クラウドサービス（SaaS）の
サプライチェーンリスクマネジメント実態調査

調査報告書

独立行政法人　情報処理推進機構

<白紙>

目次

本編

1. はじめに

1.1 調査の背景・目的

独立行政法人情報処理推進機構（以下「IPA」）では、IT システム・サービスの業務委託（以下「IT サプライチェーン」）におけるセキュリティの向上を目的とし、2017 年から IT サプライチェーンにおけるセキュリティの責任範囲の調査を行ってきた。2021 年度に実施した「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」（以下「2021 年度クラウド調査」）[1]では、サービスの業務委託として SaaS[2]に重点をおき、インシデント情報の収集と分析および今後の課題などを調査し、いくつかの今後深堀すべきポイントを得た。1 つ目はセキュリティ情報開示の慣習の確立、そして 2 つ目として SaaS 利用者への安全な利用方法の周知と案内が挙げられた。

そこで、2022 年度は、SaaS 事業者（以下「事業者」）や SaaS 利用者（利用を行う者または利用を検討している者。以下「利用者」）がセキュリティ対策の検討や実施を行うための一助とするために、「SaaS のセキュリティを保証する情報開示」および「セキュリティの高い状態で SaaS を利用してもらうための情報提供」について実態を調査することとした。

本調査では、SaaS のサプライチェーンにおけるセキュリティに関する情報の「情報開示」と「情報利用」の実態について、どのような取り組みを、どのような組織がどれくらい実施しているかなどのアンケート調査を行い、有識者へのインタビュー調査を踏まえて、事業者と利用者の間の、認識の違いによる脅威やリスク、課題などについて考察を行った。

なお、本調査における「情報開示」とは、事業者がセキュリティに関する情報を約款・利用規約・Web、サービス画面、電子メール／pdf ファイル等で情報提供する（例：マニュアル、障害情報、主要指標の統計実績、サービス変更／終了の告知など）、または要望があった場合に提示することを指し、「情報利用」とは、利用者が事業者の開示した情報を入手し、SaaS の安全な利用に資するために情報を活かすことを指すものとする。

[1] https://www.ipa.go.jp/security/economics/scrm/index.html
[2] Software as a Service（サービスとしてのソフトウェア）の略。クラウドサービスの提供形態の一つで、インターネット経由で利用者にソフトウェアパッケージを提供する。

1.2 クラウドサービスが抱えるセキュリティの課題

1.2.1 SaaS の利用拡大に伴うセキュリティの懸念

通信技術の高度化やネットワークインフラの整備により、現在、我が国のクラウドサービスの利用は急激に進みつつある。2018 年 6 月に日本政府が発表した「政府情報システムにおけるクラウドサービスの利用に係る基本方針[3]」において、情報システムを導入する際にクラウドサービスの活用を推進する方針が示され、コスト削減や柔軟なリソースの観点から、行政分野でも「クラウドサービスの利用を第一候補として、その検討を行う」クラウド・バイ・デフォルトの考え方が定義された。

一般的にクラウドサービスは、その提供形態によって「IaaS[4]」「PaaS[5]」「SaaS」の 3 タイプに分けられるが、2020 年 4 月の緊急事態宣言[6]の発出を契機に一気に利用が拡大したのが SaaS である。業務実施場所の多様化や、コミュニケーションのオンライン化など、テレワークの普及による働き方の変化は定着しつつあり、その中で SaaS の利用が増えている。総務省の「令和 4 年版情報通信白書[7]」によると、2021 年における日本のパブリッククラウドサービス市場規模は 1 兆 5,879 億円（前年比 28.5%増）となっている。また、総務省の「令和 3 年通信利用動向調査」[8]では、クラウドコンピューティングサービスを導入している企業の割合は 70.4%となり 7 割を超えている。同調査では、2020 年から 2021 年にかけてテレワーク導入企業が 29.6%から 58.2%へと急激に拡大したことも示しており、場所や機器を選ばない簡便さや、資産・保守体制のアウトソーシング化等がメリットとして認識されている。クラウドコンピューティングサービスの導入が「非常に効果があった」又は「ある程度効果があった」とする企業は、導入企業 全体の 88.2%に上った。テレワークの普及に伴いクラウドコンピューティングの利用が拡大した様子が示されている。一般社団法人日本情報システム・ユーザー協会の「企業 IT 動向調査 2022[9]」では、「クラウド活用状況」の「SaaS の活用」の項目で、売上高 100 億円以上の企業では「従来から実施」「新たに実施」「検討中・今後実施予定」を合わせると 70%を超えている。大手のユーザー企業においても業務における SaaS の利用は一般的になりつつあると言える。

一方で、SaaS の利用拡大により懸念されるのが IT サプライチェーンにおけるセキュリティリスクの増大である。2020 年度に IPA が実施した「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査[10]」（以下「2020 年度ニューノーマル調査」）では、各企業が緊急事態宣言下での業務継続を優先するため、緊急措置として SaaS の利用を認め、その後[11]も利用を継続している組織が一定数存在していることがわかっている。この「2020 年度ニューノーマル調査」では、利用者（委託元）の半数以上がテレワークに関する社内規定・規則・手順の遵守確認を実施し

---

[3] https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf
[4] Infrastructure as a Service（サービスとしてのインフラストラクチャ）の略。インターネット経由でハードウェアリソース（CPU/メモリ/ストレージ）の IT インフラを提供する利用形態。
[5] Platform as a Service（サービスとしてのプラットフォーム）の略。インターネット経由でアプリケーション実行用のプラットフォームを提供する利用形態。
[6] 新型コロナウィルス感染症の拡大を防止するため、我が国史上初の緊急事態宣言が発出され、約 2 か月間に及んで外出自粛が要請施された。
[7] https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/index.html
[8] https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000158.html
[9] 「企業 IT 動向調査 2022」（2021 年 9 月～10 月実施） 一般社団法人日本情報システム・ユーザー協会 https://juas.or.jp/library/research_rpt/it_trend/
[10] https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html
[11] 2020 年 10 月の調査時点

ていないこと、業務委託契約を行う上でのテレワークの導入、BYOD の使用などに関する業務委託契約上の要求事項について検討が進んでいないこともわかっている。

「2021 年クラウド調査」調査報告書でも、SaaS 事業者は自社のサービス開発のために外部へ開発業務の委託を行うことがあり、図 1-2-1 のようにクラウドサービス開発に関わるサプライチェーンは長大で複雑になりやすいことが示されている。

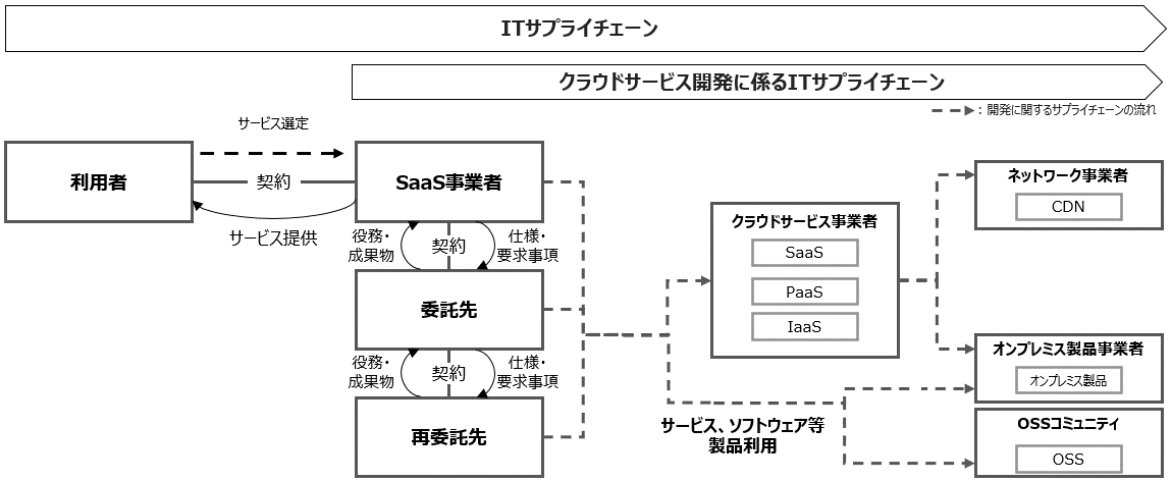


図 1-2-1 クラウドサービス開発に係る IT サプライチェーンのイメージ

（「2021 年度クラウド調査」調査報告書図表 1-3-2）

また、クラウドサービスの中でも SaaS は、IT に関する知識・経験が少ない利用者にも手軽に導入できる反面、SaaS を安全に利用するための知識・経験を獲得することは容易ではない。そのため、選定時のリスク検討が不十分なまま SaaS を導入するケースもあり、機密情報が漏洩する等のインシデントへ発展する可能性がある。近年では委託先がクラウドストレージ上にデータを暗号化せず保存していたことで、多くの個人情報が流出したインシデントも報告されている。

これまで主流であったオンプレミスの情報システムでは、利用者が、情報システムの提供または保守を行う専門の事業者に開発・保守を一任または相互に関わりながら業務を進めていく開発方法が標準的であった。しかしクラウドサービスにおいては急速に分業化・グローバル化が進んでおり、開発環境は大きく変わりつつある。また SaaS では、事業者が構築し、提供しているサービスをそのまま利用するのが一般的であり、利用者のためのカスタマイズサービスは通常は提供されない。このような状況から、SaaS においては事業者と利用者間の情報共有は希薄となっている場合が多くある。

1.2.2 クラウドサービス利用時のセキュリティ対策

オンプレミスの環境で構築されるシステムと、クラウド環境で構築されるシステムでは、セキュリティの前提となる条件が大きく異なる。オンプレミスのシステムでは、組織のネットワークの内外に境界線を設け、そのネットワーク境界線上で通信を監視し不正侵入を防御する「境界型防御」と呼ばれる方式が一般的である。一方、クラウドの環境では、保護すべきデータやシステムが外部のネットワーク上に点在し、「境界型防御」の考え方では対応できない。

SaaS をはじめとするクラウドサービスは、場所やデバイスを選ばずに利用できることが多く、その利便性が最大のメリットとなっているが、その反面、対策を講じるべきネットワーク境界線の位置が曖昧になり、セキュリティ対策面でのデメリットになっている。

このような背景から、クラウドサービスの利用にあたっては、すべての通信を信頼しないことを前提に、さまざまなセキュリティ対策を講じようとする「ゼロトラスト」の考え方が広まっている。デジタル庁が 2022 年 6 月に改定した「デジタル社会の実現に向けた重点計画」[12]においても、機器・アクセス経路等の工程ごとにセキュリティを判断する「ゼロトラストセキュリティ」が提唱されている。

また、情報セキュリティマネジメントシステム（以下、ISMS）の国際規格である ISO/IEC27001 が 2022 年 10 月 25 日に改訂され、以前の版と比較すると、クラウドサービスの利用について必要なセキュリティ対策が明示されている。

ISO/IEC 27001 の改訂により追加された管理策

A.5.7 脅威インテリジェンス(Threat intelligence)
A.5.23 クラウドサービス利用のための情報セキュリティ(Information Security for Use of Cloud Services)
A.5.30 事業継続のための ICT の準備(ICT Readiness for Business Continuity)
A.7.4 物理セキュリティモニタリング(Physical Security Monitoring)
A.8.9 構成管理/コンフィギュレーションマネージメント(Configuration Management)
A.8.10 情報削除(Information Deletion)
A.8.11 データマスキング(Data Masking)
A.8.2 データ漏洩対策/データ流出予防(Data Leakage Prevention)
A.8.16 アクティビティのモニタリング(Monitoring Activities)
A.8.23 Web フィルタリング(Web Filtering)
A.8.28 セキュアコーディング(Secure Coding)

（JIS 版における正式な表記とは異なる可能性があります）

図 1-2-2 ISO/IEC 27001 の改訂により追加された管理策

[12] https://www.digital.go.jp/policies/priority-policy-program/

ISMS の改訂版では、クラウドサービスに関連する情報セキュリティの概念を明確にしており、クラウドサービスに直接関連する箇所として「A.5.23 クラウドサービス利用のための情報セキュリティ」が追加された。管理基準 5.23 は、組織固有の情報セキュリティ要件に関連し、クラウドサービスの取得、使用、管理、および終了に必要なプロセスを概説する新しい管理基準である。この管理基準 5.23 では、組織が「クラウドサービスの利用者」という立場で、クラウドサービスに関連する情報セキュリティの概念をまず特定し、その後管理・運用することを求めている。商用クラウドサービスの範囲内で、情報セキュリティを管理する方針と手順を規定することにより、リスクを維持する予防的な措置を行うための管理策でとなっている。

図 1-2-2 の追加管理策のうち、管理基準 5.23 に加えてクラウドサービスと関連すると考えられる項目は以下の 2 点である。

・「A.8.9 構成管理」のうち、クラウドサービス設定に関連するもの（例えば ID 管理、ログ管理）

・「A.8.10 情報削除」のうち、クラウドサービス終了時の情報の取扱について

このように、SaaS をはじめとしたクラウドサービスの利用にあたっては、これまでオンプレミスでも実施されていたセキュリティ対策に、さらにクラウドサービス固有の要件を考慮した対策を付加することが必要となっている。

1.3 情報開示・情報利用が求められる背景

1.3.1 情報開示・情報利用の必要性

近年、クラウドサービスを利用する企業・組織において、情報の流失に至るインシデントが増加しており、クラウドサービスの利用におけるリスクとして社会的に問題となっている。これらの状況から、安全・安心 なクラウドサービスの利活用を推進するための対策が求められている。

また、組織における一般的な導入手順を踏まず、部門等が独自の判断で SaaS を導入する「シャドーIT」についても問題が指摘されている。シャドーIT に限らず利用者側が安易にクラウドを導入することで起こるセキュリティ事故は増えつつある。CSA が毎年公開している調査レポート「クラウドの重大セキュリティ脅威」では、2019 年以降は利用者側の設定ミスや不注意による情報セキュリティ上の脅威が大半を占めている。[13]

2022 年 7 月 21 日には「Microsoft Teams」等の Microsoft 社が提供するサービス群において障害が発生し、同サービスを利用できない事態が続くというインシデントが発生した。Microsoft 社によると、障害発生時点で日経平均株価を構成する 225 企業のうち 94%が Teams を導入しており、影響は広範囲に及んだという。この障害は復旧までに 5 時間を要したが、対応策を取れず、一時的な業務の中断といった影響を受けた組織と、対応策を講じたために影響が小さかった組織があった。サービスが停止した 5 時間は Microsoft が事前に告知していた SLA 99.99%の補償範囲内であり、利用者は事前に SLA に関する情報を入手し、評価・検討をしていれば、この程度のサービス停止は起こりうると分析できていたはずである。サービスが利用できなくなるリスクを想定して代替手段や対応手順を用意していたか否かにより、事業の継続性に大きな差が生じていたと言える。

IaaS,PaaS,SaaS 等のクラウドサービスは急速に普及しており、利用者によるクラウドサービスの比較・評価・選択等に資する情報に対するニーズが増している。これらのクラウドサービスにおいては、約款・利用規約といった事業者が公表している資料や、事業者に要求することで得られる各種の情報を用いて、利用を検討しているサービスが自社にとって適したものであるのかを判断しなければならなくない。

自社で保有せず、利用するだけであるクラウドサービスの情報システムの場合、利用者が直接セキュリティ対策を管理できないため、どのようなセキュリティ対策が施されているのか、選択や追加が可能なセキュリティ対策があるのかについても、事前に確認しておくことは重要である。

IPA が作成し公開している「中小企業のためのクラウドサービス安全利用の手引き[14]」では、「クラウドサービス安全利用チェックシート」の中で、サービスを選択する際のポイントとしてクラウドサービスの安全・信頼性をチェックするよう指導している。利用者は、それらの情報を収集することにより、サービスが提供する機能に加えて、サービスが停止した際の対応や、事業者が実施しているセキュリティ対策を知ることができるとともに、SaaS のサービスレベルやセキュリティレベルと、自社が求めるサービスレベルやセキュリティレベルとの比較を行い、サービスの導入可否を検討すると共に、サービスが停止した場合の対応策などを事前に検討することができる。

[13] https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2022/11/topthreat_morozumi_20221117.pdf
[14] https://www.chusho.meti.go.jp/koukai/kenkyukai/smartsme/2018/180330smartsme05.pdf

事業者は利用者が適切に選択するための情報提供を行うと共に、利用者から求められる個別の問い合わせについても回答する必要がある。

また事業者は、インシデントが発生した場合に備えて、自社の責任を明確にするためにも情報開示を進めるべきである。インシデントが発生した場合の自社の責任範囲を明確にしなければ、被害の範囲に応じて個別に補償を行う必要性が出てくる可能性がある。さらに SaaS の事業者は、SaaS というサービスを提供する事業者である一方で、IaaS、PaaS といったクラウドサービスの利用者であるケースも多く、IT サプライチェーンの中で複合的な立場にある。事業者は実施しているセキュリティ対策等を明確にするだけではなく、連携しているクラウドザービスや、連携するクラウドサービスに起因するインシデントが発生した場合の対応・補償範囲などについても情報開示することが望ましいだろう。

1.3.2 情報開示・情報利用のあるべき姿

ここまでで提示してきた状況から、事業者・利用者に求められる情報開示・情報利用のあるべき姿について述べる。

（1）情報開示・情報利用の指針

ここまで述べてきたとおり、クラウドサービスは組織の事業継続にとって重要な要素となりつつある。安全・安心なクラウドサービスを利用するためには、利用者は事業者が十分なセキュリティ対策を行っていることを確認する必要があり、その際に事業者から開示された情報を参考にしている。しかし、SaaS を利用する環境や、事業環境は個々に異なる。そのため利用を検討している SaaS のセキュリティに関する情報を入手し、個々の利用環境・事業環境に適したセキュリティ対策が取られていることを確認し、不足があれば必要な対策を検討し、実施する必要がある。

このような背景から、総務省ではクラウドサービスの比較・評価・選択等に資する情報の開示項目として「クラウドサービスの安全・信頼性に係る情報開示指針」[15]（以下「情報開示指針」）」を公表している。また、事業者の情報開示に関する第三者評価のしくみとして、一般社団法人日本クラウド産業協会が「ASP・SaaS の安全・信頼性に係る情報開示認定制度」を設けている他、クラウド関連の業界団体によりクラウドサービスに係わる認証・認定制度が創設されている。

表 1-3-1、表 1-3-2 に、クラウドに関連する主なセキュリティに関するガイドラインとクラウドに関連する主な認証・認定制度を示す。

15 https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000306.html

表 1-3-1 クラウドに関連する主なセキュリティに関するガイドライン（1/2）

資料名／発行者／対象	初版／ 最新版（2023 年 2 月時点）	概要
「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 クラウドサービス事業者	初版：2014 年 4 月 第 3 版：2021 年 9 月	総務省では 2008 年 1 月に「ASP・SaaS における情報セキュリティガイドライン」を策定した。しかし近年では、クラウドサービスはアプリケーション領域（ASP・SaaS）からインフラ領域（PaaS・IaaS 等）に拡大し、単独のクラウド事業者だけではなく、クラウド事業者同士が連携して新たなサービスを提供する形態も増加するなど、サービス提供形態が大きく変化しているため、サービス提供事業者が利用者との間で取り決めるべき合意（責任の分担設定など）を含めた新たなガイドラインとして本ガイドラインが策定された。
「クラウドサービスの利用・提供における適切な設定のためのガイドライン[16]」 総務省 クラウドサービス利用者	初版：2022 年 10 月	クラウドサービスを利用する際の設定ミスに起因する障害や情報漏えいといった事故が多発している。本ガイドラインは、不正アクセスの原因として、設定不備が多い状況にある中で、クラウドサービスの適切な設定の促進を図り、安全安心なクラウドサービスの利活用を推進していくため、推奨されるセキュリティ対策を指針として示している。
「クラウドサービスの安全・信頼性に係る情報開示指針」 総務省 クラウドサービス事業者・利用者	初版：2007 年 11 月 第二版：2018 年 10 月	総務省では ASPIC と合同で設立した「ASP・SaaS・クラウド普及促進協議会」における検討を踏まえて、クラウドサービスに関する情報開示を推進するとともに、利用者によるサービスの比較・評価・選択等を容易にすることを目的として、「クラウドサービスの安全・信頼性に係る情報開示指針」と総称する以下の各情報開示指針を策定し公表している。 【クラウドサービスの安全・信頼性に係る情報開示指針】 ・ASP・SaaS の安全・信頼性に係る情報開示指針[17]（2022 年 10 月改定） ・IaaS・PaaS の安全・信頼性に係る情報開示指針[18]（2011 年 12 月改定） ・データセンターの安全・信頼性に係る情報開示指針[19]（2009 年 2 月策定、2011 年 12 月改定）
「政府情報システムのためのセキュリティ評価制度（ISMAP）[20]管理基準」 ISMAP 運用支援機関 （独立行政法人情報処理推進機構） 内閣サイバーセキュリティセンター（NISC） クラウドサービス事業者	発行：2020 年 6 月 最終改定日：2022 年 11 月	ISMAP とは Information system Security Management and Assessment Program の略で、政府のセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、セキュリティ水準を確保したクラウドサービスの効率的な調達を目指している。

16 https://www.soumu.go.jp/main_content/000843318.pdf
17 https://www.soumu.go.jp/main_content/000843320.pdf
18 https://www.soumu.go.jp/main_content/000475601.pdf
19 https://www.soumu.go.jp/main_content/000138672.pdf
20 https://www.ismap.go.jp/csm

表 1-3-1 クラウドに関連する主なセキュリティに関するガイドライン（2/2）

資料名／発行者／対象	初版／ 最新版（2023 年 2 月時点）	概要
「政府機関等の情報セキュリティ対策のための統一基準群[21]」 内閣サイバーセキュリティセンター（NISC） クラウドサービス利用者	初版：2020 年 7 月	本統一基準群は、国の行政機関及び独立行政法人等において共通的に必要とされる情報セキュリティ対策である。政府機関等の情報セキュリティ対策のため統一規範（サイバー セキュリティ戦略本部 決定）に基づく機関等における統一的な枠組みの中で、統一規範の実施ため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項項を規定することにより、機関等の情報セキュリティ水準斉一的な引上げを図ることを目的としている。
「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」 経済産業省 クラウドサービス利用所	初版：2011 年 4 月 2013 年度版：2014 年 3 月	本ガイドラインは、クラウドサービスの利用者およびクラウドサービス提供者向けのガイドラインで、多くの企業が情報セキュリティの指針として活用している JIS Q27002 の構成を基に作成された。本ガイドラインには、クラウドサービスを安全に利用するために、クラウドサービス利用者が気をつけることやクラウドサービス提供者が開示すべき情報が記載されている。
「中小企業の情報セキュリティ対策ガイドライン」第 3 版＆付録 6 「中小企業のためのクラウドサービス安全利用のすすめ[22]」 独立行政法人情報処理推進機構 クラウドサービス利用者	初版：2009 年 3 月 第 3 版：2019 年 3 月 ※以降 付録 7 追加等の更新あり	「中小企業の情報セキュリティ対策ガイドライン」は、情報セキュリティ対策に取り組む際の、（1）経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法 をまとめたものである。経営者編と実践編から構成されており、個人事業主、小規模事業者をも含む中小企業の利用を想定している。

[21] https://www.nisc.go.jp/policy/group/general/kijun.html
[22] https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

表 1-3-2 クラウドに関連する主な認証・認定制度

認証制度等／認証団体等	概要	形態
ASP・SaaS（AI クラウドサービス）の安全・信頼性に係る情報開示認定制度[23] 日本クラウド産業協会（ASPIC）	ASP・SaaS（IoT クラウドサービス）の利用を考えている企業や地方公共団体などが、事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定するものである。対象は国内。	第三者認証
CS マーク[24] 日本セキュリティ監査協会(JASA)クラウドセキュリティ推進協議会	日本の特定非営利活動法人日本セキュリティ監査協会(JASA)による情報セキュリティ監査制度で、その認定マークが CS マークである。認証段階にはゴールド(第三者認証)とシルバー(自主監査)があり、レベルや目的に応じて対象を選択できる。対象は国内。	第三者認証（内部監査可）
Fed RAMP[25]（Federal Risk and Authorization Management Program）	米国政府機関がクラウドサービスを調達するにあたって採用している共通認証制度で、製品やサービスに対するセキュリティ評価、認証、継続的監視に関する標準的なアプローチを示している。対象は米国（米国政府機関向けのビジネス)。	第三者認証
政府情報システムのためのセキュリティ評価制度（ISMAP) ISMAP 運用支援機関 （独立行政法人情報処理推進機構） 内閣サイバーセキュリティセンター （NISC）	日本政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度。対象は国内。	第三者認証
ISMAP-LIU ISMAP 運用支援機関 （独立行政法人情報処理推進機構） 内閣サイバーセキュリティセンター （NISC）	政府情報システムのためのセキュリティ評価制度（ISMAP)のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とする制度。対象は国内。	第三者認証
ISMS クラウドセキュリティ認証[26](ISO27001/ISO27017) 国際標準化機構（International Organization for Standardization 略称: ISO）	ISO/IEC 27017:2015 は ISO より発行されたクラウドセキュリティに関する国際規格で、クラウドサービスの提供および利用に関する情報セキュリティ管理のためのガイドラインである。認証取得する際は、前提として ISO/IEC27001 の認証取得が必要なアドオン規格である。対象は全世界。	第三者認証
SOC2,SOC2+[27] 米国公認会計士協会(AICPA)	SOCR (Service Organization Control Reporting) は米国公認会計士協会(AICPA)が定める、委託会社の内部統制やサイバーセキュリティについての内部統制保証報告の枠組みである。対象は米国を含む全世界。	第三者認証
STAR 認証[28]（CSA Security） Cloud Security Alliance（CSA）	セキュリティ成熟度を評価する制度で、ISO/IEC 27001, SOC 2 GB/T 22080-2008 のアドオン規格である。対象は米国を含む全世界。認証にあたっては自己認証から第三者認証まで 3 段階に分けられる。	第三者認証（内部監査可）
Star Audit Certification[29] Euro Cloud Europe (ECE)	クラウドサービス提供事業者の情報、法的事項、セキュリティとプライバシー、データセンター、運用プロセス成熟度、クラウド形態の 6 つの領域に分類し、それぞれ星の数を 3 つから 5 つまでを評価する。対象は欧州を含む全世界。	第三者認証

