

中学生を対象とした暗号化と認証の仕組みを理解するための 電子商取引でのカード決済体験型教材の開発

西脇勇斗*, 阪東哲也**

本研究の目的は、中学生を対象とした暗号化と認証の仕組みを学習できる電子商取引のカード決済体験型教材の開発と活用方法の提案である。生徒がインターネット上で商品を選択し、配布されたカード情報をもとに決済を行う模擬的な電子商取引を体験できる簡易的なECサイトを構築した。教師は、Wiresharkを用いて、ECサイトでの電子商取引時の通信をキャプチャし、通信の詳細を可視化することで、暗号化の仕組みを考えさせることや、暗号化の必要性を理解させることができる。また、教材の発展的な利用方法として、カード紛失時にも対応できる認証の仕組みを考えさせ、多要素認証の必要性に気づかせる授業実践の提案をした。

【キーワード】：中学生、消費者教育、体験型教材、暗号化、パケットキャプチャ]

1. はじめに

2022年から「民法の一部を改正する法律(成年年齢関係)」が施行されることとなった。成年年齢が20歳から引き下げられ、18歳から契約が可能となったことにより、自立した消費者になるための消費者教育の充実が喫緊の課題である。田代・赤塚(2020)は、急速な社会変化と成人年齢引き下げによって、できるだけ早い時期から自身の消費行動に自覚を持つことを指摘しており、消費行動に関する中学校での授業実践を行っている[1]。また、民法改正に関する若者向けのパンフレット[2]には、消費者教育の充実が明記されており、早期段階での消費者教育の重要性が窺える。

特に、若年層の消費者トラブルとして懸念されている1つに電子商取引に関するトラブルが挙げられる。電子商取引のうち、消費者向け電子商取引とは「商取引(=企業(個人事業者も含む)の収益として計上された金銭的対価を伴う商品としてモノ、サービス、情報の交換に関わる一連の業務・行為)のうち、一部でもコンピュータを介したネットワーク上で行われ、かつ成約(=確定受発注)されたもの」と定義されている[3]。上述した成年年齢の引き下げにより、18歳からECサイト等を利用して、クレジットカード決済が可能になる。クレジットカード決済は操作が簡単であり、電子商取

引や情報通信に関する知識が十分になくても利用できる。この点、IPA(情報処理推進機構)が公開している情報セキュリティ10大脅威2022[4]として「クレジットカード情報の不正利用」がランクインしていることを踏まえれば、若者の知識不足による被害増加、被害の深刻化が懸念される。日本クレジット協会[5]によれば、クレジットカード不正利用被害額は近年増加傾向にあり、2021年の不正利用被害額の約95%を番号盗用が占めている。クレジットカード情報を狙ったサイバー攻撃として、偽サイトへ誘導しクレジットカード情報を入力させ窃取するフィッシング詐欺は、番号盗用の攻撃手法の一つであるといえる。一般利用者向けのフィッシング詐欺に対する対策としては、重要な情報を入力するページではSSL/TLS(暗号化技術)が採用されているか確認することが挙げられている[6]。暗号化された通信上で電子商取引を行うことによって、悪意のある第三者がクレジットカードを利用するために必要な認証情報の盗聴が難しくなる。アドレスバーを確認するだけで対応できるため、誰にでも容易にできる対策であるといえる。

このように暗号化通信の確認をすることが効果的な対策である一方で、通常のブラウジングでは、通信の暗号化の状況を気に留める機会は多くない。そのため、情報通信に関する知識を十分に有していない若者が暗号化通信の確認による偽サイト判別対策に、自発的に取り組むことは困難であると考えられる。クレジットカードが発行できる年齢に達する前から適切な知識を身につけることの重要性が指摘できる。

* 鳴門教育大学大学院 高度学校教育実践専攻 自然・生活系教科実践高度化コース(技術・工業・情報科教育実践分野) 大学院生

** 鳴門教育大学大学院 高度学校教育実践専攻 教科・総合系 技術・工業・情報科教育コース

そこで、早期段階として中学生段階に着目し、暗号化と認証の仕組みの理解をねらいとした電子商取引のカード決済体験型の教材を開発することとした。

2. 中学校段階から暗号化と認証の

仕組みを学ぶ重要性

中学校学習指導要領(平成 29 年告示)の技術・家庭(技術分野)[7]では、内容D(1)にて情報セキュリティの基礎的な技術の仕組みの理解と、情報の暗号化に関する学習も含まれている。

