



REPORT

# 2024 年 OT サイバーセキュリティに関する 現状レポート

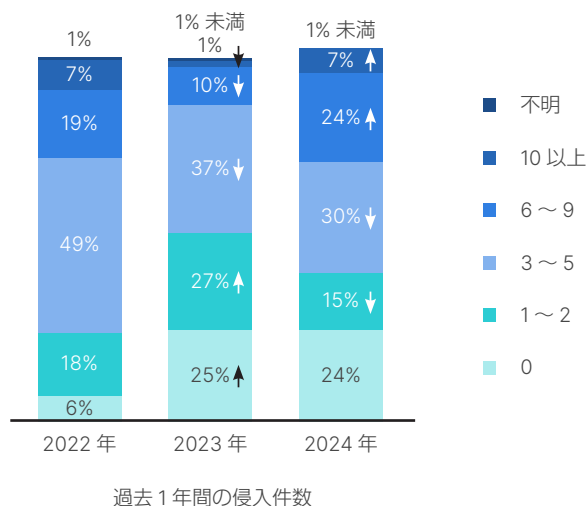
# 目次

主な調査結果 .....	3
概要 .....	5
はじめに.....	5
OT セキュリティの重要なインサイト.....	6
2024 年の調査の詳細分析.....	10
世界全体での影響 .....	14
ベストプラクティス.....	15
調査方法.....	16
まとめ.....	17

## 主な調査結果

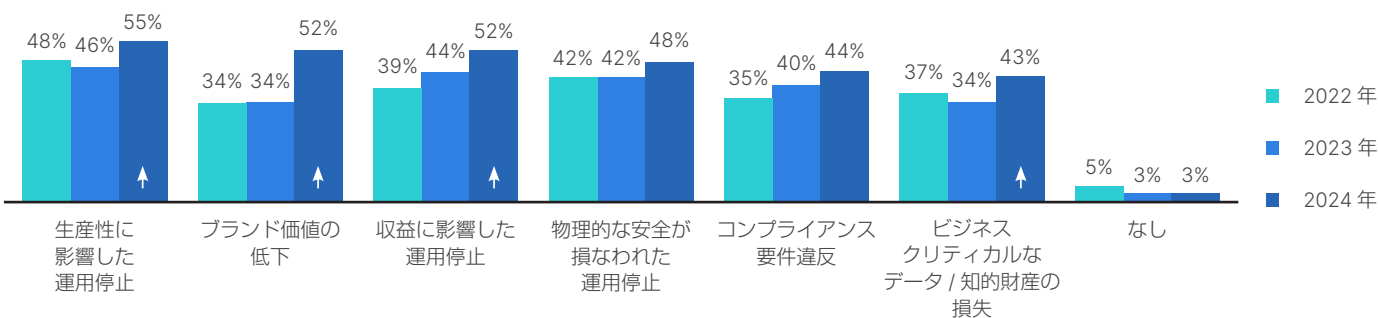
### サイバーセキュリティインシデント

調査対象者の約 3 分の 1 (31%) が 6 回以上の侵入を経験したと回答し、昨年のわずか 11% から大幅に増加しました。特に、成熟度が高い組織が今回の調査で多くの侵入を報告しました。マルウェアが減少したことを除けば、**いずれの侵入タイプも前年より増加**しました。フィッシングとビジネスメールへの侵入が最も一般的な侵入タイプで、モバイルセキュリティの侵害と Web の侵害が最も一般的な侵入手法でした。



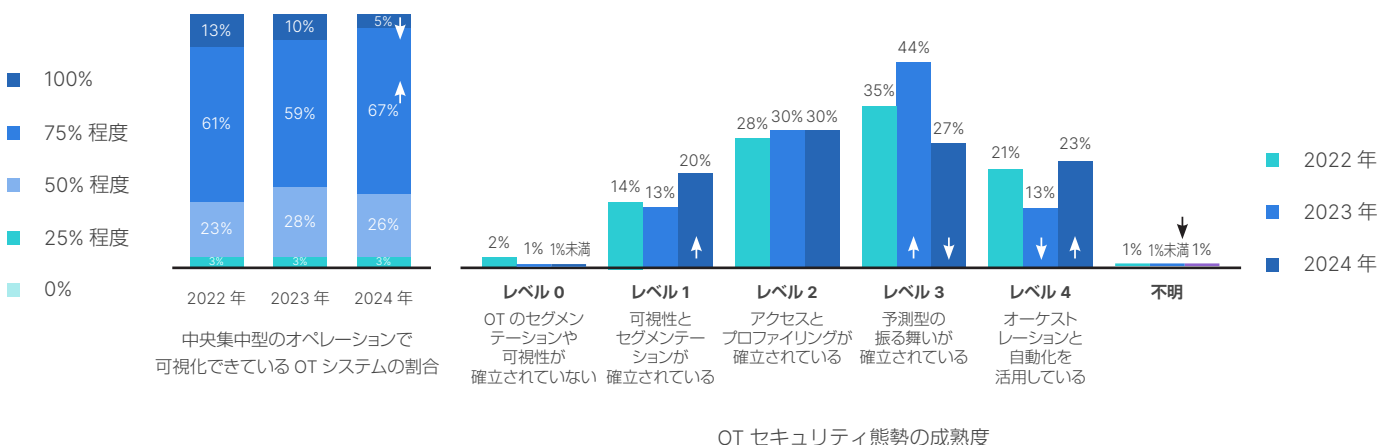
### 侵入の影響

OT の侵入による負の影響も、影響のすべてのカテゴリで悪化しました。調査対象者の半数以上 (52%) が、**ブランド価値の低下**を回答しましたが、2023 年にはこの割合は 34% でした。**ビジネスクリティカルなデータの損失と生産性の低下**も、顕著な傾向でした。(前年の 34% から 43% に増加)。



### OT がサイバーセキュリティに与える影響

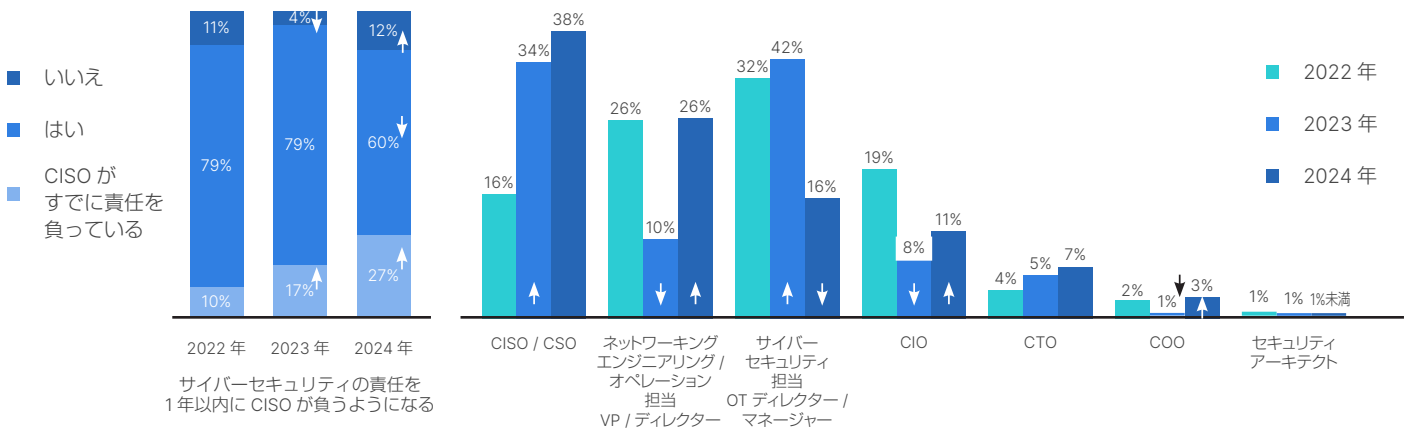
中央集中型のサイバーセキュリティオペレーションで、**OT システムを 100% 可視化できていると回答した組織が大幅に減少**しました (2022 年は 13%、2023 年は 10%、今年はわずか 5%)。恐らくこれは、組織の OT セキュリティ態勢の成熟度の上昇に伴い、その可視性の盲点を認識するようになったためです。今年の調査では、**成熟度の基本レベル** (可視化とセグメンテーションの確立) と最高レベル (オーケストレーションと自動化の機能の活用) の**両端で割合が上昇**しました。



## OT セキュリティの責任者

成熟度の上昇のもう 1 つの明確な兆候として、**CISO がセキュリティの責任をすでに負っている**と回答した組織が、2022 年にわずか 10% であったのに対し、2023 年に 17%、今年は 27% と、着実に増加している点が挙げられます。同時に、今後 1 年以内に CISO が OT セキュリティの責任を負うようになる予定はないと回答した組織が、2022 年の 11% から昨年は 4% に減少しましたが、昨年の傾向が逆転し、2024 年に再び上昇して 12% になりました。

