中小企業等の技術情報管理状況等調査

（経済産業省事業）

公募要領

平成３０年４月

株式会社　三菱総合研究所

「中小企業等の技術情報管理状況等調査」
公募要領

株式会社三菱総合研究所では、経済産業省からの受託事業「中小企業等の技術情報管理状況等調査」を実施します。その一環として、以下の要領で、上記事業における認証トライアルの実施者を公募します。

なお、経済産業省と当社との契約締結以前においては、採択予定者の決定となり、経済産業省と当社との契約締結等をもって採択者とすることとします。

１．事業の目的及び概要

自社の競争力の源泉となる技術等の情報を適切に管理することは、信頼できるパートナーとして認識されることにつながり、信頼できるパートナー間での技術等の情報の共有の円滑化がイノベーションの促進の観点等から重要となっています。

この観点から、他社における適切な技術等の情報の管理に係る認証スキームの構築等の環境整備を進め、産業界において広くデータ共有、オープンイノベーション等の他者との連携を深める動きを促していくためには、我が国の太宗を占める中小企業等における技術等の情報の管理を的確に進めていくことが不可欠です。

そのため、本事業は、信頼を醸成するための適切な認証の手法の検証や中小企業等において技術等の情報の適切な管理を進めていくための実効的なアドバイスの在り方の検討等を進め、中小企業等も含めた我が国産業界全体における技術等の情報の適切な管理を進めるための環境整備に係る資を得ることを目的として実施するものです。

本事業では、別紙１の手法により、別紙２の基準に照らした場合の中小企業等における情報の管理の状況についての確認・評価手法に係る調査（以下「認証トライアル」という。）を実施し、以下のⅰ）及び ⅱ）の内容についての提案を求めます。

ⅰ）認証トライアルを実施し、中小企業の評価結果、及び認証に係る実態や課題について報告を行うこと【事業者Ａ】

ⅱ）認証トライアルを実施し、中小企業の評価結果について報告を行うこと【事業者Ｂ】

① 認証トライアルの対象

中小企業及び中小企業における技術等の情報の管理の状況についての評価に当たって参考となる指標を得るための中堅企業（中小企業基本法（昭和３８年法律第１５４号）第２条第１項に掲げる中小企業以外の企業をいう。以下「中小企業等」と総称する。）を対象とすること。

なお、認証トライアルの対象となる中小企業等については、以下の要件を満たすこ

と。

イ 認証トライアルを受けた後に、技術等の情報の管理に係る確認・評価を受けた際の対応に当たっての留意事項、別紙２の基準を満たすために別紙２に記載されていない方法による対応を講じた事実その他の経済産業省及び当社が協議の上で決定する内容の報告を認証トライアルが完了した日から当社が別に定める日までに提出すること。

ロ 別紙２の基準を精読の上、実際に認証トライアルを受けるまでに、必要な対応を行うこと。

ハ 実際に認証トライアルを受けるまでの間に、別紙２の基準に沿って適切な管理を行う対象となる技術等の情報を特定し、事業者全体、事業所又は事業部門その他適切な範囲で認証トライアルを受ける範囲を設定すること。

２．事業実施期間

契約締結日～平成３０年９月３０日

（報告とりまとめについては、平成３０年８月中旬頃、経済産業省及び当社が指定する期日までに提出すること）

３．応募要件

次の要件を満たす企業・団体等とします。

（１）別紙１の手法により、別紙２の基準に照らした場合の中小企業等における情報の管理の状況についての確認・評価手法に係る調査を実施すること。

（２）認証トライアルの対象となる１．に示す条件を満たす中小企業等との間で、認証トライアルへの協力について了解が得られていること（または協力について了解が得られる見込みがあること）。また、その社名をリストとして提出できること。

（３）別紙１の手法の実効性、別紙１の手法に基づき講じた措置等（別紙１　１（１）の適切な措置、別紙１　４（２）⑦の期間及び当該期間での対応の困難性等）その他の当社と協議の上で決定する事項を含む報告を２．の期間中に当社に提出すること。

（４）認証トライアルの実施の期間内に、認証トライアルの対象となる中小企業等から得た情報を当該認証トライアルの目的以外には利用せず、当該中小企業等が特定される形式で経済産業省を除く第三者には開示しないことを確保する契約を当社と締結すること。

（５）本事業に関する委託契約を当社との間で直接締結でき、かつ、日本に拠点を有していること。

（６）委託契約の締結に当たっては、当社から提示する委託契約書に合意できること。

（７）本事業を的確に遂行する組織、人員、設備及び施設等を有していること。

（８）本事業を円滑に遂行するために必要な経営基盤を有し、かつ、資金、設備等について十分な管理能力を有すること。

（９）複数の者で共同提案するときは、事業全体の企画立案や運営管理等を行う能力や体制を有する統括者（統括機関）を定めること。

（１０）予算決算及び会計令第７０条及び第７１条の規定に該当しないものであること。
（１１）経済産業省所管補助金交付等の停止及び契約に係る指名停止等措置要領（平成１５・０１・２９会課第１号）別表第一及び第二の各号第一欄に掲げる措置要件のいずれにも該当しないこと。
（１２）契約形態を問わず、事業については、経済産業省と当社との協議を踏まえながら実施すること。

４．契約の要件
（１）契約形態：委託契約【事業者Ａ】、請負契約【事業者Ｂ】
（２）採択件数：１０件程度
（事業全体で、認証トライアルに協力する中小企業等５０社以上）
（３）予算規模：
中小企業等１社の認証トライアルにつき７０万円、事業全体では４，０００万円を上限とします。
なお、最終的な実施内容、契約金額については、当社と調整した上で決定することとします。
（４）成果物の納入：
事業報告書の電子媒体１部を当社に納入。
※ 電子媒体を納入する際、当社が指定するファイル形式に加え、透明テキストファイル付ＰＤＦファイルに変換した電子媒体も併せて納入。
（５）委託金の支払時期【事業者Ａのみ】：
委託金の支払いは、原則として、事業終了後の精算払となります。
※ 事業終了前の支払い（概算払い）はいたしませんので御注意ください。
（６）支払額の確定方法【事業者Ａのみ】：
事業終了後、事業者より提出いただく実績報告書に基づき原則として現地調査を行い、支払額を確定します。
支払額は、契約金額の範囲内であって実際に支出を要したと認められる費用の合計となります。このため、全ての支出には、その収支を明らかにした帳簿類及び領収書等の証拠書類が必要となります。また、支出額及び内容についても厳格に審査し、これを満たさない経費については、支払額の対象外となる可能性もあります。

５．提案書の様式
（１）提案書は、別紙資料１に基づいて作成してください。
（２）提案書は、日本語で作成してください。用紙サイズはＡ４版縦置き、横書きを基本とします。

６．提案書の提出部数

提案書の提出部数は、正（表紙に代表者印を捺印した提案書一式）１部とします。併せて、提案書のwordファイルを保存したCDも１枚提出してください。

また、提案書の提出時に「提案書受理票」１部に必要事項を記入の上、提案書とは別葉として提出してください。

７．提案書の添付書類

提案書には、次の資料又はこれに準ずるものを添付してください。

① 会社概要票（提案法人の紹介パンフレット等） １部

② 最近の事業報告書（１年分） １部
（資本金、従業員数、年商がわかるもの。記載ない場合は別紙でご提出ください）

③ 当社から提示された契約書（案）に合意することが委託先選定の要件となりますが、契約書（案）について疑義がある場合は、その内容を示す文書１部を添付してください。【事業者Ａのみ】

④ 取引先口座（銀行名、住所、口座種別、支店名、口座名義）が記載された文書１部

８．提出期限及び提出先

（１）提出期限：平成３０年５月１１日（金）１７：００必着

（２）提 出 先：株式会社三菱総合研究所
社会ICTイノベーション本部 サイバーセキュリティ戦略グループ
中小企業等の技術情報管理状況等調査（経済産業省事業）公募担当宛て
〒100-8141 東京都千代田区永田町二丁目１０番３号
電子メール：tech-info-koubo@ml.mri.co.jp
電話番号：03-6705-6047

（３）提出方法：持参または時間指定の宅配便等により提出してください。
※ＦＡＸ及び電子メールによる提出は受け付けません。
※郵送等する場合は、発送時に発送した旨を、上記の提出先までE-MAILにてご一報ください。
※平成３０年５月１日（火）、５月２日（水）はオフィス休業で持参を受け付けられませんのでご注意ください。

９．提案書の受理

（１）応募要件を満たさない者や不備がある提案書は、受理しない場合があります。

（２）提案書提出の際は、提案書様式の最後にある提案書受理票に必要事項を記入して、提案書とは別にして、合わせてご提出下さい。追って受理票をお返しします。

（３）受理した提案書は返却できませんので、予めご了承ください。

（４）提案書類に不備があり、提出期限までに整備できない場合は、当該提案書は無効となりますのでご了承ください。なお、この場合、提案書その他の書類は返却いたします。

１０．秘密の保持

（１）提案書、その他の書類は、当該事業委託先の選定のためにだけ使用します。

（２）提案書の個人情報、知的財産権に係る情報に考慮し、審査内容については公表しません。また、同様に審査内容等に関する照会には応じません。

１１．審査の方法

（１）委託先の選定は、受理した提案書及び添付資料等を基に、外部の有識者又は専門家の評価・意見等を踏まえ、委託先選定委員会において審査を行います。また、必要に応じて追加資料等の提出を求めることがあります。

