日本国内におけるDKIM普及取組の現状と課題

Japan DKIM Working Group (dkim.jp)

http://www.dkim.jp
e-mail: info@dkim.jp
Tel: 050-5817-7650

- 赤桐 壮人 (あかぎり たけひと)
  - 楽天株式会社
  - インターネットエンジニアリング推進室 室長
  - dkim.jp 議長
- 島貫 和也 (しまぬき かずや)
  - ヤフー株式会社
  - R&D統括本部 フロントエンド開発1本部
  - dkim.jp Board member

目次

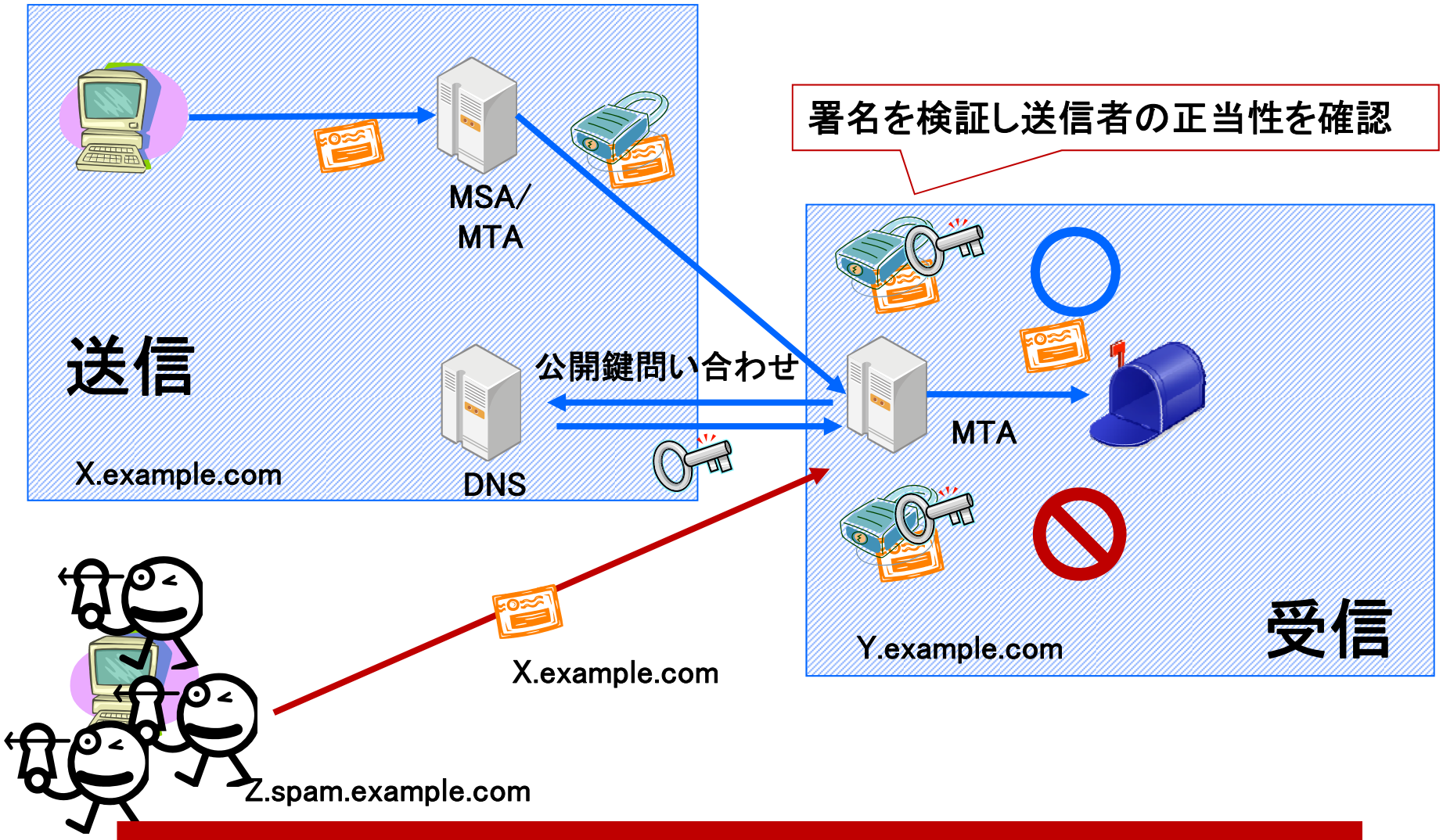
DKIM 普及の現状

企業におけるDKIM導入のためにクリアしなければならない課題

今後のDKIM導入推進への取り組み

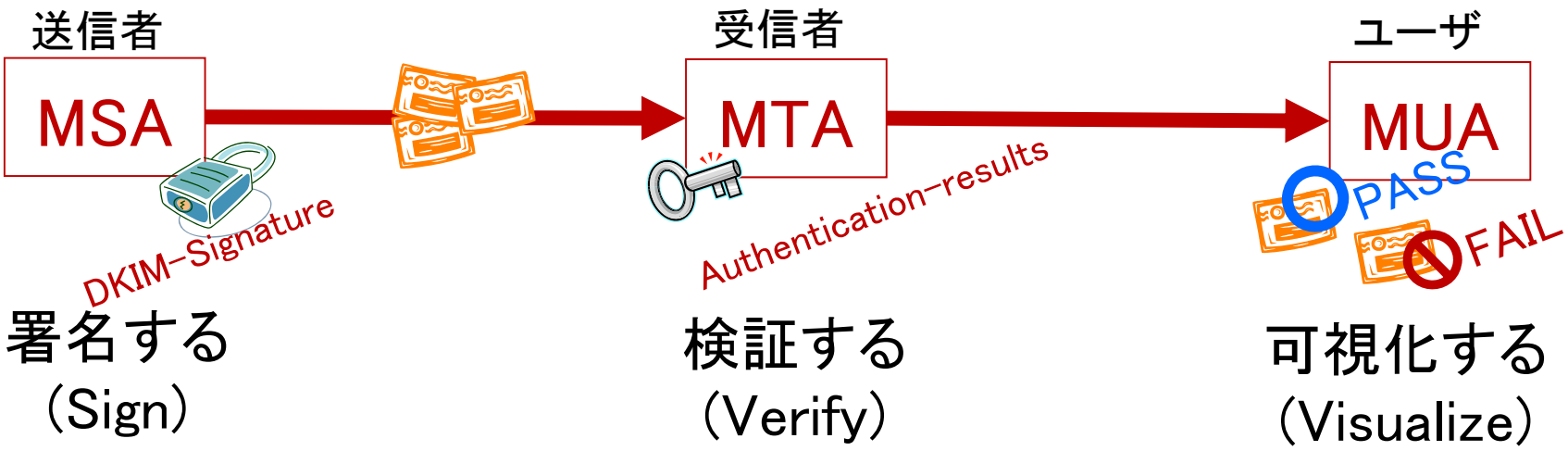
1 DKIM とは？

DKIM とは？

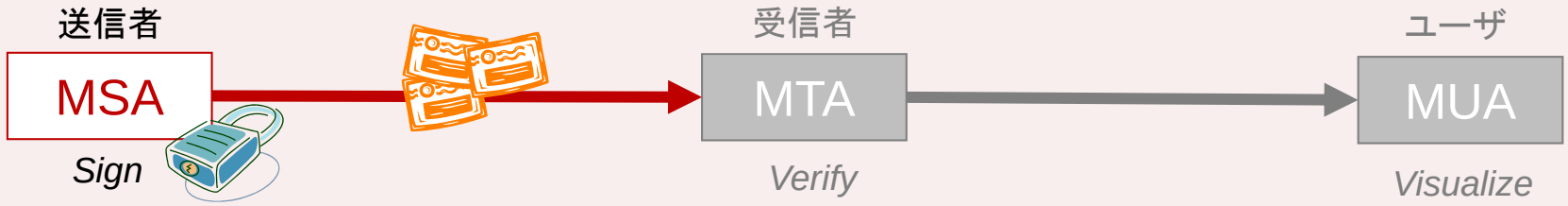


電子署名を利用した送信元認証

DKIMとシステムの関係



DKIM の「署名(Sign)」に必要な作業



STEP 1 DKIMで署名したいドメインを決定する

- あなたがドメインオーナーだと仮定して、
