

WARNING

～ウェブサイトを運営している事業者の皆様への注意喚起～

平成30年6月28日
(最終改訂：令和元年7月12日)
個人情報保護委員会事務局

1. はじめに(ウェブサイトを取り巻くリスク)

当委員会において報告を受けた不正アクセスに起因する漏えい等事案の中でも、ECサイト※や会員用ウェブサイトにおける情報漏えい事案が多く報告されています。ECサイトはクレジットカード情報を含む個人データを盗むことを、会員用ウェブサイトはポイントの不正利用や個人データを盗むことを目的として、攻撃の対象になりやすい傾向にあります。

こうした不正アクセスは、企業規模の大小や業種に関係なく、様々なECサイトや会員用ウェブサイトなどに対して仕掛けられています。そのため、ウェブサイトを運営する事業者は、こうした脅威を認識し、不正アクセスによる情報漏えいを防ぐために適切なセキュリティ対策を講じる必要があります。

※ ECサイトとは、インターネット上で商品を販売するウェブサイト、いわゆるインターネットショップのこと。

2. 本資料の目的

本資料は、ウェブサイト運営事業者がセキュリティ対策を行うに当たり、実際に発生した不正アクセスによる情報漏えい等事案を踏まえて、注意いただきたい事項を示すことを目的としています。なお、本資料に示す内容は、あくまでセキュリティ対策の一例であり、必ずしもこれらの対策を実施すれば十分というものではありません。個々のウェブサイトに応じて、システム担当者やシステム開発・保守運用の委託先と相談の上、必要な対策の実施をお願いします。

3. ウェブサイト運営事業者がセキュリティ対策を行う上で主に注意すべき事項

(1) まずは現状を確認

- ウェブサイトの構築手法は様々であるため、それぞれの実状に応じたセキュリティ対策が必要になります。
まずは、**自組織でどのようなシステム等を使用しており、誰が管理しているのか、どのようなセキュリティ対策を実施しているのか確認**し、その上で必要な対策を検討・実施しましょう。

(2) ウェブサイト構築時に 注意すべき事項

- ウェブサイトの構築（制作）・導入にあたっては、デザインやコストを重視しがちですが、セキュリティ対策についても十分に行いましょう。
- サイトの構築（プログラミング等）の段階で脆弱性に関する対策が不十分であったケースは決して少なくないため、**公開前に脆弱性診断等を行い**、見つかった脆弱性については確実に対策を行いましょう。

(3) ウェブサイト運用時に 注意すべき事項

- ウェブサイトの運用にあたっては、**OSやソフトウェアの脆弱性対策情報を収集し、必要に応じ速やかにセキュリティパッチを適用**しましょう。
- 攻撃を感知・防御する体制や仕組み（例えば**IDS/IPS※1**、**WAF※2**の導入等）を整えることが望ましいと考えられます。

※1 IDS/IPS : IDS (Intrusion Detection System) 不正侵入検知システム、IPS (Intrusion Prevention System) 不正侵入防御システム

※2 WAF : (Web Application Firewall) ウェブアプリケーションの脆弱性を狙った攻撃を防御するシステム

(4) 委託先業者の監督に おける注意すべき事項

- 委託先業者に任せきりにしていませんか？ **委託元には委託先の監督義務があります。**
- ウェブサイトの構築や、その保守・運用を委託している場合は、委託先との契約時に**セキュリティ対策の内容を明確にした上で契約を**しましょう。
- 委託先にセキュリティ監査の実施、及び報告を求め、**契約書に記載されたセキュリティ対策が委託先で適切に実施されていることを定期的に確認**するようにしましょう。

<<脆弱性とは>>

脆弱性とは、広義には外部からの不正アクセスに対してシステムの安全性が損なわれる弱点のことを指します。ウェブサイトを構成するネットワーク機器やサーバ機器における不適切な設定が脆弱性となり不正アクセスを受ける場合があります。

また、ウェブサイトの利用者が直接操作する、ウェブサイト上で動作しているソフトウェア（ウェブアプリケーション含む）のセキュリティ上における弱点も脆弱性と言います。

ウェブサイトを建物に例えると、脆弱性とは建物の外から入る抜け穴（外壁のほころびなど）で、攻撃者はこの抜け穴から侵入（攻撃）してきます。セキュリティホールと言われることもあります。

