御中

簡易リスク診断結果のご報告

報告書作成日

To Be a Good Company

東京海上日動

このたびは、弊社の「簡易リスク診断サービス」をご利用いただき、ありがとうございます。

先日ご回答いただきました内容に基づき、簡易リスク診断の結果をご報告いたします。
ご不明な点がございましたら、巻末のお問い合わせ先までご連絡ください。
あわせて弊社「サイバーリスク保険」につきましてもご検討賜りますようお願いいたします。
今後とも、何卒よろしくお引立ての程お願い申し上げます。

◆　簡易リスク診断サービスについて

「簡易リスク診断サービス」では、次の２種類の診断を行っております。

定性リスク診断

専用のヒアリングシートにご記入いただいた内容をもとに、「セキュリティ全般」「ネットワーク・セキュリティ」「クライアント・セキュリティ」「サーバー・セキュリティ」「セキュアな環境・施設・オフィス」の５つの観点から、貴社のセキュリティ体制について簡易評価いたします。

定量リスク診断

専用のヒアリングシートにご記入いただいた内容をもとに、一定のシナリオに基づいたサイバーリスクに関する予想損失額を簡易算出いたします。

ご注意事項

◇「定性リスク診断」「定量リスク診断」のいずれか一方の質問項目のみをご回答いただいている場合は、ご回答いただいたもののみのご報告を記載しております。

◇本診断結果は、簡易な質問項目に基づく「簡易リスク診断結果」となります。
より詳細な診断やその他のサービスをご希望の場合は、巻末記載の「専門事業者紹介サービス」をご利用ください。東京海上日動サイバーリスク情報センターより、貴社のご希望に応じた専門事業者をご紹介いたします。

◇本診断結果は、貴社におけるすべてのサイバーリスクを洗い出したものではなく、他にリスクが存在しないことを保証するものではありません。また、貴社においてサイバーリスクのおそれがないことを保証するものではありません。

◇貴社の事業が多岐にわたる場合は、主な事業で診断させていただいております。

定量リスク診断結果

貴社のサイバーリスク予想損失額につきまして、以下のとおり定量リスク診断結果をご報告いたします。

ご注意	・本診断結果は、貴社におけるサイバーリスクをすべて網羅したものではありません。 ・本診断結果の予想損失額は、すべて仮定の条件に基づいて算出されたものであり、サイバー攻撃時の損失額を保証するものではありません。実際の損失額や必要となる費用は、個別の事案ごとに大きく異なります。 ・予想損失額の算出にあたっては、消費税等は考慮しておりません。 ・本紙の用語の定義・表記は、保険約款上のものではなく、一般的なものとなります。 ・予想損失額の算出ロジックについては、「＜サイバーリスク＞定量リスク診断ガイドブック」をご参照ください。

想定するシナリオ　サイバー攻撃のおそれ

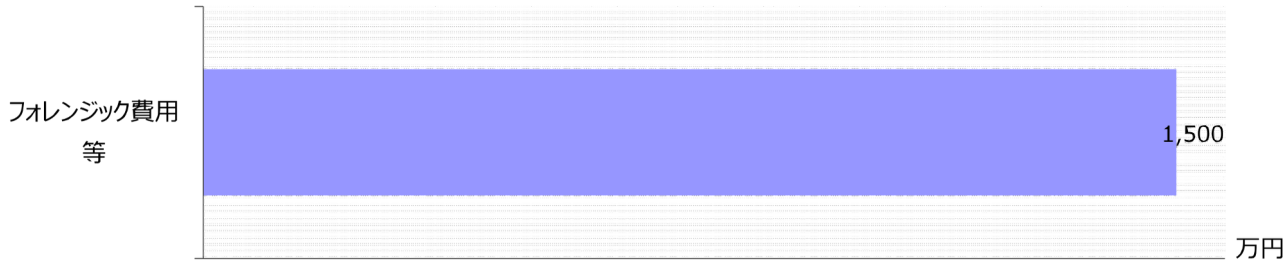
ITセキュリティ向上に努める公的機関（*）から会社に、「貴社と外部に不審な通信が確認された」旨の連絡があった。社内のシステム部門が調査したところ、1週間前に不審なメールが従業員宛に届き、一部の従業員が誤って添付ファイルを開封したことが判明した。システム部門がすぐに社内ネットワークと外部ネットワークを遮断した。社内の端末がマルウェアに感染した可能性があるが、実際にサイバー攻撃の被害にあったかどうか、被害にあったとすればその範囲や規模は不明である（どのような社内データ・システムがアクセスされ、窃取・改ざん・破壊を受けたか分からない状態）。被害状況を明らかにするため、外部の専門事業者に「フォレンジック調査」等を依頼する。

