Vol.2019-IOT-44 No.9
2019/3/7

サイバー保険の調査・分析による加入率向上への提案

Proposal for Improvement of Penetration on Investigation and Analysis of Cyber Insurance

佐久間朱里[†1]　猪俣敦夫[†2]

概要：2017 年の個人情報漏えい人数が約 520 万であった．また，攻撃を受けた場合の業務への影響，原因調査・対策，顧客への対応等に要する時間や費用は，企業にとって大きな負担となる．経済産業省の「サイバーセキュリティ経営ガイドライン」ではリスク移転策として，「サイバー保険の活用」を示している．しかし，国内企業のサイバー保険への加入率は 17.2%にとどまっている．本論文は，各国の個人情報保護法制施行を受け，世界に与える影響をセキュリティ対策・サイバー保険の市場規模の観点から調査した．これにより，日本企業におけるサイバー保険の加入しない理由の上位であった原因の対策を示せたと考える．

キーワード：サイバー保険

1. はじめに

現在，サイバー犯罪による世界の被害額は 6000 億ドルに上ると言われている．また，日本におけるサイバー犯罪件数も大幅に増加傾向にあり，サイバー攻撃を完全に防ぐことは困難な状況となっている．さらに，近年，個人情報漏えい事件が多発し，深刻な問題になっている．JNSA セキュリティ被害調査ワーキンググループが発表した情報セキュリティインシデントに関する調査報告書[1]によると，2017 年の個人情報漏えい人数が 519 万 8,142 人であった．さらに，1 件当たりの平均損害賠償額は 5 億 4,850 万円に上る．また，攻撃を受けた場合の業務への影響，原因調査・対策，顧客への対応等に要する時間や費用は，企業にとって大きな負担となる．

こうした背景を受け，経済産業省の「サイバーセキュリティ経営ガイドライン」[2]を策定した．これには，経営層が認識すべき「3 原則」・セキュリティの担当幹部に指示すべき「重要 10 項目」が提示されている．そして，サイバーセキュリティリスクの特定と対策の実装のリスク移転策として，「サイバー保険の活用」を示している．

日本では，世界的なサイバー犯罪の増加を受けて，2015 年から複数の大手保険会社で企業向けのサイバー保険の取り扱いが開始された．しかし，IT 専門調査会社の IDC Japan 社が 2017 年 4 月に発表した国内企業の情報セキュリティ対策実態調査結果によると[3]，国内企業のサイバー保険への加入率は 17.2%にとどまっており，企業におけるサイバー保険の普及率は限定的といえる．

そこで本論文では，日本におけるサイバー保険の加入率が低い理由の原因を探る．また，各国の個人情報保護法制施行を受け，世界に与える影響をセキュリティ対策・サイバー保険の活用法の観点から調査する．この結果より，諸外国と日本のサイバーセキュリティに対する相違を見つけ，サイバー保険の普及率向上への提案を行う．

2. セキュリティ被害

2.1 実態調査

情報セキュリティに関するインシデントが発生した場合，一企業の被害総額の平均は 2 億円を超えると言われている．大手企業にいたっては，被害はその倍以上になるとのデータも存在する．トレンドマイクロの「法人組織におけるセキュリティ実態調査」2016 版[4]によると，被害総額の平均は 2 億 1,050 万円となり，前年度調査の約 1.6 倍に膨れ上がっている．また，従業員数 5,000 名以上の組織になると，被害総額平均は 4 億 5,628 万円に及び，従業員数 50 名～99 名の組織の被害額平均も前年比約 2.6 倍の 1 億 3,802 万円に達している．

言うまでもなく被害額は損失であり，組織の利益を直接圧迫するものである．仮に組織の売上対利益率が 5%～10%と想定すれば，2 億円の損失をリカバーするのに 20 億円～40 億円を売り上げなければならない計算になる．情報漏えいなどのセキュリティインシデントを発生させ，組織の信用・信頼が低下する中で，それだけの売上を上積みするのは簡単なことではないと考える．

2.2 情報セキュリティインシデントに関する調査

JNSA セキュリティ被害調査ワーキンググループが 2017 年 1 月 1 日から 2017 年 12 月 31 日までにニュースサイトなどで報道された個人情報漏えいインシデントの記事，インシデントに関連した組織がウェブサイトで公表した謝罪文などを対象に関連する情報を収集した．その上で，記事や文書に書かれた内容を元に，インシデントの分析に必要な情報を整理し，漏えいした組織の業種，漏えい人数，漏えい原因，漏えい経路などについて分類・評価を行った[5].

†1 東京電機大学未来科学部情報メディア学科

†2 東京電機大学未来科学部情報メディア学科教授

個人情報漏えいインシデントのトップ 10 を図 1 に示す.

