関研究室
Seki Laboratory

研究室紹介

目次

求める人物像

- 情報セキュリティに興味がある人
- 協調性のある人
- 研究熱心な人
- リーダシップがある人
- 仕事に責任を持てる人
- 積極性のある人
- コミュニケーション能力がある人

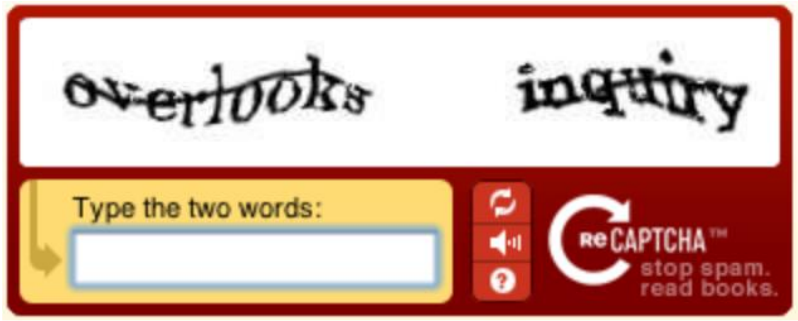
事例研究紹介

ヒトに易しく、機械による解析が難しいCAPTCHAの調査

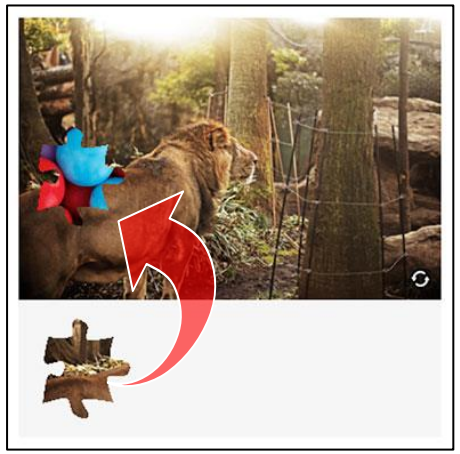
≪CAPTCHAとは≫

人間とマシンを判別するチューリングテスト

人が画像を目で見て確認し、そこに描かれている文字列などを読み取って入力することで、ログイン操作を行っているのがコンピュータではなく人間であることを担保するという技術。
→ユーザ認証ではない



↑　文字型CAPTCHA
http://www.captcha.net.
（AIの識字率が上がり現在では使用停止）
reCAPTCHA v2　→
https://www.google.com/recaptcha/about/



↑　Capy社提供パズルCAPTCHA
https://corp.capy.me/ja/product/captcha

≪パズルCAPTCHAの優位性≫

- 優れたユーザビリティ

ユーザがログインするための操作は、パズルのピースを指定場所に移動させるだけ
→ある企業で、文字CAPTCHAからパズルCAPTCHAに変更後、13%もあった離脱率が、2%にまで激減

- 高いセキュリティレベル

動かされたピースの軌跡を分析し、その動き方や速度などからヒトかボットかの判別を行っている

指紋認証の仕組みと事例調査

指紋認証　＝　アルゴリズム　×　センサ方式の2つが肝となり成り立つ

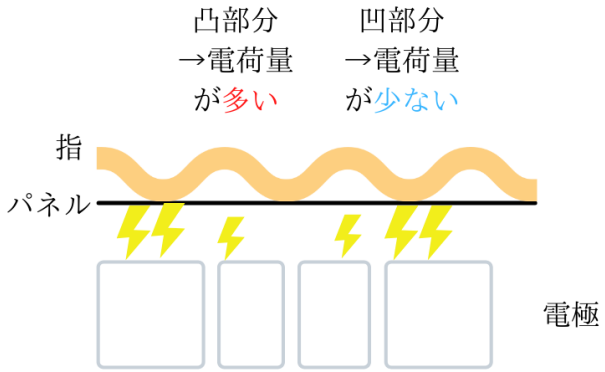
※アルゴリズムとは問題に対する解法の手順のこと
代表的な方法の中の1つを紹介します。

