AVIATION ISAC

CISO 調査結果

2025

CONTENTS

エグゼクティブサマリー

航空 ISAC が 2 度目の 10 年を迎えるにあたり、航空サイバーリスク調査の第 8 版を発表する。 今年の調査結果は、米国国立科学研究所（NIST）のサイバーセキュリティ枠組み（CSF）バージョン 2.0 の更新版にマッピングされている。

この調査の目的は、業界の CISO が戦略、プログラムの成熟度、リソースの管理をベンチマークするためのツールを提供することである。また、航空 ISAC のスタッフは、この情報を活用し、来年度メンバーが重点的に取り組む分野に力を注ぐ。

調査結果に先立ち、我々は航空業界のサイバー脅威の状況について TLP クリア版を再度掲載した。様々な動機を持つサイバー脅威アクターが、デジタルインフラやソフトウェア主導の技術への攻撃を通じて、航空エコシステムを混乱させたり、劣化させたりしようとしているのが引き続き見られる。新たな技術機能が航空業界に導入され、業界が力強い成長を続けるにつれ、攻撃対象は拡大し続けている。サイバー攻撃者は、ゼロデイを開発し、侵害からネットワーク内で影響力のある行動を起こすまでの時間を短縮することに熟練してきている。

アイデンティティ管理、認証／アクセス制御は、引き続き航空業界の CISO の関心の的となっている。ガバナンスは、NIST CSF 2.0 の新しい機能であり、今回の調査では、組織的背景とサプライチェーンリスクマネジメントという 2 つのガバナンスカテゴリーが上位 5 つの関心分野に入っている。資産管理と継続的モニタリングが上位 5 位を占めた。また、量子コンピューティングが当初の予想よりも早く実現する可能性があるとの報告もあり、新たな懸念事項が浮上した。

調査にご協力いただいた皆様に感謝する。この情報が、航空業界に対するサイバー攻撃が増加の一途をたどる中、航空業界のレジリエンスを強化するための戦略立案や取り組みの優先順位付けの指針や洞察となれば幸いである。

ジェフリー・トロイ

社長兼 CEO

航空 ISAC

脅威ランドスケープ

過去 10 年間、サイバー脅威アクターは世界の商業航空システムに悪影響を与える能力を実証してきた。航空会社や空港運営会社、航空機製造事業者、衛星会社、そしてそれらを支える複雑な航空サプライチェーンは、今後も標的にされ続けるだろう。一部の企業は、重大な業務妨害、機密データの損失、財務上の損失を経験している。Aviation ISAC による本報告書は、航空部門に影響を与える様々なタイプの悪意あるサイバーインシデントがもたらすリスクの概要を提供している。

民間航空セクターを標的にしているサイバー脅威アクターは 3 種類ある：国家による高度持続的脅威（APT）グループ、組織化されたサイバー犯罪グループ、ハクティビストである。

民間航空セクターを支える大規模かつ成長中のデジタル・インフラは、攻撃者に広範かつ広範なサイバー攻撃対象領域を提供する。さらに、マネージドサービス・プロバイダー（MSP）やクラウドサービス・プロバイダーへの依存度が高まっているため、これらのプロバイダが悪意のあるサイバー脅威者に狙われた場合、間接的なデータ侵害のリスクが高まる。

サイバー脅威者は、これらの脆弱性を十分に緩和していない組織の既知のコンピュータの脆弱性を悪用し続けているが、ゼロデイ脆弱性が公表される前にそれを発見し、悪用することにもますます長けてきている。また、サイバー脅威アクターは、従来のシグネチャベースの侵入検知システムを回避し、LOTL（Living-of-the-Land）戦術によってネットワークの永続性を維持する能力も格段に向上している。

航空 ISAC は、一部のサイバー脅威者は、世界の民間航空部門に深刻な、しかし局地的な混乱を与える能力を有している可能性が高いとアセスメントしている。

東欧、極東、中東地域における高い地域緊張は、これらの地域から発信される悪意あるサイバー活動を増加させる原動力となっている。加えて、地域紛争は、民間航空便に影響を与える GPS 妨害/なりすましの増加や、偶発的な運動攻撃のリスクの増加につながっている。

