電気通信事業ガバナンス検討会（第８回）

議事要旨

１　日時

令和３年９月15日（水）13時00分～14時55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課題について

・事務局より、資料８－１、資料８－２、資料８－３及び資料８－４に基づき、電気通信事業ガバナンスの強化に向けた検討課題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。

○電気通信事業者は、役務の円滑な提供のため、設備については、電気通信事業法のルールに従って、技術基準適合の自己確認を行っているが、金融業界の基準で定められているようにある一定の部分に関しては外部監査等の必要性を考えても良いのではないか。

○適正な管理が必要な電気通信事業に係る情報については、通信の秘密に関する情報を重要視するべきであるが、位置情報等のような利用者に関する情報も対象になるのではないか。

○設備の設置の有無に関わらず、全ての電気通信事業者に対して、情報の管理をしていくべきだと考える。電気通信事業法の中で細かい規定を作るのではなく、例えばＩＳＯ／ＩＥＣ２７０００をしっかり遵守するというようなことを記載し、それが守られているのかを監査する、といった方法が良いのではないか。

○プラットフォームサービスに関する研究会においては、利用者の権利、すなわち個人的法益のために保護するべき重要なものとして、通信関連プライバシーという考

え方が提示されている。本検討会では社会的法益、国家的法益の保護もスコープに入っていることを踏まえれば、通信の秘密だけでなく、サービスの利用情報、位置情報、ウェブの閲覧履歴等の利用者のＩＤに紐付く情報である通信関連プライバシー、加えて、通信の内容ではないが住所や家族構成などの利用者の登録情報も保護の対象とすべきではないか。

○情報の適正管理に係る規律については、登録・届出がなされている既存の電気通信事業者だけを対象とするのではなく、守るべき情報を持っている電気通信事業を営む者を対象とするべきではないか。現状では、このような者の方が個人的法益、社会的法益、国家的法益に影響を与える情報を持つようになっている。対象が徒に広くなってしまうという懸念に対しては、利用者数で限定するなどの対応が考えられる。

○情報の不適正な取扱い等による社会的な影響の大きさをどのような軸で評価するのかという点について、コミュニケーションへの萎縮効果や民主主義への影響等が考えられる。特に、通信の秘密は、憲法第２１条第２項の表現の自由のところに入っていることから見ても、その目的は、民主主義の維持、自己統治の実現等とも関連するものと考えられる。

○外国の法的環境や政治的な状況に関する収集能力を持っているのは政府なので、政府には、関係する情報を収集・分析し、企業に対して提供していくといった情報のクリアリングハウスのような役割が求められるのではないか。外国企業のアクセスを認めるのか、認めないのかといった判断をする仕組みが重要で、事業者が判断を行う際の情報提供が政府から行われるようにすることが重要ではないか。

○総務省の情報通信ネットワーク安全・信頼性基準について、これと同等のものはＩＳＯ／ＩＥＣ２７００１で、マネジメントのプロセスに対して遵守すべきことが記載されている。ＩＳＭＳを取得している電気通信事業者も多く存在するので、情報通信ネットワーク安全・信頼性基準がＩＳＭＳと対応するように整理することも手段の一つとして考えられるのではないか。

○通信の秘密は、個人的法益、社会的法益、国家的法益の全てにかかっているものだと思う。利用者に関する情報も確かに全てかかってしまうが、端的に言うと、個人的法益に関するものになると考えられる。対象とする情報の影響の大きさについて、量的な観点と質的な観点という軸で評価することになり、量については利用者数、質については、秘密性を重視せざるを得ないと考える。

○情報の漏えい・不適正な取扱い等を防止するための新たな規律については、進行しているものに対する確認に該当する監査等に加えて、事後的な対策が必要ではないか。ただし、事後的な対策については、原因解明を進めやすい形とするために、必要以上に責任や義務を求め過ぎないという観点が必要ではないか。

○情報の漏えい・不適正な取扱い等を防止するための新たな規律について、設備規律にあるような基準等を情報側でも採用して、ガバメントアクセスのような新たなリスクに対応していくという方法が考えられるのではないか。

○電気通信事業法では、情報を送る、通信をすることに対して公平であるという観点と、憲法でも遵守が求められている通信の秘密の観点が、規律の中心となるべき。電気通信事業法としては、情報を管理する体制がしっかりできているのかという議論をするべきであって、その情報の中身については、議論するべきではないと考える。

