「リスク分析シート」の利用方法

（リスク分析シートVer.1.5）

1. リスク分析シートの構成

「リスク分析シート」は、自社の情報資産に想定されるリスクを特定し、対策を検討するために利用します。6つのシートがあり、使い方は以下の通りです。

シート名	使い方
台帳記入例	**「情報資産管理台帳」シートの記入例です。** 情報資産管理台帳に記入するときに参照します。（このシートに記入しても分析はできません。）
重要度定義	**情報資産の重要度を判断するための基準です。** 情報資産管理台帳に、情報資産ごとの機密性、完全性、可用性それぞれの評価値を記入するときに参照します。
情報資産管理台帳	**洗い出した情報資産を記入するシートです。** 業務で利用する電子データや書類を、媒体や保存先などの管理方法や重要度が同じものを1行にまとめて記入します。「重要度」と「現状から想定されるリスク」は自動で表示されます。
脅威の状況	**脅威の発生頻度（起こりやすさ）を推測するためのシートです。** 典型的な脅威が自社の環境ではどの程度起こりやすいかを「対策を講じない場合の脅威の発生頻度」欄のドロップダウンリストから選択します。「対策状況」は対策状況チェックシートに入力すると自動で表示されます。
対策状況チェック	**情報セキュリティ対策の実施状況を記入するシートです。** 情報セキュリティ診断項目ごとに、実施状況を「実施状況記入」欄のドロップダウンリストから選択します。
診断結果	**各シートに記入内容をもとにリスク分析の結果を表示するシートです。** 結果を参照するだけで記入不要です。

2. 各シートの利用方法

詳細リスク分析の手順を以下に示します。中小企業の情報セキュリティ対策ガイドラインP.44～53でも説明していますので参照して下さい。

【手順1】情報資産の洗い出し　☞使用シート[情報資産管理台帳]

「台帳記入例」と下表を参考に、業務で利用している情報資産を洗い出して各項目に記入します。一部の項目はドロップダウンリストから選択します。

台帳記入欄	記入内容解説
①業務分類	情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
②情報資産名称	情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは1行にまとめます。
③備考	必要に応じて説明等を記入します。
④利用者範囲	情報資産を利用してよい部署等を記入します。
⑤管理部署	情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
⑥媒体・保存先	情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。 例）見積書「電子データを**事務所**PC に保存」「印刷して**書類**を保管」
⑦個人情報の種類	各項目が個人情報保護法、マイナンバー法で定義されています。
	〈個人情報〉 個人情報が含まれる場合は「有」を記入します。 **−個人情報の定義−** 「 生存する個人に関する情報であって当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの、又は個人識別符号が含まれるもの」 氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、役職等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。
	〈要配慮個人情報〉 要配慮個人情報が含まれる場合は「有」を記入します。 **−要配慮個人情報の定義−** 「 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取り扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」
	〈特定個人情報〉 個人番号（マイナンバー）が含まれる場合（マイナンバー法で「特定個人情報」と定義されています。）は「有」を記入します。
⑧重要度	重要度定義シートまたは中小企業の情報セキュリティ対策ガイドラインP.45表10を参照して、情報資産の機密性、完全性、可用性それぞれの評価値を記入します。3種類の評価値から中小企業の情報セキュリティ対策ガイドラインP.46表11に基づき重要度が表示されます。なお、⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「2」となります。
⑨保存期限	法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
⑩登録日	登録した日付を記入します。内容を更新した場合は更新日に修正します。

【手順2】リスク値の算定

対策の優先度を決めるため、情報資産ごとにリスク値（リスクの大きさ）を算定します。リスク値は「重要度」「脅威」「脆弱性」の数値から算定します。重要度は【手順1】で算定しているので、ここでは脅威と脆弱性を算定します。

(1)「脅威」の識別　☞使用シート[脅威の状況]

媒体・保存先ごとの脅威が、対策を講じない場合にどのくらいの頻度で発生する可能性があるかを、「対策を講じない場合の脅威の発生頻度」欄のドロップダウンリストから1～3のいずれかを選択します。