今年の調査結果は、OT サイバーセキュリティに関する最終責任者がサイバーセキュリティ担当 OT ディレクターから**ネットワークエンジニアリング / オペレーション担当 VP / ディレクター**に移行しつつあることも示しています。このように上位の役職が責任を負うようになっていることは、OT セキュリティが取締役会レベルで議論されるようになりつつあることを示している可能性があります。





## 概要

フォーティネットの「**OT サイバーセキュリティに関する現状レポート**」は、今年で 6 年目を迎えました。2024 年のレポートは、定評ある第三者調査会社が 550 人以上の OT プロフェッショナルを対象に世界規模で実施した調査で得られた包括的なデータに基づくものです。

OT 組織が新しいデジタルツールやテクノロジーを環境に導入するにつれて、セキュリティの課題がさらに複雑なものになります。NIST は、「一般的な IT システムでは、このような問題を処理することを想定してセキュリティソリューションが設計されているが、同じソリューションを OT 環境に導入する場合は注意が必要であり、OT 環境に合わせてカスタマイズされた新しいセキュリティソリューションが必要になる場合もある」と指摘しています<sup>1</sup>。

今年のレポートは、過去 1 年間に OT のセキュリティ態勢や必要不可欠なツールや機能への投資に一定の進展があったことを示しています。しかしながら、IT と OT のコンバージェンスが完了した世界で、増加の一途をたどる攻撃を効果的に管理するためにやるべきことはいくつも残されています。2024 年の調査結果から、3 つの注目すべき傾向が明らかになりました。

- 組織への侵入とその影響がこの 1 年間に悪化した。
- 上位の役職が OT サイバーセキュリティの責任を負うようになっている。
- OT セキュリティ態勢は重要な分野で成熟しつつあるが、その取り組みは道半ばである。

これらの調査結果の重要なインサイトと詳細な分析により、OT リスクの管理は動的であり、時として大きく変動することがわかりました。以上の具体的な課題を考慮し、今年のレポートでは、組織の OT セキュリティ態勢の改善に役立つ最新のベストプラクティスとヒントも紹介します。

## はじめに

OT システムに対する脅威は、対立国の政府機関、テロリスト集団、不満を抱える従業員、悪意のある侵入者、複雑さ、自然災害、内部関係者による不正行為、人為的なミスや、確立されたポリシーや手順に従わないなどの意図しない行為など、多くの理由で発生する可能性があります<sup>2</sup>。

機密度の高い OT システムは、今日のデジタル世界を想定して設計されたものではなく、比較的隔離された場所で安全に業務の遂行ができていた時代に作成されたものです。変化する環境でのこれまでとはまったく違うデジタルツールの採用は、新たな利便性と機能をもたらすのと同時に、ネットワーク接続の増加に伴うあらゆるサイバーセキュリティリスクをもたらしました。

「**2024 年 OT サイバーセキュリティに関する現状レポート**」が示すように、前年に明らかになった肯定的な成果の一部がわずか数ヶ月で消滅してしまう可能性もあります。

### OT に常に存在するリスク

今年の調査の回答は、OT 攻撃が増加しているというニュース報道を裏付けるものです<sup>3</sup>。フォーティネットの最新の**グローバル脅威レポート**によると、産業用制御システム (ICS) や OT を標的にする攻撃は昨年下半年にすでに増加傾向を示すようになり、半数の組織でエクスプロイトが報告されています (エネルギー / ユティリティが最大の標的)<sup>4</sup>。

忘れてはならないのは、OT システムが攻撃者にとって極めて魅力的な標的であるということです。効果的な保護に必要なのは、警戒を怠らないこと、リソースを適切に配分することです。侵入の増加や攻撃の影響の悪化は、成熟しつつある組織において、OT システムが中央集中型のサイバーセキュリティオペレーションで完全に可視化できていないことを明確に示すものです。

製造など特定の業種では、要求された身代金の支払いに応じる組織が多く、多くの場合に多額の身代金を要求されます。製造業の企業で発生した侵害の 25% で、100 万ドル以上の身代金が要求されました<sup>5</sup>。製造業の企業にとってダウンタイムのコストが一般的に非常に高いことを考えれば、支払いに応じる可能性が高いのは納得できることです。

### 検知方法が脅威の進化に対応できていない

グローバル脅威レポートも、ランサムウェアの検知に成功している組織が以前より減少したことを示していることは（22% から 13% へ）、ランサムウェアがさらに高度化し、標的型になっていることを再認識させるものです<sup>6</sup>。2024 年の調査結果はこのレポートと一致しており、調査対象者の 56% がランサムウェア / ワイパーの侵入を経験したと回答しており、2023 年のわずか 32% から大幅に増加しました。

調査対象者は、サイバーセキュリティ指標の監視とレポートが強化されていると回答しましたが、これらの測定は侵入の検知と修復に役立っていないようです。組織はまた、恐らくはコスト削減のために、ペネトレーションテストや侵入テストを実施する数を減らしているようです。

### OT システムの保護という目標はまだ達成されていない

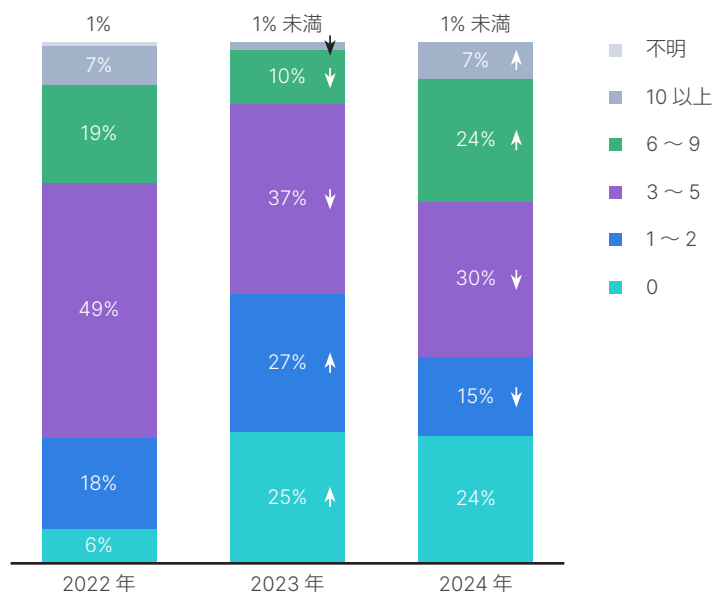
昨年のレポートでは、2024 年には OT システムの保護が大きく前進したとお伝えしたいという期待を述べましたが、報告された侵入が大幅に増加したことから、その願いをもう 1 年先延ばしにしなければならないようです。

以下に紹介する重要なインサイト、詳細の傾向分析、ベストプラクティスは、今後数ヵ月間に OT 保護を強化するための指針となるはずです。

## OT セキュリティの重要なインサイト

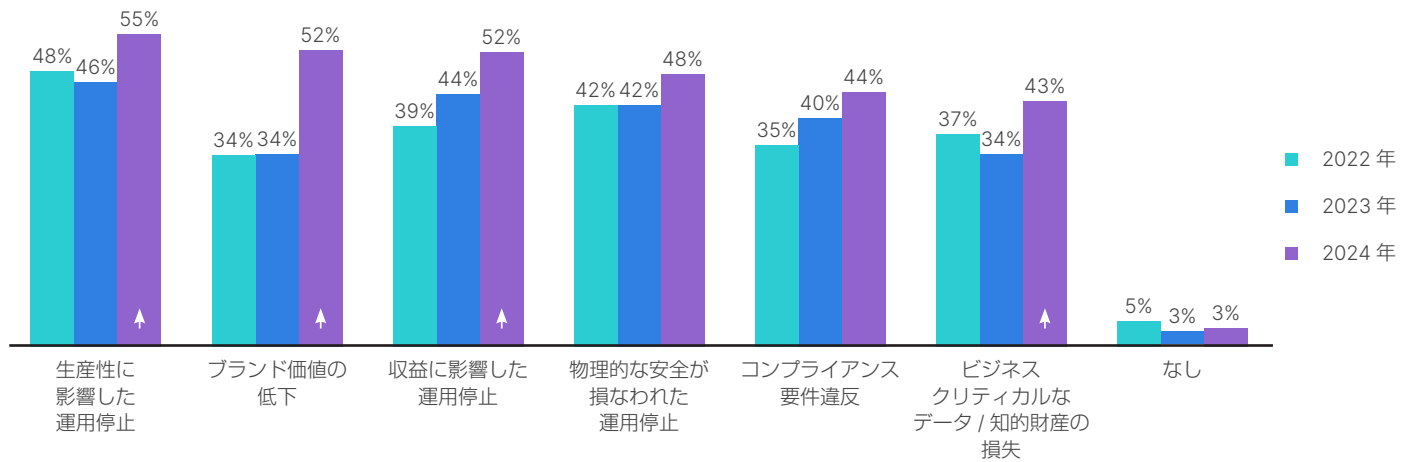
### 重要なインサイト 1：組織への侵入が増加し、影響も大きくなっている

今年の調査結果の最も重要なインサイトは、組織が経験した侵害が増えたということです。調査対象者の 3 分の 1 近くが、6 回以上の侵入を経験したと回答し、2023 年のわずか 11% から増加しました。マルウェアを除くすべてのタイプの侵入が増加したことも注目に値します。



