NTT Security

情シス818人に聞いた！

MDR＆IR利用実態調査

本調査について

近年、サイバー攻撃の手法が高度化・多様化しており、企業はより高度なセキュリティ対策を求められています。特にランサムウェア攻撃やフィッシング攻撃の増加が顕著であり、企業のセキュリティ体制の強化が急務となっています。さらに、クラウドサービス利用の増加に伴いクラウド環境におけるセキュリティ対策の重要性が増しています。

このような市場環境の中、多くの企業が自社内でのセキュリティ対策に限界を感じ、外部の専門サービスであるMDR(Managed Detection and Response)を導入するケースが増えています。MDRは24時間365日の監視と迅速な対応を提供し、企業のセキュリティ体制を強化します。また、サイバー攻撃が発生した際の迅速な対応を求め、IR(Incident Response)サービスの需要も高まっています。IRサービスは攻撃の被害を最小限に抑え、迅速な復旧を支援します。

そこで、今回、企業の情報システム担当者さまにMDRとIRの利用実態調査を行いました。実際にMDRやIRを利用している担当者さまの回答から、セキュリティ製品の導入状況、導入後の課題、そしてMDRおよびIRサービスの導入状況や導入理由、その効果について知ることができる調査結果となっています。

本調査結果が、今後のセキュリティ対策強化のお役に立てば幸いです。

NTTセキュリティ・ジャパン株式会社

目次

- MDR＆IR利用実態調査結果
- 調査結果まとめ
- NTTセキュリティのサービスのご紹介
- 参考資料）調査結果全データ

調査結果

本調査について

調査概要

- 調査期間：2024年11月28日～12月9日
- 調査方法：インターネット調査
- 調査人数：818名
- 調査対象：従業員数500名以上の規模の企業に所属している情報システム担当者
- モニター提供元：GMOリサーチ＆AI株式会社
- 調査機関： GMOリサーチ＆AI株式会社

調査項目について

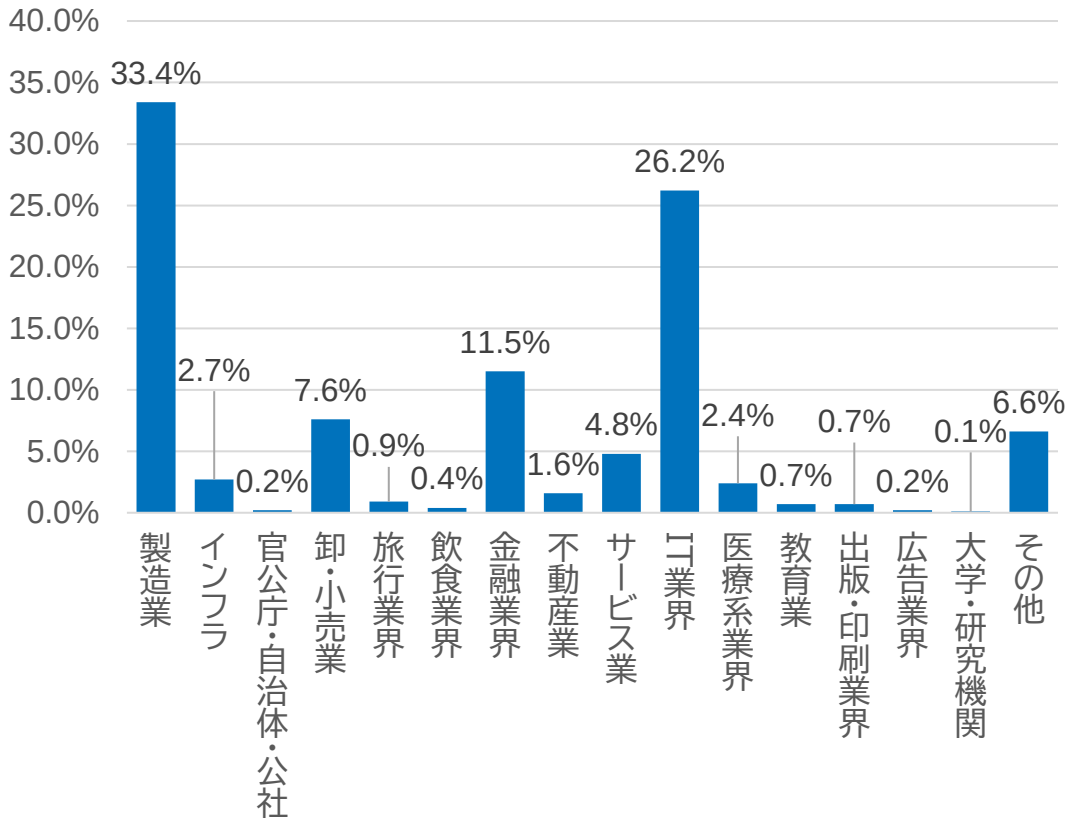
No.	調査項目	No.	調査項目
1	管理しているPC台数を教えてください。	12	社内アクセス製品(VPN/ZTNAなど)を選定した理由を教えてください。
2	アンチウィルス製品を導入していますか？	13	社内アクセス製品(VPN/ZTNAなど)導入後の課題や不満を教えてください。
3	EDR製品を導入していますか？	14	MDRサービスを導入していますか？
4	社外アクセス製品(プロキシ/SWGなど)を導入していますか？	15	どのようなきっかけでMDRサービスを導入検討しましたか？
5	社内アクセス製品(VPN/ZTNAなど)を導入していますか？	16	導入前に何を期待してMDRサービスを導入しましたか？
6	アンチウィルス製品を選定した理由を教えてください。	17	MDRサービスを導入して実際に得られた成果を教えてください。
7	アンチウィルス製品導入後の課題や不満を教えてください。	18	IRサービスを導入していますか？
8	EDR製品を選定した理由を教えてください。	19	どのようなきっかけでIRサービスを導入検討しましたか？
9	EDR製品導入後の課題や不満を教えてください。	20	導入前に何を期待してIRサービスを導入しましたか？
10	社外アクセス製品(プロキシ/SWGなど)を選定した理由を教えてください。	21	IRサービスを導入して実際に得られた成果を教えてください。
11	社外アクセス製品(プロキシ/SWGなど)導入後の課題や不満を教えてください。	22	MDRサービスやIRサービスを選定判断する際の重要な要素を教えてください。

