Google Workspace での Emotet の具体的な対策方法

メール受信時の対策

管理コンソールの設定で受信時の宛先のなりすまし防止や、添付ファイルの確認を強化することができます。

メール送信時の対策

Google Workpaceは3つのメール認証標準を用いて、メールセキュリティを高めることを推奨しています。昨今は emotet の影響でGmail 以外のメールサービスやセキュリティソフトでのセキュリティレベルが上がっており、下記項目を対応していないことで取引先にメールが届かない、迷惑メールに入るなどのトラブルが発生しています。

- **SPF (Sender Policy Framework)**
- **DKIM (DomainKeys Identified Mail)**
- **DMARC(Domain-based Message Authentication Reporting and Conformance)**

動画 https://youtu.be/8V2nfKLzc84

メール受信時の対策

高度なフィッシングと不正なソフトウェアへの対策

参照 https://support.google.com/a/answer/9157861?hl=ja

1. Google Workspace 管理コンソールにアクセス
2. ［アプリ］>［Google Workspace］>［Gmail］>［安全性］の順にクリック

・添付ファイル

・IMAPでの閲覧時の保護

・リンクと外部画像

・なりすましと認証

添付ファイルに対する設定

［添付ファイル］をクリックし、以下の設定にチェックを入れ、［保存］をクリック

・信頼できない送信者から送られる暗号化された添付ファイルに対する保護機能

・信頼できない送信者から送られるスクリプトを含む添付ファイルに対する保護機能

・今後のおすすめの設定を自動的に適用

リンクと外部画像に対する設定

［リンクと外部画像］をクリックし、以下の設定にチェックを入れ、［保存］をクリック

・短縮 URL により隠されたリンクを特定

・リンク先の画像をスキャン

・信頼できないドメインへのリンクをクリックした場合に警告メッセージを表示

・今後のおすすめの設定を自動的に適用

なりすましに対する設定

［なりすましと認証］をクリックし、以下の設定にチェックを入れ、［保存］をクリック

・類似したドメイン名に基づくドメインのなりすましに対する保護機能

・従業員名のなりすましに対する保護機能

・受信メールによるドメインのなりすましに対する保護機能

※それ以外の項目については、チェックを入れてしまうと受信したいメールが、
受信できなくなる可能性があるため、基本的にチェックが無い状態を推奨しています

上位エディションでの設定

有害な添付ファイルを検出するルールを設定する

参照 https://support.google.com/a/answer/7676854?hl=ja

セキュリティ サンドボックス

メールの添付ファイルには、従来のウイルス対策プログラムで見逃された不正なソフトウェアが含まれている場合があります。
Gmail では、セキュリティ サンドボックスという仮想環境で添付ファイルをスキャンまたは実行することで、これらの脅威を特定できます。
脅威が確認された添付ファイルは、ユーザーの [迷惑メール] フォルダに振り分けられます。

メール送信時の対策

- **SPF (Sender Policy Framework)**

  送信元ドメインが詐称されていないかを確認する仕組み

- **DKIM (DomainKeys Identified Mail)**

  送信メールにデジタル証明を追加し、対象の組織から送られていることを確認する仕組み

- **DMARC(Domain-based Message Authentication Reporting and Conformance)**

  送信メールが SPF または DKIM の検証に失敗した際のメールの処理方法を受信サーバーに指定する仕組み

SPFの設定方法

参照 https://support.google.com/a/answer/10685031?hl=ja

① DNS サーバーに SPF を登録する

1. TXTレコードに下記コードを追加する

v=spf1 include:_spf.google.com ~all

※他サービスのSPFレコードが既に存在している場合は追加方法要注意
※ご利用のドメインの管理会社によって設定方法等は異なります。

DKIMの設定方法

参照 https://support.google.com/a/answer/174126?hl=ja

① DKIM 鍵を取得する

1. 管理コンソールにアクセスします。
2. [アプリ] > [Google Workspace] > [Gmail] > [Gmail の設定] > [メールの認証] を開きま す。
3. [選択したドメイン] のプルダウンで、DKIM を設定したいドメインを選択します。
4. [新しいレコードを生成] ボタンをクリックします。
5. 表示されるポップアップ画面にて、DKIM 鍵のビット長とプレフィックスセレクタを選択します。
   DKIM 鍵は、より安全な 2048 を選択します。
   プレフィックスセレクタは、デフォルトで記載されている「google」のままで結構です。
6. [生成] ボタンをクリックすると、DNS ホストの名前と TXT レコードの値が表示されます。
   Google Workspace の画面は表示させたままにしておきます。

DKIMの設定方法

参照 https://support.google.com/a/answer/173535

② DNS サーバーに DKIM を登録する

1. ①で作成した DKIM を登録するにはご利用の DNS サーバーへの登録が必要です。
   詳細な手順については、ドメインを取得したドメインの管理会社にご確認をお願いします。

※ご利用のドメインの管理会社によって設定方法等は異なります。

DMARCの設定方法

参照 https://support.google.com/a/answer/10032169

・ホスト名

_dmarc. 貴社ドメイン

・TXT レコード（DMARC レコード）の値

v=DMARC1; p=none; rua=mailto:dmarc-reports@貴社ドメイン

TXT レコード内に記載した「p=none;」の部分については、 他の値にも変更が可能ですが、
初めて DMARC を設定する場合は「none」が 推奨値となりますので、そちらで記載しております。

※ドメインの管理会社とご相談の上、ご参考にしていただければと存じます。

Link People for Happiness

systena

DXデザイン本部
カスタマーサクセス

cs-support@systena.co.jp

株式会社 システナ

本　　社　〒105-0022　東京都港区海岸1丁目2番20号　汐留ビルディング 14F
TEL 03-6367-3871　FAX 03-3578-3016

大阪事業所　〒530-0013　大阪市北区茶屋町19番19号　アプローズタワー 18F
TEL 06-6376-3537　FAX 06-6359-7012

https://www.systena.co.jp　https://canbus.com/

東京証券取引所市場第一部（証券コード：2317）

本書に含まれる情報は、貴社内部でのご検討、評価のために提供されるものです。貴社内でのご使用、複製、開示はこの目的の為に必要な範囲でのみお願いいたします。