2020.11.20　JIPDECセミナー

なりすまし対策

～電子証明書を使った本人確認と
電子メールにおける送信元認証～

一般財団法人日本情報経済社会推進協会
（JIPDEC）
セキュリティマネジメント推進室
高倉　万記子

JIPDEC（じぷでっく）で担当している事業

インターネットトラストセンター

JCANトラステッド・サービス登録

電子化普及活動

建築確認申請、環境計量証明書、
取締役会議事録、電子契約（住宅ローン等）、eシール

セキュリティマネジメント推進室

メールなりすまし対策 の普及

安心マーク

S/MIME
エスマいぬ

DKIM
ディーキぃぬ

DMARC
ディーマーくんくん

１．電子証明書とは

マイナンバーカードに格納される公的個人認証サービスについて

公開鍵暗号方式

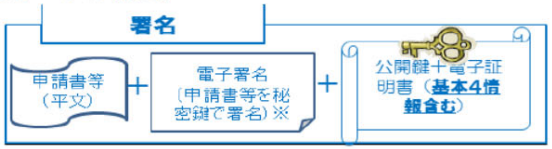
公的個人認証サービスが採用する暗号方式。秘密鍵と公開鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質をもつ。

署名用電子証明書

（性質）
インターネットで電子文書を送信する際などに、署名用電子証明書を用いて、文書が改ざんされていないかどうか等を確認することができる仕組み

（利用局面）
e-Taxの確定申告等、文書を伴う電子申請等に利用される。

（利用されるデータの概要）



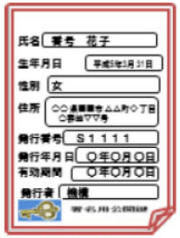
※電子署名法（平成12年法律第102号）の「電子署名」に該当し、同法第3条による「真正な成立の推定」の対象になり得る。

