FORTINET

REPORT

制御システムの現状とサイバーセキュリティレポート2020

目次

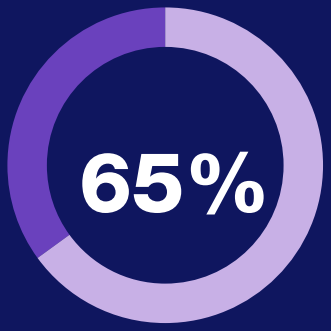
主な調査結果

フォーティネットの「制御システムの現状とサイバーセキュリティレポート 2020」では、制御システム（OT）のリーダーは組織内で高い評価を受けており、そのチームは企業の収益に欠かせないものであることがわかります。サイバーセキュリティは日常業務の不可欠な部分であり続けており、その業務は苦戦を強いられています。

10 組織中 9 組織

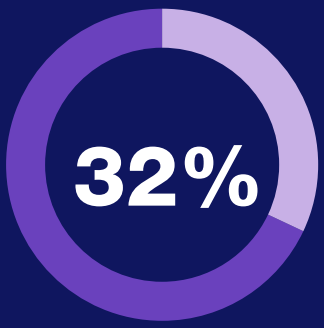
過去 1 年間に**少なくとも 1 つの OT システムへの侵入被害を経験**した組織
（2019 年から **19%** 増加）

65% が **3 回以上の侵入被害を経験**
2019 年から **18%**

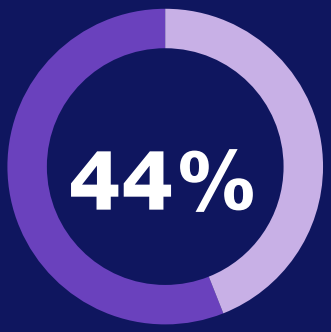


の OT リーダーがオペレーション
プロセスにセキュリティ機能を
組み込む責任があると回答

しかし、**78%** が OT セキュリティ責務を
CISO の配下に置いている
（もしくは来年その予定）と回答



がセキュリティ脆弱性の対応時間を
トップ 3 の測定値としており、
2019 年から **12%** 減



業界規制への準拠を
追跡および報告できていない

44% は、セキュリティ標準への準拠を
追跡して報告できていないと回答

最上位組織は以下のとおり：

4倍

SOC で集中的に
可視化されている
可能性

133%

発見・ブロックされた
脆弱性の追跡・報告の
可能性

2倍

現在 CISO / CSO が
OT セキュリティを
担当

フォーティネットから「制御システムの現状とサイバーセキュリティレポート 2020」完全版を入手いただけます。

概要

フォーティネットの「制御システムの現状とサイバーセキュリティレポート 2020」では、制御システム（OT）のリーダーは組織内で高い評価を受けており、そのチームは企業の収益に欠かせないものであることがわかります。サイバーセキュリティは日常業務の不可欠な部分であり続けており、その業務は苦戦を強いられています。

実際、2020 年 4 月にフォーティネットが実施した OT リーダーに関する調査では、全体として、結果に関して組織が誤った方向に動いていることが示されています。過去 12 か月間に侵入被害がなかった回答者は 8% に過ぎず、1 年前の同様の調査と比較して 18% も減少しました。また、3 回以上の侵入被害が発生した組織の割合は、同期の 47% から 65% に増加しました。これらの侵入被害は、しばしば、運用効率、収益、さらには物理的安全性に影響を与えました。

この減少には、多くの要因が関係している可能性があります。OT システムはエアギャップを失いつつあり、IT システムやインターネットとの相互接続がますます進んでいます。エンタープライズ向けネットワークはより複雑になりつつあり、全体的なこの攻撃への対策をより困難にしています。そして脅威主体はますます洗練された戦術を用いています。しかし、この調査では、基本的なセキュリティ衛生の一部の要素を OT 環境に拡張していない組織がかなりの割合を占めていることも示されています。

データを深く調べると、この傾向が強調されます。過去 1 年間に何の侵入も見られなかった回答者の状況を、侵入が 10 回以上あった回答者と比較したところ、「最上位層」の OT リーダーは、次のような多くのベストプラクティスを順守する可能性がはるかに高いことがわかりました：

- OT のサイバーセキュリティ責任を CISO（現在または翌年）の下で担当
- 基本的なサイバーセキュリティ指標の追跡と報告
- サイバーセキュリティ製品の購入決定に関わること
- OT システムの活動を集中管理、視覚的に表示
- セキュリティ予算の増加

これらのベストプラクティスは、OT リーダーが業界の変化に対応し、期間を短縮し、生産性を高め、脅威や脆弱性に対する最善のこの攻撃への対策を提供できるようにする、サイバーセキュリティに対する総合的な手法を反映しています。

イントロダクション

OT（制御システム）は、実経済にとって重要なコンポーネントです。これにより、世界中の工場、エネルギー製造･送電設備、輸送ネットワーク、ユーティリティが機能するようになります。技術の進歩により、経済全体での運用効率が大幅に向上しており、製造およびプラントの運用は例外ではありません。OT ハードウェアとソフトウェアの年間売上高は、5 年間で毎年 6% 以上成長した後、2022 年までに 400 億ドルに達すると予測されています [1]。

この新たな支出の多くは、業務の効率化と利益率向上のために、監督管理やデータ収集（SCADA）などの OT コントローラ型と IT ネットワークの融合に関連しています。これまでインターネットから隔離されていた OT システムは、リアルタイムでプラントオペレーションを効果的に管理するために、IT システムやインターネットサイトからの情報に依存するようになりました。

しかし、この改善された機敏性は、リスクの増加を犠牲にして、もたらされます。隔離されている OT システムに対する最大のリスクは、物理メディアから手動でロードされたソフトウェア更新から生じる可能性がありますが、今日の OT システムの多くは、IT システムが直面するすべての脅威に直面しています。さらに、OT システムの攻撃対象領域には、パイプラインや水道主電源に接続されたセンサなど、リモートロケーションにある IoT（Internet-of-Things）デバイスが含まれることがよくあります。

