ISAO
Standards Organization

ISAO 300-1:
情報共有入門

v1.01

2016 年 10 月 14 日

この文書は下記団体によって翻訳監修されています

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

ISAO 300-1

情報共有入門

v1.01

ISAO Standards Organization

2016 年 10 月 14 日

謝辞

本出版物は、情報共有のための統一されたガイドラインとガイダンスを自主的に作成するための継続的な取り組みの一環として、業界、政府、および学界の代表者とともに、Information Sharing and Analysis Organization Standards Organization（ISAO SO）によって作成されたものである。ISAO SO およびワーキンググループのリーダーを以下に記載する。

ISAO Standards Organization

Gregory B. White, Ph.D.
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

ワーキンググループ 1—ISAO の設立

Frank Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance (ACTRA)

Deborah Kobza
President & CEO
Global Institute for Cybersecurity & Research

ワーキンググループ 2—ISAO のサービスおよび機能

Denise Anderson
President
National Health Information Sharing & Analysis Center
Chair, National Council of ISACs (NCI)

Fred Hintermister
Manager
Electricity Information Sharing and Analysis Center
North American Reliability Corporation
Vice Chair, National Council of ISACs (NCI)

ワーキンググループ 3—情報共有

Kent Landfield
Director, Standards and Technology Policy
Intel Corporation

Michael Darling
Director, Cybersecurity and Privacy
PwC

ワーキンググループ 4—プライバシーおよびセキュリティ

Rick Howard
Chief Security Officer
Palo Alto Networks

David Turetsky
Partner
Akin Gump Strauss Hauer & Feld LLP

本出版物の作成に大きく貢献した以下の方々に、ISAO SO のリーダーおよび本書の著者から深く感謝申し上げる。

Kevin Albano (IBM)、Scott Algeier (IT-ISAC)、Carl Anderson (HITRUST)、Jon Baker (The MITRE Corporation)、Allison Bender (Hogan Lovells)、Chris Boyer (AT&T)、Adam Buteux (PWC)、Roger Callahan (FS-ISAC)、Timothy Casey (Intel Corporation)、Dan Cashman (FairPoint Communications)、Christy Coffey (ThreatConnect)、David Eilken (Soltra)、Roxanne Everetts (National Defense University)、Paul Geraci (OSIsoft)、Stuart Gerson (Epstein, Becker & Green, LLP)、Steve Hitch (NTTSecurity)、Adam Isles (Chertoff Group, LLC)、John Johnston (Axiall Corporation)、Klara Jordan (FireEye)、Akilah Kamaria (Blue Fields Digital)、Norma Krayem (Holland and Knight LLP)、Terry Leach (Astrolytes)、Tom Litchford (National Retail Federation)、Alelie Llapitan (Solutionize)、Chris Needs (NC4)、Betsi McGrath (The MITRE Corporation)、Kim Milford (Research and Education Networking Information Sharing and Analysis Center)、Bruce Parkman (The Macalan Group)、Bobbie Stempfley (The MITRE Corporation)、Roy Stephan (PierceMatrix)、Megan Stifel (Silicon Harbor Consultants, LLC)、Nick Sturgeon (The Indiana Information Sharing and Analysis Center)、Shawn Talmadge (Commonwealth of Virginia)、Jay Taylor (Schneider Electric)、Michael Thibodeaux (BASF SE)、Matt Tooley (The National Cable & Telecommunication Association)、Michael Vermilye (Johns Hopkins University Applied Physics Laboratory)、Joseph Viens (Charter Communications)、Jesse Ward (NTCA-The Rural Broadband Association)、Douglas T. White (C5T)、John Woodso (Baker & McKenzie, LLP)、そして Brandon Workentin (EnergySec)。

また、本書の作成に大きく寄与した以下の ISAO SO のアドバイザーとスタッフに、著者から特に謝意を表す。Chris Rutherford、Daniel Knight、Larry Sjelin、そして James Navarro。

改訂履歴

項番	バージョン	説明	日付
1	1.0	初版	2016 年 9 月 30 日
2	1.01	編集による更新／修正	2016 年 10 月 14 日

目次

図

表

1 エグゼクティブ サマリー

本書の目的は、サイバーセキュリティ情報共有の概要を示すことであり、情報共有分析機関（ISAO）に関連する情報共有の基礎を理解するための土台を提供することを意図している。本書では、情報共有の概念的な枠組み、情報共有の概念、組織が共有する可能性のあるサイバーセキュリティ情報の種類、組織における情報共有の推進方法、および検討すべきプライバシーとセキュリティの懸念事項について説明する。

情報共有は、サイバーセキュリティのリスクの管理者およびサイバーセキュリティのリスクを緩和する運用上の担当者を支援することを目的としている。サイバーセキュリティの特質は時間の経過とともに変化し続けている。情報共有への取り組みも、サイバーセキュリティの状況の変化に遅れることなく進展させる必要がある。本書は、サイバーセキュリティ情報共有に関するトピックと機能についての基本情報を読者に提供する。また、サイバーセキュリティ情報共有プログラムの構成要素について説明する。これは、新しいISAO の設立を検討している者、およびメンバーのニーズにさらに合致させる方法を調査している既存の ISAO を対象にしている。

本書では、*サイバーセキュリティ情報共有*、*サイバー脅威共有*、*情報共有*という用語を同じ意味で使用する。

2 はじめに

サイバーセキュリティのリスクに対処している組織にとって、一般的に*情報共有*として位置付けられている取り組みに関与することは価値がある。情報共有の利点は、広範なコミュニティーの知識、認識、理解、経験を活用する機会が得られることである。

情報共有の取り組みへの関与は主に、サイバーセキュリティを向上させることへの個人の関心、または組織の関心、あるいはその両方が発端となる。サイバーセキュリティのリスクの管理者およびサイバーセキュリティのリスクに対処するための活動の担当者は、運用環境をよりよく理解し、集団的利益に貢献するために、情報共有活動（その場限りのもの、規定されたもの、または確立されたもの）への参加を希望する場合がある。

情報共有は、組織が直面しているサイバーセキュリティの課題をすべて解決するものではないが、情報共有により、組織や他の組織に影響を及ぼす脅威環境をよりよく理解するための準備を行うことができる。他者の経験から学び、他者が発見した効果的なサイバーセキュリティ対策を理解することは、同様の状況において組織が状況認識、意思決定、行動、リソースの割り当てを行う際に役立つ。

本書は、サイバーセキュリティに関する情報共有の概要を示すように構成されている。本書は、既存の ISAO への参加を検討している者、新しい組織の設立を検討している者、現在の ISAO メンバーシップの評価を検討している者にとって有用である。

ISAO は多くの課題に直面することが予想されるが、成功に不可欠なのは、参加者に優れた「価値」を提供することである。『情報共有入門』は、情報共有と共同作業への取り組みを選択および実施する際に考慮すべき成果を ISAO に提供するように構成

されている。本書では、概念的な枠組みと情報の用途の説明に加えて、想定される ISAO のサイバーセキュリティ情報共有活動を表す一連の機能要素を示す。また、ISAO のサイバーセキュリティ情報共有機能を発展させるために検討すべき項目を示す。すべての新しい ISAO が、本書に記載されていることを完全に達成できること、または完全に達成することを望むわけではない。以下の事項は、規範的なものではなく概念的なものであり、検討事項を記載しているのは、それらを強制するためでなく選択肢を示すためである。

3 情報共有の概念

グループ、企業、組織は、採用している技術、その技術を事業や顧客が使用する方法、および他者との連携に基づいて、サイバー関連のリスクを管理する。これらのリスクの管理には、各自の内部環境および運用環境の理解（状況認識）、目標とする方向性の決定（意思決定）、実際の取り組み（行動）の詳述が伴う。これらは、組織が日々行う活動である。

ISAO は、メンバーがサイバー関連のリスクを管理するのに役立つさまざまな情報を提供できる。それらの情報は、論理的に次の 2 つの側面にグループ化できる。すなわち、**目的**、およびリソースの**時間と適用**である。

目的には、以下の 3 つの領域が含まれる:

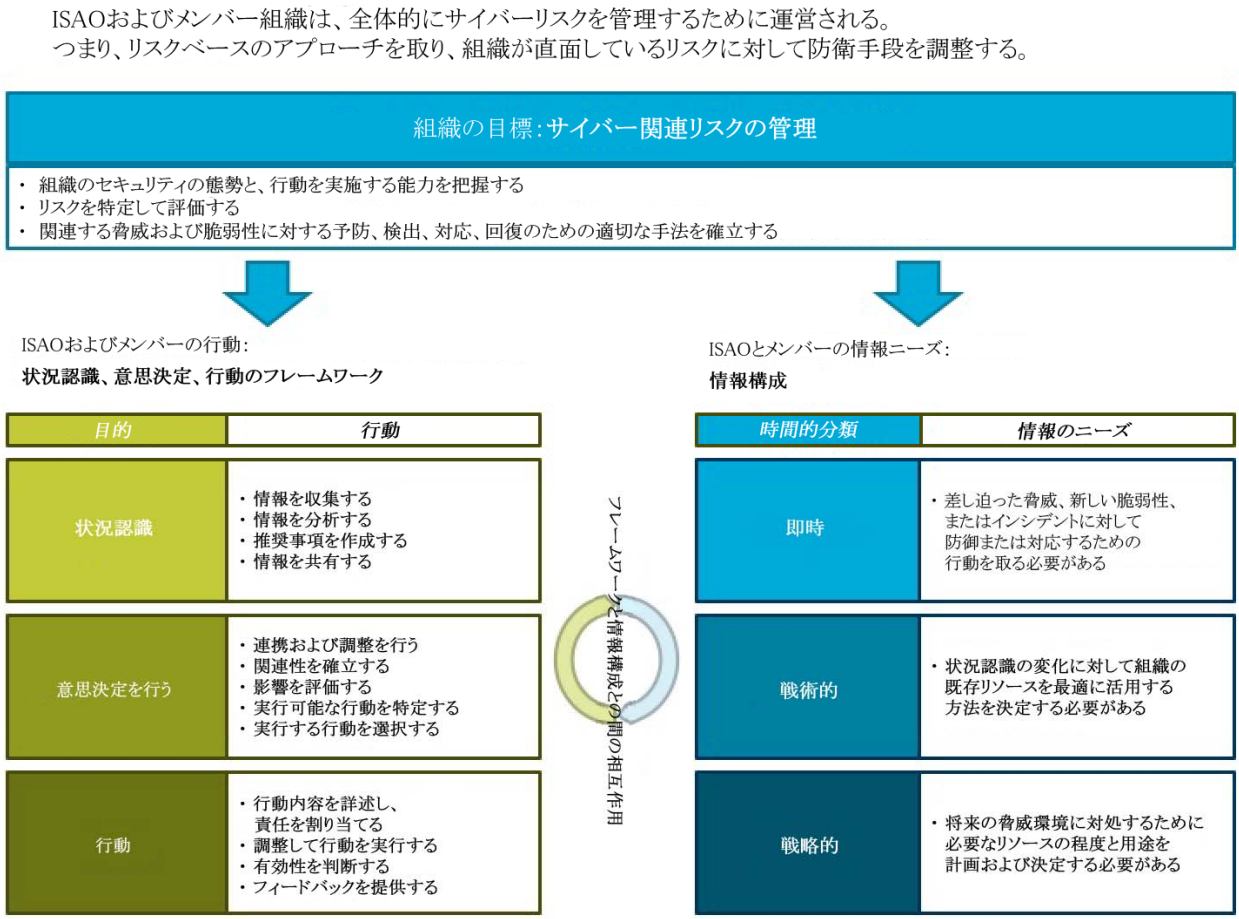
- ***状況認識***—広範な脅威状況についての認識をもたらす情報。
- ***意思決定***—特定の組織のニーズに関連する情報、およびより効果的なセキュリティ管理を可能にする情報。
- ***行動***—セキュリティを強化する特定の手段の実行を直接支援する情報。

リソースの**時間と適用**は、セキュリティに運用上関連する情報から始まり、それに基づいて展開される。この側面には以下の 3 つの領域が含まれる。

- ***即時***—新しい脅威、脆弱性、またはインシデントに対して防御または対応するための行動に関する情報。
- ***戦術的***—脅威環境の変化に対して組織の既存のリソースを最適に活用する方法の決定に関する情報。
- ***戦略的***—新しい脅威環境または将来の脅威環境に対処するために必要な作業とリソースの計画および決定に関する情報。

図 1 は、ISAO とメンバーの取り組みと、組織によるサイバー関連のリスクの管理に役立つ情報を整合させて相互作用させるための情報構成とフレームワークを示している。

図 1. 情報共有の背景



3.1 情報共有のフレームワーク

図 2 に示す情報共有の概念的フレームワークは、前述の 2 つの側面を用いて、ISAO が情報共有の目標を策定する際に検討すべきさまざまな相互作用の組み合わせの概要を示している。これらの関連性は、ISAO の概念的活動とそのメンバーの活動の両方を表している。

図 2. 情報共有の概念的フレームワーク

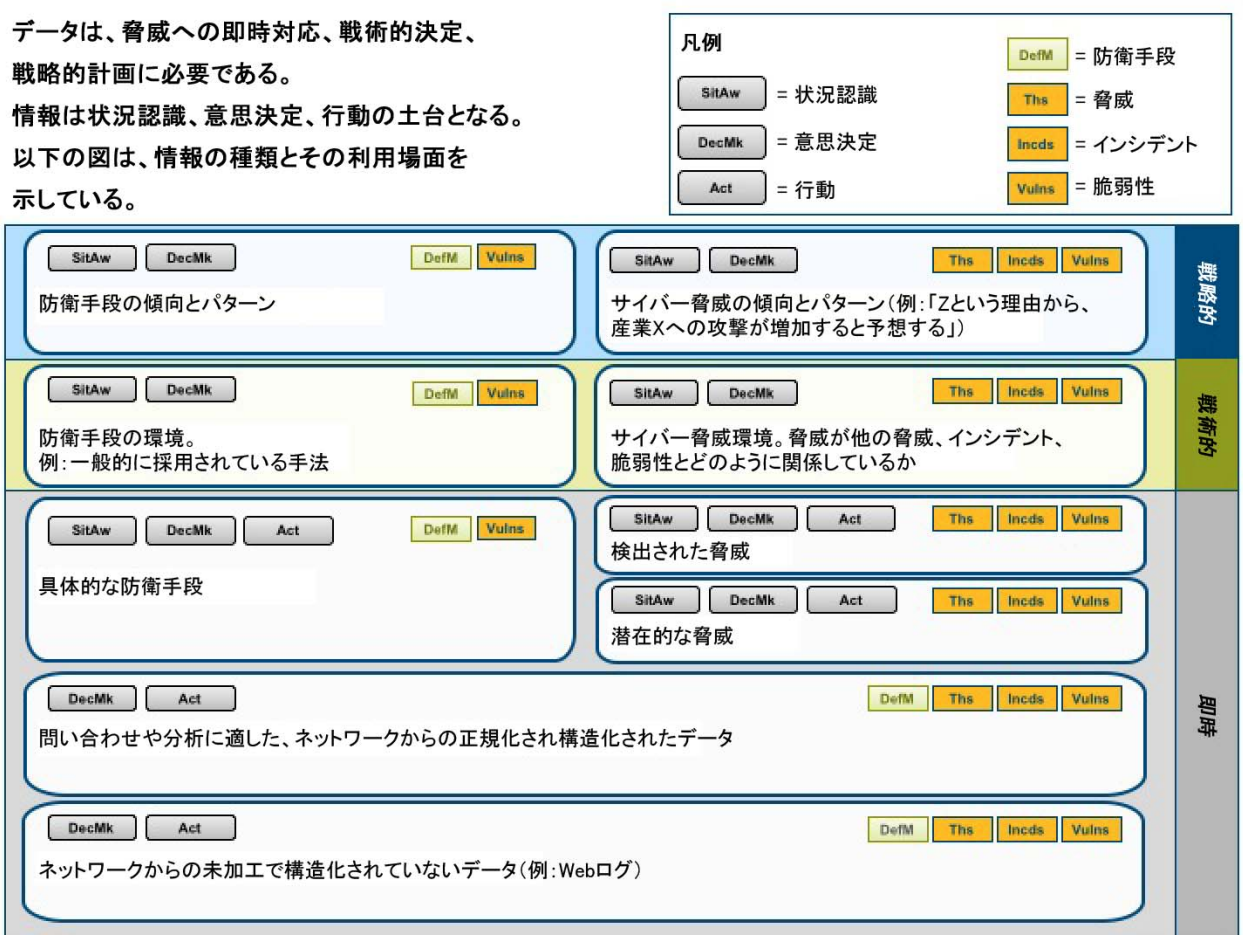
この関連性と概念的フレームワークの図は、ISAO がメンバーに提供できる利益を示している。これは、組織がサイバー関連のリスクを管理するために日々行っていることに関連する情報共有への取り組みを通じて、メンバーの情報ニーズを満たすことで達成できる。