署名用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ



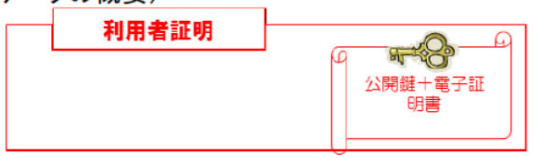
※基本4情報を記録

利用者証明用電子証明書

（性質）
インターネットを閲覧する際などに、利用者証明用電子証明書（基本4情報の記載なし）を用いて、利用者本人であることのみを証明する仕組み

（利用局面）
マイナポータルのログイン等、本人であることの認証手段として利用される。

（利用されるデータの概要）



利用者証明用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ

※基本4情報の記録なし

4

マイナンバーカードの機能のスマートフォン搭載等に関する検討会（第1回）　マイナンバーカード及び公的個人認証サービスの概要　より

紙の世界と電子の世界

※今回は、話を単純化するため、PKIの電子証明書（秘密鍵）を使ってデジタル署名をするものを「電子署名」と呼びます。

JIPDEC

紙の世界

道具

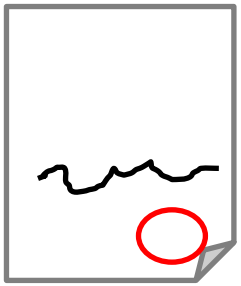
ペン

OR

ハンコ

署名または押印

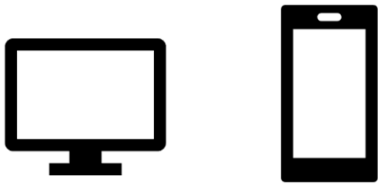
対象



電子の世界

電子証明書
（秘密鍵）

電子署名



2．電子証明書を
使ったなりすまし対策

電子証明書を使ったなりすまし対策

- 電子契約
- クライアント認証
- なりすましメール対策

電子署名で確認できること

○文書が署名後、変更されていないこと

○本人が作成したこと

文書を裁判に証拠として提出する場合、

紙の文書…「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」（民事訴訟法228条第4項）

電子文書…「本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。」（電子署名法第3条）

紙の契約と電子契約

合意、Wordで文書作成

BEFORE

乙社

２通を印刷、針閉じ、袋とじ
決裁、押印
宛名書き、切手貼付、封入、封緘、投函

甲社

受取、内容確認
決裁、押印
宛名書き、切手貼付、封入、封緘、投函
台帳記載、キャビネットに保管

乙社

受取、内容確認
台帳記載、キャビネットに保管

AFTER

甲社

決裁
電子署名＋タイムスタンプ

乙社

決裁
電子署名＋タイムスタンプ

本人確認された上で
電子証明書は発行されている
＝なりすまし防止

電子証明書を使ったなりすまし対策

- 電子契約
- **クライアント認証**
- なりすましメール対策

JIPDEC内システムへのアクセスは電子証明書が必要

社外からのアクセス

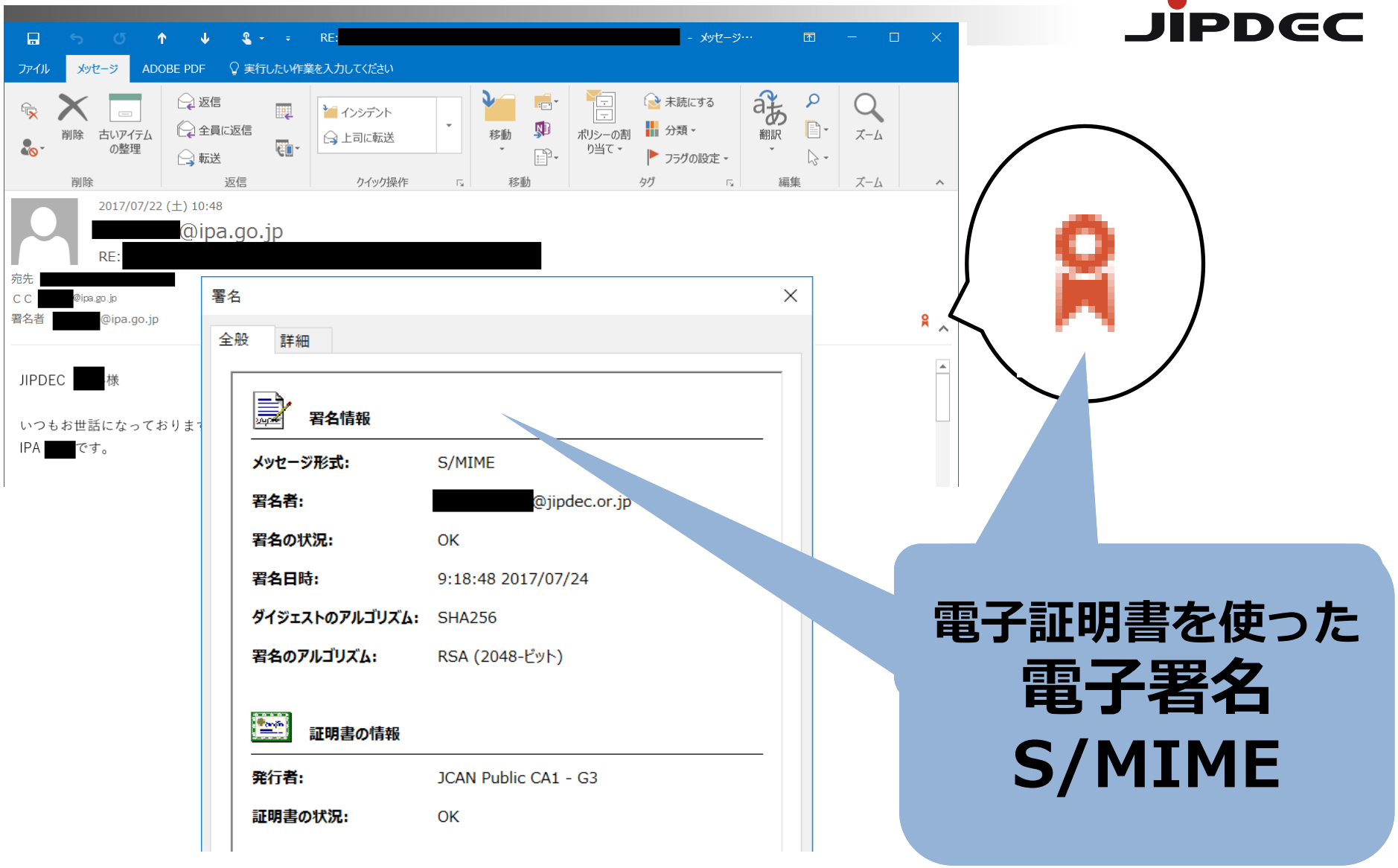
- 勤怠管理、稟議
- チャット、通話
- ファイルサーバ
- メール
- 社内報

