○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

（令和六年八月十六日）

（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、環境省告示第一号）

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。なお、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）は、廃止する。

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

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。）の漏えいを防止するため、次の表の左欄に掲げる義務項目を必ず達成するものとし、当該義務項目の達成のため、同表の右欄に掲げる手段その他の義務項目を達成するために有効な手段を講ずるものとする。

義務項目	義務項目を達成するために適切と考えられる手段
第１　事業者は、自社の情報セキュリティ対応方針の策定及び周知を実施する。	１　事業者は、自社の守秘義務のルールを策定し、当該ルールを従業員（事業者との間で雇用関係等のある者をいう。以下同じ。）が遵守するよう、以下の事項を実施する。 （１）　自社の守秘義務のルールを文書化すること。 （２）　入社時又は社外要員の受入れ時に自社の守秘義務のルールを説明すること。 （３）　退職時又は雇用期間満了時に会社の機密情報を持ち出さないことを誓約させること。

	2　事業者は、業務で利用する情報機器の利用について、個人所有機器（ＢＹＯＤ）を含めたルールの策定及び周知をする。 3　事業者は、情報セキュリティに関する法令を考慮した社内ルールを策定し、教育及び周知をする。 4　事業者は、法令の改正、社会情勢の変化、契約上の要求事項や組織の状況の変化等に伴い、社内ルールを適宜見直す。
第２　事業者は、技術等情報のうちこの告示に掲げる措置の対象とする技術等情報（以下「管理対象情報」という。）を特定することとし、その特定に当たっては以下の事項を考慮する。 　また、事業者は、当該技術等情報が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。 （１）　当該管理対象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。 （２）　当該管理対象情報が改ざんされた場合に、自らの競争力に重大な影響を与えるか否か。 （３）　当該管理対象情報が使用できなくなった場合に、自らの競争力に重	1　事業者は、管理対象情報を一覧化し、当該管理対象情報の態様、管理に関する責任を有する者（以下「管理責任者」という。）の氏名、部署名、保管場所、保管期限、開示先、連絡先等を記録する。 2　事業者は、次の（１）から（３）までに掲げる管理対象情報の態様の区分に応じて、当該（１）から（３）までに定める措置を行う。 （１）　管理対象情報が電子情報（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。）の場合　ファイル名、文書ヘッダー、文書の透かし、フォルダ名、ファイル属性情報等に管理対象情報であることを記録する。 （２）　管理対象情報が試作品又は製造装置等の場合　当該試作品若しくは製造装置等又はそれらを保管する保管容器（以下「保管容器」という。）に管理対象情報であることを表示する。 （３）　管理対象情報が書類等の紙情報（管理対象情報が記載された紙をいう。以下同じ。）の場合　表紙等の適切な場所に管理対象情報であることを表示する。 3　事業者は、管理対象情報を、アクセス可能な者を限定した書庫、フォルダ等により管理する。

大な影響を与えるか否か。 （４）　当該管理対象情報が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、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。	
第３　事業者は、管理対象情報の機密区分を設定し、その機密区分に応じて情報を管理する。また、会社が保有する情報機器及び機器を構成するＯＳやソフトウェア（プログラムの集合体をいう。以下同じ。）といったＩＴ資産の情報（バージョン情報、管理責任者、管理部門、設置場所等）を適切に管理する。	１　事業者は、機密区分に応じた管理対象情報の管理ルールを策定する。 ２　事業者は、管理対象情報を機密区分及び重要度に応じた管理ルールに沿って管理する。 ３　事業者は、機密区分及び重要度に応じたＩＴ資産の管理ルールを策定する。 ４　事業者は、ＩＴ資産の情報（バージョン情報、管理責任者、管理部門、設置場所等）について、一覧を作成する。
第４　事業者は、平時から情報セキュリティリスクを管理する体制を整備し、事件及び事故発生に至らないよう、情報収集と共有を行う。体制整備の一環として、管理責任者を選任する。管理責任者はその業務の一部の実施を他の者に委任することができる。	１　事業者は、情報セキュリティを統括する役員（ＣＩＳＯ等）や情報セキュリティ担当部署を選任し、責任及び役割を明確化する。 ２　事業者は、社内での情報収集と共有のための連絡先リストを整備する。 ３　事業者は、定期的に又は必要に応じて、管理体制を見直す。 ４　事業者は、サイバー攻撃や情報漏えいの新たな手口を学習し、対策を社内部署へ共有し、サイバー攻撃や予兆を監視及び分析する体制を整備する。 ５　事業者は、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。 ６　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情報セキュリティ事件及び事故を位置付け、それら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。

