CTC
Challenging Tomorrow's Changes

CTCエスピー株式会社

ひらめき、むすんで、その先へ
Thanks 30th ▶ Go 40th

【サマリーレポート】2022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

CTCエスピー株式会社

2023年3月

本サマリーは、フォーティネット社による「2022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」をベースにしています。

はじめに

かつて外部ネットワークから切り離されていた産業用制御システムは、IoTやBIといった技術の発展に促され、インターネットに接続されるケースが急速に増えています。その傾向は、産業用制御システムのセキュリティリスクを増大させており、セキュリティインシデント発生による経済的損失や信用喪失を未然に防ぐためにも、OTセキュリティの拡充は製造業における重要な経営課題となっています。

それでは、OTセキュリティの現状はどうなっているのでしょうか。このレポートでは、500人以上のOTプロフェッショナルを対象としてアンケート調査を実施しました。

●回答者のプロフィール

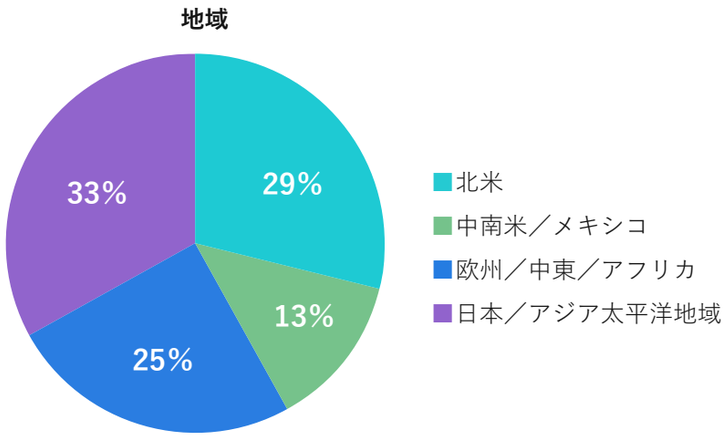