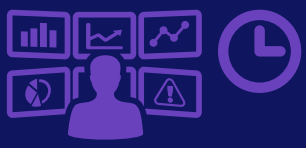
OT リーダーは最先端のテクノロジーを使用して高度な攻撃者に先行して対応する必要があるため、脅威の状況はますます高度化しています。次のセキュリティのベストプラクティスには、手間がかかるものと、手間がかからないものとがあります。ベストプラクティスを採用する際に生産性が影響を受けないように事前に計画するとともに、成功には適応性と柔軟性が必要です。

組織が脅威と脆弱性の増大、予算の停滞、人員不足、継続的な COVID-19 の危機に直面しているため、OT リーダーはこれらの課題に対応することが求められています。ベストプラクティスに従うことで、フラストレーションや失われた時間を減らすことができます。

本調査にあたって

本年度の「制御システムの現状とサイバーセキュリティレポート 2020」は、2020 年 4 月に実施された調査に基づいています。調査の質問項目は 2019 年版の報告書の基礎となった一年前の質問を採用しています[2]。回答者は、製造業、エネルギー・ユーティリティー、ヘルスケア、輸送の 4 つの産業に関わる企業で働いています。全員が製造業や工場運営の何らかの側面を担当しており、役職はマネージャーから VP まで多岐にわたっています。

本研究では、調査のデータを利用して、日常業務における運用プロフェッショナルとサイバーセキュリティとの相互作用の様子を描きます。この分析では、今年のデータに注目し、昨年の結果と比較することで、業界の状況に関するいくつかの包括的な洞察を明らかにしています。次に、データをより深く掘り下げ、過去 12 ヶ月間に侵入被害を経験していない「上位層」組織と、同期間に 10 回以上の攻撃を経験している組織で一般的に使用されているベストプラクティスを特定しています。



「サイバーセキュリティソリューションの開発に焦点を移し、増加するセキュリティのベストプラクティスに準拠していることの確認が必要なため、時間単位や分単位のタスクを達成する能力を妨げています。」

— 調査回答者：製造・製造管理責任者

OT セキュリティのための洞察

OT リーダーがサイバーセキュリティにおける役割を果たす中で、その多くが、中核となる保護機能の不足、セキュリティの測定や分析に苦労していること、組織への影響が大きい、重大な侵入被害に悩まされています。

OT リーダーには、サイバーセキュリティを含む幅広い責任があります。

OT リーダーは、一般的に、VP、COO、CEO を含め、組織内の上位レベルの人に報告します（図 1）。彼らは定期的にサイバーセキュリティに関する相談を受けており、80% が定期的にサイバーセキュリティの決定に参加しており、半数がその決定に対して最終的な発言権を持っています（図 2）。

オペレーションチームの監督と生産効率の管理に加えて、オペレーションプロセス内のセキュリティの組み込みは、OT リーダーの 64% に直接責任があります（図 3）。4 分の 3 近く（71%）が IT サイバーセキュリティ戦略に定期的に関与しており、2019 年の 56% から増加しています（図 5）。これは、セキュリティが成功の測定値であることを示しているように思われます。しかし、OT リーダーの 3 分の 1 だけがトップ 3 の成功測定値として、半分強がトップ 5 の成功測定値として挙げています（図 4）。

OT のリーダーは、サイバーセキュリティの側面を持っている可能性が高いです。明確な傾向として、OT セキュリティは CISO の下に配置されている方向に向かっています。CISO は、OT システムのセキュリティに関する事項を管理しており、今年は組織の 22% で昨年の 18% から増加しています。また、回答者の 61% が、来年には OT セキュリティの担当範囲が CISO のチームに移管されることを期待していると回答しています。これらの変更が予想通りに発生した場合、CISO のチームは来年までに 83% の組織で OT セキュリティを管理することになります。これは、接続された OT システムのリスクが高まっていることと、事業継続のための重要なインフラの性質を反映していると考えられます。

