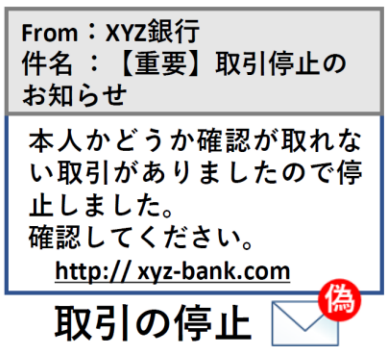
中小企業 と サイバーセキュリティ

第４回 お手軽サイバー防犯対策③
「ログインさせようとするメール、SMSは全部偽物」

「お手軽サイバー防犯対策」の第３弾。今回は、「ログインさせようとするメール、ＳＭＳは全部偽物」をご紹介します。

近年、実在するサービスや企業を装ったメール、ＳＭＳから偽サイトに誘導してＩＤ／パスワードを盗むフィッシングによるものとみられるネットバンキングの不正送金や証券口座の不正取引が多発しているほか、企業情報の搾取を狙い、業務で利用するクラウドサービスを装う手口もあり、中小企業も例外ではありません。



「【重要】アカウントのセキュリティ警告」や「【緊急】〇〇サービスで不正アクセスを検知」といった緊急性を装うメッセージは、受信者を心理的に追い込み、偽のログインページへ誘導する常套手段です。

これらのメッセージに記載されたＵＲＬを安易にクリックすると、大切な情報が攻撃者の手に渡り、甚大な被害につながるおそれがあります。

ここで知っておくべきポイントは、正規のサービスや企業がメールなどにＵＲＬを記載しログインを求めることはほぼないということです。

そこで、このようなメールなどを受信しても「全部偽物」と疑って、不審な点がないか確認する「間違い探し」を行いましょう。

もし「本当かもしれない」と思うのであれば、必ず公式サイトなどで確認をする、同僚や上司に意見を求める、情報システム担当者に連絡するなどしましょう。

また、記載された電話番号への連絡も絶対に避けるべきです。

「ログインさせようとするメール、ＳＭＳは全部偽物」

このシンプルな鉄則を社内で共有し、日々の業務の中で意識することで、巧妙なフィッシングによる被害を大幅に防ぐことが可能です。

コストをかけずにできるこの対策を、ぜひ、徹底してください。

神奈川県警察サイバーセキュリティ対策本部

※ この記事は川崎市産業振興財団機関紙「産業情報かわさき(2025年8月号)」に掲載されたコラムを再編集したものです。