JPRS トピックス＆コラム

■DNSSECに関するよくある質問と回答（基礎技術編―2011年2月版）

DNSSECに関するよくある質問と回答をQ＆A形式でまとめました。オンライン版はJPRSホームページ（http://jprs.jp/dnssec/）で公開されていますので、併せてご利用ください。

■DNSSEC の基本について

Q1 DNSSEC とは何ですか？

DNSSEC は、DNS サーバーから受信した DNS 応答が「**本当に正しい**」ということを受信側で検証可能にするための、DNS の拡張機能です。

Q2「本当に正しい」というのはどういうことですか？

受信したデータについて以下の二つが確認できた場合、そのデータは「本当に正しい」と検証できます。

① 本当にその相手が作成したものであること（**データ出自の認証**）

② 通信途中で書き換えられたり、一部が失われたりしていないこと（**データの完全性**）

つまり「正しい相手から」「そのままの形で」の二つが、「本当に正しい」の検証における必要条件となります。

Q3 DNSSEC では DNS 応答の偽造をどのように防いでいるのですか？

DNSSEC では応答送信の際に**公開鍵暗号**を利用した**署名**を付加します。受信側で付加された署名を検証することによりデータの出自認証と完全性を確認でき、DNS 応答の偽造を防ぐことができます。

Q4 公開鍵暗号とは何ですか？

データの暗号化と復号に異なる一対の鍵（**公開鍵**と**秘密鍵**）を用いる暗号方式をいいます。

公開鍵暗号方式では、外部に広く公開する公開鍵と作成者が秘匿する秘密鍵の2種類の鍵を利用します。公開鍵と秘密鍵は必ず一対になっており、一方の鍵で暗号化したデータは、他方の鍵でのみ復号できるようになっています（暗号化に使った鍵そのものも含め、別の鍵では復号できません）。

公開鍵暗号による暗号通信では、通信相手の公開鍵でデータを暗号化してから相手に送信します。このデータは相手の秘密鍵以外では復号できません。

そして、暗号化に使った公開鍵に対応する秘密鍵を持っているのは通信相手のみであるため、より安全な暗号通信を行うことができます（図1）。

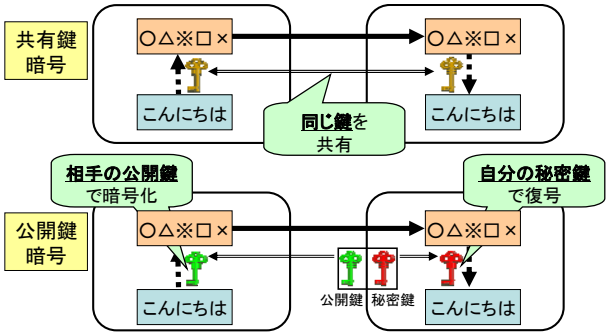

図1：共有鍵暗号と公開鍵暗号

Q5 署名とは何ですか？

公開鍵暗号の仕組みを応用することにより、そのデータが「本当に正しい」ことを検証できるデジタル署名（以下、単に「署名」とします）を実現できます。

公開鍵暗号を用いてデータに署名する場合、送信者は自分の秘密鍵でデータを暗号化してから相手に送信（あるいは広く公開）します。このデータは送信者の公開鍵で復号できるため、誰でも元のデータに復号することができます（そのため、データの秘匿性はありません）。しかし、それ以外の鍵では復号できません。

つまり、データを暗号化したのは復号できた公開鍵に対応する秘密鍵を持っている送信者以外になく、かつデータが途中で書き換えられていない、つまり「本当に正しい」ということが証明できます（図2）。

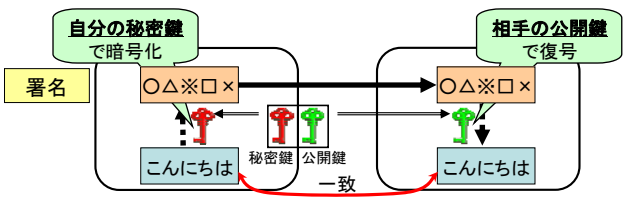

図2：公開鍵暗号による署名

※掲載内容は2011年2月現在のものです。

Q6 署名の際に使われるハッシュ値とは何で、何のために使われるのですか？

実際の署名検証ではデータそのものに代え、事前に決められた方法（ハッシュ関数）によりデータから計算した「ハッシュ値」と呼ばれる数値を使用します。

送信者は計算したハッシュ値を自分の秘密鍵で暗号化したもの（ハッシュ値に対する署名）を、元のデータと共に送信します。受信者は受信したデータからハッシュ値を計算し、相手の公開鍵で復号したハッシュ値と照合します。二つの値が一致した場合、受信したデータが「本当に正しい」ことを検証できます(図3)。

