YAMATO TRANSPORT U.S.A., INC.

米国ヤマト運輸株式会社

2017 年 4 月 21 日

【大切なお知らせ】ヤマト運輸の名前を装った添付ファイル付きの「なりすましメール」にご注意ください

お客様各位
ヤマト運輸の名前を装った添付ファイル付きの「なりすましメール」が、不特定多数のお客様に断続的に送信されていますが、ヤマト運輸からは添付ファイル付きでお届け予定 e メールや、ご不在連絡 e メールなどをお送りすることはありません。「なりすましメール」には ZIP 形式のファイルが添付されており、ファイルを開くとコンピューターウイルスに感染することが想定されます。**絶対に添付ファイルを開かず、削除いただきますようお願いいたします。**
また、ヤマト運輸は、「なりすましメール」の対策として、弊社から送信するメールが正当なサーバから送信されたメールであることを表明するドメイン認証技術 SPF（Sender Policy Framework）を導入しています。お客様よりご利用のメールサービス提供プロバイダへ SPF 設定の有効化をご確認いただきますようお願いいたします。

【メールサービス提供プロバイダの SPF 設定の確認手順】
ご利用のメールサービス提供者がどこなのかを確認

1. ご利用のメールサービス提供者が送信ドメイン認証技術 SPF に対応したサービスを提供しているかを確認
2. 送信ドメイン認証技術 SPF を活用したサービス利用方法の確認

【SPF 設定とは】
ご利用のメールサービス提供プロバイダがドメイン認証技術 SPF に対応している場合、不正なメールを検知し、「受信しない」「ゴミ箱に直接入れてしまう」「注意を促す」などの対策が可能となります。パソコンやスマートフォン、携帯電話向けに提供されるメールサービスでは「なりすましメール対策」等の名称で多くのプロバイダが提供している機能です。

ヤマトグループは、「なりすましメール」対策を推進し、情報セキュリティの向上に努めてまいります。

ご不明な場合は saleshq@yamatoamerica.com までお願いいたします。

以 上