内部監査人協会（ＩＩＡ）情報

グローバルな視点と洞察　第４号

信頼されるサイバー・アドバイザーとしての内部監査

内部監査人協会（ＩＩＡ）
訳者：桜　井　淳　一
損害保険ジャパン日本興亜株式会社　内部監査部部長、理事
大　野　陽　生
損害保険ジャパン日本興亜株式会社　内部監査部特命課長

目　次

寄稿者
南アフリカ共和国
ケープタウン市
内部監査部門長
CIA
Lindiwe Ndaba氏
情報システム 上席監査マネージャー
CIA, CCSA, CISA
Etienne Postings氏
情報システム ディレクター
Andre Stelzner氏
南アフリカ共和国
ファーストランド社
内部監査部門長
CIA, QIAL, CA（SA）
Jenitha John氏
オーストラリア連邦
インシュアランス・オーストラリア・グループ
最高情報セキュリティ責任者
Jeff Jacobs氏
内部監査部門長
Lee Sullivan氏
アメリカ合衆国
RSM US 社
セキュリティ・プライバシーリーダー
Daimon Geopfert氏
サウジアラビア王国
サウジ基礎産業公社（SABIC）
副社長兼内部監査部門長
CISA
Gregory Grocholski氏

アメリカ合衆国
内部監査人協会（ＩＩＡ）
内部監査部門長
CIA, CRMA, CFE, CGFM
Greg Jaynes氏
副事務総長兼最高情報責任者
Charles Redding氏
コロンビア共和国
ロス・アンデス大学法学部 特別教授
CFE, COBIT5 ファンデーション認定
Jeimy Cano氏
アメリカ合衆国
バージニア大学
最高情報セキュリティ責任者
Jason Belford氏
ＩＴ監査ディレクター
CISA, CRISC
Gerald Cannon氏
最高情報責任者
Virginia Evans氏
ＩＴ統括責任者
Ron Hutchins氏
内部監査部門長
CIA, CRMA, CPA
Carolyn Saint氏

諮問委員会

ＩＩＡマレーシア
CIA,CCSA, CFSA, CGAP, CRMA
Nur Hayati Baharuddin氏
ＩＩＡアフリカ地域連合
CIA, QIAL
Lesedi Lesetedi氏
ＩＩＡオランダ
CIA, CCSA, CGAP
Hans Nieuwlands氏
ＩＩＡアラブ首長国連邦
CIA, CCSA, CRMA
Karem Obeid氏
ＩＩＡ北米
CIA, CRMA, CPA
Carolyn Saint氏
ＩＩＡコロンビア
CIA, CCSA, CRMA
Ana Cristina Zambrano Preciado氏

信頼されるサイバー・アドバイザーとしての内部監査

サイバーセキュリティリスクは複雑で変化が激しいため、すべてを知ることは現実的ではないが、内部監査部門長（ＣＡＥ）は、サイバーセキュリティに精通していることが必須になってきている。実際、サイバーセキュリティのリスクとエクスポージャー（訳注：リスクに晒されている度合い）が変化していくことを考えると、有能なＣＡＥは、この注目されており難易度が高い領域において、内部監査を組織の信頼されるアドバイザーに位置付けるだろう。

衝撃的な統計

2015年の、情報漏えい対応の平均総費用は379万米ドルで、2014年の352万米ドルから増えており、2013年からは23％増加している。情報漏えい対応の費用は、急速な顧客離れを招き、顧客を取り戻す活動が必要になり、また評判や信用を失う[1]。

攻撃者は検知されるまで、平均で205日間も組織の環境にアクセスしていた。さらに69％の組織は、内部ではなく外部から攻撃を受けていた[2]。

2015年の上半期には、公表された888件のインシデントにおいて、約２億4,600万件のレコードが侵害された。これらの公表されたインシデントの少なくとも半分では、侵害さ

[1] IBM and Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, based on a study of 350 companies from 11 countries.
[2] Mandiant, “M-Trends 2015: A View from the Front Lines,” based on a distillation of Mandiant’s incident response investigations in more than 30 industry sectors.