脆弱性対策とは、この抜け穴を塞ぐための対策（セキュアなシステム構築、セキュリティパッチやアップデートの適用等）を実施することです。

4. 発生事例から学ぶセキュリティ対策

当委員会で受付けた不正アクセスを起因とする漏えい等事案の中でも、頻繁に発生している事例、自組織でも同様の事例が発生することがないか確認いただきたい事例をご紹介します。自組織のウェブサイトにも同様のセキュリティリスクがないか確認をお願いします。

対策が実施済みかチェックするために、システム担当者やシステム開発・保守運用の委託先などに対策の実施内容及び実施結果（証跡）などを確認し、不十分であれば必要な対策を検討・実施しましょう。

《事例》

- 事例 1 既知の脆弱性対策を怠っていたことによる情報漏えい事案
- 事例 2 SQLインジェクション攻撃による情報漏えい事案
- 事例 3 リスト型攻撃による情報漏えい事案
- 事例 4 ウェブサイトの機能拡張やバージョンアップに起因して情報漏えいした事案
- 事例 5 脆弱性診断ツールで脆弱性を検知できず情報漏えいした事案
- 事例 6 委託先業者のウェブサイトが攻撃され情報漏えいした事案
- 事例 7 通販サイトを改ざんされてクレジットカード情報が窃取された事案
- 事例 8 中小企業において委託契約にセキュリティ対策が含まれていなかった事案

参考情報

事例1 既知の脆弱性対策を怠っていたことによる情報漏えい事案

事例

- 使用しているソフトウェアやアプリケーションフレームワークの脆弱性が公表されたものの、セキュリティパッチの適用を速やかに行っていなかった。これにより、その脆弱性を狙った不正アクセスを受け、サーバ内に保持していたクレジットカード情報を含む個人データが窃取された！

POINT

- ソフトウェアなどに脆弱性があった場合、そのソフトウェアなどの提供元から脆弱性情報と共に、その脆弱性を修正するためのセキュリティパッチやアップデート情報が公開されます。不正アクセスを企てている攻撃者は、公開された脆弱性情報を収集し、対策（セキュリティパッチやアップデートの適用）を行っていないウェブサイトに攻撃を仕掛けます。

対策例

- 自組織のシステムがどのようなソフトウェアなどで構成されているか把握し、当該ソフトウェアなどの脆弱性対策情報の収集及びセキュリティパッチの適用やアップデートの適用状況を管理する仕組み（資産管理ソフト、脆弱性管理ソフトの導入等）を整備しましょう。
- 運用保守などを委託している場合は、委託先がバージョン管理や脆弱性管理を適切に行っているか確認しましょう。



事例2 SQLインジェクション攻撃による情報漏えい事案

※ SQLインジェクションとは、ウェブサイトが利用者から送信される情報に対して適切な取扱いをしていないことに起因して、データベースを不正に操作される脆弱性です。この脆弱性を利用する攻撃のことをSQLインジェクション攻撃と呼びます。この攻撃により、ウェブサイト運営者が意図していないデータベースの操作が可能となり、データベースに格納された個人データの漏えい、改ざん等の被害を受ける可能性があります。

事例

- ウェブサイトの予約システムに対しSQLインジェクション攻撃があり、予約者の氏名や電話番号、メールアドレスなどの個人データが窃取された！
- ECサイトの管理者IDとパスワードがSQLインジェクション攻撃により抜き取られ、悪意のある第三者により当該管理者IDとパスワードを使用して管理サーバにログインされ、ウェブサイトが改ざんされた上に、氏名、住所、クレジットカード情報などの個人データが窃取された！

POINT

- SQLインジェクション攻撃は、近年でも多くの被害事例が報告されている攻撃手法です。ウェブサイトの構築・修正等の際に脆弱性を作り込まないことが重要です。

対策例

- ウェブサイトの構築・修正の段階でセキュリティチェックシートなどを使用して脆弱性が存在していないか確認を行いましょう。
- また、ウェブサイトのリリース前に外部業者による脆弱性診断サービスや、脆弱性診断ツールを利用するなど多段階の確認を行い、ウェブサイトに脆弱性を残さないようにしましょう。
- 定期的に、ウェブサイト全体を対象として脆弱性診断を行うことも有効です。



