事例 C-2

（１）タイトル：パソコン遠隔操作事件

（２）本文：

他人の PC に対して遠隔操作を行い、殺害予告などを行ったサイバー事件が多数、発生している。

意図せず犯罪予告に加担させられた PC を持つ人は少なくとも 5 人にのぼり、犯行の手口としては以下の 2 つに分けられる。5 人のうち、1 人はウェブサイトのセキュリティの不備をついた WWW の攻撃手法の一つである CSRF（Cross site request forgeries）をしかけられた。その他の所有者は、トロイの木馬の一種である iesys.exe を仕込まれたアプリケーションソフトをダウンロード・実行し、PC が遠隔操作された。これらの操られた PC から、少なくとも 13 件の襲撃または殺害予告を行わせた［1]。

このうち、7 件の襲撃または殺害予告に関しては、書き込み時のログに残っていた IP アドレスをもとに 4 名が逮捕された。この 4 名は、踏み台にされただけであったが、警察側は、IP アドレスを人間の指紋と同様に取り扱ってしまっていたため、誤認逮捕につながった［2]。真犯人自身は、TCP/IP における接続経路の匿名化を実現するための規格である Tor (The Onion Router)を利用して複数の海外のサーバーを経由して掲示板にアクセスしており、自分の IP アドレスを隠蔽していたため、すぐに真犯人を特定することができなかった。

（３）考えてみよう

(1) 今回利用された手口は、すべてのものがつながることを想定している IoT でも注意すべきものであることが指摘されている。例えば、国内で販売されているルータの大半は、LAN 側からのアクセスは使用者からのアクセスのみを想定しており、WAN 側からのアクセスに対するセキュリティは皆無となっている［3]。仮に使用していたルータが、このようなセキュリティを考慮したものとして販売されていれば、今回の事件は防げたかもしれない。いま、あなたが、ルータの開発者である

場合、技術者として気をつけるべきことは何か？考えてみよう。

(2) 警察側は IP アドレスを人間の指紋と同様に取り扱ったが、IP アドレスが成りすましされ得るということを知っていれば、今回の誤認逮捕は防げたかもしれない。セキュリティに従事した技術者であれば当然のように知っていることであっても、異なる分野で働いている人にとっては想像できないこともあるだろう。仮にあなたが、セキュリティに従事した技術者である場合、異なる分野で働いている人に対して、考慮すべきセキュリティ情報をどのように浸透させていくべきか？考えてみよう。

付属資料

（１）事例 C-2-1：参考文献

事例 C-2-1

参考文献

1) https://ja.wikipedia.org/wiki/パソコン遠隔操作事件

2) http://takagi-hiromitsu.jp/misc/misidentification2012/tokyo.pdf、インターネットを利用した犯行予告事件における警察捜査の問題点等について, 警視庁

3) 西部；IoT 機器の脆弱性対応を考える～BB ルータ脆弱性を悪用したサイバー攻撃対処事例から～, IoT セキュリティフォーラム 2015.