2022年度
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
実態調査概要説明資料

2023年07年24日

独立行政法人　情報処理推進機構
セキュリティセンター

IPA Better Life with IT

目次

©2023 独立行政法人情報処理推進機構（IPA）

1　調査実施概要

©2023 独立行政法人情報処理推進機構（IPA）

背景と目的

<背景>

SaaSの利用拡大

「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」で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る。コスト削減や柔軟なリソース、業務多様化により民間においてもSaaSの利用が拡大。

セキュリティの懸念

クラウドサービスは利便性が高い反面、利用する際の課題も存在する。（例えば、クラウドサービスの利用拡大によって、利用者が直接マネジメントできないITサプライチェーンのリスクや、ITやセキュリティに明るくない利用者による調達・管理のリスクといったセキュリティ上の懸念が生じるなど）

2021年度調査で得られた課題

・セキュリティ情報開示の慣習の確立
・SaaS利用者への安全な利用方法の周知と案内

<目的>

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う。

©2023 独立行政法人情報処理推進機構（IPA）

情報開示・情報利用に関する実態調査

- 事業者・利用者の立場と契約前・契約後を分類し、それぞれの状況における情報開示・情報利用の状況を調査。
- 情報開示・情報収集の項目は、「クラウドサービスの安全・信頼性に係る情報開示指針」総務省に基づき有識者へのインタビューをふまえて設定。

©2023 独立行政法人情報処理推進機構（IPA）

調査概要（全体の流れ）

- 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などの「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」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。

アンケート調査（利用者）	アンケート調査（事業者）	インタビュー調査
・SaaSの利用者に向けた実態調査	・SaaSの事業者に向けた実態調査	・有識者、事業者、利用者へのインタビュー調査

©2023 独立行政法人情報処理推進機構（IPA）

調査概要(事業者向けアンケート調査)

利用者企業・組織を対象としたSaaSのセキュリティに関わる情報開示、情報利用の実態について、事業者と利用者の間の認識の違いによる脅威やリスク、課題などに関する調査をするために、アンケート調査を実施した。対象とした事業者は以下の通りである。

〇調査手法：郵送による書面アンケート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：下表のとおり

項目	内容
対象とする企業・組織	SaaSの提供者である事業者
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）
回収数	147件（うち有効回答144件）

※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。

©2023 独立行政法人情報処理推進機構（IPA）

調査概要(利用者向けアンケート調査)

利用者企業・組織を対象としたSaaSのセキュリティに関わる情報開示、情報利用の実態について、事業者と利用者の間の認識の違いによる脅威やリスク、課題などに関する調査をするために、アンケート調査を実施した。対象とした利用者は以下の通りである。

〇調査手法：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
〇調査期間：2022年12月5日～2022年12月7日
〇調査対象：下表のとおり

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>対象とする個人</td><td>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。</td></tr>
<tr><td>対象とする業種</td><td>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）</td></tr>
<tr><td>回収数</td><td>
<table>
<tr><th></th><th>大規模企業</th><th>中小規模企業</th></tr>
<tr><td>製造業</td><td>61</td><td>55</td></tr>
<tr><td>情報通信業</td><td>56</td><td>56</td></tr>
<tr><td>サービス業</td><td>58</td><td>58</td></tr>
<tr><td>卸売業・小売業</td><td colspan="2">56</td></tr>
<tr><td>金融業・保険業</td><td colspan="2">23</td></tr>
<tr><td>医療・福祉</td><td colspan="2">34</td></tr>
<tr><td>計</td><td colspan="2">457</td></tr>
</table>
</td></tr>
</table>

※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。

©2023 独立行政法人情報処理推進機構（IPA）

調査概要（インタビュー調査）

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の調査や研究に携わる有識者から、「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求等を収集するため、インタビュー調査を実施した。

〇実施形式：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
〇実施時期：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
〇実施対象：下表のとおり

	調査先	実施フェーズ
A	SaaS利用者（情報通信業）	アンケート設計段階
B	SaaS利用者（飲食業）	アンケート設計段階
C	有識者（SaaS関連団体）	アンケート設計段階 アンケート分析段階
D	有識者（SaaS関連団体）	アンケート分析段階
E	有識者（セキュリティコンサルタント）	アンケート分析段階
F	有識者（学識経験者）	アンケート分析段階
G	SaaS事業者	アンケート分析段階

©2023 独立行政法人情報処理推進機構（IPA）

2 調査結果

©2023 独立行政法人情報処理推進機構（IPA）

調査仮説

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、調査を設計した。
調査にあたって事業者・利用者それぞれの立場で実態を調査すると共に、事業者、利用者間の実態や意識の乖離があることを想定し、以下の仮説を設定した。

