ISAO
Standards Organization

ISAO 100-2:
情報共有分析機関（ISAO）の設立のためのガイドライン

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 100-2

情報共有分析機関（ISAO）の設立のためのガイドライン

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 Cent
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)、Michael Arceneaux (Water-ISAC)、Jon Baker (The MITRE Corporation)、Adam Buteux (PWC)、Roger Callahan (FS-ISAC)、Timothy Casey (Intel Corporation)、Luke Dembosky (Debevoise & Plimpton LLP)、Tim Evans (Senior Advisor of John Hopkins University Applied Physics Laboratory)、Jeremy Feigelson (Debevoise & Plimpton LLP)、Betsi McGrath (The MITRE Corporation)、Benjamin R. Pedersen (Debevoise & Plimpton LLP)、David Pedraza (BCD Solutions | IT Staffing and Managed Services)、Meeta Sidhu (Price Waterhouse Coopers)、Rick Simon (Intel Security)、Bobbie Stempfley (The MITRE Corporation)、そして Joseph Viens (Charter Communications and COMMS ISAC)。

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。Brad Howard、Daniel Knight、James Navarro、Chris Rutherford、Larry Sjelin、そして Natalie Sjelin。

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

1 エグゼクティブ サマリー

本書の目的は、情報共有分析機関（ISAO）を設立するための一連のガイドラインを示すことである。最初に、戦略計画の主要要素をいくつか説明し、新しい ISAO が最も重大な課題を早い段階で検討できるようにする。その後、これらの戦略計画の要素に沿って、運用上の主要要素に関する一連の検討事項について説明する。最後に、「信用できるコミュニティーの構築」セクションで、信用を確立するための主要な考慮事項について説明する。メンバーが積極的にサイバーセキュリティ情報を共有し参加する適切な ISAO を設立するには、信用が不可欠である。本書はガイドラインと主要な考慮事項をまとめたものであるため、規範的な性質のものではなく、最も重要な考慮事項のガイドとなるものである。増加するメンバーのニーズを満たす ISAO の設立は、反復的なプロセスである。このため、これらのガイドラインは、ISAO の設立者が ISAO を設立し、メンバーの変化するニーズに合わせて ISAO を発展させる支援となることを目的としている。

2 はじめに

これらのガイドラインは、新しい ISAO が重大な課題を検討するための支援を目的としており、設立された ISAO の健全性や状態を定期的に評価するための有効なツールである。これらのガイドラインでは、設立されるさまざまな種類の ISAO と、それぞれの ISAO が持ちうる機能が考慮されている。本書は、他の ISAO SO の文書と併せて、新しい ISAO が即時に対応すべきニーズを考慮しながら、ISAO に関連する各種のトピックに対して体系的なアプローチを提示する。

本書には規範的な性質はない。そのため、本書は何かを行うための最善の方法や、具体的にすべきことを組織に示すものではなく、最も重要な考慮事項のガイドとなるものである。

本書では、戦略計画および運用計画において考慮すべき一連の要素と併せて、信用できるコミュニティーを構築するための考慮事項に関するより詳細な解説を提供する。全体としては、ISAO の設立にのみ該当することに焦点を当てるものである。

3 戦略計画の主要要素

ISAO を設立するには、ステークホルダーのコミュニティーと協力して、構成員とメンバーシップ パートナーのサイバーセキュリティを向上させるための ISAO の価値提案、目的、および機能を定義する必要がある。これらの要素は、ステークホルダーの初期の代表集団が各要素を検討できることを前提としている。

ある領域での決定が他の領域での検討事項に影響を及ぼすため、これらの戦略計画の要素を繰り返し検討することが推奨される。戦略計画の各主要要素の決定は、本書で後に紹介する運用計画の要素を導き出し、それらに影響を与える。

さらに ISAO は、メンバーの変化するニーズに対応するために、時間の経過と共に発展する可能性がある。したがって、ステークホルダーはこれらの戦略計画の主要要素を定期的に見直して、ISAO のミッションやビジョンとの整合性を確保する必要がある。

3.1 ISAO の本質の定義

ISAO の本質を定義することは、新しい ISAO の設立にあたって重要な最初のステップである。新しい ISAO は、その設立と同時に自らのミッションとビジョンを明らかにする必要がある。新しい ISAO が以下の戦略計画と運用計画の各主要要素に取り組むにあたり、ミッションとビジョンを明確にすることで土台が築かれる。

新しい ISAO がその本質を定める際は、以下の指標となる質問について検討する:

- この ISAO メンバーが集まる経緯となった共通の目的は何か？
  ISAO のメンバーになる組織を結びつけて、情報共有コミュニティーを形成するものは何か？
- ISAO は、ISAO の情報共有パートナーとメンバーのサイバーセキュリティ状況をどのように改善するか？ISAO が解決する情報共有の課題は何か？
- ISAO が達成しようとする目標は何か？目標は、個人間で基本的な脅威インテリジェンス情報を共有することでローカルでの意識を高めることから、セクター全体にわたって技術的な脅威インテリジェンスを自動的かつ世界規模で高速リアルタイム共有することにまで及ぶ可能性がある。目標は、ISAO の規模とリソースが増えるにつれて、時間の経過とともに拡大する可能性がある。
- ISAO のビジョンは何か？ISAO のステークホルダーとメンバーは、設立から 1 年後の ISAO、5 年後の ISAO などについてどのような絵を描いているか？予定表の各マイルストーンで、ISAO は規模、地理的範囲、製品、サービス、および活動の面でどこに位置しているか？
- ISAO が計画している、他の ISAO とは異なる活動は何か？ISAO が情報共有を通してメンバーにもたらす独自の解決策は何か？

3.2 共有する情報の決定

次の検討要素は、共有する情報の種類と情報の共有方法の決定である。対象メンバーと潜在的なパートナーである ISAO の情報共有の要件を理解するための体系的なアプローチをとる必要がある。新しい ISAO は、自身が所有している情報の種類、メンバーやパートナーの ISAO から必要となる情報の種類、それらの組織が受信を希望する情報の種類を検討する必要がある。

新しい ISAO が、どのような情報をどのように共有するかを決定する際には、以下の指標となる質問を検討する:

- ISAO メンバーが必要とする情報は何か、ISAO のミッションとビジョンを支える情報は何か。その答えは、範囲の狭い自動データフィードから対面による戦略情報の共有まで多岐にわたる可能性があり、また、単一の種類の情報に限定されない可能性がある。
- ISAO メンバーは ISAO から受け取った情報をどのように使用するか？メンバーは、ISAO からの情報をサイバー脅威を緩和するためにセキュリティ運用で直接使用するか、リスク管理の意思決定を通知するために間接的に使用する可能性がある。
- ISAO は共有する情報をどのように取得するか？あるケースでは、ISAO のメンバーが情報源となり、ISAO がメンバーに再度共有する場合がある。別のケースでは、ISAO は、政府や業界のサイバーセキュリティ情報提供者など、他の情報源から受け取った情報を提供する場合がある。
- ISAO は、少なくとも最初はどのような方法で情報を共有することを計画しているか？例えば、非公式かつ口頭ベースで、オンラインポータルによって手動で、または情報共有プラットフォームを介して自動で行う方法がある。ISAO は、非公式な共有から開始して、脅威指標の迅速な共有を可能にする技術の存在を調査することで発展する可能性がある。
- ISAO メンバーは、ISAO が提供する種類の情報を利用するのに必要な機能を持っているか？
- ISAO は、共有される情報が実際に利用可能であることを確認し、そうでない場合にメンバーのニーズを満たすように情報を強化および拡張することを、どのように行うか？
- ISAO は共有する情報に対するフィードバックをどのように収集するか？フィードバックを収集することで、ISAO は情報共有を発展させ、情報がメンバーのニーズ、および ISAO のミッションとビジョンを確実にサポートするようにする。
- ISAO での情報共有は匿名で行われるか、または情報源の開示を必要とするか？情報源を開示した場合、共同作業や信用を実現しやすくし、情報の有用性が高まる可能性がある。ただし、情報源の開示によって一部のメンバーが ISAO との情報共有に不安を残す可能性がある。結局は、複合的なアプローチが必要になるかもしれない。
- ISAO が共有および受信する情報において、ISAO はどのような制約または機密レベルをサポートするか？Traffic Light Protocol (TLP)[1] などの、成熟した ISAO によって使用されている、確立された手法を確認する必要がある。ここでの決定事項は、インフラの選定から共有情報の有用性まですべてに影響を及ぼす可能性がある。利用条件を明確にすることで、ISAO の情報をより広範にわたって共有および活用

