ウェブサイト構築事業者のための
脆弱性対応ガイド

～ウェブサイト構築にかかわるすべての人に～

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 7 抜粋編

2009 年 7 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
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

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。

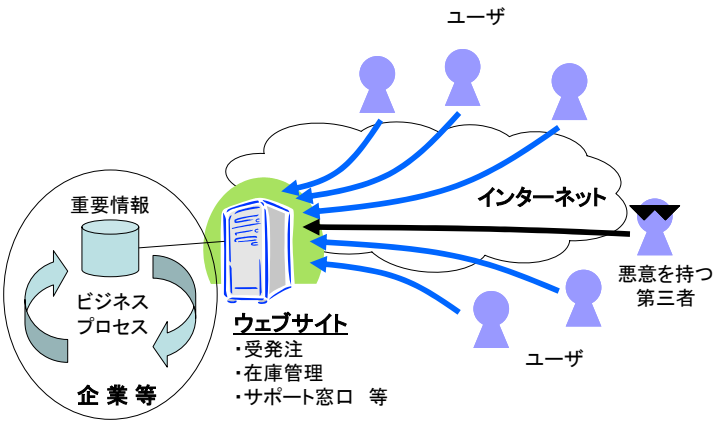


図 1-1 ビジネスプロセスの一端を担うウェブサイトとリスク

1.2. ウェブサイトで起こるトラブル

ウェブサイトで起きる情報セキュリティ上のトラブルは、たとえば以下のようなケースがあります。ウェブサイト構築事業者は、顧客であるウェブサイト運営者がこうしたトラブルに陥ることのないよう、可能な限り適切な対応を行うことが望まれます。

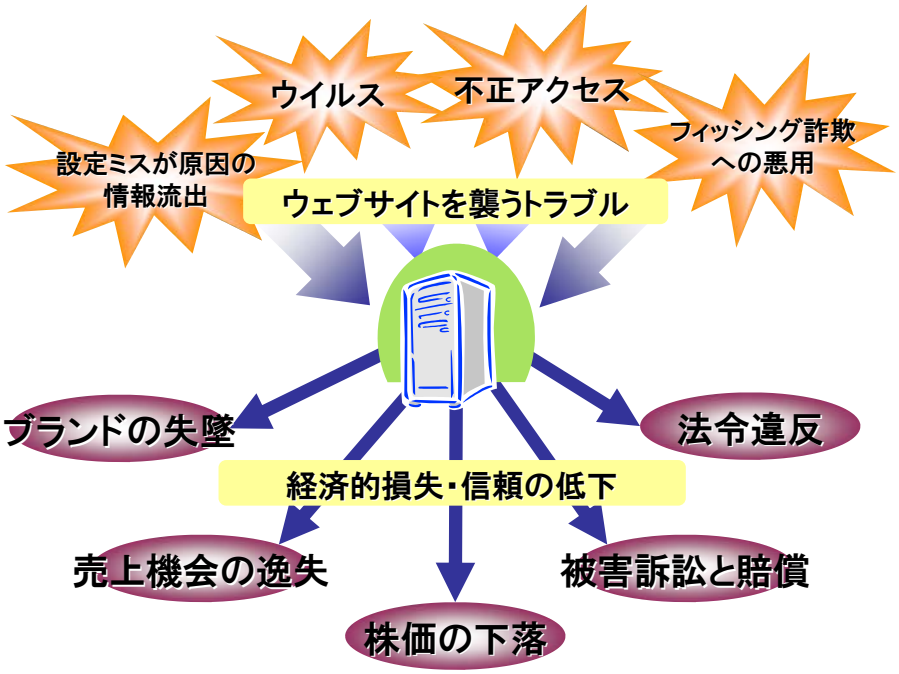


図 1-2 ウェブサイトで起こるトラブル

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を経由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、個人情報等の重要情報が詐取されたり、ウェブサイトを悪用できるように改造されることがあります。

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ました。さらに、サイトにアクセスしてきたエンドユーザにウイルスを送り込むように改ざんされていました。この背景には、攻撃者が容易に攻略可能な状態であったにもかかわらず、ウェブサイトの構築・運用の現場のリスク意識が乏しく、脆弱性が放置されていたことが挙げられます。

