

インシデントハンドリングマニュアル

一般社団法人 JPCERT コーディネーションセンター

2021年 11月 30日

目次

1. 本書の位置づけ.....	1
2. 基本的ハンドリングフロー	2
2.1 検知／連絡受付.....	3
2.2 トリアージ.....	5
2.3 インシデントレスポンス（対応）	6
2.4 報告／情報公開.....	7
3. 事象別特記事項.....	8
3.1 DDoS（分散型サービス運用妨害）攻撃	8
3.2 マルウェア感染.....	9
3.3 不正アクセス	9
3.4 フィッシング等偽サイトの設置	10
3.5 APT（Advanced Persistent Threat：先進的で執拗な脅威）	12
4. 最後に.....	13

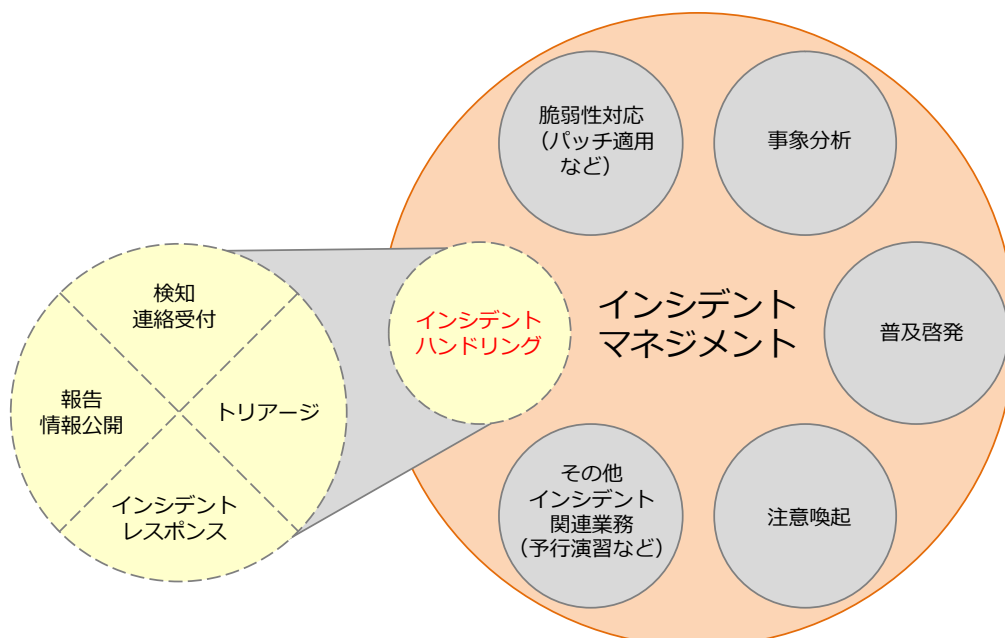
1. 本書の位置づけ

近年、組織のサイバーセキュリティに対する備えと対応のプラクティスとして、組織内の情報セキュリティ問題を専門に扱う CSIRT（シーサート: Computer Security Incident Response Team）の整備と運用が、国内外の企業や組織で広く普及しています。組織が CSIRT を構築する際に必要な作業がいくつかあります（詳細については「CSIRT ガイド」を参照）が、その中でも特に重要な項目の 1 つが、自組織において発生する可能性のある情報セキュリティ事故・事象（以降、インシデント）をリストアップし、それぞれについて対応マニュアルを用意することです。

本書は CSIRT の活動の核となるインシデント対応マニュアルを作成する際の参考として使っていただくことを目的に、代表的なインシデント種別を例にあげ、対応の考え方や注意点を示すものです。