  所有するドメインのうち**DKIM対応したいもの(“d”)**を決定する

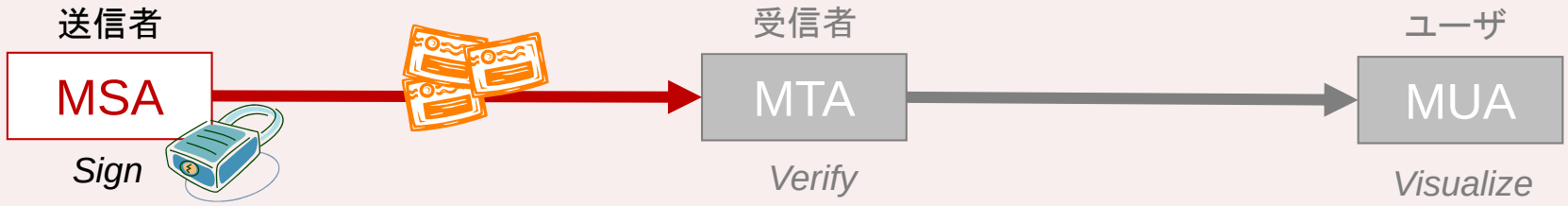
STEP 2 DKIMに使用するRSA鍵のペアを作成する

- RSA鍵ペアを生成する。「公開鍵」と「秘密鍵」が対になって生成される
  （鍵の作成の際には、その組み合わせを示す「**セレクタ名(“s”)**」を任意に決める）
- 秘密鍵は、MSA(メール送信サーバ)にファイルとして設置する。
  組織内でも運用担当者のみなど限られたアクセスとする。
- 公開鍵は、そのドメインのDNSサーバにTXT RR（テキストレコード）として設置する。
  インターネットから誰でも引けるようにしておく。

TXT RR の例

example.jpドメインのDNS TXTレコード	dkim20101115._domainkey IN TXT "v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC42q2GmH+fSCU3z/jqA2makU1NXh18FGpRtDlGg6WQ+Dm0Snh4DZhZaSUFND3kG3V7UteWYHpVojCSaeN+luHHZXTBBMJ4yqBuNphtD+QZhGgrlqAwFH4hBJII7q05cCNCEP+XFwijYuO95FOSAvtn4A9OcaGbS2gwiW9uL841mwIDAQAB"

