

ウェブサイトの脆弱性対策に関する注意喚起

～ ウェブサイト運営者はセキュリティ対策の再確認を！ ～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、ウェブサイトに対する攻撃事件が目立っていることを受け、ウェブサイト運営者に広く対策の徹底を呼びかけるため、注意喚起を発することとしました。

近年、ウェブサイトを用いたサービスが増加、多様化しており、企業活動の中核として位置づけられているものも少なくありません。こうしたサービスでは、製品やサービス提供の決済機能を有するものが多く、氏名や住所、電話番号などの個人情報のほか、クレジットカード情報など重要な情報が取り扱われています。他方、これらのサービスに対する妨害行為や、企業が保有する重要情報の奪取を意図した悪質な行為が目立ってきています。これらの事件の中には、ウェブサイトの脆弱（ぜいじやく）性を狙った攻撃によって情報が漏えいし、事業の継続に多大な影響を及ぼす結果となったものも複数存在します。例えば、2010年には、アウトドア用品のサイトにおいて1万件以上、オンラインゲームのサイトにおいて18万件以上の個人情報の漏えいがありました。

ウェブサイト運営者に対し、顧客情報の保護および事業継続の観点から、ウェブサイトにおける脆弱性対策の今一度の確認と、徹底を図るよう求めます。

ウェブサイト運営者が行うべき主な対策・対応は以下のとおりです。

1. サーバーにおける脆弱性対策

・ サーバーソフトウェアの脆弱性対策

定期的に、ウェブサイトで使用しているOSやサーバーソフトウェアの脆弱性対策を、ベンダー情報や脆弱性対策データベース「JVN iPedia」などを活用して実施してください。

・ ウェブアプリケーションの脆弱性対策

脆弱性診断を実施するなど、ウェブアプリケーションの脆弱性を再確認してください。脆弱性が見つかった場合は、「安全なウェブサイトの作り方」などを参考に、脆弱性を修正してください。脆弱性を修正できない場合などは、ウェブアプリケーションファイアウォール（WAF）などの活用も検討してください。

2. ネットワーク利用における対策

ネットワークの入口において、ファイアウォール、ネットワーク監視、アンチウイルスなどの対策を実施するとともに、ネットワーク上でやり取りされる情報の暗号化による保護などで、リスクを低減してください。

3. 重要な情報の保護

万一、ウイルス感染や不正アクセスをされた場合でも情報を保護するため、情報へのアクセス制御の実施や、重要な情報の暗号化などで多段の防御をしてください。

4. 日常的な運用監視と事後対応

日々、iLogScanner等の活用によるアクセスログの分析、データベースへのアクセス監視で、攻撃をいち早く検知できる仕掛けや体制を整備してください。また、万一、事件・事故が発覚した場合は、それに対応するマニュアルや体制を事前に確立しておくことで、二次被害を最小限に留めるように備えてください。

個人情報の取扱いに対しては「個人情報保護基本法」やプライバシーマーク制度を、またクレジットカード情報を取り扱うウェブサイトでは、業界のガイドである PCI DSS^(*)を参考にしてください。

■本件に関するお問い合わせ先

IPA セキュリティセンター 小林／金野／相馬

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp

■報道関係からの問い合わせ先

IPA 戦略企画部広報グループ 横山／大海

Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

^(*) Payment Card Industry Data Security Standard
<https://ja.pcisecuritystandards.org/minisite/en/pci-dss-v2-0.php>