改　正　後	改　正　前
サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ 令和７年５月 28 日 関係省庁申合せ 令和７年９月 25 日 一　部　改　正 令和８年　月　日 一　部　改　正	サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ 令和７年５月 28 日 関係省庁申合せ 令和７年９月 25 日 一　部　改　正
１．目的 我が国全体のサイバーセキュリティを強化するためには、官民双方向の情報共有を促すことが必要不可欠である一方、サイバー攻撃による被害報告件数は増加の一途を辿っており、また、報告先となる官公署も多いことから、サイバー攻撃を受けた被害組織に過度な報告負担がかかっている旨の指摘がされている。 特に、ＤＤｏＳ攻撃事案及びランサムウェア事案については、サイバー攻撃であることがインシデント発生時から明白であることが多く、初動対応中の報告となり、その件数も多いことから、被害組織の報告負担が極めて大きいと考えられる。 かかる状況を踏まえ、「サイバー安全保障分野での対処能力の向上に向けた提言」（令和６年 11 月 29 日付、サイバー安全保障分野での対応能力の向上に向けた有識者会議）では、「被害組織の負担軽減と	１．目的 我が国全体のサイバーセキュリティを強化するためには、官民双方向の情報共有を促すことが必要不可欠である一方、サイバー攻撃による被害報告件数は増加の一途を辿っており、また、報告先となる官公署も多いことから、サイバー攻撃を受けた被害組織に過度な報告負担がかかっている旨の指摘がされている。 特に、ＤＤｏＳ攻撃事案及びランサムウェア事案については、サイバー攻撃であることがインシデント発生時から明白であることが多く、初動対応中の報告となり、その件数も多いことから、被害組織の報告負担が極めて大きいと考えられる。 かかる状況を踏まえ、「サイバー安全保障分野での対処能力の向上に向けた提言」（令和６年 11 月 29 日付、サイバー安全保障分野での対応能力の向上に向けた有識者会議）では、「被害組織の負担軽減と

政府の対応迅速化を図るため、報告先や様式の一元化、簡素化を進めるべき」との提言が行われるとともに、サイバーセキュリティ戦略本部第42回会合（令和７年２月５日）では、「現行制度下において喫緊に取り組むべき事項」の検討事項の一つとして、被害組織の負担軽減（報告様式一元化）が掲げられたところである。 　このため、サイバー攻撃に係る被害組織の負担を軽減し、政府の対応迅速化を図るため、報告のあり方について、「ＤＤｏＳ攻撃事案共通様式（別添様式１）」、「ランサムウェア事案共通様式（別添様式２）」及び「その他サイバー攻撃等事案に係る共通様式（別添様式３）」に掲げる共通様式に記載の手続を所管する関係省庁において次のとおり申し合わせる。	政府の対応迅速化を図るため、報告先や様式の一元化、簡素化を進めるべき」との提言が行われるとともに、サイバーセキュリティ戦略本部第　42　回会合（令和７年２月５日）では、「現行制度下において喫緊に取り組むべき事項」の検討事項の一つとして、被害組織の負担軽減（報告様式一元化）が掲げられたところである。 　このため、サイバー攻撃に係る被害組織の負担を軽減し、政府の対応迅速化を図るため、報告のあり方について、別添様式１及び別添様式２に掲げる共通様式に記載の手続を所管する関係省庁において次のとおり申し合わせる。
２．対象とする手続 　重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号。以下「サイバー対処能力強化法」という。）第５条の規定による特定侵害事象等の報告等、個人情報の保護に関する法律（平成 15 年法律第 57 号）第 26 条第１項の規定による個人データの漏えい等に係る報告等、都道府県警察への相談その他の共通様式に記載の手続に関する官公署への報告等に際して、被害組織が①ＤＤｏＳ攻撃事案に該当する事象については別添様式１、②ランサムウェア事案に該当する事象については別添様式２、①②の事象以外の事象については別添様式３を用い、又は別途法令等で定める様式に添付する形で報告等を行うことを可能とする。具体的な提出先及び提出方法については、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とする。 　その際、内閣官房国家サイバー統括室において国内で発生している	２．対象とする手続