DKIM の「署名(Sign)」に必要な作業



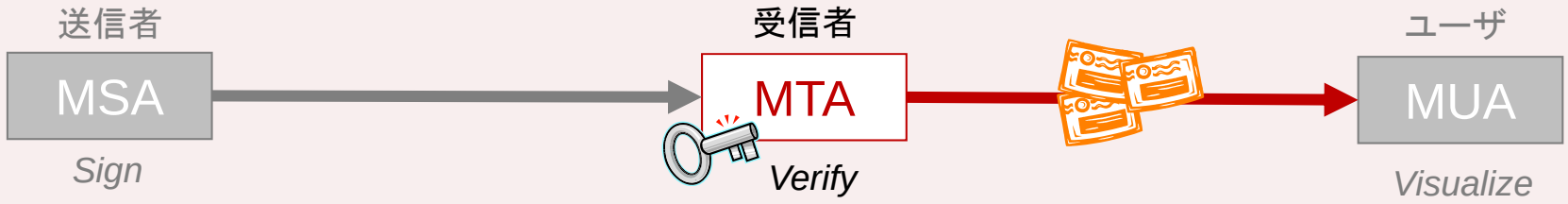
STEP 3 MSAにDKIM署名を付与する改修を実施する

- 秘密鍵とメール本文より、メールごとにDKIMの署名が生成される
- DKIMの署名は ”DKIM-Signature” という専用のヘッダに格納される

DKIM-Signatureヘッダの例

DKIM-Signature:	v=1; a=rsa-sha256; c=simple/simple; **d=**example.jp; **s=**dkim20101115; t=1308471652; bh=KF7zwHMa9ToPtsGy8urMTpCLCfTnzrcJ6mxHnrWCffQ=; h=To:Sender:MIME-Version:Subject:From:Content-Type: Content-Transfer-Encoding:Message-Id:Date; b=xdIeG4cUHIBhU0nix2V5tK9ZN7QwnKd+qYuFamqtZpon2EfsKfSwdGhSHvU6fRj3z dp6tVjGpT64hx4eayxKcnjHTYMq8yRVgEPp9naNrCD7SIX70P6LvrbFpMZc85Exxpx FZdETOXsumsY7pt6tpP9puwjN3/5EsYuwWM63AUY=

DKIM の「検証(Verify)」に必要な作業



STEP 1 MTAにDKIM署名を検証する改修を実施する

- ①DKIM署名(DKIM-Signatureヘッダ)と ②メール本文、③DNSから得た公開鍵 により、メールごとにDKIMの検証が行えるようになる

STEP 2 DKIM検証結果をメールヘッダに格納する

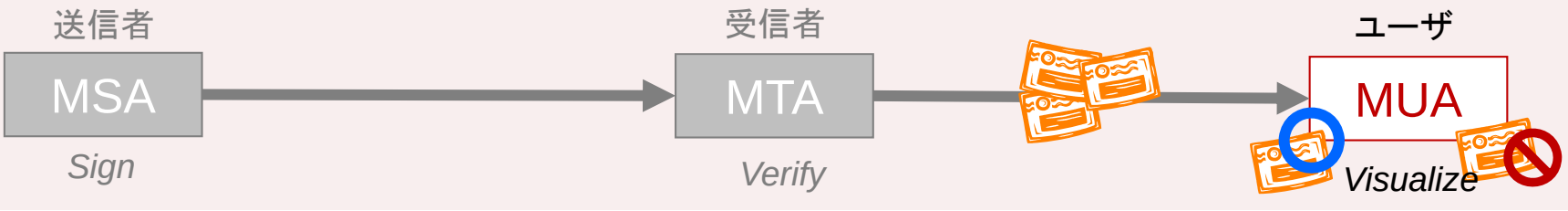
- DKIMの検証結果は ” Authentication-Results” という専用のヘッダに格納される
- このヘッダの内容を見ることで、MUAなどがメールの制御が可能になる

Authentication-Results:	example.com; sender-id=pass header.from=example.jp; **dkim=**pass (good signature) header.i=@example.jp

認証結果の一覧

主な結果	内容
pass	検証成功
fail	検証失敗
permerror	永続的検証エラー
temperror	一時的検証エラー
none, neutral	検証せず

DKIM の「可視化(Visualize)」に必要な作業



DKIM… その先の利用

- MUAでのAuthentication-Results利用
  - Authentication-Resultsヘッダだけでは分かりづらい
  - MUAやWebメール上で結果をわかりやすく表示

Gmailでの例
（特定のドメインで表示）

- Domain Reputation
  - ドメインごとに評判情報を生成し、迷惑メール判定等に利用
  - 受信者に評判の高いドメインは優先的に受信フォルダへ

- ホワイトリスト方式
  - PASS したものを「＋」に評価する
  - PASS しないものを標準と扱う

メールを如何に届けるか？

- ブラックリスト方式
  - FAIL したものを「－」に評価する
  - PASS したものは標準と扱う

なりすましを如何に拒否するか

現時点では

DKIM は「メールを如何に届けるか」という発想

※ 先にやってもリスクは少ない。逆にやらないでいるリスクは高くなる。

DKIMでは必ずしも“From: ヘッダ”のドメインで署名する必要はない

- 作成者署名
  - d= タグと From: で示すドメインが同一
  - 標準的な署名方法

DKIM-Signature:	（～略～） **d=example.jp**; **s=**dkim20101115; b=xdIeG4cUHIBhU0nix2V5tK9Z （～略～）
From:	<info@**example.jp**>
Subject:	こんにちは。
お世話になっております。 example.jp です。 …	

- 第三者署名
  - d= タグと From: で示すドメインが異なる
  - 以下の例はサブドメイン付きという違いだが、全く違うドメインでも可

DKIM-Signature:	（～略～） **d=sender.example.jp**; **s=**senderdkim20101115; b=xdIeG4cUHIBhU0nix2V5tK9Z （～略～）
From:	<info@**example.jp**>
Subject:	こんにちは。
お世話になっております。 example.jp です。 …	

基本的なメッセージとしては、

作成者署名を利用する

という大前提の元で以降のプレゼンを聞いてください。
第三者署名は作成者署名の利用が難しい場合の
Work Around と言ってもよいでしょう。

dkim.jp

DKIM署名

なるべく「作成者署名」を
できなければとりあえず「第三者署名」を

- 「作成者署名」の方が d=, From のドメインが一致しているため、受信者への見え方わかりやすい
  - Domain Reputation に利用される d=, From ドメインが一緒だから明確
  - **自分でしか**署名できないから第三者署名よりセキュア
- ただし、メール配信(設備)がある組織とそのDNSを管理する組織が異なる場合、「公開鍵を受け渡す」作業が発生
  - 公開鍵を受け渡す作業自体は難しくないが、その作業がDKIM普及のハードルになることも
  - 秘密鍵を組織間で受け渡すことは厳禁
- まずは「第三者署名」で代理的にメール配信設備側が用意したドメインで署名を開始し、こなれてきたら順次 作成者署名 に切り替えていくことでも可

