広　　報　　資　　料
令 和 ３ 年 ４ 月 ２２ 日
情 報 技 術 犯 罪 対 策 課

犯罪インフラ化するＳＭＳ認証代行への対策について

１　課題

(1)　ＳＭＳ認証とその機能

○　「ＳＭＳ認証」とは、ショートメッセージサービス（ＳＭＳ）で利用者の番号に認証コードを通知し、当該コードを用いて認証する方式。

○　通常は、利用者が自ら用いる本人確認済の携帯電話の番号に当該認証コードが通知されることから、金融機関等においては、ＩＤ・パスワードによる認証に加え、ＳＭＳ認証を利用者に実施させる「二経路認証」を採用。なりすまし等による不正認証を防止。

(2)　ＳＭＳ認証代行とその問題点

○　「ＳＭＳ認証代行」は、通信事業者とＳＭＳ機能付データ通信に係る契約をし、利用者に当該契約に係る番号を提供。また、当該番号に通知された認証コードを利用者に代わって受領し利用者に提供。

○　利用者は、ＳＭＳ認証代行から番号・認証コードの提供を受けることにより、なりすまし等による不正アカウントの設定が可能。

○　通信事業者の中には、本人確認をすることなくＳＭＳ認証代行と契約するものがおり、警察捜査における事後追跡性の確保に支障。

２　サイバーセキュリティ政策会議及びＩＴ業界団体の提言

(1)　令和２年度サイバーセキュリティ政策会議の提言

報告書において、通信事業者による上記契約時の本人確認の徹底や犯罪インフラを提供する悪質事業者の摘発強化を提言。

(2)　ＩＴ業界団体の提言

（一社）日本ＩＴ団体連盟は、ＳＭＳを用いた二経路認証の抜け道になっているとして上記契約時の本人確認の徹底を提言。

３　警察における対策

(1)　通信事業者の業界団体に対する要請

令和３年１月、総務省と連携して、（一社）テレコムサービス協会ＭＶＮＯ委員会に対し、契約時の確実な本人確認を要請。同要請を受け、同月、加盟事業者の自主的な取組として、ＳＭＳ機能付データ通信契約に係る本人確認を実施することを申し合わせ。

(2)　取締りの強化

都道府県警察に対し、ＳＭＳ認証代行を含む犯罪インフラに関し、法令に違反する悪質事業者に対する取締りの強化を指示。