HITACHI
Inspire the Next

SaaSを利用する会社のセキュリティ意識に関する実態調査

～SSPMを導入済み・導入予定・関心がある企業はトータルで約8割～

株式会社 日立ソリューションズ

Contents

1. 調査背景と概要

1.調査背景と概要

HITACHI
Inspire the Next

●調査目的
SaaSを利用する会社のセキュリティ意識に関する実態調査

●調査期間
2023年　6月29日～30日　　（2日間）

●調査方法
クローズドアンケート調査（インターネット）

●調査対象者
従業員が500人以上在籍している企業にお勤めの、情報セキュリティに関する部門に所属している会社員・団体職員（正社員）100人

●設問数
10問

2. 調査した内容

2.調査した内容

HITACHI
Inspire the Next

Q1　現在利用しているSaaSを教えてください。

Q2　あなたの会社では、SaaSサービスのセキュリティ対策としてどのようなことを行っていますか？

Q3　SaaSを利用していて、次のうち最も心配なことは何ですか？

Q4　あなたの会社では、ゲストユーザーなど、不適切アカウントがないか
　　定期的な点検・棚卸を行っていますか？

Q5　SaaSの設定ミスから情報漏洩につながった事件・事例があることを知っていますか？

Q6　SaaS利用が原因のインシデントが発生したことはありますか？
　　ある場合、どのようなインシデントでしたか？

Q7　あなたは、SSPMを知っていますか?

Q8　あなたの会社では、SSPMを導入していますか？

Q9　SSPMを導入する際の選定ポイントを教えてください。

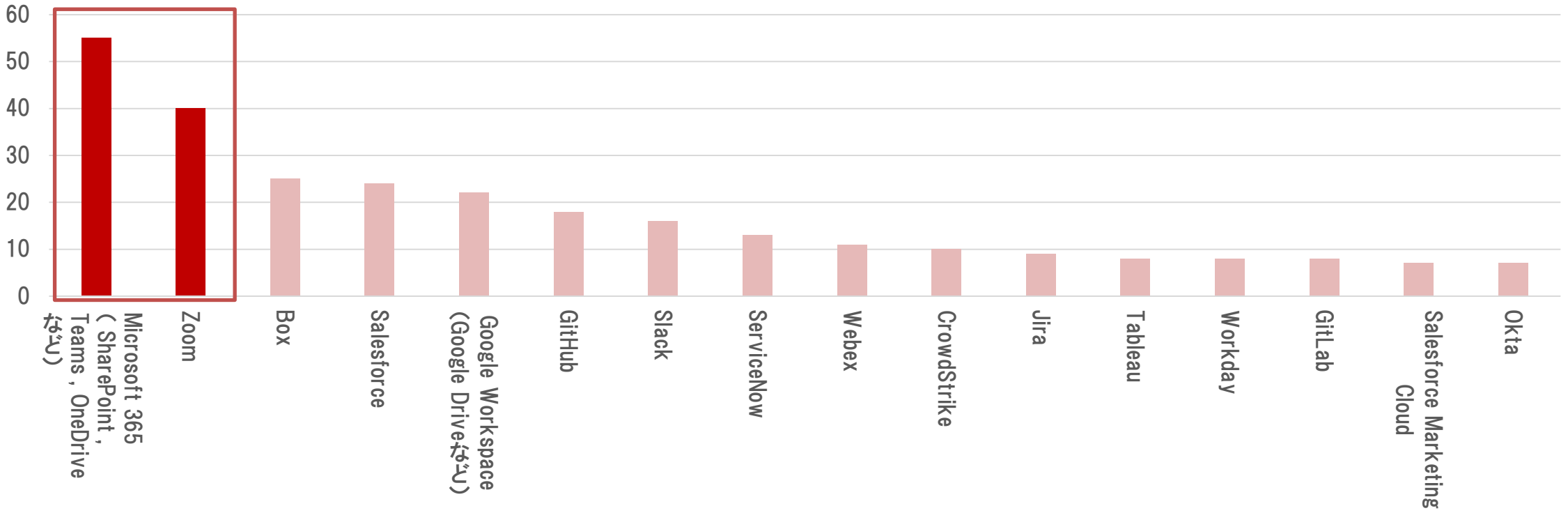
Q10　導入を考えていない方にお聞きします。その理由は何ですか？

※SSPMとは、SaaS Security Posture Managementの略で、SaaSのセキュリティリスクを継続的に監視・チェック・管理する技術を指します。

