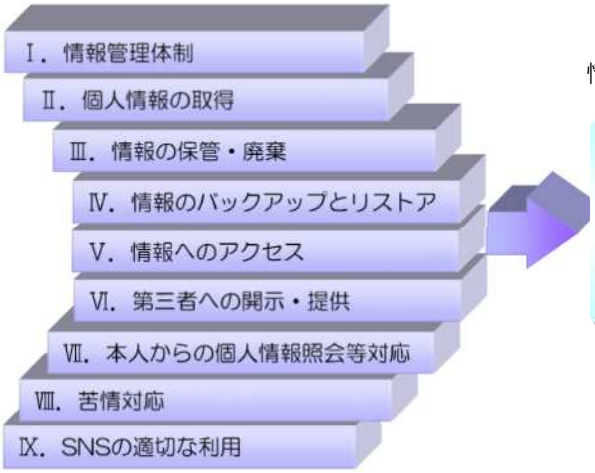
社会福祉協議会・社会福祉法人様 御中

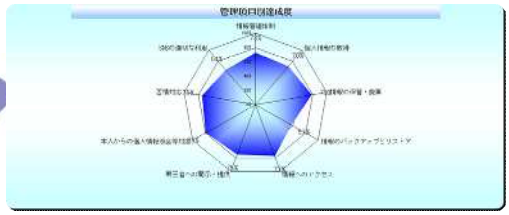
MS&AD
MS&ADインシュアランス グループ

情報セキュリティリスク診断用チェックリスト

この情報セキュリティリスク診断では、情報（個人情報及び営業秘密）の漏えいリスクならびに個人情報保護法、営業秘密管理指針対応に資する下記の9項目に関するご質問事項（全67項目）にご回答頂くことにより、弊社にて総合的な評価に基づき報告書を作成いたします。



情報セキュリティリスク診断評価報告書＜例＞



お手数ですが、各ご質問事項について、ご回答内容に該当する「1～2」または「1～3」の番号のいずれか一つを右欄に記載して下さい。

㈱インターリスク総研
三井住友海上火災保険㈱
公務第一部
公務室

Ⅰ．情報管理体制

(1) 情報の取扱いに関する基本方針・規程・ガイドライン等の社内規則がある。
1. 個人情報、営業秘密共にある　2. 一方のみある 3. ない　(1)

(2) 営業秘密に関して、組織内のどの情報が営業秘密であるかを具体的に指定している。
1. 文書で指定している　2. 口頭で指定している 3. 特に指定していない　(2)

(3) 情報管理に関する統括責任者（役員）が明確になっている。
1. 個人情報、営業秘密共になっている　2. 一方のみなっている 3. なっていない　(3)

(4) 情報毎に取扱責任者が明確になっている。
1. なっている　2. 一部なっている　3.なっていない　(4)

(5) 情報漏えいが発生した場合の、漏えいさせた本人に対する罰則を定めた社内規定がある。
1. ある　2. ない　(5)

(6) 情報漏えいが発生した場合の、漏えいさせた本人の監督責任者に対する罰則を定めた社内規定がある。
1. ある　2. ない　(6)

(7) 社内で保有している情報の種類・所在についてリスト等で台帳管理している。
1. 個人情報、営業秘密共にできている　2. 一方のみできている　3.できていない　(7)

(8) 社内で保有している情報の棚卸を年に1回以上実施している。
1. 実施している　2. 実施したことがある　3.実施していない　(8)

(9) 情報を取り扱う担当者に対して、誓約書を取り付けており、その書面は保管している。
1. できている　2. 一部できている　3.できていない　(9)

(10) 情報の取り扱いに関する社内規則、罰則について、全社員に対する教育を定期的に実施している。
1. 実施している　2. 実施したことがある　3. 実施していない　(10)

(11) 情報の取り扱いに関する社内規則・ルールの遵守状況を確認するために、定期的に監査を実施している。
1. 実施している　2. 実施したことがある　3. 実施していない　(11)

(12) 社内では、社員の身分を証明するもの（入館証や社員証等）の着用を義務付けている。
1. できている　2. 一部できている　3.できていない　(12)

(13) 情報が外部へ漏えいした際の対応手順書がある。
1. 個人情報、営業秘密共にある　2. 一方のみある 3. ない　(13)

Ⅱ. 個人情報の取得

(14) 個人情報の利用目的を予め公表（ホームページ上の開示、パンフレットの配布等）している、又は、取得後速やかに本人に通知（電子メール、電話、文書の送付等）または公表している。（18条1項）
1. できている　2. 一部できている　3.できていない　(14)

(15) 個人情報の利用目的を変更する場合、当初の目的と関連する範囲内にとどめ、これを超える場合は本人の同意を得ている。（15条2項、16条）
1. できている　2. 一部できている　3.できていない　(15)

(16) 個人情報の利用目的を変更した場合、変更後の利用目的を本人に通知、または公表している。（18条3項）
1. できている　2. 一部できている　3.できていない　(16)

