監査ガイドライン

章	節	項	番		内容					ID	確認内容	確認対象
I	第一	3			共通事項	適切な管理をする必要がある技術等情報の特定		事業者は、管理対象情報を特定した場合には、当該管理対象情報の態様が、紙情報（管理対象情報が記載された紙をいう。以下同じ。）、電子情報（管理対象情報が電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）又は試作品、製造装置等の物自体のいずれに当たるか識別し、必要に応じて保管場所等を記録した目録を作成し、合理的な期間保管する。		3	特定された管理対象情報一覧 （必要に応じて、管理対象情報目録）の現地調査を実施し、管理対象情報を特定した場合は、態様を識別し、必要に応じて保管場所等を記録した目録を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 特定された管理対象情報一覧 （必要に応じて、管理対象情報目録）
	第二	1				管理対象情報の識別と必要な措置の整理		事業者は、管理対象情報であることを明らかにするために、表示等の方法により他の技術等情報と区別して識別できるよう必要な措置を講ずるものとする。表示により識別できるようにする方法としては、例えば、紙情報の場合であればその情報が記載された紙に管理対象情報であること（社外秘等の表示）を記載し、電子情報の場合であればファイル名に管理対象情報であることを記録し、試作品、製造装置等の物の場合であれば当該物そのもの又はその保管容器に表示することが考えられ、その他の方法としては、例えば、第一の3の目録による管理や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する方法等が考えられる。		4	管理対象情報目録、識別された管理対象情報を閲覧し、管理対象情報を識別できることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報目録、識別された管理対象情報
		3						事業者は、当該管理対象情報が他者から預けられたものである場合は、当該他者からの意見を聞いてこの告示に掲げる措置のうち必要なものを決定し、当該他者からの求めがあったときは、その状況を記録し、合理的な期間保管し、報告する。		6	預託元の要求に沿った記録・保管・報告記録を閲覧し、預託情報の管理措置は、預託元の意見を聞いて決定し、要求に応じて記録・保管・報告を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 預託元の要求に沿った記録・保管・報告記録
	第三	1	(1)			管理者の選任	原則	事業者の取締役等の経営層は、管理対象情報に関し、以下に掲げる事項についての責任を有する者（以下「管理者」という。）を選任する。なお、その一部の実施を他の者に委任することを妨げない。		7	組織的対策に関する規程及び管理対象情報管理責任者選任記録、管理対象情報を取り扱う者の制限・管理記録、トレーニングの実施記録、管理対象情報の漏えいの防止措置の実施記録、管理対象情報の漏えいや兆候の把握と事象があった場合に必要な対応等の措置を定めた記録を閲覧し、経営層が管理対象情報についての責任者を定めていることを確認する。	【規定等】 組織的対策に関する規程 【記録やその他の確認対象】 管理対象情報管理責任者選任記録、管理対象情報を取り扱う者の制限・管理記録、トレーニングの実施記録、管理対象情報の漏えいの防止措置の実施記録、管理対象情報の漏えいや兆候の把握と事象があった場合に必要な対応等の措置を定めた記録
				一					管理対象情報について、第二の2により必要と決定した措置に係る必要な手順を確立させること。			
				二					管理対象情報を取り扱う者の制限及び管理を行い、当該管理対象情報を取り扱う者に対するトレーニングを行うこと。			
				三					保管容器又は立入制限区域の鍵の管理又は暗証番号の設定等の管理対象情報の漏えいの防止のために必要な措置を講じ、その状況を把握すること。			
				四					管理対象情報の漏えいの兆候や漏えいの事実の把握に努め、その事象があった場合に必要な対応等の措置を講ずること。			
				五					二から四までに掲げる事項について、記録を取得し、合理的な期間保管すること。			

章	節	項	番		内容					ID	確認内容	確認対象
			(2)					事業者は、当該事業者の従業員等（事業者との間で雇用関係等のある者をいう。以下同じ。）が多い場合、その管理対象情報が複数の事業部門にまたがるものである場合等には、社内規程に定めることや社内における掲示をすること等により、（1）の各事項の責任を誰が有しているかを当該事業者の従業員等の全ての者が認識できるように措置を講ずる。		8	管理者を記載した社内規程や社内掲示の現地調査を実施し、全ての従業員等が管理者を認識できるための措置を講じていることを確認する。（従業員へのインタビューにより、管理者を認識しているかどうかを確認する）	【規定等】 【記録やその他の確認対象】 管理者を記載した社内規程や社内掲示
		2						従業員等が少人数の場合等の措置 1にかかわらず、事業者の従業員等が少人数の場合等には、当該事業者の取締役等の経営層の判断により、経営層の者が管理者を兼務することができる。事業者の従業員等が少人数の場合等とは、例えば、取締役等の経営層が全ての従業員等を認識することが可能な程度の人数であり、当該取締役等の経営層が管理対象情報の取扱い状況をほぼ把握できるとともに、従業員等から当該取締役等の経営層に対して、管理対象情報に係る報告等が直接される取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態が確立している場合等が考えられる。		9	管理者を経営層が兼務することの記録（議事録等）、または管理者を経営者が兼務することの従業員の認識の現地調査を実施し、管理対象情報の管理者を経営層の者が兼務するにあたり、経営層が判断したことを確認する。	【規定等】 【記録やその他の確認対象】 管理者を経営層が兼務することの記録（議事録等）、または管理者を経営者が兼務することの従業員の認識
	第四					管理対象情報の管理等		事業者は、管理対象情報の作成から廃棄までのプロセスを通じて、管理対象情報を適切に管理（当該管理対象情報の正確さ及び完全さを保護すること並びに当該管理対象情報にアクセスすることを認められた者が要求したときにアクセス及び使用が可能であるようにすることを含む。以下同じ。）するための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態（管理対象情報が複製された場合の当該複製された情報（当該管理対象情報が電子情報である場合における当該管理対象情報がプリントアウトされたもの及び紙情報である場合におけるスキャナ等により電子化されたものを含む。以下この第四において同じ。）を適切に管理するための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を含む。）を確立させた上で、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、当該管理対象情報の適切な管理を行う。		10	管理対象情報の管理状況（あるいは、管理対象情報（複製含む）の管理記録）の現地調査を実施し、管理対象情報の作成から廃棄までのプロセスを通じて、管理対象情報を適切に管理するための取組が従業員等において実践されていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の管理状況（あるいは、管理対象情報（複製含む）の管理記録）
		1	(1)				管理対象情報の管理簿の作成等	管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。		11	管理対象情報管理簿を閲覧し、持ち出し、複製、廃棄等の管理対象情報の状況が記載されていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿
			(2)					管理者は、（1）の管理簿について、他者から預けられた管理対象情報についてのみの状況を管理するため、自らのものと別にして管理簿を作成する。		12	管理対象情報管理簿（預託管理対象情報）を閲覧し、預託された管理対象情報は自らのものと別に管理簿を作成していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿（預託管理対象情報）

章	節	項	番		内容					ID	確認内容	確認対象
			(3)					管理者は、(1) 又は(2) の管理簿について、保管期間を定めた上、施錠したロッカー等において保管し、又は暗号技術を用いてサーバ又はパーソナルコンピュータ(以下「サーバ等」という。)に記録する等適切に管理(当該ロッカー等の鍵の管理を含む。)する。		13	保管期間の定めがあるもの、ロッカーでの管理状況又はサーバでの管理状況を閲覧し、管理者が管理簿について保管期間を定めたうえ、施錠したロッカー等に保管もしくは暗号技術等によりサーバ等に記録する等、適切に管理(当該ロッカー等の鍵の管理を含む。)していることを確認する。	【規定等】 【記録やその他の確認対象】 保管期間の定めがあるもの、ロッカーでの管理状況又はサーバでの管理状況
			(4)					管理者は、(2) の管理簿について(3)の保管期間を定める場合は、当該管理簿に係る管理対象情報を預けた他者の確認をとる。		14	保管期間の定めがあるもの、保管期間を定めたときの預託元の承認を閲覧し、管理者が管理簿の保管期間を定めるにあたり、預託元の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 保管期間の定めがあるもの、保管期間を定めたときの預託元の承認
			(5)					管理者は、(1) 又は(2) の管理簿を定期的に点検する。		15	管理対象情報管理簿の点検記録を閲覧し、管理者が管理簿を定期的に点検していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿の点検記録
			(6)					管理者は、(1)の管理簿について廃棄をしようとする場合は事業者の取締役等の経営層に、(２)の管理簿について廃棄をしようとする場合は当該管理簿に係る管理対象情報を預けた他者に、それぞれ確認をとる。		16	管理対象情報管理簿の廃棄の確認状況(もしくは、確認記録)の現地調査を実施し、管理者が管理簿を廃棄する場合に、経営層または管理簿に係る預託元に確認を取っていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿の廃棄の確認状況(もしくは、確認記録)
			(7)					管理者は、他者から預けられた管理対象情報等他の技術等情報と明確に区別することが必要なものについて、当該管理対象情報の識別が容易になるよう体系的に管理するための手順を確立する。		17	(他の技術等情報とのく別が必要な管理対象情報を識別するための手順)の閲覧及び手順に沿った識別状況の現地調査を実施し、管理者が預託管理情報等他の技術等情報と明確に区別することが必要なものについて、識別が容易になるよう体系的に管理するための手順を定めていることを確認する。	【規定等】 (他の技術等情報とのく別が必要な管理対象情報を識別するための手順) 【記録やその他の確認対象】 手順に沿った識別状況
		2	(1)				管理対象情報の作成時の識別	管理者は、作成された技術等情報が管理対象情報である場合について、その識別をするための手順を確立する。		18	(管理対象情報を識別するための手順)を閲覧し、管理者が管理対象情報を識別をするための手順を定めていることを確認する。	【規定等】 (管理対象情報を識別するための手順) 【記録やその他の確認対象】
			(2)					管理者は、(1)の手順に従って措置が講じられていることを実地に確認すること等その措置が速やかに講じられることを確保するために必要な取組を行う。		19	管理対象情報の識別を確保する取組の実施状況に関する、管理者の上長または経営層による確認状況の現地調査を実施し、管理者が(1)の手順に従った措置が速やかに講じられることを確保するために必要な取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の識別を確保する取組の実施状況に関する、管理者の上長または経営層による確認状況

章	節	項	番		内容					ID	確認内容	確認対象
			(3)					管理者は、他者から預けられた管理対象情報が他の技術等情報と組み合わされている場合等において、当該他者から、当該管理対象情報が識別可能となるようにすることを求められたときは、当該他者の求めに応じ、下線を引く、枠囲いをする等管理対象情報が分かるよう適切な措置を講ずる。		20	管理対象情報の区別状況（自らのもの、預託管理対象情報）の現地調査を実施し、管理者は、預託管理対象情報を他の情報と組み合わせて利用する際に識別可能となるよう預託元から求められた場合に、当該管理対象情報が他の情報の中で区別できるよう適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の区別状況（自らのもの、預託管理対象情報）
		3	(1)				管理対象情報の内容の伝達	管理者は、原則として、この告示のⅡによりアクセス権を設定された者（以下「アクセス権者」という。）に限り、管理対象情報の内容の伝達（管理対象情報である紙情報や電子情報に記録された事項を当該紙情報や当該電子情報を用いずに口頭等により伝えること及び閲覧させることをいう。）がされるようにするための手順を確立する。		21	情報資産管理規程を閲覧し、管理者がアクセス権者に限り管理対象情報の内容の伝達されるための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】
			(2)					管理者は、アクセス権者がそのアクセス権者の属する事業者の他の従業員等（管理対象情報の他のアクセス権者を除く。以下この第四において「他の従業員等」という。）に対して管理対象情報の内容の伝達をしようとする場合には、当該アクセス権者から、管理者に対して承認を得るための手順を確立する。		22	情報資産管理規程を閲覧し、管理者がアクセス権者が他の従業員等に対して管理対象情報の内容の伝達する際に管理者の承認を得るための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】
			(3)					管理者は、アクセス権者から他の従業員等に対する管理対象情報の内容の伝達についての承認を求められた場合には、当該伝達が真に必要なものか否かの確認を行い、伝達の範囲を可能な限り限定した上で、これを認める。		23	管理対象情報の他の従業員等に対する内容伝達の承認要求時の手順（及び、管理対象情報管理簿）を閲覧し、管理者がアクセス権者から管理対象情報の内容の伝達についての承認を求められた場合には、伝達が真に必要なものか否かの確認を行い、伝達の範囲を可能な限り限定した上で、これを認めているか管理者の上長又は経営者が確認していることを確認する。	【規定等】 管理対象情報の他の従業員等に対する内容伝達の承認要求時の手順 【記録やその他の確認対象】 （及び、管理対象情報管理簿）
			(4)					管理者は、管理対象情報の内容の伝達について、1の（1）又は（2）の管理簿に記録する。		24	管理対象情報管理簿を閲覧し、管理者が管理対象情報の内容の伝達を管理簿に記録していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿
		4	(1)				管理対象情報の複製	管理者は、管理対象情報の複製をアクセス権者のみが行うことができるようにするための手順を確立する。		25	情報資産管理規程を閲覧し、管理者が管理対象情報の複製をアクセス権者のみに許可することを手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】
			(2)					管理者は、アクセス権者が、管理対象情報の複製をしようとする場合には、当該アクセス権者から、管理者に対して承認を得るための手順を確立する。		26	情報資産管理規程を閲覧し、管理者が、管理対象情報の複製をする際にアクセス権者を承認するための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】

章	節	項	番		内容					ID	確認内容	確認対象
			(3)				管理者は、アクセス権者から管理対象情報の複製についての承認を求められた場合には、当該複製が真に必要なものか否かの確認を行い、複製の範囲を可能な限り限定した上で、これを認める。			27	管理対象情報の複製の承認要求時の手順（及び、管理対象情報管理簿）を閲覧し、管理者がアクセス権者から管理対象情報の複製の承認を求められた場合に、必要性の確認、範囲の限定を指示のうえ、承認していることを管理者の上長又は経営者が確認していることを確認する。	【規定等】 管理対象情報の複製の承認要求時の手順 【記録やその他の確認対象】 （及び、管理対象情報管理簿）
			(4)				事業者は、電子情報である管理対象情報について、情報システム（ハードウェア、ソフトウェア（プログラムの集合体をいう。以下同じ。）、ネットワーク又は電子記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。）を構成する機器及び可搬式記録媒体（USB記録媒体、光ディスク、外付けハードディスク等パーソナルコンピュータ等に挿入し、又は接続することでパーソナルコンピュータ等に記録されている情報を記録することが可能な電子記録媒体をいう。以下同じ。）であって、個人が管理するものへの複製をするための手順を確立する。			28	情報資産管理規程を閲覧し、電子情報である管理対象情報について、個人が管理する情報システムを構成する機器及び可搬式記録媒体への複製の手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】
			(5)				事業者は、管理対象情報を複製した場合において、当該複製された情報を管理対象情報として適切に管理する。			29	（管理対象情報管理簿、及び）複製した管理対象情報の管理状況の現地調査を実施し、管理対象情報の複製にあたり、複製した情報を管理対象情報と同等の方法で管理していることを確認する。	【規定等】 【記録やその他の確認対象】 （管理対象情報管理簿、及び）複製した管理対象情報の管理状況
			(6)				事業者は、管理対象情報の内容を他の記録媒体に記録する場合等において、当該記録媒体自体を管理対象情報として管理するための手順を確立する。			30	情報資産管理規程（及び、管理対象情報管理簿）を閲覧し、管理対象情報の内容を他の記録媒体に記録する場合、記録媒体自体を管理対象情報として管理する手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 （及び、管理対象情報管理簿）
		5	(1)			管理対象情報の廃棄等	事業者は、管理対象情報の廃棄については、当該廃棄に係る管理対象情報を探知することができないよう、紙情報の場合におけるシュレッダーでの細断、電子情報の場合における完全消去や難読化等その管理対象情報の態様に応じ、焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により廃棄をするための手順を確立する。			31	情報資産管理規程（及び、管理対象情報管理簿）を閲覧し、管理対象情報は、焼却、粉砕、細断、溶解、破壊等復元不可能な方法により廃棄するための手順を定めていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 （及び、管理対象情報管理簿）
			(2)				事業者は、紙情報である管理対象情報をシュレッダーにより細断をする場合には、以下に掲げるいずれかの性能を有するシュレッダーを用いる。			32	一シュレッダーの現地調査を実施し、第四5(2)一二三の性能を有するシュレッダーを用いていることを確認する。（監査時には、シュレッダーの性能を記録する）	【規定等】 一 【記録やその他の確認対象】 シュレッダー
				一				縦横細断方式のシュレッダーであって、一辺を3mm以内とし、細断された紙の面積が4.5 平方mm以内に細断をすることができるもの				
				二				縦横細断方式のシュレッダーであって、細断された紙の面積が10平方mm以内（一辺は1mm 以内とするものに限る。）に細断をすることができるもの				
				三				縦細断方式のシュレッダーであって、一辺を1mm以内に細断をすることができるもの				

章	節	項	番		内容					ID	確認内容	確認対象
			(3)					事業者は、他者から預けられた管理対象情報について、当該他者との間の取引等が終了した場合には、当該他者との取決め等に基づき、速やかに当該他者に返却をし、及び当該他者とともにその記録をし、又は（1）若しくは（2）の方法により廃棄する等の適切な管理をするための取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		33	情報資産管理規程及び預託管理対象情報返却記録、預託管理対象情報の廃棄状況（あるいは、管理対象情報管理簿（預託管理対象情報））の現地調査を実施し、預託された管理対象情報について、取引等終了時には、預託元との取決め等に基づき、速やかに返却、記録をし、または廃棄する等が実施されていることを確認する。	【規定等】 情報資産管理規程 【記録やその他の確認対象】 預託管理対象情報返却記録、預託管理対象情報の廃棄状況（あるいは、管理対象情報管理簿（預託管理対象情報））
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。		34	管理対象情報の管理手法を示したマニュアルを閲覧し、管理対象情報の適切な管理についての具体的な実現手法を記載したマニュアルを作成していることを確認する。	【規定等】 管理対象情報の管理手法を示したマニュアル 【記録やその他の確認対象】
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。		35	管理対象情報の管理手法を示したマニュアルの周知状況の現地調査を実施し、経営層は、マニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認する。（管理対象情報を取り扱う可能性のある者へのインタビューにより、マニュアルを認識しているかどうかを確認する）	【規定等】 【記録やその他の確認対象】 管理対象情報の管理手法を示したマニュアルの周知状況
			(3)					事業者は、管理対象情報が他者から預けられた情報である場合であって、当該管理対象情報についてのマニュアルを当該他者からの求めに応じて作成するときは、当該他者に当該マニュアルの内容についての確認をとる。これを変更するときも、確認をとる。		36	マニュアル作成、変更に関する預託元の確認記録を閲覧し、預託された管理対象情報についてのマニュアルを預託元からの求めに応じて作成、変更するときは、預託元に内容の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 マニュアル作成、変更に関する預託元の確認記録
			(4)					事業者の取締役等の経営層は、第二の2により必要と決定した措置の実施の状況を管理者に記録をさせ、当該記録の保管期間を定め、定期的に確認する。		37	管理措置の実施状況記録、及びその記録の経営者の確認状況の現地調査を実施し、経営層が管理措置の実施状況を管理者に記録をさせ、当該記録の保管期間を定め、定期的に確認していることを確認する。	【規定等】 【記録やその他の確認対象】 管理措置の実施状況記録、及びその記録の経営者の確認状況
	第五					管理対象情報の適切な管理をするためのトレーニング		事業者は、アクセス権者を含む全ての従業員等への管理対象情報を含む技術等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（会議、講義、e-learning等いずれの実施形態であるかを問わない。）を受講させる機会を設け、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、管理対象情報を含む技術等情報に係る認識向上による不正行為者の言い逃れの排除等に資するよう取組を行う。		38	技術等情報管理研修の実施状況（実績）の現地調査を実施し、全ての従業員等への技術等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を設け、必要と決定した措置を実施し、管理対象情報を含む技術等情報に係る認識向上の取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 技術等情報管理研修の実施状況（実績）
		1						事業者は、アクセス権者を含む全ての従業員等に対して、技術等情報の適切な管理に関する知識及び能力の向上を図るため、以下に掲げる事項のうち必要なものに係るトレーニングを受講させる機会を設ける。		39	技術等情報管理研修の実施状況（実績）、及び研修内容（研修資料等）の現地調査を実施し、全ての従業員等に、必要と事業者が考えるもの（選択した内容）を含むトレーニングを受講させる機会を設けている。（監査時には、トレーニングに含まれる内容を記録する）	【規定等】 【記録やその他の確認対象】 技術等情報管理研修の実施状況（実績）、及び研修内容（研修資料等）
				ー					技術等情報と管理対象情報の違い			

章	節	項	番		内容					ID	確認内容	確認対象
				二					管理対象情報を適切に管理することの重要性、意識			
				三					管理対象情報を含む技術等情報の漏えいとその結果の事例			
				四					関係法令の内容			
				五					マニュアル、この告示のⅦの第四の方針又は対策等技術等情報の適切な管理に係る文書を作成している場合には、その内容			
				六					四及び五の関係法令等に違反した場合の処分等			
				七					管理対象情報の漏えいの事故等（管理対象情報の紛失の事故及び改ざん又は破壊がされた事実を含む。以下同じ。）が発生したことを発見した場合の報告手続			
				八					標的型メール等の警戒すべき手口並びに標的型メール等による情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染を防止するための対策及び感染した場合の対処の手順			
		2						事業者は、トレーニングを受講させる機会を定期的に設ける。		40	技術等情報管理研修計画及び技術等情報管理研修記録を閲覧し、トレーニングを受講させる機会を定期的に設けていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 技術等情報管理研修記録
		3						事業者は、従業員等における秘密の管理に係る意識の啓発を一層図るため、アクセス権者を含む全ての従業員等について、トレーニングに加えて、技術等情報の適切な管理に係る従業員相互間の確認を定期的に行わせるようにする。		41	技術等情報管理研修計画及び従業員相互間の定期的な確認記録を閲覧し、アクセス権者を含む全ての従業員等について、トレーニングに加えて、従業員相互間の確認を定期的に行わせていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 従業員相互間の定期的な確認記録
		4						事業者は、アクセス権者（アクセス権を設定することが見込まれる者を含む。）に対して、管理者又は当該管理者が指定する者により、例えば、Need to Knowの原則（情報は必要のある人のみ（情報へのアクセスは必要な人のみ）に伝え、知る必要のない人に伝えない（情報へのアクセスが必要ではない人にはアクセスを認めない。）という原則をいう。以下同じ。）を守ることの重要性（勤務において留意すべき事項を含む。）、管理対象情報の取扱手続の詳細や情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）を含むトレーニングを受講させる機会を設ける。		42	アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）の現地調査を実施し、アクセス権者に対して、管理者又は当該管理者が指定する者により、Need to Knowの原則を守ることの重要性（勤務において留意すべき事項を含む。）、管理対象情報の取扱手続の詳細や情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）を含むトレーニングを受講させる機会を設けていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）

章	節	項	番		内容					ID	確認内容	確認対象
		5						事業者は、アクセス権を設定することが見込まれる者については、原則として、管理対象情報にアクセスさせる前に4のトレーニングを受講させる。		43	研修の実施状況（及び、アクセス権者の設定の管理票）の現地調査を実施し、アクセス権を設定することが見込まれる者には、管理対象情報にアクセスさせる前に4のトレーニングを受講させていることを確認する。	【規定等】 【記録やその他の確認対象】 研修の実施状況（及び、アクセス権者の設定の管理票）
		6						事業者は、アクセス権者に1（1の八の対処を実践させることを含む。）及び4のトレーニングを受講させる機会を1年に1度以上設ける。		44	技術等情報管理研修計画及びアクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）の現地調査を実施し、アクセス権者への技術等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を1年に1度以上設けていることを確認する。	【規定等】 技術等情報管理研修計画 【記録やその他の確認対象】 アクセス権者の技術情報管理研修の実施状況（実績）、及び研修内容(研修資料等）
		7						事業者は、アクセス権者のうちの4のトレーニングの未受講者に対して、アクセス権の失効等の適切な措置を講ずる。		45	アクセス権者のアクセス権の設定等の管理記録の現地調査を実施し、アクセス権者のうちのトレーニングの未受講者に対して、アクセス権の失効等の適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者のアクセス権の設定等の管理記録
	第六					管理対象情報の漏えいの事故等の発生時等の報告		事業者は、従業員等が管理対象情報の漏えいの事故等が発生したことを発見した場合、従業員等が管理対象情報を漏えいさせ、又は目的外に利用することなど事業者内部において情報の取扱いに係る不正を発見した場合等における報告先を、社内規程に定めること、社内における掲示をすること等事業者内部の従業員等の全てが認識できる方法により明らかにした上で、以下に掲げる事項のうち第二の2により必要と決定した措置を実施し、管理対象情報の漏えいの事故等が発生した場合の対応を迅速に講ずる。		46	管理対象情報漏えい事故発生時の報告先の設定状況、及び周知状況の現地調査を実施し、以下の2点について確認する。 ①従業員等が管理対象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 ②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	【規定等】 【記録やその他の確認対象】 管理対象情報漏えい事故発生時の報告先の設定状況、及び周知状況
		1						事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		47	事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者を含む全ての従業員等に対して、管理対象情報の漏えい又はその疑いがある場合、直ちに、報告先に報告させるための手順を定めていることを確認する。	【規定等】 事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況

章	節	項	番		内容					ID	確認内容	確認対象
		2						事業者は、アクセス権者に対して、管理対象情報の紛失の事故及び改ざん若しくは破壊がされた事実、これらの事故若しくは事実につながる事象又はこれらのおそれのある場合等管理対象情報の適切な管理に支障が生じ、又は生じるおそれがあるとアクセス権者が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		48	アクセス権者における事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者に対して、管理対象情報の適切な管理に支障が生じるおそれがある場合に、直ちに、報告先として指定した者に報告をさせるための手順を定めていることを確認する。	【規定等】 アクセス権者における事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況
		3						事業者は、アクセス権者に対して、これまで接触がなかった者からのコンタクト（電話、メール、食事の誘い等）が著しく増加し、又は定期的に行われている場合や、保管容器等管理対象情報への物理的なアクセス制限措置（以下「物理的措置」という。）の不具合、第二の2により必要と決定した措置についてこの告示で求められる事項若しくは情報の取扱いに係る社内規程に照らした場合の不適合又はこれらの不具合若しくは不適合が発生するおそれがあることを発見した場合等管理対象情報の漏えいの兆候とアクセス権者が認める場合に、速やかに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		49	アクセス権者における事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、アクセス権者に対して、管理対象情報の漏えいの兆候とアクセス権者が認める場合に、速やかに、報告をさせるための手順を定めていることを確認する。	【規定等】 アクセス権者における事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況
		4						事業者は、アクセス権者を含む全ての従業員等に対して、以下に掲げる事項を含む管理対象情報の漏えいにつながると考えられる事象を発見した場合に、速やかに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。		50	事故発生時の報告手順及び報告手順の認知状況の現地調査を実施し、全ての従業員等に対して、管理対象情報の漏えいにつながると考えられる事象を発見した場合に、速やかに、報告をさせるための手順を定めていることを確認する。	【規定等】 事故発生時の報告手順 【記録やその他の確認対象】 報告手順の認知状況
				一					管理対象情報への業務上必要のないアクセス行為を発見した場合			
				二					業務上必要がないにもかかわらず、個人が所有する可搬式記録媒体又は通信機器で管理対象情報を取り扱っている行為を発見した場合			
				三					特定の競合他社等外部の者とアクセス権者が頻繁に接触している事象を発見した場合			
				四					物理的措置についての破損等の不具合を発見した場合			
				五					電子情報である管理対象情報を記録しているサーバ等へのアクセス回数が大幅に増加していること、当該サーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等に感染していること又は当該サーバ等への不正アクセスがされていることを発見した場合			
				六					五のサーバ等に接続されている事業者内部の情報システムの他のサーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等に感染していることを発見した場合			

章	節	項	番		内容					ID	確認内容	確認対象
		5						事業者は、アクセス権者に対し、1から4までの報告の後で、アクセス権者が講じた措置を、管理者等当該事業者が報告先として指定した者に報告をさせる。		51	アクセス権者における事故報告後の措置に関する手順を閲覧し、アクセス権者に対し、1から4までの報告の後で、アクセス権者が講じた措置を報告させていることを確認する。(アクセス権者へのインタビューにより、事故報告後の措置に関する手順を認識しているかどうかを確認する)	【規定等】 アクセス権者における事故報告後の措置に関する手順 【記録やその他の確認対象】
		6						事業者は、アクセス権者に対して、1から5までの報告の義務を怠った場合のアクセス権の失効等の適切な措置を講ずるための手順を確立する。		52	アクセス権者の報告義務を怠った場合の失効に関する認識状況の現地調査を実施し、アクセス権者に対して、1から5までの報告の義務を怠った場合のアクセス権の失効等の適切な措置を講ずるための手順を定めていることを確認する。(アクセス権者へのインタビューにより、報告義務を怠った場合にアクセス権の失効することを認識しているかどうかを確認する)	【規定等】 【記録やその他の確認対象】 アクセス権者の報告義務を怠った場合の失効に関する認識状況
		7						事業者は、管理者等事業者が報告先として指定した者が1又は2の報告を受けた場合に、速やかにその事実を取締役等の経営層に報告をする取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		53	経営層への報告手順の認識状況の現地調査を実施し、報告先が、管理対象情報の事故等の報告を受けた場合、速やかに事実を経営層に報告をする取組が行われていることを確認する。	【規定等】 【記録やその他の確認対象】 経営層への報告手順の認識状況
		8						事業者は、管理者等当該事業者が報告先として指定した者が1から4までの報告を受けた場合に、直ちに、証拠の収集により事実関係(漏えいの疑い等)を確認し、管理対象情報の適切な管理に関して必要な措置を講じ、又は講ずることをアクセス権者に指示するよう具体的な手順及び体制(確認をし、又は措置を講ずる責任体制を含む。)を確立する。		54	(管理対象情報漏えい事故対応に関する規程)及び報告先が報告を受けた場合、事実関係の確認や必要な措置を講ずる体制に組み込まれた人員における、手順の周知状況の現地調査を実施し、報告先が1から4までの報告を受けた場合、証拠の収集により事実関係を確認し、必要な措置を講じ、又は講ずることをアクセス権者に指示するよう具体的な手順及び体制(確認をし、又は措置を講ずる責任体制を含む。)を確立していることを確認する。	【規定等】 (管理対象情報漏えい事故対応に関する規程) 【記録やその他の確認対象】 報告先が報告を受けた場合、事実関係の確認や必要な措置を講ずる体制に組み込まれた人員における、手順の周知状況
		9						事業者は、管理対象情報が他者から預けられた情報である場合であって当該管理対象情報に係る5の報告がされたときに、管理者等当該事業者が報告先として指定した者により直ちに当該他者に同じ内容の報告をするための手順(報告をする責任者、連絡窓口、連絡系統図等を含み、常に最新の状態を維持するための手順を含む。)を確立する。この場合において、当該他者から、報告の詳細及び8の確認の結果(収集した証拠を含む。以下この9において同じ。)や措置の状況の報告を求められている場合には、当該報告の詳細及び8の確認の結果や措置の状況の報告の手順も確立する。		55	(管理対象情報漏えい事故対応に関する規程)及び報告先が報告を受けた場合、当該他者に同じ内容の報告をするための手順の認識状況の現地調査を実施し、預託された管理対象情報に係る5の報告がされたときに、報告先により直ちに当該他者に同じ内容の報告をするための手順(報告をする責任者、連絡窓口、連絡系統図等を含み、常に最新の状態を維持するための手順を含む。)を確立していることを確認する。預託元から求められている場合は、報告の詳細及び8の確認の結果や措置(収集した証拠を含む。)の状況の報告の手順も確立していることを確認する。	【規定等】 (管理対象情報漏えい事故対応に関する規程) 【記録やその他の確認対象】 報告先が報告を受けた場合、当該他者に同じ内容の報告をするための手順の認識状況
Ⅱ					管理対象情報への人的アクセスの制限			事業者は、原則として、アクセス権者のみが管理対象情報の取扱いを行い得ることとした上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への人的アクセスの制限を実施する。		56	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)の現地調査を実施し、アクセス権者のみが管理対象情報の取扱いを行い得ることとした上で、管理対象情報への人的アクセスの制限を実施していることを確認する。	【規定等】 【記録やその他の確認対象】 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)

