ISAO
Standards Organization

ISAO 200-1:
基本のサービスおよび機能

v1.0

2018 年 5 月 29 日

ISAO 200-1

基本のサービスおよび機能

V1.0

ISAO Standards Organization

2018 年 5 月 29 日

謝辞

本出版物は、情報共有のための統一ガイドライン集を自主的に作成する、継続的な取り組みの一環として、民間、専門家、および政府の代表者とともに、Information Sharing and Analysis Organization Standards Organization（ISAO SO）が作成したものである。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 PhD
ISAO SO–Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Allen Shreffler
ISAO SO–Deputy Director
Senior Consultant, LMI

Tommy McDowell
Director
Retail Cyber Intelligence Sharing Center

ワーキンググループ 2–ISAO の機能

Nick Sturgeon
Security Operations Center Director
Pondurance, LLC
President, Cyber Leadership Alliance

Jill Fraser
Chief Information Security Officer
Jefferson County, CO Information Vice Technology Services

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文書の共著者一同から深く感謝申し上げる。

Elyse Goldenberg（LMI）、Terry Leach（Agrepedia）、Alelie Llapitan（President and Co-Founder、Solutionize）、Chris Needs（NC4）、そして David Sula（Signal Processing Engineer、Leidos）。

また、本文書の作成において多大なる支援と指導をいただいた以下の ISAO SO のアドバイザーとスタッフに、共著者一同から格別の謝意を表する。Josef Klein、James Navarro、Allen Shreffler、そして Jeremy West。

目次

改訂履歴

項番	バージョン	説明	日付
1	1.0	初版	2018/05/29

1 エグゼクティブサマリー

新しい情報共有分析機関（ISAO）の設立には、大きな課題を伴う場合がある。ISAO が運用可能な状態になるまでには、乗り越えなければならない複雑な課題がいくつもあり、それらの課題の多くについては、ISAO 100-2 の『情報共有分析機関（ISAO）の設立のためのガイドライン』（2016 年 10 月 14 日発行）で取り上げている。ISAO 100-2 は、ISAO を設立するための第一歩を記したガイドラインであり、ISAO の設立を検討している方や、新しく設立された ISAO のための手引きを提供している。また、100-2 ではいくつかのサービスおよび機能を「基本」、「追加」、「固有」に分類し、一覧で提示している。機能およびサービスのワーキンググループ（WG2）では、ISAO 100-2 の付録 A で概説しているこれらのサービスおよび機能をさらに詳細に取り上げることが ISAO にとって有用であろうという考えに至った。本書の目的は、ISAO がそのメンバーに速やかに価値を提供できるよう支援することである。

2 はじめに

ISAO 100-2 の付録 A では、ISAO が最低限実施すると想定するいくつかのサービスおよび機能を、基本、追加、固有に分類し、一覧にて紹介した。本文書では、情報収集と配布、メンバーによる情報共有の促進、情報の分析、メンバーへのアンケートなど、ISAO がメンバーに提供することを選択できる基本のサービスおよび機能をさらに詳しく説明することで、ISAO を支援することを目的としている。ISAO が、そのサービスを中核とする、技術的、分析的、人的な機能を運用可能にする方法への理解を深める手助けとなり、メンバーのニーズにさらに応えられるようになることを期待する。本文書は、簡単な機能とサービスから始まり、より複雑なものへと発展していくような構成となっている。そのため、発展の過程にある ISAO においても、現在の状況に合った、参考になる箇所が本文書内に自ずと見つかるであろう。また、情報収集と配布を別個のサービスおよび機能として分けているため、それぞれを独自の章に記載している。これは、WG2 で情報収集と配布について、プロセスと技術を評価した結果、それぞれが独立したサービスおよび機能として十分に区別できるものであるという見解に至ったためである。

3 メンバーへのアンケート

3.1 はじめに

メンバーにアンケートを実施することは、メンバーのニーズを把握し、それをどの程度満たせているかを評価するうえで非常に有効な手段である。アンケートを以下のように定義する。

> 特定の集団（調査対象となる集団。つまり、調査員が特定の調査において対象とする、幅広い層の人々）の中から比較的大勢の調査対象を選出し、選出した各個人から比較的少量のデータを収集することである。[1]

アンケートは、記述的調査の一環として実施する。組織はアンケートを実施することで、特定の成果物やプログラムに対するフィードバックを受け取ったり、組織の使命や目的に対する全般的な意見を取り入れたりすることができる。また、アンケートは基本の機能とサービスを設計して実装する方法を決定する際にも活用できる。アンケートは、組織がメンバーに提供するサービスおよび機能に関する意見を収集するためだけに限らず、ISAO のあらゆる側面で有益なものとなる。

メンバーへのアンケートはいくつかの方法で実施でき、公式に行うことも非公式に行うこともできる。アンケートの実施は、何がうまくいっていて何がうまくいっていないのかを調べるために、各メンバーと話すくらいの簡単なものでもかまわない。メンバーへのアンケートを実施する際、自分たちにとって最適な既成の手法を用いるか、独自に開発した手法を用いるかは、組織の自由である。ただし、アンケートの実施を選ぶ際に、いくつか留意すべき事項がある。

1 つ目は、アンケートによって達成したいことを把握しておくことである。アンケートの目的に対して明確なビジョンを示す必要があり、そのためには、メンバーから集めようとしている情報や知識を明確に定義する必要がある。アンケートの質問は、回答者から情報を引き出せるよう具体的に設定する必要がある。アンケートの結果に基づきどのような議論が行われるかを理解しておくことも重要である。また、質問の設計と言葉づかいによっては回答に偏りが生じることがあるため、注意すること。

2 つ目は、アンケートの対象者を特定することである。物理的セキュリティの専門家にサイバーセキュリティの高度な問題について尋ねても、おそらく有益な意見は得られない。同様に、管理職のみにアンケートを実施しても、メンバー全体にアンケートを実施したときと同じ結果とはならない。特定のトピックに対する意見を求めるのに適切なコミュニティーを把握することで、有用で価値のある回答を得ることができる。

3 つ目は、アンケートを作成する際に、回答を得ようとしている各質問を全体にわたって十分に把握していることである。適切なデータを収集するには、具体的な質問を設計する必要がある。質問の言葉づかい、順番、構成、およびアンケート全体の流れは、

---

[1] Kelley, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research.*International Journal for Quality in Health Care*.June 2003; 15(3): 261-6.