[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を、誤ってウェブサイトの公開ディレクトリに置いてしまうケースです。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。

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の回収は事実上不可能であり、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。システム管理者のミスが、会社に金銭的損害や信用失墜という損失をもたらしたのです。

トラブル事例３　フィッシング詐欺の踏み台としての悪用

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。

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が出現しました。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。

トラブル事例４　ウェブサイトで配布していたソフトウェアの問題

ウェブサイトそのものの問題ではありませんが、公的機関Ｃのウェブサイトにおいて配布していたエンドユーザ向けのソフトウェアに脆弱性があることが発覚しました。

---

[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] 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。

1.3. 構築事業者に期待される役割

ウェブサイト構築事業者は、顧客の求めるウェブシステムを構築する立場にあります。発注仕様に基づき、機能やデザインに配慮したシステムを開発・納入することが求められているのは当然ですが、「安全」が大前提なのはいうまでもありません。

我が国では、企業の多くがウェブサイトを独自開発するため、類似の脆弱性について横断的に対処することができません。また、ユーザ企業側は脆弱性の問題について必ずしも詳しいとは限りません。したがって、ウェブサイト構築事業者が脆弱性対策に配慮し、トラブルの発生を抑制することが望まれます。

しかし、残念ながら、顧客に納入したシステムやその中に組み込まれたソフトウェアが脆弱性を内包している可能性は否定できません。少なくとも、既に公表されている脆弱性について適切な対策を行わずにシステムを納入したり、ウェブサーバに設定漏れや設定ミス等があった結果、事件・事故が発生した場合、ウェブサイト構築事業者は自らの問題として真摯に対応することが求められます。

そうした事態を避けるために、ウェブサイト構築事業者はあらかじめ見た目の品質と同様に、セキュリティ上の品質についても担保し、対策しておく必要があります。特に、個人情報や営業秘密等、顧客にとって機微な情報を扱うシステムであれば、設計・開発の段階から適切に対処しておく必要があります。

1.4.本資料の目的

本資料の想定層は、ウェブサイトの構築を行うウェブサイト構築事業者の方を想定しています。具体的には、システムインテグレータをはじめとする情報サービス企業のシステム・エンジニアや、ウェブサイトのデザイナーのように顧客に対してシステム構築サービスを提供される方、また、社内のユーザ部門の要請に応じてシステムを構築する情報システム部門の方が該当します。

本資料では、ウェブサイトに脆弱性を残さないようにするために行うべきことはなにか、またウェブサイトの脆弱性が発見された場合にどう対処するかを紹介することが目的です。特に、保守・運用の予算が乏しく、半ば作り放しになってしまうケースについても、トラブルの発生を極力防ぐよう、システムの設計・開発段階に心がけるべき点を解説します。さらに、脆弱性対策の必要性について、顧客に説明する際の資料として活用することも可能です。

2.納入前に考慮すべきこと

2.1. 契約段階で望まれること

顧客が、情報システムの有するリスク（脆弱性が突然発覚する可能性があること、そのような未知の脆弱性は開発時に排除できないため、運用時の対応が不可欠であること）を理解していないと、適切な保守が行われない可能性があります。

したがって、ウェブサイト構築事業者の方は、契約の段階から脆弱性に係る問題について十分に説明し、保守の重要性を顧客に理解していただけるよう努力することが期待されます。

■顧客に向けた事前説明

顧客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脆弱性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、保守・運用にも予算と人手をかける必要があります。保守・運用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ユーザや取引先に迷惑をかけることになりかねません。

■契約時に合意すべき事項

契約時には、以下のような脆弱性対策の取扱いについて、顧客や再委託先等の関係者と合意を取り付けることが望まれます。

・ 納入後に公表された新規の脆弱性対策

ソフトウェア製品の脆弱性のうち、納入後に製品開発ベンダや JVN[5]で公表された新規のものについては、対策を有償とすべきであり、開発とは別の保守契約で対応するのが適切と考えられます。