（２）共同提案の場合は、共同提案者全体を一つの応募者として審査を行います。

（３）委託先を選考する際の基準は、以下のとおりです。

＜委託先選考基準＞

① 「３．」の応募要件を満たしているか。

＜提案内容＞

② 事業内容（認証の手法、中小企業の選定方法等）が優れているか。

③ 日程、手順等が効率的なものとなっているか。

④ 提案内容の予算配分が効率的なものとなっているか。

＜事業の実施体制＞

⑤ 委託事業を実施するために必要な組織、人員、設備及び施設等を有しているか。

＜事業の実施能力＞

⑥ 協力可能な中小企業を集めることができるか。

１２．審査結果の通知

提出期限後、約５営業日後を目途に提案内容の審査を行い、速やかに審査結果を通知します。なお、審査結果などの照会には応じません。

１３．経費の計上【事業者Ａのみ】

（１）経費の区分

本事業の対象とする経費は、事業の遂行に直接必要な経費及び事業成果の取りまとめに必要な経費であり、具体的には以下のとおりです。

経費項目	内容
Ⅰ．人件費	事業に直接従事する者の直接作業時間に対する人件費
Ⅱ．事業費	
旅費	事業従事者に対する事業を行うために必要な国内出張に係る経費
会場費	事業を行うために必要な会議等に要する経費 （会場借料、機材借料及び茶菓料（お茶代）等）
消耗品費	事業を行うために必要な物品であって、使用に伴い概ね１年程度で減耗するもの（ただし、当該事業のみで使用されることが確認できるもの。）の購入に要する経費
印刷製本費	事業成果報告書等の印刷製本に関する経費
補助職員人件費	事業を実施するために必要な補助職員（アルバイト等）に係る経費
その他諸経費	事業を行うために必要な経費のうち、当該事業のために使用されることが特定・確認できるものであって、他のいずれの区分にも属さないもの 例）通信運搬費（郵便料、運送代、通信・電話料等） 光熱水料（電気、水道、ガス。例えば、大規模な研究施設等について、専用のメータの検針により当該事業に使用した料金が算出できる場合） 設備の修繕・保守費 翻訳通訳 速記費用 文献購入費 法定検査 検定料 特許出願関連費用等
Ⅲ．一般管理費	委託事業を行うために必要な経費であって、当該事業に要した経費としての抽出、特定が困難なものについて、委託契約締結時の条件に基づいて一定割合の支払を認められた間接経費

（２）直接経費として計上できない経費

- 建物等施設に関する経費
- 事業内容に照らして当然備えているべき機器・備品等（机、椅子、書棚等の什器類、事務機器等）
- 事業実施中に発生した事故・災害の処理のための経費
- その他事業に関係ない経費

１４．契約について

採択された申請者について、当社と提案者との間で委託契約、又は請負契約を締結することになります。なお、採択決定後から委託契約締結までの間に、当社及び経済産業省との協議を経て、事業内容・構成、事業規模、金額などに変更が生じる可能性があります。（調整の結果、委託契約を希望されても請負契約、請負契約を希望されても委託契約になる可能性があります。）

契約書作成に当たっての条件の協議が整い次第、契約を締結し、その後、事業開始となりますので、あらかじめ御承知おきください。また、契約条件が合致しない場合には、契約の締結ができない場合もありますのでご了承ください。

なお、委託契約の場合、別紙資料３として提示した契約書（案）に基づき、受託業務の実施に際し、経済産業省又は経済産業省の指名する専門家等による各種助言・調整等に従うことをご了承ください。また、委託業務の事務処理は、経済産業省が提示する最新の委託事業事務処理マニュアル
（http://www.meti.go.jp/information_2/publicoffer/jimusyori_manual.html）及び当社の指示に基づき実施していただきます。

１５．その他の留意事項

（１）提案書を作成する上で前提となる条件等が不明な場合には、事項に従って質問を行うか、又は応募者の判断として想定した前提条件を明記の上記載してください。

（２）応募者等が所有する特許権等を使用する場合は、提案書の中にその旨を明記してください。また、使用条件等について提案等がありましたら、併せて提案書の中に明記してください。

（３）経費の計上は、委託契約締結日以降に発生（発注）したもので、事業期間中に終了（支払）したもののみが対象となります。例外はありませんので、発注など（航空券の発券など）を実施する際には十分ご注意ください。

１６．問い合わせ先

本件に関する問合せは日本語とし、下記の電子メール、ＦＡＸにて受け付けます。
また、電話、来訪等による問合せには対応いたしません。

社会 ICT イノベーション本部 サイバーセキュリティ戦略グループ 江連、磯江
E-mail：tech-info-koubo@ml.mri.co.jp
ＦＡＸ：０３－５１５７－２１９５

なお、問合せは、原則として平成３０年５月１１日（金）以降は受け付けません。

（別紙１）

中小企業等における情報の管理の状況についての確認・評価手法

中小企業等における技術等の情報の管理の状況についての確認・評価（以下「認証」という。）の手法は、以下のとおりとする。

ただし、次に掲げる場合については、その認証の手法によることとする。

・５．（６）について、認証トライアルを実施する者（以下「認証機関」という。）が委員会によるレビューではなく、認証機関の代表者によるレビューを望む場合

・認証機関から受託者への提案を受け、受託者と委託者と協議して個別の認証の手法を変更する場合

なお、認証トライアルの対象となる中小企業等（以下「依頼者」という。）の数の５割以上は、変更された認証の手法によらず、以下のとおりの認証の手法（以下「基本手法」という。）に従って認証トライアルを実施するものとする。

基本手法は、委託者と受託者との協議の上で、認証トライアルを実施する前までに変更することができるものとする（変更した場合には、変更後の手法を基本手法とする。）。

１．認証業務を実施する際の公平性の確保

（１）認証機関は、技術等の情報の管理の状況の確認に係る業務（４．の予備審査、文書審査又は現地審査をいい、以下「審査業務」という。）を実施する者（他者に再委託等する場合の外部の者を含む。以下「審査業務従事者」という。）その他認証トライアルに関係する業務を実施する者に、認証は公平に行うことが重要であること及び公平性へのリスクとして生じ得る事項等を認識させるために必要な措置を適切に講じること。

（２）認証機関は、その審査業務従事者に対して、審査業務の実施中において生じた公平性へのリスクを認証機関に報告することを確保すること。

（３）認証機関は、中小企業等における技術等の情報の管理の状況の確認を実施した結果として別添２の基準の全部又は一部に適合することを評価（以下単に「評価」という。）する際は、審査業務従事者が審査業務の実施過程で得た適合又は不適合に関する客観的な証拠に基づき、適切に判断を行うこと。

２．認証トライアルの範囲

（１）認証機関は、仕様書本体３．（２）①ハに則して認証トライアルの対象となる中小企業等（以下「依頼者」という。）が設定した認証トライアルの対象範囲を確認し、依頼者と協議の上で、事業者単位、事業所単位、事業部門単位その他の単位で適切に特定すること。

（２）（１）の特定に当たって、認証機関は、依頼者が設定する認証トライアルの対象範囲が、適切に評価する範囲とはならないと考えられる場合には、認依頼者との合意により、

仕様書本体３．（２）①ハで依頼者が設定した認証トライアルの対象範囲を適切に変更すること。
（３）認証機関は、（１）（２）の特定をするに当たっては、仕様書本体３．（２）①ハで特定した技術等の情報の態様（紙媒体、電子媒体、製造設備又は試作品等「物」であるか等）にも留意すること。

３．秘密保護、目的外利用の禁止
（１）認証機関は、認証トライアルの実施の過程において依頼者から提供された情報は、原則として全て秘密として取扱うこと。ただし、公知化されている情報、認証トライアルの実施過程若しくは実施後保存している期間中に公知化された情報又は秘密保持に関する契約において対象から除外されている情報はこの限りでない。
（２）認証機関は、依頼者から提供された情報について、３．（３）の契約で明記されている場合を除き、認証トライアル以外に用いてはならないようにすること。
（３）認証機関は、依頼者との間で、認証トライアルの実施の着手の前までに、３．（１）及び（２）の内容を含む契約を仕様書本体３．（２）③ハに則して締結すること。
（４）（３）の契約においては、依頼者から提供された情報を認証機関において保存する期間及び当該保存期間が終了した後に依頼者に返還すること又は修復不可能なように廃棄すること等の適切な措置をとることを明記すること。

４．審査業務のプロセス
（１）予備審査
①認証機関は、予備審査として、別添２の基準に適合しているか否かについて依頼者が自らチェックするチェックシートの送付等による予備審査を実施すること。
②認証機関は、予備審査について、チェックシートの送付とその回答を得る方法に限らず、依頼者との調整により、両者が合意した範囲で適切に実施すること。
③認証機関は、依頼者が個人情報保護法その他の法令（行政機関又は行政機関による委任を受けた者が公表しているガイドライン、通達等を含む。以下この③、（３）チ及び５（１１）において同じ。）により情報の適切な管理を求められている場合には、依頼者に照会し、その法令の名称の確認をすること。
④予備審査が終了した後で、認証機関は、審査計画書を作成し、依頼者に送付すること。
⑤④の審査計画書には、少なくとも審査工数、想定される審査日数、審査業務従事者となる予定の者（審査業務従事者は一人であると複数であるとを問わない。）を明記すること。
⑥認証機関は、審査計画書の審査工数等について、依頼者の理解を深めるために、文書の送付のみならず適切に説明を行うこと。

