ウェブサイトの改ざん対策

○　ウェブサイトの改ざんとは

ウェブサイト改ざんとは、悪意のある者によって、ウェブサイトのコンテンツや設定が管理者の意図しない状態に変更されたり、ウェブサイトに管理者の意図しないファイルを蔵置されることを言います。

ウェブサイトを改ざんされてしまうと、正しい情報が発信できなくなったり、無関係の画像やメッセージが掲載されたりするほか、改ざんに合わせて、ウェブサイト等に保存していた個人情報が窃取されたり、ウェブサイトを閲覧した者がウイルス感染してしまうおそれがあります。

○　ウェブサイト改ざんの手口

- 窃取したアカウント情報を悪用した不正アクセスによるもの
- ソフトウェアのぜい弱性を悪用したもの
- 組織内のアクセス制御機能の不備を悪用したもの

○　よくある相談

＜相談事例１＞

「ウェブサイトが改ざんされている」と顧客から連絡があった。確認すると見覚えのない画像が掲載されており、管理画面にアクセスできなくなっていた。

＜相談事例２＞

自社のＥＣサイトが何者かに攻撃を受け、氏名、生年月日、住所、電話番号等の個人情報が外部に流出してしまった形跡が発見された。

＜相談事例３＞

「ホームページを閲覧していたらウイルス検知した」と顧客から連絡があった。ホームページのあるウェブサーバを確認したところ、マルウェアが置かれていた。

○　ウェブサイト改ざんの被害に遭ったら

被害が遭ったサーバ、ネットワーク機器等を調査する

被害の再発防止のため、ウェブサイト改ざんに関する原因等の調査をしてください。他のマルウェアやハッキングツール等の影響を受けている可能性があるため、改ざんが確認されていないサーバやネットワーク機器、パソコンも含めて調査してください。

なお、調査に当たっては、改ざんされたウェブサーバをはじめとした各種機器のログが必要となりますので、ログは、バックアップデータと同様に適切に保管してください。

ウェブアプリケーションやＣＭＳ等のぜい弱性を塞ぐ

改ざんに関する原因等の調査を基に、利用しているＯＳやソフトウェア、ネットワーク機器等の更新ファイルを適用して、ぜい弱性を塞いでください。ウェブアプリケーションやＣＭＳ（コンテンツ・マネージメント・システム）のぜい弱性が悪用され、ネットワークに侵入された事例も多数確認されています。

パスワードを変更する

改ざんに関する原因等の調査を基に、攻撃者からアクセスされた可能性があるパソコン、サーバ、ネットワーク機器等のパスワードを速やかに変更してください。ぜい弱性対策を実施したにもかかわらず、パスワードの変更を怠ったために、ネットワークに侵入された事例も多数確認されています。

アクセスログ等を保存する

ウェブサイト改ざんの被害に遭った場合は、直ちにサービスを停止し、管理者画面やデータベースへのアクセスログの保存・印字等を行い、証拠を保全してください。

警察に通報・相談する

ウェブサイト改ざんの被害に遭った場合は、アクセスログ等の資料を持参して、最寄りの警察署又はサイバー犯罪相談窓口に通報・相談してください。

なお、事前に電話で担当者と日時や持参する資料の調整をしていただくと対応がスムーズに進みます。

○　ウェブサイト改ざん発見のための着眼点等

ウェブサイトが改ざんされていないか、次に掲げる項目を確認してください。

- 会員入力画面や購入画面等に不審な JavaScript が蔵置されていないか
- 入力画面が不正なＵＲＬになっていないか、いつもと違う画面が表示されていないか
- ウェブサーバ、ＦＴＰ、ＳＳＨ等のログに不審なアクセスがないか

【改ざんされたウェブサイトの簡易発見方法】

- 大手検索サイトにおいて、「site:○○○.co.jp」など「site:」の後に自社のウェブサイトのドメイン名を入力して検索し、検索結果に見覚えのないページが表示されていないか確認する。

○　被害防止対策

ウェブサーバのセキュリティ対策を行う

ウェブサイトの改ざんの被害に遭わないためには、

- ウェブサーバのＯＳやソフトウェアを最新の状態に保つこと。
- 管理者のＩＤやパスワードを適切に管理すること。

・　ウィルス対策ソフト等を導入すること。

などの対策を講じることが重要です。詳細は、「基本的なセキュリティ対策」を確認してください。

また、次に掲げる対策を講じてください。

・　ウェブサーバ上の不要なサービスやアカウントを削除又は停止する。

・　公開を想定していないファイルをウェブ公開用のディレクトリ以下に置かない。

・　ウェブアプリケーションに対する攻撃からウェブサーバを保護するため、ＷＡＦ（Web Application Firewall）等のセキュリティ製品を導入する。

・　定期的にバックアップを取得し、正常なコンテンツと比較して、不正なファイルが置かれていないか確認する。

通信経路を暗号化する

ネットワークの盗聴を防ぐため、重要な情報を取り扱うウェブページでは、利用者のパソコンとの通信経路を暗号化してください。また、利用者に通知する重要情報は、メールで送らず、暗号化されたhttps://のページに表示するとともに、ウェブサイト運営者がメールで受け取る重要情報を暗号化してください。

採用する暗号技術は、CRYPTREC暗号リストに掲載されているものを利用することを推奨します。

利用者のパスワードをソフト付きハッシュ値の形で保管する

利用者のパスワードを平文で保存していたために、サーバ等が不正アクセスされた際に、被害が拡大した事例が確認されています。パスワードをサーバ内で保管する際は、平文ではなくソフト付きハッシュ値の形で保管してください。また、入力フィールドでは、パスワートは伏せ字で表示されるように設定してください。

詳細な対策は、独立行政法人情報処理推進機構（ＩＰＡ）の「安全なウェブサイトの作り方」をご参照ください。

○　参考リンク

・　総務省

「ＳＱＬインジェクションへの対策」