サイバーセキュリティタスクフォース
公衆無線ＬＡＮセキュリティ分科会（第３回）　議事要旨

１　日　時

平成 29 年 12 月 27 日（水）16:00～17:30

２　場　所

総務省８階　第１特別会議室

３　出席者

（構成員）石原構成員、岩浪構成員、上原構成員、佳山構成員、後藤構成員、佐々木構成員、中野構成員、北條構成員、真野構成員、三宅構成員、森井構成員

（オブザーバー）内藤データ通信課長、加藤地域通信振興課長、鈴木情報流通高度化推進室課長補佐、山下内閣サイバーセキュリティセンター参事官補佐

（総務省）谷脇政策統括官（情報セキュリティ担当）、澤田サイバーセキュリティ・情報化審議官、栁島情報流通行政局参事官（行政情報セキュリティ担当）、木村サイバーセキュリティ課長、沼田サイバーセキュリティ・情報化推進室長、福島サイバーセキュリティ課調査官、豊重サイバーセキュリティ課課長補佐

４　配付資料

資料３－１　「公衆無線 LAN セキュリティ分科会」論点整理

５　議　題

（１）開　会

（２）議　題

①　論点整理について

事務局から、資料３－１に基づき、論点整理について説明が行われた。

②　意見交換（前半）

資料３－１（５ページまで）の「論点整理における基本的考え方」及び「検討事項１」について意見交換が行われた。主な意見等は次のとおり。

真野構成員：資料３－１の３ページに記載されている eduroam は、IEEE802.1x を使用している１つのサービスであって、IEEE802.1x とは別の新しい技術ではない点を補足したい。

後藤主査：応用として使用されている例であると理解。

上原構成員：資料３－１の４ページに公衆無線 LAN におけるトレーサビリティを確保する手段として二要素認証が選択肢の一つとして挙げられているが、MAC アドレス以外の何かを取るというニュアンスとなるより適切な言葉があれば、語弊が減る。

また、自治体 Wi-Fi に関するトレーサビリティでは、KYOTO Wi-Fi で起きた議論を踏まえ、既に総務省が公募する際の認証基準として、反映していると理解している。既存の基準と本分科会における基準を整理しておくべき。

KYOTO Wi-Fi で実際に犯罪捜査に使用されたことから、トレーサビリティはある程度必要であるという議論に落ち着いたと理解している。

事務局：総務省の補助金事業としてどう整備をするかの基準は存在するが、本分科会での検討からは独立するものとして考えている。

岩浪構成員：資料３－１の３ページでは、「認証方式について」の検討事項で無線 LAN サービスを踏み台にした攻撃や悪意のある利用者による犯罪予告を防止する目的が記載されてあり、また、５ページでは、「暗号化について」の検討事項で一般的な無線 LAN ユーザーが覗き見をされないようにという目的を挙げている。目的と手段の関係が誤解を招くかもしれないので逆の構成にした方がいいのではないか。また、これは誰に向けた資料なのかがわかりづらいと感じた。

三宅構成員：何のために無線 LAN のセキュリティを高めるかといった目的があり、そのための手段として認証と暗号化の議論があると理解。

佳山構成員：この分科会のアウトプットが、今後前に進むための布石になればよい。何を問題提起して新しい施策として取り組むかを明確にし、関係団体や省庁の取組との紐付けをすることが重要。今回はどのような新しい議論が論点整理の中にあったか、補足いただきたい。

事務局：検討事項として認証、暗号化と同時に、普及について整理している。利便性と安全性のバランスを配慮し、特定のものを推奨するのではなく、さまざまな選択肢の可能性を検討してはどうか、リファレンスデザインを作ってはどうかということを念頭におき、論点整理を行っている。

佳山構成員：同様に考えており、模範事例が幾つかの選択肢を提供する形で今回のアウトプットが出ればよい。誰に対してメリットがあり、誰に対してセキュリティを考えなくてはいけないかを整理しながらアウトプット

を作りたい。

上原構成員：利用者を守る観点では、第一に認証のクレデンシャルやフィッシング等による情報窃取の危険から守るということ。また、盗聴される脅威から利用者を守る一番基本的な技術である SSL を用いれば、安全かどうかを自分で確認することができることを、ユーザーに伝えることが重要。特に、認証の際に正しい相手に対する認証要素を果たしているか確認できる仕組みが必要。

真野構成員：ステークホルダーは、利用者、設置者、サイバー空間の三つ。利用者に対する脅威は通信の盗聴や攻撃を受けること。設置者に対する脅威は設置しているサービスが品質を落とされる、あるいは悪用されること。サイバー空間にとっては、サイバー空間に対する安易な攻撃の可能性を提供されることにより、自分達が攻撃を受けることが脅威。三つのステークホルダーに対してどのような脅威があるか整理すべき。

森井主査代理：公衆無線 LAN の技術によりトレーサビリティが確保できない場合をどう考えるか、議論していただきたい。

佳山構成員：Wi-Fi ごとに異なる ID やパスワードを入れることは、利用者に大きな負荷。一方、eduroam のようなローミングサービスは利便性が非常に高く、本人認証というプロセスを介している。そのため、トレーサビリティ・利便性の両方の面で利用者にとっては良い例であり、是非題材に挙げたい。

中野構成員：総務省で実証実験など実施されている IoT おもてなしクラウド事業と訪日外国人向けの公衆無線 LAN の認証を連携することも考えられる。

森井主査代理：認証を厳密にすればトレーサビリティも確保できるが、利便性とプライバシーのバランスが難しい。さらにコストの面から必ずしも認証ができない場面があり、そこをどう考えるかを整理したい。

真野構成員：Wi-Fi の業界団体である Wi-Fi Alliance においては、三つのユースケースに分けて、議論をしている。一つ目は、利用者が基本的にセキュリティに対し寛容であるケース。二つ目は、図書館等で一時的に使用する際など、セキュリティに若干の不安があるケース。三つ目は、頻繁に使用するためクレデンシャルを発行して欲しいケース。これらの三つに共通していることはシンプルで、なるべくユーザーに簡単に何かをできるようにしたいということと、ユーザーの通信が盗聴されることは必ず止めなければならないという観点。

北條構成員：ユーザーの目的に合わせ、有料になる可能性があるセキュアなものとそうでないものを選択できるようにすべき。どの方式をとると、

何の心配があるかということを明確にして、利用者がわかりやすく選択できるようになるとよい。

③意見交換（後半）

資料３－１（６ページ以降）の「検討事項２」について意見交換が行われた。主な意見等は次のとおり。

上原構成員：利用シーンに応じた提供において、セキュリティに関してある程度許容している状況では、リスクを利用者本人が意識していればよいという議論はあるが、問題は、そのリスクを伝えるタイミングと手段。ベストプラクティスとしては、例えばキャプティブポータルのURLの表示がある。

現在の提供者向けの手引きは細かく書き込まれていないため、ベストプラクティスを一つ出していけばよい。今すぐできることは、正しいキャプティブポータルに着地していることを示せる仕組みを作ること。その先のこととして、IEEE802.1xやアプリを入れるという話がある。

三宅構成員：ユーザーでセキュリティを意識している人は多くない。仕組みとしてセキュアなものを使ってもらえる取組は必要。繋いだ瞬間にセキュアな通信を使用できることが理想であるが、ハードルが高い。ユーザーの意識が低いからといって、そのままでいいという考え方はどうかと思うので、取組は考えていくべき。

真野構成員：ユーザーに安全な通信を利用するよう啓蒙をすることは当然である。さらには、無線LANを設置する人にもリスクがあるとの意識を啓蒙すべき。日本の公衆無線LANの多くは、ベンダーとシステムインテグレーターが最もモチベーションが高いが、クオリティー・オブ・サービスのサスティナビリティに対して重きを置いていないケースが多い。ただし、ESSID、パスワード、認証方式まで書いていると、偽基地局の設置は容易であるため、キャプティブポータルのURLは隠蔽すべき。

森井主査代理：ユーザー自身がセキュアな通信を望んでいるとしても、何がセキュアな通信か判断できない人がほとんどである。セキュアな水準を満たすようにガイドラインやステッカーを与えることも対策の一つ。技術開発要素としては、アクセスポイントが正規のものであるか確認する方法が挙げられる。

後藤主査：技術的な議論を厳密にすると難しいため、よりよい何か他のサービスや取組と組み合わせ、普及することも考えられる。

上原構成員：アプリは、ユーザーに手間をかけさせずに安全な接続ができ、提供者にとってもサポートコストや契約の問題を上手くクリアできる

比較的いい方法。普及を図る観点では、アプリに対して基準を作ってはどうか。

また、公衆無線 LAN では、Web API 認証という共通のアプリケーションの枠組みがあり、クレデンシャルを抜かれるということに対してある程度担保ができる。広域を動き回る観光客や訪日外国人にとって別々のアプリを入れることは大変であるため、例えば Wi-Cert という認証連携の協議会で推している方式のアプリで統一する方法等も考えられる。

森井主査代理：アプリは一つの手段であるが、公衆無線 LAN を使うことが目的ではなく、公衆無線 LAN を使ってユーザーや団体が何をしたいかという目的があってこそのこと。一つのアプリに統一して、デジタル署名等を利用したアクセスポイント認証の共通の枠組みを作ることも考えられる。

石原構成員：実際に、公衆無線 LAN 事業者も VPN アプリを提供することもあるため、VPN アプリに関する要件や仕様を明示して、利用者が判断できるような状態にしていくのも一つの方法。

佳山構成員：訪日外国人がアプリを入れるモチベーションを高められるか。アプリを一度インストールすれば、Wi-Fi や VPN を利用できる機能を提供すると同時に本人確認も行うという手続もリファレンスデザインに組み込んではどうか。

上原構成員：訪日外国人向けのアプリは、航空会社と連携して、入管事業と一緒にクーポンを配ることはどうか。

真野構成員：空港の Wi-Fi と、現在キャリアが提供している Wi-Fi の間の認証連携をすれば、個別アカウントを取得することによりローミングできる。ユーザーにセキュリティの高い通信を使用するよう啓蒙するには、使用前に確認するよう、いかに広告をするか。導入者にセキュリティの高いものを設置するよう啓蒙するには、インセンティブとしてユースケースをどのように出していくか。地方自治体の Wi-Fi が制度支援で普及したように、セキュリティを要件に入れた導入のコストに対しての制度支援が必要。最も良い方法を一つのアウトプットとして出すことは不可能であり、競争領域を無理やり変えることには抵抗があって、例えば、スタジアムはある特定の領域で特定のベンダーが提供するエリアであることから、良いケースとなるだろう。

事前に電子チケットがあれば、オリパラに関係するスタジアムでは、都度関連する施設はログインせずとも快適に利用することができて、連携してくれるキャリアがあれば、キャリアも快適といったサクセス

ストーリーを描くことができる。

参考までに、普及のためのプロモーションでは、Wi-Fi ホームエクスペリエンスというサーティファイドプログラムが昨年立ち上がっており、同時に多数の住宅メーカーの認証を取った。要件は、サイトサーベイをしてアクセスポイントを置くと、家の隅々まで Wi-Fi の電波が届くことが保証されるというもので、認証した住宅メーカーの住宅にはロゴがついている。

例えば、日本が Wi-Fi サーティファイドスタジアムのような認定を作り、認定されたスタジアムではユーザーは非常に快適に Wi-Fi サービスを受けられるようにする。限定したところでもよいので、ユースケースを作り、日本が世界をリードしてほしい。

北條構成員：当社が提供している JAPAN Wi-Fi アプリでは、インストールするタイミングでメールリターン認証により本人確認を行っており、認証連携にも取り組んでいる。アプリを入れれば問題が全て解決するのではなく、暗号化していないエリアでは暗号化されていないエリアのローミングになる。偽 AP に関しては、偽かどうかをアプリ側で認識できるというメリットがある。

アプリを入れることには制限があり、当社のアプリにおいて利用者 400 万人のうち外国人が半数ほど。その中でアクティブに使っている方はさらに少ない状況であるため、アプリをメインに普及させていくことは厳しい。

後藤主査：利用者やエンドユーザ、設置者のほか、別のサービスを提供している人とうまくタッグを組み、セキュリティレベルを認識し合わせることも考えられる。

三宅構成員：我々もアプリを上手く使えばセキュリティを高められると考えたが、一つのアプリで全国の Wi-Fi が利用できるというわけではないので、そこをうまく使えるようにする取組が必要。

Wi-Cert の場合、Wi-Cert のみでは他のところはつながらないことが検討課題。また、事業者の呼びかけのみでは導入してくれない。単にアプリを入れるのではなく、普及させるための取組として何があるかをよく考えるべき。

佐々木構成員：当社はアプリを使わないことをメリットにフリーWi-Fi を提供しているが、アプリを利用するメリットも大きいということは認識しており、方向性を検討している。ログインを容易にするといった意味では、KDDI、NTTBP と当社で認証連携をすれば、全国同じ ID で認証ができることになる。普段は難しいが、オリンピック期間中のみの対応と

して、そのようなことを検討してはどうか。

後藤主査：無線 LAN そのものの技術開発として、偽アクセスポイントを見つけ出す技術開発の動きはあるか。

三宅構成員：技術的にはそれほど難しくはなく、やるとなればどこの会社も入れられるはず。推奨方式として各事業者に検討していただくことも可能。

佳山構成員：技術革新、開発というキーワードでは、データ利活用のためということも一つ題材にしたい。例えば、混雑情報のデータを取り、情報提供するセンシング技術を入れていく際、どのような通信経路でつなげるかということが課題となる。そこで、利用者がつなげる公衆無線 LAN だけでなく、IoT 機器をつなげるための投資であれば、IoT やデータの利活用という意味で投資を促すやり方を議題にできる。

真野構成員：日本で Wi-Fi 無線機を作っているメーカーはほとんどいない。国際基準や世界情勢を見極めて適したものを選択することを啓蒙していく必要がある。

　他方、日本の公衆無線 Wi-Fi は更新の時期に来ており、業界では従来の単純に高速通信重視ではなく効率の良い無線 LAN を開発する方向になっている。例えばセルラーからのオフロードが非常に重要な技術になっており、マルチバンドオペレーションという２つの無線局が実装されている。MVO のルールの改定の議論が FCC や Ofcom、ETSI では既に行われており、Wi-Fi Alliance がそれに対してロビイングしている。

後藤主査：選択肢の拡充、連携させるコンプリメンタリーな技術、サービスを広く組み合わせることで、普及を図ることも考えられる。

（３）閉会

以上