■ ドメイン名の乗っ取りを防止するために

JPRS
JAPAN REGISTRY SERVICES

ドメイン名の乗っ取り（ドメイン名ハイジャックとも呼ばれる）は、ドメイン名の管理権限を持たない第三者が、不正な手段で他者のドメイン名を自身の支配下に置く行為です。

企業が利用しているドメイン名が乗っ取られた場合、「正しいURLでWebにアクセスしているのに、偽のWebサイトが表示される」、「企業宛ての電子メールが盗まれ、機密情報や顧客情報が流出する」、「ドメイン名の名義が第三者のものに書き換えられてしまう」といった企業の信頼に直結する被害が発生します。

ドメイン名の乗っ取りの手法としては、主に以下の二つの手段が用いられます。

- **DNSサーバーを狙い、不正な応答を返すようにする**
- **ドメイン名の管理権限を奪い、登録情報を書き換える**

企業のWeb担当者など、ドメイン名の管理に関わる立場においては、特に後者によるドメイン名の乗っ取りを防ぐために適切な管理を行う必要があります。

▼社内におけるドメイン名管理体制の確立

企業など組織においてドメイン名の登録・利用を行う場合、組織内の複数の部門からそれぞれの利用目的のために勝手に複数のドメイン名管理サービスが利用されるような状況であると、その全容把握ができず、セキュリティ配慮に欠けた運用がなされたり、管理が放置されたりするドメイン名が発生し、ドメイン名の乗っ取りにつながるリスクが大きくなります。組織としてドメイン名の管理を担当する部門・要員、及び管理のためのルール・手順を社内で確立しておくことが必要です。

また、Whois（ドメイン名の登録情報をオンライン確認するサービス）での定期的な登録状態の確認や、ドメイン名管理サービスからの登録情報変更通知メールを一元的に確認することは、ドメイン名の乗っ取りなどの意図しない情報変更を迅速に検知するための手法として有効です。

▼ドメイン名登録者が気を付けておくべきこと

ドメイン名管理サービスからは、登録中のドメイン名に関して、ドメイン名の移転、更新／廃止、レジストラ（JPドメイン名においては指定事業者）の変更など、ドメイン名の登録者の意向を確認するための連絡が来ることがあります。

ドメイン名の登録者は、その連絡を正しく受け取ることができるように、届け出ている連絡先情報を常に最新に保ち、登録しているドメイン名に関する連絡があった場合には、必ず内容を確認し、適切な対応を行えるように気を付けておく必要があります。

▼ドメイン名管理サービス利用のための適切な認証情報の設定

ドメイン名管理サービスを利用するためのパスワードが安易であったために第三者による不正なログインが行われ、ドメイン名の登録情報やDNS情報が書き換えられてしまうという事例が発生しています。

オンラインサービスに一般的な注意事項ではありますが、類推されにくいパスワードの設定とその適切な管理、二要素認証などによるセキュリティレベルの高い認証手段の選択肢があればその利用を検討することなどが挙げられます。