さらに、情報の暗号化の目的としては、第三者に重要な情報を見られないようにすることが考えられ、その重要な情報の1つとして、認証に関する情報が挙げられる。認証とはコンピュータに利用者を識別させることである。認証に必要な情報には ID・パスワードといった知識情報、カードや認証デバイスといった所持情報、指紋や虹彩といった生体情報の3種類がある。近年では、複数の認証情報を組み合わせて認証する多要素認証が主流となっている。このように、認証と安全に(認証)情報を扱うための暗号化を一度に学ぶことにより、実社会で利用されている技術の必要性を理解させることができると考えられる。

中学校段階では、技術・家庭科(技術分野)だけではなく、家庭分野との関連も指摘できる。家庭分野の内容C(1)アには消費者被害の背景とその対応の理解が明記されている。

以上のことから、電子商取引のクレジットカード決済を題材とした暗号化と認証の仕組みを扱う学習活動を中学生に適用することは、中学校学習指導要領に沿っており、適切と判断できる。

関連する先行研究として、長谷川・上野・新谷(2015)は、クレジットカードを題材とした教材開発及び研究授業を行い、暗号化通信の必要性和確認方法の理解に関して一定の効果があることを報告している[8]。しかし、具体的な暗号化通信の仕組みやクレジットカードの不正利用防止については十分に触れられてはいない。そこで、本研究で開発する教材は、暗号化通信の仕組みを生徒が捉えられるように設計し、不正利用防止を実現するための技術である多要素認証を含めた認証の仕組みを考えられるようにした。

3. 教材開発

3.1 概要

図1に開発したECサイトの遷移図を示す。生徒

【商品選択・決済ページ】

【決済完了ページ】

図1 ECサイトの遷移図(HTTPアクセス時)

が模擬的に電子商取引を体験できる簡易的な EC サイトを開発した。生徒は事前に配布されたカードの番号とセキュリティコード(以下、カード情報)を使って EC サイトで商品選択し、決済を行う。

生徒が EC サイトにアクセスする際に、HTTP、HTTPS のどちらのプロトコルでアクセスするかを、教師が選択できるように設計した。HTTP アクセス時は生徒が利用した電子商取引に関する情報は閲覧可能になり、HTTPS アクセス時は電子商取引に関する情報は暗号化され、閲覧そのものはできるが、認証情報含め内容を確認できないことに気づかせられるように設計した。

このように、暗号化の仕組みを学ぶにあたって、重要なカード情報を生徒自身で入力する体験をすることで、暗号化の必要性の理解につながると考えられる。また、カード情報を相手に送信するまでの通信経路において、暗号化が必要な開始時点と終了時点の考察も可能になると考えられる。

3.2 システム構成図

図 2 に本教材のシステム構成図を示す。教師の PC で Web サーバを立ち上げ、同ネットワーク上にある生徒の PC で Web サーバにアクセスすることで、図 1 のサイトを閲覧できる。Web サーバは Flask[9] と呼ばれる Web フレームワークで作成している。

また、カード情報が暗号化されているかの確認には、パケットキャプチャツール Wireshark[10]を用いる。

3.3 開発した教材の使用方法

事前準備として、生徒 PC、教師 PC とともに同一の校内 LAN に接続する。授業開始前に、教師は教師 PC 上で Web サーバと Wireshark を起動する。予め

Wireshark を起動しておくことで、いつでもパケットキャプチャ可能な状態にする。

まず、HTTP 通信ではカード情報が平文で通信されていることを確かめる。生徒はブラウザを開き、教師が掲示した HTTP 対応の Web サーバへの URL を用いてアクセスする。生徒は自由に商品を選択した後、決済情報に各自に配布されているカードのカード情報を入力し、購入ボタンを押す。生徒が購入ボタンを押し終えたことを確認後、教師は Wireshark を操作し、HTTP の POST 通信のパケットの中身が Wireshark の画面で表示されていることを示す。実際に生徒が送信した商品とカード情報が平文であることに気づかせる。

