4. 連携と情報共有

現代の脅威や攻撃の性質から、インシデント対応中に組織が協力して取り組むことが、これまで以上に重要になってきています。組織は、インシデント対応活動の一部を適切なパートナーと効果的に調整するようにしなければなりません。インシデント対応における連携の最も重要な側面は情報共有であり、異なる組織が脅威、攻撃、および脆弱性の情報を相互に共有することで、各組織の知識が他の組織に利益をもたらすようにします。インシデント情報の共有は、同じ脅威や攻撃が複数の組織に同時に影響を与えることが多いため、相互に利益をもたらすことが多いです。

セクション 2 で述べたように、パートナー組織と情報を調整して共有することで、IT インシデントに効果的に対応する組織の能力を強化することができます。例えば、組織がネットワーク上で不審と思われる行動を特定し、そのイベントに関する情報を信頼できるパートナーに送信した場合、そのネットワーク内の他の誰かがすでに同様の行動を見ている可能性があり、シグネチャ、検索すべき他の指標、または是正措置の提案など、不審な行動に関する追加の詳細情報を提供して対応することができます。信頼できるパートナーとの連携により、組織は孤立して活動するよりも迅速かつ効率的にインシデントに対応することができます。

標準的なインシデント対応技術の効率性の向上だけが、組織間の連携と情報共有の唯一のインセンティブではありません。情報共有のもう一つのインセンティブは、特にその組織が中小規模の場合、単一の組織では利用できないかもしれない技術を使ってインシデントに対応できることです。例えば、小規模な組織がネットワーク上で特に複雑なマルウェアのインスタンスを特定した場合、マルウェアを完全に分析してシステムへの影響を判断するための社内リソースを持っていない可能性があります。この場合、組織は信頼できる情報共有ネットワークを活用して、マルウェアの分析を実行するのに十分な技術力を持つサードパーティのリソースに、このマルウェアの分析を効果的に外注することができるかもしれません。

このセクションでは、連携と情報共有に焦点を当てます。セクション 4.1 では、インシデント対応の連携の概要を示し、組織のインシデント対応プロセスを補完するための組織横断的な調整の必要性に焦点を当てています。第 4.2 節では、組織間で情報を共有するための技術について議論し、セクション 4.3 では、どのような情報を他の組織と共有するか、あるいは共有しないかをどのように制限するかを検討しています。

4.1 連 携

セクション2.3.4で議論されているように、組織は、インシデント対応活動を実施する過程で、いくつかのタイプの外部組織と相互作用する必要があるかもしれません。これらの組織の例としては、他のインシデント対応チーム、法執行機関、インターネットサービスプロバイダ、構成員及び顧客が挙げられます。組織のインシデント対応チームは、インシデントが発生する前に、これらの関係者とのインシデント連携を計画し、すべての関係者がそれぞれの役割を理解し、効果的なコミュニケーションラインを確立する必要があります。図 4-1 は、インシデント対応のライフサイクルの各段階で連携を行っている組織の例を示しており、連携がライフサイクル全体を通して価値あるものであることを強調しています。
 図4-1

4.1.1 連携の関係

組織内のインシデント対応チームは、調整する組織の種類に応じて、さまざまなタイプの調整に参加することができます。例えば、インシデント対応の技術的詳細を担当するチームメンバーは、複数の組織にまたがる攻撃を緩和するための戦略を共有するために、 パートナー組織の運用上の同種の部署と調整することがで

きます。あるいは、同じインシデントの間に、インシデント対応チームマネージャーは、必要な報告要件を満たすために ISAC と調整し、インシデントへの対応を成功させるためのアドバイスや追加のリソースを求めることができます。表 4-1 は、外部組織との連携時に存在する可能性のある連携関係の例をいくつか示しています。

