FTI CONSULTING

CISOの再定義:
Cクラスの認識と期待を読み解く

リスクを限定し、サイバーセキュリティのコミュニケーションギャップを解消する

はじめに *Meredith Griffanti* - シニア・マネージングディレクター
サイバーセキュリティ&データプライバシーコミュニケーションズ　グローバル責任者

当社のサイバーセキュリティ&データプライバシーコミュニケーションズのチームがグローバルに拡大し続けるなか、私は多くの国でサイバーセキュリティおよびビジネス部門のエグゼクティブと時間を過ごす機会がありました。彼らの企業は拠点を構える場所によって、ビジネスのやり方や、文化とコミュニケーションの規範が大きく異なります。この「CISO（最高情報セキュリティ責任者）再定義」調査は、当社のチームがサイバーセキュリティのガバナンスと管理に共通する難しい課題と考えているものを明らかにしています。企業がどの地域で事業を展開しているかにかかわらず、CISOは取締役会やCクラスの経営幹部と、適切に、自信を持ってコミュニケーションを取ろうと苦労しています。

サイバーセキュリティが、グローバルに展開する企業のリスクとガバナンスの最重要課題であり続けていることを踏まえて、すべての取締役、Cクラスの経営幹部、CISO（最高情報セキュリティ責任者）がこの調査を読んで、共通の基盤を見つける方法と、コミュニケーションや認識のずれがどこにあるのかを、より理解してほしいと思っています。サイバーセキュリティについては取締役会とCクラスの「レベルアップ」を求める声も多いですが、FTIコンサルティングの「Secure Your Seat」プログラムのようにCISOに特化したトレーニングの機会を求めることも、リスクを限定し、サイバーセキュリティに関するコミュニケーション
のギャップを埋める重要な要素です。

当社のデジタル&インサイツのチームが実施したこの調査が、組織の行動を促すことを願っています。

概要

サイバーセキュリティの脆弱性がもたらすリスクは、かつてないほど高まっています。シニアエグゼクティブ【上級経営幹部】がこれまで以上に、規制当局や投資家、その他のステークホルダーからサイバーセキュリティのリスクに関する説明責任を求められているなか、FTIコンサルティングはCISO（最高情報セキュリティ責任者）と情報セキュリティのリーダーを対象にその役割、リーダーシップ、業務に対する重圧の高まりを調べました。今回はそれをもとに、Cクラスの経営幹部のCISOに対する認識と期待を理解するための調査を行ないました。最初の調査ではCISOと経営幹部のコミュニケーションのギャップが明らかになりましたが、今回の一連の発見は、経営幹部のほうがそのギャップをより強く感じていることを示唆しています。

パート 1: 2022年CISO調査・概要

調査手法:

対象： **CISO165人**　　地域： **アメリカのみ**

主な結果：

- 内部および外部からの監視が強まっている。
- CISOはサイバーセキュリティの優先事項について、上級幹部とのコミュニケーションにずれがあると報告した。
- CISOは内部の上級幹部とのコミュニケーションが難しいと回答した。
- CISOは取締役会の説明において、実情より好ましい印象を与えようとしていると主張した。

パート 2: 2024年Cクラスの経営幹部の調査・イントロダクション

調査手法:

対象： **Cクラスの経営幹部 787人**　　**地域：世界５大陸**

主な調査項目：

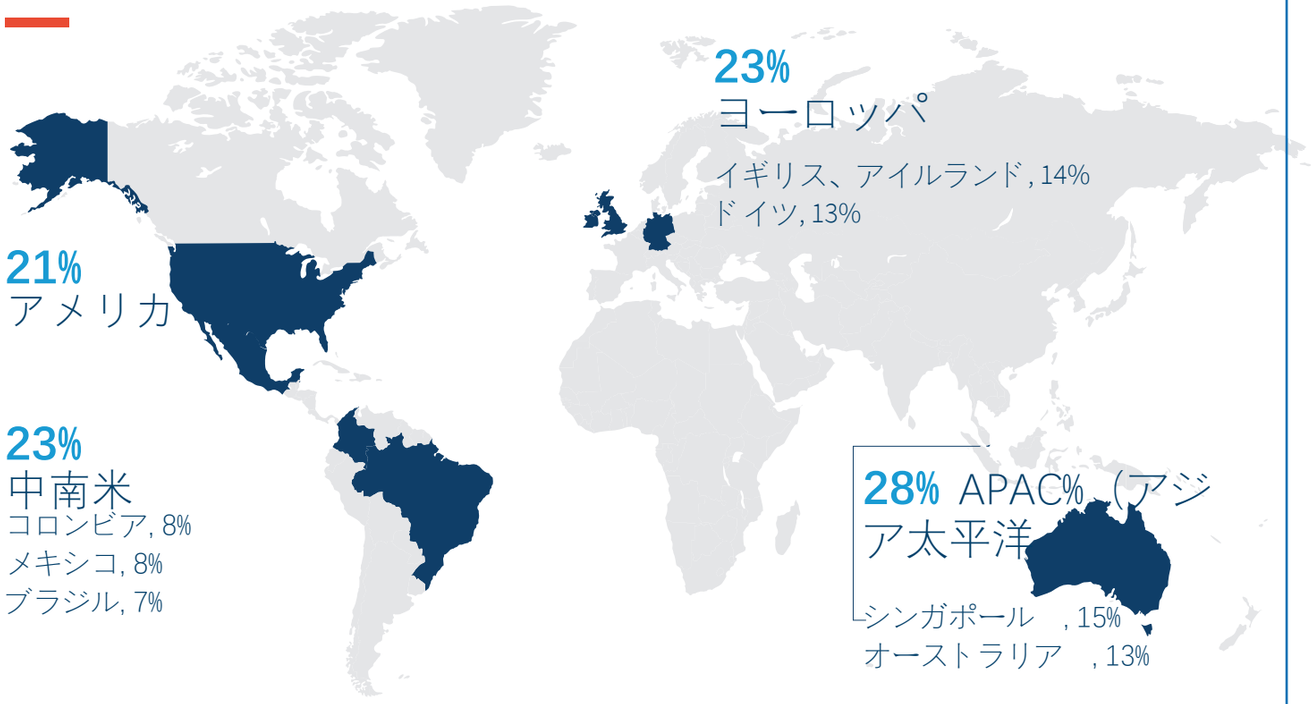
- 経営幹部はCISOと同じようにコミュニケーションのずれを感じているか? このギャップはより顕著か?
- 共通する食い違いがあるか?
- 経営幹部は重要なサイバーセキュリティの優先課題についてどのように考えているか?
- 追加のトレーニングは必要か?

