REPORT

2021 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート

目次

インフォグラフィック：主な調査結果 3

概要 4

はじめに 5

調査方法 5

OT セキュリティのインサイト 6

大手企業のベストプラクティス 10

まとめ 14

インフォグラフィック：主な調査結果

フォーティネットの「2021 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」によると、オペレーショナルテクノロジー（OT）リーダーは、引き続きサイバーセキュリティに取り組んでいますが、依然として苦心していることがわかりました。そしてこの 1 年、パンデミックにより、リーダーが直面するセキュリティ問題をさらに大きくしました。

10 社中 9 社が、過去 1 年間に少なくとも 1 回の侵入を経験しており、63% が 3 回以上の侵入を受けており、このことは 2020 年の結果と同様です。

最も多かった侵入事例は、**マルウェアが 57%、フィッシングが 58%** で、去年の **43%** から増加しています。

42% が、内部のセキュリティ侵害を経験しており、去年から **18%** 増加しています。

大手企業と中堅企業を比較：

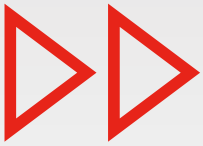
大手企業は、**オーケストレーションや自動化**を利用している傾向が高く、**セキュリティ追跡やレポート作成**を実施している。

大手企業は、自身のセキュリティオペレーションセンターで **100% 一元的に可視化**を実施している傾向が高い。

大手企業は、パンデミックに伴う**在宅勤務への対応**準備が早期に実施されていた。

概要

フォーティネットの「2021 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」によると、オペレーショナルテクノロジー（OT）リーダーは、引き続きサイバーセキュリティの課題に直面しており、パンデミックによる在宅勤務への移行により、一部のリーダーの状況は悪化しています。また、パンデミックにより、多くの組織では IT-OT ネットワークコンバージェンス（統合）も加速化しています。これは、パンデミック関連の課題により、デジタルトランスフォーメーションが加速化したためで、現時点で想定していた状況より数年進展したと指摘している他の CEO レポートとも相関しています [1,2]。



最近の「KPMG CEO」調査によると、回答者の 80% がパンデミックによりデジタルトランスフォーメーションが加速したと回答し、30% が現時点で予測していた状況より数年分進展したと回答しており、ある人物は、「わずか 3 ～ 4 ヵ月で 3 ～ 4 年分進展した」と述べています [3]。

多くの組織は、テクノロジー関連の予算を増やし、リモートワークへの移行に対応する必要がありました。パンデミックがもたらした多くの課題の結果として、現在、OT リーダーの多くは、プロセスを効率化し、コストを削減する新しい方法を模索しています。

2020 年のレポートで指摘しているとおり、OT-IT ネットワークコンバージェンスの機運は、パンデミック前から高まっていましたが、パンデミックの影響で、デジタルトランスフォーメーションが加速化し、接続性に対する必要性が高まりました。従業員は在宅勤務が必要になり、OEM やシステムインテグレーターは、移動して装置を点検できず身動きがとれませんでした。パンデミックにより、現場へのアクセスが非常に困難になった結果、サードパーティ製のセキュアなリモートアクセスに対するニーズが明らかに高まりました。また、これらの課題に対応するために、コストとリスクの両方が増加しました。

2021 年は、製造マネージャーの回答者が減り、VP やディレクターの回答者が増加するという変化がありました。OT の責任は、ネットワークエンジニアリングの VP やディレクターから、CISO や CIO に移行しています。また、2021 年は前年度と比較して、セキュリティオペレーションセンター（SOC）の設置が増加し、ネットワークオペレーションセンター（NOC）の設置も大幅に増加しました。

また、例年通り、過去 1 年間に侵入が 0 回だった回答者の取り組みと、10 回以上侵入を受けた回答者の取り組みを比較しました。「大手企業」の OT リーダーは、以下を含む多くのベストプラクティスを遵守する傾向が非常に高いことが再確認されました。

- オーケストレーションと自動化の活用、および予測行動の利用
- サイバーセキュリティのビジネスへの財務的な影響に関する追跡と報告
- 業界の規定に対するコンプライアンス、および定期的なセキュリティ評価に関するレポート

大手企業の OT 組織は、サイバーセキュリティのベストプラクティスを遵守することで、パンデミック時に発生したテクノロジーの変化、脅威、脆弱性に対して適切に対応することができました。

はじめに

オペレーショナルテクノロジー（OT）市場は、2027 年まで年平均成長率（CAGR）で 6.40% の成長が続くと予想されていますが、OT は、世界中の工場、エネルギー生産 / 送電施設、交通ネットワーク、公益事業の活動を支えており、これは意外なことではありません [4]。

オペレーションの効率と収益性を高めるため、多くの OT 企業は、SCADA（スキャダ）などの OT インフラストラクチャと IT ネットワークとの統合を進めています。競合他社の圧力の結果、以下のようなさまざまな方法で、コスト削減や効率化を行うことの緊急性が高まっています。

- デジタルツインを利用してリスクを軽減し、アセットパフォーマンス管理（APM）をサポート
- 設備総合効率（OEE）を高めて、製造利益の向上を推進
- メンテナンスを予定ベースから状況ベースに移行することで、サービス停止に伴う生産ロスを最小限に抑制
- アセットの可用性と信頼性の向上
- サービスおよびメンテナンス活動に関する紙の記録やサービスレポートのデジタル化

これらを含むデジタルトランスフォーメーションの取り組みにより、イノベーションが進展しており、これまで以上に、新しいプラットフォームや新しい働き方が求められています。ワークスタイルの変化に拍車がかかっており、従業員の在宅勤務のニーズが急激に高まっています。リモートワークへの移行は、デジタルトランスフォーメーションの顕著な例の 1 つですが、ビジネスのデジタル革新に伴い影響を受ける一連のシステムやプロセスは、OT 全体に及びます。

OT-IT ネットワークコンバージェンスよってあらゆるものの俊敏性と効率が高まりますが、リスクの増加も伴います。OT ネットワークと IT システム間の「エアギャップ（物理的な隔離）」の存在が減少するため、OT インフラストラクチャは、IT システムが従来から直面していたあらゆる脅威の影響を受けることになります。さらに、OT システムに対する攻撃対象領域は、IIoT（産業用 IoT）デバイスも対象となる可能性があります。IIoT デバイスは基幹システムを制御しており、仮にセキュリティ侵害を受けた場合、潜在的に、健全性や安全性に非常に大きな影響を及ぼす可能性があります。

大多数の OT リーダーによると、自社のセキュリティ対策の成熟度をレベル 2 以上だと回答しており、これは可視化、セグメント化、およびプロファイル化を構築していることを意味します。また、レベル 2 では、完全な役割ベースのアクセスを備え、多要素認証を強制してゼロトラストの実現への取り組みを進めている状況です。実際、調査した回答者の 99% がレベル 0 以上であり、これは OT の可視化とセグメント化を全く実施していない回答者はわずか 1% であることを意味します。