＊ こうした機関の例として、JPCERT/CCやIPAなど。
JPCERT/CC：　一般社団法人 JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center）
IPA：　独立行政法人 情報処理推進機構（Information-technology Promotion Agency, Japan）

予想損失額

予想損失額（合計）　　**15,000,000　円**

予想損失額（明細）　　以下のとおりです。



サイバー攻撃の有無およびそれによる被害を明らかにするためには、フォレンジック等の専門的なスキルが必要（費用がかかる）

ポイント

サイバー攻撃のおそれ　何らかの不正アクセスを受けた可能性はあるが、実際の不正アクセスの発生有無、被害の有無や規模は不明であること。

サイバー攻撃　何らかの不正アクセスを受け、実際に被害が生じていること。

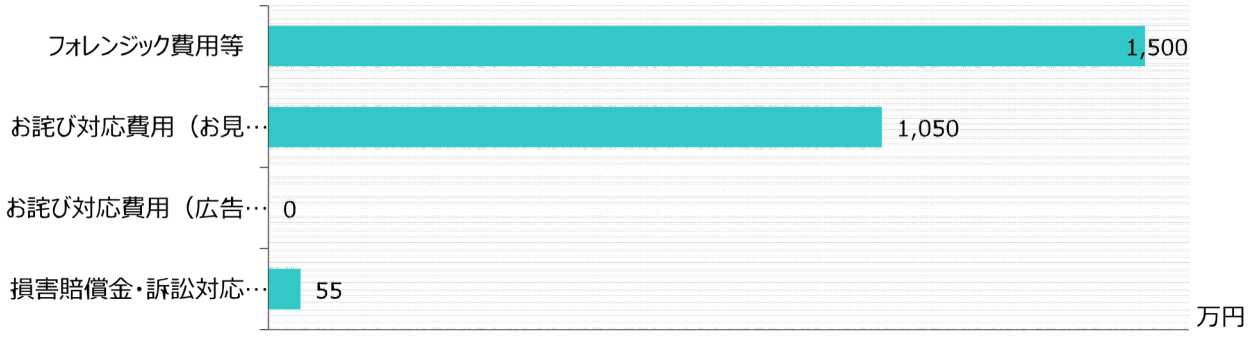
想定するシナリオ 個人情報の漏えい

お客様より、「貴社にしか記載していない個人情報が漏れているようである。ダイレクトメールや勧誘の電話がかかってきており、原因調査と早急な対処をお願いする」旨の電話があった。その後、他のお客様からも同様の電話が入った。
個人情報漏えいの痕跡について自社内で把握できなかったため、外部の専門事業者に依頼し、調査を実施した。その結果、自社従業員が標的型メール攻撃を受け、誤ってメールの添付ファイルを開封したことが判明した。社内に侵入したウイルスにより、外部から社内のお客様情報のデータベースにアクセスされ、すべてのお客様の個人情報が窃取されたと考えられる。詳細調査の結果、お客様の個人情報漏えいの事実が確定した。これにより、お客様への通知とお詫び対応（見舞金送付を含む）、広報対応、損害賠償請求等の対応が必要となった。

予想損失額

予想損失額（合計） **26,050,000 円**

予想損失額（明細） 以下のとおりです。



想定するシナリオ Web改ざん

お客様より、「最近ウイルスに感染したのだが、外部の専門事業者に調査を依頼したところ、貴社のWebサイトにアクセスしたことが原因のようである。事実確認と調査費用の負担をお願いする」旨の電話があった。 急遽、自社でも外部の専門事業者に依頼し、調査したところ、自社のWebサーバが改ざんされ、アクセスしたユーザーがウイルスに感染することが判明した。あわせて、改ざんの原因が、自社のWebサーバの重大な脆弱性の放置にあることも判明した。
ただちにWebサイトおよびサーバを停止した。Webサイトの復旧までに約10日を要し、この期間のWebサイト経由の売上・利益が失われた。また、この期間中、オフラインでのお客様対応に追われ、臨時の人件費等が発生した。さらに、ウイルスに感染したことにより、コンピュータ端末のソフトウェアの再購入を余儀なくされたお客様の一部から損害賠償を請求された。

