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2回）議事要旨

1．日時・場所

日時：令和元年12月17日（火） 15時00分～17時00分

場所：経済産業省　本館17階第1共用会議室

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(欠席)、楠委員、黒田委員、小林委員、坂下委員、島岡委員、中谷委員、永宮委員、満塩委員、森部委員

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、防衛装備庁、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：　奥家サイバーセキュリティ課長、鴨田サイバーセキュリティ課企画官、尾崎サイバーセキュリティ課課長補佐

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による本TFの検討の方向性について説明した後、自由討議を行った。委員からの意見は以下のとおり。

●属性の考え方について

資料3のp.17の新たな捉え方のところで、ヒト、モノ、データ、システムは、インスタンスとして捉えることが重要ではないかと考える。データは属性データの集まりであり、品質という意味での属性データでもあるからである。

ある人から見れば営業秘密で、ある人から見れば個人情報のように、主体によって属性が変わってくることがあり、なかなか難しい。イベントにしても、例えば、公的部門と、私的事業者で個人情報保護法がどれだけ適用されるかというのもある。他方で、医療のように一気通貫に出来るだけしたいという要請が強い部分もあるため、その辺をどう盛り込んでいくかというところは重要。

主体の議論も非常に参考になるが、難しい。エンドツーエンドで追えるようにしておけば良いということではあるが、どこが主体かと言うと、必ずしも発生したところが主体だとは限らない。日本の銀行の場合は、比較的に営業店の受付がしっかりしていることから信頼できるが、海外の話を聞いていると、フロントが打った情報をどんどん変えていくとのこと。

●場の考え方について
個人情報が大量流出したある事件では、個人情報あるいはプライバシーの問題がありつつ、顧客名簿という意味で営業秘密を不正に侵害したということで、有罪判決になったケースもある。同じデータも一種類のものというよりは場というか、保有者や視点により複数になっているということがある。

今回の資料にある場という定義を作るというのは、使い方が色々であることを考えた時に、結局は一番厳しい条件の場所に合わせて規定されてしまう。

場の大きさや、オーバーラップが大きく影響すると思っている。今回のユースケースでは、電力業界と個人情報で、傘が完全に被っている。それに対して、電力業界で扱っているデータを全く別の業界に持っていくと、電力業界のルールと移転先の業界のルールにおいて、一部ポリシーが一致しないというケースが、当然出てくる。

抽象化して考えるようにしていただいたら良いかと思っている。やはり、場というものは、データ活用を前提としたものと理解しており、どういうルールで使われるものかというのが、場を示している。使われ方が変わるということは、場が変わることではないか。場が変わると、イベントが発生して加工されて、適切な場で、適切なルールに従って使用される。また、そのイベントにより対策レベルも変わる。そういうストーリーで理解すると考えやすい。これらの理由から、一旦抽象化した上で、それぞれの具体的なユースケースを持ち出して、ここは別途、深く考えないといけないというところをブレイクダウンしていく方が良いのではないか。やはり、最後のユースケースに落とし込む時に、本当にこれで大丈夫かというところ、例えば、性善説に従えばこれで大丈夫であるが、性悪説で考えると足りないというような意見が最終的には出ると思うので、そこをどうしていくのかというところを、最後の結論の場で判断することで良いかと考える。起点としては、抽象化のスタートで良いのではないか。

●イベントの考え方について
ペイメントカード業界では、最近ライフサイクル管理が言われてきている。要は入口から出口までをライフサイクルで見ることになるが、結構、真ん中より入口や出口でリスクがあり、事故が起きていると言われている。出口というのは、データを壊す、消去、廃棄などであるが、それが確実に出来ていると本人が思っていても、テクニカルにはそうではないことがあり、そこがリスクになっている。入口のところは、結局、入口に来ないと、属性が分からないというところがある。入ってきて始めて、属性がアサインされるみたいなところだとすると、そこでどういう風に扱ったら良いのかということもあって、属性が定義されていない、アサインされていない情報は、誰がどうやって管理するのか、そもそも属性は誰が付与するのかというところも含めて、結構グレーな世界になっている。そこもしっかり議論をした方が良い

資料3のp.21の図のカテゴリのところにAは電力使用量データ、A´は昼夜人口増減データになっているが、銀行の中でもこの類のものがよく起きている。本当にそれは昼夜人口増減データなのかというように、辿ってみると電力使用量データです、ということがよく起こっている。やはり、この辺は難しい論点である。

年間で多数の情報漏洩案件に対応しているが、漏洩した後に、お客様のアカウント情報などを、無効化しており、二次被害を防止するために、事故が起きてしまった後のライフサイクルの観点も、是非このTFで議論してほしい。

●セキュリティ要件の考え方について

資料 3 の p.20 のレベルの考え方において、レベルは変わるという説明があったが、そうした場合、一番難しいのは、変わることを認識することは可能であるが、ベースが 1 なのか、2 なのか、3 なのか、ベースがどこかということである。

