2024年１月1日
以降始期用

サイバーリスク保険のご案内

このご案内書は、サイバーリスク保険(*)およびこれに付帯する特約条項の概要を紹介したものです。
上記保険に関するすべての事項を記載しているものではありません。
詳細につきましては、保険約款によりますが、保険金のお支払条件・ご契約手続き、その他ご不明な点がありましたら、
ご遠慮なく代理店または東京海上日動（以下「弊社」といいます。）までお問い合わせください。
ご契約に際しては、必ず保険約款および重要事項説明書をご確認ください。

(*)IT業務を補償対象外とするご契約に限ります。

To Be a Good Company

TOKIO MARINE
NICHIDO

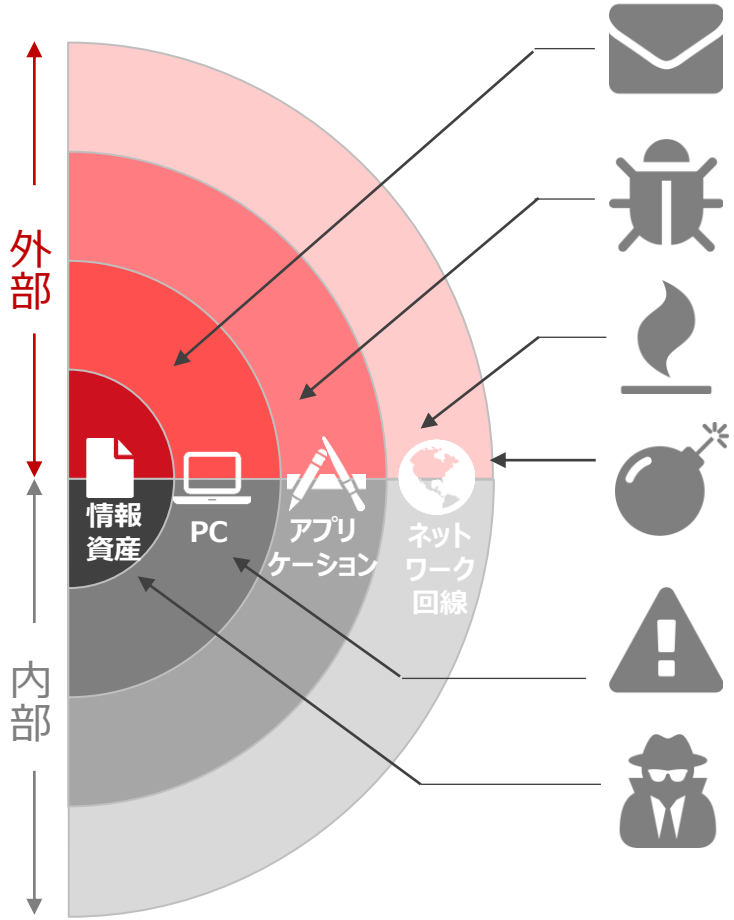
東京海上日動

Ⅰ.サイバーリスクとは

１．サイバーリスクの概要
２．ヒューマンエラー（内部原因）による情報漏えい事故
３．改正個人情報保護法の施行とその影響
４．もしサイバー攻撃による事故が起こったら

1．サイバーリスクの概要　－サイバーリスクの脅威－

サイバー攻撃は、手口が巧妙化しており、攻撃件数も今後さらに増加することが懸念されています。
強固なセキュリティを構築しても、サイバーリスクを完全に排除することは困難です。



標的型メール攻撃	主にマルウェア付きの電子メールを用いて**特定の組織**や**個人**を狙う攻撃です。
ランサムウェア	PC内の**ファイルを暗号化**したり、PCをロックしたりすることで、業務継続を困難にし、元に戻すことと引き換えに「身代金」（*）を要求するマルウェアです。
ウェブサイト改ざん	組織のウェブサイトに外部から侵入し、**ウェブサイトの内容を書き換え**てしまう攻撃です。
DDoS攻撃	複数箇所から同時に**大量の通信**を発生させ、インターネットサイト等を利用できなくする手法です。
盗難・紛失/メール誤送信	PCやUSBメモリの盗難・紛失、またはメールを関係の無い社外の人に誤って送信する等、組織内部の人間の**過失により発生する事故**です。
内部不正	組織内部の人間が、個人情報等を**社外に不正に持ち出す**等の行為です。