No.	漏えい人数	業種	原因
1	118 万 8,355 人	製造業	不正アクセス
2	67 万 6,290 人	公務	不正アクセス
3	59 万 7,452 人	情報通信業	不正アクセス
4	37 万 1,200 人	情報通信業	不正アクセス
5	19 万 9,169 人	公務	不正アクセス
6	19 万人	サービス業	管理ミス
7	18 万 4,981 人	公務	管理ミス
8	16 万 3,000 人	公務	紛失・置忘れ
9	14 万　408 人	情報通信業	不正アクセス
10	13 万 1,936 人	卸売業, 小売業	不正アクセス

図 1　2017 年個人情報漏えいインシデント　トップ 10

2.3 情報漏えい原因

情報漏えいの原因[5]は，誤操作 25.1%，紛失・置忘れ 21.8%，不正アクセス 17.4%となった．漏えい原因の分類を以下に示す[6].

- 誤操作

  宛先を書き間違える，操作ボタンを間違えて押すなどの人間のオペレーションによって情報漏えいした場合

- 紛失・置忘れ

  持ち出し許可を得た情報を，持ち出した先や移動中に置き忘れる，紛失など個人の管理ミスによって発生した場合

- 不正アクセス

  外部の第三者が，主にネットワークを経由して不正にアクセスを行って情報が漏えいした場合

3. 日本の中小企業におけるセキュリティ対策

IPA の中小企業における情報セキュリティ対策の実態調査[20]による調査結果を以下に示す.

1. 企業規模が小さい企業ほど，情報漏えい等のインシデント又はその兆候を発見した場合の対応方法を規定している割合が低い傾向がある.
2. 60%以上の企業で情報セキュリティ対策が十分ではないと認識している．また，対策を向上させる為には，「従業員の情報セキュリティ意識向上」「経営者への情報セキュリティ意識向上」のような人的側面の対策が重要であると考えている.
3. 企業規模が小さいほど，社内に情報セキュリティ担当者を置いていない.
4. 企業規模が小さいほど，情報セキュリティ教育を実施していない.

3.1 IT の活用状況

全体では，「やや活用している」が最も多く 32.5%であった．企業規模に応じて若干の差はあるが，過半数近くの企業が IT の活用に積極的であった．すなわち，IT を活用する企業において，情報セキュリティの必要性を一定レベルで理解しておく必要があると考えられる.

3.2 セキュリティへの理解度の高さ

全体では，「あまりそう思わない」の回答が最も多く 34.8%，次点は「ややそう思う」で 30.1%であった．役割別の回答で見ると，経営層の回答が最も多いのは「あまりそう思わない」で 34.5%，IT または情報セキュリティ担当者の回答が最も多いのは「ややそう思う」で 35.8%，一般社員の回答が最も多いのは「あまりそう思わない」で 35.4%であった.

業種別の回答で見ると，情報通信業と金融業・保険業では「ややそう思う」の回答が最も多く，それ以外の業種では，「あまりそう思わない」の回答が最も多かった．また，「そう思う」の回答が最も多いのは情報通信業で 34.0%，次点は金融業・保険業で 17.1%，「ややそう思う」の回答が最も多いのは情報通信で 48.1%，「あまりそう思わない」の回答が最も多いのは卸売業で 43.2%，「思わない」の回答が最も多いのは農林漁業で 22.5%であった.

3.3 情報セキュリティ対策投資について

IT 投資を実施した企業の割合は，企業規模が大きいほど多い傾向があった.

IT 投資の中に情報セキュリティに関する投資が含まれる割合は，小規模企業では 77.0%，中小企業（100 人以下）では 80.4%，中小企業（101 人以上）では 86.0%となっている．企業規模に応じて若干の差はあるが，IT 投資をする企業において，情報セキュリティの必要性を一定レベルで理解している傾向にあると考えられる.

また，情報セキュリティ対策投資が IT 投資に含まれない理由として一番多いのは，小規模企業では「どこからどう始めたらよいかわからない」で 23.7%であるが，中小企業では「コストがかかり過ぎる」が 30.8%であり，企業規模による違いが見られる.

更には，セキュリティ対策の支出を「投資」とみる企業と，「費用」とみる企業では，予算の不足状況や増減計画に明確な違いがあった．「投資」とみる企業では，7 割超が必要な予算を確保できており，4 割弱が投資額を増やす計画である．一方，「費用」とみる企業では，それぞれ，4 割強，3 割弱にとどまっている.

3.4 対策の必要性を感じたきっかけ

全体では，「法令（個人情報保護法等）の制定」が最も多く 31.6%，次いで「マイナンバー制度の開始」が 24.9%，「他社のセキュリティ事故（ニュースを含む）」で 22.1%である.

