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3回）議事要旨

1．日時・場所

日時：令和3年3月5日（金） 13時00分～15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、楠委員、黒田委員、小林委員、
島岡委員、中谷委員、永宮委員、満塩委員、和田委員

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、警察庁、金融庁、総務省、厚生労働省、
独立行政法人情報処理推進機構、一般社団法人JPCERTコーディネーションセンター

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

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。

●データマネジメントの新たな捉え方について

場という概念、その場で行われるイベント、イベントが対象とするデータ、そのデータのプロファイルというところで整理されたと理解。よく混同される問題として、APIとプロトコルがあり、最近はAPIがオープンになればロックインも解消されて全部処理できるという人も増えているが、データが流通するための共通フォーマットを含めたプロトコルが必要であり、その上でAPIがフィールドとしてのインターフェースのところで作られていく。そうすると、全体の構造として、データ自身の定義、インターフェースの部分、通信等のトランザクションに関する共通のプロトコルの部分、そして相対を含めたところでのAPIに分けて整理すると捉えることができる。

属性について、ステークホルダごとのデータの価値やプライバシー性、もしくはカテゴリが存在するはず。属性は二次元の表のような状態になり、各ステークホルダに対する価値やプライバシー性の評価がどの場によって定められているものなのかという関係性が、三次元の形で表現されるイメージを持っている。

リスクがそれぞれの場である程度捉えられ、全部重なっているとみたときに、場に係る人たちの共通の理解、共通の行動パターンなどで担保されるようにお互いが調整していきましょうということと理解。

法制度一つみても主権が及ぶ範囲は国単位であり、それに横串を指す契約法理も強行法規の前では効力がなかったりするため、かなり入り組んだ問題。最近はGDPRのように域外適用で第三国へ影響を及ぼすものに十分性認定という形で対応していくように、場が重なり合っていたりすることも事実で、問題は複雑化している。

●リスクポイントの洗い出しについて
神の目線というか、フロー全体が見えていれば、その中にどのようなリスクがあるか整理できるが、実際には相対の相手までしか見えておらず、その先は認識できていない。そのような状況でのリスクポイントの洗い出しは非常に難しく負担が大きいため、出口論として個々の事業者に落とし込んでいくときに検討が必要。また、リスクを可視化するだけではなく、リスクを受容するときに何をもってどのようなリスクを受容したのかということを可視化できると、データの流通先の事業者でも、どのようなリスクの受容のされ方をされたデータなのかが分かるのでより適切な評価ができるのではないか。

イベント類型にある移転について、移転というとAにあったものがBに移るというようなニュアンスだが、実際にはデータはAに残っていてAの主体が逐次データを更新している可能性もある。そうなったときに移転先Bにあるデータと Aに残されているデータとは違うものになるし、さらにBからCに移転されることもあるかもしれない。もともと一つだったデータが色々なところに拡散して共有されたときに、そのデータの完全性をどうやって担保していくのかのイメージが持てていない。

色々と使えると便利だというイメージは持っているが、例えばデータの機密性、完全性、可用性、移転という前にデータの信用性というものがあると思う。いま船の世界では、船が排出するCO2を報告する制度が昨年から始まるなど、最終的にはCO2の取引権を視野に入れた国際的な動きがある。そのようなときにデータの信用性、データ品質が重要となってくる。

●本タスクフォースのアウトプットイメージについて
別の会議でインシデントのトレーシングについて議論しており、国を跨いだところでトレーシングが不可能になっているという問題がすでに顕在化している。国の間での捜査協力や共通の協定が作れないと問題をトレーシングできないし、責任自体の定義ができず問題解決できない。経産省でもこの議論を参照し、協力してアイデアの共有をしてほしい。

ブロックチェーンやその上で動くDecentralized Financeのような新しいテクノロジーを見ても、場合によっては、全体に対して誰も責任を持てず、ダークウェブなどを含むセキュリティ上の様々な問題とも結びついているので、こういった概念整理は非常に重要。他方、出口論としてこのような整理をした後にどうやって実効性のあるフレームワーク、規制、ルールメイキング等に落とし込んでいくのかというところには、相当難しいだろう。

出口の話として、制度間や国の間での調整のほかに、実装に近い個別のサプライチェーンにおけるリスク対策もターゲットとすべき。特に実装では、クラウド関係の問題として、米国法が適用されるのか日本国法なのかEUなのか、というものがある。例えば暗号化する際の暗号鍵の管理を誰が行うかによってCIAが可変すると思慮。また、ISMAPでは、SaaS、PaaSのところをどう考えていくのかというところが議論になっており、そちらとの連携が重要。

どのようなアクションをすべきか、その実装のレベル、誰がどこまでの責任を負うのかというところが気になるところであり具体的なアウトプットが非常に重要。資料3 P.29のフローにおける④ユースケースから⑤ガイドライン・ツールのあたりの具体的な落とし込みが非常に大事だと思うが、上流のところで細かい認識がずれている懸念がある。例えば、現時点でいくつか典型的なユースケース例に、提起している概念や用語を当てはめるようなことをすれば、より分かりやすくなるのではないか。また、②③④あたりはまっすぐ下に行くのではなく、フィードバックがかかって上に戻ることもあるだろう。

フレームワークの考え方を製造業のサプライチェーンに応用していきたい。サプライチェーンが何百、何千という階層になっていて管理も大変であり、この考え方がゆくゆくは規格等になって、下請け会社との契約時に要求することで、管理の負担が少しでも下がればありがたい。

取組自体には意味と価値があると思う一方で、いかにそれを打ち手としてつなげるかが、非常に難しい問題と理解。転々流通を前提にした取組なので、全員がこれを守れるような形にならないと求められるような機密性、完全性、可用性等が担保できない。その中には個人もいれば、法人も大企業から中小企業までいて、グローバルにまで広がる中で、どのように遵守するか。規制だけでもなかなか守れないところもあるので、技術的なところとかを含めてどのようにサポートするか、実務に寄った議論を進めていけるとよい。

事務局にてタスクフォースでの議論をまとめたうえで、データ流通における適切なリスク把握に資する枠組み等について検討を進め、次回タスクフォースにて提示することとした。

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