アンケート結果

どうやってデータを入手するのか？

私たちは毎年、当コミュニティの CISO を対象に、新年に向けてサイバーリスク削減のための戦略を把握するための調査を行っている。この調査では、"サイバー・リスクを削減するために 2025 年に実行することを約束した 3～5 つのことは何ですか？"というたった 1 つの質問を投げかけている。

データをどのように分析するのか？

回答は、国立標準技術研究所のサイバーセキュリティ枠組み（NIST CSF 2.0）を用いて分類されている。回答を集計し、サイバーセキュリティの取り組みがどこに重点を置いているかをまとめた。その結果を、CISO のナラティブのハイライトとともに紹介する。

26%の会員が毎年恒例の 1 つの質問に回答してくれた。設問は、ネットワーク、OT、IoT、そして製品開発において、会員がセキュアな環境を構築するために避けて通れない大きな岩石を引き出そうとするものである。その結果をいくつかの観点から集計・分析した。機能別（ガバナンス、識別、防御、検知、対応、回復）、カテゴリー別、サブカテゴリー別に回答全体を見た。

我々は何を学んだのか？

2025 年の結果は、NIST CSF の更新が非常に必要であったことを反映している。回答のうち 31%は、業界全体におけるガバナンスの必要性を反映している。ガバナンス作業は、例年確実に行われていた。しかし、ガバナンス作業は NIST CSF 1.0 の他の 5 つの機能の下にカテゴリーまたはサブカテゴリーとして組み込まれていたため、その作業の普及は覆い隠されていた。ガバナンスは、すべての企業の C レベルにおいて所有されている。今年の調査結果で、ガバナンスの取り組みがこれほど重要なレベルで強調されていることを見ると、航空業界のすべての機能において、すべての経営幹部が、それらのビジネス機能におけるサイバーセキュリティのオーナーシップを認識していることの重要性が浮き彫りになる。ガバナンスの取り組みの多くは、企業が規制要件を満たしていることを確認するためのサイバーセキュリティポリシーの作成、サプライチェーンリスクの低減、サイバーリスクをより適切にマネジメントするためのビジネス機能の必要性の喚起であった。

例年通り、「防御」と「識別」の機能が重視される分野として上位に並んだ。防御に関する取り組みは、2024 年よりも 2025 年の方がより多く言及されている。ガバナンス・イニシアチブは、これまで防御に割り当てられていたスペースの多くを占めた。

と識別機能は、他の機能よりも高かった。興味深いことに、検知イニシアチブは 2025 年においても 18%と一貫しており、2024 年に呼びかけられたものよりもわずかに多かった。