サイバーリスク保険は、これらの脅威等により発生した事故の各種損害を **包括的に補償** します。

（*）「身代金」を支出したことにより被る損害は補償対象外です。

TOKIO MARINE NICHIDO

２．ヒューマンエラー（内部原因）による情報漏えい事故

情報漏えい事故は、サイバー攻撃によるものが台頭してきていますが、組織内部の人間の『過失』または『内部不正』により発生するケースも多くあります。

	内部の脅威	想定事故例
過失	誤操作	顧客の氏名、口座番号、送金金額等の個人情報が記載されたデータを、誤って別の取引先の団体に送信。被害者に対して連絡をして、説明および謝罪を実施した。
過失	盗難・紛失	住所、氏名、メールアドレス等の顧客情報が入ったパソコンを従業員が紛失し、その事実を公表。被害者に対して連絡をして、説明および謝罪を実施した。
内部不正	金銭目的の売却	従業員が顧客約10万人分の情報を不正に持ち出し、名簿業者に売却していたことが発覚した。被害者に対して連絡をして、説明および謝罪を実施した。
内部不正	競合企業への流出	従業員が、取引先の属性情報や取引履歴等の機密情報を不正に持ち出し、競合企業へ提供していた。取引先企業から損害賠償を請求された。 （※営業秘密（秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていない情報）等、知的財産権に該当する場合には補償対象外です。）

サイバーリスク保険は、

ヒューマンエラー（内部原因）による情報漏えいまたはそのおそれに起因する損害も補償します。

３．改正個人情報保護法の施行とその影響

2022年4月1日より改正個人情報保護法が施行されました。
これにより、**一定の基準を満たす個人情報の漏えい**が発生した場合

1 個人情報保護委員会への報告
2 漏えい対象となった被害者本人への通知

が義務化されました。

一定の基準を満たす個人情報の漏えいとは？

いずれかに該当するものを言います。

1. **要配慮個人情報(医療情報・犯罪歴等)の漏えい、滅失若しくは毀損、またはそのおそれ**
2. **不正利用されることにより、財産的被害が発生し、または発生したおそれのあるもの**
3. **不正の目的をもって行われたおそれがあるもの（例：サイバー攻撃による情報漏えい）**
4. **漏えいまたは漏えいのおそれのある被害者が1,000人を超えるもの**

実務でどのような影響が生じるのでしょうか？

1 個人情報保護委員会への報告

- 速報と確報の2段階。速報は報告対象事由発生から概ね3~5日以内、確報は30日以内(※)に実施。
  ※対象事由に左記❸を含む場合には、60日以内。
- 報告にあたり、原因調査、被害範囲の特定を実施する必要あり。サーバ1台あたり100～200万円程度の費用が発生。

2 漏えい対象となった被害者本人への通知

- 漏えい被害者の特定、連絡先（住所・電話番号・メールアドレス等）の確認
- 「漏えい事象の概要」、「漏えいした個人データの項目」、「原因」、「二次被害、またはそのおそれの有無」、「その他参考情報」等を含めた通知文書の作成

**原因調査・被害範囲特定等、所定の対応には一定の費用負担が生じます。
また、漏えい被害者からの賠償請求に備えることも重要です。
サイバーリスク保険では、被害者に対する損害賠償金だけでなく、上記一連の費用も補償されます。**

４．もしサイバー攻撃による事故が起こったら

サイバー攻撃への初動対応および事故対応には、多額のコストが発生します。

事故対応プロセス（例）

ケーススタディ（架空）

業種・規模：　製造業、社員数約1,000名、売上高約300億円
事故・被害：　標的型メール攻撃により、社内PC10台がマルウェアに感染。取引先の機密情報および顧客の個人情報約60,000件が流出
経緯：　セキュリティ運用管理会社に情報流出の可能性を指摘され発覚。その後本格調査に乗り出し、事故・被害の全容を把握

	検知	初動対応	対応	事態収拾	再発防止計画
求められる対応	• 検知内容の精査	• 影響の調査 • 影響箇所・範囲の特定 等	• ログ収集 • 証拠保全 • 原因・被害調査 • バックアップ復元　等	• 見舞金 • 広報対応 • 弁護士費用　等	• 再発防止のための各種施策(技術対策、教育、ルール作り等)の計画策定
想定費用	（社内で対処）	約 *500* 万円	約 *3,000* 万円	約 *4,000* 万円	約 *500* 万円

