北海道科学大学研究紀要
第52号（2024年）
研究報告

Bulletin of Hokkaido University
of Science, No.52(2024)
Research Reports

AWS を用いたゼミ紹介 Web サイトの開発

Development of a Seminar Website using AWS

杉尾　信行 *　　荒澤　孔明 *　　松川　瞬 *

Nobuyuki Sugio, Koumei Arasawa, Shun Matsukawa

鈴木　昭弘 *　　松﨑　博季 *

Akihiro Suzuki, Hiroki Matsuzaki

Abstract

We developed a seminar website using cloud computing. By utilizing AWS (Amazon Web Services) managed services in the development process, we achieved a highly available website while reducing maintenance and operational overhead. This paper reports on the results of this development.

1. はじめに

インターネットが広く一般に普及しており，様々なサービスを日々利用している．我々にとって，インターネットは日常生活には当たり前のものとなっている．その反面で，企業や個人を対象としたサイバー攻撃が増加している．サイバー攻撃関連の通信数の推移を図 1 に示す．

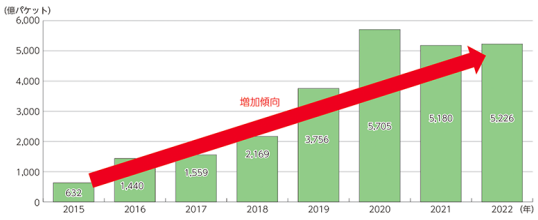


図 1　NICTER におけるサイバー攻撃関連の通信数の推移 (1)

近年，大学の研究室が Web サイトを個別に開設し，様々な情報発信を行っている．Web サイトを開設することで，研究紹介や研究成果の公表，及び研究室に所属する学生の就職状況等の情報発信が可能である．北海道科学大学では，公式 Web サイト*1に教員紹介を行う Web ページが用意されているが，研究概要や研究業績の列挙に留まっている．また，著者が責任者となっているゼミ（情報セキュリティ研究室）は，個別の Web サイト開設による情報発信を現状行っていない．

そこで本研究では，クラウドコンピューティングサービスとして注目を集める AWS（Amazon Web Services)*2を活用し，DDoS 攻撃等の Web サーバに対するサイバー攻撃に耐性を有する Web サイトの開発を行う．また，Web サイトを通じてゼミで取り組む研究内容や研究成果の情報発信を行うことを目的とする．更に，完成した Web サイトのユーザビリティ評価にてユーザ満足度の調査を行う．本論文ではその成果について報告する．

最後に本論文の構成を以下に示す．第 2 章で関連研究について記載する．第 3 章で本論文で用いる関連技術について説明する．第 4 章で提案手法について説明する．第 5 章で開発した Web サイトの評価を行う．第 6 章にて考察を述べた後，第 7 章でまとめと今後の課題を示す．

2. 関連研究

DoS 攻撃（Denial of Service attack，サービス拒否攻撃）は，Web サイトやサーバに対して過剰なアクセスやデータを送付し，サービスを不能にするサイバー攻撃である (2)．また，DDoS 攻撃（Distributed Denial of Service，分散型サービス拒否攻撃）は，複数に分散した場所から DoS 攻撃を行うサイバー攻撃である (3)．

Cook らはサーバやブラウザに変更を加えることなく，Web プロキシ機能と TLS クライアント認証を組み合わせた DDoS 攻撃対策を提案した (4)．DoS 攻撃には様々な手法があり，Singh らは HTTP-GET flood

*1 https://www.hus.ac.jp/

*2 https://aws.amazon.com/jp/

DDoS 攻撃に対する体系的な調査論文を発表している [5]．その中で，データセット，ソフトウェアツール，攻撃戦略，および基礎となるモデリング手法を明らかにした．Jaafar らは 2014 年から 2018 年までに発表されたアプリケーション層における DDoS 攻撃に関する 12 の検出方法を調査し， DDoS 攻撃に対する 4 つの防御手法（検知，緩和，防止，モニタリング）を提案した [6]．

