メールの電子署名と暗号化

山梨大学
情報システム課
2017年2月

1．はじめに

- インターネットからの脅威は日々増大しており、その被害は深刻化しています。社会問題になっている個人情報の流出は、多くがメールを媒介したウイルス感染が発端となっています。

- メールは、重要なデータをやり取りするには以下の点でセキュリティに問題があります。
  ① 送信者の本人確認が難しい
  ② 平文でやり取りする

- 上記問題の解決策として、電子証明書を利用した以下の方法があります。
  ① メールに電子署名を付与する
  ② メールを暗号化する

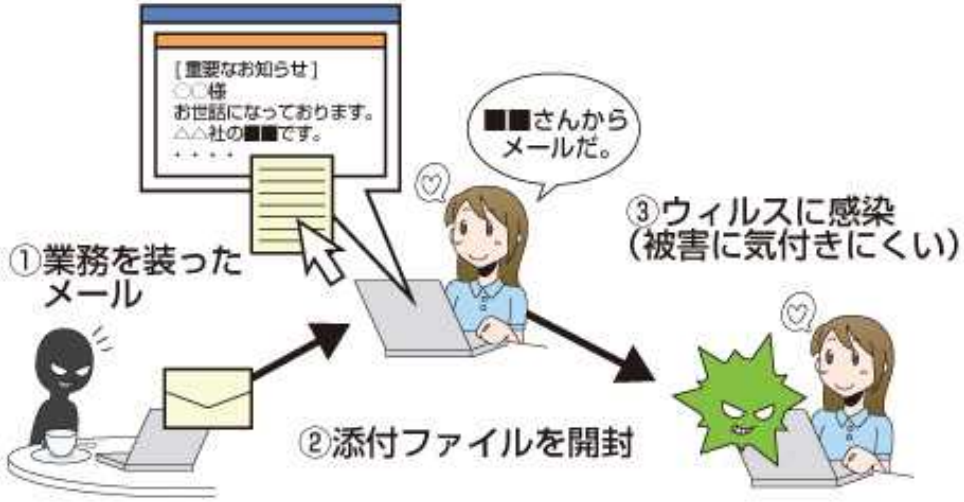
- 本書ではメールのセキュリティに関する問題と、その解決方法である電子署名および暗号化について、メールソフトの具体的な設定方法を含めて説明します。