3.2 共有情報の適用

図 3 は、サイバー関連リスクの管理と緩和に焦点を合わせた状況認識、意思決定、行動に影響を与えるように、特定の種類の情報（脅威、脆弱性、およびインシデント）を適用する方法の概要を示している。

さらに、分析を段階的に進めることで、運用環境からの未加工で構造化されていないデータを有益な知識や追加情報に変えることができる。組織はこの知識と情報を活用することで、最も一般的な脅威に対する防御または対応への取り組みに優先順位を付けることができる。

図 3. サイバーセキュリティのリスクに対する情報の適用



3.3 機能要素の説明

ISAO が共有を検討する情報の種類は、ISAO がメンバーに提供する広範な機能を分類することでも説明できる。これらの機能カテゴリを各要素に分解し、それらのサポートに必要な機能を組み合わせて示すことができる。

表 1 では、これらの分野横断的なカテゴリをサブカテゴリに分解して、それらのカテゴリのサポートに必要なより具体的な情報機能を示している。

ISAO に参加しているメンバーの個人の関心または組織の関心は、一般的に以下の点にある：

- 現在おかれている脅威および脆弱性の環境をより深く理解するための新しい知識
- 特定の脅威と脆弱性に対処するための推奨事項
- セキュリティ状態に影響を及ぼす可能性のある状況アラートの受信

- 現在の状況やインシデントへの理解度の確認
- 脅威、脆弱性、および／またはインシデントに対する現在の理解度を高める追加情報
- 他者が行っている行動の情報
- 集団行動の調整
- 他者が個人で、または集団で行っている行動の有効性に関するフィードバック

これらの個人の関心または組織の関心は、ISAO が実行できる広範な戦術的取り組みおよび戦略的取り組みを構成する以下の 4 つの機能要素カテゴリを説明するために利用できる:

- 脅威状況の認識
- 対応手段
- 調整
- 傾向分析とパターン分析

以下に示すように、これらの広範なカテゴリは、ISAO への参加者または協力者の個人の関心または組織の関心に対応するために、より具体的な機能要素と情報共有機能にさらに分解することができる。

表 1 は、これらのカテゴリとサブカテゴリについて説明し、それらをサポートする情報共有機能を示す。

表 1. 機能カテゴリと情報共有機能

機能カテゴリまたはサブカテゴリ	説明	情報共有機能
脅威状況の認識	サイバーセキュリティまたは ISAO の他の考慮事項についての現在の状況を認識する	
• 情報を収集する: – 全般	• ISAO の参加者および関心のある他の情報源から脅威、脆弱性、およびインシデント情報を入手する	• 匿名および記名による送信 • 電子メールとリストサーバー • 電話 • 会議 • セキュアポータルでの送信 • 自動フィード • サイバーセキュリティ パートナーの直接フィード • Traffic Light Protocol (TLP)のラベル付けの実施
• 関心のあるコミュニティーに焦点を合わせる	• 必要に応じて、関心のあるコミュニティーの参加者により深い信頼関係を構築するよう促す	• 上記と同様の機能(関心のあるコミュニティーの参加者のために選別したり個々に調整したりすることが可能)。

機能カテゴリまたはサブカテゴリ	説明	情報共有機能
– 適切な情報を利用可能にする	• TLP の手順およびラベル付けに従って情報を配布または利用可能にする	• 適切なコミュニケーション手段（ポータルアクセス、電子メール、自動プラットフォームなど）経由の配布
– 収集した情報を分析する	• 収集した情報のレビュー、重複の解消、確認、サニタイズ、分析を行う • 絶えず変化するまたは既に存在する脅威、インシデント、および脆弱性をメンバーにアラートするための調査または情報収集を実施する	• アナリストおよびアナリストのツール
– アラートを作成する	• ISAO の参加者および他者が関心を持つ可能性のある状況認識の変化を特定する	• アラートの重大度別の通信の仕組み • 最高レベルのアラート用の多重化の仕組み
対応手段	インフラ、運用、またはシステムに対する脆弱性またはエクスプロイトの影響を緩和または無効化するための運用上または手続き上の手段を確立する	
• アラートと迅速な通知を配信する	• 作成したアラートと通知を適切な参加者またはパートナーに提供する	• アラートの重大度別の通信の仕組み • 最高レベルのアラート用の多重かつ多様な仕組み
• 対策を立てる: – 即時 – 長期	• 参加者やパートナーと協力して、新しい脅威や脆弱性のリスクを緩和するための対策を立てる • 即時の対策に焦点を当て、次に長期の対策に焦点を当てる	• 技術者と参加者の両方のための、会議およびネットワーク作りによる協力の仕組み • 参加者が検索可能なトピックの分析を行うための機能へのアクセス
• 「ベスト」プラクティスと「グッド」プラクティスの推奨事項を策定する	• 参加者の関心事項に基づいて、サイバーセキュリティおよび他の関連リスクやインシデントを緩和したり、それらに対応したりするための「ベスト」プラクティスと「グッド」プラクティスの推奨事項を策定する	• 技術者と参加者の間の協力のための会議、ネットワーキング、フォーラム • 調査機能 • 参加者が推奨事項を確認できる参照先とリポジトリの公開および提供 • 参加者が検索可能トピックの分析を行うための機能へのアクセス
• 有効性を判断する	• 測定基準を作成し、提供されているサービスについて有効性および参加者の満足度を継続的に測定するための調査を実施する	• 参加者調査の機能
調整	ISAO によって確立された共有目標を確実に遂行するために、活動内容を一致・統合する。	
• 調整のプロセスと機能を確立する	• 共通の関心事項を持つメンバー間での議論や協力のための調整の必要性を評価するために確立されたポリシーと手順	• リーダー グループ（識別されたサブグループ）が調整を有効にする決定を下すためのコミュニケーション／ネットワークの仕組み

機能カテゴリまたはサブカテゴリ	説明	情報共有機能
• 調整を有効にする	• 調整のための「緊急」呼び出しの通知を発行する	• 「緊急呼び出し」を開始するための確立された多様なコミュニケーション機能
• 調整の行動と取り組みを策定する	• 参加者間の調整が必要となるさまざまな状況に対する「作戦計画書」を作成する	• 特定の重大度を持つ進行中のインシデントに対して、進行中の状態に関連する状況、対策、および対応情報を判断するためのカンファレンス機能を実装する
• 調整の取り組みを評価する	• 調整イベント中およびイベント後に、行われた意思決定と行動を継続的に評価する	• 調査機能 • カンファレンス機能
傾向分析とパターン分析	情報を収集し、ISAO 参加者が関心を持つ情報から導かれるパターンや傾向の特定を試みる	
• 履歴情報を保持する	• 送信、分析、決定の履歴をセキュアなデータベースに保持する	• 情報の多様な機密性を区別して対処するための適切なアクセス制御を備えたセキュアな運用データベースとソフトウェア
• 戦略分析を実行する: – 活動の傾向、不規則性、またはパターンを特定する – 脅威アクターと動機を明らかにする	• ISAO の過去の情報を他の情報と共に分析して、参加者の関心事項と深い関係がある傾向と、新たな活動についての付加価値のある洞察を提供する	• アナリストおよびアナリストのツール • アナリストが他の専門家と連携するための外部との共同作業の仕組み
• 分析結果と推奨事項を公開する	• ISAO のポリシーと手順に基づいて ISAO の参加者や他者と定期的に連絡を取る	• メンバーが分析結果を受信するためのコミュニケーション手段と交流会 • 参加者が検索可能トピックの分析を行うための機能へのアクセス

3.4 情報共有の目標設定

ISAO は、それぞれ独自のミッションとビジョンを持って設立されている。明確な情報共有の目標を策定することで、そのミッションとビジョンを実現できる。また、目標を明確にすることは、共有する情報、その情報の共有方法、およびメンバーと ISAO の期待事項の管理を決定する上でも重要な意味を持つ。

多くの場合、ISAO 自体は、リスクを管理する手段としてパートナーや他者と共同作業を行うことを選択した、同じような考え方を持つ組織のコミュニティーによって形成されている。ISAO は、初期のメンバーによって、メンバー全体のニーズを満たすように設計される。ISAO は、情報共有は目的を達成するための手段であるという理解のもとに、達成しようとしている情報共有の目標を明確に策定する必要がある。

これらの目標を定義する際に、新しい ISAO とその潜在的メンバーには、情報共有の目的を決定するために回答する必要があるさまざまな質問がある。これらの質問は、既存の ISAO を評価する際にも使用できる。

以下に、ISAO の検討対象となりうる質問を示す:[1]

- 共有された情報は、メンバーがサイバーセキュリティの目標を達成するのにどのように役立つか？
- ISAO メンバーが必要とする、適切な状況認識を示す情報の種類はどれか？
- メンバーの戦術的意思決定の支援のために ISAO が提供するのは、未加工のデータか、分析結果か、あるいはその両方か？
- メンバーは、防衛手段、ベストプラクティス、および／またはインシデント調整の手順などの行動に関連する推奨事項を希望するか？
- ISAO は、傾向、脅威アクターの標的、脅威アクターの動機などの関連事項を含む戦略的性質の分析を提供するか？
- ISAO の情報共有、緩和、および分析計画は、どのように相互に関係しているか？
- ISAO とそのメンバーの間での情報共有と信頼関係はどのように築かれるか？
- ISAO の情報共有ポリシーによって、どのように期待事項と義務事項が統制されるか？
- ISAO メンバーがお互いに共有することを望む特定の種類の情報はあるか？
- ISAO メンバーは、戦術的な意思決定においてどのような情報による支援を必要とするか？
- ISAO のリソース内で達成可能かつ持続可能な情報共有機能は何か？
- 既存の ISAO は、検討されている情報のニーズを満たしているか？

組織が集まって ISAO を設立する際は、将来のニーズを完全に理解していない場合でも、初期段階の情報のニーズを理解することから始めることになる。したがって ISAO は、その目標を明確に定め、その目標達成を支援する情報共有ポリシーを策定する必要がある。例えば、ISAO を形成するコミュニティーが特定の攻撃を緩和するための効果的な手法に関するより多くの情報を希望する場合、ISAO はこの目標を促進するポリシーを作成する必要がある。

ISAO に参加している個々のメンバーや組織は、各自のニーズおよび参加している ISAO コミュニティーに対する責任に対処する必要がある。情報共有のポリシーを策定する際、ISAO はメンバーの目的や顧客のニーズにポリシーを適合させる必要がある。

[1] ISAO 100-2「*ISAO の設立のためのガイドライン*」を参照。

4 ISAO が共有する情報

ISAO とそのメンバーは、各 ISAO、他の ISAO のメンバー、およびさまざまな政府機関と情報を共有することを検討する可能性がある。これらの組織間での情報交換は、標準化された一貫性のある用語、フレームワーク、およびデータフォーマットを使用することで容易になる。また、一貫性のあるフレームワークを活用することで、焦点が異なるさまざまなソースからの脅威情報の統合および分析が可能になる。例えば、検知指標情報と脅威アクター情報またはインシデント情報との統合などである。

4.1 主要要素

ISAO が共有するサイバーセキュリティ情報の種類を評価する際には、考慮すべき主要要素がいくつかある。また、情報共有の方法には、ネットワーク対ネットワーク、マシン対マシン、人対人、人対マシンなどのさまざまな方法がある。マシン対マシンの共有では、構造化された情報が必要である。また、相互運用性を実現するために、標準化されたデータフォーマットとプロトコルを使用する必要がある。人対人の共有においては、共通のフレームワークを使用してサイバーセキュリティ情報を記述した場合に最も効果を得られる。これによって、メンバー間での共通の理解が促進される。ただし、この場合の情報は本質的に、マシン対マシンの共有で必要とされる情報よりも構造化レベルが低くなる可能性がある。

以下では、脅威情報構造化記述形式(STIX)[2]言語を使用して、ISAO が共有を検討する情報の種類を記述する。STIX 用語は、サイバーセキュリティ情報共有の基本となるサイバー脅威の主要概念を伝達するために必要な表現を提供する。

自動制御ベースの情報交換を効果的に機能させるためには、確立された技術規格を使用する必要がある。構造化されたサイバーセキュリティ脅威情報の交換の自動化には、各種の交換用言語が使用されている。サイバー脅威インテリジェンスの共有形式を単一化する試みは長年にわたって行われてきたが、そのほとんどはインシデント対応などの特定の分野に集中していた。インシデントオブジェクト記述交換形式[3]は、そのような集中的アプローチの一例である。

STIX 言語は一般的に、サイバー脅威情報の取得と共有に使用される。STIX は、構造化された機械可読なフォーマットであり、サイバー脅威情報の伝達に特化して設計されている。STIX はサイバー脅威全体に対応する。STIX は、サイバー脅威情報を一貫した方法で表現および共有するためのフレームワークを定義する。このフレームワークは、一連の主要属性(脅威アクター、キャンペーン、インシデント、検知指標、行動方針、観測可能な事項、エクスプロイトの標的、戦術、技術、および手順(TTP)、およびこれらの主要属性間の一連の関係)から構成されている。

[2] 参照:https://stixproject.github.io/data-model/
[3] 参照:https://www.ietf.org/rfc/rfc5070.txt

STIX フレームワークは、サイバー脅威インテリジェンスの各ユースケースの全スコープに対応可能な汎用性を備えている。また、ユーザーやコミュニティーが特定のユースケースで必要とする STIX 言語のサブセットを定義するための柔軟性も備えている。STIX を使用すると、特定のサイバー脅威の共有の必要性に対応するプロファイル[4]を定義できる。これらのプロファイルは、共有時に STIX 言語のどのサブセットを使用するかを文書化する。ISAO が STIX を使用する場合、よく知られた STIX プロファイルを発展させるか活用して、所定のシナリオで交換される特定のデータ要素を文書化しておくと役立つ場合がある。STIX は、政府および業界の脅威インテリジェンス チーム、セキュリティ製品やセキュリティサービスのベンダー、情報共有分析センター（ISAC）、主要なコンピュータ緊急対応チーム（CERT）で使用されている。

以降のセクションでは、ISAO が共有を検討する可能性のある、一般的に共有されるサイバー脅威情報について説明する。これらのセクションでは、STIX の取り組みを活用するために、該当する場合は、STIX で使用されている用語と定義に合わせている。

4.2 検知指標

検知指標は、サイバーセキュリティにおいて関心のある成果物および／または行動を示すための文脈情報と併せて特定のパターンを伝達し、関心のある活動を検出するために使用される。検知指標は現在、悪意のあるファイルのハッシュから、コマンド＆コントロールの IP アドレス、フィッシングメール、およびその他のタイプに至るまで、幅広く共有されている。

効果的に検知指標を共有するには、検知指標の自身の組織への関連性の有無、検知指標の処理方法、示された TTP の内容、検知指標の有効時間枠、および関連するインシデント、脅威アクター、キャンペーンを下流の消費者が判断できるようにするための背景情報を含める。

一般的に共有されるフィールドを以下に示す：

- タイトル
- 説明
- パターン―機械可読なパターン
- 信頼度―検知指標の信頼度
- 示された TTP
- 有効な時間的位置―検知指標が有効である時間枠

検知指標の共有は、マシン対マシンの情報交換によって行うとより効果的である。自動検知指標共有の一例として、連邦政府の省庁と民間セクターの間でサイバー脅威の共有を可能にするための、米国国土安全保障省（DHS）が運営する自動検知指標共有

[4]参照：https://stixproject.github.io/documentation/profiles/

(AIS)の取り組みがある。[5]この取り組みでは、サイバー脅威情報の自動交換に STIX と検知指標情報自動交換手順(TAXII)[6]が使用されている。TAXII は、検知指標の交換を可能にするための一連の標準サービスを定義する。AIS は、検知指標を交換するための STIX 言語のプロファイルを定義済みである。AIS STIX プロファイルには、AIS によるサイバー脅威共有で使用される STIX 言語の具体的なデータ要素が記述されている。このプロファイルは、自動共有か手動共有かにかかわらず、基本的なサイバー脅威検知指標共有の有効な開始点となる。また、このプロファイルを利用して、ISAO 内および ISAO 間で検知指標を共有するための一貫したアプローチを確立できる。

検知指標は多くの場合、マルウェア分析、インシデント対応、エンドポイントとネットワークの監視を通じて生成される。したがって検知指標情報は、ISAC、CERT、セキュリティ製品やセキュリティサービスのベンダー、組織固有のセキュリティチーム、オープンソース レポートなど、さまざまな情報源から頻繁に取得される。このように検知指標の情報源が多様であると、共有される検知指標とともに背景情報を伝達する必要が生じる。今日における検知指標共有の共通課題は、環境への侵入を検知するのに適切かつ有用な検知指標を決定することである。

検知指標レポートには、検知指標の観測情報が含まれる可能性がある。このレポートでは、あるセクター内(あるいは特定の組織内)で一致した、または観測された所定の検知指標が報告される。概して、この観測情報は、特定のキャンペーンや脅威アクターの発生状況、標的の情報などを理解するのに役立つ。この総合的な観測情報は、より洗練されたサイバー脅威インテリジェンスの分析をサポートする低コストかつ低リスクの手法として広く認識されている。

4.3 脆弱性情報

脆弱性情報には、特定のシステムやインフラの脆弱性、特定のアプリケーションの脆弱性、または一般的な種類の脆弱性に関する詳細が含まれる。

一般的に共有されるフィールドを以下に示す:

- タイトル
- 説明
- 脆弱性 ID—共通脆弱性識別子(CVE)[7]の脅威識別子またはその他の既知の識別子への参照
- スコア-対象の脆弱性に対する共通脆弱性評価システム(CVSS)[8]の格付けスコアまたは同様のスコア
- 影響を受けるソフトウェア。

[5]参照:https://www.us-cert.gov/ais
[6]参照:https://taxiiproject.github.io/about/
[7]参照:https://cve.mitre.org/
[8]参照:https://www.first.org/cvss

業界の主要なソフトウェアベンダーは、製品やサービスに関連する脆弱性情報を定期的に公開している。多くの政府機関も同様に、意識向上を目的として脆弱性の報告やセキュリティ勧告を行っている。これらの政府勧告の一例として、US-CERT のアラート[9]がある。

共有される脆弱性情報により、緊急対応処置が頻繁に通知される。これは、その情報が公開システムの最新の高重大度の脆弱性に関連している場合に特に当てはまる。脆弱性の傾向およびより一般的な種類の脆弱性情報では、戦術的かつ戦略的な状況認識と意思決定に役立つ情報が定期的に通知される。

4.4 行動方針

行動方針とは、脅威を緩和したり、インシデントに対処したりするための具体的な手段である。行動方針は、特定の IP アドレスのブロックなどの比較的ターゲットを絞ったものである場合や、アプリケーションのホワイトリストの使用などの企業の手法を含む場合がある。このように、行動方針の共有は、意思決定と行動に影響を与える即時情報、戦術的情報、および戦略的情報の全範囲に及ぶ可能性がある。

一般的に共有されるフィールドを以下に示す:

- タイトル
- 説明
- タイプー訓練、監視、パッチ適用、ブロックなど
- 目標
- 影響
- コスト
- 有効性
- 行動方針—ファイアウォールや侵入検知システムのルール、具体的な設定変更など

行動方針を共有することで、脅威を緩和するための自動的なアクションを可能にするだけでなく、組織間の協力により、様々な選択肢の中で総合的な観点から最良の行動方針を採用することがでる。

4.5 インシデント

インシデント情報とは、サイバーセキュリティインシデントに関連する特定の情報、またはサイバーセキュリティインシデントの調査時や対応時に検出された特定の情報である。共有されるインシデント情報に含まれる詳細の記載量およびレベルは、共有情報の使用目的、および財務、評判、またはその他の懸案事項に関連する保護必要度に応じて

[9]参照:https://www.us-cert.gov/ncas/alerts

大きく異なる。

一般的に共有されるフィールドを以下に示す:

- タイトル
- 説明
- カテゴリ—不適切な使用、スキャンまたは調査、サービス妨害など
- 報告者—インシデントの記述の報告元
- 被害者—インシデントの被害者の詳細
- 影響を受けた資産—インシデント時に影響を受けた資産について説明する
- 影響の評価—インシデントの影響を説明する
- 関連指標—IP アドレス、ファイルのハッシュ、ドメインなど
- 使用された TTP—攻撃技術、マルウェア、ツールなど
- 原因となる脅威アクター
- 意図された効果—盗難、機能中断、アカウントの乗っ取り、詐欺など。
- 関連するインシデント
- 行動方針

米国政府は、インシデント情報とインシデント処理の報告のために、以下のようなよく知られたガイドを発行している：

- 資料『*The Federal Incident Notification Guidelines*』は、United States Computer Emergency Readiness Team (US-CERT)[10]にインシデント通知を提出するためのガイダンスを提供する。
- 米国国立標準技術研究所(NIST)は、インシデント対応に役立つ情報源である Special Publication 800-61『コンピュータ セキュリティ インシデント対応ガイド』[11]を発行している。

これらは、インシデント対応と分析をサポートするために一般的に共有されている情報に関する優れた参考資料である。

インシデント情報を共有することで、それぞれ異なるインシデント情報要件を持つさまざまなユースケースを可能にすることや、サポートすることができる。インシデント情報の共有により、サイバーセキュリティ エコシステム全体での攻撃者の傾向を明らかにするための大規模な分析が可能になる。詳細なインシデント情報の共有により、特定の脅威ア

[10]参照:https://www.us-cert.gov/incident-notification-guidelines
[11]参照:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

クターやキャンペーンに関連した高度なサイバー脅威インテリジェンス分析が可能になる場合がある。インシデント情報の共有は、悪意のある活動の主要な検知指標を明らかにして、パートナーにサイバー防衛について通知するのにも役立つ。

詳細なインシデント情報の共有により可能となる大規模なインシデント分析の代表的な例として、Verizon の DBIR（Data Breach Investigations Report）[12]がある。Verizon の DBIR を形成するために収集されたインシデント データは、VERIS（Vocabulary for Event Recording and Incident Sharing）フレームワークを使用して構成される。VERIS には、サイバー脅威活動のさまざまな側面（脅威アクター、行為、資産、およびその他のインシデント属性の詳細な分類など）についての概要が含まれている。Verizon の DBIR は、さまざまな組織から提供された多数のインシデント情報を分析した結果である。このレポートは、状況認識および意思決定に関する情報を提供するために、戦略的かつ戦術的な価値を実現することを目的としている。

4.6 脅威アクター

脅威アクター情報には、サイバー脅威を示す可能性のある、または以前から観測されていた、または既知のインシデントに関連している悪意のあるアクターが含まれる。

一般的に共有されるフィールドを以下に示す：

- 名前—脅威アクターに使用される短い名前またはエイリアス
- 説明—脅威アクターの文字による説明
- 身元—アクターを識別する情報
- タイプ—ハッカー、ハクティビスト、政府アクター、電子犯罪アクター、内部脅威など
- 動機—政治的、経済的または財政的、イデオロギー的、軍事的など
- 熟練度—未経験者、常習者、専門家、革新者など
- 意図された効果—軍事的、経済的、政治的な優位性、盗難、破壊、混乱など
- 観測された TTP—アクターによる使用が観測されている TTP
- 関連するキャンペーン—アクターに起因するキャンペーン

サイバー脅威インテリジェンスの分析には、脅威アクター情報の追跡と共有が不可欠である。組織はこの情報によって、直面している脅威、および攻撃者やグループが意図する具体的な目的や使用機能についての理解を深めることができる。組織間で脅威アクター情報を共有することは、すべての参加者がこれらの脅威をより包括的に理解するのに役立つ。

脅威アクターの情報は、政府や業界のサイバー脅威情報源から得られることが多い。

[12]参照：http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

ISAC などのより確立された共有組織は、独自のサイバー脅威分析チームを用いて、サイバーセキュリティリスクやメンバーに対するリスクの管理に関連する脅威アクターを追跡する場合がある。

脅威アクター情報は、多くの場合、本質的により戦略的であり、状況認識および意思決定に関する情報の提供に利用される。

4.7 戦術、技術、および手順

戦術、技術、および手順は、脅威アクターまたはキャンペーンの行動または能力の記述に使用される非常に広範な情報を表す。TTP は、攻撃者が何をどのように行うかを明らかにする。そのため、TTP には、特定の攻撃者の行動、使用されたリソース、標的となる被害者の情報、および標的となる脆弱性または弱点が含まれる。

一般的に共有されるフィールドを以下に示す:

- タイトル
- 説明
- 意図される効果
- 行動—特定の攻撃パターン、マルウェア、またはエクスプロイト
- リソース—ツール、インフラ、または登場人物
- 対象の被害者—標的となっている人々、組織、情報、アクセス
- キルチェーン フェーズ
- 関連する TTP

マルウェアの各サンプルは、一般的に共有される種類の TTP の 1 つを示す。
マルウェアのサンプルを共有することで、サンプルを広範囲にわたり分散して分析することが可能になる。また、マルウェアの高レベルの傾向分析および標的となっている組織の種類の高レベルの傾向分析の両方を実行できる。

TTP は、サイバー脅威インテリジェンス分析の重要な要素であり、インシデント調査時に検出された TTP を記述するために、インシデントという文脈において頻繁に関連付けられたり共有されたりする。サイバー脅威指標により、下位レベルの観測値が TTP に関連付けられ、防御者が検討すべき事項の判別が容易になる。キャンペーンおよび脅威アクターは、以前に観測された、または予期された攻撃者の能力の特性を示すために TTP に関連付けられることが多い。

サイバー脅威アナリストは、集計された TTP 情報により、脅威をより全体的に理解することや、特定の攻撃者をより詳細に理解することができる。この情報により、戦略的、戦術的、即時の状況認識、意思決定、および行動に関する情報が提供される可能性がある。

4.8 キャンペーン

キャンペーン情報により、攻撃者またはグループが意図する効果についての情報を、攻撃者またはグループが使用するツール、関与していると考えられる脅威アクター、グループに関連付けられているインシデント、およびその他の関連するキャンペーンに関連付けることができる。

一般的に共有されるフィールドを以下に示す:

- 名前—キャンペーンに使用される短い名前またはエイリアス
- 説明
- 意図された効果—軍事的、経済的、政治的な優位性、盗難、破壊、混乱など
- 関連する TTP
- 関連するインシデント
- 関連付けられたキャンペーン
- 帰属(関連する脅威アクター)

脅威インテリジェンスの分析には、キャンペーン情報の追跡と共有が不可欠である。組織はこの情報によって、直面している脅威、および攻撃者やグループが意図する具体的な目的や使用機能についての理解を深めることができる。組織間でキャンペーン情報を共有することで、すべての参加者がこれらの脅威をより包括的に理解するのに役立つ。

キャンペーン情報は保護必要度が高いため、組織はキャンペーン情報の共有の際に帰属情報を含めることに消極的になる可能性がある。キャンペーンの帰属情報を共有することは、所定のキャンペーンについての幅広い理解を促す上で必ずしも必要というわけではない。

キャンペーン情報は、政府や業界のサイバー脅威情報源から得られることが多い。ISAC などのより確立された共有組織は、独自のサイバー脅威分析チームを用いて、サイバーセキュリティリスクやメンバーに対するリスクの管理に関連するキャンペーンを追跡する場合がある。

キャンペーン情報は、多くの場合、本質的により戦略的であり、状況認識および意思決定に関する情報の提供に使用される。

4.9 分析レポート

ISAO が参加者に提供できる多くの重要な種類の情報、分析に基づいている。多くの組織が情報共有に焦点を当てているが、分析によっても、ISAO のステークホルダーにとって価値のある情報を提供できる。分析に従事する参加者は、その情報を即時の意思決定、戦術的意思決定、および戦略的意思決定に活用できる。

コミュニケーション レポートの一般的な種類は、アラート、通知、評価である。情報分析レポートの内容の例を以下に示す:

- 企業の中核機能に対する脅威の影響
- 攻撃ライフサイクルに関連する脅威活動の説明
- 組織のインフラに関連した悪意のある活動の傾向
  (例えば、最も多く標的となったインフラ、最も悪用された設定など)
- 緩和の有効性
- サイバー脅威の傾向レポート
- 脅威分類レポート
- 事前対応(評価)レポートと事後対応(インシデントの事後分析)レポート

4.10 脅威インテリジェンスのレポート

脅威インテリジェンスのレポートは、傾向の概要を示すレポートから特定のキャンペーンの詳細な分析まで幅広いカテゴリを持つサイバー脅威情報である。ベンダー、政府、および独立した組織は、オープンソース インテリジェンス レポートを含むさまざまな種類のレポートを作成する。特定のインシデントを対象とするレポートや、予測的なレポートがある一方で、現在のサイバー脅威状況を示すレポートもある。これらのレポートは、サイバー脅威インテリジェンスの全範囲が対象となる場合があり、戦略的、戦術的、および即時の応答情報を提供する。レポートには、キャンペーン、脅威アクター、TTP、および検知指標の情報が含まれることがある。一部のレポートは、数年間にわたるサイバー脅威の分析と追跡の結果である。

4.11 セキュリティの勧告とアラート

セキュリティの勧告とアラートは、国際的な CERT、政府、ソフトウェアやセキュリティツールのベンダー、ISAC、非営利組織、セキュリティ調査員など、さまざまな情報源により公開されている。これらの公開の形態は、重要なソフトウェアベンダーのセキュリティ勧告の再ブロードキャストから、新しい重要な脆弱性やセキュリティ問題への関心を高めることを目的とした専用の製品までさまざまである。

国際的な主要 CERT の多くは、セキュリティの勧告とアラートを提供している。

例えば US-CERT は、現在のセキュリティ上の問題、脆弱性、エクスプロイトに関するアラートを公開している。これらのアラートは、問題の説明、問題による影響の説明、問題に対処するために推奨される緩和策の提供を目的としている[13]。

セキュリティの勧告やアラートを共有することで、意思決定や行動に影響を与える、あらゆる範囲の即時情報、戦術的情報、戦略的情報を提供することができる。

[13]参照:https://www.us-cert.gov/ncas/alerts

4.12 運用上の手法

ISAO メンバー間で運用上のサイバーセキュリティ手法を共有することは、組織が独自のサイバーセキュリティ手法を進展させる上で、協力して信用を築き、互いに学び合い、フィードバックを収集するための重要な方法である。組織はこの種の共有により、他のメンバーが成果を得ている可能性のある問題解決の方法からメリットを受けることができる。この種の情報には、ベストプラクティスまたは効果的な手法、効果的なアーキテクチャ、効果的または効果的でないシステム設定、人員配置戦略などが含まれる可能性がある。効果がなかった取り組みを共有することは、どのような取り組みが行われたかを知ることができるため、ISAO メンバーにとって有益である場合がある。

5 情報を共有する際に検討すべきステップ

最初のステップは、ISAO とそのメンバーが共有する情報を特定することである。ISAO とそのメンバーは、ISAO の目標とミッション、およびメンバーと顧客のニーズと機能に基づいて、共有する情報、および共有するタイミングを決定する必要がある。共有する情報の特定は、その後行われる決定事項の土台となる。

共有する情報を特定したら、ISAO とそのメンバーは、共有を希望する要保護データとそのデータの処理手順を明確にする必要がある。
例えば、情報源を開示しない共有を可能にする ISAO もあれば、共有情報の共有元のメンバーを特定した開示を必須とする ISAO もある。情報源を開示しないことで、メンバーはより安心して共有を行える可能性がある。しかし、情報の共有元が分かることで、その情報の質と正確性がより保証される可能性がある。その他の例としては、個人識別情報（PII）、ビジネス要保護情報、または法的保護要件のある情報などがあるが、これらに限定されない。ISAO は、組織、メンバーシップ、および顧客の運用上のニーズと法的要件を満たす最適なポリシーを確立する必要がある。要保護データについて詳しくは、第 8 章「運用上の考慮事項」および第 9 章「情報のプライバシー」を参照。

共有する情報およびそれに伴う保護必要度の課題が特定されたら、ISAO の目標を達成するために使用される仕組みと手法についてメンバーの合意を得ることが重要である。

例えば、ISAO は以下の 1 つ以上の事項を実行できる:

- メンバーの共有のためのプラットフォームを提供して、メンバーの共有を促進する
- 情報を収集する技術を実装して管理する
- 脅威インテリジェンスのフィードを提供するサードパーティのサービスに加入する
- オープンソースのレポートを収集、集約、配布する
- パートナー組織からレポートを収集、集約、配布する

ISAO は情報共有を自動的に行うか、対面によって行うか、またはこれら 2 つを組み合わせて行うことができる。メンバーと ISAO の間の共有は、マシン対マシンによる自動制御によって行われる可能性がある。検知指標を自動化された方法で共有することで、情報のより迅速な共有、共有する検知指標の数の増加、共有データの品質の向上も可能になる。
この技術は初期段階にあり、メンバー間や場合によっては他の ISAO との間で共有する際は、組織的に確立された情報の自動交換のポリシーに従って運用する必要がある。ほとんどの場合、ISAO はメンバーとの共有に複数の手段を使用する。人対人の共有では参加者間の信用が高まるため、参加者が共有を進んで行いやすくなる。このように、自動交換と人間による交換のどちらにもメリットがある。

ISAO とそのメンバーは、ISAO の運営の基本となる目標、原則、手法を確立するために、ISAO 内やパートナー間で共有される情報の使用方法の手引となる情報共有ポリシーを策定する必要がある。これらのポリシーには、共有する情報の種類、要保護データの共有、特定、処理の適切な手法、および保護要件を含める必要がある。考慮すべき他の領域としては、以下が挙げられる:

- 共有される情報にどのように印を付けるか？
- メンバーは ISAO から受け取った情報を外部に共有できるか？
- ISAO は他のパートナーや他の ISAO と情報を共有できるか？
- 電話、仮想会議、および対面会議を介して共有される情報はどのように処理する必要があるか？
- 進行している共有情報および中断している共有情報に対して、ISAO はどのようなポリシー、プライバシー管理、保護を適用する必要があるか？

このようなポリシーを組み入れるには、さまざまな方法がある。以下にその一部を記載する:

- メンバーに秘密保持契約の締結を依頼する
- 入念に設計された情報共有プロセスを使用する
- 効果的で包括的な ISAO 従業員行動規範の順守を求める
- Traffic Light Protocol（TLP）[14]などを使用して、要保護情報が受信権限のあるユーザーにのみ共有されるようにする
- 運用理念（CONOPS）において情報をどのように使用できるかを詳述する
- 個別かつ単独の情報利用規約を ISAO 内に作成する

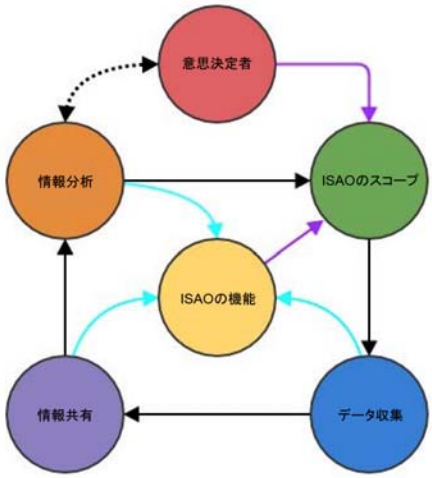
[14]参照：https://www.us-cert.gov/tlp

メンバーが自身や他者にとって有益な情報を確実に共有および受信するために、ISAO はこれらのポリシーの定期的な再評価を検討して、メンバーのニーズが常に満たされているようにする必要がある。

6 情報分析

情報の適切な共有および分析には、参画するアナリストにとって有用かつ利用しやすい実用的なインテリジェンスを生成することが不可欠である。情報分析の目的は、他のデータとの関連性を考慮に入れながらデータに含まれる価値を取得および理解し、それにより情報を生成し、隠れた洞察を導き出すことである。図 4 に示すように、情報共有と情報分析の相互依存関係が、データ収集、ISAO のスコープ、および ISAO の機能と組み合わされて、意思決定者にインテリジェンスを提供するためのフレームワークが形成される。

図 4. インテリジェンスを提供するためのフレームワーク



サイバーセキュリティ情報分析には、異常な活動または悪意のある活動の兆候または発生についてデータを調査することが含まれる。調査の結果から、類似する脅威データへの関連付けにアナリストが使用可能な成果物や証拠を特定できる。これは、有害な TTP、脅威グループ、またはキャンペーンを識別するのに有用である。すべての ISAO は何らかの形で分析を行う。それは単に関連情報を共有するための判断である場合もある。ただし ISAO は、複数の情報源からのデータをまとめて、参加者の専門知識を活用して実用的なインテリジェンスを生成する独自の立場にある。

情報分析には、利用可能なデータソースを基にした解釈および運用上の活用方法の模索が含まれる。第 1 段階は、共有データの初期調査である。例えば、ISAO は共有データを評価して、複数の組織にわたって関連する脅威を特定することができる。第 2 段階では、アナリストは関連する脅威データを解釈して、脅威グループ、キャンペーンの要約、またはビジネス上のリスク評価を作成する。

情報分析には、いくつかの固有の課題がある。1 つ目は、ISAO のメンバーにとって関心がある問題を特定することである。2 つ目は、データフィードおよびデータリポジトリの多くのデータの流れの中から該当するデータを特定することである。3 つ目は、ISAO のメンバーが適切なレベルで分析を利用できるようにして、他のデータとの関連性や組織への適用性を理解しやすくすることである。

ISAO とそのメンバーは、収集されたデータ要素と、データへのアクセス方法およびデータのセキュアな保存方法について合意する必要がある。ISAO はその後、使用する分析アプローチと、メンバーにとって有益なレポートの種類について検討することができる。ISAO の各メンバーは、インテリジェンスの使用に対してさまざまな要望を持ってい

る可能性がある。

例えば、セキュリティ運用またはネットワーク運用に焦点を当てている ISAO は、ネットワークのノイズから適切なデータをフィルタリングするための情報を必要とする可能性がある。また、ISAO によっては、複数のメンバーにわたって発生している脅威活動に対処することを選択する可能性がある。ISAO は、どの種類のレポートが最も有用か、および各メンバーがデータの収集に対してどのような貢献ができるかを理解するために、メンバーへの調査を検討する必要がある。

ISAO が提供する分析オプションには、初めて発生した活動または異常な活動の検出、ソフトウェアやネットワークの脆弱性へのエクスプロイトの識別、関連する脅威活動の収集、または発生源の特定（個人、犯罪組織、または国家）が含まれる。分析サービスを検討している ISAO は、分析を可能にするため、および脅威に関するメンバーのコミュニケーションを促進するためのデータストアまたは設備（あるいはその両方）の確保を検討する必要がある。例えば ISAO は、検出のための指標、対応のための脅威情報、およびリスク管理のための発生源の特定からなる脅威ナレッジベースを作成することができる。この脅威ナレッジベースにより、ISAO とその参加者は分析手法を使用したり、知識や評価を共有したりすることができる。

共有する分析または共同作業する分析の種類についてはすべてのメンバーが合意しなければならないが、ISAO が作成を検討できる共通レポートは多数存在する。それらのレポートには以下が含まれるが、これらに限定されるものではない：

- ピボットレポート—接続しているホップポイントを示す、観測された IP アドレス。メンバーはこのレポートを使用して、共通の懸念のある地域を特定できる。
- マルウェア—ISAO は、毎月メンバーがネットワーク上で確認したマルウェアのハッシュ値を収集することができる。
- キャンペーン—ISAO のメンバーは、ランサムウェアやビジネスメール詐欺など、特定のキャンペーンに関する情報の共有を必要とする可能性がある。また、アクターによる使用が観測された TTP を共有することもできる。

アナリストによる評価は、関連する脅威情報をよりよく理解するのに役立つ。ただし、アナリストの環境や視野によっては、脅威を分類する際や脅威活動をアクターに帰属させる際に偏りが生じる可能性がある。各 ISAO は、この偏りを緩和するための独自の立場にある。ISAO は脅威インテリジェンス共有コミュニティーを設立することにより、アナリストによる偏りを減らし、検出、メンバー同士のコミュニケーション、外部による確認を通じた継続的なフィードバックを提供するような文化を育むことができる。

メンバー間の傾向やパターン分析の共有を支援する上で、匿名によるメンバー調査が有効な手段となる可能性がある。メンバーは共同のツールを使用することで、各組織から集約された測定基準情報を合意した頻度で収集できる。これには、フィッシング試行回数、侵入試行回数、侵入成功回数、侵害されたアカウント数、分散型サービス妨害攻撃回数が含まれる。ISAO はこのデータから、具体的にいずれかのメンバーを情報の共有元として開示することなく、メンバーの傾向分析を実施できる。例えば、ISAO の

週次または月次のレポートでは、事業の規模、セクター、活動が発生した時刻、攻撃者の IP アドレスと発信元の国（判明している場合）、使用された攻撃の経路や手段などによって攻撃の種類を特定できる。

6.1 分析の検討事項

専門の情報アナリストによるサービスを提供する ISAO は、さまざまなデータソース（部外秘と公開の両方）からのデータをセキュアに格納できる必要がある。また、データのレビュー、脅威の解釈、およびインテリジェンス評価の経験が豊富なアナリストを活用できる必要がある。

分析を行う前に、ISAO はまずメンバーによるデータ品質測定を支援できる。傾向とパターン分析の有効性は、正確かつ適切な入力データによって決まる。

メンバー組織が合意する場合、ISAO はメンバーのネットワーク上にあるセンサーの利用を検討し、レポートやアラートの生成用に ISAO が管理するセキュアな共有リポジトリに、特性についての報告を返すことができる。ISAO によっては、メンバーがこのリポジトリにアクセスできるようにして、個々のメンバーが独自の分析レポートを照会・生成できるようにする場合がある。

各 ISAO は、各 ISAO 間および（任意で）政府機関との間で統合可能な共通語彙を、サイバー活動の報告で使用することを検討する必要がある。

ISAO がデータを蓄積・集約するに従って、正常な行動基準を作成し、将来の行動の異常や指標を特定する予測分析を行うことができる。

アナリストは最終的に、意思決定者に評価を伝える。コミュニケーション レポートの一般的な種類は、アラート、通知、評価である。ISAO は、メンバーに調査を行って、意思決定者にとって最適なコンテンツ形式を決定する必要が生じる場合がある。

6.2 分析サービス

ISAO は参加者に信用できる環境を提供し、各アナリストが協力して適切な情報を共有するよう促すことができる。これらの分析活動を提供、促進、主導する ISAO は、その取り組みの有効性を飛躍的に高めることができる。ISAO は、メンバーの分析を集約する役割を担うことができる。または、一定レベルの機能を ISAO に組み込むことができる。メンバーのアナリスト、または ISAO のアナリスト、あるいはその両者のいずれを用いるかは、ISAO の情報共有の目標に応じて決定する必要がある。

各 ISAO は何らかの形で分析を実行する。これは、関連情報を共有するための判断から、完全なパターンおよび傾向の分析に至るまでさまざまである。ISAO は、下記で説明する項目に加えて、運用指向の他の分析の成果物を生成することができる。また、ISAO は、これらの運用上の成果物にとどまらず、組織の将来の計画やリソース要件に影響を与える意思決定者を支援する傾向分析レポートや戦略分析を提供する立場にある場合もある。

ISAO が分析をサポートする方法の例を以下に示す:

- **リスクの認識と緩和のためのコミュニケーション。**分析において ISAO が実行可能な最も価値のある貢献の 1 つは、ISAO の参加者やアナリストなどの間の協力を促進し、サイバーセキュリティのリスクおよびそのリスクを緩和するためのアプローチについて参加者の認識の向上および教育を行うことである。場合によっては、専門家間の集合知の共有や協力には少数の ISAO 参加者しか関与しないことがあるが、ISAO 参加者とのより広範なコミュニケーションにつながる可能性がある。これらの「*戦術的*」コミュニケーション(すなわち運用に重点を置いたコミュニケーション)では、攻撃の成功を防ぐためのガイダンスの提供、特定のリスクを緩和するための手法や手順の特定、他者が採用している効果的な手法の特定、参加者の経験と参加者が取った行動の有効性に関する詳細の報告が行われる場合がある。

- このようなコミュニケーションは、ISAO 構成メンバー(経営幹部、マネージャー、運営担当者)内のさまざまな対象者に合わせて調整でき、必要に応じて、または定期的なコミュニケーションとして提供することができる。コミュニケーションの形態には、参加者や他者との間での電子メール、レポート、ブリーフィング(Web セミナー)、電話会議、その他の交流会や共同イベントなどがある。これらのコミュニケーションは、組織のために情報に基づいた意思決定を行う責任者の支援となる。

- **アラートの通知。**ISAO での情報の流れを調べることにより、ISAO は、参加者や他者が特に関心を示す、新規の、または変化する、または拡大するサイバーセキュリティのリスクやインシデントを特定する機会を得る。この分析により、メンバーやパートナーに緊急通知、危機状況の通知、またはその他のレベルの通知を行うことができる。また、この分析は、リスクを緩和するために実行できる緊急処置に関する情報および勧告を ISAO がメンバーやパートナーに提供する上で有用である。続いて更新アラートと追加分析を提供することで、ISAO およびそのパートナーなどがインシデント、脅威、またはリスクの進行状況を理解しやすくなる。