2 dkim.jp の紹介

dkim.jp

Japan DKIM Working Group

DKIM の普及を目的として設立

dkim.jp

正式名称	Japan DKIM Working Group
通称	dkim.jp
設立日	2010 年 11 月 15 日
参加企業数	国内企業約 30 社が参加 オブザーバとして数団体が参加
Web サイト	http://www.dkim.jp

メンバー一覧 1

送信事業者 （13）
株式会社 アットウェア
エイケア・システムズ株式会社
株式会社エイジア
株式会社 HDE
シナジーマーケティング株式会社
トライコーン株式会社
トッパン・フォームズ株式会社
トランスコスモス株式会社
株式会社パイプドビッツ
ユミルリンク株式会社
楽天株式会社
株式会社レピカ

ベンダ （9）
株式会社アークン
株式会社インフォマニア
クラウドマーク ジャパン
株式会社シマンテック
センドメール株式会社
TrustSphere（ 旧BoxSentry)
日本オープンウェーブシステムズ株式会社
株式会社 日立ソリューションズ
メッセージシステムズ

メンバー一覧 2

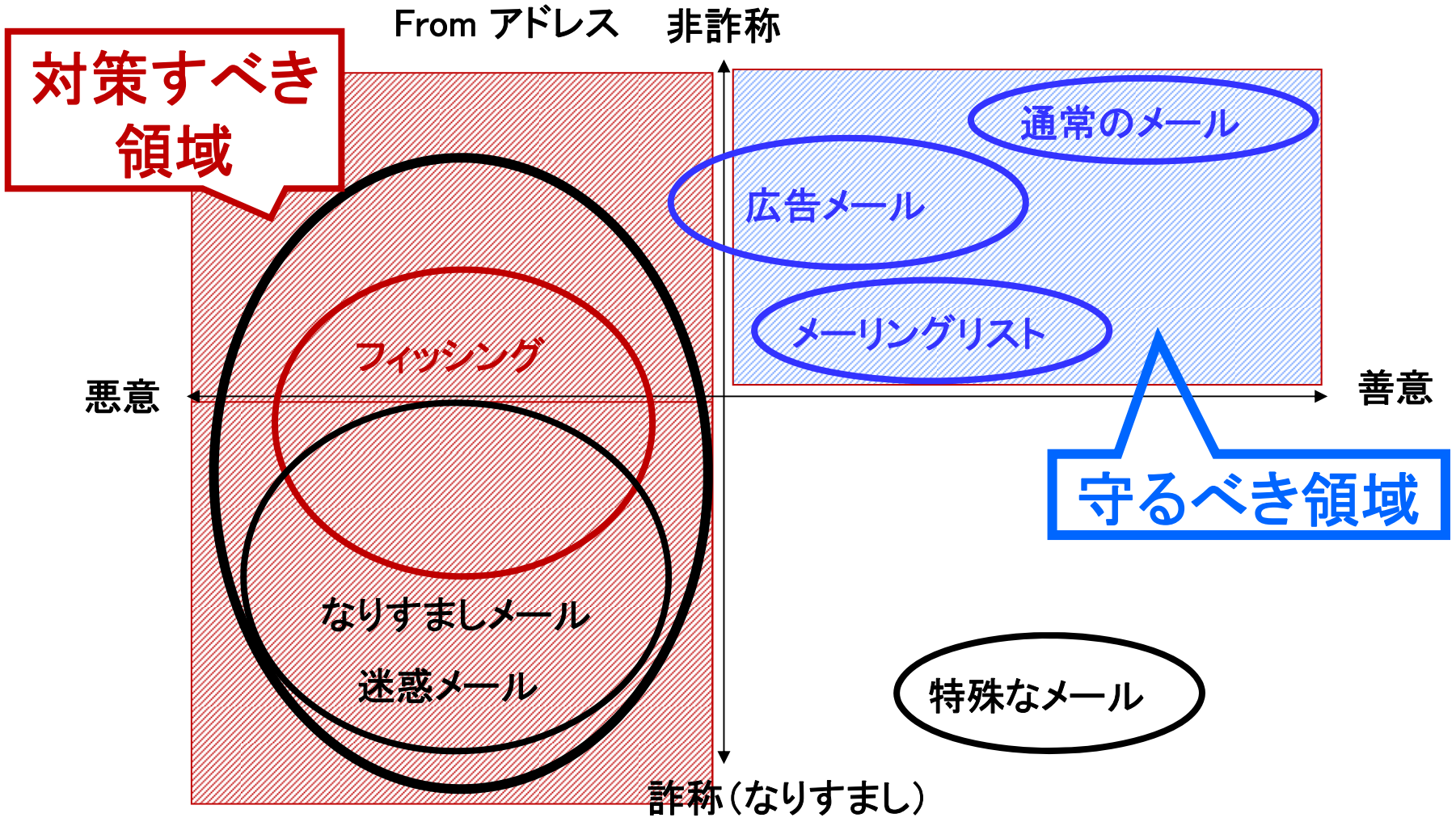
ISP （11）
イッツ・コミュニケーションズ株式会社
NECビッグローブ株式会社
株式会社NTTぷらら
ソネットエンタテインメント株式会社
株式会社テクノロジーネットワークス
株式会社ドリーム・トレイン・インターネット
ニフティ株式会社
フリービット株式会社
株式会社インターネットイニシアティブ
株式会社NTTPCコミュニケーションズ
ヤフー株式会社

協力団体・オブザーバ （6）
一般社団法人JPCERT コーディネーションセンター
eビジネス推進連合会
日本データ通信協会
総務省
フィッシング対策協議会
財団法人インターネット協会

- メンバー募集
  - ISP / ESP
  - Hosting / ASP
  - SIer
  - Vendor
  - Sender
  - MUA 開発者

