ABC株式会社　御中

2020年版

サイバーリスク簡易診断プラス レポート

アンケートご回答日：　2020年4月1日

SAMPLE

損害保険ジャパン株式会社

SOMPOリスクマネジメント株式会社

【本レポートの取扱いについて（重要）】

1．本レポートの使用責任と有効性
（1）本レポートは、貴社に対し、意思決定の参考情報を提供することを意図しており、使用に関する責任は貴社に帰属します。
（2）本レポートの一部を抜粋しての使用は、本レポートの有効性を毀損する可能性があります。
（3）本レポートは、アンケートご回答日現在の状況に基づくものです。

2．網羅性
本レポートはあくまでも限られた項目数による自己申告にもとづく診断であり、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の保証や貴社においてサイバーリスクが顕在化するおそれがないことを保証するものではありません。

3．免責
損害保険ジャパン株式会社・SOMPOリスクマネジメント株式会社は、助言を行う立場にすぎず、本レポートおよび口頭説明に関連して何らかの損害が発生した場合であっても、損害保険ジャパン株式会社・SOMPOリスクマネジメント株式会社、その代理人および従業員は、一切の責任を負わないものとします。

はじめに

近年、顧客情報や機密情報の漏えい、ウェブサイトの改ざん、DDoS攻撃によるシステム障害やサービス停止などが企業を取り巻くリスクとして軽視できないものとなっています。さらに、サイバー攻撃は標的型攻撃に代表されるようにその手口が巧妙かつ高度化してきており、これまでの対策では必ずしも有効ではないケースも増えてきています。

このような状況を踏まえると、これらの新しい脅威であるサイバーリスクにも対応できるよう実効性のあるサイバーセキュリティ態勢の整備・見直しが喫緊の課題と言えるのではないでしょうか。

そこで、本診断（以下「本レポート」という）では、貴社のサイバーリスクへの対応について、組織的・人的・物理的・技術的な観点からみた対応状況を簡易評価するとともに、サイバーリスクが顕在化した場合の想定損害額を算出しています。

本レポートを通じて、貴社に内在するサイバーリスクに対し、どこから・どのように取り組むのか、またどの程度まで対策を実施すべきかなどをご認識いただくとともに、今後のサイバーセキュリティ態勢の整備・見直しを進める際の一つの指標としていただければと思います。

本レポートが貴社のご発展の一助となりましたら幸甚です。

目次

1. 総合評価

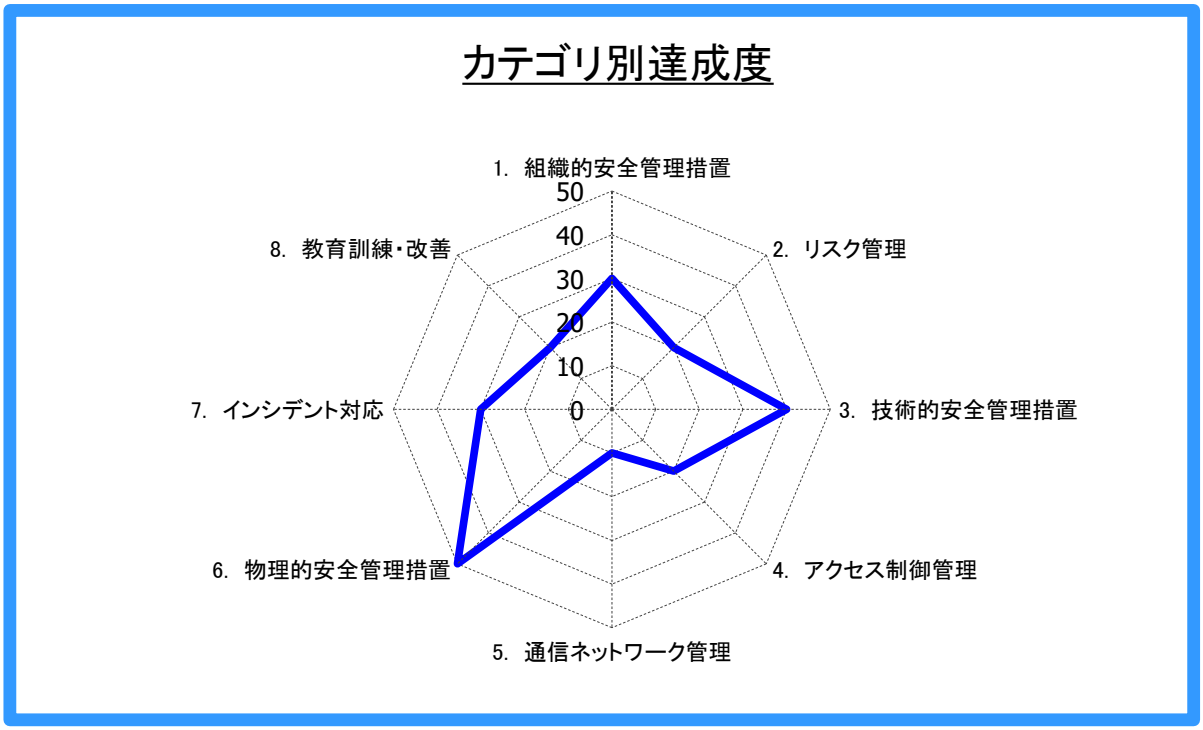
貴社のサイバーリスクに対する対応状況は以下のとおりです。
※各カテゴリの診断結果および対応アドバイスは「2. 診断結果」をご参照ください。

