

【今月の呼びかけ】

「"ガンブラー"の手口を知り、対策をいしましょう」

「有名企業や公共機関のウェブサイトが改ざんされ、そのサイトを閲覧した利用者がウイルスに感染した可能性がある」という報道が2009年末から相次いでおり、IPAへも多くの相談や問い合わせが寄せられています。一般的に「ガンブラー」と呼ばれているこの一連の攻撃は、「ウェブサイト改ざん」と「ウェブ感染型ウイルス（ウェブサイトを開覧するだけで感染させられてしまうウイルス）」を組み合わせ、多数のパソコンにウイルスを感染させようとする**手口（攻撃手法）**の一種を指します。

ここでは、「ガンブラー」がどのような手口であるのかを説明し、その影響や対策について示します。「ガンブラー」では、近年インターネットで悪用されている様々な攻撃手法が組み合わされているため、これらへの対策を行うことで、「ガンブラー」以外の脅威に対しても有効な防御策となります。インターネットを利用している全ての人に危険が生じていることを認識し、十分な対策をいしましょう。

(1)「ガンブラー」の概要

「ガンブラー」とは、特定のウイルスを指すものではなく、悪意のある者（攻撃者）が複数の攻撃手段を併用し、多数のパソコンに様々なウイルスを感染させようとするために使う、**一連の手口**のことです。このため、「ガンブラー」について理解するには、攻撃者、被害者、そしてウイルスといった個々の要素だけでなく、それらがどのように関係しているかを知る必要があります。「ガンブラー」の手口による攻撃の全体図を、図1-1に示します。

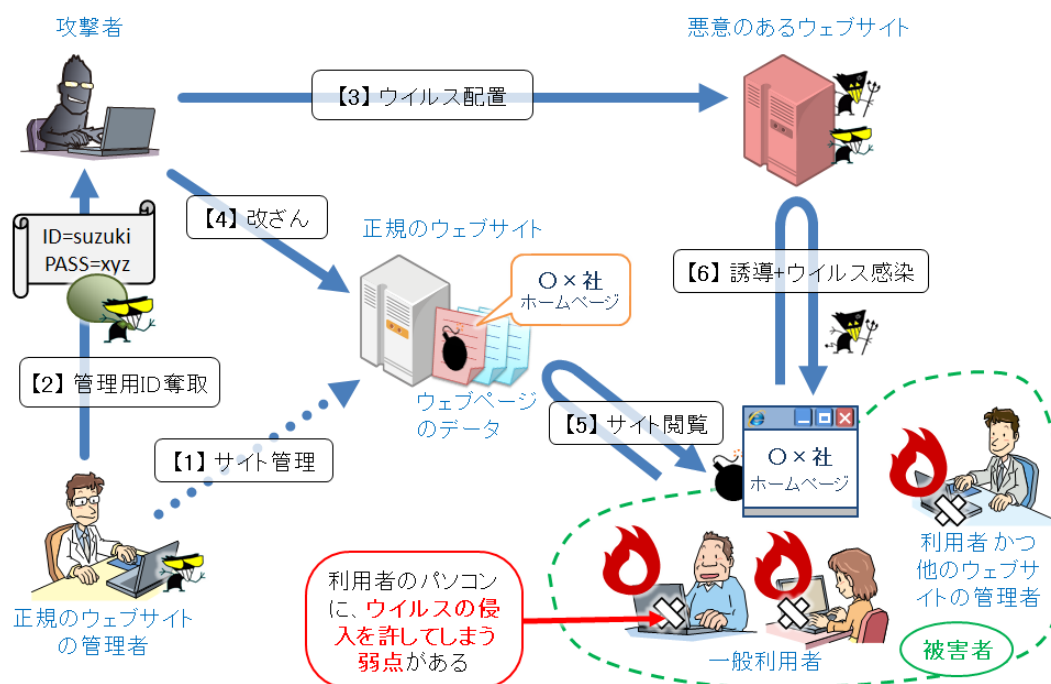


図1-1: 「ガンブラー」の手口による攻撃の全体図

詳しくは後述しますが、この手口によって利用者がさらされる危険は、主に次の3点です。

- セキュリティ対策が不十分なパソコンでは、ウェブサイトを開覧するだけでウイルスに感染させられてしまい、かつ、ウイルスに感染したことが見た目には全く分からない場合がある
- 有名企業のウェブサイトが攻撃に使われる場合があるため、「不審なウェブサイトを開覧しない」といった回避策が有効とならず、日常的に利用しているウェブサイトが突然危険なウェブサイトとなる可能性もある
- 感染させられるウイルスは特定のものではなく、攻撃者がコントロールできるため、どのようなウイルスに感染させられるか分からない

