

インシデント発生時における損害額

～サイバー保険の必要性～

2026年2月25日(水)13時30分～15時30分

サイバーリスク対策セミナー 第二部資料

あいおいニッセイ同和損害保険株式会社
福島支店 地域戦略室



パート1
サイバー攻撃を
受けると
お金がかかる

インシデント発生時において生じる損害

各種事故対応についてアウトソーシング先への支払が発生

1. 費用損害 (事故対応損害)

被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自社で直接費用を負担することにより被る損害(下記2~6に該当しないもの)

さらに、次のような損害の発生も・・・

2. 賠償損害

情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害

3. 利益損害

ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害

4. 金銭損害

ランサムウェア、ビジネスメール詐欺等による**直接的な金銭(自組織の資金)の支払い**による損害

5. 行政損害

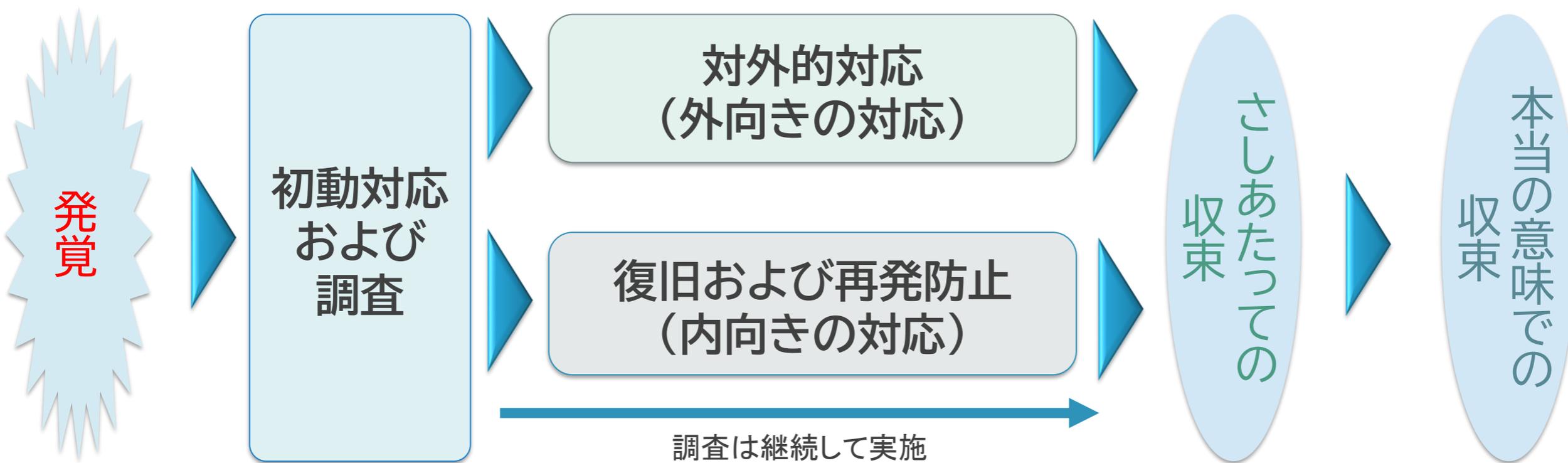
個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害

6. 無形損害

風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

インシデント発生時の流れ

各場面において、費用損害、賠償損害、利益損害が発生・・・



当面の事故対応・・・
費用損害

後からくるダメージ・・・
賠償損害、利益損害

費用損害

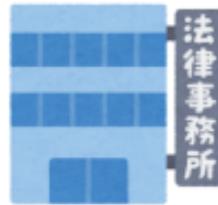
専門の会社に調査
(フォレンジック調査)を委託

900万円



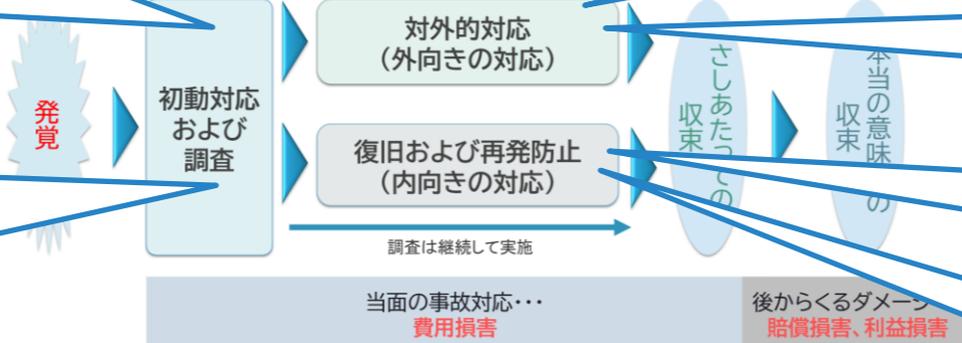
法律事務所に
対応等を相談

300万円



インシデント発生時の流れ

各場面において、費用損害、賠償損害、利益損害が発生



被害者に詫び状を送付
1,300万円

コールセンター会社に
クレーム対応を委託
6,000万円



出入りのITベンダに
システム復旧を依頼
5,000万円



セキュリティベンダに
再発防止策を依頼
2,000万円



自社だけでの対応は困難…。専門会社へのアウトソーシングも必要
その**コスト負担は過大**なものに(費用損害)

初動対応・調査①

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

事故原因・被害範囲調査費用

- ・専門業者が実施(セキュリティ業界ではこの調査をフォレンジック調査という)
- ・専門家が長時間かけ、調査・分析する
- ・思いのほか高額！
数百万円～



初動対応・調査②

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

コンサルティング費用

- ・お詫びの仕方によっては、二次被害も
- ・専門家(法律事務所、PR会社)への依頼が無難
- ・謝罪時期、謝罪文の内容等のコンサルに委託料が発生
数十万円～数百万円



対外的対応①

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

事故対応費用・社告宣伝活動費用

■詫び状作成・送付

- ・漏えい件数に応じたコストが発生
- ・漏えい件数が10,000人であれば

130万円程度
(10,000人×約120円)



対外的対応②

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

事故対応費用・社告宣伝活動費用

■コールセンター

- ・問合せ(クレーム)対応
- ・1オペレーター1時間0.5万程度
- ・1日8時間、30日間、5ブース設置
とすれば、

600万円程度 (8×30×5×0.5万円)



復旧・再発防止①

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

コンピュータシステム等復旧費用

コンピュータウイルスの除去、データの復旧等で相当のコストが発生
感染規模によるが、
数百万、数千万円の可能性も



復旧・再発防止②

STEP 1

初動対応・
調査

STEP 2

対外的
対応

STEP 3

復旧・
再発防止

再発防止費用

セキュリティの強化のための、
ソフトウェア・機器の導入で、
相当のコストが発生
対策規模によるが、
数十万円～



塵も積もれば

…山となる。



それだけじゃない・・・

追い打ちをかけるように・・・

賠償損害

利益損害

顧客離れ・
取引中止



賠償損害

◇近年、賠償問題となる事例が増加

◇個人データの漏えいについて、**個人からの損害賠償請求 ⇒×**
事故対応コストや逸失利益について、**法人からの損害賠償請求 ⇒○**

CASE1 エムケイシステム、イセトー、関通等

委託先が被害。委託元としても事故対応を迫られる
最終的に委託元から委託先に事故対応コストを求償



賠償損害

CASE2 アサヒGHD、アスクル等

メーカー等が被害。そのあおりで、サプライチェーン構成企業も事業中断
最終的に、サプライチェーン構成企業が逸失利益について損害賠償請求



アスクルの衝撃

アスクルが2026/1/28に公表した中間決算では、
特別損失**52億円のうち9割が賠償金の引当**
および物流基盤維持費用であることを公表
損害賠償リスクは看過できないものに

Q：特別損失 52 億円の内訳について教えて頂きたい。出荷期限切れ商品の評価損の金額や対象品目、物流基盤の維持費用やシステム調査・復旧費用に要した人数規模、またその中には親会社からの支援も含まれているのか？

A：特別損失（システム障害対応費用）52 億円の内容は、物流基盤を維持するための費用と、取引先様ごとに今後発生し得る損害に対する引当金の 2 点であり、この 2 つで全体の約 9 割強を占めている。期限切れ商品の評価損や廃棄損については、規模としては

利益損害

多くのシステムが生産・営業活動に直結している現在において、システムの停止は、事業中断につながり、売上高の減少をもたらす

利益損害のイメージ

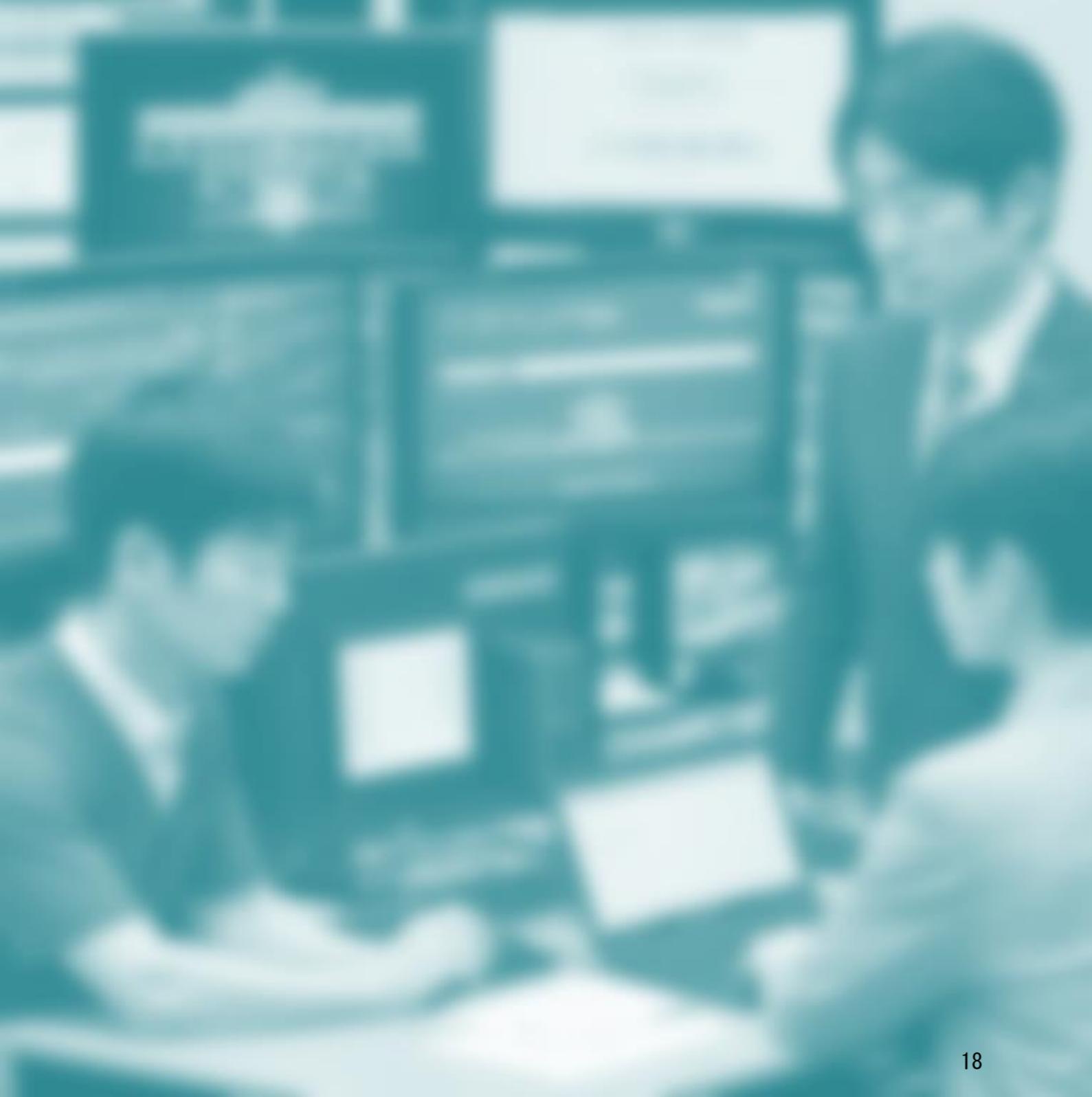
項目	平時	事業中断時	差額
売上高	10億円	6億円	▲4億円
固定費 人件費、賃料等	2億円	2億円	—
変動費 材料費、電気代等	7億円	4.2億円	2.8億円
営業利益(損失)	1億円	▲0.2億円	▲1.2億円
特別損失 前掲の費用損害、賠償損害	—	▲5億円	▲5億円
経常利益	1億円	▲5.2億円	▲6.2億円

- ◇事業中断による売上が4割減
- ◇事業が中断していても固定費は平時同様
固定費＝死に金
- ◇通常1億円稼げるのに営業損失▲0.2億円
- ◇前掲の費用損害や賠償損害は特別損失として計上
- ◇経常利益は大幅な赤字に

費用損害、賠償損害、利益損害・・・

数百、数千万円の支出の合計は**億単位**に





パート2
サイバー攻撃
の対策は
事後対策も重要

対策のポイント



経営者のリーダーシップで 進める

かつ、
経営者がリーダーシップで進めることが
できるよう**フォロワーシップ**で
従業員等一同で働きかける
「ひとつとじゃない」
自分事、自分たち事！
全員参加！

そのうえで

- ◇実際に、よくあるサイバー攻撃を踏まえた対策を！
(今、実施の対策は、よくあるサイバー攻撃の対策ですか?)
- ◇セキュリティ機器・サービスの導入(技術的対策)ほか、
組織・ルール作り、従業員教育も

対策例

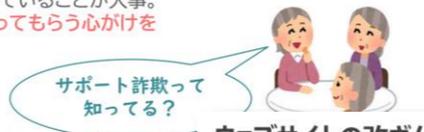
- ◇リンク、添付ファイルは開かない!
⇒攻撃手法が多様化しているので、QRを読まない、
[WIN+r][Ctrl+L][Ctrl+V]を押さない!なども…。
なので、
公式アプリや公式サイトをみる!
⇒Google検索等で正規サイトを調べると、
正規サイトを語った偽サイトが表示される
可能性があることに留意。公式サイトはお気に入り登録を
- ◇万ーリンク等を開いたとしても
クレカ番号、暗証番号等は**入力しない!**
⇒フィッシングが拡大しているなか、事業者が
メールやSMS経由でクレカ情報等の入力を要求することはあり得ない



Copyright © Aioi Nissay Dowa Insurance Co., Ltd. All rights reserved.

サポート詐欺 ～対策例～

- ◇相手にしない(ウイルスに感染していません)
- ◇ブラウザを閉じる(ESCキーを長押しする、強制終了等)
- ◇電話しない(画面に電話番号が表示していても無視)
- ◇電話しちゃってもすぐに切る(いかにもアヤシイのでわかると思います…)
- ◇とにかく、知っていることが大事。
多くの人に知ってもらう心がけを



ウェブサイトの改ざん ～対策例～

- ◇**セキュリティがわかっている**ホームページの制作会社に相談
⇒「ホームページのセキュリティ対策ができていない企業が多い」のは、
「セキュリティがわかっていないホームページ制作会社が多い」ともいえる
- ◇**それなりにお金をかける**
⇒ホームページは、セキュリティ対策コストをかけずに公開するものではない…
- ◇**セキュリティベンダのサービス**等も検討する
⇒セカンドオピニオンも含め、
セキュリティ本業の人とも対策を検討
- ◇**自社ECサイトは相当の覚悟**をもって
構築する必要アリ
⇒まずは、自社ではなく、楽天、Yahoo、Amazonでの検討
自社ECサイトのセキュリティ対策コストはかなりの額…



Copyright © Aioi Nissay Dowa Insurance Co., Ltd. All rights reserved.

情報窃取型ウイルス (インフォステイラー) ～対策例～

- ◇基本的には、冒頭のフィッシング詐欺
と同じ…。
リンク、添付ファイルは開かない
- ◇クリックフィックス等も知っておくことが必要
というより、ネットをみている際の指示にWin+R、Ctrl+Lや
Ctrl+V(貼り付け) があったら要注意



ランサムウェア ～対策例～

- ◇インターネットに接続している機器・サービスの管理徹底
とりわけVPN、リモートデスクトップツールといった、
会社のネットワークに接続するための機器・サービス!
管理を徹底すべきものの一例
①脆弱性対応
…OS・ソフトウェアの更新等(ITベンダへの確認)
②認証情報の適正な運用
…複雑なID/パスワード設定、二要素認証の導入(ITベンダへの確認)
- ◇バックアップ対策
⇒「バックアップも狙われる」ことを前提とした**オフライン**での
バックアップ。そのバックアップから、**着実・迅速な復旧**が
行えるよう**定期的な訓練**

Copyright © Aioi Nissay Dowa Insurance Co., Ltd. All rights reserved.