表 4-1 連　携

カテゴリー	定義	情報共有
チームとチーム	チームとチームの関係は、異なる組織の技術的なインシデント対応者が、インシデント処理のライフサイクルのどの段階でも仲間と協力しているときにはいつでも存在する。このタイプの関係に参加している組織は、通常、互いに権限を持たない仲間であり、情報を共有し、リソースをプールし、知識を再利用して両チームに共通する問題を解決することを選択している。	チームとチームの関係で最も頻繁に共有される情報は、戦術的かつ技術的なもの（例えば、危殆化の技術的指標、提案された是正措置）であるが、準備段階の一部として実施される場合には、他の種類の情報（計画、手順、教訓）を含む場合もある。
チームと連携チーム	チームと連携チームの関係は、組織的なインシデント対応チームと、USCERT や ISAC のような連携されたインシデント対応と管理のための中心的なポイントとして機能する別の組織との間に存在する。このタイプの関係には、連携機関がメンバー組織からある程度の報告を要求することと、連携チームが参加メンバー組織にタイムリーで有用な情報を発信することを期待することが含まれる。	チームと連携チームは、戦術的、技術的な情報だけでなく、脅威、脆弱性、および連携チームの活動対象となるコミュニティへのリスクに関する情報を頻繁に共有する。また、連携チームは、リソースと注意をどこに集中させるかを決定するために、インシデントに関する具体的な影響情報を必要とすることもある。
連携チームと連携チーム	US-CERT や ISAC などの複数の連携チーム間の関係は、複数のコミュニティーに影響を及ぼす可能性のある横断的なインシデントに関連する情報を共有するために存在する。連携チームは、それぞれの地域社会のメンバー組織を代表して行動し、コミュニティー間の対応を支援するために、横断的なインシデントの性質と範囲、および再利用可能な緩和戦略に関する情報を共有している。	連携チームが相手チームと共有する情報の種類は、「定常状態」の活動中には定期的なサマリーで構成されることが多く、その間には、戦術的、技術的な詳細、対応計画、および連携されたインシデント対応活動中の影響やリスク評価に関する情報の交換が行われる。

組織は、連携に必要な人間関係を構築することが難しいと感じるかもしれません。コミュニティの構築は、組織が属する業界や、組織が活動している地理的な地域から始めるのが適しています。組織のインシデント対応チームは、自分の属する業界や地域内の他のチームと（チーム間のレベルで）関係を築こうとしたり、すでに情報共有を促進している業界内の確立された組織に参加したりすることができます。関係性を構築するためのもう一つの考慮点は、関係性には強制的なものと自発的なものがあるということです。例えば、チ

ーム間の関係は通常任意のものであるのに対し、チーム間の関係は強制的なものであることが多いです。組織が自発的な関係を追求するのは、相互の自己利益を満たすためです。強制的な関係は、通常、業界内の規制機関または別の組織または事業体等によって定義されます。

4.1.2 協定と報告要件

外部組織と情報を共有しようとする組織は、連携作業を開始する前に、法務部に相談すべきです。議論が行われる前に、制定する必要がある契約やその他の合意があるかもしれません。例としては、組織の最も機密性の高い情報の機密性を保護するための守秘義務契約（NDA）があります。また、組織は、インシデント情報を ISAC と共有したり、より高いレベルの CIRT にインシデントを報告したりするなど、報告に関する既存の要件も考慮すべきです。

4.2 情報共有のテクニック

情報共有は、組織間の連携を可能にするための重要な要素です。たとえ小規模な組織であっても、多くのインシデントに効果的に対処するためには、仲間やパートナーとインシデント情報を共有する必要があります。組織は、インシデントが完全に解決するまで待ってから他の人とインシデントの詳細を共有すのではなく、インシデント対応のライフサイクル全体を通してそのような情報共有を行うべきです。セクション4.3では、組織が他の人と共有することを望む場合と望まない場合があるインシデント情報のタイプについて論じています。

このセクションでは、情報共有のためのテクニックに焦点を当てます。セクション4.2.1ではアドホックな方法に、セクション4.2.2では部分的に自動化された方法に注目します。最後に、セクション4.2.3では、情報共有に関連するセキュリティ上の考慮事項について論じます。

