REPORT

セキュリティリスクが IT と OT の統合を遅らせていることが独自調査により判明

目次

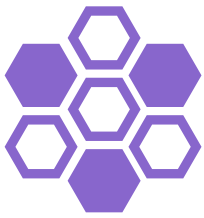
概要

フォーティネットは、Forrester Consulting と共同で、工場から精製所、通信インフラストラクチャに至るまであらゆるものを管理する産業用制御システム（ICS）や監視制御およびデータ取得（SCADA）システムなど、重要インフラストラクチャを管理 / 保守する担当者に影響するセキュリティトレンドに関する 3 回目の調査を実施しました。このレポートでは、グローバルな調査に基づいて、以下の 4 つのトレンドを明らかにしています。

- 組織は、IT と OT（オペレーショナルテクノロジー）システムの統合を予想以上に慎重に進めています。その主な理由は、重要インフラストラクチャのセキュリティを確保するためであると考えられます。
- 重要インフラストラクチャの専門家は、IoT デバイスから発生する新たなリスクや、コンプライアンスを中心とした継続的に増加している優先事項など、セキュリティに関する懸念を数多く抱えています。
- 一般的な組織では、OT セキュリティに対して戦略的かつ統合的なアプローチを導入しておらず、複数の技術的なポイントソリューションを異なるスケジュールで導入しており、場合によっては、セキュリティの特定の側面をカバーするのに 1 社以上のセキュリティのサードパーティに依存しています。
- 組織は、セキュリティに対してどうしても消極的な姿勢になりがちです。その結果、大多数の組織が ICS システムと SCADA システムの侵害を経験しており、その多くは過去 12 ヵ月以内に発生しています。

幸いなことに、回答者はより戦略的なアプローチの必要性を認識しているようで、いくつかの企業では過去 2 年以上にわたって OT システムの侵害を回避するためのベストプラクティスを採用しています。このことは、組織が新たな脅威への対応に追われている中で、将来の希望の光となっています。

インフォグラフィック：主な調査結果



15%

IT / OT システムを完全に統合している組織の割合。2018 年の 17% から減少。

2018 年から 2020 年にかけて、ICS / SCADA のセキュリティ上の懸念事項のトップ 5 の中で、デバイスの障害がマルウェアに取って代わった

78%

今年、ICS / SCADA セキュリティの予算を増額する予定の組織の割合

78%

今後 2 年間で規制の圧力が高まると予想する組織の割合

ICS / SCADA にとって最も重要な規制：GDPR、ISA、FISMA

34%

ICS / SCADA セキュリティを外部委託している組織の割合

58%

過去 12 ヵ月間に少なくとも 1 回、OT セキュリティ侵害を経験している組織の割合

一度も OT のセキュリティ侵害を経験したことがないと回答したのはわずか 10%

大手企業は、以下のように回答しています。

129% がビジネスパートナーにほとんど、またはまったくアクセス権を与えていない可能性が高いと回答

52% が IT プロバイダーに中程度以上のアクセス権を与えていないと回答

45% が高度なマルウェア検出を外部に委託していない可能性が高いと回答

はじめに

重要インフラストラクチャの所有者や運用者は、増え続けるサイバー脅威によるリスクの増大に直面しています。これは、統合についての話です。このようなインフラストラクチャを管理する ICS システムや SCADA システムは、IT システムに接続されたり、インターネットに直接接続されたりすることが多くなっており、エアギャップされていた時代には考えられなかったレベルのサイバーセキュリティリスクにさらされています。

以前は切り離されていた OT システムの多くがインターネットに接続されるようになったため、IT ベースのリサイクル攻撃と OT を狙ったセキュリティ上の脆弱性の両方が急増しています [1]。同時に、テロ、サイバー戦争、産業スパイなどの攻撃者や、単に利益を得ようとする一般的な犯罪者の攻撃も高度化しており、防御を強化していない組織に対して攻撃が成功する可能性が高まっています。このような重要インフラストラクチャへの攻撃は、金銭的損失、ブランドイメージの低下、そして時には人命の損失や国家安全保障に対する脅威にさえつながりかねません。

ほぼすべての ICS / SCADA ベンダーにおいて、過去 1 年間でセキュリティ上の脆弱性の量と発生率が増加 [2]。

しかし、IT システムと OT システムを統合することは、ビジネスとしては理にかなっています。これには、プロセスのより効果的かつ効率的なモニタリング、IoT デバイスから得たデータの意思決定への活用、消費電力の大幅なコスト削減、原材料の無駄遣いの削減、従業員の効率化などのメリットがあります。その結果、統合への取り組みが明らかなトレンドとなっていますが、このプロセスには多くのセキュリティ上の課題が伴います。たとえば、攻撃対象領域の拡大、切断されたインフラストラクチャを想定して設計されているセキュリティ機能を備えたレガシーシステム、システムの可視性の低さ、ネットワークのセグメンテーションの不備などが挙げられます。

調査方法

本レポートでは、2 年に 1 度の調査でこれらのトレンドを確認しています。フォーティネットは Forrester Consulting に依頼して、OT とサイバーセキュリティ分野におけるリーダーの現在の展望、課題と優先事項、重要な ICS と SCADA のインフラストラクチャのセキュリティを確保するための戦略を探るために、効果的な調査を実施しました。Forrester は、2016 年と 2018 年に、すでにこのテーマに関して調査を実施しており、本レポートでは、前回の調査以降に起こった変化に注目しています。

Forrester は、世界中の 400 人以上の専門家を対象に、定量的な調査を実施しました。回答者の職務等級は、マネージャーから最高責任者レベルまでとなっています。彼らは、重要インフラストラクチャの保護、インターネットプロトコル（IP）レベルのセキュリティ、SCADA システムや IoT デバイスのセキュリティなどを担当しています。従業員数 500 人以上の企業に勤務しており、米国の回答者に至っては従業員数 1,000 人以上の企業に勤めています。特に、製造業、通信業、エネルギー生産 / 流通業など、重要インフラストラクチャが分散している企業を中心に、さまざまな業種の方々が参加しています。

本レポートでは、このような方々とその所属企業に影響を与えるトレンド、特に OT システムのセキュリティと IT と OT の統合に焦点を当てています。私たちは、さまざまな角度から回答を分析し、2020 年に関する 4 つの市場トレンドを特定しました。さらに、セキュリティ侵害の経験が少ない企業と多い企業とでは、どのようなセキュリティのベストプラクティスが採用される可能性が高いかを分析しました。

重要インフラストラクチャのサイバーセキュリティトレンド

トレンド：IT と OT の統合は複雑であり、組織は計画的に移行している

最近行われたある調査によると、OT システムの 2 / 3 近くがインターネットに接続されているという結果が得られました。つまり、調査対象企業の 32% は直接インターネットに接続され、別の 32% はゲートウェイ経由でインターネットに接続されていました [3]。トレンドが統合に向かっていることは間違いありませんが、多くの企業はこのプロセスが予想以上に複雑でリスクが高いことに気づいています [4]。

実際、Forrester の調査では、統合に向けての具体的な課題を予測していないと答えた回答者はわずか 4%（図 1）でした。つまり、96% の回答者が問題を予測しています。その多くは、社内のチームやサードパーティのサービスプロバイダーが、一般的なコンバージドテクノロジーや、特に IoT デバイスのセキュリティに関する十分な専門知識を持っていないのではないかという懸念に関連したものです。その結果、データ漏洩が発生する可能性があり、これについても回答者の 40% 以上が懸念しています。これらの 3 つの懸念事項については、2018 年よりも 2020 年の回答者のほうがより多くの懸念（数ポイントの差）を示しています。