これら事案の情報集約を行うため、被害報告を行う者の同意がある場合は、各様式に基づいて報告を受けた官公署は、当該内容を内閣官房国家サイバー統括室に共有するものとする。 　また、サイバー対処能力強化法の施行に併せ、官民連携基盤の整備により報告の窓口を一元化するとともに、共通様式による報告の受理を可能とする。 　さらに、サイバー対処能力強化法の対象以外の被害組織についても官民連携基盤等の整備により報告先が一元化されるよう所要の調整を進める。	
［（１）・（２）を削る。］	（１）ＤＤｏＳ攻撃事案・ランサムウェア事案に係る報告 　先行的な対応として、個人情報の保護に関する法律（平成 15 年法律第 57 号）第 26 条第１項の規定による個人データの漏えい等に係る報告等、都道府県警察への相談その他の共通様式に記載の手続に関する官公署への報告等に際して、被害組織が「ＤＤｏＳ攻撃事案共通様式（別添様式１）」又は「ランサムウェア事案共通様式（別添様式２）」を用い、又は別途法令等で定める様式に添付する形で報告等を行うことを可能とする。具体的な提出先及び提出方法については、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とする。 　その際、内閣官房国家サイバー統括室において国内で発生しているこれら事案の情報集約を行うため、被害報告を行う者の同意がある場合は、各様式に基づいて報告を受けた官公署は、当該内容を内閣官房国家サイバー統括室に共有するものとする。 　また、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号。以下「サイバー対処能力強化法」という。）第５条の施行に併せ、官民連携基盤の整備により、共通様式に

	より報告が行われる場合における窓口を一元化するよう所要の調整を進める。 （２）サイバー対処能力強化法に基づく報告 特別社会基盤事業者は、特定侵害事象等の発生を認知した場合、サイバー対処能力強化法第５条の規定に基づき、特別社会基盤事業所管大臣及び内閣総理大臣に報告しなければならないとされているところ、当該規定に基づく報告及び（１）に掲げる報告等について、当該規定の施行に併せ、官公署への報告等に際して利用できる共通様式を整備し、さらに官民連携基盤の整備により、これらの報告の窓口を一元化するよう所要の調整を進める。
３．本申合せの適用開始時期及び見直し 本申合せのうち、別添様式１又は別添様式２を用いた報告等については、所要の制度改正やパブリックコメント等を経て、令和７年 10 月１日から適用する。 また、別添様式３を用いた報告等については、所要の制度改正やパブリックコメント等を経て、令和８年 10 月１日から適用する。 なお、本申合せは、各省庁等の適用状況や、サイバー攻撃の傾向を随時検証し、不断の見直しを行う。	３．本申合せの適用開始時期及び見直し 本申合せのうち、「ＤＤｏＳ攻撃事案共通様式（別添様式１）」又は「ランサムウェア事案共通様式（別添様式２）」を用いた報告等については、所要の制度改正やパブリックコメント等を経て、令和７年 10 月１日から適用する。 また、本申合せは、各省庁等の適用状況や、サイバー攻撃の傾向を随時検証し、２（１）に定める様式の適用開始から１年後を目途に必要な見直しを行う。

（別添様式１）ＤＤｏＳ攻撃事案共通様式

DDoS攻撃事案共通様式

年　月　日
時　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
□ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

□ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　　報
（２）速報/続報/詳報の別：　□ 速報(新規)　□ 続報　□ 詳報(確報)
（前回報告：　　年　月　日　時　分）
（受付番号※：　　）
※個人情報保護委員会より通知されている場合

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、その旨及び共有等を希望しない内容について以下に記載してください。

□　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：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。
（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等
報告根拠に記載する法令、ガイドライン等（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の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、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。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、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についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
報告をしようとする時点で把握している範囲で、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。

