SOPHOS
Cybersecurity delivered.

ランサムウェアの現状 2022年版

31 か国の中規模組織の IT プロフェッショナル 5,600 人を対象にした、
ベンダーに依存しない独自調査の結果をお届けします。

ソフォス ホワイトペーパー2022年 4月

はじめに

ソフォスが毎年行っている、最前線で働く IT プロフェッショナルが実際に体験したランサムウェアに関する調査で、攻撃環境がかつてないほど厳しくなっていることに加え、ランサムウェアが被害者にもたらす金銭的負担とオペレーションの負荷が増加していることが明らかになりました。また、ランサムウェアとサイバー保険の関係や、サイバー攻撃対策の変革を促す上で保険が果たす役割についても、新たな事実が判明しています。

調査について

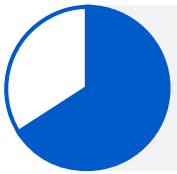
ソフォスが調査会社 Vanson Bourne 社に委託して、31 か国の中規模組織 (従業員数 100～5,000 人) に所属する 5,600 人の IT プロフェッショナルを対象に、ベンダーにとらわれない独立した調査を実施しました。調査は 2022 年 1 月から 2 月にかけて実施され、回答者には前年の経験に基づいて回答するよう依頼しました。

攻撃は増加し、その複雑さと影響も拡大している

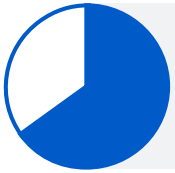
ランサムウェア攻撃を受けた組織の割合は、2020 年の 37% から増加し、2021 年は 66% でした。これは 1 年間で 78% の増加であり、攻撃者が極めて深刻な攻撃を大規模に実行する能力がかなり向上していることを示しています。 また、攻撃に必要なスキルレベルを下げることでランサムウェアの展開範囲を大幅に拡大する RaaS (Ransomware-as-a-Service: サービスとしてのランサムウェア) モデルが一層成功を収めていることも反映していると思われます。[注: ランサムウェアによる被害は、1 台以上のデバイスが攻撃の影響を受けた、さらに暗号化の有無は問わないと定義しました。]

また、攻撃によりデータの暗号化に成功する確率が高まっています。 2021 年、攻撃者は攻撃の 65% でデータの暗号化に成功しており、2020 年に報告された暗号化率 54% から上昇しています。しかし、データは暗号化されなかったが、「データを公開する」と脅迫して身代金を要求する恐喝だけの攻撃を経験した被害者の割合は、7% から 4% に減少しています。

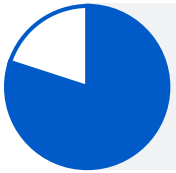
ランサムウェア攻撃が増加しているというこの現状は、厳しさと範囲が拡大している脅威環境の一端を担っています。たとえば、昨年 1 年間で、57% がサイバー攻撃全体の件数の増加を経験し、59% が攻撃が複雑化しているのを確認し、53% が攻撃の影響が増大したと回答しています。そして 72% は、これらの領域のうち少なくとも 1 つで増加を実感しています。



66%
昨年ランサムウェア攻撃を受けた企業の割合



65%
データが暗号化された攻撃の割合



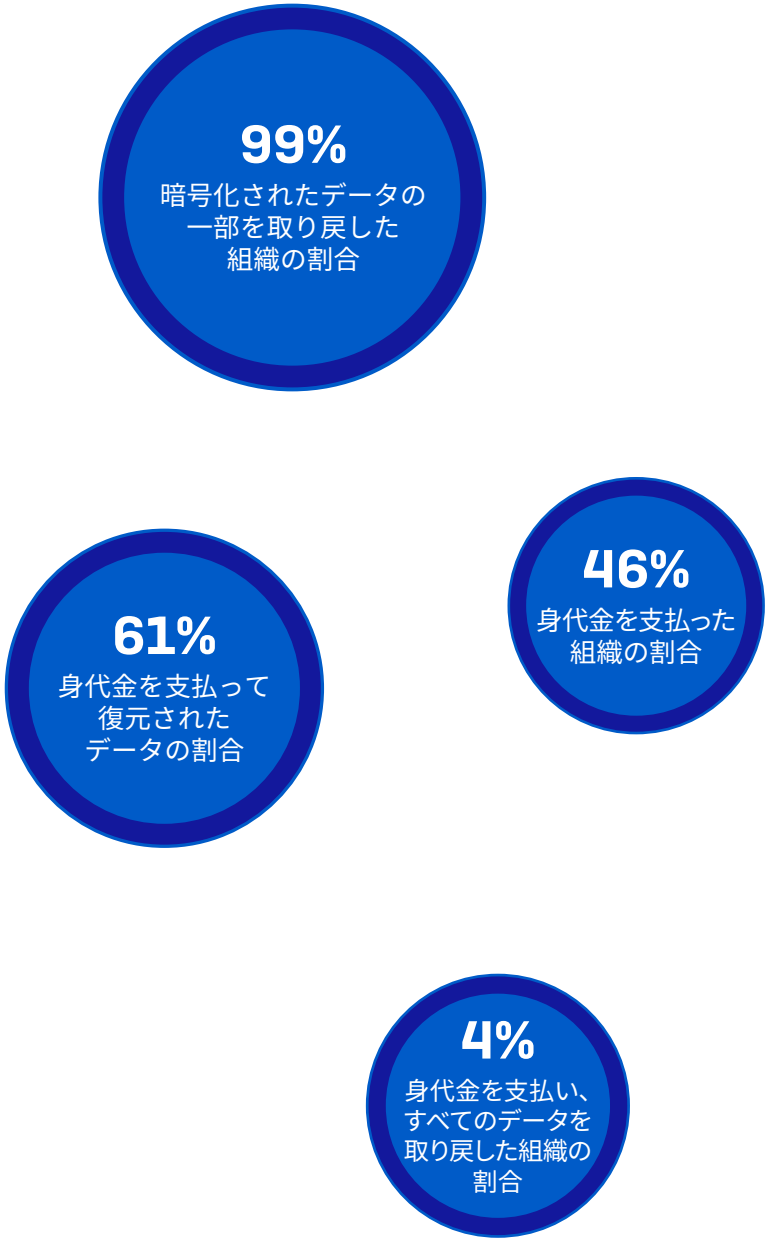
72%
サイバー攻撃の件数/複雑さ/影響の増大を経験した企業の割合

攻撃後にデータを復元する組織のスキルは上達している

ランサムウェア攻撃の拡大を受けて、防御する側の組織は攻撃の影響に対処するスキルを高めてきています。昨年ランサムウェアの被害を受けたほぼすべての組織 (99%) が、暗号化されたデータの一部を取り戻しており、これは昨年の 96% からわずかに増加しています。

データを復元するために用いられる方法の第 1 位はバックアップで、データが暗号化された組織の 73% で使用されています。同時に、46% がデータを復元するために身代金を支払ったと報告しています。この数字は、多くの組織が復旧のスピードと効果を最大化する目的で、複数の復元方法を用いていることを反映しています。全体的には、データが暗号化された組織の回答者のほぼ半数 (44%) が、データを復元するのに複数の方法を使用していました。

