資料1

技術ワーキンググループ
活動報告

2016.11.24

迷惑メール対策推進協議会

技術ワーキンググループ

活動記録

- 活動方針
  - 1回/月を目安に定期会合を目指す
  - 会合場所は構成員を中心に提供可能な場所を利用
  - 迷惑メールの状況や送信ドメイン認証技術の導入状況など定期的に情報共有
  - 必要に応じてEmail だけではなく SMS などメッセージングシステムを広く取り扱う
  - 活動の成果物 (2つのドキュメント) を作成
  - 会合の資料や議事録を事務局 (デ協) の Web で公開 (アクセスを構成員に限定)
- 会合記録
  - 第5回 2015.10.30 @ JIPDEC
  - 第6回 2015.12.01 @ Softbank
  - 第7回 2016.01.29 @ Softbank
  - 第8回 2016.03.11 @ Softbank
  - 第9回 2016.07.29 @ IIJ
  - 第10回 2016.09.09 @ Experian Japan
  - 第11回 2016.10.17 @ Biglobe

検討内容

- 対策技術の普及を目指したドキュメントの作成
  - 電気通信事業者による迷惑メールの踏み台送信対策の状況
  - 送信ドメイン認証技術とフィードバックループの推進
- DMARC技術の推進
  - 定期的な調査結果の共有 (普及状況，設定内容等)
  - 法的整理に関わる技術的ポイントの整理
- 情報共有
  - 送信ドメイン認証技術の関連技術や運用に関する紹介 (ex. ARC)

踏み台送信対策

- 背景
  - メール利用者のIDやパスワードが不正取得され，それらを用いた迷惑メール送信 (踏み台問題) が急増
  - 各社の踏み台送信問題への対策(ベストプラクティス)を共有し，国内のサービス事業者への普及を促進したい
- 概要
  - 6つの対策技術について概要をまとめる
  - 導入のための手順や準備期間等の情報を提供することで，導入負担についての情報提供もおこなう
  - 仕組みを図解することで理解を容易にする
  - 各社(10社)での6つの対策技術の導入状況を示すことで導入促進を促す

送信ドメイン認証技術とフィードバックループの促進

- 目的
  - 送信者情報を元に適切に受信判断ができる環境を目指す
  - これにより受け取るべきメールを確実に受信者に届ける
  - 踏み台送信対策や簡便なオプトアウトなど，送信側に有益な情報をフィードバックを利用して通知する
- 概要
  - これまで普及促進して来た SPF 及び DKIM の認証結果を利用する DMARC による送信ドメイン認証技術を普及させる
  - 認証したドメインを評価するドメインレピュテーションの仕組みを推奨する
  - 受信者が不要なメールを通知するフィードバックの導入を推奨する
  - 第三者等によるフィードバックの収集とそれらの情報を利用したドメインレピュテーションデータの構築，送信側への通知の仕組みの実現を目指す

ドキュメントの進捗状況

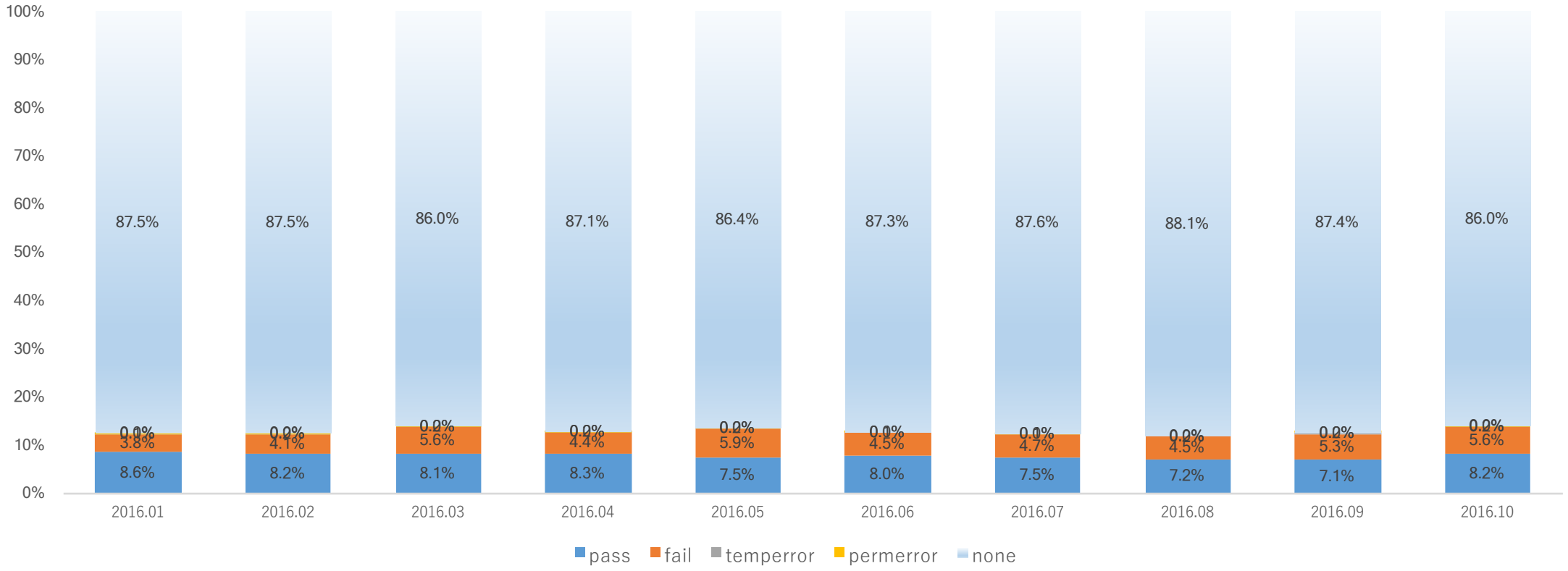
- 踏み台送信対策
  - 完成，公開を待っている状態
- 送信ドメイン認証技術とフィードバックループ
  - ほぼ完成，最終確認中
  - 前提となる DMARC の解説文書や導入マニュアルなども推進のためには必要
- 公開方法
  - 協議会のWebサイト (事務局) で公開予定 (ハンドブックや導入マニュアルと同様)
  - より多く参照して頂けるようにサイトを工夫予定
  - 迷惑メール対策カンファレンス (@ Email Security Conference 2016) で一部の内容を先行説明

情報共有
DMARC関連

- DMARC普及状況
  - 受信メールのドメインからDMARCレコードの広報状況を調査 (SBM)
  - 受信メールのDMARC認証結果割合を提示 (IIJ)
  - 他の調査結果を紹介 (Lars Eggert氏)
- DMARC関連情報
  - DMARCレコード中の宣言 Policy 割合
  - DMARCレコード中の主要レポート送信先
  - SPFとDKIMを含めた認証結果割合および認証失敗割合

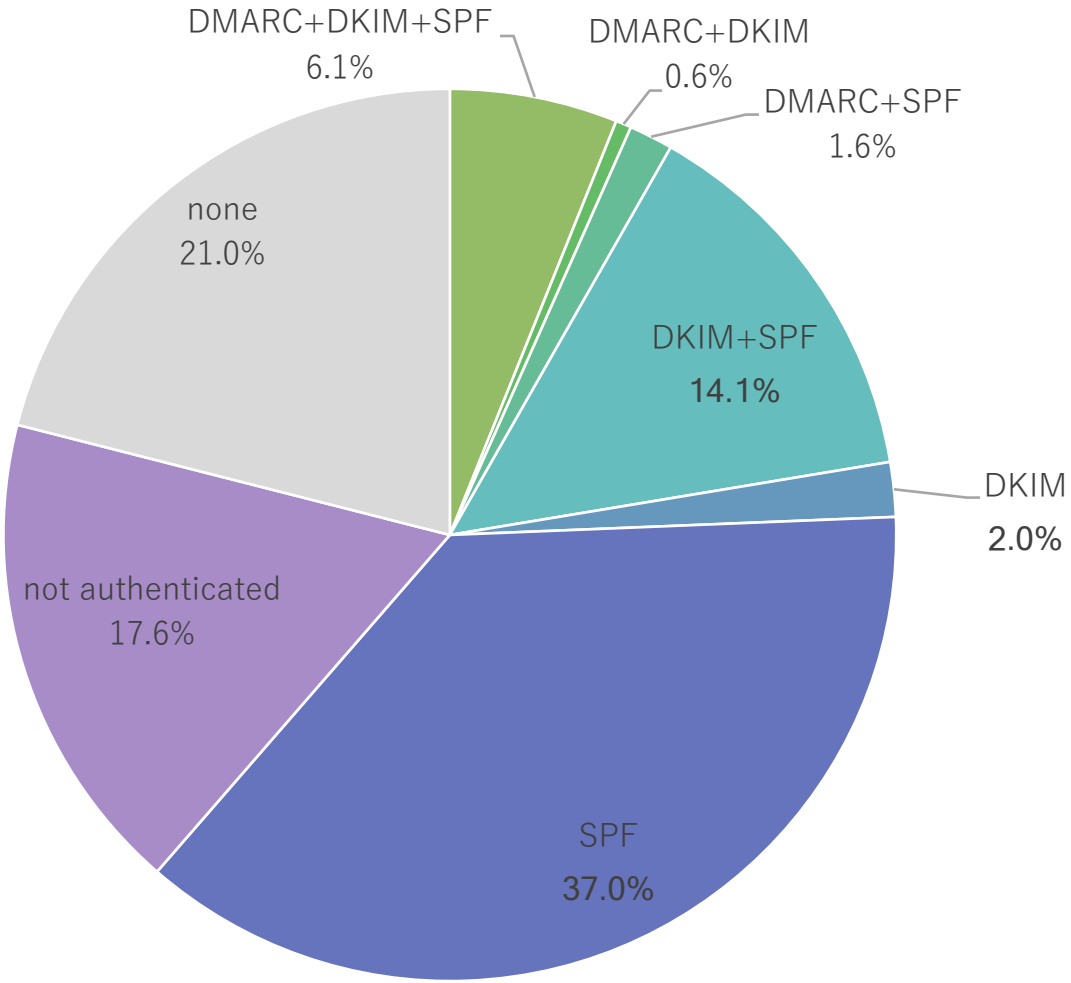
情報共有
DMARC関連 (例1)

