公開資料

セキュリティ対応組織(SOC/CSIRT)強化に向けた サイバーセキュリティ情報共有の「5W1H」

第 2.0 版

2019 年 4 月 4 日

NPO 日本ネットワークセキュリティ協会

日本セキュリティオペレーション事業者協議会 （ISOG-J）

公開資料

改版履歴

2017/10/27	初版作成
2019/4/4	第 2.0 版作成

目次

1. はじめに 1
1.1.背景 1
1.2.課題認識と本書の目的 1
2. Why と When 3
3. What 5
3.1.脆弱性情報の What 5
3.1.1. 初動対応要否判断 5
3.1.2. 検知と分析 6
3.1.3. 封じ込め/根絶/復旧 7
3.1.4. 準備 7
3.1.5. 事件後の対応 7
3.2.攻撃関連情報の What 8
3.2.1. 初動対応要否判断 8
3.2.2. 検知と分析 8
3.2.3. 封じ込め/根絶/復旧 10
3.2.4. 事件後の対応 10
3.3.実際のセキュリティ対応事例の What 11
4. 受信者側の Who と How 13
5. 発信者側の Who と How 14
6. Where 15
7. 情報を受け取った時の事例とフロー 17
7.1.脆弱性情報の場合 17
7.1.1. 脆弱性情報を受け取った場合のフロー 18
7.1.2. 各フェーズの 5W1H 19
7.2.攻撃関連情報の場合 27
7.2.1. 攻撃関連情報を受け取った場合のフロー 27
7.2.2. 各フェーズの 5W1H 27
8. 情報共有が逃れられない根本的な制約 37
9. おわりに 39

1. はじめに

1.1. 背景

サイバーセキュリティの対応における「情報共有」については、経済産業省の「サイバーセキュリティ経営ガイドライン」[1]やサイバーセキュリティ戦略本部の平成 29 年第 12 回会合「サイバー攻撃に係る情報の収集・分析・共有について」[2]などで、その重要性が説かれている。これは多様化・複雑化する攻撃者側のスピードに個々の組織が対応することは難しく、企業や組織の防御すべき側の環境（クラウドの活用、在宅勤務などの働き方、IT だけではなく OT(Operational Technology)も含めた環境）が年々複雑になり、防御側も目的を同じとする企業・組織が協力して対応する必要が出てきているためである。

実際の取り組みとして JPCERT/CC の早期警戒情報や IPA の J-CSIP、日本サイバー犯罪対策センター（JC3）、民間の ISAC や日本シーサート協議会(NCA)などで情報共有の場が整備され、運用されている。

本書ではこれらの場において情報共有を行う際の考え方を示す。

1.2. 課題認識と本書の目的

ここで、「情報共有」の大きな流れをおさらいしたい。

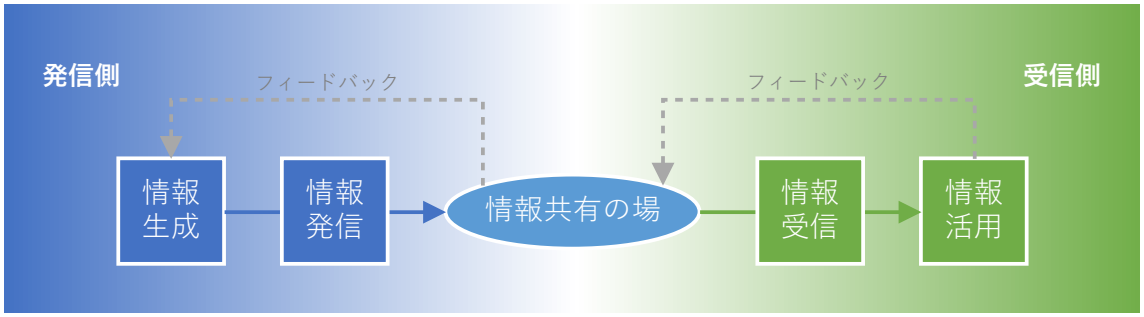

図 1　情報共有の流れ

情報を発信したいと思った側が、情報を生成し、情報共有の「場」へ発信、そしてその情報を利用したいと思っている受信側において、情報をキャッチし、活用していくというのが基本的な流れである。

[1] https://www.meti.go.jp/policy/netsecurity/mng_guide.html
[2] https://www.nisc.go.jp/conference/cs/dai12/pdf/12sankou.pdf

前述したとおり、様々な場面で情報共有の「場」が設けられてきているものの、その前後における過程はまだまだ成熟している状況とは言えず、情報発信そのものが不足していることや、共有された情報をセキュリティ対応に生かし切れていないという課題がある。

その一因は、次に示す「5W1H」の観点が整理されないまま「情報共有」というキーワードだけが先行している実態にあるのではないだろうか。

	発信側	受信側
Why	何を目的に	何を目的に
When	どのようなタイミングで	どのようなタイミングで
What	何の情報を	何の情報を
Where	どの情報共有の場において	どの情報共有の場から得て
Who	誰が	誰が
How	どのように	どのように
	発信するのか	活用するのか

表 1 サイバーセキュリティ情報共有における 5W1H

情報はそれを取り扱う人や役割によって必要となるものが異なることがある。セキュリティの情報としては技術的な情報ばかりではなく、その背景となる国家間の状況なども含み経営判断で利用されるインテリジェンスも活用されることもある。ここではセキュリティ対応組織として SOC や CSIRT のセキュリティ技術者が利用する「情報」について記載をする。

本書においては、この「サイバーセキュリティ情報共有における 5W1H」について、順を追ってその考え方をまとめる。様々な場面で行われている「情報共有」において、「情報発信」と「情報活用」活発化の参考となれば幸いである。

2. WhyとWhen

何を目的として情報共有するのかという「Why」と、その情報をどのようなタイミングで発信あるいは活用するのかという「When」は密接な関係にある。それは、セキュリティ対応の流れとリンクするからである。

NISTが発行するSP800シリーズのSP800-61「コンピュータセキュリティ・インシデント対応ガイド」を参考にすると、インシデント対応は主に「準備」「検知と分析」「封じ込め/根絶/復旧」「事件後の対応」の4つのフェーズに分かれる。

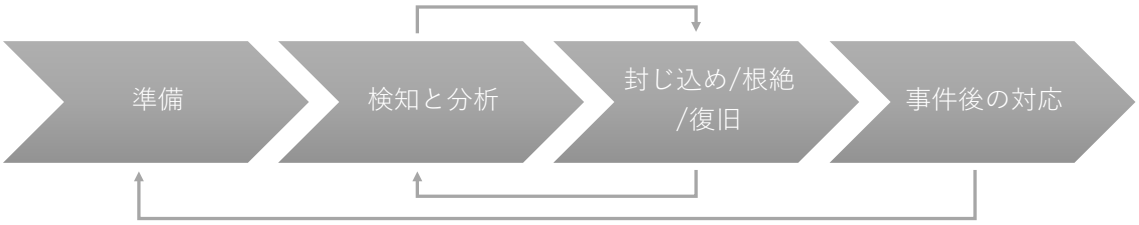

図 2　インシデント対応ライフサイクル

これはあくまで「インシデント対応」の流れであり、「情報共有」を起点として考えた場合、大きく変化する点が二つある。

一つ目は、「インシデント」は原則として対応しなければならないものであるが、共有された情報は対応が必要とは限らないという点である。例えばApache Struts2の脆弱性情報が共有されたとしても、そもそもそれを使用していなければ具体的な対応は不要である[3]。つまり、共有された情報を元に何らかの初動対応を取るかどうかを判断するフェーズが追加される。