身代金を支払えば、大抵はある程度のデータを取り戻せますが、支払い後にデータが復元される割合は低下しています。平均して、身代金を支払った組織が取り戻せたデータは 61% に過ぎず、2020 年の 65% から減少しています。同様に、身代金を支払った組織のうち、すべてのデータを取り戻した組織は 2021 年ではわずか 4% で、2020 年の 8% から減少しています。



身代金の支払いは増加している

身代金を支払った組織の回答者のうち、正確な金額を教えてくれたのは 965 名で、平均的な身代金支払額が昨年かなり増加したことが明らかになりました。

昨年 1 年間で、100 万米ドル以上の身代金を支払った被害者の割合が、2020 年の 4% から 2021 年は 11% とほぼ 3 倍に増加しています。これと並行して、1 万米ドル未満を支払った割合は、2020 年の 3 人に 1 人 (34%) から、2021 年には 5 人に 1 人 (21%) に減少しています。

全体として、身代金の平均支払額は 81 万 2,360 米ドルとなり、2020 年の平均 17 万米ドルから 4.8 倍となりました (回答者 282 名)。この金額は、8 桁の身代金支払いが 15 件あったことに影響されていますが、全体的に身代金が上昇傾向にあることはこのデータから明らかです。業種によってかなりの差があり、攻撃者は最も支払能力があると思われる相手から最も高額な身代金を引き出しています。

- 身代金の平均額が最も高かったのは、製造業および生産業の 204 万米ドル (n=38)、エネルギー、石油/ガス、公益サービスの 203 万米ドル (n=91) でした。
- 身代金の平均額が最も低かったのは、医療の 19 万 7,000 米ドル (n=83)、地方自治体/州政府の 21 万 4,000 米ドル (n=20) でした。

イタリアでは恐喝は違法であり、組織が身代金を支払うことは法律で禁じられていますが、データを暗号化された組織の 43% が、身代金を支払ったことを認めています (n=76)。この調査によって、法律の障壁を設けるだけでは犯罪者への身代金の支払いを効果的に阻止できないことが実証されました。

3x
100 万米ドル以上の身代金を支払った被害者の割合が増加

21%
1 万ドル未満の身代金を支払った組織

$ 812,360
身代金の平均支払額 (異常値を除く)

製造、公共サービス
身代金の平均支払額が最も高い (200 万ドル)

医療
身代金の平均支払額が最も低い (19 万 7 千ドル)

ランサムウェアは商業面および業務面で大きな影響を及ぼす

身代金の額は物語の一部に過ぎず、ランサムウェアの影響は暗号化されたデータベースやデバイスだけでなく、はるかに広範囲に及びます。昨年ランサムウェアの被害を受けた企業の 90% は、最も深刻な攻撃によって業務遂行能力が影響を受けたと回答しています。さらに、民間企業では、86% が取引/収入の損失を招いたと回答しています。

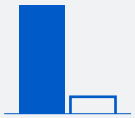
全体的には、2021 年に直近で受けたランサムウェア攻撃の影響を復旧するために組織が負担した平均コストは 140 万米ドルでした。2020 年の 185 万米ドルからの大幅な減少は、ランサムウェアの普及に伴い、攻撃による風評被害が軽減 (一般化) されたことを反映していると考えられます。同時に、保険会社はインシデント対応プロセスにおいて被害者に迅速かつ効果的なガイダンスを提供できるようになり、復旧コストが削減されています。

なお、身代金が支払われる場合、その費用を負担するのは被害者ではなく保険会社であるケースが多いようです。詳細は本レポートで後ほど扱います。

昨年攻撃を受けた企業は、最も深刻だった攻撃からの復旧に平均 1 か月を要しました (多くの企業にとって、1 か月は長すぎます)。最も復旧が遅かったのは高等教育機関と中央/連邦政府で、約 5 人に 2 人が 1 か月以上を要したと報告しています。一方、最も復旧が早かったのは製造・生産 (1 か月以上かかったのは 10%) と金融サービス (1 か月以上かかったのは 12%) で、これは復旧計画や準備のレベルが高かった結果と思われます。

さらに、一部の組織は効果のない防御策を未だ信頼し続けています。昨年ランサムウェアの被害に遭わず、今後も遭わないと考えている回答者のうち、72% が実際には組織への攻撃を阻止できないアプローチを根拠に回答していました。攻撃の被害に遭わないと考える理由として 57% がバックアップを、37% がサイバー保険を挙げており、中にはその両方を挙げていた回答者もいました。これらの要素は、攻撃からの復旧には役立っても、攻撃そのものを防ぐことはできません。

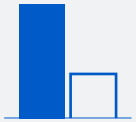
90%
ランサムウェア攻撃によって業務遂行能力が影響を受けたと回答



86%
ランサムウェア攻撃が取引/収入の損失を招いたと回答

140 万ドル
攻撃の平均復旧コスト

1 か月
攻撃からの復旧に要する平均時間



72%
攻撃を防止できないアプローチに信頼を置いている

多くの組織が、ランサムウェアを阻止するために予算とリソースを効果的に使えていない

今回の調査では、人員と予算をつぎ込むだけでは問題を解決できないことや、むしろ必要なのは適切なテクノロジーへの投資とそれを効果的に活用するスキルやノウハウであることが明らかになりました。これがなければ、投資対効果は低くなってしまいます。

昨年ランサムウェア攻撃を受けた企業の 64% は、必要以上のサイバーセキュリティ予算があると回答し、さらに 24% は適切な額の予算があると回答しています。同様に、ランサムウェアの被害者の 65% は、必要以上のサイバーセキュリティ人員を配置していると回答し、23% は適切なレベルの人員を配置していると考えています。これらの調査結果からは、多くの組織が急激に増加する攻撃の件数と複雑さに直面する中で、リソースの効果的な配備に苦慮していることが伺えます。

また、最新の攻撃手法を阻止するための適切なスキルがないことに、組織が気付いていない可能性も示唆されています。ランサムウェアの被害に遭った 58% は、疑わしい信号やアクティビティの特定を目的としたログの確認について、自社ではほぼ/完全に取り組んでいると回答し、56% は最新の攻撃ツールや手法についてほぼまたは完全に取り組んでいると回答しています。

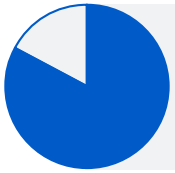
逆に、前年にランサムウェアの被害を受けず、今後も攻撃を受けると予想していない組織では、トレーニングを受けた IT セキュリティスタッフまたは攻撃を阻止する能力を備えたセキュリティオペレーションセンター (SOC) を社内に擁していることがその自信の背景あります。

ランサムウェアがきっかけでサイバー保険への加入が増加

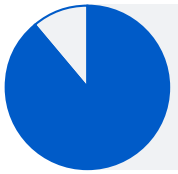
中規模組織の 5 社に 4 社以上がランサムウェアに対応したサイバー保険に加入しています。しかし、回答者の 83% がランサムウェアの被害を補償するサイバー保険に加入していると回答している一方で、34% は保険契約に除外事項/例外事項があると回答しています。エネルギー、石油/ガス、公共サービスでは、保険に加入している割合が最も高く (89%)、次いで小売業 (88%) となっています。サイバー保険への加入は組織の規模に合わせて増加し、従業員数 3,001～5,000 人の組織では 88% が保険に加入しているのに対し、100～250 人の組織では 73% にとどまっています。

