資料2-1

第2回　サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会

サイバーセキュリティインシデント発生時の報告制度等

森・濱田松本法律事務所
弁護士　　蔦　大輔

2022年6月20日

森・濱田松本法律事務所
MORI HAMADA & MATSUMOTO

サマリー

大まかには以下の４つの類型に分類できる

１．法的拘束力のある義務

（１）法令に基づく義務　（２）契約・約款上の義務

２．サイバー犯罪被害者としての対応

３．ガイドライン等に基づく推奨事項（法的拘束力なし）

（１）ガイドライン等に基づく推奨事項　（２）その他の推奨事項

４．その他任意の対応

１．法的拘束力のある義務

■ （１）法令に基づく義務

個人データの漏えい・滅失・毀損（漏えい等）に対する報告義務	一定の要件を満たす(報告対象事態)個人データの漏えい等について個人情報保護委員会等への報告義務（個人情報保護法26条） ※1 公表は「望ましい措置」、ただし本人通知の代替措置に注意 ※2 分野別の規定に留意 例）銀行法施行規則13条の6の5の2
特定個人情報の漏えい等に対する報告義務	一定の要件を満たす特定個人情報（マイナンバーを含む個人情報）の漏えい等について個人情報保護委員会への報告義務（番号利用法29条の4）
業法に基づく事故報告義務	各業法に基づく事故（サイバーセキュリティインシデントを含む）発生時の所管省庁等への報告義務 例）電気通信事業法28条（通信の秘密の漏えい・重大事故）
報告等の求めへの対応義務	➢ 当局から法令に基づく報告等の求めがあった場合、原則として対応する義務あり（情報提供・資料提出の求め等） 例）サイバーセキュリティ基本法17条3項 ➢ 報告徴収をベースとした事故報告義務 例）電気通信事業報告規則7条の3（事故の四半期報告）

１．法的拘束力のある義務

■ （２）契約・約款上の義務

上場会社の適時開示	上場会社（またはその子会社等）においてサイバーセキュリティインシデントが発生し、それが投資判断に著しい影響を及ぼす場合、適時開示が必要（有価証券上場規程（東京証券取引所）402条2項x、403条2項l）
認定個人情報保護団体対象事業者	認定個人情報保護団体（個人情報保護法54条）の対象事業者は、認定団体が定める指針に基づき、認定団体に個人情報の取り扱いに関する事故報告が求められる場合がある 例）JIPDEC個人情報保護指針　※ 負担軽減の措置あり
プライバシーマーク付与事業者	プライバシーマーク付与事業者は、個人情報に関する事故等の発生時に関係審査機関に報告しなければならない（プライバシーマーク付与に関する規約12条）　※負担軽減の措置あり ※「事故等」の範囲は個人データの漏えい等以外も含む
その他契約に基づく義務	➢ NDA、委託契約、データ取引契約等において、事故発生時等に契約の相手方に報告する義務があるケース ➢ 情報共有体制等の約款において、一定の条件の下での情報提供が求められるケース ※一般論であり、ケースとしては少ないと考えられる

２．サイバー犯罪被害者としての対応

■ **サイバーセキュリティインシデント発生時、典型的には、以下の類型の犯罪の被害者となっているケースが多い**

- 電磁的記録不正作出罪（刑法161条の2）
- 不正指令電磁的記録に関する罪（刑法168条の2、168条の3）
- 電子計算機損壊等業務妨害罪（刑法234条の2）
- 電磁的記録毀棄罪（刑法258条、259条）
- 不正アクセス禁止法違反（不正アクセス行為、フィッシング）
- 不正競争防止法違反（営業秘密侵害罪）
- 秘密保持義務違反　等

■ **警察への通報・相談等の検討**

1. 通報・相談
2. 被害届の提出（犯罪捜査規範61条）
3. 告訴（刑事訴訟法230条）

３．法的拘束力はないが推奨される事項

■ （１）ガイドライン等に基づく推奨事項

重要インフラ事業者による情報連絡	重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関する情報について、所管省庁を通じてNISCに連絡することとされている（重要インフラの情報セキュリティ対策に係る第4次行動計画（サイバーセキュリティ戦略本部））
不正アクセス等に関する届出	コンピュータウイルス・不正アクセス検知時には、IPAへ届け出ることが望ましい 「コンピュータウイルス対策基準」（平成7年通商産業省告示第429号） 「コンピュータ不正アクセス対策基準」（平成8年通商産業省告示第362号）
脆弱性発見時の届出	汎用性のある製品の脆弱性を発見した者は、IPAへその旨を届け出ることが望ましい 「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成29年経済産業省告示第19号）
分野別のガイドライン等	個人情報保護関係やセキュリティ関係のガイドラインにおいて、所管省庁等への報告や公表が求められる場合がある 「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針 」 「信用分野における個人情報保護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」 等

３．法的拘束力はないが推奨される事項

■ （２）その他推奨事項

公的機関の注意喚起	様々な機会において、関係省庁がサイバーセキュリティ対策の強化を呼びかけるケースがあり、その中で、不審な動きを検知した場合等の所管官庁への情報提供・相談を推奨 ➢ 経済産業省・金融庁・総務省・厚生労働省・国土交通省・警察庁・NISC「サイバーセキュリティ対策の強化について（注意喚起）」（2022年3月1日） ➢ 経済産業省産業サイバーセキュリティ研究会「サイバーセキュリティ対策についての産業界へのメッセージ」(2022年4月1日)
個人データ漏えい等に関する任意報告	報告対象事態に該当しない個人データの漏えい等発生時の個人情報保護委員会等への任意報告

４．その他任意の対応

■ インシデントに関する相談・情報提供先等

IPA	➢ 情報セキュリティ安心相談窓口 ➢ J-CRAT（サイバーレスキュー隊）
JPCERT/CC	インシデント対応依頼
情報共有体制	➢ サイバーセキュリティ協議会 ➢ J-CSIP（IPA） ➢ CISTA（JPCERT/CC) ➢ 各ISAC　等