二つ目は、当然と言えば当然であるが、攻撃の情報が世の中に存在しているからと言って、自組織でインシデントが発生しているとは限らない点である。インシデントが発生していない場合、「封じ込め/根絶/復旧」というフェーズは存在しない。

これら二点を加味すると、情報共有を出発点としたセキュリティ対応は次のようなフロ

[3] 「対応は不要と判断する」という対応をしていると捉えることもできるが、ここでは質の違いに着目して、異なる対応フェーズへの移行が伴うものと考える。

ーチャートとなる。

図 3　情報共有を出発点としたセキュリティ対応

このフローチャート上のどのフェーズ（「When（タイミング）」）で利用されるためのものなのかが、そのまま情報共有の「Why（目的）」となる。

情報共有の「Why（目的）」は、

- 初動対応要否判断
- 検知および分析
- 封じ込め/根絶/復旧
- 準備（予防）
- 事件後の対応

のいずれかを行うためのものであり、それぞれの「When（タイミング）」で使用する情報を収集すればよいということになる。上からその時期が早く訪れる順に記載しているが、上位のものほど、情報の網羅性よりも、判断に必要な最低限の情報をいかに早く発信/収集するかが重要になる。

3. What

では具体的に「What（何の情報）」を収集すればよいのか。前章でまとめた「Why（目的）」を意識すると整理しやすい。

ここでは情報共有で良く扱われる下記の三点について、具体的な事例を交え説明する。

- 脆弱性情報
- 攻撃関連情報
- 実際のセキュリティ対応事例

全ての情報が完全な状態で共有される必要はなく、「Why（目的）」「When（タイミング）」に合った情報を発信、収集できることが肝要である。

3.1. 脆弱性情報の What

脆弱性情報とは、悪意のある攻撃者が標的とするソフトウェアやハードウェアの不具合について、セキュリティ機関や関係者が公開した情報全般を指すものとする。共有された脆弱性情報はそれぞれの企業にとって脅威になるものと、そうではないものが存在するため、共有された内容を理解、把握する必要がある。

3.1.1. 初動対応要否判断

このフェーズでは何が必要となるだろうか。脆弱性の対応においては、具体的にどの脆弱性か明確にし、その対象となるシステムが存在するかどうかが対応要否の分岐となる。よって、下記のような事項が必要である。

- 脆弱性識別子（CVE やパッチ番号など）
- 脆弱性の対象となる
  - システム種別
  - バージョン
  - 条件（システム構成、設定など）
- 各セキュリティ製品における対応状況

条件が明らかになっていない、あるいは自システムの設定が不明といった場合は、バージョン情報までで対応要否を判断するのが一般的である。各セキュリティ製品の対応状況によってもその後の対応要否が変わる可能性があるため、確認できる場合は情報を得ておくことが望ましい[4]。

3.1.2. 検知と分析

対象となるシステムが存在し対応が必要と判断された場合、攻撃を検知する監視の実施と、被害の有無について分析する必要がある。その場合には下記の情報が役に立つ。

- 攻撃の特徴
  - 攻撃形態、関連する通信の内容
  - 核心となる攻撃コード
- 攻撃によって残る痕跡
  - 被害を受けた後の通信内容
  - サーバやクライアントに残るログ
  - サーバやクライアントに残るその他の特徴
- 各セキュリティ製品における検知名
- 上記が不明な場合、自身で調査するための PoC（Proof of Concept）[5]

なお、PoC は高度な技術力を持つセキュリティ人材を必要とするため、必ずしも扱われるものではない[6]。

[4] 初動時点では、製品ベンダーやセキュリティサービス提供事業者もパターンファイルやシグネチャ作成の真最中で情報が出せない、あるいはユーザからの問合せが殺到して対応しきれないなどのケースは実際に発生する。よって、この情報がなければ次のアクションに移れない、というような対応フローは避けるのが賢明である。
[5] 脆弱性を実証するためのプログラムのこと。
[6] さらに高度な技術力を持つセキュリティ人材がいる場合には、自ら脆弱性を見つけ出したり、ソフトウェア修正パッチの情報から自ら PoC を作り出せたりする場合もあるが、よりレアケースである。

3.1.3. 封じ込め/根絶/復旧

攻撃や被害が発生していた場合は、その封じ込めと根絶、復旧が必要となる。そのために必要となるのは下記のような情報である。

- 攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件
- 攻撃を無効化する方法（パッチの適用、設定変更など）
- 被害を受けたシステムの復旧方法

3.1.4. 準備

攻撃や被害が発生していない場合は、先んじて行うべき対応を見出す必要がある。これは「封じ込め/根絶/復旧」に準ずることとなる。

3.1.5. 事件後の対応

「3.3 実際のセキュリティ対応事例の What」にてまとめる。

3.2. 攻撃関連情報の What

「攻撃関連情報」は、ここでは、例えば「WannaCry が流行っている」「標的型攻撃が発生している」「DDoS の予告が出ている」という情報やセキュリティベンダーから出ている攻撃解析レポートなど、攻撃に関連する情報全般を指すものとする。しかし、どのような情報ソースであろうと「Why（目的)」は決まっているので、その目的を果たせる内容かどうか確かめて必要な情報を抜き出せばよい。

3.2.1. 初動対応要否判断

攻撃関連情報の場合、下記のような事項が判断に役立つ。

- 該当の攻撃情報を示す名称（攻撃名称、マルウェア名、事件名など）
- 攻撃のターゲット
- 攻撃ベクター[7]

脆弱性情報とは異なり一意に決まる識別子がない場合があるが、関係者が理解できる何らかの名称を設定する必要がある。

また、脆弱性のように対象の有無を明確に線引きできず、多くは「要対応」と判断することになるかもしれない。例えば「東欧諸国を狙った標的型攻撃」のように攻撃者のターゲットが明らかになっている場合、その情報から対応不要あるいは対応優先度を下げるなどの判断ができる。また、攻撃ベクターがはっきりすれば、「この攻撃はインターネットから来るが、このシステムはクローズドネットワーク内なので対応不要」というような判断をすることもできる。

3.2.2. 検知と分析

脆弱性情報の時と同様、攻撃を検知する監視の実施と、被害の有無について分析する必要がある。

- 攻撃の特徴
  - 攻撃の通信内容

[7] 攻撃がどこから進行してくるか。例えばマルウェアの感染経路など。

- 核心となる攻撃コード
- 攻撃に関わる HTTP 関連のインジケーター
  - IP アドレス
  - ドメイン
  - FQDN
  - URL

- 攻撃に関わるメール関連のインジケーター
  - メール件名
  - メール本文
  - メール本文に含まれる URL
  - 添付ファイルの情報
    - ファイル名
    - 拡張子
    - ハッシュ値
    - 内容
- その他のプロトコルにおける特徴、インジケーター
- 攻撃を受けた場合の痕跡
  - 攻撃を受けた後の通信内容
  - サーバやクライアントに残るログ
  - サーバやクライアントに残るその他の特徴
  - 攻撃に関連する悪性コンテンツの情報
    - ファイル名
    - フォルダ・ディレクトリパス