Darwish らはクラウドコンピューティング環境に対する DDoS 攻撃の対策を，クラウド利用形態（IaaS，PaaS，SaaS）毎に提示している [7]．また，Somani らはクラウドコンピューティング環境への DDoS 攻撃に関する調査論文を発表し，オートスケーリングや多層防御による対策が有効であるとしている [8]．Rajan はサーバレスアーキテクチャとして注目を集めている function as a service（FaaS）について，AWS Lambda を題材に調査を行っている [9]．

モバイル利用環境の普及に伴い，PC 用の Web サイトだけでなく，モバイル向け Web サイトの開発も重要となっている．常盤は WordPress を用いた大学研究所向けモバイル対応 Web サイトを開発し，大学情報基盤としての活用可能性について検討している [10]．また，日経 BP コンサルティングは「大学スマホ・サイト ユーザビリティ調査 2023-2024」を公表し，大学のスマートフォン・サイトを使いやすさの観点から評価している [11]．

3. 関連技術

3.1AWS

AWS は Amazon Web Services 社が提供するクラウドコンピューティングサービスである．クラウドコンピューティングサービスとは，サーバ，ストレージ，データベース等がインターネットを通じて提供されており，それらを利用するサービスの総称である．クラウドコンピューティングが登場する前は，自社の建物の中などにサーバー機器を購入・設置し，利用するオンプレミスが一般的であった．クラウドコンピューティングでは機器の購入やハードウェアの管理は一切必要なく，インターネットからクラウドコンピューティングサービスに接続することで，大容量のストレージ、高速なデータベースなどを必要な分だけ利用可能である．現在 AWS では 200 種類以上のサービスが用意されており，世界各国のスタートアップ企業や大企業，主要な政府機関でも採用されている．同様のクラウドサービス事業者は Google（Google Cloud Platform）や Microsoft（Microsoft Azure）などが存在するが，その中でも AWS は世界シェア No.1 のサービスである．

3.2 本研究で利用した各種 AWS サービス

本研究では，AWS CloudFront，Amazon S3，Amazon API Gateway，Amazon Lambda，Amazon SES を使用する．

Amazon CloudFront は CDN（Contents Delivery Network）の機能を持つマネージドサービスであり，クライアントへコンテンツを高速配信することが可能になる．CDN とは，システムのサーバ負荷を下げつつ，コンテンツの配信を高速化する仕組みである．CDN はオリジンサーバとエッジサーバで構成されており，オリジンサーバはコンテンツを配信するサーバの事を示す．また，エッジサーバとはコンテンツの一部を一時的にキャッシュするサーバの事である．

Amazon S3 はデータを格納・管理できるオブジェクトストレージサービスである．S3 は様々な用途として使用可能であり，例えばサーバのストレージ領域としての活用から，データバックアップや機械学習などで利用するデータの保存場所など幅広い活用方法が存在する．本研究では HTML ファイルなどの静的なコンテンツに対してアクセス可能なエンドポイント（URL）を発行する静的ウェブサイトホスティングの機能を利用し Web サイトを配信する．

Amazon API Gateway は API の作成, 公開, およびセキュア化するためのサービスである．API のバージョン管理，レスポンスのモニタリング，認証等の機能が揃っているため、開発工数の削減が期待できる．また，AWS Lambda と連携すれば，手軽にサーバーレスでの API が構築可能になるといった特徴がある．

Amazon Lambda はソースコードによる関数を設定することが可能なサービスである．基本的に AWS の他のサービスと組み合わせて利用されており，何らかのイベントが起こったら，あらかじめ設定していたソースコード（関数）が実行される，という仕組みを想定した活用が多い．アプリケーションのイベントに応じて関数を実行するため，リアルタイムアプリケーションの構築に適している．

Amazon SES は既存ドメインまたは既存メールアドレスを利用して，メール配信を行うサービスである．迷惑メールフォルダにメールが入りにくいなど配信性能の高い機能を持つ．

