弁護士法人　三宅法律事務所

Miyake　& Partners

Miyake newsletter

個人情報保護法ニュースＮｏ.13

サイバー攻撃事案報告制度の最前線 ― DDoS・ランサム対応と強化法による窓口一元化

平素より大変お世話になっております。

さて、今回は個人情報保護法ニュース**「サイバー攻撃事案報告制度の最前線 ～DDoS・ランサム対応と強化法による窓口一元化～」**をご案内させていただきます。

令和７年 10 月３日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士渡邉雅之、弁護士越田晃基、弁護士岩田憲二郎、弁護士出沼成真（執筆者）
TEL 03-5288-1021 FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

サイバー攻撃事案報告制度の最前線
～DDoS・ランサム対応と強化法による窓口一元化～

Ⅰ. 序論

近年、分散型サービス妨害（DDoS）攻撃やランサムウェア攻撃が急増し、社会インフラの停止や個人情報の漏えいなど、深刻な被害が相次いでいる。被害組織は、DDoS 攻撃やランサムウェア攻撃への初動対応（応急措置に加え、セキュリティベンダーへの連絡など外部事業者との連携等を含む。）に追われることとなる。そのような中で、被害企業は、さらに個人情報保護法（「**個情法**」）第 26 条に基づく個人情報保護委員会への報告[1]に加え、所管省庁や警察等にも重複して報告を求められる状況にあり、報告負担が過大となっていた。

こうした問題意識のもと、令和 7 年 5 月 28 日に関係省庁申合せ[2]が制定され、同年 9 月 25 日には個人情報保護委員会による規則改正[3]および告示改正[4]が行われた（いずれも令和 7 年 10 月 1 日施行）。

その結果、DDoS 攻撃事案共通様式（別添様式1）およびランサムウェア事案共通様式（別添様式2）が新たに導入され、令和 7 年 10 月 1 日から適用が開始された。これらの共通様式は、「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 5 月 23 日法律第 42 号、「**サイバー対処能力強化法**」）の報告義務の施行に伴う報告窓口一元化への橋渡しとして重要な役割を果たすことになる。

---

[1] 特にランサムウェア攻撃の場合、システム暗号化や情報窃取が行われることが通例であるから、ほとんどの事例において、個情法 26 条に基づく報告を要すると考えられる。一方で、DDoS 攻撃の場合は、必ずしも個人データの漏えい等に直結するものではないため、個人情報保護委員会（PPC）への報告要否は個別的な検討を要する。

[2] 「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」（以下「**関係省庁申し合わせ**」）（https://www.nisc.go.jp/pdf/policy/infra/ref_moushiawase0925.pdf）

[3] 個人情報の保護に関する法律施行規則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第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則の一部を改正する規則（令和 7 年個人情報保護委員会規則第 2 号、以下「**規則改正**」）

[4] 個人情報の保護に関する法律施行規則第八条第三項第一号及び第二号並びに第四十四条第三項並びに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二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則第三条第三項に規定する個人情報保護委員会が別に定める場合及びその方法を定める件（令和 7 年個人情報保護委員会告示第 12 号、以下「**告示改正**」）

Ⅱ. 関係省庁申合せと別紙様式の策定

1. 制定の経緯

サイバー攻撃の被害報告件数の増加と報告先の分散により、被害組織への負担が過度に大きくなっていた。

特に DDoS 攻撃事案・ランサムウェア事案では「発生直後から攻撃と判明」するケースが多く、被害企業としては、これら事案に対する初動対応の最中に、各種法令・ガイドライン等に基づく監督官庁への報告、（特にランサムウェア事案では）個人情報保護委員会への報告、警察への相談などの当局対応が集中することとなり、負担が突出していた。

有識者会議提言（令和 6 年 11 月）や戦略本部決定（令和 7 年 2 月）において、**報告先・様式の一元化**が明示的に課題とされた。

2. 別紙様式の策定

内閣官房国家サイバー統括室（NISC）は、「被害報告一元化に関する DDoS 事案及びランサムウェア事案報告様式」として、「別添様式１（DDoS 攻撃事案共通様式）」および「別添様式２（ランサムウェア事案共通様式）」を策定した[5]。

