DNSのレコード

これまで、WebサイトのFQDNからIPアドレスを取得する例を説明してきました。これを正引きといいます。DNSには、IPアドレスからFQDNを取得する逆引きの機能もあります。

DNSサーバには、FQDNやIPアドレスなどの情報をレコードという形式で格納しています。レコードには複数のタイプがあります。FQDNからIPアドレスを取得する正引きのためのレコードを「Aレコード」、IPアドレスからFQDNを取得する逆引きのためのレコードを「PTRレコード」といいます。表 3-3-1 に、DNSの主なレコードタイプを示します。

表 3-3-1

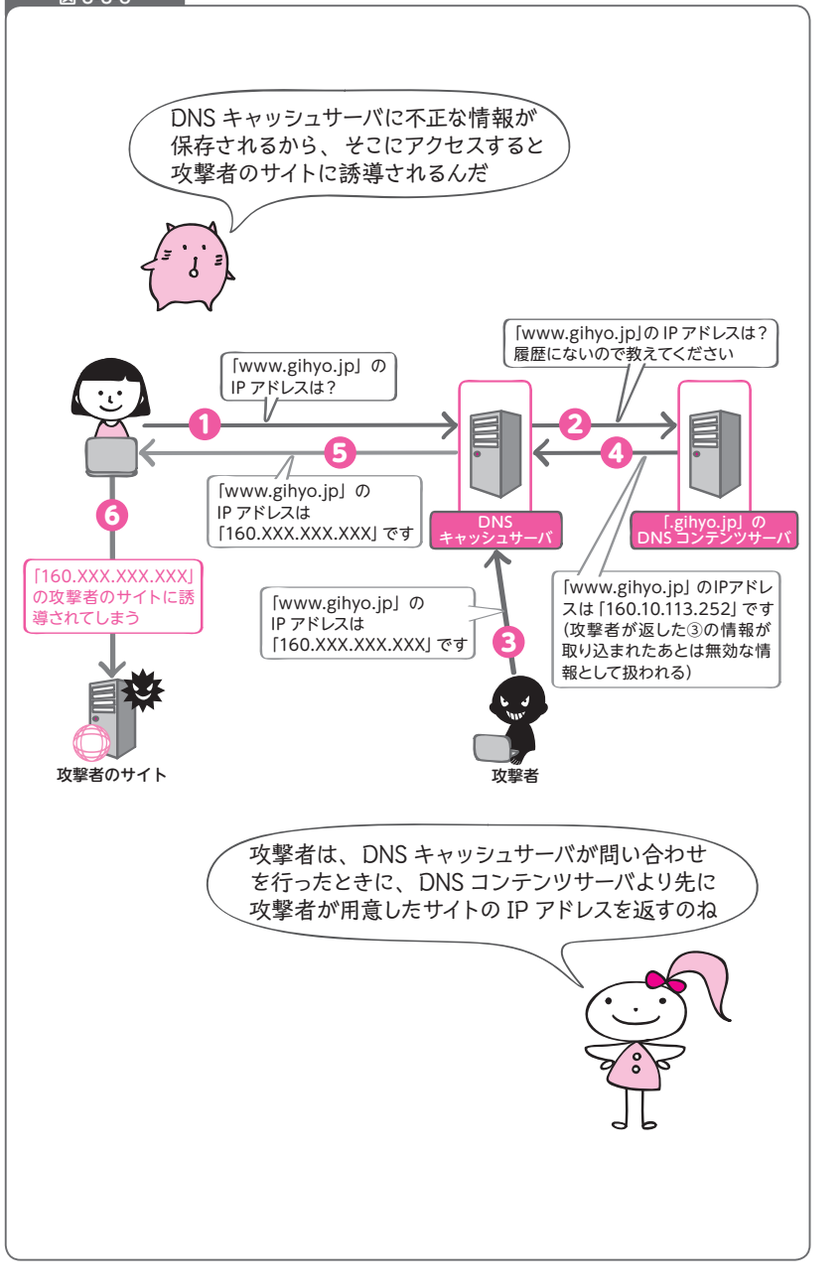
タイプ	内容
A	ホストのIPアドレス
CNAME	ホストの別名（エイリアス）
HINFO	ホストに関する追加情報
MX	ドメインのメールサーバ名
NS	ドメインのDNSサーバ名
PTR	IPアドレスに対応するホスト名
SOA	ゾーン（ドメイン）情報
TXT	テキスト情報
WKS	ホストで実行されているウェルノウンサービス情報

