

IPA

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対応ガイド ～
ぜいじゃくせい

2021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」と思っていないですか？

悪者は無差別にウェブサイトを狙っています。

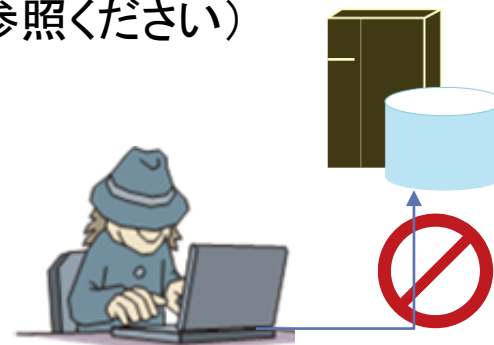
ウェブサイトは企業の規模やネームバリューには関係なく攻撃されています。

- 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)

ぜいじゃくせい
「脆弱性対策」を紹介する目的で作成しました。

- ※ ぜいじゃくせい 脆弱性は、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)



- この資料は、次の方を対象に以下のように活用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

「1.2脆弱性が元で起きる問題の例」で、実際の被害事例を紹介していますので、被害について具体的なイメージを持ってください。

そして、「3.ウェブサイトの脆弱性対策のポイント」や、紹介しているURLのコンテンツを参考にしながら、ウェブサイトの対策ができているか確認し、不足しているところがあれば対応するようにしてください。すぐに使えるチェックリストを備えたコンテンツも紹介していますので、一緒に使ってください。

■ ウェブサイト運営に関心のある経営者の皆様

「1.2脆弱性が元で起きる問題の例」で、実際の被害事例を紹介していますので、「対岸の火事」と思うことなく、自社が被害を受ける場合を想像してみてください。

その後、「3.ウェブサイトの脆弱性対策のポイント」で7つの大きな対策項目を紹介していますので、概要を把握してください。

そして、このガイドを担当者に渡して、「まずは、このガイドを見ながら、3.の(1)で紹介しているチェックリストを基にサイトのセキュリティ対策状況を確認して」と伝えてください。

0. こんな時にご覧ください	4
1. ウェブサイトを安全に運用するために	5
2. 脆弱性対策を必ず行うべきウェブサイトとは	9
3. ウェブサイトの脆弱性対策のポイント	11
参考資料	20

