COSO

トレッドウェイ委員会支援組織委員会

ガバナンスと全社的リスクマネジメント

デジタル時代のサイバーリスクマネジメント

デロイト社

メアリー・E. ギャリガン | サンディ・ヘリガース | ケリー・ラウ

著　者

デロイト＆トウシュ社

マネージング・ディレクター
メアリー・E. ギャリガン

パートナー
サンディ・ヘリガース

マネージング・ディレクター
ケリー・ラウ

謝　辞

本稿の作成にご協力いただいた次の方々に謝意を表したい。Jeff Antonelli, Neha Awal, Lauren Bady, Brooks Castaneda, Bryan Czajka, Max Kadish, Michelle Rakovsky, Shikha Sharma, ThomasZimlich.

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）理事

序　文

本プロジェクトは、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）から委嘱されたものである。ＣＯＳＯは、組織のパフォーマンスや監督を改善するとともに、組織における不正を減らすために立案された内部統制、全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先進的な考え方を提供することに取り組んでいる。ＣＯＳＯは、次の団体の協賛と資金提供によって運営されている民間部門主導の団体である。

米国会計学会（American Accounting Association）

米国公認会計士協会（American Institute of Certified Public Accountants）

国際財務担当経営者協会（Financial Executives International）

管理会計士協会（Institute of Management Accountants）

内部監査人協会（Institute of Internal Auditors）

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

ガバナンスと全社的リスクマネジメント

デジタル時代のサイバーリスクマネジメント

調査委嘱者

COSO

トレッドウェイ委員会支援組織委員会

2019 年 11 月

Design and production: Sergio Analco.

目　次

ページ

はじめに

本ガイダンスの目的は、企業の経営幹部と取締役を対象に、ＣＯＳＯ全社的リスクマネジメント（ＥＲＭ）のフレームワークで定義された原則を通してサイバーリスクマネジメントに関する概要を示すことである。本ガイダンスでは、サイバーリスクマネジメント手法の基本的な概念に関連する背景を説明するが、技術的な戦略を策定して実施するための包括的な指針となることは意図していない。本稿の対象読者と目的とする用途に関する追加情報は、以下の表を参照されたい。

対象読者	目的とする用途
取締役会	経営者が行うサイバープロセスの監督に役立つ以下のテーマを理解すること • 効果的なサイバーリスクマネジメントプログラムに取締役会と経営幹部が関与する必要性 • ＣＯＳＯのＥＲＭフレームワークを活用して、サイバーセキュリティの戦略、実施およびモニタリングプログラムを管理する方法 • サイバーリスクマネジメント戦略の重要な概念と例
監査委員	
経営幹部（最高経営責任者（ＣＥＯ）、最高情報責任者（ＣＩＯ）、最高リスク責任者（ＣＲＯ）等）	経営幹部によるサイバーリスクマネジメントの運営に役立つ以下のテーマを理解すること • ＣＯＳＯのＥＲＭフレームワークを活用してサイバーリスクを管理する方法 • サイバーリスクに関する検討事項と軽減手法の概要（例：リスク選好、リスクの優先順位づけ） • 著名な専門的サイバーセキュリティフレームワークの実例
サイバー実務者	サイバーリスクをＥＲＭアプローチに当てはめる方法を理解すること

デジタル革命

サイバー脅威と攻撃は、その数と複雑さを増し続けているが、その一方で、ビジネスの世界はますます繋がりを強め、デジタル化が進んでいる。ビジネスとテクノロジーの進化に伴い、ＣＯＳＯの「全社的リスクマネジメント－戦略およびパフォーマンスとの統合（以下、ＥＲＭフレームワーク）」も2017 年に改訂された。ＥＲＭフレームワークの改訂の基盤となった推進力の１つは、サイバー時代のリスクマネジメントの進化に対応する必要性と、進化する事業環境の要求に応えるために組織がサイバーリスクマネジメントのアプローチを改善する必要性であった。ＥＲＭフレームワークは、さまざまな方法で強化されており、戦略設定プロセスにおいてもパフォーマンスを推進する上でも、リスクを検討することの重要性が強調されている。ＥＲＭフレームワークは、

- 戦略を策定し、遂行する上での、全社的リスクマネジメントの有用性についてより深い知見を提供する。
- パフォーマンスと全社的リスクマネジメントの結びつきを向上させ、パフォーマンス目標の設定と、パフォーマンスに及ぼすリスクの影響についての理解を改善する。
- ガバナンスや監督への期待に応える。
- 市場と業務のグローバル化を認識し、個々の状況に合わせつつも、地理横断的に共通したアプローチを適用することの必要性を認識する。
- 事業の複雑性が高まる中で、目標の設定および達成に対するリスクを検討する新しい手法を提示する。
- ステークホルダーに対する透明性の高度化への期待に対応するために、リスク報告を拡充する。
- 進化し続けるテクノロジーや、激増するデータとその解析を、意思決定の支援に適応させる。
- 全社的リスクマネジメントの活動を設計し、導入し、実行するすべての階層の管理者に対し、中核となる定義、構成要素および原則を明確に示す。

2017 年版ＣＯＳＯ ＥＲＭフレームワーク戦略

出典：COSO

ビジネスとテクノロジーの革新により、インターネットが普及し、最近では容易に利用できるクラウドベースのソリューションが登場したことによって、豊富で複雑なコネクティビティ[a]を築き上げたことは明らかである。しかし、デジタル化の出現によって企業がより機動的かつ革新的になるにつれて、新たな常につきまとう脆弱性が生まれている。毎日のように、重大なサイバーインシデントに関する多くの報道がなされている。あらゆる種類と規模の組織が、サイバー攻撃を受けやすくなっている。特定の時点で、どのデータ、システムおよび資産に価値があるかは、サイバー攻撃者の動機次第である。サイバーインシデントが被害企業の評判と財政状態に悪影響を及ぼし続け、さらなる規制や法的な監視を受け続ける限り、サイバー侵害[b]も注目を集め続け、かなりの量の否定的な報道がなされるだろう。

> デジタルトランスフォーメーションに取り組んでいる北米の組織の 90%は、デジタル施策によってリスクプロファイルが拡大したと認識している。サイバーセキュリティリスクの管理は、デジタルトランスフォーメーションに取り組んでいる組織の意思決定者にとっての最大のリスクマネジメント目標である。
>
> 出典：RSA Digital Risk Study, 2019. https://www.rsa.com/content/dam/en/white-paper/rsa-digital-riskreport-2019.pdf[c]

[a] 訳注：パソコンと周辺機器との接続の簡易さや、ネットワークへの接続のしやすさなど、複数のものを連結する際の簡易性を表す。

[b] 訳注：「侵害」と訳した語は原文では「breach」である。日本では「サイバー攻撃」「ハッキング」などと表現されることが多いが、その内容は、不正アクセス、ソフトウェア改ざん、データ流出、マルウェア（不正かつ有害に動作させる目的で作成されたソフトウェアコードの総称で、バックドア、トロイの木馬、ワーム、ランサムウェア、スパイウェア、キーロガー、ボットなどがある）への感染などさまざまである。

[c] 訳注：2022 年２月の翻訳時点でこのサイトは見つからなかったが、次のサイト内の「rsa-digital-risk-report-2019.pdf」が該当すると思われる。https://wwweb.tistory.com/entry/Digital-Risk-Report-2019RSA

組織の従業員と消費者を含むサイバー攻撃被害者が経済的にも個人的にも豊かなことが、サイバー脅威の影響を助長し続けている。さらに、中小企業や地方自治体は、高度な侵入防止・検知システムを備えた大企業よりも標的になりやすく脆弱性を突かれやすいかもしれないが、大企業の方が、破壊行為や不正な収入源としては効率的かもしれない。そのため組織は、データ侵害が発生した場合の金銭的な損失に関連するリスクを移転して軽減するために、サイバー保険契約の費用対効果を検討することが重要である。ただし、風評被害に伴う費用に対して制限があったり、組織のデータ分類方針や暗号化規格等に問題があるとして保険会社が保険金の支払いを拒否したりする場合もあるため、保険契約の補償範囲や制限を理解することも同様に重要である。

> 保険会社のヒスコックス社によると、デジタルインシデントによる中小企業の被害額は平均 20 万ドルで、60%が被害を受けてから半年以内に廃業している。また、これらの攻撃の発生頻度も増加しており、過去 1 年間で全中小企業の半数以上が侵害に見舞われ、10 社中 4 社が複数のインシデントを経験した。
>
> 出典：Cyberattacks now cost small companies $200,000 on average, putting many out of business, CNBC. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

さらに、デジタルトランスフォーメーションとＩＴは、グローバルな環境下での組織の活動方法を進化させ続ける。このようなデジタル化の進展は、特に組織が外部のサービスプロバイダなどとデータを共有することが多いことを考慮すると、複雑性、変動性および組織が完全にはコントロールできないインフラへの依存度が増すことになる。組織と外部の関係者（例：サービスプロバイダ、ベンダーおよび顧客）との間では、業務を遂行するために情報と電子的コミュニケーションを共有できるような信頼関係やコントロールが構築され運用されているかもしれないが、問題が発生した場合、組織は境界外でのテクノロジー侵害の責任を問われることがよくある。また、自社のデータが安全でもベンダーの 1 社が侵害の影響を受けた場合、「連座制で有罪」になることさえある。企業は新しいテクノロジー（例：人工知能、ブロックチェーン、クラウドコンピューティング、機械学習等）を活用し続け、外部機関を利用して業務を遂行し続けるため、サイバー攻撃者は情報システムやコントロールを悪用できる新たな脆弱性を利用するようになる。2018 年の Ponemon Institute の調査「Data Risk in the Third-Party Ecosystem（サードパーティエコシステム内のデータリスク）」によると、59%の企業が、利用しているサードパーティを原因とする侵害を経験している。同調査では、機密データがサードパーティによって紛失または盗難された場合、それを知ることができると確信している企業はわずか 11%にすぎなかった。サードパーティへの依存度の高さは、企業の範囲を事実上拡大しており、情報セキュリティ侵害の大きな要因となっている。したがって、ＥＲＭプログラムは、サードパーティエコシステム内のサイバーリスクマネジメントまで拡大しなければならない。