CISOs ——— CSIOとリーダーシップのコミュニケーションのずれ ——— Cクラス

グローバルな調査手法

FTIコンサルティングのデジタル＆インサイツ・チームは当社の主要産業において、従業員500人以上の企業のCクラスの経営幹部 n=787（サンプル数787人）を対象に、2023年11月にオンラインで調査を実施しました。先行調査[1*] はCISO n=165（サンプル数165人）を対象に実施しました（本レポート内の【カギのようなマーク】の項目）。調査方法に関する質問は James.Condon@fticonsulting.com までお問い合わせください。

地域



業種

18% 小売業

14% 工業

13% ヘルスケア　ライフサイエンス（HCLS）

13% 金融サービス

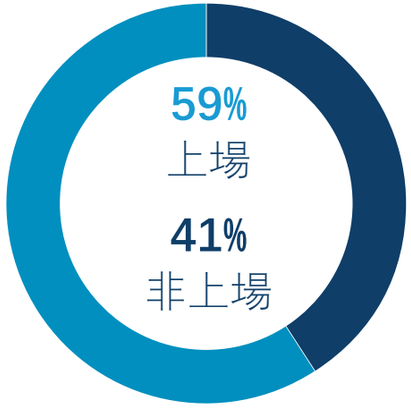
13% テクノロジー・メディア・通信（TMT）

12% 企業広報・ガバメントリレーションズ（PAGR）

11% エネルギー（ENR）

5% その他

上場 / 非上場



職位

19% CEO（最高経営責任者）

10% VP（バイスプレジデント）

23% CFO（最高財務責任者）

21% その他のCクラス

27% ディレクター / マネジャー

年間収益

21兆5,000億ドル
収益（総計）

270億ドル
平均収益

従業員数

369 万人
従業員数（総計）

4,700人
平均従業員数

[1*]"CISO Communications Redefined," FTI Consulting (2022), https://fticommunications.com/ciso-communications-redefined/

主な洞察

CISOへの期待が高まる一方で、企業は依然としてサイバーセキュリティの脅威に対して脆弱です。

インシデントは増加しており、回答者の**10人に9人が過去**12カ月間にサイバーインシデントを経験しています。

87%の経営幹部が過去12カ月間にCISOの意思決定の責任を強化したと回答しており、サイバーセキュリティの脅威が進化していることを考慮していると見られます。

CISO はリーダーシップとのコミュニケーションについて十分な準備ができていません。

上級経営幹部の**3人に1人は**、自社のCISOが経営陣に対して潜在的な脆弱性への注意喚起をためらっていると感じています。同じような割合の人が、CISO が実際の状況より楽観的に見せようとしていると考えています。

経営幹部の**10人に約4人**が、自社のCISOが社内外の主要なステークホルダーとのコミュニケーションについて十分な準備ができていないと感じています。リーダーシップとのコミュニケーションについては、3 分の1以上の人が十分な準備ができていないと感じています。

