Information Security Laboratory
ISL

JIPDEC
S/MIMEセミナー講演

30分
Rev.3
2022年2月18日

PPAP廃止に関する動向と対策案の検討

東京電機大学
研究推進社会連携センター
顧問・客員教授
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（という）
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

（注）以降パスワードのことを鍵という場合もある。

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

FaceBookのグループ

くたばれPPAP！

公開グループ・メンバー1,301人 ⇨ 2022年1月6日現在 1424人

PPAPのメリットといわれているもの

① 誤送信対策効果がある

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 ＝＞勘違いして系統的に間違う危険があり効果小

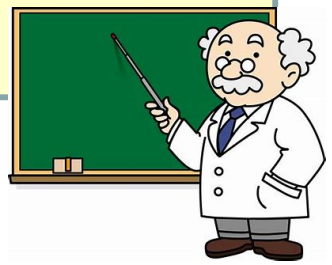
② 盗聴防止効果がある

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 いろいろな条件下で特別の手間なしに利用可能

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。 ＝＞この効果は思いのほか大きい



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

被害を受ける確率の計算式

PT：通信内容が明らかになる確率

$PT=P(A\cap B)=P(A)P(B|A) \fallingdotseq P(A)$ ――（1）

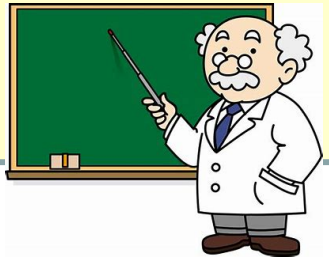
なぜなら、$P(B|A) \fallingdotseq 1$

（Aが成立するときBも同時に成立する）

A：メールの送信中に暗号文に不正アクセスされる

B：メールの送信中に鍵を不正アクセスされる

（鍵と暗号文があれば復号可能）



PPAPの問題点

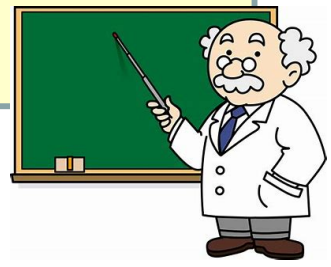
① セキュリティ向上の効果がほとんどないにもかかわらず手間がかかることを強制的にやらされる。しかも

(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 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している。



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

PPAPの問題点

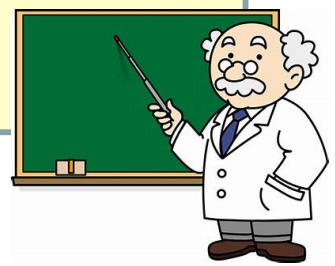
① セキュリティ向上の効果がほとんどないにもかかわらず手間がかかることを強制的にやらされる。しかも

(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 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している問題がある。＝＞ワクチンプログラムを改良すれば対応可能だが現状では問題。



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

- 平井卓也前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/

他の官庁や日立などの企業においても同様な動き。しかし、それに代わる方式については合意が取れているとは言えない。

目次

対策案の比較

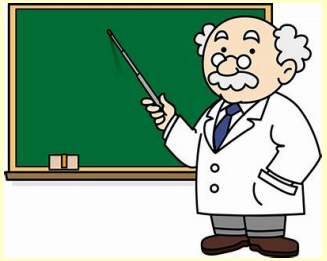
対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME署名	③S/MIME暗号化	④CS利用（ACなし）	⑤CS利用（ACあり）
			現状版	②SMSで鍵配送	組み合わせ			
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	—	○	—	—
	鍵配送の安全性	—	X	△	—	○	—	—
	認証機能	X	X	X	○	—	X	○
ウイルスチェックが可能		○	X	X	○	○	○	○
使い勝手（ユーザの手間）		○	△	△	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Control アクセス制御

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○）



PT＝P(A)

A:メールの送信中に通信内容にアクセスされる

メールサーバ間でリンクバイリンクの暗号化をするメールシステムが増えているので思いの外安全性があるが、やはり望ましい方式とはいえない。

ただし、機密性が低いファイルに対してはこの方式もありうる。

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME署名	③S/MIME暗号化	④CS利用（ACなし）	⑤CS利用（ACあり）
			現状版	②SMSで鍵配送	組み合わせ			
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	—	○	—	—
	鍵配送の安全性	—	X	△	—	○	—	—
	認証機能	X	X	X	○	—	X	○
ウイルスチェックが可能		○	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	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Control アクセス制御

対策案(2)

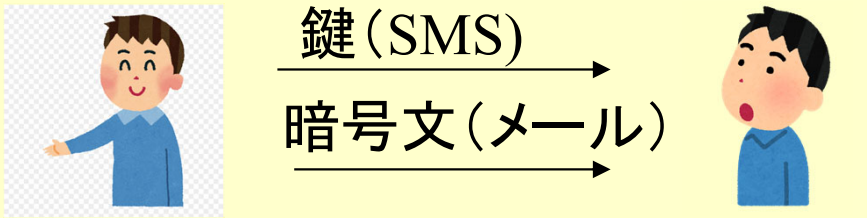
② メールに添付されるファイルを暗号化し、鍵をSMSなど別ルートで送る。＊ （安全性 △～○：使い勝手△）

PT=P(A∩B)≒P(A)P(B) （∵ AとBの独立性が高いので）

A：メールの送信中に暗号化した通信文に不正アクセスされる

B： SMSの送信中に鍵に不正アクセスされる

ウイルスチェックができない
という問題がのこる



＊ファイルだけでなく、メール自体の暗号化も実施することが望ましい。

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME署名	③S/MIME暗号化	④CS利用（ACなし）	⑤CS利用（ACあり）
			現状版	②SMSで鍵配送	組み合わせ			
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	—	○	—	—
	鍵配送の安全性	—	X	△	—	○	—	—
	認証機能	X	X	X	○	—	X	○
ウイルスチェックが可能		○	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	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Control アクセス制御

