サービス妨害攻撃への備えと対応

初版発行：　2011年9月
最終更新：　2025年3月

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

はじめに

本資料は、オーストラリア信号局（ASD）が、ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）、Akamai Technologies Ltd、Cloudflare Pty Ltd と連携し、本地域におけるサービス妨害（denial-of-service：DoS）攻撃の増加傾向に対応する目的で作成されたものです。DoS攻撃への備えと対応に向けて、最新の脅威手法を踏まえたベストプラクティスに沿った緩和策を、組織向けに提供します。

本助言は、ASD が発行する*「IoT（モノのインターネット）機器」*および*「Wi-Fi とルーターのセキュリティ対策」*とあわせてご参照いただくことを推奨します。これらの資料は、DoS攻撃に意図せず加担して他者に影響を及ぼすことを防ぐうえで役立ちます。

DoS攻撃とは、ウェブサイト、電子メール、ドメインネームシステム（DNS）などのオンラインサービスを妨害または低下させることで、正規ユーザーのアクセスを阻害することを目的としたサイバー攻撃です。この攻撃は通常、オンラインサービスに対して大量のデータ、接続、リクエストを送りつけてサービスを過負荷にし、機能を低下させることで実行されます。

DoS攻撃を成功させるには、通常、大量のネットワークトラフィックが必要とされます。このような攻撃は近年ますます一般化しており、その背景には、脆弱性を抱えた「モノのインターネット（IoT）」機器の普及があると考えられます。IoT機器の製造業者は、サイバーセキュリティよりもユーザーエクスペリエンスを優先する傾向があるため、スマートテレビ、ケトル、掃除機、セキュリティシステムなどの家庭用インターネット接続製品が、脆弱な機器となることがあります。これらの機器は、悪意のあるアクターによって遠隔操作され、ネットワークトラフィックを発生させる「ボットネット」の一部として利用される可能性があります。その結果、家庭や組織が意図せず、DoS攻撃を支えるインフラの一部となってしまうおそれがあります。

近年の動向から、悪意あるアクターが多数のIoT機器を侵害し、そのインフラをサイバー犯罪者やハクティビストに貸与または販売している可能性が示唆されています。こうした者たちは、自ら選定した標的に対してDoS攻撃を仕掛けることに強い関心を示しています。多くの場合、DoS攻撃は、組織に生産性の低下や金銭的損失をもたらすこと、または特定の目的のために社会の注目を集めることを目的として実行されます。このような活動の具体例については、ASDの注意喚起文書 *「中華人民共和国と関連のあるアクターが、ボットネット運用のためにルーターおよびIoT機器を侵害」*に記載されています。

経済のデジタル化がさらに進み、インターネットに接続されるセキュリティの不十分なIoT機器が増加する中、DoS攻撃は今後も増加し続けると考えられます。

悪意のあるアクターは、組織のオンラインサービスを妨害または機能低下させるために、さまざまな手法を用います。主な手法として、以下が挙げられます。

- 大量の不要なネットワークトラフィックをオンラインサービスに送りつけて、利用可能なネットワーク帯域を過剰に消費させることを目的とした手法
- オンラインサービスに対して意図的に設計されたネットワークトラフィックを送りつけ、コンピュータの処理リソースを過剰に消費させることを目的とした手法
- 複数のコンピュータやIoT機器、その他のインターネット接続機器を用いて、さまざまな方向から大量のネットワークトラフィックをオンラインサービスに送りつける手法（DoS攻撃の一種であり、「分散型サービス妨害（DDoS）攻撃」として知られる）
- 組織のドメイン登録情報やDNSサーバーを乗っ取り、正規のユーザーを本来のオンラインサービスとは異なる不正なサイトなどへ誘導する手法

組織がDoS攻撃の標的となることを完全に防ぐことはできませんが、攻撃に備え、その影響を軽減するために講じることのできる対策は数多く存在します。DoS攻撃への対策として最も効果的なのは、事前の備えです。あらかじめ準備をしていない場合、攻撃発生時の対応は非常に困難となり、対策の効果も限定的になってしまうおそれがあります。

組織は、DoS攻撃から自らを守ることに重点を置きがちですが、自身のオンラインサービスやインターネット接続機器が悪意あるアクターに悪用され、他者への攻撃に加担することのないよう対策を講じることも同様に重要です。

DoS攻撃への備え

地域全体でDoS攻撃の発生件数が増加する中、具体的な対策を講じる前に、まずは貴組織の事業要件を評価し、各オンラインサービスについて、攻撃発生時に運用の継続が求められるのか、あるいは一時的な中断が許容されるのかを判断する必要があります。

