



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
付録 6 抜粋編

2008 年 4 月

独立行政法人 情報処理推進機構
有限責任中間法人 JPCERT コーディネーションセンター
社団法人 電子情報技術産業協会
社団法人 コンピュータソフトウェア協会
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	3
1.1. 背景	3
1.2. ウェブサイトで起こるトラブル	4
1.3. 運営者に問われる責任	6
1.4. 本資料の目的	6
2. ウェブサイトに必要な対策	7
2.1. トラブルの原因となる脆弱性	7
2.2. 求められる継続的な対策	8
2.3. 対策実施にあたり理解すべきこと	8
3. ウェブサイトに脆弱性が見つかった場合	9
3.1. 脆弱性をどのように見つけるか	9
3.2. IPA から脆弱性に関する連絡を受けた場合	10
3.3. 対応は意思決定から始まる	10
4. ウェブサイト運営者のための脆弱性対応マニュアル	11
4.1. 対応の全体に係る留意点	12
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、インターネットユーザの拡大とともに、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したり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、今やユーザ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。

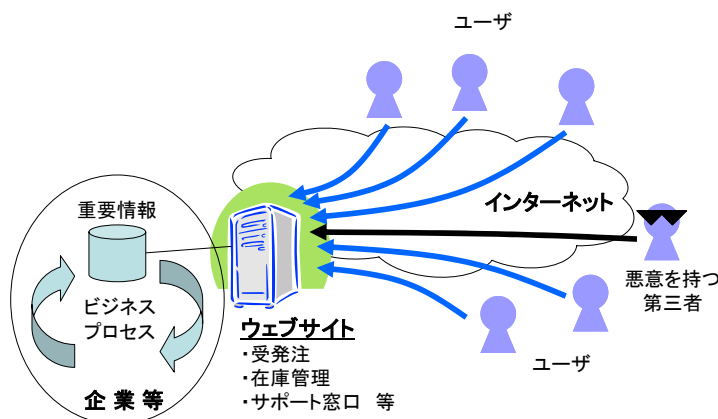


図 1-1 ビジネスプロセスの一端を担うウェブサイトとリスク

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。

トラブル事例 1 不正侵入による情報流出、踏み台化

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、個人情報などの重要情報が詐取されたり、ウェブサイトが悪用できるように改造されることがあります。

2005年5月、情報提供サービスA社では、自社の情報サイトが不正侵入されその対応が遅れたため、エンドユーザのメールアドレスが大量に流出した上に、サービスを約10日間停止せざるをえない事態に陥りました。その結果、売上は1億5000万円～2億5000万円程度減少し、90万円台後半だった株価は一時80万円台後半に急落するなどの金銭的被害を受けました。さらに、こうした影響は自社内にとどまらず、株主や取引先、エンドユーザなどのステークホルダにも及び、A社の社会的信用は大きく損なわれました。