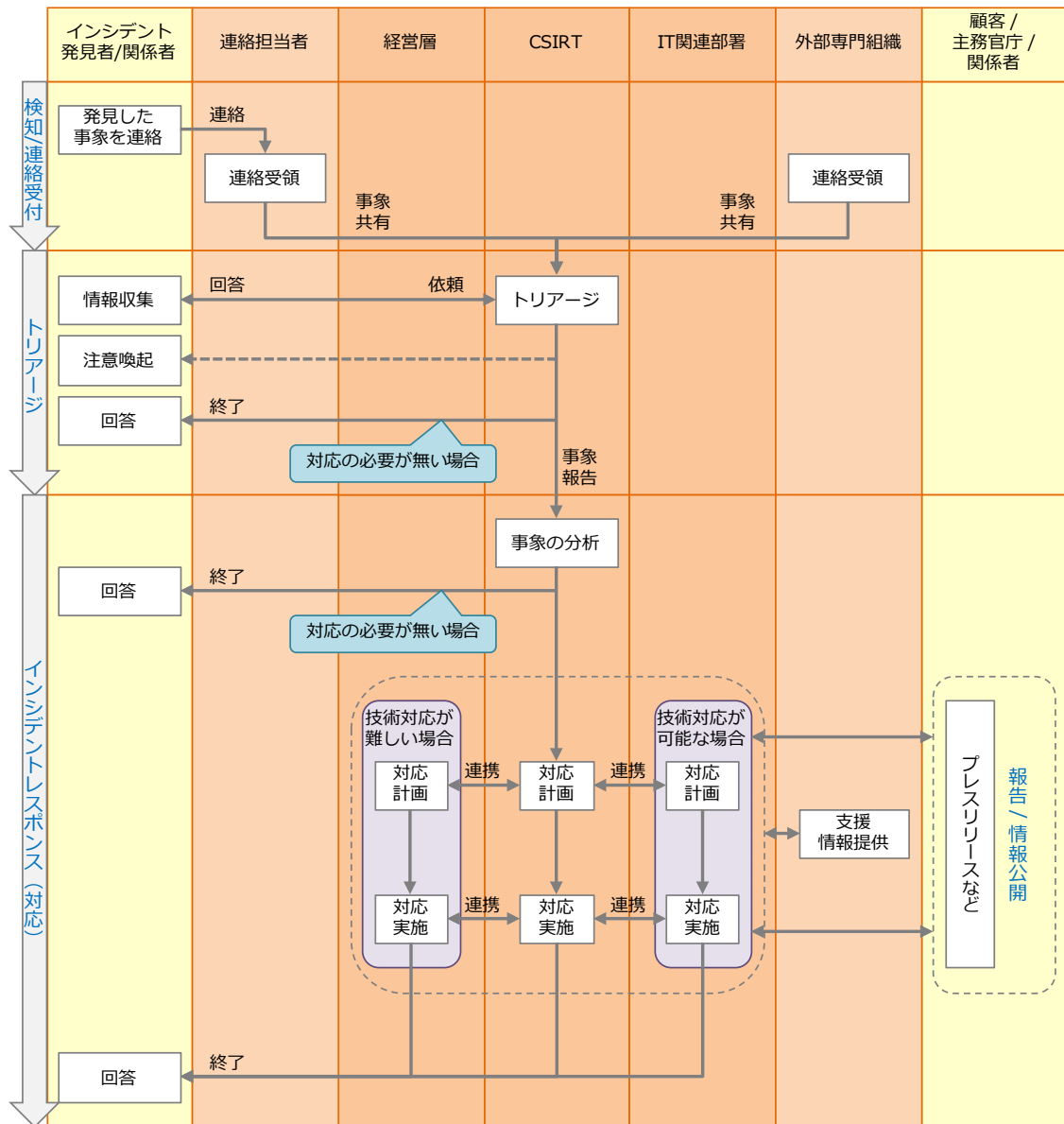
本書の初版は 2008 年に、これから自組織内に CSIRT を構築しようと考えている組織の CSIRT 担当者に向けた入門書として公表しました。その後 2015 年に、高度サイバー攻撃（APT）に関連する記述を追記した改訂版を公表しています。今回の改訂では、その後のサイバーセキュリティに関する情勢の変化や知見の蓄積を反映しいくつかの記述の修正を行っていますが、基本的な構成やメッセージは変えず、インシデント対応の考え方と手順について概要を簡潔に説明する資料として作成しました。

なお、本書が対象とするのは、CSIRT がインシデントに対して行う活動全般（「インシデントマネジメント」という）のうち、インシデント発生時から解決までの一連の処理にあたる「インシデントハンドリング」部分です。



