SOPHOS
Cybersecurity evolved.

製造/生産業のランサムウェアの現状 2021

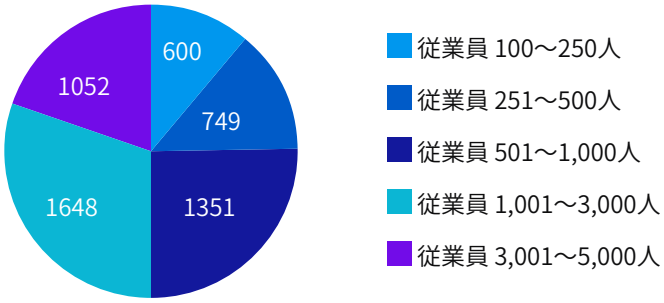
このレポートでは、438人の IT 意思決定者を対象とした独立調査に基づいて、製造/生産業でのランサムウェアの現状に関する新しい洞察を紹介します。ここでは、製造/生産業におけるランサムウェアの蔓延、被害者に対する攻撃の影響、ランサムウェアの修復コスト、および今後の攻撃に対する将来の予測と準備観点から業界がどのようにそれに匹敵していくかについて詳しく説明しています。

ソフォス ホワイトペーパー2021年 9月

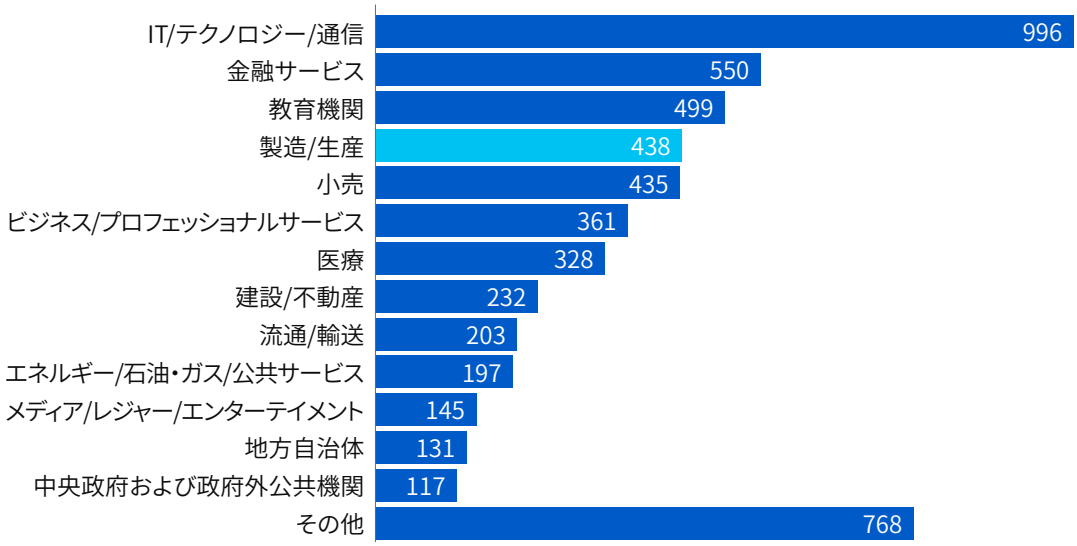
調査について

ソフォスは、独立系の調査会社 Vanson Bourne による 30 か国にわたる 5,400 人の IT 管理者を対象としたグローバル調査を依頼しました。回答は、製造/生産業から 438人の回答者を含んだ、幅広い業界から寄せられました。調査は、2021年 1月と 2月に実施されました。

世界全体の従業員数は?[5,400人]



組織の業種は?[5,400人]



各国の回答者の内訳は、50% が従業員数 100～1,000人の組織、50% が 1,001～5,000人の組織でした。回答者は、調査対象のすべての地域 (南北アメリカ、ヨーロッパ、中東、アフリカ、アジア太平洋) の製造/生産業の IT 意思決定者 438人でした。

地域	# 回答者数
北米・中南米	101
ヨーロッパ	160
中東、アフリカ	37
アジア太平洋	140

製造/生産業の IT 意思決定者 438人

製造/生産業の主な調査結果

- **昨年、ランサムウェア攻撃に受けた**製造/生産業の割合は**36%** でした
- ランサムウェア攻撃を受けた組織の **49%** は、最も深刻なランサムウェア攻撃において、サイバー犯罪者が**組織のデータの暗号化に成功した**と回答しました
- 最も深刻なランサムウェア攻撃においてデータが暗号化された組織の **19%** は、データを取り戻すために**身代金を支払いました** – 全業種の中で最も低い支払い率
- データが暗号化された組織の **68%** が、**データの復元にバックアップを使用しました**
- 身代金を支払った後、平均で **55% のデータが復元され**、ほぼ半数はデータにアクセス出来なくなりました (15 人の回答者の経験より)
- 製造/生産業の **89%** は、**マルウェアインシデントの復旧計画**があります。
- 製造/生産業における**ランサムウェア攻撃の影響を修復するための平均総額**は、ダウンタイム、人件費、デバイスのコスト、ネットワークのコスト、逸失利益、支払った身代金などを考慮すると、**152万米ドル**でした

昨年、製造/生産業では、世界の平均が 37% に対し、組織の 36% が攻撃を受けるという平均レベルのランサムウェア攻撃が発生しましたが、この業種は今後最も高いランサムウェア攻撃が見込まれる業界です。回答者の半数近く (49%) は昨年は攻撃を受けていませんが、今後数年以内に攻撃を受けると予測されています。この高いレベルの予測は、ランサムウェアの巧妙さおよび蔓延率の高まりの認識により引き起こされました。60% の組織は、攻撃の巧妙さが原因で攻撃の阻止が困難になっていると報告し、46% の組織は、ランサムウェアが蔓延しているため、攻撃を受けることは避けられないと述べています。

この業界は、ランサムウェアに直面した際に、群を抜いて最も回復力があります。製造/生産業は、調査対象のすべての業種のうちで身代金を支払う可能性が最も低く、暗号化されたデータを取り戻すために身代金を支払う組織は 5社に 1社 (19%) のみでした。これは、製造/生産業がバックアップからデータを復元する能力が非常に高いためです。ランサムウェアの被害者の 3 分の 2 (68%) がバックアップを使用して、暗号化されたデータを復元しました。これは、全業界の中で最も高い割合です。製造/生産業は、GDPR や SOC などの多くの政府規制、および SEC、FDA、EPA の規制で要求されるように、データを短期および長期保持することの恩恵を受けているようです。身代金を支払った製造/生産業が平均でデータの 55% しか回収できなかったことを考えると、この業種は主な復旧方法としてバックアップに重点を置くことが賢明です。

製造/生産業では、ランサムウェアの運用者がファイルの暗号化はしないが、身代金の要求が支払われない場合に盗まれた情報をオンラインで漏洩させると脅迫するという恐喝スタイルの攻撃が平均以上発生しています。恐喝のみの攻撃を経験しているランサムウェアの被害を受けた組織は 10分の 1 (9%) になります。 サイバー犯罪者は、ほとんどの製造業が知的財産や企業秘密などの貴重なデータを保持していることをよく認識しており、このデータを販売するという脅威を利用して被害者に支払いを強要しています。次に、この業種ではバックアップからデータを復元する能力が非常に高いため、攻撃者はデータの暗号化に依存しない他のアプローチに移行することを余儀なくされています。

実際の身代金の支払いに関しては、製造/生産業は平均を下回っており、業種間の平均である 170,404 米ドルと比較して、平均支払額は 147,917米ドルです (注: 製造/生産業は回答ベースの数が少ないため、この数字は統計的に有意ではありません)。

製造/生産業のための全体的なランサムウェアの回復コストは、世界平均よりもほぼ 330,000米ドル低くなっています。世界平均 185万米ドルに対し、152万米ドル。この全体的なコストの削減は、データを取り戻すために身代金の支払いに依存することなく、バックアップを使用して暗号化されたデータを復元するこの業種の高い能力のおかげである可能性があります。とは言うものの、152万米ドルは依然として非常に高額であり、すべての組織に大きな影響を与えるでしょう。これらの回復コストに影響を与える可能性のある要因としては、すべてのコストで運用を継続するための対応措置に多額の費用がかかるだけでなく、この業種に影響を与える評判のダメージや規制上の罰金にも高額の費用がかかります。

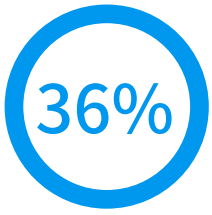
製造/生産業の IT チームは、2020年の課題によって深刻な影響を受けました。この業種では、2020年にサイバーセキュリティの仕事量の減少が最も低いと考えられていました。世界平均が 13% に対してわずか 7% がサイバーワークロードが減少したと回答しました。また、IT 問題への対応時間が改善されたと答えた回答者は最も少なく、2020年は 対応時間が短縮されたと答えたのは世界平均 20% に対してわずか 15% でした。世界がロックダウン状態に入り、この業種は生産施設のリモート管理へと急速に移行することを余儀なくされました。組織は、従来は人間による関与がかなり必要だった生産量の維持という課題に直面しました。また、パンデミックの最初の数か月で定期的に商品不足が話題になり、大きな影響を受けたサプライチェーンと協力する必要がありました。良い面としては、サイバースキルも向上し、回答者の 71% がサイバーセキュリティの知識とスキルをさらに発展させるチームの能力が 2020年に向上したと述べています。