1.特徴点抽出方式・・・指紋紋様の盛り上がった部分の端点や分岐点といった属性を特徴として捉える

○端点・・・指紋が途切れている点
○分岐点・・・指紋の線が分岐している点

※センサ方式とはセンサを用いてマッチングを行う方式
代表的な方法の中の１つを紹介します。

1.静電容量方式・・・電荷の変化の量で指紋の形を判別する方式



例えば一部iphoneに搭載されている指紋認証では・・・
特徴点抽出方式　×　静電容量方式が使われています。

顔認証における安全性とセキュリティ問題の調査

【調査理由】

- 新型コロナウイルスの影響で、非接触の生体認証はニーズが高まっている
- 普及に伴い、顔認証技術が発展している
- 自身のPCにも搭載されており、興味を持った

【顔認証の特徴】

- なりすましが困難である
- 物理的な鍵やパスワードが不要になる
- 非接触・非拘束で認証ができる
- 一般的なWebカメラで利用することができる

【顔認証の流れ】

【Windowsの顔認証の精度】

他人受入率（他人の生体情報で認証が通ってしまう確率）	認証が正常に動作する確率	本人拒否率（本人の生体情報で認証が拒否されてしまう確率）
0.001%未満	95%以上	5%未満

※Microsoft Docsより

→暗闇、マスク、メガネなどの特殊な状況においても、
上記の精度で認証が行えるのか疑問が残った

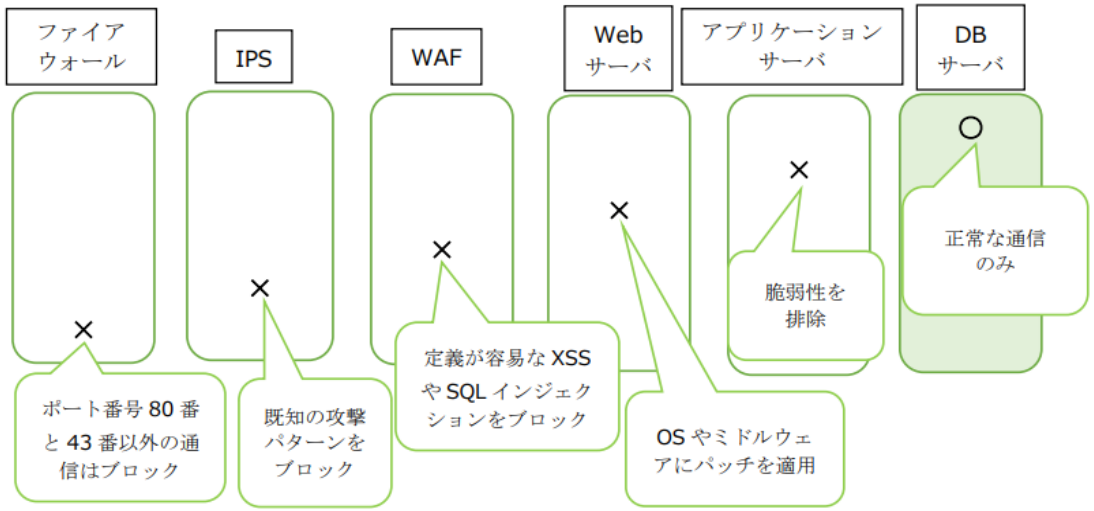
einc.co.jp)より

Web Application Firewall(WAF)の検知手法に関する調査

WAFの役割

・Web サイト上のアプリケーションに特化したファイアウォール

・通常Webサーバの前面に配置され、ユーザーからの入力やリクエストに対して、データの中身をアプリケーションレベルで解析して無害化する

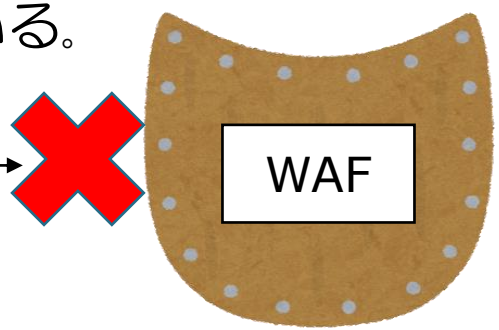


ここが、ファイアウォールと違う！

検知手法

一般的にはシグネチャによる検知が主流である。実行プロセスは、攻撃で良く利用される固有のアクセスパターン（シグネチャ）をあらかじめ登録しておき、Web サーバに送られる通信（リクエスト）の内容にマッチすれば攻撃と判定する流れとなっている。