れたレコードの件数は測定できなかった[3]。

侵害は世界中で発生している。2015年の上半期、多くは北米で発生しており（707件のインシデント）、続いて英国（94件）、アジア（63件）だった。トップ10の侵害のうち、５つは米国以外の会社だ[4]。

上記のような統計を前にして、ＲＳＡ社の社長であるAmit Yoran氏が、「（サイバー）セキュリティ業界は期待に応えていない」と述べたのは無理もない[5]。

サイバーセキュリティの重要性を疑う者はいない。インターネットに接続しているシステムは、データ損失、破壊、不正アクセス、誤操作からデータを保護する対策をとっている。頭が良く分別のある人たちの多くが、何年もの間この問題に、重点的に取り組んできた。その人たちの予想は現実的だ。サイバー攻撃を完全に根絶できるとは考えていない。

ロス・アンデス大学の法学部特別教授であるJeimy Cano氏は指摘する。「今日のデジタル環境で、『損失は避けられない』」。サイバーセキュリティは、損失を最小化するゲームだ。このゲームのゴールは、攻撃を最大限に防御し、かつ防御が突破される前提で、重要資産へ攻撃者が到達する前に発見することだ。

チームの取り組み

サイバーセキュリティ対策は、専門家だけのタスクではない。包括的に考慮しなければならない。対策に失敗した際の影響は、最低限必要な業務処理の停止や、知的資産の損失、信用失墜に及ぶ。サイバーセキュリティ対策は、テクノロジーリスクにとどまらず、ビジネスリスクであり、内部監査人が重要な役割を果たす。サイバーセキュリティ対策の成功は、ＣＡＥがアプローチするだけでなく、取締役会や監査委員会がいかに注力するかにかかっている。サイバーセキュリティ監査が、計画通りに実施されていることを確認するだけではなく、将来を見据えた、戦略的な、考え抜かれたリーダーシップを経営層に提案することによって、サイバーセキュリティは、ＣＡＥが信頼されるアドバイザーであることを証明する重要な機会となる。そのためには、サイバーセキュリティリスク、ビジネス戦略・信用への影響を識別し、経営層や役員へ適時かつ適格な討議を促し、善管注意義務の遂行を促す必要がある。

ＣＡＥが十分にその役割を果たすためには、最高情報責任者（ＣＩＯ）及び最高情報セキュリティ責任者（ＣＩＳＯ）と生産的かつ高度な協調関係を築くことが必要だ。そのような関係構築が、セキュリティチームやＩＴチームが要望していること、及び内部監査が提供できることの相互理解を促すことに寄与する。ファーストランド社のＣＡＥであるJenitha John氏によれば、ＣＩＳＯは、現在の動向と事象、世間一般で新しく発生している問題についての率直かつ先を見越した視点、つまり信頼されるアドバイザーとして将来を考慮した視点を内部監査に期待している。John氏は、「組織が直面している現在のエクスポージャーと影響に関する課題を、内部監査が明確に伝える」必要があると考えている。

ＩＩＡの副事務総長兼ＣＩＯのCharles Redding氏によると、ＣＩＯが必要としているものは、ＣＩＳＯと類似しているが異なる。ＣＩＯはテクニカル面からサイバーセキュリティに目を向けがちだ。内部監査は、経営層の「リスクを評価し、あるべきリスク許

[3] Gemalto, Breach Level Index (BLI), a database that records all publicly reported global breaches.
[4] Ibid.
[5] Hackett, R.; "'Security Has Failed': Exclusive Preview of RSA President's Conference Preview," Fortune, April 21, 2015.

容度を定義する手助けをしてほしい」という情報を提供することによって、ＣＩＯの視野を拡げる。Redding氏がコメントしている内部監査機能は、ＩＩＡのＣＡＥであるGreg Jaynes氏が率いている。Jaynes氏は「Charlesと私が一緒に執務場所にいたとき、リスクとサイバーセキュリティについて話さなかったことは一日もなかった。ＣＩＯと十分に対話しないで、有能なＣＡＥでいられるだろうか」とコメントしているように、内部監査とＣＩＯの協力関係を確固としたものにしている。

