SOPHOS
Cybersecurity delivered.

製造/生産業のランサムウェアの現状 2022

世界 31ヵ国の中規模組織の IT 専門家 5,600人のうち製造・生産業 419人を対象とした、ベンダーに依存しない独自調査の結果です。

ソフォス ホワイトペーパー2022年 10月

はじめに

製造・生産業の IT 専門家が実際に体験したランサムウェアに関するソフォスの年次調査により、攻撃はこれまで以上に厳しい環境にあることを明らかにしています。このレポートは、ランサムウェアが被害者に与える経済的および運用上の負担の増大だけでなく、ランサムウェアとサイバー保険の関係性にも注目しています。これには保険がサイバー防御の変化を推進する方法も含まれます。

調査について

ソフォスは調査機関の Vanson Bourne 社に委託して、製造・生産業 419人を含む 5,600人の IT プロフェッショナルを対象に、ベンダーに依存しない独立した調査を実施しました。回答者は、31 か国の中規模組織 (従業員数 100〜5,000 人) に所属する人達です。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。

5,600人
回答者数

419人
製造・生産業の回答者

31
か国

100〜5,000 名
従業員

2022年 1〜2月
調査の実施期間

ランサムウェア攻撃は昨年よりも増加

ランサムウェア攻撃を受けた製造・生産業の割合は、2020 年の 36% から 2021 年では 55% へと増加しました。これは 1 年間で 52% 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。[注: ランサムウェアによる被害の定義とは、1 台以上のデバイスで影響を受けたが、暗号化の有無は問わないとしています。]

実際、製造・生産業は、2021年のすべてのセクターでランサムウェア攻撃の割合が最も低い (金融業も同様) と報告されています。しかし、すべての業界の回答者の半数以上が昨年攻撃を受けたと報告しており、実際には、すべての組織が攻撃を受けた可能性が高くなります。

ランサムウェアの被害を受けた製造・生産業の半数以上 (57%) が、サイバー犯罪者によってデータが暗号化されたと報告しています。ここでも、すべての業界で最も低い割合が報告されています。なお、すべての業界の平均データ暗号化率は 65% でした。

データが暗号化される前に攻撃を阻止できたと回答した製造・生産業は 38% で、業界間平均の 31% を上回っています。これは、この業界の組織が、新しいテクノロジーの導入、スタッフのトレーニングの増加、プロセスの変更など、サイバー保険の位置づけを改善させるための変更が肯定的な結果をもたらせた可能性があります。詳細については、後ほどこのレポートで説明します。

ランサムウェア攻撃の増加は、あらゆる業界の組織に影響を及ぼしている、ますます課題となっている脅威環境の一部です。すべての業界で回答者は、サイバー攻撃の量、複雑さ、影響が増加していると報告しています。

製造・生産業では、脅威の状況の変化によって特に影響を受けており、回答者の 61% が、過去 1年間にわたり組織に対する攻撃の量が増加したと報告し (業界間の平均 57%)、66% が攻撃の複雑さが増している (業界間の平均 59%) と報告しています。

攻撃に関しては、この業界のデータの暗号化を阻止する優れた能力により、攻撃者が技術を向上させることを余儀なくされているかもしません。あるいは、この 1年間でサイバー犯罪者のこの業界への関心の高まりが反映されているのかもしれません。

製造・生産業に対する攻撃の影響の変化に関しては、半数強 (51%) が過去 1年間で増加したと報告しており、これは業界の平均とほぼ一致しています。

ランサムウェア攻撃ありの組織

55%
製造・生産業 - 業界で最も低い

66%
業界全体の平均

攻撃で暗号化されたデータ

57%
製造・生産業

65%
業界全体の平均

攻撃の件数、複雑さ、影響力の昨年の増加率

	サイバー攻撃の件数の増加率	サイバー攻撃の複雑さの増加率	サイバー攻撃の影響の増加率
製造/生産	61%	66%	51%
業界全体の平均	57%	59%	53%

被害者のほとんどは暗号化データを復元

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。ランサムウェアの被害を受け、データが暗号化されたほぼすべての製造・生産業 (96%) が暗号化されたデータの一部を過去 1年間で取り戻しました。

製造・生産業は、すべての業界でバックアップの使用率が最も低いと報告されており、暗号化されたデータを復元するためにこのアプローチを使用する回答者は、業界全体の平均である 73% と比較してわずか 58% でした。また、この業界では、製造・生産業の 68% がデータの復元のためにバックアップを使用していた前年と比較して、バックアップの使用率が減少していることも報告されています。これは、ランサムウェアやその他多くのインシデントからの復旧にバックアップが不可欠であることから、懸念すべき結果です。

興味深いことに、バックアップの使用率が低くても、身代金の支払い率が高いというわけではありませんでした。また、この業界は、2021年の身代金支払い率が最も低い業界の 1つであり、製造・生産業の回答者の 3人に 1人 (33%) しか身代金を支払っていませんでした。とはいえ、これは 2020年に身代金を支払った製造・生産業の 19% のほぼ 2倍にあたります。

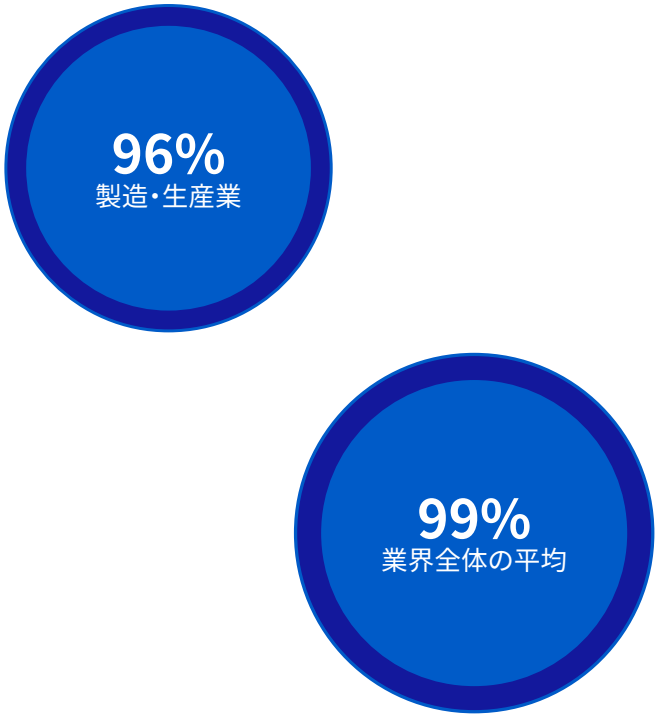
さらに、回答者の約半数 (48%) が、データの復元に他の手段を使用したと報告しています。

バックアップ、身代金の支払い、その他の手段を使用する割合を合計すると割合は明らかに 100% を超えます。これは、多くの製造・生産業が複数の復元方法を平行して使用して、インシデントの復旧を早めていることを示しています。全体として、製造・生産業の被害者の 36% が、複数の　方法を使用してデータを復元しました。

複数の復元方法を使用した割合

	身代金を支払った	バックアップを使用した	その他の方法を使用した	複数の方法を使用した
製造/生産	33%	58%	48%	36%
業界全体の平均	46%	73%	30%	44%

一部復元された暗号化データ



身代金支払い後に復元されるデータは減少

すべての業界で、身代金を支払った後のデータ平均復元率は、この 1年間で減少し、2020年では 65% だったのが 2021年では 61% となっています。この世界的な傾向に反して、製造・生産業の回答者は、復元されたデータの量が 2020年の 55% から 2021年には 59% に実際には 1年間でわずかに増加していることを確認しました。この増加は心強いものですが、回答者は平均して暗号化されたデータの 3分の 2以下しか取り戻せていないという事実が依然として残っています。

