迷惑メール対策ソフトウェアによりファックスの受信通知メールがブロックされる問題について

関連する動作

Spamhaus などの DNS ブラックリストプロバイダーによって、ファックスの受信通知メールまたはその他の通知メールが常にまたは断続的にブロックされることがあります。

概要

eFax / jFax のサービスによって送信され、お客様のメールサーバーで受信された通知メールは、メールサーバー管理の一部として設定されたルールを介して処理されます。これはしばしば Spamhaus などの DNS ブラックリストサービスによって補完されます。これらのブラックリストサービスは IP のリストを管理しており、メールが届くと送信元 IP をこのリストと照合します。送信者 IP がブラックリストに登録されていることが判明した場合、このメールはお客様のメールサーバーによってブロックされます。DNS ブラックリストサービスは有益なツールですが、一部のサービスにより有効な IP でさえも積極的にブラックリストに登録される傾向があるため、スパムではないメールまで誤ってブロックされる可能性があります。

Consensus Cloud Solutions / j2 Global Japan 有限会社は、誤って登録されてしまった弊社の IP をブラックリストから削除するために、DNS ブラックリストプロバイダーに対し多大な働きかけを行っていますが、プロバイダーからのレスポンスにはかなりの時間を要すことが多く、一度ブラックリストから削除された IP が後に再登録されてしまうこともあります。DNS ブラックリスティングの性質上、弊社がこの登録・再登録を直接解決または軽減できる手段は非常に限られています。DNS ブラックリスティングは受信メールサーバーレベルで管理されており、軽減策はそこで講じる必要があるため、送信者である弊社では制御ができません。

eFax / jFax からの通知メールが Spamhaus などの DNS ブラックリストプロバイダーによってブロックされている疑いがある場合は、弊社のエンジニアがお客様のメールログを確認し、ブラックリストが原因になっているかどうかを検証します。原因が確認されたら、お客様が直面されている問題を軽減するためにいくつかの対策を講じることができます。

弊社から送信されるすべてのメールは、弊社の SPF レコードに従い、有効な DKIM ヘッダーで署名され、DMARC ポリシー強制によってサポートされています。

役立つ用語集

「SPF レコード」

SPF (Sender Policy Framework) レコードは、eFax / jFax サービスの代わりにメールを送信することを許可されているすべての IP のリストを含む、弊社の DNS で提供される公開レコードです。これは、受信メールサーバーが受信メールが許可された送信元 IP からのものであることを検証するために使用できます。

「DKIM」

DKIM (DomainKeys Identified Mail) は、SPF 検証とは別に機能する受信メールを認証する方法で

す。SPF 検証がメッセージの送信元を検証するのに対し、DKIM はメール自体の一部として一方向ハッシュ署名を使用し、これは弊社の DNS で提供される一致する公開鍵を介してのみ復号化できます。

「**DMARC レコード**」
弊社の DMARC (Domain-based Message Authentication, Reporting & Conformance) レコードは、SPF 検証、DKIM 検証、またはその両方に失敗した場合に、弊社のドメインから受信したメールをどのように処理すべきかについての指示参照として機能します。このレコードは、受信メールサーバーがスパムレポートを送信できるチャネルも提供します。このレコードは弊社の DNS によって公開されていますが、その検証と強制は受信メールサーバーで定義する必要があります。

軽減オプション

- 影響を受けるドメイン (例：message@inbound.efax.com / message@inbound.jfax.com) からの受信メールを SPF および DKIM 検証を介してホワイトリストに登録する
    - このオプションは、メールサーバーまたはプロバイダーでのルール作成を中心としています。
        - メールエンベロープに含まれるメールドメインの SPF レコードを明示的に検証する
        - 検証が成功した場合は、ブラックリストによる拒否を上書きするか、その後のブラックリストチェックをバイパスする
        - メールルール階層で SPF 検証が対応する DNS ブラックリスト拒否ルールよりも重み付けされていることを確認する (これが逆になっていると、適切な検証またはホワイトリスト登録を通過した後でも有効なメールが拒否される可能性があります)
        - DMARC ポリシーを検証し、強制する
    - メッセージがメールサーバーで受信されると、DKIM 検証が行われ、一致する公開鍵を使用してメッセージ固有の一方向ハッシュ署名が復号化されます。このステップはメッセージがメールサーバーによって受信されるまで発生しないため、Spamhaus などの DNS ブラックリストによる拒否は、このステップに到達する前にメッセージを拒否することに注意してください。DKIM 検証が失敗した場合、DMARC ポリシー強制を使用してメッセージを希望どおりに処理できます。
    - すべての検証が通過し、DNS ブラックリストがバイパスされ、メッセージが認証されると、メッセージは安全に配信できます。
- 個々の IP アドレスをホワイトリストに登録する
    - SPF 検証とドメインホワイトリスト登録 (推奨) の代替として、メール送信に使用する個々の IP をホワイトリストに登録することも可能です。
    - お客様への配慮として、弊社はライブで定期的に更新される IP のリストを提供しており、これはお客様のローカル管理チームがお客様の内部ホワイトリストポリシーと連携して活用できます。このリストは https://ipranges.efax.com/ で見つけることができます。

        - 上記のリストは JSON ファイルとしてフォーマットされており、FAX (SMTP) や Webhook (API) 配信など、さまざまなサービスに使用される最小限の IP 範囲が含まれています。
        - このリストは、該当するサービスと地域、またはテリトリー (例：US West および US East) に基づいてフィルタリングし、含まれる範囲を絞り込むことができます。
        - IP 検証が成功すると、DNS ブラックリストによる拒否をバイパスまたは上書きするために、メールサーバーまたは管理レベルでルールを設定する必要があります。
        - 前のオプションで述べたように、上記のルールは DNS ブラックリスト拒否よりも重み付けされている必要があります。逆の場合、明示的にホワイトリストに登録された IP からのメールが依然として拒否される可能性があります。
- 別の DNS ブラックリストプロバイダーを利用する
    - 弊社はブラックリストプロバイダーと協力し、弊社のサービスが最高レベルのセキュリティとコンプライアンスを維持するためにあらゆる努力を払っていますが、弊社の IP が誤ってブラックリストに登録されるケースは依然として発生します。過去には、特定の DNS ブラックリストプロバイダー、特に Spamhaus において、有効な IP からのメールが拒否されるケースがはるかに多く見られました。このプロバイダーを使用する際に問題が発生している場合は、報告される拒否が大幅に少ない他の多くの DNS ブラックリストプロバイダーがあります。

追加注意事項

ローカルまたはネットワーク管理と同様に、メールサーバー、設定、または DNS への変更は、知識と資格のある社内 IT 管理者リソースによってのみ実行されることが不可欠です。

Consensus Cloud Solutions / j2 Global Japan 有限会社および関連リソースは、メールサーバー管理の手順やガイドラインを提供したり、上記の軽減手順を直接実行したりすることはできません。