

お客様各位

<p>Gumblar（ガンブラー）を含む Web 感染型ウイルスに感染確認した場合の ルールと対処方法・対応体制に関して</p>
--

クレバード株式会社
代表取締役 稲田 宣稚

現在、企業のホームページを中心に、ホームページを改竄（かいざん）し、閲覧者のパソコンに感染が広がる Web 感染型コンピューターウイルス「Gumblar（ガンブラー）」が猛威を振るっています。現在のところ、詳しい正体は明らかになっておらず、感染したパソコンなどの大きな被害は報告されていませんが、アクセスしたホームページも見た目には大きな改竄が発見し辛いいため、閲覧者はほとんど気づかずに感染が拡大しております。

前述通り、詳しい正体（ウイルス作成のアクセス元特定や亜種への発展等）が明らかになっていないため、対処方法もウイルス対策ソフトだけでは対応出来ないとの意見も出ています。

弊社では、感染拡大する GENO ウイルスに対応すべく、感染確認した場合の対処ルールを下記の通り策定いたしました。今後は下記ルールに則り、即時対応するグループを編成し、より信頼性の高い体制を整えていきますのでご協力の程宜しくお願いいたします。

対応要領

1. 弊社において Web 改ざんを発見する・確認をする・連絡を受ける。クライアント様からの連絡を受けた場合は<5>以降の対応を行う旨説明を行います。
2. 社員全員への連絡を行い、以下の処理を行う体制作りを行なう。
3. サーバ管理委託会社に感染の事項を連絡。下記処理を行う旨電話連絡。*¹
4. 感染を確認したクライアント様へ感染及び改ざんされている旨をお電話にて連絡、今後の対処方法に関して下記の通りの工程を報告致します。同時にクライアント様 PC 全てのウイルスチェックの依頼を行ないます。
5. FTP を含む各種管理パスワードを変更。*¹
6. 弊社内 PC における感染の有無を確認。
7. 弊社ホームページ最新情報内に下記の通り通知を行う。
8. 弊社内ネットワークより、他の PC に感染を広げないような接続環境から、WindowsUpdate 及びウイルス対策ソフトのアップデートを行った PC より FTP 接続を行い、以後この PC より全ての対応策を行なう。
9. FTP サーバのログ・更新日時等からアクセス元を出来る限りを探る。
10. ホームページ情報を全ダウンロード。
11. FTP 上ファイルを全部削除。
12. HP 公開一時停止の旨を記載した html ファイルをアップ。

13. クライアント先に上記作業が完了した旨を連絡。今後のアップ予定に関してはこの時点では未定となります。
14. サーバ管理委託会社に上記処理を行った旨連絡。^{※1}
15. 同一サーバにおける他 Web サイトの感染の有無を確認。
16. クライアント様と相談の上、感染前のデータをアップするスケジュールを決定する。

^{※1} 弊社対応グループ責任者による作業とします。

以上