DigitalArts®

国内企業・団体の
セキュリティ対策実態調査

2022年9月2日
デジタルアーツ株式会社

Contents

Theme 1 テレワークの実施率と社内ネットワークの利用状況

- テレワークの実施状況
  - ✓ 業種別
  - ✓ 規模別
- テレワーク時の社内ネットワークへの接続
  - ✓ 接続方法
  - ✓ セキュリティ対策強化

Theme 2 セキュリティ対策の現状

- ゼロトラストモデルに対する意識とセキュリティ対策の重要度
  - ✓ ゼロトラストに対する方針（全体）
  - ✓ ゼロトラストに対する方針（業種・規模別）
  - ✓ セキュリティ対策の重要度とリスク対応
  - ✓ セキュリティ人材の設置
  - ✓ 社内ルールの設置
  - ✓ セキュアゲートウェイの導入
- セキュリティ対策の実施状況
  - ✓ セキュリティ対策で重視する領域
  - ✓ セキュリティ対策の現状
    - ①導入済みのソリューション
    - ②ゼロトラスト方針別
  - ✓ 強化するソリューションの予算増額の状況
- セキュリティ対策の今後の方針
  - ✓ セキュリティ対策の今後の方針
    - ①未導入のソリューション
    - ②ゼロトラスト方針別
  - ✓ ランサムウェア、 Emotet対策のソリューション
  - ✓ セキュリティ対策予算
  - ✓ 新規導入の際に重視するポイント
  - ✓ プロキシ・Webアクセス制御で重視する点

Theme 3 2021年に発生したインシデントと被害状況

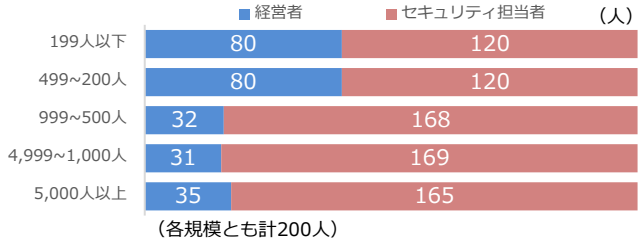
- 2021年に発生したインシデント
- ランサムウェア、 Emotet感染被害

調査概要

名称	国内企業・団体のセキュリティ対策実態調査
調査目的	国内企業・団体に対し、現状のセキュリティ対策の方針や、2021年中に経験したセキュリティインシデントの発生状況について調査し、国内企業・団体に必要とされるセキュリティ対策を明らかにすること
調査期間	2022年4月18日（月）～4月25日（月）
調査方法	インターネット調査
調査対象	民間企業および官公庁における経営者または情報セキュリティ担当者（1,000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方
有効回答数	1,000人 ※各規模とも計200人
委託調査機関	株式会社クロス・マーケティング

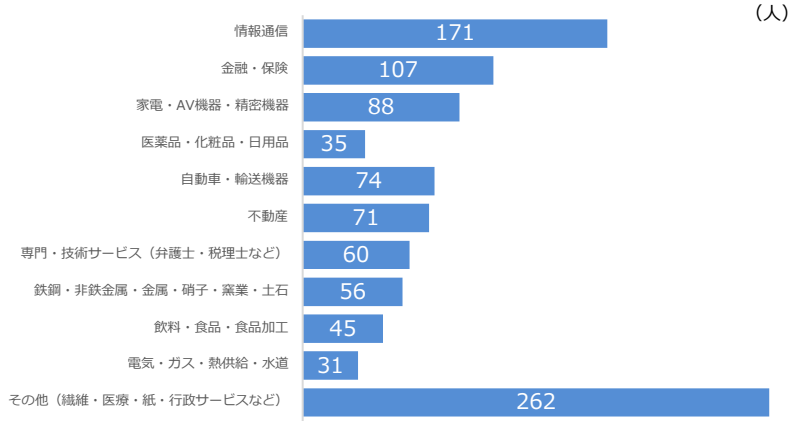
回答者の属性

➢ 従業員あるいは職員数



（各規模とも計200人）

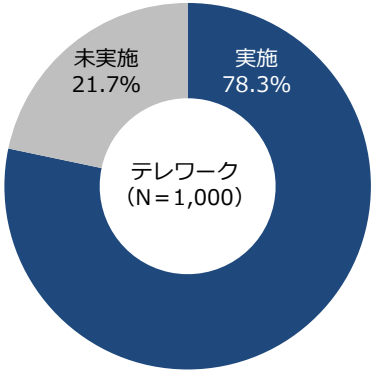
➢ 業種



Topics

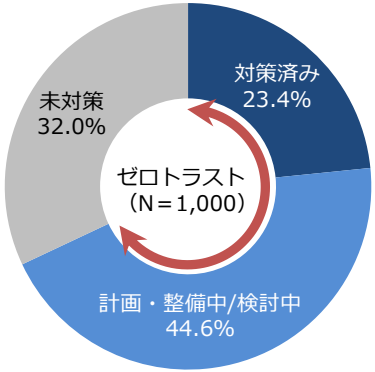
Theme 1
テレワークの実施率と社内ネットワークの利用状況

78.3%の調査対象が
テレワークを実施している
個別では、199人以下の小規模事業者は46.5%にとどまる

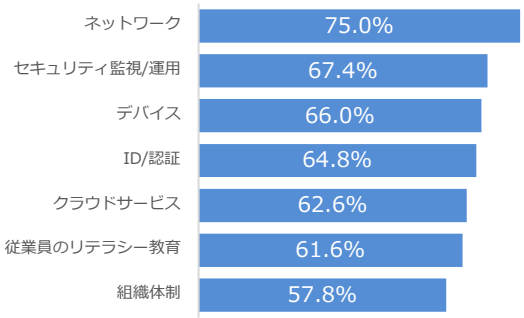


Theme 2
セキュリティ対策の現状

68.0%の調査対象が
ゼロトラスモデルの観点からセキュリティ対策を実施あるいは検討等をしている

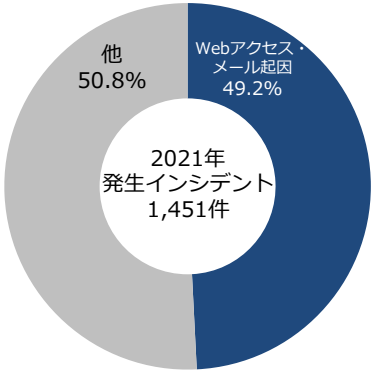


75.0%の調査対象が
セキュリティ対策として「ネットワーク」を重視し、「セキュリティ監視/運用」や「デバイス」が次いでいる



Theme 3
2021年に発生したインシデントと被害状況

49.2%のインシデントが
「メール経由の攻撃」と「不正なWebサイトへのアクセス」に起因する



Executive Summary

2021年に発生したインシデントは1,451件

メールとWebアクセスに起因するインシデントが全体に占める割合は49.2%

発生したインシデント項目の半数以上がランサムウェアやEmotetに感染

- ✓ **今回の調査によれば、ランサムウェア・Emotet感染の主な要因（感染経路）は、メール経由の攻撃や不正なWebサイトへのアクセス、OS・ソフトウェア・ネットワーク機器の脆弱性、リモートデスクトップの不備を狙った不正侵入とみられる**

- ✓ **ランサムウェア・Emotetの感染対策として、クライアントアンチウイルス、VPN、ID・パスワード認証の新規導入が多いことが明らかになったが、ランサムウェア・Emotetの被害に遭わないためには、主な要因（感染経路）である「攻撃の約半数を占めるメール経由の攻撃と不正なWebサイトへのアクセス」に対する具体的な対策も必要であると思料する**