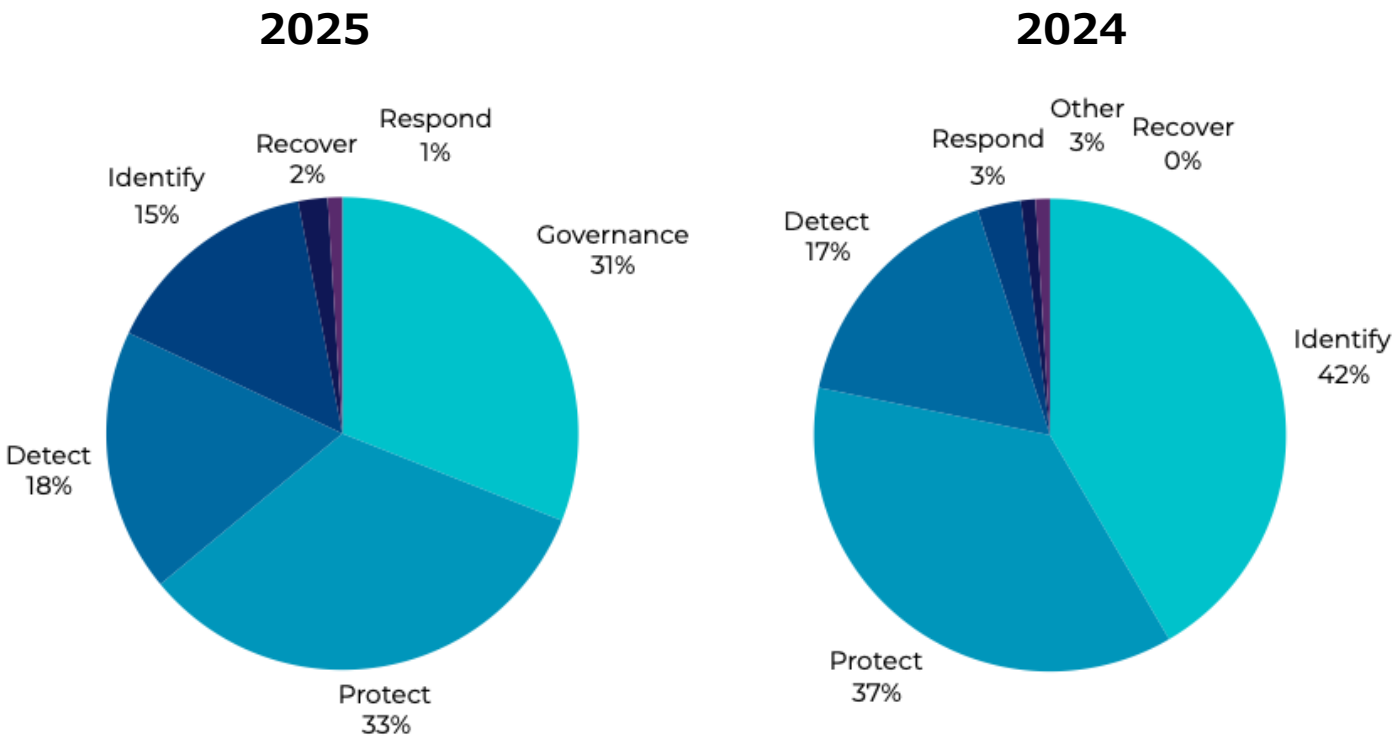


図 *2 2024* 年に *NIST CSF 1.0* にマッピングされた全セグメントの調査結果

回答者が言及したカテゴリー、サブカテゴリー、および具体的なプロジェクトの深堀りを以下に示す。NIST CSF では、対応と復旧の機能のカテゴリーとサブカテゴリーが著しく少ないため、これらの分野での取り組みが少ないと予想される。

リスク削減努力のトップ 5 カテゴリー

1 防御： (PR.AA) アイデンティティ管理、認証／アクセス制御

2 ガバナンス：(GV.OC) 組織的背景

3 識別：(ID.AM) 資産管理

4 統治: (GV.SC) サプライチェーンリスクマネジメント

5 検知：（DE.CM）連続モニタリング

調査に参加した人のうち、37 人が防御におけるイニシアチブを特定した：アイデンティティ

管理、認証、アクセス管理（PR.AA）に続き、以下の各カテゴリーで 22 が選ばれた。

ガバナンス：Organizational Context（GV.OC）と Identify（識別）である：資産管理（ID.AM）である。ガバナンスでは 21 の取り組みが挙げられた：サプライチェーンリスクマネジメント(GV.SC)では、21 の取り組みが挙げられ、上位 5 つのうち、20 の CISO が検知を改善するための 20 の取り組みを強調した：継続的モニタリング能力（DE.CM）である。以下の叙述では、NIST CSF 2.0 のサブカテゴリーのうち、インプットを得たもののみを紹介している。これらの図表に続いて、最も多くのフィードバックを得たカテゴリーに関する戦略、プロジェクト、イニシアチブの詳細を示す。