回答者の属性情報

NTT Security

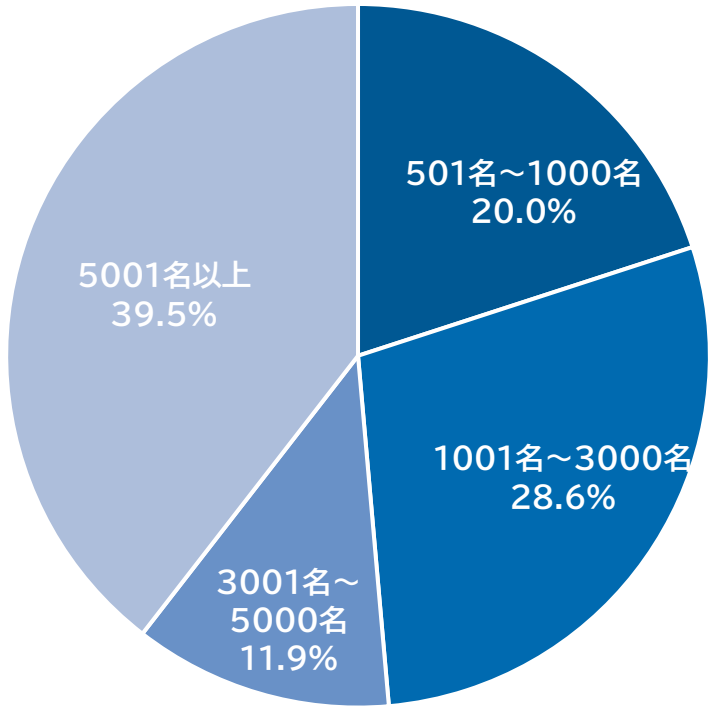
●業界

製造 33.4%、IT 26.2%、金融 11.5%、小売 7.6%で全体の約8割を占める



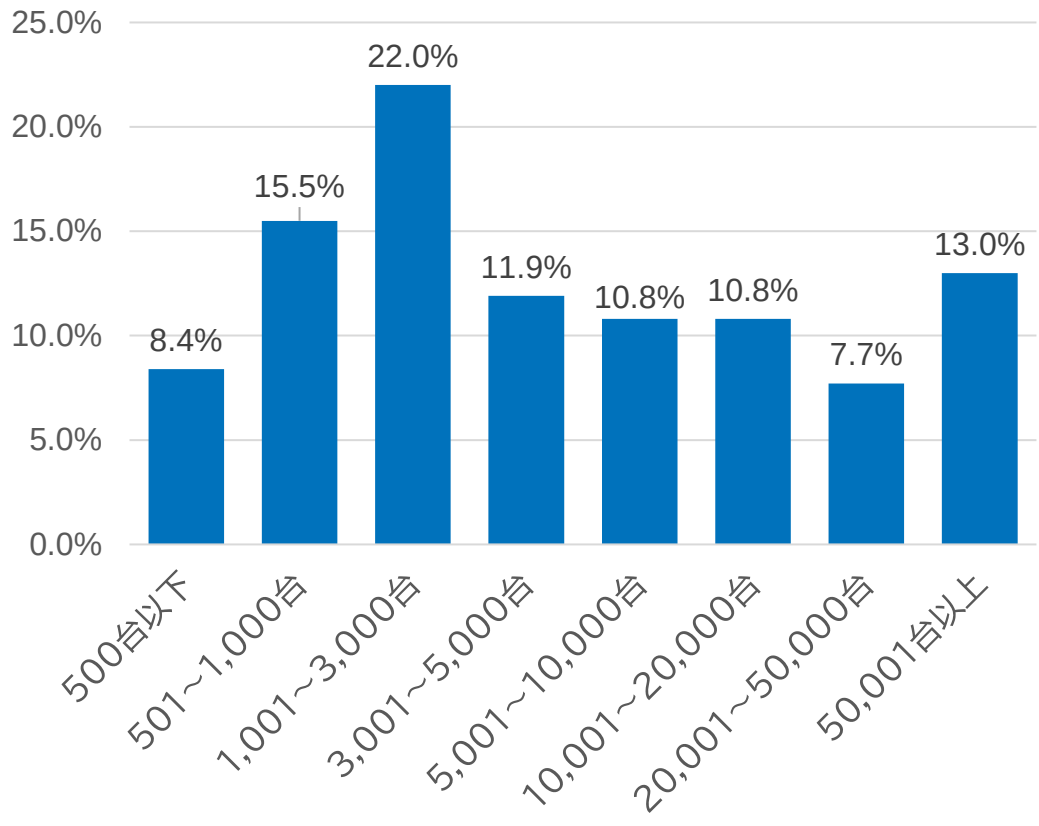
●従業員数

5001名以上が40%で最多、次いで1001～3000名が29%



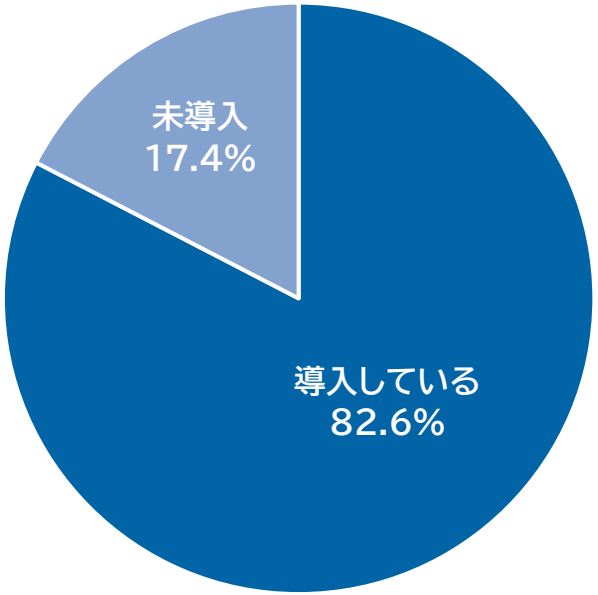
PC管理台数

Q.1 管理しているPC台数を教えてください。
（有効回答数：818）

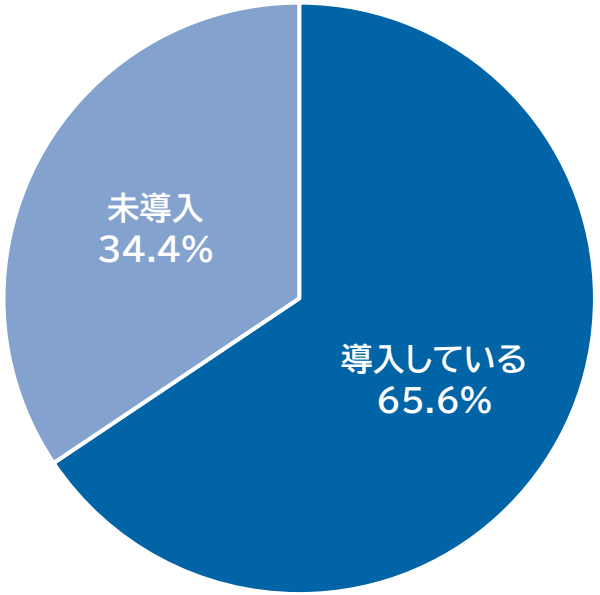


アンチウィルス・EDR製品の導入の有無

Q.2 アンチウィルス製品を導入していますか？
（有効回答数：818）

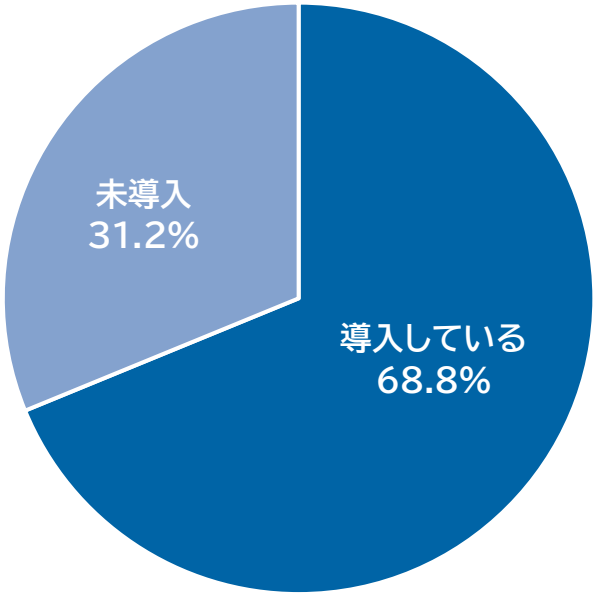


Q.3 EDR製品を導入していますか？
（有効回答数：818）

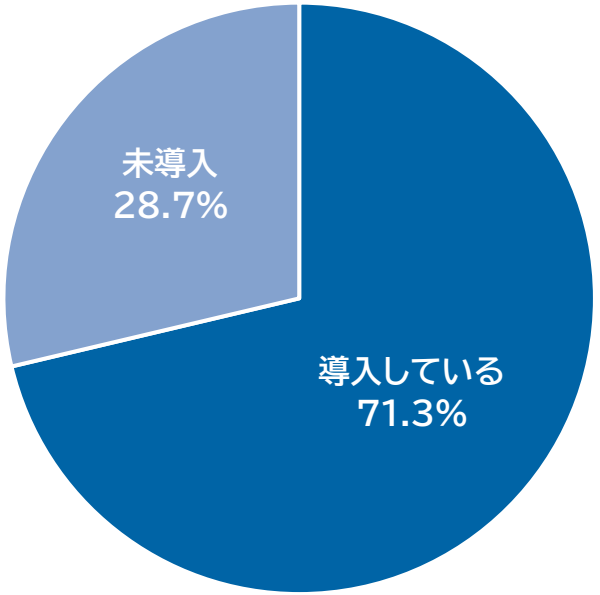


社外アクセス・社内アクセス製品の導入の有無

Q.4 社外アクセス製品（プロキシ/SWGなど）を導入していますか？
（有効回答数：818）

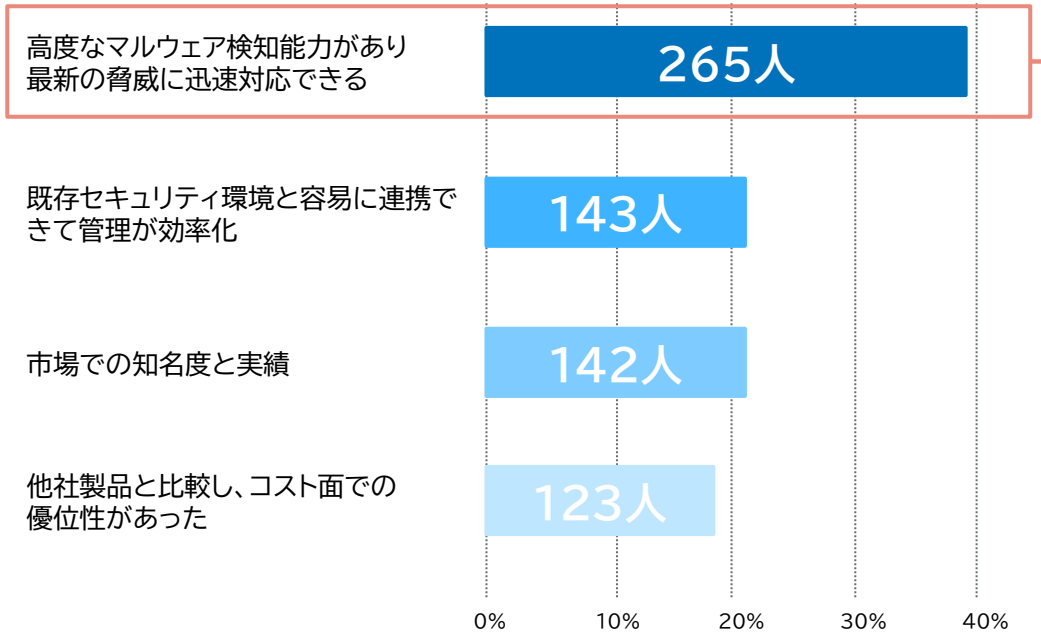


Q.5 社内アクセス製品（VPN/ZTNAなど）を導入していますか？
（有効回答数：818）

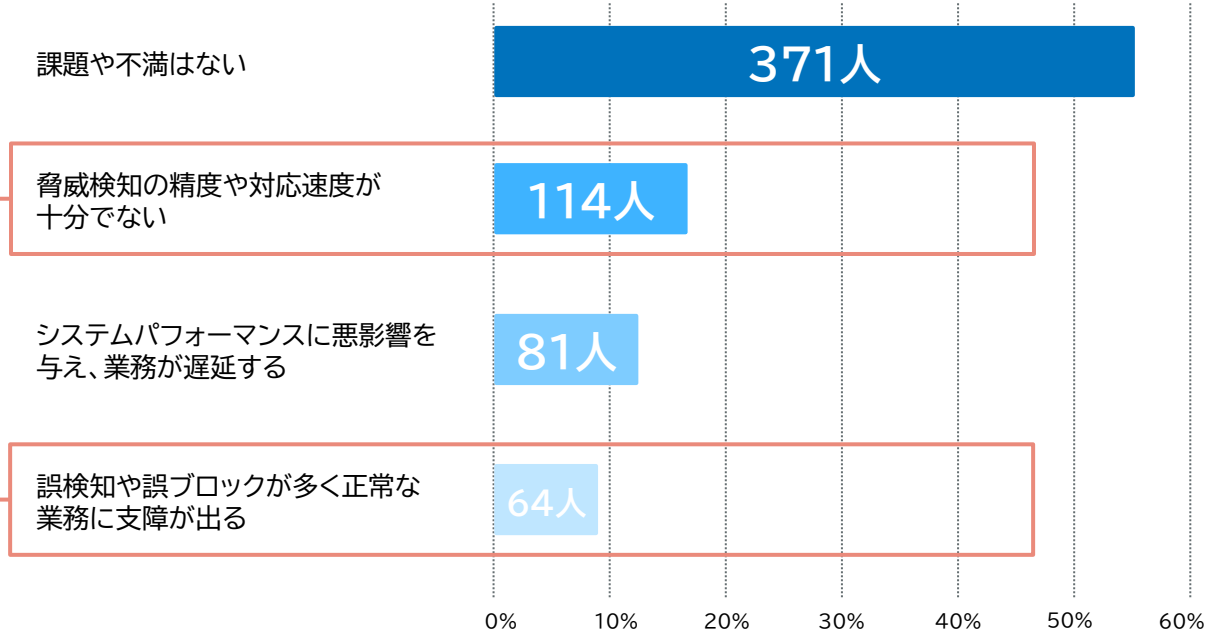


アンチウィルス製品の選定理由と導入後の課題（上位回答）※全回答は最終ページ

Q.6 アンチウィルス製品を選定した理由を教えてください。
※複数回答可（有効回答数：676）



Q.7 アンチウィルス製品導入後の課題や不満を教えて下さい。
※複数回答可（有効回答数：676）

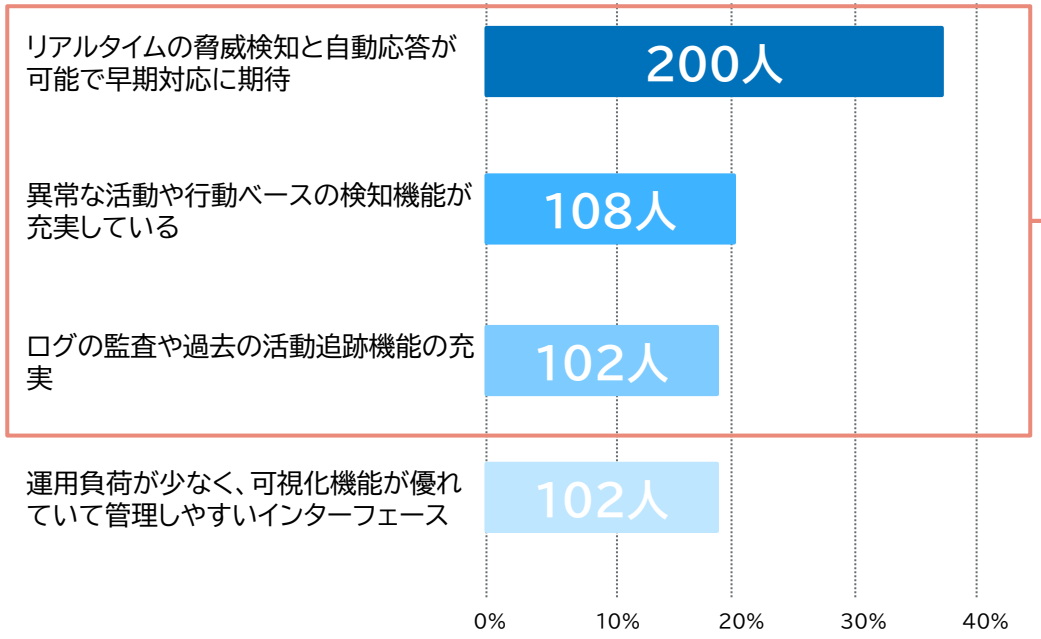


ポイント

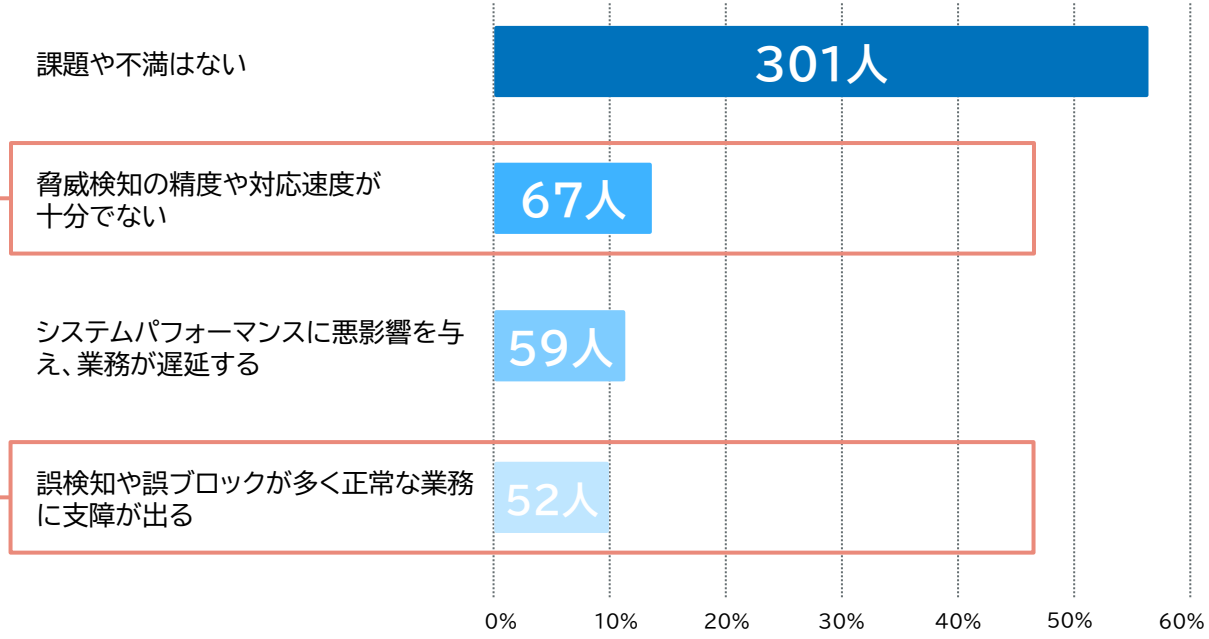
高度な脅威検知能力や迅速対応に期待して導入したものの、実際導入してみると脅威検知の精度や対応速度、誤検知や誤ブロックによる業務への支障に課題を持つケースがあるようです。
一方で、371人（55%）が導入後の課題や不満はないと回答しています。

EDR製品の選定理由と導入後の課題（上位回答）※全回答は最終ページ

Q.8 EDR製品を選定した理由を教えてください。
※複数回答可（有効回答数：537）



Q.9 EDR製品導入後の課題や不満を教えてください。
※複数回答可（有効回答数：537）

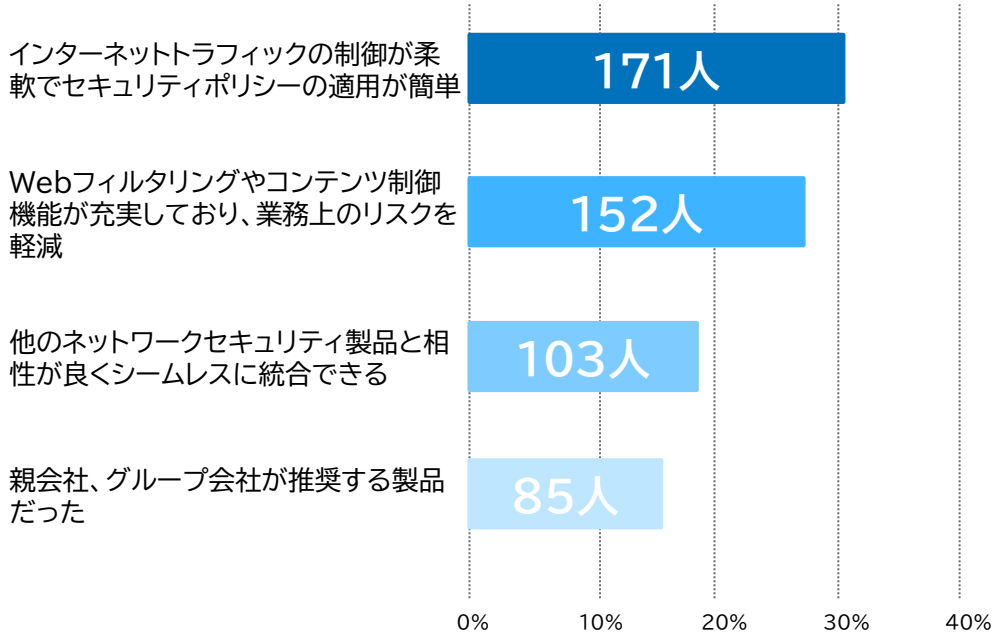


ポイント

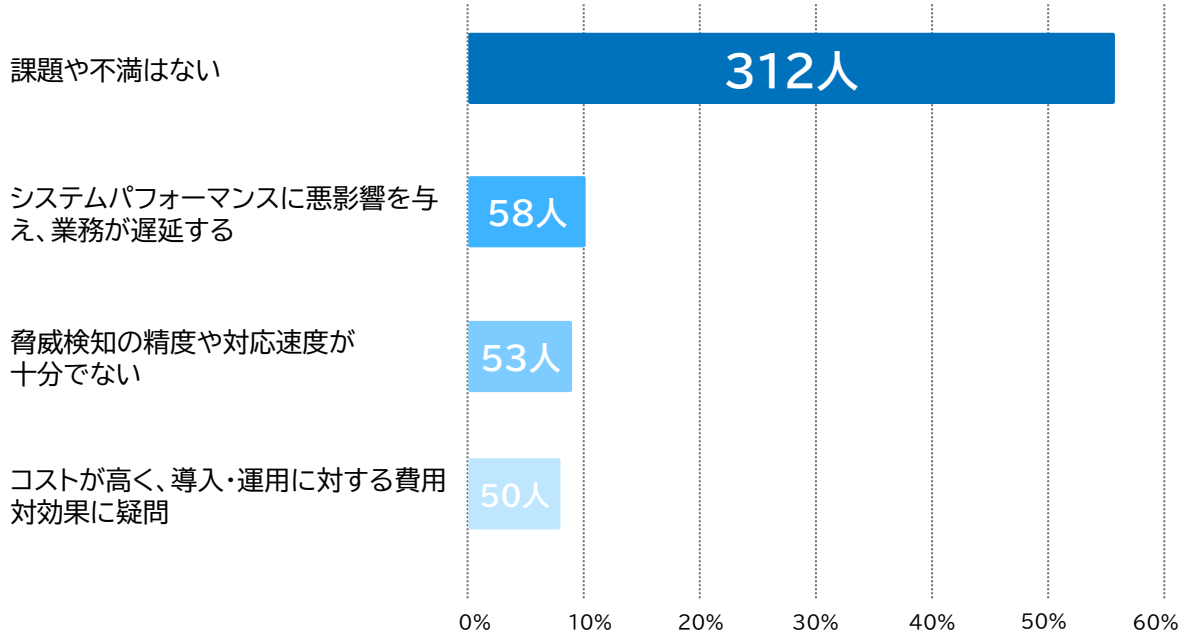
リアルタイムの脅威検知自動応答による早期対応や、検知機能、ログ監査や過去の活動追跡機能に期待が高いようです。しかし、実際導入してみると脅威検知の精度や対応速度への課題、誤検知や誤ブロックによる業務への支障に課題を持つケースがあるようです。一方で、301人（56.1%）が導入後の課題や不満はないと回答しています。