企業は事業活動を守るために、自社のテクノロジーに関する情報を社内外で共有する際には細心の注意を払っているが、サイバー攻撃者には、対極的な領域で活動する余裕がある。彼らは、法的な影響をほとんど恐れずにダークウェブを介して境界なしでオープンに情報を共有し、非常に高い匿名性を保って活動していることが多い。サイバー攻撃者はテクノロジーを活用し、方針やセキュリティ手順の不備を突こうとして、事実上どこからでも攻撃し、また事実上あらゆる種類のデータを標的にする。攻撃者は内部の脅威である場合も外部の脅威である場合もあり、その動機もさまざまである。

サイバー攻撃に加えて、破壊的なマルウェア、ランサムウェアならびに情報システムとデータの機密性、可用性および完全性を損なうために用いられるその他の方法のように、他のサイバーシナリオに関連するリスクは、組織の有形・無形の資産に大きな影響を与える可能性がある。このように広範囲に及ぶサイバー脅威にもかかわらず、特に組織の戦略、プロセスおよびテクノロジーが業務運営を支えるために進化し続けることを考えると、すべてのデータを保護することが不可能なのは明らかである。進化の都度、エクスポージャーの機会が生まれる。進化を慎重に扱うことでエクスポージャーの機会を最小限に抑えることはできるが、すべての脆弱性に対処したかを確認するのは不可能である。さらに、サイバー攻撃者は進化し続けて、弱点を突く新たな方法を見つけている。

その結果、サイバーリスクは回避できるものではなく、むしろ管理しなければならないのが現実である。組織は、収集するすべてのデータ、データの収集方法、データの保存場所を確実に把握した上で、最も重要なデータに焦点を当てて、組織の情報資産、ブランドや評判、サプライチェーン等を保護するための適切なセキュリティコントロールやその他のリスク軽減手法を展開すべきである。

組織は、ＣＯＳＯのＥＲＭフレームワーク[1]のリスクマネジメントの以下の構成要素を通じて、サイバーリスクプロファイルを検討することができる。

リスクマネジメントの構成要素

出典：COSO

- **ガバナンスとカルチャー：**ガバナンスとカルチャーはともに、全社的リスクマネジメントの他のすべての構成要素の基礎となる。ガバナンスは、全社的リスクマネジメントの重要性を強調し、それに対する監督責任を確立する事業体の気風を醸成する。カルチャーは、意思決定に反映される。
- **戦略と目標設定：**全社的リスクマネジメントは、戦略と事業目標の策定プロセスを通じて、事業体の戦略計画に統合される。事業環境を理解することにより、組織は、内外の要因とそれらがリスクに及ぼす影響についての知見を得ることができる。組織は、戦略策定と合わせてリスク選好を設定する。事業目標は、戦略の実行を可能にし、事業体の日常活動とその優先順位を形づくる。
- **パフォーマンス：**組織は、戦略と事業目標を達成する事業体の能力に影響を及ぼすかもしれないリスクを識別し、評価する。そのために、組織は戦略と事業目標の達成に影響するかもしれないリスクを識別し、評価する。組織は、リスクの重大度に応じて、また事業体のリスク選好を考慮して、リスクを優先順位づけする。そして、組織は、リスクへの対応を選択し、パフォーマンスの変化の動向を監視する。このように、組織は、戦略と全社レベルの事業目標を追求する中で受け入れたリスク量に対するポートフォリオの視点を構築する。
- **レビューと修正：**全社的リスクマネジメントの能力と実務、およびその目標に対する事業体のパフォーマンスをレビューすることにより、組織は、全社的リスクマネジメントの能力と実務が、どの程度まで長期的に価値を向上させてきたのか、さらに、大きな変化に直面した場合でも価値を向上させ続けられるかを検討できる。
- **情報、伝達および報告：**伝達は、事業体全体を通して情報を収集し、共有する継続的で反復的なプロセスである。経営者は、全社的リスクマネジメントを支援するために、内外の情報源から関連性のある情報を利用する。組織は、データと情報を入手し、処理し、管理するために、情報システムを活用する。すべての構成要素に関連する情報を利用して、組織は、リスク、カルチャーおよびパフォーマンスについての報告を行う。

サイバーリスクを管理するためのアプローチは、組織特有の事業環境に応じてカスタマイズすべきであるが、ＥＲＭフレームワークは、そのようなアプローチを設計するための基盤を提供する。以下では、ＥＲＭフレームワークの 20 の原則を説明し、これらの原則がサイバーリスクに固有のエクスポージャーにどのように対処できるかについても考察する。

ガバナンスとカルチャー

原則	説明
1．取締役会によるリスク監視を行う	取締役会は、戦略を監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目標を達成できるよう支援する。
2．業務構造を確立する	組織は、戦略と事業目標を達成するために、業務構造を確立する。
3．望ましいカルチャーを定義づける	組織は、事業体の望ましいカルチャーを特徴づける望ましい行動を定義づける。
4．コアバリューに対するコミットメントを表明する	組織は、事業体のコアバリューに対するコミットメントを表明する。
5．有能な人材を惹きつけ、育成し、保持する	組織は、戦略と事業目標にふさわしい人的資本の形成にコミットメントする。

サイバー脅威の発生頻度、複雑性および破壊力が増すにつれて、組織は戦略や事業目標の達成に対してより大きなリスクに直面する。侵害の影響には、データ損失、事業の中断、ブランドや評判の低下および規制や法律上の影響などがあり得る。そのため取締役会は、サイバーリスクをＩＴだけの問題として捉えるのではなく、より広範な全社的リスクの一部として熟考しなければならない。「デロイト社の 2019 年版「サイバーの未来に関するサーベイ」[2] によると、回答した組織のほぼ半数（49%）が、少なくとも四半期ごとにサイバーセキュリティを取締役会の議題にしている」。

> 回答した組織のほぼ半数（49%）が、少なくとも四半期ごとにサイバーセキュリティを取締役会の議題にしている。
>
> 出典：Deloitte's 2019 Future of Cyber Survey, in conjunction with Wakefield Research, of 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019, using an online survey.

取締役会は、サイバーセキュリティの専門家や関連する専門知識を持つアドバイザーを育成または獲得することが不可欠である。「テクノロジーに特化した取締役を任命した公開企業の割合は、過去 6 年間で 10%から 17%に増加した」[3]。

> テクノロジーに特化した取締役を任命した公開企業の割合は、過去６年間で 10%から 17%に増加した。
>
> 出典：Khalid Kark, Caroline Brown, Jason Lewris, Bridging the boardroom's technology gap, Deloitte University Press, June 29, 2017.

これは大幅な増加ではあるが、この数を増やすにはまだ大きな機会がある。急速に進化するサイバー脅威の状況は、取締役会に、サイバーリスクを理解し、組織のサイバープログラムと施策を評価し、組織が直面するサイバーリスクにどの程度対処しているかを評価するために、サイバー能力を高めることを求めている。例えば、取締役会の構成にサイバーリスクに関する知識や経験が不足している場合には、独立したアドバイザーを活用することで業界全体の視点からサイバーの動向を把握できる。サイバーリスクに関する取締役会のガバナンスには、組織のサイバーセキュリティの戦略、実施およびモニタリングプログラムの監督が含まれる。これには、サイバーリスク要因および / または重大なサイバーセキュリティ侵害に関する適切かつ関連性のある情報公開が確実に行われるようにすることが含まれる。例えば、取締役会は、同業他社と比較して自社のサイバーセキュリティ態勢を理解しようとすることがある。そして、公開されているリスク要因やサイバーセキュリティ侵害の量を考慮すると、取締役会は同業他社と比較して自社のサイバー情報公開を監督することも可能である。

サイバーリスクは蔓延するため、組織はＥＲＭの観点からサイバーセキュリティに取り組むことが重要である。このようなサイバーリスクに対処するための統合的な管理アプローチでは、通常、最高情報責任者または最高情報セキュリティ責任者が主導し、最高財務責任者、最高リスク責任者、法務顧問または最高執行責任者のような上級経営者で構成するサイバーリスクマネジメントチームを設置する。このチームは、部門や機能を横断した代表者で構成し、フレームワークに基づいて全社的なサイバーリスクを評価し、サイバー脅威のリスクを判断し、全社的なサイバーセキュリティマネジメント計画を作成し、サイバーリスクを軽減するための予算を策定すべきである。サイバーリスクマネジメントチームは、サイバー脅威の影響と関連するリスクマネジメント施策について取締役会に報告すべきである。組織の内部監査部門長も、このチームの一員またはチームの独立したアドバイザーであるべきである。

米国国立標準技術研究所（ＮＩＳＴ）[4]の定義によると、最高レベルの成熟度に既に到達している企業には、以下のような中核的な特徴がある。

- 経営幹部と取締役会の両方を含む首脳陣の関与を確保している。
- 組織内のＩＴ部門以外でもサイバーセキュリティの認識を高め、セキュリティ機能に対してより高いレベルで注意を払い、より大きな影響力を与えている。
- サイバーセキュリティへの取組みを、企業の事業戦略とより密接に連携させている。

