Project No.18 暗号とセキュリティ

メンバー　中村碧 Aoi Nakamura　北山奏 Kanata Kitayama　白井一樹 Kazuki Shirai　源平連太郎 Rentarou Genpei　野澤真生 Masaki Nozawa　森谷史奏 Shion Moritani

東未来翔 Mikuto Azuma　原健宏 Takehiro Hara　青山慎太郎 Shintaro Aoyama　斉藤波平 Namihei Saito　岡本英太 Eita Okamoto

担当教員　白勢政明 Masaaki Shirase　由良文孝 Fumitaka Yura

プロジェクト概要 Overview

人を守るセキュリティ技術、自分で守るセキュリティ意識、CTFに挑戦する。

一昨年の新型COVID19の影響により、オンライン授業やリモートワークが普及した。そこで、本プロジェクトは情報を守るセキュリティ技術や攻撃手法について学習し、効果的な暗号技術の利活用について考える班と、それを扱うユーザのセキュリティ意識の改善を目標とする班に分かれて活動する。また、ITに関する知識を深め様々な問題を解くCTFにも挑戦する。

Due to the impact of the COVID19 the year before last, online classes and remote work have become widespread. Therefore, this project will be divided into two groups: one group will study security technologies and attack methods to protect information and consider effective use of cryptography, and the other group will aim to improve the security awareness of users who handle such information. In addition, the group will deepen their knowledge of IT and try to solve various problems in CTF.

暗号班 Cipher

背景 Background

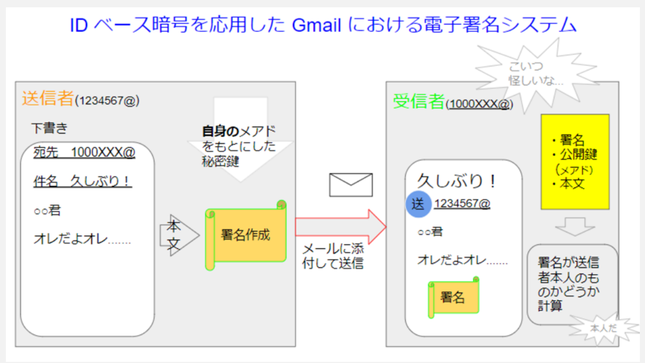
背景として標的型攻撃メールというインシデントがある。標的型攻撃メールとは対象の組織から重要な情報を盗むことを目的として、組織の担当者が業務に関係するメールだと信じてしまうように巧妙に作り込まれたウイルス付きのメールのことだ。メールの内容が送信者の意図したものであるかの確証が必要であるため、IDベース暗号を用いて電子署名をメールに追加する機能の開発を行う。

As a background, there has been an incident of targeted attack e-mails. Targeted attack e-mails are e-mails with viruses that have been cleverly designed to make the person in charge of the organization believe that the e-mail is related to his or her work in order to steal important information from the target organization. Since it is necessary to verify that the contents of the email are what the sender intended, we will develop a function to add a digital signature to the email using ID-based encryption.

成果物について Deliverables

IDベース暗号を用いることによって、公開鍵の取得が容易（受信者側が）IDベース暗号を用いることによって、電子署名を添付ファイルとして作成し、メールの受信者がその内容を検証することで、メールの内容が改ざんされていないか確認することができるシステムをchrome拡張機能に実装した。この成果物は、IDベース暗号を用いたことで、既存の電子署名より受信者側の公開鍵の取得が容易である点が特徴である。成果物を通して、IDベース暗号によるメールへの電子署名の実現可能性について示唆することができた。

By using ID-based encryption, it is easy for the recipient to obtain a public key (on the recipient's side). extension. This artifact is characterized by the fact that it uses ID-based cryptography, which makes it easier to obtain the recipient's public key than existing digital signatures. Through this work, we were able to suggest the feasibility of using ID-based cryptography to digitally sign e-mails.