01 防御：アイデンティティ管理、認証／アクセス制御

アイデンティティ管理、認証／アクセス制御（IDM）は、毎年、イニシアチブのカテゴリーで第 1 位にランクされている。調査回答者は、ネットワークやオペレーティング・テクノロジー（OT）全体に多要素認証（MFA）を導入するための複数年にわたるプロジェクトを引き続き強調している。ID 管理は、ゼロ・トラスト（ZT）戦略における重要な柱であり、より多くの IDM ツールを分析に活用している。航空会社は、4 つの IDM サブカテゴリーに最も注力している：PR.AC-1 クレデンシャル管理、PR.AC-5 ネットワーク整合性、PR.AC-4 アクセス許可管理、PR.AC-7 認証と MFA である。

PR.AA-05：アクセス許可、資格、認可がポリシーで定義され、管理され、実施され、見直され、最小特権と職務分掌の原則が組み込まれている。	29.7%
PR.AA：物理的および論理的資産へのアクセスは、認可されたユーザー、サービス、およびハードウェアに限定され、不正アクセスのリスクアセスメントに見合った管理が行われる。	24.3%
PR.AA-01：認可されたユーザ、サービス、およびハードウェアの ID とクレデンシャルが組織によって管理される。	21.6%
PR.AA-02: ID は相互作用のコンテキストに基づいて証明され、クレデンシャルにバインドされる。	16.2%
PR.AA-04：アイデンティティ主張は防御、伝達、検証される。	5.4%
PR.AA-03：ユーザー、サービス、ハードウェアの認証	2.7%

pr.aa、pr.aa-05：このカテゴリーでは、多様な取り組みが識別された。最も一般的なイニシアチブは、顧客やその他のサードパーティアクセスへの MFA の導入、ゼロトラストや新しいクラウド ID 管理機能の実装の一環としての ID 管理の利用に重点を置いたものであった。CISO はまた、クラウド用の IDM ツールの導入についても言及した。何人かのメンバーは IDM に対応する計画を挙げたが、戦略やツールの選択についてはまだ検討中であった。CISO はパスワードレス環境への移行も検討している。

PR.AA-01：Active Directory は、このサブカテゴリーで最もホットなトピックであった。CISO の戦略は両極端であり、Active Directory の利用を拡大する者もいれば、廃止を目指す者もいる。拡張の方では、オペレーショナル・テクノロジー側で AD を IDM に使用するプロジェクトや、より良い AD 管理を補完する技術を追加するプロジェクトがあった。もう一方では、ランサムウェアの攻撃者が頻繁に AD を攻撃していることから、CISO は他のソリューションを調査している。CISO は、可能な限りアクセスの幅を減らすことを念頭に、特権アクセス・アカウントと人間以外のアイデンティティのレビューを続けている。

PR.AA-02：航空会社および空港のメンバーは、より優れた ID 管理と管理を通じて、内部および外部 の不正行為を削減しようとする意向を述べた。これらの戦略には、シングルサインオンと多要素認証の使用をより多くのアプリケー ションに拡大することが含まれる。

02 統治：組織の背景

昨年の調査では、ガバナンスが CISO の行動領域のトップ 5 に入った。NIST CSF 1.0 では、ガバナンスは識別のサブカテゴリーであった。今年のガバナンスは、上位 5 つのうち 2 つを占める機能である。

ガバナンス機能における 6 つの組織背景サブカテゴリーのうち 4 つが、CISO が特定したプロジェクトと一致した。グローバルなメンバー構成は

メンバー企業は、ポリシーの変更、プロセスの変更、監査を通じて、コンプライアンスを文書化しなければならない。

GV.OC-03：プライバシーおよび市民的自由の義務を含む、サイバーセキュリティに関する法的、規制的、および契約上の要件が理解され、管理されている。	68.2%
GV.OC-02: 内部および外部の利害関係者を理解し、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待を理解し、考慮する。	18.2%
GV.OC-04：ステークホルダーが組織に依存または期待する重要な目標、能力、サービスを理解し、コミュニケーションする。	9.0%
GV.OC: 組織のサイバーセキュリティリスクマネ ジメントの意思決定を取り巻く状況（ミッション、ス テークホルダの期待、依存関係、法律、規制、 契約上の要件）を理解する。	4.5%

