ボット判定に情報セキュリティ・倫理に関する学習を織り込んだシステム DualCheck を構築

１．発表者：

矢谷　浩司（東京大学 大学院工学系研究科電気系工学専攻　准教授）

２．発表のポイント：

- ボット判定（悪意のある自動入力プログラムと実際のユーザの入力とを判別する機構）と情報倫理・セキュリティの学習を両立させるシステム DualCheck を構築しました。
- DualCheck はボット判定の信頼性を維持しつつ、情報セキュリティ・倫理の学習というユーザに対して直接的な価値を提供できる新しいインタフェース技術です。
- インターネットを利用する際に同時に情報倫理・セキュリティの学習を行う機会を提供することで、より幅広いユーザに情報倫理・セキュリティに関する知識を提供し、情報技術の安全・安心な利用方法を促進する基盤となりえます。

３．発表概要：

東京大学大学院工学系研究科電気系工学専攻の矢谷浩司准教授らのグループは、一般のユーザが情報倫理・セキュリティを学ぶ機会をより身近にするために、ボット判定に情報倫理・セキュリティ学習を織り込んだシステム DualCheck を構築しました。DualCheck は情報倫理・セキュリティに関するクイズをユーザに出題し、ユーザは 5 つの選択肢のうち 1 つをクリックして回答します。その後、DualCheck は、正答と解説を提示し、一定の待ち時間のあと、ユーザに次のページへの遷移を許可します。このような設計により DualCheck は、ユーザがインターネット上で既に行っているボット判定に必要な作業に情報倫理・セキュリティの学習という直接的な価値をユーザに提供することができる､新しいインタフェース技術となっています。

DualCheck はインターネットを利用する際に同時に情報倫理･セキュリティの学習を行う機会をより身近な形で提供することで、より幅広いユーザに情報倫理・セキュリティに関する知識を提供し、情報技術の安全・安心な利用方法を促進する新たな方法となりえます。

本研究成果は、2022 年 8 月 8 日（米国東部夏時間）に国際会議 USENIX Symposium on Usable Privacy and Security において口頭発表を行いました。

４．発表内容：

近年、多くのユーザがインターネットのサービスやコミュニケーションツールを日常的に利用するようになり、インターネットを利用する上での情報倫理・セキュリティを理解することは不可欠なものとなっています。しかし、一般のユーザが情報倫理・セキュリティを学ぶ機会は十分に確保されていません。情報倫理やリスクに関する教育は職場や教育現場などにおいて行われているものがありますが、年 1～数回程度と頻度が限られるほか、職場や教育現場に属さない人にとっては情報倫理・セキュリティに関する知識を得る定期的な機会がない現状があります。このために、新しい攻撃手法などに対してユーザが脆弱なままになってしまったり、コミュニケーションや表現における新しい価値観を取り入れることに出遅れてしまったりすることがあります。

本研究グループは、これらの問題を解決するためには、インターネットユーザが日常的にこれらの知識を手軽に得られる仕組みが重要であると考え、ボット判定に情報倫理・セキュリテ

ィ学習を織り込んだシステム DualCheck を構築しました。ボット判定とはオンライン上のアンケートフォームなどにおいて悪意のあるユーザ実行する自動入力プログラムによる情報の入力を防ぎ、人間が実際に入力した情報のみを受け付けるようにする機構のことで、インターネット利用時によく見かけるものです。DualCheck は、そのボット判定機構に、情報倫理・セキュリティに関するクイズを融合させ、ボット判定と情報倫理・セキュリティの学習を両立させるシステムです。DualCheck は情報倫理・セキュリティに関するクイズをユーザに出題し、ユーザは 5 つの選択肢のうち 1 つをクリックして回答します。その後、DualCheck は、正答と解説を提示し、一定の待ち時間のあと、ユーザに次のページへの遷移を許可します。ボットを判定する方法には、既存のボット判定（reCAPTCHA-v2）などを利用し、ユーザがクイズに正答したか否かの情報はボット判定には利用しません。これにより、既存のボット判定と同程度の信頼性でボット判定を行えることが期待できるだけでなく、ユーザに対して情報セキュリティ・倫理に関する学習の機会を提供することが可能となりました。ボット判定は従来、ユーザに対して付加的な作業を強いるもの（例えば、画像で提示された文字を入力する、指示に合致する写真を選択する、チェックボックスにチェックを入れるなど）であり、その作業がユーザの直接的な価値と感じられない問題もありました。DualCheck はボット判定の信頼性を維持しつつ、情報セキュリティ・倫理の学習というユーザに対して直接的な価値を提供できる機構であり、ユーザがインターネット上で既に行っている行為に新たな意味や価値を創生することのできる、新しいインタフェース技術です。