(17) 契約書等の書面で個人情報を取得する場合は、当該書面に記載する等して、予め本人に利用目的を明示している。（18条2項）
1. できている　2. 一部できている　3.できていない　(17)

(18) インターネット経由で個人情報を収集する場合、SSL等で通信を暗号化している。
1. できている、もしくは収集していない　2. 一部できている　3.できていない　(18)

Ⅲ. 情報の保管・廃棄

(19) インターネットに接続されたサーバで情報を保管する場合は、暗号化や、外部侵入防止策等のセキュリティ対策を講じている。

1. できている　2. 一部できている　3.できていない　(19) [ ]

(20) 情報は施錠管理されているキャビネット・部屋で保管されている。

1. できている　2. 一部できている　3.できていない　(20) [ ]

(21) 営業秘密が記録された書類、記録媒体(CD, DVD等)に秘密である旨が容易に識別できるような表示(冊子の表紙に「秘」と印字する、記録媒体に「厳秘」シールを貼付する等)をしている。

1. できている　2. 一部できている　3.できていない　(21) [ ]

(22) 営業秘密が記録された書類、記録媒体は、その他の書類・記録媒体と分離した専用スペースで、営業秘密と分かるよう保管されている。

1. できている　2. 一部できている　3.できていない　(22) [ ]

(23) 情報を保管している場所・部屋は、解錠時間と解錠者の氏名が分かるように施錠管理している。

1. できている　2. 一部できている　3.できていない　(23) [ ]

(24) 保有している個人情報を廃棄する場合の廃棄基準(保管期間、廃棄手続き等)が明確になっている。

1. なっている　2. 一部なっている　3.なっていない　(24) [ ]

(25) 利用が終了し不要となった情報は、復元不可能な方法で廃棄している。

1. できている　2. 一部できている　3.できていない　(25) [ ]

Ⅳ. 情報のバックアップとリストア

(26) 情報のバックアップデータを取得している。

1. 定期的に取得している　2. 不定期に取得している　3.取得していない　(26) [ ]

(27) 情報のバックアップ作業について、正しく終了したことを確認する手段(バックアップの作業ログを取得している、作業失敗時にアラートが発信される、等)がある。

1. ある　2.ない　(27) [ ]

(28) 情報のバックアップデータは、利用するサーバ等から隔離して保管し、火災や地震等で同時に被災しないようにしている。

1. している　2. していない　(28) [ ]

(29) 情報のリストア(バックアップからの復元)手順が整備されている。

1. されている　2.されていない　(29) [ ]

(30) 情報のリストア作業に必要な時間が見積もられている。

1. 見積もられている　2. 見積もられていない　(30) [ ]

(31) RPO(Recovery Point Objective:過去のどの時点まで遡って復旧できるようにしておくかの目標値)について利用部門等との検討を行い、バックアップ頻度等を設定している。

1. できている　2.できていない　(31) [ ]

(32) バックアップデータのリストア作業について、定期的な訓練での習熟と課題洗い出しを行っている。

1. 定期的に行っている　2.不定期に行っている　3.行っていない　(32) [ ]

Ⅴ．情報へのアクセス

(33) 不要なアクセスを制限するため、各社員がアクセス可能な領域は必要最小限に設定している。

1. できている　2. 現在検討中　3.できていない　(33)

(34) 情報へのアクセスは、あらかじめ担当者を特定し限定する等アクセスできる者を必要最小限としている。

1. できている　2. 一部できている　3.できていない　(34)

(35) ID・パスワード等といった個人を特定できる認証方法を採用している。

1. できている　2. 一部できている　3.できていない　(35)

(36) 社員各個人に付与しているID・パスワードは十分に強固(英大小数字記号混在8文字以上等)なものを利用する仕組みとし、パスワードは定期的に変更している(ID・パスワードを採用していない場合は除く。)

1. できている　2. 一部できている　3.できていない　(36)

(37) 情報を保管するデータベースサーバ、バックアップデータを保管している場所(サーバ室等)への入退室の記録を取り、「だれが」「いつ」アクセスしたかを特定できるようにしている。

1. できている　2. 一部できている　3.できていない　(37)

(38) 情報へのアクセス権限を保有した社員が担当から外れたり、異動・退職した場合には、即座にアクセス権限を削除している。

1. できている　2. 一部できている　3.できていない　(38)

(39) 情報へのアクセスは、いつ誰がどのような操作を行ったかがわかるように操作ログを取得しており、そのログは一定期間保管している。

1. できている　2. 一部できている　3.できていない　(39)

(40) 情報へのアクセスログは、定期的な確認を実施している。

1. 実施している　2. 実施したことがある　3. 実施していない　(40)

(41) 情報をコピー・ダウンロードする場合は、責任者に許可を得た上で行っており、その記録をつけている。

1. できている　2. 一部できている　3.できていない　(41)

(42) 情報が保管された外部メディアやPCを社外に持ち出す場合は、責任者に許可を得ている。

1. できている　2. 一部できている　3.できていない　(42)

(43) 情報が保管された外部メディアやPCを社外に持ち出す場合は、持ち出し記録をつけた上で持ち出している。

1. できている　2. 一部できている　3.できていない　(43)