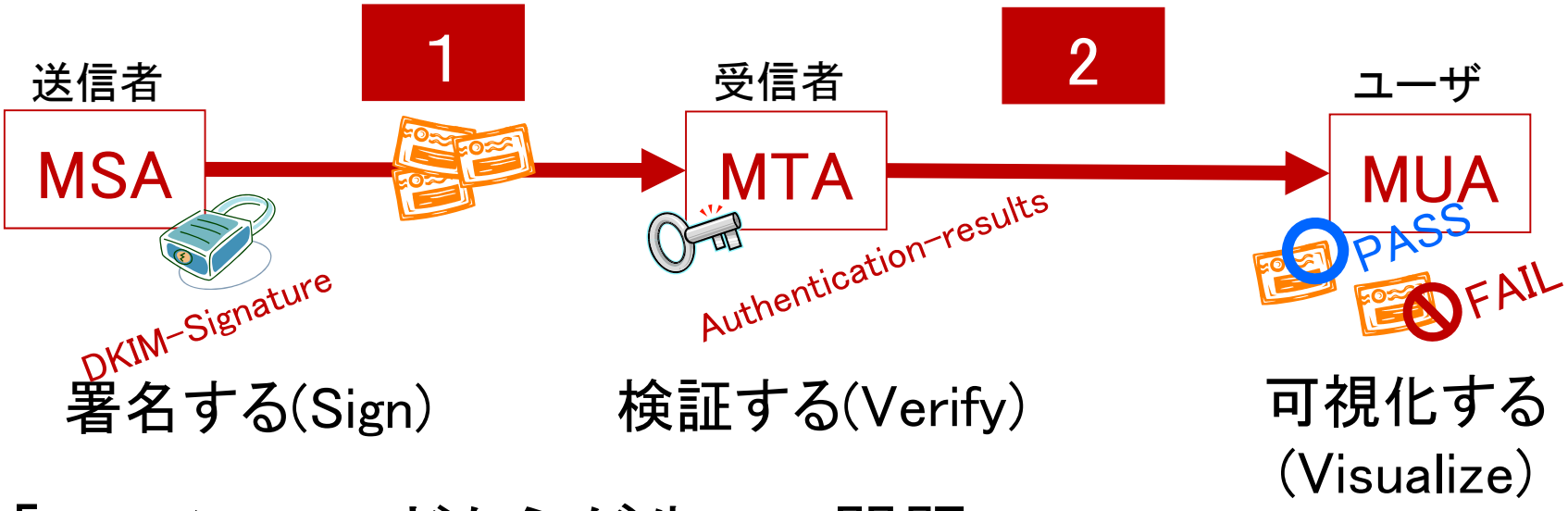
http://www.dkim.jp/dkim-jp/members/admission/