・ 既知の重要な脆弱性対策

ソフトウェア製品の既知の重要な脆弱性やウェブアプリケーションの著名な脆弱性の対策に関する著しい認識不足、ウェブアプリケーションに対する必要な設定漏れ、設定ミスなどウェブサイト構築事業者の責に帰する場合は無償とすべきです。

・ セキュリティ検査の実施の有無

ウェブサイトに対し脆弱性の有無を確認するセキュリティ検査を納入前に行うか否かにより、既知の脆弱性対策でカバーできる範囲が大きく異なります。顧客のニーズや予算に依存しますが、検査の実施と既知の脆弱性対策については連動することを説明すべきです。

・ 緊急事態時の費用負担

緊急事態の際は迅速な対策を要求されるため、顧客との間で作業範囲、費用負担について十分な協議のないまま、作業を進める状況が多々あると予想されます。契約の段階で明確にしておくべきですが、それが難しい場合にも、極力、覚書として残しておくことが望ましいと考えられます。

また、これらの事項は、顧客企業と一次請けのウェブサイト構築事業者の間の契約を想定していますが、二次請け、三次請けの事業者も同様な観点での対応を考慮しておくべきです。

■その他望ましい対応

さらに、顧客企業の担当部門のニーズによっては、経営層が投資規模について的確に判断できるよう、発見された脆弱性によって引き起こされる事件・事故による被害の大きさと対策案費用を比較した資料を作成するなどの支援を行うことも考えられます。

また、ウェブサイトは、ウェブアプリケーションとその基盤となるソフトウェア（OS, ミドルウェア等）で構成されるが、それぞれの脆弱性の対処策が異なることに留意すべきです。前者は、ウェブサイト構築事業者が新規開発する部分であり、設計・開発段階で脆弱性を残さないよう考慮する必要があります。

[5] "Japan Vulnerability Notes"の略。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト。http://jvn.jp/

一方、後者は、納入前の時点で既知の脆弱性については、あらかじめ修正プログラム（パッチ）を適用して、脆弱性対策を済ませておくことが期待されます。

2.2.安全性を確保するための取組み方

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。予算や人手、開発期間等の制約があるのは当然ですが、顧客のウェブサイトに問題が生じた場合にユーザや取引先が被る影響を考慮し、ウェブサイト構築事業者としてはできる限りの対応を行うよう、顧客と調整すべきです。すでに運用を開始しているウェブサイトにセキュリティ上の問題が発覚した場合、設計・開発レベルから修正することは難しい場合が少なくなく、場あたり的な対策で済まさざるをえないこともあります。したがって、対策は可能な限り、設計・開発段階で適用することが望まれます。

■企画段階の取組み

企画時には、ウェブシステムのセキュリティ方針について検討します。特に社外向けのサービスを提供するウェブシステムの場合、セキュリティポリシーを含む多面的な視点から、セキュリティ機能に必要な要件を十分に検討する必要があります。

【考慮すべき事項の例】

- ウェブサイトを用途（公開・管理）別に分離する必要はあるか
- アクセス制御（認証・許可・管理）を行う必要はあるか、どうやって行うか
- 個人情報を収集するか／どういったポリシーで扱い、どうやって保護するか
- ログ情報をどこまで収集するか／いつまで保護するか
- ユーザを識別するか／セッション管理をどうするか
- 予算と工数から、どれだけセキュリティの設計に回せるか
- 新技術・新製品を採用するか

■設計・開発段階の取組み

設計・開発時には、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について顧客と合意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、保守も含めた運用時の脆弱性対策を考慮した要求仕様を用意するよう、顧客と調整すべきでしょう。

もちろん、予算や期間の制約から十分な対応ができない可能性もありますが、そのような状況であっても、最低限行うべきことがあります。たとえば、図 2-1 に示したように[6]、ウェブサイトの脆弱性の中でも独立行政法人情報処理推進機構（IPA）への届出件数が非常に多いクロスサイト・スクリプティングと SQL インジェクション[7]の脆弱性は、プログラミングの際に残されるケースが大半であり、開発段階でこの 2 つの脆弱性に気をつけるだけでも大きな効果があります。これらの具体的な対策については、「安全なウェブサイトの作り方」（IPA）[8]を参照してください。

