# 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1回）議事要旨

## 1．日時・場所

日時：令和元年7月31日（水） 10時00分～12時00分

場所：経済産業省　別館9階946各省庁共用会議室

## 2．出席者

委員　　：　岡村委員（座長）、池田委員、井原委員、江崎委員(欠席)、菊池委員、楠委員、黒田委員、小林委員、坂下委員、島岡委員(代理：佐藤様)、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：　大臣官房サイバーセキュリティ・情報化審議官　三角審議官、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

## 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　本タスクフォースの議事運営について（案）

資料4　『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3,4による本タスクフォース（TF）の議事運営および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。

●データの属性について

・　全般的にプライバシーに関する観点が不足。また、企業においてはセキュリティポリシーの文化が成熟しているが、データを提供する側や受け取る側の個人で自分のプライバシーポリシーを持っている人はほとんどいない。これに対応する技術がこれから必要になってくる。

・　プライバシーはもちろん大切だが、同時にやはり技術ノウハウ等々の海外流出等々も相次いでいるので、それも併せて考えていかないとならない。また、データの性格を問わず、他社から預かった情報等は、加工し間違いをしたり漏えいをしたりした場合に契約違反に問われ得る。プライバシーは重要ではあるが、それに限ることなく、色々な点から考えていかなければいけない。

・　プライバシーデータに関しては、プライバシーイシューがあるか、ないかくらいで、基本的にはあまり細かく区分をしな

い中で、お互いが信頼できるデータを定義していくのはどうするかという議論が本TFの目的に合っていると思慮。

・ 漏えいした情報の重要性でなく、件数の大小で、漏えいのインパクトが判断される風潮がある。今後の攻撃につながり得る重要な情報漏えいは日々起こり得るが、それらに関しては公表義務もなく、リスク所管部門が、それらの重要な情報の保護を、件数が大きいために報道されがちな顧客の名前だけのようなデータの保護より劣位に置いたセキュリティポリシーを定めていることが多い。情報漏えいに関する責任は、（事業や顧客に対する）インパクトで把握すべき。

・ 産業データについて、データの信憑性や、誰が提供したデータか、というのは重要なファクターであるが、独自のセキュリティ基準を設けて信憑性を担保するために努力している。

●データの加工・流通等について

・ 第3層に誰かがデータを置くと、色々な別の主体がそのデータを置いた本人が意図したものと全く違う使い方をすることにより新たな付加価値を作っていく、というサプライチェーンのイメージが背景にあると理解。データを作った当人がどう意識するかではなくて、データを使う側がそのデータがどれだけ安全に利用できるかということは重要なポイント。

・ データが本来の意図と異なる使われ方をした際に、それを快く思う人と思わない人がいる中で、データの流通そのものが、セキュリティ攻撃ではなくいわゆる炎上のような社会的攻撃を受ける可能性があるということを考えれば、何がしかの枠組みをはめておいた方が良い。

・ 例えば、医療分野では、医療者の共通理解は、データを取り扱う単位が法人の単位ではなく医療者であるという者である。医学教育の現場においても、教育対象である学生は大学法人の構成員ではなく、彼らに対して構成員としての縛りをかけるにはどうするのかという問題もある。法の前提と各分野での運用の実態が必ずしも一致しない中で、一律のルールで守るように制度が組まれて実効性を担保し得ない。

・ クレジットカード加盟店は、PCI基準への準拠よりも取り組みやすいオプションであるカード情報の非保持化を目指すことが多いが、最近では非保持化を達成した加盟店においても、新たな攻撃の手口で情報流出事故が報告されている。これはオンラインスキミングやWebスキミングと呼ばれ、EC加盟店のウエブサイトを標的とする攻撃が世界中で確認されている。

●データを扱う場について

・ データの安全性はクラウドの安全性の議論と似ている。クラウドプロバイダが開示したシステムのセキュリティ対応情報から利用者側が残留リスクを評価し、自身で追加の対策をしてトータルのセキュリティを完結させている。プロバイダのISMSから、プロバイダと利用者の間の共同のISMSを作るというイメージで構成されることになり、その結節ポイントに監査を置いたが、基本は同じようなもの。ただし、クラウドは1対1であるのに対し、第3層の概念は1対多である点に難しさがある。

・ データマネジメントについて、インターネット上でのことか、データ交換基盤というものの設計をある程度前提にしているのか、環境ではなくて仕組みとして議論するかによって、データセキュリティをどうするか、何のためにやるか、ちゃんと実装として落ちるのか、変わってくる。