Webページ Web

背景 Background

（図）にあるようにサイバー犯罪の検挙数が毎年、増加傾向にありインターネットを利用した犯罪に巻き込まれる危険性が高くなった。そのことから、情報セキュリティの学習や意識向上を目標にして「クイズ」と「サイバー攻撃の疑似体験」が出来るWebページの作成を目指す。

As shown in the figure, the number of arrests for cyber crimes has been increasing every year, and the risk of being involved in Internet-based crimes has become higher. Therefore, we aim to create a web page where users can take a "quiz" and experience a simulated cyber-attack with the goal of learning and raising awareness of information security.

成果物について Deliverables

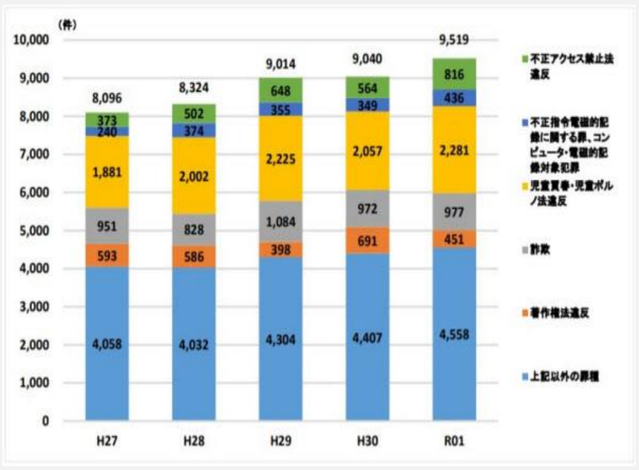
クイズページは情報セキュリティ10大脅威2022を参考に具体的なサイバー攻撃の対策を学習してもらうクイズを作成した。疑似体験ページではランサムウェアについて脅威を伝えられるようなページを制作した。

The quiz page has created a quiz to help students learn about specific cyber attack countermeasures with reference to the Information Security 10 Major Threats 2022.We created a simulated page to convey the threat about ransomware.

今後の展望 Future Tasks

アンケートの結果を受け止めて改善を行う。また、全体的なデザインの改修。

Accept the results of the questionnaire and make improvements. In addition, the overall design renovation.



（図）サイバー犯罪の検挙件数の推移
https://www.nikkei.com/article/DGXMZO56548840Z00C20A3000000/

CTF班 CTF

背景 Background

未来大生は、IT企業に就職する学生が多いにも関わらず、セキュリティ分野の講義では座学が中心であり、実践的な演習は行われない。そのため、実際にセキュリティ分野の問題に直面したときに、問題解決できる学生は少ない。本グループでは初心者向けCTFサイトを作ることを課題とした。CTF(Capture The Flag)とは、情報セキュリティの知識や技術を駆使し、隠されたFlag(正解)を見つけるハッキングコンテストの一種であり、実践的にセキュリティの技術を身に着けるために最適なコンテンツである。

Despite the fact that many Fun students are employed by IT companies, lectures in the security field are mainly classroom lectures and do not include practical exercises. As a result, few students are able to solve problems when faced with actual problems in the security field. Our group's goal is to create a CTF site for beginners, Capture The Flag (CTF), which is a kind of hacking contest to find a hidden Flag (correct answer) by making full use of information security skills and knowledge. It is the best content for practically acquiring security skills.

成果物について Deliverables

CTf班は未来大生にも優しいCTFサイトを作成した。問題のジャンルはWeb、ネットワーク、暗号、Miscである。このサイトを通じてCTFを始めるきっかけとなってくれると嬉しい。

The CTF group created a CTF site that is friendly to Future University students. The genres of the problems are Web, Network, Cryptography, and Misc. We hope that this site will help you to start CTF.

今後の展望 Future Tasks

今後の展望として、よりわかりやすい解説の作成、問題数の拡充をしていきたい。

In the future, we would like to create more easy-to-understand explanations and expand the number of questions.