ウェブサイト運営者のための
脆弱性対応ガイド

情報セキュリティ早期警戒パートナーシップガイドライン
別冊

2017年 3 月

独立行政法人 情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター
一般社団法人 電子情報技術産業協会
一般社団法人 コンピュータソフトウェア協会
一般社団法人 情報サービス産業協会
特定非営利活動法人 日本ネットワークセキュリティ協会

目　　次

1. ウェブサイトの危険性 1

1.1. 背景 1

1.2. ウェブサイトで起こるトラブル 2

1.3. 運営者に問われる責任 5

1.4. 本資料の目的 5

2. ウェブサイトに必要な対策 6

2.1. トラブルの原因となる脆弱性 6

2.2. 求められる継続的な対策 7

2.3. 対策実施にあたり理解すべきこと 7

3. ウェブサイトに脆弱性が見つかった場合 8

3.1. 脆弱性をどのように見つけるか 8

3.2. IPA から脆弱性に関する連絡を受けた場合 9

3.3. 対応は意思決定から始まる 9

4. ウェブサイト運営者のための脆弱性対応マニュアル 10

4.1. 対応の全体に係る留意点 11

4.2. 脆弱性に関する通知の受領 13

4.3. セキュリティ上の問題の有無に関する調査 15

4.4. 影響と対策の方向性の検討 16

4.5. 対策作業に関する計画 17

4.6. 対策の実施 18

4.7. 修正完了の報告 19

4.8. その他 19

付録：脆弱性について通知を受けた場合の作業 チェックリスト 20

1.ウェブサイトの危険性

1.1. 背景

多様化・高度化するウェブサイト

誰もが容易にアクセスできるウェブサイトは、インターネット利用者の拡大とともに、爆発的に増加・発展してきました。インターネット上には膨大な数のウェブサイトが稼動しており、その役割も情報発信や検索、コンテンツの投稿・共有、受発注や予約など多様化・高度化しています。

企業が自社のホームページを開設することは「当たり前」になっていて、顧客向けの広報活動はもちろん、商品の受発注や在庫管理、コンサルティングやサポート等の窓口など、ウェブサイトが企業のビジネスプロセスの一端を担っています。

インターネットの負の側面

インターネットには、世界に向けて情報を発信できる、サービスを提供できるというメリットがあります。さらに、携帯電話や無線 LAN などの進化により、今や利用者はどこにいても自由にウェブサイトを利用することができます。

その一方、誰にでも利用できるように常に公開されているウェブサイトは、悪意を持った第三者からネットワーク越しに狙われるかもしれないというリスクを抱えています。

また、設定ミスなどにより、重要情報がインターネット上に流出することもあります。一度ネットワーク上に流出した情報をすべて回収することは不可能に近いと考えられます。

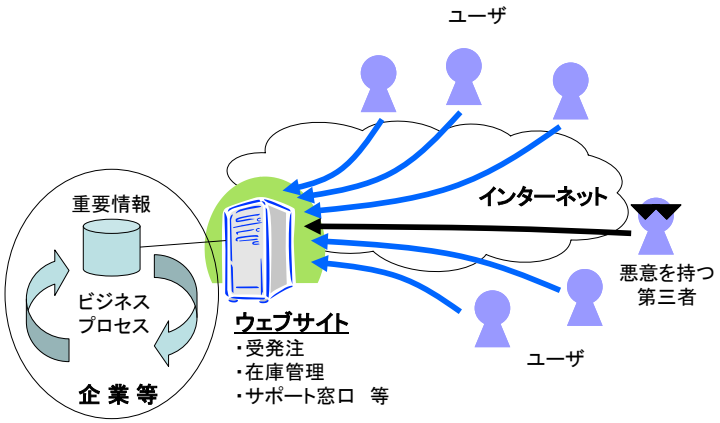


図 1-1 ビジネスプロセスの一端を担うウェブサイトとリスク

1.2. ウェブサイトで起こるトラブル

実際にウェブサイトで起きている情報セキュリティ上のトラブルとは、どのようなものでしょうか。例えば、悪意のある第三者がウェブサイトに対し不正侵入を行ったり、ウェブサイトのシステムがコンピュータウイルス[1]に感染した結果、ウェブシステムがダウンしサービス停止に陥ることもあります。また、ウェブサイトが書き換えられ、自社のウェブサイトがフィッシング詐欺[2]等の犯罪行為に悪用されることもあります。特にたとえば、ウェブサイトにクロスサイト・スクリプティング[3]の脆弱性[4]がある場合、これを悪用され、ユーザが偽サイトへ誘導され ID・パスワードやクレジットカード番号などを詐取される可能性があります。

トラブル事例 1　不正侵入によるウェブサイトの改ざん

BtoC サービス提供を行っている A 事業者のオンライン予約用のウェブサイトが不正アクセスを受け、ウェブページが改ざんされました。さらに、改ざんされたウェブページを閲覧した場合、閲覧者がマルウェアに感染する恐れがありました。改ざん発覚当日にウェブサイトを停止し、セキュリティベンダへ相談し、原因究明を行いました。ウェブサイトの脆弱性を突かれた可能性が高いことがわかっていますが、それ以上は明確になりませんでした。そのため**約 20 日間ウェブサイトを停止し、その期間の機会損失として約 1 億円、原因究明やセキュリティレベルを上げるための対策費用として約 1000 万円がかかりました。また、大口の法人顧客からアクセス制限をかけられ、信用回復までに数か月間かかりました。**

---

[1] 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能を一つ以上有するもの。（通商産業省（当時）告示「コンピュータウイルス対策基準」（平成 12 年 12 月 28 日最終改定）

[2]金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為。（フィッシング対策協議会ホームページより引用）