0. こんな時にご覧ください

■ 構築や運用など必要な場面に応じて以下をご参照ください

実際の被害事例を知りたい方

1. をご覧ください

対策が必要なウェブサイトを知りたい方

2. をご覧ください

対策状況を把握したい方

3.(1) をご覧ください

トラブルに対処したい方

3.(6) をご覧ください

構築を任された方

3.(3) をご覧ください

脆弱性に対処したい方

3.(2) をご覧ください

運用を任された方

3.(5)、(6) をご覧ください

専門家の支援を求めたい方

3.(4)、(7) をご覧ください

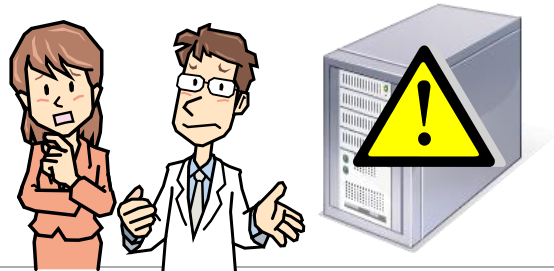
1. ウェブサイトを安全に運用するために

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。

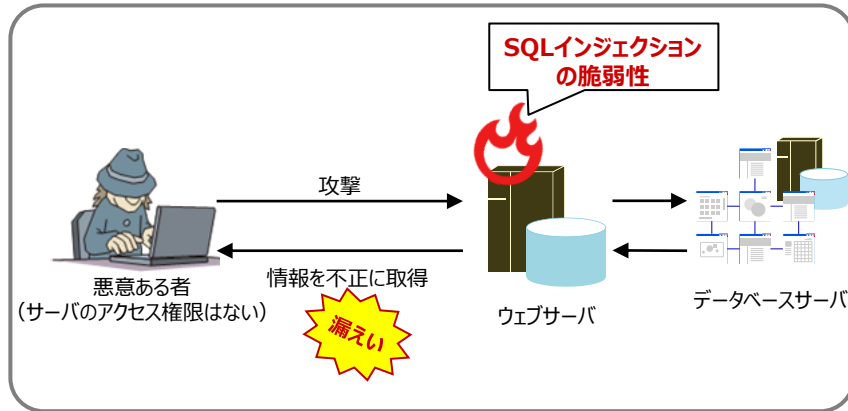


1.2. 脆弱性が元で起きる問題の例

- 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。

脆弱性を悪用したSQLインジェクションによる個人情報流出

脆弱性を悪用したSQLインジェクションにより、サーバー内にアクセスできる状態となり、個人情報が出た。

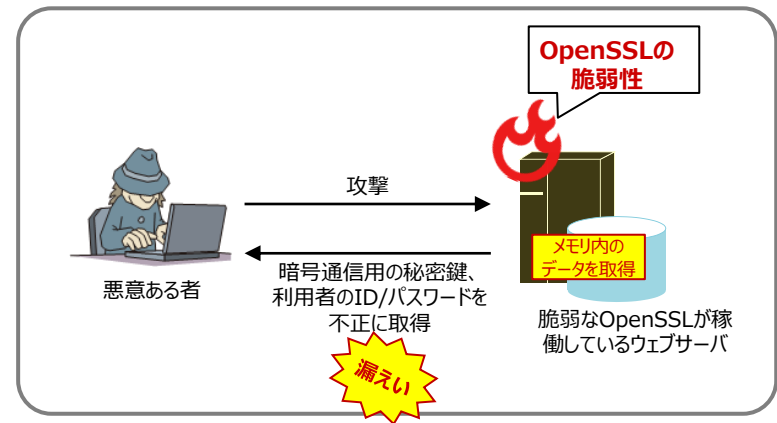


■ 求められる対策例

- 「安全なウェブサイトの作り方」に取り上げられている脆弱性への対策の実施

既知の脆弱性悪用によるクレジットカード情報流出

2014年に公開されていたOpenSSLに関する脆弱性「Heartbleed」の対応が未実施だったことから、クレジットカード情報が漏えいした。



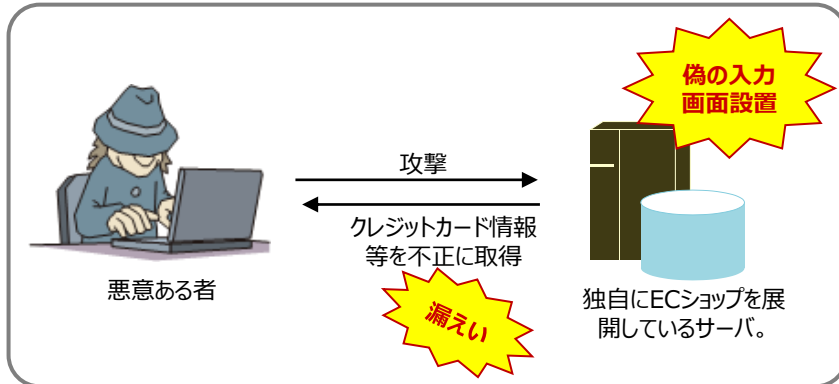
■ 求められる対策例

- ウェブサイトを構成しているソフトウェアの構成管理
- 構成管理情報を基にしたソフトウェアの脆弱性情報の収集及び、対策の定期的な実施

1.2. 脆弱性が元で起きる問題の例

偽の情報入力画面設置による クレジットカード情報流出

オンラインショップの決済時の情報入力画面にて、不正に設置された偽のカード情報入力画面が現れ、偽画面に入力を行った場合に情報が盗まれるという不正プログラムが設置されていた。再発防止策を検討するも現環境では一定のセキュリティを担保できないと判断し、ECサイト機能をオンラインモールに移行した。