企業規模別で見ると，小規模企業で最も多いのは「対策の必要性を感じたことがない」で 27.6%，中小企業（100 人以下）・中小企業（101 人以上）で最も多いのは「法令（個人情報保護法等）の制定」であった．

3.5 サイバー保険の加入率

全体では,「内容を知らないし加入していない」の回答が最も多く 61.4%，次点は「内容を知っているが加入する予定がない」で 15.8%であった．

業種別の回答で見ると，金融業・保険業では「加入している」が最も多く 9.0%，情報通信業では「検討しているが加入していない」の回答が最も多く 28.3%，他の業種では，「内容を知らないし加入していない」の回答が最も多かった．「内容を知らないし加入していない」の回答が最も多いのは農林漁業で 70.4%であった．

3.6 サイバー保険の加入率が低い理由

IPA の中小企業における情報セキュリティ対策の実態調査[20]と KPMG コンサルティング株式会社のサイバーセキュリティサーベイ 2017[21]によるサイバー保険に加入しない理由の上位を以下に示す．

- 認知度が低い
- 費用対効果が見えない
- コストがかかり過ぎる
- どこからどう対策を始めたらよいかわからない
- 情報漏えいの可能性を感じていない
- 知見のある実務担当者が足りない
- セキュリティ対策費用を確保できていない

仮に認知度が高かった場合，サイバー保険の普及・発展にどう影響しているか海外を例に調査・提案を行う．

4. 他国のセキュリティ対策

4.1 米国

4.1.1 個人情報保護法制

米国連邦政府では 1974 年の情報公開法（Freedom of Information Act）成立以来，個人情報保護を包括的な法律で扱うのではなく，電子メールやインターネットなどの情報技術の進歩とテロリズムなどの時代の要請に対応する形で，医療や金融などセクター毎に個別の法律を立法している[7].

4.1.2 市場規模

1997 年，世界で最初に，AIG 社がサイバー保険の取り扱いを開始した. 情報セキュリティ保険の商品としては，AIG の net Advantage，CAN Pro の CAN Net Protect，Chubb の Cyber Security など，さまざまな種類がある．2016 年に市場規模が 13 億ドルに達し，そのうち最大手は AIG で，市場の 7 割を占めている[8].

Allied Market Research が発行する Cyber Insurance Market Report[9]によると，北米はサイバー保険市場を支配し，2015 年にはサイバー保険市場全体の約 87%を占めている．米国のいくつかの州ではサイバーセキュリティに関する法律が制定されており，サイバー賠償責任保険の普及率が高まっている．

4.1.3 市場動向

企業規模別では，小規模企業に比べ，中規模・大企業の方がサイバーインシデントに伴う潜在的なコストに対するリスク意識が高い．IPA の報告書「企業におけるサイバーリスク管理の実態調査 2015」[10]により，役員などの企業のトップ層が積極的にサイバーリスク対策に取り組んでいる企業のサイバー保険への加入率が高いことが示された．結果を図 2 に示す．

	実施している企業のIT関連保険加入率		実施していない企業のIT関連保険加入率	全体平均
経営リスクの分析	30.5% (n=607)	4.4倍	7.0% (n=963)	16.1% (n=1,570)
リスク管理担当役員(*3)の任命	33.0% (n=485)	4.2倍	7.9% (n=1,182)	15.2% (n=1,667)
役員間でリスクに関する情報を共有	20.7% (n=1,022)	3.2倍	6.5% (n=556)	15.7% (n=1,578)
ISMSの取得	39.0% (n=349)	4.4倍	8.9% (n=1,249)	15.5% (n=1,598)

図 2　組織的対策の有無と IT 関連保険加入率

また，業界別では，保険ブローカー及びリスク管理サービス大手 Marsh 社が主に米国の自社顧客に対して行った調査によると，2015 年時点でヘルスケアや教育分野の企業の加入率が，他業界と比較して，40%～50%と高率になっていることを図 3 に示す．

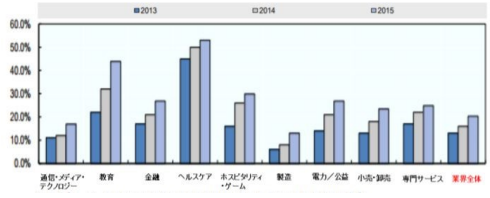

図 3　米国におけるサイバー保険の業界別普及率の推移

米国のヘルスケア業界での普及率が高い理由として，医療機関で取り扱われている情報がサイバー犯罪者にとって格好の標的になりうることが挙げられる．患者の個人情報や医療情報等の多くの情報はアンダーグラウンド市場で売買，情報を悪用すれば詐欺行為も行える．2018 年に国内の医療機関において様々なセキュリティインシデントが発生しており，対策の強化が求められている[11].

