資料２－２

SOMPO HOLDINGS | Innovation for Wellbeing

セキュリティ対策に関する情報開示とサイバー保険について

平成30年2月1日

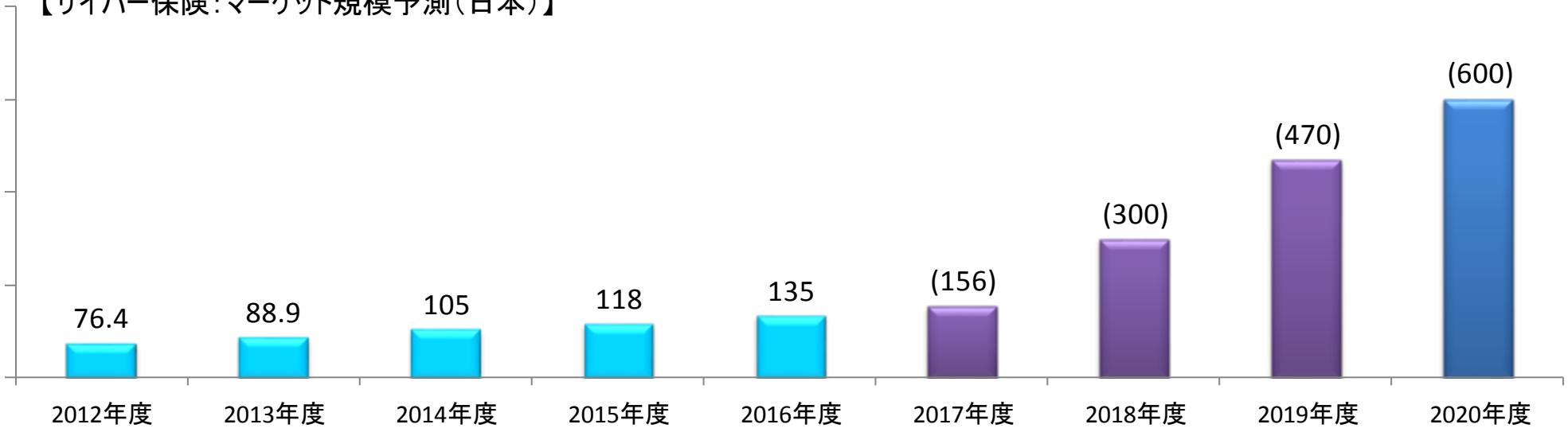
損害保険ジャパン日本興亜株式会社

サイバー保険のマーケット状況

- サイバーリスクは年々増え続けており、我が国においては2020年に東京オリパラを控え一層のリスク増加が想定される。
- それに伴いサイバー保険の需要も拡大していくことが想定され、米国と同水準の加入率となった場合、マーケット規模は約600億円になると推定される。

単位：億円

【サイバー保険：マーケット規模予測（日本）】



JNSA：2016年度 情報セキュリティ市場調査報告書

■2020年のマーケット規模
・以下のロジックに基づいて推定。
① 2020年の米国におけるサイバー保険の収保＝75億ドル（PwC予測）
② 2013年度の賠償責任保険料（米国）＝約840億ドル
③ 2013年度の賠償責任保険料（日本）＝約60億ドル
④ 2020年の日本におけるサイバー保険の収保＝①×（③÷②）≒5億ドル ⇒ 600億円（1$=120円換算）

当社サイバー保険の概要

1．サイバーセキュリティに起因して発生する損害を包括的に補償

✓ **賠償責任に関する補償**
提訴された損害賠償請求について、被保険者(補償の対象者)が負担する損害賠償金、争訟費用等の補償

✓ **事故時に急遽必要となる費用**
①損害賠償請求が発生するおそれがある場合に、その事故に対応するため被保険者が支出した各種費用の補償
②不正アクセス等の有無を判断するために支出した外部調査機関への調査依頼費用、ネットワークの遮断対応を外部委託した場合に支出する費用の補償