図1：調査対象の国と地域

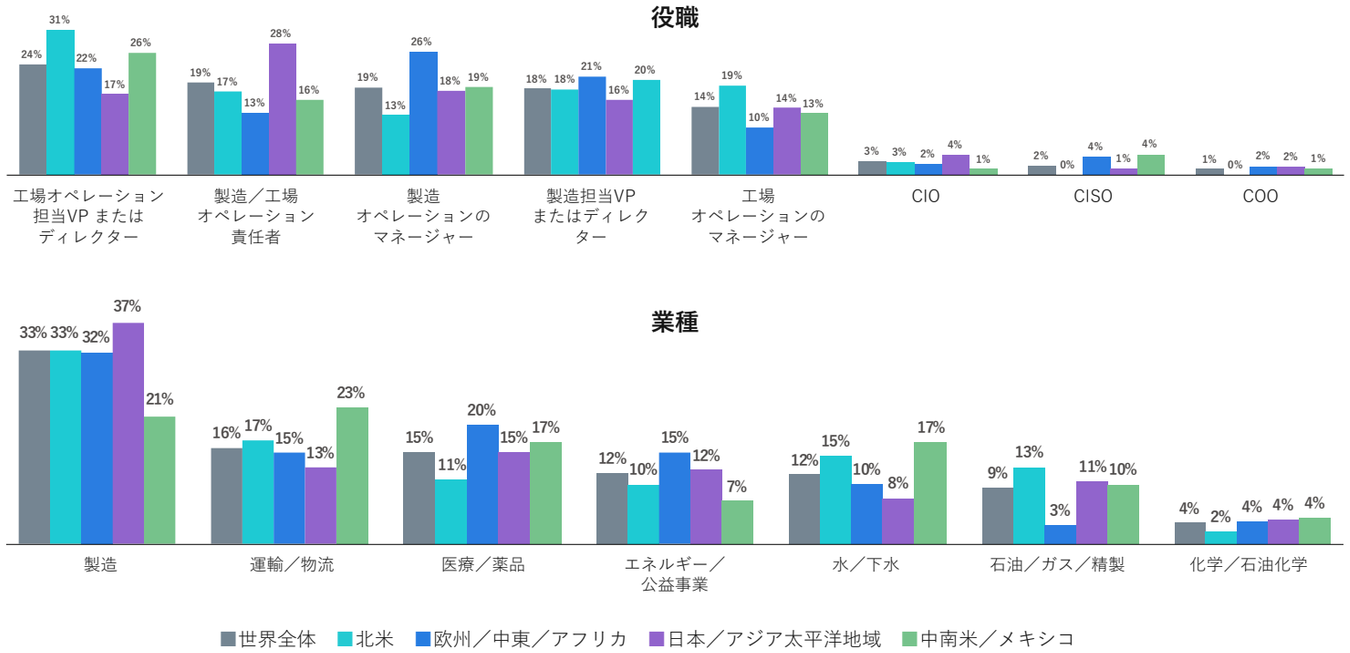
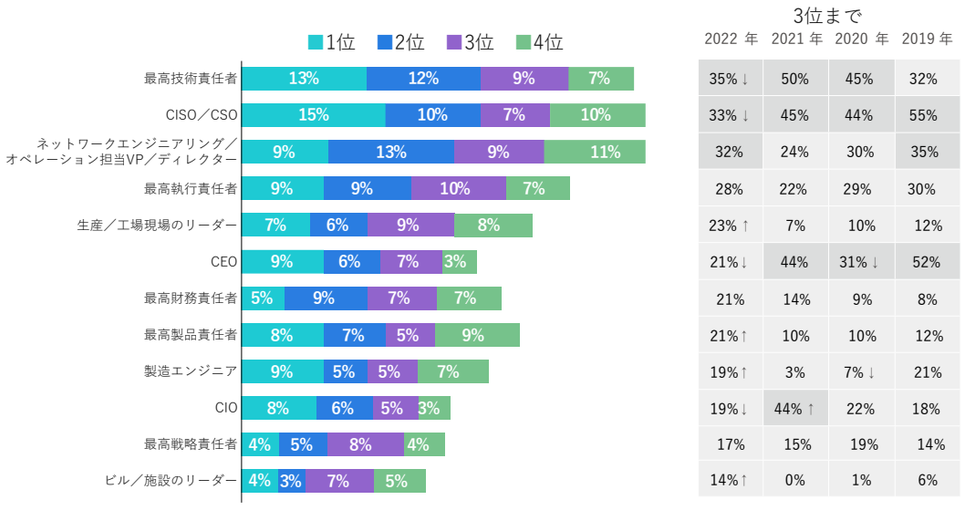


図2：地域別の役職と業種

全体の傾向

OTセキュリティの管理は セキュリティ専任ではない現場担当者に任されている

サイバーセキュリティの決定への影響力がある組織内のリーダー



	3位まで			
	2022 年	2021 年	2020 年	2019 年
最高技術責任者	35% ↓	50%	45%	32%
CISO／CSO	33% ↓	45%	44%	55%
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	32%	24%	30%	35%
最高執行責任者	28%	22%	29%	30%
生産／工場現場のリーダー	23% ↑	7%	10%	12%
CEO	21% ↓	44%	31% ↓	52%
最高財務責任者	21%	14%	9%	8%
最高製品責任者	21% ↑	10%	10%	12%
製造エンジニア	19% ↑	3%	7% ↓	21%
CIO	19% ↓	44% ↑	22%	18%
最高戦略責任者	17%	15%	19%	14%
ビル／施設のリーダー	14% ↑	0%	1%	6%