4.2 EU

ドイツ，イギリス，フランス，オランダ，スペイン，ベルギー，オーストリア，およびデンマークの 8 ヶ国に，保険会社が共同でテロリスクの一部あるいはすべてを引き受ける仕組み（テロ保険制度）が存在している．2016 年に市場規模が 5 億ドルに拡大した．

4.2.1 個人情報保護法制

2018 年 5 月に，EU 一般データ保護規制(GDPR：General Data Protection Regulation)が施行された．1995 年に，EU データ保護指令が策定されていたが，それに代わり，EU 加盟諸国に対して直接効力が発生する，より厳格な法規制として発行された．GDPR の対象となる企業は「データ管理業者」と「データ処理業者」の 2 種類に分かれる．データ管理業者とは，個人データを処理する目的や方法を決定する企業を指す．データ処理業者とは，データ管理業者の代理で個人データを処理する企業を指す．GDPR は，EU 市民，EU 市民以外で EU 諸国内に居住する人々，さらには EU 諸国を訪れている観光客など，EU のあらゆるデータ主体に適用される．また，EU データ主体の個人データを処理または監視する企業であれば，拠点が EU 諸国外であっても適用される．

違反した場合は最大でその企業の全世界での年間売上高の 4%または 2000 万ユーロ（約 2200 万ドル）のいずれか高いほうを制裁金として支払わなければならない．

4.2.1.1 英国

2015 年までは，企業のサイバーセキュリティ対策は企業の自主性に任せていた．情報共有に関しても各政府機関と企業が独自に行っていた．しかし，「国家サイバーセキュリティ戦略 2016-2021」により，サイバーセキュリティ関連機能を GCHQ 内の NCSC（National Cyber Security Center）に集中させる方針が打ち出され，大幅な政策変更が行われた．2018 年 1 月 28 日，英国政府は重要インフラ事業者に対して，効果的なサイバーセキュリティ対策を怠った場合，最大 1700 万ポンド（約 2100 万ドル）以下の制裁金を科すことがあると発表した[12]．業界専門の規制当局が任命され，重要インフラが保護されているかを評価し，指摘する体制となった．

市場規模は，2016 年末の時点でおよそ 1 億ポンド(約 1.2 億ドル)に達した．

4.2.1.2 フランス

GDPR の適用開始後，CNIL に対して 1 日平均 7 件，合計 600 件（1,500 万人分）以上の違反通知があり，3,767 件の個人による苦情申し立て（前年同期比 64%増）があった．

4.2.1.3 ドイツ

ドイツ連邦政府は 2018 年 8 月 29 日，サイバーセキュリティ機関を新設．この新機関の設立により，サイバーセキュリティ分野での野心的な研究とイノベーションのプロジェクトを促進し，資金を提供する．同機関は，アイデア段階から製品化までの研究プロセス全体を対象に支援を行う．これによって，以前よりも実用化までの時間を大幅に短縮する．同機関は 14 人でスタートし，その後，100 人規模まで拡充する予定である．

5. 各国の GDPR 対応状況

Media Pro の調査によれば，米国企業の 54%が GDPR への対応を最優先事項だとしているにもかかわらず，米国企業勤務者の 59%が GDPR について初めて聞いたと回答した．業種別に見ると，GDPR について初めて聞いたと回答したのは，金融業界で 52%，テクノロジー業界で 42%，ヘルスケア業界で 53%，サービス業界で 56%，小売業界で 65%，教育業界で 78%，公務員で 70%，その他で 69%であった．調査の結果，GDPR に向けてプライバシーと個人情報の取り扱いについて教育を行い，企業の文化と意識を変革する必要があることが明らかになった[13].

また，PwC Global が欧州の GDPR の対応状況に関する調査結果を発表した[14]. この調査レポートは，欧州でビジネスを展開している米国，英国，日本の各企業，約 300 社の最高プライバシー責任者（CPO）や最高情報責任者（CIO），プライバシーリスクを担当する役職員からの回答をもとに構成されている．米国，英国，日本の各企業の GDPR 対応状況を図 4 に示す．

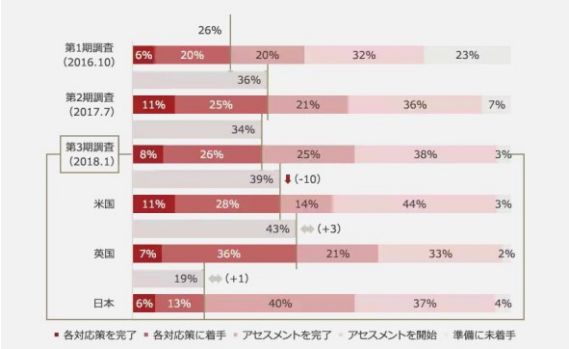

図 4　英米日の各企業の GDPR 対策状況

日本では 13%が各対応策に着手，6%が終了していると回答．また米国では，4 分の 1 以上（28%）が各対応策に着手，さらに 10 人中 1 人が作業を終了したと回答，英国では，3 分の 1 以上が各対応策に着手し，7%が終了したと回答．この結果から，GDPR 対応状況の低さがうかがえる．