CISOは重要なリーダーシップスキルを経営幹部に示そうとして苦労しています。

経営幹部の31%が、CISOが用いる技術的な概念を十分に理解していません。

経営幹部の62%が、CISOの直接的なコミュニケーションスキルが自分の期待以上ではないと回答しています。

CISOの58%が、上級幹部が理解できるように専門用語を説明することに苦労しています（2022年のCISO調査より）。

CISOの66%が、上級幹部に自分たちの役割を理解してもらうことが難しいと感じています（2022年のCISO調査より）。

経営幹部はCISO向けのコミュニケーションのトレーニングプログラムを支援しており、多くの人が緊急のニーズだと言及しています。

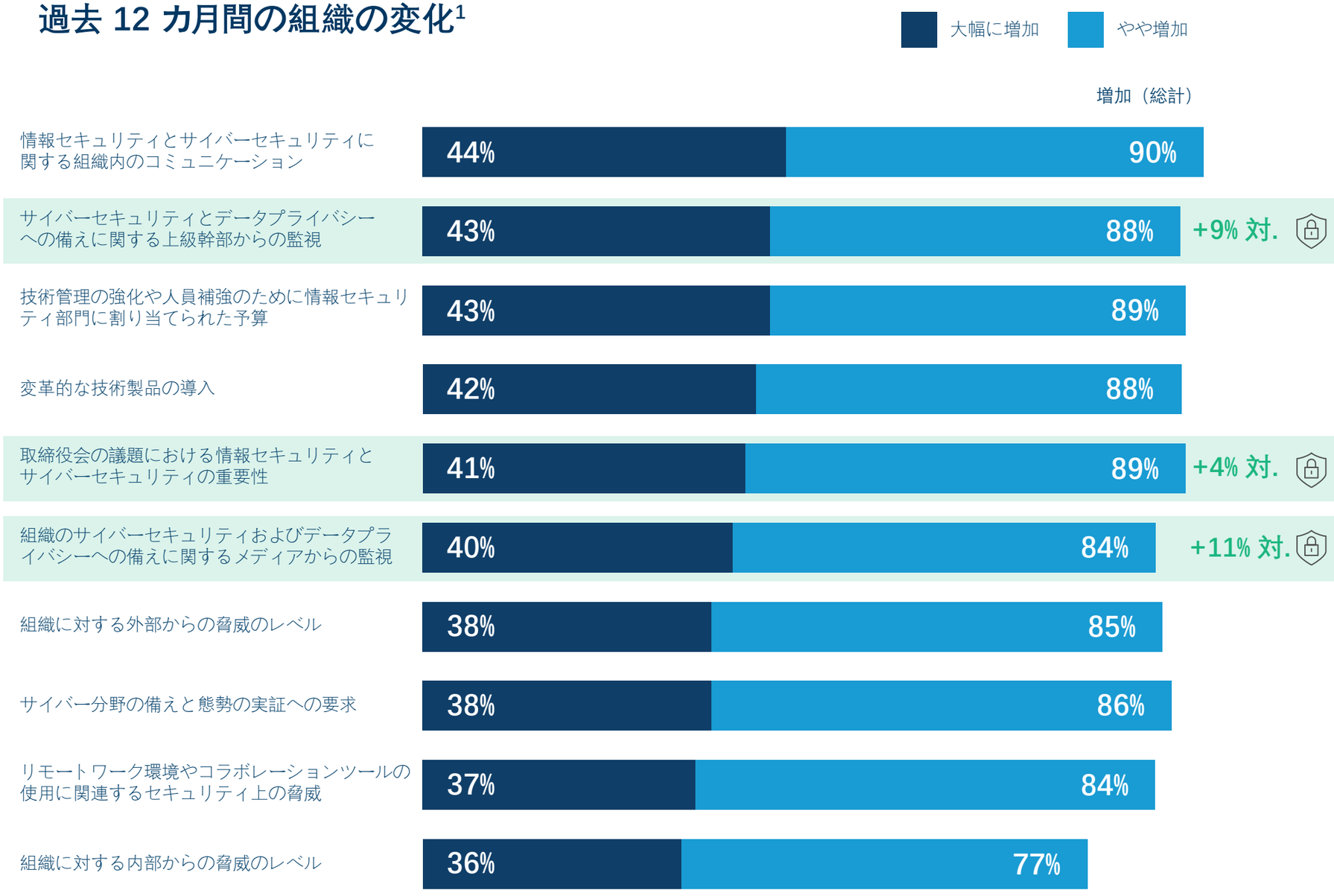
経営幹部の98%が、CISOのコミュニケーションやプレゼンテーションのトレーニングへの資金拠出に賛同しています。

経営幹部の45%が、特に従業員2,500人以上の企業では、緊急のニーズだと回答しています。

経営幹部はトレーニングで特に取り組むべき課題として、**脅威の予測、従業員の認識を高めること、ROI（投資利益率）の説明、サイバーリスクを挙げています。**

インシデントが増加するにつれて、あらゆる方向からの監視や圧力が高まり、組織はサイバーセキュリティを優先することを余儀なくされ、CISOの役割が注目されています。

過去 12 カ月間の組織の変化[1]



[1]FTIの2002年の調査CISO Communications Redefined （サンプル数165人）より集計。https://fticommunications.com/ciso-communications-redefined/

情報セキュリティとサイバーセキュリティは2024年のCクラスの最優先事項です。

94%の経営幹部が過去12カ月で情報セキュリティの重要性が高まったと回答しており、過半数の人がサイバーセキュリティを重要または高い優先事項と考えています。

興味深いことに、この数字は2022年10月の調査で同様の回答をしたCISOの割合より多く、CISOの調査では、取締役会の議題において情報セキュリティとサイバーセキュリティの重要性が高まっていると回答した人は85%にとどまりました。しかしながら、Cクラスの経営幹部とCISOの双方が、サイバーセキュリティ プログラムに対する内外の圧力の高まりを強く感じていることは明らかです。注目すべきことに、組織の優先順位についてさらに詳しく見ると、サイバーセキュリティは顧客体験 顧客満足度より6%高く評価されています。

このような圧力は、脅威の進化、規制、サイバーセキュリティ インシデントの顕在化、取締役会レベルからの注目とサイバーセキュリティ プログラムの優先度、さらにはメディアやステークホルダーのグループなど外部からの監視によるものと考えられます。

実際、Cクラスの経営幹部は、2022年に調査したCISOの意見と比べて、サイバーセキュリティの備えについて上級幹部、取締役会メンバー、メディアからの監視が一層厳しくなっていると認識しています。

94% が、過去12カ月で情報セキュリティの重要性が高まっていると回答しています。

サイバーセキュリティの優先度

組織の最優先事項

1. **39%** 情報セキュリティとサイバーセキュリティ
2. **36%** 業務の効率化とプロセスの最適化
3. **33%** 顧客体験 顧客満足度
4. **32%** サプライチェーンの最適化とベンダーの管理
5. **31%** ESG（環境 社会 ガバナンス）の取り組み

サイバーセキュリティ予算が増えるにつれて、CISO は投資対効果 (ROI) を明確に伝えることを期待されています。

サイバーセキュリティのリスクレジスター策定が進むにつれ、上級幹部はサイバーセキュリティ プログラムへの投資が大幅に増えると予想しています。適切なITインフラの整備、従業員トレーニングプログラムの実施、インシデント対応計画やプロジェクトの準備、上級幹部のトレーニングを通じて組織としてサイバーセキュリティ インシデントに備えることなど、幅広い分野で投資が増える見込みです。

特に注目すべきことに、サイバーセキュリティ予算は今後1～2年間で平均23%増加し、今後3～5年間では現在より36%増加すると経営幹部は予想しています。

投資の強化はCISOにとって間違いなく歓迎すべきことですが、組織のサイバーセキュリティ戦略と、そこにおけるCISOの役割に対する監視の目が厳しくなる可能性が高いでしょう。上級幹部と取締役会の期待に沿って投資が的確に配分されるように、そして、この投資の結果を、上級幹部の共感を得られるようなビジネス上の実際の成果に結びつけられるように、CISOは上級幹部と連携する必要があります。

特に、従業員のトレーニングとセキュリティ意識向上のプログラムは、組織が今年【2024年に】取り組むべき最優先事項の2番目に挙げられています。Cクラスの経営幹部は自社の情報セキュリティチームに対し、内部での情報の共有に時間と資金を投じることを期待しているのです。