	7　事業者は、情報セキュリティ事件及び事故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、継続的に見直す。 8　管理責任者は、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訓練を行う。 9　管理責任者は、保管容器又は立入制限区域（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、その区域の全ての入退室口を施錠することができるものをいう。以下同じ。）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。 10　管理責任者は、必要に応じて経営層へ情報セキュリティ事件及び事故による業務への影響及び対策を報告し、セキュリティ業務に関与している社内部署と共有する。 11　管理責任者は、その管理対象情報が複数の事業部門等にまたがっている場合には、社内ルール等への規定又は社内における掲示により、誰が管理責任者であり、どのような責任を有しているかを当該事業者の全ての従業員が認識できるようにする。 12　管理責任者は、方針、対策又はマニュアルが作成（変更を含む。）された場合におけるその承認や、管理対象情報の適切な管理に係る責任の明確化、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行う。
第５　事業者は、情報セキュリティ事件及び事故発生時の対応体制及び対応手順を整備し、その責任者を明確にする。	1　事業者は、情報セキュリティ事件及び事故に関連する証拠を特定、収集、取得及び保管する。 2　事業者は、情報セキュリティ事件及び事故発生時に、その概要、影響及び対応内容の記録を残す。 3　事業者は、定期的に又は必要に応じて、情報セキュリティ事件及び事故発生時の体制を見直す。 4　事業者は、マルウェア感染時の対応手順を定める。 5　事業者は、１から４までに掲げる事項を文書化した手順に沿って対応する。

第６　事業者は、従業員として注意すべきこと及び情報セキュリティの基礎に関する社内への教育を行う。	１　事業者は、電子メールのマルウェア感染に関する社内教育を行う。 ２　事業者は、インターネットへの接続に関する社内教育を行う。 ３　事業者は、機密区分に応じた管理対象情報の取扱いに関する社内教育を行う。 ４　事業者は、情報セキュリティ事件及び事故発生時の対応に関する社内教育を行う。 ５　事業者は、教育の内容を必要に応じて見直す。
第７　事業者は、自社内及び業務委託先の情報セキュリティリスクへの対策を実施する。	１　事業者は、管理対象情報において「機密性」、「完全性」、「可用性」の３要素が確保できなくなった場合の影響や被害を特定する。 ２　事業者は、１で特定した影響への対策を、策定された計画に沿って実施する。 ３　事業者は、情報セキュリティの脅威に関連する情報を収集及び分析する。 ４　事業者は、利用中の情報システム（ハードウェア、ソフトウェア、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。以下同じ。）の技術的脆弱性に関する情報を継続的に収集する。
第８　事業者は、自社の通信ネットワーク構成を把握し、関係団体（サプライヤーを含む。）との連携状態やデータの流れを監視する。	１　事業者は、自社の機器が接続している外部情報システム（関係団体の情報システム、クラウドサービス、外部情報サービス等をいう。以下同じ。）の利用ルールを策定する。 ２　事業者は、利用している外部情報システムを一覧化する。 ３　事業者は、外部情報システムの一覧を定期的に又は必要に応じて見直す。
第９　管理責任者は、取引先ごとに、取引で取り交わされる技術等情報及び取引に利用している手段を把握し、サプライチェーンにおける情報セキュリティ要件を明確化する。また、取引先から預けられた管理対象情報がある場合は、当該取引先からの意見を聴いて必要な措置を決定する。	１　管理責任者は、取引先との間で、技術等情報の取扱方法を明確化する。 ２　管理責任者は、情報セキュリティ事件及び事故発生時の取引先との役割と責任を明確化する。 ３　管理責任者は、取引先ごとに取り交わす情報及び手段（受発注の手段等、情報のやり取り）を一覧化する。 ４　管理責任者は、管理対象情報の漏えい防止に資する措置の実施状況を記録し、当該記録の保管期間を定め、定期的に確認する。 ５　管理責任者は、取引先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において、当該取引先からの意見に基づき適切な措置を講ずる。