dkim.jp のスコープ



送信者とメールの正当性を検証する

一般的な DKIM 普及の課題



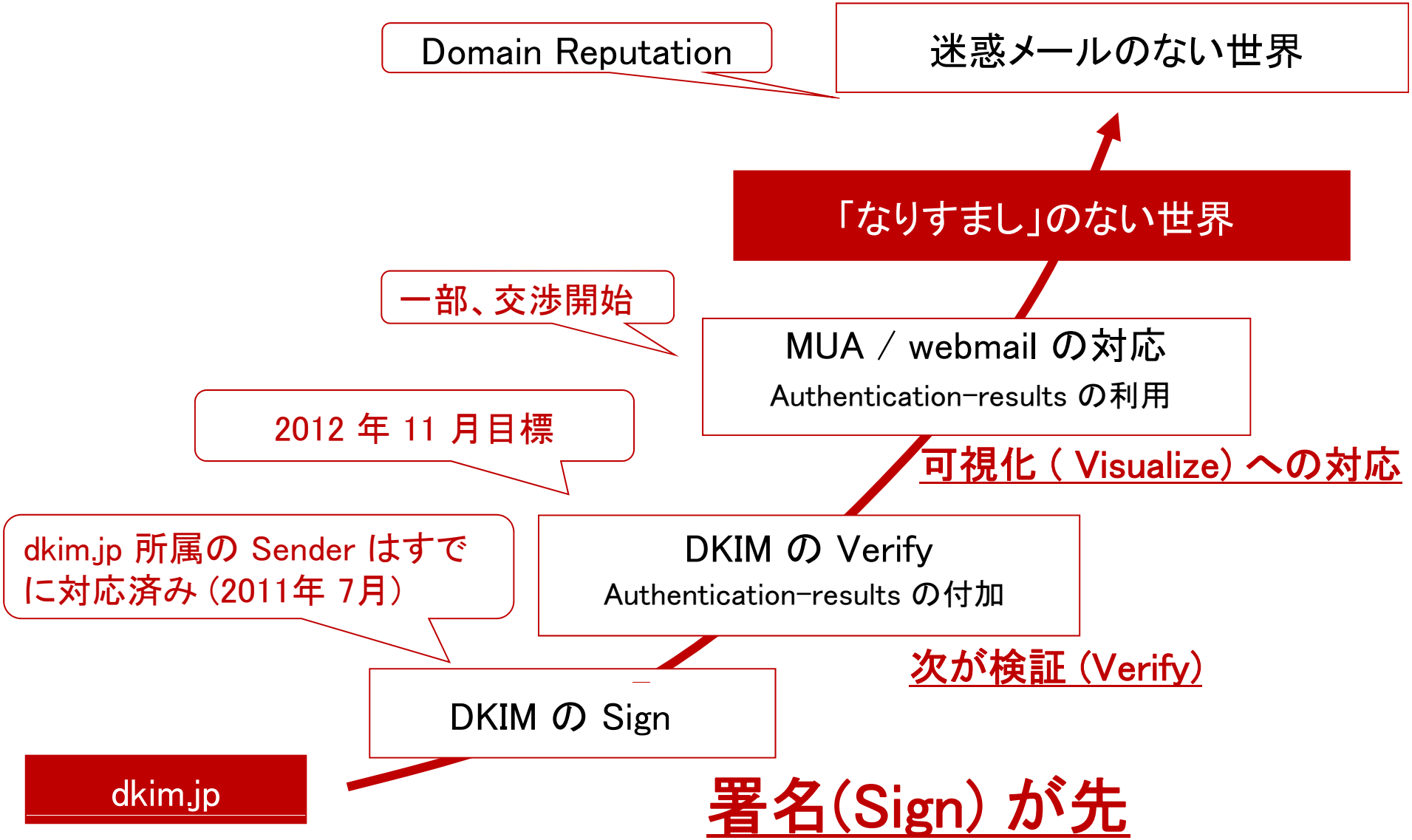
「Sign/Verify どちらが先？」問題

1	Signature（署名）がないから Verify（検証）しない Verify（検証）してないから Sign（署名）しない

「可視化」問題

2	MUA が対応してないと見た目で分からないから意味がない

dkim.jp のロードマップ



- 総会の開催
  - 現在、6回開催
- リコメンデーションの発表
  - Sender 向け発表
- Sender の DKIM Sign 対応
- RFC 6376 (4871bis02 の I-D) の和訳
- http://www.dkim.jp の web サイト公開

- Verify の促進
  - dkim.jp メンバー内：2012.11 目標
- 対応ドメイン数の増加
  - Hosting / ASP への対応の促進
- 認証結果の「可視化」へのフォーカス
  - MUA/Webmail の対応の促進

各種リコメンデーションの発表

3 DKIM の普及の現状

対応状況

- dkim.jp
  - http://www.dkim.jp/dkim-jp/dkim-services/
- データ通信協会
  - http://www.dekyo.or.jp/soudan/auth/

Sender の DKIM 署名対応状況

事業社名	DKIM対応開始（予定）	Status
トッパン・フォームズ株式会社	2008.12	対応済
株式会社パイプドビッツ	2010.9	対応済
楽天株式会社	2010.10	対応済
エイケア・システムズ株式会社	2010.12	対応済
株式会社エイジア	2011.5	対応済
株式会社アットウェア	2011.6	対応済
シナジーマーケティング株式会社	2011.6	対応済
株式会社HDE	2011.7	対応済
株式会社プロット	2011.7	対応済
ユミルリンク株式会社	2011.7	対応済
株式会社レピカ	2011.7	対応済
トライコーン株式会社	2011.9	対応済
トランスコスモス株式会社	2012.2	対応中 (新規入会)

※ dkim.jp 調査

ISP/ASP の DKIM 対応状況

	事業社名	Sign	Verify (Authentication-results 付加)
1	NECビッグローブ株式会社		○
2	ソネットエンタテインメント株式会社	○	○
3	ニフティ株式会社	○	○
4	株式会社インターネットイニシアティブ	○	○
5	ヤフー株式会社	○	○
6	Google 株式会社 (gmail)	○	○
7	Microsoft corp (Hotmail)	?	○

※ dkim.jp 調査

ISP/ASP の DKIM 対応状況

dkim.jp

	事業社名	Sign	Verify (AR 負荷)
1	イッツ・コミュニケーションズ株式会社		
2	株式会社NTTぷらら		
3	株式会社テクノロジーネットワークス		
4	株式会社ドリーム・トレイン・インターネット		
5	フリービット株式会社		
6	株式会社NTTPCコミュニケーションズ		

dkim.jp 所属企業は 2012 年 11 月 対応完了目標！

※ 対応を保証するものではありません。努力目標として 2011.11 を設定しています。

- 総務省の統計
  - http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/110302_3.pdf
  - 普及率は 10% 程度　(流量比)
  - 2011.7 に向けて普及率増加

- 当日は普及率を示すいくつかのデータを提示予定

エンタープライズ向けのサービスでは普及率が低い
（今日の主題）

企業への普及が課題

4 企業への DKIM 導入の課題

企業のメールの種類

dkim.jp

ここまでで説明してきた普及の話

これからの課題

非コミュニケーション

- メルマガ
- 販促
- パスワード
- リマインダ
- サービスのメール

コミュニケーション

- 業務用メール
- 顧客対応用、サポート利用
- メーリングリスト

ISP での Verify が始まる

DKIM の Sign をしよう

この後の主なスコープ

dkim.jp

企業のメールの DKIM 対応

Sign

B to C

- 自社「ドメイン」の保護
- 自社「顧客」の保護

→ Spammer の狙いは基本的にコンシューマ

Verify

- 自社・社員の保護

→ 最近は企業の「狙い撃ち」も

脅威の事例 (Phishing)

- Phishing → Sign
  - http://www.antiphishing.jp/
    - 2011年11月09日 セブン銀行を騙るフィッシング(2011/11/9)
    - 2011年10月18日 【注意喚起】銀行の第二認証情報を詐取するフィッシングにご注意ください(2011/10/18)
    - 2011年10月06日 三井住友銀行を騙るフィッシング(2011/10/6)

- Spear Phishing → Verify
  - 特定の企業や、企業の重要人物を狙い撃ちにする Phishing

(参考)

