2016年12月19日

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）

迷惑メール対策推進協議会
技術ワーキンググループ

Rev. 16121901

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。

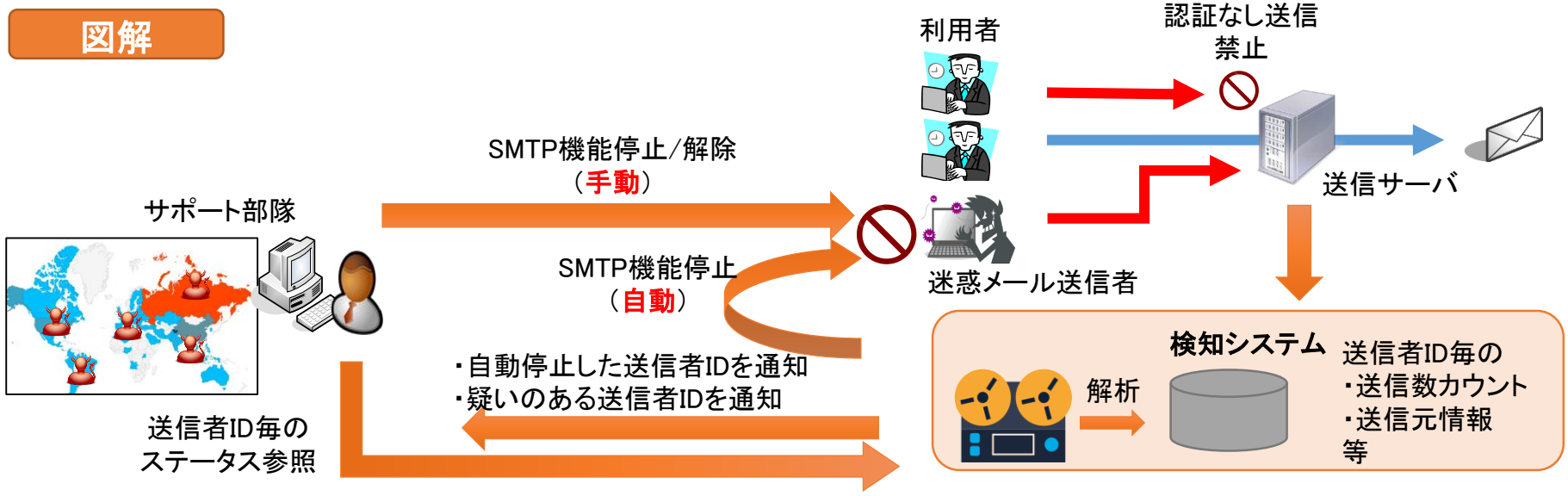
準備期間

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。

