ISAO
Standards Organization

ISAO 700-1:
分析入門

v1.0

2018 年 6 月 18 日

ISAO 700-1

分析入門

V1.0

ISAO Standards Organization

2018 年 6 月 18 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
Dr. Gregory B. White
ISAO SO–Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Allen Shreffler
ISAO SO–Deputy Director
LMI

Tommy McDowell
Senior Director
Retail Cyber Intelligence Sharing Center

*ワーキンググループ **7–ISAO** の分析*

David Sula
Signal Processing Engineer
Leidos

Ole Villadsen
Research Liaison, Cybersecurity & Information Systems
Carnegie Mellon University Libraries

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。

Richard Barger（Director of Security Research Security Markets、Splunk Inc）、Tyler Bent（Member Engagement & Programs Coordinator、IT-ISAC）、Joy Gumz（Senior Director、Project Auditors LLC）、Pierre Lamy（Threat Intelligence Lead、S&P Global）、Larry Portouw（NTK Consulting、LLC）、David Sula（Signal Processing Engineer、Leidos）、Ole Villadsen（Research Liaison、Cybersecurity & Information Systems、Carnegie Mellon
University Libraries）。

また、本文書の作成において多大なる支援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。Marlis C. Cook（Director of Lifecycle Standards Development）および Allen D. Shreffler（Deputy Director）。

本資料は、No. 2015 - PD - 128 - 000001 の裁定による米国国土安全保障省の支援を受けた取り組みに基づいている。

免責：「本文書に記載の見解および結論は共著者一同によるものであり、明示的か黙示的かを問わず、必ずしも米国国土安全保障省の公式な方針を表すものではない。」

目次

図

表

改訂履歴

項番	バージョン	説明	日付
1	1.0	初版	2018/06/18

1 エグゼクティブサマリー

分析の目的は、分析結果を関連付けてインテリジェンスを生成し、意思決定時の不確実性を軽減して、リスクを軽減することにある。本文書では、情報分析の工程の概要と、情報共有分析機関（ISAO）がそれを活用してサイバーセキュリティ脅威を特定、定義、緩和するための方法について説明する。共著者一同は、分析チームがサイバーセキュリティ情報とインテリジェンスを作成するのに必要なツールと工程についての、一般的な認識を組織に対して提示することを目的としている。

本文書は、情報とインテリジェンスの要件の策定、および ISAO メンバーにサイバーセキュリティの状況認識を提供できる成果物を作成するのに適切なデータの収集、処理、分析、活用といった、分析工程の概念的フレームワークを確立する。サイバーセキュリティの分析を共有する目的は、ISAO に実用的な情報を提供し、不確実性を軽減して、意思決定者のリスクを軽減できるようにすることである。技術面の概要として、本文書は、管理段階と運用段階での意思決定を促進することを目的としている。

2 はじめに

分析とは継続的な工程であり、サイバーセキュリティの状況を把握するうえで極めて重要である。分析の基本は、現在の状況を知ること、自分自身（事業/組織）を知ること、そして攻撃者または犯罪者の視点を持つことである。データや情報の内容やそれ自体がもたらす価値は小さいが、導き出された分析結果と理解は、意思決定者が必要とする背景情報、つまり行動につながるインテリジェンスを提供する。分析は陳腐化しやすいスキルであり、技能と体系立った方法を組み合わせたものである。そのためサイバーセキュリティの最新状況を把握し続けるためには、常に学び続けなければならない。本文書は、ISAO 300-1『情報共有入門』を発展させたものであり、ISAO に分析を導入する理由と方法について説明する。

3 業務への影響

現代のビジネスでは、世界市場で取引を行うために何らかのデジタル通信が必要である。組織の事業計画および顧客との間で通信するデータの重大性を考慮する必要もある。情報化時代が成熟するにつれて、ビジネス全体でセキュリティの優先度が高まっている。

『2017 IDG Security Priorities Study』[1]によると、調査対象とした組織の 42%が今後 12 か月間においてセキュリティ予算の増加を見込んでいる。持続的ビジネスにおける影響評価の一環として脅威情報の分析に積極的に取り組んでいる成熟した組織は、自身の形式的および文化的な立場を特定して、デジタルリスクの視点を織り込んだビジネス上の意思決定を定期的に行っている。

同じく 2017 IDG の調査によると、調査対象とした組織の 28%が、セキュリティ投資の一環でビッグデータ分析に新規に投資する、あるいは投資する可能性があると答えている。

[1] https://www.idg.com/tools-for-marketers/2017-security-priorities-survey を参照。

組織は多くの場合、コストに見合う、またはビジネスの収益増加に貢献するサイバーセキュリティ対策を探し続けている。この先 10 年、セキュリティ対策における目には見えない価値と、セキュリティ対策のコストを打ち消し、ビジネスを成功に導くデータの目には見えない価値を活用できる機会が存在する。

組織のサイバーセキュリティの向上を模索するビジネスリーダーは、往々にして、情報保証（IA）チームと協力し、社内の戦略的、運用的、戦術的情報技術（IT）プログラムを社外のイベントやビジネス活動に整合させることで、より幅広い状況認識を得たり、リスク管理工程を組織に伝達したりしている。たとえば、合併や買収においては、IA チームは、機密情報を漏えいさせる可能性のあるインサイダーの脅威を検知する役割を担うことがある。あるいは、ネットワークに繰り返しアクセスし、ネットワーク移行時に組織の煩雑な処理の抜け穴を悪用して組織の事業計画にアクセスするリモート攻撃を試みる者を見つけだすことに注力する場合もある。

3.1 人的資源のプール

最近のデジタルリスクの動的な性質と複雑性は、技術分野だけでなく、地理・社会・政治の分野もあわせた専門知識を必要とすることが多い。組織のリスクを減らす責務を担う個々の貢献者やセキュリティチームが短時間で知るべきこと、やるべきことは、あまりにも多い。

幸いにも、このように人的資源に制約があることは、個々の貢献者とセキュリティチームをまとめ上げるきっかけとなり、その結果、作業成果物の品質を、その断片を組み合わせたもの以上にすることができる。やる気に満ち、マトリクス型組織で、職務の枠を超えたチームの活用を模索している組織は、ステークホルダー間で共通のセキュリティ計画を推進することで、組織的に大きな成功を収める体制を整えている。

人的資源を組織内にプールしておく戦略は、ISAO、セキュリティ製品のユーザーグループ、あるいは民間のセキュリティ研究者で構成される信頼できるグループなどの協力機関に参加することで、組織外にも拡張できる。同一の業界にあるさまざまな組織の担う責務や、分析するリスクが重複していることは、ビジネス的にいえばもったいないことである。個人のグループや組織は、分散処理の効果を手本に、分析の共通課題を分解して、共有のワークフローに落とし込むことができる。また、共通の脅威を特定することで、各組織は人的資源と共同作業に優先順位を付けやすくなり、どの組織でも適用できる戦略がもたらされる場合がある。2017 年の WireX ボットネットを駆除した共同作業がその例である。

3.1.1 歴史的背景の保持

スピアフィッシング行為などのセキュリティインシデントを調査し、そのインシデントの詳細を後から分析、記録、共有するセキュリティ担当者は、それらの情報を歴史的背景として保持しておくとよい。そうすることで、将来のセキュリティ担当者や管理職が、継続した関連情報を得ることができ、将来のセキュリティイベントと比較できるようになる。これにより、このような組織のノウハウが、将来的なセキュリティチームの人員の入れ替わりに影響されず、企業のために蓄積されることになる。このようなチームにより、今後のセキュリティ調査の効率が向上し、新しい分析者や既存の分析者が調査に要する時間が短縮されるだろう。

3.1.2 時間への初期投資に対する指数関数的な効果

組織があるイベントの詳細を ISAO やそのメンバー組織の内部または適切な外部グループの分析コミュニティーに共有し、多数の分析者が個々に初期の所見を調査し、追加の背景情報を提供して対応した場合、組織は分散された膨大な分析時間を、追加費用の負担なしに得ることができる。時間と労力への初期投資は、共通の関心分野に他者が投資するきっかけとなる。さらに、さまざまなデータセットにアクセスできる他者から付加的な見解を得られることは、例えば、長らく放置された仮説に挑戦するよう周囲を促す可能性すらある。

3.1.3 可視性と分析の向上

「集団認識」の概念とは本能に語りかけるものであり、これは自然界でも見られる。注意深く観察すると、鳥や魚の群れは共通の天敵を回避するため、集団として完璧に揃った動きをほんの一瞬で行っており、その完全に一体となって移動する姿の美しさには感嘆することがある。

成功を目指す社会的な生き物である私たちは、共同作業を通して成功を手にする方法を検討する必要がある。具体的には、類似する問題に遭遇している、取り組んでいる、あるいはそれらの問題を共有している個人が協力関係を築くことができる確かなコミュニティーの活用である。たとえば、地域的な会合、電子メール、チャットベースで連絡を取り合う信頼できるグループ、あるいは会議ベースの同じ興味を持つ人々の集会などである。私たちの環境がデジタル環境と緊密に結合していくことを認識できるようにするには、デジタルメディア全体にわたる効果的なコミュニケーションと組織化が必要である。