回答に大きな影響をもたらす場合がある。

最後に、回答者への連絡手段を把握することが重要になる。アンケート手法にはいくつか種類があり、電話でのやり取り、オンラインアンケート、対面でのやり取りなどが挙げられる。ISAO メンバーの好みに基づき、最適な回答が得られる手法を使用する。各種アンケート手法の詳細については、後続のセクションで説明する。アンケートを設計する際に以上のことを念頭においておかないと、回答に偏りが生じたり、価値のないものになったりしてしまう場合がある。

3.1.1 メリット

ISAO がメンバーにアンケートを実施する理由として、次のメリットが挙げられる。

- 短時間で準備できる。
- 実世界の調査に基づいたデータを得られる。[2]
- 大規模な集団の意見が反映されたデータを得られる。[3]
- 短期間で大量のデータを得られる。[4]
- メンバーが ISAO に関与できる仕組みを提供する。
- メンバーが有意義な意見を提示できる仕組みを提供する。

3.1.2 デメリット

アンケートの実施におけるデメリットは次のとおりである。

- 時間がかかる場合がある。
- データの有意性が回答率に左右される。
- 質問が特定の対象範囲に絞られすぎている場合、データの有意性に影響が出かねない。[5]
- 調査対象のトピックに対してデータが詳細に欠ける恐れがある。[6]
- アンケートへの参加が容易ではない。

3.2 アンケート手法

適切なデータを取り込むには、手法を ISAO メンバーのニーズを最も満たすものにすればよい。新しい ISAO にとって、この過程は非常に簡単でありながら、非常に価値のある情報を提供する。設計できるアンケート手法にはいくつかの種類がある。以下のセクションでは、それらの手法をいくつか説明する。特定の手法を選択する過程では、他にも考慮すべき要素がある。上述のように、アンケート設計のいくつかの要素は、アンケートの結果に直接影響を及ぼす。公式または非公式なアンケートであるかどうかを問わず、アンケートの設計時には 3 つの原則である、「言葉づかいの原則」、「調査範囲

---

[2] 同書
[3] 同書
[4] 同書
[5] 同書
[6] 同書

の原則」、そして「全体的な設計」を念頭に置いておく。[7] これらの原則を適用する重要なメリットの 1 つとして、偏りを最小限にとどめられることが挙げられる。アンケートの手法と設計が完成したら、次の 11 個の要素を考慮に入れて具体的な質問の作成を開始する。[8]

- 質問の言い回しや言葉づかい
- 自由回答形式の質問または選択回答形式の質問
- 肯定的な質問、否定的な質問
- 二重質問
- あいまいな質問
- 記憶に依存する質問
- 誘導質問
- 前提を含んだ質問
- 社会的に望ましい質問
- 質問の長さ
- 質問の順序

注：上記に記載しているメリットとデメリットに加え、アンケート手法によっては、個別のメリットやデメリットがある場合もある。

3.2.1 郵送アンケート

一般的に、答えを出すべき具体的な質問がある場合や、注目している要素に対する既知の評価基準がある場合は、用紙を用いて実施するのが最適である。[9] 用紙を用いたアンケートの実施には、郵送、電話、Web ベースなどさまざまな方法がある。 郵送アンケートのデメリットとしては、Web ベースのアンケートより費用がかかる傾向にあることや、若者や移動中の人々からの回答率が低いことなどが挙げられる。[10] しかし、郵送アンケートは、電話や Web によるアンケートと比較して高い回答率を得られる。[11]

3.2.2 Web ベースのアンケート/電子アンケート

メンバーにアンケートを実施する際の最も分かりやすい方法は、アンケート Web サイトを使用してアンケートを作成することである。この手法では、組織はメンバーまたはパートナーから回答を得たい具体的な質問事項を特定し、オンラインのアンケート機能に掲載する。この手法のメリットは、組織は特定の人々、あるいは大勢の人々にアンケートを電子送信できること、アンケートにかかる費用が非常に安く管理が容易であること、すぐに配信できること、すべての回答が確認と分析のために 1 か所に集約しやすいことが挙げられる。[12] Web ベースのアンケートの最大のメリットは、多くの場合、メンバー

---

[7] Sekaran, U., & Bougie, R. (2010). Research Methods for Business: A Skill-Building Approach.Chichester, West Sussex, U.K., Wiley.
[8] 同書
[9] 同書
[10] de Leeuw, Edith, & Toepoel, Vera (2017). *Mixed-Mode and Mixed-Device Surveys*, 51–61. 10.1007/978-3-319-54395-6_8.
[11] 同書
[12] Sekaran & Bougie, 2010.

