

日調連発第14号
令和5年4月20日

各土地家屋調査士会長 殿

日本土地家屋調査士会連合会長

会員において発生した情報セキュリティインシデント情報共有について（依頼）

標記について、法務省民事局民事第二課から別添のとおり依頼がありました。

つきましては、貴会会員に周知いただきますとともに、貴会において情報セキュリティインシデントが発生した場合又は会員から報告があった場合は、速やかに当連合会へ報告いただきますようお願いいたします。



事 務 連 絡
令 和 5 年 4 月 5 日

日本土地家屋調査士会連合会 御中

法務省民事局民事第二課

会員において発生した情報セキュリティインシデント情報共有について
(依頼)

貴会におかれては、平素から法務行政に御理解と御協力を賜り厚く御礼申し上げます。

昨今、事業者に対するサイバー攻撃等が顕在化し、国民生活・経済活動に著しい影響を及ぼすリスクが増大しており、社会的な影響が生じた事案が確認されていること等を踏まえ、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）から、政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）等で定められている情報共有に加え、各府省庁が所管する業法に基づく所管分野の事業者等に係る情報セキュリティインシデントが発生した場合についても、所管する府省庁を経由して、NISC宛てに情報共有するよう依頼がありました。

つきましては、下記のとおり情報共有に係る連絡体制等を整備することとしましたので、各単位会及び会員に依頼するとともに、各単位会から報告があった場合は、速やかに当課に報告願います。

記

- 1 会員は、以下に該当する情報セキュリティインシデントの可能性を認知した場合は、速やかに可能な範囲で別紙様式を参考に、所属する土地家屋調査士会及び日本土地家屋調査士会連合会を通じて当課宛てに情報を共有するとともに、その後、当該情報セキュリティインシデントに係る新たな情報が確認された場合についても、同様に情報を共有すること。

(1) 国民生活・経済活動に著しい影響を及ぼす可能性があるインシデント

(2) 外交・安全保障に関わるおそれがあるインシデント

(3) 世論の反響が強く、社会的に大きな影響があるインシデント

2 会員は、上記1の情報セキュリティインシデントに係る攻撃技術情報(攻撃手法、攻撃者の活動を示す情報等)について、関係機関から求めがあった場合は提供すること。

昨今、事業者に対するサイバー攻撃等が顕在化し、国民生活・経済活動に著しい影響を及ぼすリスクが増大しており、社会的な影響が生じた事案を確認。

➡ 被害調査に必要な情報の共有や被害の未然防止のため、各府省庁が所管する業法に基づく所管分野の事業者等に係る情報セキュリティインシデントが発生した場合に、同インシデントに係る情報を共有するための仕組みを検討

1 情報共有の対象となる情報セキュリティインシデント

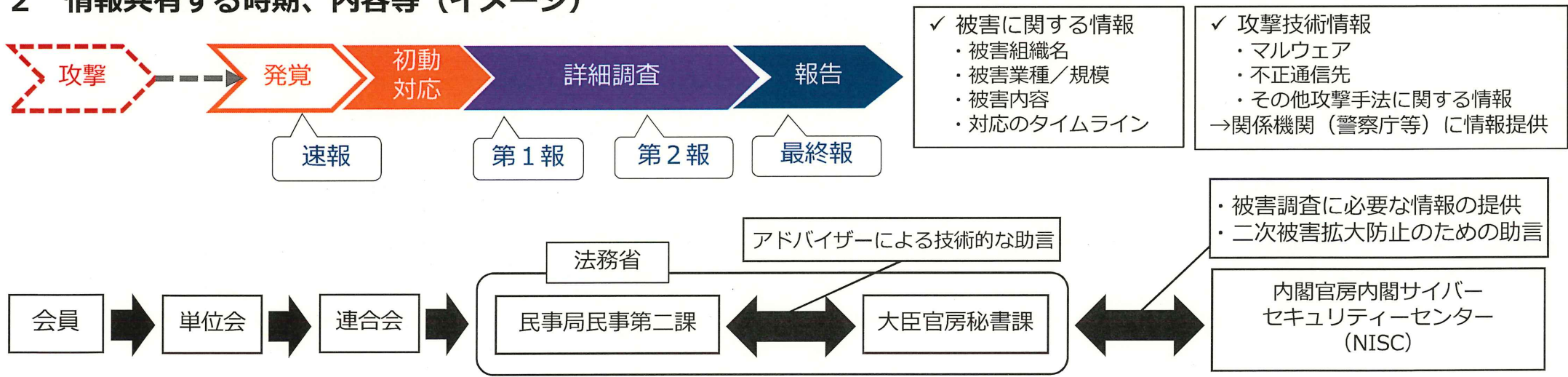
- ① 国民生活・経済活動に著しい影響を及ぼす可能性があるインシデント
- ② 外交・安全保障に関わる恐れがあるインシデント
- ③ 世論の反響が強く、社会的に大きな影響があるインシデント