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

IETF：Internet Engineering Task Force

S/MIME利用のイメージ

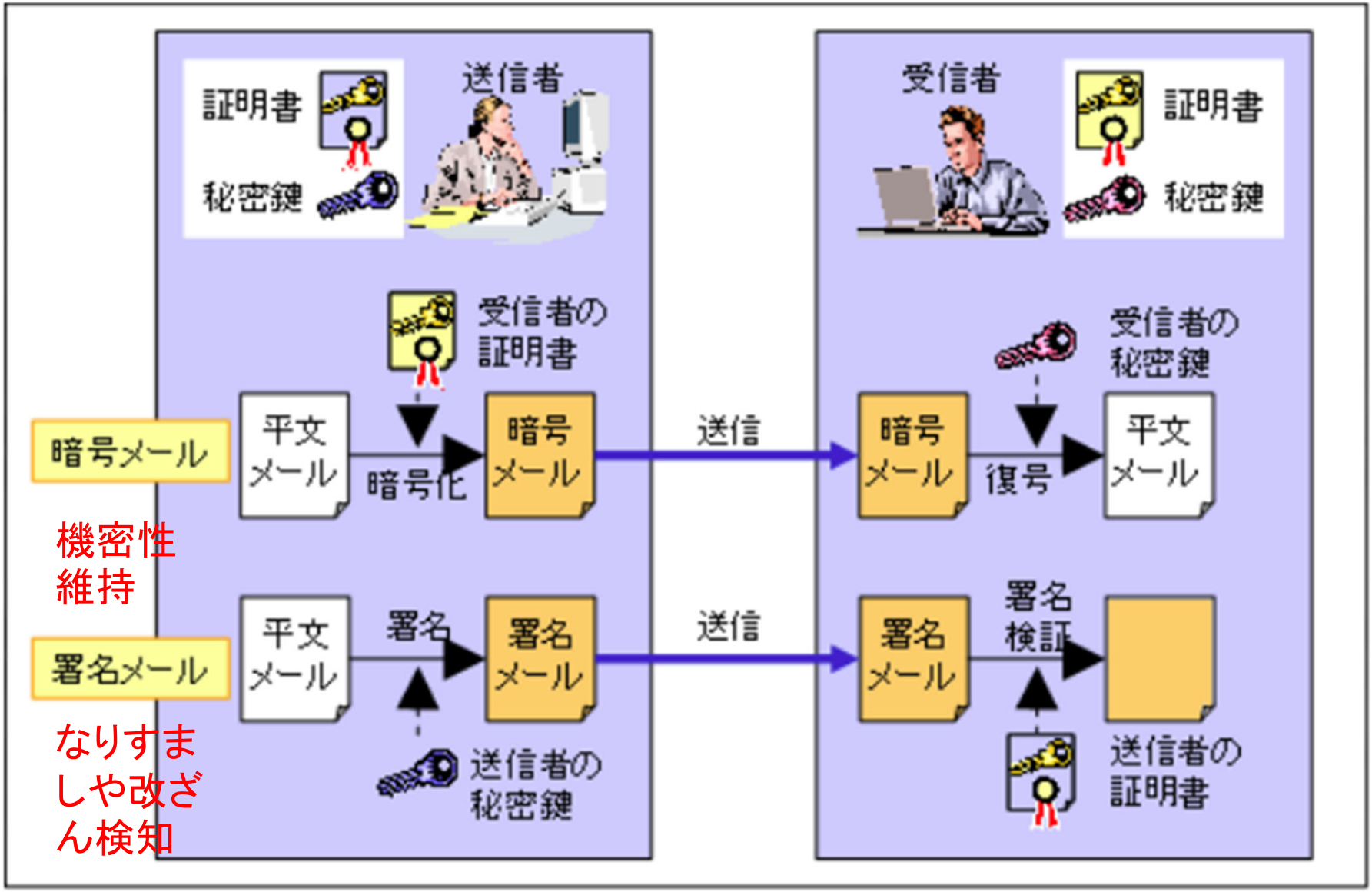
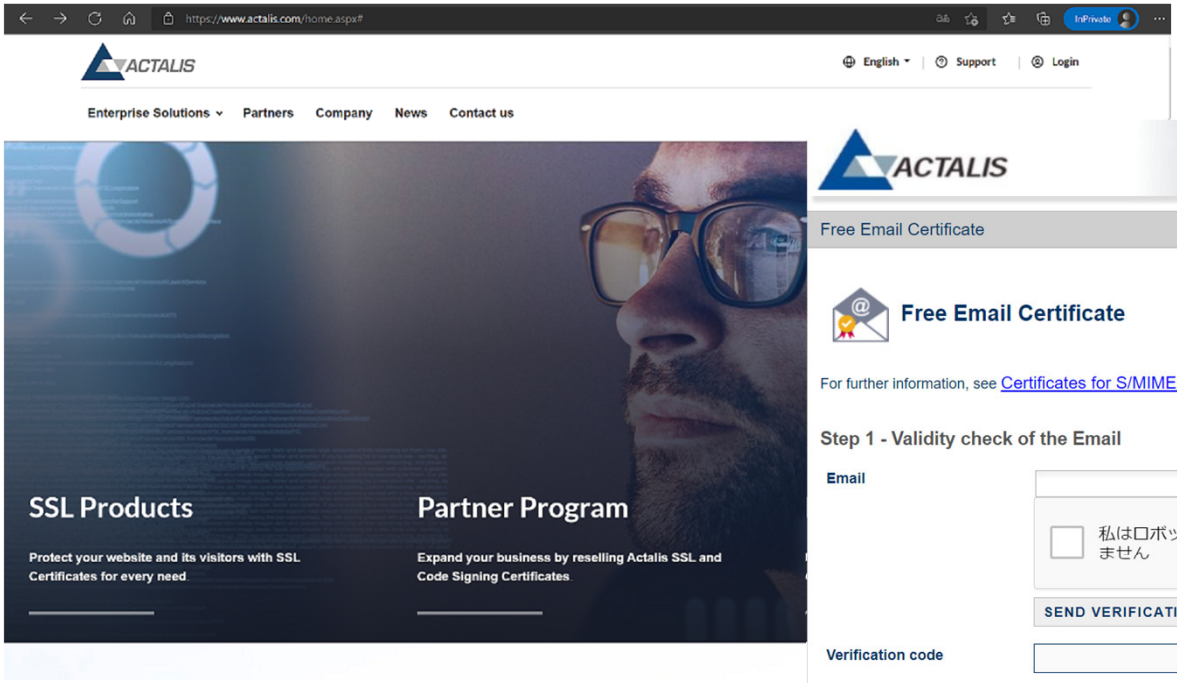
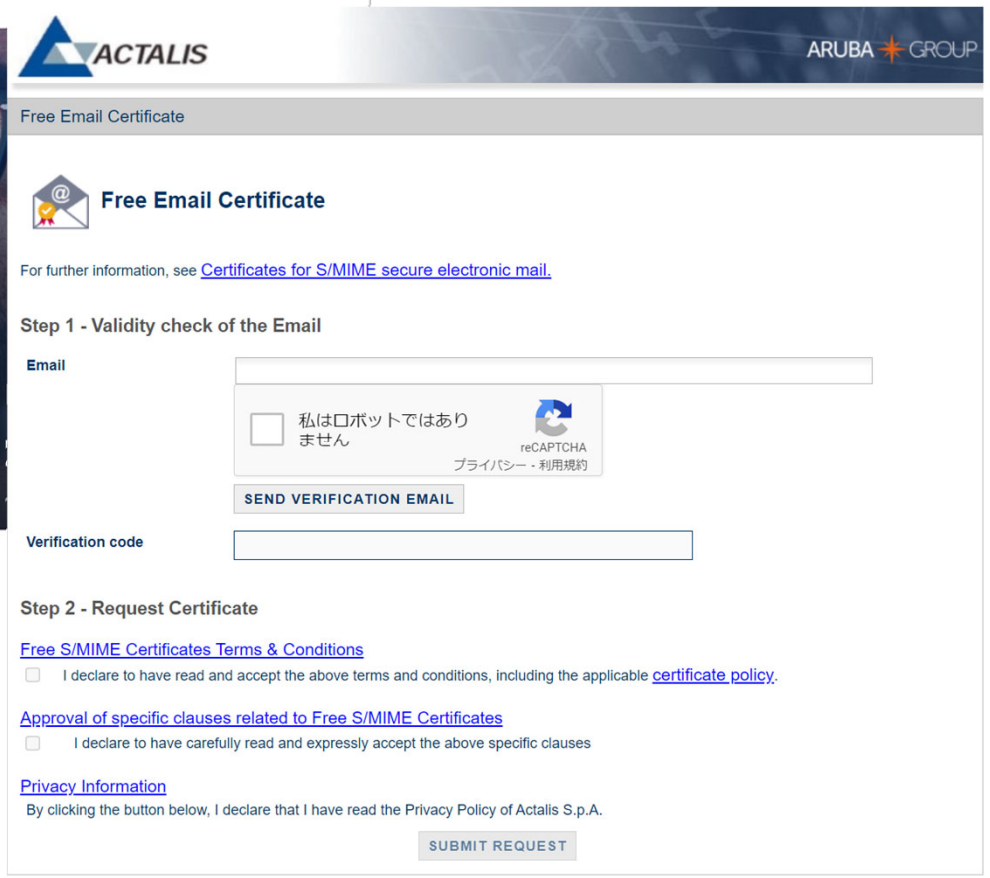


図1：S/MIMEの利用イメージ（出典：IPA「情報セキュリティ - S/MIME」）

電子証明書の入手

① 認証局にアクセスする。例えば無料の証明書を発効する
https://www.actalis.it/en/home.aspx などへアクセス

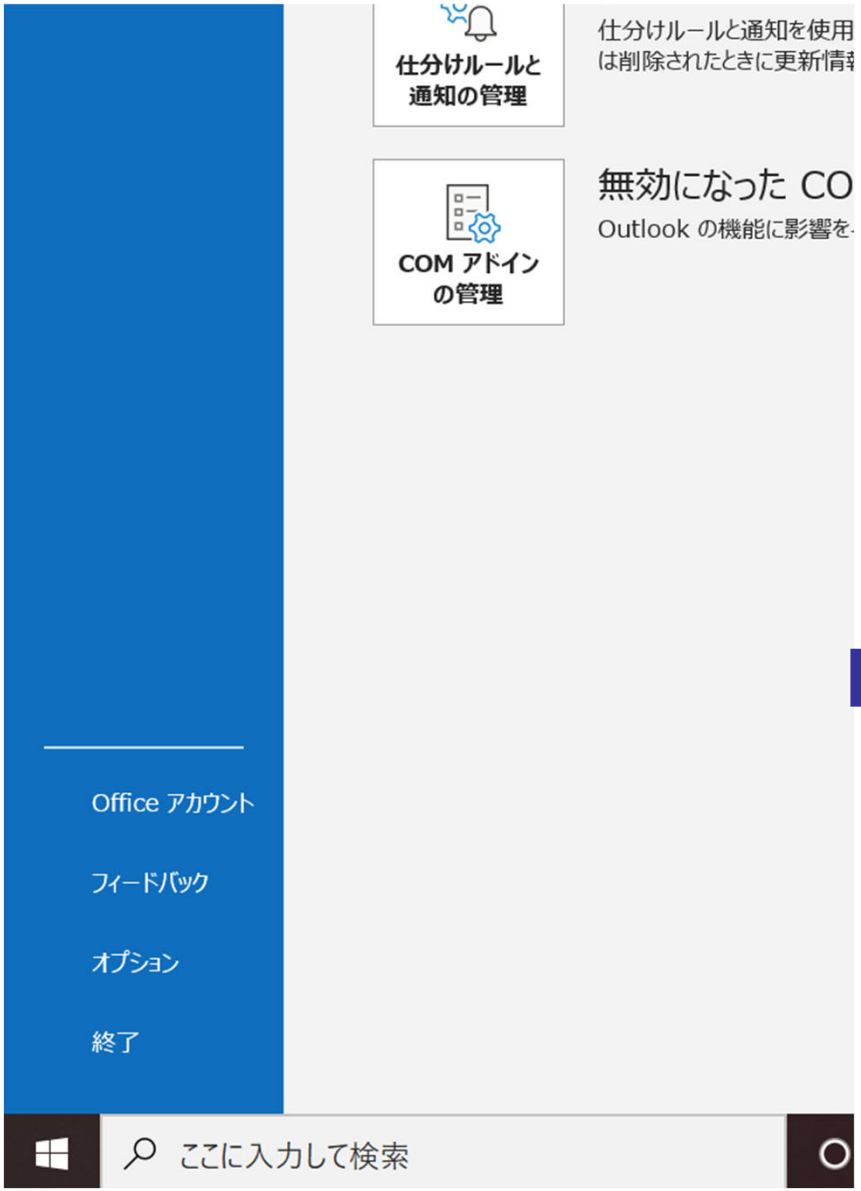




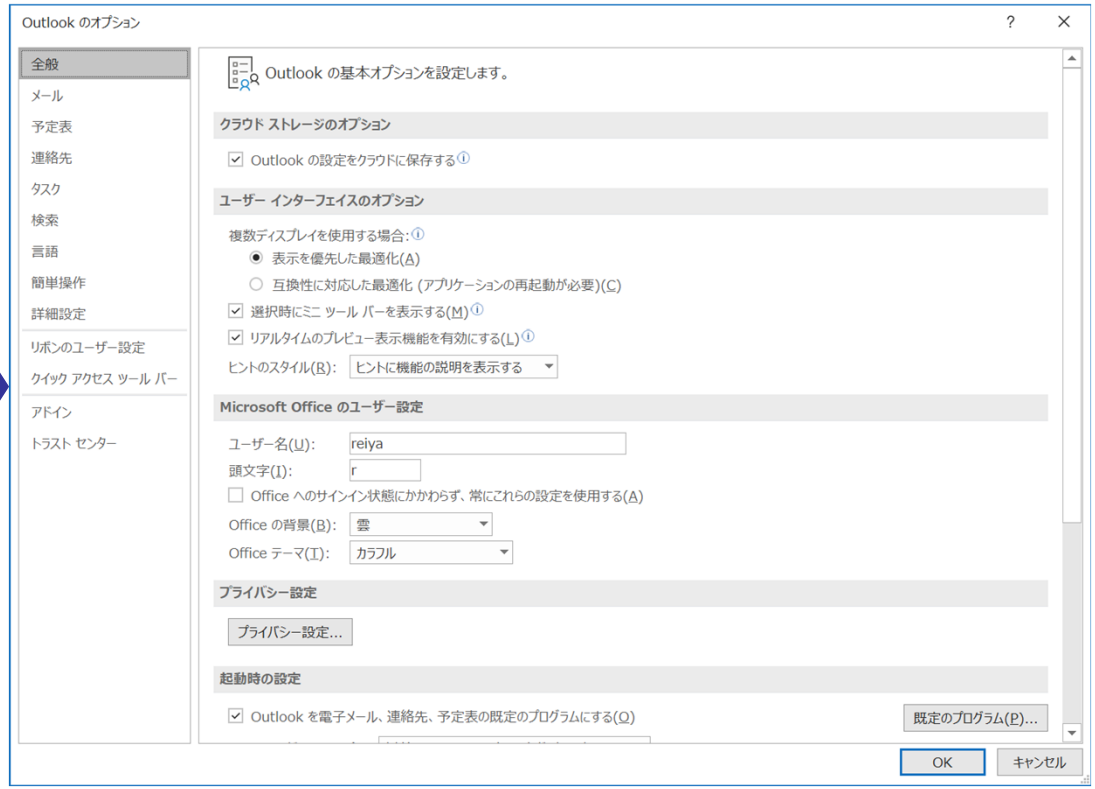
② 証明書を入手するための種々の処理

慣れない人にとって容易ではない

Outlookでの証明書のセットアップ



- 上にある「ファイル」タブから左下の「オプション」をクリックして「Outlookのオプション」ウィンドウを開く。



慣れない人にとって容易ではない

Outlookで署名や暗号化をする

Outlookの画面

署名や暗号化の処理は、アイコンをクリックするだけなので、だれにでも比較的容易に実施可能

S/MIME利用のイメージ

暗号化するには、相手の証明書の中の公開鍵が必要なので、実際には、①双方で署名メールを送りあい、相手の証明書が自分のメーラにセットされたのち、②暗号メールを送るとので少し手間がかかる。

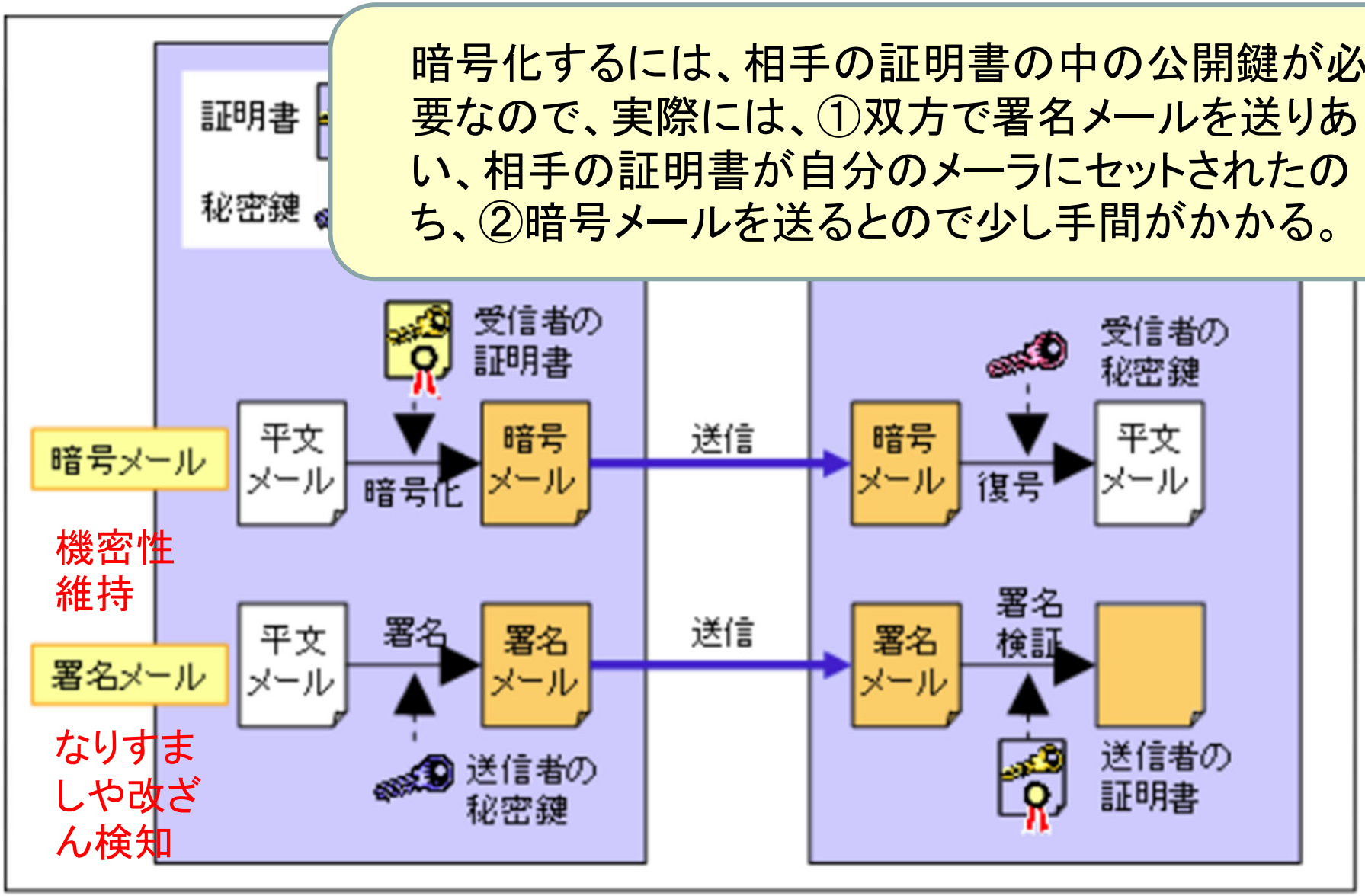


図1：S/MIMEの利用イメージ（出典：IPA「情報セキュリティ - S/MIME」）

S/MIMEのバージョン

（1）S/MIME は、v2とv3、v4が存在。v2,v3は脆弱な暗号アルゴリズムが使われており、v4が必須と考えられる。

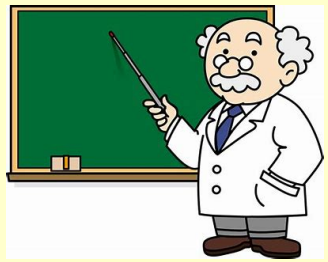
（2）v4は、ハッシュ関数としてSHA-256，SHA512

署名は、RSA　PKCS＃1　v1.5　with　SHA-256

ECDSA with curve25519 P-256, SHA-256 など

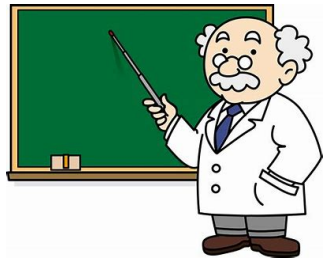
暗号化は　AES-128、AES-256など

鍵配送には　ECDHなど



https://datatracker.ietf.org/doc/html/rfc8551#page-12

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る。＊

② S/MIME署名によって本人性と通信文の非改ざん性が確保できる＊＊。

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。

＊End―Endの暗号化により運用者であってもこの内容を知ることはできない
＊＊標的型攻撃などのかなりの部分が防止できこの期待効果は大
もちろん、鍵管理をしっかりやるとともに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。

S／MIMEの現状の問題点

① 公開鍵証明書入手のコストが大

② 各種メーラのS/MIME互換性が確認されていない。

③ WebメールでS/MIMEを利用できるものが少ない

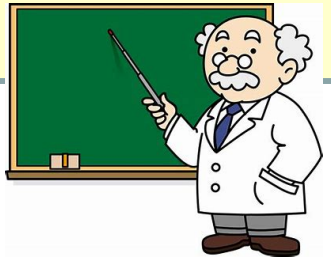
④ 使い勝手の悪い部分がある

（a）公開鍵証明書の入手がIT初心者には困難

（b）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。

（c）同報と暗号化を同時に行おうとすると手間がかかる

など



S/MIMEの評価

安全性　○　　使い勝手　X

メールベースでやるならこの方式が本命、使い勝手などの見直し必要

目次

メール以外のコミュニケーション手段

1. クラウドストレージ（Boxなど）
2. ビジネスチャット（Slackなど）
3. WEB会議（Zoomなど）
4. IRM(Rights Management Services)他

メールなど使わなくてもいいではないかという意見も

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME署名	③S/MIME暗号化	④CS利用（ACなし）	⑤CS利用（ACあり）
			現状版	②SMSで鍵配送	組み合わせ			
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	—	○	—	—
	鍵配送の安全性	—	X	△	—	○	—	—
	認証機能	X	X	X	○	—	X	○
ウイルスチェックが可能		○	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	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Control アクセス制御