電子証明書を持っていないとログインできない

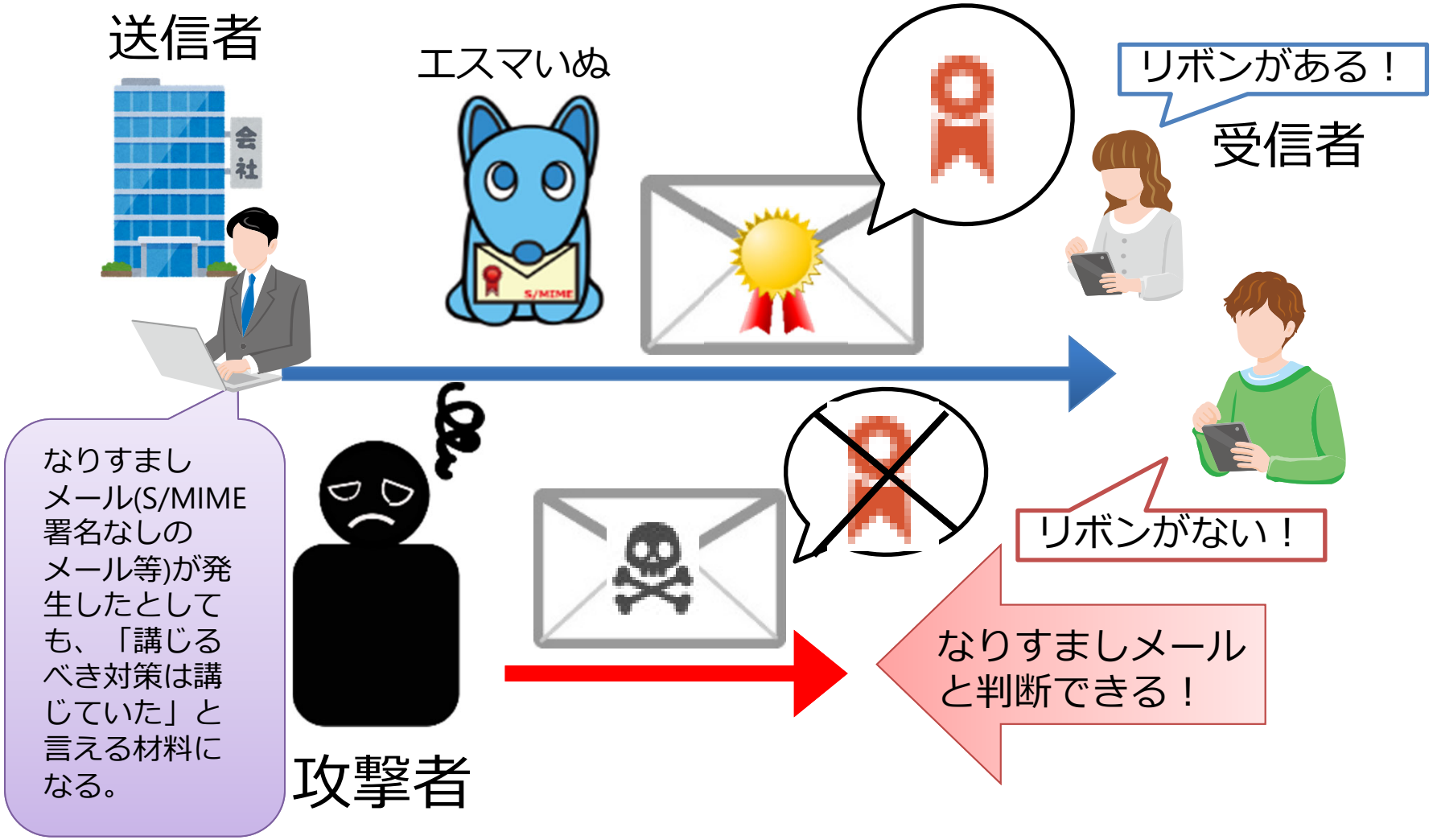
電子証明書を使ったなりすまし対策

- 電子契約
- クライアント認証
- なりすましメール対策

なりすまし対策（S/MIME）をしたOutlookの表示例



電子署名（S/MIME）を付けるとなりすましと区別がつく



情報セキュリティ10大脅威 2020（IPA）

順位	組織の脅威
1位	標的型攻撃による機密情報の窃取
2位	内部不正による情報漏えい
3位	ビジネスメール詐欺による金銭被害
4位	サプライチェーンの弱点を悪用した攻撃
5位	ランサムウェアによる被害
…	…