が簡単に参加しやすく、匿名で回答を送信できるため率直な意見を述べやすいことである。デメリットは、インターネットへアクセスする機会が回答者層によって異なることにより、対象者が不足したり、回答率が低くなったりする恐れがあることである。[13] Web ベースのアンケートツールの例としては、Survey Monkey、SurveyGizmo、Google Forms、Typeform、SurveyLegend、Polldaddy などが挙げられる。（注：これらのサービスを推奨するものではない。）

3.2.3 電話インタビュー

メンバーへのアンケートを実施する別の方法として、電話による一対一の個別通話がある。電話アンケートは柔軟性があり費用対効果が高く、最も有益な情報を得られる可能性がある。[14] アンケート実施時はすべてのメンバーに同じ質問を尋ねることが重要であるが、一対一の会話により、組織は特定のトピックについてより詳しい意見を引き出すことが可能になる。このような詳細情報によって有益な背景情報やアイディアを追加で得ることができ、メンバーのニーズへの理解を深めることができる。また、個人への連絡は、メンバーとの関係を築く絶好の機会にもなる。電話アンケートは、コンピュータ支援型電話インタビュー（CATIs）を使用して実施でき、使用も管理も簡単である。[15] CATIs を使用するもう 1 つのメリットは、インタビューでより正確なデータを収集でき、分析が速いことである。デメリットとしては、言語外の回答者の様子を汲み取れない点や、インタビューを短時間に抑える必要がある点などが挙げられる。[16] また、なるべく対象者の携帯電話へ連絡するようにして回答率をあげるよう努力しているにもかかわらず、電話アンケートの回答率は史上最低の水準となっている。[17]

3.2.4 オンライン Web セミナー

メンバーへのアンケートを実施する 3 つ目の手法は、一般的な Web セミナーやグループ通話である。この手法では、メンバーは他のメンバーとともに通話や Web セミナーに参加するよう招待され、そこでアンケートの質問に回答する。アンケートは各オンライン Web セミナーの最後に組み込むこともできる。この手法では、個別に電話を掛ける必要がないため時間を節約できるというメリットがある反面、メンバーは他の通話メンバーの手前、率直に意見を述べにくい場合があり、フィードバックを得る効果が薄まる恐れがある。同様に、1 社または 1 名だけが話し続けることがあり、通話での議論の場が支配され、意見が偏ってしまう恐れがある。しかし、共通の通話で複数のメンバーにアンケートの内容を議論させることで、個々のアイディアをグループ内で掘り下げることができ、効果的な「ブレインストーミング」の場となり得る。

---

[13] de Leeuw & Toepoel, 2017.
[14] 同書
[15] Sekaran & Bougie, 2010.
[16] 同書
[17] de Leeuw & Toepoel, 2017.

3.2.5 対面インタビュー

もう 1 つのアンケート手法は、ISAO が実施する対面インタビューである。この手のインタビューは、構造化インタビューにも非構造化インタビューにもできる。非構造化インタビューでは、あらかじめ質問の順序が決められていない。非構造化インタビューの例には、メンバーとコーヒーを片手に話し合うことも含まれる。 構造化インタビューでは、集めたいデータまたは情報が事前に分かっており、あらかじめ定義された質問が用意されている。[18] 対面インタビューには、ISAO が、ISAO のオフィス、メンバーのオフィス、あるいは別の場所で実施するインタビューを含む。

この手法のメリットは、ISAO が個々のメンバーにアンケートの目的を説明できるため、他の手法よりも回答率が高いことである。[19] なお、対面インタビューの実施を決定する前に、メリットとデメリットを検討しておくことが必要である。 対面インタビューの最大のメリットは、インタビュアーが、言語外の回答者の様子やボディランゲージを汲み取れることである。これにより、回答者が質問を理解しているかどうかが分かる。また、対面インタビューでは、回答者が質問者に、理解できなかった質問を確認することもできる。[20] 対面インタビューにはいくつかのデメリットがあり、時間がかかること、地理的な制約があること、インタビュアーの先入観によって回答の解釈に影響が出ること、インタビュアーのトレーニングに費用がかかることなどが挙げられる。[21]

（アンケートのサンプルについては、付録 A を参照。）

[18] Sekaran & Bougie, 2010.
[19] Kelley et al., 2003.
[20] Sekaran & Bougie, 2010.
[21] 同書

3.3 この章のまとめ

アンケートは、ISAO が短時間で大量のデータを集めることができる強力な手段となり得る。集めた情報は、ISAO の成果物とサービスがメンバーにどのように評価されているかの理解を助け、ISAO の今後の方向性を決める際や、メンバーが ISAO に積極的に参加できる機会を提供する際に活用できる。各アンケート手法には独自のメリットとデメリットがある。調査は、メンバーとコーヒーを飲みながら会話することや、メンバーリストに電子メールを送信することから始めてもかまわない。使用するアンケート手法を選ぶ際は、特定のアンケート手法の実施における課題、制約、予想される結果、メリットを考慮することが重要である。先に述べたとおり、この章の内容は ISAO がメンバーへのアンケートに使用できるいくつのアイディアと手法を示すものであり、組織は役立つ手法を自由に採用できる。ほとんどの取り組みと同じで、組織がメンバーとのやり取りに最適な方法を見つけるには、ある程度の試行錯誤が必要となる。

4 情報収集

4.1 説明

本章の目的は、サイバー脅威情報（CTI）やメンバーが重要とみなす情報（物理的脅威、天候などを含む）を収集するための運用機能、技術的機能、分析機能、人的機能を、ISAO が理解できるよう支援することである。CTI について具体的に説明すると、米国国立標準技術研究所（NIST）の Special Publication（SP）800-150『Guide to Cyber Threat Information Sharing』に定義されているとおり、CTI には「検知指標、脅威アクターが使用する戦術、技術、および手順」と、組織が「サイバー脅威の識別、評価、監視、および脅威への対応」に使用できる情報が含まれる。[22] データや情報はさまざまな情報源から得ることができる。 情報源は、最初のうちは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に関するブログやホワイトペーパー、他の ISAO や情報共有分析センター（ISAC）、政府の関係者や報告書などの各所で公開されているレポートから収集するのでも、ISAO メンバーから直接取得するのでもかまわない。CTI などのデータセットを収集することは、ISAO が実施できる重要なサービスおよび機能の 1 つである。NIST によれば、組織はサイバー脅威情報を収集、生成、または格納するためのさまざまなツール、センサー、リポジトリを選択することもできる。[23]

