産業サイバーセキュリティ研究会WG1
『第3層：サイバー空間におけるつながり』の
信頼性確保に向けたセキュリティ対策検討タスクフォース
（第4回）議事要旨

1．日時・場所

日時：令和3年6月30日（水） 14時00分～16時00分

場所：Web開催

2．出席者

委員　　：岡村委員（座長）、池田委員、井原委員、江崎委員、菊池委員、楠委員、黒田委員、坂下委員、
島岡委員、中谷委員、永宮委員、満塩委員、矢野委員

オブザーバ：内閣官房　内閣サイバーセキュリティセンター、金融庁、厚生労働省、独立行政法人情報処理推進機構

経済産業省：大臣官房　江口サイバーセキュリティ・情報化審議官、奥家サイバーセキュリティ課長

3．配付資料

資料1 議事次第・配布資料一覧

資料2 委員名簿

資料 3『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性

資料 4「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案

4．議事内容

事務局から資料3に基づいて説明した後、以下のとおり自由討議を行った。委員からの意見は以下のとおり。

●「場」について

「場」が曖昧な場合も世の中には多く、例えばオープンソースのコミュニティや研究コミュニティなどは、暗黙知に基づいてルールが形成、運用されていることがある。そのようなものも「場」として扱うのか否かわかるようになっていると良い。

法律とは異なるレイヤーでプラットフォーム企業が制定している規約等のルールがあり、そのプラットフォームに参加するためにはそのルールを遵守するということも生じている。そのような要素も視野に入れて考えた方が良い。

公的な法令だけではなく、相対での契約や商慣習が、サプライチェーンの中でルールやアルゴリズムのように機能していることがあり、これを含めたサプライチェーンの把握と見える化が必要ではないか。特に特定のプレーヤーによるブラックボックス化を防ぐことをフレームワークの目的の一つに掲げている中では、その点を意識すべき。

●「イベント」について

「保管」と「廃棄」の定義について、「廃棄」が「データセット全体について、完全に、使用不可能な状態にすること」とされているが、使用不可能であってもデータを保有していれば、実務上「保管」と整理している分野もある。まさに、フレームワークが、コミュニケーションにおける誤解をなくすのに役立つ例だと思う。

必ずしも全てのデータを完全消去しなければいけないことはなく、軽い消去でも十分アクセス制御に役立つものもなど、廃棄にもレベルがあるのではないか。完全に使用不可能というのは一つのレベルに見えるので、将来的な改定に関しても含みを持たせる形で、幅のある書きぶりにした方が良い。

「イベント」としての「加工・利用」に「閲覧」が入っている点に違和感。デジタルは基本的にはコピーをしたからといって、元データが消えるわけではない。共有のため移転行為が繰り返され、権利者が複数になることを考えると、「閲覧」は「移転・提供」に入れた方が良い。

時間軸の表現の仕方について、ある瞬間、最後のスナップショットで見ているのか、それとも時間軸が移り変わっていく様子を見ているのか考えた方が良い。クラウドサービスを利用する例で考えれば、複数の権利者や管理主体が出てくる場合というのは、「場」毎に管理者と権利主体は異なるが、同時に発生し得る、という表現になるのではないか。また、複数がバックアップを取ったりすれば、より複雑になる。一種のイメージ図として描かざるを得ないという限界があることは承知しているが、整理してユースケースとして示して欲しい。

●「属性」について

データを受け取った人がどのようにデータを信頼し使えると判断したかというリスク評価結果に関して、どのようなリスクを受容したのかという点は他のステークホルダにとっても有用であることから「属性」として扱うという考え方もある一方、本フレームワークは分析のためのツールであり、リスク評価結果は分析の結果として現れるものであることから、属性として可視化すべきものとして扱うのは難しいのではないか。

データを流通させていく中で次に伝えるべき情報としては、少なくとも客観的な情報と主観的な情報を分けておくべき。検証可能な情報かどうかが重要だと思うので、もし価値を「属性」として載せるのであれば、検証可能な価値がステークホルダ間で共有されるようにするべき。

「属性」の情報が変わったときに、「場」が変わるのか変わらないのか、というところが分かりづらいのではないか。例えばルールが同じで利用目的が変わった場合にどう考えるべきかが分かりにくい。「属性」の一つに利用目的を位置づけて、その範囲内で利用する、即ち「場」を変えないように留意して利用するという活用方法になると思う。

「データ管理主体」、「データ権利者」について、「データ管理主体」はdata controllerと理解している。「データ権利者」は、データに対するrights holderかと思う。法律上もデータ権利者は複数たり得る。おそらく権利には2通りあり、転々譲渡していく過程の中で加工した人にライセンス等の形で対象データの契約関係から発生する権利と、そのデータが帰属している主体であるが故に発生するプライバシー等の本人の権利がある。例えば、GDPR17条における自己のパーソナルデータに関する「消去の権利」などが、GDPRにおける「データ主体」、日本法で言う「本人」の権利であるのに対し、顧客名簿は不正競争防止法で言う営業秘密になったりデータベース著作物として別の権利者が発生することもある。

●その他

P17のCollective Actionは、Collaborative等の別の訳語も考えられるが、マネジメント用語として比較的使われている Collective managementを意図してCollective Actionという言葉を使っているというもの。用語の使い方を早めに定義しておくと問題は少ないのではないか。

データ管理主体をdata controllerと解釈するところは同意見だが、GDPRにおけるdata processerに該当するものは、日本の仕組みには無いと認識。英語でのパブリックコメントを実施する際に、日本固有で海外の人に分かりにくい概念に委託がある。直訳が難しい表現もあると思うので十分に注意が必要。

プロセスの自動化を進める中で、プロセスを見える化することでインシデント対応にも役立てることができるのではないか。

全体の話や最初の事例や最後のユースケースを聞くと、色々な、例えばテスト支援ツールのバックドアの話や、SaaSの関係などが書かれている。想定読者のところはデータ交換が少し強調されているので、もう少し広く書いた方が良い。

抽象的な表現ばかりでは具体的なイメージを持ちづらいため、具体的な説明で補完することが良いと思うが、あまり細かく示しすぎると、それが独り歩きして深く考えずにその例をそのまま使ってしまうということも起こり得るので注意が必要。

このフレームワークは複数のプレーヤー間を情報が行き交う空間への適用を想定している。ISMSの組織的な対象は任意に決められ、複数の事業者が共同で範囲設定し対応することもできる。

各委員からいただいた意見を踏まえて座長に相談し、フレームワーク骨子案修正を加えた上で、パブリックコメントを実施することで了承を得た。

以上

お問合せ先

商務情報政策局　サイバーセキュリティ課

電話：03-3501-1253