メンバーは、ヨーロッパ、アジア太平洋地域、アメリカ大陸、そして航空業界に特化した業界団体から、SOC2 や PCI といった自主的・強制的な要件など、規制遵守の課題を訴えた。ヨーロッパの会員は、NIS2 と Part IS に注目している。メンバーの中には、他国が制限している国に乗り込んだり、他国での展開が制限されている可能性のある技術を使用している者もおり、CISO はこれらのツールの使用が許可されていることを確認している。米国では、自主的に CMMC を検討している加盟国もある。また、監査証拠の収集を自動化するプロジェクトや、イベント発生前の報告要件をよりよく理解するために、法律やプライバシーの専門家との連携を強化するプロジェクトについても言及した。

03 識別する：資産管理

ID マネジメントの終わりのない課題と同様に、資産管理への取り組みも年々、2025 年の CISO のサイバーリスク削減戦略の一部となっている。

ID.AM-01：組織が管理するハードウェアのインベントリを保持する。	18.2%
ID.AM-03：組織の認可されたネットワークコミュニケーションと内部及び外部ネットワークのデータフローが維持されている。	18.2%
ID.AM：組織が事業目的を達成するための資産（データ、ハードウェア、ソフトウェア、システム、施設、サービス、人材など）を識別し、組織の目的および組織のリスク戦略に対する相対的な重要性と整合させて管理する。	13.6%
ID.AM-02：組織が管理するソフトウェア、サービス、システムのインベントリを維持する	13.6%
ID.AM-04：サプライヤーが提供するサービスの在庫を管理する。	9.1%
ID.AM-05：分類、重要性、資源、ミッションへの影響に基づき、資産に優先順位を付ける。	9.1%
ID.AM-07：指定されたデータタイプのデータと対応するメタデータのインベントリが維持されている。	9.1%
ID.AM-08：システム、ハードウェア、ソフトウェア、サービス、およびデータは、そのライフサイクルを通じて管理される。	9.1%

資産管理に取り組む CISO は、主にオペレーショナル・テクノロジー（OT）とモノのインターネット（IoT）環境をよりよく把握することに重点を置いていた。さらに、相手先商標製品製造事業者（OEM）は、工場現場の環境をよりよく把握することに重点を置いていることを指摘した。数名の CISO は、資産管理ポリシーの更新を計画していると述べた。さらに、何人かの CISO は、2025 年に向けて資産管理プロセスの改善に焦点を当てたワークアウトを実施すると述べた。

04 ガバナンス：サプライチェーンリスクマネジメント

本調査では、サプライチェーンリスクを低減するための取り組みについて、多くの回答があった。この機能のサブカテゴリのほとんどは、ビジネス機能を管理する自社の経営幹部に対する CISO の関与や、サイバーセキュリティがエンタープライズ全体のリスクマネジメント計画の一部であることを確認することに直接言及している。

GV.SC-07：サプライヤー、その製品・サービス、その他のサードパーティがもたらすリスクを理解し、記録し、優先順位を付け、アセスメントし、対応し、関係を通じてモニタリングする。	40.0%
GV.SC-08：対応するサプライヤー及びその他のサードパーティが、インシデントの計画、対応、復旧活動に含まれる。	10.0%
GV.SC-03：サプライチェーンリスクマネジメントが、サイバーセキュリティ及びエンタープライズのリスクマネジメント、リスクアセスメント、改善プロセスに統合される。	10.0%
GV.SC-01：サイバーセキュリティサプライチェーンリスクマネジメントプログラム、戦略、目的、方針、およびプロセスが確立され、組織の利害関係者によって合意されている。	10.0%
GV.SC-09：サプライチェーンセキュリティの実践が、サイバーセキュリティ及びエンタープライズリスクマネジメントプログラムに統合され、そのパフォーマンスが、技術製品及びサービスのライフサイクル全体を通じて監視される。	5.0%
GV.SC-02：サプライヤー、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、コミュニケーションされ、社内外で調整される。	5.0%
GV.SC-05：サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件が設定され、優先順位が付けられ、サプライヤやその他の関連するサードパーティとの契約やその他の種類の合意に組み込まれる。	5.0%
GV.SC-04：サプライヤーを把握し、重要度により優先順位をつける。	5.0%
GV.SC-06：正式なサプライヤーまたはその他のサードパーティとの関係に入る前に、リスクを低減するための計画とデューデリジェンスが実施される。	5.0%

GV.SC-10：サプライチェーンリスクマネジメント計画には、パートナーシップまたはサービス契約締結後に発生する活動に関する規定が含まれる。	5.0%

サプライチェーンリスクマネジメント（SCRM）の課題は、業界全体に蔓延している。CISO は、SCRM 戦略の全面的な見直しから始まる数多くのイニシアチブを特定した。興味深いことに、多くの CISO がこれを重点分野としているが、 成功への道筋は明確にされていない。何人かの CISO は、その道筋には主要サプライヤーの継続的な監視の強化が含まれると指摘した。さらに、今年は SCRM を行うためのより良い方法を模索するとしている。航空パートナーとの共通アセスメントを増やす、サプライヤーとの契約におけるサイバーセキュリティ条項を増やす、サプライヤーにソフトウェア部品表の提出を求める、などのアイデアが強調された。

05 検出：連続モニタリング

CISO は、継続的モニタリングの取り組みを後押ししているいくつかの環境要因を指摘している。多くの CISO は、同じ SIEM ツールセットを 5 年以上使用しており、新しいベンダーを検討することに前向きである。また、多くのセキュリティ・ツールに人工知能が統合されたり、統合が計画されたりしていることも、セキュリティ・オペレーション・センターのツールやネットワーク・モニタリング・ツールのリプレース検討の原動力となっている。

DE.CM-01：ネットワークとネットワークサービスは、潜在的に有害な事象を発見するために監視される。	70.0%
DE.CM-02：潜在的に有害な事象を発見するために、物理的環境をモニターする。	10.0%
DE.CM-03：潜在的な有害事象を発見するため、従業員の活動および技術利用を監視する。	10.0%
DE.CM-06：外部プロバイダの活動およびサービスを監視し、潜在的に有害な事象を発見する。	5.0%
DE.CM-09：コンピューティングのハードウェアとソフトウェア、ランタイム環境、およびそれらのデータを監視し、潜在的に有害な事象を発見する。	5.0%

CISO は、改善されたロギングプラクティスを実施することで、OT および IoT 環境の可視性を高めることに、より焦点を当てている。同様に、多くの CISO がクラウド環境の可視性を高めようとしている。これらの CISO は、クラウドネイティブのモニタリングツールとサードパーティ製のオプションの両方を検討している。一部の CISO は、強化されたユーザー行動分析（UEBA）ツールの展開や、法務部門、物理セキュリティ部門、人事部門との連携強化を通じて、内部脅威プログラムの強化に注力している。

その他の注目すべき回答

検知：有害事象分析

数多くのメンバー企業が SIEM をリプレースし、SOC 内の他のツールを更新し、イベント分析の自動化をさらに進めようとしている。何社かのメンバーは、イベント管理プラットフォームの上にケース管理機能を追加する計画であると述べている。CISO は、SIEM はノイズが多すぎると指摘し、アラートをより適切に調整する努力を再開するとしている。メンバーは引き続きバグ報奨金プログラムを実施し、チームによる脅威インテリジェンスの収集量を増やす予定である。

防御：データセキュリティ

データセキュリティの取り組みに関する議論では、2 つの大きなテーマが浮上した。2025 年にデータセキュリティの改善を優先する CISO は、人工知能を使用するアプリケーションで処理されるデータのエクスポージャーリスクに関する懸念に重点を置いていた。CISO は、これらのアプリケーションでデータがどこで処理され、どこに保存されるのかについて、引き続き理解を深めている。これは、アプリケーションの使用に関するガバナンスにも影響を与えるだろう。2 つ目の焦点は、データ損失防止（DLP）ツールの導入または利用拡大である。