同時に、すべてのデータを取り戻した製造・生産業の割合は、前年比 7% で一定のままでした。

ここで重要なのは、身代金を支払っても、暗号化されたデータの一部しか復元されない可能性があるということです。暗号化されたすべてのデータが正常に復元される可能性は低いです。

身代金を支払って復元されたデータの割合

59%
製造・生産業

61%
業界全体の平均

身代金を支払った後に、すべてのデータを取り戻した被害者の割合

7%
製造・生産業

4%
業界全体の平均

身代金の支払いが最も多かった製造・生産業

あらゆる業界で、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 2021年にかなり増加したことが明らかになりました。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)。

製造・生産業の回答者 38 人が、正確な身代金の支払い額を共有し、平均身代金が 2,036,189ドルという、すべての業界の中で最も高い金額であることが明らかになりました。これは、製造・生産業の回答者 15人が 2020年に報告した 147,917ドルから大幅に増加しています。注: 2020年の平均身代金額は、低い回答数に基づくものであり、統計的に有意というよりは、指標としてみなす必要があります。

身代金の支払いをさらに掘り下げてみると、製造・生産業は、すべての業界の中でも身代金の広がりが最も大きい業界の 1つであり、回答者は幅広い支払い範囲を報告しています。回答者の 10人に 1人 (11%) が 1千米ドル未満を支払った一方で、回答者のほぼ 3分の 1 (37%) が 10万米ドル以上を支払っています。回答者の 8% が 100 万米ドル以上を支払いました。

非常に高額な多くの身代金が、全体的な平均を押し上げていますが、支払額は明らかに前年比で増加傾向にあります。

製造・生産業が支払う身代金:

203.6万米ドル 製造・生産業

81.2万米ドル 業界全体の平均

11%
1,000米ドル未満の支払い

37%
10万米ドル以上の支払い

8%
100万米ドル以上の支払い

製造・生産業に大きな影響を及ぼすランサムウェア

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をはるかに超えて組織に影響を与えるため、身代金の総額は話の一部に過ぎません。

ランサムウェアの被害を受けた製造・生産業の 77% が、攻撃が運用能力に影響を与えたと回答し (業界平均:90%)、71% が攻撃が組織のビジネス/収益を失う原因になったと回答しています (業界平均:86%)。これらの割合は、業界平均を下回っていますが、ランサムウェアが運用や収益に与える影響が大きいことを反映しています。

業務遂行能力への影響

77%
製造・生産業

90%
業界全体の平均

ビジネス/収益への影響

71%
製造・生産業

86%
業界全体の平均

ランサムウェア攻撃の修復コストの減少

すべての業界の全体的な修復に関しては、直近で受けたランサムウェア攻撃の影響を修復するための平均コストは、2020年の 185万ドルから、2021年では 140万ドルに減少しています。

この傾向に伴い、製造・生産業のランサムウェア攻撃を修復するために費やした全体的な費用は昨年より減少し、2020年の 152万米ドルから 2021年には 123万米ドルになりました。とはいえ、123万米ドルは依然として非常に大きな金額であり、あらゆる業界の中小企業組織に多大な影響を与える可能性があります。

一見すると、平均的な復旧請求額が平均的な身代金支払い額よりも少ないというのは常識では理解しがたいかもしれません。しかし、多くの場合、保険会社が身代金の支払いを補償しています。

製造・生産業の復旧請求額が平均を下回る要因としていくつかが考えられます。まずは、ランサムウェアがこの業界の運用と収益に与える影響が平均より低いことです。次に、データが暗号化される前に攻撃を阻止するこの業界の優れた能力は、修復コストを低く抑えるのに役立ちます。最後に、このレポートでさらに詳しく説明するように、製造・生産業は、攻撃に関連する特定のコスト (ダウンタイムや機会損失などのコスト) に対する保険金支払い率が最も高く、このことがこの業界の復旧コストの総額に相応の影響を与えた可能性があります。

ランサムウェア攻撃からの復旧にかかった時間に関しては、製造・生産業では、被害者の 3分の 2 (67%) が 1週間以内に復旧して稼働していることが報告されています。これは、世界全体の業界別平均 (53%) よりもかなり高く、製造・生産業は攻撃から回復するのに適した状況にあることを示しています。

さらに、製造・生産業では、回復に要した期間が 1カ月から 6カ月と答えた回答者がわずか 10% だったのに対し、この期間内に回復した世界平均は 20% でした。

最近発生した攻撃の平均復旧コスト

123万米ドル 製造・生産業

140万米ドル 業界全体の平均

ランサムウェア攻撃からの復旧に要する時間

所要時間	製造/生産	業界全体の平均
1週間以内	67%	53%
1 ～ 6ヶ月	10%	20%

ランサムウェアのサイバー保険の補償

製造・生産業の回答者のうち、ランサムウェア攻撃に対する補償があると回答したのは 75% に過ぎず、業界平均では 83% でした。そのため、多くの組織がランサムウェアの復旧にかかる高額なコストにさらされています。

サイバー保険市場はこの 1年間で硬直化しています。製造・生産業でサイバー保険に加入している企業の 95% が、補償を確保するためのプロセスに次のような変化を経験しました。

- 35% が、「サイバー保険を提供している保険会社が少ない」と回答
- 56% が、「サイバー保険に加入するために必要なサイバーセキュリティのレベルが高くなった」と回答
- 53% が「保険が以前よりも複雑になった」と回答
- 30% が「以前よりも手続きに時間がかかる」と回答
- 42% が「以前よりも高額になった」と回答

これらの変化は、サイバー保険金請求の最大の要因であるランサムウェアと密接に関連しています。ここ最近、ランサムウェア攻撃は増加し、身代金および支払い金額は高騰しています。その結果、一部の保険会社は、採算が合わなくなったという理由だけで市場から撤退しました。

サイバー保険の保険会社が少ないため、売り手市場になっています。保険会社が采配を振るい、どのクライアントをカバーするかを選択することができます。残っている保険会社は、リスクとエクスポージャーの軽減を図り、価格も大幅に押し上げています。強力なサイバー攻撃対策は、必要な保険に加入できる可能性が大幅に向上することになります。

サイバー攻撃対策の改善を促進するサイバー保険

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製造・生産業の 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次のような変更を加えています。

- 70% が新しいテクノロジー/サービスを導入済み - 全業界で最も高い
- 63% がスタッフのトレーニング/教育活動を強化 - 全業界で最も高い
- 59% がプロセス/行動を変更

新しいテクノロジー/サービスを導入し、スタッフのトレーニング/教育活動を強化した割合は、全業界で最も高くなっています。これにより、組織の保険の位置付けが向上し、サイバー防御が強化され、コストのかかる攻撃の被害者になる可能性が減少します。

サイバー攻撃対策の改善を促進するサイバー保険

	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	新しいテクノロジー/サービスを導入	スタッフのトレーニング/教育活動を強化	プロセス/行動を変更
製造/生産	97%	70%	63%	59%
業界全体の平均	97%	64%	56%	52%

製造・生産業の平均を下回る身代金支払い率

あらゆる業界で、ランサムウェアの攻撃を受けた場合、サイバー保険会社はほとんど何らかの費用を負担しています。実際、サイバー保険に加入している製造・生産業は、97%の支払率を報告しています。

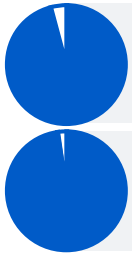
詳細を見ると、この業界は、クリーンアップコストの支払い率が 75% であり、世界平均の 77% とほぼ一致しています。

しかし、注目すべきことは、この業界がすべての業界の中で最も低い身代金支払い率を報告していることです: 30% 対 40% (世界平均)。この低い支払い率は、この業界の身代金支払い率が低いことに関連していると思われます。しかし、製造・生産業が平均身代金が最も高いと報告されていることを考えると、この業界の企業は、保険契約において必要な補償を備えていることを確認する必要があります。