フィッシング対策協議会 (フィッシングレポート 2011)

http://www.antiphishing.jp/report/pdf/phishing_report_2011.pdf

日本の企業の 9 割は中小企業

MX RR の存在する jp ドメイン数: 94万ドメイン強

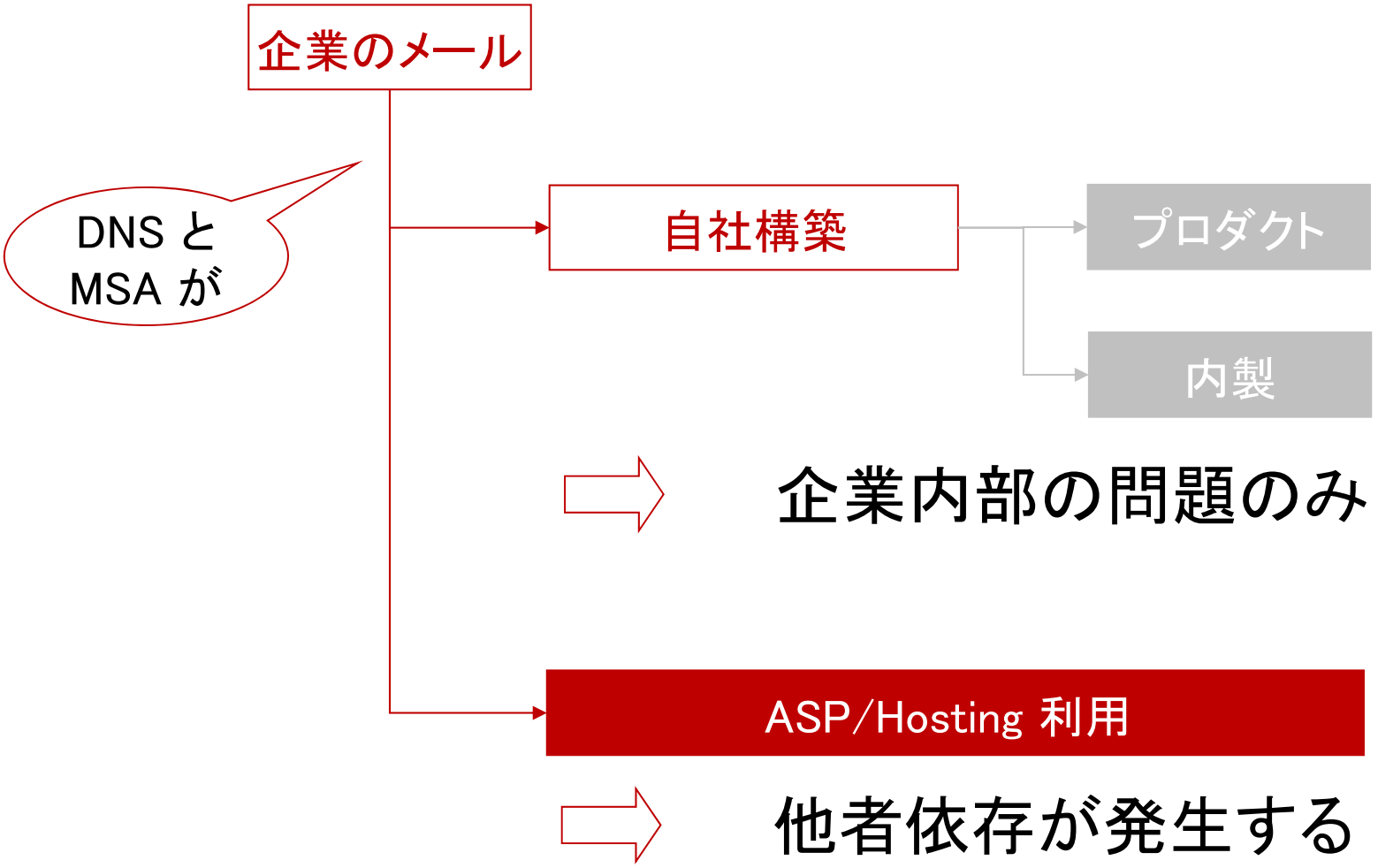
既に DKIM のサインされているドメイン数：約 5,000

（参考）

WIDE Project

http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

企業のメールの利用形態

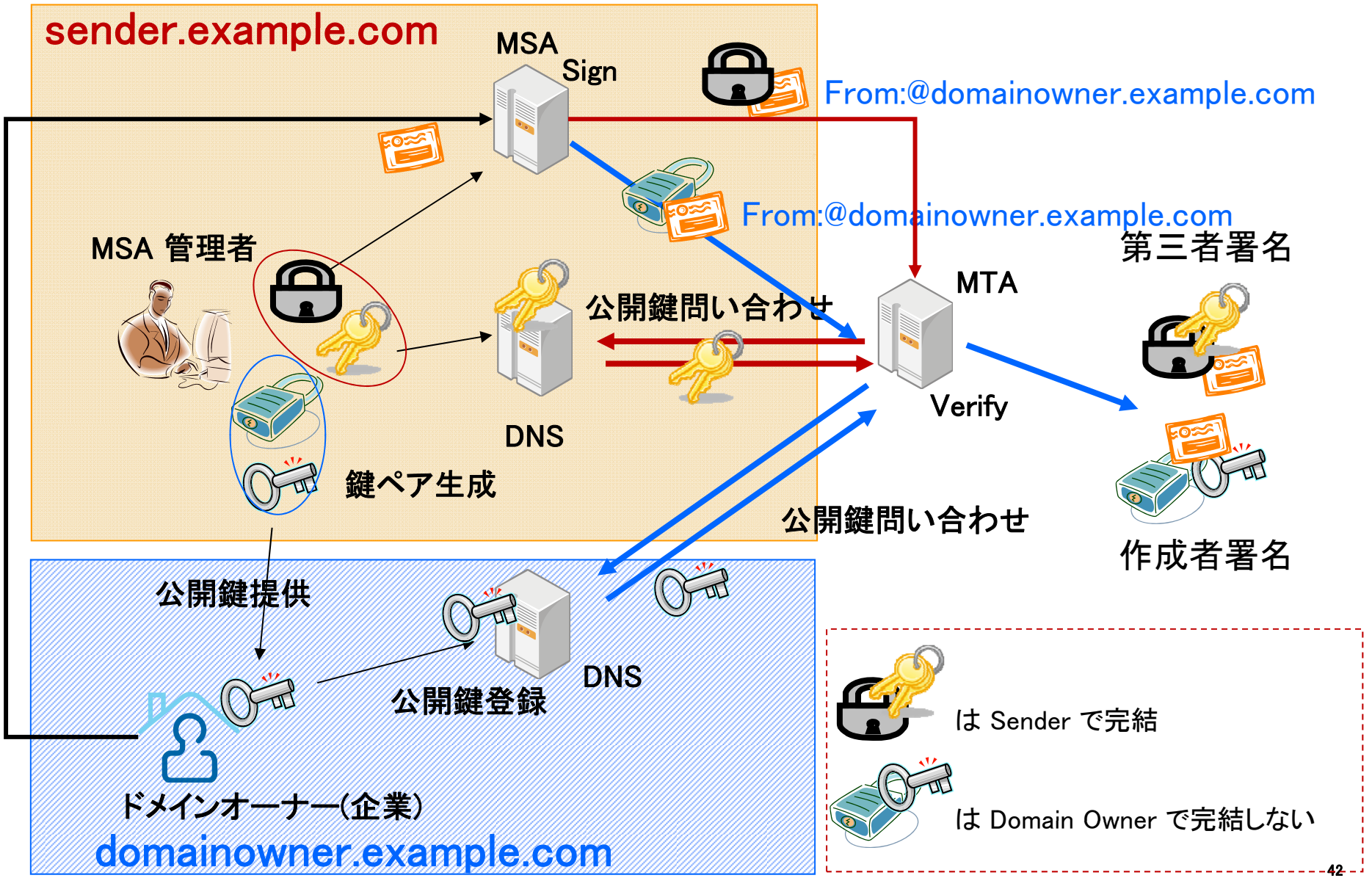


ASP/Hosting 利用