3. 調査結果レポート

3-1　現在利用しているSaaS

Q1　現在利用しているSaaSを教えてください。（お答えはいくつでも）



※わからない7　除く

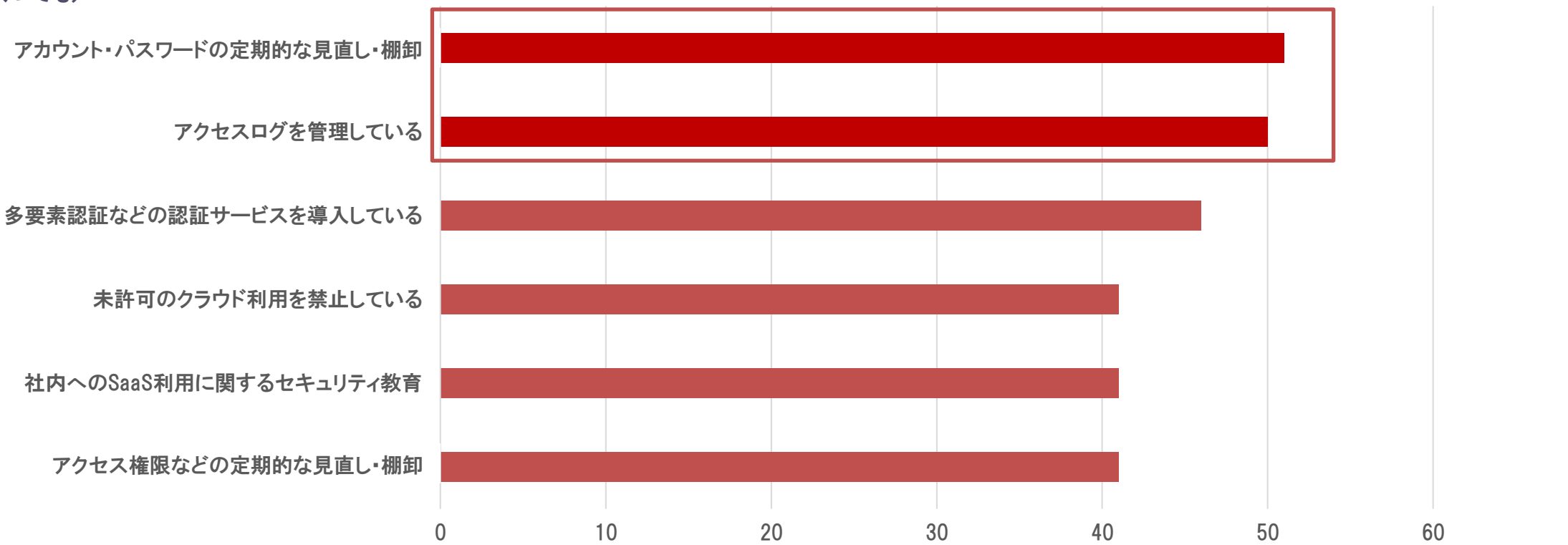
現在利用しているSaaSは Microsoft 365 が最も多く、次にZoomが続きます。
利用していると回答した人数が10人以上のものは10種類あり、さまざまなSaaSが使用されていることがわかりました。

3-2 SaaSのセキュリティ対策

HITACHI
Inspire the Next

Q2 あなたの会社では、SaaSサービスのセキュリティ対策としてどのようなことを行っていますか？

（お答えはいくつでも）



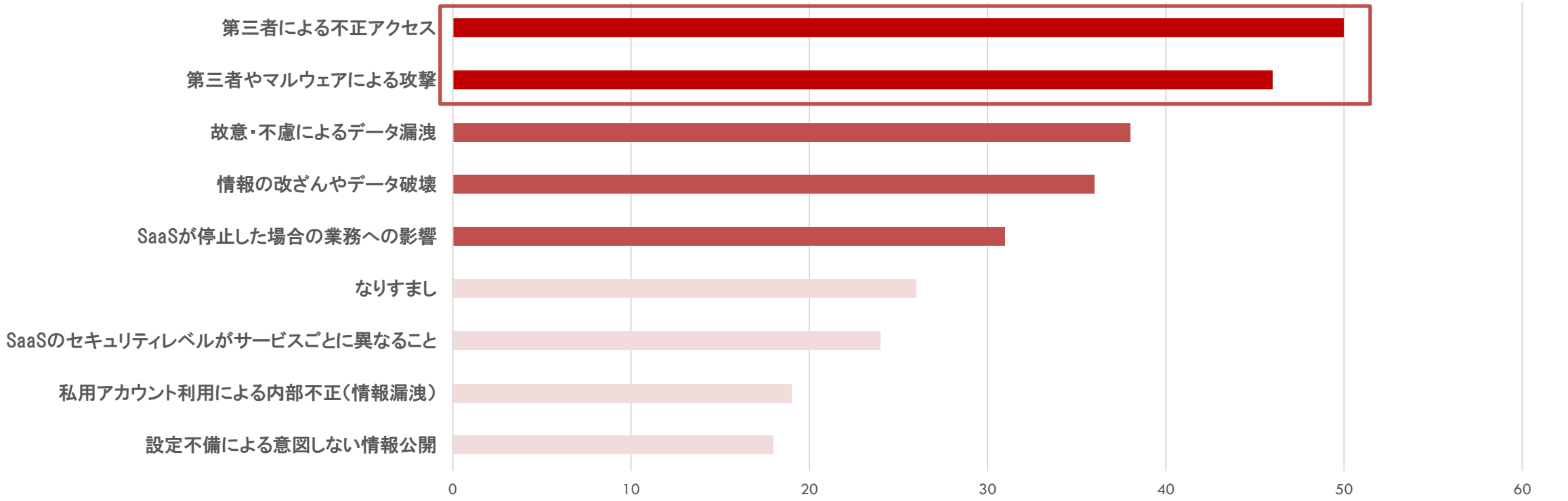
※わからない16 とくに対策はしていない4 除く

SaaSのセキュリティ対策としては「アカウント・パスワードの定期的な見直し・棚卸」が最も多い結果に。ただし他の項目についても40人を超えており、SaaSサービスのセキュリティ対策としてどの会社もさまざまな策を実施していることがわかりました。