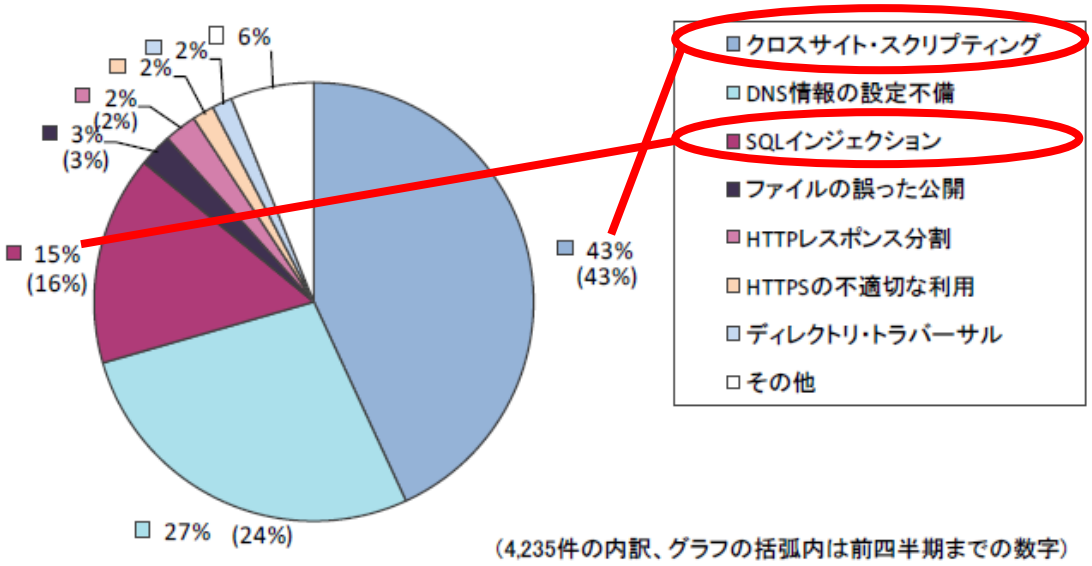


図 2-1　ウェブサイトの脆弱性種類別内訳
（届出受付開始から 2009 年 3 月末まで）

[6] 最新の状況は次の URL の「脆弱性関連情報の届出状況」を参照下さい。
http://www.ipa.go.jp/security/vuln/report/press.html

[7] 悪意あるリクエストにより、データベースの不正利用をまねく可能性がある脆弱性。データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にデータベースへの命令文を組み立てるが、命令文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性がある。

[8] http://www.ipa.go.jp/security/vuln/websecurity.html

2.3. 問題を招きやすいケース

契約から納入までのプロセスにおいて、脆弱性に係るトラブルを招く原因となりやすい事象として、たとえば以下のケースが挙げられます。

■曖昧なセキュリティ要件

仕様におけるセキュリティ要件が曖昧であったために、本来は契約外である脆弱性対策の負担をウェブサイト構築事業者に求められることがあります。本来の機能・処理に関する仕様が優先され、セキュリティ要件の策定は後回しにされやすいこと、また技術的な詳細が理解しにくいため、包括的な記載になりがちであることなどから、結果的に、納入後に判明した新しい脆弱性の対策まで、すべて対応するように読める場合があります。

したがって、脆弱性対策の部分については、記載事項を定型化しておき、契約段階であらかじめ意思表示しておくことが望ましいと考えられます。

■サンプルプログラムの流用

予算や開発期間を抑制するため、サンプルプログラムを流用することもありますが、そこに脆弱性が含まれているケースが見られます。一般に、サンプルプログラムは、わかりやすさを優先するため、セキュリティ的な配慮が乏しいことが多いためと考えられます。

したがって、安全性が担保されていないサンプルプログラムを安易に流用することは避けるべきでしょう。少なくとも、ID・パスワードの処理（セッション管理を含む）、ユーザの入力欄の処理、データベースの処理等については、慎重に検討すべきです。できれば、広く利用されている開発フレームワークを活用することが望ましいと考えられます。

