Information-technology
Promotion
Agency, Japan

第 13-27-295 号
2013 年 7 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 止まらないウェブ改ざん！ 」
～　ウェブサイトの管理の再検討を！　～

IPA セキュリティセンターは前回 2013 年 6 月の呼びかけにおいて、「ウェブ改ざん」の被害が多発していることをうけ、主にシステム管理者向けに総合的な対策を取るよう呼びかけました。しかしその後も様々な企業のウェブサイトが改ざんされる報道が相次いでいます。 今後も被害の連鎖が続くものと思われ、喫緊の対策が求められるため、再度呼びかけを行います。

2009 年から 2010 年にかけて頻発した「ガンブラー」（図 1-1）では、パソコンの脆弱性の悪用によりウイルス感染し、クライアントパソコンから FTP のアカウント情報を窃取されたことが原因で「ウェブ改ざん」されました。しかし昨今の「ウェブ改ざん」は、ウェブサーバーの弱点を攻撃してウェブ改ざんを試みる手口が加わったことが特徴です。ウェブサーバーで安易な FTP パスワードを設定していたために推測等でパスワードが破られたり、ウェブサーバーの脆弱性が悪用されてサーバーに侵入されたりすることで、改ざんされてしまいます（図 1-2 参照）。

脆弱性を解消していないパソコンで、改ざんされたウェブサイトを閲覧すると、ウイルスに感染するのはもちろんのこと、そのパソコンでウェブサイト管理を行っていた場合は、当該ウェブサイトが新たに改ざんされ、被害の連鎖につながります。

このように「ウェブ改ざん」のためにクライアントパソコンを狙うだけでなく、ウェブサーバーも標的としていることから、今回の呼びかけでは、IPA に寄せられた実際の事例を解説するとともに、ウェブサイト管理者向けにウェブサイトの改ざんを免れる対策を整理して紹介します。

(1) ウェブ改ざんの事例

IPA に届けられた、ウェブ改ざんに関する事例を次に示します。

【事例 1】ウェブサーバーの脆弱性を悪用した攻撃

被害に気付いたきっかけ	クレジットカードを入力する画面に文字化けが発生、原因を探るため運用委託社に調査を行ってもらったところ、ウェブが改ざんされ、バックドアツールが設置されている事を発見した。
被害内容	ウェブページの改ざん、クレジットカード情報などの流出
原因	ウェブアプリケーション（Apache Struts 2）のバージョンが古かったため、脆弱性を悪用された。

【事例 2】ウイルス感染による、管理パソコンからのパスワード漏えい

被害に気付いたきっかけ	複数のウェブサイトを、それぞれ別のレンタルサーバー業者のサーバーで運用していたが、その一方の業者からコンテンツファイルのタイムスタンプが変だとの連絡を受け調査したところ、ウェブが改ざんされていることを発見した。その後、もう一方のレンタルサーバー上のサイトも確認したところ、同様に改ざんされていた。
被害内容	ウェブページの改ざん

原因	管理パソコンにウイルスが感染し、パスワードが漏えいしていた可能性が高い。それは十分な強度を持つ管理者パスワードをサイト毎に設定しており、しかもログイン失敗のアクセスログが無く、いずれのアクセスも一回でログインできていたことから、正しいパスワードが窃取されたことによる、なりすましログインだったと推測できる。

【事例 3】脆弱な管理者パスワードを悪用した攻撃

被害に気付いたきっかけ	ウェブサーバーを経由したメール送信が行われているとの連絡があり、調査を行ったところウェブページが改ざんされ、同時に不審なプログラムファイルがサーバー上にアップロードされていた。このプログラムによって、不正にメールが送信されていた。
被害内容	ウェブページの改ざん、迷惑メールの送信
原因	コンテンツマネージメントシステム（MODX）に、容易に推定できる管理者パスワードを設定していたため、これを悪用されウェブページの改ざんと不正プログラムのアップロードが行われた。

【事例 4】管理者アカウントの共有

被害に気付いたきっかけ	ウェブサーバーのメンテナンス日以外にウェブページの更新が行われていた。調査を行ってみるとウェブページが改ざんされていた。
被害内容	ウェブページの改ざん
原因	ウェブサーバーの管理画面へのアクセスに必要なアカウントとパスワード情報を社内管理者とメンテナンス業者で共有していた。これが何らかの要因により外部に漏えいしたものと思われる。