製造/生産業は、攻撃の影響を最小限に抑えるために、バックアップと災害復旧への取り組みに引き続き投資する必要があります。また、テクノロジーと人間主導の脅威ハンティングを組み合わせて、今日の高度な人間主導の攻撃を無効化することで、ランサムウェア対策の防御を強化することも検討する必要があります。

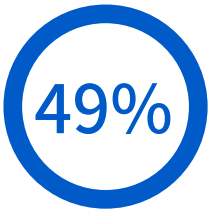
製造/生産業のランサムウェアの普及率

昨年、ランサムウェアの被害に遭った製造/生産業

調査対象となった 438人の製造/生産業の回答者のうち、36% が過去一年間にランサムウェアの被害に遭っていました。ランサムウェア攻撃によって、複数のコンピューターが影響を受けていましたが、必ずしもコンピューターのデータが暗号化されていたわけではありませんでした。



昨年ランサムウェア攻撃を受けた割合



昨年はランサムウェア攻撃を受けなかったが、今後攻撃を受けるであろうと予測する割合 – すべての業種の中で最も高い

昨年はランサムウェア攻撃を受けておらず、今後も攻撃を受けないと予測する割合

昨年、ランサムウェア攻撃を受けましたか？[製造/生産業の回答者 438 名]

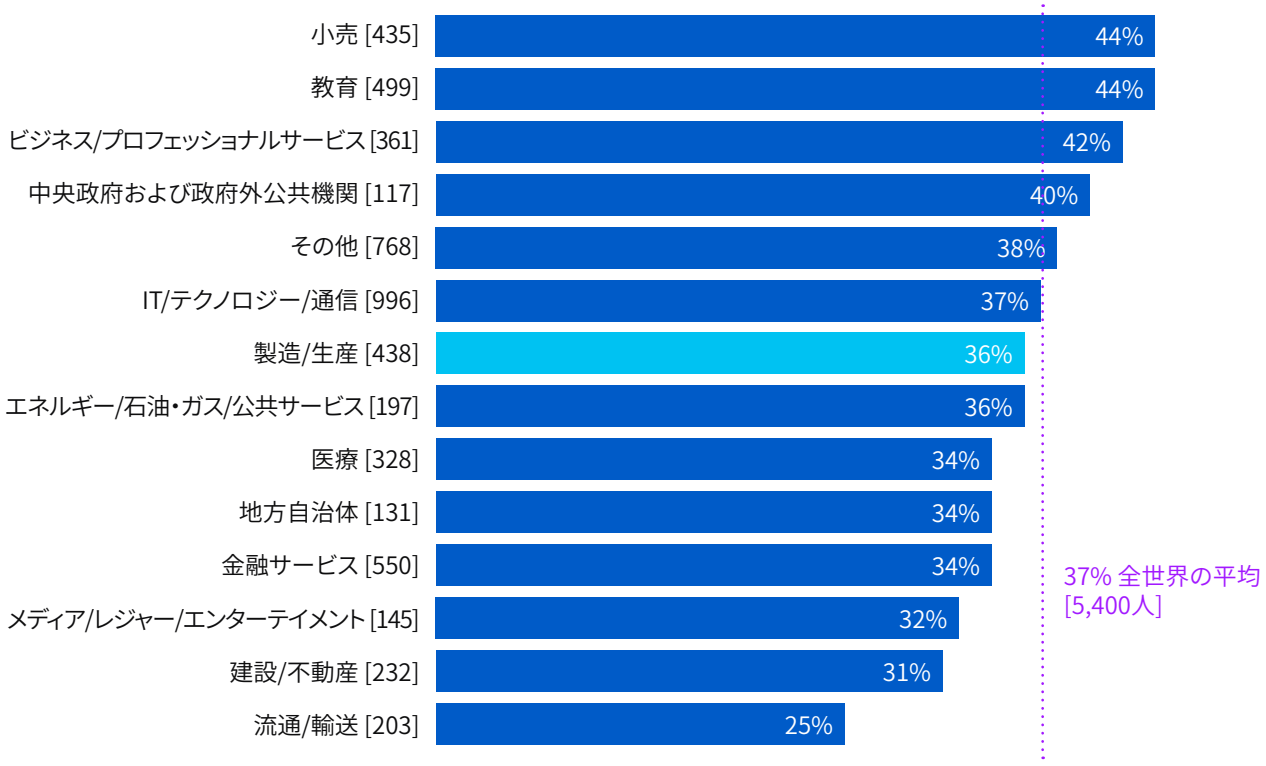
過去 1 年間で攻撃を受けたことはありませんでしたが、調査対象のすべての業種で最も高い割合である 49% の回答者が、将来的にランサムウェアの被害に遭うと予測していました。このレポートの後半で説明するように、将来的に被害を受けるという高いレベルの予測は、ランサムウェアの巧妙化と普及率の高まりを認識していることによってもたらされます。同時に、回答者の 15% は将来の攻撃から安全であると確信していました。

レポートの後半では、今後、攻撃を受けることを予測する理由と、今後も攻撃を受けないと自信を持てる理由についてさらに深く掘り下げます。

将来的にランサムウェア攻撃を受ける可能性が最も高い業種

ランサムウェアの被害を受けたと報告した**製造/生産業**の組織の数 (36%) は、業種間の世界平均 (37%) よりわずかに少なくなっています。**小売業**および**教育機関**は、ランサムウェア攻撃を受ける割合が最も高くなっており、これらの業界の回答者の 44% が攻撃を受けたことを報告しています。

昨年、ランサムウェア攻撃を受けた回答者の割合



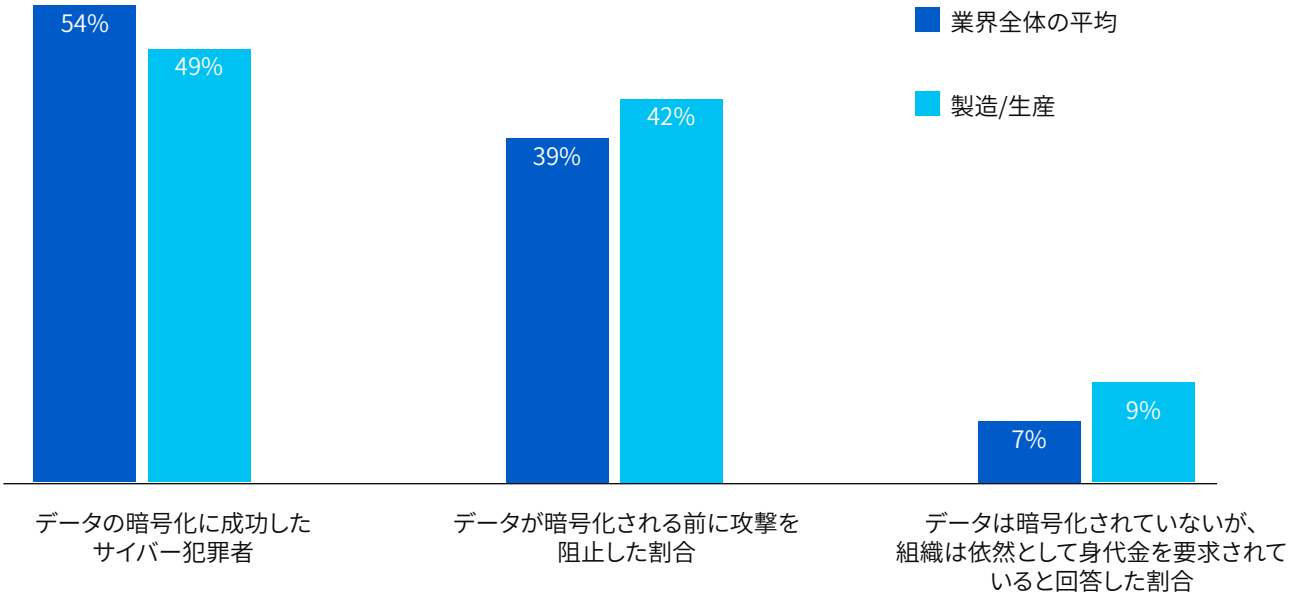
昨年、ランサムウェア攻撃を受けましたか？はい、[回答した組織数] 一部の回答の選択肢を省略し、業界ごとに分割

世界中のすべての業種で、過去一年間にランサムウェアに攻撃された組織の割合は、51% が攻撃を受けたことを認めた昨年より大幅に減少しました。この減少は歓迎すべきニュースですが、SophosLabs と Sophos Managed Threat Response チームによって観察された攻撃者の行動の進化が一部原因である可能性があります。例えば、多くの攻撃者は、大規模で自動化された汎用性の高い攻撃から、手動によるハッキングなど、従来よりもさらに標的型の攻撃にシフトしています。攻撃の総数は減少しましたが、ソフォスの経験から、このような標的型攻撃から被害を受ける可能性ははるかに高いことがわかっています。

