割分担ができる． ・様々なクラウドサービスを一元管理することができる． ・ツールが自動作成したレポートを出力できる．	・利用者側でツールの設定やユーザ連携等の設定等を行うため，多少作業・学習コストがかかる． ・継続して確認できるツールは高価なものが多い．
企業が提供しているサービスを利用	・サービス提供側が主導となって実施するため，利用者側の作業コストが低い． ・具体的な対処方法や脅威等が記載された報告書が提供され，結果についての具体的な問い合わせができることが多いため，利用者側で対処がしやすい． ・他の対策では対応していないクラウドサービスでも設定確認できる場合がある．	・他の対策と比較して高価になることが多い（継続的に確認するサービスではより高価になる）．

4.4　クラウドサービスの信頼性の確認と管理

クラウドサービスの信頼性の確認について，3章でも紹介した通り，様々なガイドラインを参考に企業ごとにチェックシートを作成して運用しているケースがあるが，様々な課題もある．例えば，企業内で多くのクラウドサービスを確認する場合はリソースの関係上確認が追いつかなくなる，チェックシート自体が更新されず陳腐になってしまう，既に確認したクラウドサービスの信頼性については継続的に確認できていない等がある．そのため，各クラウドサービスのリスク評価を代替して行い，データベース化してクラウドサービス利用者にセキュリティ情報を開示する支援サービスが登場している．具体的には「Assured」や「Conoris®」といったサービスがある．

また信頼性の評価を行った後は，シャドーIT[*8]を防ぎ，企業内で利用されているクラウドサービスを管理しなければならない．クラウドサービスの利用を可視化して管理するサービスとして，CASB（Cloud Access Security Broker）がある．なお，利用を可視化することに加えて，企業で定めたポリシーに準じてコンプライアンスを管理する機能や，データの改ざんの検知やアクセス権限の設定を行う機能，不審な行動やマルウェア等の脅威を検知する機能を持つ．具体的には「Skyhigh CASB」や「Netskope® CASB」といったサービスがある．

5. お　わ　り　に

様々なクラウドサービスが登場し，そのサービスの利便性や導入後の効果の高さについては大きく宣伝されているが，サービスのセキュリティ対策については広く知られていないこともある．クラウドサービス利用者がクラウドサービスの信頼性を正確に判断し，実際に利用する際にはどのようにセキュリティを維持して運用していくかを考慮しないと，本稿で述べたようなセキュリティ事故に直面することになる．これは言葉にすると簡単ではあるが，実践するのは弊社を含め容易ではない．組織のプロセスを継続的に見直し，完備性を高めていくことが肝要である．本稿は一貫してクラウドサービス利用者の視点で，どうすればクラウドサービスを安全・安心に利用できるかについて述べた．本稿がクラウドサービスを安全・安心に利用するための一助になれば幸いである．

最後に，本稿の執筆にあたりご助言とご指導を頂いた方々に，この場を借りて深く御礼申し上げる．

＊1　「利用している」を「比重調整後集計企業数」で割った値．情報通信業（123/132），金融・保険業（27/29），建設業（86/102），不動産業（32/38）．

＊2　パスワードスプレー攻撃とは，アカウントを乗っ取る攻撃手法の一つで，多数のアカウントに対してよく利用されるパスワードでログインを試みる手法．アカウントロックを回避しながら攻撃を行う．

＊3　https://www.cyberagent.co.jp/news/detail/id=24503

＊4　https://global.toyota/jp/newsroom/corporate/38095972.html

＊5　アクセス権限の運用についての原則の一つ．必要最低限の権限しか与えないようにすること．

＊6　米国国家安全保障局（NSA），国防情報システム局（DISA），米国立標準技術研究所（NIST）等の政府機関と，企業，学術機関等が協力して，インターネット・セキュリティ

標準化に取り組む目的で設立された米国の非営利団体のこと．

＊ 7　CIS Benchmarks の例
「CIS Amazon Web Services Foundations Benchmark v2.0.0」の場合
1.5 Ensure MFA is enabled for the ‘root’ user account.
訳：「root」ユーザアカウントで多要素認証が有効になっていることを確認する．

＊ 8　シャドー IT とは，企業が使用を許可していない，あるいは従業員が利用していることを企業側が把握できていないデバイスやシステム，クラウドサービスなどのこと．

参考文献

［1］ 情報通信白書令和 5 年版 データ集，総務省，2023 年 7 月，
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html

［2］ 令和 4 年通信利用動向調査報告書，総務省，2023 年 5 月 29 日，
https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202200_002.pdf

［3］ 個人情報漏えい・紛失事故 2 年連続最多を更新 件数は 165 件，流出・紛失情報は 592 万人分 ～ 2022 年「上場企業の個人情報漏えい・紛失事故」調査 ～，東京商工リサーチ，2023 年 1 月 19 日，
https://www.tsr-net.co.jp/data/detail/1197322_1527.html

［4］ コンピュータウイルス・不正アクセスの届出状況［2022 年（1 月～ 12 月）］，独立行政法人情報処理推進機構，2023 年 2 月 8 日，
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108005.pdf

［5］ クラウドサービスのサプライチェーンリスクマネジメント調査，独立行政法人情報処理推進機構，2022 年 5 月 31 日，
https://www.ipa.go.jp/security/reports/economics/scrm/ug65p90000019cza-att/000096929.pdf

［6］ クラウドサービス利用・提供における適切な設定のためのガイドライン，総務省，2022 年 10 月，
https://www.soumu.go.jp/main_content/000843318.pdf

［7］ iSECURE 脆弱性診断サービス，BIPROGY，
https://www.biprogy.com/solution/service/vulnerability_diagnosis.html

※　上記注釈および参考文献に含まれる URL のリンク先は，2023 年 10 月 3 日時点での存在を確認．

執筆者紹介

佐々木　大地（Daichi Sasaki）
2018 年日本ユニシス(株)に中途入社．入社後，脆弱性診断，クラウドセキュリティ，セキュリティコンサル等の業務を担当．情報処理安全確保支援士，CISSP．