- ✓ **デジタルアーツは、マルウェア感染による情報窃取・情報漏洩対策として、入口対策のメールセキュリティ、出口対策のWebアクセス制御を以前から推奨している。さらに万が一マルウェア感染してしまった場合の対策として、機密情報が入ったファイルの暗号化も有効な手段であると考える**

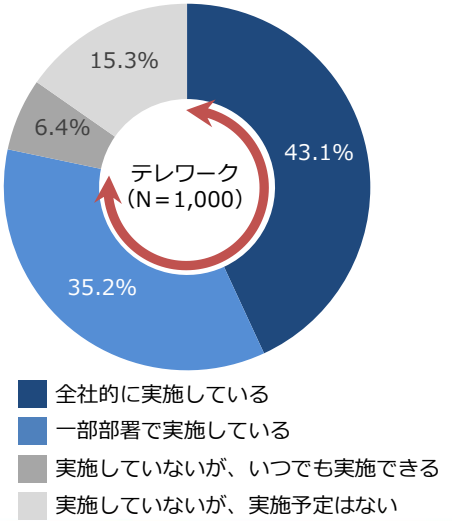
テレワークの実施率と社内ネットワークの利用状況

- テレワークの実施状況
- テレワーク時の社内ネットワークへの接続

テレワークの実施状況

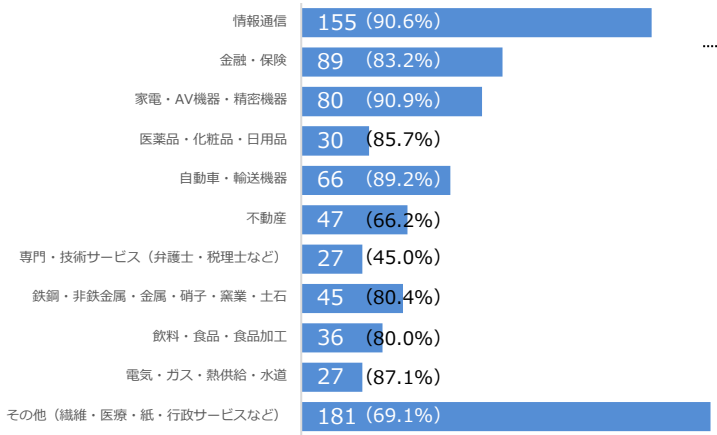
【Q1】あなたの組織ではテレワークを実施していますか

78.3%の調査対象がテレワークを実施している



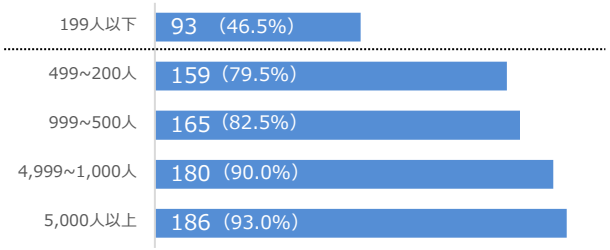
80.0%超えの業種が多く、「専門技術サービス」、「不動産」、「その他の業種」で実施が遅れている

【業種別の実施数とその割合】



約80.0%の実施率を超えないのは、「199人以下」の従業員規模

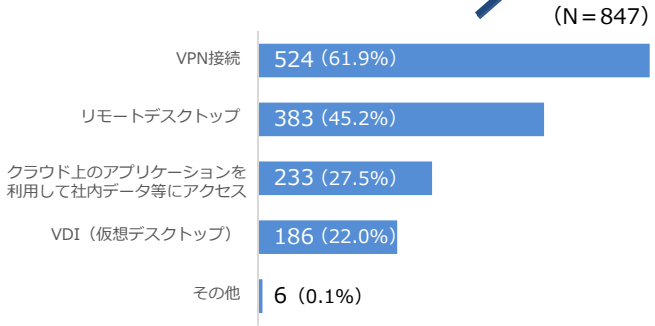
【従業員規模別の実施数とその割合】



テレワーク時の社内ネットワーク

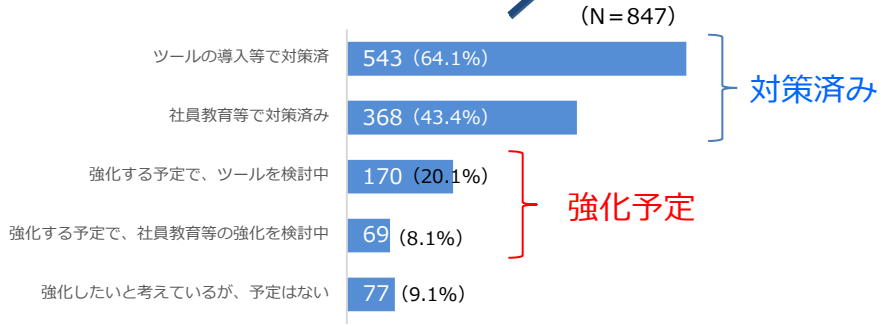
【Q2】テレワーク時の社内ネットワークへの接続はどのように行っていますか（複数回答）