さらに、ダウンタイムや機会損失など、攻撃に関連するその他のコストの支払い率が最も高いと報告されています。支払い率は 34% で、世界平均は 27% でした。

サイバー保険は、組織が以前の状態に戻るのに役立ちますが、「改善」は対象外であることを覚えておくことをお勧めします。組織は、攻撃につながった弱点に対処するために、より優れたテクノロジーとサービスに投資する必要があります。

保険の支払い率:



97%
製造・生産業

98%
業界全体の平均

クリーンアップコストの支払い率:

75%
製造・生産業

77%
業界全体の平均

身代金の支払い率:

30%
製造・生産業 -
業界の中で最も低い支払い率

40%
業界全体の平均

その他のコストの支払い:

34%
製造・生産業 -
業界の中で最も高い支払い率

27%
業界全体の平均

まとめ

製造・生産業の組織が直面するランサムウェアの課題は、今後も拡大し続けます。ランサムウェアの被害を受ける組織の割合は、過去 1年間で大幅に増加し、サイバー犯罪者は攻撃の半分以上においてデータの暗号化に成功しています。

このようにランサムウェアが常態化しつつある中で、製造・生産業は攻撃後の影響への対処能力を高め、ほぼすべて (96%) が暗号化されたデータの一部を取り戻しています。暗号化されたデータを復元する方法としては、バックアップが第一位でした。しかし、この業界は業界全体の中でバックアップ使用率が最も低いと報告されています。

製造・生産業の身代金の支払率は最も低く、世界平均 の 46% に対して 33% でした。同時に、この業界は平均身代金の最高額である 2,036,189米ドルを支払っていると報告しています。これに対し、業界全体の平均身代金額は 812,360米ドルでした。

身代金を支払った後に製造・生産業によって復元された暗号化データの割合は、2020年から増加しています。しかし、業界全体の平均である 61% と比較して、データが復元されたのは 59% で、世界平均を下回っています。

明るいニュースとしては、製造・生産業におけるランサムウェア攻撃を修復するための全体的なコストは、昨年 (2020年の 152万米ドルから 2021年には 123万米ドルに減少)、世界平均の 140万米ドルを下回っています。

多くの製造・生産業は、サイバー保険に加入することで、ランサムウェア攻撃に関連した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、この業界は「その他のコスト」の支払い率が最も高い一方で、身代金の支払い率も最も低くなっています。

製造・生産業は保険に加入することが以前より難しくなっているため、ほとんどの製造・生産業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。この業界は、すべての業界の中でランサムウェアの保険加入率が最も低いと報告されていますが、新しいテクノロジー/サービスの導入やスタッフのトレーニングの強化という点では、この業界がリードしていることは心強いことです。

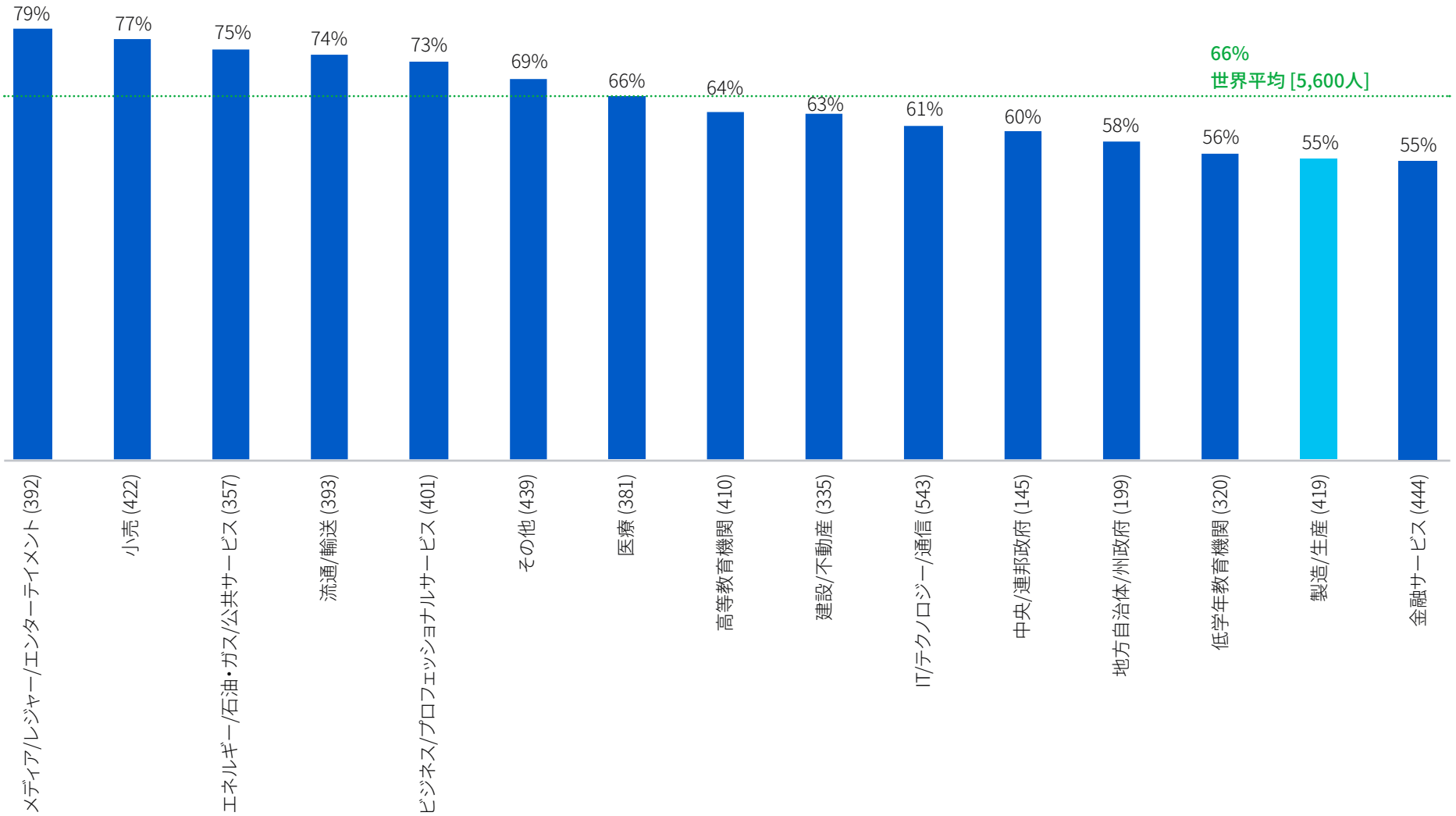
提言

これらの調査結果を踏まえ、ランサムウェアの防御を最適化することは、これまで以上に重要です。5つの重要なポイントは次のとおりです。

- 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。
- 攻撃が実行される前に攻撃を阻止できるように、脅威を事前に検出します。社内に時間とスキルが場合は、MDR (Managed Detection and Response) サイバーセキュリティサービスの専門家を利用してください。
- 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、および関連した脆弱性など、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。
- 最悪の事態に備えてください。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、バックアップからデータを復元する練習をします。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。