デジタルネットワークやソーシャル（個人またはプロ）ネットワークを生み出し、共有組織を作成する機会について検討すると同時に、グループ間の状況認識を高めるために、コミュニティーに未加工のデータ、情報、知識、インテリジェンスを取り入れることができる。自身のデータセットをベースにして共有を行う組織は、共有先から付加的な検知指標を得られる場合が多く、それによって組織のメンバーは効率的に対応できるようになる。取り込まれるデータまたは情報のすべてが「実用的」なわけではないが、それでも、脅威または脅威アクターに対する認識は促進され、データセットの質が向上し、過去、現在、将来のイベントの形跡を特定することが可能になる。

さらに、これらの共有データにアクセスできる多数の組織や人々は、付加価値のある背景情報(調査対象を拡大し、将来の攻撃を阻止する実用的なインテリジェンスになる)を提供することもできる。

3.1.4 防御対策の周知を可能にする

分析を共有する団体では、どの個人または組織が主な参加者または後援者であるかが明確に認識されていることが多い。このような共有団体に積極的に参加して関与する組織は、業界において、同社のセキュリティプログラムが他社も目指すべきビジネス成功への鍵として認識され、安心感を得られる。結果として、業界におけるリーダーシップ獲得の機会がもたらされ、市場形成に対する知見や全体像を提示できるようになる。後者の主な例と

しては、ベストプラクティスや教訓を共有することなどが挙げられる。これらは過小評価されるが、非常に価値のあるリソースである。

3.1.5 共通のリスク

2004 年、防衛産業基盤への標的型攻撃の頻度が増加し、防衛および航空宇宙の市場はこれを問題視するようになった。勢力の伯仲した過酷な競争をしている市場においてでさえ、互いの見方を変え、市場全体が共通のリスクに直面していることを認めなければならなかった。これらの組織は、ビジネス分野で競争している間にも、自分たちの情報技術とセキュリティ人員が、国家主体による巧妙な侵害を受ける恐れといった共通のリスクに、共同で対抗する手段を模索せざるを得ないことを確認し合った。

これを受けて設立され始めたのが、国家サイバー捜査共同タスクフォース（National Cyber Investigative Joint Task Force）や防衛産業基盤サイバーセキュリティ情報共有プログラム（Defense Industrial Based Cybersecurity Information Sharing Program）といった、情報共有と共同作業を目的とした団体である。これらの団体は、国家の安全、防衛、航空宇宙当局にもたらされる共通のリスクに対応している。

増加する圧力と勢いを受け、2015 年のサイバーセキュリティ情報共有法（CISA: Cybersecurity Information Sharing Act）では、民間組織のネットワークや知的財産を保護しながら、組織が直面していた法的な障害を緩和することを目指した。民間組織を標的とする脅威グループの多くは、政府部門の各省や機関も標的にしていたため、CISA では、共通のリスクに取り組む公的組織と民間組織の間でのサイバー脅威情報の共有における責任を限定するための手段を定めた。

今日では、重要な社会基盤のために結成された ISAO や情報共有分析センター（ISAC）といった、概念的に共通するリスクに対抗するさまざまな共同作業モデルが存在し、個人および組織が共通のリスクを特定して削減するために共同で作業することが可能になっている。

4 優先順位の確立

4.1 はじめに

情報の要件に優先順位を付けることで、インテリジェンスサイクルのすべての段階を同時に飛躍させることができる。また、優先順位を付けることで的を絞ることができ、より望ましく実用的な成果が得られるようになる。[2]

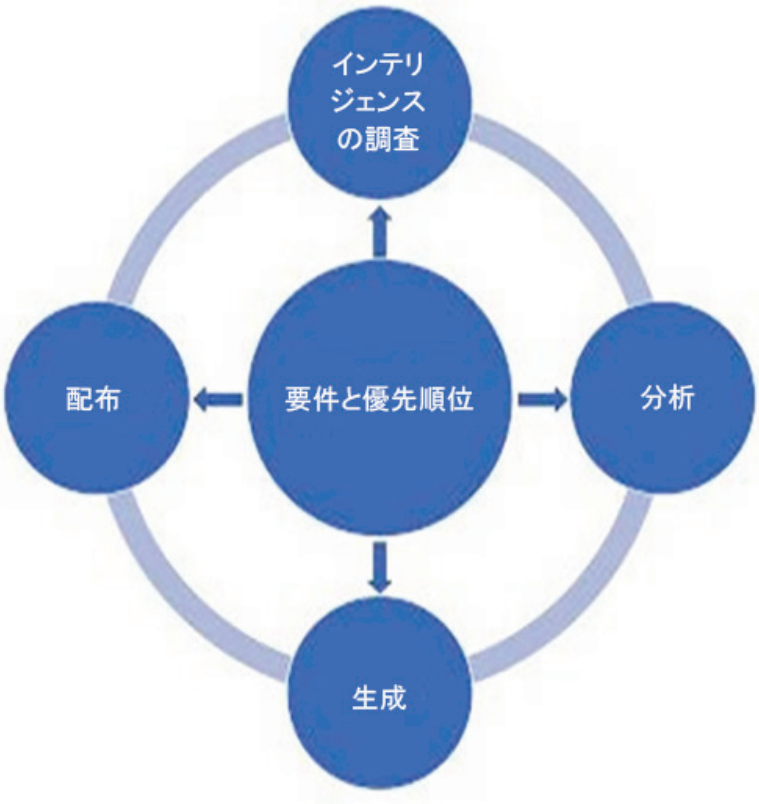

図 1.ISAO インテリジェンスサイクルのフレームワーク

このサイクルの各段階の作業は、優先順位を付ける必要があり、優先順位の根拠は、実施する活動（分析活動）によって設定された必須の活動や最終的な優先順位にある。優先順位は動的かつ状況に応じたものであり、受領者の志向に応じて、修正と変更が頻繁に発生する。優先順位を付ける目的は、入ってくるデータと情報を最適な量に絞り込み、関連性が高く焦点の合ったインテリジェンスを獲得することにある。

[2] ISAO インテリジェンスサイクル、Larry Portouw、NTK Consulting, LLC.

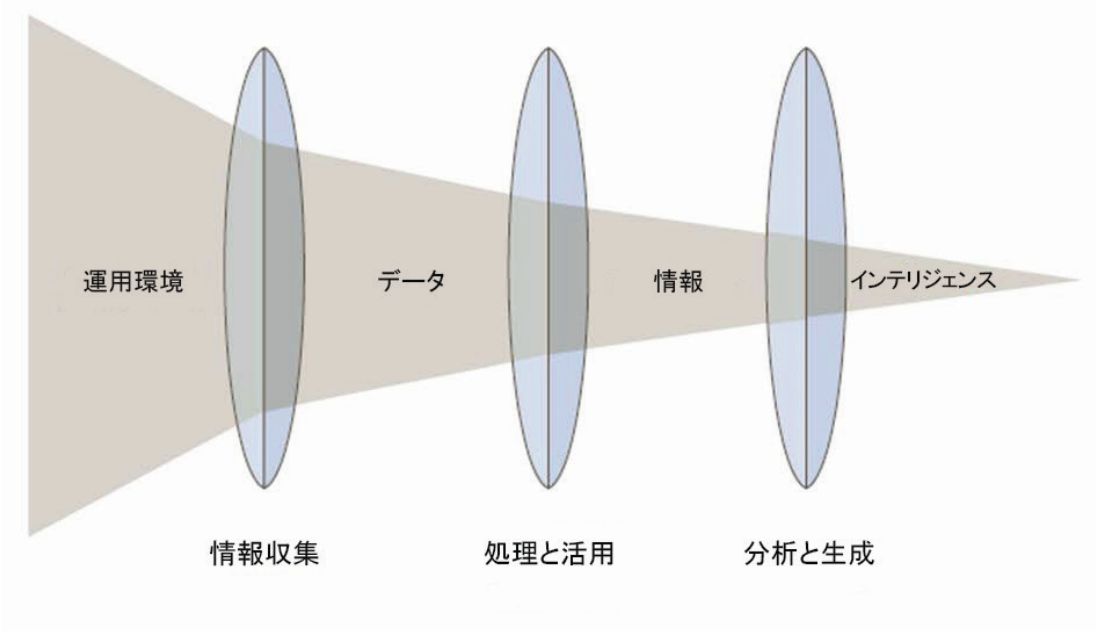

図 2 データ、情報、インテリジェンスの関係 [3]

4.2 情報の要件

データと情報の要件は、一般に情報収集の要件と呼ばれ、インテリジェンス生成サイクルのどの段階でも策定することができ、足りないと認識された情報が反映される。要件の優先順位付けは、ISAO メンバーが行うか、メンバーに代わって ISAO 分析チームが行う。インテリジェンス生成サイクルは、主に情報収集の要件に基づいており、ビジネス目標の達成に関連した要件の定義と混同すべきではない。インテリジェンスの要件は、インテリジェンスの生成を促進するよう意図された、的が絞られ期限が定められた要求事項であり、買収、アーキテクチャ開発、知的財産保護といったビジネスプロセスにおける意思決定において曖昧さを軽減するものである。

