S/MIME推進協議会
キーノートスピーチ

2023年８月２８日
１４：００－１４：４５

S/MIME推進協議会 発足にあたって

S/MIME推進協議会会長
東京電機大学
名誉教授・客員教授
佐々木良一

自己紹介

＜現職＞
佐々木良一
東京電機大学
名誉教授　兼
同大学サイバセキュリティ
研究所客員教授

＜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月より特命教授、2020年4月より客員教授、2022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

目次

セキュリティ上の問題点とS/MIME

問題点	対策	実装
偽メールによる膨大な被害（フィッシング・標的型攻撃など）	公開鍵暗号を利用した電子署名の採用	メールソフトにS/MIMEの機能の採用が望ましい
メールの盗み見対策として問題のあるPPAPの利用	公開鍵暗号を利用した安全な鍵配送が可能な暗号方式の採用	

にもかかわらず普及してない。状況を把握し、対策を探る。

S/MIME（Secure / Multipurpose Internet Mail Extensions）

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。

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。

（1990年台より）

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

S/MIME暗号

S/MIME署名

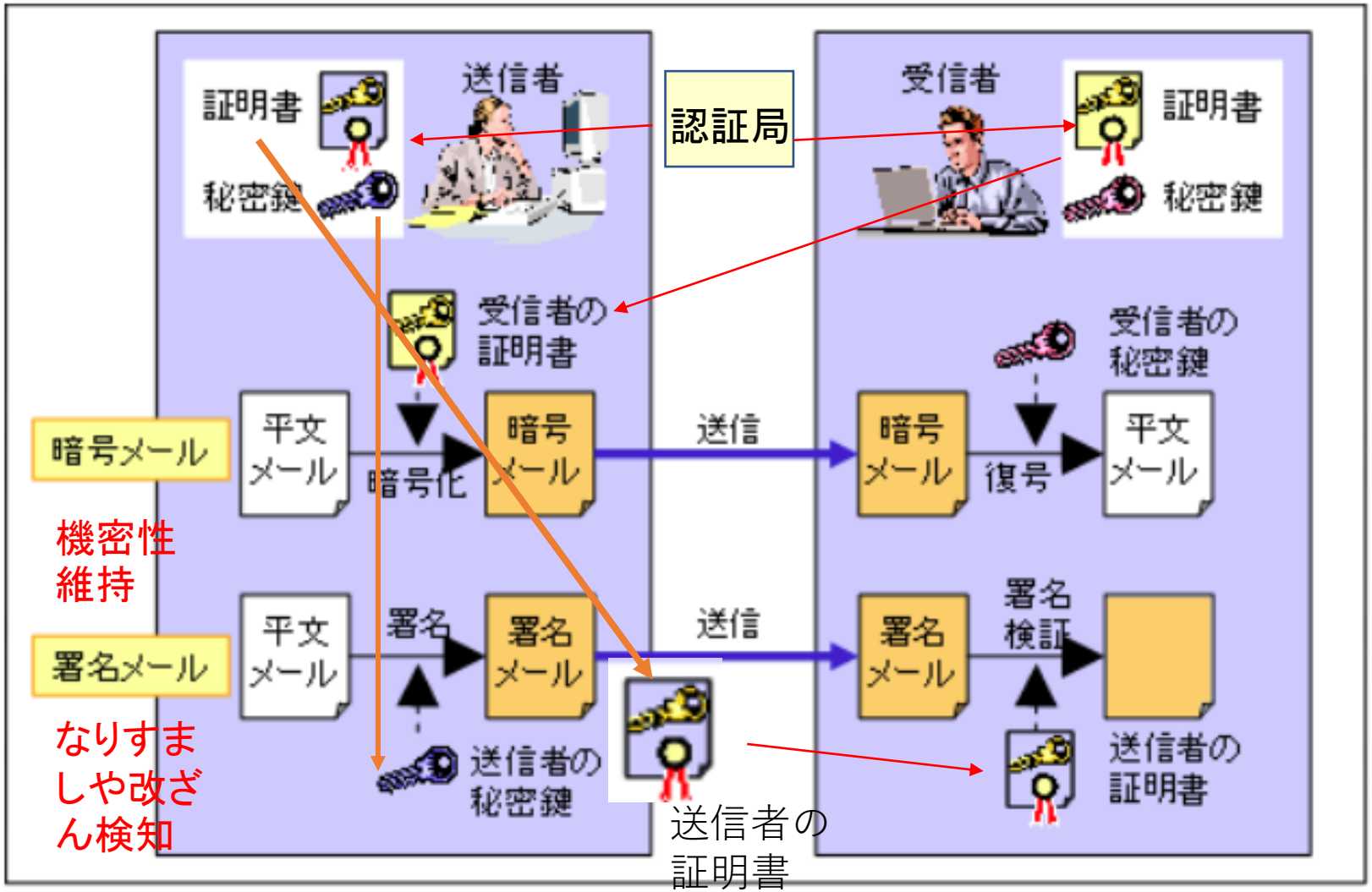
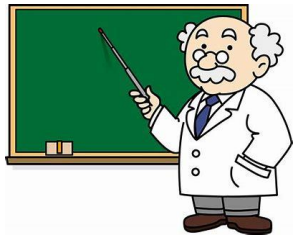


図1：S/MIMEの利用イメージ（出典：IPA「情報セキュリティ - S/MIME」）

公開鍵暗号（暗号化のカギと復号のカギが異なるが一対一に対応）を利用する方式

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（RFC 8551）が必須と考えられる。

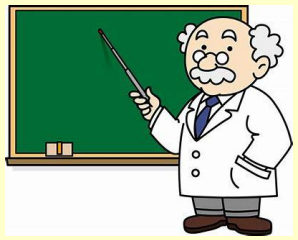
（2）v4は、ハッシュ関数としてSHA-256，SHA512

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

目次

なりすましメールの仕組み

被害事例：2017年12月に日本航空（JAL）が被害を受けた事例。取引先の金融会社を装ったなりすましメールに、支払先口座を変更した旨の情報が記載されていた。担当者はなりすましメールと気づかず、約3億6千万円を指定口座に入金してしまった。