[23] https://www.aspicjapan.org/nintei/asp-nintei/about.html
[24] https://jcispa.jasa.jp/cloud_security/cs_mark/type_cs_mark/
[25] https://www.gsa.gov/technology/government-it-initiatives/fedramp
[26] https://isms.jp/isms.html
[27] https://www.aicpa.org/topic/audit-assurance/
[28] https://cloudsecurityalliance.jp/
[29] https://staraudit.org/

（2）情報開示・情報利用の対象となる情報

事業者・利用者の双方が情報開示・情報利用を行う際に参考とするべき指針（表 1-3-1 参照）のうち、「情報開示指針」では以下の項目について必須または選択方式のいずれかで開示するよう要求している。項目は多岐にわたるため、ここではカテゴリと情報開示項目 1 のみ抜粋して掲載した。

これらの項目を基に SaaS の情報開示・情報利用を行うことで、安全・安心に SaaS を利用することができると言えるだろう。

表 1-3-3「情報開示指針」に掲載されている項目（カテゴリ・情報開示項目 1 のみ抜粋）

カテゴリ	情報開示項目 1
全般	開示情報の時点
事業所・事業	事業所等の概要
	事業の概要
人材	経営者
	従業員
財務状況	財務データ
	財務信頼性
資本関係・所属団体	資本関係
	所属団体
コンプライアンス	組織体制
	個人情報
	守秘義務
	従業員教育等
	委託
	文書類
サービス基本特性	サービス内容
	サービスの変更・終了
	契約の終了等
	サービス料金
	サービス品質
	契約者数

カテゴリ	情報開示項目 1
アプリケーション等	連携
	セキュリティ
ネットワーク	回線
	セキュリティ
ハウジング（サーバ設置場所）	施設建築物
	非常用電源設備
	消火設備
	避雷対策設備
	空調設備
	セキュリティ
サービスサポート	サービス窓口（苦情受付・問合せ）
	サービス通知・報告

（3）情報開示・情報利用の方法

事業者が情報開示を行い、利用者が情報を収集しただけでは安全な SaaS の利用にはつながらない。利用者は入手した情報に対し、自社のセキュリティ要件と照らし合わせて評価する必要がある。評価したうえで、問題ないことを確認する、もしくは、不足部分についてリスクとして受容するのか、あるいはリスク低減のための対策を検討する必要がある。事業者においても、利用者が利用しやすい形で提供することが必要となる。

「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」[30]（以下「クラウド設定ガイドライン」）では、利用者・事業者に対し以下のとおりの基本的な考え方を述べている。

30 https://www.soumu.go.jp/main_content/000843318.pdf

① クラウドサービス利用者・事業者双方において、クラウドサービスの特性や、クラウドサービスの利用・提供におけるリスクについて認識すること

② クラウドサービス利用者・事業者双方において、自身の責任範囲や役割を理解し、それを共通認識とすること

③ クラウドサービス利用者・事業者間でコミュニケーションを密なものとしつつ、双方における設定不備の抑止・防止の対策を適切に実施すること

また、事業者は情報を提供するためにどのような手段で、どのようなタイミングで届けるのかについても、検討しなければならない。「クラウド設定ガイドライン」では、クラウドサービス事業者は、クラウドサービス利用者が正しく環境の設定ができるように、環境の設定に関する正しく適切な情報をタイムリーに提供する必要がある、とされている。

事業者にとっては利用者が利用しやすい形で情報を提供することが必要であると共に、利用者は情報を基に適切に情報利用を行う必要があるだろう。これらの情報提供の実態、および、情報開示・情報収集の頻度について調査している。調査結果は 4.1、4.2 を参照いただきたい。

（4）責任共有モデル

近年は、クラウドにおける「責任共有モデル」の考え方も広がりつつある。図 1-3-1 は責任共有モデルを図示しており、SaaS の構成要素について、クラウドサービス利用者とクラウドサービス事業者がそれぞれ管理する範囲を示しており、管理範囲に含まれる要素はそれぞれが責任を持つ。

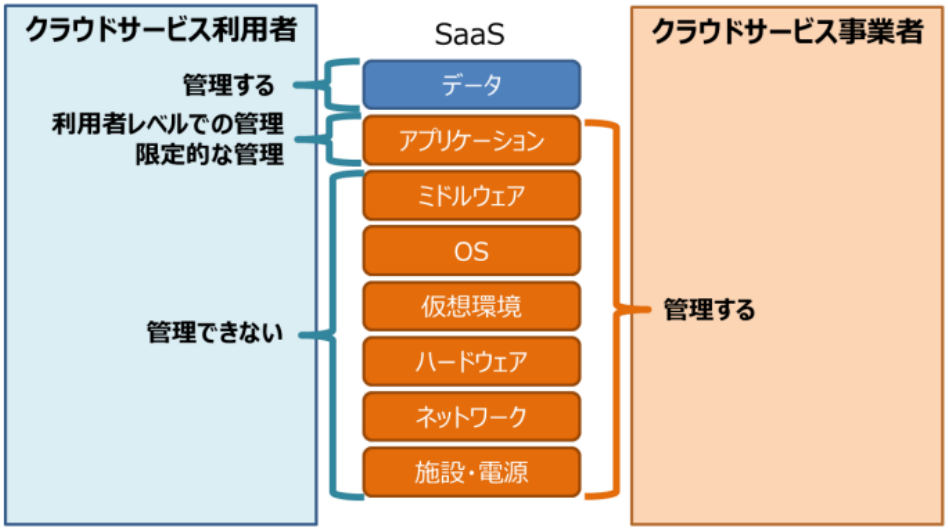


図 1-3-1　責任共有モデル

出所：総務省「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の概要」

「責任共有モデル」において、「クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有することが必要」[31]とされている。ここでは、利用者はリスクを所管する最終的な責任（説明責任）を負っており、事業者にリスク管理の一部を移転しているに過ぎない。事業者は、提供しているサービスの定められた部分に関しては責任を持つが、それ以外については利用者に責任が残っていると考えるべきである。

SaaS をはじめとしたクラウドサービスでは、責任範囲の所在が不明瞭であるためにトラブルが発生する可能性がある。 クラウドサービスでは事業者に運用・保守をすべて任せることができると利用者が認識していることが多く、事業者と利用者の責任範囲の認識のずれとなってトラブルを大きくするおそれがある。株式会社 Legal Force が実施した「SaaS の導入実態調査（2021 年 12 月実施）」[32]では、SaaS 導入理由として「運用保守体制を社内に持つ必要がない」が 39.9%と最も多く選択されており、「機器の場所を選ばずに利用できるから」の 29.5%を 10 ポイント近く上回っている。SaaS を導入することで、自社の業務の一部を SaaS に置き換えることを目的としているものと思われる。

しかしこれは、SaaS を導入することで運用保守体制を縮小することができる一方で、利用者の責任がなくなるわけではなく、あくまでも責任の一部を事業者に任せているに過ぎない。

そこで、責任共有モデルの考え方を基に事業者と利用者で責任範囲を明らかにする必要がある。事業者が情報開示した内容を基に、利用者は自らの責任範囲を理解し、不明な点があれば事業者に問い合わせることにより、事業者と利用者の双方で安全・安心な SaaS の利用を実現することが大切である。

このように、事業者は、利用者が自組織の置かれている事業環境にとって適切な SaaS を導入するために、比較・評価・選択に必要な情報を、利用者が利用しやすい方法で提供しなければならず、また、運用時においてもこれらの情報を利用者が利用しやすい形で、必要な時期に提供しなければならない。また、利用者も、自組織の置かれている事業環境や自組織のセキュリティレベルに適した SaaS を比較・評価・選択するために、事業者から信頼できる情報を取集し、SaaS を比較・評価・選択すると共に、得た情報を用いて自社の責任範囲を認識し、必要なリスクマネジメントを適切な時期に行わなければならないだろう。

[31] 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の概要（総務省）
[32] https://lp.legalforce-cloud.com/rs/585-ZXJ-799/images/LegalForce_saasjittai12.pdf

2　調査仮説

2.1　調査仮説の概要

本調査では、「2021 年度クラウド調査」の結果から、利用者がセキュリティの高い状態で SaaS を利用するための情報提供・情報利用が適切に行われていないのではないかとの問題意識を発端とし、IT サプライチェーンにおける現状の課題を整理するため、次節に示す仮説（表 2-1-1）を設定し、事業者・利用者それぞれの立場における実態を調査した。

仮説の設定に当たっては、「2021 年クラウド調査」において SaaS の事業者・利用者における情報開示・情報利用の非対称性が課題として挙げられていたことから、事業者・利用者間に意識の乖離があることを想定し、「情報開示」「情報利用」の状況に焦点をあてた。具体的には、利用者と事業者間の立場の違いと、契約前と契約後の時期の違いに着目することとした。これらを区分することで、立場・時期による情報の非対称性の発生状況をあきらかにできると考えたためである。

また、仮説を検証するために、利用者と事業者を対象としたアンケート調査と有識者へのインタビュー調査を行った。

2.2　調査仮説の内容

本調査で設定した仮説は以下のとおりである。この仮説に基づく調査内容については 3 章、仮説の検証結果については 4 章に示す。

表 2-1-1　調査仮説

報告書掲載箇所	仮説
4-1	契約前（選定時）における情報開示・情報利用
	1-1 事業者は利用者が SaaS を選定するために必要なセキュリティに関する情報を開示していない。
	1-2 利用者は SaaS を選定するために必要なセキュリティに関する情報を収集していない。
4-2	契約後（運用時）における情報開示・情報利用
	2-1 事業者は利用者が SaaS を利用するために必要なセキュリティに関する情報を提供していない。
	2-2 利用者は SaaS を利用するために必要なセキュリティに関する情報を収集していない。
4-3	利用者が収集した情報の利用状況
	3-1 利用者は選定するために収集したセキュリティに関する情報を利用できていない。
	3-2 利用者は SaaS 導入後に入手したセキュリティに関する情報を利用できていない。（仕様変更や新機能のリリース、関連する SaaS のインシデントなど）
4-4	利用者が参照しているセキュリティの基準・標準
	4-1 利用者は SaaS を選定する際に参照すべききセキュリティの標準が何かわからない。
4-5	SaaS の認証制度・認定制度の取得・利用状況
	5-1 事業者は SaaS の認定制度や認証制度を取得していない。
	5-2 利用者は選定の際に SaaS の情報開示認定制度や認証制度を選定の基準としていない。

3　調査の実施

調査はアンケート調査、インタビュー調査の手法を用いて行う。内容は以下のとおり。

・アンケート調査　：事業者・利用者向け調査
・インタビュー調査：有識者・事業者・利用者向け調査

3.1　アンケート調査（事業者向け）の調査

3.1.1　事業者向け調査の概要

事業者を対象に SaaS のセキュリティに関わる情報開示、情報提供の実態と課題に関する意識などについて、アンケート調査を実施した。

対象とする事業者は、クラウド関連団体の会員情報並びにその他の公開されている情報を基に抽出した。調査にあたっては、１事業者につき１サービスを想定して依頼し、複数のサービスについての回答が混在しないように留意したうえで調査を設計した。

〇調査手法：郵送による書面調査とウェブアンケートを併用
〇調査期間：2022 年 11 月 29 日～2022 年 12 月 28 日
〇調査対象：表 3-1-1 のとおり

表 3-1-1　アンケート対象（事業者）

項目	内容
対象とする企業・組織	SaaS の提供者である事業者[33]
対象とするサービス	業務での利用を目的とした SaaS
回答する単位	サービス
回答者	サービス担当者もしくは準ずる役員、従業員（自社で提供している SaaS の開示情報や利用者向けの情報発信に関する質問に回答できる人）

[33] 日本国内の企業・組織向けに提供している SaaS で、日本語で情報開示を行っている事業者を対象とした。

3.1.2　回収結果（事業者向け調査）

配布数 1,923 件に対し、回収数は 147 件、有効回答数は 144 件であった。回収率は 7.6%である。

3.1.3　回答者の概要（事業者向け調査）

回答者のプロファイルは図 3-1-1～3 のとおりである。回答者の本社所在地は 67.4%が関東であった。従業員数では、100 人以下が 60.4%と全体の半数以上を占めた。

主な事業内容では、アプリケーション・サービス・コンテンツ・プロバイダが最も多く、パッケージソフトウェア業、受託開発ソフトウェア業、情報処理サービス業が続いた。

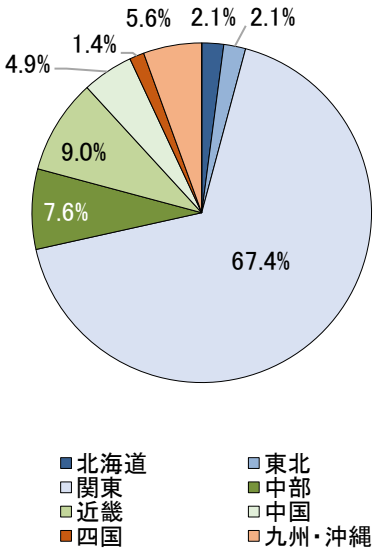


図 3-1-1　本社所在地（事業者）

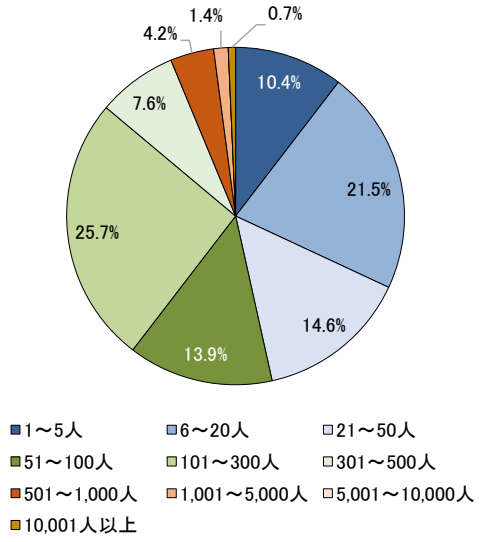


図 3-1-2　従業員数（事業者）

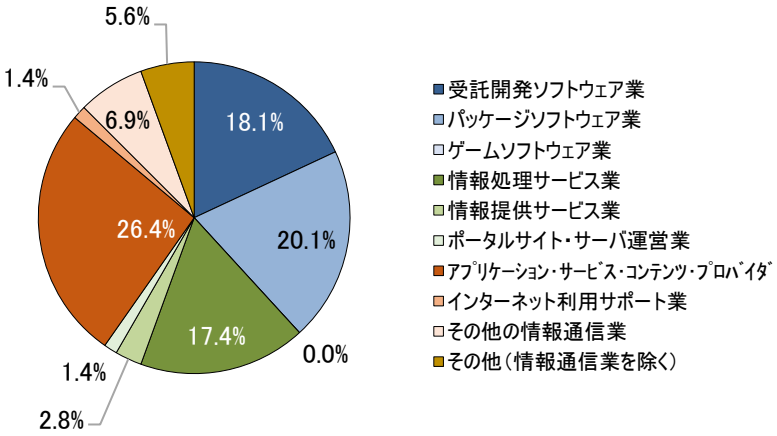


図 3-1-3　主な事業内容（事業者）

事業者に対して、提供している代表的な SaaS を一つ選定してもらい、そのサービスの内容等について回答を求めた。回答された SaaS のプロファイルは図 3-1-4、図 3-1-5 のとおりである。SaaS の適用分野（分類）では「その他」が 49.3%を占め、選択肢として提示した分類のうち複数の分類をカバーするサービスの回答もあり、SaaS の多様性を示す結果となった。SaaS の適用分野（業種）では業界横断型が 74.3%と全体の 4 分の 3 近くを占めた。

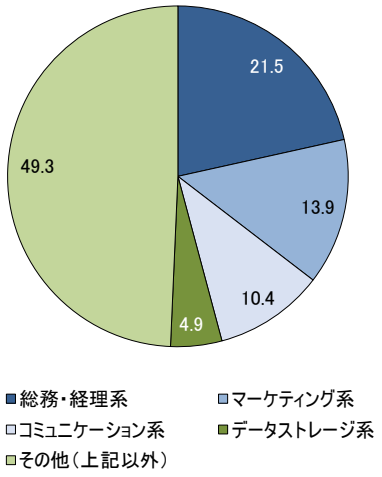


図 3-1-4　SaaS の適用分野（分類・事業者）

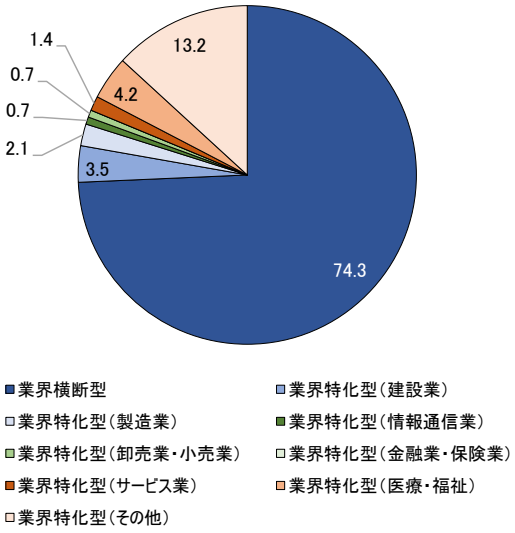


図 3-1-5　SaaS の適用分野（業種・事業者）

3.2 アンケート調査（利用者向け）の調査

3.2.1 利用者向け調査の概要

利用者企業・組織に所属する個人を対象にSaaSのセキュリティに関わる情報収集、情報利用のと課題に関する意識などについて、アンケート調査を実施した。

なお、2020年4月は新型コロナウィルス感染拡大に伴い第一回目の緊急事態宣言が発出されたタイミングであり、1.2.1に述べたとおりこの時期にSaaSの利用が拡大している。このことから、表3-2-1に示す内容を調査対象者の条件に含めることとした。

○調査手法：リサーチ会社登録モニターを利用したウェブアンケート
○調査期間：2022年12月5日～2022年12月7日
○調査対象：表3-2-1、表3-2-2のとおり

表3-2-1　アンケート対象（利用者）

項目	内容
対象とする個人	業務でSaaSを利用している企業・組織に属し、2020年4月以降にSaaSの導入に際して選定や承認に従事した経験を有する役員、従業員、および、IT部門（IT担当者）に属する従業員。
対象とする業種	情報通信業、製造業、卸売業・小売業、金融業・保険業、医療・福祉、サービス業（他に分類されないサービス業[34]）

表3-2-2　アンケート収集件数（業種別・利用者）

	大規模企業[35]	中小規模企業
製造業	50件以上	50件以上
情報通信業	50件以上	50件以上
サービス業	50件以上	50件以上
卸売業・小売業	規模を問わず50件以上	
金融業・保険業	規模を問わず20件以上	
医療・福祉	規模を問わず20件以上	

[34] 他に分類されないサービス業には、運輸業、郵便業、不動産業、物質賃貸業、学術研究、専門・技術サービス業、宿泊業、飲食サービス業、生産関連サービス業、娯楽業、教育、学習支援業を含む。
[35] 製造業については従業員数が301人以上、情報通信業とサービス業については従業員数が101人以上を大規模とした。

3.2.2　回収結果（利用者向け調査）

回収数・有効回答数ともに 457 件であった。業種別および企業規模別の回収状況は次の表 3-2-3 のとおりである。

表 3-2-3　アンケート回収数（業種別・企業規模別・利用者）

	大規模企業[36]	中小規模企業
製造業	61	55
情報通信業	56	56
サービス業	58	58
卸売業・小売業	56	
金融業・保険業	23	
医療・福祉	34	
計	457	

3.2.3　回答者の概要（利用者向け調査）

回答者のプロファイルは図 3-2-1、図 3-2-2 のとおりである。回答者の本社所在地は 49.5%が関東であった。事業者と比較して、関東の割合は少なかった。回答者の立場では、情報システム部門が 26.9%と最も多かった。

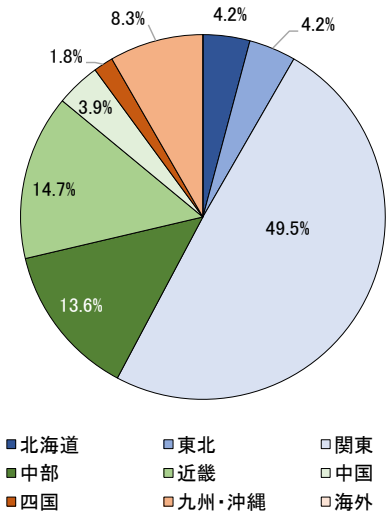


図 3-2-1 本社所在地（利用者）

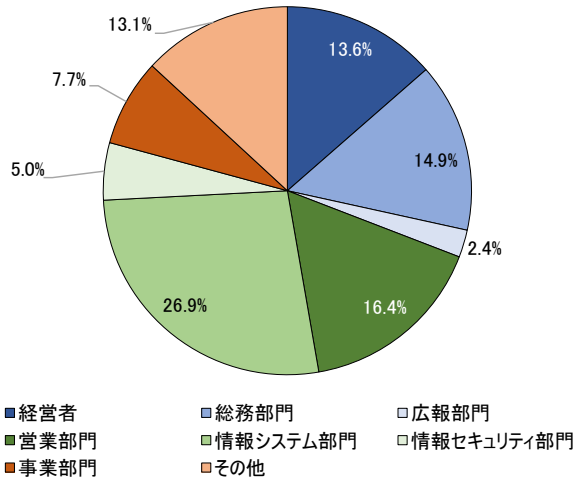


図 3-2-2 回答者の立場（利用者）

[36] 製造業については従業員数が 301 人以上、情報通信業とサービス業については従業員数が 101 人以上を大規模とした。

調査では、2020 年 4 月以降に導入または契約更新に携わった業務用の SaaS について回答してもらった。回答された SaaS のプロファイルは図 3-2-3、図 3-2-4 のとおりである。SaaS の適用分野（分類）では総務・経理系（人事労務・経理・会計・電子契約）が 30.9%、マーケティング系（営業・販売管理）が 22.5%であった。SaaS の適用分野（業種）では業界横断型が 28.4%、業界特化型が 71.6%であった。事業者では業界横断型 SaaS の回答が多かったが、利用者からは業界特化型の回答が多かった。業界特化型 SaaS で回答された業種を比較すると、製造業の業界特化型 SaaS が最も多く回答された。

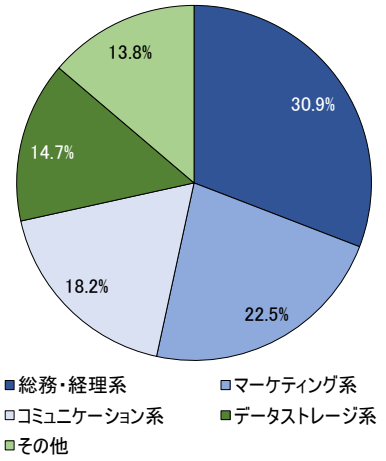


図 3-2-3　SaaS の適用分野（分類・利用者）

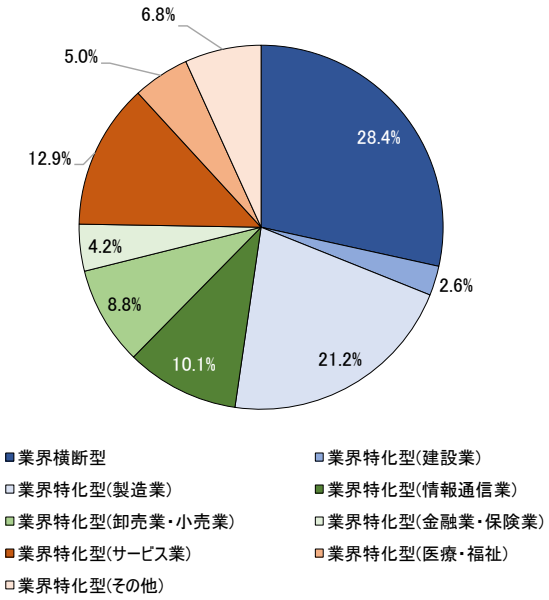


図 3-2-4　SaaS の適用分野（業種・利用者）

3.3 インタビュー調査

3.3.1 インタビュー調査の概要

SaaS の事業者および利用者、SaaS 事業者が加盟している団体やコミュニティに属する有識者および SaaS の調査・研究に携わる有識者などから、「SaaS のセキュリティを保証する情報開示」および「セキュリティの高い状態で SaaS を利用してもらうための情報提供」の動向、アンケート調査結果に対する意見、政府や IPA の取り組みに対する要望等を収集するために、インタビュー調査を実施した。調査先のプロファイルは表 3-3-1 のとおり。

○実施形式：Web 会議ツールを利用し、オンラインでのインタビューを実施
○実施時期：アンケート設計段階…2022 年 10 月
　　アンケート分析段階…2023 年 1 月
○調査対象：表 3-3-1 のとおり

表 3-3-1 インタビュー調査先

記号	区分	調査先	実施フェーズ
A	利用者	SaaS 利用者（情報通信業 A 社）	アンケート設計段階
B	利用者	SaaS 利用者（飲食業 B 社）	アンケート設計段階
C	利用者	SaaS 事業者 C 社	アンケート分析段階
D	有識者	有識者（セキュリティコンサルタント会社 D 社）	アンケート分析段階
E	有識者	有識者（クラウド関連団体） 日本クラウドセキュリティアライアンス	アンケート設計段階 アンケート分析段階
F	有識者	有識者（クラウド関連団体） 一般社団法人　日本クラウド産業協会	アンケート分析段階
G	有識者	有識者（研究者）　情報セキュリティ大学院大学	アンケート分析段階