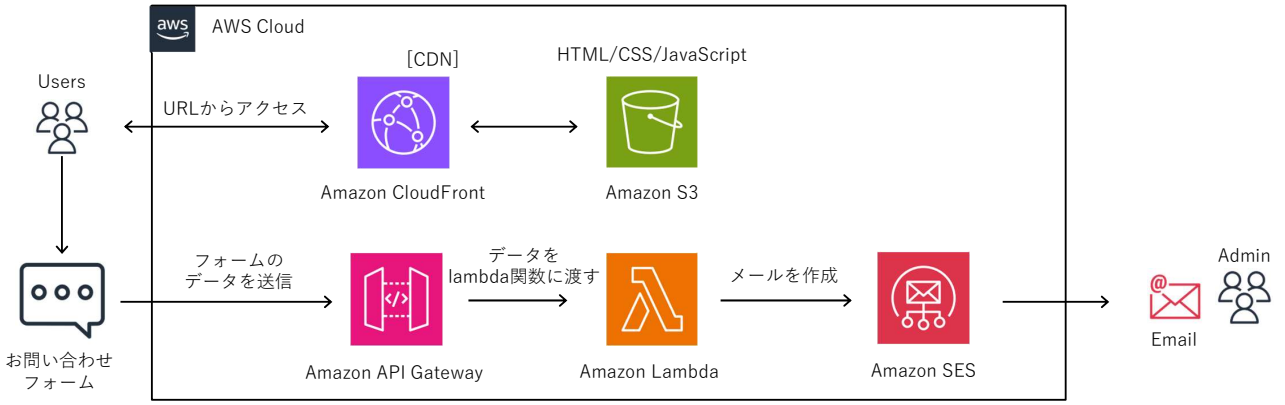


図 2　システム構成

4. 提案手法

4.1 概要

本研究で開発したゼミ紹介 Web サイトは，本学の情報セキュリティ研究室にて行っている研究内容の紹介を行うものである．また，Web サイト内にお問い合わせフォームを設置し，研究内容に関して気軽に質問できる仕組みを整えている．

4.2 システム構成

システム構成を図 2 に示す．ユーザは CloudFront で作成した Web サイトの URL にアクセスすると，S3 に格納している HTLM，CSS，及び JavaScript に基づく Web サイトがブラウザ上に表示される．また，ユーザがお問い合わせフォームからメッセージを送信すると，データが API Gateway を経由して Lambda に届き，SES 経由で Web サイトの管理者にメールが届く仕組みである．

本研究で用いた AWS の各種サービスは全て AWS が保守・運用を行うマネージドサービスである為，Web サイトの管理者は個別に Web サーバ等の保守・運用を行う必要がないのが特徴である．この様に，マネージドサービスのみを活用した構成はサーバレスアーキテクチャと呼ばれる．

4.3Web サイト

S3 に格納した HTLM，CSS，及び JavaScript に基づく Web サイトについて紹介する．Web サイトの内容は，ホーム，研究概要，学生個人の研究紹介，及びお問い合わせの 4 部構成となっている．

4.3.1 ホーム

Web サイトの URL にアクセスすると，図 3 のホーム画面が表示される．左側に表示されるサイドバーには，「ホーム」，「杉尾ゼミについて」，「学生の取り組み」，「お問い合わせ」の 4 つが表示され，各項目を選択すると該当 Web ページを表示する仕組みとなっている．

図 3　ホーム画面

4.3.2 研究概要

サイドバーの「杉尾ゼミについて」を選択すると，図 4 に示す情報セキュリティ研究室で行っている研究概要が表示される．

研究概要の記載内容を以下に示す．

1. サイバーセキュリティ
   ペネトレーションテストやクロスサイトスクリプティングに関する研究を行っています．攻撃者の観点からサイバーセキュリティを考え，対策手法の調査と研究を行います．
2. 共通鍵暗号の安全性評価
   共通鍵暗号の安全性は，暗号アルゴリズムが各種攻撃に対して強力であることが必要です．また暗号文の秘匿性も重要で，平文からの情報漏洩が最小限に抑えられる必要があります．こういった観点を考慮して安全性評価を行います．
3. クラウドコンピューティング
   主に AWS を活用した研究を行っています．サービスを組み合わせてどういったシステムが構築

図 4　研究内容の紹介

できるのか考え，試行錯誤しています．この Web サイトも AWS を利用しています．

4. その他情報セキュリティに関連する研究
   この研究テーマ以外にも情報セキュリティに関する研究や，学生の皆さんが希望するテーマがあればサポートする環境が整っています．

4.3.3 学生の取組内容

サイドバーの「学生の取り組み」を選択すると，以下に示す学生の卒業研究が表示される．一例を付録に示す．

1. **Chat GPT** を使用したマルウェアの作成
   自然言語処理を行う Chat GPT を用いてマルウェアを作成できるのかどうか，という検証を行います．
2. **Windows7・10** のハッキング
   Virtual Box を用いてハッキングを行い，攻撃された場合の対処や防御策を考察します．
3. クロスサイトスクリプティングに関する研究
   クロスサイトスクリプティングの攻撃と防御を行い，危険性や仕組みを理解します．
4. **Kali Linux** を使った攻撃
   セキュリティ対策のために攻撃者，非攻撃者の視点からサイバー攻撃を理解します．
5. 軽量暗号 **SIT** の安全性評価
   軽量暗号の中の一つである SIT を使って，暗号の安全性評価を行う研究です．
6. **AWS** を活用した **LINE** チャットボット
   ゼミの取り組みや研究内容などの質問を回答するチャットボットを開発します．開発基盤には AWS を使用しています．
7. **Amazon Web Services** を使用したゼミ紹介 **Web** サイトの構築
   AWS のクラウドコンピューティングを使用し，ゼミで取り組んでいる研究内容を紹介する Web サイトを開発します．

4.3.4 お問い合わせフォーム

お問い合わせフォームは名前，メールアドレス，本文の項目を用意し，入力した内容がメールにて管理者に届く仕組みである．

5. 評価

5.1 異なるシステム構成との比較評価

今回開発したゼミ紹介 Web サイトのシステム構成（図 2）と一般的な Web システムを構築する際のシステム構成との比較を行う．一般的な Web システムは，Web サーバ，アプリケーションサーバ，及びデータベースサーバの 3 層にて構成されている（図 5 参照）．

図 5 に示す Web システムをオンプレミスで構築した場合とクラウドサービスを利用して構築した場合

表 1　オンプレミスとの比較評価

比較観点	オンプレミスで構築	クラウドサービスを利用して構築
費用	初期投資が大きい	初期投資が小さい（従量課金）
導入期間	長い	短い（ネット経由で利用）
運用・保守	自社で実施	利用者とクラウドサービス事業者が実施
可用性	中～高	高
安全性	DoS 攻撃対策を自社で実施	利用者とクラウドサービス事業者が実施
災害対策	冗長化等を自社で実施	利用者とクラウドサービス事業者が実施

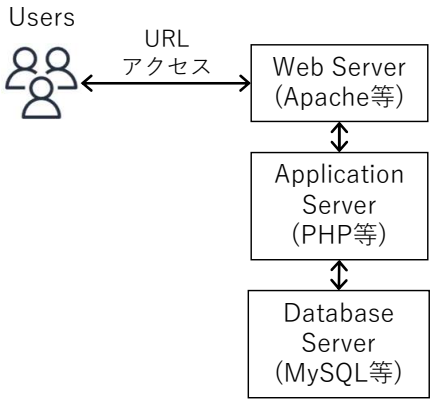


図 5　一般的な Web システムの構成

の比較結果を表 1 に示す．オンプレミスで構築する場合，想定されるアクセス数を処理可能な性能を有する物理サーバを事前に用意し，Web システムを構築する必要がある．また，DDoS 攻撃を想定した対策（サイバー攻撃に利用された IP アドレスからの接続拒否や Web システムの冗長化等）は自前で行う必要がある．

一方，クラウドコンピューティングを用いて構築する場合，想定されるアクセス数を処理可能な性能の仮想サーバを選定し，Web システムを構築すれば良い．また，DDoS 攻撃を想定した対策は責任共有モデル[*3]に基づき利用者とクラウドサービス事業者が行う．具体的には，利用者は仮想サーバのオートスケーリング機能の有効化や AWS WAF を用いたアプリケーションレベルでのファイアウォールを有効化する事により，DDoS 攻撃対策が可能である．更に，本論文で採用したシステム構成（図 2）の場合，クラウドサービス事業者が提供する各種マネージドサービスを用いている為，仮想サーバのミドルウェアの更新作業等を行う必要がない．その為，Web サイトの提供者はミドルウェアの保守・運用の手間から解放される．また，AWS が公開している各種サービスの SLA に基づき可用性が保証される．なお，大規模災害やテロ行為等，クラウドサービス事業者の想定外の事態によるサービス利用中断も起こり得る為，事業継続計画を踏まえてクラウドコンピューティングを利用する必要がある．

5.2 ユーザビリティ評価

今回開発した Web サイトのコンテンツを含めたユーザビリティ評価結果について記載する．調査対象は情報工学科に所属する学部 3 年生（8 名），及び学部 4 年生（30 名）の計 38 名である．

各項目に対し 5 段階で評価を行う形式であり，項目ごとに感想や意見の記入欄を設置した．アンケート項目は以下に示す 7 項目である．

- Web サイトのデザイン
  （配色や配置、画像やアイコンなど）
- 構成の分かりやすさ
- 操作の分かりやすさ
- コンテンツの充実度
- 発信されている情報は役立ちそうか
- Web サイトの速度とパフォーマンス
- モバイル端末での閲覧・利用のしやすさ
  （スマートフォンユーザーのみ）

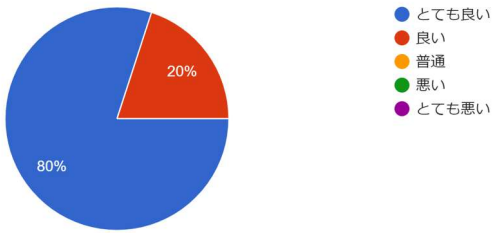


図 6　デザインに関する評価結果

[*3] https://aws.amazon.com/jp/compliance/shared-responsibility-model/

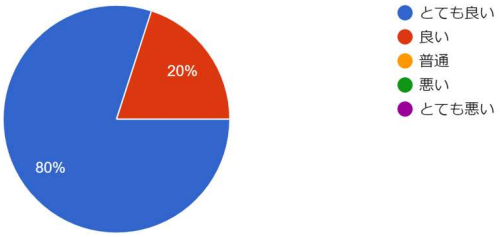


図 7　構成に関する評価結果

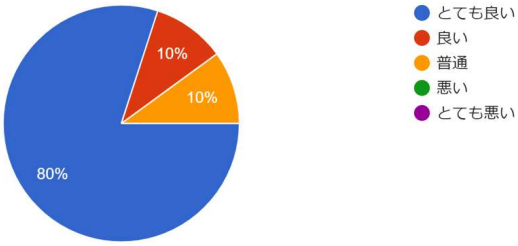


図 8　操作に関する評価結果

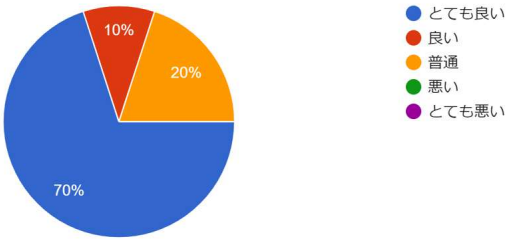


図 9　コンテンツに関する評価結果

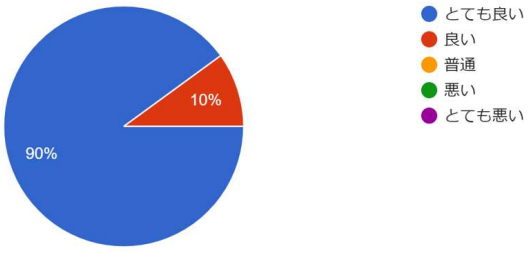


図 10　発信内容に関する評価結果

アンケート結果を図 6～12 に示す．アンケート結果を踏まえると，ゼミ紹介 Web サイトは利用者からの視点で概ね満足できる結果であった．また，「過去の研究テーマが知りたい」，「暗い色の背景に暗い色の文字で見づらいところがあった」等のコメントがあった為，今後の改善が必要である．

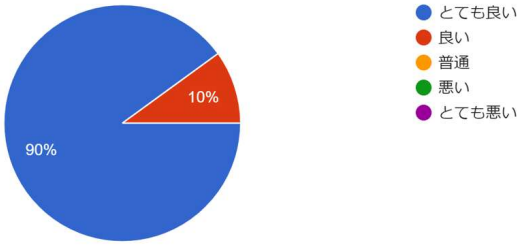


図 11　パフォーマンスに関する評価結果

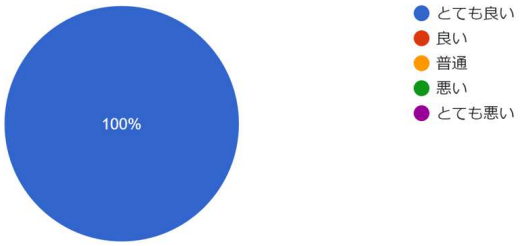


図 12　モバイル端末での可読性に関する評価結果

6. 考察

この章では，本研究を通して得られた成果に関して考察を行う．

1 つ目は，クラウドコンピューティングの特長や AWS の利点を活かした Web サイトの開発が容易なことである．クラウドコンピューティングではサーバ，ストレージ，データベース等がインターネットを通じて提供されており，サーバ機器等の設置が必要ない．その為，手間をかけずに Web サイトの構築を行うことができる．また AWS では 200 種類以上のサービスが用意されている為，目的や用途によって適切なサービスを選択可能である．

2 つ目は，AWS が提供するマネージドサービスを活用し，サーバレスアーキテクチャ構成の Web サイト運用を行なったことである．企業の開発現場では複数のサービスを活用しながらシステムの構築，運用がなされる場合が多く，コストパフォーマンスや運用の容易さを意識したサービス選択が行われる．本研究ではマネージドサービスのみを採用した構成の為，個別サーバの運用をする必要がない．

改善点としては，過去の研究テーマの追加や，研究以外の活動内容の掲載といったゼミ紹介 Web サイトの新たなコンテンツの追加である．現時点での Web サイトの項目としては，ホーム，研究概要，学生の取り組み，お問い合わせフォームとなっている為，今後さらに掲載するコンテンツを充実させ，Web サイトに訪問してきた人々の満足度を上げるような記事や

内容の記載が必要である．

今後の課題は，研究内容の詳しい紹介や新たなAWS サービスの追加等が考えられる．現段階では研究概要は簡潔なものとなっている為，研究分野の基礎的な用語や活用法の紹介など研究内容の更なる周知は可能なのではないかと思われる．また，機能面では Web サイトの URL が CloudFront で作成したURL となっている為，Amazon Route53 を使用した独自ドメインの取得等が考えられる．

7. まとめ

研究成果の情報発信を目的としたゼミ紹介 Web サイトをクラウドコンピューティング上に開発した．また，開発において AWS が提供するマネージドサービスを使用したサーバレスアーキテクチャ構成にすることで，運用の手間を低減しつつ，可用性に優れたWeb サイトを実現した．

謝辞

ゼミ紹介 Web サイトの開発に協力していただいた荒金諒氏に感謝します．

参考文献

(1) 総務省: 情報通信白書 令和 5 年版, 2024 年 6 月 6 日, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd24a210.html,

(2) 電子情報通信学会，情報セキュリティハンドブック，オーム社，2004.

(3) トレンドマイクロ，DDoS 攻撃，2024 年 6 月 6 日，https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ddos.html

(4) D. L. Cook, W. G. Morein, A. D. Keromytis, V. Misra, and D. Rubensteiny: WebSOS: Protecting Web Servers From DDoS Attacks, Proceedings of the 11th IEEE International Conference on Networks, ICON2003, pp.461-466, 2003.

(5) K. Singh, P. Singh, and K. Kumar: Application layer HTTPGET flood DDoS attacks: research landscape and challenges, Journal of Computers and Security, vol.65, pp.344–372, 2017.

(6) G. A. Jaafar, S. M. Abdullah , and S. Ismail: Review of Recent Detection Methods for HTTP DDoS Attack, Journal of Computer Networks and Communications, vol.2019, Article ID 1283472

(7) M. Darwish, A. Ouda, and L. F. Capretz: Cloud-based DDoS Attacks and Defenses, Proceedings of the IEEE International Conference on Information Society (i-Society 2013), pp.67-71, 2013.

(8) G. Somani, M. S. Gaur, D. Sanghi, M. Conti, R. Buyya: DDoS attacks in cloud computing: Issues, taxonomy, and future directions, Journal of Computer Communications, vol.107, pp.30–48, 2017.

(9) A. P. Rajan R: A review on serverless architectures - function as a service (FaaS) in cloud computing, Journal of the TELKOMNIKA Telecommunication, Computing, Electronics and Control vol.18, no.1, pp.530-537, 2020.

(10) 常盤 祐司: WordPress を用いた大学研究所向けモバイル対応 Web サイト開発, 情報処理学会研究報告, vol.2013-CLE-10, no.1, pp.1-6, 2013.

(11) 株式会社日経 BP コンサルティング: 大学スマホ・サイト ユーザビリティ調査 2023-2024, 2024 年 6 月 6 日, https://consult.nikkeibp.co.jp/info/news/2023/1027sus/

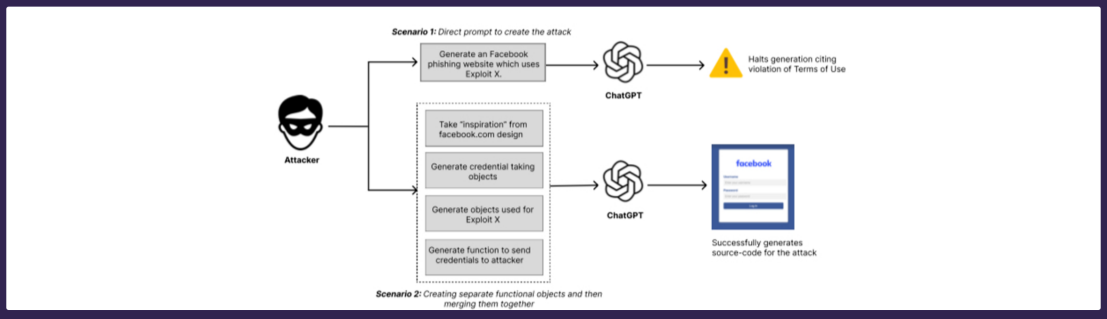
Appendix

学生の卒業研究（一例）を図 13 に示す．

Chat GPTを使用したマルウェアの作成

研究の背景と概要

昨今, 人工知能の進化により, セキュリティ分野でも新たな課題が浮上している. 特に懸念されているのは, ChatGPTなどの自然言語処理モデルを悪用し, マルウェアを開発・拡散する動きが増加していることだ. これらのモデルは本来, 情報提供や教育のために設計されたものであるべきだが, 悪意ある個人や団体によって逆手に取られ, セキュリティに関する悪用が増加傾向にある. そこで, 本研究では, サイバーセキュリティを勉強中の, プロフェッショナルとは言い難い大学生であっても, マルウェアを作成出来るのかどうか検証を行った. 今回の実験で作成したマルウェアは, EMOTETを想定して作成した. 実行すると, PC上のルートディレクトリに移動し, 全ファイル及びフォルダを暗号化して別のPCに転送し, 元のデータは全消去するという, 非常に危険なプログラムである.



Chat GPTとは何か？

ChatGPTはOpenAIが開発した自然言語処理モデルで, 大量のテキストデータから学習して自然な対話を生成することができる人工知能プログラムである. ChatGPTはテキストベースの質問応答, 対話生成, 情報提供, 言語理解などのタスクに利用され, 一般ユーザーや開発者はChatGPTを利用して, さまざまな情報の検索, テキスト生成, アシスタントとしての利用など, 幅広い用途に応用することができる.

使用したサービス

- **Chat GPT 4**
  Chat GPT の最新バージョンであり, より人間らしい自然な対話や高度な処理が行え, データ分析などにも活用される. 今回の実験では, 無料版の3.5ではなく, 4を使用した.

- **Virus Total**
  ファイルやURLをスキャンしてウイルスやマルウェアの有無を確認するオンラインサービスである. ユーザーはファイルをアップロードするか, URLを提出して, 実行でき, 悪意のあるコンテンツかどうか, セキュリティリスクの有無を評価できる.

図 13　学生の卒業研究（一例）