Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

グループ企業におけるインシデント情報連携を阻害する要因の分析

情報セキュリティ大学院大学 稲葉研究室 博士前期課程 2 年
木下 英治
E-mail : mgs195506@iisec.ac.jp

概要：近年、グループ企業を標的とした外部からのサイバー攻撃が多く発生し、企業の経営において大きな脅威となっている。サイバー攻撃による被害を抑制するために、企業や組織では情報セキュリティインシデント（以降インシデント）を発生前に防止することや、インシデントが発生した場合に迅速な対応をとることが求められる。そのためにもグループ企業内で発生したインシデント情報の共有が重要であるが、これが困難である実態があると推察された。そこでグループ企業内での情報共有に着眼し、先行研究と現状を調査した結果、特に、下位組織から上位組織への情報の流れに問題があることがわかった。本研究は、グループ企業内部におけるインシデント情報共有を促進する手法を提案するために、下位組織から上位組織へ共有されない要因を網羅的に分析した。

キーワード：グループ企業、セキュリティインシデント、情報連携、阻害要因

Analysis of factors that hinder the sharing of incident information among group companies

Institute of Information Security, Inaba Lab. Master’s Program (2nd year)
EIJI KINOSHITA

Abstract: In recent years, many external cyber-attacks targeting group companies have become a major threat to corporate management. In order to control the damage caused by cyber-attacks, companies and organizations are required to prevent information security incidents (hereinafter referred to as incidents) before they occur, and to take prompt action when an incident occurs. For that reason, sharing of incident information that occurred within the group companies is important, but it is presumed that this is difficult. Therefore, as a result of investigating the previous research and the current situation focusing on information sharing within the group companies, it was found that there is a problem in the flow of information from the lower organization to the upper organization. In this study, in order to propose a method to promote the sharing of incident information within the group companies, we comprehensively analyzed the factors that are not shared from the lower organization to the upper organization.

Keywords: Group companies, Security incident, Information sharing, hindrance

１．はじめに

１－１．背景

日本企業では、単独の企業だけでなく複数の企業がグループとして事業活動を共にする企業グループが多く存在する。総務省統計局が 2014 年に調査した「経済センサス‐基礎調査の集計結果-」[1]によると企業グループ数は 23,159 で、その会社企業数は 79,653 社であった。その企業グループの 2013 年(1 年間)の売上(収入)は、833 兆円で会社企業全体の売上(収入)に含む割合は 7 割以上で、日本経済の根幹を成している。

近年のサイバー攻撃は、セキュリティ対策が不十分な組織を狙うケースが増え、グループ企業ではグループ全体のセキュリティ確保が重要な課題となっている。経済産業省が 2019 年 6 月 28 日に策定した「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」[2]では、サイバーセキュリティ対策の在り方として、グループ企業全体の対策検討が必要で、不祥事等の早期発見や被害最小化のため迅速な対応を適切に行うべきとしている。また、子会社で不祥事等が発生した場合には、事案の態様や重大性、子会社の対応可能性等を勘案し、原因究明、事態の収束、再発防止対応を、親会社の主導で行うことが期待されるとしている。

グループ企業が情報セキュリティを統括管理する際には、グループ企業内のセキュリティ対策状況の情報収集やリスク評価・リスク分析だけでなく、グループ企業全体での情報連携を推進することが重要視されている。産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）が 2019 年に「ユーザ企業のためのセキュリティ統括室構

Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

築・運用キット（統括室キット）Part2 統括室編 ver1.0」[3]を公開した。その中で、セキュリティ統括室の機能として情報共有・連携を挙げており、サプライチェーン先との連絡体制・連携体制を構築することやグループ企業全体での情報連携を推進することが示されている。