そして，米英と日本との違いが明確に表れたのは，

「GDPR の施行後，監督当局は GDPR の制裁措置をいつから開始すると思うか」という質問に対する回答であった．結果を図 5 に示す．

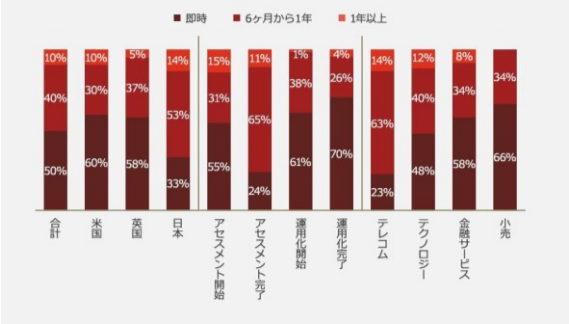

図 5　制裁措置の開始に対する各国の考え

当局による制裁措置の発動のタイミングについて，米国と英国は 6 割が即時に発動されると考えているのに対し，日本で同じように考えている企業は 3 割強に過ぎず，米英の半分という結果となった．日本の半分以上の企業は，6 カ月から 1 年以内で，当局による制裁が行われると考えている．

また，アセスメントが完了したとする企業のうち，62%の企業が 100 万ドル（約 1 億 1200 万円）以上，26%が 500 万ドル(約 5 億 6000 万円)以上の投資を見込んでおり，運用具体化が完了したと回答した企業のうち，88%の企業が 100 万ドル以上を，59%の企業が 500 万ドル以上の投資を予定している[15]．結果を図 6 に示す．

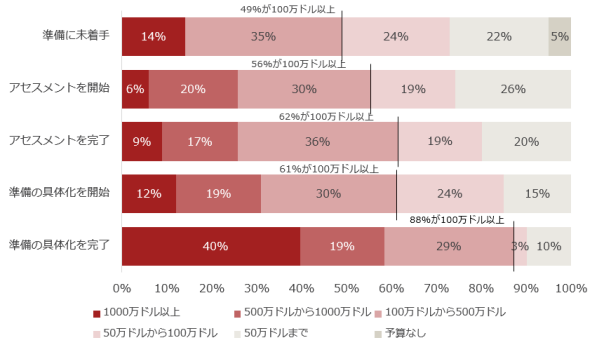

図 6　GDPR 対応に対する投資額

6. サイバー保険

サイバー保険とは，サイバー攻撃などの不正アクセスによる「個人情報漏えい」や「業務妨害」などに備えるための保険のことで，「サイバーセキュリティ保険」，「サイバーリスク保険」とも呼ばれる(以下サイバー保険に統一する)．

世界で最初にサイバー保険が発売されたのは，21 年前の 1997 年である．米国 AIG 社が最初のサイバー保険の取り扱いを開始した．その後，サイバーリスクの増加とともに市場は拡大し続け，現在では多くの保険会社がサイバー関連保険を取り扱っている．具体的な補償内容を 6.1 に示す．

6.1 補償内容

① 賠償責任に対する補償
② 行政手続きに対する補償
③ 危機管理対応のための費用に対する補償
④ コンピュータ・ネットワーク中断に対する補償

主に以上 4 点の保証を中心に補償される．追加でオプションとして担保を増やすことができる．

7. サイバー保険の給付例

サイバー保険によりカバーされた事例を紹介する．

- ターゲット社

2013 年 12 月に情報漏えいに見舞われ，POS マルウェアで 4000 万件のカード情報，7000 万件の個人情報が漏えいした．

2014 年度第四半期時点で累積 2.52 億ドルの対策コストを計上し，2015 年 3 月には集団訴訟により 12.2 億ドルの賠償金を支払うことで和解した．報道によると，2014 年年度第四半期時点で 0.9 億ドルは保険によりカバーされていると報じられており，実質的な対策費は 1.62 億ドル，対策コストの約 35.7%が保険によりカバーされていると考えられる．

- ホーム・デポ社

2014 年 9 月に 5600 万枚のカード情報が流出した．Bloom berg Business の報道によれば，対策費は 6200 万ドルになり，2700 万ドルは保険で払い戻される見通しとして，対策コストの 43.5%が保険でカバーされたと考えられる．

- ソニーピクチャーズ社

2014 年 11 月にハッキング攻撃を受け，未公開画像や従業員・有名ハリウッド女優の個人情報などが漏えいした．その想定被害額は 120 億円以上だという試算がされているが，保険により全額カバーされていると報じられた．

8. サイバー保険比較

日本では現在，6 社の損害保険会社がサイバー保険を取り扱っている．会社が違えば，補償内容や保険料等も異なる．しかし，サイバー保険は，個人情報漏えい保険を進化させたようなもので，発売されてからまだ 2 年～3 年しか経っていない．そのため，企業間による比較ではなく，サイバー保険の詳細を把握するために業界別・企業規模別・保険料金の相場を比較する．

8.1 業界別の比較

中小企業用のサイバー保険を世界で初めて作成した XL Catlin 社のサイバー保険の補償内容を例に示す[16].