- **インシデント対応の調整。**ISAO によっては、サイバーセキュリティ関連のインシデントへの対応を理解する役割を想定する場合もあれば、インシデントへの対応に積極的に関与する役割を想定する場合もある。ISAO は、一部のメンバーからインシデント対応の支援を依頼されることがある。そのような場合、ISAO は、必要な運用調整の判断および状況が進行して解決された際に実行する対応処置の有効性の判断のために、メンバー組織のアナリスト間での協力の機会を提供することができる。
  事後レポートおよび根本原因レポートを作成して、ISAO 参加者および他者の間で共有される有益な情報を提供できる。
  ISAO がインシデント対応を調整する役割を担う場合、そのインシデント対応の役割の具体的な価値、インシデント対応における役割、およびそれをアクティブ化するトリガーを特定することを検討する必要がある。

7　アーキテクチャの検討事項

人はさまざまな方法で情報を共有するが、情報共有は、共有モデル、共有方法、および共有の仕組みの 3 つのアーキテクチャ構造で捉えることができる。

モデル、方法、および仕組みの実装方法は根本的に、ISAO メンバーのニーズ、管理者の能力、コミュニティーの目標、利用可能な技術、コミュニティーにおける信用の中心と推進力に応じて大きく異なる。

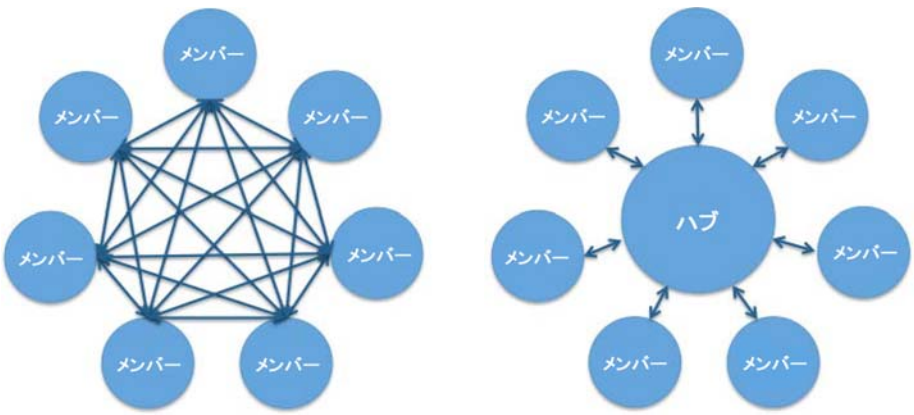
各 ISAO は、それぞれの運用上の要件に適したモデルと仕組みについて検討する必要がある。これを行うのに最も適した方法は、すべての情報共有と分析のサービスおよび接点を、持続可能なメンバーの価値を提供する取り組みに対して包括的にマッピングする方法である。これにより、ISAO は情報共有と分析のアーキテクチャを構築し、メンバーの価値および ISAO の存続と発展を長期に渡って戦略的に持続させることができる。

7.1　共有モデル

このセクションでは、ISAO が採用を検討する可能性のある 2 つの一般的な共有モデルであるピアツーピア共有モデルとハブアンドスポーク共有モデルについて詳しく説明する。これらのモデルは、主に情報の「責任者」の立場の者によって推進される。また、これらのモデルは複合的アプローチで使用することができる。

ピアツーピア共有モデルとハブアンドスポーク共有モデルは、恐らく新しい ISAO が設立の際に検討できる最も有用な基本的取り決めである。

図 5. 共有モデル



7.1.1　ピアツーピア

ピアツーピア共有モデルは一般的に、コミュニティーの任意のメンバーが他のメンバーと対話・共有する能力によって定義される。ピアツーピア ネットワークは、小規模なコミュニティーや、メンバーがコミュニティーの一部のメンバーとしか対話しない場合に特に有益である。また、メンバーの信頼関係が対等ではない ISAO、および構成や現在の脅威などに応じて頻繁に変化する非常に動的な状況下でメンバーが共有を行う ISAO に

とっても、特に有益である可能性がある。一般的に、コミュニティー内の誰と共有するかを決定する際の選択において、メンバーには高い自由度がある。このモデルには、イベントごとの共有や、共有の方法および内容を管理する「見張り役」は存在しない。これは、責任者（ISAO の経営陣など）が共有ポリシーの策定や施行、あるいは他の管理的な業務を行わないということを意味するものではない。言い換えれば、コミュニティーのメンバーは一般的に、策定された ISAO のポリシーと手順に基づいて、および使用されるツールの範囲内で、適切と見なしたタイミングで、適切と見なした内容を、適切と見なした相手と共有する。

このモデルの課題は、コミュニティーのメンバーが増加した場合に多数の信頼関係を管理するのが困難な点である。さらに、このモデルでは同じ情報を重複して共有する可能性が高く、ISAO の技術やその他の条件によっては、非効率な「混乱」が生じる可能性がある。

7.1.2 ハブアンドスポーク

一般的に、ハブアンドスポーク共有モデルには、コミュニティーの中心すなわちハブに「見張り役」が配置される。メンバーはハブを介して共有を行うが、人、プロセス、技術の組み合わせによって、コミュニティーの他の部分への再配布が促進される。この共有モデルにより、コミュニティーの利益のために情報交換を一元化する機会、形式化する機会、または他の方法で影響を与える機会が得られる。
これは ISAO が管理する形式をとる場合がある。この ISAO の管理には、多種多様なメンバーやベンダーの脅威インテリジェンスの配布と検証、メンバーの脅威分析サービスを代行することによるスケールメリットの実現、ポリシーの施行、あるいは単に、ISAO の日々の活動におけるより中心的で明確な役割の遂行がある。さらにハブは、ポリシーと手順、最近のインシデントやキャンペーンの分析、または ISAO に関連するその他の分野のいずれに関わるものであっても、コミュニティーにとって唯一の「正しい情報」が存在する論理的な場所である。

このモデルには検討すべき課題がいくつかある。ハブへの依存は、想定通りにハブが機能していない場合に問題が発生する可能性がある。
この共有モデルを成功させるためには、ハブにおける人、プロセス、技術に高い信用が必要である。
また、ハブの信用レベルにかかわらず、メンバーは常に ISAO の任意のメンバーとの間にさまざまなレベルの信頼関係を構築する。常にハブを通じて脅威データまたはサイバー脅威指標を配布することは、ISAO メンバー間の個人的な関係の発展を阻害する可能性がある。関係の構築はメンバー間の信用につながる。信用はまた、脅威インテリジェンス共有を成功させるための主要なパフォーマンス指標といえる。

7.1.3 複合的アプローチ

ISAO は、ピアツーピア モデルおよびハブアンドスポーク モデルの課題に対処するために、これら両方の要素を組み合わせた複合的アプローチを形成することができる。これは実質的に制限なく形成することができるが、考慮すべきいくつかの可能性を以下に示す：

- ハブの強みおよび中核となる機能に基づいて、再配布または分析用に一部の種類の脅威インテリジェンスを、ハブを介して伝達する。予算、人材、技術、地理、およびメンバーの要件や目標に対するこれらの要素の影響といった検討事項はすべて、ハブがどのような義務とタスクを負うことが適切かを判断するのに役立つ。
- 戦略的インテリジェンスなどの特定の種類のインテリジェンスについてはピアツーピア共有を活用する。例えば、脅威アクターのプロファイルを作成するためにパートナーと共同作業することは、コミュニティーのリソースを活用し、ISAO のメンバー間で関係と信用を構築し、ISAO コミュニティーに積極的に貢献するための優れた方法である。また、ピアツーピア モデルとハブアンドスポーク モデルの両方の側面を組み合わせて、ISAO ハブを介して作業の成果物を再配布できる。

これらの共有モデルは、ISAO がどのように情報を共有できるかを高レベルで概念化したものである。新しく形成する ISAO で何をすべきかをよく理解したうえで、その ISAO で採用する適切な共有方法と共有の仕組みを選択することは、作業を効率的かつ効果的に実行する上で重要である。

7.2 共有手法

このセクションでは、上記のいずれかのモデルに適用できる手法について詳述する。共有手法は主にコミュニティーの要件と運用の概念に従っており、特定の種類の共有を可能にするために ISAO によって採用されたツールや技術にも関連している。

7.2.1 パブリッシュ／サブスクライブ

脅威インテリジェンスを共有するパブリッシュ／サブスクライブ方式は、定期的または不定期に情報を公開するプロデューサーで構成される。プロデューサーが公開した情報は、コミュニティーの 1 人以上のメンバーによって個別に購読される。このアプローチは、ピアツーピア共有モデルにもハブアンドスポーク共有モデルにも適用できる。ピアツーピア ネットワークの場合は、例えばプロデューサーは、他のメンバーがフィードを取得するリポジトリでサイバー脅威検知指標の共有を自動化できる。あるいは、プロデューサーが掲示板／フォーラムに投稿し、加入者がアラートを受信することができる。ハブアンドスポーク モデルの場合、ISAO ハブがパブリッシャーとなる場合がある。プロデューサー（メンバー）は、ISAO 加入者層に公開する前に、処理（通常は、検証、修正、重複排除、または他の既知の脅威インテリジェンスとの関連付け）を行うためにハブに送信できる。ハブの厳密な役割は、ISAO CONOPS やその他の条件によって大きく異なる。ハブアンドスポーク モデルでのパブリッシュ／サブスクライブ手法の利点の 1 つは、ISAO が情報を中央で集約・分析することで、インシデントまたはアクターのより詳細かつ完全な実態を公開できることである。この手法は、多くの参加者がさまざまな知見および分析を共有するような、急速に変化する環境において非常に有用である。

7.2.2 クラウドソーシング

クラウドソーシングは、ISAO の各メンバーがディスカッション スレッド、自動サイバー脅威共有リポジトリ、またはその他のシステムに共同で寄与して、粒度の細かい脅威データをより一貫性のある脅威インテリジェンスに有機的に変換する際に行われる。インテリジェンスのクラウドソーシングに参加することにより、メンバー間で情報も共有される。上記のパブリッシュ／サブスクライブ方式と同様に、クラウドソーシングはピアツーピア ネットワークとハブアンドスポーク ネットワークの両方で実行できる。主な違いは、一方ではクラウドソーシングをハブ経由で主導する中央機関が存在するが、もう一方ではコミュニティー間で有機的に自由に行動できる点である。当然、どちらも非常に効果的である。クラウドソーシングの利点の 1 つは、ISAO メンバー間の仮想的な相互交流によって信用が築かれ、コミュニティーが強化されることである。

上記の手法は、ISAO が CONOPS をサポートするために使用するツールおよび技術に密接に関連する、一般的な 2 つの共有手法である。新しい ISAO は、既に有効と見なした共有手法を導入するための特定のツールを検討できる。あるいは既に使用しているツールによって、使用可能な共有方法が決まる場合がある。

7.3 共有の仕組み

ISAO のメンバーとパートナー間での情報共有には、さまざまな仕組みと手法が使用される。表 2 は、ISAO が初期のまたは追加の共有機能として検討できる仕組みと手法の種類を示している。選択した仕組みと手法は、共有される情報の範囲、適時性、保護必要度に合わせて調整する必要がある。

情報共有は、1 対 1、1 対多、多対多、多対 1 で行われる可能性がある。そのため、ISAO がコミュニケーションと情報共有に対して選択する手法は、メンバーのために達成しようとしている全体的な目標を反映している必要がある。

情報の保護必要度を満たすため、情報共有に使用される手法や仕組みは、ISAO のポリシーやその他の権限機関の制限に従って、情報の保護および権限のあるメンバーへの情報の提供が可能でなければならない。例えば、要保護情報の処理および配布に Traffic Light Protocol（TLP）を使用する ISAO は、TLP ポリシーに準拠するための機能を提供する仕組みを使用する必要がある。

情報源の匿名性が必要な場合は、追加の情報共有プロセス、手順、および機能が ISAO で必要になる。そのため、ISAO が選択した手法とその運用手順は、ISAO メンバーの目標を達成するために必要な運用機能、セキュリティ機能、および管理機能を提供する必要がある。

また、情報共有の仕組みは、ISAO 参加者による情報の受信の重要性、適時性、緊急性も考慮して選択する必要がある。メンバーは、所定の情報源から取得する情報を認証および信用できなければならない。場合によっては、時間的緊急性がある情報を確実に配信するために、情報の受信を能動的に確認する必要がある。

ISAO 間での効果的な情報共有の方法には、主要な検知指標と防衛手段のための自動情報共有プラットフォームの使用と、ISAO メンバーからの追加情報が含まれる。また、ISAO は、脅威インテリジェンス提供機関から受信したフィードを取り入れてメンバーに情報を提供する場合がある。または、メンバーがこれらのフィードを購読して ISAO や他のメンバーに関連情報を中継する場合もある。電子メール、チャット、およびソーシャルメディアの各プラットフォームを使用して、ISAO メンバーの担当者間の共同作業と情報共有を可能にすることもできる。

下記の表 2 に、検討すべきいくつかの共有の仕組みを示す。

表 2. 検討すべき共有の仕組み

以下に記載する仕組みは、さまざまなオプションとその適用性に関する一般的なガイダンスを示す。								
説明		**対象（※注）**				**匿名性を確保できるか**	**アクセス制御機能**	**補足**
		1 対 1	1 対多	多対多	多対 1			
対面会議	個人が、承認された者に限定された参加者と物理的に対面する。		X	X		いいえ	単一レベル：承認された者すべてが情報を受信する。	情報へのアクセス制御は、各手順を通じて選択した参加コミュニティーに限定できる。
テレビ会議／WebEx など	会議および共同作業用の商業サービス		X	X		いいえ／はい	単一レベル：承認された者すべてが情報を受信する。	匿名性の確保には中央管理機能が必要。通常は匿名ではない。情報へのアクセス制御は、各手順を通じて選択した参加コミュニティーに限定できる。
電子メール（通常）	インターネットベースの電子メール	X	X	X	X	いいえ／はい	配信を制限可能	匿名性の確保には中央管理機能が必要。通常は匿名ではない。配信の制限は可能であるが、参加者が多数の場合に管理が困難である。
電子メール（暗号化メッセージを使用）	暗号化されたファイルまたはメッセージ	X	X			いいえ／はい	制限に基づく情報へのアクセス	エンドツーエンドの暗号化メカニズムの使用。 例：S/MIME、PGP など
電子メール – リストサーバー	メーリングリストを管理するためのサービス		X	X		いいえ／はい	配信を制限可能	匿名性の確保には中央管理機能が必要。通常は匿名ではない。
メッセージングサービス（ショートメッセージ、拡張メッセージ、マルチメディアメッセージ）	キャリアおよびベンダーが提供するサービス	X	X			いいえ	配信を制限可能	例えば Slack や HipChat など。チャレンジレスポンス認証は、なりすましを防止できる。
ピアツーピアネットワーク	サーバーレスネットワークとして位置づけられる。			X		いいえ	配信を制限可能	さまざまなリスクがあるため、許容可能な P2P ソフトウェアの種類、それらを介して共有できる情報を定義するセキュリティポリシーを実装する必要がある。