- DMARCの認証結果割合の推移



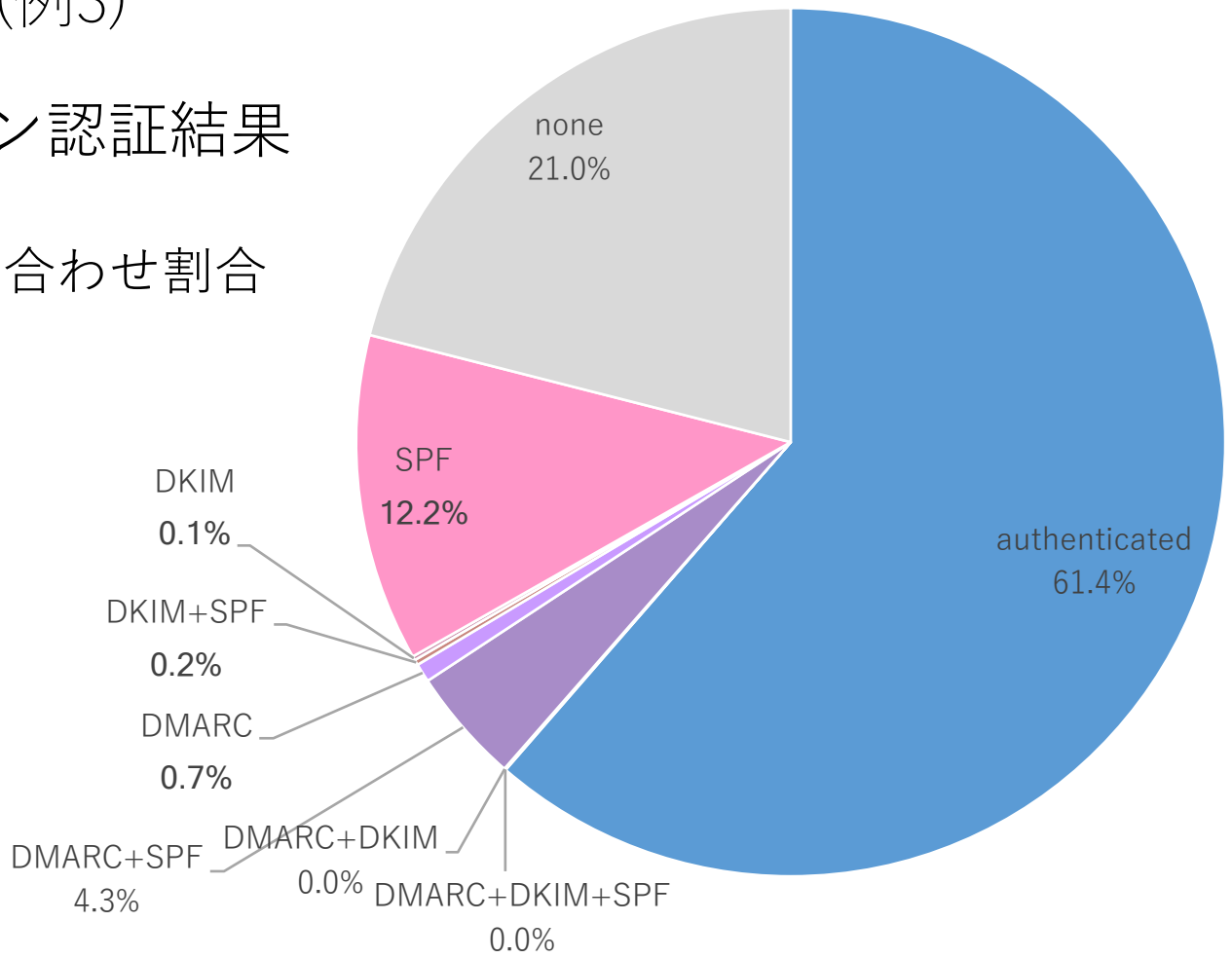
情報共有
DMARC関連 (例2)

- 送信ドメイン認証結果
  - 2016.10
  - pass の組み合わせ割合



情報共有
DMARC関連 (例3)

- 送信ドメイン認証結果
  - 2016.10
  - fail の組み合わせ割合



DMARC導入に向けた法的整理

- 概要
  - DMARCは既に整理がなされているSPF及びDKIMの認証を基盤とした技術
  - メール送信者が認証が失敗したメールの処理方法をポリシーとして表明(DMARCレコード) できる
  - メール受信側は認証結果をDMARCレポートして送信ドメインにレポーティングする仕組みがあり，これを用いてSPFおよびDKIMの設定改善に役立てることができる
  - 既に海外ではDMARCのポリシーに沿った受信処理を実施しているメールサービス事業者が複数存在している
  - ドイツの eco による「ドイツ法におけるDMARC準拠に関する報告」の共有
- 議論のポイント
  - DMARCレコードを表明するための要件 (もし必要であれば)
  - メール受信側がDMARCレポートを送信するための要件
  - メール受信側がメール送信側のポリシーに沿った処理ができるための要件

2016 年 11 月 15 日

送信ドメイン認証技術と
フィードバックループの推進

Rev.16101501

迷惑メール対策推進協議会
技術ワーキンググループ

1 はじめに

迷惑メールの問題は，受け取ることが単に迷惑というだけでなく，受け取ってしまうことで引き起こされる，様々な形での情報漏洩，計算機資源の不正利用といった，セキュリティ上の問題を引き起こす可能性の高い，より深刻なものへと変化してきている．そのためメールの受信側では，不要なメールを受け取らないようにするための対策を様々な段階で講じる必要性に迫られている．こうした対策の一方で，電子メールがコミュニケーションのためのツールとして，段々と使いづらくなってきているのではないかと懸念している．例えば，各種受信フィルタの影響で必要なメールが届かなかったり，届かなかった事実そのものが送信者に伝わらないことで，送り手と受け手の間で意思疎通が悪くなったり冗長なやりとりが別途必要になる，などが頻繁に発生しているのではないか，といったことである．

電子メールが配送される基本的な仕組みは，これまで長い間にわたって変更されてこなかったが，迷惑メールなどの問題を背景として，いくつかの新しい技術が拡張的に提案されてきた．送信ドメイン認証技術は，こうした新しい技術の一つであり，メール受信時に示された送信者を示す情報が，正しく表明されているかを検証することができるようになる．メールの送信者を明確に判断できることによって，迷惑メールによって引き起こされる様々な問題やメールの疎通問題を改善できる，メールの基盤技術として普及が期待されている．日本においても，送信ドメイン認証技術の一つである SPF (Sender Policy Framework) が，特に送信側での導入が進み，受信側でも認証結果を有効活用可能な段階まで普及が進んできた．今後は，送信ドメイン認証技術をメールの受信側を含めてより普及，活用していくことで，メールの利用環境を向上させていくことができると考えている．

本文書では，こうした送信ドメイン認証技術をさらに普及させ活用の機会を増やすことを目的に，送信ドメイン認証技術を中心とした新しい仕組みや技術が，現在のメールシステムの中で果たす役割やそれによって得られる効果を示す．具体的には，送信ドメイン認証技術をより普及させることで，受け取るべきメールを峻別できるようになること，メール受信者からのフィードバックを受けることでメール送信を改善していく，新しいメールの枠組みについて述べる．この枠組みを実現することで，必要なメールが確実に届き，不要なメールが送信されない，快適なメール利用環境を実現したいと考えている．

本文書の内容は，迷惑メール対策推進協議会の技術ワーキンググループで検討した内容を元にまとめられたものである．

2 取り組む課題

ここでは，新しいメール環境の枠組みが実現することによって，解決しようとする課題や軽減できると考えている問題について述べる．

- 届けるべきメールを見極め確実に受信者に届ける
- 不要なメールが届かないようにする
- 何らかの要因でメールサーバが不正利用された場合に速やかに対処できるような環境を目指す

