6X-01

Android擬似マルウェアによるパーミッションとリスクの関係の学習の有効性評価

加藤　真†　　松浦　佐江子‡

芝浦工業大学大学院　理工学研究科　電気電子情報工学専攻†‡

1.はじめに

Android マルウェアの一つに，アプリケーションが要求するパーミッション（情報やハードウェア機能等へのアクセス権限）の範囲で悪事を働くものがある．パーミッションは，アプリケーションインストール時にそれがマルウェアか見極める判断要素の一つである．しかし，ユーザの多くはパーミッションを許可することで読み書き可能になる情報や実行可能になる機能，それらの行為の組み合わせから発生し得る脅威，脅威によるリスクが分からないためマルウェアの侵入を許している．

現在，上述したマルウェアから身を守るためのセキュリティ知識の学習に関する研究はあまり行われていない．しかし，ユーザは増加の一途を辿っており，幅広い層に使用されているため，セキュリティ学習は重要である．

そこで我々は今までに，Android 擬似マルウェアを用いてリスクを擬似体験することで，どんなリスクがどんな行為から発生し，その行為の原因たるパーミッションは何かという関係性を学習することを目的とした学習方法を提案してきた[1]．本稿では，提案手法を基に開発した Android 用学習アプリケーションを用いて評価実験を行い，その学習方法の有効性を議論する．

2.Androidにおける資産・脅威・リスク

情報セキュリティ評価基準の Common Criteria[2]では，「脅威は，資産（所有者が一般に価値を認めるエンティティ）に対する脅威エージェント（資産に悪影響を及ぼす行為を行うことの出来るエンティティ）の有害なアクションから構成される．有害なアクションとは脅威エージェントが資産に対して行うアクションであり，資産の 1 つ以上の特性に影響を与える．資産への影響に基づいて，脅威から資産に対するリスクが生じる．」とセキュリティの概念と関係を定義している．これを基に，マルウェアから身を守るために必要な知識である Android における資産・脅威・リスクを分析し，図 1に整理した．

アプリケーション実行の観点から資産を，アプリケーション実行の環境である「端末」，その時の「設定」，アプリケーションが使用できるユーザの「情報」の 3 つに大別した．これらの資産は細分され 48 種類ある．

そして，資産に対して実行できるアクションがある．端末に対してはシステムやハードウェア機能の使用，設定に対しては読み書き，情報に対しては読み書きと通信による情報の送信である．これらの実行にはパーミッションが必要であり資産を保護しているが，それが許可されアクションが不正に実行されると，端末不正使用，設定改竄，情報改竄，情報漏洩の脅威が発生する．

脅威から発生するリスクは，脅威の対象である資産によってどんな影響があるのかによってその性質が，また影響する範囲やリスク発生後に元の状態に復元できるか，リスク発生を認識できるかによってその規模が異なる．

よって，これら資産・脅威・リスクの関係を学習することで，パーミッションを許可することで資産に対してどんなアクションを実行でき，どんな脅威・リスクが発生するか分かり，マルウェアから身を守ることができる．

3.パーミッションとリスクの関係の学習方法

資産・脅威・リスクの関係を学習するためのアプリケーションを開発した．学習アプリケーションは，学習前に必要な前提知識（例えばパーミッションとは何か，資産や脅威などのキーワードなど）を学習する部分と，リスク擬似体験とそのリスクで影響を受ける資産，影響を与える脅威との関係の学習を脅威毎，及び脅威が対象とする資産の種類毎に行うエクササイズで構成される．

リスク擬似体験では，擬似マルウェアの擬似的な有害アクションの挙動（脅威）によって，資産にどんな影響（リスク）が及んだかを，具体値を用いて影響を可視化し体験させる．セキュリティ学習において重要なのは，発生リスクを危険，怖いと思えるかどうかであるため，擬似体験時にはユーザの資産を用いてリスク発生を演出する．また，擬似マルウェアを脅威毎，及び脅威が対象とする資産の種類毎に用意し，同じ脅威でも資産によってリスクが異なることを体験する．