	6　管理責任者は、取引先から預けられた管理対象情報の一覧を定期的に又は必要に応じて見直す。
第 10　管理責任者は、持出し、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し、保管する。	1　管理責任者は、管理簿について、保管期間を定めた上、施錠することができるロッカー等において保管し、又は暗号技術を用いて情報システムに記録する等適切に管理する。 2　管理責任者は、管理簿が適切に管理されていることを定期的に点検し、必要に応じて見直す。 3　管理責任者は、取引先から預けられた管理対象情報がある場合、当該管理対象情報の状況を管理するため、当該取引先ごとに管理簿を作成し、当該取引先に共有する。また、管理簿の保管期間を定める場合及び廃棄をする場合も当該取引先の確認を取る。
第 11　事業者は、管理対象情報の廃棄については、その管理対象情報の態様に応じ、復元不可能な方法により廃棄をする。	1　事業者は、書類等の紙情報又は試作品等である管理対象情報を廃棄する場合には、シュレッダーにより細断する等、復元できない状態にする。 2　事業者は、電子情報である管理対象情報を消去する場合には、上書き消去（データの完全消去）等、復元できない状態にする。 3　事業者は、電子情報である管理対象情報を記録した可搬式記録媒体を廃棄する場合には、データを消去した上で、当該可搬式記録媒体を物理的に破壊する等、復元できない状態にする。

Ⅱ　管理対象情報へのアクセス権の管理

事業者は、管理対象情報へのアクセス権を管理するため、次の表の左欄に掲げる義務項目を必ず達成するものとし、当該義務項目の達成のため、同表の右欄に掲げる手段その他の義務項目を達成するために有効な手段を講ずるものとする。

義務項目	義務項目を達成するために適切と考えられる手段

第１　事業者は、管理対象情報へのアクセス権の付与においては、権限の付与が見込まれる者についてのレビューをし、統一的な判断基準（考え方）の下で、以下の事項を考慮し行う。 （１）　Need to Know の原則（「情報は知る必要のある人のみに伝え、知る必要のない人には伝えない」という原則）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。 （２）　事業者内部における情報の取扱いに係る社内ルールへの違反履歴があるか否か。 （３）　権限の付与が見込まれる従業員の退職、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があるか否か。	１　事業者は、全ての管理対象情報へのアクセス権の設定を行っている管理責任者が一人の場合には、当該アクセス権の設定に係るレビューを当該管理責任者の上司等の他の者に行わせる。 ２　事業者は、管理責任者以外の者が管理対象情報へのアクセス権の設定を行っている場合には、当該管理責任者以外の者から管理責任者に対し、管理対象情報へのアクセス権を有する者（以下「アクセス権者」という。）の氏名等必要な事項を連絡させる。 ３　管理責任者は、アクセス権者以外の者による管理対象情報へのアクセスについて、Need to Know の原則を満たすものであるかを評価する。
第２　管理責任者は、アクセス権者の管理を行う。	１　管理責任者は、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　管理責任者は、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　管理責任者は、人事異動等に伴うアクセス権の管理ルールを策定する。 4　管理責任者は、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、社内教育の受講の状況等アクセス権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、一定期間保管する。 5　管理責任者は、３の管理ルールに沿ってアクセス権の発行、変更、無効化及び削除を実施する。 6　管理責任者は、アクセス権者の見直しを定期的に又は必要に応じて実施する。 7　管理責任者は、アクセス権者に対し、社内教育、周知及びその後の定期的な上司からの説明等により、アクセス権者としての責任を明確に認識させる。 8　管理責任者は、アクセス権者が定められた手順を守らない場合、アクセス権者のアクセス権を失効させる。
第３　事業者は、アクセス権者としての責任を明確にするため、アクセス権者との間で、以下の事項が記載された秘密保持に係る誓約書の取得又は秘密保持契約の締結等の措置を取る。 （１）　守秘義務を厳守すること。 （２）　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。 （３）　マニュアルその他の事業者内部	1　事業者は、誓約書等の記載事項の定期的な確認を実施する。 2　事業者は、情報の適切な管理に係る状況の変化が生じた場合又は情報セキュリティ事件及び事故が発生した場合は、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。 3　事業者は、アクセス権者を含めた従業員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、当該従業員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ルールに定める。 4　事業者は、アクセス権者を含めた従業員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に周知する。