図3：セキュリティの決定に対する影響力がある組織内のリーダー

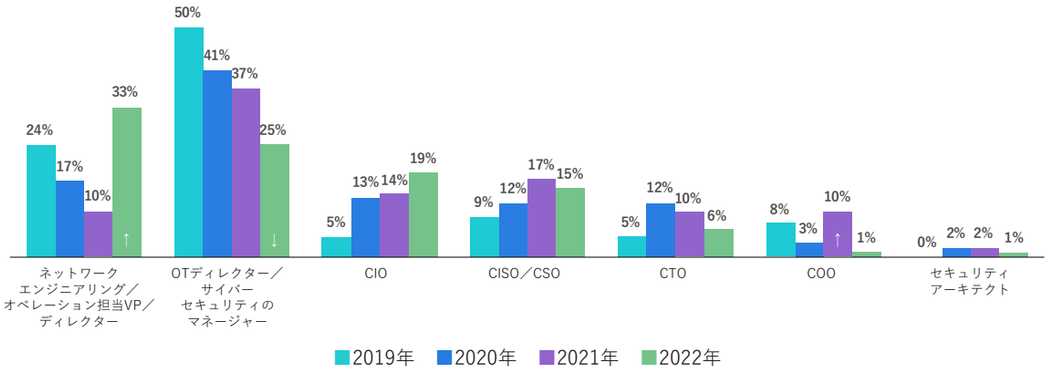


図4：現在のOTサイバーセキュリティの責任者

OTセキュリティの重要性は強く意識されつつあるものの、今回の調査は、脅威に対する備えが今も断片的で不完全であることを明らかにしています。

左図が示すように、OTセキュリティの決定に対するCISOの影響力が大きな組織（3位以内）はわずか33%に過ぎず、2021年の45%から大きく減少しています。

OTセキュリティの最終責任者は誰かという質問では「ネットワークエンジニアリング／オペレーション担当のバイスプレジデント／ディレクター」という回答が最多で3分の1を占めており、必ずしもセキュリティ専任ではない現場担当者に任されてしまっていると言えます（図4）。