情報の要件は、適切で具体的、かつ実用的な要求事項であるといわれる。報告の要件も同様ではあるが、要求事項に対する回答が適切でなくなった場合に、策定にかかる時間はさらに制約を受ける。以下の要件の例は、運用活動から、または内部の分析活動からもたらされている点に留意する必要がある（表 1）。

[3] http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/2-0-Intelligence-Series を参照。

表 1.有効な情報要件と報告要件の策定

不十分な 情報要件	十分な 情報要件	報告要件
XYZ は個人識別情報（PII）を失ったか？ （広範すぎる）	XYZ は、過失、意図的な違法行為、または盗難により、PII の説明責任を失ったか？盗難が原因の場合、どのような攻撃手法が用いられ、アーキテクチャのどのような弱点が侵入を許したか？	PII の損失が確認され次第すぐに報告する。
過去 24 時間に発表された重大 CVM はどれか？（大雑把すぎる）	発行された重大 CVM の内、XYZ 企業への影響が評価されていないものと、リリースから 24 時間以内に緩和されていないものはどれか？	CVM と XYZ への考えられる影響を発行から 2 時間以内に報告する。XYZ の脆弱性における CVM の緩和の状況を、完了まで 8 時間おきに 報告する。
先週、ABC 業界のネットワークから全クライアントデータの登録が盗み出された。次は XYZ の番か？ （非常に具体的ではあるが、この要求事項は実行可能性を示せず（回答しにくい）、期限も定められていない。）	ある業界における攻撃の成功やデータ盗難と、同じ業界における後続の攻撃には、相関関係があるか？ （ある業界において、脅威の成功は将来の攻撃を示唆するものとなるか？）	盗難とデータの種類を確認してから 24 時間以内に ISAO に報告する。 攻撃者の戦術、技術、および手順（TTP）を報告する。
XYZ はインサイダーの脅威に対して脆弱か？	XYZ のネットワーク/システム管理者の個人的な権限の範囲が拡大していないか？ 解雇された従業員の電子メールアカウントをすぐに無効にしているか？	IT 管理者はすべてのユーザーと管理者を確認し、権限の範囲が拡大しているものを報告する。
XYZ は会社のノートパソコンを紛失したまたは盗難されたか？	XYZ は暗号化せずに保存されていた企業データを紛失したまたは盗難されたか？	紛失した、または盗難された機器を、保存データを含めて、すぐに報告する。
セキュリティ規定の内容とあわないソフトウェア/ハードウェアを最近導入したか？	ネットワークシステム構成の変更によって矛盾が生じたり、セキュリティアプリケーションが 動作しなくなったりしていないか？	情報システムの競合をすべて報告して解決する。
いつ、どこで、どのようにしてハッカーは XYZ のデータやネットワークのアクセス権を手に入れたか？	無許可のユーザーがいつ、どの TTP を使用して XYZ の情報システムのアクセス権を手に入れたか？	XYZ のネットワークや設備への無許可のアクセスを 報告する。

4.3 分析の要件

分析の優先順位は、分析を行う組織によって設定され、活動の優先順位、情報の要件、使用できるリソース、要件に応える能力の間のバランスで決定される。要件と優先順位の決定を、組織のすべてのメンバーに定期的に共有する必要がある。分析における優先順位の設定は医療トリアージに似ている。

回答しにくい要件や、限られた時間内に回答できない要件は優先順位が低くなる可能性がある。複数の要件の優先順位を検討する中で、運用に与える影響が高く、使用できるリソースや時間で対処できる要件事項は、優先順位が高くなる可能性がある。分析の優先順位は静的ではなく、新しい要件事項を受け取ったり、運用状況が変わったりすると定期的に調整される。

要件事項の記録と優先順位を、メンバーのすべての活動とともに定期的に共有する必要がある。

4.4 生成の要件

生成の優先順位は分析組織によって決められ、必要となる活動の分析の優先順位、使用できるリソース、運用の要件に基づく。

配布する成果物の生成は、自動レポート(基本的には作成の通過地点である)から公式出版物まで多岐にわたる。生成形式は、生成時間を最小限に抑え、成果物の適時性と正確性を満たすことに重点を置くために、標準化するべきである。

4.5 報告の要件

サイバーセキュリティ情報の共有は自主的になされるものであり、各団体は何を共有すべきか検討しなければならない。詳しくは、セクション 8「報告」を参照のこと。

配布と報告は 2 つのカテゴリに分類でき、(1)一般的または計画的な報告と(2)臨時報告である。どのような場合であっても、報告の優先順位は情報の要件と生成の優先順位に基づく。

計画的な報告と成果物の優先順位は分析組織毎に設定し、リリーススケジュールに従う。これらは定期的な定型報告などであり、内容はメンバー組織の要求に基づく。

臨時報告は、特定の条件が満たされた場合に行っても、生成の要件と時間的制約を踏まえた 1 回限りとしてもよい。たとえば、脅威アクターが脆弱性を見つけ、初めて利用したことをきっかけに報告を行い、情報収集と生成の優先順位を変更することが考えられる。

5 データ/情報の選択

セクション 4 で取り上げたインテリジェンスサイクルでは、データを未加工の状態から、意思決定者やネットワーク管理者が最も効果的にネットワークを保護するために使用できる、完成された成果物に変える工程を紹介した。分析を行う必要のあるデータは要件の変更によって異なるが、データソースを選択する基本工程は変わらない。

本文書では取り上げていないが、米国政府は業界団体や政府機関と情報を共有するための各種プログラムを用意しているため、その点に留意することが重要である。当該プログラムのいくつかは、ISAO 600-2『U.S. Government Relations』で説明している。政府の当該プログラムでは、業界や政府からの大量のデータだけでなく、傾向、戦術、技術、および手順に関する情報を示す分析結果にもアクセスすることが可能になる。しかし、これらのデータを公開する工程は時間がかかることがあり、データが公開される頃には古くて価値のな

いものになってしまっている可能性がある。

5.1 データセットまたは情報の種類（プッシュ/プル）

一般的に言って、分析を実施する際の最大の課題は、メンバーの要件に応える分析を行うのに適切なデータセットや情報を特定して取得することであろう。分析に使用できるデータ/情報の量はほとんど無限であるため、要件を理解して優先順位を付けることが必要となる。内部の情報源（例：セキュリティ情報イベント管理［SIEM］システムなど）からのデータ/情報も非常に貴重ではあるが、このセクションでは外部の情報源から得られる可能性のあるデータ/情報に焦点を合わせている。外部の情報源からプルまたはリクエストして収集するデータセットや情報を選択する際、それが ISAO とそのメンバーのニーズをいかに支援するかを考慮することが重要である。これを決定する際は、各メンバー企業が、規模、区分、能力に応じて、異なるデータセットや情報に価値を見いだす可能性があるという点を考慮することが重要である。

このように、ISAO がそのメンバーのニーズを理解していないと、効果的な分析は不可能である。組織がメンバーのニーズを理解し、それを満たすには、「インテリジェンスの要件」の工程を用いることが役立つ。組織はメンバーのニーズを理解することで、メンバーにとって重要なデータの種類だけでなく、データ/情報を有意義な方法で提示する方法も把握できる。

たとえば、専任の IT 担当者がいない小規模企業は、分析されていない大量の「未加工データ」を有益であるとは判断しない可能性が高い。しかし、熟練かつ専任の IT チームをかかえる企業は、納得できる対価であれば、そのようなデータを有益であると判断するだろう。いずれの組織も、ISAO と提携すると幅広いデータセットを取得できるというメリットがあり、分析の要件を一元化された形式に移行できる可能性がある。

5.2 情報源の選択（公的/私的）

ISAO は、分析作業をサポートするために使用すべきデータの情報源を選択する際に複数の要素を検討しなければならない。しかし最も重要な検討事項は、メンバー組織によって策定された要件に応えるのに適切な情報を提供する情報源を特定することである。

「公的」情報源には 2 つの基本的な種類がある。すなわち、(1) 誰もがアクセスできるニュースサイト、ブログ、公開されている未加工のデータフィードといった、公的な場で入手できるものと、(2) 政府の各部局から得られるデータや情報である。これらの種類の情報源から取得できる具体的な情報の種類について詳しくは、ISAO 300-1『情報共有入門』を参照のこと。

米国政府は、業界および政府で情報を共有するための各種プログラムを用意している。こ

れらのプログラムについては、ISAO 600-2『U.S. Government Relations, Programs, and Services』[4]で説明している。政府のプログラムでは、業界や政府からの大量のデータだけでなく、TTP に関する情報を示す分析結果にもアクセスすることが可能になる。しかし、これらのデータを公開する工程は時間がかかることがあり、データが公開される頃には古くて価値のないものになってしまっている可能性がある。

オープンソースのレポートは、データや情報の優れた供給源となる。これらの資料の中には、組織が無料でアクセスできるものが多数存在する。この種類のレポートは、公的な場で入手可能なブログ、ニュース記事、プレゼンテーションなど、さまざまなルートから得ることができる。また、公開されているデータフィードも多数あり、疑わしいファイルハッシュ値、インターネットプロトコル（IP）アドレス、ドメインネームといった、侵害の検知指標を提供している。オープンソースのデータ/情報の課題は、ISAO 固有の要件に対する適合性だけでなく、その情報の正確性と真実性である。いかなる場合であっても、情報の供給源の正確性と偏りは確認すべきである。