サウジ基礎産業公社（ＳＡＢＩＣ）の副社長兼ＣＡＥであるGregory Grocholski氏は、チームの取り組みの重要性に同意する。しかし、サイバーセキュリティに関連するＣＡＥの役割は、協力関係を促進することより、若干踏み込んだものだと指摘する。ＣＡＥは、構造モデル（開発されたアプリケーション）と非構造モデル（Excel、Wordなど）の中にあるデータを理解している必要がある。両方とも攻撃者が興味を惹くものかもしれない。

ＣＡＥは、組織への出入口であるすべてのサイバー経路を熟知している必要がある。組織のすべての階層で、サイバー経路について必要性、適切なコントロール、リスクによる影響度、リスク許容度を適切に検討していることを確認する。いかなるときでも、ＣＡＥは何か発生したときの準備だけでなく、未然防止にも注力すべきだ。

トップの支援

事実上、あらゆる組織、あらゆる重要なプロジェクトにとって、トップの積極的な関与が不可欠だ。しかし、経営層は、サイバーセキュリティへの取り組みへの全面的な支援には消極的だ。最近のある調査によると、26％のＣＩＳＯや最高セキュリティ責任者（ＣＳＯ）は、セキュリティについて経営層向けに年１回しか報告していない。まったく報告していないのは、ほぼ同じ割合（28％）だ。約３分の１は、取締役会や取締役は、サイバーリスクに関与してないとしている。監査委員会がサイバーリスクに関与している割合は15％に過ぎない[6]。

しかし、旧来のサイバーセキュリティへの消極的な姿勢は、姿を消しつつあるようだ。

経営層は、サイバーセキュリティと組織内の関連リスクについて、今まで以上の情報を要求し始めている。これは、経営層がサイバー攻撃による潜在的な損害度合いを理解しただけでなく、規制への対応が念頭にあるためだ。2014年６月に証券取引委員会のコミッショナーであるLuis Aguilar氏が発表した「サイバーリスク・マネジメントへの経営層による監督が、サイバー攻撃で生じうる損害を適切に防御・準備するうえで非常に重要だ。（中略）経営層が、サイバーセキュリティの監督責任の重要性に見向きもしなかったり、軽視したりするのであれば、危険を覚悟する必要がある」[7]。

取締役会、監査委員会、経営層は、責任を果たすために情報が必要だ。経営層との接点という特権を有する内部監査人こそが、経営課題であるサイバーセキュリティの維持に関与できる。ＣＡＥの役割は明確であるとファーストランド社のJohn氏は確信している。「ＣＡＥは発見事項を正しいガバナンスのレベルに適切に位置付けることで、必要不可欠な注意を受け取り、最新の改善状況を把握する必要がある」。インシュアランス・オーストラリア・グループ（ＩＡＧ）のＣＡＥであるLee Sullivan氏は、自身の報告が取締役会に『サイバー脅威へのＩＡＧの対応能力につい

[6] PwC, “US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey,” July 2015.
[7] Security Intelligence, “Why is Your Board of Directors Finally Asking about Cyber Risks?,” October 13, 2015.

て客観的な視点』を提供していると述べる。

ＣＡＥは、来る法規制改定、あらたな保険引受ニーズへの要請、新種の集団訴訟のような業界の動向、その動向を監査範囲を決める際に考慮する方法に注目することで、サイバーセキュリティに関する報告において、自分が最も効果を発揮できる立場になれることを理解しているだろう。ＣＡＥは、適切な要員とチーム（例えばインシデント対応チーム、及びリスクを評価する第三者機関）がサイバーセキュリティの専門領域に対処していることをアシュアランス（訳注：客観的に検証）できたらいいと考えているかもしれない。

ＣＡＥは、進行中のサイバーセキュリティ・プロジェクトへ提言する義務がある。すなわち、それらのプロジェクトが直面しているリスクを効果的に低減しているか、最重要なリスクに集中して対応することについて資源を効率的に活用しているか、脅威を防御・検知するために十分に強健かつ厳格であるかについて、提言する義務を負う。バージニア大学のＣＡＥであるCarolyn Saint氏は次のように述べた。サイバーセキュリティへの内部監査の関与が、組織の最高レベルで沸き起こっているニーズに付言することによって、経営層の取り組みの有益性を補強する。

