# グループ企業におけるインシデント情報連携を促進する手法の提案

Effective methods to promote incident information sharing among group companies

木下 英治・法制倫理分科会・情報セキュリティ大学院大学

Abstract: In recent years, many cyber-attacks targeting Japanese group companies have occurred, which has become a major threat. Each organization that makes up the group company has various differences such as industry, business scale, culture, system, and information security measure level. In addition, the number of companies expanding group businesses through M&A is increasing year by year, and the situation of group companies is becoming more complicated. When an information security incident occurs within a group company, there is a problem that the information is not shared and the damage caused by the incident spreads. The purpose of this study was to clarify the risk factors for information sharing that group companies should take priority measures. By conducting preliminary analysis and questionnaire surveys of group companies to identify factors, and by analyzing and evaluating risk factors, we identify factors that impede incident information sharing within diverse group companies.
, I considered the countermeasures.

## 1.研究概要・目的

近年、日本のグループ企業を標的としたサイバー攻撃が多く発生し、大きな脅威となっている。そのグループ企業を構成する各組織には、業種や事業規模、文化、体制、情報セキュリティ対策レベルなど、多様な違いが存在する。またM&Aによるグループ事業を拡大する企業が年々増加傾向にあり、グループ企業のおかれた状況は複雑になっている。グループ企業内で情報セキュリティインシデントが発生した場合、その情報が共有されずインシデントによる被害が拡大する問題がある。本研究は**グループ企業が優先的に対策を講じるべき情報共有のリスク要因を明らかにすることを目的とした**。要因特定のために、予備的分析とグループ企業へのアンケート調査を実施し、リスク要因の分析と評価を行うことで、多様性のあるグループ企業内で、インシデント情報共有を阻害する要因を特定し、その対策について考察した。

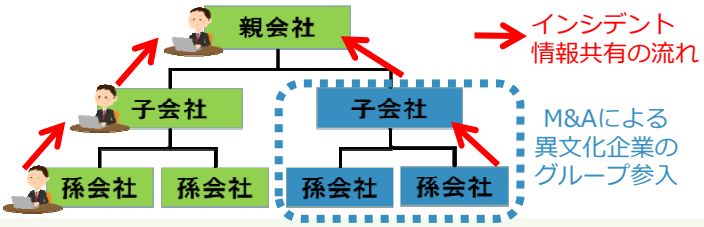
## 2.背景・現状

### ■グループ企業の特徴

(1)グループ企業は、そのグループを構成する各社の形態に**「バラつき」がある**

(2)グループ事業の拡大で**「M&A」**により組織文化の異なる企業がグループへ新規参入するケースが近年増加している

**※本研究で対象とする「グループ企業」の形態（３階層）**




### ■先行研究

**●異なる企業間のインシデント情報共有を阻害する要因**
（2017,Koepke）
- 法的（プライバシーの懸念）
- 管理（情報管理が不十分）
- 技術（情報の互換性の相違）
- 組織（機密情報の管理制御）
- 情報（情報の信頼性担保）
- 影響（評判低下/顧客損失）
- 連携（組織間の信頼性担保）
- 費用（人的/技術的コスト）

**●日系グループ企業のグループマネジメントの在り方**
（2019, 宮元）
- グループ各社のビジネス構造が異なれば、子会社のマネジメント形態は異なる（全社に最適な形態は無い）
- 子会社から親会社への情報連携に課題あり

グループ企業内でのインシデント情報共有を阻害する要因に関する**先行研究は無い**。複雑化したグループ企業内で、**下位から上位への情報共有の阻害要因**について**リスク分析・評価**を実施

## 3.研究工程

先行研究調査 → 要因予備分析 → 仮説立案 → 要因分析 → 要因評価 → 対策提示

## 4.研究手法

**<要因の予備分析>**
(1)先行研究の要因に加え、m-SHELLモデルの起因別(*)に整理
(*)本人、経営層や従業員、手順、機器、業務環境、組織管理
(2)ブレーンストーミングを実施し要因の網羅性を向上

**<要因の分析・評価>**
グループ企業のセキュリティ業務担当者へ**アンケートを実施**
・各要因への「**関与度（要因が発生すると感じる頻度）**」と「**対策すべきと感じる重要度**」を5段階で回答を依頼

**アンケート対象企業（合計12社 下記の形態ごとに各3社）**

| | |
|---|---|
| グループ企業に3年以上所属する**子会社＆孫会社** | M&Aによりグループへ参入後3年未満の**子会社＆孫会社** |

## 5.研究仮説／検証結果 (支持○ 支持しない×)

(1)ISMS認証の未取得企業より取得企業は,全ての起因で重要度が高い（重要度○）
(2)子会社より孫会社は,全ての起因で関与度が高い（関与度○）
(3)IT事業がある企業より,IT事業がない企業は,全ての起因でいずれも高い（関与度○　重要度×）
(4)大企業より中小企業は,機器と組織管理で,いずれも高い（関与度○　重要度(機器× 組織管理○)）
(5)既存企業よりM&A参入はコミュニケーション関連でいずれも高い（関与度○　重要度○）
(6)既存企業よりM&A参入は,業務環境で関与度が高い(関与度○)

## 6.対策

①共有されないことで被害拡大したインシデント事例を説明
②下位組織の管理を含めたグループ全体の共有ポリシーを策定
③M&A参入企業のシステムをグループ共通のシステムへ統合
④インシデント情報を共有する場（定例会等）を継続して設定

## 7.結論　※各要因への対策は上記「6.対策」の通り

**■各社のバラつき（IT事業を展開しない企業）による要因**
①共有しなくとも**上位組織で検知・対応してくれると認識**
②**下位組織で発生**したインシデントの**共有ルールがない**
**■M&Aで参入した企業に存在する要因**
③自社と上位組織で**業務環境（システム等）が異なる**
④自社と上位組織との**コミュニケーションが希薄**