このように、「ガンブラー」による攻撃は、インターネットを利用している全ての人に危険を及ぼしています。以降、この手口について詳しく説明し、利用者として施すべき対策を示します。

(2)「ガンブラー」の手口の詳細

本項では、「ガンブラー」の手口を詳しく説明します。なお、この手口は細かく分類すると様々なパターンがあり^(*)、また、現在も巧妙化を続けています。ここでは、2009 年末から流行中の典型的な手口を例として紹介します。以降、「【1】」などと表記した場合、図 1-1 の図中に対応していますので、図を参照しながら読み進めてください。

(*) 実際は、この手口のうち 2009 年 3 月から 5 月に流行したものに「ガンブラー (Gumblar)」という名前が付けられ、以降は手口の巧妙化に合わせて別の名前が付けられてきました。最近では、これらの手口を総称して「ガンブラー」や「ガンブラーの亜種」などと呼ばれています。

【1】 正規の管理者によるウェブサイトの管理

この【1】は「ガンブラー」の手口の一部ではありませんが、背景として説明します。

インターネット上のウェブサイトは、そのウェブサイトの管理者によって管理・運営されており、そこにはウェブページ（画面）のデータが複数格納されています。ウェブサイト管理者は、ウェブページの作成・更新を行う際、ウェブサイト管理用の秘密の ID とパスワードを使うことで、他者が勝手にウェブページを書き換えることが出来ないようにしています。

【2】 正規のウェブサイトの管理用 ID とパスワードの奪取

【2】～【4】は、「ガンブラー」の手口で行われる、悪意のある攻撃者による下準備です。

まず、攻撃者は何らかの方法で、正規のウェブサイトの管理用の ID とパスワードを、そのウェブサイトの管理者から盗みます。手段として、情報を盗み出すタイプのウイルス（スパイウェア）等が使われていることが推測されます。

【3】 悪意のあるウェブサイトへのウイルス配置

攻撃者が悪意のあるウェブサイトを作成^(*)し、そこに複数のウイルスを配置します。攻撃者は、いつでもこれを任意の（例えば新種の）ウイルスに入れ替えることができると考えられます。

(*) 悪意のあるウェブサイトは、追跡されることを難しくするために、様々な工夫がなされた上で構成されています。

【4】 正規のウェブサイトの改ざん

下準備の最後として、【2】で入手した「ウェブサイト管理用の ID とパスワード」を使い、攻撃者はウェブサイトの管理者になりすまし、格納されているウェブページのデータを不正に改ざんします。具体的には、攻撃者はウェブページの中に「このページを開いたパソコンを、悪意のあるウェブサイト（【3】で用意したもの）へ誘導する」という**悪意のある命令**を埋め込み、罠を仕掛けます。

【5】 改ざんされたウェブサイトの閲覧

【5】と【6】では、パソコン利用者側が、ウェブサイトを訪問してウイルスに感染させられてしまうまでの動作を説明します。

まず、利用者がいつものように正規のウェブサイトを開きます。この時、パソコン上のブラウザ（インターネット閲覧ソフト）は、目的のウェブページのデータを取得し、画面を表示します。

今回の場合、そのウェブページは**攻撃者により【4】で改ざんされたもの**です。たくさんあるウェブページのうち、**どのページが改ざんされているかを、利用者が事前に知ることはできません**。

パソコンの画面では、**見た目には改ざんされる前との違いがないウェブページが表示された状態**となりますが、**挙動に変化のないまま、【4】でウェブページの中に仕掛けられた悪意のある命令が、ブラウザの中で動作を始めます**。