次に、暗号化によって、商品やカード情報が秘匿化されることに気づかせる活動に取り組む。生徒には HTTPS 対応の Web サーバにアクセスさせ、HTTP 通信時と同じ手順で購入及び決済を行う。教師も同様にキャプチャを行い、HTTPS 通信で送信した際には、パケットの中身が暗号化されて全く中身が読めないことを生徒に示す。

3.4 暗号化の仕組みの理解に向けて

暗号化は、通信経路中の第三者による盗聴を防ぐことで機密性向上を担っている一方、暗号文のまま相手に届くと、受け取った相手は内容を理解することができない。そこで生徒には、カード情報を含めた重要な情報はどこで暗号化されてどこで復号されるかを、実際に暗号化通信をさせながら考察することで、暗号化の仕組みの理解をより深めることができる。なお、暗号化を支える仕組みである共通鍵暗号方式及び公開鍵暗号方式は、高等学校「情報 I」の学習範囲に相当するため、

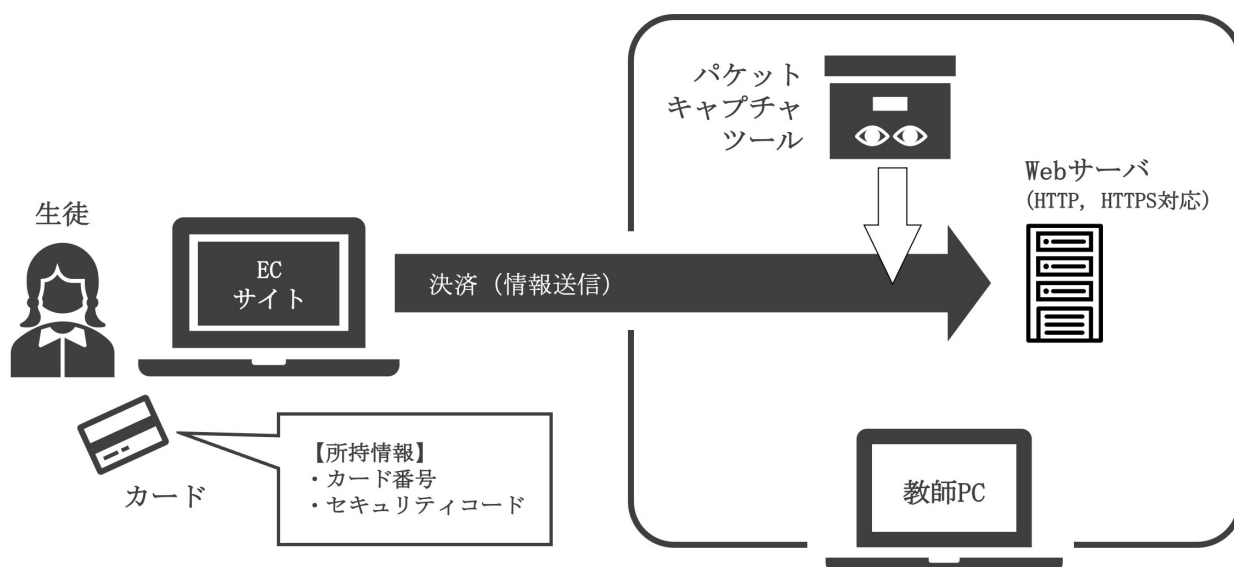


図 2 システム構成図

中学校段階で学習するには難易度が高いと考えられる。そのため、重要な情報をインターネット経由で相手まで送信する経路において、暗号化が必要な開始時点と終了時点を考えることで、暗号化の仕組みを簡易的に理解できる。

また、Wireshark を用いることによって、第三者がどのように暗号化された情報を盗聴できるかを確かめるため、暗号化の必要性の理解につながる事が期待できる。図 3 に HTTP 通信、図 4 に HTTPS 通信時のパケットキャプチャの様子を示す。HTTP 通信時は購入した商品とカード情報であるカード番号、セキュリティコードがそのまま平文で見えている。HTTPS 通信時は全ての通信が暗号化されており、どのパケットに購入情報や決済情報が含まれるかの特定もできない。

