# project No.19 暗号とセキュリティ


メンバー　今井徹雄 Tetsuo Imai　相馬尚輝 Naoki Soma　廣井悠真 Yuma Hiroi　村上光 Hikaru Murakami　山端祐輝 Yuki Yamahata
岩舘玲於奈 Reona Iwadate　小原賢太 Kenta Ohara　佐藤壱馬 Kazuma Sato　多田龍生 Ryusei Tada　松村涼 Ryo Matsumura　山崎将也 Shoya Yamazaki

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

**"自分が守られる"セキュリティ技術と、"自分で守る"セキュリティ意識について考える**

主に昨年度から新型コロナウイルスの影響により、オンライン授業やリモートワークの増加した。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、より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把握と改善を目標とする班に分かれて活動する。

**Thinking about security technology that "protects us" and security consciousness that "protect by myself".**

Online lessons and remote work had increased mainly influenced by COVID-19 since last year. Therefore, this project is divided into two groups. One group learns about security technology that protects information and attack methods and thinks about effective use of cryptographic technology. The other group aims to understand and improve the security consciousness that the user handles.

## Web ページ作成班 Web page creation

### 背景 Background

昨年行ったアンケートから未来大生のセキュリティ意識が低いことがわかった。また、IPA の調査より、フィッシング詐欺の遭遇率が高いことや、10 代と 20 代の半数がセキュリティ対策をしていないことがわかった。我々はこの状況を危機的な状況と考えこの問題を解決するため、サイバー攻撃疑似体験班とクイズ作成班に分かれて**未来大生のセキュリティ意識を向上させることを目的とした Web ページ**を作成した。

From the questionnaire conducted last year, it was found that the security awareness of FUN students is low. In addition, an IPA survey found that the rate of encounters with phishing scams was high, and that half of teens and twenties did not take security measures. We consider these situations to be critical situations, and in order to solve this problem, we divided into a cyber attack simulated experience group and a quiz creation group and created a web page aimed at raising the security awareness of FUN students.

### サイバー攻撃疑似体験 Cyber attack simulated experience

フィッシング詐欺の疑似体験ができる Web ページを作成した。メールからの誘導によって個人情報を盗まれる流れをブラウザ上にて再現しており、擬似体験後にフィッシング詐欺の対策を学べる構成になっている。なお、擬似体験後のページには、フィッシング詐欺の対策などの情報と他のサイバー攻撃についての情報を掲載した。

We have created a web page that gives you a simulated experience of phishing scams. This website reproduces the flow of personal information being stolen by e-mail guidance on the browser, and is structured so that you can learn countermeasures against phishing scams after a simulated experience. In addition, on the page after the simulated experience, information such as countermeasures against phishing scams and information on other cyber attacks are posted.

### クイズ作成 Quiz creation

自分の環境に適したセキュリティソフトを提示する Web ページを作成した。二者択一の 6 問に答えるだけで、最適なセキュリティソフトを知ることができる。また、コンピュータウイルスの種類や感染経路、セキュリティの向上方法などの情報を掲載した。

We created a web page that presents security software suitable for my environment. You can know the most suitable security software just by answering 6 alternative questions. In addition, information such as the types of computer viruses, infection routes, and security improvement methods is posted.

図 1．Web ページの QR コード
https://ganshishi.github.io
/FUN2021_project19_security_top/

## メールクライアント班 Email software development

### 背景 Background

コロナの影響で選挙の際、実際に現地に行き投票することが難しくなり、メールでの投票システムが注目された。そこで本グループはメールでの**投票システムに使われる送信者が受信者の復号できる日時を指定できるタイムリリース暗号**をメールシステムに実装した。

Due to the effects of Corona, it became difficult to actually go to the site and vote during elections, thereby, an e-mail voting system attracted attention. So, our group implemented a time-release cryptosystem that allows the sender to specify the date and time when the recipient can decrypt the message.

### 方法・仕様 Method / Specifications

①: 送信者がパラメータを貰う
②: 送信者は復号時刻の文字列を鍵として暗号化したファイルと復号時間をメールサーバを通して受信者に送る
③: 受信者は送られてきた復号時間を鍵生成局に渡す
④: 鍵生成局は時間になったら受信者に復号鍵 ( 時間鍵 ) を渡す

①: The sender gets the parameters.
②The sender sends the encrypted file and the decryption time to the recipient through the mail server using the decryption time string as the key.
③The recipient passes the decryption time to the key generation station.
④The key generation station passes the decryption key (time key) to the recipient when the time is up.

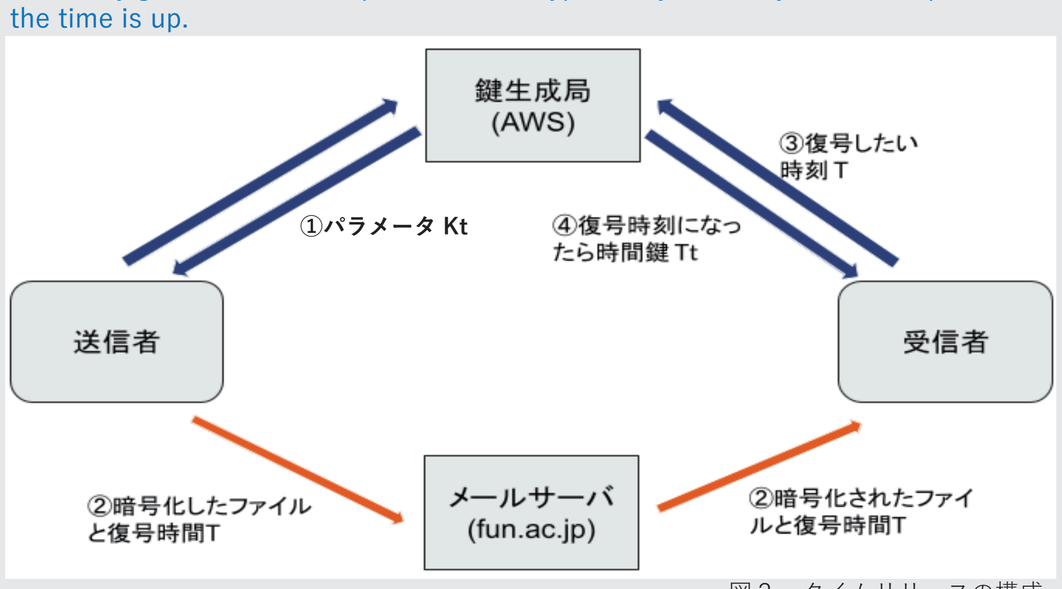


図 2．タイムリリースの構成

### 課題・展望 Issues / Prospects

Chrome 拡張で実装した関係上、添付したファイルを直接暗号化や復号をすることができないこと
　　ー＞新規にメールシステムを作成する際には応用が可能

Due to the fact that it was implemented as a Chrome extension, it is not possible to encrypt or decrypt the attached file directly.
　　ー＞It can be applied when creating a new mail system.

## スケジュール Schedule