オペレーショナルテクノロジー（OT）と情報テクノロジー（IT）を統合した場合、セキュリティ上の課題として認識または予測されるものは以下のどれですか？

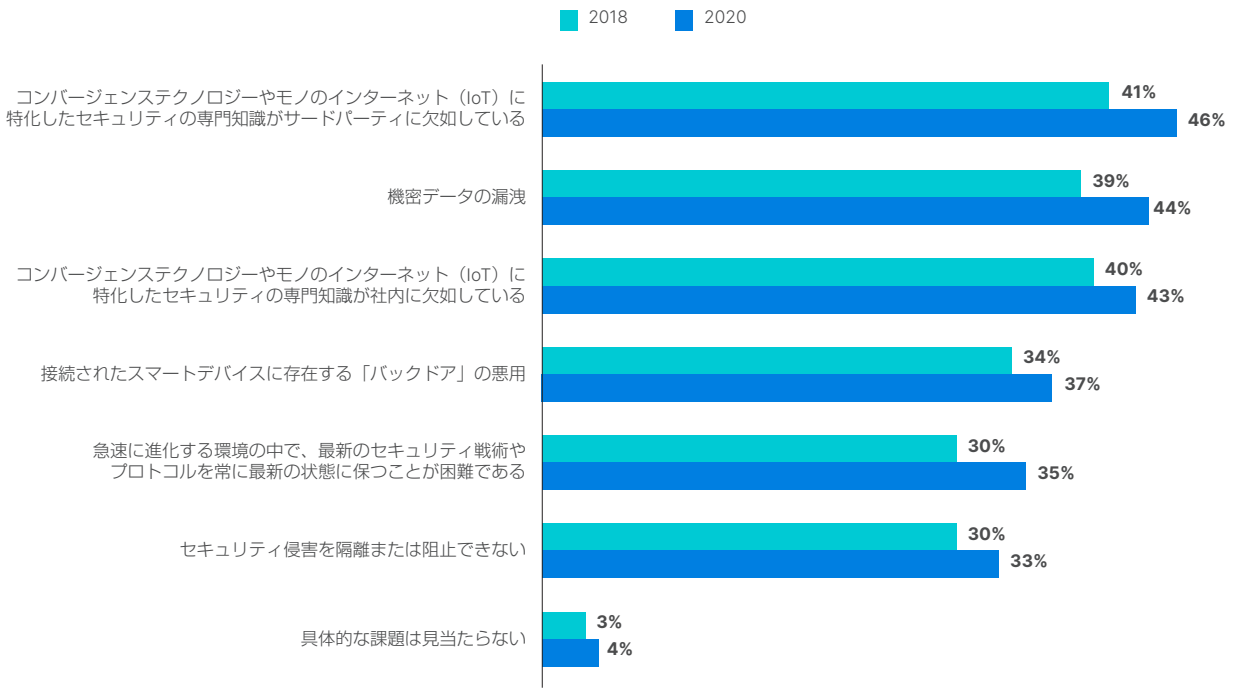


図 1：IT / OT の統合に関する課題

特に、2020 年の回答と 2018 年の回答を比較したデータは、この不安を裏付けています。この 2 年間で、IT システムと OT システムが深く統合されたと答えた回答者の割合は実際には 2 ポイント減少し、一方で OT システムが完全にエアギャップされていると答えた回答者の割合は横ばいでした（図 2）。これらの特定の結果は、OT システムが孤立しているという傾向ではなく、2 つのサンプルのわずかな違いを反映していると考えられますが、多くの人が予想していたような急速な統合への移行ではないことを示唆しているようです。

OT システムが接続されている場合、それは必ずしも意図的で戦略的な決定を反映しているわけではありません。場合によっては、OT システムのインターネットへのゲートウェイは、OT システムとインターネットの両方に別々に接続された 1 台の PC と同じくらい無害です。また、統合の過程では、インターネットからデータを取得したり、企業の IT システムにデータを報告したりする IoT デバイスの大規模な導入や依存がますます一般的になっています。企業は OT 環境にさまざまな IoT デバイスを採用していますが、過去 2 年間で最も増加したのは、リアルタイムの位置情報トラッキングと GPS トラッキングデバイスでした（図 3）。

組織がオペレーショナルテクノロジー（OT）と情報テクノロジー（IT）をどのように統合させているか、次のうち最も適切なものはどれですか？

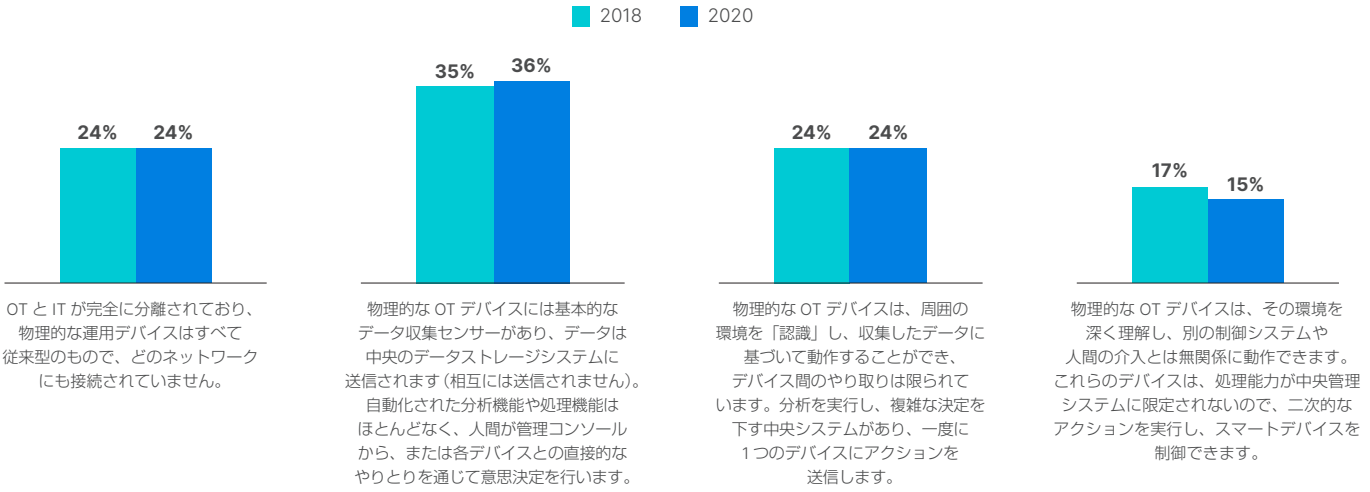


図 2：組織における IT / OT の統合

現在、組織のネットワークに接続されているモノのインターネット（IoT）技術を以下の中から選んでください（該当するものをすべて選択してください）。

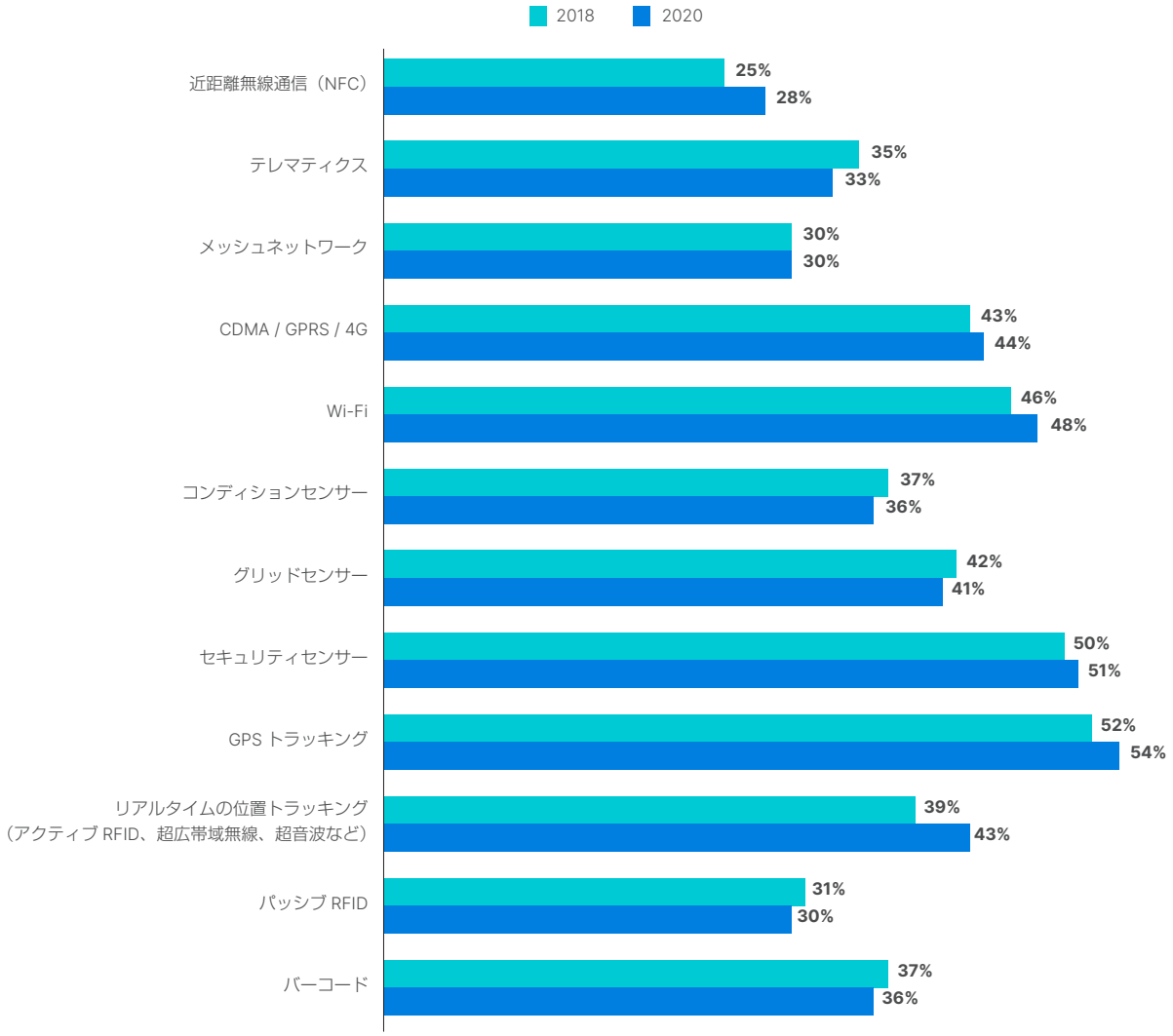


図 3：コネクテッド IoT 技術

トレンド：重要インフラストラクチャの保護には多くのセキュリティ上の懸念がある

ICS および SCADA システムのセキュリティに関しては、過去 2 年間で回答者の最大の関心事が多少変化しています。2018 年にはマルウェアが重要インフラストラクチャの専門家の最大の懸念事項でしたが、2020 年にはこの懸念事項はトップ 5 から外れ（図 4）、2 年間で回答者が 13% 減少しています。逆に、2020 年には回答者の 4 分の 3 近くが指摘しているように、デバイスやソフトウェアの障害が同じ期間で懸念事項として増加しています。

