

IPA テクニカルウォッチ：「サーバソフトウェアが最新版に更新されにくい現状および対策」の公開

～ウェブサイトでサポート終了後のPHP^(*)（ピーエイチピー）を使用している割合は80%～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、IPAが脆弱性の届出を受けたウェブサイトそれぞれで使用されているウェブサーバ関連ソフトウェアのバージョン確認を実施し、その結果を踏まえ、ウェブサイト運営組織および管理者向けに「サーバソフトウェアが最新版に更新されにくい現状および対策」を2014年4月25日からIPAのウェブサイトで公開しました。

URL：<http://www.ipa.go.jp/security/technicalwatch/20140425.html>

ウェブサイトは今や企業、組織の事業運営に深く関わり、一般的に24時間、365日間断なく稼働しています。仮にウェブサイトに情報セキュリティ上の不備があれば、常に被害を受ける可能性があるといえます。実際、2013年には、ウェブサイトが改ざんを受ける例が7,409件も発生しました⁽²⁾。その中には、悪意ある仕掛けが施され、利用者は閲覧しただけでウイルスに感染してしまう事象（ドライブバイダウンロード）もあり、閲覧者のウイルス感染や、ウェブサイトからの情報漏えいが発生しています。この原因の1つとして、ウェブサーバ構築に使用されているソフトウェアが古いバージョンのまま、脆弱性が未修正であったことが挙げられます。

このため、IPAでは2008年2月から2013年9月の間に脆弱性の届出があったウェブサイトで使用されていたサーバ関連ソフトウェア⁽³⁾のうち、「PHP」「Apache」「IIS」を対象に届出時点のバージョンの調査を実施⁽⁴⁾しました。その結果、プログラミング言語処理系「PHP」については、80%でサポートが終了したバージョンが使用されている可能性が高い⁽⁵⁾ことがわかりました。

	サポート範囲内	サポート終了後 1年以内	サポート終了後 1年以上	合計
PHP	285 (20%)	215 (15%)	915 (65%)	1,415
Apache HTTP Server	1,450 (85%)	40 (2%)	222 (13%)	1,712
IIS	496 (94%)	4 (1%)	25 (5%)	525

⁽¹⁾ ウェブアプリケーションを稼働させるためソフトウェアの一種。PHP言語で書かれたウェブアプリケーションを稼働させることができる。プログラミング言語処理系に分類される。

⁽²⁾ 2013年4月15日から2014年1月16日にかけてJPCERTコーディネーションセンターが発表した四半期別のインシデント報告対応レポート、4通をもとに算出。

<https://www.jpccert.or.jp/ir/report.html>

⁽³⁾ 本調査で対象としたのはウェブサーバ、ウェブアプリケーションサーバ、ウェブアプリケーションフレームワーク、プログラミング言語で、詳細は本テクニカルウォッチP3を参照のこと。

⁽⁴⁾ 外部からアクセスした際に得られるレスポンスヘッダから、製品名とバージョンを取得。それを、製品開発元によるサポート終了時期と調査時点を比較し、サポート範囲内であるか、否か（サポート終了後1年以内か、それ以上か）を集計した。詳細は本テクニカルウォッチP6を参照のこと。

⁽⁵⁾ ソフトウェアの正確なバージョンは、外部からのアクセスでは正確に把握できない場合があり、実態は調査結果よりも安全である可能性がある。また、届出されたウェブサイトを対象にしているため、一般的なウェブサイトの傾向とは必ずしも一致しない可能性がある。

旧バージョンのままウェブサイトの運営を継続するのはサイバー攻撃の標的とされかねないことから、IPA では中長期的な視点に立ったウェブサイト構築および運営のための組織的な管理のあり方を IPA テクニカルウォッチ：「サーバソフトウェアが最新版に更新されにくい現状および対策」としてまとめ、4月25日より公開しました。

運営管理の体制整備において提案しているのは、以下のような手順です。

① サービスレベル目標の設定

稼働時間の検討、運営期間の決定、想定する障害発生率等

② 運営体制の整備

決定したサービスレベルに基づき、それを実現するための体制（工数・人材・ノウハウ）を確保する。

③ 実務の設計

決定した運営体制を元に、運用チームの編成、手順の標準化・教育、事前のトラブル対策、維持管理のための点検項目の整理等

旧バージョンが使用され続けるその理由には、①最新バージョンに移行すると旧バージョンで作成したウェブアプリケーションが動かなくなる互換性の問題、②開発時の担当者が既に不在、対応・運用手順書も無く最新バージョンへ移行ができないという、工数・人材・技術継承など運用管理上の問題、があります。

しかし、最新でない状態でウェブサイトを運営し、万が一脆弱性を悪用された場合、事業継続への影響のみならず利用者にも迷惑が及び、事後対応に相応のコストが生じることは避けられません。

本書では IPA が実際に運営するウェブサイトをケーススタディとして、適切な体制を整えることで問題を事前に防ぐ例も示しています。これらも参考に、安全なウェブサイトの運営のために中長期的かつ、組織的な管理方法を検討し、実施することを期待します。

■ 本件に関するお問い合わせ先

IPA 技術本部 セキュリティセンター 永安／板橋

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

■ 報道関係からのお問い合わせ先

IPA 戦略企画部 広報グループ 横山／白石

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