https://www.ipa.go.jp/security/vuln/10threats2020.html

対策/対応（情報セキュリティ 10 大脅威 2020　５３ページ）
・メールに電子署名を付与（S/MIME）
取引先との間で請求書等の重要情報をメール で取り扱う場合、
S/MIME による電子署名 の付与がなりすまし防止対策として有効である。

S/MIME導入の広がり１

2019年6月　**九州電力グループ**の社員約14,300人でS/MIMEの運用開始。

電子証明書の自動発行・更新・運用管理の仕組みを開発（特許6715379）。

九州電力
ずっと先まで、明るくしたい。

キーワードを入力してください　文字サイズ　小 中 大　SELECT LANGUAGE

新着情報・お知らせ

停電情報
落雷情報
お問い合わせ（お便りBOX）
営業所
よくあるご質問
公式Facebook
公式Twitter

個人のお客さま
電気料金・各種手続きのご案内

法人のお客さま
電気料金・各種サービスのご案内

企業・IR情報
企業情報・CSR・TCFD関連情報 ・採用情報のご案内

発電
原子力・火力・再生可能エネルギー

ホーム > 新着情報・お知らせ > お知らせ > 電子メールのなりすまし対策として、九州電力の全社員に「電子署名付きメール：S/MIME（エスマイム）」を導入しました

シェア　ツイート

電子メールのなりすまし対策として、九州電力の全社員に「電子署名付きメール：S/MIME（エスマイム）」を導入しました

2019年６月25日
九州電力株式会社

電子メールのなりすまし対策として、九州電力の全社員に「電子署名付きメール：S/MIME（エスマイム）」を導入しました

当社は、電子メールのなりすまし対策として、九州電力株式会社、株式会社九電ハイテック、株式会社九電ビジネスパートナー（以下、九州電力ほか）の全社員（職員、出向受入者、派遣社員、パートタイマー等を含む）に「電子署名付きメール：S/MIME」（以下、S/MIME）を導入し、６月から運用を開始しました。

標的型攻撃メールはますます巧妙化しており、電子メールの安全性確保が喫緊の課題となっていますが、S/MIMEは、認証局と呼ばれる第三者機関が、電子メール利用者の身元情報を認証する電子証明書を発行し、電子署名を付したメールをやり取りする仕組みです。（図１参照）

万記子1

S/MIME導入の広がり２

2020年４月　**一般社団法人 日本クラウドセキュリティアライアンス**から

発信される全メールでS/MIME運用開始

スライド 17

万記子1　万記子 高倉, 2020/11/19

S/MIME導入の広がり3

2020年10月　**防衛装備庁**の全職員約2,000名でS/MIMEの運用開始

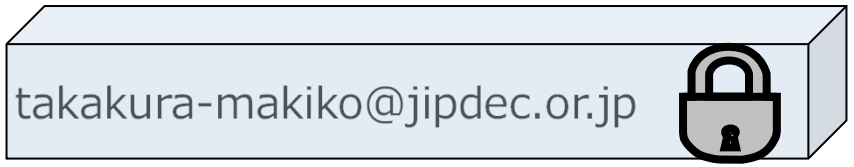
３．その他のなりすまし
メール対策

S/MIMEとDKIMの違い

エンド　to　エンド

S/MIME
エスマいぬ

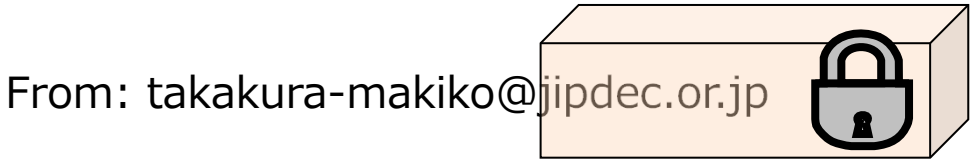
エスマイム（**S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions）



