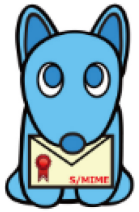
S/MIME

2015年11月19日



S/MIME
エスマいぬ

JIPDEC【法人番号**1010 4050 09403**】
(一般財団法人日本情報経済社会推進協会)
安信簡情報環境推進部　事業推進室
室長　大泰司 章(おおたいし あきら)

１．はじめに

２．S/MIME（最初に説明すること）

３．トピックス

１．はじめに

JIPDECの組織

- **名称**　JIPDEC【法人番号1010 4050 09403】（じぷでっく）
  一般財団法人日本情報経済社会推進協会
  Japan **I**nstitute for **P**romotion of **D**igital **E**conomy and **C**ommunity

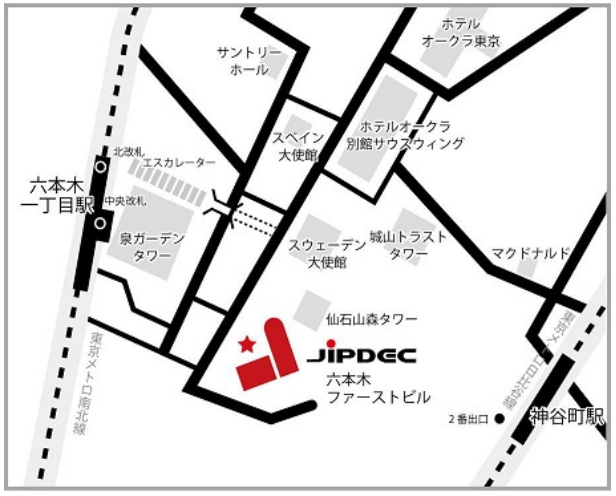
  以前は、財団法人日本情報処理開発協会
  Japan **I**nformation **P**rocessing **DE**velopment **C**orporation

- **設立**　昭和42年12月20日

- **基金**　39億9,900万円

- **事業規模**　25億1,610万円（平成27年度予算）

- **職員数**　108名（平成27年4月現在）



JIPDEC事業案内

●制度

- プライバシーマーク制度の運用
- 電子署名・認証制度に基づく特定認定業務の調査
- ISMS/ITSMS/BCMS/CSMS適合性評価制度の運営

●サービス

S/MIME

- **サイバーID証明書JCANの普及**
- 標準企業コードの登録・管理
- **サイバー法人台帳ROBINSの運用**
- マイナンバー対応支援サービスの提供

マイナンバー(法人番号)

マイナンバー(個人番号)

●提言

IoT

- 電子情報の利活用基盤の整備のための調査研究
- 産学官連携による課題の検討、政府への提言
- IT資産マネジメントに関する調査研究
- 電子情報利活用に関するさまざまな情報提供