61.9%がVPN接続
次いでリモートデスクトップによる接続



【Q3】【Q2】の社内ネットワーク接続方法に関して、セキュリティ対策を強化する予定はございますか（複数回答）

64.1%がツール導入等で対策済み。また、20.1%がツールによる強化を検討している



Theme 2

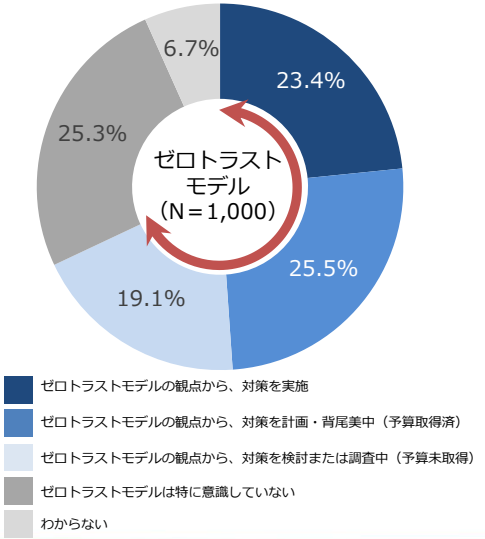
セキュリティ対策の現状

- ゼロトラストモデルに対する意識とセキュリティ対策の重要度
- セキュリティ対策の実施状況
- セキュリティ対策の今後の方針

ゼロトラストに対する方針

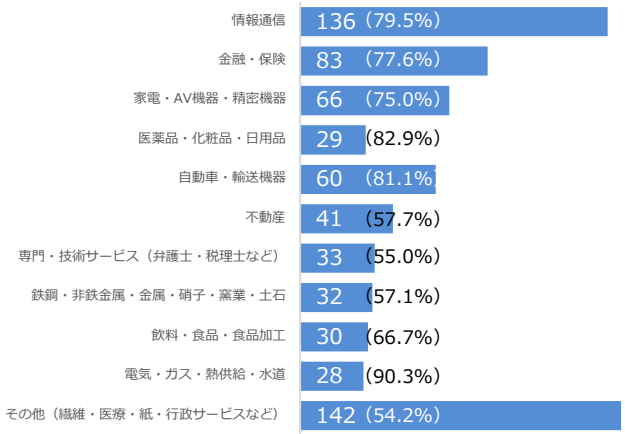
【Q4】ゼロトラストモデルの観点から、セキュリティ対策を実施されていますか

68.0%の調査対象がゼロトラスモデルの観点からセキュリティ対策を実施あるいは検討等をしている



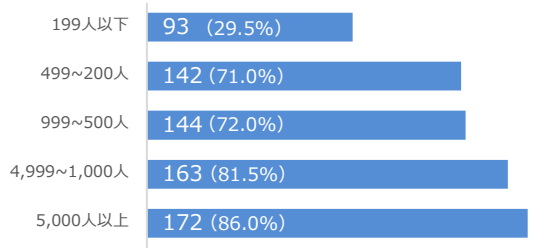
50.0%を超えどの業種もゼロトラストに積極的

【業種別のゼロトラストへの積極性※】



199人以下の従業員規模がゼロトラストへの積極性が他に比べて大きく低い

【従業員規模別のゼロトラストへの積極性※】

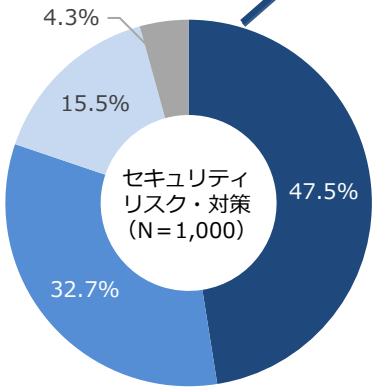


※積極性：ゼロトラストモデルの観点から対策を実施済み、または対策を計画・整備中、または対策を検討・調査中と回答した人の合計

セキュリティ対策の重要度とリスク対応

【Q5】貴社ではセキュリティリスクは経営課題の一つとして認識されていますか
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

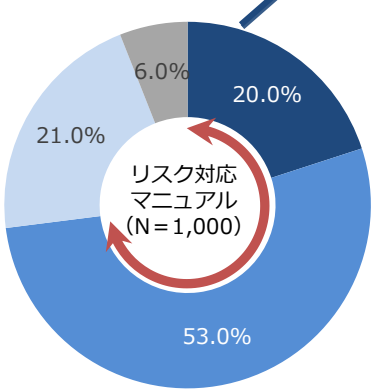
47.5%の調査対象がセキュリティ対策を経営会議等で決定している



- 経営会議等で審議・決定
- 重要課題として認識
- 重要課題として認識されていない
- わからない

【Q6】貴社ではインシデントが発生した際の対処フローを規定したリスク対応マニュアル等を用意し対応できる体制を整えていますか

73.0%の調査対象がインシデント発生時のリスク対応マニュアルを整えている

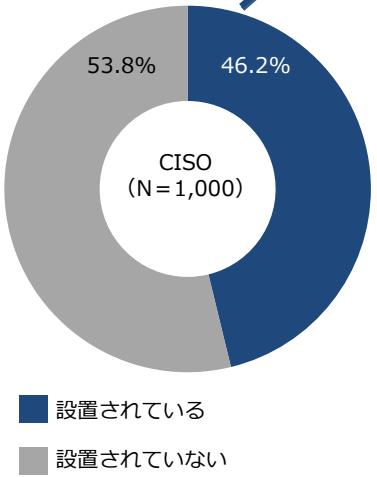


- 充分備えている
- 概ね備えている
- あまり備えられていない
- 全く備えていない

セキュリティ人材の設置

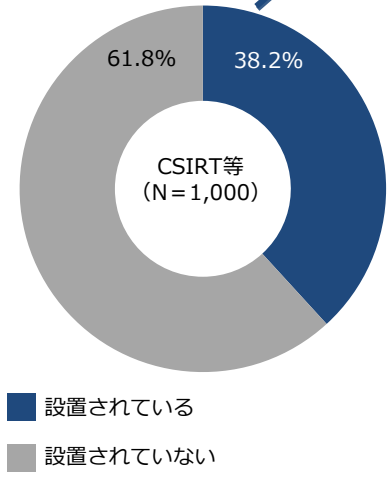
【Q7_1】貴社ではCISO（最高情報セキュリティ責任者）は設置されていますか

46.2%の調査対象がCISOを設置している



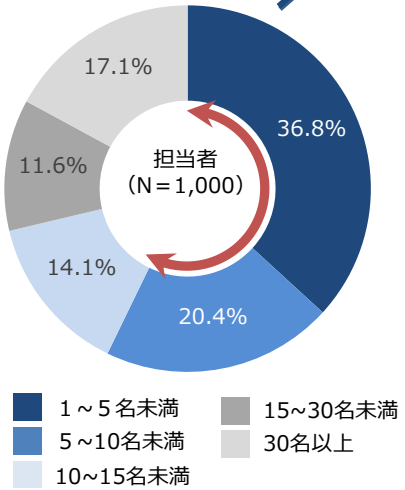
【Q7_2】貴社ではCSIRTなどインシデント対応を担当する専門チームは設置されていますか

38.2%の調査対象がCSIRT等の専門チームを設置している



【Q7_3】貴社では情報セキュリティに携わる担当者は何名いますか

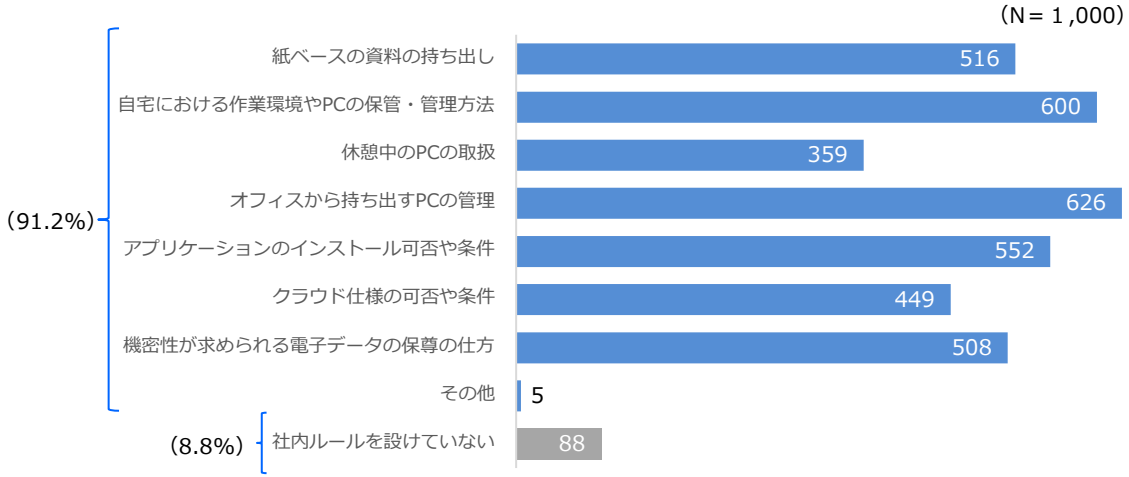
57.2%の調査対象が10名未満のセキュリティ担当者を設置



社内ルールの設置

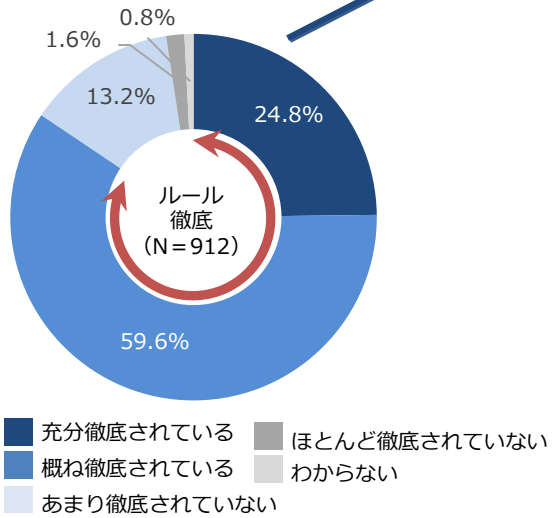
【Q8】貴社では情報取り扱いに関する社内ルールにはどのような項目を規定していますか（複数回答）