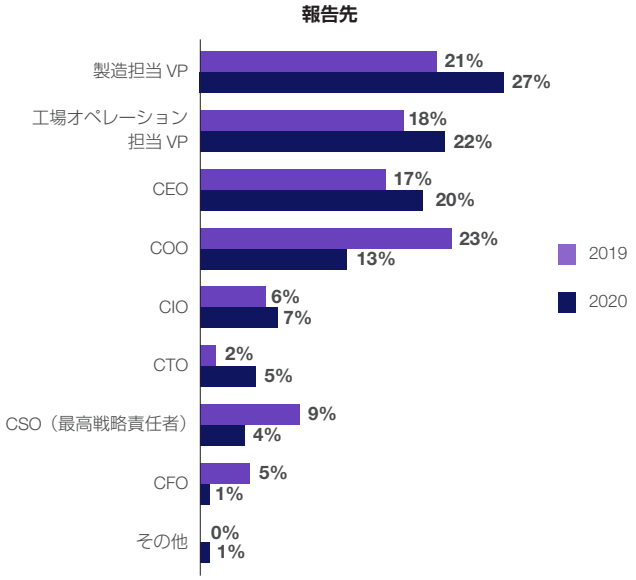


図 1：OT リーダーの直属の上司

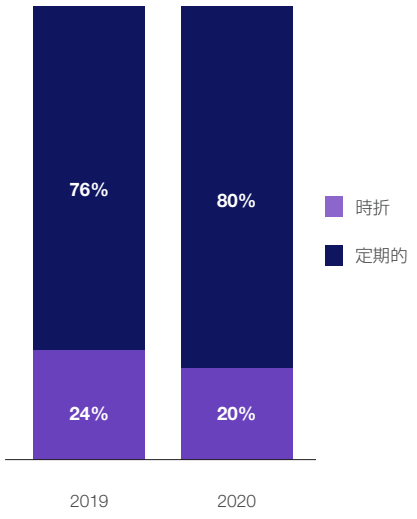


図 2：サイバーセキュリティにおける大手企業の関与の度合い

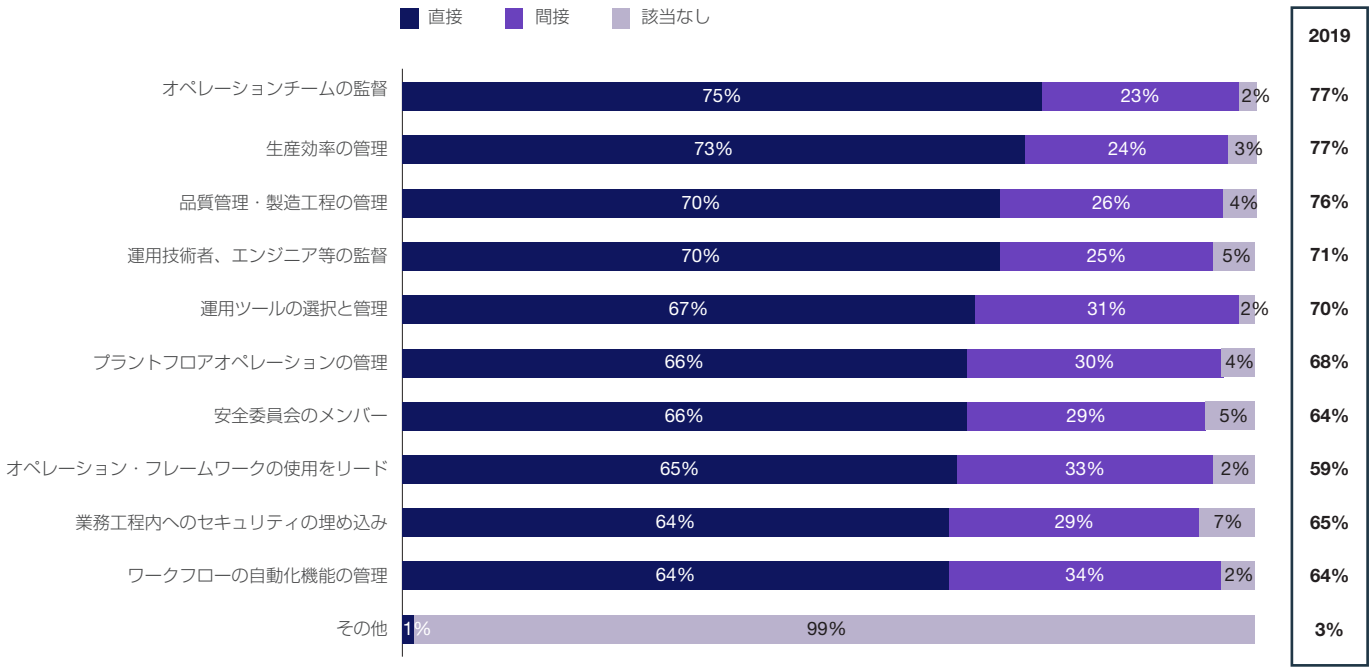


図 3：OT リーダーの業務責任

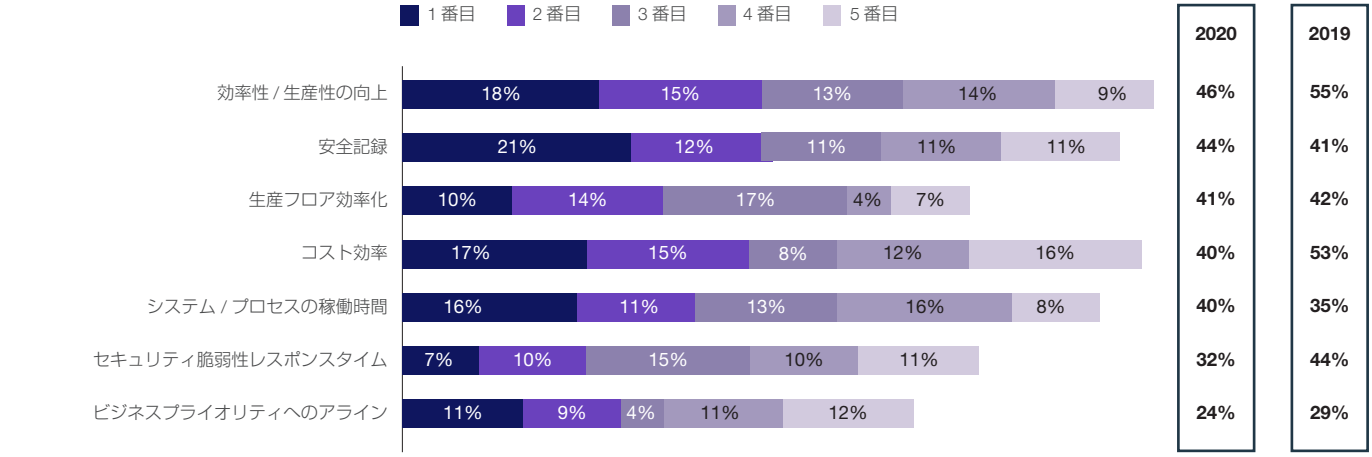


図 4：OT リーダーの成功の測定方法（ランキング）

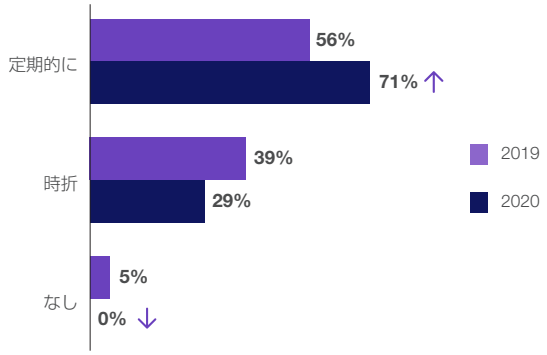


図 5：IT サイバーセキュリティ戦略への OT リーダーの関与

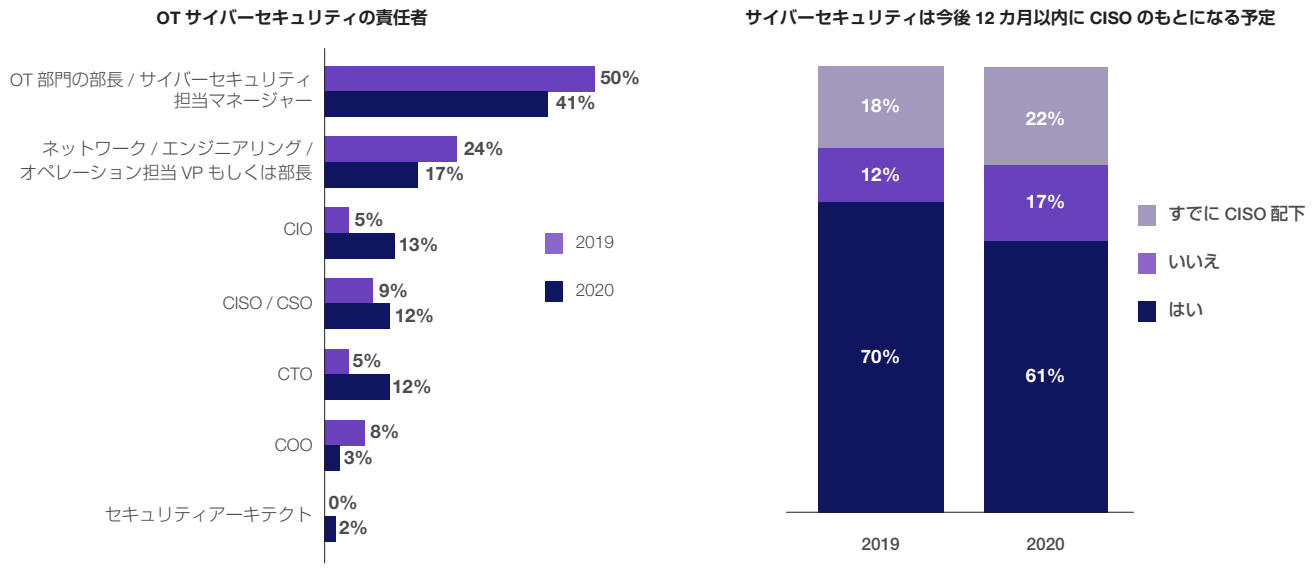


図 6：現在と今後 12 か月間のサイバーセキュリティの責任者

多くの OT インフラは未だにサイバーセキュリティの中核的な保護を欠いている

OT リーダーは、サイバーセキュリティやセキュリティ機能を多数導入していますが、多くは重要な分野で不足しています。例えば、セキュリティ情報・イベント管理（SIEM）ソリューションは、最もよく引用されるセキュリティ機能ですが、10 人に 4 人近くがこのツールをまだ持っていません（図 7）。半数近くがテクニカルオペレーションセンター（TOC）とセキュリティオペレーションセンター（SOC）がなく、半数以上がネットワークオペレーションセンター（NOC）を欠いています。SOC を設置している人のうち、77% は、セキュリティオペレーションチームがすべての OT 活動を一元的に可視化していない（図 8）。また、ゼロトラスト・アクセスを可能にする機能である、内部ネットワークのセグメンテーション（47%）、ネットワークアクセス制御（59%）、多要素認証など、多くの組織で不足しています。

幸いなことに、2020 年には 58% の組織が予算の増加を見ており、13% のみが劇的な増加を見込んでいます（図 9）。懸念されるのは、15% の組織でセキュリティ予算が減少しており、その数が前年比 10% 増となっていることです。さらに、COVID-19 が契機となり、こうした削減が減収やグローバルビジネスの縮小につながる可能性があります。