同研究グループは、DualCheck を用いることによる知識定着効果と DualCheck のユーザビリティ（可用性）の評価を目的とした、実験参加者 34 名に対する 15 日間のユーザ実験も実施しました。その結果、検証に用いた情報セキュリティ・倫理に関するクイズ 10 問のうち 9 問において、実験前後での正答率の有意な向上が確認されました（図 4）。さらに、これらの類題 10 問のうち 5 問において、DualCheck を利用していないインターネット利用者と比較して正答率が有意に高くなることも示され、DualCheck が情報セキュリティ・倫理に関する知識の向上に役立つ可能性が示されました。また、画像で提示された文字を入力する、指示に合致する写真を選択するといった既存のボット判定手法と比較し、DualCheck のユーザビリティが有意に高く評価されたことも確認しました。さらに、実験参加者からは、「フィッシング詐欺など最近の巧妙化する詐欺に対して不安を感じているので、そういった問題が沢山あると良いと思いました。操作性の悪いパズル等をやるよりもこちらの方がずっと勉強になって良いので、ぜひ一般的なサイトで実装されて欲しいと考えます。」や、「スマホも PC も使わない人はいない時代なので、このようなクイズ形式で学べたのはとても良いと思った。」といった意見が得られました。

今後は、今回の研究成果を基に、クイズの内容をユーザ個人個人に合わせて提示したり、クイズの内容を自動的に言い換えたりすることで、学習効果をより高める技術の構築を目指していきます。

５．発表詳細：

国際会議名：USENIX Symposium on Usable Privacy and Security

論文タイトル：DualCheck: Exploiting Human Verification Tasks for Opportunistic Online Safety Microlearning

著者：Ryo Yoshikawa*, Hideya Ochiai, Koji Yatani*

６．問い合わせ先：

<研究に関すること>

東京大学 大学院工学系研究科 電気系工学専攻
准教授　矢谷 浩司（やたに　こうじ）

<報道に関すること>

東京大学 大学院工学系研究科 広報室

７．参考動画：

本研究成果のデモ動画
https://www.youtube.com/watch?v=5W16fpjeg4M

８．添付資料：

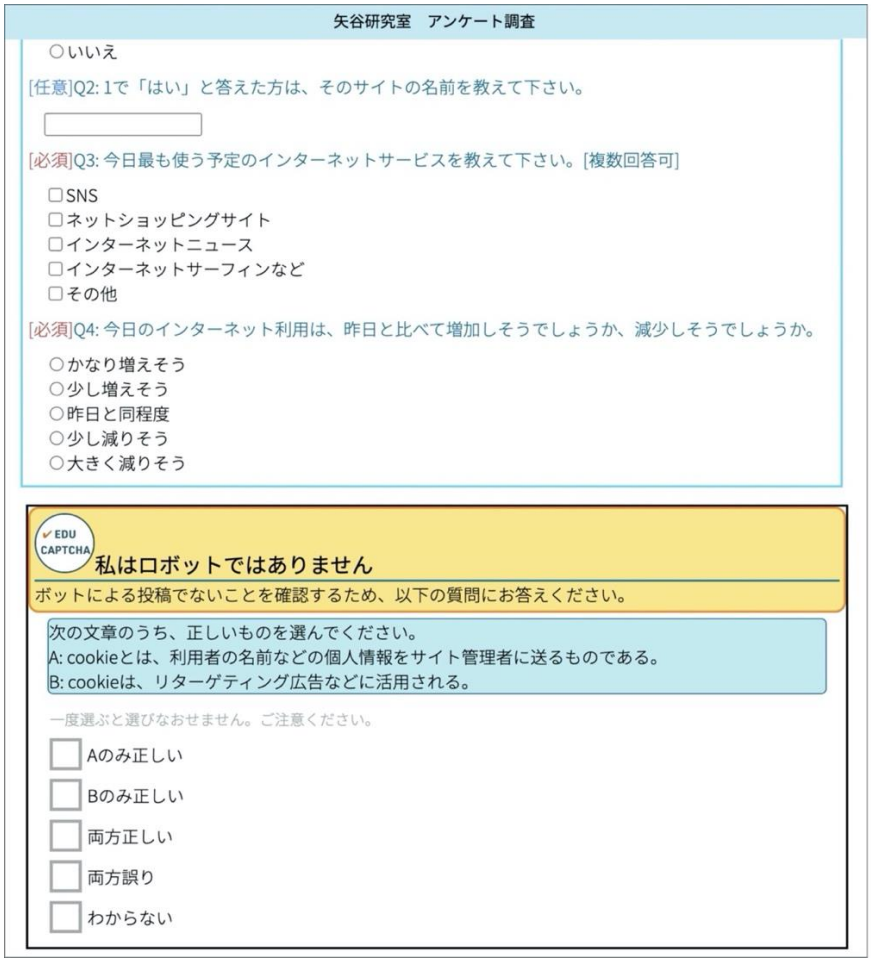

図 1. オンラインフォームに組み込まれた DualCheck の例。なお、学習効果を検証することを主な目的としたため、現在のプロトタイプにはボット判定の機能は組み込まれていません。