④ ACなしのCS利用リスク評価（1）

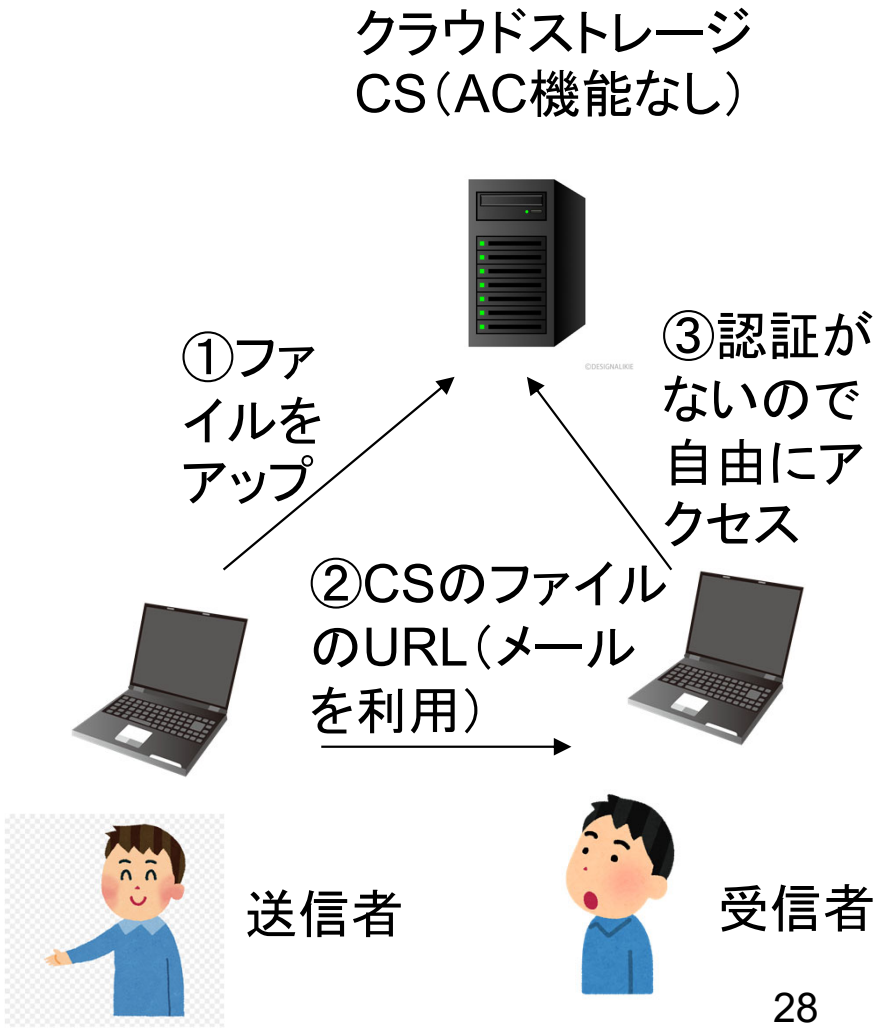
正規の手順

① 送信者はCSに送信したいファイルをアップ
（ファイルのあり場所のURLなどを入手）

② 送信者はCSのファイルのURLを受信者にメールで送信

③ 受信者は、AC機能がないのでCSにアクセスして、ファイルを入手

（CSと送信者PC間はTLSなどで暗号化）

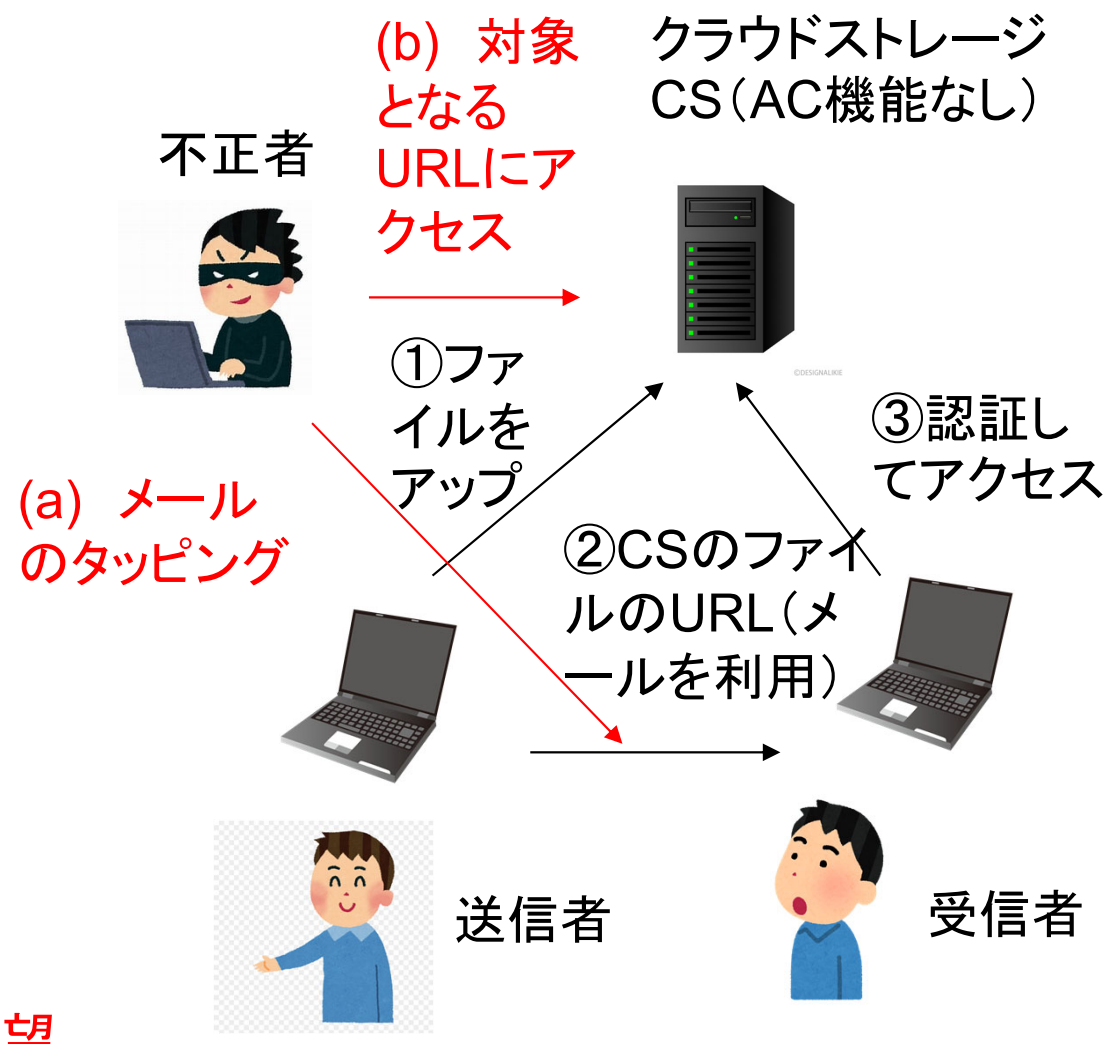


TLS: Wudqvsruw#Od|hu#Vhfxulw

④ ACなしのCS利用リスク評価（2）

＜攻撃方法＞
(a)不正者が送信中のメールにタッピング
(b)CSにアクセスを試行

＜評価＞
(1) メールのタッピングによりCSのURLがわかれば、アクセス制御がないのでCS内のファイルに容易にアクセス可能



安全性 X　使い勝手 ○
機密性の高いファイルに対しては望ましい方式とは言えない

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME署名	③S/MIME暗号化	④CS利用（ACなし）	⑤CS利用（ACあり）
			現状版	②SMSで鍵配送	組み合わせ			
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	—	○	—	—
	鍵配送の安全性	—	X	△	—	○	—	—
	認証機能	X	X	X	○	—	X	○
ウイルスチェックが可能		○	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	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Control アクセス制御