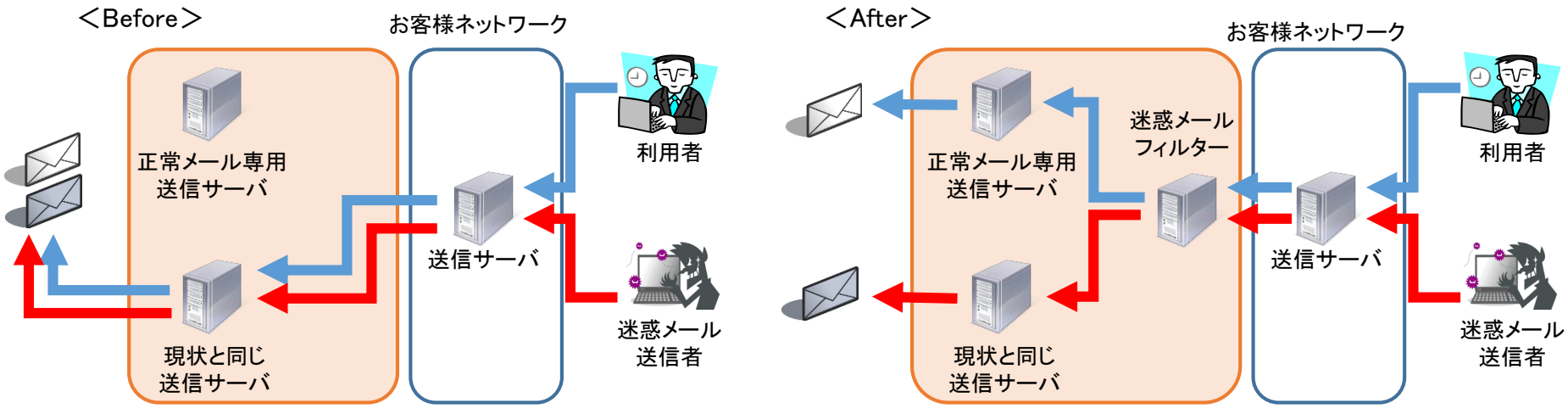
準備期間

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。

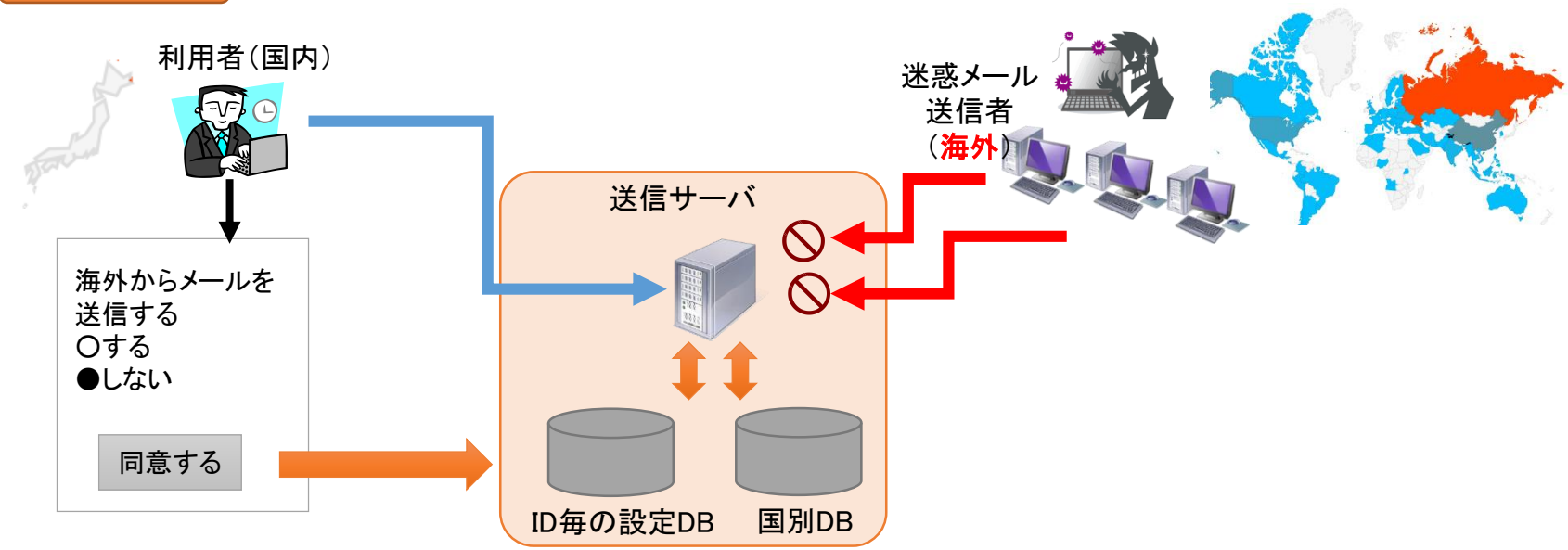
準備期間

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。

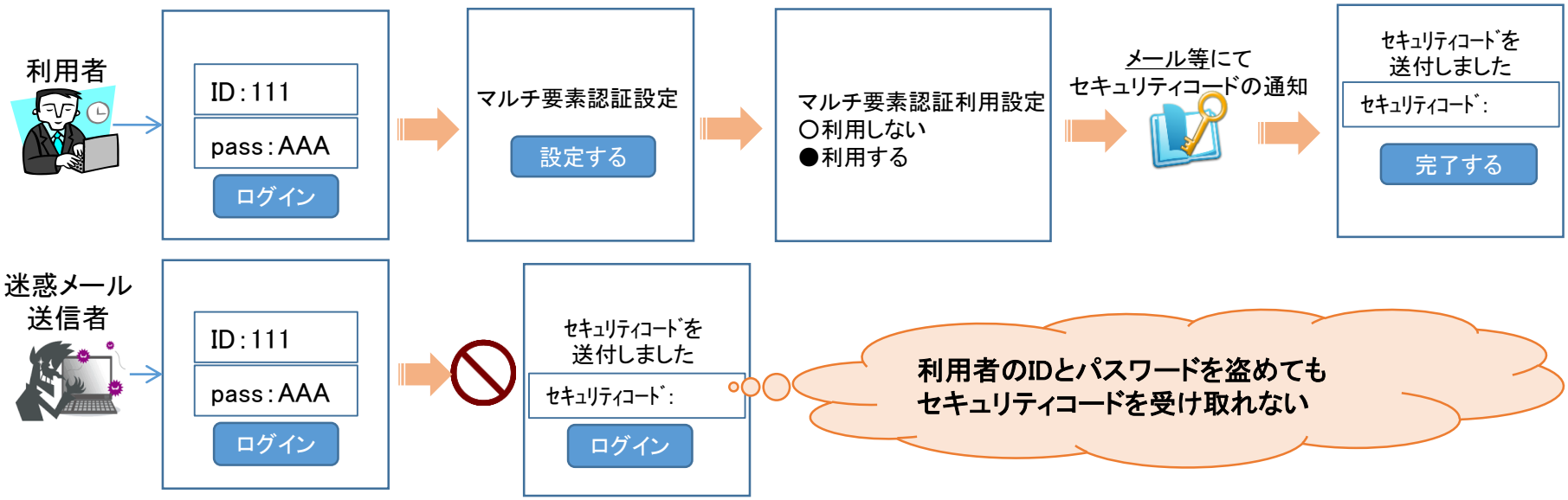
