

企業の情報セキュリティリスク対策に遅れ

シャドーITの検知・対応ができていない企業は19.4%

対応予定も4割どまり

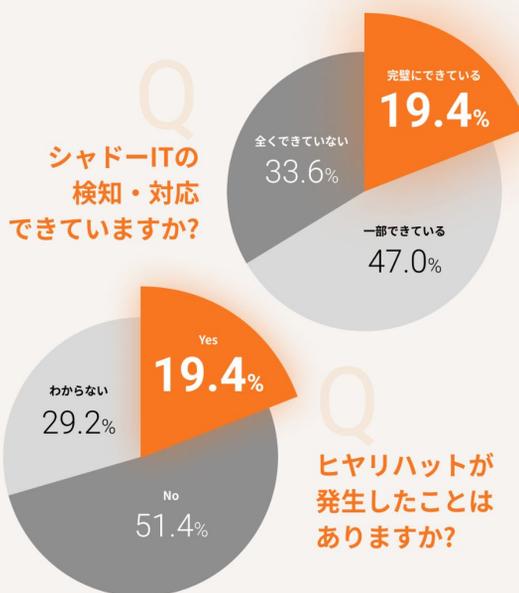
約2割の企業で退職者アカウント消し忘れによる情報漏洩やヒヤリハットが発生

ITデバイスやSaaS管理などのコーポレートIT業務を自動化を可能とするプラットフォームを運営するラクスルグループのジョーシス株式会社(本社:東京都品川区、代表取締役社長CEO:松本恭攝、以下「ジョーシス」)は、ポストコロナにおけるセキュリティリスクの高まりをうけ、情報システム部門で働く全国1000名を対象にIT管理の実態について調査を実施しました。

 **ジョーシス**

IT管理の実態調査レポート

- ・ シャドーITの検知・対応ができていない企業はわずか19.4%
- ・ 今後対応予定も4割どまり
- ・ 約2割の企業で退職者のアカウント消し忘れによる情報漏洩事故やヒヤリハットが発生



調査結果サマリー

 **ジョーシス**

- 01 コロナを起因にクラウドサービスを利用する企業は4年間で10%増加し (*1) 76%となった。また、約半数がクラウドサービスの利用が増加と回答
- 02 クラウドサービス (SaaS)を全て把握できている企業はわずか23.8%
- 03 シャドーIT(従業員や各業務部門の判断で導入・使用され、システム管理部門による把握や管理が及んでいないもの)の検知対応ができていない企業はわずか19.6%。8割以上の企業が対策できていない
- 04 今後シャドーITの検知・対応を予定している企業はわずか4割
- 05 7割以上の企業が退職者のクラウドサービスのアカウントの削除に抜け漏れがあるかもしれないと回答。また、19.4%が退職者のアカウント消し忘れによる情報漏洩リスクやヒヤリハットを経験

コロナをきっかけにテレワークが浸透し、働く場所の多様化や、SaaSツールの急速な拡大でクラウドサービスの利用が一般的になりました。その一方で、導入のしやすさゆえに従業員や各業務部門の判断でSaaSが導入・使用され、「シャドーIT」(システム管理部門による把握や管理が及んでいないもの)が生まれ、セキュリティ対策漏れによる情報漏洩など企業がリスクにさらされる機会が急増しています。

