

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にや企業が利用しているDNSサーバに対して、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ーバやDNSサーバは、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。

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（インターネット接続事業者）に準備する。影響を受けない非常時にネットワークを事前

DDoS攻撃への備えを

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

DDoS攻撃の主な手口として、攻撃者に

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（インターネット接続事業者）に準備する。

影響を受けない非常時にネットワークを事前

準備する。

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

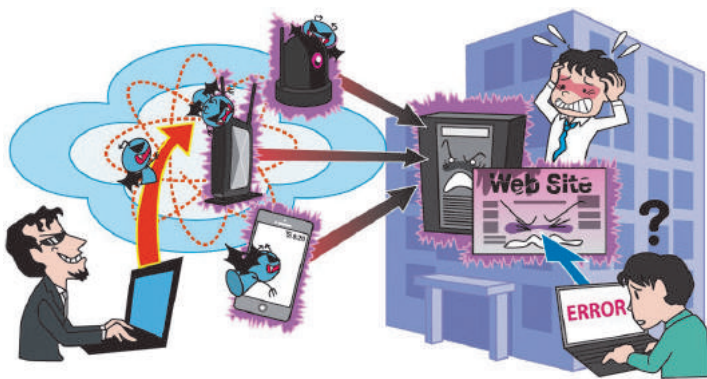
DDoS攻撃の主な手口として、攻撃者に

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（インターネット接続事業者）に準備する。

影響を受けない非常時にネットワークを事前

準備する。

サービス妨害攻撃のイメージ



の告知用サーバや、SNS（ソーシャルネットワーク）の企業公式アカウント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）のウェブページ（<https://www.ipa.go.jp/security/>）の公開資料を参考にしてください。
- （独立行政法人情報処理推進機構・江島将和）