【6】 悪意のあるウェブサイトへの誘導とウイルス感染

続いて、**悪意のある命令**により、利用者への確認なしに、ブラウザは悪意のあるウェブサイトへ誘導（勝手に接続）されます。そして、最初のウイルスのファイルがダウンロードされます。

この最初のウイルスは、正確には「攻撃コード」と呼ばれるもので、直接パソコンに被害を与えるものではなく、まずパソコンの「ウイルスの侵入を許してしまう弱点」を悪用して侵入することを目的としたものです。ブラウザは、「攻撃コード」を含むファイルを開こうとします。それが動画ファイルであれば動画再生用のソフト、といったように、ブラウザ本体以外の機能が使われることもあります。この時、パソコン内のOS、ブラウザ、その他のアプリケーションソフトに「ウイルスの侵入を許してしまう弱点」が存在すると、そこを突かれて（悪用されて）ウイルスに侵入されてしまいます。

侵入に成功すると、そのウイルスは、悪意のあるウェブサイトから更に別のウイルスをダウンロードし、パソコンに感染させるという動作をします。【3】で示した通り、攻撃者はウイルスを随時入れ替えることができるため、利用者が最終的にどのようなウイルスに感染させられるかは分かりません。

ここまでの一連の動作は、多くの場合パソコンの画面への変化がないまま行われるため、利用者が危険に気付くことは難しいと思われれます。

▼ 「ウイルスの侵入を許してしまう弱点」について

改ざんされたウェブサイトを開覧してしまい、【5】と【6】で示したような動作が行われたとしても、基本的にOSやブラウザをはじめとする様々なソフトウェアは安全性が考慮されており、ウイルスに感染させられることはないように作られています。しかし、ソフトウェアにはセキュリティ上の不具合が後から発見されることがあり、それが「ウイルスの侵入を許してしまう弱点」となる場合があります。この弱点のことを、「脆弱性（ぜいじゃくせい）」と呼びます。

「ガンブラー」の手口では、【2】～【4】の攻撃者による下準備と、【5】と【6】での利用者による改ざんされたウェブサイトの閲覧に加え、「利用者のパソコンに脆弱性がある」ということが前提条件となっており、これら全てが揃ったときに攻撃が成立します。

最新版でないソフトウェアには脆弱性が残っている可能性があるため、古いものを使い続けるのは危険です。(5)で後述する対策を実施し、ソフトウェアを最新に保ちましょう。

(3) 改ざんサイト増加のサイクル

本項では、「ガンブラー」による攻撃が拡大し、ウェブサイトの改ざんが相次いでいる理由について説明します。

図 1-1 の右下の被害者たちの中に「利用者 かつ 他のウェブサイトの管理者」がいます。この被害者は、ウェブサイトを管理するためのパソコンを使って、様々なウェブサイトの閲覧も行っています。攻撃者は、こういった利用者が罠にかかることを想定した上で、「ウェブサイトの管理用の ID とパスワードを盗み出すウイルス」を「悪意のあるウェブサイト」に配置しています。

【2】では、“何らかの方法で” 攻撃者がウェブサイトの管理用の ID とパスワードを盗み出す、と説明しましたが、その方法自体も「ガンブラー」の手口の一部となっていると言えます。これにより、攻撃者は更に別のウェブサイトの管理者になりすますことが可能となるため、次々とウェブサイトを改ざんすることで、攻撃範囲を広げているものと考えられます（図 1-2）。