なりすましメールは、「エンベロープFrom」「ヘッダFrom」という2つの送信元メールアドレスの仕組みを悪用
メールソフトに見知った送信元メールアドレス（ヘッダFrom）が表示されている。しかし、よくよく調べてみると、全く知らないメールアドレスがエンベロープFromに設定されている

https://www.kagoya.jp/howto/it-glossary/mail/dkim/

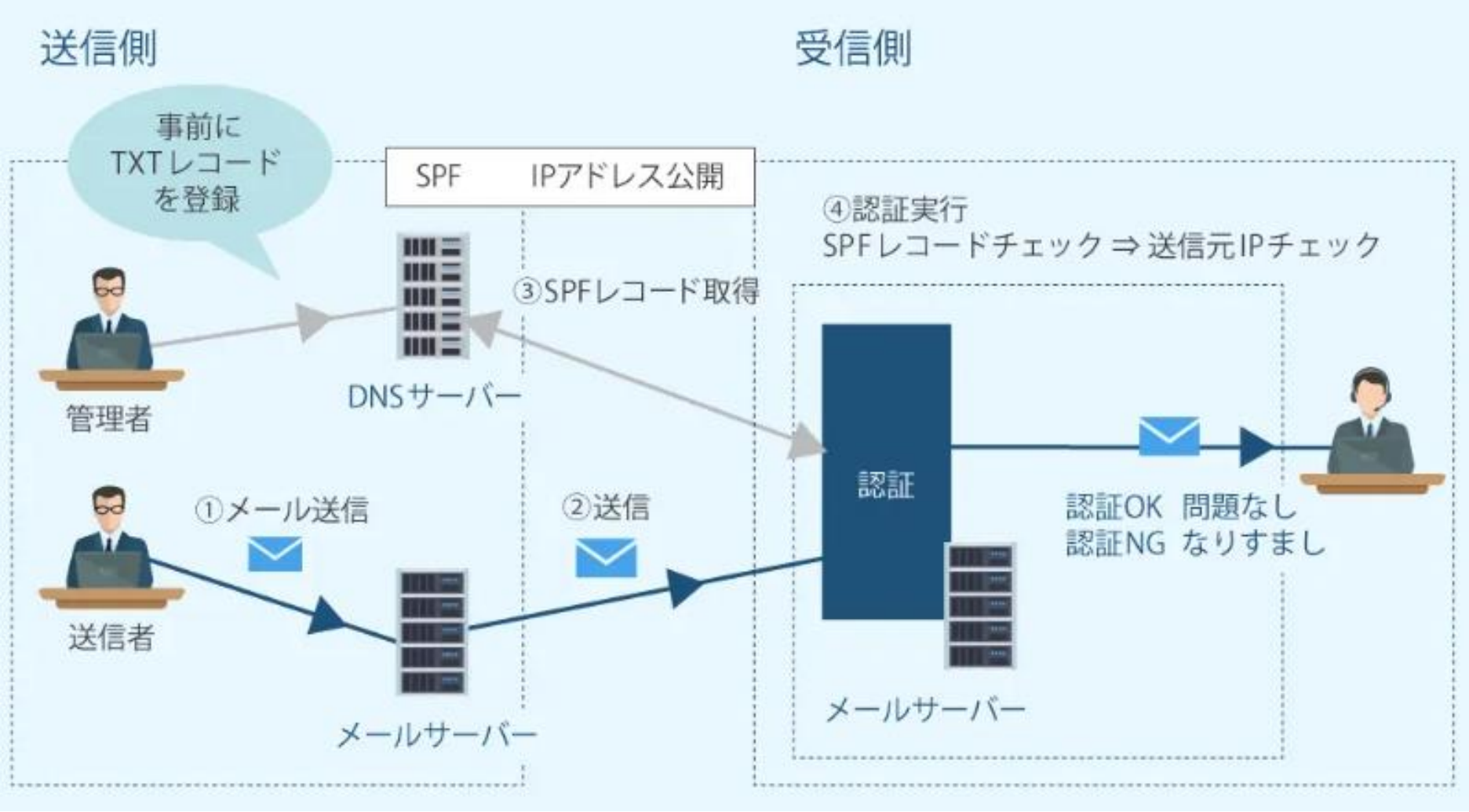
発信者のなりすまし防止機能のある方式

1．SPF（Sender Policy Framework）

2．DKIM（DomainKeys Identified Mail）

3．DMARC（Domain-based Message Authentication, Reporting, and Conformance）

SPFの概要



送信元メールサーバーのIPアドレスで、なりすましメールか否かを判断

SPF:
Sender Policy Framework

https://www.kagoya.jp/howto/it-glossary/mail/dkim/

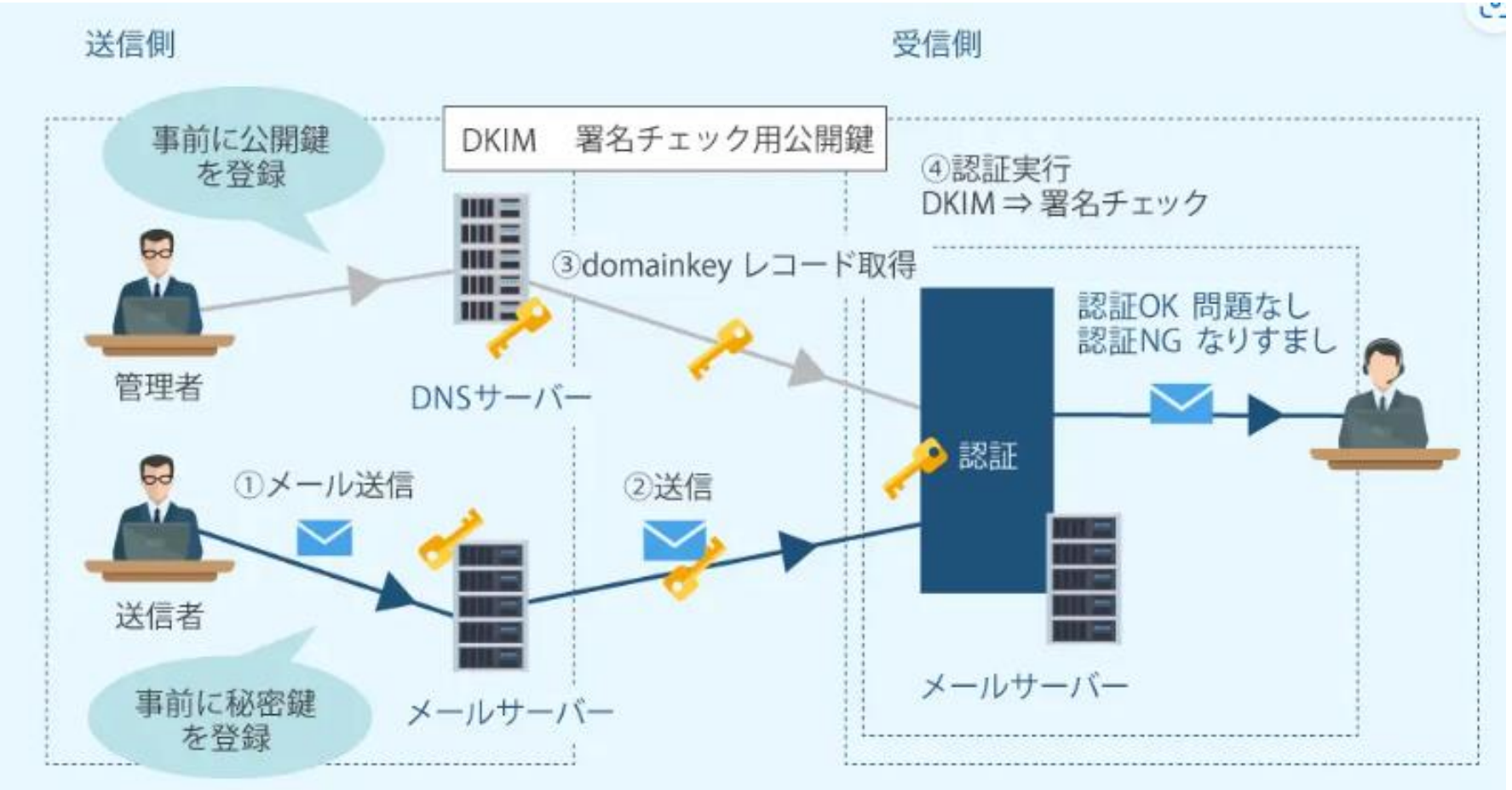
発信者のなりすまし防止機能のある方式

1．SPF（Sender Policy Framework）

2．DKIM（DomainKeys Identified Mail）

3．DMARC（Domain-based Message Authentication, Reporting, and Conformance）

DKIMの概要



送信メールに電子署名を付与して、なりすましメールでないことを証明

DKIM
(DomainKeys
Identified
Mail)