[3] ウェブサイトの掲示板などのプログラムを介して、悪意のあるコードがユーザのブラウザに送られてしまう脆弱性。

[4]脆弱性（ぜいじゃくせい）： ソフトウエア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

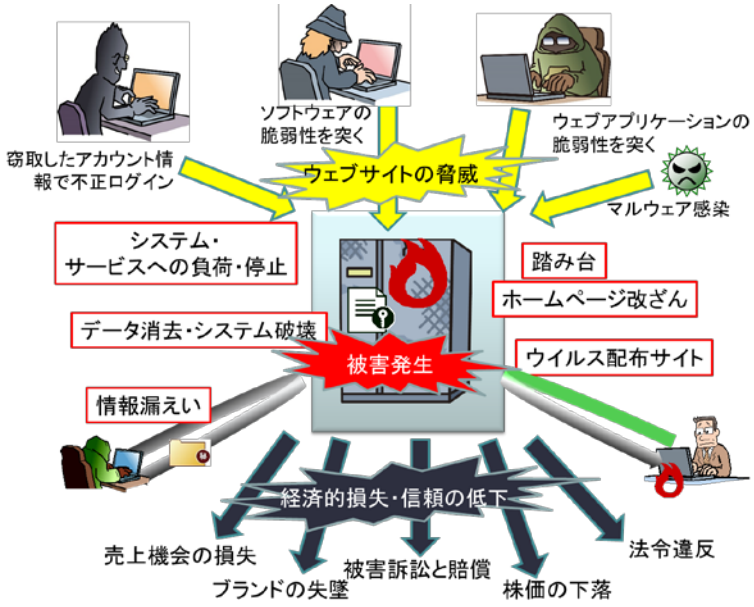


図 1-2 ウェブサイトで起こるトラブル

トラブル事例２　クレジットカード情報等の窃取

ウェブサイトの改ざん以上に被害が大きくなる事例としては、クレジットカード情報等を含む個人情報が窃取される場合です。特に SQL インジェクション [5]によって、個人情報等の重要情報が窃取される事件が増加しています。個人情報（クレジットカード情報を含む）を取り扱う場合、ウェブサイトでクレジットカード情報を保持せずに、決済代行サービス等を利用する手段があります。万が一情報漏えいが起きた場合にも、上記のような手段を採用していることで、被害を低減することができます。また、不正アクセスに気づき、すぐにウェブサイトを停止したものの、ログデータを十分に保存していなかった場合、攻撃手法や被害内容の特定が困難となり、ウェブサイトの再開までに時間がかかってしまいます。早期復旧には適切なログの収集・保管が重要となります。

通信販売 B 事業者のウェブサイトが不正アクセスを受け、顧客のクレジットカード情報、氏名等 400 件超が流出しました。即座にクレジットカード決済機能を停止し、問い合わせ用回線を設置して、漏えいが判明した顧客にはハガキで連絡した上で、お詫び代として 1000 円分の商品券を送付しました。また、クレジットカード決済機能停止（利便性の悪さ）と情報漏えいという管理状態の不信などによる信用失墜で**最悪期は売上が半分程度まで落ち込んでいたため、事件発覚から現在までの累計で損害額は 1 億円を超えると考えられます。**

[5]データベースと連携したウェブアプリケーションに、問合わせ命令文の組み立て方法に問題があるとき、ウェブアプリケーションへ宛てた要求に、悪意を持って細工された SQL 文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまう問題。（IPA　SQL インジェクション　https://www.ipa.go.jp/security/vuln/vuln_contents/sql.html）

また、金銭的な被害以外に、取引先からの信用失墜などの間接的な被害もありました。事件発生より数か月経過した**現在も事件前の売上の 4 分の 3 程度しか回復していません。**

トラブル事例３　ウェブサイトの脆弱性によるクレジットカード情報漏えいの判例

不正アクセスを未然に防止することも重要ですが、万が一発生してしまった場合、その責任の所在をあらかじめ明確にし、自社の被害を最小限にすることも重要です。契約書にセキュリティ対策に関して記載していなかったため、セキュリティレベルの低いウェブサイトを構築した事業者へ損害賠償請求をおこなっても、請求できる額が減じられることがあります。

C 社の通信販売用サイトが SQL インジェクションによる不正アクセスを受け、過去に利用した顧客のクレジットカード情報を含む個人情報が流出しました。C 社は通信販売用サイトを構築した D 社に対して、**個人情報漏えい対応や原因究明のための調査費用および売り上げの減少に対して約 1 億円の損害賠償請求**を行いました。

裁判では、SQL インジェクション対策を講じていなかったこと、クレジットカード情報を暗号化せずデータベースへ保存していたことが D 社の債務不履行かどうかが主要な争点となりました。技術水準として妥当なレベル[6]の SQL インジェクション対策を講じていなかったこと等は D 社の重過失であり、損害額は約 3200 万円とされました。情報の暗号化については契約書に明示されていなかったこと、また **C 社の担当者が D 社からの改修提案を受けたものの、対策せず放置したことから C 社の過失（3 割の過失相殺相当）**となりました。**D 社は損害賠償として C 社の過失を相殺した約 2300 万円の支払いを命じられています。**（東京地判平成 26 年 1 月 23 日判時 2221 号 71 頁）

[6] 2008 年に IPA が公開した「大企業・中堅企業の情報システムのセキュリティ対策～脅威」

1.3. ウェブサイト運営者に問われる責任

ウェブサイトで情報セキュリティ上のトラブルが発生した場合、そのウェブサイトの運営者は、どのような立場に置かれるでしょうか。

まず、個人情報の流出が発生した場合には、ウェブサイトの運営者はその事実を所管省庁に報告するとともに、架空請求などの二次被害を防ぐ意味でも、流出した個人情報の本人にその旨を連絡する必要があります。

また、ウェブサイト運営者は、ウェブサイト利用者に対してウェブサイトのセキュリティを確保する責任を果たしていなかった点を問われて、訴訟の対象となる可能性があります。実際にはそのウェブサイトの運営を外部の事業者に委託していて、自身ではトラブルの発生に関与していなかったとしても、被害者から見た「責任者」は一義的にはウェブサイト運営者であり、訴訟の際に被告となることは免れません。