送信ドメイン認証技術の普及により，メールの送信元が明確になることで，不要なメールをドメイン単位で判別したり，受け取るべきメールを峻別することが可能になる．また，送信元が明確であり相手が信用できる相手であるとすれば，一度購読手続き (オプトイン) をしたメールマガジン等を，購読解除 (オプトアウト) の

手続きを容易にできるようになると考えている．メール利用者がオプトアウトを簡便にできるのであれば，オプトイン自体も気軽にできるようになるはずである．これは，メール配信事業者にとっても，不要なメールを送信するコストを軽減し，必要な利用者に確実にメールを届ける機会を増やす，望ましい方向であると考えている．

近年，様々な形で ID やパスワードが流出し，それらが不正利用されるケースが頻繁に発生している．メールサーバの悪用もその一つで，何らかの方法で漏洩あるいは搾取したメール送信時の認証 (SMTP-AUTH) に利用する ID とパスワードを悪用し，正規のメールサーバを利用して迷惑メールを大量送信するケースが発生している．いわゆるメールサーバの踏み台問題である．こうした問題にも対処するため，受信したメールを送信側へフィードバックする仕組みを構築し，メール環境をより健全なものへと改善することを目指す．

3 課題解決に向けた施策

課題に対処するために，送信ドメイン認証技術とフィードバックループを活用する．具体的な活用方法について，以下に述べる．

- SPF[*1] や DKIM[*2] による認証結果とメール受信者が参照可能なメールヘッダ上の送信者情報と関連づける DMARC[*3] の利用へと発展させ，普及をはかる
- 認証したドメイン情報を利用してフィルタリングに活用する
- フィードバックループを利用し，フィルタリングに利用するためのドメイン情報の収集のために，認証された情報を含めて集約し分析する
- 認証された情報を元に不要なメールの購読解除 (opt-out) を円滑に行う
- フィードバックループを利用して不正利用された踏み台元に通知を行い改善を促す

3.1 DMARC の普及と活用

送信ドメイン認証技術の SPF と DKIM は，いずれもドメイン単位で送信者情報を認証するが，それぞれ認証に利用する送信者情報に違いがある．しかも，メール受信者が参照可能で通常は送信者と考える，メールヘッダ上の送信者情報 (RFC5322.From) とは異なる情報であるため，認証結果と見かけ上の送信者が必ずしもリンクしないことには注意すべきである．つまり，SPF や DKIM などの送信ドメイン認証はパスさせながら，送信者情報 (RFC5322.From) には別のメールアドレスを設定するといった，なりすましが簡単にできてしまう現在の仕組みを正しく理解しなければならない．また，送信者に何か特別な理由があって別々のドメインを設定している場合もあるので，全てがなりすましを目的に異なったドメインを設定しているとは限らないことにも留意が必要である．

DMARC は，SPF あるいは DKIM で認証したドメインと，メールヘッダの RFC5322.From 上のドメインが同じである[*4]かどうかを判断して認証する仕組みである．以下に，それぞれの送信ドメイン認証技術で参照する送信者情報の違いを示す．

DMARC では，メール送信側のドメインで認証が失敗したメールの取り扱いをポリシーとして表明するこ

[*1] RFC7208, Sender Policy Framework for Authorizing Use of Domains in Email, Version 1
[*2] STD76, DomainKeys Identified Mail Signatures
[*3] RFC7489, Domain-based Message Authentication, Reporting, and Conformance
[*4] もしくは親和性が高いドメインであることが前提

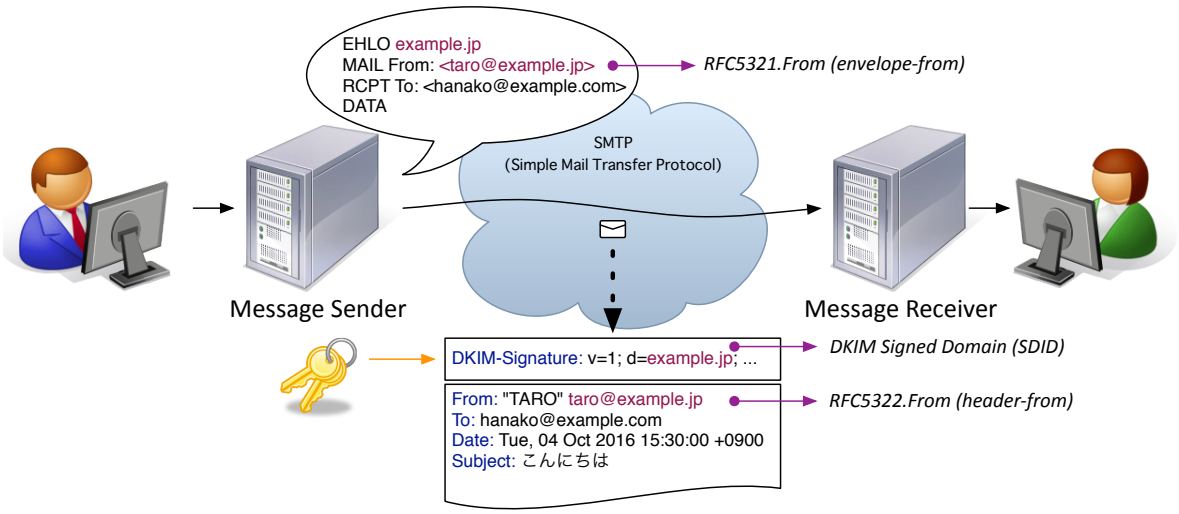


図 1　送信ドメイン認証技術で認証するドメイン

送信ドメイン認証技術	認証する送信ドメイン
SPF	RFC5321.From (envelope-from)
DKIM	署名ドメイン (SDID: Signing Domain Identifier)
DMARC	SPF あるいは DKIM で認証ドメインと一致する RFC5322.From (ヘッダ From)

とができる．このポリシーを受信拒否などより強い設定にすることで，メール受信者に対して認証が失敗したなりすましメールの扱いについての情報を与えることができる．

メールの送信側が，より強いポリシーを設定するためには，送信したメールの認証結果を知ることが重要である．DMARC では，認証が失敗した場合に送信者のドメイン管理元にレポートを通知する機能がある．このレポートを活用することで，意図せず正規のメールが認証失敗してしまうメールを特定することができ，送信側の設定等を改善することができる．また，正規のメールでない詐称メールがどの程度送信されているのかを把握することができる．これらの特徴により，今後 DMARC は，SPF および DKIM を含めて，より普及していく技術と考えている．

DMARC を利用し，メール受信者にも参照が容易な送信者のドメインを認証することで，送信者情報の詐称を防ぐことができる．これまでも述べられてきたことだが，メールの詐称を防ぐだけでは迷惑メール対策としては不十分であり，認証された詐称されていないドメインが，受け取るべき送信者のドメインであるかを判断をした上で受信すべきである．この受け取るべき送信者のドメインのリストを，データとして保持しておけば，DMARC 認証と組み合わせることで，必要なメールを確実に受け取ることができる．こうした受け取るべきドメインをホワイトリストとして集めて共有することができれば，より広い範囲でメールの疎通を向上させることが期待出来る．ホワイトリストの利用側は，各種迷惑メールフィルタが誤判定 (false positive) したとしても，受け取るべきメールが確実に届く環境を受信者に提供できる．

ホワイトリストに登録されているドメインのメールサーバが，踏み台に悪用された場合の対策も必要となる．この対策は，後述するフィードバックループにより実現され，逆にこのフィードバックループに適切に対

応できる送信側が，ホワイトリストとして登録されるべきドメインとして取り扱われるべきである．

3.2 ドメインレピュテーション

受け取るべきドメインを集めてホワイトリストとして管理することができれば，その逆の利用方法として，受け取るべきでない迷惑メール等の送信ドメインを同じように集めて利用することも考えられる．このようなメール受信時に，認証された送信ドメインに対して，受信すべきかどうかの判断基準を与えるドメイン評価の仕組みは，ドメインレピュテーションとよばれる．フィッシングなど，送信者情報を詐称したり紛らわしいドメイン名を取得して送信する悪質性の高いメールについては，送信ドメイン認証技術と組み合わせたドメインレピュテーションの利用が，対策として有効に機能すると考えている．

ドメインをホワイトリストに含めるかどうかの判断は，メール受信者が必要と考えるかどうかが基本であるが，フィードバックループと関連させた何らかの基準も必要と考えている．踏み台問題にみられるように，本来受け取るべきドメインであるが，突然不正なメールを送信する事案が度々発生している．いわゆるレピュテーションハイジャックと呼ばれる手法で，こうしたレピュテーションの高い，受信されやすいドメインを乗っ取る手法に対して，迅速に対処できる体制がホワイトリストのドメインには求められる．こうした基準が，ドメインレピュテーション自体の評価を高める上でも必要であると考えている．

