参考：2025年12月25日の公表資料

写

提 供 日　2025/12/25
タイトル　セキュリティサービス提供事業者における不正アクセス被害について
担　　当　企画部 電子県庁課
連 絡 先　技術管理班
TEL 054-221-2939

セキュリティサービス提供事業者における不正アクセス被害について

１　要旨

・県と県内市町（浜松市を除く）は、「自治体セキュリティクラウド」を共同運用し、株式会社TOKAIコミュニケーションズ（以下、TOKAI）に委託しています。
・12月19日、TOKAIは、法人向けに提供するメールサービスが外部からの不正アクセスを受け、情報が漏えいした可能性があることを公表しました。
・この一部として「自治体セキュリティクラウド」にて利用しているメールサービスのログ情報が漏えいした可能性が疑われています。
・現時点で、第三者への情報漏えいの事実は確認されていません。
・県及び県内市町（浜松市を除く）と電子メールの送受信を行った法人・個人に対し、自治体をかたる不審な電子メールが送付される可能性があることから、注意喚起をします。

２　情報漏えいの可能性のある団体

・静岡県
・浜松市を除く県内３４市町
※浜松市は「自治体セキュリティクラウド」と同等のサービスを、独自に構築しているため、共同運用をしていません。

３　情報漏えいの可能性がある情報（ログ情報）

・令和５年４月以降に上記団体との間で送受信した電子メールのヘッダ情報の一部
（送信者・受信者のメールアドレス、件名、送信日時、その他メールシステム等で付加された情報）
・漏えいした可能性があるメールアドレスは約２万件（速報値）

４　不正アクセス判明後の対応

・TOKAIは、外部セキュリティ専門会社と連携した調査を実施中
・県は、TOKAIにログ情報の管理方法に関する改善を求め、TOKAIはこれに対応
・県は、静岡県公式ホームページに注意喚起を本日掲載

５　静岡県からのお願い

・情報漏えいの事実は確認されていませんが、本件に関連した詐欺等の悪意あるメールが送信されるおそれがあります。
・心当たりのないアドレスや、自治体をかたる不審な電子メールが届いたときには、添付ファイルや、URLのリンクを開かないようにしてください。
・気になる場合は、不用意に返信せず、アドレス帳や過去に受信したメールのアドレスを使って、送信元に確認してください。

６　不正アクセスの原因等

・TOKAIは、高品質のサービスを提供するため、使用するアプリケーションやプラットフォームに対して、毎年、脆弱性診断を実施していたと報告を受けています。

・今回の不正アクセスの原因は、法人向けに提供するメールサービスで使用するサーバー機器に未知の脆弱性※があり、この脆弱性を悪用されたことによります。

・TOKAIは、サーバー機器のメーカーと連携し、調査の実施や対応策の検討を進めています。

※未知の脆弱性

ＯＳやソフトウェアの脆弱性が発見されたときに、メーカーが修正プログラムを配布する前に、その脆弱性を利用して行われる攻撃です。
脆弱性が公開されてから、メーカーが対応策を検討して修正プログラムを開発することも多いため、完全な対策は困難といわざるを得ません。
そのため、指摘された脆弱性の内容を確認し、危険となる行為を行わないなど、修正プログラムを適用するまでの間は十分な注意が必要です。
（引用元：総務省「国民のためのサイバーセキュリティサイト」の「脆弱性とは？」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/11/
）