被害組織は、これら様式を単独で使用するか、既存の報告様式に添付して提出することが可能となる[6]。

また、報告者が同意すれば、受理した官庁から内閣官房国家サイバー統括室（NISC）へ情報が共有される仕組みも整備された。適用開始は令和 7 年 10 月 1 日とされ、導入後 1 年を目途に見直しが行われることになっている。

Ⅲ. 個情法規則改正・告示改正

令和 7 年 9 月 25 日に公布された規則改正・告示改正は、個人情報保護法第 26 条第 1 項（民間報告）及び第 68 条第 1 項（行政機関等報告）、並びに番号法[7]第 29 条の 4 第 1 項（マイナンバーを含む報告）に基づき、個人情報保護委員会への報告方法を見直したものである。

---

[5] 「「被害報告一元化に関する DDoS 事案及びランサムウェア事案報告様式」（案）に関する意見の募集について」（https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&id=060250710&Mode=0）

[6] 本文のとおり、関係官庁申し合わせでは、既存の報告様式に添付する形での報告も可能とするが、この場合、却って被害企業の負担が増加するように思われる。関係官庁における共通様式の適切かつ制定趣旨に沿った運用に期待したい。

[7] 正式名称は「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」

具体的には、関係省庁申合せ２.（１）に規定するランサムウェア事案に係る報告を行う場合、現行の規定に基づき電子情報処理組織を使用する方法等に加え、関係省庁申合せ別添様式２を提出する方法が正式に認められた。

さらに、事業所管大臣への報告方法についても同様の見直しが行われた。すなわち、施行規則別記様式第１による報告書提出に加えて、関係省庁申合せ別添様式２を提出する方法が利用できるよう制度整備された。

この改正により、ランサムウェア事案に関しては、事業者は従来の個情法に基づく報告方式を利用することも可能であるが、個人情報保護委員会（PPC）のみならず他の所管省庁への報告をも要する場合には、共通様式（別添様式２）を用いることで、個人情報保護委員会（PPC）および所管省庁双方に対応できる仕組みが明確化された。これにより、二重提出の解消と、共通様式を通じた横断的な情報共有の促進が可能となったのである。

Ⅳ. 個情法との関係

DDoS 攻撃事案（別添様式１）は、外部からの大量通信によりサービス提供を妨害するものである。したがって、サービス停止のみで個人データの漏えいが生じない場合には個情法第 26 条の報告義務は生じない。ただし、共通様式を用いて所管庁や警察に報告することは可能である。

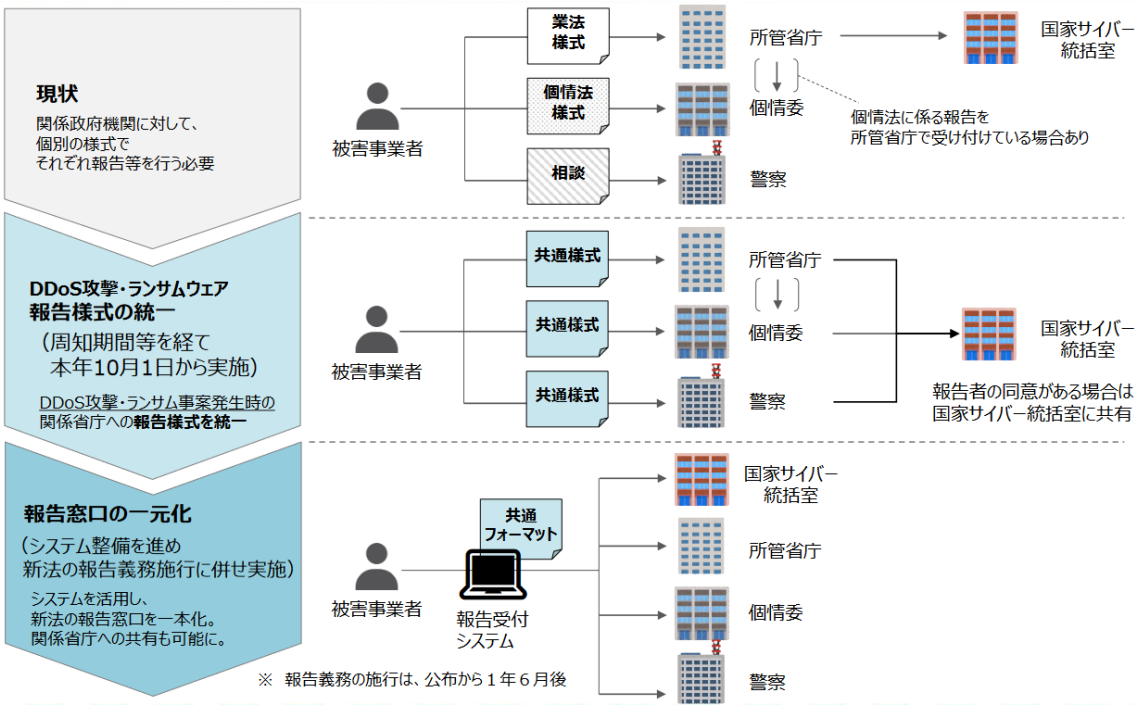
これに対して、ランサムウェア攻撃事案（別添様式２）は、暗号化や窃取、公開脅迫を伴う場合が多く、個人データの漏えいや毀損につながる可能性が極めて高いため、個情法報告義務との関連が最も強く、別添様式２の利用が実務上重要となる。