3.3 フィードバックループ

これまで不要なメールに対する返信については，メールの送信者に返信をするとメールアドレスが実在し利用していることを送信側に知らせることになるため，あまり推奨されてこなかったという経緯がある．送信ドメイン認証が導入されることによって，送信者情報が明確になったとしても，一般的なメール利用者からみれば，認証された送信ドメインやメールソフト上に表示されている送信者情報などの情報から，本当に信頼できる送信者であるかどうかを判断することは難しい．

メール受信者からの不要なメールを通知するフィードバックループとしては，直接送信者に通知するのではなく，信頼できる第三者に送信することが望ましいと考えている．フィードバックを受け取る第三者は，通知されたメール (ヘッダ部分も含めた受信メールそのものが望ましい) を解析し，実際の送信者を見極め，信頼できる送信者からのメールであれば受信者が不要である旨を通知することで改善等を促す．実際の送信者を見極めるためには，メール受信側は送信ドメイン認証技術 (DMARC が望ましい) を導入し，その認証結果をヘッダ上に示しておく必要がある．

不要なメールを通知するとはいえ，フィードバックされるメールは適切に取り扱う必要があり，メール受信側とフィードバックの通知先の関係，フィードバック受信元から通知を送る送信者との関係それぞれには，契約等何らかの十分な信頼関係を事前に構築すべきと考えている．

フィードバックを受け取る側の利点は，こうした不要なメールの情報を集めることで，送信ドメインの情報やレピュテーションデータの構築に活用できることである．集められたレピュテーションの情報は，フィードバックを通知するメール受信側に提供することで，メール受信時の判断にドメインレピュテーションとして利用することができる．この提供するドメインレピュテーションの情報に，不要なレピューテーションの低いドメイン情報だけでなく，信頼できる送信者のドメインをホワイトリストとして含めることもできる．

3.4 メール環境の全体像

以下に，これまで述べた送信ドメイン認証技術 DMARC とドメインレピュテーション，フィードバックループを含めたメールシステムの全体構成の例を示す．

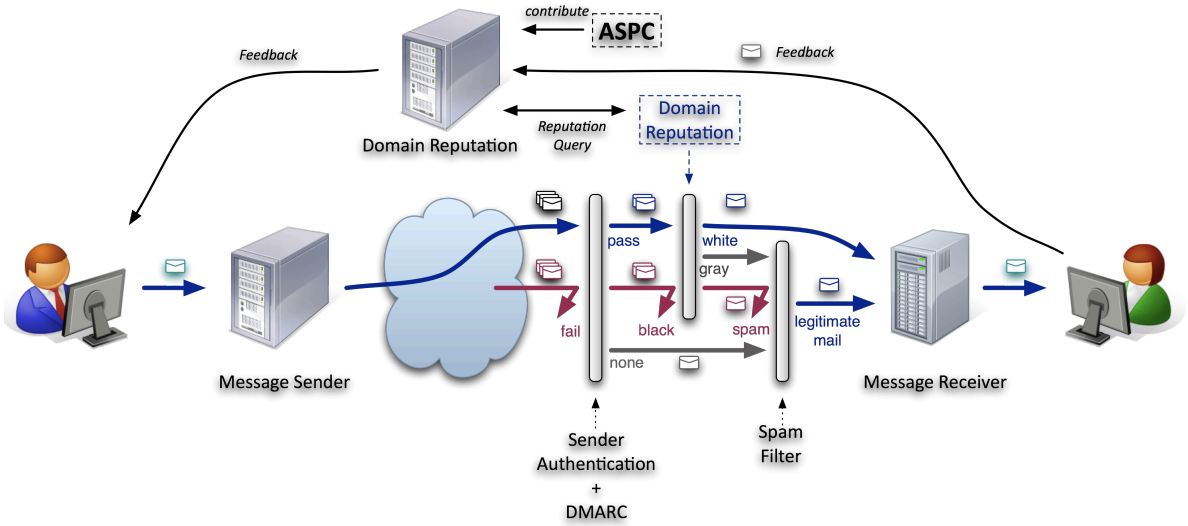


図 2　送信ドメイン認証技術とフィードバックループによるメールシステムの全体構成

これまで挙げた課題を解決していくためには，ここで挙げたメール環境における各構成要素が，それぞれの立場で新たに果たすべき役割や実現すべき機能要件が必要となる．これらの要件について，次節で述べていく．

4 メールシステムに於いて果たすべき要件

4.1 メール送信側

ここで対象とする“メール送信者”には，実際にメールを送信するメールサーバの運用者と，それらメールサーバから送信するメールが利用する送信者情報のドメイン (送信ドメイン) 管理者の両方が含まれる．これは，送信ドメイン認証技術を送信側として導入する場合には，必ず DNS への設定が必要となるためである．ドメイン名は組織を示すブランドの一つでもあるため，その維持および管理は適切に実施していく必要がある．メールの送信側に対する要件は，以下の通りである．

- DMARC を導入する，そのために SPF および DKIM も導入する
- フィードバックループのレポートを受け，受信者が不要と判断したメールの是正処理を行う
- メール配信事業者は，簡易的にオプトアウトできる仕組みの導入を検討する

4.1.1 送信側としての DMARC の導入

メール受信側が，受け取ったメールを DMARC で認証できるように送信側として DMARC を導入する．DMARC を導入するには，SPF および DKIM の導入が必要であるため，最終的には両方 (SPF と DKIM) を導入することを推奨する．SPF だけあるいは DKIM だけでも DMARC の認証ができる場合があるが，これまでも指摘されてきたように，正規のメールであっても SPF あるいは DKIM の認証が失敗していまうメールの運用形態の課題がある．こうした運用形態でも，SPF と DKIM の両方を利用することで，どちらかの認証ができてその結果 DMARC も認証できるようになる．できる限り SPF と DKIM の両方を導入することが望ましい．

全ての送信メールが，常に DMARC で認証できる状態を維持する．具体的には，DMARC レポート (aggregate report および failure report) を受信できるよう DMARC レコードを設定し，正規の送信メールが認証失敗している場合には，原因を特定し SPF あるいは DKIM の設定の見直しを行う．宣言すべき DMARC レポートのポリシーについては，ここでは正規の送信メールが DMARC 認証をパスすることを前提としているため，送信ドメインの管理者として，メール受信側がなりすましたメールをどう扱ってほしいかを検討した上で，適切なポリシーを設定するべきである．

4.1.2 フィードバックループの対応

メール受信者からのフィードバックを受けるドメインレピュテーション側から，不要なメールの通知を受け取り，同様のメールが同じ受信者に送信されないよう対応していく．

この対応は，メール送信者の立場によっても異なってくる．例えば，ISP など特定多数の利用者にメールサービスを提供している事業者では，メールの利用者がどのような状態でメール送信をしているのかが把握することが難しい．例えば，多数のメールアドレスに対して，意図して迷惑メールを送信している場合もあれば，利用している PC などが不正プログラム (マルウェア) に感染しており，利用者が認識せずに外部から勝手に制御されて迷惑メールを送信している場合などもある．いずれにしても，ISP としては，フィードバックを受けた場合に，そのメールの送信者を特定し，当該利用者がメール送信ができないように一時的に利用を停止するなどの措置が必要である．メールの送信者を特定するためにも，メール送信時に認証を行う SMTP 認証 (SMTP-AUTH) を必須とすべきである．SMTP 認証は，メール送信を一時的に停止する場合にも有効な手法であり，認証を無効とすることで，メール送信を抑制することができる．ISP は，こうした一時的な停止の一方で，メール利用者に連絡をとり適切な対応をすべきである．

顧客からメール内容と宛先リストを受け取り，メール配信設備をもたない顧客に代わって送信するメール配信事業者の場合，対応が難しい場合がある．メール配信事業者の場合，配送依頼元から委託されて配送処理を行うといった構造のため，指定された宛先がメールを必要としているのか，メールの内容が適切なものであるかを事前に把握することが難しいためである．つまり，メール受信者から送られてきたメールが不要であると意思表示された場合，配信事業者が，そうしたメールを配送すべきかどうかを決める権限やそもそも止めるための仕組みを持っていないなどのケースが考えられるためである．しかしながら，メール配信事業者がフィードバックを受けた場合，同様のフィードバックを配送依頼元にも通知し，何らかの改善を促す対応が必要であろう．また，あまりにもフィードバックが多い場合など，配信事業者の判断でメール配送を一時中断するなどの措置がとれるようにすべきである．

4.1.3 簡易オプトアウト機能の導入

ここで述べているメールシステムの全体構成では，メール受信者が不要なメールをフィードバックとして通知する流れとしており，フィードバックの通知先としては，ドメインレピュテーションを想定している．メールの仕組みの中では，以前からメール受信者が直接メール送信元にメールが不要であることを通知する仕組みが規格[*5] として提案されている．この規格では，メーリングリストに対するコマンドの幾つかをメールヘッダとして記述する．このメールヘッダの一つに，List-Unsubscribe ヘッダがあり，これを利用することでメーリングリストからの退会が可能になる．

設定例

```
List-Unsubscribe: <http://www.example.com/list.cgi?cmd=unsub&lst=list>,
        <mailto:list-request@example.com?subject=unsubscribe>
```