IPA への「届出」に加えて「相談」や「情報提供」などから、ウェブサイト改ざんの流れを整理してみると、“閲覧したらウイルスがダウンロードされ、改ざんされた”という事例の報告が目立っています。近年のウェブサイト改ざんの増加は、先述した「ガンブラー」の手口（図 1-1）（※1）が応用されています。最近はこれに加えて「ウェブサーバーの脆弱性」や「簡単な FTP パスワード」を“攻略”して侵入するという改ざん手口が加わっていることによって、ウェブ改ざんの連鎖が拡大しています（図 1-2）。

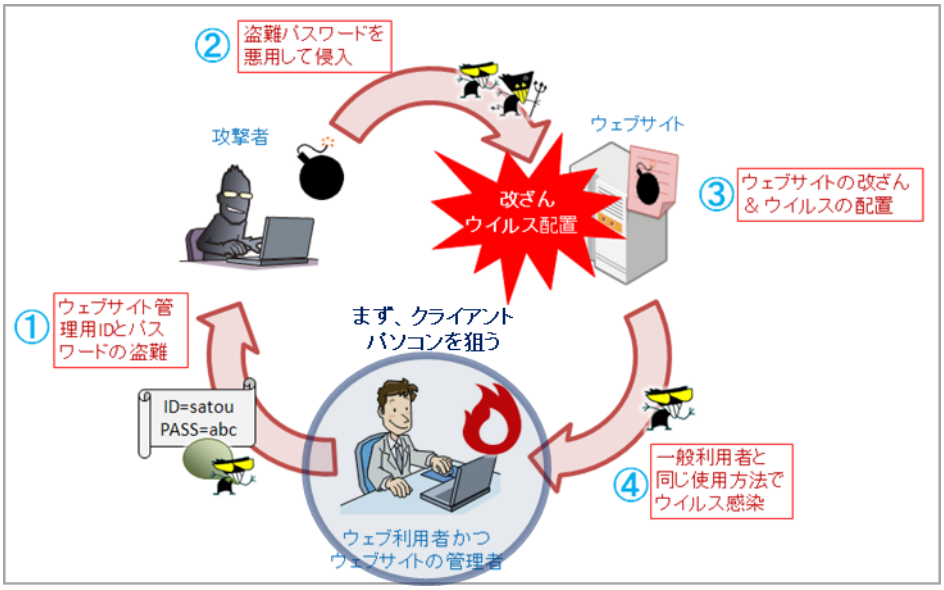

図 1-1：「ガンブラー」の手口によるウェブ改ざん拡大の“連鎖”