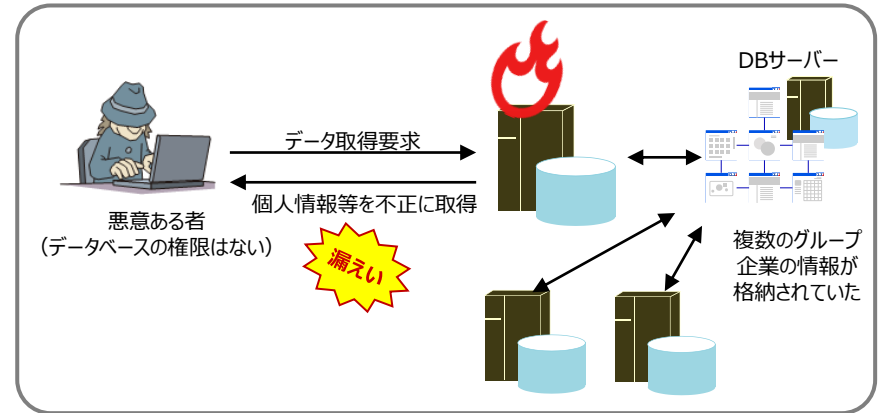


■ 求められる対策例

- 自組織内で一定のセキュリティを担保できない場合は、セキュリティ対策が含まれるサービスの活用も検討。

グループ会社ウェブサイトの脆弱性を悪用による 複数グループ企業サイトの個人情報流出

グループ内企業のホームページから、グループで個人情報を保管していたサーバが不正アクセスを受け、グループ内複数企業の利用者の個人情報が外部に流出した。



■ 求められる対策例

- ネットワーク機器等を利用して、ネットワーク境界及び、データへのアクセス制限見直し、適切な設定実施。
および、不正な通信の監視、遮断をする環境の構築。

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

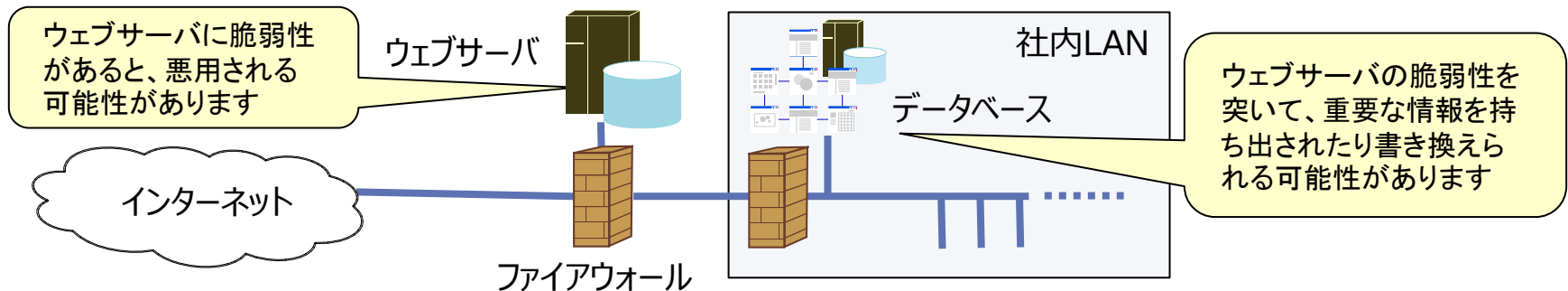
- 安全な管理を怠って個人情報を流出させた場合、罰則が適用されることもあります。
- 契約で厳格な管理が求められる情報(例:お客様情報、設計情報、試験データ等)を預かる場合、流出させると損害賠償を求められることがあります。