3-3 SaaSの利用における心配事項

HITACHI
Inspire the Next

Q3 SaaSを利用していて、次のうち最も心配なことは何ですか？
（お答えはいくつでも）



※とくに心配なことはない13 除く

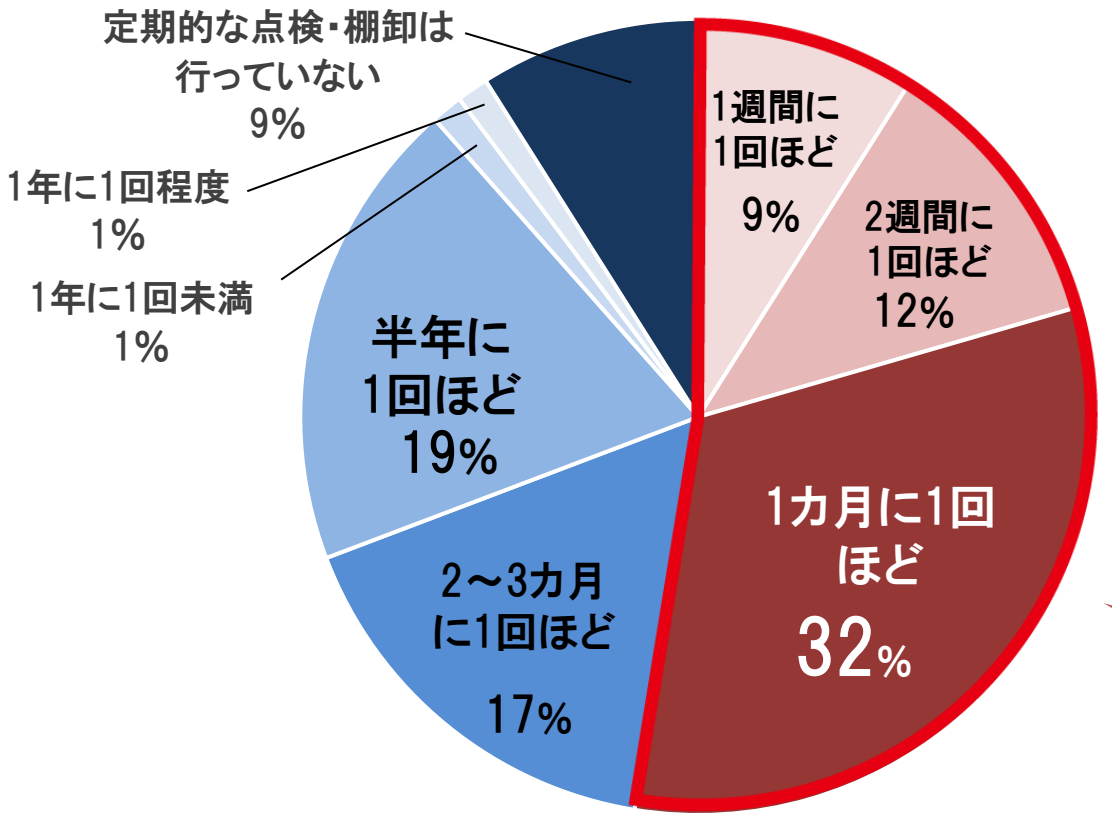
最も心配なことは、「第三者による不正アクセス」が最も多く、「第三者やマルウェアによる攻撃」が続く結果となりました。社内からのデータ漏洩や破壊よりも、第三者の侵入の方が警戒されていることがわかりました。

3-4　定期的な点検・棚卸の実施状況

HITACHI
Inspire the Next

Q4　あなたの会社では、ゲストユーザーなど、不適切アカウントがないか定期的な点検・棚卸を行っていますか？

（お答えは1つ）



1カ月以内に1回 合計53%

※わからない22　除く

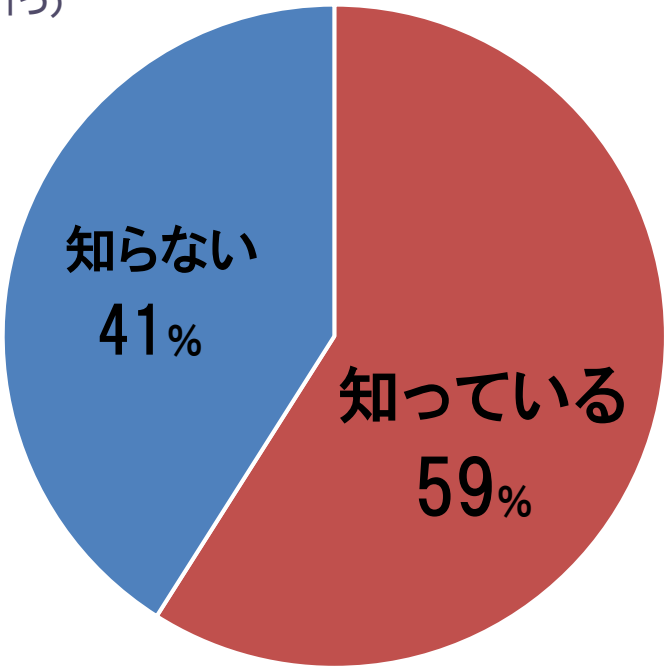
定期的な点検・棚卸の頻度は1カ月以内に1回ほどの合計が53%を占める結果となりました。従業員500人以上の企業では、大半が、短期間に定期的な点検・棚卸を行っていることがわかりました。