ドロップダウンリスト	解説
1:通常の状況で脅威が発生することはない	通常業務を行っている状態では発生しない、または発生する可能性が極めて低い場合は「1」を選択します。 例）業務でモバイル機器を使っていないので「モバイル機器」に考えられる脅威は「1」である。
2:特定の状況で脅威が発生する（年に数回程度）	頻度は少ないが、たまに必要だったり、通常とは異なる環境で業務を行うことがあり、そのような特定の状況で発生する可能性がある場合は「2」を選択します。 例）月末の繁忙時に私有のUSBメモリでデータを持ち帰り、自宅のノートパソコンで業務を行っている人がいるので「可搬電子媒体」「モバイル機器」に考えられる脅威は「2」である。
3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	日常的に、典型的な脅威が発生しうる業務を行っている、または、これまでに何度か発生したことがある場合は「3」を選択します。 例）取引先や顧客との重要情報のやりとりは、全て電子メールにファイルを添付して送受信しているので「事務所PC」「モバイル機器」「社外サーバー（メールサーバー）」の脅威は「3」である。

(2)「脆弱性」の認識　☞使用シート[対策状況チェック]

情報セキュリティ対策の実施状況を、「実施状況」欄のドロップダウンリストから1～4のいずれかを選択します。

ドロップダウンリスト	解説
1:実施している	情報セキュリティ診断項目の通りか、それ以上の対策を実施している場合は「1」を選択します。
2:一部実施している	情報セキュリティ診断項目の一部か、実施状況が不十分である場合は「2」を選択します。
3:実施していない/わからない	情報セキュリティ診断項目を全く実施していないか、実施しているかどうか、または実施方法が分からない場合は「3」を選択します。
4:自社に該当しない	情報セキュリティ診断項目が自社にあてはまらない場合は「4」を選択します。 例えば、自社で情報システム開発を行っていない場合の、システム開発に関する項目などがこれにあたります。

(3) リスク値の算定　☞使用シート[情報資産管理台帳]

【手順1】と【手順2】が完了すると、「現状から想定されるリスク」欄に、情報資産ごとに「脅威の発生頻度」「脆弱性」「被害発生可能性」「リスク値」が表示されます。

現状から想定されるリスク（入力不要・自動表示）	表示処理の方法
脅威の発生頻度 **※「脅威の状況 」シートに入力すると表示**	情報資産の媒体・保存先の特性に応じて想定される脅威について、脅威の発生頻度（起こりやすさ）を示す1～3のうち、最大値を表示します。
脆弱性 **※「対策状況 チェック」シートに入力すると表示**	情報資産の媒体・保存先特有の脆弱性について、対策状況チェックシートをもとに、脆弱性（つけ込みやすさ）を示す1～3の値を表示します。
被害発生可能性	脅威の発生頻度と脆弱性をもとに、情報資産に被害が発生する可能性を1～3で表示します。
リスク値	情報資産の「重要度」と「被害発生可能性」をもとにリスク値を4～6大・1～3中・0小で表示します。

[手順3] 情報セキュリティ対策の決定　☞使用シート[診断結果]

【手順1】と【手順2】が完了すると、情報セキュリティ対策の種類ごとに「情報セキュリティ関連規程策定の必要性」「対策状況チェックの診断結果（対策の実施率）」「対策検討・実施の要否」が表示されます。

情報セキュリティ関連規程策定の必要性	情報セキュリティ対策を検討し、規程を策定する必要があるかどうかを次の記号で表示します。 ◎ 該当する規程類がないのであれば必要 ○ 該当する情報資産があるので必要 △ システム開発・重要情報の取扱いの委託がある場合は必要 ー 該当する情報資産がないので不要
対策状況チェックの診断結果（対策の実施率）	「対策状況チェック」シートへの記入結果をもとに、対策がどの程度実施されているかを、パーセンテージで表示します。なお、情報資産の種類によっては不要な対策もあるので、すべての対策を実施していなくても実施率が100%になることがあります。
対策検討・実施の要否	上記2つの診断結果をもとに、新たに対策を検討し、実施する必要があるかどうかを次のいづれかで表示します。 「対策を維持し適切性・妥当性・有効性を継続的に改善して下さい」 「不足する対策を検討・実施してください」 「（該当する情報資産なし）」

また、「情報資産管理台帳に基づく管理すべき情報資産の状況」として「情報資産管理台帳」に記入した情報資産のうち、媒体・保存先ごと、個人情報、重要度別の件数が表示されますので、対策を検討する際に参考にしてください。

