2023年度ISSスクエアシンポジウム研究成果発表

OSINTで探る企業のセキュリティ意識
～パスワードに関するガイドラインの適用実態調査～

2024年3月1日

マネジメント分科会

分科会紹介

研究リーダー：稲葉 緑 准教授

メンバー：6名

M2：1名、M1：5名

情セ大5名、中央大1名

片岡、澤、福井、齋藤、KANG、加藤

- 様々なルール・基準と実際との乖離に注目
- 実際のシステムや環境、予算、組織文化・人に合わせた対策を調査・議論を通して、総合的に検討

過去のテーマと今年のテーマ

過去に分科会で研究したテーマ（ガイドラインの提案・提言が主）

2022年：日本企業におけるＢＹＯＤ標準指針に関するガイドライン作成

2021年：企業におけるビジネスチャットアプリケーションの安全利用

2020年：変化する社会情勢に適したセキュリティポリシーマネジメント

2019年：組織におけるメール誤送信対策

2018年：ITプラットフォーマーへの個人情報提供管理

今年からは方向性を変えて…

OSINTで探る企業のセキュリティ意識

パスワードに関するガイドラインの適用実態調査

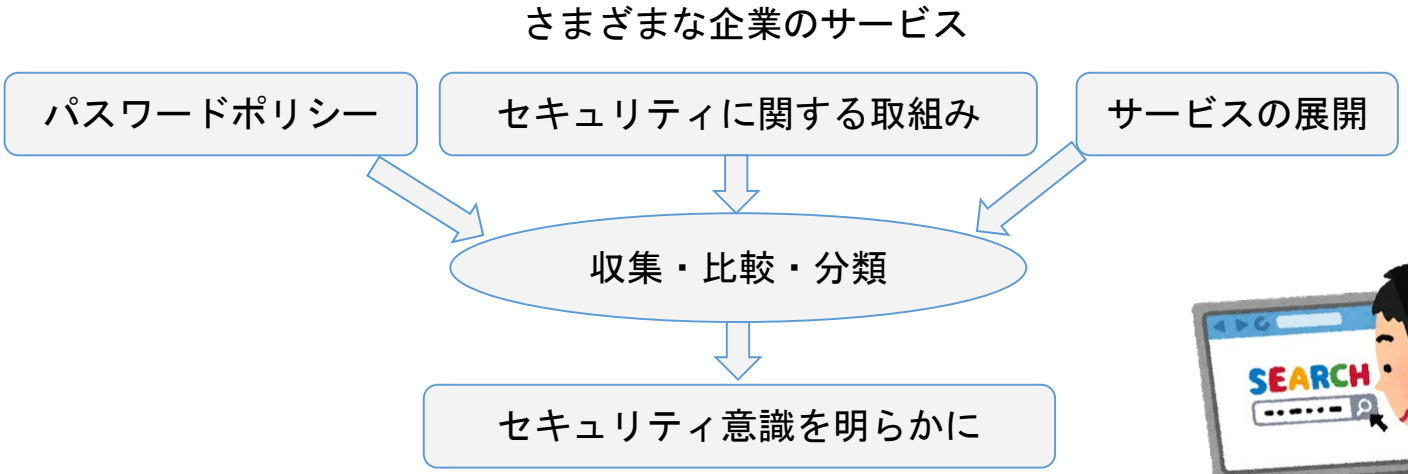
分科会ならではのマンパワーを活かしたOSINTに挑戦！

はじめに

- セキュリティに関するガイドラインと実態との乖離を見かけることがある
  - 認証の手段として身近でよく利用されるパスワードに注目する
  - パスワードに関する古い慣習が残っている
  - ベストプラクティスとされるNIST SP800-63に準拠しないWEBサイトやサービスが多い
    - パスワードに記号を使いたいのに使えない
    - 長いパスワードを設定したいのにできない

- パスワードポリシーに合わないサービスはどれくらいあるのか明らかにする
  - パスワード等の認証方法とインターネットで収集できる組織のマネジメントに関する情報から企業のセキュリティに対する取り組み姿勢の評価を試みる
  - 古いパスワードポリシーを強要される利用者がサービス提供者のセキュリティ態勢に疑念を抱く可能性がある
  - 推奨されるパスワードポリシーと実態に乖離のある企業はセキュリティ面で懸念がありそうか？

OSINTの取り組み



- 調査期間：2023年10月28日～2024年1月12日
- 限界と注意事項
  - セキュリティに対する取り組みが不十分そうに見えても…
    - その理由まではわからない
    - 本当にセキュリティが弱いと言えるものではない
  - 人力調査なので、たまに調査・集計のミスがあるかも
  - 結果の受け取り方はその人次第です

