# サプライチェーンにおけるダークウェブ情報流出分析

## Analysis of Dark Web Data Leaks in Japanese Supply Chains

卓珮如・ネットワーク分科会・情報セキュリティ大学院大学

This research investigates the increasing cyber threats targeting supply chains in Japanese industries, particularly in electronics and automotive sectors. Using specialized dark web search engines (Ahmia, Torch, and Haystack), we analyzed data leaks related to Japanese companies and their suppliers. Our initial findings revealed that while most discovered data were from previously known incidents, there is a critical need to enhance current research methodologies. This study aims to develop more effective approaches for comprehensive dark web data collection and supply chain risk assessment.

## 1．背景と目的

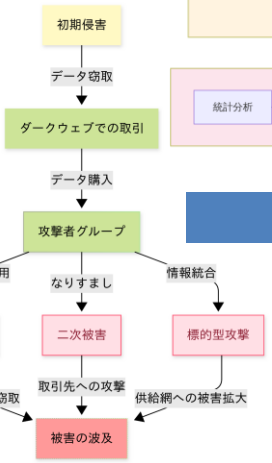
### ダークウェブの脅威

■ 匿名性の高いネットワークでの違法取引・情報漏洩の増加
■ サイバー犯罪のビジネス化
マルウェアの低価格化（月額20ドル）
攻撃ツールのサービス化


### 現状

■ 中小企業のセキュリティ対策の脆弱性
- セキュリティ専門チームの不在
- セキュリティ投資の不足
- 基本的な防御体制の欠如

■ サプライチェーンにおけるリスク
- 大企業への侵入経路としての悪用
- セキュリティ意識の格差
- コスト制約による対策の限界



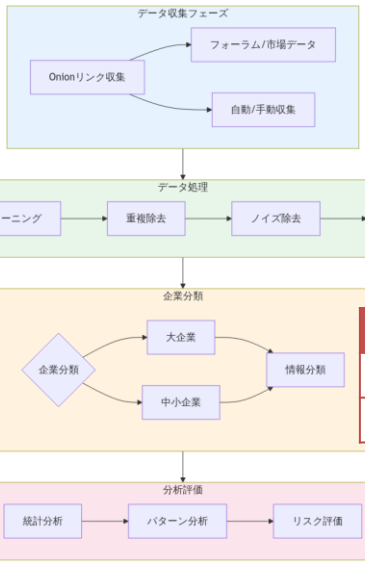

### 期待される成果

**1. OSINTを活用した脅威の早期発見**
- ✓ 自動モニタリングシステムの構築
- ✓ 情報流出の初期段階での検知
- ✓ クレデンシャル情報の追跡・監視

**2. 効率的な情報収集・分析手法の確立**
- ✓ 機械学習による情報の自動分類
- ✓ リスクレベルの自動評価
- ✓ サプライチェーン関連性の分析

**3. 予防的セキュリティ対策の支援**
- ✓ リスクベースの対策優先順位付け
- ✓ インシデント予測モデルの開発
- ✓ サプライチェーン全体での防御戦略策定

## 2．研究内容




### データ収集

1. サイト：Ahmia、Torch、Haystack…
2. 検索キーワード：
data leak database, 企業名
credentials, VPN access…

### データ処理

Github、Python
自然言語処理 (NLP) SpaCy…

### 日本の電子・半導体・自動車産業

| 分類 | 資本金 | 従業員数 |
|---|---|---|
| 大企業 | 3億円超 | 300人超 |
| 中小企業 | 3億円以下 | 300人以下 |

### データ分析

1 .情報の出現頻度の統計分析
2 .取引価格帯の分析
3 .攻撃ツールの種類と使用傾向
4. 標的となる業種・企業規模の特定

## 3．初期結果

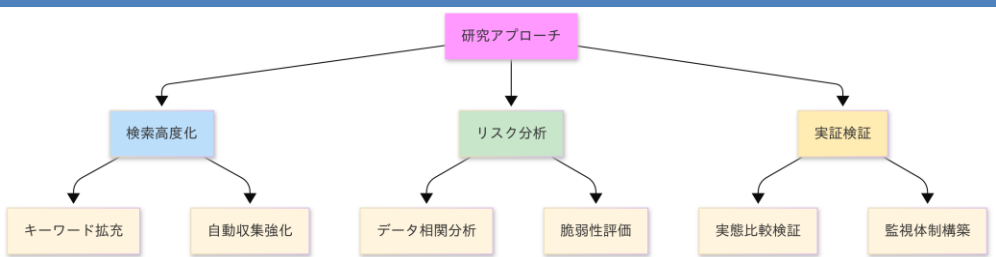
| データ | データ数（万件） | 価格（JPY） |
|---|---|---|
| 就活データ | 469 | 11,000 |
| 不動産情報 | 5 | 7,000 |
| 厚生労働省データ | 2,000 | 13,000 |
| ショッピングデータ | 52 | 11,000 |
| 婚活データ | 4 | 7,000 |
| 総務省データ | 928 | 4,000 |
| マッチングアプリデータ | 400 | 400 |
| 車両所有者データ | 489 | 13,000 |
| 企業情報データ | 50 | 18,000 |

※代表的な事例の抜粋、価格は概算値

### 初期調査における主な課題

■ データの偏り個人情報が中心
■ サプライチェーン関連データが不足
■ サプライチェーン攻撃との関係性が不明
■ サプライヤー情報の不足
■ 企業間ネットワーク情報の欠如
■ データの信頼性
■ リスク評価の難しさ

## 4．今後




1. 検索手法の高度化
- サプライヤー固有キーワードの体系化
- データ収集の精度向上

2. リスク分析の強化
- 取引データとリスクの相関分析
- サプライチェーンの脆弱性評価

3. 実証的検証
- 企業の実態調査との比較検証
- リアルタイム監視体制の確立