トラブルを起こしたウェブサイトを停止した結果、取引先の売上げに悪影響を及ぼす可能性があります。契約によっては、損害賠償を要求されることになります。

さらに、自らが被害者であるにもかかわらず、コンピュータウイルスを撒き散らす「加害者」となっていた場合、ネットワーク社会の一員である企業として社会的責任を果たしていないと非難されるでしょう。この場合、コンピュータウイルスの駆除だけでなく、その感染の原因を調べて問題を解決しない限り、再びウェブサイトが感染し、同じトラブルを繰り返すことになりかねません。

1.4. 本資料の目的

本資料は、主にウェブサイト運営者に向けて、ウェブサイトの脆弱性がもたらすトラブルや必要な対策の概説、さらにウェブサイト運営者による脆弱性対応の望ましい手順などを紹介しています。

関係者の方々は、脆弱性対応に向けた体制の検討や、実際の対応に際し、本資料を参考にご対応くださいますようお願い申し上げます。

2. ウェブサイトに必要な対策

2.1. トラブルの原因となる脆弱性

ウェブサイトで起こる情報セキュリティ上のトラブルの原因の多くは、ソフトウエア製品の脆弱性にあります。脆弱性とは、プログラムや設定上の問題に起因する「弱点」です。悪意のある第三者が脆弱性を悪用した攻撃を行うと、たとえば想定外の入力データがメモリ上にあふれ、本来許容しないはずのコマンドを受け入れてしまい、そうした混乱を悪用されて、ネットワーク越しに権限の奪取やデータの流出、サービス停止などの不正な操作をされてしまいます。

ウェブサイトの脆弱性は、CGI（Common Gateway Interface）プログラムなどシステムの作り方や設定ミスに起因するものが多く見られます。さらに、OS 等の基盤ソフトやウェブサーバ等アプリケーションソフトの脆弱性などもトラブルの原因となります。

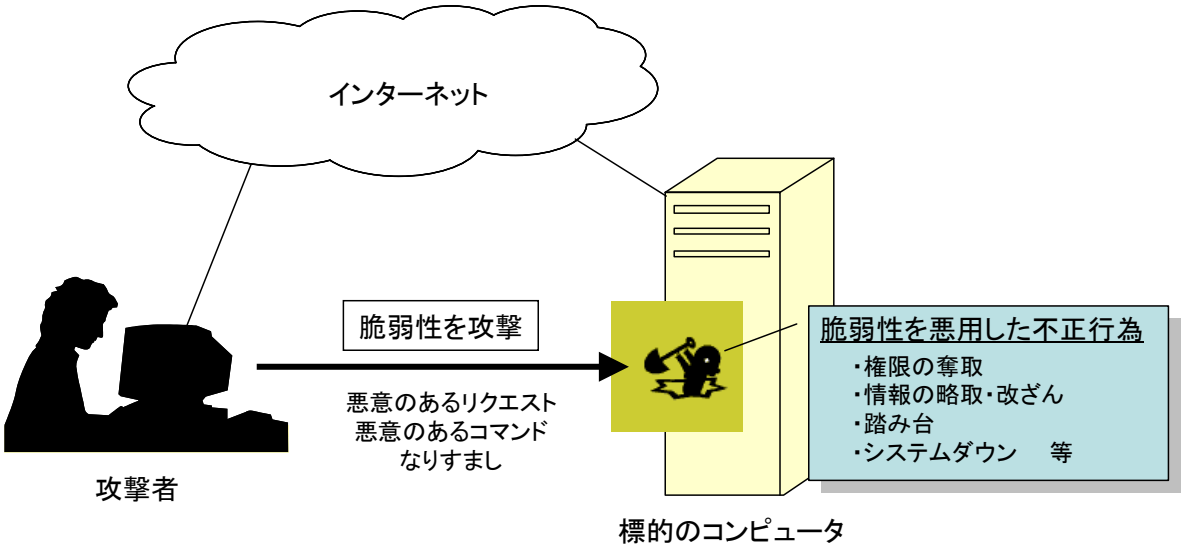


図 2-1　脆弱性を悪用した攻撃イメージ

2.2.求められる継続的な対策

脆弱性対策は、ウェブシステムの企画・設計・開発から運用・保守まで、様々な局面で継続的に取り組む必要があります。

企画時には、ウェブシステムの提供するサービスに係るセキュリティ機能構成の方針を定めます。ウェブサービス全体のセキュリティのスタンスを決めることから、セキュリティポリシーを含む多面的な視点での検討が望まれます。

次に、設計時には、扱う情報資産の重要性、サービスの継続性・信頼性に対する要求レベル、サービスの公開範囲などを踏まえ、望まれるセキュリティ要件を明確にする必要があります。さらに、業務上の機能要件だけでなく、運用時の脆弱性対策を考慮した要求仕様を用意して、開発者に発注すべきでしょう。

また、ウェブサイトの運用時には、基盤ソフトやアプリケーション、ソフトウエア製品の部品等の脆弱性が突然発見されて、トラブルを招くことがあります。それらの脆弱性情報が公表された際に適切に対応できるように、システム構成を把握し、継続的に管理することが必要です。構築・改修後に、脆弱性の確認・診断を行うことも有効です。さらに、システムのメンテナンスや新システムへの移行の際には、設定や操作上のミスがないかチェックすることも重要です。

2.3. 対策実施にあたり理解すべきこと

企業における情報システムの統括責任者の方には、ウェブサイトの脆弱性対策に関する以下の点を理解していただく必要があります。

まず、脆弱性のない完璧なシステムを構築することは非常に難しいという点です。完全なシステムを追求するためには膨大な予算を投入しなければならず、コスト的に割に合いません。