防御：プラットフォームのセキュリティ

CISO は、プラットフォーム・セキュリティの強化に向けた幅広い取り組みについて言及した。CISO が最も多く挙げたのは、2025 年のモバイル・セキュリティへの注力であった。OEM は、製品への MFA の組み込みなど、製品をよりサイバーレジリエンスに優れたものにするための製品開発イニシアチブを挙げている。同様に、CISO は、コンピュータ・プラットフォームをよりセキュアにするための単発のプロジェクトも数多く挙げており、これには、特定のデバイス・タイプや製造事業者をよりセキュアなオプションに完全に置き換えたり、USB デバイス管理を改善したりすることが含まれる。

リスクマネジメント

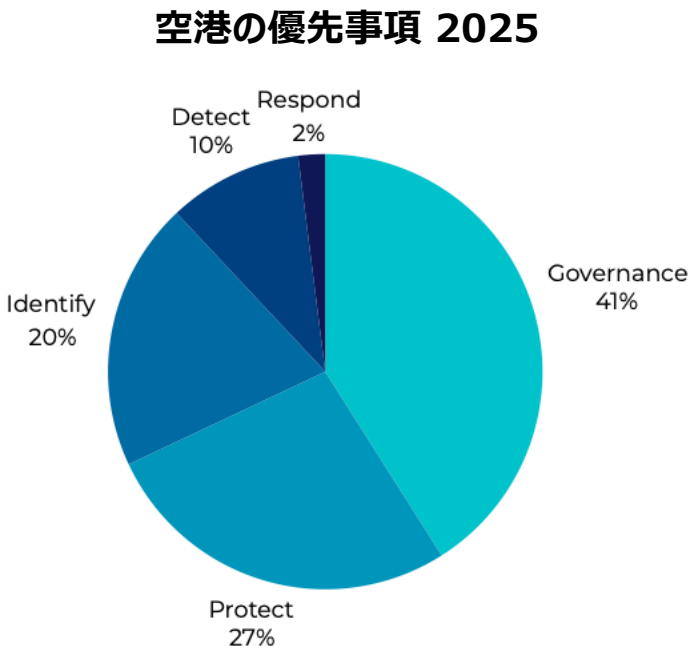
多くの CISO が、規制リスクアセスメントを実施中、または最近実施したと述べている。これらの組織は、これらのアセスメントを通じて特定されたギャップを埋めるための 戦略を準備するために、これらのアセスメントを利用しているか、利用する予定であった。こうした議論の一環として、CISO は、IST や PCI など、政府レベルでも業界団体レベルでも、多くの規制スキームが拡大していることを指摘した。

毎年この調査を実施するたびに、1 人か 2 人の CISO が懸念を表明する。今年は、量子コンピューティングをリスクマネジメントのマトリックスに入れるべきかどうかという懸念である。保護、防御、検知、レジリエンスに対して、量子はどのようなリスクをもたらすのか。議論では主に、リスクとそれが影響を及ぼす可能性のある時期について、より深く学び、理解する必要性に焦点が当てられた。

