中小企業 と サイバーセキュリティ

第3回 お手軽サイバー防犯対策②

「そのメール、開く前に確かメル」

　前回から、コストを抑えて取り組める「お手軽サイバー防犯対策」を紹介しておりますが、第二弾となる今回は「そのメール、開く前に確かメル」をご紹介します。

　個人の金銭や企業・組織の重要な情報を狙うサイバー犯罪、サイバー攻撃では、実在のサービスや企業を騙り、偽のメールやSMSでフィッシングサイトに誘導しＩＤやパスワードなどを盗み取る「フィッシング詐欺」、

取引先や自社の経営者等になりすまして、偽のメールを送って入金を促す「ビジネスメール詐欺」、企業や組織から情報を盗むため、担当者を特定して業務関係を偽ったウイルスメールを送り付ける「標的型メール攻撃」など、メールを使う手口が多くあります。

　ということは、メールに対する備えを万全にすることでかなりのリスク低減になると考えられます。

　では、どのようなメールへの備えが必要でしょうか。

　「怪しいメールは開かない」といったことは、誰もがわかっていると思いますが、攻撃者側もわかっているので、「怪しいメール」ではなく「怪しくないメール」が使われます。

　ですから、「怪しくないメール」でも、メールアドレスが普段と違う、内容に違和感がある、予定のない添付ファイルが付いている、URLやリンクへのアクセスを促している、「緊急」、「重要」などといった場合には、開く前に送信元に電話等で確認する事が必要となります。

　「メールに気をつける」といったことは「当たり前」と思われるかもしれませんが「**凡事徹底**」のサイバーセキュリティが重要な事なのです。

　凡事徹底のサイバーセキュリティを推進するために、職場で「**そのメール、開く前に確かメル**」という標語を掲げてみてはどうでしょうか？

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5月号)」に掲載されたコラムを再編集したものです。