2. 基本的ハンドリングフロー

インシデント全般に対して共通したフローを示したのが次の図です。

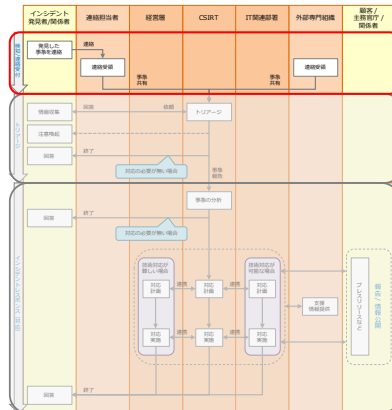


2.1 検知／連絡受付

インシデントの発生を検知するには大きく分けて 2 つの方法があります。

一つは、保守作業の中で発見したり、あらかじめ設置したセキュリティ機器やシステムによって異常を検知するといった、自組織内で検知する方法です。

ここで重要なのは、定期的または不定期に行われる保守作業において、侵入や改ざんの痕跡を調べるといったインシデントの検知に必要なチェック項目と、チェックの方法をあらかじめ明確にしておくことです。またそれらの手順を自動化した「異常検知システム」を導入する場合は、誤検知を可能な限り抑えるため、「何を持って異常とみなすのか」といった点を整理しておくことも重要です。



もう一つは、外部からの通報をもとにしてインシデントの発生を「検知=認知」する方法です。インシデントが発生した他者から「お前のところから不審なアクセスを受けた」といったようなクレームとして通報を受けるケースや、外部の第三者やセキュリティベンダー等による調査活動によって自組織で発生していたセキュリティ侵害やシステムの脆弱性が発見され、彼らが善意によって通報してくるケースが考えられます。そのような外部からの問い合わせや報告を受ける場合に備えて、インシデント報告用の窓口（電子メールアドレス、電話番号、ファックス番号など）を用意し、自組織の Web サイトに掲載するなどして公開しておきます。また、窓口用に用いられるコミュニケーションチャネル、特にインターネット接続については、不通になった場合に備えて、何らかの方法で冗長化しておくことが推奨されます。

インシデントに関する通報は、組織の従業員など、サービス対象者からなされる場合もあります。この場合、たとえ通報の内容が実際に対応する必要のないものであったとしても、サービス対象者に代わって「判断」をするのも CSIRT の役目と考え、誠実に対応することが望まれます。

一方、インシデントに関連した問い合わせは、多くの場合、IP アドレスやドメイン名から検索された宛先に送付されます。具体的には JPNIC や JPRS などが提供するサービスから検索された「技術連絡担当者」や「登録担当者」です。

IP ドメイン名に関する情報を検索できるサービス

JPRS WHOIS <https://whois.jpri.jp/>

IP アドレスに関する情報を検索できるサービス

JPNIC WHOIS Gateway <https://whois.nic.ad.jp>

これらのサービスに登録した連絡先に問い合わせが来たときに、確実に対応できる仕組みを用意しておく必要があります。例えば、登録する電子メールアドレスを個人アドレスではなく、グループアドレスにすることで、確実に誰かがメールの内容を確認できるようにしておきます。

また他にも、対外的に公開されている窓口には、常にインシデントに関する問い合わせが来る可能性があります。問い合わせをする側はこちらの事情を必ずしも考慮してくれるとは限りません。せっかくインシデントに関する報告受付用の窓口を用意していても、そんなこととはお構いなしに、無関係なウェブマスターの電子メールアドレスへ問い合わせを送ってくる可能性があるのです。

例えば、**root@ドメイン名**や **administrator@ドメイン名**、また **RFC2142** で紹介されている **abuse@ドメイン名**、**noc@ドメイン名**、**security@ドメイン名**といった電子メールアドレスは、インシデントに関する問い合わせが送られてくる可能性の高いものの典型例です。