https://www.kagoya.jp/howto/it-glossary/mail/dkim/

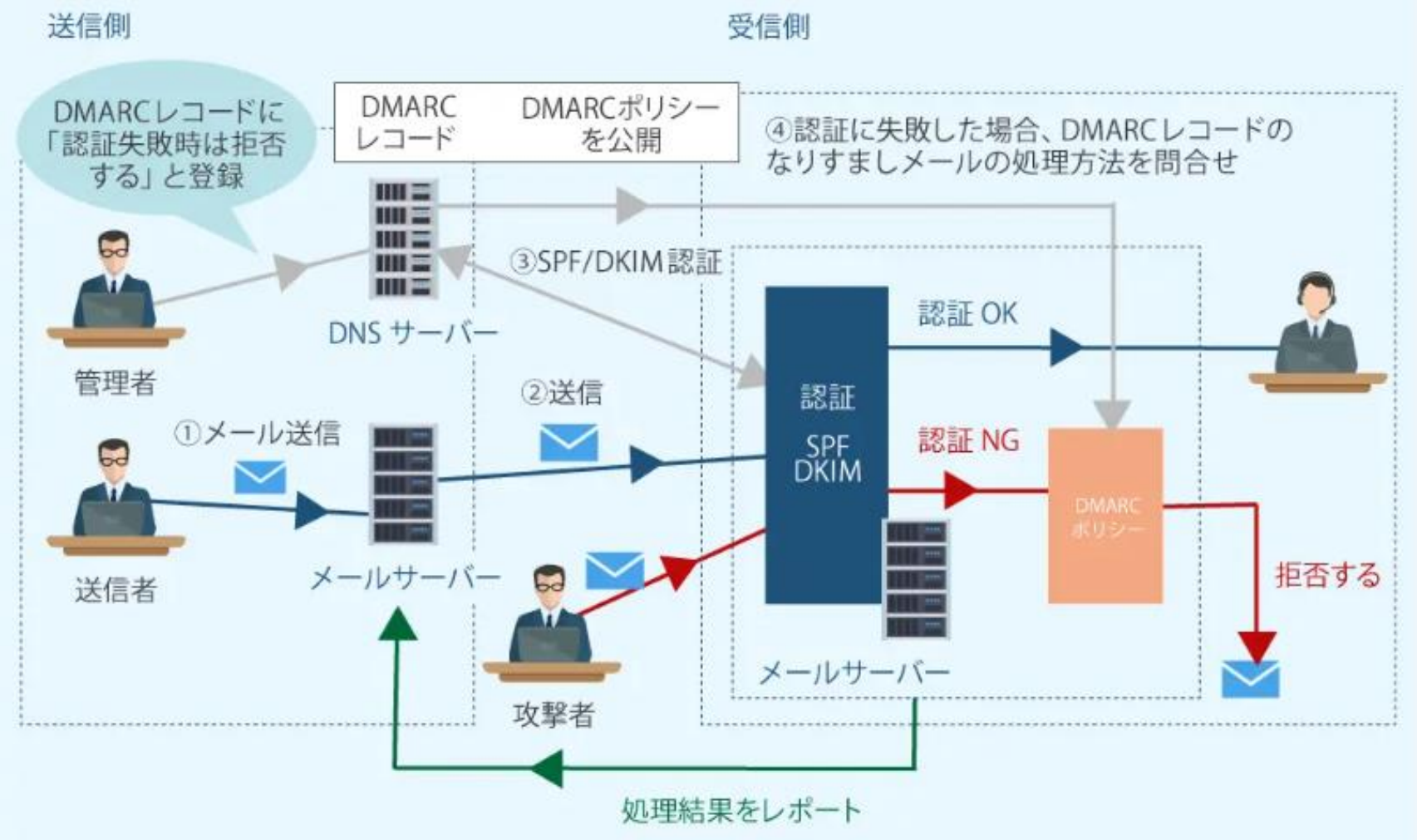
発信者のなりすまし防止機能のある方式

1．SPF（Sender Policy Framework）

2．DKIM（DomainKeys Identified Mail）

3．DMARC（Domain-based Message Authentication, Reporting, and Conformance）

DMARC方式の概要



SPF・DKIMの検証結果をもとに、メールを処理するポリシーを設定する

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

https://www.kagoya.jp/howto/it-glossary/mail/dkim/

3方式の比較

	SPF	DKIM	DMARC
概要	送信元メールサーバーのIPアドレスで、なりすましメールか否かを判断	送信メールに電子署名を付与して、なりすましメールでないことを証明	SPF・DKIMの検証結果をもとに、メールを処理するポリシーを設定する
設定の負担/難易度	最も簡単で手間がかからない	SPFより設定の手間がかかり、専門知識も必要	最も専門知識を必要とし、設定の負担も大きい
対策の有効性	3つのうちでは最も有効性は限られる	SPFより有効	最も有効

https://www.kagoya.jp/howto/it-glossary/mail/dkim/

S/MIMEとSPFなどとの効果の比較

効果＼方式	S/MIME	DKIM DMARC	SPF
発信者のなりすまし防止	効果あり	効果あり	効果あり
メール文の改ざん検知	効果あり	効果あり	効果なし
暗号化機能	あり	なし	なし