における情報の取扱いに係る社内ルールを遵守すること。 （４）　管理対象情報の漏えいにつながり得る事象等を発見した場合に、管理責任者等事業者が指定した者に報告を行うとともに、情報セキュリティ事件及び事故が発生した場合に、Ｉの第５において定める対応手順に従って措置を講ずること。 （５）　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があること。 （６）　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、アクセス権を返却すること等所要の対応が求められること。	
第４　管理責任者は、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伝えること及び閲覧させることをいう。）及び複製の対象を管理する。	１　管理責任者は、管理対象情報の内容の伝達及び複製の対象者を原則として、アクセス権者に限る。 ２　アクセス権者は、他の従業員（管理対象情報の他のアクセス権者を除く。３において同じ。）に対して管理対象情報の内容の伝達又は複製をしようとする場合には、管理責任者の承認を得る。 ３　管理責任者は、アクセス権者から他の従業員に対する管理対象情報の内容の伝達又は複製についての承認を求められた場合には、真に必要なものか否かの確認を行い、

	伝達又は複製の範囲を可能な限り限定した上で、これを認める。 4　管理責任者は、管理対象情報の内容の伝達及び複製について、Ｉの第 10 の管理簿に記録する。 5　管理責任者は、電子情報である管理対象情報について、情報システムを構成する機器、可搬式記録媒体又はネットワークを介して接続するストレージサービスであって、事業者の管理に属さないものへの複製をするための手順を定める。 6　管理責任者は、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。

Ⅲ　管理対象情報が物である場合のアクセス制限等

事業者は、管理対象情報が物（書類等の紙情報、試作品又は製造装置等をいう。）である場合には、管理対象情報への物理的アクセスを制限するため、次の表の左欄に掲げる義務項目を必ず達成するものとし、当該義務項目の達成のため、同表の右欄に掲げる手段その他の義務項目を達成するために有効な手段を講ずるものとする。

義務項目	義務項目を達成するために適切と考えられる手段
第１　管理責任者は、保管容器及び立入制限区域の鍵、警備の体制を適切に管理する。また、事業者は、管理対象情報及び保管容器を、立入制限区域に設置するとともに、持ち出す場所についても制限する。	1　管理責任者は、保管容器及び立入制限区域の鍵の貸出し、共有を管理するための管理簿を作成し、一定期間保管する。 2　管理責任者は、施錠することができる保管容器を用いている場合にあっては、当該保管容器の解錠手段を、以下のような事象が生じた都度、変更する。 （１）　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 （２）　管理責任者又は管理責任者の委任を受けたアクセス権者が変わった場合 （３）　暗証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責任者又はアクセス権者が認めた場合

	3　管理責任者は、立入制限区域に係る入退室口を、業務時間中のみ開錠する。 4　管理責任者は、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）を記録し、事後的に確認可能とするため以下のような適切な措置を講ずる。 （1）　鍵の貸出しに係る管理簿の作成 （2）　受付の設置による受付簿の管理 （3）　ＩＤによる認証の導入 （4）　作業をしている者以外の者による同行と確認の実施 5　管理責任者は、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又は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を管理する。 6　管理責任者は、立入制限区域内に保管容器や製造設備等の管理対象情報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や製造設備等を物理的に持ち出せないようにする。 7　管理責任者は、管理対象情報を持ち出す際に、持出先となり得る場所について以下の事項等を事前に指定することとし、以下の事項をＩの第 10 の管理簿に記載する。 （1）　住所 （2）　建物・施設名 （3）　部屋番号 （4）　持出先の部屋の配置 （5）　保管場所
第２　管理責任者は、管理対象情報を保管容器から持ち出し、運搬すること等を、アクセス権者又は管理責任者が指定した者に限ることとし、当該持出し、運搬等に当	1　管理責任者は、管理対象情報の運搬の際に、外部から当該管理対象情報を視認できないようにする。 2　管理責任者が指定した者は、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、管理責任