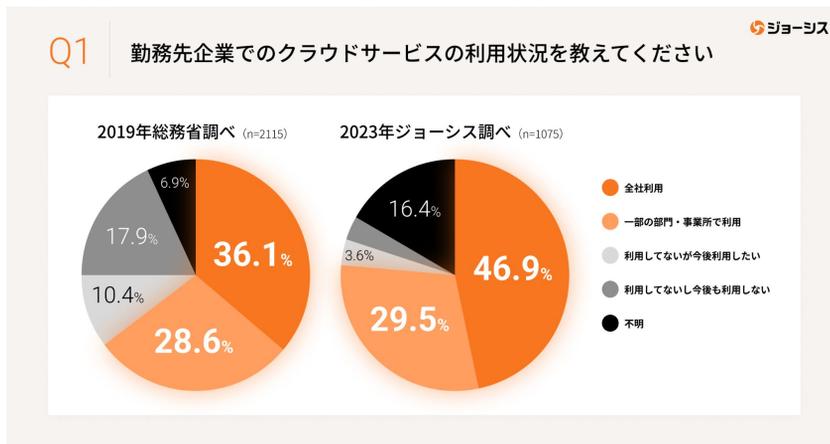
今回ジョーシスによる「IT管理の実態について」の調査結果から、急速にクラウドサービスの利用が進む中で各社の管理対策が不完全であり、情報セキュリティガバナンスに大きな課題があることが明らかになりました。特に「シャドーIT」の問題は情報セキュリティガバナンス確立の障壁であり、大きなリスク要因ですが、対策を講じている企業は非常にわずかで、8割以上の企業が対策できていないと回答しています。「シャドーIT」の解決には、CASB(*2)などを利用し、IT管理部門における運用負荷の軽減を実現しながら、セキュリティ課題に向き合う姿勢が求められています。

情報漏洩のリスク要因としては、中途退職者による漏洩(*3)が主な原因です。「退職者のアカウントを完璧に削除できている」という回答はわずか25%に過ぎず、7割以上の企業が不安を感じていることがわかりました。多くの企業がアカウント削除漏れにより、退職者による情報漏洩事故が発生してしまうリスクを孕んでいることとなります。また、実際に約2割の企業が「情報漏洩リスク、ヒヤリハットの経験がある」という回答結果からも企業のセキュリティ対策が急務であるといえます。

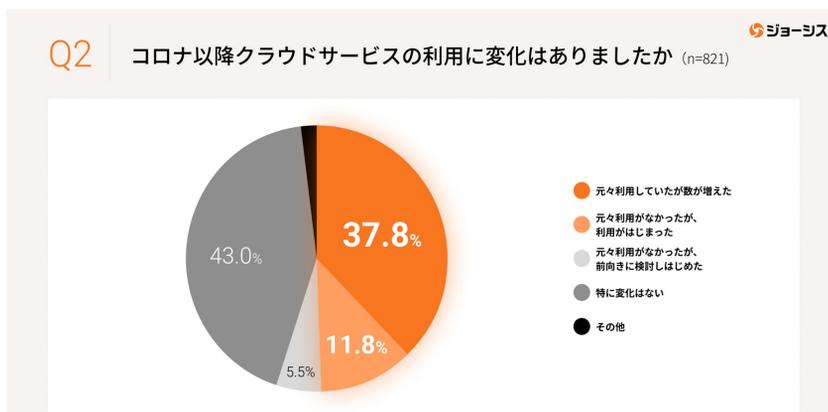
今後もクラウドサービスの利用が増加する中、まずは「誰が」「何」を使っているのか、従業員ごとの利用状況の可視化が急務であり、把握と管理の徹底を行うことが何より重要です。