（別添様式１）ＤＤｏＳ攻撃事案共通様式

DDoS攻撃事案共通様式

年　月　日
時　分

（報告先機関の長）殿

新規又は続報の別：□ 新規　□ 続報（前回報告：　年　月　日　時　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、その旨及び共有等を希望しない内容について以下に記載してください。

□ 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：

（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。
○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
○警察への相談
○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．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）
法人番号（13桁）	
業種・業種番号	
報告者の住所 又は居所	〒 －
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする） 所属部署　　電話番号 E-mail

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（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）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・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

（３）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

※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）
法人番号（13桁）	
事務連絡者の氏名	（フリガナ） 所属部署　　電話番号 E-mail

２．業務への影響

（１）事案の概要

（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）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・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

（３）事実経過（時系列）

３．影響を受けたシステム

４．事案に関する技術的な事項（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

攻撃発生：	月	日	時	分
攻撃収束：	月	日	時	分
特記事項：				

（２）攻撃類型

①分類（複数選択）（※選択肢は、MITRE ATT&CKのTechniques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

②詳細

（３）通信プロトコル

（４）送信元情報

（５）送信先情報

（６）通信量

※送信元IPアドレスなど、記載内容が多数になる場合は別ファイルで御提出ください。

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：	月	日	時	分
攻撃収束：	月	日	時	分
特記事項：				

（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

②詳細

（３）通信プロトコル

（４）送信元情報

（５）送信先情報

（６）通信量

※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．事案への対応に関する事項

（１）公表の実施状況

事案の公表：　□　実施済　　【公表日：　　年　　月　　日】

公表URL：

□　実施予定　　【公表予定日：　　年　　月　　日】

□　検討中

□　予定無し

公表の方法：　□　ホームページに掲載

□　記者会見

□　報道機関等への資料配付

□　その他：　（　　）

公表文：

（２）今後の予定

□　事象継続中

□　対応策を継続中

□　対応完了

（３）外部機関による調査の実施状況

□　実施済又は実施中

□　実施予定

□　検討中

□　予定なし

（詳細：　　）

６．その他特記事項

５．今後の対応

（１）公表の実施状況

事案の公表：　□　実施済　　【公表日：　　年　　月　　日】

□　実施予定　　【公表予定日：　　年　　月　　日】

□　検討中

□　予定無し

（２）今後の予定

□　事象継続中

□　対応策を継続中

□　対応完了

（３）本様式の届出先・報告の根拠規定等

６．その他（有効な対策等）

ランサムウェア事案共通様式

年　月　日
時　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
□ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

□ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　　報
（２）速報/続報/詳報の別：　□ 速報(新規)　□ 続報　□ 詳報(確報)
（前回報告：　　年　月　日　時　分）
（受付番号※：　　）
※個人情報保護委員会より通知されている場合

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、その旨及び共有等を希望しない内容について以下に記載してください。

□　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：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。
（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、別紙１から別紙３までの内容を除き、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等
報告根拠に記載する法令、ガイドライン等（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の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、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。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、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についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
①共通
報告をしようとする時点で把握している範囲で、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。
②個人情報の保護に関する法律第26条第１項の規定による漏えい等報告を行う場合
別紙１も記載してください。
③個人情報の保護に関する法律第68条第１項の規定による漏えい等報告を行う場合
別紙２も記載してください。
④行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告を行う場合
別紙３も記載してください。

２．ランサムウェア感染時の留意事項
被害拡大防止、原因究明・再感染防止のため、初期対応時において、感染端末に対して以下の対応の御検討をお願いします。感染経路が分からなくなると、復旧に支障が生じる場合があります。
・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

（別添様式２）ランサムウェア事案共通様式

ランサムウェア事案共通様式

年　月　日
時　分

（報告先機関の長）殿

新規又は続報の別：□ 新規　□ 続報（前回報告：　年　月　日　時　分）
（受付番号※：　）
※個人情報保護委員会より通知されている場合

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、その旨及び共有等を希望しない内容について以下に記載してください。

