事例 A-4

（１）タイトル：無線 LAN の脆弱性

（２）本文：

２００８年９月、大学のある研究者 A が、その当時、無線 LAN で最も使用されていた暗号方式 WEP を一瞬で解読する方法を実証したとして、コンピュータセキュリティの国際会議で発表を行った。

無線 LAN の対象暗号を解読する方法としては、既に別の大学研究者から発表されていたが、その方法では、通常の環境では解読が難しく、短時間で解読するためには、特別な仕掛けが必要があった。 これに対して、今回の手法は、通常の通信環境下において暗号鍵を作成して、極めて短時間で解読できる事が特徴であった。

研究成果は、多いに世の注目する事となったが、この成果を発表するまでに、研究者 A は、問題を抱えていた。

例えば、この発表の為に、研究者 A は、独自のアルゴリズムに基づくプログラムを開発し、さらに実験室だけでなく、実際に、空港や駅等で使用されている公衆無線 LAN 環境下においても実験を行い、通常の PC を用いて鍵の解読が可能であることを示そうと計画したが、断念した。その理由は、この実験が電波法に抵触する可能性があったからである。一般に、無線を傍受する事自体は法律に触れる事は無いが、内容および傍受している事自体を第３者に公表する事は電波法５９条に抵触し、さらに、暗号化された公衆無線 LAN に関しては、電波法１０９条２項も抵触する可能性があるからである。もし、公衆無線 LAN における実験が可能であり、その脆弱性を実際に示す事が出来ていたら、より広い議論を巻き起こせたのではないかとの思いが残った。

実は、研究者 A は、この研究に関しては、かなり以前に完成させていたが、発表の時期で悩んでいたのだ。WEP 方式の無力化を指摘し、より高度な暗号方式の使用を強く進めることで、研究者としての業績を上げ、責務は果たせるかもしれないが、その当時、WEP 方式はすでに多くの民生機器に使用されており、しかも、それらの機器は他の暗号方式をサポートしておらず、他の暗号方式への移行が出来ない状況があり、発表による産業界

の混乱が予想されたからである。そのため、発表の時期を延ばしていたのであるが、民生機器が改良され、高度な暗号方式への対応が可能となる体制が整ったことを見て、WEP 方式の使用禁止を呼びかける良いタイミングと判断したのである。

また研究者 A は、開発したプログラムを使った簡易な暗号解析ツールが開発されることを恐れ、プログラムの公開について見合わせた。ただし、WEP を解読するためのツールは既に出回っており、論文を参考にすれば他の人間が同様のツールを簡単に開発することも可能だとして、早急に高度な暗号への意向を、国際会議に集まった人々やマスメディアに呼びかけた。

ソフトウエアの脆弱性は、いつでも存在する。その場合、上記のように、その脆弱性を公表することが社会の混乱を生む事になるケースが多く、日本には、脆弱情報を発見者から報告を受け、ソフトウエア製品開発者による対策が準備できた段階で公開する「脆弱性情報ハンドリング制度」(1)がある。一般公表前に脆弱性関連情報を製品開発者に連絡し、対応（パッチ、ワークアラウンドなどの作成）を依頼できる。同時に、製品開発者に加えて海外の関係機関とも連携し、脆弱性関連情報を全世界で同時に公表するために、一般公表日を調整することが可能となっている。

（３）考えてみよう。

(1)あなたが、研究者 A の立場にいたら、研究者としての成果を出す事と、社会環境を考慮して発表時期を延ばす事と、どちらを選びますか？

(2)「脆弱性情報ハンドリング制度」での取り組み内容について、調べてみましょう。

付属資料

(1)事例 A-4-1：電波法

(2)事例 A-4-2：参考文献

事例 A-4-1

★電波法　第５９条（秘密の保護）　何人も法律の別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第４条第１項又は第１６４条第２項の通信であるものを除く。第１０９条並びに第１０９条の２第２項及び第３項において同じ。）を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。

★ 電波法　第１０９条の２　暗号通信を傍受した者または暗号通信を媒介する者であって当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、１年以下の懲役または５０万円以下の罰金に処する。

事例 A-4-2

参考文献

(1) 情報セキュリティ早期警戒パートナーシップガイドライン-2016 年版
https://www.ipa.go.jp/security/ciadr/partnership_guide.html