Information Security Laboratory
ISL

セキュリティフーラム 2021

2021年6月9日

「PPAP廃止」とその対策に関する考察

東京電機大学　客員教授
JSSEC代表理事
佐々木良一
r.sasaki@mail.dendai.ac.jp

目次

PPAPとは

Password付きZIP暗号化ファイルを送ります
Passwordを送ります
Aん号化（暗号化）
Protocol

縦に並べてPPAP

ピコ太郎のヒット曲「ペンパイナッポーアッポーペン（Pen-Pineapple-Apple-Pen）」の略称にかけた造語

命名したのは、日本情報経済社会推進協会（JIPDEC）を経て「PPAP総研」を設立した大泰司章氏

https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/

目次

FaceBookのグループ

くたばれPPAP！

公開グループ · メンバー1,301人

PPAPのメリットといわれていたもの

① **誤送信対策**

ファイル添付メールとパスワード記載メールのどちらか1通を誤送信しても情報は流出しない　＝＞**効果小**

② **盗聴防止**

データを暗号化しているので盗聴されても中身を読まれない

＝＞パスワード付きファイルを盗聴されるということは、同じ経路を流れるパスワードも盗聴される可能性が高いので**効果小**

③ **使いやすくて分かりやすい**

暗号化ZIPはWindowsなどが標準で対応しているので、一手間をかけなくても復号できる。暗号化する機能（パスワードを設定する機能）は標準では対応していないものの、どのアーカイバー（圧縮・解凍ソフト）も対応しているし相互運用性も高い。　＝＞**この効果はあるが**やはり使いにくい

https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/

PPAPの問題点

① 使いにくい

（a）パスワードが記載されたメールを探すのに時間がかかる場合もある。

（b）同じ相手から複数のメールが送られてきた場合には、どの添付ファイルがどのパスワードに対応しているのか迷うこともある。

② セキュリティ向上の効果がほとんどない。

③ マルウエア（ウイルス）攻撃に悪用される

Emotetマルウエアなどではパスワード付きZIPで圧縮して検出を回避する

https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/
を参考に改良

被害を受ける確率の計算式

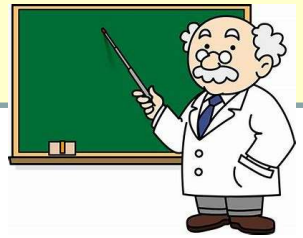
PT：全体としての被害を受ける確率

$$PT=P(A\cap B)=P(A)P(B|A) \fallingdotseq P(A) \quad \text{――(1)}$$

なぜなら、$P(B|A) \fallingdotseq 1$

A：メールの送信中に鍵をアクセスされる

B：メールの送信中に通信内容にアクセスされる



PPAPの問題点

① **使いにくい**

（a）パスワードが記載されたメールを探すのに時間がかかる場合もある。

（b）同じ相手から複数のメールが送られてきた場合には、どの添付ファイルがどのパスワードに対応しているのか迷うこともある。

② **セキュリティ向上の効果がほとんどない。**

③ **マルウエア（ウイルス）攻撃に悪用される**

Emotetマルウエアなどではパスワード付きZIPで圧縮して検出を回避する

https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/
を参考に改良

デジタル改革担当大臣の対応

- 平井卓也デジタル改革担当大臣は2020年11月24日の記者会見で、暗号化ZIPファイルをメールで送付した後に別のメールでパスワードを追送する手順、通称「PPAP」を内閣府と内閣官房で11月26日に廃止すると発表した。

https://xtech.nikkei.com/atcl/nxt/column/18/00001/04878/

目次

対策案の比較

		①暗号化なし	PPAP		③クラウドサーバ利用	④S/MIME 署名	④S/MIME 暗号化
			現状版	②SMSで鍵配送		この組み合わせが本命	
メールベースか		Yes	Yes	Yes	No	Yes	Yes
安全性	暗号強度	X	△	△	○	—	○
	鍵配送の安全性	—	X	△	X	—	○
	メール改ざんと送信者なりすまし検知	X	X	X	△	○	—
使い勝手（ユーザの手間）		○	△	△	○	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難

他にSTARTTLSなどあるがこれは、サーバ間の暗号用

対策案(1)

① メールの添付ファイルを暗号化しないまま送る。

（安全性　x:使い勝手〇）

PT＝P(A)