私的な情報源とは、一般的に、非政府団体が提供する一般には公開されない情報を指す。未加工のデータフィードを含む私的な情報源は、多くの場合、極めて高度な能力と専門のアナリストを抱える企業によって、ISAO の要件に直接関係する可能性の高いカスタマイズされたレポートとともに提供される。このような情報源にはコストがかかる場合が多く、小規模な組織や、位置づけが不明確な組織には手が出せないかもしれない。しかしこれらのコストは、パートナーシップの構築などの相互支援を取り決めることで、低下させたり、削減したりできることがある。

結論として、公的情報源および私的情報源はいずれも、組織の分析に対して価値を提供できる。しかしそれが可能なのは、提供するサービスが ISAO とメンバー組織のニーズを満たしている場合に限られる。

5.3 伝達の頻度

一般的には、共有されるデータが多いほど、より優れた成果か得られると見なされる。これは多くのケースで当てはまるが、常に適切であるとは限らない。入手できる情報の量は日々増えていくため、アナリストたちは情報過多によってすぐに疲弊してしまう。提供する情報が多すぎることで顧客や組織がそれを活用できないようであれば、それは何も提供していないのと変わらない。ほとんどの組織は、データ/情報を量ではなく、有用性に基づいて評価している。情報源の選択は、可能な限り有益なデータをメンバーに送るための鍵となる。

[4] https://www.isao.org/products/isao-600-2-us-government-relations-programs-and-services を参照。

5.4 配布と開示

一部のデータ/情報には機密または専有の情報が含まれており、広範に、または一般に共有することができず、結果として ISAO の実効性が落ちてしまう可能性がある。このような影響を最低限に抑え、できる限り広範な配布を可能にするため、メンバーは、共有する情報を分類するための手法を特定し、共有先と共有情報の保護方法を明確にする必要がある。

このような共有工程を管理する完璧なシステムは存在しないが、ISAO が利用できる選択肢の 1 つにトラフィックライトプロトコル[5]（TLP）がある。TLP は、米国コンピュータ緊急事態対策チームができる限り多くの対象者にインテリジェンスレポートを共有するために使用している。表 2 に示されているとおり、TLP はカラーコードによって適切な対象者および関連する共有条件を特定している。

表 2.トラフィックライトプロトコルの定義[6]

色	対象となる情報	共有方法
TLP:RED 公開禁止、情報提供元に限定。	情報が他の関係者にとって有効な行動を起こせるものでなく、悪用された場合に当事者のプライバシー、評判、経営に影響を及ぼす可能性がある場合に、情報提供者は TLP：RED を使用できる。	受領者は、TLP：RED の情報が最初に開示された特定のやり取り、会議、会話以外で、他の関係者にその情報を共有してはならない。たとえば会議という状況においては、TLP：RED の情報はその会議の出席者に限定される。ほとんどの状況において、TLP：RED は口頭または対面でやり取りされるべきである。
TLP:AMBER 限定公開、関係者の組織に限定。	その情報に基づいて有効な行動を起こすためにはサポートを必要とするが、情報が組織の外部に共有された場合にプライバシー、評判、経営に対するリスクが伴う場合に、情報提供者は TLP：AMBER を使用できる。	受領者は、自分が所属する組織のメンバーと、自身を保護し、さらなる損害を防ぐためにその情報を必要とするクライアントや顧客に限り TLP：AMBER の情報を共有できる。情報提供者は共有の対象範囲を自由に追加指定でき、それらは必ず遵守されなければならない。
TLP:GREEN 限定公開、コミュニティーに限定。	幅広いコミュニティーや区分に属するメンバーだけでなく、すべての参加組織への啓発のために有用な情報の場合、情報提供者は TLP：GREEN を使用できる。	受領者は、所属する区分やコミュニティーのメンバーやパートナー組織と TLP：GREEN の情報を共有できるが、公的にアクセスできるような方法では使用しないこと。このカテゴリの情報は、特定のコミュニティー内で広範囲に配布できるが、コミュニティーの外部には公開すべきでない。
TLP:WHITE 公開制限なし。	悪用のリスクが少ないか、予測可能なリスクのない情報の場合、適用される一般公開のルールや手順を踏まえて、情報提供者は TLP：WHITE を使用できる。	標準の著作権法に従い、TLP：WHITE の情報は制限なく配布できる。

[5] https://www.us-cert.gov/tlp を参照。
[6] https://www.us-cert.gov/tlp を参照。

TLP は業界標準として幅広く受け入れられているため、TLP を使用することで、ISAO メンバーの大多数が慣れている可能性が高い使いやすい基盤がもたらされる。

6 ベースラインの確立

インテリジェンスサイクルにおけるインテリジェンスの調査および分析の段階に取り組む際、重要となる部分は、動作が通常であること、あるいは普段とは異なる動作であることを判別するためのデータ比較を行うことができる、確固たる開始点を用意することである。この開始点は、多くの場合、ベースラインと呼ばれる。ほとんどの組織は、ベースラインとなるネットワークの調査を実施することで、さまざまな要件の土台を築くことができる。このような調査は一般的に、ネットワークの観点から見た通常の運用状態を定める一連の尺度基準を確立し、異常な動作を識別するための比較対象を管理者に提供して、ネットワークパフォーマンスの限界を明確にするために行われる。ネットワーク使用の変化を時間と曜日に基づいて予測できるようにするには、複数の時点で測定値を取得し、正確な評価基準を得る必要がある。

ISAO に伝える必要があるベースラインデータの種類は、メンバーが受け取ることを期待する分析の水準に応じて異なる。ISAO は、メンバーネットワークにおける分析の主要な構成要素として機能している可能性があり、データの完全なコピーを求めることが多い。それに対し、ベースラインは、単にメンバーが ISAO に異常を知らせる必要がある場合の基準を設定するために使用することができる。

6.1 標準化

ISAO がメンバー組織から提供されたデータを効率的に解析して分析するためには、ISAO 全体で使用できるデータセット標準を策定しておく必要がある。ISAO 全体にわたって標準データセットを収集できるよう、メンバー組織はいくつかの点に同意する必要がある。

主な検討項目としては、監視が必要なネットワーク要素、収集の頻度、そして正確な評価を提供するために必要となる明確なデータポイントの定義などが挙げられる。これらの項目以外にも、収集されるデータの種類において受け入れられる開示レベルや、使用される匿名化技術に対して、すべての ISAO メンバーが同意しなければならない。

6.2 検討事項

ネットワークのベースラインは、無数にあるツールを利用することで達成できる。簡易ネットワーク管理プロトコルのようにさまざまなプラットフォームで使用できるツールもあれば、特定のオペレーティングシステムやネットワークタイプで動作するよう設計されているものもある。ベースラインの実行に必要なツールは、関係のあるシステム、ツールのコスト、データの確認に使用できる時間、データを有用なものにするために必要な詳細の度合いといった、複数の要因によって決定される。

詳細について言えば、ISAO は運用の開始点として、2 つの包括的なデータ詳細度を選択できる。1 つ目は、最上位のデータに的を絞ることである。このデータは、ネットワークの使用やパフォーマンスの変化の先行指標として利用するものであり、より詳細な分析やデ

ータ収集を行う必要がある。このオプションでは、必要となる事前作業が少ない代わりに、重要なデータを見逃してしまうリスクがある。2 つ目は、毎回非常に詳細なデータセットを取り込むことである。データを見逃してしまうリスクは軽減されるが、データの収集と確認に必要な時間は増加する。

ほとんどの ISAO においては、両方のアプローチを組み合わせて、主要なネットワークセグメントからは詳細な情報を、堅牢な部分やあまり重要でない部分からは最小限のデータを収集すると、高い効果が期待できる。重要な検討事項としては、情報の収集、保管、分析にかかるコストも挙げられ、これらのコストはベースラインの範囲が広がるにつれて増加する。

7 分析

7.1 メンバーから提供された情報の分析

ISAO が担う主要機能の 1 つは、コミュニティーメンバーによる投稿を収集し、レポートの情報源の秘匿化およびサニタイズを行い、データを拡充して相関付けてから、幅広くコミュニティーに共有することである。このようなレポートは、情報源が精査されているというメリットがあり、業界特有の幅広いコミュニティーに適合するだけでなく、すべてのメンバーの警戒姿勢も向上させる。これらの活動を実施する工程は、データの拡充と相関付けの 2 つの段階に分けることができる。

7.1.1 情報源の秘匿化

ISAO メンバーから得たレポートは、情報源を特定できる情報を取り除いた状態で、すぐに投稿追跡システムに入れるべきである。情報源を特定できる情報には、マスキングされていないシステム名、RFC1918 に記載されているプライベート IP ネットワーク以外の IP アドレス、ドメインネームなどが含まれる。アナリストは、あらかじめサニタイズされたデータセットで作業することで、最終的なレポートから非公開とすべき（そして関係のない）詳細情報を共有してしまう恐れを軽減できる。最終的なレポートを保存して共有する前に、情報源を特定できる情報が取り除かれていることをダブルチェックするために、別のアナリストによってレポートを査読してもらうべきである。