⑤ ACありのCS利用リスク評価（1）

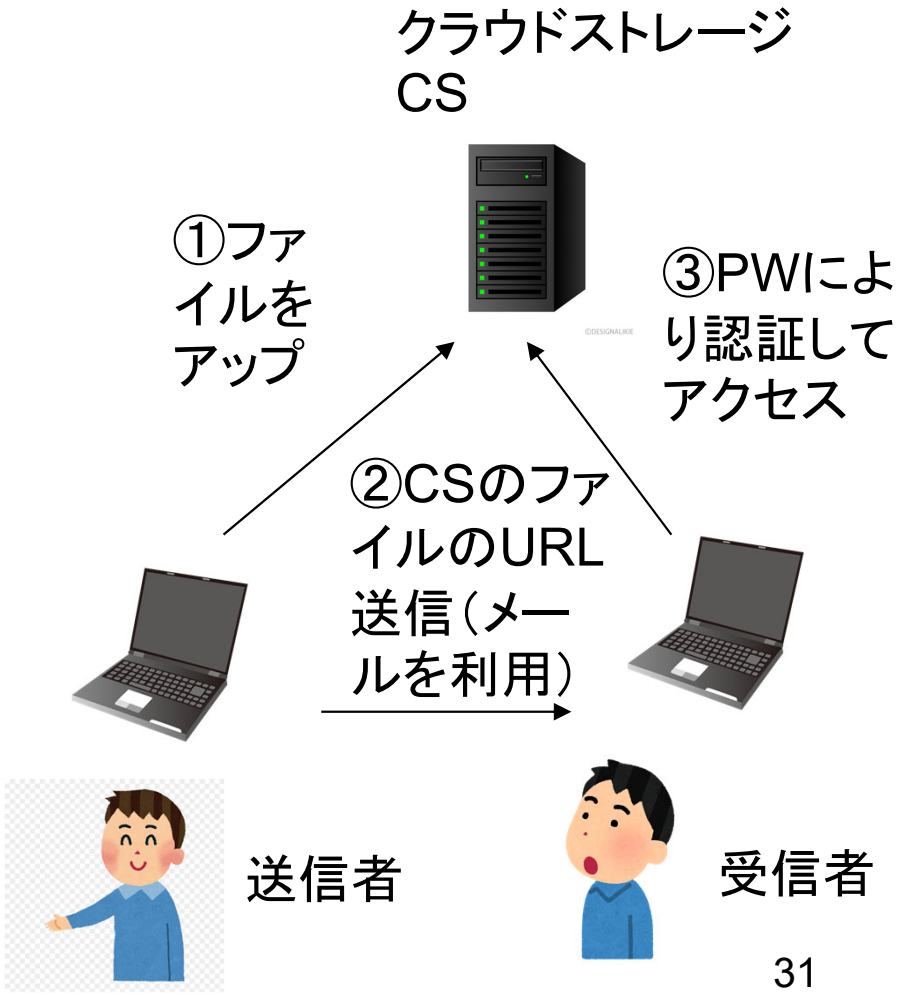
正規の手順

① 送信者はBoxのような機能を持つCSに送信したいファイルをアップロード（ファイルのあり場所のURLなどを入手）

② 送信者はCSのファイルのURLを受信者にメールで送信

③ 受信者は、BoxなどのCSにPWを入力してアクセスし、ファイルを入手

（CSと受信者PC間はTLSなどで暗号化）



⑤ ACありのCS利用リスク評価（2）

ケース1：メール受信者がメールアドレスに対応してPWなどの認証手段をCS向けにすでに確立している場合

＜攻撃方法＞

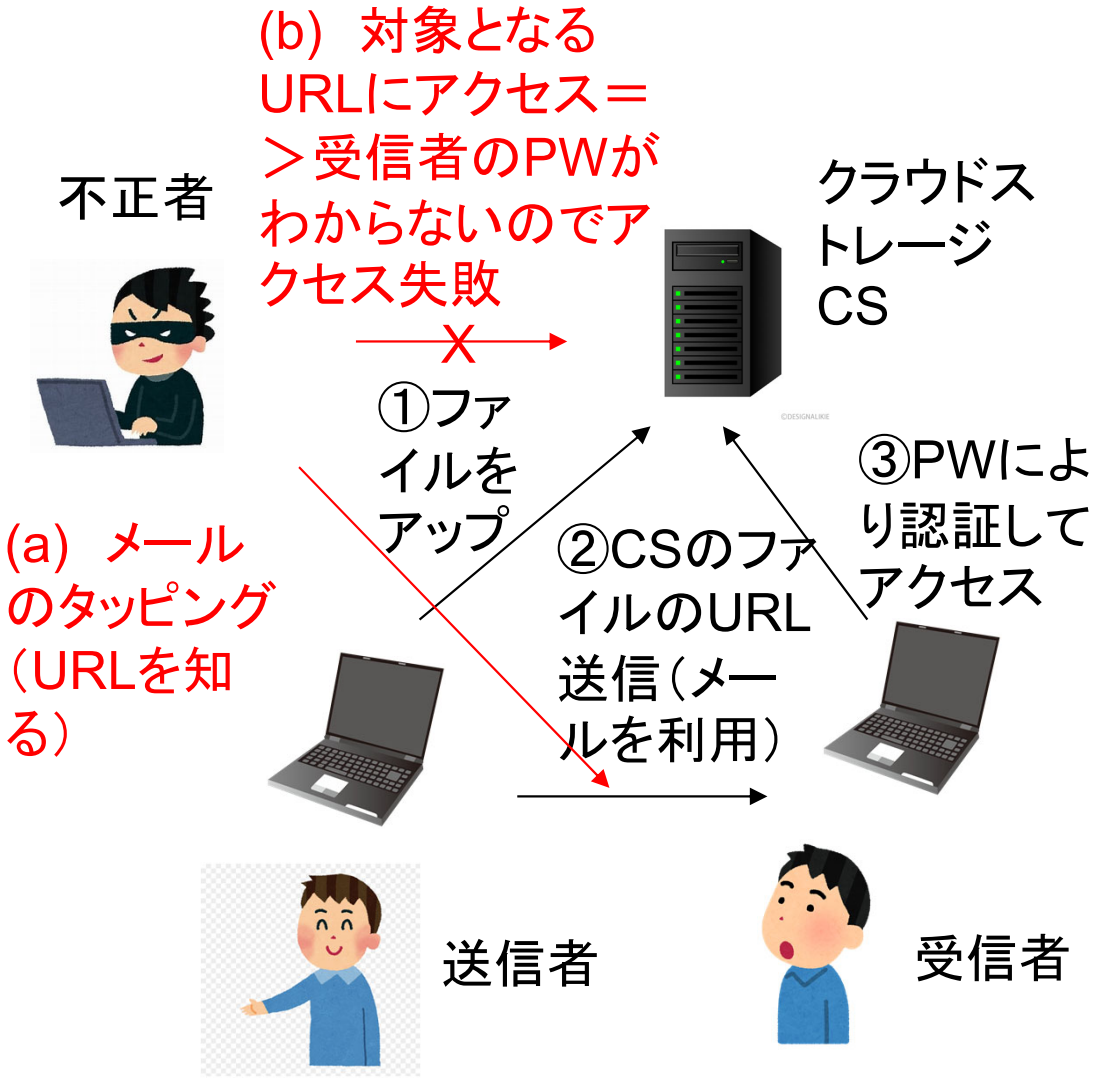
(a) 不正者が送信中のメールにタッピング

(b) BoxなどのCSに不正アクセスを試行

＜評価＞

(1) 受信者が事前に設定しているメールアドレスに対応したPWを不正者が知らないのでアクセスできず安全

(2) PCとCS間は、TLSで暗号化しているので安全

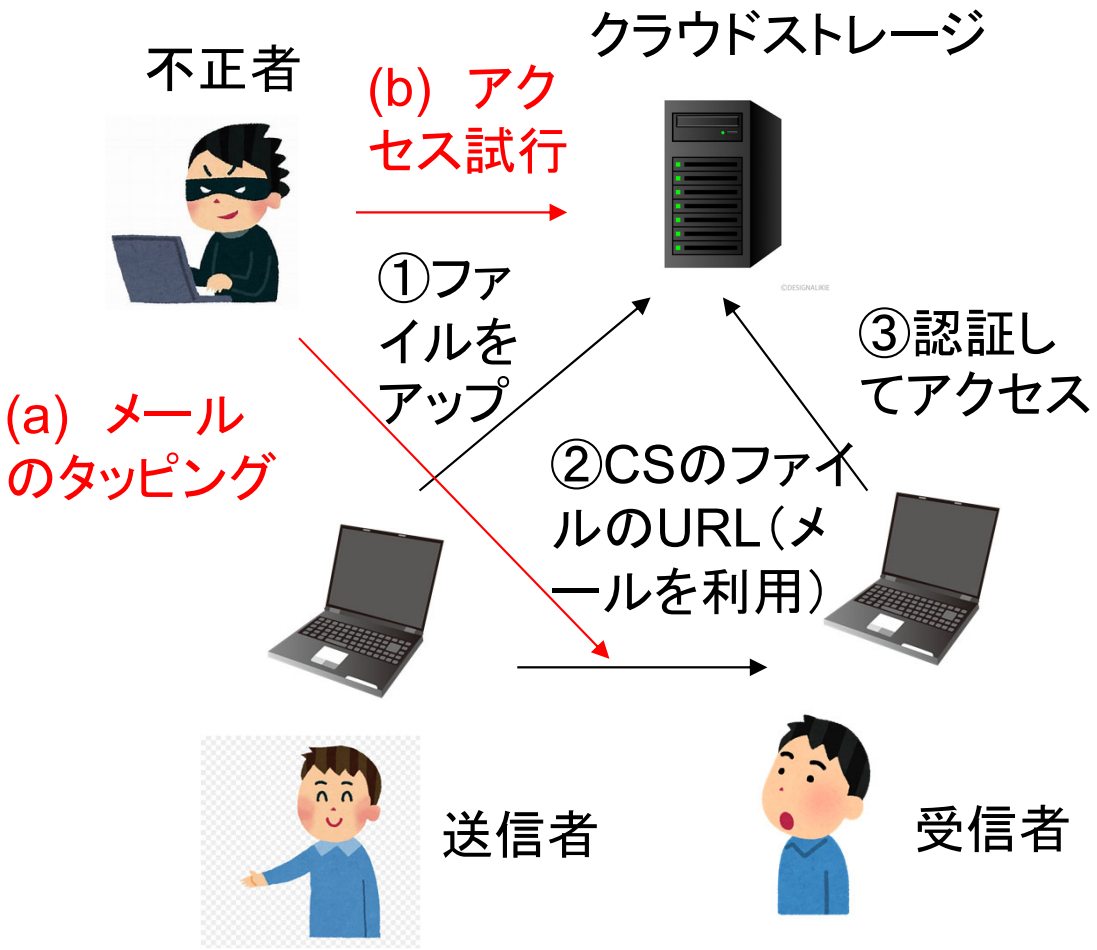


安全性 ○　使い勝手 ○　望ましい方式の1つ

⑤ ACありのCS利用リスク評価（3）

ケース2：メール受信者がメールアドレスに対応してPWなどの認証手段をまだ確立していない場合

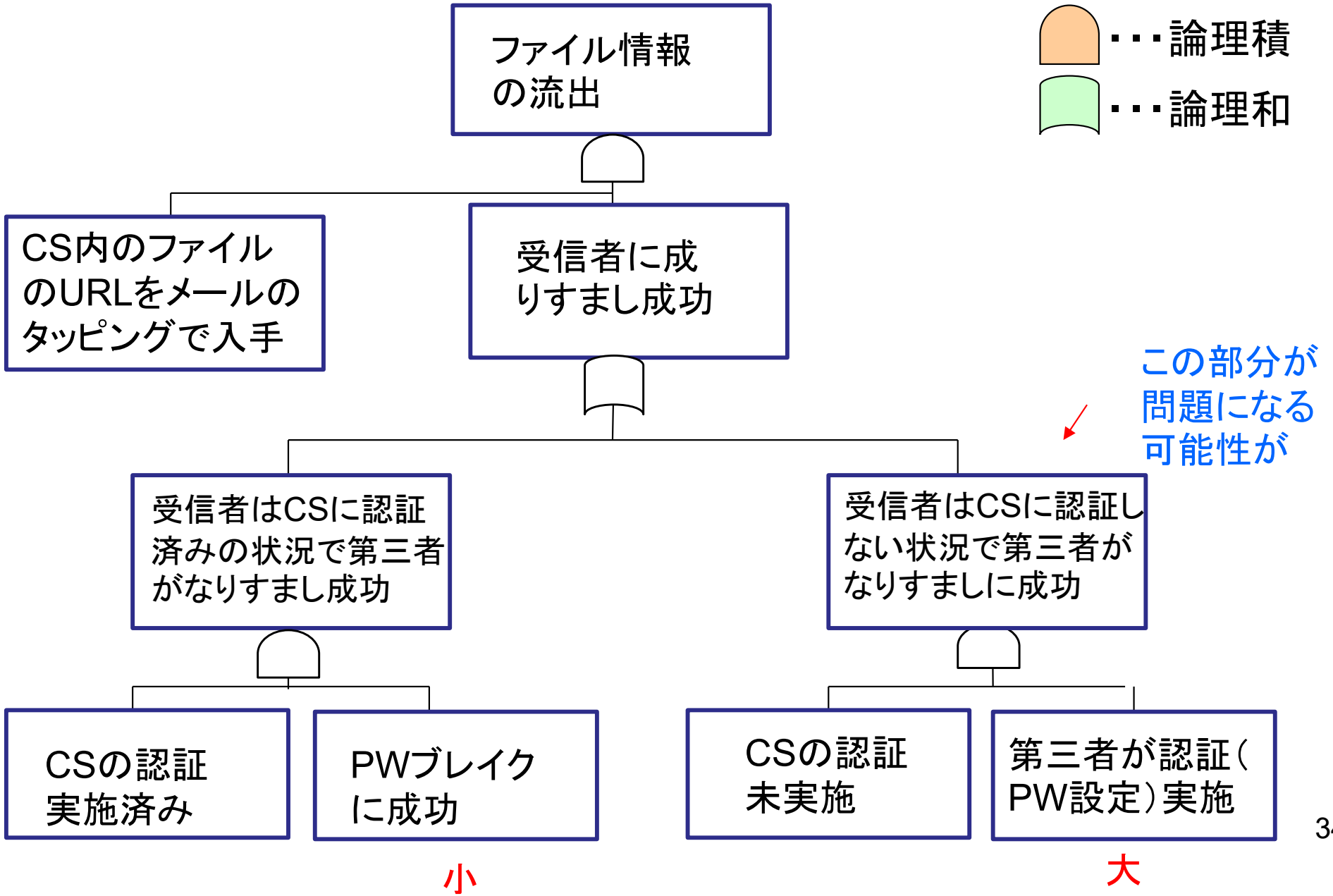
＜攻撃方法＞
(a) 不正者が送信中のメールにタッピング
(b) BoxなどのCSにアクセスを試行
＜評価＞
受信者が事前にメールアドレスに対応したPWを設定してないので、受信者のメールアドレスで不正者が新規にPWの設定が可能である。＝＞大きなリスクが存在



したがって、AC機能付きCS方式を採用していれば安全とは言えない

⇨ 受信者はURLを受け取る前にPW設定するという運用が必要

CSへのアタックツリー分析



目次

コミュニケーションパターンと手段

利用パターン ＼ 作業	定型作業	非定型作業