Ⅴ. サイバー対処能力強化法との接続

サイバー対処能力強化法（令和 7 年法律第 42 号）は、能動的サイバー防御（Active Cyber Defense）の法的基盤を整えるものであり、重要電子計算機の届出義務、通信付随情報の収集・分析、攻撃サーバに対する無害化措置権限、独立監視機関によるガバナンスといった要素を包含する。

特に第５条の施行に併せて、報告窓口の一元化が制度化されることが予定されている。将来的には、一本化されたシステムを通じて報告が提出され、内閣官房国家サイバー統括室（NISC）・個人情報保護委員会（PPC）・所管庁に共通フォーマットで自動的に共有される仕組みが整備される。これは現行の「同意があれば内閣官房国家サイバー統括室（NISC）に共有」という限定的運用から一歩進み、国家レベルでの迅速な情報集約を可能にする。施行時期は公布から 1 年 6 か月以内（2026 年 11 月頃まで）とされており、共通様式はこの移行に向けた暫定的かつ実務的な橋渡しとして機能する。

○被害報告一元化の実現に向けたタイムライン



出所：サイバーセキュリティ戦略本部（令和７年５月 29 日第 43 回会合資料 5－1）

Ⅵ. 通常漏えい報告様式とランサムウェア事案共通様式（別添様式２）の比較[8]

通常漏えい報告様式とランサムウェア事案共通様式（別添様式２）の違いは以下のように整理できる。

まず、報告の目的において、通常漏えい報告様式は件数や影響範囲の把握を重視し、個人の権利利益侵害のおそれを評価することを中心にしている。一方で、ランサムウェア事案共通様式は、攻撃手口、システムへの影響、事業継続への影響を含め、国家的な対応体制の基盤となる情報を集約することを目的としている。

[8] 以下は、「個人情報の保護に関する法律施行規則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第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則の一部を改正する規則（案）等に関する意見募集の結果について」（https://public-comment.e-gov.go.jp/pcm/1040?CLASSNAME=PCM1040&id=240000116&Mode=1）における意見・回答も参考としている。

技術的報告項目の範囲も大きく異なる。通常様式は原因分類（誤送信、紛失、不正アクセスなど）にとどまるのに対し、ランサムウェア事案共通様式では、侵入経路、マルウェアの名称・亜種情報、IOC（侵入兆候としての不審 IP やハッシュ値）、攻撃者からの要求内容（身代金額や二重恐喝の有無）、さらにはログ保全やデジタルフォレンジック対応状況まで詳細に記載が求められる。

業務影響の評価でも、通常様式は対象件数や個人属性に重点を置くが、ランサム様式ではシステム停止範囲、停止期間と復旧見込み、代替手段、BCP（事業継続計画）の発動有無まで問われ、被害が事業運営や社会的機能に与える影響を包括的に捉えることが可能となっている。