昨年ランサムウェアの被害に遭った組織は、被害に遭わずに済んだ組織に比べて、サイバー保険への加入率が非常に高くなっています。被害を受けた組織では、89% がサイバー保険に加入しているのに対し、被害を受けなかった組織では 70% が加入しています。現時点ではその因果関係は明確ではありません。ランサムウェアのインシデントを直接経験したことで、多くの組織が将来的に攻撃の影響を軽減するために保険に加入するようになったのかもしれません。あるいは、攻撃者は、身代金が支払われる可能性を高めるために、保険に加入していることが分かっている組織を標的にするかもしれません。また、防御の弱点を補う目的で保険に加入する組織もあるようです。実際は、上記の 3 つの組み合わせであると思われます。

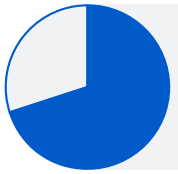
サイバー保険の加入率は、攻撃を受けておらず、今後も攻撃を受けるとは考えていない組織の間では 61% まで低下しています。このグループの多くが、ランサムウェアを阻止できないアプローチに信頼を置いており、保険に加入していないということは、インシデント発生時にはコストをすべて被ることになります。



83%
ランサムウェアに対応する
サイバー保険に加入している



89%
ランサムウェアの被害に遭い
サイバー保険に加入している



70%
ランサムウェアの被害に遭っていないが
サイバー保険に加入している

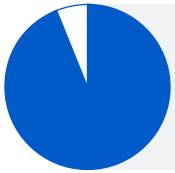
サイバー保険はサイバー攻撃対策の改善を促進する

サイバー保険に加入している組織の 94% が、保険加入のプロセスが昨年に比べて変わったと回答しています。

- 54% が「加入に求められるサイバーセキュリティのレベルが高くなった」と回答
- 47% が「保険が以前よりも複雑になった」と回答
- 40% が「サイバー保険を提供する会社が少なくなった」と回答
- 37% が「以前よりも手続きに時間がかかる」と回答
- 34% が「以前よりも高額になった」と回答

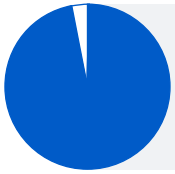
サイバー保険の大幅な値上げが 2021 年第 2 四半期と第 3 四半期に始まったことを考えると、調査時点ではこの変化の影響を経験していない回答者が多かったと思われます。

サイバー保険市場が硬直化し、加入が難しくなる中、サイバー保険に加入している組織の 97% が、サイバー保険の等級を向上させるためにサイバー攻撃対策に変更を加えていることが判明しました。64% が新しいテクノロジー/サービスを導入し、56% がスタッフのトレーニング/教育を強化し、52% がプロセス/行動を変更しました。



94%

過去1年間でサイバー保険への加入が難しくなったと感じた組織の割合



97%

サイバー保険に加入していて、サイバー保険の等級を上げるために攻撃対策に変更を加えた組織の割合

ほぼすべてのランサムウェアの請求で サイバー保険金が支払われている

サイバー保険に加入している組織にとって心強いことに、ランサムウェアの被害に遭い、ランサムウェアをカバーするサイバー保険に加入していた 98% が、最も深刻な攻撃で保険金が支払われたと回答しています (2019 年には 95% でした)。以下に挙げる多くの国で、支払われる割合は 100% に上昇しました。スイス (n=52) 、メキシコ (n=131) 、スウェーデン (n=68)、ベルギー (n=66)、ポーランド (n=75)、トルコ (n=51)、UAE (n=49)、インド (n=218)、シンガポール (n=91)。

サイバー保険の補償内容を調査したところ、クリーンアップ費用の支払いは増加し、身代金の支払いは減少していることが明らかになりました。77% の回答者が、クリーンアップ費用 (業務を再開させるために発生したコスト) を保険会社が支払ったと回答しており、2019 年の 67% から増加しています。逆に、保険会社が身代金を支払ったと回答したのは 40% で、2019 年の 44% から減少しています。

ただし、身代金が支払われる割合は業種によってかなりの差がありました。最も高かったのは、低学年教育 (K-12/初等・中等教育) (53%)、地方自治体 (49%)、医療 (47%) で、最も低かったのは製造・生産 (30%) と金融サービス (32%) です。興味深いことに、身代金の支払い率が最も低い業種は、最も短時間でインシデントから復旧できる業種でもあり、このことからディザスタリカバリ (災害復旧) の計画と準備の重要性が浮き彫りになっています。

サイバー保険は以前の状態への復旧を支援してくれますが、「改善」、つまり攻撃につながった脆弱性に対処する優れたテクノロジーやサービスへの投資についてはカバーできないことを覚えておく必要があります。

98%
ランサムウェアの請求で保険金が支払われる割合

△ クリーンアップコストの支払い △

2019	2021
67%	77%

▽ 身代金の支払い ▽

2019	2021
44%	40%

まとめ

組織が直面するランサムウェアの問題は増加する一方です。ランサムウェアの影響を直接受けた組織の割合は、2020 年の 3 分の 1 強から 2021 年には 3 分の 2 と、12 か月でほぼ倍増しています。

このように常態化しつつある中で、防御する側の組織は攻撃の影響への対処能力を高めてきています。ほぼすべての組織が暗号化されたデータの一部を取り戻し、約 4 分の 3 がバックアップを使用してデータを復元できるようになっています。

同時に、身代金を支払った後に暗号化されたデータが復元された割合は低下し、平均で 61% になっています。にもかかわらず、100 万ドル以上の身代金を支払う被害者の割合は、3 倍近くに増加しています。

今回の調査では、人員と予算をつぎ込むだけでは問題を解決できないことや、むしろ必要なのは適切なテクノロジーへの投資とそれを効果的に活用するスキルやノウハウであることが明らかになりました。組織は、サイバーセキュリティへの投資効果を向上させ、防御力を高めることができる専門家との提携を検討する必要があります。