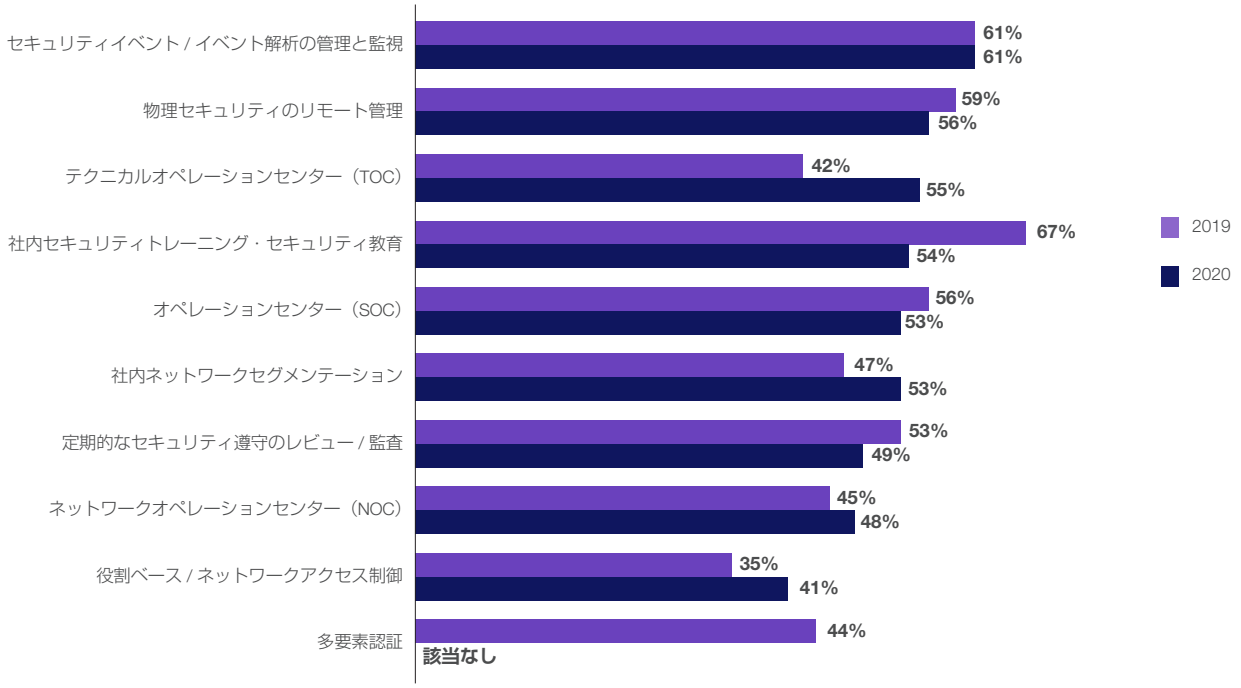


図 7：サイバーセキュリティと充実のセキュリティ機能の配備状況

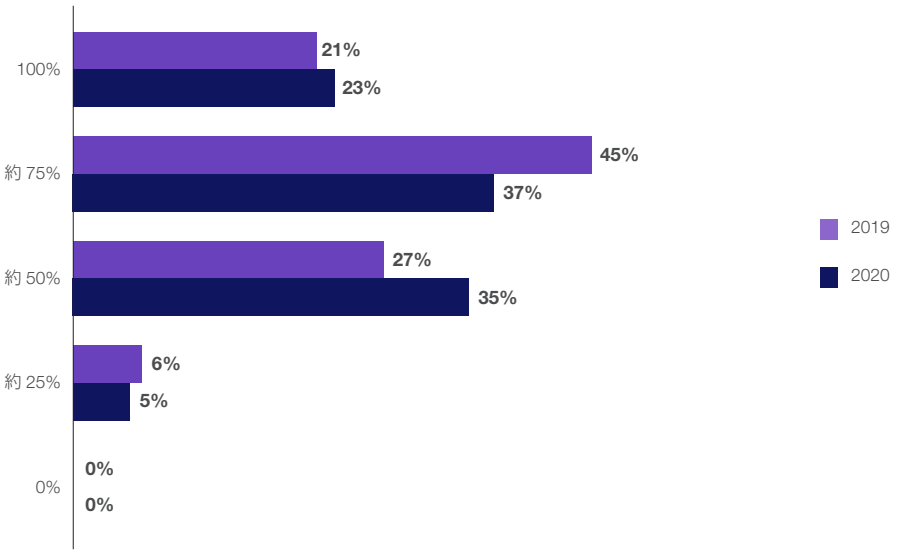


図 8：OT アクティビティの集中管理と可視化できている。

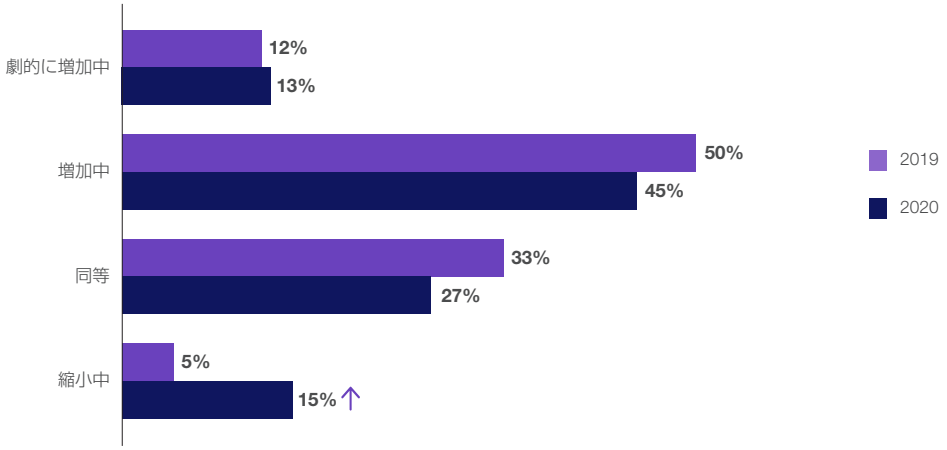


図 9：2020 年のセキュリティ予算

OT リーダーは、セキュリティの測定と分析にいまだに苦戦している

一部のサイバーセキュリティ測定値は、ある程度の一貫性を保って追跡され報告されていますが、組織の 36% から 57% の間では、標準的な測定指標のリストで各項目を測定することができていません（図 10）。脆弱性（64%）、侵入被害（57%）、サイバーセキュリティの取り組みによるコスト削減（58%）が追跡され、最も頻繁に報告されており、コスト削減の追跡は昨年の 23% を上回っています。最も一般的に報告されている指標は、有形のリスク管理で 43% となっています。このことは、OT のサイバーセキュリティが企業レベルのリスクの検討に完全に統合されていない可能性があることを示唆しています。

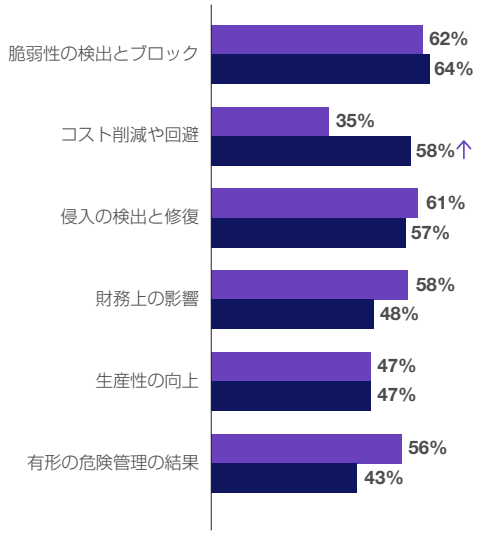
同様に、39% から 50% の組織では、基本的なサイバーセキュリティのデータをシニアリーダーやエグゼクティブリーダーと日常的に共有していません（図 11）。セキュリティ侵害とセキュリティ標準への準拠は、多くの場合、それぞれ 61% と 57% で共有されています。今年は、侵入テストの結果の報告が大幅な減少（22% から 52%）を示しました。

「遠隔地の従業員も対象とし、世界中のすべての企業資産を同様に保護するソリューションが必要です。」

– 調査回答者：プラントもしくは製造現場の VP もしくは部長

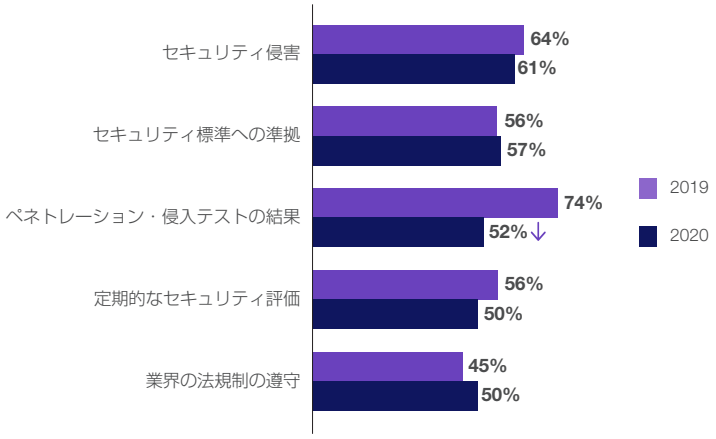
セキュリティソリューションのどの機能が最も重要であるかを尋ねると、セキュリティ解析、モニタリング、評価の各ツールが最も一般的に引用され、上位 3 で 58% が占められた（図 12）。このことは、OT のリーダーたちが、セキュリティに対するより戦略的でデータ主導型のアプローチの必要性を認識していることを示唆しています。興味深いことに、回答者のわずか 38% が攻撃検知を 3 つの最も重要な機能の 1 つと認識しており、2019 年の 61% から減少しています。

