保険業界のサプライチェーンにおける
サイバーセキュリティ対策とその課題

日本アクチュアリー会 IT 研究会第５グループ

【担当委員】

ﾄｰﾏﾂ	長瀬　正憲
三菱 UFJ 信託	山北　一平

【メンバー】

大樹生命	池亀　弘晃
富国生命	延原　謙
アフラック生命	木村　健太郎
ＦＷＤ富士生命	春日　大志
ＡＩＧ損害	久保坂　祐士
ソニー損害	薗部　正裕
ＭＳ＆ＡＤシステムズ	杉野　泰
ニッセイ情報	名和　朋彦
ニッセイ情報	石原　斉治

目次

はじめに

企業においてIT技術が欠かせないものになった近年、サイバーセキュリティの重要性は高まっており経営リスクの一つと捉えられるようになった。企業を狙うサイバー攻撃は高度化・組織化が進んでおり、サイバーセキュリティに関するリスクも日に日に高まっている。特に、昨今ではセキュリティ対策が脆弱な関連企業（以下、サプライチェーン）を狙ったサイバー攻撃（いわゆるサプライチェーン攻撃）も増加しつつあり、自社のみならずサプライチェーンを含めた包括的なリスク管理の重要性が叫ばれている。

多くの保険会社はこうしたサイバー攻撃の脅威に対して、ウイルス対策や不正侵入防止といった技術的対策やサイバーセキュリティの知見を持った人材採用・育成といった組織的対策などの取り組みを進めている。その一方で、保険会社のサプライチェーンである中小の委託先や保険代理店においては、対策導入コストや対策を推進する人材不足といった問題で、十分なセキュリティ対策が取られていない可能性がある。

上記のような現状を踏まえ、当研究グループは、保険業務を遂行する上で欠かせない保険代理店や委託先など重要なサプライチェーンにおけるサイバーセキュリティ対策とその課題について考察し、保険業界のリスク管理高度化に資する提言を行う。具体的には、保険業界に特化した共助組織を設立し、その組織の中でサプライチェーンを対象としたリスク評価を行うことが有効であると考えた。

第Ⅰ章　サプライチェーンを狙うサイバー攻撃

Ⅰ―１．サイバーセキュリティを取り巻く状況

（１）近年におけるサイバー攻撃の状況

情報漏えい、標的型攻撃、ハッキング、ネット詐欺などサイバー攻撃に関する言葉を聞かない日はなく、サイバー攻撃は日進月歩で進化している。特に現在(2020年２月)は「Emotet」(エモテット)と呼ばれる攻撃メール(マルウェア)が国内外の組織で広く確認されている[1]。

Emotet の特徴は、感染したパソコンのメールの情報を利用し、被害を拡大させる点である。Emotet に感染すると、メールアドレスやメールボックスのデータを盗み出し、新たな攻撃メールに利用する。その結果、Emotet の感染者とやりとりしていた人物に対し、あたかも感染者本人が送ったかのような攻撃メールが送られてくる。このようなメールの添付ファイルを開くと Emotet に感染してしまう(図Ⅰ―１)。

保険会社がこのようなマルウェアへの対策を盤石にしていても、対策が手薄な保険代理店や委託先が感染する可能性はある。その保険代理店や委託先のメールボックスに残された個人情報が搾取され、サプライチェーンや顧客に対して攻撃メールが送付されることが考えられる。このようにサプライチェーンから感染が拡大するマルウェアは大きな脅威となっている。

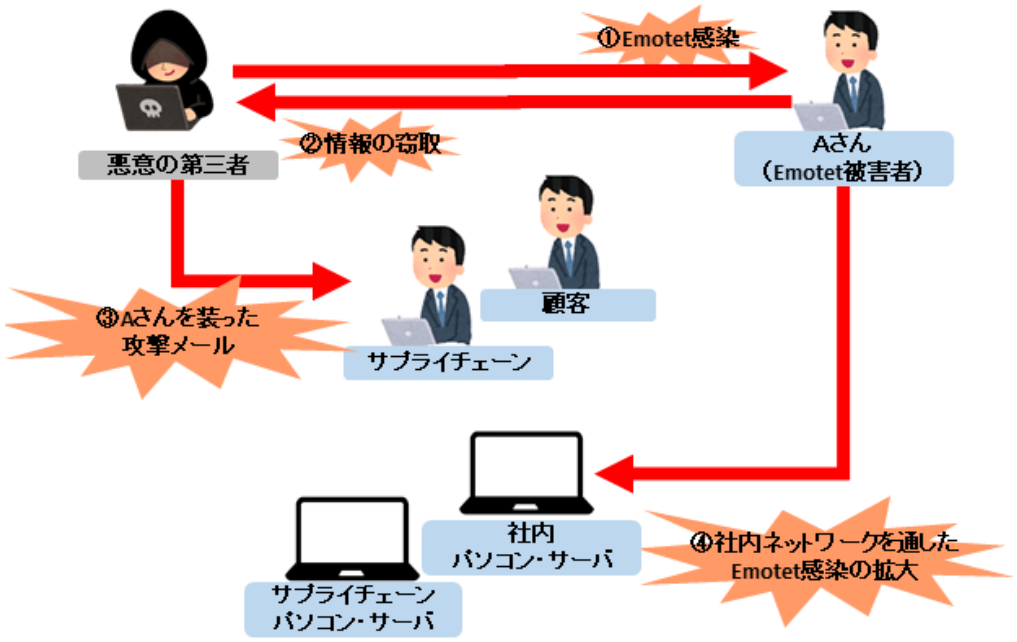


図　Ⅰ―１：Emotet による感染被害の例。A さんが Emotet に感染した場合、A さんのメールアドレスやメールボックスのデータを窃取され、サプライチェーンや顧客に A さんを装った攻撃メールが届く可能性がある。また社内ネットワークから感染が広がる可能性がある。

---

[1] JPCERT/CC「マルウエア Emotet の感染に関する注意喚起」
https://www.jpcert.or.jp/at/2019/at190044.html

（２）国内の金融機関におけるサイバー攻撃被害

金融機関へのサイバー攻撃被害事例をまとめた資料[2]によれば、保険代理店や証券会社、クレジットカード会社など様々な金融機関がサイバー攻撃の被害にあっている（表Ⅰ―１）。

保険業界の被害事例としては、2017 年 12 月に保険代理店で利用しているメールサービスから 5,400 件の顧客情報が漏えいしており、大量の顧客情報を保有する保険会社として、サプライチェーンを含めたセキュリティ対策が求められている。

また、銀行のサイバー攻撃被害について日本銀行が行ったアンケート[3]によると。2017 年以降に「サイバー攻撃を受けた」と回答した銀行は約 4 割にのぼっている。そして、1 割の銀行は「何らかの被害にあった」と回答しており、全てのサイバー攻撃を完全には防ぎきれていない状況がうかがえる。

こうした金融機関を狙ったサイバー攻撃は今後ますます増加していく可能性があり、サイバー攻撃への対策は非常に重要な課題となっている。

表　Ⅰ―１：国内の金融機関におけるサイバー攻撃の被害事例。毎年のようにサイバー攻撃被害が発生していることがわかる。

公表年月	金融機関名	概要	具体的な被害
2017/11	証券会社	情報漏えい （攻撃手口非公開）	顧客情報の漏えい 83 件
2017/12	保険代理店	利用していたメールサービスへの不正アクセスによる情報漏えい	顧客情報の漏えい 約 5,400 件
2018/01	仮想通貨取引所	利用者口座への不正アクセスによる不正出金、不正取引	不正出金 37 件 不正取引 137 件
2018/12	電子決済サービス会社	漏えいしたクレジットカード情報を悪用した不正利用	不明
2019/06	クレジットカード会社	不正アクセスによる情報漏えい	不正アクセス 1,917 件 不正利用 2,200 万円

[2] 佐々木 稔「金融機関を標的としたサイバー攻撃等の動向について」、2019 年 9 月公表
https://www.fsa.go.jp/frtc/seika/discussion/2019/DP2019-3.pdf

[3] 日本銀行金融機構局「サイバーセキュリティの確保に向けた金融機関の取り組みと課題－アンケート（2019 年 9 月）調査結果－」、2020 年 9 月公表
https://www.boj.or.jp/research/brp/fsr/data/fsrb200131.pdf

Ⅰ―２．新たなサイバー攻撃「サプライチェーン攻撃」

（１）サプライチェーン攻撃とは

前述したEmotetのように、サプライチェーンから感染拡大を狙うサイバー攻撃が増加している。この背景には、中小企業はセキュリティに割ける人員や予算などが大企業より少なく、セキュリティ対策が脆弱になりやすいことが挙げられる。

こうしたセキュリティ対策が脆弱な企業を狙って仕掛ける攻撃をサプライチェーン攻撃と呼ぶ。サイバー攻撃者は、初めにセキュリティ対策が脆弱なサプライチェーンを攻撃し、その攻撃が成功した後、そのサプライチェーンのネットワークや盗んだパスワードなどを利用して大企業やサプライチェーンへ攻撃を広げていく（図Ⅰ―２）。

委託先の再委託先など間接的に繋がりのある企業もサプライチェーンに含まれ、どこか一か所の綻びであっても不正侵入されてしまうと、営業秘密・重要技術・個人情報などの流出や、それに伴う顧客離れ、金銭被害に繋がり、大きな損失が発生することになる。

図　Ⅰ―２：サプライチェーン攻撃の説明図。本社のサイバーセキュリティ対策が万全だったとしても、子会社のサイバーセキュリティ対策が万全でなければ、ネットワークを通して子会社からサイバー攻撃を受ける。

（２）サプライチェーン攻撃被害の事例１－チケット事業会社の例―

2017 年にチケット事業会社が取り扱う顧客情報（約 15 万件）が流出した。サプライチェーンである委託先がサイバー攻撃を受けたことに起因して被害が発生したため、サプライチェーン攻撃による被害と言える。

当該事例では、チケット事業会社が運用委託する EC サイト[4]運営会社の WEB アプリケーションが持つ脆弱性を攻撃された。サイバー攻撃者は EC サイト運営会社のシステムへ侵入し、チケット事業会社が取り扱うクレジットカード情報を盗んだとされている。

EC サイト運営会社は EC サイトの開発をシステム開発会社へ再委託していたが、再委託先は仕様書に沿った開発を行っていなかった。その結果、強固なセキュリティを有したネットワーク内のサーバに保存されるはずであった顧客情報が、セキュリティの脆弱なサーバに保存されていた。

チケット事業会社は脆弱性の存在を認識していたが、EC サイト運営会社へ対策を講じているか確認をしていなかった(図Ⅰ―３)。

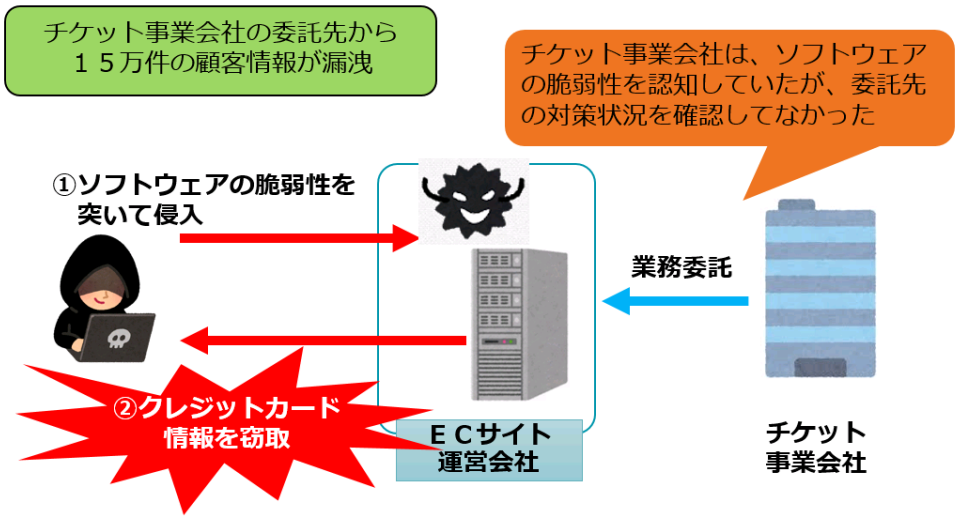


図　Ⅰ―３：事業会社のサプライチェーンに対する攻撃事例（脆弱性の悪用）。チケット事業会社は EC サイト運営会社に運用委託していた。EC サイト運営会社がサイバー攻撃を受けたことで、チケット事業会社の顧客情報が流出した。委託会社が狙われたサプライチェーン攻撃の事例といえる。