- ✧ プロセス名
- ✧ ハッシュ値
- ✧ レジストリ変更内容
- ✧ 検体（悪性コンテンツそのもの）[8]

- 各セキュリティ製品における検知名

もちろん、これら以上に詳細な情報も存在するが、それらの情報を理解して活用できる体制が無ければ宝の持ち腐れとなる。「自組織が活用できる情報は何か」をしっかり把握し、効率的に情報収集することが推奨される。

3.2.3. 封じ込め/根絶/復旧

攻撃や被害が発生していた場合は、その封じ込めと根絶が必要となる。そのために必要なのは脆弱性情報の時と同様に、下記のような情報である。

- 攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件
- 攻撃を無効化する方法（パッチの適用、設定変更など）
- 被害を受けたシステムの復旧方法

3.2.4. 事件後の対応

「3.3 実際のセキュリティ対応事例の What」にてまとめる。

[8] 検体の取り扱いは危険を伴うため、厳格なルールを定め、その役割を担う一定のスキルを持ったメンバーによって、厳重な管理のもとに活用する必要がある。

3.3. 実際のセキュリティ対応事例の What

実際のセキュリティ対応事例とは、組織や企業が自身に発生したセキュリティ事象やその対応方法を「事件後の対応」として取りまとめたものになる。

ここまで言及してきた脆弱性情報や攻撃関連情報に関して、一次情報源の発信者となるのは一般的な組織においては難しいかもしれない。しかし、組織としての実際の対応事例は下記の観点を意識することで、誰でも発信者となることができる。

- 初動対応要否判断
  - いつどこから情報を得たか
  - どのように対応要否を判断したか（プロセス、ルールなど含めたその時の状況）
- 検知と分析
  - 攻撃や被害の有無を確認した具体的な方法（どのログをどのような条件で探した、具体的にこんな痕跡があった、など）
  - 攻撃や被害についての数値データ（攻撃発生数、被害端末数など）
- 封じ込め/根絶/復旧と準備（予防）
  - 実際に行った対応内容（システムにどんな設定を行ったか、どのセキュリティ製品にどんな設定を行ったか、など）
  - 対応した結果の数値データ（対応数、対応完了率など）
- 対応全体通して
  - うまくいった点
  - うまくいかなかった点
- 今後の具体的な改善ポイント

これらの情報は、次のセキュリティ対応事案に備えるために有用であるとともに、CISO など重要関係者へインプットする基礎情報にもなる。すべての項目が埋まらないケースもあるだろうし、組織を越えて開示することは難しい内容も多いだろう。しかし、可能な範囲で内外の組織へ情報共有すれば、貴重な情報となるはずである。また、開示した内容に対し

て類似した経験をもつ組織からフィードバックをもらえることもあるだろう。

4. 受信者側の Who と How

共有された情報を有効に活用し、対応していくためには、「Who（誰が）」「How（どのように）」行動するのかは事前に取り決めておかなければならない。

ここでは「Why（目的）」ごとに、「セキュリティ対応組織の教科書」[9]で記述されているどの機能・役割にあたるかを列挙する。自組織に置き換え、具体的な「Who（誰が）」「How（どのように）」を考えてみてほしい。

- 初動対応要否判断
  - 「A-2. トリアージ基準管理」「A-3. アクション方針管理」に従い判断する。着手後は「E-3. 脆弱性管理・対応」によって組織的に対応していく。
- 検知と分析
  - 「B. リアルタイムアナリシス（即時分析）」を行い、より詳細な調査が必要な場合は「C. ディープアナリシス（深掘分析）」へ進む。
- 封じ込め/根絶/復旧
  - 実害があった場合はインシデントとなる。「D. インシデント対応」を実施する。
- 準備（予防）
  - 今後被害が発生しないようにするため、「G. セキュリティ対応システム運用・開発」の機能が中心となり、具体的な対策を実装する。改めて「E. セキュリティ対応状況の診断と評価」を行うと、より万全な準備ができるだろう。
- 事件後の対応
  - 「F. 脅威情報の収集および分析と評価」において、実施した対応内容を客観的に評価し、改善を実施する。対応に問題が多かった場合には、「A. セキュリティ対応組織運営」の中で抜本的な運営体制の見直しが必要なのかもしれない。さらにもう一つ大切なのは、「I. 外部組織との積極的連携」を促進するために自身が発

[9] http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

信者となっていくことである。成功談と失敗談、どちらも非常に価値のある情報である。

5. 発信者側の Who と How

情報発信する際に登場する「Who（誰が）」は、概ね下記にまとめられる。

1. 実際に情報発信を行う者
2. 発信内容を承認する者
3. 発信後の状況を観察する者
4. 発信した情報に責任を持つ者

セキュリティ対応組織からの情報発信を考えるにあたっては、必要以上の情報が出てしまうことや、発信した情報がもとでいわゆる「炎上」が起こることを避けなければならない。「1」と「3」、「2」と「4」は同一の人物（あるいは役職）でも構わないが、全てを一人が担うのは、管理統制の観点から推奨しない。情報発信に当たっては、プロセスやルールを設け、スムーズに運営できるよう事前にしっかり計画しておくことが重要である。そのルールには「How（どのように）」も組み込んでおく必要があり、特に下記の点を意識する必要がある。

- どのような情報を
- どのような開示範囲で
- どのような伝達手段で
- どのような形式で

これらは「Where（どの情報共有の場において）」に強く依存するため、情報発信先の「場」を想定し、情報発信のルールを定めておくとよい。特に組織外へ発信する情報（Global Threat Intelligence）と、組織内でのみ流通させる情報（Local Threat Intelligence）を区別し、情報共有の場において、必要な情報が必要な範囲内で活用されるようにルール化することが大切である。そのためには、組織外での情報共有では TLP（Traffic Light Protocol）

[10]の活用や、組織内であれば、ISMS で規定されているような情報ラベルの付与などの工夫も必要となる。

6. Where

情報共有の場（Where）は様々だが、一般的には下記のいずれかに分類されるのではないだろうか。

- 組織内
  - 所属部署内
  - 自組織内の関係部署
  - 上層部
- 組織外
  - 関連会社（親会社・子会社）、関連組織
  - アウトソーサー
  - 各種団体（NCA、各種 ISAC など）
  - 一般公衆

この「Where」のうち、どの場を発信対象とするのか、あるいはどの場を受信元とするのか具体的にリストアップしておくことが大切である。初めから色々な場へ発信するのは難しいかもしれないが、関係の深い範囲で実績を作り、徐々に外へと共有範囲を広げていけるよう「Who」と「How」も整理しながら進めていくことが推奨される。また、「一般公衆」からの情報[11]については、適切な「場」に情報を集めるために組織としての受付窓口等を設け、その存在を対外的に明らかにしておく必要もある。