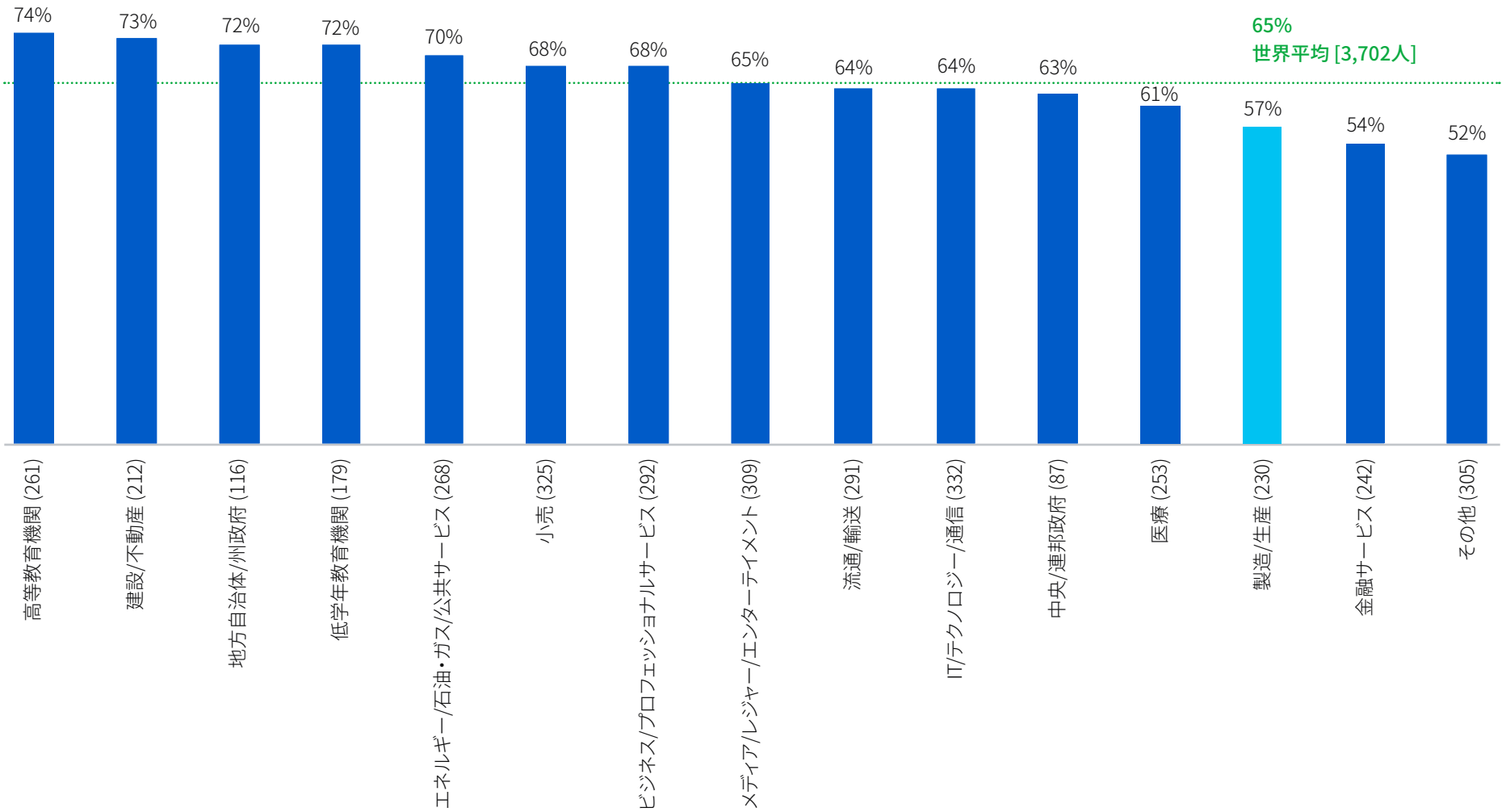
個々のランサムウェアグループの詳細については、ソフォスのランサムウェア脅威インテリジェンスセンターをご覧ください。

攻撃率が最も低い製造・生産業



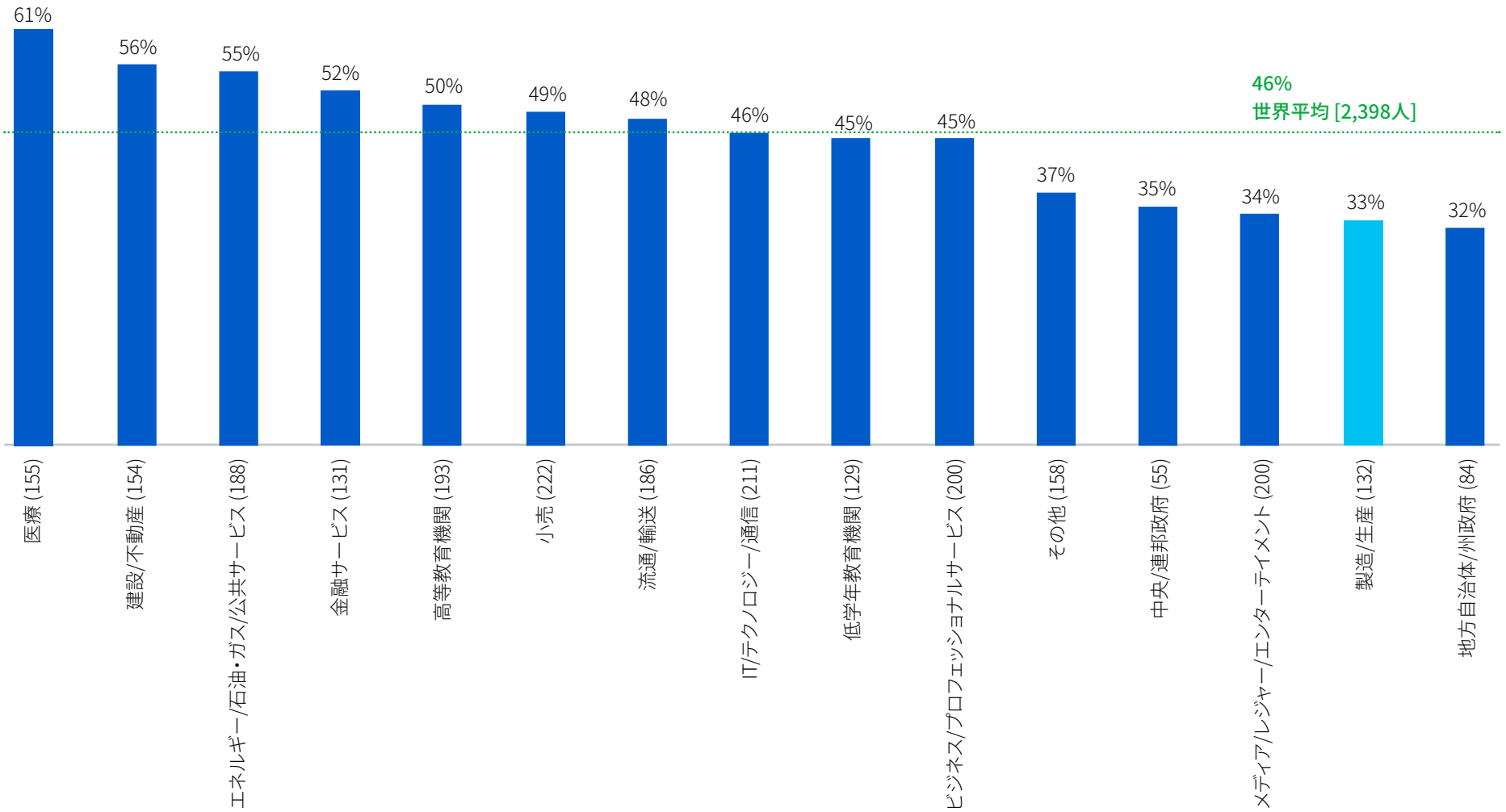
過去 1 年間にランサムウェア攻撃を受けましたか？[組織数=5,600社]