取り組みは前進していますが、まだ改善する余地もあります。大半の OT 組織は、オーケストレーションと自動化を活用しておらず、新型コロナウイルスの危機によって、セキュリティ対応の負担が大きくなりました。OT リーダーは、OT-IT ネットワークコンバージェンスに加え、増大する高度な脅威ランドスケープ、パンデミック関係の問題が重なったことで、対処することがより困難になっています。セキュリティのベストプラクティスを実施することは、時間とお金がかかりますが、実施した各組織は、パンデミックがもたらす変化に適切に対応することができました。

調査方法

今年の「オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」は、2021 年 2 月 24 日～ 2021 年 3 月 1 日にかけて実施したアンケートに基づいています。質問内容は、2019 年と 2020 年に同様の調査で要求があった内容を反映しました。回答者は、製造業、エネルギー / 公益事業、ヘルスケア、運輸の 4 つの業界に関わる企業に勤務しています。全員が、製造や工場のオペレーションの何らかの責任者であり、職位は、マネージャーからバイスプレジデントまでとなっています。この調査では、アンケートのデータを活用して、オペレーションの専門家が日々の業務でサイバーセキュリティに対してどのように対処しているかを紹介します。今回の分析では、今年のデータを確認し、それを昨年のデータと比較することで、業界の状況について包括的なインサイトがいくつか得られました。次に、データをさらに掘り下げて、過去 12 ヵ月間に 10 件以上の侵入を受けた組織と比較して、同期間の間に侵入が 0 件だった「大手企業」が、最も一般的に採用するベストプラクティスを明らかにしました。

OT セキュリティのインサイト

上記のように、OT リーダーは、OT-IT コンバージェンスに関する課題に引き続き取り組んでいます。また、新型コロナウイルスが原因で突如、予算を大きく増やす必要があったことも、2020 年の結果に大きく影響しています。各リーダーは引き続き、セキュリティ測定と分析、および多数の侵入（特に内部脅威からの）に関する課題に直面しています。

インサイト1：OTリーダーでは引き続き、組織に影響を及ぼす多数の侵入が確認されました。生産性や収益性に影響を与える停止や、物理的な安全性に対するリスクが上昇しています。

今回のアンケートに参加した OT リーダーが代表を務めるグループや組織では、サイバー犯罪者によるシステムの侵入を防止する点で、ほとんど成功していませんでした。10 社中 9 社の組織で、過去 1 年間に 1 回以上の侵入を受けており、これは去年の調査結果とほぼ同じです。パンデミックは異常な状況でしたが、侵入の 90% は、OT リーダーが関与する大きな問題となっています。

内部侵害の事例は大きな変化があり、42% に増加しました。不正なリンクをクリックする従業員など、意図しないセキュリティ事件とは異なり、不正行為者は悪意を持っているため、OT リーダーはシステムへのアクセス権を持つ人物を慎重に検討する必要があります。また、非常に多くの従業員が在宅勤務しているため、ホームネットワーク関連のセキュリティ問題が、問題の原因となっている可能性があります。たとえば、仮想プライベートネットワーク（VPN）のフィルタが適切に設定されていない場合、企業ネットワークでは通過できないフィッシング E メールが通過する可能性があります。また、企業は、境界ベースのネットワークアプローチから脱却して、ゼロトラストモデルに移行する必要性が高まっています。