4.2 メリット

- 公開、非公開を含め、情報源は多数存在する。
- サイバーセキュリティベンダーやブログといった外部の情報源から情報を収集することで、既存の内部情報を拡充し、ISAO にとってより使える情報を展開することができる。 [24]
- 情報源を一元化して提供することで、情報収集におけるメンバー間での重複作業を最小限に抑え、メンバーのコストを削減できる。
- このサービスおよび機能では、複数の情報源から情報収集するため、ISAO は脅威の情勢をより深く理解できる。
- メンバーから直接情報を得た場合は、情報の信頼性が高く、検証しやすい。メンバー間での情報共有は共有の文化を醸成し、メンバーが情報共有しやすい環境をはぐくむ。

4.3 課題

- 製品やデータソースが多岐に渡る。
- オープンソースのフィードは、精査が困難であり、信頼性に疑念がある。
- 分類すべきデータが多すぎる場合がある。

---

[22] Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (October 2016). *Guide to Cyber Threat Information Sharing*. NIST. doi:https://dx.doi.org/10.6028/NIST.SP.800-150.
[23] 同書
[24] 同書

- フォールスポジティブの可能性が高い。
- 必要なデータの水準、形式、配布の頻度に応じた、人材、時間、手順、技術が必要となる場合がある。
- メンバーが使いやすい形式を採用するまで、適切な情報およびメンバーが必要とする情報を特定するまでには、時間を要したり、共有する内容の深い理解が求められたりする場合がある。
- 技術、サービス、手法にコストがかかる場合がある。

より多くの情報を収集するほど、その情報の精査、格納、分析により多くのリソースが必要となる。

4.4 情報源と手法

データ収集の情報源と手法には実にさまざまなものがあるため、新しい ISAO は途方にくれてしまうかもしれない。このような問題を解決するために考えられるアプローチとしては、まずは簡単なことから始め、情報源と手法を 2、3 個に限って選ぶことである。それらの準備が整い、必要とする価値がその情報によってもたらされることを確認して初めて、追加の情報源や手法を検討すべきである。このセクションでは、情報源の精査方法について取り上げ、情報収集の方法を記載する。

4.4.1 情報源

データソースやニュースメディアのフィードは、内部または外部の情報源から得られる。最初に、どのような情報が重要であるかを定義する。次に、メンバーがどういった情報を誰とであれば共有したいと思うのか、どういった情報であれば合法的に共有できるのかを定義し、そうした情報が含まれているシステムや情報源を特定する。さまざまな情報源から情報収集することで、すぐに高次な情報共有を行うことができるようになる。

4.4.2 フォーマット

検知指標/インディケータを共有するための「標準化された」フォーマットは何種類か存在する。付録 C にこれらのフォーマットの一覧を掲載している。メンバーにとって何が最も効果的かに応じて、ISAO はこれらのフォーマットを完全または部分的に取り入れたり、まったく採用しないという判断を下してもよい。

4.4.3 収集方法

データ収集にはさまざまな手法がある。ISAO の成熟度によっては、これらの手法のいくつかは高度であり、基本となる機能が確立されてから検討した方がよい場合がある。ここでは一般的な高度であったり、特殊な手法も取り上げているが、これらの手法を計画段階の早い時期に把握しておくことで、ISAO を戦略的に成長させる助けになる可能性がある。これらの手法は次のとおりである。

- 以下のような、ベンダー、フィード、ISAO、ISAC、または政府からのレポート。

  o 内部の情報源（電子）

o アナリスト（内部または外部）

o 電子メール

- 以下を使用した関連テキストの構文解析。

  o 人手

  o スクリプト

  o Web スパイダーまたはクローラ

  o マルチメディアの取り込みとインデックス付け

  o OCR スキャン

4.4.4 情報源の精査と検証

ISAO のメンバーが受け取る情報、警告、通知が信頼に足るものであることは非常に重要である。つまり、正しい情報を受け取れなければ、正しい対応もできない。前述のように、メンバーから情報を得ることやメンバー間で情報交換することで、ISAO 内で情報の信頼性を担保することができる。その工程において、情報の精査と検証は重要である。それには、ISAO による手法、手段、情報源の精査が不可欠である。情報源が疑わしかったり、データが当てにならないものだと発覚したりすると、ISAO が共有する情報に少なからぬ疑念が生じてしまう場合がある。ISAO には、使用する情報源（パートナー組織を含む）の評価や精査を行うことを強く推奨する。この章では、データソースを精査する方法と、収集した情報の完全性と確度を担保する方法について記述する。

ISAO が新しい情報源のデータを精査する際は、メンバーとの関連性、情報源の信頼性、データの背景の理解、情報源を検証する能力について考慮が必要である。基礎段階の情報源の精査と検証では、著名なグループや個人に連絡し、一緒に検証することもある。

- オープンソースのデータフィードを精査するための最初の方法の 1 つは、他の ISAC や ISAO に尋ねることである。
- 収集した情報から不適切な情報を取り除く工程と標準手順を作成する。
- 別の組織から情報を収集することを検討している場合、データ共有に関する合意、覚書、秘密保持契約（NDA）を締結するのが賢明である。

4.5 収集後のステップ

NIST などの組織では、データ収集の手順についての手引きを作成している。NIST SP 800-150 では、外部フィードから得た検知指標の使用方法が提供されている。基本的な工程だけでなく、その他の応用的な工程についても記述されており、ISAO はそれらの実装を検討できる。ISAO はこれらの工程によって、収集、分析、配布するデータの取り扱いのワークフローを細分化できる。