章	節	項	番		内容				ID	確認内容	確認対象
	第一	1			従業員等へのアクセス権の設定		事業者は、社内規程に定めること、社内における掲示をすること等事業者内部の従業員等の全てが認識できる方法により、アクセス権者のみが管理対象情報を取り扱い得ることを明らかにする。		57	アクセス権者のみが管理対象情報を取り扱い得ることを明らかにした社内掲示等の現地調査を実施し、従業員等の全てが認識できる方法により、アクセス権者のみが管理対象情報を取り扱い得ることを明らかにしていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者のみが管理対象情報を取り扱い得ることを明らかにした社内掲示等
		2					管理者は、管理対象情報へのアクセスができる者のアクセス権の設定を行う際は、以下の事項を考慮する。		58	アクセス権者管理簿を閲覧し、管理者がアクセス権の設定を行う際は、第一の2の事項を考慮していることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者管理簿
				一				Need to Knowの原則に照らし、グローバル競争が進む中での国外への技術等情報の流出リスク等を考慮しつつ、必要最小限の範囲となっているか否か。			
				二				事業者内部における情報の取扱いに係る社内規程への違反履歴			
				三				その従業員等の退職、研修員の派遣元への復帰等近い将来において管理対象情報を保有する事業者の直接の管理の対象から外れる可能性			
		3					管理者は、2に掲げる事項のほか、個人情報保護など関連する法令等に抵触しない範囲において、現に有する情報（法令の違反履歴、社内における飲酒トラブルの報告等をいう。この3において同じ。）又は入手することが可能な情報に基づき、その従業員等についてのレビューをした上で、管理対象情報へのアクセスができる者のアクセス権の設定を行う。		59	アクセス制御設定時のレビュー状況の現地調査を実施し、アクセス権の設定を行う際は、従業員等についてのレビューをした上で行っていることを確認する。（管理者へのインタビューにより、アクセス制御設定時のレビュー状況を確認する）	【規定等】 【記録やその他の確認対象】 アクセス制御設定時のレビュー状況
		4					管理者は、アクセス権の設定について、統一的な判断基準（考え方）の下で行う。		60	（アクセス権設定に関する手順）及び（アクセス制御設定管理簿）の現地調査を実施し、管理者がアクセス権の設定について、統一的な判断基準の下で行っていることを確認する。	【規定等】 （アクセス権設定に関する手順） 【記録やその他の確認対象】 （アクセス制御設定管理簿）
		5					事業者は、全ての管理対象情報へのアクセス権の設定を一人の管理者が行っている場合には、当該アクセス権の設定に係る監査を当該管理者の上司等の他の者が行うことを確保するための仕組みを設ける。		61	アクセス権設定に係る監査の実施状況の現地調査を実施し、アクセス権の設定を一人の管理者が行っている場合には、アクセス権の設定に係る監査を他の者が行うことを確保するための仕組みを設けていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権設定に係る監査の実施状況

章	節	項	番		内容				ID	確認内容	確認対象
		6						事業者は、管理者以外の者がアクセス権の設定を行っているときは、当該管理者以外の者に対し、管理者にアクセス権の設定をされた者の氏名等必要な事項を連絡させる。	62	(管理者以外の者によるアクセス権の設定に関する手順)及び管理者以外でアクセス権の設定をされた者に関する事項の管理者への連絡状況の現地調査を実施し、管理者以外の者がアクセス権の設定を行っているときは、管理者以外の者に対し、管理者にアクセス権の設定をされた者の氏名等必要な事項を連絡させていることを確認する。	【規定等】 (管理者以外の者によるアクセス権の設定に関する手順) 【記録やその他の確認対象】 管理者以外でアクセス権の設定をされた者に関する事項の管理者への連絡状況
		7						事業者は、管理対象情報が他者から預けられた情報である場合には、当該他者からの要請に応じ、当該他者が、当該他者における当該管理対象情報の管理と同程度の管理を実現するために必要となるアクセス権の設定に係る調査をアクセス権の設定をすることが見込まれる者の同意の下で行う場合があることを、アクセス権の設定をすることが見込まれる者に対して説明をする。	63	預託元からの要請の有無、アクセス権の設定に係る調査時の説明記録の現地調査を実施し、預託元からアクセス権の設定に係る調査が行われる場合があることを、アクセス権の設定をすることが見込まれる者に対して説明していることを確認する。	【規定等】 【記録やその他の確認対象】 預託元からの要請の有無、アクセス権の設定に係る調査時の説明記録
	第二	1				アクセス権の管理		管理者は、アクセス権者の範囲を、定期的に、少なくとも個別のアクセス権の設定に係る業務の終了時点(例えば研究開発プロジェクトに係るアクセス権の設定であれば当該プロジェクトの終了時点)等の適切な時点で見直す。	64	(アクセス制御設定管理簿)の現地調査を実施し、管理者が、アクセス権者の範囲を定期的に、見直していることを確認する。	【規定等】 【記録やその他の確認対象】 (アクセス制御設定管理簿)
		2						管理者は、アクセス権者の従事する管理対象情報に係る業務の内容等に応じ、当該アクセス権者のアクセスの範囲を限定し、その責任を明確にする。	65	(アクセス権設定に関する手順)及び(アクセス制御設定管理簿)の現地調査を実施し、管理者が、アクセス権者の業務の内容等に応じ、アクセス範囲を限定し、その責任を明確にしていることを確認する。	【規定等】 (アクセス権設定に関する手順) 【記録やその他の確認対象】 (アクセス制御設定管理簿)
		3						管理者は、アクセス権者の従事する管理対象情報に係る業務の状況を確認すること等を通じて適切に状況を把握し、管理対象情報の適切な管理に関して必要な対応をアクセス権者に指示する。この場合において、管理者は、当該アクセス権者以外のアクセス権者に、手順を定めて、状況を把握させ、管理対象情報の適切な管理に関して必要な対応を指示させることができる。	66	管理者によるアクセス権者の業務の確認状況、管理者からアクセス権者への必要な対応の指示状況、当該アクセス権者以外のアクセス権者における対応手順の現地調査を実施し、管理者が、アクセス権者の管理対象情報の適切な管理に関して必要な対応をアクセス権者に指示していることを確認する。	【規定等】 【記録やその他の確認対象】 管理者によるアクセス権者の業務の確認状況、管理者からアクセス権者への必要な対応の指示状況、当該アクセス権者以外のアクセス権者における対応手順
		4						管理者は、退職等により必要のなくなった従業員等のアクセス権を直ちに失効をさせること等によりアクセス権を適切に管理する。	67	(アクセス制御設定管理簿)の現地調査を実施し、管理者が、必要のなくなったアクセス権を直ちに失効をさせること等によりアクセス権を適切に管理していることを確認する。	【規定等】 【記録やその他の確認対象】 (アクセス制御設定管理簿)
		5						管理者は、アクセス権の管理を確実なものとするため、アクセス権者の氏名、役職、アクセス権の設定年月日、トレーニングの受講の状況等アクセス権者の範囲及びアクセス権者の状況を記録した管理簿を作成し、合理的な期間保管する。	68	アクセス制御設定管理簿の現地調査を実施し、管理者が、アクセス権者の情報を記録した管理簿を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス制御設定管理簿

章	節	項	番		内容					ID	確認内容	確認対象
	第三	1				アクセス権者に対する秘密保持等に関する担保		事業者は、アクセス権者としての責任を明確にするため、アクセス権者から、以下の事項のうち必要なもの（一以上に限る。）を確保する秘密保持の誓約書を得、又は秘密保持契約を締結する等文書（当該アクセス権者が、アクセス権を設定される前に当該事業者に提出した誓約書又は当該事業者と締結した秘密保持契約を含む。）により確認する（以下誓約書及び秘密保持契約を総称して「誓約書等」という。）。		69	秘密保持の誓約書等を閲覧し、アクセス権者から、秘密保持の誓約書等を得ていることを確認する。	【規定等】 【記録やその他の確認対象】 秘密保持の誓約書等
				一					第三者に対する守秘義務を厳守すること。			
				二					アクセス権の設定の解除の後（退職後も含む。）、も 当該アクセス権が設定されている間に知り得た管理対象情報について、公知になったものを除き、不正に開示し、又は使用しないこと。			
				三					マニュアルその他の事業者内部における情報の取扱いに係る社内規程を遵守すること。			
				四					管理対象情報の漏えいにつがなり得る事象等を発見した場合に管理者等事業者が指定した者に報告を行うとともに、管理対象情報の漏えいの事故等が発生した場合に必要な措置を講ずること。			
				五					管理対象情報へのアクセスのログ等をアクセス権の設定を行った者等から確認されること。			
				六					管理対象情報に接する必要がなくなった場合は、速やかに、返却すること等所要の対応が求められること。			
		2						事業者又は管理者は、誓約書等の記載事項の定期的な確認を実施するための手順を確立する。		70	誓約書等の定期的な確認手順を閲覧し、事業者又は管理者が、誓約書等の記載事項の定期的な確認を行う手順を定めていることを確認する。	【規定等】 誓約書等の定期的な確認手順 【記録やその他の確認対象】
		3						事業者又は管理者は、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等が発生した場合は、その都度、誓約書等の内容の見直しを実施し、必要に応じて、変更した誓約書等によりアクセス権者の責任を確認するための手順を確立する。		71	誓約書等の確認手順を閲覧し、事業者又は管理者が、状況の変化や事故等が発生した場合は、誓約書等の内容の見直しを実施し、必要に応じて、誓約書等によりアクセス権者の責任を確認するための手順を定めていることを確認する。	【規定等】 誓約書等の確認手順 【記録やその他の確認対象】
		4						事業者は、1に掲げる事項のうち誓約書等の記載事項として含まれていないものを定期的な上司からの説明等によりアクセス権者に理解させるための取組を行う。		72	誓約書等の記載事項として含まれていないものに関する説明記録を閲覧し、誓約書等の記載事項として含まれていないものをアクセス権者に理解させるための取組を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書等の記載事項として含まれていないものに関する説明記録

章	節	項	番		内容					ID	確認内容	確認対象
		5						事業者は、トレーニングによる周知並びにその後の定期的な上司からの説明及び認識の確認等の方法により、アクセス権者としての責任を明確に認識させる。		73	アクセス権者に対する責任に関する周知、説明記録を閲覧し、トレーニングによる周知や定期的な上司からの説明・認識の確認等により、アクセス権者としての責任を明確に認識させていることを確認する。	【規定等】 【記録やその他の確認対象】 アクセス権者に対する責任に関する周知、説明記録
		6						事業者は、他者がアクセス権の設定に際し調査を行う場合には、アクセス権を設定することが見込まれる者に対し、当該調査の後で、1の誓約書等を当該他者に提出することが求められることがあることを説明する。		74	誓約書等の提出が求められることの説明記録を閲覧し、他者がアクセス権の設定に際し調査を行う場合、アクセス権を設定することが見込まれる者に対し、誓約書等の当該他者への提出が要求されることがあることを説明していることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書等の提出が求められることの説明記録
		7						事業者は、アクセス権者が確立された手順を守らない場合、マニュアル等の管理対象情報の取扱いに係る社内規程への違反等があった場合にアクセス権者のアクセス権の失効をさせる等の措置を講ずるための手順を確立する。		75	（アクセス権者の違反等の場合のアクセス権失効等のための手順）アクセス制御設定記録を閲覧し、アクセス権者が手順を守らない場合、社内規程への違反等があった場合にアクセス権の失効をさせる等の措置を講ずるための手順を定めていることを確認する。	【規定等】 （アクセス権者の違反等の場合のアクセス権失効等のための手順） 【記録やその他の確認対象】 アクセス制御設定記録
		8						事業者は、アクセス権者を含めた従業員等がマニュアルに違反し、管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合に関し、当該従業員等を解雇等の懲戒処分とすることについて就業規則等に定めるとともに、刑事告発や民事訴訟の法的手続に関する規程を社内規程に定める。		76	懲戒処分に関して記載された就業規則等、法的手続きに関する社内規程を閲覧し、従業員等が管理対象情報の漏えい等をした場合に関し、従業員等を懲戒処分とすることについて就業規則等に定めている。法的手続に関する規程を社内規程に定めていることを確認する。	【規定等】 懲戒処分に関して記載された就業規則等、法的手続きに関する社内規程 【記録やその他の確認対象】
		9						事業者は、アクセス権者を含めた従業員等が管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合には、当該不正の事例及びその処分の内容を全ての従業員等に周知する。		77	インシデント発生時の周知内容、周知時期の記録（実際に発生した場合。なお、発生がある場合、従業員へのインタビューにより、周知内容を認識しているか確認）を閲覧し、従業員等が管理対象情報を漏えい等をした場合には、不正事例及び処分内容を全ての従業員等に周知していることを確認する。	【規定等】 【記録やその他の確認対象】 インシデント発生時の周知内容、周知時期の記録（実際に発生した場合。なお、発生がある場合、従業員へのインタビューにより、周知内容を認識しているか確認）

章	節	項	番		内容					ID	確認内容	確認対象
	第四	1				その他の場合のアクセス権の設定		管理者は、管理対象情報を保有する事業者のアクセス権者以外の従業員等や、当該事業者の従業員等以外の者等（以下この第四において「訪問者」という。）による管理対象情報へのアクセス、例えば、立入制限区域にある管理対象情報である製造設備の見学のように一時的なアクセスについて、訪問者がNeed to Knowの原則を満たすものであるかを評価する。		78	アクセス制御及び認証や物理的対策に関する規程及びアクセス制御設定管理簿や施設の入退館記録を閲覧し、管理者が、アクセス権者以外の従業員等や訪問者による管理対象情報へのアクセスについて、例えばNeed to Knowの原則を満たすものであるかを評価していることを確認する。	【規定等】 アクセス制御及び認証や物理的対策に関する規程 【記録やその他の確認対象】 アクセス制御設定管理簿や施設の入退館記録
		2						事業者は、管理対象情報にアクセスする訪問者から、その訪問により得られた管理対象情報を第三者等に開示しないこと等を誓約する書面を得る。		79	誓約書、及び施設の入退館記録を閲覧し、訪問者から、管理対象情報を第三者等に開示しないこと等を誓約する書面を得ていることを確認する。	【規定等】 【記録やその他の確認対象】 誓約書、及び施設の入退館記録
		3						管理者は、訪問者の管理対象情報へのアクセスについて、アクセス権者の立会い等管理対象情報を保護するために適切な措置を講ずる。		80	訪問者アクセスから管理対象情報を保護するための適切な措置、及びこれらの措置の管理者の上長または経営者による確認状況の現地調査を実施し、管理者が、訪問者の管理対象情報へのアクセスについて、アクセス権者の立会い等管理対象情報を保護するために適切な措置を講じていることを確認する。（管理者、及び管理者の上長または経営者へのインタビューにより、措置の状況や確認状況を確認する）	【規定等】 【記録やその他の確認対象】 訪問者アクセスから管理対象情報を保護するための適切な措置、及びこれらの措置の管理者の上長または経営者による確認状況
Ⅲ					管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等			事業者は、管理対象情報が、書類等の紙情報や試作品等の物であって、その管理対象情報が金庫等の保管容器に保管することができるものである場合には、当該管理対象情報を保管容器に施錠して保管するとともに、その保管容器から持ち出して当該管理対象情報の取扱いをする場合には、その取り扱う場所を限定する取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への物理的アクセスを制限する。		81	保管容器、保管容器の取扱場所、管理者による保管容器の管理状況の確認状況の現地調査を実施し、以下の点について確認する。 ①管理対象情報の保管には施錠することができる保管容器を用いること ②管理対象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すること ③管理者が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	【規定等】 【記録やその他の確認対象】 保管容器、保管容器の取扱場所、管理者による保管容器の管理状況の確認状況
	第一	1				管理対象情報を保管するための保管容器		事業者は、管理対象情報を保管する保管容器について、施錠することができる保管容器を用いる。		82	物理的対策に関する規程及び管理対象情報の保管記録、保管容器を閲覧し、施錠された保管容器を用いていることを確認する。	【規定等】 物理的対策に関する規程 【記録やその他の確認対象】 管理対象情報の保管記録、保管容器
		2						管理者、又は管理者の委任を受けたアクセス権者は、保管容器の鍵について、差込み式の鍵である場合にあってはその鍵の貸出しを、文字盤鍵である場合にあってはその鍵番号の設定等を行うことにより、鍵等を管理する。この場合において、管理者又は管理者の委任を受けたアクセス権者が、鍵の貸出し又は鍵番号の共有等をするときは、共有をする相手方をアクセス権者に限るものとする。		83	鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順を閲覧し、アクセス権者は、保管容器の鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順を定めている。その手順に従って、管理者又は管理者の委託を受けたアクセス権者が管理している。	【規定等】 鍵の貸出しや文字盤鍵の鍵番号の設定等による鍵等の管理手順 【記録やその他の確認対象】
		3						管理者は、アクセス権者が貸出しをされた鍵等の管理を適切に行うための手順を確立する。		84	アクセス権者に貸し出された鍵等の適切な管理手順を閲覧し、管理者が、アクセス権者に貸し出された鍵、共有された鍵番号の取扱いの手順を定めていることを確認する。	【規定等】 アクセス権者に貸し出された鍵等の適切な管理手順 【記録やその他の確認対象】

