大規模メールシステムにおける メールの不正送信対策について

3.1 はじめに

IIJでは長年、数十万ユーザから数百万ユーザ規模のサービスプロバイダ向け大規模メールシステムの構築サービスや大規模メールASPサービスを提供しています。大規模メールシステムの運用には多くのノウハウが必要とされますが、中でも効果的な不正利用対策の組み込みには多くの知見と経験が必要とされます。メールシステム管理者の業務の大半は、メールシステムの不正利用に起因した対応やそれに付随する障害対応ですから、この対策をシステム的にしっかり行うことは、メールシステム管理者の負担を軽減し、またエンドユーザに対する安定したサービス提供にも大きく寄与します。

不正利用の傾向は日々変わるため、メールシステム管理者が都度対処することはいたちごっこであり、対処を続けても不正利用をなかなか減らすことができず、体力を大きく消耗する不毛な戦いになりがちです。一方で、ポイントを押さえてシステム的な運用対応が取れるような仕組みを準備することで、不正利用を相当数減らすことも可能です。

今回は、いろいろなメールシステムでの導入や運用の経験に基づき、効果が見られたメールの不正利用対策をいくつか取り上げ、解説を加えます。なお、ここで述べる対策は、サービスプロバイダが提供するメールサービス約款の定義やユーザ同意が必要なものを含むため、適用に関しては、それぞれのサービスプロバイダにおいて検討が必要となる点に注意が必要です。

3.2 メールの不正利用対策の重要性

エンドユーザがサービスプロバイダのメールサーバを利用してメールを送信する場合は、一般的にMUAからSMTP認証や、Webメールを利用します。SMTP認証及びWebメールの利用には認証IDとパスワードが必要ですが、容易に推測できるパスワードが設定されている場合や、PC自体がウイルスに感染することで認証IDとパスワードが漏えいしやすくなります。この漏えいした認証IDとパスワードを用いて正規のエンドユーザになりすまし、迷惑メールが送信されているケースが多く存在します。

迷惑メール送信は、総じて機械的に繰り返し大量のメールを送信することが多く、その結果、メールシステムに大量のメールが流入し、最終的にインターネットに送信されます。大量の迷惑メールがインターネットに送信されると、インターネット側では、メールシステムの送信出口のIPアドレスを迷惑メールの送信元として認識し、ブラックリストに登録します。ブラックリストに登録されると、主に以下のような影響があります(図-1)。