全体の傾向

OTセキュリティ体制の成熟度は全体として緩やかに改善している

フォーティネットでは、5段階のOTセキュリティ成熟度を設定し、回答者に自社の成熟度を自己申告していただきました。

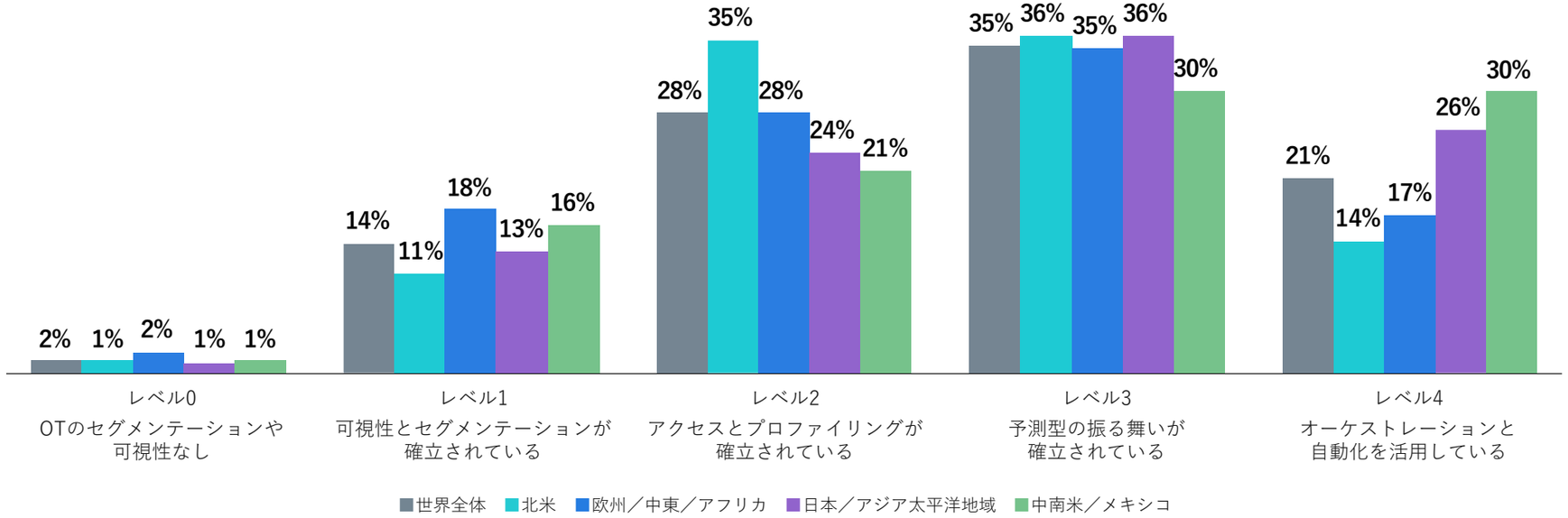


図5：OTサイバーセキュリティ態勢の成熟度

84%の回答者がレベル2以上と回答し、アクセスとプロファイリングが確立されていることがわかりました。また、56%がレベル3以上（予測型の振る舞い検知機能を取り入れている）、21%がレベル4（オーケストレーションと自動化が確立されている）と回答しました。レベル3以上と回答した組織は2021年の41%から増加しており、緩やかな改善傾向にあると言えます。

しかし、次頁以降に見られるように、具体的な取り組みに注目していくと成熟度の問題には微妙なニュアンスの違いがあることがわかります。

取り組みの現状

OT活動の可視化と追跡

すべてのOT活動の一元的な可視化を実現しているのはわずか13%

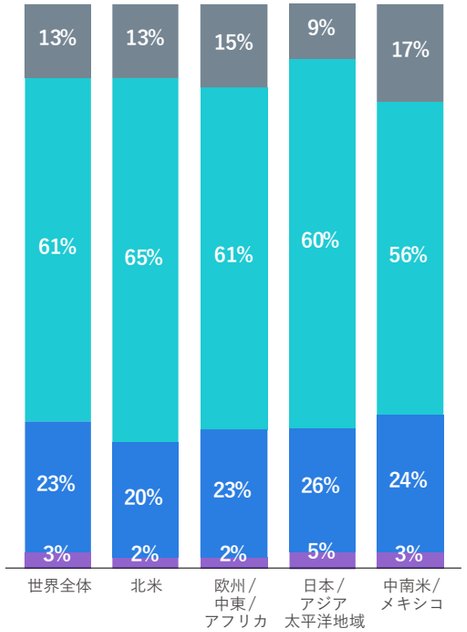
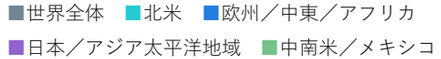


図6：セキュリティオペレーションによるOT活動の可視化

OTセキュリティ成熟度のレベル1には、OTプロセス可視化の確立が含まれていますが、そのきめ細かさは一様ではありません。

前頁で98%の回答者が成熟度をレベル1以上と回答した一方で、図6を見ると、OT活動の4分の3以上をセキュリティオペレーションチームが可視化しているという回答は74%にとどまっています。北米エリアの場合、100％可視化の割合にいたってはわずか13%で、2020年の23%から大きく減少しています。

SOCからすべてのOT活動を追跡できるという回答も52%



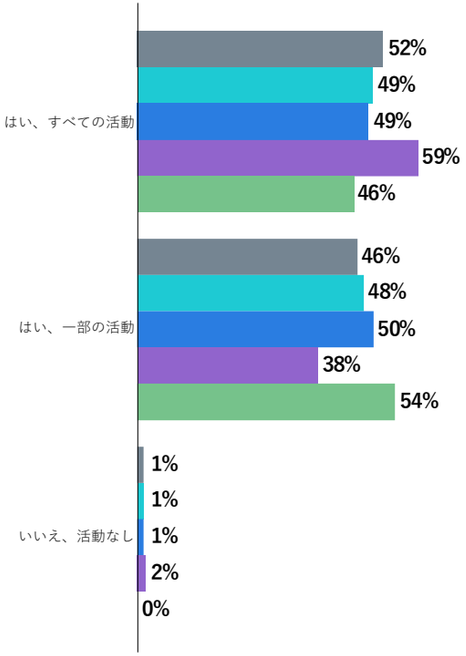


図7：すべてのOT活動をSOCが監視し、追跡している

IT脅威からOT システムを保護する必要が生まれたのは最近であり、その手法がまだ標準化されていないことがわかりました。

SOCをOTセキュリティ管理に利用するのも1つの方法で、ほぼすべての回答者が一部のOT活動に採用しています。しかし、SOCチームがすべてのOT活動を監視・追跡できていると回答した組織は52%にとどまり、この調査を開始した4年前からほぼ横ばいです。