List-Unsubscribe ヘッダでは，mailto:に続くメールアドレスや URL などを指定することができる．メール受信者が，これらの宛先にメールで連絡したり URL にアクセスすることで，送信側が登録を解除する．主要なメーリングリストソフトウェアや，幾つかのメール配信事業者などでは，既に List-Unsubscribe ヘッダを利用できる仕組みを提供している．メール受信側でも，Web メール機能の一つとして，List-Unsubscribe ヘッダがある場合にリスト登録解除のアクションがとれるような表示 (ボタンやクリック可能なリンクの表示等) を行う，といった機能を提供しているところがある．

こうした，メール受信者がメール送信側に直接意思表示ができるような機能は有益であるが，注意も必要である．これまでも，迷惑メールの本文の末尾等に示された宛先に登録解除の連絡をしたことで，逆にメールの存在を伝えることになり，さらに迷惑メールが増加したといった事例などもよく指摘されてきた．メール受信側では，List-Unsubscribe ヘッダがある場合に，単純に登録解除ボタンを表示するのではなく，送信ドメイン認証を行い送信者情報がなりすまされていないか，認証が通ったドメインが正しく登録解除する送信元であるかを評価した上で，表示をすべきである．メール受信側が，こうした判断を適切に行うためにも，送信ドメイン認証技術とドメインレピュテーションが有効に機能すると考えている．

4.2 メール受信側

メール受信側では，受信したメールを送信ドメイン認証技術 DMARC で認証し，適切な処理をする．受信したメールの処理方法については，メール利用者も含めて受信側で判断すべきだが，図 2 では一例として，認証したドメインをドメインレピュテーションを利用して篩い分ける流れを示した．

メール受信側に対する要件は以下の通りである．

- 受信メールを SPF と DKIM, DMARC で認証する
- 認証したメールを受信側の方針に基づいて適切に処理する
- メール受信者が届いたメールの中で，不要あるいは届けるべきメールではないとメール受信側に示すことのできる機能 (Web メールでのボタンなど) を提供する
- メール受信者が申告した不要なメールを契約等の関係を結んだドメインレピュテーションに送信する

[*5] RFC2369, The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields, https://www.ietf.org/rfc/rfc2369.txt

DMARC で認証するためには，SPF および DKIM でも認証する必要がある．そのため，メール受信側としては，受信メールを SPF, DKIM, DMARC それぞれで認証できるように各認証機能の導入が必要となる．

認証されたメールの扱いとして，受信側ですべきことは，届けるべき送信ドメインからのメールとメール受信者に参照できるようにすることである．ここで届けるべきメールとは，いわゆるホワイトリストに登録されているような送信元 (ドメイン) で，フィードバックを受けた場合に適切に対応できる送信者のドメインなどを想定している．もちろん，メールサーバを踏み台にされて，参照するだけでも危険なマルウェア等を含むメールがホワイトリストのドメインから送信される可能性もある．そのため，メール受信者を守る立場の受信側としては，ホワイトリストドメインからのメールであってもアンチウイルス等のフィルタでの検査はすべきであるし，引き続き危険度の高い実行形式の添付ファイルなども制限すべきかもしれない．

不要なメールを簡便にフィードバックを行う方等として，Web メールなどのインタフェースで迷惑メールなどのボタンの提供がある．メール受信者がこのボタンをクリックすることで，当該メールをフィードバックとして，メール受信側が関係を結んだドメインレピュテーションに送信する．Web フォームや申告先のメールアドレスを提供する方法もあるが，フィードバックには，ヘッダ情報も含めてメール全体を送信することが必要となるため，通常の MUA[*6]の転送機能等では情報が不十分な場合がある．

送信の方法としては，受け取るドメインレピュテーション側にも依存するが，メールのフィードバックであることから，メールでの送信が適していると考える．送信するフィードバックのメール形式は，既に ARF[*7] として規格が提案されている．当然のことながらフィードバックは，受信するドメインレピュテーション側で DMARC で認証可能なメールとして送信すべきである．

メール受信者がフィードバックする際には，不要なメールとはいえメール受信者宛に届いたものなので，メール受信側は，その内容がドメインレピュテーションという第三者に送信されることの同意を取ることが望ましい．最初に迷惑メールボタンを押した際に，対象のメールの利用目的等とともに第三者に送信することを示し，同意のボタンを押してもらうなどの仕組みを用意するなどの方法が考えられる．メール受信者に対して，不要なメールを積極的にフィードバックしてもらうためにも，申告したメールがどのような用途に用いられるのかを示し，申告することで迷惑メールがかえって増えることが無いのか等の不安を払拭するべきである．

4.3 メール受信者

メールを最終的に受け取る受信者としてすべきことは，不要なメールが届いた場合に，メール受信側の機能等を利用してフィードバックすることである．もちろん，自身がオプトインをして購読を登録したメールマガジン等については，そのオプトアウト方法が明確であれば，正規の手段でオプトアウトすべきである．

4.4 ドメインレピュテーション

ドメインレピュテーションとは，送信ドメイン認証技術等で認証されたドメイン名に対して，さらに受け取るべき送信ドメインであるかを判断する指標である．ここでのドメインレピュテーションは，フィードバックを受信者から受け，適切な送信者に通知を行いながら，不要なメールの情報からドメインを分析することを含めてドメイン評価の指標を構築する役割を指す．

[*6] Mail User Agent, Outlook や Thunderbird などのメールの送受信を行うソフトウェア

[*7] RFC5965, An Extensible Format for Email Feedback Reports, https://www.ietf.org/rfc/rfc5965.txt

メールの受信者および受信側が，フィードバックを送るべきかどうかを，メール送信者 (=フィードバックの宛先) 情報から個別に判断することは一般に難しい．メール受信者が，一律に不要なメールを信頼できるフィードバックの受け手 (=ドメインレピュテーション) に送信し，ドメインレピュテーション側が適切に判断した上でメールの送信者に通知する仕組みであれば，メール受信者も安心してフィードバックができるようになる．ドメインレピュテーション側では，多数のメール受信者から不要なメールの情報を多く受け取ることで，受け取るべきでないドメインの情報量が増え，より精度の高いドメインレピュテーションの分析が可能となる．通知される送信者にとっても，送信したメールに対する評価がより多くの情報から得られる方が，信頼性も高まる．このように，ドメインレピュテーションを介したフィードバックにはそれぞれのメール利用者にとって，大きな利点があると考えている．ドメインレピュテーションが果たすべき役割について以下に述べる．

- メール受信者からのフィードバックを受ける
- フィードバックの内容を解析し，適切な送信者に通知を行う
- 通知すべき相手が存在しないフィードバックの場合，送信元情報を利用しレピュテーションデータとして活用する

以下，それぞれの役割で果たすべき要件を述べる．

4.4.1 フィードバックの受信

フィードバックの受信時，これがフィードバックを受け取るべき送信元であるかを DMARC など送信ドメイン認証技術で確認する．不特定多数からのフィードバックは，迷惑メールの場合と同様に偽のフィードバック情報を元に送信側へ誤った通知してしまう危険性があるため，信頼できるフィードバック送信元からのメールに限定すべきである．

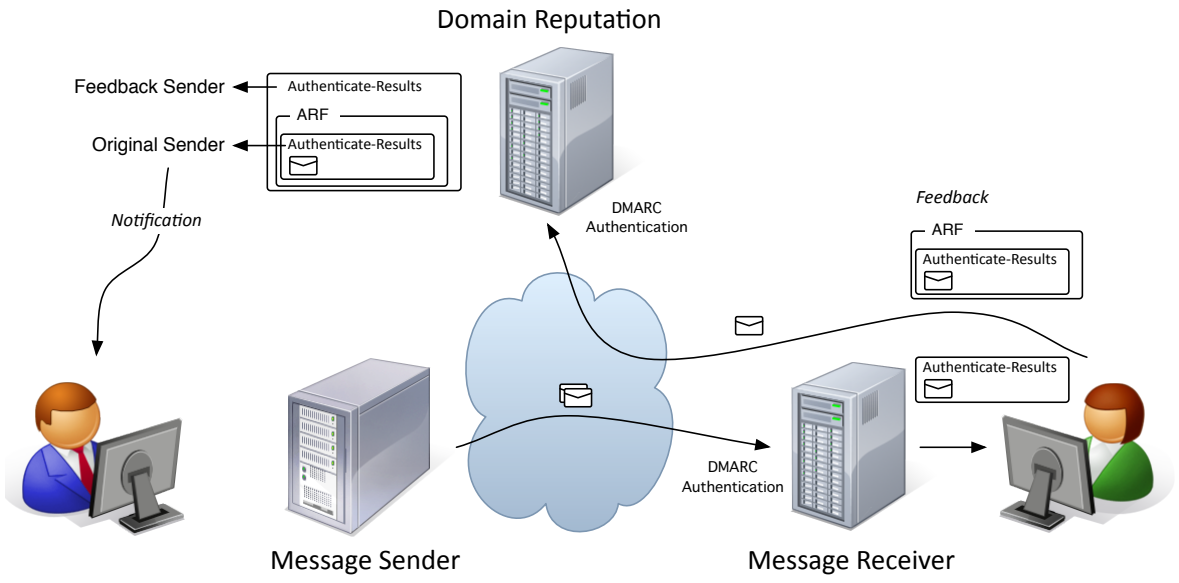


図 3　フィードバックの受信

正しい情報をフィードバック先である送信側に通知するためには，フィードバック送信元の認証結果，フィードバック情報に含まれる不要なメールの送信元の認証結果，その不要なメールの送信元がフィードバックの通知先であることが確認できる仕組みが求められる．これらそれぞれの段階での確認にも，送信ドメイン認証技術 DMARC を使って認証を行うことが望ましい．認証したドメインを判断 (評価) していくことで，最終的に送信者に通知すべきフィードバックであるかどうかを判断する．