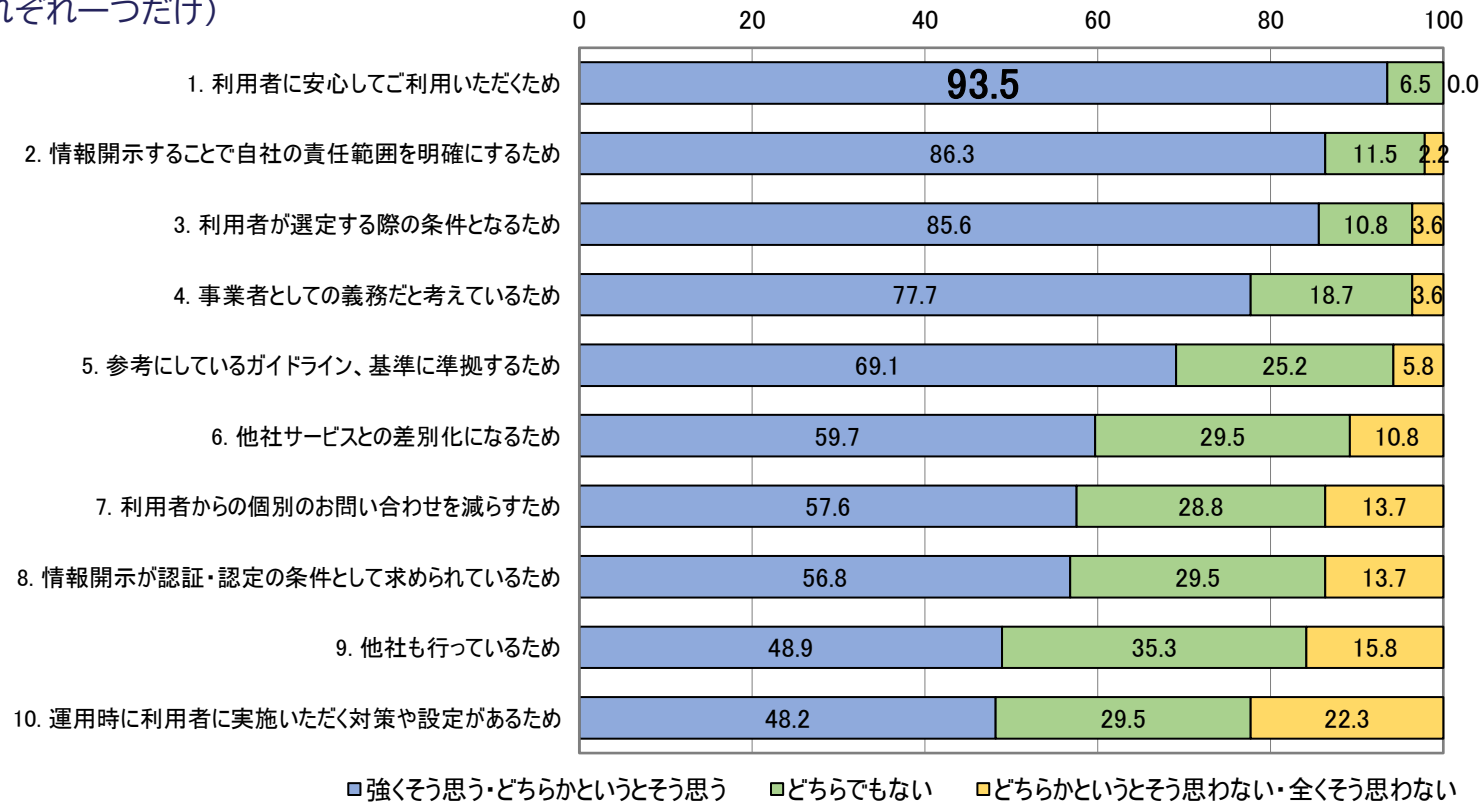
	調査仮説	検証結果
1	契約前（選定時）における情報開示・情報利用	事業者：開示する準備はしている 利用者：収集しきれていない。収集しても利用しきれていない。
	1-1 事業者は利用者がSaaSを選定するために必要なセキュリティに関する情報を開示していない。	
	1-2 利用者はSaaSを選定するために必要なセキュリティに関する情報を収集していない。	
2	契約後（運用時）における情報開示・情報利用	
	2-1 事業者は利用者がSaaSを利用するために必要なセキュリティに関する情報を提供していない。	
	2-2 利用者はSaaSを利用するために必要なセキュリティに関する情報を収集していない。	
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。	
4	利用者が参照しているセキュリティの基準・標準	基準や標準はあまり用いられていない
	4-1 利用者はSaaSを選定する際に参照すべきセキュリティの標準が何かわからない。	
5	SaaSの認証制度・認定制度の取得・利用状況	事業者：取得していない 利用者：一定数基準としている
	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。	