91.2%の調査対象で、何かしらの社内ルールを規定している
※社内ルールを設けていない調査対象（8.8%）を減算



【Q9】【Q8】でお答えいただいた社内ルールは徹底されていますか

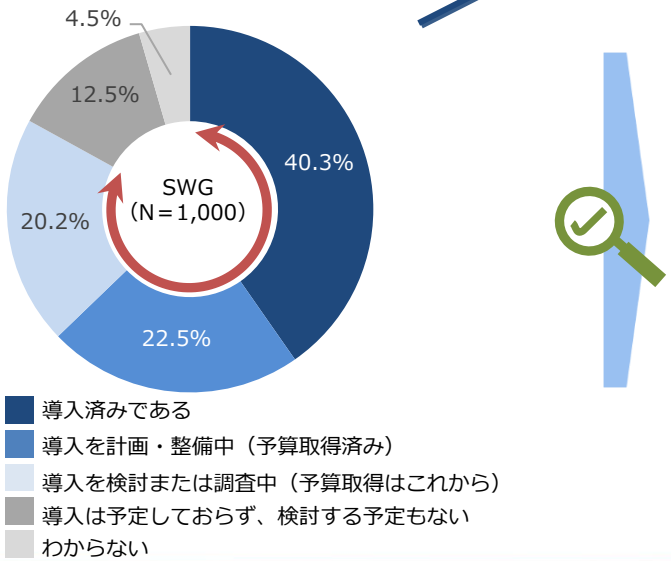
84.4%の調査対象で、
充分または概ね社内ルールの徹底がなされている
※社内ルールを設定している調査対象（N=912）に限定



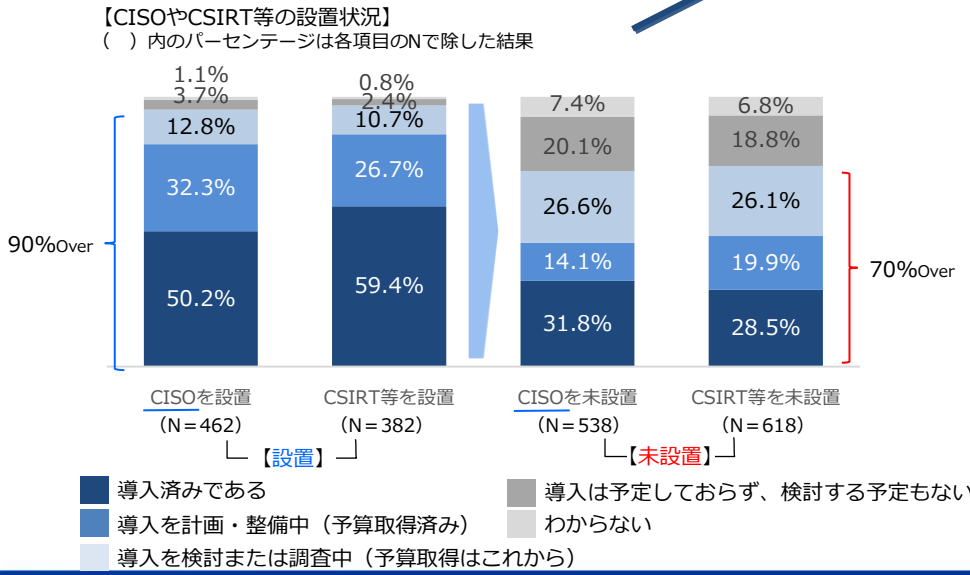
セキュアウェブゲートウェイの導入

【Q10】Webセキュリティの対策として、セキュアゲートウェイ（SWG）の導入を検討されていますか

83.0%の調査対象が、セキュアウェブゲートウェイ（SWG）の導入に前向きな方針。その内、40.3%は「導入済み」で、42.7%が「計画・整備中」「調査中」の状況



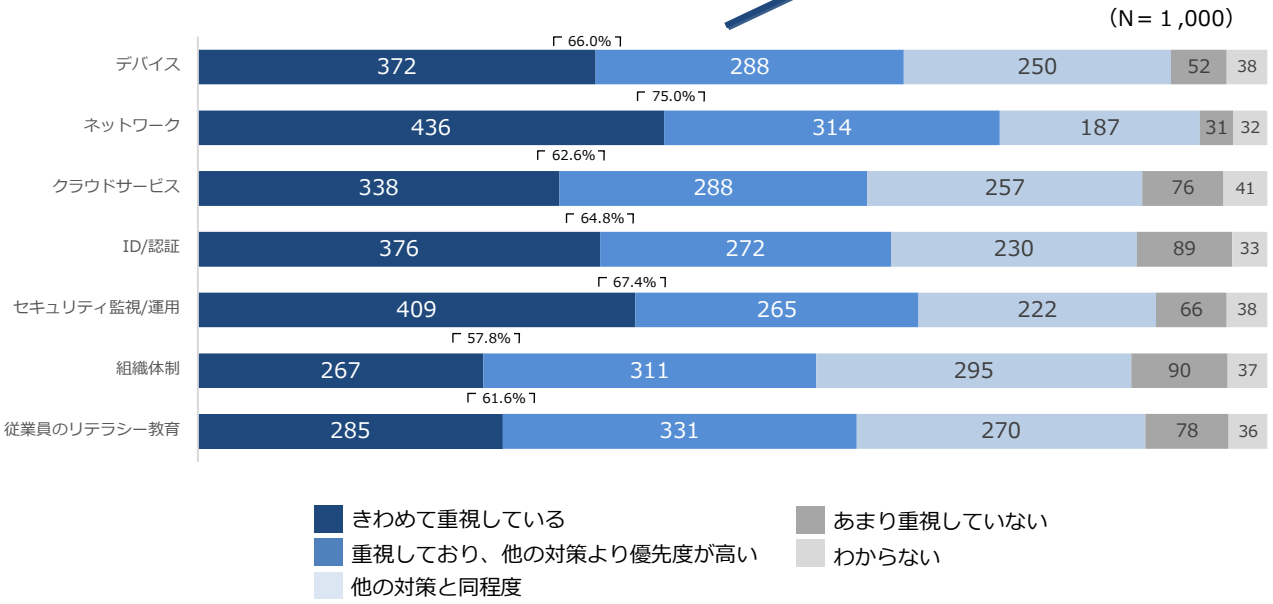
90%超と「CISO設置」あるいは「CSIRT等設置」の調査対象ではセキュアウェブゲートウェイ（SWG）の導入に前向きな方針であるが、 「CISO未設置」あるいは「CSIRT等未設置」の調査対象では70%超にとどまっている