A:メールの送信中に通信内容にアクセスされる

PPAP対策のためこのような対応をした製品もある。

しかし、安全性の面からは望ましい方式ではない。

対策案の比較

		①暗号化なし	PPAP		③クラウドサーバ利用	④S/MIME 署名	④S/MIME 暗号化
			現状版	②SMSで鍵配送		この組み合わせが本命	
メールベースか		Yes	Yes	Yes	No	Yes	Yes
安全性	暗号強度	X	△	△	○	—	○
	鍵配送の安全性	—	X	△	X	—	○
	メール改ざんと送信者なりすまし検知	X	X	X	△	○	—
使い勝手（ユーザの手間）		○	△	△	○	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難

他にSTARTTLSなどあるがこれは、サーバ間の暗号用

対策案（2）

② メールに添付されるファイルを暗号化し、鍵をSMSなど別ルートで送る。（安全性　△：使い勝手△）

PT=P（A∩B）≒P(A)P(B)

A：SMSの送信中に鍵にアクセスされる

B：メールの送信中に通信内容にアクセスされる

PPAP対策のためこのような対応をした製品もある。

短期的にはありうる方式。

対策案の比較

		①暗号化なし	PPAP		③クラウドサーバ利用	④S/MIME 署名	④S/MIME 暗号化
			現状版	②SMSで鍵配送		この組み合わせが本命	
メールベースか		Yes	Yes	Yes	No	Yes	Yes
安全性	暗号強度	X	△	△	○	—	○
	鍵配送の安全性	—	X	△	X	—	○
	メール改ざんと送信者なりすまし検知	X	X	X	△	○	—
使い勝手（ユーザの手間）		○	△	△	○	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難

他にSTARTTLSなどあるがこれは、サーバ間の暗号用

対策案（3）

③ クラウドストレージを用いてファイルを共有する

（安全性：x　使い勝手〇）

クラウドストレージにファイルを格納し、共有リンクとPW（復号かぎ）をメールで取引先に伝える方式。

$PT=P(A\cap B)=P(A)P(B|A) \fallingdotseq P(A)$

なぜなら、$P(B|A) \fallingdotseq 1$

A：メールの送信中に共有リンクとPWにアクセスされる

B：クラウドストレージのファイルにアクセスされる

この方式ではPPAPでメール転送する方式の安全性しかない。

＝＞さらに改良が必要。

対策案の比較

		①暗号化なし	PPAP		③クラウドサーバ利用	④S/MIME署名	④S/MIME暗号化
			現状版	②SMSで鍵配送		この組み合わせが本命	
メールベースか		Yes	Yes	Yes	No	Yes	Yes
安全性	暗号強度	X	△	△	○	—	○
	鍵配送の安全性	—	X	△	X	—	○
	メール改ざんと送信者なりすまし検知	X	X	X	△	○	—
使い勝手（ユーザの手間）		○	△	△	○	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難

他にSTARTTLSなどあるがこれは、サーバ間の暗号用

目次

S／MIMEとは

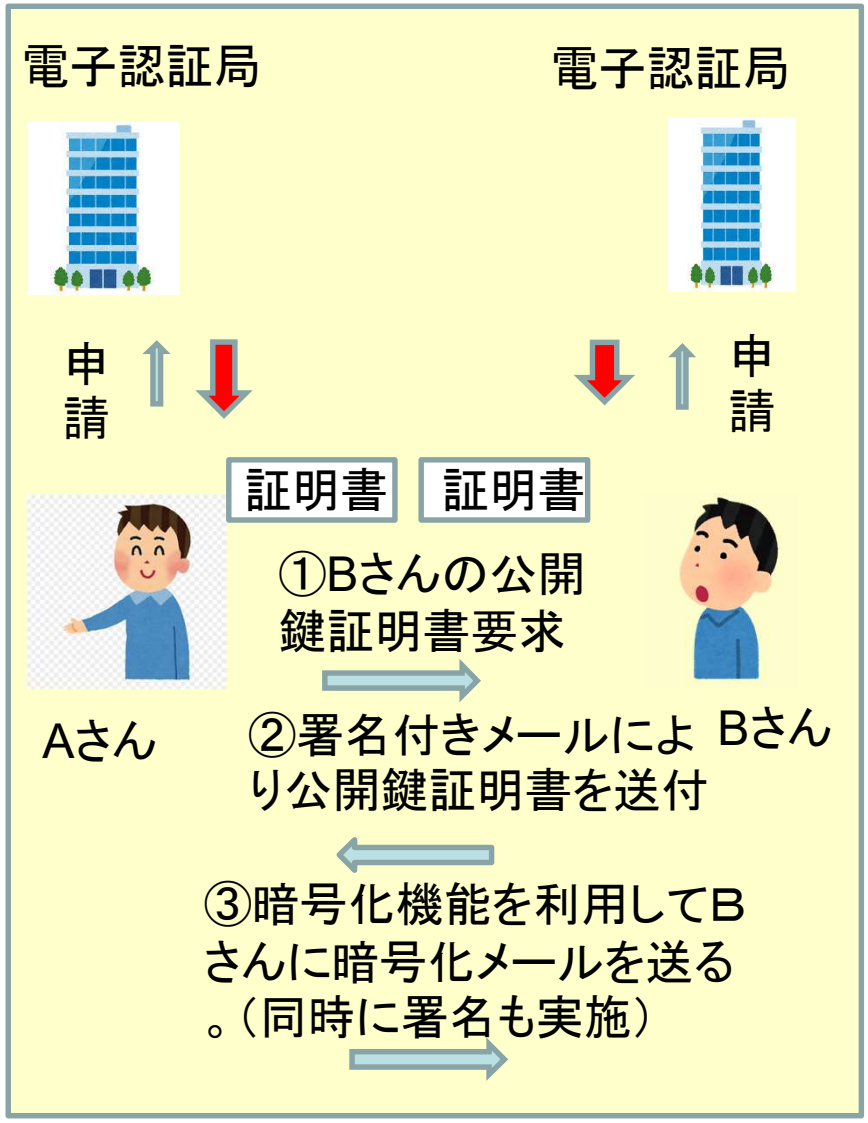
S/MIME（Secure / Multipurpose Internet Mail Extensions）とは、電子メールのセキュリティを向上する暗号化方式のひとつで、電子証明書を用いてメールの暗号化とメールへ電子署名を行うことができる。

