テレワーク導入組織に対する
セキュリティ対策意識調査

2021年6月21日

デジタルアーツ株式会社

調査概要

調査名	テレワーク導入組織に対するセキュリティ対策意識調査
調査目的	新型コロナウイルス感染症拡大に伴い、2020年中にテレワークが急速に普及しました。合わせて、コロナ感染に便乗したサイバー攻撃やシステムの脆弱性を狙った攻撃により組織のインシデントも増加しています。 今回は、国内でテレワークを導入する組織が、2020年中に経験したセキュリティインシデント発生要因及びセキュリティ対策の実施状況について調査しました。 これにより、テレワーク導入組織の今後の継続意向とセキュリティ対策に関する今後の課題について考察してまいりたいと考えています。
調査方法	インターネット調査
調査対象	民間企業及び官公庁におけるITシステム・情報セキュリティ担当者（1,065名） ※自組織のインシデント状況を把握し情報セキュリティ対策の意思決定に関わる ※2020年1月～12月に何らかのインシデントが発生した組織に限る
調査期間	2021年4月16日（金）～4月21日（水）
調査機関	株式会社クロス・マーケティング

調査結果概要

■**今回の回答者（組織のIT・情報セキュリティ担当者1,065名）全員が、自組織はテレワーク導入継続の意思があると回答。**
継続しないと回答した組織は0であった。

■これらの組織が**2020年に経験した****セキュリティインシデント全3,334件のうち、2,782件/83.4%が、Webとメールに起因するもの**であった。

■インシデントを経験した組織の多くは、セキュリティ対策についても重要視しているとしながら、**セキュリティ対策を経営会議で決定している組織は全体で54.6%**であった。
・CSIRT等インシデント対応専門チームが概ね機能していると回答した組織は81.5%。
・インシデントが発生した際のリスク管理体制が整備されている組織は87.9%。

■ゼロトラストモデルに基づく**セキュリティ対策を重視する組織は**76.5%。
・Secure Web Gatewayを検討中の組織が45.2%、42.7%は導入済みであった。
・SASE（Secure Access Service　Edge）を検討中の組織が51.0%、21.6%は導入済みであった。

■**テレワーク下のセキュリティ対策で重視する領域の上位は、端末/サーバ環境/従業員のセキュリティ教育やルール作り**などであった。
・エンドポイント対策として重視する領域は、**アンチウイルス/個人情報（ファイル）/電子メール**などであった。

エグゼクティブサマリー

インシデント要因の8割以上がWebアクセスとメールに起因
端末対策やリスク対応など出口対策・内部対策を重視する傾向
テレワーク導入組織はインシデントを経験しつつもテレワーク継続意向は100%
テレワーク恒久化に向け、攻撃手法に合わせた入り口対策が改めて重要に

今回の調査では、テレワークを導入している組織が2020年に経験したインシデントの8割以上が、Webアクセスとメールに起因しており、組織規模に関わらずインシデントに遭遇しているということがわかりました。

これらの組織はセキュリティ対策を重要課題と位置付けており、ゼロトラストなど従来の境界型に依存しないセキュリティモデルの対策も重視しています。但し、情報セキュリティを「経営課題」とまで認識している組織は全体の半数に留まっています。また、対策の中身を見ると、端末のウイルス対策、セキュリティルール構築や従業員のセキュリティ教育などの優先度が高いようです。

攻撃の要因がWebアクセスやメールがほとんどであるのに、これらの対策よりも端末や人的資源の対策が優先される理由は、サイバー攻撃が巧妙化したことで入り口対策が困難とされ、侵入された際の内部の対策や出口対策が重視されるようになったためと考えられます。しかし、今回判明したように、侵入の経路は依然としてWebアクセスとメールがほとんどです。テレワークにより社内と社外との境界は開かれているため、侵入経路の入り口でしっかりと攻撃をせき止められるかどうかが非常に重要になってきます。

テレワーク導入組織では、セキュリティ脅威は認識しつつも、テレワークに対して前向きに捉えて実施継続していく方向であることが伺えました。テレワーク需要は今後も拡大していきます。
この際のセキュリティ対策には、攻撃の手法に合わせた入り口対策をすることが改めて必要となります。