3.5 本教材の発展的な利用方法

本教材の基本的な使用方法としては、所持情報であるカード情報を用いた認証と暗号化を扱う方法を紹介した。発展的な利用方法として、知識情報であるパスワードを使った認証を追加した多要素認証の疑似体験もできる。

例えば、カード紛失時には、所持者ではない者がカード情報をもとに決済することができてしまう。この状況は暗号化通信だけで対応することはできない。

生徒には、カードの所持情報だけの認証では、紛失時に対応できないことに気づかせ、パスワードによる知識情報を加える（一般的には、クレジットカード本人認証サービス(3D セキュア)と呼ぶ)ことで、紛失時にカードを悪用されるリスクを大幅

に低減できることから、多要素認証の仕組みと必要性を気づかせられる。

このような多要素認証の体験には、上述したシステムに FeliCa を追加することで可能となる。FeliCa とは、ソニー株式会社が開発した非接触型 IC カード技術である[11]。生徒は自分の PC に PaSoRi を接続し、自分のカードを認識させ、ブラウザ上でパスワードを登録する。図 5 に PaSoRi 接

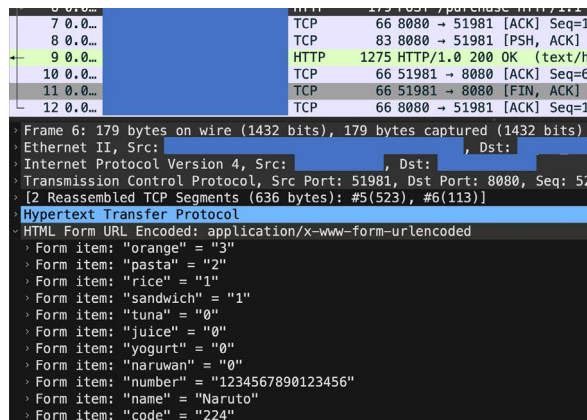


図 3 HTTP 通信時のパケットキャプチャ

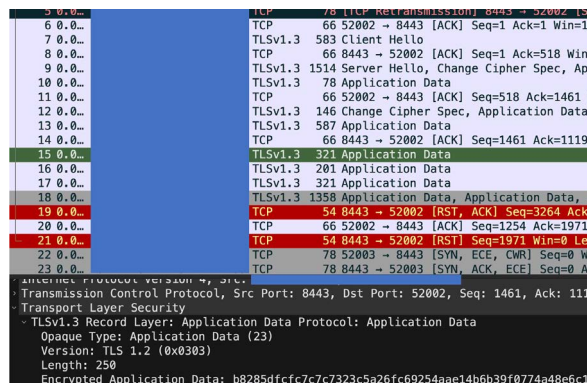


図 4 HTTPS 通信時のパケットキャプチャ

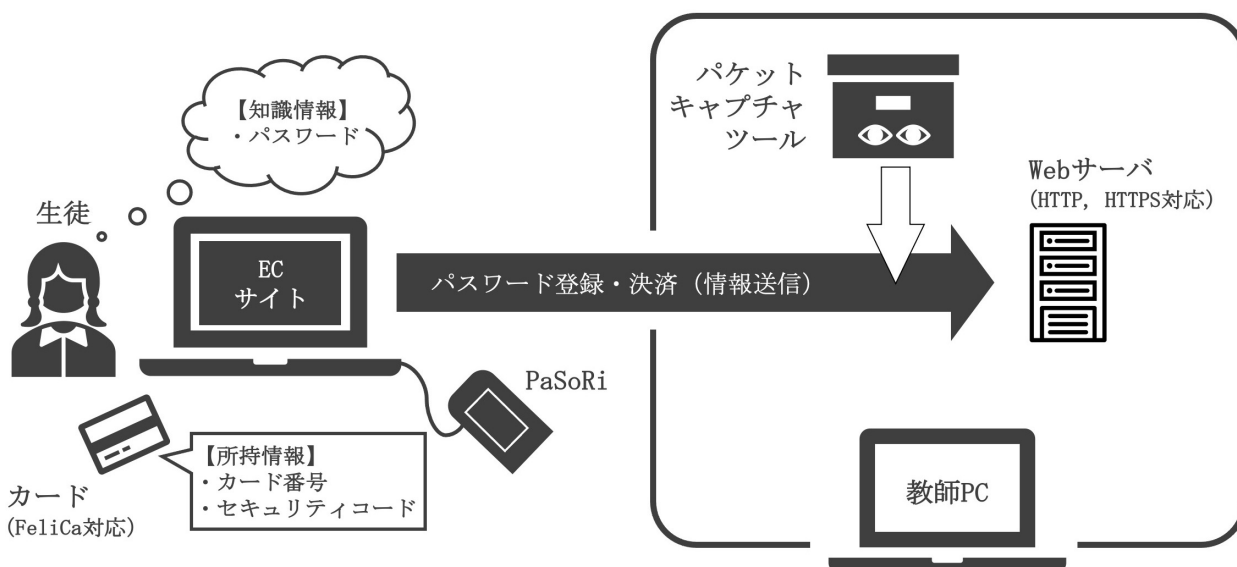


図 5 多要素認証導入後のシステム構成図

続時の新たなシステム構成図を示す。

多要素認証を扱う本授業は、暗号化の学習と認証の学習の2時間で実施することが想定される。1時間目は前項の通りである。2時間目はパスワードの登録が暗号化通信で行う必要があることで前時の復習を行い、パスワードを登録した後に生徒のカードをシャッフルし、カードの正式な所持者ではない第三者の立場として決済を試みる。カードの所持情報だけでは認証が通らないことを体験することで、暗号化と認証の仕組みと相互の関連性を学ぶことができる。

4. まとめ

本論文では、中学生を対象に、暗号化と認証の仕組みの学習を目標とした電子商取引のカード決済体験型の教材を開発した。また、教材の発展的な利用として、多要素認証の仕組みも学習できる授業実践の提案を行なった。

生徒は、配布されたカードにある情報をもとに、ECサイトで商品選択及び決済を行う体験を通じて、暗号化の仕組みの理解につながるとともに、必要性を理解させることができる。そこから、日常的な暗号化通信の確認につなげられる。また、発展的内容として多要素認証を扱うことで、情報セキュリティ意識の向上にも期待できる。