S/MIMEの方式を用いるには、送信者と受信者側との両方がS/MIMEに対応する電子メールソフトを使用している必要があるが、Microsoft社のOutlookやiPhone・iPadのメールソフトなど多くのメールソフトが対応している。

元々S/MIMEは米国RSA Data Security Inc.によって開発され、変更管理はそれ以来IETFの手に委ねられた。

https://jp.globalsign.com/service/clientcert/about_smime.html
https://ja.wikipedia.org/wiki/S/MIME

S/MIMEの手順



AさんからBさんに暗号メールを送りたい場合

① Bさんの公開鍵証明書がない場合は、Aさんはメイルをに送り、Bさんの公開鍵証明書の送付を依頼

② BさんはS／MIME署名機能を利用して、公開鍵証明書付きのメイルをAさんに送る。

③ Aさんは、S／MIME暗号化機能を利用してBさんに暗号化メールを送る。（S／MIME署名機能を利用し同時に署名も実施）

その後、Bさんは、自分の秘密鍵を用いデータを復号するとともに、Aさんの公開鍵を用い、署名を検証。

2回目からは①②は不要

S/MIMEのメリット

① S/MIME暗号は公開鍵暗号を使っており、鍵の配送が容易であり、End-Endの暗号化が可能であり、安全性も高い。

② S/MIME署名が重要だと考えており、これが普及すればなりすましが抑え込まれいろいろな被害が減ると思っている＊。

