令和３年１２月　７日

西宮市政記者クラブ各位

西宮市総務局デジタル推進部長

庁内グループウェアへのサイバー攻撃について

１．事実内容

令和３年１２月６日、職員等が利用する庁内グループウェアへのサイバー攻撃によりユーザ情報が流出し、職員へのなりすましによる庁内外へのメール送信が確認されました。

２．経過

【令和３年１２月５日（日）】

１５：１８　庁外から、庁内グループウェアの一部機能である議会行事予定ページの脆弱性を突いたＳＱＬインジェクション攻撃※が開始

２３：１１　複数のデータベースへのアクセスを試みた結果、管理者権限のパスワードが流出、庁内メールシステムの管理者画面に手動で不正ログイン（以降、１２月６日の１６時１０分まで断続的にアクセス）

２３：５７　管理者画面から職員Ａのユーザ情報（ユーザＩＤ・パスワード）を閲覧

【令和３年１２月６日（月）】

１１：０８　管理者画面から職員Ｂのユーザ情報（ユーザＩＤ・パスワード）を閲覧

１３：５２　管理者画面から職員Ｃのユーザ情報（ユーザＩＤ・パスワード）を閲覧

１４：４５　職員Ｃのユーザ情報を用いて庁内メールシステムに不正ログインし、外部アドレスに１通の送信を試み

１６：０１　職員Ｃのユーザ情報を用いて庁内メールシステムに再度不正ログイン

１６：０６　職員Ｃになりすまし、外部アドレスに３通の送信を試み、その後７通のメールを庁内の７３０アドレスに送信

（職員Ａ・Ｂへのなりすましの記録はない）

１６：３０　庁内の複数部署より不審メールが送付された旨、デジタル推進課に報告があり事象を確認、庁内への注意喚起を実施し調査に着手

１８：５０　デジタル推進課においてＳＱＬインジェクション攻撃の痕跡を発見

１９：００　デジタル推進課において庁内メールシステムへの外部からのアクセスを停止

【令和３年１２月７日（火）】

９：２０　　調査および対策を実施のうえ再開

※ＳＱＬインジェクション攻撃とは

ＷＥＢサイトの検索ボックスや入力フォームなどに記入する文字列に、データベース操作を行う命令を意図的に「注入」することにより、不正なデータベース操作を行う攻撃

３．影響

職員３名のユーザＩＤおよびパスワードが流出し、その内１名の職員になりすましされたことで、庁外の１アドレスおよび庁内の７３０アドレスに不審メールが送信されました。（４通外部への送信を試みているが３通は送信できていない）

４．原因

庁内グループウェアの一部機能である議会行事予定ページを外部公開したときから、プログラムに脆弱性が含まれた状態であったこと、また、外部の脆弱性診断でも検知されず、庁内設置のセキュリティ機器でも攻撃を防御できなかったことが原因です。

５．対策

プログラム上の脆弱性対策を徹底するとともに、攻撃の検知機能の強化見直しを行います。

６．見解

市が管理するシステムにおいて、サイバー攻撃により不正アクセス事案を発生させてしまい申し訳ございませんでした。なお、住民の皆様の個人情報はインターネットには接続されていないネットワークにおいて厳重に管理いたしており、影響はございません。ご心配をお掛けいたしましたことをお詫び申し上げます。

【お問い合わせ先】
西宮市総務局デジタル推進部デジタル推進課
担　当：南　晴久
電　話：0798-35-3519