質問：過去 1 年間に組織で発生した侵入の数は何件ですか？

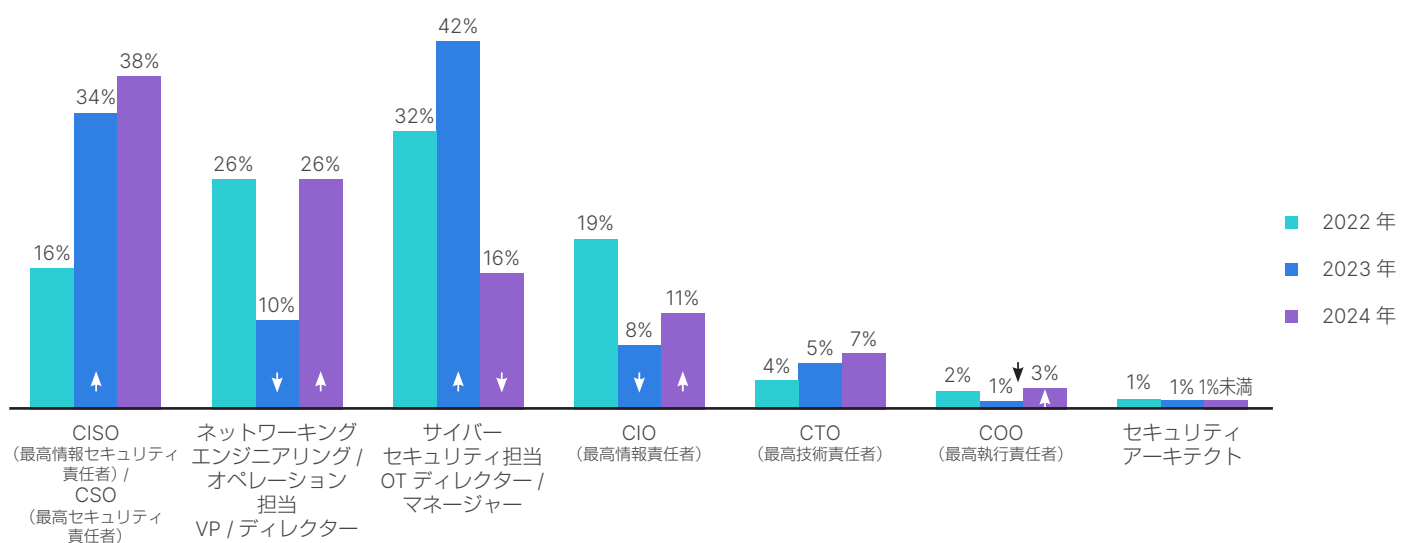
不正侵入の組織に対する影響も悪化しています。攻撃が成功したことでブランド価値が低下したという回答が増加しました。米国 SEC(米国証券取引委員会)のサイバーセキュリティ開示規則などの多くの法規制により、侵害を適切な時期に公表することが義務付けられるようになりました<sup>7</sup>。また、侵害の直接的な結果として、ビジネスクリティカルなデータの損失や生産性の低下を経験した組織が増加したこともわかりました。



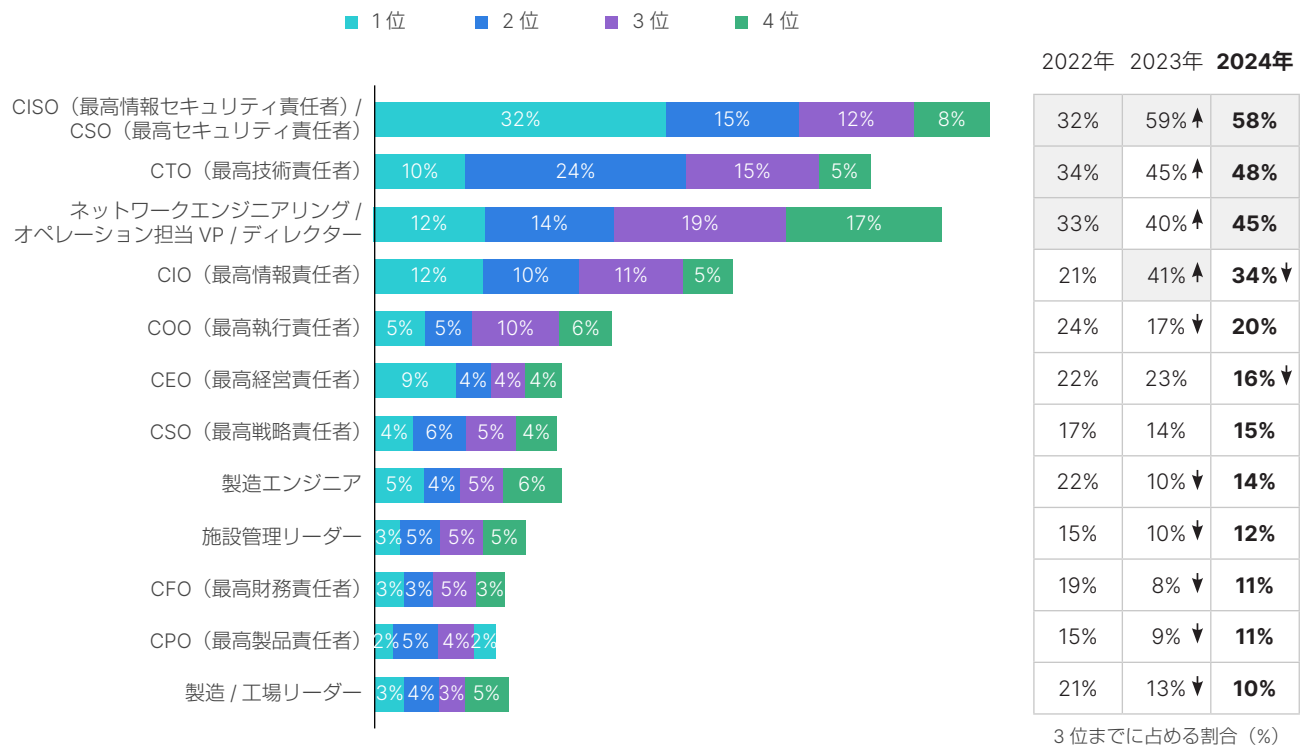
質問：侵入は組織にどのような影響を与えましたか？

## 重要なインサイト 2：上位の役職が OT セキュリティの責任を負うようになっている

OT サイバーセキュリティの管理責任が、OT のサイバーセキュリティ担当ディレクターから、ネットワークエンジニアリング / オペレーション担当 VP / ディレクターや CISO に移行しつつあります。上位の役職が説明責任を負うようになれば、OT セキュリティが、重要な問題として取締役会レベルで議論されるようになります。また、サイバーセキュリティの意思決定に影響する社内の最上位のリーダーが CIO から CISO / CSO、CTO、ネットワークエンジニアリングオペレーション担当 VP / ディレクターに移行しているのも興味深いことです。