（２）文書審査
①審査業務従事者は、別添２の基準において定めることが求められる文書及び現地審査の前

に確認すべき事項に係る文書等について、当該文書の有無、記載内容等を確認すること。
②①の確認は、依頼者の事務所、事業所その他依頼者と認証機関が合意する場所で実施することを妨げない。
③認証機関は、文書審査の結果を、依頼者に通知すること。
④③の通知において、認証機関は、別添２の基準に適合していない部分がある場合には、その旨を指摘すること。
⑤認証機関は、④の内容を含む通知をした場合において、当該通知を受けた依頼者からの要請に応じ、どの部分が適合していないのかを説明し、理解を求めること。
⑥認証機関は、文書審査が終了した時は、依頼者に対して、現地審査における審査事項、現地審査に当たり依頼者において準備すべきことその他必要な事項を依頼者に対して説明をすること。
⑦認認証機関は、現地審査の内容について、依頼者の理解を求め、依頼者から現地審査の受入れ可能時期について、現地審査に着手する日の一定期間前には通知してもらうよう要請すること。
⑧認証機関は、文書審査の結果により、審査計画書に変更が生じる場合には、（１）④から⑥までの規定に従い審査計画書の変更を適切に行うこと。

（３）現地審査
①現地審査は、実際に依頼者が認証を受けようとする事業所その他２の認証トライアルの範囲の対象となる事業者の所在地等に審査業務従事者が実際に赴き、審査を行うものとすること。
②審査業務従事者は、現地審査において、主に以下の点についての審査を実施するものとし、審査報告書の作成等に当たって必要となる証拠等を適切に確認していくこと。
イ　別添２において物理的措置などハードウエアに関して明確な措置が求められている事項については、個別具体的に依頼者が実施している措置が別添２に適合しているか否かを確認すること。
ロ　教育訓練の状況や情報管理のプロセス等に関しては、依頼者の職員等のうち当該教育訓練を受け、又は情報管理のプロセス等を実践している者からの聞き取り等により、文書審査又は現地審査により確認した社内規程等が実践されているか否かを確認すること。
ハ　教育訓練の状況や情報管理のプロセス等に関しては、その実践が、将来にわたって継続することを書面その他の証拠により確認すること。
ニ　情報セキュリティについては、社内規程等が実際にシステムにどう反映されて運用されているかを模擬等によりテストをしてもらうこと等を通じて確認すること。
ホ　依頼者における情報管理の責任者からの別添２の基準に係る理解度、実践状況の認識及び将来計画等についての聞き取りを実施すること。
ヘ　ホの情報管理の責任者より上位の者が技術等の情報の漏えいが発生した場合の対応の

責任者の場合には、当該責任者からの実際の対応状況等についての聞き取りを実施すること。

ト　別添２の基準の表中の推奨措置について依頼者が実施している措置がある場合には、その措置の内容を確認すること。

チ　認証機関は、予備審査により、依頼者が個人情報保護法その他の法令により情報の適切な管理を求められていることを確認した場合には、当該法令により求められていることが遵守されているか否かを確認すること。

５．審査の検証のための審査報告書の作成と評価・交付

（１）現地審査終了後、審査業務従事者は、審査に当たって得た証拠を踏まえた審査報告書を作成すること。

（２）審査報告書には、少なくとも以下の事項を含むこと。

・氏名又は名称、住所その他依頼者の特定のために必要な事項
・認証の範囲
・審査業務従事者氏名
・審査業務を実施した日時及び場所
・審査各項目の適合状況及びその証拠
・審査業務の実施中に行われた課題解決に向けた指導助言の実績及びその内容

（３）審査報告書を基に評価する前に、認証機関は、依頼者における理解を得るため、最終的な結論の方向性その他必要な事項を当該依頼者に説明すること。

（４）（３）の説明に当たり、依頼者からの意見等がある場合には、その旨を審査報告書に付記すること。

（５）認証機関は、審査報告書を基礎として、評価をすること。

（６）（５）の評価に当たって、認証機関は、別添２の基準の全部に適合している旨の審査報告書を評価する場合には、（７）の委員会におけるレビューを行った上で最終的な判断を行うこと。

（７）委員会の構成は、認証機関内部の者及び外部の者から構成されるものとして、外部の者が半数を超えるように設置すること。

（８）認証機関は、（６）のレビュー後に、レビューを審査報告書に付した上で、当該審査報告書に係る依頼者に送付すること。

（９）依頼者に送付する審査報告書には、別添２の基準の全部に適合している旨を明確に示すこと。

（１０）（５）の評価に当たって、認証機関は、別添２の基準の一部に適合している旨の審査報告書を評価する場合には、（７）の委員会におけるレビューの代わりに認証機関の代表者によるレビューとすることができる。

（１１）依頼者が個人情報保護法その他の法令により情報の適切な管理を求められている場合において、その遵守状況に疑義がある場合には、認証機関は、速やかに、関係行政機関

に報告を行うとともに、評価を中止すること。

（別紙２）

技術等の情報の適切な管理のための基準

技術等の情報の適切な管理のための基準は、「製造産業における重要技術の情報の適切な管理に関する基準となる考え方の指針（ガイドライン）」の２から９までの規定によるものとする。

ただし、次の表の左欄に掲げる事項は、それぞれ右欄に掲げるものとして援用するものとする。

なお、委託者と受託者との協議の上で、この基準は、認証トライアルを実施する前までに変更することができるものとする（変更した場合には、変更後のものを別添２の基準とする。）。

製造産業における重要技術の情報の適切な管理に関する基準となる考え方の指針（ガイドライン）	技術等の情報の適切な管理のための基準
「を推奨」とされている事項	援用しない。 ただし、「推奨」とされる事項を実施している場合には、依頼者はその旨を伝え、認証機関は、そのことを確認する（別添１　４（３）②ト参照。）。
２．重要技術に係るリストの作成と重要技術の情報である旨の表示（マーキング）と管理 （１）重要技術に係るリストの作成	援用しない
（２）重要技術の情報の表示（マーキング）と管理 重要技術の情報として適切な管理の対象であることを明らかにするために、民間企業では、重要技術の情報を作成した時点で当該重要技術の情報そのものに重要技術の情報である旨の表示をするものとする（例えば、紙であれば紙媒体に記載し、電子情報であればファイル名に記録する。また、製造工程であれば、その製造工程を構成する製造設備が設置された時点で、建屋の入口への表示を行	（２）適切な管理を行う技術等情報の識別のための措置と管理 ３．（２）①ハで特定された技術等の情報（以下「技術等情報」という。）は、適切な管理の対象であることを明らかにするために、当該技術等情報そのものに適切な管理の対象となる技術等情報である旨の表示その他適切な管理の対象となる技術等情報であることを識別できる方法により識別できるように必要な措置を講ずるものとする。

う。）。 重要技術である旨の表示については、「部外秘」「社外秘」など民間企業の判断により様々な文言を用いることが考えられるが、重要技術の情報については、表示を見た者が、その情報が重要技術の情報であることを容易に識別できるよう、可能な限り統一的な表記を用いるものとする。 重要技術の情報を保有する民間企業においては、重要技術の情報の作成（評価・整理によるものを含む。以下「作成等」という。）、処理、保管（保存）、手交（送信）又は廃棄（削除）のプロセスを、このガイドラインに則して適切に管理をすることができるように手順を定めるものとする。	 表示としては、例えば、紙であれば紙媒体に適切な管理の対象であること（社外秘などの表示）を記載し、電子情報であればファイル名に記録し、又は適切な管理の対象となる技術等の情報が製造工程そのものであれば、その製造工程が置かれている建屋の入口等の見える場所への表示を行うことが考えられる。 また、その他適切な管理の対象となる技術等情報であると識別できる方法としては、例えば、台帳による管理、電子情報について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。 技術等情報については、作成、処理、保管（保存）、手交（送信）又は廃棄（削除）のプロセスを、この基準に則して管理をすることができるように手順を定めるものとする。
<u>３．重要技術の情報の管理の責任者</u> 重要技術の情報を保有する民間企業は、このガイドラインに則して重要技術の情報の管理を的確に進めていくための責任者として重要技術情報管理責任者を置くものとし、当該重要技術情報管理責任者には、部門の長等を任命するものとする 。 また、重要技術の情報を保有する民間企業では、全ての従業員等が、それぞれの重要技術の情報毎に、誰が管理の責任を有しているかを認識できるように、社	<u>３．技術等情報の管理の責任者</u> 技術等情報管理責任者として、部門の長等を任命するものとする。 また、技術等情報を保有する民間企業では、全ての従業員等が、それぞれの技術等情報ごとに、誰が管理の責任を有しているかを認識できるように、社内規程に定めること、社内における掲示するこ

