安全なウェブサイト運営にむけて

～ 企業ウェブサイトのための脆弱性（ぜいじゃくせい）対応ガイド ～

2013年3月

独立行政法人**情報処理推進機構**

うちの会社にはサイバー攻撃は関係ない？

- 「サイバー攻撃で狙われるのは大手／有名企業のウェブサイト（ホームページ）だけ」と思っていませんか？
  悪者は無差別にウェブサイトを狙っています。
  ウェブサイトは企業の規模やネームバリューには関係なく攻撃されています。

- この資料は、中小企業の皆様がインターネットに公開するウェブサイト（ホームページ）をサイバー攻撃から守り、安全に運用するために大切な「脆弱性（ぜいじゃくせい）対策」を紹介する目的で作成しました。

- この資料は、次の方に読んでいただくことを想定しています
  - 中小企業のウェブサイト担当者の皆様
  - ウェブサイト運営に関心のある経営者の皆様

※ 脆弱性（ぜいじゃくせい）は、情報セキュリティ上の「弱点」「ほころび」です。
ウェブサイトに脆弱性があると攻撃を受けて、情報流出やシステムの改ざん、停止などの事態が起こることもあります。（参考1.もご参照ください）

目次

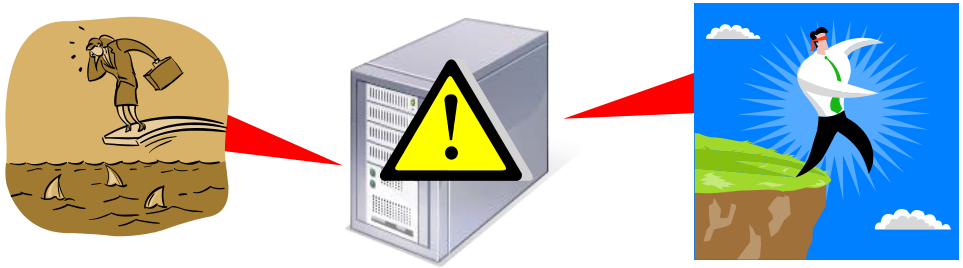
1. ウェブサイトを安全に運用するために

1.1. ウェブサイトと脆弱性

- 企業のウェブサイトは、いまや企業活動を行う上で不可欠なものとなっています。
  その企業のあらましや住所・電話番号等を伝えるだけでなく、顧客との取り引きや問い合わせの窓口としても活用されています。
- ただし、ウェブサイトは「動いているから問題が無い」ように見えても、時間が経つにつれてその安全性は低下していきます。
  ウェブサイトの脆弱性（ぜいじゃくせい）が発見され、脅威が高まるためです。
- ウェブサイトを安全に保ち、安全なサービスを維持するためには、脆弱性対策が重要になります。（参考1.もご参照ください）

※ 脆弱性（ぜいじゃくせい）とは：

- 脆弱性とは、情報セキュリティ上の「弱点」「ほころび」です。
- 脆弱性は、ウェブサイト構築後に時間が経つほど発見されやすくなります。
- 脆弱性対策を誤ると、ウェブサイトの利用者の信頼を失う結果につながります。



1.2. 脆弱性が元で起きる問題の例

■ ウェブサイトの脆弱性対策を怠ると、攻撃を受けやすくなり、企業活動に影響を及ぼす可能性があります。

事例1： ウェブサイトの改ざんと顧客等のウイルス感染	中小企業向けオンラインショップサイト構築ツールの脆弱性が狙われて自社のウェブサイトが改ざんされ、ウイルスに感染させるサイトに顧客を誘導してしまいました。ウェブサイトが改ざんされると、サイトを利用する顧客や取引先等に迷惑をかけることになります。
事例2： ウェブサイトからの個人情報の流出	大手メーカの子会社が運営していたウェブサイトが侵入され、氏名やパスワード情報など約1億件の個人情報が外部に流出しました。サーバの脆弱性を悪用したと見られ、対応に係る費用は1年で約140億円と試算されています。
事例3： ウェブサイトからの個人情報流出	アフィリエイト事業やショッピングサイトを運営するベンチャー企業のウェブサイトが不正に侵入されました。顧客の氏名やクレジットカード情報約10万件が流出した可能性があると見られ、カードの不正利用などの実害も発生しています。経済産業省から個人情報保護法に基づく報告の聴取を受けるなど、社会的な信用を損ねる事態を招きました。