[1] 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。詳しくは、https://www.us-cert.gov/tlp を参照。

することが可能になる。同様に、機密扱いの情報を共有するかどうかを検討する。

サイバーセキュリティ情報共有の詳細な説明（情報の種類や、その情報の共有方法など）については、ISAO 300-1 の『*Introduction to Information Sharing（情報共有入門）*』を参照。

3.3 ISAO エコシステムでの役割の特定

ISAO とそのメンバーは、一般に各組織間および各 ISAO 間で情報が共有されるサイバーセキュリティ情報共有エコシステムに参加している。このエコシステム内では、相互利益のために提携する機会、分析機能を配布する機会、インシデント対応で共同作業する機会などがある。このエコシステムを念頭に置き、このエコシステムにおける潜在的な役割を慎重に検討することは、新しい ISAO にとって非常に有益である。

新しい ISAO がサイバーセキュリティ情報共有エコシステムでのその役割を特定する際には、以下の指標となる質問について検討する（前述のように ISAO が、特にエコシステムの発展とともに、このプロセスに立ち戻ることは有益である）：

- ISAO の対象コミュニティーは誰か？
- ISAO は 1 つの業界セクターまたはサブセクターに限定されるか？複数セクターを含むか？非営利団体、または地理的領域をサポートするか？ ISAO は、オリンピックなどの特定の 1 つのイベントに限定されるか、あるいはランサムウェアなどの特定の 1 つの脅威に焦点を合わせるか？
- ISAO は、対象コミュニティー全体で ISAO を支持するためにコミュニティーのリーダーを特定し、参加を促しているか？対象コミュニティーでは既に情報を共有しているか？
- ISAO の地理的焦点は何か？局地的、地方的、全州的、国家的、国際的かを検討する。国際的である場合は、法的な観点および／または「安全に共有を行える文化」の観点から、国際パートナーとの情報共有に対して課題があるかどうかを検討する。
- ISAO は 法の執行を含めてどの範囲まで各種政府機関と情報をやりとりするか？関連する検討事項については、ISAO 600-2 の『*U.S. Government Relations, Programs, and Services*』を参照。
- この新しい ISAO が、既存の ISAO や対象コミュニティーにサービスを提供している他の組織（例：サイバー脅威フィード プロバイダー）と類似する点、異なる点は何か？[2]

3.4 パートナーおよび協力

新しい ISAO は、他の組織（他の ISAO など）との提携および協力を慎重に検討する必要がある。

[2] 既存の情報共有機関については、https://www.isao.org/information-sharing-groups/ を参照。

候補となる提携先および協力者を評価する際は、以下の指標となる質問について検討する:

- ISAO は、重要インフラ、業界、事業、または政府の保護を強化するために、何を共有パートナーのコミュニティーに提供する必要があるか。
- ISAO は、戦略的な情報共有パートナーを定義しているか？戦略的パートナー提携による相互利益の目的が定義されているか？
- 類似する ISAO は現在何を提供しているか？また、どのように調整、協力、共同作業ができるか？
- 他に提携できる ISAO はあるか？早期の決定フェーズおよび運用への移行を支援するメンターおよびサポートとして、他の ISAO を検討する。進行中の協力について、他の ISAO を検討する。
- ISAO は、受信した情報の価値を高めるために他のパートナーと協力するか？ ISAO は他の ISAO とオープンに情報を共有するか？
- 内部および外部との協力は、ISAO の本来のワークフローか？

3.5 サービスおよび機能の定義

このセクションでは、ISAO がメンバーのニーズを満たすための一連のサービスと機能を設計・実装する際に検討するためのガイドラインを示す。

「付録 A サービスおよび機能の表」では、ISAO が検討できるサービスと機能の事例を提供する。また、各サービスまたは機能の記述情報、各項目の利点と課題点、実装に対する広範な推奨事項を提供する。ISAO は、本書に記載されている例の枠を超えて、リソース環境内でのメンバーの価値の提供に最適な革新的なアプローチを採用することが推奨される。革新的なサービスは、情報共有エコシステム全体の機能向上の促進に役立つという付加的な利益をもたらす。

付録 A に記載されているサービスと機能の説明リストを確認することで、ISAO は以下のような運用計画における重要な質問に先んじて回答できる可能性がある:

- ISAO がメンバーに価値をもたらすために提供する基本サービスは何か？例えば、サイバー脅威や防衛手段を共有するためのハブとして機能すること、データを分析して「利用可能な」インテリジェンスに変えること、もしくはその両方など。
- 情報共有サービスの中核を超えて、ISAO がメンバーにさらなる価値をもたらすために提供する追加サービスは何か？

- ISAO が、ISAO、メンバー、およびミッションの特有な面に対応して提供する独自サービスは何か？ISAO は、どのように自身を他の組織と戦略的に差別化して、メンバーにとって実際に特有な価値を提供するか？
- ISAO の将来のサービス提供計画は何か、またそれらの提供に役立つ機能は何か？
- ISAO は、メンバーに共有される情報に適用する分析機能を取得すること、および ISAO 外部に分析論を共有することを計画しているか？
- ISAO には、サイバーセキュリティおよび情報共有の特別な専門知識があるか？
- ISAO は、提供する基本サービス、追加サービス、独自サービスと、それらをサポートする機能を探す際に、どのようにコミュニティー全体にわたって他の ISAO から学習し、他の ISAO と新しいものを共有することができるか？

3.6 メンバーシップ基準の定義および対象メンバーの特定

明確なメンバーシップ基準一式を確立することは、ISAO にとって非常に役立つ。メンバーシップ基準は各 ISAO 間で異なっている。新しい ISAO にとって、他のより成熟した ISAO が実施しているアプローチを理解することは有益である。

メンバーシップ基準を定義する際は、以下の指標となる質問について検討する:

- メンバーシップの基本要件は何か？また、それらの要件をどのように監視および順守するか？要件は、運用機能、メンバーが ISAO とやり取りする方法、メンバーが共有する情報の量と種類、または業界標準の順守（例：NIST SP 800-53 Rev. 4『連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策』[3]、ISO/IEC 27001『情報セキュリティマネジメントシステム要求事項』[4]）などに集中する可能性がある。
- 参加要件や従事要件はあるか？一部の ISAO では、情報共有を確実にし、投資対効果を向上させるために、能動的な参加が要求される。別の ISAO では、より受動的な参加が許される。
- メンバーシップの対象は組織か、個人か、あるいはその両方か？組織である場合、組織的な参加に制限はあるか？個人と組織の場合に、組織と個人とで異なる要件が存在するか？
- ISAO は、メンバーやステークホルダーによる参加や協力をどのように確認し、手配し、促すか？サポートメンバーの参加は、ISAO 内での活発な情報共有のために重要である。多くの場合、共有の活発さはメンバーの組織の上級幹部によるサポートや奨励に比例する。幹部層からの明確な「進め」の合図がないと、情報を共有するかどうかに対するあいまいさから、ネットワークの防御者やアナリストは慎重になり「共有しない」という決定を下す可能性がある。

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[4] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

- すべてのメンバーが同等と見なされるか、またはメンバーシップのレベルや階層を定義するか。階層を確立する場合は、各メンバーシップ グループのニーズを満たすために、サービスとデータアクセスも階層化するかどうか、またどのように階層化するかを検討する。

対象メンバーを特定する際には、以下の指標となる質問について検討する:

- メンバーの特定、指名、募集に関する戦略はどのようなものか？この進行中のプロセスで、誰が責任を負うのか、ISAO メンバーシップがどのような役割を果たすかを検討する。
- さまざまなメンバーが予想される場合、ISAO はこの多様性をどのように管理するか？メンバー組織の規模（中小企業と大企業）とサイバー脅威に対する準備レベル（基本的なサイバー防衛機能と高度な機能）の両方について多様性を考慮する。
- 新しいメンバーはどのように ISAO に参加するか？ISAO メンバー間の信用への影響と、これらの新しいメンバーが既存のメンバーシップにどのように導入されるかを検討する。
- ISAO のミッションとビジョンを実現するためには、新しいメンバーに対してどのような審査が必要か？
- 新しいメンバーにどのようなコミュニケーションと訓練を提供するか？

3.7 有効性の評価

新しい ISAO の設立の早い段階で、ISAO によってサポートされるサービス、機能、および情報共有の全体的な有効性の評価に役立つ一連の評価基準を作成することを検討する。

対象メンバーを特定し、既存メンバーの維持に努める際には、以下の指標となる質問について検討する:

- メンバーシップの投資対効果を実証するためには、どのような評価基準が必要か？ISAO が受け取ったサイバーセキュリティ情報の種類に関する集約データを追跡し、続いてメンバーが利用できるようになった情報に関する集約データを追跡することは、メンバーが投資対効果を理解するのに役立つ。同様に、ISAO によって実施された分析の価値を示す詳細な例を提供することも、投資対効果を実証するのに役立つ。ISAO はメンバーの「成功事例」の収集も、おそらく非常に重要な事項として検討する必要がある。個々のメンバーの成功事例は、ISAO がメンバーにどのように役立つかを一般メンバーがよりよく理解するのに役立つからである。

- ISAO がサービス、機能、情報共有の有効性を改良するためには、どのような評価基準が必要か？ISAO がその提供物を改良する際に役立つ評価基準の一例に、確定されたフィードバック プロセスがある。このプロセスは、メンバーが ISAO から受け取ったサイバー脅威インテリジェンスに対するフィードバックを提供できるようにする。
- サービス、機能、情報共有のニーズを特定するのに役立つ評価基準はあるか？体系的な調査やメンバーへの直接インタビューによって、定期的にメンバーのニーズを評価することを検討する。
- ISAO の管理をサポートするために、これらの要素を時間の経過に沿ってどのように測定できるか？これらの要素の測定頻度は？

4 運用計画の主要要素

ISAO の設立が成功するかどうかは、有効な戦略計画だけでなく、運用計画の主要要素にも依存する。ISAO が設立されたら、製品とサービスの効果的な実施と発展のために組織モデルを作成する必要がある。運用計画の主要要素には、役割、ガバナンスモデル、事業計画のサポートが必要な可能性のある法人の種類または形式の決定が含まれる。

4.1 ガバナンスモデルの確立

個人および小さなグループは、非公式の意思決定モデルで機能する場合がある。しかし実際の ISAO では、大規模である可能性のある、多様なグループのメンバーに影響を与える決定を下す方法を検討することが非常に役立つ。ISAO をどのように指揮し、監督するかを明示した定義済みのガバナンスモデルの必要性は、新しい ISAO の重要な初期要件である。これらのガイドライン全体にわたって挙げられている検討すべき課題は、競合する優先順位、異なるニーズ、ISAO の目標に到達するための異質なアプローチを調整するために、定義済みのガバナンスモデルが必要であることを示している。ISAO を最初に組織する際に、ISAO の組織ポリシーを決定および策定する権限を与えられた運営組織を設立する必要がある。

法律などの考慮事項が多く複雑に見えるが、ガバナンスの選択は ISAO のビジョンと目標から簡単に導き出されることに留意すること。ISAO はそのビジョンと目標に応じて、より緩やかな運用規則を備えた非公式グループとして設立することも、始めから正式な事業体として設立することもできる。ISAO のビジョン、目標、およびメンバーシップは、時間の経過とともに大きく変化する可能性があることを認識することが重要である。このことは、ISAO をより小さな、より非公式な組織として開始し、ISAO が発展・成熟するにつれてガバナンス体制の変更を検討するという考えの裏付けとなりうる。

4.1.1 公式のガバナンス体制と非公式のガバナンス体制

ISAO を非公式のガバナンス体制と公式のガバナンス体制のどちらで設立するかの意思決定に役立つ以下の質問について検討する:

- **メンバーシップ要件。**ISAO は、メンバーが書面によるメンバーシップ要件に公式に同意することを求めるか？同意を求める場合、これを実施する方法の 1 つは公式な法人を作ることである。メンバーはこの法人に対して、メンバーシップ同意書、覚書、情報共有同意書、または同様の文書を通じて合意できる。
- **メンバーシップの費用／支払い。**ISAO が支払いを行うまたは受け取る場合、それらは税の観点ならびに適用される法律および法的規制に従ってどのように扱われるか？公式の法人（地方および連邦の法律に当てはまれば非営利法人も含む）が最善の方法である可能性がある。
- **第三者。**ISAO が第三者との契約を必要とする活動に従事することが予測されるか？そうでない場合は、少なくとも ISAO でそのようなニーズが発生するまで、別個の法的ガバナンス体制は必要ではない可能性がある。

4.1.2 公式な法人の種類

ISAO のニーズと要件に最も適した法人の種類は何か？例えば、重要なリソースを持つ非常に大規模な ISAO は、地方や州の法律の下で法人化することによる、最も公式なガバナンス体制および責務からの最も明確な保護を検討することもできる。対照的に、単に別個に認められた法人として事業を行う能力を必要とする小規模の ISAO は、有限責任会社（LLC）などの、より公式性の低い体制、またはガバナンスの柔軟性の高い体制を必要とする可能性がある。

さらに ISAO は、ISAO が交流し契約を結ぶことを望む後援者、規制当局、および他の第三者が、LLC と比較して、関連する法律および判例法がより発展している組織である株式会社に、より安心感を持つ可能性について検討すべきである。

前述の質問に基づいて、ISAO が、ISAO メンバーのニーズに応えるためには ISAO を公式の法人として設立することが必要であると結論づけた場合、ISAO とそのステークホルダーは、ISAO のニーズを満たすのに最適な法的体制の選択をサポートするために、弁護士への相談を検討する必要がある。法人、取締役会、非営利法人などのガバナンス体制の決定には、地方、州、および連邦の法律に関する知識が必要である。

4.2 ビジネスモデルの作成

ISAO は、ビジネスモデル、資金調達を特定および維持する方法、メンバーシップの参加を維持する方法、共同作業と分析活動のサポートに必要な情報技術を確立および維持する方法、およびメンバーの期待に応えるための ISAO の機能の実行を監視する方法を、時間をかけて検討する必要がある。検討すべきビジネスモデルの主要要素を以下に示す。

4.2.1 マーケティング計画

通常、マーケティング計画とは、企業の広告とマーケティングの計画を記録した文書である。マーケティングの目標が明確にされ、計画はそれらの目標を達成するために必要な活動を記述する。

マーケティング計画は、ISAO の継続的な定義付けをサポートし、メンバーシップに働きかけ、全体的な運営を可能にする。マーケティング計画は、公式の詳細な文書にすることも、ISAO のスタッフおよびメンバーが実施する非公式の活動にすることもできる。以下の検討事項は、ISAO のビジョンの定義の一環である。ISAO のマーケティング計画を特徴づけるのに役立つ以下の各項目を検討する:

- マーケティングの根本的なポリシーとプロセス:計画の定義、開発、維持を行うのは誰か?
- 目標、想定される機能、提供しようとする価値と利益、他の ISAO との違いなど、ISAO の基本的なポジショニング ステートメントは何か?
- 求人活動、外部のコミュニケーション、メンバーのコミュニケーションでどのようにポジショニング ステートメントを使用するか?
- ISAO の対象者への接触
  - マーケティング コミュニケーションのポリシー:マーケティング コミュニケーションの規則、責任、権限はどのようなものか?
  - ISAO は対象者とのコミュニケーションにどのような戦術的マーケティング手段を使用するか(例:イベント、オンライン資料および文書による資料、広報活動、広告、非公開求人など)?
  - 収入となる広告機会を ISAO が受け入れる予定の場合、ISAO の特性を取り巻くポリシーや、ISAO の特性に関する広告のプロセスはどのようなものになるか?

4.2.2 コミュニケーション戦略

コミュニケーション戦略とは、適切なコミュニケーション目標を選択し、ISAO の具体的な意識目標を明確にすることである。コミュニケーション戦略は、メンバー、見込みメンバー、パートナーとの関わりに焦点を合わせている。これは、サイバーセキュリティ情報の共有に関連するものではなく、すべてのステークホルダー間で効果的なコミュニケーションを可能にすることが目的である。

ISAO には、ISAO の規模、スコープ、複雑さ、慣習、目標、ミッション、およびリソースに適したコミュニケーション戦略が必要である。ISAO のコミュニケーションに関する決定には、メンバーと ISAO スタッフの役割、責任、および規則に関する基本的な運用ガイドラインが含まれていなければならない。戦略に詳述されているスコープと戦術は、ISAO の運用コストに影響する可能性がある。以下の質問を検討する:

- **外部コミュニケーション**（サイバーセキュリティ情報共有を含まない）
  - 外部コミュニケーションのポリシー：外部コミュニケーションの規則、責任、権限はどのようなものか？
  - 外部コミュニケーションのガバナンスの手法とアプローチ：ISAO は、ガバナンス事項について他の ISAO、ISAO 管理機関、戦略的提携先、政府組織とコミュニケーションを取るのにどのような手法やアプローチを使用するか？
  - 外部コミュニケーションの戦術ツール：ISAO が外部とのコミュニケーションに使用する戦術ツールは何か（例：リストサーブ、ポータル、ニュースレター、電子メール、ニュースフィード、カレンダー）？
- **ISAO メンバーのコミュニケーション**（サイバーセキュリティ情報共有を含まない）
  - メンバー コミュニケーションのポリシー：メンバー コミュニケーションの規則、役割、責任、権限、および活動はどのようなものか？
  - メンバー コミュニケーションのガバナンスの手法とアプローチ：採用や登録、進行中のポリシーや機能の開発、戦略計画、成果などの事項について ISAO メンバーとコミュニケーションを取るための手法やアプローチはどのようなものか？
  - 制限された ISAO メンバー コミュニケーションのポリシー：ISAO メンバー間で明確に制限されているコミュニケーションはどのようなものか？それは業界や政府の規制に基づいたものか、それとも業界や政府によって制限されたものか？そうである場合は、それらの制限されているコミュニケーションはどのようなものか？
  - メンバー コミュニケーションの役割：情報を送受信する ISAO メンバーの役割と、各役割が送受信する情報の種類はどのようなものか？
  - メンバー コミュニケーションの戦術ツール：ISAO がメンバーとコミュニケーションを取るために使用する戦術ツールは何か（リストサーブ、ポータル、ニュースレター、電子メール、ニュースフィード、カレンダーなど）？

4.2.3 財務計画

ISAO は、その資産、支出、および収入を慎重に評価することで、現在および将来の財務状態を理解している必要がある。財務計画は、これらの要素を記録して ISAO が持続可能な未来を計画できるようにする。

ISAO には立ち上げのコストに対処する財務計画が必要となるが、ISAO の目標、スコープ、およびサービスをサポートするには継続的な収入が必要である。特定の短期的な問題に対処するために形成された小規模な ISAO であっても、基本的な資金供給に対処しなければならない。ISAO の収入の流れは、メンバーシップ料やサービス料も含めて、ISAO が選んだビジネスモデルの種類に依存する。ISAO のビジネスモデルの種類に基づいて、資金調達オプションと潜在的な収入源を検討する必要がある。

4.2.4 コスト要因

ISAO の運用および財務計画に対する基本要件や主な投入資本を特定するために、外部環境および市場の評価を実施することがある。ここに記載されている項目は、事業計画と運営予算の策定における議論を導くために提供されている。各 ISAO は、規模、スコープ、リソースの点で大きく異なる場合がある。

ISAO がサービスを提供するために必要とするサービス、スキル、および技術によっては、ISAO の運用支出のかなりの部分を特定のコストが占めていると判明する場合がある。固定コストか変動コストかといった各種類のコストの性質、およびメンバーシップの増加に伴ってこれらのコストがどのように変化するかは、検討に値する。ISAO は、支出のタイミングを収入のタイミングに合わせることで利益が得られる（例えば、使用量に基づいて毎月請求が行われるクラウドベース ソリューションの技術提供か、初期設備投資が必要となるサーバー購入か、など）。ISAO を設立し維持するための、および日々の運用のための、以下の主要なコスト要因、経費、資本要件を検討する：

- **管理と運用**
  - 組織構成：法的サービス、州／連邦の法的規制、および税務／会計サービス。
  - ISAO のスタッフ：ISAO に所属するメンバーの規模や人数にかかわらず、ISAO の管理と日々の運用に必要なサポートスタッフについては慎重に検討する必要がある（例えば、経営幹部、マネージャー、アナリスト、製品開発者、メンバーID 管理者、リスクおよびコンプライアンスのスタッフ、メンバーシップ開拓スタッフ、財務スタッフ、販売宣伝スタッフ、弁護士など）。
  - 専門サービス（コンサルティング、税務、経理、法的支援など）：ISAO は、地域、州、または連邦の法律および規制に従って特定の活動について助言するための共有メカニズムまたは法的サービスの立ち上げを支援するために、技術者などの外部専門家の助言を必要とする活動に従事するか？ISAO は、フルタイムまたはパートタイムの従業員を雇用するか、または情報の共有と分析を促進するためにコンサルタントや請負業者に依頼するか？
  - ガバナンス：取締役会、最高経営責任者、必須である可能性のある他の役割（ISAO の法的体制による）。これらの役割は、金銭的な報酬を受け取る個人に割り当てられるか？

- **インフラと技術。**ISAO では技術が重要な役割を果たしており、各技術ソリューションのコストは大きく異なる。ISAO をサポートおよび維持するために、ISAO は以下を含む運用要件およびインフラ要件を決定する必要がある:
  - ソフトウェア:次のアプリケーションとライセンス料 - 中核となる ISAO サービス(情報の取得/配布/分析/アラート(構築するか購入するかの決定))、機密データを扱うためのツール(例:匿名化)、ISAO の日常業務をサポートするアプリケーション(財務、セキュリティ、情報技術サービス管理、メンバーシップ開拓、共同作業用ツールなど)。
  - 分析:必要な分析処理機能と、データの分析とデータの拡充をどこまでサポートするか(組織内、外部委託、またはハイブリッドモデル)。
  - ハードウェア:オンサイトまたはクラウドコンピューティング、システムセキュリティ、大容量ストレージの要件、災害復旧など。
  - データ フィード プロバイダー:ISAO がメンバーシップに提供する、データ分析の強化をサポートできるフィードと製品を提供する外部ベンダー。
- **プロモーション コスト**:ISAO が対象とする市場のコミュニティーで関心を高め、メンバーシップを増やし、メンバーの関係を管理するために、組織内のマーケティング機能およびアウトリーチ機能を開発すること。
- **メンバーのニーズ**:コストに影響を及ぼす ISAO メンバーシップ対象コミュニティー(メンバーの人数、規模を含む)とメンバーのニーズ(例えば、予想される脅威フィード数、ISAO 情報共有インフラコミュニティーへのメンバーの登録および統合など)。
- **訓練と教育**:経営陣とサポートスタッフの継続的な訓練(物理的な面とサイバー面での両方におけるすべての損害に関するセキュリティ)、ISAO のポリシーと手順、ISAO のインフラ情報交換/共有プラットフォーム、情報共有のポリシーとプロトコル、および ISAO の提供するすべての追加サービス
- **オフィススペース**:ISAO が定期的に直接会合する場合、ISAO はそのためのスペースを借りる必要があるか、または特定のメンバーが ISAO の経営陣とメンバーが会合できるスペースを提供するか?ISAO が会合や運営のためのスペースを借りる必要がある場合、メンバー個人が名乗り出て賃貸借契約に署名するのか、または ISAO が署名する必要があるのか?あるいは、カンファレンススペースや会合スペースの短期レンタルを利用できる可能性がある。
- **財務管理**:ISAO は、サービスへの支払いや資金の受け取り用に独自の銀行口座を必要とするか?
- **保険**:メンバーは、ISAO がその活動内容がカバーされる保険に入ることを求めるか?

- **認定、メンバーシップ、または加盟**：ISAO は、認定、メンバーシップ、または加盟を取得または維持する必要があるか？

5 信用できるコミュニティーの構築

ISAO は、各メンバー間、メンバーと ISAO 間、ISAO とパートナー間に一定レベルの信用が存在しなければ機能しない。信用のレベルが高いほど、ISAO の実効性は高まる。参加者間での自由な情報の流れには信用が必要である。特に、共有パートナーがメンバーおよび共有情報を公平に扱うという前提をメンバーが信頼する必要があるような重大な状況では、信用が不可欠である。最低限の信用がなくては、メンバーが受け取るデータの正確性および共有する情報の責任ある取り扱いについてメンバーに疑いが生じることになる。これにより、有意義なデータが交換される可能性が低くなり、ISAO の真の目的が阻まれる。信用は、ISAO の価値を実現するための鍵である。

人生のその他のあらゆる面と同じく、公式に設立された ISAO であっても信用は自然に形成されるものではない。信用は獲得するものであり、関係を通じて、時間をかけて、そして多くの場合試行錯誤を経て築くものである。メンバーは信用を築きながら、個人的な関係や法的な関係、そして組織体系を活用して情報交換を開始したり支援したりすることができる。時間が経つにつれ、そして試行を重ねることで、ISAO 内で信用のレベルが高まり、有効かつ適時で有益な情報共有が可能になる。