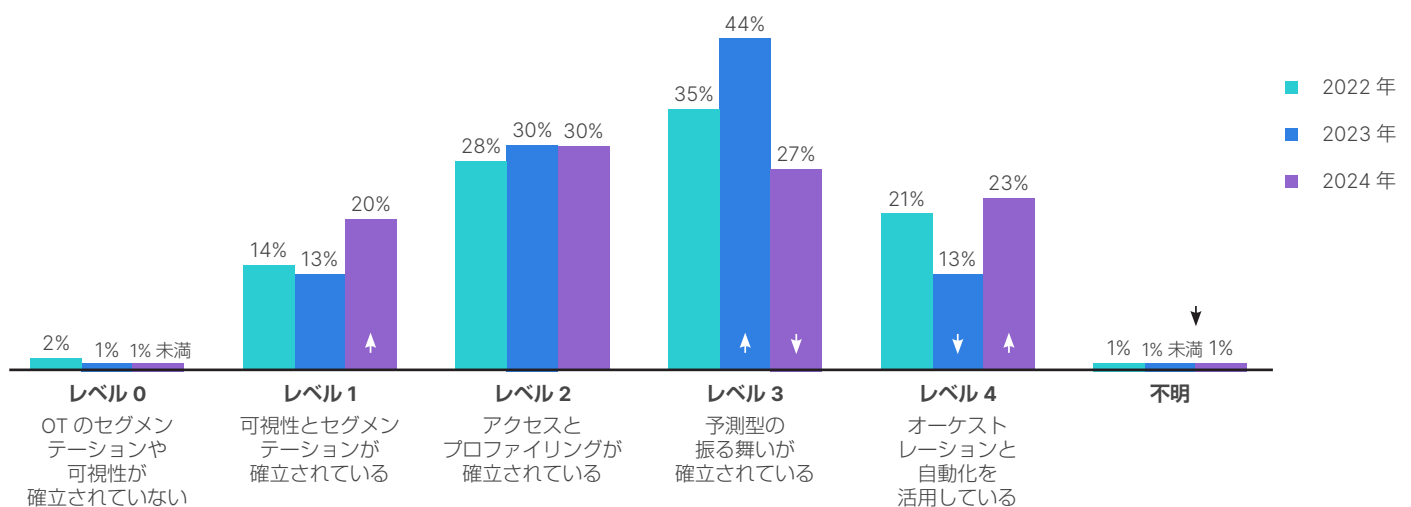
質問：組織の OT サイバーセキュリティに関する最終的な責任者は誰ですか？



質問：サイバーセキュリティに関する意思決定に影響を与える社内のリーダーは誰ですか？（4位まで）

### 重要なインサイト 3：OT サイバーセキュリティ態勢の成熟度は上昇している

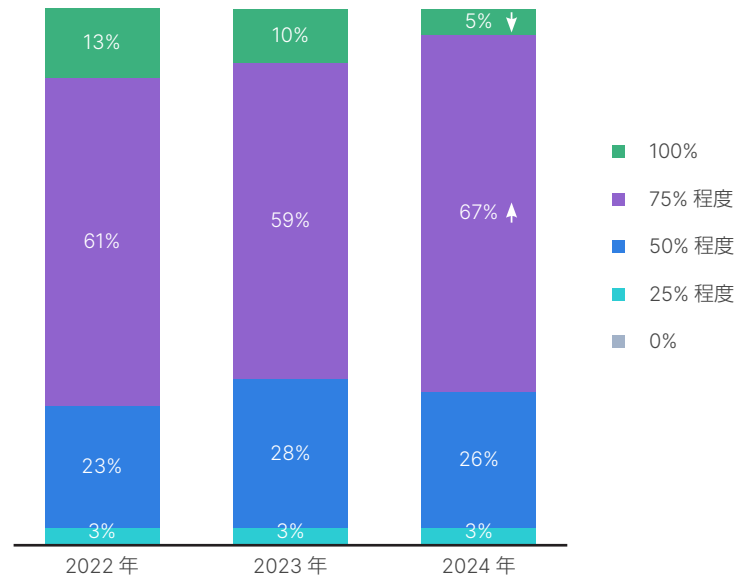
効果的なサイバーセキュリティ対策の実装という点で、IT インフラストラクチャは OT システムよりも大きく先行しています。とはいえ、OT セキュリティ態勢は、テクノロジーの成熟度の両端で大きく前進しました。最も基本的なレベルでは、20% の組織が可視性を確立し、セグメンテーションを実装していると回答し、前年のわずか 13% から増加しました。セキュリティ態勢の成熟度が最も高いレベル（オーケストレーションと自動化の機能の活用）も前年比で増加し、13% から 23% に上昇しました。



質問：貴社の OT セキュリティ態勢の成熟度はどれに該当しますか？

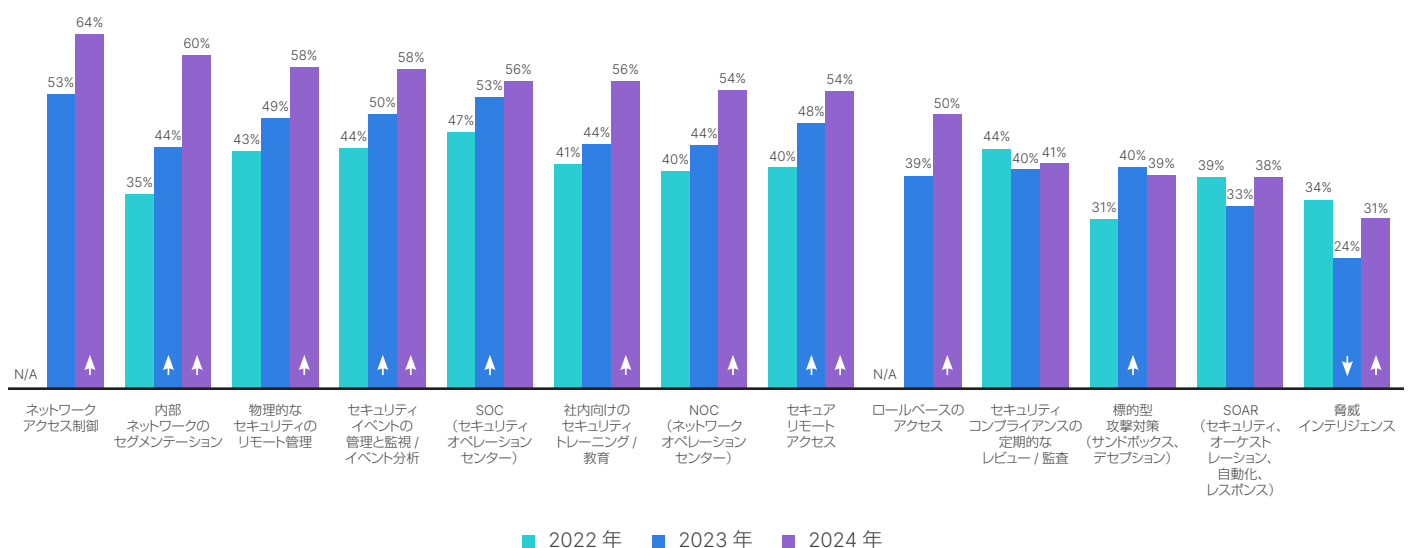


中央集中型のサイバーセキュリティオペレーションで OT システムが 100% 可視化されているという回答が昨年より減少しましたが（10% から 5% へ）、約 75% は可視化が向上したと回答しました。このような可視性に対する相反するとも思える自信は、たとえ「何がわからないかわからない」という理解だとしても、組織が自社の態勢をより現実的に理解するようになっているという点で、OT セキュリティの成熟度が上昇していることを示すものであるのかもしれません。多くの組織が昨年急増したセキュリティインシデントを調査する過程で、自社のインフラストラクチャに存在する盲点を発見した可能性があります。



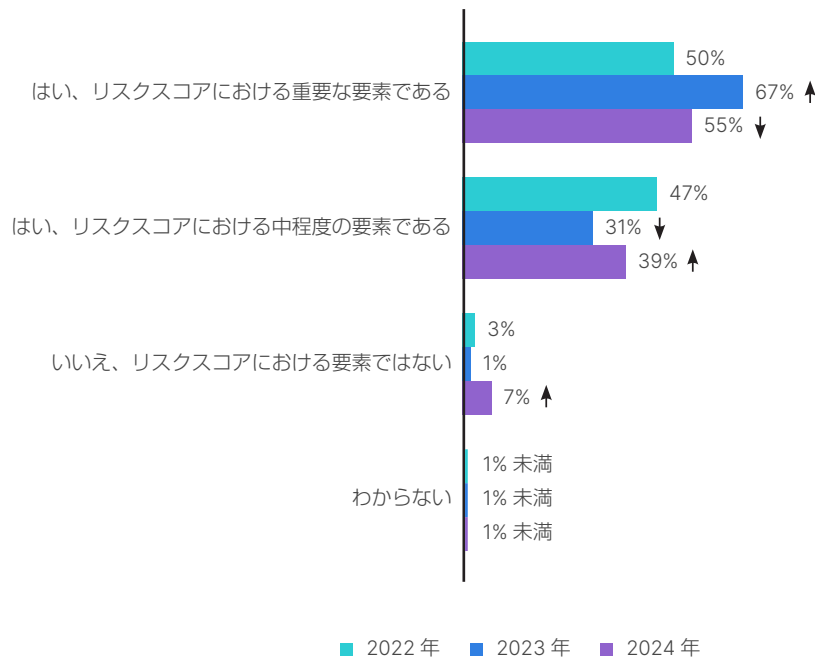
質問：貴社の中央集中型のサイバーセキュリティオペレーションで、何 % の OT システムを可視化できていますか？

OT プロフェッショナルが利用するサイバーセキュリティの機能やプロトコルは増え続けています。内部ネットワークのセグメンテーション、社内のセキュリティのトレーニングや教育、ロールベースのアクセスが、今年の増加率が最も大きかった分野です。これらの投資は前進を意味するものではありませんが、侵入の成功件数が今年大幅に増加したことは、OT に対する標的型攻撃の急増に対応するために必要とされる対策が多く残されていることを強調するものです。



質問：現在、どのようなサイバーセキュリティ対策とセキュリティ機能を導入していますか？

成熟度に関する気掛かりな傾向の1つは、より広範なリスクの算出に占める OT システムの割合が減少していることです。調査対象者は、組織の全体的なリスクスコアの決定にあたっての OT セキュリティ態勢の影響は小さくなっていると回答しました。最も注目すべきは、OT はリスクスコアの決定の「要因ではない」という回答が、2023 年のわずか 1% から 2024 年の 7% へと、前年比で大幅に増加したことです。