また、グループ企業内での情報共有は、日本企業では特に重要である可能性がある。NRI セキュアテクノロジーズ社が、2018 年に 5 ヵ国（日本、アメリカ、イギリス、シンガポール、オーストラリア）の 1,100 企業を対象にしたアンケート調査[4]である。日本企業のセキュリティ担当者が最も対応に困っていることとして、1 位が「セキュリティインシデント発生時の緊急対応」、2 位が「自社セキュリティ対策の遅れ」、3 位が「グループ会社・国内外拠点のセキュリティ統制・管理」であった。アンケート実施時期の過去 1 年で発生した事件・事故として、1 位が「電子メール、FAX、郵便物等の誤送信・誤配送」、2 位が「情報機器・外部記憶媒体の紛失・置き忘れ・棄損」で、3 位が「マルウェア感染」であった。

メールの誤送信や紛失といったヒューマンエラーのインシデントは、システムで自動検知することが困難で、発生した事象は共有されなければ把握できない。対応が困っていることとして挙げられたグループ企業を管理・統制する上で、グループ企業内での情報共有が必要となる。

このようにグループ企業内の情報共有が重要視されながら、これが不十分な実態があると推察される。それは昨今のサイバー攻撃事例として、大企業グループにおいて子会社や孫会社といったグループ企業内部の端末がマルウェアに感染し、本社の重要な企業情報が漏洩する被害として 2020 年 5 月に発生した日本経済新聞社グループの事例[5]など、複数発生していることによる。

また、2018 年 2 月 28 日には、東芝グループの子会社が保有する情報システムに外部から不正アクセスがあり、従業員 100 名分のメールデータが漏洩した事件が発表[6]された。この事例では、東芝グループの子会社が、外部委託先の企業から「不正アクセスが行われた可能性がある」という報告を 2018 年 2 月 10 日に受け、実際に情報漏洩の可能性を親会社で把握したのは 4 日後の 2018 年 2 月 14 日であったと報告されている。

親会社で被害の実態を詳細に調査した後、不正アクセスの経路遮断など対処していることから、グループ企業内でインシデント情報の共有が遅れた場合、それだけ被害が拡大していた可能性が考えられる。このようなインシデントに迅速な対応を行うために、グループ企業内でのインシデント早期検知と情報共有は重要なポイントとなる。

2019 年 3 月 18 日には、三菱電機グループで、中国に拠点をもつグループ会社からマルウェアが侵入し、同年 4 月 3 日に日本拠点へ侵入を拡大した結果、国の防衛に関わる情報が流出した可能性があるという事件が発生した。三菱電機社の報告書(第 3 報)[7]によると、2019 年 6 月 28 日に、ウイルス対策ソフトで端末の不審な挙動を検知していながら、不正アクセスと認識したのは 10 日後の同年 7 月 8 日で、不正な通信先の遮断を完了したのが 7 月 17 日であった。三菱電機社の報告書による今後の対策として、グループ全体の情報セキュリティ体制強化に向け、迅速な判断とインシデント発生時の関係機関との早期情報共有等を目的に、セキュリティ対策全般を一元的に担う統括組織を新設すると発表した。

これはインシデント検知後の対応が遅れたことにより被害が拡大した事例と言える。インシデント情報を迅速に把握し対応できていれば、被害を縮小できた可能性が考えられる。

そこで本研究は、グループ企業内における内部発生インシデント情報が、グループ企業内で情報共有・連携されない問題に着眼した。

１－２．用語定義

グループ企業の捉え方には、様々な見方が存在する。親会社・子会社・関連会社といった、資本関係に基づいて形成される企業群や、業務委託などの契約関係に基づいて形成される企業群、建設・不動産業などに見られる共同企業体（ジョイントベンチャー）、海外法人と共同出資して新会社を設立する合併会社など、グループ企業と呼ぶ対象と範囲は様々である。

本研究における「グループ企業」とは、親会社・子会社・関連会社といった、資本関係に基づいて形成される企業群を対象とする。それは連結決算の対象となる企業群が、株主等のステークホルダーに与える影響が大きいため、サイバー攻撃による被害発生においても、企業経営に与える影響が非常に大きいためである。