組織のサイバーセキュリティカルチャー、セキュリティ意識およびそれらに関連する従業員の望ましい行動は、取締役会と経営者から始まり全従業員に及ぶ。サイバーセキュリティカルチャーは、組織のカルチャーに根づくべきである。サイバーセキュリティに対する意識、研修およびデータ損失防止を重視した強固なカルチャーがある組織は、フィッシング詐欺、ソーシャルエンジニアリングおよびその他の形態のサイバー攻撃の影響を受けにくくなる可能性がある。組織のカルチャーとは、「「ここでの仕事の進め方…」であり、価値観、信念、行動、成果物および報酬制度など、人々の日々の行動に影響を与えるものである。それはトップのリーダーシップによって推進され、無数のプロセス、報酬制度および行動を通じて組織に深く根づくようになる」と定義されている[5]。

> サイバーとＩＴの問題は、平均的な内部監査計画の 20%近くを占めるまでに伸びてきた一方で、個々のこれらの重要な問題は、業務、財務、報告およびコンプライアンス・規制などよりも取締役会から低リスクと見なされており、他の問題に比べて依然として遅れている。
>
> 出典：内部監査人協会 2019 年版北米の内部監査の動向調査

組織のサイバーリスクマネジメントプログラムは、取締役会と上級経営者が確立した組織のコアバリューと整合する必要がある。このプログラムの方針、基準、従業員への期待、アカウンタビリティおよび関連するすべてのコミュニケーションは、組織のコアバリューを支持していることを示すべきである。例えば、経営者は望ましい行動を強制しようとするのではなく、サイバーへの警戒の重要性を理解してもらうために従業員との信頼を築くよう努めるべきである。また、首脳陣は望ましいサイバー行動や習慣を示して正しく方向づけるべきである。

効果的なサイバーカルチャーがある組織は、そのカルチャーと望ましい行動を具現化するために首脳陣の賛同と関与を得ている。継続的なサイバー研修に投資し、サイバーリスクに対する従業員の見方を定期的にモニタリングすれば、サイバーセキュリティにおける自身の役割およびサイバーセキュリティプログラムで説明されている従業員の行動や習慣に対する従業員の意識を高めるはずである。例えば、多くの組織では、エンドユーザがフィッシング攻撃を回避できるかをテストする研修プログラムを実施している。エンドユーザが偽のフィッシングリンクをクリックすると、通常とは異なる電子メールは慎重に判断する必要があると再認識させられる。別の組織では、エンドユーザのセキュリティ対策の悪い例を撮影したビデオを従業員と共有してユーザを教育している。また、多くの組織では、メールフィルタリングプログラムの一環として、外部の電子メールアドレスや不適切なリンクが含まれている可能性のある電子メールを識別するソフトウェアを使用してフィルタリングしている。さらに研修の一環として、従業員は潜在的なサイバー問題を報告する方法と場所を理解すべきであり、報告を奨励されるべきである。

組織のサイバーリスクマネジメントプログラム

サイバー脅威は、より速いスピードで進化し続け、より複雑になり、新たな攻撃手段を取り込んでいる。組織のサイバーリスクを効果的に評価し、リスク軽減策を実施し、サイバーセキュリティプログラムの有効性をモニタリングするためには、資格を持ったサイバーリスク専門家の関与が不可欠である。適切な資格を持った社内の専門家がいる組織もあれば、資格を持った外部の専門家の支援が必要な組織もある。例えば、一部の組織では、関連性のある認定資格（例：Certified Information Security Services Professional（ＣＩＳＳＰ）資格）を義務づけるなど、情報セキュリティチームのサイバー能力に対する最低限の期待を定めている。その上、技術的リソースを持つ組織は、新しいアーキテクチャやプラットフォームの設定ミスに関連するリスクを理解していないことに起因するリスクを管理するために、新たに採用した技術に対するスキルの向上および / または研修が不可欠である。また、特殊なスキルセットが必要な場合には外部の企業を雇って、サイバーリスク評価、レジリエンス対策の導入および / またはサイバーセキュリティプログラムの有効性の定期的評価について支援を受ける場合もある。さらに、組織が重大なサイバーセキュリティインシデントや侵害を経験した場合には、フォレンジックや調査作業を行うために外部の専門家の支援が必要になることもある。

ガバナンスには、データ管理とレガシーシステム終了のための仕組みも含めるべきである。よくある最悪の失敗は、ネットワーク上に残っているレガシーシステムであり、パスワードがデフォルトのままであったりアクセス権が過度に与えられたりなどの脆弱性があり、本来ならば使用中止や廃棄となっているはずのハードウェアやデータに、ユーザがアクセスできてしまうことである。これは、古いストレージデバイスやデータベースに存在していることを少数のＩＴスタッフしか覚えていないダークデータ[d]のリスクでもあり、脆弱性を突かれる可能性が高くなる。

「ガバナンスとカルチャー」は、サイバーリスクを管理するための重要な基盤となる要素であるため、職責やシステムへのアクセスについての職務分離と、組織全体で複数のディフェンスラインを組み込んだ事業戦略の実施を推進すべきである。

[d] 訳注：企業に蓄積されたビッグデータのうち、有効利用されずに保存されているデータのことを指す。ビッグデータの一種で、分析不可能で価値が不明なデータのこと。

戦略と目標設定

原則	説明
6．事業環境を分析する	組織は、リスクプロファイルに対する事業環境の潜在的影響を検討する。
7．リスク選好を定義する	組織は、価値の創造、維持、実現の観点からリスク選好を定義する。
8．代替戦略を評価する	組織は、代替戦略とリスクプロファイルに対する潜在的影響を評価する。
9．事業目標を組み立てる	組織は、戦略と結びつき、かつ、戦略を支える事業目標をさまざまな階層において設定する際にリスクを検討する。

「事業環境」とは、組織の現在と将来の戦略や事業目標に影響を与えるトレンド、関係性およびその他の要素を指す。変化の激しい今日の環境下で企業が変化し続ける状況に適応するためには、現在のサイバー環境を理解する必要がある。そのためには、戦略と事業目標の定期的な見直しの中で、現在と将来の組織の事業目標を達成するために不可欠な情報とテクノロジーを考慮すべきである。

> 2021 年までに、サイバー犯罪による被害額は年間 6 兆ドルに達すると予想されており、これは世界経済の約 10% に相当する。
>
> 出典：https://Deloitte.wsj.com/cio/2019/07/11/cyber-incidents-and-breaches-the-data-dilemma/

一例として、あるメーカーは現在、従来の小売チャネルから得る収益を通じて株主価値に関わる事業目標を実現している。このような現状では、企業間取引の製造と出荷に関連する情報とシステムが、株主価値に関連する最も重要な資産である。経営者は、組織の複数年にわたる戦略計画の中で将来を見据えて、消費者への直接販売チャネルに大幅な投資をして成長させる計画をしている。従来のオペレーションは全般的な事業目標を支え続けるが、将来の事業目標を達成するためには、テクノロジーとマーケティングのロードマップの中で、新しい情報とシステムを検討しなければならない。

変化が起こると組織は、新しいシステム、インターネット上の電子商取引の足跡、モバイルアプリケーションのセキュリティおよびカスタマーロイヤルティプログラムの情報と完全性の保護に関して、新たなサイバーリスクを考慮しなければならない。絶えず変化する組織の業務環境下では、事業環境の進化に合わせてサイバーセキュリティを考慮しなければならない。

企業は、サイバー空間上の現在のリスク、トレンドおよびインフルエンサーを常に把握しておく必要がある。2021 年までに、サイバー犯罪による被害額は年間 6 兆ドルに達すると予想されており、これは世界経済の約 10%に相当する[6]。サイバー犯罪者は、企業を攻撃する新しい革新的な方法を見つけている。通常、ある攻撃方法が有効であることが示されると、同じ方法が複数のサイバー犯罪者によって使用される。デロイト社の 2019 年版「サイバーの未来に関するサーベイ」への回答によると、調査対象となった経営幹部[e]のほぼ全員（95%）が、自社がさまざまなサイバー攻撃を経験し、収益、評判およびリーダーシップの安定性に深刻な影響があったと認めている。さらに、90% の組織が、過去 1 年以内に機密性の高い本番データ[f]の公開を少なくとも 1 回経験し、41%は 5 回以上の事例を経験した。

リスク選好の定義およびサイバーリスクと報酬との適切なバランスの決定は、すべての組織が考慮しなければならない。リスク選好の 1 つの側面として、デジタル施策でますます重要になってきているのが、高度なテクノロジーの採用やテクノロジー能力の拡大を行わない場合の費用対効果である。組織は、より迅速に行動し、より高度なテクノロジーを導入しなければならないことに気づいているため、特定の状況下では、既存の事業運営で組織が従来受け入れてきたリスク選好を調整する必要があるかもしれない。組織が現在のサイバー環境の評価に取り組む際、経営者はサイバープログラムの展開を計画する範囲を評価する必要がある。このプロセスの一環として、組織は重要な資産の棚卸をし、リスクを識別し、サイバー脆弱性がどこに存在するかを判断する必要がある。

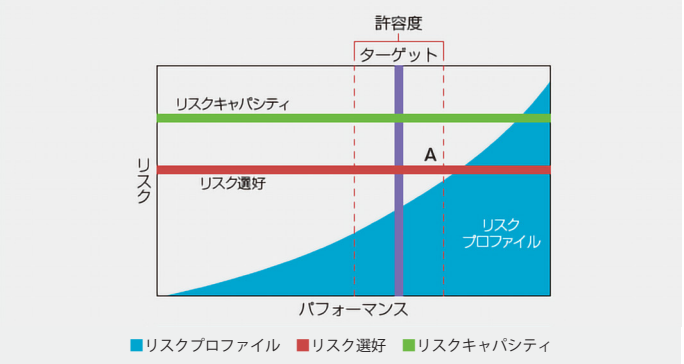
[e] 訳注：原文は「C-level executives」。
[f] 訳注：原文は「production data」。