※ 上記金額はあくまで想定です。個社の状況、事故の内容、対応業者等により金額は変わります。

Ⅱ．想定事故例

１．想定事故例①（小売業）
２．想定事故例②（製造業）
３．想定事故例③（建設業）

1．想定事故例①（小売業）

イメージいただくための想定事例であり、事故内容を踏まえた対応や関連した損害額は、個社ごとに状況に応じた判断や対応する業者等によって異なりますのでご注意ください。なお、損害額は保険金とは異なります。
（保険金の額は損害額を踏まえ契約内容に従って決まります。）

会社概要

年間売上高：5千万円
従業員数：5名
売上高の80%がECサイト経由の販売

事故内容

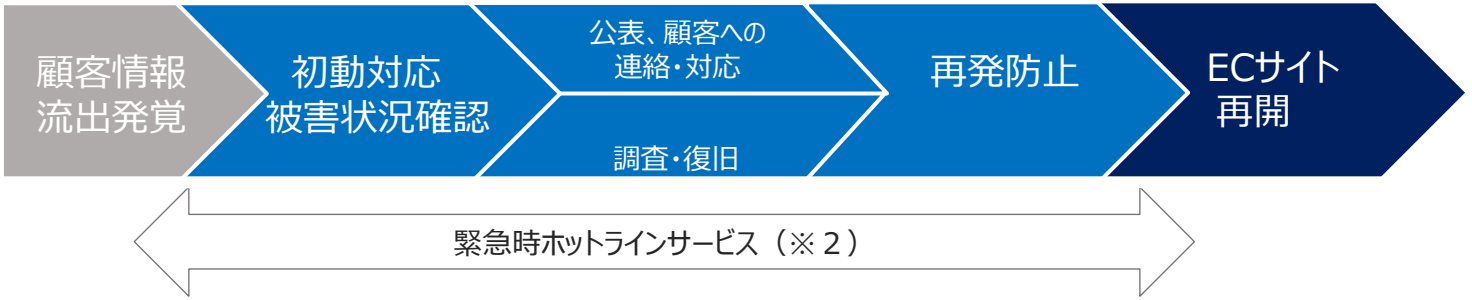
ECサイトへの不正アクセスにより、
顧客情報(※1)1,000件が流出。
調査・復旧に時間がかかり、20日間ECサイトを閉鎖した。
（※1)住所・氏名・電話番号・クレジットカード番号・セキュリティコード・有効期限

本事例で想定している主な対応と損害額

■サーバのフォレンジック調査・復旧：500万円
■お客様対応にかかる弁護士相談：150万円
■お客様への情報漏えいにかかる通知：10万円
■お客様へのお見舞いの支払い：100万円
■営業停止に伴う喪失利益の発生：200万
合計960万円

上記以外に主に以下の対応が必要となることも想定されます。
・コールセンターの設置
・再発防止

対応の流れ



（※2）お客様に発生した様々なサイバーリスクに関するトラブルやインシデントについて、専門の担当者がご支援を実施するサービスを提供します。詳細は代理店または弊社までお問合せください。

TOKIO MARINE NICHIDO

2．想定事故例②（製造業）

イメージいただくための想定事例であり、事故内容を踏まえた対応や関連した損害額は、個社ごとに状況に応じた判断や対応する業者等によって異なりますのでご注意ください。なお、損害額は保険金とは異なります。
（保険金の額は損害額を踏まえ契約内容に従って決まります。）

会社概要

年間売上高：8千万円
従業員数：5名

事故内容

社員のパソコンが標的型メールによりウイルス感染し、社内イントラ経由で生産ラインの管理パソコンも感染、30日間にわたり生産停止。
加えて、ウイルス感染されたパソコンを踏み台に関連会社になりすましメールが送られ、関連会社も感染。（踏み台攻撃）