予想損失額

予想損失額（合計） **17,037,000 円**

予想損失額（明細） 以下のとおりです。

想定するシナリオ DoS攻撃

会社の端末が突然使用不能となった。原因を調査したところ、外部からのDDoS攻撃（Distributed Denial of Service attack）により、会社の基幹システムを運用するサーバ等が停止したようである。また、攻撃は海外にある「DDoS攻撃」代行サイト（*）が発信源であることが判明した。
DDoS攻撃は丸一日近くにおよび、攻撃が終わった後も引き続きサーバに支障が生じ、会社業務に影響が及んだ。この期間中、会社の重要システム（メールシステム、経理・計上システム等）が使えず、個別のお客様との商談等についての電子ファイルにアクセスできなかったため、オフラインでの対応に追われた。最初の攻撃が終息した後も、短時間のDDoS攻撃が繰り返し発生した。

＊ こうしたサイトは「サーバへの負荷の検証」の名目であるが、実質的にはDDoS攻撃サイトとなるケースも少なくない。1時間数ドル程度で対象サーバにDDoS攻撃を行うことが可能である。

予想損失額

予想損失額（合計） **17,593,000 円**

予想損失額（明細） 以下のとおりです。

ポイント

DoS攻撃
（Denial of Service attack）
対象のサーバや回線に過剰な負荷をかけ、サービスの正常な提供を妨害する攻撃。

DDoS攻撃
（Distributed Denial of Service attack）
DoS攻撃のうち、攻撃元がネットワーク上に分散している攻撃。マルウェア等に感染した数多くのコンピュータ端末から攻撃が行われることから、対処が難しく、真の攻撃元を特定にしにくい。

予想損失額の内訳の説明

フォレンジック費用等	サイバー攻撃を受けたかどうか、受けた場合の被害の程度を明らかにするために、外部の専門事業者に委託する調査の費用。調査範囲や規模によって費用が変動する。（調査対象は感染したコンピュータ端末、サーバ、場合によっては通信記録・ログなど）
お詫び対応費用（お見舞金）	個人情報が漏えいしたお客様すべてに対するお見舞金（金券）の送付とその諸経費。
お詫び対応費用（広告費用）	新聞紙上でのお詫び広告の掲載に関わる費用。
損害賠償金・訴訟対応費用	損害賠償金とは、被害者が事故に関する損害賠償を請求した場合の金額。情報漏えいにおける賠償額は漏えいした情報の「量」と「質」（どんな情報か）によって変動する。 訴訟対応費用とは、賠償請求に関する弁護士費用で、着手金と報酬金で構成される。弁護士費用は、損害賠償請求額等によって変動する。
休業損失	サイバー攻撃によるWebサーバ・Webサイトの停止により、業務が停止し、本来得られるはずだったが喪失された利益の額。
営業継続費用等	Webサーバの停止により、通常業務を継続するために必要な措置をとった場合の費用。（手動やオフラインでの業務継続のための超過人件費等）