ランサムウェアによる被害

データ暗号化を阻止する製造/生産業の能力

昨年ランサムウェア攻撃を受けたと回答した組織を対象に、サイバー犯罪者によってデータが暗号化されたかどうかを質問しました。製造/生産業の回答者の 49% が「はい」と回答しましたが、これは世界平均 54% よりも低くなっています。



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？[過去一年間でランサムウェアの被害に遭った製造/生産業 158社/2,006社]

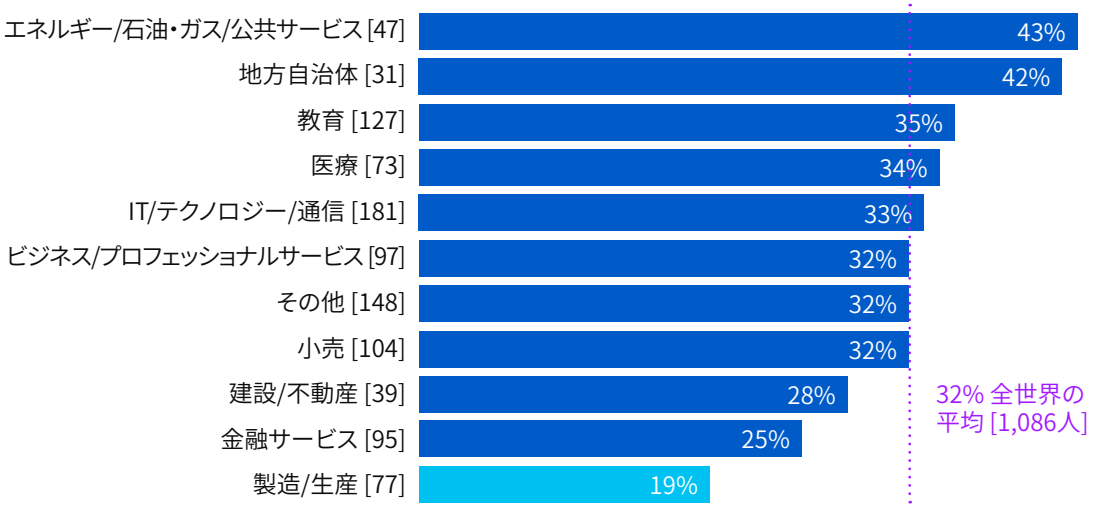
製造/生産業は世界平均よりも暗号化の阻止に成功しました (攻撃の 39% が平均なのに対し、42% が阻止されました) が、この業種は小規模でありながら成長を続ける新しい傾向、つまりランサムウェアの運用者がファイルの暗号化はしないが、身代金を支払わない場合に盗まれた情報をオンラインで漏洩させる脅迫する、恐喝のみの攻撃に対して脆弱でした。実際、ランサムウェアに感染した製造/生産業の 9% が恐喝攻撃を受けました。サイバー犯罪者は、ほとんどの製造業が保持している知的財産や企業秘密などの貴重なデータをよく認識しており、このデータを販売するという脅威を利用して被害者に支払いを強要しています。もう 1つ考えられる理由は、(後ほど説明するように) この業種がバックアップからデータを復元する能力が非常に高いため、データの暗号化に依存しない他のアプローチを攻撃者に実行させます。

昨年、SophosLabs では、この種の攻撃の増加が見られました。暗号化や復号化が不要なため、攻撃者側の労力は少なくて済みます。また、攻撃者は、被害者に支払いをさせるさらなる努力を求めて、データ侵害に対する懲罰的な罰金を悪用することがよくあります。

身代金の支払いに応じる最も低い傾向

調査の結果、製造/生産業は、調査対象の全業種の中で身代金を支払う傾向が最も低いことが明らかになりました。データが暗号化された製造/生産業のわずか 5 分の 1（19%）が身代金の要求に応じたのに対し、世界平均は 32% でした。この理由として、後に説明するように、バックアップを使用して暗号化されたデータを復元する能力がこの業種では優れていることが考えられます。これは、すべての業種の中で最も高い能力です。

データを取り戻すために身代金を支払った割合



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？はい、身代金を支払った、[回答した組織数] 最も深刻なランサムウェア攻撃においてデータが暗号化されたと回答した組織の割合、一部の回答の選択肢を省略し、業種ごとに分割

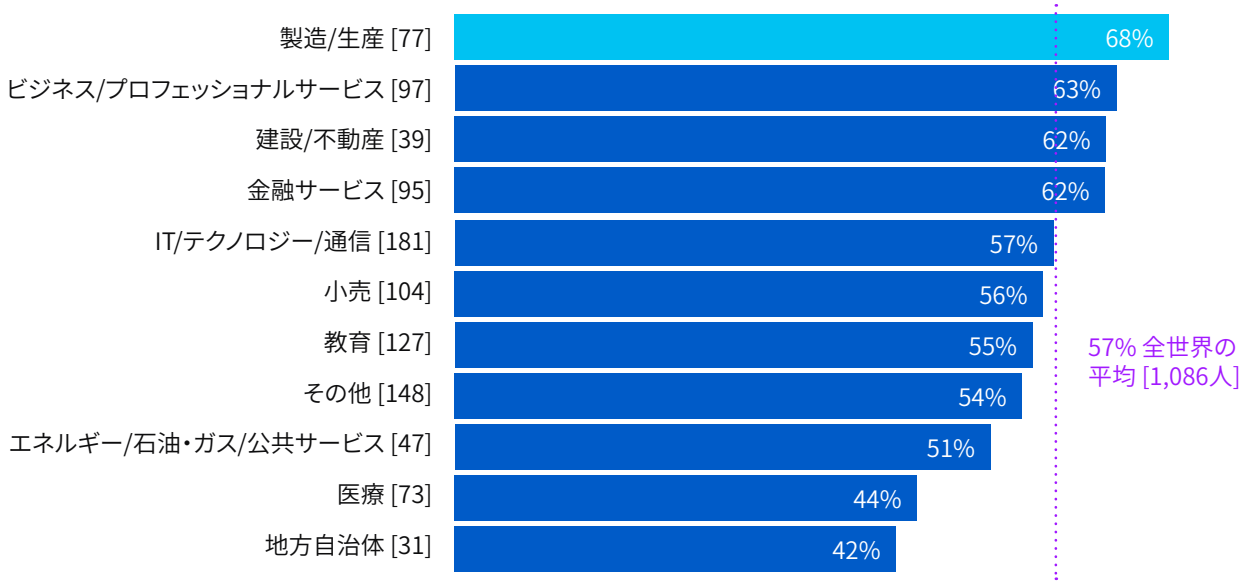
業種全体で、**エネルギー、石油/ガス、公益サービス**が身代金を支払う可能性が最も高く、43% が身代金の要求に応じました。この業界では、一般に、簡単にアップデートできないレガシーインフラを利用していることが多く、被害を受けた組織は、事業を継続するために、身代金を支払わざるを得ないと感じているのかもしれません。

地方自治体は、身代金の支払いが 2番目に多いです (42%)。これは、データが暗号化されている可能性が最も高い業界でもあります。地方自治体が、身代金の支払いに応じる傾向が高いことから、集中的に、複雑でより効果的な攻撃の対象にされている可能性さえあります。

データの復元にバックアップを使用する能力

このグラフを前のグラフと比較すると、バックアップからデータを復元する能力と身代金を支払う傾向との相関関係がはっきりと分かります。バックアップを最も使用できる業種は、支払いが最も少ない傾向にもあります。

暗号化されたデータをバックアップを使用して復元した割合

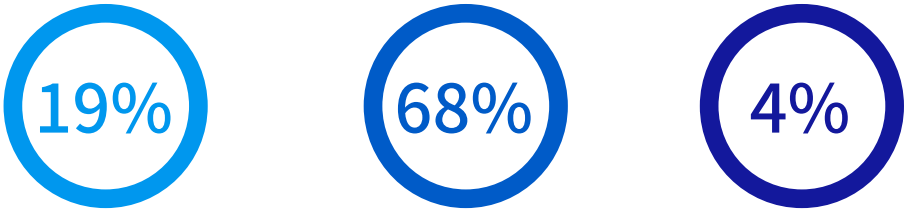


最も深刻なランサムウェア攻撃においてデータを取り戻すことができましたか？

はい、バックアップを使用して、データを復元した、[回答した組織数] 最も深刻なランサムウェア攻撃において、サイバー犯罪者によってデータが暗号化された組織の割合、一部の回答の選択肢を省略し、業種ごとに分割

製造/生産業の回答者 (68%) は、暗号化されたデータをバックアップを使用して復元する能力が最も高かったです。これは、製造/生産業が、グローバルかつ規制された経済での運用の複雑さに対応するために、運用、インフラストラクチャ、およびデータのほぼ継続的な可用性を必要とするためだと考えられます。業界のベストプラクティス。SOC、ISO 27001、GDPR などの政府規制、および SEC (米国証券取引委員会)、FDA (食品医薬品局)、EPA (米国環境保護局) の規制により、データの短期および長期保持が必要とされています。バックアップを作成し、そこからデータを復元することに慣れておくことは、この業種の事前準備として不可欠になります。

91% が暗号化されたデータの取り戻しに成功



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？[77] サイバー犯罪者が最も深刻なランサムウェア攻撃でデータの暗号化に成功した製造/生産業企業。