OT のリーダーたちは、サイバーセキュリティツールが仕事の妨げになり、その結果、プロとしての成功にマイナスの影響を与えていると認識し続けています。回答者は、セキュリティソリューションは運用上の柔軟性を妨げ（53%）、より複雑性を生み出す（50%）と主張しました。（図 13）



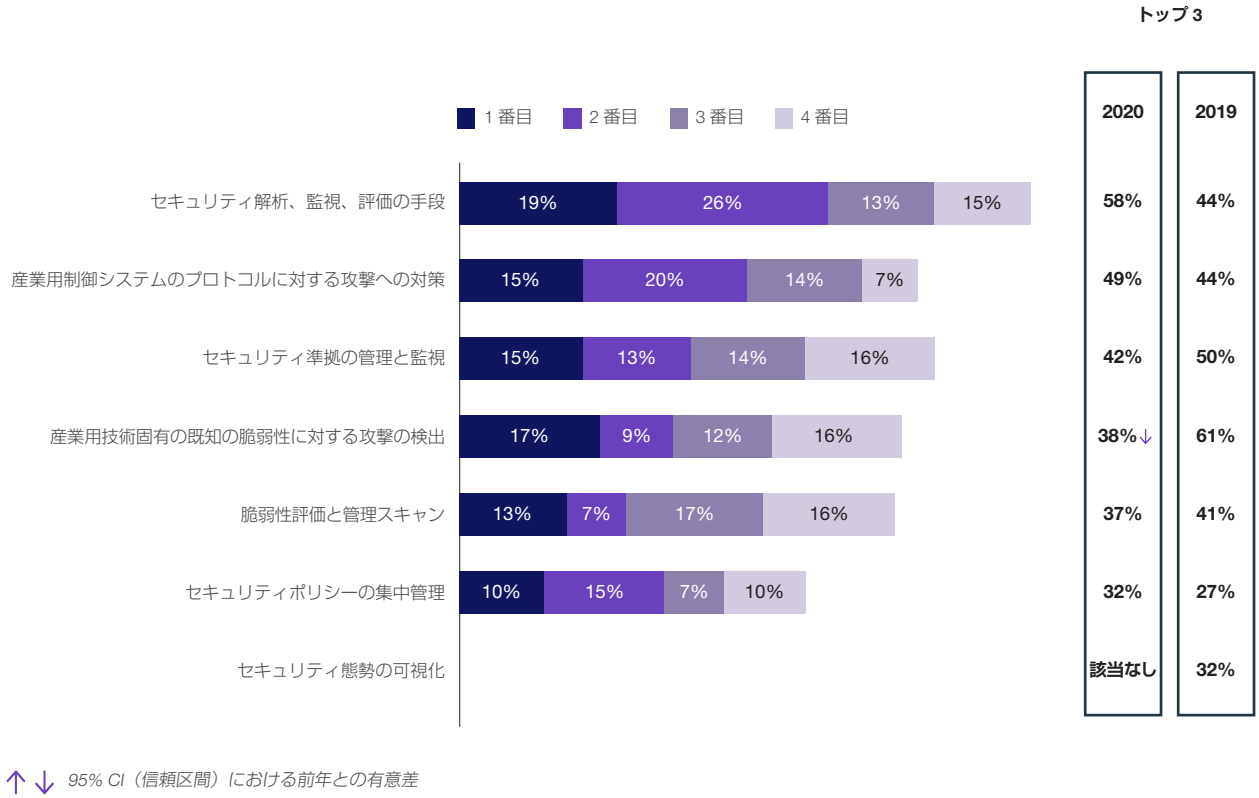
↑↓ *95% CI（信頼区間）における前年との有意差*

図 10：追跡および報告されたサイバーセキュリティ測定のタイプ



↑↓ *95% CI（信頼区間）における前年との有意差*

図 11：報告された OT サイバーセキュリティ問題のタイプ



↑↓ *95% CI（信頼区間）における前年との有意差*

図 12：最重要セキュリティソリューション主な特長（順位）

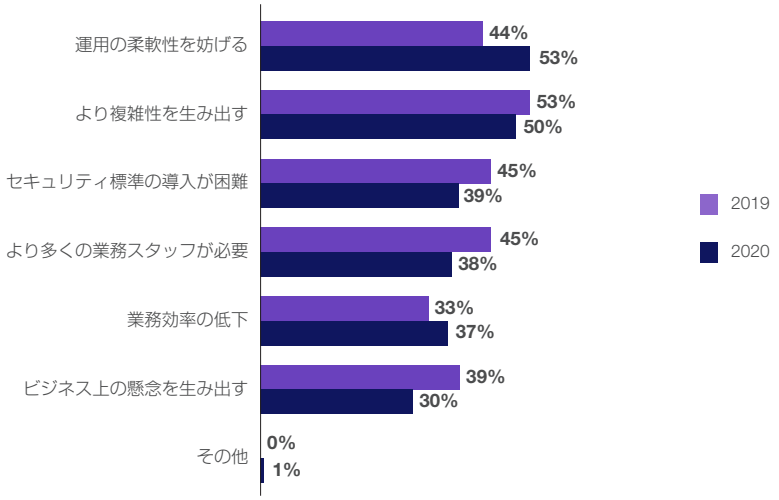
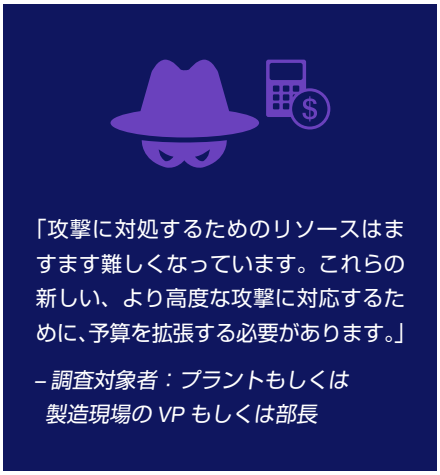


