Information-technology
Promotion
Agency, Japan

第 13-25-293 号
2013 年 6 月 4 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 ウェブサイトが改ざんされないように対策を！ 」
～　サーバーやパソコンのみならず、システム全体での対策が必要です　～

IPA セキュリティセンターではコンピュータウイルスや不正アクセスに関する届出を受け付けています。特に不正アクセスの中の「ウェブ改ざん」に着目すると、4 月 1 日から 5 月 31 日までの間に既に 10 件ものウェブ改ざんに関する届出が寄せられています。過去には、いわゆる「ガンブラー」の手口が流行した 2010 年第 1 四半期と、去年 9 月に近隣諸国からと思われる攻撃が多発した 2012 年第 3 四半期に、それぞれ 16 件のウェブ改ざんが届け出られていますが（図 1 参照）、それに匹敵する件数です。

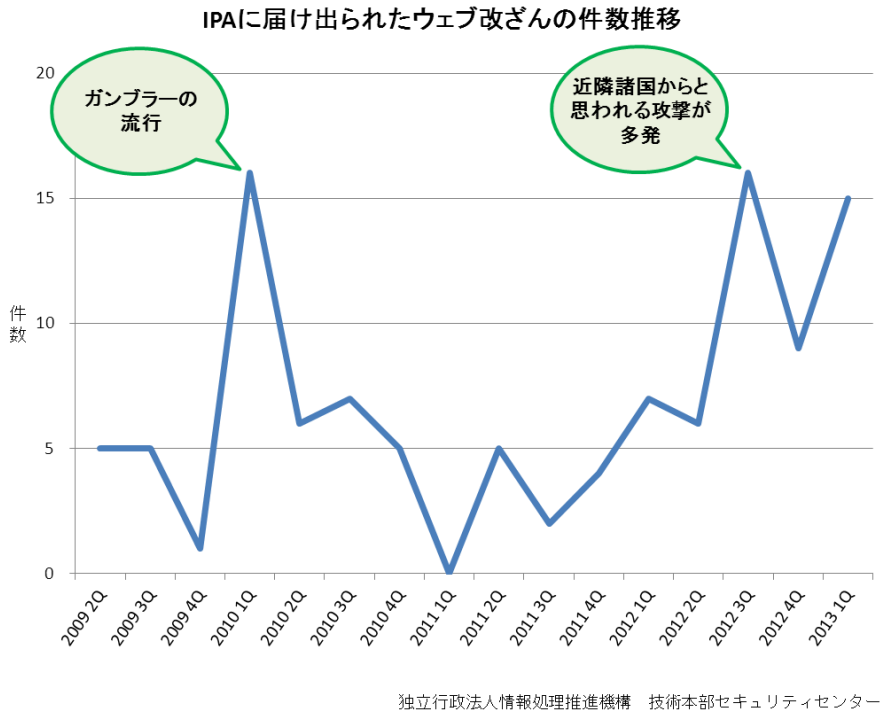

図 1：IPA に届け出られたウェブ改ざんの件数推移（直近 4 年間）

「ウェブ改ざん」というとサーバーの弱点を悪用されるものと思われがちですが、それ以外にも、ウェブページの更新に用いられるパソコンの脆弱性が解消されていなかったためにウイルスに感染し、FTP アカウント情報※が流出してしまった結果、自社のウェブサイトが改ざんされてしまうケースがあります。最近 1 年間で見ても、パソコン内の FTP アカウント情報を悪用されたと思われる届出は、原因が特定されているものの中で、サーバーの脆弱性悪用に次いで 2 番目に多い状況です（図 2 参照）。

サーバー側でいくら対策を施しても、組織内ユーザーのパソコンがウイルスに感染して FTP アカウント情報が漏えいしてしまうと、第三者が正規の管理者になりすまして FTP ログインすることが可能になります。つまり、対策としてはサーバー側だけでは不十分で、社内パソコンを含めた総合的な対策が必要です。

ウェブ改ざんの被害に遭うと、「改ざんされた」という事実によって組織としての信用が低下するだけでなく、もしウイルス配布サイトに改ざんされてしまった場合は、改ざん後のページを閲覧した顧客などのパソコンがウイルス感染する恐れがあるので、システム管理者は適切な対策を実施する必要があ

ります。
今月の呼びかけでは、組織におけるシステム管理者と、個人のウェブサイト所有者向けに、ウェブ改ざんの事例と対策について説明します。

※FTP アカウント情報：
ウェブサイトのコンテンツを追加・修正・削除などする際に、ウェブサーバーに FTP ログインするための ID、パスワードと、ログイン先のサーバーの情報。

（1） 最近のウェブ改ざんの事例

① 脆弱性の悪用によるもの

サーバー上で動作するプログラムのバージョンが古いままだったために、脆弱性を悪用されて改ざんされてしまったケースがありました。この脆弱性悪用は、IPA に寄せられるウェブ改ざんの原因で、最も多いものです（図 2 の円グラフ参照）。

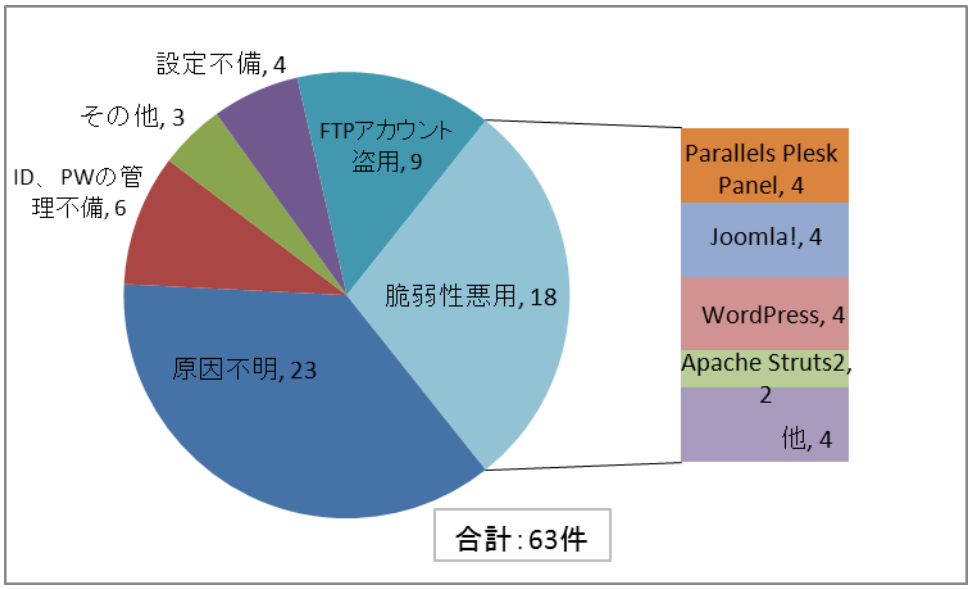

図 2：ウェブ改ざんの「原因」による分類（2012 年 1 月～2013 年 5 月）

今年 4 月以降では、以下の製品の脆弱性を悪用されたウェブ改ざん届出が寄せられました。

- Joomla！
- WordPress
- Apache Struts2

最近 1 年間で見ると、脆弱性悪用の中では、Parallels Plesk Panel の脆弱性を悪用されたウェブ改ざんが多い状況です（図 2 の棒グラフ参照）。Parallels Plesk Panel が稼働しているサーバーには、付随して様々なプログラム（MySQL、BIND、phpAdmin など）がインストールされている可能性があり、ウェブサイト管理者はこれらのプログラムを意識しないまま、古いバージョンで稼働させている場合があるので注意が必要です。

（ご参考）
旧バージョンの Parallels Plesk Panel の利用に関する注意喚起（JPCERT/CC）
http://www.jpcert.or.jp/at/2013/at130018.html

ウェブサイト管理者は、サーバー上で動作するプログラムを常に最新にしておく必要があります。

② FTP アカウント情報の漏えいによるもの

“FTP ログインアカウントには複雑で類推しにくいパスワードを設定していたにも関わらず、

様々なパスワードを試した痕跡がなく、初めの 1 回でログインに成功されてしまった”というケースがありました。このケースでは何らかの理由によってパスワードが盗まれてしまった可能性があるため、パソコンがウイルスに感染したことによってパスワードが漏えいしたことを疑う必要があります。

“パソコンの Java のバージョンが古いままだったために FTP アカウント情報を漏えいさせるウイルスに感染した”というウイルス感染のケース※もありました。このケースでは当該パソコンでウェブサイト管理を行っていなかったため、FTP アカウント情報の漏えいはありませんでしたが、ウイルス感染によってウェブ改ざん被害を受ける可能性があることを示す事例です。

※　このウイルスは他にメールアカウント情報を流出させる機能を有しており、実際に迷惑メール送信の踏み台に悪用されていました。

（2） 改ざん有無の確認方法

もし既にウェブを改ざんされていて、そのことに気付かないままウェブサイトを運営していると、企業・団体としての信用が低下するだけでなく、もしウイルス配布サイトに改ざんされてしまった場合は、改ざん後のページを閲覧した顧客などのパソコンがウイルスに感染する恐れがあります。

まず最初に、今現在改ざんされていないかどうかを確認するために、以下を参考に改ざんの有無をチェックしてください。

・サーバ上 HTML ソースと、手元においてあるオリジナルの HTML ソースを比較。
（ページを見ただけではわからないように、HTML ソースを埋め込み転送させる仕掛けを施している場合があります）
・HTML ソースをセキュリティソフトでスキャン。
・ftp アクセスログを確認。

万が一改ざんされていることが判明した場合、被害の拡大を防ぐために早急な対応が求められます。まずはウェブサイトの公開を一旦停止した上で、原因究明と修正作業を実施してください。

ウェブサイトの利用者に向けては、改ざんの事実と、改ざん内容によってはウイルスに感染する危険性があった旨を注意喚起し、謝罪文を掲載することを勧めます。また、利用者からの問い合わせに対応できるよう、窓口を設けるなどの体制を敷いておくことが望ましいでしょう。

ウェブサイト改ざんの被害に遭った際は、できれば IPA への届出を行ってください。届けられた情報は、個人や組織を特定できる情報を除いた上で分析および統計処理し、対策情報の発信のために活用させて頂きます。

（ご参考）
「情報セキュリティに関する届出について」
http://www.ipa.go.jp/security/todoke/

ウェブサイト改ざん被害に遭われた場合、被害の再発を防ぐために、後述の（3）、（4）の対策を実施してください。

今被害に遭っていない場合でも、今現在適切に対策が取られているかどうかを、後述の（3）、（4）を参考にチェックしてください。

（3） 組織内ユーザー、ウェブサイト所有・管理者向け対策

ウェブ改ざん対策というと、サーバーだけを対策していれば良いと考えがちですが、パソコンでの対策も重要です。前述の通り、組織内のパソコンがウイルス感染してしまうと、パソコン内に格納されている FTP アカウント情報が漏えいしてしまう可能性があるからです。

ウェブサイトを所有・管理している個人の方も、普段使いのパソコンでウェブサイトを管理することが多いため、下記を参考に対策を実施してください。

① OS と各種プログラムを常に最新状態にする（パソコンの脆弱性を解消する）

OS や各種プログラムの脆弱性を悪用されないようにするために、古いバージョンのままにせず、常に最新の状態に保つことが一番の対策になります。

前述の Java に加えて、Flash Player、Adobe Reader も特に狙われやすいため、更新通知が画面に表示されたらその都度更新してください。プログラムの自動更新機能を利用することも有効です。

（ご参考）

「ソフトウェアの自動更新を利用しましょう！」
https://www.ipa.go.jp/security/txt/2012/06outline.html

「Windows XP サポート終了： Windows XP のサポート終了について」
http://www.ipa.go.jp/security/anshin/faq/faq-xp.html

IPA では、パソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を無償で公開しています。ぜひ活用してください。

（ご参考）

MyJVN バージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/

かつては「怪しいサイトを閲覧しなければ大丈夫」と言われていたこともありましたが、近年ではどのサイトが不正に改ざんされているか分からないため、セキュリティ対策を実施していないパソコンでインターネットを利用することは非常に危険です。従って、利用者自身で対策を行い自衛することが不可欠です。