□ 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：

（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、別紙１から別紙３までの内容を除き、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、ランサムウェアにより生じ、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。
○個人情報の保護に関する法律第26条第１項の規定による漏えい等報告
○個人情報の保護に関する法律第68条第１項の規定による漏えい等報告
○行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告
○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
○警察への相談
○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共通
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。
②個人情報の保護に関する法律第26条第１項の規定による漏えい等報告を行う場合
別紙１も記載してください。
③個人情報の保護に関する法律第68条第１項の規定による漏えい等報告を行う場合
別紙２も記載してください。
④行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告を行う場合
別紙３も記載してください。

２．ランサムウェア感染時の留意事項
被害拡大防止、原因究明・再感染防止のため、初期対応時において、感染端末に対して以下の対応の御検討をお願いします。感染経路が分からなくなると、復旧に支障が生じる場合があります。
・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）
法人番号（13桁）	
業種・業種番号	
報告者の住所 又は居所	〒 －
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする） 所属部署　　電話番号 E-mail

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（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）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・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

（３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

□　別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

□　別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

□　別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

※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）
法人番号（13桁）	
業種・業種番号	
報告者の住所 又は居所	
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ）
事務連絡者の氏名	（フリガナ） 所属部署　　電話番号 E-mail

２．業務への影響

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（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）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・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

（３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

□　別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

□　別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

□　別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

３．影響を受けたシステム

4．事案に関する技術的な事項（攻撃技術情報）
（※報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。）
（1）ランサムノート（身代金を要求する文言等）

（2）暗号化されたファイルの拡張子

（3）ランサムウェアの類型

（4）攻撃の手口・侵入経路・攻撃の時系列

※システム構成が分かる図やフォレンジック結果報告書を提出する場合は別ファイルとしてください。

（5）ランサムウェアの特徴（インディケータ情報）

※IPアドレスやログ情報など、記載内容が多数になる場合は別ファイルで御提出ください。

（6）悪用された脆弱性

・製品開発者への報告の有無：　□ 有　□ 無

5．事案への対応に関する事項
（1）公表の実施状況
事案の公表：　□ 実施済　【公表日：　年　月　日】
公表URL：
□ 実施予定　【公表予定日：　年　月　日】
□ 検討中
□ 予定無し
公表の方法：　□ ホームページに掲載
□ 記者会見
□ 報道機関等への資料配付
□ その他：　（　）
公表文：

（2）今後の予定
□ 事象継続中
□ 対応策を継続中
□ 対応完了

（3）外部機関による調査の実施状況
□ 実施済又は実施中
□ 実施予定
□ 検討中
□ 予定なし
（詳細：　）

6．その他（特記事項等）

4．攻撃技術情報（※記入可能な項目を記載してください。）
（1）ランサムノート（身代金を要求する文言等）

（2）暗号化されたファイルの拡張子

（3）ランサムウェアの類型

（4）侵入方法

（5）ランサムウェアの特徴（インディケータ情報）

5．今後の対応
（1）公表の実施状況
事案の公表：　□ 実施済　【公表日：　年　月　日】
□ 実施予定　【公表予定日：　年　月　日】
□ 検討中
□ 予定無し
公表の方法：　□ ホームページに掲載
□ 記者会見
□ 報道機関等への資料配付
□ その他：　（　）
公表文：

（2）今後の予定
□ 事象継続中
□ 対応策を継続中
□ 対応完了

（3）外部機関による調査の実施状況
□ 実施済又は実施中
□ 実施予定
□ 検討中
□ 予定なし
（詳細：　）

（4）本様式の届出先・報告の根拠規定等

6．その他（特記事項等）

［別紙１～３　略］	［別紙１～３　同左］

（別添様式３）その他サイバー攻撃等事案共通様式（不正アクセス、情報窃取等）

その他サイバー攻撃等事案共通様式
（不正アクセス、情報窃取等）

年　月　日
時　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
□ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

□ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　報
（２）速報/続報/詳報の別：　□ 速報（新規）　□ 続報　□ 詳報（確報）
（前回報告：　年　月　日　時　分）
（受付番号※：　）
※個人情報保護委員会より通知されている場合