※区分およびインタビュー実施フェーズの順に記載

4 情報開示・情報利用の調査結果

本章ではアンケート調査およびインタビュー調査から得られた情報に基づき、2.1 調査仮説に記載した本調査における仮説について検証する。

4.1 契約前（選定時）における情報開示・情報利用

本節では、以下の 2 つの仮説について、アンケート調査およびインタビュー調査の結果を踏まえて検証を行う。なお、本調査における「選定するために必要なセキュリティに関する情報」とは、契約を開始する前に利用者が情報を収集することが望ましい情報と定義した。また「開示」とは、利用者が適切に情報を利用できるために適した方法で情報を提供することと定義した。

- 仮説 1-1 事業者は利用者が SaaS を選定するために必要なセキュリティに関する情報を開示していない。

- 仮説-1-2 利用者は SaaS を選定するために必要なセキュリティに関する情報を収集していない。

4.1.1 調査結果

（1）契約前（選定時）における情報開示・情報利用の状況

調査では、「情報開示指針」及びアンケート設計段階で行ったインタビュー調査における有識者の意見を基に「SaaS を選定するために必要なセキュリティに関する情報」を検討し、項目を決定した。それらの調査項目について、事業者、利用者に対し、情報開示・情報利用の方法を調査した。なお、ここでは情報開示のうち情報提供、情報利用のうち情報収集に焦点をあてた。

事業者側の情報開示の状況について、図 4-1-1 で示す調査項目ごとに「約款、利用規約で開示」「ＨＰ等で広く一般に開示」「メール配信（メルマガ等)」「セミナー」「要求項目に対し開示」「行っていない」の選択肢を提示した。「約款、利用規約で開示」「ＨＰ等で広く一般に開示」「メール配信（メルマガ等)」「セミナー」「要求項目に対し開示」を「行っている」、いずれも行っていないとの回答を「行っていない」として分析したところ、27 項目のうち 22 項目では「行っている」の組織が 70%を超えた。一方、「インフラの物理的な状況（建物形態、耐震・免震構造)」「脆弱性診断（脆弱性診断の有無、診断の対象等）の結果」「サービス稼働設定値」の項目では「行っている」組織が 70%を下回っていた。

次に、事業者側の情報開示の方法について回答してもらった。調査項目ごとに情報開示の方法を複数選択で回答してもらった結果が図 4-1-2 である。「約款、利用規約で開示」に着目すると、「事業者の自己責任の範囲と補償範囲」「サービス変更・終了時の事前告知」「個人情報の利用目的」の回答が多いことが分かった。

利用者側に対しては、事業者向け調査と同じ項目について契約前（選定時）の情報利用の状況に関する調査を行った。調査結果は図 4-1-3 のとおりである。すべての項目で「いずれかの方法で情報収集している」の回答が 70%を下回っており、事業者側の認識と大きく異なっていた。逆に

「収集しない」と回答された割合はすべての項目で 30%を超えることになり、中でも「インフラの物理的な状況」は 42.2%が収集していない結果であった。

事業者の情報開示状況のうち「行っていない」が多かった項目に着目した。「約款、利用規約」による情報開示が比較的行われていない項目は、事業者が SaaS のセキュリティ対策として自らの責任で行う項目が多くを占めていた。事業者が自らの責任で行う項目であるため、利用者に対策状況を開示する必要はないとの考え方もあるが、「脆弱性診断（脆弱性診断実施の有無、診断の対象等）の結果」等の項目や「データの改ざん防止対策」といった項目は利用者にとっても重要な項目である。また、ウイルス対策の有無や、診断実施の有無などといった項目は、開示することで事業者の信頼性を高めることにもなるだろう。

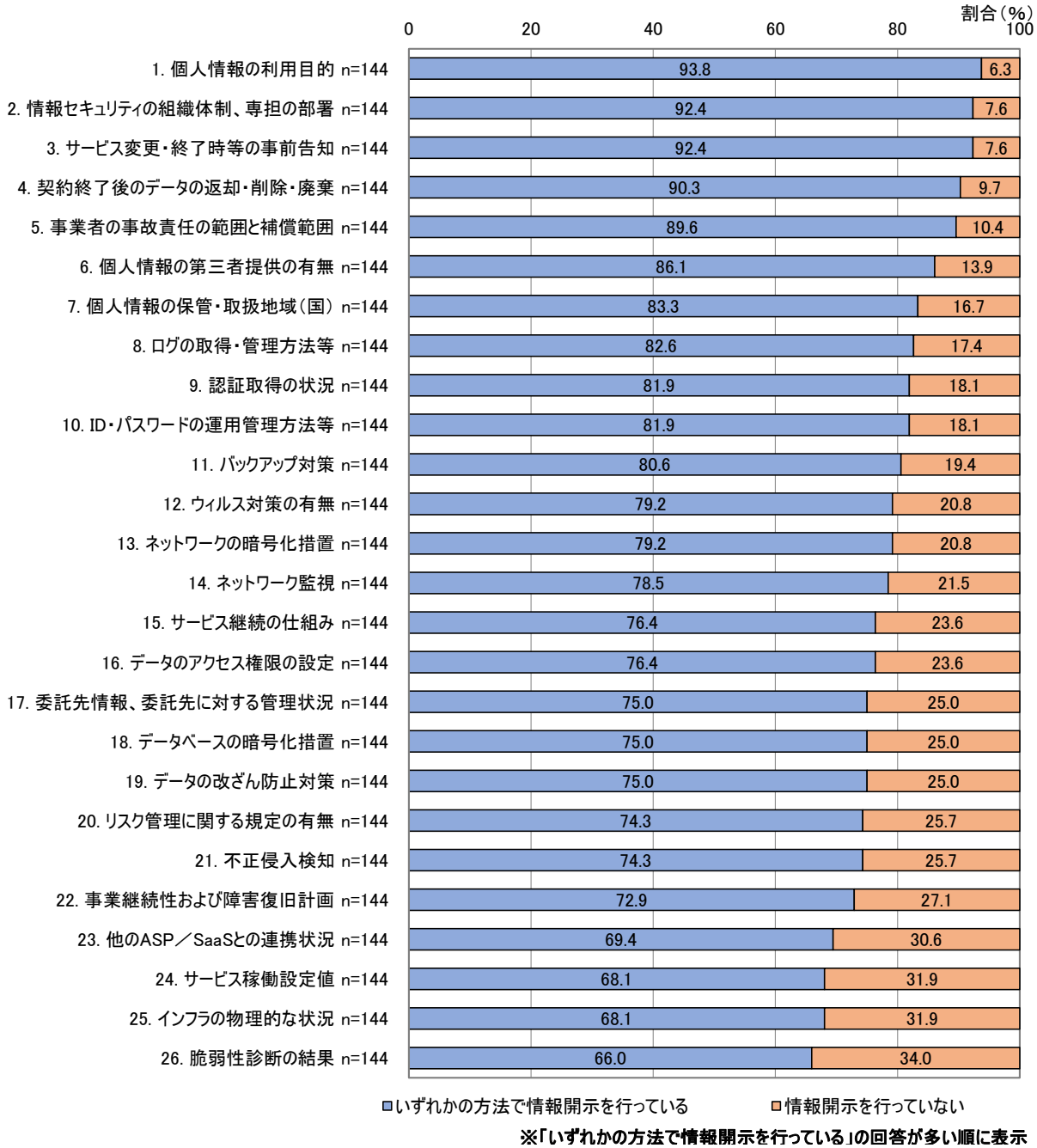


図 4-1-1　契約前（選定時）の情報開示の状況（事業者）　n=144

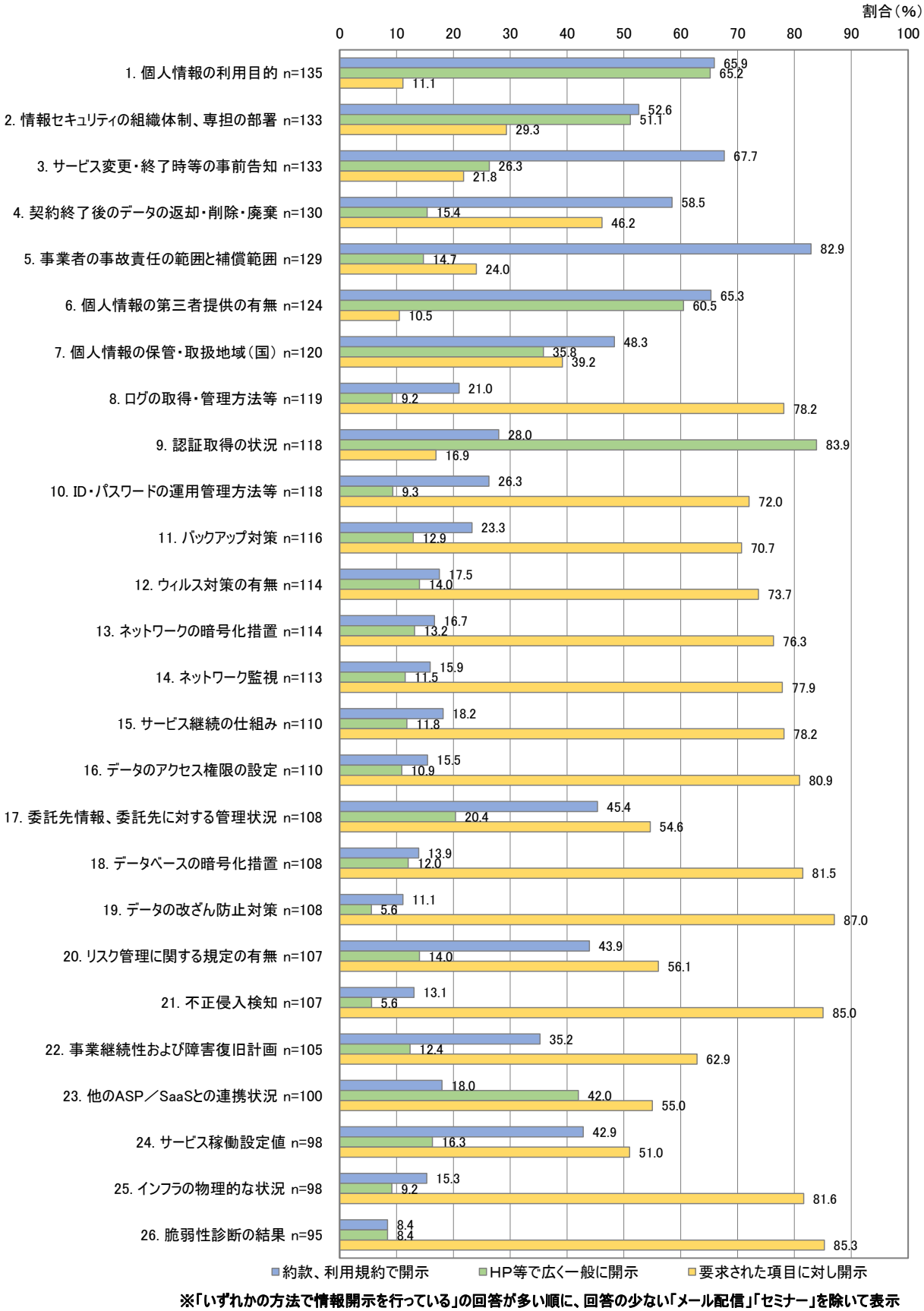
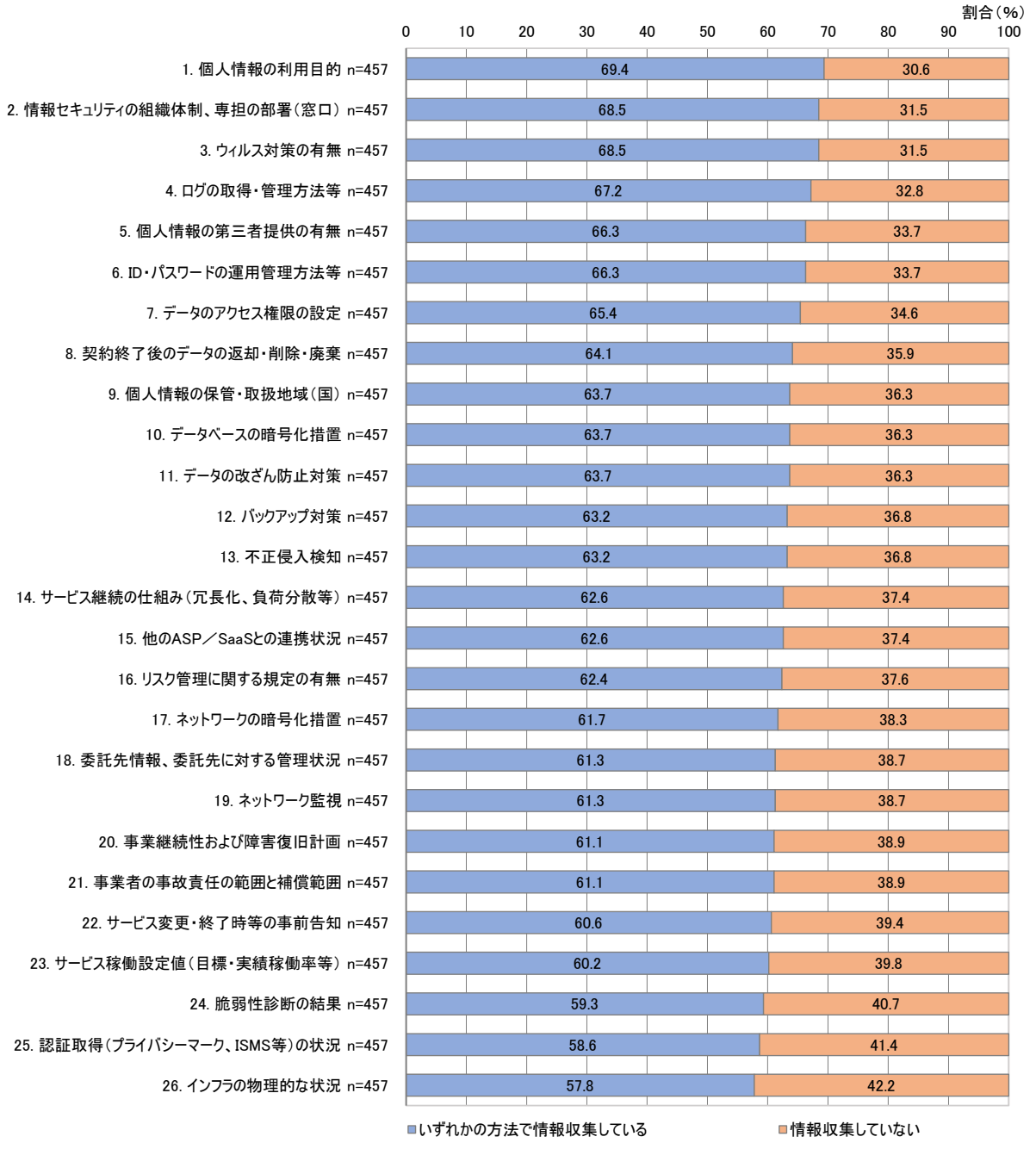
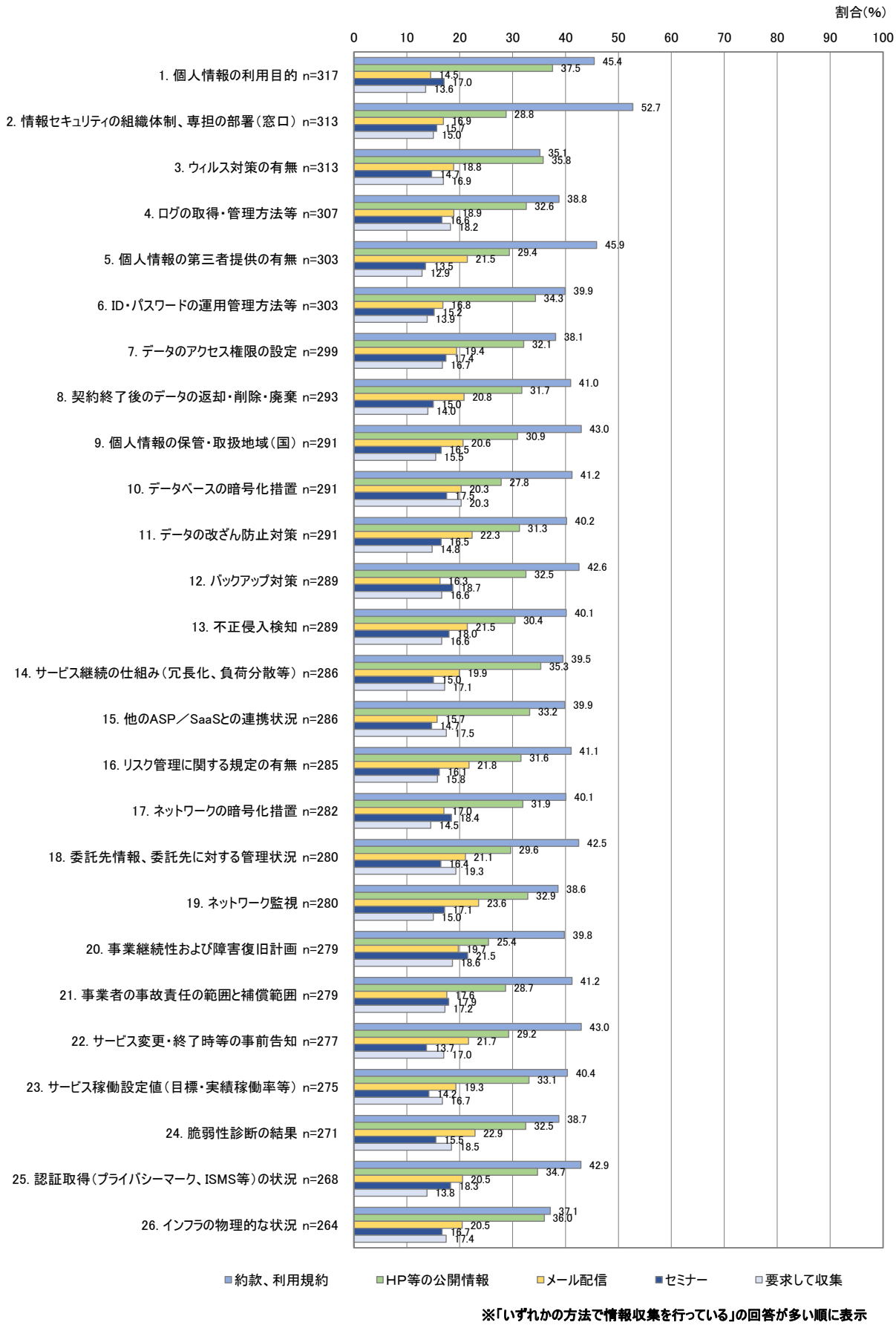


図 4-1-2　契約前（選定時）の情報開示の方法（事業者）　n=144（複数選択あり）



※「いずれかの方法で情報収集を行っている」の回答が多い順に表示

図 4-1-3　契約前（選定時）の情報収集の状況（利用者）　n=457



※「いずれかの方法で情報収集を行っている」の回答が多い順に表示

図 4-1-4　契約前（選定時）の情報収集の方法（利用者）　n=457（複数選択あり）

利用者向け調査の情報収集・情報利用の方法を比較すると、一部の項目を除き「約款・利用規約」が最も割合が大きく、次いで「ＨＰ等の公開情報」となっていた（図 4-1-4）。事業者に対し「要求して収集」は、最も割合が大きい「データベースの暗号化措置」でも 20.3%にとどまった。事業者への情報開示の要求や問い合わせなどといった、事業者に対する行動を起こさずに、公開された情報や、既に入手している約款・利用規約を利用する傾向がみられた。

利用者の情報利用の方法に係わる調査結果のうち「約款、利用規約」に着目すると、「情報セキュリティの組織体制、専担の部署（窓口）」が最も多く 50%を超えており、次いで「個人情報の利用目的」「個人情報の第三者提供の有無」の順となっていた。

（２）契約前（選定時）における情報開示・情報利用の頻度

開示している情報を提供する頻度について事業者に調査を行った。結果は図 4-1-5 のとおりである。「常に公表」の回答に着目すると、「認証取得の状況」「個人情報の第三者提供の有無」「個人情報の利用目的」の順に多く回答されており、割合は 70%を超えていた。

一方、「脆弱性診断の結果」「不正侵入の検知」「データの改ざん防止対策」「インフラの物理的な状況」では「常に公表」の割合は 10%を下回っていた。

過半数の項目において「要望があれば提示」の割合が最も大きく、開示した内容に変更があっても積極的に通知を行っておらず、最新の情報が利用者に届いていない可能性があることが分かった。「サービスの変更・終了時等の事前告知」「サービス稼働設定値（目標・実績稼働率等）」の項目など、利用者にとって特に重要と思われる項目であっても、内容に変更があった場合に通知されていない可能性がある。

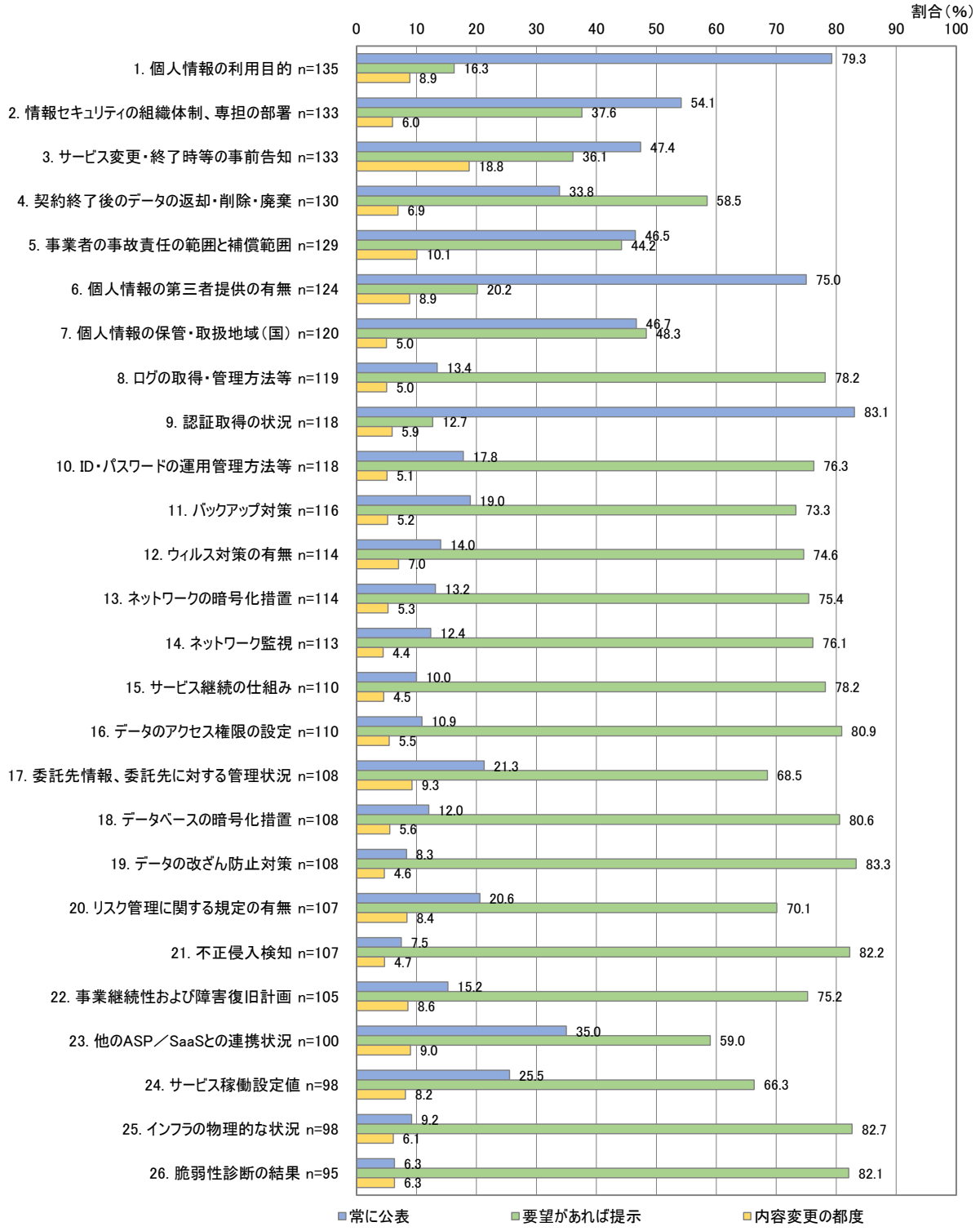


図 4-1-5　契約前（選定時）の情報開示の頻度（事業者）　n=144（複数選択あり）

（３）契約前（選定時）における情報利用の企業規模による分析

利用者の「選定するために必要なセキュリティに関する情報」の利用状況について、企業規模別に分析を行った。企業規模は、業種ごとに中小企業庁の定義に従い区分した。詳細は 3.2.2 を参照いただきたい。結果は図 4-1-6 のとおりである。

いずれの項目でも大規模の企業（以下、大規模企業）よりも中小規模の企業（以下、中小規模企業）では「情報収集していない」の割合が多く、中小規模企業では大規模企業と比較し情報収集が行われていなかった。有識者からも、大規模企業ではクラウドに適した規約やルールが整備されている傾向にあるものの、中小規模企業ではそのような規約の整備がクラウドの利用拡大に追い付いておらず、規約が無い、またはクラウドサービスに対応できていない傾向にあるようだとのコメントがあった。

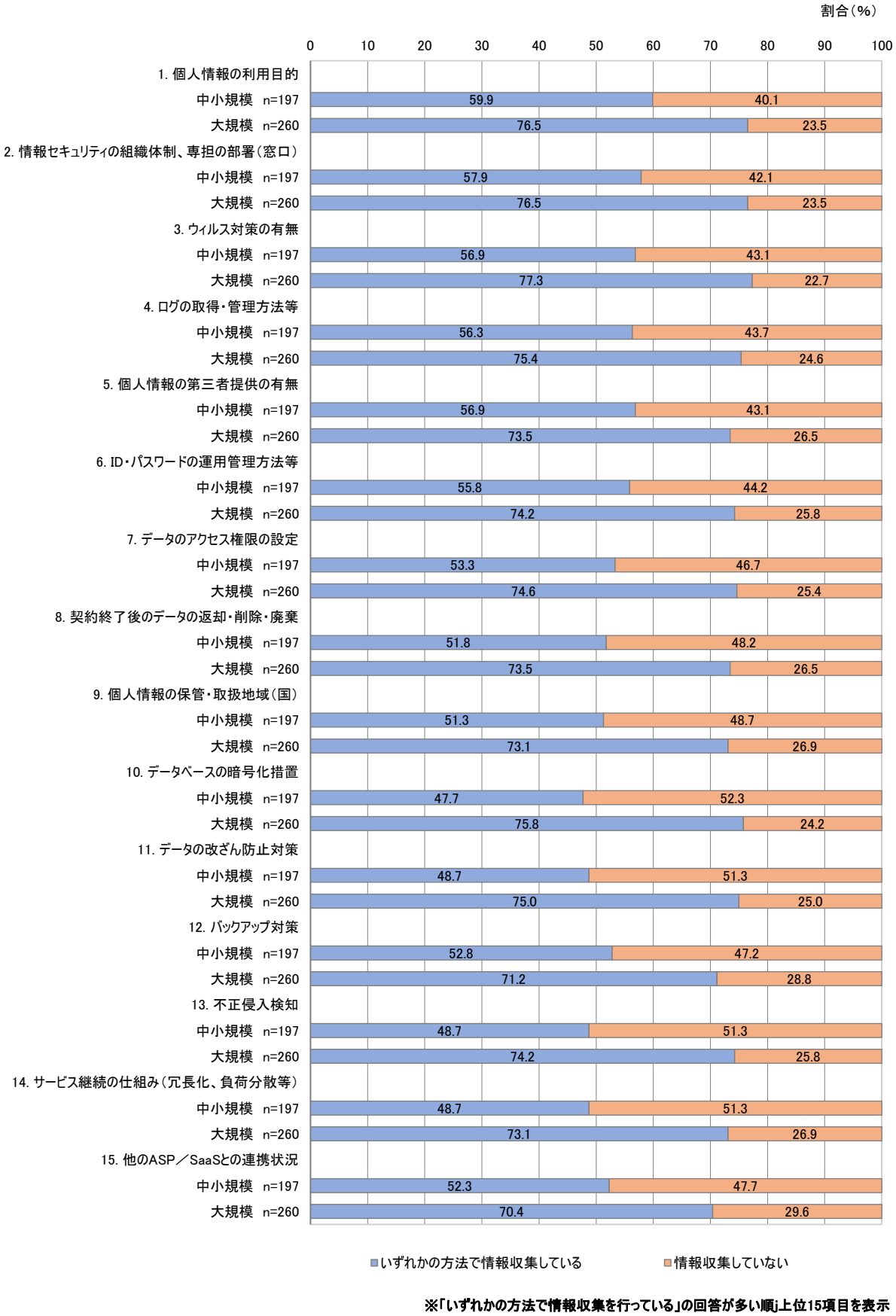


図 4-1-6 契約前（選定時）の情報利用の状況（利用者）（企業規模別）

（４）契約前（選定時）に利用する情報

利用者が SaaS の選定に当たりどのような情報を利用しているのか調査した。結果は図 4-1-7 のとおりである。最も参考にされた項目は「SaaS 事業者の Web サイトやカタログに掲載された情報」であり、次に「レビューサイトや口コミ、ランキングなどの情報」の順となった。4.1.1 で得られた調査結果と同様に、利用者は公開された情報の収集を行う傾向が強いことがわかる。

SaaS 事業者が直接提供する情報として「SaaS 事業者の Web サイトやカタログに掲載された情報」「SaaS 事業者への問い合わせを行った結果」に着目した。「SaaS 事業者の Web サイトやカタログに掲載された情報」は 25.4%が情報収集しておらず、「SaaS 事業者への問い合わせを行った結果」は 29.3%が情報収集していないと回答した。SaaS の利用に当たり、事業者が提供している情報にアクセスしていない利用者が一定数存在することが示される結果となった。

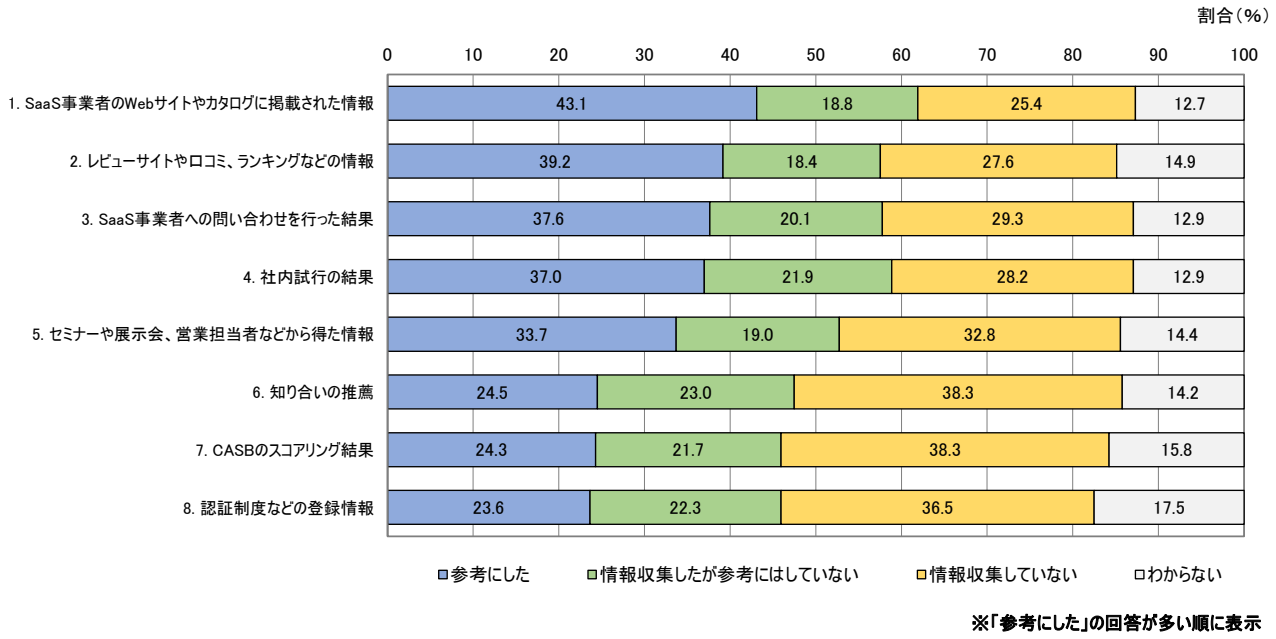


図 4-1-7　契約前（選定時）に利用する情報（利用者）　n=457

次に、利用者が契約前（選定時）に利用する情報について企業規模別に分析を行った。結果は図 4-1-8 のとおりである。項目により企業規模による差が大きく、「CASB のスコアリング結果」「SaaS 事業者へ問い合わせを行った結果」では「参考にした」について 15 ポイント近く差が開いた。これらの背景として、CASB の認知度や、企業規模により情報収集に工数をかけられるか否かが影響しているものと思われるが、有識者へのインタビューでは、大規模企業は中小規模企業と比較して社内ルールの整備が進んでいる状況にあることが指摘されており、それらの要因が合わさった結果であろう。

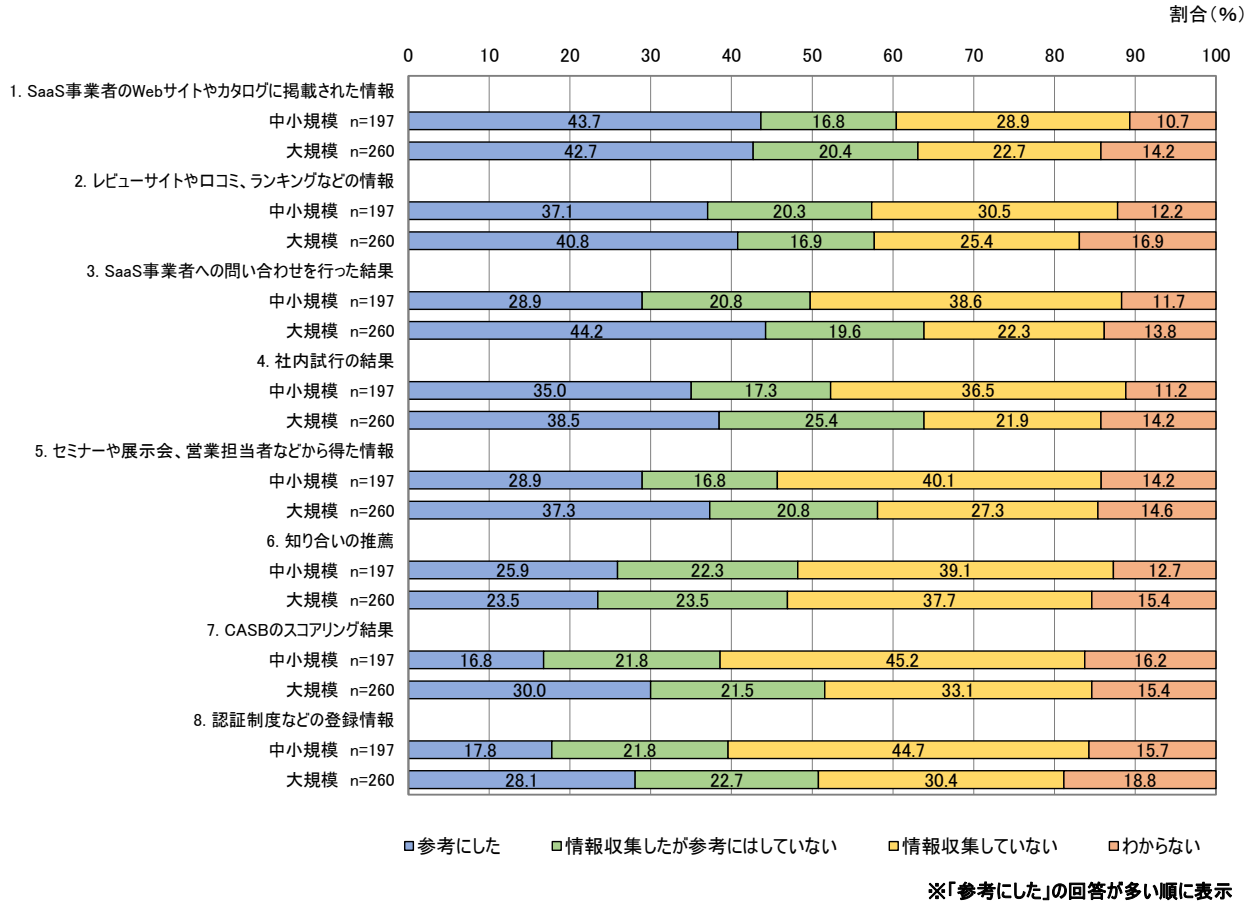


図 4-1-8　契約前（選定時）に利用する情報（企業規模別・利用者）　n=457

（５）契約前（選定時）における情報開示・情報提供の目的（事業者）

事業者が情報開示・情報提供を行う理由について調査した。結果は図 4-1-9 のとおりである。「利用者に安心してご利用いただくため」の項目では「強くそう思う・どちらかというとそう思う」の割合が最も多く、「情報開示することで自社の責任範囲を明確にするため」「利用者が選定する際の条件となるため」と続いた。情報開示を行うことは、提供しているサービスの利用者にとって必要なことであり、情報開示を行うことが利用者からの高評価につながると考えている事業者が一定数存在している。

仮説の設定に際し、情報提供を行うことは事業にとって負担であると考える事業者が多いため情報開示が進んでいないのではないかと考えていたが、90%以上の事業者が利用者への安心材料として情報開示を積極的に捉えていることがわかる。

事業者へのインタビューにおいても、利用者への情報提供は事業者の責任であるとの意見と共に、情報開示をしていない SaaS は利用の対象としていない企業もあることから、情報開示は選定されるために必要な条件でもあるとの状況が示された。

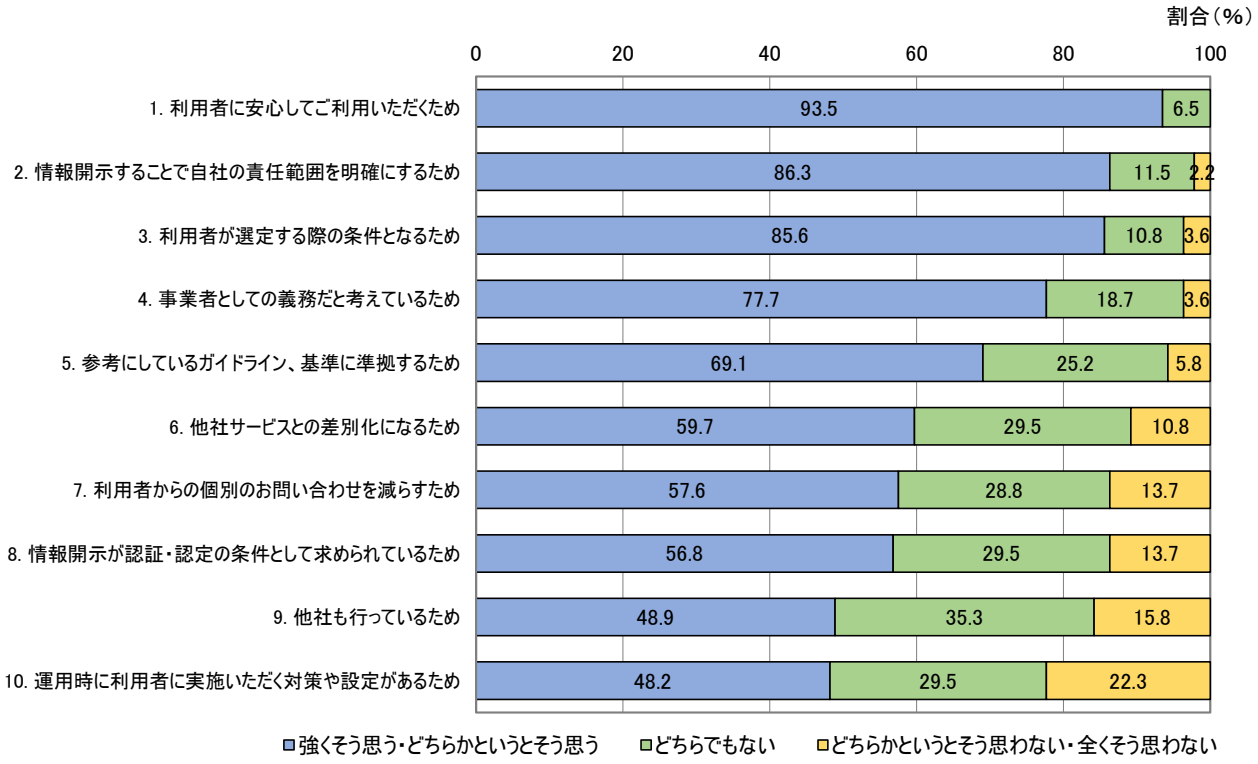


図 4-1-9　契約前（選定時）における情報開示・情報提供の目的（事業者）　n=138

（６）契約前（選定時）における情報開示・情報提供と収集する情報の分析

事業者が情報開示・情報提供を行う情報と利用者が収集する情報について、さらに分析を行った。図 4-1-10 に結果を示す。

事業者については、情報を自主的（HP やカタログで公開）に開示する（縦軸）のか、それとも要求（問い合わせ）があった場合にのみ開示する(横軸)のかを青い点で示した。その結果、右下がりの直線状に点在した。自主的に開示する方が要求に対して開示するよりも多い項目は、「認証取得の状況」「事業者の事故責任の範囲と補償範囲」「サービス変更・終了時等の事前告知」及び個人情報に関連する項目等、契約条件や法令に関連するものが多い。自主的に開示するよりも要求に対して開示する方が多い項目は、「委託先情報、委託先に対する管理状況」「リスク管理に関する規定の有無」といった組織的対策、ウイルス対策、暗号化対策、監視など技術的対策に関連するものが多い。事業者は情報開示指針等で求められている項目については概ね開示するが、開示方法は情報の内容によって変えており、特に技術的対策については問い合わせ等により開示するが多いことが分かった。

利用者については、情報を公開情報から収集する（縦軸）のか、それとも事業者に要求（問い合わせ）して収集する（横軸）のかを赤い点で示した。その結果、公開情報からの収集は 35%～55%、要求して収集は 10%～25%の間に集中していた。このことは、利用者は項目によって情報収集方法を変えることがあまりなく、しかも、利用者が収集している情報は、事業者が開示している情報の一部にとどまっており、十分入手できていないということが分かった。

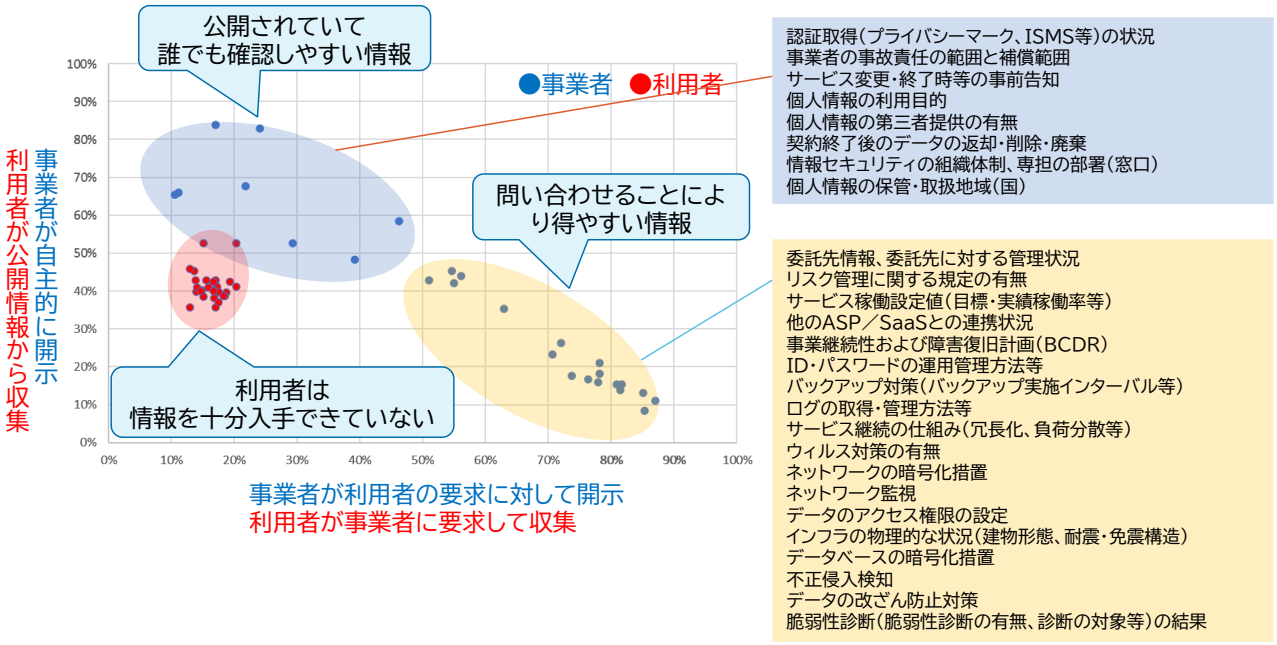


図 4-1-10　契約前（選定時）における情報開示・情報提供（事業者）と情報収集（利用者）の状況

事業者　N=144,　　利用者　N=457

4.1.2 まとめ

本節では、「事業者は利用者が SaaS を選定するために必要なセキュリティに関する情報を開示していない。」「利用者は SaaS を選定するために必要なセキュリティに関する情報を収集していない。」との仮説に対する調査結果を提示した。事業者の調査結果からは、情報の内容によりあらかじめ約款等で情報開示している項目と、要求があった場合に情報開示する項目とに分かれる傾向がみえた。一方、利用者は情報の項目・内容共に情報収集が出来ているとはいえない状況にあった。

また、本調査で明らかになった問題点として、事業者が開示する際の方法と、利用者が収集する際の方法との間で差が生じている点が挙げられる。「要求があれば提示する」と事業者が回答する割合が多かった項目について、利用者が「事業者に要求する」と回答した割合は 10%程度にとどまっている。事業者は「SaaS の選定に必要なセキュリティに関する情報」を開示する準備はしているものの、利用者は開示を要求していない。このため、事業者が開示するべきと考えている項目は実際には利用者に届いていない可能性が高い。これらの結果から、事業者は、利用者が利用しやすい方法で提供できているとは言えず、利用者は必要な情報を入手することが出来ていない。

利用者においては、情報収集の方法は公開情報に偏っており、収集すべき情報のうち公開されている情報では足りない情報を事業者から収集することができていない。こういった状況から、事業者から信頼できる情報を収集して SaaS を比較・評価・選択することはできておらず、安全なクラウドサービスの利用が出来ているとは言えないだろう。

このように、事業者が提供する準備を行っている情報と、実際に利用者が収集する情報に差がある状況については有識者からも言及があった。事業者に実施したインタビューでも、情報開示の要求を受けた場合に備えて情報を開示する準備を行っており、要求した利用者に対しては情報開示を行っているが、情報開示を要求する利用者は決して多くなく、要求をしない利用者については対応が出来ていないとのことであった。また、情報収集を行った利用者を含め、SaaS の利用者が収集したセキュリティに関する情報を利用し、比較・評価・選択を行っているか把握できていないものの、利用者は公開している情報を利用してくれているとの性善説で考えていた。

事業者は利用者にとって利用しやすい形で情報提供を行い、利用者は提供された情報を収集し、情報が足りなければ事業者に対し要求を行うべきであるが、実態は出来ていなかった。この要因の一つとして、SaaS の特性が挙げられるだろう。先に述べたように、オンプレミスの環境で情報システムを構築する際に、事業者と利用者が情報共有し信頼関係を構築していた状況と大きく異なり、SaaS において情報共有は希薄である。事業者が利用者の状況を把握することは困難であり、利用者もオンプレミスのシステムと同じように、自組織に適した内容を自組織に適したタイミングで情報共有してもらうことは困難である。また、有識者からは利用者のクラウドセキュリティに関する知識や有識者の不足について指摘されている。利用者側の情報収集・情報利用が進んでいない理由の一つは、利用者のクラウドに適したセキュリティに対する認識の不足も挙げられるだろう。

なお、事業者向け・利用者向けアンケートで挙げられた課題については 4.6 で分析を行った。

4.2 契約後（運用時）における情報開示・情報利用

本節では、以下の 2 つの仮説について、アンケート調査およびインタビューの結果を踏まえて検証を行う。なお、本調査における「選定するために必要なセキュリティに関する情報」とは、契約を開始する前に利用者が情報を入手することが望ましい情報と定義した。「情報開示」とは、事業者がセキュリティに関する情報を約款・利用規約・HP 等で公表、または要望があった場合に提示することを指し、「情報利用」とは、利用者が事業者の開示した情報を入手し、SaaS の安全な利用に資するために情報を活かすことを指す。

- 仮説 2-1 事業者は利用者が SaaS を利用するために必要なセキュリティに関する情報を提供していない。

- 仮説-2-2 利用者は SaaS を利用するために必要なセキュリティに関する情報を入手していない。

4.2.1 調査結果

（1）契約後（運用時）における情報開示・情報利用の状況

調査では、有識者の意見を基に「契約後（運用時）に利用するために必要なセキュリティに関する情報」として図 4-2-1 で示す項目について事業者、利用者に対し情報開示・上違法利用の状況と方法を調査した。なお、ここでは情報開示のうち情報提供に、情報利用のうち情報収集に焦点をあてた。

図 4-2-1 のとおり、事業者側の情報開示の状況について、項目ごとに「約款、利用規約で開示」「ＨＰ等で広く一般に開示」「メール配信（メルマガ等)」「セミナー」「要求項目に対し開示」を「行っている」、いずれも行っていないとの回答を「行っていない」として分析したところ、9 項目のうち 7 項目では「行っている」の組織が 70%を超えた。一方、「ネットワークの監視状況」では「行っている」組織が 70%を下回っていた。

情報開示の方法では、図 4-2-2 のとおり「インシデント発生時の連絡先・問い合わせ窓口」「通常運用時の利用方法等の問い合わせ窓口」「サービスの障害対応情報（被害の範囲や原因等)」については専用窓口（サービスデスク）で対応するとの回答が多かったが、安全に運用するための設定方法」「サービス稼働状況」「脆弱性情報」「ネットワーク監視状況」の項目では「要求項目に対し開示」が多かった。

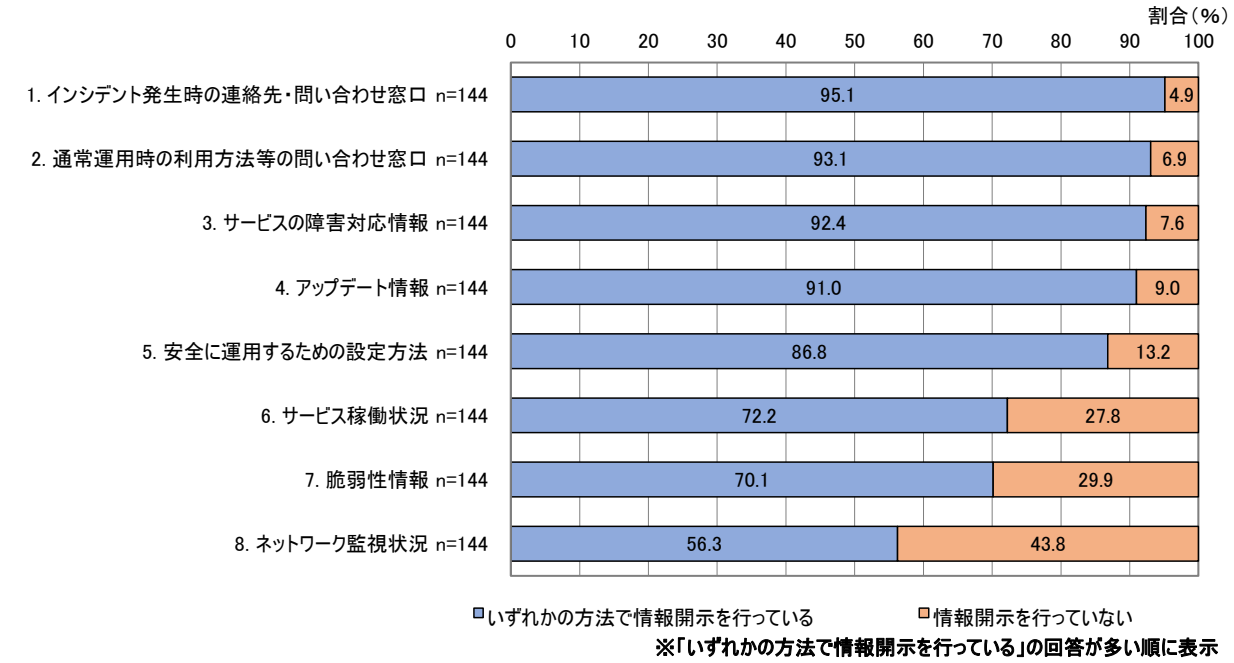


図 4-2-1　契約後（運用時）の情報開示の状況（事業者）n=144

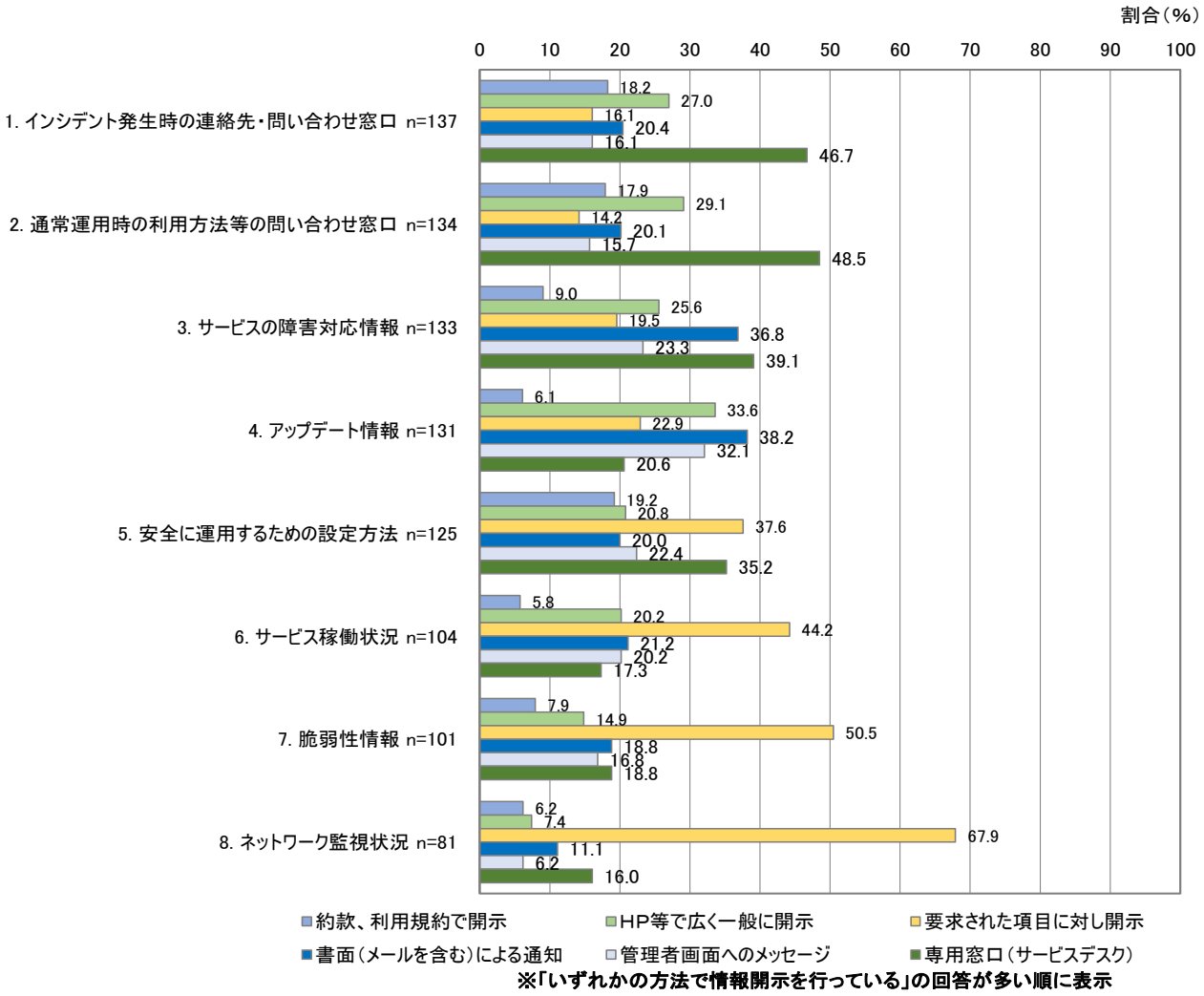


図 4-2-2 契約後（運用時）の情報開示の方法（事業者） n=144

開示している情報を提供する頻度について事業者に調査を行った。結果は図 4-2-3 のとおりである。「常に公表」の回答に着目すると、「通常運用時の利用方法等の問い合わせ窓口」「インシデント発生時の連絡先・問い合わせ窓口は」50%以上が「常に公表」としていた。「要望があれば提示」の回答に着目すると、「安全に運用するための設定方法」「サービス稼働状況」「脆弱性情報（脆弱性テストの結果)」「ネットワーク監視状況」では「要望があれば提示」が最も多く選択されており、利用者が積極的に情報を収集しないと必要な情報を得られないことがわかる。

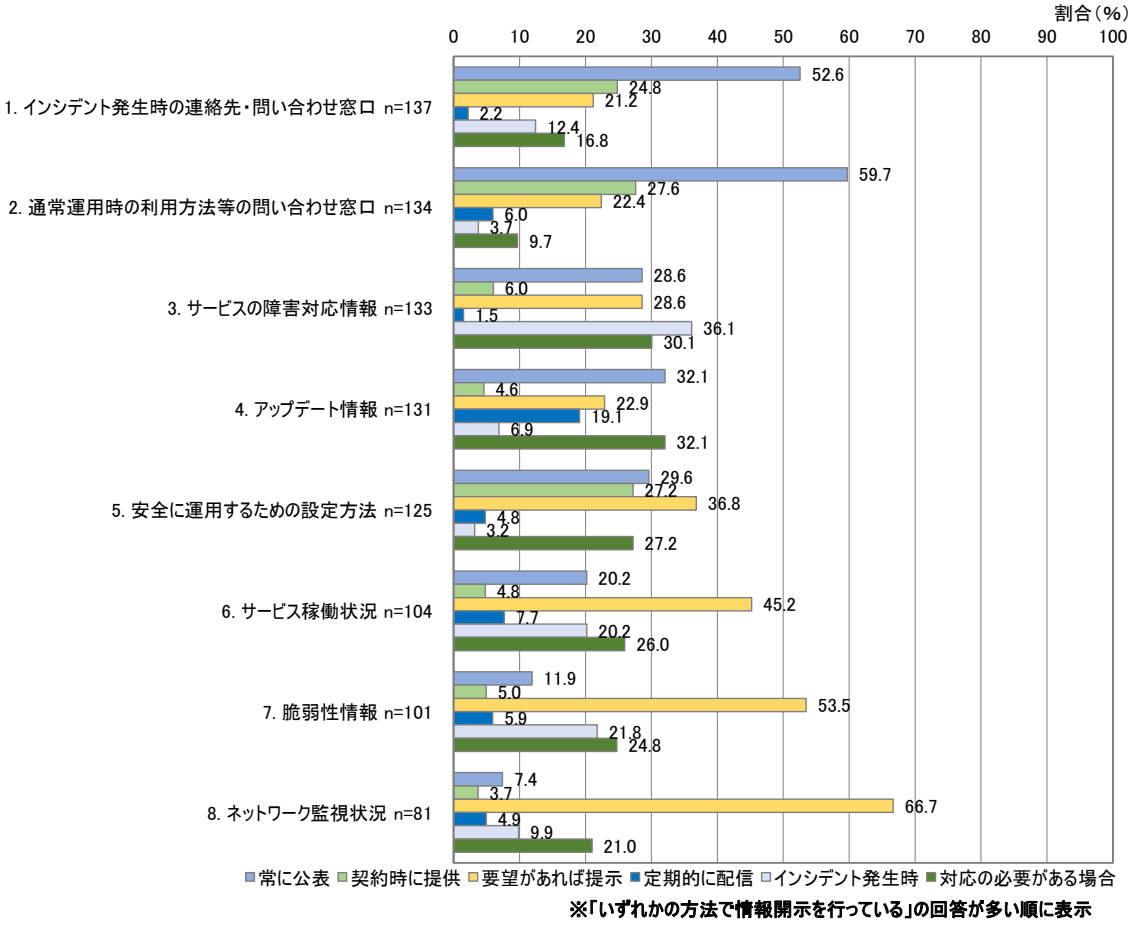


図 4-2-3　契約後（運用時）の情報開示・情報提供の頻度（事業者）n=144

利用者側に対し、契約後（運用時）の情報利用の状況に関する調査を行った。結果は図 4-2-4、図 4-2-5 のとおりである。情報収集している割合の項目による差は少なく、最も多い項目で 76.8%、最も少ない項目で 69.4%と差は 7.4 ポイントであった。

情報収集の方法に着目すると、いずれの項目でも「約款、利用規約で収集」または「ＨＰ等の公開されている情報で収集」が最も多く選択されており、公開されている情報を利用する傾向が強かった。

事業者と利用者の回答結果を比較すると、「ネットワーク監視状況」の項目では、事業者が「常に公表」「契約時に提供」を選択した割合はそれぞれ 7.4%、3.7%であったが、利用者では 29.3%が「約款、利用規約で収集」、26.5%が「ＨＰ等の公開されている情報で収集」を選択していた。

利用者向け調査で回答された SaaS と、事業者向け調査で回答された SaaS は適用分野が異なる傾向があるため一概には言えないが、同じ情報の開示状況・収集状況に差が生じていた。

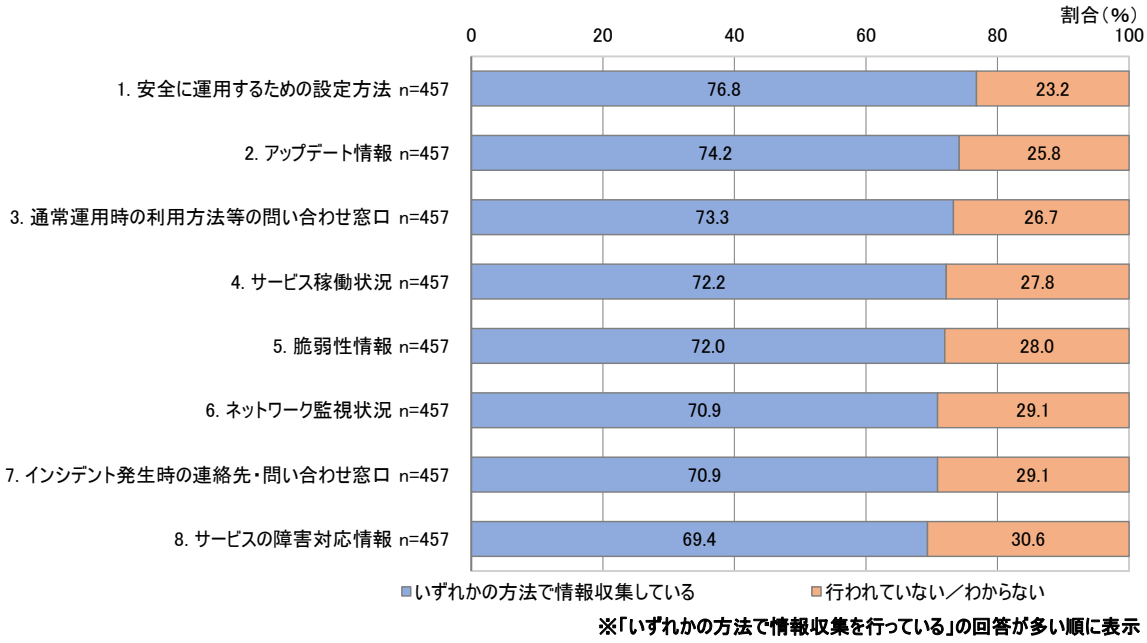


図 4-2-4　契約後（運用時）の情報利用の状況（利用者）　n=457

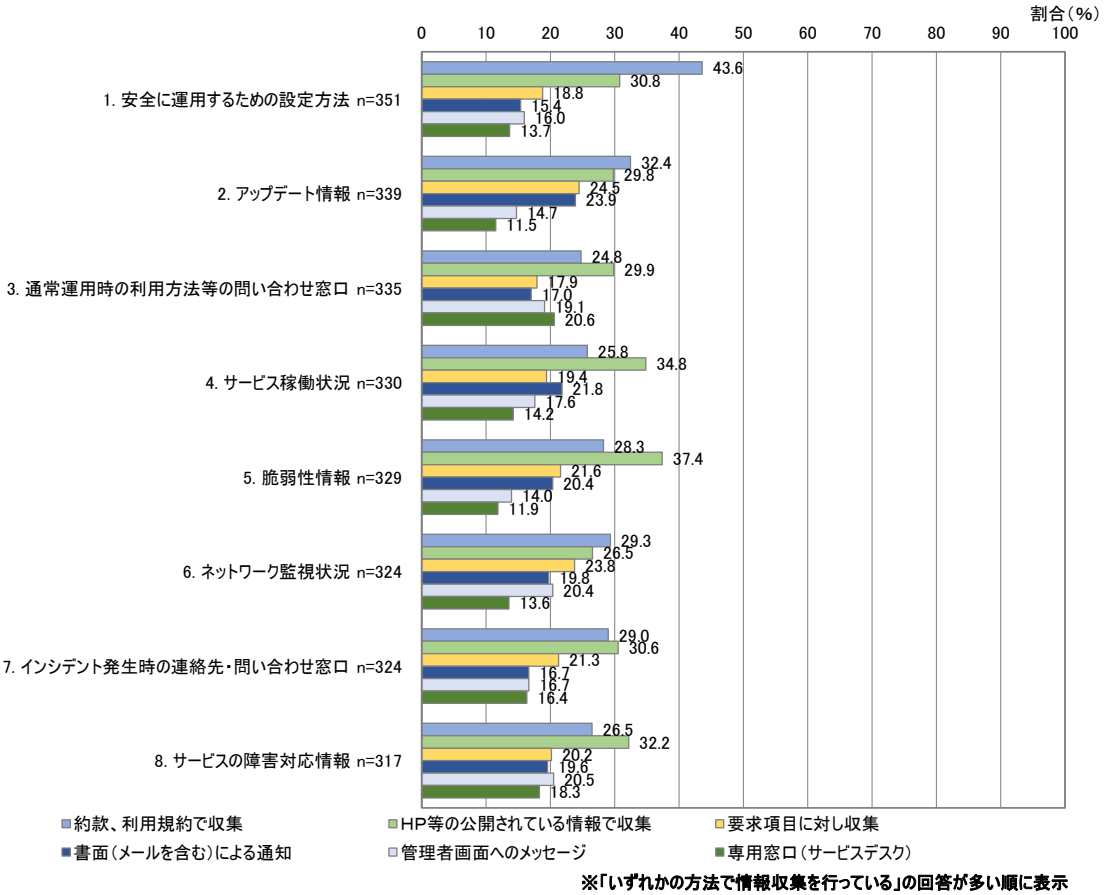


図 4-2-5　契約後（運用時）の情報収集の方法（利用者）

（２）契約後（運用時）における情報利用の企業規模による分析

利用者の契約後における情報利用の状況について、企業規模別に分析を行った。企業規模は、業種ごとに中小企業庁の定義に従い区分した。詳細は 3.2.2 を参照いただきたい。結果は図 4-2-6 のとおりである。

4.1.1 で示した契約前における情報収集の状況と同様に、企業規模により傾向の差が見られた。「いずれかの方法で情報収集している」の回答はすべての項目で中小規模企業よりも大規模企業の方が多かった。特に差が大きい「アップデート状況」「ネットワーク監視状況」では 10 ポイント以上の差があった。

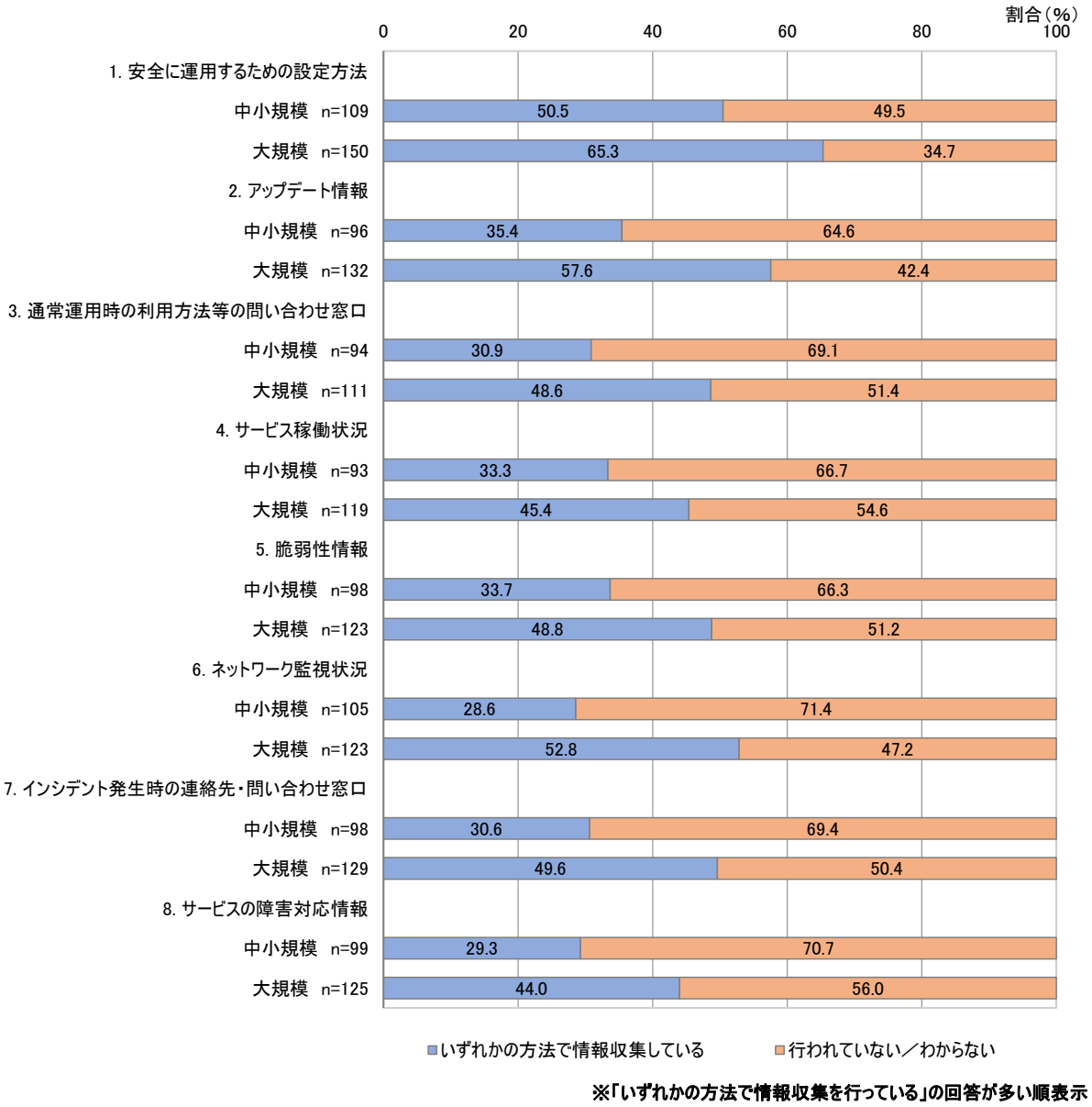


図 4-2-6 契約後（運用時）の情報利用の状況（企業規模別・利用者）　n=144

4.2.2 まとめ

本節では「事業者は利用者が SaaS を利用するために必要なセキュリティに関する情報を提供していない。」「利用者は SaaS を利用するために必要なセキュリティに関する情報を入手していない。」との仮説に対する調査結果を提示した。調査結果から、事業者・利用者共に「利用するための情報」について情報提供・情報収集は進んでいない状況がわかった。

事業者による情報提供については、契約前と同様に情報の内容によって情報開示している項目と、情報開示していない項目に分かれる傾向があった。利用者の情報収集・情報利用では、契約前と比較すると行われている傾向にあるものの、企業規模別にみると中小規模企業では行われていない傾向が顕著であった。また、情報開示・情報利用の方法に差が生じている傾向は契約前の情報開示・情報利用と同様であり、事業者は「SaaS を利用するために必要なセキュリティに関する情報」を提供する準備はしているものの、利用者は提供を要求していない。このため、事業者が提供するべきと考えている項目は実際には利用者に届いていない可能性が高い。

企業のセキュリティ対策に助言を与える立場の有識者の意見として、導入時の情報収集と比較すると、利用段階に移行した後には情報収集は積極的に行われていない状況にあるとのことである。実際に情報収集を要求される事業者からも、運用中の利用者からセキュリティに関する情報開示要求を受けることは極めて少ない状況であるとの声が聞かれた。

設問で設けた「SaaS を利用するために必要なセキュリティに関する情報」の項目では、問い合わせ窓口の状況等については公表される傾向にあったものの、その他の項目は多くが基本的に開示されておらず、インシデント発生時や必要がある場合にのみ開示される傾向にあった。この状況について、インタビュー調査の有識者からは基本的に開示するべき情報はすべて開示するべきであるとの意見と、調査項目のうち「ネットワーク監視状況」などは利用者に不要な情報であり、すべてを開示する必要はないとの意見があった。しかし、利用者にとって、SaaS の運用状況を確認し、インシデントが発生した場合に備えることはリスクマネジメントとして重要であり、インシデントが発生した後に対応方法を伝えられても間に合わない可能性がある。対応が後手になることで、事業の継続に支障をきたす可能性を考えると、運用状況について把握し、備えることは重要と言える。

ISMS（ISO/IEC27001）が 2022 年 10 月 25 日に改訂され、以前の版と比較し、情報セキュリティやクラウドに関する要求事項が増えている。世界的に見ても、クラウド・非クラウドを問わず情報システムに関する情報セキュリティの管理体制を強化することへの認識が高まりつつあるといえよう。

情報開示・情報利用においては選定時の情報収集に重点が置かれる傾向にあるが、利用を開始した後においても事業者・利用者共に適切な情報開示・情報収集を行わねばならない。

後述の調査結果に示すとおり、利用者、事業者共に ISMS の取得・認知が進んでいることから、ISO27001 の改定版が浸透することで、クラウドに関する情報収集が進む可能性にも期待したい。

4.3 情報利用の状況と目的

本節では、以下の 2 つの仮説について、アンケート調査およびインタビューの結果を踏まえて検証を行う。

- 仮説 No.3-1 利用者は選定するために入手したセキュリティに関する情報を利用できていない。

- 仮説 No.3-2 利用者は SaaS 導入後にセキュリティに関する情報を利用できていない。（仕様変更や新機能のリリース、関連する SaaS のインシデントなど）

4.3.1 調査結果

（1）利用者が SaaS の契約前（選定時）に入手した情報の利用状況と目的

利用者向けのアンケート調査では情報収集・情報利用のうち、契約前段階の情報収集に焦点をあて、調査を行った。その結果、SaaS の選定に際し、何らかの情報収集を行ったとの回答は 457 件中 401 件であった。項目ごとの情報利用の状況については図 4-1-3、図 4-1-4（4.1.1 節参照）のとおりである。

「何らかの情報収集を行った」と回答した対象者に対し、情報収集の目的について項目ごとのあてはまり具合を回答してもらった。結果は図 4-3-1 のとおりである。「自分たちが安心して利用するため」「SaaS 事業者の責任範囲を確認するため」「自社の責任範囲を明確にするため」といった項目で「あてはまる・ややあてはまる」の度合いは 60%以上となった。特に「責任範囲の明確化」は SaaS の利用にあたって、利用者と事業者の責任の所在を明確化することであり、セキュリティに関する認識の違いに伴う責任範囲の不明瞭な状況を防ぐために重要な事柄である。利用者は、利用者と事業者の責任の所在を明確にした上で SaaS を選定している、またはしたいと考えている傾向が見られた。