③ S/MIME署名とS/MIME暗号を組み合わせることにより、非常に高い安全性が確保できる。

＊もちろん公開鍵証明書発行時点の本人確認の精度を上げる必要があると思うが、マイナンバーカードとリンクすることにより技術的には可能かと思う。

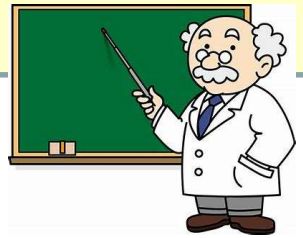
S/MIMEの現状の問題点

① 十分安全な暗号方式を使っているか疑問

② 公開鍵証明書が高価

③ 各種メーラのS/MIME互換性が確認されていない。

④ 使い勝手の悪い部分がある



S/MIMEにおける暗号利用

① S/MIMEv2：

ハッシュ関数としてmd5,sha-1

共通かぎ暗号としてRC2、TripleDES

公開鍵暗号として鍵長1024のRSA

など現在では、使ってはならない暗号方式を推奨

② すでにS／MIMEv3、S／MIMEv4が出ており、安全性が高いとされている暗号方式を推奨（例えばsha-256、AES暗号、鍵長2048のRSAなど）

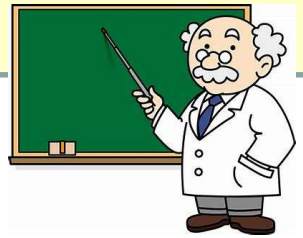
S/MIMEの現状の問題点

① 十分安全な暗号方式を使っているか疑問

② 公開鍵証明書が高価

③ 各種メーラのS/MIME互換性が確認されていない。

④ 使い勝手の悪い部分がある

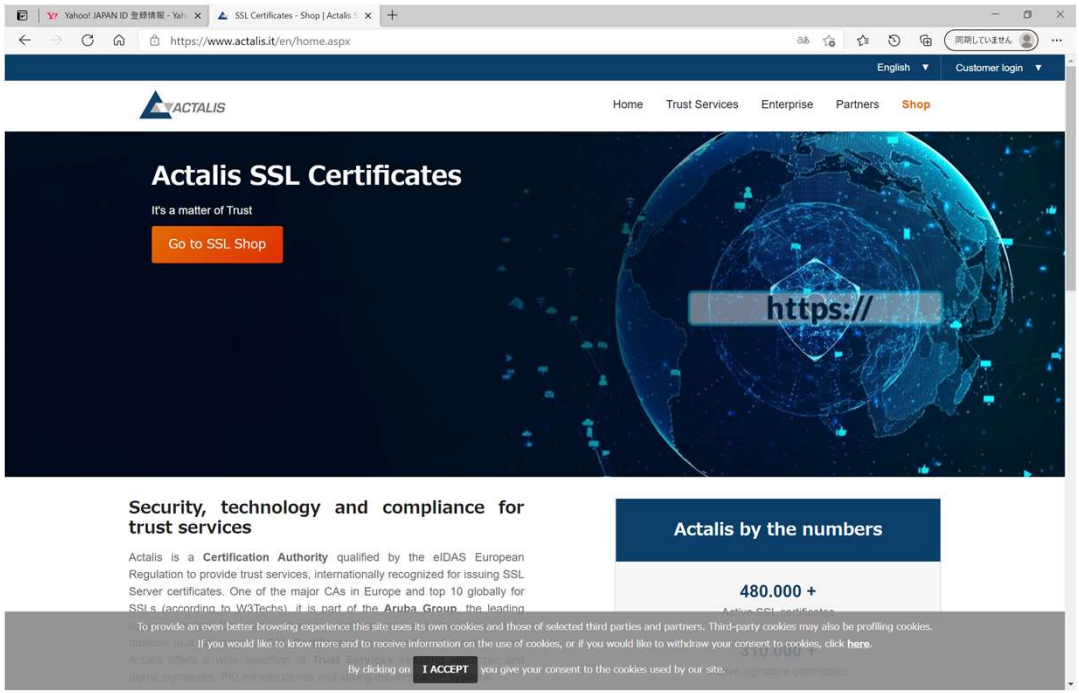


