（別添様式１）ＤＤｏＳ攻撃事案共通様式

【重要】各シートは削除しないこと
セルが黄色になる場合は入力エラーのため修正すること

DDoS攻撃事案共通様式

西暦で記載

2025 年 10 月 10 日
20 時 40 分

24時表記で記載

宛先は変更不要

（報告先機関の長）殿

第1報は「新規」にチェック。第2報以降は新規のチェックを外して「続報」にチェック

前回報告は1つ前の報告の際の報告日時を記載

新規又は続報の別：　☐ 新規　☑ 続報（前回報告：　2025 年 10 月　5 日 13 時　30 分）

本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。

記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び内容について以下に記載してください。

共有等を希望しない場合はチェック

☐ 内閣官房国家サイバー統括室への共有等を希望しない。

共有等を希望しない内容：

共有等を希望しない場合は必ず共有を希望しない内容を記載

（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、内閣官房国家サイバー統括室に共有されることがあります。

１．記載の手引き

（１）本様式の対象となる手続

次に掲げる手続のうち、DDoS攻撃により生じ、又は生じたおそれがある被害について、事業者等が希望する場合に利用することができる。

〇次に掲げる法令、ガイドライン等に基づく報告（重要インフラのサイバーセキュリティに係る行動計画において、重要インフラ分野として指定されている分野に係る報告。具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。）

・電気通信事業法(業務停止等の報告)第28条
・放送法(重大事故の報告)第113条、第122条、第137条
・主要行等向けの総合的な監督指針
・中小・地域金融機関向けの総合的な監督指針
・系統金融機関向けの総合的な監督指針
・清算・振替機関等向けの総合的な監督指針
・事務ガイドライン第三分冊：金融会社関係(12電子債権記録機関関係)
・保険会社向けの総合的な監督指針
・金融商品取引業者等向けの総合的な監督指針
・金融商品取引所等に関する内閣府令第112条
・社債、株式等の振替に関する法律(事故の報告)第19条
・一般振替機関の監督に関する命令(事故)第17条
・金融商品取引法(金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務)第188条
・金融商品取引清算機関等に関する内閣府令(金融商品取引清算機関の業務に関する提出書類)第48条
・事務ガイドライン第三分冊：金融会社関係(14資金移動業者関係)
・事務ガイドライン第三分冊：金融会社関係(５前払式支払手段発行者関係)
・航空分野における情報セキュリティ確保に係る安全ガイドライン
・空港分野における情報セキュリティ確保に係る安全ガイドライン
・鉄道分野における情報セキュリティ確保に係る安全ガイドライン
・電気関係報告規則第３条、第３条の２
・ガス関係報告規則第４条
・地方公共団体における情報セキュリティポリシーに関するガイドライン
・医療情報システムの安全管理に関するガイドライン
・水道分野における情報セキュリティ確保に係る安全ガイドライン
・物流分野における情報セキュリティ確保に係る安全ガイドライン
・石油化学分野におけるサイバーセキュリティガイドライン
・割賦販売法(後払分野)に基づく監督の基本方針
・クレジットCEPTOARにおける情報セキュリティガイドライン
・石油分野における情報セキュリティ確保に係る安全ガイドライン
・港湾分野における情報セキュリティ確保に係る安全ガイドライン
・港湾運送事業法第33条

〇警察への相談
〇その他所管省庁から本様式により報告を行うよう要請等があった場合

（２）記載事項

１から６までの内容を記載してください。また、続報として提出する場合には、前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。

※1　いずれの項目も、全ての項目を記入する必要はなく、報告をしようとする時点で把握している範囲で、その内容を記載すること。
※2　自由記述欄は、記載例を参考に適宜記載すること。

１．報告者の概要

報告者の氏名 又は名称	（フリガナ）	マルマルカブシキガイシャ
		○○株式会社
法人番号（13桁）		1234567890123
事務連絡者の氏名	（フリガナ）	ナイカク　ゴシチノキリ
		内閣　五七桐
	所属部署	サイバー総括部　　電話番号　000-1111-2222
	E-mail	ELPMAXE@EXAMPLE.JP

２．業務への影響

（１）事案の概要

○株式会社管理サービスが運営する入会登録HP（http://・・・・・・）
・10月5日に入会登録HPにおいて、入会登録情報が1分間に約1000件の申請があり、HPがつながりにくい状況が発生
・10月10日に当該HPに同様の1分間に約1000件の申請があり、前回と同様にHPがつながりにくい状況が発生

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙○のとおり」と記載し別紙を別ファイルで添付の順で対応

（２）重要インフラサービス維持レベルについて（重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要イ[illegible]合に記載すること。該当しない場合は記載を要さない。）