2．S/MIME（最初に説明すること）

S/MIMEの目的

- 読み方： **エスマイム**


エスマいぬではありません。

- **S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions

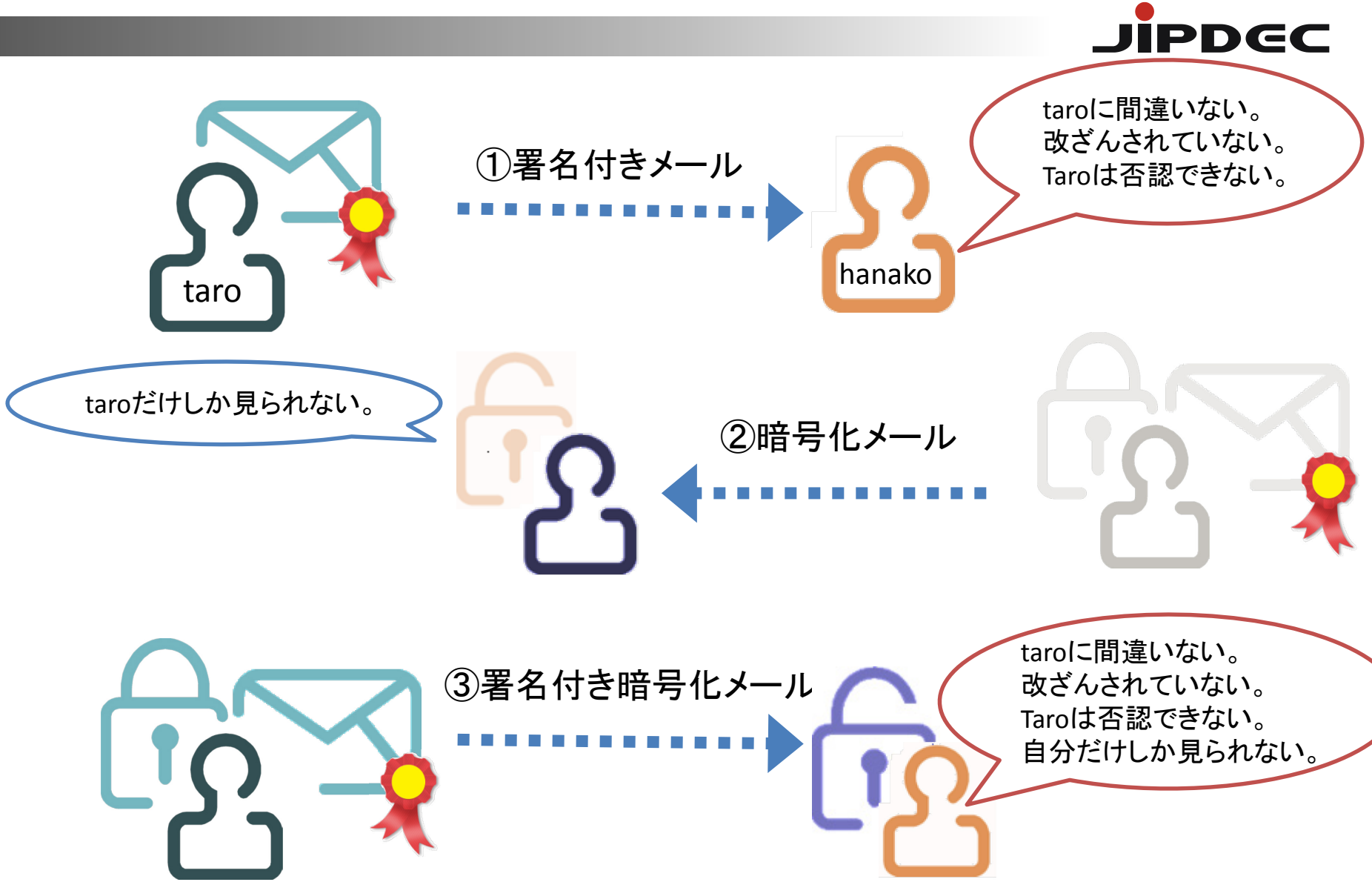
- 署名：

・送信者は、自分の秘密鍵で署名をする。
・受信者は、相手の公開鍵で検証する。
→メールの**送信者が誰**であるか分かる。
　メールが**改ざんされていない**ことが分かる。