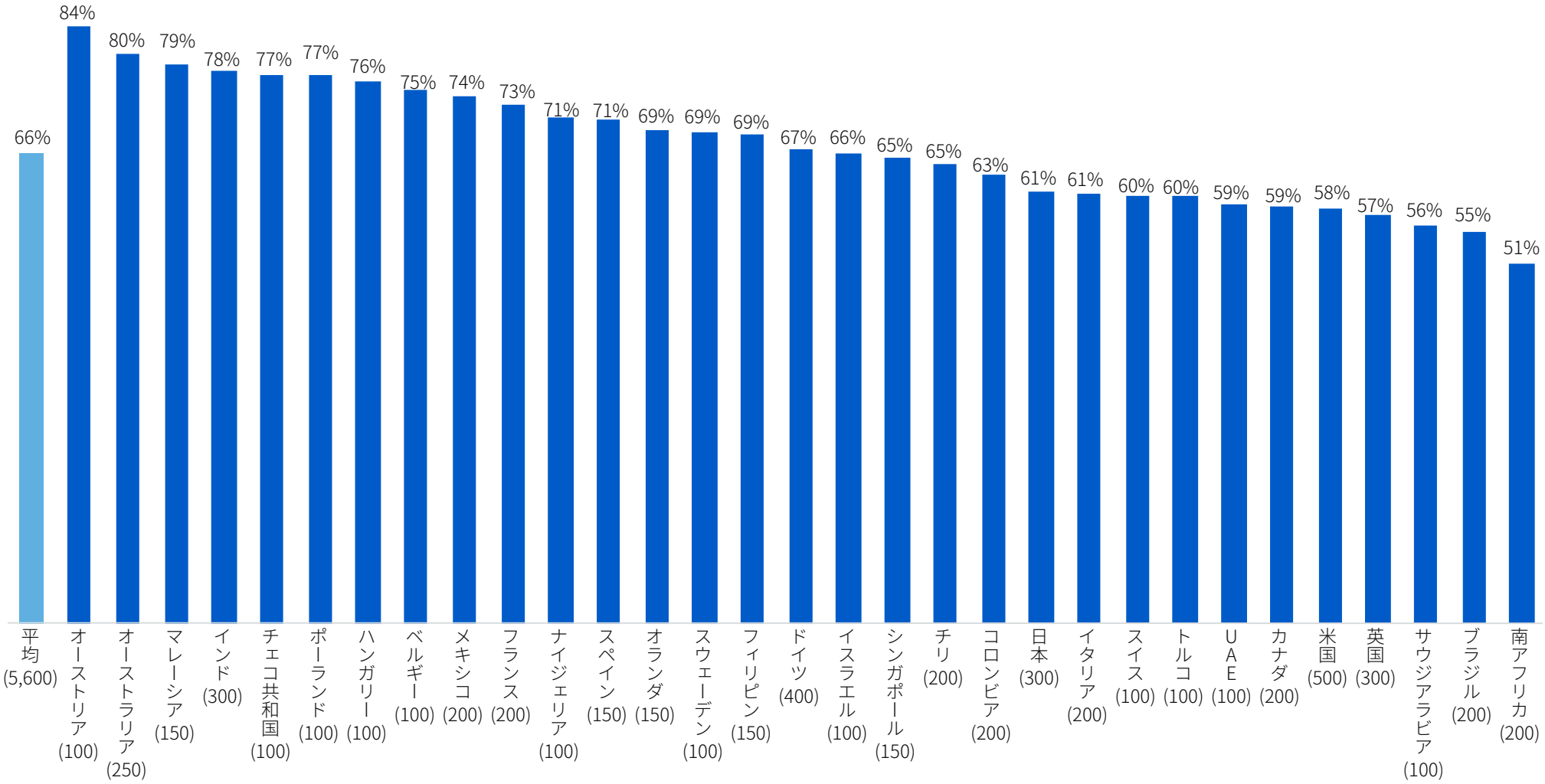
ほとんどの組織は、サイバー保険に加入することで、攻撃に関連した金銭的リスクを軽減しようとしています。そうした組織にとって、保険会社がほぼすべての請求に対して何らかの費用を負担してくれることは心強いことです。しかし、保険への加入は以前より難しくなっているため、ほとんどの組織がサイバー保険の等級を上げるために、サイバー攻撃対策を変更する必要に迫られています。

保険への加入を検討しているかどうかにかかわらず、サイバーセキュリティを最適化することは、すべての組織にとって必要不可欠です。ソフォスからの主なアドバイスは次の 5 つです。

- 自社のすべてのポイントに高品質なエンドポイント保護製品を導入してください。既存のセキュリティコントロールを見直し、今後もニーズに応えられるようにしてください。
- プロアクティブに脅威を発見し、攻撃が実行される前に攻撃者を阻止します。社内に時間的余裕やスキルがない場合は、MDR のプロバイダーにアウトソーシングしてください。
- パッチが適用されていないデバイス、保護されていないマシン、オープンになっている RDP ポートなど、セキュリティギャップを探し出し、塞ぐことでインフラを強化します。Extended Detection and Response (XDR) は、この目的に最適なソリューションです。
- 最悪の事態に備えます。サイバーインシデントが発生した場合に何をすべきか、誰に連絡する必要があるかを把握しておきます。
- バックアップを作成し、そこからデータを復旧します。最小限の混乱で迅速に復旧させることを目標としてください。

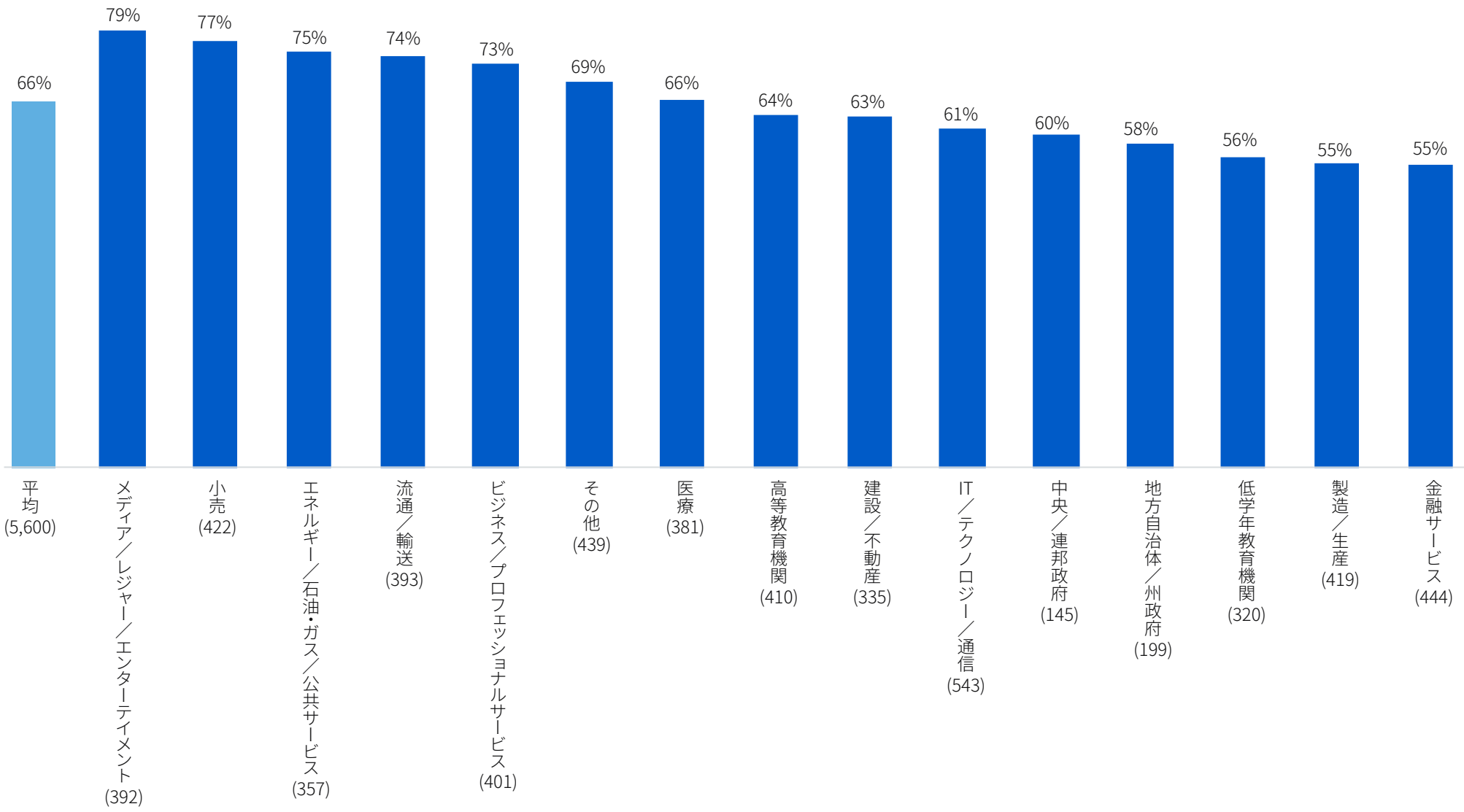
個々のランサムウェアグループの詳細については、ソフォスのランサムウェア脅威インテリジェンスセンターをご覧ください。