[4] EC サイト：電子商取引サイト。自社や他社の商品をインターネット上の Web サイトで販売するサイトのこと。

（３）サプライチェーン攻撃被害の事例２－保険代理店の例―

保険業界でも 2017 年に保険会社が取り扱う顧客情報（約 5,400 件）が流出した。保険代理店がサイバー攻撃を受けたことが原因であり、保険業界におけるサプライチェーン攻撃の事例と言える。

具体的には、保険会社から業務委託を受けた保険代理店があり、保険代理店の担当者は業務メールとしてメールサーバを利用していた。メールサーバは ID とパスワードを入力することでログインするメールサービスを提供していた。

この担当者が利用するメールアカウントの ID 及びパスワードがサイバー攻撃者に流出した。そしてサイバー攻撃者は当該メールアカウントの ID とパスワードを用いてメールサービスへログインし、メールボックスに残っていた顧客情報を窃取した。ID 及びパスワードが流出した経緯はわかっていないという。

窃取された顧客情報には、氏名、住所、電話番号、メールアドレス、生年月日、性別、証券番号、所有する自動車の車台番号、銀行口座情報、健康状態などが含まれており、保険会社のサプライチェーンにおいても重要な情報を保有していることがわかる（図Ⅰ―４）。

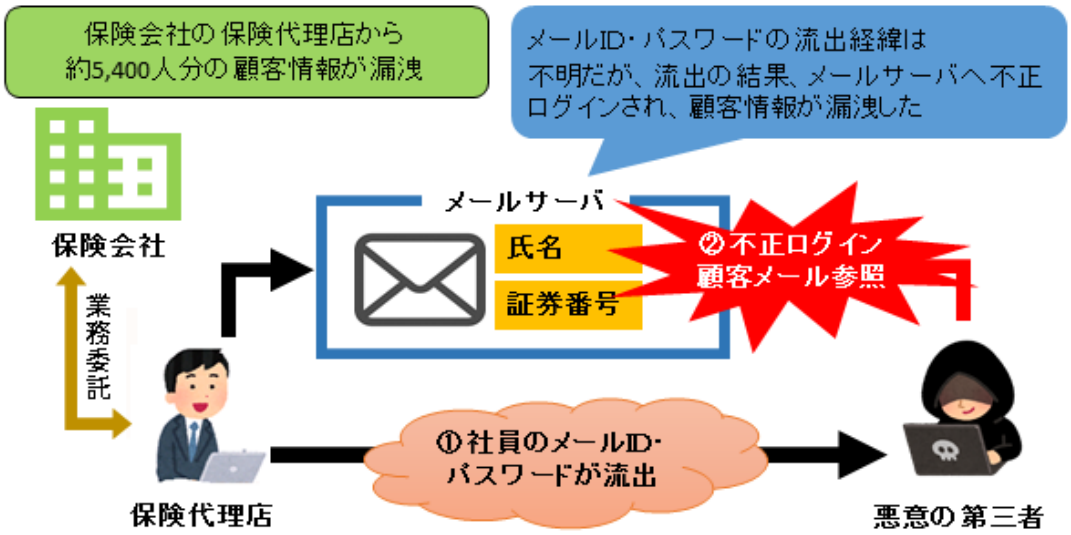


図　Ⅰ―４：保険会社のサプライチェーンに対する攻撃事例（不正アクセス）。保険代理店の担当者がメールサービスの ID とパスワードを盗まれたとされている。保険会社の顧客情報が窃取された、サプライチェーン攻撃の被害事例といえる。

Ⅰ―３．結論：保険会社にとってサプライチェーン攻撃の脅威は大きい

ここまで述べてきた通り、サプライチェーン攻撃の脅威が高まっている。そして保険会社にとってもサプライチェーン攻撃は脅威であると言えるだろう。

情報処理推進機構(IPA)が公表している「組織に対する情報セキュリティ１０大脅威」でも、「サプライチェーンの弱点を悪用した攻撃の高まり」としてサプライチェーン攻撃が新たに注目されている(表Ⅰ―２)。大企業ではセキュリティ対策が強化されているため、サイバー攻撃者はセキュリティ対策が不十分なサプライチェーンへの攻撃へシフトしている現状が反映された結果と言える。

他のランクインしている項目のほとんどが攻撃の「手段」であることに対して、サプライチェーンの弱点を突いた攻撃は「概念」として記載されていることに当研究グループは着目した。当研究では「サプライチェーンの弱点を突いた攻撃に対しては有効な対策が確立できていない」という仮説を立て、保険業界のサプライチェーンにおけるサイバーセキュリティ対策とその課題を検討する。

表　Ⅰ―２：組織に対する情報セキュリティ 10 大脅威 2019[5]

順位	組織に対する情報セキュリティ 10 大脅威	前年順位
1	標的型攻撃による被害	1
2	ビジネスメール詐欺による被害	3
3	ランサムウェアによる被害	2
4	**サプライチェーンの弱点を悪用した攻撃の高まり**	**NEW**
5	内部不正による情報漏えい	8
6	サービス妨害攻撃によるサービスの停止	9
7	インターネットサービスからの個人情報の窃取	6
8	IoT 機器の脆弱性の顕在化	7
9	脆弱性対策情報の公開に伴う悪用増加	4
10	不注意による情報漏えい	12

[5] 独立行政法人 情報処理推進機構(IPA)「情報セキュリティ 10 大脅威 2019」、2019 年 1 月公開
https://www.ipa.go.jp/security/vuln/10threats2019.html

第Ⅱ章　保険業界が守るべきサプライチェーンとは

Ⅰ章ではサプライチェーン攻撃が脅威となっていることを述べた。本章では保険業界において守るべきサプライチェーンとは何かを考察する。

「組織」「販売チャネル」「システム」の３つの観点から保険業界のサプライチェーン、および生命保険業界と損害保険業界のサプライチェーンの違いを考察し、その上で保険業界として守るべきサプライチェーンを定義する。

Ⅱ―１．組織から見た保険業界におけるサプライチェーン

セキュリティ対策は組織として行うものであり、組織のつながりをサプライチェーンと呼ぶことができると考えた。保険会社における組織のつながりには「保険会社」「グループ会社」「海外子会社」「保険代理店」「委託先」「再委託先」がある(図Ⅱ―１)。

（１）保険会社

保険業界におけるサプライチェーンの頂点は保険会社と考えることができ、セキュリティ対策は自社で行う。当然、サプライチェーンとは言えない。

（２）グループ会社

保険会社のグループ会社もサプライチェーンと考えることができる。しかしセキュリティ対策は親会社(保険会社) の指示に従う場合が多く、「守るべきサプライチェーン」というよりも保険会社の一部としてセキュリティ対策を実施するべきである。

（３）海外子会社

海外子会社は現地の法規制等に従う必要があり、国内の子会社とは遵守するべきセキュリティ対策が異なると考えられる。しかし、セキュリティ対策の実施に際しては、グループ会社と同様に親会社の指示に従う場合が多く、「守るべきサプライチェーン」というよりも保険会社の一部としてセキュリティ対策を実施するべきである。

（４）保険代理店

保険代理店は保険会社の子会社やグループ会社が担うことができるようになった。しかし、生命保険業界と損害保険業界の違いはあるが、外部へ委託する場合が圧倒的に多い。また個人情報なども多く保有しており「守るべきサプライチェーン」であるといえる。

（５）委託先

ここでいう委託先とは、保険代理店以外の業務を委託する組織としている。IT の目線で言えば、システム開発・運用を委託している企業が委託先といえる。このような委託先は保険会社の情報を多く共有しており、またシステムを通して重要な情報にアクセスできる

状態であるため、「守るべきサプライチェーン」であるといえる。

（６）再委託先

上記の委託先もさらに業務委託する場合があり、この委託先を再委託先と呼ぶ。特に IT 業界は再委託を二次受け、三次受け、と繰り返す多重請負構造になっており、前述したシステム開発・運用などの委託先には多くの再委託先があっても不思議ではない。これらの再委託先も、委託先と同様に保険会社の情報を多く共有しており、またシステムを通して重要な情報にアクセスできる状態であるため、「守るべきサプライチェーン」であるといえる。

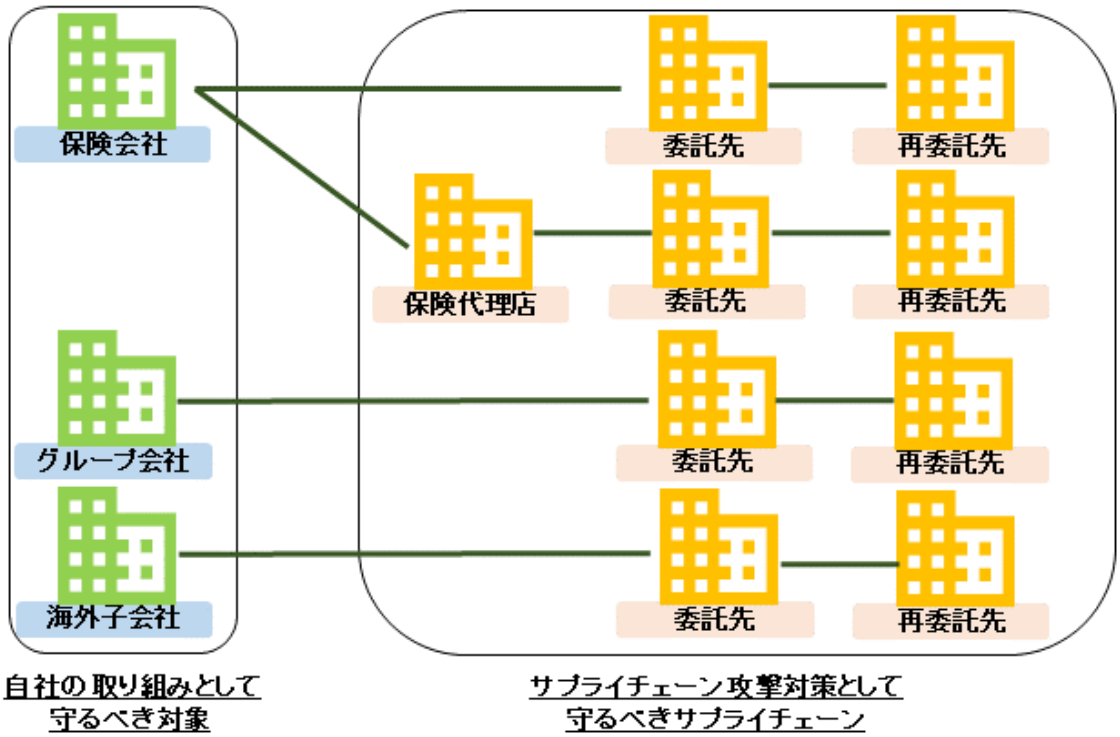


図 Ⅱ―１：組織の観点からみた守るべきサプライチェーン

Ⅱ－２．システムから見た保険業界におけるサプライチェーン

近年では自社システムが外部システムと接続することは一般的になっている。また自社システムについてもシステム開発・運用・保守の一部を外部へ委託することも一般的となっており、さまざまなサプライチェーンが存在している。