✓ **利益損害・営業継続費用を包括的に補償（オプション）**
ネットワークを構成するIT機器等が機能停止することによって生じた①利益損害、②営業継続費用の補償

2．付帯サービスの充実（緊急時サポート総合サービス）

✓ 事故発生時には、平時の業務を行いつつスピーディーに緊急時対応の体制に移行することが求められるが、実際に必要となる対応を自らで判断し手配できる企業は少ない

✓ 緊急時サポート総合サービスでは、事故時に必要となるサポート機能をワンストップで対応可能なサービスを提供している

✓ 上記に係る費用は保険金でお支払い

事故時の各種サポート機能と提携会社

調査・応急対応支援機能	緊急時広報支援機能		コールセンター支援機能	信頼回復支援機能	コーディネーション機能	ファイナンス機能
事故判定 原因究明・影響範囲調査支援 被害拡大防止ｱﾄﾞﾊﾞｲｽ	記者会見実施支援 報道発表資料のチェックや助言 新聞社告支援 など	SNS炎上対応支援 （公式ｱｶｳﾝﾄ対応ｻﾎﾟｰﾄ） WEBﾓﾆﾀﾘﾝｸﾞ・緊急通知（ｽﾎﾟｯﾄ対応）	コールセンター立上げ コールセンター運用 コールセンターのクロージング支援 など	再発防止策の実施状況について証明書を発行 格付機関として結果公表を支援　など	必要となる各種サポート機能の調整 法令対応等について協力弁護士事務所を紹介　など	事故受付＆緊急時サポート総合サービスの利用連絡 保険金支払い
㈱ラック AOSリーガルテック㈱	㈱ブラップジャパン ウエーバー・シャンドウィック ワールドワイド㈱	㈱エルテス	㈱ベルシステム24	㈱アイ・エス・レーティング	SOMPO リスケアマネジメント㈱	損害保険ジャパン日本興亜㈱

当社の取り組み　企業のセキュリティ対策と連動した保険制度①

情報セキュリティ認証制度（ISMS認証制度、プライバシーマーク）

認証制度の取得により企業のセキュリティ水準が上がることで、サイバー保険の保険料水準を下げることに繋がる。

- 情報セキュリティ認証を取得している事実をもって、一定以上の水準でセキュリティ対策がなされていると判断
- 認証制度の内容に応じて保険料割引と保険料算出に係る手続きの簡素化を実施
- 保険料割引がインセンティブとなり認証制度の普及が促進され、認証制度の普及により企業のセキュリティ水準が向上する好循環を実現

認証制度	ＩＳＭＳ認証	プライバシーマーク
主な取得企業	大企業・中堅企業	中堅企業
企業数	約５０００社	約１５０００社
保険料割引	６０％	３５％
事務手続き	告知書簡素化	告知書簡素化

当社の取り組み　企業のセキュリティ対策と連動した保険制度②

SECURITY　ACTION（セキュリティ対策自己宣言）

セキュリティ対策の取組みを競争力に繋げるためには、様々なステークホルダーに情報発信し評価されることが重要。
当社はSECURITY ACTION普及賛同企業として以下の支援策を実施している。

- 「5分で出来る　情報セキュリティに関する自己診断」を実施し二つ星を取得した企業に対し、最大30%の割引を提供
- 第二者開示に活用できる専用の保険付保証明書を提供

SECURITY ACTION ★
セキュリティ対策自己宣言

SECURITY ACTION ★★
セキュリティ対策自己宣言

《第二者開示》
- ✓ 取引先からの評価
- ✓ 顧客からの評価
- ✓ 株主からの評価
- ✓ 同業者の意識喚起

- ✓ 保険料の割引
- ✓ 付保証明書の提供

- ✓ 自社診断の実施
- ✓ セキュリティポリシーの公開

情報セキュリティ5か条

①OSやソフトウェアは常に最新の状態にしよう！
②ウィルス対策ソフト導入しよう！
③パスワードを強化しよう！
④共有設定を見直そう！
⑤脅威や攻撃の手口を知ろう！

- ✓ 「情報セキュリティ5か条」に取組む

サイバーセキュリティの普及に向けた課題　これまでの取組みを通じての示唆

1. 意識醸成の必要性

◆ 企業内の専門人材以外の知識不足、理解不足

企業においてはシステム担当等の専門人材以外はサイバーセキュリティについての知識が乏しいため、サイバーリスクと対策の必要性が認識されていない。保険担当は総務担当であることが多く、リスクを認識しているシステム担当と認識が共有されない結果、保険加入の検討が進まないケースが多い。
✓ 専門人材向けではない、企業の全従業員を対象としたレベルの資格制度等があるとよいのではないか。
✓ また、サイバー攻撃をわかりやすく可視化するツールや、脆弱性を示すツールの開発も有効ではないか。

経営層（意思決定層）の知識や認識が不足しており、保険加入の社内稟議が通らないケースも多い。
✓ 情報開示を通じて社内外での対話の進展のより経営層の認識・理解に繋がるのではないか。

◆ 企業間、業界間での情報共有の必要性

認証制度と連動した取組み等も、企業間、業界間で情報共有がなされない結果、一部の意識の高い企業を中心とした限定的な普及に留まってしまう。
✓ 情報開示により意識の高い企業の対策が共有されることで、他の企業の意識啓発が進むのではないか。
✓ また、情報開示のベストプラクティスの提示や、表彰制度等により、普及や保険への関心が進むのではないか。

2. 最適なセキュリティ対策の基準の必要性

◆ サイバーセキュリティ対策の水準が不明瞭

サイバーセキュリティ対策の必要性を認識しても、対策として何をどのレベルまで行えばよいかの基準が不明瞭であることが、企業のサイバーセキュリティへの積極的な投資を妨げている。
✓ サイバーセキュリティ対策のベストプラクティスの提示等により、セキュリティ対策のベンチマークを示すことが必要ではないか。

セキュリティ対策に関する情報開示について　～情報開示と保険～

第二者開示と第三者開示の整理

・第二者開示：特定顧客との間で行われる情報開示　（例：融資の信用調査（銀行）、保険加入時の告知（損保、生保）　等）

・第三者開示：公表し第三者に向けて行われる情報開示　（例：各種ディスクロージャー、取得した認証の公表　等）

保険料の算出と割引の考え方

・当社では、サイバー保険の保険料算出にあたり、企業の売上高と業種により基礎となる保険料率を算出した上で、告知書にて企業毎のセキュリティレベルを確認している。（第二者開示による確認）

・告知書はサイバーセキュリティに関する以下の6カテゴリーからなる項目について申告いただくもの。申告いただく内容は定量面（売上高、営業利益等）と定性面（組織体制、セキュリティ状況等）から構成。

・申告内容から、セキュリティ対策が進んでおりサイバー攻撃により損害が発生するリスクが低いと判断することができれば、保険料を割引を適用。

【告知書の構成】
①組織的安全管理　②契約・監督　③通信・システム　④開発・保守、アクセス制御管理措置　⑤技術的安全管理措置　⑥その他

情報開示と連動した保険料割引制度の検討

・サイバーセキュリティに関する情報開示は粒度によってはサイバー攻撃の誘発になりかねず、定量面の情報については割引適用可否を判断できるほどの粒度での開示を求めることは難しい。

・告知項目のうち以下のような定性面の項目についての詳細を開示・公表している企業に対して割引を提供する。

組織的安全管理	契約・監督	その他
➢ 派遣先を含む従業員との情報セキュリティに関する就業上の義務 ➢ 従業員への情報セキュリティに関する教育体制 ➢ セキュリティポリシー ➢ CISOの設置有無等サイバーセキュリティ体制について	➢ サプライチェーンのサイバーセキュリティ対策管理	➢ 情報セキュリティに関する認証取得有無

セキュリティ対策に関する情報開示について　～その他～

	特徴	活用案
第二者開示	✓ 当事者間のため詳細まで開示することが可能 ✓ 広く開示されないため攻撃を誘発しにくい	✓ 委託契約書でセキュリティ対策を要件化する
第三者開示	✓ 経営者の目に触れやすいため意識醸成に効果的 ✓ 他企業の意識啓発にも繋がる ✓ 投資家や消費者からの評価に影響	✓ セキュリティ対策についての情報等、詳細が開示できないものについて格付け、認証で示すことが可能 ✓ 開示内容に応じ有事の際に取組みを公表（しっかりと取組まれていれば救済）