外部対応の項目も、通常様式では本人通知や公表の有無にとどまるのに対し、ランサムウェア事案共通様式では警察への通報・被害届提出、所管庁や内閣官房国家サイバー統括室（NISC）への報告、セキュリティベンダーや弁護士への依頼、さらには攻撃者との交渉状況まで含まれる。これにより、攻撃後の多面的な対応が制度的に可視化される。

提出運用についても差異があり、通常様式は速報と確報が中心であり、不明点の記載は限定的である。他方、ランサムウェア事案共通様式は速報、中間報告、確報の三段階で提出が求められ、不明点については「調査中」と明記することが認められる。これにより、初動段階からの迅速な報告と継続的な情報更新が可能となっている。

個人情報保護委員会は、ランサムウェア事案に関する「統一様式」をエクセルで公表しており、こちらを実務上は利用することになる[9]。

Ⅶ. 制度の意義

今回の制度改正と共通様式導入の意義は多岐にわたる。第一に、関係省庁申合せと規則・告示改正を通じて、これまで分散していた報告窓口が整理され、事業者の負担が大幅に軽減される点である。特に、従来は個情法報告、所管庁報告、警察相談が並行して求められていたが、今後は共通様式の活用により、同一内容を複数回記載する必要がなくなる。

第二に、個情法を中核としつつ、DDoS やランサムといった新たなサイバー脅威への対応が包括的に可能となる点である。通常漏えい様式では把握できなかった攻撃態様や業務継続への影響を、共通様式が補完することで、国家レベルのインシデント対応が強化される。

第三に、令和 7 年 10 月 1 日からの適用開始によって、即時に運用効果が発揮されると同時に、将来的なサイバー対処能力強化法の施行に向けた実務的準備段階としての意味を持つ点である。特に第 5 条に基づく報告窓口一元化制度への移行を円滑にする「橋渡し」として位置づけられる。

[9] https://www.ppc.go.jp/personalinfo/legal/leakAction/#cloud

第四に、政府横断的な情報集約が可能となることで、単に事業者の報告義務を履行させるにとどまらず、国家的なサイバーセキュリティ戦略の基盤として機能する点である。共通様式を通じて収集された技術的データや業務影響情報は、攻撃トレンドの分析、早期警戒、他組織への注意喚起などに直結する。これにより、個別事業者の被害対応に加えて、社会全体の防御力が強化される。

Ⅷ. 結論

令和 7 年 9 月 25 日の規則改正・告示改正は、関係省庁申合せを背景として、DDoS 攻撃共通様式（別添様式１）とランサムウェア事案共通様式（別添様式２）を導入し、令和 7 年 10 月 1 日から適用を開始した。特にランサムウェア事案共通様式は通常漏えい報告様式との差異を通じて、攻撃態様、業務継続リスク、外部対応の全体像を包括的に把握することを可能にした点で大きな意義を有する。さらに、これらの共通様式は、2026 年 11 月頃までに施行されるサイバー対処能力強化法による窓口一元化への橋渡しとして位置づけられ、国家レベルでの迅速な情報集約と対処力の強化を実現する重要な制度的基盤となる。

（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理由:

（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。

〇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

〇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

〇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

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。

★様式本体

※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

・サービス提供への影響、想定される最大リスク　等

（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

・影響を受けた機器の種類・台数　等 ・システムの稼働状況（影響無し/停止中/一部稼働中/復旧済） ・設置環境 ・システムの接続形態図

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）

・（スクリーンショットその他表示された内容がわかるものでも可）

（2）暗号化されたファイルの拡張子

・（ファイル名.xxx）

（3）ランサムウェアの類型

・暗号化の有無/リークサイトや SNS 等を通じた情報漏えいが行われた旨の公開の有無/身代金要求の有無

（4）侵入方法

・脆弱性の悪用/フィッシングメール

（5）ランサムウェアの特徴（インディケータ情報）

・マルウェア情報/通信先の IP アドレス等/判明した事案に係るログ情報等

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布
□ 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

（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（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：　☐　自宅/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を委託を受けた者（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　☐　授業員情報　　☐　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　　□ 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）　略

別紙３（特定個人情報）　略