セキュリティ指標の追跡とレポート

基本的なセキュリティ指標を追跡しているという回答は約半数

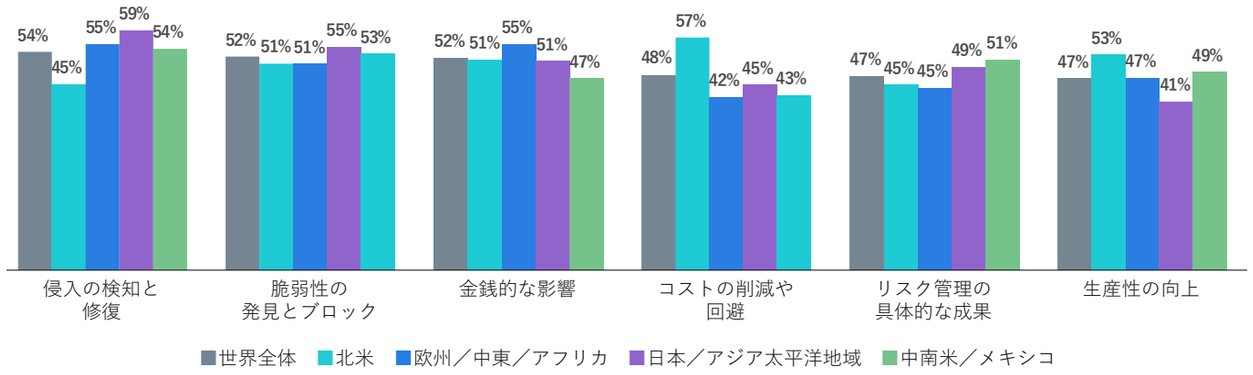


図8：サイバーセキュリティ測定値の追跡とレポート

セキュリティ指標の追跡とレポートについての結果には、ばらつきがありました。すべての組織が確実に追跡する必要のある基本的なサイバーセキュリティ指標を挙げて質問したところ、そのいずれかを追跡しているとの回答は52%にとどまりました（図8）。

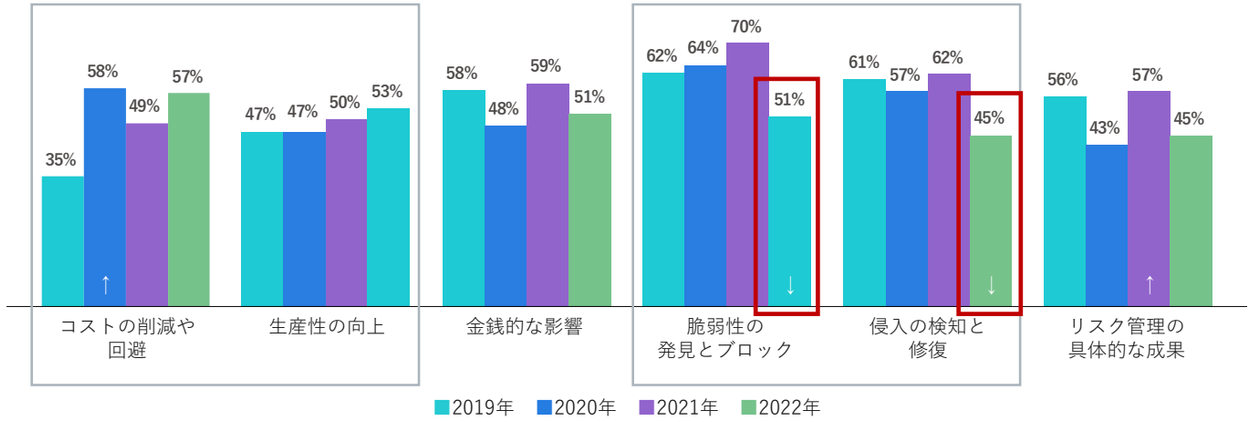


図9：サイバーセキュリティ測定値の追跡とレポート（北米）

北米の結果を過去と比較すると、脆弱性の発見とブロック、侵入の検知とその修復などのいくつかの指標を追跡し、レポートしている割合が2021年から大幅に減少しました（図9）。