セキュリティ対策で重視する領域

【Q11】セキュリティ対策で重視している領域はどこですか

75.0%の調査対象が、セキュリティ対策として、「ネットワーク」を重視するとの回答が最も多く、「セキュリティ監視/運用」や「デバイス」が次いでいる



セキュリティ対策の現状　①導入済みのソリューション

【Q12】提示したセキュリティーソリューションの内、どれを導入していますか（複数回答）
【Q13】【Q12】で「導入済み」と回答されたソリューションについて、強化する予定がありますか

（凡例）

（領域）		
（ソリューション名）	「導入済み」と回答した割合(N=1,000)	「導入済み」と回答のうち、そのソリューションを「強化する」と回答した割合

70.0%を超える導入率は「ファイヤーウォール」「メールセキュリティ」「ID・パスワード認証」
導入率が30%台のソリューションは、70%を超えて今後強化予定とされている

デバイス		
クライアントアンチウイルス	68.5%	67.3%
端末監視	48.3%	70.4%
MDM	44.0%	70.0%
※重複を除く導入割合		78.2%

クラウドサービス		
CASB	39.8%	**76.6%**

リテラシー教育		
標的型メール訓練	46.0%	75.4%
その他従業員のリテラシー教育	49.2%	71.1%
※重複を除く導入割合		57.1%

ネットワーク		
VPN	68.3%	64.7%
ゲートウェイアンチウイルス	53.8%	65.6%
サンドボックス	30.4%	**76.6%**
ファイヤーウォール	**70.3%**	63.2%
不正検知システム	50.6%	71.1%
侵入防止システム	52.2%	70.3%
プロキシ、Webアクセス制御	56.7%	68.3%
メールセキュリティ	**71.9%**	64.1%
※重複を除く導入割合		89.6%

ID/認証		
ファイル暗号化	58.4%	67.5%
ID・パスワード認証	**74.3%**	62.9%
生体認証	30.5%	**77.4%**
ID管理	63.5%	66.6%
※重複を除く導入割合		83.0%

セキュリティ監視/運用		
SOC	44.2%	75.1%
ログ監視、SIEM	53.1%	70.4%
その他セキュリティ運用	36.8%	**74.7%**
ポリシー整備	53.6%	69.2%
脆弱性診断	46.7%	73.4%
※重複を除く導入割合		72.3%

セキュリティ対策の現状　②ゼロトラスト方針別

【Q12】および【Q13 】の回答に対して、ゼロトラストに対する積極性でクロス集計した結果

（凡例）

（領域）				
（ソリューション名）	ゼロトラストに**積極的**(N=680)		ゼロトラストに**消極的**(N=320)	
	「導入済み」と回答した割合	そのソリューションを**「強化する」**と回答した割合	**「導入済み」**と回答した割合	そのソリューションを**「強化する」**と回答した割合

ゼロトラストへの方針（積極的/消極的）の違いによる各ソリューションの導入率は、（「サンドボックス」を除き、）積極的な方針の場合は消極的な方針に比べて、20%程度導入率が高くなる傾向※にある

※「積極的な場合の導入率」-「消極的な場合の導入率」≧20%

デバイス				
クライアントアンチウイルス	74.7%	77.8%	55.3%	37.3%
端末監視	59.0%	76.3%	25.6%	41.5%
MDM	54.1%	75.0%	22.5%	44.4%
クラウドサービス				
CASB	51.3%	81.1%	15.3%	44.9%
リテラシー教育				
標的型メール訓練	55.9%	82.6%	25.0%	41.3%
その他従業員のリテラシー教育	57.4%	79.0%	31.9%	41.2%

ネットワーク				
VPN	75.4%	73.1%	55.1%	36.7%
ゲートウェイアンチウイルス	61.9%	73.4%	45.4%	33.7%
サンドボックス	39.7%	80.0%	31.8%	42.9%
ファイヤーウォール	73.1%	74.2%	54.3%	32.9%
不正検知システム	61.5%	78.0%	47.9%	34.7%
侵入防止システム	63.1%	76.7%	48.4%	36.1%
プロキシ、Webアクセス制御	66.3%	75.2%	49.9%	36.1%
メールセキュリティ	75.6%	75.5%	57.1%	33.3%

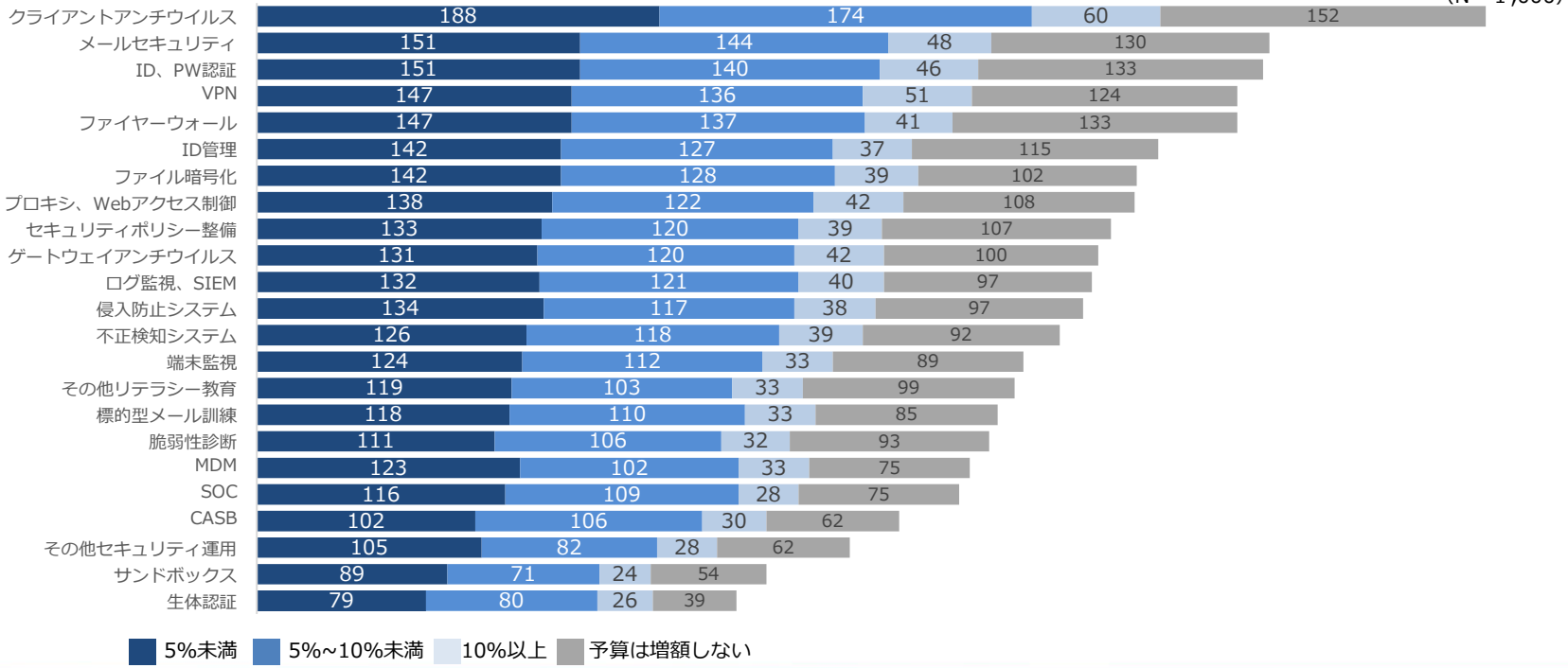
ID/認証				
ファイル暗号化	67.9%	74.9%	38.1%	39.3%
ID・パスワード認証	79.4%	74.3%	63.4%	32.5%
生体認証	38.2%	83.1%	14.1%	44.4%
ID管理	70.4%	75.4%	48.8%	39.7%
セキュリティ監視/運用				
SOC	56.0%	79.3%	19.1%	49.2%
ログ監視、SIEM	63.5%	78.2%	30.9%	36.4%
その他セキュリティ運用	46.3%	80.3%	16.6%	41.5%
ポリシー整備	63.8%	76.7%	31.9%	37.3%
脆弱性診断	56.9%	80.1%	25.0%	41.3%

