メール配信システムは放置厳禁！

過去に導入したメール配信システムを、使用しなくなり、削除もせずにそのまま放置状態にしている、なんてしていませんか？

危険です！

“脆弱性放置”が原因による被害が発生中！

例：ａｃｍａｉｌｅｒの脆弱性を悪用された不正アクセス被害（イメージ）

　　攻撃者は脆弱性が放置されている状態のメール配信システムに対して、脆弱性を突いてログインＩＤ・パスワードを書き換え、管理権限を乗っ取ります。

　　その後、攻撃者は乗っ取ったメール配信システムを悪用し、なりすましメールを送信します。

　　事例のａｃｍａｉｌｅｒは簡単にメール配信ができるシステムですが、ログインＩＤ・パスワードが外部から書き換え可能となる脆弱性等が発見されており、開発元の企業が公開している修正バージョンへのアップデートを行わずに脆弱性を放置していたために、管理権限を乗っ取られ、なりすましメールの配信等に悪用されしまう被害が発生しています！

過去に使用していたものの、現在は使わなくなり、そのまま削除せずに放置していたために不正アクセスされたという事例もあり、注意が必要です！

対策

　　ａｃｍａｉｌｅｒを使用している場合は、最新版にバージョンアップする！

　　利用しなくなったａｃｍａｉｌｅｒは放置せずに必ず削除する！

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！

https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/