(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。



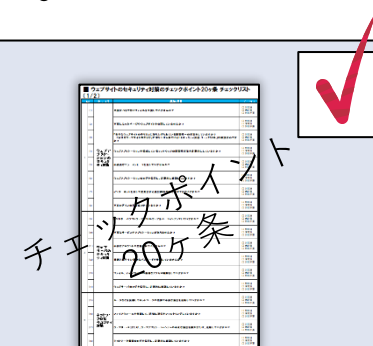
3. ウェブサイトの脆弱性対策のポイント

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) 実施しているセキュリティ対策を把握する

- 運用中のウェブサイトのセキュリティ対策の状況を把握することから始めましょう。
 - ウェブサイトのセキュリティ対策のチェックポイント20ヶ条
<https://www.ipa.go.jp/files/000070296.xlsx>



(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。
- 「ウェブ健康診断」を試してみましょ。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：
 - ウェブ健康診断仕様
<https://www.ipa.go.jp/files/000017319.pdf>
- 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：
 - 安全なウェブサイトの作り方
<https://www.ipa.go.jp/security/vuln/websecurity.html>
- 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



a) ウェブサイトを構築する前に配慮すべき事項

- 自組織のリソースやスキルに応じた運用形態を選定しましょう。
 - ウェブサイト開設等における運営形態の選定方法に関する手引き
<https://www.ipa.go.jp/security/technicalwatch/20180530.html>
- クラウドサービスを利用する前に安全に利用するための確認事項を把握しましょう。
 - 中小企業の情報セキュリティ対策ガイドライン
付録6: クラウドサービス安全利用の手引き
<https://www.ipa.go.jp/files/000072150.pdf>
- 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:
 - 安全なウェブサイトの作り方
<https://www.ipa.go.jp/security/vuln/websecurity.html>



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



b) ウェブサイトを構築中に配慮すべき事項

- OS等を安全な設定にすることも重要です。
- 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。
 - 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:
 - 安全なウェブサイトの運用管理に向けての20ヶ条
～セキュリティ対策のチェックポイント～
<https://www.ipa.go.jp/security/vuln/websitecheck.html>
 - CMSを用いたウェブサイトにおける情報セキュリティ対策のポイント
<https://www.ipa.go.jp/security/technicalwatch/20160928-1.html>

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



c) ウェブサイトを構築後(サービスインまで)に配慮すべき事項

■ 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。

- 脆弱性を悪用する攻撃への効果的な対策についてのレポート
<https://www.ipa.go.jp/about/technicalwatch/20130926.html>
- 脆弱性対策の効果的な進め方(実践編)
～ 脆弱性情報の早期把握、収集、活用のおススメ ～
<https://www.ipa.go.jp/security/technicalwatch/20150331.html>
- 脆弱性対策の効果的な進め方(ツール活用編)
～ 脆弱性検知ツール Vuls を利用した脆弱性対策 ～
<https://www.ipa.go.jp/security/technicalwatch/20190221.html>

■ できればサイトの稼働前に脆弱性検査を行いましょう。

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:

- 安全なウェブサイトの運用管理に向けての20ヶ条
～セキュリティ対策のチェックポイント～
<https://www.ipa.go.jp/security/vuln/websitecheck.html>

3. ウェブサイトの脆弱性対策のポイント ②構築と運用

(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。
 - 運用形態に応じて、委託先やサービス提供者のセキュリティ対策の作業範囲を確認しましょう。
- ウェブサイト開設等における運営形態の選定方法に関する手引き
<https://www.ipa.go.jp/security/technicalwatch/20180530.html>

(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。
- セキュリティの担当者と委託先との作業範囲や責任範囲を明確にしましょう。
 - 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～
<https://www.ipa.go.jp/files/000058491.pdf>

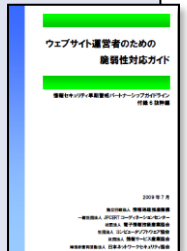
3. ウェブサイトの脆弱性対策のポイント ③トラブルと相談先



(6) 脆弱性の報告やトラブルには適切に対処する



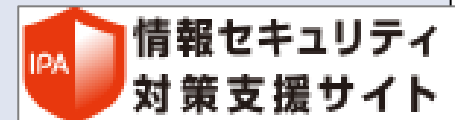
- ウェブサイトの脆弱性やセキュリティ上の問題について指摘を受けた場合には、落ち着いて対処しましょう。具体的な手順は参考3.や次の資料を参考にしてください：
 - ウェブサイト運営者のための脆弱性対応ガイド
<https://www.ipa.go.jp/files/000058492.pdf>
 - IPAやJPCERT/CCからウェブサイト運営者に連絡を行う場合もあります。
- ウィルス対策だけでなく、脆弱性を修正して問題の原因を解決しましょう。
 - 脆弱性を悪用するウィルスは、駆除やファイル復旧だけをしても再感染することがあります。
- 個人情報等が流出した可能性がある場合には、本人や取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。
情報セキュリティ対策支援サイト
<https://security-shien.ipa.go.jp/>
- 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」 <https://www.ipa.go.jp/security/anshin/>
JPCERT/CC「インシデントの報告」 <https://www.jpcert.or.jp/form/>



3. ウェブサイトの脆弱性対策のポイント

脆弱性対策で必要となる参照情報と簡易的なチェックリストの有無を示した情報です。



大項目	項目	リンク情報	チェックリスト有無	
①まずはこれから	(1)実施しているセキュリティ対策を把握する	安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～ https://www.ipa.go.jp/security/vuln/websitecheck.html	○	
	(2) 脆弱性への対処をより詳しく検討する	ウェブ健康診断仕様 https://www.ipa.go.jp/files/000017319.pdf	—	
		安全なウェブサイトの作り方 https://www.ipa.go.jp/security/vuln/websecurity.html	○	
②構築と運用	a)構築前	ウェブサイト開設等における運営形態の選定方法に関する手引き https://www.ipa.go.jp/security/technicalwatch/20180530.html	○	
		中小企業の情報セキュリティ対策ガイドライン 付録6：クラウドサービス安全利用の手引き https://www.ipa.go.jp/files/000072150.pdf	○	
		安全なウェブサイトの作り方 https://www.ipa.go.jp/security/vuln/websecurity.html	○	
	b)構築中	安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～ https://www.ipa.go.jp/security/vuln/websitecheck.html	○	
		CMSを用いたウェブサイトにおける情報セキュリティ対策のポイント https://www.ipa.go.jp/security/technicalwatch/20160928-1.html	○	
	c)構築後(サービス前)	(3) ウェブサイトの構築時にセキュリティに配慮する	安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～ https://www.ipa.go.jp/security/vuln/websitecheck.html	○
			脆弱性を悪用する攻撃への効果的な対策についてのレポート https://www.ipa.go.jp/about/technicalwatch/20130926.html	—
			脆弱性対策の効果的な進め方（実践編） ～ 脆弱性情報の早期把握、収集、活用のスゝメ ～ https://www.ipa.go.jp/security/technicalwatch/20150331.html	—
			脆弱性対策の効果的な進め方（ツール活用編） ～ 脆弱性検知ツール Vuls を利用した脆弱性対策 ～ https://www.ipa.go.jp/security/technicalwatch/20190221.html	—