以下に記載する仕組みは、さまざまなオプションとその適用性に関する一般的なガイダンスを示す。								
説明		**対象（※注）**				**匿名性を確保できるか**	**アクセス制御機能**	**補足**
		1 対 1	**1 対多**	**多対多**	**多対 1**			
Web サイト（公開）	サイトの URL で利用可能なすべてのページ		X			いいえ／はい	制限なし	投稿された情報の匿名性を保証する責任を負う中央管理機能。
Web サイト（非公開）	Web サイトの一部のページではアクセス資格情報が必要		X			いいえ／はい	単一レベル：Web サイトのアクセス資格情報を持つ者	投稿された情報の匿名性を保証する責任を負う中央管理機能。
セキュアポータル	Web ブラウザーを使用してインターネット経由でアクセスできる、デジタルのファイル、サービス、および情報のコレクションへのコンピュータ ゲートウェイ。検索可能なデータベースへの複数レベルのアクセス制御を備えたクライアントサーバーベースのシステム。		X	X	X	いいえ／はい	承認されたアクセスポリシーと資格情報に基づいた複数レベルのアクセス制御。	中央管理機能によって、承認およびルールベースのアクセス制御ポリシーが実施される。匿名性は、匿名アクセス資格情報の配布プロセスと、ポータル管理のポリシーおよび手順による投稿／レビューによって確保される。
自動化の仕組み	機械処理の仕組みにおいて、信用できるパートナーおよびコミュニティー間で自動的に共有されるサイバー脅威情報の構造化表示。	X	X	X	X	はい	承認されたアクセスポリシーと資格情報に基づいた複数レベルのアクセス制御。	例として STIX™（脅威情報構造化記述形式）言語が挙げられる。<https://www.mitre.org/sites/default/files/publications/stix.pdf>
通知サービス	通知サービスは、メッセージを生成して、サービスに加入しているユーザーまたは他のアプリケーションに送信する。	X	X			いいえ	承認されたアクセスポリシーと資格情報に基づいた複数レベルのアクセス制御。	通知は、電子メール、電話、ファックス、テキストメッセージなどで行われる。

※注:　1 対 1　1 人の送信者と 1 人の受信者
1 対多　1 人の送信者と複数の受信者
多対 1　複数の送信者と 1 人の受信者
多対多　複数の送信者と複数の受信者

8　運用上の検討事項

効力のある ISAO の形成に不可欠である信頼関係を実現する最良の方法は、組織がメンバー、パートナー、および情報共有者との間で運用セキュリティを共有する文化を構築することである。この文化は、適切に策定された ISAO の運用ポリシー、手順、認識、優れた手法を通して実現可能である。

ISAO の運用セキュリティへの取り組みには、次の検討事項を考慮する必要がある:

- ISAO への参加資格を有する者の基準と審査プロセスを確立する。
- ISAO が処理および伝達する要保護情報の全範囲を検査する。その後、リスクベースの評価を使用して、ISAO 全体および ISAO とやり取りをする際のメンバーに対して実施される ISAO の運用規則[15]、情報ポリシー、制御を策定する。
- ISAO が作成する分析成果物と併せて、メンバーシップの識別、ISAO と共有する情報の所有権、共有された情報の使用、およびメンバー間や他者との情報共有に対処する各ポリシーを定義する。これらのポリシーを実施するには、メンバーが実行する合意済みの制御と手法を文書化して、ISAO への参加条件とする必要がある。
- ISAO とそのメンバーへの情報の提供方法を、内容の機密性とプライバシーの保護のために実施される可能性のあるレビューのプロセスとともに指定する。
- 情報の適時共有を促す手順および情報の適時共有に優先順位を付ける手順を確立する。これにより、メンバーが最大の価値を実現できるようにするとともに、攻撃によって引き起こされる可能性のある差し迫った脅威に対処できるようにする。
- ISAO 内およびメンバー間で処理される各種の要保護情報にラベルを付けて処理するための手順を定義する。これには、当該用途で ISAC や他者によって現在使用されている Traffic Light Protocol (TLP)[16]アプローチの使用が含まれる場合がある。
- 情報源の匿名性によってメンバー間での共有と信用を促進させる手順と手法を規定し、ISAO の運用においてそれらを維持する。実際には、情報の所有者が匿名性は必要でない、または実用的でないと判断した場合に、情報所有者の権利に応じて手順を調整する必要が生じることがある。
- ISAO のリーダー／経営陣は、ISAO のセキュリティとプライバシーのポリシーに従って、メンバーに所定の行動規範と自身の責任を常に認識させるための積極的かつ定期的な認識への取り組みを行う必要がある。すべての変更は、参加者とともに十分に審査してから参加者に公表する必要がある。
- ISAO がリアルタイムまたはほぼリアルタイムの情報共有のために自動化機能を使用している場合、そのような機能は、ISAO または情報の自動共有に参加している者に重大な影響(良い影響と悪い影響の両方)を及ぼす可能性があるため、具体的な運用規則を策定しておく。
- ISAO の信用および契約に違反したメンバーを除籍するための手順と基準を設定する。ISAO メンバーとして人員を割り当てる組織は、割り当てた人員の状態に変更があった場合に ISAO に通知する。また、アクセス許可を定期的に確認して、有効でなくなったアクセス許可を即座に削除する手順を整備する。

[15]例:FS-ISAC の『Operating Rules』(https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf)を参照。
[16]参照:https://www.us-cert.gov/tlp

これらの運用上の検討事項は、ISAO が検討する必要がある一般的な事項のみを取り上げている。ISAO の具体的な運用セキュリティのポリシーと手順は、ISAO の固有の運用および取り扱う情報の保護必要度に対応する必要がある。ISAO の運用は時間とともに変化するため、運用セキュリティの手順およびポリシーの定期的なレビューによって更新が必要になる可能性がある。年次のレビューは、手順およびポリシーを最新状態に維持する上で効果的な確認手段となりうる。すべての変更内容は、組織の管理資料と整合していなければならない。

9 情報のプライバシー

サイバー脅威検知指標やその他の情報を任意のサイバーセキュリティ情報共有プロセスを通じて受信、分析、保持、使用、または配布する ISAO にとって、プライバシーの検討事項を十分に考慮および擁護すること、ならびに適用されるプライバシー法を認識および遵守することは重要である。ISAO は、情報のプライバシーの管理に焦点を慎重に合わせ続ける必要がある。プライバシー保護の確保は、情報共有プロセスに不可欠であり、ISAO 自体の全体的な体制に対するパートナーの信用を高める。ISAO は、プライバシーに配慮することにより、メンバーおよびパートナーの自主的な共有に関する障壁および懸念を管理または排除できる。個別のプライバシー責任者が存在するかどうかは ISAO の参加者により異なる場合があるが、これらの問題を ISAO 自体が管理できることは重要である。こうした成果は、ISAO の業績および実行可能性の持続と継続的な改善に役立つ。プライバシー保護の徹底に重点を置いたアプローチを取ることで、情報共有の全体としての利益をより広く認識できる。またこれは、適切なリスク管理構造の重要な部分でもあり、すべての ISAO にとって重要である。

プライバシーに関する検討事項には少なくとも、組織の個々のメンバー、法律で定められている範囲でサイバー脅威検知指標にデータを含めることができる個人のプライバシー、その他のあらゆる構成員、顧客、個人を含める必要がある。ISAO は、目標を達成しながらプライバシーを適切に保護するためには、サイバー脅威情報の許容される共有とプライバシー保護との間で均衡をとる上で役立つガイドを、メンバー、参加者、ISAO スタッフに提供することが重要である。このセクションの目的は、既存のすべての法律、およびその法律を適用するタイミング、方法、場面を記述することなく、ISAO がその均衡をとることを支援することである。

サイバー脅威検知指標を共有する前に、以下を含めて、共有される情報のプライバシーの関係事項を考慮することが重要である:

- 特定の個人に関する個人情報であることまたは、特定の個人を識別する情報であることを共有時に ISAO が把握した情報が検知指標の中に含まれるかどうか。
- その識別情報がサイバーセキュリティ脅威に直接関係していないかどうか。
- 関係している場合は、ISAO またはメンバーがそのような情報を特定し、必要に応じて削除したかどうか。

サイバー脅威検知指標の性質上、個人情報がサイバーセキュリティ脅威に直接関係している個人には、多くの場合、そのような情報の収集、入手、または修正への関与に同意する機会はない。ISAO は、収集したデータが個人のプライバシーに及ぼす影響を、可能な場合は制限し、サイバー脅威情報共有の取り決めの有効性を維持しようと努めなければならない。

サイバー脅威検知指標の一部として個人情報を共有することは 2015 年のサイバーセキュリティ情報共有法案(CISA)[17]で許可されているが、これは共有時にその情報が脅威に直接関係している場合に限られる。個人識別情報(PII)がサイバー脅威検知指標の一部ではない場合、その情報の受領、保持、使用、および配布を適切に制限しないと、ISAO は CISA の法的責任についての保護の対象から外れる以上のリスクにさらされる可能性がある。[18]DHS は、米国政府と共有する情報に関するプライバシー ガイダンス[19]を発行している。場合によっては、サイバー脅威情報の取り扱い時に要保護情報(PII、知的財産、企業秘密など)に意図せずに遭遇することがある。そのような情報を不適切に開示することは、個人、企業および他者に害を及ぼす可能性がある。したがって組織は、この情報を無許可の開示や改ざんから保護するために必要なセキュリティとプライバシーの制御および処理手順を検討して実施する必要がある。

多くの場合、データは法律、規制、契約上の義務のいずれかによって保護される必要がある。これには、サーベンス・オクスリー法、ペイメントカード業界(PCI)のデータセキュリティ標準、医療保険の携行性と責任に関する法律(HIPAA)[20]、2014 年の連邦情報セキュリティ近代化法(FISMA)、グラムリーチブライリー法(GLBA)、経済的および臨床的健全性のための医療情報技術に関する法律(HITECH)、および児童オンラインプライバシー保護法(COPPA)などの下で保護される PII やその他の要保護情報が含まれる。
連邦取引委員会と各州は、それぞれがプライバシーとデータの保護に取り組む。また、個人情報の情報源と種類、および関連性のある国境を越えた移動の有無によっては、

[17]参照:https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf
[18]米国商務省、国立標準技術研究所の『Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)』を参照
(http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf)
[19]参照:https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
[20]参照:https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

米国以外の管轄の法律が適用される可能性がある。これらの法令のすべてまたはいずれかの対象となる情報をすべての ISAO が取り扱うわけではないため、ISAO は必ずしもこれらのすべての法律を理解する必要はない。しかし ISAO は、受信、所有、または共有する情報がある場合、いずれが特定の規制の対象であるかを把握し、それらの情報を特定して適切に保護することが重要である。

ISAO は、サイバー脅威検知指標に関連しない PII やその他の要保護データの共有に関するポリシーを確立する必要がある。上述のように、ISAO は、保持または保管するデータについて HIPAA、PCI、または他の規制の対象となる可能性がある。例えば、クレジットカードの支払いを収集する ISAO は PCI 規制の対象となり、従業員の健康記録は HIPAA 規制の対象となる。そのため、当該情報または関連情報の保管または収集を行っている ISAO は、該当する規則における義務を理解することが重要である。

ISAO は要保護情報を特定して保護するための手順を策定する際に、さまざまな規制のフレームワークに詳しい法律、プライバシー、およびデータセキュリティの専門家に必要に応じて相談して、連邦、州、地方、および国際の各レベルにおいて既存のプライバシー規制および法的規制のすべてに確実に準拠する必要がある。

9.1 基本原則

セキュリティポリシーと同様に、プライバシーポリシーの確立は ISAO 設立の最も初期の段階で行うと最も有効である。収集および共有される情報の内容および場所によっては、適用される各種法律を満たすプライバシーポリシーの策定は複雑になることがある。適切な弁護士への相談が必要な場合がある。このようなポリシーを策定するにあたって、ISAO とそのメンバーは以下の原則を考慮する必要がある:

- ISAO メンバーは、ISAO や他のメンバーと共有される PII を最小限に抑えるように努めることに加え、脅威の特定に不可欠な検知指標を特定して提供することが推奨される。また、連邦、州、地方、および国際の各レベルにおいて既存のプライバシー規制および法的規制のすべてに確実に準拠することが推奨される。
- サイバー脅威検知指標に直接関係しない PII をメンバーが誤って ISAO に送信した場合、メンバーは ISAO に通知するための適切なプロセスを知っている必要がある。
- ISAO は、ISAO メンバーからの通知を受けた際に PII や他の種類の要保護情報を削除および修復するための手順の整備を検討する必要がある。これには、特定の個人に関する個人情報または特定の個人を識別する情報を含むサイバー脅威検知指標を適時に破棄または返却するための、合理的かつ適切な時間枠を提供するポリシーと手順の策定が含まれる場合がある。
- ISAO には、メンバーに共有対象パートナーについての透明性を提供するポリシーと、ポリシーまたは手法への重大な変更の通知について検討することが奨励される。また ISAO は(必要な法的アドバイスを得た後で)、法的責任について保護を受けるために CISA の適用範囲内で活動しようとしているかどうか、およびそうするための方法について、その選択肢によるプライバシーや他の事項への潜在的なリスクと影

響も含めて、メンバーに公表することを真剣に検討する必要がある。

9.2 補助原則

DHS は、業界と政府との間で共有を行う際のプライバシー問題に関するガイダンスを公開している。このガイダンスでは、共有が業界内に限られており、かつその共有に政府が関与しない場合にも、プライバシーと共有に関する CISA の有限の法的責任についての保護の適用が認められている。このガイダンスでは、米国の法律に基づく有限の法的責任についての保護を受けるために使用しなければならないプロセスが示されている。ISAO とその参加者およびメンバー組織は、適用されるプライバシー法とポリシーをよく理解し、適切な義務およびポリシーの規定をメンバー規則、基本文書、およびユーザー契約に組み込むことが重要である。

ISAO は、適用される州のプライバシー法およびその他のプライバシー法に確実に準拠し、関連する問題が生じた場合に対処するための責任と権限を有する特定のスタッフメンバー、役員、または外部の第三者（請負人または弁護士など）を指名することを検討できる。

保護必要度の高い個人情報の特別な取り扱いを必要とする可能性のある、特定のデータフィールドを識別するプロセスをセグメンテーションという。これは、ISAO がサイバー脅威検知指標を作成する際に役立つ可能性がある。セグメンテーションには、何らかのレビューを必要とする特定のデータフィールドを常に識別する、またはサンプリング（フィールド別、項目別、組み合わせなど）によって識別するプロセス、PII を返却、削除、または最小化する手順、および必要な配慮が不足した状態で PII を頻繁に取り扱うメンバー存在する場合、そのメンバーに対する勧告や助言の方法が含まれる可能性がある。共有する情報が常には ISAO によるプライバシー レビューの対象とならない場合は、法的専門家と相談して、責任への影響や法的責任についての保護の可能性を明確にする。

DHS と自動検知指標を共有する場合、ISAO は、DHS の自動情報共有（AIS）の利用規約[21]を含むさまざまな慣例や契約への準拠が求められる可能性がある。

[21]参照：https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf

いくつかの重要な DHS の要件が以下の利用規約に記載されている:

- 第 3.2 条「AIS 提供者は、共有される検知指標または防衛手段が提供の時点で正確であるように合理的な努力をしなければならない。さらに AIS 提供者は、NCCIC (National Cybersecurity and Communications Integration Center) で定義されているように、作成する検知指標または防衛手段を適切な情報処理レベルに関連付ける。」
- 第 3.3 条「各 AIS 提供者は、NCCIC に提供された検知指標または防衛手段から、サイバーセキュリティ脅威に直接関係しない情報 (AIS 提供者が、特定の個人を識別する個人情報であることを共有時に把握している情報) を削除するために合理的な努力をする。」
- 第 3.4 条「各 AIS 提供者は、検知指標または防衛手段を、手違いによって、誤って、または適切な情報処理レベルを使用しないで (誤ったマーク付け、またはマーク漏れに起因) 開示した場合、速やかに NCCIC に通知し、バージョニング更新の通知など、緩和のための合理的なすべての措置を準備ができ次第実施することに同意する。」