事例3 リスト型攻撃による情報漏えい事案

※ リスト型攻撃とは、攻撃対象とは別のウェブサイトなどから何らかの方法で不正に入手したIDとパスワードの組み合わせの一覧（リスト）を使用して、ウェブサイトなどにログインを試みる攻撃手法です。利用者が同じIDとパスワードの組み合わせを複数のウェブサイトで使用する傾向にあることを利用した攻撃です。

事例

- リスト型攻撃により会員用ウェブサイトへ不正にログインされ、登録されていた会員情報を閲覧されるとともに、ポイントプログラムのポイントを使用し商品を購入されてしまった！
- ECサイトにリスト型攻撃があり、登録してある会員情報が閲覧されるとともに、登録クレジットカードによる商品の不正購入が行われた！

POINT

- 自組織のシステムからIDやパスワードのリストを窃取されないように対策を行うことはもちろんですが、リスト型攻撃によって不正ログインされ、個人データが漏えいしないよう対策を行いましょう。

対策例

- 事業者自身の対策としては、ID・パスワード以外の認証要素（多要素認証）を導入することや、不正ログインの試行を検知・防御するセキュリティツールを導入することが有効と考えられます。
- 事業者側から利用者に対しては、他ウェブサイトのパスワードとの重複を避けることをアナウンスすることが有効と考えられます。



事例4 ウェブサイトの機能拡張やバージョンアップに起因して情報漏えいした事案

事例

- ECサイトのプログラムを修正（機能拡張など）した際に脆弱性が生成され、この脆弱性を狙った不正アクセスにより個人データが窃取された！
- ウェブサイトを構築しているパッケージソフトのバージョンアップを行った際、バージョンアップに伴ってシステムの設定が変更になったことにより、サイト構築時に内在していた脆弱性が表面化し攻撃を受けた！

POINT

- ウェブサイトのプログラム修正、バージョンアップなどの変更・修正を行った場合は、機能面の確認だけでなく、脆弱性の有無についても確認することが重要です。

対策例

- ウェブサイトのプログラム修正、システムのバージョンアップなど変更・修正を加えた場合は、リリース前にセキュリティチェックシートなどを使用し、ウェブサイトに脆弱性がないか網羅的に確認を行いましょう。
- 自組織で行うことが難しい場合は、外部業者の脆弱性診断サービスを利用することや、脆弱性診断ツールを使用するなどの方法があります。ウェブサイトの運用保守などを委託している場合は、委託先から脆弱性診断の結果（セキュリティチェックシート等）の提出を受けるなど、脆弱性対策が適切に実施されているか確認しましょう。



事例5 脆弱性診断ツールで脆弱性を検知できず情報漏えいした事案

事例

- ウェブサイト用の脆弱性診断ツールを利用して診断していたものの、脆弱性診断ツールを適切に使用できていなかったため、脆弱性を検知できず、不正アクセスにより個人データが窃取された！

POINT

- 脆弱性診断ツールを利用して診断しているから大丈夫！と思っていないですか？診断ツールを利用していても、そのツールの使い方を十分理解していないと、診断したつもりの箇所が診断できておらず、脆弱性を見逃してしまう場合があります。

対策例

- まずは、使用している脆弱性診断ツールの機能を確認しましょう。そして、診断ツールの診断対象範囲について確認を行うなど、適切に診断ができているか確認を行きましょう。
- 定期的に、ウェブサイト全体を対象として脆弱性診断を行うことも有効です。



事例6 委託先業者のウェブサイトが攻撃され情報漏えいした事案

事例

- ウェブサイトの顧客対応システムに関して、外国に所在するシステム業者に開発や運用等を委託していた。
- 当該システムの脆弱性を狙った不正アクセスを受け、氏名、住所、クレジットカード情報などの個人データが窃取された！
- また、当該システムを利用している国内の委託元が多数あり、同様な被害が発生した！

POINT

- 委託先業者にセキュリティ対策を任せっきりにしていませんか？
- 委託先が外国に所在していても、委託元には、委託先を監督する義務があります。

対策例

- 委託先にセキュリティ監査の実施、及び報告を求め、契約書等に記載されたセキュリティ対策が委託先で適切に実施されていることを定期的を確認するようにしましょう。
- また、漏えい等の事案の発生時に備え、あらかじめ報告連絡体制等を確認しましょう。
- 委託先が第三者機関によるセキュリティ診断等を定期的を受けているか、確認することも有効です。