内規程等に重要技術情報管理責任者である者の役職等を定めるものとする。 重要情報技術管理責任者については、以下のことを確実に行うための権限と責任を有することを社内規程等に定めることを推奨する。 ・重要技術の情報の作成等から廃棄まで適切に管理するための手順を確立させること ・従業員等に対するアクセス権の管理を行うとともに、アクセス権の設定を行った従業員等に係る管理名簿を作成、管理すること ・保管容器、立入制限区域の鍵、暗証番号の設定など重要技術の情報の管理に必要な措置を実施すること ・アクセス権の設定を行った者へのトレーニングを行うこと ・重要技術の情報の管理に関する脅威又は重要技術の情報の漏洩等の兆候の把握に努めるとともに、脅威、漏洩等があった場合の必要な措置を講じること ・上記の事項の実施に必要な手順・手続を定めること ・上記の実施状況を含む重要技術の情報の管理に関する状況について、定期的（少なくとも１年に１度以上）に、社内の情報保護に関する総括的な責任者（又は重要技術情報管理責任者の上司たる取締役等）に対して	とその他の方法に技術等情報管理責任者である者の役職等を定めるものとする。 技術等情報管理責任者は、以下のことを確実に行うことを職務とする。ただし、その一部の実施を他者に委任することを妨げない（委任した場合には、当該委任を受けた者について、委任した事項とともに、社内規程に定めること、社内における掲示をすることその他の方法により、全ての従業員等が認識できるように措置すること。） ・技術等情報の作成から廃棄までを管理するための手順を確立させること ・従業員等に対するアクセス権の管理を行うとともに、アクセス権の設定を行った従業員等に係る管理名簿を作成、管理すること ・保管容器や立入制限区域の鍵、暗証番号の設定など技術等情報の管理に必要な措置を実施すること ・アクセス権が設定された者へのトレーニングを行うこと ・技術等情報の管理に関する脅威又は技術等情報の漏えい等の兆候の把握に努めるとともに、脅威、漏えい等があった場合の必要な措置を講じること ・上記の事項の実施に必要な手順・手続を定めること ・技術等情報の管理に関する状況について、社内の情報保護に関する総括的な責任者（又は技術等情報管理責任者の上司たる取締役等）に対して報告を行うこと

報告を行うこと	
４．重要技術の情報への接近防御 （１）重要技術の情報への人的アクセスの制限 ①従業員等へのアクセス権の設定に当たっての考慮 重要技術の情報を保有する民間企業は、社内規程等により、当該重要技術の情報へのアクセスを認めた者に限り、当該重要技術の情報の取扱いを行い得ることを明らかにするものとする。 それぞれの民間企業において、当該民間企業において保有する重要技術の情報へのアクセスができる者の設定を行う際は、以下の点を考慮して設定するものとする（以下アクセス権を設定された者を「アクセス権者」という。）。 ⅰ）Need to Know原則 に照らし、グローバル競争が進む中での国外へ技術の流出リスクなどを考慮しつつ、必要最小限の範囲となっているか否か ⅱ）民間企業内における情報の取扱いの非違の履歴 また、民間企業において、アクセス権を設定する際は、従業員等の退職、研修員の派遣元への復帰など近い将来において重要技術の情報を保有する民間企業の直接の管理の対象から外れる可能性を確	４．技術等情報への接近防御 （１）技術等情報への人的アクセスの制限 ①従業員等へのアクセス権の設定に当たっての考慮 社内の文書により、当該技術等情報へのアクセスを認めた者に限り、当該技術等情報の取扱いを行い得ることを明らかにするものとする。 技術等情報へのアクセスができる者の設定を行う際は、以下の点を考慮して設定するものとする（以下アクセス権を設定された者を「アクセス権者」という。）。 ⅰ）Need to Know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。）との考え方）に照らし、グローバル競争が進む中での国外へ技術の流出リスクなどを考慮しつつ、必要最小限の範囲となっているか否か ⅱ）民間企業内における情報の取扱いの非違の履歴 アクセス権を設定する際は、従業員等の退職、研修員の派遣元への復帰など近い将来において技術等情報を保有する民

実に考慮するとともに、個人情報保護、個人識別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、飲酒トラブル、信用状態、犯罪記録等のレビューをすることを推奨する。	間企業の直接の管理の対象から外れる可能性を確実に考慮するとともに、個人情報保護、個人識別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、入手可能な情報（社内規程への違反履歴、法令の違反履歴、社内における飲酒トラブルの報告等）のレビューをすることとする。
②アクセス権の設定の権限 　民間企業における従業員等に対するアクセス権の設定は、重要技術情報管理責任者若しくは民間企業内の情報保護に関する総括責任者など当該民間企業における秘密情報の取扱いについての責任を有する者又はこれらの者による委任を受けた者が行うものとする。	②アクセス権の設定の権限 　アクセス権の設定は、技術等情報管理責任者若しくは情報保護に関する総括的な責任者など秘密情報の取扱いについての責任を有する者又はこれらの者による委任を受けた者が行うものとする。
アクセス権の設定は、重要技術の情報を保有する民間企業において統一的な判断基準（考え方）の下で行うこととし、全ての重要技術の情報へのアクセス権の設定を一人で行っている場合については、当該アクセス権の設定に係る監査を、当該アクセス権の設定の権限を有する者の上司等が行うものとする。	アクセス権の設定は、統一的な判断基準（考え方）の下で行うこととし、全ての技術等情報へのアクセス権の設定を一人で行っている場合については、当該アクセス権の設定に係る監査を、当該アクセス権の設定の権限を有する者の上司等が行うことを確保するための仕組みを設定することとする。
なお、重要技術情報管理責任者以外の者がアクセス権の設定を行っている場合には、当該重要技術情報管理責任者以外の者は、そのアクセス権を設定した重要技術の情報の重要技術情報管理責任者に、アクセス権の設定をした者の氏名等必要な事項を連絡するものとする。	なお、技術等情報管理責任者以外の者がアクセス権の設定を行っている場合には、当該技術等情報管理責任者以外の者は、そのアクセス権を設定した技術等情報の技術等情報管理責任者に、アクセス権の設定をした者の氏名等必要な事項を連絡するものとする。
③アクセス権の管理 　重要技術情報管理責任者は、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	③アクセス権の管理 　技術等情報管理責任者は、アクセス権

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）で見直すこととし、必要のなくなった従業員等のアクセス権の停止を適宜に行うなど、その適切な管理を行うものとする。 この管理を確実なものとするため、重要技術情報管理責任者は、アクセス権者の管理名簿（氏名、役職、アクセス権設定日時、アクセス権の範囲、４．（１）④に定める誓約書等の提出日、トレーニング受講歴がわかるもの。）を作成するものとする。ただし、既に、当該民間企業において、上記の管理名簿の記載事項を満たすリストを作成している場合には、当該リストをもって替えることができるものとする。 ④アクセス権者と民間企業との間の秘密保持等に関する担保 重要技術の情報を保有する民間企業は、４．（１）①のアクセス権の設定におけるプロセスを経て、従業員等にアクセス権を設定した際には、重要技術の情報の管理に係る従業員等としての責任を明確にするため、アクセス権者に対して秘密保持の誓約書の提出を求め、又は秘密保持契約を締結するものとする（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。）。 この誓約書等は、少なくとも以下の点の誓約・同意を求める内容を含めるものとする。 ・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重要技	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）で見直すこととし、必要のなくなった従業員等のアクセス権の停止を適宜に行うなどの管理を行うものとする。 この管理を確実なものとするため、技術等情報管理責任者は、アクセス権者の管理名簿を作成するものとする。当該名簿は、複数の情報の組合わせにより、氏名、役職、アクセス権設定日時、アクセス権の範囲が記載されている誓約書等の提出日、トレーニング受講歴が関連して識別できることをもって代えることができる。 ④アクセス権者における秘密保持等に関する担保 アクセス権者の従業員等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ものとする（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。）。なお、誓約書等において以下の事項が確保されていない場合には、他の適切な措置（例えば、トレーニングによる周知及び上司からの説明等の実施並びに認識の確認。）により確保するものとする。 ・アクセス権の設定の解除の後（退職

術の情報について、公知になったものを除き、不正に開示・使用しないこと ・第三者に対する守秘義務を厳守すること ・情報の漏洩につがなり得る事象等を発見した場合に適切に報告を行うとともに、情報の漏洩等の事故が発生した場合に適切な措置を講ずること ・重要技術の情報へのアクセスのログ等をアクセス権の設定の行った者等から確認されること	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技術等情報について、公知になったものを除き、不正に開示・使用しないこと ・第三者に対する守秘義務を厳守すること ・情報の漏えいにつがなり得る事象等を発見した場合に報告を行うとともに、情報の漏えい等の事故が発生した場合に措置を講ずること ・技術等情報へのアクセスのログ等をアクセス権の設定の行った者等から確認されること
⑤その他の場合のアクセス権の設定 重要技術の情報を保有する民間企業のアクセス権者以外の従業員等や外部関係者等における重要技術の情報へのアクセス、例えば、見学のように一時的な訪問者によるアクセスついては、当該訪問者につきneed to know原則を満たすことを重要技術の情報を保有する民間企業の重要技術情報管理責任者で評価し、当該訪問者から重要技術の情報を第三者等に開示しないことを誓約する書面を得て、アクセス権者の立会いなど重要技術の情報の保護に関する適切な措置を講じた上で認めるものとする。	⑤その他の場合のアクセス権の設定 技術等情報を保有する企業のアクセス権者以外の従業員等や外部関係者等における技術等情報へのアクセス、例えば、見学のように一時的な訪問者によるアクセスついては、当該訪問者につきneed to know原則を満たすことを技術等情報管理責任者で評価し、当該訪問者から技術等情報を第三者等に開示しないことを誓約する書面を得て、アクセス権者の立会いなど技術等情報の保護に関する措置を講じた上で認めるものとする。
（２）重要技術の情報への物理的アクセスの制限 ①保管容器（金庫） 重要技術の情報を保管する保管容器については、三段式文字盤鍵のかかる金庫若しくは鋼鉄製の箱又はこれらに準じる強度を有するもの とし、原則として、当該保管容器は、立入制限区域内に置くものとする。	（２）技術等情報への物理的アクセスの制限 ①保管容器（金庫） 技術等情報のうち書類や小さい試作品、技術等情報が記録された媒体その他保管容器に保管することができるものの保管容器については、三段式文字盤鍵のかかる金庫若しくは鋼鉄製の箱又はこれらに準じる強度を有するもの（これらに

	準じる強度を有するか否かは、技術等情報管理責任者が判断する。）とする。
三段式文字盤鍵の鍵番号は、重要技術情報管理責任者又はその委任を受けた者（アクセス権者に限る。以下この４.（２）①②において同じ。）が設定することとし、その鍵番号については、少なくとも１年に１度変更することを推奨する。	三段式文字盤鍵の鍵番号は、技術等情報管理責任者又はその委任を受けた者（アクセス権者に限る。以下この４（２）①②において同じ。）が設定することとする。
なお、鍵番号の共有は、アクセス権者に限るものとし、鍵番号を記したメモ等について、他の者の目につく場所には置かないことをアクセス権者に徹底するものとする 。	なお、鍵番号の共有は、アクセス権者に限るものとし、鍵番号を記したメモ等について、他の者の目につく場所には置かないことをアクセス権者に周知するものとし、物理的な鍵を用いる場合には、立入制限区域の施錠に係る鍵の取扱いに準じて管理を行うものとする。
また、保管容器のある場所が立入制限区域の外の場合については、視認性を確保するため、セキュリティカメラの設置等を推奨する。	保管容器のある場所が立入制限区域の外の場合については、セキュリティカメラの設置若しくは人感センサーの設置又は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ンス権者が視認できるような視界の確保のためのレイアウト等）を採るものとする。
特に守秘性の高い重要技術の情報の保管容器からの持出しについては、重要技術情報管理責任者が事後的に追跡可能なように、持出しに係る事実関係（持ち出した者、持出し日時、返却日時等）の記録を作成するものとする。	技術等情報の保管容器からの持出しについては、技術等情報管理責任者が事後的に追跡可能なように、持出しに係る事実関係（持ち出した者、持出し日時、返却日時等）の記録を作成するものとする。
②立入制限区域 保管容器における保管が困難な場合等として、以下ⅰ、ⅱに該当する場合は、原則として、アクセス権者のみの立入り	②立入制限区域 保管容器における保管が困難な場合等として、以下ⅰ、ⅱに該当する場合は、

が認められる区域（立入制限区域）において、当該重要技術の情報を保管し、又は取り扱うものとする。 ⅰ）重要技術の情報の化体したものの態様、サイズ等から保管容器での保管が困難な場合 ⅱ）ものの態様、サイズは保管容器で保管可能であるが、業務上、保管容器から出して使うことが必要な場合	原則として、アクセス権者のみの立入りが認められる区域（立入制限区域）において、当該技術等情報を保管し、又は取り扱うものとする。 ⅰ）技術等情報の化体したものの態様、サイズ等から保管容器での保管が困難な場合 ⅱ）ものの態様、サイズは保管容器で保管可能であるが、業務上、保管容器から出して使うことが常時必要な場合 ただし、技術等情報が電子情報である場合等において、当該技術等情報を一次的に取り扱うときは、技術等情報管理責任者の承認を得て、当該一次的に取り扱う場所として立入制限区域によらないことができる。
立入制限区域への立入りについては、重要技術情報管理責任者による確認が事後的に可能なように、立入制限区域への全ての立入者に係る事実関係（氏名、日時、入退室時間等）の記録を作成するものとする。	立入制限区域への立入りについては、技術等情報管理責任者による確認が事後的に可能なように、立入制限区域への全ての立入者に係る事実関係（氏名、日時、入退室時間等）の記録を作成するものとする。
立入制限区域は、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として、その区域の外と接触する全ての入退室口を施錠可能とした上で、原則として業務時間のみ解錠するものとする。	立入制限区域は、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として、その区域の外と接触する全ての入退室口を施錠可能とした上で、原則として業務時間のみ解錠するものとする。
立入制限区域への入退室口の施錠の方法は、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）など民間	立入制限区域への入退室口の施錠の方法は、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）など適切

企業で適切と判断する方法を用いるものとする。 　この方法については、重要技術情報管理責任者が立入制限区域へのアクセスそのものを管理でき、かつ、立入制限区域へのアクセスについての事実関係を、立入制限区域の入室管理の記録簿と照合することで確認することが可能なような方法を用いるものとして、例えば、鍵を用いる場合には、鍵の管理は、重要技術情報管理責任者又はその委任を受けた者が行うこととし、鍵の貸出しは、重要技術情報管理責任者又はその委任を受けた者の承認を得た上で、鍵の貸出日時、返却日時を記録することなどの措置をとるものとする。 　また、鍵の管理に当たっては、当該鍵に対応する立入制限区域を含む構内（例えば工場敷地内）から持ち出さないことを徹底する 。 　災害等緊急時対応のため、マスターキーの製作等が必要な場合には、そのマスターキー等の管理は、重要技術情報管理責任者自らの管理とすることを推奨する。 　加えて、立入禁止区域の窓は施錠可能なものとし、業務時間外は施錠するとともに、外部からの侵入を防止できる処置をとることを推奨する。 　なお、立入制限区域には、セキュリテ	の方法を用いるものとする。 　この方法については、技術等情報管理責任者が立入制限区域へのアクセスそのものを管理でき、かつ、立入制限区域へのアクセスについての事実関係を、立入制限区域の入室管理の記録簿と照合することで確認することが可能なような方法を用いるものとして、例えば、鍵を用いる場合には、鍵の管理は、技術等情報管理責任者又はその委任を受けた者が行うこととし、鍵の貸出しは、技術等情報管理責任者又はその委任を受けた者の承認を得た上で、鍵の貸出日時、返却日時を記録することなどの適切な措置をとるものとする。 　鍵の管理に当たっては、当該鍵に対応する立入制限区域を含む構内（例えば工場敷地内）から持ち出さないことを徹底する（キーパッド式の鍵の暗証番号等については、保管容器の鍵番号に準じて取り扱うものとする。）。 　災害等緊急時対応のため、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や共通パスワードの設定等が必要な場合には、そのマスターキー等の管理は、技術等情報管理責任者が定める方法により適切に管理とするものとする。 　立入禁止区域の窓は施錠可能なものとし、業務時間外は施錠するとともに、外部からの侵入を防止できる処置をとることとする。 　立入制限区域には、セキュリティカメラの設置、警報装置など警備システムの導入、警備員の配置等により不審者等の

ィカメラの設置、警報装置など警備システムの導入、警備員の配置等により視認性を高める装置の導入等を推奨する。	侵入に係る視認性を高める装置の導入を行うこととする。
③立入制限区域へのアクセス制限の実効性を高めるための対応 立入制限区域については、２．（２）のとおり、その区域が立入制限区域であることを示す表示として、民間企業の判断により「立入禁止区域」や「アクセス権者以外立入禁止」などの表示を行うものとする。なお、この表示の表記については、重要技術の情報に係る立入制限区域につき、統一的な表記を行うものとする。	③立入制限区域へのアクセス制限の実効性を高めるための対応 立入制限区域については、その区域が立入制限区域であることを従業員等が識別するための適切な措置をとるものとする。
立入制限区域への全ての立入者については、他の者から視認できる形で、当該立入禁止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。	立入制限区域への全ての立入者については、他の者から視認できる形で、当該立入禁止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。
また、立入制限区域内には、カメラ、通信機器等携帯型情報通信・記録機器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、重要技術情報管理責任者の承認を得るものとする。 立入制限区域内における情報通信・記録機器の利用については、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ものとする。	立入制限区域内には、カメラ、通信機器等携帯型情報通信・記録機器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、技術等情報管理責任者の承認を得るものとする。 立入制限区域内における情報通信・記録機器の利用については、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ものとする。
立入制限区域内にパソコン等を設置す	立入制限区域内にパソコン等を設置する場合には、当該パソコン等を物理的に持ち出せないようにワイヤ等で固定する。