2. 脆弱性対策を必ず行うべきウェブサイトとは

2. 脆弱性対策を必ず行うべきウェブサイトとは

次のケースに該当する場合、脆弱性対策を行うことが特に強く望まれます。
（参考2のチェックリストもご参照ください）

(1) 個人情報、顧客情報等の重要な情報を預かっている

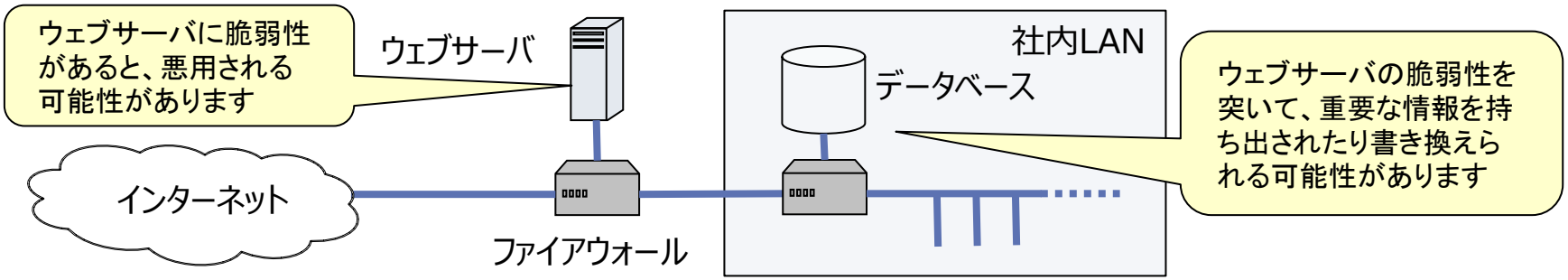
- 安全な管理を怠って個人情報を流出させた場合、罰則が適用されることもあります。
- 契約で厳格な管理が求められる情報（例：お客様情報、設計情報、試験データ等）を預かる場合、流出させると損害賠償を求められることがあります。

(2) ウェブサイトに脆弱性となりやすい機能がある

- たとえば、ユーザ登録画面や入力欄フォーム等に脆弱性があると、不正侵入や情報の盗み出しに悪用される可能性があります。

(3) ウェブサイトの構築後にメンテナンスをしていない

- ウェブサイト構築用のソフトウェアが古いバージョンの場合、構築したウェブサイトに脆弱性が残っていることがあります。



3. ウェブサイトの脆弱性対策のポイント

3. ウェブサイトの脆弱性対策のポイント ①まずこれから

以下に示す7つの項目は、脆弱性対策のうち、「少なくともこれだけは実施しておいた方がよい」という作業です。ただし、これだけでは十分ではない点にご注意ください。

(1) まず脆弱性を知る

- 運用中のウェブサイトの状況を把握することから始めましょう。
- 「ウェブ健康診断」を試してみましょう。
  具体的な方法については、次の資料を参考にしてください：
  - IPA「ウェブ健康診断仕様」
    http://www.ipa.go.jp/security/vuln/documents/website_security_shindan.pdf

(2) 脆弱性への対処をより詳しく検討する

- 脆弱性がありそうなら本格的な検査と修正を行いましょう。
- 影響を検討して、計画的に対処しましょう。
  具体的な対処方法については次の資料を参考にしてください：
  - IPA「安全なウェブサイトの作り方」
    http://www.ipa.go.jp/security/vuln/documents/website_security.pdf
- すぐに対処できない場合、ウェブサイトを一時的に停止する選択もあります。