サーバ間

DKIM
ディーキぃぬ

ディーキム（**D**omain**K**eys **I**dentified **M**ail）



S/MIMEとDKIMの違い

S/MIME
エスマいぬ

○ 銀行を中心に普及してきた。
主要なPCのメーラーが対応済み。

× Webメールなど未対応

DKIM
ディーキぃぬ

○ 大手ISPとメール配信事業者が対応済み。

× 受信者には簡単には見分けがつかない。

DMARCの機能

DMARCの機能

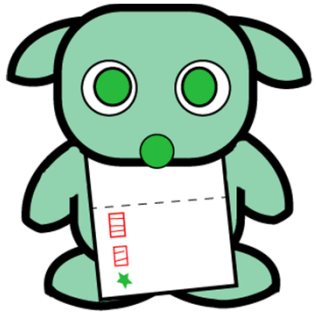
1．受信側でSPFかDKIMで検証される
2．先方への認証失敗メールの扱いを決められる
　　何もしない or 隔離 or 拒否
3．認証結果が、レポート（XML）で届くようになる

レポートの解析が大変なため、
わかりやすく解析表示するサービスが普及しつつある

DMARCの設定条件

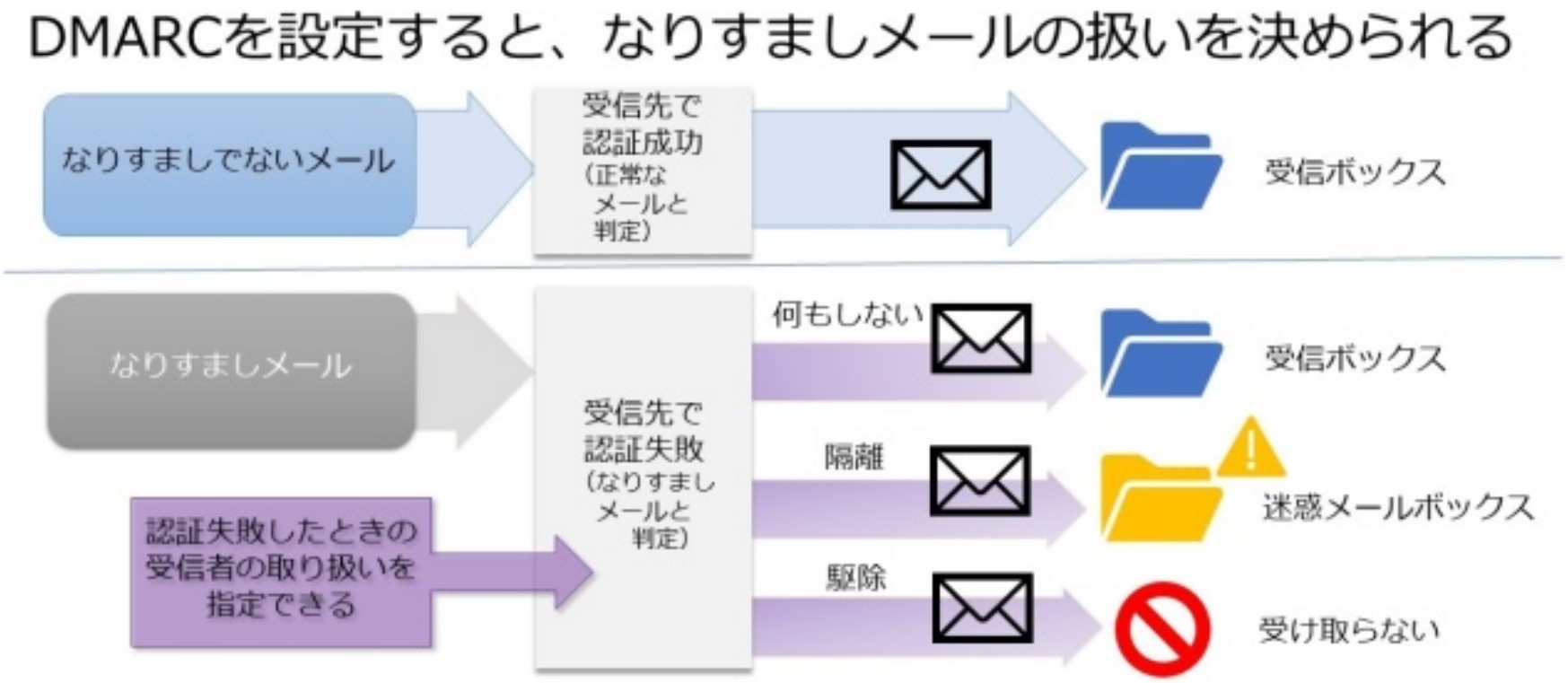
1．SPFかDKIMを設定していること
2．DNSサーバに1行書く

※SPF…送信ドメイン認証



ディーマーくんくん

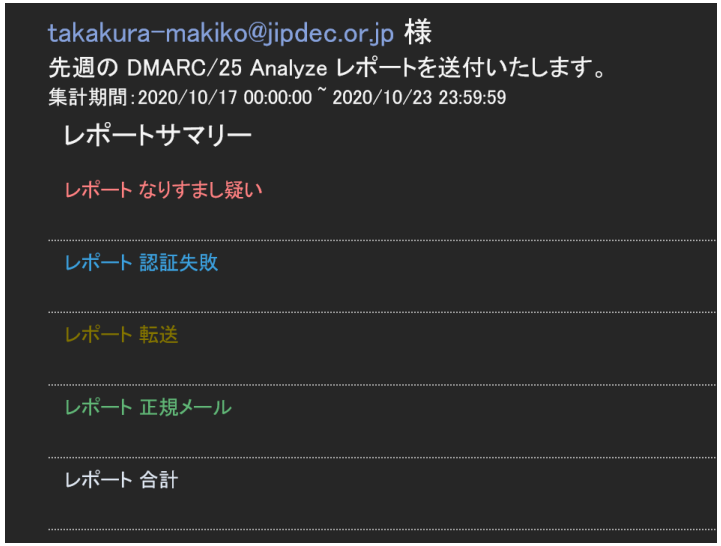
なりすましメールの判定と処理



JIPDECでのDMARC利用

- DNSサーバのレコードに一行を追加。
- レポート提供・解析サービスも利用

TwoFive社：dmarc/25



cyxtera社（旧Easy Solutions社）

DMARC設定状況（国内）

○今年報道された設定状況

日経平均株価採用社（225社）　**23.0%**（9/14 日経新聞）

自治体の防災メール発信（1,026自治体）　**14.2%**（10/20 JIPDEC発表）

○JPドメイン名の種別ごとにおける送信ドメイン認証技術の設定状況（2020年6月末時点）

種別		設定割合
AD . JP	JPNIC会員等	4.4%
AC . JP	高等教育機関および学校法人	1.7%
CO . JP	企業	1.1%
GO . JP	政府	4.1%
OR . JP	非営利法人	0.8%
NE . JP	NW事業者	1.8%

種別		設定割合
GR . JP	任意団体	1.0%