DNSの脆弱性を狙う攻撃

DNSにはいくつか脆弱性があり、それを狙って攻撃がしかけられることがあります。その1つが、昔からよく知られている「DNSキャッシュポイズニング」です。

DNSキャッシュサーバは、問い合わせを受けたとき、回答となり得る情報が履歴にあればその情報を返しますが、履歴に情報がない場合（または履歴の有効期間が過ぎている場合）はDNSコンテンツサーバに問い合わせます。ここで、DNSコンテンツサーバからの回答より先に不正な情報をDNSキャッシュサーバに送り、不正な情報を履歴に保存させる攻撃をDNSキャッシュポイズニングと呼びます（図 3-3-5）。

図 3-3-5



エクスプロイトキットを活用した攻撃

クライアント端末に対する攻撃では、ペイロードを含むエクスプロイトコードをマルウェアとして作成し、配布する方法が最も一般的です。

攻撃者は、クライアント端末に導入されたアプリケーション（プログラム）の脆弱性を狙っています。頻繁に狙われるアプリケーションとして、Java、Adobe Reader、Adobe Flash、Internet Explorerなどが挙げられます。

クライアント端末で使用するアプリケーションが脆弱性をもつバージョンであると、エクスプロイトが成功します。あらかじめ、標的の環境を入念に調べたうえで狙い撃ちするような攻撃（標的型サイバー攻撃など）でなければ、エクスプロイトを狙ったマルウェアの成功率は必ずしも高いとは言えません。そこで、攻撃者は、エクスプロイトの成功率を上げるため、エクスプロイトキットと呼ばれるツールキットを活用します。

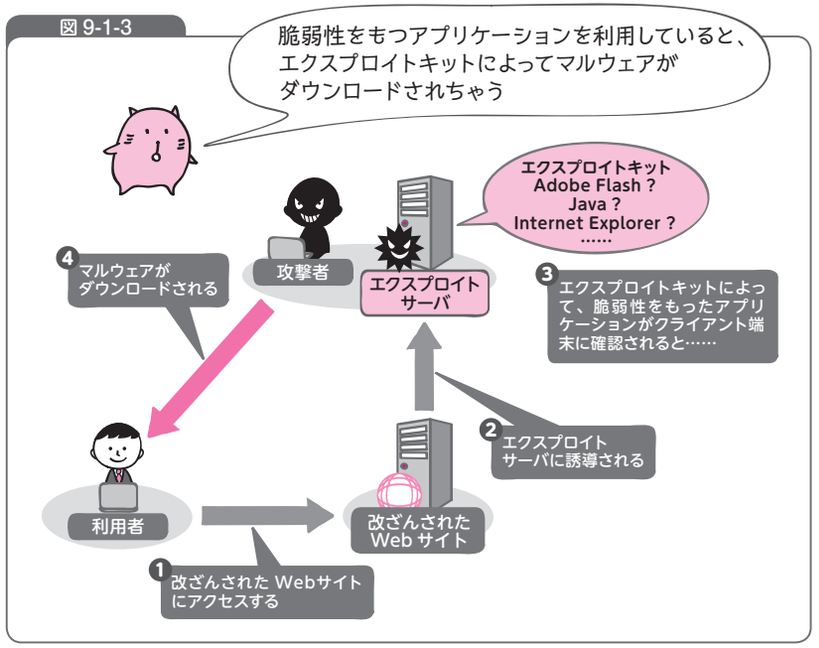
エクスプロイトキットとは

クライアント端末に対して、広く効率良くマルウェアを配布し、感染させるために、攻撃者は、「エクスプロイトキット」と呼ばれるツールキット（スクリプト）を利用します。

エクスプロイトキットは、クライアント端末上のアプリケーションを確認してから、脆弱性をもつバージョンに合致するマルウェアをダウンロードさせ、マルウェアの配布と感染を効率良く行うしくみを実装しています。

利用者が改ざんされたWebサイトにアクセスすると、悪意あるエクスプロイトサーバに誘導され、そこに仕込まれたエクスプロイトキットによってクライアント端末に導入されているアプリケーションとそのバージョンが確認されます。脆弱性をもつバージョンが確認されると、その脆弱性を狙ったマルウェアがダウンロードされます（図 9-1-3）。

図 9-1-3



有名なエクスプロイトキットには、PhoenixやAngler EK（Exploit Kit）などがあります。エクスプロイトキットで悪用される脆弱性は定期的に更新されており、新しく確認された脆弱性や未知の脆弱性（ゼロデイ脆弱性）が利用されていたケースも確認されています。

エクスプロイトを防ぐために必要なセキュリティ対策

エクスプロイトは、ソフトウェアの脆弱性を悪用した攻撃であるため、根本的な対策として脆弱性を保護することが重要となります。その方法としては、OSやソフトウェアの迅速なアップデート、脆弱性を保護するセキュリティ製品（脆弱性を突く攻撃を検知・制御する対策製品）の活用などがあります。未知の脆弱性を悪用した攻撃も発生していることから、ゼロデイ攻撃への対策の検討も重要です。