3. ウェブサイトの脆弱性対策のポイント



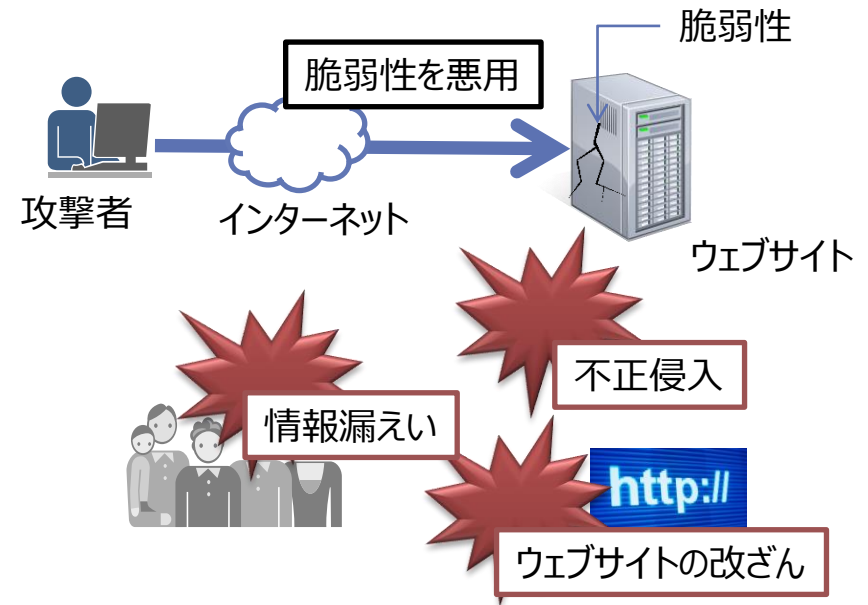
大項目		項目	リンク情報	チェック リスト有無
②構築 と運用	d)運用時	(4) セキュリティ対策を外部に任せる	ウェブサイト開設等における運営形態の選定方法に関する手引き https://www.ipa.go.jp/security/technicalwatch/20180530.html	○
		(5) セキュリティの担当者と作業を決めておく	ウェブサイト構築事業者のための脆弱性対応ガイド ～ウェブサイト構築にかかわるすべての人に～ https://www.ipa.go.jp/files/000058491.pdf	○
③トラブルと相談先		(6) 脆弱性の報告やトラブルには適切に対処する	ウェブサイト運営者のための脆弱性対応ガイド https://www.ipa.go.jp/files/000058492.pdf	—
		(7) 難しければ専門家に支援を頼む	IPA「情報セキュリティ対策支援サイト」 https://security-shien.ipa.go.jp/	—
			IPA「情報セキュリティ安心相談窓口」 https://www.ipa.go.jp/security/anshin/	—
		JPCERT/CC「インシデントの報告」 https://www.jpcert.or.jp/form	—	

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
 - 問題箇所を作り直したり、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。
 知っていますか？脆弱性(ぜいじゃくせい)
https://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きましょう。

- サイト利用者の個人情報ウェブ上で入力させている。
- 個人情報※などの重要情報を、ウェブサーバ上で管理している。
※クレジットカード情報は非保持の対応が求められています。
- 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：