国際的なパートナーとの協力、または国境を越えた情報共有を行う場合は、ISAO とそのメンバーは、国際的なプライバシー法が米国の連邦、州法、または地方の法律とは異なる可能性があることを認識している必要がある。例えば、ISAO に欧州連合 (EU) の構成メンバーが含まれている場合、メンバーシップおよび状況によっては、ISAO は、米国・EU 間の合意 (プライバシーシールド[22]、EU 一般データ保護規則 (GDPR)[23]、およびネットワーク情報セキュリティ指令 (NIS)[24]など) への準拠が必要な情報を理解するよう努めなければならない (その情報を共有する場合)。

ISAO が米国国土安全保障省の NCCIC または他の政府機関との脅威検知指標または防衛手段の共有を決定した場合、特にその共有において CISA の下で受けられる明示的な法的保護を確保しようとする場合は、CISA の要件、および関連するプライバシー ガイダンスを (必要に応じて弁護士の支援を受けて) よく理解することが重要である。

ISAO は、CISA の下で受けられる法的責任についての保護のすべての適用範囲を対象にすることを選択した場合、CISA に準拠した適切なプロセスと手順を実施する必要がある。このガイダンスは、NCCIC を通じて連邦政府と共有しているのか、民間セクターのみで共有しているのかにかかわらず、プライバシーを保護すること、および CISA の下で受けられる共有に関する法的保護を確保するための道筋を示すことを目的としている。CISA に準拠するには、共有組織は、共有時に、サイバーセキュリティ脅威に直接関連しない PII を削除する必要がある。

[22]参照:https://www.commerce.gov/page/eu-us-privacy-shield
[23]参照:http://www.eugdpr.org/
[24]参照:https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

DHS の資料「*Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*」[25]では、脅威検知指標の一部となる可能性があり、かつ共有される可能性のある、特定の個人識別情報の例が示されている。その中には、特定の状況における固有の IP アドレスが含まれている。また、共有すべきではない個人情報やその他の情報の例、および共有情報の許可されない使用の例が含まれている。

以下に、ISAO がその機能を果たすために開発したプロセスおよび手順において検討および対処できる行動の追加の例を示す:

- ISAO が受信すべきでない PII を受信した場合に ISAO のマネージャーが何をすべきかを把握して適切に対応するように、プロセス、手順、計画、および演習を調整する。
- 米国国立標準技術研究所(NIST)の「Framework for Improving Critical Infrastructure Cybersecurity」(The Cybersecurity Framework とも呼ばれる)[26]のプライバシーのセクションなどの、プライバシーの検討事項に関するさまざまなガイダンスをレビューして、関連性があり、運用時の使用が望ましい推奨行動を特定する。
- 紛失、盗難、不正アクセス、不正取得、開示、コピー、使用、または改ざんから保護するために、組織内の PII ライフサイクルの全段階で必要とされ、PII の保護必要度に比例する予防手段を明確にする。
- 不要になった PII をセキュアに廃棄、非特定化、または匿名化するためのプロセスと手順を明確にする。
- PII を含むデータベースへのアクセスを監査するプロセスを明確にする。独立した監査機能の一環として PII を記録して、サイバーセキュリティ活動を効果的に実施するとともに、そのような PII を最小限に抑える方法を特定する。
- AIS ポータルの DHS プロファイルを、プライバシー要件を含めて評価する。
- 共有する情報を、ISAO が対象とする脅威に対処するために必要なデータのみに最小化するために、最小限の情報交換プロセスが必要かどうかを判断する。
- データ保護のための予防計画(システムと人間の両方の要素が含まれたもの)を策定し、同時に、違反があった場合の明確な修復計画も策定する。
- 従業員、顧客、および取引相手のニーズと期待に応える暗号化ポリシーを策定する。
- 中核となるメンバーと対象者を決定し、メンバーシップに応じた成熟度レベルに一致するセキュリティ要件とプライバシー要件を組み込む。その際、情報を受け取る機関

[25]参照:https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
[26]参照:https://www.nist.gov/cyberframework

または参加者のすべてに同等の能力または同等のプライバシーの検討事項があるわけではないことを考慮に入れる。

- メンバーの能力および共有される情報の重要度に適合するプライバシー制御とセキュリティ制御を導入する。例えば、明確に特定された受信者への電子メールや電話による脅威情報の共有は、広範囲のメンバーへのポータルを介した情報の配布よりも影響が少ない可能性がある。そのため、セキュリティ要件とプライバシー要件は、ISAO が実装しているツールに応じて異なる。
- データの保持と処分に関する明確なポリシーと手順を確立する。

10 情報セキュリティ

各 ISAO の規模、成熟度、機能はさまざまであり、共有する情報の量と種類もそれぞれ異なる。しかし、すべての ISAO は、その成熟度にかかわらず、共通するセキュリティ上の課題に直面している。ISAO は、これらのセキュリティ上の課題を検討し、ISAO のビジネスプロセスの始めにセキュリティの検討事項を適切なガバナンス、リスク、セキュリティのポリシーに含める必要がある。これにより、成功が促進される。これは、ISAO とそのメンバーが、メンバー間、およびメンバーと ISAO 間の信用をより効果的に築けるようになるためである。設立済みの ISAO もこのガイダンスを使用して自身のセキュリティを評価することができる。全体的な ISAO のガバナンスの一環としてセキュリティに対処することで、ISAO メンバーと見込みメンバーは情報共有活動への参加について適切なリスク判断を行うことができる。

ISAO のセキュリティポリシーは、共有されている各種情報、その情報の保護レベルの差異、およびその情報のメンバー間での共有手法が反映され、それぞれ異なる可能性がある。例えば、自動検知指標の共有に関するセキュリティポリシーは、PDF 文書の共有に関するセキュリティポリシーとは異なる可能性がある。同様に、オープンソースのニュースを保管するポリシーは、要保護のメンバー投稿あるいは機密または非公開のメンバー投稿を保管するポリシーとは異なる可能性がある。

ISAO のメンバーは、必要とされるセキュリティのレベルを引き上げる可能性もある。個々のメンバーが堅牢なセキュリティ機能を有する ISAO は、メンバーが有する機能が比較的高度ではない ISAO よりも、単一の ISAO としてより堅牢なセキュリティ手順を有する可能性が高い。ISAO および／またはメンバーの一般的な機能の差異は、情報共有エコシステムにおける異なる法的規制、リスク許容度、業界慣行、または成熟度によって拡大する可能性がある。組織が営利目的であるか非営利目的であるか、大きいか小さいかにかかわらず、セキュリティは ISAO の成功の重要な要素である。

米国司法省（DOJ）と DHS が発行している CISA 指定ガイダンスは、民間企業が連邦政府とサイバーセキュリティ情報を共有する際に従う手順を概説している。このガイダンスには、企業が DHS との情報共有プロセスに参加するために満たす必要がある基本構造とセキュリティ要件も含まれている。CISA はまた、強力なプライバシー保護を規定している。これについては付録で詳しく説明されている。さまざまな理由によりすべての ISAO がこの DHS プログラムに参加するわけではないが、DHS ガイドラインは、プログラムへの参加を選択する ISAO にとって重要な参考資料になる可能性がある。参加しないことを選択した ISAO でも、独自の情報共有のポリシーと手順を策定して実施する際に、CISA および AIS プログラムのセキュリティ要件を理解することで、少なくとも比較対象として役立てることができる可能性がある。DHS と DOJ は、民間セクター向けの CISA 実施ガイダンスを発行している。

10.1 ISAO のための基本的なセキュリティ要素

ISAO を設立する際、および設立後定期的に、ISAO のメンバーは、ISAO で期待される基本機能の実行に必要な最低限のセキュリティレベルについて検討および議論する必要がある。

10.1.1 セキュアなコミュニケーション

ISAO とそのメンバーは、ISAO の設立時、および設立後定期的に、通信の安全を確保するための適切な要件（暗号化の適切な使用など）について検討して決定する必要がある。内部要件を確立したら、ISAO はその要件を満たすための適切な手段を採用することができる。

ISAO の設立時に、メンバーは個々のメンバーのセキュリティのレベルと機能を把握する必要がある。これにより、すべてのメンバーにとって効果的かつ適切な方法でセキュリティポリシーが策定されるようになる。ISAO が形成および設立されたら、ISAO は定期的なレビューを行って、その機能とポリシーをメンバーの常に変化する機能と要件に合わせて適切に調整する必要がある。

ISAO は、他のさまざまな情報共有プログラムへの参加（または予想される参加）について評価し、そのようなプログラムのセキュリティ要件を検討することができる。DHS が提供する情報共有プログラムでは、共有情報をどのように保管および処理する必要があるかに関するセキュリティ要件が定義されている。例えば、DHS の Cyber Information Sharing and Collaboration Program（CISCP）[27]には、組織が CISCP 情報をどのように保管する必要があるかに関する具体的な参加要件がある。ISAO がそのようなプログラムに参加しようとする場合、ISAO はこれらの要件を満たすセキュリティポリシーを確立しなければならない。

[27]参照：https://www.dhs.gov/ciscp

10.1.2 公開鍵基盤（PKI）と「セキュリティ バイ デザイン」

ISAO は、情報共有のプラットフォームを構築または購入する前に、メンバー間の情報共有の促進に必要な基本セキュリティ要件を確立する必要がある。セキュリティ要件を前もってシステムに組み込むことは、後で追加するよりもはるかに簡単で安価である。ISAO に参加する団体は、ISAO 自体がセキュアであるという基本的な期待も抱いている。

これには、暗号化が必要かどうか、必要であればどのレベルの暗号化が適切であるかを検討することが含まれる。

例えば、各ポリシーには、すべてのメンバーが PKI 交換の仕組みによる電子メールの署名と認証に証明書を使用するかどうか、ISAO が複数要素認証を採用するかどうか、および共有される文書が PKI プロセスとは別に暗号化されるかどうかについて詳しく記載できる。

10.1.3 アクセス制御

セキュリティの重要な要素の 1 つはアクセス制御である。これは、必ずしも組織内の全員がすべての文書にアクセスする必要はないという事実に基づいている。したがって、アクセスが許可されている文書にのみアクセスできるように、適切な制御を実施する必要がある。また、ISAO とそのメンバーが、メンバー内の ISAO スタッフおよび個人に対する適切なアクセス制御について議論して決定することが適当である。

アクセス制御のもう 1 つの要素は、組織内での役割が変わった者や、組織を完全に離れる者の資格を取り消す機能である。したがって、ISAO とそのメンバーは、メンバーまたは従業員が情報へのアクセスを許可されなくなった際に、個人の資格を確実に取り消すための方法に関する共通ポリシーに合意することが適当である。

もう 1 つの一般的なセキュリティ原則として、データは重要度に基づいて統合する必要があるという原則がある。したがって、データの種類によってアクセス制御が異なる可能性がある。例えば、マーケティング部門の責任者が組織のオープンソースのニュース レポートのコレクションにアクセスできるようにすることは適切である一方で、その責任者がメンバーやパートナーが共有する保護必要度の高い検知指標にアクセスする必要はない可能性がある。

10.1.4 サイバーセキュリティ攻撃と情報漏洩の通知

ISAO は、メンバー間の信用と信頼のレベルを維持するために、ISAO とそのメンバーに影響を及ぼすサイバーセキュリティ攻撃の被害者となった場合の内部の報告計画およびメンバーとの通信手段を確立しておく必要がある。ISAO は、州および地域の情報漏洩通知法の対象でもあり、ISAO の従業員、請負業者、メンバー、またはパートナーのために保持する PII、知的財産またはその他の要保護データに影響を及ぼすサイバー攻撃の被害者となる可能性もある点に注意する必要がある。ISAO は本質的に地域に限定したものである場合もあれば、さまざまな州のメンバーが ISAO に含まれる場合もある。そのため、ISAO はさまざまな州の情報漏洩に関する法律を認識している必要

がある。また、ISAO のメンバーは、攻撃および攻撃に伴う漏洩が特定の州法の通知レベルまで達しない場合でも、法律で要求されるよりもさらに踏み込んだ独自のベースライン要件を ISAO 内の信用要素の一部として確立することができる。最後に、いくつかのセクターには、ISAO が精通する必要がある、特定の種類の通知に対する連邦政府のさまざまな要件がある。その内のいくつかの要件はサードパーティ ベンダーにも及ぶ。

10.1.5 データの分類、配布、およびラベル付け

もう 1 つの一般的なセキュリティ原則として、情報への適切なマーク付けおよびラベル付けの必要性がある。これには、特定の文書に対する具体的な取り扱い指示の記録や、一般的な分類を用いたマーク付けが含まれる。このようなマーク付けは、情報がどのように使用され、保管されるかを ISAO メンバーが理解するのに役立つ。ISAO とそのメンバーは、それぞれのセキュリティポリシーに適合する分類方式を開発することができる。また、一般的な手法として、文書を所有する団体がその情報の共有方法を制御できるようにするという手法がある。この概念は、一般に「発信者制御」として知られている。セキュリティポリシーで検討すべき潜在的な要素の例を以下に示す:

- Traffic Light Protocol (TLP)などの分類基準の使用。これは、メンバーがデータ分類基準に従って情報を共有する方法を理解するのに役立つ。
- メンバーによる共有検知指標の使用方法について詳しく記載したポリシー。例えば、メンバーはこれらの検知指標を使用して顧客を保護できるか、特定のネットワークのみを保護できるかなど。
- メンバーが非セキュリティ機密情報を共有するリスクを制限する内部構造およびポリシー。
- さまざまなレベルの要保護情報を受信または保管するメンバーの権限を反映する複数の共有グループまたはフォーラムを ISAO が設立する必要があるかどうかの判断。
- メンバーの提出データの匿名化に関する課題、および匿名化する場合の共有に関する要素の策定に関する課題。
- データの保持と処分の明確なポリシーと手順。
- 自動取得および自動配布、電子メール、およびその他の方法などの情報共有のオプション。
- メンバーによる口頭での提出に関するポリシー。

例として、電子メールを介したデータ共有のルールを設定するための配布ポリシーを検討すると参考になる。各ポリシーでは以下のような事項を扱うことができる:

- いつブラインドコピーメール機能を使用するか
- どの情報を暗号化メールで送信するか
- 誰がメーリングリストにアクセスでき、誰をメーリングリストに登録できるかの基準
- いつ「全員に返信」機能を使用するか

10.2 ISAO メンバーのセキュリティ

ISAO 自身のセキュリティと個々のメンバーのセキュリティはいずれも非常に重要である。ISAO を介しておよび ISAO 内で共有される情報を、他のメンバーがどのように処理し保管するかをメンバーが把握している場合に信用が高まる。したがって、ISAO とそのメンバーは、メンバー組織のセキュリティ上の責任に関するポリシーを策定することを検討する必要がある。潜在的な検討事項には以下が含まれる:

- 共通のメンバー契約書または他のすべてのメンバーに共通する文書に、ISAO を介して共有される情報を保護する上での各メンバーの責任について詳しく記載する。
- 情報共有に使用されるツールと、メンバーにこれらのツールへのアクセスを許可するポリシーについて詳しく記載する。
- ISAO のセキュリティポリシーにおけるメンバーの責任についてメンバーに伝達および／または指導するための手法を確立する。