情報収集の際は「Where」に合わせ「How」を明確にしておく必要がある。目的を定めない情報収集は際限なく実施することができ、収集する行為ばかりに時間を費やしてしまうことになる。情報を集めすぎて取捨選択できなくなったり、情報に踊らされてしまったりしないよう、自組織が確実に活用できる範囲に集中するべきである。そして、被害の有無や大

[10] https://en.wikipedia.org/wiki/Traffic_Light_Protocol
参考：https://www.nisc.go.jp/conference/seisaku/kihon/dai9/pdf/9siryou_ref04.pdf

[11] 第三者からの申告、通報、通達あるいは報道など。

小に関係なく情報を積極的に発信することが重要であり、可能な限り広く情報共有が行われるような風土を作ることが、それぞれの「場」において求められる。

7. 情報を受け取った時の事例とフロー

ここまで情報共有についての現状の課題や解決に向けた方策を提示した。ここでは実際に情報を共有されて受け取った場合の事例とフローについて具体化する。脆弱性情報の場合と攻撃関連情報の場合の 2 つのパターンを示す。

7.1. 脆弱性情報の場合

脆弱性情報を受け取った場合として、Struts と Drupal のケースを比較しつつ紹介する。Struts のケースではある程度これまでに経験もあるため対応が理解しやすいと思われるが、比較して Drupal の脆弱性が現れた際には現場の混乱もみられた。それぞれにどんな違いがあったかも含めて例示を行う。

7.1.1. 脆弱性情報を受け取った場合のフロー

全体のフローチャートを描くと下記のようになる。フローは個別の事例をすべて網羅するわけではなく、汎用的なものとして記載した。個別の事例や各組織のすでにあるフローによっては異なる部分も存在する。

フローは別紙として添付しており、拡大してみる場合はそちらを参照いただきたい。

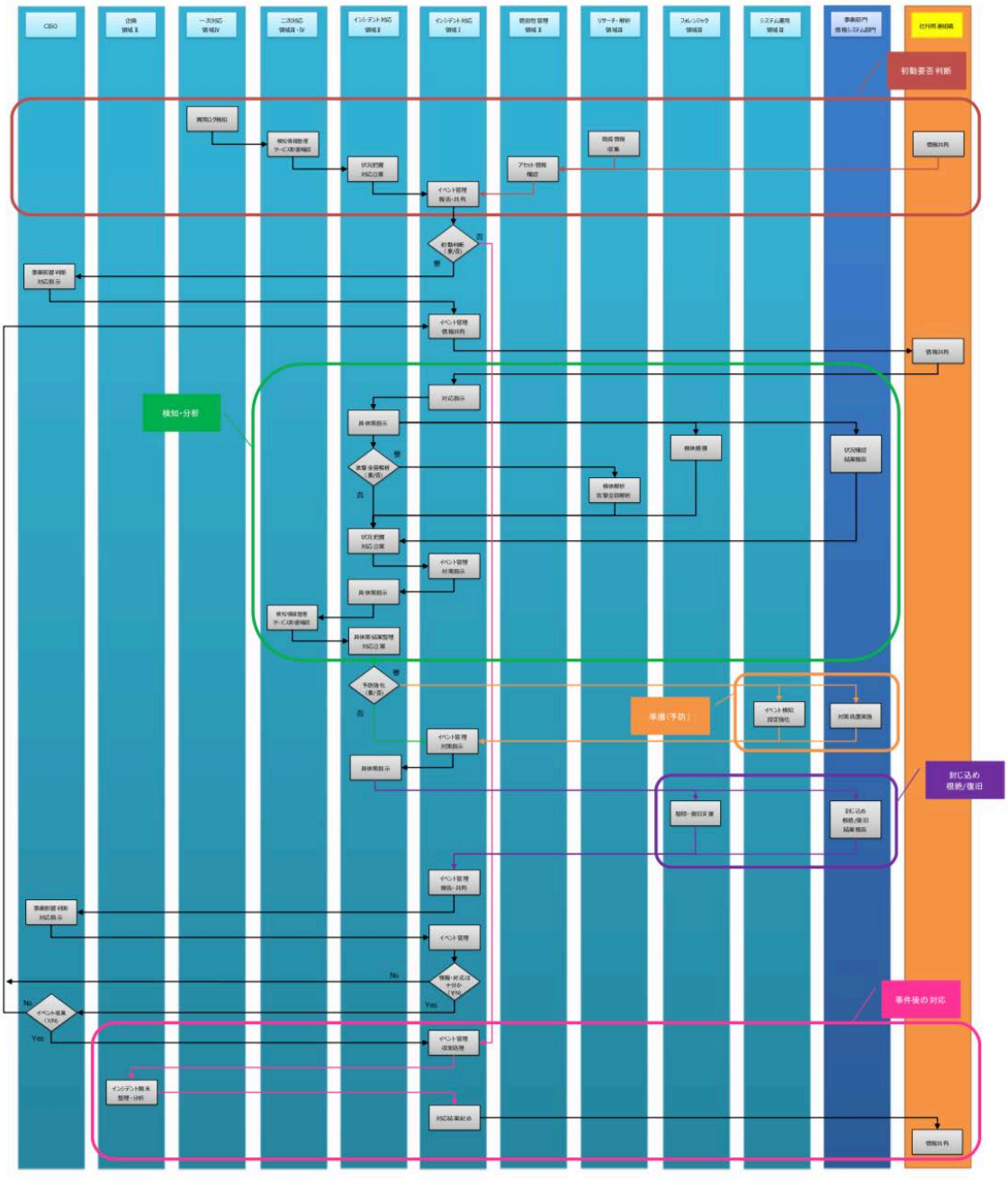

図 4 情報共有のフロー

7.1.2. 各フェーズの 5W1H

全体のフローから、各フェーズでの 5W1H がどうなるのかを例示する。

初動対応要否判断

Why は初動要否判断のため、When は共有された情報を受け取った直後の初動要否判断を行うフェーズである。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[12]を参考に各機能の担当として例示する。

D. インシデント対応

起きてしまったインシデントに対し、脅威の拡散抑止や、原因となったシステムを安全に復旧し脅威を排除する役割

E. セキュリティ対応状況の診断と評価

脆弱性診断や標的型メール訓練などによりセキュリティレベルを適切に維持・向上できているかを評価する役割

F. 脅威情報の収集および分析と評価

ネット上のセキュリティニュースやこれまで自組織で見つけたインシデントを取りまとめ、次に生かす役割

[12] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

- What

	Struts	Drupal
脆弱性識別子 (CVE やパッチ番号など)	CVE-2017-9805[13] （2017/9/6）	CVE-2018-7600[14] （2018/3/28）
脆弱性の対象となる システム種別	Web アプリケーションフレームワーク（ミドルウェア）	CMS（ミドルウェア）
バージョン	2.1.2 から 2.3.33 までのバージョン、および 2.5 から 2.5.12 までのバージョン	7.58, 8.5.1 より前 サポート終了の 6 系、8.3.x, 8.4.x も影響
条件 （システム構成、設定など）	該当するバージョン Struts REST Plugin を有効化して XML によるリクエストを受け付けている	該当するバージョン
セキュリティ製品における対応状況	・設定による緩和策あり ・1 週間程度で WAF 各社から対応の発表あり [15][16][17][18]	・緩和策なし ・1 週間程度で WAF 各社から対応の発表あり（カスタムシグネチャの提供もあり[19]）