このような変化の理由は不明ですが、企業が 2 年前と比較してマルウェア対策ソリューションを強化し、信頼性を高めていることが考えられます。逆に、接続された IoT デバイスに重要インフラストラクチャシステムがますます依存するようになると、それらのデバイスのダウンタイムが懸念されるようになるかもしれません。

「ここ数年、サイバーフィジカル攻撃は深刻な脅威として注目されてきました。しかし近年、これらの攻撃は徐々に理論から現実へと姿を変えています [5]」

SCADA / ICS ネットワークのセキュリティに関連して、以下の項目について懸念される度合いについてお答えください。

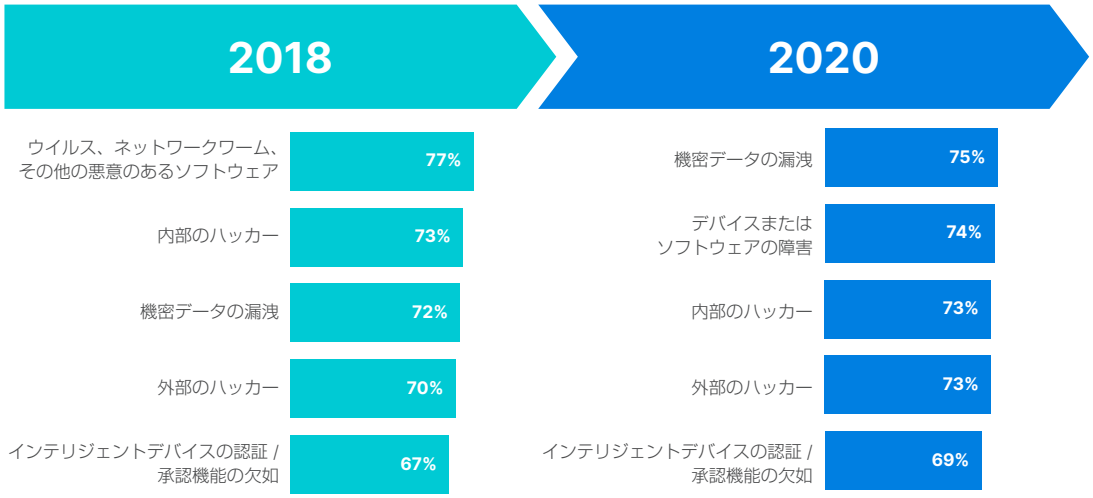


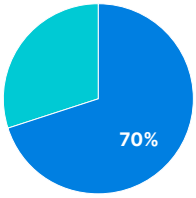
図 4：ICS / SCADA のセキュリティに関する懸念

重要インフラストラクチャを持つ企業にとって、もう 1 つの大きなセキュリティ上の懸念事項として、コンプライアンスが挙げられます。回答者の 10 人に 7 人は、過去 1 年間で自社に対する規制の圧力が高まったと答えています（図 5）。また、78% の回答者が、今後 2 年間でこれらの圧力がさらに高まると答えています。このことは、次に挙げるような企業が直面している膨大な数のさまざまな要件が物語っています。リスト化された 20 種類の規格のうち、回答者の過半数が、19 種類の規格に「ほぼ規制されている」または「完全に規制されている」と回答しています（図 6）。

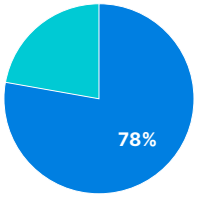
企業全体、特に ICS および SCADA システムに対するコンプライアンスの最優先事項は驚くべきものではありません（図 7 ～ 8）。いずれの質問に対しても、トップ 3 の回答は EU の一般データ保護規則（GDPR）、国際自動化協会（ISA）規格、米国連邦情報セキュリティ管理法（FISMA）の要件でした。

このような複雑なセキュリティ上の懸念を背景に、組織では OT セキュリティへの大規模な投資を計画しています（図 9）。全体では、回答者 10 人のうち 8 人近く（78%）が、今後 1 年間に OT のセキュリティ支出の増加を計画しており、半数以上（51%）が 5% 以上の増加を計画しています。OT のセキュリティ予算が変わらないと答えた回答者はわずか 10% で、これは、OT インフラストラクチャ自体の予算が増えないと回答した回答者の半数以下でした。全体的に見ると、他のどの支出分野よりも OT セキュリティの予算を増やすと答えた回答者が多くいました。

以下の各項目について、どの程度同意されるかお答えください。



過去 1 年間、規制による圧力は高まっている。



今後 24 ヵ月間、規制上の圧力は継続的に増加すると予想している。

図 5：企業に対する規制上の圧力

組織が以下の法律 / 規格に基づいて規制されている程度について、最もよく当てはまるものはどれですか？

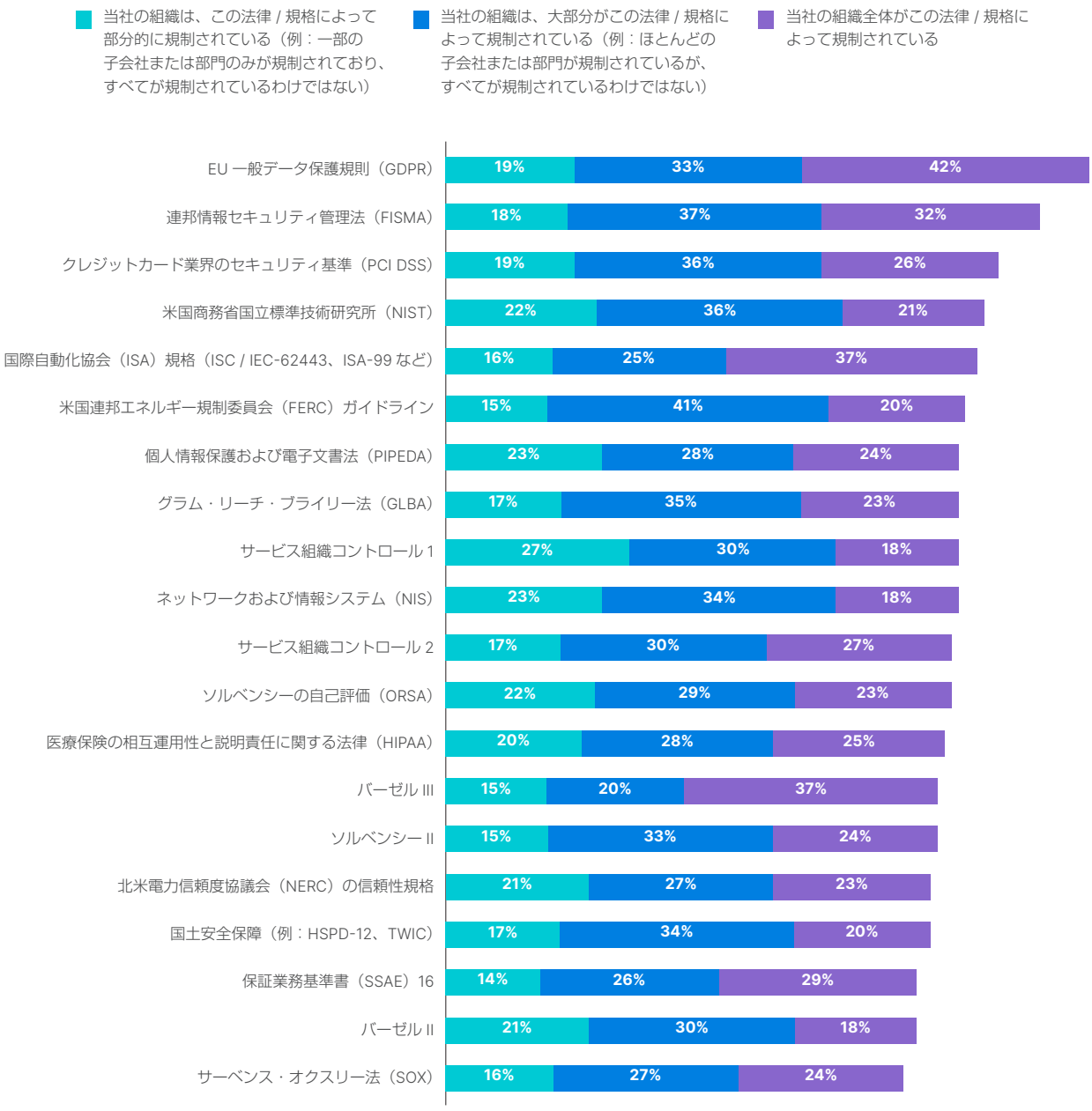


図 6：組織全体に影響を及ぼす規制および規格

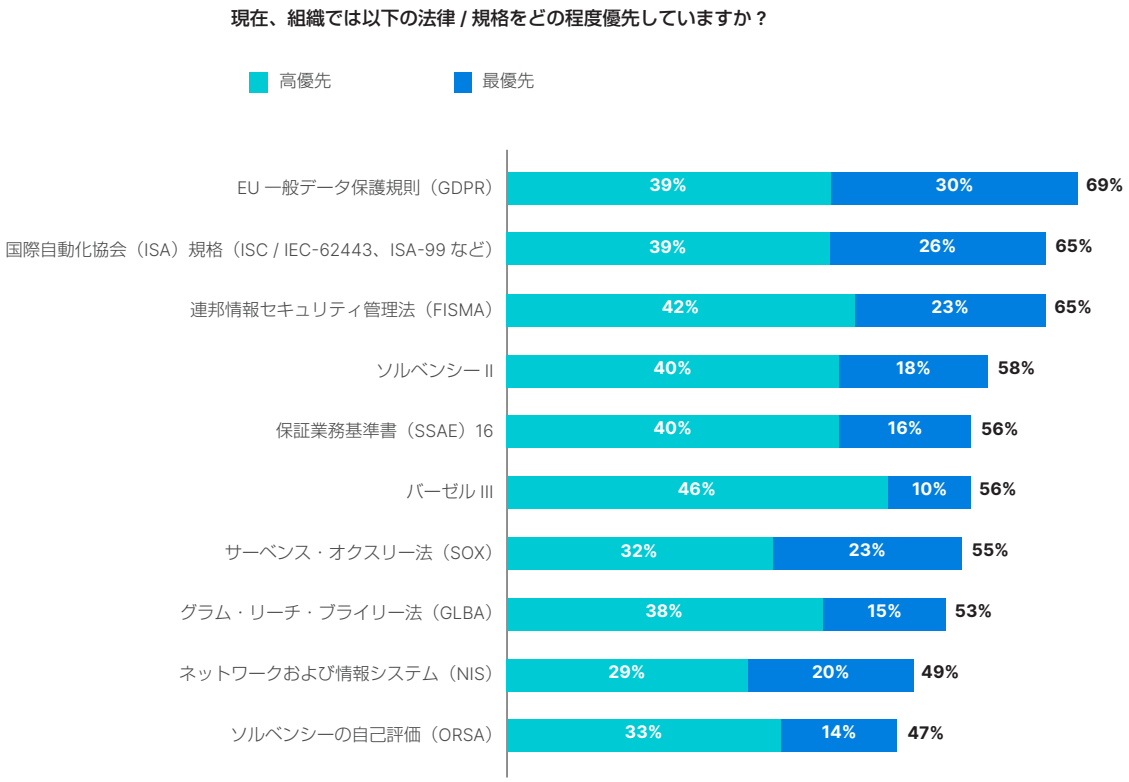


図 7：規制と規格の優先順位

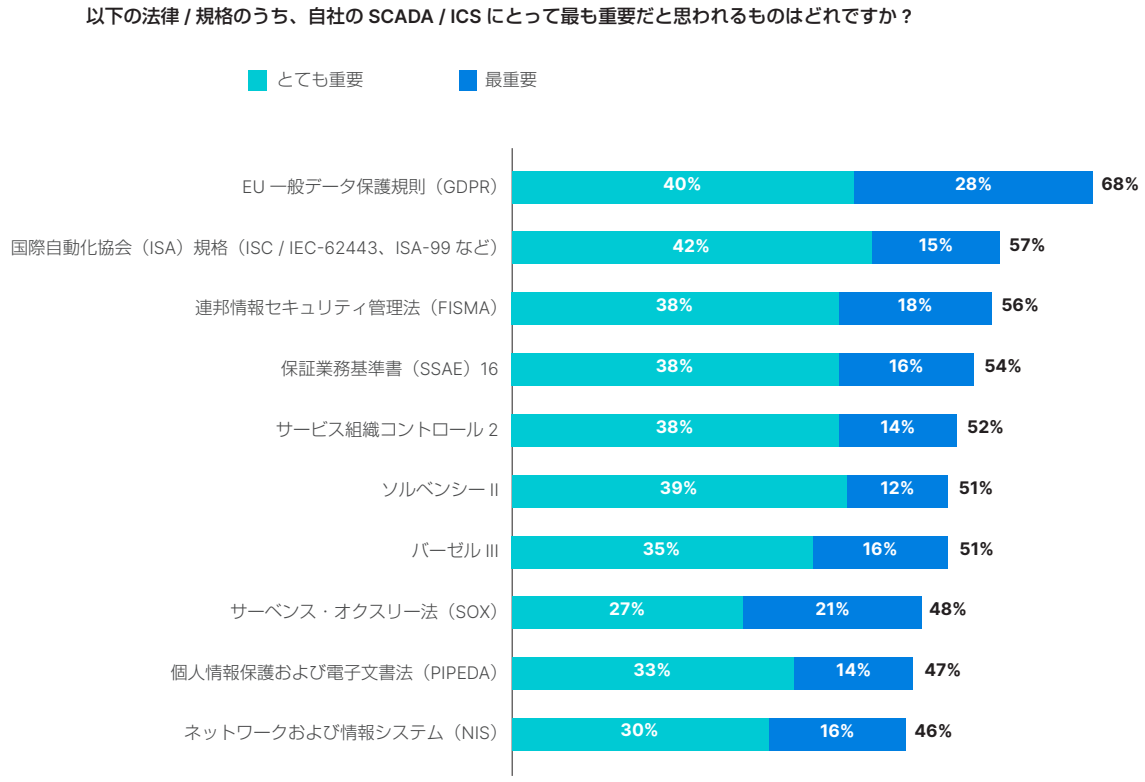


図 8：ICS および SCADA システムに関する最も重要な規制および規格

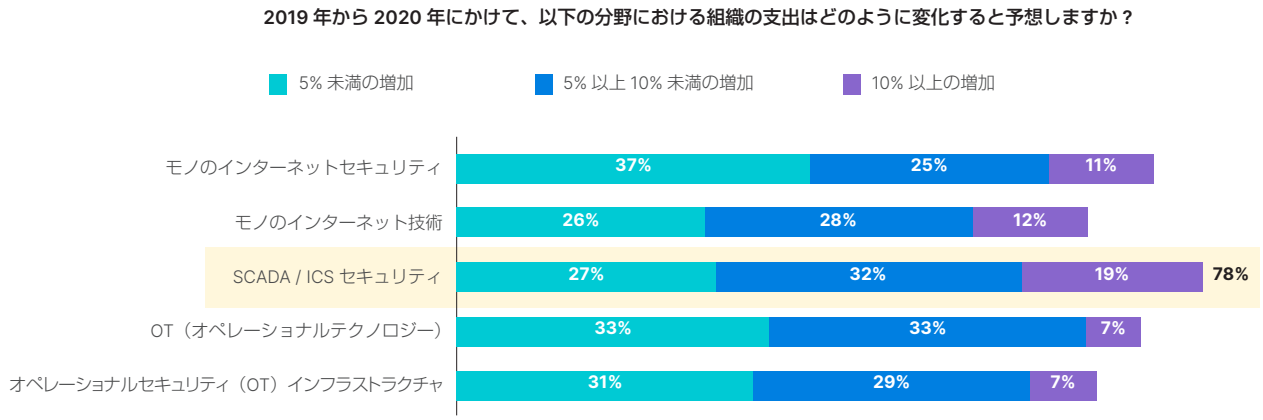


図 9：今後 12 ヵ月間の組織のセキュリティ支出の優先順位

トレンド：ICS / SCADA システムのセキュリティ保護は複雑で、行き当たりばったりのアプローチも珍しくない

OT セキュリティのさまざまな側面について質問したところ、回答者の多くが断片的なアプローチを取っていることが明らかになりました（図 10）。現在、組織で採用されているセキュリティ対策は、SSH または TLS による暗号化が 52%、堅牢なセキュリティ分析が 74% と多岐にわたっています。現在、暗号化を採用している組織はわずか半数に過ぎないことから、30% の組織が今後 1 年間に暗号化を導入する予定であることは驚くべきことではありません。これは、特権 ID 管理（PIM）技術（31%、図 10）に次いで 2 番目に多い新規プロジェクトです。