関連諸問題

サイバーセキュリティ特有の課題は、サイバーレジリエンス（訳注：サイバー攻撃を受けた際に元の状態に復旧するための回復力）に収斂する。絶え間ないサイバー攻撃に対応するために、インシデント発生前・発生中・発生後に、インフォメーション及びコミュニケーションのシステム（及びそれに依存するもの）の回復力を強化することだ。サイバーレジリエンスは、全従業員のサイバーセキュリティに関する知識や意識を改善することも含む。その結果として、従業員が関連リスクの性質や影響をより深く理解し、かつサイバー攻撃への強固な防御前線の構築につながる。ＣＡＥは、内部監査スタッフがサイバーセキュリティの知識や意識を向上させるよう導く。ＩＩＡの内部監査に関する2016年の北米調査によると、内部監査スタッフのサイバーセキュリティに関する専門知識の欠如は、サイバーセキュリティリスク監査の対処能力に影響する最大の障害だ[8]。

バージニア大学のＣＩＳＯであるJason Belford氏は、サイバーレジリエンスをサイバーセキュリティの基本的な理念であり、個別に対応するものだとみなしている。同大学のＩＴ統括責任者であるRon Hutchins氏は同意する。「高い可用性と信頼性を目指している。しかし、すべてのサービスが同じレベルの防御を必要とはしていないと理解している」。

さらに、ケープタウン市（南アフリカ共和国）の情報システム・ディレクターであるAndre Stelzner氏は、その概念を総括する。明らかに、堅牢かつレジリエントであるための最良の方法は、自分たちの脆弱性と脆弱性の低減方法を知ること、及びサイバー攻撃に対応・復旧するための計画を策定することから始まる。

プライバシーと機密性も、取り扱われているデータの種類、保存場所、アクセスする人とその方法という点において、サイバーセキュリティの主な要素だ。

インシュアランス・オーストラリア・グループでは、顧客からの信頼を維持することが非常に重要であるため、最高顧客責任者（ＣＣＯ）は、プライバシー責任者及びＣＩＳＯと協力して、顧客データを保護している。多くの組織で、プライバシー部門は、関連する基準の定義を支援し、方針と手続を策定する。

[8] The IIA, “2016 North American Pulse of Internal Audit,” February 2016.

また、従業員へのサイバーセキュリティに関する教育にも責任を持つことがある。

内部監査は、主要なステークホルダーとしてプライバシーに関する責任を認識すべきであり、また、プライバシー関連規制への準拠は、関連するすべての監査の主要な要素になるべきだ。プライバシー部門への調査と観察で、組織のサイバーセキュリティ対策の成熟度に関するさらなる手がかりを得られる。データオーナー、テクノロジーオーナー、プライバシーチーム／法務チームは、組織が展開しているフレームワークの中で、相互に対話し、協力し合うべきだ。もしそうしていなければ、問題として調査する価値があるだろう。

まとめ

ＣＡＥ、情報技術担当役員、セキュリティ担当役員の視点は明確だ。サイバーセキュリティは今そこにある課題だ。Cano氏（ロス・アンデス大学法学部 特別教授）によると、「新しい産業革命であり、デジタル・破壊・レジリエントが主流となった新時代の変革だ」。情報漏えいの新しい教訓になることを避けたい事業体は、適切な専門知識を獲得し、防御対策に投資し、関連規制を遵守し、全世界のサイバーセキュリティに関する動向を把握し、すべての利害関係者にデータ侵害やデータ損失の徹底的な防止に取り組むことを保証しなくてはいけない。目的を果たすには継続的な取り組みが必要だ。

ＣＡＥには、信頼されるアドバイザーの役割を果たすために、成果をもたらすための重要な役割がある。ＣＡＥは、サイバーセキュリティの専門知識を獲得・実証し、信頼を築くことや、政治的に配慮した適時的確な質疑応答を適切な識者と実施することでこの役割を果たす。組織は、サイバーセキュリティに関する一貫性のある価値観をはっきりと示しているか？　方針と手続は、価値観に基づいて策定されているか？　他組織は何をしているか、他組織と比較してどうか？　問いかける際には、解決策を見つけるために、積極的かつ油断のない傾聴、業界知識、ビジネスセンス、テクノロジーへの知見等を併せて活用する必要がある。