©2023 独立行政法人情報処理推進機構（IPA）

事業者の開示目的は
利用者に安心してご利用いただくため

- 事業者の90%以上が「利用者に安心して利用していただくため」と回答
- 次いで責任範囲を明確にすることが目的と回答

Q12. Q10で行っている情報開示・情報提供の目的について、以下の項目のあてはまりの度合いをご回答ください。
（それぞれ一つだけ）



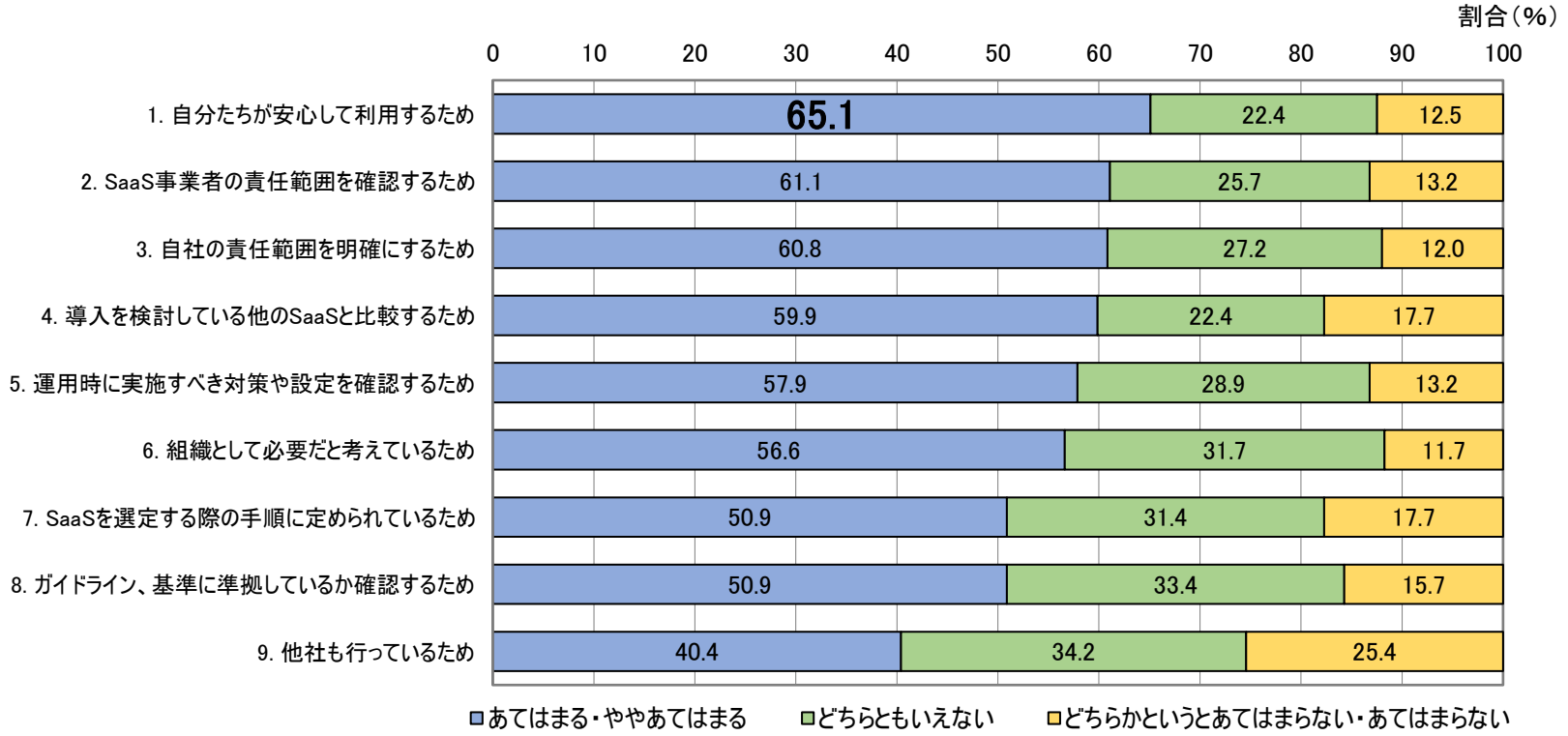
SaaSのセキュリティ情報を開示している目的（事業者：Q12）

©2023 独立行政法人情報処理推進機構（IPA）

利用者の収集目的は 自分たちが安心して利用するため

- 利用者の65%が「安心して利用するため」と回答
- 次いで責任範囲を明確にすることが目的と回答

Q8. Q7で行っている情報収集の目的について、以下の項目のあてはまりの度合いをご回答ください。(それぞれ一つだけ)

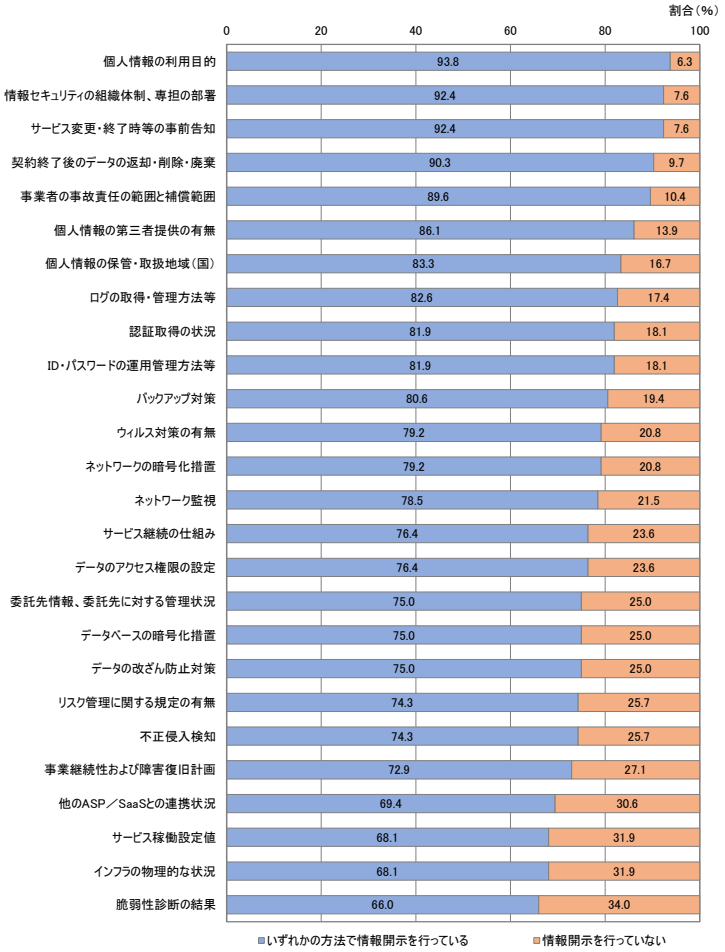


契約前(選定時)にSaaSのセキュリティ情報を収集している目的(利用者:Q8)

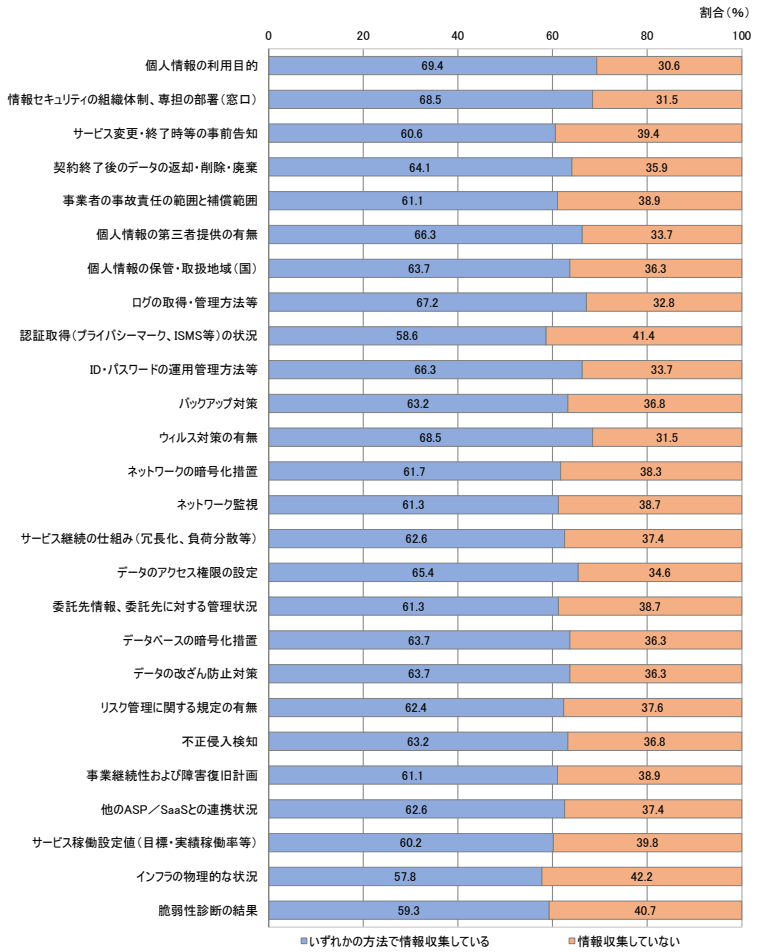
©2023 独立行政法人情報処理推進機構 (IPA)