☆☆☆

（最高ランクは☆が5つです）

個別にコメントが記載されます。

（注）☆☆☆☆☆は「総点が320点以上」、☆☆☆☆は「総点が240点以上320点未満」、☆☆☆は「総点が160点以上240点未満」、☆☆は「総点が80点以上160点未満」、☆は「総点が80点未満」を示しています。



カテゴリ毎の評点

1. 組織的安全管理措置	30
2. リスク管理	20
3. 技術的安全管理措置	40
4. アクセス制御管理	20
5. 通信ネットワーク管理	10
6. 物理的安全管理措置	50
7. インシデント対応	30
8. 教育訓練・改善	20
計	220

【想定損害額】

貴社でサイバーリスクが顕在化した場合の貴社の規模および業種における想定損害額は、以下のとおりです。

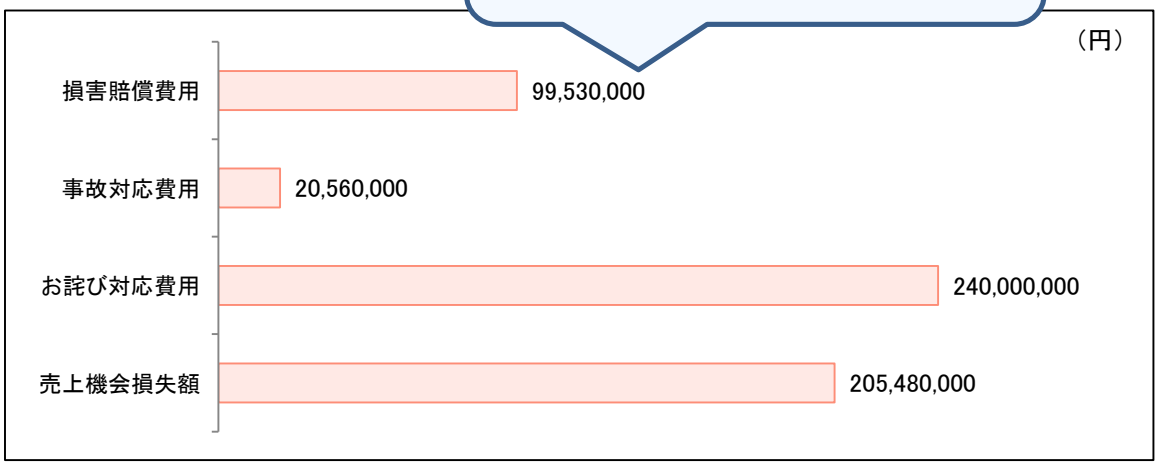
＜ご注意＞

- □ 本想定損害額は、ご回答いただきました内容に基づき簡易算出したものであり、貴社がサイバー攻撃を受けた際の最大の損害額を表した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。
- □ 貴社の事業が多岐にわたる場合は、主な事業で簡易算出させていただいています。
- □ 本結果は、貴社におけるすべてのサイバーリスクを網羅したものではなく、5つのシナリオ（情報漏えい、金融取引、恐喝、DDoS攻撃、IT停止）に限定させていただいており、今回想定したシナリオ以外にもサイバーリスクが発生する可能性があります。
- □ 本算出において使用する用語の表記・定義は、保険約款上のものではなく、一般的なものとなります。