インデックス

①回答者の属性（P6-9）

②テレワーク継続意向と環境（P10-14）

③インシデント要因とリスク管理体制（P15-18）

④従業員規模別ゼロトラスト/SecureWebGateway/SASEの
導入方針（P19-22）

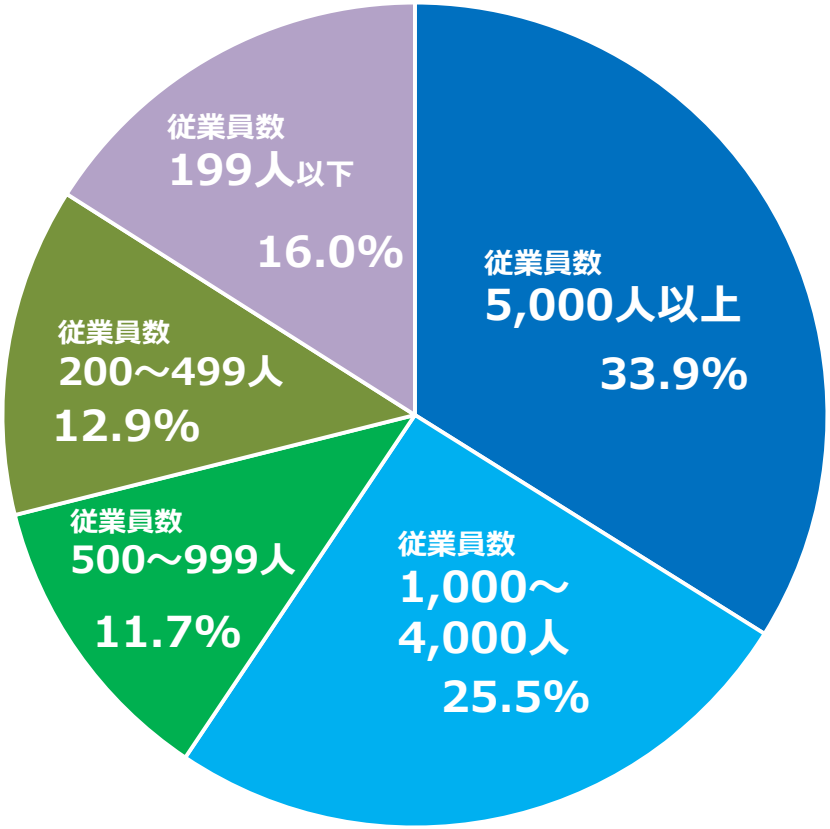
⑤テレワークにおけるセキュリティ対策の優先度と満足度（P23-25）

⑥テレワークにおけるエンドポイント対策の優先度と満足度（P26-28）

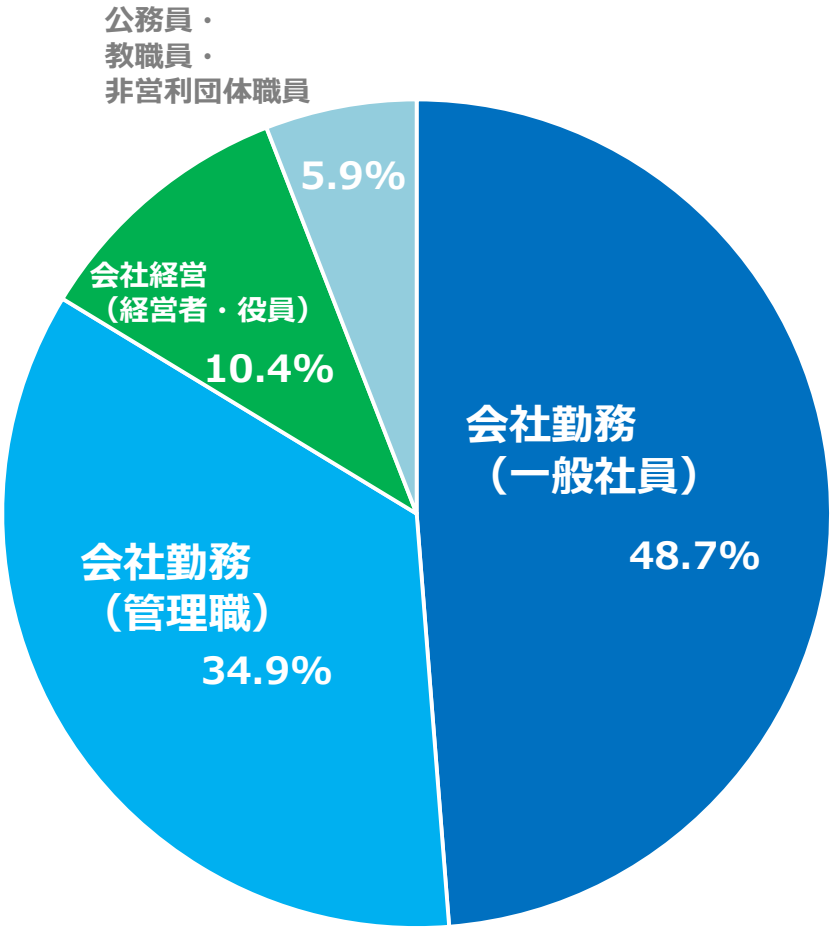
①回答者の属性

組織の従業員規模/職業

Q. あなたの組織の従業員規模をお知らせください。



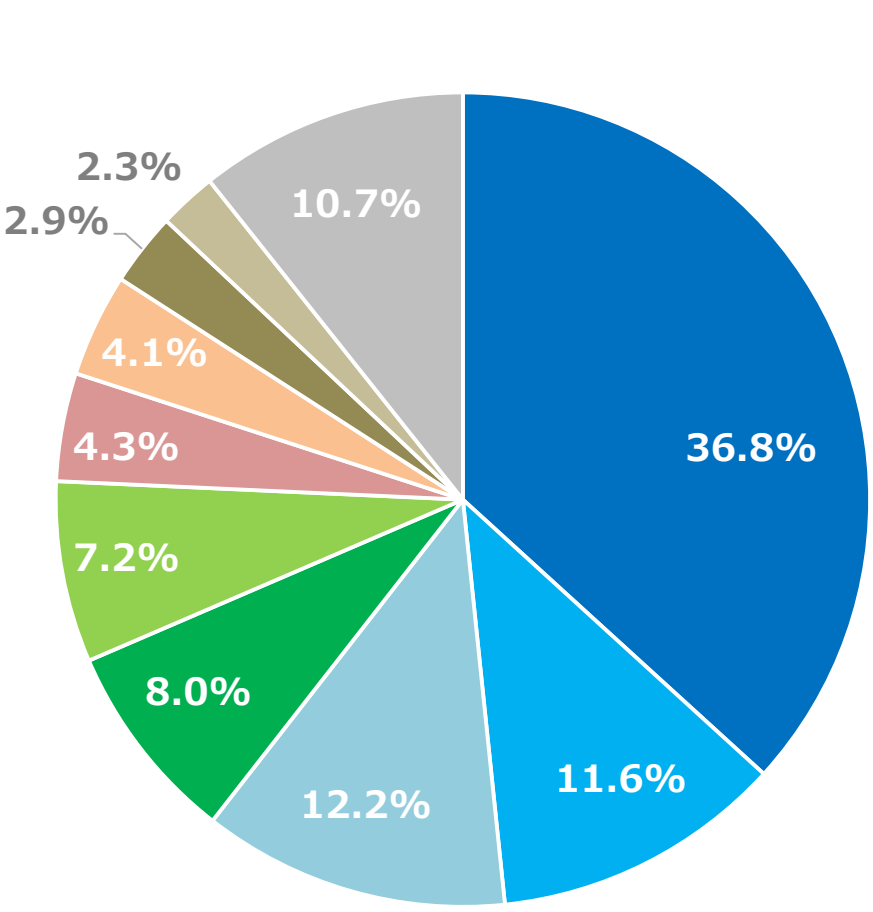
Q. あなたが現在従事している業務部門を
以下の中からお選びください。



N＝1,065人

業種

Q. あなたの勤務先の業種をお知らせください。

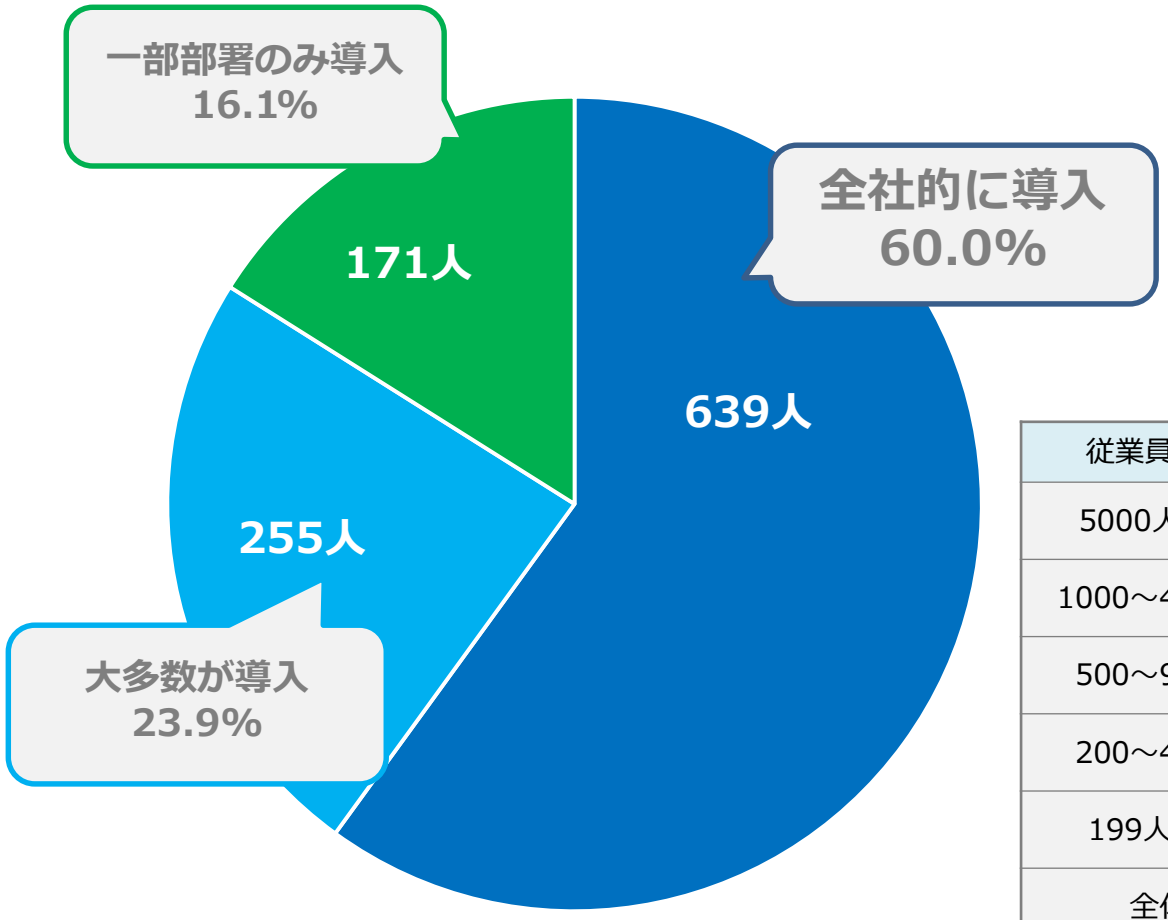


- 情報通信
- 金融・保険
- 家電・ＡＶ機器・精密機器
- 自動車・輸送機器
- 不動産
- 鉄鋼・非鉄金属・金属・硝子・窯業・土石
- 医薬品・化粧品・日用品
- 電気・ガス・熱供給・水道
- 飲料・食品・食品加工
- その他

N＝1,065人

テレワークの導入状況

Q. あなたの組織ではテレワークを導入または導入を検討していますか。



従業員規模	全社的に導入	大多数導入	一部部署のみ
5000人以上	71.75%	18.56%	9.70%
1000～4999人	55.15%	30.88%	13.97%
500～999人	56.00%	26.40%	17.60%
200～499人	53.28%	26.28%	20.44%
199人以下	51.18%	20.59%	28.24%
全体	60.00%	23.94%	16.06%