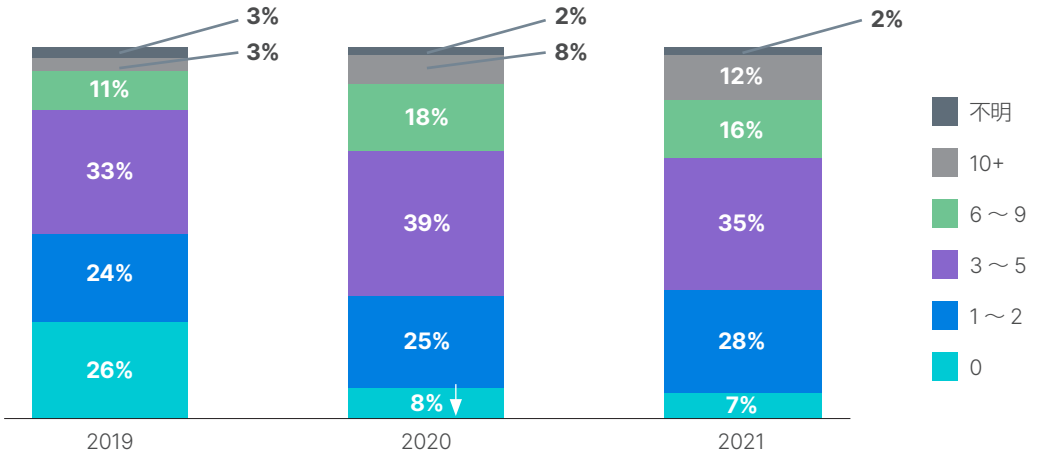


図 1：昨年の侵入数

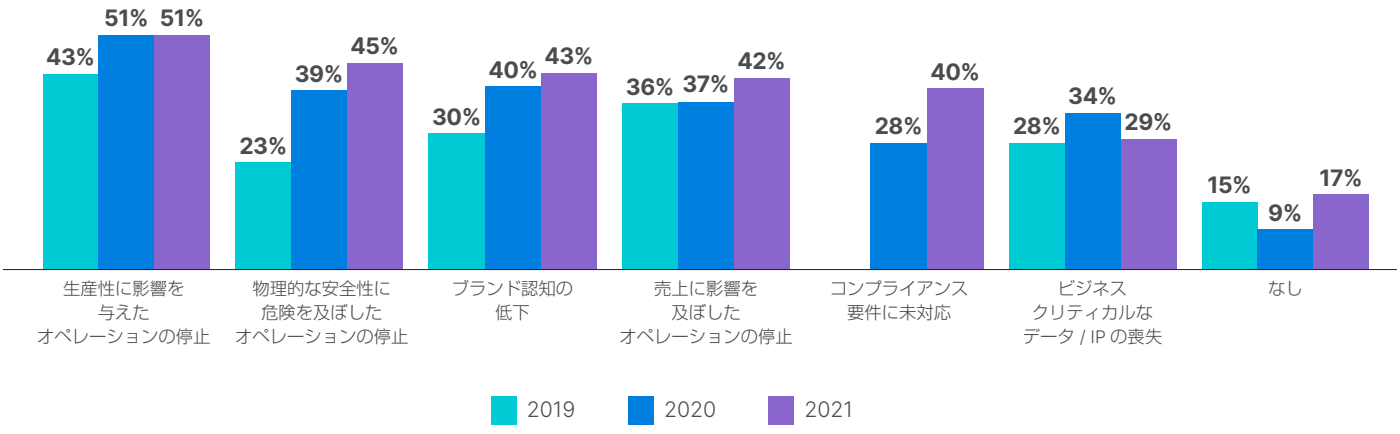


図 2：組織に対する影響

インサイト2：OTリーダーは、パンデミックに関連する課題への対応ができておらず、迅速に予算を増やしプロセスを変更する必要がありました。

少数の大手企業を除き、OT リーダーは、IT-OT ネットワークコンバージェンスに関連するプロセス管理、および在宅勤務対応の必要性のため、迅速に支出を増やす必要がありました。これらの別件の 2 つの問題はどちらもテクノロジー予算に影響を及ぼしました。パンデミックにより、デジタルトランスフォーメーションが加速し、安全なリモートアクセスの接続に対するニーズが増加したことが理由で、SOC や NOC では、スタッフや装置を増やす必要がありました。従業員は、在宅勤務が必要になり、OEM やシステムインテグレーターは移動できず身動きがとれませんでした。以前は、OEM の技術者は飛行機に乗って現場に行き、装置を点検することができましたが、パンデミック中に企業の出張規定や政府が課す移動制限が厳格化され、現場に移動できませんでした。パンデミックにより、技術スタッフは現場で直接対応できなかったため、サードパーティ製のセキュアなリモートアクセスのニーズが加速しました。

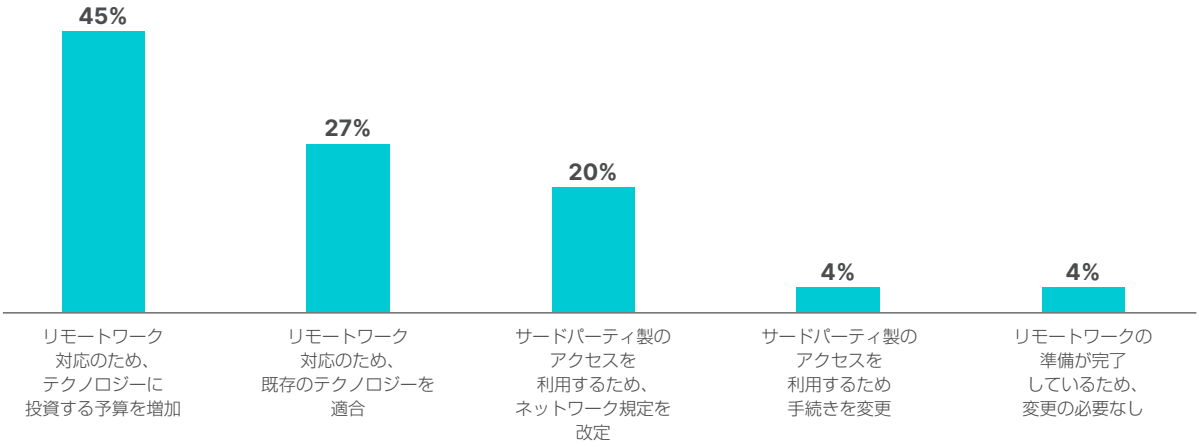


図 3：在宅勤務を推進する上で最も大きな課題

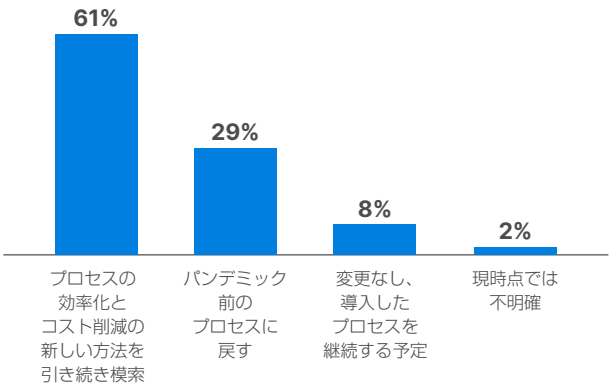


図 4：パンデミック後の作業プロセスの調整

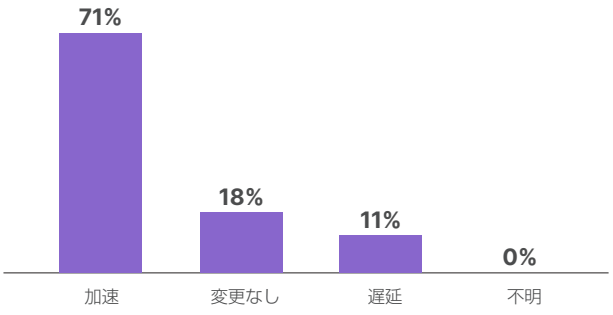
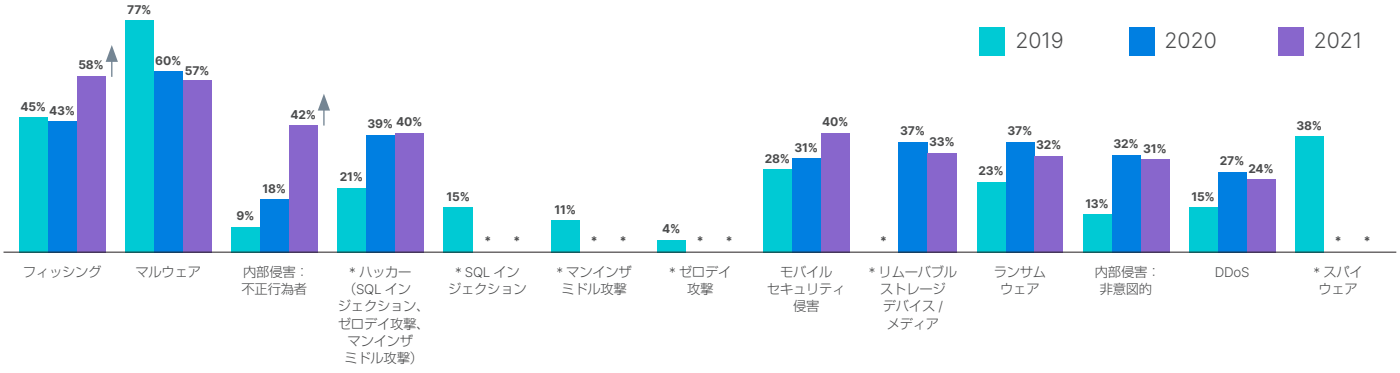