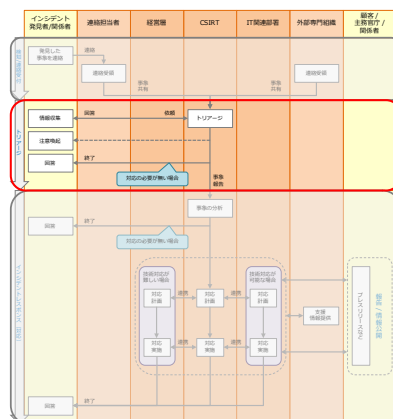
善意の第三者がインシデントに関連する事象を発見し通報しようとするとき、相手組織の正しい窓口を手間をかけて探すことはしないかもしれません。そのような通報者は、インシデント報告窓口が組織の **Web** サイト等で明示されていなければ、**WHOIS** の登録情報や **RFC2142** で定義される一般的な窓口としてのメールアドレスへ通知を試み、もしそれがエラーになるようであれば、その時点で通報を諦めてしまうでしょう。その結果、組織は有用なインシデント関連情報を受け取ることができず、問題が放置されることになりかねません。

あるいは、それらの一般的な窓口へインシデントを通報するメールが届いたとしても受信者がそれを **CSIRT** へ速やかに転送しなければ、やはり問題に対して適切な対処がとられないばかりか、通報された問題について通報者と **CSIRT** が適切なコミュニケーションを取ることができません。その結果、通報者は組織からの応答がなくても自身が送ったメールがエラーにならなかったことをもって通報が組織に受理されたものとみなして、通報者が定める情報公開ポリシーに基づいて、一定期間の後に、インシデントへの対応がなされたか否かにかかわらずインシデントに関する情報を公表するかもしれません。

このため、対外的に公開されている窓口への問い合わせを受け取る人や部署に対して、インシデントに関する通報や問い合わせがあった場合に速やかに **CSIRT** に転送する手順と判断基準を用意しておき、普段から適切に指導しておきます。また、定期的に演習を実施して、情報の伝達・転送がスムーズに行われることを確認することも重要です。

2.2 トリアージ

CSIRT の資源（人的、設備的など）は無限ではありません。したがって CSIRT に依頼されたすべてのインシデントに対応できるとは限りません。そこでインシデントのトリアージ（対応の優先順位付け）は、CSIRT の活動の中でも重要なものとなります。そのためには、あらかじめトリアージのための判断基準を明確に定めておきます。トリアージの判断基準は、CSIRT にとって「守るべきものは何か」といった基本的な活動ポリシーによって変わります。



トリアージを行う目的は対応のための単なる優先順位付けではありません。

CSIRT が「検知=認知」したすべてのインシデントが、その CSIRT が対応すべきインシデントとは限らないからです。

例えば、インシデントと思われたものが実はインシデントではなかったという可能性があります。システムの誤検知や通報者の勘違いは少なくありません。検知システムに誤作動がなかったか、またオペレーターの誤操作によって発生した一時的な異常をインシデントと間違えてしまったのではないかといった可能性を検討した上で、インシデントであるか否かを判断する必要があります。

他にも、自組織に全く関係のないインシデントであるにもかかわらず、報告者が誤って対応を依頼してくる可能性もあります。

また、悪意を持つ者による虚偽の報告、マルウェア感染や業務妨害などを意図した報告の可能性についても想定しておくべきです。もしそのような疑いがある報告を受けた場合は、それが CSIRT に対する直接的な攻撃行為である可能性だけでなく、その裏で進行するより重大な侵害行為から目を逸らすことを意図した可能性についても考慮すべきでしょう。

いずれの場合でも、トリアージで必要なのは「冷静な判断」です。インシデントでないものをインシデントと見なして対応してしまったり、自組織とは無関係のインシデントに対応してしまったりすると、本来は秘匿すべき情報を無関係の第三者に開示してしまう可能性もあります。また、最優先で対応すべきインシデントを見失った結果、被害を拡大してしまうかもしれません。「間違った判断」に基づいた活動は、それ自体がインシデントを引き起こしたり、インシデントを大きくする原因になってしまうのです。

「冷静な判断」を行うには、まず取り扱っているインシデントに関して、「いつ (when)」「どこで (where)」「何が (what)」「どのように (how)」起こったのか、また当事者および