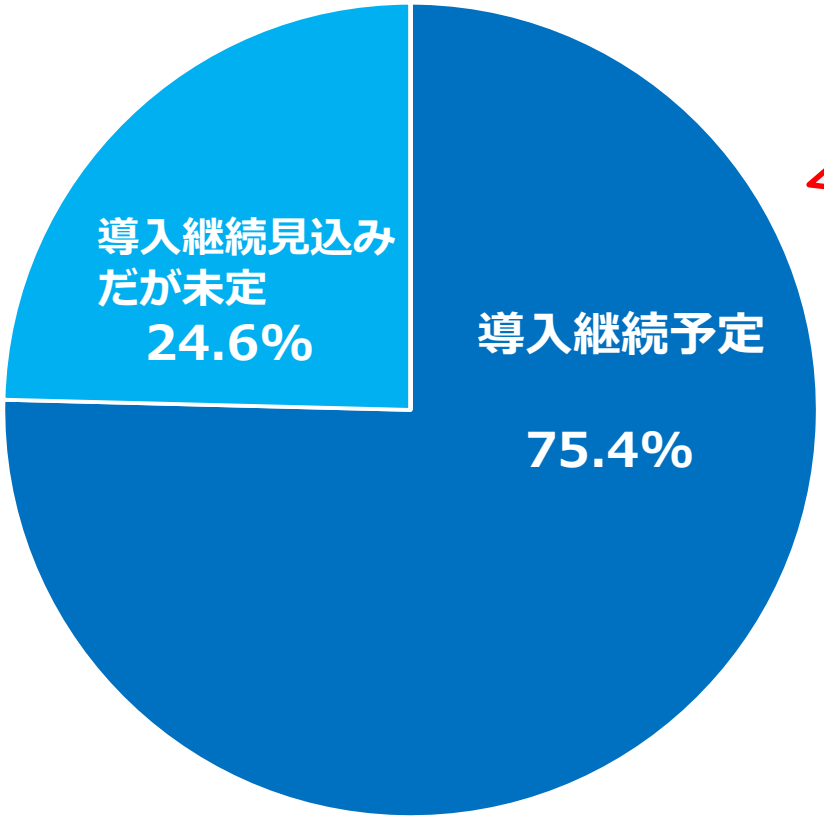
N＝1,065人

②テレワーク継続意向と環境

テレワークの導入継続意向

■**テレワークを導入する組織全てが、今後の継続を見込んでいる**
継続しないと回答した組織は0

Q. あなたの組織では継続的にテレワークを導入する予定ですか。



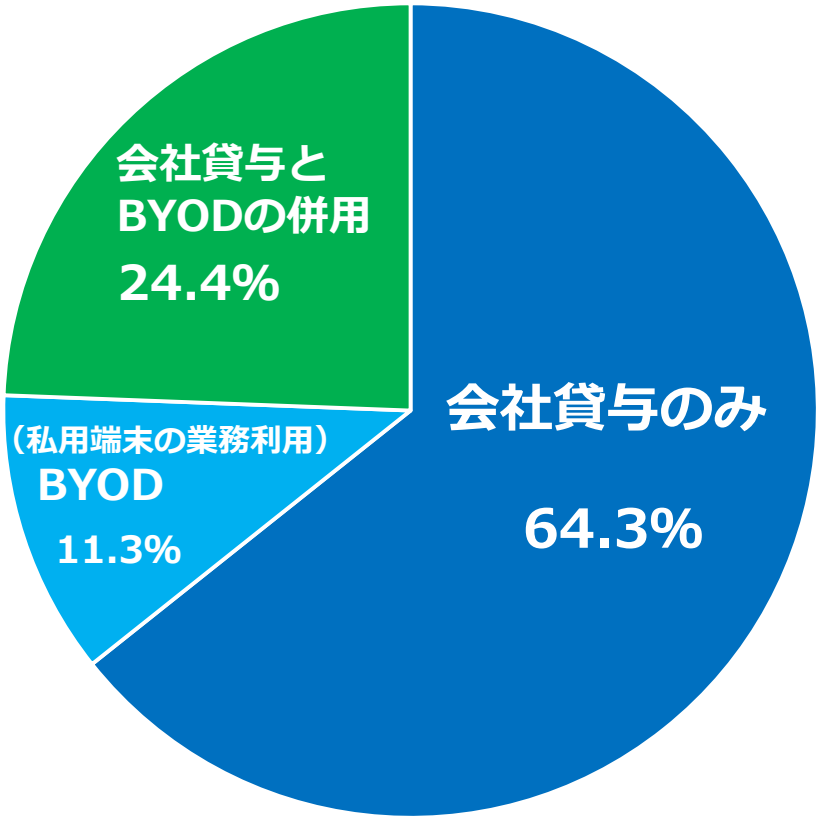
導入しない予定とした組織は
0%

N＝1,065人

テレワーク環境＜端末＞

■テレワークで使用する端末は会社貸与のみとする組織が64.3%
BYODを取り入れている組織は35.7%（会社貸与との併用も含む）

Q. テレワーク時に社員が使用するＰＣや携帯電話・スマートフォン等の端末は、どのように取り扱っていますか。

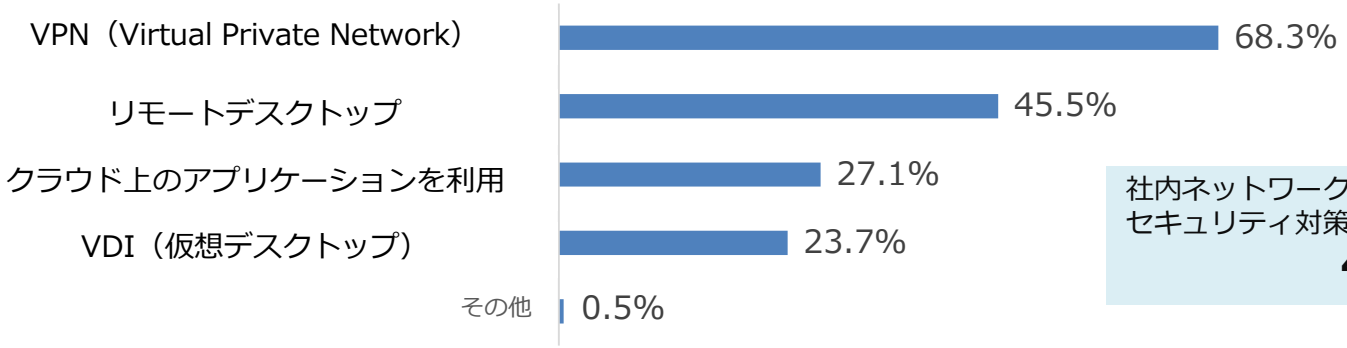


N＝1,065人

テレワーク環境＜社内ネットワーク/社内ファイルサーバー＞

社内ネットワーク

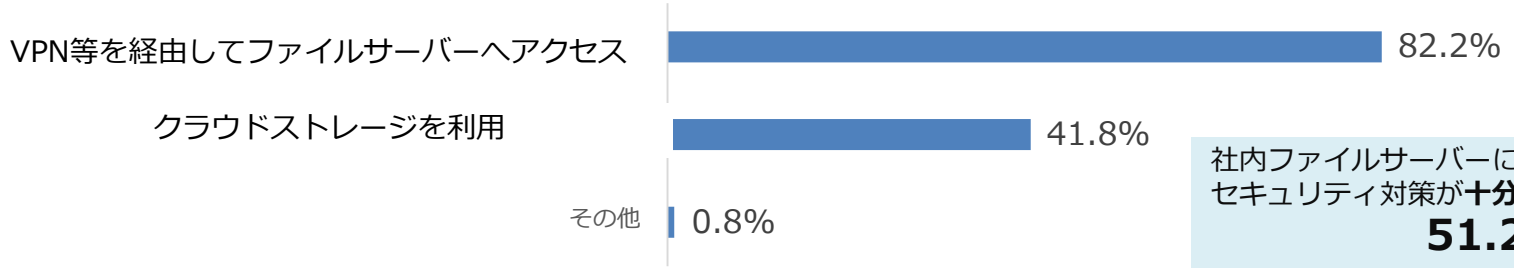
Q. テレワーク時の社内ネットワークへの接続はどのように行っていますか。（複数回答可）
また、セキュリティ対策は十分だと感じていますか。



