資料 1-2

共有・公表ガイダンス検討に向けた各ポイントについて

【外部との連携等について（仮)】

〇情報共有活動

〇専門組織との連携

〇警察への通報・相談

〇行政機関への連絡

・行政機関への連絡（義務に基づくもの）

・上記以外の何らかの指針に基づくもの

・行政機関への連絡（義務に基づかないもの）

※専門組織、警察、行政機関での情報共有活動の意義・目的を明確にし、行政機関での情報集約に触れることで、窓口一元化の論点についての課題感と当面の方向性を示す。

【共有と公表に関する総論】

〇「共有」と「公表」の分離について

2 つが混在すると情報共有効果を得られなくなることや、「技術情報」と「コンテクスト情報」の分類により早期の情報共有が可能になる点について解説

〇「共有」と「公表」の連動について

上記の通り、2 つを分離させることで早期の情報共有が行えるが、一方で 2 つはまったく別々の活動ではなく、相互に連動するものである点について解説（同時に発生するケースや、2 つの時間間隔が開きすぎる問題について）

〇「情報共有」と「注意喚起」と「ノウハウ共有」の違いについて

「共有」と「公表」が混同されがちな背景として、それぞれの「目的」に応じて、手段やタイミングが異なる点への理解不足があるため、これを解説

■委員意見概要

（想定読者、視点）

・主な想定読者として、情報共有活動に参加している者だけではなく、情報共有に慣れていないため、何をしたら良いか分からない組織も想定した方が良いのではないか。

・ガイダンスの性質上、情報を受領する側の視点になるのはやむを得ない面があるが、情報を提供する側から見て、どのようなメリットがあり、提供先たる機関にどのような役割があり、どのようなことを行うのかも書けると望ましい。

・共有、公表等において、被害組織で様々な負担が生じるが、中小企業は対応能力にも差がある。レイヤーを分けて議論を行うなど、中小企業の負担軽減についても考慮要素としていただきたい。

（法律に基づかない報告）
・「共有」、「公表」以外に、「法律に基づかない報告」のカテゴリがあるのではないか。被害企業としては、顧客や取引先等に対する被害の報告は重要な関心事であるし、B2B 企業か B2C 企業かによってもスタンスは異なる。また中小企業は千差万別であり対応能力にも差があるので、その点は考慮して欲しい。

【共有について】

〇共有の目的／効果

・組織毎／共有活動毎に異なる共有の「目的」ついて
・攻撃類型や共有するタイミングによって異なる共有の「効果」について

〇共有のタイミング

・共有による効果を発揮できる共有タイミングがあることについて

〇共有する内容

・技術情報とコンテクスト情報の分離について
・技術情報の解説
    ・マルウェア情報
    ・通信先情報
    ・その他 TTP 情報
    ・脆弱性悪用に関する情報
    ・その他の技術的情報
    ・「時間」情報の重要性について
・被害は発生していない事案に関する情報共有について
・公開情報であっても共有効果のある情報について

〇共有の方法／共有相手

・情報共有活動の類型について
    ・ハブ・スポーク型
    ・n 対 n 型
    ・共有活動に参加しない情報共有
・情報の伝達方法について
・情報共有による「フィードバック」について
・専門組織が仲介する情報共有について
    ・インシデント対応における NDA 契約との関係について
    ・「公開情報」について
    ・専門組織によるレポート公表について

■委員意見概要
（技術情報）

・技術情報と一口にいってもイメージは様々なので、具体的に何を意味しているのか、何を共有して欲しいのか、（ガイダンスの最初の方に）分かりやすく書く必要がある。
・公表は出来なくとも共有できる情報があることを示すべき。また、共有の目的は、注意喚起したいのか、自社環境においてブロックしてほしいのか、連続的ではありつつも区別できるものである。「●●目的のためにこの情報は早期に共有して欲しい」という形で書くことも考えられる。