る場合には、当該パソコン等を物理的に持ち出せないようにワイヤ等で固定するとともに、社内の一般システムや外部との接続のないスタンドアローンのものとすることを推奨する。	
５．重要技術の情報の作成等、運搬、複製運搬、廃棄の取扱い （１）作成等 紙媒体、電子媒体等で重要技術の情報を作成し、又はある技術が重要技術であると評価された時において当該重要技術の情報がある場合には、当該重要技術の情報には、重要技術情報管理責任者が定める手順に従って、速やかに重要技術の情報である旨の表示（マーキング）を行うものとする。 （２）運搬 ①重要技術の情報の保管容器との立入制限区域との間の運搬 重要技術の情報について、立入制限区域の外に置かれている保管容器から立入制限区域で取り扱うために行う運搬は、アクセス権者又は重要技術情報管理責任者が重要技術の情報の運搬をすることを承認した者により行わせるものとする。 重要技術情報管理責任者により重要技術の情報の運搬の承認をされた者が、当該重要技術の情報のアクセス権者ではない場合には、外部から運搬する内容が視認できず、かつ、運搬中に不正があった場合に確認ができるよう重要技術の情報を封筒に入れる等の措置を、当該重要技術の情報のアクセス権者において講じるとともに、当該承認をされた者は、その重要技術の情報の受渡し時に、受領者に	５　技術等情報の作成等の段階における識別のための措置、運搬、複製、廃棄の取扱い （１）作成等の段階における識別のための措置 技術等情報管理責任者は、技術等情報について、２（２）の識別をするための措置を速やかに講じるための手順を定め、当該手順に従って、速やかに技術等情報であることを識別するための措置を講ずること。 （２）運搬 ①技術等情報の保管容器又は立入制限区域から事業所等構内の別の場所への運搬 技術等情報について、保管容器又は立入制限区域から、構内の別の場所において取り扱うために行う運搬は、アクセス権者又は技術等情報管理責任者が技術等情報の運搬をすることを承認した者により行わせるものとする。 技術等情報管理責任者により技術等情報の運搬の承認をされた者が、当該技術等情報のアクセス権者ではない場合には、外部から運搬する内容が視認できず、かつ、運搬中に不正があった場合に確認ができるよう技術等情報を封筒に入れる等の措置を、当該技術等情報のアクセス権者において講じるとともに、当該承認をされた者は、その技術等情報の受渡し時に、受領者によるサイン、日時の

よるサイン、日時の記載がされた受領証を受け取り、重要技術情報管理責任者に提出するものとする。 　また、送付側と受取側は、アクセス権者以外に重要技術の情報を運搬させた場合は、相互に、内容、個数等の運搬した内容のチェックを行うものとする。 ②重要技術の情報の構外等への運搬 　重要技術の情報を、当該重要技術が現にある立入制限区域の以外の場所や構外に運搬する必要がある場合は、重要技術管理責任者は、当該運搬する先の者（場所）について、以下の点を確認するものとする。 ・当該運搬の先が社外の者である場合には、このガイドラインの６．に則して評価等がなされ、秘密保持契約の締結がされた後の者であるか否か ・当該運搬の先が、同一構内、同一社内の他事業所などの民間企業の内部である場合には、当該他事業所で当該重要技術の情報を取り扱わせる必要性、当該他事業所における重要技術の情報の取扱いに関して重要技術の情報の管理を適切に行うための措置が講じられているか否か 　重要技術の情報の構外への運搬に関しては、構内での運搬の方法に準じ、又は信頼できる輸送機関若しくは運搬事業者により行うものとする。 　また、重要技術の情報の構外への運搬における運搬の先の受領者がこのガイドラインの６．に定める外部委託先等である場合には、その外部委託先等との秘密	記載がされた受領証を受け取り、技術等情報管理責任者に提出するものとする。 　送付側と受取側は、アクセス権者以外に技術等情報を運搬させた場合は、相互に、内容、個数等の運搬した内容のチェックを行うものとする。 ②技術等情報の構外等への運搬 　技術等情報を、当該技術等情報が現にある事業所の構外に運搬する必要がある場合は、技術等情報管理責任者は、当該運搬する先の者（場所）について、以下の点を確認するものとする。 ・６に則して評価等がなされ、秘密保持契約の締結がされた後の者であるか否か ・当該運搬の先が、同一社内の他事業所などの内部である場合には、当該他事業所で当該技術等情報を取り扱わせる必要性、当該他事業所における技術等情報の取扱いに関して技術等情報の管理を行うための措置が適切に講じられているか否か 　技術等情報の構外への運搬に関しては、構内での運搬の方法に準じ、又は信頼できる輸送機関若しくは運搬事業者により行うものとする。 　技術等情報の構外への運搬における運搬の先の受領者が６に定める外部委託先等である場合には、その外部委託先等との秘密保持契約において限定された技術等情報の取扱いを行う者による受領の日時、サインを得ることとし、同一社内で

保持契約において限定された重要技術の情報の取扱いを行う者による受領の日時、サインを得ることとし、同一社内である場合には、当該重要技術の情報のアクセス権者である受領者による受領の日時、サインを得るものとする。	ある場合には、当該技術等情報のアクセス権者である受領者による受領の日時、サインを得るものとする。
（３）重要技術の情報の複製 　重要技術の情報の複製（重要技術の情報が保存されたサーバーからアクセス権者の個人のパソコンへのダウンロードやプリントアウトを含む。）は、重要技術情報管理責任者の承認を得て、アクセス権者のみが行うことができるものとし、複製された情報は、その元となる重要技術の情報と同じ取扱いを行うものとする。 　重要技術情報管理責任者は、アクセス権者からの重要技術の情報の複製の承認の求めがあった場合には、当該複製が真に必要なものか否かの確認を行い、可能な限り限定された範囲での複製を認めるものとする。	（３）技術等情報の複製 　技術等情報の複製は、事前に技術等情報管理責任者の承認を得て、アクセス権者のみが行うことができるものとし、複製された情報は、その元となる技術等情報と同じ取扱いを行うものとする。 　技術等情報管理責任者は、アクセス権者からの技術等情報の複製の承認の求めがあった場合には、当該複製が真に必要なものか否かの確認を行い、可能な限り限定された範囲での複製を認めるものとする。
（４）重要技術の情報の廃棄 　重要技術の情報の廃棄については、紙媒体の場合にはシュレッダー（クロスカット方式のシュレッダーを推奨する。）による裁断をすることとし、他の物件については、重要技術の情報を探知することができないよう焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により廃棄するものとする。	（４）技術等情報の廃棄 　技術等情報の廃棄については、紙媒体の場合にはシュレッダーによる裁断をすることとし、他の物件については、技術等情報を探知することができないよう焼却、粉砕、細断、溶解、破壊等の復元不可能な方法により廃棄するものとする。
６．重要技術の情報に係る外部委託先等のマネジメント （１）外部委託先等に重要技術の情報を取り扱わせる前の確認	６．技術等情報に係る外部委託先等のマネジメント （１）外部委託先等に技術等情報を取り扱わせる前の確認

重要技術の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ものとする。 重要技術の情報の取扱いを外部委託先等に行わせる場合については、当該外部委託先等が、重要技術の情報を適切に管理し、かつ、自社からの情報管理の要請に適切に対応できる能力を有するか否かを事前に調査・確認するものとする。その際、例えば、自社で講じている秘密の保護に係る取組と同等以上の取組が相手方において行われているか否かを調査・確認するものとし、当該調査・確認の評価の社内手続を定めることを推奨する。 特に、外部委託先等が海外企業である場合には、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洩リスクが高まる可能性も考えられるため、より確実に事前の調査・確認を行うものとする。	技術等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ものとする。 技術等情報の取扱いを外部委託先等に行わせる場合については、当該外部委託先等が、技術等情報を管理し、かつ、自社からの情報管理の要請に対応できる能力を有するか否かを事前に調査・確認するものとする。 その際、例えば、自社で講じている秘密の保護に係る取組と同等以上の取組が相手方において行われているか否かを調査・確認するものとし、当該調査・確認の評価の社内手続を定めることとする。 外部委託先等が海外企業である場合には、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、より確実に事前の調査・確認を行うものとする。
（２）秘密保持契約の締結 重要技術の情報を外部委託先等において取り扱わせる場合には、当該外部委託先等と必ず秘密保持契約を締結するものとし、その秘密保持契約には、第三者開示の禁止など基本的事項に加えて、以下の事項を含むものとする。 ・外部委託先等における重要技術の情報の取扱者を限定するとともに、当該取扱者の氏名等を明らかにするこ	（２）秘密保持契約の締結 技術等情報を外部委託先等において取り扱わせる場合には、当該外部委託先等と必ず秘密保持契約を締結するものとし、その秘密保持契約には、第三者開示の禁止など基本的事項に加えて、以下の事項を含むものとする。ただし、秘密保持契約の内容として規定されていない場合には、技術等情報管理責任者が認める別の措置により実質的に担保することをもって足りるものとする。 ・外部委託先等における技術等情報の