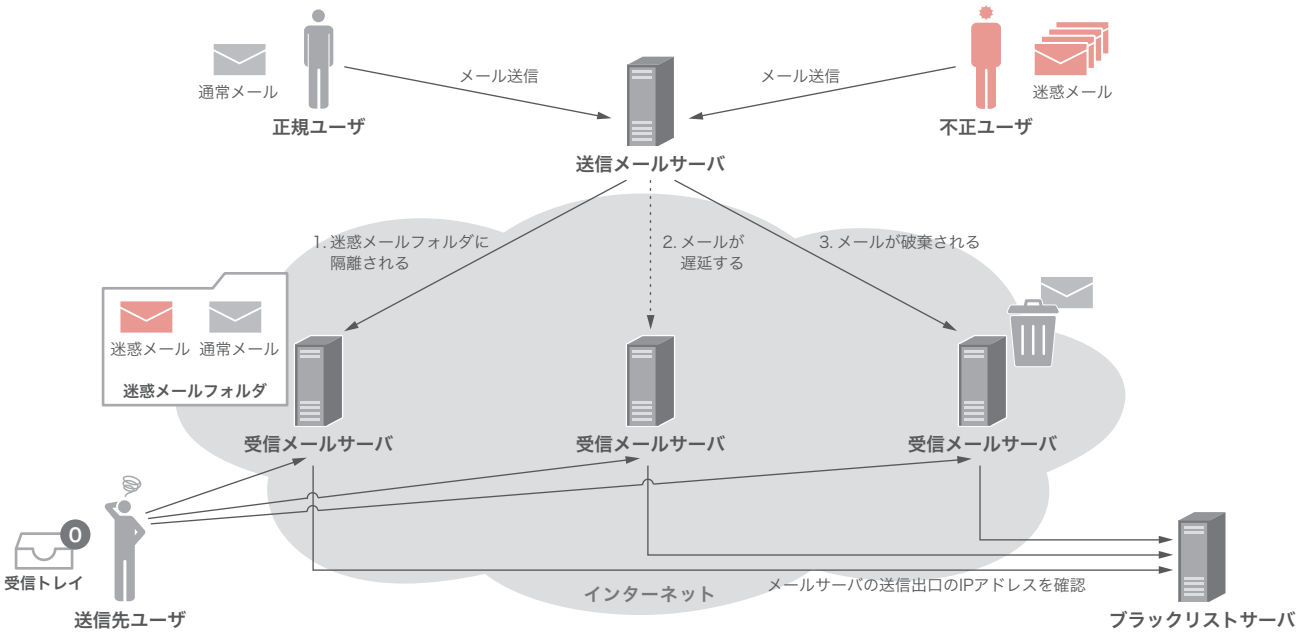


図-1 メールの不正送信における影響

1. 通常のメールまで迷惑メールと判定される(gmail・hotmail・yahoo.com・キャリアメールのケースが多い)
2. 今まで届いていたメールが遅延する
3. メールが破棄されて、まったく届かなくなる

ブラックリストから解除されるためには、原因を取り除いて正常化する必要があります。しかし、原因調査や対策検討には手探りの部分が多く、システム管理者が大きく疲弊するところでもあるため、効果的なメールの不正利用対策はシステム運用上非常に重要なポイントになります。

3.3 メール不正送信の傾向

メールの不正送信の形態は時々刻々と変わってきています。今のトレンドは国外からのメールの不正送信が大半であり、以下のような事例が挙げられます。

1. 国外から単一の認証IDを利用した大量メール送信
2. 国外から複数の認証IDを利用した同時多発的なメール送信
3. 国外からWebメールを利用した大量メール送信

基本的に国外からの通信が関係しているため、メールの送信元IPアドレスを元に送信元の国を判断する仕組みがあれば、効果的なメールの不正送信対策を取ることができます。

国判定の仕組みには、送信元IPアドレスに基づいて国を判別するデータベース及びそれらを容易に利用可能なシステム作りが必要です。国データベースはMaxMind GeoIP2をはじめ数種類存在しますが、有償・無償、サポート有・無、国以外の情報有・無(地域レベルやgmailのレンジ判別など)・更新頻度などの違いがあるため、必要に応じて選択する必要があります。

また国データベースの利用形態には、APIでの利用とダウンロードして整形する方法があります。サービスプロバイダレベルの大規模メールシステムでは、大量のメールを受け取る都合上、国データベースの参照回数が多くなる傾向があり、かつ国データの更新頻度は経験上それほど重要ではないので、ダウンロードして整形する運用が適していると考えています。ダウンロードした国データベースは後述するログ解析やメールサーバでのリアルタイム国判定に利用します。図-2に構成例を記載します。