製造/生産業にとっての朗報は、データが暗号化された企業の 91% がそれを取り戻したことです。これまで見てきたように、19% が身代金を支払い、68% がバックアップを使用してデータを復元し、4% が他の手段を使用してデータを取り戻しました。

身代金を支払っても、データの一部しか戻らない

しかしながら、身代金を支払った組織は、すべてのデータを取り戻すことはできませんでした。身代金を要求する攻撃者は、組織が身代金を支払ったとしても、すべてのデータを復元できる可能性は低いということははっきりとは言いません。

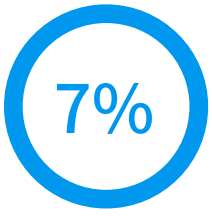
身代金を支払って復元された データの割合 業界全体の平均

身代金を支払って復元できた データの割合 製造/生産業界の平均

最も深刻なランサムウェア攻撃において、取り戻すことのできたデータの割合の平均[344社 / 15社] データを取り戻すために身代金を支払った組織

製造/生産業の回答者の基本数は、確固とした結論を引き出すのに十分な数ではありません。しかし、伝えられるところによると、製造/生産業の回答者は、身代金を支払った後、平均してデータの 55% しか戻ってこないため、データのほぼ半分にアクセスできなくなったとの報告があります。これは、復元されたデータの割合が 65% という世界平均よりもかなり低いです。

データの部分的な復号化は、攻撃者による意図的な策略ではなく、攻撃者が復号化ツールよりも強力な暗号化ツールの開発により多くの時間と労力を費やしていることが反映されている可能性があります。



すべてのデータを取り戻した

データの半数以下を取り戻した

最も深刻なランサムウェア攻撃において、組織が取り戻すことのできたデータの割合[15] データを取り戻すために身代金を支払った製造/生産業企業

この点をさらに強調すると、身代金を支払った製造/生産業のわずか 7% がすべてのデータを取り戻し、40% は半分以下のデータを取り戻しました。身代金を支払っても明らかに割に合いません。繰り返しになりますが、製造/生産業の基本数は少ないため、単なる指標として見なす必要があります。

ランサムウェアのコスト

明らかにされた身代金支払い額

業種全体で、身代金を支払ったと回答した 357人のうち、282人が支払った正確な金額を共有しました。

170,404米ドル

身代金支払い額の世界平均

147,917米ドル

製造/生産業の平均的な身代金の支払い

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？
[282社 / 12社] データを取り戻すために身代金を支払った組織
注: 製造/生産業界は、回答ベースの数が低い。

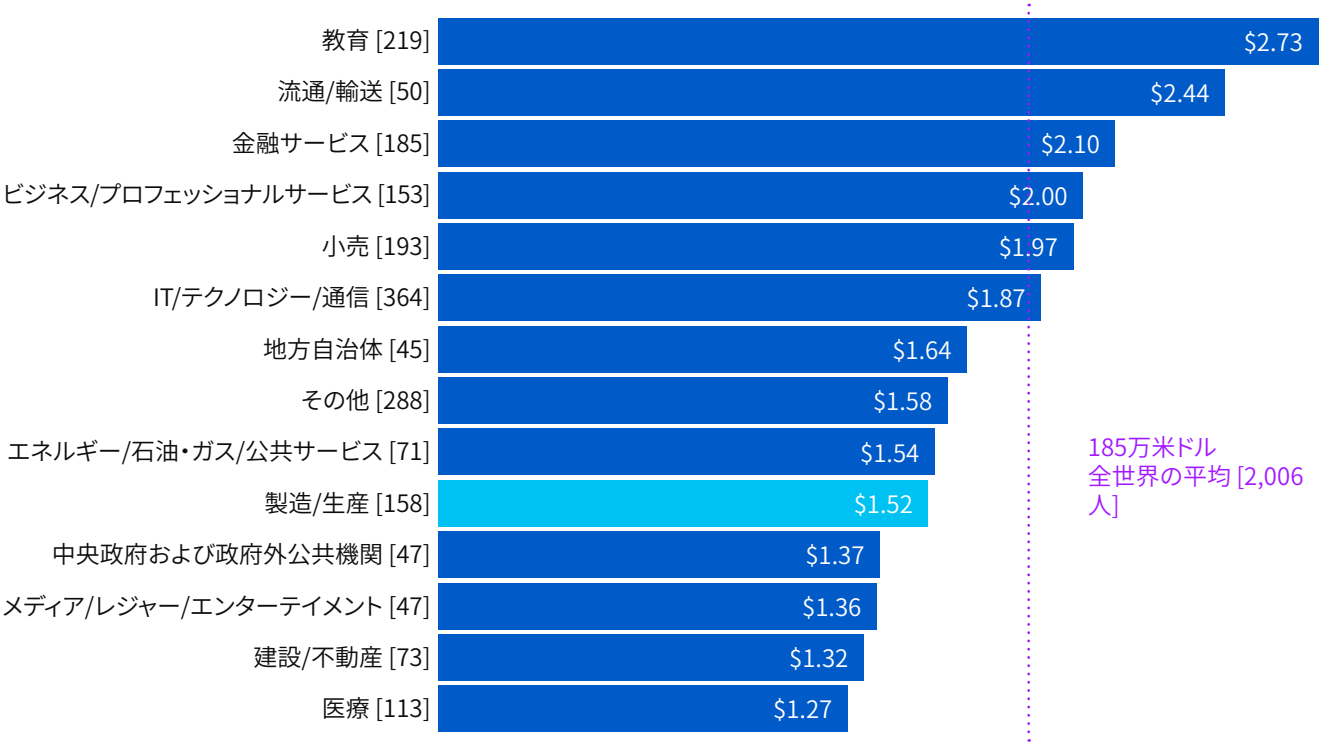
世界的に**業界全体**での身代金の支払い金額の平均は 170,404米ドルでした。伝えられるところでは、製造/生産業の回答者 12人は平均で 147,917 米ドルで支払っています。この低い支払いレベルは、一部には、バックアップを使用してデータを復元するこの業種の高いな能力によるものと考えられます。

世界的に、身代金の支払い額は、数千万ドルなどと新聞の見出しで取り上げられる値とは大きく異なっていますが、それには次のような複数の理由があります。

- **組織の規模。**この調査の回答者は、大規模な組織と比較すると、一般に資金力が少ない、従業員数が 100〜5,000人の中堅規模の組織の IT 意思決定者です。ランサムウェアを使用する攻撃者は、標的組織の支払い能力に応じて身代金の要求額を調整しており、通常、小規模な企業であれば、低額の身代金を要求して受け入れています。従業員数が 100〜1,000人の組織が支払った身代金の平均額は 107,694米ドルで、従業員数が 1,001〜5,000人の組織が支払った身代金の平均額は 225,588米ドル、というデータはこれを裏付けます。
- **攻撃の特徴。**ランサムウェア攻撃者は多数存在し、ランサムウェアの攻撃手法も多岐にわたります。個別の標的に合わせて高度な TTP (戦術、手法、手順) を使用するスキルの高い攻撃者から、「既製品」のランサムウェアを使用し、運任せに無差別な攻撃を実行し高度なスキルを持たない攻撃者までさまざまな攻撃者が存在します。標的型攻撃に多大な投資を行っている攻撃者は、その労力に見合った高額な身代金を求めますが、汎用的な攻撃を行っている攻撃者の多くは、「薄利多売」のようなビジネスを展開しています。
- **地域性。**最初に述べたように、この調査では、GDP レベルが一様でない、世界 30か国を対象としています。攻撃者は、欧米先進国の標的に高額な身代金を要求していますが、これは、欧米先進国には多額の身代金を要求されても支払い能力がある組織が多いと考えているためです。身代金の支払い額のトップ 2件の報告者は、いずれもイタリアの回答者でした。一方、インドの身代金の平均支払い額は 76,619米ドルで、世界平均の半分以下でした (対象回答者：86人)。

製造/生産業におけるランサムウェアの回復コスト

身代金は、ランサムウェア攻撃から回復するためのコスト全体のほんの一部に過ぎません。被害者は、IT システムの再構築とセキュリティ保護、PR、フォレンジック分析などに関する、さまざまな追加費用に直面します。



最近発生したランサムウェア攻撃の平均の修復コスト (ダウンタイム、人件費、デバイスのコスト、ネットワークのコスト、逸失利益、身代金など)、[回答した組織数] 昨年ランサムウェア攻撃を受けたと回答した組織を業種別に分割、単位：100万米ドル

この調査では、製造/生産業は 152万米ドルの平均を下回るランサムウェアの修復コスト (ダウンタイム、損失時間、デバイスコスト、ネットワークコスト、逸失利益、身代金、法律上および規制上の罰金など) が発生することが明らかになりました。これは、世界平均である 185万米ドルよりもかなり低い額です。これは、データを取り戻すために身代金の支払いに依存することなく、バックアップを使用して暗号化されたデータを復元するこの業種の能力が高いためである可能性があります。