と（Need to Know原則に照らして必要最小限の範囲であることを、重要技術の情報を保有し、外部委託先等に提供する者（以下この６．（２）（３）において「委託元」という。）において確認する。） ・限定された重要技術の情報の取扱者による重要技術の情報へのアクセス記録を外部委託先等において記録・管理すること ・委託元から提供された重要技術の情報の複製、廃棄などが行われた場合の記録簿の作成、適時の報告を委託元に対して行うこと ・契約満了時又は契約解除時において、提供した重要技術の情報を廃棄（又は委託元へ返還）すること。廃棄する場合は、委託元への廃棄の手法と廃棄の結果の報告を求めること ・重要技術の情報の管理状況について、外部委託先等から委託元に対して定期的に報告をすること、定期的又は不定期の委託元からの重要技術の情報の管理に係る監査を外部委託先等において受け入れること ・実際の重要技術の情報の受渡しについては、両当事者で定めた表示を明示的に付して行うとともに、受渡しをした重要技術の情報のリストを作成し、両当事者協力の下で最新のものに更新を行うこと	取扱者を限定するとともに、当該取扱者の氏名等を明らかにすること（Need to Know原則に照らして必要最小限の範囲であることを、技術等情報を保有し、外部委託先等に提供する者（以下この６．（２）（３）において「委託元」という。）において確認する。） ・限定された技術等情報の取扱者による技術等情報へのアクセス記録を外部委託先等において記録・管理すること ・委託元から提供された技術等情報の複製、廃棄などが行われた場合の記録簿の作成、適時の報告を委託元に対して行うこと ・契約満了時又は契約解除時において、提供した技術等情報を廃棄（又は委託元へ返還）すること。廃棄する場合は、委託元への廃棄の手法と廃棄の結果の報告を求めること ・技術等情報の管理状況について、外部委託先等から委託元に対して定期的に報告をすること、定期的又は不定期の委託元からの技術等情報の管理に係る監査を外部委託先等において受け入れること ・実際の技術等情報の受渡しについては、両当事者で定めた表示を明示的に付して行うとともに、受渡しをした技術等情報のリストを作成し、両当事者で最新のものに更新を行うこと
７．重要技術の情報の管理を確実に実行	７．技術等情報の管理を確実に実行してい

していくためのトレーニング 秘密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、重要技術の情報を保有する民間企業は、従業員等（アクセス権者のみならずその他の従業員等を含む。）への秘密の管理に関する意識の涵養を図るためのトレーニングを受講させるとともに、特に、アクセス権者については、重要技術の情報を的確に取り扱わせるための手順についてのトレーニングを受講させるものとする（トレーニングは会議、講義、e-learning等いずれの実施形態であるかを問わない。）。 また、従業員等における秘密の管理に係る意識の涵養を一層図るため、全ての従業員等について、トレーニングに加えて、秘密情報保護に係るセルフチェックを定期的に行うようにするとともに、重要技術の情報を保有する複数の部署が存在する場合には、当該部署間での相互チェックを行うことを推奨する。 （１）全ての従業員等に対するトレーニング 重要技術の情報を保有する民間企業は、全ての従業員等に対して、定期的（一年に１回以上を推奨する。）に、秘密保全に関するトレーニングを受けさせる機会を設けるものとし、トレーニングの内容については、最低限、以下の事項を含めるものとする。 ・秘密の情報の管理の重要性、企業における秘密情報の分類と取扱い ・秘密の情報の漏洩とその結果の事例 ・関係法令の内容	くためのトレーニング 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、従業員等（アクセス権者のみならずその他の従業員等を含む。）への技術等情報の適切な管理に関する意識の涵養を図るためのトレーニングを受講させるとともに、特に、アクセス権者については、技術等情報を的確に取り扱わせるための手順についてのトレーニングを受講させること（トレーニングは会議、講義、e-learning等いずれの実施形態であるかを問わない。）。 また、従業員等における秘密の管理に係る意識の涵養を一層図るため、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セルフチェックを定期的に行うようにする。 （１）全ての従業員等に対するトレーニング 定期的に、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トレーニングを受けさせる機会を設けるものとし、トレーニングの内容については、最低限、以下の事項を含めるものとする。 ・技術等情報の適切な管理の重要性 ・技術等情報の漏えいとその結果の事例

・秘密の情報の漏洩等の兆候・端緒があった場合の報告手続 ・標的型メールなどの警戒すべき手口 ・秘密の情報の管理に係るセルフチェックの実施とその方法 （２）アクセス権者に対するトレーニング 　アクセス権者に対するトレーニングの内容は、７．（１）の全ての従業員等向けのトレーニングの内容に加えて、具体的な重要技術の情報の取扱手続、情報の漏洩等の兆候・端緒のケーススタディを含むものとする。	・関係法令の内容 ・技術等情報の漏えい等の兆候・端緒があった場合の報告手続 ・標的型メールなどの警戒すべき手口 ・技術等情報の適切な管理に関するセルフチェックの実施の意識付けとその方法 （２）アクセス権者に対するトレーニング 　アクセス権者に対して、技術等情報管理責任者又は技術等情報管理責任者が指定する者により、具体的な技術等情報の取扱手続、情報の漏えい等の兆候・端緒のケーススタディに関するトレーニングを、少なくとも１年に１度受講させる機会を設けること。
８．重要技術の情報に係る漏えいの兆候把握、事故発生時の報告等の対応 （１）全ての従業員等が報告すべき事象 　重要技術の情報を保有する民間企業は、全て従業員等に対して、少なくとも、以下の①②のような事象を発見した場合には、重要技術情報管理責任者又は当該重要技術の情報を保有する民間企業の情報の保護に関する総括的な責任者に報告を行わせるものとする。 　重要技術の情報の漏洩等に係る報告が、情報の保護に関する総括的な責任者に行われた場合には、当該責任者は、重要技術情報管理責任者に当該報告を共有するものとする。 ①　兆候等 ・秘密の情報を保管しているサーバーや記録媒体へのアクセス回数の大幅な増加や業務上必要のないアクセス	８．技術等情報に係る漏えいの兆候把握、事故発生時の報告等の対応 （１）全ての従業員等が報告すべき事象 　全て従業員等に対して、少なくとも、例えば、以下の①②のような技術等情報の漏えいに関連するおそれがある事象を発見した場合には、技術等情報管理責任者又は情報の保護に関する総括的な責任者に報告を行わせるものとする。 　技術等情報の漏えい等に係る報告が、情報の保護に関する他の責任者に行われた場合には、当該責任者は、技術等情報管理責任者に当該報告を共有するものとする。 ①兆候等 ・技術等情報を保存しているサーバーや記録媒体へのアクセス回数の大幅

行為を発見した場合 ・特定の競合他社など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 ・保管容器など重要技術の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。）についての破損などの不具合を発見した場合 ②発生等 ・重要技術の情報に関する表示が付された書類、物件等へのアクセス権を有する者以外の者が、アクセス権者が近傍にいない状態で取り扱っていることを発見した場合 この報告の責務については、民間企業においては、少なくともトレーニングの機会を通じて全ての従業員等に対して周知を図ることとし、一般的な秘密保持契約や秘密保持に係る誓約書においても明記することを推奨する。 （２）アクセス権者が報告すべき事象 アクセス権者は、全ての従業員等が報告を行う必要のある事象に加えて、以下①②の事象を発見した場合には、重要技術情報管理責任者に対する報告を行う義務を負う。この義務については、重要技術の情報に係る誓約書等において担保するものとする。 また、アクセス権者が、重要技術の情報の漏えい等の事故の発生を発見した場合には、速やかに重要技術の情報の管理を適切に行うための措置をとるものと	な増加や業務上必要のないアクセス行為を発見した場合 ・特定の競合他社など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 ・保管容器など技術等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。）についての破損などの不具合を発見した場合 ②発生等 ・技術等情報へのアクセス権を有さない者が、アクセス権者が近傍にいない状態で、技術等情報を取り扱っていることを発見した場合 この報告の責務については、トレーニングの機会を通じて全ての従業員等に対して周知を図ることとする。 （２）アクセス権者が報告すべき事象 アクセス権者は、全ての従業員等が報告を行う必要のある事象に加えて、以下①②の事象を発見した場合には、技術等情報管理責任者に対する報告を行わせるものとする。この報告の責務については、アクセス権者向けのトレーニングの機会を通じて全てのアクセス権者に対して周知を図ることとする。 アクセス権者が、技術等情報の漏えい等の事故の発生を発見した場合には、速やかに技術等情報の管理を行うための措