DoS攻撃に対する耐性を高めるためには、攻撃が発生する前に、可能かつ現実的な範囲で以下の対策を積極的に講じることが推奨されます。

- コンテンツ・デリバリー・ネットワーク（CDN）を利用している場合は、可能かつ現実的な範囲で、以下の追加策を講じることが推奨されます。
  - アプリケーション層およびネットワーク層に対するさまざまな攻撃からオリジンウェブサーバーを保護する機能を備えたCDNの利用を検討してください。こうした保護機能は、CDNによっては、エッジに配置されたウェブアプリケーションファイアウォール（WAF）の一部として提供されていることがあります。
  - オリジンウェブサーバーのIPアドレスを不必要に公開しないようにし、やむを得ず公開する場合は、DoS攻撃から適切に保護されていることを必ず確認してください。
  - オリジンウェブサーバーには、悪意あるアクターに予測されやすいIPアドレスを使用しないようにしてください。たとえば、既にオンラインサービスで公開されているIPアドレスと同一のネットワークサブネット内のアドレスなどは、避けるべきです。
  - ファイアウォールなどのネットワークアクセス制御を使用し、CDNおよび貴組織の許可された管理ネットワークのみがオリジンウェブサーバーにアクセスできるようにしてください。
  - オリジンウェブサーバーに対してより高いレベルの保護が求められる場合は、CDNプロバイダとの間にプライベートネットワーク接続を含む、耐障害性のある多様なネットワーク接続を検討してください。
  - CDN、オリジンウェブサーバー、クライアントにおけるHTTPヘッダーを適切に設定し、キャッシュ量の最適化を図ってください。

  - より高い可用性が求められる場合は、低リスクのIPアドレスからのリクエストと高リスクのIPアドレスからのリクエストを分離して処理できるよう、オリジンウェブサーバーを分割することを検討してください。
- 正当なユーザーにとって許容可能な機能やサービス品質、それらを維持するための方法、そしてDoS攻撃発生時に不要と考えられる機能をあらかじめ特定しておくことが重要です。
- クラウド型のDoS攻撃対策サービスの導入および活用を検討してください。
- 以下の手段を講じることで、貴組織の攻撃対象領域（アタックサーフェス）を縮小できます。実施を検討してください。
  - DNSなどの基盤的なオンラインサービスを、DoS攻撃への耐性を備えた信頼性の高いサービスプロバイダに委託する
  - 電子メールなどの重要なオンラインサービスと、ウェブサイトなど攻撃の標的となりやすい他のオンラインサービスを分離する
  - DoS攻撃の緩和サービスが、対象のオンラインサービスに関連するネットワークポートの通信のみを許可するように設定する
- DoS攻撃に対する予防および緩和戦略の詳細について、サービスプロバイダと事前に協議してください。特に、以下の点を確認することが重要です。
  - 世界各地からのDoS攻撃に耐えうる実績ある対応能力
  - DoS攻撃および包括的な公認DoS攻撃テストの両方に対応した実績
  - ネットワークトラフィックの手動分析など、人手を介さずにほとんどの種類のDoS攻撃を自動的に軽減する能力
  - サービスの料金体系（例：固定料金制、ネットワークトラフィック量やコンピュータ処理リソースの使用量に応じて変動する従量課金制、請求上限の設定が可能かどうかなど）
  - DoS攻撃時の通知やオンラインサービス停止に関する判断基準
  - DoS攻撃時に実行可能な、事前承認済みの対応措置
  - 上流プロバイダーとのDoS攻撃防止に関する取り決め
- システムの可用性、ネットワークトラフィック、コンピュータ処理リソース、関連コストなどをリアルタイムで監視・警告するための対策を講じてください。
- DoS攻撃発生時にもサービスを継続できるよう、処理負荷と帯域幅の消費を最小限に抑えた静的バージョンのウェブサイトを事前に用意してください。
- 大容量の帯域幅、十分なコンピュータ処理リソース、地理的に分散したホスティング拠点、および望ましくないネットワークトラフィックを除去するクラウド型のトラフィックスクラビング機能を備えた、高い耐障害性を有するオンラインサービスの導入と活用を検討してください。これには一般的に、信頼性の高いCDNを利用して静的コンテンツをキャッシュし、オリジンウェブサーバーを不要なネットワークトラフィックから保護することが含まれます。
- レジストラロックの使用や、ドメイン登録時の連絡先情報およびその他登録情報の正確性の確認を通じて、貴組織のドメイン名を適切に保護してください。あわせて、ASDが発行する「*ドメイン所有者のためのDNSセキュリティ*」に記載されている追加策にも従うことが推奨されます。
- サービスプロバイダの連絡先情報を常に最新の状態に保つとともに、貴組織の連絡先情報もサービスプロバイダと適切に共有してください。また、必要に応じて、すべての連絡先が対応可能であること（たとえば24時間365日）を確認することが重要です。
- 通常の通信手段が利用できない事態に備え、信頼性の高い連絡手段として、貴組織のアウトオブバンド連絡先情報をサービスプロバイダに提供してください。
- DoS攻撃への耐性が求められる各オンラインサービスについて、想定されるさまざまな種類のDoS攻撃に対応するサイバーセキュリティインシデント対応計画を策定・実施・維持してください。この計画は少なくとも年に1回は実施されるべきです。

- コンピュータ処理リソースを多く消費したり、追加費用が発生したりする機能（例：SMS送信）については、悪用されるリスクを考慮し、アプリケーションを適切に設計してください。
  - 保護手段には、リクエスト数の制限（レートリミット）や、リクエストが人間によるものであることを確認する仕組みが含まれます。
  - アプリケーション機能における不適切なロジックフローを狙ったものを含め、DoS攻撃を想定したテストを実施してください。
  - DoSベクターを特定し、対処するために、広範な負荷テストを実施してください。

