ニッキン

BCP見直し急務

目的不明のDDoS多発

金融界

金融界でオンラインサービスの停止に備えたBCP（業務継続計画）の見直しが急務となっている。大手行グループや他業界で2024年末から25年始めにかけて「DDoS（ディードス）」と呼ぶサイバー攻撃で、一時的にサービスが利用しにくくなる事案が相次いだため。NTTデータ経営研究所の大野博堂・金融政策コンサルティングユニット長は「バックアップへの切り替えができない場合を想定して、今一度手順のアップデートを図ることが目先で必要」と強調する。

三菱UFJ銀行は24年12月26日、生体認証の仕組みを利用できなくなった。また、みずほ銀行はインターネットバンキングに影響が出た。りそなホールディングス傘下のりそな、埼玉りそな、関西みらい、みなとの4行も「マイゲート・グループアプリ」、三井住友カードが会員向けサービスで被害に遭ったとみられる。

DDoS攻撃は大量のデータを送りつけてコンピューターの負荷を高めることで、システムをダウンさせる手法だ。政治・社会的な主張をハッキングと組み合わせる「ハクティビスト」の関与も疑われるが、今回の一連の事案では犯行声明がない。

そのため、社会的混乱を招くのが目的の「愉快犯」「嫌がらせ」による行為との見方が強い。

ただ、サーバーをダウンさせる以外の狙いを持っていた可能性も捨て切れない。例えば、サービス停止中にフィッシングサイトを立ち上げ顧客のIDとパスワードを盗むほか、エンジニアが復旧にあたっている間に情報システムなど他システムで攻撃を成功させるといったことが想定される。このため、複合攻撃を念頭に置いた対応策の策定が求められる。

「BCPが陳腐化している金融機関もある」（前出の大野氏）ほか、エンジニアが限られている金融機関もあり、BCPの点検が急がれる。相次いだDDoS攻撃については、金融庁も金融機関に注意を呼びかけている。

ニッキン 2025年1月31日号1面