また、これまでに触れてきたとおり、コンピュータシステムは、時間が経つと内在していた問題が発覚するリスクを常に抱えていて、今は安全でもいつ安全でなくなるかわかりません。つまり、システムの安全性は時間とともに劣化すると考えるべきです。安全性を維持するためには適切なメンテナンスが不可欠であり、運用・保守にも予算と人手をかける必要があります。運用・保守のスタッフを確保できない場合には、外部の事業者に委託することも有効です。

さらに、運用中のウェブサイトに脆弱性が発見された場合には、予想される脅威や影響を勘案して、適切な対策を選択すべきです。予算や人手の不足を理由に脆弱性を放置していると、1.2 で示したようなトラブルが発生してウェブサイト利用者や取引先に迷惑をかけることになりかねません。

3. ウェブサイトに脆弱性が見つかった場合

3.1. 脆弱性をどのように見つけるか

ウェブサイトに深刻な脆弱性があったとしても、トラブルもなく稼動している場合、問題に気づくことは容易ではありません。

まず、ウェブサイトで使用している基盤ソフトやアプリケーションの脆弱性が公表されることがあるので、常に情報収集に目配りする必要があります。バージョンによっても対応は異なるので、自ウェブサイトの最新の構成情報を確認しておくべきでしょう。

また、悪意の第三者による不正アクセス、コンピュータウイルスへの感染等のトラブルやその予兆をきっかけとして、プログラムの問題や設定ミスに気づくことがあります。ウェブシステムが不審な挙動を示した場合、外部から脆弱性を攻撃されたことが原因である可能性を検討すべきです。

さらに、自社のウェブサイトの脆弱性について、第三者から指摘を受けることがあります。たとえば、ウェブサイト利用者がウェブサイトを閲覧していて、偶然、重要情報にアクセスできてしまう可能性や、プログラムの動作から何らかの問題を内包している疑いに気づくことがあります。そうしたウェブサイト利用者から問い合わせを受けた場合には、速やかに調査し、脆弱性の有無を確認すべきでしょう。

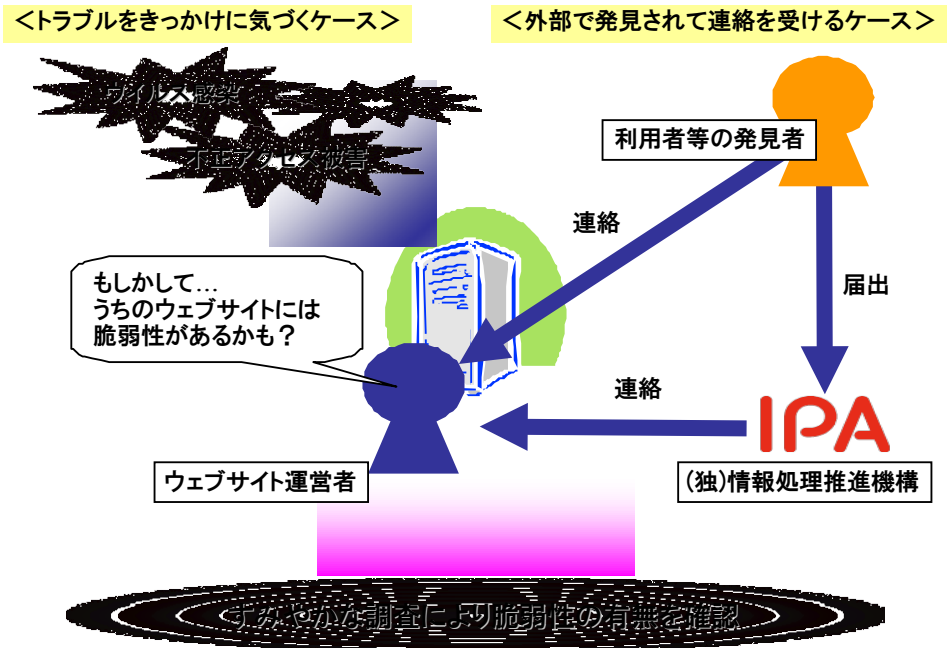


図 3-1　脆弱性に気づいたら

3.2.IPA から脆弱性に関する連絡を受けた場合

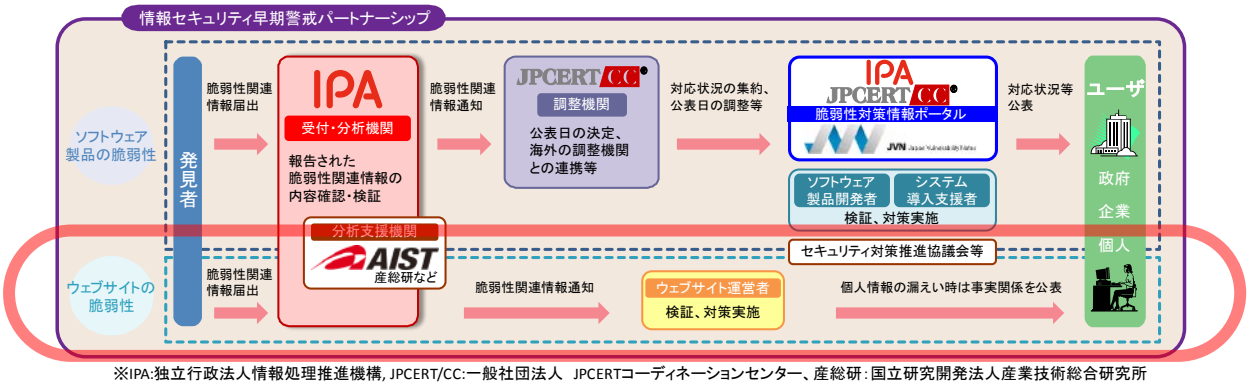
独立行政法人情報処理推進機構（IPA）では、経済産業省告示を踏まえ、2004年７月からソフトウエア製品及およびウェブアプリケーションの脆弱性に関する届出を受け付けています[7]。

(参考)