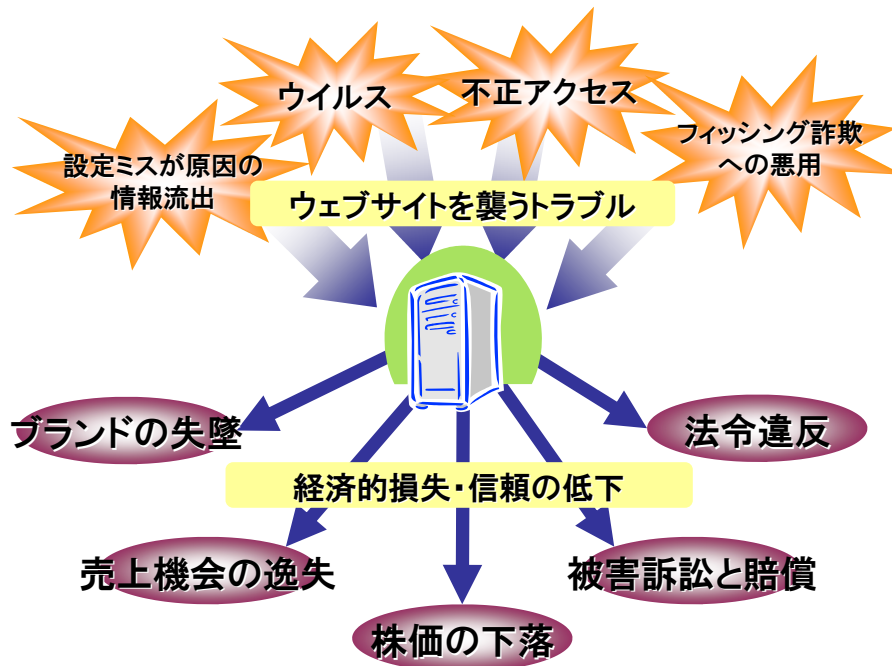


図 1-2 ウェブサイトで起こるトラブル

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))

トラブル事例2 設定ミスによる個人情報の流出

システム管理者の設定ミスが情報流出のトラブルを招くこともあります。たとえば、個人情報の含まれた重要ファイルが、誤ってウェブサイトの公開ディレクトリに置かれているケースです。こうしたミスは、サーバの更新や新システムへの移行などの変更時に生じることが多いと考えられます。

2002年5月、エステティック事業のB社が運営するサイトで、約5万人分の個人情報を含む電子ファイルが誤って閲覧可能な状態になっていたため、外部に流出してしまいました。流出した電子ファイルは、回収することが事実上不可能で、今なおファイル共有ソフトを介してネットワーク上で流通していると見られます。複数の被害者がB社を相手にプライバシー侵害に関する訴訟を起こし、地裁はB社に一人当たり数万円の賠償金を支払うよう命じる判決を下しました。

トラブル事例3 フィッシング詐欺への悪用

自社のウェブサイトをフィッシング詐欺²などの犯罪行為に悪用されることもあります。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。

2006年には、米最大手のオークションサイトにクロスサイト・スクリプティングの脆弱性が発見され、さらに、この脆弱性を悪用したフィッシングサイトも出現しました。同サイトのユーザが脅威にさらされたことによって、顧客との信頼関係がビジネス基盤である同社のブランドの失墜が懸念されました。

そのほか、ウェブシステムがダウンしサービス停止に陥ったり、表示内容が書き換えられるといったトラブルが発生する可能性があります。

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 Web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）： ソフトウェア等において、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つては、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。

1.3. 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、ウェブサイトの運営者は、ユーザに対して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」は一義的にはそのサイトの運営者であり、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を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、ソフトウェア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たり、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。