3. ウェブサイトの脆弱性対策のポイント ②構築と運用

(3) ウェブサイトの構築時にセキュリティに配慮する

- 新たにウェブサイトを構築する際にはセキュリティ要件（仕様）を決めましょう。
  - ウェブサーバのセキュリティ対策の具体的方法は次の資料を参考にしてください：
  - IPA「安全なウェブサイトの作り方」
    http://www.ipa.go.jp/security/vuln/documents/website_security.pdf
- OS等を安全な設定にすることも重要です。
- できればサイトの稼働前に脆弱性検査を行いましょう。
- 構築ツールなどのソフトウェアは可能な限り最新版を使いパッチもあてましょう。
  使っているソフトウェアの名前やバージョンは控えておきましょう。

(4) セキュリティ対策を外部に任せる

- ホスティングなど、セキュリティ対策が含まれるサービスも活用しましょう。
- 委託先を選定する際、セキュリティの知見・技術力も考慮しましょう。
  - ITコーディネータ、システム事業者など、信頼できる専門家を見つけましょう。
  - セキュリティ要件について委託先と約束した事項は、文書にして残しておきましょう。

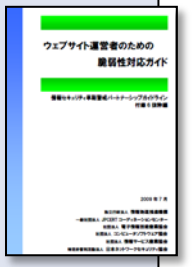
(5) セキュリティの担当者と作業を決めておく

- ウェブサイトのセキュリティを担当する人とその作業内容を決めましょう。
- トラブル発生時の社内連絡先と、公開停止等の判断を下す人を決めましょう。

3. ウェブサイトの脆弱性対策のポイント ③トラブルと相談先

(6) 脆弱性の報告やトラブルには適切に対処する

- ウェブサイトの脆弱性やセキュリティ上の問題について指摘を受けた場合には、落ち着いて対処しましょう。具体的な手順は参考3.や次の資料を参考にしてください：
  - IPA「ウェブサイト運営者のための脆弱性対応ガイド」
    http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf
  - IPAやJPCERT/CCからウェブサイト運営者に連絡を行う場合もあります。
- ウイルス対策だけでなく、脆弱性を修正して問題の原因を解決しましょう。
  - 脆弱性を悪用するウイルスは、駆除やファイル復旧だけをしても再感染することがあります。
- 個人情報等が流出した可能性がある場合には、本人や取引先に連絡しましょう。



(7) 難しければ専門家に支援を頼む

- 自社で対処できなければ、ウェブサイトやセキュリティの専門家に相談しましょう。
  - ITコーディネータ、システム事業者など、信頼できる専門家を見つけましょう。
  - IPAでも、情報セキュリティ対策に悩む企業の相談先として、専門家（セキュリティプレゼンター）を紹介しています。
    IPA「情報セキュリティ対策支援サイト iSupport」
    http://www.ipa.go.jp/security/isec-portal/index.html
  - IPAやJPCERT/CCにトラブル発生時の対応や再発防止について相談することもできます。
    IPA「情報セキュリティ安心相談窓口」 http://www.ipa.go.jp/security/anshin/
    JPCERT/CC「インシデントの報告」 https://www.jpcert.or.jp/form/