3-5 SaaS関連の事件・事例やインシデント

HITACHI
Inspire the Next

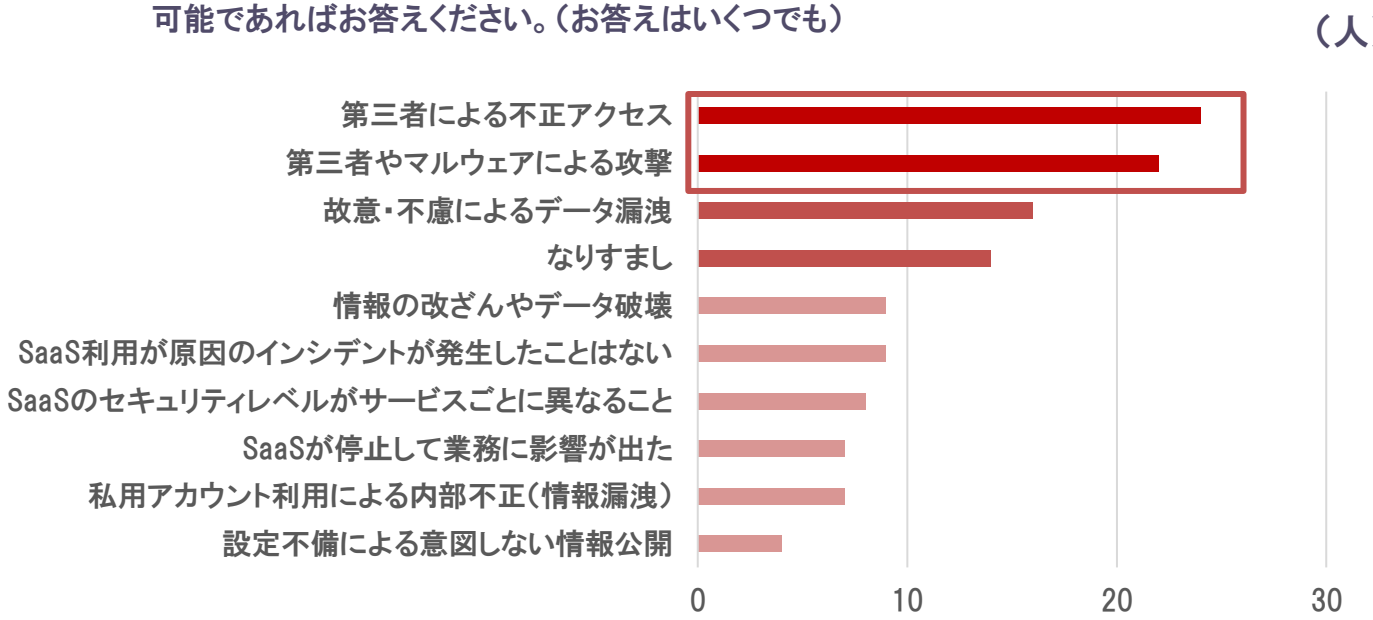
Q5 SaaSの設定ミスから情報漏洩につながった事件・事例があることを知っていますか？

（お答えは1つ）



Q6 SaaS利用が原因のインシデントが発生したことはありますか？ある場合、どのようなインシデントでしたか？

可能であればお答えください。（お答えはいくつでも）



※回答者は前問で知っていると答えた59人

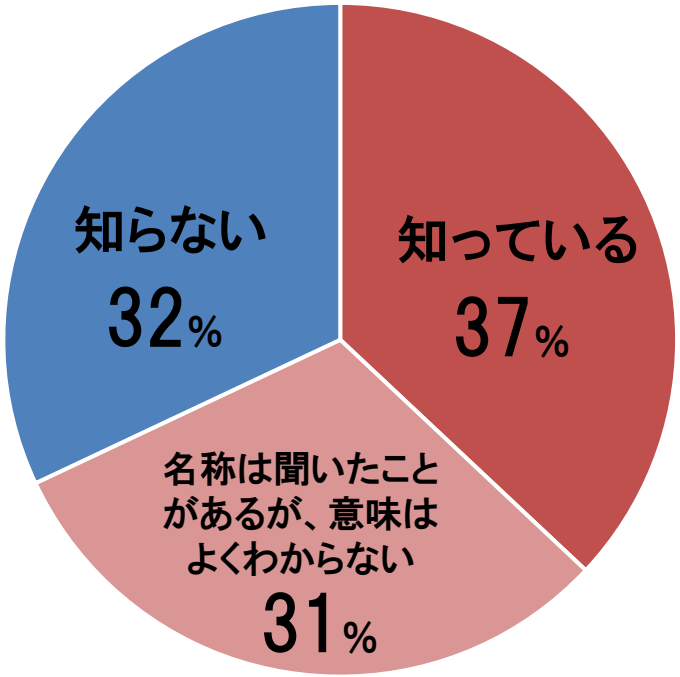
情報漏洩につながった事件・事例については、59%が「知っている」と回答しました。
自社で発生したインシデントについては、「第三者による不正アクセス」が最も多く、第三者やマルウェアによる攻撃が続きました。右のグラフの総票数は120で回答者数は59人のため、一人あたり平均約2件はSaaS利用が原因のインシデントが発生したことがあるようです。

3-6 SSPMの認知と導入状況

HITACHI
Inspire the Next

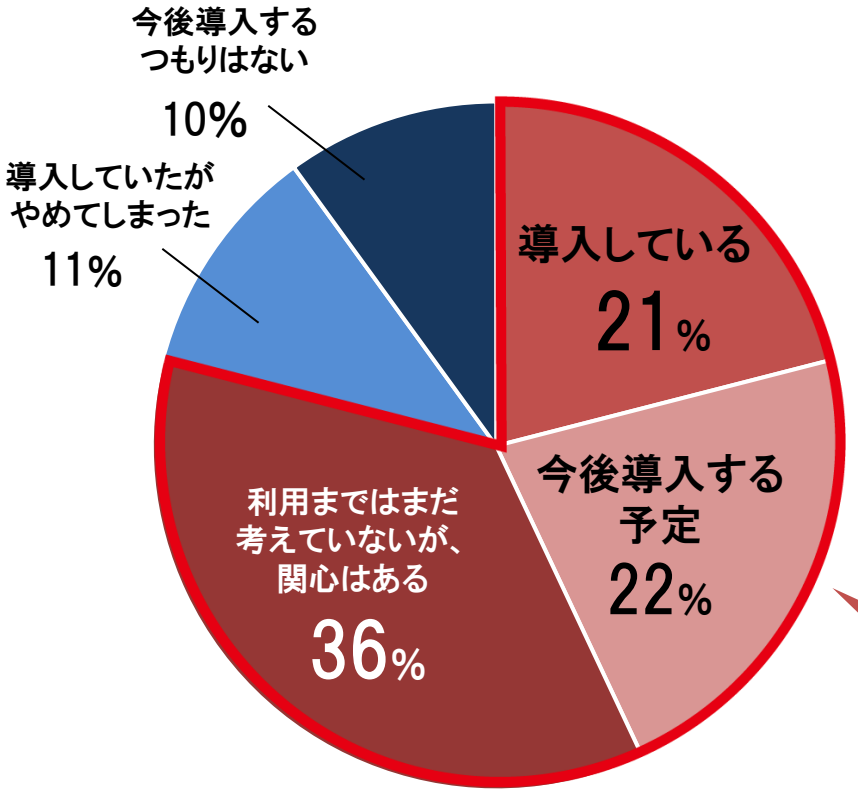
Q7 あなたは、SSPMを知っていますか？

（※「SSPM」は「SaaS Security Posture Management」の略で、SaaSのセキュリティリスクを継続的に監視・チェック・管理する技術を指します。）（お答えは1つ）



Q8 あなたの会社では、SSPMを導入していますか？

（お答えは1つ）



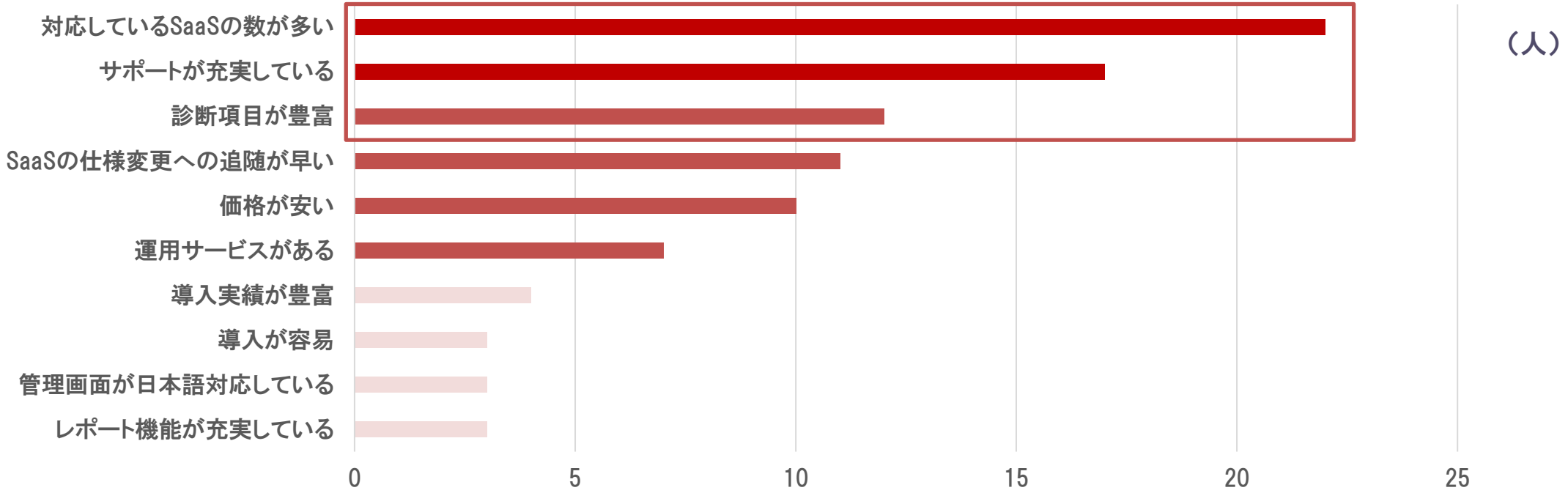
導入済み～関心あり 合計79%

SSPMを「知っている」と答えた人は37%で、認知度はまだ高いとは言えません。ですが、SSPMを導入している人から関心はある人までの合計は79%と高く、多くの企業がSSPMの導入に前向きであることがわかりました。今後も、導入する企業は増えるかもしれません。