組織内	クラウドストレージ（Box等） ビジネスチャット（Slack等） IRMなどのAPソフト	メール ビジネスチャット（Slack等） WEB会議（Zoom等）
組織間	クラウドストレージ（Box等） IRMなどのAPソフト メール	メール ビジネスチャット（Slack等） WEB会議（Zoom等）
組織対個人	IRMなどのAPソフト メール	メール メッセンジャー（LINEなど）
個人間	メッセンジャー（LINEなど） メール	メール メッセンジャー（LINEなど）

メールは不要だという人もいるが――。

安全なメールの必要性

1，メールの役割は低下しているが、それでも非定型作業対応のコミュニケーションを中心にして必要性は高い

2．今も、すぐに世界中の誰とでも通信できる中心的手段はメールではないか（メールアドレスがIDとなっている）

S/MIMEをより安全で使いやすいものにしていくニーズはある

S／MIMEの使い勝手上の問題点

＜ユーザ側＞

（a）電子証明書の入手がIT初心者には困難＊

（b）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。＊

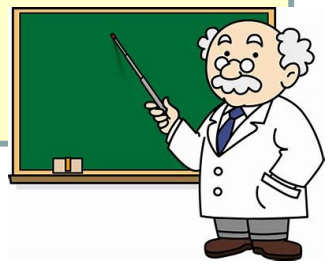
（c）同報と暗号化を同時に行おうとすると手間がかかる

（d）転送などの処理をすると、転送先で読めないなどの問題が

（e）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　など

＜管理者側＞

ユーザからの問い合わせが多い



＊B to Bで使うような場合には、あまり問題にならない

S/MIME利用普及のための解決すべき課題

	課題	対応策
1	公開鍵証明書入手の金銭的コスト	無料や低コストのものもあり普及すれば安く成りうる
2	各種メーラのS/MIME互換性確保の必要性	実装規約の確認と対応
3	WebメールでS/MIMEを利用できないものがある	実装の働きかけ
4	使い勝手の悪さ	使い勝手の向上（次表参照）

