参考資料１

ICT サイバーセキュリティ政策分科会（第５回）議事要旨

１．日　時）令和６年４月５日（金）13：00～15：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、新井構成員、上原構成員、栗原構成員、小山構成員、篠田構成員、盛合構成員

【オブザーバー】
内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】
山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当)、小川サイバーセキュリティ統括官室参事官（総括担当)、酒井サイバーセキュリティ統括官室参事官（政策担当)、佐藤サイバーセキュリティ統括官室企画官、道方サイバーセキュリティ統括官室企画官、牧野サイバーセキュリティ統括官室統括補佐、井上サイバーセキュリティ統括官室参事官補佐、宮野サイバーセキュリティ統括官室参事官補佐

【発表者】
本間輝彰（KDDI 株式会社)、安田義明（Open Worldwide Application Security Project（OWASP))、
太田陽基（KDDI 株式会社)、小川博久（株式会社三菱総合研究所）

４．配布資料

資料５－１	令和５年度「通信アプリに含まれうる不正機能の検証に関する実証」について（KDDI）
資料５－２	スマートフォンプライバシーアウトルック X（KDDI）
資料５－３	アプリ診断の取組紹介(OWASP)
資料５－４	e シールの制度化に向けた検討状況について
資料５－５	令和５年度「通信分野における SBOM の導入に向けた調査の請負」について（KDDI）
資料５－６	令和５年度 ISP におけるネットワークセキュリティ技術の導入及び普及促進に関する調査（三菱総合研究所）
参考資料１	利用者情報に関するワーキンググループ（第１回）事務局資料（抜粋）
参考資料２	RPKI の ROA を使ったインターネットにおける不正経路への対策ガイドライン案
参考資料３	DNSSEC による DNS 応答の認証技術ガイドライン案
参考資料４	電子メールのなりすまし対策、迷惑メール対策技術である DMARC 等（SPF、DKIM を含む）のメール認証技術ガイドライン案
参考資料５	ICT サイバーセキュリティ政策分科会第３回　議事要旨

５．議事概要
（１）開会

（２）議題
◆議題（１）「スマートフォンのセキュリティ確保に向けた取組状況」について、KDDI 本間氏より資料５－１及び資料５－２を説明。事務局より参考資料１に沿って、KDDI から提案のあった、SPI の見直しにおいてセキュリティ要素を盛り込む点について、本分科会の議論を踏まえて利用者情報に関するワーキンググループにおいて議論する旨補足説明。OWASP 安田氏より資料５―３について説明。

◆構成員の意見・コメント
新井構成員）

資料５－１の利用者情報の外部送信に係る実態について、アプリの収益としてユーザからの課金もあるが、広告が収益の柱であると認識している。しかし、実際には広告関連情報が外部送信される割合が低いのはなぜか。また、事業者間でアプリの解析能力に差がある点について、技術基準の把握という事業の目的に沿った成果だと思う。その上で、我が国の技術水準自体の底上げをしていくために何をすべきか伺いたい。技術水準の向上のためには教育が中心になると思うが、今後生成 AI を用いたデコンパイルなど、解析ツールによる支援ができれば技術水準の向上や解析能力の属人性の低減に寄与できるのではないかと思う。

KDDI 本間氏）
広告関連情報の外部送信について、新井構成員の御指摘のとおりの部分もある一方で、広告関連情報を必要としないアプリや広告関連情報以外の情報を広告に活用する例もある。もう少し広告関連情報の割合が高いと予想していたが、あくまで詳細結果で確認できた情報の範囲でグラフ化していると捉えていただきたい。また、アプリ解析について、解析事業者の協力を得て実施しているが、いわゆる脆弱性診断のように開発元から依頼を受けて診断しているのではなく、マーケット上のアプリをダウンロードして調査している。解析事業者からも、年々セキュリティ対策に係る機能や技術のレベルが高くなっているため、解析側の技術の向上が大きな課題だと聞いている。解析事業者としては本事業のような解析にビジネスとして投資することは難しいため、本件のような事業を通じて最新の様々なアプリを調査していき、解析スキルを向上させることが重要だと思う。また、生成 AI の活用については御指摘のとおりで、解析事業者とも今後の活用の必要性について話をしている。

後藤主査）
解析の難しさは段々厳しくなっていると思うが、iOS とその他のアプリで開発言語の違うことの影響があるとのことが、実際に解析への影響はどれほど差があるのか。例えばアンドロイドに比べ人件費が何倍かかるなど教えていただきたい。

KDDI 本間氏）
解析事業者は自前でゼロから解析するのではなく、インターネットなどに既にある様々なツールを活用して調査を行っており、Android の方がアプリ解析の手法やツールがインターネットなどで出回っていて充実している。使用言語の観点でも Android は Java、iOS は C 言語だが、解析技術者のスキル的にも Android の方が読みやすく、比較的簡単だと言われている。具体的にどれくらいかお示しすることは難しいが、ある解析事業者の話では iOS はおよそ Android の 1.5 倍ほどではないかと聞いている。

後藤主査）
議題（１）については、KDDI 本間様から、事業を踏まえ SPI にプライバシーだけでなくセキュリティ確保の観点も加えていくべきとの提案があり、OWASP の安田様からもアプリ診断の取組を紹介いただいた。SPI について提案のあった件について、反対やネガティブな意見がないところ、SPI の見直しにおいてセキュリティの観点をしっかり盛り込んでいただくよう、ICT サービスの利用環境に整備に関する研究会 利用者情報に関するワーキンググループにインプットすることとしてよいか。
（特段異議なし（「同意します」とのチャット投稿あり）。）
後藤主査）
それでは、インプットすることとしたい。

◆議題２）「情報通信ネットワークの安全性・信頼性の確保に向けた取組状況」について事務局より資料５－４、KDDI 太田氏より資料５－５、三菱総合研究所 小川氏より資料５－６を説明。

◆構成員の意見・コメント
上原構成員）
e シールに関して、普及について課題があるのではないかと思う。資料５－４では、日常的に使われることを核としてユースケースが記載されていたが、e シールの対象は非常に広く、幅広いフォーマット、データを扱えるようにする必要がある。電子署名がここまで普及するのに苦労したことを考えると、e シールについても制度を作るだけではなく、様々な仕掛けが必要だと思う。検討会の中で普及のために何が必要か議論されているか。

盛合構成員）
e シールのユースケース例について、保証レベルによって総務大臣の認定を取得したものと取得せずに大量発行されるものとが区分されているところ、いずれの場合も e シールにデジタル署名を使うことには変わりないと思うが、その際の安全性の基準について、例えば CRYPTREC に示される暗号や署名アルゴリズムを使うなどといった議論がされていれば教えていただきたい。あわせて、国際基準等、どういったものに依拠して設計をしているかなども教えていただきたい。

酒井参事官）
e シールの普及については上原構成員からの御指摘のとおり、普及させるためには制度だけでなく様々な取組が必要だと考えている。幅広いユースケースを記載しているが、文書の形態のものを認定制度の当面のターゲットとし、発行元の証明が必要なものを選んでいる。気象データや機器測定データなどは時間を要すると認識している。文章の信頼性を確保するためのサービスには様々なものがあるので、e シールに関する技術基準を策定した後、どのサービスが技術基準に合致するか、また、既存サービスにおいてどれほどの対策を講じることで安全性が高まるかなどが明解になっていくと思われる。既存の様々なサービス事業者が制度をうまく活用して普及に繋

げていただけるのではないかと期待している。また、電子署名もタイムスタンプも利用が広がるまでには時間を要したが、電子帳簿保存法の改正により、税務関係文書の保存にあたってタイムスタンプを活用した保存方法が具体的に例示されたことで普及が広がったという側面があった。電子署名、タイムスタンプ、e シールといった各トラストサービスの使い分けについても話が出てくるが、文書作成に関する法令や規制等において、e シールを採用してもらうことで弾みがつくと思う。盛合構成員の御質問について、策定する基準は PKI（公開鍵基盤）でいうところの認証局の技術基準及び運営基準であり、基本的には既に電子署名法、タイムスタンプにおいて策定している基準を踏襲するような形で進めていくことになる。既存のサービスと e シールとの差分として法人の存在確認に関する点が加わることになると思う。電子署名法でも CRYPTREC が参照されており、e シールでも同様とすると思う。これまでの議論の中で、技術基準が満たしているかの確認を外部の審査機関が行うことになっているところ、電子署名、タイムスタンプ、e シールそれぞれの認証局の審査は共通する部分が多いため、可能な限り近い基準にした方が良いのではないかといった指摘もいただいている。そういった議論も踏まえて、今年度具体的な検討を行う。

小山構成員）
SBOM の導入時の運用の負担が大きいと導入が進まないのではないかといった危惧も様々なところで聞く。通信業界の場合、同様のサービスを同じような機器、システムを導入して提供しているという共通性があるが、業界で連携して負担を軽減するような取組ができるのか伺いたい。

新井構成員）
弊社では 2 年程前から社内で開発している特定のシステムに対して SBOM 出力を原則必須化している。様々なツールを入手、活用することで SBOM は簡単に作成できるが、システムの変更が頻繁にあり、また、新しいライブラリや機能を追加したことにより新しいソフトウェアの部品が必要になるような場面も頻繁にあるため、その時点で再度 SBOM を作成し直すことになり、SBOM の維持管理に相当のコスト・体制を要することが知見として得られた。そういった課題に関して、事業を通じて解決策・ヒントがあれば伺いたい。

篠田構成員）
ICSCoE（産業サイバーセキュリティセンター）において、過去数年間 SBOM よりもう少し流度が高い、会社全体でシステムアップデートやシステムの脆弱性把握するようなツールを提供してきた。現在は Excel を用いてシステムの把握を行っている企業が多いが、SBOM を作成しても最終更新が数年前というケースもあると聞く。新井構成員からあったように、依存関係の把握、その管理が Excel でも、ツールを活用しても大変なため、体制に加え、更新のしやすい、把握のしやすいツールは非常に重要だと思う。事業の説明であったツールについて、既存のツールを支援するということであれば、そのツールの開発に意見をするなど一緒に開発に関わるといった考えはあるか。

KDDI 太田氏）
小山構成員からの御質問について、経済産業省においても産業界全体の観点から取り組まれているが、今回通信分野・通信機器の観点で SBOM 事業を実施しており、通信機器ならではの特徴、問題点について、通信事業者や通信機器ベンダなどの関係者とも議論しながら進めていきたい。昨年度の段階でも、通信事業者や海外のベンダにヒアリングし、求められているものと事業で取り組んでいる内容がかけ離れていないよう意見を踏まえながら実施している。最終的に SBOM 作成・運用観点の留意事項を取りまとめる予定だが、経済産業省の手引きと関連する部分もあれば、通信分野独自の部分もあるため、通信業界全体で連携できる点があればよいと思う。今年度もヒアリングを予定しており、その中でうまく連携させていただきたい。新井構成員からの御質問について、御指摘のとおり、SBOM の更新のタイミングや頻度については課題として認識している。海外の機器ベンダにヒアリングをしたところ、ソフトウェアを更新するごとに SBOMを更新した方がいいのではないかという意見が多かったこともあり、取り組んでいく必要がある。一方で頻繁にソフトウェアが更新される場合、それにあわせて SBOM の更新を行うのは非常に難しく、体制面もコスト面も負担となる。意見が分かれるかもしれないが、通信業界・通信分野が他の業界と少し異なる点として、通信機器の安定稼働を重要視しているのもあるため、一般的なシステムに比べるとソフトウェアの更新頻度が低いのではないかと考えている。通信機器に問題が生じた際の影響が非常に大きいため安定稼働を重視し、例えばメジャーアップデートは年 1 回しか実施しないなど、通信事業者・通信機器ならではの特徴を生かした更新の頻度を考えて留意事項に盛り込んでいきたい。篠田構成員からの御質問について、まず弊社では、まだ SBOM を導入しておらず、現在も別の脆弱性管理ツールを使って弊社内のシステムの管理を実施している。やはりアセット情報の入力・更新に人手がかかるためなかなか更新が進まず、リアルタイムで更新できていないという課題がある。今回 SBOM の導入に向けて、課題解決できるかを検証していければよいと思う。ツールについて、私の考えではこの事業の中でこのツールが良いとはなかなか言い切れず、特に国の事業で行っているため特定のベンダのツールが良いと示すのは難しいと考えている。一方で、現時点ではこの事業の中でツールを開発することまではスコープに入っておらず、既存のツールを検証し、ツールの特徴を生かした活用方法について留意事項に盛り込みたいと考えている。

事務局　酒井参事官）

今回の事業では SBOM を導入することで脆弱性の管理が簡単になるのではないかという仮説の下、いくつかのツールを試しているフェーズ。昨年度１年間を通して、通信機器ならではの特性や、現状のツールが黎明期にあり性能や機能もバラバラであること、標準自体も様々なものがあることなどが分かってきたところ。まずはこの調査をしっかり実施していく。

後藤主査）
SBOM のサプライチェーンの観点について、説明のあった富士通の製品に関してはサプライヤの作った SBOM との組み合わせについての議論もあった。また SBOM の課題として管理のコストなどが挙げられていたが、サプライチェーンが広がることでどのような影響があるか、新しい課題が出てくるのかなどサプライチェーン上の課題を伺いたい。

KDDI 太田氏）
令和５年度は、富士通と NEC、そしてサプライヤに参加してもらったが、契約のあるサプライヤが対象であったため、富士通も NEC もサプライヤの部品についてもソースコードが入手できる立場にあり、ソースコードが入手できる状況で SBOM を作成した。今年度、サプライチェーンリスクを考慮する点に関して、現時点でどこまでベンダ、サプライヤに参加してもらうか確定していないが、ベンダ、Tier1、Tier2 の３階層のうち、３階層目の Tier2 については、例えば直接的な契約が無い状況やソースコードが入手できずバイナリーファイルしか入手できない状況など、様々な可能性がある。バイナリーファイルを解析できるツールは限られており、また、バイナリーファイルを解析する場合はソースコードを使った解析よりも精度が落ちてしまうところ、バイナリーファイルしか入手できない状況で SBOMを作成した上で、しっかりと精度の良いものが作成できるかを含めて検証していく必要があると考えている。今年度、契約の有無、ソースコードの入手の可否、バイナリーファイルしか入手できないかといった、契約の関係性の観点も含めて検証していきたい。

後藤主査）
参考資料として配布している３つのガイドライン案の扱いについて、今後の予定を教えていただきたい。

三菱総合研究所 小川氏）
３つのガイドライン案については、発行して終わりではなく、今後の技術的な改定や運用体制も含め検討している。発行後のメンテナンスが可能な団体にホストして公開してもらえるよう調整しているところであり、近日中に公開をしたいと考えている。

（３）閉会

以上