3-7 SSPMの選定ポイント

HITACHI
Inspire the Next

Q9 SSPMを導入する際の選定ポイントを教えてください。（お答えは3つまで）



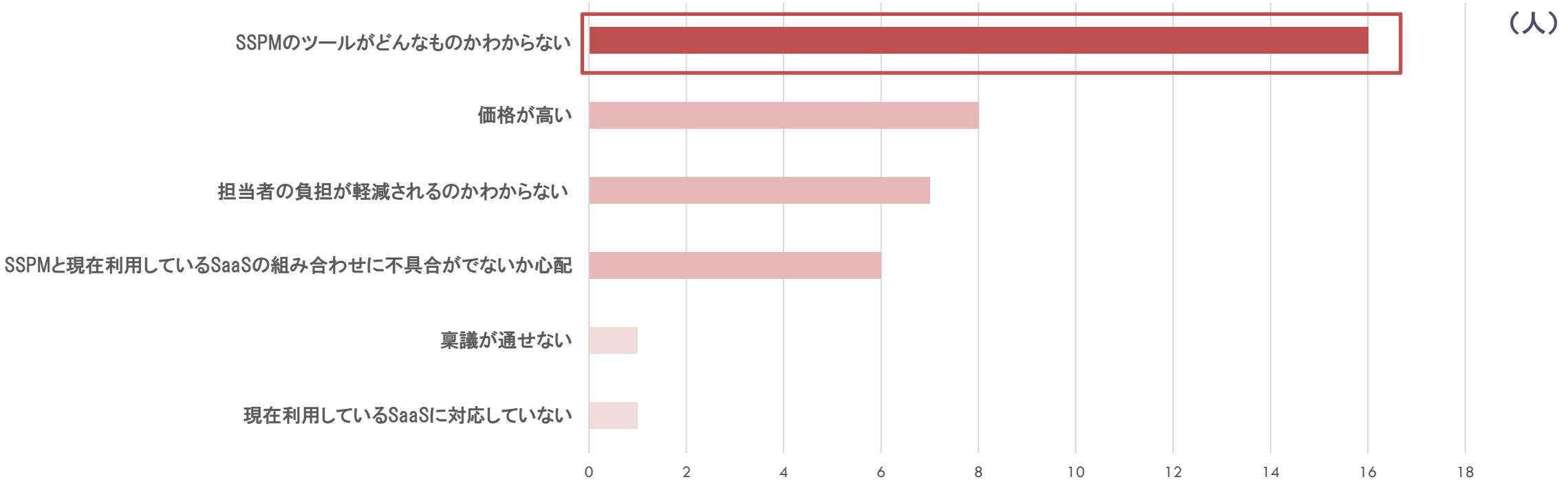
※回答者：前問で「導入している」「今後導入する予定」と答えた43人

SSPM導入の際の選定ポイントは「対応しているSaaSの数が多い」が最も多い結果に。Q1でもさまざまなSaaSを導入している企業が多かったので、自社が使っているSaaSに対応しているかは重要なポイントのようです。その他のポイントとしては、「サポートが充実している」・「診断項目が豊富なこと」が続きました。

3-8 SSPMの導入を考えていない理由

HITACHI
Inspire the Next

Q10 SSPMの導入を考えていない方にお聞きします。その理由は何ですか？（お答えはいくつでも）



※回答者：Q8で「今後導入するつもりはない」「利用まではまだ考えていないが、関心はある」と答えた46人
※わからない17　除く

導入を考えていない人の理由は、「SSPMのツールがどんなものかわからない」との意見が圧倒的に多い結果に。SSPMがどんなものか理解する企業が増えてくれば、さらにSSPMを導入しようとする動きになるのではないかと考えられます。

3-9 まとめ　SaaS利用時のセキュリティインシデント発生を防ぐためにも対策の強化が重要

HITACHI
Inspire the Next

現状

現在利用しているSaaSについて、「利用している」と回答した人数が10人以上のものは10種類あり、さまざまなツールが使用されていることがわかった。
SSPMを知っていると答えた人は37%であり、認知度はまだ高いとは言えないが、導入している企業・関心があるという企業の割合をまとめると、79%の企業はSSPM導入に前向きであると言える。

課題

SaaS利用時に発生したインシデントがあるか聞き、「ある」と回答した企業で最も多かったのは「第三者による不正アクセス」であった。またその次には、「第三者やマルウェアによる攻撃」が続いた。今回の調査によると、1社あたり平均約2件は、インシデントが発生したことがあるとわかった。