（１）システム開発・運用・保守の委託先／再委託先

システム開発・運用・保守する際には IT 企業にシステム開発を委託する場合が一般的である。システム開発は短期的に人手を集める必要があるため、直接システム開発の業務委

託を受けた IT 企業は他の IT 企業へ再委託する場合が多い(図Ⅱ―２)。

保険会社は自社でシステム開発することが少ないため、システム開発については社内システムに詳しい特定の委託先・再委託先に依存している場合が多い。そのため、委託先・再委託先はシステムにある顧客情報などに触れる機会も多く、「守るべきサプライチェーン」と言える。

（２）社内システムと接続している外部システム

社内システムが外部システムと接続することは一般的になっている。保険業界特有の外部システムとしては「保険共同ＧＷ」などがあるが、デジタル化が進みクラウドサービスなどの新しい外部システムへ接続する場合も増えている。

このような外部システムがサイバー攻撃を受けると、システムのつながりから社内システムに侵入されることも考えられるため、「守るべきサプライチェーン」と言える。

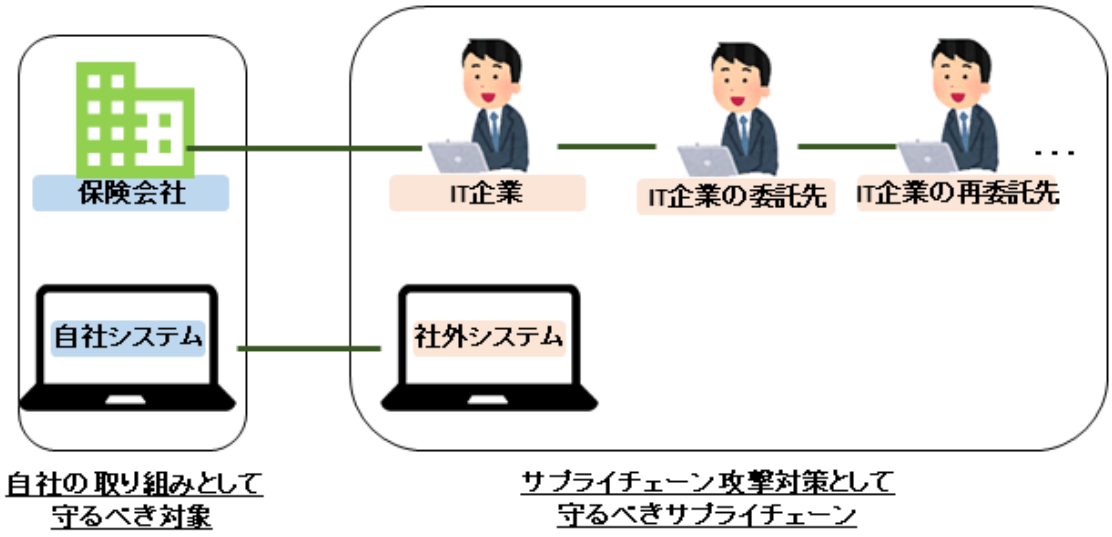


図 Ⅱ―２：システムの観点から見た守るべきサプライチェーン

Ⅱ―３．販売チャネルから見た保険業界におけるサプライチェーン

販売チャネルは顧客の個人情報などの重要な情報を保有している。また代理店システムや営業職員用の端末など、システムと接する部分も多く、セキュリティリスクは高い。よって販売チャネルから「守るべきサプライチェーン」の考察をすることは重要と考えた。

なお保険ブローカーは契約者から依頼するため、保険会社が守るべきサプライチェーンには含めないこととした(図Ⅱ―３)。

（１）生命保険の場合

生命保険業界では生保レディと呼ばれる営業職員が主な販売チャネルであった。しかし規制緩和に伴い販売チャネルが多様化し、営業職員以外にも多くの販売チャネルが存在す

る。

ａ．営業職員

営業職員は保険会社が直接指導しており、自社でセキュリティ教育・対策を実施するため、サプライチェーンとは言えない。

ｂ．保険代理店／来店型保険ショップ・窓口販売(銀行窓口・銀行員)

生命保険の販売を委託している販売チャネルとして、保険代理店や来店型保険ショップ、銀行窓口がある。前述したように大企業ほどセキュリティに人・予算を割けるため、銀行窓口などは保険会社が積極的に守る必要性はないかもしれない。しかしサプライチェーンという意味では「守るべきサプライチェーン」に含めることができる。

ｃ．ダイレクトチャネル(ネット保険・通販保険)

ネット保険はインターネットを通した販売チャネルであるが、一般的に保険会社がWebサイトを運営し、直接販売している。そのためサプライチェーンというより、自社としてセキュリティ対策を行うべきである。郵送申し込みも同様である。

（２）損害保険の場合

損害保険業界では保険代理店が主な販売チャネルであった。しかし、生命保険業界と同様、販売チャネルが多様化しており、販売チャネル自体は生命保険業界と大きな違いはない。ただし保険代理店が主な販売チャネルであった背景から、損害保険の保険代理店は様々な形態が存在する。ここでは「専業代理店」と「副業代理店」に分類して考察する。

ａ．営業職員（ソリシター）

損害保険業界では主に保険代理店を販売チャネルとするため、営業職員は保険代理店のサポートが主な役割となる。顧客接点は生命保険の営業職員よりは少ないが、もちろんセキュリティ意識は必要である。しかし自社としてセキュリティ教育を実施するべきであり、サプライチェーンとは言えない。

ｂ．専業代理店

専業代理店とは保険販売のみ行う保険代理店である。さらに個人が販売する個人代理店、法人が販売する法人代理店などがある。これらの保険代理店はプロ代理店とも呼ばれており、販売チャネルとして重要な役割を担ってきたが、一部では高齢化が進みITリテラシーの低下が懸念されている。こういった専業代理店はセキュリティに関するサポートの必要性も高く、個人情報などの情報も多く保有しているため、「守るべきサプライチェーン」と言える。

c．副業代理店

副業代理店は損害保険販売とは別に本業を持っている保険代理店である。形態はさまざまであり、例えば、自動車関連業や不動産業などの副業代理店がある。本業が忙しく、保険販売に多くのリソースを割くことができないという特徴がある。こういった副業代理店も個人情報などの情報を多く保有しているため、「守るべきサプライチェーン」と言える。

d．直販(ダイレクト型、通販型)

インターネットや電話申し込みによる損害保険の販売チャネルを直販と呼ぶ。インターネット経由であっても、一般的に Web サイトは損害保険会社が運営しており、自社として守るべき対象であり、「守るべきサプライチェーン」とは言えない。

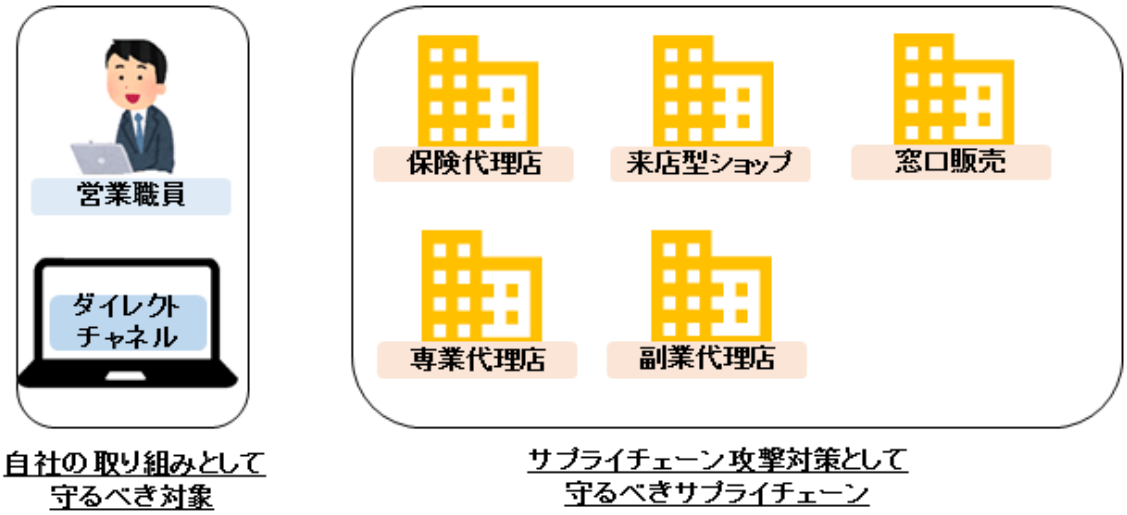


図 Ⅱ―３：販売チャネルの観点から見た守るべきサプライチェーン

Ⅱ－４　結論：保険会社は保険代理店と委託先を守るべきである

サプライチェーン攻撃を防ぐために守るべきサプライチェーンは「保険代理店」や「委託先」「再委託先」である。システムの目線から見れば、業務委託している IT 企業や外部システムが対象となるため「委託先」にまとめることができる。また生命保険業界と損害保険業界のサプライチェーンの違いは主に販売チャネルであるが、守るべきサプライチェーンという観点では両者とも保険代理店であり、業界間の違いはないと考える。

こうした保険業界のサプライチェーンの中心に位置する保険会社は、セキュリティ対策をリードしていく立場にある。一般的な IT セキュリティリスクへの対策には、新たなウイルス対策ソフトの導入といった防衛手段の構築や、情報セキュリティに特化した組織である CSIRT 等を立ち上げて管理態勢を整える等があげられる。しかしながら、これでは従来

の保険会社のみの防衛策の枠組みを超えておらず、サプライチェーン攻撃に対する対策としては不十分である。

そこで当研究グループはサプライチェーンを「委託先管理」の枠組みの中で守るべきであると考えた。サイバーセキュリティ対策はどのようなサプライチェーンでも必要であるため、保険代理店や再委託先も委託先としてとらえ、保険会社は委託先管理の枠組みの中でサプライチェーン攻撃の対策を行うのである。

サプライチェーンを守るためには、何がサプライチェーンのリスクなのかを正確に把握する必要があり、同時にセキュリティに関するリスク評価を精緻に実施する必要がある。リスク評価のためには、まずサプライチェーンのリスクを洗い出し、その重要性を評価した上で、そのリスク評価結果を踏まえてどのようなリスク対策（リスク受容・リスク低減・リスク移転・リスク回避）を行うか判断するという手順を踏む必要がある。

しかし、このような手順を踏むのには多くの課題がある。例えば、委託先や保険代理店などに対するリスク評価においては、契約がリスク評価を行うための障壁となってしまい、詳細なセキュリティ対策状況の確認を行うことが難しいことがある[6]。また、中小規模の委託先や保険代理店においては、経営層のセキュリティ意識が乏しいためリスクを適切に管理できていないことや、人材不足や予算不足などによりサイバーセキュリティ対策をしっかりと行えていないことがある。

セキュリティに関するリスク評価を精緻に実施していくために、どのような課題があるのか確認しなければならない。

---

[6] 例えば「委託先と締結した契約書にセキュリティ対策について明記されておらず、委託先から対策を謝絶されてしまった場合」や「再委託先のように保険会社と直接の契約関係がなく、対策を謝絶されてしまった場合」には対策ができない。

第Ⅲ章　保険業界における委託先管理の実態と課題

Ⅲ－１．委託先管理におけるサイバーセキュリティリスク管理

（１）委託先管理の概要

第Ⅱ章で述べたとおり、サプライチェーン攻撃への対策はサプライチェーンのセキュリティ対策状況を把握し、必要に応じて是正指示を行うなどの委託先管理が重要である。

金融情報システムセンター(FISC)の「金融機関等のシステム監査基準」[7]では、外部委託に関するリスクとコントロール[8]を定義し、金融機関が IT に係る業務の一部を外部委託する場合に行うべきコントロールの指標を示している(表Ⅲ－１)。

委託元である保険会社は、外部委託に関するリスクを認識し、それに対応したコントロールを行うことが求められている。ただし、実際には委託先の状況やコストの関係から、リスクをゼロにすることは現実的に難しく、残ったリスクに対するコンティンジェンシープランの策定を行うことが必要である。また、その対策は環境変化に応じて見直す必要がある。