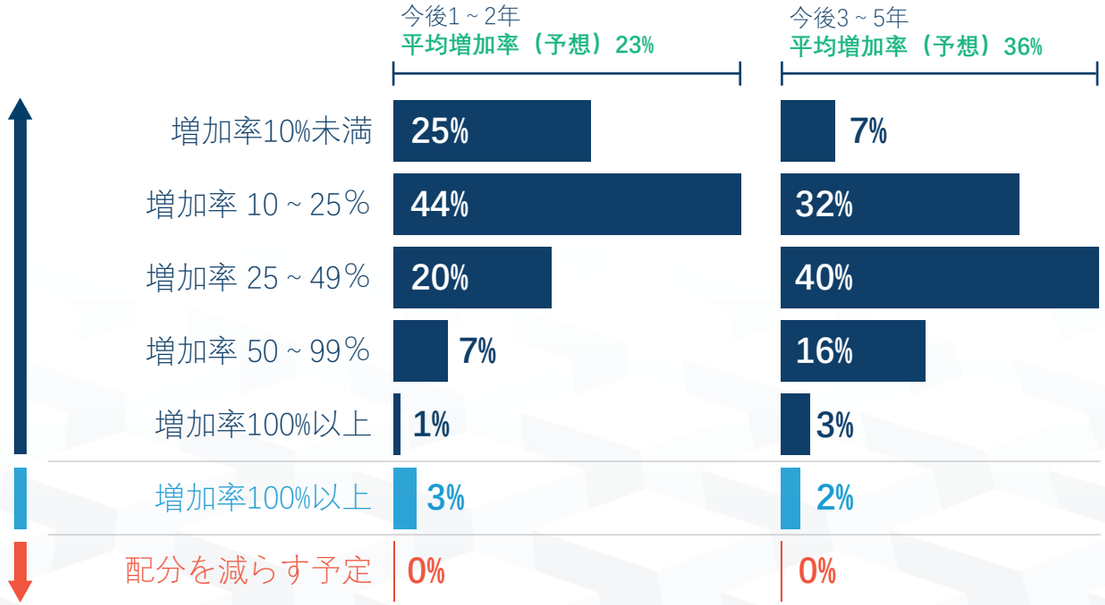
「組織にとってサイバーセキュリティの優先順位が高まり、関連支出が増えるのに伴い、CISOは舞台裏から最前線に出てくることを求められています。」

Orla Cox
シニア ディレクター
サイバーセキュリティ&データプライバシー コミュニケーションズ

期待される投資

1. **43%** ITインフラの更新またはアップグレード
2. **42%** 従業員トレーニングおよびセキュリティ意識向上プログラム
3. **40%** 事業継続と災害復旧、インシデント対応、危機コミュニケーションの計画の更新
4. **38%** サイバー危機の備えに関する評価および卓上演習またはシミュレーションの実施
5. **37%** 上級幹部チームが予想外の危機を管理するための準備

予算増額の見込み



サイバーセキュリティの監視が強化され、予算が増えるにつれて、CISOはサイバーリスクとそれを軽減するための戦略的計画をより明確に説明することを求められていますが、多くの場合は不十分です。

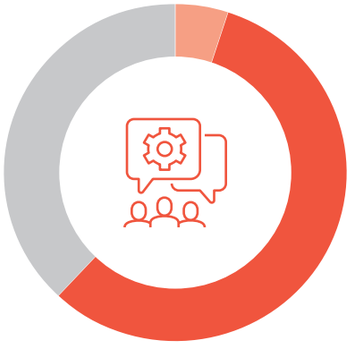
予算の増加、CISOの責任の拡大、サイバーセキュリティに対するリーダーシップの監督強化が相まって、Cクラスの経営幹部はサイバーセキュリティ プログラムのROI（投資対効果）がより可視化されることを望んでいます。

しかし、多くの経営幹部は、自社のCISOがROIの説明に苦労していると感じています。彼らがおそらく現実が示唆するより楽観的な評価をしていて、自分たちの計画をより広いビジネス領域で共有できる言葉でわかりやすく説明できずにいると考えています。

経営幹部の3人に1人は、CISOが説明に使う技術的概念を十分に理解しておらず、サイバーセキュリティに関する直接的なコミュニケーションのレベルが自分たちの期待に見合わないことを示唆しています。

2022年の調査で判明したとおり、CISOの66%は、組織における自分たちの役割を上級幹部が十分に理解していないと考えています。つまり、CISOの側も、理解をめぐるこうしたギャップを意識しているようです。特に、関連予算の増加に伴い、この食い違いはCFO（最高財務責任者）のあいだで最も強く見られました。

CISOに対する期待は高まっていますが、リスクの受容、サイバー投資のリターン、セキュリティの成熟度に関する長期戦略計画の進捗状況などの概念の説明は複雑で、漠然としたものになりやすいでしょう。しかし、これらを理解することは、幹部にとっても取締役会にとっても重要です。したがって、CISOがコミュニケーションのスキルを磨き、取締役会に向けて四半期ごとに簡潔で明瞭なプレゼンテーションを行って、最新の情報を提供する必要性がさらに高まっています。

