資料２－３

サイバーセキュリティタスクフォース
情報開示分科会（第２回）プレゼンテーション資料

2018年2月1日

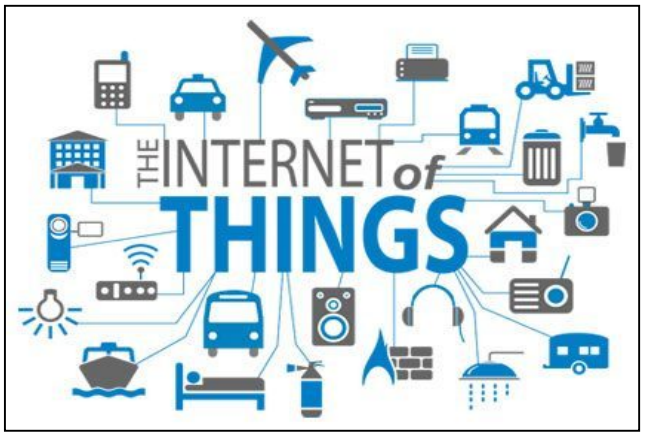
To Be a Good Company

TOKIO MARINE NICHIDO

東京海上日動

保険会社にとってのサイバーリスクの考え方

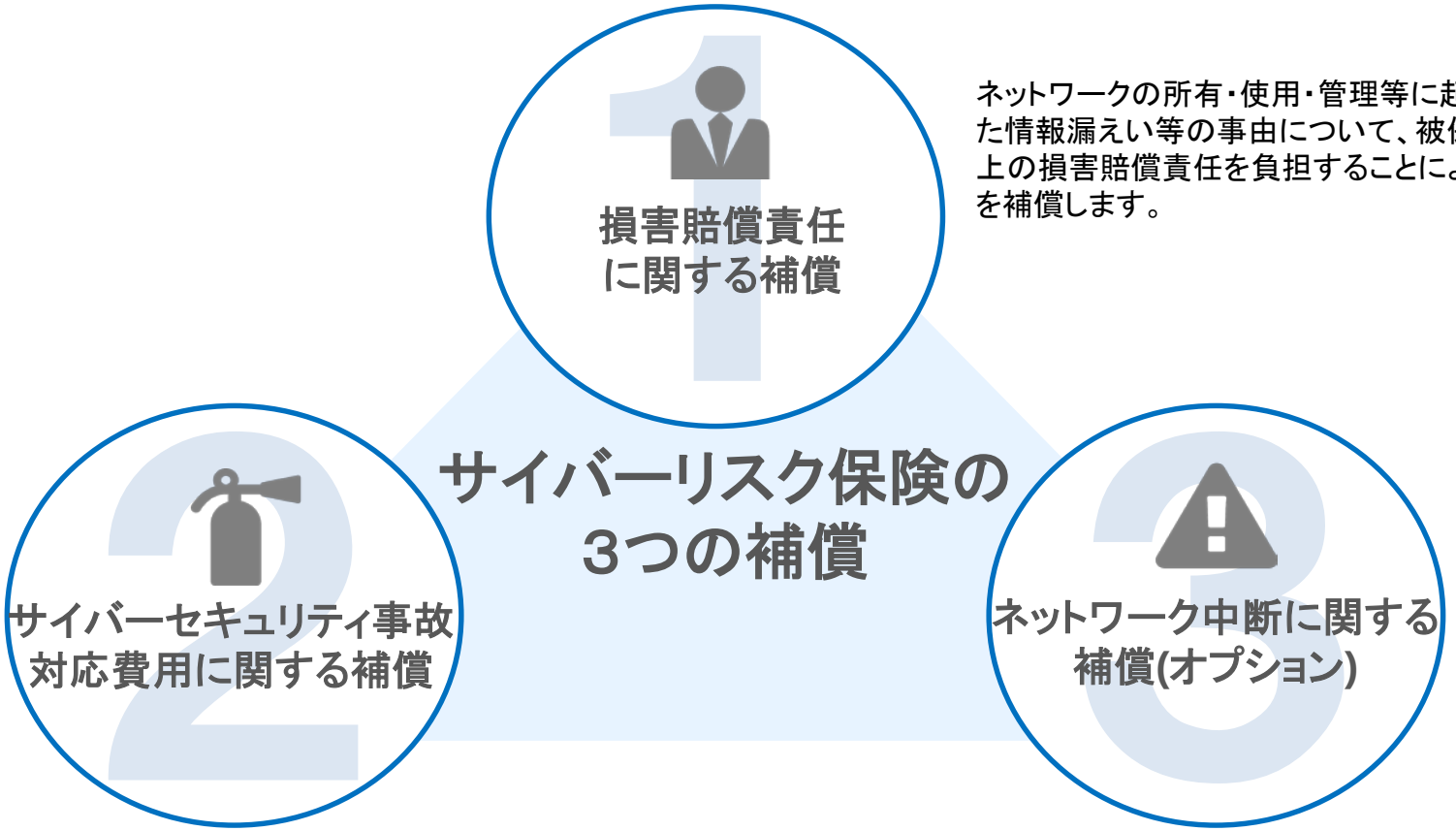
サイバーリスクの難しさ ① データ収集が困難（表に出ない、変化しているなど）
② リスクが集積する（同時多発攻撃など）
③ リスク因子が多様（技術的要因、人的要因など）



TOKIO MARINE NICHIDO

サイバーリスク保険の3つの補償

サイバーリスク保険は、セキュリティ事故に起因して発生した各種損害を1つの保険で包括的に補償します。



ネットワークの所有・使用・管理等に起因して発生した情報漏えい等の事由について、被保険者が法律上の損害賠償責任を負担することによって被る損害を補償します。

情報漏えい、不正アクセス等に起因して一定期間内に生じた危機管理対応費用、訴訟対応費用を被保険者が負担することによって被る損害を補償します。

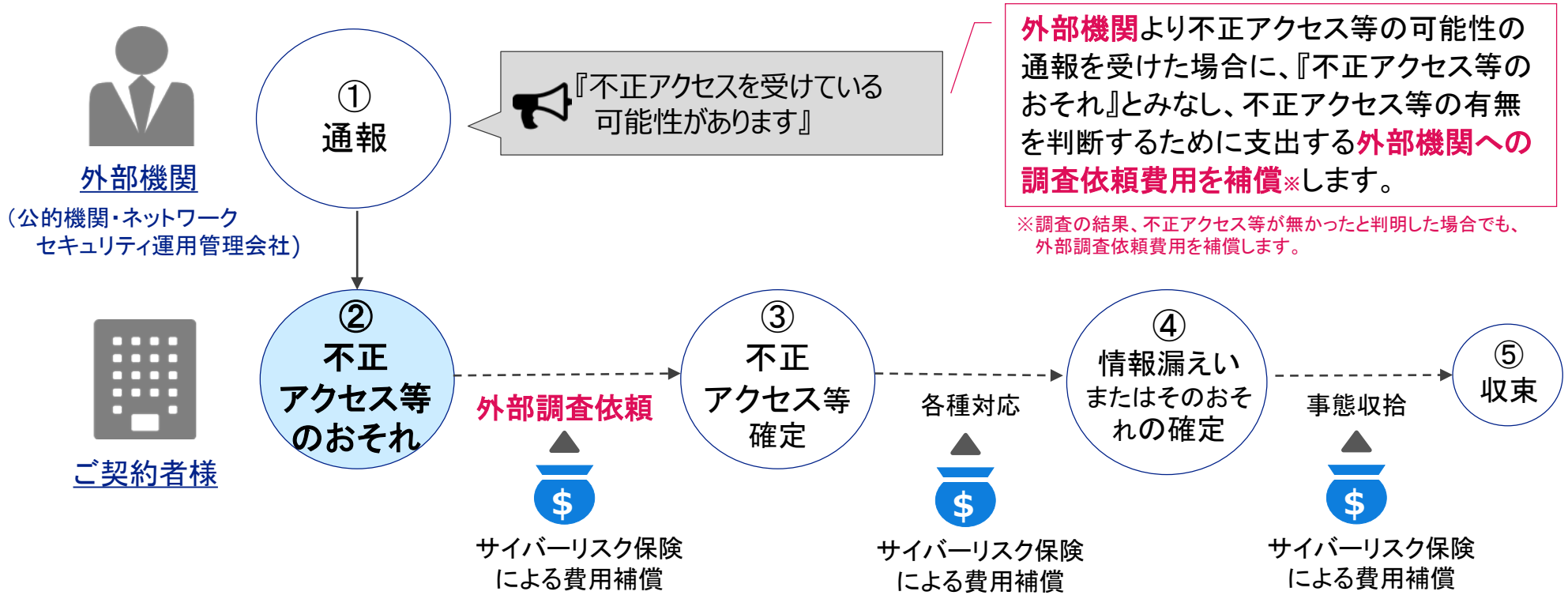
不測かつ突発的な事由に起因して、ネットワークを構成するIT機器等が機能停止することによって生じた被保険者の ①利益損害、②営業継続費用を補償します。

TOKIO MARINE NICHIDO

サイバーリスク保険の特長

不正アクセス等が確定する前の、『不正アクセス等のおそれ』が発見された時の外部機関への調査依頼費用も補償の対象となります。

事故発生から収束までの一般的な対応フロー



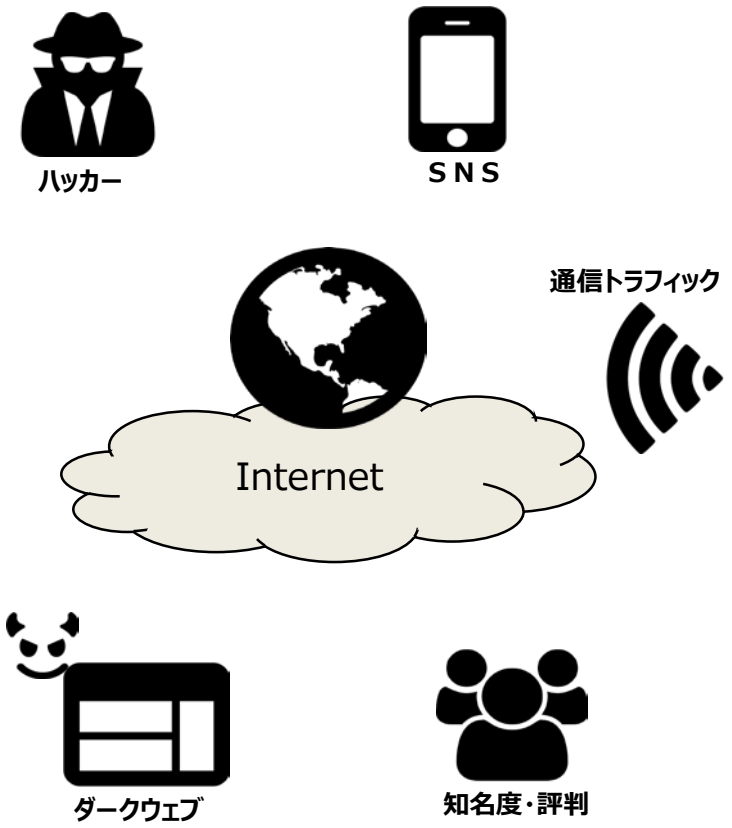
期待効果

外部調査依頼費用を保険金で賄うことで、早期に十分な調査ができ、被害拡散防止も期待できます。

「ベンチマークレポートサービス」とは

デジタルビジネスの進化により企業はネットワーク内外に様々な潜在的サイバーリスクを抱えています。

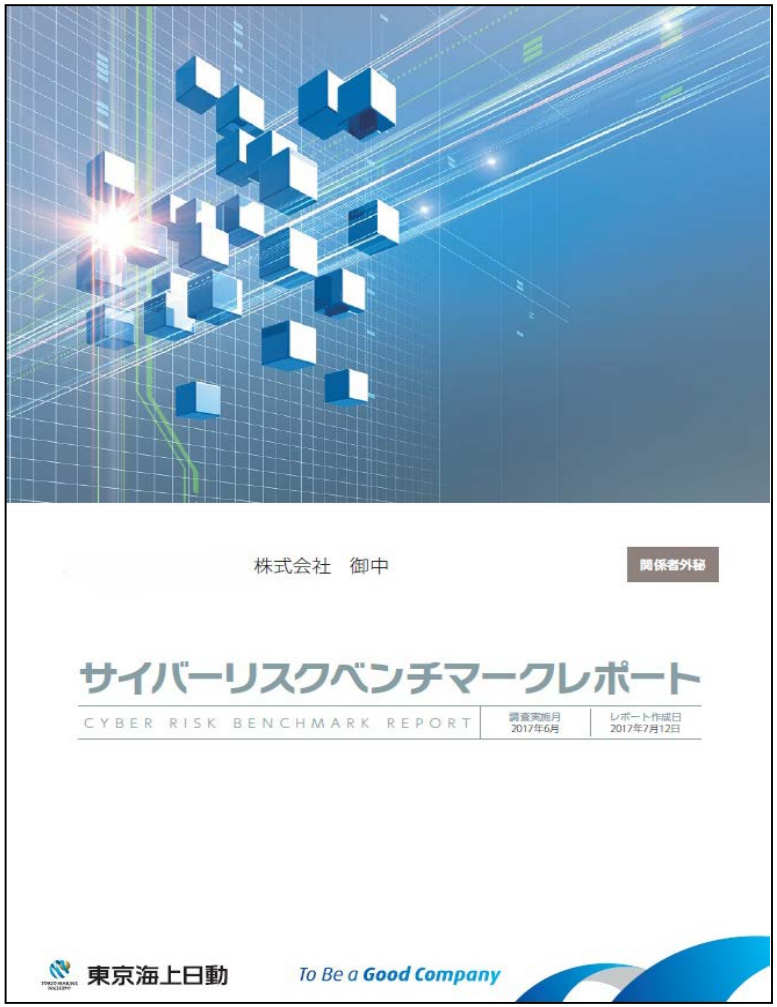
企業ネットワーク外



企業内ネットワーク内

「ベンチマークレポートサービス」とは

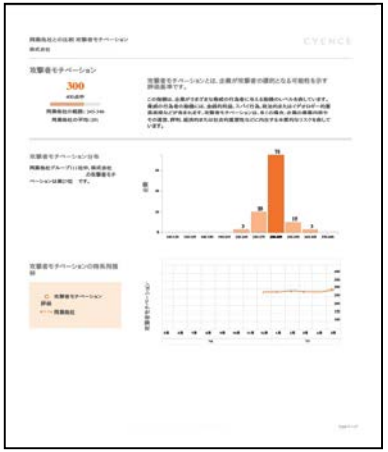
サイバーリスク保険のご契約者様に限り、「サイバーリスクベンチマークレポート」をご提供いたします。



ベンチマークレポートサービスとは、米国サイエンス社（※）のノウハウを活用し、インターネット上で取得できる客観的なデータに基づいて、

①企業のネットワークへの侵入しやすさを表す技術的指標
②攻撃者の標的となる可能性を表す人的リスク指標

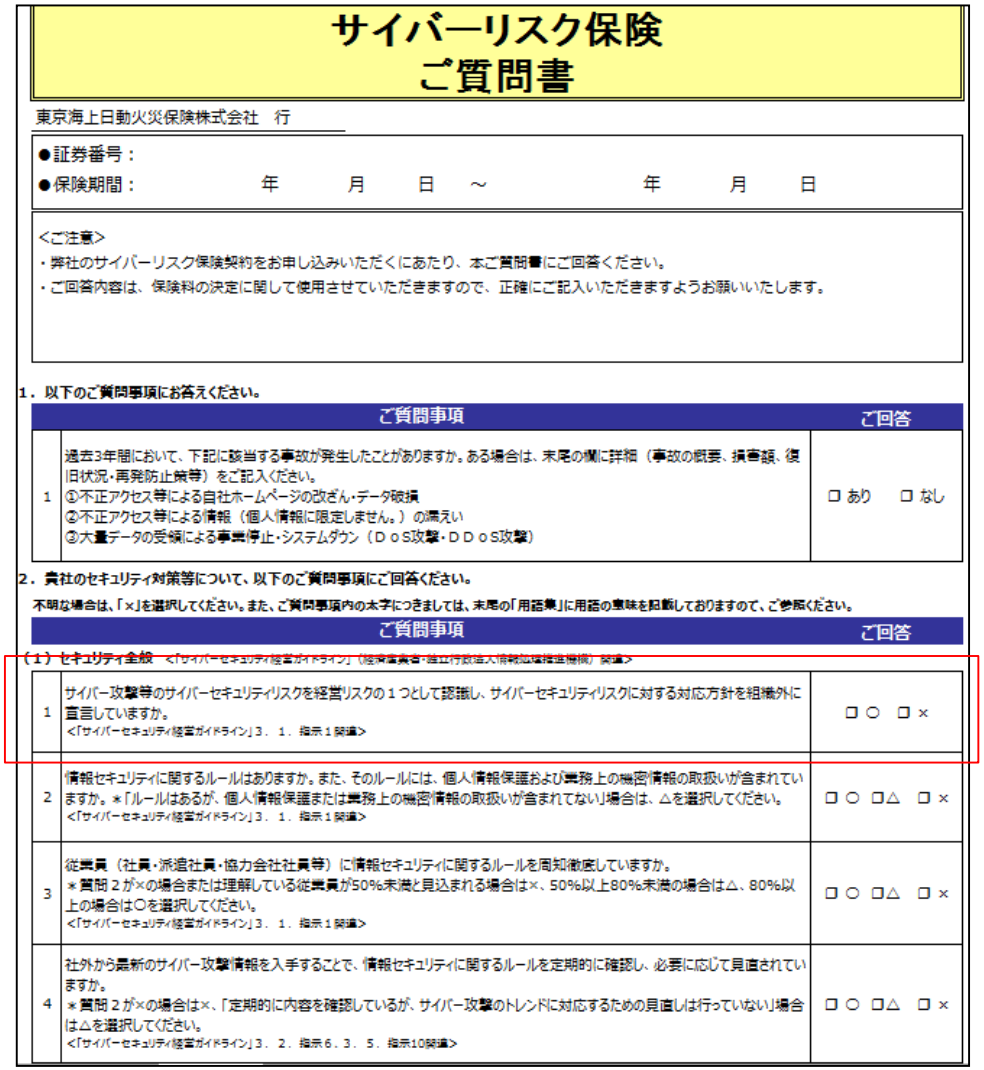
をスコアリングすることで、企業のサイバーリスクを同業他社と比較したり、毎年の推移を定点観測できる「サイバーリスクベンチマークレポート」をご提供するサービスです。



（※）サイエンス社とは

米国シリコンバレーを拠点とするサイバーリスク分析プロバイダーで、サイバーリスクに関するデータ収集やリスク分析およびリスクモデルの構築に高い専門性を有しております。同社は変化し続けるサイバーリスクのデータを独自の手法で継続的に収集し、分析することにより、サイバーリスク固有のモデルを構築しています。

リスク評価割引について



サイバーリスク保険
ご質問書

東京海上日動火災保険株式会社　行

●証券番号：
●保険期間：　　年　　月　　日　～　　年　　月　　日

<ご注意>
・弊社のサイバーリスク保険契約をお申し込みいただくにあたり、本ご質問書にご回答ください。
・ご回答内容は、保険料の決定に関して使用させていただきますので、正確にご記入いただきますようお願いいたします。

1．以下のご質問事項にお答えください。

	ご質問事項	ご回答
1	過去3年間において、下記に該当する事故が発生したことがありますか。ある場合は、末尾の欄に詳細（事故の概要、損害額、復旧状況・再発防止策等）をご記入ください。 ①不正アクセス等による自社ホームページの改ざん・データ破損 ②不正アクセス等による情報（個人情報に限定しません。）の漏えい ③大量データの受領による事業停止・システムダウン（ＤｏＳ攻撃・ＤＤｏＳ攻撃）	□ あり　□ なし

2．貴社のセキュリティ対策等について、以下のご質問事項にご回答ください。
不明な場合は、「×」を選択してください。また、ご質問事項内の太字につきましては、末尾の「用語集」に用語の意味を記載しておりますので、ご参照ください。

	ご質問事項	ご回答
	（１）セキュリティ全般　<「サイバーセキュリティ経営ガイドライン」（経営者責者・独立行政法人情報処理推進機構）関連>	
1	サイバー攻撃等のサイバーセキュリティリスクを経営リスクの１つとして認識し、サイバーセキュリティリスクに対する対応方針を組織外に宣言していますか。 <「サイバーセキュリティ経営ガイドライン」３．１．指示１関連>	□ ○　□ ×
2	情報セキュリティに関するルールはありますか。また、そのルールには、個人情報保護および業務上の機密情報の取扱いが含まれていますか。＊「ルールはあるが、個人情報保護または業務上の機密情報の取扱いが含まれてない」場合は、△を選択してください。 <「サイバーセキュリティ経営ガイドライン」３．１．指示１関連>	□ ○　□△　□ ×
3	従業員（社員・派遣社員・協力会社社員等）に情報セキュリティに関するルールを周知徹底していますか。 ＊質問２が×の場合または理解している従業員が50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 <「サイバーセキュリティ経営ガイドライン」３．１．指示１関連>	□ ○　□△　□ ×
4	社外から最新のサイバー攻撃情報を入手することで、情報セキュリティに関するルールを定期的に確認し、必要に応じて見直されていますか。 ＊質問２が×の場合は×、「定期的に内容を確認しているが、サイバー攻撃のトレンドに対応するための見直しは行っていない」場合は△を選択してください。 <「サイバーセキュリティ経営ガイドライン」３．２．指示６．３．５．指示10関連>	□ ○　□△　□ ×

【概要】
- ご契約時に「ご質問書」の取付け（必須）
- 回答内容にしたがい、最大30%の割引が可能

【特徴】
- 6つのカテゴリー、36問のご質問
- 「セキュリティ経営ガイドライン」、「SECURITY　ACTION」の内容にも準拠
- 「情報開示」についても評価項目の一つとして参入

【運用上の課題】
- 大企業、中堅企業、中小企業の受止め方
- リスク実態との乖離

サイバーリスク保険の普及にあたっての課題

【事業者の状況】
- セキュリティ対策が十分に行き届いていない（中小企業）。
- インシデント被害が顕在化されていないため、保険の必要性を感じていない（特に中小企業）。
- 自社が加害者となった場合の法的責任関係が不明確。

【引受面の課題】
- 「ご質問書」のみで企業のリスク実態を見極めるのは限界がある。
- 統計的な事故データが存在していない。

【リスク管理面の課題】
- 同時多発的に発生するインシデントをどのように管理するのか。
- 物理的損壊を伴うインシデント（サイレントサイバーリスク）への対応

セキュリティ対策に係る情報開示の考え方

「情報開示」に対する保険会社の考え方

- 保険会社にとって情報開示の最大の効果は、
  - ① 企業のリスク実態が明らかになり適切なリスク評価が可能となること（割引or割増）
  - ② 情報開示により企業のセキュリティ意識が向上すること

開示が望ましい項目

- 技術的対策の状況
- 過去の事故情報、再発防止策

想定される事業者の反応

- 「対策状況を開示することで、標的となるリスクが高まるのでは」

参考資料

世界のサイバー保険市場の動向

日本のサイバーセキュリティ保険市場規模
（2017年度は予測）

出典:日本ネットワークセキュリティ協会　2016年度　情報セキュリティ市場調査

米国市場の状況

米国ではクレジットカード払いが日本よりも一般的であり、大企業から個人商店まで顧客情報の取扱量が多い。このため、情報漏えいのリスクマネジメント（カード漏洩による不正利用モニタリングを含む。）の重要性・危機意識が高い。

- **規制環境**:40以上の州において被害者保護の観点より、情報漏えい・紛失時の被害者への通知義務が義務化されており、企業が自社のリスクヘッジ手段として保険を購入することが一般的になっている。
- **市場規模**:2015年の保険市場規模は約1,500億円（弊社推定）、年率約30%のペースで拡大している。

欧州市場の状況

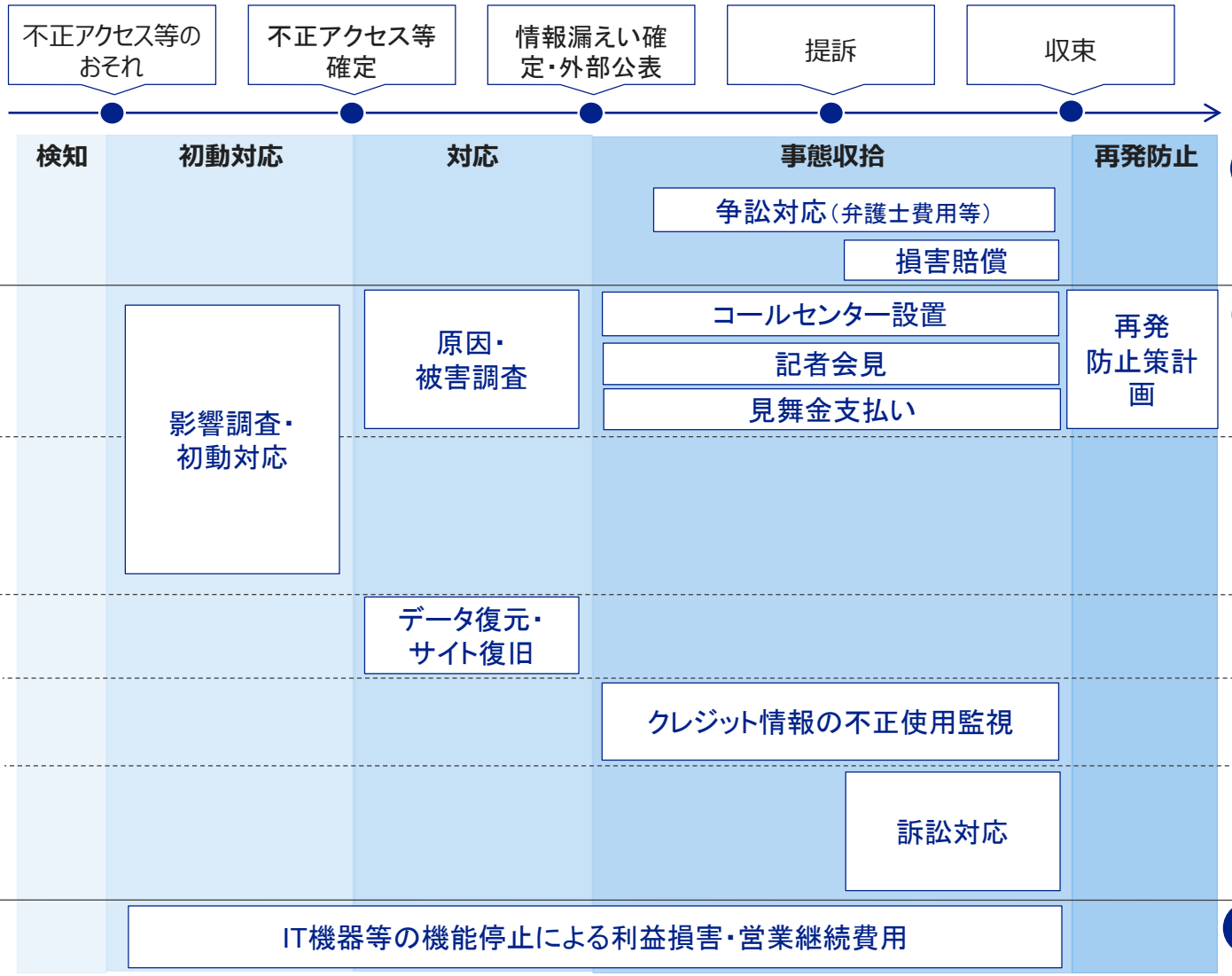
- **規制環境**:2018年5月にGDPR（一般データ保護規則）が施行される予定であり、企業の法的責任が強化されることから、今後リスクヘッジ手段として保険がより普及する可能性が高い。
- **市場規模**:2015年度の保険市場規模は約200億円（弊社推定）

日本市場の状況

- **規制環境**:情報漏えい・紛失時の被害者への通知義務は課されておらず、企業が保険を購入するインセンティブは低い。
- **市場規模**:2015年の保険市場規模は約118億円（情報セキュリティ保険合算）

サイバーリスク保険の補償概要

【ご注意】
本ページは、不正アクセス等により情報漏えいが発生し、それを外部に公表した場合の事例をもとに、サイバーリスク保険の補償概要を記載しています。



(*1) 保険契約においてお支払いする保険金の額は、すべての保険金を合算して、①損害賠償責任部分で設定された保険期間中支払限度額が限度となります。
記載の金額は設定可能な上限値を表示しています。

支払限度額*1

1 損害賠償責任に関する補償

被保険者が法律上の損害賠償責任を負担することによる損害を補償します。

最大**10億**円（1請求・保険期間中）

2 サイバーセキュリティ事故対応費用に関する補償

(a) 不正アクセス等確定後、原因調査および事態収拾に係る費用を補償します。

最大**1億**円（1事故・保険期間中）

※賠償責任の支払限度額（1請求）が1億円未満の場合は、その金額で設定

(b) 外部からの通報で不正アクセス等のおそれを検知し、不正アクセス等の有無を判断するための調査依頼費用を補償します。(縮小支払割合75%)

1,000万円（1事故・保険期間中）

※調査の結果、不正アクセス等が無かった場合は(b)の費用で補償、不正アクセス等が実際に生じていた場合は、(a)の費用で補償します。

(c) 消失したデータの復元費用、または改ざんされたウェブサイトの復旧費用を補償します。

1,000万円（1事故・保険期間中）

(d) 情報漏えいの被害者のクレジット情報について、不正使用を監視するための費用を補償します。

500万円（1事故・保険期間中）

(e) 被保険者に対して提起された損害賠償請求訴訟に対応するために必要な費用（意見書・鑑定書の作成費用等）を補償します。

1,000万円（1請求・保険期間中）

※弁護士費用等の争訟費用は「❶損害賠償責任に関する補償」で補償します。

3 ネットワーク中断に関する補償（オプション）

IT機器等が機能停止することによって生じた利益損害、営業継続費用を補償します。

（支払限度額・保険金額はご契約時に設定）

サイバーリスク総合支援サービスについて

サービス		概要	ご利用対象	提供主体
情報・ツール提供サービス（無料）	1. 情報提供サービス	サイバーリスクニュースやサイバー関連の情報誌といった情報のご提供、およびサイバーリスクセミナーを優先的にご案内いたします。	サイバーリスク保険ご契約者様限定	東京海上日動サイバーリスク情報センター
	2. ツール提供サービス	従業員の皆様を対象としたサイバーリスクに関する教育支援ツールをご提供いたします。		
ベンチマークレポートサービス（無料）	3. ベンチマークレポートサービス	米国サイエンス社のノウハウを活用し、企業がさらされているサイバーリスクの要因を様々な角度で分析し、業界内でのベンチマークや定点観測としてご利用いただけるサイバーリスクベンチマークレポートをご提供いたします。		
簡易リスク診断サービス（無料）	4. 定性リスク診断サービス	お客様のセキュリティ管理体制を簡易診断し、定性的にリスク診断を実施いたします。	どなた様でもご利用いただけます	弊社
	5. 定量リスク診断サービス	一定のシナリオに基づいたサイバーリスクに関する想定最大損害額（PML）を簡易算出し、定量的にリスク診断を実施いたします。		
専門事業者紹介サービス	6. 平時の紹介サービス	事故発生前のセキュリティコンサルティングや脆弱性診断、セキュリティログ監視等、お客様のご希望に応じた専門事業者をご紹介いたします。		東京海上日動サイバーリスク情報センター
	7. 有事の紹介サービス	事故発生時の駆けつけ支援、調査・応急対応支援、コールセンター設置支援等、お客様のご希望に応じた専門事業者をご紹介いたします。		