ED . JP	18歳未満向け教育機関	0.8%
LG . JP	地方公共団体	0.2%
地域型・都道府県型		1.9%
汎用		1.4%
合計		1.3%

総務省　迷惑メール対策ページより

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei

DMARC設定状況（海外）

政府　強制力を持った設定

- **英国**　GovernmentDigital Service（GDS、内閣府の一部）

  2016年10月1日までにオンラインサービスを保護するために
  他の政府部門がDMARCを採用することを要求

  https://dmarc.org/2016/06/dmarc-required-for-uk-government-services-by-october-1st/

- **米国**　国土安全保障省（DHS）の運用指令（強制的な指示）18-01

  1．指令の発行後30日以内に有効なDMARC設定
  少なくとも「p = none」のDMARCポリシー
  集約レポートや障害レポートの受信者として定義された1つ以上のアドレス
  2．指令の発行後1年以内
  「拒否」のDMARCポリシーを設定します

  https://cyber.dhs.gov/bod/18-01/

企業　5か国で5割以上の企業が対応されている

11/13 Security NEXT 報道　https://www.security-next.com/119894

7.2. 1 電子メール

遵守事項
(1) 電子メールの導入時の対策

	H28	H30
(a)	情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中 継を行わないように設定すること。	変更なし
(b)	情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。	変更なし
(c)	情報システムセキュリティ責任者は、電子メールのなりすまし の防止策を講ずること。	変更なし
(d)	（H30新設）情報システムセキュリティ責任者は、インターネットを介して通信する電子メー ルの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。	