強化するソリューションの予算増額の状況

【Q14】【Q13】で「すでに強化した」、または「強化する予定」したソリューションについて、「どの程度予算を増額された」または「増額する予定」ですか（複数回答）

強化するソリューションとして、予算増額が最も多いのは「クライアントアンチウイルス」であった
また、予算増額が少ないのは「生体認証」と「サンドボックス」であった

（N＝1,000）



セキュリティ対策の今後の方針　①未導入のソリューション

【Q15】　【Q12】で「未導入」と回答されたソリューションについて、新規で導入予定がありますか（複数回答）

（凡例）

（領域）		
（ソリューション名）	「未導入」と回答した割合(N=1,000)	「未導入」と回答のうち、そのソリューションを「新規導入する」と回答した割合

20%台未満と未導入の割合が低いソリューションは「クラインアントアンチウイルス」、「VPN」、「ファイヤーウォール」、「メールセキュリティ」、「ID管理」であった

デバイス		
クライアントアンチウイルス	**23.2%**	59.1%
端末監視	41.2%	20.1%
MDM	45.0%	19.8%
クラウドサービス		
CASB	46.7%	18.2%
リテラシー教育		
標的型メール訓練	42.9%	20.5%
その他従業員のリテラシー教育	40.5%	21.0%

ネットワーク		
VPN	**22.6%**	27.0%
ゲートウェイアンチウイルス	35.4%	24.6%
サンドボックス	53.3%	17.3%
ファイヤーウォール	**20.8%**	27.4%
不正検知システム	36.8%	20.9%
侵入防止システム	52.2%	14.9%
プロキシ、Webアクセス制御	31.7%	21.8%
メールセキュリティ	**20.6%**	28.6%

ID/認証		
ファイル暗号化	33.1%	21.5%
ID・パスワード認証	19.6%	20.4%
生体認証	59.8%	15.4%
ID管理	**29.3%**	18.1%
セキュリティ監視/運用		
SOC	43.4%	18.2%
ログ監視、SIEM	35.9%	21.7%
その他セキュリティ運用	49.7%	19.7%
ポリシー整備	35.8%	24.6%
脆弱性診断	41.1%	20.4%

セキュリティ対策の今後の方針　②ゼロトラスト方針別

【Q15】の回答に対して、ゼロトラストに対する積極性でクロス集計した結果

（凡例）

（領域）				
（ソリューション名）	ゼロトラストに**積極的**(N=680)		ゼロトラストに**消極的**(N=320)	
	「未導入」と回答した割合	そのソリューションを**「新規導入する」**と回答した割合	**「未導入」**と回答した割合	そのソリューションを**「新規導入する」**と回答した割合

ゼロトラストへの方針が積極的な調査対象は、消極的な調査対象に比べ、未導入ソリューションを新規で導入する意向が高い（30.5%＞9.2%）

デバイス				
クライアントアンチウイルス	20.9%	81.7%	28.1%	23.3%
端末監視	35.4%	28.2%	53.4%	8.8%
MDM	39.0%	27.9%	57.8%	8.1%
クラウドサービス				
CASB	40.7%	24.9%	59.4%	8.4%
リテラシー教育				
標的型メール訓練	35.7%	29.2%	58.1%	9.1%
その他従業員のリテラシー教育	35.1%	29.7%	51.9%	8.4%

ネットワーク				
VPN	18.1%	39.0%	32.2%	12.6%
ゲートウェイアンチウイルス	31.3%	34.3%	44.1%	9.9%
サンドボックス	49.0%	21.9%	62.5%	9.5%
ファイヤーウォール	20.0%	35.3%	22.5%	12.5%
不正検知システム	29.9%	31.0%	51.6%	8.5%
侵入防止システム	28.5%	32.5%	50.3%	9.3%
プロキシ、Webアクセス制御	25.9%	32.4%	44.1%	8.5%
メールセキュリティ	19.7%	37.3%	22.5%	12.5%

ID/認証				
ファイル暗号化	26.9%	33.3%	46.3%	6.8%
ID・パスワード認証	16.2%	30.0%	26.9%	8.1%
生体認証	54.1%	20.4%	71.9%	7.4%
ID管理	24.0%	28.2%	40.6%	5.4%
セキュリティ監視/運用				
SOC	36.8%	26.0%	7.6%	57.5%
ログ監視、SIEM	29.9%	30.5%	10.3%	48.8%
その他セキュリティ運用	44.4%	26.5%	9.2%	60.9%
ポリシー整備	29.3%	36.2%	10.1%	49.7%
脆弱性診断	34.7%	29.2%	8.6%	54.7%