これらの調査結果から、入手した情報を利用して社内で検討を行うなど、利用者は、契約前の段階から情報を活用していることがわかる。

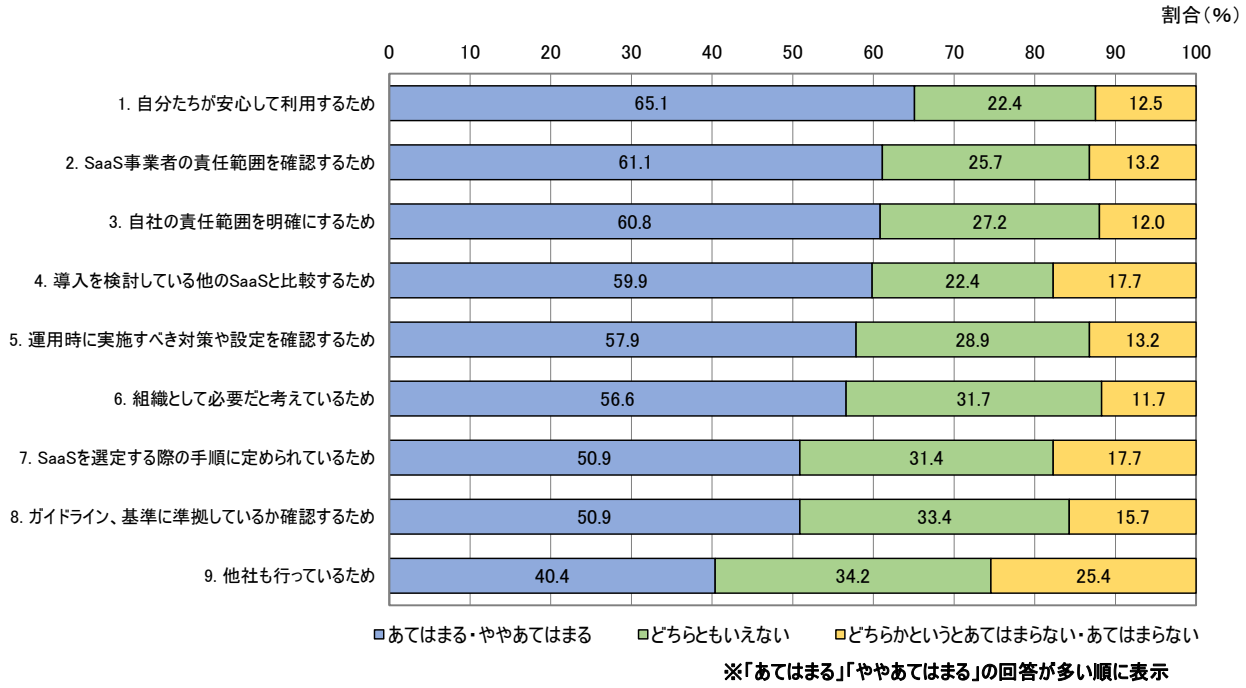


図 4-3-1　契約前（選定時）の情報収集の目的（利用者）　n=457

（２）利用者が SaaS の契約後（運用時）に収集した情報の利用状況と目的

SaaS を利用中の利用者が、必要に応じて、または定期的に情報を収集しているかについて調査を行った。ここでは、入手した情報の利用状況について、利用目的の選択肢を設け、あてはまり度合いを回答してもらった。結果は図 4-3-2 のとおりである。

「あてはまる・ややあてはまる」を「あてはまる」とし、「どちらかというとあてはまらない・あてはまらない」を「あてはまる」として表示している。全ての項目で「あてはまる」が最も多く回答されている。「あてはまる」の割合が最も多かった項目は「運用時に対応するべき対策や設定の情報を入手するため」で 70.4%を占めていた。「組織のルールで規定されているため」との回答は 58.7%となり、6 割近くの組織で情報入手が規定されていることがわかる。

有識者へのインタビューでは「SaaS のネットワークの状況や稼働状況に関する情報の開示割合は高くないが、SaaS の稼働を保証することは事業者の責任であり、利用者があえて入手する必要がない情報なのではないか」との指摘があったが、「稼働状況を確認するため」情報を入手している割合は 68.1%を占めており、利用者にとって稼働状況は重要な確認事項であることがわかる。

他の有識者へのインタビューにおいて、SaaS が事業の継続にとって必要不可欠になっているケースも多いと指摘もあり、SaaS の稼働が保証されることが利用者の事業継続にとって重要になってきているとものと思われる。

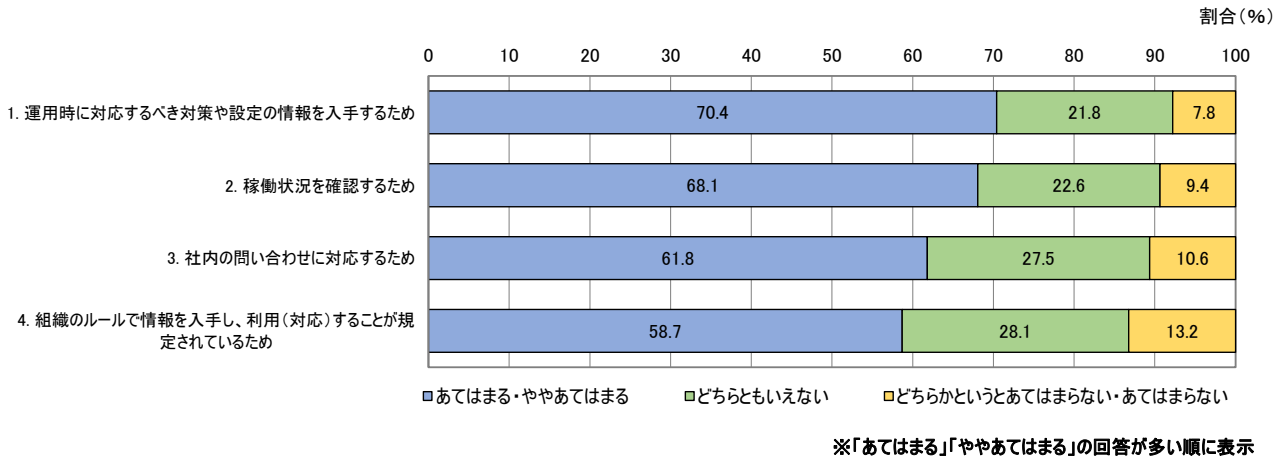


図 4-3-2　契約後（運用時）の情報収集の目的（利用者）　　n=457

利用者が入手した情報をどのように活かしているのかについて調査した。結果は図 4-3-3 のとおりである。「社内（事業部門・IT 部門など）で共有し、セキュリティ対策や運用に活かす」「担当者が参照し、セキュリティ対策や運用に活かす」がそれぞれ 45.5%、51.2%となり、実際に利用するために入手している様子が見られた。一方で「組織のルールとして入手している（利用の用途は把握していない）」が 20%を占め、規定しているもののその後の利用を把握できていない状況が一定程度見られた。

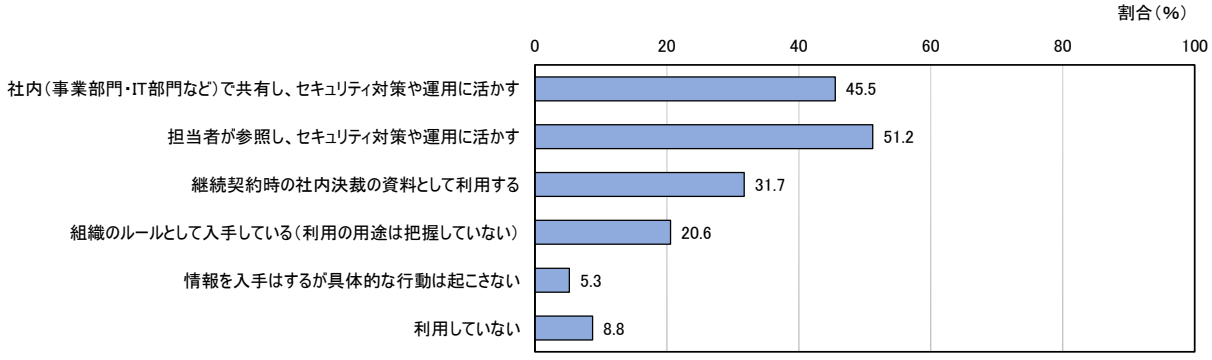


図 4-3-3　入手した情報の利用状況（利用者）　n=457

4.3.2 まとめ

本節では、「利用者は選定するために入手したセキュリティに関する情報を利用できていない。」「利用者は SaaS 導入後にセキュリティに関する情報を利用できていない。（仕様変更や新機能のリリース、関連する SaaS のインシデントなど）」との仮説に対する調査結果を提示した。調査結果から、利用者は入手した情報をセキュリティ対策等に利用している状況がわかった。

利用者は、安心して利用するためといった目的や、責任範囲を明確にするといった目的で情報を入手している。しかし利用者は「安全に SaaS を使用するために必要な情報」をすべて入手しているとはいえない状況であることが、4.1 節、4.2 節で明らかになっている。利用者は入手した情報を SaaS の安全な利用のために用いていると考えているものの、実態としては入手している情報の内容は十分ではない。このような状況から、必要な項目について情報利用ができている、とはいえない状況がわかった。

この背景として、「安全に SaaS を使用するために必要な情報」の認識が足りていない状況が挙げられるだろう。先に述べたように、クラウドとオンプレミスで開発・運用する環境は異なり、特に SaaS とオンプレミスで構築される情報システムの差は大きい。複数の有識者から、SaaS のセキュリティの情報を適切に入手・利用するためには利用者にクラウドセキュリティの知識が必要であることが言及されている。しかしながら同時に、利用者にクラウドセキュリティについて理解している人材が不足している点についても指摘があった。

これらの問題点については社内の技術者の育成や社外の有識者の活用といった対策が必要となると思われるが、これらの対策には一定程度の時間を要する、費用がかかるといった課題がある。人材育成を行うと共に、適切なガイドラインの利用や、信頼性のある認証制度の活用といった外部の情報を利用することで、クラウドセキュリティに関する情報を補完し、適切な情報利用を行うことができるだろう。

4.4　利用者が参照しているセキュリティの標準

本節では、以下の仮説について、アンケート調査およびインタビューの結果を踏まえて検証を行う。

- 仮説 No.4-1 利用者は SaaS を選定する際に基準とするべきセキュリティの標準がわからない。

4.4.1　調査結果

（1）利用者が用いるセキュリティの標準

利用者が行う情報収集・情報利用について、自社で備えている組織の規定や参照しているガイドライン等について調査した。調査結果は図 4-4-1、図 4-4-2 のとおりである。契約前（選定時）、契約後（運用時）ともに最も多く選択された選択肢は「他社の事例やコンサルタントなどの情報を参考にしている」であった。この調査結果について、有識者からは、コンサルタントであれば「情報開示指針」をはじめとした基準に基づいて情報提供を行っていると思われるが、他社の事例を参照している場合に、その他社がベストプラクティスであるかは疑問であるとの指摘があり、参考情報として適切ではない情報に基づき、情報取集が行われている可能性がある。

「他社の事例やコンサルタントなどの情報を参考にしている」に続いて多く選択された項目は「参照しているものはない」であった。「参照しているものはない」と回答した企業は、自社に蓄積された知識や経験を基に、自社に適したセキュリティ標準を作っているものと思われるが、そのセキュリティ標準がクラウドに適しているか、ベストプラクティスであるのかについては自ら確認・検証する必要があるだろう。事業者にインタビューを行ったところ、利用者からセキュリティに関する情報開示を求められる際に、オンプレミス前提のチェックシートが送られてくることもあり、クラウドサービスについての認識が不足していると感じることもあるとの声が聞かれた。

契約後（運用時）に入手する情報に関する組織の規定やルールについても調査を行った。調査結果は図 4-4-3　のとおりである。「クラウドサービス利用の規程・手順がある」は 42.5%であった。「クラウドサービス固有ではないが情報システム調達の規程・手順がある」「規程・手順にはなっていないが選定のルールがある」はそれぞれ 42.0%、19.0%となっており、クラウドに適した規定ではない規定・手順やルールに従って運用している可能性が高い利用者が一定数見られた。

契約前（選定時）に収集するセキュリティの情報について、「情報開示指針」を利用しているとの回答は 21.2%にとどまった。「情報開示指針」は、事業者向けに作られており、利用者が用いるべきものではないと思われている可能性がある。しかし、利用者が SaaS の利用に際し情報収集・情報利用を行う項目の指針として用いることも可能であり、より適切な情報収集が可能となると思われる。

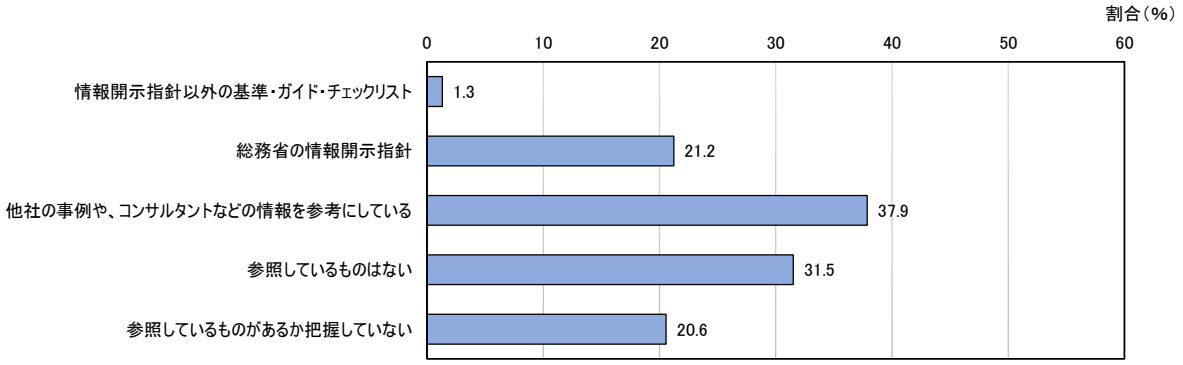


図 4-4-1 契約前（選定時）に収集するセキュリティの情報について参照しているガイドライン等（利用者）n=457

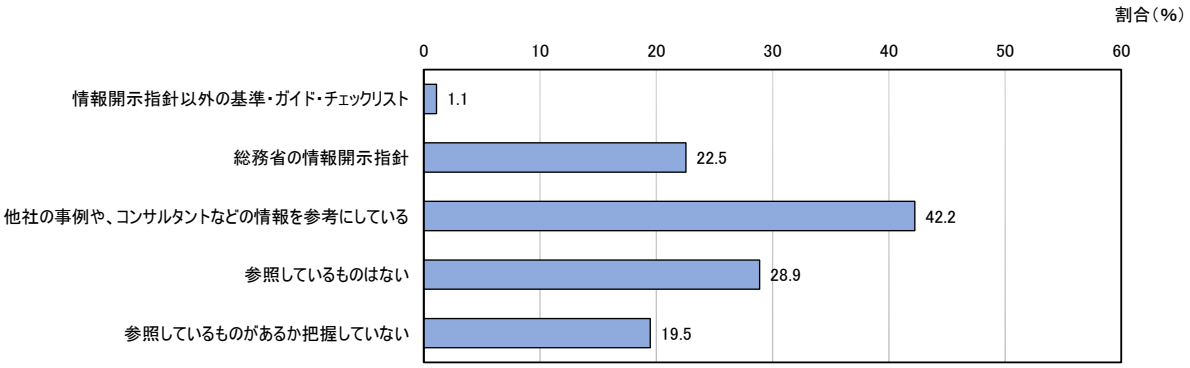


図 4-4-2 契約後（運用時）に収集するセキュリティの情報について参照しているガイドライン等（利用者）n=457

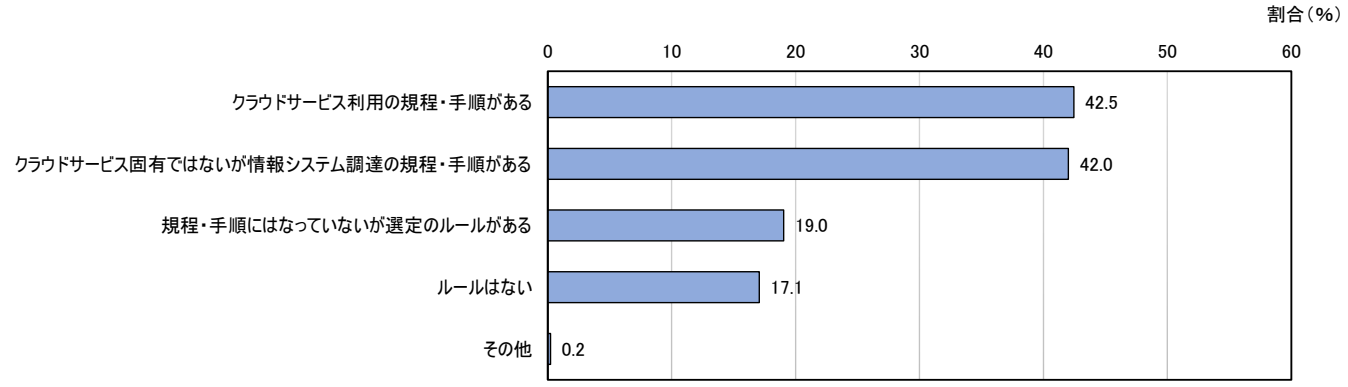


図 4-4-3　契約後（運用時）に入手する情報について組織の規定やルール（利用者）n=457

（2）事業者が用いるセキュリティの標準

利用者が行う情報収集と比較するために、事業者に行った調査についても取り上げる。調査結果は図 4-4-4 のとおりである。最も多く選択されたのは「他社が開示している情報を参考にしている」の 53.5%であり、総務省の「情報開示指針」は 44.4%と約半数にとどまった。

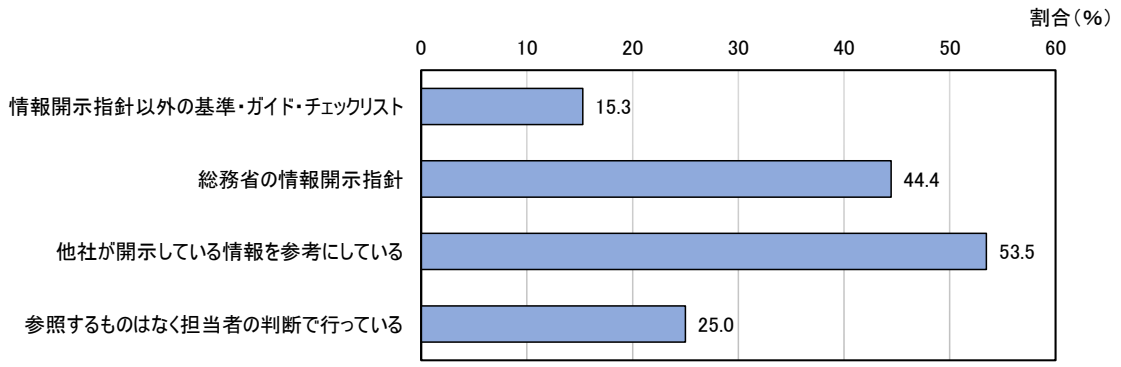


図 4-4-4　情報開示・情報提供を行う内容を決定する際に参照しているガイドライン等（事業者）n=144

4.4.2　まとめ

本節では「利用者は SaaS を選定する際に基準とするべきセキュリティの標準がわからない。」との仮説に対する調査結果を提示した。調査結果から、利用者は何らかのセキュリティ標準を備えているものの、そのセキュリティの標準が「情報指針」等の公的な基準やガイドラインに基づいていない可能性が高いことがわかった。

「ルールはない」を選択した 17.1%を除く 80%以上が何らかのセキュリティ標準を備えていたが、セキュリティの情報を入手する際に参照しているガイドラインとして、「参照しているものはない」が契約前（選定時）で 31.5%、契約後（運用時）で 28.9%となっており、「参照しているものがあるか把握していない」の回答も多くなっている。セキュリティの規定やルールがあっても、その規定やルールが基準や標準に基づいていない可能性が高いことが明らかになった。

利用者が情報収集時に参照しているガイドライン等の調査結果では、契約前（選定時）、契約後（運用時）ともに「他社の事例や、コンサルタントなどの情報を参考にしている」が最も多く回答された。この結果は事業者も同様であり、事業者に行った調査でも「他社が開示している情報を参考にしている」の項目が最も多く選択された。

この調査結果について、有識者へのインタビュー調査では、「社内の説明材料として、他社が行っていることと同様の対応を取るといった“寄らば大樹の陰”の姿勢が強く、自組織の状況にあわせたセキュリティ対策が行われておらず、セキュリティ対策が組織のリスクマネジメントの一環であるという自覚が薄いのではないか」という意見があがった。リスクマネジメントという点においては、他の有識者からも情報システム部門や利用部門に SaaS の管理を任せるのではなく、組織全体として SaaS のリスクマネジメントを行っていくことが必要であるとの提言があった。SaaS の利用が進み、組織にとって重要な事業の一部にも SaaS が利用されるようになりつつあるなか、SaaS のリスクマネジメントは経営課題の一つとして考えるべきであろう。

セキュリティの標準が備えられていても、その標準が適切でない場合には、情報収集・情報利用に抜けや漏れが生じる可能性もあるだろう。利用者においても、適切な指針・ガイドラインの項目を参

考に、セキュリティ標準を見直したり、情報収集すべき項目のチェックリストを作成したりといった「安全・安心な SaaS の利用」のための行動を進める必要がある。

4.5 SaaS の認定制度・認証制度の取得・利用状況

本節では、以下の 2 つの仮説について、アンケート調査およびインタビュー調査の結果を踏まえて検証を行う。なお、本調査で提示した「SaaS の情報開示認定制度や認証制度」は有識者のインタビューをもとにクラウドセキュリティに関連する主要な情報開示認定制度や認証制度を選んだ。クラウドセキュリティに関連する認定制度・認証制度への比較として、一般的に認知度が高いと思われる認証制度を選択肢として挙げ、事業者・利用者に対し取得・利用の実態を調査した。

- 仮説 No.5-1 事業者は SaaS の情報開示認定制度や認証制度を取得していない。

- 仮説 No.5-2 利用者は選定の際に SaaS の情報開示認定制度や認証制度を選定の基準としていない。

4.5.1 調査結果

（1）事業者の情報開示認定制度・認証制度の認知・取得状況

調査では、図 4-5-1 に挙げた項目について事業者に対し調査を行った。本調査に関連する情報開示認定制度・認証制度の詳細は 1.2.2 を参照いただきたい。

事業者側における情報開示認定制度・認証制度の認知・取得状況の調査結果は図 4-5-1 のとおりである。最も取得されている認定制度や認証制度は「ISMS（JIS Q 27001)」、次に「プライバシーマーク」であった。いずれも一般的な組織体制に関連する認証であり、クラウドセキュリティに直接関連する認証制度ではないが、認知度が高いことから取得が進んでいると思われる。

クラウドに関連した認証では「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証」（以下、ISMS クラウドセキュリティ認証）次に「ASP・SaaS の安全・信頼性に係る情報開示認定制度」が多く取得されていた。しかし、クラウドに関連した認証の中で最も多く取得されている「ISMS クラウドセキュリティ認証」でも、「既に取得している」「取得に向けて準備している」を合わせた割合は 23.4%であり、取得が進んでいるとは言えない。

認定制度や認証制度の認知状況について、「既に取得している」「取得に向けて準備している」「制度は理解しているが取得を検討していない」を「認知している」、「名前を知っている程度」「知らなかった」を「認知していない」としてみてみると、10 項目のうち 7 項目で「認知していない」の方が多くなった。

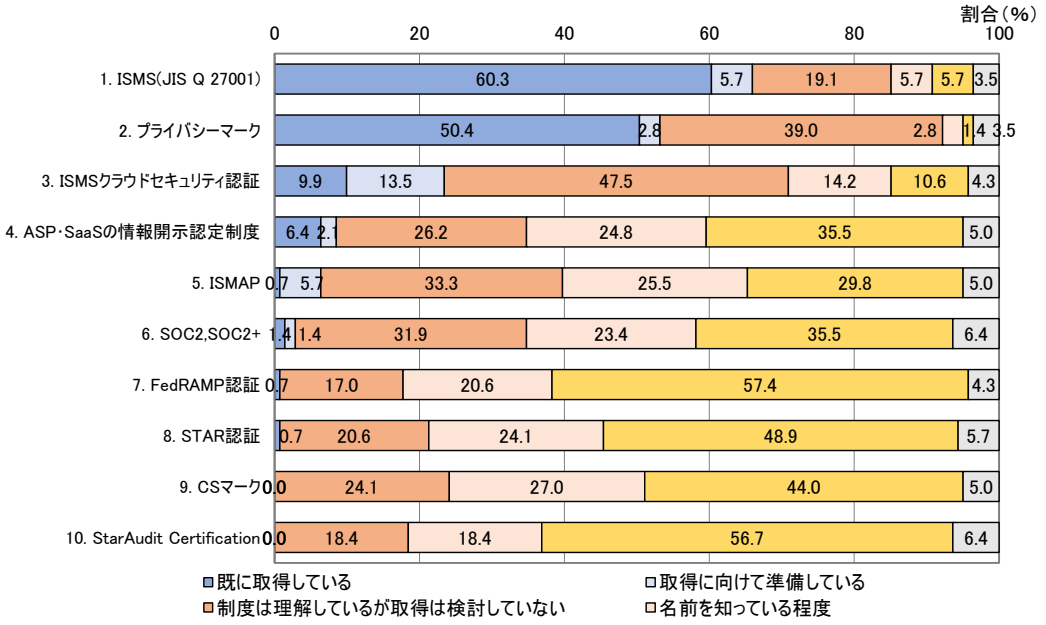


図 4-5-1　SaaS の情報開示認定制度や認証制度の認知・取得状況（事業者）　n=144

（２）利用者の情報開示認定制度・認証制度の認知・利用状況

利用者における情報開示認定制度・認証制度の認知・利用状況の調査結果は図 4-5-2 のとおりである。「知っており、選定の条件としている」「知っており、選定時に参考にしている」とした選択肢をあわせて「利用している」としてみてみると、最も「利用している」が多かった項目は「プライバシーマーク」であり、次に「ASP・SaaS の安全・信頼性に係る情報開示認定制度」が続いた。「ASP・SaaS の安全・信頼性に係る情報開示認定制度」は大規模企業を中心に利用されており、企業規模別の分析では大規模企業の 47.7%が利用していた。

事業者側で各種認証制度の取得状況が低かった一方で、利用者側では SaaS の情報開示認定制度や認証制度を事業者の選定条件として利用する傾向がみられた。今回の調査では、組織として SaaS を選定・導入している担当者を対象としていることから、組織として SaaS を選定・導入する際には、事業者の情報開示認定制度や認証制度の取得状況を参考としている事例が多いのではないかと思われる。