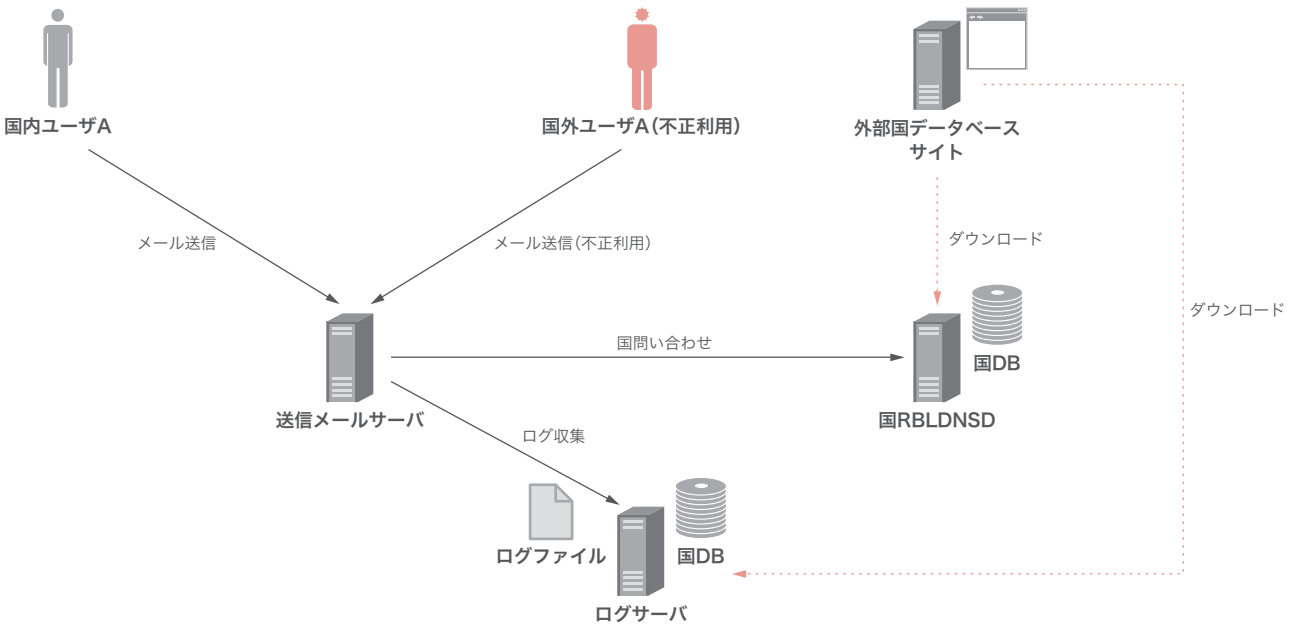
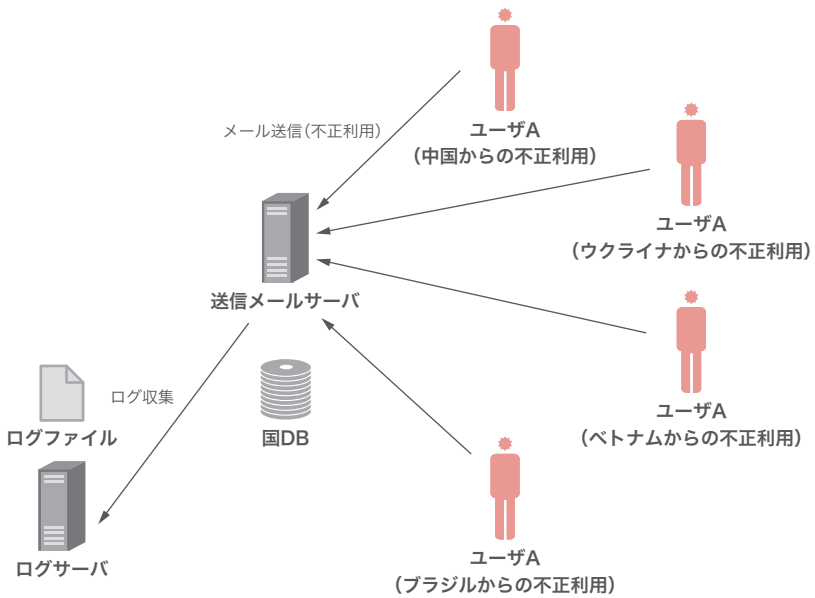


図-2 国データ判定システム概要

3.4 メールログを利用した国外判定の実装

一般的にメールサーバのログにはSMTP認証で利用された認証ID及び送信元IPアドレスが記載されます。前述した国データベースを用いたメールサーバのログを解析するプログラムを作成することで、認証IDごとの国別送信数、全送信数などを解析できるようになり、メールの不正利用を容易に特定できるようになります（図-3）。