■不十分なコードレビュー

予算や開発期間の制約等により、コードレビューが不十分になることがあります。その場合、ブラックボックステスト（ペネトレーションテスト）では見つけられない脆弱性を内包してしまう可能性が高くなります。

少なくとも重大なリスクが想定されるコードについては重点レビューを行ったり、コード検査を自動化するなどして、より早期のコーディング段階で脆弱性を作りこまないように対処しておくべきです。

■不十分な開発標準、自作の開発フレームワークの使用

Spring や Struts など、広く利用されている開発フレームワークはセキュアな機能を内包していますが、開発者がそうした機能を使用していないケースが見受けられます。

そのようなことのないよう、設計者は、開発プロジェクトで使用する開発標準を作成する際、セキュリティに関して十分考慮し、全ての開発者が徹底順守するようにルールを定める必要があります。

また、自作の開発フレームワークの場合は、脆弱性対策が不十分になりやすいため、セキュリティ専門家の設計レビューを行うなど、より注意が必要と考えられます。

3. 納入後に考慮すべきこと

納入後のウェブサイトに影響する脆弱性が発見される可能性があります。たとえば、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るようなケースです。それらの脆弱性対策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。また、改修後には脆弱性の確認・検査を行うことも効果的です。

ウェブサイト構築事業者は、保守・運用のサポートを受けていない顧客から、脆弱性対策について助言を求められることがあります。したがって、少なくとも瑕疵担保期間は、ドキュメント等を管理し、そうした問合せに対応できるようにしておく必要があります。

3.1.脆弱性はどのように見つかるか

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、問題に自ら気づくことは容易ではありません。多くの場合、外部からの情報によって発覚すると考えられます。

■脆弱性の公表

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製品開発ベンダや JVN で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、保守業務を受託していない場合には、ウェブサイトの構成情報を確認しておくことを顧客に薦めるべきでしょう。

■第三者からの指摘

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。また、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）に基づき、独立行政法人情報処理推進機構（IPA）がウェブサイトの脆弱性について当該サイトの運営者に連絡し、脆弱性対策の実施を促すこともあります[9]。

[9] http://www.ipa.go.jp/security/vuln/report/index.html

そうした問い合わせを受けた場合には、速やかに脆弱性の有無を調査するよう、顧客に薦めてください。

■悪意の第三者による攻撃

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るよう、助言すべきです。

3.2.問題を招きやすいケース

納入後のプロセスで、脆弱性に係るトラブルを招く原因となりやすい事象として、たとえば以下のケースが挙げられます。

■システムのメンテナンスや統合・移行時の設定

納入当初は適切な設定であっても、システムのメンテナンスや統合・移行の際に、設定上のミスが生じることがあります。保守・運用を受託していないウェブサイト構築事業者には、対応の義務があるわけではありませんが、顧客のシステムにトラブルが生じる可能性をできる限り抑制するため、システムの構成情報や設定上の留意点に関する情報をドキュメント化して、顧客側に適切に引き継いでおくことが望まれます。

■環境の変化

開発当初の想定から逸脱した構成に移行したため、脆弱ではなかったものが脆弱になってしまうことがあります。たとえば、開発当初はクローズドな社内システムとして運用されていたものが、その後、会社の方針が変更され、外部ネットワークと接続されたことで、様々なセキュリティ上の問題が顕在化してしまうようなケースです。

こうした事態を避けるためには、変更を行う前に予想される問題を洗い出し、対策の適用に要するコストと変更による利便性の向上を比較して、その是非を判断することが望まれます。

■担当者や責任者の不在

システムを立ち上げた際の開発担当者や責任者がすでに退職していて、当時

の状況がわからなくなることがあります。また、企業買収や倒産等が原因で開発事業者そのものが存続しておらず、開発担当者に連絡を取ることできなくなるケースも考えられます。

