（別添）
プレスリリース
2013 年 9 月 6 日
独立行政法人情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター

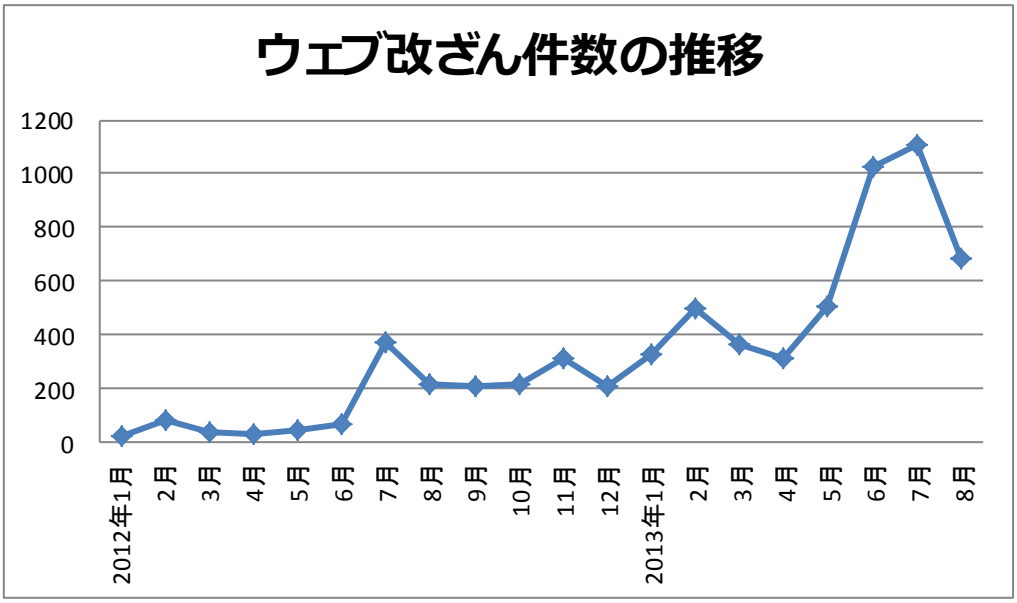
ウェブサイト改ざん等のインシデントに対する注意喚起

～ウェブサイト改ざんが急激に増えています～

IPA（独立行政法人情報処理推進機構、理事長：藤江　一正）および JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター、代表理事：歌代　和正）は、ウェブサイト改ざん等のインシデントの急激な増加を受け、ウェブサイト運営者及び管理者に対し、改めて点検と備えを呼びかけます。

1. 概要

JPCERT/CC によれば、ウェブサイト改ざんの被害件数が 2013 年 6 月、7 月には 1,000 件を越えるなど、急激な増加が見受けられます（2013 年 4 月：314 件、5 月：505 件、6 月：1028 件、7 月：1106 件、8 月：687 件）[1]。IPA への届出も同じく増加が見られ、2013 年 6 月、7 月に「今月の呼びかけ」[2]で注意喚起を実施してきました。



図：ウェブ改ざん被害の推移（JPCERT/CC への報告による）

インターネット上における組織の入口ともいえるウェブサイトが改ざん等の攻撃を受けると、組織活動の停止あるいは遅滞、閲覧者のウイルス感染、秘匿情報（クレジットカード情報等）の漏えいなど、深刻な被害を及ぼします。また例年、この時期にはウェブサイトへの攻撃が多くなっていることを踏まえ、ウェブサイト改ざんに対する注意喚起をするものです。

2. 昨今のウェブサイトへの攻撃

昨今増加しているウェブサイトへの攻撃の代表的な例は、次のようなものがあります。

① ウェブサイトの管理端末への侵入によるウェブサイト改ざん

ウェブサイトを管理する端末における OS やアプリケーションの脆弱性を狙ったウイルスによって、ウェブサイトを管理する端末に侵入され、その管理端末からウェブサイトを管理するための認証情報を窃取されてしまいます。

---

[1] JPCERT/CC インシデント報告対応レポート【2013 年 4 月 1 日～2013 年 6 月 30 日】※7 月、8 月分については 10 月に報告予定
https://www.jpcert.or.jp/pr/2013/IR_Report20130711.pdf

[2] 2013 年 6 月の呼びかけ「ウェブサイトが改ざんされないように対策を！」
http://www.ipa.go.jp/security/txt/2013/06outline.html
2013 年 7 月の呼びかけ「止まらないウェブ改ざん！」
http://www.ipa.go.jp/security/txt/2013/07outline.html

このような方法で窃取された認証情報が悪用され、ウェブサイトを改ざんされるという被害が 2008 年頃より多数発生します。

② パスワードリスト攻撃

パスワードリスト攻撃とは、悪意のある者が、何らかの方法で事前に入手した ID とパスワードのリストを流用し、自動的に連続入力するプログラムなどを用いてそれら ID とパスワードを入力することで、ログインを試みる手口です。

そのため、利用者が複数のインターネットサービスで同じ ID とパスワードを使い回している場合に、その中のいずれかでアカウント情報が漏えいしてしまうと、悪意のある者が別のインターネットサービスで同じ ID とパスワードを用いて、利用者になりすまして不正にログインすることが出来てしまいます。

「全てのインターネットサービスで異なるパスワードを！」
～ 多くのパスワードを安全に管理するための具体策 ～
http://www.ipa.go.jp/security/txt/2013/08outline.html

③ ソフトウェアの脆弱性を狙った攻撃

＜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

2013 年 7 月 16 日に公表された Apache Struts 2 の脆弱性に対する情報とパッチが公開されました。この脆弱性情報が公開された後、この脆弱性を狙った攻撃が急増したというセキュリティベンダ等からの注意情報が公表されています。

＜WordPress 用 Xhanch - My Twitter プラグインにおけるクロスサイトリクエストフォージェリの脆弱性＞
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-003693.html

WordPress 用 Xhanch - My Twitter プラグインの admin/setting.php には、クロスサイトリクエストフォージェリの脆弱性が存在します。第三者により、管理者の認証を乗っ取られ、不特定の設定を変更される可能性があります。

＜Parallels Plesk Panel に任意のコードが実行される脆弱性＞
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-002926.html

Parallels Plesk Panel が稼働しているウェブサーバにおいて、phppath のエイリアス設定に関する問題と、CVE-2012-1823 の問題が同時に存在する場合に、任意のコードが実行される可能性があります。

＜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

旧バージョンの Parallels Plesk Panel に存在する SQL インジェクションの脆弱性を用いてアカウント情報が窃取されたり、初期設定のパスワードや簡易なパスワードを設定している場合には辞書攻撃によりアカウント情報が特定されて、不正なログインが行われている事例を確認しています。また、ログイン後、Parallels Plesk Panel の cron manager 機能を用いて不正なスクリプトを動作させ、結果として不正な Apache モジュールが設置されている事も確認しています。

④ SQL インジェクション攻撃

ウェブサイトを構築するウェブアプリケーションに SQL インジェクションの脆弱性が存在する場合、その脆弱性を狙った攻撃が実施されることで、ウェブサイトを改ざんされる等の被害を受ける可能性があります。

3. 対策方法

上記に挙げた代表的な攻撃に対する対策は、それぞれ次のものがあります。

① ウェブサイトの管理端末への侵入によるウェブサイト改ざんへの対策

ウェブサイトの管理端末の OS やアプリケーションを最新の状態にしてください。また、下記のサイト等を参考に、必要があれば「ウェブサイトを更新できる端末を限定」する等の対策も実施してください。
ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起
一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起
http://www.ipa.go.jp/security/topics/20091224.html

② パスワードリスト攻撃への対策

ID・パスワードを使い回さないことをウェブサイト利用者に対して呼びかけるほか、システム上、ID・パ

スワード以外の、例えば携帯電話等の持ち物等といった本人確認の要素を取り入れる「2 要素認証」等の仕組みを入れることを検討してください。

③ ソフトウェアの脆弱性を狙った攻撃

脆弱性について対処済みのバージョンへアップデートしてください。
OS やミドルウェアのサーバ製品に関しても可能な限り最新版の利用を推奨します。

④ SQL インジェクション攻撃への対策

＜自組織で作成している場合＞

「安全なウェブサイトの作り方」「ウェブ健康診断」等を参考にして、SQL インジェクションの有無の確認、および SQL インジェクションの対策を実施してください。

「安全なウェブサイトの作り方」「別冊：ウェブ健康診断」
http://www.ipa.go.jp/security/vuln/websecurity.html
SQL インジェクション対策について
http://www.ipa.go.jp/files/000024396.pdf

＜コンテンツ管理システム（CMS）等を利用している場合＞

ウェブサイトの作成・管理等に「コンテンツ管理システム（CMS）」を使用している場合は、それらのバージョンの出来るだけ最新のものを利用してください。

4. ウェブ改ざん等の発見、被害に関する連絡先

ウェブサイトの改ざん等を発見した方、被害に遭われた方は、以下の問い合わせ先までご連絡ください。

	JPCERT/CC インシデント報告
E-mail	info@jpcert.or.jp
FAX	03-3518-2177 ※インシデント報告以外のものは 03-3518-4602 宛にお願いします。
Web フォーム	https://www.jpcert.or.jp/form/#web_form

ウェブサイトに関する不安やご相談がおありの方は以下の窓口へご連絡ください。

	IPA 情報セキュリティ安心相談窓口の問合せ先
電話	03-5978-7509 （相談対応員による対応は、平日の 10:00～12:00 および 13：30～17:00）
E-mail	anshin@ipa.go.jp （このメールアドレスに特定電子メールを送信しないでください。）
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

■ 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 金野／相馬
Tel: 03-5978-7527 Fax: 03-5978-7518
E-mail: vuln-inq@ipa.go.jp
JPCERT/CC 早期警戒グループ 中谷／満永
Tel: 03-3518-4600 Fax: 03-3518-4602
E-mail: ww-info@jpcert.or.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
JPCERT/CC 事業推進基盤グループ 広報 江田
Tel: 03-3518-4600 Fax: 03-3518-4602
E-mail: pr@jpcert.or.jp