データのセンシティビティが、どのタイミングで上がるのかというのは、かなり重要な論点であり、その整理を間違えると、ほとんどのデータが活用できなくなってしまうのではないかと危惧している。例えばCookieを、どこまで規制するかという論点で若干センシティブな話をすると、検索履歴とか、閲覧履歴は、直ちに個人情報と紐づいていない場合には、これまで割と自由に流通してきた経緯があるが、どこを端緒として本人情報と紐づくかは、ケース・バイ・ケースであり、実際はかなり簡単に紐づき得るものである。検索履歴の中には、どの政党を支持しているのか、あるいは病気を疑っている時に、その治療法を検索する等を含めて、いわゆる要配慮個人情報に当たるものが、かなり分かってしまう。そこも含めて、恐らく仕組みとして統制しているデータの機微度と、そこにインプットされるデータの機微度は全然違っており、それをデータそのものの内容のセンシティビティによりセキュリティレベルを変えろと言われてしまうと、多分世に存在するほとんどのものが最高水準のセキュリティを要求されてしまう。

一般論として、セキュリティ要件を上げていく時にコストが上がると思うが、現状 B to B の在り方も複雑化しており、受益者負担の原則というのが通用しなくなっている状況であるため、コストが上がるのは嫌なので、セキュリティを下げるということが、ほぼ通用しなくなっている状況だと個人的に感じている。従って、コストとは別で、例えば、プライバシーの軸でも良いし、使い勝手が下がってしまうとか、先程のセキュリティを上げようとすることで母集団が特定出来てしまってプライバシーのリスクが上がるので、サンプリングに使えなくなるとか、そういう様々なトレードオフがあるため、そういう色々な意味でのトレードオフをきちんと信頼性の項目の特性、評価軸の中に入れてほしい。

議論の中でセキュリティ要件という言葉を使っていることが問題である気がする。要件を技術的に定めると、要件そのものが陳腐化する、要件は条件によって変わってしまうので、外形的に定めるのは結構難しい。テンプレートを作っていて、この上で整理する、もしくは、リスクアセスメントをすることそのものが、要件ということを基本的な建付けにしておかないと訳が分からなくなる。

センシティブなデータと機械から出る産業データにおいて、セキュリティ要件の考え方が違うと思っており、このフレームワークに産業データを全部入れるというのは、少し違和感がある。産業データの場合は、B to B になりがちであり、当社では利用目的でコントロールしている。

ペイメントのセキュリティ分野で要件に対する考え方の見直しが現在行われており、セキュリティ要件というと、何をどうしなさいということで定義づけることになるが、そういう考え方からオブジェクティブベースという考え方にシフトしている。

●データの信頼性について

状態がトランジションする、情報がマージされたり、抜かれたり、定義が変わったりということを、全部マネジメントすることは無理がある。そこでエンドツーエンドを思い出してみると、要はエントリーしたポイントが分かっていれば、使う時に、そこがトレース出来るようにしておき、最初に生成した人に問合せられるようにしておくなど、エンドのところで確かめられるという形であれば良いのではないか。

資料 3 の p.18 に「データの信頼性」との記載があるが、イベントの信頼性と、場の信頼性だけでなく、誰が作ったのか、誰が持っているのか、誰が管理した情報なのか、というところの、誰が、が信頼できないと、そもそもの信頼が出来ないのではないか。これは認証問題等色々あるが、こういったところを考えていかなければならないため、モデルの中に主体という概念を入れた方が議論は明確になる。

データそのものが流通する前提になった場合、流通した先で適切にコンテクストを理解し、そのデータの特性に応じた利用が出来ない場合も結構ある。今、脅威として、信頼性の低いセンサで得られた情報であったり、悪意を持った人が使った違ったデータを流し込むような脅威は想定しているように見えるが、実はデータ分析における問題はそれだけではなく、ある条件で取得したデータのそもそも母集団に偏りがあったり、その項目に持たせている元々の意味と、後の分析者がそれをどのように理解して分析するかという意識のギャップがあった場合は、仮に全て善意の人で、正しく集計していたとしても、データとして間違えるということはたくさんある。

トラストワージネス は、あくまで信頼される側が示す指標である。それを使ってどうトラストするかというのは、あくまで信頼する側の判断である。この信頼する側の判断は、トラストワージネス だけで決まるわけではなく、それ以外の色々な文脈だとか、前提を踏まえて決まる。セキュリティと言えば高めた方が良い、一方、その暗黙としてその横にコストが必ずある。トラストワージネス と、トラストは全く相対する評価軸であることを、ご存じだと思うが、指摘しておきたい。
製品の図面を下請けに分割して展開したとしても、それらを集めて、将来的に全然違う切り口で見たら、元の製品の性能が想定される可能性があるということは厄介な課題。

●規制・ルールの考え方について
データの使い方に対して規制をかけるか、データそのものに全体のフレームワークとして規制をかけるか、というところは割と根本的な議論である。

データ A からデータ A´に移行する時の遷移過程で、誰がどこまで責任を負い、しかも、その責任の受け渡しに漏れがないか、ということをやらないと、漏れがあればそこで信頼は欠落することになる。その辺のルール化も考えておかなければならない。

社会的利益を大きくしたり小さくしたりするのは、規制の強度により比例する。資料3の前半にある海外の取り組みについて見ていると、技術的な観点と、制度的な観点と、人的な観点で工夫して欲しいとしか読めない。データマネジメントの新たな捉え方が、資料3のp.23に載っているが、マネジメントというのは、管理ではなく、コンプライアンスだと考える。

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