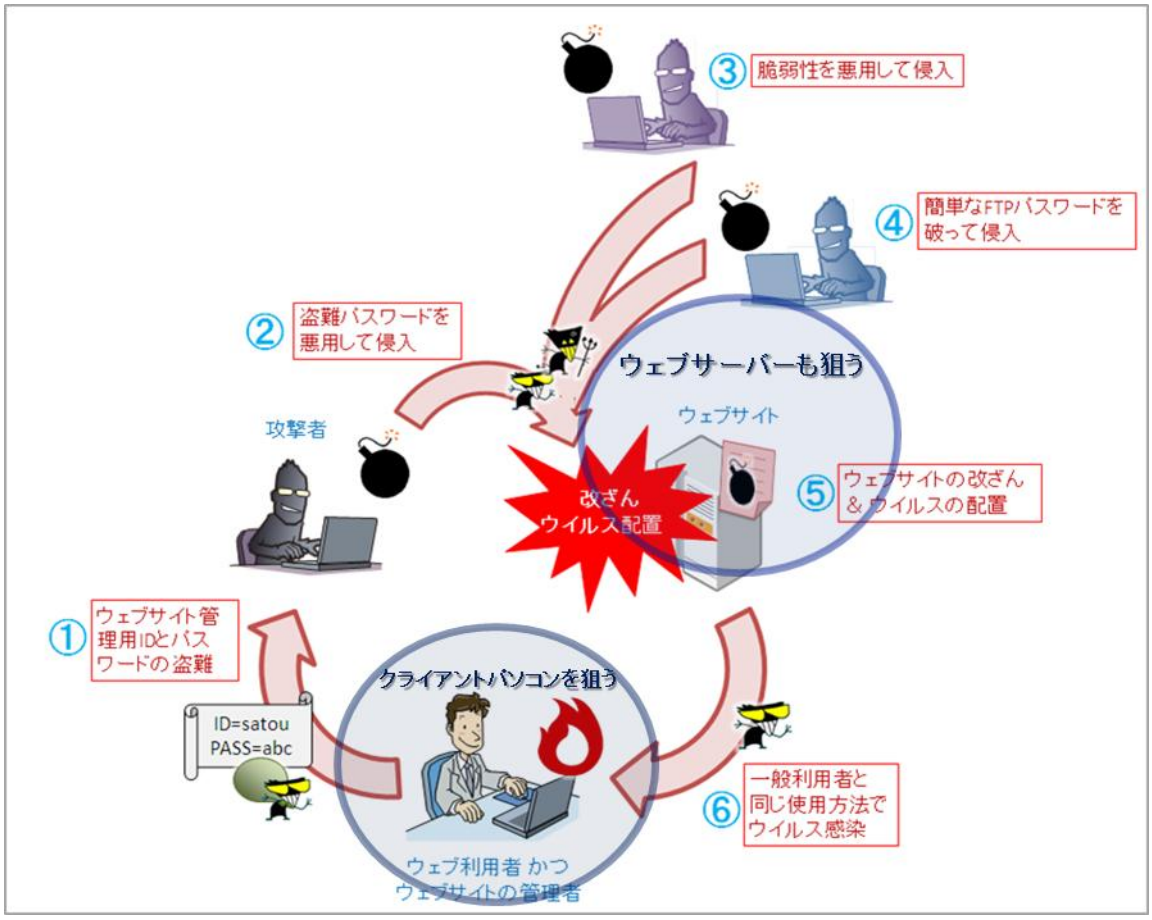

図 1-2：新たな手口の追加による“ウェブ改ざん連鎖”の拡大

（※1）2010 年 1 月の呼びかけ「 "ガンブラー" の手口を知り、対策を行いましょう 」1-(3)参照
http://www.ipa.go.jp/security/txt/2010/02outline.html

(2) ウェブ改ざんへの対策

繰り返しになりますが、ウェブサイトが改ざんされた主な原因として、「ウェブサーバーの脆弱性への攻撃」「ウェブサイト管理用パソコンがウイルスに感染することによる FTP パスワード漏えい」「サイト管理用 FTP パスワードを容易に推測できてしまうよう不適切に設定」「サイト管理者の FTP アカウントの複数人による共有」などがあげられます。以下、各々についての対策を示します。

【1】ウェブサーバーの脆弱性に対する攻撃への対策

① サーバーの脆弱性対策を実施する

サーバーにも脆弱性対策は必須です。サーバー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。

IPA では、サーバーにインストールされている主要な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（サーバー用）」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（サーバー用）
http://jvndb.jvn.jp/apis/myjvn/vccheckserv.html

また Joomla！、WordPress などの CMS を利用している場合、プラグイン（拡張機能）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りますので、それらすべてを最新にしてください。

【2】ウェブサイトを管理しているクライアントパソコンのウイルス感染による FTP パスワード漏えい向け対策

① 管理用パソコンの OS と各種プログラムを常に最新状態にし、パソコンの脆弱性を解消する

管理用パソコンの 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。Java、Flash Player、Adobe Reader は特に狙われやすいため、更新通知が画面に表示されたら速やかに更新してください。またプログラムの自動更新機能を利用すると都度更新が不要となり便利です。

（ご参考）
2012 年 6 月の呼びかけ「ソフトウェアの自動更新を利用しましょう！」
http://www.ipa.go.jp/security/txt/2012/06outline.html
よくある相談と回答(FAQ)：Windows XP のサポート終了
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/

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の閲覧を防止する機能（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れば、感染を未然に防げることがあります。

③ パーソナルファイアウォールを導入する

ウイルス感染に気がつかず、不正プログラムがインストールされてしまった場合に備えて、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導入により、自分が許可したプログラムだけを外部に通信可能とし、ウイルスや不正プログラムが行う通信を遮断することで、感染してしまっても外部に情報が漏えいすることを水際で防ぐことができます。

④ ウェブサイトを更新する場所を限定する

万が一、FTP アカウントの情報が漏えいしてしまっても、ウェブサイトを更新する場所を限定することで、ウェブページの改ざん被害を低減させることができます。ウェブページ更新でサーバー接続する IP アドレスを組織内に限定し、それ以外の IP アドレスからの接続を許可しないようにします。また、ネットワークやサーバーの構成を見直すことも検討してください。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は、VPN を導入するなどして、更新できる場所の限定を検討してください。

