一般社団法人電子情報技術産業協会
一般社団法人コンピュータソフトウェア協会
一般社団法人情報サービス産業協会
特定非営利活動法人日本ネットワークセキュリティ協会　御中

Web サイト改ざんへの対策の実施について（協力依頼）

平成２５年９月９日
経　済　産　業　省
商 務 情 報 政 策 局
情 報 処 理 振 興 課
情 報 通 信 機 器 課
情報セキュリティ政策室

本年に入り、国内の企業等の Web サイトが改ざんされる被害が急増しています。一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT コーディネーションセンター」という。） に 2013 年前半期（１月から６月の間）に報告された Web サイト改ざんの被害件数は 3031 件に上り、前年（同期比）で 11 倍の増加となっています。

Web サイト改ざんによる被害の多くは表示される内容が書き換えられるものですが、書き替えられた内容がマルウエア配付サイトへ誘導するスクリプトの挿入等である場合には、自社のサイトを閲覧した顧客をマルウエアに感染させる攻撃に加担することになってしまうことから、企業の信用にもかかわる問題となり得ます。また、一部では、改ざんに併せ、ユーザのアカウント情報などの機微な情報が窃取される被害も発生していることから、Web サイト改ざんへの対応を適切かつ速やかに実施する必要があります。

このため、技術的に必要な対策を下記の通り周知させていただきますので、団体各社への情報展開等、御協力をお願い申しあげます。

記

１．Web サイトの改ざんの手法についての理解の周知

現在発生している Web サイト改ざんは、一部には Web サイト管理用の ID やパスワードを何万回も試行してログインを試みるブルートフォース攻撃や辞書攻撃が確認され、また、

マルウエアに感染させた PC 等から窃取した正規の ID、パスワードの悪用によるとみられる事例も存すると見込まれますが、多くの場合は、Web サイトに使用されているソフトウエアの脆弱性を突いてファイルを改ざんする手法によっています。

脆弱性を突く攻撃は、Web サイトのコンテンツを総合的に管理する「CMS(Content Management System)」や、動的なコンテンツの作成を容易にする「Web アプリケーションフレームワーク」といった製品の脆弱性を悪用するものが多くを占めています。このような脆弱性を悪用する攻撃は、多くの場合、製品開発ベンダが提供する修正済みソフトウエアに更新することで防ぐことが可能です。

特に、7 月に公表された Web アプリケーションフレームワークである「Apache Struts の脆弱性（S2-016)」は、悪用が容易であり、かつ攻撃用ツールが多数開発・公開されていることから、今後大きな被害に発展することが懸念され、この脆弱性に未対応である場合には、至急の対応が必要となります。(既に一部で被害が発生しているとの情報もあります。)ただし、一般的にはソフトウエアの更新に伴って不具合が発生し、製品が正常に動作しなくなるといったケースが少なからず発生することから、更新時には、システムを熟知した専門家による事前の動作検証が重要となります。

２.「Apache Struts の脆弱性（S2-016)」の検証レポートの配布

JPCERT コーディネーションセンターは、今般、顧客からの委託等に基づいて脆弱性への対応を実施するシステム構築事業者やシステム運用受託事業者が、この脆弱性の脅威を正確に理解し、適切な対応を行うための参考資料として、当該脆弱性について調査し、その対策、攻撃の検知についてまとめた「Apache Struts の脆弱性（S2-016)」の検証レポートを作成しました（添付)。本レポートについて、貴団体の関係企業等に配布いただき、Web サイト改ざんへの対応の際の参考に活用していただくよう、改ざんによる被害拡大の抑止に御協力をよろしくお願いいたします。

Apache Struts の脆弱性（S2-016）に関する注意喚起
https://www.jpcert.or.jp/at/2013/at130033.html

※「Apache Struts の脆弱性（S2-016)」の検証レポートの取扱いについて

なお、本レポートについては、自組織外を含む必要な範囲への情報転送が可能です。ただし、Web サイトや公開のメーリングリストなどを使用して一般へ公開することは出来ません。情報転送をされる場合には、情報の取扱いルールについても併せて伝達をお願いし

ます。

３．その他

なお、ウェブサイトの改ざんについては、この脆弱性以外にも、WordPress やそのプラグインに関する脆弱性、Parallels Plesk Panel の脆弱性などを悪用して行うものも多数確認されており、これら製品に関する対応についてもあわせてご確認をお願いいたします。

旧バージョンの Parallels Plesk Panel の利用に関する注意喚起
https://www.jpcert.or.jp/at/2013/at130018.html

以　上