「ソフトウエア製品等の脆弱性関連情報に関する取扱規程[8]」（平成 29 年経済産業省告示第 19 号）」

「受付機関及び調整機関を定める告示（平成 29 年経済産業省告示第２０号）」

IPA では、ウェブサイトの脆弱性に関する届出を受け付けた場合、当該ウェブサイトの運営者にその旨を連絡し、脆弱性対策の実施を促します。



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

図 3-2　情報セキュリティ早期警戒パートナーシップのしくみ

3.3. 対応は意思決定から始まる

ウェブサイトの脆弱性が発見され、悪意の第三者による攻撃やコンピュータウイルスの問題が発生した場合のトラブル対応は、扱いを誤るとブランドイメージの失墜や経営基盤を揺るがす損失につながりかねません。したがって、事務機器の故障のような日常的問題の延長として捉えるのではなく、事業継続管理や危機管理の観点で捉え、企業としての意思決定に基づく対処指針や姿勢を提示すべきです。

また、外部の事業者に保守業務を委託している場合には、脆弱性対策についても契約に含め、緊急時にも円滑な対応が得られるよう、体制や費用等についてあらかじめ合意しておくことが望まれます。

---

[7] https://www.ipa.go.jp/security/vuln/index.html
[8] http://www.meti.go.jp/policy/netsecurity/index.html

4.ウェブサイト運営者のための脆弱性対応マニュアル

ウェブサイト運営者は、脆弱性の有無についての調査を基に確認し、必要であれば脆弱性修正プログラムの適用といった対策を行います。また、脆弱性について関係する内部・外部の相手や、ウェブサイト利用者との間の連絡窓口を設置し、ウェブサイト運営関係者への情報の集約と管理を担当します。

対処にあたっては全体方針や、対策の計画をウェブサイト運営者自身の判断に基づいて行うことが必要となります。

ウェブサイト運営者が脆弱性に関する連絡を外部から受け取った際の対処の流れを下図に示します。

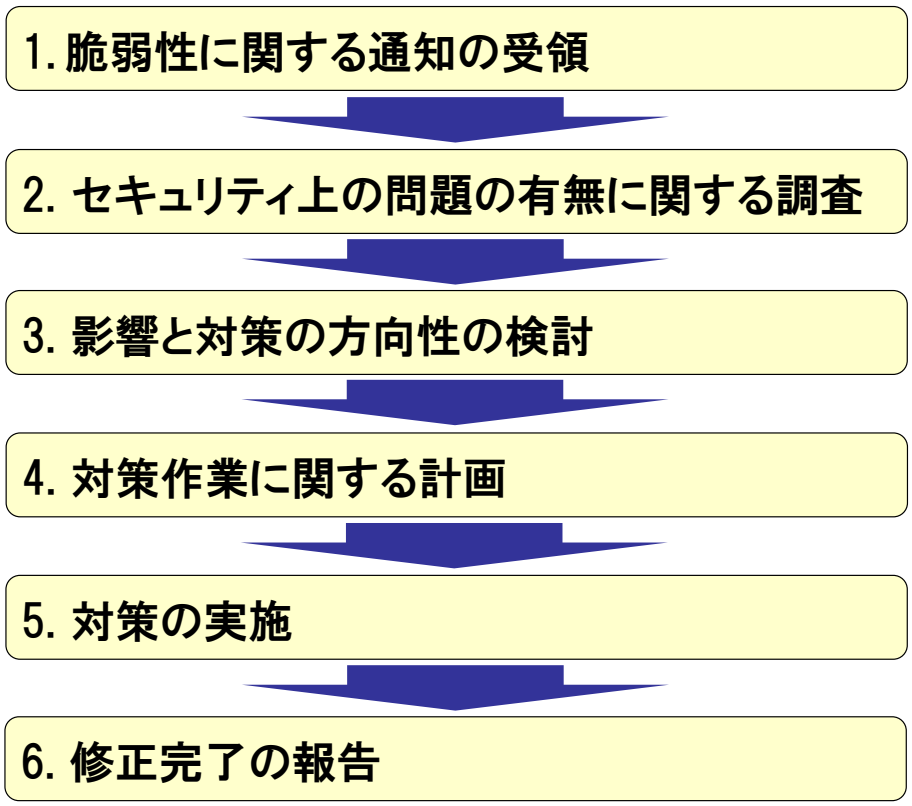


図 4-1 脆弱性関連情報への対処の流れ

4.1.対応の全体に係る留意点

（1）外部から連絡を受けた際の対応

外部から脆弱性関連情報の通知を受けた際には、IPA／発見者を含む関係者間で良いコミュニケーションを維持することが対応を成功させる鍵となります。

自発的・定期的に行われる脆弱性修正に比べると、外部から事実確認を急ぐよう求められることとなります。ウェブサイト運営者にとっては負担にもなりますが、対処の方針・計画を整理した上で、可能な範囲で説明し理解を求めることが大切です。

（2）トラブルが発生している時の脆弱性への対応

ウェブサイトにおけるセキュリティ上のトラブルに対しては、発見後の迅速な対応が必要です。不正アクセスの踏み台にされている場合、フィッシング詐欺等に悪用されている場合、ウイルスを撒き散らしている場合には、まずウェブサイトを停止し被害拡大を防ぎます。加えて、個人情報の漏洩やウェブサイト利用者へのウイルス送信等が発生した際には、速やかな被害事実の公表も望まれます。

トラブルは、ウイルスや不正アクセス等にウェブサイトの弱点＝脆弱性を狙われて起きます。被害防止のためには、ウイルス等の駆除や監視強化等の処置だけでなく、ウェブサイトの脆弱性が原因である可能性を考慮し、丁寧な調査を行って「穴を見つけて塞ぐ」ことが大切です。

脆弱性への手当てが十分でないままサービスを継続して提供すれば再び被害を受ける可能性もあります。脆弱性の調査や修正には作業時間を取る必要があります。場合によってはウェブサイトを一時的に停止するといった決断も必要です。