4.2.1 アドホック※

ほとんどのインシデント情報の共有は、従来、電子メール、インスタントメッセージングクライアント、電話などのアドホックな方法で行われてきました。アドホックな情報共有メカニズムは、通常、パートナー組織のインシデント対応チームの従業員との個々の従業員のつながりに依存しています。従業員は、これらのつながりを利用して仲間と情報を手動で共有し、インシデントに対応するための戦略を構築するために仲間と連携します。組織の規模にもよりますが、このようなアドホックな手法は、パートナー組織と情報を共有するための最も費用対効果の高い方法かもしれません。しかし、アドホックな情報共有は非公式なものであるため、情報共有プロセスが常に機能することを保証できません。例えば、特にコネのある従業員がインシデント対応チームを辞めた場合、そのチームは一時的に、外部組織との効果的な連携のために頼りにしていた情報共有チャネルの大半を失う可能性があります。

また、アドホックな情報共有方法は、どのような情報が伝達され、どのように伝達されるかという点で、標準化されていないことがほとんどです。標準化されていないため、手動での介入が必要となり、部分的に自動化された方法よりも処理にリソースがかかる傾向があります。可能な限り、組織は、パートナー組織との正式な合意や、情報共有の部分的な自動化に役立つ技術的なメカニズムを通じて、情報共有戦略を正式なものにすることを試みるべきです。

※「特定の目的の」「その場限りの」という意味のラテン語

4.2.2 部分的な自動化

組織は、組織間の連携を効率的かつ費用対効果の高いものにするために、情報共有プロセスを可能な限り自動化することを試みるべきです。実際には、すべてのインシデント情報の共有を完全に自動化することは不可能であり、また、セキュリ ティと信頼性の観点からも望ましいことではありません。組織は、自動化された情報共有と、情報の流れを管理するための人間中心のプロセスとのバランスを取ることを試みるべきです。

自動化された情報共有ソリューションを設計する際には、組織はまず、パートナーとどのようなタイプの情報をやり取りするかを検討する必要があります。組織は、共有したいすべての組織や事業体等間の関係を列挙した正式なデータ辞書を構築したいと思うかもしれません。組織が共有する情報の種類を理解したら、この情報を取り込むための形式的で機械処理可能なモデルを構築する必要があります。可能な限り、組織は共有する必要のある情報を表現するために、既存のデータ交換標準を使用すべきです※。組織は、データ交換モデルを決定する際、パートナー組織と協力して、選択した標準がパートナー組織のインシデント対応システムと互換性があることを確認すべきです。既存のデータ交換モデルを選択する場合、組織は、インシデント対応領域の異なる側面をモデル化した複数のモデルを選択し、モジュール方式でこれらのモデルを活用し、ライフサイクルの特定の意思決定ポイントで 必要な情報のみを通信することを好むかもしれません。付録Eは、インシデント対応ドメインに適用可能なデータ交換モデルを定義する既存の標準の非網羅的リストです。

インシデント情報を共有するためのデータ交換モデルを選択することに加えて、組織は、パートナー組織と協力して、情報交換が自動化された方法で行われるための技術的な転送メカニズムに合意しなければなりません。これらのトランスポートメカニズムには、少なくとも、情報を交換するためのトランスポートプロトコル、情報リソースと通信するためのアーキテクチャモデル、および特定の組織で情報リソースにアクセスするための適用可能なポートとドメイン名が含まれます。例えば、パートナー組織のグループは、各組織のDMZ内の特定のドメイン名のポート 4590 のハイパーテキスト転送プロトコルセキュア（HTTPS）を介してIODEF/Real-Time Inter-Network Defense（RID）データを交換するために、REST（Representational State Transfer）アーキテクチャを使用してインシデント情報を交換することを決定することができます。

※ National Technology Transfer and Advancement Act (NTTAA)によると、「すべての連邦政府機関および省庁は、自主的なコンセンサス基準機関によって開発または採択された技術基準を使用しなければならない」とされています。詳細は http://standards.gov/nttaa.cfm を参照のこと。