図 13：サイバーセキュリティソリューションが OT プロフェッショナルの成功（上位 3 位）にどのように悪影響を及ぼす可能性があるか。

ほとんどの OT リーダーが重大な侵入を目にしており、これらの影響は拡大します

調査に参加した OT リーダーに代表される組織は、グループとして、サイバー犯罪者のシステムへの侵入を防ぐことがほとんどできていません。過去 1 年間に 10 組織のうち 9 組織が少なくとも 1 回の侵入被害を経験し、72% が 3 回以上、26% が 6 回以上を経験しました（図 14）。組織のわずか 8% だけが、12 か月以上の侵入を受けていませんでした。この数値は、2019 年に何の侵入も報告しなかった回答者の 26% と比較して、一部の組織で問題が増大している可能性があることを示唆しています。

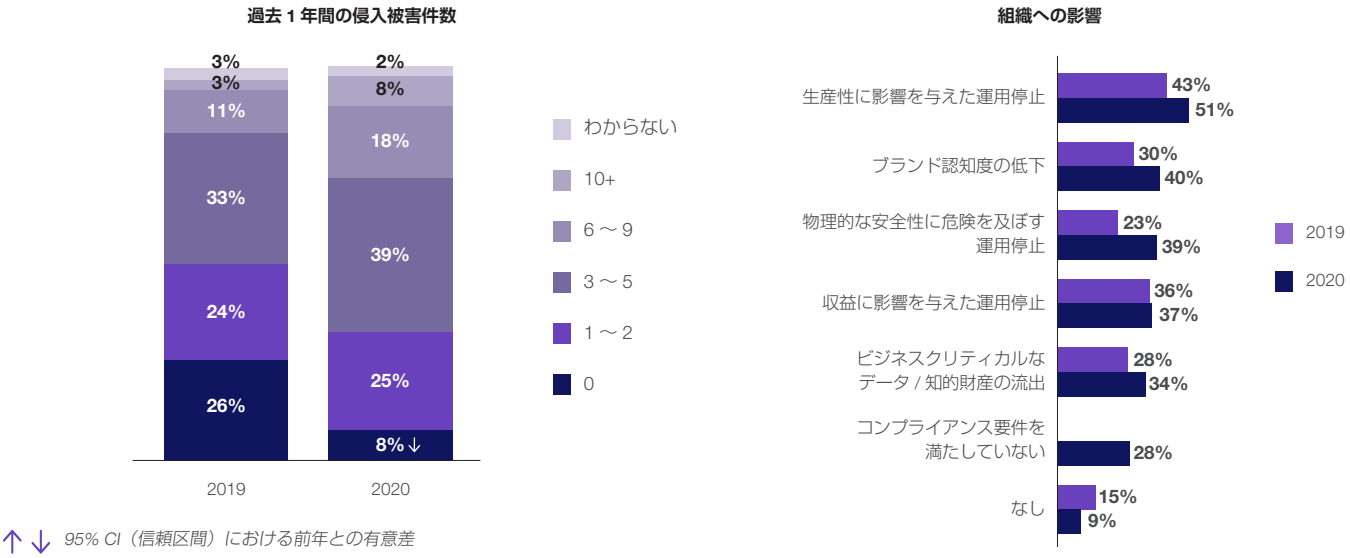
これらの侵入の影響は些細なことではありませんでした。半数以上の回答者が生産性に影響を与える侵入を報告し、37% が業務停止で収益に影響を与えていると回答しています。10 件中 4 件（39%）近くが、侵入によって物理的安全性がリスクにさらされたと報告しています。昨年の 16% から上昇。後者は、産業施設に内在する危険性を考えると、現実的な懸念です。



「攻撃に対処するためのリソースはますます難しくなっています。これらの新しい、より高度な攻撃に対応するために、予算を拡張する必要があります。」

– 調査対象者：プラントもしくは製造現場の VP もしくは部長

最も一般的な侵入は、マルウェア（60%）、フィッシング（43%）、ハッカー（39%）でした。過去 1 年間に被害を受けた団体数はハッカーについてのみ大幅に増えました（図 15）。ランサムウェアや DDoS 攻撃、内部犯行（意図的でない、意図的である場合の両方）も、昨年に比べて侵入件数が増えました。



↑ ↓ *95% CI（信頼区間）における前年との有意差*

図 14：侵入の被害と組織への影響

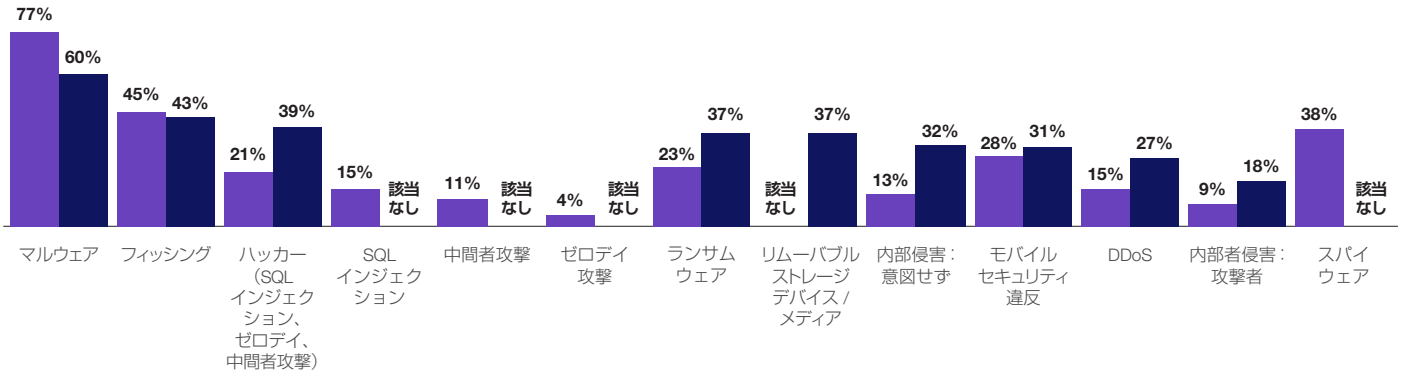


図 15：発生した侵入のタイプ

最上位組織のベストプラクティス

前述したように、OT リーダーの 8% のみが過去 1 年間に侵入がなかったと報告しており、さらに 8% の回答者が 10 回以上侵入があったと報告しています。この 2 つのサブセット、つまり「最上位層」と「最下位層」の回答者からの調査回答を比較しました。この分析では、最上位の OT リーダーが採用する可能性の高いベストプラクティスが多数特定されました：