7.1.2 データの拡充と相関付け

一般的には、メンバーの提供情報には、メンバーが行った調査の過程で特定された、侵害の検知指標（IOC）または TTP が含まれているはずである。添付された IOC または TTP には、以下に関する情報が説明的に記載されているべきである。まず、イベントのおおまかな内容とメンバーの環境で何が起こったか、次に、IOC や TTP の拡充と分析のためにこれまでに活用したリソースの履歴、脅威アクターの巧妙化の調査、最後に、可能であれば IOC または TTP を Lockheed Martin 社の Cyber Kill Chain™モデル [7]に結び付けた情報である。

[7] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html を参照。

IOC および TTP を適切に分析できるかどうかは、データを相関付ける段階で、これらを以前のイベントに結び付けられるかにかかっている。そしてデータを拡充する段階で、当該イベントおよび関連イベントから得た各検知指標間の関係性を詳細に説明し、文書化しやすくするために、これまであいまいだった、あるいは明らかでなかった参照資料を複数用意する。

ISAO が行う分析では、メンバーの提供情報に対する情報源の秘匿化とサニタイズと、IOC や TTP の抽出と拡充が完了すると、相関付けの工程が必要となる。これらの工程はツールに大きく依存するものではあるが、おおまかには、同じデータポイントに関係する以前の事例を分析によって探すことになる。たとえば、ある特定のドメインを利用するフィッシングキャンペーンは、他の組織にもフィッシングメールを送信していることが確認されている IP アドレス上にホスティングされている場合がある。こうした事実を結び付けることで、そのフィッシングキャンペーンは当該メンバーを明示的に標的にしているわけではないことが推測できる。

しかし、TTP や IOC が初見のものである場合、攻撃者の巧妙さが高度化してきているという根拠となる場合がある。これらの事実を文書化しておくと、そうした判断を円滑に進めることができる。

分析チームは、相関付けのワークフローを、再現可能な形で構築すべきであり、これには以下に示す種類の情報源を活用することが含まれる。

- 検索エンジン
- ISAO データベース（以前の提供情報など）
- オープンソースのセキュリティ関連情報
- ベンダーのポータルやデータベース（通常は有料）
- 非公開の信頼できるグループ
- 1 対 1 の関係
- パッシブ Domain Name System（DNS）（通常は有料）
- ドメイン履歴データベース（通常は有料）

ISAO のうち、特に、脅威インテリジェンスへの投資があまり進んでいない業界の ISAO は、相関付けに使用するデータを得るために用いる有料の情報源に投資するために、メンバーから使用料や手数料を徴収することが必要になるかもしれない。これらの情報源は、パッシブ DNS、ディープ Web やダーク Web のデータ、ドメイン履歴といった、非常に特殊なデータであるため、極めて貴重なものである。ISAO のような一元的なリソースを活用することで、脅威インテリジェンスへの投資が少ない小規模な組織でもメリットを得ることができる。

7.2 分析工程の文書化

分析の過程では、元の提供情報と、拡充および相関付けされたデータの両方を明らかに

する。その際、関連する情報源の情報、データポイント、未加工のデータなどを保存しておくだけでなく、実施した工程も文書化しておくことが重要である。防御アプローチが成功したことや、脅威の疑いのあったものが実はフォールスポジティブだったことを示す場合があるため、分析の結果、脅威は認められなかったという結果についてもこの工程で文書化することが望ましい。

これらのビジネスプロセスを記録しておくことは、後に分析結果を文書化する段階で非常に役立つ場合がある。ISAO は分析結果をフォレンジック分析のようなレベルで文書化する必要はないが、分析結果に至ったステップを文書化し、なおかつ文書の形式も揃えるべきである。

第三者サイトに分析結果を保存する場合は、そのデータへの参照に加えて、ローカル環境にコピーを保存しておく。これらはすべて、ISAO のセキュリティポリシーに従って事例ファイル追跡システムに保管する。

すべての分析工程（情報源の秘匿化とサニタイズ化、拡充、相関付け、文書化）が完了すると、アナリストは、おそらく最も難易度の高い段階である、体験談の盛り込みを開始できる。

7.3 体験談の盛り込み

分析結果を伝えるために体験談を盛り込む際は、以下の点に留意する。

- 分析はタイムリーで、関連性が高く、実用的なものであること。
- 情報提供者を特定できる情報が含まれていないこと。
- 分析が完了していて、説得力があること。説明が不十分な分析は、他のメンバーに受け入れられないだろう。

重大度、影響、範囲といった背景を欠く単独のインシデントも、各メンバーがどのように評価したかという視点を盛り込むことで、ISAO はイベントの全体像を作り上げることができる。IOC、TTP、範囲、影響、そして重要度を一緒に盛り込み、それらの詳細情報を効果的に伝達することで、メンバー組織はそれらの要素をすべて自身の運用に関連付けることができる。

ほとんどの分野のメンバーが特に関心を示すのは、学んだ教訓、ベストプラクティス、そして推奨される手順である。たとえば、レポートにはマルウェアの指揮管理ポイントとして使用された IP アドレスのリストと、推奨する対策として以下の内容を含めることができる。

- 過去に同一のものがないか、SIEM やログを検索する
- 周辺に設置されているゲートウェイでこれらの IP アドレスをブロックする
- 今後同一のトラフィックが発生した場合に備えてアラートを設定する

当該動作を実施するために特定の脆弱性や TTP が利用された場合は、それらについての詳細も記述し、組織がネットワークを防御するための手助けとなるベンダーパッチやリソースへのリンクを添えておく。最初の侵入地点として誰でもアクセスできる状態の Remote

Desktop Protocol（RDP）ホストが使用された場合は、以下のような対策が推奨される。

- 組織に誰でもアクセスできる状態の RDP システムがないか調べる
- これらのシステムが正当な目的を果たしている場合は、RDP ホストのセキュリティ強化ガイドを実装する
- RDP ホストで多要素認証を使用するようにする

あらゆる推奨事項や観測事項を精査し、詳細なサードパーティリソース（ブログ記事、ベンダーレポートなどへのリンク）を参考文献として提示しなくてはならない。近年、脅威インテリジェンスのコミュニティーで、推測や確度の評価を正確に行うための取り組みが盛んになっている。マルウェア情報共有プラットフォーム（MISP）[8]のプロジェクトでは、以下のような分類法を文書化している。

- *情報源の信頼性*
  - A. 完全に信頼できる
  - B. ほぼ信頼できる
  - C. やや信頼できる
  - D. ほぼ信頼できない
  - E. 信頼できない
  - F. 信頼性を判断できない
- *情報の確実性*
  - 1. 他の情報源によって確認済み
  - 2. おそらく真実である
  - 3. 真実である可能性がある
  - 4. 疑わしい
  - 5. 真実である可能性が低い
  - 6. 確実性を判断できない

共通の分類法に従うことで、アナリストは一般に知られている分類法を用いて自分の評価に説得力を持たせることができる。

最後に付け加えると、すべての成果物に説得力を持たせる必要はないが、重大イベント

[8] https://github.com/MISP/misp-taxonomies/tree/master/admiralty-scale を参照。

に関するレポートには説得力を持たせるよう特に努力しなければならない点に留意しておく必要がある。脆弱性や注目を集めるイベントについての業界の警告に対して注意を払わなかった組織は、極めて重大なセキュリティ上の問題に直面してきた。注目を集めるイベントについて詳しく説明しているレポートは、公開は早いが説明が不十分なレポートよりも間違いなく重要であろう。

7.4 完成した成果物の保管

最初のレポートや、情報源を秘匿化してサニタイズした提供情報、拡充や相関付け、その他のドキュメントといったすべての成果物は、ISAO のセキュリティポリシーに従って保管しておく必要がある。さらに、完成したレポートと IOC は、脅威インテリジェンスプラットフォームに保管されるべきである。そうすることで、将来の調査でそれらのデータを拡充と相関付けに活用できる。一般的には、完成したデータは ISAO メンバーが検索できるようにしておく。

7.5 オープンソースのレポートの分析

オープンソースのレポート、ニュース、そしてインテリジェンスは、ISAO とそのメンバーにとって非常に価値のあるリソースである。情報過多である状態は、よく「消火ホースから水を飲む」ようなものだと例えられるが、いくつかの手法を用いれば、実用的なインテリジェンスを安定的に得ることができる。これらの情報源に関する懸念事項は、提示されるデータの妥当性である。誤ったデータや不完全なデータを提供する情報源を使用すると、それらの影響を受けたガイダンスが作成されてしまう恐れがある。