社外アクセス製品の選定理由と導入後の課題(上位回答) ※全回答は最終ページ

Q.10 社外アクセス製品を選定した理由を教えてください。
※複数回答可（有効回答数:563）



Q.11 社外アクセス製品導入後の課題や不満を教えてください。
※複数回答可（有効回答数:563）

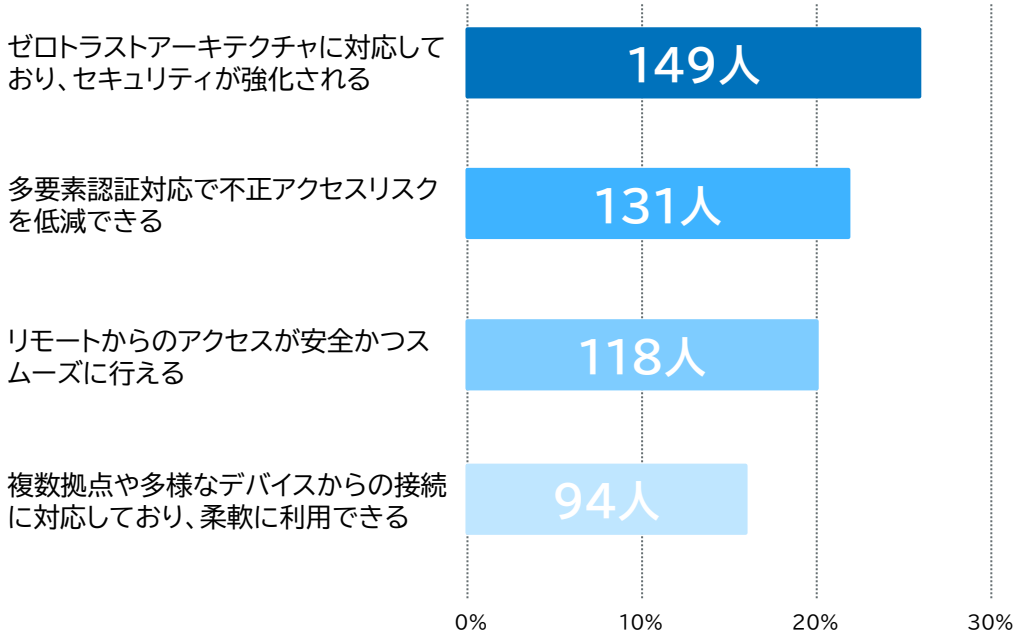


ポイント

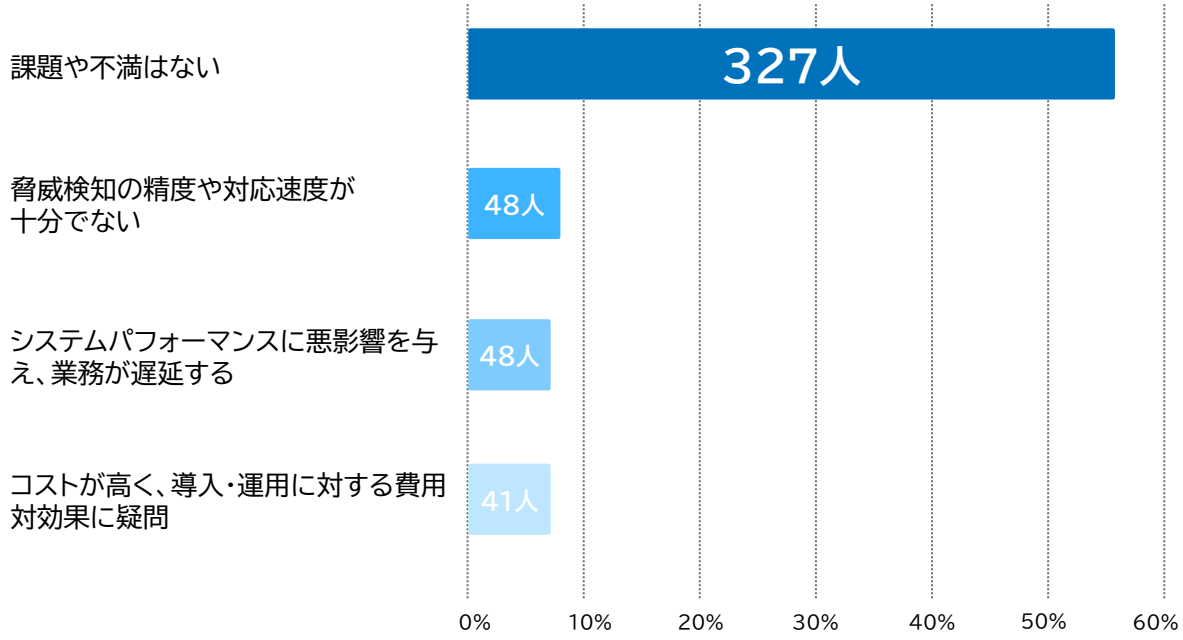
セキュリティポリシー適用の簡単さや業務上のリスクを軽減できる機能の充実が選定理由上位となりました。一方で実際に運用してみると、半数以上が課題や不満はないと回答するものの、システムパフォーマンスへの悪影響や検知精度、コストに課題感をもつケースが一部見受けられます。

社内アクセス製品の選定理由と導入後の課題（上位回答）※全回答は最終ページ

Q.12 社内アクセス製品を選定した理由を教えてください。
※複数回答可（有効回答数：583）



Q.13 社内アクセス製品導入後の課題や不満を教えてください。
※複数回答可（有効回答数：583）

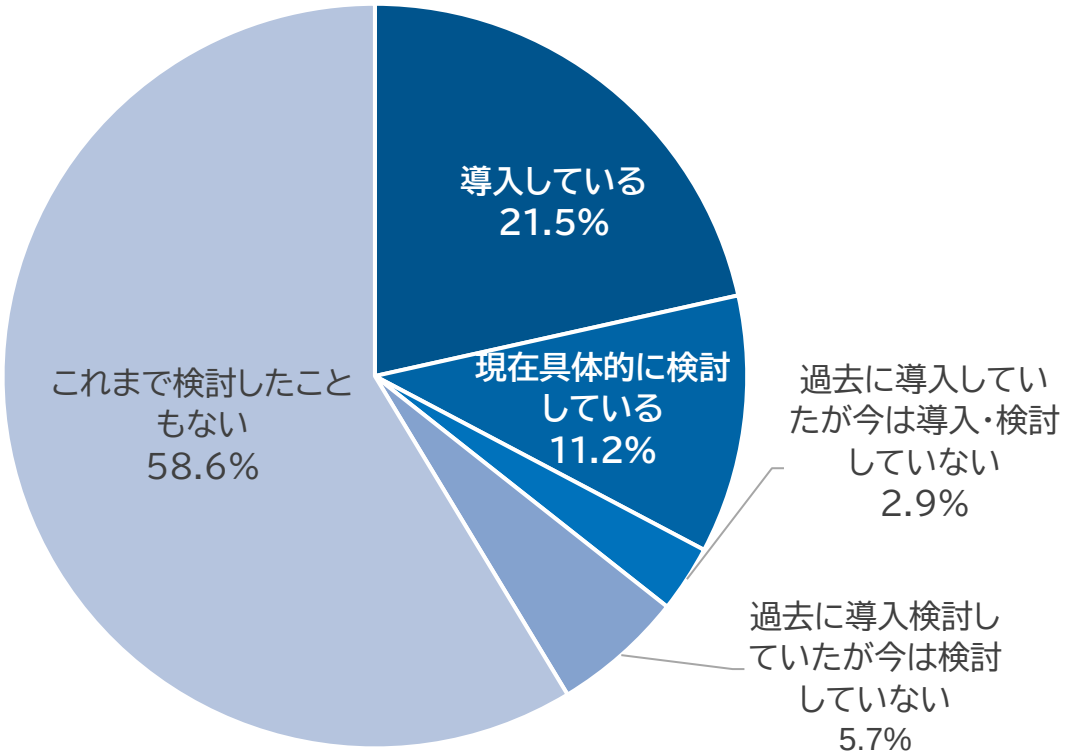


ポイント

ゼロトラストアーキテクチャへの対応や多要素認証対応が選定理由上位となりました。一方で半数以上が導入後の課題や不満はないと回答するものの、システムパフォーマンスへの悪影響や検知精度、コストに課題感をもつケースが見受けられます。