- ウェブサイト運営者のための脆弱性対応ガイド <https://www.ipa.go.jp/files/000058492.pdf>

1. 脆弱性に関する通知の受領

2. セキュリティ上の問題の有無に関する調査

3. 影響と対策の方向性の検討

4. 対策作業に関する計画

5. 対策の実施

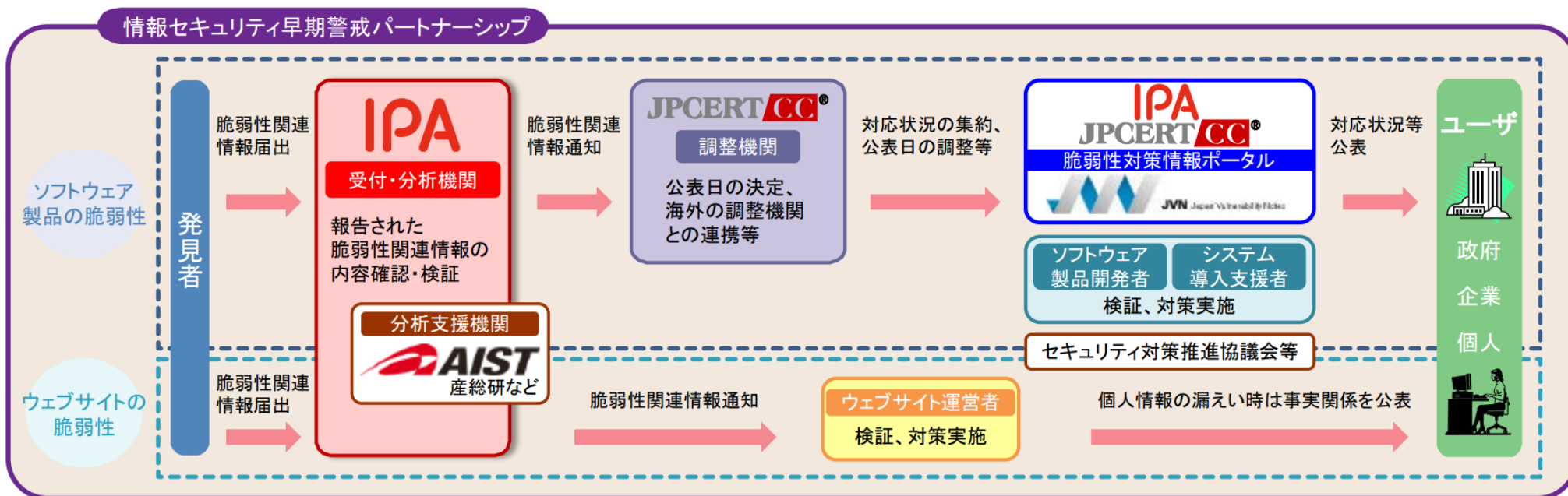
6. 修正完了の報告

参考4. 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、経済産業省告示を踏まえ、2004年7月からソフトウェア製品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。

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

- 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

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)
 - <https://www.ipa.go.jp/security/anshin/>
- 情報セキュリティ対策支援サイト
(独立行政法人情報処理推進機構)
 - <https://security-shien.ipa.go.jp/>
- 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)
 - https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 情報システムの安全を維持していただくために
～脆弱性(ぜいじゃくせい)対策のお願い～
(独立行政法人 情報処理推進機構)
 - <https://www.ipa.go.jp/files/000059697.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)
 - <https://www.ipa.go.jp/files/000058492.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)
 - <https://www.ipa.go.jp/files/000058491.pdf>
- ウェブサイト開設等における運営形態の選定方法に関する手引き
 - <https://www.ipa.go.jp/security/technicalwatch/20180530.html>
- 中小企業の情報セキュリティ対策ガイドライン
付録6: クラウドサービス安全利用の手引き
 - <https://www.ipa.go.jp/files/000072150.pdf>
- 安全なウェブサイトの運用管理に向けての20ヶ条
～セキュリティ対策のチェックポイント～
 - <https://www.ipa.go.jp/security/vuln/websitecheck.html>
- ウェブサイト運営のファーストステップ
～ウェブsite運営者がまず知っておくべき脅威と責任～
 - <https://www.ipa.go.jp/files/000071949.pdf>
- 安全なウェブサイトの作り方
 - <https://www.ipa.go.jp/security/vuln/websecurity.html>
- 安全なSQLの呼び出し方
 - <https://www.ipa.go.jp/files/000017320.pdf>
- ウェブ健康診断仕様
 - <https://www.ipa.go.jp/files/000017319.pdf>
- 知っていますか? 脆弱性(ぜいじゃくせい)
 - https://www.ipa.go.jp/security/vuln/vuln_contents/
- 脆弱性対策情報ポータルサイト「JVN」
 - <https://jvn.jp/>
- 脆弱性対策情報データベース「JVN iPedia」
 - <https://jvndb.jvn.jp/>
- 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」
 - <https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html>
- ウェブサイト攻撃の検出ツール「iLogScanner V3.0」
 - <https://www.ipa.go.jp/security/vuln/iLogScanner/index.html>
- 脆弱性を悪用する攻撃への効果的な対策についてのレポート
 - <https://www.ipa.go.jp/about/technicalwatch/20130926.html>
- 脆弱性対策の効果的な進め方(実践編)
～脆弱性情報の早期把握、収集、活用のスゝメ～
 - <https://www.ipa.go.jp/security/technicalwatch/20150331.html>
- 脆弱性対策の効果的な進め方(ツール活用編)
～脆弱性検出ツール Vuls を利用した脆弱性対策～
 - <https://www.ipa.go.jp/security/technicalwatch/20190221.html>
- CMSを用いたウェブサイトにおける情報セキュリティ対策のポイント
 - <https://www.ipa.go.jp/security/technicalwatch/20160928-1.html>