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、その旨及び共有等を希望しない内容について以下に記載してください。

□　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：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。
（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、別紙１から別紙３までの内容を除き、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等
報告根拠に記載する法令、ガイドライン等（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の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、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。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、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についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
①共通
報告をしようとする時点で把握している範囲で、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。
②個人情報の保護に関する法律第26条第１項の規定による漏えい等報告を行う場合
別紙１も記載してください。
③個人情報の保護に関する法律第68条第１項の規定による漏えい等報告を行う場合
別紙２も記載してください。
④行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告を行う場合
別紙３も記載してください。
※②から④までの報告を行う場合においては、サイバー攻撃事案に伴う漏えい等事案に伴う報告であることに留意する。（ただし、所管省庁から別途要請等があった場合はこの限りでない。）

２．マルウェア感染時の留意事項
被害拡大防止、原因究明・再感染防止のため、初期対応時において、感染端末に対して以下の対応の御検討をお願いします。感染経路が分からなくなると、復旧に支障が生じる場合があります。
・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

［別添様式を加える。］

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）
法人番号（13桁）	
業種・業種番号	
報告者の住所 又は居所	〒　－
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする） 所属部署　　電話番号 E-mail

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（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）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・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

（３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

□　別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

□　別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

□　別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

4．事案に関する技術的な事項（攻撃技術情報）
（※報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。）

（1）攻撃の手口・侵入経路・攻撃の時系列

※システム構成が分かる図やフォレンジック結果報告書を提出する場合は別ファイルとしてください。

（2）サイバー攻撃等の類型

（3）サイバー攻撃等の特徴（インディケータ情報）

※IPアドレスやログ情報など、記載内容が多数になる場合は別ファイルで御提出ください。

（4）悪用された脆弱性

・製品開発者への報告の有無：　☐ 有　☐ 無

5．事案への対応に関する事項

（1）公表の実施状況

事案の公表：　☐ 実施済　【公表日：　年　月　日】
公表URL：
☐ 実施予定　【公表予定日：　年　月　日】
☐ 検討中
☐ 予定無し

公表の方法：　☐ ホームページに掲載
☐ 記者会見
☐ 報道機関等への資料配付
☐ その他：　（　）

公表文：

（2）今後の予定

☐ 事象継続中
☐ 対応策を継続中
☐ 対応完了

（3）外部機関による調査の実施状況

☐ 実施済又は実施中
☐ 実施予定
☐ 検討中
☐ 予定なし
（詳細：　）

6．その他（特記事項等）

別紙1（個人情報取扱事業者における個人データ等の漏えい等報告）
【民間事業者・個人情報の保護に関する法律第58条第1項各号に掲げる法人等（いわゆる規律移行法人）の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（1）報告の種別
速報又は確報の別：　□ 速報　□ 中間報　□ 確報

（2）事態の概要
発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ
発見者：　□ 自社/委託先　□ 取引先　□ 顧客/会員
□ カード会社/決済代行会社　□ その他（　　）
規則第７条各号該当性：　□ 第１号（要配慮個人情報）
□ 第２号（財産的被害）
□ 第３号（不正の目的）
□ 第４号（千人超）
□ 非該当（上記に該当しない場合の報告）
報告者に個人データの取扱いを委託した者（委託元）の有無：
□ 有（名称：　　）
（住所：　　）
（電話：　　）
□ 無
報告者から個人データの取扱いの委託を受けた者（委託先）の有無
□ 有（名称：　　）
（住所：　　）
（電話：　　）
□ 無

（3）漏えい等が発生し、又は発生したおそれがある個人データの項目（該当する□に印を付けること。）
媒体：　□ 紙　□ 電子媒体　□ その他（　　）
種類：　□ 顧客情報　□ 従業員情報　□ その他（　　）
項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ クレジットカード情報　□ パスワード
□ その他（　　）

（4）漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明
人数：（　　）人　うちクレジットカード情報含む（　　）人