分科会活動としてOSINTは初の試み！

調査結果の用途・期待される効果

調査結果は次のような場面での活用が考えられる

- 自社のセキュリティ強化提案のための説得材料
  - セキュリティ対策を進めるにはお偉方を説得するステップがある
    - 基準と比較して、自社のパスワードポリシーが弱いというだけではシステムの改修を承認してもらえない
  - 日本人は世間体や外圧を気にするもの…
    - さまざまなサービスのパスワードポリシーを比較することで、ポリシーから外れていると、どのように見えるか？

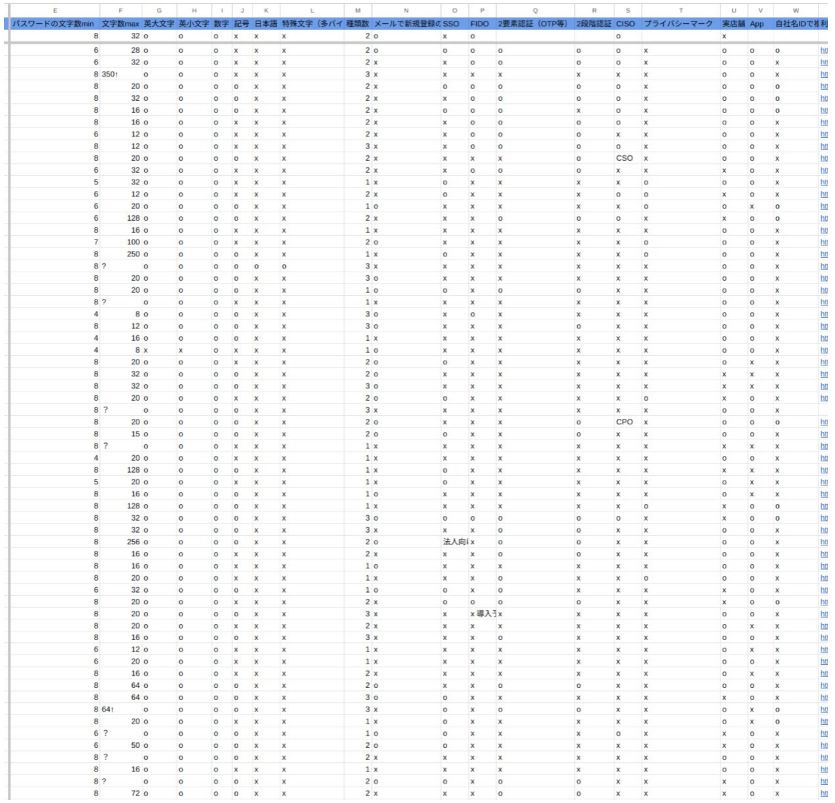
- さまざまな判断材料
  - サービス利用者が安心できるサービスを選択するため
  - 投資家がセキュリティリスクの少なそうな企業に投資するため
  - 業務提携先としてセキュリティリスクの少ない企業選定のため

調査方法

日本に拠点を置く企業・サービスについて93件、Webサイトにアクセス、アプリをダウンロード等行い、パスワードポリシーを調査した。

調査項目

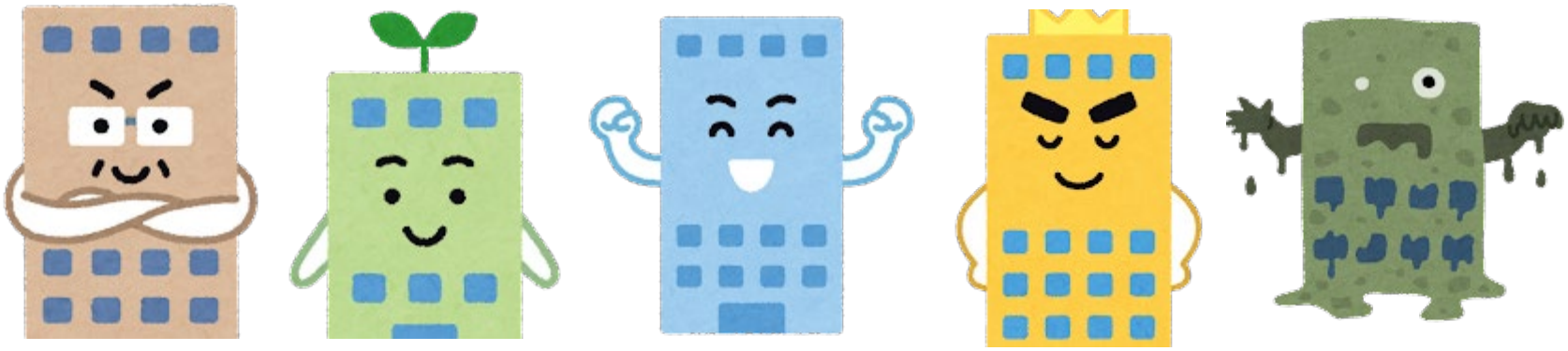
- パスワードの最小文字数
- パスワードの最大文字数
- 使用可能な文字の種類
  - 英大文字
  - 英小文字
  - 数字
  - 記号
  - 日本語
  - 特殊文字
- 使用文字最低種類数
- メールで新規登録リンクが届くか
- SSOの有無
- FIDOの有無
- 二要素認証の有無
- 二段階認証の有無
- CISOの有無
- Appサービス提供の有無
- プライバシーマーク取得の有無
- 自社IDの複数サービス展開の有無