初動要否判断において、Struts と Drupal ともに CVE 番号とともに情報が出た際には必要な情報に大きな差はなかった。

バージョンアップの対象となるかどうかについては公表されており、対応可否の判断に必要な情報はあった。

その他の情報として、Struts の場合は条件が設定により緩和されることが示されていた。

- How

上記 What で集められた情報と社内で検知している情報によってイベントとして管理を行い、「A-2. トリアージ基準管理」「A-3. アクション方針管理」に従い判断する。着手後は「E-3. 脆弱性管理・対応」によって組織的に対応していく。

---

13 https://www.ipa.go.jp/security/ciadr/vul/20170906-struts.html
14 https://www.ipa.go.jp/security/ciadr/vul/20180329-drupal.html
15 https://www.imperva.com/blog/cve-2017-9805-analysis-of-apache-struts-rce-vulnerability-in-rest-plugin/
16 https://www.scutum.jp/information/technical_articles/apache_struts.html
17 https://jpn.nec.com/infocage/siteshell/apachestruts2_20170914.html?
18 https://www.shadan-kun.com/news/datail20170906.html/
19 http://www.intellilink.co.jp/article/vulner/180424.html

対応に差が出たポイントの考察として、Struts は開発で利用していたことやこれまでの経緯から対応に慣れていたことが挙げられる。一方、Drupal は CMS(Content Management System)であるため、利用有無の状況やバージョンの確認などの把握が遅れたと考えられる。

初動要否の判断をどのように行うかにおいて、対象となる脆弱性を持つソフトウェアを利用しているのか、どこに対象のサーバが存在するのか、どのようにバージョンアップをするか、サイトの再開やリリースに向けた必要なチェックは何を確認すべきであるかといったスムーズな対応ができるように普段から確認や訓練を行っておきたい。

検知および分析

Why は検知および分析のため、When は初動要否判断の後に影響が出ていないかを調べるタイミングのフェーズである。

ここでの検知および分析については、初動要否判断において初動が必要となった場合に、今の状況で検知ができているか、組織に影響が出ているか、攻撃が成功しているかなどを確認して分析をするフェーズである。

まだ攻撃が来ていない、もしくは成功していないと判明した場合は、準備/予防フェーズに進み、攻撃が来ていて成功しているなどが判明した場合は封じ込め/根絶/復旧フェーズに進むことになる。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[20]を参考に各機能の担当として例示する。

B. リアルタイムアナリシス（即時分析）

セキュリティ製品のログを常時監視して、ウイルスの感染がないかなどを分析しインシデントを発見する役割

D. インシデント対応

起きてしまったインシデントに対し、脅威の拡散抑止や、原因となったシステムを安全に復旧し脅威を排除する役割

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

[20] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

- What

攻撃の特徴	Struts	Drupal
攻撃形態、関連する通信の内容	GET によるリクエスト	GET, POST によるリクエストができ、cookie も利用される [21]
核心となる攻撃コード	公開された攻撃コード [22]	(4/12 以降に)公開された攻撃コード [23]。
攻撃によって残る痕跡	（攻撃手法による）	（攻撃手法による）
被害を受けた後の通信内容	（ケースによる）	（ケースによる）
サーバやクライアントに残るログ	Tomcat や Web サーバのログ	Web サーバのログ
サーバやクライアントに残るその他の特徴	（攻撃手法による）	（攻撃手法による）
各セキュリティ製品における検知名	（各種製品による）	（各種製品による）
上記が不明な場合、自身で調査するための PoC(Proof of Concept)	公開された攻撃コード	(4/12 以降に)公開された攻撃コード

このフェーズでは、攻撃がすでに来ているのか、攻撃が成功しているのかを確認するために、共有された情報を利用する。

検証用のコード(PoC, Proof of Concept)を参考に、どのように攻撃されるか、攻撃された際にはどのようなログがどこに出力されるかを確認することとなる。

「各セキュリティ製品における検知名」については、利用している製品によって名前が異なるため、各社から提供される情報を参考にされたい。

- How

検知としては、「サーバやクライアントに残るログ」や「サーバやクライアントに残るその他の特徴」を利用して、事業部門・システム運用部門に影響がないか確認を行う。

脆弱性のあるソフトウェアを利用しているサーバに残るログから、攻撃の痕跡がないかを確認する。攻撃が来ているかどうか、来ている場合攻撃が成功しているかの確認を行う。

[21] https://research.checkpoint.com/uncovering-drupalgeddon-2/
[22] https://github.com/jas502n/St2-052
[23] https://github.com/a2u/CVE-2018-7600

セキュリティ製品を活用している場合は「各セキュリティ製品における検知名」も利用して、「B. リアルタイムアナリシス（即時分析）」を行う。

検知だけではなく分析などのより詳細な調査が必要な場合は「C. ディープアナリシス（深掘分析）」へ進む。

結果としてインシデントである場合は、インシデント対応を行う判断を行い、封じ込め/根絶/復旧のフェーズへ進む。

準備（予防）

Why はまだ攻撃が来ていない状態での攻撃に対応する準備や予防のため、When は検知および分析で攻撃の影響がないことが確認できた後のタイミングにあたるフェーズである。

ここでの準備（予防）は世の中で話題になっているからかどうかではなく、初動要否判断で自組織の資産に脆弱性があることがわかっていることが前提である。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[24]を参考に各機能の担当として例示する。

G. セキュリティ対応システム運用・開発

セキュリティ対応に必要なシステムを設置したり、管理したりするお仕事

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

[24] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

- What

	Struts	Drupal
攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件	（各社から提供されるシグネチャ）	（各社から提供されるシグネチャ）
攻撃を無効化する方法(パッチの適用、設定変更など)	パッチ Struts REST Plugin を有効化、XML によるリクエストを受け付けている	パッチ
被害を受けたシステムの復旧方法	再構築	再構築

攻撃に対する準備や予防のために、セキュリティ製品を利用するのであればどのようなシグネチャを設定するかや、根本的な対応としてパッチを利用するのか緩和策を利用するかとなる。

- How

被害の発生を予防する、あるいは攻撃への対応を準備するため、「G. セキュリティ対応システム運用・開発」の機能が中心となり、具体的な対策を実装する。

ここの例では、「攻撃を無効化する方法（パッチの適用、設定変更など)」を活用し、パッチを適用して脆弱性を無効にするか、設定を変更して攻撃に対する緩和策を実施する。

改めて「E. セキュリティ対応状況の診断と評価」を行うと、より万全な準備ができるだろう。

初めての脆弱性であり、環境のアップデートをどのようにするのかが不明である場合、提供されたパッチをそのまま適用して他に影響がないか、問題が起こらないかの確認をどうするか、という部分が課題となる。

事前に更新する手段を確認しておく、普段からバージョンがアップするたびにその都度更新をしておくなど日々の活動をする中でどのように準備（予防）を行うかを確認しておきたい。