4.6 収集ツールとリソース

ISAO が使用できるツールとリソースは多岐に渡る。完全に無料で使用できるツールもあれば、一括払いを必要とするものや、定期支払い（月額または年額）を必要とするものもある。付録 C にはツールとリソースの一覧を掲載しているが、この一覧は網羅性を保証するものではなく、これらの製品を公認するものでもない。この一覧は、一部のツールとリソースを例示し、ISAO の検討を補助するものである。

4.7 この章のまとめ

先に述べたように、情報収集の工程は、ISAO が実施する有用なサービスおよび機能の 1 つである。このサービスは、組織の核となるサービスとして、慎重に計画し実装されるべきである。新しい ISAO や設立したばかりの ISAO にとっては、手法、ツール、情報源を限定した方がよい場合がある。最初から手法、ツール、情報源が多すぎると、工程が複雑になり、ISAO が提供する情報の質を損なう場合がある。手法、ツール、情報源を限定してから開始し、広く知られていて信頼できる 2、3 の情報源から情報を収集することに注力することが重要である。ただし、ISAO がノウハウや専門知識を有するようになれば、幅広い情報源から情報を取り込んで使いこなすことができる。また、ISAO は、ベストプラクティスや他のサイバー関連情報を共有する運用に留め、自身では情報を保管せず、受け渡すだけにすることもできる。

5 情報分析

5.1 はじめに

脅威情報の分析は、最も基本的なレベルに限定しても、方法が多岐に渡る。この工程では、データセットの分析にシステムやツールを使用することも、人手で行うこともできる。最も基本的なレベルの分析作業は、ISAO のメンバーにどの情報を共有するかを決める、といった単純なものでもよい。新しい ISAO や設立したばかりの ISAO の場合、あるマルウェアがどの程度、システムを破壊する可能性があるかを判断するような高度な分析工程を盛り込む必要はない。この章では、基本のサービスおよび機能についてはあまり掘り下げない。詳しい情報については、ISAO 700-1 の『分析入門』を参照のこと。本文書の目的は、情報分析について ISAO へ紹介し、情報分析ができる ISAO を作り上げていくための基本的な知識をメンバーへ提供することである。本文書では、基本要件の策定、基本要件に対する適切なデータの収集、データの処理と活用、結果の分析、分析結果を内外へ共有する際の土台となる成果物の作成といった、分析工程の概念的なフレームワークを確立する。

情報分析については、いくつか留意しておくべき側面がある。まず、この工程は手間がかかり、適切に遂行するには特殊なスキルを要する場合がある。次に、ISAO はその分析工程をとおして、教訓、脅威の警告、傾向分析といった有益かつ実用的な情報をメンバーに提供できる。実用的な情報が提供できる分析工程の例としては、ISAO が複数のメンバーネットワークへの偵察行為のパターンを特定し、その結果として、すべてのメンバーに通知し、標的型攻撃キャンペーンが行われている可能性を警告して、脅威を識別する方法の手引きを提供することなどが挙げられる。ISAO がメンバーに提供できる最高の価値の 1 つは、その分析工程にあると言える。

5.2 メリット

ISAO 組織に参加することで、メンバーはデータとリソースをどちらも集積することができ、アナリストは確認できる情報の量が増え、脅威の情勢を幅広く把握できるようになる。基本的なレベルでは、ISAO は、メンバーが一般的な問題や傾向について議論したり確認したりできる討論の場となる。さらに、ISAO メンバーから提供されるデータフィードが増えてくると、傾向の分析や相関分析が容易にできるようになる。最終的には、情報がどのように関連しているかの分析結果を提供されるようになると、効率的に情報認知と状況認識ができるようになる。分析をもとに得た情報は、ISAO がメンバーに提供する情報に非常に大きな価値を付加する。

5.3 課題

分析への組織的な取り組みに参加するにあたり、メンバーは数多くの困難に直面する可能性がある。人的資源の観点からすれば、有能なアナリストを養成したり雇用したりするにはコストがかかる可能性がある。また、要件やデータ量が増加していくのに伴い、単に人的な要件を追加投入していくだけの対応となる場合がある。メンバー個人においては、機密性の高いデータが漏えいすること、あるいはメンバーの組織にとって不利益な情報が暴露されることを懸念して、一部のデータセットを ISAO に提供したくない、または提供できないことがある。

5.4 この章のまとめ

ISAO がこの基本のサービスおよび機能を提供する場合、適切な方法で行うことが非常に重要となる。効果的な分析は、ISAO メンバーに適時かつ実用的な情報を提供する。しかし、分析のスキルや工程が不十分である場合、それは ISAO にとって重大なリスクとなり得る。分析工程の詳細と詳しい考察については、ISAO 700-1 の『分析入門』を参照のこと。

6 情報の配布

6.1 はじめに

配布とは、「あるもの、特に情報を、広く行き渡らせること」(Oxford Dictionaries)と定義されている。ISAO がメンバー間に価値を生み出すことができる方法の 1 つに、情報共有がある。これにより、組織はビジネスに影響を及ぼす可能性のある最新のニュースを受け取り、コミュニケーションを取ることができる。

最も基本的なレベルの情報配布として、簡単な方法がいくつかある。情報をタイムリーで適切なものにするため、ISAO はメンバーと協力し、情報共有のための具体的な仕組み、共有する情報の種類、共有する情報と共有先、そして情報配布の頻度を決定することを強く推奨する。情報共有の目的としては、迅速な対応を引き出すこと、行動の変化を促すこと、支援を依頼すること、そして特定のトピックや状況について教育することなどが考えられる。以下のセクションでは、情報共有におけるさまざまな検討事項について詳細に説明する。他のサービスおよび機能と同様に、どの手段や手法を採用するかは、ISAO メンバーのニーズを踏まえて決定する。