社内ネットワークに対する
セキュリティ対策が**十分である**と考える割合
48.8%

社内ファイルサーバー

Q. テレワーク時の社内ファイルサーバーへの接続はどのように行っていますか。（複数回答可）
また、セキュリティ対策は十分だと感じていますか。

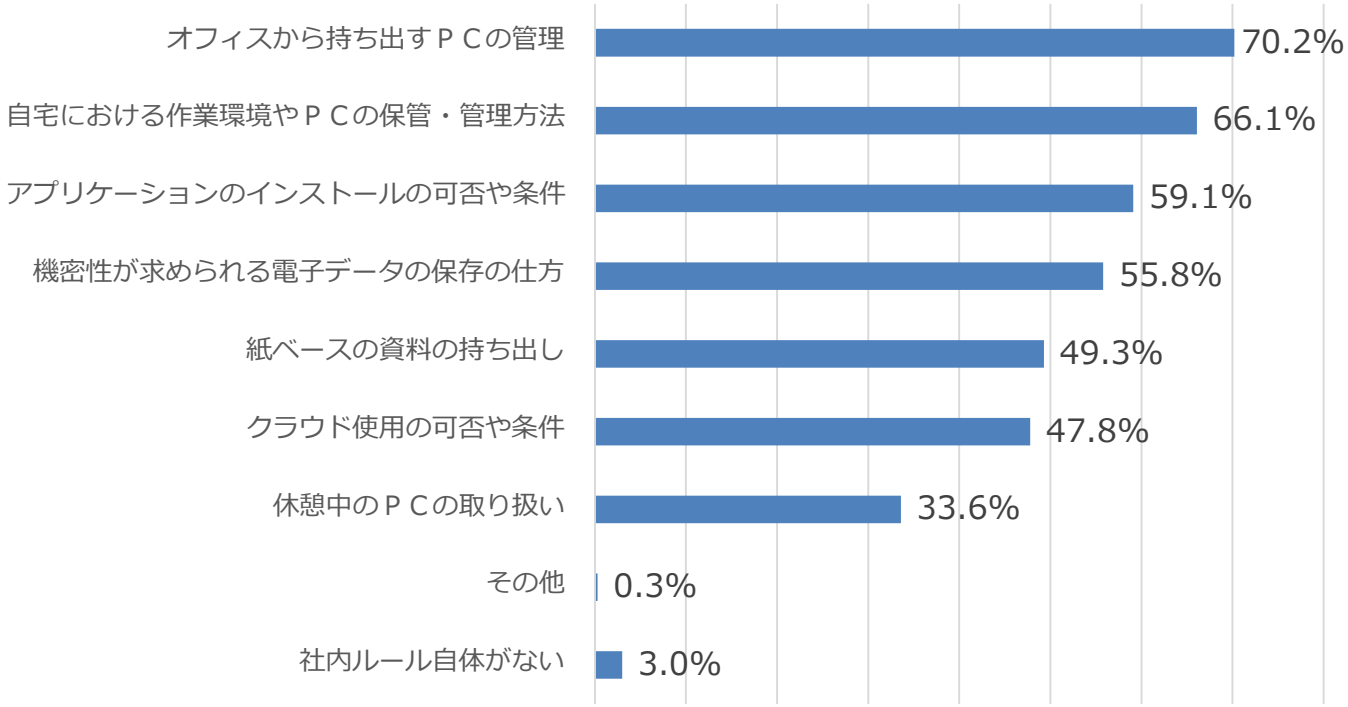


社内ファイルサーバーに対する
セキュリティ対策が**十分である**と考える割合
51.2%

N＝1,065人

テレワーク環境＜社内ルール＞

Q. テレワーク時の社内ルールはどのような項目を規定していますか。（複数回答可）



Q. その社内ルールは徹底されていますか。

N＝1,065人

③インシデント要因とリスク管理体制

2020年中に遭遇したインシデントランキング

Webアクセスとメールに起因するインシデントが8割以上

Q. あなたの組織ではどのようなセキュリティインシデント（以下インシデントとする）が発生しましたか。（複数回答可）。

セキュリティインシデント内訳			
フィッシングメールの受信	**695件**	**ビジネスメール詐欺のメール受信**	**534件**
不正サイトへのアクセス	**395件**	**メール誤送信など意図しない情報漏洩**	**380件**
標的型攻撃	**345件**	**ランサムウェア感染**	**309件**
サービス妨害（Dos/DDos）攻撃	179件	内部不正による情報漏洩（職員の情報持ち出し等）	177件
Emotet等マルウェア感染	**124件**	サプライチェーンの弱点を悪用した攻撃	98件
自社サイトの改ざん	81件	その他	17件

Webアクセスとメールに起因するインシデント件数 **2,782件（83.4%※）**

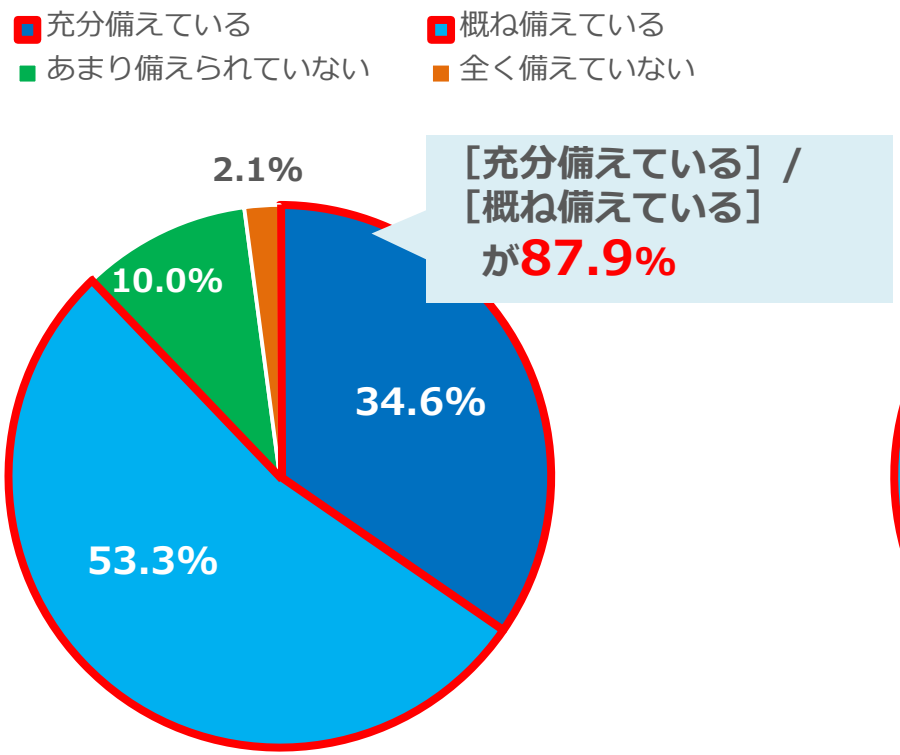
全体のインシデント件数　**3,334件**

※回答者1,065名に対し、2020年に組織内で発生したインシデントを複数回答可で尋ねたところ、全体の回答数が3,334件であった。
このうち、不正メールの受信・不正サイトへのアクセスに起因するインシデントの件数が合計で2,782件、全体の回答数のうち83.4%にあたる。

