

参考資料 1 - 3

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、内閣サイバーセキュリティセンターに共有されます。内閣サイバーセキュリティセンターは、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、内閣サイバーセキュリティセンター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。

☐ 内閣サイバーセキュリティセンター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、内閣サイバーセキュリティセンター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の下線を引くなど、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お願い

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 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

--

(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 (個人情報の保護に関する法律第26条第1項により報告する場合) 【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 (同法第68条第1項により報告する場合) 【行政機関等の方】
- ☐ 別紙3 (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項により報告する場合) 【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

（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の漏えい等に係る項目

※ 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(該当する口に印を付けること。)

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(該当する口に印を付けること。)

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(該当する口に印を付けること。)

有無: ☐ 有 ☐ 無 ☐ 不明

詳細:

(7) 本人への対応の実施状況(該当する口に印を付けること。)

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に係る項目

※ 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（該当する口に印を付けること。）

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に係る項目

※ 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 ☐ 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（該当する口に印を付けること。）

有無： ☐ 有 ☐ 無 ☐ 不明

詳細：

--

(7) 本人への対応の実施状況（該当する口に印を付けること。）

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

--