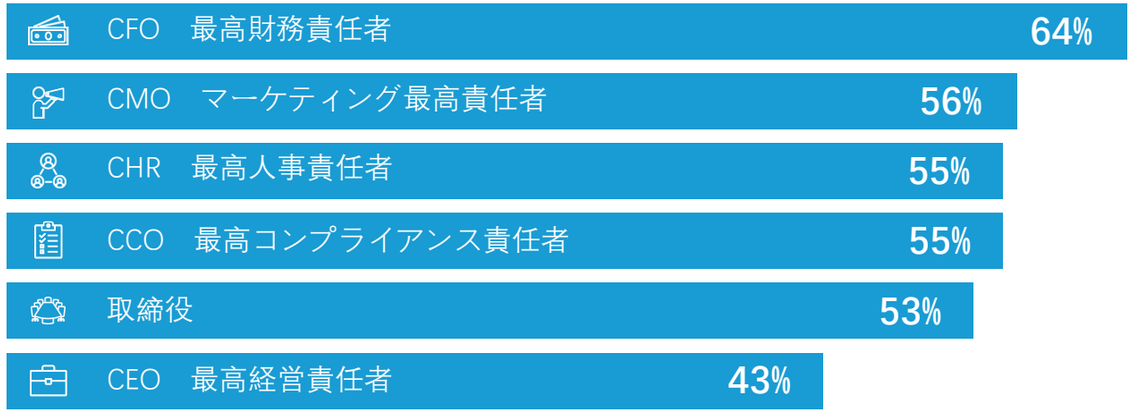


62%
CISOからの直接コミュニケーション**が期待以上ではない**

▲ 中南米　65%

31%
CISOが説明する技術的概念を**十分に理解していない**

CISOの役割を十分に理解していない経営幹部



CISOは経営幹部から期待されている重要なリーダーシップの能力を、十分に示すことができていないようです。彼らは社内外の関係の管理に苦労していますが、そうした力学は組織の収益や評判に直接影響する場合もあります。

CISO がより大きな責任を与えられ、ビジネスリーダーとしての期待が高まるにつれて、企業の内外でCISO の認知度と影響力を高めるために、組織としてトップダウンでサイバーセキュリティの「文化」を構築することが強く求められています。

経営幹部によると、CISOに必要な特性の上位 5つのすべてがリーダーシップの資質に集中しており、さらに5つのうち4つは、コミュニケーションに根ざす重要な能力をCISOが活用する必要性を明確に定義しています。ただし、経営幹部は自社のCISOがリーダーシップや組織全体にとって目に見える存在になることを望んでいるにもかかわらず、CISOが現在最も苦戦しているのはこれらのスキルセットです。

経営幹部の36％が自社のCISOに対外的な関係の構築と管理に長けていることを期待する一方で、2022年の調査ではCISOの52％が、インシデントに対応する際に社内外のステークホルダーとのコミュニケーションを管理することが最も難しいと主張しています。コミュニケーションにおけるこの食い違いは、突き詰めれば、インシデントの発生前、進行中、発生後に社内外の関係を管理することの重要性と価値を強調しています。

さらに、経営幹部の36%がCISOに社内での関係の構築と管理を期待していますが、一方で23%の人が、情報セキュリティに対するアプローチがサイロ化していると考えています。この「サイロ化」した考え方は、誤った情報につながり、組織全体のサイバーセキュリティを混乱させ、コミュニケーション不足を引き起こしかねません。

全体として、今日のCISOは単なる技術の専門家ではなく、ビジネスリーダーとしてその役割に取り組まなければなりません。

CISOに必要な特性

1. **45%** セキュリティ関連の予算とリソースを効果的に管理する
2. **38%** 専門用語を速やかにわかりやすい用語に置き換えられる
3. **38%** 危機的状況で熟練したリーダーシップをとる
4. **36%** 外部との関係の構築と管理に精通している
5. **36%** 内部の関係を構築して維持できる

「今日のリスク情勢と、新たな規制と、厳しくなる監視の最中で、CISOは進化する役割の新たな要求に応えるために、ビジネス中心のスキルセットを習得する必要があります。」

Jamie Singer
シニア　マネージングディレクター
サイバーセキュリティ＆データプライバシーコミュニケーションズ　共同責任者

経営幹部はサイバーセキュリティのリーダーと戦略的な連携が取れていないと感じており、それが組織的なリスクをさらに高めています。

意思決定の権限が強化され、予算が拡充され、CISOがリーダーシップの役割を担うことが期待されているにもかかわらず、Cクラスの経営幹部の回答者は半分近くが、自分たちのリーダーシップの優先順位と、情報セキュリティおよびサイバーセキュリティ部門のリーダーシップの優先順位が完全に一致していると考えていません。そしてCISOの53%も、自分たちの優先順位が上級幹部の優先順位と完全に一致していないと回答しています。

さらに、2022年の調査ではCISOの82%が、取締役会ではポジティブに誇張する必要性を感じると主張しています。興味深いことに、調査対象の経営幹部の31%も、この点がCISOの最大の課題であると認識しています。これはおそらく、サイバーセキュリティと情報セキュリティのリーダーがリスクを適切に伝える方法を知らず、自分たちのプログラムに悪い影響を与えることを恐れているからでしょう。

さらに、経営幹部の30%は自社のCISOが組織の脆弱性をめぐる懸念を提起することをためらっていると感じており、その結果、サイバーセキュリティ　プログラムの内部に懐疑論が蔓延しています。