図 5：IT-OT コンバージェンスに対するパンデミックの影響

インサイト3：OTリーダーは、内部脅威とフィッシングの大幅な増加に直面しています。マルウェアの問題は継続しています。

今回の調査によると、フィッシング攻撃が大幅に増加しており、58% がこの種の侵入を報告しており、昨年の 43% から増加しています。フィッシングの増加は、2020 年初頭に見られた働き方の急速な変化に伴う脆弱性を、攻撃者が悪用することに起因しています。誰も耐性を持っておらず、OT 組織も他者と同様に影響を受けました。

同様に、従業員の在宅勤務を拡大する決定は、あらゆるタイプの組織に影響を及ぼしており、OT も例外ではありません。不正行為者は、セキュリティの脆弱性を悪用できるため、OT を標的にしました。また、不正行為者は幅広い脆弱な攻撃対象領域を把握しているため、不正行為の成功率が上昇しています。不確実で急激な変化の時期には、攻撃者は新たなリスク領域を悪用するため、エクスプロイトが増加するのが一般的であり、この数字は驚きではありません。従業員のリモート作業が今後も続くと、OT 組織はゼロトラストを従業員のエンドポイントまで拡張し、攻撃対象領域を削減する必要があることは明らかです。



↑ ↓ は、95% の信頼区間で前年との有意差を示す

＊ 2020 年の回答を調整：SQL インジェクション、マンインザミドル攻撃、ゼロデイ攻撃を削除。ハッカー（例：SQL インジェクション、ゼロデイ攻撃、マンインザミドル攻撃など）を追加。スパイウェアを削除リムーバブルストレージデバイス / メディアを追加。

図 6：侵入を受けた経験

インサイト4：OTリーダーは引き続き、セキュリティ測定や把握に苦心している。

OT リーダーは、サイバー攻撃の測定値を継続的に追跡し、報告していますが、コストの優先順位はリスク評価やビジネスへの影響より低くなっています。追跡および報告されるサイバーセキュリティの測定値の上位は常に、脆弱性（70%）と侵入（62%）ですが、今年は、具体的なリスク管理結果（57%）が多く見られました。OT のサイバーセキュリティ問題は、シニアリーダー / エグゼクティブリーダーに均等に報告されていますが、ペネトレーションテスト / 侵入テストの結果は、他の問題ほど多く共有されていませんでした。

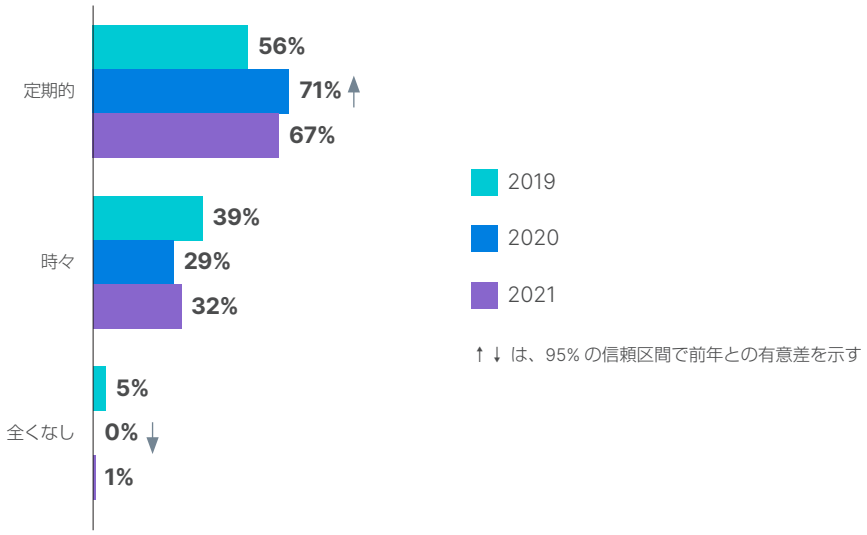
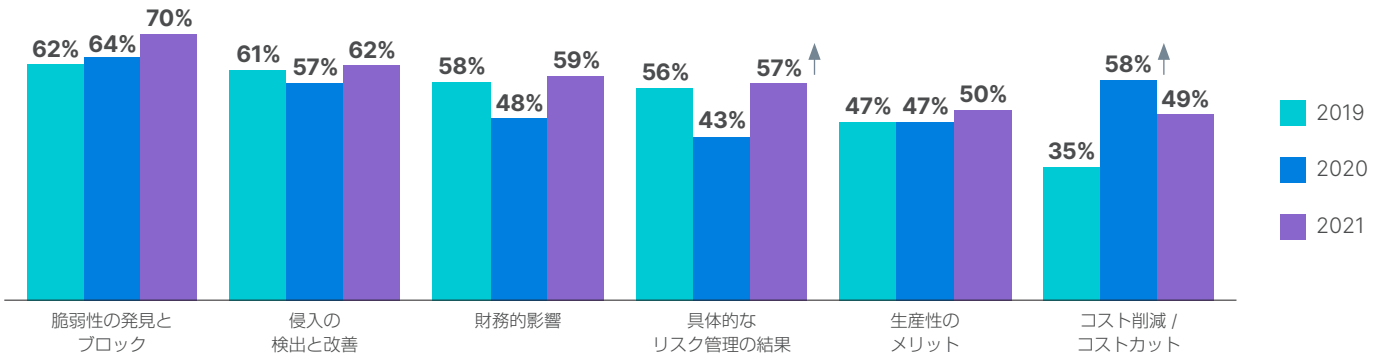
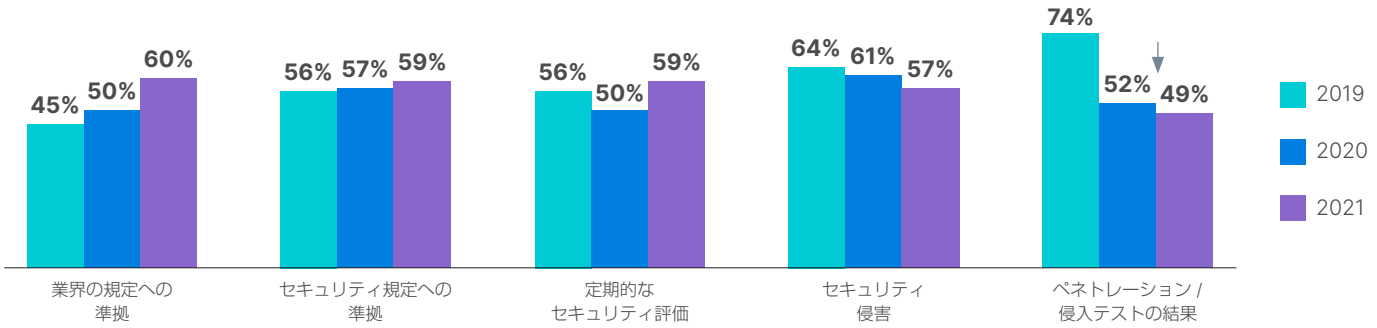