サイバーセキュリティを成功させるためには、企業データを狙う攻撃者が組織内外の両方にいることを理解する必要がある。攻撃は止まらない。Grocholski氏（サウジ基礎産業公社　ＣＡＥ）の言葉は現実を的確に表現している。「私たちはデジタル世界に住んでいる」。「自分の家と家族を守るように、組織の資産を防御する」。

より詳しい情報の参照先

- International Organization for Standardization, “ISO/IEC 27001 – Information security management,” 2013（www.iso.org）
- National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” February 2014（www.nist.gov）
- Privacy by Design,（www.ipc.on.ca/english/Privacy/Introduction-to-PbD）
- The IIA, “Cybersecurity: Keeping IP Under Lock and Key,” Tone at the Top, February 2014（www.globaliia.org/Tone-at-the-Top）
- The IIA, “The Cybersecurity Imperative,” Internal Auditor, August 2015（https://iaonline.theiia.org）
- The IIA, “Logging In: Auditing Cybersecurity in an Unsecure World,” 2016（www.theiia.org/AuditingCybersecurity）

別紙１

有能なＣＡＥは、アドバイザーとして利害関係者との関係を構築しており、存在感を示している

インシュアランス・オーストラリア・グループ

インシュアランス・オーストラリア・グループ（ＩＡＧ）では、ＣＩＳＯであるJeff Jacobs氏に、サイバーセキュリティ管理全般への説明責任がある。ＩＡＧにおけるサイバーセキュリティリスクを低減するために、Jeff Jacobs氏は、ＣＡＥであるLee Sullivan氏、第２のディフェンスラインのリスクチーム、プライバシー担当チームと協力して仕事をしている。

Lee Sullivan氏とJeff Jacobs氏は、サイバーセキュリティ戦略策定で最近協働した。Jacob氏が戦略策定を主導した。戦略には、現状能力の評価、新たなリスクの明示、規範の骨子とリスクに対処するための詳細な工程表・計画を記載した。Sullivan氏は、戦略策定後すぐに、その結果について、客観的にレビューするためのチームを結成した。２人は経営層や取締役会に同じ言葉やメッセージで伝えるために、サイバーセキュリティに関する同一のフレームワークを使うことに同意し、レビュープロセスを通して協力した。

戦略における課題としては次のようなものがある。

- ■基本を正しく理解することの重要さ：最たる例は、サイバーセキュリティの観点で許容可能とそうでないものの判断に関して組織を導く原則。
- ■単に防御に注力するのではなく、検知と的確な対応を強化する必要性（方向性に注力するだけではなく、方向性を強化し対応する必要がある）：ツールに投資することで組織を守れるというのは、すでに古い考え方だ。実際のところはJacob氏によると、「完全には防御できないので、検知能力、侵害された際の対応能力を今以上に高める必要がある」。
- ■設計段階からのサイバーセキュリティ対応：サイバーセキュリティ対策の後付がとても多い。設計や開発の最初の段階からセキュリティ対策を組み込むことが必須だ。
- ■サイバーセキュリティに関する意識：最善のテクノロジー、プロセス、専門家が揃っていたとしても、最も狙われるのはいつも人が原因のセキュリティ・ホールだ。解決策はセキュリティについて従業員に考えさせることだ。そうすることで、危険に関する意識を向上させ、脅威へ適切に対応できるようになる。

ＩＡＧには、外部からの脅威が日々増大かつ高度化しているという共通認識がある。そのため、サイバー脅威に関する十分なフレームワークで対応する必要がある。一方、サイバー戦略における他の部分と違って、サイバー対応能力を向上させるための必要な投資額は必ずしも明確ではない。サイバーセキュリティに注力することで、デジタルによる変革が予定より遅れるという懸念もある。Jacob氏は異議を唱える。「いずれかが重要ということではなく、両方をどのように実施するかが重要だ」。

バージニア大学

バージニア大学のＣＡＥであるCarolyn Saint氏、ＣＩＯであるVirginia Evans氏、ＣＩＳＯであるJason Belford氏、ＩＴ責任者のRon Hutchins氏、ＩＴ監査ディレクターのGerald Cannon氏は、Hutchins氏のいう『一般的に最もよく使われている３つの対策』というサイバーセキュリティへの取り組み方に注目している。方針を策定すること、方針を実行すること、方針の順守状況を監査することだ。重要なことは、各段階のすべての部署