章	節	項	番		内容					ID	確認内容	確認対象
		4						管理者又は管理者の委任を受けたアクセス権者は、鍵の貸出し又は鍵番号の共有を管理するための管理簿を作成し、合理的な期間保管する。		85	鍵の貸出し又は鍵番号の共有を管理するための管理簿の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が管理簿を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 鍵の貸出し又は鍵番号の共有を管理するための管理簿
		5						管理者又は管理者の委任を受けたアクセス権者は、文字盤鍵で施錠することができる保管容器を管理対象情報の保管をするために用いている場合にあっては、当該保管容器の文字盤鍵の鍵番号を1年に1回以上変更する。		86	保管容器の文字鍵版の番号の変更記録の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が鍵番号を1年に1度以上変更していることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器の文字鍵版の番号の変更記録
		6						管理者又は管理者の委任を受けたアクセス権者は、文字盤鍵で施錠することができる保管容器を管理対象情報の保管をするために用いている場合にあっては、当該保管容器の文字盤鍵の鍵番号を、以下のような事象が生じた都度、変更する。		87	イベント毎の発生、鍵番号の変更実績の現地調査を実施し、管理者又は管理者から委任を受けたアクセス権者が、イベント毎に鍵番号を変更していることを確認する。	【規定等】 【記録やその他の確認対象】 イベント毎の発生、鍵番号の変更実績
				一					保管容器の購入後、使用する場所に備え付け、又は使用する場所を変更した場合			
				二					管理者又は管理者の委任を受けたアクセス権者が替わった場合			
				三					鍵番号がアクセス権者以外の者に漏えいし、又はそのおそれがあると管理者又はアクセス権者が認めた場合			
		7						事業者は、管理対象情報を保管するための保管容器について以下に掲げる強度を有するものを用いる。		88	保管容器を閲覧し、管理対象情報を保管する保管容器について、7（1）～（4）に掲げる強度を有するものを用いていることを確認する。（監査時には、保管容器の仕様を記録する）	【規定等】 【記録やその他の確認対象】 保管容器
			(1)					材質について、JISG3141の冷間圧延鋼板及び鋼帯に定める標準厚さ1.2mmの鋼板（保管容器の内部に用いられる鋼板にあっては0.8mm以上の鋼板、裏板に用いられる鋼板にあっては1.0mm以上の鋼板）を使用した場合に得られる強度以上の強度を有する鋼板を用いている保管容器				
			(2)					材質及び構造について、JISS1037の耐火金庫と同等以上の性能を有する保管容器				
			(3)					扉について、丁番が破壊された場合であっても、その開放を防止することができる構造となっている保管容器				
			(4)	一				以下のいずれかの施錠装置を有する保管容器	三段式文字盤鍵で施錠することができる保管容器であって、三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるもの			

章	節	項	番		内容					ID	確認内容	確認対象
				二					三段式文字盤鍵及び差込み式の鍵の組合せにより二重以上の施錠方式で施錠することができる保管容器			
				三					三段式文字盤鍵及び差込み式の鍵の組合せにより二重以上の施錠方式で施錠することができる保管容器であって、その三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ 100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるもの			
				四					生体認証システム及び差込み式鍵の組合せ等により二重以上の施錠方式で施錠することができる保管容器			
		8						事業者は、保管容器を、セキュリティカメラが設置・運用され、又は人感センサーの設置等保管容器に近づく者を適切に確認するための措置（保管容器に近づく者をアクセス権者が視認できるよう視界を確保するためのレイアウト等を含む。）がとられた場所に設置する。		89	保管容器と設置状況の現地調査を実施し、保管容器に近づく者を適切に確認するための措置（保管容器に近づく者をアクセス権者が視認できるよう視界を確保するためのレイアウト等を含む。）がとられた場所に設置していることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器と設置状況
		9						事業者は、保管容器を、この告示のⅣの立入制限区域に設置する。		90	立入制限区域、保管容器の設置状況の現地調査を実施し、保管容器を立入制限区域に設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域、保管容器の設置状況
		10						事業者は、8又は9の場所に保管容器を設置した場合において、ワイヤで固定すること等により保管容器を物理的に持ち出せないよう適切な措置を講ずる。		91	保管容器の設置状況を閲覧し、保管容器をワイヤで固定すること等物理的に持ち出せないような措置が講じられていることを確認する。	【規定等】 【記録やその他の確認対象】 保管容器の設置状況
	第二	1				管理対象情報の取扱いをする場所		管理者は、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所を限定するための手順を確立する。		92	アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順及び手順に沿っているかの管理者の確認状況の現地調査を実施し、アクセス権者が管理対象情報を保管容器から持ち出して、立ち入り制限区域でのみ取り扱うための手順を管理者が作成していることを確認する。	【規定等】 アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順 【記録やその他の確認対象】 手順に沿っているかの管理者の確認状況

章	節	項	番		内容					ID	確認内容	確認対象
		2						管理者は、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所をこの告示のⅣの立入制限区域に限定するための手順を確立する。この手順には、アクセス権者が管理対象情報の取扱いをする場所をこの告示のⅣの立入制限区域ではない場所で取り扱う(管理者が当該場所で管理対象情報を取り扱うことによる当該管理対象情報の漏えいの事故等が生じ、又はそのおそれがないと認める場合に限る。)ための承認の手順を含むことができる。		93	アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順を閲覧し、アクセス権者が管理対象情報を保管容器から持ち出して、その取扱いをする場所を立入制限区域に限定していることを確認する。アクセス権者が管理対象情報を保管容器から持ち出して、立入制限区域ではない場所で取り扱うための承認の手順を含むことができる。	【規定等】 アクセス権者が管理対象情報を保管容器から持ち出す場所を限定する手順 【記録やその他の確認対象】
	第三	1				管理対象情報の運搬		管理者は、管理対象情報を保管容器から持ち出し、当該管理対象情報を取り扱うために当該管理対象情報を取り扱う場所に運搬すること、当該取り扱う場所から保管容器に運搬すること等を、アクセス権者又は管理者が指定した者に限り認めるための手順を確立する。		94	管理対象情報の運搬に関する手順及び(管理対象情報管理簿)を閲覧し、管理対象情報の運搬について、アクセス権者又は管理者が指定した者に限り、認めるための手順を管理者が定めていることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 (管理対象情報管理簿)
		2						管理者は、管理対象情報を管理者が指定した者が運搬する場合に、外部から当該管理対象情報を視認することができず、かつ、運搬中に不正があった場合に確認等ができるよう、当該管理対象情報を封筒に入れて封印する等の適切な措置を講ずるための手順を確立する。		95	管理対象情報の運搬に関する手順及び(管理対象情報管理簿)を閲覧し、管理対象情報を管理者が指定する者が運搬する場合に、外部から当該管理対象情報を視認することができないようにする等のため、封筒に入れて封印する等の適切な手順を管理者が定めていることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 (管理対象情報管理簿)
		3						管理者は、管理者が指定した者が、管理対象情報を運搬し、当該管理対象情報を取り扱うための場所等においてアクセス権者に引き渡したときに、当該アクセス権者から受領証を受け取り、管理者に提出するための手順を確立する。		96	管理対象情報の運搬に関する手順及びアクセス権者からの受領証の現地調査を実施し、管理対象情報の運搬について、管理者が指定した者が運搬する運搬し、アクセス権者に引き渡したときに、当該アクセス権者から受領証を受け取り、管理者に提出することを内容とする手順を管理者が定めており、その手順に従って管理者が指定した者から受領証が管理者に提出されている。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 アクセス権者からの受領証
		4						管理者は、管理対象情報を管理者が指定した者が運搬する場合に、当該管理対象情報を引き渡した者及び引き渡された者が相互に、その内容等についての確認を行うための手順を確立する。		97	管理対象情報の運搬に関する手順及び引き渡す側と引き渡された側の相互の確認結果の現地調査を実施し、管理対象情報の運搬について、管理者が指定した者が運搬する場合に、引き渡す側と引き渡された側で、相互に、その内容についての確認をするための手順を管理者が定めており、その手順に従って相互で確認している。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 引き渡す側と引き渡された側の相互の確認結果

章	節	項	番		内容					ID	確認内容	確認対象
		5						管理者は、管理対象情報が保管されている保管容器の設置された場所のある事業所以外の当該管理者の属する事業者の事業所等に運搬する必要がある場合又は当該管理者の属する事業者以外の者の事業所等に管理対象情報を運搬する必要がある場合に、その運搬を信頼できる輸送機関又は運搬事業者により行わせるための手順（その運搬中に管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果に基づき当該事故等への対応をするための手順を含む。）を確立する。		98	管理対象情報の運搬に関する手順及び輸送機関又は運搬事業者の確認結果を閲覧し、管理対象情報が保管されている保管容器の設置された場所のある事業所以外の事業所等に管理対象情報を運搬する場合に、その運搬を信頼できる輸送機関又は運搬事業者により行わせるための手順（その運搬中に管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果に基づき当該事故等への対応をするための手順を含む。）があり、その手順に従い信頼できる輸送機関又は運搬事業者に運搬を行わせている。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 輸送機関又は運搬事業者の確認結果
		6						管理者は、当該管理者の属する事業者以外の者に管理対象情報を運搬する必要がある場合には、当該者の情報の管理について評価し、及び当該者と秘密保持契約を締結しているかを確認するための手順（当該者が管理対象情報を受領した場合に、受領した日付、受取者のサイン等を受領証に記載する手順を含む。）を確立する。当該事業者以外の者から当該事業者に運搬する場合も同様とする。		99	管理対象情報の運搬に関する手順及び秘密保持契約、及び受領証を閲覧し、管理者の属する事業者以外の者に管理対象情報を運搬する又は当該者から当該事業者に運搬する場合には、当該者の情報の管理について評価し、及び当該者と秘密保持契約を締結しているかを確認するための手順（当該者が管理対象情報を受領した場合に、受領した日付、受取者のサイン等を受領証に記載する手順を含む。）があることを確認する。	【規定等】 管理対象情報の運搬に関する手順 【記録やその他の確認対象】 秘密保持契約、及び受領証
Ⅳ					管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等			事業者は、管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等には、当該管理対象情報が置かれ、又は置かれようとす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取組が習慣化し、文書等に定めがなくても当該事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報への物理的アクセスの制限を実施する。		100-1	物理的対策に関する規程及びアクセス制御設定管理簿や立入制限の入退室記録を閲覧し、以下の点について確認する。 ①管理対象情報が製造装置である場合等に、保管容器に保管することが困難な場合、当該管理対象情報が置かれ、又は置かれようとす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 ②立入制限区域の状況、立入制限された場所の管理の状況を確認していること	【規定等】 物理的対策に関する規程 【記録やその他の確認対象】 アクセス制御設定管理簿や立入制限の入退室記録
								なお、事業者の管理対象情報を取り扱う事業所等が当該事業者以外の他者の所有に係る場合等には、当該他者（当該事業所等の管理をする者を含む。）、に Ⅵの秘密保持契約及び施錠、巡回監視等当該事業所等の適切な管理を依頼する契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第二の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。		100-2	委託管理に関する規程及び他者との秘密保持契約、警備委託契約を閲覧し、管理対象情報を取り扱う事業者の事業所等が当該事業者以外の他者の所有に係る場合等には、他者に秘密保持契約及び施錠、巡回監視等当該事業所等の適切な管理を依頼する契約を締結した上で、自社が定めた対策を実施していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 他者との秘密保持契約、警備委託契約

章	節	項	番		内容				ID	確認内容	確認対象
	第一	1			立入制限区域の構造と管理		事業者は、壁その他の物理的な境界で他の区域と区分することができる区域であってその区域が他の区域と接触する全ての入退室口を、差込み式の鍵、文字盤鍵、キーパッド式の鍵、認証システム（ICカード認証、生体認証、ワンタイムパスワード、PIN入力等）等により施錠することができる区域を立入制限区域として設定する。		101	物理的な境界、立入制限区域の施錠可能状況を閲覧し、物理的な境界で区分でき、全ての入退室口を施錠できる区域を立入制限区域として設定していることを確認する。	【規定等】 【記録やその他の確認対象】 物理的な境界、立入制限区域の施錠可能状況
		2					事業者は、立入制限区域に係る入退室口を、原則として業務時間中のみ開錠する。		102	立入制限区域の解錠・施錠記録を閲覧し、立入制限区域に係る入退室口を、原則として業務時間中のみ開錠していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の解錠・施錠記録
		3					事業者は、鍵の管理簿の作成、受付の設置による受付簿の管理、IDによる認証の導入、作業をしている者以外の者による同行と確認等により、立入制限区域へのアクセス権者を含む全ての者の立入りの状況（立入者の所属、氏名及び立入りの目的等を含む。）を記録し、合理的な期間保管することで事後的に確認可能とするための適切な措置を講ずる。		103	事後的に確認可能な措置の状況（鍵の管理簿、受付簿、認証状況、作業者以外の同行・確認状況等）を閲覧し、鍵の管理簿の作成、受付の設置による受付簿の管理、IDによる認証の導入、作業者以外の者による同行と確認等により、立入制限区域への全ての者の立入りの状況（立入者の所属、氏名及び立入りの目的等を含む。）を記録し、事後的に確認可能とするための適切な措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 事後的に確認可能な措置の状況（鍵の管理簿、受付簿、認証状況、作業者以外の同行・確認状況等）
		4					事業者は、立入制限区域の鍵を三段式文字盤鍵又は認証システム及び差込み式の鍵の組合せ等による二重以上の施錠方式のものとする。		104	立入制限区域の施錠状況の現地調査を実施し、立入制限区域の鍵を三段式文字盤鍵又は認証システム及び差込み式の鍵の組合せ等による二重以上の施錠方式のものとしていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の施錠状況
		5					事業者は、立入制限区域の鍵を三段式文字盤鍵とする場合は、その三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、それぞれ100目盛とし、内蔵回転盤は1目盛ごとに任意の番号に調整できる組合せで、その組合せは100の3乗以上となるものを用いる。		105	立入制限区域の施錠状況の現地調査を実施し、立入制限区域の鍵の三段式文字盤鍵のダイヤル及び内蔵回転盤の目盛は、5に定められるものを用いていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の施錠状況
		6					事業者は、立入制限区域の内側に緊急時に開錠するための非常開閉装置を設ける。		106	立入制限区域の非常開閉装置の設置状況の現地調査を実施し、立入制限区域の内側に非常開閉装置を設けていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の非常開閉装置の設置状況
		7					事業者は、立入制限区域についての一定の強度を確保するため、当該立入制限区域を、以下に掲げる構造を有する施設にする。		107	立入制限区域の現地調査を実施し、立入制限区域を、第一の7の構造を有する施設にしていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域

章	節	項	番		内容					ID	確認内容	確認対象
				一					その立入制限区域と他の区域とを区分する壁や天井、床について、鉄筋コンクリート又は不燃性の資材を用いた堅固な構造			
				二					その立入制限区域と他の区域とを区分する壁や天井、床について、厚さ10cm以上の鉄筋コンクリートを用いた堅固な構造又は以下に掲げるいずれかの方法による堅固な構造 イ 補強コンクリートブロックを用いる場合 中空部をコンクリートで充填した厚さ15cm以上のコンクリートブロックを用いた上で、直径9mm以上の鉄筋を縦40cm以下、横20cm以下の間隔で配筋する構造 ロ 鉄板を用いる場合 厚さ3.2mm以上の鉄板を用いて強化する構造（当該立入制限区域の内側と外側にそれぞれ鉄板を用いる場合には、それぞれの鉄板が1.6mm以上とすることを含む。） ハ 不燃性の資材を用いる場合 厚さ10cm以上の鉄筋コンクリートと同等以上の強度を有する不燃材を用いて強化する構造			
				三					その立入制限区域の天井の裏が、他の区域の天井の裏と接続している場合に、その境界部に金網を設置すること等により他の区域からの侵入を防止する構造			
				四					その立入制限区域の入退室口を一箇所とする構造（非常用の入退室口を別に設ける場合にあっては、立入制限区域の内側からのみ開けることができる扉とする構造）であって、当該入退室口の扉の上に常夜灯（停電時でも作動するものに限る。）を設けている構造			
				五					その立入制限区域の入退室口の扉として鋼鉄を用いている構造			
				六					その立入制限区域の入退室口の扉について、厚さ3.2mm以上の鋼鉄を用いたものであって、当該扉の丁番が当該立入制限区域の内側に埋め込まれたものを有する構造（当該丁番が切断された場合でも扉の開放を防止することができるものに限る。）			
				七					その立入制限区域の入退室口の扉に備え付けられるのぞき窓がドアスコープとなっている構造			
				八					その立入制限区域の入退室口の扉が両開きである場合には、その合わせ目に定規ぶちを取り付けている構造			

