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5回）議事要旨

1．日時・場所

日時：令和3年12月13日（月） 18時00分～19時35分

場所：オンライン開催（Microsoft Teams）

2．出席者

委員　　：岡村委員（座長）、池田委員、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、峰委員、満塩委員、矢野委員

オブザーバ：警察庁、金融庁、総務省、厚生労働省

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、奥田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）」

資料5 パブリックコメントで寄せられた御意見に対する考え方（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。

●用語について

データの「ライフサイクル」という表現は、データの生成から廃棄までを想起する言葉であり、To Beとしてライフサイクル全般のデータマネジメントを目指すことには異論はないが、現状ではライフサイクル全般に渡ってコントロールする枠組みとして描ききれていないと感じており丁寧な補足が必要ではないか。ライフサイクルではなく「データフロー」という表現にするというのも一案。

「コレクティブマネジメント」そのものの概念の解説があると全体が分かりやすいのではないか。DFFT等を考えると、それぞれの場によってライフサイクルが違い、場に応じて適切な処理をするという概念になると思う。

●ユースケース「A-2．高齢者生活支援事業の提供」について

高齢者生活支援事業の提供においてサービス事業者に渡す情報は、個人情報や個人関連情報など、色々な可能性があるのではないか。実務的には、共同利用や委託のような形態が一般的。個別事案の話に実務的なことを持ち込むと具体性が出て良い反面、普遍性がなくなるというジレンマがあるため、そのバランスは今後も検討する必要。また、改正個人

情報保護法を踏まえた記載であることなど、パブコメの際に誤解が無いよう明確にしてほしい。

●ユースケース「A-3. IaaS、PaaS、SaaS等を利用してサービスを提供する例」について
クラウドサービスプロバイダとカスタマとの関係で、いきなり「監査」と書いてしまうと、カスタマがプロバイダに突然監査を申し込むように見える。監査は契約や規約に基づくものであり、実務的には、クラウドサービスプロバイダ自体がシステム監査やセキュリティ監査を受け、その監査報告書をカスタマが監査法人などから有償で取得することでチェックするような形で進んでいる。そのような点を注釈として入れることも考えられる。

資料3　P32の図においてA社サービス利用規約の場が全体を縛っているが、実際はサービス利用規約で縛られるのはA社とユーザの間の契約であり、契約と場の関係の表現が適切ではないのではないか。最初から一枚にしようとするのではなく分けて考えた上で、最終的にそれぞれの場がセロファンのように重なっている様子を上から見たような図になるのではないか。P25の図を代替できるように表現することが首尾一貫性の意味でも必要ではないか。

●今後の第3層TFの進め方について
将来的には、具体的なユースケースとして、コレクティブなことが求められるような場においてどのようなリスク分析をすれば各主体がリスク認識を共有できるのか、体制や利害とかが異なる中で、どのようにコレクティブマネジメントを実現していくのかの深堀にも期待。

製造業の工場における遠隔監視など、OT系のユースケースを入れていけば、広く活用されるのではないか。今後の課題として検討いただきたい。

新たなデータマネジメントのフレームワークが浸透していけば力になるだろうと思う一方で、概念が難しいため、分かりやすいものとすることが、浸透させるうえでは非常に重要。

本プロジェクトは大変野心的であり、色々なそれぞれのシステム間の相互依存関係が複雑になっていく中で、どのように解きほぐしてモデル化していくかということは非常に重要。フレームワークを世に出した後に、どのように具体的に活用していくかという点では、まだまだ多くの課題が残っていると認識。

行政システムにおいても、IaaS、PaaS、SaaSを利用した構成でサービス提供されることが増えてきている。そのような現実に則した事例をモデリングしていただくことが理解の促進に繋がると思う。

●その他
場を主体的にまとめるプレーヤは誰が望ましいか、もう少し議論を重ねた方が良いのではないか。例えば、ユースケース2の場合は誰がやるべきかという議論があった方が良い。

移転の単位を4つに整理しているが、これは結局マネジメントのことを言っており、マネジメントをどのレベルでやっているのかということで整理していくものだと思うので、そのような文章にした方が良いのではないか。

Root of TrustとChain of Trustの話は、水に例えるとRoot of Trustは水源、Chain of Trustは水道管として、その信頼性の担保と考えていくとわかりやすいのではないか。GAIA-XのIDSコネクタには、トラスティッドコネクターというものがあり、それ

がRoot of Trustや、Chain of Trustの考え方に近いので確認すると良いのでないか。

Root of Trustについて、トラストアンカーをいったいどこにおくのかという点が気になっている。センサーデバイスがトラストアンカーになるモデルは、膨大な数のトラストアンカーができることになるため、ワークするのかどうかというところが疑問。まだ議論の途中ということと理解。

各委員からいただいた意見を踏まえて座長に相談し、フレームワーク案に修正を加えた上で、第2回の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