MDRサービスの導入有無

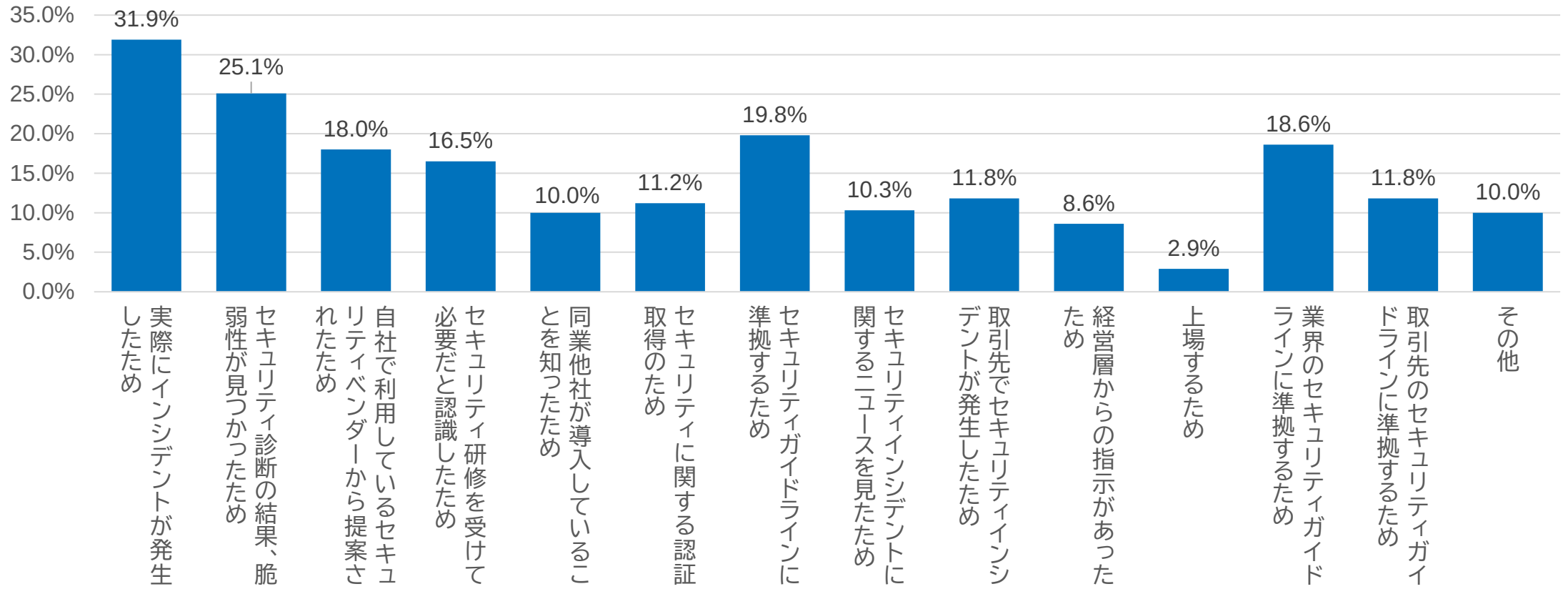
Q.14 MDRサービスを導入していますか？
（有効回答数：818）



MDRサービス導入のきっかけ

Q.15 どのようなきっかけでMDRサービスを導入検討しましたか？

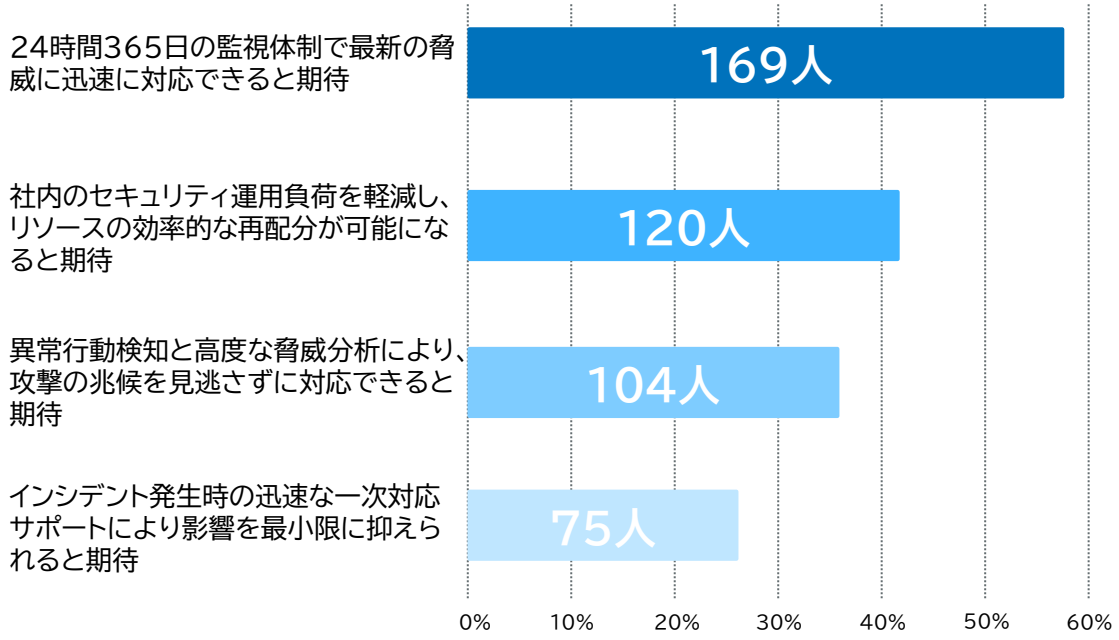
※複数回答可（有効回答数：339）



MDRサービスの選定理由と導入後の成果（上位回答）※全回答は最終ページ

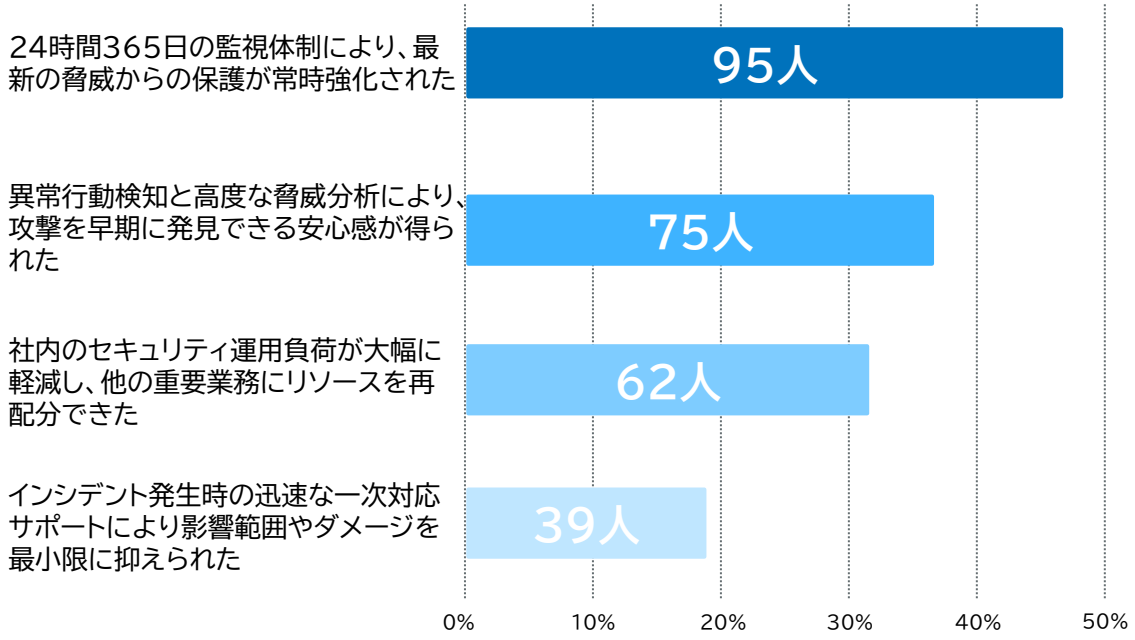
Q.16 導入前に何を期待してMDRサービスを導入検討しましたか？

※複数回答可（有効回答数：292）



Q.17 MDRサービスを導入して実際に得られた成果を教えてください。

※複数回答可（有効回答数：200）

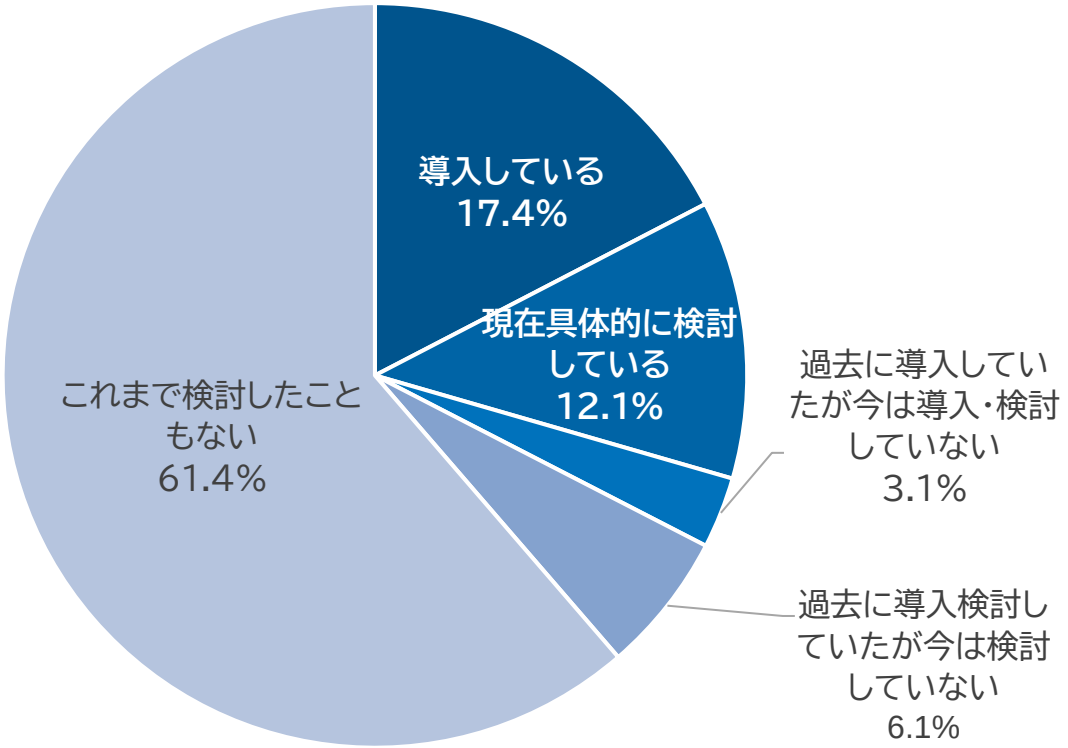


ポイント

24時間365日監視による迅速対応、社内の運用負荷軽減など、導入前の期待上位がそのまま、得られた成果につながる結果となりました。

IRサービスの導入有無

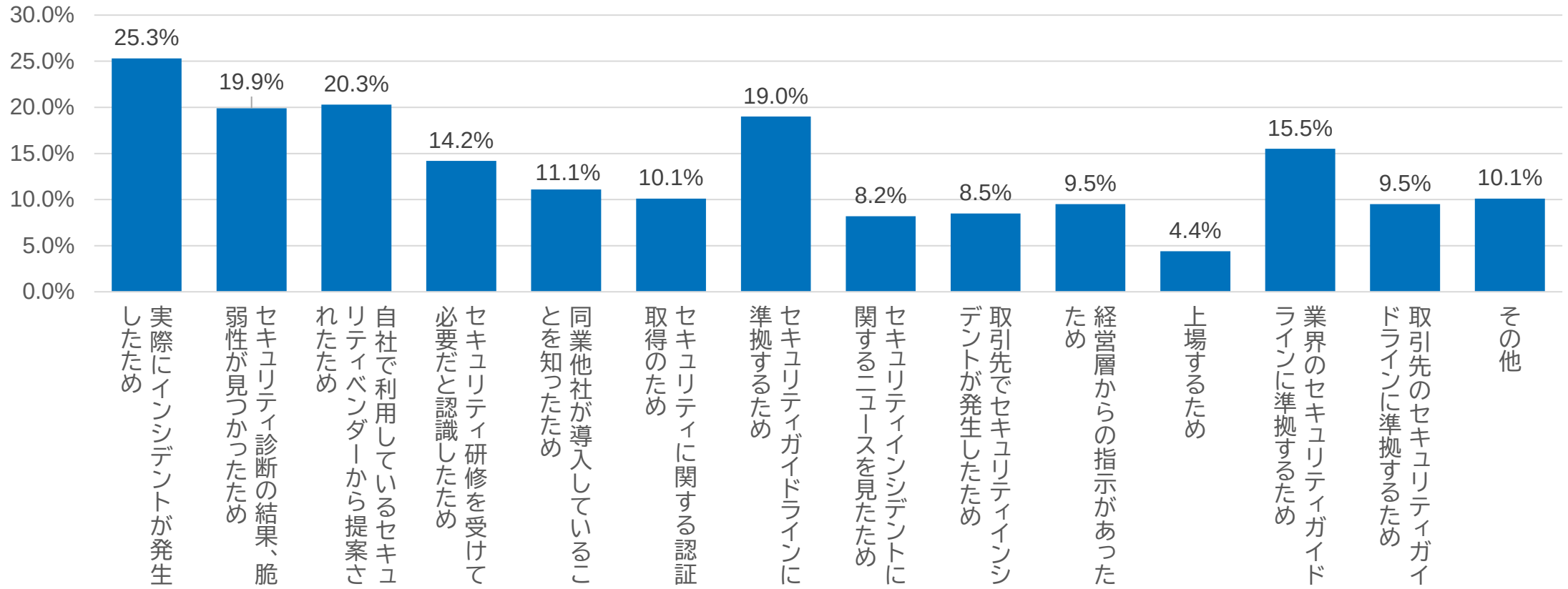
Q.18 IRサービスを導入していますか？
（有効回答数：818）



IRサービス導入のきっかけ

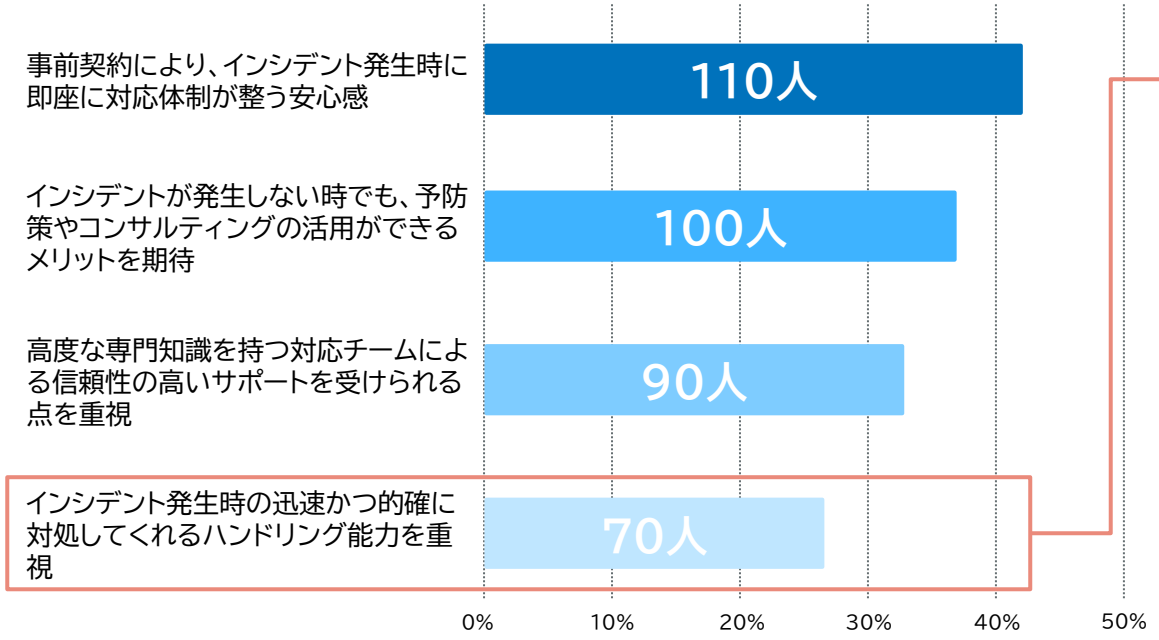
Q.19 どのようなきっかけでIRサービスを導入検討しましたか？

※複数回答可（有効回答数：316）

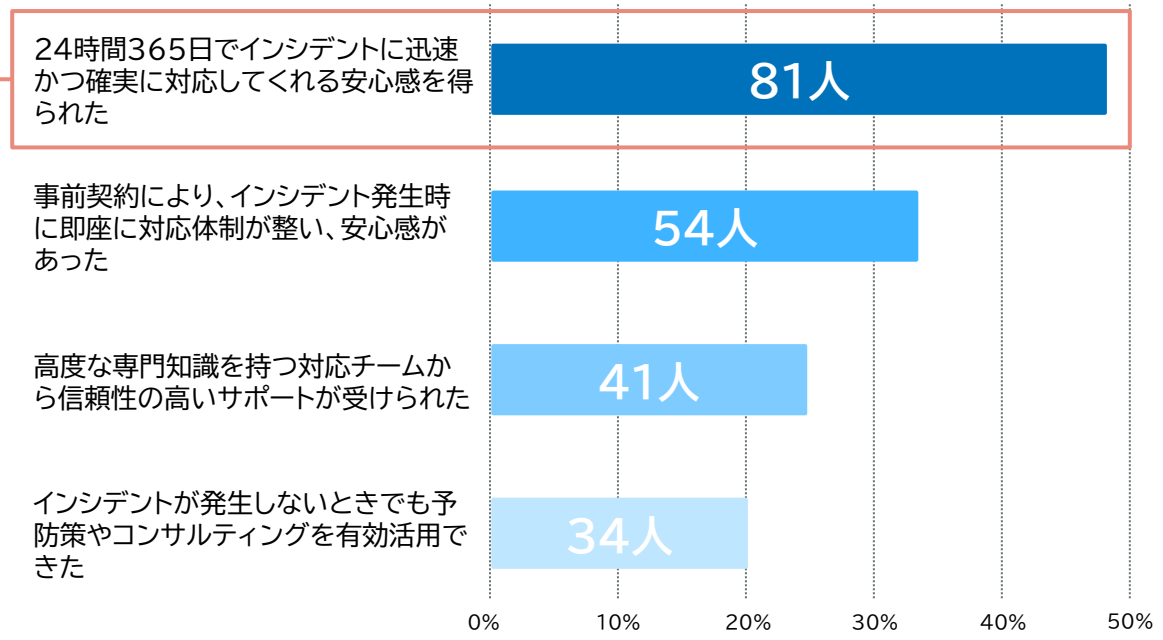


IRサービスの選定理由と導入後の成果（上位回答）※全回答は最終ページ

Q.20 導入前に何を期待してIRサービスを導入検討しましたか？
※複数回答可（有効回答数：266）



Q.21 IRサービスを導入して実際に得られた成果を教えてください。
※複数回答可（有効回答数：167）

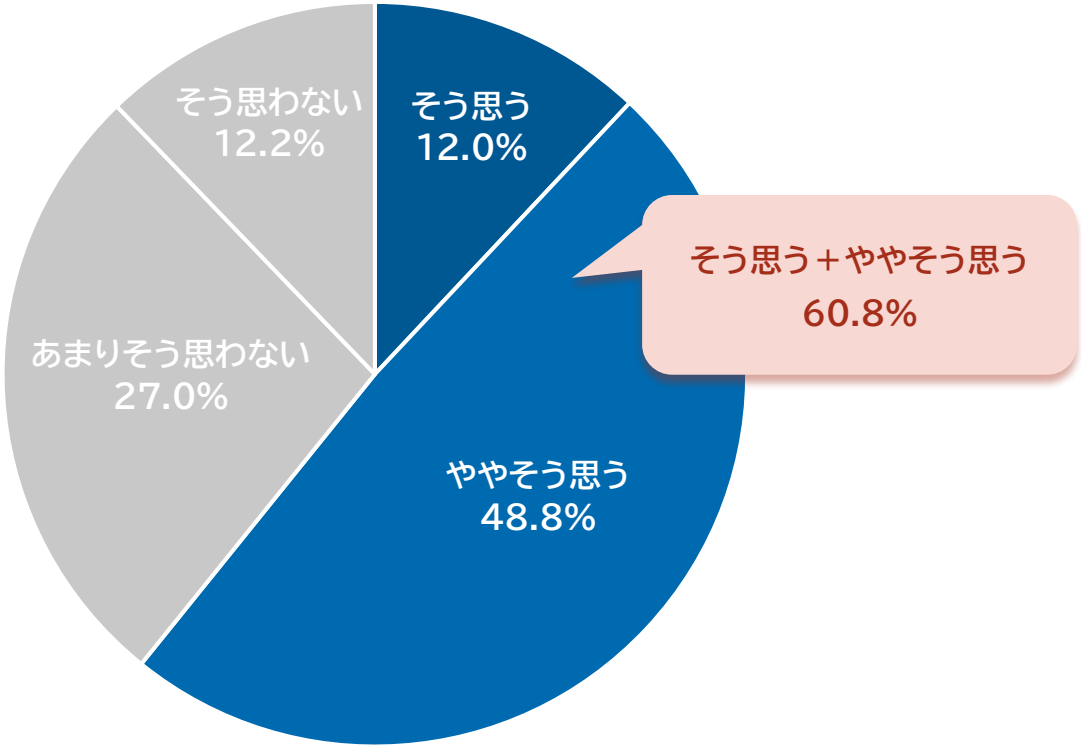


ポイント

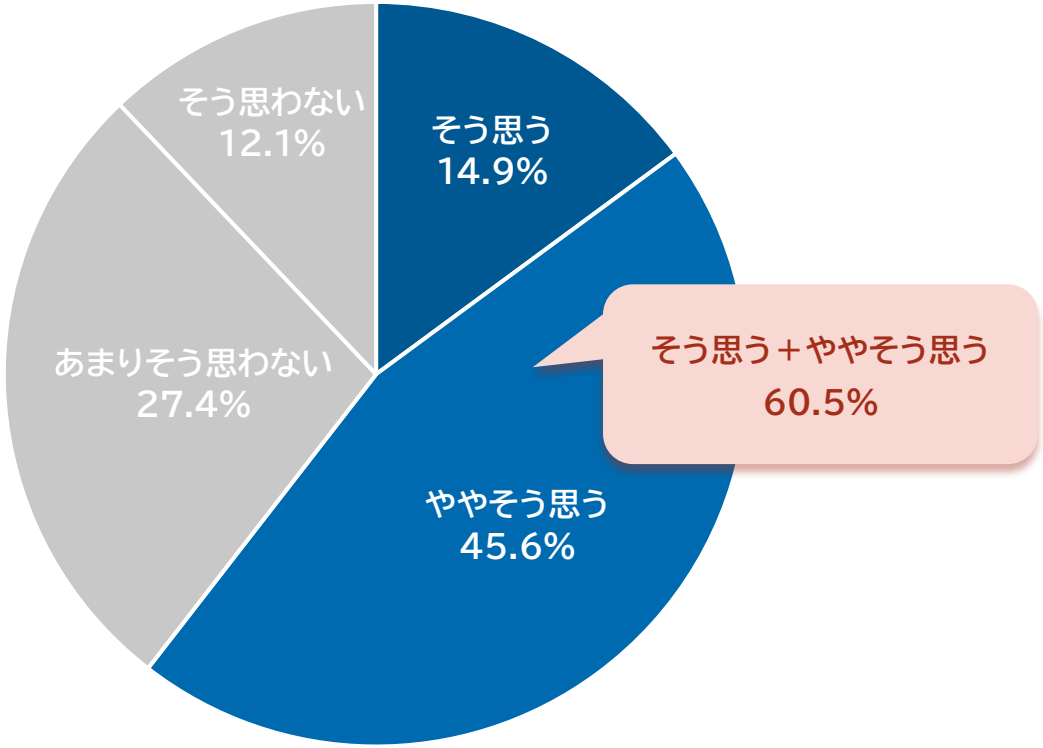
導入前の期待と導入後の成果の上位の項目は変わらないが、インシデント発生時の迅速かつ的確な対応による安心感が導入後の実感として表れる結果となりました。

Q22:MDR・IRサービス選定時の判断要素

- MDRサービスやIRサービス選定において、高い専門性や豊富な実績を持つ提供企業であれば、ある程度の高価格でも選定したいと感じる
（有効回答数：818）



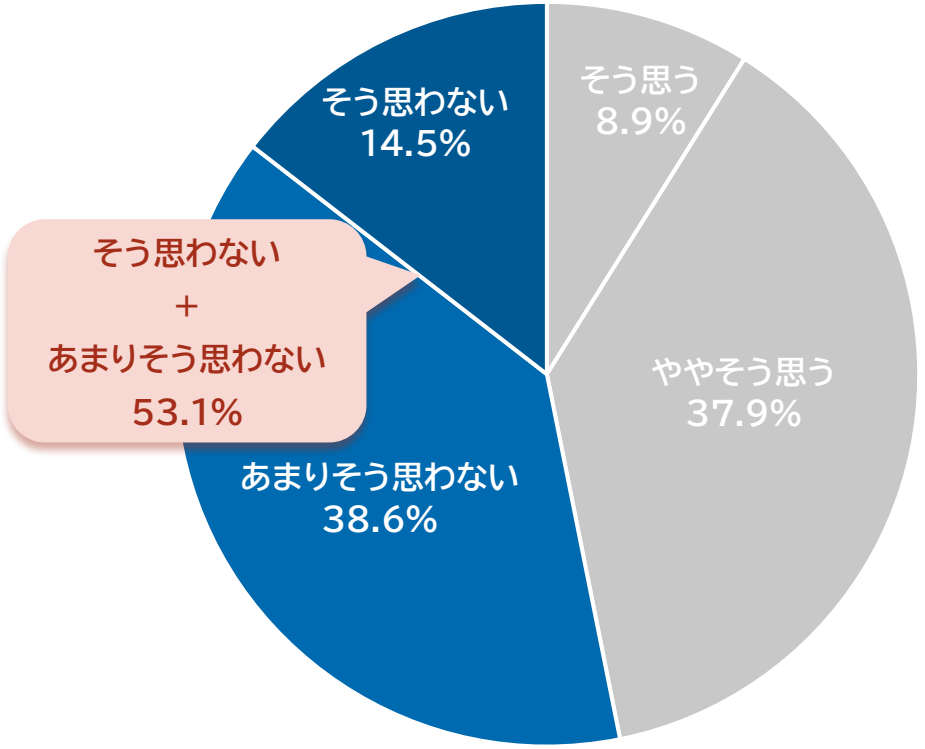
- EPPやEDRの製品とMDRサービスを異なるベンダーが提供している場合、第三者的な視点での監視が可能となり客観性が高まり安心できる
（有効回答数：818）



Q22:MDR・IRサービス選定時の判断要素

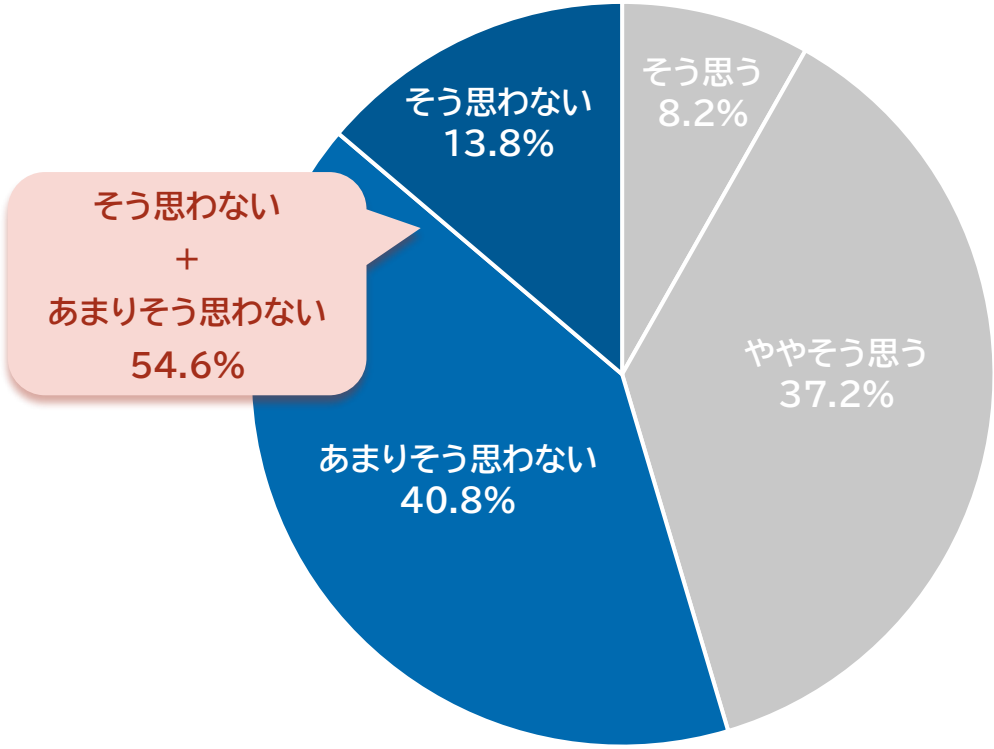
- 信頼のおけるMDRサービスがあれば、追加でIRサービスを導入する必要はないと感じる

（有効回答数：818）



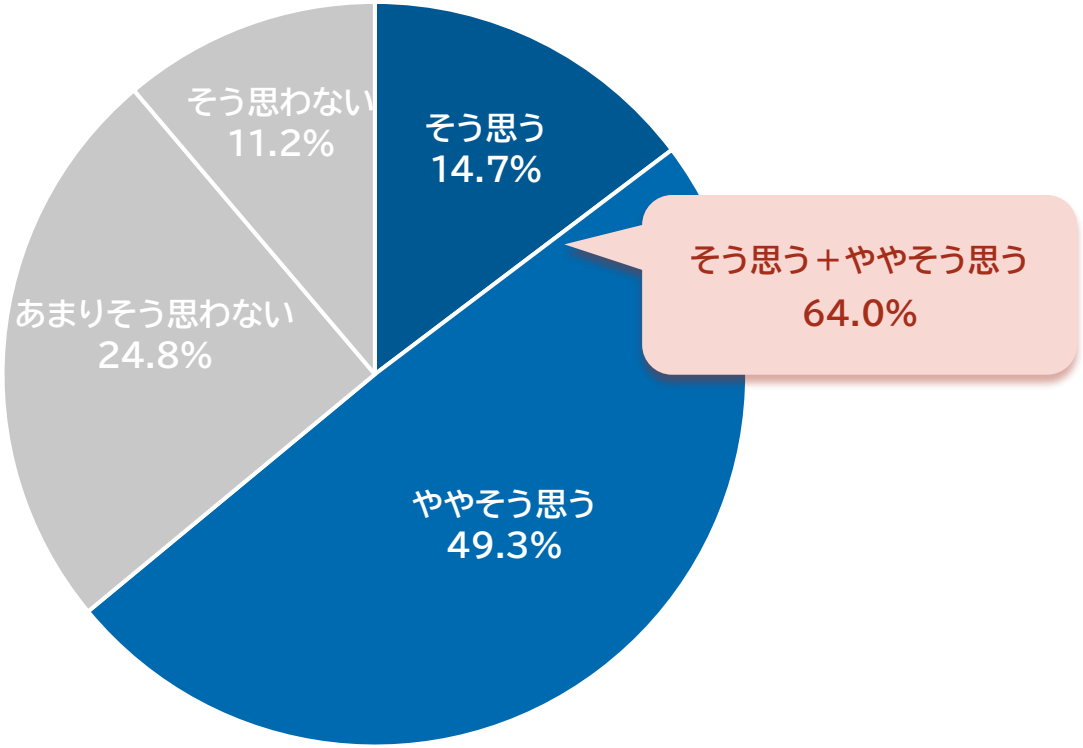
- 信頼のおけるIRサービスがあれば、特にMDRサービスを導入する必要はないと考える

（有効回答数：818）

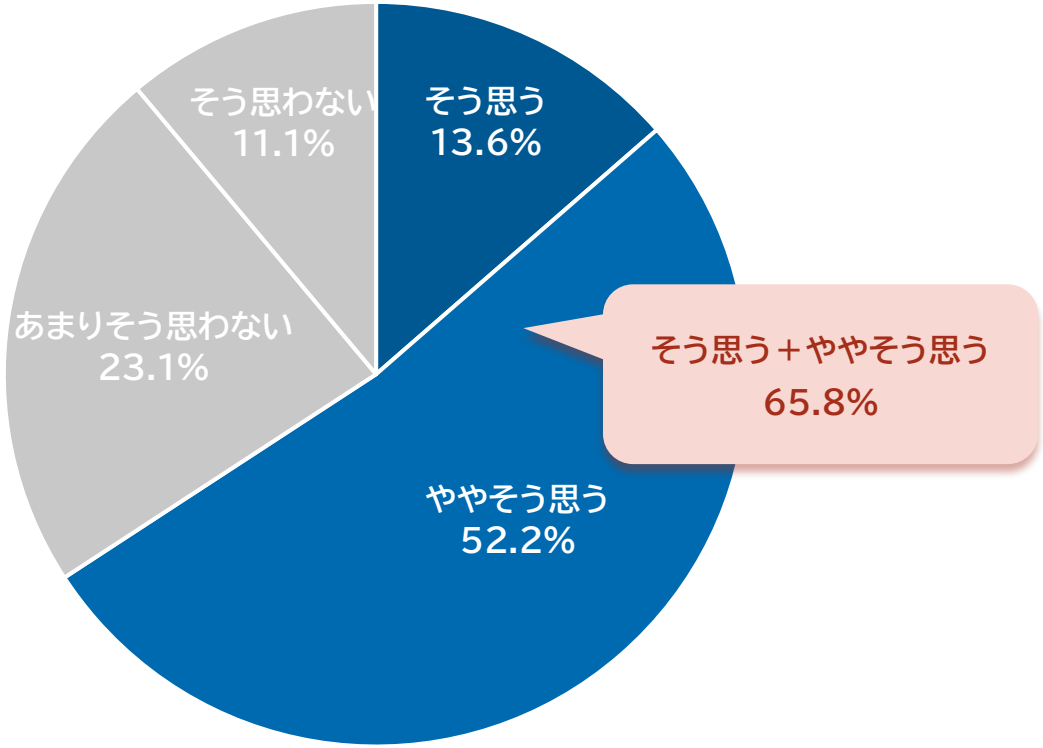


Q22:MDR・IRサービス選定時の判断要素

- MDRサービスとIRサービスを同一ベンダーに統一することで、情報共有が迅速化し、インシデント対応の信頼性が向上すると感じる
（有効回答数：818）



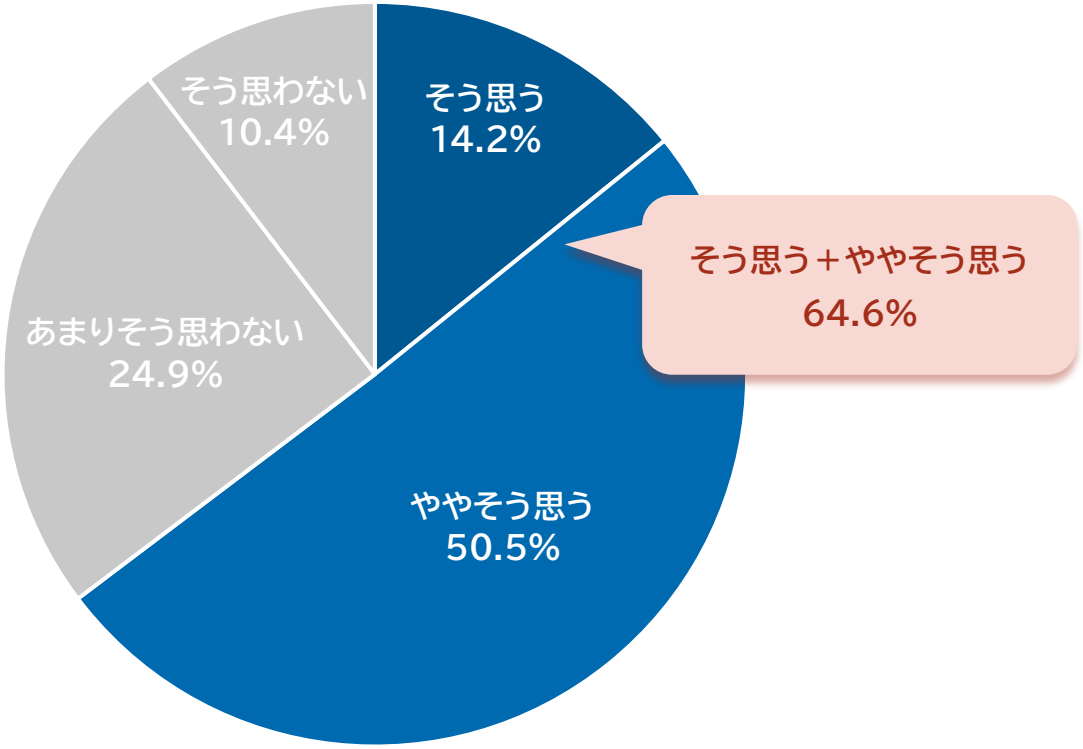
- MDRサービスとIRサービスが同一ベンダーで提供され、専用のSOCルームなどで厳格に管理された環境下で双方作業し、連携・情報共有が行われることで、信頼性が一層高まると思う
（有効回答数：818）



Q22:MDR・IRサービス選定時の判断要素

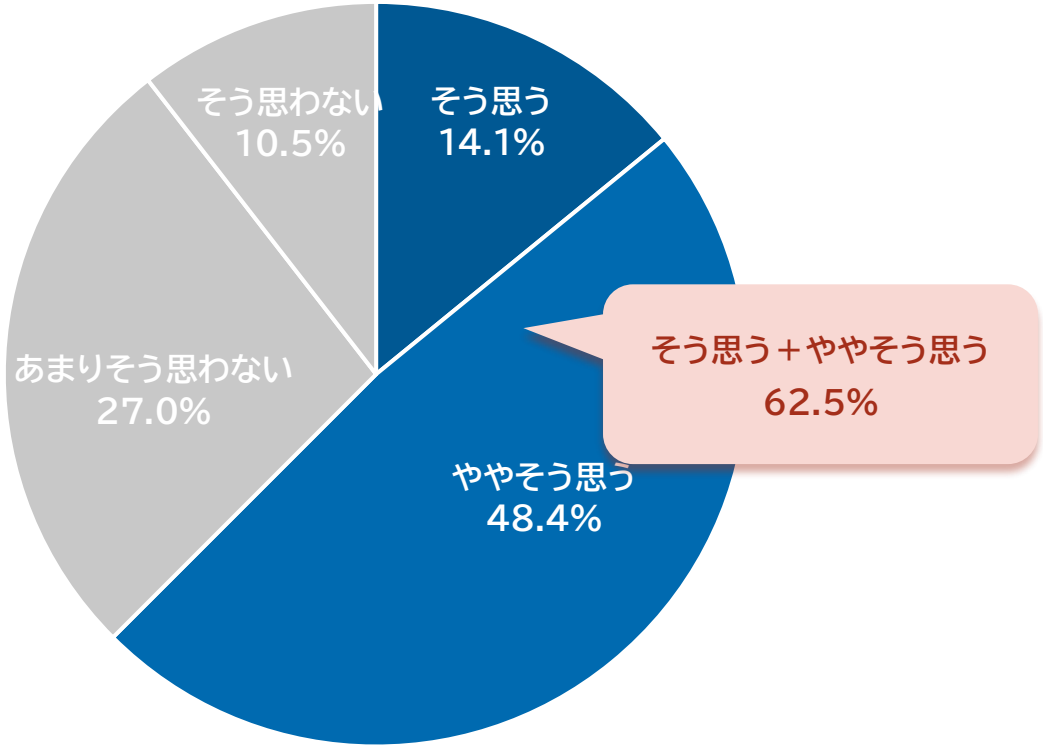
- IRサービスの事前契約があることで、緊急時に即応できる安心感を得られる

（有効回答数：818）



- 平時にもセキュリティ強化メニューを提供するIRサービスは、インシデントが発生しなくても価値があると感じる

（有効回答数：818）



調査結果まとめ

調査結果まとめ

従来のセキュリティ製品で安心しない

アンチウィルス製品，EDR，社外アクセス製品，社内アクセス製品の導入率は、6-8割を占めており、そのうち**約半数以上が課題や不満はない**、と回答しています。しかし、攻撃者はAIや自動化ツールを利用して、より高度で複雑な攻撃を仕掛けてくるなど、**サイバー攻撃は日々進化**しています。また、現代の脅威は非常に迅速に進行するため、**リアルタイムでの脅威検知と対応**が求められます。

このようなことから、**現代の脅威に対応できる環境を整える必要**があります。

インシデント発生後の導入検討では遅い

MDRやIRサービスの導入率は、MDRサービスが21.7%、IRサービスが17.6%と低く、導入のきっかけで一番多かったのは「実際にインシデントが発生したため」、次いで「セキュリティ診断の結果、脆弱性が見つかったため」でした。発生前にインシデントを防げなければ、**システムやデータの被害拡大、顧客などのステークホルダーの信頼喪失、業務中断によるビジネスへの影響など多大な被害**が考えられます。また、その被害の修復、調査、再発防止策の導入など、**多くのリソースやコストが必要**となります。

そうした被害を防ぐためにも、**定期的に自社のセキュリティ状況を診断し、最新の脅威に対応できるツール導入の検討**をおすすめします。

調査結果まとめ

MDRサービス・IRサービス選定のポイント

実際にMDRやIRサービスを導入する際、どのようなポイントをおさえて選定すればよいでしょうか。

まず、調査結果からは、**MDR、IRサービスのいずれか片方だけではなく、両方導入した方が良い**という回答が半数以上、得られました。特に**IRサービスは事前契約をする**ことで緊急時に即時対応できる安心感を感じるとの回答が6割に達しています。また、MDRとIRサービスは同一ベンダーを採用したほうが、**情報共有が迅速化し、インシデント対応の信頼性が向上**するという回答が6割以上となりました。価格的にも、単に安価なものを求めるのではなく、**高い専門性や豊富な実績を持つベンダーを選定**したいという傾向が見られました。

リスク予測から診断、防御、脅威検知、インシデント対応、復旧まで一貫したサービスを提供する

NTTセキュリティ・ジャパン

に、ご相談ください

NTTセキュリティのサービスについて

NTTセキュリティ・ジャパンの製品・サービス一覧

セキュリティコンサルティング・教育・相談

- セキュリティコンサルティング構築

セキュリティリスクアセスメント
組織が日々運用しているセキュリティ対策について、第三者機関が客観的に評価を行います。これにより、現在のセキュリティレベルを可視化し、改善すべき点を明確にすることで、より強固なセキュリティ体制の構築を支援します。

セキュリティポリシー策定支援
組織におけるさまざまな情報セキュリティ対策の指針となる情報セキュリティポリシー文書の作成を支援します。お客さまが作成した文書レビューや改定のアドバイス、または文書ドラフトの作成代行を行います。

セキュリティプランニング
情報セキュリティ対策を、人、技術、物理環境など多角的な視点から評価し、最適な対策を提案するサービスです。

CSIRT構築支援・運用訓練
CSIRTはサイバー攻撃が発生した場合に迅速かつ適切に対応するための専門チームです。貴社の状況に合わせて最適なCSIRTを構築や運用を改善するためのコンサルティングを行います。

- セキュリティ教育

社長向けセキュリティ研修
社長をはじめ企業の経営トップとして、セキュリティに関してどのような意識の持ち方や行動が必要となるか、専門家による講義と実践的な演習を通して学習する機会を提供します。

- 個別相談対応型アドバイザリー

アドバイザリーサポート
お客さまからの情報セキュリティに関する各種お問い合わせに対する受付窓口(リサーチャー)を設置し、助言・情報提供を行います。

セキュリティ管理

- アクセス管理

特権アクセス管理
特権アクセス管理製品の要件定義、設計、導入、設定、試験、プロジェクトマネジメントなどの導入支援を実施します。

- 資産管理

脆弱性見える化ソリューション
組織内のIT資産を網羅的に管理し、脆弱性を自動的に検出、可視化することで、セキュリティレベルの向上を支援します。

セキュリティ監視・検知

- MSS

マネージドセキュリティサービス
アナリストがセキュリティ監視センター(SOC)から、セキュリティ機器の設定や運用、高度なセキュリティ監視を24時間365日行います。

- リスク検知

マネージドUEBA
お客さまのログデータや管理情報を機械学習を用いて統合的に分析し、通常時と異なる不審な行動を検知します。さらに専門アナリストが検知結果を精査することで、高精度な内部リスクの見える化を実現します。

- 情報提供サービス

OSINTモニタリング
公開されている情報を分析して、お客さまシステム環境に関するサイバー脅威を検出時に随時報告するサービスです。

フィッシングモニタリング
お客さまに代わってフィッシングサイトを探索・テイクダウンし、被害を最小限に抑えます。ロゴやドメイン名などを悪用した巧妙な手口にも対応し、お客さまのブランドと顧客を守ります。

NTTセキュリティ・ジャパンの製品・サービス一覧

セキュリティ診断・評価・調査

- 脆弱性診断

脆弱性診断（WEBアプリケーション診断）
専門のセキュリティエンジニアが診断し、知見に基づき評価、結果を報告します。

脆弱性診断（プラットフォーム診断ベーシック）
手軽に脆弱性診断を始めたいお客さま向けのプランです。商用ツールを用いた効率的な診断で、定期的な脆弱性チェックをサポートします。

脆弱性診断（プラットフォーム診断スタンダード）
専門家による詳細な分析と、複数のツールを組み合わせた網羅的な脆弱性診断をご提供します。よりリスクの高い脆弱性を洗い出し、システム全体のセキュリティ強化に貢献します。

セルフ脆弱性診断（Qualys）（Tenable）
お客さま自身で継続的にアセットの脆弱性を把握し、対策を実施するための環境を提供します。

- RedTeam

RedTeam/TLPT
攻撃者の視点からシステムに侵入を試みることで、人・プロセス・テクノロジーの観点から攻撃耐性を評価します。

- 感染端末特定

標的型マルウェア感染端末調査
環境全体の端末上から取得したデータを一括で調査し、マルウェア感染時の特徴的な痕跡を調査することで、環境内のマルウェア感染端末の有無を判断します。フォレンジック的手法を用いたアノーマリ解析により、アンチウィルス/EDRでは見逃す恐れのあるマルウェアの検知を行います。

標的型マルウェア感染プロキシログ調査
プロキシログを分析することで、通信の挙動などから環境内のマルウェア感染端末の有無を判断します。統計的アプローチを用い、未知C2通信の検知も行います。

セキュリティインシデント対応・調査

- インシデント対応・調査

IR共通チケット
インシデント発生時に迅速対応を行うための事前契約サービスです。契約期間中にインシデントが発生しなかった場合も予防・トレーニングに転用可能となっています。

総合インシデントレスポンス
セキュリティインシデント発生時、専門家が迅速に原因究明と再発防止を支援します。 初動調査から詳細解析（フォレンジック、マルウェア解析等）、改善提案まで、お客さまの状況に合わせて最適な対応を提供します。

会社概要

NTT Security

20年にわたり幅広い業種のお客さまを支援しています

2003年のセキュリティオペレーションセンター創設以来自動車や化学、重要インフラなどさまざまな業種のお客さまに伴走し、セキュリティの課題解決を支援してきた実績があります。

状況や課題に応じて最適なセキュリティ対策を提供します

コンサルティングから先進技術ソリューション、マネージドセキュリティサービス(MSS)までワンストップで提供しています。手軽に導入できるツールから、専門家による高度なマネジメントまで幅広いセキュリティ対策のご提案が可能です。

NTTグループのセキュリティ分野を担う専門組織です

NTTグループの研究所が開発した最先端技術を現場で実用化してきた経験を踏まえ、セキュリティの専門家が、OT環境特有の課題に的確に対応します。OTセキュリティとITセキュリティの両領域に精通しているため、相互の環境に与える影響を考慮した対策をご提案します。

会社名	NTTセキュリティ・ジャパン株式会社
本社所在地	東京都千代田区外神田 4-14-1 秋葉原UDX 20F/21F
事業内容	マネージドセキュリティサービス セキュリティプロフェッショナルサービス(コンサルティング) セキュリティ対策提供サービス(機器及び保守)
代表取締役	関根 太郎
株主	NTTセキュリティ・ホールディングス株式会社(100%)

お気軽にお問い合わせください。

NTTセキュリティ・ジャパン株式会社
営業本部ダイレクトセールス＆アライアンス営業部

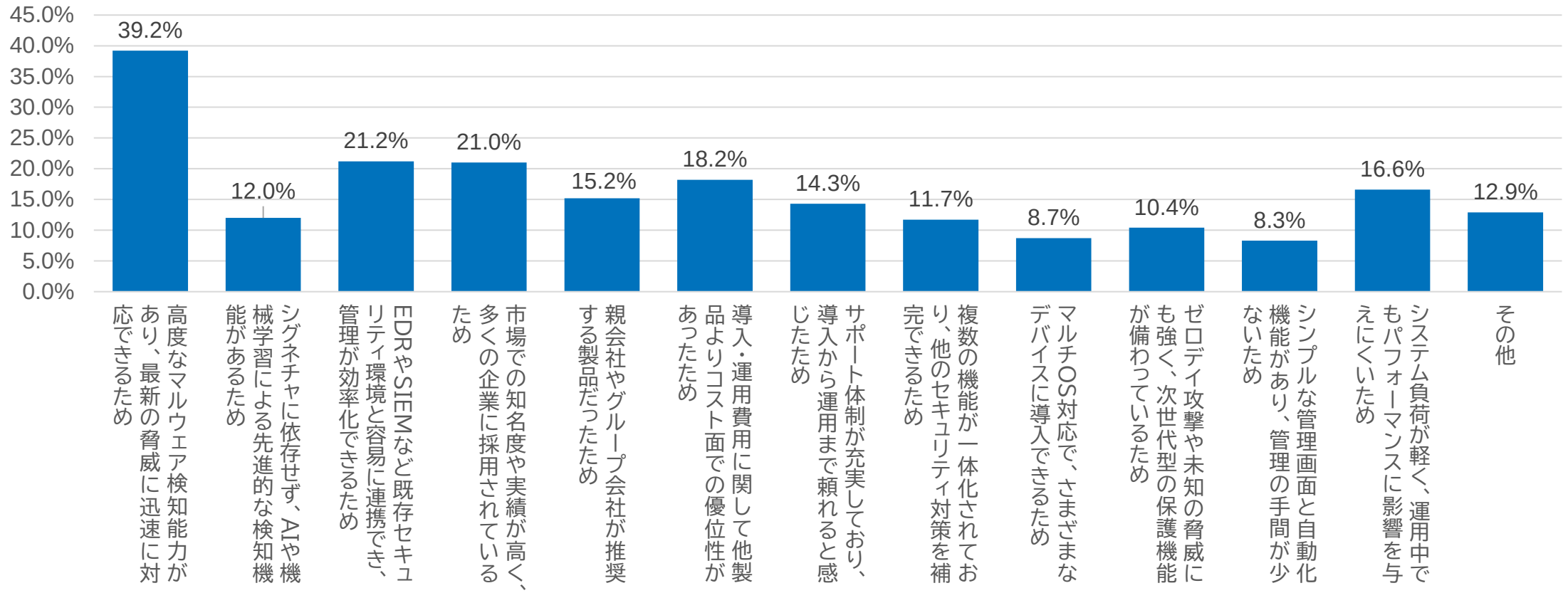
問い合わせフォームへのリンク

調査結果全データ

アンチウィルス製品の選定理由(全回答)