OTセキュリティへのアプローチ

特定のOTセキュリティツールやOTセキュリティを担保する方法を使用していない組織は47%以上

今回の調査では、OTセキュリティのツールや機能について、できるだけ多くのソリューションを挙げましたが、47%以上の組織が、特定のOTセキュリティツールやOTセキュリティを担保する方法を使用していません（図10）。

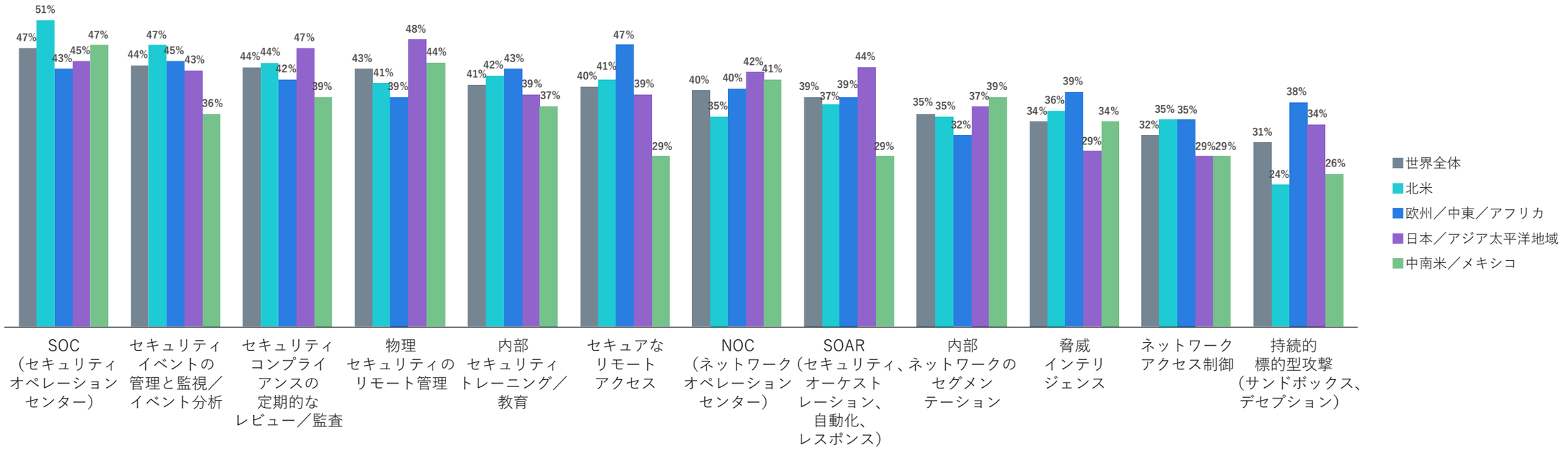


図10：使用しているサイバーセキュリティとセキュリティの機能

このような「機能のいくつかを利用する」アプローチは、さまざまな組織がさまざまなアプローチを試しており、OTセキュリティへの取り組みがまだ初期段階にあることを示しています。