封じ込め/根絶/復旧

Why は封じ込め/根絶/復旧のため、When は検知および分析の後に影響が出ておりインシデントが起きていた場合の対応を行うタイミングのフェーズである。

- Who

C. ディープアナリシス(深堀分析)

発見されたインシデントにおいて、どんな攻撃手法で何の情報が盗まれたのかなどより深い分析をする役割

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

- What

情報の内容的には「検知および分析」と「準備（予防)」フェーズと同じである。

攻撃によって残る痕跡の調査が必要なため、「検知および分析」の「攻撃によって残る痕跡」の情報を中心に痕跡から分析を行う。

攻撃を受けた後の通信内容や、サーバやクライアントに残るログの特徴的な変化といった情報を利用する

- How

こちらも「準備（予防)」フェーズと同じである。

セキュリティ製品による検知・遮断、攻撃を無効化する手段、被害を受けたシステムの復旧といった情報を利用する。

事件後の対応

Why は事件後の対応のため、When はインシデント対応が完了した後のタイミングのフェーズである。

- Who

ここでの who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[25]を参考に各機能の担当として例示する。

F. 脅威情報の収集および分析と評価

ネット上のセキュリティニュースやこれまで自組織で見つけたインシデントを取りまとめ、次に生かす役割

I. 外部組織との積極的連携

社内外問わず勉強会などへ参加したり催したり、人との繋がりを増やす役割

- What, How

What や How については事件後の情報共有のため、決まった形式はない。

しかしながら、どのようにして被害にあったのかを共有することで、今後の被害が拡大しないように各組織が参考にすることができるため、積極的に情報を公開・共有することが望まれる。

また、情報を共有したことについても積極的に評価されるべきである。

被害後の外部への対応などについては、的確な情報を共有する意味を持ち、各所で検討などが進んでいる。例えば JNSA の「調査研究部会 [26]」の「セキュリティ被害調査 WG」などでも検討が進められている。

[25] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
[26] https://www.jnsa.org/active/2018/surv.html#incident

7.2. 攻撃関連情報の場合

「＊＊＊を騙る」フィッシングの例と「請求書.xlsx」のように悪性の添付ファイルがある例を紹介する。

7.2.1. 攻撃関連情報を受け取った場合のフロー

全体のフローは先の脆弱性情報の場合のフローと同じとなる。先ほどのフローと大きな違いはなく、違いがあるとすれば「予防（準備）」のフェーズの対象が脆弱性の対象のシステムではなく、人間に対する注意喚起に変化しているくらいである。ただし、攻撃の関連情報において、PC の OS やブラウザ、プラグインの脆弱性を突いたような攻撃に関連する場合は、脆弱性情報と同様に、システムに対する対処と同じようになる。

7.2.2. 各フェーズの 5W1H

全体のフローから、各フェーズでの 5W1H がどうなるのかを例示する。

初動対応要否判断

Why は初動要否判断のため、When は共有された情報を受け取った直後の初動要否判断を行うフェーズである。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[27]を参考に各機能の担当として例示する。

D. インシデント対応
起きてしまったインシデントに対し、脅威の拡散抑止や、原因となったシステムを安全に復旧し脅威を排除する役割

E. セキュリティ対応状況の診断と評価
脆弱性診断や標的型メール訓練などによりセキュリティレベルを適切に維持・向上できているかを評価する役割

F. 脅威情報の収集および分析と評価
ネット上のセキュリティニュースやこれまで自組織で見つけたインシデントを取りまとめ、次に生かす役割

[27] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

ここでは、「E. セキュリティ対応状況の診断と評価」は共有される情報に影響される。攻撃に関する情報において、脆弱性を悪用するようなものであれば、対象となるシステムが存在するかなどの確認が必要になる。

- What

	＊＊＊を騙るフィッシング	悪性の添付ファイル
該当の攻撃情報を示す名称（攻撃名称、マルウェア名、事件名など）	「＊＊＊を悪用したフィッシング」	「請求書.xlsx」が添付されたメール
攻撃のターゲット	ばらまき型	ばらまき型
攻撃ベクター　攻撃がどこから進行してくるか、例えばマルウェアの感染経路など	フィッシングによるアカウント ID とパスワードの窃取	メールに添付してクリックさせることでマルウェア本体をダウンロードして実行させて感染する

- How

「F. 脅威情報の収集および分析と評価」などによって集められた情報(What)と社内で検知している情報によってイベントとして管理を行う。

「A-2. トリアージ基準管理」「A-3. アクション方針管理」に従い「D. インシデント対応」で総合的に初動要否の判断をする。着手後は「E-3. 脆弱性管理・対応」によって組織的に対応する。

主には外部からのメールに関する情報となり、情報で示されたようなメールが届いているのか、ターゲットが自組織であるかなど判断をして、アクション方針管理に従い判断を行う。

悪性の添付ファイルが OS やアプリケーションの脆弱性を悪用するようなものであれば、脆弱性管理・対応により対応を行うこととなる。

組織によっては、初動要否判断のフェーズにおいて、初動要否判断の結果、準備(予防)のフェーズを先に行い注意喚起や感染の予防を先に行い、その後で検知や分析を行うフローこともあるので、各組織のフローや社会的な影響度に応じて対応されたい。

検知および分析

Why は検知および分析のため、When は初動要否判断の後に影響が出ていないかを調べるタイミングのフェーズである。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[28]を参考に各機能の担当として例示する。

B. リアルタイムアナリシス（即時分析）

セキュリティ製品のログを常時監視して、ウイルスの感染がないかなどを分析しインシデントを発見する役割

D. インシデント対応

起きてしまったインシデントに対し、脅威の拡散抑止や、原因となったシステムを安全に復旧し脅威を排除する役割

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

[28] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

- What

	＊＊＊を騙るフィッシング	悪性の添付ファイル
攻撃の特徴 攻撃の通信内容	偽サイト	(xlsx の解析による通信先の解析が必要) http://example.com/xx.exe
攻撃の特徴 核心となる攻撃コード	攻撃コード無し	攻撃コードではなく、マクロなど
攻撃の特徴 攻撃に関わる HTTP 関連のインジケーター （IP アドレス、ドメイン、FQDN、URL）	（メールに含まれる URL を OSINT で解析した各種データ)	（xlsx の解析による通信先の解析が必要） http://example.com/xx.exe 通信先からさらに OSINT で解析した各種データ
攻撃に関わるメール関連のインジケーター メール件名、メール本文、メール本文に含まれる URL	（メールを参照する）	（メールを参照する）
攻撃に関わるメール関連のインジケーター 添付ファイルの情報（ファイル名、拡張子、ハッシュ値、内容）	添付無し	添付ファイルの情報（ファイル名、拡張子、ハッシュ値、内容）
その他のプロトコルにおける特徴、インジケーター	無し	無し
攻撃を受けた場合の痕跡 攻撃を受けた場合の通信内容	アカウントとパスワードの窃取際のアクセスログのみ	最終的にマルウェアをダウンロードした通信
攻撃を受けた場合の痕跡 サーバやクライアントに残るログ	Proxy ログ	Proxy ログ