・ データをクラウドに集め、業界を超えてやりとりすることは、今後とても重要なこと。その際、産業界側は安全サイドに寄せることになるので、単純にはセキュリティのレベルの高い方に寄せて行うことになると考えている。基本的に、標準化された技術を使って暗号化や認証、通信の保護を行っているため、業界によって技術的な面での差はあまりないが、運用面や仕組みでは大きな違いがあると考えられる。このTFでは、一定の基準を作り、最低限これを守ってくださいという形になるのか、それとも別のアウトプットになるのか、認識合わせできるといい。

●データに関わる法律等について

・ 個人情報保護法の影響か、個人情報の該当性という所に議論が集中する傾向があるが、今後はむしろ、全ての情報は個人情報に関係する可能性があることを受け入れた上で、適切に流通するためにはどのような枠組みがあるかということを考えていかなければならない。

・ 同じデータでも、由来する個人のために使う場合や研究などの公益的に使う場合、商用目的で使う場合など、利用されるシチュエーションによって適用される法律や、レギュレーションが異なる。考え方も変わるし、トレーサビリティや要求も違う。データに対して区分という整理をするとき、そうした制度的ハードルを考える必要がある。

・ 米国における NIST SP800-171 への対応についていろいろ課題がある。例えば、どこまで CUI としての性格を持つのかという境界がはっきりしていない。本 TF におけるメタ化に関する議論などに期待。

●データの信頼性について

・ ポイント①について、セキュリティの観点と、データの加工に関する観点は分けて議論すべきではないかと思う。前者に関しては、ISMSを初めとする色々な仕組みや民間のテスト会社も十分あり、成熟してきている。それに対して、データの加工を正しく行うことを保証する仕組みがない。この加工の正しさを測る仕組みが我々には無いと感じている。

・ ポイント②について、真正性（authenticity）という言葉は、一般的にはエンティティが本物であるかを保証する言葉であって、データが正しいかどうかを保証する言葉ではないように思う。データが正しいかどうかを保証する言葉としては、加工が外から確認できるかという概念であるトランスペアレンシーがある。

・ ポイント③について、トレーサビリティは重要。正しくデジタル署名をしてデータを送受信することを担保するCMS (Cryptographic Message Syntax)を初めとする技術がいくつもあるが、クライアント証明書の利用率の低さを鑑みるに、技術的に解決しているnon-repudiationを普及させ、一般的に使えるような仕組みにしていくのは、また別の仕組みのように感じている。

・ 第3層の概念については世界で手が付けられていないため、日本がやるというのは非常に意義があると思う。信頼の構成要素は、プロセスと、どういう社会集団に属しているかと、制度的裏打ちがあるかの3つ。元々、信頼性という言葉は哲学から始まっている。資料4におけるポイント①は、まさにプロセスをいっている。ポイント②は、どの社会集団に属しているかを指している。ポイント③も、どちらかというとポイント①に関連するのかと思っている。ここを落とし込んでいって最後に制度的裏打ちをする／しない、という議論をすれば、フレームワークはまとまると考える。

・ データは目的毎に信頼度が変わってくるため、Peer to Peer でお互い確認しながらデータ交換しないと、信頼性を最終的に担保できないと思っている。

●TFにおける議論の方向性について

- サプライチェーンにおける課題として2つの観点があると考える。新しい状況において新しい問題が発生し、それに対処しなければならないという点と、教科書通りにすればちゃんと動作するものが、教科書通りに作れなくなっている点。このような研究会では、新しい脅威に対する課題を議論すべきだと思うが、現実に直面している問題は、これまで出来ていたことが出来なくなっているという問題のほうがより切迫した脅威である可能性がある。本当に新しい脅威の部分と、これまで出来ていたことが出来なくなっているという点と、両面議論していく必要がある。

- 本 TF のビジョンは非常に広い。色々な要素の議論が入り込んで、錯綜することも考えられる。各国の文書や規格について、どういう観点でこの規格が作られているか、という点を少し整理したほうが良い。

- 新しいセキュリティ対策が考案され、実行されても、それを上回る攻撃の手口が現れ新たな脅威、リスクをもたらす。そのため策定後の定期的なメンテナンスにより、常に新しい脅威への対応策を取り込むことが重要。対策を構築した後のメンテナンスの枠組みを念頭に置いて議論をする必要がある。

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