② セキュリティソフトを使用する

セキュリティソフトを導入し、定義ファイルを最新に保ちながら使用してください。有害なウェブサイトを閲覧することを防止する機能（ウェブレピュテーション機能など）を持つ、統合型セキュリティソフトを使用することで、感染被害を未然に防げる場合があります。

③ 万が一に備えてパーソナルファイアウォールを導入する

万が一、気づかないうちにウイルス感染や、不正プログラムがインストールされてしまった場合、パーソナルファイアウォール※の導入による出口対策をお勧めします。パーソナルファイアウォールの設定により、自分が許可したプログラムだけを外部と通信可能とし、ウイルスや不正アプリが行う通信を遮断することで、感染してしまっても情報が外部の第三者に窃取されるなど、最悪の事態を防ぐことができます。

※パーソナルファイアウォール：
個々の端末（パソコンやモバイル機器など）に導入するもので、端末と外部ネットワークの間の通信を制御するソフトウェアです。通常、“事前に許可した通信以外を通過させない”、“許可するプログラムを事前に登録しておき、未許可のプログラムの通信を遮断する”といった機能を持ちます。OS の機能として組み込まれているほか、製品単体としても販売されていますが、「統合型セキュリティソフト」と呼ばれる製品の中にパーソナルファイアウォール機能を併せ持つものもあります。

パソコンのウイルス感染によって、FTP アカウント情報の漏えいのみならず、メールアカウント情報

など他の情報が漏れてしまう恐れもあります。実際、前述の FTP アカウント情報漏えいのウイルスに感染した例では、メールアカウント情報も窃取されており迷惑メール送信に悪用されていました。従業員 1 人のパソコンのウイルス感染によって業務上重要な情報が漏えいする恐れがあるので、システム管理部門は各従業員に対して脆弱性対策を徹底してください。

（4） システム管理者向け対策

① サーバーの脆弱性対策を実施する

パソコンと同様、サーバー上でも脆弱性対策が重要です。サーバー上で稼働するすべてのプログラムを最新の状態に保ってください。

Joomla！、WordPress などの CMS を利用していて、さらにそのプラグイン（拡張機能）も利用している場合は、プラグインも含めて最新にしてください。

Parallels Plesk Panel などのサーバー管理ツールを利用している場合、他のプログラムが付随してインストールされている場合があるので、それらすべてを最新にしてください。

（ご参考）

MyJVN バージョンチェッカ（サーバー用）

http://jvndb.jvn.jp/apis/myjvn/vccheckserv.html

② ウェブサイトの運用を再確認する

(a) アカウント管理の見直し

ウェブサイト更新用のアカウント情報が適切に管理されているか、下記の点を見直してください。

・使用するパスワードは、十分な長さと複雑さをもったものにしてください。

・ウェブサイト更新用のアカウントは、更新を実施する人のみが知るようにし、必要以上の人に知らせないようにしてください。

(b) ウェブサイトを更新できる場所を限定

サーバーに接続する時の接続元 IP アドレスを限定し、ウェブサイトを更新する場所を組織内のみに限定するよう、ネットワークやサーバーの構成を見直すことを検討してください。もし、インターネット経由でウェブサイトを更新する必要がある場合でも、VPN を導入するなどして、更新できる場所を限定することを検討してください。

この対策を実施することにより、万が一 FTP アカウント情報が漏えいしてしまっても改ざん被害を防止できる場合があります。

(c) ウェブサイト更新専用 PC の検討

ウェブサイトを更新するための専用 PC を導入することを検討してください。この PC では、ウェブサイト更新作業のみを行い、ウェブの閲覧など他の作業をしないようなルールの設定が必要です。これによって、ウイルスによる被害を防止することが可能です。

（5） こんなときは…

IPA 安心相談窓口では、コンピュータウイルスや不正アクセスに関する相談を受け付けております。

改ざん対策についての相談や、実際に被害を受けた際の相談などがありましたら、下記の IPA 安心相談窓口までご連絡ください。

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、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

※迷惑メール対策などで「メールの受信/拒否設定」が設定されている場合、IPA からのメールを受信できない場合があります。 IPA からの返信メールを受信できるように、「anshin@ipa.go.jp」や「ipa.go.jp ドメイン」からのメールを受信できるように設定をしてください。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／田中
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp