平成 26 年 2 月

広島県警察本部
サイバー犯罪対策課
082-228-0110
(内線 705-586)

～激増するウェブサイト改ざんに要注意～

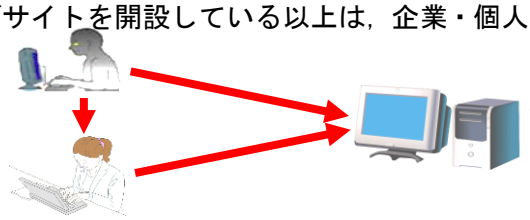
貴方の会社は
大丈夫？

■　ウェブサイト改ざん被害の現状

昨年から企業・自治体や個人のウェブサイトが何者かに書き換えられ，このサイトを閲覧した一般のインターネット利用者がウイルスに感染するという事案が激増しています。

昨今，ニュースでも話題になっていますが，日本国内の多くのサイトが攻撃対象となり，ウェブサイトの改ざん被害に遭っています。**攻撃対象は，大手企業に限らず，中小企業，個人のウェブサイトと多岐に渡っています。**

改ざんの被害は年に数千件単位で確認されているため，ウェブサイトを開設している以上は，企業・個人を問わず，脅威にさらされていることになります。



■　ウェブサイト改ざんの手口

1　パスワードの盗み出しによる改ざん

ウェブサイトの管理を行っているパソコンをウイルスに感染させたり，総当たり攻撃や辞書攻撃（自動プログラムによる推測打ち手法）によって ID・パスワードを盗み出し，改ざんが行われます。

2　システムの脆弱性を利用した改ざん

ウェブサーバの OS やプログラムの脆弱性を突いて，外部から侵入し改ざんが行われます。

■　ウェブサイト改ざんの被害にあってしまうと・・・

攻撃者がウェブサイトの改ざんをする目的の一つに，改ざんしたサイトの閲覧者をさらに，ウイルスに感染させるというものがあります。

最近の特徴として，攻撃者が仕込むウイルスは，明らかに日本人をターゲットとしたものが見受けられ，感染したパソコンを監視し，日本国内のネットバンキング，オンラインショッピングサイト，クレジットカードサイト等を閲覧した場合に，パスワードを盗み取ろうとするものが多いようです。

昨年から全国で被害が急増し，社会問題化している「インターネットバンキング不正送金事案」（平成 25 年中，全国で 1315 件が認知され，被害総額は約 14 億円に上る）についても，多くが，まさにこの手口で正規利用権者の ID やパスワードを盗み取り，犯行に及んだものと考えられています。

単純に自社のウェブサイトを書き換えられたという被害だけにとどまらず，そのサイトを閲覧した一般利用者にまで金銭的な被害を及ぼす可能性があります。

そのような事態となった場合，セキュリティの甘さを追及され，会社の社会的信用を下げてしまうことも十分に考えられます。

■　ウェブサイト改ざんへの対策

1　攻撃者は，会社の規模，業種に関係なく，ウイルスを仕込むべく攻撃をしてきます。サーバの OS やプログラムのアップデート等は怠ることなく随時行う必要があります。

2　最近では，標的型メール等の人為的なミスを突いた攻撃も増えています。システム自体のセキュリティを高めることはもちろんのこと，従業員のセキュリティ意識や知識も高める必要があります。

3　信頼のおけるホスティングサービス（レンタルサーバ）を利用する方法もあります。