これらの ISAO セキュリティポリシーは、ISAO メンバー企業の企業全体でのサイバーセキュリティ手法に置き換わるものではない点に注意することが重要である。また、ISAO メンバー企業が従う必要のある法的規制や義務に置き換わるものでもない。ISAO のメンバーは、各自の企業を保護するために適切なあらゆる措置を取る必要がある。ISAO のメンバーがサイバーリスクを管理するのに役立つガイドは、NIST のサイバーセキュリティ フレームワークをはじめ、数多く存在する。ISAO セキュリティポリシーのポイントは、ISAO から受信する情報、または ISAO と共有する情報のセキュリティの確保に固有のメンバーの責任について詳しく記載することである。

10.3 グローバルなセキュリティの課題

ISAO にグローバルな企業や団体が含まれている場合、ISAO は、情報セキュリティ、サイバーセキュリティ、プライバシー、およびサイバー情報共有全体に関する他のメンバー要件を認識して議論することが重要である。

- 情報共有で国境を越えるデータ転送がある場合、ISAO は、統制上の国際的な要件についてよく理解する必要がある。例えば米国と EU は、欧州市民に関するデータの収集、使用、および転送の方法についての指令を含むプライバシーシールドな

らびに関連する情報セキュリティとプライバシーの要件に合意している。[28]注意すべき他の重要な EU の要件としては、EU GDPR と EU ネットワーク情報セキュリティ指令がある。[29]米国は、G7 諸国と G20 諸国との間で、サイバーセキュリティと情報共有のさまざまな側面について協定を締結している。また、個人データを使用する前に個人から同意を得ることに関する要件は各国で異なる。これは、ISAO とそのメンバーが事前に十分に認識しておく必要がある情報共有にも関連する。

- ISAO は必要に応じて、世界各国の法的規制を認識し、統合する必要がある。場合によっては、これらの要件はベンダーや第三者にも及ぶため、ISAO はそのような要件に注意を払い、準拠する必要がある。

[28]参照：https://www.privacyshield.gov/welcome
[29]参照：http://ec.europa.eu/justice/data-protection/reform/index_en.htm
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

付録 A 補足資料

この付録では、ISAO にとって有用な情報が記載された資料のリストを示す。

サイバーセキュリティ情報共有法（CISA）

https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

民間セクター向けの CISA 実施ガイダンス

https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

Cyber Information Sharing and Collaboration Program (CISCP)

CISCP は、US-DHS National Cybersecurity Communications Integration Center が管理するプログラムであり、公的機関と私的機関との間の主要な情報共有プログラムである。

https://www.dhs.gov/ciscp

米国国土安全保障省、United States Computer Emergency Readiness Team（US-CERT）の自動検知指標共有（AIS）

https://www.us-cert.gov/ais

https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf .

米国国土安全保障省および司法省

2016 年 6 月 15 日付けの「Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015」。14 ページ目と『Annex 1: Sharing of Cyber Threat Indicator and Defensive Measure Sharing between Non-Governmental Entities under CISA』を含む。

https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

欧州一般データ保護規則（GDPR）

これらは、個人のデータ保護を強化するための欧州連合諸国の一連の規制である。

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

EU ネットワークおよび情報セキュリティ（NIS）指令

NIS 指令は、EU 各国のサイバーセキュリティ機能の強化および向上を目

的とした欧州全体の法令である。

https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

公開鍵基盤（PKI）

PKI は、2 者間のセキュアな通信を確立するために使用されるすべてのポリシー、手順、および技術で構成される。公開鍵暗号（非対称鍵暗号とも呼ばれる）は、鍵ペアを使用して暗号化と復号化を行う。これらの鍵は、1 つの公開鍵と 1 つの秘密鍵で構成されており、両方の鍵が数学的に関連付けられている。

https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

http://searchsecurity.techtarget.com/definition/PKI

https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm

PCI Security Standards Council, LLC（2016）の「Requirements and Security Assessment Procedures Version 3.2」（マサチューセッツ州ウェイクフィールド）

ペイメントカード業界データセキュリティ基準（PCI DSS）の要件およびセキュリティ基準。

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1470830604318

米国国立標準技術研究所（NIST）の「Framework for Improving Critical Infrastructure Cybersecurity」

NIST のサイバーセキュリティ フレームワークは、サイバーセキュリティを強化し、重要なインフラへのリスクを軽減するための一連の任意基準である。

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

米国下院（2014）による「連邦情報セキュリティ近代化法」（ワシントン D.C.）

連邦情報セキュリティ近代化法は、2002 年の電子政府法のタイトル III、すなわち 2002 年の連邦情報セキュリティマネジメント法（FISMA）で開始されたフレームワークを更新および拡張するものである。

https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

米国下院（1999）による「グラムリーチブライリー法」（ワシントン D.C.）

グラムリーチブライリー法（GLBA）は 1999 年の金融近代化法であり、金融機関が個人識別情報（PII）およびその他の要保護データを取り扱う方法につ

いての制御を設けている。

https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf

米国下院（1996）による「医療保険の携行性と責任に関する法律」（ワシントン D.C.）

医療保険の携行性と責任に関する法律（HIPAA）は、個人のあらゆる形態の医療情報に対して、アクセスできる者を制限し、保護を提供する。

https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

米国下院（2009）による「経済的および臨床的健全性のための医療情報技術に関する法律」（ワシントン D.C.）

2009 年の経済的および臨床的健全性のための医療情報技術に関する法律（HITECH）は、2009 年の米国再生・再投資法（ARRA）の一環として制定された。この法律の目的は、医療情報技術の実装と「有意義な利用」の奨励である。

https://www.congress.gov/111/plaws/publ5/PLAW-111publ5.pdf

http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

米国下院（2002）による「サーベンス・オクスリー法」（ワシントン D.C.）

2002 年のサーベンス・オクスリー法（SOX）は、企業および監査の責任・透明性に関する法律である。

https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf

US-CERT の Traffic Light Protocol

Traffic Light Protocol は、要保護情報を指定して、その情報が正しく配布されるようにするために US-CERT によって開発された。

https://www.us-cert.gov/tlp

付録 B 用語集

本書で使用する一部の用語の定義を以下に記載する。

アラート（Alert）：現在のセキュリティの問題、脆弱性、エクスプロイトについての適時情報。

分析（Analysis）：悪意のある活動を特定するためにデータの詳細な調査を行うこと。また、手元にあるデータについてより有益な情報を提示するために、特定された悪意のある活動を既存の脅威情報に照らし合わせて評価すること。

サイバーセキュリティ情報の自動共有（Automated Cybersecurity Information Sharing）：主にマシンでプログラムされた受信、分析、配布、統合の手法を利用して、情報システムのセキュリティの向上に関わるデータ関連のリスクや手法を交換すること。

キャンペーン（Campaigns）：サイバーセキュリティにおいて、企業によるサイバー空間上の情報を標的とした一連の活動や攻撃のこと。その目的は、コンピュータ環境またはコンピュータインフラの混乱、無効化、破壊、悪意のある制御、データの完全性の破壊、または制御された情報の窃取などである。

コンピュータセキュリティインシデント（Computer Security Incident）：「インシデント」を参照。

コンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team (CSIRT)）：コンピュータセキュリティに関連するインシデントへの対応を支援する目的で設立された機能。Computer Incident Response Team（CIRT）または CIRC（Computer Incident Response Center、Computer Incident Response Capability）とも呼ばれる。

サイバー脅威情報（Cyber Threat Information）：情報システムや運用システムに対する攻撃者、攻撃者の意図、または行為に関する情報（例えば、兆候、戦術、技術、手順、行動、動機、攻撃者、標的、脆弱性、行為の過程、または警告など）。

サイバーセキュリティ情報（Cybersecurity Information）：情報システムのセキュリティ向上に関するデータ関連のリスクや手法。

サイバーセキュリティ情報共有（Cybersecurity Information Sharing）：情報システムのセキュリティ向上に関する、データ関連のリスクや手法の情報交換。

サイバーセキュリティ脅威（Cybersecurity Threat）：情報システムに対する行為または情報システムを介した行為のうち、情報システム、または情報システムが扱う情報（保存されている情報、処理される情報、通信される情報）のセキュリティ、可用性、機密性、完全性に悪影響を与える不正行為を招く可能性のあるもの。消費者利用規約や消費者ライセンス契約の違反にのみ関連する行為はこの用語に含まれない。

サイバー脅威指標（Cyber Threat Indicator）：以下を説明または識別するのに必要な情報。

- 悪意のある偵察行為（サイバーセキュリティ脅威やセキュリティ脆弱性に関連する技術情報の収集を目的として送信されたと考えられる異常な通信パターンなど）
- セキュリティコントロールを破る、またはセキュリティ脆弱性をエクスプロイトする手法
- セキュリティ脆弱性（セキュリティ脆弱性の存在を示すような異常な動作など）
- 情報システム、または情報システムが扱う情報（保存されている情報、処理される情報、通信される情報）への正当なアクセス権限を持つユーザーが、意図せずにセキュリティコントロールを無効化する、またはセキュリティ脆弱性のエクスプロイトを可能にするような手法
- 悪意のあるサイバー コマンド & コントロール
- あるインシデントによって引き起こされた実際のまたは潜在的な損害（特定のサイバーセキュリティ脅威による結果として盗み出された情報の記述など）
- 上記の組み合わせ

防衛手段（Defensive Measure）：既知のまたは疑わしいサイバーセキュリティ脅威やセキュリティ脆弱性を検出、防止、または緩和する行為、デバイス、手順、シグネチャ、技術、またはその他の手段。情報システム、または情報システムが扱う情報（保存されている情報、処理される情報、通信される情報）に適用される。

インシデント（Incident）：コンピュータのセキュリティポリシー、利用規定・規約、または標準的なセキュリティ手法への侵害または差し迫った侵害の脅威。

インシデントハンドリング（Incident Handling）：セキュリティポリシーおよび推奨される手法への侵害の緩和。

インシデント対応（Incident Response）：セキュリティ侵害や攻撃（インシデントとも呼ばれる）による影響に対処し、管理するための組織化されたアプローチ。損害を抑え、復旧時間とコストを低減する方法で状況を処理することが目標。

検知指標／インディケータ（Indicator）：攻撃者が攻撃を準備していること、攻撃が現在進行中であること、または侵害が既に発生している可能性があることを示唆する成果物または観察可能な証拠。

マルウェア（Malware）：データを破壊するか、有害プログラムや侵入プログラムを実行するか、あるいは被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、可用性を侵害する意図で、別のプログラムやシステムにひそかに挿入されたプログラム。

悪意のあるサイバー コマンド & コントロール（Malicious Cyber Command and Control）：情報システム、または情報システムが扱う情報（保存されている情報、処理さ

れる情報、通信される情報）に対する、リモートでの不正な識別、アクセス、または使用のための手法。

悪意のある偵察行為（Malicious Reconnaissance）：セキュリティ脆弱性を特定する目的で情報システムを能動的に調査するか受動的に監視する手法のうち、既知のまたは疑わしいサイバーセキュリティ脅威に関連付けられているもの。

監視（Monitor）：情報システムが扱う情報（保存されている情報、処理される情報、通信される情報）を取得、識別、スキャン、または保有すること。

緩和（Mitigation）：セキュリティの脆弱性や露出による重大性、深刻さ、困難の度合いを軽減する行為。

運用分析（Operational Analysis）：脅威、脆弱性、インシデント、または手法のあらゆる組み合わせを調査すること（例えば、インシデント分析、特定の戦術、技術、手順、または脅威アクターの識別など）。その結果として、特定のデータ、インフラストラクチャ、または機能を保護する手法が得られる。

セキュアポータル（Secure Portal）：Web ベースの技術を使用して、関連する情報資産（情報コンテンツ、アプリケーション、およびビジネスプロセス）への制御された安全なアクセスを、その情報資産の利用者に対して個別に提供する Web 対応のリソース。

セキュリティコントロール（Security Control）：情報システムまたは情報システムの情報の機密性、完全性、可用性に悪影響を与える不正行為から保護するために使用される管理、運用、および技術の制御。

セキュリティ脆弱性（Security Vulnerability）：セキュリティコントロールを破ることを可能にするか、または容易にすることができるハードウェア、ソフトウェア、プロセス、または手順の特性。

要保護情報（Sensitive Information）：紛失、誤用、または不正アクセスや改ざんによって、国益や連邦制度の実施、または 5 U.S.C.セクション 552a（プライバシー法）によって規定されている個人のプライバシーに悪影響を及ぼす可能性があるが、大統領令または議会制定法によって制定された基準では、それらを国防または外交のために機密にすることを明確には認められていない情報。

シグネチャ（Signature）：ウイルスに含まれるバイナリ文字列や、システムへの不正アクセスを取得するために使用される特定のキー操作など、攻撃に関連付けられた認識可能な識別パターン。

状況認識（Situational Awareness）：収集された情報、観測、分析、および知識や経験に基づいた、現在のおよび進行中のセキュリティ状態とリスクに関する情報の把握。

脅威（Threat）：情報システムを介した情報への不正アクセス、情報の破壊、情報の開示、情報の改変、およびサービス妨害によって、組織運営（ミッション、役割、イメージ、評判を含む）、組織資産、個人、他の組織、または国家に悪影響を与える可能性がある

状況またはイベント。

脅威アクター（Threat Actor）：悪意のあるサイバー活動に関与する個人またはグループ。

脅威源（Threat Source）：脆弱性の意図的なエクスプロイトを目的とする意思や手法、または偶発的に脆弱性をエクスプロイトする可能性のある状況や手法。

傾向分析（Trend Analysis）：広範な行為、明らかでない行為、または新たな行為のあらゆる組み合わせを特定するためのデータの調査（例えば、脅威アクターのキャンペーンと意図、エクスプロイトされた一般的な脆弱性と構成、評価などの非類似データストリームとの操作分析のマージなど）。

脆弱性（Vulnerability）：脅威源によってエクスプロイトされる可能性のある、情報システム、システムセキュリティの実施手順、内部統制、または実装における弱点。

付録 C 略語

AIS	検知指標情報自動共有（Automated Indicator Sharing）
CERT	コンピュータ緊急対応チーム（Computer Emergency Response Team）
CISA	サイバーセキュリティ情報共有法案 （Cybersecurity Information Sharing Act）
CVE	共通脆弱性識別子（Common Vulnerabilities and Exposures）
CONOPS	運用概念（Concept of Operations）
DHS	米国国土安全保障省（Department of Homeland Security）
EU	欧州連合（European Union）
GDPR	一般データ保護規則（95/46/EC 指令） （General Data Protection Regulation (Directive 95/46/EC)）
HIPAA	医療保険の携行性と責任に関する法律 （Health Information Portability and Accountability Act）
HITECH	経済的および臨床的健全性のための医療情報技術に関する法律 （Health Information Technology for Economic and Clinical Health Act）
IP	インターネットプロトコル（Internet Protocol）
ISAC	情報共有分析センター（Information Sharing and Analysis Center）
ISAO	情報共有分析機関（Information Sharing and Analysis Organization）
IT	情報技術（Information Technology）
NCCIC	全米サイバーセキュリティ・通信統合センター （National Cybersecurity & Communications Integration Center）
NIS	ネットワーク情報セキュリティ指令（Network and Information Security Directive）
NIST	米国国立標準技術研究所 （National Institute of Standards and Technology）
PCI	ペイメントカード業界（Payment Card Industry）
PII	個人識別情報（Personable Identifiable Information）
SO	標準化機関（Standards Organization）
STIX	脅威情報構造化記述形式（Structured Threat Information eXpression）
TAXII	検知指標情報自動交換手順 （Trusted Automated eXchange of Indicator Information）
TLP	トラフィックライトプロトコル（Traffic Light Protocol）
TTP	戦術、技術、および手順（Tactics, Techniques & Procedures）