4.4.2 送信者への通知

フィードバックされたメールを確認し，元々の送信者を特定することで，正しく通知すべき送信側を特定する．通知すべき送信側とは，単にフィードバックされたメールから送信元を特定し，自動的に全ての送信元を対象にするのではなく，通知することで適切に対応することが予想される相手に限定して通知を行うべきである．

こうした通知すべき送信者を判断する方法の一つとして，あらかじめ送信側と契約等の取り決めを結ぶことが考えられる．例えば，通知方法 (メール等) や通知先 (メールアドレス)，通知のタイミングや通知に対する処理結果等の連絡を必須とするのかなど，事前に明確にしておくことが望ましい．ドメインレピュテーションとしても，こうしたフィードバックの通知を適切に対応していくメールの送信者であるか，繰り返し同じようなフィードバックが受信者から送られてこないか，などのデータを蓄積することで，ドメインレピュテーションデータを役に立つデータとして維持管理していくことができる．例えば，通知を受けてからの対応処理の時間が短い，処理結果を迅速に連絡する，など受信者にとって好ましい対応する送信側に対しては，ホワイトリストなど高いレピュテーションの指標を与えるといったことが考えられる．

ドメインレピュテーションの責任としては，メール本文に示された連絡先にオプトアウト連絡をしても，効果が薄いどころかかえって迷惑メールが増えるといったことを繰り返さないような役割を果たすべきである．

4.4.3 レピュテーションデータの構築

レピュテーション側には，通知すべき送信者のいないフィードバックも多数集まることが予想される．こうしたフィードバック情報については，メール受信者が不要と判断しているメールであり，受信側で送信ドメイン認証されたドメイン情報を含む貴重なデータである．従来から，迷惑メールを送信してくる IP アドレスの情報を集め，ブラックリストとして提供している組織が幾つか存在している．こうした組織と同様に，認証されたドメインの情報や，送信元の IP アドレスの情報などを蓄積，分析することで，より有益な迷惑メール対策のための情報として利用することができると考えている．

5 普及に向けて

ここでは，送信ドメイン認証技術 DMARC とドメインレピュテーション，フィードバックそれぞれの概要と関連について述べ，現在のメールシステムが抱えている課題について解決すべき方向性を示した．その中で，メールシステムの全体構成を示し，メールの送受信者やドメインレピュテーションなど，各構成要素が果たすべき要件について述べた．

新しい機能や仕組みを普及させるには，それを導入することの利点が不明確な状態ではなかなか進展しないと考えている．本構成では，いずれの構成要素に対しても，十分な利点があると考えており，メールシステム全体にとっても，届けるべきメールが確実に届き，不要なメールが送受信しにくくなる状況に近づけていけるものと考えている．今後，ここで述べた要件を具体的に機能させていくことで，想定された利点が実現されて

いるのかを検証していきたいと考えている．

迷惑メール対策推進協議会の技術ワーキンググループでは，他の関連団体とも協力しつつ，送信ドメイン認証技術 DMARC とフィードバックの仕組みを実現すべく，こうした検討や取り組みを続けていきたいと考えている．

電気通信事業者による迷惑メールの踏み台送信対策の状況（概要）

背景

近年、利用者の送信者IDおよびパスワードが何らかの方法で大量に不正取得され、それらを用いた迷惑メール送信が急激に増加している。言い換えれば、迷惑メールは事業者各社の正規の送信サーバから大量に発信されている。そのため、事業者の送信サーバがブラックリストへ登録されやすく、利用者のメールが届きにくい状況（特に海外宛）が発生している。

このような迷惑メール送信方法は「迷惑メールの踏み台送信」と呼ばれ、SMTP認証や送信トラフィック制御といった従来の迷惑メール対策技術だけでは防止することが困難になっている。ここでは、各社の踏み台送信問題への対策（ベストプラクティス）を共有し、国内のサービス事業者全体で踏み台送信問題に取り組んでいくきっかけとする。

主な対策技術と効果

対策名	対策概要	踏み台送信問題への効果等
①SMTP認証と送信通数制限	送信者IDあたりの送信通数に制限を設ける方法。	すでに導入事例は多く、基礎となる対策といえる。
②送信IPアドレスの分離	送信メールの内容を元にしたレピュテーションを用いて、迷惑メールと判定したメールとそうでないメールを別々のIPアドレスから送信する方法。	ブラックリスト登録の影響範囲を局所化する効果がある。
③接続元情報による制限	接続元のIPアドレスや地域情報を元にしたレピュテーションを用いて、迷惑メール発信元と判定した場合にはペナルティを与える方法。	現在は、海外接続や複数地域からの同時接続が多いため、効果は高い。
④マルチ要素認証	SMTP認証やパスワード認証以外の方法で本人認証を実施し、送信者IDの不正利用を防止する方法。	不正利用の防止効果は高いが、利便性低下が懸念される。
⑤送信者詐称の制限	SMTP認証結果と、送信者情報の一致性を用いて、なりすましを見分ける方法。	効果は高いが、第三者送信による偽陽性も考えられる。
⑥利用者への啓発	不正利用のリスクを伝え、対策を知ってもらう方法。	フィッシングを未然防止する意味で、効果はある。

対策技術の紹介（①SMTP認証と送信通数制限）

対策概要

SMTP認証を用いて送信者IDを特定し、送信ID／単位時間あたりの通数制限をする。また、POP before SMTP や認証なしの送信も禁止する。

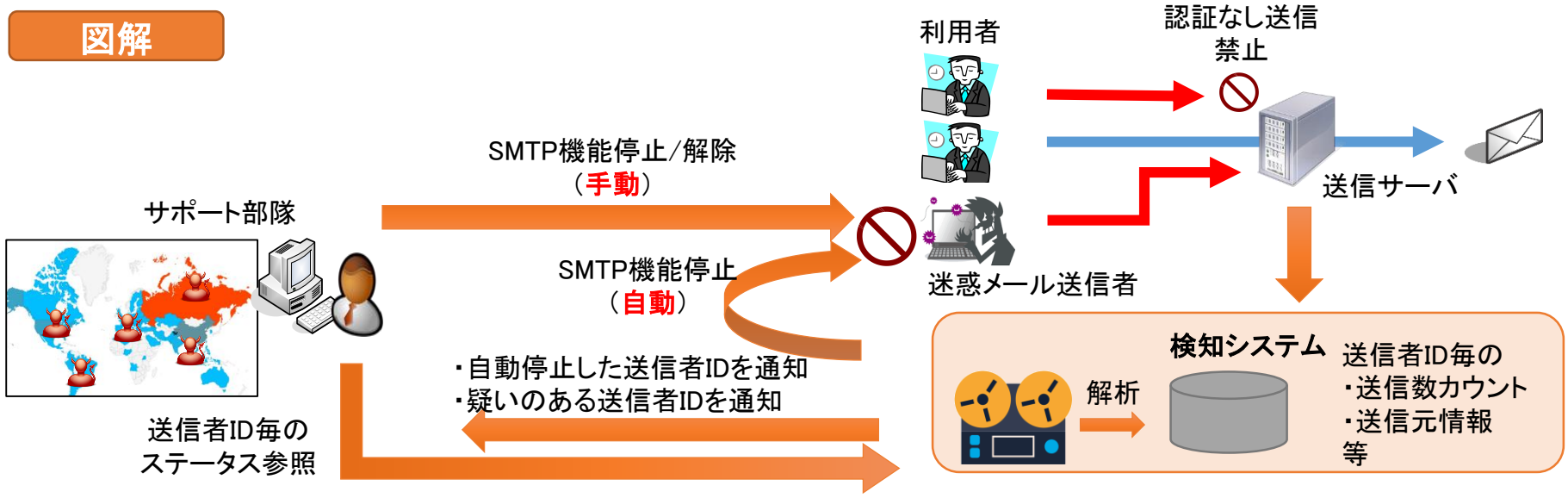
準備期間

準備期間： 6か月 （B社の場合）

導入準備

1. 利用者／サポート部隊への周知
2. 利用規約／契約約款の変更
3. 疑わしい送信者IDの検知や自動停止する仕組みの実装
4. サポート部隊向けの支援ツールの作成
   - 送信者IDごとの送信数／送信元IPアドレスを調べる機能
   - 送信者IDのSMTP機能だけを停止する機能
   - 送信IPアドレスが多い送信者IDを調べる機能
5. サービス提供