情報開示（事業者）と情報収集（利用者）の状況

- 事業者：いずれかの方法で「情報開示を行っている」企業が70%以上
- 利用者：情報により差が見られるもの、6～7割の情報を収集している



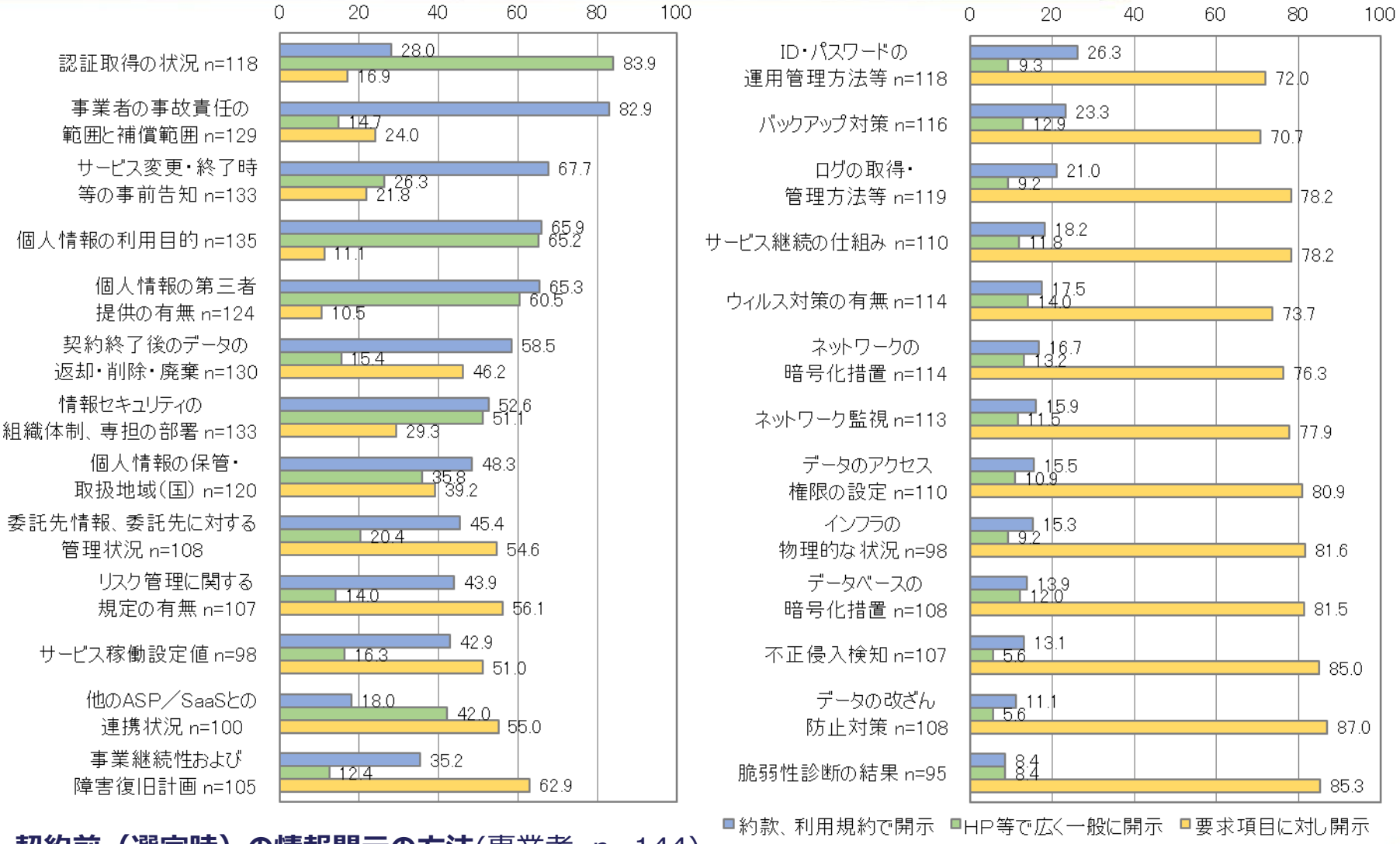
契約前（選定時）の情報開示の状況（事業者　n＝144）



契約前（選定時）の情報収集・利用の状況（利用者　n=457）

©2023 独立行政法人情報処理推進機構（IPA）

事業者は契約前（選定時）の情報開示の方法を情報ごとに決めている

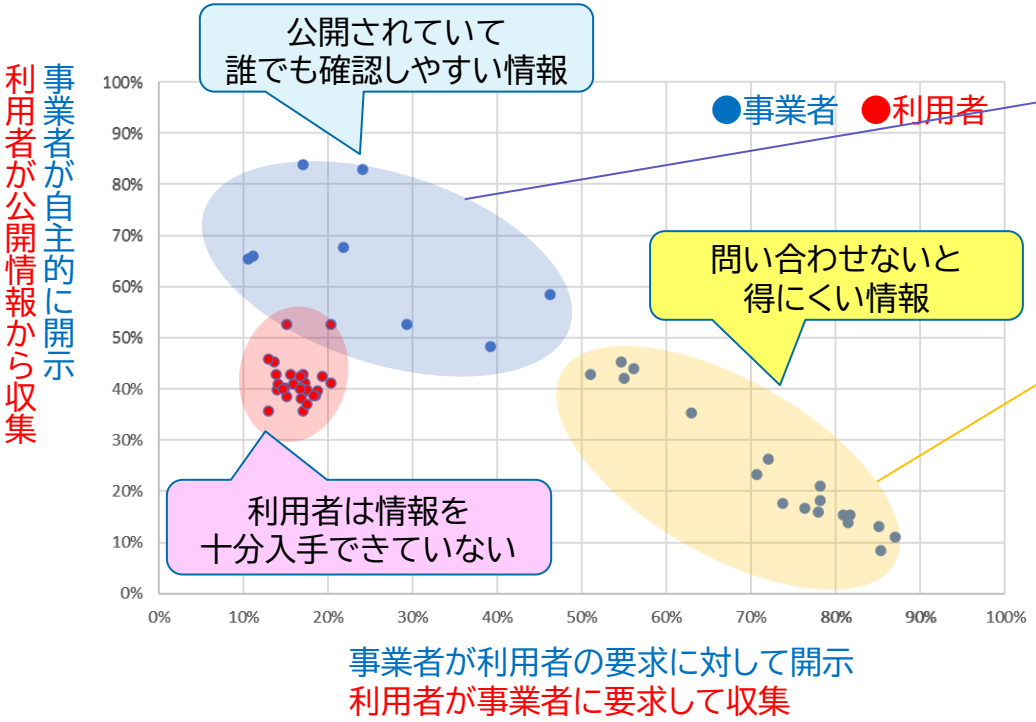


契約前（選定時）の情報開示の方法(事業者　n=144)

©2023 独立行政法人情報処理推進機構（IPA）

公開情報に頼りがちな利用者には情報が届いていない恐れあり

- 技術的対策は事業者に要求（問い合わせ）しないと得られない情報が多い。
- 利用者は公開情報に頼りがちであり、対策の検討のための情報が不足している。



契約前（選定時）に開示している情報と開示する方法（事業者：Q10）
契約前（選定時）に収集している情報と収集する方法（利用者：Q7）

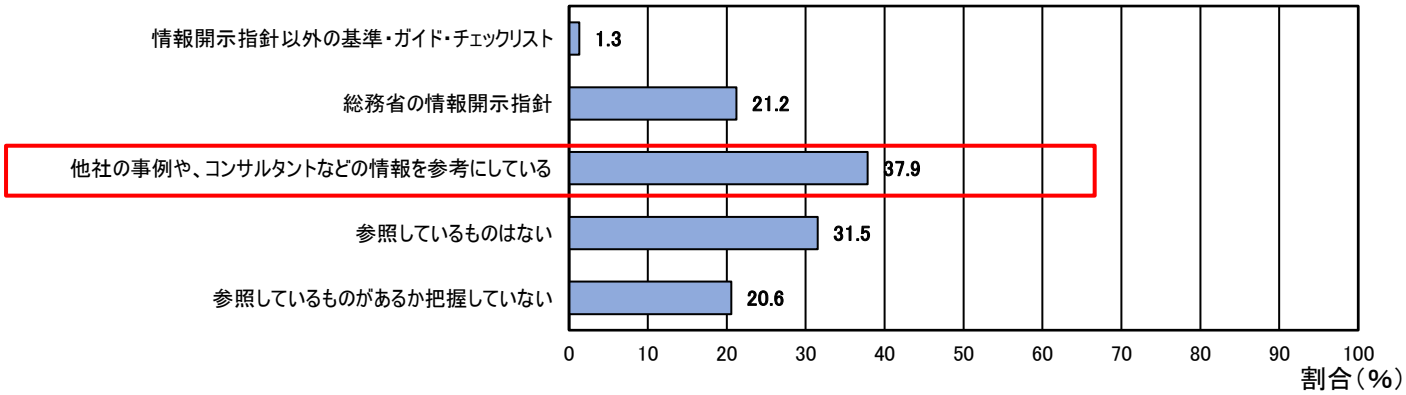
認証取得（プライバシーマーク、ISMS等）の状況
事業者の事故責任の範囲と補償範囲
サービス変更・終了時等の事前告知
個人情報の利用目的
