電気通信事業ガバナンス検討会（第９回）

議事要旨

１　日時

令和３年10月４日（月）13時00分～14時45分

２　場所

Web開催

３　議事

（１）電気通信事業ガバナンスの強化に向けた検討について

・事務局より、資料９－１に基づき、電気通信事業ガバナンス強化に向けた検討状況の整理について説明があった。

・各構成員からの主な意見は以下のとおり。

【全体】

○リスク対策の実施主体について、利用者に対する一義的な責任を有する通信サービス提供者が責任を負うのが本来あるべき姿。一方、それでは対応や周知広報が遅れることが多いのであれば、逆に、実際のサービス運用において責任を有するのは誰なのか、契約に当たって利用者に明確に示しておくやり方もあり得ると思う。

○電気通信事業ガバナンスの強化に向けた方策として、リスク対策の後に利用者等への情報提供が記載されているが、冒頭に、情報の適正な取扱いについて記載した方が良いのではないか。

【①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策】

○利用者情報について、コンテンツまで含めて全て利用者情報だとすると、少しでも通信をしているほとんど全ての情報サービスを、電気通信事業法の範疇でコントロールしないといけなくなるのではないか。

○昨今の事案では、国の利益を害するリスクをもたらし得るということが教訓の１つ

として考えられるが、透明性の部分で虚偽があった場合には、厳しく責任を問うような考え方もあって良いのではないか。

○基本的に影響度の大きさという点では、情報の量に着目することになると思うが、質の面では、一般に公開されていないという観点に着目することになるのではないか。

○適正管理を行うべき情報について、原則として、秘匿性の有無に関わらずできるだけ広くということが意識されるべきだと考える。侵襲性の高い機微な情報ではなく、ささいな情報の集積が、個人・社会・国家に大きなインパクトをもたらし得ることも考えられる。

○適正管理を行うべき情報の分類について、「通信サービス上の行動履歴や利用者の状態に関する情報」として例示されているものの中には、「通信の秘密に係る情報」の例示されているものよりも、通信の内容に深く関わる情報も含まれているので、情報の種類の分類の見直しが必要ではないか。

○電気通信設備に関する技術基準の考え方と、ＩＳＯ／ＩＥＣ２７０００シリーズにおけるリスク管理やセキュリティ管理について、通信の秘密や責任分界点等、重なる部分があるので、うまく差別化又は利活用するのか、明確にした方が良い。

○電気通信設備を設置する電気通信事業者が技術基準を満たすこと等により、電気通信役務の円滑な提供が行われてきたが、それだけでは不足する部分も出てきたのではないかと考えられる。ＩＳＯのセキュリティの考え方では、情報漏えいの防止だけでなく、継続的なサービスの提供も含めた概念も含まれているので、その視点で整理するのが良いのではないか。

○利用者情報について、公開されているものとそうでないものがあるが、いずれであっても第三者提供により自由に使えて悪用できてしまうので、電気通信事業を営む者はＯＴＴ事業者も含めて規制すべきであり、データの取扱いについて一定の整理

は必要だと思う。

○情報を置くとリスクの高い地域について、例えば、サイバーセキュリティ戦略の中でも具体的な国名が挙げられるようになっているので、もう少し明確にリスクとして取り上げ、踏み込んだ形でのリスク対策を取ることができるのではないか。

○通信の秘密の保護について、一般的には、内容だけではなく識別や行動履歴も含むものと解釈されると考える。表現の自由は、思想・信条を外部に出す行為についての自由であるのに対して、通信の秘密は、通信の秘密とそれを包含する生活上の自由を保障しているのではないかと考える。利用者に関する情報は全体として、通信の秘密に関する内容として保護されるべきものなので、しっかり整理した方が良いと思う。

○特定他者との間のコミュニケーションで、この人にしか知らせたくないということが通信の秘密の本質、核心に関わるものだと考える。それをどう守るか、又はそれに対する萎縮効果をどう考えていくか、という観点から、情報の種類を整理していくことが必要ではないか。

○ウェブの閲覧履歴について、日本では、氏名等と結びつかない場合は原則として個人情報として扱われないので、個人情報にも通信の秘密にも該当しない利用者に関する情報の取扱いを、電気通信事業法の枠組みにおいて考える必要があるのではないか。

【②ネットワークの多様化等を踏まえた通信サービス停止に対するリスク対策】

○重要インフラという立場での通信サービスを考えたときに、サービスの継続は非常に大事で、通信サービス停止に対するリスク対策は非常に重要。設備やシステム設定に関わる情報を守ることがリスク対策にもなるという意識が大事だと考える。

○サイバー攻撃対策において、平時の連携も大事な議論だと思う。個人を守るためにあえて交換しないといけない情報があるので、透明性を確保した上で、必要な情報

は使えるようにするための取組も重要なのではないか。

○サイバーセキュリティは通信の秘密と対立する利益ではなく、通信の秘密はサイバーセキュリティによって支えられている部分もあるので、サイバー攻撃への対処にあたっては、時間をかけて違法性阻却事由を個別に検討することなく、対策を適切に進めていくための法制度が必要だと考える。

○平時からサイバー攻撃のフロー情報等をモニタリング・分析して、分析結果を共有していくには色々な整理が必要になるが、これまであまりなかった取組で非常に良いと思う。法制度にうまく反映されると、より電気通信事業者間の連携が評価されるのではないか。

○セキュリティの確保に向けた積極的な行動が空振りに終わったときに、法的な責任を問われることになると事業者が萎縮してしまうと考えられるので、免責措置や、正当業務行為としての違法性の阻却といった可能性も含めて議論を進めていく必要がある。

○事故の兆候段階からの報告義務について、事故の未然防止や被害軽減のために、報告や共有の仕組みを構築することは重要。サイバー攻撃の予兆を把握し、報告対象を具体化していくことは難しいと考えられるので、検討の際に留意が必要。

○どういう情報であれば公開して良いのか、事業者間での連携の仕方を検討していくことは大事だと考える。一方で、予兆の把握は難しいと考えられるので、どこまでの情報を政府に報告する必要があるかについては慎重な検討が必要。

○予兆に関する報告が、結果的に、間違っていた、不正確であった、ということもありうると思うが、社会のためにやろうとしたことに関しては、免責措置のような救済する仕組みが必要だと考える。

【③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供】

○利用者等への情報提供について、事業者の説明責任の観点も入れていただきたい。

○情報提供の意味は、正しい情報を伝えて、その結果を判断できるということなので、情報提供とその真実性の担保はセットだと考える。

○電気通信事業者は、事故が起きている範囲、原因、復旧見込み等がはっきりしてから利用者に周知しようとする傾向があるが、利用者への第一報を急いだ方が良いようなケースも存在する。利用者目線では、まずは一部でトラブルが生じているといったところから始めて、判明したことから順次公開し、事故が解消した後、その履歴を全て残しておくことが重要なのではないかと考える。

（2）その他

・事務局より、今後の予定について説明があった。

以上