日本企業の情報露出脅威：OSINTに基づく分析

Analysis of IoT Security Threats in Japanese Enterprises

卓珮如・システム分科会・情報セキュリティ大学院大学

背景と研究目的

近年、情報技術の発展とデジタル変革が進む中、企業の情報セキュリティの重要性が増しています。特に、企業がネットワーク上に公開している情報が、外部の脅威にさらされるリスクが高まっている。
この研究の主な目的は、日本の企業が網上で直面している情報露出の問題を明らかにし、その問題に対する情報セキュリティ評価の方法論を提案することである。
情報の不適切な露出や漏洩は、企業のブランドイメージ、顧客信頼性、そして経済的な損失につながる可能性があるため、適切な対策が必要であるとされる。

先行研究：OSINTの応用

- 問題識別
  - 日本企業のセキュリティ脆弱性の特定
  - 情報漏洩の原因と影響の分析
- AIや機械学習の組み合わせ
  - 情報源の効率的なフィルタリング
  - 脆弱性の自動検出と分類
- 脅威予防と対応戦略
  - 発見された脆弱性に基づくリスク軽減策
  - 即応性のあるセキュリティ対策の策定
- ケーススタディと実証分析
  - 実際の企業事例を用いた方法論の検証
  - 実用性と有効性のデモンストレーション
- ツールと技術の開発
  - OSINTツールのカスタマイズと改善
  - 企業環境向けの新技術の開発
- 既存システムとの統合
  - 既存のセキュリティ架構との連携強化
  - 総合的なセキュリティソリューションの提供

今後の予定（三段階）

情報収集と分析
（OSINT＋Python+AI）

- ■ 特定設備で露出したプロトコル、IPを収集
- ■ 80/443ポートopenのIPを探索
- ■ サプライチェーン関連分析

- ■ サプライヤー内部での脆弱性探知
- ■ 産業制御プロトコルに対して利用可能なN-Day CVEの脆弱性を探索

- ■ APT攻撃シナリオで評価
- ■ 脅威予防と対応戦略