たっての手順を定める。	者に提出する。 3　管理責任者は、管理対象情報の運搬を信頼できる輸送機関又は運搬事業者に行わせる。 4　管理責任者は、当該管理責任者の属する事業者以外の者（以下この４において「運送事業者」という。）に管理対象情報を運搬させる必要がある場合には、当該運送事業者の情報の管理について評価し、当該運送事業者と秘密保持契約を締結する。管理対象情報を当該運送事業者以外の者から当該運送事業者に運搬する場合も、同様とする。 5　管理責任者は、管理対象情報を持ち出す際に、持出しを行う持出人を最小限とし、その持出人をＩの第 10 の管理簿に記録する。 6　管理責任者は、管理対象情報を持ち出す際に、持出しを行う目的を可能な限り限定し、その目的をＩの第 10 の管理簿に記録する。
第３　事業者は、立入制限区域への不審者の侵入に係る視認性を高める。	1　事業者は、立入制限区域に赤外線警報装置、セキュリティカメラ等の警備システムを導入する。 2　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。 3　事業者は、立入禁止区域の周辺に立入りが禁止されていることを視覚的に認識できるようにする。 4　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分かる標識の着用を求めるものとする。

Ⅳ　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、管理対象情報へのアクセスを制限するため、次の表の左欄に掲げる義務項目を必

ず達成するものとし、当該義務項目の達成のため、同表の右欄に掲げる手段その他の義務項目を達成するために有効な手段を講ずるものとする。

義務項目	義務項目を達成するために適切と考えられる手段
第１　事業者は、管理対象情報へのアクセスをアクセス権者に制限する手順を定める。	１　事業者は、情報システムのセキュリティに配慮したログイン手順、電子メールで管理対象情報を送付する手順等の操作手順書を作成する。 ２　事業者は、業務で利用する情報システムを構成する機器（個人所有の物を含む。）の利用開始時、利用終了時の手続、利用中の遵守・禁止事項、紛失時の手続を含む利用手順を定める。
第２　事業者は、サーバ等の設置エリアには、物理的セキュリティ対策を行う。	１　事業者は、管理対象情報を取り扱う情報システム（以下「管理情報システム」という。）を構成する機器のうちサーバ等は立入制限区域に設置する。 ２　事業者は、サーバ等の設置エリアに入場可能な者を定める。 ３　事業者は、サーバ等の設置エリアを施錠等で入場を制限する。
第３　事業者は、自社が構築する管理情報システムを構成する機器の選定に当たって、信頼性を考慮した上で機器を選定する。	１　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。 ２　事業者は、管理対象情報をクラウド等自社以外の者のサーバ等で保存する場合には、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）する。 ３　事業者は、管理対象情報を自社以外のデータセンターに自らのサーバ等を設置して保存している場合、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）する。

	4　事業者は、サーバ等を設置する立入制限区域への管理情報システムの構成機器以外のサーバ等の持込みを禁止する。管理情報システムの構成機器を新設する場合には、内蔵ソフトウェアの状況を確認した上で、当該構成機器が従業員個人の所有物ではないものに限り認める。
第４　事業者は、自社が構築する管理情報システムを構成するネットワーク、システム及びアプリケーションについて不正アクセスを防止するために、必要な措置を講ずる。	1　事業者は、管理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。 2　事業者は、ＩＤＳ（Intrusion Detection System）等により、管理情報システムへの不正なアクセスを検知し、管理情報システムの維持に責任を有する者（以下「情報システム管理者」という。）に通知するシステムを導入する。 3　事業者は、ＩＰＳ（Intrusion Prevention System）等により、管理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。 4　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し、匿名でのネットワークへの接続（Anonymous 接続）を禁止する。 5　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。 6　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、情報システム管理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、導入を認めない。 7　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（定期的に又は情報セキュリティ事件及び事故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。 8　事業者は、管理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。 9　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ポート及びシリアルポートを物理的に閉塞することで、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。 10　事業者は、管理情報システム、情報機器及びソフトウェアへセキュリティパッチやアップデート適用を適切に行う。 11　事業者は、パソコン及びサーバに、マルウェア感染を検知及び通報するソフトウェア（ウイルス対策ソフト）を導入する。 12　事業者は、ウイルス対策ソフトのパターンファイルを常に最新化する。 13　事業者は、業務で利用する情報機器の自社ネットワークへの接続ルールを策定する。
第５　事業者は、情報システムを継続的に利用できるよう、必要な措置を講ずる。	１　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。 ２　事業者は、情報システムを置く施設を、設備の不具合による停電その他故障から保護するための取組を行う。 ３　事業者は、必要に応じて情報システムを復元する手順を整備する。 ４　事業者は、情報システムが停止した際も業務が遂行できる代替手段を用意する。 ５　事業者は、情報システムの運用に当たって、現在の及び予測される容量並びに能力の要求事項に合わせて、資源の利用を監視し、調整する。
第６　事業者は、情報システム管理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。	１　事業者は、情報システム管理者について、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。 ２　事業者は、１の作業ログについて、情報システム管理者の上司等が確認することにより、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、定期的に点検する。 ３　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。