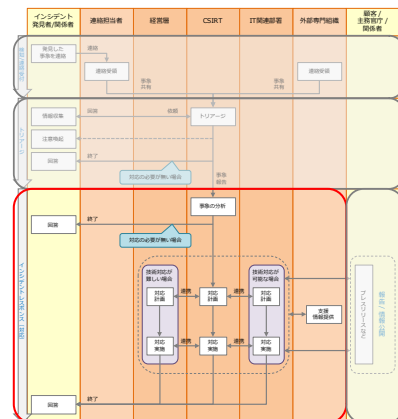
関係者は「誰か (who)」といった点を整理するとよいでしょう。なお、この時点では「原因 (why)」の究明は後に回します。

トリアージの流れは一般的に次のようになります。

- (1) 得られた情報に基づいて、事実関係を確認し、CSIRT が対応すべきインシデントか否かを判断します。その際には、必要に応じて、インシデントの報告者やインシデントに関係する可能性のあるサイトの運営者（以降、関係者）と情報をやり取りして詳細を確認します。
- (2) CSIRT が対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織のポリシーなどに照らして可能な範囲で詳細に、報告者や関係者に連絡します。
- (3) CSIRT が対応する、しないにかかわらず、関係者に速やかな対応を依頼すべき、または情報提供すべきと判断した場合は、注意喚起などの情報発信を行います。
- (4) CSIRT が対応すべきと判断した場合には、インシデントを「レスポンス（対応）」の対象とします。

2.3 インシデントレスポンス（対応）

- (1) トリアージの結果、CSIRT が対応すべきと判断したインシデントに対して、まず事象の分析を行います。それが本当に CSIRT の対応すべき事象か否かを再度検討するだけでなく、技術的な対応が可能か否かを判断します。
- (2) 対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織の情報セキュリティポリシーに照らして可能な範囲で詳細に、報告者に回答します。

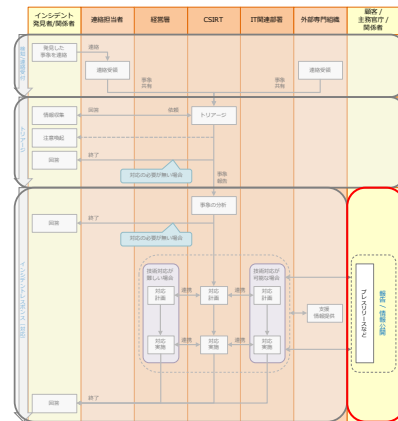


- (3) 自組織での技術的な対応が困難な場合（例えば外注先でなければ対応ができないような問題など）は、主に経営層と連携し、対応計画を策定し、実施します。もちろんその過程においては必要に応じて IT 関連部署との情報共有や連携も行います。
- (4) 自組織での技術的対応が可能な場合は、主に IT 関連部署と連携し、対応計画を策定し、実施します。もちろんその過程においては経営層との情報共有を行います。
- (5) 技術的対応の可否によらず、対応計画の策定や実施に際しては、必要に応じて外部専門機関や当該インシデントに関係している可能性のあるサイト（関係者）に対して、対応の支援を依頼したり、必要な情報を提供してもらったりします。
- (6) 対応計画を実施し終わったところで、改めて問題が解決しているか否かを確認します。もし問題が解決していない場合は、再度事象を分析し、対応計画を策定し、実施します。
- (7) 最終的に問題が解決したところで、ことの顛末を報告者に、自組織の情報セキュリテ

ポリシーに照らして可能な範囲で詳細に回答します。

2.4 報告／情報公開

対応計画の策定および実施と並行して、必要に応じて、メディアや一般に向けたプレスリリースや監督官庁への報告を行います。そのた、組織内部への情報展開なども検討する必要があります。



3. 事象別特記事項

3.1 DDoS（分散型サービス運用妨害）攻撃

【検知／連絡受付】および【トリアージ】

発生している事象が DDoS 攻撃であるかどうかの判断は一般的に容易ではありません。それは、表面上見えている事象だけでは、正規の利用者のアクセスが単に集中しているだけの状態と区別が付かないことが多いからです。そこで、アクセス元の IP アドレスとアクセス頻度、パケットの内容などを確認し、平常時の状態と比較した上で判断します。

例えば、日本語で書かれた Web コンテンツに対して、平常時ではありえない海外の大量の IP アドレスから高頻度のアクセスがある場合は、一般的には DDoS 攻撃と判断してよいでしょう。（海外のメディアでその Web コンテンツが紹介されたことが原因となっている場合もあります）