4.2.3 セキュリティに関する考慮事項

インシデント対応チームが情報共有を計画する際にセキュリティ上の考慮事項がいくつかあります。一つは、インシデント情報のどの部分を誰が見ることができるかを指定できることです（例えば、機密情報の保護）。また、インシデント情報から前兆、兆候、およびその他の技術情報の情報を乱すことなく、センシティブなデータの断片を除去するために、データのサニタイズまたはスクラビングを行うことも必要かもしれません。また、インシデント対応チームは、他の組織がチームと共有した情報を保護するために必要な措置が取られていることを確認する必要があります。

また、データ共有に関して考慮すべき多くの法的問題もあります。追加情報については、セクション4.1.2を参照のこと。

4.3 粒度の高い情報の共有

組織は、情報共有の利点と機密情報を共有することの欠点のバランスをとる必要があり、理想的には、必要な情報を共有し、必要な情報のみを適切な関係者と共有する必要があります。組織は、インシデント情報を、ビジネスに影響を与える情報と技術的な情報の2つのタイプで構成されていると考えることができます。ビジネスに影響を与える情報は、セクション4.1.1で定義されているように、チームと連携チームの関係の中で共有されることが多いですが、技術的な情報は、3つのタイプの連携関係の中で共有されることが多いです。このセクションでは、両方のタイプの情報について説明し、詳細な情報共有を実行するための推奨事項を提供します。

4.3.1 ビジネスへの影響情報

ビジネスへの影響情報には、ミッションへの影響、財務上の影響などの観点から、インシデントが組織にどのような影響を与えているかが含まれます。このような情報は、少なくとも概要レベルでは、インシデントによって引き起こされた損害の推定値を伝えるために、より高いレベルの連携対応チームに報告されることが多いです。連携対応チームは、報告組織に提供すべき支援の程度に関する意思決定を行うために、この影響情報を必要とする場合があります。また、連携チームは、特定のインシデントが自分たちが代表するコミュニティの他の組織にどのような影響を与えるかを決定するために、この情報を使用することもあります。

連携チームは、メンバー組織に対し、ある程度のビジネスへの影響情報の報告を要求することがあります。例えば、連携チームは、第3.2.6項で定義されたカテゴリーを使用して、影響情報を報告することをメンバー組織に要求することができます。この場合、ある組織は、仮想的なインシデントについて、機能的影響は「中程度」、情報的影響は「なし」、 回復可能時間の延長が必要であると報告することになります。この高レベルの情報は、メンバー組織がインシデントから回復するために、ある程度のレベルの追加リソースを必要とすることを連携チームに警告します。連携チームは、その後、メンバー組織との追加コミュニケーションを追求し、インシデントについて提供された技術情報に基づいて、どの程度のリソースが必要か、また、リソースの種類を決定することができます。

ビジネスへの影響情報は、インシデントが発生した組織の使命を確実にすることに何らかの関心を持つ組織に報告するためにのみ有用です。多くの場合、インシデント対応チームは、明確な価値提案や正式な報告要件がない限り、外部組織とのビジネスインパクト情報の共有を避けるべきです。同業者やパートナー組織と情報を共有する場合、インシデント対応チームは、セクション4.3.2で概説されているように、技術的な情報の交換に焦点を当てるべきです。

4.3.2 技術情報

組織内でのインシデントの発生を示す技術的な兆候には、さまざまな種類があります。これらの兆候は、攻撃するホストのホスト名や IP アドレス、マルウェアのサンプル、類似のインシデントの前兆や兆候、インシデントで悪用された脆弱性の種類など、インシデントに関連するさまざまな技術情報に由来しています。セクション 3.2.2 では、進行中のインシデントを特定するために、組織がこれらの兆候をどのように収集し、活用すべきかの概要を説明しています。さらに、セクション 3.2.3 では、インシデント兆候データの一般的な情報源のリストを提供します。