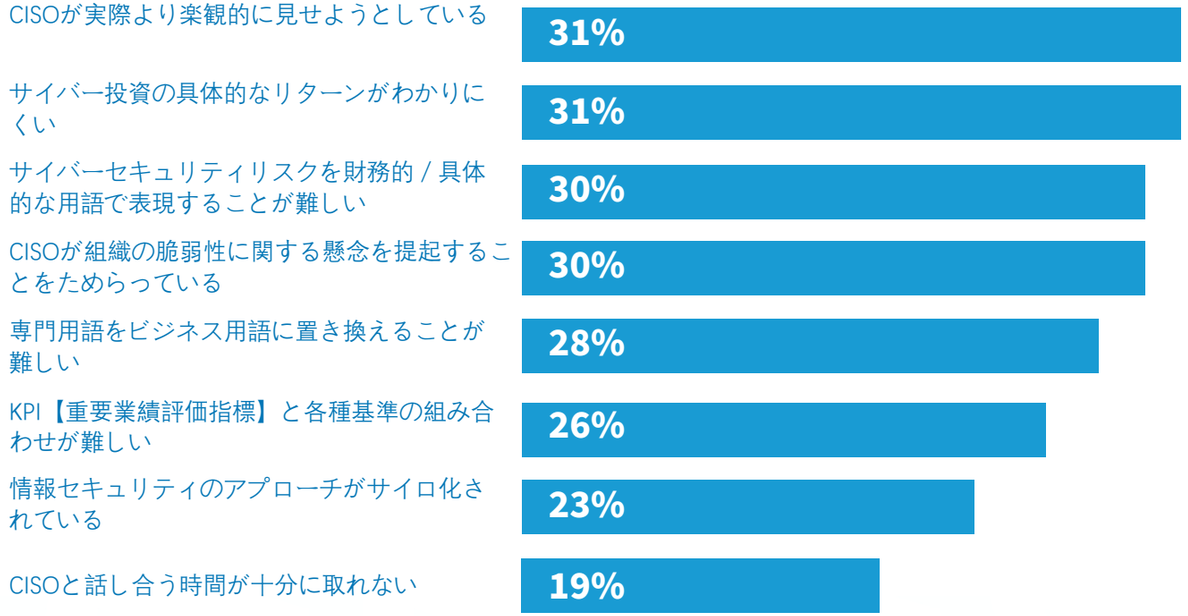
このような食い違いや、サイバーセキュリティのリスクを適切に伝えることができないこと、そして伝えるのをためらうことは、組織にとって重大な課題です。規制当局やその他のステークホルダーが上級幹部にサイバーセキュリティの説明責任を求める声が高まるなか、組織のサイバーリスクのレベルを明確かつ正確に把握して、それを管理するために適切な方策を講じることが、極めて重要になります。経営幹部とCISOの双方が優先順位の食い違いを認めていますが、多くの組織はこのずれに対処する計画を具体化できずにいます。

組織の優先順位とサイバーセキュリティ対策

46%
の経営幹部がCISOと完全に連携できていないと感じている

53%
のCISOが経営陣と完全に連携できていないと感じている

共通の課題



「CISOが現実より楽観的なイメージを描きがちなことはよくあります。これは大きな問題です――企業のリーダーシップは、自分たちが直面しているサイバーリスクを正確に理解しなければなりません。それができなければ、組織の効果的なガバメントが働かず、情報漏えいが発生してから初めて気づくことになります。」

Meredith Griffanti
シニア　マネージングディレクター
サイバーセキュリティ＆データプライバシーコミュニケーションズ　グローバル責任者

興味深いことに、CISOとCクラスの経営幹部の双方が、組織内でCISOの役割が直面している認識の食い違いと課題を認識しています。

CISOが上級幹部とのコミュニケーションで感じている課題

66%
上級幹部が組織におけるCISOの役割を十分に理解していない

82%
取締役会では実際より好ましく見える説明をしなければならない

58%
上級幹部が技術的な言葉を理解できるように伝えるのに苦労している

上級幹部がCISOとのコミュニケーションで感じている課題

30%
CISOはサイバーセキュリティのリスクを財務的 / 具体的な用語で表現するのが難しい

31%
CISOは状況を実際より楽観的に説明している

31%
サイバー投資の具体的なリターンがわかりにくい

28%
CISOは専門用語をビジネス用語に置き換えるのに苦労している

30%
CISOは組織の脆弱性に関する懸念の提起をためらっている

19%
CISOと話し合う時間が足りない

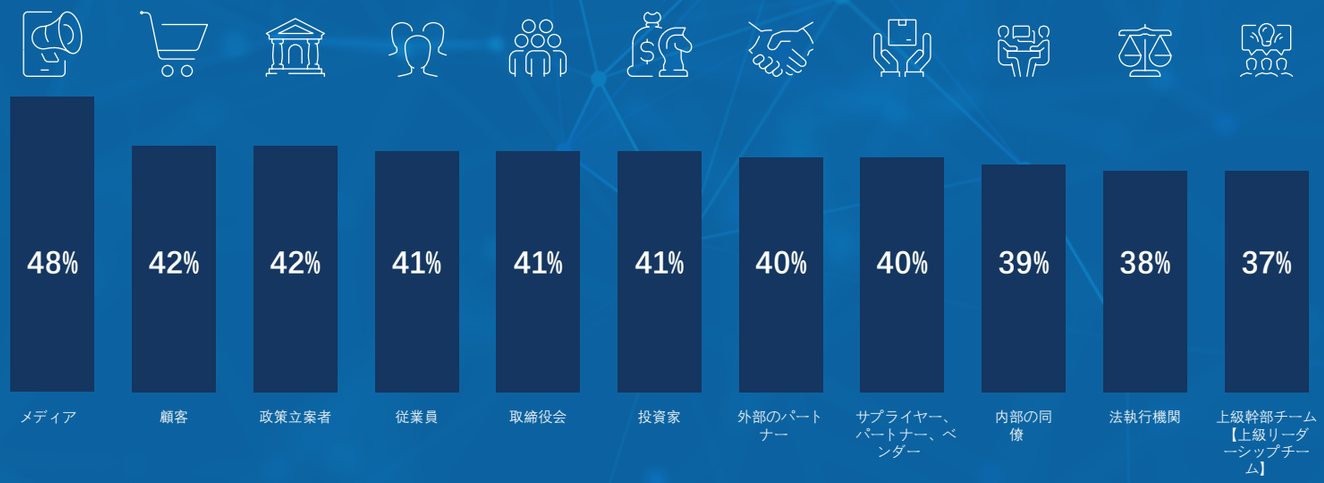
同時に、多くの経営幹部が、CISOは取締役会や経営陣とコミュニケーションを取る準備が十分ではないと感じています。

サイバーインシデントが発生した際に、CISOは自社にとって最も重要な社内外のステークホルダーとコミュニケーションを取る準備が完全にはできていないと、多くの調査対象の経営幹部が考えています。特に、インシデントに関する企業の対応を代弁し、組織の収益に直接影響を与えるような意見を提供する幅広い領域の重要なステークホルダーについて、準備不足を指摘しています。今日の状況で、CISOはビジネスリーダーへと進化して新しいスキルセットを習得することを求められていますが、彼らがビジネスに重大な影響を与える可能性のある重要なステークホルダーとコミュニケーションを取る準備ができているとは、経営幹部は基本的に考えていません。