図 7：IT サイバーセキュリティ戦略への関与



↑ ↓ は、95% の信頼区間で前年との有意差を示す

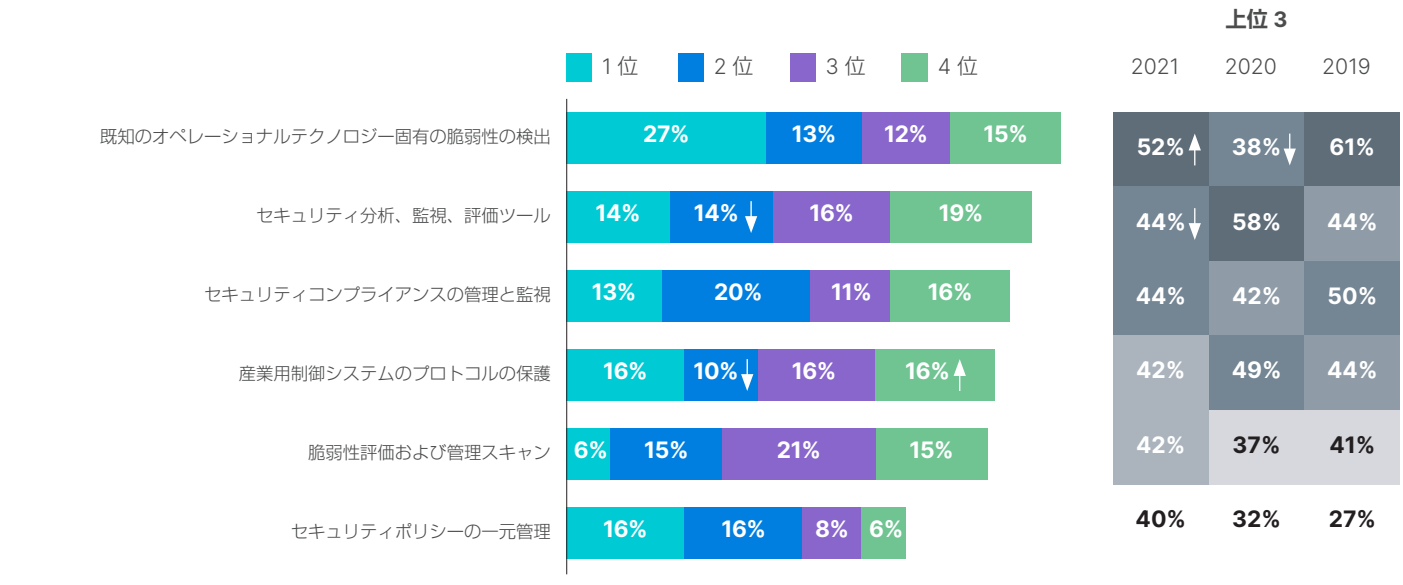
図 8：サイバーセキュリティの測定値の追跡と報告



↑ ↓ は、95% の信頼区間で前年との有意差を示す

図 9：報告された OT サイバーセキュリティ問題

セキュリティソリューションで最も重要な機能を質問したところ、攻撃検出ツールという回答が最も多く、2020 年に下がった重要度が回復し、2021 年は再び最も重要なセキュリティソリューションとなりました。回答の結果、セキュリティ分析、監視、評価ツールは、2020 年と比較して、2021 は大きく重要性が低下しました。



↑ ↓ は、95% の信頼区間で前年との有意差を示す

図 10：セキュリティソリューションの最も重要な機能（ランキング）

過去数年、回答者は、サイバーセキュリティソリューションは、オペレーションの柔軟性を損なうと述べていましたが、2021 年は「ビジネス上の懸念を生む」という回答が増加しました。企業にとって侵害がニュースになることは好ましくなく、サイバーセキュリティ教育の充実化によって認識が高まり、OT リーダーは、セキュリティソリューションを必要な戦略の一部として捉えるようになったと考えられます。

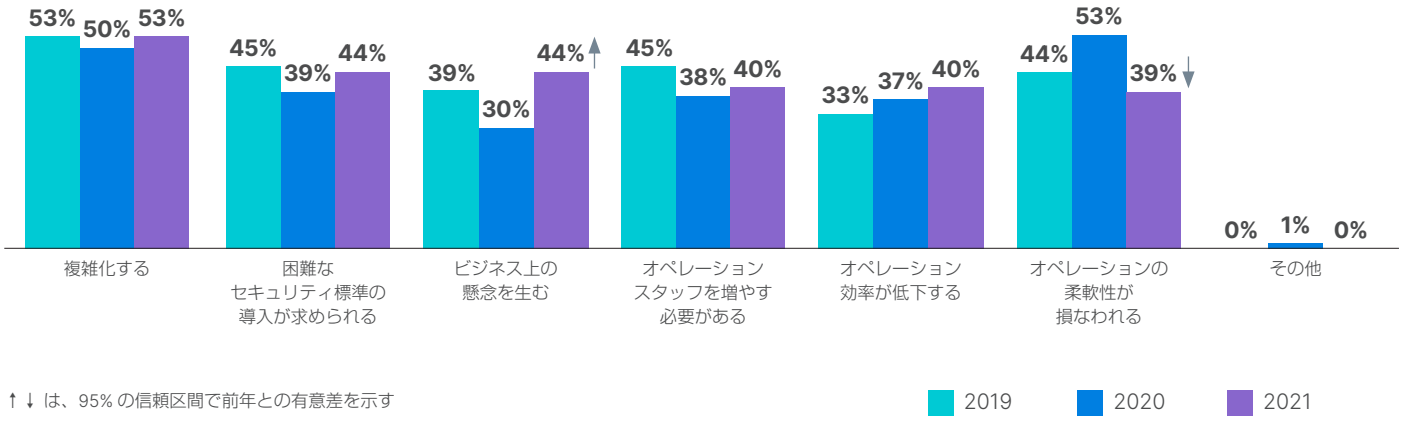


図 11：OT の専門家の活動に及ぼすサイバーセキュリティソリューションの否定的な影響（上位 3）

大手企業のベストプラクティス

今年の調査では、侵入がなかったと報告した OT リーダーはわずか 7% である一方で、回答者の 12% が 10 回以上の侵入がありました。当社は、「大手企業」と「中堅企業」のこれらの 2 つのサブセットの回答者の調査回答を比較しました。この分析により、大手企業の OT リーダーが採用している傾向が高いいくつかのベストプラクティスが明らかになりました。

1. 大手企業は、財務的影響の追跡と報告を実施している傾向がありました。

古い格言にあるように、測定したものが改善されます。セキュリティの脆弱性に対する財務的影響は、大手企業の 74% が追跡および報告していました。また、脆弱性の発見とブロック（74%）、および具体的なリスク管理の結果（60%）も追跡しています。