（5）発生原因（該当する□に印を付けること。）
主体：　□ 報告者　□ 委託先　□ 不明
原因：　□ 不正アクセス
（攻撃箇所：（　　））
（攻撃手法：（　　））
詳細：

（6）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□ 有　□ 無　□ 不明

詳細：

（7）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□ 対応済（対応中）　□ 対応予定

□ 予定なし

詳細（予定なしの場合は、理由を記載）：

（8）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（9）その他参考となる事項

別紙2（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（1）報告の種別

速報又は確報の別：　□ 速報　□ 中間報　□ 確報

報告者の組織区分：　□ 行政機関等　□ 地方公共団体等

（2）事態の概要

発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ

発見者：　□ 自組織/委託先　□ 取引先
□ 取引先以外の外部指摘（国民等からの指摘）
□ カード会社/決済代行会社　□ その他　（　　）

規則第43条各号該当性：　□ 第１号（要配慮個人情報）
□ 第２号（財産的被害）
□ 第３号（不正の目的）
□ 第４号（百人超）
□ 第５号（条例要配慮個人情報）
□ 非該当（上記に該当しない場合の報告）

報告者に保有個人情報の取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

報告者から保有個人情報の取扱いの委託を受けた者（委託先）の有無

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

（3）漏えい等が発生し、又は発生したおそれがある保有個人情報の項目（該当する□に印を付けること。）

媒体：　□ 紙　□ 電子媒体　□ その他（　　）
種類：　□ 国民等　□ 職員　□ その他（　　）
項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ クレジットカード情報　□ パスワード
□ その他（　　）

（4）漏えい等が発生し、又は発生したおそれがある保有個人情報に係る本人の数

状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明
人数：（　　）人　うちクレジットカード情報含む（　　）人

（5）発生原因（該当する□に印を付けること。）

主体：　□ 報告者　□ 委託先　□ 不明
原因：　□ 不正アクセス
（攻撃箇所：（　　））
（攻撃手法：（　　））
詳細：

（6）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□ 有　□ 無　□ 不明
詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定
□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

別紙3（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（1）報告の種別

速報又は確報の別：　□ 速報　□ 中間報　□ 確報

報告者の組織区分：　□ 行政機関　□ 独立行政法人等　□ 地方公共団体等　□ 事業者

（2）事態の概要

事務の内容：　□ 個人番号利用事務　□ 個人番号関係事務　□ その他

事務の名称：　（　　）

特定個人情報保護評価の実施の有無：　□ 実施（義務）　□ 実施（任意）　□ 実施していない

評価の種類：　□ 基礎項目評価　□ 重点項目評価　□ 全項目評価

発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ
□ 法第９条違反　□ 法第９条違反のおそれ
□ 法第19条違反　□ 法第19条違反のおそれ
□ その他　（　　）

発見者：　□ 報告者　□ 委託者
□ その他　（　　）

規則第２条各号該当性：　□ 第１号（情報提供ネットワークシステム等）
□ 第２号（不正の目的）
□ 第３号（不特定多数の者に閲覧）
□ 第４号（百人超）
□ 非該当（上記に該当しない場合の報告）

報告者に特定個人情報の取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

報告者から特定個人情報の取扱いの委託を受けた者（委託先）の有無

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

（3）特定個人情報の項目（該当する□に印を付けること。）

媒体：　□ 紙　□ 電子媒体　□ その他（　　）

種類：　□ 顧客情報　□ 住民情報　□ 従業員情報
□ その他（　　）

項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ パスワード　□ その他（　　）

（4）特定個人情報に係る本人の数

状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明

人数：（　　）人

（5）発生原因（該当する□に印を付けること。）

主体：　□ 報告者　□ 委託先　□ 不明

原因：　□ 不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

詳細：

（6）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□ 有　□ 無　□ 不明

詳細：

（7）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□ 対応済（対応中）　□ 対応予定　□ 予定なし

詳細（予定なしの場合は、理由を記載）：

（8）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（9）その他参考となる事項