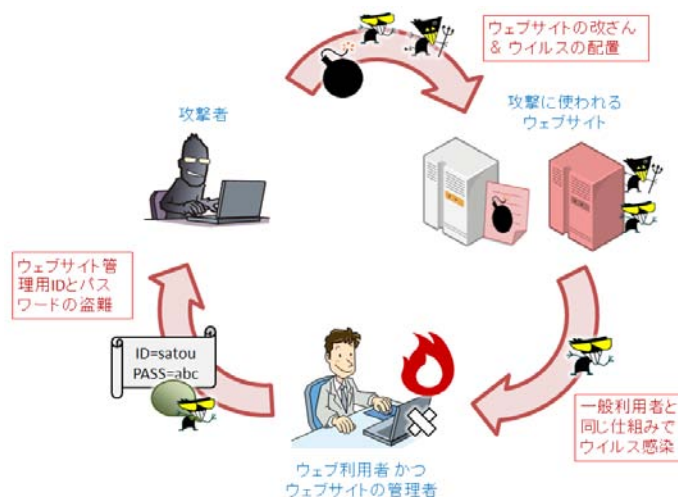


図 1-2 : 「ガンブラー」の手口による攻撃の拡大のサイクル

▼ まとめ

以上の (2) (3) で示した「ガンブラー」による攻撃の特徴をまとめると、次の 3 点となります。

- 攻撃者が、正規のウェブサイトの管理用 ID とパスワードを盗み、正規のウェブサイトを改ざんして罠を仕掛ける
- セキュリティ対策が不十分なパソコンを狙い、改ざんされたウェブサイトを閲覧するだけで感染させるウイルスを攻撃に使用する
- 攻撃者はウイルスを使用して更に別のウェブサイトの管理用 ID とパスワードを盗み、改ざんサイト（攻撃範囲）を拡大していく

(4) 被害の内容

前述した通り、「ガンブラー」は「ウイルスを感染させるための手口」であり、最終的に利用者のパソコンがどのようなウイルスに感染し、どういった被害が発生するかは分かりません。また、使われるウイルスも時間と共に変化しています。

現在のところ、次に挙げるウイルスに感染した事例が報告されています。

- 偽セキュリティ対策ソフト（ウイルスが発見されたという偽の表示を行い、駆除するために偽セキュリティ対策ソフトの「有償版」の購入を迫るウイルス）
- ウェブサイト管理用の ID とパスワード（ftp のアカウント情報）を盗み出すウイルス

また、次のような症状がある場合、原因が「ガンブラー」とは限りませんが、ウイルスに感染している疑いがあります。

- Windows Update、Microsoft Update が実行できない
- 各種セキュリティソフトのベンダー（開発、販売会社）のウェブサイトへ接続できない
- ウイルス対策ソフトのウイルス定義ファイル（パターンファイル）を最新のものに更新できない

近年流行しているウイルスとしては、パソコン内のデータを破壊するタイプだけではなく、個人情報やオンライン banking / オンラインゲーム等の ID とパスワードを盗み出すウイルス（スパイウェア）、パソコンを乗っ取って遠隔操作を可能とするウイルス（ボット）などがあります。今後、これらのウイルスの拡散のために「ガンブラー」の手口が使われる可能性があり、注意が必要です。

ウェブサイトを運営している企業や管理者にとっては、運営しているウェブサイトを閲覧した利用者に対して、ウイルス感染の被害を与える加害者となってしまうことで、信頼を損なうおそれがあります。十分な対策を実施し、被害の拡大防止に努めてください。

(5) 対策

「ランバラー」は、複雑な手口により利用者をウイルスに感染させるものですが、一連の手口の中で使われている個々の攻撃手法は、特に新しいものではありません。従来と変わらず、基本的なウイルス対策を漏らさず実施していくことで、十分防御していくことが可能です。ここでは、その対策を改めて示しますので、確実に実施してください。

(i) 脆弱性の解消

【6】で説明した通り、「ウェブ感染型ウイルス」はパソコン内にある「**ウイルスの侵入を許してしまう弱点**」、すなわち脆弱性を悪用して侵入してきます。従って、この脆弱性を解消することが、重要な対策の一つです。

脆弱性は、OS (Windowsなど)、ブラウザ (Internet Explorerなど)、その他のアプリケーションソフト、それぞれに存在する可能性があります。パソコンに導入しているソフトウェアについては、できる限り全てを最新版に更新し、脆弱性を解消しましょう。