6.2 メリット

情報を適切に配布することには、いくつかのメリットがある。

- アラートと勧告によって、最新のアクティブなインシデント、脅威、報告された脆弱性をすぐにメンバーに知らせることができる。
- 脅威環境への理解の向上により、組織はサイバーセキュリティに関するリソースに優先順位を付けやすくなる。
- 特定のトピックを共有することで、パートナーシップの確立を促進したり、研修によりコミュニティーメンバーの知識を向上させたり、あるいはメンバーが ISAO コミュニティーの他のメンバーに支援を求めることができるようになる。

6.3 課題

情報を配布する際は、乗り越えなければならないいくつかの課題がある。

- メンバーが時間的制約を受ける成果物の価値を認めない場合がある。
- 実用的な成果物を作成するには運用に関する予備知識が必要となることがあるが、そのような知識を持つ人材の獲得、雇用、あるいは人材への投資は困難な場合がある。
- 内容を絞り込まずに情報を流すと、メンバーが情報を確認するのに疲れや負担を感じるようになり、読者が減少したり、情報の価値を損なう場合がある。
- 必要なデータのレベル、形式、配布の頻度に応じた、人材、時間、手順、技術が必要となる場合がある。
- 情報が再配布される際もセキュリティと統制を維持しなければならない。
- 特に緊急で情報共有を行う場合には、配布情報の作成、管理、維持にかかる費用がかさみ、多くの努力を求められ、高度なことを要求される場合がある。

6.4 実装のガイドライン

6.4.1 配布の手法

技術的な仕組みをさほど持たずとも、ISAO がメンバーへの情報配布に使用できる情報共有手法は何種類かある。

- 電話
- 電子メール（ブロードキャストまたはメーリングリストサービス）
- 対面
- Web サイト

各手法には個別のメリットとデメリットがある。ISAO が導入できる手法は 1 種類に限定されない。特に運用の継続性のためにも、予備の手法を用意してくことを推奨する。

6.4.2 配布するコンテンツ

ISAO がメンバーに配布できるコンテンツにはいくつかの種類がある。良質で有意義なコンテンツを配布することで、ISAO メンバーに最大の価値をもたらすことができる。各種のコンテンツには以下のものがある。

- アラートや勧告
- 定期的な出版物
- 定期的なレポート
- 支援や情報のリクエスト
- ISAO メンバーへの教育、研修、啓発
    - o Web キャスト
    - o オンサイト/対面
    - o オンライン資料

配布手法と同様に、各形式にも個別のメリットとデメリットがある。ただし、どの形式を選択するにしても、共有情報がスパムまがいのものになってしまったり、読者がアラート疲れを起こさないように留意する必要がある。アラート疲れの対策方法の 1 つは、情報の影響度、緊急度、重要度を決め、メンバーに配布する情報の等級を事前に伝えておくことである。戦略の 1 つとして検討すべきものは、プッシュプルを用いた手法である。例えば、迅速な対応を必要とする項目については、電子メールやアラート通知で情報をプッシュする。情報提供のみを目的とする項目については、その情報を共有ドライブ、Web サイト、または共通しているエリアに公開し、メンバーが都合のよいときにプルできるようにする。別の戦略としては、共有される情報の緊急度をメンバーが把握できるよう、電子メールにラベルを付けるシステムを開発することが挙げられる。

6.4.3 配布の形式

理解しやすい形式で情報を提供すると、ISAO メンバーに最大の価値をもたらすことができる。形式に関する考慮事項を以下に記載する。

- 情報の概要
- 緊急度と重大度の定義
- 推奨される対応策とベストプラクティス

6.4.4 方針に関する検討事項

情報の格納、処理、共有の方法に関する詳細な方針を策定することは、信頼を得るために不可欠である。このような方針においては、ISAO は以下の点を検討する。

- 暗号化
- 保管/保持期間
- 頻度
- 情報処理と共有のためのトラフィックライトプロトコル（TLP）の使用や、情報分類のためのその他のシステムの使用

6.5 この章のまとめ

この機能とサービスを構築する際は、考慮すべき重要な点がいくつかある。まず、収集や分析と同じように、情報を配布するためのツールと手段は多岐に渡る。ISAO メンバーに情報を配布するには、2、3 個の簡単な手段から始めることが重要である。2 つ目に、情報が、その戦術的および戦略的価値にふさわしい速度と頻度で配布されるようにする。3 つ目に、情報はタイムリーなものであるだけでなく、有用なものである必要がある。4 つ目に、情報の形式に一貫性があること、専門性に基づき書かれた情報であること、そして適切な読者を対象とした資料であることが重要である。最後に、情報の機密性、その処理方法、受け取り側の保持期間を考慮することが重要である。

7 メンバーによる情報共有の促進

出版物 100-2（付録 A）で定義しているとおり、メンバーによる情報共有の促進とは、属性表明の有無を問わず、メンバーが互いに、また ISAO と情報を共有できるようにする過程のことである。つまり、このサービスおよび機能における ISAO の最も重要な成果は、メンバー間での信頼関係を促進して維持することである。ISAO 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、信頼の構築は容易である。本章では、ISAO がメンバー間での共有を促進するための基本原則について取り上げる。

7.1 メリット

先に述べたように、ISAO はメンバーによる情報共有を促進することで、さまざまなメリットが得られる。ISAO は、メンバーがサイバー脅威情報やその他の機密情報となり得るデータを共有するための、信頼できる中立的な媒介となる。