	4　情報システム管理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に設定することにより、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行う。
第７　事業者は、管理情報システムを最新の状態に更新し、適切に機能を提供するための取組を実施する。	1　事業者は、管理情報システムを構成する機器について、更新されたウイ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、パッチの更新等を行う。 2　事業者は、管理情報システムに対する脆弱性診断を定期的に実施する。 3　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。 4　事業者は、管理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、利用されていない場合には、当該ソフトウェアを消去する。 5　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。
第８　事業者は、管理情報システムへのアクセスログを保管する。	1　事業者は、アクセスログをその記録のあった日から一定期間保管し、情報システム管理者により定期的に点検させる。 2　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イン又はログアウト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。 3　事業者は、法令や契約上の要求事項及びリスクを考慮し、監査ログの保管期間を決定した上で、２の監査ログを当該期間保管し、定期的に点検する。
第９　事業者は、管理対象情報を外部に送信することによる管理対象情報の流出を防	1　事業者は、管理対象情報を電子メール等によりネットワークを経由して外部に送信する場合は、送信する管理対象情報又は電子メールそのものを暗号化する。

止する。	2　事業者は、管理対象情報を電子メール等によりネットワークを経由して外部に送信する場合は、そのログを一定期間保管する。
第 10　事業者は、管理対象情報を記録した可搬式記録媒体を適切に管理し、管理対象情報の流出を防止する。	1　情報システム管理者は、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（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、一定期間保管する。 2　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保管し、その鍵等を適切に管理する。 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、暗号化する。 4　事業者は、個人所有機器（ＢＹＯＤ）で、管理対象情報を取り扱わせない。
第 11　事業者は、管理情報システムを構成する機器の持出しを制限する。	1　情報システム管理者は、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を作成し、一定期間保管する。 2　事業者は、保守及び点検の記録、持ち出した場合の持出しの記録、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を１の管理簿に記録する。 3　事業者は、情報システム管理者が、管理情報システムを構成する機器の持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。 4　事業者は、管理情報システムを構成する機器を譲渡する場合は、管理対象情報が復元できない状態であることを確認させる。
第 12　事業者は、管理情報システムの保守及び点検を第三者に行わせる場合、当該第	1　事業者は、第三者が管理情報システムの保守及び点検を行うときは、情報システム管理者の指示の下で、管理対象情報を他の記録媒体に移した上で、管理情報システム内の管理対象情報を復元できないように消去する。