そして擬似体験後に，実行されたアクションを制限するパーミッションを示すことで，パーミッションとアクションの関係を学習し，どんなリスクがどのアクションの組み合わせから発生したかを示すことで，アクションとリスクの関係を学習する．また，擬似体験した脅威が対象とする他の資産を示すことで，網羅的に脅威に対する資産を学習する．このように学習し，資産・脅威・リスクの関係を知識として体系化する．

4.評価実験

4.1. 実験概要

2 つの観点について実験した．一つはリスクを擬似体験して学習した場合とない場合において，学習後のテスト結果を比較し，リスク擬似体験による学習効果があるかを確認すること，もう一つは，学習前と後で同じテストを行い，その結果を比較し，学習によって資産・脅威・リスクの関係を知識として体系化できたかを確認することである．擬似体験無しの場合は，有りの場合と同じ擬似マルウェアを題材に要求するパーミッションから，実行可能なアクションとその組み合わせから発生し得るリスクの組み合わせの関係をエクササイズで学習する．

テストでは，パーミッションの許可により実行可能になるアクション，発生するリスク，そのリスクを実現するアクションの組み合わせを解答させ，パーミッション

Evaluating Effectiveness of Method for Learning Relationship between Android Permissions and Risks by Pseudo Android Malware

† Makoto Kato ‡ Saeko Matsuura

†‡ Division of Electrical Engineering and Computer Science, Graduate School of Engineering and Science, Shibaura Institute of Technology

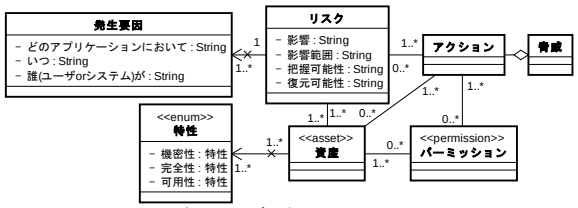

図 1 資産・脅威・リスクの関係

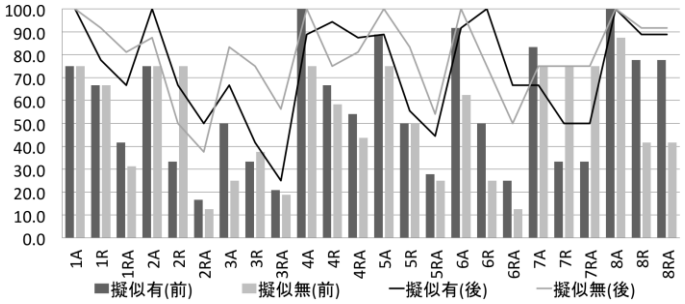

図 2 テストの各問題における平均正答率

とアクション及びアクションとリスクの関係を学習出来ているかを確認する．問題は各脅威について一問ずつ出題し，それは擬似マルウェアで学習した内容を理解しているかを確認する基本問題 4 問，擬似マルウェアでは扱わなかったパーミッションやアクションの組み合わせについて，学習したことを応用して考えられるか確認する発展問題 4 問の計 8 問から構成される．

4.2. 結果と考察

図 2は擬似体験の有無及び学習の前後における各問題での平均正答率を表しており，横軸は問題の番号と種類を表し，A はパーミッションからアクション，R はリスク，RA はリスクを発生させるアクションの組み合わせ，をそれぞれ答える問題である．被験者は Android ユーザで，擬似体験有りが 6 人，無しが 4 人である．

図 2からリスクの擬似体験の有無に関わらず正答率が増加しており，基本問題も発展問題も正答率が増加しているため学習効果があり，また応用して考える能力を得られたことがわかる．どの学習者も学習の前後で全体的に 20%前後向上しており，被験者の中には，Android アプリケーション開発の経験者や学習前からパーミッションの知識を持つ者がいたが，それらの属性に関わらず正答率は増加している．特に問題 A は正答率が平均して約 9 割まで増加しており，点数のばらつきが減少傾向にあるためパーミッションとアクションの関係については学習効果があると言える．問題 R 及び問題 RA についても正答率は増加傾向にはあるものの，問題 A ほど正答率は高くなく，特に問題 RA の正答率は低い．また，擬似体験有りと無しではほとんど正答率に差はなく，擬似体験による学習効果は見られない．

