

役員等を騙る不審メールにご注意ください！



- ・実在する企業の役員や元役員名を騙り「LINEのグループトークを作成してQRコードを返信してください」といった不審メールが複数確認されています。
- ・メールの内容に従うと会社の資金を送金させられる等の詐欺被害の恐れが！

【詐欺メールの例】

●● (自社の会社名)

自社の社名



差出人 (会社の役員や元役員、自社の社員名など)
宛先

自社の社員など

いつもお世話になっております。

株式会社●● (差出人名) でございます。

LINEのグループトークを作成させる

業務上の都合により、恐れ入りますが、会社のLINEグループを作成していただき、社内の財務ご担当者様をグループに招待いただけますでしょうか。

お手数ですが、グループ作成後、参加用のQRコードを本メールへの返信にてお送りいただけますと幸いです。

こちらでQRコードを確認の上、参加させていただきます。

QRコードを送信させる



犯罪者

指示通りLINEのグループトークに参加してしまうと…

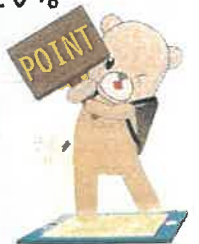
当社の口座残高をスクリーンショットして送ってほしい

別の会社に振り込む手続きをしてほしい



会社の資金を送金させられるなどの詐欺被害の恐れが！

- ・このようなメールが届いても決して返信せず、組織内で情報共有してください。
- ・送金に関するメールを受信した際は、メール以外の方法で内容を確認してください。
- ・連絡する際は、メールに記載された連絡先ではなく、別途資料（アドレス帳や名刺等）を確認してください。
- ・添付ファイルやリンク先を不用意に開かないでください。



埼玉県警察本部サイバー局サイバー対策課

S.P.P Cyber Bureau Cybercrime Countermeasures Division



緊急時はこちら！

最寄りの警察署又はサイバー犯罪相談窓口

▼埼玉県警察ホームページ

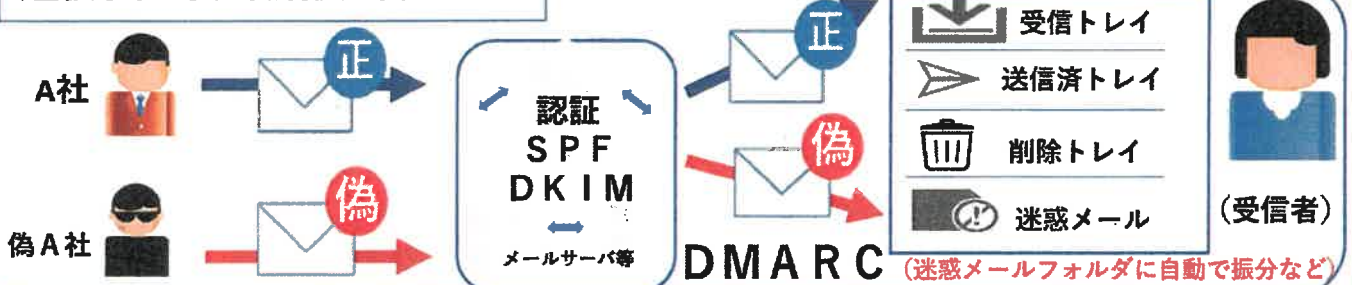


<http://www.policetokyo.net/saitama/cybercrime/>

なりすまし被害防止！ 送信ドメイン認証技術を導入しよう！

- ◆ フィッシングによる被害を防止するためには、**DMARC**などの**送信ドメイン認証技術**を活用し、**なりすましメールを受け付けない**ようにすることが有効です。
- ◆ フィッシングメールやビジネスメール詐欺などのなりすましによる被害を防止するために、送信ドメイン認証技術を導入しましょう！

送信ドメイン認証のイメージ



認証が失敗したときの事前対処マニュアル～DMARC

SPF・DKIMによる認証が失敗した場合の対応を事前に決めることで、受信をしない「拒否」や迷惑メールに「隔離」するなど、自動で対処できる技術

送信元情報を事前登録する～SPF

事前に送信元のIPアドレスを登録し、送信元がなりすましのアドレスか識別できるよう確認する技術。

電子署名をメールに付与する～DKIM

電子署名が正しいものか検証し、なりすましかどうかを識別する技術

(参考) 「送信ドメイン認証技術導入マニュアル」
迷惑メール対策推進協議会から公表されています。

<https://www.dekyo.or.jp/soudan/aspc/report.html>

