2010 年 1 月 8 日

株式会社ヒューマネージ
コンプライアンス統括室

「Gumblar」ウイルスに対する弊社セキュリティ管理策について

弊社は、情報セキュリティ基本指針に則り、弊社の管理する情報資産を、その周囲を取り巻く脅威から確実に保護するために、適切な情報セキュリティ管理策を確立し、実施しております。

このたびの「Gumblar」ウイルス感染によるホームページの改竄につきましても、弊社のサービス環境下では問題は発生しておりません。

「Gumblar」ウイルスに対する弊社のセキュリティ管理策は以下の通りです。

記

1. はじめに：「Gumblar」ウイルスとは

別名 Geno、JSRedir などとも言われるコンピュータウイルス。主に Web を媒介として感染が広がる。ウイルスに感染させるスクリプト（*1）が埋め込まれた Web ページ（感染元） を脆弱性のある PC で閲覧した場合に感染する。PC に感染したウイルスは、その PC の通信を監視し、FTP（*2）による通信が行われると ID とパスワードを抜き出し、その情報を特定のサイトに送信、悪用者はこの情報を利用して、サーバーにアクセスし、サーバー内のファイルを書き換え、Web ページにスクリプトを埋め込み、その Web サイトを感染元にする。PC のユーザーがサーバー等を管理・運用している場合、管理しているサイトにもウイルスが埋め込まれ、被害者が加害者になりうることがある。

（*1）スクリプト　:機械語への変換作業を省略して簡単に実行できるようにした簡易プログラム。

（*2）FTP　　:ファイル転送プロトコル。PC からサーバーへファイルを転送するための仕組み。

2. 「Gumblar」ウイルスに関連するセキュリティ管理策と対応状況

◆ クライアント PC について

PC にインストールされているソフトウェアが、全て最新のバージョンであるように保つ。

（1） ブラウザやそのプラグインなどのソフトウェアのバージョンアップにより最新化するとともに、ソフトウェア製品が発行するセキュリティパッチを適用する。

（2） オペレーティングシステム（OS）に関しても、最新のセキュリティパッチを適用する。

◆ ネットワークについて

不正な通信は、物理的に遮断する。

（1） リスクとして判明しているサイト・通信先（IP アドレス） 情報をタイムリーに入手し、ファイアウォールや Proxy（*）で通信を遮断する。

（*）Proxy　　:企業などの内部ネットワークとインターネットの境にある。ネットワークに出入りするアクセスを一元管理し、内部から特定の種類の接続のみを許可したり、外部からの不正なアクセスを遮断するために用いられる。

◆　サーバーついて

ホームページの制作者やシステムの開発・運用担当者は特に以下の点を留意し徹底する。

(1)　開発用、コンテンツ更新用パソコンの感染状況を確認（問題なし）
　　リスクとして判明している IP アドレスへの通信状況確認とオンラインスキャンの実行

(2)　使用しているソフトウェアが最新の状態であるかを確認（問題なし）

(3)　サーバーのログイン履歴に普段利用しない IP アドレスからのログインがないか確認（問題なし）

(4)　ホームページのコンテンツに不審な文字列が追加されていないか確認（問題なし）

現時点において、上記については全て実施され、適切に管理策がとられていることを確認しております。

以上