現在のセキュリティ強化の取り組みは、OT システムの脅威がますます高度化し、懸念されるようになっていることに対応するものです（図 11）。どのような要因が、現在の ICS / SCADA セキュリティ戦略に寄与したか尋ねたところ、典型的なサイバー犯罪者（75% 対 62%）と国家的な攻撃者（66% 対 62%）の両方について、今年は 2018 年よりも懸念が高まっています。顧客向けシステムに影響を与える攻撃を恐れる回答者が増えました（75% 対 67%）。これは、急速に進化する市場において、顧客向けシステムの重要性が増していることを反映していると考えられます。逆に、従業員が業務用デバイスとして個人所有のテクノロジーやクラウドテクノロジーを使用することへの懸念は低くなっています（58% 対 65%）。これは、シャドー IT や個人所有デバイスの業務利用（BYOD）などの問題に対処するための対策を講じている組織があるためだと思われます。

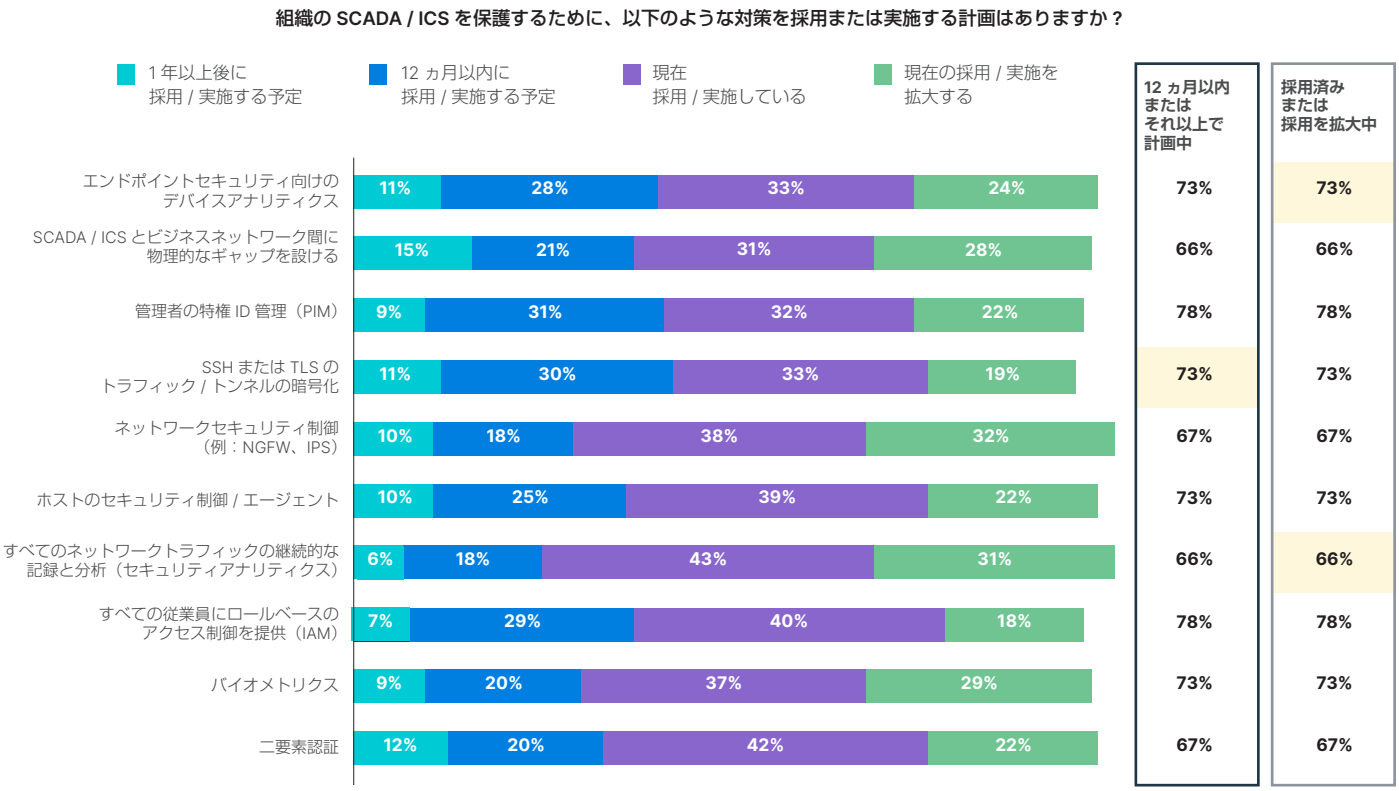


図 10：さまざまな OT セキュリティ対策の状況

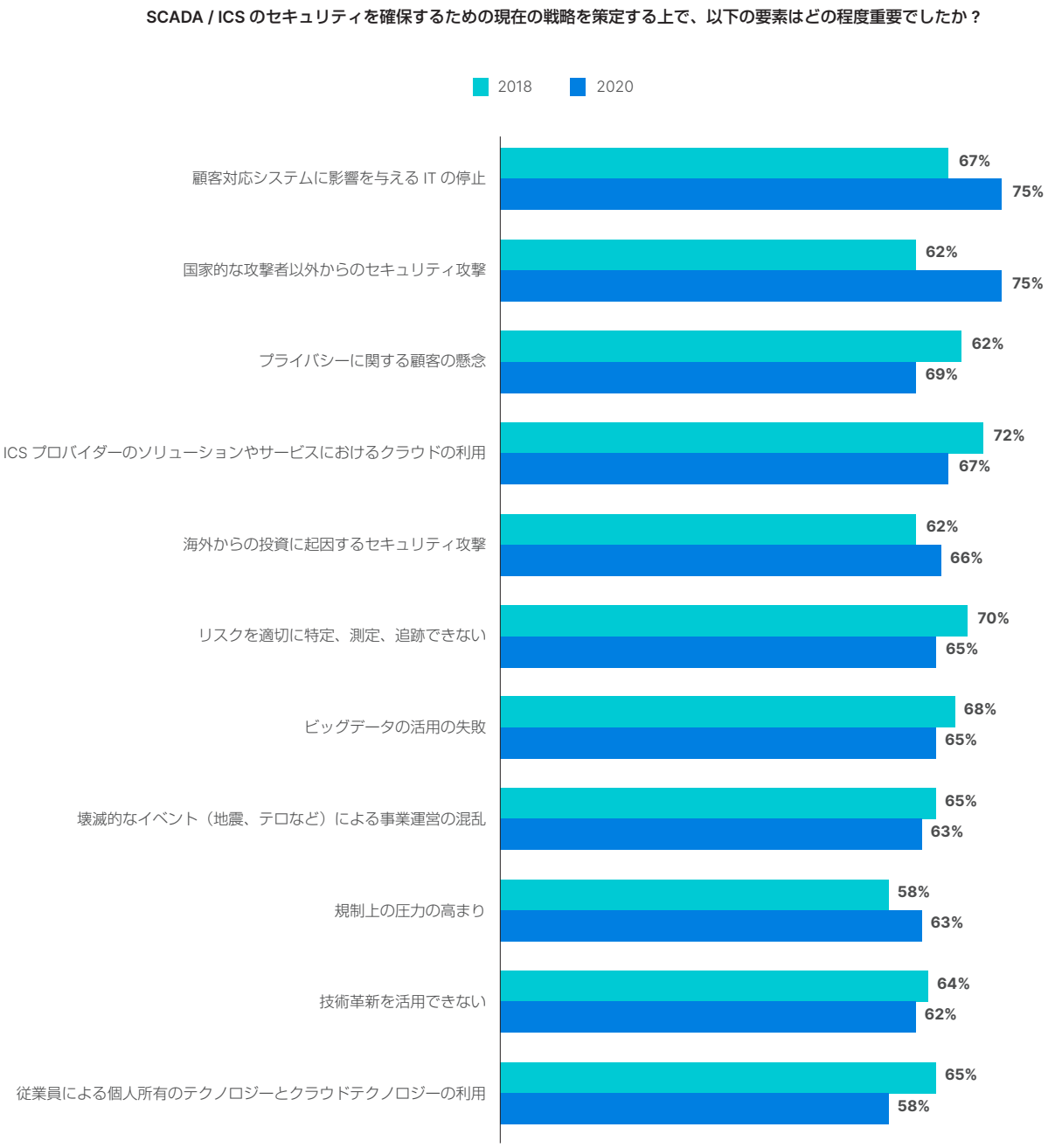


図 11：ICS / SCADA のセキュリティ戦略において、最重要である考慮事項と、非常に重要な考慮事項

断片的なアプローチは、OT セキュリティのさまざまな側面をアウトソースするかどうかを決定する際にも適用されます。組織の 1/3（33%）が OT インフラストラクチャをアウトソースしていますが、これは 2018 年には 27% でした（図 12）。しかし、OT セキュリティの側面をアウトソーシングしている組織の割合は、35% から 34% へと減少しましたが、横ばいでした。これらの違いは小さく、単に異なるサンプルを反映しているだけかもしれませんが、企業がセキュリティよりもインフラストラクチャのための新しいアウトソーシングの取り決めを積極的に検討しているように見えるのは興味深いことです。

セキュリティ機能の一部を外部委託している企業では、侵入防止システム（IPS）、ワイヤレスセキュリティ、IoT セキュリティが最も一般的で、全体の 41% がそれらの機能をアウトソースしています（図 13）。新たなセキュリティニーズとして、IoT セキュリティのアウトソーシングが、2018 年以降、同グループ内で 5% 増加しました。全体として、アウトソースしている企業の 55% が複数のセキュリティサービスベンダーに依存しています（図 14）。特に米国企業では、マルチベンダーアウトソーシングの利用が 2 年間で 53% から 67% に増加しました。このようなマルチベンダーのポイントソリューションへの依存は、OT システム保護の断片化を悪化させ、複雑さが増し、運用効率を低下させるおそれがあります。

セキュリティに対して、戦略的なアプローチではなく戦術的なアプローチをとっていることを示すもう 1 つの兆候は、回答者がサードパーティに付与しているアクセスレベルを報告する際にみられます。組織の 2 / 3 近く（65%）が IT プロバイダーに対し、完全なアクセス権、または非常に高度なアクセス権を付与しており、ビジネスパートナー（59%）や政府機関（53%）にも同様のアクセス権を与えている組織が多数を占めています。大多数の組織が断片的なマルチベンダー方式を採用していることから、多くの場合、IT プロバイダーやその他のサードパーティは、業務を遂行するのに必要以上のアクセス権を付与されていると考えられます。現状のシステムでは、役割に応じてアクセスを明確に制御するためのインテリジェントなセグメンテーションができていない可能性があります。