製造・生産業は暗号化率が低い



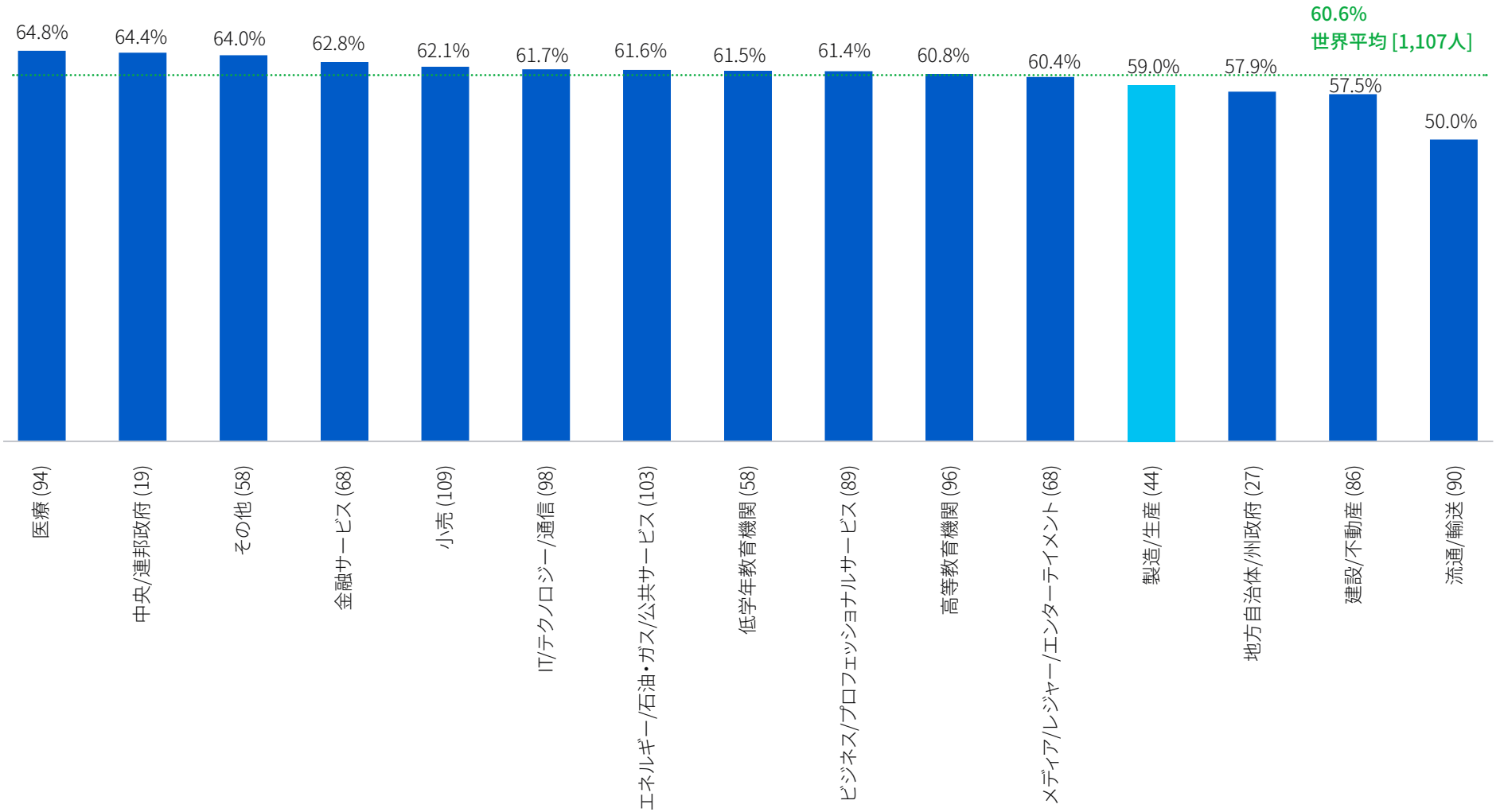
「最も深刻なランサムウェア攻撃においてデータは暗号化されましたか？」(組織数=3,702社、過去 1 年間にランサムウェア攻撃を受けた組織):「はい」

最も低い身代金支払率の 1つである製造・生産業



「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？」
(データが暗号化された組織数 = 2,398社): はい、身代金を支払いデータを取り戻しました

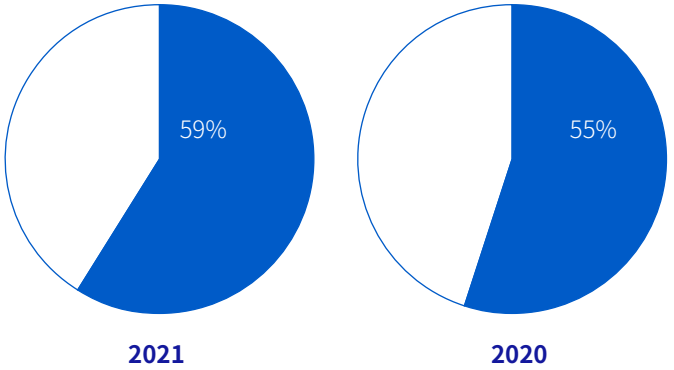
身代金支払い後に復元されるデータ



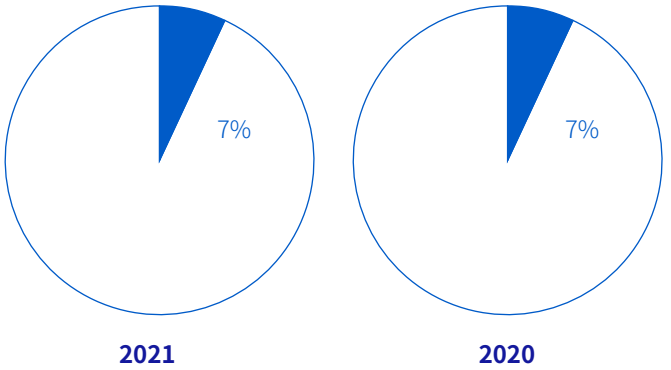
「最も深刻なランサムウェア攻撃において、どの程度データを取り戻すことができましたか?」
(身代金を支払いデータを取り戻した組織 1,107社)

昨年に製造・生産業が復元したデータ

身代金を支払って復元されたデータの割合

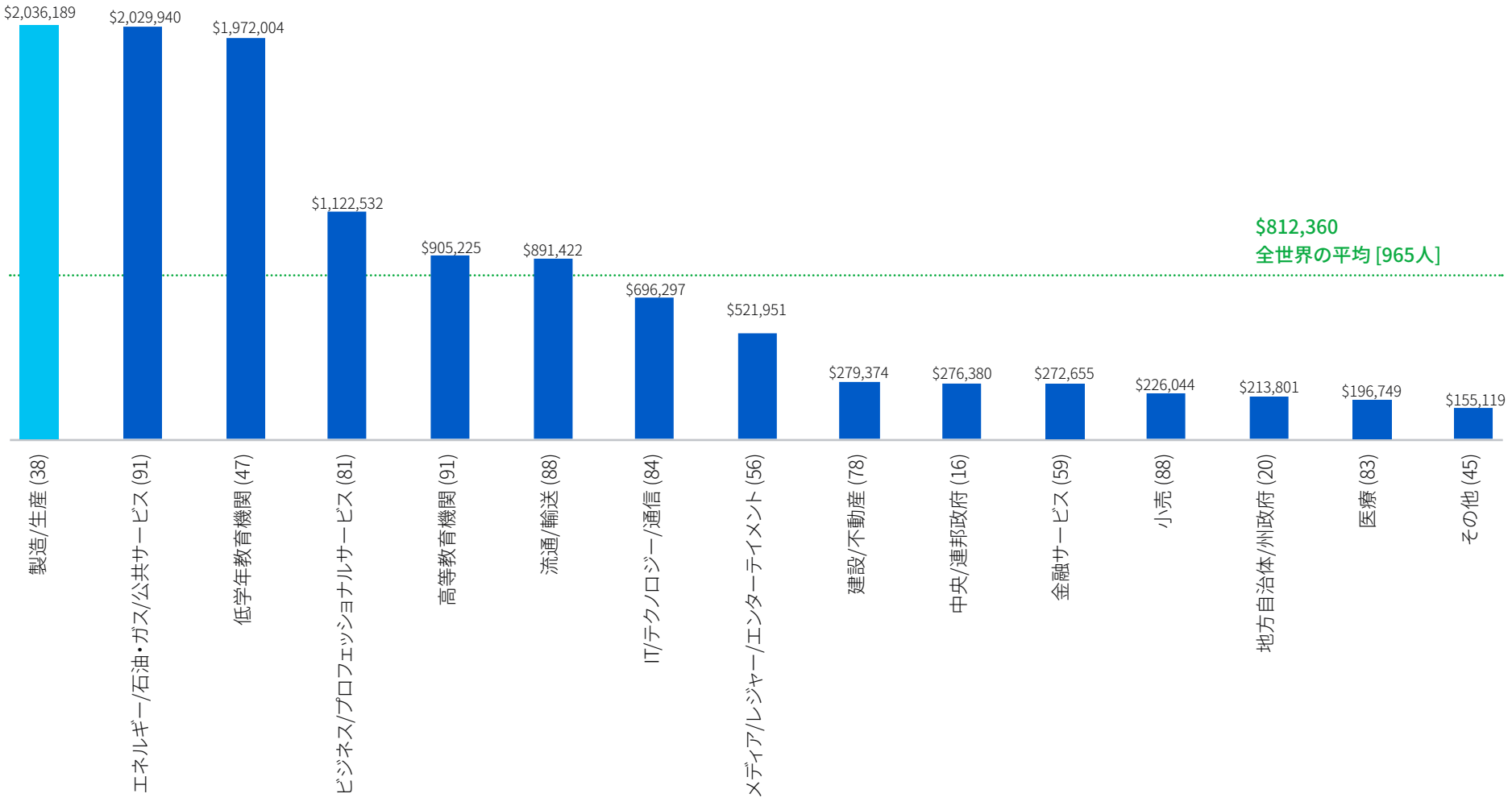


身代金を支払った後に、すべてのデータを取り戻した被害者の割合



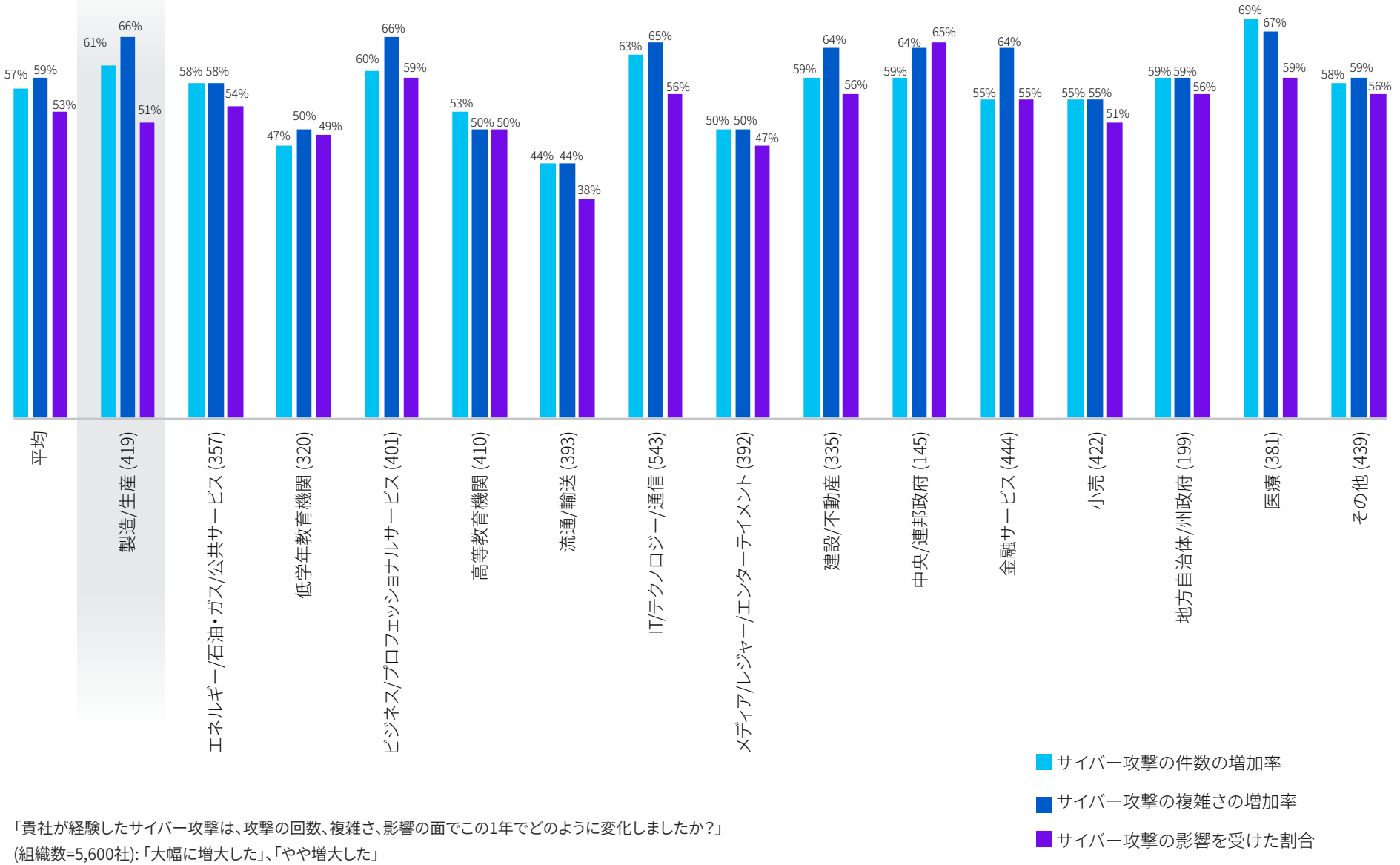
「最も深刻なランサムウェア攻撃において、どの程度データを取り戻すことができましたか？」
身代金を支払ってから、データを取り戻した製造・生産業 44/15

最も高い身代金を支払ったのは製造・生産業



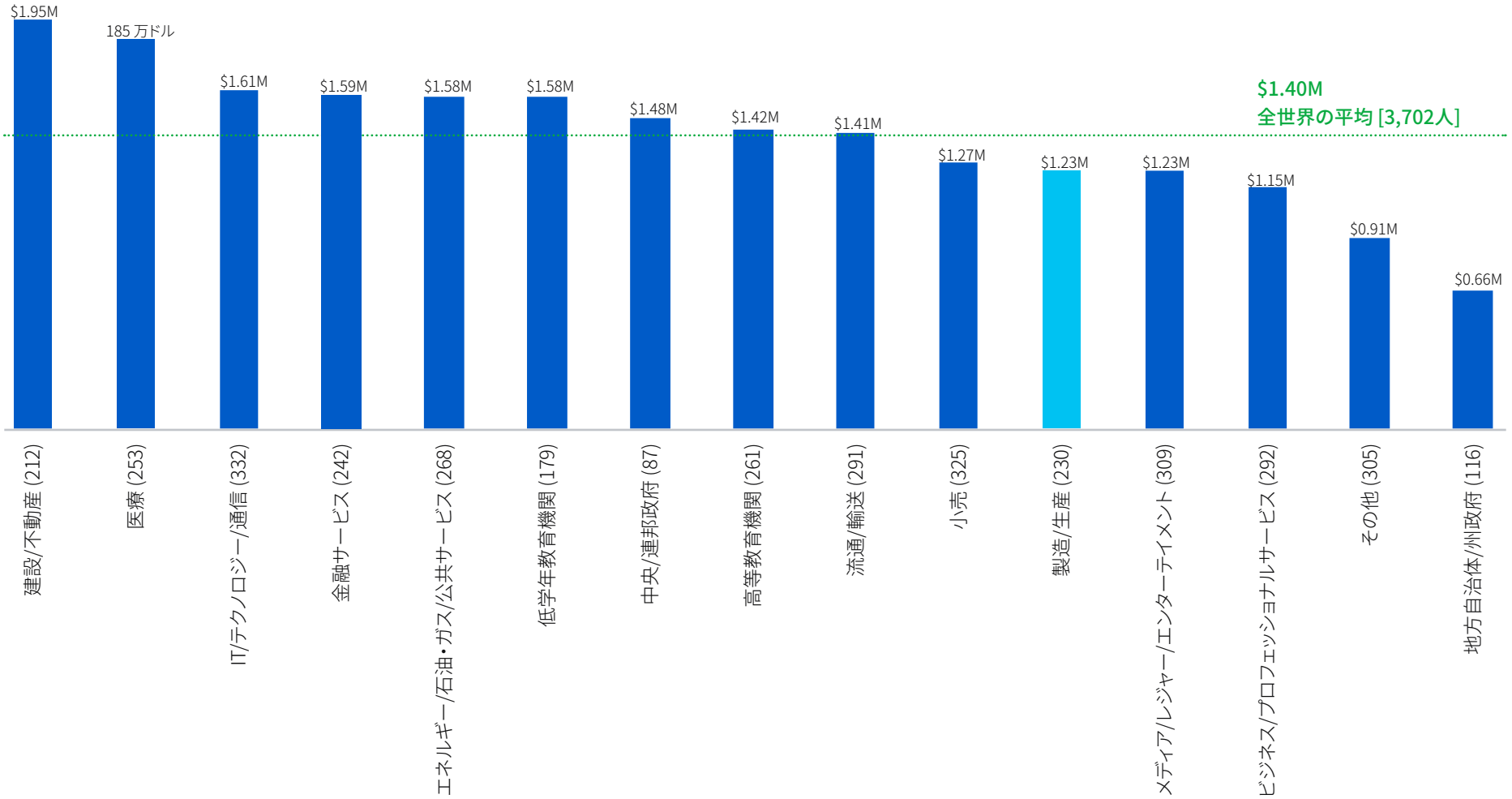
最も深刻なランサムウェア攻撃において、支払った身代金はいくらでしたか？(単位: 米ドル)回答数はグラフ内。
「わからない」は除外。注: 回答数が少ない業界に関しては、参考値としてお考えください。

各業界との比較: 異なる攻撃体験



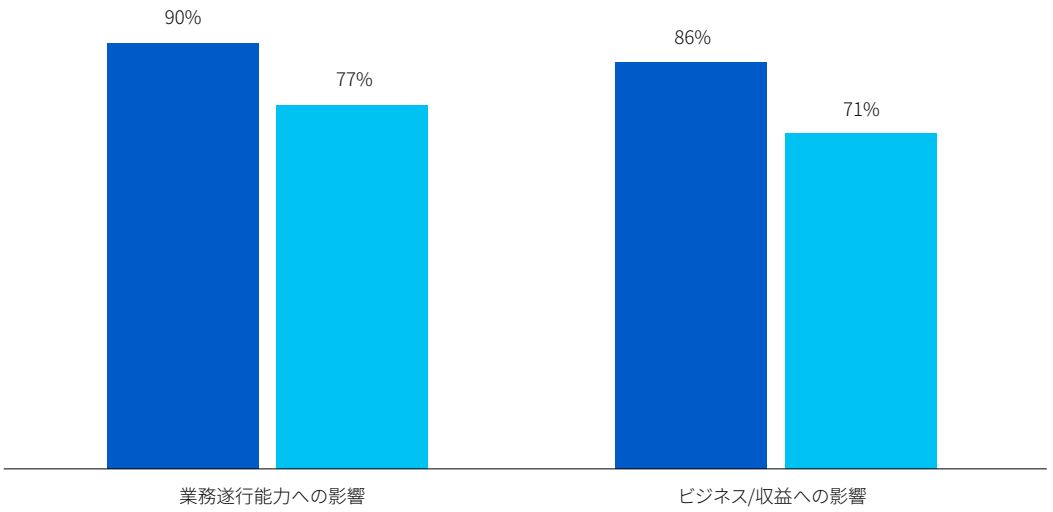
「貴社が経験したサイバー攻撃は、攻撃の回数、複雑さ、影響の面でこの1年でどのように変化しましたか?」(組織数=5,600社):「大幅に増大した」、「やや増大した」

攻撃から復旧するためのコストの減少



「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、ランサムウェアの支払いなど) はどれぐらいですか？」(ランサムウェア攻撃を受けた 3,702 の組織)

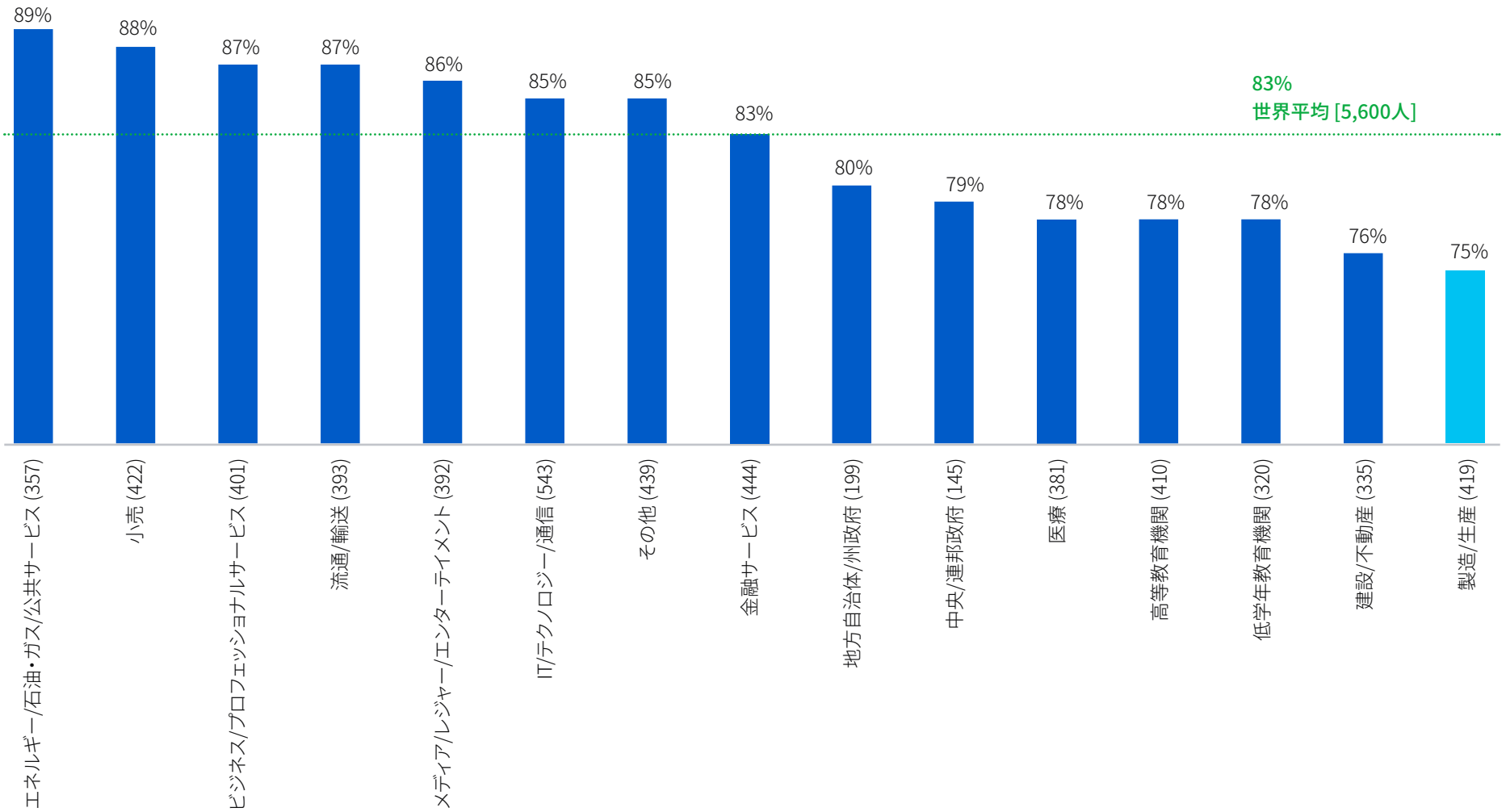
製造・生産業のランサムウェアのより広範な影響



注: ビジネス/収益の損失について質問されたのは、民間企業だけです。このデータには、公的機関の回答者は含まれていません。

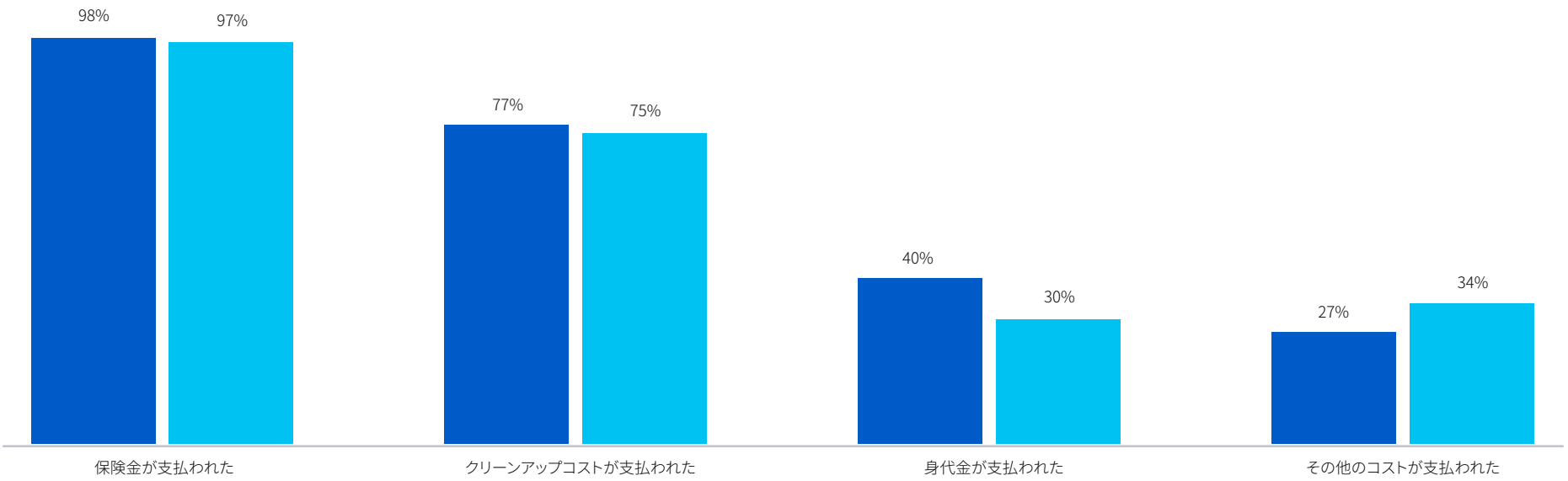
最も重大なランサムウェア攻撃は、組織の業務遂行能力に影響を与えましたか？最も重大なランサムウェアの攻撃により、自社のビジネス/収益に損失を招きましたか？(組織数=3702社; 230社の製造・生産業が前年度にランサムウェアの被害を受けた) 一部の回答オプションを除く。

製造・生産業はランサムウェアに対するサイバー保険の加入率が最も低い



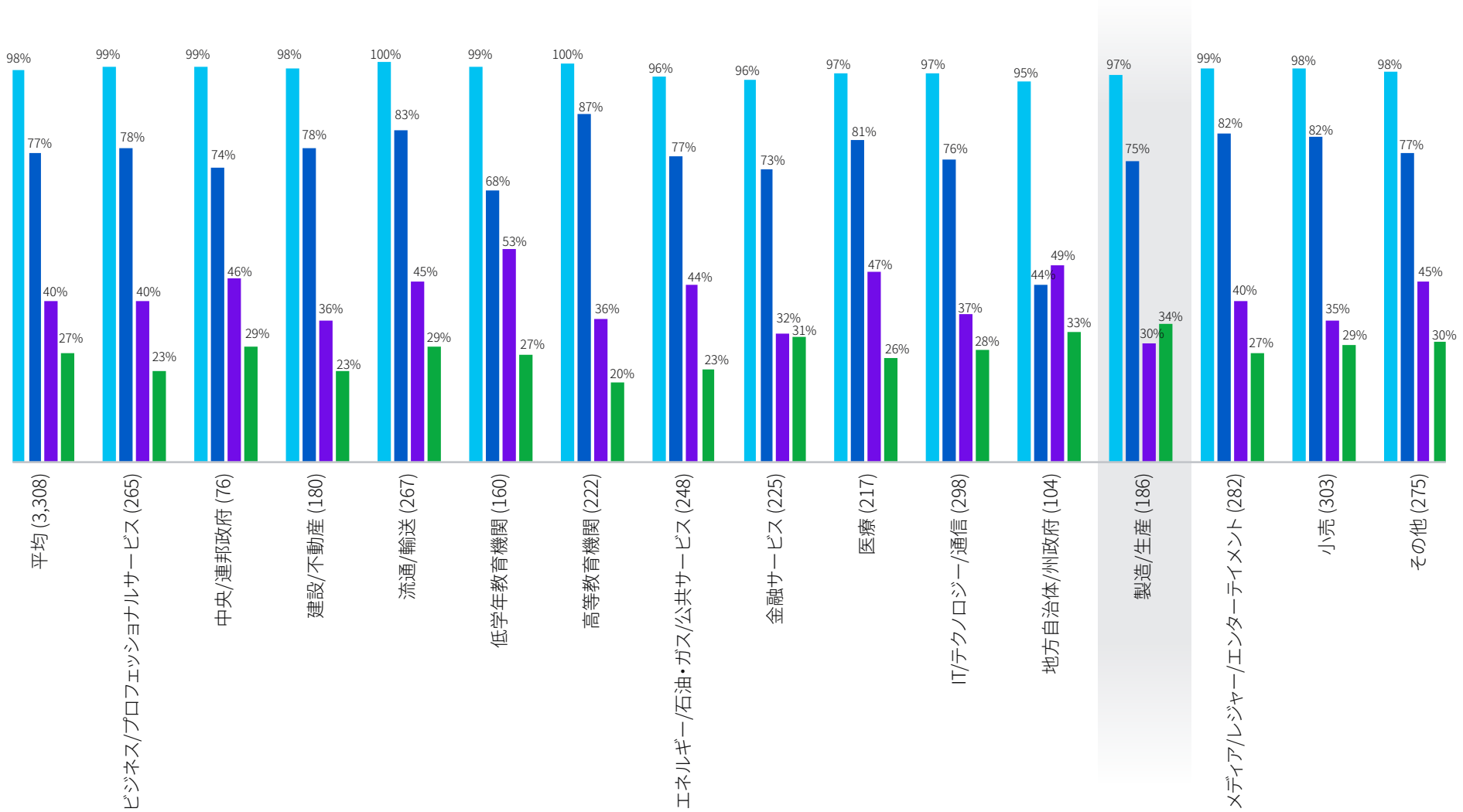
「ランサムウェア攻撃を受けた場合に補償を受けられるサイバー保険に加入していますか?」(回答数はグラフ内。)
「はい」「はい、ただし保険契約に除外事項/例外事項がある」

製造・生産業の平均を下回る身代金支払い率



「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？」(組織数=3,308社/前年にランサムウェアの被害を受けた 186社の製造・生産業、および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。」

サイバー保険金の支払い率 (業界別)



「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？」(組織数=3,308社、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。」

保険金が支払われた　クリーンアップコストが支払われた
身代金が支払われた　その他のコストが支払われた

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。

2022-10-06 (WP-NP)

SOPHOS