参考：https://www.nisc.go.jp/active/general/kijun28.pdf
https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf

地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省)

６．技術的セキュリティ

6.1. コンピュータ及びネットワークの管理

解説

(１４) 電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び、外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いた **DKIM**（DomainKeys Identified Mail）  や **SPF**（Sender Policy Framework）等の対策を行うとともに、 **DMARC** （ Domain-based Message Authentication, Reporting & Conformance）  も行わなければならない。

参考：地方公共団体における 情報セキュリティポリシーに関するガイドライン(平成 30 年 9 月版)
https://www.soumu.go.jp/main_content/000592786.pdf

JIPDECでは　LINEスタンプで普及啓発

４．Emotetと暗号化ZIP

暗号化ZIPファイルを悪用したEmotetも流行中

発表日	社名（敬称略） ※各社の発表より抜粋
9月18日	ニッセイコム社
9月18日	建設業技術者センター
10月16日	京セラ社
10月20日	鳥羽洋行社
10月22日	SEcuSTATION社

相談急増／パスワード付きZIPファイルを使った攻撃の例

2020年9月2日、「パスワード付きのZIPファイルを添付したEmotetの攻撃メール」（図8）を確認しました。この手口では、添付ファイルが暗号化されていることから、メール配送経路上でのセキュリティ製品の検知・検疫をすり抜け、受信者の手元に攻撃メールが届いてしまう確率が高く、より注意が必要です。ZIPファイルの中には、これまで同様、悪意のあるマクロが仕掛けられたWord文書ファイルが含まれています

「Emotet」と呼ばれるウイルスへの感染を狙うメールについて

独立行政法人情報処理推進機構　セキュリティセンター

https://www.ipa.go.jp/security/announce/20191202.html#L13

デジタル改革アイデアボックス 取りまとめ

アイディアー覧（総合）　人気順１～５位

※11/6（金）時点で評価ポイント（賛成票数−反対票数）が高い順

1位

4.省庁職員の声

232ポイント
249票
45コメント

モグラさん

暗号化した添付ファイルを送って、その直後にパスワードが来るPPAPと言われる日本特有のメールの悪慣習はセキュリティ上も意味がないと言われているし、管理を煩雑にしている。行政はPPAPをやめる、PPAPを受け取らない、としたらどうか。

2位

2.IT業界の声

184ポイント
228票
295コメント

タナックス太郎さん

インターネットでの投票を実現してほしい。最近の投票率は50%を切るなど低迷している。20代は最も低い。インターネット投票を導入したら、投票率の上昇につながると思う。投票所に出向く手間も省け、より気軽に選挙に参加できると思う。

3位

2.IT業界の声

145ポイント
166票
30コメント

nabeponさん

日本では公的機関でIEを前提とするものが多いが、セキュリティ面の懸念から使用するべきでない。IEの使用は危険が伴うとして非推奨だと宣言すべき。IE以外の使用が難しければ、CHromiumをベースにした日本国家のブラウザを作れば済む。

投稿アイデア数約3,300件の中で第1位（11月6日までのアイデア）

デジタル改革関連法案ワーキンググループ（第３回）

https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai3/gijisidai.html

プライバシーマーク推進センターはPPAP推奨してません

メール添付のファイル送信について

昨今、個人情報を含むファイル等をメールで送信する際に、ファイルをパスワード設定により暗号化して添付し、そのパスワードを別メールで送信することについて、お問合せを多くいただいております。

プライバシーマーク制度では上記の方法による個人情報を含むファイルの送信は、メールの誤送信等による個人情報の漏洩を防げないこと等から、従来から推奨しておりません。

プライバシーマーク付与事業者におかれましては、個人情報を含むファイルをメールで送受信する場合、送信先や取り扱う情報等を踏まえ、リスク分析を行ったうえで、必要かつ適切な安全管理措置を講じていただきますようお願いいたします。

https://privacymark.jp/news/system/2020/1118.html

本日のおさらい

電子証明書でできる、なりすまし対策
・電子契約（電子署名）
・クライアント認証
・なりすましメール対策（S/MIME）

その他なりすましメール対策（DMARC等）