昨年ランサムウェア攻撃を受けた企業の割合



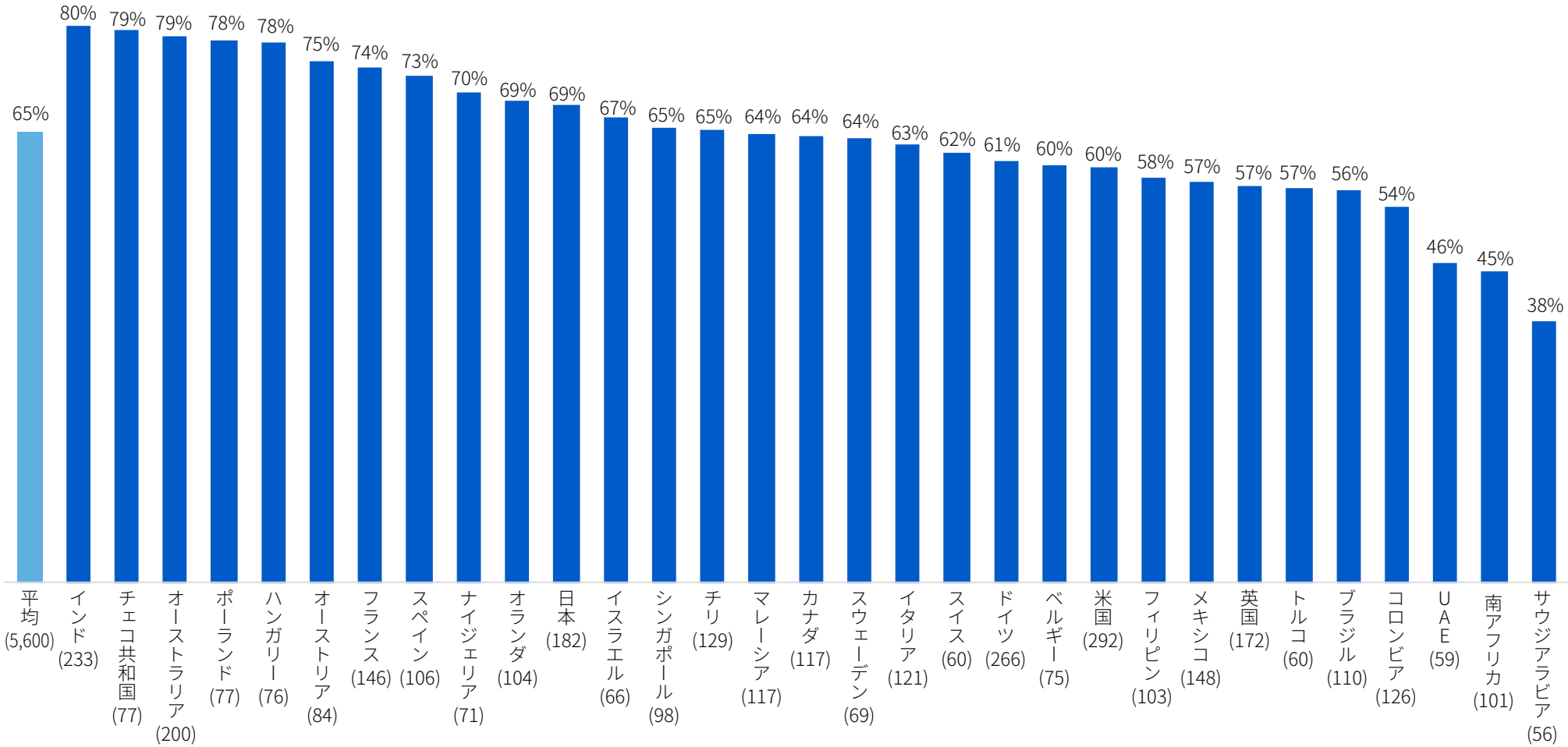
「昨年、ランサムウェア攻撃を受けましたか？」 (n=5,600) :「はい」

昨年ランサムウェア攻撃を受けた企業の割合



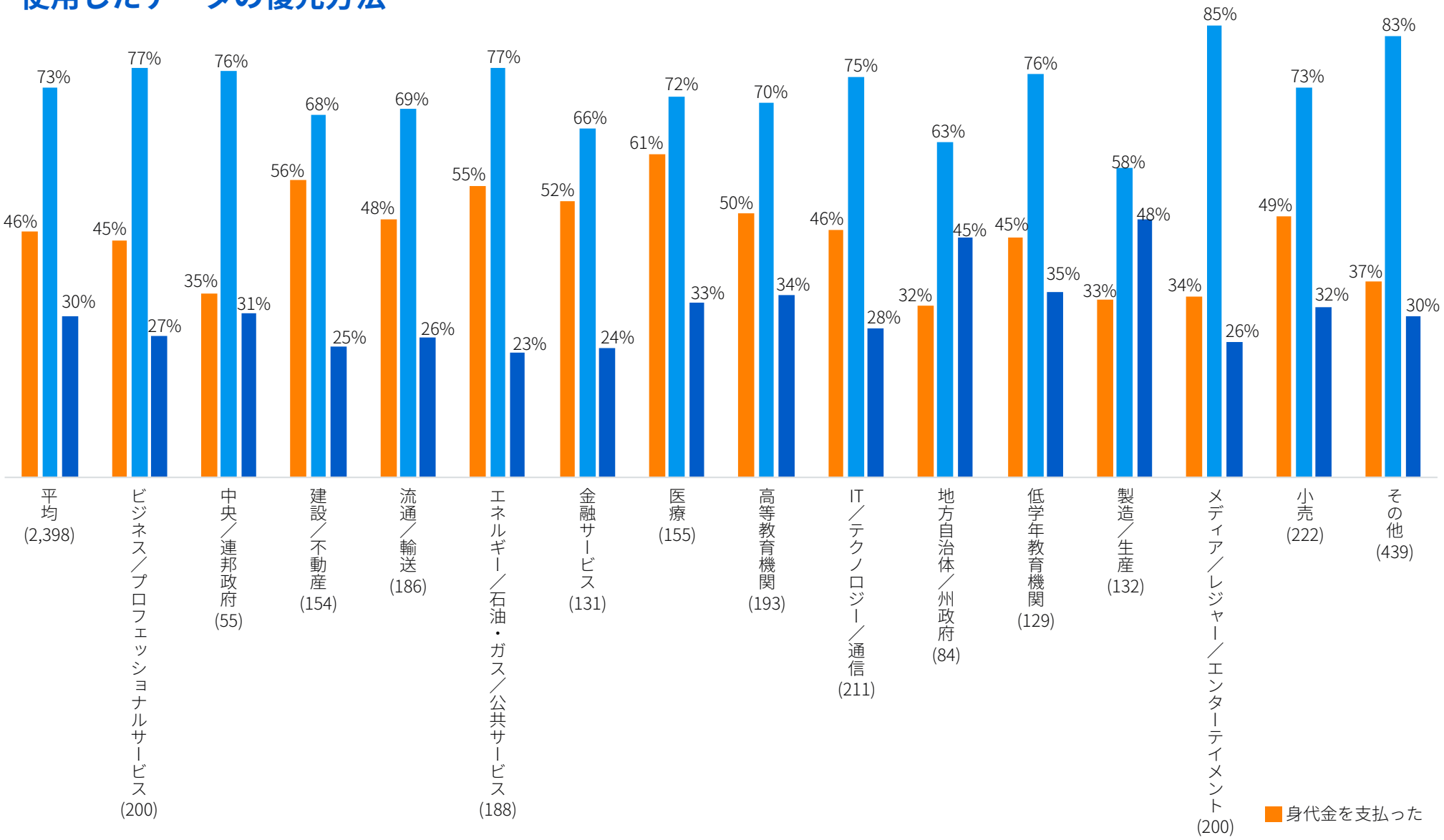