準備期間

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。

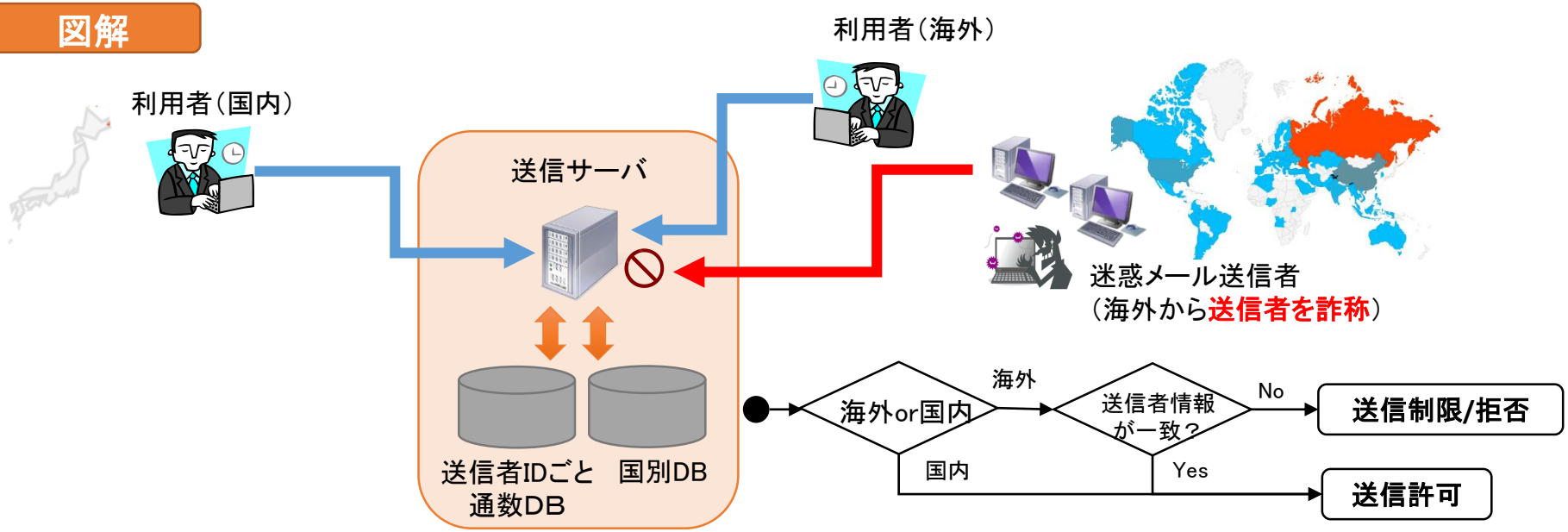
準備期間

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

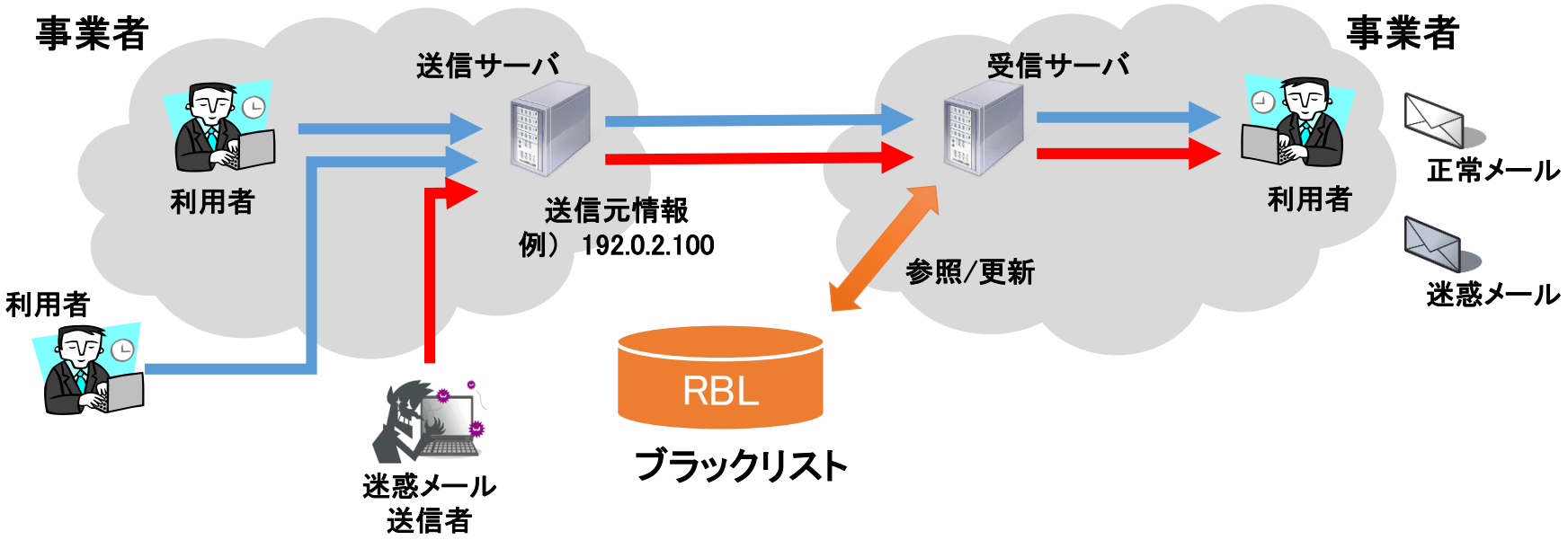
1. メールによる利用者周知
   例　全利用者に重要なお知らせのメールを配信する
2. ポータルサイトによる利用者周知
   例　ポータルサイトにセキュリティへの取り組みや対策内容に対するFAQを記載する
3. システム対応
   例　長期間パスワード変更がない場合に、ポップアップを表示する
   例　二か国以上の送信元からメール送信があった場合に、パスワード変更を推奨する
   例　大量のメール送信があった場合に、強制パスワード変更した旨を通知する

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。