章	節	項	番		内容					ID	確認内容	確認対象
				九					その立入制限区域に窓がない構造又は窓がある場合には、必要最低限の数の不透明な窓となっており、かつ、当該窓に直径13mm以上の鉄棒で、その間隔が10cm以下となるよう鉄格子を堅固に取り付けた構造			
				十					その立入制限区域に備え付けられたダクト、通風調節装置、天窓、下水溝等の開口部が、大きさ、形状等から人の侵入、人による盗み見又は盗聴のおそれがあると認められるものである場合に、当該開口部に直径13mm以上の鉄棒で、その間隔が10cm以下となるよう鉄格子を堅固に取り付け、又は金網を取り付けた構造			
		8						事業者は、立入制限区域の扉を開けたときに、中が見えないようにカーテン又は衝立等を設置する。		108	立入制限区域の現地調査を実施し、立入制限区域の中が見えないようにカーテン又は衝立等を設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		9						事業者は、ある施設の内部に間仕切りを用いて立入制限区域を設定する場合には、当該間仕切りは7の一又は二の資材を用いて天井まで届く高さの不透明な構造（特に高い天井の場合には、代用天井を用いて天井と代用天井の間を金網で補強する構造）とする。		109	立入制限区域の現地調査を実施し、立入制限区域の間仕切りは7の一又は二の資材を用いて天井まで届く高さの不透明な構造としていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		10						事業者は、赤外線警報装置、セキュリティカメラ等の警備システムの導入により、立入制限区域への不審者の侵入に係る視認性を高める。		110	立入制限区域に帯する警備システムの現地調査を実施し、立入制限区域への不審者の侵入に係る視認性を高めていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域に帯する警備システム
		11						事業者は、立入制限区域の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。		111	警備体制又は警備委託契約を閲覧し、立入制限区域の警備員等の駆けつけ体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備体制又は警備委託契約
		12						事業者は、警備員等がモニターにより立入制限区域及びその周辺を常時監視する体制を確保する。		112	常時監視体制又は警備委託契約を閲覧し、警備員等が立入制限区域及びその周辺を常時監視する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 常時監視体制又は警備委託契約

章	節	項	番		内容					ID	確認内容	確認対象
		13						事業者は、警備員等により立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保する。		113	巡回監視体制又は警備委託契約を閲覧し、立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 巡回監視体制又は警備委託契約
		14						管理者は、災害等緊急時の対応のため、立入制限区域の全ての鍵の解錠が可能なマスターキーの製作、共通パスワードの設定等がされている場合には、そのマスターキー等の管理の手順を確立する。		114	マスターキーや共通パスワード等の管理手順及びマスターキーや共通パスワード等の管理状況の現地調査を実施し、管理者が、立入制限区域のマスターキー、共通パスワード等の管理の手順を定めていることを確認する。	【規定等】 マスターキーや共通パスワード等の管理手順 【記録やその他の確認対象】 マスターキーや共通パスワード等の管理状況
		15						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とする。		115	立入制限区域の現地調査を実施し、立入制限区域を、他の区域と物理的に独立した施設としていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		16						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、当該施設の周囲を1.8m以上の壁又はフェンス等で覆うこと等により不審者の容易な侵入を防ぐ措置を講ずる。		116	立入制限区域の現地調査を実施し、立入制限区域を他の区域と物理的に独立した施設とし、周囲を1.8m以上の壁等で覆うこと等により、不審者の容易な侵入を防ぐ措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		17						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、当該施設の基礎をコンクリートで固定する。		117	立入制限区域の現地調査を実施し、立入制限区域を他の区域と物理的に独立した施設とし、当該施設の基礎をコンクリートで固定していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		18						事業者は、立入制限区域を、独立した建屋とすること等により他の区域と物理的に独立した施設とし、かつ当該施設が複数ある場合に、その複数の施設を一つの区画に集め、当該区画の周囲を2m以上の壁、フェンス等で覆うことにより不審者の容易な侵入を防ぐ措置を講ずる。		118	立入制限区域の現地調査を実施し、立入制限区域を、他の区域と物理的に独立した施設としている。複数の施設を一つの区画に集め、当該区画の周囲を2m以上の壁、フェンス等で覆っていることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域

章	節	項	番		内容					ID	確認内容	確認対象
		19						管理者は、立入制限区域に管理対象情報が置かれていない状態であっても、アクセス権者以外の立入りを制限する。		119	立入制限区域の入退室記録の現地調査を実施し、管理者が、立入制限区域に管理対象情報が置かれていない状態でも、アクセス権者以外の立入りを制限していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域の入退室記録
		20						事業者又は管理者は、立入制限区域の入退室口の施錠のための鍵又は鍵番号等の管理、警備の体制等立入制限区域を適切に管理するための手順及び体制を確立する。		120	立入制限区域を適切に管理するための手順及び体制の閲覧及び立入制限区域の入退室口の施錠や警備状況の現地調査を実施し、事業者又は管理者は、立入制限区域の入退室口の施錠のための鍵又は鍵番号等の管理、警備の体制等立入制限区域を適切に管理するための手順及び体制を定めていることを確認する。	【規定等】 立入制限区域を適切に管理するための手順及び体制 【記録やその他の確認対象】 立入制限区域の入退室口の施錠や警備状況
	第二	1				立入制限区域への立入者の視認性を高めるため等の措置		事業者は、立入制限区域への全ての立入者について、他の者から視認できるよう、当該立入制限区域に立ち入ることが許されていることがわかる標識の着用を求めるものとする。		121	立入制限区域を適切に管理するための手順の閲覧及び立入制限区域の立入者の標識着用状況の現地調査を実施し、立入制限区域への全ての立入者が視認できるよう、標識の着用を求めていることを確認する。	【規定等】 立入制限区域を適切に管理するための手順 【記録やその他の確認対象】 立入制限区域の立入者の標識着用状況
		2						管理者は、立入制限区域内へのカメラ、携帯型の情報通信機器等の持込みを原則として禁止し、持ち込む必要がある場合には、あらかじめ、管理者の承認を得ることを求めるための手順を確立する。この場合において、立入制限区域内におけるこれらの機器の利用について、管理者は、アクセス権者（当該アクセス権者が自ら使用する場合には別のアクセス権者）の視認できる範囲内においてのみ利用することができる旨を説明する。		122	立入制限区域を適切に管理するための手順の閲覧及び立入制限区域の現地調査を実施し、立入制限区域内へのカメラ、携帯型の情報通信機器等の持込みを原則として禁止し、必要な場合には管理者の承認を得ることを求める手順を定め、アクセス権者の視認できる範囲内においてのみ利用できる旨を説明していることを確認する。	【規定等】 立入制限区域を適切に管理するための手順 【記録やその他の確認対象】 立入制限区域
		3						事業者は、立入制限区域内に、製造設備等の管理対象情報を設置する場合には、当該機器を物理的に持ち出せないようにワイヤ等で固定する。		123	立入制限区域の現地調査を実施し、立入制限区域内の製造設備等の管理対象情報は、物理的に持ち出せないようにワイヤ等で固定していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域
		4						事業者は、立入者の立入制限区域からの退室に際し、当該立入者について、持ち物検査、体重検査等を実施する。		124	立入制限区域の現地調査を実施し、立入制限区域からの退室に際し、持ち物検査、体重検査等を実施していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域

章	節	項	番		内容					ID	確認内容	確認対象
		5						管理者は、アクセス権者以外の者（以下この5において「部外者」という。）の立入制限区域への立入りを認めるための手順（部外者の立入りによる当該立入制限区域に置かれている管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果を踏まえた対応をするための手順、Need to Knowの原則を満たすこと等の立入りの要件及び当該立入制限区域に係る管理対象情報が他者から預けられたものである場合に当該他者により立入りが認められた者に限り立入りを認めるときは、その手続を含む。）を確立する。		125	立入制限区域への立入りを認めるための手順及び立入制限区域への立入り記録を閲覧し、管理者が、アクセス権者以外の者の立入制限区域への立入りを認めるための手順（部外者の立入りによる当該立入制限区域に置かれている管理対象情報の漏えいの事故等が生じ、又は生じるおそれを評価し、その評価の結果を踏まえた対応をするための手順、Need to Knowの原則を満たすこと等の立入りの要件及び当該立入制限区域に係る管理対象情報が他者から預けられたものである場合に当該他者により立入りが認められた者に限り立入りを認めるときは、その手続を含む。）を定めていることを確認する	【規定等】 立入制限区域への立入りを認めるための手順 【記録やその他の確認対象】 立入制限区域への立入り記録
	第三					管理対象情報の運搬		管理者は、管理対象情報の運搬について、この告示のⅢの第三のうちⅠの第二の2により必要と決定した措置を実施する。		126	管理者が、告示Ⅲの第三のうちⅠの第二の2により管理対象情報の運搬について必要と決定した措置を実施していることを確認する。	【規定等】 【記録やその他の確認対象】
Ⅴ					管理対象情報が電子情報である場合のアクセスの制限等			事業者は、管理対象情報が電子情報である場合には、可搬式記録媒体（パーソナルコンピュータを含む。以下このⅤにおいて同じ。）の持ち出しを管理し、当該電子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は、ID認証、パスワード等により当該電子情報へのアクセスをアクセス権者に制限した上で、以下に掲げる事項のうちこの告示のⅠの第二の2により必要と決定した措置を実施して、管理対象情報へのアクセスの制限を実施する。なお、当該電子情報がクラウド等当該事業者以外の者のサーバ等で記録されている場合には、そのクラウド等を管理する者の信頼性を確認（例えば、ISO／IEC27017の認証の取得の状況、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるCSマークの取得の状況等を確認）、し 又は当該事業者以外の者であるデータセンターに自らのサーバ等を設置している場合は、当該データセンターの信頼性を確認（例えば、日本データセンター協会のデータセンターファシリティスタンダードのティア1からティア4を取得しているデータセンターのうち自らの管理対象情報の価値等に応じてデータセンターのサービスを適切に提供し得ること等を確認）、し 当該クラウド等を管理する者又はデータセンターとの間でⅥの秘密保持契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第二の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。		127	IT基盤運用管理に関する規程、クラウド等外部事業者の利用規程及び可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者との秘密保持契約、信頼性確認結果（認証取得状況の確認等）を閲覧し、以下の点について確認する。 ①可搬式記録媒体の持ち出しを管理している。 ②当該電子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。 ③当該事業者以外の者のサーバ等で記録されている場合には、その管理者の信頼性を確認し、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。	【規定等】 IT基盤運用管理に関する規程、クラウド等外部事業者の利用規程 【記録やその他の確認対象】 可搬式記録媒体の持ち出し管理簿、アクセス権設定状況、外部事業者との秘密保持契約、信頼性確認結果（認証取得状況の確認等）
	第一	1				情報システムの管理等		事業者（自らの情報システム（以下単に「情報システム」という。）の維持に責任を有する者を含む。以下2から10までにおいて同じ。）は、情報システムのセキュリティに配慮したログオン手順、電子メールで管理対象情報を送付する場合の手順等を含む操作手順書を作成し、常に利用者が利用可能な状態にする。		128	操作手順書を閲覧し、内容がセキュリティに配慮したログオン手順、管理対象情報を送付する場合の手順などが含まれているか、同操作手順書について常に利用可能な状態におかれているかを確認する。	【規定等】 操作手順書 【記録やその他の確認対象】

章	節	項	番		内容					ID	確認内容	確認対象
		2						事業者は、情報システムとインターネットの間にファイアウォールを導入する。		129	IT基盤運用管理に関する規程及びネットワーク図、セキュリティ対策機器の設定情報等を閲覧し、情報システムとインターネットの間にファイアウォールを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ネットワーク図、セキュリティ対策機器の設定情報等
		3						事業者は、情報システムへのアクセスログ等を取得する。		130	IT基盤運用管理に関する規程及びアクセスログを閲覧し、情報システムへのアクセスログ等を取得していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセスログ
		4						事業者は、3のアクセスログをその記録のあった日から合理的な期間以上保存し、情報システムの維持に責任を有する者（情報システムの管理を当該事業者以外の者に委託等をしている場合には、当該者を含む。以下この第一において同じ。）により定期的に点検させ、当該アクセスログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。		131	IT基盤運用管理に関する規程及びアクセスログ点検記録を閲覧し、アクセスログを合理的な期間以上保存し、情報システムの維持に責任を有する者によりアクセスログを定期的に点検させ、アクセスログを保護するために適切な措置を講じていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセスログ点検記録
		5						事業者は、IDS（Intrusion Detection System）等により、情報システムへの不正なアクセスを検知して、情報システムの維持に責任を有する者に通知するシステムを導入する。		132	IT基盤運用管理に関する規程やインシデント対応手順及びネットワーク図、もしくはシステム構成図を閲覧し、IDS等情報システムへの不正なアクセスを検知し、通知するシステムを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図
		6						事業者は、4の点検の結果により不正なアクセスが発見された場合、5の通知があった場合等に、情報システムの維持に責任を有する者が速やかに、適切な措置を講ずるための手順を確立する。		133	IT基盤運用管理に関する規程やインシデント対応手順を閲覧し、4の点検の結果により不正なアクセスが発見された場合、5の通知があった場合等に、情報システムの維持に責任を有する者が速やかに、対応するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】
		7						事業者は、IPS（Intrusion Prevention System）等により、情報システムへの不正なアクセスを検知し、防御するシステムを導入する。		134	IT基盤運用管理に関する規程やインシデント対応手順及びネットワーク図、もしくはシステム構成図を閲覧し、IPS等により、情報システムへの不正なアクセスを検知し、防御するシステムを導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図
		8						事業者は、ネットワークに接続するサーバについて、不要なポートを閉鎖すること、匿名でのネットワークへの接続（Anonymous接続）を禁止すること等を実施する。		135	IT基盤運用管理に関する規程やインシデント対応手順を閲覧し、ネットワークに接続するサーバについて、不要なポートを閉鎖し、匿名でのネットワークへの接続を禁止すること等を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】

章	節	項	番		内容					ID	確認内容	確認対象
		9						事業者は、最新の脆弱性情報を常時入手し、当該脆弱性情報を、情報システムのセキュリティの向上をしていくために反映等をさせていく仕組みを確立する。		136	IT基盤運用管理に関する規程やインシデント対応手順脆弱性情報入手記録、入手した脆弱性情報の対応記録を閲覧し、最新の脆弱性情報を常時入手し、情報システムのセキュリティ向上のために反映等をさせていく仕組みを確立している。その仕組みに沿って、最新の脆弱性情報を常時入手し、情報システムへの影響を把握し、必要な措置を実施することで、情報セキュリティの向上を実現していることを確認する。	【規定等】 IT基盤運用管理に関する規程やインシデント対応手順 【記録やその他の確認対象】 脆弱性情報入手記録、入手した脆弱性情報の対応記録
		10						事業者は、情報システムを構成するハードウェア、ソフトウェア等について、サポート窓口が明確であり、当該サポート窓口に常時連絡がとれる事業者から導入する。		137	IT基盤運用管理に関する規程及びハードウェア・ソフトウェア管理簿やメーカサポート体制の一覧等を閲覧し、ハードウェア、ソフトウェア等について、サポート窓口が明確であり、サポート窓口に常時連絡がとれる事業者から導入していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ハードウェア・ソフトウェア管理簿やメーカサポート体制の一覧等
		11						情報システムの維持に責任を有する者は、情報システムを構成するハードウェア、ソフトウェア等の管理簿（保守（修理を含む。以下同じ。）及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応の記録を含む。）を作成し、合理的な期間保管する。		138	ネットワーク図、もしくはシステム構成図、ハードウェア・ソフトウェア管理簿を閲覧し、情報システムの維持に責任を有する者は、情報システムを構成するハードウェア、ソフトウェア等の管理簿（保守（修理を含む。以下同じ。）及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応の記録を含む。）を作成し、合理的な期間保管していることを確認する。	【規定等】 【記録やその他の確認対象】 ネットワーク図、もしくはシステム構成図、ハードウェア・ソフトウェア管理簿

章	節	項	番		内容					ID	確認内容	確認対象
		12						事業者（管理者等管理対象情報を取り扱う情報システム（以下このⅤにおいて「管理情報システム」という。）の維持に責任を有する者を含む。22から24までを除き、以下このⅤ及びⅦの第一の3において同じ。）、は 管理情報システムを最新の状態に更新されたウィルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行い、パッチの更新を行うこと等により、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護し、適切に機能を提供するための取組を実施する。		139	IT基盤運用管理に関する規程及びウイルス対策方法が記されたユーザマニュアル等を閲覧し、管理情報システムを最新のウィルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行い、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護し、適切に機能を提供するための取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等
		13						業者は、一定期間（例えば、1週間）電源の切られた状態にある管理情報システムを構成する機器については、再度の電源投入時に12の取組を実施する。		140	IT基盤運用管理に関する規程ウイルス対策方法が記されたユーザマニュアル等を閲覧し、一定期間電源の切られた状態にある管理情報システムを構成する機器については、再度の電源投入時に12の取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等
		14						事業者は、管理対象情報を記録するための可搬式記録媒体について、12又は13の取組を実施する。この場合において、13中「電源の切られた」とあるのは「使用されていない」、「電源投入時」とあるのは「使用の前」とする。		141	IT基盤運用管理に関する規程及びウイルス対策方法が記されたユーザマニュアル等を閲覧し、管理対象情報を記録するための可搬式記録媒体について、12又は13の取組を実施していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ウイルス対策方法が記されたユーザマニュアル等
		15						事業者は、管理情報システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限するための手順を確立する。		142	IT基盤運用管理に関する規程を閲覧し、管理情報システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】
		16						事業者は、管理情報システムにソフトウェアを導入する場合、管理者等管理情報システムの維持に責任を有する者によりソフトウェアの安全性が確認された場合を除き、認めないための手順を確立する。		143	IT基盤運用管理に関する規程を閲覧し、管理情報システムにソフトウェアを導入する場合、ソフトウェアの安全性が確認された場合を除き、認めないための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】

章	節	項	番		内容					ID	確認内容	確認対象
		17						事業者は、管理情報システムに対するペネトレーションテストを定期的に実施する。		144	IT基盤運用管理に関する規程ペネトレーションテスト報告書、ペネトレーションテスト後の対処状況を閲覧し、管理情報システムに対するペネトレーションテストを定期的に実施し、実施結果を踏まえて必要な対処が実施されているか確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ペネトレーションテスト報告書、ペネトレーションテスト後の対処状況
		18						事業者は、この告示のⅣの立入制限区域に管理情報システムを構成する機器のうちサーバ等一定のものを設置する。この場合において、管理者等管理情報システムの維持の責任を有する者は、当該一定のもの以外のサーバ等の持込みを禁止し、及びサーバ等を新設する場合の内蔵ソフトウェアの状況を確認した上で、当該サーバ等が従業員等の個人の所有にかからないものに限り認めるための手順を確立する。		145	IT基盤運用管理に関する規程を閲覧し、立入制限区域には管理情報システムを構成する機器のうちサーバ等一定のものを設置し、それ以外の持込みについて状況を判断のうえ、必要最小限認めるための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】
		19						事業者は、管理情報システムを構成する機器及び立入制限区域等の特定の場所でのみ使用する可搬式記録媒体について、施錠できるラック等への設置、セキュリティワイヤでの固定等不正な持ち出し、盗難等から保護するための措置（ラック等の鍵について、管理者等管理情報システムの維持に責任を有する者による管理を含む。）を講ずる。		146	物理的対策やIT機器利用、IT基盤運用管理に関する規程の閲覧及び管理情報システム構成機器の設置場所の現地調査を実施し、管理情報システムを構成する機器及び可搬式記録媒体について、施錠できるラック等への設置、セキュリティワイヤでの固定等不正な持ち出し、盗難等から保護するための措置（ラック等の鍵について、管理者等管理情報システムの維持に責任を有する者による管理を含む。）を講じていることを確認する。	【規定等】 物理的対策やIT機器利用、IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システム構成機器の設置場所
		20						事業者は、管理者等管理情報システムの維持に責任を有する者が、当該管理情報システムを構成する機器の持ち出しに伴うリスクを回避することができると判断し、その承認をした場合を除き、当該機器を持ち出させないための手順（持ち出しをする場合の記録を含む。）を確立する。		147	IT機器利用やIT基盤運用管理に関する規程及びシステム機器持ち出し管理簿を閲覧し、管理者等情報システムの維持に責任を有する者が、管理情報システムを構成する機器の持ち出しを承認した場合を除き、機器を持ち出させないための手順（持ち出しをする場合の記録を含む。）を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 システム機器持ち出し管理簿
		21						事業者は、管理情報システムを構成する機器について、不要なネットワークポート、USBポート、シリアルポートを物理的に閉塞すること等当該機器に可搬式記録媒体を接続することによる管理対象情報の流出を防止する措置を実施するための手順を確立する。		148	IT機器利用やIT基盤運用管理に関する規程及び管理情報システム構成機器のポートの状況の現地調査を実施し、管理情報システムを構成する機器について、不要なポートを物理的に閉塞すること等当該機器への可搬式記録媒体の接続を防止する措置を実施するための手順を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 管理情報システム構成機器のポートの状況

章	節	項	番		内容					ID	確認内容	確認対象
		22						事業者は、管理者等管理情報システムの維持に責任を有する者の利用権限を必要最低限にとどめ、当該利用権限が最低限であることを定期的に監査するための手順を確立する。		149	IT基盤運用管理に関する規程及びアクセス権設定記録を閲覧し、管理者等情報システムの維持に責任を有する者の利用権限を必要最低限にとどめ、利用権限が最低限であることを定期的に監査するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 アクセス権設定記録
		23						事業者は、管理者等管理情報システムの維持に責任を有する者について、その者による当該管理情報システムの設定変更や運用に関する作業ログを取得する。		150	IT基盤運用管理に関する規程及び機器のセキュリティログ情報等を閲覧し、管理者等情報システムの維持に責任を有する者による管理情報システムの設定変更や運用に関する作業ログを取得していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 機器のセキュリティログ情報等
		24						事業者は、23の作業ログについて、管理者等管理情報システムの維持に責任を有する者の上司等により、又はデータ解析ツール（データマイニングツール）を活用すること等により、定期的に点検させる。		151	IT基盤運用管理に関する規程及び機器のセキュリティログ情報等を閲覧し、23の作業ログについて、管理者等情報システムの維持に責任を有する者の上司等により、定期的に点検させていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 機器のセキュリティログ情報等
		25						事業者は、管理情報システムに係るサービス、システム、機器の保守及び点検をサプライヤー含む外部の第三者に行わせる場合であって、管理対象情報に関わるときは、管理者等管理情報システムの維持に責任を有する者の指示の下で、管理対象情報を他の記録媒体に移した上で、管理対象情報を復元できないように消去する等の措置を実施し、又は従業員等が保守及び点検業務に立ち会い、若しくは作業ログを取得し、若しくはカメラを設置すること等により、作業を監視することができる状況で行わせる手順を確立する。		152	IT基盤運用管理や委託管理に関する規程及び業務委託契約や委託先作業記録を閲覧し、管理情報システムに係る保守及び点検を外部の第三者に行わせ、管理対象情報に関わるときは、管理者等管理情報システムの維持に責任を有する者の指示の下で、管理対象情報を他の記録媒体に移した上で復元できないように消去する等の措置を行い、又は作業を監視することができる状況で行わせる手順を定めていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や委託先作業記録
		26						事業者は、管理情報システムに係るサービス、システム、機器の第三者による情報システムの保守及び点検に当たって、当該第三者の作業者にIDを付与することが必要な場合には、一時的なIDを付与することとし、作業終了後は、その権限を無効化するための手順を確立する。		153	IT基盤運用管理や委託管理に関する規程及び管理情報システムへのアクセス権設定記録を閲覧し、管理情報システムの第三者による保守及び点検に当たって、当該第三者の作業者には一時的なIDを付与し、作業終了後は、その権限を無効化するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 管理情報システムへのアクセス権設定記録

章	節	項	番		内容					ID	確認内容	確認対象
		27						事業者は、管理情報システムを構成する機器をこの告示のⅣの立入制限区域に設置する場合であって、当該管理情報システムを構成する機器の保守及び点検をサプライヤーを含む第三者に行わせるときは、Ⅵの秘密保持契約を締結した上で行わせる。この場合において、管理者等管理情報システムの維持に責任を有する者は、当該第三者の作業者についてこの告示のⅣの第二の6の手順を確立しているときは当該手順に従い、若しくは当該手順を確立していないときは作業者を確認し、当該作業者の立入りを認め、並びに当該立入制限区域内の保守及び点検の対象となる機器以外の機器（当該立入制限区域内に保守及び点検の対象となる機器に記録された管理対象情報以外の管理対象情報が置かれている場合には当該管理対象情報を含む。）を撤去すること等により作業者が当該保守及び点検の対象となる機器以外の機器への接触を防止するための措置を講じた上で、作業者が作業を実施している間は管理者等管理情報システムの維持に責任を有する者が常時立ち会うようにし、又はその指定する者に立ち会わせ、当該指定する者からの作業の状況の報告を受けるものとする。		154	IT基盤運用管理や委託管理に関する規程及び業務委託契約や機密保持契約、委託先作業記録を閲覧し、立入制限区域に設置する管理情報システムを構成する機器の保守及び点検を第三者に行わせるときは、Ⅵの秘密保持契約を締結した上で行わせている。管理情報システムの維持に責任を有する者は、第三者の作業者について告示のⅣの第二の6の手順に従い、若しくは作業者を確認し、立入りを認め、並びに作業者が当該保守及び点検の対象となる機器以外の機器（当該立入制限区域内に保守及び点検の対象となる機器に記録された管理対象情報以外の管理対象情報が置かれている場合には当該管理対象情報を含む。）への接触を防止するための措置を講じた上で、作業間は常時立ち会う、又は指定する者に立ち会わせ作業状況の報告を受けることにより、作業の状況の報告を受けるものとしていることを確認する。	【規定等】 IT基盤運用管理や委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や機密保持契約、委託先作業記録
		28						事業者は、クラウド等を管理する者又はデータセンターのサーバ等で管理対象情報を管理している場合におけるその従業員等が、当該サーバ等の保守及び点検を行うときは、以下のいずれかの措置を実施する。		155	委託管理に関する規程や、クラウドやデータセンターにおける管理規程を閲覧し、クラウド等を管理する者又はデータセンターのサーバ等で管理対象情報を管理している場合、その従業員等が保守及び点検を行うときは、第一の28に定めるいずれかの措置を実施していることを確認する。	【規定等】 委託管理に関する規程や、クラウドやデータセンターにおける管理規程 【記録やその他の確認対象】
				一					その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等である場合 当該保守及び点検を行う従業員等を確認する等の措置			
				二					その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等以外である場合 当該クラウド等を管理する者又はデータセンターにおいて25、26に掲げる措置等適切な措置を講ずることを確認する等の措置			
		29						事業者は、管理対象情報について、定期的な保存（バックアップ）を実施し、当該保存された情報を管理対象情報として適切に管理する。		156	IT基盤運用管理に関する規程及びデータバックアップ管理簿を閲覧し、管理対象情報について、定期的な保存（バックアップ）を実施し、バックアップを管理対象情報として適切に管理していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 データバックアップ管理簿

章	節	項	番		内容					ID	確認内容	確認対象
		30						事業者は、管理情報システムで取り扱われた管理対象情報の漏えいの事故等が発生した場合、その疑いがある場合及び管理対象情報が記録されたサーバ等に情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染又は不正アクセスが認められた場合等に、その証拠を収集するための手順を確立する。		157	IT機器利用やIT基盤運用管理、インシデントの対応手順及びを閲覧し、管理情報システムで取り扱われた管理対象情報の漏えいの事故等が発生した場合等、その証拠を収集するための手順を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】
		31						事業者は、管理情報システムを構成する機器を再利用する場合は、管理対象情報が復元できない状態であることを点検した後で再利用する。		158	IT機器利用やIT基盤運用管理に関する規程及び管理情報システム構成機器のデータ消去記録を閲覧し、管理情報システムを構成する機器を再利用する場合は、管理対象情報が復元できない状態であることを点検した後で再利用していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 管理情報システム構成機器のデータ消去記録
		32						事業者は、管理情報システムの利用の状況、管理情報システムにおける管理対象情報へのアクセス（アクセス権者が利用した管理情報システムを構成する機器並びに当該機器へのログオン又はログオフの日時及びその成否並びに使用されたプログラムを含む。）及び例外処理を記録した監査ログを取得する。		159	IT機器利用やIT基盤運用管理、インシデントの対応手順及び機器のセキュリティログ情報等を閲覧し、管理情報システムの利用状況、管理対象情報へのアクセス（アクセス権者が利用した管理情報システムを構成する機器並びに当該機器へのログオン又はログオフの日時及びその成否並びに使用されたプログラムを含む。）及び例外処理を記録した監査ログを取得していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】 機器のセキュリティログ情報等
		33						事業者は、32の監査ログを記録のあった日から三月以上保存し、定期的に点検し、当該監査ログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。		160	IT機器利用やIT基盤運用管理、インシデントの対応手順及び機器のセキュリティログ情報等を閲覧し、32の監査ログを記録のあった日から三月以上保存し、定期的に点検し、当該監査ログを改ざん又は不正なアクセスから保護するために適切な措置を講じていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理、インシデントの対応手順 【記録やその他の確認対象】 機器のセキュリティログ情報等
		34						事業者は、管理情報システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめる。		161	管理情報システムに対する監査ツールの利用状況の現地調査を実施し、管理情報システムの監査に用いるツールについて、必要最低限の使用にとどめていることを確認する。	【規定等】 【記録やその他の確認対象】 管理情報システムに対する監査ツールの利用状況
		35						事業者は、情報システムを構成するソフトウェアの利用状況を確認し、利用がされていない場合には、当該ソフトウェアを消去する。		162	IT機器利用やIT基盤運用管理に関する規程の閲覧及びソフトウェアの利用状況・削除の確認記録、ソフトウェアの利用状況の現地調査を実施し、情報システムを構成するソフトウェアの利用状況を確認し、利用がされていない場合には、当該ソフトウェアを消去していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 ソフトウェアの利用状況・削除の確認記録、ソフトウェアの利用状況
		36						事業者は、管理情報システム及びネットワークを通じて管理情報システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせる。		163	IT基盤運用管理に関する規程及びシステム構成図を閲覧し、管理情報システム及びネットワークを通じて管理情報システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 システム構成図

章	節	項	番		内容					ID	確認内容	確認対象
		37						事業者は、管理情報システムの共有ネットワーク（インターネット等）への接続については、その接続に伴うリスクから保護するため、アクセス権者の職務内容に応じて設定するアクセス制御の方針（定期的又は管理対象情報の漏えいの事故等があった場合に見直すことができるものに限る。）を定め、これに基づいて認めるための手順を確立する。		164	管理情報システムから共有ネットワークへのアクセス制御方針及び管理情報システムから共有ネットワークへのアクセス制御状況を閲覧し、管理情報システムの共有ネットワークへの接続についてのアクセス制御の方針を定め、これに基づいて認めるための手順を定めていることを確認する。	【規定等】 管理情報システムから共有ネットワークへのアクセス制御方針 【記録やその他の確認対象】 管理情報システムから共有ネットワークへのアクセス制御状況
		38						事業者は、情報システムから外部への通信についてログの取得等により監視する。		165	IT基盤運用管理に関する規程及び情報システムから外部への通信ログを閲覧し、情報システムから外部への通信についてログの取得等により監視していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 情報システムから外部への通信ログ
		39						事業者は、管理情報システムを構成する機器について、無線でのネットワークへの接続をすることができるものを用いない。		166	IT基盤運用管理に関する規程及びシステム構成図等を閲覧し、管理情報システムを構成する機器について、無線ネットワークへの接続をすることができるものを用いていないことを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 システム構成図等
		40						事業者は、管理情報システムを構成する機器を廃棄する場合には、当該機器に記録された管理対象情報が復元できない状態であることを確認し、当該機器を物理的に破壊し、廃棄する。		167	IT機器利用やIT基盤運用管理に関する規程及びIT機器等の廃棄管理簿を閲覧し、管理情報システムを構成する機器を廃棄する場合には、管理対象情報が復元できない状態であることを確認し、物理的に破壊し、廃棄していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 IT機器等の廃棄管理簿
		41						事業者は、立入制限区域の内部のみで利用する管理情報システムを、有線により配線接続して構築し、当該立入制限区域の外部への通信を行わせないための手順を確立する。		168	IT基盤運用管理に関する規程の閲覧及び管理情報システムのネットワーク接続状況の現地調査を実施し、立入制限区域の内部のみで利用する管理情報システムを、有線接続して構築し、外部への通信を行わせないための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システムのネットワーク接続状況
		42						事業者又はアクセス権者は、管理情報システムが無人状態に置かれる場合、使用していない管理情報システムを構成する機器の電源を切り、又は機器の表示画面の表示停止と再表示時にパスワードが必要なよう設定すること等により、無人状態であっても管理対象情報が適切に保護されるよう必要な対応をする。		169	IT基盤運用管理に関する規程の閲覧及び管理情報システムの状況の現地調査を実施し、事業者又はアクセス権者は、管理情報システムが無人状態に置かれる場合、使用していない機器の電源を切り、又はの画面の表示停止とパスワード設定等により、無人状態であっても管理対象情報が適切に保護されるよう必要な対応をしていることを確認する。	【規定等】 IT基盤運用管理に関する規程の閲覧 【記録やその他の確認対象】 管理情報システムの状況

章	節	項	番		内容					ID	確認内容	確認対象
	第二	1				電子情報である管理対象情報へのアクセスに関する対応		事業者は、管理情報システムの利用者の職務内容に応じて、利用できる機能を制限した上で、これを提供する。		170	管理情報システムのアクセス制御及び認証に関する方針及び管理情報システムの機能の利用設定を閲覧し、管理情報システムの利用者の職務内容に応じて、利用できる機能を制限した上で、提供していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 管理情報システムの機能の利用設定
		2						事業者は、アクセス権者による管理情報システムへのアクセスを許可し、適切なアクセス権を付与するため、管理情報システムの利用者としての登録及び人事異動等に伴い速やかに登録の削除をするための手順（定期的な見直しを含む。）を確立する。		171	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、アクセス権者による管理情報システムへのアクセスを許可し、適切なアクセス権を付与するため、管理情報システムの利用者としての登録及び人事異動等に伴い速やかに登録の削除をするための手順（定期的な見直しを含む。）を定めていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況
		3						事業者は、管理情報システムの利用者に対して、初期又は仮のパスワードを発行する場合には、容易に推測されないパスワードを発行する等その適切な管理に配慮した方法で発行する。		172	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、管理情報システムの利用者に対して、容易に推測されない初期又は仮のパスワードを発行していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況
		4						事業者は、管理情報システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させる。		173	管理情報システムのアクセス制御及び認証に関する方針及びアクセス権設定状況を閲覧し、管理情報システムの利用者ごとに一意な識別子を保有させていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】 アクセス権設定状況
		5						事業者は、アクセス権設定等の特別な権限を持つ管理者等管理情報システムの維持に責任を有する者の管理情報システムへのログインに対して、二つの認証機能（パスワード、生体認証、電子証明書等）を組み合わせた二要素認証を導入する。		174	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムへのログイン環境の現地調査を実施し、特別な権限を持つ管理者等の管理情報システムへのログインには、二要素認証を導入していることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムへのログイン環境
		6						事業者は、アクセス権者においてパスワードを自ら設定させ、パスワードを設定する場合には、当人の関連情報（例えば、名前、電話番号、誕生日等）に基づかないこと、辞書攻撃に脆弱でないこと（辞書に含まれる語からだけで成り立っていないこと）、同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではないことを求めること等アクセス権者以外の者から容易に類推されないような設定とするようアクセス権者に周知し、又は管理情報システムでパスワードを設定する者に対してその要求をするようにする。		175	管理情報システムのアクセス制御及び認証に関する方針の閲覧及びアクセス制御及び認証に関する方針の周知状況、又はパスワード設定状況の現地調査を実施し、アクセス権者においてパスワードを設定する場合には、アクセス権者以外の者から容易に類推されないような設定とするようアクセス権者に周知し、又は管理情報システムでパスワードを設定する者に対してその要求をしていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 アクセス制御及び認証に関する方針の周知状況、又はパスワード設定状況

章	節	項	番		内容					ID	確認内容	確認対象
		7						事業者は、管理情報システムそのものに、必要に応じてパスワードの変更を利用者に促す機能やパスワードの再利用を防止する機能等を持つようにする。		176	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムのパスワード設定に関する機能の実装状況の現地調査を実施し、管理情報システムそのものに、パスワードの変更を利用者に促す機能やパスワードの再利用を防止する機能等を持たせていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムのパスワード設定に関する機能の実装状況
		8						管理者等管理情報システムの維持に責任を有する者は、アクセス権者等に対して、管理情報システムにログオンするためのパスワードを記載した紙を目に見えるところに置かないこと等を周知する。		177	パスワード管理に関する周知状況の現地調査を実施し、管理者等は、アクセス権者等に対して、管理情報システムにログオンするためのパスワードを記載した紙を目に見えるところに置かないこと等を周知していることを確認する。	【規定等】 【記録やその他の確認対象】 パスワード管理に関する周知状況
		9						事業者は、管理情報システムへのアクセスについては、複数者間で同じパスワード（共通パスワード）を使用しないための手順を確立する。		178	管理情報システムのアクセス制御及び認証に関する方針の閲覧及び管理情報システムのパスワード設定に関する機能の実装状況、又はパスワード管理に関する周知状況の現地調査を実施し、管理情報システムへのアクセスについては、複数者間で同じパスワードを使用しないための手順を定めていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針の閲覧 【記録やその他の確認対象】 管理情報システムのパスワード設定に関する機能の実装状況、又はパスワード管理に関する周知状況
		10						事業者は、アクセス権者によるテレワーク等外部からの管理情報システムの管理対象情報へのアクセスについて、利用者の認証を行うための手順（管理者等管理情報システムの維持に責任を有する者は、あらかじめ、認めた範囲でのみ認証をするためのものを含む。）を確立するとともに、可能な限り暗号化された通信路を用いさせる。		179	管理情報システムのアクセス制御及び認証に関する方針を閲覧し、アクセス権者による外部からの管理対象情報へのアクセスについて、利用者の認証を行うための手順（管理者等管理情報システムの維持に責任を有する者は、あらかじめ、認めた範囲でのみ認証をするためのものを含む。）を定めていることを確認する。可能な限り暗号化された通信路を用いさせていることを確認する。	【規定等】 管理情報システムのアクセス制御及び認証に関する方針 【記録やその他の確認対象】
		11						管理者等管理情報システムの維持に責任を有する者は、電子政府推奨暗号を用いて暗号化する等の措置を講じた上で管理情報システムにおいて管理対象情報を適切に管理するための手順を確立する。		180	IT基盤運用管理に関する規程を閲覧し、管理者等管理情報システムの維持に責任を有する者は、電子政府推奨暗号を用いて暗号化する等の措置を講じた上で管理情報システムにおいて管理対象情報を適切に管理するための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】

章	節	項	番		内容				ID	確認内容	確認対象
	第三	1			管理対象情報の取扱い		事業者は、可搬式記録媒体に管理対象情報が記録されている場合には、当該可搬式記録媒体を管理対象情報そのものとして取り扱うための手順（可搬式記録媒体の使用を事業者が承認し、当該可搬式記録媒体を他の技術等情報が記録された可搬式記録媒体と容易に区別することができるよう措置するための手順を含む。）を確立する。		181	IT機器利用やIT基盤運用管理に関する規程を閲覧し、可搬式記録媒体に管理対象情報が記録されている場合には、可搬式記録媒体を管理対象情報そのものとして取り扱うための手順（可搬式記録媒体の使用を事業者が承認し、当該可搬式記録媒体を他の技術等情報が記録された可搬式記録媒体と容易に区別することができるよう措置するための手順を含む。）を定めていることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】
		2					管理者等管理情報システムの維持に責任を有する者は、管理対象情報を記録し、又は記録のために用いる可搬式記録媒体の管理簿（保守及び点検の記録、持ち出した場合の持ち出しの記録、データの消去の記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等の記録を含む。）を作成し、合理的な期間保管する。		182	IT機器利用やIT基盤運用管理に関する規程及び可搬式記録媒体管理簿、及び可搬式記録媒体の保存期間を閲覧し、管理者等は、可搬式記録媒体の管理簿（保守及び点検の記録、持ち出した場合の持ち出しの記録、データの消去の記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等の記録を含む。）を作成し、合理的な期間保管していることを確認する。	【規定等】 IT機器利用やIT基盤運用管理に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿、及び可搬式記録媒体の保存期間
		3					事業者は、電子情報である管理対象情報を可搬式記録媒体に記録する場合は、暗号技術を用いる。		183	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、管理対象情報を可搬式記録媒体に記録する場合は、暗号技術を用いていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿
		4					事業者は、管理対象情報を記録した可搬式記録媒体を施錠することができるロッカー等に集中的に保管し、その鍵等を適切に管理する。		184	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、管理対象情報を記録した可搬式記録媒体を施錠することができるロッカー等に集中的に保管し、その鍵等を適切に管理していることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿
		5					事業者は、可搬式記録媒体に記録した管理対象情報を消去する場合には、復元できないように上書き消去（データの完全消去）を速やかに行うための手順を確立する。		185	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、可搬式記録媒体に記録した管理対象情報を消去する場合には、復元できないように上書き消去を速やかに行うための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿
		6					事業者は、5の手順に従い管理対象情報が消去された可搬式記録媒体に限り、その使用を認める。		186	IT機器利用に関する規程及び可搬式記録媒体管理簿を閲覧し、5の手順に従い管理対象情報が消去された可搬式記録媒体に限り、その使用を認めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿

章	節	項	番		内容					ID	確認内容	確認対象
		7						事業者は、管理対象情報が記録されたサーバや可搬式記録媒体の廃棄を行う場合には、ハードディスクドライブ等全体に対して上書き消去（デー タの完全消去）を行い、その消去を確認した上で、物理的な破壊を行うための手順を確立する。		187	IT基盤運用管理に関する規程及び可搬式記録媒体管理簿、又はサーバ廃棄記録を閲覧し、管理対象情報が記録されたサーバや可搬式記録媒体の廃棄を行う場合には、ハードディスクドライブ等全体に対して上書き消去を行い、その消去を確認した上で、物理的な破壊を行うための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿、又はサーバ廃棄記録
		8						事業者は、管理情報システムを構成する機器の廃棄を行う場合には、データを消去すること等により読み取りができない状態にするための手順を確立する。		188	IT基盤運用管理に関する規程ハードウエア・ソフトウエアの管理簿、又は廃棄記録を閲覧し、管理情報システムを構成する機器の廃棄を行う場合には、データを消去すること等により読み取りができない状態にするための手順を定めていることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 ハードウエア・ソフトウエアの管理簿、又は廃棄記録
		9						事業者は、管理情報システムを構成する機器及び可搬式記録媒体であって、個人が所有するもので、管理対象情報を、取り扱わせないための手順を確立する。		189	IT機器利用に関する規程を閲覧し、管理情報システムを構成する機器及び可搬式記録媒体であって、個人が所有するもので、管理対象情報を、取り扱わせないための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】
		10						事業者は、管理対象情報を電子メールで送信する場合は、送信する管理対象情報又は電子メールそのものについて暗号化すること等の適切な措置を講ずるための手順を確立する。		190	電子メール利用に関する規定を閲覧し、電子メールで管理対象情報を送付する場合は、暗号化すること等の適切な措置を講ずるための手順を定めていることを確認する。	【規定等】 電子メール利用に関する規定 【記録やその他の確認対象】
		11						事業者は、管理対象情報を電子メールで送信する場合又は受信する場合に、その送受信のログを合理的な期間保存する。		191	IT基盤運用管理に関する規程及び電子メールの送受信ログ、及びログ保存期間を閲覧し、管理対象情報の電子メールでの送受信ログを合理的な期間保存していることを確認する。	【規定等】 IT基盤運用管理に関する規程 【記録やその他の確認対象】 電子メールの送受信ログ、及びログ保存期間
		12						事業者は、管理対象情報を可搬式記録媒体に保存した上で管理情報システムからの消去を行うこと、他者から預けられた管理対象情報であって可搬式記録媒体に記録されたものを事業者の可搬式記録媒体にのみ保存し、利用すること等により、当該管理対象情報を、必要最小限の範囲で取り扱うための手順を確立する。		192	IT機器利用に関する規程可搬式記録媒体管理簿を閲覧し、管理対象情報を可搬式記録媒体に保存した上で管理情報システムからの消去を行うこと、他者から預けられた管理対象情報であって可搬式記録媒体に記録されたものを事業者の可搬式記録媒体にのみ保存し、利用すること等、管理対象情報を、必要最小限の範囲で取り扱うための手順を定めていることを確認する。	【規定等】 IT機器利用に関する規程 【記録やその他の確認対象】 可搬式記録媒体管理簿
Ⅵ					管理対象情報をその管理対象情報を保有する事業者以外の者に渡す場合の措置			事業者は、管理対象情報を当該事業者の管理に属する従業員等以外の者（以下「外部委託先等」という。）に渡し、取り扱わせる場合には、当該管理対象情報の第三者への開示の禁止等を含む秘密保持契約を締結した後で引き渡す取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立した上で、以下に掲げる事項のうちこの告示のＩの第二の2により必要と決定した措置を実施することを通じて、外部委託先等における管理対象情報の適切な管理を確保する。		193	委託管理に関する規程及び秘密保持契約を閲覧し、管理対象情報を外部委託先等に渡し、取り扱わせる場合には、管理対象情報の第三者への開示の禁止等を含む秘密保持契約を締結した後で引き渡す取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約

章	節	項	番		内容				ID	確認内容	確認対象
	第一	1			外部委託先等に管理対象情報を取り扱わせる前の確認		事業者は、管理対象情報を外部委託先等に取り扱わせる場合には、当該外部委託先等からの情報の流出等のリスクを考慮し、真に必要な取引であるかを検討した上で行う。		194	委託管理に関する規程を閲覧し、管理対象情報を外部委託先等に取り扱わせる場合には、真に必要な取引であるかを検討した上で行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】
		2					事業者は、管理対象情報の取扱いを外部委託先等に行わせる場合には、当該外部委託先等が、管理対象情報を適切に管理し、かつ、当該事業者の要請に適切に対応できる能力を有するか否かについて事前に確認する。この確認は、基本的には、自らが講じている管理対象情報の適切な管理に係る取組と同等以上の取組が外部委託先等において行われているか否かを確認し、特に、外部委託先等が海外企業である場合等には、物理的に管理が行き届かないことや、法律や商慣行の違い等により漏えいリスクが高まる可能性も考えられるため、より確実に行う。		195	委託管理に関する規程及び業務委託契約を閲覧し、管理対象情報の取扱いの外部委託先等が、管理対象情報を適切に管理し、かつ、事業者の要請に適切に対応できる能力を有するか否かについて事前に確認していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 業務委託契約
		3					事業者は、管理対象情報を外部委託先等に渡す場合の当該外部委託先等の事前の確認及び評価のための手順を確立する。		196	委託管理に関する規程を閲覧し、管理対象情報を外部委託先等に渡す場合の当該外部委託先等の事前の確認及び評価のための手順を定めていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】
		4					事業者は、必要に応じて、外部委託先等に対して、作成したこの告示のⅦの第四の方針等を周知する。		197	委託管理に関する規程及び業務委託契約や委託先作業管理簿を閲覧し、外部委託先等に対して、作成した方針等を周知していることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 業務委託契約や委託先作業管理簿
	第二	1			秘密保持契約		事業者は、管理対象情報を外部委託先等に提供する前に、以下の事項のうち必要なものを含む秘密保持契約の締結又はこれに準ずる法的拘束力のある取決めを交わす取組が習慣化し、文書等の定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。		198	委託管理に関する規程及び秘密保持契約を閲覧し、管理対象情報を外部委託先等に提供する前に、秘密保持契約の締結又はこれに準ずる法的拘束力のある取決めを交わす取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約
				一				外部委託先等は、提供された管理対象情報の取扱者を限定すること。			
				二				外部委託先等は、提供された管理対象情報の取扱者の氏名等を明らかにすること。			
				三				外部委託先等における提供された管理対象情報の取扱者の範囲がNeed to Knowの原則に照らして必要最小限であることを、当該管理対象情報を提供する者が確認すること。			
				四				外部委託先等は、外部委託先等における提供された管理対象情報の取扱者による管理対象情報へのアクセスを記録し、管理すること。			

章	節	項	番		内容					ID	確認内容	確認対象
				五				外部委託先等は、提供された管理対象情報の複製、廃棄等をした場合の管理簿を作成し、合理的な期間保管すること。				
				六				外部委託先等は、管理対象情報を提供する者から求められている場合には、当該管理対象情報を提供する者に対して、当該管理対象情報の複製、廃棄等をした旨の通知を行うこと。				
				七				外部委託先等は、提供された管理対象情報に係る契約の満了時又は解除時において、当該管理対象情報を速やかに廃棄又は返還等をすること。				
				八				外部委託先等は、管理対象情報を提供する者に対して、当該管理対象情報の状況について、定期的に報告をすること。				
				九				外部委託先等において、定期的又は不定期に管理対象情報を提供する者からの監査を受け入れること。				
				十				管理対象情報を提供する者及び外部委託先等の両者の責任の下で、管理対象情報が秘密保持契約等の対象である旨の表示を提供する管理対象情報に付し、提供された管理対象情報の目録を作成し、最新のものに更新し、維持すること。				
		2						事業者は、秘密保持契約又は取決めのひな形を定める。		199	委託管理に関する規程及び秘密保持契約のひな型を閲覧し、秘密保持契約又は取決めのひな形を定めていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 秘密保持契約のひな型
Ⅶ	第一	1			その他の管理対象情報の管理を強化するための措置	管理対象情報の段階を分けた管理と対応		事業者は、管理対象情報をその価値等に応じて段階を設けて管理し、当該段階に応じてこの告示のⅠの第三の管理者を選任（複数の段階の管理対象情報に係る管理者を一の者とすることを含む。）し、価値の高いものであればよりアクセス権者を限定し、物理的措置を複数組み合わせて強化する等の措置を講ずる。		201	管理対象情報の段階分けルール及び価値の高い管理対象情報に対する対策強化の状況の現地調査を実施し、管理対象情報をその価値等に応じて段階を設けて管理し、段階に応じてⅠ第三の管理者を選任（複数の段階の管理対象情報に係る管理者を一の者とすることを含む。）し、価値の高いものは対策を強化する等の措置を講じていることを確認する。	【規定等】 管理対象情報の段階分けルール 【記録やその他の確認対象】 価値の高い管理対象情報に対する対策強化の状況

章	節	項	番		内容					ID	確認内容	確認対象
		2						事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって、この告示のⅠの第四の1の(1)の管理簿を作成するときは、その段階に応じて、管理簿を分けて作成する。		202	管理対象情報管理簿(段階別)を閲覧し、管理対象情報を段階を設けて管理する場合、段階に応じて、管理簿を分けて作成していることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報管理簿(段階別)
		3						事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって、当該管理対象情報が電子情報であるときの管理情報システムが提供する機能について、アクセス権者に対し、提供する機能を制限する。		203	管理情報システムの提供機能の現地調査を実施し、管理対象情報を段階を設けて管理する場合、管理情報システムが提供する機能について、アクセス権者に対し、提供する機能を制限していることを確認する。	【規定等】 【記録やその他の確認対象】 管理情報システムの提供機能
		4						事業者は、管理対象情報のうち特に価値の高いもの等を管理するために立入制限区域の内部で間仕切りする場合には、入退室口及び警報装置を間仕切りした区画ごとに独立して設置する。		204	立入制限区域内の間仕切り区画の現地調査を実施し、立入制限区域の内部を間仕切りする場合には、入退室口及び警報装置を間仕切りした区画ごとに独立して設置していることを確認する。	【規定等】 【記録やその他の確認対象】 立入制限区域内の間仕切り区画
	第二	1				管理対象情報のより強固な管理のための敷地全体の防護		事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を金網等で囲う。		205	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を金網等で囲っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周
		2						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を、高さ2m以上の金網等で囲う。		206	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を、高さ2m以上の金網等で囲っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周

章	節	項	番		内容					ID	確認内容	確認対象
		3						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周を囲う金網等の上部に2本以上の有刺鉄線等で敷地の外側に向かって角度をつけた忍び返しを設け、全体の高さを2.4m以上の外柵とする。		207	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周を囲う金網等の上部に2本以上の有刺鉄線等で敷地の外側に向かって角度をつけた忍び返しを設け、全体の高さを2.4m以上の外柵としていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周
		4						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周には、赤外線警報装置、セキュリティカメラ等警備システムの導入により不審者の侵入に係る視認性を高める措置の導入を行う。		208	敷地の外周の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周には、不審者の侵入に係る視認性を高める措置の導入を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 敷地の外周
		5						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。		209	警備員等の駆けつけ体制の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周の警備システムが作動した場合の警備員等の駆けつけ体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備員等の駆けつけ体制
		6						事業者は、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周及びその周辺をモニターにより警備員等が常時監視する体制を確保する。		210	警備員等の常時監視体制の現地調査を実施し、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周及びその周辺を警備員等が常時監視する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 警備員等の常時監視体制

章	節	項	番		内容					ID	確認内容	確認対象
		7						事業者は、警備員等により、管理対象情報に係る保管容器、立入制限区域又はサーバ等が設置された事業所等全体の敷地の外周及びその周辺を4時間に1回以上巡回監視を実施する体制を確保する。		211	巡回監視体制の現地調査を実施し、警備員等により、管理対象情報に係る保管容器等が設置された事業所等全体の敷地の外周及びその周辺を4時間に1回以上巡回監視を実施する体制を確保していることを確認する。	【規定等】 【記録やその他の確認対象】 巡回監視体制
	第三	1				外部委託先等における管理対象情報をより的確に管理するために考えられる措置		事業者は、外部委託先等に管理対象情報を提供する場合には、可能な限り分割して引き渡すことにより、管理対象情報の全体が外部委託先等から見てわからないようにする取組を行う。		212	及び委託先への管理対象情報受け渡し状況の現地調査を実施し、外部委託先等に管理対象情報を提供する場合、可能な限り分割して引き渡すことにより、管理対象情報の全体が外部委託先等から見てわからないようにする取組を行っていることを確認する。（管理者へのインタビューにより、委託先への管理対象情報受け渡し状況を確認する）	【規定等】 【記録やその他の確認対象】 委託先への管理対象情報受け渡し状況
		2						事業者は、製造設備のリモートメンテナンス等、管理対象情報そのものを渡すことにはならない一方で、長期にわたり徐々に技術等情報がリモートメンテナンス等を行う事業者に蓄積され、管理対象情報を構成することができるような事例にも対応するため、この告示のⅥの措置を組み合わせて、外部委託先等が技術等情報を適切に管理し、かつ、自らの要請に適切に対応できる能力を有するか否かについて事前に確認をし、蓄積された管理対象情報の目的外利用の禁止（例えば、リモートメンテナンスであればリモートメンテナンス目的のみに利用することを規定する。）、第三者への開示の禁止を契約で明記し、条件違反等契約に違反した場合に損害賠償請求等の法的措置をとる旨の記載を行う等の取組を行う。		213	委託管理に関する規程及び契約書等を閲覧し、長期にわたり徐々に技術等情報がリモートメンテナンス等を行う事業者に蓄積され、管理対象情報を構成することができるような事例にも対応するため、外部委託先等が技術等情報を適切に管理し、かつ、自らの要請に適切に対応できる能力を有するか否かについて事前に確認をしている。蓄積された管理対象情報の目的外利用の禁止、第三者への開示の禁止を契約で明記し、条件違反等契約に違反した場合に損害賠償請求等の法的措置をとる旨の記載を行う等の取組を行っていることを確認する。	【規定等】 委託管理に関する規程 【記録やその他の確認対象】 契約書等
		3						事業者は、管理対象情報を外部委託先等において取り扱わせる場合において、当該外部委託先等で管理対象情報に関連するもの（例えば、製造委託をした場合の製造設備）に係るメンテナンス等を第三者に行わせる場合については、当該メンテナンス等を通じて管理対象情報が漏えいしていくことも念頭におき、当該メンテナンス等を行う事業者について、当該管理対象情報を提供した者の承認を条件とすること等の適切な管理をする。		214	外部委託契約書の現地調査を実施し、外部委託先等において管理対象情報に関連するものを第三者に行わせる場合については、管理対象情報を提供した者の承認を条件とすること等の適切な管理を行っていることを確認する。	【規定等】 【記録やその他の確認対象】 外部委託契約書
		4						事業者は、外部委託先等として、当該事業者と内外の他の事業者等とのジョイントベンチャー（以下「JV」という。）を組み、当該JVを構成する企業（以下「JV企業」という。）に管理対象情報を提供する場合については、JVの契約において、当該事業者からの取締役の派遣等コーポレートガバナンスを確実に効かせる措置を講ずる。		215	JVの役員構成等コーポレートガバナンスの状況の現地調査を実施し、外部委託先等として、JV企業に管理対象情報を提供する場合は、JVの契約において、コーポレートガバナンスを確実に効かせる措置を講じていることを確認する。	【規定等】 【記録やその他の確認対象】 JVの役員構成等コーポレートガバナンスの状況

章	節	項	番		内容					ID	確認内容	確認対象
		5						事業者は、JV企業における管理対象情報の受入れに関しては、4の取締役の派遣とともに、管理対象情報の受入れについて当該JV企業の取締役会の全会一致の仕組みとすること等により、JV企業側において、組織機能的に、当該事業者からJV企業に管理対象情報が容易に引き渡されないような手順を確立する。		216	JV企業における管理対象情報の取り扱い手順を閲覧し、JV企業における管理対象情報の受入れに関しては、4の取締役の派遣とともに、JV企業側において、組織機能的に、管理対象情報が容易に引き渡されないような手順を定めていることを確認する。	【規定等】 JV企業における管理対象情報の取り扱い手順 【記録やその他の確認対象】
	第四	1				管理対象情報を継続的かつ適切に管理するための体制の構築等について		事業者は、管理対象情報ごとに、これを取り扱う関係部署の責任及び役割（複数の関係部署にまたがる場合には、これらの分担を含む。）を明確にする。		217	管理対象情報に関する関係部署の組織図、又は所掌が示された社内規程等を閲覧し、管理対象情報ごとに、関係部署の責任及び役割（複数の関係部署にまたがる場合には、これらの分担を含む。）を明確にしていることを確認する。	【規定等】 管理対象情報に関する関係部署の組織図、又は所掌が示された社内規程等 【記録やその他の確認対象】
		2						事業者は、管理対象情報の適切な管理に関する基本的な方針（以下この第四において「方針」という。）を作成する。		218	管理対象情報の管理方針を閲覧し、管理対象情報の適切な管理に関する基本的な方針を作成していることを確認する。	【規定等】 管理対象情報の管理方針 【記録やその他の確認対象】
		3						事業者は、方針及びこの告示のⅠの第二の2により必要と決定した措置に沿って、管理対象情報の適切な管理に向けた対策（以下この第四において「対策」という。）を作成し、当該対策が確実に実施されていることについての記録をする。		219	管理対象情報の対策の作成状況、実施の記録状況の現地調査を実施し、管理対象情報の適切な管理に向けた対策を作成し、当該対策が確実に実施されていることについての記録をしていることを確認する。	【規定等】 【記録やその他の確認対象】 管理対象情報の対策の作成状況、実施の記録状況
		4						事業者は、管理対象情報が他者から預けられた情報である場合であって、当該管理対象情報に係る方針又は対策を定めたときは、当該他者に当該方針又は対策の内容についての確認をとる。		220	預託管理対象情報に係る方針又は対策を定めたときの預託元への確認状況の現地調査を実施し、預託元に、管理対象情報に係る方針又は対策の内容の確認をとっていることを確認する。	【規定等】 【記録やその他の確認対象】 預託管理対象情報に係る方針又は対策を定めたときの預託元への確認状況

章	節	項	番		内容					ID	確認内容	確認対象
		5						事業者は、方針又は対策について、管理対象情報を取り扱う可能性のある全ての者に周知し、方針に基づき、これらの者（誓約書等を提出していない者に限る。）から情報の取扱いに係る社内規程やマニュアルに従った手続の履行に関する誓約書を取得する。		221	方針又は対策の周知状況、手続の履行に関する誓約書の現地調査を実施し、方針又は対策について、管理対象情報を取り扱う可能性のある全ての者に周知し、方針に基づき、これらの者から情報の取扱いに係る社内規程やマニュアルに従った手続の履行に関する誓約書を取得することを確認する。	【規定等】 【記録やその他の確認対象】 方針又は対策の周知状況、手続の履行に関する誓約書
		6						事業者は、方針、対策又はマニュアルについて、定期的に見直しを実施し、当該方針、対策又はマニュアルを適切、有効かつ妥当なものに維持するための手順を確立する。		222	方針、対策又はマニュアルの見直し手順を閲覧し、方針、対策又はマニュアルについて、定期的に見直しを実施し、当該方針、対策又はマニュアルを適切、有効かつ妥当なものに維持するための手順を定めていることを確認する。	【規定等】 方針、対策又はマニュアルの見直し手順 【記録やその他の確認対象】
		7						事業者は、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等への対応、内部及び外部からの攻撃に関する監視、測定、評価の結果から教訓を導き出し、その都度管理対象情報を管理するプロセスを継続的に改善する体制を確立する（方針、対策又はマニュアルを作成している場合には、これらを必要に応じて変更することを含む。）。		223	組織的対策に関する規程及び管理対象情報リスク評価結果や経営者によるマネジメントレビューの結果を閲覧し、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等への対応、内部及び外部からの攻撃に関する監視、測定、評価の結果から教訓を導き出し、管理対象情報を管理するプロセスを継続的に改善する体制を確立（方針、対策又はマニュアルを作成している場合には、これらを必要に応じて変更することを含む。）していることを確認する。	【規定等】 組織的対策に関する規程 【記録やその他の確認対象】 管理対象情報リスク評価結果や経営者によるマネジメントレビューの結果

章	節	項	番		内容					ID	確認内容	確認対象
		8						事業者の取締役等の経営層（管理対象情報が他者から預けられた情報である場合は、当該預けられた情報を活用し、事業を実施する部門の長を含む。）は、方針、対策又はマニュアルが作成（変更を含む。）された場合はその承認をすることや、管理対象情報の適切な管理の責任の明確化、自らの関与の明示等により、管理対象情報の適切な管理を確立するための取組を行う。		224	方針、対策又はマニュアルの作成・変更の際の経営層の承認状況、または管理責任の明確化や自らの関与の明示等の状況の現地調査を実施し、経営層は、方針、対策又はマニュアルが作成された場合、その承認や、管理対象情報の管理責任の明確化、自らの関与の明示等により、管理対象情報の適切な管理を確立するための取組を行っていることを確認する。 経営層は、方針、対策又はマニュアルが作成・変更された場合はその承認をすることや、管理対象情報の適切な管理の責任の明確化、自らの関与の明示等により、管理対象情報	【規定等】 【記録やその他の確認対象】 方針、対策又はマニュアルの作成・変更の際の経営層の承認状況、または管理責任の明確化や自らの関与の明示等の状況
		9						管理者は、方針、対策又はマニュアルについて、その責任の範囲において、これらの遵守状況（技術的な遵守状況も含む。）を確認する。		225	方針、対策又はマニュアルの遵守状況に関する管理者の確認状況の現地調査を実施し、管理者は、方針、対策又はマニュアルについて、その責任の範囲において、これらの遵守状況（技術的な遵守状況も含む。）を確認していることを確認する。	【規定等】 【記録やその他の確認対象】 方針、対策又はマニュアルの遵守状況に関する管理者の確認状況
		10						管理者は、管理対象情報の適切な管理について、定期的に、又は情報の適切な管理に係る状況の重大な変化が生じた場合に監査を実施し、必要に応じた是正措置を講ずるための手順を確立する。この場合において、管理者は、監査の結果を、合理的な期間（管理対象情報が他者から預けられた情報である場合は当該他者が求める期間）、当該結果を施錠することができるロッカー等において、又は暗号技術を用いて電子化し、適切に管理（当該ロッカー等の鍵の管理を含む。）する。		226	監査及び是正措置を講ずるための手順及び監査結果の管理状況の現地調査を実施し、管理者は、管理対象情報の適切な管理について、定期的に、又は情報の適切な管理に係る状況の重大な変化が生じた場合に監査を実施し、必要に応じた是正措置を講ずるための手順を定めていることを確認する。管理者は、監査の結果を合理的な期間、施錠することができるロッカー等において、又は暗号技術を用いて電子化し、適切に管理（当該ロッカー等の鍵の管理を含む。）していることを確認する。	【規定等】 監査及び是正措置を講ずるための手順 【記録やその他の確認対象】 監査結果の管理状況
		11						事業者は、あらかじめ、自らの事業継続計画、コンティンジェンシープラン等に管理対象情報の漏えいの事故等を位置付け、当該漏えいの事故等が発生した場合の影響の最小化と事業継続のための措置を決定する。		227	事業継続計画を閲覧し、自らの事業継続計画、コンティンジェンシープラン等に管理対象情報の漏えいの事故等を位置付け、当該漏えいの事故等が発生した場合の影響の最小化と事業継続のための措置を決定していることを確認する。	【規定等】 事業継続計画 【記録やその他の確認対象】
		12						事業者は、管理対象情報の漏えい等の事故等に係る対応により得られた教訓を事業継続計画、コンティンジェンシープラン等に反映させ、継続的に見直していくための手順を確立する。		228	管理対象情報の漏えい等の事故等に係る対応により得られた教訓を事業継続計画、コンティンジェンシープラン等に反映させ、継続的に見直していくための手順を定めていることを確認する。	【規定等】 【記録やその他の確認対象】