不正侵入の経験

組織のセキュリティ成果は、この1年でほとんど改善されていません

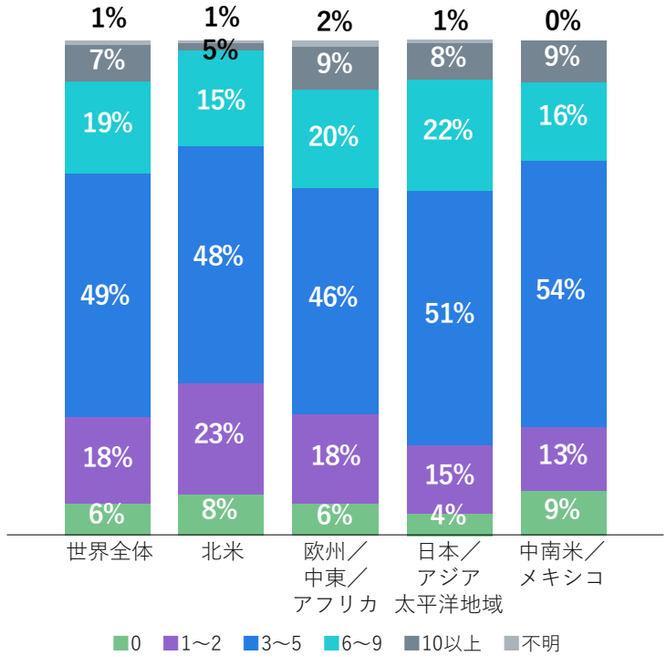


図11：過去1年間の侵入件数

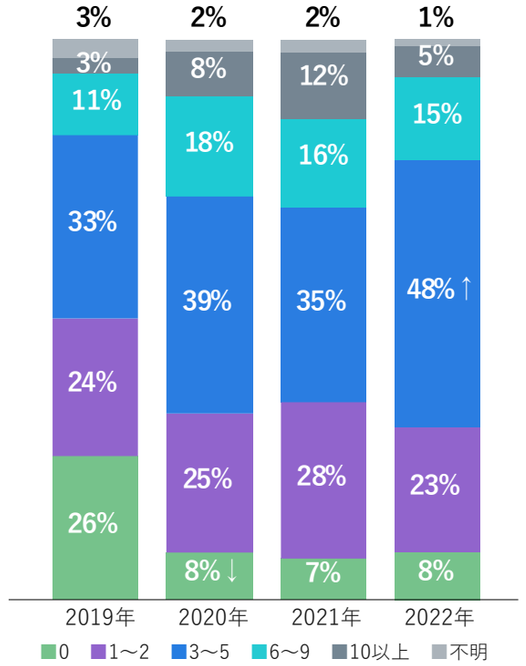


図12：過去1年間の侵入件数（北米）

93%の組織がこの1年に不正な侵入を1回は経験しています。75%が3回以上、19%が6回以上、7%が10回以上の不正侵入を経験したと回答しました。侵入がなかったという回答はわずか6%でした（図11）。

4年間の北米の結果に注目すると、2020年以降に3回以上の侵入を経験した組織の割合に大きな変動はなく、全体として状況は好転していません（図12）。

不正侵入による影響

OTシステム攻撃の影響は大きく、何らかの対応が必要

不正侵入のビジネスへの影響は決して小さなものではなく、半数近くの回答者が生産性に影響する運用停止を経験し、3分の1以上が収益、データ損失、コンプライアンス、ブランド価値への影響、さらには物理的な安全への脅威を経験しました（図13）。また、90%が、サービスの復旧に数時間以上かかったと回答しました（図14）。