経営幹部はさらに、差し迫った問題を法執行機関や政策立案者に効果的に伝えるための準備不足を指摘しています。

このように新たな意思決定の権限を得た今、CISOにとって、対応策や意思決定の要点を明確にし、経営陣の質問に答えること、特にインシデントが進行している最中の行動に関する質問に答えることが、非常に重要になっています。CISOと彼らが取締役会にサイバーセキュリティの助言をする役割に対し、規制当局が批判的な見方を強めるにつれて、この問題は今後数年間でさらに大きくなるでしょう。リスクと脆弱性を認識することも彼らの仕事ですが、問題を解決できないときや、場合によって社内で十分な問題提起ができないと、CISOと組織の経営陣【リーダーシップチーム】にはその役割ゆえの責任が生じます。これは、顧客の減少や収益の損失、法的措置、組織の評判に対する永続的な損失など、ビジネスに多大な結果をもたらしかねません。

ステークホルダーとのコミュニケーションに対する準備の課題



「Cクラスがコミュニケーションに期待することとCISOの業務上の現実とのあいだには、明確な軋轢があります。CISOは企業のスポークスパーソンとしての役割を求められていますが、彼らの多くは単にその準備ができていません。」

James Condon

マネージングディレクター

リサーチ、デジタル＆インサイト　責任者

このように認識されているコミュニケーションのずれを解消し、その結果生じる組織のリスクに対処するために、経営幹部はCISOのコミュニケーションやプレゼンテーションのトレーニングに対する投資の強化に賛同しています。これらの領域は組織のサイバーセキュリティ対策の一環として、CISOに早急に求められていることであると、経営幹部の多くが考えています。

責任と期待が高まるにつれて、経営幹部は自社のCISOに投資し、サイバーセキュリティをめぐる社内の円滑なコミュニケーションを促して収益に影響を与えるようなトレーニングプログラムを支援することに、より積極的になっています。

このような問題への対処を間違えるとビジネスにより大きな影響を及ぼしかねないため、回答者のほぼ全員が、CISOのコミュニケーションとプレゼンテーションのトレーニングの資金を増やすことに賛同しており、半数近くが緊急のニーズと位置付けています。

現在のところ、経営幹部は、より良いコミュニケーションの手法や、ステークホルダーのリスクの定量化を重視するなど、専門的なトレーニングで対処できる大きな溝もいくつかあると考えています。CISOの役割が進化し続けるなか、CISOはサイバーセキュリティの社内の提唱者としても、社外に向けたスポークスパーソンとしても、コミュニケーションに対する責任を負っています。

経営幹部は、サイバーリスクと投資のリターンを定量化する能力がサイバーセキュリティの責任者に求められるスキルセットであることを理解しており、CISOを成功に導きたいと考えています。コミュニケーションのトレーニングやコーチングは、CISOの人生をスムーズにするだけでなく、ひいては会社に成功をもたらし、よりスマートで迅速な意思決定につながるでしょう

98% の経営幹部がCISOのプレゼンテーションとコミュニケーションのトレーニングへの投資の強化に賛同している

サイバーセキュリティの優先度

- 45% 直ちに必要
- 44% いずれ必要になる
- 11% 必要ではない

55% APAC（アジア太平洋）
37% アメリカ
48% 従業員2500人以上
40% 従業員2500人未満

CISOのコミュニケーションのトレーニングで重要なテーマ

1. **31%** 将来のサイバー脅威とトレンドを予測して影響を弱める戦略
2. **27%** 従業員のセキュリティ意識向上のトレーニングのための共同アプローチ
3. **27%** サイバーセキュリティのリスクを定量化してステークホルダーに伝える方法
4. **27%** 技術情報を明確かつ正確に伝えるためのガイダンス
5. **26%** 積極的で適応力のあるサイバーセキュリティの文化を構築するプローチ

「［情報漏洩において］最大の味方はコミュニケーションと選択肢です。コミュニケーションとは、物事の状況を説明して、全員を確実に同じ方向へ進ませることができる能力です。規制当局に現状と計画を伝えることができ――同時に顧客を安心させて、反対側に舵を切ってもだいじょうぶだと確信させることです。」

Evan Roberts
シニア・マネージングディレクター
サイバーセキュリティ＆データプライバシーコミュニケーションズ　共同責任者

FTIのCISOコミュニケーション・トレーニングプログラムを通じて、コミュニケーションギャップの解決に投資してください

SECURE YOUR SEAT

COMMUNICATIONS TRAINING PROGRAM

FTI コンサルティングのデータプライバシーおよびサイバーセキュリティコミュニケーションズのプラクティスは、サイバーセキュリティの複雑な問題に対処し、理解しやすい概念に分解するという比類ない能力を備えています。多くのCISOはインシデントが発生した後に、四半期ごとの取締役会でのプレゼンテーションや一般的なコミュニケーションスキルを磨き、会社のリーダーシップとより共鳴できるようにしたいと考えて、私たちに継続的な支援を求めます。私たちはCISOのために独自に開発した研究主導のコミュニケーションおよび取締役会対策のトレーニングプログラム「Secure Your Seat (SYS)」を立ち上げ、当社のサイバーセキュリティとコミュニケーションの専門性をCISOの皆さんに大いに活用してほしいと願っています。

6週間のプログラムでは、カスタマイズされた週1回の1対1のトレーニングセッションを通じて、上級幹部とのコミュニケーションを改善し、取締役会の期待に応え、専門用語やKPI【重要業績評価指標】をわかりやすい言葉に置き換えて、四半期および年次の取締役会でのプレゼンテーションを強化します。さらに、1対1のメッセージングとプレゼンテーションのトレーニングを受けて、サイバーセキュリティの専門知識を持つCクラスの経営幹部と現職取締役で構成される多彩な顔ぶれのアドバイザリーカウンシルの前で、取締役会のプレゼンテーションの練習をすることができます。