目次

PPAPとは

現在よく使われているメールの暗号方式

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/

ＰＰＡＰのメリットといわれているもの

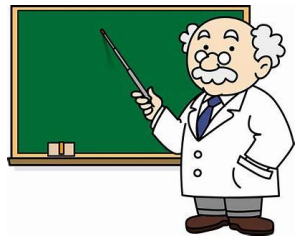
① 誤送信対策効果がある

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



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

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

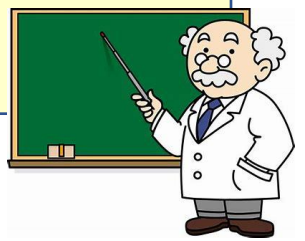
なぜなら、 $P(B|A)\fallingdotseq 1$

（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）



＝＞　暗号化しないのとほぼ同じ安全性

PPAPの問題点

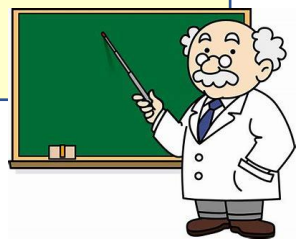
① セキュリティ向上の効果がほとんどないにもかかわらず手間がかかることを強制的にやらされる。しかも

（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

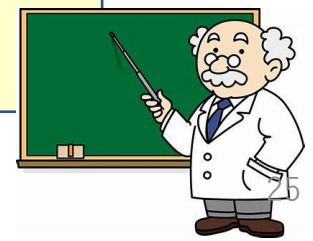
① セキュリティ向上の効果がほとんどないにもかかわらず手間がかかることを強制的にやらされる。しかも

（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。

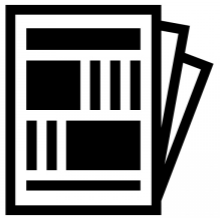


https://xtech.nikkei.com/atcl/nxt/column/18/00676/112100065/
を参考に改良

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。

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP		③S/MIME 暗号化	備考 S/MIME署名
			現状版	②SMSで鍵配送		
メールベースか		Yes	Yes	Yes	Yes	Yes
安全性	暗号強度	X	△	△	○	—
	鍵配送の安全性	—	X	△	○	—
	認証機能	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）		○	△	△	X	△

目次

S/MIMEの問題点

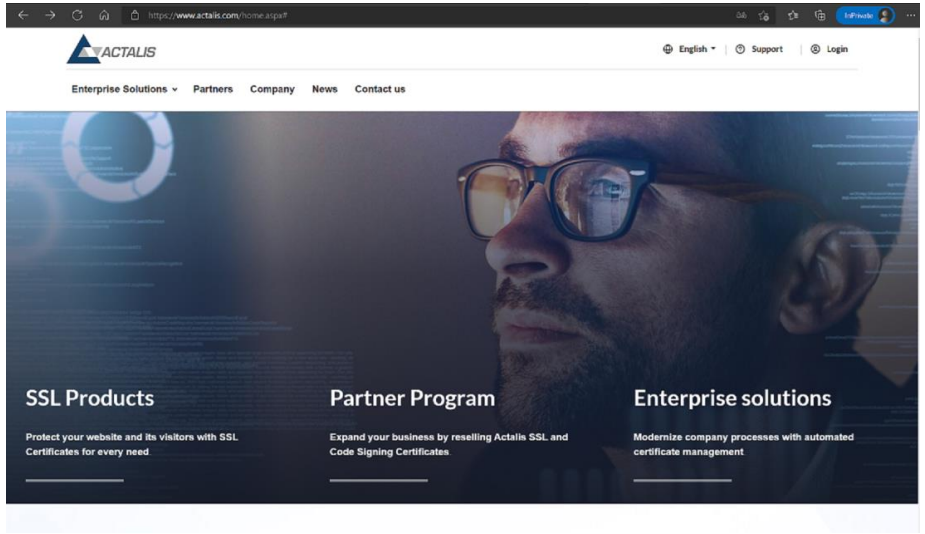
（１）公開鍵証明書（電子証明書ともいう）の入手にお金がかかる

（２）ITリテラシーの低い人や慣れない人には使いにくい部分がある

（３）使い慣れても実装されたプログラムとして使いにくい部分がある

公開鍵証明書の入手

- 無料のサービスや非常に安くサービスをしている認証局もある。



無料の認証局の一例
（ただし、メールの持ち主であることの証明のみ）

年間3850円

普及すれば安くなりうる

S/MIMEの問題点

（１）公開鍵証明書（電子証明書ともいう）の入手にお金がかかる

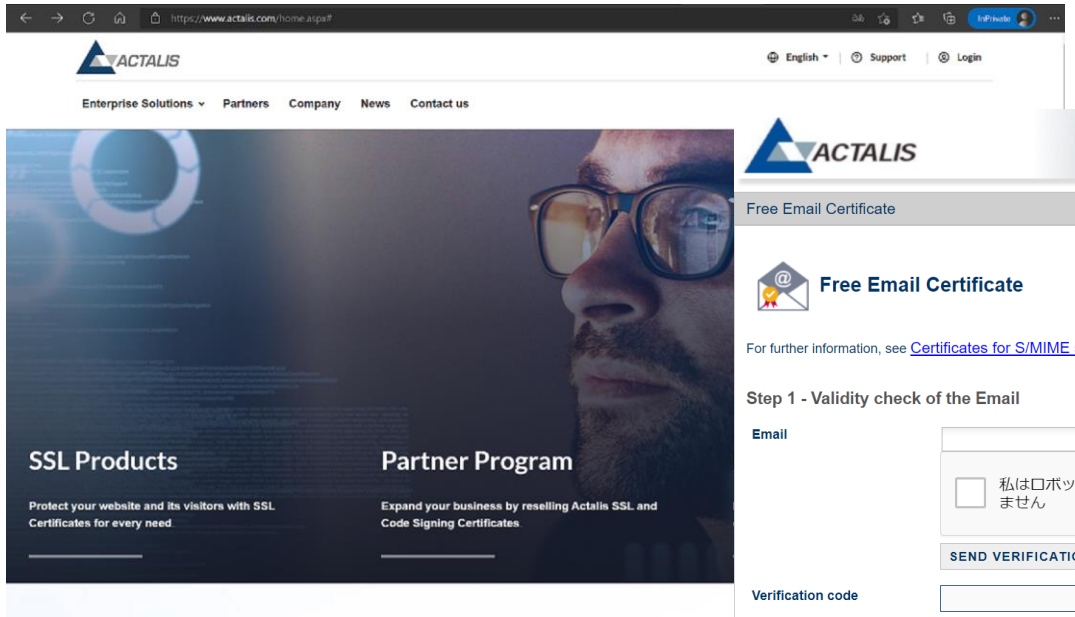
（２）ITリテラシーの低い人や慣れない人には使いにくい部分がある

（３）使い慣れても実装されたプログラムとして使いにくい部分がある

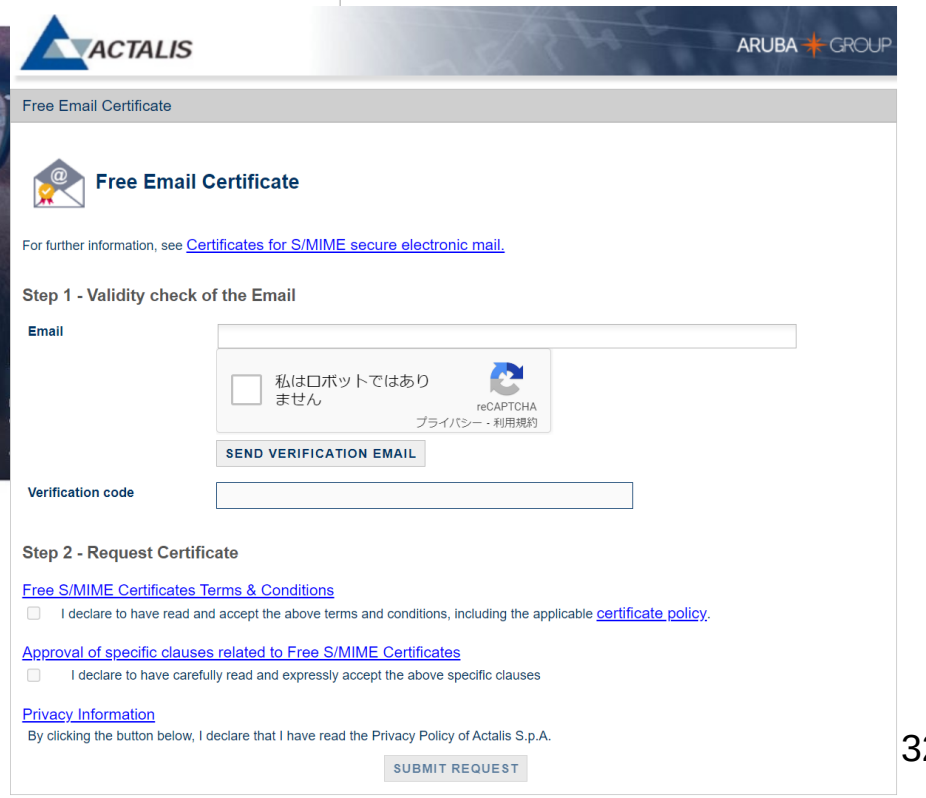
電子証明書の入手

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

慣れた人には問題なし
慣れない人にはややむつかしい



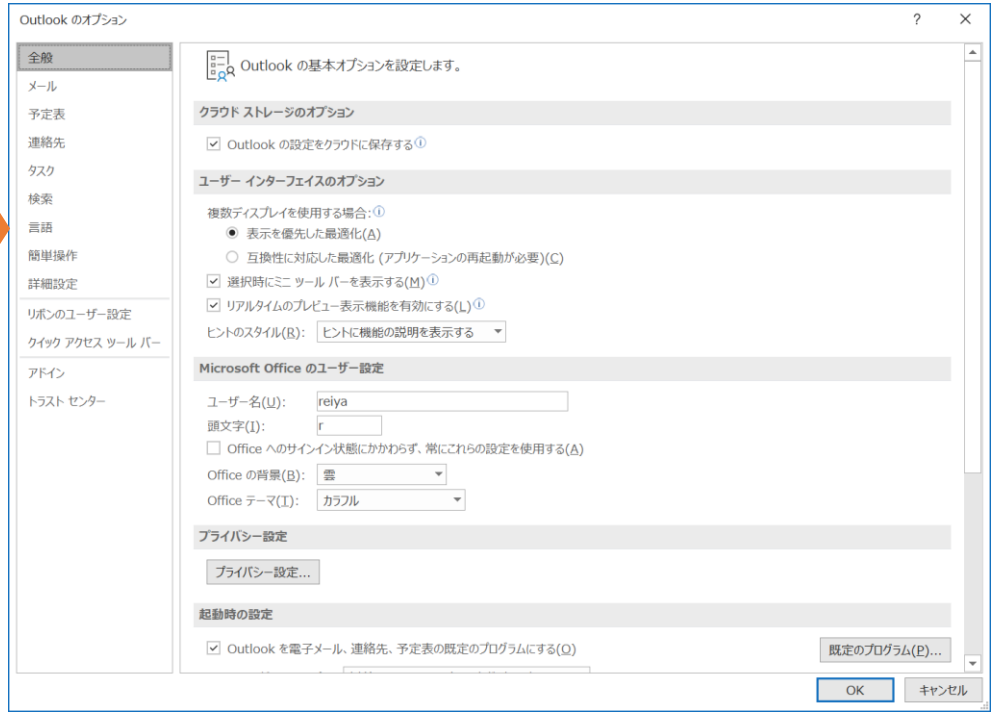
② 証明書を入手するための種々の処理



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。

慣れた人には問題ない
慣れない人にとってはややむつかしい



Outlookで署名や暗号化をする

Outlookの画面

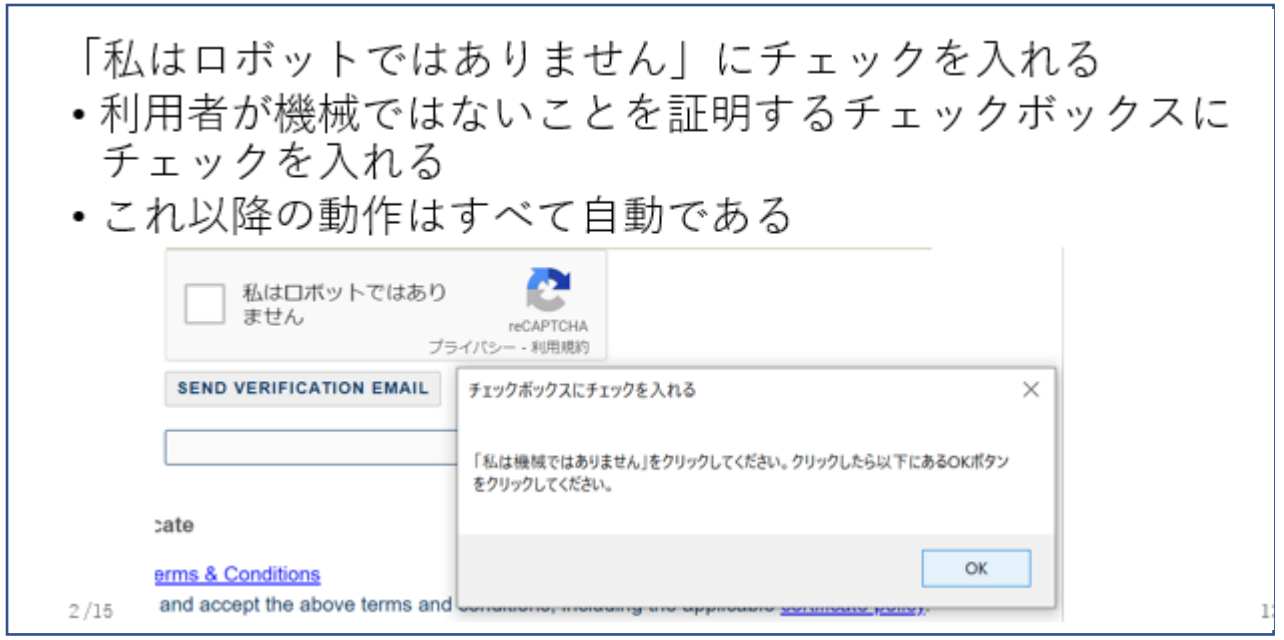
署名や暗号化の処理は、ならびに署名検証や復号は、自動化されていたり、アイコンをクリックするだけなので、だれにでも比較的容易に実施可能

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



電子証明書の入手がむつかしい人はRPAで作ったプログラムの実行もむつかしいということで断念

東京電機大学の学生が実行した研究

S/MIMEの最初の利用のイメージ

送信者：
企業等での
サービス
ITリテラシー
はあり
（業務連絡や
メールマガジ
ンの発送な
ど）
これが偽物だ
といろいろな
不正につなが
るので①の
S/MIME署名
を利用