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）					
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			2	2	2	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		2	2	1	2	5年	2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	社内サーバー	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			2	1	1	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	モバイル機器	有			2	1	1	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	社内サーバー				1	1	1	1		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部	書類				1	2	1	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	社内サーバー				0	1	1	1		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	書類				0	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	可搬電子媒体				0	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
営業	キャンペーン応募者リスト	20xx年のキャンペーン応募者情報	営業部	営業部	社内サーバー	有			2	1	0	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
調達	委託先リスト	外部委託先（直近5年間に実績があるもの）	総務部	総務部	社内サーバー				0	1	1	1		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
調達	発注伝票	発注伝票（過去10年分）	総務部	総務部	社内サーバー				1	0	0	1		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク中
調達	発注伝票	発注伝票（過去10年分）	総務部	総務部	書類				1	0	0	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
技術	製品設計図	現役製品の設計図	開発部	開発部	社内サーバー				2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
技術	製品設計図	現役製品の設計図	開発部	開発部	書類				2	2	2	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中

＜記入内容についての解説＞

① **業務分類**	情報資産と関連する業務や部署を記入します。情報資産が少なければ省いても構いません。
② **情報資産名称**	情報資産の名称や内容を表すものを簡潔に記入します。正式名称がないものは社内通称で構いません。
③ **備考**	情報資産名称だけでは個人情報の有無や重要度が判断できない場合に説明を記入してください。
④ **利用者範囲**	情報資産を利用してよい部署等を記入してください。アクセスコントロールに利用することができます。
⑤ **管理部署**	情報資産に対して情報セキュリティ上の管理責任がある部署等を記入してください。小規模事業者であれば担当名でも構いません。
⑥ **媒体・保存先**	情報資産の媒体や保存場所をリストから選択してください。書類と電子データの両方を保有している場合は2行に分けて記入してください。この項目から脅威と脆弱性を想定します。
⑦ **個人情報の種類**	個人情報※1、要配慮個人情報※2、特定個人情報が含まれる場合は、該当欄に「有」を記入します。 ※1要配慮個人情報も特定個人情報も個人情報ですが、「個人情報」の欄には要配慮個人情報と特定個人情報以外の個人情報に「有」を記入してください。※2本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実等が含まれる個人情報
⑧ **重要度**	情報資産の機密性、完全性、可用性のそれぞれの評価値（0～2）を選択します。3つの評価値から重要度（2～0）が表示されます。⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「2」となります。
⑨ **保存期限**	法律で定められた保存期限または利用目的が完了して廃棄や消去が必要となる期限を記入します。必要な期間以上に保有し続けるより廃棄・消去したほうがリスクが小さくなる場合に利用します。
⑩ **登録日**	情報資産管理台帳に登録した日付を記入します。内容に変更があった場合はその更新日に修正します。
⑪ **脅威の発生頻度**	「脅威の状況」シートにおける「対策を講じない場合の脅威の発生頻度」欄に記入された3段階の値のうち、媒体・保存先ごとにもっとも大きい値を表示します。（記入の必要はありません）
⑫ **脆弱性**	「対策状況チェック」シートで選択された実施状況をもとに、脆弱性への情報セキュリティ対策の実施状況を3段階で表示します。（記入の必要はありません）
⑬ **被害発生可能性**	「脅威」と「脆弱性」をもとに、現状で被害が発生する可能性を高・中・低の3段階で表示します。
⑭ **リスク値**	情報資産の「重要度」と「被害発生可能性」の積をもとにリスクの大きさを大・中・小の3段階で表示します。

【表10】情報資産の機密性・完全性・可用性に基づく重要度の定義

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ[12]として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	1	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	0	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	1	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているEC サイト ●顧客に提供しているクラウドサービス
	1	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	0	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

12 ▲限定提供データ　不正競争防止法で次のように定義されています。「第二条 7 この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

【表11】情報資産の重要度判断基準

判断基準	重要度
機密性・完全性・可用性評価値のいずれかまたはすべてが「2」の情報資産	2
機密性・完全性・可用性評価値のうち最大値が「1」の情報資産	1
機密性・完全性・可用性評価値すべてが「0」の情報資産	0

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）			
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性	リスク値