攻撃を受けた場合の痕跡 サーバやクライアントに残るその他の特徴	フィッシングサイトの URL へのアクセス履歴	マルウェア本体への URL へのアクセス履歴
攻撃を受けた場合の痕跡 攻撃に関する悪性コンテンツの情報 （ファイル名、フォルダ・ディレクトリパス、プロセス名、ハッシュ値、レジストリ変更内容、検体（悪性コンテンツそのもの））	無し	マルウェア本体のファイル名
各セキュリティ製品における検知名	Proxy 製品などにおける、Web サイトレピュテーションにおけるカテゴリ名(例：phishing site, malicious site など)	アンチウイルスソフトでの検出名 例：HEUR：Trojan.Script.Agent[.]gen, Trojan.Win32.Yakes[.]wjcc

- How

検知としては、「サーバやクライアントに残るログ」や「サーバやクライアントに残るその他の特徴」を利用して、事業部門・システム運用部門に影響がないか確認を行う。

主にメールに関する情報であるため、もたらされた情報に感染したメールが届いていないか、届いている個人が開封していないか、URL をクリックしていないか、添付ファイルを開いていないかなどの確認をすることとなる。

状況から「D. インシデント対応」で初動が必要だと判断されると、その対応が発生する。脆弱性を悪用するような攻撃の場合は PC やシステムの状況を「X. 事業部門・システム運用部門」で確認を行う。

セキュリティ製品を活用している場合は「各セキュリティ製品における検知名」も利用して、「B. リアルタイムアナリシス（即時分析）」を行う。

検知だけではなく分析などのより詳細な調査が必要な場合は「C. ディープアナリシス（深掘分析）」へ進む。

結果としてインシデントである場合は、インシデント対応を行う判断を行い、封じ込め/根絶/復旧のフェーズへ進む。

検知および分析のフェーズにおいて、情報の取り扱いを間違えるとアクセスすべきでな

い URL にアクセスしてしまうことや、情報を展開しようとしてそのまま転送してしまい二次被害が起こるようなこともあるため、試しにクリックする、添付ファイルを開いてみる、情報をそのままメールで転送するなどの事故が発生しないように注意されたい。

準備（予防）

Why はまだ攻撃が来ていない状態での攻撃に対応する準備や予防のため、When は検知および分析で攻撃の影響がないことが確認できた後のタイミングのフェーズである。

ここでの準備（予防）は世の中で話題になっているからかどうかではなく、初動要否判断で自組織に攻撃の可能性があることがわかっていることが前提である。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[29]を参考に各機能の担当として例示する。

G. セキュリティ対応システム運用・開発

セキュリティ対応に必要なシステムを設置したり、管理したりするお仕事

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

- What

	＊＊＊を騙るフィッシング	悪性の添付ファイル
攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件	URL やドメイン名などをブラックリストとして設定	添付をアンチウイルスソフトが検出するなら、パターンファイルのアップデート 通信先の悪性URLをブラックリストとして設定する EDR やアプリケーション制御などの仕組みにブラックリストとして登録する
攻撃を無効化する方法（パッチの適用、設定変更など）	ユーザへの注意喚起 （自組織のサイトを騙られている場合は）しかるべき機関など [30]にフィッシングであることを報告する	ユーザへの注意喚起 アンチウイルス事業者への検体の提出によるパターン作成の依頼

[29] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
[30] https://www.antiphishing.jp/

準備（予防）の情報としてはシステムで予防（準備）する方向と、ユーザに呼びかけて被害を防ぐ 2 つの方向である。

- How

対策としては、ユーザに注意喚起をすることも大事であるが、「G. セキュリティ対応システム運用・開発」において監視を強化する必要もある。そのためにアンチウイルスソフトの更新や URL のブラックリストの登録を行う。脆弱性が悪用されるソフトウエアについては「X. 事業部門・システム運用部門」でパッチの適用も必要となる。

封じ込め/根絶/復旧

Why は封じ込め/根絶/復旧のため、When は検知および分析の後に影響が出ておりインシデントが起きていた場合の対応を行うタイミングのフェーズである。

- Who

C. ディープアナリシス(深堀分析)

発見されたインシデントにおいて、どんな攻撃手法で何の情報が盗まれたのかなどより深い分析をする役割

X. 事業部門・システム運用部門

対象となる事業を行なっている部門や対象となるシステムを運用している部門である。

事業部門・システム運用部門は「セキュリティ対応組織の教科書」では規定しておらず、本書の説明のために“便宜上作成した機能”である。連携して対応を行う必要があるため、ここでは明記している。

- What

基本的には「準備（予防)」のフェーズと同じものになる。

	＊＊＊を騙るフィッシング	悪性の添付ファイル
攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件	URL をブラックリストとして設定	添付をアンチウイルスソフトが検出するなら、パターンファイルのアップデート 通信先の悪性URLをブラックリストとして設定する
被害を受けたシステムの復旧方法	ユーザが入力してしまったアカウントのパスワード変更や ID の変更	再インストール

- How

すでに感染しているなどした場合は「C. ディープアナリシス(深堀分析)」で駆除や復旧の支援を行う必要がある。環境によっては「X. 事業部門・システム運用部門」で封じ込めや根絶、復旧を行う必要がある。

事件後の対応

Why は事件後の対応のため、When はインシデント対応が完了した後のタイミングのフェーズである。

- Who

ここでの Who については、「セキュリティ対応組織(SOC,CSIRT)の教科書」[31]を参考に各機能の担当として例示する。

F. 脅威情報の収集および分析と評価

ネット上のセキュリティニュースやこれまで自組織で見つけたインシデントを取りまとめ、次に生かす役割

I. 外部組織との積極的連携

社内外問わず勉強会などへ参加したり催したり、人との繋がりを増やす役割

- What, How

What や How については事件後の情報共有のため、決まった形式はない。

しかしながら、どのようにして被害にあったのかを共有することで、今後の被害が拡大しないように各組織が参考にすることができるため、積極的に情報を公開・共有することが望まれる。

また、情報を共有したことについても積極的に評価されるべきである。

前述の脆弱性情報を受け取った場合と同様であるが、現在事件後にどのような報告を行うべきかが各所にて検討されているので、そちらを参照いただきたい。

[31] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

8. 情報共有が逃れられない根本的な制約

ここでは情報共有が持つ根本的な制約について書き記す。これは情報共有に携わる者すべてにとって逃れられない事項であるため、しっかりと認識しておく必要がある。

まずは、理想的な情報共有とはどのような性質を持つか考えてみよう。例えば、「早くて、正確で、抜け漏れがない」ものであればどうだろうか、誰しもが満足できるのではないだろうか。

しかし、本当にそれは実現可能であろうか。

答えは NO である。急いで情報を共有しようとすれば、その正確性は犠牲になる。網羅性を担保しようと思えば時間はかかってしまう。当たり前の話である。このジレンマは情報共有のトライアングルとして取り上げられている [32,33]。