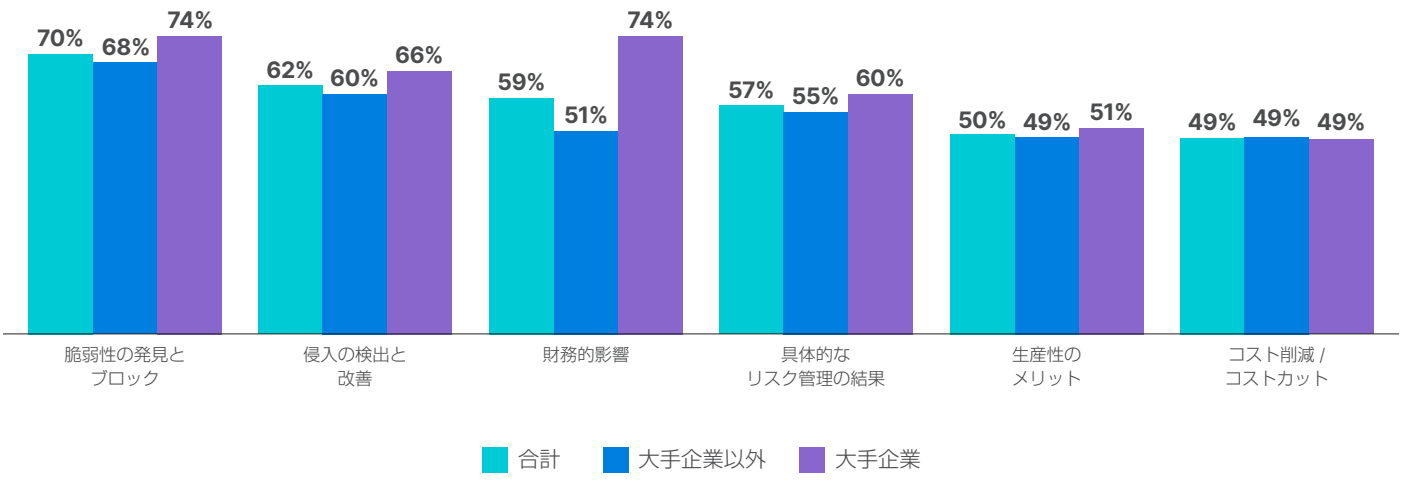


図 12：サイバーセキュリティの測定値の追跡と報告

2. 大手企業は、業界の規定への準拠を報告し、定期的なセキュリティ評価を実施している傾向があります。

組織のトップリーダーにとって、コンプライアンスはますます大きな課題となっていますが、レポートを手動で作成する必要がある場合、多くの OT 組織では、監査人が要求する頻度より多い報告は実施しない可能性があります。一方で、大手企業は、定期的なレポートを作成しており、企業全体のコンプライアンスレポートを自動的に作成していることがうかがえます。レポート作成のリアルタイムなアプローチが増えるほど、セキュリティ態勢を改善できます。

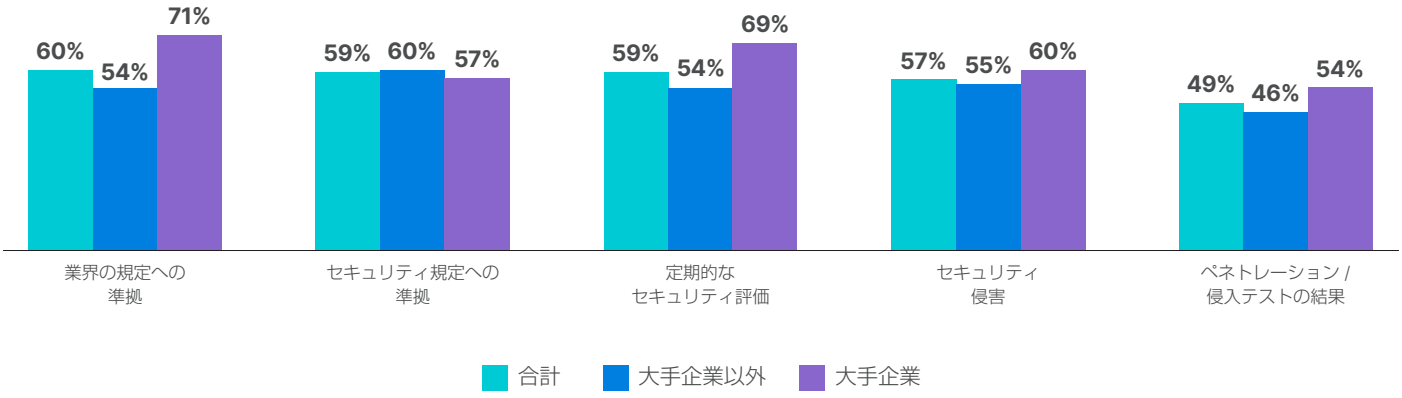


図 13：報告された OT サイバーセキュリティ問題

3. 大手企業は、OT活動を100%可視化している傾向があります。

企業全体で効果的なセキュリティ保護を実現するには、一元化した可視化が不可欠であり、OT システムも例外ではありません。大手企業は、完全に可視化している傾向があります。