平均を下回っていますが、ランサムウェアの費用はこの業種にとって依然として非常に高く、いくつかの要因が原因である可能性があります。 評判のダメージによるビジネスの損失費用に加えて、ランサムウェア攻撃の影響を受けた場合に本番環境を実行できなくなるコストも莫大なものとなる可能性があります。製造業者は、他の製造/生産業と並んでサプライチェーンの一部を形成することがよくあります。業務の中断は、サプライチェーンの他の部分の生産に深刻な影響を及ぼし、大規模な事業損失をもたらす可能性があります。これにより、製造/生産業は、コストに関係なく、できるだけ迅速に稼働を再開することが求められます。

さらに、製造/生産業は、コンプライアンス違反に対して莫大な罰則を課せる SOC やGDPR などの無数の業界規制および政府規制を遵守する必要があります。ランサムウェア攻撃の一部として発生したデータ侵害に対する罰金は、全体的な復旧コストに追加されます。

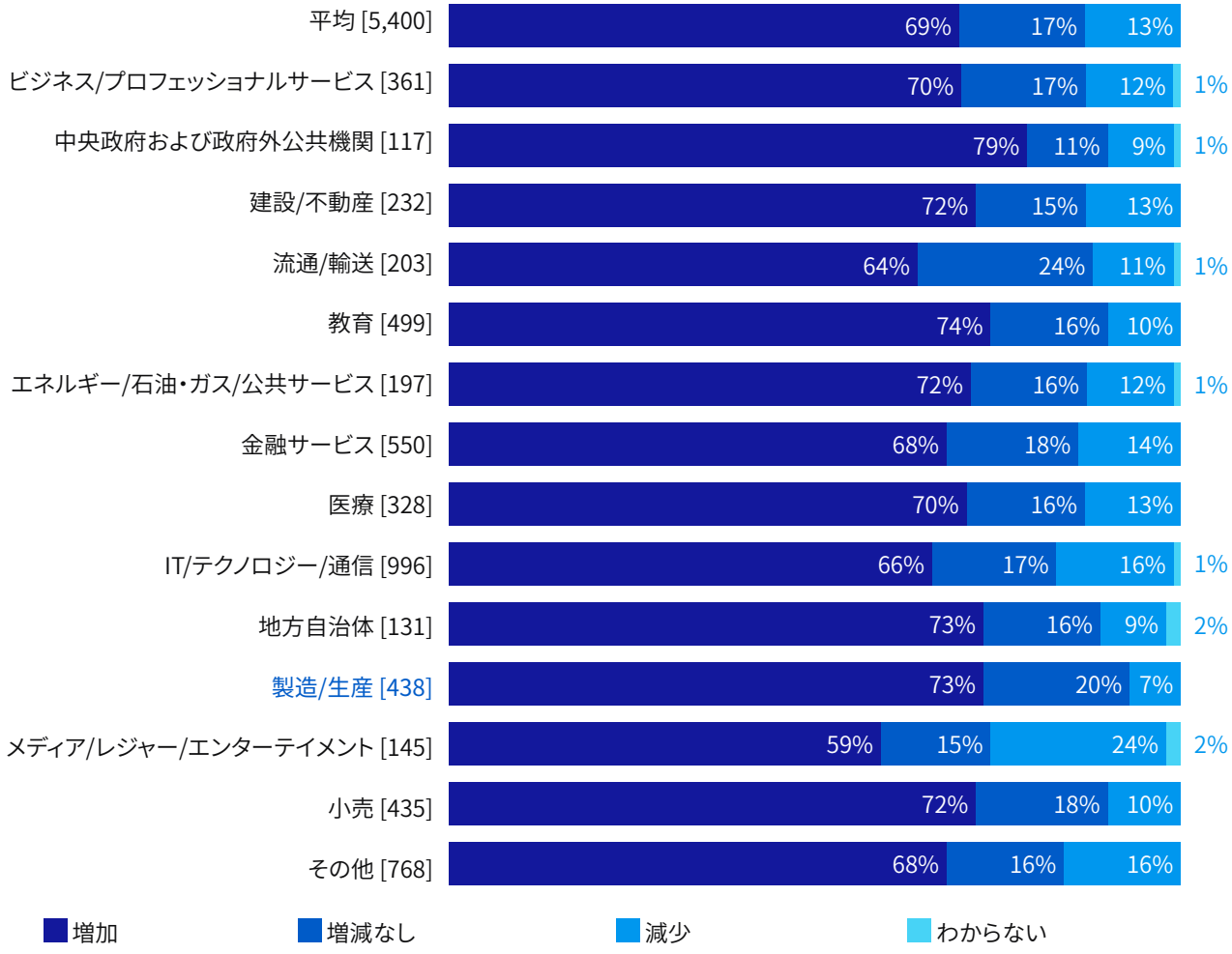
ランサムウェアは、サイバーセキュリティの課題の1つに過ぎない

ランサムウェアは、製造/生産業にとってサイバーセキュリティの大きな問題ですが、唯一の問題ではありません。IT チームは、同時に複数のサイバーセキュリティの問題に対処していますが、問題はパンデミックによって悪化しました。

2020年にサイバーセキュリティの仕事量は増加

製造/生産業の IT チームは、最もパンデミックの影響を受けた業界であり、73% の組織が、2020年にサイバーセキュリティの仕事量が増加したと回答しています。これは、年間のワークロードの減少率が最も低いと報告された業種でもあります。

2020年の 1年間のサイバーセキュリティの仕事量の変化



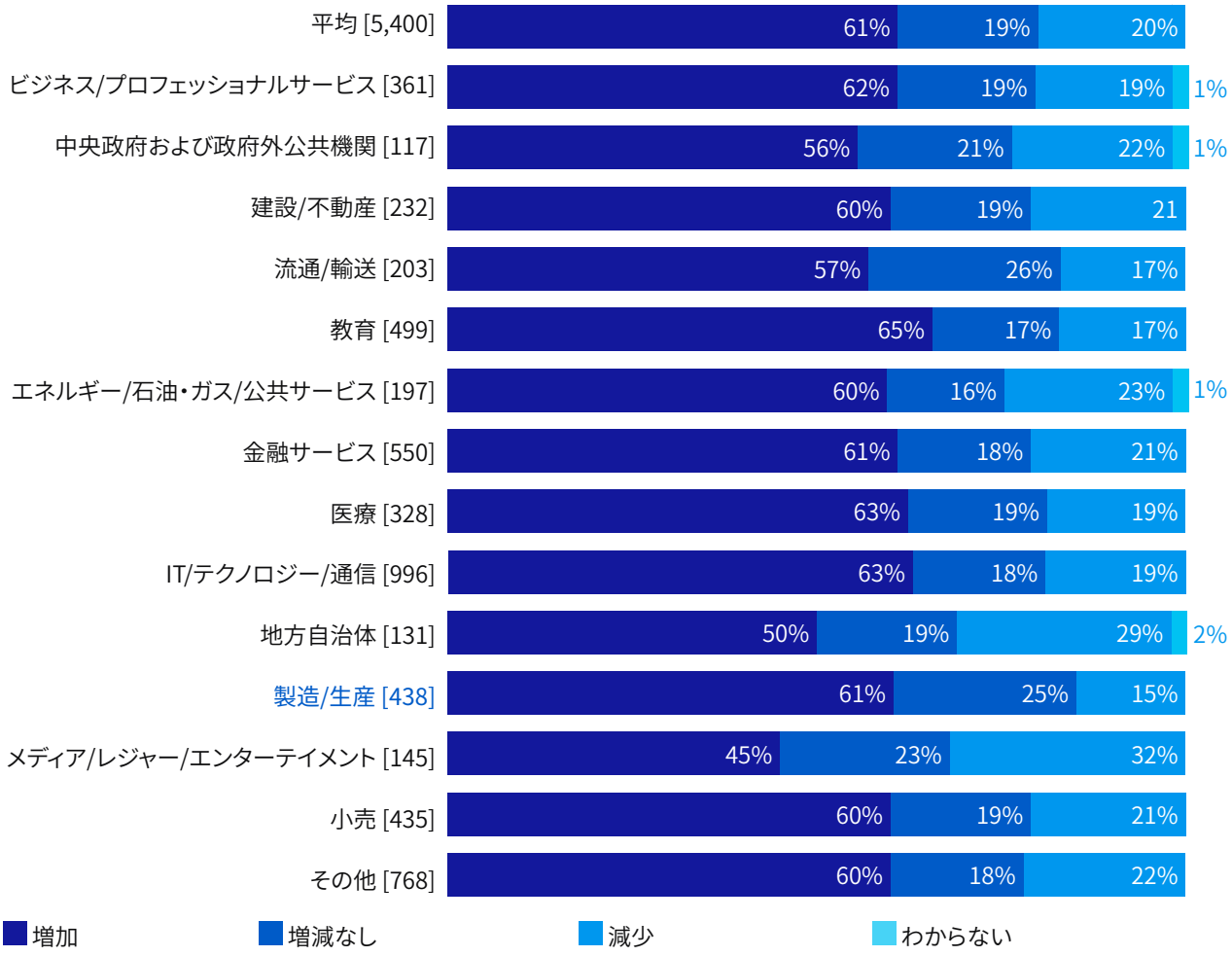
2020年の 1年間、サイバーセキュリティの仕事量は減少した / 増加した / 増減なしだった [回答した組織数]、業界ごとに分割。

