産業サイバーセキュリティ研究会
WG1『第2層：フィジカル空間とサイバー空間のつながり』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11月27日（水） 9時00分～10時50分

場所：経済産業省　別館11階1111各省庁共用会議室

2．出席者

委員　　：松本委員（座長）、青木委員、石原委員、伊藤委員、岩崎委員、荻野委員、梶屋委員、神余委員、北澤委員、戸枝委員、西貝委員、野口委員、松元委員、渡部委員

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、総務省、厚生労働省、防衛装備庁、国立研究開発法人産業技術総合研究所、独立行政法人情報処理推進機構、技術研究組合制御システムセキュリティセンター、独立行政法人製品評価技術基盤機構、一般財団法人電気安全環境研究所、電子商取引安全技術研究組合、一般財団法人日本情報経済社会推進協会、一般財団法人日本品質保証機構

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、商務情報政策局　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．配布資料

資料1　議事次第・配布資料一覧

資料2　委員名簿

資料3　『第２層：フィジカル空間とサイバー空間のつながり』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　CCDS のサーティフィケーションプログラムについて

4．議事内容

事務局から資料3に基づき本タスクフォース（TF）の検討の方向性について説明し、荻野委員から資料4に基づき説明いただいた後、自由討議を行った。委員からの意見は以下のとおり。

●カテゴライズの考え方について

リカバリ出来る／出来ないの定義は難しい。どのレベルでのリカバリが出来るのか、どの時点でリカバリ出来るのか、という設定によって要求自体がかなり上下する。

資料 3 の p.18 について、影響を分けて捉えるということには賛成だが、人へのダメージと経済的影響への度合いについて、お金と人の命は対等ではなく別次元である。リスク論から言うと人間の死ぬ可能性が 10 の-10 乗から-9 乗に上がることと、1 億円を損失することが意味合いとして整合が取れるものなのか、度合いという考え方をきちんと整理しないと感覚的な尺度になり、混乱を与えてしまう。

資料 3 の p.18 について、個別の機器でのマッピングに違和感がある。同じ機器でも、システムの中で重要な位置づけのものもあれば、別のものでリカバー出来るものもあり、機器単体ではなくシステムで捉えるべき。システム論的なアプローチからマッピングする方向性は大事だが、対外的に納得できるものを整理することは難しい。

個人情報が漏れた際、それと合わせてどういう情報が漏れたかによって損害の大小が変わってくる。秘匿性の高い情報であれば慰謝料は高額になる。最終的にはお金でどう解決するかという話になるが、リカバリの困難性をどう定義づけるかは難しい。

資料 3 の p.21 について、名誉とプライバシーは違う概念である。広く見ると人格権という権利があり、その中にプライバシーや名誉が位置づけられている。大まかにいえば、名誉については、社会や外部からどう思われるのかといった評価を内容とし、プライバシーについては、外部に知られたくない私生活の情報などを内容とするものであるが、少なくともどちらが上という関係にないため、プライバシー/名誉というような位置づけにした方がより正確ではないか。

影響の度合いを考えるにあたって、いわば「質と量」の観点を両方とも入れ込んだ表で整理すれば、それなりに矛盾なく議論できるのではないか。

資料 3 の p.21 について、資産やレピュテーションに対し、生活への影響や社会的な影響はもう少し上位の概念に属しており、資産やレピュテーションに何が起きているのかというような波及効果的なものがあるのではないか。また、個人や家庭内という特定少数に対する被害しか問題にならない場合と、社会に対して問題が起きる場合とがある。社会に対して問題が起きる場合にも、ビルのセキュリティ問題などビルの中という特定された範囲に影響が及ぶケースと、電力プラントが停止するといった影響が出るフィジカル空間を特定しにくい程度の大きな被害が生じるケースがある。特定少数、特定多数、不特定多数というように与えられる影響、その度合いを評価する基準が作れると、生活影響や社会影響に書かれている内容をより正確に分析出来るかもしれない。

リカバリの困難性と経済影響の 2 軸の整理は非常に分かりやすい。また、運用者がシステムをどう使うのかが重要であり、セキュリティ・セーフティ要求という第 3 の軸に運用者の認証の有無という観点が入っており、運用者にきちんと責任を負わせるという形で見ていけるということが非常に良い。

資料 3 の p.18 のマッピングについて、本 TF の対象は第 2 層であり製品だけでなくサービスも関連するため、製品ではなく機能的な部分で整理した方が良いのではないか。ただ、製品と機能をどう表現するかは悩みどころ。

●セキュリティ・セーフティ要求の考え方について
資料 3 の p.22 に示されているように可能性の議論はなかなか難しいため、まずは被害だけで考える方針はよい。整理には、時間/ライフサイクルで追うか、組織/ステークホルダで割るか、空間で分けるくらいしかない。整理する軸があると網羅的な提案ができる。

サイバーリスク保険では、サイバーリスクを全部補償するように見えているかもしれないが、実は個人情報漏えいがベースになっている保険で、こうしたリスクを包括的に補償する保険ではない。人命に関わるところは製造物責任に関わってくるところであるため現状は PL 保険の対象となる。プログラムのバグが原因なのか、サイバー攻撃が原因なのか等、区別していかなければならず、その部分は現時点では判別は困難。P.21 のような社会的なサポートの面から考えた時、保険です

べて補償出来る訳ではないので、カテゴライズ基準に従い、しっかりとリスクを洗出していかなければいけないと考える。

運用の中にネットワークを入れられないかと考える。ネットワーク構成やネットワーク機器の問題は IoT のセキュリティ・セーフティに非常に関係するところであり、ネットワークの認証という話ではなく、ネットワークをどう作っていくか、ネットワークの正確性が、この全体のリスクの大きさを変えるということが分かるものになるとより良い。

本 TF のスコープが、転写における安全性とセキュリティ体制の担保に主眼を置くものであることから考えると、今回提示されたマッピングの細かい議論は不要で、どのように安全性、信頼性を担保するのかというところに話を持っていかないと発散してしまうのではないか。資料 3 の p.25 でまとめられているように、個々の機器やシステムが、どういうレベルで安全性と信頼性を担保していくべきかを一般の方々に示していかなければならない。

個々の機器のマッピングが入ってくると議論が紛糾するため、むしろこういうフィロソフィーの基に資料 3 の p.23 にあるどういうセーフティ・セキュリティ要求があるのかという個別の話に移った方が良いのではないか。

本 TF のまとめ方に関して、p.23 以降のような方向で良いと思うが、CPSF のモデルを使えないか。第 1 層、第 2 層、第 3 層に対して、こういった対策をやりなさいという形でまとめられるときれいである。セーフティ、セキュリティの両方を考えた場合に、第 1 層に入ってくるのは、物理セキュリティと安全が多い。第 3 層は、ほぼサイバーセキュリティ、IT セキュリティ。第 2 層は、しっかりした IoT 機器が必要ということに加え、エンジニアリングが大事。そのように CPSF で対策や要求を整理していったので、その方法でやると整合が取れて分かりやすい。

セキュリティ・セーフティ要求というものが具体的に開示されると、それが攻撃を誘発するといった議論は昔からある。実装はどんどん進歩していくため、例えばコモンクライテリアにおける、何々についてアクセスコントロールの機能を持ちなさい、というような粗いセキュリティ・セーフティ機能要求とすることで、サーティフィケーションの運用で時々の技術に対応していくやり方がある。

近年、製品のライフサイクルが長くなった。また、センサノード等は億の単位で世の中に出回っており、攻撃者が入手することも容易。セキュリティ・セーフティ要求の中のどこかに、ライフサイクル管理を入れるべき。今出たばかりの製品と、5 年先の製品と 10 年先の製品とでは、対応が変わるのでは。

●個別分野から見たカテゴライズの考え方への示唆について
医療機器分野では、FDA が、2 年前くらいからインターオペラブル・デバイスについて、使う側に対して意図する使用を明確に提示する観点からラベリングに注意するよう指示している。医療機器は止まったとしても患者が死んではいけないため、3 軸の中で人命というところをある程度切り分けて要求事項としているところは妥当である。

医療機器では、サイバーセキュリティの中でエンドオブライフ（EOL）とエンドオブサービス（EOS）を定義するよう現在策定中の IMDRF（International Medical Device Regulators Forum） N60 文書で求めている。メーカも、昔は耐用年数というのを保険や製品の償却のベースにしているが、米国では個々の病院で定義している。EOL、EOS をどこまでやるかが問題。

資料 3 の 18 ページにおいて、経済的影響の度合いの軸の上位には、第 4 次行動計画で国民生活と社会経済活動に大きく影響をする重要インフラ分野が挙げられるのではないか。

分野毎に色々な難しさが存在。機器の寿命が長いといっても、管理・サービスをいつまで担保するかというのは別問題だし、いつ止まるかわからないが安いというサービスもあったりする。また、電子証明書やタイムスタンプというセキュリティの基盤となるようなサービスが倒れてしまっては困るため、公的なところのバックアップがあるなど経営状態も含めて安定していないと、そもそもサービスが許されないと決められている業界もある。

●セキュリティ対策等に要するコストの考え方について
セキュリティ対策のコストを上乗せしないことが美徳のようなイメージを持たれては非常に困る。コストは必ずプライスに反映させるべき。我々もセーフティ、セキュリティにコストをかけているが、それをプライスに反映させないことには、セーフティ、セキュリティはビジネスとしては成り立たない。成り立たないということは最終的にはおざなりなる。1 つの方法論として、マークを張ることがブランドとなり、いわゆる付加価値という形でプライスに反映できる。国の方針として「コストは製品の売価に転嫁してください」という方向性を示していただきたい。

海外の製品と日本の製品が戦う時に、セーフティ、セキュリティのコストを一般の消費者に分かりやすくしておかないと、なぜ日本の製品は高いのかという議論になる。セキュリティにかけるべきコストの値ごろ感が分からず稟議も難しいため、経営トップがセキュリティにお金をかけろと言わない限り対策が進まない。コストではなく投資という考えを経営者が持つためには、どこかでブレークスルーが必要である。

セーフティ、セキュリティ、利便性というものに対してはコストがかかるということを、国民全体に理解していただかなければならない。ボランタリーベースではなく、セキュリティやセーフティをやるためには、こうすべきであるということを認識するようなシステムとしていく必要がある。

質と量の問題は、どれだけコストをかけるかに影響を受ける。人命でも、1 つの事故で 1 人の人がなくなることと、1 回で多くの人が亡くなることはインパクトが違う。医療機械の場合、直接亡くなるのは 1 人かもしれないが、その機械に不備があるという可能性があるとその医療を受ける多くの人が一度に不安になるという影響パターンもある。単に直接的な死亡が起きる、起きない以上に人命の問題はそういう影響も考えないといけない。

●認証の考え方について
サイバーセキュリティの世界は日々技術革新が起こっており、技術的な対策も変わっていく状態。その中で、サーティフィケートを発行するという行為が本当に妥当なのか疑問。

国際標準の世界では、applicability の問題の議論を通じて、技術的な内容を詰めてもあまり意味がないという論調になっている。システムインテグレータやアセットオーナなど、人に対して力量などの要件を求め、技術的な要件はそういう人達に任せるという方向性になってきている。いわゆる CoPC(Certification of Personnel Competence)という要員力量認証プログラムなど、細かい技術的なことは要員の力量に任せるべきではないかという方向。

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