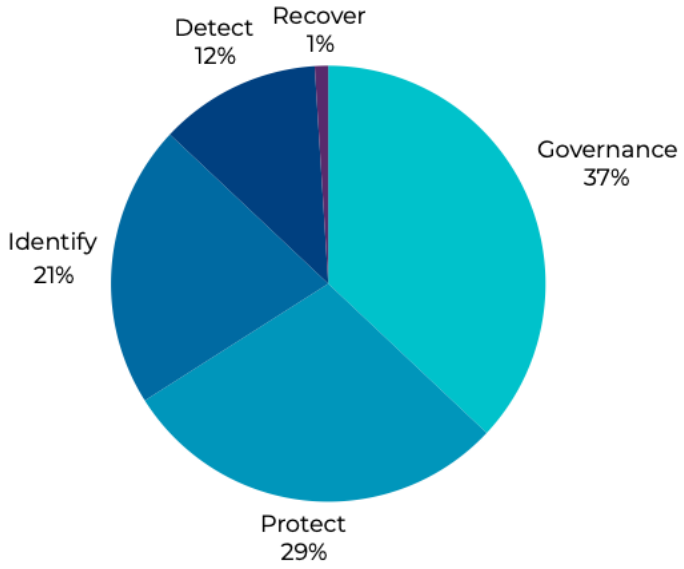
業種別に結果を分析する

以下のグラフは、今年度だけの機能別取り組み比率を表したものである。このグラフは、今回の調査で使用した 3 つのセグメントごとに整理されている：空港、OEM/サービス会社、航空会社である。NIST CSF 2.0 のリリースに伴い、2025 年の業界セグメント分析のみを掲載している。過年度のデータと比較した場合、2025 年のデータは過年度のデータセットとうまく整合しなかった。今後、2025 年以降の分析は、より直感的なものとなるだろう。

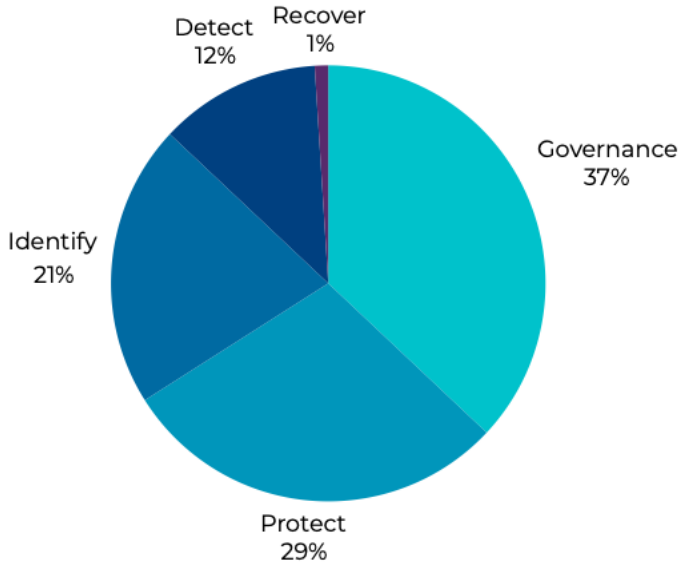
NIST SCF 2.0 を使用した 3 つのセグメントすべてにおいて、優先度の高い 4 つの分野が完全に一致した。優先順位は、すべてのセグメントで「ガバナンス」、「防御」、「識別」、「検知」の順となっている。空港は、他の 2 つのセグメントよりも対応能力の改善に重点的に取り組んでいることが顕著であった。



OEM/サービスプロバイダーの優先事項 2025 年



航空会社の優先事項 2025



概要

本報告書は、サイバーセキュリティの年間優先事項に関する業界動向分析である。特定の企業の重点を反映したものではない。本報告書の価値は、航空業界の CISO が自社のサイバーセキュリティ戦略、プログラムの成熟度、リソースの管理を業界と比較してベンチマークする際に役立つ点にある。

時間を割いて 2025 年に向けた考えや戦略を共有してくれた多くの CISO に感謝したい。

航空業界におけるサイバー・レジリエンスには、コミュニティ全体が一体となった取り組みが必要である。航空 ISAC は、航空業界に対する共通の情熱と業界を守るためのコミットメントを原動力とする献身的なコミュニティである。私たちの目標は、企業がサイバー脅威による混乱なしに活動できる公平な競争の場を確保することである。私たちは、サイバー脅威のインテリジェンスを共有し、サイバー攻撃を保護、検知、対応、緩和するためのベストプラクティスを開発するための安全で信頼できるプラットフォームを提供している。私たちのコミュニティへの参加についての詳細は、www.a-isac.com。

コンタクト

1997　アナポリス
エクスチェンジ・プライスウェ
スイート 300
アナポリス, MD 21401

membership@a-isac.com
www.a-isac.com