世界がロックダウン状態に入り、この業種は生産施設のリモート管理へと急速に移行することを余儀なくされました。また、パンデミックの最初の数か月で定期的に商品不足が話題になり、大きな影響を受けたサプライチェーンと協力する必要がありました。製造/生産業の IT チームは、従来は人間による関与がかなり必要だった生産量の維持をサポートするという課題に直面しました。産業施設へのリモートアクセスを容易にし、在宅勤務の従業員のための安全なリモートソリューションを提供する必要性が、IT チームの作業負荷の増加を大きく左右する要因と考えられます。新しいオンラインプラットフォームでのセキュリティ確保に重点を置いたことで、ランサムウェアの脅威を監視したり、対応したりする IT チームの能力が低下した可能性があります。

仕事量が増加したことで対応時間が遅延

サイバーセキュリティの仕事量が 2020年に増加した結果の 1つとして、IT 問題への対応時間が遅くなりました。製造/生産業はかなりの影響を受け、回答者の 61% が応対時間が昨年よりも増加したと回答しています。また、この業種は、IT に関する問い合わせの応対時間が短縮される可能性は最も低いです。

2020 年の IT に関する問い合わせへの対応時間の変化



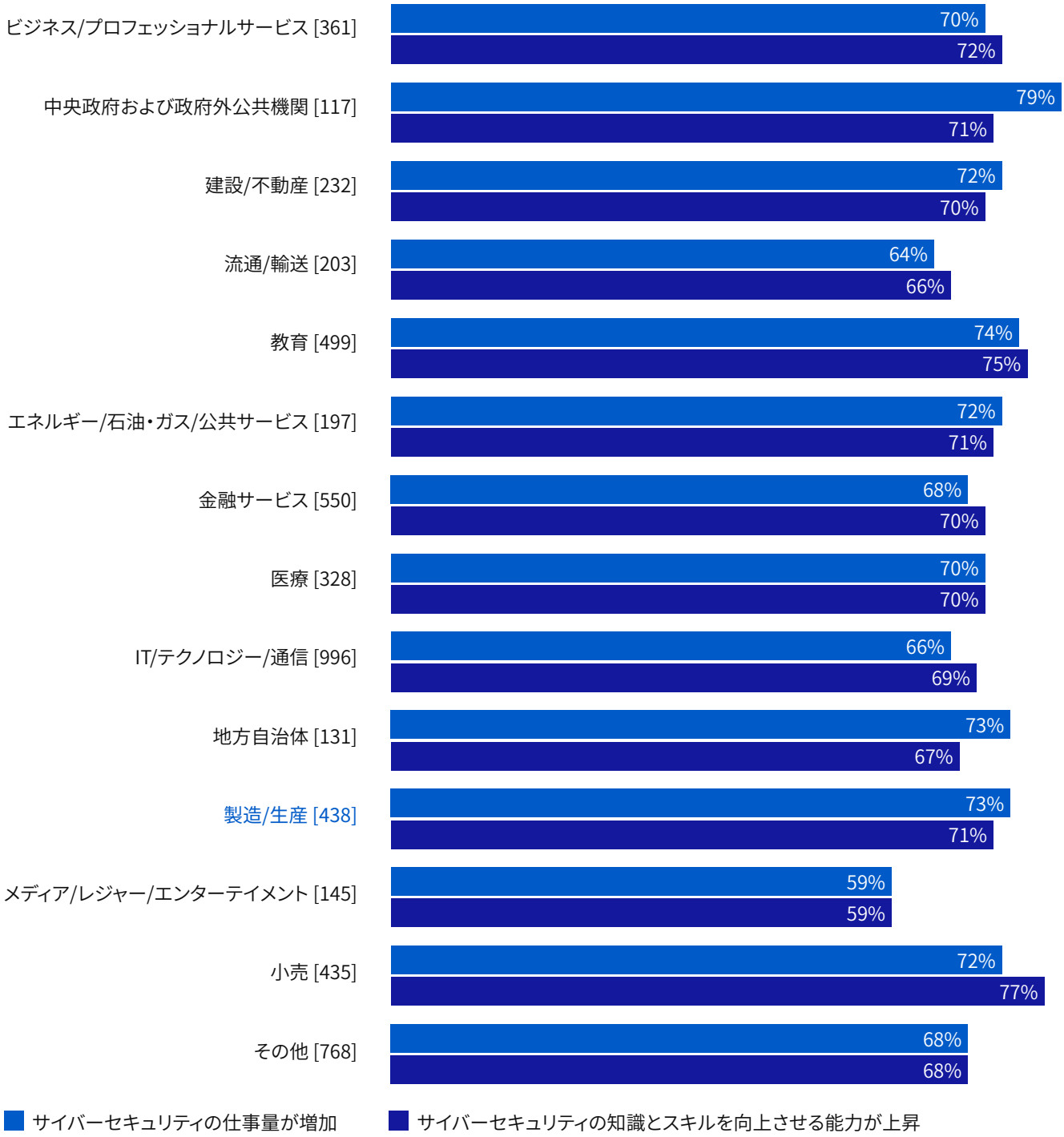
2020年、IT 問題への対応時間は減少した / 増加した / 増減なしだった。[回答した組織数]、業界ごとに分割。
注：四捨五入の影響で、一部の合計は 100% を超えています

攻撃者が組織の環境に侵入した場合、できるだけ早くその動作を阻止することが不可欠です。ネットワークを探索してデータにアクセスできる期間が長ければ長いほど、攻撃による金銭的被害および運用上の影響は大きくなります。したがって、対応時間の遅延は警戒を促します。

仕事量の増加により、知識とスキルが向上

このような状況でも、ポジティブなことがあります。サイバーセキュリティの仕事量の増加と、サイバーセキュリティに関する知識とスキルの開発能力の向上にははっきりとした相関関係があります。

サイバーセキュリティの仕事量の増加とサイバーセキュリティに関する知識とスキルの開発能力の向上



2020年の 1年間、サイバーセキュリティの仕事量またはサイバーセキュリティの知識とスキルを向上させる能力は増加した [回答した組織数]、業界ごとに分割

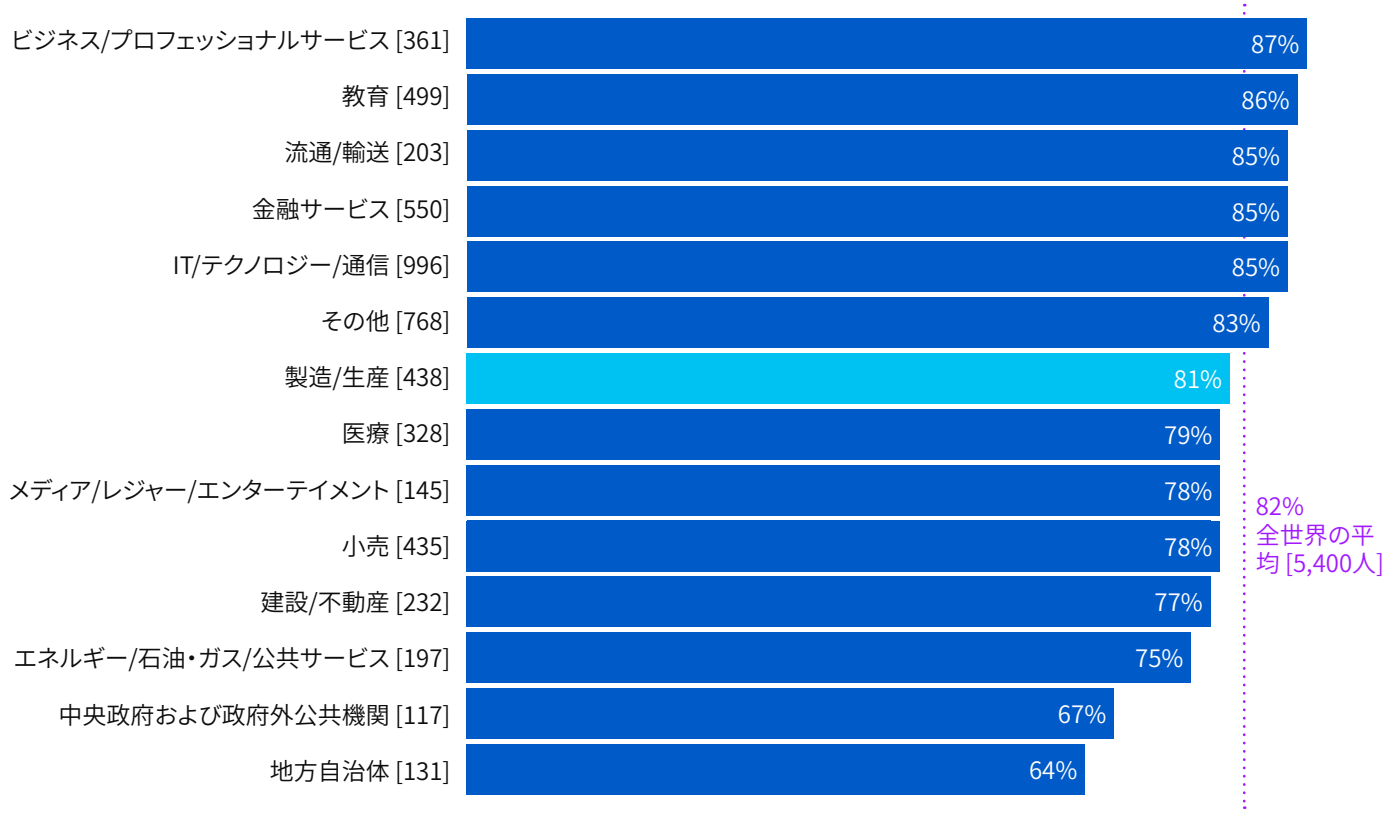
製造/生産業の IT チームの 71% は、2020年の 1年間、サイバーセキュリティの知識とスキルを向上させる能力が高まったと回答しています。