「昨年、ランサムウェア攻撃を受けましたか？」(n=5,600):「はい」

ランサムウェア攻撃で暗号化される割合



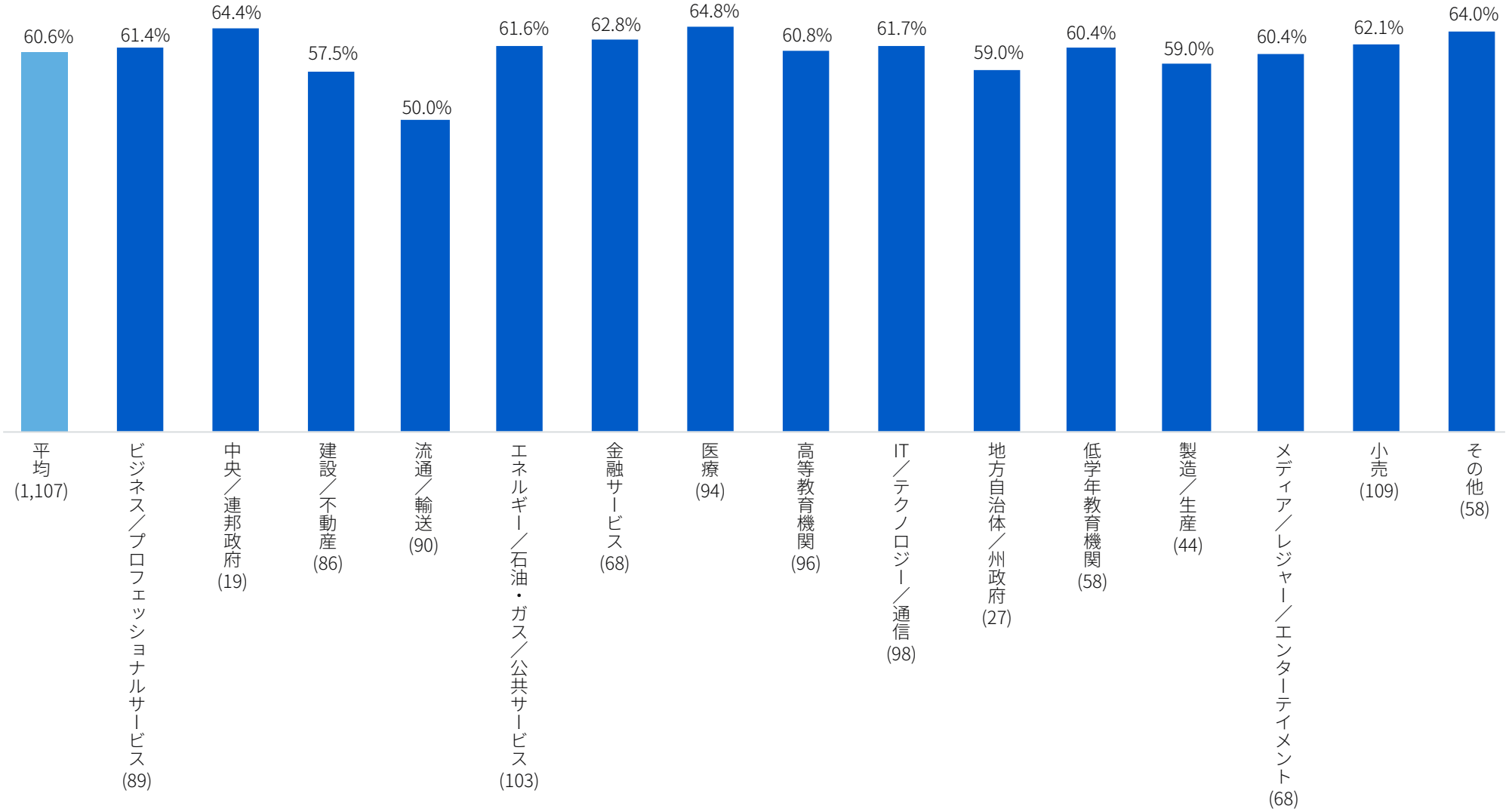
「最も深刻なランサムウェア攻撃においてデータは暗号化されましたか？」
(n=3,702、昨年ランサムウェア攻撃を受けた組織): 「はい」