表 1　業界別の補償内容例

業界	補償内容例
金融機関	データ回復費用, 事業所得の損失, ATM Web ベースのコントロール, インターバンク・メッセージング・システムおよびモバイル・バンキング・プラットフォームの追加費用
ヘルスケア	データ復旧費用, ビジネス収入の損失, インターネットおよびテレヘルスプラットフォームに接続された医療機器の追加費用
小売業者	プライバシーおよびセキュリティに対処する第三者の責任範囲, モバイル販売技術に起因する不正行為リスク, PCIDSS の罰金と費用に加え，加盟店サービス契約の違反に対する契約上の除外の例外をカバー

8.2 保険料金の相場

サイバー保険料金の相場は大きく分けて以下の 5 点で計算されることが多い[3].

1. 売上高：一般的に，売上高の高い企業ほど保有情報の価値は高まり，攻撃者にとって魅力的なターゲットになる.
2. 業種 : ソフトウェア開発などの IT 系業界は不正アクセスの対象となりやすく，保証金は上昇する．逆に不動産業や卸売業などは低く抑えられる.
3. 補償内容：被害発生時の補償金はもちろん，カバーする項目も金額に影響を与える.
4. 企業セキュリティの状況：導入している企業セキュリティの高低も，保険料に影響する．脆弱なシステムは被害発生の直接なリスクとなるからである.
5. 過去のインシデント：過去情報漏えいなどを起こしている企業は，保証金額が高くなる.

8.3 保険料の例

米国の損害保険会社を例にとり，保険料を比較した結果を表 2 に示す[17]．顧客規模は売上に応じて，区分しており小企業は 2500 万ドル以下，中企業は 2500 万～10 億ドル，大企業は 10 億ドル以上である.

表 2　サイバー保険料比較

会社名	顧客規模	保険料 (ドル)	最大補償金額(ドル)
A 社	小企業 中企業 大企業	3000 4 万 50 万	10～50 万 100～500 万 500～1500 万
B 社	中企業 大企業		100～400 万 400～1000 万
C 社	小企業 中企業 大企業	1000 5 万 変動	50 万 400 万 500～1500 万
米国平均	**小企業 中企業 大企業**	**2000 11~15 万 250 万**	**50 万 1000 万 1 億**

9. 市場動向

9.1 業界別

グローバルなサイバー保険市場を分析するために，企業の規模，職種，地理に基づいて区分した．企業は，中小企業 (250 万～9900 万ドル)，中小企業 (1 億～29 百万ドル)，中堅企業（300 億～10 億ドル），大企業（11 億ドル以上）に分類. 医療，小売，金融サービス，情報技術とサービス，その他（ユーティリティ，エネルギー，教育，政府，製造，建設，運輸）など，さまざまな業種が含まれる.

9.2 国・地域別

北米，特に米国がサイバー保険市場を支配し，欧州が続く．現在，アジア太平洋地域ではサイバー保険市場でのシェアはごくわずかであるが，大幅な成長が見込まれる．理由は，この地域の企業は，サイバー攻撃に対する保護が貧弱であるために攻撃を受けやすい傾向にあるからである．サイバー保険市場は，まだ初期段階にあるが，インドでは 2016 年に比べ，2017 年にサイバー保険の需要が 50%以上に増加した.

10. 個人情報漏えい保険との比較

10.1 損害費用例

企業がサイバー攻撃による不正アクセスを受けた際，発生した被害や想定される危険性に対応して様々な支出を求められる．不正アクセス事件が発生した際の代表的な支払項目を下記に示す.

- 情報漏えいにより発生した被害に対する法的な賠償費用
- 不正アクセスによる企業内システムの損壊及びデータ復旧に伴う費用
- 不正アクセス可能性を調査するための第三者機関への調査費用

- 訴訟対応のために必要な費用
- ネットワーク中断によるサービス停止中の費用的損害

10.2 個人情報漏えい保険

サイバー保険と個人情報漏えい保険の最大の相違点は「損害の補償範囲」である．従来型の IT 保険である個人情報漏えい保険は，何らかの攻撃や事故により発生した損失のうち「情報漏えい部分の賠償損害・費用損害」の補填に限られる．ところが，サイバー保険はネットワーク事件や事故を包括的かつ全般的に補償する．公的機関の指摘による調査費用やネットワークの中断による費用損害などの「情報漏えい以外の IT 被害部分」もカバーすることができる，カバー範囲に富んだサービスである．サイバー保険と個人情報漏えい保険の違いを表 3 に示す．