⑤ ウェブサイト更新専用パソコンを使用する

ウェブサイトを更新するための専用パソコンの導入を検討してください。このパソコンではウェブサイト更新作業のみを行い、“作業と無関係なサイトを閲覧しない”、“セキュリティ対策が不十分な USB メモリを挿入しない”といったルールの設定が必要です。これによってウイルス感染の可能性を低減することができます。

【3】 サイト管理者用 FTP のパスワードが漏洩しないための対策

① 適切なアカウント設定

ウェブサイト更新用のアカウント情報が適切に設定されているか、下記の点を確認してください。

- 使用するパスワードは、“アルファベットの大文字と小文字”、“数字”、“記号” を組み合わせた文字列にしてください。
- 少なくとも 8 文字以上のパスワードにしてください。
- 辞書に載っているような単語や人名を、パスワードに含めないでください。

【4】サイト管理者用 FTP アカウントの不適切な利用による漏洩への対策

① アカウントを共有しない

複数の者で管理者アカウントやパスワードを共有していると、アカウント情報などが漏えいする確率が高くなります。また実際に「ウェブ改ざん」が行われた場合、その手法や原因の究明が非常に困難になる場合があります。管理者アカウントやパスワードは共有せず、またこれを与えた者には「管理責任」があることを周知徹底してください。

(3) ウェブ改ざんの被害発生時の対処

ウェブサイトが改ざんされてしまった場合、ウェブサイト管理者は被害者であると同時に、ウェブサイト利用者に対する加害者となってしまう可能性があります。被害の拡大を防ぐために、次に示すような対応が求められます。

① まず初めに行うべきこと

まず初めに行うことは、早急にウェブサイトの公開を停止することです。同時に FTP のパスワードの変更も行ってください。このとき、これまでウェブサイトの管理に利用していたパソコンには、FTP アカウント情報を窃取するウイルスが感染している可能性があるため、別のパソコンから操作することを勧めます。

同時に、別のウェブサイトを立てるなどして、ウェブサイト利用者に対して調査状況の説明や、問い合わせ用窓口を設けるなど、随時情報提供に努めてください。

② 改ざん箇所の洗い出しなどの調査

上記の対応を行ったのち、保管しておいたクリーンなファイルとウェブサーバー上のファイルの比較などの方法で、全ての改ざん箇所の洗い出しを行ってください。また、同じパソコンで管理しているウェブサイトが複数ある場合、他のウェブサイトにも改ざんが及んでいる可能性があるため、必ず全てのウェブサイトのファイルを確認してください。

また、改ざん期間などを把握するため、改ざん箇所ごとに FTP のアクセスログの確認などを行なって、被害状況などの調査を行ってください。

③ ウェブサイトを再公開する場合

上記の対応で全ての改ざん箇所の修正を行った上で、ウェブサイトの公開を再開する場合、必ずウェブサイト利用者への改ざんの事実の告知も掲載してください。ウェブサイト再開の際には、判明した範囲で、次に示す情報を告知することを勧めます。

(a) 改ざんの事実の説明
(b) 改ざんされていた箇所
(c) 改ざんされていた期間
(d) ウェブサイト利用者が改ざんされていた箇所を閲覧した場合に想定される被害（ウイルス感染など）の説明
(e) ウイルスのチェック方法の説明（必要に応じてオンラインスキャンサイトの紹介など）
(f) 問い合わせ窓口の連絡先

（ご参考）
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

また参考として、セキュリティ関連の組織や企業が提供している、無料でウイルスチェックができるウェブサイトを紹介します。

（ご参考）
「ボットの駆除対策手順」（サイバークリーンセンター）
https://www.ccc.go.jp/flow/
「オンラインウイルススキャン」（カスペルスキー）
http://www.kaspersky.co.jp/virusscanner/
「オンラインスキャン」（トレンドマイクロ）

http://www.trendflexsecurity.jp/housecall/
「Virus Removal Tool」（ソフォス）
http://www.sophos.com/ja-jp/products/free-tools/virus-removal-tool.aspx
「エフセキュア オンライン スキャナ」（エフセキュア）
http://www.f-secure.com/ja/web/home_jp/online-scanner

ウェブサイト改ざんの被害に遭った際は、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します。

（ご参考）
不正アクセスに関する届出について
http://www.ipa.go.jp/security/ciadr/index.htm

(4) こんなときは…

IPA 情報セキュリティ安心相談窓口では、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 情報セキュリティ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。

	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

※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