Q.6 アンチウィルス製品を選定した理由を教えてください。

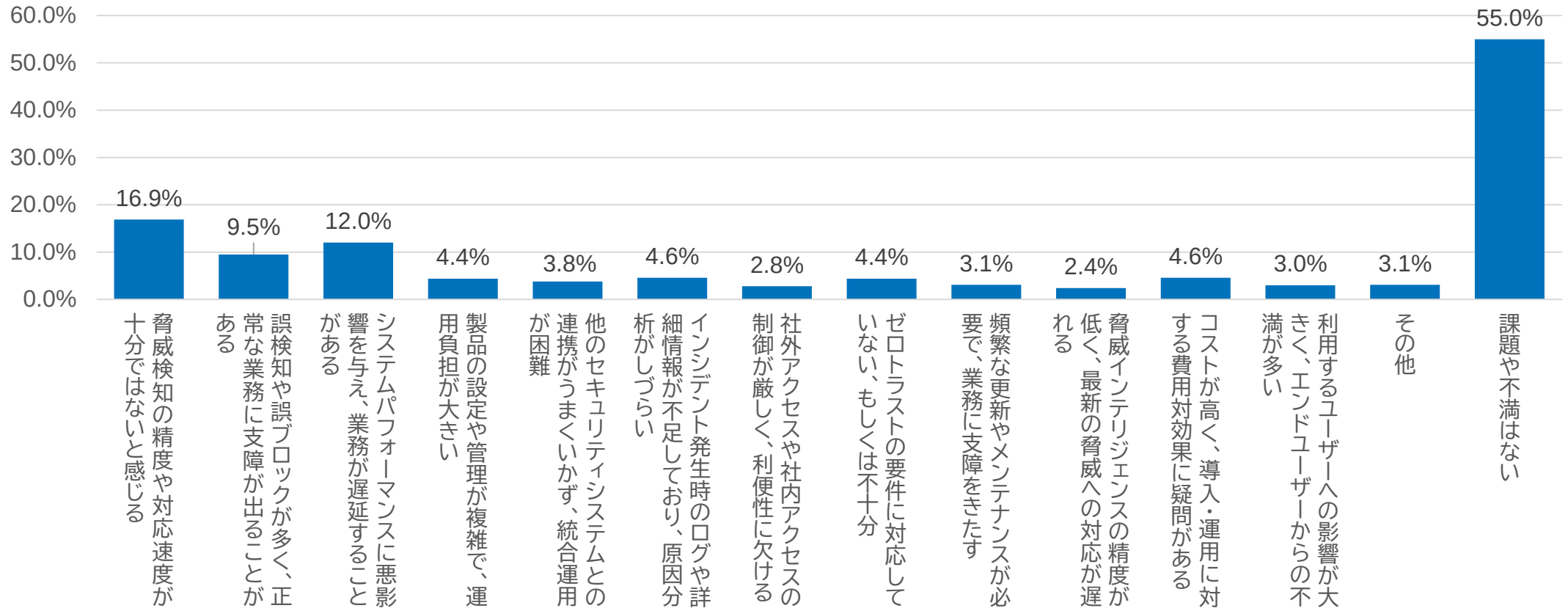
※複数回答可（有効回答数：676）



アンチウィルス製品の導入後の課題(全回答)

Q.7 アンチウィルス製品導入後の課題や不満を教えてください。

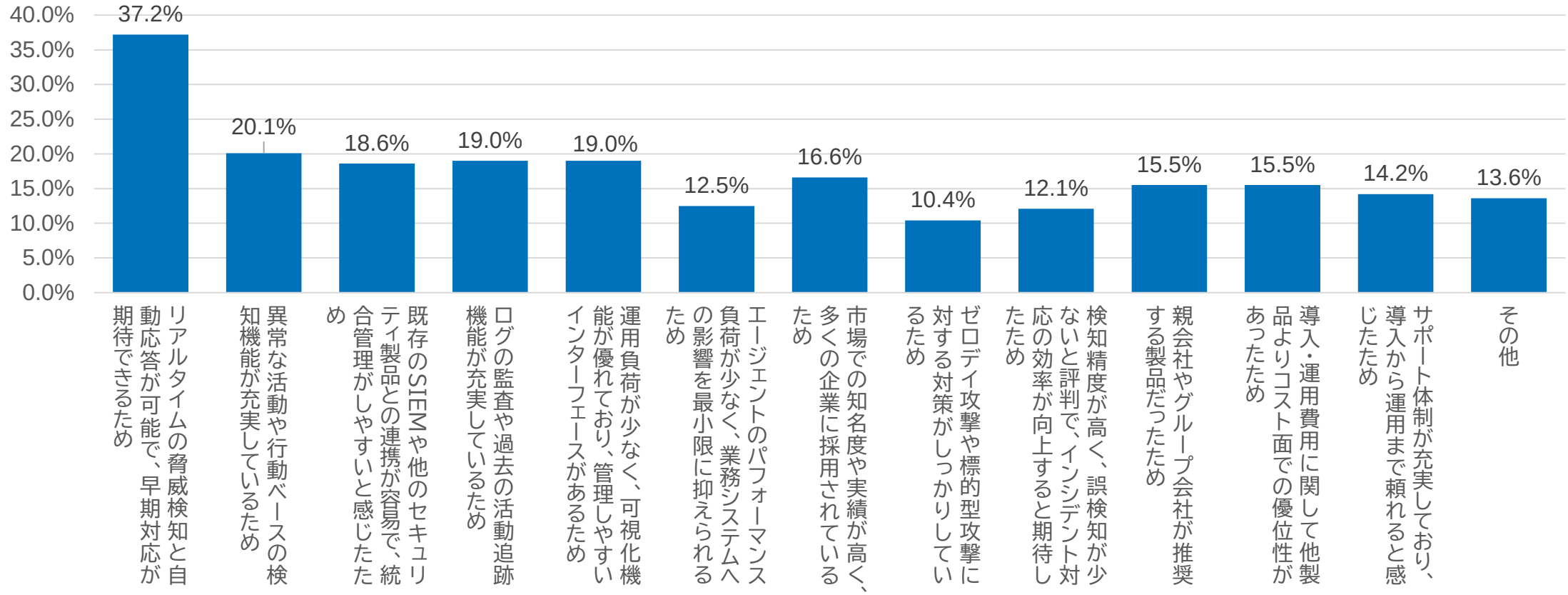
※複数回答可（有効回答数：676）



EDR製品の選定理由（全回答）

Q.8 EDR製品を選定した理由を教えてください。

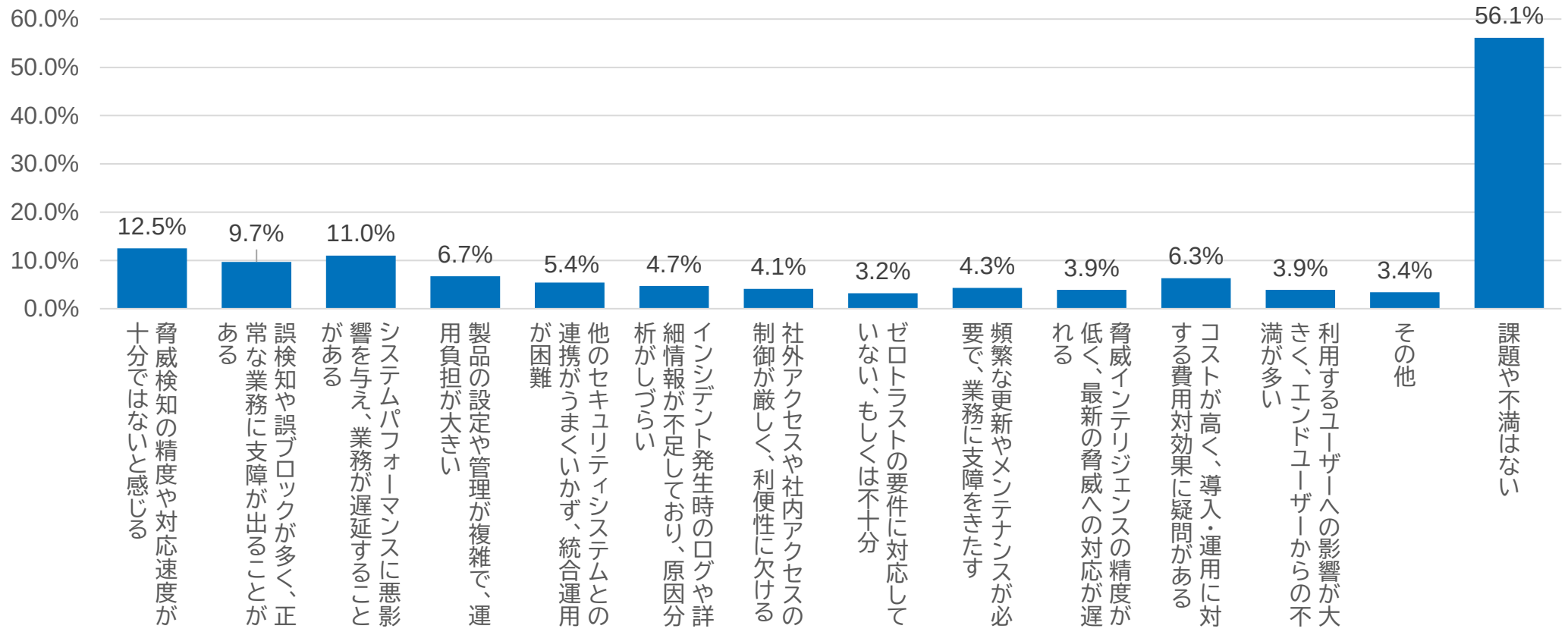
※複数回答可（有効回答数：537）



EDR製品の導入後の課題(全回答)

Q.9 EDR製品導入後の課題や不満を教えてください。

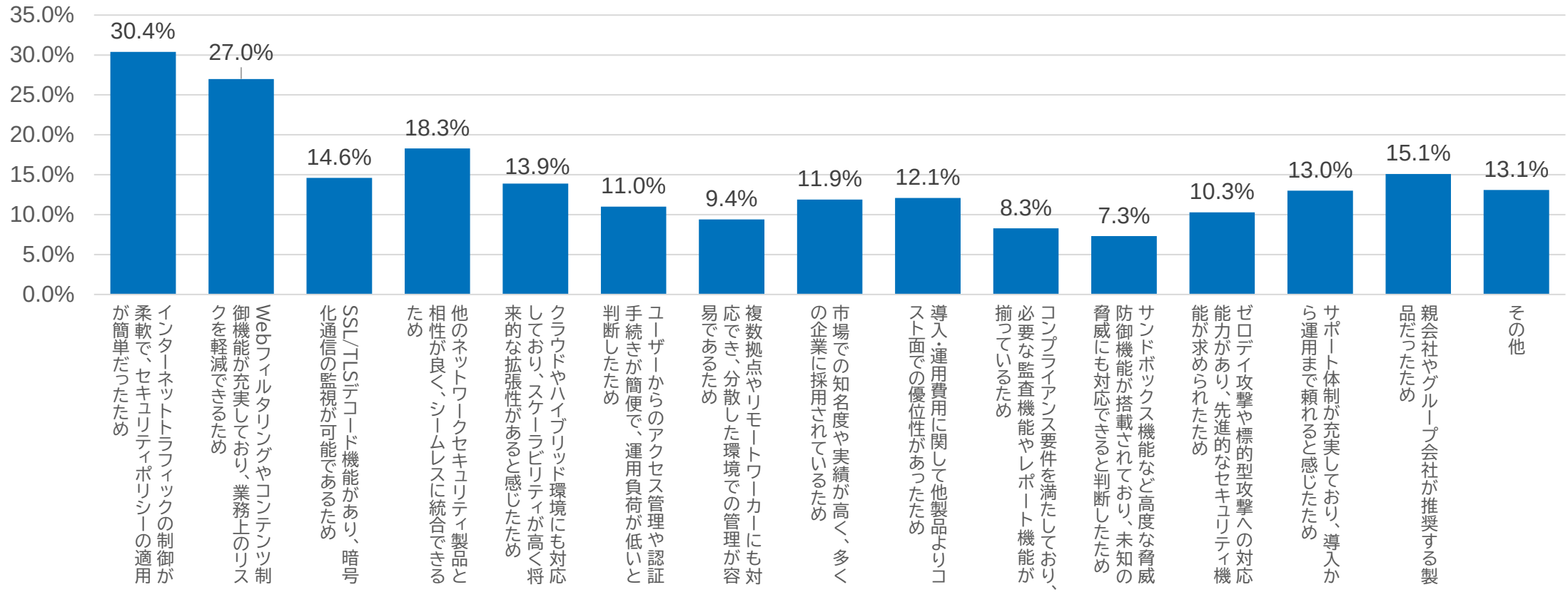
※複数回答可（有効回答数：537）



社外アクセス製品の選定理由(全回答)

Q.10 社外アクセス製品を選定した理由を教えてください。

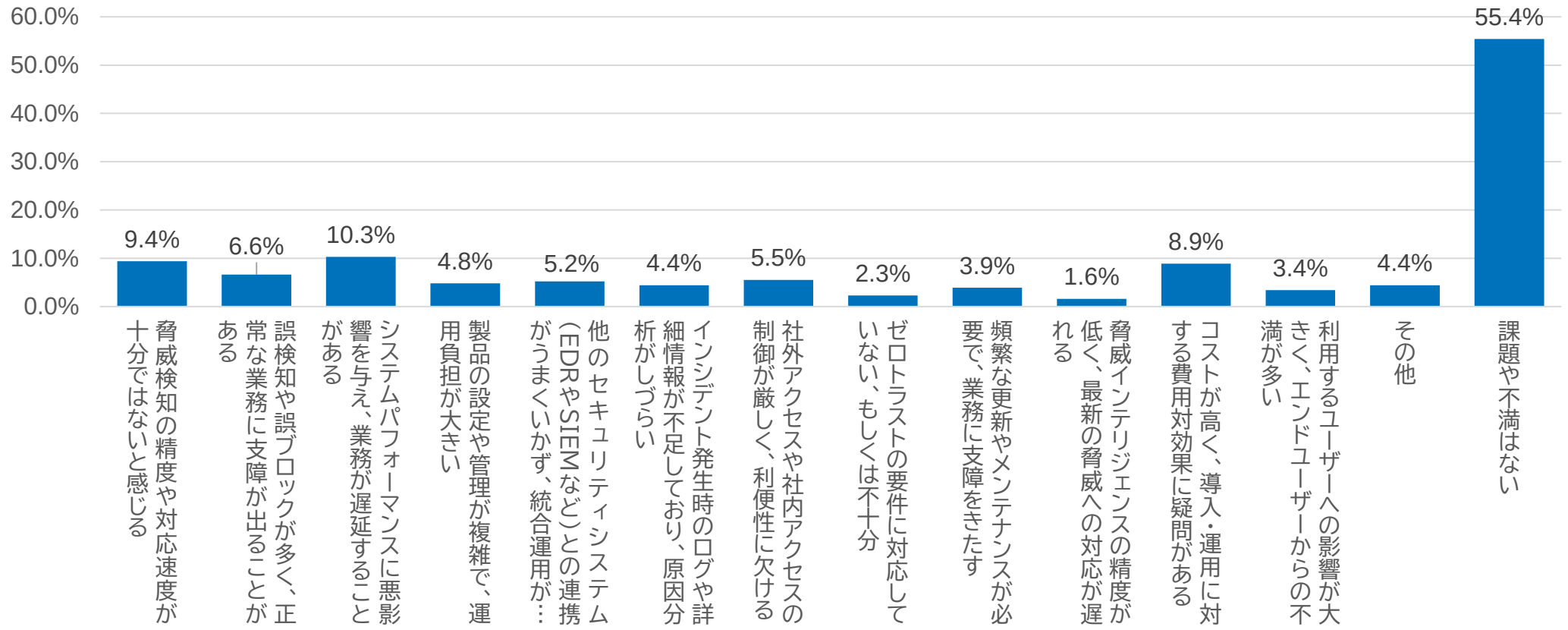
※複数回答可（有効回答数：563）



社外アクセス製品の導入後の課題(全回答)