表 3　サイバー保険と個人情報漏えい保険の違い

	サイバー保険	個人情報漏えい保険
情報漏えいの損害費用	○	○
情報漏えいの賠償損害	○	○
IT 被害の損害費用	○	×
IT 被害の損害賠償	○	×
ネット中断の損害費用	○	×

11. サイバー保険の今後・課題

11.1 中小企業の保険料

中小企業の加入率の増加の主な要因は 2 つある．1 つの要因は，契約者が増加したため，サイバー保険の価格が下落していることである. Cyber Policy のレポートによると，2017 年 4 月には，補償金額が 100 万ドルの保険の毎月の保険料は平均 271 ドルであった．2018 年 6 月には，同じ保険が，補償範囲が拡大して，わずか 77 ドルで販売された．また，サイバー保険の新規契約数が，中小企業所有者の間で増加しており，過去 1 年間にわたって 1 四半期に 34%増加している．Cyber Policy の契約者は補償金額がさらに大きい保険を求めており，中小企業の 90%は補償金額が 100 万ドル～500 万ドルの保険を購入している[18][19].

もう 1 つの要因は, 契約上の義務である. 中小企業の 46%は契約上の要件がサイバー保険を購入する主な理由である.

企業は保険会社がサイバーセキュリティ侵害の責任を誰が負うかを現在よりはるかに積極的に判断するようになると考える必要がある.

11.2 日本の現状と課題

2014 年 11 月にサイバーセキュリティ基本法が国会で可決し，その後 2016 年 4 月に改正法が成立．重要インフラ事業者が情報共有を含むサイバーセキュリティ確保を促進するよう定めている．しかしながら，諸外国が整備し始めつつある「法規制による情報共有の強化」に関して日本ではいまだに整備できていない．仮に日本で，諸外国のように「セキュリティ事故検知後 72 時間以内に当局への報告」を義務付けた場合，日本ではどこに何を報告した時点で報告完了とするのかを定義する必要がある．これは，日本企業で情報漏えい等の事故が発生した場合，報告すべき公的機関等が複数あるためである[18].

諸外国のセキュリティ対策やサイバー保険の普及率より，将来的に日本でもサイバーセキュリティ事故に関する報告義務や罰則規定等の法制度の整備を検討する必要があると考える.

12. 考察

3 章の中小企業における情報セキュリティ対策の実態調査の結果より，サイバー保険の普及率の向上には，IT または情報セキュリティ担当者以外のセキュリティへの理解度の低さが関わっていることが分かった．企業規模に比例して IT 投資額が多い傾向がある一方で，IT 投資にセキュリティ対策費用が割当られておらず, 企業規模が小さいほど, そもそものセキュリティ対策の情報収集先が十分でない可能性がある.

更に，サイバー保険に加入しない理由に「サイバー保険の内容を知らないから加入していない」と回答したひとが 6 割に上った為，サイバー保険の補償内容・保険料金の相場や給付例を取り上げ比較した．それらの結果より，補償内容は，6.1 であげた 4 点を中心に補償され追加オプションで担保を増やすまたは，業界別に特化した保険で補償することができると分かった．また，保険料金の相場は，大きく分けて「売上高」「業種」「補償内容」「企業セキュリティの状況」「過去のインシデント」の 5 つが関わっていた．よって，サイバー保険を検討する上で抑えておきたいポイントであると考える.

個人情報漏えい保険との違いを知ることで，サイバー保険はネットワーク事件や事故を包括的かつ全般的に補償し，公的機関の指摘による調査費用やネットワークの中断による費用損害などの「情報漏えい以外の IT 被害部分」もカバーすることができることが分かった.

GDPR が施行されてもなお，対応状況は，日本で 19%・米国で 4 分の 1 程度の 28%・英国で 43%という現状がある．日本が圧倒的に低水準である要因は，法制に対する役職員の考え方にあると考える．当局による制裁措置の発動タイミングについて，米英は 6 割が即時に発動させると回

答したのに対し，日本で同等に考えている企業は 3 割強に過ぎず，米英の半分という結果であった．

また，GDPR 対策を維持するためのコストについて米英日の回答者の約半数が，GDPR コンプライアンス及びモニタリングに 100 万ドル以上と回答．しかし，優先投資先については，日本企業はデータライフサイクルの管理やモニタリングに対して予算を配分し，米英は，インシデント管理を優先的な投資先として考えていることが分かった．

13. まとめ

本論文は，各国の個人情報保護法制施行を受け，世界に与える影響をセキュリティ対策・サイバー保険の市場規模の観点から調査した．また，各国のサイバー保険の保険料および補償内容を比較した．これにより，日本企業におけるサイバー保険の加入しない理由の上位であった原因の対策を示せた．