上記は利用者向けの検討、管理者向けの検討も必要に

S/MIMEの使い勝手向上策

	課題	対応策
a	公開鍵証明書の入手がIT初心者には困難	証明書の半自動入手機能の実現＊
b	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	希望する相手の公開鍵証明書の自動配布機能の追加など
c	同報と暗号化を同時に行おうとすると手間がかかる	同報と暗号化を同時に行なう機能の実現
d	転送などの処理をすると、転送先で読めないなどの問題が	復号した後、処理をする機能の追加
e	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	アラート機能の実現

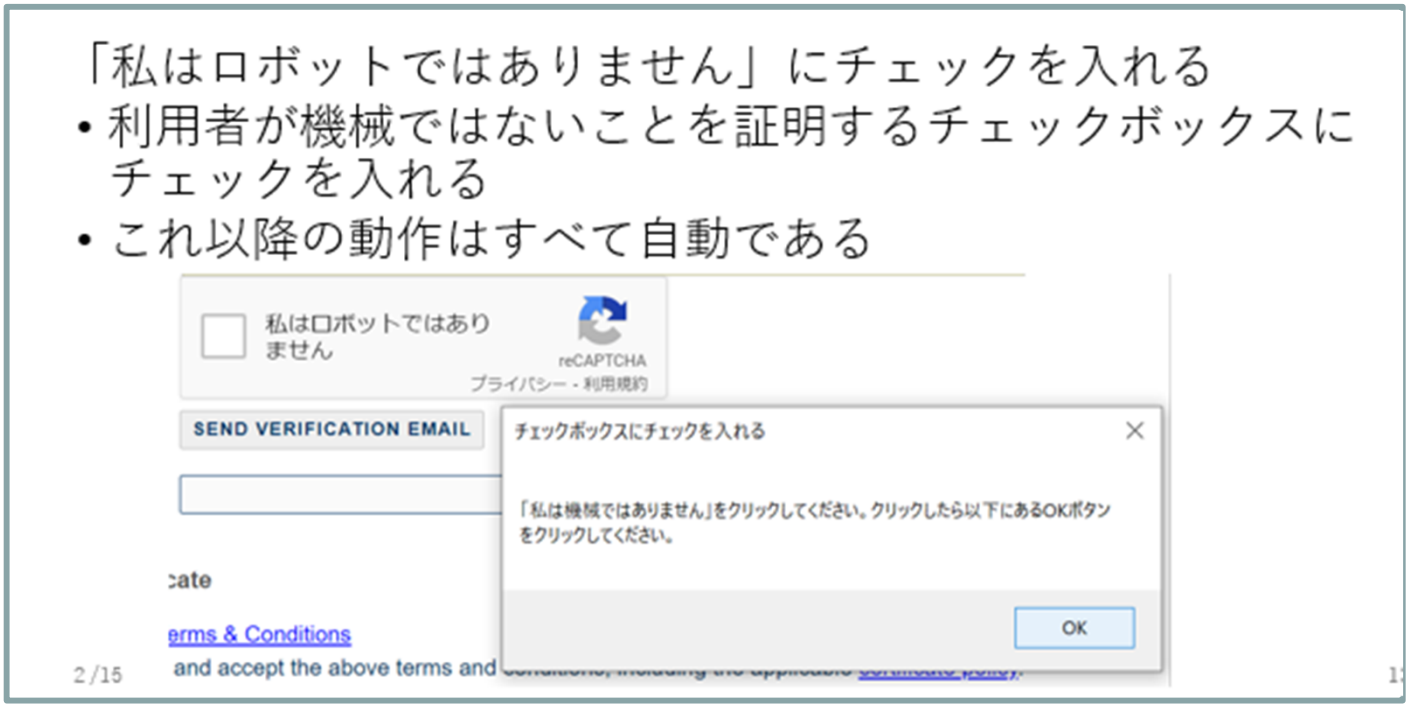
＊ RPA（Robot Process Automation）などを用いた実験を実施

RPAを用いて証明書の（半）自動入手の試み

① マイクロソフトのRPA（Robotic Process Automation）であるPower Automate Desktopのダウンロードをする

② 開発した（半）自動実行のためのテキストファイルを張り付ける

③ ガイドに沿って操作し、半自動で電子証明書をダウンロード



東京電機大学の学生が実行中の研究

S/MIMEの使い勝手向上策

	課題	対応策
a	公開鍵証明書の入手がIT初心者には困難	証明書の半自動入手機能の実現＊
b	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	希望する相手の公開鍵証明書の自動配布機能の追加など
c	同報と暗号化を同時に行おうとすると手間がかかる	同報と暗号化を同時に行なう機能の実現
d	転送などの処理をすると、転送先で読めないなどの問題が	復号して保存する機能の追加
e	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	アラート機能の実現

＊ RPA（Robot Process Automation）などを用いた実験を実施

目次

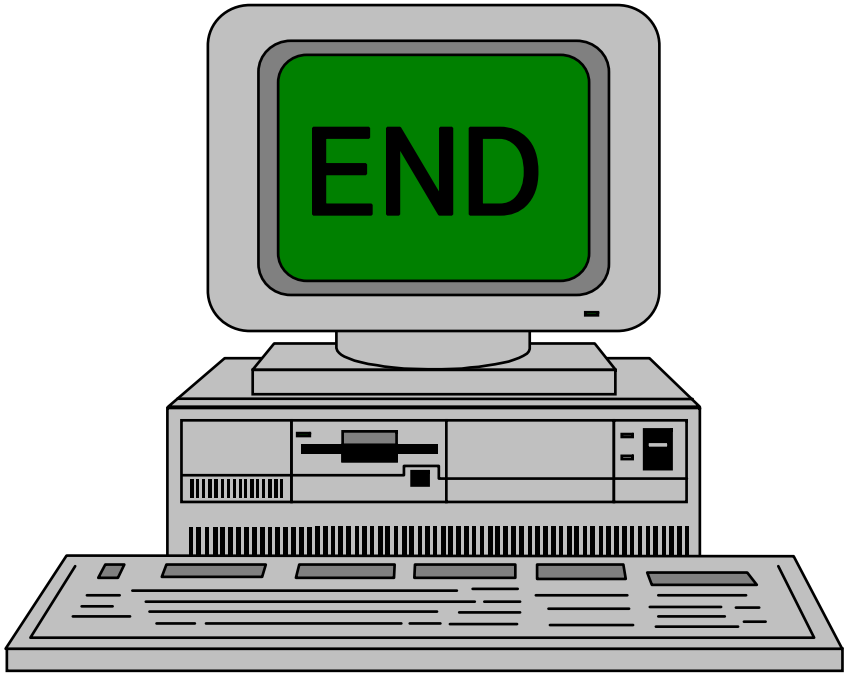
おわりに

① PPAPの問題点を確認。しかし、それに代わるものの合意は取れていない。

② そこで、メールを用いて安全性を高める方式やメール以外の手段を用いて安全性を確保する方式を、安全性と使い勝手の面から比較評価

③ メールを用いて安全性を高める方式の1つであるS/MIMEを用いる方法のニーズを明確にするとともに、その長所と要改善策を明確化

④ 今後は、安全で使いやすいS/MIMEの実装と普及の支援


END

自己紹介

＜現職＞
佐々木良一
東京電機大学
研究推進社会連携センター
顧問・客員教授
名誉教授

＜略歴＞
1971年日立製作所入社。システム開発研究所にて、システム高信頼化技術やセキュリティ技術（1984年より）等の研究開発に従事　同研究所部長や主管研究長兼セキュリティシステム研究センタ長を歴任

2001年4月から2018年3月まで東京電機大学教授、2018年4月より2020年3月特命教授、2020年4月より現職

日本セキュリティ・マネジメント学会会長，
デジタル・フォレンジック研究会会長
内閣官房サイバーセキュリティ補佐官
などを歴任