経営者はこの分析から、どの事業部、拠点、テクノロジープラットフォームを、どの程度までサイバープログラムに組み込む必要があるかをより適切に判断できる。これらの要因は、サイバーセキュリティに関連したリスク選好を定めて継続的に更新するのに役立つ。例えば、テクノロジーへの依存度が高く、電子商取引を頻繁に行っている企業では、電子商取引の業務に関連するテクノロジーや情報に対するサイバーリスク選好が低いかもしれない。また同じ企業でも、主要な事業目標を達成する上で中核とならない情報やシステムに対するリスク選好は高いかもしれない。サイバーセキュリティに対する組織のリスク選好を決定したら、経営者はこれを事業のすべての主要なステークホルダーに伝え、最終的には取締役会の監督を通じてモニターする必要がある。組織のリスク選好は変化する可能性があるため、変化が予想される場合と変化が起きた場合に、リスク選好の決定をどのように管理するかを検討することが重要である。前述の例では、従来の小売チャネルを持つメーカーが消費者への直接販売分野への変更を見込んでいる場合、消費者への直接販売に進出した初期段階での収益は小さいかもしれない。しかし、その段階に至るまでの投資は多額で、市場での評判リスクも高いと考えられる。このような状況では、この特別な事業拡大に対するリスク選好は低くなり、組織の事業目標を支える将来の収益計画の重要性に基づいて、サイバーセキュリティとレジリエンスに対してより多くの経営資源を投入することを選択する可能性がある。

一旦サイバーセキュリティのリスク選好が定義されると、経営者はサイバーリスクマネジメントプログラムを管理するためのセキュリティモデルを特定する。経営者がどのようなサイバーセキュリティモデルを導入するかを決定する際には、組織にとって適切なサイバー戦略を特定することと併せて、いくつかの要因を評価する必要がある。これらの要因には、資本、経営資源およびテクノロジーなどがある。ＮＩＳＴの Cybersecurity Framework[7]、国際標準化機構（ＩＳＯ）の ISO 27001/2[8]、米国公認会計士協会（ＡＩＣＰＡ）の Cybersecurity Risk Management Reporting Framework[9] などのいくつかのサイバーセキュリティフレームワークは、組織がサイバーセキュリティプログラムの有効性を確立して報告するのに役立つように策定されている。組織は、自社の業務運営、現在のコントロール構造およびその他の状況に応じて、最適なサイバーセキュリティフレームワークを判断しなければならない。サイバーセキュリティフレームワークの実例は、**付録**を参照されたい。

経営者にとっては、サイバーセキュリティプログラムを事業目標と整合させて、ターゲットを設定することが重要である。リスクを定量化してリスク許容度評価のための値を導き出すためには、オープン・グループのＦＡＩＲ（Factor Analysis of Information Risk：情報リスクの要因分析）のような手法が活用できる。リスクマネジメントプログラムが、経営者のリスク選好に基づいて定義された最大許容値（下記の「リスク許容度の境界値」の「Ａ」）を含む、定義され理解された境界内で運営されることを確実にするためには、一定の許容度、すなわちパフォーマンスの許容可能な差異を設定することができる。重要でない資産については、経営者は重要な資産よりも積極的でないサイバーセキュリティモデルを決定する可能性がある。さらに、サイバー空間でのダイナミックな動きを考慮すると、サイバーセキュリティプログラムの再評価は重要である。評価の結果、ターゲットが未達だったり、定められた許容度を超えたりした場合には、サイバーセキュリティのリスク選好および/またはサイバーガバナンスモデルを見直す必要がある。

リスク許容度の境界値



「戦略と目標設定」は、サイバーリスクを管理するための鍵であり、全般的な戦略や事業目標と統合されなければならない。

パフォーマンス

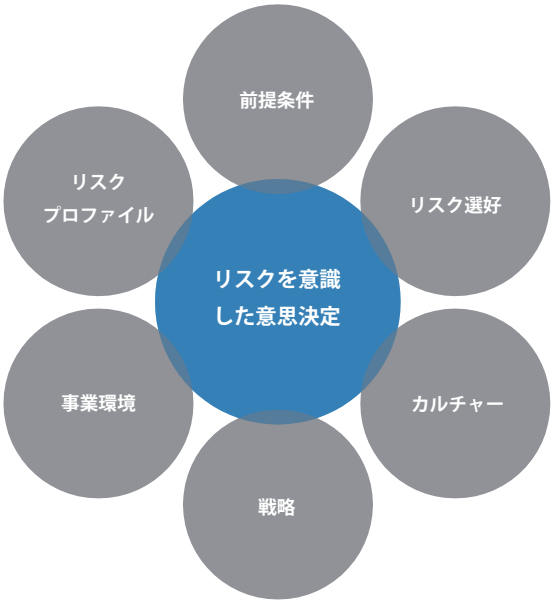
原則	説明
10. リスクを識別する	組織は、戦略および事業目標のパフォーマンスに影響を及ぼすリスクを識別する。
11. リスクの重大度を評価する	組織は、リスクの重大度を評価する。
12. リスクの優先順位づけをする	組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。
13. リスク対応を実施する	組織は、リスク対応を識別し、選択する。
14. ポートフォリオの視点を策定する	組織は、リスクのポートフォリオの視点を策定し、評価する。

すべての組織は、外部や内部の要因からのさまざまなサイバーリスクに直面している。サイバーリスクは、ある事象が発生して組織の目標達成に悪影響を及ぼす可能性に対して評価される。悪意のある行為者、特に金銭的な利益を動機とする行為者は、コストと報酬を基準にして活動する傾向がある。サイバー攻撃の犯罪者とその背後にある動機は、一般に次のような大まかなカテゴリーに分類される。

- **国家とスパイ：**軍事上および競争上の優位性のために知的財産や企業秘密を得ようとする敵対的な外国（例：国家安全保障上の秘密や知的財産を盗もうとする国）。
- **組織犯罪者：**高度な手段を用いて金銭または企業の消費者に関する私的な機密情報を盗む犯罪者（例：個人情報の窃盗）。
- **テロリスト：**インターネットを利用して、金融機関などの重要インフラへのサイバー攻撃を目的とした悪質なグループや個人。
- **ハクティビスト：**組織の機密情報を窃盗または公開することで、社会的または政治的な主張をしようとする個人やグループ。
- **インサイダー：**組織の機密情報を販売または共有する、組織内部で信頼されている個人。

リスク評価の結果は、最終的には、サイバーリスクを防止、検知および管理するために設計されたリスクマネジメント対応に向けて企業の経営資源を配分する原動力となるべきであるが、リスク評価のプロセス自体にも投資する必要がある。組織の経営資源は有限なので、これらの対応策への投資の決定は、企業にとって最も重要な情報システムへの資金提供を優先するような、関連性のある質の高い情報に基づいて行われなければならない。

組織のサイバーリスク評価プログラム

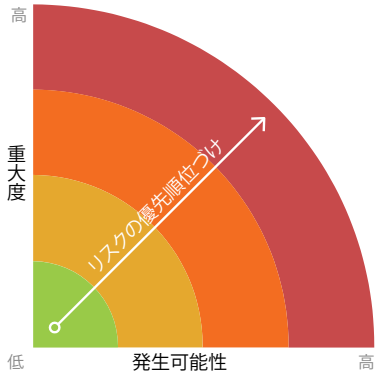


組織のサイバーリスク評価は、まず、組織にとって価値のある情報とシステムを把握することから始めるべきである。その価値は、企業の目標に対する潜在的な影響（事業目標の達成に間接的な影響を与え得る、法律や規制のコンプライアンス違反による潜在的な影響を含む）と比較して測定すべきである。例えば、さまざまな業種（例：金融サービス、テクノロジー、医療）の企業は、企業の資産ならびに商取引、業務プロセスおよびシステムが高度に自動化されているという性質を考慮すると、サイバー犯罪の主な標的となる可能性がある。

サイバーリスク評価は、企業の目標を支える情報システムに対するリスク対応の展開方法についての経営者の意思決定に影響を与えるため、上級経営者やその他の重要なステークホルダーは、企業の目標に沿って保護すべきものを特定するようにリスク評価プロセスを推進することが重要である。多くの組織では、組織にとって本当に重要な情報システムを把握するために十分な時間をかけておらず、また、情報がどこにどのように保管されているかを把握することが困難な場合もある。そのため、すべてを保護しようとすると、特定の情報システムを過剰に保護し、他の情報システムを過小に保護することになりかねない。

情報システムを評価するには、事業部門とＩＴの関係者が高度に協力する必要がある。組織は、限られた時間、予算および利用可能な経営資源の中ではすべてのリスクには対処できないため、経営者は、組織が受容可能なリスクの許容度を決定し、最も重要な情報システムを保護するために努力を集中すべきである。

リスク評価の優先順位づけ



原則 10 と原則 11 の結果として、組織は、組織目標を達成するために重要な情報システムを明確に把握すべきである。次に原則 12 を適用して、組織がサイバーリスクの事象や結果の重大性と発生可能性に関してリスクを評価して優先順位をつけることで、リスク評価がより深く行われる。上級経営者が主導し、事業部門とＩＴの関係者が協力する場合、組織は組織全体の目標達成に影響を与え得るリスクを評価できるようになる。