無料の公開鍵証明書

- イタリアのサイトであるActalisでは無料でS/MIMEの電子証明書を手に入れることができる

- https://www.actalis.it/en/home.aspx

にアクセスする。



他に、JCANの1年の有効期間で3850円など廉価なものも

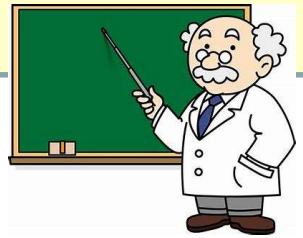
S／MIMEの現状の問題点

① 十分安全な暗号方式を使っているか疑問

② 公開鍵証明書が高価

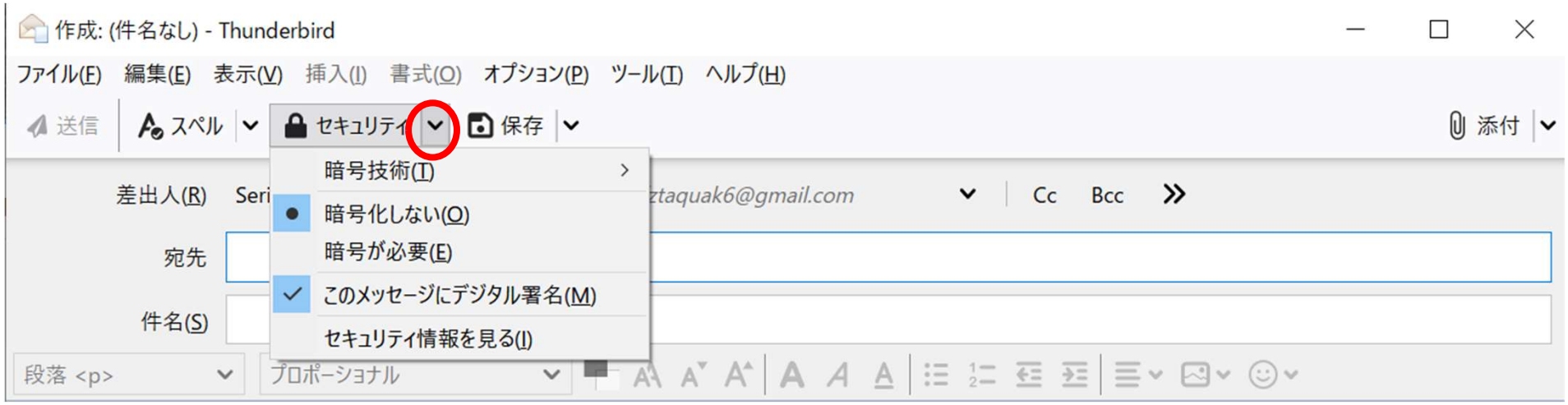
③ 各種メーラのS/MIME互換性が確認されていない。

④ 使い勝手の悪い部分がある



Thunderbirdでの実装

- 実際に使用する際には、メール作成時に、「セキュリティ」右の矢印を押して、「このメッセージにデジタル署名」にチェックを入れるとデジタル署名を、「暗号が必要」に「・」をつけると暗号化がされる。

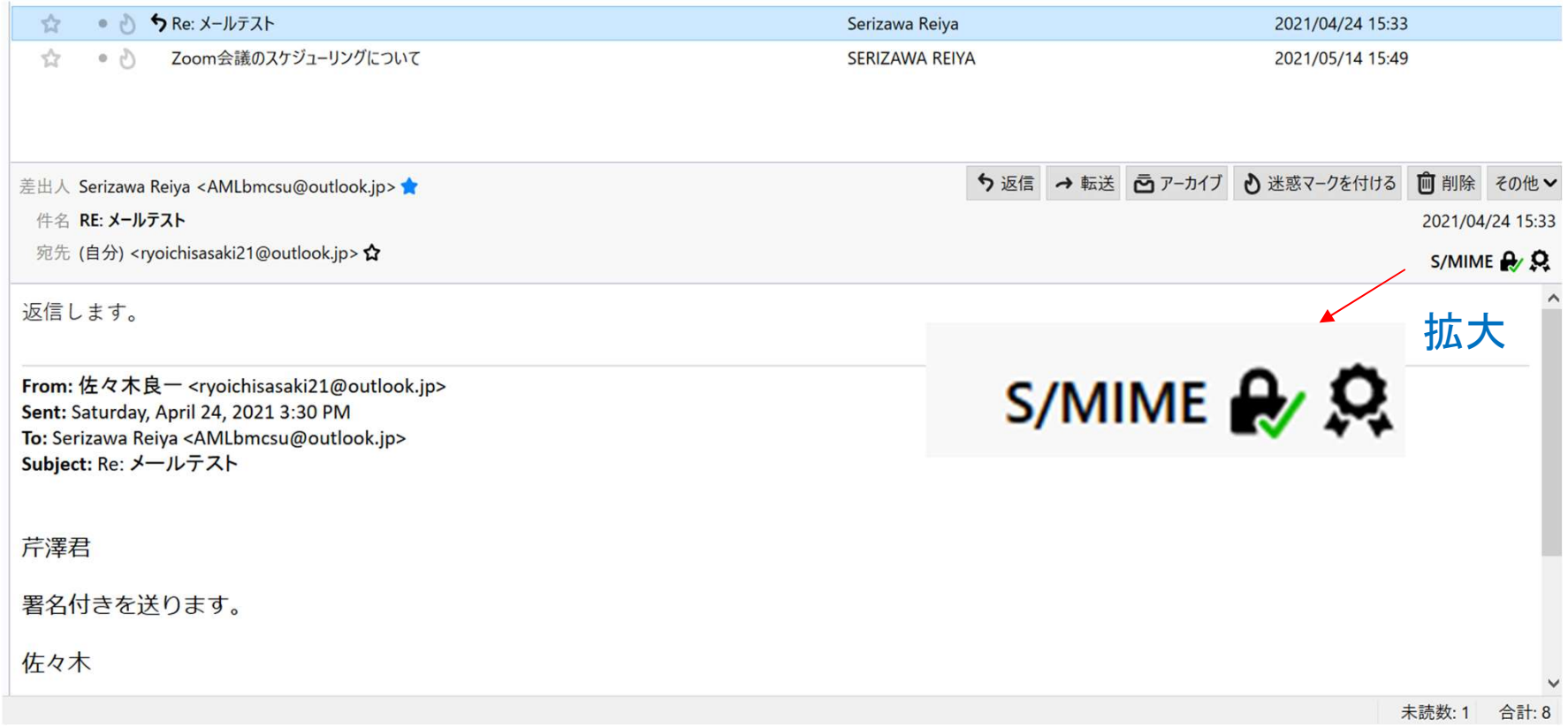


この辺りの操作は簡単

Outlookでの実装

- メール作成時、リボンにある「オプション」をクリックし、「暗号化」にある署名をクリックするとデジタル署名を、暗号化をクリックすると暗号化をすることができる。
- 「署名」や「暗号化」をクリックすると、その背景が濃くなるので、それで署名や暗号化できたか判断できる。

