2014 年 8 月 20 日
NRI セキュアテクノロジーズ株式会社

企業が一元的に存在を把握している自社 Web サイトは約 5 割にとどまるーインベントリ管理の再考を
～企業情報システムのセキュリティに関する分析結果(2014 年版)～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：増谷 洋、以下「NRI セキュア」）は、顧客企業に提供した各種の情報セキュリティ対策サービスを通じて得られたデータ[*1]の分析を元に、最新のセキュリティ脅威の動向と推奨する対策を「サイバーセキュリティ 傾向分析レポート 2014（以下「本レポート」）」として取りまとめました。本レポートは、企業や公的機関の情報セキュリティ対策の推進を支援する目的で、2005 年度以降、毎年発表しており、今回で 10 回目となります。

今回の分析で明らかになった、情報セキュリティ関連の問題点は以下の 3 つです。

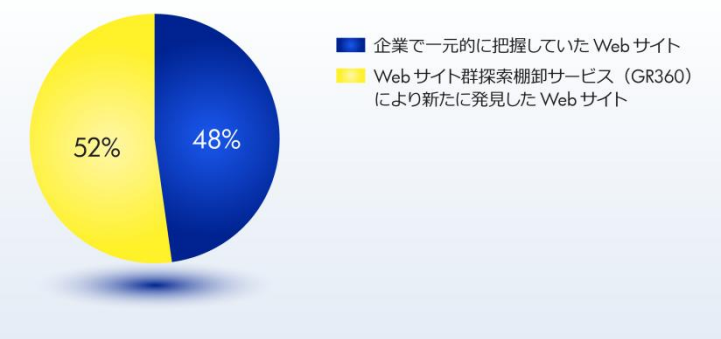
○ 企業が一元的に存在を把握している Web サイトは約 5 割に過ぎない
○ サポート切れソフトウェア製品のバージョンアップが進んでいない
○ CSIRT[*2]（情報セキュリティ対策チーム）の運営に必要な人材の確保が困難である

■企業が一元的に存在を把握している Web サイトは約 5 割、Web サイトのインベントリ管理の再考が必要

企業が管理すべき Web サイトの棚卸を実施した結果、企業が一元的に存在を把握できていた Web サイトは約 5 割にとどまることがわかりました。危険度が高い脆弱性が公表された際には、各サイトについて脆弱性を抱えるバージョンのソフトウェア製品を利用しているかどうかに加え、そのサイトがインターネットに公開されているか否かといったネットワークの構成情報も考慮に入れた調査が必要になります。

しかし、一元的に把握できていない約 5 割の Web サイトについては、そもそも、その調査対象に含まれないため、脆弱性が放置されたままで公開されている可能性があります。

【図 1： Web サイトの把握状況に関する棚卸結果（n=5338 サイト）】



Web サイトのセキュリティ対策を講じる上では、管理対象を洗い出す作業が真っ先に必要です。企業の規模が大きく、また組織が複雑になればなるほど実践が難しい作業であるとも言えます。クラウドサービスの台頭、企業の再編や海外進出等を背景として、Web サイトにおけるインベントリ管理の仕組みを見直す必要性が高まっています。

■ソフトウェア製品のサポート切れリスクの認識と対応が必要

2013 年度、PHP[*3] と Struts[*4] に対して公表された危険度が高い脆弱性は、2012 年度に公表された類似のものと比べて、脆弱性の公表日から攻撃を観測するまでの期間が短期化（1～3 日程度）しています。このような攻撃への根本的な対策は、攻撃を受ける前に迅速にセキュリティパッチを適用[*5]することですが、Web サイトで利用されているソフトウェア製品の中には、セキュリティパッチを入手できない「サポート切れ」の状態で稼働しているものがあります。例として、PHP と Apache[*6] のサポート切れの状況は図 2 の通りです。