攻撃者



Webサーバ

卒業研究紹介

卒業研究

ファイルレスマルウェアの特徴を善用した電子投票システムに関する研究

メディア情報学部　情報システム学科

1872093　　山口拓人

研究背景

- 「ファイルレスマルウェア」と呼ばれるサイバー攻撃の被害が増加している

- ウィルス対策ソフトの検知を逃れるために他のマルウェアとは異なる特徴を持っている

ファイルレスマルウェアの特徴

- OS に標準で搭載されている機能を利用する[1]
- マルウェアをメモリ上に呼び出して実行する[2]
- 実行ファイルを持たない[3]
- ソースコードの難読化が容易である[3]

[1] 山田拓也,”ウイルス対策ソフトを突破?「ファイルレスマルウェア」PowerShell が備える、システム管理の利便性とセキュリティリスク”,
https://bizdrive.ntt-east.co.jp/articles/dr00095-001.html
[2] 宮田昌紀,”ファイルレスマルウェアとは”,
https://www.amiya.co.jp/column/fileless_20210129.html
[3] マカフィー株式会社 マーケティング本部,”ファイルレスマルウェアの脅威！仕組みと感染経路からみる実践的対策”,
https://blogs.mcafee.jp/what-is-fileless-malware#2-3

ファイルレスマルウェアの仕組み

ファイルレスマルウェアは、４ 段階で攻撃を行う[1]

第 １ 段階：攻撃者がマルウェアを呼び出すスクリプトが
含まれた添付ファイル付きメールを送信

第 ２ 段階：添付ファイルを開くことで感染

第 ３ 段階：感染後、外部の C&C サーバに接続

第 ４ 段階：様々なマルウェアをメモリ上で実行

[1] 山田拓也,”ウイルス対策ソフトを突破?「ファイルレスマルウェア」PowerShell が備える、システム管理の利便性とセキュリティリスク”,
https://bizdrive.ntt-east.co.jp/articles/dr00095-001.html