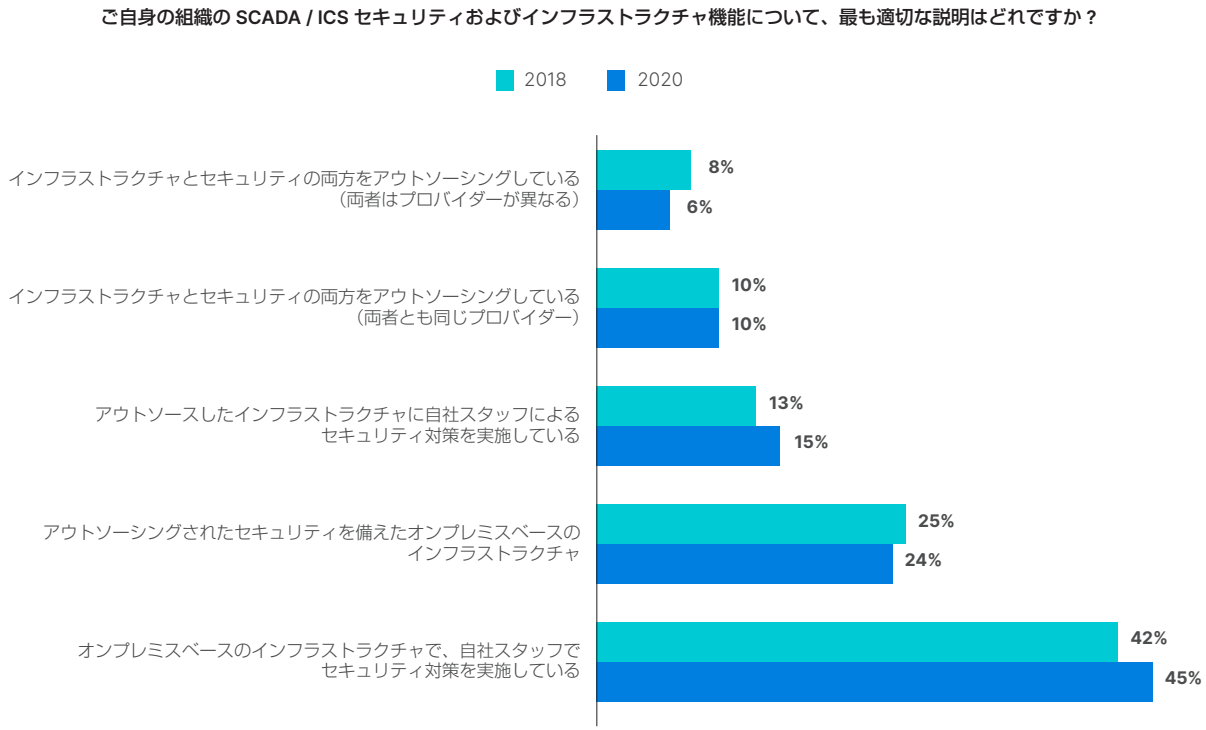


図 12：ICS / SCADA セキュリティのアウトソーシングの状況

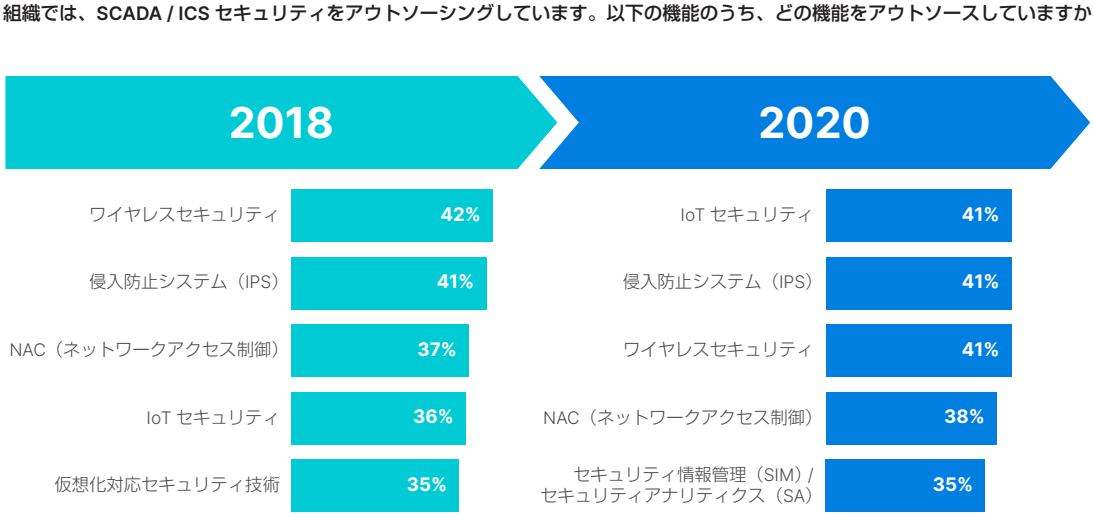


図 13：アウトソーシングされた ICS / SCADA セキュリティ機能

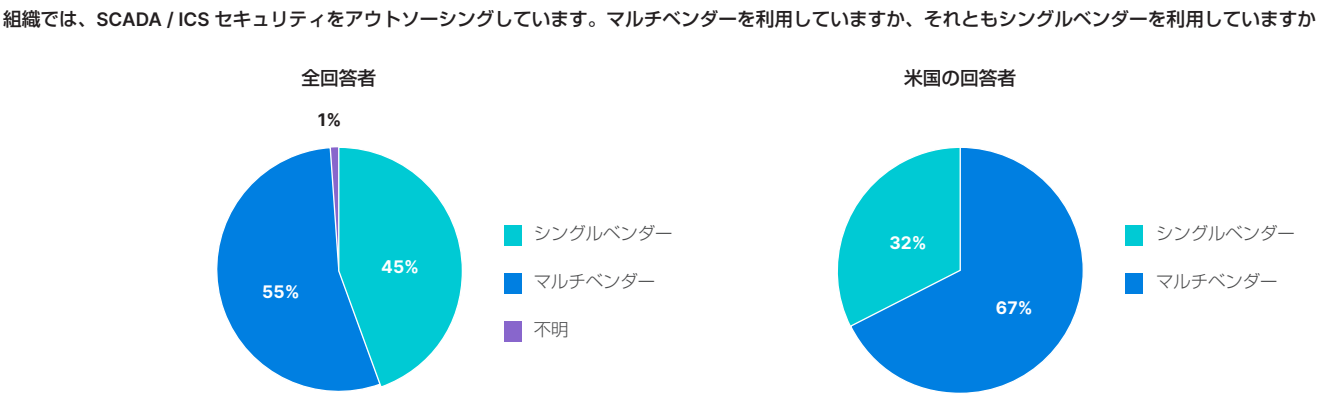


図 14：ICS / SCADA セキュリティ向けの単一ベンダー / マルチベンダーのアウトソーシング

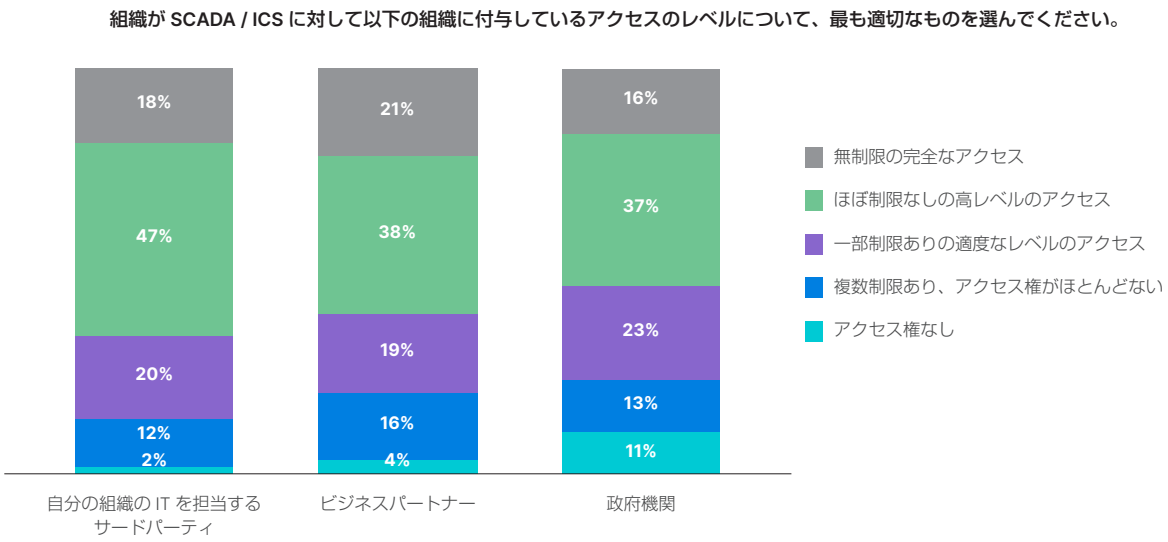


図 15：サードパーティに付与されるアクセスのレベル

トレンド：OT セキュリティは後手に回りがちで、ほとんどの OT システムが侵害されている

このような細分化の進行に加えて、組織は依然として OT のセキュリティに対して消極的な姿勢を取る傾向があります。このことを示す一つの例が、組織がリソースをどのように消費するかです。回答者は、平均で予算とスタッフの時間の約半分（49%）を攻撃への対応に費やしており、脅威の予防のために積極的に対策を練る目的で費やされる時間はわずか 21% だと推定しています（図 16）。

企業は、より戦略的なアプローチの必要性を認識しています。IT と OT の統合に関する課題の克服に役立つと考えられるアクションのトップ 3 を尋ねたところ、圧倒的に多かったのは、ビジネスおよび運用リスクの完全な評価を実施することでした（図 17）。今回の調査で提示された選択肢の中では、サードパーティの支援を求めることが後回しにされていることが顕著です。これはおそらく組織が、セキュリティ機能のアウトソーシング、特に細分化された方法でのアウトソーシングが決して特効薬ではないことを認識していることを示しています。

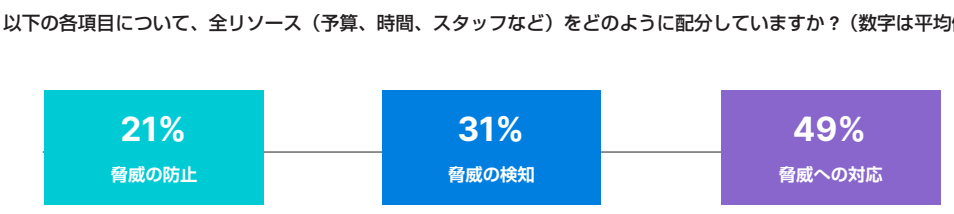


図 16：セキュリティのさまざまな側面に費やされるリソースのすべて

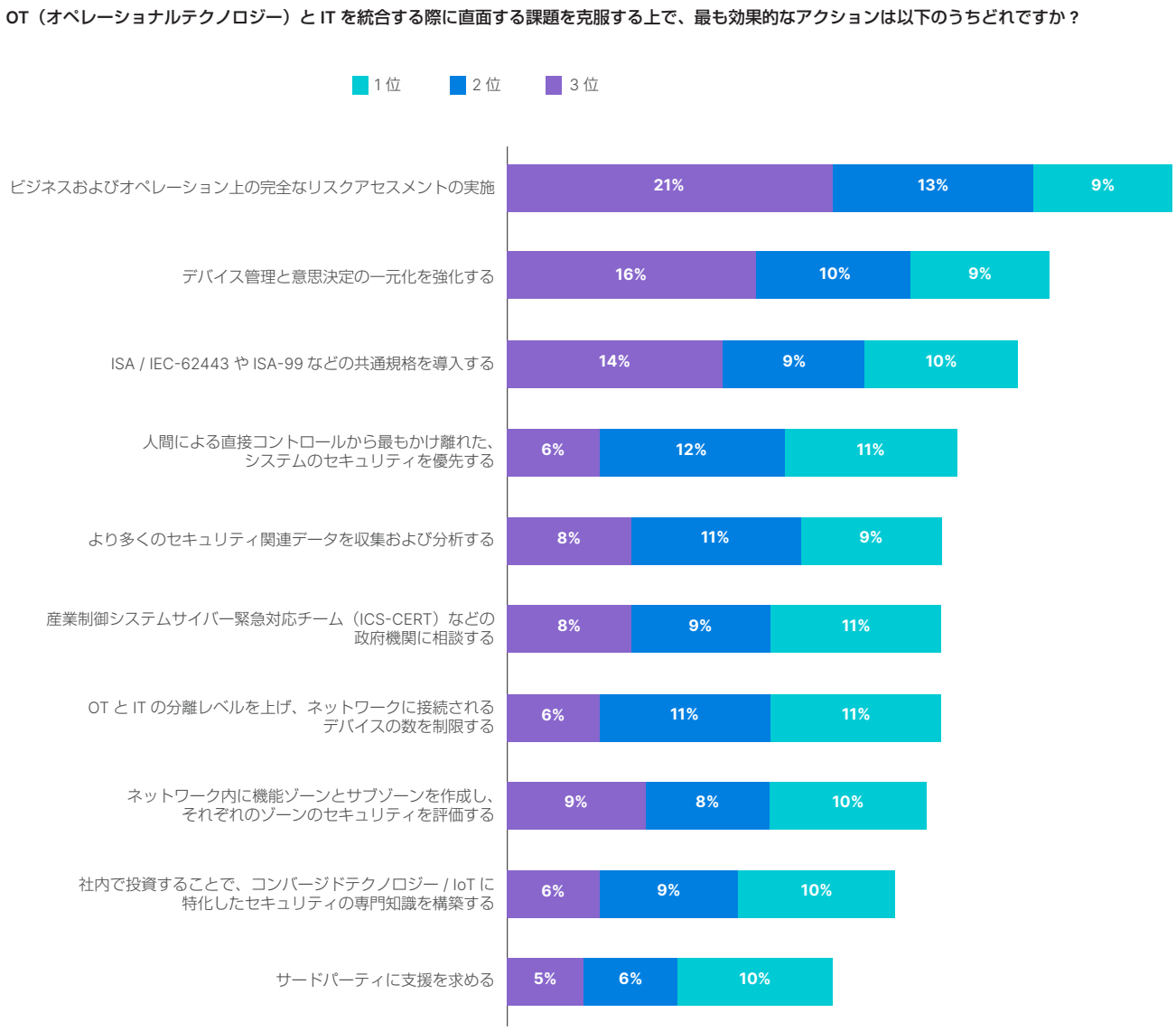


図 17：IT / OT 統合の課題に対処するための主なアクション

多くの組織が採用している OT セキュリティに対する場当たり的で消極的な姿勢を考えれば、そのような組織が頻繁にセキュリティイベントに見舞われていることは、おそらく驚くべきことではありません。全体では、58% の組織が過去 12 ヵ月の間に OT システムで少なくとも 1 回のセキュリティ侵害を経験しており（図 18）、このような侵害を受けたことがないと回答した組織はわずか 10% でした。IT および OT インフラストラクチャ全体を見ると、2 / 3 近く（66%）の組織が過去 12 ヵ月間にセキュリティ侵害を 4 回以上経験しています（図 19）。

これらの侵害の影響は、決して些細なものではありません。10 人の回答者のうち 6 人以上が、ICS および SCADA システムへの攻撃によって、コンプライアンス、財務、運用、さらには物理的な安全性に影響を受けたと報告しています（図 20）。

「季節的な変動や多種多様なターゲットにもかかわらず、データは 1 つのことを明確に示しています。つまり、OT システムに対する IT ベースの攻撃が増加している、ということです [6]」