(44) 情報が保管された外部メディアやPCを持ち出す場合は、第三者が読み出せないようなセキュリティ対策を講じている。(BIOSパスワード、ハードディスク・ファイルの暗号化等)

1. できている　2. 一部できている　3.できていない　(44)

(45) 情報が保管されたサーバに対して疑似アタック等のセキュリティ診断を定期的に実施し、外部からの攻撃に対する脆弱性を洗出している。

1. できている　2. 検査したことがある　3.検査したことがない　(45)

Ⅵ. 第三者への開示・提供

(46) 個人情報を第三者に提供する場合、本人の同意を得ている。あるいは、第三者提供を利用目的とする旨、提供する情報の内容、提供方法、本人の求めに応じて第三者提供を停止する旨、本人の求めを受け付ける方法を明示している。(23条)

1. できている　2. 一部できている　3.できていない　(46) [ ]

(47) 個人情報の取扱事務を外部業者に委託する場合に、個人情報の取扱ルール等、委託業者における管理体制を定期的に確認している。

1. できている　2. 一部できている　3.できていない　(47) [ ]

(48) 個人情報の取扱事務を外部業者に委託する場合に、第三者への提供の禁止、保管方法、委託終了時の返却方法等を契約書で定めている。

1. できている　2. 一部できている　3.できていない　(48) [ ]

(49) 営業秘密を取引先等の外部者に開示する場合、契約書を交わすなど秘密性を保持するために必要な行為をしている。

1. できている　2. 一部できている　3.できていない　(49) [ ]

(50) 外部委託先の従業員が自社に出入りして作業を行う場合に、業務上取り扱う必要のない個人情報にアクセスできないようにしている。

1. できている　2. 一部できている　3.できていない　(50) [ ]

(51) 外部委託先の作業終了後に、個人情報が返却又は廃棄されたことを確認する書面の提出を受けている。

1. できている　2. 一部できている　3.できていない　(51) [ ]

Ⅶ. 本人からの個人情報照会等対応

(52) 本人からの個人情報開示、訂正、利用停止等の依頼を受け付ける窓口を設け、公開している。

1. できている　2. 一部できている　3.できていない　(52) [ ]

(53) 本人からの個人情報開示、訂正、利用停止等の依頼を受けた場合、決められた方法で、確実に本人確認を実施している。

1. できている　2. 一部できている　3.できていない　(53) [ ]

(54) 本人からの個人情報開示、訂正、利用停止等の依頼を受けた場合、合理的な理由がない限り応じている。(28・29・30条)

1. できている　2. 一部できている　3.できていない　(54) [ ]

(55) 本人からの個人情報開示、訂正、利用停止等の依頼に応じない場合、その理由を説明している。

1. できている　2. 一部できている　3.できていない　(55) [ ]

(56) 本人からの個人情報開示、訂正、利用停止等の依頼内容と対応に関する記録が残されている。

1. できている　2. 一部できている　3.できていない　(56) [ ]

Ⅷ. 苦情対応

(57) 個人情報の取扱に関する苦情対応窓口を設け、公開している。

1. できている　2. 一部できている　3.できていない　(57) [ ]

(58) 苦情を受け付けた際の対応手順が明確化されている。

1. できている　2. 一部できている　3.できていない　(58) [ ]

(59) 苦情の内容と対応結果に関する記録が作成されている。

1. できている　2. 一部できている　3.できていない　(59) [ ]

(60) 受け付けた苦情に対し、迅速かつ適切に対応できているか定期的に確認している。

1. できている　2. 一部できている　3.できていない　(60) [ ]

Ⅸ. ＳＮＳ(ソーシャルメディア)の適切な利用

(61) ソーシャルメディアの利用に関するガイドラインにおいて、従業員が個人としてソーシャルメディアを適切に利用する旨、不適切な利用があった場合における就業規則に則った罰則等を規定している。

1. ある　2. 一部ある　3.ない　(61) [ ]

(62) SNSの利用に関するガイドラインにおいて、顧客などの個人情報や機密情報の投稿を禁止する旨規定されている。

1. 規定されている　2. 一部規定されている　3.規定していない　(62) [ ]

(63) SNSの利用に関するガイドラインにおいて、著作権、肖像権などの第三者の権利を尊重する旨規定している。

1. 規定している　2.規定していない　(63) [ ]

(64) パート・アルバイトを含めた全従業員に対して定期的にSNS利用ルールに関する教育・研修などを実施している。

1. 全従業員に実施している　2. 一部の従業員に実施している　3.実施していない　(64) [ ]

(65) SNS上でトラブルが発生したとき、速やかに主管部門へ報告させる体制が整備されている。

1. できている　2. 一部できている　3.できていない　(65) [ ]

(66) SNS上で発生したトラブルを適切に分析し、対応方法を検討するフローが確立されている。

1. できている　2. 一部できている　3.できていない　(66) [ ]

(67) 広報対応も含めたSNSトラブル発生時における緊急対応ルールが制定されている。

1. 制定されている　2.制定されていない　(67) [ ]