が独立していつつも、協働していることだ。Evans氏が述べるように、「サイバーセキュリティ対策がうまくいくただ一つの方法は、チームとして機能するかどうかだ」。

Saint氏は、サイバーセキュリティの取り組みを包括的・標準的にカバーし、コントロールが存在するかだけではなく、コントロールの有効性も評価するために、内部監査に、フレームワーク・アプローチを用いている。Evans氏は「以前の監査チームは、完全に準拠性だけを評価した。今はリスクの予見に比重を置いている」と明言している。

Belford氏、Hutchins氏、Evans氏の３人は、内部監査が協働・コンサルティングの役割を担うことは非常に有益であることで意見が一致している。Belford氏がいうところの「悪く見えるようにする方法を探す」という内部監査の従来の評価ではなく、『一緒に課題を解決する』という意味での、パートナーシップ・アプローチに３人はより注目している。

Saint氏は、ＣＩＯとＣＩＳＯにとってサイバーセキュリティにおける内部監査の役割と価値における懸念事項は教育だが、それをＣＡＥの責任の一つであると考えている。Saint氏は付け加える。「ＣＡＥの役割の一つは、リスクが組織のあらゆるレベルの課題として認識されている状態にすることだ」。

バージニア大学は、米国の規制への準拠に取り組んでいる。連邦情報セキュリティ管理法（ＦＩＳＭＡ）に大学が準拠するための現在の課題は、通常のサイバーセキュリティの取り組みを超えて、チームと他のクロスファンクショナルチームを結びつけることである。進捗はしているが、ＦＩＳＭＡの規制要件を充足し、かつ測定可能な環境を構築するという、計画的な取り組みは骨が折れる。

それでも、複合的な取り組みは実行されている。Saint氏が指摘するように、「サイバーは、すべての内部監査計画においてトップリスクであり、多分、この先何年もそうだろう」。

ケープタウン市

ケープタウン市（南アフリカ共和国）のチームは、リスクを低減するコントロールより、テクノロジーが常に速く変化していることを認識している。そのため、防御・検知・是正する対策へ投資し続ける必要がある。それでも、攻撃を回避できる保証はない。成功させるには、チームが侵害を迅速に検知し、効果的・効率的・経済的に脅威を低減できるか次第だ。

チームは、ＣＡＥであるLindiwe Ndaba氏、情報システムの上席監査マネージャーであるEtienne Postings氏、情報システム・ディレクターであるAndre Stelzner氏の３人で構成されている。サイバーセキュリティへはリスクベースで取り組んでいる。最初に、多様な情報源、アシュアランス提供者が確認した自組織におけるＩＴリスクの種類を見極める。ＩＴ監査とＣＩＯで、自組織におけるサイバーリスクの動向、関連する外部組織のリスク、組織に影響を与えうる一般的な動向に関して詳しく協議し、ＩＴリスクを補完する。

Stelzner氏は、サイバーセキュリティ対策において、チーム全員が各自の強みを発揮する必要があると言う。そのため、内部監査は、組織の安全状況についての独立したアシュアランス提供者であり、脅威を低減するためにＩＴ部門が導入する方針・システム・サービスをレビューする必要がある。情報システム・ディレクターは現時点では以下を認めている。「ある程度達成しているが、自分たちのＩＴに関する方針への順守状況を評価するだけのレベルで、導入したセキュリティ対策への総当り攻撃テストのようなものではない」。

チームに関与することが、内部監査とセキュリティチームでの協働につながる。内部監査人が、課題を検討し、解決方法を策定するセキュリティ会議に出席する。全員が同じゴールに向かう。可能な限り堅牢なタスク、シ

ステム、プロセスを策定する。

継続的な内部監査の計画におけるサイバーセキュリティの重要さを述べたSaint氏のコメントが繰り返されると、Ndaba氏とPostings氏は確信している。「サイバーセキュリティとＩＴ監査は、常に内部監査の戦略において絶対に必要な課題だ」。