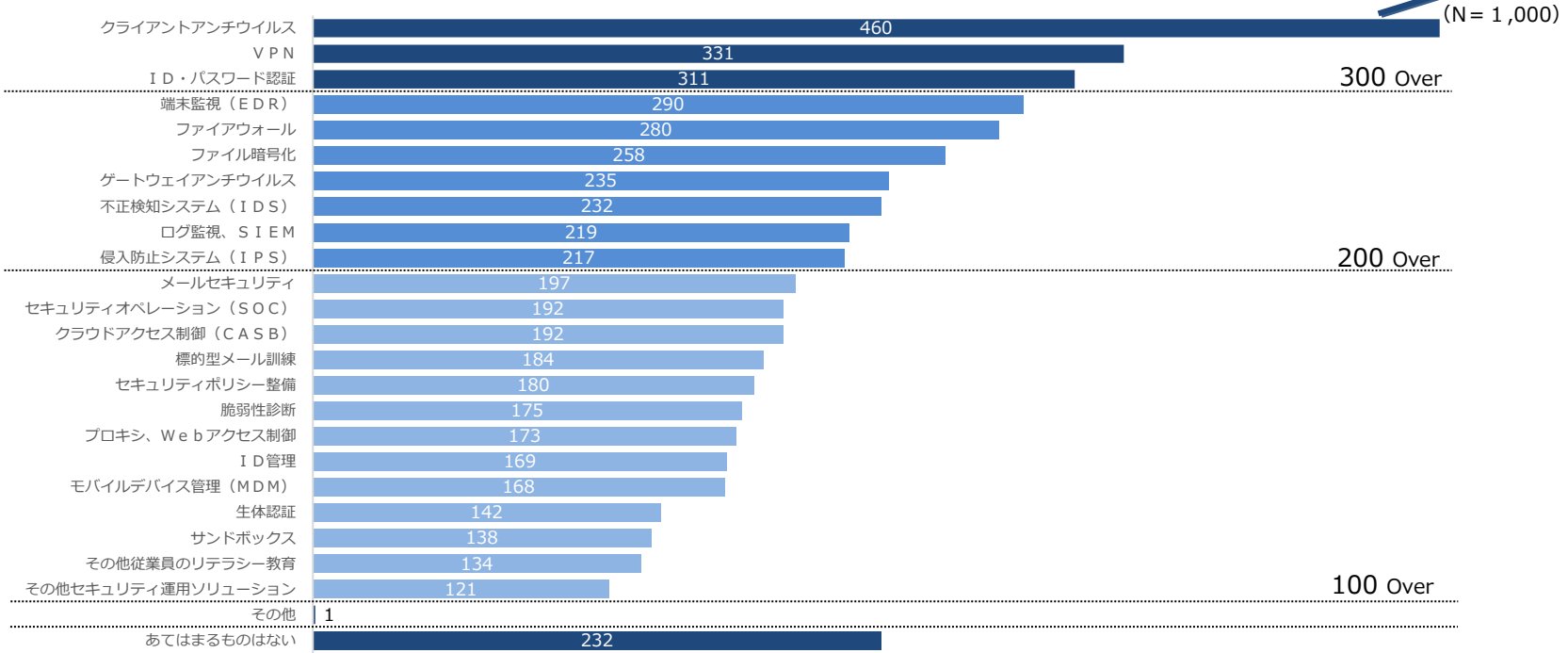
（平均）

	ゼロトラストに**積極的**(N=680)	ゼロトラストに**消極的**(N=320)
未導入	全体平均　31.5%	全体平均　47.6%
うち、新規導入する	**全体平均　30.5%**	**全体平均　9.2%**

ランサムウェア、 Emotet対策のソリューション

【Q16】ランサムウェア、 Emotetの対策とした「強化した」、または「新規導入した」ソリューションはありますか（複数回答）

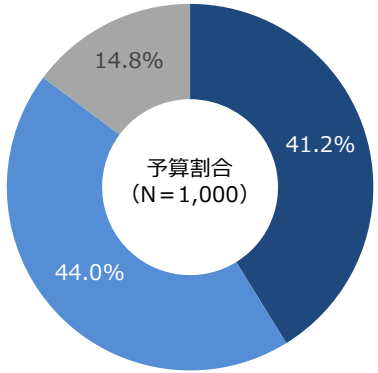
ランサムウェア、 Emotet対策として強化・新規導入したのは「クライアントアンチウイルス」が最も多く、 「 VPN 」 、 「 ID・パスワード認証」が次ぐ



セキュリティ対策予算/新規導入の際に重視するポイント

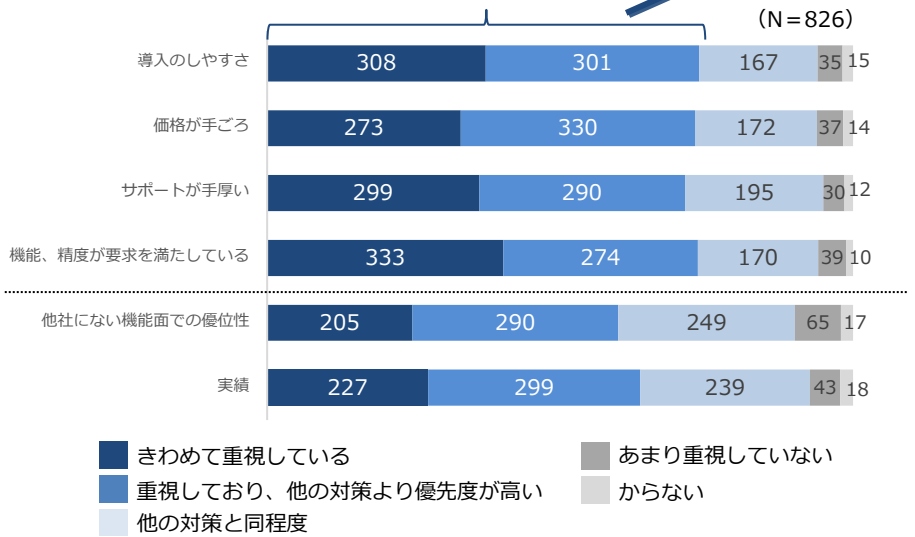
【Q17】2022年度のIT予算に対するセキュリティ対策予算はどのくらいの割合でしょうか

41.2%の調査対象が、IT予算に占めるセキュリティ対策予算の割合が5%未満であり、
IT予算に占めるセキュリティ対策予算の割合が5%~10%未満の44.0%とほぼ同程度であった



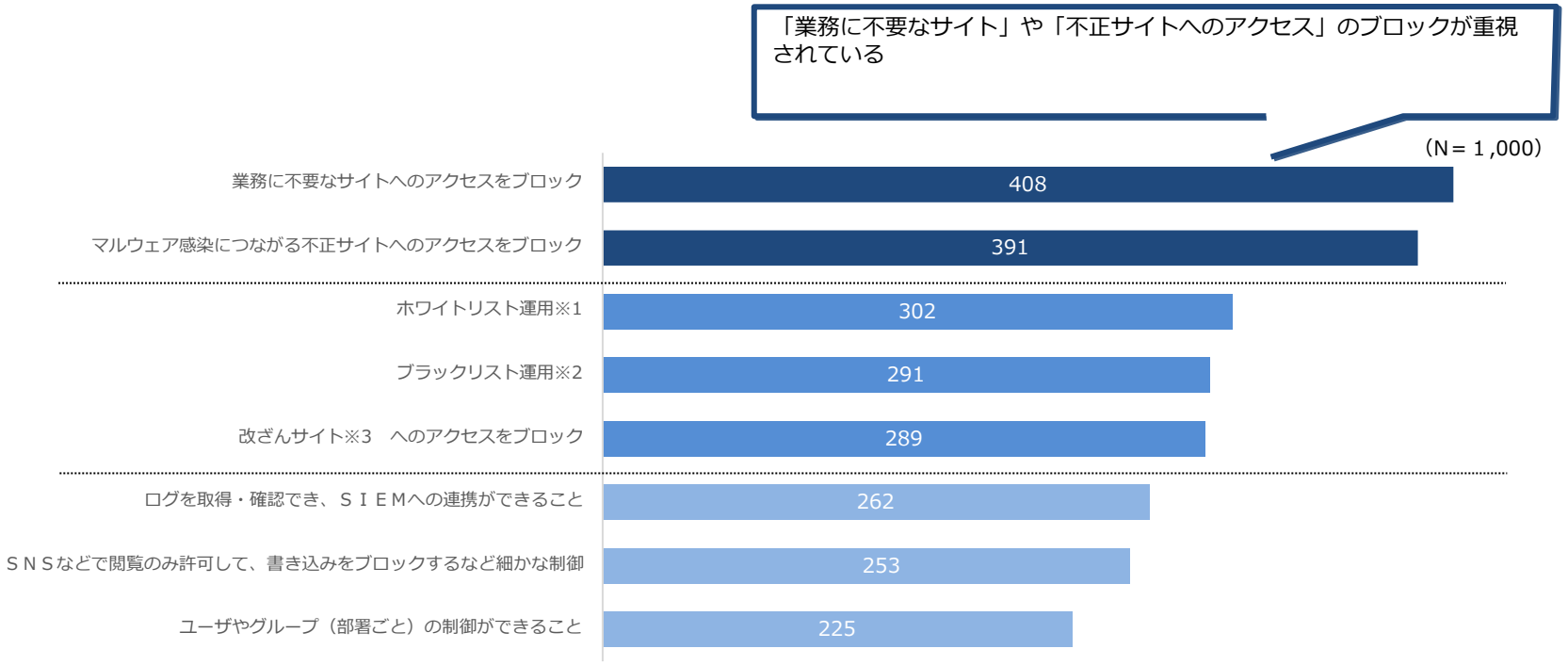
【Q18】ソリューションを新規導入するにあたり、重視するポイントについてお聞かせください