■調査結果詳細について

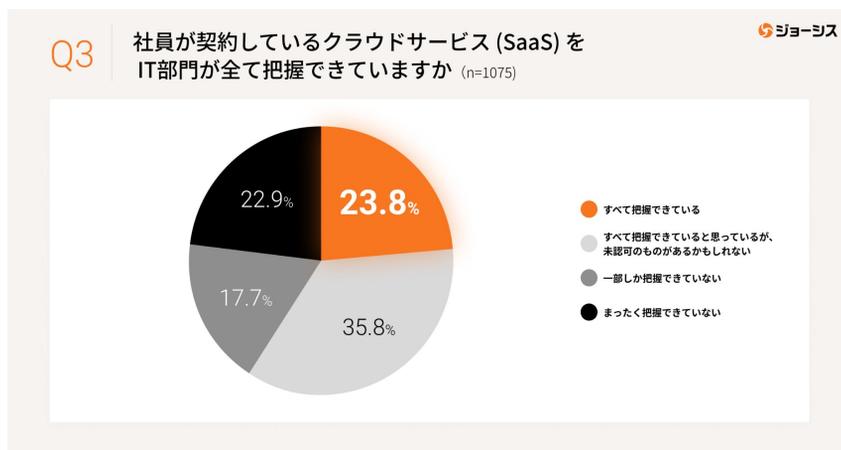
Q1.「勤務先企業でのクラウドサービスの利用状況を教えてください」という質問に対し、全社利用が46.9%、一部の部門・事業所で利用が29.5%とクラウドサービスを利用する企業は76.4%という回答となりました。2019年度の総務省実施の調査に比べ10%以上も増加しています。



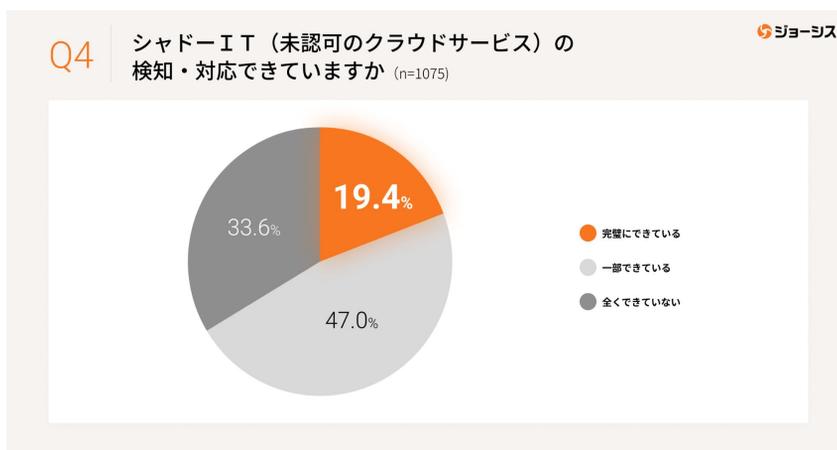
Q2.「コロナ以降クラウドサービス利用に変化はありましたか」という質問に対し、約半数の49.6%が利用が増えた、利用が始まったという回答になりました。



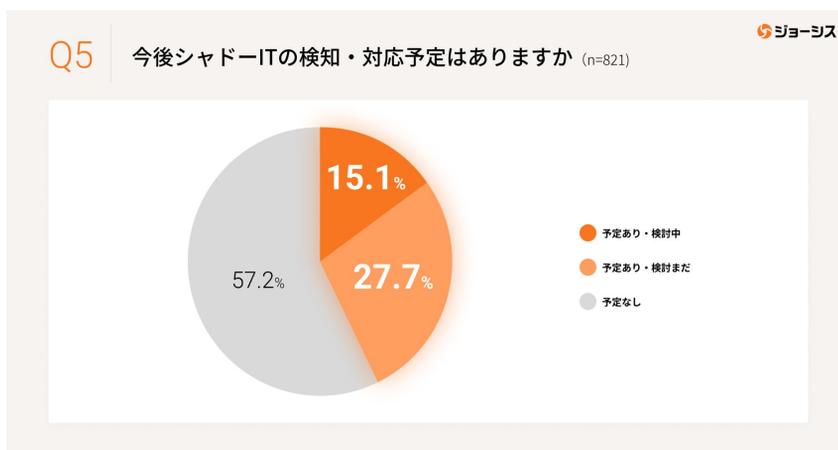
Q3.「社員が契約しているクラウドサービス (SaaS) を IT部門が全て把握できていますか」という質問に対し、すべて把握できていると回答した企業はわずか23.8%でした。8割近くが契約管理が不完全な状態ということになります。