三者が管理対象情報を漏えいさせないようにする。	2　事業者は、第三者が管理情報システムの保守及び点検を行うときは、事業者の従業員による立会い、作業ログの取得又はカメラの設置等により、保守及び点検業務を監視する。 3　事業者は、第三者による管理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ＩＤを無効化する。 4　事業者は、管理情報システムの保守及び点検を第三者に行わせるときは、当該第三者と秘密保持契約を締結する。 5　情報システム管理者は、第三者が管理情報システムの保守及び点検を行うときは、当該第三者の作業者を確認し、作業者の立入りを管理し、並びに立入制限区域内の保守及び点検の対象外の機器を撤去すること等により作業者の当該保守及び点検の対象となる機器以外への接触を防止する。 6　事業者は、クラウド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は、当該サーバ等を管理する事業者が１から５までに掲げる措置に相当する措置を講ずることを確認する。
第 13　事業者は、管理情報システムへのアクセスを通じた管理対象情報の流出を防止する。	1　事業者は、管理情報システムに保存した管理対象情報へアクセスする者を必要最低限に限る。 2　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、利用できる管理情報システムの機能を制限した上で、これを提供する。 3　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の登録を適切に管理し、人事異動等に伴いアクセス権者に変更が生じた際は速やかに登録内容を変更する。 4　事業者は、アクセス権設定等の特別な権限を持つ情報システム管理者の管理情報システムへのログインについて、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。 5　事業者は、テレワーク等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。 6　事業者は、テレワーク等外部からの管理対象情報へのアクセスについて、可能な限り暗号化された通信路を用いさせる。 7　事業者は、管理対象情報を電子政府推奨暗号を用いて暗号化する。
第14　事業者は、アクセス権を設定した管理対象情報を管理情報システムに保存する場合、当該管理対象情報へのアクセスを行う際のログインＩＤ及びパスワードを適切に管理する。	1　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。 2　事業者は、管理情報システムそのものに、漏えい、なりすましが疑われる事態になった際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つようにする。 3　事業者は、アクセス権者に対して、管理情報システムにログイ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。 4　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）を使用させない。 5　事業者は、ユーザーＩＤを個人ごとに割り当てる。 6　事業者は、ユーザーＩＤと情報システム管理者ＩＤの権限を分離する。 7　事業者は、パスワード設定に関するルールを策定し、周知する。 8　事業者は、ユーザーＩＤ及び情報システム管理者ＩＤを定期的に又は必要に応じて見直しを行い、不要なＩＤを削除する。

Ｖ　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、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ため、次の表の左欄に掲げる義務項目を必ず達成するものとし、当該義

務項目の達成のため、同表の右欄に掲げる手段その他の義務項目を達成するために有効な手段を講ずるものとする。

義務項目	義務項目を達成するために適切と考えられる手段
第１　事業者は、外部委託先等に管理対象情報を取り扱わせる前に、外部委託先等の情報管理の体制等を確認する。	１　事業者は、外部委託先等に管理対象情報を取り扱わせる取引を行う場合、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、当該取引が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、当該外部委託先等が、管理対象情報を適切に管理し、かつ、自ら当該管理対象情報の適切な管理の要請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。 ３　事業者は、管理対象情報を外部委託先等と共有する際に、情報セキュリティ事件及び事故発生時の、関係者ごとの役割と責任を明確化する。 ４　事業者は、外部委託先等のサービスも含めた外部情報システムの一覧を作成し、定期的に又は必要に応じて見直す。 ５　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分からないようにする。
第２　事業者は、管理対象情報を外部委託先等に提供する場合は、適切な管理を行うために以下の事項のうち必要な条項を含む秘密保持契約又はこれに準ずる法的拘束力のある取決めを締結する。 （１）　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。 （２）　外部委託先等は、提供された管理	１　事業者は、秘密保持契約又はこれに準ずる法的拘束力のある取決めのひな形を定める。 ２　事業者は、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外部委託先等に蓄積され、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、秘密保持契約又はこれに準ずる法的拘束力のある取決めに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し、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明記し、条件違反等契約に違反した場合に損害賠償

対象情報の取扱者の氏名等を明らかにすること。 （３）　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。 （４）　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。 （５）　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、一定期間保管すること。 （６）　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。 （７）　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	請求等の法的措置をとる旨の記載を行う。 ３　事業者は、管理対象情報に関連する物のメンテナンス等を外部委託先等に委託し、更に当該外部委託先等が当該メンテナンス等を第三者に再委託する場合には、事前に当該管理対象情報を提供する者の承認を得ることを条件とする。

速やかに廃棄又は返還等をすること。 （８）　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。 （９）　外部委託先等は、定期的に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。 (10)　外部委託先等の管理対象情報の管理責任者が管理簿を廃棄する場合は、事前に取締役等の経営層に確認すること。	