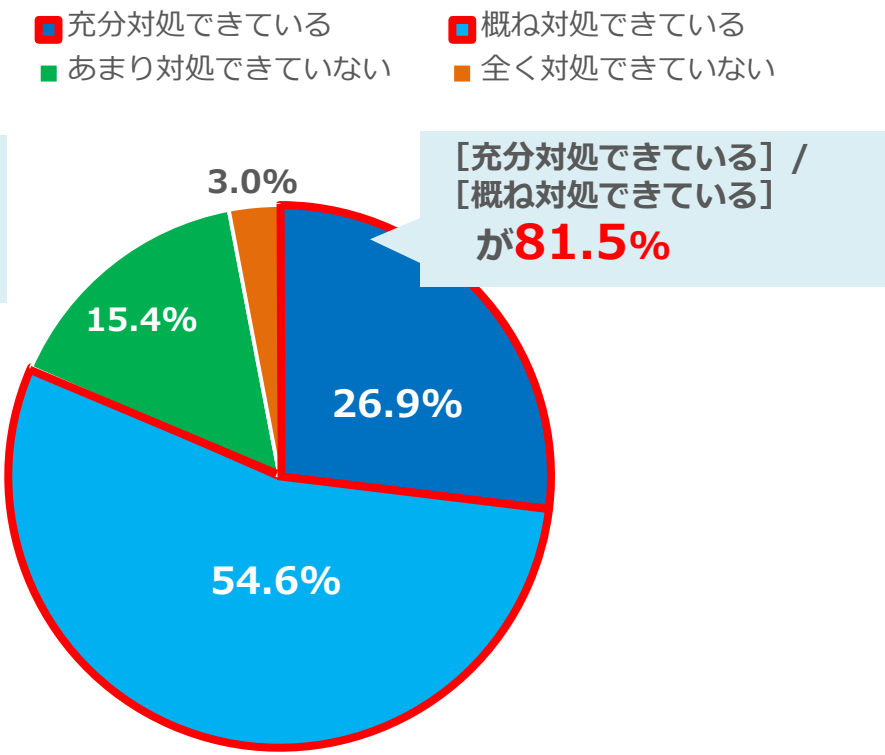
インシデントに遭遇した組織のリスク管理

インシデントに遭遇した組織の80%以上は概ねリスク対応に備えている

Q. インシデントが発生した際の対処方法フローを規定した、リスク対応のマニュアル等を用意し、体制を整えているか。



Q. 組織内にCSIRTなどインシデント対応を担当する専門チームが実効性を持って対処しているか。

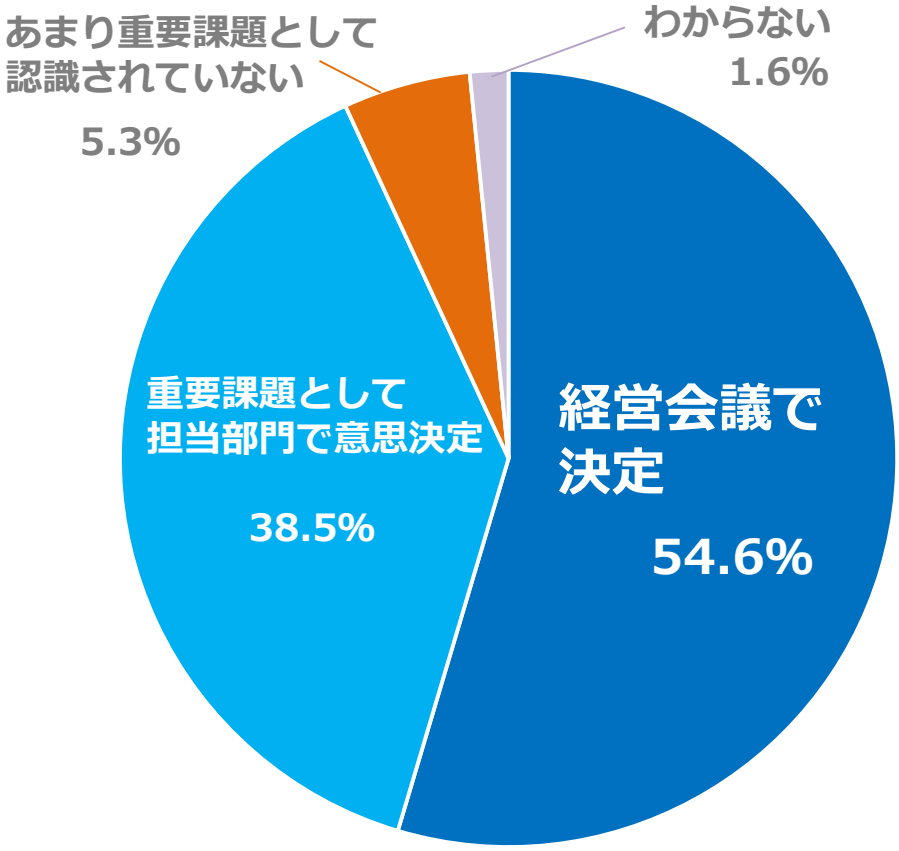


N＝1,065人

セキュリティ対策の重要度

■情報セキュリティを経営課題と認識している組織は54.6%
38.5%はセキュリティ対策について担当部門のみで意思決定している

Q. 経営層はセキュリティリスクを経営課題として認識していますか。
また、セキュリティ対策については経営会議等で審議・決定されていますか。



内訳				
従業員規模別	経営会議で決定	担当部門で決定	重要視されていない	わからない
5000人以上	64.3%	31.6%	2.5%	1.7%
1000~4999人	58.1%	38.2%	3.7%	0.0%
500~999人	44.8%	46.4%	6.4%	2.4%
200~499人	48.2%	40.1%	9.5%	2.2%
199人以下	41.2%	46.5%	9.4%	2.9%

N＝1,065人

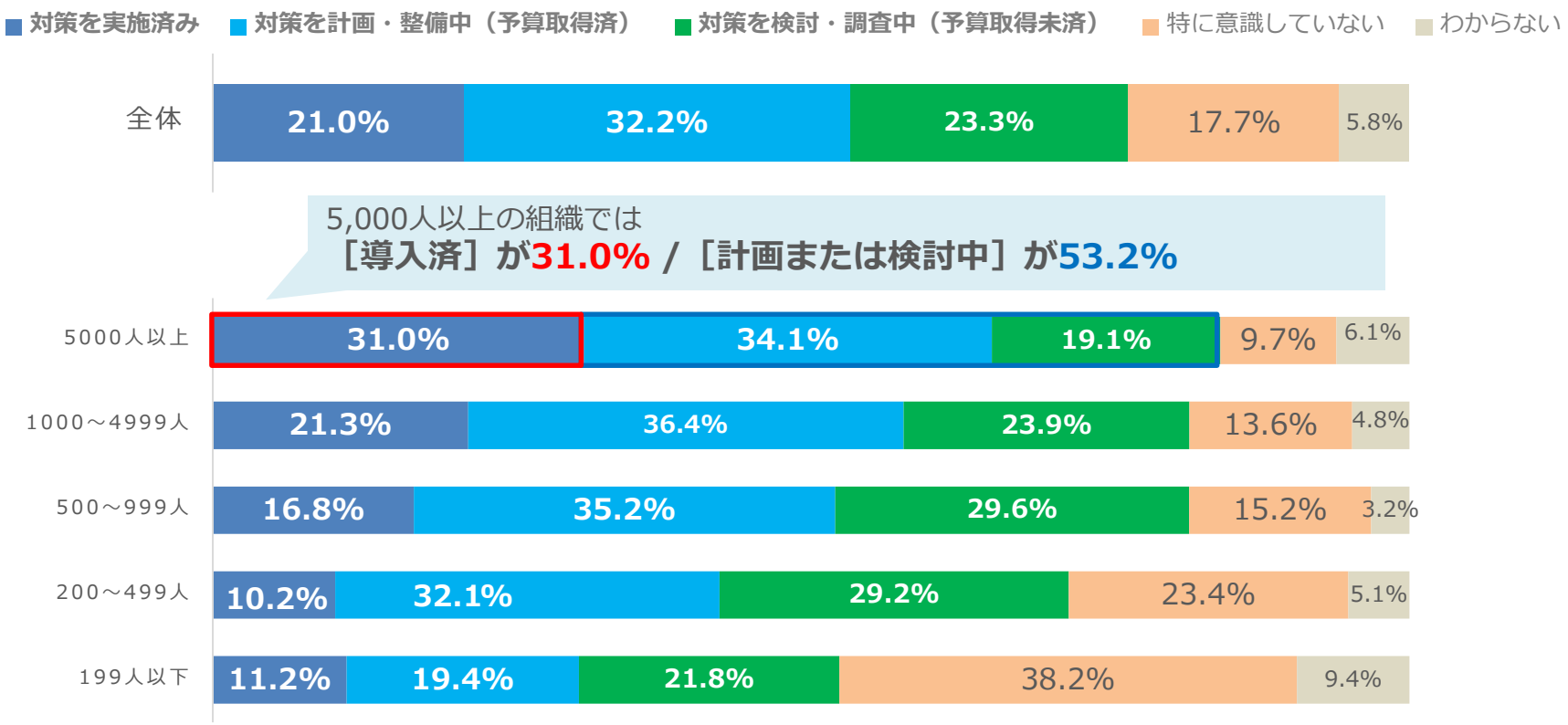
④従業員規模別ゼロトラスト/SecureWebGateway/SASEへの意識調査

ゼロトラストについての方針

■21.0%の組織がゼロトラストに基づき対策を実施済と回答
55.5%の組織は対策を計画または検討中

Q. ゼロトラスト※についてどのような方針をお持ちでしょうか。

※ゼロトラストとは、従来のように組織内と組織外との境界のみでセキュリティ対策を行うのではなく、「全て信頼しない」という考え方から、組織外へのアクセスや組織内で起こるトラフィック全てを信頼できないものと仮定してセキュリティ構築を行う考え方です