S/MIME署名・暗号メールの受信画面



Thunderbirdの受信画面

S/MIMEアイコンをクリックすると

署名証明書を表示をクリック

Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	E1:9D:61:3F:EE:7C:69:83:1C:DE:33:9A:F6:76:44:E7:AC:1
Miscellaneous	
Serial Number	01:04:1B:D3:29:A1:39:81:4A:AB:3B:9D:55:FF:66:6F
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
ダウンロード	PEM (証明書) PEM (チェーン)

互換性の検討

① 使用したOUTLOOKとThunderbird間では、S/MIME署名ならびにS/MIME暗号化とも基本的操作では互換性がある

② これらの確認はS/MIMEv3までであり、v4の実装状況については不明

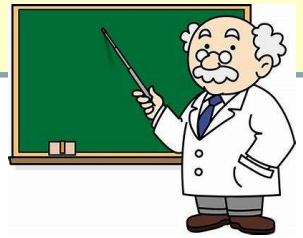
S／MIMEの現状の問題点

① 十分安全な暗号方式を使っているか疑問

② 公開鍵証明書が高価

③ 各種メーラのS/MIME互換性が確認されていない。

④ 使い勝手の悪い部分がある



S/MIMEの使い勝手の悪さ

(a)S／MIME暗号化において、暗号メール送信先の公開鍵がわからず暗号化できないときがある。