- **数時間以内に複数国からメールを送信された場合**
  例えば、中国、ウクライナ、ベトナム、ブラジルからほぼ同時刻に、同じ認証IDを使ってメールを送信された場合は、ほぼ同時刻に同じユーザが世界各国を移動できるはずもないため、認証IDが不正利用されていると考え、当該認証IDからのメール送信を停止するアクションを取りやすくなります。
- **単一国外から大量にメールを送信された場合**
  単一国外からメールを大量送信されるケースも往々にして発生します。この場合は先ほどと異なり明示的に不正利用されているかどうかの判断がつきにくいことがあるのですが、一定時間中に常識的なメール送信数を大きく超過した場合は、一時的にメール送信を停止する対処が考えられます。なお、国外の事業所から正規のメールを大量に送信するケースも存在するため、特定の認証IDをホワイトリストに登録して運用することも考慮に入れる必要があります。



●中国からのメール送信ログ（中国のIPアドレス: 1.0.*.***から認証ID: example@example.comで接続している例）
May 25 03:34:09 server11 smmta[16316]: AUTH=server, relay=from.example.com [1.0.*.***] (may be forged), authid=example@example.com, mech=PLAIN, bits=0
May 25 03:34:09 server11 smmta[16316]: w4OIY9On016316: from=from@example.com, size=0, class=0, nrcpts=1, proto=ESMTP, daemon=MSA, tls_verify=NONE, auth=PLAIN, relay=from.example.com [1.0.*.***] (may be forged)

●ブラジルからのメール送信ログ（ブラジルのIPアドレス: 23.97.**.***から認証ID: example@example.comで接続している例）
May 25 03:35:23 server11 smmta[16319]: AUTH=server, relay=from.example.com [23.97.**.***] (may be forged), authid=example@example.com, mech=PLAIN, bits=0
May 25 03:35:23 server11 smmta[16319]: w4P5Y60n028961: from=from@example.com, size=0, class=0, nrcpts=1, proto=ESMTP, daemon=MSA, tls_verify=NONE, auth=PLAIN, relay=from.example.com [23.97.**.***] (may be forged)

図-3 ログ解析を用いた不正利用判定

このように、ログに基づいた対処は、大半のメールシステムにおいて適用できる点では汎用的かつ効果の高い有用な手法です。しかし、ログ処理はバッチ方式を用いられることが多く、リアルタイム性が落ちることで、メールの不正送信を止めるまでに1万通レベルでのメールを打ち込まれてしまい、結果的にブラックリストに登録されてしまったというケースも散見されます。このため、大規模メールシステムにおいては、メールログ解析だけでは効果を上げきれない場合があります。

3.5 メールサーバでのリアルタイム国外判定の実装

メールサーバが国データベース(独自構築した国RBLDNSDなど)に送信者の送信元IPアドレスを問い合わせることで、送信元の国をリアルタイムに判別する方法があります(図-4)。本方法はメールサーバレベルでリアルタイムに判定できるため、同一時間帯に複数の国から送信された場合は不正利用と見なして即座に停止する対策をとることができます。これにより、メールログ解析で問題となっていた停止までの時間差をゼロにすることができるため、気がついたときには大量のメールが送信された後だったという事態を防ぐことができ、高い導入効果が得られます。

また実装を工夫することで、メール送信全体ではなく国外からのメール送信のみを停止する実装も可能なため、国内利用が大半であるエンドユーザへの影響を小さくすることが可能です。ユーザサポートの観点でも優れた対応と言えます。

一方でメールサーバにリアルタイム検知の機能を実装するにはMilterプログラムの導入、PostfixやsendmailなどのOSSメールサーバの改造、あるいはプログラミング機能を持つ商用メールサーバ(Cloudmark Security Platform for EmailやVade Secureなど)の導入が必要であり、導入効果が高い反面、技術的な難度が高い点が懸念事項として挙げられます。実際、過去の導入時は相当数時間をかけて入念なテストを繰り返して品質を担保することが必要でした。

3.6 Webメール経由でのメールの不正送信の対策

前述のメールの不正送信対策はSMTP認証を利用した送信を対象としていましたが、現在はWebメール経由でのメールの不正送信も増えています。日本のメール業界における代表的なWebメールソフトウェアは数種類あり、ログイン方法やメール送信方法はソフトウェアごとにまったく異なるにもかかわらず、それぞれのソフトウェアに対応した形で大量のメールが送信されたという事実もあります。また、Webメール送信の痕跡が残らないように、送信後は送信済みのメールボックスを空にしてから行儀よくログアウトするという話もあり、相当高度化している印象があります。