したがって、システムの構成情報や設定上の留意点に関する情報をドキュメント化して、保守・運用の契約がない場合には、顧客側に適切に引き継いでおくことが望まれます。

■委託元と委託先の連携不足

委託元と開発・運用の委託先が遠方の場合、脆弱性発覚時の切迫感が共有できず、柔軟な対応や細かい打合せができない可能性があります。

また、海外にサイトを設置し、その運用を現地の事業者に委託している場合、脆弱性が発見されると、その対応について英語でやりとりしなければならないため、意思疎通がスムーズにいかなかったり、時間がかかったりする可能性があります。

■配布するソフトウェアの版管理

必ずしもウェブサイト構築事業者の担当する部分とは限りませんが、顧客がウェブサイトで配布する目的で用意したソフトウェアに影響する脆弱性が発見された場合、顧客には問題について関係者に連絡するとともに、当該ソフトウェアの脆弱性を解決した版を配布し直すことが求められます。

ウェブサイト構築事業者は、ダウンロード等の処理を委託されている場合、配布ソフトの脆弱性対策を早急に行うよう、顧客に促すことが望ましいと考えられます。

3.3.脆弱性対応

ウェブサイト運営者である顧客は、脆弱性の可能性があれば調査・確認作業を行い、必要に応じてパッチ（脆弱性修正プログラム）の適用等の対策作業を行うことが求められます。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、情報の集約や管理にも取り組む必要があります。

こうした状況は、多くの顧客において不測の事態であり、自力では適切な対応が困難なことも考えられます。したがって、ウェブサイト構築事業者は、契約に基づきそうした顧客の危機をサポートするとともに、可能な範囲で対応について助言することが望まれます。

ウェブサイト構築事業者が調査・確認作業を代行する場合には、経緯と既に得た情報について顧客（ウェブサイト運営者）から説明を受けてください。顧客（ウェブサイト運営者）から脆弱性関連情報等の提供を受けた際には、受領通知を提出するようにします。この時点でウェブサイト構築事業者が確認した内容について顧客（ウェブサイト運営者）に簡潔に報告してください。

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）[10]を参考としてください。

■外部から連絡を受けた場合

外部から脆弱性関連情報の通知を受けた際には、通知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。顧客（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。ウェブサイト構築事業者は、顧客（ウェブサイト運営者）とともに通知者との情報交換を行い、方針・計画の策定や対外説明を支援します。

通知は、IPA が顧客（ウェブサイト運営者）に通知してくる場合と、発見者が顧客（ウェブサイト運営者）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、顧客（ウェブサイト運営者）には、通知を受け取った旨の返信を速やかに行うよう説明してください。

・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）を利用し行われます。また、迅速な対応をするためには、IPA からの連絡窓口（セキュリティ対応部署）を設置しておくことも有効です。

・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

[10] http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

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。

■トラブルが発生している場合

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。ウェブサイト構築事業者は、顧客（ウェブサイト運営者）を支援し、問題解決やその技術的支援を行います。

4.補足

4.1.情報セキュリティ早期警戒パートナーシップ

独立行政法人情報処理推進機構（IPA）では、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）[11]の告示を踏まえ、2004 年 7 月からソフトウェア製品及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[12]。