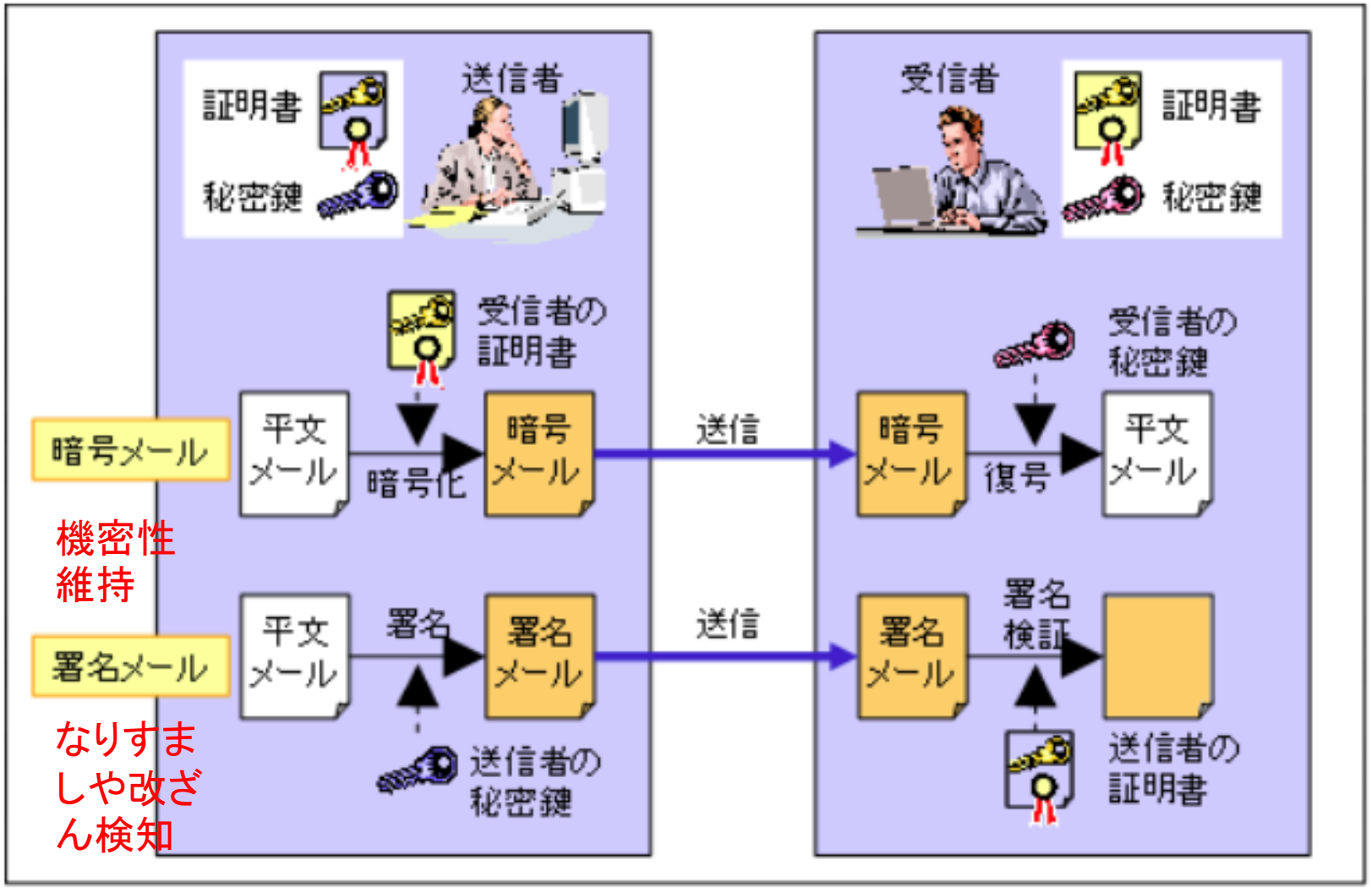


図1：S/MIMEの利用イメージ（出典：IPA「情報セキュリティ - S/MIME」）

受信者：
ITリテラシー
のない慣れな
い人が多い

S/MIME署名なら
検証作業を
S/MIMEプログラ
ムで自動的に実行
し証明書の入手な
どの手間が不要＝
＞こちらから普及
させる方が良いか

＜B２Bでは
S/MIME暗号の同
時実施も可能＞

S/MIMEの問題点

（１）公開鍵証明書（電子証明書ともいう）の入手にお金がかかる

（２）ITリテラシーの低い人や慣れない人には使いにくい部分がある

（３）使い慣れても実装されたプログラムとして使いにくい部分がある

Ｓ／ＭＩＭＥの実装上の問題点

①　各種メーラのS/MIME互換性が確認されていない。

②　WebメールでS/MIMEを利用できるものが少ない

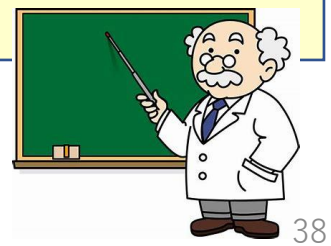
③　使い勝手の悪い部分がある

（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）同報と暗号化を同時に行おうとすると手間がかかる

（ｃ）暗号化されたメールの転送ができない場合がある

（ｄ）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　等



Ｓ／ＭＩＭＥの実装上の問題点

①　各種メーラのS/MIME互換性が確認されていない。

②　WebメールでS/MIMEを利用できるものが少ない

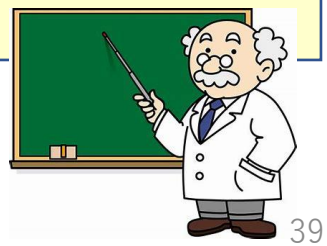
③　使い勝手の悪い部分がある

（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）同報と暗号化を同時に行おうとすると手間がかかる

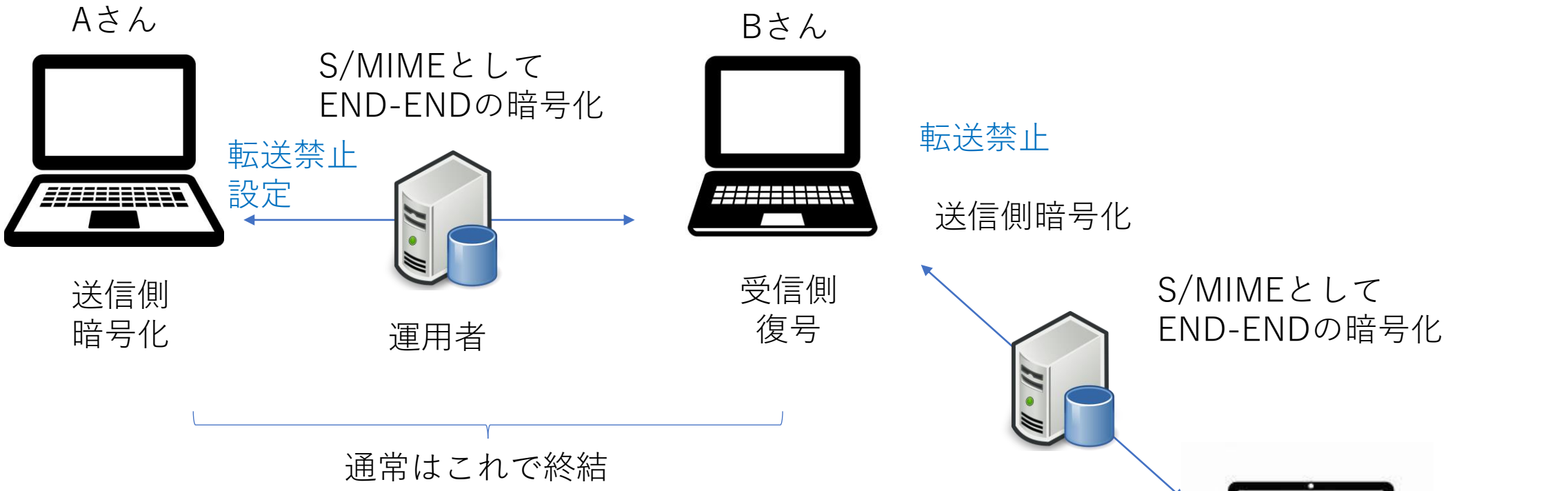
（ｃ）暗号化されたメールの転送ができない場合がある

（ｄ）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　等



これらの問題は広く使われるようになればプログラムの改良や運用で解決しうる問題

転送に伴う処理



暗号化メールは、転送を禁止することが可能になっているものも。
一方、受け取った方では、社内などに転送して情報を共有したい場合もあり使いにくい。
対応案：送信者に依頼して、可能なものについては転送禁止設定を外してもらう運用にするよう交渉をする