表 Ⅲ－１：外部委託に関するリスクとコントロール

フェーズ	リスク	コントロール
外部委託方針・計画	・情報システム戦略と外部委託計画の不整合により、外部委託により期待される効果を上げることができないこと。 ・適切な外部委託先が選定できないことにより、サービスレベルや業務の継続性に支障をきたすこと。	・情報システム戦略に基づいた外部委託契約を策定すること。 ・外部委託先の選定にあたっては選定基準を策定し、客観的に評価すること。
契約締結時	・契約条項が不十分であることにより、要求事項、責任分界、補償等、契約締結後に問題が発生する、又は解決できないこと。 ・要求事項が明確に示されないことにより、外部委託業務のサービスレベルが確保できず業務運営に支障をきたすこと。	・全社共通の契約書の雛形を活用するとともに、法務部門等のチェックを受けること。 ・外部委託業務の種類や範囲に応じて、ＳＬＡ等によりサービスレベルの合意をとること。
契約期間中	・委託業務における不正や契約時の要求事項に対するサービスレベルの低下により、重要な情報資産の安全性や信頼性が損なわれること。 ・外部委託先で発生した問題に対して速やかに対応できないこと。	・外部委託先との契約内容及び選定基準に基づいた評価を継続すること。 ・外部委託管理態勢を整備し、委託業務遂行状況を確認すること。
契約終了時	・外部委託先の選定基準や評価プロセスに潜在している問題点が改善されず、外部委託業務で期待される効果を上げられないこと。 ・システムの廃棄やドキュメントの改修が適せずに実施されず、外部委託先から重要な情報が漏洩すること。	・外部委託先における業務実施状況及び業務の結果を分析・評価し、外部委託先の選定基準や評価プロセスについて見直しを行うこと。 ・消去証明書等の廃棄記録を受領することにより、システムの廃棄及びデータ消去の完了を確認。

[7] 公益財団法人金情報システムセンター(FISC)「金融機関等のシステム監査基準」、2019 年 3 月発行

[8] コントロール：リスクを低減するための行動。

以上のことから、委託先管理とは外部委託における計画から契約終了までの各フェーズに対してコントロールを繰り返し、外部委託先の統制を高めていくことであると言える（図Ⅲ―１）。

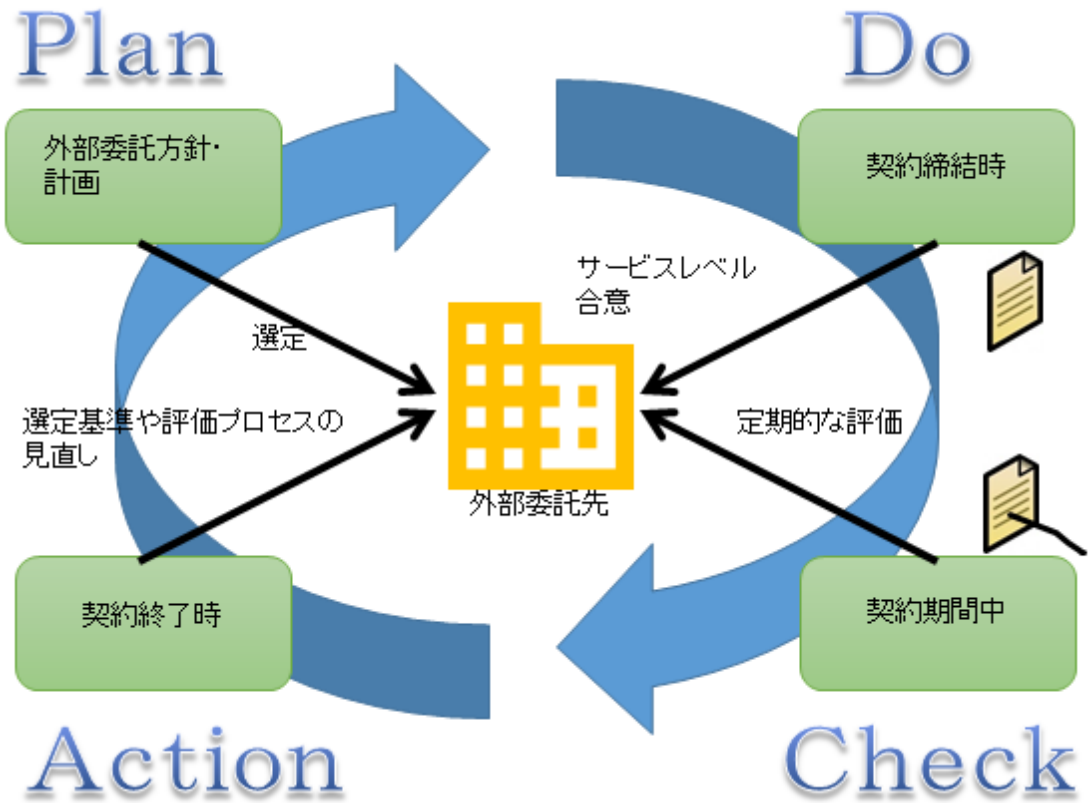


図 Ⅲ―１：委託先管理のイメージ図

（２）サイバーセキュリティリスク管理の必要性

委託先管理では様々な観点で委託先をリスク管理する必要があり、リスクは「事業継続性」、「コンプライアンスリスク」、「オペレーショナルリスク」、「情報セキュリティリスク」に分類される。どのリスク分類も、顕在化すると委託業務における安全性の低下に繋がる。特に「情報セキュリティリスク」が顕在化した場合、顧客情報を扱う委託業務については、当該リスクが顕在すると委託元へのダメージのみならず、顧客にも直接ダメージが及ぶ。そのためリスク管理の重要性としては優先度が高い。

また、第Ⅰ章で述べたとおり、最近では直接金銭的な利益を目的としたサイバー攻撃が増加しており、金融機関が標的とされる攻撃の増加が予想される。したがって、「情報セキュリティリスク」の中でもサイバーセキュリティリスク管理は必要性が高まっている。

（３）保険業界における委託先管理に関する課題の仮説

一般的には、委託先管理を十分に行うことで委託先の情報セキュリティへの十分な対策を促し、サプライチェーン攻撃のリスクを減らすことができる。しかし実際には、第Ⅰ章の事例 2 で説明したように、保険業界においても委託先や保険代理店へのサイバー攻撃を防ぎきれずに少なくない被害が出ている。したがって保険業界においてもより委託先管理を高度化し、サプライチェーン攻撃のリスクを低減させなければならない。

では、保険業界における委託先管理は何が課題となっているのだろうか。

例えば、米国連邦金融機関検査協議会(FFIEC)では、金融機関が自組織におけるリスクの識別とサイバーセキュリティの成熟度レベルを評価するために「Cybersecurity Assessment Tool[9]」を公表している。当該ツールでは評価要素を 5 つの領域にわけた評価が提唱されている(表Ⅲ―２)。当該ツールを利用して委託先の評価を行う場合、サイバーセキュリティの観点だけでも評価範囲が広くなる。また、全ての委託先にこの評価を実施するため、保険会社の負荷が非常に高い(図Ⅲ―２)。

このことから、当研究グループはリスク評価に課題があると考え、以下の 3 つの仮説を立てた。

仮説１：妥当性・客観性をもって委託先のリスク評価ができていない

監督省庁等で委託先管理の共通の指標が公開されているが、守るべき最低限の指標となっており、実際は各社が独自にリスク評価項目を定めてリスク評価を行っている。その結果、妥当性・客観性をもって委託先のリスク評価ができていないのではないだろうか。

仮説２：委託先のリスク評価を行うことが保険会社の負荷となっている

保険会社は個人情報など重要な資産を大量に保有しており、委託先に求めるセキュリティ水準も高くなり、リスク評価項目が膨大になっている。また保険代理店を含めた委託先の数が非常に多く、保険会社がリスク評価するべき対象が非常に多い。その結果、委託先のリスク評価を行うことが保険会社の負荷となっているのではないだろうか。

仮説３：委託先のリスク評価に多大な時間がかかっている

多くの委託先に対して膨大なリスク評価項目を用いてリスク評価していることにより、リスク評価に多大な時間がかかっていると考えられる。このことにより、実態はプロジェクト開始前に IT 企業のリスク評価が終わらなかったり、リスク評価が終わる前に IT 企業と契約してしまったりすることが発生しているのではないだろうか。

次節ではリスク評価の実態を確認し、上記の仮説の観点で課題の考察を行う。

---

[9] 米国連邦金融機関検査協議会(FFIEC)「FFIEC Cybersecurity Awareness」、2017 年 5 月
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

表Ⅲ－２：サイバーセキュリティ成熟度評価の領域と評価要素[10]

領域	評価要素
領域 1：サイバーリスクの管理と監督	ガバナンス、リスク管理、リソース、研修と企業文化
領域 2：脅威情報の収集と共有	脅威情報、モニタリングと分析、情報共有
領域 3：サイバーセキュリティ統制	防御、検知、改善
領域 4：外部依存関係の管理	外部との接続、関係管理
領域 5：サイバーインシデント管理とレジリエンス	・インシデントレジリエンスに関する計画策定と戦略 ・検知、対応および低減 ・エスカレーションと報告

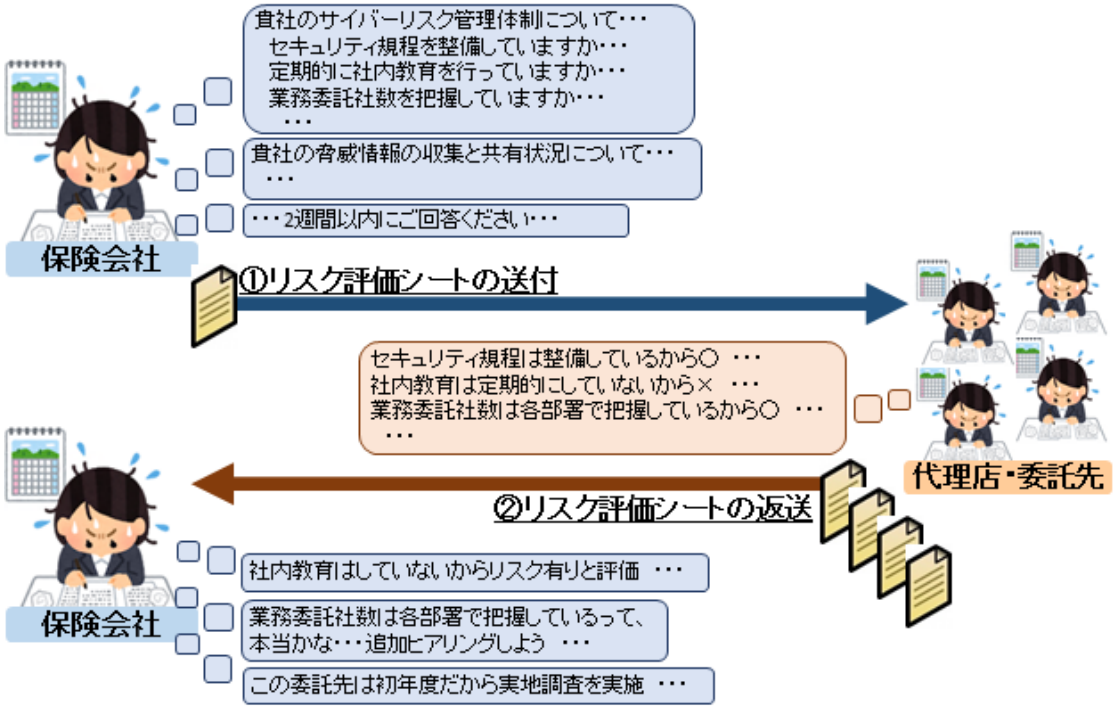


図 Ⅲ―２：保険会社におけるリスク評価の例。保険会社は膨大なリスク評価項目を洗い出し、全ての委託先にリスク評価シートを送付する。さらに返送されたリスク評価シートを元に委託先のリスクを評価する。リスク評価における保険会社および保険会社から評価を受ける委託先の作業負荷は非常に高い。

[10] NTT データ「FFIEC Cybersecurity Assessment Tool に関する調査研究」、2016 年 3 月 https://www.fsa.go.jp/common/about/research/20160815-1/01.pdf

Ⅲ－２．委託先管理におけるリスク評価の課題に対する考察

サプライチェーン攻撃件数の増加を受けて、各公的機関・セキュリティ専門会社は外部委託リスクに関する報告書を公表しており、その中で各業界の企業向けに実施したアンケートの結果が示されている。本節では下記の外部機関が実施したアンケートの結果および当研究グループにて実施した保険会社向けのアンケート結果をもとに、一般企業と保険会社の状況を比較し、保険業界の委託先管理におけるリスク評価の課題を考察する。

（１）参考としたアンケートについて

一般企業の状況を確認するために情報処理推進機構(以下、IPA)が実施したアンケート[11]およびEY Japanが実施したサーベイ[12]を参考にした。保険業界については委託先管理について公表アンケートがないため、当研究グループで実施したアンケートのみを参考とした。

a．IPAにて実施したアンケート（以下、IPAアンケート）

IT サプライチェーンリスクマネジメントへの取り組み向上に資することを目的としたアンケートである。IT サプライチェーン[13]における対策状況、およびインシデント発生事例について調査している。国内のITシステム・サービスの業務委託にかかわる業務部門を対象とし、対象企業は「資本金3,000万円以上かつ従業員数50人以上」とし、有効回答数は499社となっている。

b．EY Japanにて実施したサーベイ（以下、EYサーベイ）

サード・パーティー・リスク管理機能の管理、モニタリング、強化に関する洞察を提供することを目的として実施されたサーベイである。2017年10月から12月にかけてグローバルな金融機関54社を対象に行われている。

c．当研究グループにて実施したアンケート（以下、独自アンケート）

保険業界におけるサイバーセキュリティ対策の現状調査することを目的に行ったアンケートである。2019年8月にアクチュアリー会に所属する保険会社のIT部門を対象にアンケートを実施し、38社から回答を得ている。

---

[11] 情報処理推進機構(IPA)「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」、2018年3月公表
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html

[12] EY Japan「グローバル金融機関向けサード・パーティー・リスク管理サーベイ」、2018年4月公表
https://www.eyjapan.jp/services/advisory/global-contents/pdf/EY-TPRM-survey-2017-201804-ja.pdf

[13] ITサプライチェーン：ITシステム・サービスに関する業務を系列企業やビジネスパートナー等に外部委託し、その委託が再委託先、再々委託先と連鎖する業務委託の形態。

（１）リスク評価の妥当性・客観性

ａ．一般企業における実態と課題

IPA アンケートによれば「委託先の情報セキュリティ対策の確認等においてどのような点が課題だと考えますか」の問いに対し、最も多かった回答は「社内に十分な知見・スキルを持った人材がいない」（58.1%）であった（図Ⅲ－３）。委託先セキュリティ対策についての適正な評価には、十分な知見・スキルが必要不可欠であることを考えると、58.1%の企業は十分な品質のリスク評価が実施できていないといえる。

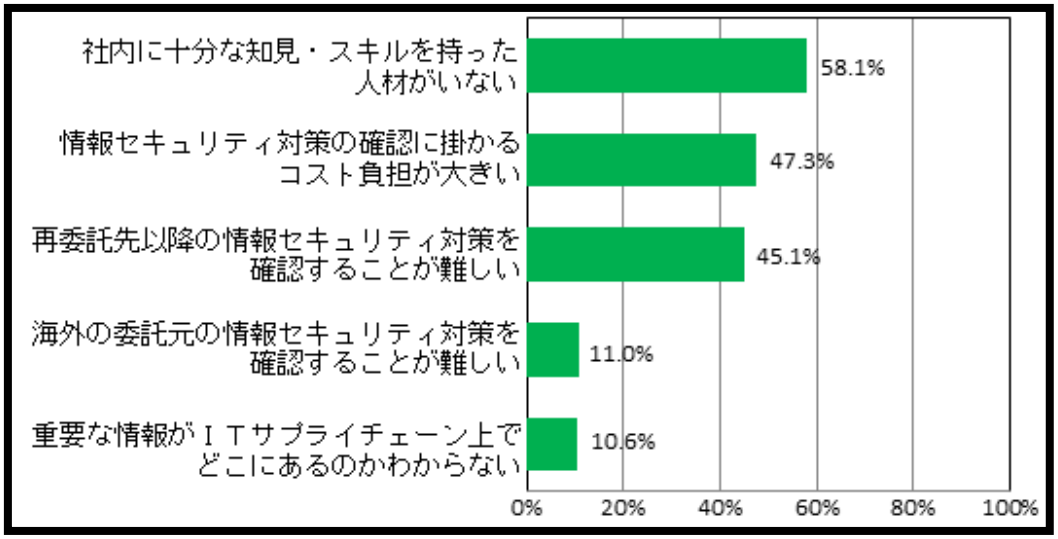


図 Ⅲ－３：「委託先の情報セキュリティ対策の確認等においてどのような点が課題だと考えますか」に対する回答（IPA アンケート）

また EY サーベイの「貴社が委託先の自己評価に使用する調査票[14]は、主に何を基準にしていますか」の問いに対し、「独自で作成したもの」及び「米国立標準技術研究所（NIST）のもの」が共に最も多い回答となっている（図Ⅲ―４）。

「米国立標準技術研究所（NIST）」が新しい評価基準のテンプレートを展開した事により、テンプレートを利用する会社は増加傾向にあるが、未だ多くの企業では独自で作成したリスク評価シートを使用して委託先管理を実施しているのが実情であると言える。独自で作成したリスク評価シートは妥当性・客観性は保証されない。

以上より、一般企業のリスク評価の実態として、リスク評価のための十分な知見・スキルが不足しており、評価基準の妥当性・客観性の確保が課題であるといえる。

[14] 調査票：ここではリスク評価シートと同義とする。

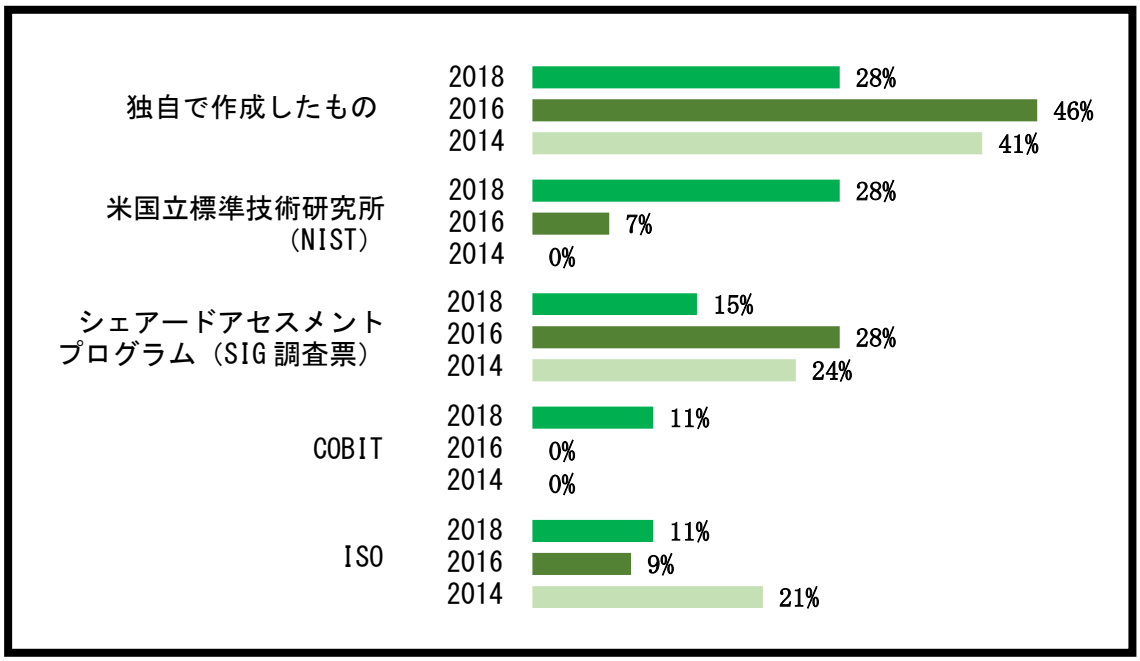


図 Ⅲ―４：「貴社が委託先の自己評価に使用する調査票は、主に何を基準にしていますか」に対する回答（EY サーベイ）

ｂ．保険業界における実態と課題

独自アンケートの「サイバーセキュリティに関する予算と人材について、当てはまるものをお選び下さい」の問いに対しては、サイバーセキュリティに関して「予算も人材も不足している」の回答が最も多かった(図Ⅲ―５)。

このことから、保険業界においても一般企業と同様に、予算や知見をもつ人材を十分に確保できない状況の中、リスク評価に必要な検討が不十分のまま独自のリスク評価シートを作成していると推察される。

以上より、保険業界のリスク評価の実態としても「妥当性・客観性のあるリスク評価が困難である」ことが課題であると言える。特に膨大な個人情報を扱う保険会社は、情報漏えいに繋がるインシデント発生を抑える必要があるため、リスク評価における妥当性確保が急務である。

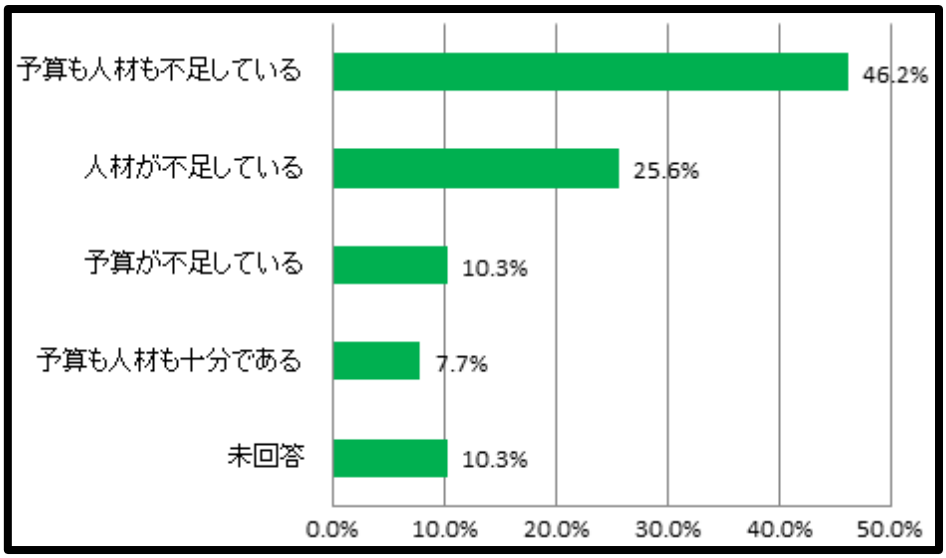


図 Ⅲ―５：「サイバーセキュリティに関する予算と人材について」に対する回答（独自アンケート）

（２）リスク評価の作業負荷

ａ．一般企業における実態と課題

前述した図Ⅲ－３の IPA アンケートでは「委託先の情報セキュリティ対策の確認等においてどのような点が課題だと考えますか」の問いに対し、「情報セキュリティ対策の確認にかかるコスト負担が大きい」を選択する企業が２番目に多かった。

委託元が負う責任として、委託契約締結後も契約時に合意した内容どおりに業務が進捗しているか、及びセキュリティ対策が遵守されているか等を定期的に評価する必要がある。定期評価の流れは一般的に「委託先へのリスク評価シートの送付」、「回答の評価」、及び必要に応じて「委託先での実地点検」と１社あたりにかかる作業負荷は大きい。このことが回答結果に現れていると考えられる。

EY サーベイの「貴社の重要な委託先は何社ありますか」という問いに対し、「20 社以下」及び「21～40 社」の回答が多いが、「100 社以上」の回答も 20%となっており、リスク評価の作業負荷が高まっていると想像できる(図Ⅲ―６)。

以上より、一般企業においては重要な委託先が増加しており、その数に比例してリスク評価の作業負荷が高まっていることが課題と言える。

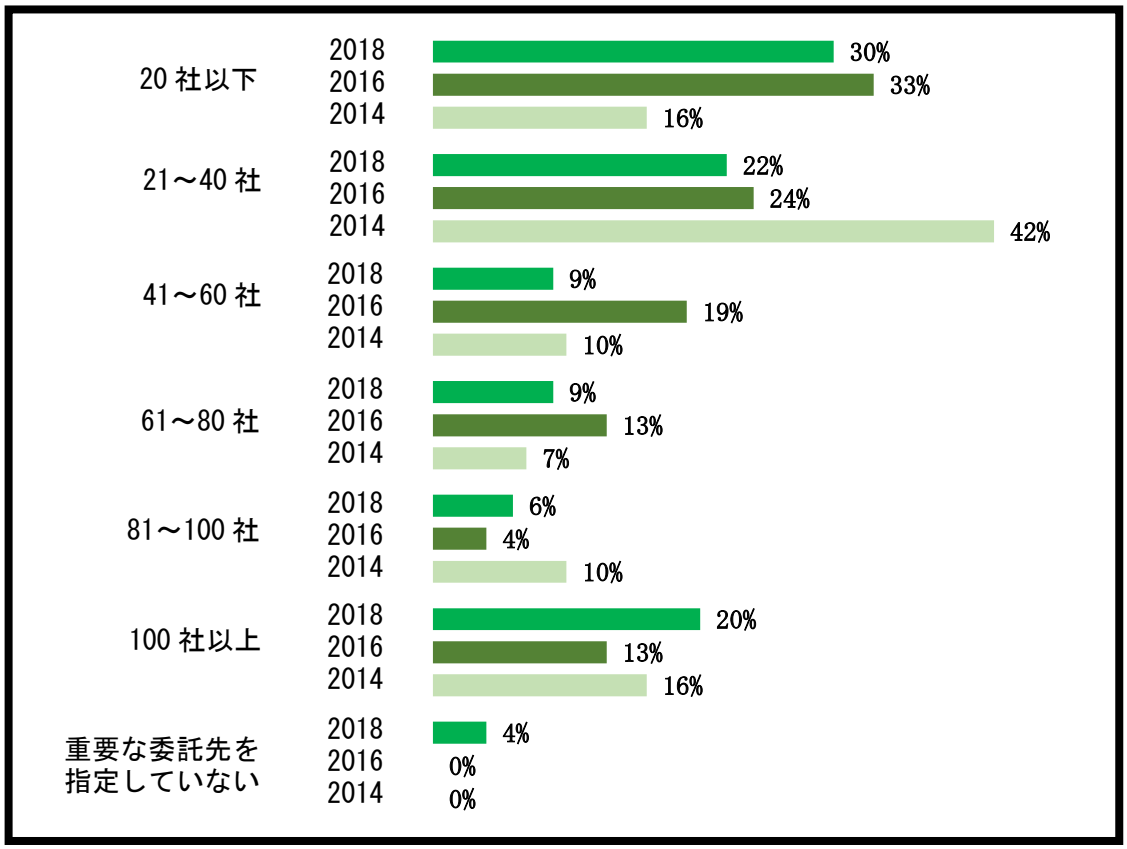


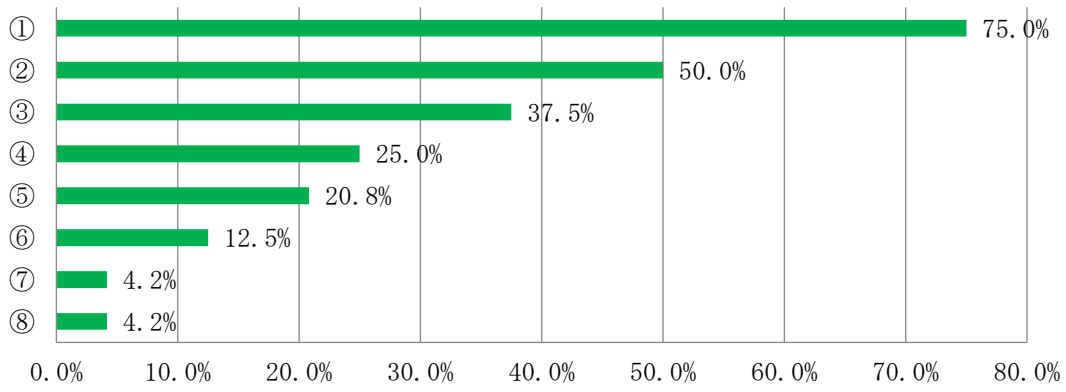
図 Ⅲ―６：「貴社の重要な委託先は何社ありますか」に対する回答(EY サーベイ)

b．保険業界における実態と課題

独自アンケートでは「代理店の情報セキュリティ対策について、どのような点が課題だと考えますか」の問いに対し、「セキュリティ対策状況を確認するための負荷が大きい」との回答が 3 番目に多かった(図Ⅲ―７)。

保険会社における委託先は保険システム構築等のシステム・サービス関連企業の他、保険業務の重要なビジネスパートナーである保険代理店がある。それぞれが個人情報を扱うためリスク評価は必須である。損害保険の保険代理店の数は 180,319 店（2018 年度時点）[15]であり、そのリスク評価にかかる工数は他業界と比較して非常に多い。このような背景から、保険業界において「セキュリティ対策状況を確認するための負荷が大きい」といえる。

以上より、保険業界においても「リスク評価にかかる作業負荷が大きいこと」が課題であると言える。



【回答選択肢】
① 多種多様な代理店（個人・法人／専属・乗合等）に対して統一的なルールを適用できない
② 代理店に所属する人材のITリテラシーが期待した水準に達していない
③ 代理店のセキュリティ対策状況を確認するための負荷が大きい
④ 代理店のセキュリティ対策を検討するため十分な予算・人材等が確保できない
⑤ 代理店のセキュリティ対策状況は、経営課題として未だハイリスク懸念の事案としていない
⑥ 代理店の数が多すぎるため、包括的な管理ができない
⑦ インシデント発生時における責任分界点について、代理店と確り協議できていない
⑧ 代理店との連絡体制が未整備のため、インシデント発生時に速やかな対応が取れない恐れがある

図 Ⅲ―７：「代理店の情報セキュリティ対策について、どのような点が課題だと考えますか」に対する回答(独自アンケート)。未回答 14 社を除く [16]。

[15] 日本損害保険協会「2018 年度損害保険代理店統計」、2019 年 7 月公表
https://www.sonpo.or.jp/news/release/2019/1907_03.html

[16] 未回答の理由は「代理店がない」「不明」など。アンケート対象が IT 部門であったことも未回答が多かった潜在的な理由と考えられる。

（３）リスク評価の作業時間

ａ．一般企業における実態と課題

リスク評価にかける作業時間に関して、委託先の自己評価の設問数の調査結果をもとに考察する(図Ⅲ―８)。

この調査は、企業が委託先の統制状況を評価する際に使用しているリスク評価シートの設問数を確認したものであるが、調査結果を見ると、半分近い企業で 251 問以上の設問があるリスク評価シートを使用していることが分かった(2017 年で 251 以上の設問がある調査票利用割合：47%)。

近年のサイバーインシデント発生状況を踏まえると、様々な観点で委託先のリスク評価を行う必要があるため、それに応じてリスク評価シートの設問数も用意する必要があると考えられる。以前であれば、基本的なセキュリティ対策状況を確認すれば済んでいた調査も、より踏み込んだ設問を用意し、委託先の具体的なセキュリティ対策やインシデント発生時の対応態勢なども評価することが求められていると推察できる。

また、委託先が回答したリスク評価シートを評価するにあたっては、項目数に比例した作業時間がかかると考える。例えば、「委託先の不正侵入対策の整備状況」を問う設問があった場合、「対策できている」という回答で可とするか、具体的な対策内容を追加確認するかで大きく作業時間も変わってくる。しかし、委託先に内在するリスクを適切に洗い出すためには、これまで以上に精緻なリスク評価が必要であり、それには相応の作業時間を要すると考える。

以上より、一般企業についても精緻にリスク評価を行うことが求められており、１つの委託先に対するリスク評価に多くの時間を要することが課題と考えられる。

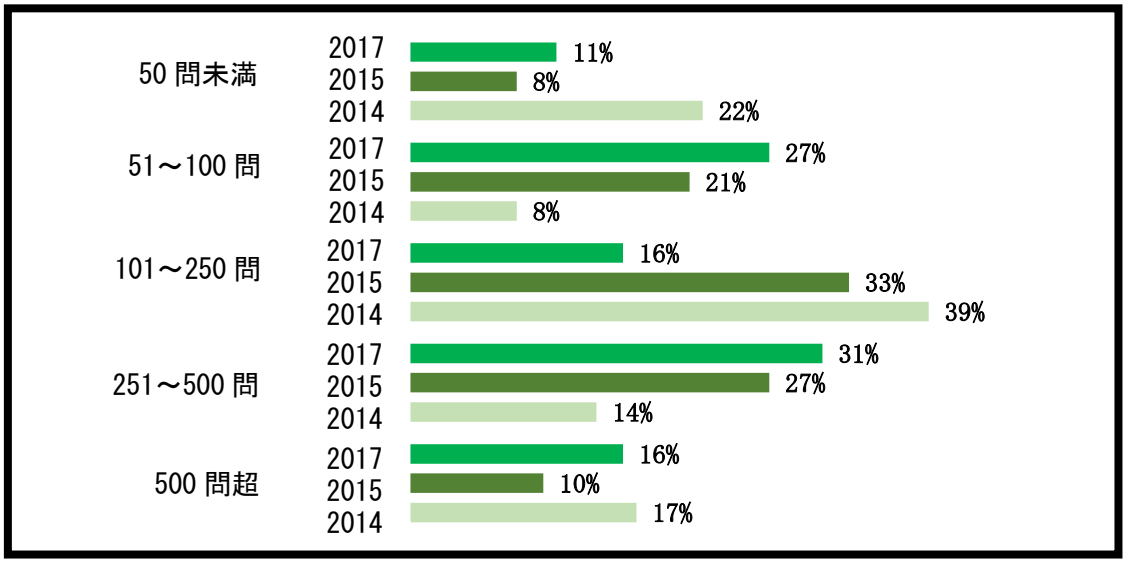


図 Ⅲ―８：「委託先の統制の自己評価に使用する貴社の調査票には設問が何個ありますか」に対する回答(EY サーベイ)

ｂ．保険業界における実態と課題

保険業界においてはリスク評価の指針が監督省庁等から示されている。「保険会社向けの総合的な監督指針[17]」では、保険会社が委託先の選定を行う場合、選定基準に基づく評価や適切なリスク管理が行われていることを確認することを求めている。また、サイバーセキュリティ観点でも、「サイバーセキュリティ経営ガイドライン V2.0[18]」が言及しているように、「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」を行うことが示されている。

こうした背景を踏まえると、保険会社がリスク評価に用いるリスク評価シートの設問数も、一般企業と同等もしくはそれ以上の設問数が用意されていると推察される。一方で、多種多様な委託先（保険代理店を含む）が存在する状況下で、短期間で適切なリスク評価を行うことは困難といえるだろう。何千人の従業員を抱える委託先も、ほとんど一人で事業を行っているような委託先も、同一基準でリスク評価するのは実質的に不可能であり、リスクベースでのアプローチ[19]が不可欠となる。すなわち、自社で重点的に管理するべき委託先とそうでない委託先を見極め、効率的なリスク評価を行うことが重要となる。そのためリスク評価に時間がかかっていると言うことができる。

以上から保険業界においても 1 つの委託先に対し「リスク評価に多くの時間を要する」ことが課題であると言える。

---

[17] 金融庁「保険会社向けの総合的な監督指針」、2018 年 2 月改正
https://www.fsa.go.jp/common/law/guide/ins/index.html

[18] 経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0」、2017 年 11 月公開
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[19] リスクベースでのアプローチ：守るべき対象を明確にし、重要度を評価することで、個別のリスクに見合った対策を行うというリスク管理の考え方。

Ⅲ－３．結論：保険業界における委託先管理の課題

保険業界における委託先管理の実態について、委託先のリスク評価に課題があると仮定し、「妥当性・客観性」、「作業負荷」、「リスク評価に要する時間」の３つの観点で考察を行ってきた。その結果、十分なリスク評価が出来ている保険会社は多くないと推察し、以下の３つの課題があると考えた。

課題１：妥当性・客観性のあるリスク評価が困難

各保険会社は十分な知見やスキルを保有する人材が不足する中、それぞれ独自の判断基準に基づき委託先のリスク評価を実施していると推察される。そのため、妥当性や客観性をもって、委託先のリスク評価を行うことが難しい状況下にあり、内在するリスクの検出やそのリスクを踏まえた判断ができているのか懸念が残る。

課題２：リスク評価にかかる作業負荷が大きい

各保険会社のほとんどは、委託先として非常に多くの保険代理店を抱えており、それらに対するリスク評価も大きな負荷となっていると考えられる。この課題は、リスク評価を受ける保険代理店にとっても同様であり、保険会社および保険代理店・委託先双方にとっての負荷になっている。

課題３：リスク評価に多くの時間を要する

リスク評価のチェック項目は多岐に渡り、多くの時間を要することが挙げられる。多数の委託先に対して、多くのチェック項目の確認を行うため、1 社ごとのリスク評価が希薄化する恐れが考えられる。

また、委託先管理のリスク評価に関しては、セキュリティリスク以外にも事業継続性やコンプライアンス等の評価の必要性もあるため、企業にとって効率的なリスク評価の仕組みを構築することが望まれていると推察する。

これらの課題を解決するためには、リスク評価を行う人材や関係する委託先の数など様々な課題があり、自社組織だけで解決することは容易ではない。そこで当研究グループでは保険業界に特化した共助組織が必要であると考えた。

第Ⅳ章　保険業界に特化した共助組織の提案

これまでの章で考察した委託先管理における課題を解決するため、当研究グループは新たな共助組織を設立し、その中でリスク評価を進めることを提案する。本章では、組織設立に伴う課題や懸念点、更に今後の展望について論じる。

Ⅳ－１．委託先管理における課題解決のための組織：情報共有コンソーシアム

委託先のリスク評価における様々な課題に対し、我々は「情報共有コンソーシアム」を設立することで課題解決につながると考える。情報共有コンソーシアムとは、保険会社における保険代理店や委託先のリスク評価を保険会社に代わり、一括で担う機関をさす。
情報共有コンソーシアムの特徴として、妥当性・客観性のあるリスク評価を、効率的かつ低コストで行える機能を備えている。これまで個々の会社で行われているリスク評価を情報共有コンソーシアムにアウトソースすることで、自社にとって必要な業務に注力することができるようになると考える。

この情報共有コンソーシアムが備える 6 つの機能について、以下に記載する。

（1）「課題１：妥当性・客観性のあるリスク評価が困難」を解決するための機能

機能１：妥当性・客観性のあるリスク評価結果の提供

情報共有コンソーシアムにリスク評価に精通した人材を集約し、各保険会社の代わりに一括で委託先や保険代理店のリスク評価を実施する。各保険会社でリスク評価を行う場合、担当者の知見やスキル不足によってリスク評価の精度が変動する恐れがあるが、第三者機関である情報共有コンソーシアムが専任で担当することで、妥当性と客観性のあるリスク評価を行うことが可能となる。

機能２：保険業界の知見を集約

情報共有コンソーシアムに参加する保険会社の知見や情報を集約・共有することで、業界のベストプラクティスとして活用することが可能となる。他社で実施したリスク評価結果に加え、リスク評価の基準などを共有し、より高度なリスク評価プロセスの構築を図る。保険業界に特化したセキュリティの課題を集中的に議論することで、これまで以上に有効な対策や改善策の創出ができると考える。

機能３：専門人材の確保・育成

今後、ますます確保が難しくなるセキュリティ人材を集中させ、専門人材の育成につなげることが可能となる。また、各保険会社と情報共有コンソーシアムで人材交流を行うことで、保険業界全体のセキュリティレベルの向上が図れる。情報共有コンソーシアムで収集したサイバーセキュリティの知見を各保険会社へ還元することで、自社内のセキュリティ対策もより一層強固に改善できると期待される。

（2）「課題２：リスク評価にかかる作業負荷が大きい」を解決するための機能

機能４：一括でリスク評価することで負荷軽減

各保険会社が実施していたリスク評価を情報共有コンソーシアムにアウトソースすることで、負荷軽減につながる。リスク評価を行う保険会社は、多数の委託先のリスク評価を行う必要はなく、情報共有コンソーシアムからのリスク評価結果を受け取ることで代替することができる。被評価側である委託先としても、各保険会社から類似のリスク評価を受ける必要はなく、一度のリスク評価を受けるだけで済む。そのため委託元・委託先双方にとって負荷軽減のメリットが大きいと考える。

機能５：実態を踏まえたリスク評価

セキュリティの専門家が委託先に対して実地調査を行うことで、地に足のついたリスク評価が可能となる。リスク評価シートの回答だけでなく、直接現場に赴き、セキュリティ対策状況を確認することで信頼性の高いリスク評価結果が得られるようにする。委託先の規模や委託業務の重要性等に応じて、リスク評価の深度に濃淡をつけることで、効率的なリスク評価を推進できる。

（3）「課題３：リスク評価に多くの時間を要する」を解決するための機能

機能６：蓄積されたリスク評価の活用で時間削減

情報共有コンソーシアムでは、各保険会社が行なったリスク評価結果を活用することができるため、自社のリスク評価に要していた時間を大きく削減することが可能となる。こうした作業時間の削減によって、重点的に確認すべき他の対象に、リソースを割くことができる。

Ⅳ－２．情報共有コンソーシアム設立に向けて

実際に情報共有コンソーシアムを設立する上で必要な要素について、人材、組織、システム、コストといった観点で考察を行う。

（1） コンソーシアムの運営に必要な人材

情報共有コンソーシアムとしては、各保険会社のサイバーセキュリティリスク評価部門の人材を集め、効率的にリスク評価を行える組織を構築することが必要である。保険会社は、サイバーセキュリティリスク評価をアウトソースすることで余裕ができた人材を、情報共有コンソーシアムへ出向させることで、より専門的な人材に育成することができる。情報共有コンソーシアム単体で不足する人材やスキルは、セキュリティベンダーや監査法人等の専門会社と協業することで補完することを想定している。

（２） コンソーシアムの運営に必要な組織と役割

情報共有コンソーシアムを組成するにあたり、組織構成としてリスク評価チーム、評価基準検討チーム、改善フォローチームの 3 つの役割を想定する。それぞれのチームは、情報共有コンソーシアム専任のメンバー、及び各保険会社から出向されるメンバーで構成される。必要に応じて、セキュリティベンダーや監査法人等の外部の知見を活用しながら組織運営することが想定される。

各チームの役割や作業範囲については、以下に記載する。

a. リスク評価チームの役割

リスク評価チームは、委託先のサイバーセキュリティリスクの評価を行う役割を担う。各保険会社からの依頼や定期的な評価値の更新スケジュールに基づき、リスク評価を実施する。評価方法としては、被評価先から受領する設問回答だけでなく、必要に応じて被評価先への実査等がある。リスク評価で得られた結果はコンソーシアム内部でチェックされた後、リスク評価管理データベースへ反映され、各保険会社から参照できるようになる。なお、リスク評価管理データベースは、各保険会社が保有しているリスク評価データも反映可能とし、既存データの有効活用を推進する（図Ⅳ―１）。

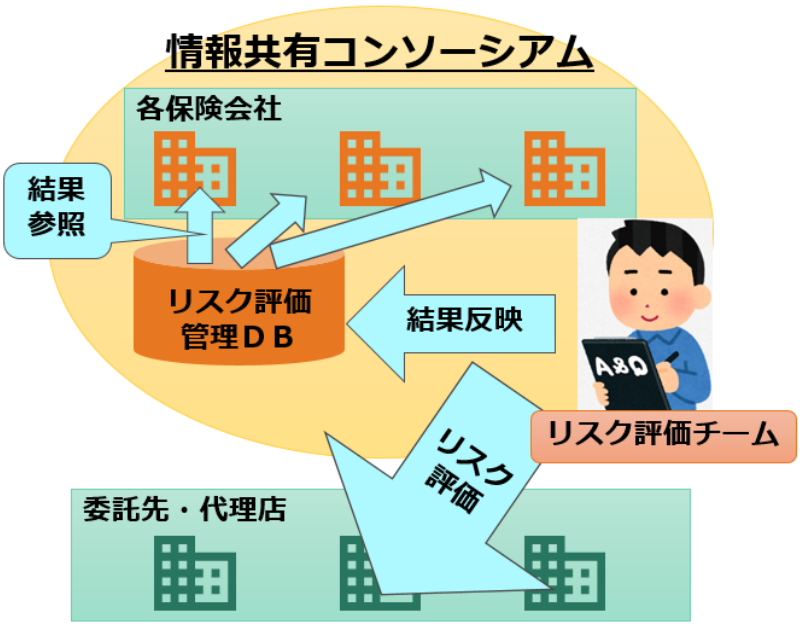


図 Ⅳ―１ ：リスク評価チームの役割イメージ図

ｂ．評価基準検討チームの役割

評価基準検討チームは、国内外のサイバーセキュリティに関するガイドラインや法規制等を踏まえ、保険会社として把握すべきリスク評価の基準を整備する役割を担う。各保険会社で利用されている評価基準を基に、リスク評価基準のベストプラクティスを整備する。評価基準が、委託先や保険代理店の重要度や最新のサイバーセキュリティ状況に合致するように、定期的な見直しを行う(図Ⅳ―２)。

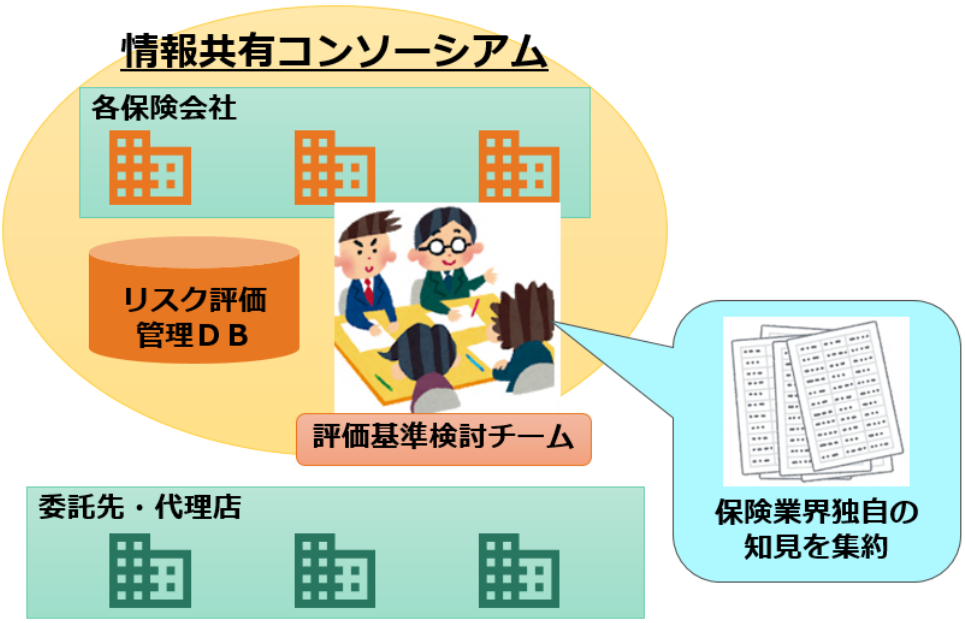


図 Ⅳ―２：評価基準検討チームの役割イメージ図

ｃ．改善フォローチームの役割

改善フォローチームは、リスク評価によって発覚した委託先や保険代理店の課題について、改善プロセスの支援を行う役割を担う。支援にあたり、セキュリティ関連規定の改訂等のガバナンスの整備のみならず、技術的対策の実装支援といった領域まで幅広く対応できる体制とする。コンソーシアムの要員だけでなく、監査法人やセキュリティベンダー等の外部協力会社と協業しながら支援を行う（図Ⅳ―３）。

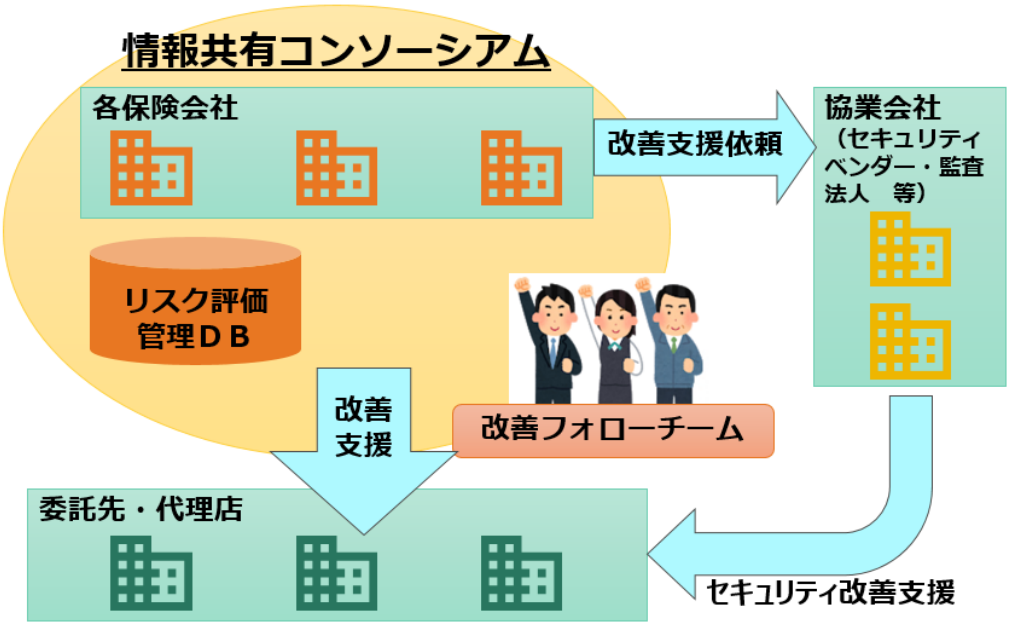


図 Ⅳ―３：改善フォローチームの役割イメージ図

（2）コンソーシアムの運営に必要なシステム

リスク評価の効率的な情報管理を行うために、情報共有コンソーシアム独自のシステムを構築する必要がある。リスク評価結果の登録・更新・参照等の機能を有したシステムを介して、各保険会社と委託先・保険代理店との間の情報連携をスムーズに行うことが可能となる。こうしたシステムの概要について、以下に記載する。

ａ．リスク評価管理システム

リスク評価管理システムに委託先や保険代理店のリスク評価結果が一元管理され、各保険会社は当システムへアクセスすることで、精緻化されたリスク評価結果を参照することができる。また、委託先や保険代理店に対して、セキュリティに関する設問回答をWeb上で実施できる機能も用意することで、データの標準化と負荷軽減を実現する。

リスク評価管理システムでは、被評価先からの自己評価や実査による確認結果等を総合的に勘案したスコアリングが行われ、セキュリティ格付けのような形で明示できるようにする。また各保険会社が過去に実施した委託先や保険代理店のリスク評価結果をリスク評価管理システムへ取り込み、有効活用することで、リスク評価実施の負荷を削減することが可能となる。

ｂ．リスク評価基準

「コンソーシアムの組織構成と役割」で述べた通り、リスク評価基準は評価基準検討チームによって整備される。各保険会社がそれぞれにリスク評価基準を策定するのではなく、保険業界特有のリスクに特化した統一的なリスク評価基準を用意し、リスク評価を実施する。各社の知見を持ち寄ることで、信頼性の高い評価基準を確立し、精度の高いリスク評価が実施できるようになると考える。

保険業では顧客の医療情報や事故情報など、厳格な管理が求められるデータを大量に取り扱うため、他の業界よりも大きな情報漏洩リスクを抱えている。こうした情報の管理方法に関しては、保有するデータ件数やデータの重要度等に応じた管理基準を定め、適切なセキュリティ対策が実装されていることを確認する必要がある。

（3）コンソーシアム運営に必要なコスト

情報共有コンソーシアムを運営する上でコストは、原則参加する保険会社で費用分担することを想定する。被評価者である委託先や保険代理店から費用を徴収する方法も考えられるが、作業負荷に加え、費用負担を求められることによって、情報共有コンソーシアムへの積極的な協力が得られない恐れがある。こうした点を加味すると、情報共有コンソーシアムの運営コストは、保険会社で費用分担することが望ましいと考える。費用の負担方法としては、固定費に加え、委託先・保険代理店へのリスク評価依頼数やリスク評価結果の照会量等に応じた従量課金が考えられる。

情報共有コンソーシアムの利用を促す上でも、リスク評価管理データベースで保有する評価結果の量や質が重要となる。そのための施策として、情報提供や要員支援等のリスク評価に貢献する活動を行った保険会社に対して、徴収する運営費を割り引くといった方法が考えられる。

Ⅳ－３　情報共有コンソーシアムを運営していく上での懸念点

この章では情報共有コンソーシアムを運営していく上での懸念点について論じる。

（1）インシデント発生時の責任

極めて精度の高いリスク評価を行い、委託先の保有するリスクは少ないと評価されたとしても、絶対にインシデントの発生がないと情報共有コンソーシアムが保証することは不可能である。なぜなら、インシデントの発生は自社環境のみならず、サイバー攻撃の種類・方法の変化や利用するソフトウェアの脆弱性といった外部環境にも影響を受けるためである。また、情報共有コンソーシアムのリスク評価にかけるリソースも有限であり、サプライチェーンの全ての情報を確認することはできないため、確認できていない領域のリスクをある程度は検討しておく必要がある。

インシデント発生時の責任主体は保険会社または委託先にあり、情報共有コンソーシアムは確立した作業手順に基づいて検出したリスクを報告するという点に責任を持つ。そのため、保険会社はリスク評価結果を踏まえつつ、インシデント発生時には委託先との契約に基づいた対応が必要となることを理解した上で、情報共有コンソーシアムにリスク評価を依頼することが重要である(表Ⅳ―１)。

表 Ⅳ―１：情報共有コンソーシアムの責任主体

情報共有コンソーシアムの責任	✓ 保険会社に対して、委託先のリスク評価結果を開示する ✓ 保険会社、または委託先からの依頼に基づき、セキュリティ改善支援を行う ✓ 適切な手順に従い、リスク評価を行う
保険会社の責任	✓ 受領したリスク評価結果を踏まえ、自社の責任の下で委託先の選定を行う ✓ 契約締結後の委託先の管理を行う

（2）定期的な評価の必要性

リスク評価を一度行ったらそれで終わりではなく、最新のセキュリティ情勢や監督官庁等の動向などを踏まえて定期的に再評価を行う必要がある。

具体的には、国内外の主要な評価基準の変更、被評価団体の組織変更や合併、インシデントの発生、保険会社からの要請等があった場合に、再評価を行っていく。再評価の結果、

新たなリスクの検知やリスク値の大きな変動などが生じた場合、その被評価先を利用している保険会社、並びにその被評価先に対して通知を行う。

なお再評価の方法としては、全ての評価項目をチェックする方法と一部の項目を重点的にチェックする方法を用意し、リスク評価の負荷軽減と効率性向上を図る。

（3）組織形態（営利・非営利）の議論

現時点で情報共有コンソーシアムの組織形態としては、非営利での活動を想定している。理由として、発足時はコンソーシアムが保険会社の協力無しには実現しないため完全に独立した運営が難しいこと、そしてその状況下での営利の活動は利益相反が発生する蓋然性が高くなると考えるためである。

営利の活動で運営を開始した場合、当初から高いレベルで妥当性や信頼性のあるリスク評価結果が求められることになる。また組織立ち上げからリスク評価実施までのプロセスを確立するまでには少なくない時間がかかると推察され、情報共有コンソーシアムの利用を広めていく上で大きなハードルとなると考えられる。まずは喫緊の課題であるサプライチェーンリスクに対応するため、可能な限り速やかに情報共有コンソーシアムを立ち上げ、保険業界全体のセキュリティレベルを高めることが重要である。

今後、独立性を保ち、妥当性かつ客観性のあるリスク評価ができる体制を確立出来た場合には、組織や機能をより発展させていくためにも営利団体へ移行することも検討対象と考える。

Ⅳ－4　情報共有コンソーシアムの展望

この章では情報共有コンソーシアムの展望について論じる。

（1）セキュリティ格付けの発行

委託先のセキュリティ対策レベルによって、認定資格やランキングなどを設けることを将来的には考えている。業界特有のサプライチェーンに応じたサイバーセキュリティ対策のベストプラクティスを共有することは、サプライチェーンリスクを低減する上でも非常に有効である。

セキュリティ対策レベルを可視化し、そのレベルによって保険会社各社が保険代理店手数料などのインセンティブにつなげていくことにより、保険業界、及びそれを取り巻くサプライチェーン全体のセキュリティ対策レベルを高めていくことができるのではないだろうか。

（2）他業界への展開

本論文では保険業界向けの情報共有コンソーシアムとして設立意義や運営構想を論じてきたが、これは他業界でも応用可能だと考えている。サイバーセキュリティの問題は保険

業界のみならず、全ての業界で喫緊の問題となっている。日本政府からの要請等によるトップダウンの働きかけだけではなく、今後は業界全体で密接に協力するボトムアップの活動も必要となってくるだろう。

今回論じた情報共有コンソーシアムのリスク評価の仕組みとそれぞれの業界特有の知識・慣習を掛け合わせていけば、様々な業態に広げられることが可能だと考える。

おわりに

今回論じてきた通り、もはやサイバー対策は自社だけ対応してれば良いものではなく、自社のサプライチェーンを含めサイバーセキュリティ対策を行う必要がある。よって、それぞれの会社が各々にリスク対策を行うのではなく、保険業界全体で知識や人材を共有し合い、業界全体でセキュリティ対策レベルの底上げを行っていくことが重要である。

保険業界という社会的に重要な金融インフラを担うものとして、この論文がより質の良い安心感のあるサービスを作る一助になれば幸いである。

謝辞

当研究の実施に際し、技術支援やヒアリングにご協力いただきました関係各社の皆様、アンケートにご協力いただきましたアクチュアリー会賛助会員各社の皆様、私たちの研究活動を支えてくださった多くの方々に、この場をお借りして深く御礼申し上げます。また、ご多忙の中、IT 研究大会開催の準備にご尽力いただき、当研究の発表の場を提供いただきましたアクチュアリー会ならびに IT 委員各位に、深く御礼申し上げます。

最後に、IT 研究会への参加を支援いただきました各研究メンバーの所属会社へ厚く感謝いたします。