▶ 組織規模が大きい方がゼロトラストを重視

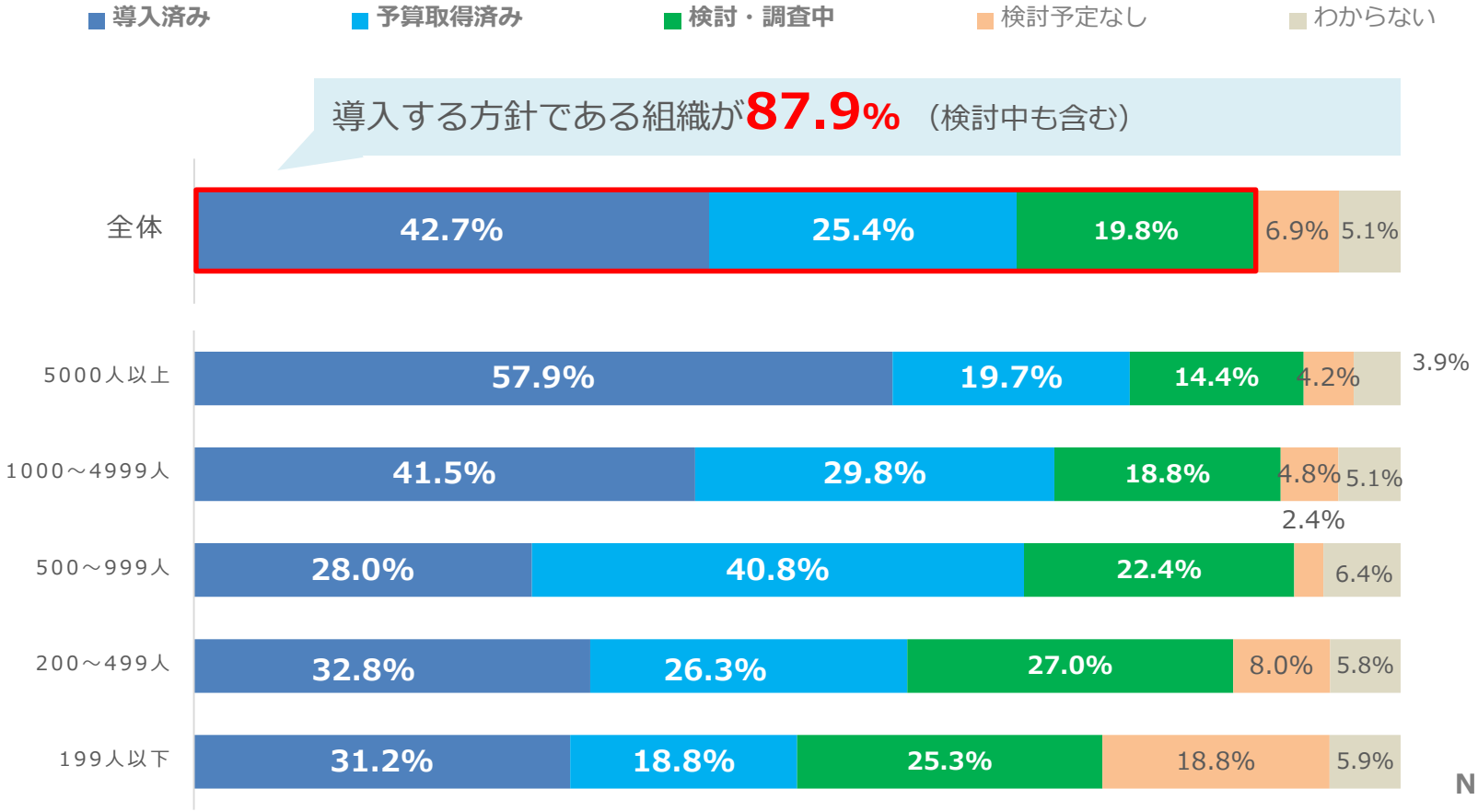
N＝1,065人

Secure Web Gatewayの導入方針

■検討中も含め、87.9%がSecure Web Gatewayを導入する方針
42.7%が導入済み、45.2%は導入予定、検討中であるとした組織は19.8%

Q. Webセキュリティの対策として、セキュアウェブゲートウェイ※の導入は検討されていますか。

※セキュアウェブゲートウェイとは、プロキシ機能/URLフィルタリング機能、アンチウイルス機能等Webセキュリティ管理機能を統合したクラウドサービスです（オンプレ版は除く）



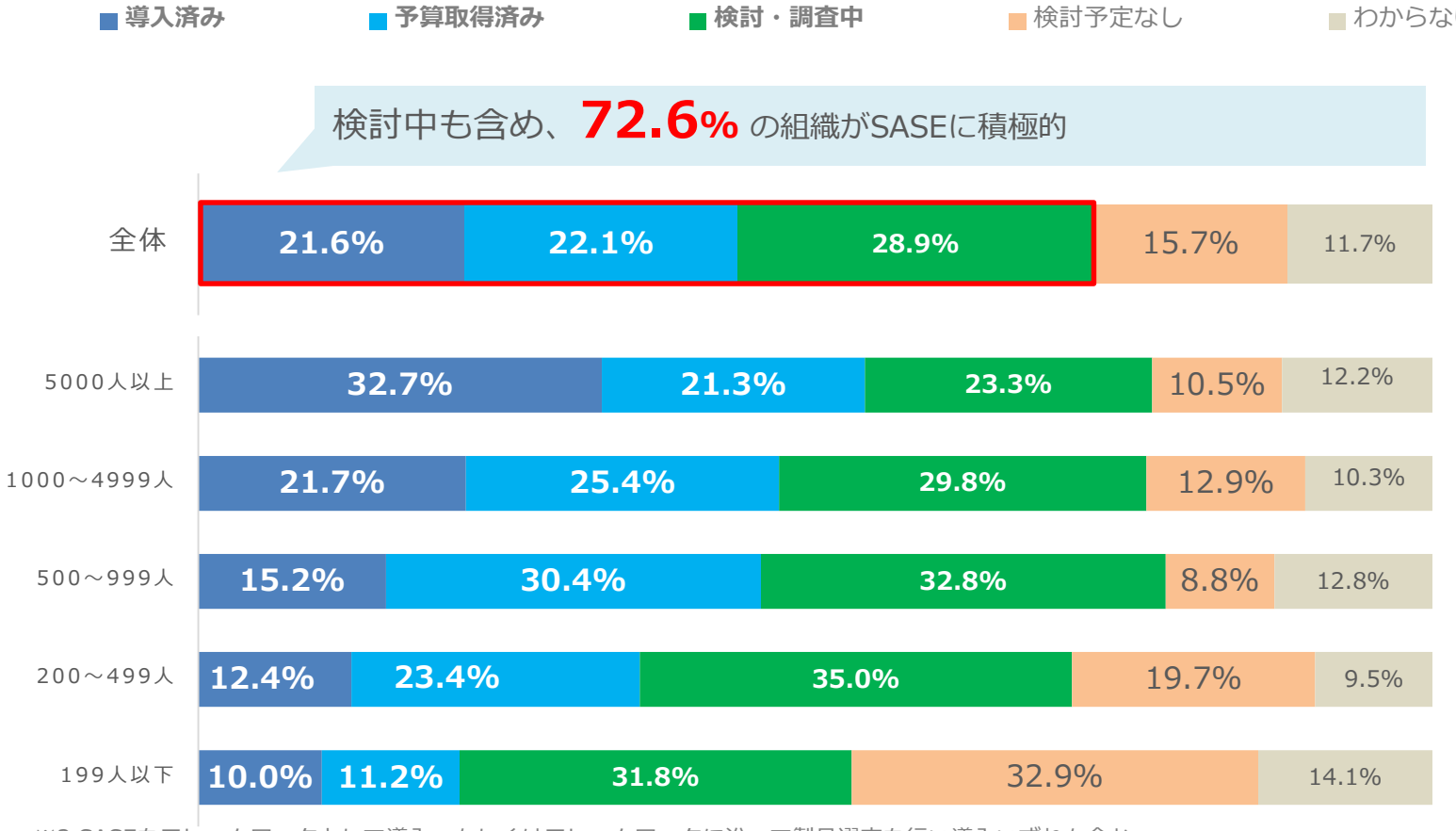
N＝1,065人

SASEの導入方針

■検討中も含め、SASEに積極的な組織が72.6%

Q. SASE（Secure Access Service Edge）※1について、導入※2を検討されていますか。

※1 SASEとは、米Gatner社が提唱した最新のセキュリティフレームワークの一つで、ネットワークセキュリティ機能とWAN機能の両方を提供することで、企業や組織の動的なセキュアアクセスニーズに応える様々な機能を提供するものです