ウェブサイト運営者は、被害事実の公表やサービス再開のタイミングを考慮しながら、脆弱性に関する技術的作業を進めていく必要があります。

（3）SI 事業者との協力

ウェブサイトの運営形態によっては、SI 事業者に情報を渡して相談し、脆弱性の確認や対策実施に関する具体的作業を依頼する場合も想定されます。脆弱性への対処について SI 事業者の協力を得る場合については各手順に留意点を示しますので参考にしてください。

対処の詳細な作業については「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のためのガイダンス」（一般社団法人情報サービス産業協会、一般社団法人電子情報技術産業協会）[9]も参考となります。

[9] https://www.ipa.go.jp/files/000002992.pdf

4.2. 脆弱性に関する通知の受領

ウェブサイト運営者は、ウェブサイトのウェブアプリケーションの脆弱性関連情報について通知を受け付ける立場にあります。

この段階では、ウェブサイト運営者は以下の作業を行います。

⑴ 脆弱性関連情報の適切な担当者への受け渡し ⑵ 通知を受領した旨の返信 ⑶ IPA／発見者との連絡手段の確立（窓口の一元化、暗号化メールの使用、返答期限の設定、連絡記録の作成） ⑷ 組織内の対応体制の確認（担当者、報告先・報告内容、意思決定プロセス） ⑸ SI 事業者への作業依頼を行うかどうかの判断 ⑹ 発見者と直接情報交換を行うかどうかの判断 ⑺ IPA／発見者への確認（当該脆弱性を知る人は誰か、脆弱性関連情報が今後公表される可能性と時期 等）

脆弱性の通知は、IPA から連絡を受ける場合と、発見者から直接連絡を受ける場合の２つに大きく分けることができます。以下にそれぞれの場合を示します。

いずれの場合についても、ウェブサイト運営者は、通知を受け取った旨の返信を速やかに行うよう努めてください。

■ IPA から連絡を受ける場合の対応

ウェブサイトに関する脆弱性関連情報が発見者からIPAに届出られた際には、IPA からウェブサイト運営者に通知を行います。IPA からの通知は主に電子メール(vuln-contact@ipa.go.jp)を利用し２段階で行われます。

第１段階：

IPA は脆弱性の可能性があるウェブサイトに記載された連絡先アドレス宛にメールを送ります。このメールでは脆弱性の可能性があるウェブサイトの URL を知らせますが、脆弱性の詳細な情報は送りません。

ウェブサイト運営者は、より詳細な情報を受け取る連絡先（対応窓口とするアドレス)、連絡方法（パスワード保護／暗号化を用いるか否か）を記載したメールを IPA に返信してください。

第２段階：

ウェブサイト運営者が示した対応窓口アドレス宛ての電子メールで、より詳細な脆弱性関連情報を通知します。脆弱性関連情報は、主に技術的な情報で、脆弱性の種類や、現状から想定されるリスク等の情報を含みます。

また、この通知以後のメールには、取扱番号（例：IPA#12345678）が付されます。IPA と連絡を行う際にはこの番号を用います。

IPA から脆弱性関連情報を受け取った後には、受領した旨を IPA に返信してください。

IPA に脆弱性関連情報を通知した発見者の名前はウェブサイト運営者には通知されません。しかしながら、調査などでウェブサイト運営者が希望し、発見者もこれに同意した場合には、交換されるすべての写しを IPA に提供することを条件に、脆弱性関連情報の詳細に関して発見者と直接情報交換を行うことも選べます。

■ 発見者から直接連絡を受ける場合の対応

発見者がIPA を介さずに直接ウェブサイト運営者に脆弱性関連情報を通知してくることがあります。この場合は、発見者と誠実な対話に努めるようしてください。改めて IPA に届出るように発見者に求めるという選択もあります。

脆弱性関連情報を通知された場合には、以下の関連情報が含まれるかを確認します。これらの情報が含まれていない場合には IPA あるいは発見者に問い合わせてください。

1）脆弱性関連情報を既に IPA や他者に通知（公表）したかどうか。
2）脆弱性関連情報を発見者が公表する意思、公表手段と予定する時期。

＜SI 事業者に相談する場合＞

ウェブサイトの運用について SI 事業者に依頼している場合、あるいは、通知を受けたもののウェブサイト運営者自身による対処が困難と判断される場合には、SI 事業者と相談しながら対応を進める事をお奨めします。

4.3. セキュリティ上の問題の有無に関する調査

ウェブサイト運営者は、通知を受けた脆弱性についてその有無を確認し、受け取った情報の正誤を評価します。

この段階では、ウェブサイト運営者は以下の作業を行います。

⑴　確認作業に必要なリソースの確保、関係者への協力要請
⑵　問題があるウェブシステムの特定
⑶　指摘された脆弱性につながる現象の再現
⑷　脆弱性の原因と発生条件の特定
⑸　IPA あるいは発見者への進捗連絡

脆弱性の存在を確認しただけのこの段階では、もたらされ得る被害、適切な対策は未だ明確ではありません。想定される被害や対策を明らかにする作業については、ある程度の状況把握を済ませた後に改めて計画的に作業を行います。

脆弱性の存在の有無が明確になった段階で、脆弱性に関して連絡を寄せてきた相手（IPA あるいは発見者）に、脆弱性の存在および通知内容について正誤を確認した旨を連絡してください。

IPA から通知を受けた際には、IPA に相談しながら対処を進めることもできます。もし脆弱性をうまく再現できない等の場合にはご相談ください。

＜SI 事業者に調査を依頼する場合＞

確認作業について SI 事業者に依頼する場合には、経緯と既に得た情報について説明してください。SI 事業者に脆弱性関連情報等を提供した際には受領通知をもらうようにします（以後の手順でも同様です）。この時点において SI 事業者が確認した内容については簡潔な報告を受け取ってください。