貴社のサイバーリスクが顕在化した場合の想定損害額

565,570,000 円

業　　種：機械、電気、電子製造
従 業 員数：100人以下
前年売上高：15,000百万円



＜想定損害額の内訳の説明＞

損害賠償費用(※1)	情報漏えいやシステム障害・停止に起因して損害賠償を請求された場合の損害賠償金および賠償請求に関する訴訟対応費用
事故対応費用(※2)	サイバー攻撃を受けたかどうかや攻撃を受けた場合の影響範囲や原因を調査するための費用（フォレンジック費用）やデータ・ソフトウェアの復旧費用、応急処置や再発防止のためのセキュリティ強化費用
お詫び対応費用(※3)	個人情報が漏えいしたお客さまに対するお詫び文書やお詫びのしるし（お見舞金：金券）の送付とその諸経費
売上機会損失額(※4)	サイバー攻撃に起因してECサイトや社内システムの停止によって、業務が停止し、本来得られるはずだった売上機会の損失額

2. 診断結果

2．1　組織的安全管理措置（1／2）

本カテゴリの診断結果として、アンケート項目ごとに「貴社の回答」および「アドバイスコメント」を掲載していますので、ご参照ください。

Q01　サイバー攻撃等のサイバーリスクを経営リスクの一つとして認識し、サイバーセキュリティ対応方針を策定して組織外に宣言していますか。

貴社の回答：　〇（はい）
アドバイスコメント：
サイバー攻撃等の増加によって、サイバーリスクが経営リスクの一つとして認識されつつあり、サイバーリスクに対する行動指針を示すことが重要です。
そのため、自組織がサイバーリスクに対してどのように取り組むのかを示したサイバーセキュリティ対応方針を策定して、組織外に宣言することを推奨します。

Q02　情報セキュリティを統括する役職（CISO等）を任命する等、定期的に組織としてセキュリティ状況を把握できる体制を整備していますか。

貴社の回答：　×（いいえ）
アドバイスコメント：
サイバーリスクにおける管理体制が整備されていない場合、サイバーリスクの把握ができず、万が一サイバー攻撃を受け、事業の継続性に支障が生じるようなシステム停止等の判断が必要な局面においても適時・適切な準備ができない可能性があります。
そのため、CISOを任命して必要な権限を付与する等、定期的にセキュリティ状況を把握できる組織体制を整備しておくことが望まれます。

Q03　自社にある情報（個人情報・機密情報）や情報システム等の資産を適切に管理するためのルールを整備していますか。

貴社の回答：　×（いいえ）
アドバイスコメント：
自社にある情報（個人情報・機密情報）や情報システム等の資産を管理できていない場合、自組織の外部・内部からのサイバー上の脅威に対して適切に対処できない可能性があります。
そのため、自社にある情報（個人情報・機密情報）や情報システム等の資産を適切に管理するためのルールを整備しておくことが望まれます。

Q04　派遣を含む全ての従業員に対し、採用・退職の際に本人または派遣会社等と守秘義務に関する書面を取り交わすことで、情報セキュリティに関する就業上の義務を明確にしていますか。

貴社の回答：　〇（はい）
アドバイスコメント：
従業員の就業上の義務として、業務上取扱う情報資産を適切に保護する義務を明確にし、それを意識付けさせることが重要です。
そのため、派遣を含む全ての従業員に対し、採用・退職の際に本人または派遣会社等と守秘義務に関する書面を取り交わすことことを推奨します。