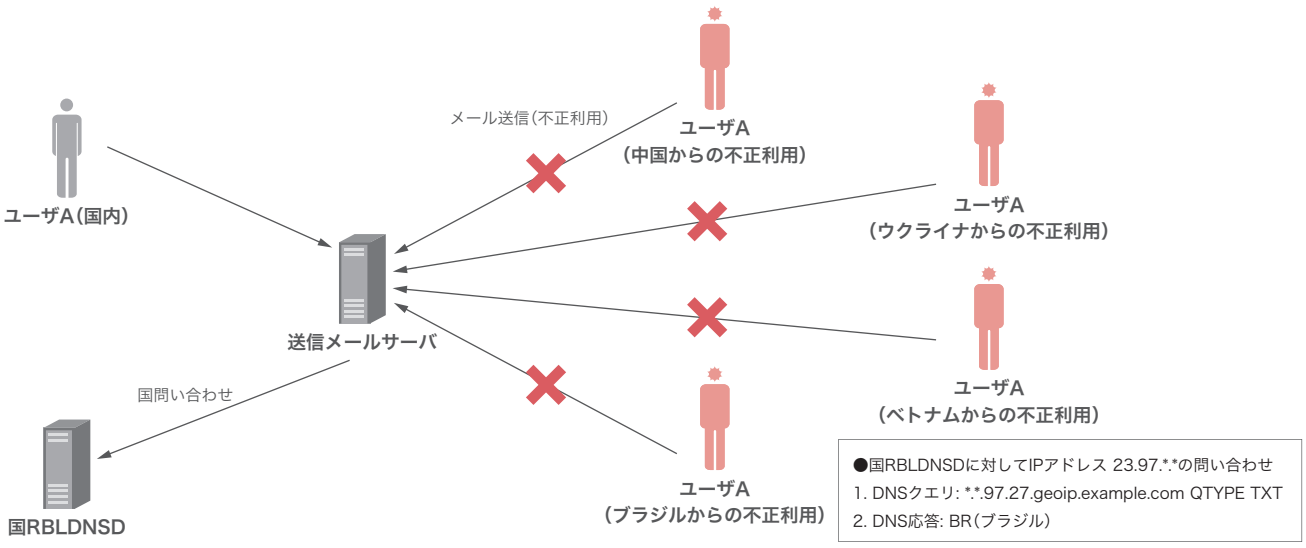


図-4 不正利用のリアルタイム判定

一般的に、Webメールから送信されたメールの送信元IPアドレスは、受信側のメールサーバでは分からないため、前述した国判定が行いにくいのが実情であり、結果的に不正利用の判別が難しく、メールの不正送信の第二の手法として攻撃者に狙われていると考えられます。対策としては、送信元IPアドレスをメールヘッダに埋め込むことが可能なWebメールソフトウェアを採用し、更にメールサーバ側でヘッダ情報を利用した制御を実装するようにしました(図-5)。本方法をとることで、国判定をメールサーバ側でリアルタイムに行うことが可能になり、不正利用の早期発見や対策ができるようになりました。また不正利用アカウントについては、Webメールの利用停止、もしくは国外からのWebメールの利用に限って停止できるようにWebメールを改造したこともあります。

3.7 ユーザ選択による国外からのメール利用制御

国外からのメールアクセスの制御をユーザ選択に委ねるという方法もあります(図-6)。具体的にはSMTP認証を用いたメール送信・Webメール送信・POP/IMAPなどのメール受信を国外から許可する・しないをユーザに選択してもらい、メールサーバサイドでユーザごとのアクセス制御をかける手法になります。

本手法を利用することで、通常時は国外からのメール送信やメール受信、Webメールログインを制限しつつ、国外への出張や旅行の際には管理画面から許可するような運用が可能になります。