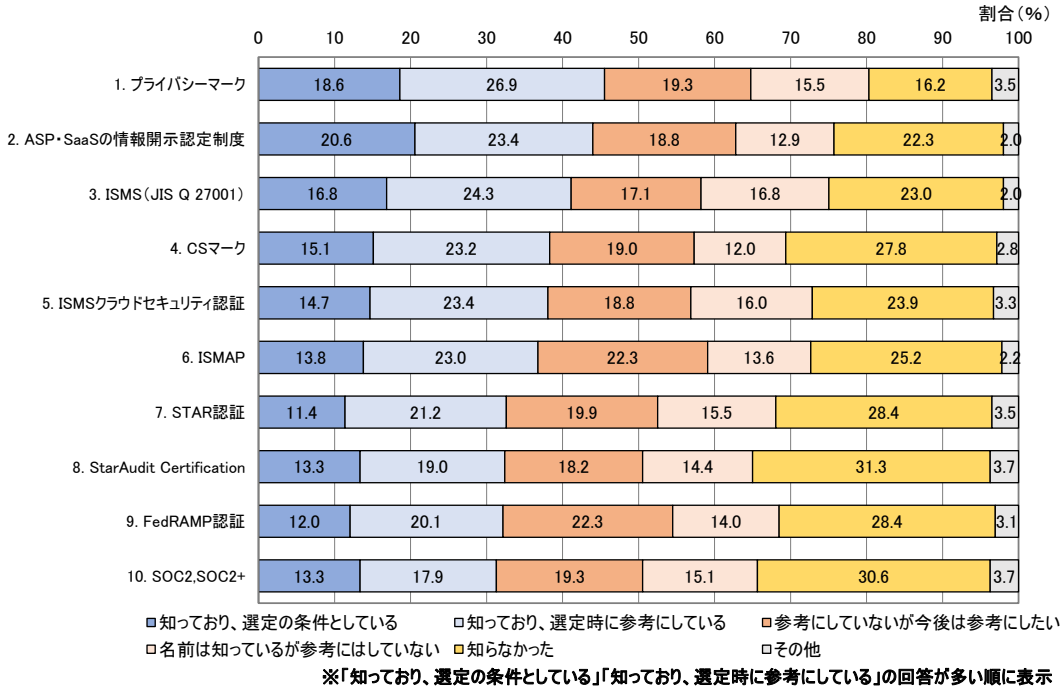


図 4-5-2　SaaS の情報開示認定制度や認証制度の認知・利用状況（利用者）n=457

（3）SaaS の情報開示認定制度や認証制度の認知・取得・利用状況についてのインタビュー

SaaS の情報開示認定制度や認証制度の認知・取得・利用状況について、有識者や事業者・利用者に対しインタビューを行った。

有識者からは「情報開示認定制度や認証制度は、事業者にとって SaaS のセキュリティを証明する手段として有効であり、利用者にとって SaaS を選定する際に積極的に活用することで利用者の知識を補い、選定時の工数を削減することにつながるものである。また利用者はリスクアセスメントとして、運用時にも認証を活用していくことができる」との提言がなされた。

事業者向けのインタビューでは「情報開示認定制度・認証制度は有効と思われるが、クラウドに関連する認証制度よりも、FISC 安全対策基準（金融機関が情報システムを構築する際の安全対策基準）など、認証を取得することで事業の範囲が広がる認証や基準を優先したい」との声が聞かれた。利用者向けのインタビューでは、大規模企業に属する利用者から「情報開示認定制度・認証制度を活用している」とのコメントがあったが、中小規模企業に属する利用者からは「情報開示認定制度・認証制度を必ずしも参考にはしていない」とのコメントがあり、それぞれの立場による違いが見られた。

事業者の認証・認定制度の認知・取得状況についてインタビューしたところ、認証・認定制度に詳しい有識者から「事業者は認定制度・認証制度の取得や更新に係る工数がかけられないようだ」とのコメントがあった。認定制度・認証制度の取得に要する工数が負荷となり、これらの取得が低調となっている可能性がある。

4.5.2 まとめ

本節では「事業者は SaaS の情報開示認定制度や認証制度を取得していない。」「利用者は選定の際に SaaS の情報開示認定制度や認証制度を選定の基準としていない。」との仮説に対する調査結果を提示した。調査結果から、事業者はクラウドに関連する認定制度・認証制度に対して認知しているものの取得に対し積極的ではない一方で、利用者は認証を利用して SaaS のセキュリティを判断していることがわかった。

このように事業者と利用者で SaaS の情報開示認定制度や認証制度の認知・取得・利用状況に差が生じており、意識の違いが浮き彫りとなった。

本調査では様々なクラウドに関する認証制度・認定制度を項目として挙げており（1.3 参照）いずれの制度も方式は異なるものの、優れた制度である。事業者・利用者共に適切に認定・認証制度を利用することで利用者が SaaS を安全な状態で利用することにつながるだろう。有識者によるインタビューでも「利用者が個々のセキュリティをチェックすることが困難であれば認証制度を活用することで知識を補い、工数を削減することができるのではないか」と提言されている。

このように優れた制度ではあるものの、認証制度・認定制度の取得・更新には費用・工数を要する。後述のとおり、情報開示・情報利用に係わる課題として事業者・利用者共に工数の不足を挙げており(4.7.1 参照)、すべての事業者に認証制度・認定制度の取得・利用を求めることは現状では困難であろう。

認証制度・認定制度を活用しつつ、ガイドラインや指針等を用いた情報開示・情報利用を進めていくことが必要である

4.6　事業者と利用者が感じている課題

本節では、アンケート調査およびインタビュー調査から浮かび上がった事業者・利用者が感じる情報開示・情報利用における課題について取り上げ、分析する。

4.6.1　調査結果

（1）事業者が感じる課題

事業者向けのアンケート調査において、SaaS の情報開示・提供における課題として想定される項目について「強くそう思う」「どちらかというとそう思う」「どちらでもない」「どちらかというとそう思わない」「全くそう思わない」のいずれかを選択してもらった。結果は図 4-6-1 のとおりである。なお、図 4-6-1 においては「強くそう思う」「どちらかというとそう思う」を「そう思う」とし、「どちらかというとそう思わない」「全くそう思わない」を「そう思わない」とし、三区分で表示した。

「情報開示・情報提供に対応する工数がかけられない」の項目が 40.3%と最も多く選択された。インタビュー調査においても「事業者から“人が足りていない”との意見が多く寄せられている」とコメントがあり、アンケート調査の結果と一致していた。

「メンテナンスができていない」は「そう思わない」を 50.7%と半数近くが選択した一方で、25.7%が「そう思う」を選択しており、四分の一の SaaS では情報を適切に更新できていないことがわかった。

また、事業者向けのインタビュー調査では「情報開示しているにも関わらず問い合わせが減らない」ことが課題として挙げられていたが、アンケート調査では「そう思う」が 16.7%と多くはなく、情報開示によって問い合わせが減っていることが分かった。

「情報開示・情報提供の必要性がわからない」を選択したのは 8.3%、「情報開示・提供について職場で反対される」は 2.8%にとどまり、事業者として「情報開示は必要である」との考えが広く浸透していることがわかった。

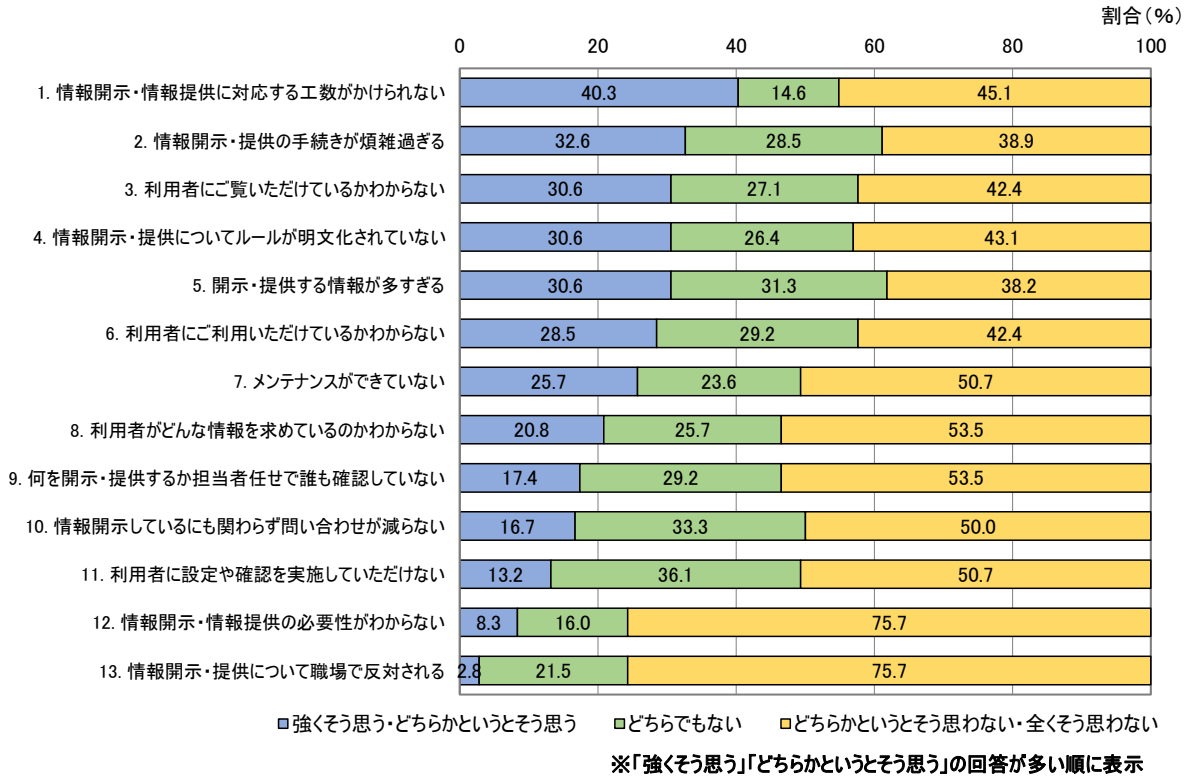


図 4-6-1　情報開示・提供における課題（事業者）

（２）利用者が感じる課題

利用者向けのアンケート調査では、事業者向けアンケートと同様に SaaS の情報収集・利用における課題として想定される項目について「強くそう思う」「どちらかというとそう思う」「どちらでもない」「どちらかというとそう思わない」「全くそう思わない」のいずれかを選択してもらった。結果は図 4-6-2 のとおりである。なお、図は（１）と同様に三区分で表示した。

事業者向けアンケートと異なり、項目間の差は少なく、かつ「そう思う」「どちらでもない」「そう思わない」がほぼ三等分になる結果となった。最も多く選択された項目は「情報収集・利用する情報が多すぎる」の 39.2%であり、「情報収集・利用に対応する工数がかけられない」が 38.5%と続いた。

利用者においても情報収集・情報利用を行う工数が負担になっていると思われる結果となった。

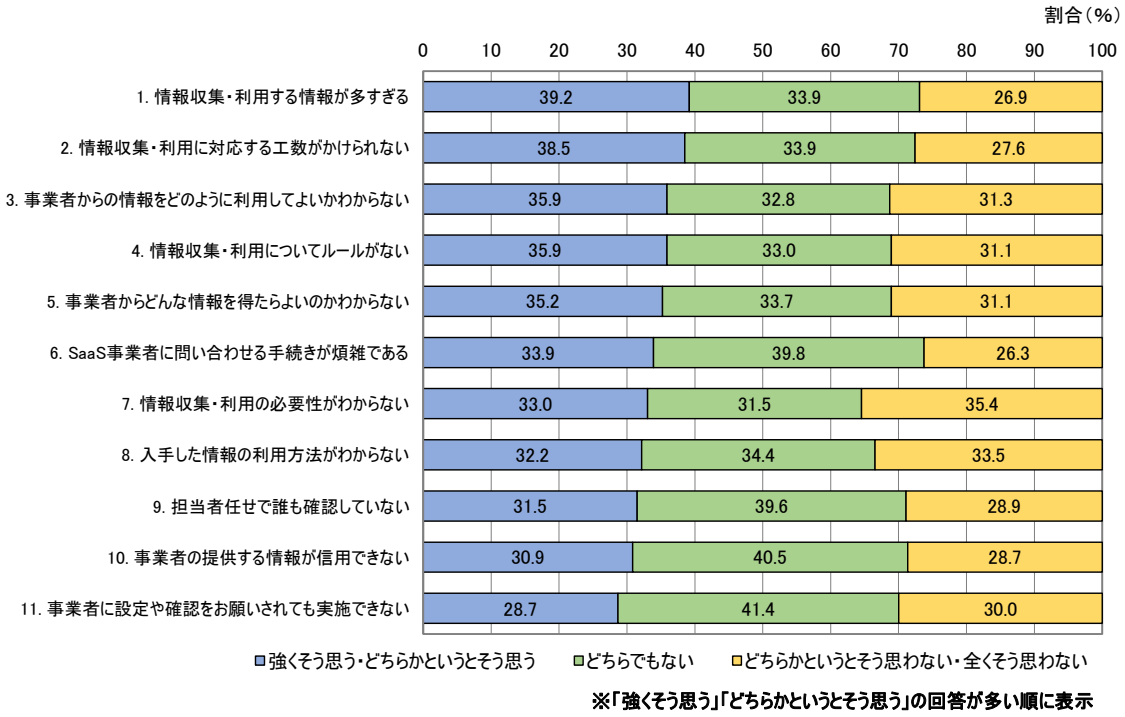


図 4-6-2　情報収集・利用における課題（利用者）

利用者における課題について、企業規模による分析を行った。結果は図 4-6-3 のとおりである。大規模企業では、各項目で「そう思わない」を選択する割合が低く、大規模企業では情報収集・情報利用に対する課題感が中小規模企業よりも小さいことがわかる。

次に、業種による分析を行った。結果は図 4-6-4 のとおりである。製造業では、11 項目のうち 6 項目で課題に対し「強くそう思う」「どちらかというとそう思う」が多く選択された。各項目において「情報通信業」では「そう思わない」の割合が多く、比較的課題として捉えられているが少なかったが、「入手した情報の利用方法が分からない」「事業者の提供する情報が信頼できない」はいずれも業種による差は少なく、「入手した情報の利用方法が分からない」では 40%近く、「事業者の提供する情報が信頼できない」はいずれの業種でも 45%以上が選択していた。

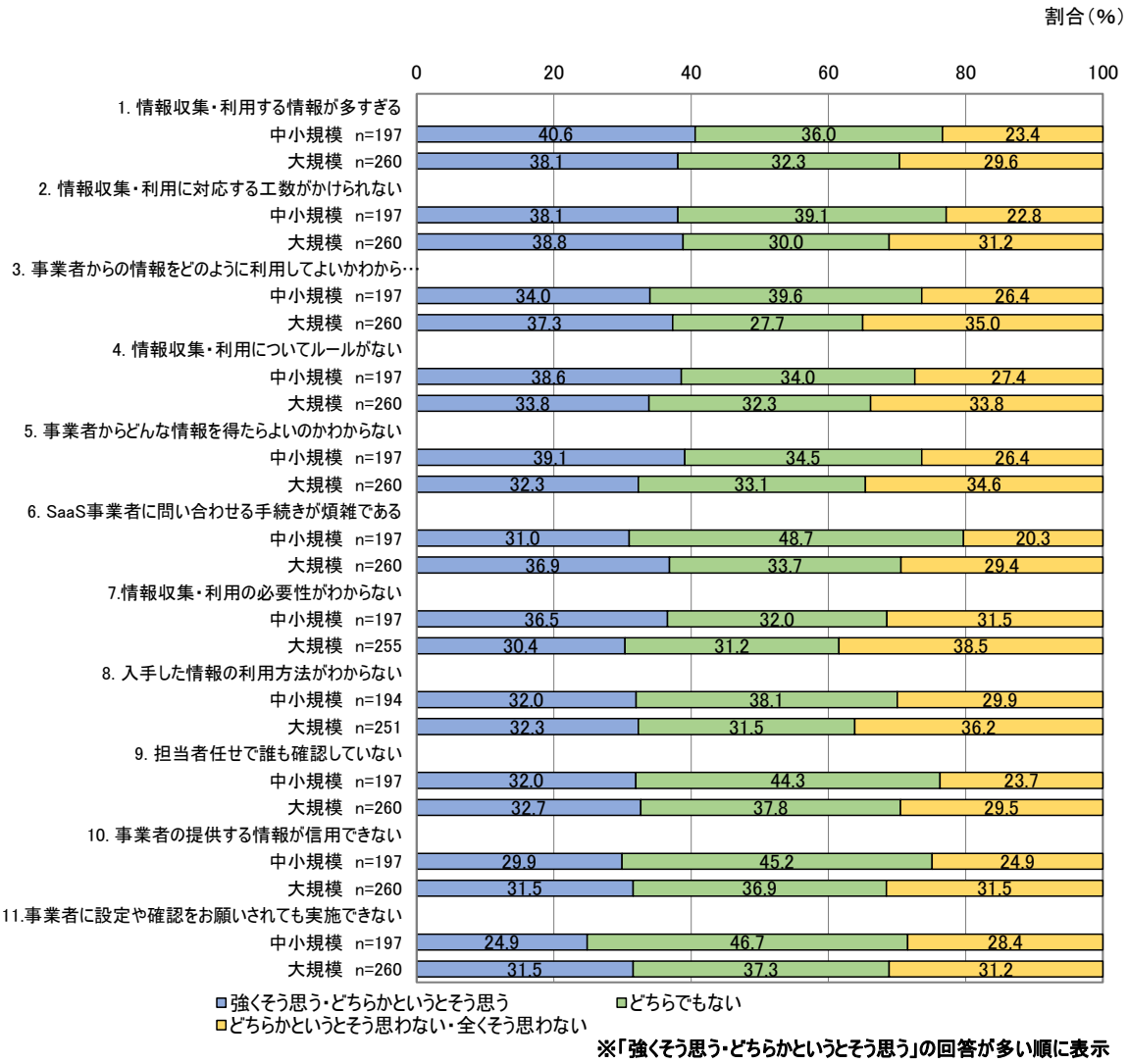
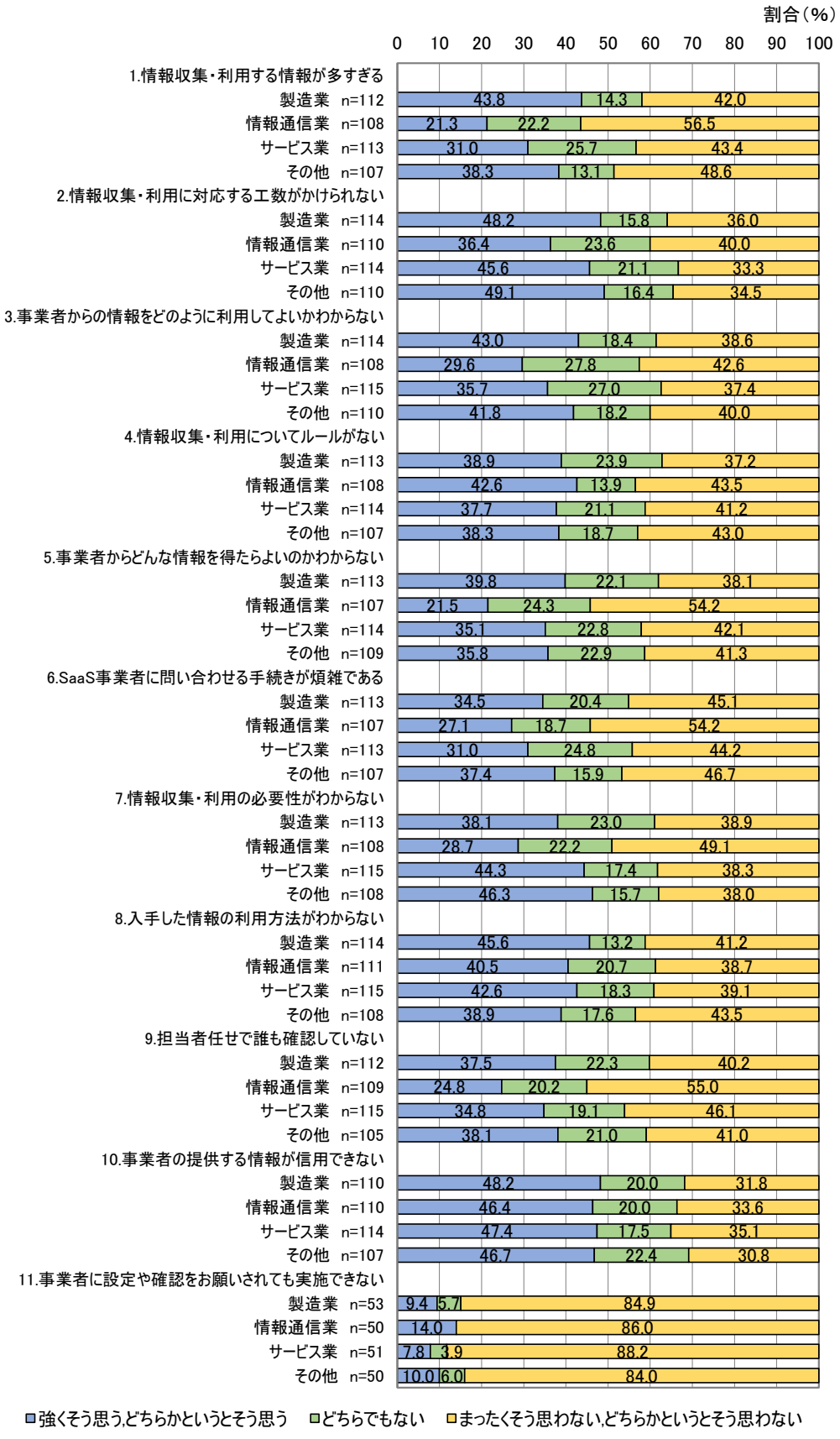


図 4-6-3　SaaS の情報収集・利用における課題（利用者・規模別）



※「強くそう思う・どちらかというとそう思う」の回答が多い順に表示

図 4-6-4　SaaS の情報収集・利用における課題（利用者・業種別）

（3）インタビュー調査による課題の分析

これらの事業者・利用者アンケートで浮かび上がった課題について、有識者へのインタビューを通じて背景を探った。

利用者向けアンケートでは、規定やルールに従って情報収集をおこなっているものの、それらを用いて比較・分析など行われていない利用者が一定数存在していた。この点について事業者へ行ったインタビューでも、情報開示・情報提供はするものの、利用者がそれらを用いてリスク管理等の対応を行っているのかはわからないとの課題が挙げられた。

一方、組織にセキュリティのコンサルティングを行う有識者へのインタビューでは「企業規模による差や業種による差は少なく、経営者や情報セキュリティに対する認識の差の方が大きい」との意見があった。

また事業者から、「セキュリティに関する情報は間違いが許されないため、情報開示に際して社内で複数の担当者に確認が必要となり、時間を要する傾向にある」と工数がかかる要因についてもコメントがあった。

4.6.2 まとめ

事業者・利用者共に情報提供・情報利用に対する課題を抱いており、主として工数について課題を感じていることがわかった。

事業者向け調査では課題として挙げられた上位 5 項目のうち 3 項目が、情報開示に係わる工数や業務内容に関する課題であり、これらの影響が大きいことがわかった。事業者は、情報提供の重要性を認識しているものの、情報開示に工数をかけられずにいる。その背景として、セキュリティにかかわる情報は間違いが許されないとの認識が更に事業者の負担を増していることがうかがえた。

利用者向け調査では、課題として提示した 11 項目のうち 10 項目で「強くそう思う」「そう思う」が 30%以上選択されており、情報収集・利用において複数の課題を感じている利用者が多い様子がうかがえた。利用者においても上位 5 項目のうち 3 項目が工数に関する課題であり、情報収集・利用に関する工数が課題として大きいことがわかる。

利用者の課題は企業規模や業種による傾向の差は小さく、いずれの項目も利用者に共通した課題であることがわかった。

工数に関わる課題をすぐに解決することは困難であるが、情報開示・情報収集に関わる業務については有識者より「AI ツールの活用により課題の解決を目指すことができるのではないか」との提言があった。

5 情報開示・情報利用の現状に関する課題

本章では、4 章で述べた調査結果から明らかになった情報開示・情報利用の現状と課題そしてあるべき姿と実態の差について考察する。

5.1 情報開示・情報利用の重要性に関する調査結果

1 章において、事業者・利用者双方に情報開示・情報利用が重要であることを述べてきたが、本節では調査結果を踏まえ、情報開示・情報利用の重要性とその背景について考察したい。

「情報開示指針」では、資料の目的を「クラウドサービスに係る情報開示が進展することにより、各サービスの情報を横並びで比較でき、クラウド利用者がより安全・安心にクラウドサービスを利用できることを期待するものである。」としており、安全・安心なクラウドサービスのために情報開示・情報利用が重要であることを示している。

今回、学術分野の有識者に行ったインタビュー調査では、利用者に安心して SaaS を利用してもらうための事業者の情報開示の必要性と、利用開始前に情報を入手し理解してもらうこと、利用開始後にも情報を利用してもらうことの重要性について言及があった。

利用者が導入前に行う情報収集によって自社のセキュリティポリシーに則した SaaS を選択することが重要であると共に、SaaS 製品の設計意図や背景を知ることで、より適切に利用できる。また、利用にあたり自組織に適したセキュリティ対策を行っている製品を選ぶこともできるだろう。利用者向け調査でも、SaaS 選定時の情報収集の目的として「自分たちが安心して利用するため」が多く選ばれており、利用者にとって導入前の情報収集は安全・安心な利用に有効な情報と考えられる。また、利用開始後の情報利用も重要である。自社の状況の変化やサービスの提供内容に変化があれば、自社が求めるセキュリティレベルと差が生じる可能性があり、常に情報利用を行うべきであろう。

事業者が行う情報開示は利用者の安全・安心につなげるため重要であるが、事業者と利用者の責任範囲を明確にするために行うメリットもある。1.3.2 で述べた「責任共有モデル」を機能させるためには、事業者自身が負う責任範囲を明確にしたうえで利用者が負うべき責任範囲を明確にし、利用者にそれらを認識してもらう必要がある。情報開示を進め、利用者との責任共有を進めることは事業者にとってもメリットであろう。