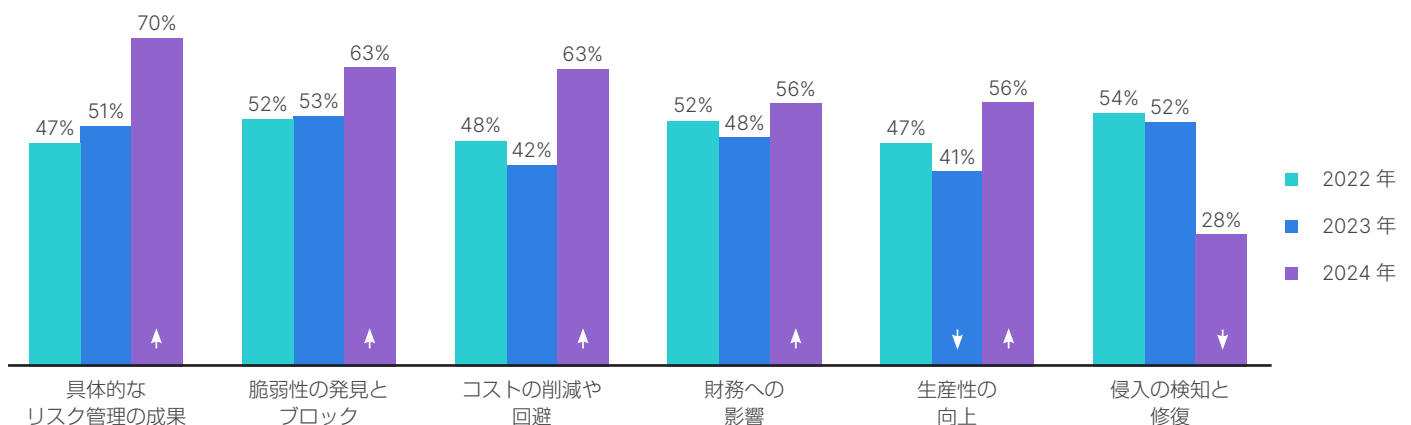
質問：OT のサイバーセキュリティ態勢は、経営幹部や取締役会に共有される広範なリスクスコアに含まれていますか？

## 2024 年の調査の詳細分析

質問：どのようなサイバーセキュリティの測定基準を追跡して報告していますか？

組織が追跡し、レポートするサイバーセキュリティ指標は多様化しています。しかしながら、例外として、侵入の検知と修復の追跡は大幅に減少し、2023 年の 52% から 2024 年には 28% にとどまりました。

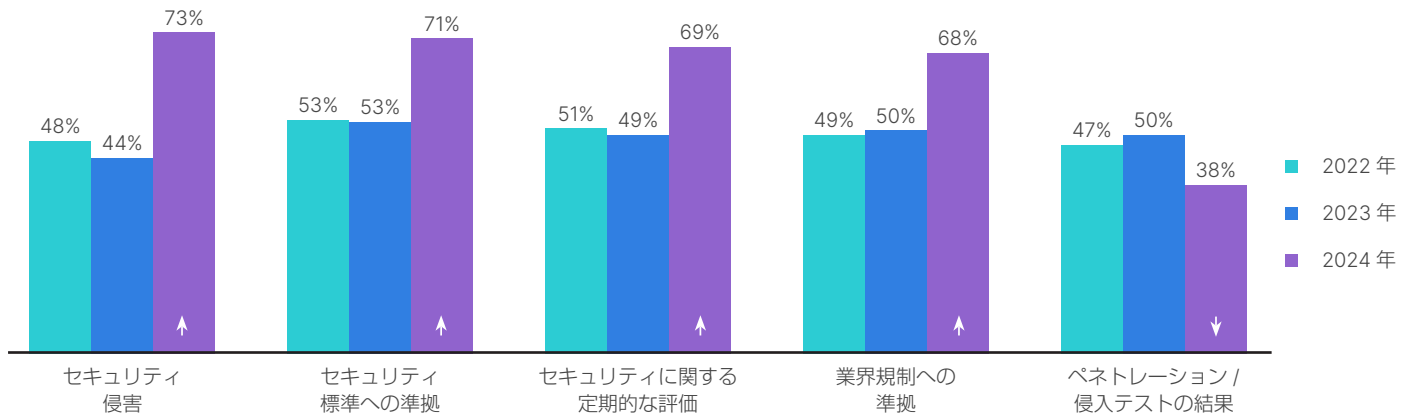
これを OT に影響を及ぼす侵入が今年増加したという現実と合わせて考慮すると、サイバーセキュリティ測定値の追跡の増加と実際の侵入の検知の減少という、この矛盾する結果は、測定値が誤った自信につながっていることを示すものである可能性もあります。



### 質問：どのような OT サイバーセキュリティの問題を上級管理職に報告していますか？

侵害、定期的な評価、コンプライアンス要件を始めとする、OT サイバーセキュリティのほぼすべての問題に関して、上級管理職に情報を報告しているという回答が増加しました。

ただし、例外として、ペネトレーションテストや侵入テストの結果が報告される割合は低下しました。この種のテストは多くの場合に高価で複雑でもあるため、この分野への投資を縮小し、追跡するサイバーセキュリティ指標を増やしてセキュリティ態勢を判断することを優先させている可能性があります。

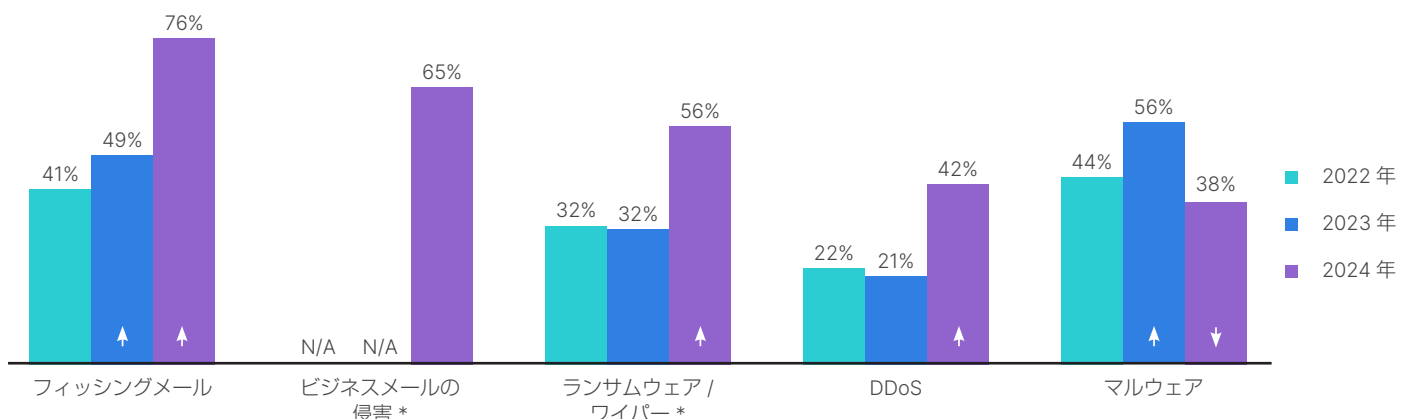


### 質問：どのような種類の侵入が発生しましたか？

重要なインサイトのセクションで紹介したように、今年の調査では、多くの調査対象者が、侵入が大幅に増加したと回答しました。これらの攻撃の背後にある具体的な原因を質問したところ、フィッシングメールが前年比で最も増加し、49% から 76% へと大幅に増加しました。2024 年にこの調査に新たに追加した「ビジネスメールの侵害」が、侵入タイプの首位（全組織の 3 分の 2 近くが経験）になりました。

ランサムウェアとワイパーによる侵入も大幅に増加し、2023 年の約 3 分の 1 から 2024 年は半数以上になりました。FortiGuard Labs の最近のレポートで指摘したように、ランサムウェアの数に減少の兆しはなく、RaaS（Ransomware-as-a-Service）が普及したことで、攻撃者がより高度で複雑な亜種を使用してネットワークに侵入するようになっています<sup>8</sup>。

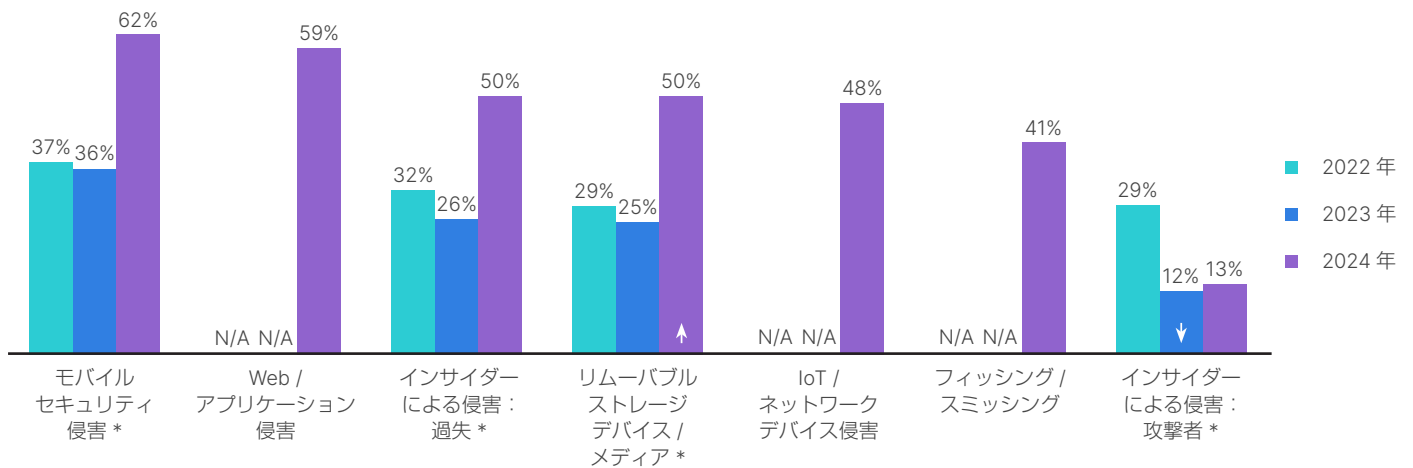
DDoS 侵入も昨年の 2 倍になり、減少したカテゴリはマルウェアだけでした。



\* 2024 年の調査の変更点:「ランサムウェア」を「ランサムウェア / ワイパー」に変更しました。「ビジネスメールの侵害」を新しいカテゴリとして追加しました。「標的型攻撃」、「モバイルセキュリティ侵害」、「リムーバブルストレージデバイス / メディア」、「インサイダーによる侵害:過失」、「インサイダーによる侵害:攻撃者」を削除、または新しい質問に移動しました。

### 質問：侵入にはどのような手法が使われていましたか？

攻撃者が使用する手法と侵入のタイプをより明確に分類するため、今年の調査では質問を少し整理しました。その回答から、侵入に複数の手法が使用されていることがわかりました。モバイルセキュリティ侵害と Web 侵害が最も多く、攻撃者によるインサイダーの侵害が最も少ないことがわかりました。

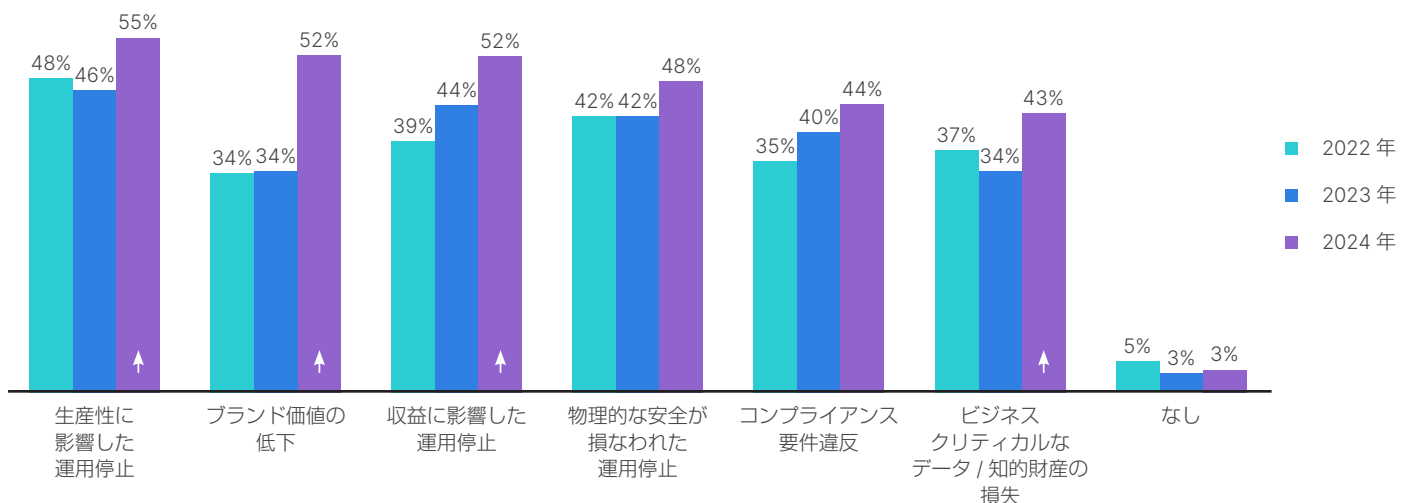


\* 2024 年以前のレポートでは、「どのようなタイプの侵入を経験しましたか？」という設問の回答項目でした。

### 質問：侵入は組織にどのような影響を与えましたか？

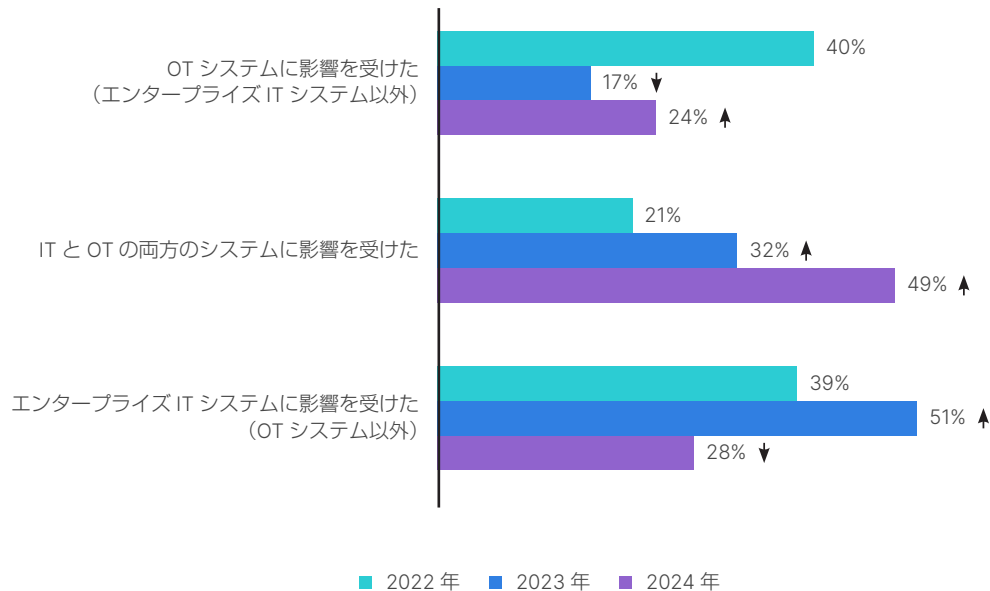
今年の調査で、報告された侵入の数が増加しただけでなく、侵入による組織への影響も悪化していることがわかりました。調査結果によると、最も増加したのはブランド価値の低下で、前年比で約 3 分の 1 から 2 分の 1 以上へと大幅に増加しました。法規制で違反の公表が義務付けられていることが多いため、ブランド価値の低下は避けられないことです。ブランド価値が低下すれば、最終的には顧客維持率や売上成長率が低下する可能性もあります<sup>9</sup>。

生産性に影響した運用停止という影響についても、半数以上（55%）の組織が経験したと回答しました。ビジネスクリティカルなデータや知的財産（IP）の損失を経験したと回答した割合も、2024 年に 34% から 43% に上昇しました。



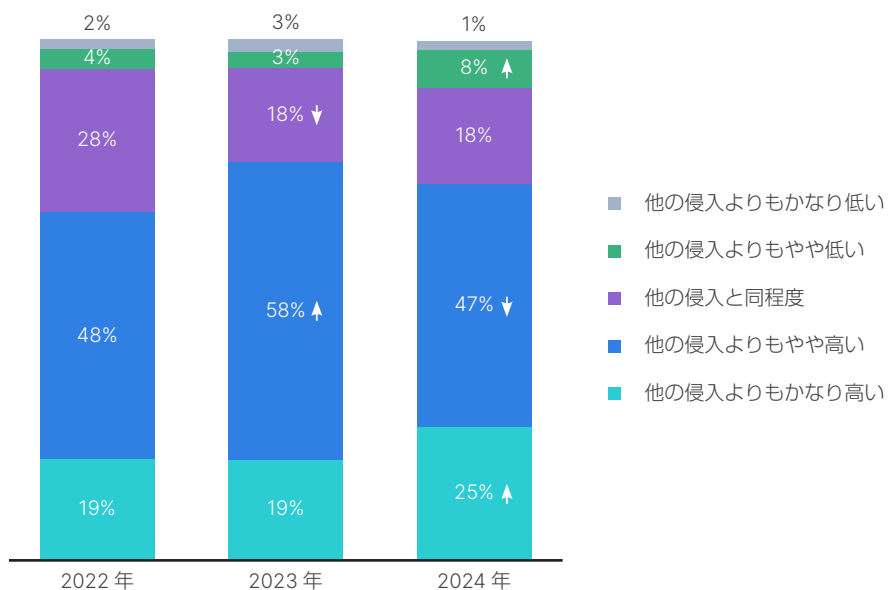
### 質問：過去 1 年間にどのような環境がサイバーセキュリティ侵入の影響を受けましたか？

侵入が OT システムに何らかの影響を与えるという傾向がさらに顕著になっています。2023 年は、調査対象者の 49% が、OT システムのみ、または IT システムと OT システムの両方に影響する侵入を経験したと回答しましたが、今年は、約 4 分の 3（73%）の組織が影響を受けたと回答しました。また、OT システムのみに影響を与えた侵入も前年比で増加しました（17% から 24% に増加）。



### 質問：他の侵入と比較した場合、ランサムウェアが OT 環境に与える影響についての懸念はどの程度ですか？

ランサムウェアが自社の環境に与える影響は他のタイプの侵入より「かなり高い」という回答が、2022 年と 2023 年には 19% でしたが、2024 年には 25% に増加しました。しかしながら、ランサムウェアに対する懸念が高いという回答の割合（「かなり高い」と「やや高い」の合計）は、前年の 77% からわずかに減少して 72% になりました。

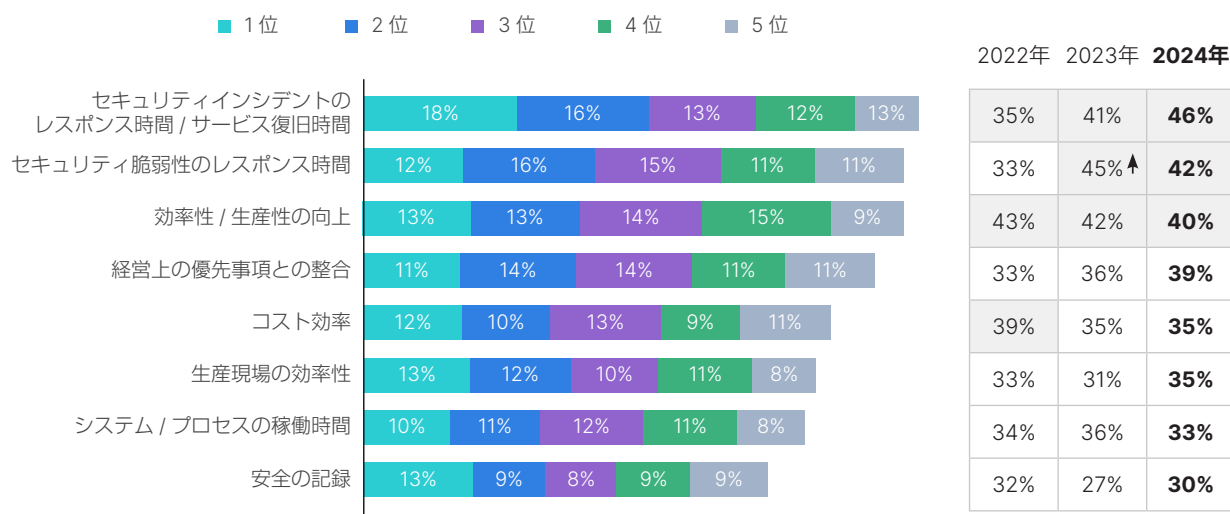


## 世界全体での影響

### 質問：成功を評価する測定基準は何ですか？（5 位まで）

組織はいくつかの方法で成功を測定していますが、「セキュリティインシデントへのレスポンス時間 / サービスの復旧までの時間」という回答が全体として最も多く、調査対象者の半数近く（46%）がこれを成功の要因の 3 位までに挙げました。企業が復旧までの時間に基づいて成功を測定しているのは、注目に値することです。

その理由が、復旧に向けての作業でシステムの復旧を優先して身代金を払いたくないのか、あるいはできるだけ早く身代金を払って攻撃者に業務を再開できるようにしてもらいたいのかのいずれであったとしても、インシデントからの復旧を想定しているというのは、注目に値する情報です。多くの企業は、回避できない攻撃を経験した場合のサイバーレジリエンスとして、最小限の混乱でシステムを復旧させて稼働させることで迅速なレスポンスを可能にすることが成功のより現実的な目標であると考えているようです<sup>10</sup>。

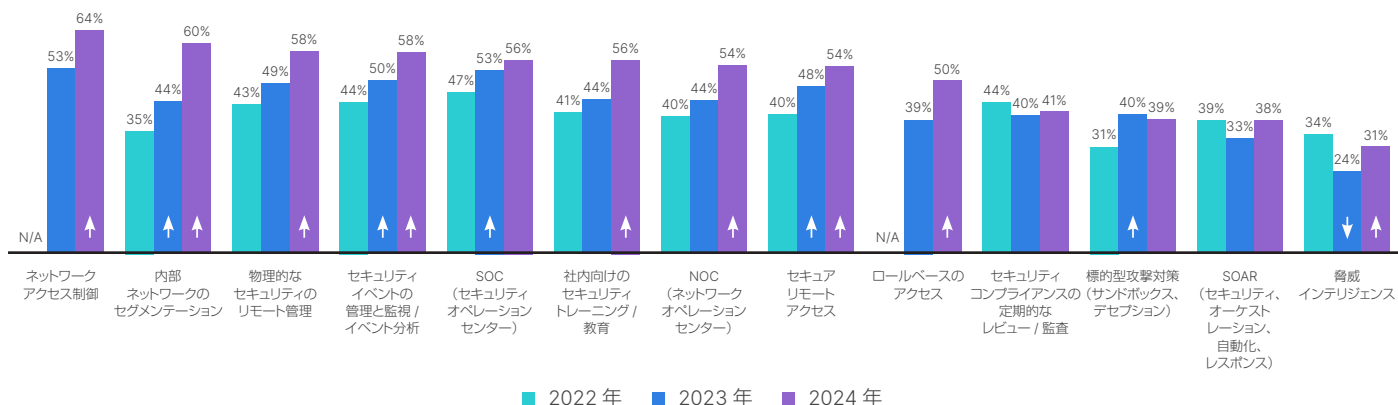


### 質問：現在、どのようなサイバーセキュリティ対策とセキュリティ機能を導入していますか？

侵入に対するセキュリティ対策を強化するため、OT プロフェッショナルは、利用するサイバーセキュリティ対策やテクノロジーを次々と追加することで、サイバーセキュリティのレベルを向上させようとしています。今年の回答では、ほぼすべてのカテゴリが増加しましたが、内部ネットワークのセグメンテーションやロールベースのアクセス制御ソリューション、社内のセキュリティのトレーニングや教育をサポートするプログラムへの投資が大幅に増加しました。

IT と OT のネットワークのコンバージェンスにより、以前はエアギャップで分離されていた機密度の高い OT システムに一般的な脅威がアクセスするのを防止することが求められるようになりました。そのためには、包括的な可視性、ネットワークをセグメンテーションによるネットワーク境界の保護、定義されたルールに基づく OT システムへのユーザーのアクセスの監視と制御が必要になります。これらの機能を組み合わせることで、セキュリティに対するゼロトラストアプローチのサポートが可能になります。

サイバー犯罪の活発化により、上位の役職が OT セキュリティに対する責任を負うようになっていることで、この分野への投資も増えています。投資の増加が良い傾向であるのは事実ですが、OT への侵入の規模、巧妙さ、その後の影響が拡大しているため、増加する攻撃に遅れることなく対応し、OT システムを効果的に保護するには、さらに多くのリソースが必要であることを示しています。





# ベストプラクティス

今年の調査結果に基づくベストプラクティスを以下にまとめて紹介します。

## 1. セグメンテーションを導入する

侵入を減らすには、強力なネットワークポリシー制御をすべてのアクセスポイントに適用することで、OT 環境を強化する必要があります。このような防御を可能にする OT アーキテクチャは、ネットワークゾーンやセグメントの作成から開始します。ISA/IEC 62443 などの標準は、セグメンテーションによって OT ネットワークと IT ネットワークの間に制御を適用するように求めています<sup>1)</sup>。

さらには、ソリューション管理の全体としての複雑さを評価し、一元管理が可能な統合型あるいはプラットフォームベースのアプローチの利点を検討する必要もあります。



ヒント：安全なネットワーキングの戦略を実装します。資産のインベントリとセグメンテーションの基本ステップから開始し、次のステップとして、OT 脅威保護やマイクロセグメンテーションなどのより高度な制御を検討します。

## 2. OT 資産を可視化し、制御でそれを補完する

組織は、OT ネットワークに存在するすべてを認識し、理解する必要があります。可視性が確立されたら、次のステップとして、脆弱性が存在する可能性のあるデバイスを保護する必要がありますが、これには、機密度の高い OT デバイス向けに設計された保護対策が必要です。プロトコル対応のネットワークポリシー、システム間のやり取りの分析、エンドポイント監視などの機能により、脆弱な資産の侵害を検知し、防止できるようになります。



ヒント：アプリケーションレイヤーのポリシー、OT 脆弱性保護、仮想パッチを組み合わせることで、脆弱なレガシーシステムが外部に公開されるリスクが大幅に軽減されます。

## 3. OT をセキュリティオペレーション (SecOps) とインシデントレスポンス計画に統合する

組織における IT と OT の SecOps は成熟の途上にあります。SecOps やインシデントレスポンス計画においては、OT に固有の考慮すべき点があり、それは主として、OT と IT の環境にはそれぞれに固有のデバイスタイプが存在し、OT 侵害がクリティカルなオペレーションに与える影響が広範であるためです。

この方向への重要なステップは、OT 環境を自社のプレイブックに組み込むことです。このような高度な備えにより、IT チーム、OT チーム、製造チームのコラボレーションが推進され、サイバーリスクと生産リスクを正しく評価できるようになります。また、CISO がそれらのリスクを正しく認識して優先度を判断し、予算や人員を配分できるようになります。



ヒント：効果的な機械学習の機能を備えたセキュリティツールは、データのアグリゲーションと分析を強化し、潜在的な脅威の迅速な検知とレスポンスを可能にします。

## 4. プラットフォームアプローチをセキュリティアーキテクチャ全体に採用することを検討する

急速に進化する OT の脅威と拡大する攻撃対象領域に対処するため、多くの組織が、異なるベンダーの多様なセキュリティソリューションを導入しています。結果として、セキュリティアーキテクチャがあまりに複雑になって可視性が阻害されるだけでなく、セキュリティチームの限られたリソースが大きな負担を強いられることとなります。

プラットフォームベースのセキュリティのアプローチは、ベンダーの統合とアーキテクチャの簡素化に役立ちます。IT ネットワークと OT 環境の両方に特化した機能を備えた堅牢なセキュリティプラットフォームは、ソリューションの統合を可能にすることでセキュリティの効果を向上させ、一元管理を可能にすることで管理の効率化を実現します。統合により、脅威に対する自動レスポンスの基盤も提供されます。



ヒント：コンテキスト対応の生成 AI の機能を備えたセキュリティプラットフォームは、デバイスの脆弱性のトラブルシューティングや脅威ハンティング分析などの自動化ツールにより、セキュリティ態勢のさらなる強化と運用の効率化に役立ちます。

## 5. OT に特化した脅威インテリジェンスとセキュリティサービスを採用する

OT セキュリティは、差し迫ったリスクのタイムリーな認識と正確な分析に基づくインテリジェンスなくして成立しません。プラットフォームベースのセキュリティアーキテクチャは、脅威インテリジェンスを適用することで、最新の脅威、攻撃タイプ、リスクからのほぼリアルタイムの保護を可能にするものでなければなりません。脅威インテリジェンスとコンテンツのソースのフィードやサービスに強固で OT に特化した情報が含まれていることを確認する必要があります。



ヒント：脅威インテリジェンスとセキュリティサービスに、OT アプリケーションとデバイスを標的にする不正トラフィックを検知してブロックすることを前提に設計された専用の侵入防御システムのシグネチャが含まれている必要があります。

## 調査方法

調査対象者のほとんどが「プラントオペレーション」または「製造オペレーション」の役職に就き、4 分の 1 以上（28%）がプラントオペレーション担当のバイスプレジデントまたはディレクターでした。調査対象者のほとんどが、役職に相違はあるものの、サイバーセキュリティ購入の意思決定に深く関与しています。調査対象者の半数以上（58%）が OT の購入決定について最終的な決定権を持っている一方で、今年の調査では、グループとしてこれらの決定を下す組織が増加していることが明らかになりました（2023 年の 28% から 38% に増加）。

### 調査の目的

フォーティネットは、調査に関する専門知識を有する第三者調査会社である InMoment の協力を得て、OT プロフェッショナルのペルソナを開発しました。同社の協力により作成した調査項目により、以下の詳細な理解が可能になりました。

- 組織における調査対象者の職務
- セキュリティ機能の活用方法
- 情報の追跡と報告の方法
- 影響と成功要因

### アプローチ

パネルサンプルを使用して、従業員が 1,000 人以上の企業（一部の例外を除く）から、以下の業種で働く 558 人を対象に調査を実施しました。

- エネルギー / ユーティリティ
- 医療 / 製薬
- 運輸 / 物流
- 製造
- 化学 / 石油化学
- 石油 / ガス / 精製
- 上下水道

調査対象者の選定にあたり、以下の条件も考慮しました。

- オペレーショナルテクノロジーに責任を負う部門に勤務している
- 製造またはプラントのオペレーションのレポートに責任を負っている
- サイバーセキュリティ購入の意思決定に関与している

2022 年から、調査の範囲を世界全体に拡大しました。

- 調査対象者は、オーストラリア、ニュージーランド、アルゼンチン、ブラジル、カナダ、中国本土、フランス、ドイツ、香港、インド、日本、メキシコ、ノルウェー、南アフリカ、韓国、スペイン、台湾、タイ、英国、米国を始めとする世界中の異なる場所から抽出されました。

## まとめ

OT は、重要インフラ、医療システム、製造を始めとする世界中の企業や政府機関にとって極めて重要であり、OT システムや ICS システムが不可欠であるという特性がリスクを高くする要因であることに疑いの余地はありません。NIST によると、OT のセキュリティ目標では多くの場合に完全性と可用性が優先され、次に機密度が優先されますが、安全性も包括的な優先事項として考慮する必要があります<sup>12</sup>。

「2024 年 OT サイバーセキュリティに関する現状レポート」によると、多くの組織で OT セキュリティの成熟度が上昇傾向にあるという明るい兆しがあります。しかしながら、それと同時に、前年に上昇したいくつかの分野が今回の調査では後退し、組織が経験した侵入が増加し、リスクスコアの決定にあたって OT が重視される度合いが低くなっています。このような傾向を逆転させるには、機密度の高い OT システムの保護を新たな方法で周知し、リソースを割り当てて、効果的で目的に特化したセキュリティアーキテクチャを構築する必要があります。

<sup>1</sup> 「[Guide to Operational Technology \(OT\) Security](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf)」、Keith Stouffer 他共著、NIST、2023 年 9 月（英語）：  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>

<sup>2</sup> 同上

<sup>3</sup> 「[Global agencies warn of increased cyberattacks against OT devices](https://www.iiotnews.com/news/2024/may/02/global-agencies-warn-of-increased-cyberattacks-against-ot-devices/)」、Ryan Daws、IIoTnews、2024 年 5 月 2 日（英語）：  
<https://www.iiotnews.com/news/2024/may/02/global-agencies-warn-of-increased-cyberattacks-against-ot-devices/>

<sup>4</sup> 「[フォーティネットグローバル脅威レポート 2023 年上半期版](https://www.fortinet.com/jp/demand/gated/TR-23H1)」、フォーティネット、2023 年 8 月：  
<https://www.fortinet.com/jp/demand/gated/TR-23H1>

<sup>5</sup> 同上

<sup>6</sup> 同上

<sup>7</sup> 「[Cybersecurity Disclosure](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214)」、Erik Gerding、US Securities and Exchange Commission、2023 年 12 月 14 日（英語）：  
<https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214>

<sup>8</sup> 「[2023 年上半期 FortiGuard Labs グローバル脅威レポートの主な調査結果](https://www.fortinet.com/jp/blog/threat-research/fortiguards-labs-threat-report-key-findings-1h-2023)」、Douglas Jose Pereira dos Santos、フォーティネット、2023 年 8 月 7 日：  
<https://www.fortinet.com/jp/blog/threat-research/fortiguards-labs-threat-report-key-findings-1h-2023>

<sup>9</sup> 「[The real impact of cybersecurity breaches on customer trust](https://www.csoonline.com/article/644219/the-real-impact-of-cybersecurity-breaches-on-customer-trust.html)」、Shashi Samar、CSO、2023 年 7 月 3 日（英語）：  
<https://www.csoonline.com/article/644219/the-real-impact-of-cybersecurity-breaches-on-customer-trust.html>

<sup>10</sup> 「[Cybersecurity plans should center on resilience](https://mitsloan.mit.edu/ideas-made-to-matter/cybersecurity-plans-should-center-resilience)」、Beth Stackpole、MIT Sloan、2024 年 3 月 27 日（英語）：  
<https://mitsloan.mit.edu/ideas-made-to-matter/cybersecurity-plans-should-center-resilience>

<sup>11</sup> 「[How to Define Zones and Conduits](https://gca.isa.org/blog/how-to-define-zones-and-conduits)」、Maximillian Kon、ISA、2024 年 5 月 7 日（英語）：  
<https://gca.isa.org/blog/how-to-define-zones-and-conduits>

<sup>12</sup> 「[Guide to Operational Technology \(OT\) Security](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf)」、Keith Stouffer 他共著、NIST、2023 年 9 月（英語）：  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>



フォーティネットジャパン合同会社

〒106-0032

東京都港区六本木 7-7-7 Tri-Seven Roppongi 9 階

[www.fortinet.com/jp/contact](http://www.fortinet.com/jp/contact)

お問い合わせ