1. 最上位層の組織では、すべての OT 活動がセキュリティ運用チームに集中的に見えるようになる可能性が 4 倍になります。

企業全体の効果的なセキュリティ保護には、一元化された可視性が不可欠であり、OT システムも例外ではありません。上位層の回答者はすべて、OT 活動の少なくとも半分の可視性を達成しており、半分は完全な可視性を達成しています。

2. 最上位層の OT リーダーは、検出およびブロックされた脆弱性を追跡してレポートする可能性が 133% 高くなります。

今年のソフトウェア脆弱性では、データ侵害のほぼ半分が追跡されていましたが、以前はわずか 26% でした [3]。上位層の回答者のほぼすべてが脆弱性を追跡して報告していますが、下位層の回答者の半数以下がこのベストプラクティスを順守しています。

3. 最上位層の組織は、現在 OT セキュリティを担当している CISO または CSO が 2 倍の確率で存在しています。

OT の接続が増えるにつれて、OT システムのセキュリティがより大きなサイバーセキュリティインフラストラクチャの一部であることがより重要になってきています。最上位組織は、この曲線よりも先行しています。幸いなことに、最上位層と最下位層の組織の大多数は、まだそうでなければ、来年にはこのベストプラクティスに従うことを計画しています。

4. 最上位層の OT リーダーは、OT 処理にセキュリティを埋め込む直接的な役割を持つ可能性が 25% 高くなります。

セキュリティが OT テクノロジーの基盤の一部である場合、後から追加するのではなく、同時にデプロイすると効果的になる可能性が高くなります。最上位層の OT リーダーの半分以上は、このベストプラクティスを保証する直接の責任があります。

5. 最上位層の組織は、ネットワークオペレーションセンター（NOC）を持つ可能性が 25% 高いです。

IT および OT 環境全体のネットワーク活動の集中的な可視性と監視は、ビジネスに不可欠な OT システムのパフォーマンスとセキュリティの両方を確保するのに役立ち、最上位層の組織がこれを達成した可能性が高くなります。

6. 最上位層の OT リーダーは、セキュリティ脆弱性へのレスポンスタイムによって測定される可能性が 25% 高くなります。

古い格言にもあるように、測定されたものは改善されます。最上位層の回答者の半数以上がセキュリティ脆弱性に対する回答期間を第 1、第 2 の優先順位にランク付けし、最上位層にない回答者の 2 倍が第 3、第 4、または第 5 位にランク付けしました。

7. 最上位層 OT リーダーは、業界規制への準拠をエグゼクティブリーダーシップに報告する可能性が 25% 高くなります。

コンプライアンスは、組織のトップリーダーにとってますます重要な課題になっていますが、レポートを手動で作成しなければならない場合、リーダーは監査人よりも頻繁に更新を受けることはありません。これらの定期的なレポートを作成する可能性が高くなるため、エンタープライズ向け全体でコンプライアンスレポートの作成を自動化することをお勧めします。これにより、より多くのリアルタイムなレポート作成アプローチと改善の機会が可能になります。

結論

OT システムのサイバーセキュリティをかなりの成功を収めて管理している組織もあるが、それ以上に多くの組織が苦労しています。これは、OT システムへの侵入がない組織の割合が昨年と比較して 19% 減少していることからも明らかです。

課題の性質は、組織ごとに固有です。中には、人手不足や十分な訓練を受けていないチームメンバーなど、スタッフの配置が問題となっている場合もあります。脅威や脆弱性に対処するためのツールが不十分であることに挑戦している人もいます。これらを提供するためのコストに挑戦している人もいます。多くは、脅威の頻度と回数、および脅威を管理するための適切なセキュリティを維持するために必要な期間を課題として抱えています。数人を除いて、この 1 年で少なくとも 1 回は侵入被害を受けており、複数の侵入者がいました。

このレポートで特定された特定のベストプラクティスに従うものは、侵入が大幅に少なくなる傾向がありました。これらの推奨事項は、地球を揺るがすようなものではありません。むしろ、これらは、セキュリティの基本的な安全対策の多くから成り立っており、一元的な可視性と制御に向けて積極的に取り組んでおり、基本的なサイバーセキュリティ指標の追跡と報告を行っています。OT システムは空白を失い、IT システムやインターネットと統合されるようになったため、OT リーダーはチームのセキュリティ意識を強化し、適切なセキュリティこの攻撃への対策でシステムを強化する必要があります。

「ゼロデイ攻撃は、たとえセキュリティ対策が整っていても、非常に大きな損害をもたらす可能性があります。リアルタイムにデータを確実にバックアップしなければなりません。それによって、決して時間とお金を失う必要はありません。」

– 調査回答者：プラント及び製造現場、エネルギー、ユーティリティの所長

[1]「Global Operational Technology Market — Industry Trends and Forecast to 2024」、Data Bridge Market Research、2017 年 10 月（英語）：https://www.databridgemarketresearch.com/reports/global-operational-technology-market

[2]「OT（Operational Technology）セキュリティトレンドレポート 2019 年版」、フォーティネット、2019 年：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ja_jp/ot-security-trends-2019.pdf

[3]「2020 Data Breach Investigations Report」、Verizon、2020 年 5 月（英語）：https://enterprise.verizon.com/resources/reports/dbir/

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

Copyright© 2020 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

Report-2020-OT-Cybersecurity-202009-R1