【図 2： ソフトウェア製品のサポート切れ状況（一部紹介）】

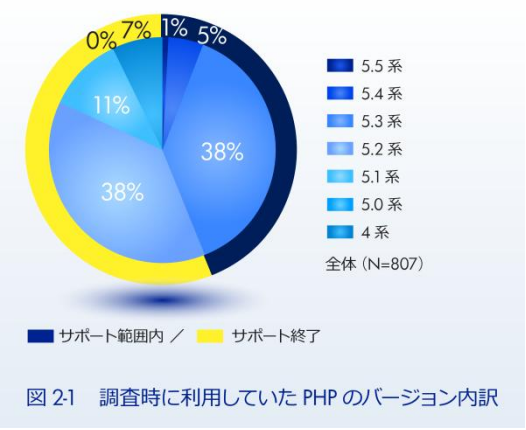


図 2-1　調査時に利用していた PHP のバージョン内訳

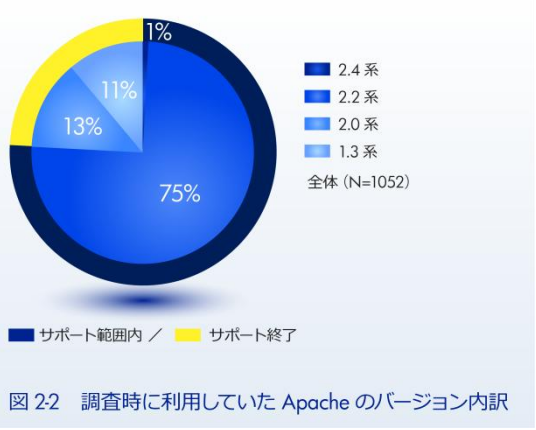


図 2-2　調査時に利用していた Apache のバージョン内訳

セキュリティパッチを入手するためには、サポート切れの製品をバージョンアップして、サポートを受けられる状態にする必要があります。しかし、その際に Web アプリケーションの改修が必要になる場合も多く、また改修には一定期間を要するため、脆弱性の公表日から攻撃を受けるまでの短期間のうちに対策を完了することは非常に困難です。バージョンアップを実施するまでの暫定措置としては、WAF[*7]（Web アプリケーションファイアウォール）の活用が有効です。

■CSIRT 運営には、システムと人材の融合と継続的な訓練・教育が不可欠

セキュリティ対策の一つとして、CSIRT の重要性が認知されてきています。しかし、実際に CSIRT を立ち上げて運営していくには、CSIRT で提供するサービス範囲に応じて、セキュリティ基盤の設計や構築といったシステム面の工夫と、高度な専門性を有する人員の確保をはじめとする人材面での手当てという、2 つの要素が必要です。これら 2 つの要素を

適切に融合できなければ、昨今の高度化・多様化するサイバー攻撃に迅速かつ正確に対応していくことは困難です。さらに、CSIRT には持続的な活動が求められることから、継続的な運用訓練や教育を通じて、日々進化する攻撃への対応力を維持し続けることが、最も難しくかつ重要なポイントです。

「サイバーセキュリティ 傾向分析レポート 2014」の詳細については、下記の Web サイトを参照ください。

http://www.nri-secure.co.jp/news/2014/0820_report.html

*1　本レポートで分析対象としたデータ：
NRI セキュアテクノロジーズが、2013 年度（2013 年 4 月 1 日～2014 年 3 月 31 日）に、顧客企業に提供した情報セキュリティ関連サービスから得られたデータ、および 2008 年度からの経年データ。

*2　CSIRT（Computer Security Incident Response Team）：
組織内において、情報セキュリティの問題に対して専門に対応する組織。

*3　PHP（PHP:Hypertext Preprocessor）：
Web サーバ上で動作する、動的なウェブページを作成するためのプログラム言語。

*4　Struts：
Java を用いた Web アプリケーションの開発ツール群。

*5　セキュリティパッチの適用：
脆弱性があるプログラムに対して、修正ファイル（パッチ）を適用すること。

*6　Apache：
Web サーバを構築するためのソフトウェア製品。

*7　WAF（Web アプリケーションファイアウォール）：
Web アプリケーションへの攻撃を防止するセキュリティ対策製品。

【お知らせに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部　十河、海藤
TEL：03-6270-8100　E-mail：kouhou@nri.co.jp

【レポートに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　テクニカルコンサルティング部　深尾
TEL：03-6706-0500　E-mail：info@nri-secure.co.jp