諸外国との比較で，日本企業の情報セキュリティ対策への「楽観視」の実情が垣間見えた．2018 年度の情報セキュリティ投資は前年に比べ増加傾向にある．しかし，約 6 割の企業では，セキュリティ予算は決めておらず，戦力的セキュリティ投資がなされていない．その中で，サイバー保険の補償対象にならない不正アクセスによる情報漏えい以外の情報漏えいの原因である，誤操作・紛失置忘れによる漏えいに対する補償方法も整える必要があると考える．

参考文献

[1] 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”，http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf，2018 年 12 月 18 日参照．
[2] EY Japan，“EU 一般データ保護規則（GDPR）の概要と企業が対応すべき事項”，https://www.eyjapan.jp/library/issue/info-sensor/2017-02-05.html，2018 年 12 月 18 日参照．
[3] サイバー保険比較.com，“サイバー保険とは？その補償範囲や価格など徹底解説”，https://cyberhoken-jp.com/cyber-hoken/，2018 年 12 月 18 日参照．
[4] トレンドマイクロ“法人組織におけるセキュリティ実態調査”，https://www.trendmicro.com/ja_jp/about/trendpark/coretech-threatintelligence-201611-03-01.html，2018 年 12 月 18 日参照．
[5] 特定非営利活動法人日本ネットワークセキュリティ協会，“【速報版】2017 年情報セキュリティインシデントに関する調査報告書”，https://www.jnsa.org/result/incident/，2018 年 12 月 18 日参照．
[6] 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ，“情報セキュリティインシデントに関する調査報告書”，https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_attachment_ver1.0.pdf，2018 年 12 月 18 日参照．
[7] ニューヨークだより 2018 年 2 月，“米国等における個人情報保護と利活用に関する近況”，https://www.ipa.go.jp/files/000064473.pdf，2018 年 12 月 21 日参照．
[8] ニューヨークだより 2017 年 11 月，“米国におけるサイバー保険の現状”，https://www.ipa.go.jp/files/000062714.pdf，2018 年 12 月 18 日参照．
[9] Allied market research“Cyber Insurance Market to Reach $14 Billion, Globally, by 2022”，https://www.alliedmarketresearch.com/press-release/cyber-insurance-market.html，2018 年 12 月 21 日参照．
[10] 情報処理推進機構，“「企業におけるサイバーリスク管理の実態調査 2015」報告書について”，https://www.ipa.go.jp/security/fy27/reports/cyber-ins/index.html#L2，2018 年 12 月 23 日参照．
[11] トレンドマイククロセキュリティブログ，“医療機関が見落としがちなセキュリティリスクとは”，https://blog.trendmicro.co.jp/archives/19789，2018 年 12 月 18 日参照．
[12] J 一般社団法人 日本サイバーセキュリティ・イノベーション委員会 Japan Cybersecurity Innovation Committee (JCIC)，“諸外国におけるサイバーセキュリティの情報共有に関する調査”，https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf，2018 年 12 月 21 日参照．
[13] HELPNETSECURITY，“More than half of US-based employees have never heard of GDPR”，https://www.helpnetsecurity.com/2018/01/10/usa-employees-unaware-gdpr/，2018 年 12 月 21 日参照．
[14] ZDNet Japan，“日本と欧米で異なる GDPR 対応の予算規模や優先事項--PwC 調査”，https://japan.zdnet.com/article/35120591/，2018 年 12 月 18 日参照．
[15] PwC Japan グループ，“EU の General Data Protection Regulation (GDPR-一般データ保護規則)対応状況に関する調査”，https://www.pwc.com/jp/ja/knowledge/thoughtleadership/gdpr.html，2018 年 12 月 18 日参照．
[16] INSURANCE JOURNAL，“XL Catlin Introduces Cyber Insurance Endorsements for Specific Industries”，https://www.insurancejournal.com/news/national/2016/10/24/430337.htm，2018 年 12 月 18 日参照．
[17] IPA 独立行政法人 情報処理推進機構，“米国等のサイバーセキュリティに関する動向”，https://www.ipa.go.jp/files/000044581.pdf，2018 年 12 月 21 日参照．
[18] Barracuda，“サイバー保険の良い点，悪い点，および醜い点を受け入れる”，https://www.barracuda.co.jp/column/detail/961，2018 年 12 月 21 日参照．
[19] Barracuda，“Coming to Terms with the Good, Bad and Ugly of Cyber Insurance”，https://blog.barracuda.com/2018/11/09/coming-to-terms-with-the-good-bad-and-ugly-of-cyber-insurance/，2018 年 12 月 21 日参照．
[20] IPA 独立行政法人 情報処理推進機構，“2016 年度中小企業における情報セキュリティ対策の実態調査-調査報告書-”，https://www.ipa.go.jp/files/000058502.pdf，2019 年 1 月 14 日参照．
[21] KPMG コンサルティング株式会社，“サイバーセキュリティサーベイ 2017”，https://assets.kpmg.com/content/dam/kpmg/jp/pdf/jp-cyber-security-survey-2017.pdf，2019 年 1 月 28 日参照．