N＝1,065人

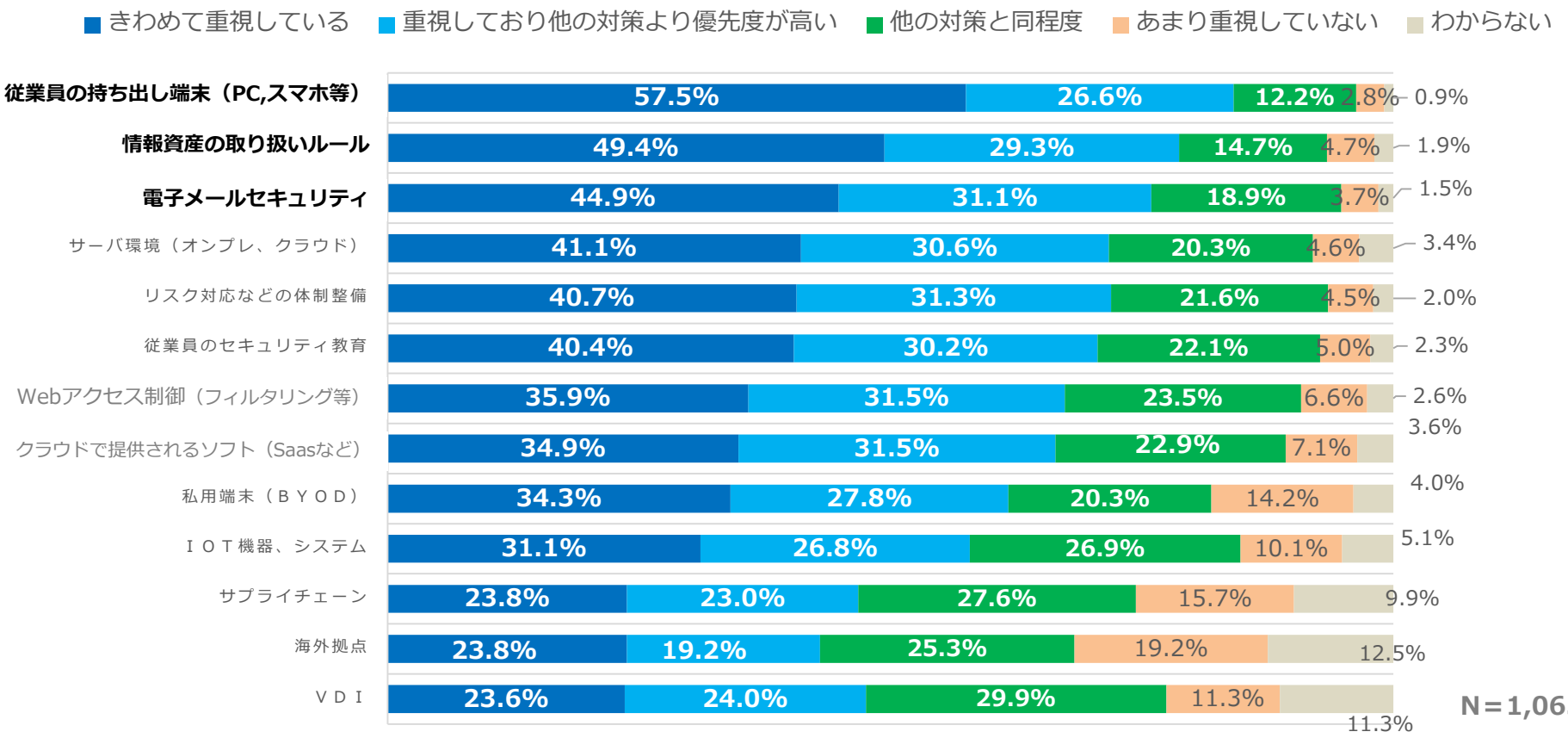
※2 SASEをフレームワークとして導入、もしくはフレームワークに沿って製品選定を行い導入いずれも含む。