DoS攻撃への対応

貴組織がDoS攻撃への備えを事前に講じていない場合でも、攻撃発生時に上記の一部対策を講じることは可能です。ただし、これらの対策は即効性に欠け、実施までに時間を要する可能性があるため、結果として対応力が低下するおそれがあります。

DoS攻撃発生時には、適切かつ実行可能な範囲で、以下の対策を実施してください。

- サイバーセキュリティインシデント対応計画を実施してください。
- サービスプロバイダーに対し、即時に対応措置を講じることが可能かどうかを事前に確認してください。あらかじめ対応可否について協議していない場合、対応が行われない、対応を拒否される、あるいは追加料金を請求される可能性があります。
- 現在のDoS攻撃の効果を高める要因となっている、必須ではない機能やコンテンツは、オンラインサービスから無効化または削除してください。たとえば、検索機能、動的コンテンツ、大容量ファイルなどを含まないバージョンのウェブサイトを展開することが有効です。
- DoS攻撃緩和サービスプロバイダーを含む各種サービスプロバイダや顧客との連絡体制を維持するとともに、貴組織のオンラインサービスの可用性について継続的に監視してください。
- オリジンウェブサーバーが直接的な標的となっている場合は、IPアドレスの変更を検討してください。ただし、新しいIPアドレスについては、適切な保護策が講じられるまでは、公開しないようにしてください。
- DoS攻撃が発生した場合は、本資料の「連絡先」欄に記載されているASDおよびNCSC-NZを含む関係機関に速やかに報告してください。

DoS攻撃への加担を防ぐために

貴組織が意図せず他者へのDoS攻撃に加担することを防ぐため、以下の対策を実施してください。

- 不要なもの、セキュリティ設定が不十分なもの、または適切に保守管理されていないサービス、IoT機器、その他のインターネット接続機器を、インターネット上に公開しないようにしてください。
- インターネットに公開するサービス、IoT機器、その他のインターネット接続機器については、適切に設定・保守を行うとともに、継続的に監視してください。
  - 小規模事業者向けの追加のガイダンスについては、ASDが発行する「*IoT機器*」および「*Wi-Fiとルーターのセキュリティ対策*」に掲載されています。

貴組織がオンラインサービスを運用している場合は、以下の追加対策を実施してください。

- 米国サイバーセキュリティ・インフラセキュリティ庁（CISA）の助言文書「*UDPベースの増幅攻撃*」に記載されている対策プロトコルを優先的に検討してください。

- 新たな増幅ベクターが特定された場合には、それを監視し、貴組織のオンラインサービスがそれらに対して脆弱にならないよう保護してください。
- 許可されたオンラインサービスおよび組織へのアクセスを制限するため、インバウンドおよびアウトバウンドの両方について、適切なネットワークアクセス制御を設定してください。
- 必要がない場合は、増幅攻撃の標的となりやすいオンラインサービスへの匿名のパブリックアクセスを遮断してください。
- ブロックやアクセス制御の適用が困難または適切でない場合には、悪用による影響を軽減する手段として、レート制限の実装を検討してください。

詳細情報

ASDの*「情報セキュリティマニュアル」*は、サイバー脅威からシステムやデータを保護するために組織が適用できるサイバーセキュリティフレームワークです。*「サイバーセキュリティインシデント」*を軽減するための戦略」および「エッセンシャルエイト」の助言は、同フレームワークを補完する内容となっています。

*「ニュージーランド情報セキュリティマニュアル」*は、情報保証および情報システムセキュリティに関するニュージーランド政府の公式マニュアルです。同マニュアルは、各機関の情報セキュリティ責任者に加え、機関にサービスを提供するベンダー、請負業者、コンサルタントのニーズにも対応した実務者向けマニュアルです。

各種DoS攻撃に関する詳細情報は、CISAが発行する*「DDoSクイックガイド」*および*「分散型サービス妨害（DDoS）攻撃を理解する」*に掲載されています。

連絡先

（オーストラリア国内から）本ガイダンスに関してご不明な点がある場合は、*ASD*まで文書でお問い合わせいただくか、1300 CYBER1（1300 292 371）までお電話ください。

（ニュージーランド国内から）サイバーセキュリティインシデントを報告する場合は、incidents@ncsc.govt.nz 宛に電子メールを送信いただくか、NCSC-NZの「インシデント報告」ページをご参照ください。

免責事項

このガイドブックの内容は一般的なものであり、特定の事情や緊急事態においては法的な助言や依拠すべき助言とみなされるべきものではありません。重要な事柄については、ご自身の状況に応じて、独立した専門家から助言を受けることをおすすめします。

このガイドブックに含まれる情報に依拠した結果生じた損害、損失や費用に対して豪連邦政府はいかなる責任も負いません。

さらに詳細な情報について、またはサイバーセキュリティ事件の通報は以下の連絡先まで：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

この電話番号はオーストラリア国内でのみご利用いただけます。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre