サイバー保険検討のススメ

独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム　８期生「経営と財務を守るサイバーリスクマネジメント」プロジェクト

改訂履歴

改訂年月日	改訂箇所	改定内容
2025年09月30日	-	初版公開

著作権

- 本資料の著作権は中核人材育成プログラム ８期生「経営と財務を守るサイバーリスクマネジメント」プロジェクトに帰属します。
- ただし、本資料に含まれる第三者の著作物・商標等は各権利者に帰属します。
- 利用に際しては著作権法で認められている範囲でご利用ください。また、引用の際には出典を明記してください。

免責事項

- 本書は単に情報として提供され、内容は予告なしに変更される場合があります。
- 本書に誤りがないことの保証は一切ないものとします。
- 本書の利用によるトラブルに対し、本書著者は一切の責任を負わないものとします。
- 本書に記載されている内容は、本プロジェクトの見解に基づいております。
  独立行政法人情報処理推進機構（IPA）および産業サイバーセキュリティセンターの意見を代表するものではありません。
- 本書の有効期限は、発行日（２０２５年９月）から１年間とします。

本書の目的

組織のサイバーレジリエンス向上のため、サイバー保険の導入検討に役立つポイントを以下の観点から整理した資料です。

1.有事における財務的なセーフティネット
2.外部専門家の活用による対応能力向上

スコープ

日本国内におけるサイバー保険の導入要否判断、補償設計・交渉、運用設計に関する検討の参考となる情報・事例をスコープとします。

✓ サイバー保険の特徴と代替手段の比較
✓ 補償範囲・付帯サービス・利用場面の整理
✓ 要否判断の観点（資金確保、被害額評価、体制・要員、ノウハウ）
✓ 補償設計・契約交渉・運用設計に関する留意点
※特定商品の優劣比較、保険料の詳細試算、海外制度の解説は対象外

対象読者

日本国内の中小～大企業における、サイバー保険の検討と運用に関与する組織横断メンバーを主対象とします。
（経営層、経営企画、財務・経理、法務、リスク管理、BCP/事業継続担当、サイバーセキュリティ、情報システム）

目次

1.はじめに

「大変申し訳ございません。今回の設備故障で発生した大損害、保険金が支払われないようです。」

経営層の皆さん、このような報告を受けるとしたらどうでしょうか。
リスク管理担当者の皆さん、このような報告を自社の経営層にしないといけないとしたらどうでしょうか。

実は、**これは現実に起こり得ます**。2017年のNotPetya攻撃では世界で約100億ドル規模の被害が発生し、既存保険契約での補償可否が大きな争点となりました[1]。その後、ロイズ市場は2022年に「国家関与型サイバー攻撃」を不担保とする条項の導入を全社に指示[2]しました。ただし対象は“国家が関与する攻撃”に限定されています。
一方、日本では国際的な動向や「サイレント・サイバー」整理を背景に、**火災・機械など従来型の保険でサイバー攻撃全般を免責とする特約**が導入されています。大手保険商品の中には「直接・間接を問わずサイバーインシデントに起因する損害は支払わない」と明記され、企業総合保険や動産総合保険でも同様の規定が広がっています。しかし、この実態は十分に知られていません。**多くの企業が「既存の保険で守られる」と誤解したまま、重大な“空白リスク”にさらされているのです。**だからこそ今、自社の補償範囲を見直し、サイバー保険の必要性を正しく理解することが不可欠です。本書が自社リスクを再評価するきっかけとなれば幸いです。

脚注（出典）
1.金 奈穂 「サイレント・サイバーリスクを巡る動向－米国・イギリスを中心に－」 損保総研レポート 第126号 2019.1
2.Lloyd’s, Market Bulletin: State backed cyber-attack exclusions (Ref: Y5381), 16 August 2022.

プロジェクトの背景

経営におけるサイバーリスクの課題：

- 経営とは、事業目的を達成するために、保有する経営資源を運用し、持続的に価値を創造し提供し続ける長期的な活動と言えます。
- 経営には経営資源が不可欠であり、重要経営資源（人、モノ、カネ、情報など）が短期的に機能しない、または不足する場合に備えBCPが策定されます。
- BCPの基本は原因事象（サイバー、自然災害、感染症など）が企業の重要経営資源に与える影響を分析し対策することです。
- **サイバーリスクを例に考えると、主にモノと情報に作用し、生産ラインの停止や、受発注ができないなどの障害を引き起こすことで、カネ（＝企業の資金繰り）に多大なインパクトを与える**と考えられます。サイバーリスクの要因となる脆弱性は、セキュリティ対策（ハード、ソフト、教育など）をすることである程度低減することはできますが、ゼロにすることはできません。むしろ、**人の悪意により日々巧妙な手法が考案され、脆弱性は増え続けている**のです。
- ここが、他の原因事象と大きく異なる点です。例えば地震リスクに対しては、「国内外含めて地震・噴火リスクの少ない場所に本社や工場などを物理的に分散すること、あるいは同一原因事象で同時被災しない場所に分散させることなどで業務が完全停止するリスクを事実上無視できるレベルまで下げることができる」とされています。
- 経営においては、**サイバーリスクをゼロにできない事実を受け入れ、どのように組織のレジリエンスを事前に構築していくかが課題**と言えるでしょう。

提案するソリューション：

- 私たちは、中核人材育成プログラムの中で 1 年間、サイバーセキュリティの専門家として技術を磨いてきました。このプロジェクトも当初は、サイバーリスクの課題に対し、組織・運用・技術の観点（ハード、ソフト、教育）からアプローチしようと考えていました。しかし、**過去事例の調査・分析を進める中で、生産ラインの停止や財務データの喪失などにより資金繰りが逼迫し倒産するケースがある**ことを知りました。
- **サイバーインシデントによる資金繰り悪化への代表的な対策は、銀行の融資枠の事前審査・予約（コミットメントライン）とサイバー保険**であることも判明しました。
- サイバー保険は様々な理由から日本ではまだ浸透していません。そこで、私たちの研究活動の副産物として、ここに**リスクファイナンスの有効な手法のひとつであるサイバー保険を企業目線から分析し、サプライチェーンへの展開の可能性を含め具体的に解説**していきたいと思います。

サイバー保険を検討する前の注意点　１／２

保険に入ってもサイバーリスクへの対応能力を獲得・維持・見直すことは依然必要

本書ではサイバー保険導入のメリットについて説明しますが、以下の点を忘れてはいけません。

いくらサイバーセキュリティ対策をしてもサイバーリスクをゼロにすることはできません。
サイバーリスクへ立ち向かうためには、**予防と事故対応の双方が不可欠**です。

【予防】
- ✓ 組織における**ビジネスリスクを認識**し、許容しないリスクを設定します。許容しないリスクを引き起こすサイバー要因（サイバーリスク）を特定し、事故対応可能か・事故対応により許容内の被害に収められるか評価します。
- ✓ 評価に応じたリスク対応として、**発生可能性の低減・引き起こされる被害の低減・被害範囲の縮小**を目的とした対策を実施します。

【事故対応】
- ✓ 事故対応では**検知・対応・復旧体制を事前に構築しておく**必要があります。
- ✓ リスクが顕在化し、インシデント発生の可能性を示すなんらかの兆候や異常を検知したら、まずは初動対応として迅速な情報収集・分析を行い、インシデントか否かの判断を行います。
- ✓ インシデントと判断した場合は直ちに封じ込めを行い、被害拡大を防止します。
- ✓ 次に影響範囲の特定を実施し、証拠保全や原因分析といったフォレンジック調査を進めます。並行して応急処置としての再発防止策を講じ、事業停止を最小限に抑えるため段階的に復旧作業を進めます。
- ✓ その後、恒久的な再発防止策を策定・根本原因を解消し、復旧を完了します。
- ✓ これらは定期的な演習を通じて**実効性ある体制・手順か確認し、見直しをする**ことが必要です。

【統制・推進】
- ✓ これらサイバーリスクへ立ち向かう一連の活動を組織として適切に統制するため、明確な責任体制や指揮命令系統・部門間のコミュニケーションを整え、経営層のリーダーシップによって継続的な推進をすることが必要です。

サイバー保険を検討する前の注意点　２／２

資金の確保という視点では、サイバー保険以外の手段もある

検討する目的によってはサイバー保険以外の手段もあります。財務・経理部門と連携し比較・ご検討ください。

選択肢	概要
コミットメントライン	コミットメントラインとは、組織が金融機関から事前に融資審査を受け、一定額まで融資を受けられる極度貸付契約を結び、緊急時にすぐに融資を受けられる枠組みです。サイバー保険は、被害発生後の損失を保険会社が補償するのに対し、コミットメントラインはあくまでも「借入」であり、後日返済が必要ですが、借り入れが発生するまで金利はかかりません。ただし、借入していない場合でも融資枠を確保している手数料は発生することがあります。
自家保険（積み立て）	自家保険は、組織が保険会社に年間保険料を支払う代わりに、自社で資金を積み立て損害リスクに備える方法です。外部の保険を利用するサイバー保険と異なり、費用を抑えられる反面、巨額の損害を被った場合は積立資金をオーバーする可能性があります。
キャプティブ保険	キャプティブ保険は、自社グループ専用に設立した保険子会社が提供する保険のことです。自社グループ全体のリスクを直接引き受け、設立時の資本や積み立てられた保険料で損害を補償します。保険子会社は、保険をセカンダリーマーケットへ再保険に出すことでリスクを低減することができます。外部の保険会社が補償を提供するサイバー保険に対して、キャプティブは主体的に運営に関与できるため、柔軟にリスクをカバーでき保険コスト最適化を期待できます。
CATボンド	CATボンドとは、Catastrophe（大規模災害）とBond（債券）を合わせた造語です。国債も債券ですが、多くの民間企業も社債という債券を発行することで金融市場から直接資金を調達することができます。CATボンドは地震や台風、サイバー攻撃など、特定の大規模災害が発生した場合に、企業が市場から調達した資金の返済を免れることを条件に債権の利回りを高く設定する特殊な社債です。返済を免れた資金は大規模災害などによる損失補填などに利用することができます。日本では東京ディズニーランドを運営するオリエンタルランドが発行したCATボンドの実例があります。

サイバー保険を検討すべき理由

＃１　有事に必要な復旧資金などを保険金として受け取ることができる
サイバーインシデントによる突発的な経済的損失が補償されることで、
事業継続を支援する財務的なセーフティネットとなるため

※保険金は後払いのため、短期的に必要となる資金は別途手当てが必要となる場合有り
※保険料（掛け金）は経費計上できるため節税効果も期待できる

＃２　充実した付帯サービスを無償で利用できる
自社の体制不足を補う形で、保険会社のネットワークを通じ
フォレンジックや法務・広報支援などの外部専門家リソースをスポットで
確保でき、サイバーインシデントへの対応能力向上を期待できるため

※無償利用可能な付帯サービスについては後述

＃１　サイバーインシデントによる突発的な経済的損失

全体の半数で1千万円以上の**突発的支出が発生。１億円以上の被害事例も。**

ランサムウェア被害の
調査・復旧等に要した総額費用

警察庁 「令和６年におけるサイバー空間をめぐる脅威の情勢等について」より
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

ランサムウェア被害事例　※左記の円グラフとは出典が異なります。

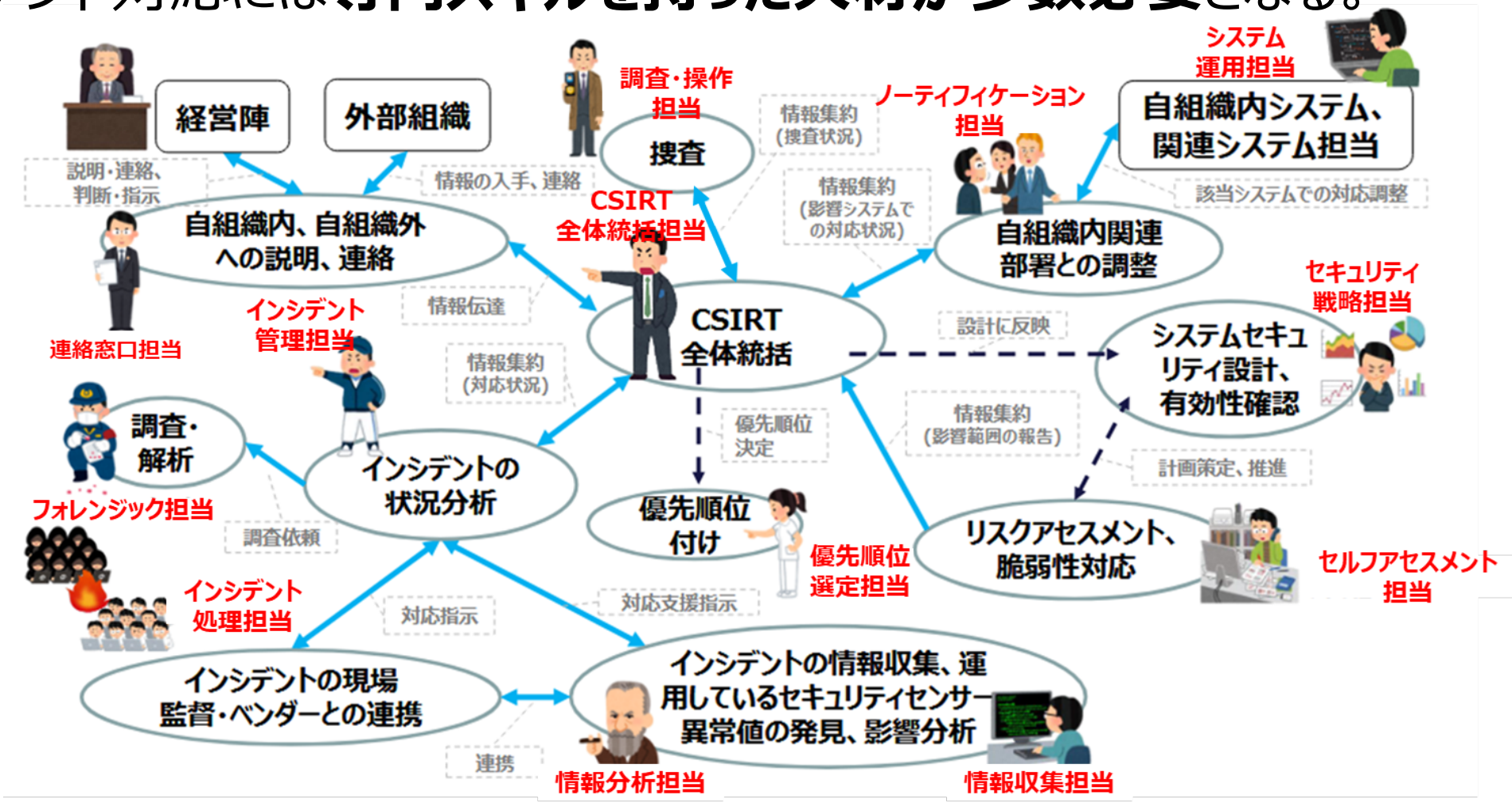
業種：製造業，従業員規模：20~999名
被害額合計：1億2,400万円
※社内システム復旧に２ヶ月を要している。逸失利益は不明。
※被害額は業種・規模・被害範囲・被害内容・復旧までの期間により異なる

損害	項目	金額	備考
費用	原因調査 被害範囲調査費用	800万円	
	法律相談費用 コンサルティング費用 ダークウェブ調査費用	1,600万円	
	詫び状送付費用 見舞い品など購入費用	4,500万円	クオカードなどの送付
	コールセンター費用	600万円	
	システム復旧費用	4,000万円	新規システム構築のコスト
	再発防止費用	900万円	・新規セキュリティ対策（EDR/MDR）の導入 ・VPN機器の保守の見直し、 AD（アクティブディレクトリ）管理の見直し

JNSA 「インシデント損害額調査レポート第2版 別紙 被害組織調査」より
https://www.jnsa.org/result/incidentdamage/data/2024-2.pdf

＃２　サイバーインシデントの対応に必要な人的リソース

インシデント対応には**専門スキルを持った人材が多数必要**となる。

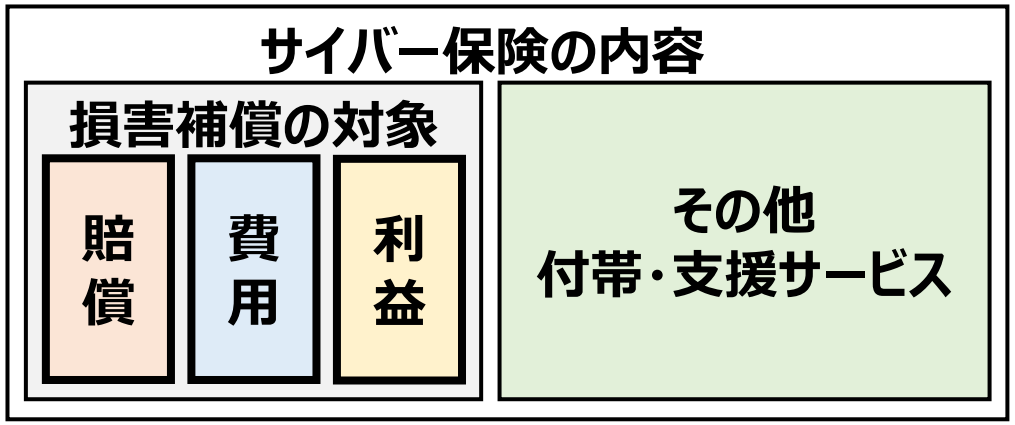


日本シーサート協議会 「CSIRT人材の定義と確保 Ver.2.1.pdf」より
https://www.nca.gr.jp/activity/PDF/recruit-hr20201211.pdf

2.サイバー保険の概要

サイバー保険の概要　１／２

損害補償だけでなく、併せて様々な**サイバーセキュリティ支援サービス**も提供



補償対象

- ✓賠償損害・費用損害・利益損害の3つ
- ✓賠償損害を基本に設計されることが多い
- ✓利益損害はオプション（特約）扱い
- ✓支援サービス費用は費用損害
  ※補償対象外となるケースもある

付帯・支援サービス（例）

インシデント時の対応サービス

- ✓緊急問い合わせ
- ✓外部専門家の紹介
  - ✓フォレンジック調査
  - ✓弁護士相談
  - ✓広報支援・コールセンター設置

インシデント対応計画とサポート

- ✓再発防止支援
- ✓リスクモニタリング
- ✓外部専門家の紹介
  - ✓セキュリティコンサルティング
  - ✓ログ診断
  - ✓脆弱性診断

※ 複数の保険会社のサイバー保険に関するパンフレット等を参考に作成しています。
保険会社により提供されるサービス内容が異なりますので、必ず保険会社へご確認ください。

サイバー保険の概要　２／２

補償額や年間保険料のレンジは保険商品により異なる

補償額

✓パッケージ商品

賠償損害上限10億円・費用損害上限5億・利益損害上限1億の補償

年間保険料：数万円～数百万円　※年間保険料は補償内容・業種・事業内容により異なる

✓オーダーメイド商品

パッケージ商品を超える補償はオーダーメイドとなり、保険料が高額になりやすい

加入条件（パッケージ商品のみ）

✓告知（売上、業種、過去数年のインシデント実績）

※ セキュリティ対策の実施状況次第で割引き・割増しもある

※ 複数の保険会社のサイバー保険に関するパンフレット等を参考に作成しています。
保険会社により提供されるサービス内容が異なりますので、必ず保険会社へご確認ください。

コラム１　サイバー保険は何が対象？何が免責？

サイバー保険はサイバーインシデントの急増・保険市場に影響を受け変化し続けている商品である。対象範囲についての理解が曖昧であり、周知も不十分と本プロジェクトを通じて感じた。ゆえに、ここで簡単に補償対象と免責事項（補償対象外）を挙げておく。

サイバー保険の補償対象は、賠償損害と費用損害と利益損害の3つである（利益損害はオプション扱いであることが多い）。

①**賠償損害**では、**サイバー起因の事故で法律上の損害賠償金や争訟費用（弁護士費用・訴訟/調停/示談費用）などを補償**する。具体的には、第三者からの個人情報漏えい・業務阻害・権利侵害等からの賠償請求に対する、協力費用や訴訟対応費用である。一方で、罰金・課徴金などは補償対象外となる。

②次に**費用損害**では、**事故対応費用、原因・被害範囲の調査（フォレンジック）、広告・広報・コールセンター、法律相談、コンサル費用、見舞金などが補償対象**である。商品によっては、さらにクレジット監視、公的調査対応、そしてコンピュータシステムなどの復旧、再発防止費用までが対象に含まれることもある。自社の財物損害として主に対象になるのは電子データやシステム等IT資産の復旧費用である。自社の建物や機械・人が被る損害に対する補償は限定的であり、補償の空白が存在する。例えば動産に関する火災や損傷などを幅広く補償する「動産総合保険」など、多くの保険でサイバー起因の損害は補償対象外となっている（サイバー攻撃に関する不担保特約）。

③最後に**利益損害**では、**サイバー攻撃や運用過誤でシステム機能が停止し、営業が休止/阻害した際の喪失利益（例：収益減少×利益率から付保経常費の免れ分等を控除）、収益減少防止費用（標準営業収益の減少を防ぐための必要かつ有益な追加費用）、営業継続費用（復旧期間中にかかる追加費用）が補償対象**となる。ただし、免責期間が設定されるため、免責期間を越えない中断は補償対象外となる。また喪失した利益を対象とするため、売上の計上が遅れているだけでは補償されない。

このような補償対象と免責事項は細かく約款で定義されているが、それでも、サイバー保険請求時において訴訟に発展する場合はある。訴訟に発展するのは、保険会社と契約者の補償対象に対する認識のずれや約款の解釈の違いや、契約者は請求要件を満たしていると考えているが保険会社側は満たしてないと主張するような場合である。このような事態を避けるためにも事前に契約内容を確認して、なにが補償対象に含まれ、なにが免責事項となっているか保険会社と契約者の双方が合意しておくことで不要な争訟を避けることができる。

「将来想定される損害に対して手を打っていたはずが有効に機能しなかった」、「有事への対応でただでさえ忙しいのに保険会社との調整が難航し疲弊した」、「信じて頼りにしていたのに裏切られた」。本書により契約者の皆さんがこのような憂き目にあわないことを願っている。

サイバー保険の利用場面

サイバー攻撃対応時のみならず、平時にも利用するケース有り

	平時	サイバー攻撃のおそれ	サイバー攻撃確定	外部公表提訴	収束	平時
	定期点検	**初動対応**	**対応**	**事態収拾**	**再発防止・復旧**	**対策見直し**
補償		調査費用補償	調査費用補償	対応費用補償	再発防止・ 復旧費用補償	
支援	✓リスクモニタリング ✓ベンチマーク レポート	✓ホットライン ✓影響調査 ✓証拠保全	✓原因調査 ✓影響範囲特定 ✓ログ収集 ✓暫定対策	✓コールセンター 設置 ✓記者会見手配 ✓訴訟対応	✓恒久対策 ✓システム復旧	✓セキュリティ コンサルティング ✓脆弱性診断

※ 保険でカバーできない費用が発生する場合があります。
支援に要する費用がサイバー保険の補償対象となるか必ず保険会社へご確認ください。

※ 複数の保険会社のサイバー保険に関するパンフレット等を参考に作成しています。
保険会社により提供されるサービス内容が異なりますので、必ず保険会社へご確認ください。

コラム２．ログを取ってれば、サイバー攻撃がわかる！？

ログは、サイバー攻撃を受けた際の事象の分析や、サイバー攻撃の立証のため証拠の一部として利用することができ、とても重要な存在です。ただし、「ログを取っているから大丈夫」という考えには穴があるかもしれません。みなさんのシステムでは、もちろんログを取っているでしょう。しかし、**「ログを取っている＝サイバー攻撃がわかる」ではありません。サイバー攻撃に備えるためには、ログの「取得」「保管」「分析」の三つの観点で平時から取り組む必要があります。**これらの観点でありがちな不足している点について触れていきます。

まず、**「取得」の観点**です。ログは色んなログがありますので、全ては語れないためOSのログを例にあげて説明します。Windowsのイベントログ やLinuxのSyslogは、標準で出力されるログです。このログを出力しているだけの状態を「ログを取っている」と捉えがちです。**ログは目的に応じた内容を追加で取得する必要があり、標準のログだけでは、サイバー攻撃を受けた際の、分析につながる重要な情報が不足しています。**

次に、**「保管」の観点**です。**ログの保管状態そのものに課題があるかもしれません。**「ログを取っている」だけで適切なログファイルサイズの見積もりとそれに合わせたディスクの割り当てを行わないと、保管容量の限界がきて、正常にログが保存されていない場合があります。あるいは、**ログのバックアップが複数の方法で保管されていない場合、攻撃者の手によりログの改ざんやログ自体の暗号化が行われ、分析できない状態にされる可能性があります。**

最後に、**「分析」の観点**では、平時からの準備が不足している可能性があります。**攻撃者の行動を見つけるために、システムの情報（システムの資産情報、構成図、IPアドレスなど)や普段どのような通信・ログが発生しているか確認しておき、すぐに異常を見つけられるよう備える必要があります。**先に述べた「取得」と「保管」の観点と合わせて、平時から備えることによりログを効果的に活用できる状態になります。これにより、サイバー攻撃を受けた際に平時とのログの違いを見つけ、サイバー攻撃の影響の把握に繋がります。

昨今のサイバー攻撃は巧妙化しており、完璧に防ぐことは困難です。だからこそ、平時の取り組みを進め、万が一の損失や初動コストに備えとしてサイバー保険の併用も視野に入れてください。本書では、サイバー保険が有事だけでなく、平時に活用できる支援があることを紹介しています。**平時の取り組みは有事への備えです。有事にログを活用できるように、ログの「取得」「保管」「分析」を見直すことを提案します。**

3.サイバー保険の導入検討

検討開始時から運用設計までのTips

サイバー保険を導入する上での検討事項として、本プロジェクトで調査・議論した内容を４つの観点でまとめた。
特に入口となる「そもそも、サイバー保険を俎上に載せるか」では、サイバー保険の用途となるリスクファイナンスとインシデント対応に対する組織のケイパビリティに関し個別に説明している。
検討に割ける工数や部門間での連携状況などで実行に制約はあるが、参考としていただきたい。

- ✓そもそも、サイバー保険を俎上に載せるか
- ✓検討開始時の留意点
- ✓要求仕様検討・見積取得時の留意点
- ✓運用設計の留意点

そもそも、サイバー保険を俎上に載せるか

４つの問いかけに対し全てYesなら、社内外のニーズに応じて判断
１つでも判断に迷うなら、俎上に載せた方がよい
１つでも不明なら、まずは自社の体制・状態を確認せよ

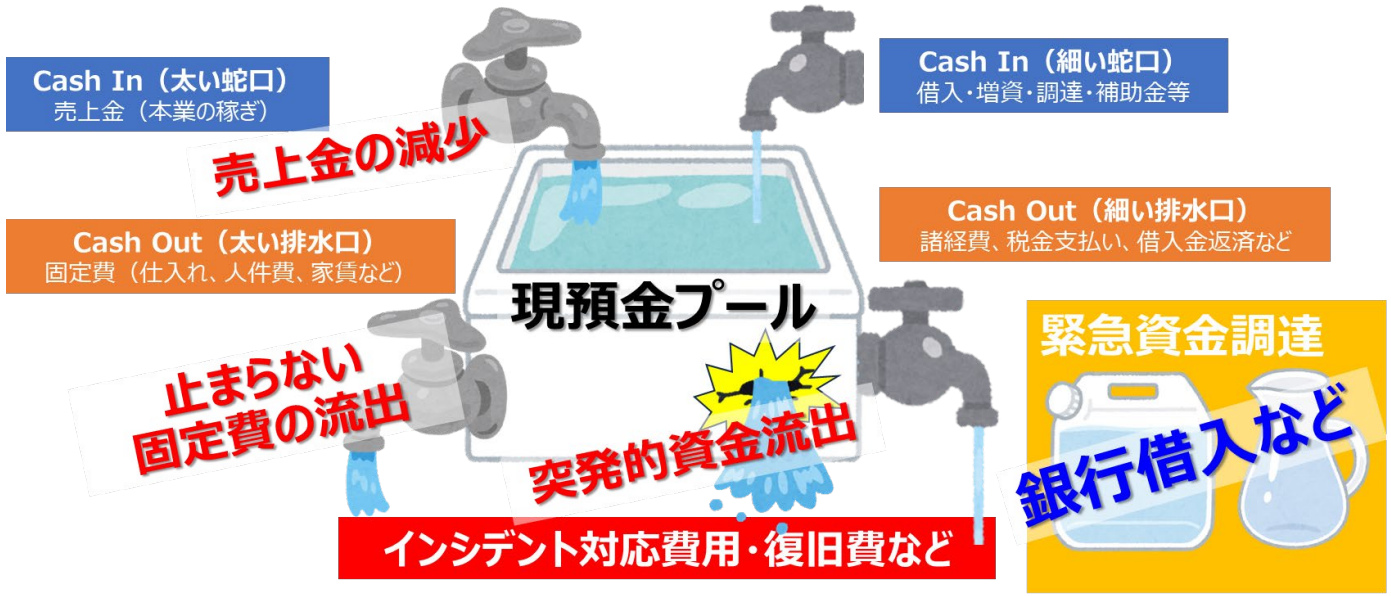
#	問いかけ
1	サイバーインシデント発生時に対応する資金を確保しているか？もしくは調達可能か？
2	サイバーインシデントにより想定される被害額は経営上十分許容できる額か？
3	インシデント対応をする体制や要員は整っているか？
4	サイバーセキュリティのノウハウは蓄えられているか？または相談する専門家は確保できているか？

＃１　サイバーインシデント発生時に対応する資金を確保してるか？

資金が無ければインシデント対応を十分に行えない。
経営上、今すぐ出せる手元資金が少ないなら確保が必要。

現預金など流動資産の減少は資金繰りの悪化へとつながり、枯渇させてしまうと最悪の場合倒産へ至る。
日本の企業全体では月商の約2カ月分の手元資金を保有している。
日本政策投資銀行 「負債とキャッシュが積み上がる日本企業」より
https://www.dbj.jp/topics/investigate/2023/html/20240301_204681.html

これは日々の支払い用やすぐに動かせない資金を含む。
すぐに利用できる資金を確保し、緊急時に即時決済し、スピード感をもって対応することが被害を抑えることにつながる。

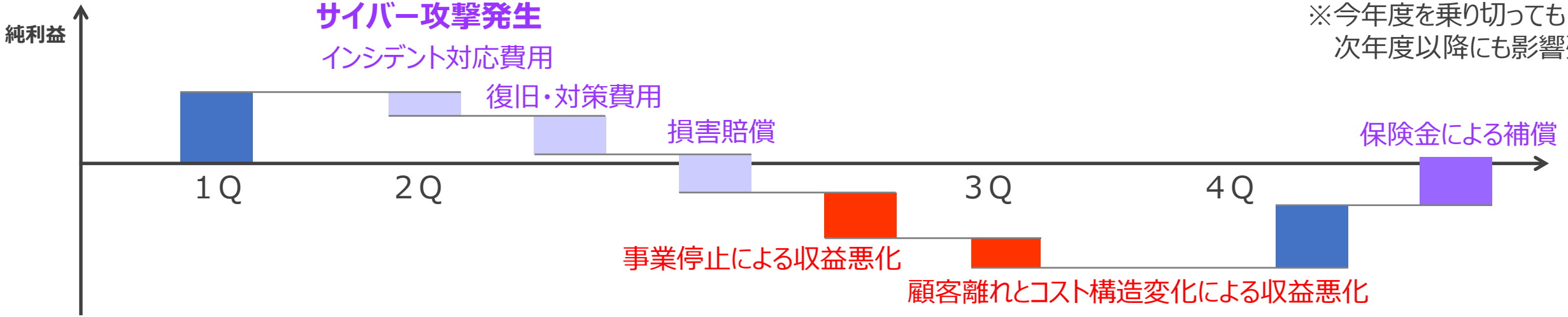


※**資金調達は需要に合わせて手当てできる手段を用いることが必要。**
例えば、保険金は数か月後の受領となる可能性があるため、当座の資金繰りには適さない。
しかし、保険金を返済の裏付けとして銀行から借入交渉を行うことはできる。

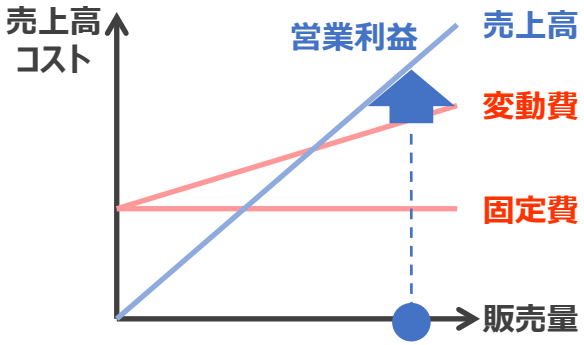
＃２　想定される被害額は経営上十分許容できる額か？

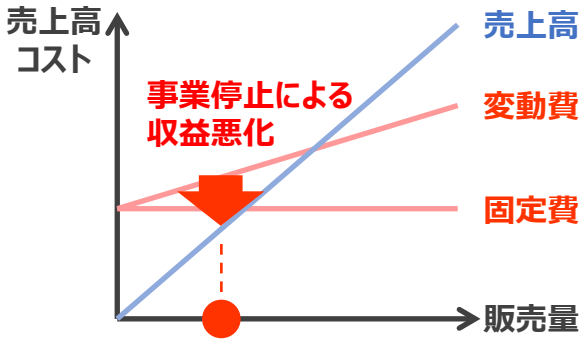
まず「**今年度を黒字で乗り切れるか**」は経営者としての関心事

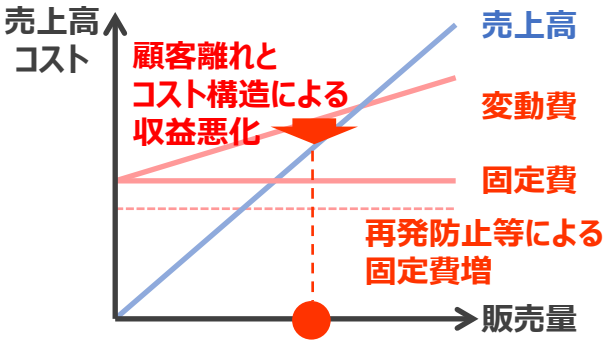
過去事例や同業他社の事例を参考に、自社ではどの程度の被害が想定されるかケーススタディをする。
それはステークホルダーへ約束している単年度計画に対し挽回できる程度の被害額か、他部門と協議し、リスクとして認識する。

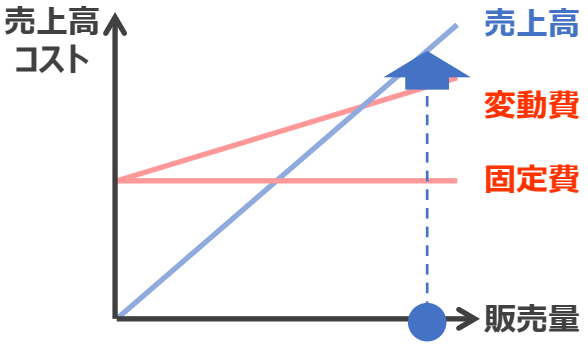


※今年度を乗り切っても
次年度以降にも影響残









＃３　インシデント対応をする体制や要員は整っているか？

自社リソースで乗り切れるか、不足を外部専門家で補えているか検証

日本国内でサイバーセキュリティ人材は11万人不足 ⇒ 全ての組織で人材確保し、体制構築できるわけではない

出典：ISC2「Cybersecurity Workforce Study 2023」より

保険会社のコネクションを通じて外部専門家を利用することも一つの選択肢となる

インシデントレスポンスのアクションと人材の例

想定
- 社内体制：サイバーセキュリティ担当（兼務者）がインシデント対応を取り纏め、情報システム部門が現場対応にあたる。
- 外部支援：ログの監視を委託。フォレンジック調査の専門家と契約しているが、法対応のノウハウは無い。

フェーズ	分類	アクションの例	中心となる専門人材	整備状況
初動対応	緊急トリアージ	重大度判定、エスカレーション、初動方針策定	インシデント管理担当、CSIRT全体統括	☑内製 □外注 □未整備
	監視、端末防御	端末隔離、セキュリティ監視、侵害情報の共有	情報収集担当、情報分析担当	□内製 ☑外注 □未整備
	証拠保全	ログ収集、媒体保全、改変防止措置	フォレンジック担当、法務担当	□内製 □外注 ☑未整備
対応	フォレンジック調査	メモリ・ネットワーク等調査、原因・侵害経路の特定	フォレンジック担当、情報分析担当	□内製 ☑外注 □未整備
	影響範囲特定	侵害範囲特定、流出データ・件数の推定	情報分析担当・法務担当	□内製 ☑外注 □未整備
	封じ込め、隔離	アカウント停止、ネットワーク分離、暫定対処	インシデント処理担当、システム運用担当	☑内製 □外注 □未整備
事態収拾	弁護士相談	法的報告義務の有無判断、報告対応、訴訟対応	法務担当	□内製 □外注 ☑未整備
	広報、コールセンター	公表準備、メディア対応、問い合わせ体制構築	広報担当	□内製 □外注 ☑未整備
再発防止復旧	再発防止	根本原因分析、恒久対策の設計・実装	セキュリティ戦略担当、システム運用担当	□内製 ☑外注 □未整備
	システム復旧	クリーンビルド、バックアップ復元、整合性確認	システム運用担当	☑内製 □外注 □未整備

＃４　サイバーセキュリティのノウハウは蓄えられているか？

人数だけでなく、役割に応じたスキルに成熟しているか

サイバーセキュリティ専任者が配置されている組織は少ない。兼務中心の体制では、インシデント対応で求められるフォレンジック等専門性の高い業務を自社のみでの完遂が難しい場合もある。そのため演習や訓練を通じ実行性を確保しておくことと共に外部支援の活用が選択肢として有効。フォレンジックの要求スキルの参考として外部フォレンジック支援利用時の仕様例を示す。

外部フォレンジック支援の仕様例

項目	内容
目的	サイバーインシデントの背景と侵入経路・被害範囲の特定
役割分担と作業範囲（責任分界点）	自社：情報システム部門が影響システムの隔離・復旧対応を実施 フォレンジック会社：サイバーインシデントの証拠取得と原因究明
調査範囲	対象システム（サーバ・パソコン・クラウド）、ログの期間、第三者・委託先システムの扱い、ベンダ連携窓口
証拠保全の要件	取得対象（ディスクイメージ、メモリ、ネットワークログ等）、取得方法（フォレンジック専用ツールなど）、 チェーン・オブ・カストディ（証拠保全・取扱い記録）
成果物	初動報告（状況・影響・仮説）、最終報告（時系列・原因・攻撃経路・被害範囲）、 経営層へのサマリー、再発防止策の提案、行政機関・警察への報告、法的証拠として提出
作業環境	現地作業時の手続き、作業時間帯の制約、機器の持込・持出制限、リモート接続方法
連絡窓口	報告・問い合わせ先、報告頻度（逐次の作業状況、日次の進捗報告）、24/365体制、SLA（応答・報告の時間基準）
承認フロー	事前承認が必要な作業とそれに対する承認者

コラム３．海外の倒産事例を調査して

サイバーセキュリティはIT部門の仕事、そう考えている経営者の方は多いかもしれません。しかし、サイバー攻撃により倒産した企業の事例調査を重ねていくうちに明らかになった最も重要な点は、**サイバー攻撃単体で倒産するとは限らない**ということです。**元々抱えていた財務的な脆弱性がサイバー攻撃により加速し、決定的な引き金となっているケースも少なくありません。**

精密機器メーカーS社は、サイバー攻撃前から継続的な赤字と資金繰りの厳しさという問題を抱えていました。そこへランサムウェア攻撃が追い打ちをかけ、生産停止と売上入金遅延が発生し、わずか2週間で倒産手続きを申請する事態に陥りました。老舗鉄骨建築企業U社も同様です。サイバー攻撃前から、鉄鋼関税によるコスト増で業績が悪化傾向にありました。そこにランサムウェア攻撃が襲いかかり、会計システムや製造データを含む**ほぼ全ての財務・業務データが失われたことで、事業継続を断念**するに至りました。

サイバー攻撃が企業を破産に追い込む要因は、金銭的な損失だけではありません。U社の事例では、ランサムウェア攻撃によって「財務記録そのもの」が破壊されました。**誰にいくらの売掛金があるのか、支払うべき債務はいくらかといった基本的な財務状況が把握できなくなり、営業継続が不可能**になりました。これは、**金銭的補償だけでは回復できない、事業そのものの機能不全**を意味します。

介護サービスを展開していたP社は、自社が直接攻撃されただけでなく、サプライチェーンの決済サービス企業がサイバー攻撃を受けたことで、**保険金の受け取りが滞り、財務状況に深刻な打撃**を受けました。また、大規模データ侵害を起こした身辺調査サービスJ社の事例は、保険の限界を示しています。同社は包括的賠償責任保険（GL保険：General Liability Insurance）に加入していましたが、**データ漏洩による補償請求を保険会社に拒絶**されました。**GL保険は対人・対物の物理的リスクが主な対象であり、サイバーリスクは契約上含まれていなかった**ためです。同社はサイバー攻撃以前は黒字経営を続けていましたが、顧客からの信頼失墜と、多額の民事請求や集団訴訟費用を賄いきれなくなり、破産に至りました。この事例は、適切なサイバー保険に加入していなければ、十分な補償を得られないリスクを物語っています。

これらの調査でわかったことは、**サイバーリスクは企業の存続を左右する「経営課題」であるということです。サイバーリスクに対する「予防」と同時に、万が一の事態に備え、迅速に対応し立ち直る「レジリエンス（回復力）」を構築することが不可欠です。**皆さんの会社は、サイバー攻撃という見えないリスクから身を守る準備ができていますか？

サイバー保険の検討開始時の留意点

関係部門や経営層と共通のリスク認識を持ち、自分事として取り組む体制作り

#	検討開始時の留意点
1	組織の抱えるサイバーリスクを、業界・同業他社でのサイバーインシデント発生実績と共に共有する
2	サイバーリスクに関し誰がリスクオーナーか、関連部門の役割や責任、コスト負担について明確にし合意を得る
3	サイバーインシデントにより想定される被害額を定量的に評価し共有する
4	サイバーインシデント発生時に事故対応をする人員・スキルや復旧期間などについて共有する

サイバー保険の要求仕様検討・見積取得時の留意点

保険が機能しない落とし穴を避け、保険料と残余リスクのバランスを最適化する

#	要求仕様検討・見積取得時の留意点
1	自社の要求が過大であり、ミスマッチの場合は期待値調整をする （戦争行為や国家支援型の攻撃など、交渉の余地がない免責事由の補償を求めるなど）
2	保険金の補償限度額・自己負担額・特約を調整し、リスクシナリオの想定被害額を許容内に収める
3	保険金の支払事由・免責事由を交渉し、補償を受ける条件を満足させる
4	サイバー攻撃の立証要件を明確にし、自社が対応できる体制を整える
5	事故調査や支払査定に要する期間を考慮し、緊急資金調達手段の準備要否について担当部門と相談する
6	想定しているリスクに対し、導入済み保険の補償との重複、逆に補償の抜け漏れが無いか確認する

サイバー保険の運用設計の留意点

保険金請求を見据えた事故対応プロセスの見直しと請求プロセス・条件の整理

#	運用設計の留意点
1	保険会社指定の外部専門家以外を利用する場合、補償対象となるか保険会社へ事前確認する
2	外部専門家の利用を想定している場合、どの部門がどのように連携するか事前に整理する
3	外部専門家のサービス提供開始時間と対応可能時間を事前確認する
4	保険金請求時の立証を見据え、証拠保全や調査内容の記録についてインシデントレスポンスの手順書へ反映させる
5	インシデント発生時に保険会社や外部専門家へ早急に直接つながる連絡先・連絡方法を整備する
6	保険金の減額やフォレンジック調査可否に繋がるため、いつまでに・どのようなアクションをする前に連絡するか確認する
7	保険適用を判断する部門とのインシデントレスポンス時の情報連携フローを整える
8	保険金請求実績により更新後の保険料値上がりの可能性があるため、保険適用する被害額を社内で合意しておく
9	環境の変化によりリスクは変わるため、保険で十分な補償がされているのか、リスクのモニタリングと補償の見直しをする
１０	毎年の保険更新時など、サイバーセキュリティ担当者も加わりサイバー保険会社との交渉・コミュニケーションをする

コラム４．サプライチェーンへの展開

これまでサイバーリスクに対する自社のリスクファイナンスとインシデント対応能力向上の手段としてサイバー保険について解説してきました。次の一歩として、事業継続を支えるサプライチェーンへと視野を広げます。

サイバーインシデントによりサプライチェーンを構成する一社が事業停止し、それが連鎖して自社の生産・販売・物流プロセスの広範な停滞を引き起こす可能性があります。例えば製造業において、影響の起点は部品サプライヤーにとどまりません。業務委託（運用・保守）、IT基盤（認証・ID連携・データ連携など）、クラウドサービス（受注・決済・生産管理・物流など）も単一障害点となり得ます。

そのような単一障害点になり得る**重要取引先に対しては、サイバーインシデントへの対応体制・手順の整備を取引条件として求めることが有効**です。しかし、取引先が必ずしも対応に必要な経営資源（人材・体制・ノウハウ・当座資金）を持ち合わせているとは限りません。そこで**サイバー保険の導入を促し、保険会社が提供する付帯・支援サービスを含む外部専門家の即応体制と費用補償の枠組みを平時から整備してもらうことで、対応力の底上げと復旧の迅速化が期待できます。サプライチェーン全体のレジリエンスを確保することで、自社の事業継続性、すなわち組織のレジリエンス向上につながります。**

注意点として、下請代金支払遅延等防止法（下請法）における「購入・利用強制」や、独占禁止法における「優越的地位の濫用」や「拘束条件付取引」に該当し得るおそれのある運用は回避すべきです。特定の保険会社や商品・サービスを指定せず、補償水準や運用要件といった機能要求で示すなど、法務部門と協議のうえ進めるとよいでしょう。

コラム５．保険料の調整

ここまでの説明でサイバー保険の導入を検討してみようという気持ちになったでしょうか。ただ、加入するにあたり、予算不足という障壁にぶつかってしまうかもしれません。でも、予算が足りない！っとなった場合でもまだ諦めないでください。保険料は、調整余地が多分にあります。

保険料算定の構成要素

保険料（掛金）は、

①売上規模（売上高）・業種
②過去（3～5年が一般的）のセキュリティ事故発生歴
③導入済みのセキュリティ対策（質問書や申告書の回答で評価されることが一般的）
④補償範囲や付帯サービス

といった要素に基づき算定されます。④のうち、特に補償範囲を細やかに設定することで、保険料の削減につながる場合があります。

補償範囲に関する保険料の調整で用いる主なポイント

補償対象：情報漏えい、利益損害、第三者への損害賠償費用など、どこまでを対象とするかを選択できる場合があります。
対象範囲を広げれば安心感は増しますが保険料も上昇するため、移転したいリスクを中心に設計することが重要です。

補償額　：支払上限を設定することで保険料を抑制できる場合があります。

免責額　：自己負担額を増減して保険料の調整ができる場合があります。
特に大きな補償額を必要とする際に、一定の損害までなら自己負担とすることで保険料低減につながります。

補償割合：保険会社と企業の負担割合を設定できる場合があります。例えば70%補償とすれば保険金は抑えられますが、残り30%は自己負担となるため、許容範囲を見極める必要があります。

また、自社が親会社の場合には、グループ全体を包括対象とする契約※にすると、売上規模に応じた一括評価が可能となり、個別契約よりもコスト効率や交渉力の面で有利に働くケースが多いです。自社単体では保険料負担は大きくなるものの、グループ全体では保険料割引につながることもあるため、ぜひ検討してみてください。

※親会社が一括で負担すると子会社への利益供与とみなされる場合もありますが、親会社のレピュテーションリスク低下などの自社リスク低減のための必要な自社投資としてみなされることもあります。親会社負担でグループ一括加入を検討される場合には、弁護士や法務や財務部門に相談の上、検討をしてください。

4.おわりに

サイバー保険の留意点

サイバー保険はサイバーインシデントによる突発的な経済的損失を補償し、事業継続を支援する財務的なセーフティネットとなることを伝えてきました。しかし、サイバー保険により得られる財務的補償・支援のみでは、組織のレジリエンスを高めることはできません。

なぜなら、サイバー攻撃がビジネス化されている昨今、一度サイバー攻撃を許してしまった組織はその後も攻撃を受け経済的損失を受ける可能性があるからです。いくら資金を補償されても何度も被害にあっては組織の信頼は地に落ち、顧客離れ・新規契約の減少・株価の下落といった影響が懸念されます。それらは保険でまかなえるものではありません。

重要なことは環境変化と組織の抱えるリスクを常に認識・モニタリングし、適切な対応を取り続けることです。その対応とは、セキュリティ製品の導入といった技術的対策だけでなく、教育や体制整備といった組織的な対策や業務プロセスの見直し、サプライチェーンも含めたセキュリティ強化など、**多角的なアプローチによりサイバーリスクへの対応能力を向上することが求められます。**

本書が、サイバー保険の検討をしている担当者のサポート、並びにサイバーリスクに対する組織のレジリエンスを高める一助となることを願っております。

謝辞

本書の作成にあたり、ご協力いただいた企業の皆様には、貴重なご意見ならびに多大な
ご支援・ご尽力を賜りました。ここに謹んで御礼申し上げます。

また、名古屋工業大学の渡辺研司先生には、企業との橋渡しに多大なるお力添えをいただきました。
厚く御礼申し上げます。

さらに、本プロジェクトのメンターを務めていただいた越島一郎先生、佐柳恭威先生、宮本大輔先生、
門林雄基先生、佐々木弘志先生に加え、産業サイバーセキュリティセンター中核人材育成プログラムの
諸先生方からも、ひとかたならぬご指導・ご助言を賜りました。ここに深く感謝申し上げます。

最後に、本書の作成および本プロジェクトの推進にご尽力くださったメンバーの皆様にも、
心より御礼申し上げます。

本書は、独立行政法人情報処理推進機構 産業サイバーセキュリティセンター
中核人材育成プログラムにおける卒業プロジェクト「経営と財務を守るサイバーリスクマネジメント」の
成果物として作成されました。

プロジェクトメンバー

リーダー	二瓶　真光
サブリーダー	榎本　祐二
サブリーダー	塚田　竣介
メンバー	岩田　紫苑
メンバー	山本　大貴

サイバー保険検討のススメ