問題 RA の中で正答率の低い問題の解答を分析した結果，学習者に共通する 2 つの誤った認識を発見した．一つは情報取得アクションのみで漏洩のリスクが発生するというもの，もう一つは情報及び設定の変更アクションのみで改竄のリスクが発生するというものである．漏洩は取得情報を外部送信するアクション，改竄は取得情報・設定を変更するアクションがなければそれらは発生しないが，これらが必要であるという認識が欠落している．

擬似体験無しの場合が有りの場合と比べ問題 RA の正答率が高いのは，有りの学習者はみなエクササイズを一度ずつしか学習しなかったのに対し，無しの学習者はみな繰り返し学習しており，平均して約 45 分長く学習したからであると考える．また，実験後インタビューでは，有りの学習者の多くからリスク擬似体験部分と学習部分の繋がりが分かりにくいという回答を得られた．しかし，リスクの怖さはよくわかったという回答を得られており，リスクの怖さを理解させることは成功しているが，それを発生させるアクションの組み合わせと紐付けられていないことがわかる．これは，リスクの怖さを学習させるためのリスク発生時の具体値，パーミッションとアクションの関係，アクションとリスクの関係で情報を分割し，一度に表示する情報量を抑えるようにしたために，それらの繋がりが薄れてしまったことが原因であると考える．

5. 関連研究

新谷ら[3]は，アプリケーションをインストールさせて個人情報を盗み取り，金銭を脅し取る近年のワンクリック詐欺を擬似体験できる Android アプリケーションを開発している．ワンクリック詐欺アプリケーションは情報を取得するパーミッションを要求し，その情報を表示するもので，もし通信のパーミッションも要求していた場合，情報漏洩が発生することを擬似体験から学習する．この手法を用いて評価実験を行った結果，学習者は脅威・リスクの危険性を理解し，またセキュリティに関する理解度が向上したという結果が得られている．

パーミッションの範囲で悪事を働くマルウェアから身を守るためには，パーミッション許可からどの資産に対してどんな影響が発生するのかを認識出来なければならないが，この研究では情報取得パーミッションがどの情報を取得するのか分からない．また，ワンクリック詐欺アプリケーションが要求するパーミッションとして「電話/通話」，「現在地」等が挙げられているが，その他にも情報を取得するパーミッションは存在するため，それを要求された場合，対処することができない．本学習方法では資産・脅威・リスクの関係を学習するため，パーミッションと情報を取得するアクションの関係が分かり，情報漏洩が対象とする資産を網羅することができる．

6. まとめと今後の課題

実験結果から正答率が増加しており，パーミッションとアクションの関係の知識の体系化については成功していると言えるがアクションとリスクの関係については不十分である．また擬似体験による効果はほとんど見られないが，リスクの怖さを学習することは成功しているといえる．よって，4.2節で述べたリスクを擬似体験部分とパーミッションとアクション，アクションとリスクの関係を学習する部分の繋がりが分かりにくい問題に対して，繋がりが分かるように擬似体験の時点でパーミッションやアクションなどとの関係を提示することで，擬似マルウェアを用いたリスクの擬似体験による学習方法の学習効果をより向上させることができると考える．

参考文献

[1] 加藤真，松浦佐江子：擬似マルウェア体験による Android パーミッションと脅威の関係の学習，信学技法，114(227)，pp. 69-74(2013)
[2] Common Criteria, http://www.commoncriteriaportal.org
[3] 新谷洋介，長谷川元洋：Android スマートフォンユーザ向けワンクリック詐欺擬似体験教材の開発，情報処理学会論文誌，54(8)，pp. 2131-2135 (2013)