また TCP SYN flood など通信自体が異常であるパケットが送りつけられている場合も「攻撃」を受けていると判断することができます。実際の対応判断については事例ごとに異なってくるのが現実です。

【インシデントレスポンス（対応）】

技術的な対応は（原則として）接続している ISP に依頼するのが一般的です。具体的には、

- 特定の IP アドレスからのアクセス遮断、帯域調整
- TCP SYN flood など「通信自体が異常」なパケットの遮断

などです。また上記のうち、下の項目は「事前対策」としてもある程度有効です。さらに、攻撃対象のシステムの IP アドレスを変更したり、多重化して負荷分散したりする方法も、ある程度の効果が期待できますが、攻撃内容によっては無意味な場合もありますので、事象分析の段階でどのような攻撃であるかを可能な限り正確に把握する必要があります。ISP との連携については、DoS 攻撃を検知してから連絡先を確認するのではなく、平常時に ISP の担当者と話し合い連絡先や連絡するべき内容などを明らかにしておくことが必要です。

【その他】

事前対策としては、

- TCP SYN flood など「通信内容自体が異常」なパケットの遮断をネットワーク境界上で設定
- 正常な状態との比較で異常（アノマリ）を検知して、自動的にレートコントロールする仕組みの導入などが有効です。
- 自組織に対する DDoS 攻撃を誘引する可能性のあるハクティビストの動きや、同業他社等に対して観測された攻撃活動などの情報招集を行うことで、攻撃発生前に攻撃対象を一時的に多重化して負荷分散するなどの「準備」ができる場合があります。

3.2 マルウェア感染

最近のマルウェアは新種の発生頻度が高い上に、ウイルス対策ソフトによる検知を回避する技術が進んできているため、ウイルス対策ソフトでは検知ができない可能性が少なくないという現実があります。つまり、100%の感染防止は不可能という前提を特に意識した上で対応を考える必要があります。

【検知／連絡受付】

ネットワークレベルで検知のためのチェック項目を整理し、それらの項目を自動的に検知する仕組みを導入します。具体的には、内部から外部への通信をチェックし、ユーザーの意図しない通信や一時的な大量の通信、マルウェアと関係している特定サイトへのアクセスなどがある場合には、マルウェア感染の可能性が極めて高いと言えます。またインターネット接続自体は問題ないのにウイルス対策ソフトベンダーへのアクセスのみができないといった状態もマルウェア感染の可能性を示しています。さらに、マルウェアによる通信は暗号化されることもあり、その場合ネットワーク上では通信の内容を知ることはできないため、通信先や通信元のアドレスおよび通信の頻度などをもとにした判断が求められます。

3.3 不正アクセス

ここでは、「不正アクセス」として、Web コンテンツが改ざんされた場合と、SQL インジェクションに代表される Web アプリの脆弱性を悪用された場合について説明します。

【検知／連絡受付】

Web コンテンツの改ざんに対しては、システムの改ざん検知と同様に行います。例えば、コンテンツを変更するたびにチェックサム（メッセージダイジェスト）を保存し、定期的な比較するなどの改ざん検知の仕組みを導入します。

Web アプリの脆弱性を悪用したインシデントについては、保守作業の際に発見されることもあります。情報処理推進機構（IPA）や、セキュリティベンダー、研究者などの外部の第三者*からの通報で知ることが少なくありません。

※IPA では Web アプリの脆弱性に関する届出を受け付け、当該 Web サイトの運営者への連絡と修正依頼を行っています。

情報処理推進機構（IPA）セキュリティセンター 脆弱性関連情報の届出受付

<https://www.ipa.go.jp/security/vuln/report/index.html>

また、外部の研究者やセキュリティベンダーが調査活動の結果発見した Web アプリの脆弱性について、当該 Web サイトの運営者に対して通報を行うことも珍しくありません。そのため、2.1 項で述べたように、外部からの通報に対して適切に対応できる体制を準備し