脅威の状況シート

媒体・保存先	想定される脅威 （考えられる典型的な脅威）	対策を講じない場合の脅威の発生頻度 （1～3から選択）	対策状況 （対策状況チェックシートに入力すると自動で表示）
書類	秘密書類の事務所からの盗難		
	秘密書類の外出先での紛失・盗難		
	情報窃取目的の内部不正による書類の不正持ち出し		
	業務遂行に必要な情報が記載された書類の紛失		
可搬電子媒体	秘密情報が格納された電子媒体の事務所からの盗難		
	秘密情報が格納された電子媒体の外出先での紛失・盗難		
	情報窃取目的の内部不正による電子媒体の不正持ち出し		
	業務遂行に必要な情報が記載された電子媒体の紛失		
事務所PC	情報窃取目的の事務所PCへのサイバー攻撃		
	情報窃取目的の事務所PCでの内部不正		
	事務所PCの故障による業務に必要な情報の喪失		
	事務所PC内データがランサムウェアに感染して閲覧不可		
	不正送金を狙った事務所PCへのサイバー攻撃		
モバイル機器	情報窃取目的でのモバイル機器へのサイバー攻撃		
	情報窃取目的の不正アプリをモバイル機器にインストール		
	秘密情報が格納されたモバイル機器の紛失・盗難		
社内サーバー	情報窃取目的の社内サーバーへのサイバー攻撃		
	情報窃取目的の社内サーバーでの内部不正		
	社内サーバーの故障による業務に必要な情報の喪失		
社外サーバー	安易なパスワードの悪用によるアカウントの乗っ取り		
	バックアップを怠ることによる業務に必要な情報の喪失		

対策状況チェックシート

情報セキュリティ対策の種類	情報セキュリティ診断項目	実施状況
1 組織的対策	経営者の主導で情報セキュリティの方針を示していますか？	
	情報セキュリティの方針に基づき、具体的な対策の内容を明確にしていますか？	
	情報セキュリティ対策を実施するための体制を整備していますか？	
	情報セキュリティ対策のためのリソース（人材、費用）の割当を行っていますか？	
2 人的対策	秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員などを含む）に対して、就業規則や契約などを通じて秘密保持義務を課していますか？	
	従業員の退職に際しては、退職後の秘密保持義務への合意を求めていますか？	
	会社の秘密情報や個人情報を扱うときの規則や、関連法令による罰則に関して全従業員に説明していますか？	
3 情報資産管理	管理すべき情報資産は、情報資産管理台帳を作成するなど何処にどのようなものがあるか明確にしていますか？	
	秘密情報は業務上必要な範囲でのみ利用を認めていますか？	
	秘密情報の書類に㊙マークを付けたり、データの保存先フォルダを指定するなど識別が可能な状態で扱っていますか？	
	秘密情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりするなどの盗難・紛失対策を定めていますか？	
	秘密情報は施錠保管やアクセス制限をして、持ち出しの記録やアクセスログをとるなど取り扱いに関する手順を定めていますか？	
	重要なデータのバックアップに関する手順を定め、手順が順守されていることを確認していますか？	
	秘密情報の入ったパソコンや紙を含む記録媒体を処分する場合、ゴミとして処分する前に、データの完全消去用のツールを用いたり、物理的に破壊したりすることで、データを復元できないようにすることを定めていますか？	
4 アクセス制御及び認証	業務で利用するすべてのサーバーに対して、アクセス制御の方針を定めていますか？	
	従業員の退職や異動に応じてサーバーのアクセス権限を随時更新し、定期的なレビューを通じてその適切性を検証していますか？	
	情報を社外のサーバーなどに保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合は、アクセスを許可された人以外が閲覧できないように、適切なアクセス制御を行うことを定めていますか？	
	パスワードの文字数や複雑さなどを設定するOSの機能などを有効にし、ユーザーが強固なパスワードを使用するようにしていますか？	
	業務で利用する暗号化機能及び暗号化に関するアプリケーションについて、その運用方針を明確に定めていますか？	
5 物理的対策	業務を行う場所に、第三者が許可無く立ち入りできないようにするための対策（物理的に区切る、見知らぬ人には声をかける、など）を講じていますか？	
	最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？	
	重要な情報やIT機器のあるオフィス、部屋及び施設には、許可された者以外は立ち入りできないように管理していますか？	
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体などの持込み・利用を禁止していますか？	
6 IT機器利用	セキュリティ更新を自動的に行うなどにより、常にソフトウェアを安全な状態にすることを定めていますか？	
	ウイルス対策ソフトウェアが提供されている製品については、用途に応じて導入し、定義ファイルを常に最新の状態にすることを定めていますか？	
	業務で利用するIT機器に設定するパスワードに関するルール（他人に推測されにくいものを選ぶ、機器やサービスごとに使い分ける、他人にわからないように管理する、など）を定めていますか？	
	業務で利用する機器や書類が誰かに勝手に見たり使ったりされないようにルール（離席時にパスワード付きのスクリーンセーバーが動作する、施錠できる場所に保管する、など）を定めていますか？	
	業務で利用するIT機器の設定について、不要な機能は無効にする、セキュリティを高める機能を有効にするなどの見直しを行うことを定めていますか？	
	社外でIT機器を使って業務を行う場合のルールを定めていますか？	