- 大半のドメインはこのパターン？
- メール流量は少ないがドメイン数は多い

- エンジニアが管理しているとは限らない
  - DNS と Sign する MTA が同じ管理下にあるとは限りらない （企業メールの特色？）
  - そもそも担当者がいないかもしれない

モデル化



STEP 1 第三者署名を展開する

-MSA の管理者だけで対応できる

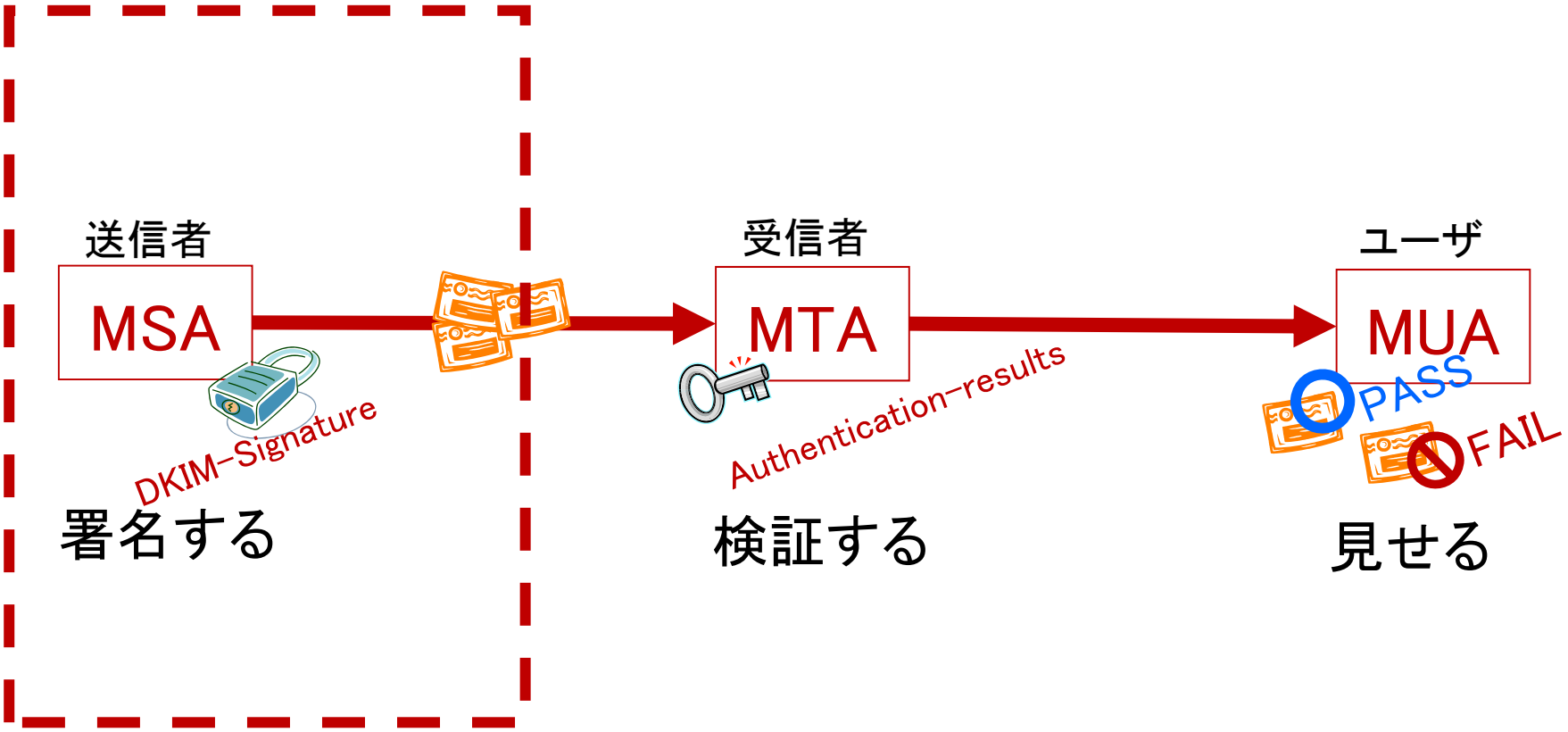
-この段階では、ドメインオーナーは何もしなくていい（ADSP は unknown を宣言するか、書かない）

STEP 2 作成者署名を展開する

-作成者署名が出来るなら、最初から作成署名で！

（エンタープライズドメインを扱う事業者へのメッセージ）

5 まとめ



まずは Sign を！！