一方、事業者が挙げる情報開示のデメリットとして、情報開示に起因したサイバー攻撃を懸念する声があると有識者からコメントがあった。しかし、別の有識者からは「機密性の高いアクセス権情報や脆弱性情報などの情報は開示する必要はないが、対策の取り組み状況を開示することは、組織の透明性や安全・安心な利用をしていただきたいという会社の姿勢を表すものであり、むしろ事業者が情報開示を拒むことは、うしろめたさやセキュリティ対策の自身のなさを露呈することになるのではないか」といった意見もあり、今後はこれらの実態について更なる調査が必要である。

利用者が収集した情報を利用しないことで生じるデメリットも存在する。その一つは情報共有・情報管理に不備が生じうる点である。事業者から開示された情報を組織内の利用者に対して展開、共有するといった対応をおろそかにした場合、利用方法の教育や障害発生時の復旧対応に時間がかかり非効率になる可能性もある。また、セキュリティに関する情報は多岐にわたるため、情報の入手方法、共有方法が整理されていない場合には業務が非効率化し、情報管理の不備が生じる可能性もあることにも留意する必要がある。

5.2 事業者と利用者の間の認識の違いによる脅威やリスク、課題

ここでは、アンケート調査並びにインタビュー調査の結果から明らかになった、事業者と利用者の間の認識の違いによる脅威やリスク、課題について考察する。

5.2.1 事業者と利用者の間の認識の違いによる脅威やリスク

事業者と利用者の間の認識の違いとして、事業者・利用者の双方が情報開示・情報利用が相手任せになっている点が挙げられる。事業者は「必要な情報であれば、利用者は開示を要求するはずであり、要求されなければ開示する必要はない」と思っており、利用者は、「必要な情報であれば開示されているはずであり、わざわざ情報開示を求める必要はない」と考えている状況があった。つまり、双方とも情報開示・情報利用を行う準備はしており、実際に行っているものの、事業者の情報は利用者に届いていない可能性がある。この状況が続けば、利用者が入手するべき情報を得ないことで、自社が求めるセキュリティレベルを満たしていないサービスを導入してしまう可能性がある。事業者にとっても、利用者が適切な利用方法等の情報を得ないまま利用することで、インシデントが発生することは望ましくないだろう。

情報開示は事業者が主体的に行わない限り、利用者は情報を入手することが出来ない。事業者がサービスに責任をもって対応することは重要であるが、対応を行っていても情報開示を行わなければ、利用者にリスクマネジメントの機会を失わせることになりかねないだろう。

5.2.2 事業者と利用者の間の認識の違いに係わる課題

利用者が要求した情報を事業者が開示するという構図が成立するためには、利用者が、事業者に求めるべき情報を十分に認識している状態が成立せねばならない。本来であれば、SaaS の情報利用・情報収集は、自社の状況や、導入を予定している SaaS に求めるセキュリティレベル等を検討しながら行うべきものであり、SaaS が組織の根幹である事業に係るものであれば、そのための情報収集・情報利用を行う必要がある。今回の調査結果から、「情報開示・情報利用を行うべき情報」については、事業者・利用者共に他社の情報を参考にしている傾向が強いことがわかっている。「情報開示・情報利用」の前提とする「情報」そのものの認識が事業者・利用者間で異なることは、課題の一つであろう。

また、事業者・利用者間のセキュリティに関する情報への考え方の相違は大きな課題であるといえる。事業者に行った課題に関する調査結果からも「利用者に利用いただけているかわからない」「利用者がどのような情報を求めているのかわからない」といった項目が課題として挙げられており、事業者・利用者間でセキュリティについての共通認識を得るためには情報共有に課題があるといえる。

5.3 情報開示・情報利用のあるべき姿と実態

5.1 で述べたとおり、クラウド利用者がより安全・安心にクラウドサービスを利用するためには各種サービスの比較・検討を可能とするための情報開示が必要である。

ここでは、1.3.2 で取り上げた情報開示・情報利用のあるべき姿について調査の結果を踏まえて考察する。

インタビュー調査では、多くの有識者から情報開示における「情報開示指針」の重要性について言及があり、「情報開示指針は非常に優れた資料であり、活用することで SaaS を安全・安心に利用することができる。積極的に活用するべきである」との提言があった。

また、利用者の情報利用においても「情報開示指針」は参考とすべき資料である。「情報開示指針」は事業者が活用していくべき指針であると解釈されていることも多いが、利用者が事業者に情報開示を求める際に根拠とするべき項目が提示されており、これらの項目に基づき情報開示を求め、情報収集を行うことで利用者にとって必要な情報を網羅することが可能となるだろう。

事業者の情報開示においては、情報開示の手段も検討する必要がある。1.3.2 で述べたとおり、「クラウド設定ガイドライン」では、情報を提供する時期や手段についても検討するべきとされている。アンケート調査・インタビュー調査では、事業者は「情報開示指針」の項目に従い利用者からの情報開示の要求に応じる準備をしていても、利用者から情報開示について要求されるケースが少ない傾向がわかった(4.1.1 参照)。利用者が効率的に情報収集を行える環境を整えるためにも、事業者は「情報開示指針」の項目について積極的に開示していく必要があると思われる。

クラウドサービスの利用において重要な概念である、責任共有モデルについては 1.3.2 で述べたとおりである。責任共有モデルは「クラウド設定ガイドライン」でも取り上げられており、安全・安心な SaaS の利用のために欠かすことが出来ない考え方である。事業者・利用者の責任範囲を明確にし、インシデントが発生した際には、自社が負うべき責任の範囲内でリスクマネジメントを行う必要があることは本調査のインタビュー調査でも有識者から指摘されている。利用者が SaaS を利用できなくなった場合に自組織に与える影響の大きさを判断し、その影響が大きくなる場合には自組織の判断で対策を講じる必要がある。

こういった SaaS の可用性についての情報は、利用者が知りえない事業者の情報である一方で開示は進んでいない状況が見られる(4.1.1 参照) 。利用者はリスクマネジメントのための情報として、事業者に対し情報開示を求めていく必要がある。利用者が事業活動をする上で、SaaS の利用をリスク要因の一つとして捉え、SaaS を導入する際の選定の条件や SaaS を運用する際に入手、活用すべき情報として何が必要であり、何を活用するべきであるのか判断する資料として、「情報開示指針」は有効である。そのためにも事業者は「情報開示指針」に提示された項目に基づいて情報開示を行うことが望ましい。なお、その際には利用者が収集・利用しやすい形式に留意して行うべきであろう。

利用者は「情報開示指針」提示された項目に基づいて情報収集を行い、収集した情報を基に SaaS の比較・評価・検討を行い、不足する情報があれば事業者に要求する必要がある。その際には、自組織が必要とする機密性・可用性等のリスクレベルを勘案したうえで選定を行わなければならない。また、入手した情報に基づくリスクマネジメントを行うことで、SaaS の利用に伴うリスクに対応していく必要がある。

これらの情報開示・情報収集は契約後も行うべきであり、事業者は定期的に情報開示を行い、状況

の変化などの必要があれば適宜情報開示を行うべきである。利用者も定期的な情報収集を通じて評価を行い、自組織の状況の変化に応じて適宜リスクマネジメントを行うべきである。

事業者は情報開示をサービスの一環として行うだけではなく、情報開示は事業者に求められる責任の一つであると考える必要がある。

利用者は、SaaS を安全に使うために、セキュリティをはじめとした SaaS の情報の開示を事業者任せにするのではなく、利用者自らが選定の時点からセキュリティを意識し、常にリスクをマネジメントしていく必要がある。

5.4 情報開示・情報利用のあるべき姿と実態の乖離

5.4.1 情報開示・情報利用のあるべき姿と調査結果から得られた実態の比較

1.3 並びに 5.2 において示した情報開示・情報利用のあるべき姿と、本調査の調査結果から得られた実態とを比較した。結果は以下のとおりである。

・事業者の情報開示は行われているものの、情報の内容により開示状況が異なる。また、開示の方法については利用者が利用しやすいものとはいえない（4.1. 1 参照）。
・利用者が情報収集する項目は必要な項目と比較して不足している。また収集した情報を利用できているとは言えない（4.1.1、4.3.1 参照）。

5.4.2 情報開示・情報利用のあるべき姿と調査結果から得られた実態の乖離の要因

あるべき姿と調査結果との乖離の要因として以下が考えられる。

・事業者が情報開示を行う際に従うべきガイドライン・指針が十分に認知されていない
・利用者のクラウドセキュリティに関する認識に不足がある
・事業者と利用者で情報開示・情報利用の方法に差がある

（1）事業者におけるガイドライン等の認知

事業者の情報開示の状況について調査したところ、項目によって情報開示の状況に差が生じていることがわかった。

事業者にとって情報開示は必要であり、行うべきであるとの考え方は浸透している（4.1.1 参照）。情報開示する項目として指針・ガイドライン等に従うことが望ましいものの、調査結果では「他社が開示している情報を参考にしている」が指針・ガイドラインを参考にしているとの回答よりも多くなっており、基準とするべき資料を用いていない実態がわかった（4.4.1 参照）。

何を開示するべきであるのか、事業者に伝わっていないことが、事業者の開示状況に差が生じる一因と思われる。

（2） 利用者におけるクラウドセキュリティへの意識

次に利用者の状況を分析すると、クラウドセキュリティに関する認識が不足していることが大きな要因として浮かび上がった。

1.2.2 クラウドサービスのセキュリティ対策で述べたとおり、クラウドとオンプレミスのシステムでは開発・運用の前提が大きく異なるが、その実態が利用者に認識されているとは言い難い。事業者へのインタビューにおいても、クラウドサービス選定のための情報として利用者から要求されたセキュリティチェックシートであるにも関わらず、内容は境界防御型の体制や対策などオンプレミスを想定した項目ばかりで、クラウドサービスのセキュリティ要件が含まれていない事例があったとの声が聞かれた。

また、情報システムを提供するベンダーも多様なクラウドサービスの利用に精通していないことも

あるため、利用者は注意が必要である。利用者に行ったインタビュー調査では、情報システムの開発を請け負ったベンダーがクラウドの機能仕様、サービス仕様や動作環境といった情報を精査せず、安易にシステムの基盤をクラウドへ移行したことで、一部のシステムがクラウド上で動作しなくなりトラブルが発生したとの事例が挙げられた。このケースでも、クラウドをオンプレミスと同様に認識しているのではないかと思われる。自社のルール・規定に関する設問（4.4.1 参照）では、クラウドサービスに関する規定を備えているとの回答は 42.5%であり、半数以上は規定をクラウドサービスに適した形で備えていないことが分かった。

オンプレミスとクラウドにおけるセキュリティ対策の違いと、利用者の責任について認識がされていない傾向にあることは、有識者へのインタビューでも指摘されている。オンプレミスのシステムで用いることが多い、重要な機器や情報を外部から隔離して防御する境界防御の考え方と、クラウドサービスで取り入れられている場所や機器を基本的に制限せずに、すべての通信を信頼しないことを前提にセキュリティ対策を講じるゼロトラストの考え方とでは、セキュリティ対策が大きく異なる。また、責任共有モデルで示されているとおり、クラウドにおいては利用者が主体となって情報収集・情報利用を行い、自社が負うべき責任範囲を認識して行動しなければならない。

（３） 事業者・利用者間の情報開示・情報利用の効率化

本調査では、事業者と利用者間で、情報開示・情報収集の方法に差が生じていることがわかった。事業者は今回の調査で提示した「情報開示するべき項目」のうち、一定以上は要求があれば開示を行うという結果であったが、利用者は公開情報を利用する割合が高く、事業者に要求して情報を収集するとの割合は少なかった（4.1.1 参照）。事業者はすべての情報を約款や HP 等で公開していないが、要求された場合に回答する準備はできており、利用者に対して、必要に応じて問い合わせしてほしいと考えている。一方、利用者は、情報収集に工数がかけられず、情報収集するべき項目についての認識も不足しているため、約款や HP などの公開されている情報だけで判断する傾向にある。情報収集するべき項目について指針・ガイドラインなどの基準に照らして検討しなければ、公開されていない情報のうち何を要求すればいいのかもわからないだろう。

これらの結果から、事業者が情報開示する準備をしていても、利用者は実際にはその情報を入手できていないことがわかる。

有識者へのインタビューでは、インフラの物理的な状況（建物形態、耐震・免震構造）やネットワークの状況など、事業者にとって情報を開示するためには内容が複雑であったり、調査に時間を要したりといった項目が開示されていない傾向にあるのではないかという指摘があった。こういった項目は利用者から要望があれば提示するものであるとの認識も聞かれたが、アンケート調査の結果、利用者が情報開示を要求する割合は少ない。利用者が事業者に情報開示を要求しないと得る事ができない情報を入手出来ていない可能性がある状況では、利用者が公開情報等を用いて情報収集を行い、得られた情報とには内容の偏りが生じる。

これらの情報収集における課題について、複数の有識者から利用者側にもクラウドセキュリティに関する技術者が必要であるとの提言があった。利用者側に技術者がいなければ、クラウドセキュリティに関する業務の一部を外部に委託する方法も考えられるが、コストの面からも簡単には実現できないだろう。また、社内で技術者を育成するためには時間がかかり、すぐに対応することは困難である。

これらには、長期的視点と短期的な視点のそれぞれの解決策が必要である。有識者からも「長期的

には技術者の育成を進めていく一方で、利用者においては各種の指針・ガイドラインや認証・認定制度を利用することにより選定時のセキュリティにかける工数を減らすといった方法や、協会・団体が提示しているチェックリストを用いることで、利用を検討、または利用中の SaaS のセキュリティをチェックする方法があるだろう」という提言があった。

6 情報開示・情報利用における課題の解決に向けて

6.1 課題解決のために事業者・利用者が実施すべき対策と課題への対応

本節では、実態調査で明らかになった情報開示・情報利用の課題について、解決のために実施すべき施策を検討する。

6.1.1 指針・ガイドラインを用いた情報開示・情報利用の網羅性の確保

4.1 に述べた調査結果のとおり、事業者の情報開示の方法と利用者の情報利用の方法に傾向の違いがみられた。これらの要因の一つとして、事業者・利用者が適切な指針やガイドラインに従っていないことが考えられる。契約前（選定時）の情報開示の状況（図 4-1-1）では、今回の調査で開示すべき項目として設定した項目のうち、契約前の情報開示では比較的網羅されている傾向にあったが、契約後の運用時については情報開示が行われているとは言い難い傾向にあった（4.2.1 参照）。また、事業者が情報開示にあたって参考としている指針やガイドラインに関する調査では「他社が開示している情報を参考にしている」との回答が最も多くなっていた（4.4.1 参照）。参考としている他社が、指針やガイドラインに基づく開示を行っているのであれば、自然と「情報開示指針」等の指針やガイドライン等の資料にたどりつくはずであり、この調査結果を勘案すると、事業者が開示している項目の妥当性には疑問が残る。

利用者向けのアンケート調査でも、契約前に参考としている指針やガイドラインについて調査したところ、「他社の事例や、コンサルタントなどの情報を参考にしている」の回答が 37.9%、「参照しているものはない」の回答が 31.5%となっていた。事業者と同じく利用者についても情報収集・情報利用している項目の網羅性には疑問が残る。

これらの状況について、インタビュー調査で、事業者・利用者が参照すべき指針やガイドラインについて有識者にたずねたところ、複数の有識者が総務省の「情報開示指針」を取り上げ、事業者にとどまらず、利用者も広く利用すべきであるとの提言がなされた。

また、総務省が公表している「クラウド設定ガイドライン」は利用者・事業者双方を対象としており、事業者だけではなく、利用者にとっても有用なガイドラインとなっている。

SaaS を安全・安心に使うための情報開示・情報利用は重要であるものの、項目に不足があれば、有効な情報開示・情報利用が出来ているとは言えない。有識者によって作成された指針やガイドラインに基づくことで、必要な項目を網羅することが出来ると考える。

6.1.2 利用者におけるリスクマネジメントの重要性に係わる認識の向上

SaaS の利用拡大に伴い、事業の根幹となる情報システムの一部に SaaS が用いられるケースも増えてきている。そういったケースでは、事業継続計画の一環として、SaaS にインシデントが発生した場合の影響について、会社としてリスクマネジメントを行うことが重要である。

2021 年に発生した Amazon Web Services の大規模障害や、第一章で述べた Microsoft の大規模障害に見られるとおり、大手の事業者が提供するクラウドサービスであっても障害やサービス停止が起こらないわけではない。これらのインシデントでも明らかとなったように、事前に情報収集・情報利用を行い、リスクマネジメントを行った利用者はインシデント発生時に適切な対応策を取ることが出

来た一方で、リスクマネジメントを行っていなかった利用者は事業者のサービス再開を待つことしかできなかった。

また、SaaS を利用するフェーズや事業の状況により、SaaS に求めるセキュリティのレベルやサービスレベルは異なる。スピードを重視する情報発信、情報収集などの業務に利用するのか、止めてはいけない基幹業務に利用するのかといった用途の違いや、SaaS で取り扱う情報の重要度によって、SaaS を選定する際に比較・検証すべき項目は異なってくるだろう。

SaaS をはじめとしたクラウドサービスの利用は増えていく方向性にある。SaaS の用途が多様化し、次々と新しいサービスが生まれ、新規事業者が市場に参入しつつある。クラウドサービスは相互に連携し、複雑な構造ともなりつつあるため、一つの小規模な SaaS のサービスが停止してしまった場合でも、社会に与える影響は大きくなる恐れがある。

利用者は情報収集した内容を自社のセキュリティポリシーや規定、自社の状況と比較し、リスクの特定、評価、対応を行い、リスクマネジメントのサイクルを回していく必要がある。

6.1.3 クラウドセキュリティ人材の育成

アンケート調査では、情報開示・情報利用の課題として、事業者・利用者の双方で「対応するための工数が足りない」という回答が多かった（4.7.1 参照）。また 6.1.2 で述べたとおり、クラウドセキュリティに関する認識が不足していると思われることから、クラウドセキュリティ技術者の必要性は増している。

これまでの IT 人材に関する需給動向調査[37]でも先端 IT 技術者の不足が指摘されており、クラウドセキュリティを担う IT 技術者の育成は我が国にとって喫緊の課題である。経済産業省では、サイバーセキュリティの体制を構築し、人材を確保するための要点をまとめた「サイバーセキュリティ体制構築・人材確保の手引き」を公開し、経営層を含めてセキュリティに対応するため体制を構築する必要性を訴えている[38]。

また、2022 年 12 月に公開された経済産業省の「DX 推進スキル標準[39]」では、5 つの人材類型の一つとして「サイバーセキュリティ」が示されている。

[37] 経済産業省「IT 人材需給に関する調査」調査報告書（2019 年 3 月）
https://www.meti.go.jp/policy/it_policy/jinzai/houkokusyo.pdf
[38] https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html
[39] https://www.meti.go.jp/press/2022/12/20221221002/20221221002.html

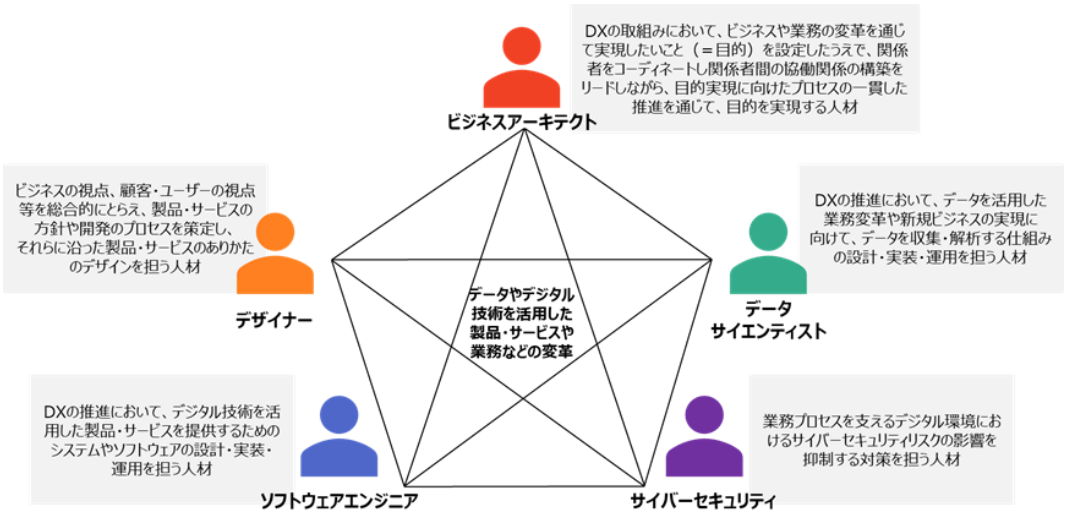


図 6-1-1　経済産業省「DX 推進スキル標準」の人材類型の定義

今回のインタビュー調査でも、有識者より、社外の有識者の活用と共に、社内の IT 技術者をクラウドセキュリティの人材を育てる必要性について提言される中で、セキュリティ人材はいないのではなく、組織内で認識され、評価される仕組みがないのではないかという声があった。一般的に、これまで日本は専門職としての働きではなくゼネラリストとしての働き方を評価される傾向にあり、セキュリティに詳しい人材などの専門性は人事評価制度の中で評価されにくかった。社内には少なからずセキュリティに詳しい人材はいるはずであり、クラウドに限らず、情報セキュリティ全般について詳しい社員を評価するような制度を構築するべきであろうと提言された。

システム開発を行う事業者では、一般的に技術者に「システムエンジニア」等の名称をつけ、スキル評価にあわせて人事を行っている。しかし利用者側の組織において、クラウドサービスのセキュリティに携わる要員を技術者として評価する人事制度は決して多くはないと思われる。それらの要員に技術者として名称を付け、評価することが人事制度として難しいのであれば、人材に付属するスキルとしてセキュリティの知識を評価する制度を構築することも検討するべきであろう。

IPA においても、企業のセキュリティ対策が「セキュリティ人材」のみでは対処できなくなる状況を鑑み、セキュリティが必要である業務を担う人材にも、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけてもらうことを目指し、この状態を「プラス・セキュリティ」と定義している[40]。このように定義することで、セキュリティ人材の活用を進めることにもつながるだろう。

セキュリティ技術者の育成・確保や、社内人材への教育を通じてセキュリティの人材を育成することで、これらの課題の解決につなげることができるはずである。

[40] https://www.ipa.go.jp/jinzai/itss/itssplus.html

6.2 今後への提言

近年急速に発展しているクラウドサービスでは、これまでのオンプレミスを前提とした IT サプライチェーンとは異なる対応が必要とされている。利用者がシステム開発を委託する場合は個別契約が基本であり、場合によっては契約書の見直しを契約後に行ったり、確認・要求を行い、是正を要求したりといったことも可能であった。しかし、SaaS をはじめとしたクラウドサービスでは、事業者が提示する条件の範囲内で契約を結ぶため、基本的には事業者に個別対応や是正要求を求めることは困難である。このような状況から、利用者は契約前の時点から情報開示を求め、SaaS の安全な利用に資するために入手した情報を活かす必要がある。

日本政府が進める「ガバメント・クラウド実行計画[41]」においても「クラウド・バイ・デフォルト」が原則とされるなど、クラウドサービスの利用は今後も一層進展していくことが見込まれる。業種・業態・規模を問わず、クラウドサービスを活用することが求められている。クラウドサービスを適切に利用することが誰にとっても必要となるだろう。

クラウドサービスの利用拡大を受けて、本調査では、「SaaS のセキュリティを保証する情報開示」および「セキュリティの高い状態で SaaS を利用してもらうための情報提供」についてアンケート調査・インタビュー調査を行い、事業者・利用者間の認識の違いによる脅威やリスク・課題を明らかにすることを目指した。調査結果から、事業者・利用者間の情報開示・情報収集に対する認識の違いにより、事業者が開示している情報が利用者に届いていない実態が浮かび上がった。また、事業者・利用者共に指針やガイドラインに基づく情報開示・情報利用が進んでいない状態にあり、情報開示・情報利用の重要性を認識していても、情報開示・情報利用する内容に網羅性が無く、セキュリティリスクを把握する際に抜けや漏れがある状態であるとすれば望ましくない。

これらを解決するためには事業者・利用者それぞれが「何の」情報を開示し、利用していくべきか、認識する必要がある。そのためには、指針・ガイドラインの利用が有効であろう。事業者にとっても指針・ガイドラインは重要であることはもちろんであり、利用者が指針・ガイドラインに基づき情報収集・情報利用を行えば、事業者・利用者間の情報の偏りは改善されるだろう。加えて、利用者が主体性をもって SaaS の情報を収集し、得られた情報を利用した選択・比較・評価や SaaS のリスクマネジメントを行う必要がある。利用者が主体性をもって情報収集を行うことで、事業者も情報利用が容易な情報開示を行う動機となるだろう。

新しい分野に予算や人員を配置することは、企業にとって簡単ではないだろう。しかし、SaaS をなぜ使うのか、組織として目的を認識し、どのように対応し、管理するべきであるのかを認識し、情報利用をコストではなく、SaaS を活かすために必要な投資と考えていくべきである。

今後は、事業者・利用者における情報共有をいかに進めていくべきであるか等、事業者・利用者にとって比較・利用が容易である SaaS の評価方法についても検討を進めていくべきである。それらの課題が解消されることで安全・安心な SaaS の利用がさらに進んでいくことと思われる。

2022 年 11 月には ISMAP　LIU が運用開始されるなど、行政機関においても SaaS の利用が進む傾向にある。行政機関における SaaS の利用推進は、民間にとっても影響が大きいと思われる。今後の SaaS の利用は官民ともに加速するだろう。

[41] https://cio.go.jp/digi-gov-actionplan

事業者・利用者が更に情報開示・情報利用を進めることで、安全・安心に SaaS を運営し、利用することが期待される。

付　録

付録１－１　アンケート調査票（事業者向け調査）

付録１－２　アンケート調査票（利用者向け調査）

付録２－１　アンケート単純集計結果（事業者向け調査）

付録２－２　アンケート単純集計結果（利用者向け調査）