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。

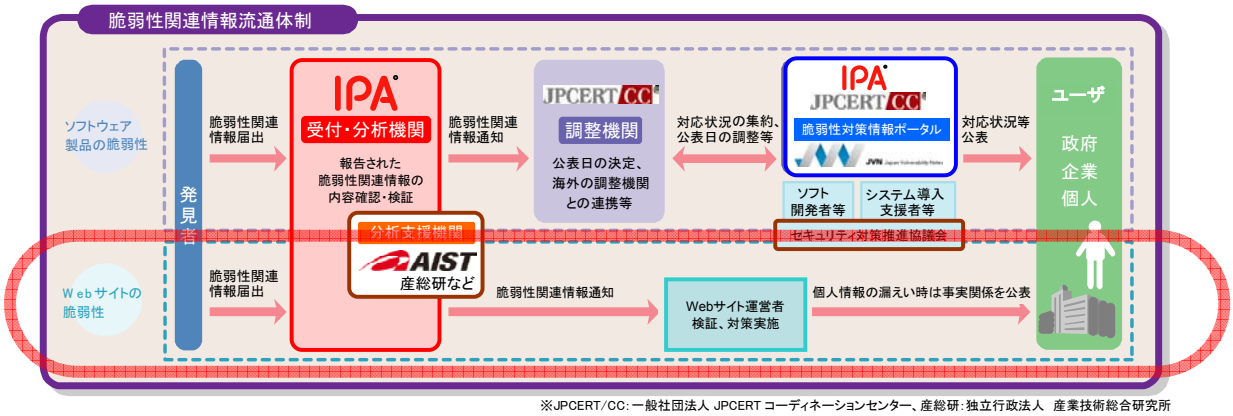


図 4-1　情報セキュリティ早期警戒パートナーシップのしくみ

[11] http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
[12] http://www.ipa.go.jp/security/vuln/report/index.html

4.2.参考 URL

- 「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」（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他）
  http://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 「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）
  http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf
- 「脆弱性対策」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/vuln/
- 「脆弱性関連情報の届出」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/vuln/report/
- 「脆弱性関連情報の届出状況」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/vuln/report/press.html
- 「安全なウェブサイトの作り方」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/vuln/websecurity.html
- 「知っていますか？脆弱性(ぜいじゃくせい)」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/vuln/vuln_contents/
- 「セキュア・プログラミング講座 Web アプリケーション編（新版）」（独立行政法人情報処理推進機構）
  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

・本資料の位置づけ

近年、日本国内においてソフトウエ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、経済産業省告示「ソフトウエ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（2009 年 7 月 8 日改訂版）の付録 7「ウェブサイト構築事業者のための脆弱性対応ガイド」を全文抜粋し、ガイドラインを補足するために、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などを追記したものです。

主にウェブサイト構築事業者による活用を想定しており、ウェブサイト構築事業者による脆弱性対応の望ましい手順について、一つの方針を示しています。

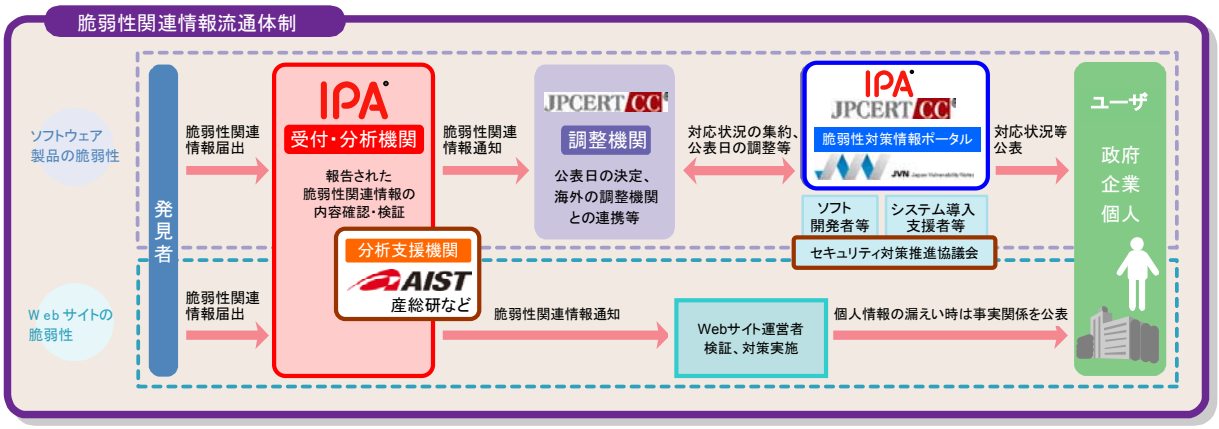
関係者の方々は、脆弱性対応に向けた体制の検討や、実際の対応に際し、本資料を参考にご対応くださいますようお願い申し上げます。

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。

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

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

・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：一般社団法人 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

ウェブサイト構築事業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 7 抜粋編 －

２００９年　６月　８日　第１版発行

２００９年　７月　８日　第２版発行

［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