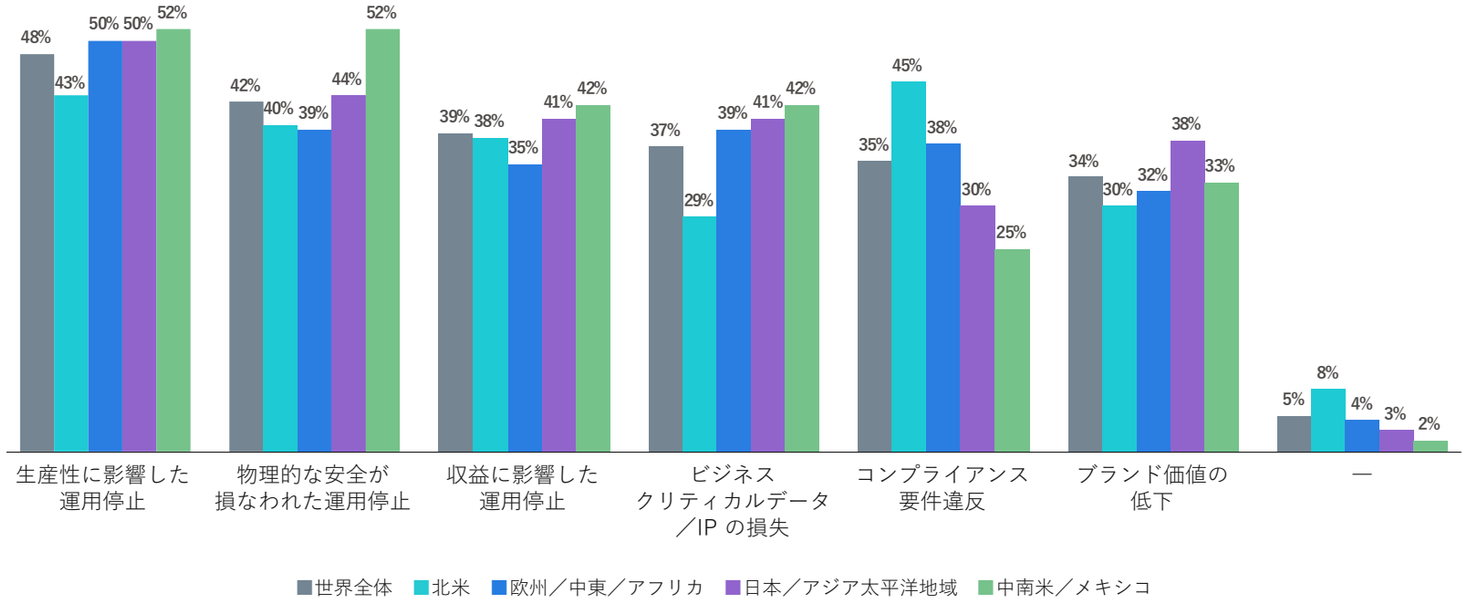


図13：侵入の組織への影響

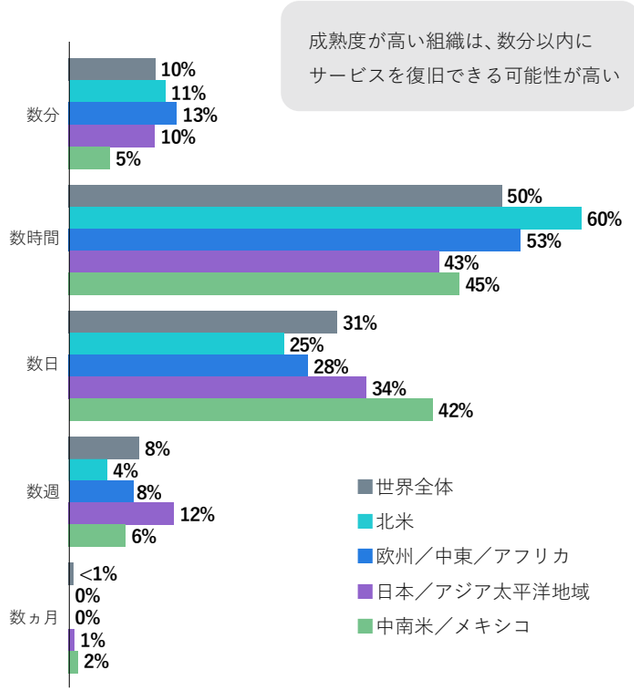


図14：侵入後の最長だったサービス復旧時間

OTセキュリティのベストプラクティスを含む、
本レポートの完全版を無料でお読みいただけます。
下記のURLよりダウンロードしてください。

https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-2022-ot-cybersecurity.pdf

CTCエスピーでは、Fortinet製品を活用し、
貴社の課題にフィットしたOTサイバーセキュリティソリューションを提供しています。
お気軽にご相談ください。

https://www.ctcsp.co.jp/information/lp/fortigate/