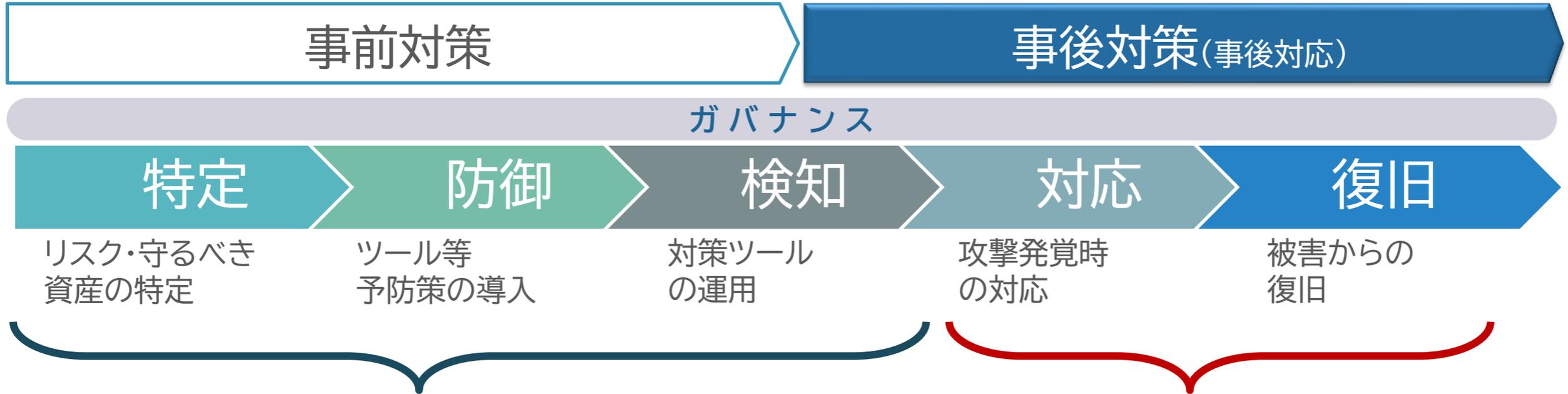
事後対策について

◇対策は、復旧までを考える必要あり



事前対策ほか、復旧まで考えた
事後対策の両方が必要！

保険の必要性



事前対策

ウイルス対策ソフトは当然のこと、
UTM、バックアップ等による技術的対策
従業員教育による人的対策
ルール作り等の組織的対策 など

+

事後対策

被害の極小化、早期復旧
のための経済的な備え
⇒サイバー保険

など

サイバー保険

対象とする事故

- ① **サイバー攻撃**
- ② 他人の**情報の漏えい**またはそのおそれ
- ③ IT事故(※)

※コンピュータシステムの所有、使用もしくは管理、または電子情報の提供に伴う、他人の業務の阻害、電子情報の消失など

不測かつ突発的な事由によるネットワーク停止

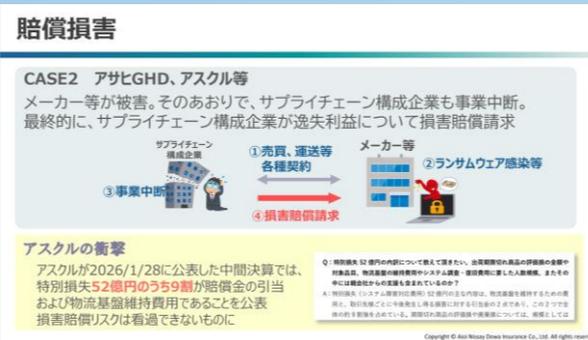
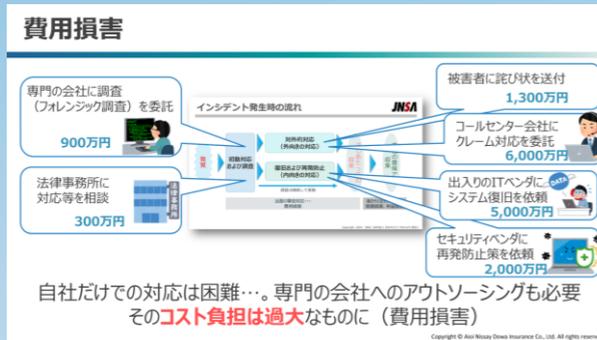
対象とする損害

①②③による
費用損害(当面の事故対応にかかる自社コスト)

②③による
賠償損害(損害賠償金、弁護士報酬等)

利益損害(営業利益、固定費等)

具体例



前掲、**費用損害、賠償損害、利益損害を補償**

一例：事後対策（事後対応）のサービス

あいおいニッセイ同和損保
MS&AD INSURANCE GROUP
まだ誰も知らない安心を、ともに。

令和6年4月以降保険始期用
全力サポート
サイバーセキュリティ保険

サイバー攻撃を受けたとき、
各種事故対応の**相談先を確保されていますか？**

火災の場合・・・**消防署（119番）**
すぐに消防署に連絡して
火を消してもらわないと！
119!

サイバー攻撃の場合・・・「???'
脅迫文が表示されている？
サイバー攻撃にやられた～
あれ？誰に相談すれば
いいのだけ？

サイバーセキュリティ保険の機能は、
保険金のお支払い（経済的な損失の補てん）
だけではありません！事故対応の支援
が、その大きな機能となっています！！

詳しくは裏面をご覧ください。

- ◇火事が起きたら「119番」・・・
サイバー攻撃が起きたら？
- ◇保険会社が事故対応を支援
⇒24時間365日の電話相談、
事故原因の調査を行う専門業者
の紹介・コーディネイトなど
- ◇サイバー保険の機能は、
保険金支払だけではなく、
この事故対応の支援が大きい