7.6 優先順位付け—関連度が高く、適時性があり、実用的であることの確認

使用する情報源は業界ごとに異なる可能性があるが、関連性、適時性、実用性に関する評価を判断するとき、誰もが ISAO の分析チームに頼っている。おおまかに定義すると、あるアイテムの関連性とは、メンバー組織に悪影響をもたらす可能性が高いかどうかであり、あるアイテムの適時性とは、最近観測されているかどうかである（とはいえ古いアイテムの中にも、最初に観測されてからずっと後になって明らかになるものがある）。アイテムが実用的となるかどうかの評価は、レポートに含まれている詳細情報に大きく依存する。しかし、最も重要な懸念事項は、メンバー組織が検出、ブロック、または別の方法でその環境を変更できるかどうか、あるいは、脅威を緩和するために取り得る対抗措置について他の部署に助言できるかどうかである。

7.7 オープンソースのレポートをめぐる意見

脅威インテリジェンスのアナリストは、オープンソースの情報源から特定のトピックに関する調査をして報告することに、時間の大半を費やしていると言っても過言ではないだろう。この作業は、閉じられたチャネルからは入手できない開発、脆弱性、分析結果についての情報を、ISAO メンバー組織が常に把握できるようにする極めて貴重な作業である。これらのトピックをタイムリーに報告することで、新しく注目されているトピックの最新情報をメンバーが意思決定者に提供するのを支援できる。

ある時から急によく見かけるようになったトピックに対しては拡充と分析の量が少なくなりがちだが、ISAO アナリストはそのトピックの関連性について 1、2 行の解説を提供するだけでも、コミュニティーにとって助けとなる。ISAO で推奨し、新しい脆弱性、観測、TTP による予期せぬ影響について、メーリングリストでの自由な意見交換がなされるようにするべきである。

7.8 ツールとリソース

ISAO は、メンバーが増加し、コミュニティーを支えるビジネスプロセスが発達してくるのに従い、脅威インテリジェンスのためのツールや有料情報源、拡充と相関付けを行うベンダー、そしてデータ分析とストレージシステムにリソースを投じることを検討すべきである。また、さまざまなツールやベンダーに投資すると同時に、多岐に渡るスキルと経歴を持ったチームの拡大にも同様に投資すべきである。

7.9 拡充と相関付け

拡充と相関付けの活動をサポートする最も一般的なツールを、以下にいくつか紹介する。

- Paterva 社の Maltego
- 脅威インテリジェンスプラットフォーム [9]（以下に例を示す）
  - Anomali Threatstream
  - Collaborative Research Into Threats
  - MISP
  - ThreatConnect
  - IBM X-Force Exchange
- Palantir
- IBM i2 Analyst's Notebook

ツールやプラットフォームを選ぶ際に重要となるポイントは、組織、予算、専門知識によって異なる。紹介したツールのいずれも公認や推奨をするわけではないが、市場で手に入るソリューションを比較検討する参考として上記の一覧は有用である。

ISAO が最初に導入するであろうツールの 1 つとして拡充と相関付けのプラットフォームが挙げられるが、パートナーとベンダーのアプリケーションプログラミングインターフェース（API）やフィードに対応できるよう、拡張可能であるべきだ。こうした統合に対応できる拡張性や柔軟性を備えたソリューションは、ISAO にとって極めて重要な懸念事項である、長期的な持続可能性を達成するうえで手助けとなる。また、1 年に及ぶ履歴データを照会できる機能や、異なるベンダー間でデータポイントを相関付けることができる機能も、非常に重要である。

[9] https://wi2017.ch/images/wi2017-0188.pdf を参照。

7.10 データストレージ

脅威インテリジェンスのプラットフォームは、拡充と相関付けにとどまらず、インテリジェンスレポートを ISAO メンバーに共有するプラットフォームを提供するなど、さまざまな機能を持たせることができる。各種プラットフォームの機能はそれぞれ異なるが、ISAO のアナリストチームがレポートを公開し、メンバーがそれらを手動で、または API を使用したプログラムによって利用することは、どのプラットフォームでも可能である。また、このようなプラットフォームを使用することで、メンバーは拡充と相関付けのための個別のツールを、その貴重なリソースに連携させることができる。ISAO は完成したインテリジェンスの配布手法として最初のうちは電子メールを利用できるが、この手法では新しい ISAO メンバーが過去のレポートにアクセスできない。

詳細については本文書のセクション 10「セキュリティ」で説明しているが、事例ファイル、調査結果、提供情報のデータ保存場所は、脅威インテリジェンスのプラットフォームとは別に保管すべきである（このプラットフォームは完成したレポートのために使用するべきである）。この隔離されたストレージには、非常に機密性の高いデータが保存されるため、適切なセキュリティポリシーとツールをもって保護するべきだろう。同じく重要なこととして、証明書、パスワード、API キー、製品キーの保護も必要である。

7.11 スキルと専門知識

脅威インテリジェンスのアナリストは、その役割を果たすために幅広いスキルを必要とし、その多くは ISAO に固有の課題や対象に特化している。アナリストは、以下のスキルの一部またはすべてを最低限持っている必要がある。

- 調査の心構え
  - 好奇心
  - 質問し、掘り下げた調査を行う能力
  - メモを取る
  - 矛盾がない
  - 事実を取り込み、体験談や仮説をまとめ上げる
  - 攻撃者特有の思考傾向を理解する
- 文章作成スキル
  - 対象読者に向けて明確かつ簡潔に書く能力
  - 意見と事実を区別する
  - 事実を根拠で裏付ける
  - 意見を参照資料や過去の事例で裏付ける

- 技術的な能力
  - Python スクリプト作成
    - Ruby、Go、Java、Perl、C、アセンブリ言語といった他の言語も有用であるが、Python は脅威の研究者やレッドチームの間で共通語となっている。
  - JSON および API
  - DNS、電子メール、Web プロトコル、セキュアソケットレイヤ、Transmission Control Protocol、User Datagram Protocol、IP ネットワーク

上記の主要スキルを踏まえると、最も成功する脅威インテリジェンスアナリストの中には、警察、軍隊、国家情報機関、報道やプロとしての執筆、セキュリティ上の問題に特化したシステムおよびネットワークの分析、セキュリティの運用/エンジニアリング/アーキテクチャの経験を有している者もいるだろう。複数のメンバーから成るチームは、技術アナリストと元警察官をペアにするなど、スキルと経験を多様にすることを目指すべきである。脅威インテリジェンスのアナリストは、他のどのようなチームよりも、重大インシデントの発生時には各種専門分野において専門家として振る舞わざるを得ないが、多様な経験やスキルが融合することにより、調査と推奨事項の速度、効率性、質が向上する。

成熟した脅威インテリジェンスチームにとっては、性別、年齢、人種、そして文化の多様性もまた、専門分野の多様性と同じ理由で価値のあるリソースである。脅威インテリジェンスの新しいアナリストを雇用する際は、候補者の技術や専門性による長所だけでなく、このような多様性による隔たりを橋渡しする能力も考慮すべきである。

8 レポート

脅威インテリジェンスレポートは、上述の分析結果を、上級管理職、中級管理職、運用スタッフといったあらゆる階層の意思決定者に伝えるのに効率的な方法である。一般的にこのようなレポートは、政府機関、民間のサイバー脅威インテリジェンス企業、あるいはこの作業につぎ込めるリソースを十分に有するその他の中～大規模の組織によって発行される。いくつかの ISAC も脅威インテリジェンスレポートを発行しているという背景もあり、ISAO としても、メンバーへの脅威インテリジェンスレポートの配布に取り組んでもよいかもしれない。

データ交換の標準に準拠した、マシン読み取り形式の自動配信フィードとは異なり、脅威インテリジェンスレポートは一般的に、定型にとらわれない文章やテキストであることが多い。インテリジェンスレポートは脅威データだけでなく、「意思決定時に必要となる背景情報を提供するために集約、変換、分析、解釈、あるいは拡充された情報」[10]を伝える。また、脅威レポートではデータを可視化する技術も活用し、大規模なデータセットを分析した結果を伝えることもできる。

[10] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing*. National Institute of Standards and Technology Special Publication, 800, 150.