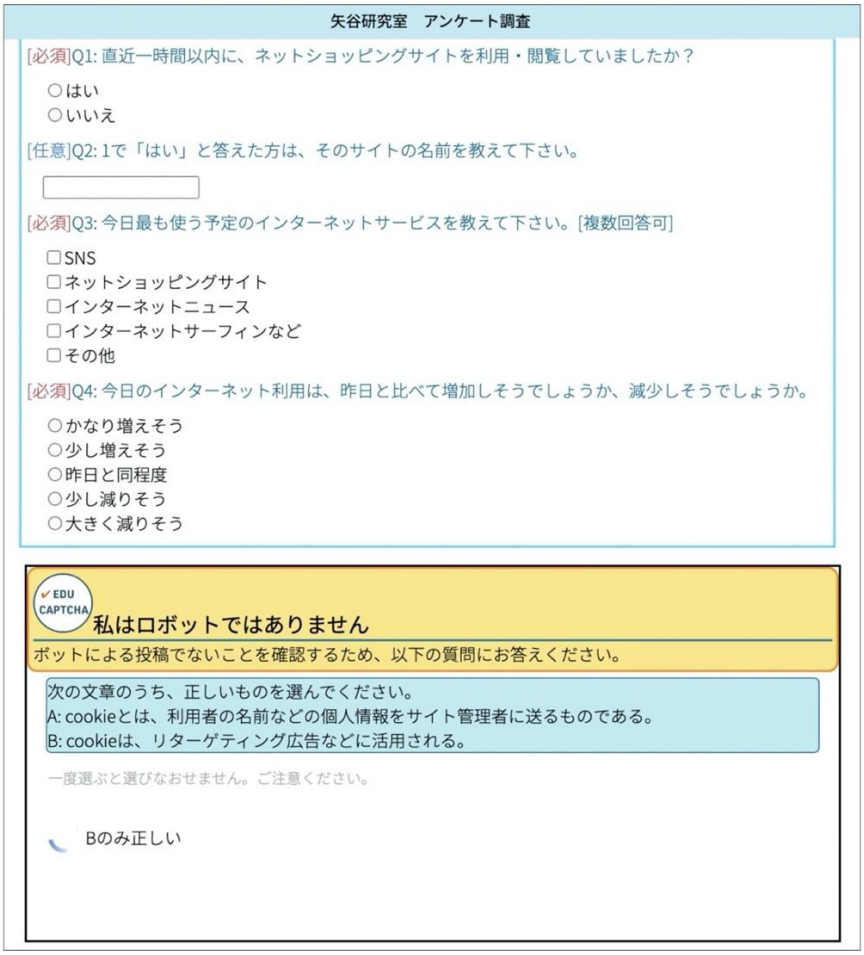

図 2. DualCheck が提示する問題を読んで、ユーザが選択肢の 1 つを選びます。回答に使用するチェックボックスは、既存のボット判定（reCAPTCHA-v2）のインタフェースの挙動を模倣するものとなっています。