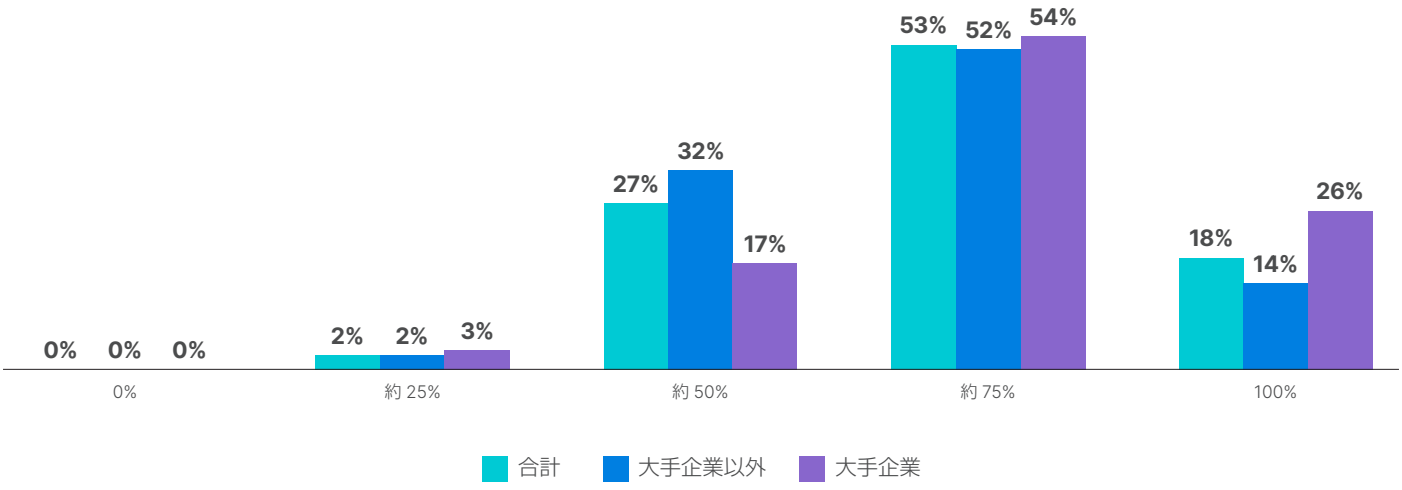


図 14：一元的に可視化している OT 活動の割合

4. 大手企業では、在宅勤務の推進で問題が少なく、一部は全く何もする必要がない組織もありました。

大手企業で、在宅勤務を促進するために必要だった最も大きな変更は、予算、テクノロジー、ネットワークポリシーで均等でした。また、11% は、リモートワークの準備が完了していたため、変更の必要がなかったと回答しています。

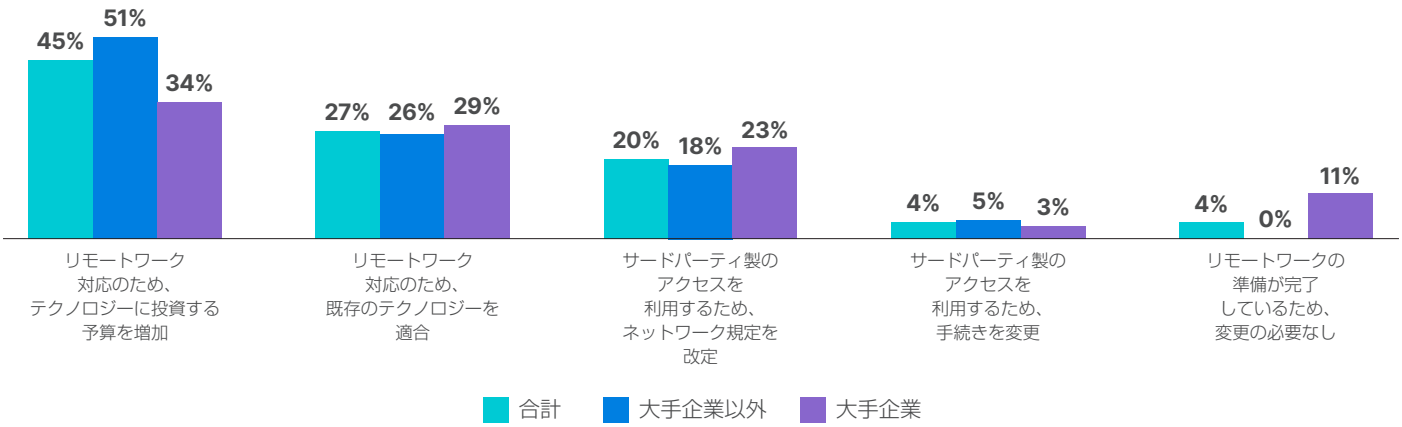


図 15：在宅勤務を推進する上で最も大きな課題

5. 大手企業では、パンデミック後、プロセスを効率化し、コストを削減する傾向があります。

今回のパンデミックにより、大半の OT 組織では IT-OT ネットワークコンバージェンスが加速しましたが、大手企業では、パンデミック後も引き続きプロセスの効率化とコスト削減の方法を模索すると回答する傾向がありました（74%）。

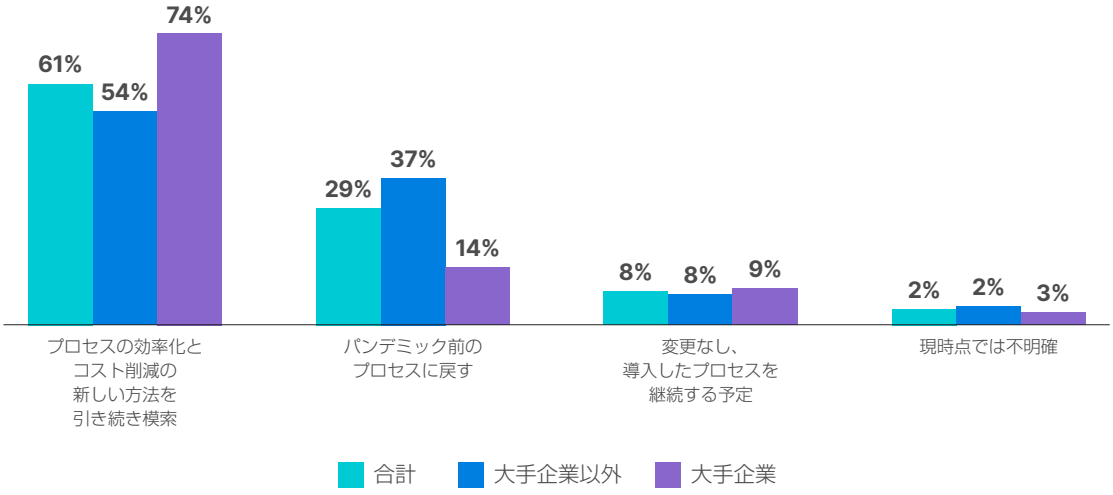


図 16：パンデミック後の作業プロセスの調整

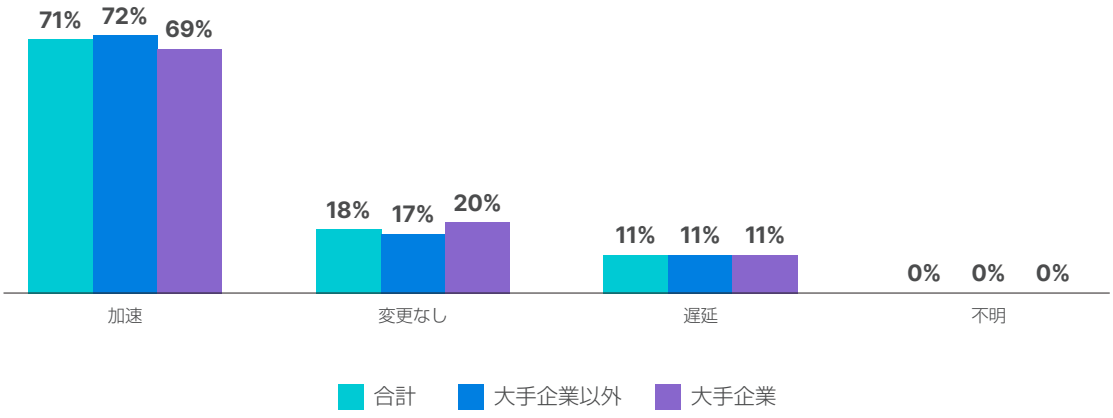


図 17：IT-OT コンバージェンスに対するパンデミックの影響

6. 大手企業は、OTの責任の所在はCIOである傾向があります。

一般的に、OT の責任の所在は、ネットワークエンジニアリングの VP やディレクターから、CISO や CIO に移行している傾向があります。組織のタイプにかかわらず、OT サイバーセキュリティの最終責任者は、OT ディレクターである傾向がありますが、大手企業では、CIO が責任者である傾向が高く（23%）、OT の責任を CISO の配下に置くことを予定している傾向は低くなります。