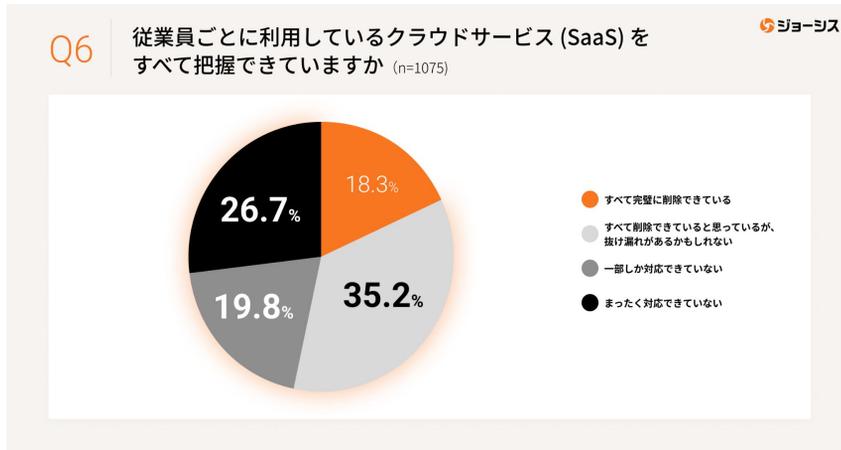
Q4.「シャドーIT (未認可のクラウドサービス) の検知・対応ができていますか」という質問に対し、検知対応が完璧にできていると回答したのは19.4%と2割以下でした。シャドーITのリスクに気づいていながらも対策が打っていません。



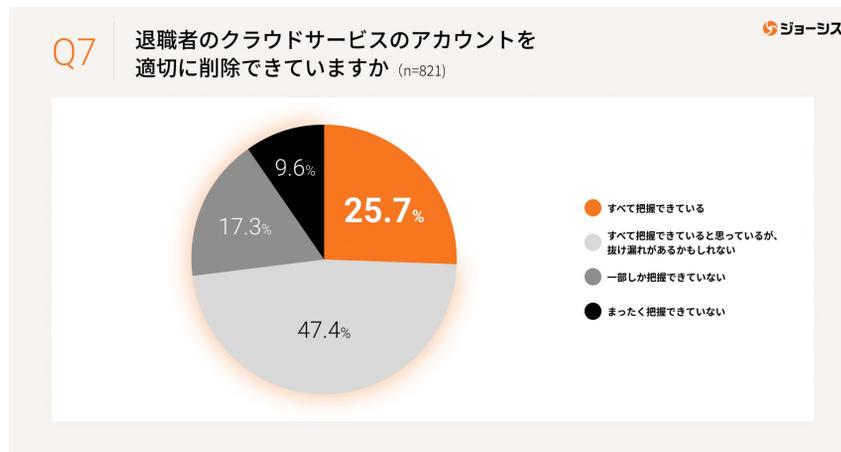
Q5.現在未対応の企業に向け、「今後シャドーITの検知・対応予定はありますか」という質問に対して「対応を予定している」と回答した企業はたった4割という結果になりました。



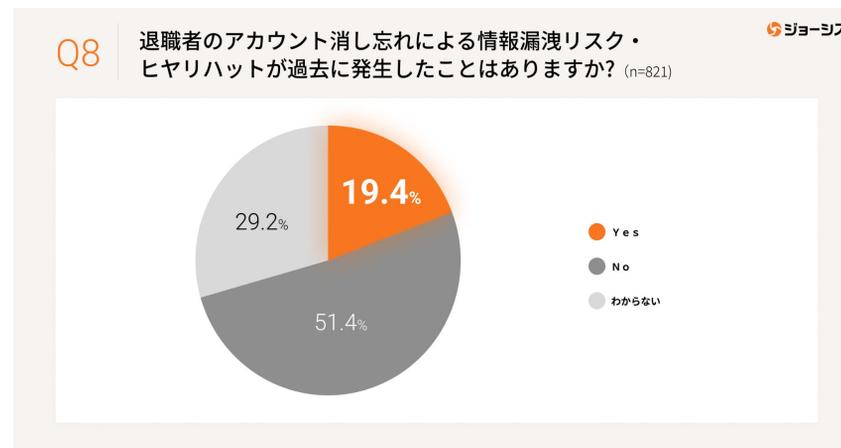
Q6.「従業員ごとに利用しているクラウドサービス (SaaS) をすべて把握できていますか」という質問に対し、「すべて把握できている」と回答した企業はわずか18.7%と2割も満たしていませんでした。