ておくことが重要です。

【インシデントレスポンス（対応）】

(1) Web コンテンツが改ざんされた場合、特に Web コンテンツにアクセスしてきたユーザーの PC にマルウェアを仕込ませるような改ざんをされた場合は、利用者保護の観点から速やかに Web サービスを停止します。

また Web アプリの脆弱性が指摘された場合は、その脆弱性による利用者への危険度とサービス停止に伴う業務への影響など、取り巻くさまざまな状況を分析して、サービスを停止するか否かを判断します。

Web サイトやサービスの一時停止を告知するページ（いわゆる「Sorry ページ」）を公開する際は、インシデントの影響が及ばない安全な場所で公開しなければなりません。

(2) ユーザーの PC にマルウェアを感染させた、または顧客の個人情報が漏えいしたといった何らかの被害を生んだ可能性がある場合は、被害の拡大を防ぐために、速やかに顧客などの利用者に対して、事実関係を可能な限り正確に告知します。具体的には、被害の発生時期や被害の範囲、被害者側の対応（復旧）方法などの内容を、個別の電子メールや郵便、プレスリリースなどで告知します。また問い合わせ窓口（電話、電子メールなど）を設置し、あわせて告知します。この場合、営業担当など外部とのやり取りがある者に対しても、直接問い合わせが来る可能性があるため、問答集を作成し、組織内の各人が適切な対応ができるように指導しておきます。

【その他】

Web アプリが外部の開発業者に発注して作成されたものである場合、改修などの保守契約が結ばれていなければ、運用開始後に脆弱性が見つかったとしても、それを修正できない、または修正が極端に遅れることとなります。

あらかじめ Web アプリ開発業者との契約内容を確認し、改修に関する保守契約があるか、また契約がある場合はどのような内容かを確認しておきます。

また、Web アプリの導入時には、発注仕様にセキュリティ要件を明示し、脆弱性が見つかった場合の改修などを含めた対応全般に関する契約を交わします。IPA の「安全なウェブサイトの作り方」や、他の組織や団体から示されているガイドライン等が、発注先に示すセキュリティ要件の参考となるでしょう。

情報処理推進機構（IPA）セキュリティセンター「安全なウェブサイトの作り方」

<https://www.ipa.go.jp/security/vuln/websecurity.html>

3.4 フィッシング等偽サイトの設置

ここではフィッシングサイトなど、自組織のサイトを騙った偽サイトの存在を検知した場

合の対応について説明します。

【検知／連絡受付】

フィッシングサイトの検知は、フィッシングメールを受け取ったユーザーなどの外部からの通報によって知ることが多いため、外部からの通報に対して適切に対応できる体制を準備しておきます。

偽サイトの立ち上げを防ぐことは不可能ですが、自ら積極的に偽サイトを探すことは可能です。ただし、そこまでの労力をかけるべきか否かは顧客保護をどこまで積極的に行うか、あるいは自組織のブランドおよび知的財産の保護などの考え方によって判断が分かります。なお、偽サイトを積極的に探す作業を有償で請け負うベンダーもあります。

【トリアージ】

検知した偽サイトが本当に自組織を騙った偽サイトであるか否かを判断します。その際には、たまたま似ているだけかもしれないといった可能性も考慮する必要があります。

【インシデントレスポンス（対応）】

- (1) 顧客保護の観点からプレスリリースや Web サイトでの告知などで偽サイトの存在と、そのサイトに関する情報（危険性など）を告知する注意喚起を行います。
- (2) 立ち上がっている偽サイトを停止するには、当該サイト（IP アドレスまたはドメイン）管理者などに停止を「依頼」します。この依頼作業を有償で請け負う事業者もありますが、国際的な調整を行っている JPCERT/CC に依頼することも可能です。

JPCERT/CC インシデント報告の届出

<https://www.jpcert.or.jp/form/>

- (3) 警察（フィッシング 110 番）へ届け出ます。

フィッシング 110 番

<https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>

- (4) フィッシング対策協議会へ情報を提供します。

フィッシング対策協議会（フィッシングに対する情報収集・提供、注意喚起等の活動を中心とした対策を促進する団体）

<https://www.antiphishing.jp/>

【その他】

偽サイトの立ち上げを極力抑える方法としては、自組織のドメイン名と似ている紛らわしいドメイン名を取得しておき、似たドメイン名を使った偽サイトを勝手に立ち上げられないようにする方法がありますが、自組織のドメイン名と似た紛らわしいドメイン名をすべて網羅して確保することは現実的ではありません。