3. 参考資料

3．1　【参考】最近のサイバー攻撃等による情報漏えい事例（公表資料より）

シナリオ	業種	時期	概要	事後対応・事業への影響
情報漏えい	教育通信	2014年	システム開発・運営を行っているグループ会社の業務委託先の再委託先社員が、3,504万件分の個人情報を不正取得し、名簿業者への売却した。	■お詫び対応の原資として、200億円を準備した。 ■漏えいが確認された顧客にお詫びと報告の手紙を送付し、お詫びの品として図書カード500円の金券/基金への寄付のいずれかの選択を用意した。 ■被害者の会集団訴訟による係争中（2016年8月時点） 原告1,170名　請求額原告一人あたり55,000円、総額6,435万円
	サービス	2015年	サービス運営委託先のサービスサイトが不正アクセスされ、6,187件分の個人情報（他社の個人情報含め総数12,014件）が漏えいした。	■サイトからのサービス導入を中止した。 ■サービス優待券進呈/クーポン券との交換、お詫びとして1,000円の金券を配布した。
	航空	2014年	ウイルスに感染した3台の業務端末が顧客情報管理システムと交信して4,131件分の個人情報が外部に流出した。	■ギフト券への特典交換サービスを一時停止した。 ■情報漏えいのお詫びとして1名あたり500円の金券を配布した。
	製造（食品）	2015年	ウェブサイトへの不正アクセス（SQLインジェクション：データベースへの不正操作による攻撃）により、約21万件の個人情報が漏えいした。	■ウェブサイトでの通販・工場見学予約機能の利用を停止し、全面再開まで約3ヵ月かかった。 ■お詫びとして500円の金券を配布した。
	製造（半導体）	2014年	提携先の元従業員が不正に技術に関する機密情報を持ち出して、韓国の同業者に提供した。	■不正競争防止法に基づく損害賠償等請求で国内事業者が韓国同業者と2億7,800万米ドル（330億円）の和解金支払いで合意した。 ■和解を機に協業拡大を合意した。
	小売	2013年	ソフトウェアの脆弱性を利用したウェブサーバーへの不正アクセスで、オンラインショップ顧客の2,059件分のクレジットカード情報が漏えいした。	■流出した可能性のある最大12,036件（※実際の件数は2,059件）に対して、1,000円分の商品券を配布した。 ■クレジットカード不正利用最大損害想定額305万3,000円 ■オンラインショップ停止およびアクセス遮断し、再開まで約5ヵ月かかった。
DDoS	小売	2016年	通販サイトに大量のデータを送りつける不正な通信（DDoS攻撃）によって、インターネットサービスが断続的に繋がりにくい状態が続いたため一時閉鎖した。	■復旧までの約2日間サイトを閉鎖した。
IT停止	運送	2014年	外部からの不正アクセスでサイトが改ざんされ、閲覧すると仕掛けられた不正なウイルスに感染する可能性があり、サイトを一時閉鎖した。	■17日間のサイト閉鎖により機会損失が1億円程度になった。
	サービス	2012年	顧客企業が利用していたレンタルサーバー約5,700台のデータをほぼ消失させる大規模障害が発生した。	■親会社が損害賠償金支払いなどのための特別損失「システム事故関連損失」として12億円を計上した。
恐喝	医療	2014年	米国の病院で院内ネットワークで共有する電子カルテシステムがウイルス（ランサムウェア）に感染し、ファイルが暗号化されたため、電子カルテシステムが動作しなくなり診療不能になった。	■暗号化を解除するために約1万7,000ドル（192万円）相当の仮想通貨であるビットコインを攻撃者に支払い暗号解読キーを入手した。