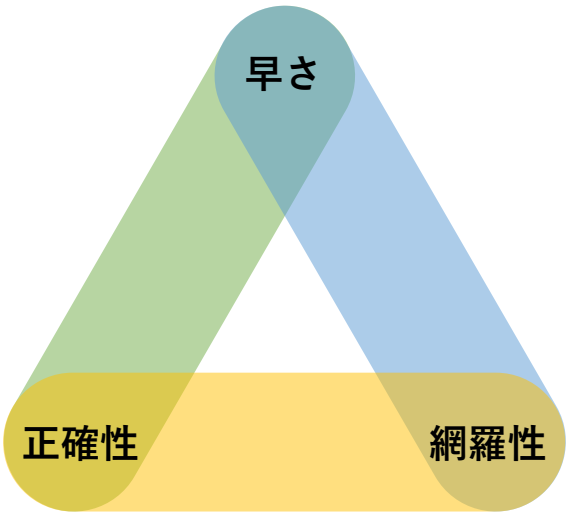

図 5　情報共有のトライアングル

要するに、早さと正確性、網羅性はいずれか 2 つしか満たせないというものであるが、改めて整理すると次のように言える。

- 早くて正確なものは網羅性に問題が出る

[32] 27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)
[33] https://www.first.org/resources/papers/conf2015/first_2015-rasmussen-rod_cutting-through-cyberthreat-intelligence-noise_20150615.pdf

- 例：攻撃に関する情報として特定の IP アドレスが提示されたものの、他にも関連していた IP アドレスが多数あったことがあとから判明する

- 早くて網羅的なものは正確性に問題が出る
  - 例：攻撃に関連する情報として多数のドメインが提示されていたものの、無害なドメインも含まれてしまっている

- 正確で網羅的なものは早さに問題が出る
  - 例：攻撃に関連する情報として、IP アドレスもドメインも抜け漏れなく、正確に整理されたものが提示されるのは、しばらく時間がたってからである

事態が深刻であればあるほど、早さが求められてしまう現実があり、その「早さ」に応えようとすれば、正確性か網羅性が犠牲になってしまう。これは逃れようのない制約である。そのため、せっかく早く共有してもらった情報に対し「網羅性がない！」「正確ではない！」と責め立ててしまうのは悪手である。情報発信者を萎縮させ、情報が提示されにくい環境を生み出してしまう。誰が行うにしても、正確で網羅的な情報を作り上げるには時間がかかるのである。これは、情報に関する苦痛のピラミッド[34] (the Pyramid of Pain)として言及されるところでもある。

文句を言わず情報を受け入れるべし、ということではない。フィードバックもまた重要である。共有された情報に不足を感じたのであれば、自身がそれを補う発信をすべきであるし、正確性に問題があるのであれば正しい情報を発信するべきである。

フィードバックが建設的であればあるほど、良い情報共有の場となるということは、情報発信の立場であっても情報受信の立場であっても忘れないようにしたい。

1. [34] http://detect-respond.blogspot.jp/2013/03/the-pyramid-of-pain.html

9. おわりに

本書では「5W1H」を切り口に、サイバーセキュリティ情報共有の「いろは」を整理した。基本を押さえた先には大きな課題がある。例えば下記のような事項である。

- 発信者側と受信者側の「How」の標準化、自動化
- 情報の信頼度、有効性の可視化
- 発信者と受信者をつなぐ、フィードバックの機構
- 国内外の情報共有のトレンドの把握

発信者側の「How」の標準化については STIX[35]、TAXII[36]や CybOX[37]といった仕様が策定されているものの、まだまだ一般的に普及した状態とは言えず、発信者側も受信者側も共通的な処理で情報を発信したり、活用したりすることができないという課題がある。また、共有された情報の信頼度をどのように可視化するかも真剣に考えなければならない。情報は絶えず変化するものであり、時間経過により無効化するものもある。さらに、悪意に満ちた偽の情報が混入する可能性もあるなど、正確性、信頼性を担保するのは難しい。その解決の糸口の一つとして受信者による「フィードバック」が考えられるが、そのフィードバック自体が「発信」であるため、情報共有の場をもっと活性化されなければならない。仮に活性化がうまくいったとしても、フィードバックが散在して参照しづらい状態では発信者側も他の受信者も拾うことができないため、共通の情報共有基盤が不可欠になる。しかし、現状のように情報共有の「場」自体が散在している状態では、それは難しいと言わざるを得ない。

米国では、国土安全保障省（DHS）がサイバーセキュリティの情報共有の枠組みとして「Automated Indicator Sharing（AIS）[38]」を推進している。STIX をベースとした情報基盤を構築し、多くの組織がその情報を活用するなど先進的な事例も出てきた。自動化についても IETF において MILE[39]や I2NF[40]の議論が活発化している。EU では 2018 年 5 月に NIS 指令が発効された。本指令では EU 加盟国は自国の重要インフラ事業者に適切なセキュリティ対策を講じさせ、サービスに重大な影響を与えるセキュリティ事故の報告を義務付けることが求められている。また日本としては 2019 年 4 月 1 日に「サイバーセキュリティ協議会」[41]が創設され、新たな情報共有・連携体制の構築が行われている。

35 https://www.ipa.go.jp/security/vuln/STIX.html
36 https://www.ipa.go.jp/security/vuln/TAXII.html
37 https://www.ipa.go.jp/security/vuln/CybOX.html
38 https://www.dhs.gov/ais
39 https://datatracker.ietf.org/wg/mile/about/
40 https://datatracker.ietf.org/wg/i2nsf/about/
41 https://www.nisc.go.jp/conference/cs/kyogikai/index.html

このように国内外で様々な「情報共有」の取り組みが行われているため、サイバーセキュリティに携わるものとしてこれらの「情報共有」の活動の動向については今後も注視していく必要がある。

最後に読者の皆様におかれましても、情報共有の場で、活発な発信、適切な活用を行えるよう、本書でまとめた"サイバーセキュリティ情報共有の「5W1H」"で基本を押さえ、より一層のセキュリティ対応組織(SOC/CSIRT)強化へ繋げていただければ幸いである。

執筆

日本セキュリティオペレーション事業者協議会（ISOG-J）

セキュリティオペレーション連携 WG(WG6)

ももい やすなり	株式会社インターネットイニシアティブ
早川 敦史	NEC ソリューションイノベータ株式会社
亀田 勇歩	SCSK 株式会社
阿部 慎司	NTT セキュリティ・ジャパン株式会社/ISOG-J WG4 リーダー
河島 君知	NTT データ先端技術株式会社
武井 滋紀	NTT テクノクロス株式会社/ISOG-J WG6 リーダー
彦坂　孝広	NTT テクノクロス株式会社

（執筆関係者、社名五十音順）

初版執筆

亀田 勇歩	SCSK 株式会社
阿部 慎司	NTT セキュリティ・ジャパン株式会社/ISOG-J WG4 リーダー
武井 滋紀	NTT テクノクロス株式会社/ISOG-J WG6 リーダー
市川 隆義	ソフトバンク・テクノロジー株式会社
佐々木 将信	株式会社富士通ソーシアルサイエンスラボラトリ
	（協力者）
ももい やすなり	株式会社インターネットイニシアティブ
河島 君知	NTT データ先端技術株式会社

（執筆関係者、社名五十音順）