2-1. 標的型攻撃メールとは

- 標的型攻撃メールとは、組織や個人を特定してウイルス付のメールを送信することをいいます。これは悪意のある第３者が個人情報等を盗む目的で行われます。

- メールの添付ファイル開封によりPCがウイルス感染してしまい、そこから個人情報が流出する恐れがあります。

- メールの内容は受信側をだまして添付ファイルを開かせようとするもので、通常の業務メールと注意して見分ける必要があります。

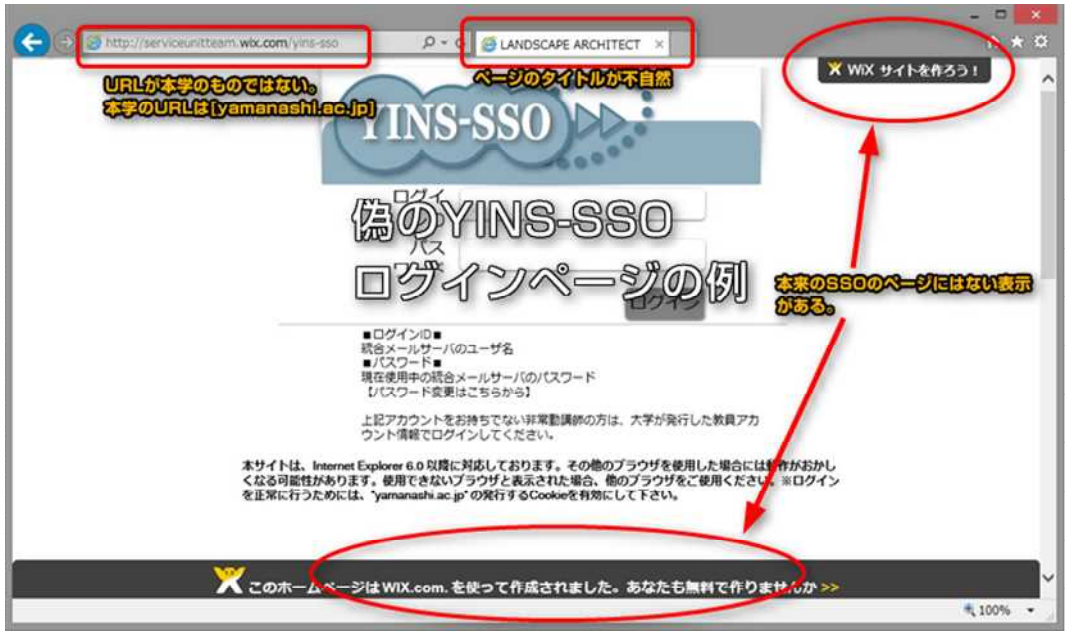


総務省HPより

2-2. フィッシングメールとは

- フィッシングメールとは、システム管理者等になりすまし、アカウント情報を盗み取ろうとするメールのことをいいます。

- 山梨大学での例（2015年4月）
  偽のYINS－SSOポータルに誘導するためのメールが、不特定多数の教職員宛に送信されました。
  このサイトで教職員がログインを試みることにより、アカウント情報を盗み取ろうとしたと考えられます。

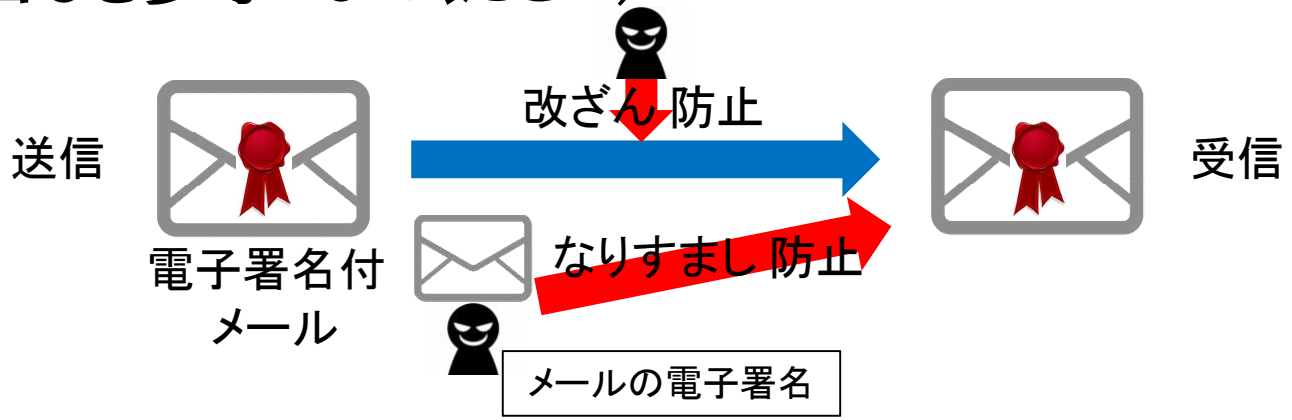


3．メール電子署名とは

- 日常的に送られてくるメール差出人の本人確認を行うこと、または差出人が送信するメールに信頼性があることを、受信者へ提示することはとても困難です。

- メールの差出人を本人確認する方法として、電子署名があります。電子署名をメールに付与するには、電子証明書が必要です。電子証明書は、認証局と呼ばれる第３者機関が、差出人の身元情報を認証して発行したものです。