３．２　【参考】貴社のアンケート回答結果　１／３

貴社のセキュリティ対策に関するご回答内容を掲載いたします。なお、未回答の場合には、「－」を表記しています。

番号	アンケート項目	回答結果
Q01	サイバー攻撃等のサイバーリスクを経営リスクの一つとして認識し、サイバーセキュリティ対応方針を策定して組織外に宣言していますか。	○
Q02	情報セキュリティを統括する役職（CISO等）を任命する等、定期的に組織としてセキュリティ状況を把握できる体制を整備していますか。	×
Q03	自社にある情報（個人情報・機密情報）や情報システム等の資産を適切に管理するためのルールを整備していますか。	×
Q04	派遣を含む全ての従業員に対し、採用・退職の際に本人または派遣会社等と守秘義務に関する書面を取り交わすことで、情報セキュリティに関する就業上の義務を明確にしていますか。	○
Q05	各種団体が提供するサイバーセキュリティに関する注意喚起情報を定期的に入手していますか。	○
Q06	自社で保護すべき重要な資産（情報やシステム等）を網羅的に特定し、定期的にその内容を見直していますか。	○
Q07	重要な資産の取扱状況に応じて定期的にサイバーリスクを含む情報セキュリティにおけるリスク評価を行っていますか。	×
Q08	リスク評価の結果をもとに、適時かつ適切な対策を講じるための目標や計画を策定していますか。	×
Q09	系列企業やサプライチェーンのビジネスパートナーのセキュリティ対策状況を把握していますか。	×
Q10	ITシステム管理等の外部委託先へのサイバー攻撃を想定し、委託先のセキュリティを確保していますか。	○
Q11	不正プログラム（ウィルス、ワーム、トロイの木馬等）対策としてウィルス対策ソフトを導入し、必要なパターンファイルを更新していますか。	×
Q12	自社の端末やサーバ等で利用しているOSやアプリケーション等の脆弱性情報を確認し、必要なセキュリティパッチを適用していますか。	○
Q13	自社のWebサイト等に使用しているウェブアプリケーションのセキュリティ実装の実施状況を確認していますか。	○
Q14	情報システムやアプリケーション等を導入や変更する場合には、他の情報システムへの影響を考慮し、適切に環境設定やテスト等を行った上で導入していますか。	○
Q15	故障や誤操作などによって重要情報が消失しないように、重要な情報は定期的にバックアップを行っていますか。	○
Q16	業務利用している情報や情報システムは、重要度に応じて、必要なアクセス制限を行っていますか。	×
Q17	業務利用しているOSやアプリケーション等には、個人毎にアカウント（ID等）を設定していますか。	×
Q18	業務利用しているOSやアプリケーション等には、パスワード等の認証機能を設定し、パスワードポリシーを定めていますか。	○
Q19	雇用終了時や請負等の契約先との契約終了時等において、IDの発行・削除等のアカウント管理（アクセス権限の変更も含む）を速やかに行っていますか。	○
Q20	システム管理者がシステム操作を行うための特権アカウントの種類・付与対象者・付与人数を把握していますか。	×

4. 用語集

アイエスエムエス／ISMS（Information Security Management System）	
	企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組み。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系のことを指す。
アイティーエスエムエス／ITSMS（Information Technology Service Management System）	
	IT サービスを提供する企業が利用顧客のニーズに合致した適切なサービス提供を実現し、その運用の維持管理を行っていくための仕組みのこと。
アイディエス／IDS（Intrusion Detection System）	
	通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステム。ネットワーク上を流れるパケットを分析し、パターン照合により不正アクセスと思われるパケットを検出して、管理者に通知する。製品によっては疑わしい通信を切断するなどして防衛措置を講じる場合もある。
アイピーエス／IPS（Intrusion Prevention System）	
	サーバやネットワークへの不正侵入を阻止するツール。ネットワークの境界などに設置する専用の機器(アプライアンス)や、サーバに導入するソフトウェアなどの形で提供される。
ウイルス／Virus	
	広義：自己伝染機能・潜伏機能・発病機能のいずれかをもつ加害プログラムのこと。 狭義：他のファイルやシステムに寄生・感染（自己複製）する機能をもつプログラムのこと。
ウェブアプリケーションファイアウォール／WAF（Web Application Firewall）	
	ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護するソフトウェア、またはハードウェアのこと。脆弱性を修正するといったウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策。
キューエムエス／QMS（Quality Management System）	
	品質に関して組織を指揮し、管理するためのマネジメントシステムのこと。
シーサート／CSIRT（Computer Security Incident Response Team）	
	定められた範囲内のサイトに関するセキュリティインシデントについてコーディネーション、サポート、対応を行う組織のこと。
セキュリティパッチ／Security Patch	
	ソフトウェアに保安上の弱点(セキュリティホール)が発覚した時に配布される修正プログラム。セキュリティパッチは、ソフトウェア内でセキュリティホールの原因となっているファイルを、問題のないファイルに置き換える。
通信の暗号化	
	Webページの送受信データなどネットワークを通じてデータをやり取りする際、データを利用者以外にはわからなくするために、表記方法を変えること。
ディードスこうげき／DDoS攻撃（Distributed Denial of Service attack）	
	複数の攻撃元からコンピュータやネットワークに過剰な負荷をかけてホームページ等のサービス提供を妨害する攻撃のこと。


SOMPO ホールディングス
安心・安全・健康のテーマパーク