4.4. 影響と対策の方向性の検討

具体的にウェブサイトの調査を行い、問題箇所が及ぼす影響をより明確にし、修正方法を検討します。この段階では以下の作業を行います。

⑴　作業に必要なリソースの確保、関係者への協力要請
⑵　脆弱性の影響範囲の調査
⑶　対策適用の影響度の調査
⑷　修正方法の検討
⑸　スケジュールの見積もり
⑹　対応費用の見積り
⑺　検討報告および対応方針案のとりまとめ

IPA から通知を受けた場合、スケジュールについては、詳細情報の通知を受けてから 3 ヶ月以内を目処に対応してください。3 ヶ月以内での対応が難しい場合、対応に要する期間の見積りを IPA にご連絡ください。

＜SI 事業者に対策の検討を依頼する場合の進め方＞

SI 事業者には上記の⑵～⑺の具体的項目についての調査検討を依頼します。ウェブサイト運営者は SI 事業者に上記の調査作業を進める上で必要なシステムに関する情報、作業に必要な環境や権限等を適宜提供し、SI 事業者がとりまとめた検討報告および対応方針案を受けとってください。

4.5. 対策作業に関する計画

対策作業に取り掛かる前に計画を立てます。SI 事業者に対策の実施を依頼する場合には、作業計画他幾つかの事項について調整をはかり合意をとります。この段階では以下の作業を行います。

⑴　これまでに収集した情報の整理と共有 ⑵　当該ウェブサイトに関する契約の確認 ⑶　対策基本姿勢・優先事項の明確化 ⑷　費用、人員、作業時間、その他対策実施に必要なリソースの確保 ⑸　対策計画の確定 ⑹　作業時の連絡体制の確認 ⑺　作業実施に係る SI 事業者との調整

問題のあったウェブサイトに関して、外部の構築担当者や運用担当者との間で結んだ契約があれば、その内容を確認しておきます。

ここまでに明らかになった情報を整理して関係者で共有し、要点を確認します。ウェブサイト運営者として、問題となる脆弱性にどのような対応を行うかについて基本的な対応方針を決定します。合わせて対策作業に必要な費用、人員、作業時間等のリソースの確保についても組織内で同意を取っておきます。

これまでの作業で作成した対策案をベースに対策に関する計画を確定させます。また、作業時の連絡体制についても確認しておきます。

＜SI 事業者に対策の実施を依頼する場合＞

SI 事業者に対策の実施（次項）を依頼する場合には、検討報告・対応方針案をベースにして、ウェブサイト運営者と SI 事業者の双方で計画を具体化します。これには費用、スケジュール、その他リソースの確保についての調整が含まれます。また、SI 事業者から進捗報告を受けるタイミングについても計画しておきます（作業の大きな節目、作業が長引く場合には一定期間 等）。

4.6. 対策の実施

作業計画に基づく対策を実施します。技術者による修正作業が中心となりますが、同時にウェブサイトの運用に関する留意も必要となります。

ウェブサイト運営者から SI 事業者に実施を依頼する場合には、SI 事業者は事前に調整した作業を実施します。この段階では以下の作業を行います。

⑴　対策作業に伴う一時停止等に関するウェブサイト利用者へのアナウンス
⑵　ウェブサイト利用者への作業実施期間中の代替手段の提供・案内
⑶　修正の作成
⑷　試験環境でのテストと実施手順作り
⑸　対策の実施適用
⑹　対策効果の確認
⑺　ウェブサイト利用者からの問い合わせへの対応
⑻　進捗報告の作成

ウェブサイト運営者は、ウェブサイト利用者に対して作業に伴うウェブサイト一時停止等のアナウンスを行います。あわせて作業中に生じうるウェブサイト利用者への対応（代替手段の提供、問い合わせへの返答 等）について必要な手配を行います。

対策実施の技術的な部分の手順は、修正の作成、試験環境でのテストと実施手順作り、対策の実施適用、対策効果の確認、の 4 段階からなります。

対策効果の確認に際しては、適切かつ有効な対策が施されていることを診断・確認します。最新の対策について情報を持つ外部の監査ベンダを利用することも有効です。

＜SI 事業者に対策の実施を依頼する場合＞

対策の実施について SI 事業者に作業を依頼する場合には、前項に示すように計画に沿って進めてください。進捗については適宜報告を受けるようにします。

4.7. 修正完了の報告

脆弱性の対応が完了したら、ウェブサイト運営者は以下の作業を行います。

（1） IPA／発見者への修正完了報告

IPA から連絡を受けて対応に当たった場合には修正完了報告（取扱番号、対象のウェブサイト URL、対応の内容を含む報告）を IPA へお願いします。

4.8. その他

問題となった脆弱性に関連して、個人情報漏えい等のトラブルが発生した場合には、事故に関する報告を行います。これには、ウェブサイト利用者への告知、主務官庁等への報告等が含まれます。また、個人情報が流出した場合には、二次被害を防ぐために、影響を受ける可能性のある本人に可能な限り連絡することが望まれます[10]。

（詳細は「個人情報保護 個人情報の保護に関するガイドラインについて」を参照してください）。

[10]個人情報保護委員会「個人情報保護 個人情報の保護に関するガイドラインについて」
http://www.ppc.go.jp/files/pdf/personal_guideline_ministries.pdf

付録：脆弱性について通知を受けた場合の作業 チェックリスト

IPA／発見者より脆弱性に関する連絡を受けた際の対処について、全体の流れが分かるように、各段階の概要を簡潔に示し、各段階でウェブサイト運営者が取る行動を一覧形式で示します。