信用に基づくやり取りが実現される組織体系を、「信用構造」と呼ぶ。組織では多くの信用構造が利用されており、各 ISAO は、組織構造の一部として、目に見える永続的な構造から恩恵を受ける。信用構造は、ISAO スタッフが個人的に連携しているメンバーのみに対応するような単純なものであったり、参加者の法的代理人が管理する継続的な契約に関するやりとりの過程と同じくらい複雑なものであったりする可能性がある。すべての信用構造には長所と短所があり、すべての ISAO はその選択肢を検討して、参加者のニーズに最も適した構造を構築する必要がある。

承認された公式の信用構造は、たとえ非常に単純なものであっても、多くの理由で ISAO にとって貴重である。信用構造は、共有の基本原則を規定する。これによりすべてのメンバーが自身が同意した内容および自身の責任を理解するようになる。すべてのメンバーがそれらの同意および責任に基づいて行動することで、信用が実証され強化される。また構造はある組織について、潜在的なメンバーが、自身が参加したい組織であるかどうかを判断するのに役立つ。同様に、他の ISAO が潜在的な協力相手を特定するのに役立つ。さらに、必要に応じて、メンバー間の対立を解消するように導くことができる。

5.1 ISAO での信用の構築

単一の信用モデルが、すべての ISAO に適合することはない。 各 ISAO は、その組織を設立する活動の一環として独自の信用構造を作り上げる必要がある。効果的な信用構造を作り上げるには、各 ISAO がそれぞれ独自の状況における実務の詳細に取り組む必要があるため、時間を要する。個々の状況にかかわらず信用を高めるというニーズを満たすには、ISAO の計画と運用のあらゆる面の開発において、信用を中心に据

えることが必要である。標準テンプレートは存在しないため、信用構造を確立または変更する際に検討すべき事項を以下に示す:

- ISAO でのメンバーシップの権限と予想される事柄のすべてが記述された書面によるメンバー契約を作成する。
- 組織の全体的なタイプ(例えば、人対人、組織対組織、制限されたメンバーシップまたはオープンなメンバーシップ)を決定する。
- 秘密保持契約(NDA)などの法的契約が必要か?あるいはメンバーは個人的な関係に依存することを不快に思わないか?いずれの場合でも、この事項に関しては法定代理人に相談することが有用であると考えられる。
- NDA などの法的な構造を使用する場合は、組織のすべてのメンバーに対して理解しやすく、拘束力があり、実施可能であることを確認する。
- 情報の使用方法を理解する。例:
  - メンバーである団体内でどのように情報が共有されているか?
  - メンバーは非メンバーと情報を共有できるか?
  - 各政府機関(州、地方、連邦、米国以外)は、それぞれの透明化に関する法の下で、どのように共有情報を開示から保護するか?
- ISAO の最適な規模は?限定的なメンバーシップの中で信用を維持することが最も簡単であるが、情報源も限られる可能性がある。
- メンバーの加入または脱退をすべてのメンバーに通知する方法を決定し、誰がコミュニティーのメンバーであるかをすべてのメンバーが分かるようにする。
- メンバー契約への違反に対処する仕組みを用意する。例えば、最初の違反での書面による警告、違反している組織への制裁金、メンバーシップの停止、または違反しているメンバーの組織からの追放などが挙げられる。
- メンバーが ISAO 自体を信頼できるようにする。メンバーが ISAO と安全に情報を共有できるように、データの取り扱い、データの保護、データの使用について明確な条件を提供する。データのセキュリティに関する追加情報については、ISAO 300-1 の『*Introduction to Information Sharing (情報共有入門)*』を参照。

ISAO の信用のレベルが高まるにつれて、メンバー間のどのような要素によって信用が築かれたり損なわれたりするかを、よりよく理解できるようになる。この信用のレベルの向上については、次のセクションで取り上げる。

5.2 信用の構築と維持

ISAO は最初にメンバー間で一定の信用を築く。この信用は、ISAO とそのメンバーの行動に基づいて時間の経過と共に向上する。以下に、信用のレベルの構築と維持に役立つ行為の例を示す:

- 誰かに「最初に行わせる」ことによって信用を作り出す:
  - 特定のメンバーを選んで特定の情報を共有するように求める。
  - 慎重に扱うべき問題についてのプレゼンテーションをメンバー全体に対して行うようメンバーに依頼する。
- 少数の団体で開始して、メンバーがお互いを知り、交流するように小さなコミュニティーを維持する。
- セキュリティに対して共通のニーズまたは関心事を持つ団体または組織からメンバーを勧誘する。
- 既に信用の要素や確立されたビジネス関係を持つ団体または組織からメンバーシップを構築する。
- 商工会議所、政府機関、地方の非営利団体や非政府組織、選出された役職者、または事業者団体などのコミュニティー内の信頼される団体に対して、組織を推薦し、他者の参加を促してもらうように依頼する。
- メンバーに定期的に信用モデルのメカニズムとそのルールを再認識させる。
- 信用のレベルを時間をかけて積極的に測定・追跡し、ISAO とそのメンバーの行為が信用のレベルにどのように影響するかを評価する。信用は、メンバーとの関わりを通じて直接的に測定することも、信用のレベルに代わるものとして他の測定基準(例えば、共有される情報の内容や量など)を用いることで間接的に測定することもできる。
- 信用に反する行為がある場合は、それを明らかにし、是正する。問題をなかったものとして処理せず、直接的かつ公表した形で解決する。

ISAO は、時間をかけて丁寧で誠実な交流を行うことで、メンバーとパートナーの間で強固な信用を築くことができ、情報共有において明確な利益を享受できる。

6 最終検討事項

ISAO の確立および発展は、反復的なプロセスである。本書に記載されているガイドラインは、考慮すべき戦略上および運用上の最も重要な要素を提示することで、このプロセスを支援することを目的としている。各 ISAO においては、その発展とともに、これらのガイドラインを定期的に再評価することを推奨する。

さまざまな ISAO が情報共有エコシステムに参加しており、現在、多くの設立された ISAO および発展中の ISAO が存在する。各 ISAO は、共通のニーズを満たし、他の ISAO の経験から学ぶために、積極的にパートナーシップを確立する必要がある。

ISAO SO は、このガイドライン一式に加えて、ISAO の主要リソース集を作成している。[5] 各 ISAO においては、これらのリソースを確認して活用することを推奨する。

[5] https://www.isao.org/resources/resource-library/

付録 A サービスおよび機能の表

この付録では、ISAO の共通のサービスや機能、各サービスの利点、課題、実装ガイドラインを記載したリストを示す。
サービスは以下の 3 種類に大きく分類される:

- **基本**のサービスと機能は、ほとんどの ISAO のベースラインとなるサービスとして一般的に想定されているが、これらは ISAO のメンバーのニーズに基づいて確立される。いくつか例を挙げると、サイバー脅威インテリジェンスを送受信するための標準的な手法の使用、メンバーの審査(信用能力)、サイバーセキュリティ情報の保存などがある。
- **追加**のサービスは、ISAO をさらに差別化するか、特定の運用環境やビジネス環境のニーズと制約を満たすためのものである。これらのサービスは、基本のサービスによって提供される範囲を超えて拡張されたサービスを提供し、ISAO が、メンバーのニーズに対応するように設計されたサービスのポートフォリオを作成する際に役立つ。例えば、受信するサイバーセキュリティ情報を、メンバーのニーズに対する適合性を評価するために分析することなどが挙げられる。
- **固有**のサービスは、特定のニーズや機会に対応するために組織が開発または採用する特有の機能または行為である。「基本」または「追加」として識別されないものは固有サービスである。固有サービスは、ISAO によって選択的に作成および適用される。これには、効果的なファイアウォール設定を理解すること、メンターとプロテジェ(メンターに指導を受ける者)の間の機会を拡大すること、リストサーブの仕組みを導入することなどが挙げられる。下の表の記載されている例と併せて、これらが「固有」に分類される可能性のある潜在的なサービスまたは機能の代表例である。

ISAO のサービスと機能は、組織によって選択され、メンバーのニーズをサポートする。ISAO は、ISAO と認められるために、以下に列挙した基本のサービスまたは機能のすべてを提供する必要はないことに注意すべきである。むしろ下記の表は、関係する組織が、ISAO を設立したりそのサービスおよび機能を発展させたりする過程での評価および使用のために、各サービスの長所と短所に関する情報を提供することを目的としている。

サービス／機能	説明	利点	課題	実装ガイドライン
データの収集と配布	データはメンバーのニーズに基づいていなければならない。データには、脅威アクターが使用する脅威、脆弱性、リスク、インシデント、戦術、技術、または手順に関する情報が含まれる場合がある。また、データの種類は、IP アドレス、MD5 ハッシュ、コマンド & コントロールの情報などの、侵害の実際の検知指標（IOC）になる場合がある。データはオープンソースのレポートを抜粋することでさまざまなソースから得ることが可能である。ソースの例として、サイバーセキュリティベンダー、メディアの記事、サイバーセキュリティブログなどのサイトから、ホワイトペーパーから、他の ISAO や ISAC から、政府機関や政府報告書から、そしてメンバーから直接などがある。ISAO は、関連するデータを解析したり、メンバーへの関連事項を追加したり、単に詳細情報へのリンクを付けてソースを配布したりすることを選択できる。各項目は、アラート、日次レポート、ポータル／データベース、Web サイト、リストサーバー、ニュースレター、または他の手段を介して配布することができる。配布形式は、メンバーが望むものであればテキスト、PDF、HTML など何でもかまわない。配布頻度もまたメンバーの要望に基づいていなければならないが、毎日、毎週、または毎月が考えられる。	DHS インフラ レポートや ISAC 日次レポートなどの日次レポートを既に作成している別の組織と提携して、メンバーに日次レポートを電子メールで配布することで、基礎レベルにおいて、情報収集と配布を簡単かつコスト効率よく行うことができる。一度プロセスが確定されれば、情報を集める手段をルーチン化できる。データの収集と配布は ISAO の基本的な活動であり、関連性のある有益なデータをコミュニティーに提供するための非常に簡単な方法となり得る。	必要なデータのレベル、配布の形式や頻度に応じて、このプロセスには人材、時間、工程、技術が必要となる可能性がある。プロセスを開発し、ソースを選別するには時間を要する。また、メンバーが使いやすい形式を見つけて、メンバーに関連することやメンバーが求めることを判断するには、時間とメンバーの理解が必要である。セキュアポータルを開発する場合や、マシン対マシン（自動）形式で IOC を共有するためのプラットフォームを作成する場合など、ニーズに応じて、技術についてもその立ち上げおよび保守に大幅なコストがかかることがある。データを自動的に提供または取り込む機能をメンバーが持っていない場合がある。	基本：メンバーが容易にデータを共有できるようにする。既存の日次レポートを取得するか連携して、メンバーに電子メールで配布する。電子メールによる調査で、メンバーが閲覧を希望する内容と、最良の配布形式を決定する。 ベンダーのブログ、ニュースメディアのフィード、ISAO または ISAC からの他のレポート、政府からのレポートなど、メンバーに関連するオープンソース情報のリストを作成する。有益な閲覧のために適切な文書について説明し、リンクを作成する。メンバーが望む形式および手段で配布する。 追加：メンバーがデータを送信するためのセキュアポータルを作成し、メンバーが利用するための関連文書と指標を提供する。 固有：「基本」に記載されているレポートを作成し、脅威インテリジェンスの視点と、メンバーシップ解説の注釈を各項目に追加する。
メンバーによる情報共有の促進	情報源が開示されているかどうかにかかわらず、メンバーがお互いに、また ISAO と情報を共有できるようにするプロセス。	コミュニティーのメンバーがお互いをよく知っていれば、容易に信用を築くことができる。 Traffic Light Protocol（TLP）は、メンバーに共有プロトコルに同意してもらうための簡単な方法である。 NDA のような文書も非常に明確であり、信用を築くのに利用できる。 共有によって、メンバー全体の状況認識を強化し、リスクに基づいた意思決定を伝えることができる。	信用できる環境の構築は、特にコミュニティーのメンバーがお互いをよく知らない場合は、非常に困難である。 セキュアな環境を作成するには（必要な場合）コストがかかる。 完全に匿名の環境を作成するにはコストがかかる。 メンバーが情報共有を行うようにすることも課題である。あるメンバーが信用を損なうと、情報の共有が停止される可能性がある。	基本：メンバーを審査し、基本的な NDA を作成し、メンバーが合意する TLP の種類を確立する。 電子メール リストサーバーを作成し、コミュニティー内に賛同者を見つけて共有を開始する。 アナリストまたはスタッフは、匿名による共有のブローカー役を務めることができる。 追加：メンバーが求める場合は、基本ステップに加えて、セキュアな手段で共有を確立する。 匿名の情報共有を送信するためのポータルを開発する。ポータル環境には、信用を築きセキュアな環境を作るための認証と識別の手法が含まれる場合がある。共有によるインセンティブと報酬を策定する。

サービス／機能	説明	利点	課題	実装ガイドライン
関連性と傾向に関する情報の分析	一般的には、あるステークホルダー グループのメンバーは、自身の特定の業務／利益に関連する分析に関心がある。 分析によりメンバーに関連しないデータを除外することでメンバーに有用な情報を生成でき、グループ内で、またはグループに関連性や重要性のある領域で見られる傾向に関する情報を提供できる。	傾向を示すデータは非常に有益であり、メンバーがそれぞれの環境内で何が起こっているのかを理解するのに役立つ。 関連性についての分析を提供することで、より有益な情報と状況認識が得られる。	メンバーが自身で分析を行いたい場合、メンバーにベンダー競合の問題がある場合、あるいはメンバーが追加のリソース要件を提示する場合がある。 グループ、関連しているデータ、および傾向の見きわめ方と分析方法をよく理解している熟練した分析スタッフを見つけることは難しく、コストがかかる可能性がある。 データの傾向の分析は、特にグループによって提供されているデータに依存している場合には、時間を要することがある。	基本:メンバーが一般的な問題や傾向を議論し、特定するためのフォーラムを提供する。 追加:関連するオープンソースの情報を見つけるには、グループのメンバーとニーズを理解する必要がある。オープンソースからの傾向レポートは、状況認識のために配布することができる。 固有:アナリストスタッフを雇用または外部委託して、分析手法を適用し、グループに関連するデータを収集して分析することにより、グループのデータに関する意見または戦略的観点を適用する。スタッフまたは第三者は、その環境内にあるデータを収集するためにメンバーを調査したり、ISAO のプロセスまたはオペレーション内で共有された情報を入手したり、その他の情報源を利用して適用可能な傾向やレポートを作成することができる。
メンバーへの情報の配布	メンバーと情報を共有するための、メンバーのニーズに基づいて確立および合意された仕組みを用意する。アラート、勧告、および／または月次レポートや週次レポートなどの定期的な出版物などが挙げられる。	アラートと勧告は、最新のアクティブなインシデントと脅威、そして新たに報告された脆弱性を適時にメンバーに知らせる。 定期的な情報の配布は、脅威、リスク、脆弱性、準備、回復や緩和、および組織的な活動やその他の活動に関する情報を適時にメンバーに知らせる。	電力、携帯電話、インターネットの停止により、メンバーが電子メールでアラートを受信できなくなることがある。 メンバーが時間的制約のある成果物の価値を認識しない可能性がある。 実用的な成果物を作成するには運営のバックグラウンドが必要な場合があるが、その取得、保持、投資は困難である。 作成、管理、維持のためのコスト、努力水準、およびリソースの各ニーズは、特に緊急の期限を守るためには、高くなる可能性がある。 内容を絞り込まずに情報を流すことは、情報疲労やメンバーへの負担を招き、読者や価値を減少させる可能性がある。	基本:配布は以下のようにして達成することができる。 1)デスクトップアプリケーションまたは Web メール 2)ブロードキャスト電子メールサービス 3)LISTSERV™などの電子メーリングリストサービス 4)電話 5)Web サイト 6)上記の組み合わせ。 追加:セキュアポータル、暗号化された電子メール チャネルまたはその他のセキュアな手段を介して、または緊急警報システム経由で。