使用したデータの復元方法



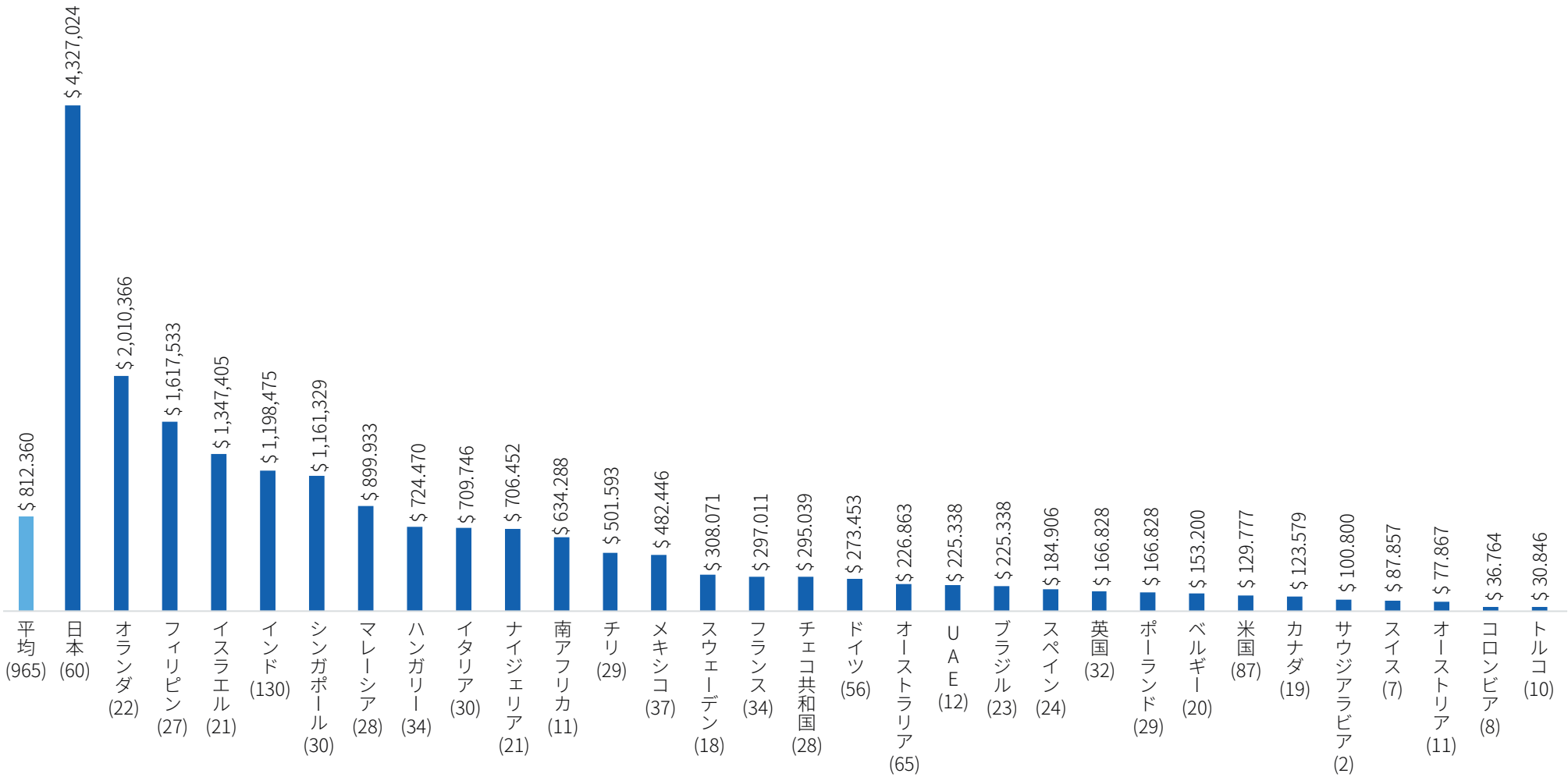
「最も深刻なランサムウェア攻撃においてデータを取り戻すことができましたか？」(n=2,398、データが暗号化された組織):
「はい、身代金を支払ってデータを取り戻しました。」「はい、バックアップを使用してデータを復元しました。」「はい、他の手段でデータを取り戻しました。」

身代金を支払って復元できたデータの割合



「最も深刻なランサムウェア攻撃において、どの程度データを取り戻すことができましたか？」
(n=1,107、身代金を支払いデータを取り戻した組織)

身代金の平均支払い額 (国別)



「最も深刻なランサムウェア攻撃において、支払った身代金はいくらでしたか？」(単位: 米ドル)回答数はグラフ内。「わからない」と異常値は除外。
注: 回答数が少ない国に関しては、参考値としてお考えください。

攻撃の影響の復旧に組織が負担した平均コスト (単位: 100万米ドル)

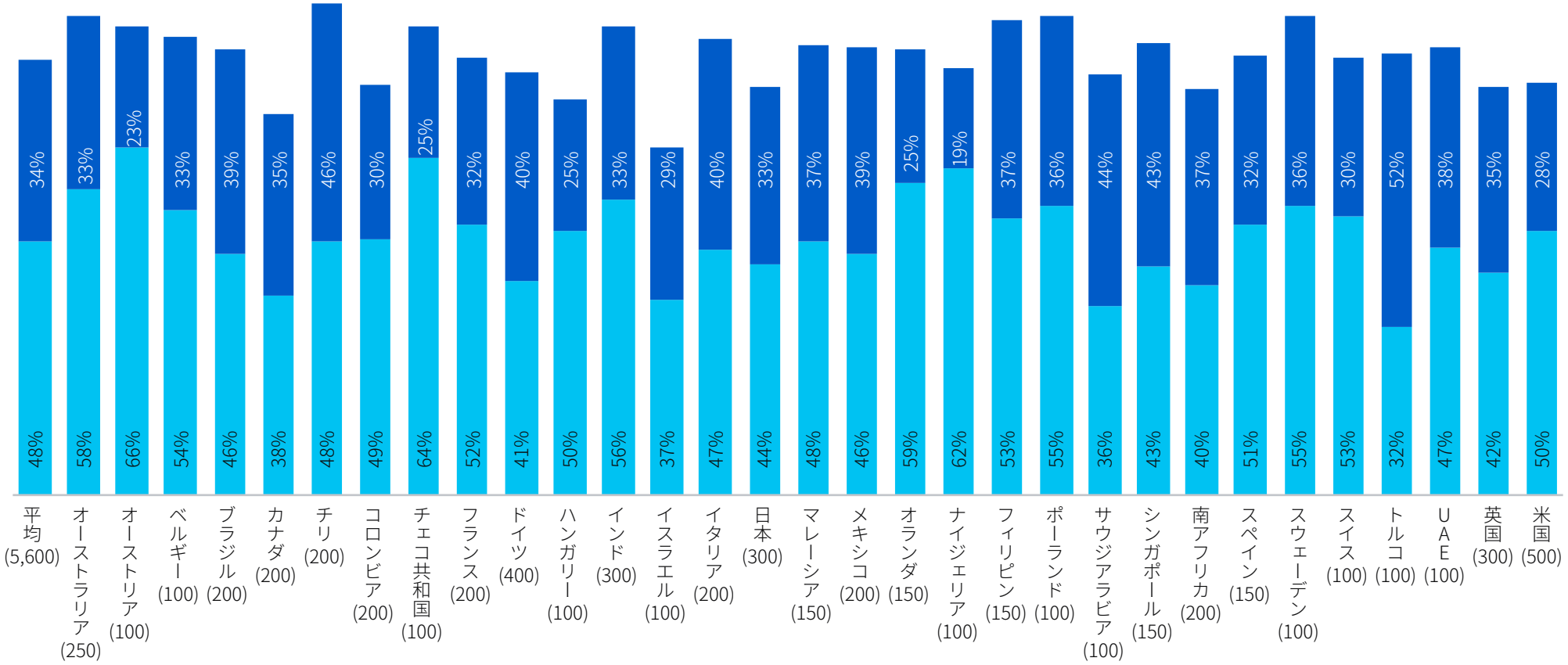
国	2021	2020	対前年増減率
平均 (3,702)	$ 1.40	$ 1.85	-24%
オーストラリア (200)	$ 1.01	$ 1.84	-45%
オーストリア (84)	$ 0.81	$ 7.75	-90%
ベルギー (75)	$ 3.71	$ 4.75	-22%
ブラジル (110)	$ 0.69	$ 0.82	-16%
カナダ (117)	$ 0.65	$ 1.92	-66%
チリ (129)	$ 1.58	$ 0.73	116%
コロンビア (126)	$ 0.50	$ 1.26	-60%
チェコ共和国 (77)	$ 2.58	$ 0.37	589%
フランス (146)	$ 2.03	$ 1.11	83%
ドイツ (266)	$ 1.73	$ 1.17	48%
ハンガリー (76)	$ 1.51	該当なし	該当なし
インド (233)	$ 2.81	$ 3.38	-17%
イスラエル (66)	$ 1.41	$ 0.57	148%
イタリア (121)	$ 1.65	$ 0.68	141%
日本 (182)	$ 0.96	$ 1.61	-40%
マレーシア (118)	$ 1.22	$ 0.77	58%