- 電子署名を利用することにより、メール差出人のなりすまし行為及びメールの改ざんを防止することができます。（詳しくは項目５を参考にしてください）



4. メール暗号化とは

- 外部とメールを送受信する際は、インターネットの多くの部分で暗号化せずに流れています。そのため、メール本文や添付ファイルは中身をのぞき見られる恐れがあります。

- 暗号化していないメール本文では、重要な情報をやり取りしないことが原則になります。また、添付ファイルを送信する場合は、パスワードを設定するなどの対応が必要になります。

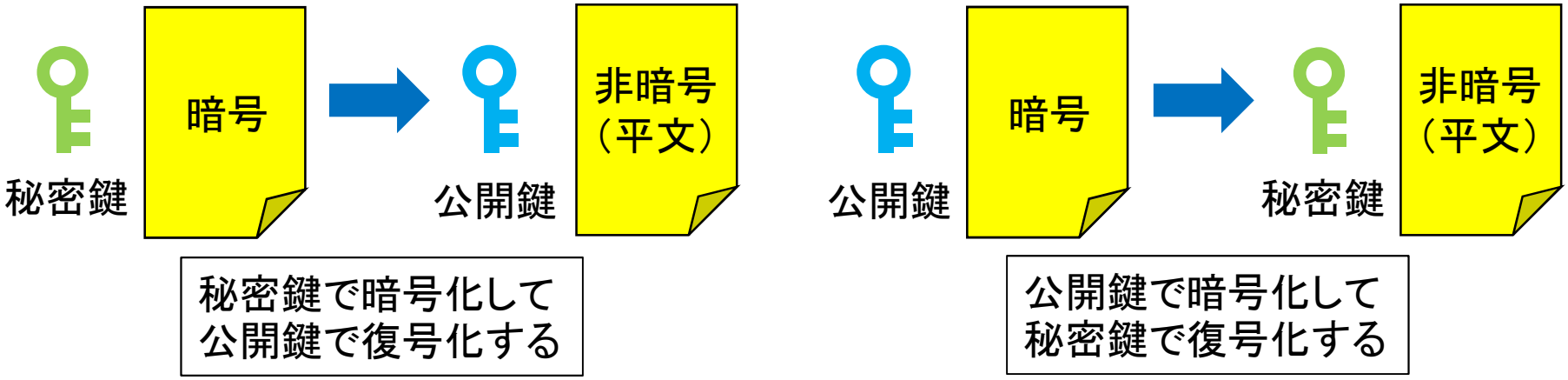
- 機密性の高いメールをやり取りするには、一つの方法として電子証明書を利用したメールの暗号化があります。（詳しくは項目５を参考にしてください）

メールの暗号化

5-1．S／MIMEとは（参考）

- S／MIME（Secure Multipurpose Internet Mail Extensions）とは、公開鍵暗号方式により、メールの電子署名および、メールを暗号化する仕組みです。

- 【公開鍵暗号方式】
  公開鍵暗号方式では、「公開鍵」と「秘密鍵」がペアになっています。暗号化と復号化には、それぞれの鍵を使います（どちらの鍵でも暗号化してもよい）。



- 「公開鍵」は、誰でも取得できる公開されている鍵です。
- 「秘密鍵」は、鍵の所有者だけが保持する鍵です。

5-2. S／MIMEとは（参考）

- **【メール電子署名】**
  送信者は自身の秘密鍵を使って、電子署名をメールに付与します。受信者はメールに添付されている公開鍵を使ってメールの改ざん・なりすましがないか確認することができます。

① 送信者の秘密鍵を使って電子署名を付与する。

② 電子証明書（公開鍵）を併せて送付する

③ 送信者の公開鍵を使って不正がないか確認する。

- **【メール暗号化】**
  送信者は事前に入手した受信者の公開鍵を使って、メールを暗号化します。受信者は自身の秘密鍵を使って、メールを復号化します。

① 受信者の公開鍵を使ってメールを暗号化する。

② 受信者の秘密鍵を使ってメールを復号化する。