研究目的

ファイルレスマルウェアはウィルス対策ソフトに
対して「秘匿性」を持っている

→ 既存の情報システムに有効利用できないか

ファイルレスマルウェアの持つ特徴と仕組みに着目し、
善用した電子投票システムの提案・検証を行う

提案する電子投票システム

投票システム：　投票システムの本体

ダウンローダ ：　外部サーバ上から投票システムをメモリにダウンロード・実行する

選挙管理者　：　投票システムを実行し、選挙情報入力やパスワードの配布を行う

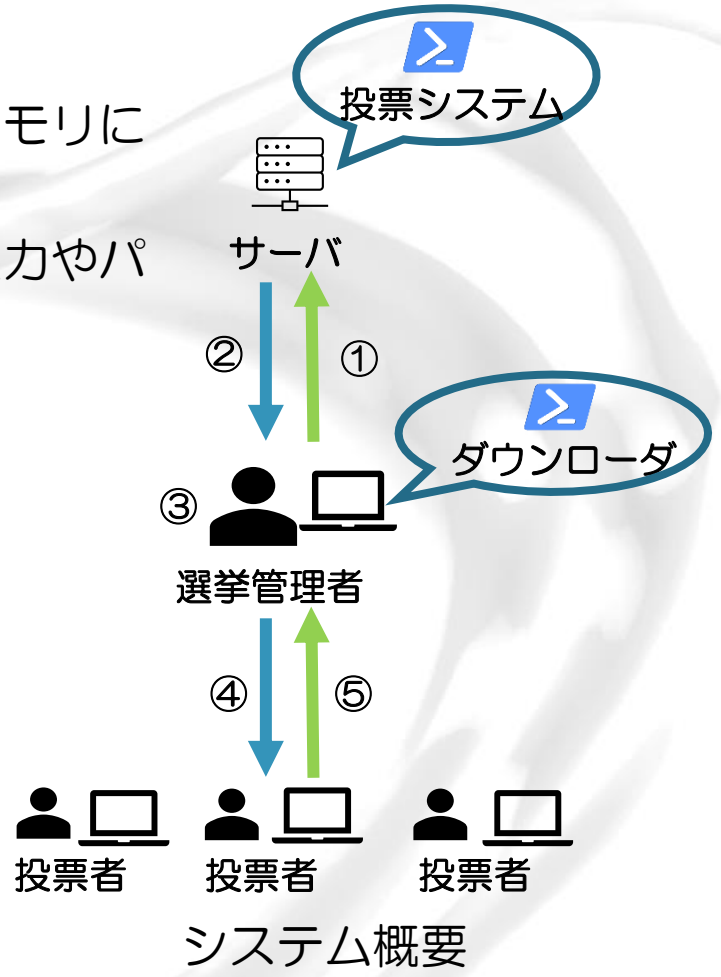
① ダウンローダから投票システムを呼び出す

② 投票システムを選挙管理者PCのメモリ上でダウンロード・実行

③ 投票に必要な情報を入力

④ 投票用のURLとパスワードを配布

⑤ URLにアクセスし、選挙管理者のPCへ投票



システム概要

投票システムに取り入れた特徴

- OS に標準で搭載されている機能を利用する
  → ダウンローダと投票システム本体をWindows 10に標準されている「PowerShell」を利用
- メモリ上で実行する
  → ダウンローダから投票システムを選挙管理者PCのメモリ内に呼び出す

検証項目

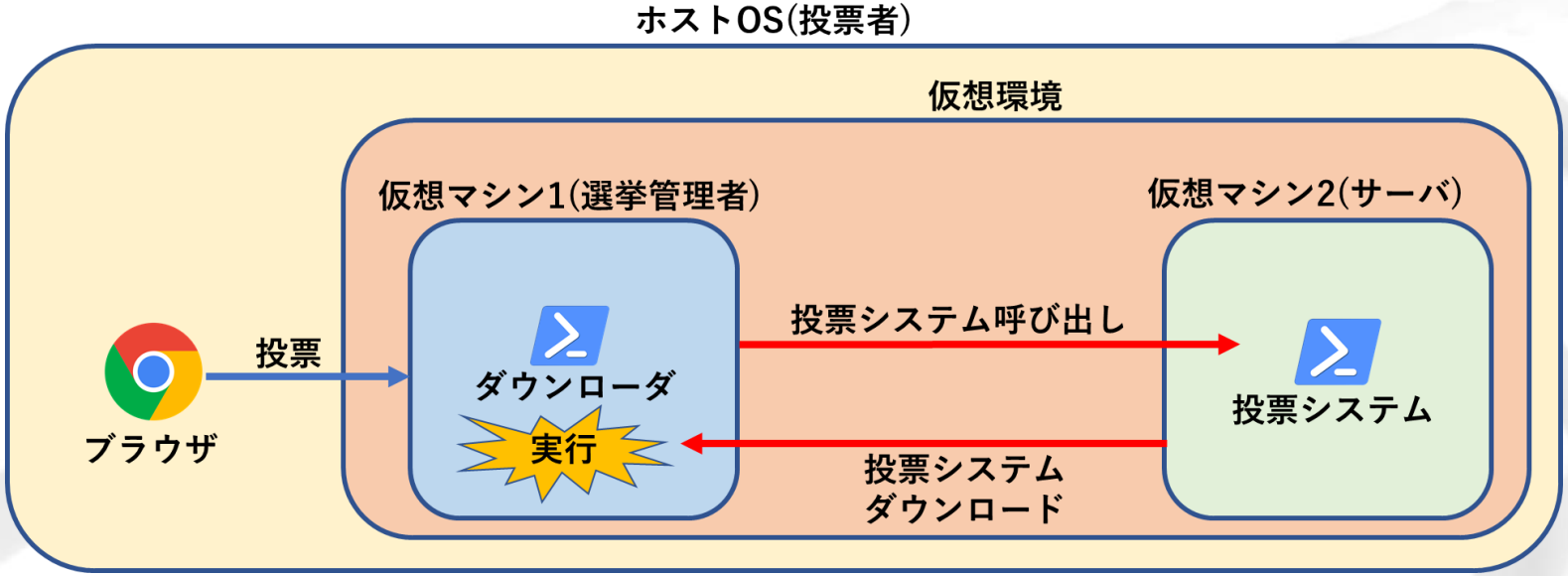
- 「ブロックチェーンの分散台帳を利用した投票における集合知の構成」[5]の「Secure Electronic Voting」[6]は 12 項目の理想的な電子投票システムの要件を提示している
- 12項目の中から5項目を抜き出して検証
- 今回は4、5の2項目について説明を行う