事例7 通販サイトを改ざんされてクレジットカード情報等が窃取された事案

事例

- 通販サイトの運営にあたり、クレジットカード決済の接続方式として「リンク型（画面遷移方式。決済代行会社の決済画面に移動して全ての決済処理を行う接続方式のこと。）」を導入している。
- 通販サイトの脆弱性を狙った不正アクセスを受け、偽の決済画面に誘導するように通販サイトを改ざんされた。
- その結果、偽の決済画面を通じて、顧客のクレジットカード情報が窃取された！
- 各種通販サイトにおいても、上記と同様な手口による被害が発生！

POINT

- リンク型決済方式は、運営事業者がクレジットカード情報を非保持化するため、セキュリティ対策の1つとして有効な手段ですが、通販サイトに脆弱性があれば不正アクセスを受け、クレジットカード情報等が第三者に窃取される可能性があります。
- 偽の決済画面が作成された場合、顧客が気付くことは極めてまれです。
- このため、不正アクセスを受けないためのセキュリティ対策を講じることが必要です。

対策例

- 通販サイトのセキュリティ対策を定期的を確認するようにしましょう。また、脆弱性が発見された場合、適切に対策を講じましょう。改ざん検知ツール等を導入し、不正アクセス等の有無を確認することも有効です。
- 通販サイトの管理者等のIDやパスワードも適切に管理するようにしましょう。
- 標的型メールでの被害も確認されているので、不審なメール（標的型メール）は開封しないようにしましょう。



事例8 中小企業において委託契約にセキュリティ対策が含まれていなかった事例

事例

- 情報システムに詳しい社員がいない事業者が、構築・運用保守をシステム事業者に委託してECサイトを立ち上げた。しかし、保守契約における作業範囲にセキュリティ対策は含まれていなかった。
- 稼働から数年経ったある日、クレジットカード代行業者より、ECサイトからお客様のクレジットカード情報が漏えいしている可能性があるとの連絡があった。
- フォレンジック調査の結果、システムの脆弱性を突かれて不正アクセスを受けていた可能性が判明した。事業者は保守作業にセキュリティ対策も含まれていると思っていたが、あらためて保守契約書を確認したところそのような記載はなかった。

POINT

- ECサイトの構築・運用保守の委託を契約する際に、適切なセキュリティ対策を必ず盛り込んでおく必要があります。
- 情報システムに詳しい社員がいないからといって、委託先に全てを任せることは望ましくありません。委託元として何を委託し、委託内容が確かに実施されているかなど、適切に確認して管理する必要があります。

対策例

- 運用保守の契約内容に、必要なセキュリティ対策に関する事項が盛り込まれていることを確認しましょう。
- 委託先に全てを任せるのではなく、社内にも情報セキュリティのわかる社員を育成するために、中小企業向け情報セキュリティ対策資料や、企業向けセキュリティ対策セミナーなどを活用し、情報セキュリティに関する知識の習得に努めましょう。



情報セキュリティ対策に関する中小企業向け参考資料

- ・ NISC （内閣サイバーセキュリティセンター）

「小さな中小企業とNPO向け情報セキュリティハンドブック」

https://www.nisc.go.jp/security-site/blue_handbook/index.html



- ・ IPA （独立行政法人 情報処理推進機構）

「中小企業の情報セキュリティ対策ガイドライン」

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>



- ・ 東京都

「中小企業向けサイバーセキュリティ対策の極意」※

<http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/>

※都内に事業所を有する中小企業（個人事業主を含む）を対象に作成されたもの。



ウェブサイトの構築、運用に関する参考情報

独立行政法人 情報処理推進機構（IPA）ホームページより

- ・ 「安全なウェブサイトの作り方」
: <https://www.ipa.go.jp/files/000017316.pdf>
- ・ 「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>
- ・ 「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>
- ・ 「ウェブサイト運営者のための脆弱性対応ガイド」
: <https://www.ipa.go.jp/files/000058492.pdf>
- ・ 「セキュリティ担当者のための脆弱性対応ガイド」
: <https://www.ipa.go.jp/files/000058493.pdf>
- ・ 「IPA脆弱性対策コンテンツリファレンス」
: <https://www.ipa.go.jp/files/000051352.pdf>

Japan Vulnerability Notes（JVN）ホームページより

- ・ 「脆弱性対策情報のデータベース」
: <https://jvndb.jvn.jp/>