IPA 情報セキュリティ 安心相談窓口

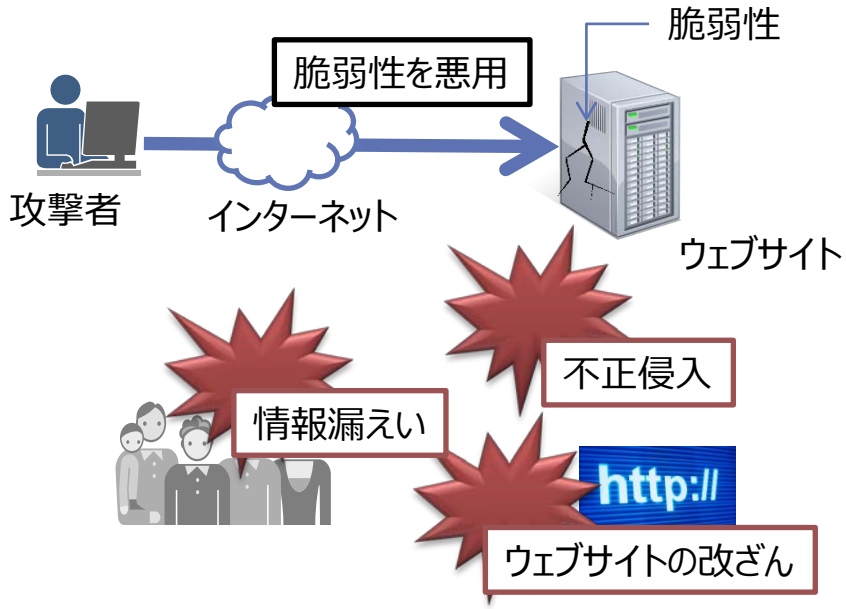
参考資料

参考1. 脆弱性（ぜいじゃくせい）とは？
参考2. ウェブサイトの脆弱性対策の要否に関するチェックリスト
参考3. 脆弱性の指摘への対処
参考4. 情報セキュリティ早期警戒パートナーシップ
参考5. 参考URL

参考1. 脆弱性（ぜいじゃくせい）とは？

- 脆弱性（ぜいじゃくせい）とは、
  情報セキュリティ上の「弱点」、「ほころび」のことです。

- 脆弱性を悪用されると『ウェブサイトの改ざん』や『不正侵入』をされてしまいます。
  - 『個人情報の漏えい』や『社の重要な情報の漏えい』につながります。
  - 『ウイルスをばらまく』、『詐欺サイトそのものにされたり、詐欺サイトに誘導するように作り変えられる』、『他のサイトへのサイバー攻撃に使われる』など、セキュリティ上の問題を引き起こして、顧客、取引先、他の企業等にも迷惑をかけてしまいます。



- 脆弱性対策を行い、トラブルを未然に防ぎましょう
  - 問題個所を作り直したり、ソフトウェア製品の修正プログラム（パッチ）を適用する必要があります。
  - 脆弱性の問題は、ウイルス対策ソフトウェアでは解決しません。
    - ウイルスを駆除しても脆弱性を修正しなければ、再感染や再侵入の可能性があります。

詳細は以下の文献をご参照ください。
IPA「知っていますか？脆弱性(ぜいじゃくせい)」
http://www.ipa.go.jp/security/vuln/vuln_contents/