サービス／機能	説明	利点	課題	実装ガイドライン
メンバーの調査	調査は、メンバーに関する情報を学ぶのに役立てることができ、メンバーの活動やニーズをすばやく理解する手段にもなる。	メンバーの状況やニーズを判断するために使用できる。	調査の実施と分析には時間を要する。 一部の調査ツールの利用は、組織によっては許可されていない。 メンバーを調査に参加させることは、特にインシデント中は困難である。	基本：基本的な電子メール調査を実施したり、電話で話したり、顔を合わせての打ち合わせを行ったりする。 追加：メンバーからの調査依頼を受けて調査を進めるための調査委員会を設置し、行動や理解のために結果を分析する。 固有：インシデント時のアラートと調査のためのカスタム ツールを作成して、メンバーの状況を素早く把握し、すべてのニーズや関連情報を判断する。
メンバー間の共同作業のためのセキュアなオンライン会議スペースやその他のオンラインフォーラムの開催	メンバーが仮想的かつセキュアに共同作業や共有を行える手段を用意する。これには、セキュアなリストサーバー、二要素認証か他のセキュアな認証を使用するポータル、または Web セミナーや、審査されたステークホルダーにアクセスを制限するクラウド コラボレーション ツールなどが挙げられる。	メンバーがセキュアな環境下で共同作業を行ったり、同僚、当該分野の専門家（SME）、ISAO スタッフから脅威、脆弱性、ベストプラクティスについての助言を求めたりする機会を提供する。 セキュアなオンライン空間を提供することで、信用が向上し、要保護情報の共有が促進される。	作成、保守、および維持のためのコスト、努力水準、およびリソースのニーズが高くなる可能性がある。 メンバーが、合理化されたアプローチ、技術レベルの低いアプローチ、接触頻度の低いアプローチ、自動化されたアプローチ、またはその他のアプローチを好む場合がある。 複雑さが増し、ISAO とメンバーの両方にとって、参加、共有が減少しコストが発生する可能性がある。	追加：カスタマイズ可能な Web ベースのソリューションを使用する。（そのようなツールを実装する場合）ISAO のオンラインポータルと統合できるものが望ましい。 このサービスのプロバイダーは多数存在する。
セキュリティ脅威の緩和に関する情報とリソースの収集および配布	セキュリティ脅威の緩和に関する情報は、メンバーを含むさまざまな情報源から得ることができ、攻撃の予防および防御に使用できる。	セキュリティ脅威の緩和に関するリソースが信頼できるものであり、メンバーのニーズに適合し、リスク管理に良い影響を与える場合、メンバーの提供価値と ISAO の存続可能性に貢献する。 コミュニティーの回復力を高める。	適切に管理されていない場合は責任に関する懸念に対してリスクが生じる可能性があり、追加の人材、時間、工程、技術が必要になる可能性がある。	追加：さまざまな情報源からの緩和戦略を記載したレポートを提供する。 悪意のある活動をブロックするコードなどの緩和戦略のメンバー間での共有を促す。
対応情報および回復情報ならびにリソースの収集および配布	対応情報および回復情報は、メンバーを含むさまざまな情報源から得ることができ、攻撃の予防および防御に使用できる。	対応および回復が信頼できるものであり、メンバーのニーズに適合し、リスク管理に良い影響を与える場合、メンバーの提供価値と ISAO の存続可能性に貢献する。 コミュニティーの回復力を高める。	適切に管理されていない場合は責任に関する懸念に対してリスクが生じる可能性があり、追加の人材、時間、工程、技術が必要になる可能性がある。	追加：さまざまな情報源からの対応戦略と回復戦略を記載したレポートを提供する。 メンバー間での対応戦略や回復戦略の共有を促す。

サービス／機能	説明	利点	課題	実装ガイドライン
関連する政府機関との関係の構築と維持	政府や法執行機関とのパートナーシップにより、インシデント時における追加情報の提供および共同作業の促進が可能になる。	新しい分析やその他の成果物に関するより深い認識を与える。 サイバーアナリストやインテリジェンスアナリストへ接触できる可能性がある。 相談、共同作業、パートナーシップの機会に繋がる可能性がある。	アクセス権を得るためにセキュリティクリアランスやバッジ等のマークが必要となる可能性、共同作業を可能にするための追加要件が発生する可能性、および共有によってメンバーの信用上の懸念が高まる可能性がある。 法執行機関の要求（当該関係内に存在する場合）への対応は、他のサービスからリソースを流用させる可能性がある。	追加：メンバーに価値をもたらす連邦、州、地方の機関を特定する。 既に機関と交流している可能性のある業界パートナーと関係を確立する。
メンバーと情報を共有するためのセキュアなオンライン文書リポジトリの設置	オンラインポータルは、メンバーが関連情報にアクセスするためのセキュアな手段を提供する。	メンバーのために中心となる文書用クリアリングハウスを提供する。 電子メール メッセージに文書を添付することにより文書の配布に対する代替手段を提供する。 「私用禁止」や、TLP の赤、黄、緑などの印が付けられた文書など、メンバー専用の資料を保持するためのアクセス制限のあるスペースを提供する。	作成、保守、および維持のためのコスト、努力水準、およびリソースのニーズが高くなる可能性がある。 メンバーが、合理化されたアプローチ、技術レベルの低いアプローチ、接触頻度の低いアプローチ、自動化されたアプローチ、またはその他のアプローチを好む場合がある。 メンバーがさらに別のポータルへのログインを望まない可能性がある。	追加：記事や文書の組み合わせを投稿でき、メンバーが閲覧やダウンロードを行えるようにするパスワードで保護されたオンライン空間を開発する。 考えられるソリューションとしては、情報資産プラットフォーム、カスタムメイドのプラットフォーム、DHS の国土安全保障情報ネットワーク プラットフォームなどが挙げられる。
自動検知指標共有への参加	マシン間での脅威検知指標の共有。	より多くのデータを適時に共有するためのアクセスと機能を提供する。 ISAO 間および他のセキュリティパートナーとの共有を促進する可能性がある。 ISAO エコシステム全体でリスクの状況認識を促進する可能性がある。	作成、保守、および維持においてコスト、努力水準、およびリソースが課題となる可能性がある。 検知指標の数が増えると分析がより困難になる。 検知指標の情報源の信用レベルが、検知指標の有用性に影響を及ぼす可能性がある。 自動検知指標を取り込んだりプッシュしたりする機能をメンバーが持っていない場合がある。	追加：オープンソースのツールやベンダーを検討する。詳しくは、OASIS のワーキンググループを参照。
ベンダーの脆弱性通知の提供	ソフトウェアベンダーおよびハードウェアベンダーは、自社製品の脆弱性に関する通知を提供する。	より詳細な状況認識。	メンバーに配布するための追加コストが発生する可能性がある。 メンバーが既にベンダーから直接受け取った通知と重複する可能性がある。	追加：アラートのフィードを購読するか、スタッフにアラートを収集および公開してもらう。 固有：メンバーへの影響について、アラートに関する分析を提供する。
サイバー要員を育成するためのメンバーの取り組みの支援	アナリスト向け研修プログラムや認定プログラム。 カンファレンス、Web セミナー、ワークショップ、およびその他の方法による教育と研修。	より多くの提供物やサービスを提供する ISAO は、メンバーのニーズを満たすことで追加の収入源を生み出すことができる。 ISAO メンバーがお互いに学び交流する機会を提供する。	必要とされるメンバーの提供価値の範囲外である可能性がある。 努力水準によっては、多くのリソースとコストが必要になる可能性がある。 登録料、旅費、およびその他の費用が必要となる場合がある。 メンバーの参加が難しい場合がある。	追加：ISAO のメンバーやスタッフを活用して内容を作成して提示するか、第三者を活用する。 固有：ISAO のコミュニティーを活用して、認定プロバイダーの割引を得る。 組織内の専用の研修プログラムを作成する。

サービス／機能	説明	利点	課題	実装ガイドライン
メンバーが SME に相談できるリーチバック サービス（当該 ISAO の外部から情報や助言を得られるサービス）の提供	他のメンバーや組織を援助するために、メンバーまたはメンバー以外から、SME を迎え入れる能力。	類似するリスクモデルを持つ他のメンバー組織の SME を活用する。 問題を解決するソリューションを無料または低コストで提供できる可能性がある。 ソリューションのリポジトリを使用できる可能性がある。	これらの関係の発展および維持のために膨大なリソースを使用する可能性がある。 メンバーの非現実的な期待につながる可能性がある。	追加：メンバーを対象に調査を行ってニーズをよりよく理解してから、SME のコミュニティーを 1 つ以上作成する。 SME のためにメンバー コミュニティーからボランティアを募る。 ポータル、電話ブリッジ、チャット、電子メール、Web セミナーなどを利用して情報交換を容易にする。メンバーと SME の両者を保護するために、秘密保持契約または免責同意書を作成して使用する。
共通脆弱性識別子（CVE）の出版物へのアクセスの提供	CVE の出版物は、脆弱性に関する技術情報を集めたものである。	より詳細な状況認識。	メンバーの提供価値や関心の範囲を超えている可能性がある。このサービスを使用・適用するには、またはもたらされる価値についての理解を得るには、大規模なメンバー教育が必要となる可能性がある。 他者によって行われる可能性がある、競合の問題。	追加：新しい（または過去の）CVE の自動フィード（電子メール）がいくつか存在する。自動化された NCICC CVE のフィードがある。また、脆弱性情報データベースもあり、ここでは、メンバーが特定のハードウェアやソフトウェアのプラットフォームに対する脆弱性を尋ねる場合に、ISAO が CVE について具体的な検索を実行できる。 CVE の告知の取得方法とその配布方法を策定する。メンバーのニーズやアラートを受け入れる手段によっては、さまざまな配布の手法が存在する場合がある。メンバーのために、パッチ／バグフィックスを適用するための段階的な手順を作成する。
メンバーの関心のある委員会、ワーキンググループ、または特別なコミュニティーの形成	メンバー間での共同作業のために委員会、ワーキング グループ、またはフォーラムを設立する。各委員会は、ビッグデータなどの主題に沿って形成することも、メンバー、製品およびサービス、または他の望ましいグループなどの機能に関連づけて形成することもできる。	特別な注意を要する脅威、脆弱性、その他の問題がある場合に役立つ。 メンバーが多面評価の有用性を理解する可能性がある。 メンバーを関与させ、特定のタスクやプロジェクト／トピックに焦点を合わせるための簡単で費用のかからない方法である。	一般的には、努力水準が非常に高くなる。 さまざまなサービスレベルにおけるメンバーの不和を生み出す可能性がある。 メンバーの価値提供は、他のサービスオプションと比較すると、効果によって実証するのが難しい可能性がある。 作成および保守に追加のコストがかかる可能性がある。 メンバーの参加と関与に成功が左右される。	追加：重点を置く必要のある主題を特定する。 対面フォーラムと仮想フォーラムのどちらが望ましいかを判断する。 仮想フォーラムが望ましい場合は、リストサーブ、インターネット上の掲示板などのコラボレーション ソリューションを特定する。 憲章（必要な場合）およびグループリーダーを決定する。