別紙２

信頼されるサイバー・アドバイザーでいる

信頼されるサイバー・アドバイザーとして、ＣＡＥは、組織の変革を促す立場にある。啓蒙と周知、リスク・マネジメント、アシュアランスに注力することは、ＣＡＥが信頼されるサイバー・アドバイザーとして成長する一助となる。

	信頼されるサイバー・アドバイザーとして基礎的なレベル	必要十分なレベル
啓蒙と周知	サイバーセキュリティの概念、仕組み、構成要素を理解する。	❑ 現在のＩＴ監査機能を拡張し、サイバーセキュリティに関して、先を見通した実行可能な洞察を提示する。 ❑ 来る法規制改定、新たな保険引受ニーズへの要請、新種の集団訴訟、その他動向に関する優れた業務知識を維持する。 ❑ 監査プログラムに上記の動向を取り入れる。
	サイバーに関する意識を啓蒙するために、組織内の適切な機能と協働する。	❑ サイバーにおける役割と責任に関して、各リーダーに戦略的なアドバイスを提供する。
	ＩＴスタッフだけにサイバーセキュリティの専門知識を期待する。	❑ 効果的なタレント・マネジメント／専門能力育成プログラムにより、ＣＡＥとスタッフにサイバーセキュリティに関する能力を身につけさせる。 ❑ コソース（共同実施）を戦略的に活用し、適切な人材・専門性を必要なときに使えるようにする。
リスク・マネジメント	リスク評価で組織におけるサイバーリスクの発生可能性と潜在的な影響を見極める。	❑ サイバーセキュリティにおける過失の頻度と影響度を継続して確認する。 ❑ サイバー脅威による組織の最大損失を確認し、監査計画に織り込む。 ❑ 新たなサイバーセキュリティリスクを積極的に把握する。
	組織のサイバーセキュリティ対策、及び関連リスクを低減するための計画と実施状況を把握する。	❑ サイバー脅威へ対応するための組織のリスク対応態勢を把握する。 ❑ サイバーセキュリティの経営層によるコントロールについて、妥当性と有効性を継続して監査する。
	第三者機関による監査報告書をレビューする。	❑ ＣＩＯやＣＩＳＯと連携して、第三者機関の候補を評価する。 ❑ 第三者機関の候補に関するリスク特性を進言する。 ❑ サイバーセキュリティに関する戦略や価値観に、契約している第三者機関が合致しているかアドバイスする。

	信頼されるサイバー・アドバイザーとして基礎的なレベル	必要十分なレベル
アシュアランス	サイバー関連の方針や手続を順守しているか評価する。	❑ 方針や手続の策定前に、サイバーセキュリティ戦略を独立した立場でレビューする。 ❑ サイバーリスクを後付けするのではなく、最初から取り組むように、テクノロジープロジェクト推進チームの一部を担う。 ❑ 関連するフレームワークに基づき、方針や手続の十分性と有効性を評価しテストする。
	従業員へのサイバーセキュリティ訓練が必要な要件を満たしているか評価する。	❑ 訓練の成果と保有知識を評価する。 ❑ 訓練がサイバーセキュリティ戦略と本質的に合致しているか洞察を提供する。
	サイバーセキュリティ・プログラムへのアシュアランスを提供する。	❑ 中立性を維持する一方で、第１及び第２のディフェンスラインにおける豊富な人材と一緒に、内部監査の機能を活用する。 ❑ サイバーセキュリティにおける３つのディフェンスラインが協働するようリードする。
	インシデント対応、復旧、事業継続計画においてアシュアランスを提供する。	❑ 計画の進行管理とビジネス戦略との整合性について洞察を提供する。 ❑ 必要に応じて、内部監査スタッフが危機的な状況にいつでも介入し支援できるように準備する。
	サイバーセキュリティへの取り組み結果を経営層及び取締役会／監査委員会へ報告する。	❑ 経営層及び取締役会／監査委員会と先を見据えて議論し、サイバー攻撃に対する組織の脆弱な面について十分に検討するように支援する。 ❑ サイバーセキュリティに関する組織のリスク選好（訳注：リスクを積極的にとる度合い）を設定するプロセスについて、アドバイス・支援する。