※情報セキュリティインシデント
マルウェアの感染、不正アクセス又は機密情報の流出など、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高い情報セキュリティ上の脅威となる事象。

具体的には……

- ・ 会員が管理（利用）している情報システムに対してサイバー攻撃等され、個人情報が出た可能性が発覚。
 - ・ 日頃利用しているパソコンに不審なメールが届き、添付されていたファイルを開く、又は不審なURLをクリックした結果、パソコン上で不審な動きが確認され、パソコンに入っている情報（顧客情報など）が出た可能性が発覚。
- など

2 情報共有する時期、内容等（イメージ）



情報セキュリティインシデント（の可能性）発生報告書（記載例）

1	会員氏名（法人名）等	事業者名を記入。発生事案に関し、社会的にインパクトのある事業者との委託関係を有する場合等はその旨も記載。 発生した時点と現時点での事業者の名称が異なる場合には現時点での名称も併記。
2	主な事業内容等	事案発生事業者に関する基本情報について、事業者ホームページなどを参照して記載。
3	発生日	事案の発生日時を記載。 ※ 事案発生時点では不明であることも想定される。この場合は、「不明」「調査中」など、その時点の状況を記載。
4	発覚日	本件を事案発生事業者等が認知した日時を記載。
5	事案の概要	原因を含めて、事案の概要を可能な限り詳細に記載（調査中であれば調査中であることを記載）。 （1）被害の状況については、攻撃の態様・被害の性質を記載。 （2）事業への影響については、事業への影響、他社への影響可能性については、把握可能な範囲で記載。 （3）取組状況については、事業者における本事案に対する取扱状況を記載。 【記載例】 （1）被害の状況 〇〇（株）において、（月日/時間）に、（どういったサイバー攻撃）により、△△の被害が発生。 （2）事業への影響 現在、〇〇のサービスを停止中。 （3）取組状況 現在、〇〇（株）において、原因究明中。
6	経過（時系列）	発生から報告時点までの経過について、時系列で概要を記載。 【記載例】 ・（日時）に、（社名）のウェブサイトにて〇〇の障害が発生。 ・（日時）に、〇〇の脆弱性によるものである可能性が判明し、不正ファイルの存在を確認したため、〇〇サービスを停止。 ・調査の結果、（日時）に、（サイバー攻撃発生日時）に不正アクセスがあったことを確認。 ・（日時）に、〇〇に係る個人情報〇万件の漏えいの可能性を把握。 ・（日時）に、事業者から第一報。（第一報のみ記載） ・（日時）に、事業者が公表予定。 ・（日時）に、原因究明調査終了し、停止していたサービスを再開。

7	今後の予定	<p>検討中（確認中）であれば検討中（確認中）である旨を記載。想定されるスケジュールがあれば記載。</p> <p>【記載例】</p> <p>(1) 事案の公表有無 ○月○日に公表を予定</p> <p>(2) 個人情報保護委員会への報告 報告済（○月○日）</p> <p>(3) 復旧状況 △△により○月○日には復旧</p> <p>(4) 被害の全容、調査・原因究明</p> <p>(5) 再発防止</p>
8	被害を受けたシステムの概要	<p>被害を受けたシステムについての用途などを含めた概要を可能な限り詳細に記載。（保有データの種類や件数（漏えいがあればその件数））</p>
9	当省の対応	<p>【記載例】</p> <ul style="list-style-type: none"> ・ 今後、速やかな原因究明を指示。 ・ ○日頃に業界向けに注意喚起を周知予定。現在準備中。
10	備考	<p>サプライチェーンへの影響など、その他情報があれば記載。</p>

情報セキュリティインシデント（の可能性）発生報告書

1	会員氏名（法人名）等	
2	主な事業内容等	
3	発生日	
4	発覚日	
5	事案の概要	
6	経過（時系列）	

7	今後の予定	
8	被害を受けたシステムの概要	
9	当省の対応	
10	備考	