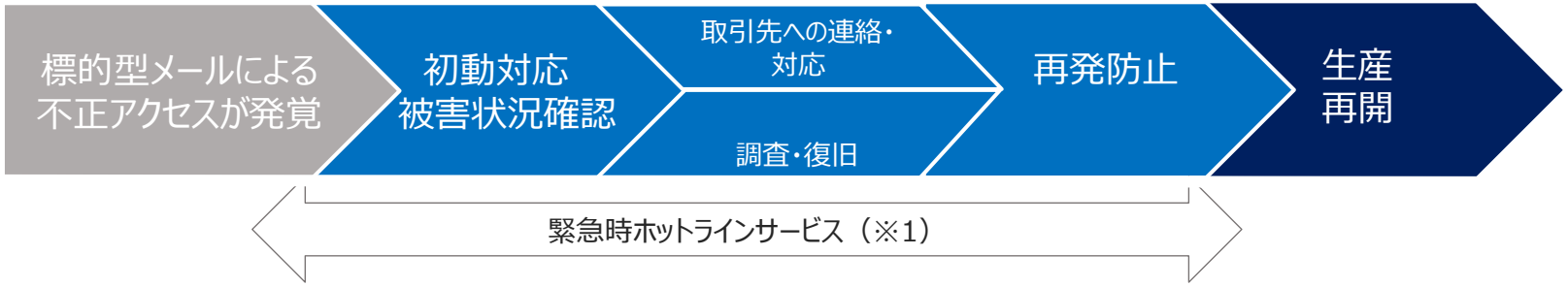
本事例で想定している主な対応と損害額

■パソコン・サーバのフォレンジック調査・復旧：400万円
■関連会社対応にかかる弁護士相談：150万円
■営業停止に伴う喪失利益の発生：300万円

合計850万円

上記以外に主に以下の対応が必要となることも想定されます。
・再発防止

対応の流れ



（※1）お客様に発生した様々なサイバーリスクに関するトラブルやインシデントについて、専門の担当者がご支援を実施するサービスを提供します。詳細は代理店または弊社までお問合せください。

TOKIO MARINE NICHIDO

3．想定事故例③（建設業）

イメージいただくための想定事例であり、事故内容を踏まえた対応や関連した損害額は、個社ごとに状況に応じた判断や対応する業者等によって異なりますのでご注意ください。なお、損害額は保険金とは異なります。
（保険金の額は損害額を踏まえ契約内容に従って決まります。）

会社概要

年間売上高：1億円
従業員数：10名

事故内容

従業員のパソコンがウイルス感染し、過去に送受信したメールが不正に閲覧される・流出するなどして、取引先に対して不審なメールを発信してしまった。

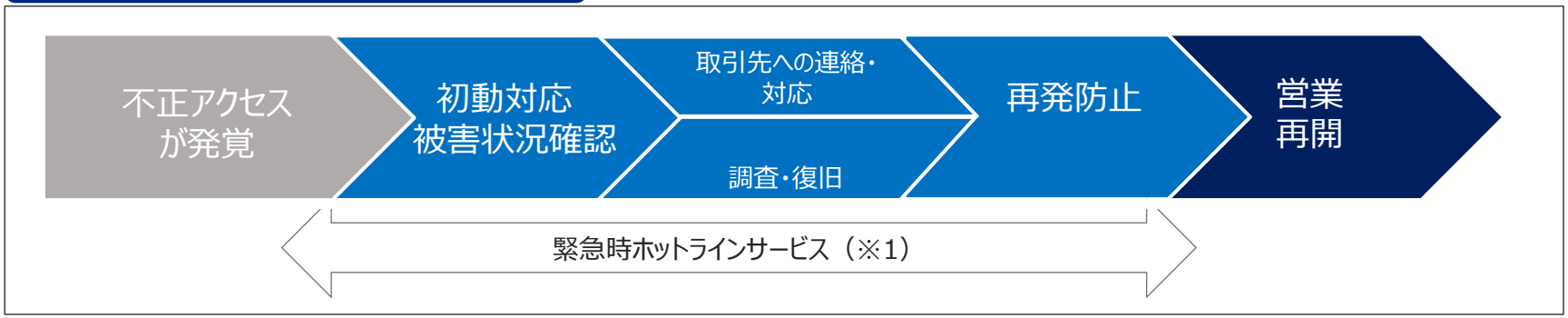
本事例で想定している主な対応と損害額

■パソコン・サーバのフォレンジック調査・復旧：1,000万円
■取引先対応にかかる弁護士相談：150万円

合計1,150万円

上記以外に主に以下の対応が必要となることも想定されます。
・再発防止

対応の流れ



（※1）お客様に発生した様々なサイバーリスクに関するトラブルやインシデントについて、専門の担当者がご支援を実施するサービスを提供します。詳細は代理店または弊社までお問合せください。

TOKIO MARINE NICHIDO

Ⅲ.サイバーリスク保険の補償内容

１．サイバーリスク保険の２つの補償
２．サイバーセキュリティ事故対応費用に関する補償
３．サイバーリスク保険の補償概要

１．サイバーリスク保険の２つの補償

サイバーリスク保険は、次の２つの補償により、事業活動を取り巻くサイバーリスクを包括的に補償します。

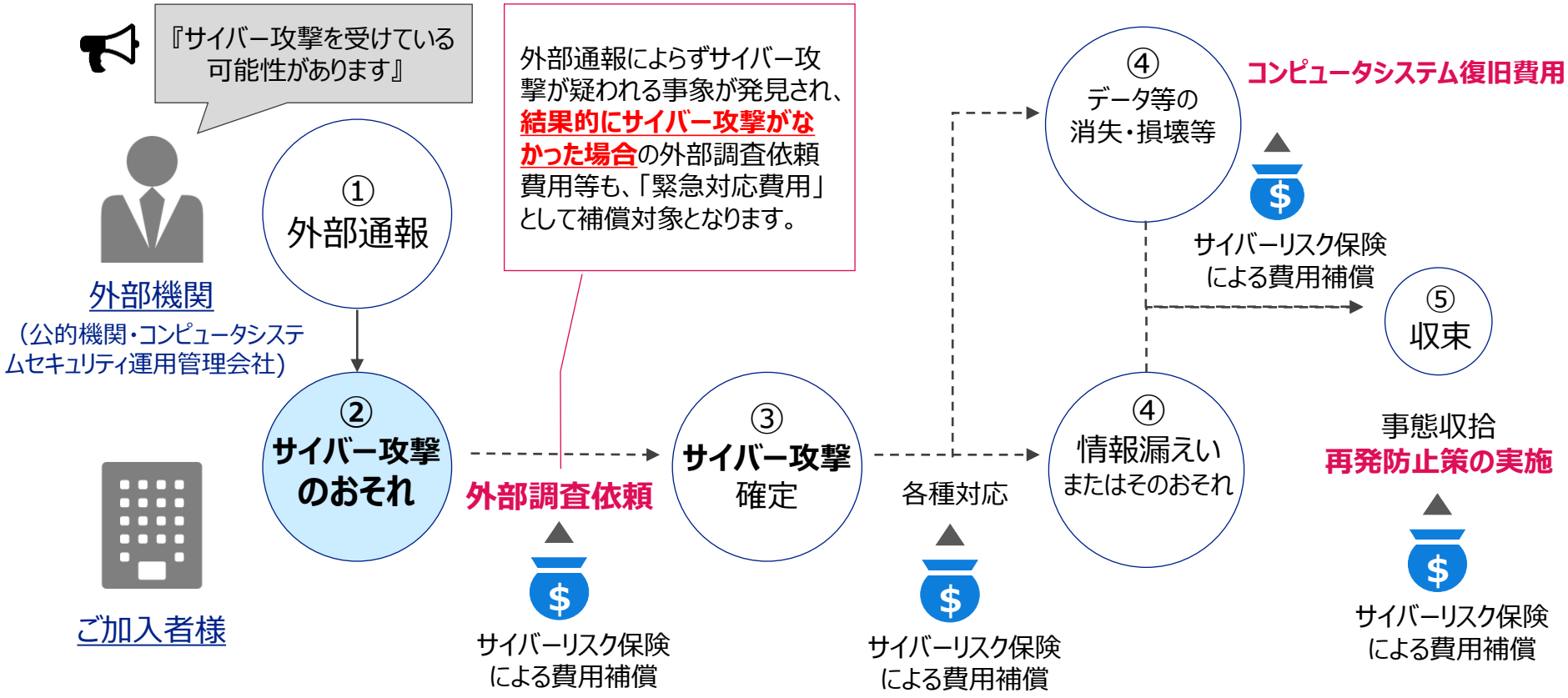
自社コンピュータシステムの所有・使用・管理等に起因して発生した他人の事業の休止または阻害や情報漏えいまたはそのおそれ、人格権・著作権等の侵害について、被保険者が法律上の損害賠償責任を負担することによって被る損害を補償します。

情報漏えい、サイバー攻撃等に起因して一定期間内に生じたサイバー攻撃対応費用・再発防止費用等や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。