リスク評価プロセスのこの段階では、サイバーリスクを単に広く捉えるのではなく、業種ごとに捉えることも重要である。サイバー攻撃の加害者には、業種ごとに異なる特有の目的がある。例えば、小売業では、組織犯罪者が攻撃者となる可能性が高く、利益につながる情報（例：クレジットカードデータや個人（識別）情報（ＰＩＩ））を含むシステムの脆弱性を利用することに主眼を置いている。また、石油・ガス産業は、将来の探査地に関する戦略的なデータを盗むことを目的とした国家の攻撃対象となるかもしれない。化学薬品会社は、自社製品を取り巻く環境問題が認識されているため、ハクティビストの標的となる可能性がある。

攻撃の動機、可能性の高い攻撃方法、攻撃者が使用するかもしれない技術、ツールおよびプロセスを慎重に評価することで、組織は起こり得ることをより良く予測し、潜在的なサイバー攻撃による混乱を最小限に抑え、価値の高い資産を安全に保つために非常に効果的なコントロールやその他のリスク対応を設計できる。

リスクに対するポートフォリオの視点は、組織の最も重要な情報システムを保護するためのサイバーリスクマネジメント活動の展開に影響を与え得る変化を反映するために、継続的に更新すべきである。変化する脅威の状況の注意深いモニタリングとリスク評価プロセスから情報が得られたら、上級経営者やその他のステークホルダーは、サイバーリスクのエクスポージャーから組織を守る最善の方法について十分な情報に基づく判断をするために、これらの情報を共有して議論しなければならない。

リスク対応には、組織がその結果を許容できる場合にはリスクの受容、他者がそのリスクをより効果的または効率的に管理できる場合にはリスクの移転、あるいはそのようなリスクを軽減または低減するための行動、という形がある。これらの決定はリスク評価によって行われるため、そのような対応が組織のリスク選好に適しているかを検討することが重要である。このようなリスク対応を決定した場合、組織は通常、統制活動を展開する。統制活動とは、目標達成に対するリスクを軽減するために、経営者の指示を確実に守って組織内の個人が行う活動のことである。このような統制活動は、統制活動が組織全体で一貫して実施されるようにするために、方針の中に記載すべきである。

前述のとおり、サイバーリスクは回避できないが、適切な対応策と復旧プロセスを慎重に整備して運用することで、そのようなリスクを管理できる。組織は、（リスク評価プロセスを通じて）想定される攻撃方法と脆弱性を突く経路を検討することで、サイバー侵害が組織の目標に与える潜在的な影響を最小限に抑えることができる。組織は、サイバー侵害が避けられないという現実を受け入れ、適切なサイバーリスク評価を行った上で、最初の防御レイヤーに侵入された後に、侵入者が情報システムを自由に移動できないように、あるいは侵入されたことが検知できるように、統制構造を階層的に展開すべきである。さらに、効率的で強固な復旧プロセスの重要性が指摘されているが、その程度は、攻撃の種類やエクスポージャーのレベルによって異なる場合がある。例えば、データにアクセスするための「鍵」を得るために身代金を支払うまで組織の情報資産へのアクセスを制限する大規模なランサムウェア攻撃では、復旧プロセスが非常に重要であり、「鍵」が提供されなかったりランサムウェアが削除されなかったりしても取り戻せない暗号通貨での支払いには、数十万ドルの費用がかかることがある。この種の攻撃では、業務を再開するために最新のデータバックアップから各デバイスを再イメージング[g]および復元し、身代金の支払いのリスクを回避し、追加の支払いを要求する攻撃者の恒常的な標的になることを避ける必要がある。しかし、ある従業員のラップトップコンピュータにマルウェアがインストールされ、他のデバイスに影響を与える前に組織のネットワークから切り離されたようなケースでは、復旧プロセスはそれほど重要ではないかもしれない。

サイバーリスクのエクスポージャーは、組織の内外を問わず、さまざまな侵入口から生じる可能性があるため、サイバーリスクを軽減するためには予防的コントロールと発見的コントロールの両方を導入すべきである。適切に設計された予防的コントロールは、侵入者を組織の内部ＩＴ環境外にとどめて情報システムを安全に保つことで、攻撃の実現を阻止できる。また、追加の予防的コントロール（例：ハニーポットシステム[h]）を内部ＩＴ環境内に実装し、侵入者の動きを鈍らせる障害物として機能させることもできる。脆弱性の悪用が起きた場合でも、発見的コントロールによって組織は侵害を適時に検知することができ、経営者はできるだけ早期に是正措置を講じたり潜在的な損害を評価したりできる。是正措置を講じた後、経営者は根本原因を評価し、将来発生する可能性のある同様の脆弱性の悪用を防止または検出するためにコントロールを改善することが重要である。

最終的に組織は、包括的な方針を採用して継続的に更新しなければならず、また、サイバー攻撃に効果的に対応して復旧するために、災害復旧、事業継続、データセキュリティ、危機管理および広報に関する研修を実施しなければならない。そのため、戦略や事業目標の達成に対するリスクを識別、優先順位づけおよび対応するための強固なプロセスを持つことが、パフォーマンスを発揮する上で極めて重要である。

[g] 訳注：整合性のとれた１つの基本イメージから複数のデバイスにソフトウェアをコピーすること。
[h] 訳注：サイバー攻撃者がどのように行動し何を狙っているのかを、セキュリティ担当者が確認するために、攻撃者を引き寄せるように設計されたコンピュータシステムのこと。

レビューと修正

原則	説明
15. 重大な変化を評価する	組織は、戦略や事業目標に重大な影響を与え得る変化を認識し、評価する。
16. リスクとパフォーマンスをレビューする	組織は、事業体のパフォーマンスの結果をレビューし、リスクを考慮する。
17. 全社的リスクマネジメントの改善を追求する	組織は、全社的リスクマネジメントの改善を追求する。

ＩＴの急速な進化、従業員によるＩＴの採用、グローバルなサプライチェーンおよび産業用モノのインターネット（ＩＩｏＴ）の企業への浸透により、組織に対するサイバー攻撃の脅威が高まっている。サイバー攻撃が成功すると、組織に大きな財務上や評判上の影響を与える可能性がある。サイバー攻撃が成功した場合のリスクを軽減するために、組織は重大な変化が戦略、事業目標およびリスク選好にどのような影響を与えるかを識別して評価するプロセスを策定すべきである。

例えば、人工知能やネットワークセンサーを利用したスマートファクトリーソリューションの導入を計画しているメーカーは、発生するサイバーセキュリティリスクに対応するために、既存の業務、財務および技術の戦略を見直す必要がある。この見直しには、強固なサイバーリスクマネジメントプログラムの開発、資格のあるサイバーリスク専門家の雇用や既存の従業員の再教育、または新たなセキュリティ脆弱性の継続的な評価の実施などの費用対効果の分析を必然的に伴う。さらに組織は、サイバー侵害が成功した場合のコミュニケーションを含め、ベンダー、顧客および規制当局への影響のような外部環境を管理する必要がある。

サイバーリスク評価プロセスは、組織の内部環境や外部環境に変化が生じたときに繰り返される。組織は各変化を評価して全社的な影響を判断し、サイバーリスクを最適に管理する方法を決定しなければならない。

組織は、サイバーセキュリティの脅威や潜在的な攻撃に関連するリスクを識別して軽減できているかを判断するために、サイバーセキュリティリスクの評価施策を常に評価すべきである。経営者は継続的な評価を行うために、目標、パフォーマンスの測定指標およびターゲット未達の場合の結果を明確にしなければならない。ターゲット未達の場合の影響は、潜在的な侵害のリスクと影響に比例したものでなければならない。その後、サイバーリスクに関連するコントロールの有効性のアシュアランス（例：リスクコントロールがどのように定期的にモニタリングされテストされているか）は、内部監査部門または独立した報告を目的とする外部監査人が行うことができる。例えば、ＡＩＣＰＡは、「System and Organization Controls ("SOC") for Cybersecurity というガイダンスを公開しており、公認会計士はこのガイダンスを通じて、組織の全社的なサイバーセキュリティリスクマネジメントプログラムについて報告する。この情報は、上級経営者、取締役会、アナリスト、投資家およびビジネスパートナーが、組織の取組みをより良く理解するのに役立つ[10]」と、組織のサイバーセキュリティプログラムの有効性と成熟度に関する独立した意見を述べている。

例えば、フィッシングメールは組織にとって高リスクである、と経営者が判断したとする。経営者は、従業員がそのリスクを確実に認識するために従業員研修プログラムを実施した。その目標は、全従業員がフィッシングメールをクリックしないようにすることでもあった。この研修プログラムを実施した後もフィッシングに関して無視できないほどの問題が残っていた場合は、プログラムを再検討して、従業員研修に加えてフィッシングのような電子メールをスキャンするソフトウェアを導入するなどの修正を行う必要がある。

新しいテクノロジーを進化させて導入しようとしている組織にとって、サイバーリスクの回避は有効な戦略ではないかもしれない。そのため経営者は、効果的なサイバーリスク戦略を実施して、より警戒心を強めなければならない（例：広範な脅威の状況を包括的に監視する）。包括的なリスクモニタリングからのフィードバックは、リスク評価プロセスに反映すべきである。

新しい技術的進歩、サイバーセキュリティ評価からのフィードバック、組織の変更、リスク選好の見直し、コミュニケーションプロセスの改善および他業種や競合他社との比較は、リスクマネジメントプロセスの改善に役立つインプットの例である。例えば、人工知能やネットワークセンサーを利用したスマートファクトリーソリューションの導入を計画しているメーカーは、以前のリスク評価では、コネクテッドデバイス[i]に対するサイバー侵害の影響を考慮していなかったかもしれない。しかし、テクノロジーの変化と事業目標の変更に伴い、新たなサイバーリスクを織り込むために、リスク評価プロセスの改善が必要となる。