個人情報の第三者提供の有無
契約終了後のデータの返却・削除・廃棄
情報セキュリティの組織体制、専担の部署（窓口）
個人情報の保管・取扱地域（国）

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
サービス稼働設定値（目標・実績稼働率等）
他のASP／SaaSとの連携状況
事業継続性および障害復旧計画（BCDR）
ID・パスワードの運用管理方法等
バックアップ対策（バックアップ実施インターバル等）
ログの取得・管理方法等
サービス継続の仕組み（冗長化、負荷分散等）
ウィルス対策の有無
ネットワークの暗号化措置
ネットワーク監視
データのアクセス権限の設定
インフラの物理的な状況（建物形態、耐震・免震構造）
データベースの暗号化措置
不正侵入検知
データの改ざん防止対策
脆弱性診断（脆弱性診断の有無、診断の対象等）の結果

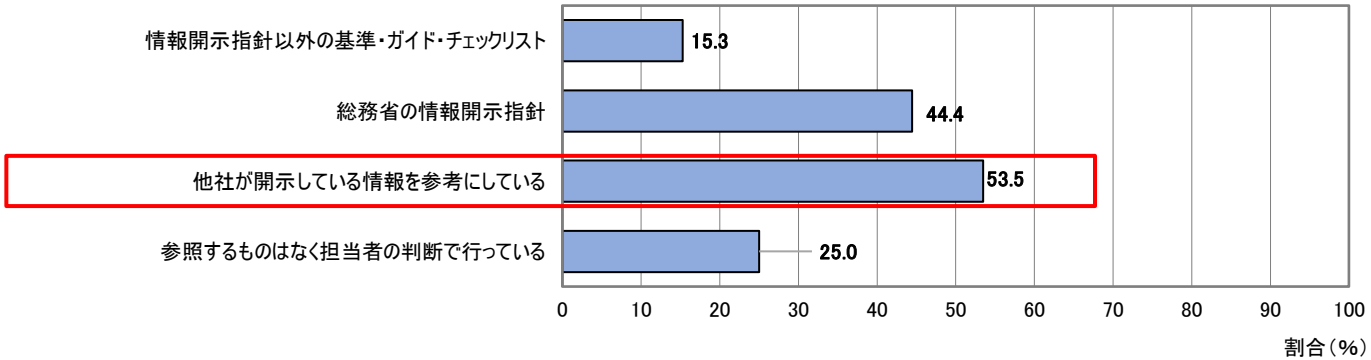
©2023 独立行政法人情報処理推進機構（IPA）

利用者は開示指針・ガイドライン等の利用が2割程度、網羅性に課題

- 事業者・利用者ともに他社の事例を参考にしている割合が高い
- 「情報開示指針」「情報開示指針以外の基準・ガイド・チェックリスト」の利用割合は高くない



利用者が契約前(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:Q10)