TOKIO MARINE NICHIDO

2．サイバーセキュリティ事故対応費用に関する補償

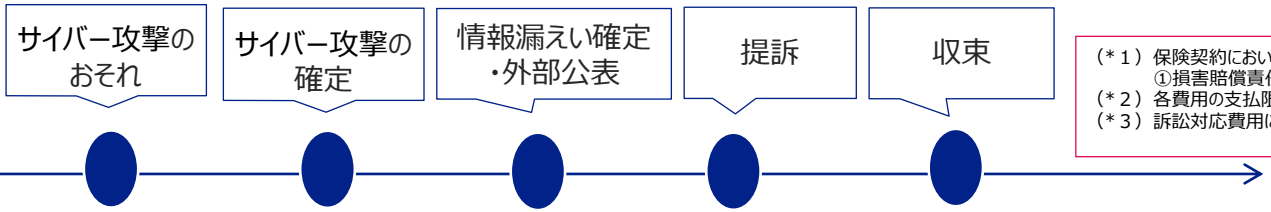
下記のような事故発生から収束までの一般的な対応フローにおいて、各種費用をトータルで補償します。



期待効果

- ✓ 外部調査依頼費用：早期段階での十分な調査による被害の拡散防止
- ✓ コンピュータシステム復旧費用：事業活動の早期再開
- ✓ 再発防止費用：情報セキュリティ体制の整備による将来的な被害の防止

3．サイバーリスク保険の補償概要



（＊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。
（＊２）各費用の支払限度額は、費用全体での支払限度額（最大5,000万円）の内枠で適用されます。
（＊３）訴訟対応費用については１請求となります。

検知	初動対応	対応	事態収拾	再発防止
			争訟対応（弁護士費用等）	
			損害賠償	
	影響調査・初動対応	原因・被害調査		
		データ・コンピュータシステム復旧		
			コールセンターの設置、記者会見、見舞品の購入	
				再発防止策の計画・実行
			訴訟対応	

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。

支払限度額（＊１）（1請求・保険期間中）
最大**5億**円

2 各種費用に関する補償

支払限度額（＊２）（1事故（＊３）・保険期間中）

（結果としてサイバー攻撃が生じていなかった場合）

- 緊急対応費用
  サイバー攻撃が疑われる突発的な事象が発見された場合に、損害の発生または拡大の防止のために支出したサイバー攻撃の有無の確認費用等を補償します。
  緊急対応費用 **1,000万**円（縮小支払割合90%）

（サイバー攻撃が生じていた場合、または、結果としてサイバー攻撃は生じていなかったがそのおそれが外部通報によって発見されていた場合）

- サイバー攻撃対応費用
- 原因・被害範囲調査費用
- 相談費用（弁護士費用、コンサルティング費用、風評被害拡大防止費用）

(A) 5000万円
または
(B) 3,000万円（縮小支払割合90%）（＊4）

- コンピュータシステム復旧費用
  消失、改ざん等の損害を受けたデータ、ウェブサイトの復旧費用、損傷したサーバ等のコンピュータシステムの復旧費用を補償します。

3,000万円

- その他事故対応費用
  コールセンターの設置、記者会見、見舞金支払い等、事態の収拾に係る費用を補償します。

うち、個人情報漏えい見舞費用 **1名1,000円**
うち、法人見舞費用 **1法人5万円**

- 再発防止費用
  事故の再発防止に係る費用を補償します。
  （外部機関による認証取得のための費用等）

3,000万円（縮小支払割合90%）

- 訴訟対応費用
  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

最大5000万円

(*4) (A) セキュリティ事故の発生またはそのおそれの事実が公表等の措置により客観的に明らかになった場合
(サイバー攻撃対応費用については、かつ、結果としてサイバー攻撃が生じていた場合)
(B) セキュリティ事故のうち（A）以外の場合および風評被害事故の場合

※ 上記条件は、「5億円プラン」にご加入頂いた場合のものです。詳細は、保険約款でご確認ください。

TOKIO MARINE NICHIDO

ご高覧ありがとうございました。
ご検討の程、何卒よろしくお願い申し上げます。

本保険に関するお問い合わせは、下記までお願いいたします。

取扱代理店　キューアンドエー株式会社（弥生会員様向けサイバー保険相談窓口運営会社）

（ＴＥＬ）0120-008-588
（受付）平日9:00-17:00（土日･祝日、年末年始は休業）

24T-001336　2024年10月作成

東京海上日動火災保険株式会社