Q.11 社外アクセス製品導入後の課題や不満を教えてください。

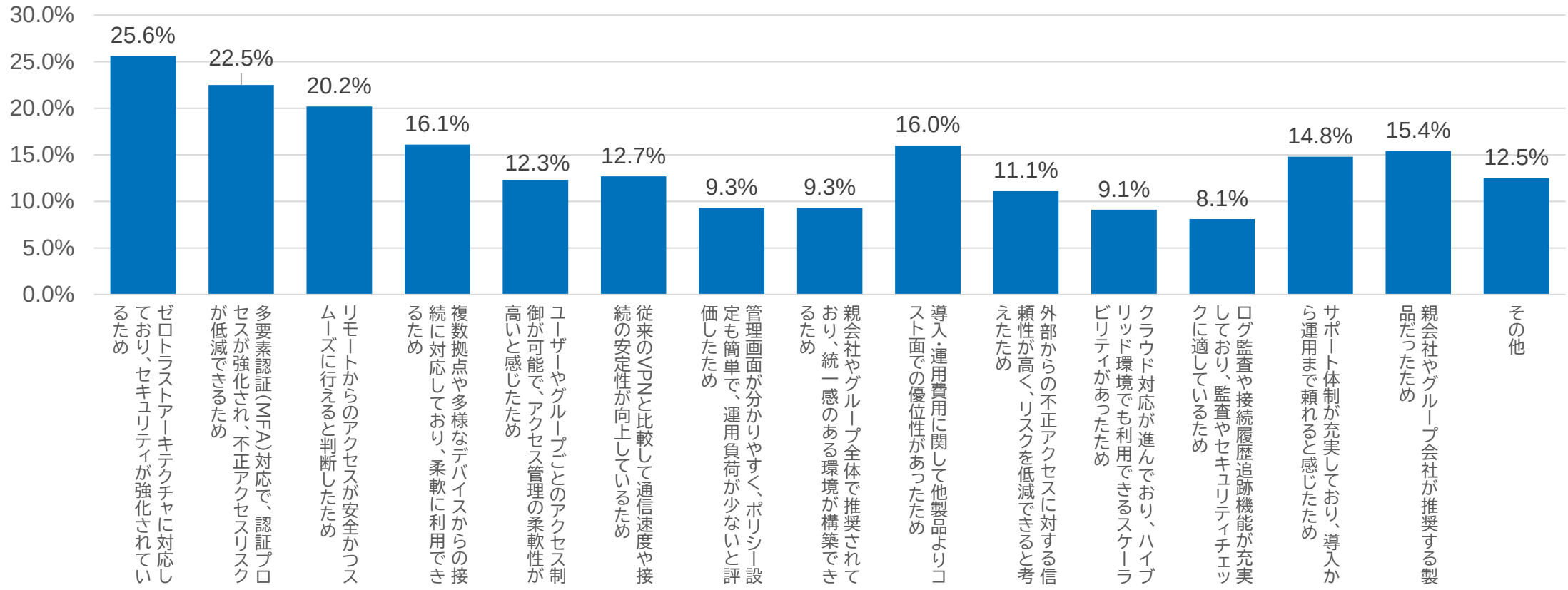
※複数回答可（有効回答数：563）



社内アクセス製品の選定理由(全回答)

Q.12 社内アクセス製品を選定した理由を教えてください。

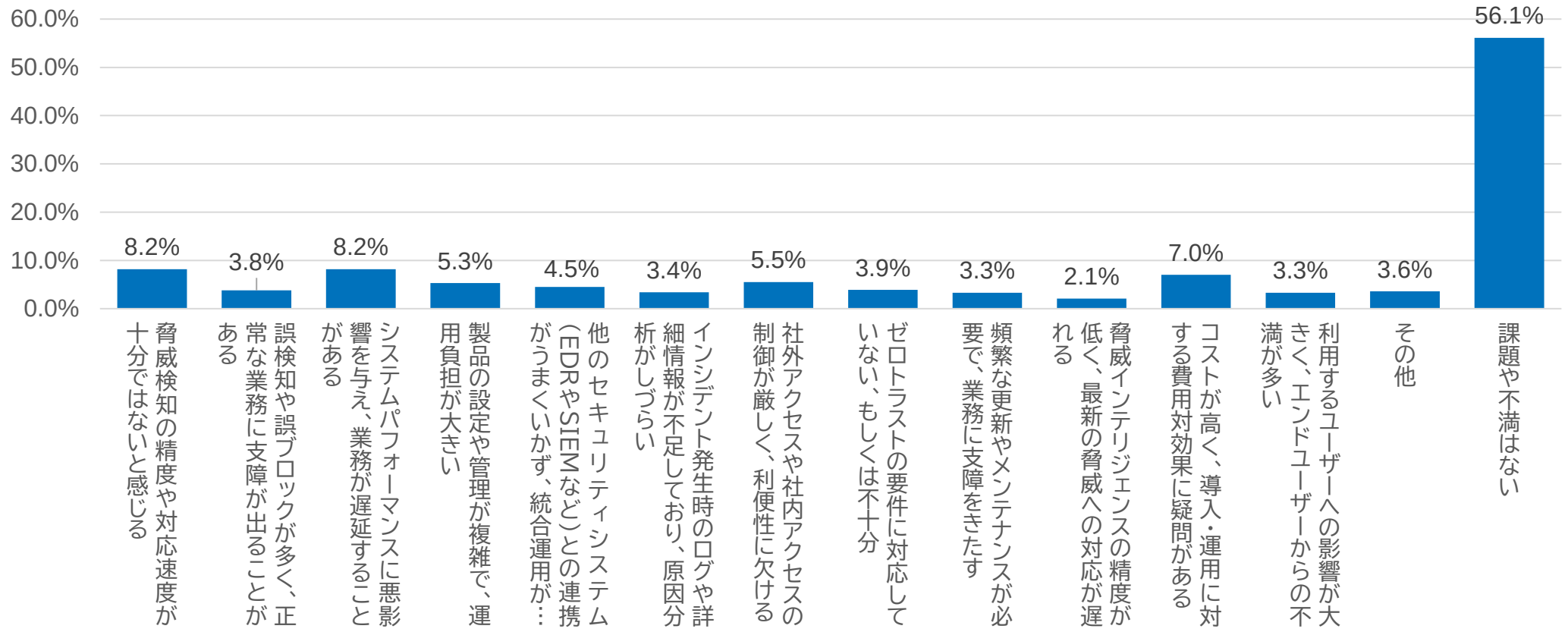
※複数回答可（有効回答数：583）



社内アクセス製品の導入後の課題(全回答)

Q.13 社内アクセス製品導入後の課題や不満を教えてください。

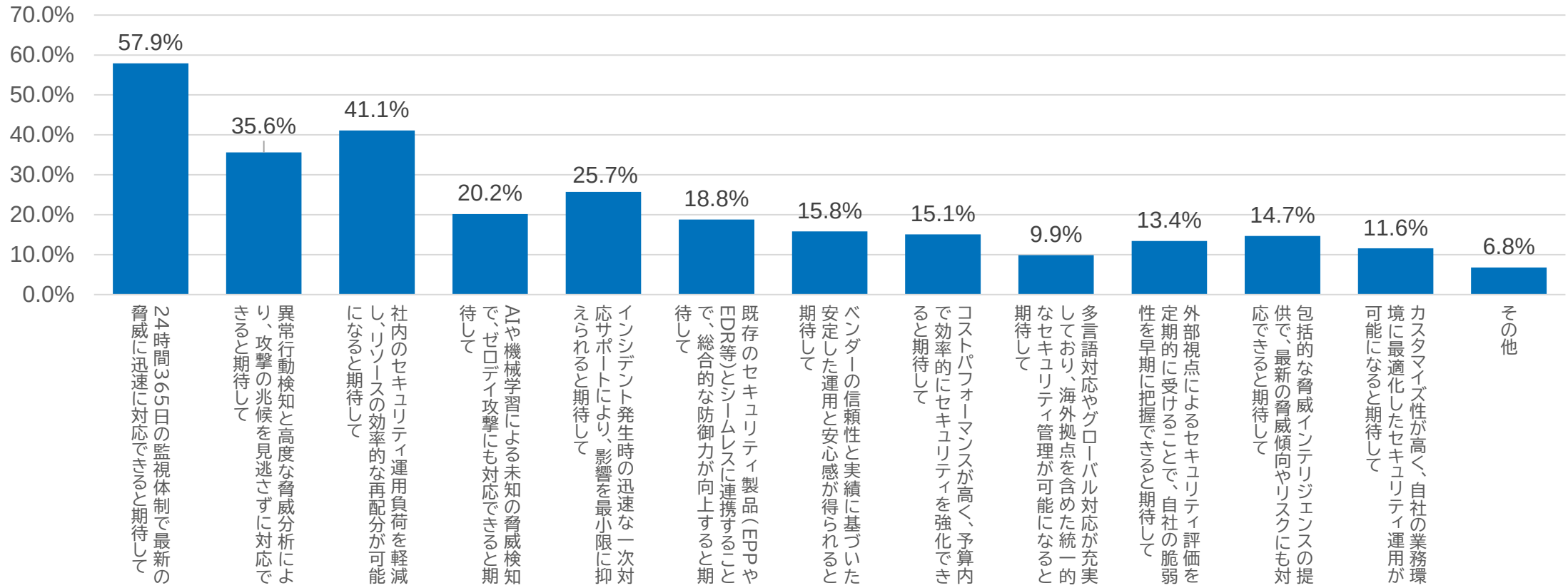
※複数回答可（有効回答数：583）



MDRサービスの選定理由（全回答）

Q.16 導入前に何を期待してMDRサービスを導入しましたか？

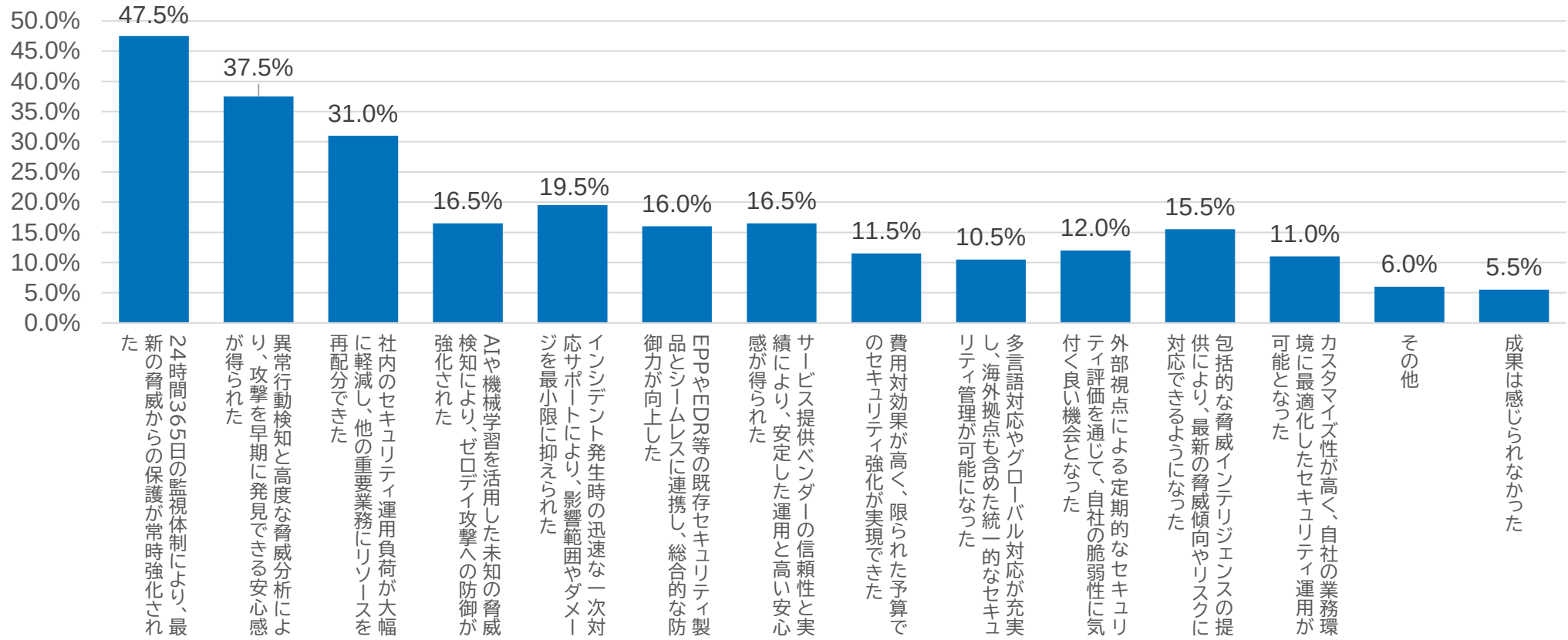
※複数回答可（有効回答数：292）



MDRサービスの導入の成果(全回答)

Q.16 MDRサービスを導入して実際に得られた成果を教えてください。

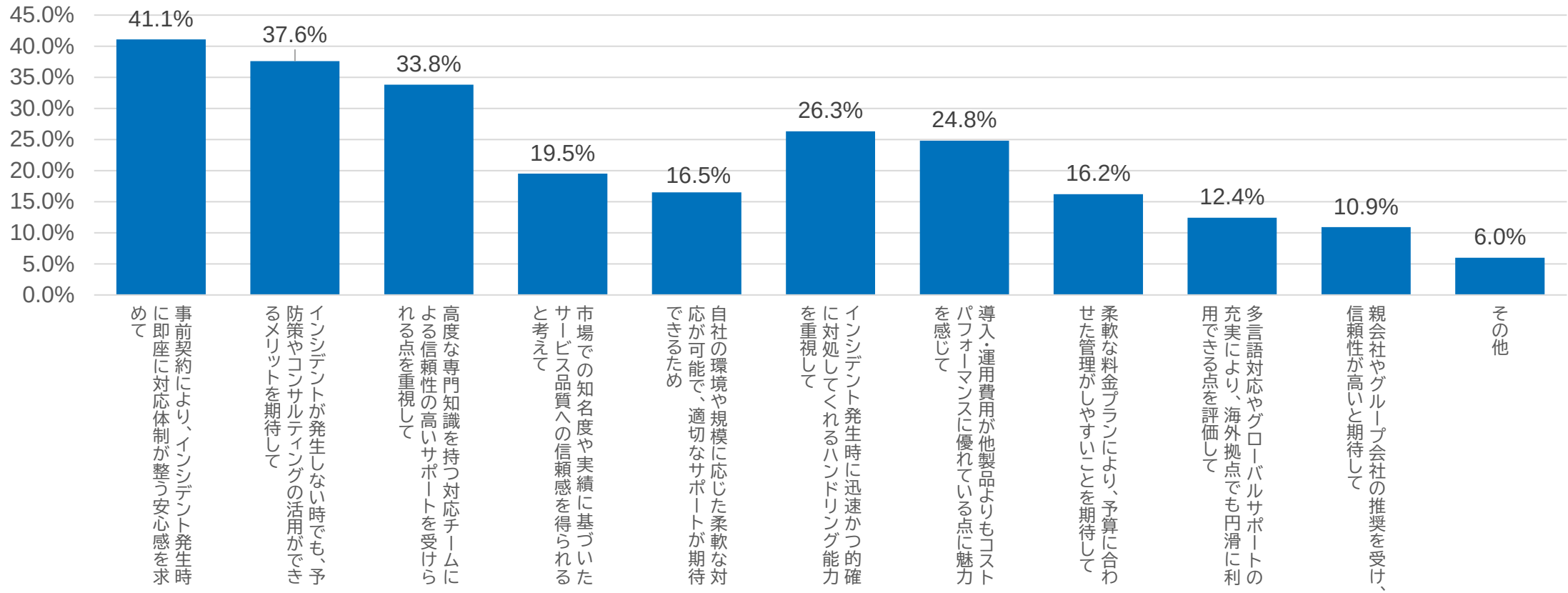
※複数回答可（有効回答数：200）



IRサービスの選定理由(全回答)

Q.20 導入前に何を期待してIRサービスを導入しましたか？

※複数回答可（有効回答数：266）



IRサービスの導入の成果(全回答)

Q.21 IRサービスを導入して実際に得られた成果を教えてください。

※複数回答可（有効回答数:167）