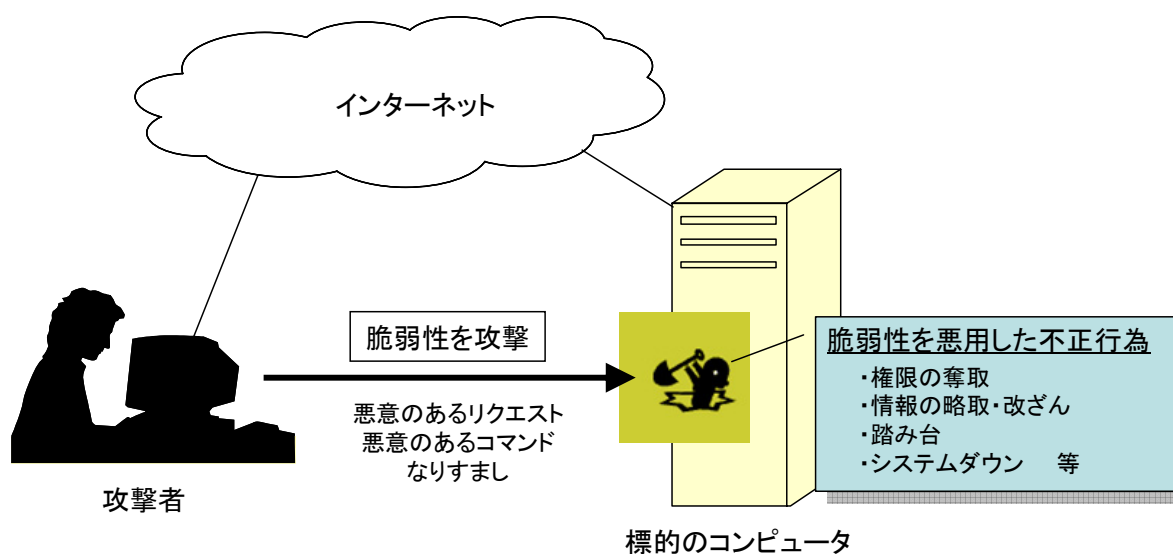


図 2-1 脆弱性を悪用するイメージ

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、ソフトウェア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、外部の事業者へ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ユーザー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、ユーザがウェブサイトを利用していて、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。そうしたユーザ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。

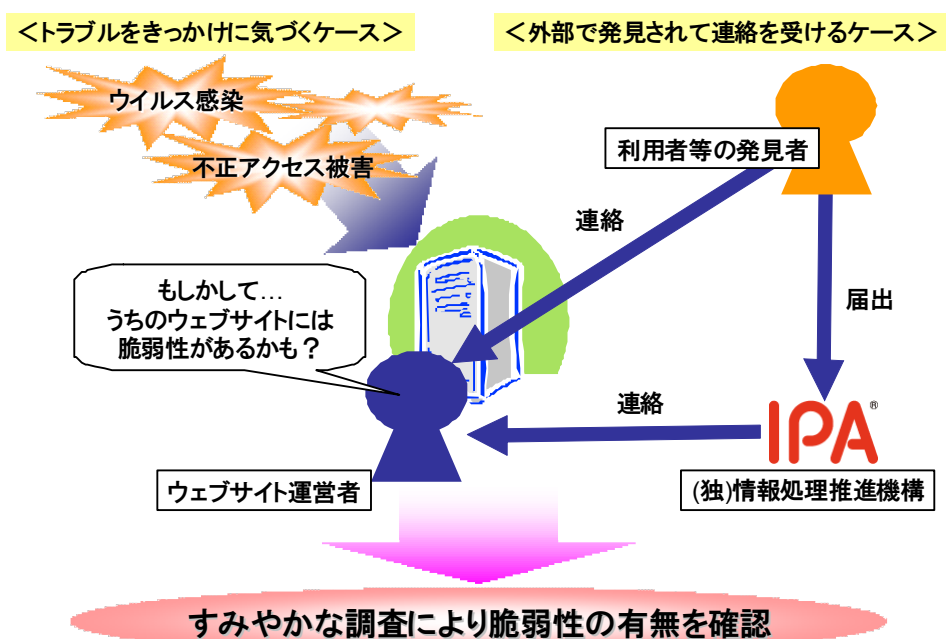


図 3-1 脆弱性に気づいたら

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、サイトの利用者との間の連絡窓口を設置し、ウェブサイト側で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。