ご存知の限りにおいて、組織の SCADA / ICS はセキュリティ侵害を経験したことがありますか？

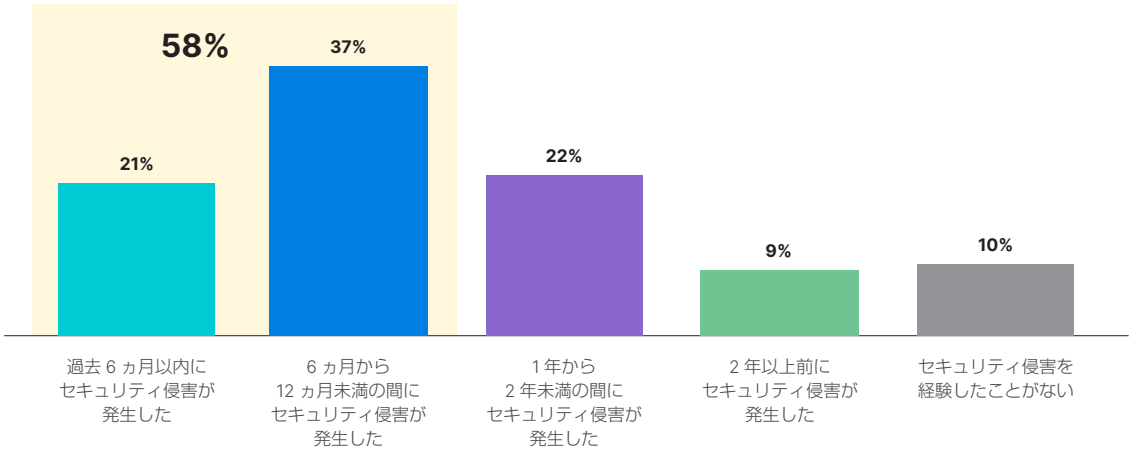


図 18：ICS / SCADA システムのセキュリティ侵害

過去 1 年間に何件のセキュリティ侵害が発生しましたか？

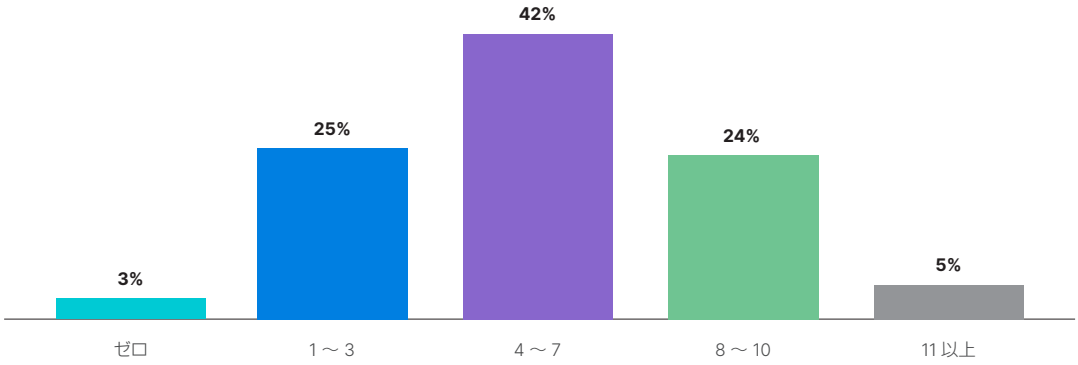


図 19：12 ヵ月間にわたる IT および OT システムのセキュリティ侵害

ご存知の限りにおいて、組織の SCADA / ICS に対するセキュリティ侵害により、以下のような影響がどれぐらいありましたか？

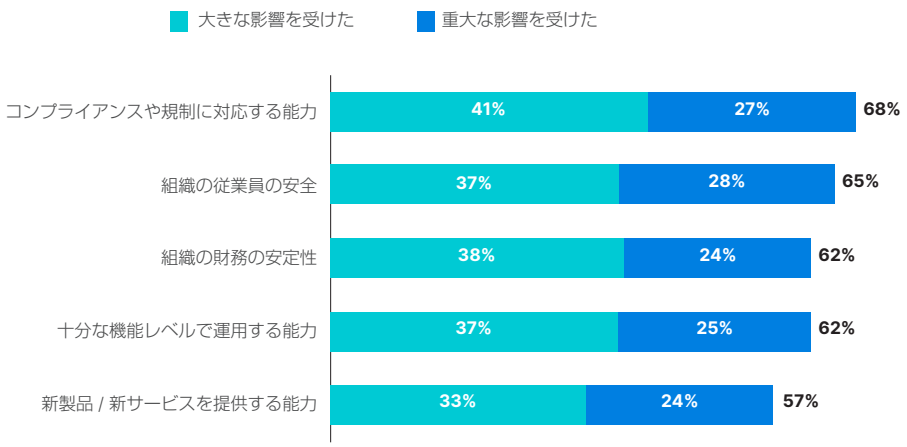


図 20：ICS / SCADA のセキュリティ侵害の影響

大手企業のベストプラクティス

前述のとおり、Forrester Consultingのアンケートの回答者の中には、侵害を防ぎ、リスクを最小化することに成功している組織もあります。実際、調査に回答いただいた組織の 58% が過去 12 ヵ月間に OT システムの侵害を少なくとも 1 回経験している一方で、2 年以上そのような侵害を経験しなかった組織は 19% に過ぎませんでした。

データをより詳細に分析するために、2 つのサブセット（サンプル中の「大手企業」と「中堅企業」の組織）のセキュリティ対策を比較しました。その結果、最近侵害を経験していない組織では、以下のようなベストプラクティスを実践している可能性が高いことがわかりました。

1. 大手企業では、ビジネスパートナーにネットワークアクセス権をほとんどまたはまったく付与していない可能性が 129% 高くなっています。

パートナーは、特定のリソースへのほぼリアルタイムのアクセスを必要とすることが頻繁にありますが、安全性に関する意識が最も高い企業ではそのようなアクセスを高度に制限している可能性が 2 倍以上高いです。おそらくそれを可能にするようなインテリジェントな方法でネットワークをセグメント化していると考えられます。

2. 大手企業は、政府機関に付与するアクセス権を厳しく制限する割合が 75% に達しています。

もちろん、地域や業界によって要件は異なりますが、知る必要性に基づいてデータへのアクセスを戦略的に制限している組織は、侵害の被害が少ない傾向にあります。

3. 大手企業では、IT サービスプロバイダーに適度なネットワークアクセス権しか付与していない可能性が 52% 高くなっています。

これらのサードパーティは、多くの場合、業務を遂行するためにかなりのアクセス権を必要としますが、一律にアクセスを許可するのではなく、厳格なアクセスポリシーを実施している組織のほうが、より良い結果が得られる傾向にあります。

4. 大手企業では、45% が高度なマルウェア検知をアウトソースしていない可能性が高いです。

一部の組織では、特定の機能を社内でより効果的に実行できる場合があり、侵害をうまく回避できた会社では、脅威の検知を社内システムに依存している傾向があります。

5. 大手企業では、36% がネットワーク分析と可視性をアウトソースする可能性が高くなっています。

十分に構築されたセキュリティオペレーションセンター（SOC）を持たない会社にとって、このような全体的な機能を、潤沢なリソースを有するパートナーに委ねることは、理にかなっていることが多いです。

終わりに

今回の調査では、重要インフラストラクチャの専門家の状況はさまざまです。一方で、OT システムの運用とセキュリティは、IT と OT の統合が遅れているか、停滞しており、セキュリティ対策が依然として断片的で場当たり的な方法で実施されているため、不安定な状態にあります。その結果、侵害が頻繁に発生するようになり、そのようなインシデントが企業の収益に大きく影響します。

その一方で、ICS および SCADA システムのセキュリティをビジネスのニーズに結びつけ、サイバーセキュリティのリスクを企業の全体的なリスクポートフォリオに統合するような、より戦略的なアプローチが必要であることが明確に認識されています。一部の組織では、特にサードパーティによるアクセスの分野で、この方向に大きく舵を切っており、その結果、侵害件数が減少する傾向にあります。

この肯定的な傾向が広まれば、IT から OT に至るまで、統合された企業の最小必要数にわたって、サイバーセキュリティに対するより包括的なアプローチが可能になると期待されています。この潜在的な変化が本格的に始動するにつれて、重要インフラストラクチャの専門家にとって、今後 2 年間で戦略や戦術がどのように進化していくのかが注目されます。

参考文献

[1] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019年5月8日（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.pdf

[2] 同上

[3] 「The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns」、Barbara Filkins 著、SANS Analyst Program、2018 年 7 月（英語）：
https://cdn2.hubspot.net/hubfs/2755567/White%20Papers%20and%20Briefs/Sans%20IIOT%20Survey.pdf

[4] 「Is Converging Your IT and OT Networks Putting Your Organization at Risk?」、John Maddison 著、Fortinet、2018 年 5 月 9 日（英語）：
https://www.fortinet.com/blog/industry-trends/is-converging-your-it-and-ot-networks-putting-your-organization-.html

[5] 「Six Cyber-Physical Attacks the World Could Live Without」、Elizabeth Montalbano 著、The Security Ledger、2017 年 1 月 18 日（英語）：
https://securityledger.com/2017/01/six-cyber-physical-attacks-the-world-could-live-without/

[6] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019年5月8日（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.pdf

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-Forrester-IT-OT-Covergence-202108-R1