	項目
1	投票資格の検査と本人確認
2	二重投票の防止
3	投票内容の正確性
4	投票内容の改変不能性
5	個人の投票内容と方法の秘匿性

[5] 山崎 重一郎,"社会を変えるブロックチェーン技術：5. ブロックチェーンの分散台帳を利用した電子投票による集合知の構成 -対称的な非集中型監査と絶対中立的な非可逆的記録-",情報処理学会 情報処理会誌「情報処理」Vol.57 No.12 (2016.11.15)
[6] Dimitris Gritzalis,"Secure Electronic Voting",7th Computer Security Incidents Response Teams Workshop Syros, Greece, September 2002
http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.211.6135

検証環境

- 検証では、選挙管理者とサーバを仮想環境で選挙を再現

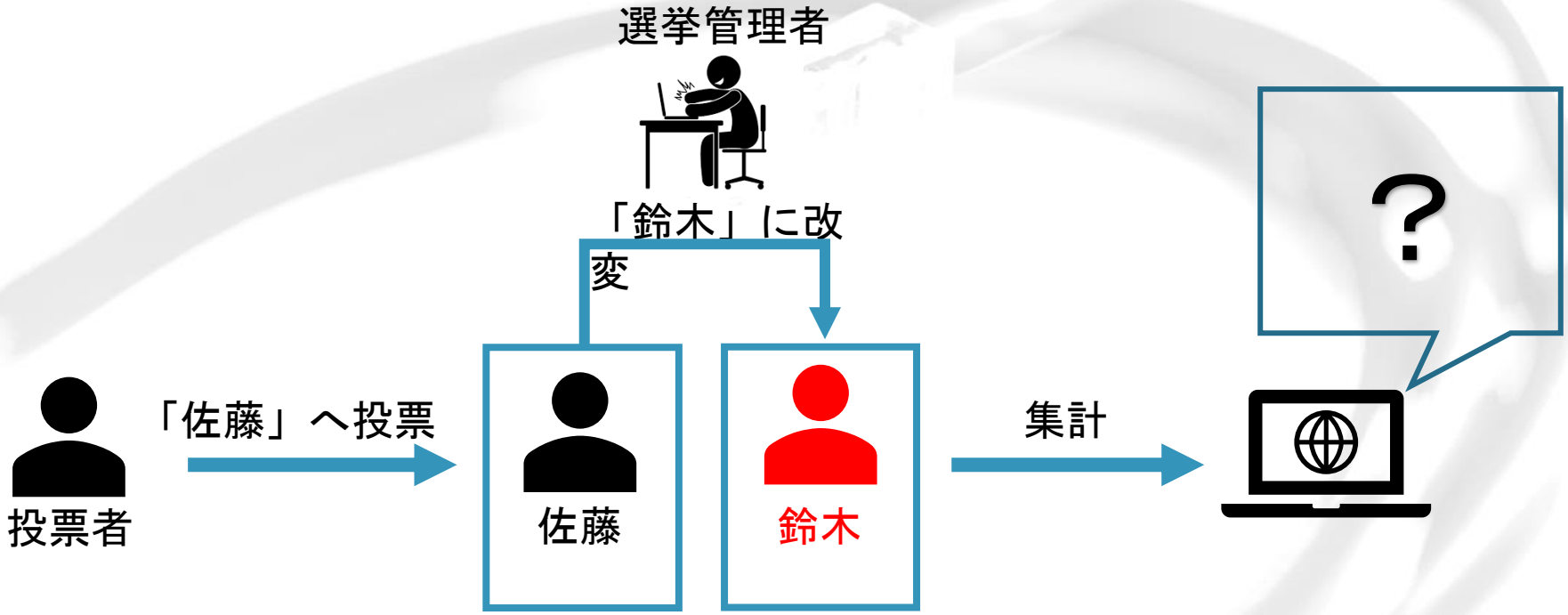


各設定

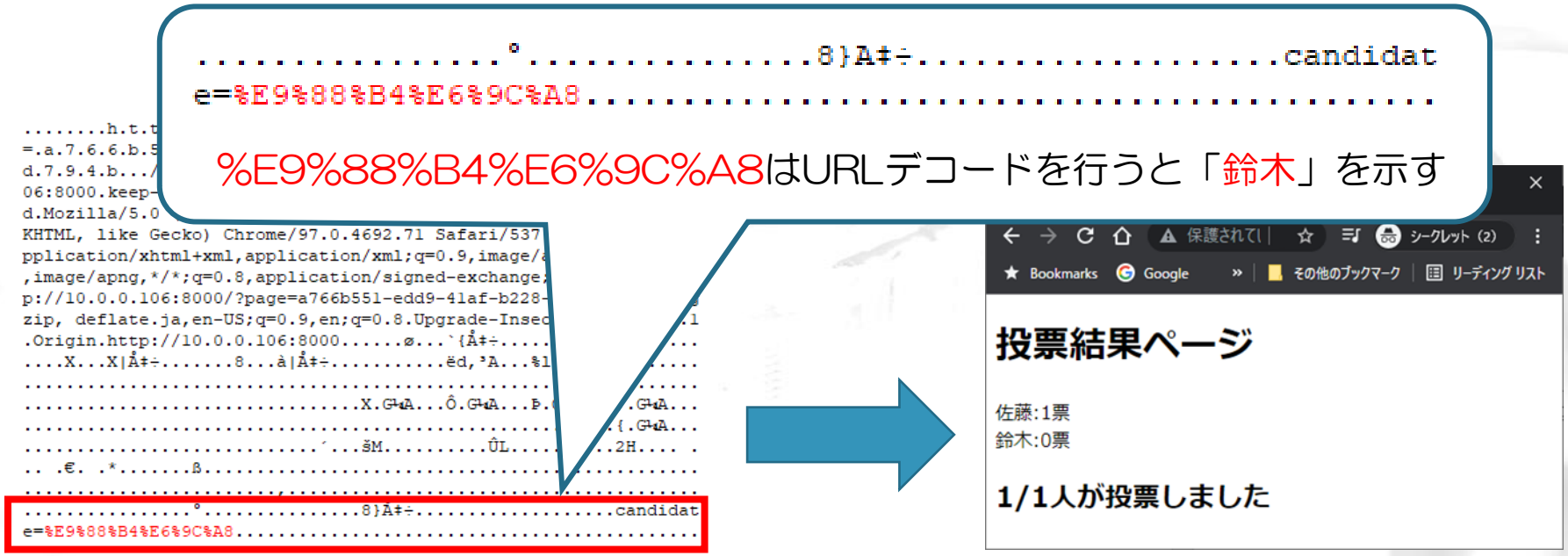
ホストOS(投票者)	仮想マシン1(選挙管理者)	仮想マシン2(外部サーバ)
OS：Windows 10 Home IPアドレス：10.0.0.1 ブラウザ：Google Chrome	OS：Windows 10 Pro IPアドレス：10.0.0.106 PowerShell Ver： 5.1.19041.1320	OS：Linux Kali IPアドレス：10.0.0.2 Webサーバ： Apache2/2.4.46

投票内容の改変不能性 検証内容

- 候補者「佐藤」に投票後、送信された候補者の名前を「鈴木」に改ざんし、投票結果に変化があるか確認



投票内容の改変不能性 結果と考察



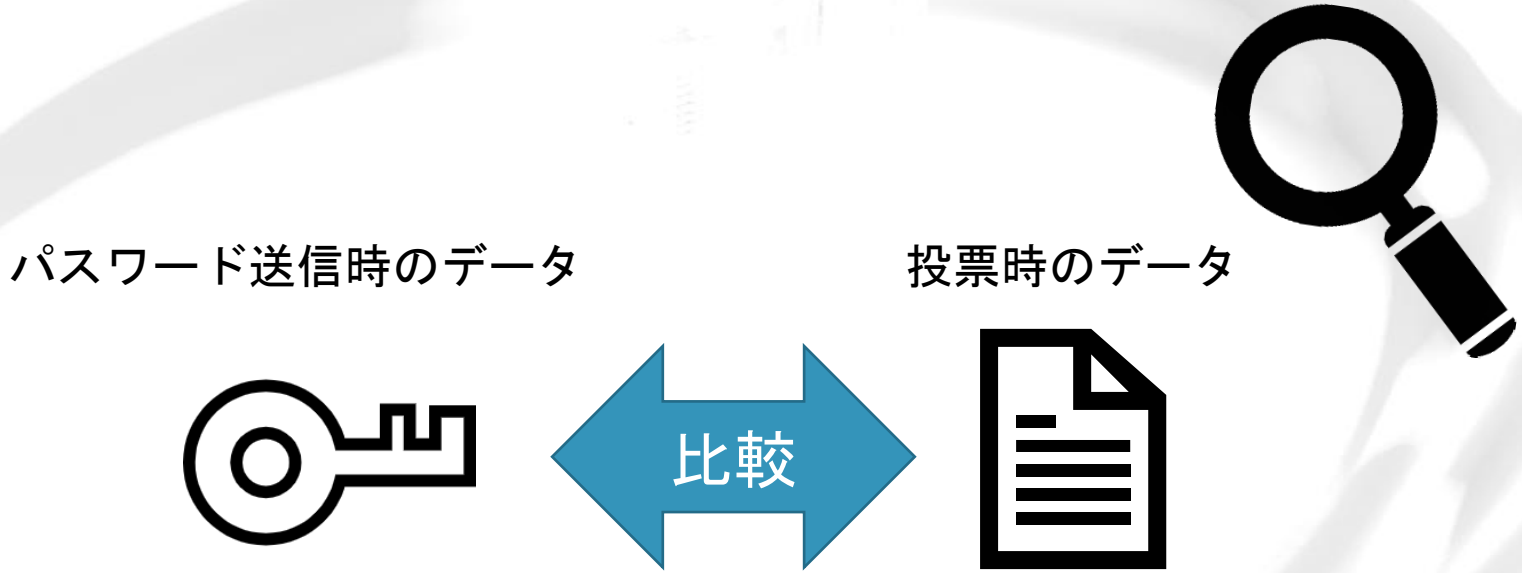
「佐藤」から「鈴木」に改ざんしている様子

結果に変化は見られなかった

投票後に改変を行っても、すでに得票処理が行われてしまい、投票結果に反映されなかった

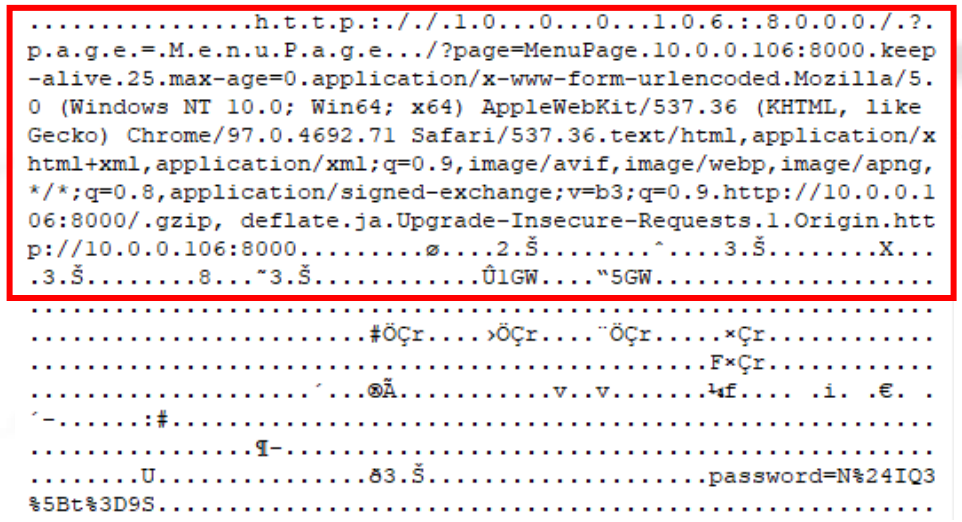
個人の投票内容と方法の秘匿性 検証内容

- パスワード送信時と投票時の2つのデータを比較・分析することで投票者とその投票先の特定を試みた



個人の投票内容と方法の秘匿性 結果と考察

パスワード送信時と投票時の2つのデータには
特定つながる情報は見つからなかった



パスワード送信時のデータ

投票時のデータ

投票者とその投票先を結びつけることができないために特定が不可能
特定するためには、送信元のIPアドレスが必要である

まとめ

- 本研究では ファイルレスマルウェアの特徴と仕組みを善用する電子投票システムを提案した
- 理想的な電子投票システムの要件の5項目について検証し、満たすことを確認した
- 問題点
  - 提案したシステムでは、一部のセキュリティ機能を無効にしなければならないため、改善が必要
  - ダウンローダをC&Cサーバに接続するように書き換えて配布されるとマルウェアを実行させられてしまう

年間スケジュール

年間スケジュール

就職活動して進学する場合

	事例研究	卒業研究
4月	研究室配属	卒業研究着手
5月		
6月	企業研究,自己分析	
7月		
8月	担務配属，インターンシップ参加	卒業研究中間発表，卒業研究テーマ決定
9月	1回目輪講開始	
10月	2回目輪講開始，適性試験準備	
11月	事例研究着手，適性試験，面接準備	卒業研究本論仮提出
12月	面接	5大学研究発表会　発表
1月		卒業研究概論及び本論提出
2月	事例研究発表会	卒業研究発表
3月	事例研究概論提出	卒業式

年間スケジュール

大学院に進学する場合

	卒業研究	大学院
4月	卒業研究着手	入学
5月		
6月		横浜祭，大学院英語研究発表会
7月		企業研究，自己分析，修士研究の方向性及び学会などの調整
8月	卒業研究中間発表，卒業研究テーマ決定	インターンシップ
9月	大学院入試	
10月		学会学生会員
11月	卒業研究本論仮提出	
12月	5大学研究発表会発表	大学院英語研究発表会
1月	卒業研究概論及び本論提出	
2月	卒業研究発表会	
3月	卒業式	学会全国大会発表

担務紹介

各担務

ゼミ長担当

全体をまとめる
横浜祭参加

懇親担当

イベントの企画

企画担当

勉強会などの企画

環境担当

研究室内の
ネットワーク環境を運営

広報担当

HP・資料の作成
SNSの運用

最後に

所属メンバーの詳しい情報等はホームページにて！

研究室ホームページ

http://www.yc.tcu.ac.jp/~seki_lab/

都市大　関研究室

検索