図解



対策技術の紹介（②送信IPアドレスの分離）

対策概要

送信メールのヘッダー情報や本文をもとにして迷惑メールとそうでないメールに分類し、それぞれを異なる送信IP アドレスを持つ送信サーバから配送し、ブラックリストによる影響を局所化する。

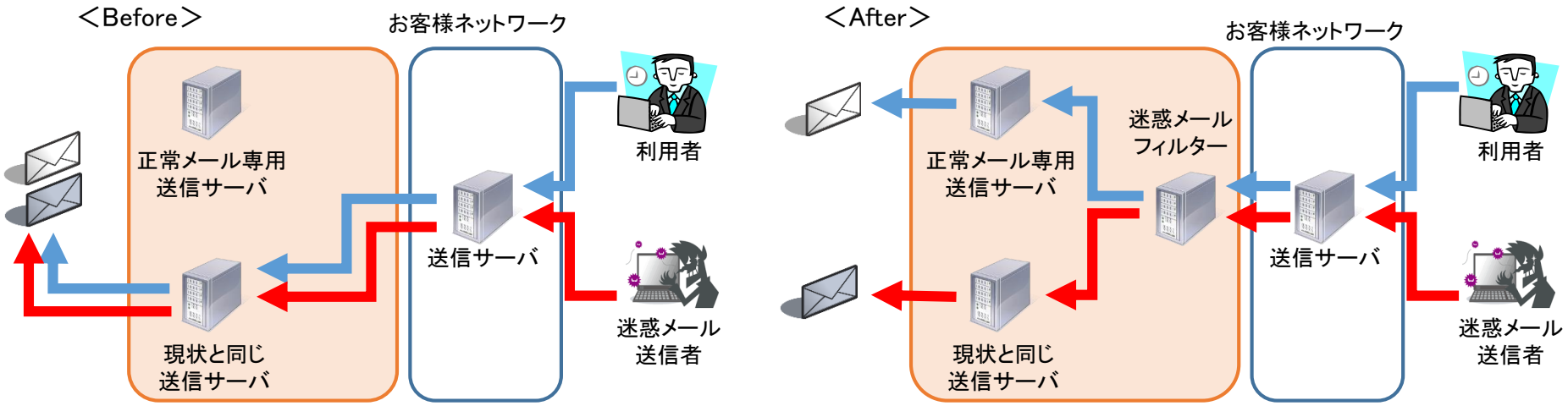
準備期間

準備期間： 12か月 （F社の場合）

導入準備

1. 利用者／サポート部隊への周知
2. 利用規約／契約約款の変更
3. 迷惑メールではないメール用途の綺麗な IPアドレスの送信サーバの新設、振り分けの仕組みの実装
4. サービス提供（新規利用者のみ）
5. 既存利用者には、設定画面にログインした際に、本対策の概要と同意画面を表示。
   同意されれば、綺麗な IPアドレスの送信サーバも利用するよう配送経路を変更。

図解



対策技術の紹介（③接続元情報による制限）

対策概要

海外からのメール送信を禁止する選択機能を利用者に提供、海外からの不正利用を低減する。

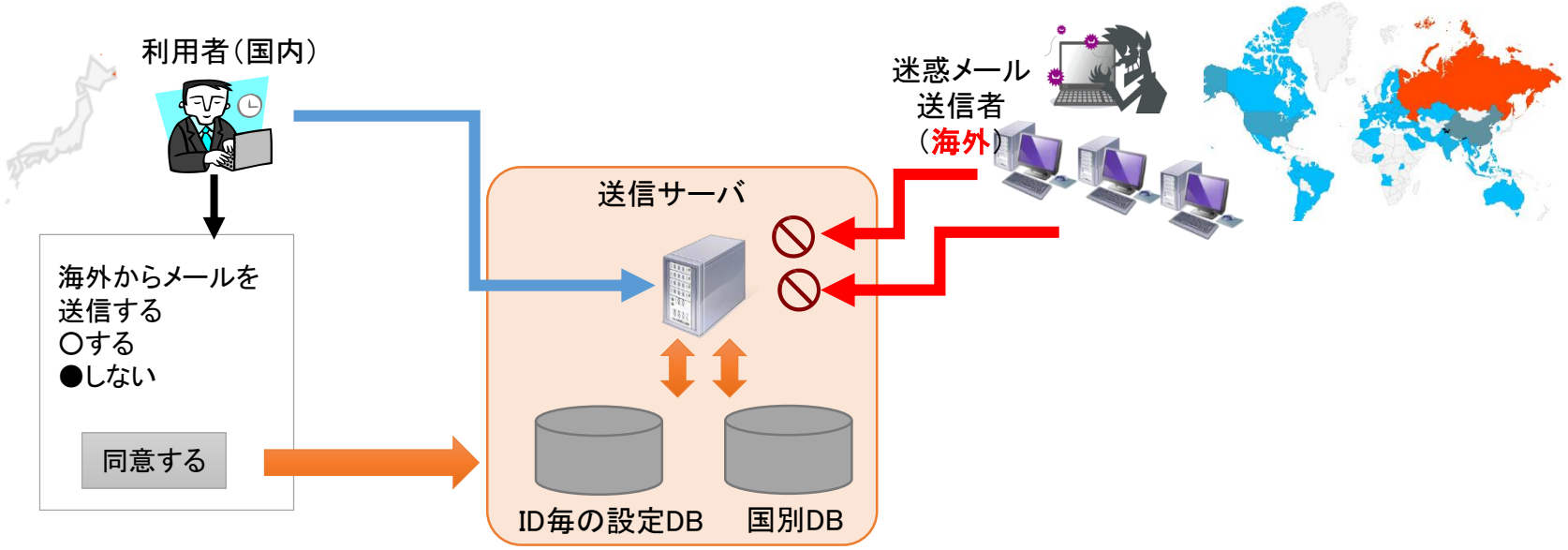
準備期間

準備期間： 4か月 （A社の場合）

導入準備

1. 国別情報のデータベース化（最低限、日本国内と海外の区別ができる仕組み）
2. 送信メールサーバプログラムの修正（例　判定プログラムのMilter化）
3. 送信者ID毎の設定変更ウェブページの作成（例　海外からの接続許可： ON／OFF）
4. カスタマーサポートへの周知
5. サービス提供

図解



対策技術の紹介（④マルチ要素認証）

対策概要

（Webメールにおいて）従来のパスワード認証の他の認証機構を設けて、不正利用の難易度を高め、踏み台送信を防止する。

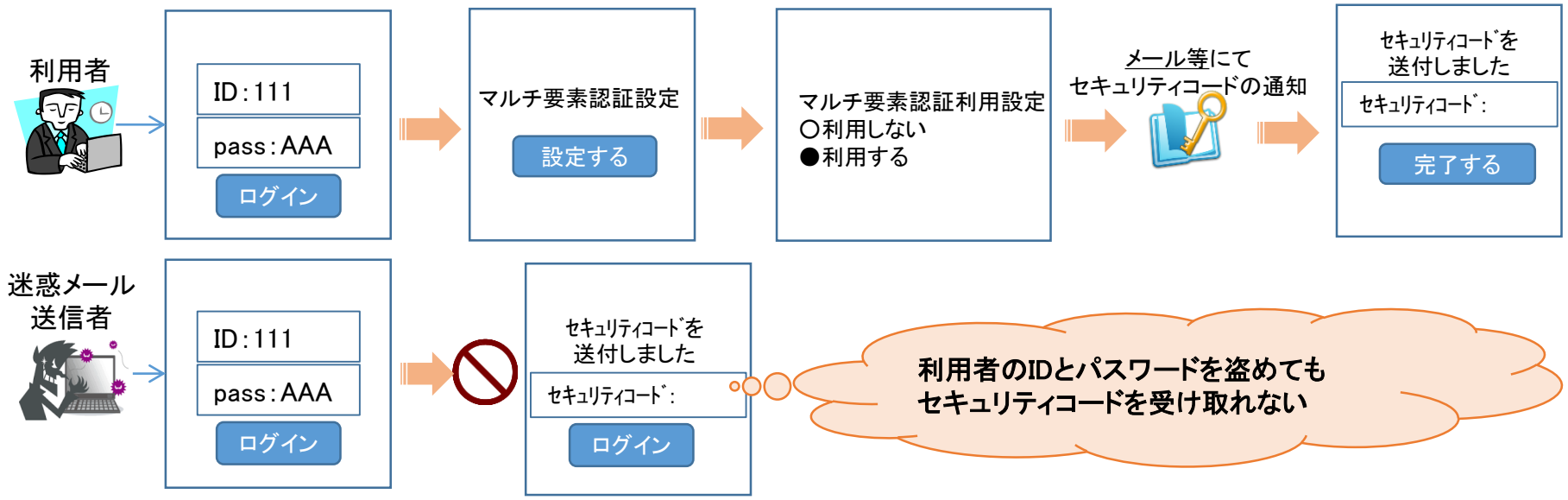
準備期間

準備期間： 6か月 （E社の場合）

導入準備

1. 利用規約／契約約款の変更
2. 新たな認証システム・機能の作成
3. 利用者向けの設定変更ウェブページの作成
4. マルチ要素認証に関する紹介ウェブページの作成
5. サービス提供