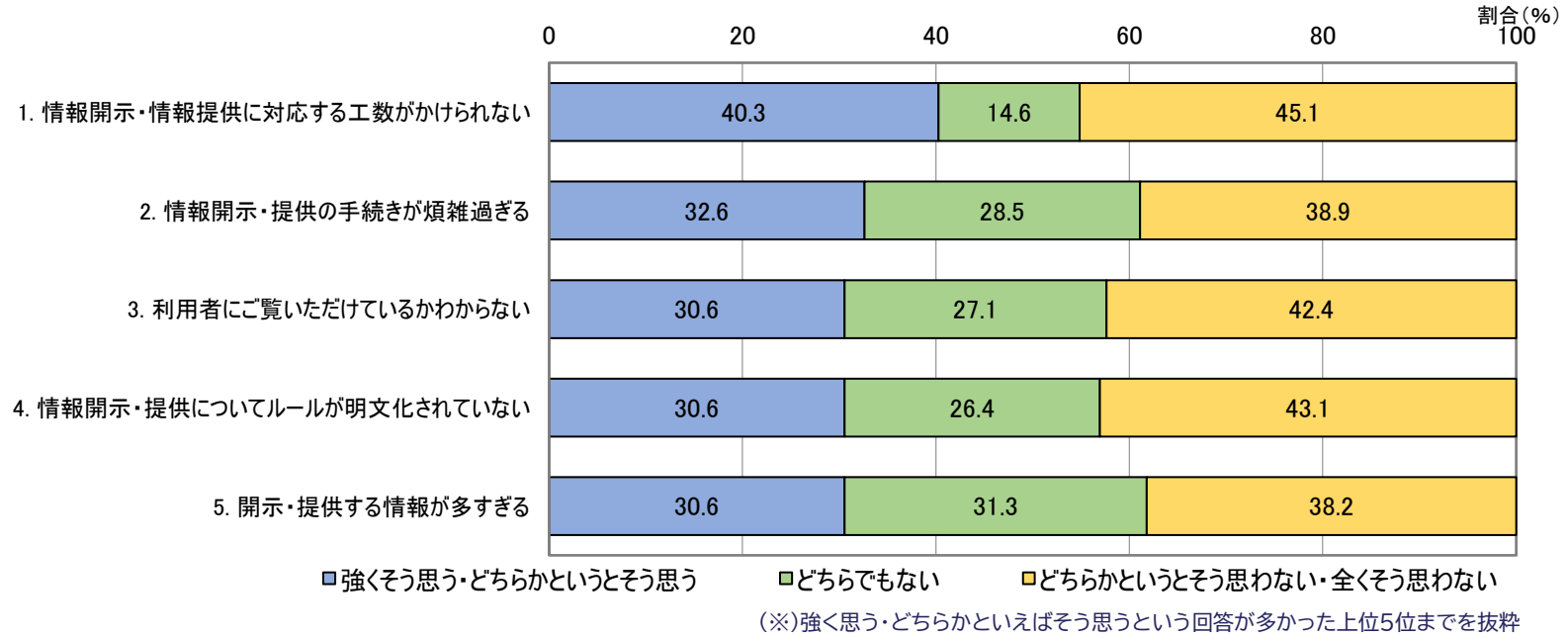
事業者が開示するセキュリティの情報を決定するために参照しているガイドライン等(事業者:Q18)

©2023 独立行政法人情報処理推進機構（IPA）

事業者は情報開示作業の効率化、手続きの見直しが課題

- 「工数がかけられない」「手続きが煩雑すぎる」など、事業者側の工数や作業にかかわることが課題

Q20. SaaSの情報開示・提供における貴社の課題は何でしょうか。以下の選択肢の中からあてはまりの度合いをご回答ください。(それぞれ一つだけ)



(※)強く思う・どちらかといえばそう思うという回答が多かった上位5位までを抜粋

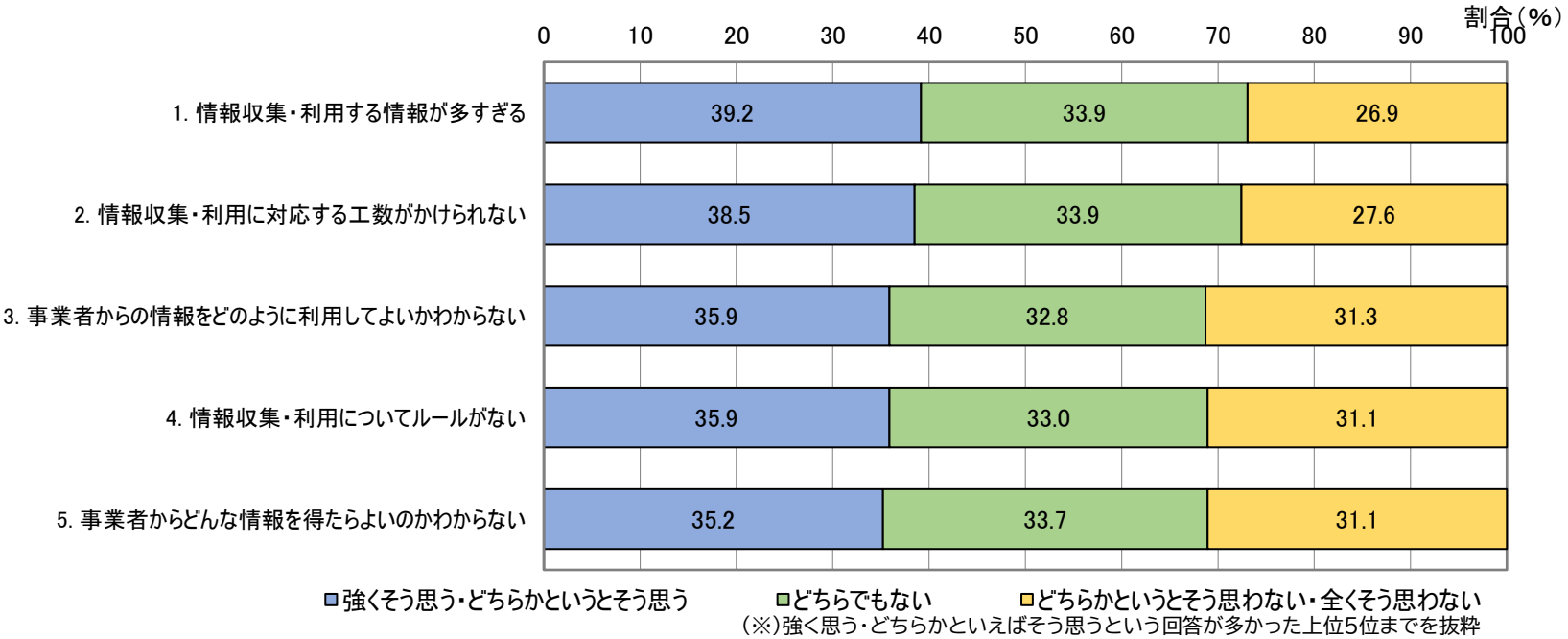
事業者の課題(事業者:Q20)