「きわめて重視している」、「重視しており、他の対策より優先度が高い」までを含めると、「他社にない機能面での優位性」や「実績」は他の項目に比して重視されていない



プロキシ・Webアクセス制御で重視する点

【Q19】プロキシ・Webアクセス制御で重視するポイントや運用方法はなんでしょうか（複数回答）



※1　ユーザーがアクセスできるURLやコンテンツを指定し、その他のURLやコンテンツはアクセスを禁止する方法
※2　ユーザーがアクセスできないURLやコンテンツを指定し、その他のURLやコンテンツはアクセスを許可する方法
※3　管理者以外の第三者によって管理者の意図しない変更が勝手になされてしまい、サイバー攻撃に悪用されるサイト

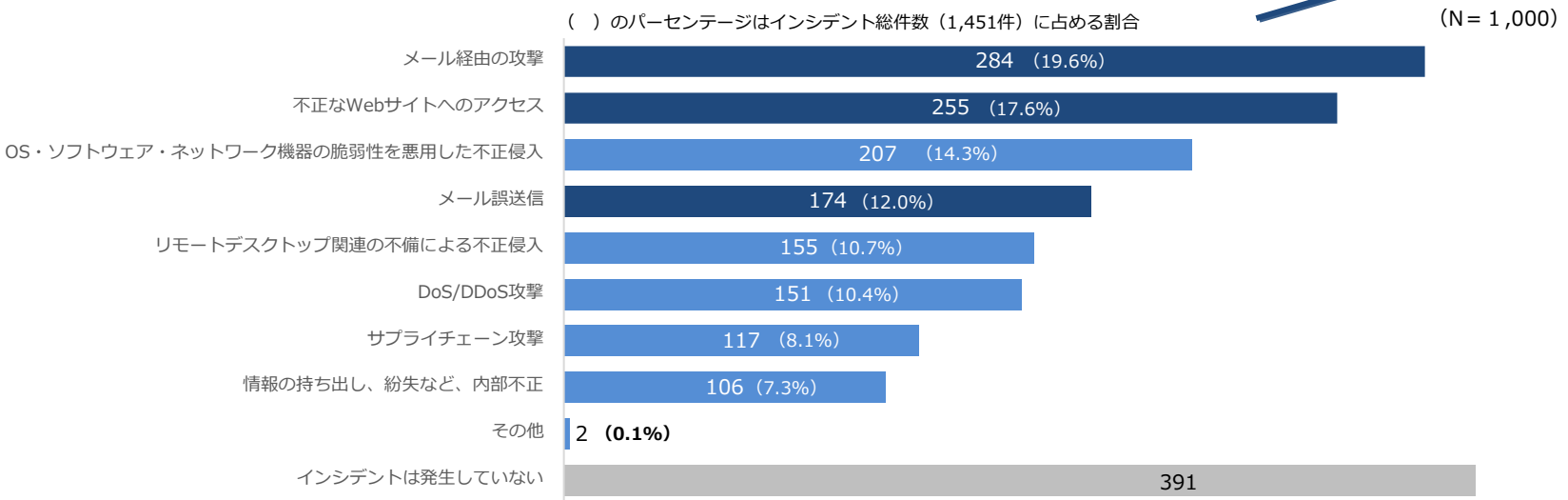
2021年に発生したインシデントと被害状況

- 2021年に発生したインシデントと被害状況
- ランサムウェア・Emotet感染被害

2021年に発生したインシデント

【Q20】貴社では、2021年1月~2021年12月の間、セキュリティインシデントは発生しましたか
発生したインシデントをお答えください（複数回答）

1,451件のインシデントが調査対象で2021年に発生している
49.2%のインシデントがメールとWebサイトアクセスに起因している



2021年インシデント総件数	うち、メールとWebアクセスに起因するインシデント
1,451件	713件（49.2%）

ランサムウェア・Emotet感染被害

【Q21】【Q20】で発生したインシデントについて、ランサムウェアまたはEmotet感染はありましたか（複数回答）

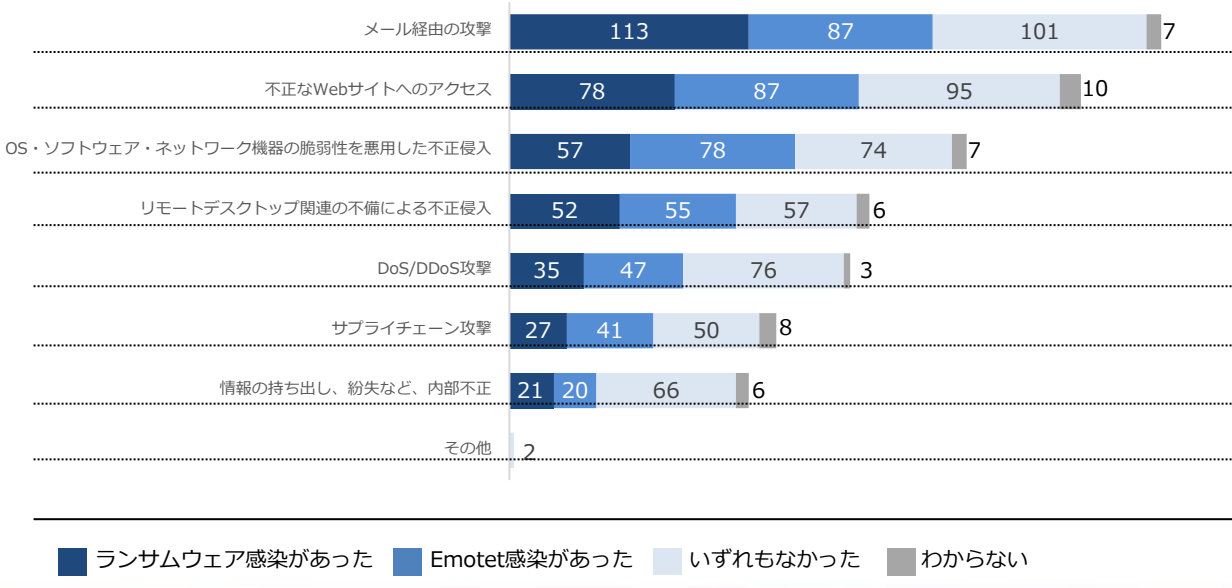
1,277件※のインシデント中、62.5%（798件）がランサムウェア・Emotet感染

「メール経由の攻撃」や「不正なWebサイトへのアクセス」、「脆弱性の悪用」、「リモートデスクトップ関連の不備」によって発生したインシデントでは、ランサムウェア・Emotetの感染割合はいずれも60.0%を超え、中でも「メール経由の攻撃」は70.0%を超えた

※【Q20】のインシデント総件数1,451件から「メール誤送信」の回答174件を減算

（N＝435）

※【Q20】で「インシデントは発生していない」と「誤送信」の回答計565を減算



【ランサムウェア・Emotetの割合】

インシデント被害 件数	ランサムウェア・Emotetの 件数	ランサムウェア・Emotetの 割合
284件	200件	70.4%
255件	165件	64.7%
207件	135件	65.2%
155件	107件	69.0%
151件	82件	54.3%
117件	68件	58.1%
106件	41件	38.7%
2件	0件	0%
計1,277件	計798件	62.5%

-より便利な、より快適な、より安全な
インターネットライフに貢献していく-

DD-11536-001