⑤テレワークにおける
セキュリティ対策の優先度と満足度

テレワーク時のセキュリティ対策で重視する領域

■持ち出し端末/情報取り扱いルールなどの対策が重視されている

Q.　テレワーク導入においてセキュリティ対策で重視している領域はどこですか。

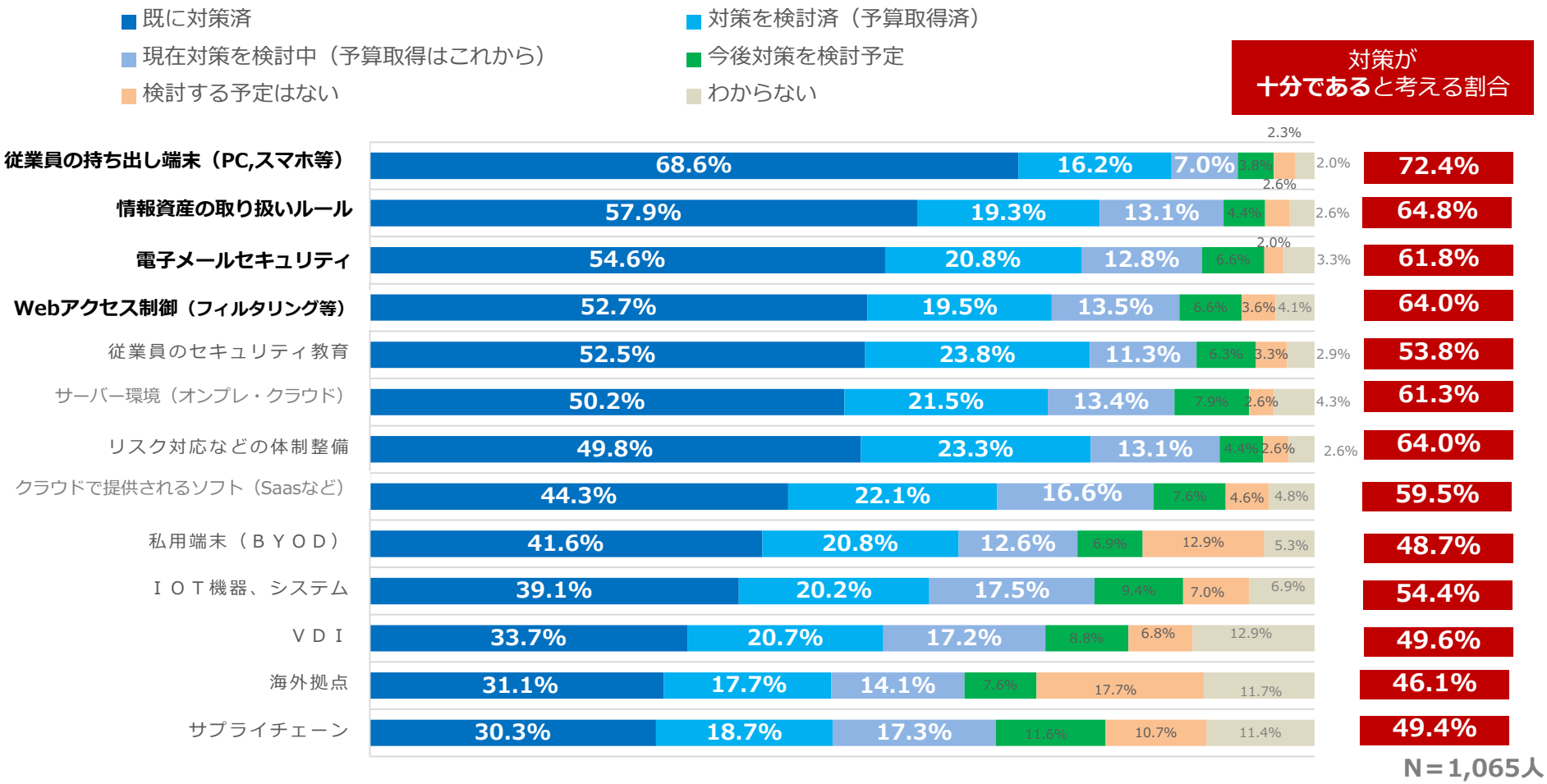


N＝1,065人

テレワーク時のセキュリティ対策実施状況と満足度

■重視する比重の高い領域である端末/情報取り扱いルールに加え、メールセキュリティやWebフィルタリングの実施率は高い

Q.　テレワーク環境における各領域のセキュリティ対策の実施状況をお聞かせください。



N＝1,065人

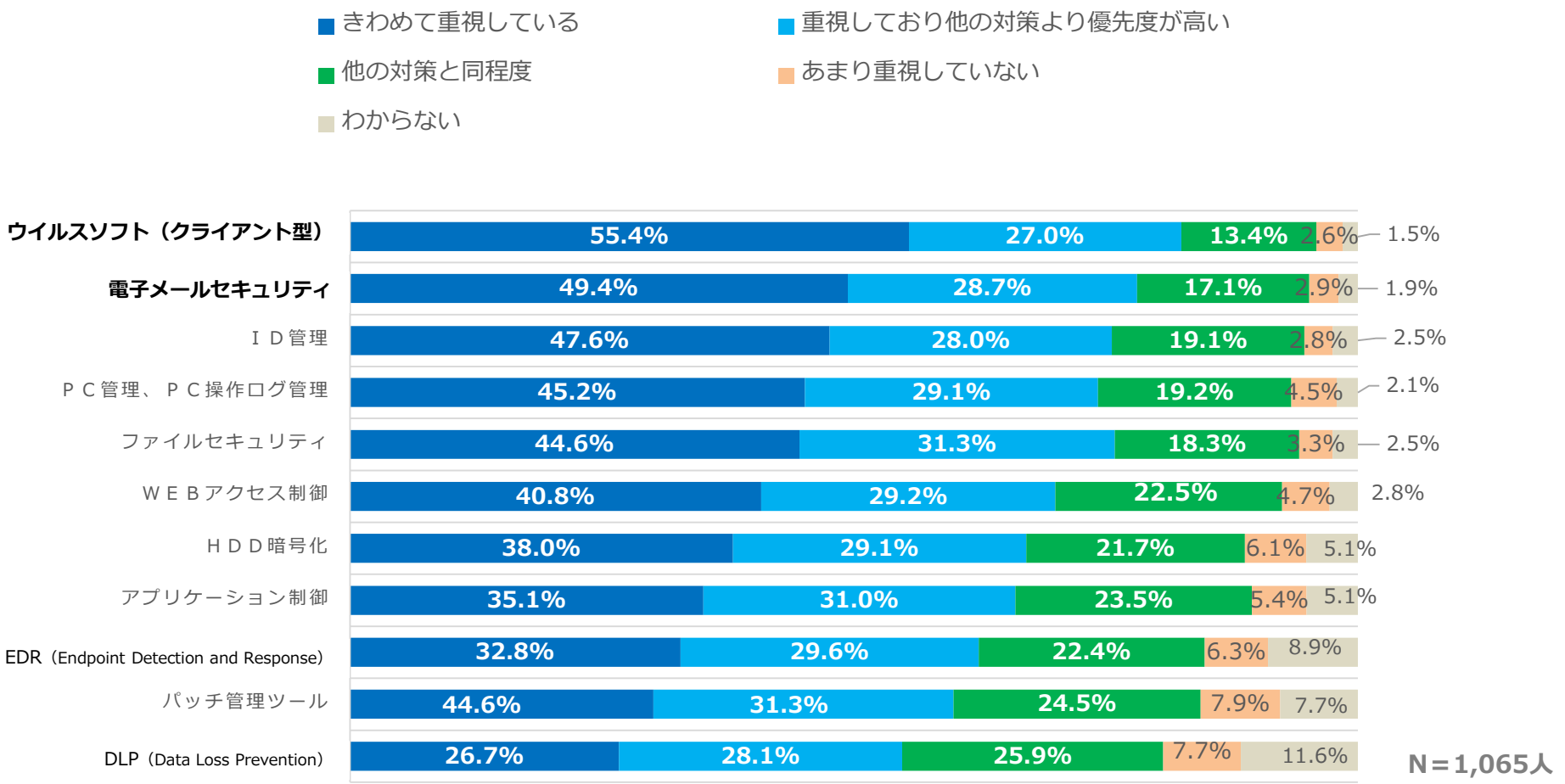
⑥テレワークにおける
エンドポイント対策の優先度と満足度

テレワーク時のエンドポイント対策で重視する領域

■重視する比重が大きい領域は、ウイルス対策/メールセキュリティなど

次いでID管理、PC操作ログ管理、ファイルセキュリティなどが挙げられる

Q　エンドポイント対策で重視している領域はどこですか。

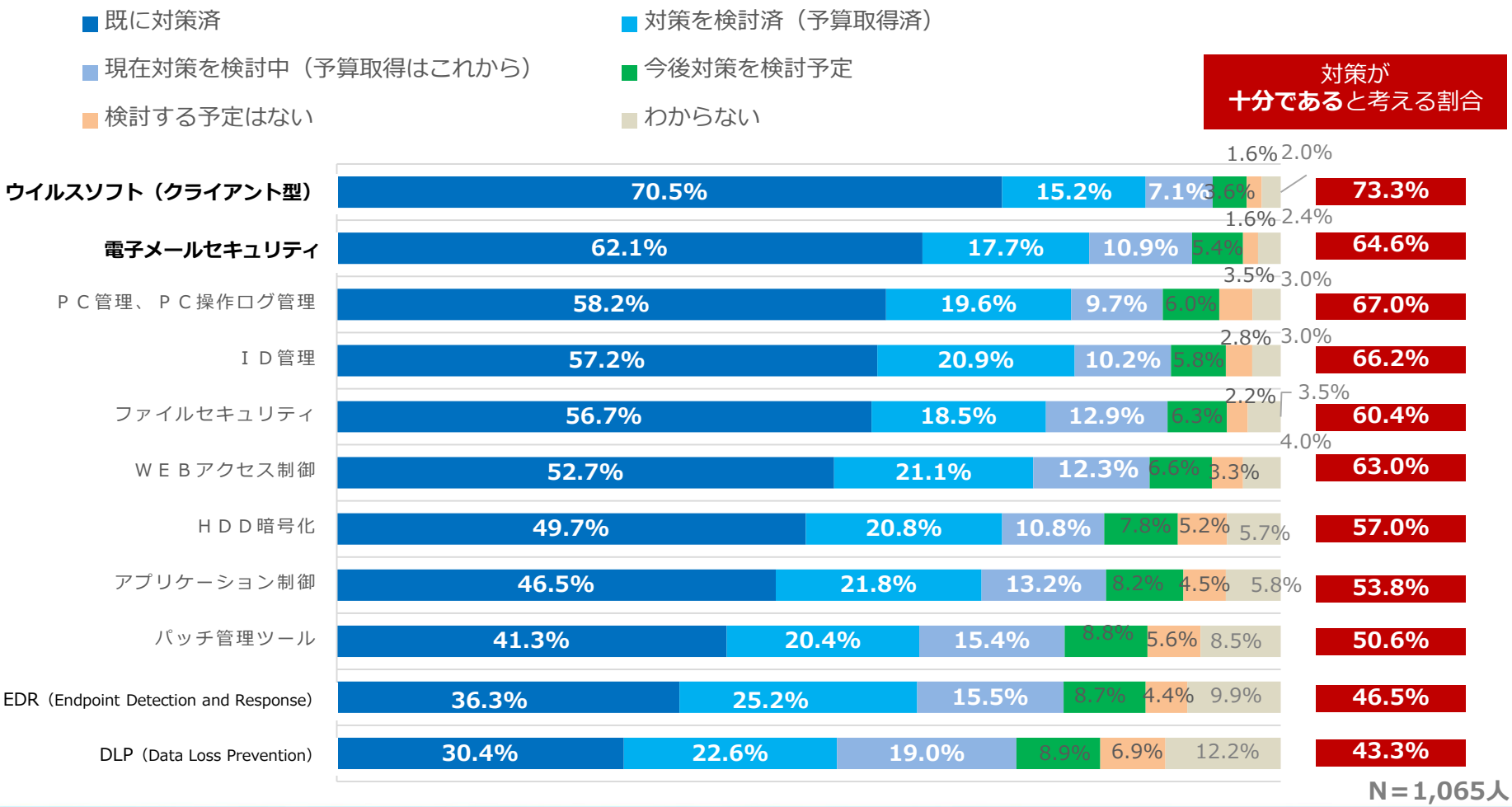


N＝1,065人

テレワーク時のエンドポイント対策実施状況と満足度

■重視する比重の高い領域であるウイルス対策ソフト/メールセキュリティ/PCログ管理等について実施率が高い

Q　各領域のエンドポイント対策の実施状況をお聞かせください。



N＝1,065人