- 暗号化：

・送信者は、相手の公開鍵で暗号化する。
・受信者は、自分の秘密鍵で復号する。
（実際には共通鍵を公開鍵で暗号化している。）
→MUA間で**暗号通信**が可能。

S/MIMEの利用シーン



S/MIMEの証明書管理

- 「信頼モデル」、「認証局のあり方」は、TLSと同じ。

→島岡さんの資料の「ブラウザ」を「メーラ」に読み替えてください。

- トラストアンカーの配布方法

（メーラ・OSにあらかじめルート証明書がインストールされている）パブリック証明書の利用が前提。

（どこから来るか分からない送信者が使う証明書のルートをインストールしておくのは無理。ただし、プライベート証明書の社内・グループ内利用はありえる。）

- 自分の証明書取得方法

認証局から購入する。

- 相手の証明書取得方法

署名つきメールを受け取ると、メーラが自動インストールする。

メールアドレスで証明書を検索するサービスは、いつの間にかなくなってしまった。

S/MIMEの鍵管理

- 証明書の購入を前提とすると、
  鍵のライフサイクル＝証明書のライフサイクル
（ただし、自分の秘密鍵を捨ててはいけません。）

- 「古いメールに×（ばってん）問題」
  パブリック証明書の有効期間は最大39か月。来たメールの相手の署名が期限切れを起こす。（実害はないが･･･）

- 「古いメールが読めない問題」
  端末やメーラを変えたときに、自分の古い証明書（秘密鍵）を引き継がないと、過去の暗号化メールが読めなくなる。

S/MIMEとDNS(DNSSEC)との関わり

- SMIMEA
  DNSのSMIMEA RRに証明書情報を登録

→CAの（パブリック）証明書なしでS/MIMEができる？

or

→CAの（パブリック）証明書は使うが、二重に検証してよりセキュアに？

- 署名：　署名検証で使う
  送信先のMUAの検証機能が実装されなければ、送信側からは使い始めづらい？

- 暗号化：　相手の証明書（公開鍵）取得に使う
  あらかじめ署名付きメールを送る（受け取る）手間が省けるか？
  証明書（公開鍵）がスパマーの手に渡らないようにできるか？？

※うれしいことはありそうだが、S/MIMEにはそれ以前の問題も多く…

3．トピックス

運用者（管理者）視点　～企業の場合～

- 従業員が自分で秘密鍵を管理
  - 問い合わせ対応等で業務効率低下。
  - 企業によっては、やってできないことではない。
- 企業が従業員の秘密鍵を管理
  - ゲートウェイ製品の利用。新たなコスト。
  - 監査、マルウェア検知の観点からはむしろ望ましい。
（添付ファイルのzip暗号化＋パスワードよりは･･･）

運用者（管理者）視点　～消費者の場合～

- ユーザーが自分で秘密鍵を管理
  - できる人はできる。できない人はできない。
  - ISPに問い合わせが来るしくみだと、サポートコストは膨大。
- ISPがユーザーの秘密鍵を管理
  - 踏み台問題。そもそもアカウントの認証は弱い。
  - ユーザーがISPに秘密鍵を預けるだろうか？
  - ユーザーが追加費用を支払うだろうか？
（ISPとしてメールシステムへの投資は難しい。）

S/MIME利用状況

- 銀行：　お客様へのメルマガや通知メール
- 官公庁：　METIメルマガ
- 外資系企業：
- メーカー：
- キャリア：
- 関連団体：　JIPDEC、IPA
- ISPのサービス：　NIFTY、biglobe、ぷららの証明書発行オプション

メールソフトの対応状況

	PCメーラ	Webメール	スマホ
Microsoft	○ Outlook	△ OWA ×Hotmail	○ Windows Phone
Apple	○ MAC OS	—	○ iOS
Google	—	× gmail	× Android ○Djigzo, CipherMail
Mozilla	○ Thunderbird	—	? FirefoxOS
CTC	—	○	—
エアー	—	○	—
Zimbra	—	○	—
Roundcube	—	○	—

にわとりたまご問題

	送信者	受信者	備考
署名 （一斉配信）	・費用負担 (1通あたりは小)	・受益者	・なりすまし防止 ・開封率向上
署名	・費用負担 (メアド数に比例)	・受益者	・なりすまし防止 ・開封率向上？
暗号化	・受益者 （送るデータの秘匿）	・費用負担 (メアド数に比例)	・営業秘密の保護

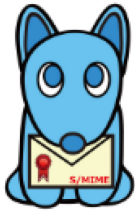
S/MIME普及のシナリオ

- 認知度向上（シンポジウム開催等）

  S/MIME普及シンポジウム2015　2015年9月4日
  http://jcan.jipdec.or.jp/topics/event/2015/20150904event.html

- 先進事例づくり
- 政府への政策面でのはたらきかけ
- メーラ・メールシステムのS/MIME対応とUI改善
- 以上をさらに推進する普及団体設立予定
  （DNSSECの普及もやりますか？）

よろしくお願いしますわんっ！



S/MIME
エスマいぬ

エスマイム（S/MIME）ファンクラブ ～エスマいぬのページ～
https://www.facebook.com/SmimeFanClub

エスマいぬ（S/MIME）
@esumainu