安全な未来、私たちが創る！

令和5年度　卒業研究サイバーセキュリティ科

2023 年 12 月 22 日(金)　9:00-11:35　卒業研究中間発表会(オンライン)
2024 年　2月　6 日(火) 14:00-16:35　NS/NE 合同卒業研究発表会(904教室)
2024 年　2月 16 日(金) ～ 17日(土)　卒業制作展　サイバーセキュリティ科(511 実習室)

「AI とセキュリティ」をテーマに、セキュリティ監視・運用業務における AI 活用方法や AI 自身のセキュリティに関する研究結果を報告します。

～ 令和5年度 NE 科「卒業研究」タイトル一覧 ～

A 班

「AIを組み込んだメールサーバで有害メールの検知は可能か？」
～データセットを利用した特徴表現学習～

B 班

「ChatGPTの個人情報流出を防ぐには？」
～やるべき ChatGPTの設定と入力すべきではない入力情報～

C 班

「DoS 攻撃を AI を用いて検知・解析が可能か?」
～AI による HTTP フラッド攻撃を検知・解析の検証及び異常検知～

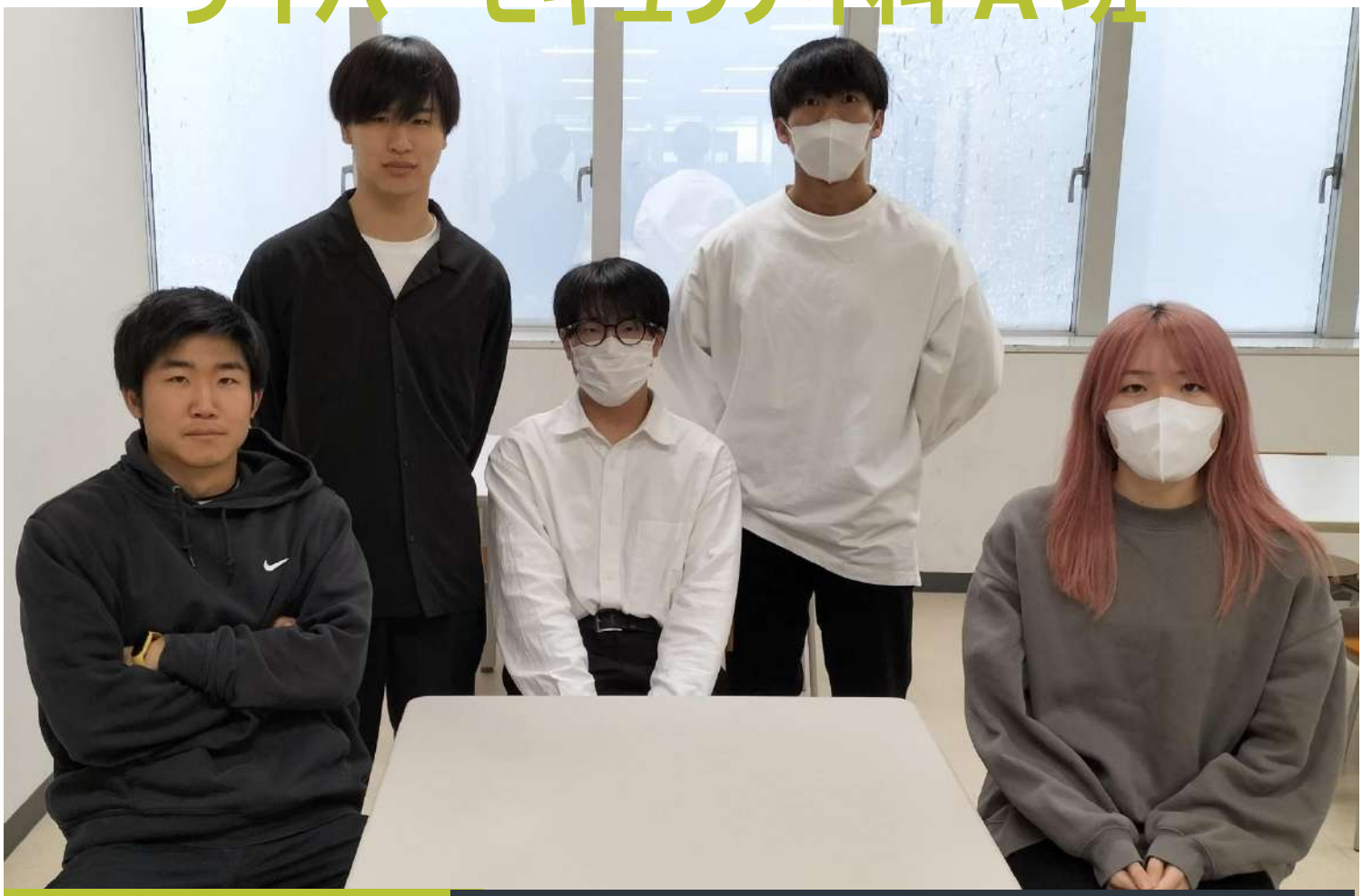
D 班

「AI を利用して不明な IP アドレスからの接続を検知することは可能か？」
～Elastic Stack の機械学習を用いた不正アクセス検知におけるデータ分析とアラートの自動化～

E 班

「キーボードのタイプ音から AI を使って入力文字を解析できるのか？」
～ディープラーニングベースの音響サイドチャネル攻撃コードを
用いたソフトの精度と対処法の検討～

サイバーセキュリティ科 A 班



メンバー紹介

- ネットワーク環境構築担当

  木村茂樹

- AI 開発担当

  安藤大輝
  森岡柊哉
  角掛彩月

- プロジェクト管理担当

  寺崎涼貴（リーダー）

「AI を組み込んだメールサーバで有害メールの検知は可能か？」
～データセットを利用した特徴表現学習～

＜研究の背景＞

・AI を有効に活用できるから。
・年々フィッシングメールによる被害数が増加していっているから
・有害なメールの被害にあいかけた班員がおり、より身近なサイバー攻撃に感じたから

＜期待される効果＞

・未知の脅威に対する防御の向上
・特徴表現学習により有害なメールの検出率向上と、誤検知率の低下
・予測モデルの高度な特徴表現学習により、メールサーバの攻撃検知を　自動化できる

＜研究の特色＞

・データセットから有用な特徴を抽出し、自作の AI に学習させる

＜研究の意義＞

有害なメールの攻撃は企業や個人にとって重大なリスクであるとともに個人情報や機密データの漏洩などの数多くのリスクも伴う。そのためこの研究でセキュリティの向上及びユーザの保護につなげる。また、メールは日常的なコミュニケーションの手段であり、安全性は個人や組織の日常生活に大きな影響を与えるため、セキュリティの向上は個々の安心感及び、利益をもたらす可能性がある。

東北電子専門学校　ネットワーク・セキュリティ系　サイバーセキュリティ科
〒980-0013 仙台市青葉区花京院 1-3-1　電話番号: 022. 224. 6501
https://jc-21.ac.jp/course/ne/

サイバーセキュリティ科 B 班

メンバー紹介

- ChatGPT セキュリティ調査・検証担当
  佐々木　海斗
  齋藤　優太
- 卒研プレゼン担当
  佐々木　海斗（※兼任）
  齋藤　優太（※兼任）

「chatgpt の個人情報流出を防ぐには？」
～やるべき chatgpt の設定と入力すべきではない入力情報～

＜研究の目的＞

ChatGPT で行われているセキュリティ対策について理解を深め、安全性に配慮した活用を目指す。

＜研究の背景＞

近年、ChatGPT などの生成 AI への関心が高まっている。ChatGPT は入力された情報を学習データとして活用しているため、セキュリティ上の課題が存在する。この状況を踏まえ、卒業研究では ChatGPT を安全に使用できるように調査を行う。

＜研究の意義＞

ChatGPT のセキュリティ上の問題点や危険性について調査する。

＜研究の特色＞

実際に ChatGPT を使用して調査や検証を行い、ChatGPT のセキュリティ対策の有効性を確認する。

＜期待される効果＞

ChatGPT のセキュリティ対策に関する学習が進む。

東北電子専門学校　ネットワーク・セキュリティ系　サイバーセキュリティ科
〒980-0013 仙台市青葉区花京院 1-3-1　電話番号: 022. 224. 6501
https://jc-21.ac.jp/course/ne/

サイバーセキュリティ科 C 班

メンバー紹介

- サーバ構築担当
  菅野 匡寛（リーダー）
- AI 構築担当
  相馬 優里香
  細田 大誠
- 仮想ネットワーク構築・管理担当
  小澤 尚則
  鳥居 優輝

「DoS 攻撃を AI を用いて検知・解析が可能か？」
～AI による HTTP フラッド攻撃を検知・解析の検証及び異常検知～

《研究の目的》

リアルタイムでのアクセスログから不正なアクセスや異常なトラフィックを自動的に検出するシステムを構築し、AI を用いて、従来の手法よりも高度な検出能力を持つシステムを開発する。

《研究の背景》

DoS 攻撃は、システムやネットワークに深刻な影響を及ぼす可能性があり、有名なオンラインサービスや企業がサービス提供の中断や経済的な損失が発生したケースがある。DoS 攻撃は高度なテクニカルスキルを必要とするため、DoS 攻撃に対する対策を研究することで、技術的なスキルを向上させる機会となり、新たなセキュリティ対策 や防御戦略を研究し、イノベーションの機会を提供する。

《研究の意義》

DoS 攻撃手法の中に HTTP フラッド攻撃がある。HTTPフラッド攻撃は数ある DoS 攻撃手法の中で検出が困難といわれている。HTTP フラッド攻撃は通常のトラフィックに非常に似ており、攻撃者は合法的な HTTPリクエストを用いて攻撃を行うため不正なトラフィックと区別するのが難しい。今回は、AI を用いて困難と言われている HTTP フラッド攻撃を検知し、Web サーバに対するセキュリティを向上させていく。

《研究の特色》

AI という先進技術をログ解決の領域に適用することで、高度な分析を可能にする。また、AI の応用範囲を拡大し、他のサイバーセキュリティ領域への展開も可能とする。包括的で強固な防御体系を構築する。

《期待される効果》

・高度な異常検知能力を持つシステムの開発
・Web サイトのセキュリティ強化
・AI と機械学習を活用したセキュリティ対策の新たな手法の提供

東北電子専門学校 ネットワーク・セキュリティ系 サイバーセキュリティ科
〒980-0013 仙台市青葉区花京院 1-3-1　電話番号: 022. 224. 6501
https://jc-21.ac.jp/course/ne/

サイバーセキュリティ科 D 班

「AI を利用して不明な IP アドレスからの接続を検知することは可能か？」
～Elastic Stack の機械学習を用いた不正アクセス検知におけるデータ分析とアラートの自動化～

メンバー紹介

- ElasticStack 構築班
  湯瀬 倖大（リーダー）
  机地 祐斗
- 情報収集班
  小林 光貴
  鎌田 蓮
- 記事制作担当
  鎌田 蓮（※兼任）

・研究の目的

日々問題となっている不正ログインに対し、ElasticSearch の機械学習の機能を使用し、試行回数や施行時間、IP アドレスの観点から予測しアラートを出すまでの一連の動作を自動化する

・研究の背景

セキュリティ問題に大きくかかわっている不正ログインに対して、機械学習を用いてそのパターンを学習し、検知することができるのではないかと考えた。それを実現するうえで 2 年時に学習した ElasticSearch に教師ありの機械学習を活用する機能があることを発見したため、ElasticSearch の機能をより深く理解するためにもこの機能を使用することを決めた。ElasticSearch には、検知からアラートまで幅広い機能が備わっているためそれら一連の動作を自動化することで、ブルートフォースなどの攻撃に対し２４時間３６５日対応することができる

・研究の意義

セキュリティの強化や自動化された検知、アラートによる業務効率の向上を ElasticSearch により実現できることを示す。それにより、人的な作業を減らし一連の作業をより効率よく正確に行う機能を目指す。また、ElasticSearch の機能を使用することによって機械学習により不正検知をより身近なものとなるようにしていきたい。

・研究の特色

ElasticSearch に関する機能をより深く理解し、検知からアラートまでが自動化されてるため手動の監視や分析の必要が減少と早期発見による素早い対応による、被害を最小限に抑えることができる。

・期待される効果

セキュリティ向上のための効果として主に早期検出と対応、効率的な運用の２つが挙げられる。

早期検出と対応は、インシデントを早期に見つけ対応を図ることで攻撃によるセキュリティ侵害の影響を最小化することができる。また、効率的な運用は一連の作業を自動化させることによって人的リソースが少なくより正確に検出を行うことができる。これにより、不正アクセスによる侵入のリスクや被害を低減し、個人情報などの情報資産の保護を強化する効果を期待できる。

東北電子専門学校 ネットワーク･セキュリティ系 サイバーセキュリティ科
〒980-0013 仙台市青葉区花京院 1-3-1　電話番号: 022. 224. 6501
https://jc-21.ac.jp/course/ne/

サイバーセキュリティ科 E 班

メンバー紹介

- AI 開発担当
  北嶋　優翔
- データセット開発担当
  柴田　和茂
- プレゼンテーション製作担当
  村上　陽斗
- プロジェクト管理担当
  阿部　凪透（リーダー）

「キーボードのタイプ音から AI を使って入力文字を解析できるのか？」
～ディープラーニングベースの音響サイドチャネル攻撃コードを用いたソフトの精度と対処法の検討～

研究目的

テレワークの普及による音響サイドチャネル攻撃の拡大をうけ、攻撃の防御策と対処法、精度を研究する。

＜研究の背景＞

事例を見てとても高い興味を持ったこと テレワークを用いることが近年増えてきて、入力内容を推測可能とのことで身近に攻撃ができることの啓蒙

＜研究の意義＞

音響サイドチャネル攻撃の研究は、情報セキュリティの多様性と深さを理解し、それに応じた対策を講じることの重要性を強調している。

＜研究の特色＞

物理的環境から得られる音響データを利用して情報を漏洩または推測する点にある。システムだけでもなく物理的な攻撃を研究する。

＜期待される効果＞

セキュリティの向上

新しい攻撃手法の発見

ハードウェアの安全性の確認

セキュリティ教育・啓発

基礎研究

東北電子専門学校　ネットワーク・セキュリティ系　サイバーセキュリティ科
〒980-0013 仙台市青葉区花京院 1-3-1　電話番号: 022. 224. 6501
https://jc-21.ac.jp/course/ne/