図解



対策技術の紹介（⑤送信者詐称の制限）

対策概要

送信者IDと送信者情報（エンベロープFrom、ヘッダーFrom等）が一致しない場合は、不正利用とみなして送信を制限する。

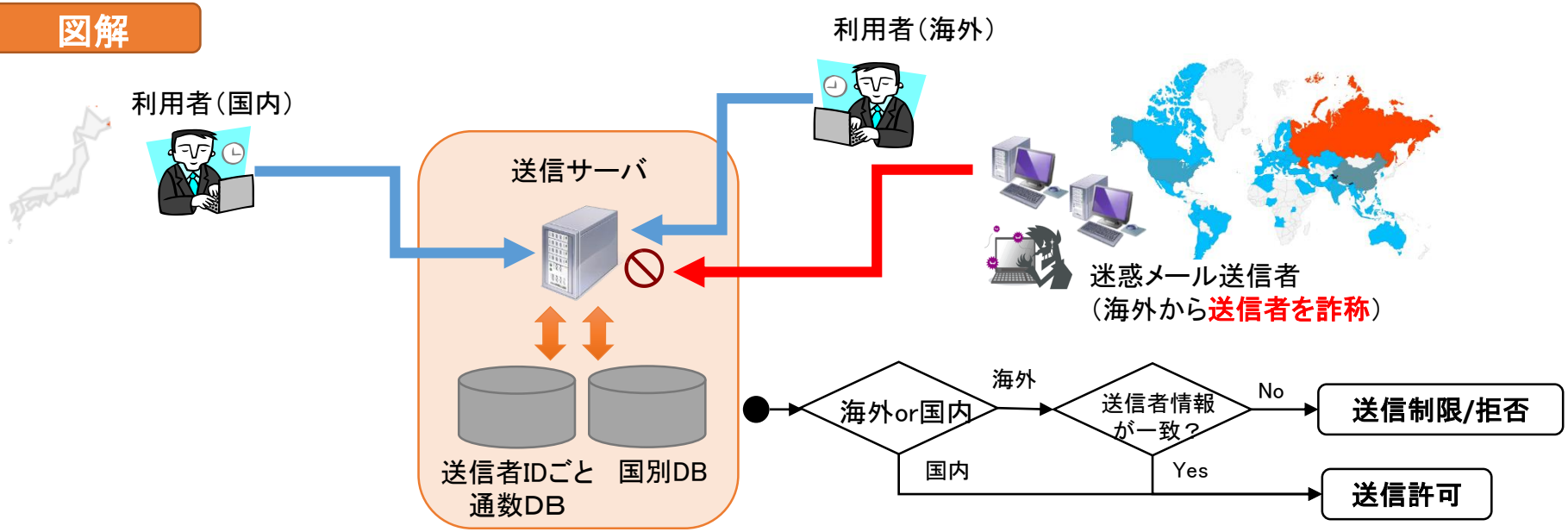
準備期間

準備期間： 2か月 （A社の場合）

導入準備

1. 制限範囲の決定（本人による第三者送信を考慮して、海外からの接続のみに限定）
2. 国別情報のデータベース化（最低限、日本国内と海外の区別ができる仕組み）
3. 送信者IDごとの送信数／送信ピッチのデータベース化
4. 送信メールサーバプログラムの修正（1および2とデータ連携するプログラムの修正）
5. カスタマーサポートへの周知
6. サービス提供

図解



対策技術の紹介（⑥利用者への啓発）

対策概要

事業者から利用者に対して、不正利用の手法や危険性を伝えることで、利用者の理解を深めつつ、様々な対策の利用を促進する。

準備期間

準備期間： 1か月～ （C社・G社の場合）

導入準備

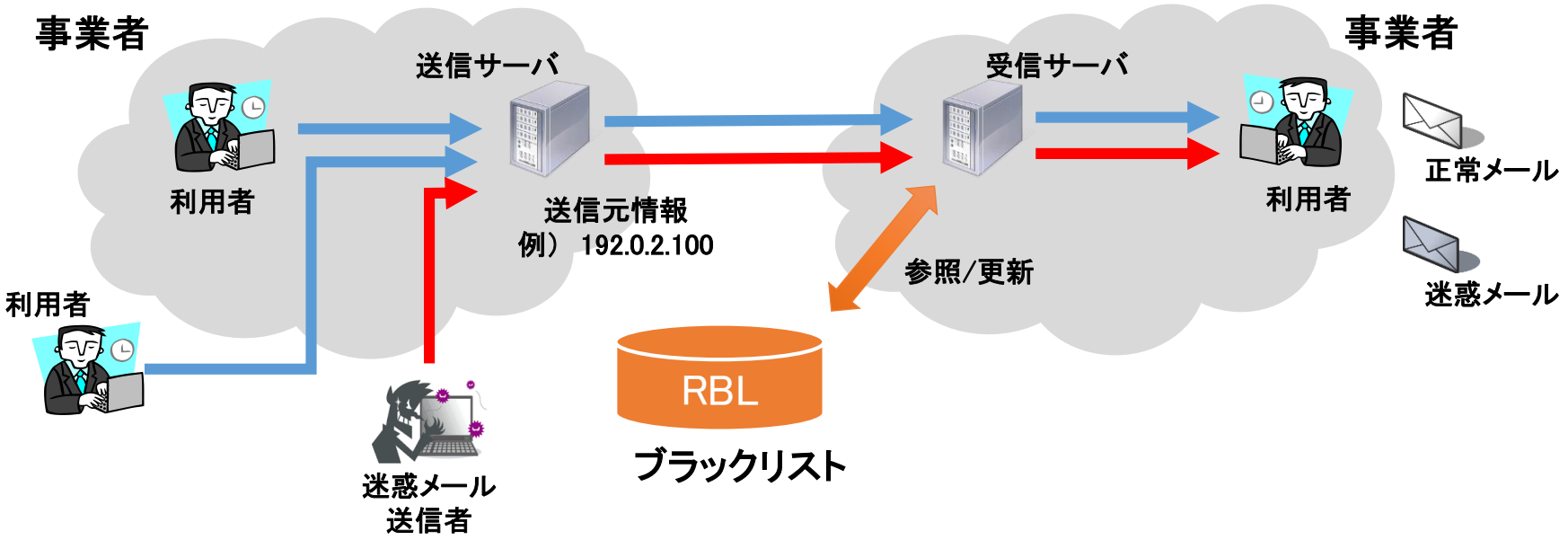
1. メールによる利用者周知
   例　全利用者に重要なお知らせのメールを配信する
2. ポータルサイトによる利用者周知
   例　ポータルサイトにセキュリティへの取り組みや対策内容に対するFAQを記載する
3. システム対応
   例　長期間パスワード変更がない場合に、ポップアップを表示する
   例　二か国以上の送信元からメール送信があった場合に、パスワード変更を推奨する
   例　大量のメール送信があった場合に、強制パスワード変更した旨を通知する

電気通信事業者による提供状況

◎：実施済　〇：一部実施済　×：未実施　―：対象外

	①SMTP認証と送信通数制限	②送信IPアドレスの分離	③接続元情報による制限	④マルチ要素認証	⑤送信者詐称の制限	⑥利用者への啓発
A社	◎	×	〇	〇	〇	◎
B社	◎	×	◎	×	〇	◎
C社	◎	×	×	〇	〇	◎
D社	◎	×	◎	×	×	〇
E社	◎	×	―	〇	〇	◎
F社	◎	〇	〇	〇	×	◎
G社	◎	〇	×	〇	〇	◎
H社	◎	◎	◎	〇	〇	×
I社	◎	〇	〇	×	×	×
J社	◎	×	×	×	×	◎

（参考）本資料での用語について



用語	説明
事業者	メールサービスを提供するISPや企業、自治体などを指す。
利用者	事業者の提供するメールサービスを利用するものを指す。事業者の提供する送信サーバを利用して、メールの送信や受信ができる。
送信元情報	事業者が利用者に提供する送信サーバのドメイン名やIPアドレスを指す。
送信IPアドレス	送信元情報のうち、インターネットへ送出する際のソースIPアドレスを指す。
送信者ID・パスワード	事業者が利用者に貸与する認証アカウント情報を指す。
送信者情報	利用者あるいは事業者がメールを送信する際に指定する差出人情報を指す。一般的に、ヘッダーFrom情報やエンベロープFromアドレス、送信者IDなどがある。
ブラックリスト	第三者機関が作成した送信元情報の評価データベースを指す。
第三者送信	利用者がメールを送信する際に、その事業者が管理しないメールアドレスを送信者情報に指定してメールを送信することを指す。本資料では、送信者の詐称ではない場合を指す。