組織は、サイバーリスクプロファイルを変える可能性のある変化を捉えて評価するように、ガバナンスプロセスを運用しなければならない。これには少なくとも、製品やサービス、ＩＴや進化するデジタル戦略、業務プロセス、合併・買収・再編成および法律や規制について、新たな動きや変化の見込みを把握することが含まれる。これらの各事項は、広範なサイバーリスクマネジメントプログラムの中で業務を行っている、資格を持った主要なステークホルダーによって評価されなければならない。さらに、組織のサイバーリスクプロファイルに変化があるかをモニタリングする上で、主要な指標とコントロールテストの重要性は最優先事項であり続けなければならない。

絶え間なく進化するサイバー世界の混乱とデジタル化により、サイバーリスクマネジメントの変更と強化の必要性が続くため、「レビューと修正」の要素は重要である。

[i] 訳注：インターネットに接続することを前提としたデバイスや機器全般のこと。

情報、伝達および報告

原則	説明
18. 情報とテクノロジーを有効活用する	組織は、全社的リスクマネジメントをサポートするために、事業体の情報とテクノロジーシステムを有効活用する。
19. リスク情報を伝達する	組織は、全社的リスクマネジメントをサポートするために、コミュニケーション経路を利用する。
20. リスク、カルチャーおよびパフォーマンスについて報告する	組織は、リスク、カルチャーおよびパフォーマンスを複数の階層に、また、全社にわたって報告する。

組織は、ＥＲＭおよび戦略上や業務上の目標に関連する意思決定を支援するためのインプットとして、複数のテクノロジーシステムからのデータを活用している。完全で正確かつ適切な情報という要件は、さまざまな意思決定プロセスにおける経営者の見積もりや判断のベースラインとして機能するため、極めて重要である。しかし、特に侵害が適時に検出および解決されない場合、サイバーインシデントは侵害されたシステムからのデータの信頼性に影響を与える可能性がある。

さらに、リアルタイムで意思決定を行わなければならないインターネットに接続されたデジタル環境では、データの信頼性だけでなく、データを報告したり消費したりするスピードも重要な要素である。ある種のサイバーインシデントに関連する大きな脅威は、インシデントが、機動的なリスクマネジメントと戦略的な意思決定に不可欠な組織のシステムと基礎データの可用性に影響を与え得ることである。一例として、ランサムウェアはますます高度化しており、攻撃後にデータを回復するための重要なバックアップを収めたコネクテッドデバイスを含め、組織のネットワーク全体に伝播して機能を停止させる可能性がある（例：WannaCry、Ryuk）。

> ”
>
> ランサムウェアの攻撃者は、システムの脆弱性を見つけて企業と都市の両方に定期的に打撃を与えている。多くの場合、悪意のある電子メールにファイルを添付して送信し、重要なデータをロックし、復号鍵と引き換えに支払いを要求する。
>
> こうした攻撃は毎日のように行われているがその多くは公表されていない、とサイバーセキュリティの専門家は言う。地方自治体では、機器やセキュリティをアップグレードしたりバックアップデータを保護したりするためのリソースが不足している場合、特に脆弱になる可能性がある。
>
> 出典：The Wall Street Journal, “Hackers Strike Another Small Florida City, Demanding Hefty Ransom,” Jon Kamp and Scott Calv.

また、多くのソフトウェア企業が、特定のテクノロジープラットフォーム向けの標準的なコンプライアンスルールを含む、ガバナンス、リスクおよびコンプライアンス（「ＧＲＣ」）や統合リスク管理（「ＩＲＭ」）のシステムを提供していることから、組織はサイバーリスクの管理と報告を容易にする情報システムとツールを利用できる。さらに、セキュリティ情報イベント管理（「ＳＩＥＭ」）システムは、アラートをリアルタイムに解決するのに役立つイベント駆動型の通知と自動化のための有益な手段であり、重大度、インシデントタイプ、関連デバイス、発生回数等に基づいてアラートを分類して解決プロセスを支援する。

サイバーセキュリティのモニタリングと報告は、サードパーティがマネージドサービスとして提供することも可能であり、ＩＴリソースや支援ツールが限られている組織にとっては価値ある投資となり得る。ただし、サイバーセキュリティに関連する業務を外部委託する場合、組織は以下を実施することが不可欠である。

- インシデントを認識するために、サービスプロバイダと定期的にコミュニケーションをとる
- 組織の事業環境が変化し、サイバー脅威の状況が進化し続けるのに伴い、新たな脅威や潜在的な脅威について話し合う
- 重大なインシデントや侵害が発生した場合に直ちに上申するための、オープンなコミュニケーションラインを用意する

組織が機動的で、新たな脅威や発生しつつある脅威に適時かつ迅速に対処できれば、重大なサイバーイベントの影響の防止や軽減に役立つため、組織がサイバーリスクに関連する問題について社内外にコミュニケーションをとる能力は不可欠である。例えば、ほとんどの企業は、インシデント対応プログラムと並行して使用される、複数の正式に確立された内部コミュニケーションチャネルを持っている。これらのコミュニケーションチャネルは、組織の電子メールユーザに影響を与える大規模なフィッシングの試みなど、リアルタイムのイベントが検知されたときに従業員に警告するように設計されている。このような状況では、企業は、すべての電子メールユーザに状況を認識させ、疑わしい電子メールの取り扱いと報告に関する方針を強化するために、警告を発することができる。また、どの社員がこれらのメールを受信、開封または削除したかを組織が追跡できるプログラムもある。このようなメッセージは、企業内の電子メールアドレス帳に送信される電子メールキャンペーンと、企業内のイントラネットサイトに掲載される警告の両方の形で伝えることができる。組織にとっては、社内のリソースとサードパーティのサービスプロバイダ、特に組織のデータにアクセスできるサービスプロバイダとのコミュニケーションチャネルを重視することも同様に重要である。

以下の引用文は、米国証券取引委員会（ＳＥＣ）の「Interpretive Guidance on Public Company Cybersecurity Disclosures」採択に関するプレスリリースからの抜粋である。

”

ＳＥＣのジェイ・クレイトン委員長は、「これらの事項に関する当委員会の見解を示すことで、サイバーセキュリティのリスクやインシデントに関する企業のより明確で充実した開示が促進され、結果として投資家がより完全な情報を入手できるようになると確信している」と述べた。

出典：U.S. Securities and Exchange Commission,"SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures."

組織は、潜在的なサイバー脅威に十分に対処するために、ＩＴ環境内のシステムの目的だけでなく各システムに保存されている可能性のあるデータの種類についても、全体像を把握する必要がある。例えば、ある組織では、システムの変更や重要なインシデントを追跡するために、クラウドベースのチケットシステムを使用している。このチケットシステムは、取引を処理しておらず顧客データの管理にも使用していないため、経営者のＥＲＭプログラムでは重要なアプリケーションとは考えられておらず、サイバー侵害のリスクは低いと判断されている。しかし、意識の低下や研修の不足により、ユーザがチケットに添付する補助書類に機密データ、サーバのＩＰアドレス、ユーザ認証情報等が含まれている場合があれば、組織のネットワークのさまざまな侵入口を悪用される可能性がある。

また、サイバー関連事項について外部のステークホルダーとコミュニケーションできることも同様に重要である。国内外のさまざまなセキュリティ規制で概説されているコミュニケーション要件を理解することは不可欠である。適切な深度、対応および適時性でインシデントの情報公開を行わなかった場合、複数の機関から多額の罰金を科せられる可能性がある。今日の世界では、企業はテクノロジーによって、さまざまな方法で外部のステークホルダーと関わりを持つことができる。例えば、ある取引での最新の顧客体験に関してフィードバックを求める電子メールメッセージから、オンライン顧客ポータルに組み込まれた安全なメッセージ機能による支払い期限の通知、さらには個人情報に影響を与える可能性のあるデータ侵害についての郵便や電子メールによる通知に至るまでである。外部のステークホルダーとのコミュニケーションの性質、機密性および緊急性に応じて適切な方法を決定するプログラムを実行することは、企業のＥＲＭプログラム全体を実現する上で極めて重要な部分である。

組織は、サイバーインシデントに関連する情報を、他社、政府機関およびその他の規制当局に開示する際の要件についても検討する必要がある。米国では、連邦取引委員会が提供するガイダンス「Data Breach Response: A Guide for Business」で、ほとんどの州が個人情報を含むセキュリティ侵害の通知を義務づける法律を制定していることが説明されている。また、事業に基づいて適用される他の法律や規制があり得るため、影響を受ける組織は、具体的な報告と情報公開の要件について州や連邦の法律や規制を確認する責任がある[11]。さらにＳＥＣは、発行者や公開会社、投資顧問会社、ブローカーやディーラーおよび自主規制機関に向けて、さまざまなサイバーセキュリティ規制とガイダンスを発表しており、また、サイバー関連の執行措置とコンプライアンス違反に関連する罰則を担当するサイバー・ユニットと呼ばれる独立した部門を設置した[12]。ニューヨーク州金融サービス局も、多くの金融サービス会社が遵守しなければならないサイバーセキュリティ規制を設けている[13]。

組織は、ＥＲＭプログラムがサイバーリスクを十分に識別して適切に対応できるようにするために、さまざまなレベルで関連性のある適時な報告を行うための明確に定義されたプロセスを実施しなければならない。組織は、ＡＩＣＰＡのCybersecurity Risk Management Reporting Framework のような既存のルールセットを活用してベースラインを確立し、このプロセスを促進できる。報告にあたっては、関連する事実と必要な詳細レベルが関係者間で異なる可能性が高いため、特定の対象者ごと（例：情報セキュリティチーム、サイバーリスク管理チーム、経営者および取締役会）に合わせて報告しなければならない。軽微なインシデントやより詳細なインシデントデータは、情報セキュリティチームやサイバーリスクマネジメントチームに報告して定期的に解決しなければならないが、資産の損失やシステムの停止を伴うより深刻なインシデントは、経営幹部や、場合によっては取締役会に上申する必要があるかもしれない。経営者は、取締役会に伝達する事例の種類と重大度について、取締役会と細かく意思疎通すべきである。

事前に手順を定めておくと、組織がサイバーインシデントの準備と対応をする上で大いに役立つ。段階を追った手順を策定し、災害復旧イベントと同様のシミュレーション環境で手順を実施すれば、対応に要する時間と組織への影響を軽減できる。さらに、侵害がなかったからといって必ずしもサイバーリスクプログラムの十分性が証明されるわけではなく、リスクは新しいプロセスやテクノロジーの導入とともに進化し続けるため、ＥＲＭプログラムの中でサイバーリスクに関連する主要指標を定義することも同様に重要である。

> 企業がサイバーセキュリティに関連する包括的な方針と手続を採用することを奨励する。また、サイバーセキュリティの開示に関連するコントロールと手続の十分性を含め、遵守状況を定期的に評価することを推奨する。
>
> 出典：SEC's Statement and Guidance on Public Company Cybersecurity Disclosures (17 CFR Parts 229 and 249).