7.2 課題

他の基本のサービスおよび機能と同様に、ISAO はこのサービスおよび機能を運用可能にする際も課題に直面する可能性がある。最初の課題は、信頼できる環境を構築することである。設立したばかりの ISAO では、コミュニティー内のメンバーはお互いをよく知らない場合があるため、この課題は特に困難なものになる。2 つ目の課題は、必要に応じてセキュアな環境を構築することである。セキュアな環境の構築に必要となる工程と技術にはコストがかかるが、設立したばかりの ISAO の場合は資金が限られている場合も多いであろう。3 つ目の課題は、匿名化できるような環境を整えることであるが、これもコストがかかる。4 つ目の課題は、メンバーの一部が信頼を損なった場合にどうするかということである。メンバー間で信頼を築くにはかなりの時間を要するが、失うのは一瞬である。最後に、情報共有や参加してくれるメンバーを集めること自体も課題となる。メンバーが参加したくないと感じる理由は多岐に渡る。共有の工程が複雑すぎるという理由、メンバーが情報共有の価値を見いだせないという理由だけでなく、ただ気遣いに欠けるだけということもあり得る。

7.3 メンバー間での情報共有を促進するための手法

ISAO がメンバー間での情報共有を促進するには、いくつかの簡単な手法がある。当該の基本のサービスまたは機能に対応する技術の多くは、コストのかかるものではない。最初はクラウドなどのオンラインサービスを使用すれば、コストを節約できるだけでなく、ISAO がこれらのサービスおよび機能を提供するための準備時間も短縮できる。

- メーリングリストサービスの作成は、設立したばかりの ISAO がこのサービスおよび機能を導入するのに手早くて手軽なアプローチである。
- 共有時のプロトコルを新たに作成したり、TLP のような既存のプロトコルを使用したりすることは、メンバーから情報共有への同意を得るための手軽な方法である。
- NDA のような文書を締結すると、誰にとっても非常に分かりやすく、信頼を生むのに役立つ。

- ISAO とメンバーとの間で必ず覚書（MOU）を交わすと、参考となる場合がある。MOU とは、活動の意図を概説する文書である。法的拘束力を持つ文書である必要はないが、期待する事項を定義しておくのに役立つ場合がある。
- 情報共有には、メンバー全体の状況認識が強化されるというメリットがあることを周知することで、リスクに基づいた意思決定の助けとなる場合がある。
- メンバーと連絡を取れるチャネルを複数用意しておくと役立つ可能性がある。例えば、週次または月次のニュースレターの作成や、月次または四半期ごとの説明会の開催などが挙げられる。説明会には、各メンバーのオフィスを持ち回りで利用することを検討するのもよいだろう。

7.4 この章のまとめ

ISAO が、メンバーの交流をいかに支援、奨励、推進できるかで、その ISAO の成功度合いが決まる。すべての技術が整い、設計どおりに実行される状況下では、そのプログラムの成功は ISAO メンバーの関与次第である。ISAO のリーダーとスタッフ（存在する場合）は、メンバーと密にコミュニケーションを取る必要がある。このような交流により、メンバーが継続的に参加してくれるようになる。また、ISAO とメンバーとの間だけでなく、メンバー間で信頼関係を築き、維持することにもつながる。

付録 A. アンケートの例

アンケート例 1

このアンケートで得た情報は、今後のイベントの向上のために使用いたします。

1) **ISAO への全体的な満足度はどの程度ですか:**
☐ 非常に満足 ☐満足 ☐ やや満足 ☐ どちらともいえない ☐ 不満

2) **ISAO が提供する情報はどのくらい役立ちましたか:**
自宅: ☐ 非常に役立った ☐役立った ☐ やや役立った ☐ どちらともいえない ☐ 役立たなかった
職場: ☐ 非常に役立った ☐役立った ☐ やや役立った ☐ どちらともいえない ☐ 役立たなかった

3) **ISAO のサービスを全体的に評価してください:**
☐ 1 ☐2 ☐ 3 ☐ 4 ☐ 5

4) **ISAO が提供する情報はどのくらい実用的ですか:**
☐ 非常に実用的 ☐実用的 ☐ やや実用的 ☐ あまり実用的でない ☐ まったく実用的でない

5) **情報は適時に配布されていますか:**
☐ はい ☐ いいえ

6) **法人ですか** **あるいは 個人ですか**
a. 法人の場合は、業界を教えてください: ☐金融 ☐ 教育 ☐ IT ☐ 製造
☐ 政府 ☐ 医療 ☐ その他_____
b. 会社の規模 ☐小規模(50 人以下) ☐中規模(51～249 人) ☐ 大規模(250 人以上)

7) **情報を受け取る手段として好ましいものはどれですか:**
☐ Twitter ☐ 友人 ☐Web サイト:_____
☐ Facebook ☐ LinkedIn ☐ その他:_____

以下の手段を評価してください:

Twitter	☐非常に良い	☐ 良い	☐ やや良い	☐ 普通	☐ 悪い
電子メール	☐非常に良い	☐ 良い	☐ やや良い	☐ 普通	☐ 悪い
自動通知	☐非常に良い	☐ 良い	☐ やや良い	☐ 普通	☐ 悪い
Web アラート	☐非常に良い	☐ 良い	☐ やや良い	☐ 普通	☐ 悪い

Cybersecurity News & Alerts への登録に興味がありますか？ 以下に連絡先情報をご記入ください。

名前:_____

電子メール:_____

コメントや提案があればご記入ください:

_____

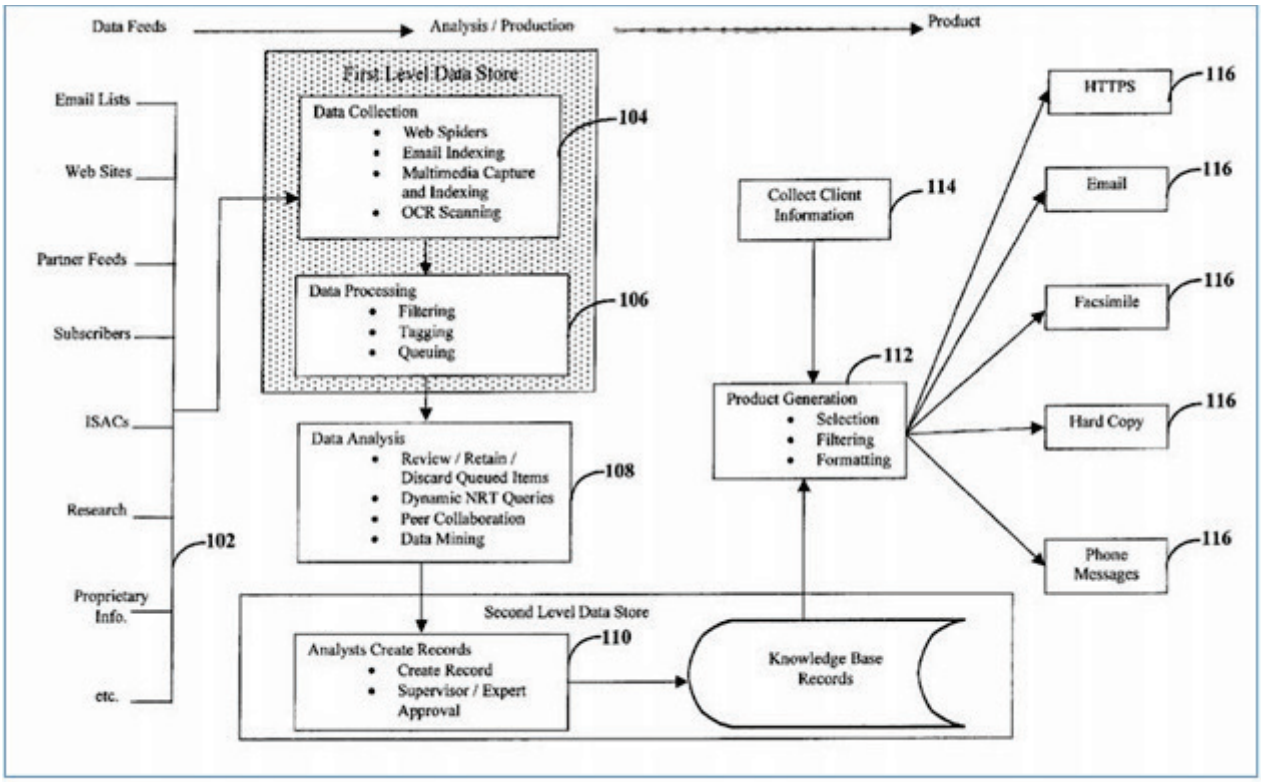
_____

_____

付録 B 情報収集と分析のためのシステムと手法の例

図 B-1 に示されている情報収集と分析のためのシステムと手法は、これらの工程を表したモデルの可能性の 1 つにすぎない。

図 B-1.情報収集と分析のためのシステムと手法



出典:U.S. Patent No. US 2002/0038430 A1, 2002

付録 C. 標準化フォーマット

表 C-1.標準化フォーマット一覧

フォーマット	説明
CAPEC	CAPEC™（Common Attack Pattern Enumeration and Classification：共通攻撃パターン一覧）の取り組みでは、共通攻撃パターンを直観的な方法で分類したカタログを、各パターンに属する攻撃について説明し、それらの情報を共有するための包括的な概要とともに、公的に入手可能な形で提供することを目標としている（https://capec.mitre.org/about/index.html）。
CybOX	CybOX™（Cyber Observable eXpression：サイバー攻撃観測記述形式）は、サイバー攻撃の観測事象に関する確度の高い情報を変換して通信するための標準言語である（http://cyboxproject.github.io/about/）。
IODEF（RFC5070）	IODEF（Incident Object Description Exchange Format：インシデントオブジェクト記述法と交換フォーマット）は、コンピュータセキュリティインシデント対応チーム間で通常交換されるコンピュータセキュリティインシデントに関する情報を共有する際の枠組みとなるデータの表現方法を定義する。（http://cyboxproject.github.io/about/）。
IDMEF（RFC4765）	*Experimental*。IDMEF（Intrusion Detection Message Exchange Format：侵入検知メッセージ交換フォーマット）の目的は、侵入検知システムと応答システム、およびそれらと連携する管理システムに、対象となる情報を共有するためのデータ形式と交換プロシージャを定義することである（https://tools.ietf.org/html/rfc4765）。
MAEC	MAEC™（Malware Attribute Enumeration and Characterization：マルウェア特徴属性一覧）（発音は「マイク」）は、マルウェアの振る舞い、痕跡、攻撃パターンなどの属性に基づいたマルウェアに関する確度の高い情報を変換して通信するために、コミュニティーにより開発された構造化言語である（http://maecproject.github.io/about-maec/）。
STIX	STIX™（Structured Threat Information Expression：脅威情報構造化記述形式）はサイバー脅威情報を記述するための構造化言語であり、これを用いることでサイバー脅威情報を一貫性のある方法で共有、保管、分析できるようになる（http://stix-project.github.io/about/）。
TAXII	TAXII™（Trusted Automated eXchange of Indicator Information：検知指標情報自動交換手順）は、サイバー脅威情報の自動交換手順を標準化するための、自由に情報をやり取りできる仕組みである（http://taxiipro- ject.github.io/about/）。
VERIS	VERIS（Vocabulary for Event Recording and Incident Sharing：イベント記録とインシデント共有のための言語）は、セキュリティインシデントを体系的かつ再現可能な方法で記述するために共通の言語を提供する目的で定められた一連の基準である。VERIS は、セキュリティ業界における最も重大かつ継続的な課題の 1 つである、有用な情報の欠如に対応するものである（http://veriscommunity.net/index.html）。