エンドユーザに選択権を与えることで利用者の同意を取りやすくし、国外からのアクセスが不正利用されやすい点についての啓蒙活動も兼ねることができる点では有用な手法と言えます。一方で国外からのアクセスをデフォルトで制限するにはユーザの同意を得る必要があり、メールの不正利用を大きく低減する手法とは言いきれない一面もあります。

3.8 SMTP接続DoS攻撃の対応

話題の方向性が少し変わりますが、メールの不正送信の一例として、複数の認証IDを利用して同時多発的にメールサーバにSMTP接続し、その状態を長時間維持させることで、メールサーバのコネクションをわざと枯渇させるケースも見られます。これらは当該メールサーバのタイムアウトの仕組みを把握・利用した巧妙なDoS攻撃であり、新規のSMTP接続がまったくできないケースにも発展し、サービス提供に大きな影響を与える悪質な攻撃です(図-7)。

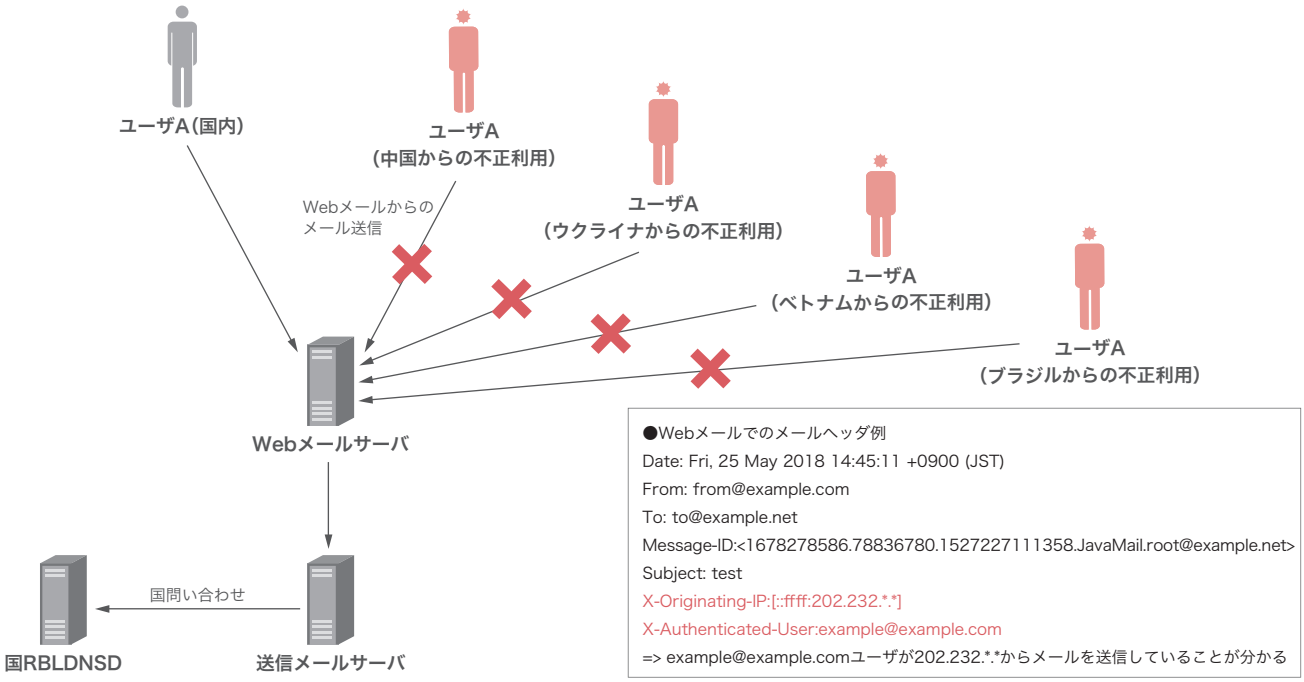


図-5 Webメールを用いた不正送信判定

SMTP接続の長時間維持の対応としては、一般的にメールサーバのタイムアウトを短縮する方法があります。メールサーバ標準のタイムアウトが長いケースも散見されるため、導入時にはタイムアウトを適切にチューニングする必要があります。一方でRFC5321(Simple Mail Transfer Protocol)4.5.3.2. TimeoutsでSMTPタイムアウトの推奨値が定義されており、不用意な設定を行うと正規のメール送信に影響が出ることもあるため、短縮できないことも多く、タイムアウトの調整だけでは限界もあります。