Secure Your Seat: CISOコミュニケーション・トレーニングプログラムの概要

- 改善が必要な分野を特定するための調査
- 目標設定
- ブランド分析
- パブリックスピーキング
- メッセージの洗練とプレゼンテーションの実践ワークショップ
- 四半期 / 年次の取締役会で提示するサイバー関連資料の強化
- 取締役会に適した職務経歴書の準備【Board-Ready Curriculum Vitae】
- 模擬プレゼンテーションとフィードバック　セッション（SYSアドバイザリーカウンシルの前で行う）

Secure Your Seatの詳細は **SYS@fticonsulting.com** および担当チームのメンバーにお問い合わせください。

「FTIのSecure Your Seat Programは、サイバー分野のコミュニケーションに精通している世界トップクラスの専門家チームが運営しています。新任のCISOも、私のようなベテランのCISOも、サイバーセキュリティの目標とリスクと機会を組織の最上級幹部に説明できるサイバーセキュリティのリーダーを育成するために、このプログラムが不可欠です。」

Jesse Whaley

アムトラックCISO

CISOの再定義:
Cクラス幹部の認識と期待をナビゲートする

MEREDITH GRIFFANTI
シニア　マネージングディレクター
サイバーセキュリティ&データプライバシーコミュニケーションズ　グローバル責任者
meredith.griffanti@fticonsulting.com

EVAN ROBERTS
シニア　マネージングディレクター
サイバーセキュリティ&データプライバシーコミュニケーション　共同責任者
evan.roberts@fticonsulting.com

JAMIE SINGER
シニア　マネージングディレクター
サイバーセキュリティ&データプライバシーコミュニケーション　共同責任者
jamie.singer@fticonsulting.com

JAMES CONDON
マネージングディレクター
リサーチ、デジタル&インサイト　責任者
james.condon@fticonsulting.com

CLEMENTINE BOYER
シニア　ディレクタ
サイバーセキュリティ&データプライバシー　コミュニケーションズ
clementine.boyer@fticonsulting.com

ORLA COX
シニア　ディレクタ
サイバーセキュリティ&データプライバシー　コミュニケーションズ
orla.cox@fticonsulting.com

COURTNEY BERRY
ディレクター
サイバーセキュリティ&データプライバシー　コミュニケーションズ
courtney.berry@fticonsulting.com

ELIZABETH MURPHY
ディレクター
サイバーセキュリティ&データプライバシー　コミュニケーションズ
elizabeth.murphy@fticonsulting.com

BRANDON CHATTIN
ディレクター
デジタル&インサイト
brandon.chattin@fticonsulting.com

ALLISON HUFNAGEL
シニア　リサーチ　アナリスト
デジタル&インサイト
allison.hufnagel@fticonsulting.com

さらに詳しい情報は、以下にお問い合わせください。

野尻 明裕
シニア マネジング ディレクター
ストラテジック コミュニケーションズ
Akihiro.Nojiri@fticonsulting.com

浅見 晃子
シニア　ディレクタ
ストラテジック コミュニケーションズ
akiko.asami@fticonsulting.com

FTIコンサルティングについて

FTI コンサルティングは、組織が変化を管理し、リスクを軽減し、財務、法務、経営、政治・規制、風評、取引などの紛争を解決できるように支援することを専門とする独立系のグローバルビジネスアドバイザリー企業です。FTI コンサルティングのプロフェッショナルは、世界中の主要なビジネスセンターでクライアントと緊密に連携しながら、複雑なビジネス上の課題や機会を予測し、明確にして、克服します。

FTI Consulting, Inc.は子会社および関連会社を含め、コンサルティング会社であり、公認会計士事務所や法律事務所ではありません。

本レポートの見解は各執筆者のもので、必ずしもFTIコンサルティング、その経営陣、子会社、関連会社、執筆者以外のプロフェッショナルの見解ではありません。

FTIストラテジック・コミュニケーションズについて

世界中のCクラスの経営陣、取締役会、ビジネスリーダーが、多様なスキルセットと統合された専門性を必要とする最も複雑でビジネスクリティカルな課題を抱えてFTIコンサルティングのもとに来ます。

当社のストラテジック・コミュニケーション（戦略的コミュニケーション）部門は、多くの上級経営幹部や著名人のソーシャルメディア戦略、コンテンツ、チャネル管理を支援しており、数十年にわたる奥深い専門知識と機能的・分野的経験を組み合わせて、リスクの軽減と評判の向上をサポートしています。.

FTIサイバーセキュリティ＆データプライバシーコミュニケーションズについて

当社のサイバーセキュリティ＆データプライバシーコミュニケーションズは、業界でも有数のサイバーセキュリティ・コミュニケーション部門です。サイバーセキュリティ・エクセレンス・アワーズで2021年、2022年、2023年に「サイバーPRファーム・オブ・ザ・イヤー」に選出され、Chambers & Partnersから世界トップクラスの危機管理コミュニケーション【クライシス・コミュニケーション】のプロバイダーとして認められています。サイバーセキュリティへの備えとインシデントのライフサイクル全体に関して危機管理コミュニケーションの専門的な助言と支援を提供し、世界中の企業がインシデントの発生前、進行中、発生後にリスクを軽減し、事業の継続性を高め、ステークホルダーとの関係を維持できるように支援します。

つまり、私たちはクライアントがあらゆるチャネルを通じて効果的なコミュニケーションを図り、主要なステークホルダーとの利益を保護・強化できるように支援します。

FTIデジタル＆インサイツについて

デジタル＆インサイツはFTIコンサルティングの多面的なサービスの中核です。データサイエンス、一次調査、デジタルおよびクリエイティブ戦略の立案と実行の専門家が結集して、各分野の担当メンバーと共に、包括的でオーディエンス重視のアプローチを提供します。これらの洞察は、統合的なコミュニケーション作戦を構築する基盤となります。

さらに詳しい情報と担当チームへの連絡は**CICO Redefinedのサイトを参照してください。**

FTI CONSULTING