サービス／機能	説明	利点	課題	実装ガイドライン
立案者または当事者としての演習への参加	サイバー演習は、ハードウェアレベルおよびソフトウェアレベルでサイバーセキュリティを向上させるために、最新の（および過去の）サイバー脅威とベストプラクティスを理解するための優れた手段となる。また、同じ考えを持つ専門家のソーシャルネットワーキングの改善に役立つ。	運用機能の不足している箇所を特定できる。 潜在的なパートナーとの関係を構築する機会を提供する。	一般的には、多くのリソースを必要とする。 演習への参加や意欲の支障となるような独自またはその他の懸念をメンバーが抱く可能性がある。 監視および規制の環境により、既存の厳しいメンバー演習要件と競合する可能性がある。	追加：公的機関および私的機関が主催する演習に参加する。 組織内または第三者によって開発された内部演習を発展させて実行する。
メンバー間での相互支援の促進	相互支援には、インシデント時のリソースや知識の共有が含まれる。	インシデント時に相互に支援できるように類似の組織を支援する。 メンバーのための機能向上とダウンタイムの短縮。 メンバー間の信用を高める。 ISAO のメンバーシップの価値を高める。	調整にはリソースや時間の割り当てが必要な場合がある。支援の約束が守られない場合、支援を必要としているメンバーに悪影響が及ぶ可能性がある。 法的体制の欠如は、責任と賠償の問題につながる可能性がある。	固有：ISAO を通じて、またはメンバー間で直接的に相互応援協定を締結する。
管理されたセキュリティサービスの提供	メンバーへのサービスは、ネットワークトラフィックにおける異常や攻撃の監視、アプリケーションおよびオペレーティングシステムのセキュリティパッチの配信、ファイアウォールやルータのアクセス制御リストの管理、最大限のサイバーセキュリティをメンバーに提供することを最終目的とした他のサービスのホストの提供を含む可能性がある。	メンバーに付加価値を提供して、メンバーの脱退を防ぐ手段となる可能性がある。 メンバーの意識を向上させる。 収入源になる可能性がある。	ISAO には、文書化されたサービス契約とともに専門家と経験豊富なスタッフが必要となる。 メンバーのネットワークやシステムへのアクセスは、責任問題を引き起こす可能性がある。 一般的には、多大なリソースとコストがかかる。	固有：組織内で開発するか、第三者と契約を結ぶ。
脅威インテリジェンスの生成および／または提供	実行可能な脅威インテリジェンスとは、情報に基づいた意思決定を可能にし、より良い結果をもたらす、行動の基準となる洞察である。 ISAO は脅威インテリジェンスを開発および提供して、メンバーが直面している脅威や、その脅威に対してとり得る処置へのメンバーの理解を助ける。	脅威インテリジェンスは非常に有益であり、メンバーがそれぞれの環境内で何が起こっているのかを理解するのに役立つ。	人材、時間、工程が必要になる可能性がある。 また、追加のセキュリティ対策と情報保証要件が必要になる場合がある。同じ情報を他の手段や情報源から入手できる可能性がある。 グループおよび脅威インテリジェンスの収集と生成をよく理解している脅威インテリジェンスの熟練スタッフを見つけることは、困難であったり、コストがかかったりする可能性がある。 脅威インテリジェンス プログラムの開発は、特にグループや他の情報源によって提供されている情報に依存している場合には、時間を要することがある。 セキュリティクリアランスと機密扱いの情報へのアクセスを有するスタッフが必要となる可能性がある。	固有：この機能に対する人員を雇用または外部委託するか、メンバー内でグループを形成して、脅威インテリジェンスに対応する。

サービス／機能	説明	利点	課題	実装ガイドライン
攻撃者の戦術、技術、および手順(TTP)に関するライブラリへのアクセスの提供	攻撃者の TTP に関するライブラリまたはコレクションとは、脅威アクターと、その攻撃の手法および戦略のリストである。	より詳細な状況認識。	セキュリティ上の課題が生じる可能性がある。 不正確な情報によって責任問題が生じる可能性がある。 このサービスを利用・適用するには、またはもたらされる価値についての理解を得るには、大規模なメンバー教育が必要となる可能性がある。 作成と保守に多大なリソースを必要とする可能性がある。	固有:これらの TTP を保持しているサイトへのリンクのリソースライブラリを作成し、使用されている手法や手段についての実用的なインテリジェンスを作成する。 多くの情報源、特に米国の CERT から入手できるオープンソースの脅威データに基づいて TTP に関する規則書を組織内に作成し、維持する。入手できる情報には、アラート、脆弱性報告、および技術的に精通したスタッフ向けの詳細情報(各種レベルの要保護情報の共有のタイミング、モバイルデバイスへの脅威など)が含まれる。サードパーティのサービスを購読することで、脅威と検知指標の多くの情報源を使用できる。 TTP を含む自動検知指標共有の情報源から規則書を作成することもできる。
マルウェア分析のためのメンバーによるテストベッドへのアクセスの提供	ISAO のテストベッドとは、ISAO 自身および／またはメンバーが、隔離された環境において、1 つ以上のコンピュータネットワーク環境をエミュレートするネットワーク(通常は仮想的にセットアップされる)を使用する手段である。 テストベッドは、セキュリティ構成のテスト(特に脆弱性を緩和しようとする際の変更に対するテスト)を可能にし、運用にどのような影響が生じるかを観察する。	ISAO はテストベッドを使用して、メンバーをサポートするセキュリティ構成の設定をテストし、動作中断や予期しないイベントを引き起こす可能性のある実装を行う前に、メンバーのセキュリティへの対応を推進させる手段として設定を提供することができる。 実際のマルウェアの影響をテストし、保護対策の結果を確認するために使用できる。 メンバーへの決定事項と推奨事項を確認できる。	メンバーのネットワーク、仮想環境に関するスタッフの高度な専門知識、および仮想ネットワーク構造を可能な限り複製するためには、追加の支出が必要となる。 メンバーの活動によって ISAO にリスクが生じる可能性、作成または維持のコストが伴う可能性、メンバーのアクセスおよび使用における ISAO との争議が生じる可能性、特に他のメンバーにとっての価値と比較した場合に、メンバー グループ間で価値が均等に提供されないか、メンバーが望む価値が提供されない可能性、メンバーであると同時に ISAO のステークホルダーであるベンダーと競合する可能性がある。 メンバーが、マルウェアに対処するのに十分な知識がない可能性がある。	固有:第三者と契約するか、組織内で機能を開発する。

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）：情報システムのセキュリティを何らかの形で向上する可能性を特定するための、サイバーセキュリティ情報の要素や構成の詳細な調査。

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。

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。

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）への安全で制御されたアクセスを、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。

共有（Sharing）:「サイバーセキュリティ情報共有」を参照。

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。

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

DHS	米国国土安全保障局（Department of Homeland Security）
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）
LLC	有限責任会社（Limited Liability Company）
NDA	秘密保持契約（Nondisclosure Agreement）
NIST	米国国立標準技術研究所 （National Institute of Standards and Technology）
SO	標準化機関（Standards Organization）
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, and procedures）