©2023 独立行政法人情報処理推進機構（IPA）

利用者への必要性の啓発とともに、限られた工数で安全性をどうやって担保するかが課題

- 「利用する情報が多すぎる」「情報収集・利用に工数がかけられない」など、対象の絞り込みや作業効率化に課題
- 「強くそう思う」が最も多かったのは「情報収集・利用の必要性が分からない」だった

Q19 SaaSの情報収集・利用における貴社の課題は何でしょうか。以下の選択肢の中からあてはまりの度合いをご回答ください。(それぞれ一つだけ)



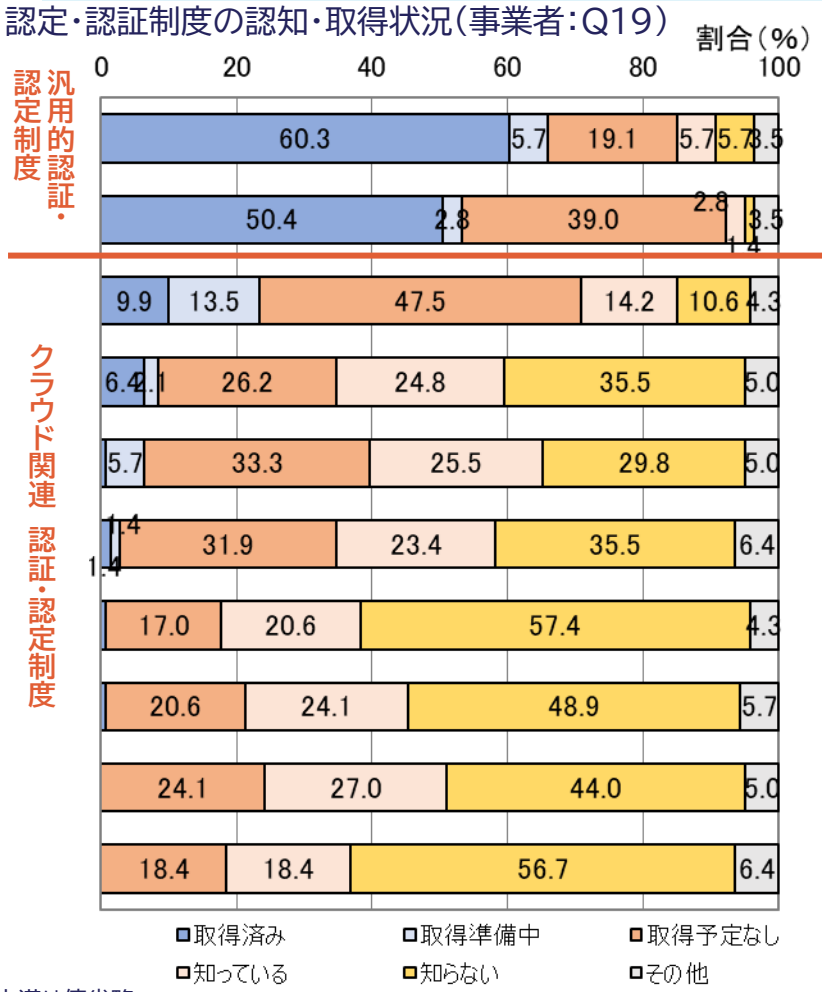
(※)強く思う・どちらかといえばそう思うという回答が多かった上位5位までを抜粋

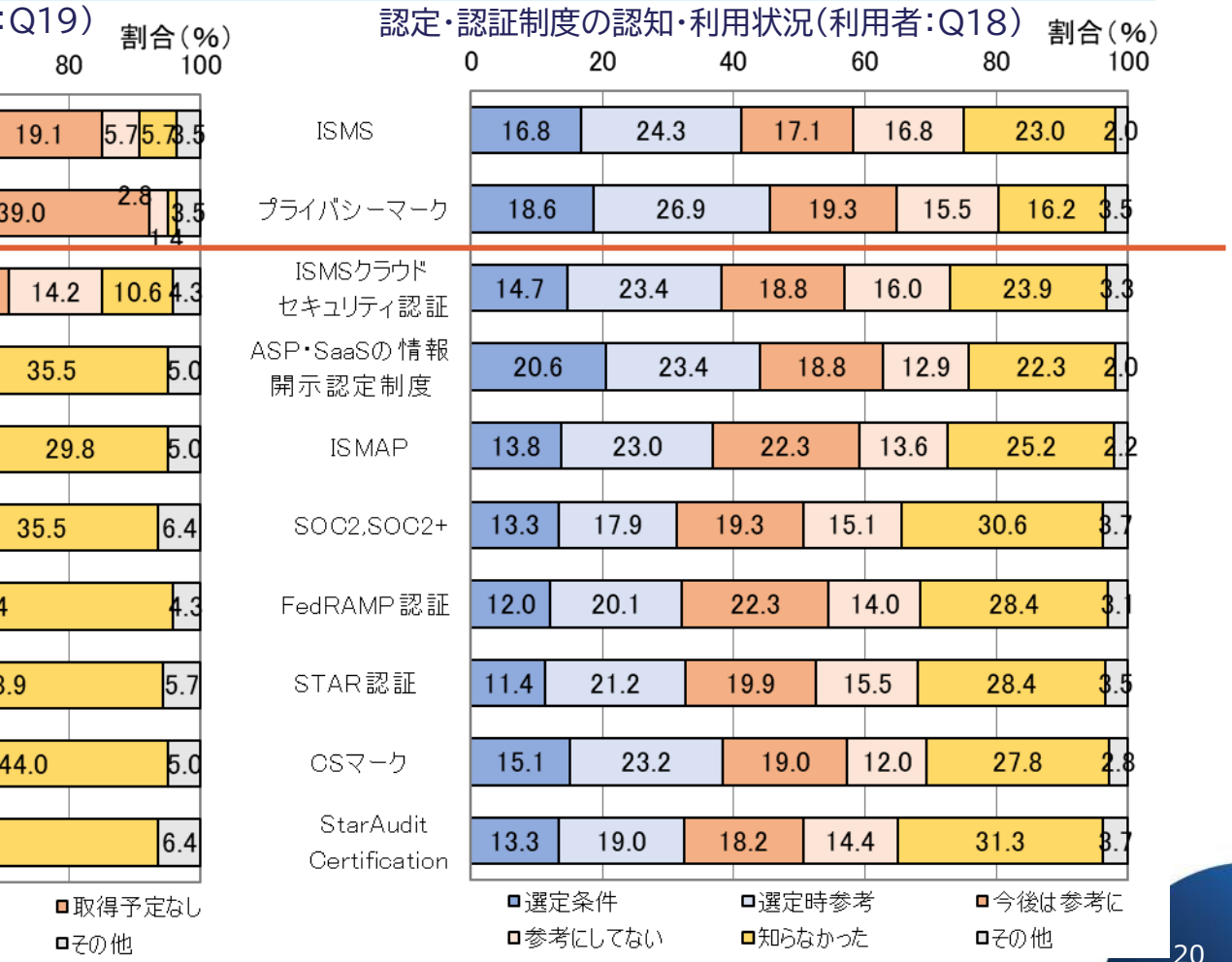
利用者の課題(利用者:Q19)

©2023 独立行政法人情報処理推進機構（IPA）

利用者はSaaSに関する認定・認証取得を選定条件・参考にしたい

- 約３～４割の利用者がなんらかの認証・認定制度の取得を選定の条件や参考にすると回答
- 事業者側のクラウド関連の認証・認定制度の取得状況は1割以下





1%未満は値省略

©2023 独立行政法人情報処理推進機構（IPA）

アンケート調査結果（まとめ）

- 事業者と利用者では情報の開示と収集に認識の違いがみられたが、目的は一致している
- 指針・ガイドラインの利用状況は進んでいるとは言えない
- 認証・認定の取得と利用状況の考え方に違いがある

情報開示・情報利用の調査結果	
情報開示と 情報収集の状況	事業者と利用者の認識に違いがある（双方が相手任せの状態） 事業者：**一定の情報は開示（公開）している** 開示していない情報においても**要求があれば開示する準備をしている** 利用者：**主に公開された情報を収集**しているケースが多い 公開されていない情報を事業者に**要求するケースは少ない**
情報開示と 情報収集の目的	事業者（情報開示）と利用者（情報収集）の目的は一致している 事業者：利用者に**安心して利用**してもらうため、責任範囲を明確にするため 利用者：**安心して利用**するため、責任範囲を明確にするため
指針・ガイドラインの 利用状況	「情報開示指針」や「ガイドライン」等の利用が進んでいるとは言えない状況にある 事業者と利用者は共に「**他社の状況**」を**参考**にしている傾向がみられ、 **情報開示指針やガイドライン**などの利用は**多くない**