【ご参考】 貴社のご回答内容

ご回答日:　2024/6/6

本定量リスク診断は、貴社にご回答いただきました次の内容に基づき実施しております。

ヒアリング項目		ご回答	
Ⅰ．貴社について教えてください。			
1 本社が所在する都道府県を教えてください。		東京都	
2 コンピュータ端末（パソコン）は何台程度ありますか？	約	[redacted]	台
3 従業員は何名程度ですか？（正社員以外の従業員を含む）	約	[redacted]	名
Ⅱ．貴社の事業について教えてください。			
1 貴社の規定年間営業日数を教えてください。		[redacted]	日
2 貴社の規定勤務時間を教えてください。		[redacted]	時間
3 貴社の年間の営業利益を教えてください。		[redacted]	円
4 貴社の年間の経常費（人件費、システム維持等）を教えてください。		[redacted]	円
5 貴社の年間の売上高を教えてください。		[redacted]	円
6 貴社の最も売上高が高い月の月間売上高を教えてください。 ※月間格差が小さい場合、5の回答を12で割り戻した数を入力してください。		[redacted]	円
7 貴社の売上高のうち、どの程度がWebサイトを経由したものですか？	約	[redacted]	%
8 Webサイト1日あたりのアクセス数は何件程度ですか？（アクセスページ数ではなく、アクセス元IP数）	約	[redacted]	件
Ⅲ．貴社が保有する個人情報について教えてください。			
1 貴社が保有する個人情報の数はどの程度ですか？	約	[redacted]	名様分
2 貴社が保有する個人情報はどのような情報が含まれますか？ 次の項目のうち、含まれるものは「YES」、含まれないものは「NO」でご回答ください。			
① 氏名			
② 住所			
③ 生年月日			
④ メールアドレス			
⑤ ログインアカウント			
⑥ 免許証番号			
⑦ 社会保険・年金関連番号			
⑧ 電話番号			
⑨ マイナンバーおよび準ずる個人番号			
⑩ 身体情報（身長、体重、スリーサイズ等）			
⑪ 生体情報（指紋、顔認識情報等）			
⑫ 病歴・健康状態・レセプト情報			
⑬ 位置情報			
⑭ 賞罰歴・違反歴			
⑮ 試験結果・成績			
⑯ 政治思想・人種・信条・社会的身分			
⑰ 労働組合への加盟状況			
⑱ 本籍地			
⑲ 口座番号のみ、クレジットカード番号のみ			
⑳ パスポート番号			
㉑ パスワード情報			
㉒ 商品・サービスの購入履歴			
㉓ 年収・所得・資産・納税（区分）情報			
㉔ 与信・借入記録			
㉕ クレジットカード番号、有効期限			
㉖ 口座番号＆暗証番号			
㉗ 前科前歴・犯罪歴			
㉘ 与信ブラックリスト			
Ⅳ．貴社の情報漏えい時等の対応について教えてください。			
万が一、お客様情報がもれた場合等はどのような対応を行う予定ですか？当てはまるものすべてに「YES」でご回答ください。			
① 自社ホームページ上での公表			
② 新聞・雑誌等での広告によるお詫び記事掲載			
③ 新聞広告によるお詫びを実施する場合は、全国紙を利用される予定ですか？			
④ お客様へのお詫び状の送付			
Ⅴ．会社の重要サーバ停止時の対応について教えてください。			
重要システムが使えない状況下でも、業務を継続するため、お客様への連絡や個別の商談・納品等を対応する必要があり、 従業員の労働時間が通常より増加することが予想されます。 従業員の増加労働時間を算出する際、貴社の事業ではどちらの方が適切ですか？			
1 **＜顧客数ベース＞** お客様への対応は個別性が高いため、現在商談進行中の顧客数等による。BtoBビジネスに多い。 **＜従業員数ベース＞** お客様の数がきわめて多いため、代替業務は顧客数に関係なく、全従業員で分担しながらシステマチックに対応する。 BtoCビジネスに多い。			
2 上記１．で＜顧客数ベース＞とご回答した方のみお答えください。			
(1) 自社のシステム停止による影響を受けるため、至急で連絡をとる必要がある顧客は何社程度ですか？	約	[redacted]	社
(2) 自社のシステム停止による影響を受けるため、連絡以上の対応をとる必要がある顧客は何社程度ですか？ （たとえば、今日・明日の商談・契約・納品の顧客は何社程度ありますか？）	約	[redacted]	社

その他のサイバーリスク総合支援サービスのご案内

● 情報・ツール提供サービス（無料）

サイバーリスク保険
ご契約者様限定

サイバーリスク保険のご契約者様（希望者のみ）に、次のサービスをご提供いたします。

情報提供サービス	**サイバーリスクニュースのご提供** 直近に発生したインシデント（情報管理やシステム運用に関する保安上の脅威となる事象）の解説、サイバー攻撃の実態等のサイバー関連情報をご提供いたします。
	リスク情報誌のご提供 サイバー関連の詳細情報を掲載したリスク情報誌をご提供いたします。
	サイバーリスクセミナーの優先ご案内
ツール提供サービス	**教育支援ツールのご提供** 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）

サイバーリスク保険
ご契約者様限定

サイバーリスク保険のご契約者様（希望者のみ）に、次のサービスをご提供いたします。

ベンチマークレポートサービス	**サイバーリスクベンチマークレポートのご提供** お客様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、スコアリングした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。

● 専門事業者紹介サービス

どなた様でも
ご利用いただけます！

弊社ネットワークを活用し、お客様のニーズに合った専門事業者をご紹介いたします。

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。
インシデント発生時の紹介サービス	事故発生後の駆けつけ支援、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。

ご高覧ありがとうございました。

本件に関するお問合せは、下記までお願いいたします。

<保険会社>

東京海上日動火災保険株式会社

（担当）　東京新都心支店専業チーム

（所在地）　〒151-8560　東京都渋谷区代々木2-11-15　新宿東京海上日動ビル５階

（TEL）　03-3375-8258

（FAX）　050-3385-6759

To Be a ***Good Company***

TOKIO MARINE NICHIDO 東京海上日動