組織は、独自の内部兆候を収集することで価値を得ますが、パートナー組織から受け取った兆候を分析したり、外部の分析・利用のために内部兆候を共有したりすることで、さらなる価値を得ることができます。組織が見ていないインシデントに関連する外部兆候データを受け取った場合、その兆候データを使用して、インシデントが発生し始めた時点でそのインシデントを特定することができます。同様に、組織は、特定の兆候データを取得するための内部リソースが不足しているために気づかなかった進行中のインシデントを検出するために、外部兆候データを使用することができます。組織は、内部兆候データを外部組織と共有することでも利益を得られます。例えば、組織が経験しているインシデントに関連する技術情報を共有した場合、パートナー組織は、そのインシデントに対処するための改善策を提案して対応することができます。

組織は、このような情報を可能な限り共有すべきです。しかし、組織が悪用された脆弱性の詳細を明らかにしたくない理由には、セキュリティ上の理由と 責任上の理由があるかもしれません。攻撃の一般的な特徴や攻撃するホストの身元などの外部指標は、通常、他の人と共有しても安全です。組織は、どのような種類の技術情報を様々な関係者と共有すべきか、あるいは共有すべきでないかを検討し、適切な情報を可能な限り他の組織と共有するように努めなければならりません。

技術的兆候データは、組織が実際のインシデントを特定できる場合に役立ちます。しかし、外部ソースから受け取ったすべての兆候データが、それを受け取った組織に関係するわけではありません。場合によっては、この外部データは、受信した組織のネットワーク内で誤検知を発生させ、存在しない問題にリソースが費やされる可能性があります。

インシデント情報の共有に参加している組織は、共有コミュニティから技術的兆候情報を取得し、その情報を企業全体に、できれば自動化された方法で発信することに長けたスタッフを持つべきです。また、組織は、実際のインシデントを意味すると比較的高いレベルで確信できる兆候のみを共有するように努めるべきです。

4.4 推奨事項

本セクションでは、インシデントへの対応に関する主な推奨事項を以下にまとめています。

■ インシデントが発生する前に、外部関係者とのインシデント連携を計画する。
外部関係者の例としては、他のインシデント対応チーム、法執行機関、インターネット・サービス・プロバイダー、および構成員や顧客が挙げられます。この計画は、すべての関係者がそれぞれの役割を理解し、効果的なコミュニケーションラインが確立されていることを確認するのに役立ちます。

■ 連携作業を開始する前に、法務部に相談する。
協議を行う前に、契約やその他の合意が必要な場合がある可能性があります。

■ インシデント対応のライフサイクル全体を通して、インシデント情報の共有を行う。
情報共有は、組織間の連携を可能にするための重要な要素です。組織は、インシデントが完全に解決するのを待たずに、他の連携チームとインシデントの詳細を共有すべきです。

■ 情報共有プロセスを可能な限り自動化させる。
これにより、組織横断的な連携が、効率的かつ費用対効果の高いものになります。組織は、自動化された情報共有と、情報の流れを管理するための人間中心のプロセスとのバランスを図るべきです。

■ 情報共有の利点と、機密情報を共有することの欠点とのバランスをとる。
理想的には、組織は必要な情報を適切な関係者と共有し、必要な情報のみを共有すべきです。ビジネスに影響を与える情報は、チームと連携チームの関係で共有されることが多いですが、技術的な情報は、あらゆる

種類の連携関係の中で共有されることが多いです。同業者やパートナー組織と情報を共有する場合、インシデント対応チームは技術情報の交換に重点を置くべきです。

■ 適切なインシデント情報を可能な限り他の組織と共有する。

組織は、どのタイプの技術情報を様々な関係者と共有すべきか、あるいは共有すべきでないかを検討すべきです。例えば、攻撃の一般的な特徴や攻撃するホストの身元などの外部指標は、通常、他の人と共有しても安全ですが、組織が悪用された脆弱性の詳細を明らかにしたくない理由として、セキュリティ上の理由と責任上の理由の両方があるかもしれません。