

ガンブラーウイルスについて

【重要】不正アクセスによる WEB 改ざん被害について

更新：2010年2月18日

平素より社団法人東京都柔道接骨師会のホームページをご覧いただき、誠にありがとうございます。
近頃、ガンブラー(Gumblar、別名 GENO ウイルス)と呼ばれるウイルスによりホームページの FTP 情報が盗まれ、WEB が改ざんされるという事象が発生しております。

以下の案内をご一読いただき、セキュリティ対策を実施いただきますようお願いいたします。

ガンブラー等のウイルスによる被害事例

FTP による不正なアクセスを受け、スクリプトタグが埋め込まれる事象を複数確認しております。
その一つの事象は、以下のような経緯で発生していると推測されます。

1. ウイルス感染したサイトを閲覧し、利用していた PC がウイルスに感染。
※一般的な通販サイトから感染が広まっているという情報があります。
2. ウイルスに感染した環境の PC から、FTP アカウント・パスワードなどの情報が第三者に流出。
3. 第三者が、入手した FTP アカウント・パスワードにてサーバへ FTP 接続。
4. WEB サイトにて利用している HTML や PHP などのファイルをダウンロード。
5. ダウンロードしたファイル内に、ウイルスをダウンロードさせようとするスクリプトタグを埋め込みサーバへアップロード。
6. 改ざんされた WEB ページへアクセスした PC が、ウイルスに二次感染。

上記のような事例は、関連機関でも案内されております。ご確認ください。

- 独立行政法人情報処理推進機構 (IPA)
【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>

実施していただきたいセキュリティ対策

閲覧者ご自身での対策

ご利用の PC のセキュリティ対策を万全にし、ウイルス感染していないことを確認してください。

- Windows Update を実施する。
- セキュリティ対策ソフトを利用する。
- ウイルス定義ファイルを更新し、ウイルススキャンを定期的実施する。
- Adobe Reader と Flash Player を最新版にする。

【ウイルスに感染した場合の挙動】

- 海外のサーバからウイルスファイルをダウンロードしようとする。
- コマンドプロンプトやレジストリエディタが起動しなくなる。
- Adobe 関係のバージョンアップ要求が頻繁に起こる。
- CPU の稼働率が高くなる。

【ウイルスに感染した場合の対処】

- 対象の PC のネットワーク接続を停止する。 ※社内、家庭内感染を防ぐため
- ウイルス感染してしまった PC は、OS をクリーンインストールする。

当ホームページのセキュリティ対策

- FTP パスワードは定期的に推測されにくいものに変更。
- 不必要な FTP アカウントの削除。
- FTP アクセス制限機能を利用。
- 管理担当者の PC の定期的なウイルススキャン。

社団法人 東京都柔道接骨師会