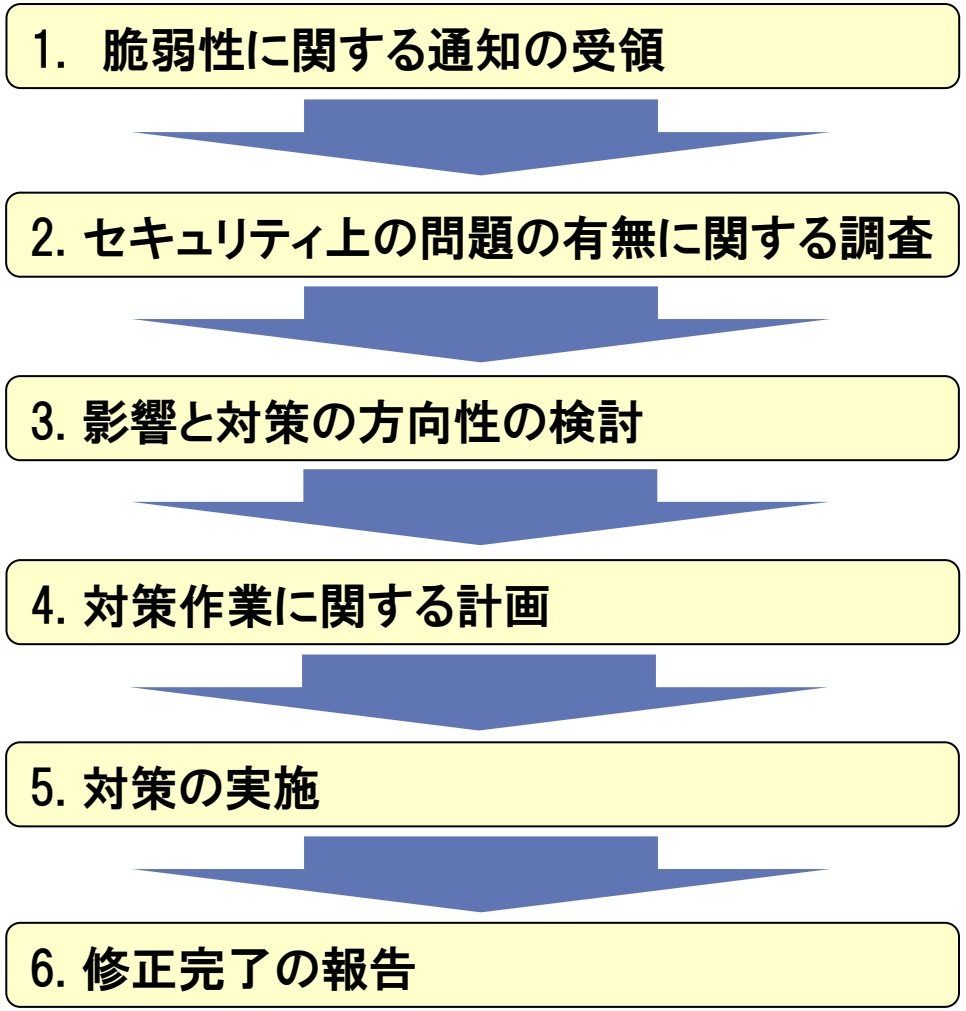
参考2. ウェブサイトの脆弱性対策の要否に関するチェックリスト

以下の項目に1つでも該当するならば、ウェブサイトの脆弱性対策を行いましょう。

- □ サイト利用者の個人情報をウェブ上で入力させている。
- □ 個人情報やクレジットカード情報などの重要情報を、ウェブサーバ上で管理している。
- □ 顧客等から預かった重要情報[1]をウェブサーバや社内のPCに置くことがある。
  1) 例：顧客のお客様情報、アンケートデータ、発注仕様、設計情報、試験データ等
- □ 自社の重要情報[2]をウェブサーバや社内のPCに置くことがある。
  2) 自社のビジネス上流出すると致命的な情報
- □ 自社のサイト上に以下のいずれか1つ以上の機能・画面がある。
  - ・ユーザ登録
  - ・登録済みユーザのログイン
  - ・ユーザによるフォームへの入力（問合せ、掲示板等を含む）
  - ・入力された情報の確認のための表示
  - ・ユーザへのメールの自動送信
  - ・サイト内の検索と結果表示
  - ・アクセスログやメール等の内容の画面表示
- □ サイト構築に使用したウェブサイト構築用のソフトウェアが最新のバージョンではない。
- □ ウェブサイトを構築した後でメンテナンスや修正を行っていない。