「情報、伝達および報告」は、サイバーインシデントの予防、検知または対応に使用できる指標を共有するための鍵となる。

結　論

サイバーセキュリティは、悪意のある行為者がサイバー攻撃の侵入口として混乱とデジタル化を利用しようとする中で進化し続けている。大手企業は、全社的サイバーリスクを管理するための体系的なアプローチを必要としている。ＣＯＳＯのＥＲＭフレームワークは、サイバーセキュリティプログラムを構築するための基盤となるものであり、サイバーリスクマネジメントの概念を戦略、事業目標およびパフォーマンスの要素と統合することで事業価値の向上につなげることができる。

本ガイダンスは、組織がサイバーリスクを識別して管理する能力を向上させるために、効果的なリスクマネジメントの 5 つの構成要素と 20 の原則がどのように活用できるかについて洞察を示している。本ガイダンスを基盤とし、前述のサイバーセキュリティフレームワーク（例：ＮＩＳＴ、ＩＳＯ、ＡＩＣＰＡ）の１つ以上を採用すると、組織は今のデジタル時代のサイバーリスクを管理する準備がより良く整えられる。

取締役会、監査委員および経営幹部などのガバナンス責任者は、トップの強い姿勢を示し、重大度と切迫感を伝え、組織のあらゆる階層でＥＲＭプログラムの現状とサイバーセキュリティ意識について疑問を投げかけることが不可欠である。サイバーディフェンスとリスクマネジメントは、全従業員と企業全体の共通の責任である。サイバー脅威は日々急速に進化して複雑さを増しているため、組織のリーダー、サードパーティのサービスプロバイダおよび従業員は、巧妙な攻撃や侵害への対応方法に備えるだけでなく、新たな脆弱性や未知の脆弱性の一歩先を行くことが求められる。従来通りのサイバーリスクマネジメントでは、これらの目標を達成することはできず、組織のあらゆる階層のステークホルダーに壊滅的なダメージを与えることになる。

付　録

サイバーセキュリティフレームワーク―実例

支援団体名	フレームワーク名	使用目的	フレームワークの説明
米国国立標準技術研究所（ＮＩＳＴ）	NIST Cybersecurity Framework	一般的な基準	Cybersecurity Framework は任意のフレームワークであり、サイバーセキュリティ関連のリスクを管理するための基準、ガイドラインおよびベストプラクティスで構成されている。Cybersecurity Framework の、優先順位づけされ、柔軟性があり、費用対効果の高いアプローチは、重要インフラおよび経済や国家安全保障にとって重要な業種の保護とレジリエンスを高めるのに役立つ。 出典：https://www.nist.gov/cyberframework
米国国土安全保障省（ＤＨＳ）The Cybersecurity and Infrastructure Security Agency（ＣＩＳＡ）	該当なし―NIST Cybersecurity Framework に基づいた業種別ガイダンス	業種固有基準と国別基準	The Cybersecurity and Infrastructure Security Agency（ＣＩＳＡ）は、サイバーセキュリティとインフラセキュリティに関する広範な知識と実務を関係者に提供し、その知識を共有することでより優れたリスクマネジメントを可能にし、それを実施することで国家の重要なリソースを保護している。 ＣＩＳＡは、NIST Cybersecurity Framework に依拠しつつ、重要インフラ業種（例：化学薬品、商業施設、重要製造業、連邦、医療・公衆衛生）に向けて業種別のガイダンスを提供している。 出典：https://www.us-cert.gov/resources/cybersecurity-framework
国際標準化機構（ＩＳＯ）	ISO 27001/2	一般的な基準	ISO / IEC JTC 1 / SC 27 規格は、情報セキュリティのための国際的な管理システム規格の開発に専念する専門家委員会を設けており、情報セキュリティ管理システム（ＩＳＭＳ）ファミリー規格としても知られている。 組織はＩＳＭＳファミリー規格を使用することにより、財務情報、知的財産および従業員情報などの情報資産または顧客やサードパーティから預かった情報のセキュリティを管理するためのフレームワークを開発して導入できる。また、これらの規格は、情報保護に適用されているＩＳＭＳの独立的評価の準備にも使用できる。 出典：https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
米国公認会計士協会（ＡＩＣＰＡ）	Cybersecurity Risk Management Reporting Framework	一般的な基準	ＡＩＣＰＡは、Cybersecurity Risk Management Reporting Framework を策定した。このフレームワークは、組織がサイバーセキュリティリスクマネジメントプログラムの有効性について関連性のある有用な情報を伝える際に役立つものである。このフレームワークは、公認会計士が組織の全社的なサイバーセキュリティリスクマネジメントプログラムを報告する、新しいＳＯＣ（System and Organization Controls）for Cybersecurity 業務の重要な構成要素である。この情報は、経営者、取締役会、アナリスト、投資家およびビジネスパートナーが組織の取組みをより良く理解するのに役立つ。 出　典：https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html
クレジットカード業界（ＰＣＩ）セキュリティ基準カウンシル	Payment Card Industry Data Security Standard (PCI DSS)	業界固有の基準	PCI Security Standards Council は、世界中の何億人もの人々の生活に関わっている。世界的な組織であり、カード会員データの安全性を確保するために、クレジットカード業界の基準を維持、進化および推進している。 支払のセキュリティの維持は、カード会員データを保存、処理または伝送するすべての事業者に求められる。支払のセキュリティを維持するためのガイダンスは、ＰＣＩセキュリティ基準に記載されている。ＰＣＩセキュリティ基準は、支払取引の受付や処理を行う組織と、支払取引に使用するアプリケーションやデバイスのソフトウェア開発者や製造者向けに、技術上と運用上の要件を定めている。 注：PCI Security Standards Council は、ＰＣＩ ＤＳＳフレームワークと NIST Cybersecurity Framework のマッピングを例示している。 出典：https://www.pcisecuritystandards.org/pci_security/

付　録（続き）

サイバーセキュリティフレームワーク―実例

支援団体名	フレームワーク名	使用目的	フレームワークの説明
HITRUST Alliance	HITRUST CSF	一般的な基準	HITRUST は、あらゆる業種のグローバル企業やサードパーティのサプライチェーン全体で、機密情報を保護し、情報リスクを管理するプログラムを支持してきた。HITRUST は、官民のプライバシー、情報セキュリティおよびリスクマネジメントのリーダーと協力して、広く採用されている共通のリスクとコンプライアンスのマネジメントフレームワーク、関連する評価およびアシュアランスの方法を開発して維持し、広く利用できるようにしている。 出典：https://hitrustalliance.net/about-us/
Center for Internet Security (formerly sponsored by SANS)	CIS Controls Version 7.1	一般的な基準	世界中の組織が、サイバー防衛力を向上させるために CIS Controls のセキュリティベストプラクティスを活用している。CIS Controls Version 7.1 では、ＣＩＳ実装グループ（ＩＧｓ）と呼ばれるコントロールの利用を優先するための新しいガイダンスを導入している。ＩＧｓは、組織が自らを分類し、CIS Controls の価値を活用しながら、セキュリティリソースと専門知識を集中させるための、シンプルで利用しやすい方法である。 出典：https://www.cisecurity.org/controls/
ＩＳＡＣＡ	COBIT 2019 – Governance & Management Objectives	一般的な基準	ＣＯＢＩＴは、情報とテクノロジーのガバナンスとマネジメントのためのフレームワークである。 ＣＯＢＩＴフレームワークでは、ガバナンスとマネジメントを明確に区別している。ガバナンスとマネジメントは、異なる活動を網羅し、異なる組織構造を必要とし、異なる目的を果たすものである。 The COBIT® 2019 Framework: Governance and Management Objectives では、40 のコアとなるガバナンスとマネジメントの目標、そこに含まれるプロセス、その他の関連構成要素を包括的に説明している。このガイドは、他の基準やフレームワークも参照している。 出典：http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx[j]
Cloud Security Alliance（ＣＳＡ）	Cloud Security Alliance Cloud Controls Matrix (CCM)	技術的な特定の基準	Cloud Security Alliance（ＣＳＡ）の Cloud Controls Matrix（ＣＣＭ）は、クラウドベンダーの指針となる基本的なセキュリティ原則を提供し、将来のクラウド利用者がクラウドプロバイダーの全体的なセキュリティリスクを評価する際に役立つように特別に設計されている。ＣＳＡ ＣＣＭ は、13 のドメインのＣＳＡガイダンスに沿ったセキュリティの概念や原則を詳細に理解するためのコントロールフレームワークを提供する。CSA Controls Matrix の基盤は、ISO 27001/27002、ＩＳＡＣＡ ＣＯＢＩＴ、ＰＣＩ、ＮＩＳＴ、Jericho Forum および NERC CIP など、業界で認められている他のセキュリティ規格や規制、コントロールフレームワークとのカスタマイズされた関係にあり、クラウド事業者が提出するサービス組織のコントロールレポートの証明において、内部統制の方向性を増強または提供する。 出典：https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

[j] 訳注：2022 年 2 月の翻訳時点でこのサイトは見つからなかった。

出　典

[1] Committee of Sponsoring Organizations of the Treadway Commission, COSO Enterprise Risk Management Framework, 2017.（邦訳は、『ＣＯＳＯ全社的リスクマネジメント―戦略およびパフォーマンスとの統合―』同文舘出版、2018 年。）

[2] Deloitte's 2019 Future of Cyber Survey, in conjunction with Wakefield Research, polled 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019, using an online survey.

[3] Khalid Kark, Caroline Brown, Jason Lewris, Bridging the boardroom's technology gap, Deloitte University Press, June 29, 2017.

[4] National Institute of Standards and Technology (NIST), "Framework for improving critical infrastrucurity," April 16, 2018.

[5] Marc Kaplan, et al., "Shape Culture, Drive Strategy," Global Human Capital Trends 2016, Deloitte University Press, 2016.

[6] Deloitte Wall Street Journal article. deloitte.wsj.com/cio/2019/ 07/11/cyber-incidents-and-breaches-the-data-dilemma/.

[7] National Institute of Standards and Technology, Cybersecurity Framework. nist.gov/cyberframework.

[8] International Organization for Standardization. iso.org/.

[9] American Institute of Certified Public Accountants, System and Organization Controls for Cybersecurity, USA, 2017. us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative[k].

[10] American Institute of Certified Public Accountants, System and Organization Controls for Cybersecurity, USA, 2017. us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative[l].

[11] Federal Trade Commission, "Data Breach Response: A Guide for Business", April 2019 ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

[12] Securities and Exchange Commission, "Spotlight on Cybersecurity, the SEC and You", retrieved September 2019, sec.gov/spotlight/cybersecurity.

[13] New York State Department of Financial Services, "Cybersecurity Requirements for Financial Services Companies", effective March 2017 dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf [m].

[k] 訳注：原文に記載されているウェブサイトは存在しなかったが、こちらのウェブサイトが該当する。
[l] 訳注：同上。
[m] 訳注：2022 年２月の翻訳時点でこのサイトは見つからなかった。

著者について

デロイト＆トウシュ社、マネージング・ディレクター、メアリー・E．ギャリガン

メアリー・ギャリガンは、デロイト社のサイバー部門のマネージング・ディレクターである。経営者が直面する危機管理の課題、特にサイバーリスクについて助言をしている。また、サイバー脅威によるビジネスへの影響を防止および軽減するためのセキュリティプログラムの開発と実施を支援している。これには、米国におけるサイバーセキュリティに関する官民の協力体制が整いつつある中での、役員教育、サイバーウォーゲームおよびその他の戦略的取組みなどがある。フォーチュン 500 企業だけでなく、非公開企業の 70 以上の取締役会にサイバー意識向上のための説明会を行ってきた。また、全米取締役協会の多数のイベントやスタンフォード大学のディレクターズカレッジでも講演を行っている。サイバーリスクや危機管理の分野でリーダーシップを発揮していることから、紙媒体とテレビの両方の報道機関から進化しつつあるサイバーイベントについて頻繁にコメントを求められている。

米国連邦捜査局（ＦＢＩ）での輝かしいキャリアを経て 2013 年に退職後、デロイト社に入社した。ニューヨーク市における国家安全保障と犯罪者のサイバー侵入に関するＦＢＩのすべての捜査を監督し、プレッシャーのかかる状況下で多くの金融機関、報道機関および法律事務所に助言を与えた。直近では、ニューヨーク事務所のサイバー・スペシャル・オペレーション担当特別捜査官として、ＦＢＩ最大の技術的･物理的な監視活動を指揮した。

2001 年 9 月 11 日のテロ事件ではＦＢＩの調査を監督し、米艦コール襲撃事件の際にはイエメンで現場指揮官の 1 人として、また、ニューヨーク市の特別イベントとＳＷＡＴを担当する特別捜査官として、危機管理の重要な経験を積んでいる。

ＦＢＩでの 25 年間の在職中に、次の指導的役割を果たした。

- 女性初のＦＢＩニューヨーク担当特別捜査官
- ＦＢＩの首席監察官
- リスク・ベースド・マネジメントに関するディレクターズ・イニシアティブの主導

フォーダム大学（ニューヨーク州ブロンクス）で学士号、ニュースクール･フォー･ソーシャル･リサーチ（ニューヨーク州ニューヨーク）で心理学の修士号､マリアン大学（ウィスコンシン州フォンデュラック）で名誉法学博士号を取得した。また、ＦＢＩ認定のクライシス・ネゴシエーターおよびクライシス・マネージャーでもある。

デロイト＆トウシュ社、パートナー、サンディ・ヘリガース

サンディ・ヘリガースは、デロイト社のグローバル・アシュアランス・マーケット・オファリングと米国のインフォメーション・テクノロジー・スペシャリスト・グループを率いている。消費財・工業製品業界と金融サービス業界における内部統制と情報セキュリティに焦点を当ててキャリアを積んできた。1998 年からリスクファイナンシャル・アドバイザリー部門に所属し、シカゴとデトロイトのオフィスで業務を行ってきた。

デロイト社の大規模かつグローバルなクライアントに対する内部統制監査サービスを担当し、全社レベル、ビジネスサイクルおよびＩＴのテストの分野を率いている。この役割には、大規模で国境を越えたデロイト社のチームを率いて、完全に外部委託された複雑で多様なＩＴ環境や急速に変化する厳しい事業環境と内部統制環境に対応するスキルが含まれる。

リーダーシップの観点からＩＴ監査サービスの品質を監督しており、最大かつ最も複雑な統合監査でＩＴと内部統制関連事項のコンサルテーションリソースとしての役割を果たしている。また、ＩＴ専門家のための監査手法、ツール、実務支援および学習方法の開発を率いている。

デロイト社を代表して、Center for Audit Quality Cyber Working Group や AICPA ASEC Cyber Security Working Group など、情報セキュリティや内部統制に関連する外部の施策にも参加している。

デロイト＆トウシュ社、マネージング・ディレクター、ケリー・ラウ

ケリー・ラウは、デロイト社のリスク・ファイナンシャル・アドバイザリー部門のマネージング・ディレクターで、アシュアランスと内部監査を専門としている。2002 年にデロイト社に入社し、内部統制やＩＴに関するさまざまな問題で企業を支援してきた。フォーチュン 500 の企業数社との契約で内部統制チームを率い、全社レベル、ビジネスサイクルおよびＩＴのコントロールの整備と運用の有効性について、理解、評価および改善してきた。また、デロイト社の全米オフィスのリーダーの一員としてＩＴ監査サービスの品質を監督しており、最大かつ最も複雑な統合監査でＩＴと内部統制関連事項のコンサルテーションリソースとして役割を果たしている。

Certified Information Systems Security Professional（ＣＩＳＳＰ）と公認情報システム監査人（ＣＩＳＡ）の資格を有しており、セントラルミシガン大学で経営学修士号と会計学学士号を取得している。

ＣＯＳＯについて

1985 年に設立されたＣＯＳＯは、５つの民間団体の共同イニシアチブであり、全社的リスクマネジメント（ＥＲＭ）、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて、先進的な考え方を提供することに取り組んでいる。ＣＯＳＯの支援団体は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）、管理会計士協会（ＩＭＡ）である。

デロイト社について

本稿で「Deloitte（デロイト社）」とは、Deloitte LLP の子会社である Deloitte & Touche LLP（デロイト＆トウシュ社）を意味する。デロイト社の法的構造の詳細については、deloitte.com/us/about を参照されたい。
一部の証明業務は、公開会社に関する会計の規則上、顧客に提供できない場合がある。

一般社団法人日本内部監査協会

内部監査および関連する諸分野についての理論および実務の研究、ならびに内部監査の品質および内部監査人の専門的能力の向上を推進するとともに、内部監査に関する知識を広く一般に普及することにより、わが国の産業、経済の健全な発展に資することを目的に活動。

また、国際的な内部監査の専門団体である内部監査人協会（The Institute of Internal Auditors：ＩＩＡ）の日本代表機関として世界的な交流活動を行うとともに、内部監査人の国際資格である " 公認内部監査人（Certified Internal Auditor：ＣＩＡ）" 等の認定試験を実施している。1957（昭和 32）年創立。

公益財団法人日本内部監査研究所

内部監査に関する研究調査を推進するとともに、わが国の内部監査の普及発展に貢献することにより、わが国経済、社会の健全な発展に資することを目的として、2020 年７月に設立。2021 年７月に公益財団法人としての認定を受け「公益財団法人日本内部監査研究所」となった。

監訳者

八田　進二　（大原大学院大学　会計研究科　教授　／　青山学院大学　名誉教授）
橋本　　尚　（青山学院大学大学院　会計プロフェッション研究科　教授）

訳　者

堺　　咲子　（内部監査人協会（ＩＩＡ）国際本部理事　専門職資格担当　／　インフィニティコンサルティング　代表　／
プレミアアンチエイジング株式会社　社外取締役　／　ＣＩＡ，ＣＲＭＡ，ＣＣＳＡ，ＣＦＳＡ）

ガバナンスと全社的リスクマネジメント

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

デジタル時代のサイバーリスクマネジメント

COSO

トレッドウェイ委員会支援組織委員会

coso.org