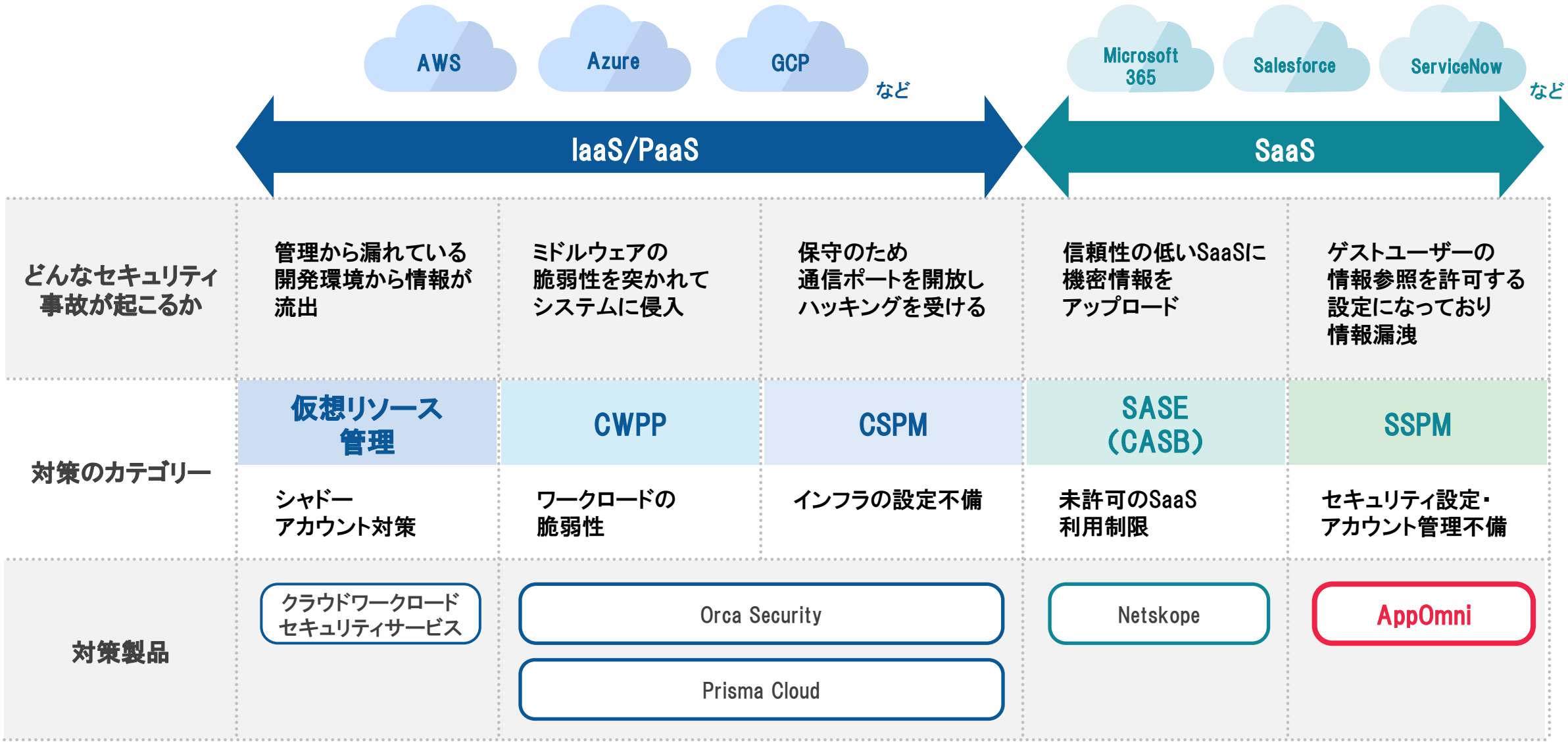
結論

SaaS利用時にインシデントが発生したことのある企業は多く、1社あたり平均約2件は遭遇している。
そういった企業はSaaS利用時のセキュリティリスクの継続的な監視・チェック・管理を行うSSPMを導入することで、リスクの低減をはかることができる。さまざまなSaaSを利用している企業も多いので、対応しているSaaSの数が多く、診断項目が豊富なSSPMを導入するのが重要である。
また、約8割の企業がSSPMに前向きであることから、今後もさらにSSPMの導入は進んでいくと予想される。

4. 日立ソリューションズが提案するSSPMサービス

4-1　クラウドサービスのセキュリティ対策

HITACHI
Inspire the Next



AWS：Amazon Web Services, Azure：Microsoft Azure, GCP：Google Cloud Platform, IaaS：Infrastructure as a Service,
PaaS：Platform as a Service,　CWPP：Cloud Workload Protection Platform, CSPM：Cloud Security Posture Management,
SASE：Secure Access Service Edge, CASB：Cloud Access Security Broker