8.1 レポートの種類

サイバー脅威インテリジェンスを発信する各組織ではいくつか共通の種類のインテリジェンスレポートを用意しているため、ISAO はそのサービスの一環として、そうしたレポートを活用して共有することを検討するとよい。ISAO、またはその他の脅威インテリジェンスを発信する組織は、作成するレポートの種類を選択する前に、意思決定者に直接意見を聞くかアンケートを取って、意思決定を支援するのに最も有用な情報は何かを判別しておくことが望ましい。

8.1.1 傾向分析と新しい脅威

傾向分析と新しい脅威を報告するレポートでは、組織の情報セキュリティに対する既存の、または新たな脅威の予兆とみられる傾向について過去に遡って特定するために、さまざまな組織や場所にまたがる検知指標（ウイルスシグネチャ、ハッシュ、IP アドレス、ドメインネームなど）が集約されて分析されている。これらのレポートには、ダーク Web から収集した攻撃を企図していることを示す情報など、背景情報を付け足すその他の関連情報が含まれる場合もある。ISAO は、メンバー組織から得た検知指標を集約して精査し、そのような傾向を特定して注意喚起したり、これらの脅威を緩和または無効化する手法を提供したりするのにちょうどよい立場にあると言えるだろう。この種のレポートは、急速に拡大する差し迫った脅威や、急速に進行するイベントをめぐる集約情報を分析することがいかに重要であるかを強く示すものである。これらのレポートは、経営幹部や管理職向けであり、技術的な問題よりも戦略的な意味合いを重視している。

8.1.2 対象またはキャンペーン分析

この種のレポートには、脅威アクターの TTP、標的、動機、目的などとともに、特定の脅威アクターやランサムウェアやフィッシング等のキャンペーンに関する情報が含まれる。ISAO は、メンバー組織を標的とする可能性の高い脅威アクターやキャンペーンに関するレポートを生成または配布することを検討できる。そのようなインテリジェンスは、レポートの受領者が脅威情勢や脅威アクターの能力と目的への理解を深めるのに役に立つだろう。対象またはキャンペーン分析のレポートは、傾向分析と新しい脅威のレポートよりも戦術的なものであり、より技術的な詳細情報が含まれる。

これらのレポート（特に傾向分析と対象/キャンペーン分析）では、大量の複合データに根拠を置く場合は特に、「データストーリーテリング」や「分析ストーリー」といった分析手法を活用して効果を高めることもできる。細部については意見が異なる場合があるが、これらの手法には一般的に、分析中の新しい動き（例：特定の業界に対する一連のフィッシング攻撃）に言及すること、回答される主要な質問または新しい動きに対する「So What?（だから何）」分析（例：そのキャンペーンが業界にとって重要である理由）に言及すること、体験談（背景情報を付け足し、イベントについて追跡しやすい方法で説明する）によって時間を遡ってデータを精査すること、そしてデータの可視化を活用することで、このような体験談を伝わりやすくすることが含まれる。

さらに、脅威インテリジェンスにおける分析ストーリーの主要な構成要素として、サイバー脅威に関する体験談だけでなく、脅威を検出、緩和、無効化できる方法といった、運用担当者や意思決定者にとって有用な情報と分析が含まれる場合がある。最後に、脅威インテリジェンスの分析レポートでは、使用された分析手法だけでなく、分析評価の自信の度合いもすべて明らかにされなければならない。

8.1.3 差し迫った脅威の警告またはセキュリティアラート

最近になって明らかになった重大な脆弱性や、急速に増大している攻撃キャンペーンといった情報セキュリティへの差し迫った脅威に対抗し、ISAO には、その脅威について現時点で分かっていることや、それらから保護するために必要な対策などとともに、差し迫った脅威に関する警告やセキュリティアラートを生成してメンバーに配布することを推奨する。差し迫った脅威の警告レポートは、変化する危険に関する新しい情報が入り次第、徐々に発展させていくことができる。これらのレポートは完全に戦術的なものであり、セキュリティ体系、構成、および特定の技術的な検知指標に焦点を合わせている。脅威情報の自動共有について詳しくは、ISAO-SO 300-2（現在草稿中）を参照のこと。

8.2 レポート作成の頻度

レポート配布のタイミングや頻度は、意思決定に影響を与える情報を提供する能力に重大な影響を及ぼす。セキュリティアラートや差し迫った脅威の警告といった一部の種類のレポートは、即時かつ臨時的に配布し、迫り来る脅威に対して受領者が行動するのに十分な時間を持てるようにするのが望ましい。戦術面を重視したその他の種類のレポートは、計画的または定期的に提供できる。

ISAO を含め、脅威インテリジェンスを発信する組織は、レポートをいつ配布すれば、情報セキュリティの問題に関連する意思決定をする上で効力が最大となるかを把握するため、受領者と緊密に連絡を取ることを検討するとよい。例えば、業界または組織に迫りくるサイバー脅威に関する戦略的レポートは、組織の情報セキュリティに対する予算、技術、準備などについて議論する上層部会議の直前に提供すると最も影響力があるだろう。

8.3 教訓

セキュリティインシデントの発生直後に、脅威インテリジェンスを発信する組織は、教訓の検討会に参加することを検討し、今後の意思決定に生かせるような、インシデントから得られる情報は何かを判別するとよい。このような事後の取り組みには、組織内の異なる部署からも情報セキュリティ担当者が多数参加できる。ISAO はこうした検討会に参加し、情報の共有および分析に関連する技術、専門知識、ノウハウのうち、向上させる分野を特定するとよいだろう。

9 フィードバックおよび成果物の評価

ISAO が組織のメンバーに分析レポートを配布した後、情報の質と、レポート作成の工程を向上するための改善点に関するメンバーからのフィードバックを、分析スタッフが受け取れるようにする仕組みが必要となる。最初のうちは、成果物を改良してメンバーからの要件に適切に応えられるようにするために、アナリストは頻繁にフィードバックを受け取る必要

があるが、時間の経過とともに ISAO が成熟し、標準化できてくるにつれ、フィードバックは減ってくるだろう。評価に必要な情報は、生成したレポートの種類により若干異なるが、フィードバックの形式には原則として同じ基本項目を含めるべきである。

9.1 適時性

レポートの質と有用性を向上させるためには、すべての評価において 3 つの主要な要素を取り扱うべきである。最初に挙げられるのは適時性である。ほとんどのレポートでは、そこに含まれる情報に時間的制約があり、メンバーに届くのに時間かかかるほど価値が減少する。この要素への取り組みでは、質の高いレポートの作成に必要となる時間と、脅威に対策を打つ時間的余裕とのトレードオフを調整するために、何度も変更を繰り返すことが多い。この評価を行った結果、時間的制約を克服するために、別のレポートタイプを作成する必要性が明らかになる場合がある。

9.2 対象読者

次の要素として、対象読者のレベルにあわせてレポートを書くことが挙げられる。受領者がレポートの情報を確実に活用できるようにするには、作成するレポートに応じて用語や説明の詳細さを変えることが必要になる。専門用語を過度に用いて作成されたレポートは、意思決定者にとって分かりにくいだろう。かといって技術的な説明に欠けるレポートでは、管理者がネットワークの保護のために必要とする情報が伝わらない。このような課題は克服可能ではあるが、それには各レポートの対象読者を把握するためにメンバーと ISAO との間で明瞭なコミュニケーションが必要となる。また、幅広い読者に対応できるよう、いくつかのレポートの形式を変更する必要があることが判明するかもしれない。

9.3 頻度

最後に、評価すべき要素として、レポートが発行される頻度が挙げられる。セキュリティパッチが見つかり次第、それに関する通知を個別に送信することは賢明であるが、脅威の活動がないことを示す日次レポートは好ましくない。なぜなら、ほとんど価値のないレポートに管理者が慣れてしまい、レポートに価値を見出さなくなり、確認しなくなってしまう恐れがあるためである。適時性と同様に、レポートを作成する必要がある頻度と、レポートの内容に応じてスケジュールを変更するかどうかを決定するために、レポートの作成基準を確立しなければならないという状況が発生する場合がある。

9.4 配布

ISAO はフィードバックを提供してもらうための適切な形式を決定するだけでなく、これらの評価結果を展開する方法も決定する必要がある。ほとんどの場合、評価結果を確認すべき対象者は、自分たちの手順を何かしら改善する役割を担うことになる分析スタッフである。しかし、すべてのメンバーに評価結果を展開することや、改善を促したりすることには懸念がある。前者は ISAO 全体に影響を及ぼす恐れがあり、後者は他のメンバーに悪影響を及ぼす恐れがあるためである。また、後者の可能性については、評価を下す方法や、正しい工程を最終決定する ISAO メンバーについての疑義も生じかねない。

10 セキュリティ

通信の機密性が確保されて初めて、メンバー組織は ISAO の提供するインテリジェンスを受領したり、ISAO と情報共有してもよいと思える。そのため、ISAO は最低限の通信セキュリティメカニズムを提供しなければならない。一般的に、インテリジェンスの共有には、電子メールと Web ポータルのいずれかの手法が使用される。これらの手法はどちらも、インテリジェンスレポートやデータを収集して配布するために幅広く活用されている。以下はセキュリティ対策として最低限であり、将来的には追加のセキュリティについて再考するのが望ましい。

確固たるセキュリティ対策の必要性を実証できるワークフローと手法の例として、次の事項を考慮する。

1. メンバー組織はデータ侵害に関する TLP Red の詳細情報を共有し、ISAO が TLP Amber に該当する情報のみを抽出し、情報を共有できるようにする。
2. ISAO アナリストは、メンバー組織から、その組織の詳細情報、その組織に対する影響分析、および技術的な検知指標が含まれたレポートを受け取る。
3. ISAO アナリストは、メンバー組織が特定されるような情報を含まないように注意し、関連する検知指標やおおまかな影響評価の含まれたメンバー向けのレポートを生成する。

10.1 暗号化

Web サイトと電子メールのサーバーでは暗号化を利用し、特に Web サーバーについては Hyper Text Transfer Protocol Secure のみを利用するのが望ましい。電子メールサーバーには、セキュアソケットレイヤ上でインターネットメッセージアクセスプロトコルを使用するといった、証明書を必要とするレベルのセキュリティを常に使用するべきである。推奨される証明書の強度は年々変化するため、組織は証明書を必ず更新するようにし、更新時点で最も堅牢な証明書を選択するようにする。

