中小企業のセキュリティー対策

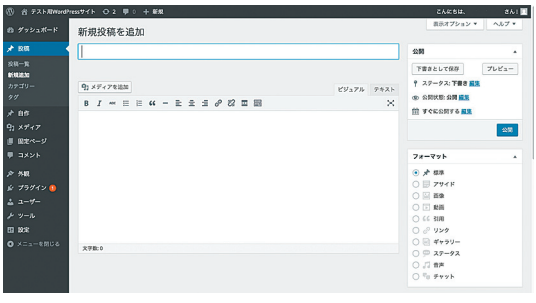
－7－

サイト改ざんで加害者に

CMSを悪用した被害が急増

ウェブサイトは今や企業にとって事業案内や求人、製品・サービスの訴求など多岐にわたる役割を果たし、事業運営に不可欠な存在である。しかし、ウェブサイトが改ざんされると、政治的主張などを掲載されたり、ウイルス配布に悪用されたりする。ウイルス配布に悪用された場合、見た目では分からないようにウイルスやウイルス配布サイトへのリンクをウェブサイトに埋め込まれるため、ウェブサイトの管理者や利用者が気付くのが遅れ、長期間にわたって利用者がウイルスに感染するなどの被害を与え続けることになる。このようにウェブサイト改ざんは、改ざんされた企業が被害に遭うだけでなく、加害者になってしまう深刻な問題である。

近年、被害報告の中でも増えているのが、WordpressやJoomla!などのCMS（コンテンツマネジメントシステム）で構築されたウェブサイトである。CMSを利用すると、ウェブサイトのコンテンツ作成・更新・管理が容易であるため、中小企業でも利用する企業が増えている。しかし、CMSを初期設定のまま利用したために管理画面に不正アクセスされたり、CMSやCMSの拡張機能（プラグイン、テーマ）の脆弱（ぜいじゃく）性が報告されても放置したままで利用したりすることで攻撃を受けていたりする。



Wordpressの管理画面

CMSの脆弱性情報が公表された場合、そのCMSで構築されたウェブサイトは一律で攻撃を受け、改ざんの被害が急増する恐れがある。本年2月に発生したWordpressの脆弱性を突いた攻撃では、脆弱性の公表から2週間で150万件を越えるウェブサイトが改ざん被害にあったと報道されている。

できるだけ早くアップデートを

CMSを用いたウェブサイトの改ざん対策として、以下の対策を実施することを推奨する。

①ソフトウエア（CMSや拡張機能を含む）の脆弱性対策をする

脆弱性情報が公開された場合、できるだけ早くアップデートする必要がある。ただし、利用しているサーバーの契約によっては、ウェブサイト運営者自身でアップデートできない場合があるので、ウェブサイト構築に当たり事前に契約内容を確認しておきたい。

また、ソフトウエアの脆弱性は、CMSや拡張機能だけに限った話ではない。OSやサーバーソフトウエアなどサーバーに組み込まれている全てのソフトウエアの脆弱性情報に注意する必要がある。

②認証を突破されないための対策をする

CMSの管理画面にアクセスするためには、必ず認証画面での認証が必要になる。認証を突破されないために、認証画面をインターネット上に公開しないよう設定を変更したり、認証画面を守るプラグインを導入したり、強固なパスワードを使用するようにしたい。

また、管理者の管理端末（PC）からの認証情報窃取にも気を付ける必要がある。管理端末へのウイルス対策ソフトの導入やソフトウエアの脆弱性対策を行い、フィッシングサイト（偽の認証画面）にアカウント情報を入力しないように注意してほしい。

CMSを用いたウェブサイト構築における情報セキュリティー対策の詳細は、独立行政法人情報処理推進機構（IPA）のウェブサイト（https://www.ipa.go.jp/security/）に掲載する技術資料を参考にしてほしい。

（独立行政法人情報処理推進機構・江島将和）