２．グループ企業の現状

２－１．グループ企業の形態と情報共有

Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

日本のグループ企業は、各企業の Web 公開情報をもとに整理すると、親会社と子会社の２階層構造（図１）、さらに子会社の子会社（以降「孫会社」と表記）まで存在する３階層構造（図２）で、グループ経営がされている。

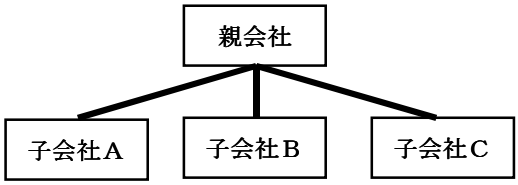

図 1：グループ企業の 2 階層構造

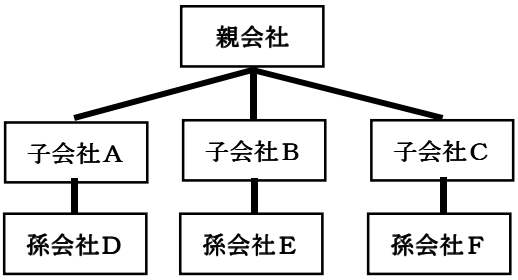

図 2：グループ企業の 3 階層構造

これらの親・子・孫の階層構造において、グループ経営に関する様々な情報を、各会社間で共有・連携しながら経営されている。共有・連携する情報の流れは、親会社から子会社、子会社から親会社、子会社から子会社、など様々なルートがある。グループ企業内における情報共有は、各会社同士の関係性や役割、文化や風土、コミュニケーションレベル、判断基準など会社ごとに違いがある中で、日常的に行われているものである。

また、グループ企業の特徴として M&A による事業の拡大がある。新たな子会社のグループ企業参入は年々増加傾向にあり、新規参入企業はグループ参入前後で業務が変わらないため、グループ外のような実態の中で情報共有が行われている。(株)レコフの調査結果[8]によると、日本のグループ企業における M&A の件数は 2017 年が 1,465 件、2018 年が 1,759 件、2019 年が 1864 件と増加傾向にある。M&A 後にはグループ企業全体で、業務効率化やコスト削減のために、システムやネットワークを統合するケースが多い。M&A でグループに新規参入した企業は、経営統合先のグループ企業と、業種や業務が異なる場合があり、システムやネットワーク統合の検討や調整には多大な時間を必要とする。

グループ企業は、同一のグループで経営を共にしてきた既存の企業と、M&A である日を境にグループ参入した企業では、文化や風土の違いなどお互いの状況把握や、コミュニケーションをとりづらい状況にあると推察する。しかしながら、グループの子会社でサイバー攻撃による情報漏洩などが発生すると、対外向けにその内容を発表[6][7]するのはグループの親会社であるため子会社のインシデント対応には関与せざるを得ない。

２－２．グループ企業のインシデント体制

グループ企業内におけるインシデント対応の体制は、各企業により様々な形態が存在する。グループ階層の最上位に位置する親会社でセキュリティ対策を統括管理するケースや、IT 系の子会社が管理するケース、また子会社にその傘下となる孫会社のセキュリティ管理責任を与えるケースなど、多岐に渡る。外部組織とインシデント情報を共有・連携する窓口のグループ企業 CSIRT は、各企業により様々な形態で多様化しており、各グループ企業の役割も一意ではない。各グループ企業の経営方針も異なることで、インシデント対応を行う組織や CSIRT のあり方を各社が模索している状況にある。

この多様性を以下に説明する。各グループ企業における CSIRT の構成と活動の実態を把握するために、NCA（日本シーサート協議会）の会員登録情報[9]を調査した。NCA は各組織の CSIRT が会員登録企業と情報共有・連携する場を提供する非営利組織で、近年インシデント体制を整備する組織が増えてきている。2020 年 7 月 20 日時点で NCA の Web サイトに公開されている会員情報をもとに、会員加入年別の会員組織数を集計したものを図 3 に示す。

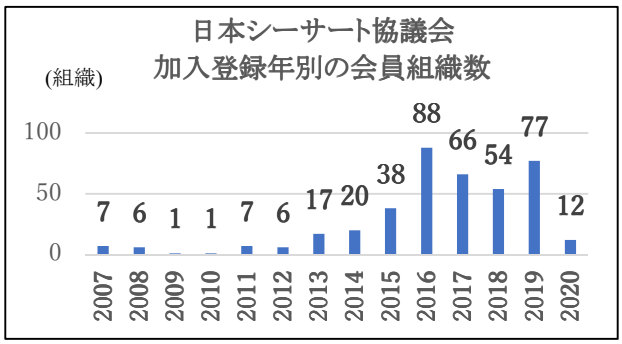

図 3：日本シーサート協議会 会員組織数

会員 400 組織の中でグループ企業に注目すると、他組織とインシデント情報を共有・連携するグル

Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

ープ企業の形態は様々である。会員組織は企業以外に大学など教育機関もあるが、グループ企業の CSIRT では大部分がグループ会社内で中核となる 1 企業だけで会員登録をしている。持株会社の最上位組織となる「ホールディングス」の CSIRT だけで会員登録しているグループ企業は、32 社であった。同一グループ企業内で複数の組織が会員登録しているケースは、2 社～10 社で、NTT グループでは親会社の他に、9 つのグループ企業がそれぞれ登録し、NTT グループ企業として 10 組織が登録している。同一グループ企業内で 10 組織が NCA に会員登録しているのは、全グループ企業の中で最多となる。「日本郵政」は、親会社に加えて子会社の 3 組織も全てが会員登録し、孫会社の会員登録はない親子体制の形式をとっている。これは孫会社のインシデント管理を各子会社の CSIRT に委ね、運営しているものと推察する。ANA グループでは、親会社の CSIRT が会員登録せず、IT 系子会社の「ANA システムズ」だけ会員登録する形態をとっている。

また、グループ企業でインシデント対応を迅速・効率化するために、インシデント管理システムを導入する企業が増えているが、ヒューマンエラーの検知ができないなど万能ではなく、システム導入による実際の効果についても公表されていない。IDC Japan 株式会社が 2019 年 4 月に国内ユーザ企業 829 社を対象に実施したセキュリティ対策の実態調査[10]で、サイバーレジリエンス強化のために、エンドポイントでの不審な挙動検出を行う EDR（Endpoint Detection and Response）製品や MDR（Managed Detection and Response）サービスを利用する企業は 23.4％導入していることを示した。AI や機械学習といった自動化の導入率は 10.3％で、インシデントレスポンスの迅速化と、セキュリティ人材不足の観点から、今後も導入需要が見込まれるとしたが、導入企業は一部にとどまる。

３．先行研究

今回の研究対象であるグループ企業のインシデント情報連携に関する先行研究は見つけることができなかった。そこで今回の研究対象について検討するために、「企業間のインシデント情報共有」、「グループ企業のインシデント体制」、「グループ企業の情報共有」に関する先行研究を調べ、参考にすることとした。

３－１．企業間のインシデント情報共有

はじめに、独立した企業間のインシデント情報共有に関する知見を調べた。

Koepke（2017）[11]は、企業が外部の組織へサイバーセキュリティやインシデントの情報を共有する際の「障壁（阻害要因）」について、下記の 8 つのカテゴリで整理・分析した。

＜阻害要因の分類＞
①憲法／法的：プライバシー懸念
②技術：互換性の欠如（独自言語）
③情報：情報量や信頼性を検証する困難さ
④コラボレーティブ：組織間の信頼確立
⑤管理：共有情報の不十分な管理
⑥組織：リソース不足、機密情報の管理と制御
⑦パフォーマンス：企業評判の低下、顧客損失
⑧費用：人的費用、技術導入費用、誤検知対応

Fuentes ら（2017）[12]は、異なる組織間でインシデント情報を共有することは協調的なサイバー防御戦略をとるために重要であるとしながら、情報共有の阻害要因として、共有する情報に含まれるプライバシーの問題を挙げた。共有先の組織に対する信頼やインフラストラクチャが安全でない場合でも、暗号化技術によりプライバシーを保護し、情報共有可能なモデルを提示した。

Rasmussen[13]は、企業間のインシデント情報共有における根本的な制約として、「早さ」「正確性」「網羅性」の 3 つ全てを担保した情報共有は困難であると発表した（図 4）。早くて正確な情報は網羅性に問題があり、早くて網羅的な情報は正確性が問題となり、正確で網羅的な情報は早さが問題になる、というものである。

図 4：情報共有のトライアングル

企業間のインシデント情報共有に関する知見から、以下のことが考えられた。グループ企業内での情報共有の困難には、グループ企業特有の形態に関する要因が存在すると考えられる。一方、企業同士の情報共有という点では、グループ企業内の情報共有においても一部共通する部分があ

り、参考にできると考えた。また、企業間の情報共有を阻害するプライバシーの問題は、経営を共にするグループ企業においては阻害要因にならないと考えられる。そして、インシデント情報共有で「早さ」「正確性」「網羅性」すべてを担保できない点は、グループ企業が各社ごとにインシデント対応スキルが異なることから、正確性の担保は困難であると考え、本研究では「早さ」と「網羅性」を重視する。

３－２．グループ企業のインシデント体制

次に、グループ企業のインシデント体制の全般的な問題に関する知見を紹介する。これらの問題はインシデント情報の連携にも大きく影響を与えると考えたためである。

太田ら(2019)[14]は、プラントを扱う企業のインシデント対応に必要な役割として、業務担当者と IT 担当者をうまく連携させるために「セキュリティマネージャー」がスーパーバイザーの立ち位置でマネジメントする必要があるとした。サイバー攻撃によらないプラントの異常時は、業務担当者だけでプラントの安全を確保するが、サイバー攻撃によるプラントの異常時には、業務担当者だけでなく IT 担当者の別途対応が必要となる。そこでセキュリティマネージャーが両者の連携をサポートする役割として、存在する必要性を説いている。これは、サイバー攻撃によるインシデントが発生から安全確保（対処完了）までに、業務担当者側と IT 担当者だけでは連携が困難であることに起因するとしている。

グループ企業の上位組織であれば、上記のようなセキュリティマネージャーを体制に入れることは可能と考えられるが、下位組織ではリソース面で現実には困難な状況にあると推察する。

小野ら(2015)[15]は、企業内で発生したインシデントへの対応において、SOC 要員の作業効率化を目的に、過去のインシデント情報から関連インシデントを自動抽出する方式を提案した。提案方式は以下の流れで抽出するものである。

①新規インシデントの基本情報を SOC ポータルへ登録。
②関連インシデント抽出機能で過去に対応したインシデント情報の類似度を算出。
③類似度から関連インシデントを抽出。

SOC 要員の対応スキルにより、インシデント対応にばらつきが生じる問題を取り上げ、インシデント対応業務の効率化をテーマとしている。提案手法の検証は、過去に蓄積されたインシデント情報をもとにした妥当性評価にとどまり、実際の SOC 要員に対して効率化の有効性は検証していないことを課題とした。

インシデント対応の人的負荷の問題は、本研究の情報連携においても同様の問題があると推察し、共有活動の効率化も重要な要素とする。グループ企業の上位組織では、その役割から要員のスキルは一般的に高いと考えられるが、逆に下位組織では企業ごとの異なる組織形態により、要員スキルのバラつきで結果が左右される懸念がある。

３－３．グループ企業の情報共有

最後に、インシデント時に限らない、グループ企業の情報共有に関する問題についての知見を示す。

山崎（2014）[16]は、B to B 企業のコーポレート・コミュニケーションに着眼し、先行研究では B to C に関する研究がほとんどで、B to B のコミュニケーションに関する研究が十分蓄積されていないことを明らかにした。近年の経営の傾向として、M&A による企業・事業の統廃合や、グループ経営を挙げ、今後は B to B 企業特有のコーポレート・コミュニケーションの知見が必要であると提言した。

宮元（2019）[17]は、グループ企業経営には親会社と子会社双方の密で頻繁なコミュニケーションが必要であることを、通信系事業者や製造業 4 社へのインタビューにより明らかにした。また、グループ企業マネジメントの観点で、各社のビジネス構造が異なれば子会社マネジメントの形態にも違いが現れ、どの形態が優れているとは一概に言えないとした。M&A によるグループシナジーの創出は、企業同士が共通言語によって、責任の所在とマネジメントの実態を透明化することが必要だと提言した。また、親会社が子会社を遠隔監視し、一方的に官僚的で硬直的な意思疎通は、異文化な背景をもつ子会社のマネジメントには馴染まず、どういう方法とルールを作るべきかに着目し、手を入れることが必要と考察した。

以上のグループ企業の情報共有の知見から、親会社とのコミュニケーションレベルは子会社ごとに異なることを認識できた。そのため、組織の形態がそれぞれ異なる下位組織から上位組織への情報連携には課題があると考える。

Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

4．研究目的

日本企業の現状は、インシデントへの緊急対応や、グループ会社・国内外拠点のセキュリティ統制・管理に課題を感じている企業が多く、実際にグループ企業の子会社を狙ったサイバー攻撃の被害事例も増加している。

グループ企業を構成する各企業は、それぞれ文化や風土、業種、規模、CSIRT 体制、セキュリティ担当者のスキル、コミュニケーションレベル、判断基準などが異なる。そのような違いにより、グループ企業内の発生インシデントを、下位組織から上位組織への情報連携に課題がある可能性を示した。また、インシデントには発生・検知した当該企業の対処だけでは不十分なものが存在し、グループのセキュリティを統括管理する上位組織でインシデントを把握することが望まれる。

先行研究では、グループ企業ではない外部企業とのインシデント情報共有に関する研究は多く存在するが、グループ企業内でのインシデント情報共有に関する研究は少ない。グループ企業は内部の組織でありながら、外部のような実態もある複雑な関係で成り立っているため、先行研究の内容では、グループ企業内特有の情報共有に関する問題は解決できないと考える。

本研究は、グループ企業内における内部発生インシデント情報が、下位組織から上位組織へ共有されない要因を網羅的に分析し、その対策の実現可能性と効果を明らかにすることで、インシデントによる被害拡大防止の一助となることを目的とする。

5．研究手法

まず、一般的な（グループ企業内ではない）企業間でインシデント情報共有する際の阻害要因について、先行研究で挙げられたものを参考にする。

その上で、グループ企業の下位組織から上位組織へインシデント情報を共有する際の阻害要因について、自身で考察した阻害要因と、グループ企業でセキュリティ業務に従事する担当者へインタビューすることで、要因の網羅性を補填する。

次に各阻害要因に対する対策を考察し、その実現可能性と対策の実施効果について考察する。

その対策について、グループ企業でセキュリティインシデント対応に従事する担当者へヒアリングし、評価・分析する。（表 1）

表 1：研究工程

①	グループ企業内におけるインシデント情報共有の阻害要因を網羅的に分析
②	上記①の各阻害要因に対策案を考察
③	上記②の対策案の効果と実現可能性を考察
④	グループ企業でセキュリティインシデント対応に従事する担当者へヒアリングし、評価・分析

要因分析の初めに、一般的なグループ企業の組織構成をもとに、下位組織から上位組織へ情報共有されないパターンを以下の 3 つのカテゴリで分類した（図 5）

「①孫会社から子会社へ共有されないケース」
「②子会社から親会社へ共有されないケース」
「③孫会社から子会社には共有されたが、その後子会社から親会社に共有されないケース」

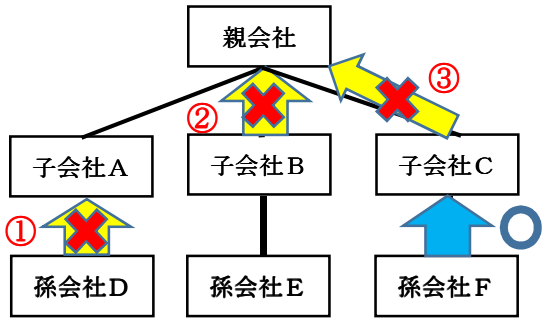

図 5：上位組織へ情報共有されないパターン

次に、情報共有を阻害する要因の在り処について、以下の 3 つのカテゴリで分類した。

「①会社そのもの」
「②担当者」
「③各会社とすぐ上の会社との関係」

以上の「上位組織へ情報共有されないパターン」と「情報共有を阻害する要因の在り処」の各分類について、マトリクスで組み合わせ「9 通り」の観点で、阻害要因を網羅的に洗い出した。洗い出しは先行研究の内容を引用し、筆者自身で列挙した後、グループ企業でセキュリティ業務に従事する担当者へヒアリングすることで、不足する内容を補完した。

グループ企業の下位組織から上位組織へ、インシデント情報を共有する際の阻害要因について、洗い出した結果（一部）を「表 2」に記す。

Vol.2020-CSEC-91 No.4
Vol.2020-SPT-40 No.4
Vol.2020-EIP-90 No.4
2020/11/25

表 2：グループ企業内におけるインシデント情報共有の阻害要因（一部）

情報共有のルート	阻害要因の在処	阻害要因の内容	先行研究より引用
孫会社から子会社へ	会社そのもの	インシデント情報共有の経験が不足	
		インシデント情報共有のノウハウが蓄積されていない	
		インシデント情報共有のポリシーが存在しない	
		インシデント情報共有の報告様式が不明確	○
		インシデント情報共有に関する経営層（孫会社）の認識・理解が不足	
		インシデント情報共有に関する従業員（孫会社）の認識・理解が不足	
		インシデント情報共有に関する社内教育が不足	
		インシデント情報共有を行う人材が不足	
		インシデント情報共有を行う組織体制が未整備	
		インシデント情報共有を効率的に行うツールがない	
		インシデント情報共有を行うツールが使いづらい	
		インシデント情報共有を行うツールが使えない（システム障害等）	
		インシデント情報共有を行う対応コストが発生	○
		インシデント情報共有活動を評価する制度や仕組みがない	
		グループ企業全体のインシデント情報共有ポリシーとは異なる 孫会社独自のインシデント情報共有ポリシーが存在	
		グループ企業全体のシステムやネットワークとは異なる 孫会社独自のシステムやネットワークが存在	
		コミュニケーションの取りづらい業務環境（在宅勤務等）	
		インシデント発覚による自社（孫会社）の評価が低下する懸念	○

孫会社から子会社へインシデント情報を共有する際の阻害要因を分析すると「会社そのもの」に関するものは「機会」が最も要因タイプとして要因の数が多く、担当者は「能力」と「動機」に起因する要因が比較的多い傾向が見られた。「会社そのもの」の要因は「機会」に起因するものが 10 項目あり、インシデント情報共有に関するポリシーやルール、人員、体制、ロケーションといった会社ごとの環境の違いが多くあるためと考えられる。また、「担当者」の要因としては「能力」が 6 項目、「動機」が 8 項目で比較的多く、担当者ごとのスキルや心的能力の違いが多くあるためと考えられる。「各会社とすぐ上の会社との関係」では、子会社と孫会社の役割分担や、会社同士の日頃のコミュニケーションに影響する要因が存在している結果となった。

6．まとめと今後の研究

日本企業はインシデントへの緊急対応や、グループ会社・各拠点のセキュリティ統制・管理に課題を感じている企業が多く、実際にグループ企業の子会社・孫会社を狙った攻撃の被害事例が増加している。グループ企業は企業ごとに文化や風土、規模、業種、CSIRT 体制、など形態に違いが存在する。グループ企業において下位組織から上位組織へのインシデント情報連携に課題がある可能性を示し、その情報共有の阻害要因を洗い出した。

阻害要因の分析結果は、「会社そのもの」は「機会」に関する要因が最も多く存在し、「担当者」は「能力」と「動機」に関する要因が多かった。「各会社とすぐ上の会社との関係」では、子会社と孫会社の関係性（役割分担やコミュニケーション）による阻害要因が存在していることが明らかとなった。

今後の研究では、各阻害要因への対策を示し、その対策の実施効果と実現可能性を考察・評価する。

参考文献

[1]総務省統計局,「我が国の「企業グループ」の現状について–経済センサス 基礎調査の集計結果から-」(2016) https://www.stat.go.jp/training/2kenkyu/pdf/gakkai/toukei/2016/yagishita.pdf

[2] 経済産業省,「グループ・ガバナンス・システムに関する実務指針（グループガイドライン）」（2019） https://www.meti.go.jp/press/2019/06/20190628003/20190628003_01.pdf

[3] 産業横断サイバーセキュリティ人材育成検討会 セキュリティ経営戦略検討 WG,「ユーザ企業のためのセキュリティ統括室構築・運用キット(統括キット)Part2【統括室編】」（2019）
https://cyber-risk.or.jp/contents/Security-Supervisor_Toolkit_Part2_v1.0.pdf

[4]NRI セキュアテクノロジー(株),「企業における情報セキュリティ実態調査」（2018）
https://www.nri-secure.co.jp/report/2018/analysis_global2018

[5](株)日経新聞社,「サイバー攻撃による社員等の個人情報流出について」（2020）
https://www.nikkei.co.jp/nikkeiinfo/news/release_20200512_01.pdf

[6](株)東芝,「当社グループのメールサーバへの不正アクセスについて」（2018）
https://www.toshiba.co.jp/about/press/2018_02/pr_j2802.htm

[7]三菱電機(株),「不正アクセスによる個人情報と企業機密の流出可能性について」（2020）
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

[8](株)レコフ,「ｸﾛｽﾎﾞｰﾀﾞｰM&A ﾏｰｹｯﾄ情報」（2019）
https://www.recof.co.jp/crossborder/jp/market_information/

[9]一般社団法人 日本シーサート協議会 会員一覧
https://www.nca.gr.jp/member/

[10]IDC Japan(株),「国内情報セキュリティユーザー調査：企業における対策の現状」(2019)
https://www.idc.com/getdoc.jsp?containerId=prJPJ45163119

[11] Priscilla Koepke,「Cybersecurity Information Sharing Incentives and Barriers」In : Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, Room E62-422（2017）

[12] Jose M.de Fuentes,Lorena Gonzalez-Manzano,Juan Tapiador,Pedro Peris-Lopez,「Privacy-preserving and aggregatable cybersecurity information sharing」In : Computers & Security 69（2017）p.127-141

[13] Rod Rasmussen,「Quality Over Quantity CUTTING THROUGH CYBERTHREAT INTELLIGENCE NOISE」,In : FIRTST Conference, Berlin,（2015）

[14]太田結隆,加藤勇夫,加藤瑠人, 越島一郎, 橋本芳宏,「インシデント対応プログラムに関する基礎研究～事前対応のためのフレームワーク～」, 国際 P2M 学会研究発表大会予稿集 p.458-475 (2019)

[15]小野裕美,白木宏明,大松史生,「セキュリティインシデント管理機能に関する関連インシデント抽出方法の提案」, 情報科学技術フォーラム講演論文集 2015 年 14 巻 4 号 p.273-274

[16]山崎方義,「BtoB 企業のステークホルダー・マネジメントにおけるコーポレート・コミュニケーションの考察」,日本広報学会 2014-03 p.78-90

[17]宮元万菜美,「グローバル企業におけるグループ企業マネジメント-日系グローバル企業の事例から-」, 日本管理会計学会誌 2019 年 27 巻 2 号 p.61-72