# 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５回）　議事要旨

## １　日　時

平成 30 年３月 16 日（金）10:00～10:50

## 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、神薗構成員、押鐘代理（佳山構成員代理）、後藤構成員、佐々木構成員、中野構成員、吉田代理（北條構成員代理）、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、沼田サイバーセキュリティ・情報化推進室長、渋谷情報流通高度化推進室長、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、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５－１　公衆無線ＬＡＮセキュリティ分科会報告書（案）に対して提出された意見及びその意見に対する公衆無線ＬＡＮセキュリティ分科会の考え方（案）

資料５－２　公衆無線ＬＡＮセキュリティ分科会報告書（案）

## ５　議　題

（１）開　会

（２）議　題

①　報告書（案）に対する意見募集の結果について

事務局から、資料５－１及び資料５－２に基づき、報告書（案）に対して提出された意見及びその意見に対する公衆無線ＬＡＮセキュリティ分科会の考え方（案）及び報告書（案）の修正箇所について説明が行われた。その後、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：資料５－２の２１ページ、加筆されたＶＰＮの形態の書きぶりについて、「コンシューマ向け」とあるが、他のところは「利用者向け」で統一しており、分ける意味はないと思うので、「利用者向け」で統一してはどうか。

事務局：ご指摘のとおりかと思うので、修正については、後ほど後藤主査と相談させていただきたい。

中野構成員：資料５－１の意見４に、ＳＳＩＤはＡｎｙ（見える）から見えないにすることとある。Ａｎｙにすることによって端末が無線ＬＡＮにつながりにくいという事象も実際の現場では起きており、Ａｎｙにするとセキュリティは確かに向上する可能性はあるが、ユーザーの視点では使いにくい場合があるかもしれないことを補足しておきたい。

事務局：ご指摘のとおり、ＳＳＩＤがどうあるべきかについては、利便性と安全性のバランスと考えており、考え方４に、「利便性と安全性のバランスに配慮しつつ」という文言を加えている。

後藤主査：全体として利便性と安全性のバランスを示し、それに関わる個別の技術論ではなく、考え方を示している。

上原構成員：同じく資料５－２の２１ページ、脚注に「2018 年３月時点において、ＴＬＳ１．２が最新バージョンである」とあるが、具体的に、最新バージョンであるべきか、最新バージョン以外はだめかという記載がない。適切な設定についてはＣＲＹＰＴＲＥＣが出しているＴＬＳのガイドラインに示されている旨の記載を加えるか、あるいは、最新バージョンであるべきとするか。最新バージョンであるべきかどうかは議論があり、現状、ＴＬＳ１．０の範囲で少し実装上の工夫をすれば、安全にすることができるという議論もある。ＣＲＹＰＴＲＥＣの出しているガイドラインでは、ＴＬＳ１．０の範囲での設定が示されているので、無線ＬＡＮとしては十分と言える。

　もう一点、資料５－１の考え方８の接続アプリの箇所について。意見８は、認証そのもの、接続アプリのいろいろな機能についての意見であるのに対して、考え方８は、接続アプリが信用できればいいというずれた書きぶりになっている。接続アプリの提供するべき機能についての議論は十分していないが、基本的にはフィッシング対応が一番大きなところであり、もう少し何か書けないか。つまり、ＶＰＮ機能がなければだめだという話ではなく、バックドアへの情報提供は接続アプリを信頼すれば大丈夫という話、あるいは、暗号化が必ずオンになっているか確認しなくてはいけない機能があるかどうかという話も少し違うと思うので、接続アプリの信頼性を担保する仕組みが何を指すかを、もう

少し示すことはできないか。

後藤主査：まず、ＴＬＳに関する表現について、確かに単純に最新バージョンであればいいということもなく、世の中の別のアプリでは最新にするとダウンする場合もあるので、うまい表現が必要かと思う。ＣＲＹＰＴＲＥＣに関して表現を追加することは検討してよいか。

事務局：ＴＬＳ１．２にすべきとは考えておらず、ＳＳＬと相対的に比べたときにＴＬＳが適当であると示しているのは、ＩＰＡにおいてこのような示し方がされているのを見つつ、単にＴＬＳと書いている。

ＣＲＹＰＴＲＥＣに関して表現を追加することについては、後ほど後藤主査と相談させていただきたい。

後藤主査：もう一点、意見８の考え方についてはどうか。細かい議論になるところは、考え方としてはあまりふさわしくなく、何か一言でうまく言えればよいが。例えば、仕組みなどの幅広い検討が必要であるといった考え方を示すのはどうか。

神薗構成員：意見８は、例えば、認証した場合でも、攻撃者がその中に入っていた場合に、ＡＲＰスプーフィングによる攻撃で中間者攻撃ができることを言っていると思う。アクセスポイントとして認証したということは、正規のアクセスポイントを使ったという担保になるだけで、個人の通信の漏えいが守られるわけではないことをどこか明記しないといけないと読める。正しい認証をしたからといって、完全に安全であるわけではないことを書くと、上側のところは認識が合うと感じた。

上原構成員：意見８の上側の意見は、アクセスポイントに対して、利用者が他の利用者になりすます危険のことを言っているのではないか。改めて読むと、どちらかというと提供者が不正に利用される危険のことを言っている気がする。

後藤主査：利用者に向けていろいろな選択肢を与えると同時に、提供者側が工夫をしましょうという点。利用者も提供者も注意しましょうということはもちろん取組として入っているということで整理したい。

石原構成員：参考資料１２で、イメージ図の生徒から攻撃者に流れているところが「暗号化キー」になっている。ＰＳＫ方式は、事前共有鍵を共有しており、これでよく使われるのがパスフレーズ。パスフレーズから、実際に暗号化する暗号化キーが生成されるので、ここで書かれている「暗号化キー」は「パスフレーズ」に修正したほうがよい。

参考資料２４でも「暗号鍵」とあるが、ここでは事前共有鍵、いわゆるパスフレーズのことを言っているので、こちらもあわせて修正を検討いただければと思う。

後藤主査：もう一度チェックし、修正することとしたい。
三宅構成員：資料５－１の意見８の下側に、ＳＩＭが「店頭奥等で組織的にコピーされていた場合」とあり、ＳＩＭがコピーできるようなことが書いてあるが、このようなことは技術的に困難であると申しておきたい。通信事業者として、このような問題が存在していると捉えられることに不安がある。このことについて、パブリックコメントの考え方に何も触れられていないことが気になる。
事務局：ここは、公衆無線ＬＡＮセキュリティ分科会の考え方として示していただきたく、ご議論いただきたい。
三宅構成員：パブリックコメントの考え方として、技術的内容について細かいところを議論する気はないが、パブリックコメントを読んだ人が「コピーできる」と信じてしまうことが、通信事業者の立場からの懸念としてある。
事務局：本分科会の議事要旨は公開しており、そのような発言があったことを書きとめることはできる。
三宅構成員：それで結構なので、残していただきたい。
後藤主査：議事要旨で我々の意図を示すことにしたい。報告書案等の修正については、主査一任とさせていただきたい。

② その他

公衆無線 LAN セキュリティ分科会の検討結果については、後藤主査から、親会であるサイバーセキュリティタスクフォースに報告することとなった。

また、谷脇政策統括官から挨拶があった。

（３）閉会

以上