普及のための作戦

① S/MIME暗号の普及は時間がかかる

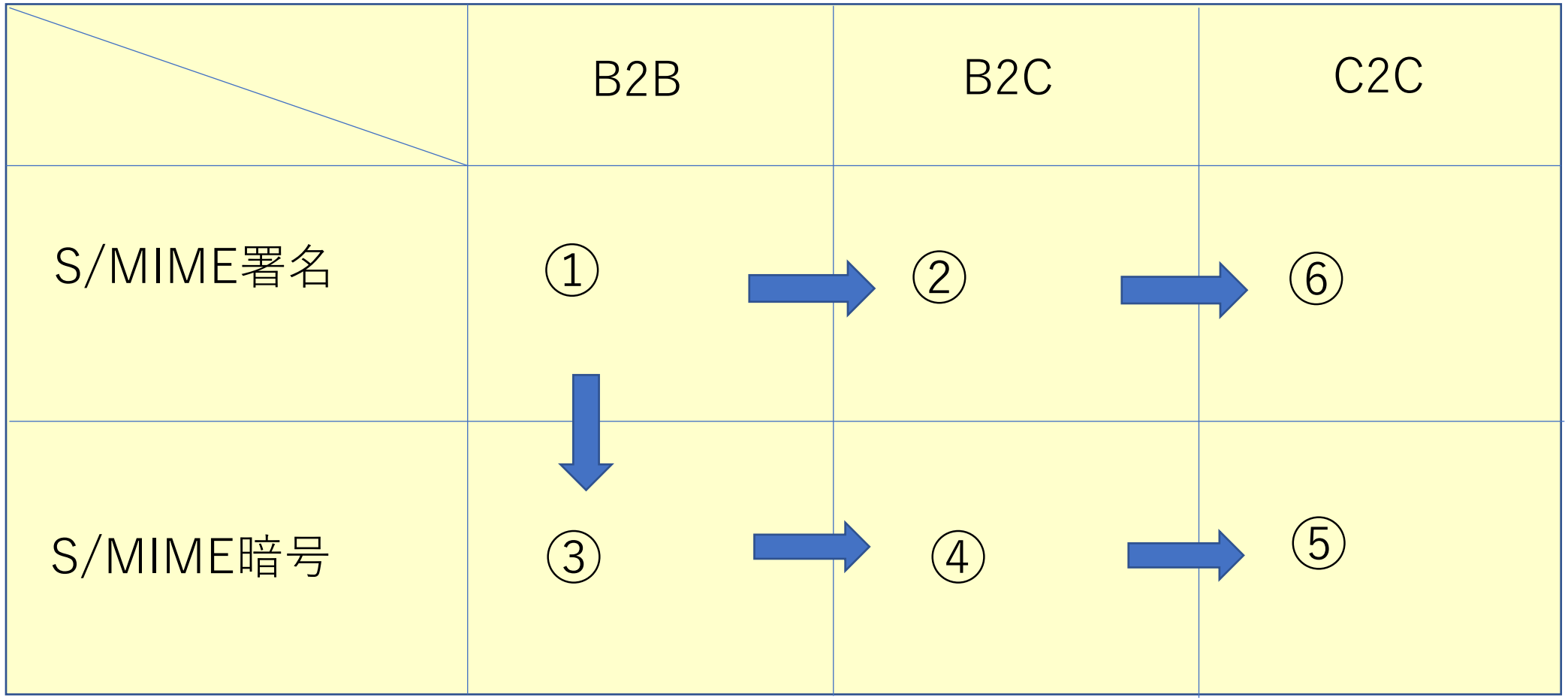
（１）暗号化のためには、メール送信先の公開鍵証明書を入手しておく必要があるが、すべての人に公開鍵証明書を入手して送ってもらう仕組みは普及するのに時間がかかる。

（２）S/MIME暗号の運用はすでに述べたように、現状のままではyaya困難な点がありプログラムの改良などが望ましいが時間がかかる。

② 一方、電子署名によりメールの作成者のなりすましやメール文の改ざんの検知機能の運用は、メール（特にニュースレターなど）の発信者だけが、公開鍵証明書を入手し電子署名を添付すればよいので実用化が簡単

➡ S/MIME署名の普及を企業などで先行させる

S/MIMEの普及戦略



B2Bも組織的にやるものも個別にやるものが考えられる

その後の進展

- このようにしてS/MIMEの使用になれていけば、一般ユーザもS/MIMEの扱いに慣れてきて暗号化への適用が可能になると考えられる。
- また、使う人が増加すれば、プログラムの改良や運用方法の充実で対応できることも多い。
- さらに、S/MIMEの機能を持たないメールソフトやメールソフト間の細かい差異の問題も使う人が増えれば時間とともに解決していくことが期待できる。

目次

コミュニケーションパターンと手段

もうメールは必要ないという人もいるが

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）

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大きい

S/MIME推進協議会の概要１

- そのような思いの人たちが、S/MIME推進協議会を発足させ、私が会長を務めることに

- **会長**
- 佐々木良一
  東京電機大学名誉教授　兼同大学サイバーセキュリティ研究所客員教授
- **顧問**
- 辻井重男

  中央大学研究開発機構 フェロー・機構教授 東京工業大学名誉教授
- **事務局長**
- 諸角昌宏
  合同会社鵜パートナーズ　代表

S/MIME推進協議会の概要 2

- **運営委員**
- （あいうえお順）
- 大泰司章　合同会社ＰＰＡＰ総研 代表社員　JIPDEC客員研究員
- 菊谷誠
- 田上利博　サイバートラスト株式会社 マーケティング本部 プロダクトマーケティング部 担当部長
- 藤原敏樹　インフラウェア株式会社 代表取締役
- 諸角昌宏　合同会社鵜パートナーズ　代表
- 渡辺雅久　Qsol株式会社 営業本部　産業営業部　担当部長

主な活動項目

- S/MIME推進協議会は、以下の活動を行います。

1.情報発信（ウエブサイト）

1. S/MIMEの導入・利用方法に関する技術的・管理的な情報
2. S/MIME、メールサーバーレベルのソリューション情報
3. S/MIME、メールクライアントの情報
4. S/MIME、電子証明書発行事業者の情報
5. S/MIME、ユースケース
6. ブログ、その他の情報

2.啓発活動

1. セミナー開催（会員、非会員すべてを対象）
2. S/MIME勉強会開催（会員、非会員すべてを対象）
3. S/MIME研究会開催（会員向け。S/MIME関連情報の共有等を実施）
4. ニュース配信（会員向け。S/MIME関連情報のメール配信）

3.S/MIME普及の阻害要因に対するアプローチ

1. S/MIME非対応メールソフトのS/MIME対応の促進
2. メール配信サービスに対するS/MIME対応の促進
3. その他、S/MIME未対応の組織・環境へのS/MIME対応の促進

目次

期待するもの

- このS/MIME推進協議会の活動に賛同する人や組織が増え、メールのなりすましなどの問題から解放され、「真正性の文化」を享受できるようになる人がまずは増えることを期待

- さらにS/MIMEが普及し、S/MIME暗号の処理になれる人が増え、S/MIMEプログラムが改良されれば、BtoB、BtoCだけでなくCtoCでも安全なメール通信が普及可能に

S/MIMEの普及と、より安全で使いやすいものにしていくためにご協力を期待する。


END