○これまでは電気通信事業者を設備中心に規制しておけば利用者を守ることができたが、電気通信事業者の機能が分化して、設備を持たない者を含む様々な者が参入してきている中で、設備だけの規制では、利用者の保護が難しくなってきているので、直接的に電気通信サービスの利用者を保護するルールを志向する必要があり、守るべき利用者の情報の内容を考えざるを得なくなってきていると考える。

○ＩＳＯ／ＩＥＣ２７０００ファミリーでは、扱う情報をいかに体系的に健全に保護、管理するかということに焦点を当てており、その情報の内容については触れていない。特に、電気通信事業者の立場から記載されているＩＳＯ／ＩＥＣ２７０１１や

ＩＴＵ－Ｔ　Ｘ．１０５１では、通信の秘密を守っていくということについては確保するとされているが、クラウドの活用やＣＤＮについては責任分界点の明確化等をするという方向性になっている。

○電気通信事業者が扱う通信の秘密としての情報について対象を決めようということではなく、これまでの整理を前提としつつも、環境変化に応じて社会へ影響のある情報がほかにもあるのではないかという問題意識から、規制を検討すべき対象として、利用者に関する情報がクローズアップされているところではないか。

○情報の内容、性質ということを無視して、もともと通信の秘密というものを重要な保護の対象としている電気通信事業法を語ることは難しいのではないか。

○情報の取扱いに係る委託先の透明性について、今後は「委託する目的」も公表すべきではないか。

○単独の事業者では対応困難なリスクへの対応について、利用者にとって重大な影響を及ぼすリスクなども事業者間の連携協力が必要だと思われ、リスクの把握や評価分析等を政府が関与する形で進めていくとともに、利用者への配慮の観点も入れていただきたい。

○情報の漏えい・不適正な取扱い等や事故への対応について、国への報告は当然必要だが、事案によっては利用者に対する報告も重要なのではないか。また、報告時期についても事象によって違ってくるのかと思う。報告内容については、事業者による問題解決だけでなく、利用者における対処の仕方も含めてほしい。

○事業者間で連携して情報をやり取りする場合について、もともと形式的な通信の秘密の侵害が例外的に許容される場面は、同意がある場合か、違法性阻却事由がある場合の２つに限られ、違法性阻却事由の中には、正当業務行為、正当防衛、緊急避難の３つしかない。近年のサイバー攻撃の複雑化・巧妙化を踏まえると、違法性阻却事由で例外的に許容するだけではなく、本来はもう少し広い意味で許容されるべ

きではないかと思うようなケースも見受けられる。

○サプライチェーンリスクについては、法的な対応も含め信頼性を確保するための仕組みは検討しても良いのではないか。

○サイバー攻撃は基本的に複数の事業者にまたがっているので、事業者間での連携が非常に重要。ＩＣＴ－ＩＳＡＣでは、事業者間で連携して、対策を練って事象に臨む仕組みを作ってきているので、それを強化するような視点も考えられる。

○サプライチェーンリスクや海外の法的環境による影響等のリスクについて、政府を含む社会全体としての取組の強化は必要だが、サプライチェーンの話と一般的なサイバー攻撃の話は分けて考える必要があるのではないか。

○事故の兆候段階の事態については、いわゆる攻撃や事故に起因する兆候、例えばスキャンイベントや、認証のトライアルなどからオペレータの単純なミスなどが該当するものと考えられ、オペレータのミスについては一般的な電気通信事業者ではヒヤリハットと呼ばれている。インシデントそのものと比較すると、兆候事案の事態の方が圧倒的に多いが、該当する事案の類型化や整理には検討が必要と考える。

○サプライチェーンに関して政府が一定の役割を果たすことを考えた場合、事業者が使う機器やサービスについて、ガイドラインレベルを超えて、諸外国のような規制をかけるのであれば、電気通信事業法の目的には合わないのではないか。

○重大な事故等の兆候段階に該当する事案の類型化や整理は、非常に難しい問題だと思うが、想定していなかったインシデント等が起きたときに、報告すべき事案や事業者間で共有すべき内容に関する検討は必要だと考える。電気通信事故検証会議でも、公開して問題ない範囲については報告書として公開しているが、現状は事業者目線で、他の事業者に役立ててもらうという位置付けなので、今後はエンドユーザーの視点も取り入れられると良いのではないか。

（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