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