

監査ガイドライン－必須項目

共通事項			No.	主たる 監査対象	監査技法	監査手続	
1	重要情報の 識別	重要情報であることを明らかにするために、「関係者外 秘」などの表示等を行っている。	I 共通事項 第二 1	1-1	重要情報目録	閲覧（レビュー）	重要情報目録に、重要情報が記載されていることを確認する。
				1-2	重要情報	観察（視察）	重要情報を識別（明らかに）していることを確認する。 (例) ・紙情報の場合 ：その情報が記載された紙に重要情報であること（社外 秘等の表示）の記載 ・電子情報の場合 ：ファイル名に重要情報であることの記録 ・試作品、製造装置等の物の場合 ：当該物そのもの又はその保管容器に表示 ・その他の方法 ：目録による管理、電子情報にアクセス可能な者を限 定したフォルダにより管理
				1-3	重要情報目録	閲覧（レビュー）	重要情報を識別（明らかに）している記録を、責任者が確 認していることを確認する。
2		他者から預けられた重要情報は、当該他者からの意 見に基づき管理方法を決定している。	I 共通事項 第二 3	2-1	預託元の要求 に沿った記録・ 保管・報告記 録	閲覧（レビュー）	他者から預けられた重要情報の管理方法は、当該他者の 意見を聞いて決定することが定められていることを確認する。
				2-2	預託元の要求 に沿った記録・ 保管・報告記 録	閲覧（レビュー）	当該他者の要求に応じて、預けられた重要情報の記録・保 管・報告を行っていることを確認する。
				2-3	預託元の要求 に沿った記録・ 保管・報告記 録	閲覧（レビュー）	当該他者の要求に応じて、預けられた重要情報の記録・保 管・報告を行っていることを、責任者が確認していることを確 認する。

3	管理者の選任	<p>経営層は、以下の重要情報の管理に関わる責任者を定める。</p> <p>(1)情報管理の手順を確立する。</p> <p>(2)情報を取り扱う者の制限・管理、トレーニングを行う。</p> <p>(3)情報漏洩防止対策を実施し、その実施状況を把握する。</p> <p>(4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。</p> <p>(5)(2)-(4)の記録を取得し、保管する。</p>	I 第三1(1)	3-1	組織的対策に関する規程	閲覧(レビュー)	<p>経営層が重要情報について以下を実施する責任者を定めていることを確認する。</p> <p>(1)情報管理の手順を確立する。</p> <p>(2)情報を取り扱う者の制限・管理、トレーニング(会議、講義、e-learning等実施形態は問わない)を行う。</p> <p>(3)情報漏洩防止対策を実施し、その実施状況を把握する。</p> <p>(4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。</p> <p>(5)(2)-(4)の記録を取得し、保管する。</p>
				3-2	管理対象情報管理責任者選任記録	閲覧(レビュー)	<p>重要情報についての責任者が、(1)-(5)を実施している記録を確認する。</p> <p>(1)情報管理の手順を確立する。</p> <p>(2)情報を取り扱う者の制限・管理、トレーニング(会議、講義、e-learning等実施形態は問わない)を行う。</p> <p>(3)情報漏洩防止対策を実施し、その実施状況を把握する。</p> <p>(4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。</p> <p>(5)(2)-(4)の記録を取得し、保管する。</p>
				3-3	管理対象情報管理責任者選任記録	閲覧(レビュー)	<p>重要情報についての責任者が、(1)-(5)を実施している記録を経営者が確認していることを確認する。</p> <p>(1)情報管理の手順を確立する。</p> <p>(2)情報を取り扱う者の制限・管理、トレーニング(会議、講義、e-learning等実施形態は問わない)を行う。</p> <p>(3)情報漏洩防止対策を実施し、その実施状況を把握する。</p> <p>(4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。</p> <p>(5)(2)-(4)の記録を取得し、保管する。</p>

				3-4	管理対象情報 管理責任者選 任記録	閲覧（レビュー）	重要情報についての責任者が、(2)-(4)の記録の方法を定 めていることを確認する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、 講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握す る。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時 に必要な対応を行う。
				3-5	管理対象情報 管理責任者選 任記録	閲覧（レビュー）	重要情報についての責任者が、(2)-(4)の記録・保管の方 法・期間を定めていることを確認する。 (2)情報を取り扱う者の制限・管理、トレーニング（会議、 講義、e-learning等実施形態は問わない）を行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握す る。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時 に必要な対応を行う。
4		従業員が多い場合や、重要情報が複数部門に跨がっ ている場合は、全従業員が責任者を明確に認識させ るようにしている。	I 第三1（2）	4-1	社内規程、社 内掲示	閲覧（レビュー）	全ての従業員が閲覧可能な状況で、責任者を認識できる 方法を定めていることを確認する。
				4-2-1	社内規程、社 内掲示	閲覧（レビュー） 観察（視察）	全ての従業員が閲覧可能な状況で、責任者を認識できる 社内規程・社内掲示がなされているかを確認する。
				4-2-2	従業員	質問（ヒアリング）	責任者を認識しているかどうかを確認する。
				4-3	責任者を認識 できる方法の実 施記録	閲覧（レビュー）	全ての従業員が閲覧可能な状況で、責任者を認識できる 方法についての実施状況を責任者が確認していることを確 認する。

5	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	I 第四 柱書き	5-1	管理状況（管理記録）	閲覧（レビュー）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が定められていることを確認する。
				5-2-1	管理状況（管理記録）	閲覧（レビュー） 観察（視察）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを確認する。
				5-2-2	従業員	質問（ヒアリング）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを確認する。
				5-4	管理状況（管理記録）	質問（ヒアリング）	重要情報の作成から廃棄までのプロセスを通じて、適切に管理するための取組が実施されていることを、責任者が確認していることを確認する。
6	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	I 第五 柱書き	6-1	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させる機会について、その対象・内容・方法・期間等を設けていることを確認する。
				6-2	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させていることを確認する。
				6-3	研修の実施状況（実績）	閲覧（レビュー）	全ての従業員等への重要情報の適切な管理に関するトレーニングを受講させていることを、責任者が確認していることを確認する。

7	管理対象情報の漏えいの事故等の発生時等の報告	情報漏えいの事故が発生した場合の報告先を定め、全従業員に対して周知している。	I 第六 柱書き	7-1	管理対象情報漏えい事故発生時の報告先の設定状況	閲覧（レビュー）	従業員等が重要情報の漏えいの事故等の発生を発見した場合、事業者内部で情報の取扱いに係る不正を発見した場合等の報告先を、社内規程に定めていることを確認する。
				7-2	周知状況	閲覧（レビュー） 観察（視察）	報告先は、社内に掲示をする等従業員等が認識するようにしていることを確認する。
				7-3	周知状況	閲覧（レビュー）	報告先は、従業員等が認識するようにしていることを責任者が確認していることを確認する。
8	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	II 柱書き	8-1	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を定めていることを確認する。
				8-2	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー） 観察（視察）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を実施していることを確認する。
				8-3	管理対象情報への人的アクセスの制限状況（アクセス制御設定管理簿）	閲覧（レビュー）	重要情報へアクセス可能な者を定め、アクセス可能な者以外がアクセスできない方法を実施していることを責任者が確認していることを確認する。

管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）							
9	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	Ⅲ 柱書き	9-1	保管容器の管理状況	閲覧（レビュー）	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定することを定めている。
			9-2	保管容器	観察（視察）	重要情報の保管には施錠することができる保管容器を用いていることを確認する。	
			9-3	保管容器の取扱場所	観察（視察）	重要情報を保管容器から持ち出して利用する際、取り扱う場所を限定していることを確認する。	
			9-4	保管容器の管理状況	閲覧（レビュー）	責任者が重要情報の保管の状況や取り扱う場所の限定等の管理状況を確認していることを確認する。	

管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）							
10	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	IV 柱書き	10-1	物理的対策に関する規程、又はアクセス制御設定管理簿	閲覧（レビュー）	重要情報が置かれる場所を立入制限区域としてアクセス権者以外の者の立入りを制限することを定めている。
				10-2	立入制限の入退室記録	観察（視察）	立入制限区域の状況、立入制限された場所にはアクセス権者以外の入室がないことを確認する。
				10-3	物理的対策に関する規程、又はアクセス制御設定管理簿	閲覧（レビュー）	立入制限区域の状況、立入制限された場所にはアクセス権者以外の入室がないこと責任者が確認していることを確認する。
11		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	IV 柱書き	10-1	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施することを定めている。
				10-2	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施していることを確認する。
				10-3	委託管理に関する規程及び他者との秘密保持契約、警備委託契約	閲覧（レビュー）	重要情報を外部で保管する場合には、委託事業者に対して、秘密保持、施錠、巡回監視等の契約を締結し、自社が定めた対策を実施していることを責任者が確認していることを確認する。

管理対象情報が電子情報の場合							
12	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	V 柱書き	11-1	IT基盤運用管理に関する規程	閲覧（レビュー）	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を行うことを定めている。
				11-2	クラウド等外部事業者の利用規程	閲覧（レビュー）	重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結することを定めている。
				11-3	可搬式記録媒体の持ち出し管理簿	閲覧（レビュー）	可搬式記録媒体の持ち出しを管理していることを確認する。
				11-4	アクセス権設定状況	観察（視察）	重要情報が事業者の内部のサーバ等で記録されている場合に、情報へのアクセスをアクセス権者に制限する等の必要な措置が実施されていることを確認する。
				11-5	外部事業者の信頼性確認結果（認証取得状況の確認等）	閲覧（レビュー）	重要情報が外部データセンター等で管理する場合には、その管理者の信頼性を確認していることを確認する。
				11-6	外部事業者との秘密保持契約	閲覧（レビュー）	重要情報が外部データセンター等で管理する場合には、秘密保持契約を締結した上で、必要な措置を実施していることを確認する。
				11-7	可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者の信頼性確認結果（認証取得状況の確認等）、外部事業者との秘密保持契約	閲覧（レビュー）	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限の実施状況について責任者が確認していることを確認する。