「有」か「無」のどちらかにチェック

・重要インフラサービスのサービス維持レベルの逸脱の有無：　□ 有　☑ 無
・他の事業者等への波及の可能性：　□ 有　☑ 無

・サービス提供への影響、想定される最大リスク　等

（３）事実経過（時系列）

10/5 10：00　外部より入会登録HPに異常な数の申請（1分間に約1000件）が行われていることを検知。
※平時は、1日10件程度
10/5 10：10　総務部とシステム担当部署で情報共有を行い対策を検討
10/5 10：26　一時的に当該HPへのアクセス遮断を実施
10/5 13：30　DDoS攻撃事案共通様式を用いて○○へ第１報を送付
10/5 14：00　HPを復旧
10/10 18：20　外部より入会登録HPに異常な数の申請（1分間に約900件）が行われていることを検知。
10/10 18：30　総務部とシステム担当部署で情報共有を行い対策を検討
10/10 18：30　一時的に当該HPへのアクセス遮断を実施
10/10 20：40　DDoS攻撃事案共通様式を用いて○○へ第2報を送付

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙○のとおり」と記載し別紙を別ファイルで添付の順で対応

３．影響を受けたシステム

・○○株式会社の入会登録ウェブサイト
・システムの稼働状況（停止中）

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙○のとおり」と記載し別紙を別ファイルで添付の順で対応

４．攻撃技術情報（※記入可能な項目を記載してください。また、間隔を空けて別種の攻撃（波）がある場合は、攻撃（波）毎に本項目を作成することも可能。）

（１）観測期間

攻撃開始：　10月　5日　10時　00分
攻撃収束：　10月　5日　10時　10分
特記事項：第2波
攻撃開始：10月10日18時20分
攻撃収束：10月10日18時30分

24時表記で記載。攻撃開始・攻撃収束は第１波を記載。第2波以降について記載する場合は「特記事項」に本項目を追加することも可能

（２）攻撃類型

①分類（複数選択）　（※選択肢は、MITRE ATT&CKのTechnicを参照しています。）

- ☑ ネットワークへのサービス拒否攻撃　Network Denial of Service（T1498）
  ※以下に記載のT1498-001又はT1498-002のいずれに該当するかが不明な場合
- ☐ ネットワークへのフラッド攻撃（UDPフラッド攻撃等）　Direct Network Flood（T1498-001）
- ☐ ネットワークへのリフレクション攻撃（DNSリフレクション攻撃等）　Reflection Amplification（T1498-002）
- ☐ エンドポイントへのサービス拒否攻撃　Endpoint Denial of Service（T1499）
  ※以下に記載のT1499-001からT1499-004までのいずれに該当するかが不明な場合
- ☐ OS枯渇フラッド（TCPステート枯渇攻撃等）　OS Exhaustion Flood（T1499-001）
- ☑ サービス枯渇フラッド（HTTPフラッド攻撃等）　Service Exhaustion Flood（T1499-002）
- ☐ アプリケーション枯渇フラッド　Application Exhaustion Flood（T1499-003）
- ☐ アプリケーション又はシステムの脆弱性悪用によるサービス妨害攻撃 Application or System Exploitation（T1499-004）
- ☐ その他（
- ☐ 不明

複数選択可。該当項目が無い場合は、「その他」にチェックしたうえで、カッコに内容を記載

②詳細

（例：ＤＮＳサーバに対するランダムサブドメイン攻撃、SYN Flood攻撃 等）

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（３）通信プロトコル

（例：TCP/UDP/HTTP 等）

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（４）送信元情報

・送信元のIPアドレス
・送信元のポート番号
・送信元の機器・ボットネットワーク

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（５）送信先情報

・送信先のIPアドレス
・送信先のポート番号
・標的とされている機器・アプリケーション　等

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（６）通信量

（例：10Gbps，1000pps，1万RPS 等）

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

※送信元IPアドレスなど、多数になる場合は別ファイルで御提出ください

５．今後の対応

（１）公表の実施状況

事案の公表：
- ☑ 実
- ☐ 実
- ☐ 検
- ☐ 予

公表の実施状況は、
・事案の公表は、「実施済」、「実施予定」、「検討中」、「予定無し」のいずれか1つのみチェック
・「実施済」欄には初回の公表日を記載。公表が累次にわたる場合でも、初回の公表日を記載し、以後変更する必要はない。
・「実施予定」欄には初回の公表予定日を記載。報告時点で初回の公表が未了である場合、今後の公表予定日を記載（公表予定日が未定の場合は日付は空欄でも構わない）
※公表が累次にわたる場合には、「公表文」枠中に、初回公表文のあとに、2回目以降の公表文及び公表日を追記（「実施済」と「実施予定」に合わせてチェックしない）

（２）今後の予定

- ☐ 事象継続中
- ☑ 対応策を継続中
- ☐ 対応完了

今後の予定は、いずれかの項目をチェック。「事案継続中」とは「続報がある場合」にチェックを入れる。「対応策を検討中」とは「続報が無い」が対応策を検討している場合にチェックを入れる。すべての対応が終了している場合には「対応完了」にチェック

（３）本様式の届出先・報告の根拠規定等

（手引き欄に記載のいずれの法令等に基づく報告かを記載すること。）

６．その他（有効な対策等）

これまでの項目で記載できない内容（特記事項等）があれば記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付、の順で対応すること。スクリーンショット等を貼り付けることも可