悪意のあるデバイス Bad USB による攻撃のリスク調査

山本　拓巳 †　　菊池　浩明 †

† 明治大学総合数理学部　先端メディアサイエンス学科

1　はじめに

BadUSB は PC に危害を加えることを目的として作られた USB デバイスである．一見するとただの USB メモリだが，PC に挿すとキーボードと認識され攻撃者の仕組んだ操作が勝手に行われる．USB メモリを介して感染するコンピュータウイルスではなく，オートラン機能を悪用している訳でもない．USB メモリにおいて PC の CPU に該当するファームウェアを書き換えることで悪意のある動作を行わせる．ファームウェアが改ざんされているので，ウイルス対策ソフトでの検出が出来ない．デバイスドライバのインストールも多くの場合自動で行われ，表示も短時間しかされないので注意深く見ていなければ見落としてしまう．

BadUSB の脅威は，通常の USB と見分けがつかず，不正に PC が操作されてもそれに気づかないことである．不正操作に気づくには，PC の利用経験の長さやセキュリティに関する知識の有無が関係すると考えられる．そこで，本研究では，どのような不正行為ならば気づかれにくいか，セキュリティの知識があれば不正行為を検出できるか，といった疑問に答えて，BadUSB によるリスクの大きさを明らかにすることを目的とする．そのために，31 人の被験者に対して評価実験とセキュリティ指向度の調査を行った．これらのデータから被験者の傾向，BadUSB の脅威度などの関係性を明らかにする．

2　評価実験・アンケートの実施

2.1　評価実験

本実験では Arduino を使って次の 5 つの BadUSB を実装した．Arduino のキーボードとマウスを操作するライブラリを活用した．

(1) マウスをランダムな方向にランダムな周期で動かす
(2) カメラアプリを起動し，1 枚写真を撮影する
(3) 何もなし（比較用）
(4) テキストファイルを作成して中身に記入した後，拡張子を変更する
(5) PC を再起動させる

これらの 5 つの BadUSB について，被験者は順番に挿して，それぞれがどのような挙動をしているのかを答える．実験時には被験者が BadUSB を挿してから答えを記入し終わるまでの時間を計測した．実験後にはアンケートを実施し，名前，学年，性別，コンピュータ経験年数，使用 OS，使用ブラウザ，BadUSB への認知を確認し，実験の正解を提示してから各 BadUSB の脅威度を 5 段階で評価する（以降脅威度を T とおく）．加えて次節で述べるセキュリティ指向度調査を行う．

2.2　IT 指向度調査

IT に関する以下の 3 つの事項を提示し，経験があるものの数で IT 指向度を測る．

i) 自身のコンピュータで OS のインストールまたは再インストールを行った
ii) 家のネットワーク設定をした
iii) ウェブページを作成した

2.3　セキュリティ指向度調査 (SeBIS)

SeBIS[1] と呼ばれるセキュリティ指向度調査では，「席を離れる際にスクリーンロックを自動で実行する」等の 18 問の質問について，しない (1)，まれに (2)，時々 (3)，頻繁に (4)，常に (5) の 5 つから当てはまるものを選び，合計したものをセキュリティ指向度として算出する．

3　実験結果の分析

3.1　評価実験の実験データ

評価実験とセキュリティ指向度調査で得られたデータから，セキュリティ意識のレベルの違いによって，どういった攻撃が脅威になるのか明らかにしていく．

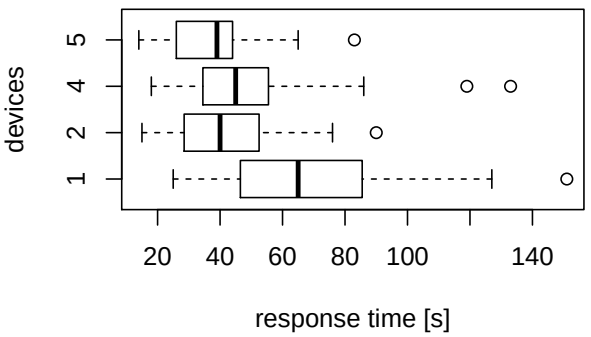

図 1　4 つのデバイスについての被験者の回答時間分布

表 1　評価実験における平均正答率と平均脅威度

	(1)	(2)	(4)	(5)	平均	最大	最低
正解度	66.1	71.0	51.6	100	72.2	100.0	37.5
脅威度	2.2	4.5	3.4	3.3	3.3	4.0	3.0

図 1 に各 BadUSB に対する回答時間を示す．USB 番号は 2.1 で述べた BadUSB に対応している．いくつか

Risk Evaulation of threat by malicious device BadUSB.

†Takumi YAMAMOTO　†Hiroaki KIKUCHI

†Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

表 2　(1) の正答率と脅威度の分割表

	(1)					(2)					(4)					(5)				
T	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
○	2	3	2	0	2	0	0	1	0	2	0	1	1	2	1	2	6	8	10	5
△	1	2	0	0	0	0	0	1	2	9	0	6	4	8	2	0	0	0	0	0
×	4	10	4	1	0	0	2	1	3	10	0	1	2	2	1	0	0	0	0	0

の外れ値が見られるが，これは不正動作が行われた後に PC 内のフォルダを一つずつ確認した数名の被験者である．(2) や (5) といった目に見えてわかりやすいものはあまり回答まで時間がかかっていない．逆にマウス操作のような地味なものはかなり時間がかかっている．

表 1 に各 BadUSB に対するそれぞれの平均正解度と平均脅威度を示す．正解度 (Accuracy) は (○の人数 + △の人数*0.5)*100/被験者数と定義する．脅威度は 1 が最も脅威度が低く，5 が最も高い．平均正解度の内，最も高いのが (5) の 100 %，最も低い正答率は (4) の 51.6 % だった．平均脅威度について，(2) の脅威度が最も高い．(4) と (5) の脅威度にそれほど差は出なかったが，(1) に高い脅威度をつける被験者はほとんどいなかった．(1) はマウスを操作するだけのものであり，正解度に関わらず脅威に感じる人が少なかったと思われる．(2) は最も脅威度が高くなっているが，正解度を見ると 71.0 % と 2 番目に高い．対して最も正解度の低い (4) は脅威度は 3.4 とそれほど高くない．被験者は自分が気づかなかったものより，目に見えてかつ顔写真といった情報を取られる方が脅威に感じると考えられる．

3.2　IT 指向度調査・セキュリティ指向度調査のデータ

表 3　IT 指向度の分布

IT 指向度	0	1	2	3
人数	4	12	10	5

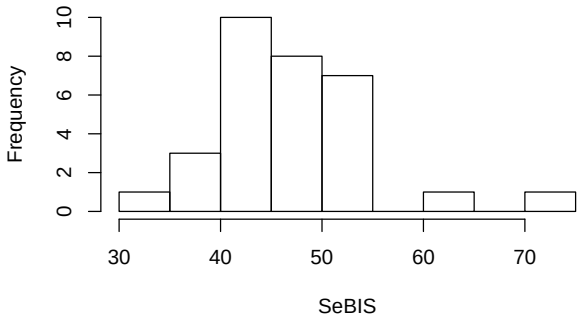

図 2　セキュリティ指向度 SeBIS の分布

表 3 に IT 指向度，図 2 にセキュリティ指向度の分布を示す．それぞれの指向度平均は 1.5，47 である．

3.3　評価実験の実験データに対する考察

図 3 に SeBIS と正解度の散布図を示す．SeBIS が幅広く分布しているのに対して，正解度が平均の 75 %付近に集中している．相関係数は 0.2 で，両者には弱い正の相関がある．

表 4 に SeBIS S の平均値 $\mu(S)$ 以上か否かによって，不正デバイスを正しく認識した被験者数を示す．それぞれ，平均正解度 $\mu(A)$ と平均脅威度 $\mu(T)$ との対応を示している．SeBIS によって被害が変わるか，自由度 1 のカイ二乗検定を行った．p 値はそれぞれ 0.6，0.9 であり，有意水準 0.05 を大きく超えたため，セキュリティ指向度と不正デバイスの認知率は独立である帰無仮説が受理された．

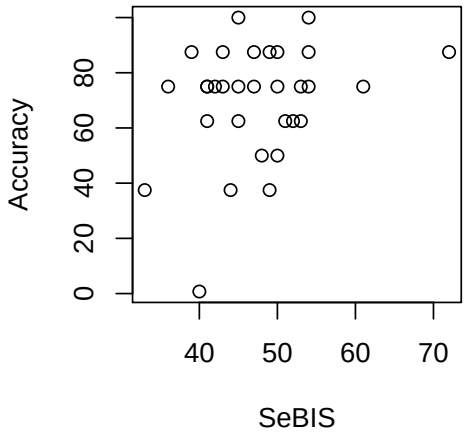

図 3　セキュリティ指向度に対する正解度の散布図

表 4　SeBIS と正解度，脅威度の分割表及びカイ検定の結果

	正解度			脅威度		
	$A < \mu(A)$	$A \geq \mu(A)$	p 値	$T < \mu(T)$	$T \geq \mu(T)$	p 値
$S < \mu(S)$	4	10	0.6	8	6	0.9
$S \geq \mu(S)$	6	11		7	10	

4　まとめ

本研究によって，一部を除いてセキュリティ指向度と BadUSB への認知に関連性はなく，セキュリティ指向度によって攻撃のリスクが高くなるわけではないことが明らかになった．

本実験では被験者は必ず BadUSB を挿すと仮定した状況だったが，BadUSB のリスクを明らかにするには被験者は不正デバイスの正体を知らない状況でどうするかを調査する必要がある．より実際の状態に近づけた状況での評価の実施を今後の課題とする．

参考文献

[1] Matthew Tischer, et. al, ”Users Really Do Plug in USB Drives They Find”, ACM CHI’15, 2015.

[2] S. Egelman and E. Peer, ”Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS),” in SIGCHI Conference on Human Factors in Computing Systems (CHI ’15). ACM, 2015.