中小企業の

セキュリティー対策

—30—

DDoS攻撃への備えを

大量処理要求で高負荷状態に

近年、多くの企業がインターネット上で、ウェブサイトなどを運営し、情報の発信やサービスの提供を行っているが、そうしたウェブサイトや企業で利用しているDNSサーバーに対して、大量の処理要求を送信して高負荷状態にさせるDDoS（分散型サービス妨害）攻撃が確認されている。処理が追い付かなくなるほどの処理要求を受けたウェブサイトやDNSサーバーは、閲覧ができなくなったり、レスポンスが遅延したりするなど、サービスを正常に保つことができなくなるため、機会損失による損害などが発生することになる。

2018年10月には、動画サイトにおいて、サービスが利用できなくなったり、画面表示に時間がかかったりするなどの不具合が発生した。動画サイトの運営者は、システム量のアクセスを行い、に過剰な負荷を及ぼす異常な量の通信が観測されたことを受け、その通信を遮断したが、攻撃者は手段を変えて同事象を発生させるなどして、執拗（しつよう）なDDoS攻撃が行われたと報道されている。

DDoS攻撃の主な手口として、攻撃者に乗っ取られた複数のサーバーやIoT機器から形成されるネットワーク（ボットネット）に攻撃命令を出し、標的企業のウェブサイトやDNSサーバーへ大量のアクセスを行い、高負荷を掛けてくる。また、送信元のIPアドレスを標的組織のサーバーに偽装して、多数のルーターやDNSサーバーなどに問い合わせを送り、応答結果を標的組織に送り付け、高負荷を掛けてくる場合もある。

近年は、違法取引などが行われるダークウェブなどにあるDDoS代行サービスを利用してDDoS攻撃を行うケースも確認されている。DDoS攻撃のための専門的な技術や設備がなくても攻撃が行えるため、ウェブサイトなどを運営している企業は規模にかかわらずDDoS攻撃への備えを怠ることはできない。

アクセス制限し被害予防

DDoS攻撃に対する被害予防として以下が挙げられる。

・ISP（インターネット接続事業者）などのサービスを利用している場合は、サービスの価値とかける費用を考慮して、最大許容量の見直しなどを行う。また、オプションなどでDDoS対策が提供されている場合はそれを利用する。

・外部から不要なサーバーやサービスへのアクセスを制限する。

・システムの冗長化などの軽減策を実施する。

・ネットワークを冗長化し、DDoS攻撃の影響を受けない非常時用ネットワークを事前に準備する。

・DDoS攻撃を受けてサービスを停止させられることを想定して、サービス停止時の代替サーバーや、サービス停止によって利用者を混乱させないための告知用サーバーや、SNS（ソーシャルネットワーキングサービス）の企業公式アカウントなどの連絡手段を用意しておく。

また、DDoS攻撃の被害を受けた後の対応として以下が挙げられる。

・CSIRT（セキュリティー対応組織）へ連絡する。

・攻撃元IPアドレスからの通信をブロックなどの通信制御を行う。

・利用者へ状況の告知を行う。

・影響調査および原因の追究、対策の強化を行う。

DDoS攻撃対策の詳細については、独立行政法人情報処理推進機構（IPA）のウェブサイト（https://www.ipa.go.jp/security/）の公開資料を参考にしてほしい。

（独立行政法人情報処理推進機構・江島将和）

サービス妨害攻撃のイメージ