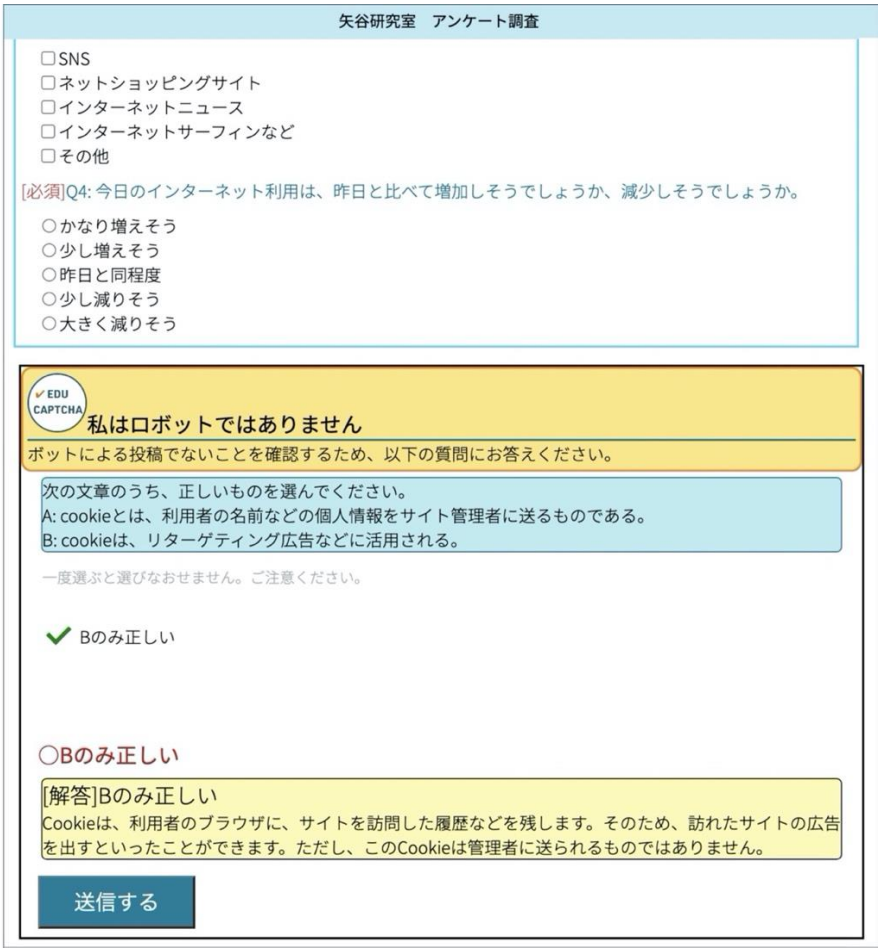

図 3. DualCheck は、与えられた問題に対する正解と解説を提示します。正解と解説が表示されてから 5 秒後に送信ボタンが有効になり、次のページへの遷移を許可します。この時間を利用してユーザは正解・解説を読むことができます。本システムでは、ユーザが正解を選択したか否かはボット判定の結果に影響せず、reCAPTCHA-v2 のようにクイズに回答する際の挙動で判定することを想定しています。

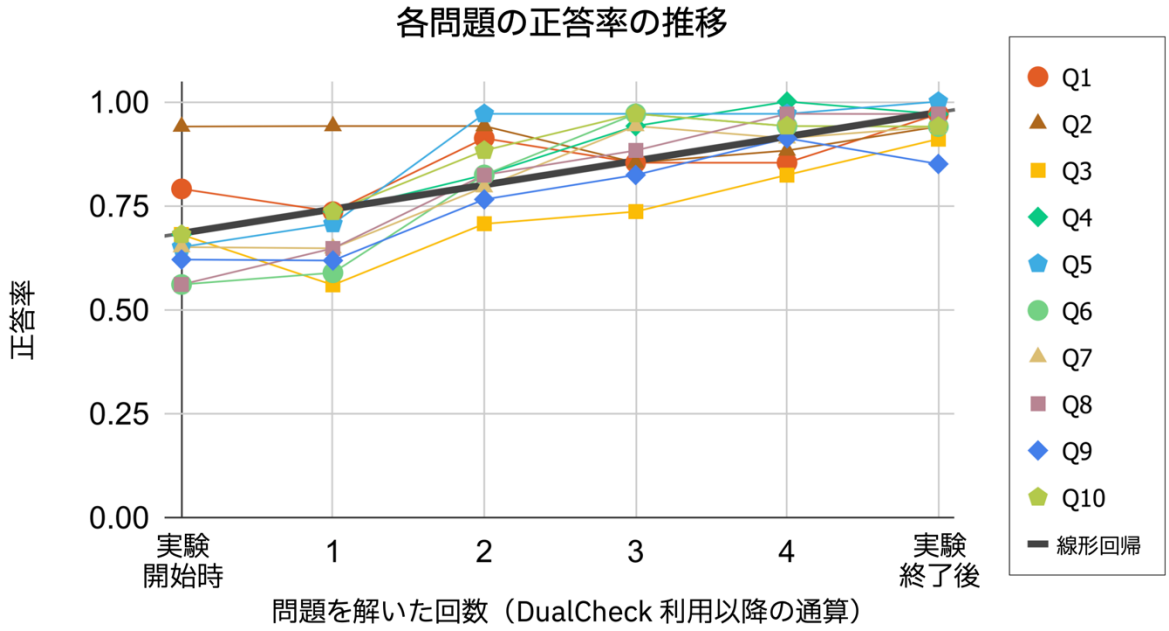

図 4. ユーザ実験におけるクイズの正答率の推移。「実験開始時」、「実験終了後」はそれぞれ、15 日間の実験開始前、終了後の正答率を表しています。15 日間の実験において、各クイズは合計 4 回実験参加者に対して提示されました。線形回帰の結果（黒線）は、$y = 0.06x + 0.68$（adjusted R2=0.57）となり、回数を重ねる毎に正答率が上がっており、一定の学習効果があったことが確認されました。