(b)公開鍵証明書の有効期間が過ぎると、実装によっては復号できない場合がある

(c)送られてきたメールを転送すると転送先で読めないなど

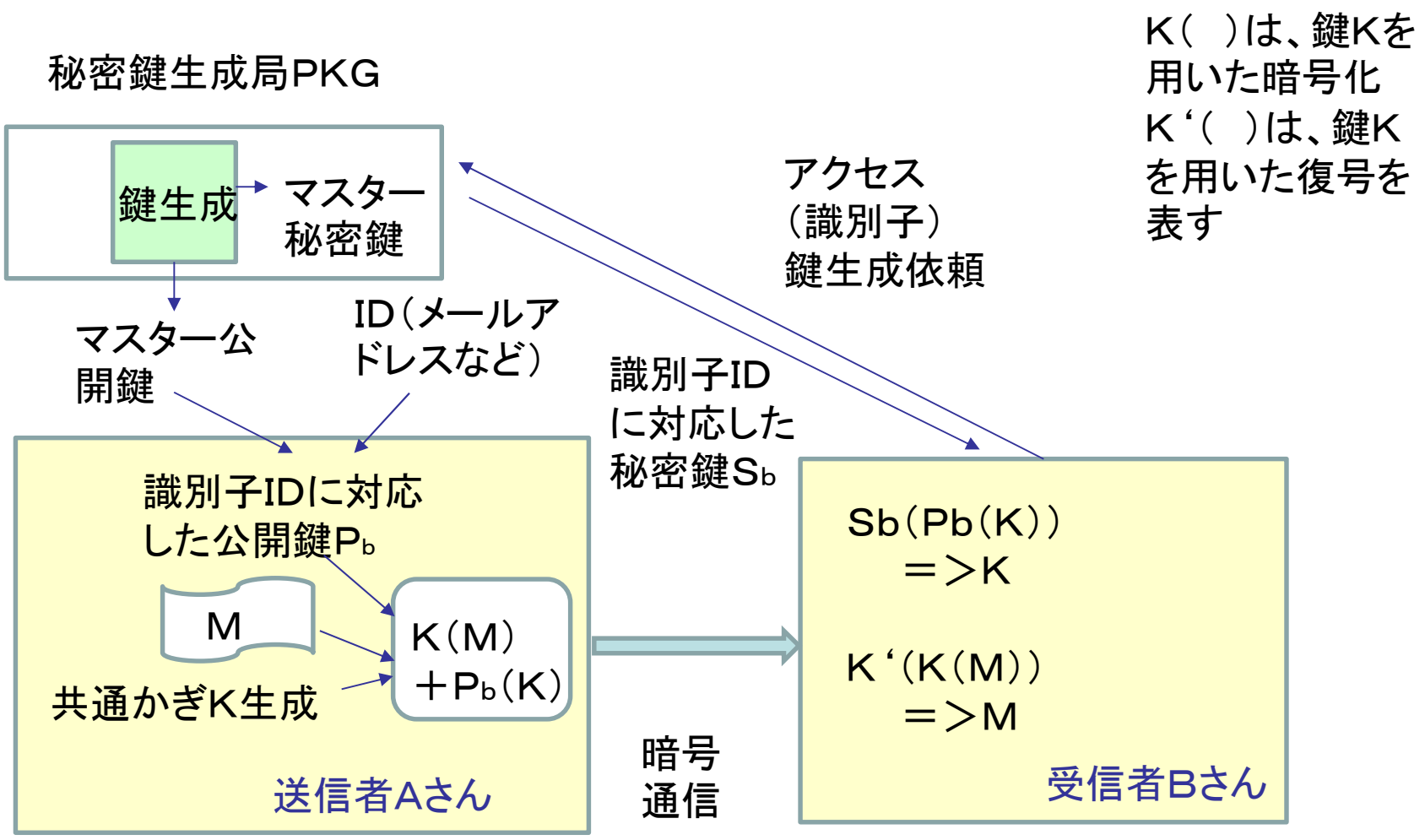
送信先の公開鍵暗号の容易な入手法案

（1）IDベース暗号を用いて、相手の公開鍵を入手する方法
　　＝＞IDベース暗号の実装自体がかなり複雑なのと、鍵生成局への十分な信頼が不可欠という問題がある。

（2）送信先に公開鍵証明書要求特殊メールを送り、このメールが来ると、自動的に公開鍵証明書を返送する機能を持たせる　＝＞この機能を悪用して情報を抜き出されないか十分な検討必要。

（3）S/MIME署名付きのメールを送るのを文化とする。また、送信者Aさんから、公開鍵証明書が欲しいとのメールがBさんに送れれたらS／MIME署名付きメールを返送するのを文化とする。

IDベース暗号の仕組み



送信先の公開鍵暗号の容易な入手法案

（1）IDベース暗号を用いて、相手の公開鍵を入手する方法
　　＝＞IDベース暗号の実装自体がかなり複雑なのと、鍵生成局への十分な信頼が不可欠という問題がある。

（2）送信先に公開鍵証明書要求特殊メールを送り、このメールが来ると、自動的に公開鍵証明書を返送する機能を持たせる　＝＞この機能を悪用して情報を抜き出されないか十分な検討が必要。

（3）メールの送信は）S/MIME署名付きで送るのを文化とする。また、送信者Aさんから、公開鍵証明書が欲しいとのメールがBさんに送れれたらS／MIME署名付きメールを返送するようにする。