国	2021	2020	対前年増減率
メキシコ (148)	$ 0.88	$ 2.03	-57%
オランダ (104)	$ 0.98	$ 2.71	-64%
ナイジェリア (71)	$ 3.43	$ 0.46	644%
フィリピン (103)	$ 1.34	$ 0.82	63%
ポーランド (77)	$ 1.78	該当なし	該当なし
サウジアラビア (56)	$ 0.65	$ 0.21	212%
シンガポール (98)	$ 1.91	$ 3.46	-45%
南アフリカ (101)	$ 0.71	該当なし	該当なし
スペイン (106)	$ 0.75	$ 0.60	25%
スウェーデン (69)	$ 0.75	$ 1.40	-46%
スイス (60)	$ 1.64	$ 1.43	15%
トルコ (60)	$ 0.37	$ 0.58	-36%
UAE (59)	$ 1.26	$ 0.52	144%
英国 (172)	$ 1.08	$ 1.96	-45%
米国 (292)	$ 1.08	$ 2.09	-49%

注: 回答数は 2021年のデータのみ。　　*注: 金額の単位は 100 万米ドル*

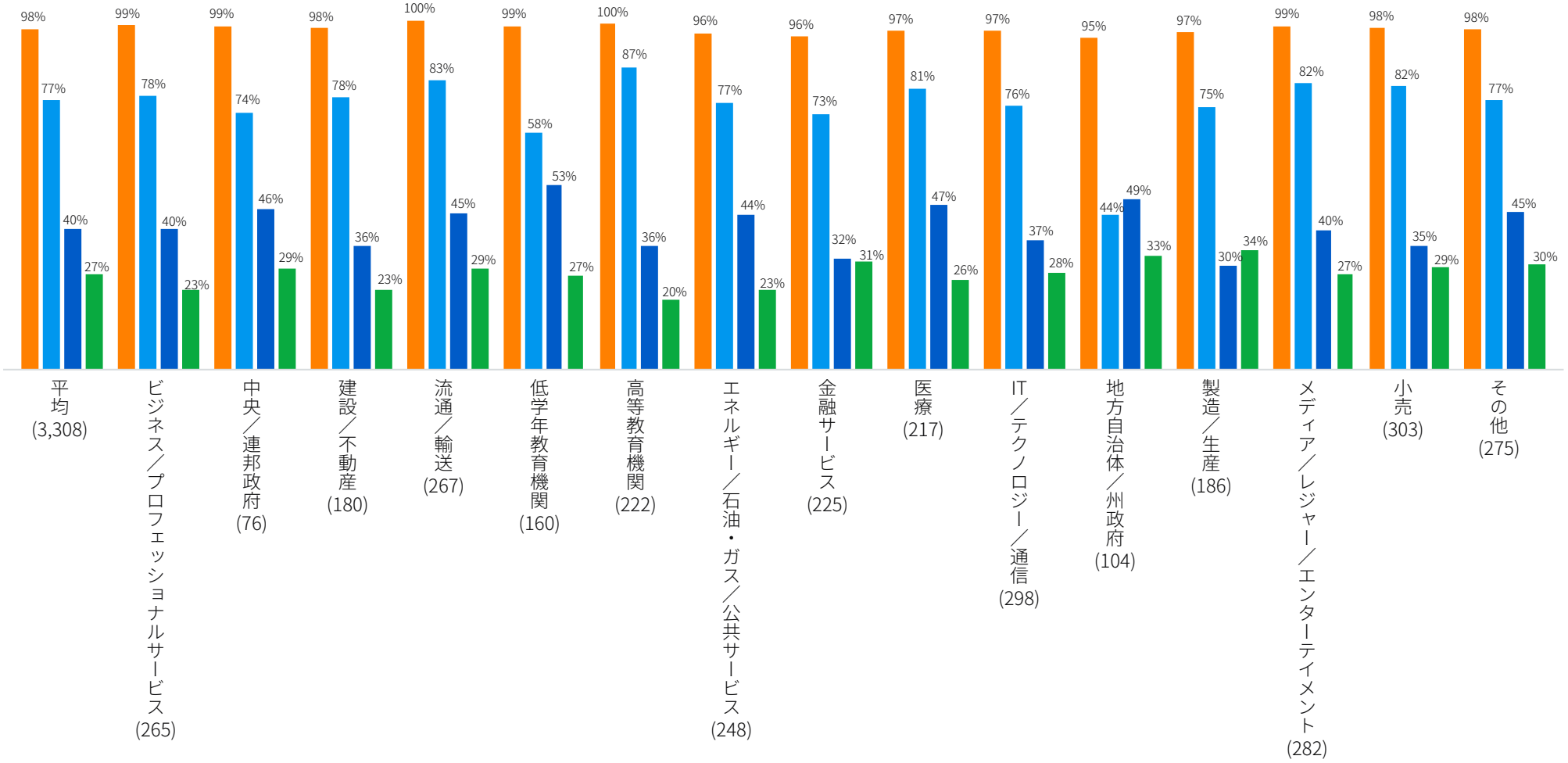
「最近発生したランサムウェア攻撃の影響において、組織が復旧に要した概算コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益、身代金など)はどれぐらいですか？」(n=3,702、前年にランサムウェアの被害を受けた組織)

サイバー保険に加入している組織の割合



「ランサムウェア攻撃を受けた場合に補償を受けられるサイバー保険に加入していますか？」(n=5,600)。「はい」「はい、ただし保険契約に除外事項/例外事項がある」

サイバー保険の支払い率



「組織が受けた最も深刻なランサムウェア攻撃に関連するコストを、サイバー保険は補償してくれましたか？」(n=3,308、前年にランサムウェアの被害を受け、ランサムウェアに対応したサイバー保険に加入していた組織)。「はい、クリーンアップコスト (業務を再開させるためのコストなど) が支払われた。」、「はい、身代金が支払われた。」、「はい、その他のコスト (ダウンタイムコスト、逸失利益など) が支払われた。」

ランサムウェアの詳細と、ソフォス製品がお客様の企業の防御に
どのように役立つかをご覧ください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2022-04-04 (WP-NP)

SOPHOS