参考3. 脆弱性の指摘への対処

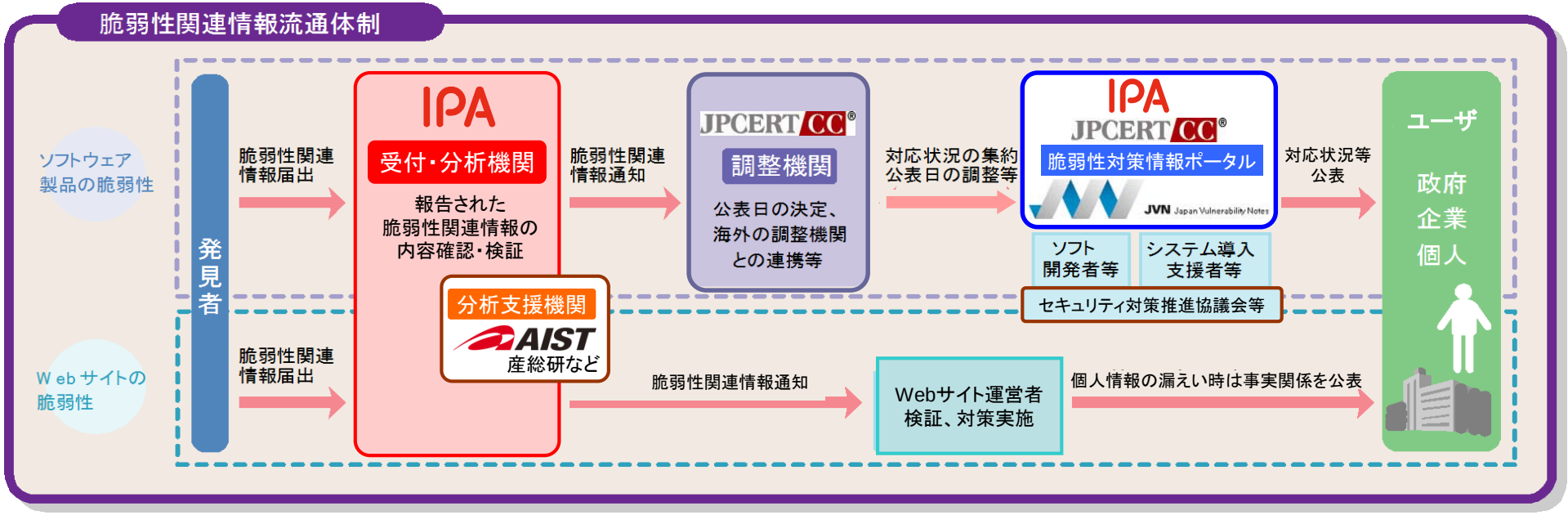
- 脆弱性について外部から指摘を受けた場合には、外部との間で良いコミュニケーションを維持することが対応を成功させる鍵となります。
- 対処の方針・計画を整理した上で可能な範囲で外部にも状況を説明し、理解を求めることが大切です。
- 対処の方針や計画は、ウェブサイトの運営者自身の判断に基づいて行う必要があります。
- 不正アクセスの踏み台にされている場合や、ウイルスを撒き散らしている場合など、トラブルが発生しているならば特に迅速な対応が必要です。



- 詳しい手順は次の資料を参考にしてください：
  - IPA「ウェブサイト運営者のための脆弱性対応ガイド」 http://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf

参考4. 情報セキュリティ早期警戒パートナーシップ

- 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）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 。
- 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。



※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

参考5. 参考URL

- 「情報セキュリティ安心相談窓口」
  （独立行政法人情報処理推進機構）
  - http://www.ipa.go.jp/security/anshin/
- 「情報セキュリティ対策支援サイト iSupport」
  （独立行政法人情報処理推進機構）
  - http://www.ipa.go.jp/security/isec-portal/index.html
- 「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
- パンフレット「情報システムを安全にお使いいただくために」
  （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/vuln_taisaku.pdf
- 「ウェブサイト運営者のための脆弱性対応ガイド」
  （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/vuln_website_guide.pdf
- 「ウェブサイト構築事業者のための脆弱性対応ガイド」
  （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/vuln_sier_guide.pdf
- 情報セキュリティ監査企業台帳（経済産業省）
  - http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html
- 「安全なウェブサイトの作り方」
  - http://www.ipa.go.jp/security/vuln/websecurity.html
- 「安全なSQLの呼び出し方」
  - http://www.ipa.go.jp/security/vuln/documents/website_security_sql.pdf
- 「ウェブ健康診断仕様」
  - http://www.ipa.go.jp/security/vuln/documents/website_security_shindan.pdf
- 「安全なウェブサイト運営入門」
  - http://www.ipa.go.jp/security/vuln/7incidents/
- 「知っていますか？脆弱性(ぜいじゃくせい)」
  - http://www.ipa.go.jp/security/vuln/vuln_contents/
- 脆弱性対策情報ポータルサイト「JVN」
  - http://jvn.jp/
- 脆弱性対策情報データベース「JVN iPedia」
  - http://jvndb.jvn.jp/
- 脆弱性対策情報収集ツール「My JVN脆弱性収集ツール」
  - http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
- ソフトウェア製品のバージョン確認「My JVNバージョンチェッカ」
  - http://jvndb.jvn.jp/apis/myjvn/vccheck.html
- ウェブサイト攻撃の検出ツール「iLogScanner V3.0」
  - http://www.ipa.go.jp/security/vuln/iLogScanner/index.html