No　　チェック項目	チェック	SI 事業者が協力可能な項目
1.脆弱性に関する通知の受領		
(1)　脆弱性関連情報の適切な担当者への受け渡し	□	
(2)　通知を受領した旨の返信	□	
(3)　IPA／発見者との連絡手段の確立	□	
(4)　組織内の対応体制の確認	□	
(5)　SI 事業者への作業依頼を行うかどうかの判断	□	
(6)　発見者と直接情報交換を行うかについての判断	□	○
(7)　IPA／発見者への確認	□	○
2.セキュリティ上の問題の有無に関する調査		
(1)　確認作業に必要なリソースの確保、関係者への協力要請	□	
(2)　問題があるウェブシステムの特定	□	○
(3)　指摘された脆弱性につながる現象の再現	□	○
(4)　脆弱性の原因と発生条件の特定	□	○
(5)　IPA あるいは発見者への進捗連絡	□	
3.影響と対策の方向性の検討		
(1)　作業に必要なリソースの確保、関係者への協力要請	□	
(2)　脆弱性の影響範囲の調査	□	○
(3)　対策適用の影響度の調査	□	○
(4)　修正方法の検討	□	○
(5)　スケジュールの見積もり	□	○
(6)　対応費用の見積り	□	○
(7)　検討報告および対応方針案のとりまとめ	□	○

4.対策作業に関する計画		
(1) これまでに収集した情報の整理と共有	□	○
(2) 当該ウェブサイトに関する契約の確認	□	
(3) 対策基本姿勢・優先事項の明確化	□	○
(4) 費用、人員、作業時間、その他対策実施に必要なリソースの確保	□	
(5) 対策計画の確定	□	○
(6) 作業時の連絡体制の確認	□	○
(7) 作業実施に係るSI事業者との調整	□	○
5.対策の実施		
(1) 対策作業に伴う一時停止等に関するウェブサイト利用者へのアナウンス	□	
(2) 利用者への作業実施期間中の代替手段の提供・案内	□	○
(3) 修正の作成	□	○
(4) 試験環境でのテストと実施手順作り	□	○
(5) 対策の実施適用	□	○
(6) 対策効果の確認	□	○
(7) 利用者からの問い合わせへの対応	□	
(8) 進捗報告の作成	□	○
6.修正完了の報告		
(1) IPAあるいは発見者への修正完了報告	□	

・本資料の位置付け

近年、日本国内においてソフトウエア製品やウェブアプリケーションの脆弱性が発見されることが増えており、これらの脆弱性を悪用した不正アクセス行為やコンピュータウイルスの増加により、企業活動が停止したり情報資産が滅失したり個人情報が漏洩したりといった、重大な被害が生じています。

そこで、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した、「ソフトウエア等脆弱性関連情報取扱規程」が制定されました（平成 29 年経済産業省告示第 19 号）。この告示をふまえ、関係者に推奨する行為をとりまとめた「情報セキュリティ早期警戒パートナーシップガイドライン」 が公表されています。

本資料は、このガイドラインの別冊資料であり、ウェブサイトの脆弱性がもたらすトラブルや運営者に問われる責任、ウェブサイトに求められる継続的な対策、脆弱性が見つかった場合の対応手順などを概説したものです。主にウェブサイト運営者による活用を想定しており、脆弱性に関する通知を受けた場合の望ましい対応手順について、一つの方針を示しています。

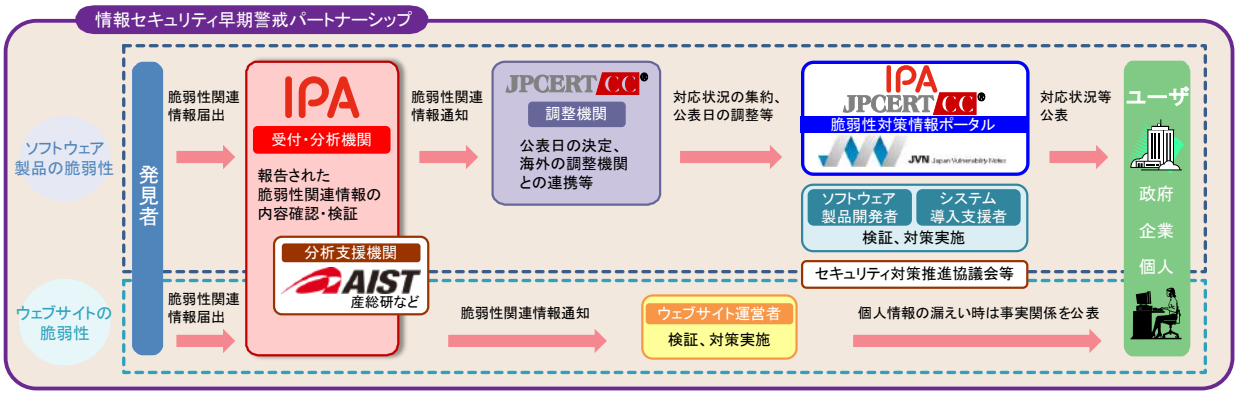
関係者の方々は、脆弱性対応に向けた体制の検討や、実際の対応に際し、本資料を参考にご対応くださいますようお願い申し上げます。

本資料の配布に制限はありません。本資料は、次の URL からダウンロードできます。

https://www.ipa.go.jp/security/ciadr/partnership_guide.html

http://www.jpcert.or.jp/vh/index.html#link_japan

・「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

・本資料に関するお問合わせ先

独立行政法人情報処理推進機構（略称:IPA）　技術本部　セキュリティセンター

〒113-6591　東京都文京区本駒込二丁目 28 番 8 号　文京グリーンコートセンターオフィス 16 階

https://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7552

ウェブサイト運営者のための脆弱性対応ガイド

－ 情報セキュリティ早期警戒パートナーシップガイドライン－

２００８年　２月２８日　第１版発行
２００９年　７月　８日　第２版第２刷発行
２０１３年　３月２９日　第２版第３刷発行
２０１５年　３月２６日　第３版発行
２０１７年　３月３０日　第３版第２刷発行
［著作・制作］　情報システム等の脆弱性情報の取扱いに関する研究会
［事務局・発行］　独立行政法人情報処理推進機構