S/MIMEの使い勝手の悪さ

(a)S／MIME暗号化において、暗号メール送信先の公開鍵がわからず暗号化できないときがある。

(b)公開鍵証明書の有効期間が過ぎると、実装によっては復号できない場合がある

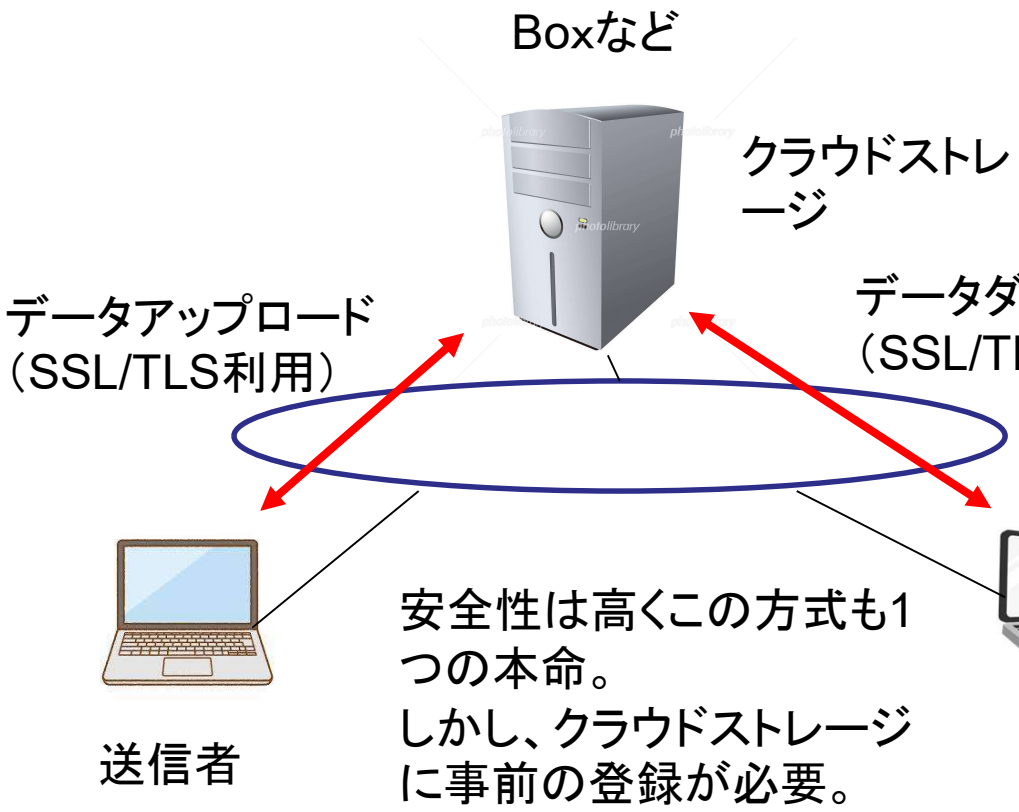
(c)送られてきたメールを転送すると転送先で読めない　など

送られてきた暗号文は、平文化して管理するようにする
（新しい標準化が必要になるか）

目次

クラウドストレージを用いる方式

クラウドストレージを用いてファイルを共有する方式の改良版を検討してみた



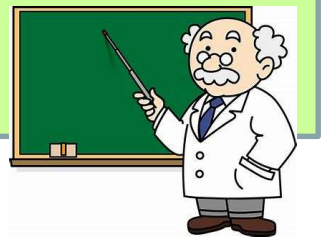
SSL/TLSの概要
①クラウドサーバの公開鍵証明書を送信
②公開鍵暗号を用いて、共通かぎを共有
③　データの送信

目次

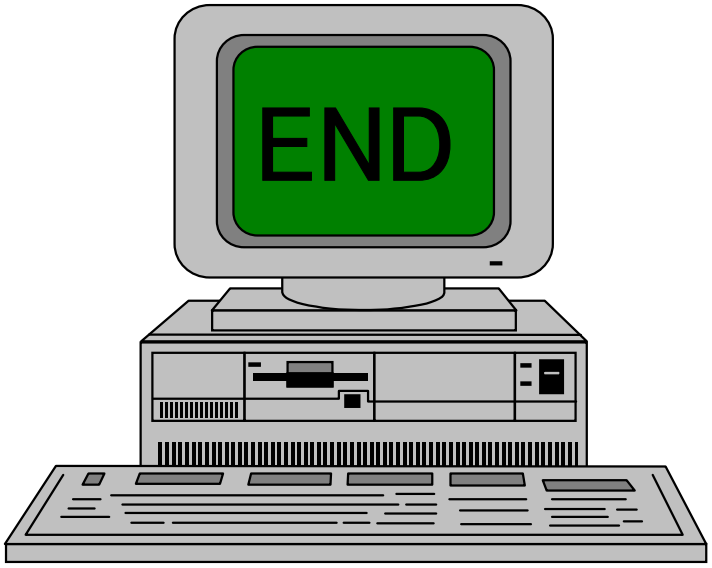
今後必要な研究

1．S/MIME中心で検討する場合
　（a）各種ユーザによるS/MIME実用実験の実施
　（b）RPAを用いたS/MIME簡易利用支援ツールの開発

2．クラウドストレージ中心で検討する場合
　　実装されているサービスの調査など



RPA（Robotic Process Automation）


END

電子証明書無料サイト

1. Thawte Inc.は、デジタル証明書のプロファイルに一部制限があるものの、メール(S/MIME)に無料で利用できる「Personal E-mail Certificates」を提供している。
https://www.atmarkit.co.jp/fwin2k/win2ktips/647freeca/freeca01.html

2. マイナンバーカード
https://www.kojinbango-card.go.jp/jpki/

S/MIMEソフト

ホスト型 S/MIME を有効化してメールの安全性を高める - Google Workspace 管理者 ヘルプ

代替案

1．オンラインストレージ利用型

(1) Smooth File
DAPP（**Device-Authenticated Password Protocol**）利用

https://www.smoothfile.jp/lp/dapp/?gclid=CjwKCAjw-e2EBhAhEiwAJI5jg2kj_o8BcRWbRukmqv74EQpyak9XU5ogOdX3AuHmJmKtTCmA5juYkxoCRgYQAvD_BwE

(2) オンラインストレージ＋SSLベースの暗号化
これは1つの行き方