（NDA）

・NDA の問題については、NDA に抵触するから出せないのか、後で揉めると面倒なので NDA の所為にしている場合とがあるように思う。
・ベンダーが情報提供するのではなく、被害組織が提供する建前にすれば、NDA の点はクリアしやすいのではないか。フォーマットに沿って埋めるだけならハードルも下がると思われる。

（取扱いに留意すべき情報の共有）

・被害情報の共有に当たって、当該情報が国の安全、利益に損害を与えるおそれのある情報である場合には、情報の取扱い等の面で十分に信頼ができ、その内容を真に知るべき者に限って共有すべきではないか。重大な脆弱性情報等は、悪用されるリスクも踏まえて、多数の者が参加するような情報共有活動ではなく、しっかりとした取扱いがなされる者の間で共有される必要がある。

（情報共有先の信頼性確保）

・本ガイダンスの領域外であると認識しているが、サイバーセキュリティ関係の機微な情報の共有について、信頼性の確認がなされた相手先と情報を共有できるような仕組みが将来的に必要になると考える。

【公表について】

〇公表の目的／効果

・既存の法令・制度上もとめられる公表について
・二次被害防止のために行う公表について
・被害事実が推測／認知される可能性が高い場合に行う公表について
・その他の判断理由で行われる公表について

〇公表のタイミング

・公表まで時間がかかる背景について
・速報や第 n 報など複数回公表することについて
・「注意喚起」「情報共有」目的の公表について
・「共有」と「公表」を同時に行う場合について

〇ステークホルダーや他の被害組織との関係について

公表判断を被害組織自身だけでは判断できないケースや、ある被害組織からの公表が他の未公表の被害組織に影響するケースについて解説

〇公表する内容

・技術情報とコンテクスト情報の分離について

・コンテクスト情報の解説

〇公表する方法

Web サイトからの公開のほか、Web サイトが使用できない場合の代替手段（SNS 等）の事前準備の必要性について解説

〇公表の社会的意義について

■委員意見概要

・被害企業自身が被害を公表することは企業活動の透明性や説明責任の確保のために重要なだけでなく、攻撃被害情報のような公共的な情報は、国民の知る権利を守る観点からも重要である。ガイダンスではこれらの価値を明記した上で、分かりやすく公表するためのポイントを示すべきである。

・国の作成するガイダンスが、実名の公表を控えることを推奨する方向となったり、報道のあり方について詳細な報道を控えるべきという趣旨のことを書いたりするのは、報道の自由や国民の知る権利との関係で適切ではないのではないか。

・当の被害組織が被害を公表していない段階で、他者によって実名入りで被害内容がオープンにされてしまうこと、特に、被害組織が悪者であるような取り上げ方がされてしまう場合があることについては疑問なしとしない。また、「リークサイトに●●社から漏えいしたと思われる情報が掲載されていた」というような内容がオープンになると、それに接した者が当該リークサイトにアクセスし、被害拡大するだけである。リークサイトの存在を伝えるべき対象は、一般読者ではなく、漏えいの対象となった人や組織なのではないか。

・漏えい情報はメディア等で話題になれば目立つが、当事者が知ることもなく悪用されることもある。

・事案がオープンになることで過剰に被害組織叩きが行われてしまうと、被害組織としても、公表はしたくないという判断になってしまう。公表の社会的意義は十分に理解しているが、被害者保護の観点も加味することが必要。

・公表の目的等に合わせて、どのような情報を示すことが適切であるかという点も示してはいかがか。

【その他の論点（被害者保護等）】

〇「被害情報」の性質について

〇被害組織が推測される情報

・外形上攻撃被害が認知される場合

・漏えい情報の公開や犯行声明がなされる場合

・関係者による情報発信により認知される場合

・解析結果から被害が推測される場合
・その他公開情報から被害が推測される場合

〇第三者に影響する情報

・第三者の被害発覚につながる情報について
・脆弱性情報の取り扱いについて