仕事量の増加はプレッシャーを与えることになりますが、新しいことを学ぶ機会が増えることも意味します。パンデミックの独特な状況によって、IT チームは、これまでに要求されたことのない成果を出す必要があった可能性があります。

将来の課題に対応できる環境の準備

製造/生産業の回答者の 81% は、組織内で疑わしいアクティビティを検出した場合、世界平均 (82%) に沿って、きちんと調査するために必要なツールや知識を持っていると思うと回答しています。この業種でサイバーセキュリティの仕事量が増加していることは、素晴らしいニュースです。サイバー脅威を調査して対処するには、適切なツールと知識が不可欠です。

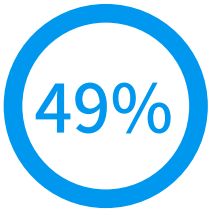
疑わしいアクティビティを調査するためのツールと知識がある



組織内の疑わしい活動を検出した場合、それを完全に調査するために必要なツールと知識がある。
強くそう思う、そう思う。一部の回答の選択肢を省略 [回答した組織数]、業界ごとに分割

展望

今後のランサムウェア攻撃への予測



将来的に攻撃を受けることを
予測している割合

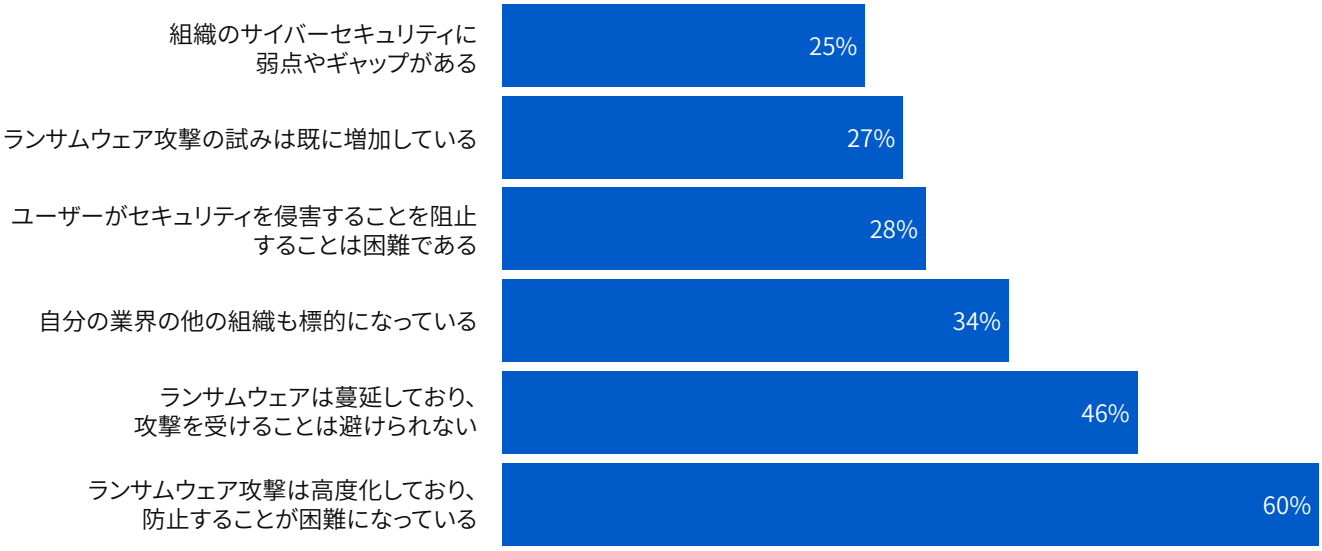
将来的に攻撃を受けることを
予測していない割合

[438人]「昨年、ランサムウェア攻撃を受けましたか？」という質問に「いいえ」と答えた製造/生産業の回答者数

このレポートの冒頭で述べたように、製造/生産業の回答者の 64% は、昨年ランサムウェア攻撃を受けませんでした。49% は将来的に攻撃を受けることを予測しています。逆に、15% は攻撃を予測していません。

製造/生産業が攻撃を受けると予測する理由

ランサムウェア攻撃は受けなかったが、今後受けると予測している製造/生産業企業の回答者のうち、最も多かった理由としてのは、ランサムウェア攻撃は高度化しているため、阻止するのがますます難しくなっているというものです (60%)。この割合は高いですが、このような組織が、ランサムウェアの進化を警戒していることはよいことであり、慎重な姿勢が、昨年の潜在的なランサムウェア攻撃を正常にブロックできた一因であるという可能性さえあります。



今後、組織がランサムウェア攻撃を受けると予測する理由は何ですか？[215人 過去 1年間、ランサムウェア攻撃を受けなかったが、今後受けると予測する製造/生産業の回答者数、一部の回答の選択肢を省略]

さらに、回答者の 46% は、ランサムウェアが非常に蔓延しているため、攻撃を受けることは避けられない、というものです。34% は、業界内の他の組織が標的にされており、攻撃を受ける可能性が高いと考えています。

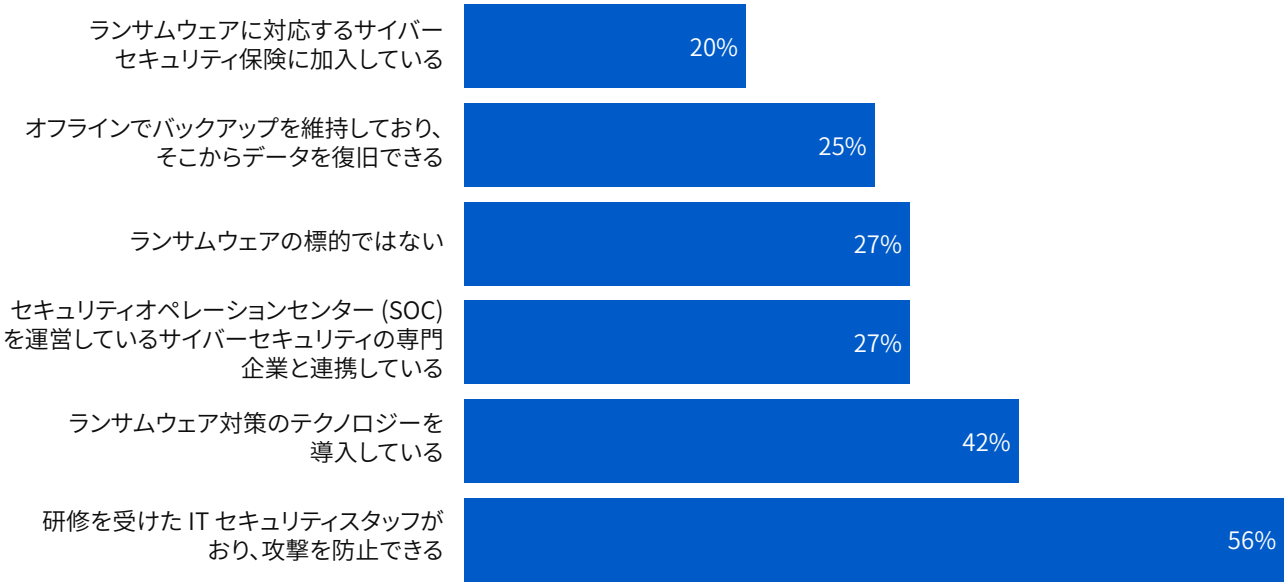
回答者の 28% は、今後ランサムウェア攻撃を受ける主な原因として、従業員のセキュリティが侵害されることを挙げています。巧妙な攻撃を受けている中で、多くの IT チームが個別のユーザーを非難するという安易な選択肢を取らないことは心強いことです。

同様に、製造/生産業の回答者の 25% が、組織内のサイバーセキュリティ対策には弱点やギャップがあることを認めています。もちろん、セキュリティホールがあることは良いことではありませんが、これらの問題を認識することは、防御力を高めるための重要な第一歩です。

製造/生産業がランサムウェア攻撃を受けないと予測する理由

64人の製造/生産業の回答者は、昨年はランサムウェア攻撃を受けておらず、今後も受けないであろうと予測しています。

今後、ランサムウェア攻撃を受けないと予測する理由



今後、組織がランサムウェア攻撃を受けないと予測する理由は何ですか？[64人] 昨年、ランサムウェア攻撃を受けておらず、今後も攻撃を受けないと予測する製造/生産業の回答者数、一部の回答の選択肢を省略