通信経路を保護するための基本的な暗号化手法に加え、機密性の高いデータが含まれる電子メールや共有ファイルには、Pretty Good Privacy などの暗号化技術を常に活用するべきである。電子メールとファイルの暗号化によって、受領者のみがインテリジェンスの成果物を閲覧できるようにすることで、信頼性と機密性を高めることができる。

こうした暗号化の技術と手法を新しい ISAO メンバーに伝えるには、新規加入者研修あるいは定期的な連絡（毎月など）を利用するとよいだろう。メンバーには、ISAO との情報共有に暗号化を使用することを強く推奨する。

上記のステップ 1 の例では、メンバー組織には、詳細で機密性の高いレポートを ISAO と共有するための要件があるだろう。すべてのファイルのコンテンツの暗号化だけでなく、メールまたは Web の暗号化も活用することで、メンバー組織はレポートの内容を受け取って読んでいるのは ISAO のアナリストのみであることを確信できる。

10.2 保存データ

新しいインテリジェンスをキュレーションし、信頼できるパートナー、ベンダー、メンバーから受領するレポートが増えていくに従い、機密性の高い情報に対する ISAO の責任は増大していく。例えメンバーのセキュリティに関するニーズに応えるサービスを提供していたとしても、ISAO 自身が深刻なリスクの原因となってしまう可能性は否めない。そのため、ISAO 内に保存されているデータコレクションの機密性、可用性、完全性には、細心の注意を払う必要がある。

このようなデータを保護するためには、おおまかに次のような基本的なセキュリティ対策を講じるべきである。

- 定期バックアップのルーチン化。これには、オフサイトでの暗号化されたテープやドライブへのバックアップが含まれる（従来のバックアップアプローチ）
- ネットワークファイルシステムを使用したオフサイトでの暗号化ファイルのミラーリングやバックアップ
- （クラウドによるアプローチ）
- ファイルの完全性の監視
- ファイルをバックアップから復元する定期テストのルーチン化
- ISAO のサーバーやオフィスへのアクセスを制限する物理的なセキュリティ手法。防犯カメラやカードキーなどが挙げられる
- 暗号鍵やパスフレーズ/パスワードの保護。これらのデータは、空間的に隔離されたシステム上で保護すべきである
- ホストベースまたはネットワークベースのセキュリティ技術
- ISAO のコンピュータシステムの定期メンテナンスを必ず実施すること。これには、システムが最新の状態に保たれていること、ライセンスが最新であること、そして組織的なセキュリティツールが適用されていることが含まれる
- セキュリティ対策に対する確固たる組織方針と研修
- アクセス権やアカウントに関して、ユーザーの身元チェックや管理者権限チェックを繰り返し実施すること。これには退職者によるアクセスの確認も含まれる
- 事業継続計画の演習

上述のステップ 2 の例では、ISAO のアナリストはメンバーの提供情報の内容を確認する。関連するファイルと通信を暗号化しておくことで、アナリストはデータの機密性が保持されていることを確信できる。

10.3 情報の保証—信頼性

セクション 5.4 では、レポートを分類するための標準モデルについて取り上げた。ほとんどの場合、メンバーの提供情報にはその情報源の組織を特定できるデータが含まれるため、これらのレポートは TLP Red に分類される。通常、技術的な脅威データを最大限得ながら、情報源を特定できるような情報は含めたとしても、提供情報の正当性を説明する最小限の範囲にとどめることで、信頼とインテリジェンスを共有する際の最大のメリットが得られる場合が多い。

データの暗号化手段と保存データのセキュリティ対策は、どちらも信頼モデルに寄与する。データの暗号化は、提供情報が信頼できる送信者から供給されたという一定の保証を提供し、提供情報の正当性に寄与する。保存データのセキュリティ対策は、インテリジェンスの情報源の属性を保護するのに有用である。

この方程式の最後の要素は ISAO アナリストチームであり、チームがインテリジェンスの機密解除と配布を従来どおりのやり方で行うことである。完成したインテリジェンス成果物を残りのメンバーに提供しようとする ISAO アナリストチームメンバーのあらゆる取り組みには、情報源を秘匿化（匿名化）すること、技術的な検知指標を検証して確認すること、そして最後に、一般的な影響と重大度を記述し、ガイダンスに信ぴょう性を与えることが含まれるべきである。最終的なインテリジェンス成果物が完成したら、電子メールや Web の暗号化技術を使用してメンバーに共有する。

10.4 機密性、完全性、および可用性

このセクションで概説した保護対策は、ISAO が組織内でリードすべき役割の一部に過ぎない。保護手順の詳細情報を定期的にメンバーに伝えること、技術的観点およびポリシーの観点での定期セキュリティ検討会を実施すること、およびメンバー組織と協力して継続的に発展していくことは全て、ISAO にとって重要である。

要約すると、機密性、完全性、および可用性は、転送データの暗号化、保存データの暗号化、バックアップ、およびファイルの完全性または可用性の監視と確認を活用することや、情報処理のベストプラクティスを厳密に実施することで達成できる。

付録 A—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):データを綿密に調査して悪意のある活動を特定し、それを既存の脅威情報に照らして評価することで、手持ちのデータについて有益な見解を示すこと。

異常(Anomaly):標準的な状態、通常の状態、または想定されていた状態から逸脱していること。

属性(Attribute):人物、または物事の特徴や固有の部分と見なされる特質や特性。データベース内のフィールドや、タグのプロパティ、表示される文字列の項目の性質を示す情報。

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。

ビッグデータ分析(Big data analytics):大規模で多岐にわたるデータセット(**ビッグデータ**)を調査する処理のこと。組織が十分な情報に基づいて意思決定を下せるよう、一見しただけでは分からないパターン、未知の関連性、市場動向、顧客の好みなどの役立つ情報を明らかにする。

キャンペーン(Campaigns):サイバーセキュリティにおいて、企業が利用す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。

クラスタリング(Clustering):ある複数のデータをその特性に基づいてグループ化し、類似点に準じて集約すること。

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):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 または computer incident response center、computer incident response capability とも呼ばれる。

クラウドソーシング(Crowd sourcing):大勢の人々が利用するサービスに登録し、情報や、タスクまたはプロジェクトへの協力を得ること。このようなサービスには有料のものと無料のものがあり、一般的にインターネット経由で提供される。

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。例としてハードウェアやソフトウェアの脆弱性、対応方針、警告などが挙げられる。

サイバーセキュリティ情報共有（Cybersecurity information sharing）：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

サイバー脅威情報（Cyber-threat information）：IT 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）。

データ（Data）：参照用や分析用に集積された事実や統計情報。

データセット（Data sets）：関連する情報のセットの集合。個別の要素から構成されているが、コンピュータで 1 つの単位として操作できる。

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。

強化されたサイバーセキュリティ情報（Enriched cybersecurity information）：より包括的なデータセットを生成するため、複数の異なるデータセットやストリームを組み合わせたサイバーセキュリティ情報。

イベント（Event）：ネットワーク内またはシステム内で発生した観測可能な事象。

フォールスネガティブ（False negative）：特定の脅威を検出するセキュリティツールが脅威を見逃してしまうこと。

フォールスポジティブ（False positive）：セキュリティツールが誤って正常なコンテンツを悪意のあるコンテンツとして分類してしまうこと。

フィード（Feeds）：1 つ以上のソースから現在の情報が更新されたことをユーザーに知らせるため、継続的に配信される構造化されたデータ。データフィードはデータの配信手法として表現されることが多い。例えば Rich Site Summary フィードは、XML ベースのファイル形式を使用して複数のソースからユーザーにコンテンツを配信する。

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や推奨される手法への侵害を緩和すること。

インシデント対応（Incident response）：「インシデントハンドリング」を参照。

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。

情報（Information）：何らかの意味が得られるよう処理されたデータのこと。

インテリジェンス（Intelligence）：米国内外で収集された、国家、国民、財産、権益への脅威、大量破壊兵器の開発、拡散、使用、あるいは米国の国家安全保障または国土安全保障に関わる他のあらゆる問題に関連する情報のこと。

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。

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。

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。

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。

運用分析（Operational analysis）：脅威、脆弱性、インシデント、および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）。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。

即時情報共有（Real-time information sharing）：「サイバーセキュリティ情報の自動共有」を参照。

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。

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。

ソーシャルエンジニアリング（Social engineering）：システムやネットワークの攻撃に使用されかねない情報（パスワードなど）を個人から詐取しようとする行為。

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、漏えい、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。［出典：MITRE 社、脅威情報構造化記述形式］。

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操作分析とのマージなど）。

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 B—略語

API　アプリケーションプログラミングインターフェース（application programming interface）

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（Critical Vulnerabilities Exposures）

DNS　ドメインネームシステム（Domain Name System）

IA　情報保証（information assurance）

IOC　侵害の検知指標（indicator of compromise）

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）

MISP　マルウェア情報共有プラットフォーム（Malware Information Sharing Platform）

PII　個人識別情報（personable identifiable information）

RDP　リモートデスクトッププロトコル（Remote Desktop Protocol）

SIEM　セキュリティ情報イベント管理（security information and event management）

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）