他の手段としては、定期的にSMTP接続数を確認し、システム上限の接続数に近づいてきた場合は、アイドルタイムアウトが長いセッションを判別し、サーバサイドから当該コネクションを切断する方法があります(tcpkillコマンドなど)。同時に、不正利用アカウントに対するSMTPセッションの切断も併せて実施することで、SMTPセッションも蓄積しにくくなり、SMTP接続DoS攻撃のリスクを下げることができます。

3.9 おわりに

大規模メールシステムにおけるメールの不正送信対策には多様な手法が存在し、複数の仕組みを効果的に組み合わせる必要があります。導入にはコストや技術的な難度を伴いますが、メールサービスの維持やシステム管理者の運用負担の大きな低減及びモチベーション向上を考えると、何かしらのメールの不正送信対策の導入は必要不可欠と考えています。今回の記事が安定したメールシステム運営の一助になれば幸いです。

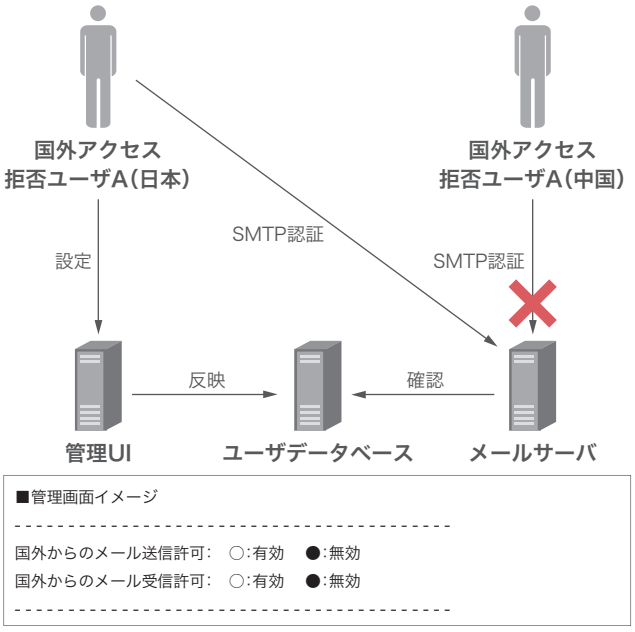


図-6 ユーザ選択による国外利用制御

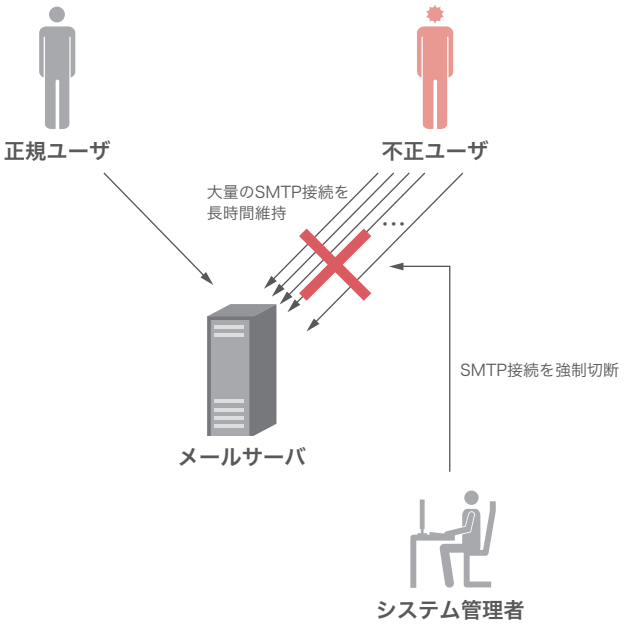


図-7 SMTP接続DoS攻撃

執筆者:
衣笠 茂浩(きぬがさ しげひろ)
IIJ クラウド本部 エンタープライズソリューション部 メールソリューション課 課長。