Q7.「退職者のクラウドサービスのアカウントを適切に削除できていますか」という質問に対し、「全て完璧に削除できている」と回答した企業はわずか25.7%でした。



Q8.「退職者のアカウント消し忘れによる情報漏洩リスク・ヒヤリハットが過去に発生したことはありますか」という質問に対し、19.4%がはいと回答しています。既に約2割の企業で情報漏洩事故やヒヤリハットが発生しています。



■調査概要

調査機関 : 2022年12月27日～2023年1月4日
対象者 : 情報システム部門に勤務する1000名
調査エリア : 全国
調査方法 : 第三者機関インターネット調査(ジョーシス調べ)

<利用条件>

情報の出典元として「ジョーシス株式会社」の名前を明記してください。

*1 参照: 2019年総務省調べ

*2 CASBとは、企業などが利用するサイバーセキュリティ製品の一つで、社内から外部のクラウドサービス利用を監視し、指定されたセキュリティ基準に基づいて制御する機能を提供するもの

*3 参照: 独立行政法人情報処理推進機構による「企業における営業秘密管理に関する実態調査」

■ITデバイス&SaaSの統合管理クラウド「ジョーシス」について

ITデバイス & SaaS の統合管理クラウド「ジョーシス」では、従業員に紐づけたITデバイス・SaaSの台帳管理や、入退社に伴うSaaSアカウント発行・削除、退職者の削除漏れアカウントの検知、PC購入やキitting・ヘルプデスクのアウトソースなど、あらゆるコーポレートIT業務を自動化する機能を提供し、コーポレートITの業務負荷を軽減し、セキュリティ体制を強化します。

- ・社名: ジョーシス株式会社
- ・代表取締役社長: 松本 恭攝
- ・設立: 2022年2月1日
- ・資本金: 1億円※2022年2月1日時点
- ・本社: 東京都品川区上大崎2-24-9 アイケイビル1F
- ・企業URL: <https://corp.iosys.com/>
- ・利用に関するお問い合わせ: <https://iosys.com/contact>

【ラクスルグループについて】

「仕組みを変えれば、世界はもっと良くなる」という企業ビジョンのもと、印刷、広告や物流といったデジタル化が進んでいない伝統的な産業にインターネットを持ち込み、産業構造を変えることで、より良い世界にすることを目指します。現在ではネット印刷・集客支援のプラットフォーム「ラクスル」、マーケティングプラットフォームを提供するノバセル株式会社、物流プラットフォームのサービスを提供するハコベル株式会社、コーポレートITのサービスを提供するジョーシス株式会社を運営しております。(URL: <https://corp.raksul.com/>)

【ラクスルが取り組む“産業DX”】

私たちは、シェアリングプラットフォームによる取引の効率化、ソフトウェア(SaaS)による業務の効率化、それらに基づく付加価値サービスの3つを統合したプラットフォームの構築により、パーティカルに各産業の課題を解決し生産性・収益性の高い業界に変革していきます。ラクスル株式会社は産業変革者として、デジタル化が進んでいない伝統的な産業に対して、統合パーティカルプラットフォームを通じてDXを推進し、世界をより良いものにしていきます。

【本件に関するお問い合わせ】

ジョーシス広報担当 福本・星

TEL: 03-6629-4892(広報) FAX: 050-3606-0419 Mail: pr@raksul.com