このような自信を持てる最大な理由は、攻撃を阻止できるトレーニングを受けた IT スタッフを採用していること (56%) で、続いてランサムウェア対策テクノロジーの使用 (42%) です。ランサムウェア対策を効果的に実施するためには、高度で自動化されたテクノロジーが不可欠ですが、人間が手動で実行している攻撃を防止するには、高いスキルを有する専門家による監視と介入も必要です。自社のスタッフでも外部の専門家でも、人間の専門家は、ランサムウェアを操る攻撃者が自社を狙っていることを示すいくつかの動かぬ兆候を見分けることができます。ランサムウェアの脅威が継続するなかで、すべての組織の担当者が専門知識を身に付けることを強く推奨します。

ランサムウェアの被害を受けないと予測している製造/生産業の回答者の 27% は、セキュリティオペレーションセンター (SOC) を運営するサイバーセキュリティ企業の専門家と連携しています。組織が必要に応じてサイバーセキュリティの専門知識をアウンとソーシングし、保護を拡大しているのを見るのは心強いことです。

しかし、朗報ばかりではありません。懸念される結果も明らかになっています。

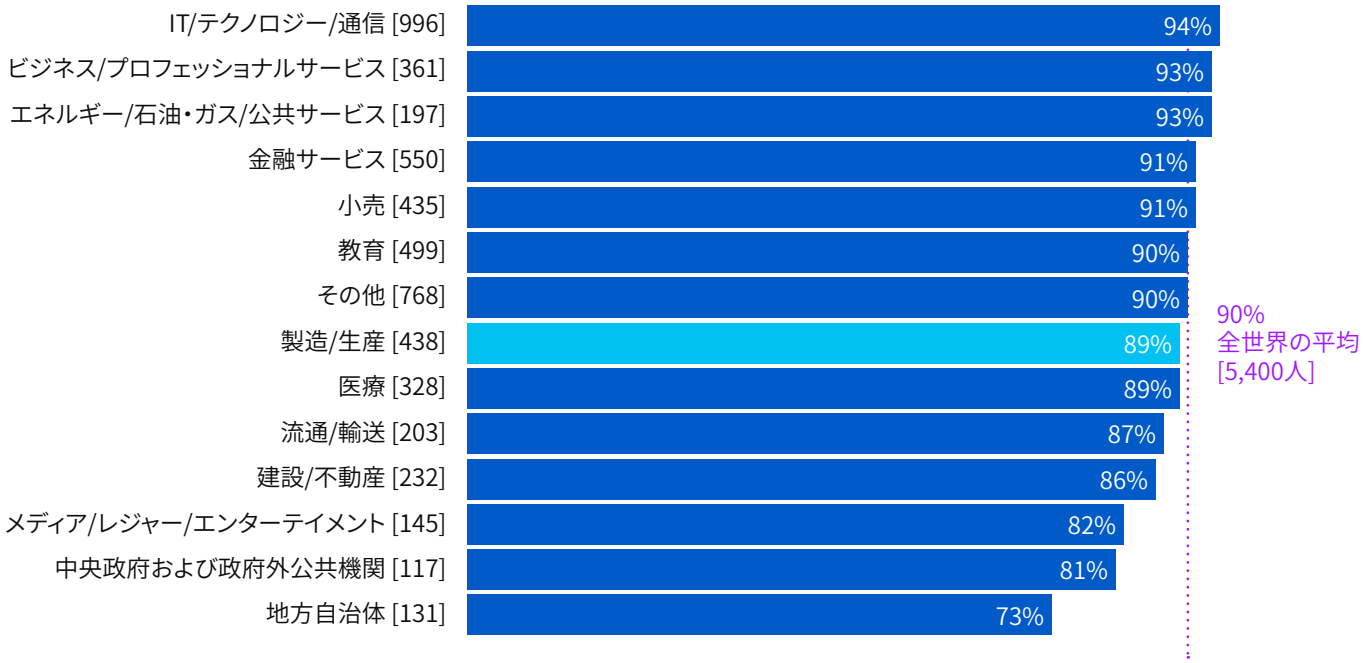
- 攻撃を受けないと予測している製造/生産業の回答者の 38% は、ランサムウェア攻撃に対する保護をまったく提供しないアプローチを妄信しています。
  - 20% が、ランサムウェアに対するサイバーセキュリティ保険への加入を挙げています。保険は、攻撃に対処するコストには対応していますが、攻撃自体は阻止しません。
  - 25% がオフラインでのバックアップを維持 - バックアップは攻撃後のデータを復元する手段として貴重ですが、バックアップがあっても、攻撃を防ぐことはできません。

    注：一部の回答者は上記の両方の選択肢を選択しており、38% がこれら 2つの選択肢の少なくとも 1つを選択しています。
- 27% は、ランサムウェアの標的ではないと考えています。残念ながらこれは事実ではありません。まったく安全な組織というものは存在しません。

製造/生産業は十分な準備が整っている

大規模なサイバー攻撃やインシデントへの対応は、非常に大きなストレスとなります。攻撃への対応によるストレスを完全に排除することはできませんが、効果的なインシデント対応計画を導入すれば、影響を必ず最小限に抑えることが可能です。

大規模なマルウェアインシデントからの復旧計画を策定している割合



組織の事業継続計画 (BCP) / 災害復旧計画 (DRP) には、大規模なマルウェアインシデントの復旧計画が含まれていますか？はい、マルウェアインシデントからの包括的で詳細な復旧計画を策定している。はい、マルウェアインシデントからの部分的な復旧計画を策定している、[回答した組織数] 一部の回答の選択肢を省略し、業種ごとに分割

そのため、製造/生産業の 89% がマルウェアインシデントの復旧計画を作成、半数弱 (49%) が完全かつ詳細な計画を作成、そして計画の一部を作成しているのは 41% であるということが分かったのは心強いことです。これらの統計情報は、業界間の平均値に沿っています (90%)。

提言

この調査結果を踏まえて、ソフォスの専門家は、すべての業界のすべての組織に対して次のベストプラクティスを提言します。

1. **攻撃を受ける前提で対策を講じてください。**ランサムウェアは依然として多く発生しています。業界、国、組織の規模を問わず、このリスクから免れることはできません。サイバー攻撃についても「備えあれば憂いなし」です。

2. **バックアップを作成してください。**バックアップは、攻撃を受けた後に組織がデータを復旧するための最も重要な手段です。また、身代金を支払っても、すべてのデータが戻ってくることはほぼ皆無ですので、攻撃を受けた場合には、いずれの場合でもバックアップを利用する必要があります。

バックアップ戦略のヒントは、3-2-1 の法則です。これは少なくとも **3**つのコピーを作成し (現在使用しているデータの他に 2つ以上のコピーを保管)、少なくとも **2**つの異なるバックアップシステムを使用し (1つのバックアップシステムで障害が発生した場合に備えて)、少なくとも **1**つのコピーをオフラインで、できればオフサイト (攻撃者が改ざんできない場所) に保存する戦略です。

3. **多層防御を導入してください。**恐喝型の攻撃が大幅に増加している中で、攻撃者を組織の環境に寄せ付けないことがこれまで以上に重要になっています。サイバー犯罪者はネットワーク環境内のさまざまな場所を攻撃しています。これらの多くの場所で攻撃を防御できるように多層防御のアプローチを使用してください。

4. **人の専門家とランサムウェア対策テクノロジーを融合させてください。**ランサムウェアを阻止するには、ランサムウェア対策の専用のテクノロジーと人間主導の脅威ハンティングを組み合わせた防御が鍵となります。これらのテクノロジーにより、大規模で自動化された攻撃を防止できるようになります。一方で、人間による専門家は、高度なスキルを有する攻撃者による侵入の痕跡を検出・特定する戦術、技術、手順において優れた能力を発揮します。組織内にスキルを持つ担当者がいない場合は、サイバーセキュリティの専門企業のサポートを検討してください。SOC は現在、あらゆる規模の組織にとって現実的なオプションとなっています。

5. **身代金は支払わないでください。**ランサムウェア攻撃により組織の業務が停止してしまった場合は、身代金を支払って問題を解決したいと思うかもしれません。しかし、倫理的な問題に関係なく、データを取り戻すために身代金を支払うことは効果的な方法ではありません。身代金を支払うことに決めた場合でも、攻撃者から復元できるファイルは平均で全体の 3分の 2 ほどであることを念頭に入れて、費用対効果を分析してください。

6. **マルウェア攻撃からの復旧計画を策定してください。**サイバー攻撃が甚大な侵害をもたらすセキュリティ侵害に発展するのを防ぐには、事前に準備をすることが最善です。攻撃の被害に遭った多くの組織は、インシデント対応計画を適切に導入していれば、多額のコスト、被害、混乱を回避できたと考えています。

その他の資料

ソフォスのインシデント対応ガイドは、組織がサイバーセキュリティのインシデント対応計画のフレームワークを定義し、計画に追加するべき 10 の重要な対策について説明しています。

セキュリティ対策の担当者の方は、インシデント対応の専門家による 4つの重要なヒントもご覧ください。サイバーセキュリティインシデントへの対応に関する大切な教訓を紹介しています。

この 2つの資料は、数千件ものサイバーセキュリティのインシデントに連携して対応してきた Sophos Managed ThreatResponse チームと SophosRapid Response チームの実際の経験をベースに作成されています。

ランサムウェアの詳細と、ソフォス製品が組織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。

2021-09-20 (SB-NP)

SOPHOS