このように、署名対象をデータそのものから、より短い数値であるハッシュ値に変更することにより、署名検証にかかる負荷を軽減できます。

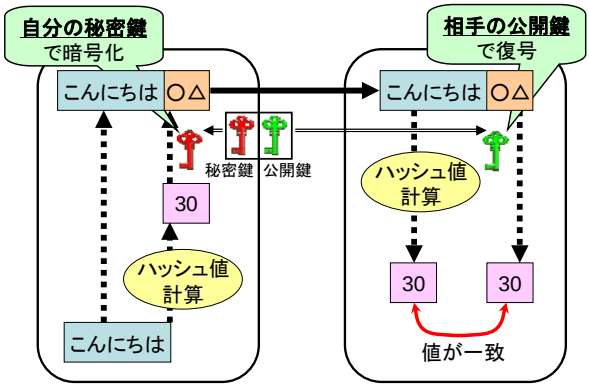

図3：ハッシュ値の照合による署名の検証

Q7 RSA 暗号とは何ですか？

公開鍵暗号を実現するために 1977 年に開発された暗号方式で、DNSSEC を含む多くの分野で使われています。「RSA」という名前は、この方式を発明した3人の暗号研究者の頭文字に由来しています。

Q8 キャッシュポイズニング攻撃とは何ですか？

偽の DNS 応答をキャッシュ DNS サーバーに記憶させることにより、フィッシングや電子メールの盗み見などを図る攻撃方法をいいます[1]。

キャッシュポイズニング攻撃そのものは古くから知られていましたが、2008 年に発表された**カミンスキー型攻撃手法**により、攻撃のリスクが飛躍的に高まりました。

Q9 カミンスキー型攻撃手法とは何ですか？

キャッシュポイズニング攻撃を高効率で成立させるための攻撃方法です。DNS プロトコル上の脆弱性に起因しており、根本的な対策として DNSSEC の導入が有効になります。

カミンスキー型攻撃手法の詳細については JPRS トピックス&コラム No.9「新たなる DNS キャッシュポイズニングの脅威」をご参照ください。

■DNSSEC の機能について

Q10 DNSSEC で実現されることは何ですか？

DNSSEC の導入により、受け取った DNS 応答が「本当に正しい」ことを受信側で検証できるようになります。そのため、前述したキャッシュポイズニング攻撃の防止に対し有効です。

Q11 DNSSEC では実現されないことは何ですか？

DNSSEC では DNS 応答の暗号化を行いません[2]。

DNSSEC は DNS に対する付加機能であり、HTTP などの DNS 以外の通信の安全性を保証するためには、IPsec や SSL などの技術を別途用いる必要があります。

DNSSEC では、ドメイン名の見間違いや打ち間違いを狙うタイプのフィッシングには対応できません。

Q12 DNSSEC と SSL の違いは何ですか？

DNSSEC では、相手との**通信開始前**に必要となる、名前解決の安全性を保証します。

これに対し SSL では、相手との**通信時**の本人証明、及び通信データの暗号化を行っています。

Q13 私は既に SSL を導入しています。DNSSEC を追加導入する必要がありますか？

DNSSEC と SSL は双方とも、暗号技術により利用者の安全性を高めるための技術です。しかし DNSSEC と SSL では保護の対象が異なっており、他方の機能を包含するものではありません。そのため SSL が導入済みであっても、DNS の名前解決の安全性を確保するためには DNSSEC を別途導入する必要があります。

---

1 誤認に基づくフィッシングと異なり、**ブラウザーのアドレスバーに正当な Web サイトと全く同じ URI が表示される**ため、危険性が高くなります。

2 DNS 登録情報は公開情報であり、暗号化を必要としません。