情報セキュリティ対策の種類	情報セキュリティ診断項目	実施状況
	個人で所有する機器の業務利用について、禁止するか、利用上のルールを定めていますか？	
	受信した電子メールが不審かどうかを確認することを求めていますか？	
	電子メールアドレスの漏えい防止のためのBCC利用ルールを定めていますか？	
	インターネットバンキングやオンラインショップなどを利用する場合に偽サイトにアクセスしないための対策を定めていますか？	
7 IT基盤運用管理	IT機器の棚卸（実機確認）を行うなど、社内に許可なく設置された無線LANなどの機器がないことを確認していますか？	
	サーバーには十分なディスク容量や処理能力の確保、停電・落雷などからの保護、ハードディスクの冗長化などの障害対策を行っていますか？	
	業務で利用するすべてのサーバーに対して、脆弱性及びマルウェアからの保護のための対策を講じていますか？	
	記憶媒体を内蔵したサーバーなどの機器を処分または再利用する前に、秘密情報やライセンス供与されたソフトウェアを完全消去用のツールを用いたり、物理的に破壊したりすることで、復元できないようにすることを定めていますか？	
	業務で利用するすべてのサーバーやネットワーク機器に対して、必要に応じてイベントログや通信ログの取得及び保存の手順を定めた上で、ログを定期的にレビューしていますか？	
	重要なITシステムに脆弱性がないか、専用ツールを使った技術的な診断を行うことがありますか？	
	ファイアウォールなど、外部ネットワークからの影響を防ぐための対策を導入していますか？	
	業務で利用しているネットワーク機器のパスワードを初期設定のまま使わず、推測できないパスワードに変更して運用していますか？	
	クラウドサービスなどの社外サーバーを利用する場合は、費用だけでなく、情報セキュリティや信頼性に関する仕様を考慮して選定していますか？	
	最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有していますか？	
8 システム開発及び保守	情報システムの開発を行う場合、開発環境と運用環境とを分離していますか？	
	セキュリティ上の問題がない情報システムを開発するための手続きを定めていますか？	
	情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにするための対策を講じていますか？	
9 委託管理	契約書に秘密保持（守秘義務）、漏洩した場合の賠償責任、再委託の制限についての項目を盛り込むなどのように、委託先が順守すべき事項について具体的に規定していますか？	
	委託先との秘密情報の受渡手順を定めていますか？	
	委託先に提供した秘密情報の廃棄または消去の手順を定めていますか？	
10 情報セキュリティインシデント対応ならびに事業継続管理	秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故の発生に備えた準備をしていますか？	
	インシデントの発生に備えた証拠情報の収集手順を定め、運用していますか？	
	インシデントの発生で事業が中断してしまったときに再開するための計画を定めていますか？	
11 個人番号及び特定個人情報の取り扱い	個人番号及び特定個人情報の取り扱いルール（管理担当者の割当て、収集・利用・保管・廃棄の方法）を定めていますか？	
	個人番号や特定個人情報に関する漏えいなどの事故に備えた体制を整備していますか？	
	個人番号や特定個人情報の安全管理についてルールや手段を定めていますか？	

診断結果

＜凡例＞
◎ 該当する規程類がないのであれば必要
○ 該当する情報資産があるので必要
△ システム開発・重要情報の取扱いの委託がある場合は必要
ー 該当する情報資産がないので不要

情報セキュリティ対策の種類（付録5 情報セキュリティ関連規程名称）		情報セキュリティ関連規程策定の必要性	対策状況チェックの診断結果（対策の実施率）	対策検討・実施の要否
1	組織的対策	◎		
2	人的対策	◎		
3	情報資産管理	ー		
4	アクセス制御及び認証	ー		
5	物理的対策	◎		
6	IT機器利用	ー		
7	IT基盤運用管理	ー		
8	システム開発及び保守	△		
9	委託管理	△		
10	情報セキュリティインシデント対応ならびに事業継続管理	◎		
11	個人番号及び特定個人情報の取扱い	ー		

情報資産管理台帳に基づく管理すべき情報資産の状況

		情報資産の件数
媒体・保存先ごとの件数	書類	0件
	可搬電子媒体	0件
	事務所PC	0件
	モバイル機器	0件
	社内サーバー	0件
	社外サーバー	0件

		個人情報の件数
個人情報の種類別件数	個人情報	0件
	要配慮情報	0件
	マイナンバー	0件

		情報資産の件数
情報資産の重要度	重要度:2	0件
	重要度:1	0件
	重要度:0	0件