本教材は、高等学校の情報Ⅰにおいても活用できると考えられる。Wiresharkに表示されたパケット情報をより詳細に考察させることで、パケットの中身の詳細確認や、受け手と送り手の通信を可能にするIPアドレスの学習にも活用できる。情報セキュリティに関する基礎的知識を体験しながら身につけることができるように、今後も教材開発に取り組んでいきたい。

参考文献

[1] 田代百里恵・赤塚朋子：中学校家庭科教育「消費生活と環境」における「深い学び」の効果的な指導方法。宇都宮大学教育学部教育

実践紀要，2020，7，pp.185-192.

- [2] 法務省，民放改正(成年年齢の引き下げ)パンフレット，<https://www.moj.go.jp/content/001300586.pdf>(最終閲覧日：2023年2月23日)
- [3] 経済産業省，消費者向け電子商取引実態調査・用語の解説，<https://www.meti.go.jp/statistics/tyo/denshi/pdf/21yougo.pdf>(最終閲覧日：2023年2月26日)
- [4] IPA(情報処理推進機構)，情報セキュリティ10大脅威2022[個人編]，<https://www.ipa.go.jp/files/000096899.pdf>(最終閲覧日：2023年2月23日)
- [5] 日本クレジット協会，日本のクレジット統計2021年度版，https://www.j-credit.or.jp/information/statistics/download/statistics_domestic_2021.pdf(最終閲覧日：2023年2月23日)
- [6] 総務省，国民のためのサイバーセキュリティサイト，https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_security01_05.html(最終閲覧日：2023年2月23日)
- [7] 文部科学省，中学校学習指導要領(平成29年告示)，東山書房
- [8] 長谷川元洋・上野顕子・新谷洋介：クレジットカード決済によるネットショッピング疑似体験教材と体験型授業の開発．消費者教育，35，pp.127-136.
- [9] Pallets, Flask's documentation, <https://flask.palletsprojects.com/>(最終閲覧日：2023年2月23日)
- [10] Wireshark Foundation, Wireshark, <https://www.wireshark.org/>(最終閲覧日：2023年2月23日)
- [11] SONY, FeliCa とは，<https://www.sony.co.jp/Products/felica/about/>(最終閲覧日：2023年2月23日)