認証・認定の取得と 利用状況	事業者の取得状況(*1）と利用者の利用状況（*2）の考え方に違いがある 事業者：ISMSやPマークは積極的、**クラウド独自の認証・認定制度は様子見** 利用者：一定数が**クラウドにかかわる認証・認定もSaaSの選定条件**にしている

（＊1）認証・認定の取得 （＊2）認証・認定取得をSaaSの選定条件とすること

©2023 独立行政法人情報処理推進機構（IPA）

事業者と利用者の間の認識の違いによるリスクと課題

【リスク】

事業者は「利用者から要求が無ければ情報を開示せず」、利用者は「公開されている情報に頼りがち」であり、開示すべき情報が開示されていないもしくは収集するべき情報を収集できていない。また、情報開示指針やガイドラインが公開されてはいるものの、利用は進んでおらず利用者と事業者の間で必要な情報が共有できていないつまり、**利用者は十分な情報を基にサービスを選定していない、安全な利用に必要な情報が利用者に届いていない恐れ**がある。

事業者：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、
セキュリティインシデントにつながる可能性がある。

利用者：自社の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
適切な利用方法を知らずに利用を続けてしまう

【課題】

- SaaSを安全に選定・運用するにあたり、事業者が開示すべき情報と利用者が収集すべき情報の認識の違い合わせる必要がある
- 安全な利用の為の行動を利用者が取るためのスキル、知識が足りない。

©2023 独立行政法人情報処理推進機構（IPA）

安全・安心なSaaSの利用のために行うべきこと

指針・ガイドラインを用いた情報開示・情報収集の網羅性の確保

利用者：**指針やガイドラインを参考**として、自社のSaaSの選定や運用に必要な情報を取り決め、事業者から公開されていない情報については問い合わせて収集することが望ましい

事業者：指針やガイドラインを参考として、**利用者が収集しやすい情報開示方法**（あらかじめ公開or要求されたら回答）を行う配慮が求められる

認証・認定制度を活用した安全な提供・導入・運用

利用者：認証・認定制度を選定条件にすることで、一定レベルのセキュリティが担保されたSaaSの導入が可能となる（**セキュリティ人材を確保できない組織でも、認証・認定制度を条件とすることで、一定レベルのセキュリティを担保したSaaSの導入が可能**）

事業者：**認定・認証の取得、活用**により、提供するSaaSの信頼性および安全性を示す事ができる

©2023 独立行政法人情報処理推進機構（IPA）

©2023 独立行政法人情報処理推進機構（IPA）