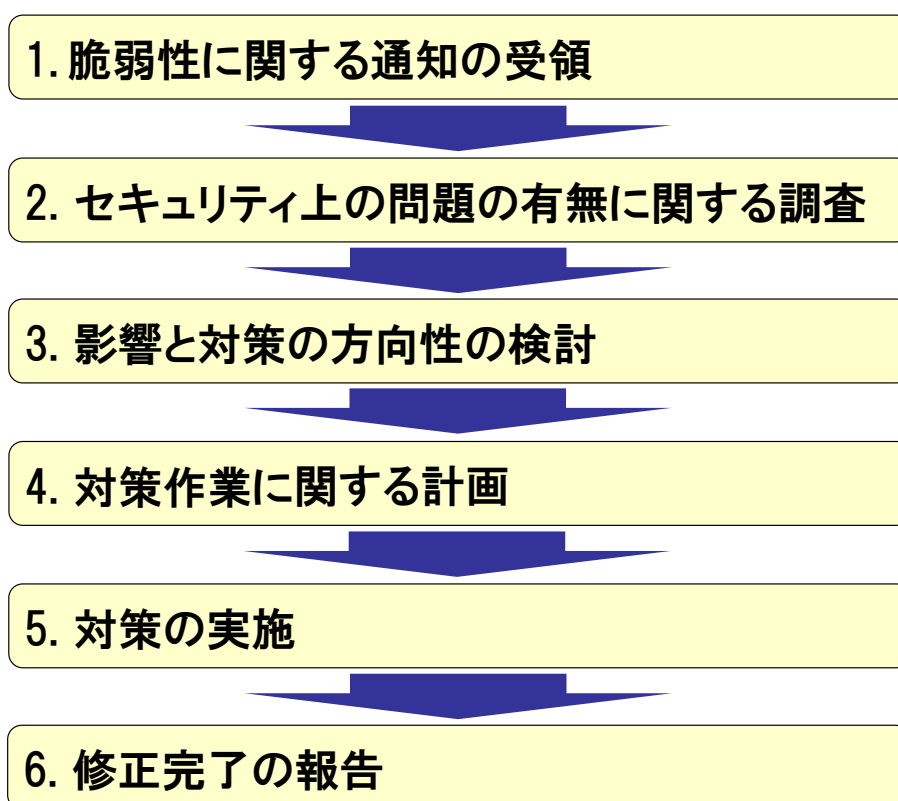


図 4-1 脆弱性関連情報への対処の流れ

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、個人情報の漏洩や利用者へのウイルス送信等が発生した場合には、速やかな被害事実の公表も望めます。

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

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」（社団法人 情報サービス産業協会、社団法人 電子情報技術産業協会）⁷も参考となります。

⁷ http://www.jisa.or.jp/report/2004/vulhandling_guide.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、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。

- (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（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）
- (4) 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）
- (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どうかの判断
- (7) 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）

通知は、IPA がウェブサイト運営者に通知してくる場合と、発見者がサイト運営者に直接通知してくる場合の 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について示します。

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 3 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）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に宛てた電子メールで、今後の連絡メールに用いる暗号化について確認します。

第3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から詳細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事業者にご相談する場合>

サイト運用について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。

- (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

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 より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 事業者調査を依頼する場合>

確認作業についてSI 事業者へ依頼する場合には、経緯と既に得た情報について説明してください。SI 事業者へ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。

- (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

IPA より通知を受けた場合、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(2)～(7)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。

- (1) これまでに収集した情報の整理と共有
- (2) 当該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

問題のあったサイトに関して、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 事業者を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。

- (1) 対策作業に伴う一時停止等に関する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

ウェブサイト運営者は、サイトの利用者に対して作業に伴う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る利用者への対応（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ー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 より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 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、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⁸。

⁸ 内閣府 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://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html>

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	<input type="checkbox"/>	
(2)	通知を受領した旨の返信	<input type="checkbox"/>	
(3)	IPA／発見者との連絡手段の確立	<input type="checkbox"/>	
(4)	組織内の対応体制の確認	<input type="checkbox"/>	
(5)	SI事業者への作業依頼を行うかどうかの判断	<input type="checkbox"/>	
(6)	発見者と直接情報交換を行うかについての判断	<input type="checkbox"/>	○
(7)	IPA／発見者への確認	<input type="checkbox"/>	○
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	<input type="checkbox"/>	
(2)	問題があるウェブシステムの特定	<input type="checkbox"/>	○
(3)	指摘された脆弱性につながる現象の再現	<input type="checkbox"/>	○
(4)	脆弱性の原因と発生条件の特定	<input type="checkbox"/>	○
(5)	IPAあるいは発見者への進捗連絡	<input type="checkbox"/>	
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	<input type="checkbox"/>	
(2)	脆弱性の影響範囲の調査	<input type="checkbox"/>	○
(3)	対策適用の影響度の調査	<input type="checkbox"/>	○
(4)	修正方法の検討	<input type="checkbox"/>	○
(5)	スケジュールの見積もり	<input type="checkbox"/>	○
(6)	対応費用の見積り	<input type="checkbox"/>	○
(7)	検討報告および対応方針案のとりまとめ	<input type="checkbox"/>	○

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	<input type="checkbox"/>	<input type="radio"/>
(2) 当該サイトに関する契約の確認	<input type="checkbox"/>	
(3) 対策基本姿勢・優先事項の明確化	<input type="checkbox"/>	<input type="radio"/>
(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	<input type="checkbox"/>	
(5) 対策計画の確定	<input type="checkbox"/>	<input type="radio"/>
(6) 作業時の連絡体制の確認	<input type="checkbox"/>	<input type="radio"/>
(7) 作業実施に係るSI事業者との調整	<input type="checkbox"/>	<input type="radio"/>
5.対策の実施		
(1) 対策作業に伴う一時停止等に関するサイト利用者へのアナウンス	<input type="checkbox"/>	
(2) 利用者への作業実施期間中の代替手段の提供・案内	<input type="checkbox"/>	<input type="radio"/>
(3) 修正の作成	<input type="checkbox"/>	<input type="radio"/>
(4) 試験環境でのテストと実施手順作り	<input type="checkbox"/>	<input type="radio"/>
(5) 対策の実施適用	<input type="checkbox"/>	<input type="radio"/>
(6) 対策効果の確認	<input type="checkbox"/>	<input type="radio"/>
(7) 利用者からの問い合わせへの対応	<input type="checkbox"/>	
(8) 進捗報告の作成	<input type="checkbox"/>	<input type="radio"/>
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	<input type="checkbox"/>	

・本資料の位置付け

近年、日本国内においてソフトウェア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、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」が制定され、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(2008年4月4日改訂版)の付録6「ウェブサイト運営者のための脆弱性対応マニュアル」を全文抜粋し、ウェブサイトの脆弱性をもたらす具体的なトラブルや運営者に問われる責任、ウェブサイト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。

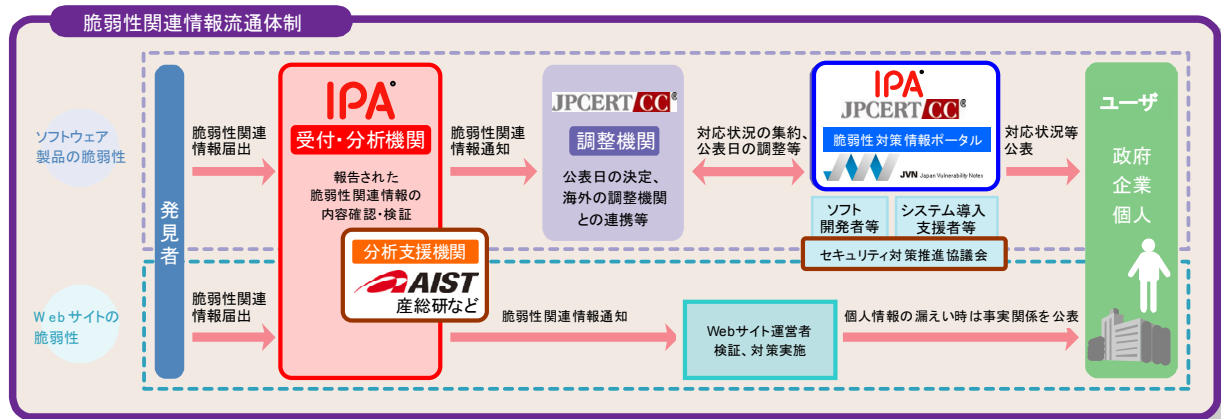
関係者の方々は、脆弱性対応に向けた体制の検討や、実際の対応に際し、本資料を参考にご対応くださいようお願い申し上げます。

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。

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

<http://www.jpccert.or.jp/vh/#guideline>

・脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※JPCERT/CC:有限責任中間法人 JPCERT コーディネーションセンター、産総研:独立行政法人 産業技術総合研究所

・本資料に関するお問い合わせ先

独立行政法人 情報処理推進機構(略称:IPA) 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

<http://www.ipa.go.jp/security/> TEL: 03-5978-7527 FAX: 03-5978-7518

ウェブサイト運営者のための脆弱性対応ガイド

ー 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 付録6 抜粋編 ー

[発行] 2008年 2月28日 第1版
2008年 4月 4日 第2版

[編著者] 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] 独立行政法人 情報処理推進機構