4-2 AppOmniとは

HITACHI
Inspire the Next

ゲストユーザーの権限が過剰
知らぬ間に取引先情報が流出

Microsoft 365

退職者のアカウントが悪用され
機密情報が流出

30種類以上のSaaSに対応

SaaSからの情報漏洩を防ぐ

Salesforce

ServiceNow

AppOmni

Zoom

Workday

セキュリティ対策不備の診断・監視

疑わしいアクセスの検知

コンプライアンス基準での評価

各種レポート出力

不要なサードパーティー
アプリケーションのアクセスを許可

GitHub

開発環境からソースコードや
システムのアクセスキーが流出

4-3 何ができるか

HITACHI
Inspire the Next

AppOmni

セキュリティ対策不備の監視
（セキュリティ設定・権限・アカウント管理）

疑わしいアクセスの検知

NIST,ISO,SOC2など
コンプライアンス基準での安全性評価

ポリシーのカスタマイズ

監査に便利な各種レポート

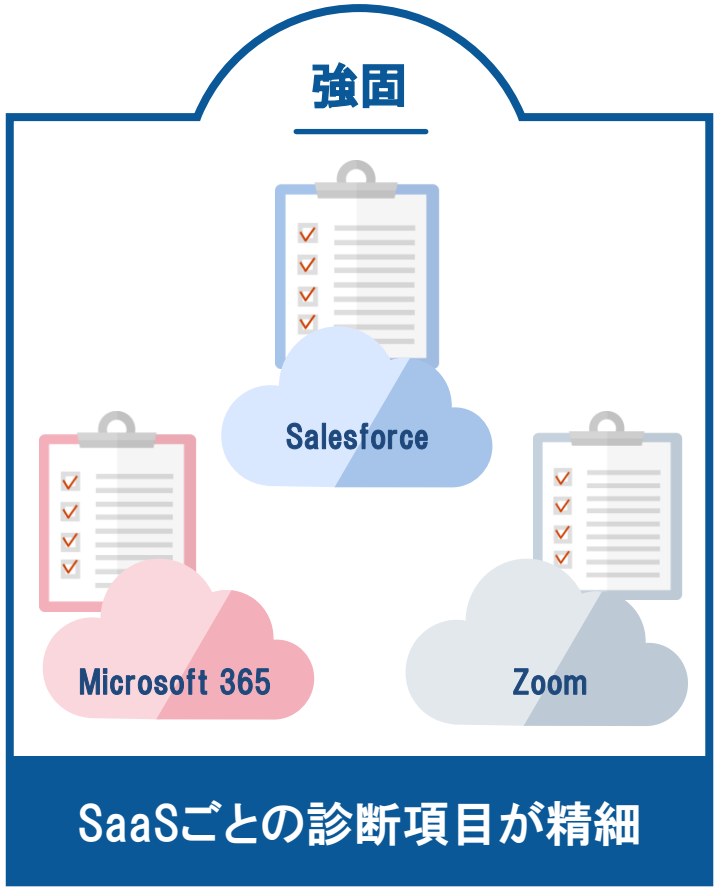
独自SaaSの監視
（開発プラットフォーム）

NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

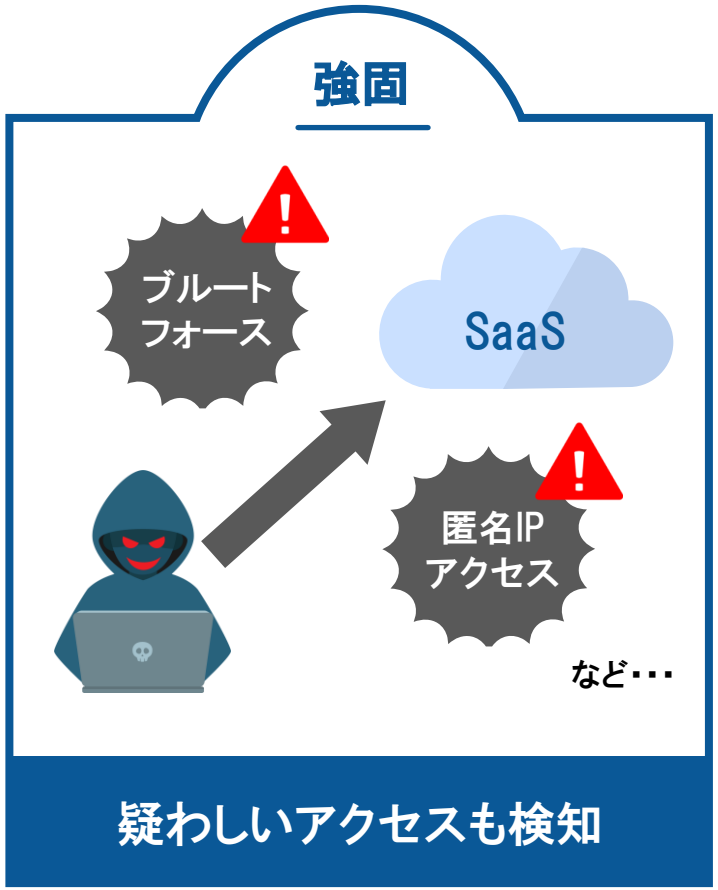
4-4 セールスポイント

HITACHI
Inspire the Next

強固かつ運用が楽



SaaSごとの診断項目が精細



疑わしいアクセスも検知

SaaS仕様変更にも自動追従
AppOmni Insights

4-5 対応SaaS

HITACHI
Inspire the Next

30種類以上のSaaSを一元管理(2023年5月時点)

拡大中

- Google Workspace
- Microsoft 365
- Salesforce
- ServiceNow
- Workday
- Auth0
- Azure Active Directory
- Box
- Confluence
- Microsoft Exchange Online
- Fastly
- GitHub
- HubSpot
- Microsoft Intune
- Jira Software
- JumpCloud
- Microsoft Defender
- monday.com
- Okta
- Microsoft OneDrive
- Ping Identity
- SendGrid
- Microsoft SharePoint
- Slack
- Smartsheet
- Snowflake
- Tableau
- Microsoft Teams
- Veeva Vault
- Zendesk
- Zoom
- CrowdStrike
- Cisco Secure Access by Duo
- Jamf
- GitLab
- Lucid
- NetSuite
- Wizcloud

AppOmni

4-6　AppOmniのトライアル利用について

HITACHI
Inspire the Next

無償でトライアル利用ができます！

2週間
まで

トライアルの条件

1. AppOmni社とお客さま間でNDA契約が必要
2. トライアル前に次の点をご提示いただく必要があります
   - ✓ トライアルの目的
   - ✓ 採用・不採用の判定基準
   - ✓ 評価観点
3. トライアル後の結果をフィードバックしていただくこと

トライアル実施時はリモート会議で設定作業をご支援できます。

AppOmni

本レポートの利用について

本レポートの利用に関する注意書き

本レポートの利用について

■本レポートの利用に関して

・当レポートのすべての内容（情報・画像など）の著作権は、当社が保有します。許可なく複製・転用・販売などへの二次利用は禁じます。

・本レポートの全文または一部を転載・複製する際は著作権者の許諾が必要ですので、当社までご連絡ください。

■AppOmni Webサイト

https://www.hitachi-solutions.co.jp/security/lp/appomni/

■お問い合わせ

株式会社　日立ソリューションズ

https://www.hitachi-solutions.co.jp/inquiry/products/form/?id=appomni