

ウェブサイトに対する攻撃への警戒について



宮崎県企業・警察サイバーセキュリティ連携協議会
宮崎県警察本部サイバー犯罪対策課

1 概要

県内において、採用情報ページのエントリーフォームを通じ、採用担当者に対し大量のメールが送りつけられたと思われる事案がありましたので、情報共有及び注意喚起を致します。

2 判明事項

現時点、実害はありませんが、ウェブサイトの委託先事業者の調査で、海外からのアクセスであることが判明しています。

3 攻撃手法及び対策

ウェブサイトの問い合わせフォーム等に対しSQLインジェクション（ウェブサイト内に保存されたデータ等を不正に取得する攻撃手法）等のぜい弱性がないかを調査するためのもので、以前から国内外の複数のサイトで確認されているようです。

下記セキュリティ情報サイトで概要が説明されていますので、参考にしてください。

<https://ccsi.jp/3182/>

なお本件については、ボット（自動化プログラム）による攻撃とみられ、投稿フォーム等の不正利用を防止する無料のツール

Googleリキャプチャ（reCAPTCHA）

の導入が有効です。

※参考サイト <https://tart.co.jp/google-recaptcha/>

4 被害に遭った時には

各会員様におかれましては、できる範囲での対策をとっていただき、同様の事案を認知した際は警察への通報をお願い致します。