産業サイバーセキュリティ研究会
ワーキンググループ1（制度・技術・標準化）（第7回） 議事要旨

1. 日時・場所

日時：令和2年10月15日（木）～10月23日（金）（書面開催）

2. WG1委員等

委員　　：佐々木委員（座長）、岩見委員、上原委員、江崎委員、太田委員、岡村委員、
片山委員、九野委員、小松崎委員、其山委員、高倉委員、坂委員、平田委員、
藤井委員、松尾委員、松本委員、渡部委員

専門委員　：瓜生専門委員、坂下専門委員、田中専門委員

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、外務省、
文部科学省、厚生労働省、農林水産省、国土交通省、防衛装備庁

3. 配布資料

資料１　議事次第・配付資料一覧
資料２　委員名簿
資料３　第２層タスクフォース及びソフトウェアタスクフォースの検討状況等について
資料４　パブリックコメントで寄せられたご意見に対する考え方（案）
資料５　IoT セキュリティ・セーフティ・フレームワーク（案）

4. 議事内容

書面審議の結果、委員からの主な意見は以下のとおり。

- IoT-SSF は「強制力を持つものではない」という言い方がよい。
- IoT-SSF の運用時には、エンドユーザ、SI、製品提供者の責任分界点の明確化が鍵になると思われるため、製品のライフサイクルを意識できるようにすることが必要。また、第2層に対する直接的な対策（ハードウェア堅牢化、マルウェア対策、アクセス制御など）について、機器・サービスによって異なるので詳細に触れることが難しいことを明確にすべき。
- IoT-SSF 活用推進の観点から、活用した組織等へのインセンティブ（税制、補助金等）の検討を。また、人材育成の観点から、情報処理安全確保支援士の必須研修の内容に CPSF 及び本フレームワークの具体的な内容、アセスメント方法を加えることの検討を。さらに、活用推進及び活用人材育成の観点から、上記のインセンティブの推進と併せて CPSF や IoT-SSF を活用したアセスメントやコンサルティングができる企業を認定又は台帳化（サービサー側の人材育成の動機付け）し、活用企業を後押しできる制度の検討を。
- IoT-SSF の中で、「例えば第 2 の観点に係る要求が無くとも、第 1 や第 3 の観点に係る要求により対策を構成することも考え得る。」について、現実には、脆弱性対策を放棄し、運用でカバーすることが常態化していることが気になる。「例えば第 2 の観点に係る要求が無くとも、第 1 や第 3 の観点に係る要求により対策を構成することも考え得る。また、ある観点での対策に時間を要するのであれば他の観点で一時的に補うことも想定

できる。」のような表現で、「常態化させるものではない」ということを記述すべき。

- わかりやすいユースケースの整理を進め、IoT-SSF が有効に使えるような取組みを。
- 様々な IoT 機器がクロスドメインで組み合わせられるようになると、組合せの都度、セキュリティとセーフティのバランスをトータルとして図っていく必要が出てくる。そのような状況で（各ドメインのセキュリティ・セーフティに関する）考え方が整合的であるということは重要であり、今後の展開を期待。
- IoT-SSF の考え方が世の中に貢献し、かつ産業界で利用されるようになるためには、多様なユースケースを早急にまとめ、多様性があることが IoT-SSF の概念の本質であることを理解していただくことが重要。最終的には、第 3 軸の詳細内容が企業ごとの様々な違いを吸収・平準化し、業界・分野ごとのルール・制度・認証・規制等への要望・提言となってあらわれてくれば、この概念が世間に定着したことになる。各業界・企業の事業内容に基づくマッピングに早急に取り組めればよい。
- OSS の適用範囲拡大とともに、頻繁に発生する脆弱性対応等へ個社で対応するのが難しくなる。各社の事例を集めるとともに課題も共有し、共通で対処していけるような仕組みづくりに繋がることを期待。
- OSS 利活用に係る事例集は、非常に重要。ビジネスにおける OSS 利用は今後さらに普及すると想定される一方、OSS は枝葉が広がるうえ、例えば脆弱性が露見した際の影響範囲を確認する手段などは技術的にも簡単ではない。資料 3 では OSS におけるセキュリティの注意事項がうまく整理されており、その内容に沿って利用例などまとめていただければありがたい。

各委員から頂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公開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