○技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準

（平成三十年九月二十五日）
（内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第三号）

産業競争力強化法（平成二十五年法律第九十八号）第二条第二十四項第一号の規定に基づき、技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準を次のように定める。

技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準

Ⅰ　共通事項

第一　適切な管理をする必要がある技術等情報の特定

１　事業者は、技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報（以下「技術等情報」という。）について、その技術等情報の価値等に応じて選別し、第三以下に掲げる措置のうち必要と判断されるものの対象とする技術等情報（以下「管理対象情報」という。）を特定する。

２　技術等情報のうち管理対象情報の特定に当たっては、事業者の経営層も関与した上で、以下の事項を考慮する。

一　その技術等情報が漏えいした場合に、自らの競争力に重大な影響を与えるか否か。

二　他者から契約等に基づき預けられた情報であること等により、その技術等情報が漏えいした場合に自らの信用、他者との信頼関係等に対して重大な影響を与えるか否か。

３　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。

第二　管理対象情報の識別と必要な措置の整理

１　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、第四の１の管理簿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。

２　事業者は、管理対象情報について、その価値及び態様等に応じて、この告示に掲げる措置のうち必要なものを決定する。

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。

第三　管理者の選任

１　原則

（１）　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。

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情報の管理についての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。

（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。

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。

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。

１　管理対象情報の管理簿の作成等

（１）　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。

（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。

（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。

（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。

（５） 管理者は、（１）又は（２）の管理簿を定期的に点検する。

（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。

（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。

２ 管理対象情報の作成時の識別

（１） 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。

（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。

（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。

３ 管理対象情報の内容の伝達

（１） 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。

（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。

（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。

（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。

４ 管理対象情報の複製

（１） 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。

（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。

（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。

（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。）、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。

（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管理する。

（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。

５　管理対象情報の廃棄等

（１） 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。

（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。

一　縦横細断方式のシュレッダーであって、一辺を３㎜以内とし、細断された紙の面積が4.5平方㎜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㎜以内（一辺は１㎜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１㎜以内に細断をすることができるもの

（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。

６　管理対象情報の適切な管理についての文書の作成等

（１） 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（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。）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。

（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。

（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。

（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、当該期間の保管期間を定め、当該記録を定期的に確認する。

第五　管理対象情報の的確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。

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。

一　技術等情報と管理対象情報の違い

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。

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。

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。

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。

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。

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。

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等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。

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。

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。

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。

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。

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

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。

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。

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。

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。

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。

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。

第一　従業員等へのアクセス権の設定

１　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。

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。

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。

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。

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。

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。

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。

第二　アクセス権の管理

1　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。

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。

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。

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。

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。

第三　アクセス権者に対する秘密保持等に関する担保

1　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。）。

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。

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。

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。

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。

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。

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。

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。

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。

第四　その他の場合のアクセス権の設定

1　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。

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。

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。

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。

第一　管理対象情報を保管するための保管容器

1　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。

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。

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。

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。

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。

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。

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。

（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 1.2㎜ の鋼板（保管容器の内部に用いられる鋼板にあっては 0.8㎜ 以上の鋼板、裏板に用いられる鋼板にあっては 1.0㎜ 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）以下のいずれかの施錠装置を有する保管容器

一　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

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。

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。

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。

第二　管理対象情報の取扱いをする場所

1　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。

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。

第三　管理対象情報の運搬

1　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。

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。

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。

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。

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。

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。

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。

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。

第一　立入制限区域の構造と管理

1　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。

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。

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。

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。

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。

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。

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。

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９㎜ 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 3.2㎜ 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 1.6㎜ 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 3.2㎜ 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

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 13㎜ 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 13㎜ 以上の鉄棒で、その間隔が 10㎝ 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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

第二　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

１　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。

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。

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。

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。

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。

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。

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。

第一　情報システムの管理等

1　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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

13　事業者は、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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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管理する。

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。

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。

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対象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。

33　事業者は、32 の監査ログを記録のあった日から３か月以上保存し、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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

第二　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

1　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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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対象情報を管理情報システムにおいて適切に管理するための手順を確立する。

第三　管理対象情報の取扱い

1　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。

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。

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。

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。

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。

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。

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。

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。

9　事業者は、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。

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。

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。

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。

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、管理対象情報の外部委託先等における適切な管理を確保する。

第一　外部委託先等に管理対象情報を取り扱わせる前の確認

1　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。

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、当該事業者自らの情報の管理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。

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。

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。

第二　秘密保持契約

１　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。

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。

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管理の状況について、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。

Ⅶ　その他の管理対象情報の管理を強化するための措置

事業者は、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、管理対象情報の管理の強化を実施する。

第一　管理対象情報の段階を分けた管理と対応

１　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。

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。

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。

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。

第二　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

１　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。

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。

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。

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。

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。

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。

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。

第三　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

１　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。

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。

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等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等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。

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。

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流れないような手順を確立する。

第四　管理対象情報を継続的かつ的確に管理するための体制の構築等について

1　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。

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。

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。

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指針の内容についての確認をとる。

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。

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。

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。）。

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。

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。

10　管理者は、管理対象情報の管理の状況について、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。

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。

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。