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）

参考資料２－２

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。