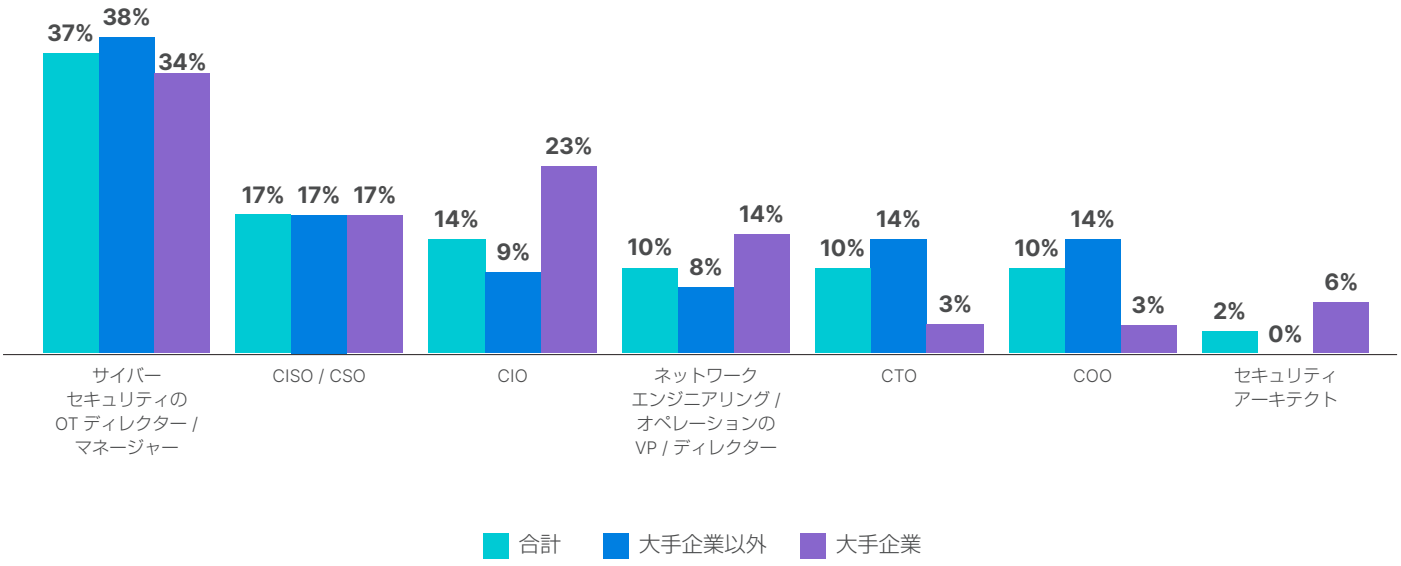


図 18：OT のサイバーセキュリティの責任の所在

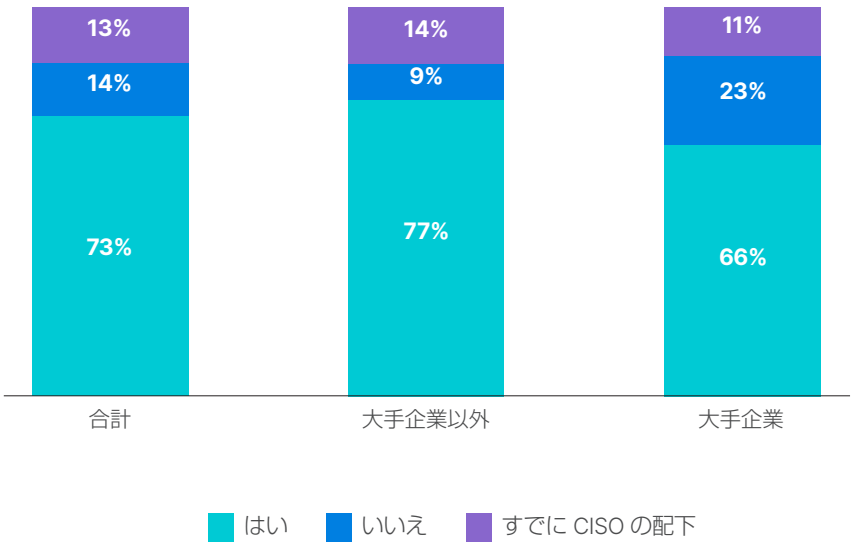


図 19：今後 12 ヵ月でサイバーセキュリティが CISO の配下となる予定

まとめ

OT 環境の保護を担う企業では、昨年に引き続きリスクは高くなっています。世界的なパンデミックが重なったことを考えると、この結果はそれほど悪くはありません。何よりこの 1 年は、各組織にとって、適切なセキュリティ投資を継続することの重要性が示されました。OT ネットワークは、IT ネットワークやインターネット接続とのエアギャップがほとんどないため、OT システムは高い脆弱性を持っています。OT システムは、IT やネットワークを介した攻撃リスクの増加に直面しています。内部脅威の増加により、OT の組織は引き続き、リモートユーザーに対するゼロトラストアクセスの確立に取り組みながら、組織全体のセキュリティ認識やトレーニングに注力する必要があります。

参考文献一覧

[1]「KPMG 2020 CEO Outlook: COVID-19 Special Edition」、KPMG International、2020 年 9 月（英語）：
https://home.kpmg/content/dam/kpmg/xx/pdf/2020/09/kpmg-2020-ceo-outlook.pdf

[2]「The State of Industrial Cybersecurity in The Era of Digitalization」、Thomas Menze 氏著、ARC Advisory Group、2020 年 9 月（英語）：
https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf

[3]「KPMG 2020 CEO Outlook: COVID-19 Special Edition」、KPMG International、2020 年 9 月（英語）：
https://home.kpmg/content/dam/kpmg/xx/pdf/2020/09/kpmg-2020-ceo-outlook.pdf

[4]「Global Operational Technology Market—Industry Trends and Forecast to 2027」、Data Bridge Market Research、2020 年 7 月（英語）：
https://www.databridgemarketresearch.com/reports/global-operational-technology-market

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Report-2021-OT-Cybersecurity-202107-R1