また自組織からの電子メールにはすべて電子署名を付けるようにする方法もあります。これにより、署名のない電子メールで自組織の名を騙ったメールを、利用者が偽メールと判断できるようになります。この場合は、電子署名を付けるということをあらかじめ電子メール以外の手段で顧客に告知しておきます。こういった電子署名技術を利用した送信ドメイン認証（SPF/DKIM/DMARC）を活用することも有効です。

3.5 APT（Advanced Persistent Threat：先進的で執拗な脅威）

高度サイバー攻撃（APT）の疑いのある活動を検知した場合の対応について説明します。

【検知／連絡受付】

高度サイバー攻撃（APT）の検知は、JPCERT/CC や外部の CSIRT 等の情報共有パートナーからの通報によって認識されることが多いため、通報に対して適切に対応できる体制を準備しておきます。

【トリアージ】

検知した攻撃活動に対して、それが実際に高度サイバー攻撃（APT）によるものであるかどうかの検証を実施します。

【インシデントレスポンス（対応）】

検知した活動が高度サイバー攻撃（APT）による攻撃であると判断した場合、攻撃によるリスクと自組織のリスク許容度、攻撃による脅威を直ちに排除する必要があるか、あるいは攻撃の範囲特定を試みるべきかなどについて討議し、その結果に基づいて下記のような対応内容の実施を検討します。

- (1) すみやかに脅威を排除する場合、通信遮断・システム隔離・マルウェアフォレンジックなどの措置を実施します。
- (2) 攻撃の全貌を把握したい場合、インシデント範囲の特定を実施してから脅威排除の措置を実施します。

4. 最後に

インシデントにはさまざまな種類があり、復旧のための「インシデントレスポンス (対応)」活動の実際の内容は、「3. 事象別特記事項」に記したように、インシデントの種類ごとに異なります。しかし、インシデントハンドリングにおいて重要なポイントはいずれも基本的には同じです。それは、いかに速やかに検知し、リスクを評価し、対応に移せるかということです。

そこで、まず自組織において想定されるインシデントをリストアップしたら、それらの各インシデントを検知する技術的方法や運用での工夫などを検討し、そのためのシステムや運用体制を導入します。そして、定期的（3カ月から6カ月を目安）に、想定したインシデントのリストを見直し、それらの検知の仕組みが正常に動作することを検証します。

また検知（報告受付）からトリアージまでの一連の流れがマニュアルどおりに機能するか、定期的に演習などを通じて確認し、問題があれば適宜マニュアルや運用体制を修正します。さらに、必要であれば情報セキュリティポリシーの見直しも行います。

もちろん、コミュニケーションフローだけでなく、「インシデントレスポンス (対応)」についても、演習や実運用において問題が発生した場合には、マニュアルや運用体制、セキュリティポリシーを見直します。

このような作業を繰り返すことで、自組織に最適化された対応マニュアルとして熟成され、完成度が高まります。つまり、マニュアルは一度作れば終わりというものではないのです。

一方、あらかじめ想定していなかったインシデント、すなわち対応マニュアルのないインシデントが発生する可能性もあります。マニュアルに縛られるあまり、想定外のインシデントに対応できなくなってしまっただけでは CSIRT の本来の目的は達せられません。マニュアルに従って対応できるインシデントに対してはマニュアルに従い、マニュアルにないインシデントに対しては、「何を守るのか」という CSIRT の基本ポリシーに立ち返って柔軟に対応できるように、普段からさまざまなインシデントに関する情報を収集しておきます。そして、収集した情報を蓄積して CSIRT メンバー間で共有します。その上で、想定外のインシデントに遭遇し対応した際は、その経験をもとに新規に対応マニュアルを作成します。

このように、マニュアルは単なる手順書であるだけでなく、CSIRT の経験や知見を蓄積したナレッジデータベースでもあるのです。

この「CSIRT の宝」とも言うべきマニュアルを作成するための第一歩として、本書が少しでもお役に立てれば幸いです。