対象企業・サービスの選定理由

- メンバーが思いついた企業・サービス
  - 利用しているものが中心

- gTLDを取得している企業が提供するサービス
  - それを取得するほどの財力とITに関する知見があるなら、セキュリティにも十分に取り組めていると期待できる



項目の選定理由①

対応しているとセキュリティが強そう

- **パスワードの文字数・文字種**：SP800-63Bに対応していると最新のガイドラインに沿ったアップデートに気を遣っていそう
- **メールで新規登録リンクが届く**：システム設計時になりすまし登録を念頭に置いたセキュリティの検討ができている（よく情報処理安全確保支援士の文章問題に出てくる）
- **SSO**：ユーザーのパスワードの使いまわしや脆弱なパスワードの使用、ずさんな保管体制による情報漏洩を念頭に置いたセキュリティの検討ができており、サイバー攻撃対策を強化している
- **FIDO**：サーバーがユーザーのパスワードや生体情報などを管理しないことで情報漏洩のリスクを回避している
- **二要素認証**：リスト型攻撃のような不正ログインによるデータの流出を念頭に置いたパスワード認証の脆弱性対策ができている
- **二段階認証**：パスワード流出による不正ログインを念頭に置いたセキュリティの検討ができている
- **CISO**：CISOを置く会社はセキュリティマネジメント態勢を整えていると見られる
- **プライバシーマーク取得**：個人情報について適切な保護措置を講ずる体制を整備していると見られる

項目の選定理由②

各社の事業展開の方向性がわかりそう

- **自社名IDの複数サービス展開**：オンラインでさまざまなサービスを展開する、オンラインに力を入れている会社はセキュリティにも力を入れているのではないか？
- **実店舗**：実店舗がなく、オンライン中心のサービスを提供する会社はセキュリティに力を入れているのではないか？
- **Appサービスの提供**：
  - スマホアプリで良いサービスを提供したい。ITに注力するのでセキュリティも頑張ってるかも？
  - フィッシングメールのようなURLを使用するアクセスからの情報流出を念頭に置いたセキュリティ対策ができているのではないか？

結果発表！

～〇〇な会社は××なように見えませんか？というお話～

パスワードポリシーの実態

- 8文字以下のパスワードを設定可能：28社（30%）
- 64文字より短いパスワードに制限：66社（70%）
- 記号が使えない：39社（41%）
- 英字が使えない：1社（1%）
- 数字が使えない：0社（0%）
- 文字種の制限
  - 1種類でOK：28社（30%）
  - 2種類必要：39社（41%）
  - 3種類必要：24社（25%）
  - 4種類必要：2社（2%）
- ポリシーがバラバラだと…
  - ブラウザのパスワード管理ツールを使いにくい
  - 個々人のパスワード生成パターンに合わないパスワードを忘れやすい

SP800-63の文字数に準拠している会社

NIST SP800-63 「電子認証に関するガイドライン」

パスワードの長さ：最小8文字以上、最大64文字以上を推奨

準拠していたのは19社

- CISOがいる会社は0（意外な結果だった）
- 業種は小売(6社)、情報・通信業(7社)が多い

企業名等はホームページ版では非公開

CISOを置く会社

- CISOを置く会社なら、よいパスワードポリシーが設定されているのでは？
  あるいは、パスワード以外の認証手段も用意しているのでは？
- 19社が該当
  - うち13社が自社名を冠するIDでサービス展開（13/19）
  - SP800-63Bに合うパスワードポリシーの会社はなかった（意外な結果）
  - SSO、FIDO、2要素認証、2段階認証のいずれかには対応していた
    - パスワード以外の方法で追加のセキュリティを確保していた