ソフトウェアの更新の方法について、次に補足します。

- Windows (OS 本体)、Internet Explorer、Microsoft Office (Word や Excel) の更新
 - パソコンの設定によっては「自動更新」の機能がオンになっており、その場合は自動的に最新版に更新されます。手動で更新を行う場合は、「Windows Update」または「Microsoft Update」を使用します。詳しくは、下記の Microsoft 社のウェブページを参照してください。
 - (ご参考) 「Microsoft Update 利用の手順」(Microsoft社)
http://www.microsoft.com/japan/security/bulletins/j_musteps.msp
- 「MyJVN バージョンチェッカ」による確認
 - IPA では、Adobe Flash Player など、ウイルスによって狙われることが多いソフトウェアについて、それらがパソコンに導入されているか、および最新版となっているかをチェックできるツールを公開しています。詳しくは、下記の「MyJVN バージョンチェッカ」のウェブページを参照してください。
 - (ご参考) 「MyJVN バージョンチェッカ」(IPA)
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>
※ 2010 年 2 月現在、Windows XP と Vista に対応しています。
- その他のソフトウェア
 - ソフトウェアの更新の方法は、それぞれ異なります。自分のパソコンに導入されているソフトウェアを把握し、定期的に更新を行うことが理想です。パソコン初心者がすぐに実施するのは難しいのが現状ですが、自己防衛のために身に付けていきましょう。
 - IPA では、一般利用者の多いソフトウェアに脆弱性が発見された場合、注意喚起を行っています(下記の「緊急対策情報・注意喚起 一覧」のウェブページを参照)。注意喚起が行われた場合は、自分のパソコンに該当するソフトウェアが入っているかを確認し、対応しましょう。
 - (ご参考) 「緊急対策情報・注意喚起 一覧」(IPA)
<http://www.ipa.go.jp/security/announce/alert.html>

(ii) ウイルス対策ソフトの導入

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入してしまったウイルスを駆除することができます。近年のウイルスは、パソコンの画面の見ただけでは感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、危険なウェブ

ブサイトを閲覧しようとした時にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。なお、「ガンブラー」の手口に対して、ウイルス対策ソフトは、次のタイミングで効果を発揮することが期待できます。

- 改ざんされたサイトを開こうとした時（【5】）に、それを阻止する
- 悪意のあるウェブサイトからダウンロードされる「攻撃コード」（【6】）の侵入を阻止する
- 「攻撃コード」に続いてダウンロードされるウイルス（【6】）の侵入を阻止する
- ウイルスに感染してしまった場合でも、後日、発見・駆除する

(iii) 「ゼロデイ攻撃」への対策

脆弱性の解消について (i) で説明しましたが、「脆弱性が発見されてから、その修正プログラムが公開されるまでの期間」は、脆弱性を解消できない状態となります。この期間を狙う攻撃を「ゼロデイ攻撃」と呼びます。「ゼロデイ攻撃」に対しては、脆弱性を解消できないため、できる限りの「回避策」を取ることで対応します（「回避策」は、問題となっているソフトウェアによって様々です）。

「ガンブラー」の手口でも、一部で「ゼロデイ攻撃」が行われたことが確認されています。「ゼロデイ攻撃」についての詳細は、下記のウェブページを参照してください。

（ご参考）

「修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について」（IPA）

<http://www.ipa.go.jp/security/virus/zda.html>

(iv) ウイルスに感染してしまった、あるいは感染しているか不安な場合

既にウイルスに感染してしまったか、感染しているかどうか分からないといった場合、取りうる手段は、ウイルス対策ソフトによる検査と駆除です。ウイルス対策ソフトが発見できない、未知のウイルスに感染している場合もありますが、数日後にはウイルス対策ソフト側が対応し、発見できるようになる可能性があります。

明らかに動作がおかしく、またウイルス対策ソフトによるウイルスの発見や駆除ができないような場合、確実にウイルスを除去する最終的な手段としては、パソコンの初期化（購入時の状態に戻す）を行うしかありません。

ウイルスに対しては、感染してからの対処ではなく、感染を予防する (i) ～ (iii) の対策が重要です。

(v) ウェブサイト管理者としての対策

ウェブサイト管理者については、上記以外にも講じるべき対策があります。詳しくは、下記のウェブページを参照してください。

（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」（IPA）

<http://www.ipa.go.jp/security/topics/20091224.html>