企業名等はホームページ版では非公開

自社名IDで複数サービス展開をする会社

自社名を冠するIDを使用している会社はセキュリティ意識も高そうか？

- セキュリティ意識が低そうなグループには一つも属しておらず、 セキュリティ意識が高そう
- 該当する会社：21社
  - CISOがいる割合が高い：11社（50%）
- 該当しない会社：72社
  - CISOがいる割合が低い：8社（11%）

企業名等はホームページ版では非公開

別な認証手段を提供しているグループ

SSO、FIDO、2要素認証、2段階認証により、パスワード以外の認証方法を提供しているグループ

当てはまった49社の内

- SP800-63準拠(8社)
- 自社名IDで複数サービス(18社)
- CISO(16社)、CPO(1社)
- 調査した銀行は全てこのグループに属する(5行)

企業名等はホームページ版では非公開

ログインパスワードに注力したくなさそうグループ

SP800-63に非準拠だが、別な認証手段を提供している

パスワードポリシーを変更することよりも効果的な手段を選んだのではないか？

当てはまった40社のうち

- CISOがいる(16社)、CPO(1社)
- 調査した銀行は全てこのグループに属する(5行)

企業名等はホームページ版では非公開

パスワードに記号を使えない会社

- ブラウザのパスワード自動生成機能では、記号入りのパスワードが生成される。
- パスワードに記号が使えないと、ブラウザ自動生成パスワードが使えない。
- 不便なサイトというイメージにつながる。
- 35社が該当

企業名等はホームページ版では非公開

セキュリティ意識が低そう

「SP800-63への準拠」、「CISOの設置」、「プライバシーマークの取得」、「別な認証手段」、「メールで新規登録のリンクが届く」が全て×

- 全て実店舗あり
- Webサービスのみの会社は該当しなかった
- 10社が該当
  - 安心して使うには頑張ってほしいけど…
  - 1件のサービスの単価が低そうなところが多い？

企業名等はホームページ版では非公開

パスワード最小4文字でOK！利便性重視？

- 鉄道系の会社には、パスワードの文字数が最小4文字の会社が複数見られた
- セキュリティより利便性を重視しているのではないか？
  - 発車時刻をすぐに確認したい
  - 指定席をすぐに確認したい
- クレカ決済時にはクレカの認証がある
- 鉄道系3社が該当

企業名等はホームページ版では非公開

関連研究

パスワードポリシーの大規模調査が行われ、ACM CCS 2023で発表された。

Alroomi Suood, and Frank Li. 2023. “Measuring Website Password Creation Policies At Scale.” In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 3108–22. CCS ’23. New York, NY, USA: Association for Computing Machinery.

- Alroomiらの研究では、パスワードポリシーの調査をツールを作成して自動化し、世界中の約2万件のサイトを調査していた
  - 75%のサイトが8文字よりも短いパスワードを許可
  - 40%のサイトがパスワードの長さを64文字よりも下に制限
  - 一部のガイドライン（OWASP、NCSC 2018）がほとんど採用されていないことが明らかに

- 我々の取り組みでは、手動で国内約100件程度サイトの調査と数・範囲は限定的だが、セキュリティマネジメントに関する項目の調査も同時に行っている点での付加価値がある

今後の展開

- 調査の自動化
  - 関連研究のような自動化ツールの作成
  - 調査を大規模に行えるようになる
- Webサービス作成の委託先の特定
  - 同じ委託先が作ったサイトは同じパスワードポリシーなのではないか？
- さまざまな情報を調べて表に追加していくと各社のセキュリティ取り組み姿勢が見えてくるかもしれない
  - 登録支援士が何人所属しているか？
  - セキュリティポリシー（規約）の記述量や更新年月日
  - 監査報告書の公開状況や記述量
- 追跡調査
  - 時間の経過とともにパスワードポリシーが変化すれば、どのような会社が柔軟にポリシーを変更していけるのかわかるかもしれない

おわりに

- 日本に拠点を置く企業のサービスについて、パスワードポリシーを中心に公開情報からセキュリティに対する取り組み姿勢を調べた
  - 分科会でOSINTは初の試み！

- 今後さらに大規模な調査を行えば、傾向や内情も見えてくるかもしれない