し、具体的な措置内容については、重要技術情報管理責任者において手順として定める。 ①兆候等 ・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）が著しく増加した場合 ・物理的措置についての不備など、このガイドライン及び社内の情報の保護に関するルールと照らして不具合と考えられるもの又は不具合が発生するおそれがあることを発見した場合 ②発生等 ・重要技術の情報の紛失、流出、漏えい等の事故の発生又は発生のおそれがある場合 ・重要技術の情報の漏えい等の事故の発生等があった場合に講じた措置 （３）報告があった場合の対応 重要技術情報管理責任者は、重要技術の情報の漏えいの兆候等に関する報告・共有があった場合には、直ちに事実関係（漏えいの疑い等）を確認するとともに、重要技術の情報の管理に関して必要な措置を講じ、又は講じることをアクセス権者に指示するものとし、その手順の細則を定めるものとする。	置をとるものとし、具体的な措置内容については、技術等情報管理責任者において手順として定める。 ①兆候等 ・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）が著しく増加した場合 ・物理的措置についての不備など、本基準及び社内の情報の保護に関するルールと照らして不具合と考えられるもの又は不具合が発生するおそれがあることを発見した場合 ②発生等 ・技術等情報の紛失、流出、漏えい等の事故の発生又は発生のおそれがある場合 ・技術等情報の漏えい等の事故の発生等があった場合に講じた措置 （３）報告があった場合の対応 技術等情報管理責任者は、技術等情報の漏えいの兆候等に関する報告・共有があった場合には、直ちに事実関係（漏えいの疑い等）を確認するとともに、技術等情報の管理に関して必要な措置を講じ、又は講じることをアクセス権者に指示するものとし、その手順の細則を定めるものとする。
９．情報セキュリティ（電子情報の保護等）について 重要技術の情報について、電子情報として保存がされている場合であっても、基本的には、他の媒体と同じように管理	９．情報セキュリティ（電子情報の保護等）について 技術等情報について、電子情報として保存がされている場合であっても、基本的には、他の媒体と同じように管理を行

を行うものとするが、電子情報の特性等に応じて、以下の付加的な管理に係る措置を講じるものとする。 　なお、これらの措置を重要技術の情報を保有する民間企業内部のリソースで講じることが難しい場合には、信頼のあるセキュリティの専門事業者などに協力を求めることを推奨する。	うものとするが、電子情報の特性等に応じて、以下の付加的な管理に係る措置を講じるものとする。 　情報セキュリティに関する措置は、信頼のあるセキュリティの専門事業者などを積極的に活用することとする。この場合において、当該専門事業者については、その活用の前に、６の規定に則して評価を実施する。
（１）電子情報である重要技術の情報の取扱いに係る管理 ①作成時の対応 　作成された電子情報である重要技術の情報については、ファイル名に当該電子情報が重要技術の情報であることの表示を付すとともに、当該電子情報へのアクセスに、IDによる認証又はパスワード設定による認証を求めるように設定するものとする。	（１）電子情報である技術等情報の取扱いに係る管理 　①作成時の対応 　当該電子情報へのアクセスに、IDによる認証又はパスワード設定による認証を求めるように設定するものとする。
電子情報である重要技術の情報へのアクセスについて、パスワードを設定する場合には、以下の措置を講ずるものとする。 ｉ）アクセス権者毎にパスワードを設定する場合 a）当人の関連情報（例えば、名前、電話番号、誕生日）から他の者が容易に推測できる又は得られる事項に基づかないこと、 b）辞書攻撃に脆弱でない（辞書に含まれる語からだけで成り立っていないこと）、	電子情報である技術等情報へのアクセスについて、パスワードを設定する場合には、以下に掲げる措置その他適切な措置を講ずるものとする。 ｉ）アクセス権者ごとにパスワードを設定する場合 a）当人の関連情報（例えば、名前、電話番号、誕生日）から他の者が容易に推測できる又は得られる事項に基づかないこと、 b）辞書攻撃に脆弱でない（辞書に含まれる語からだけで成り立っていないこと）、 c）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

c）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ものとし、パスワードの設定に係る要求事項を、プログラムやソフトウェア等の設定とすることを推奨する。	
ⅱ）重要技術の情報である電子情報そのものにパスワードを設定する場合 重要技術情報管理責任者又はその委任を受けた者（アクセス権者に限る。）がパスワードを設定するものとし、そのパスワードについては、少なくとも１年に１度変更することを推奨する。 パスワードの共有は、アクセス権者に限るものとし、アクセス権者に限定して伝達する方法により周知を行うこととし、パスワードを記したメモ等を目につく場所に置くことを禁止する。	ⅱ）技術等情報である電子情報そのものにパスワードを設定する場合 技術等情報管理責任者又はその委任を受けた者（アクセス権者に限る。）がパスワードを設定するものとする。 パスワードの共有は、アクセス権者に限るものとし、アクセス権者に限定して伝達する方法により周知を行うこととし、パスワードを記したメモ等を目につく場所に置くことを禁止する。
電子情報である重要技術情報については、プログラムやソフトウェアの設定等により簡単に改ざんされないような措置を講じるものとする。	電子情報である技術等情報については、プログラムやソフトウェアの設定等により簡単に改ざんされないような措置を講じるものとする。
②保存時の対応 電子情報である重要技術の情報が保存されるサーバーは、社内の他の情報システムとの間にファイアーウォールを設定することを推奨する。	②保存時の対応 電子情報である技術等情報が保存されるサーバーは、社内の他の情報システムとの間にファイアーウォールを設定することその他容易に技術等情報の保存されるサーバーへのアクセスができないように設定すること。 電子情報である技術等情報であってサ

電子情報である重要技術の情報であってサーバーで保存されているものについては、自由にダウンロードができないようなプログラム、ソフトウェア等の設定を行うものとする（サーバーからダウンロードされた先の記録媒体は、重要技術の情報そのものとする。）。	ーバーで保存されているものについては、自由にダウンロードができないようなプログラム、ソフトウェア等の設定を行うものとする（サーバーからダウンロードされた先の記録媒体は、技術等情報そのものとする。）。
なお、電子情報である重要技術の情報の保存がされたサーバーについて、設置される場所が構内の場合における当該サーバーが設置される場所は、本ガイドラインの立入制限区域の考え方を参考に、重要技術情報管理責任者の指示の下、適切な物理的措置をとるものとする。	電子情報である技術等情報の保存がされたサーバーについて、設置される場所が構内の場合における当該サーバーが設置される場所は、この基準の立入制限区域の考え方を参考に、技術等情報管理責任者の指示の下、物理的措置をとるものとする。
サーバーを除くパソコン、USBなど可搬式記録媒体に電子情報である重要技術の情報が保存されている場合には、当該可搬式記録媒体を重要技術の情報そのものとして取り扱うこととし、当該電子情報については、文書作成ソフト等の利用により、複製（コピー）、印刷、他の記録媒体への記録ができないような設定をするものとする。	サーバーを除くパソコン、USBなど可搬式記録媒体に電子情報である技術等情報が保存されている場合には、当該可搬式記録媒体を技術等情報そのものとして取り扱うこととし、当該電子情報については、文書作成ソフト等の利用により、複製（コピー）、印刷、他の記録媒体への記録ができないような設定をするものとする。
重要技術の情報が保存されたパソコンは、USBメモリの差込口がないものや差込口を無効化、物理的に塞ぐ部品を取り付けたパソコンとすることを推奨する。	技術等情報が保存されたパソコンは、USBメモリの差込を禁止する。
重要技術の情報の取扱い等に外部のクラウド事業者のサーバーを利用する場合、本ガイドライン６．の外部委託先等のマネジメントを参照し、当該クラウド事業者等と秘密保持契約を締結するとともに、クラウド事業者等に対して、メン	技術等情報の取扱い等に外部のクラウド事業者のサーバーを利用する場合、６．の外部委託先等のマネジメントを参照し、当該クラウド事業者等と秘密保持契約を締結するとともに、クラウド事業者等に対して、メンテナンスなど技術等

テナンスなど重要技術の情報に関わる作業者を指定すること、操作ログを付け、操作ログの定期的な報告を行うことを求めるものとする。 　なお、テレワーク等外部から電子情報である重要技術の情報へのアクセスは認めないように設定するものとする。 ③送信時の対応 　電子情報である重要技術の情報を電子メールで送信する場合は、送信する情報そのものについて電子政府推奨暗号による暗号化をすることを推奨し、送信の際の送付先として、必ず重要技術情報管理責任者をCcで入れるものとする。 　パスワードを設定して重要技術の情報を電子メールで送信する場合は、パスワードは別メールで送信するものとする。 ④削除・廃棄時の対応 　電子情報である重要技術の情報が不要となった場合には、重要技術情報管理責任者又はその指定する者（アクセス権者に限る。）は、速やかに、復元出来ないように上書き消去（データの完全消去）を行うものする。 （２）電子情報である重要技術の情報へのアクセスに関する対応 電子情報である重要技術の情報を保有する民間企業では、誰が、どの通信機器か	情報に関わる作業者を指定すること、操作ログを付け、操作ログの定期的な報告を行うことを求めるものとする。 　なお、テレワーク等外部から電子情報である技術等情報へのアクセスは、あらかじめ、技術等情報管理責任者が認めた範囲でのみ認めるものとする。 ③送信時の対応 　電子情報である技術等情報を電子メールで送信する場合は、送信する情報そのものについて暗号化をすること、パスワードを設定することその他の適切な措置をとるものとする。 　誤送信の際の被害の拡大を防止するため、送付先として、技術等情報管理責任者をCcで入れるものとすること、パスワードを設定して技術等情報を電子メールで送信する場合のパスワードは別メールで送信することその他適切な措置をとるものとする。 ④削除・廃棄時の対応 　電子情報である技術等情報が不要となった場合には、技術等情報管理責任者又はその指定する者（アクセス権者に限る。）は、速やかに、復元出来ないように上書き消去（データの完全消去）を行うものとする。 （２）電子情報である技術等情報へのアクセスに関する対応 　誰が、どの通信機器から、いつ、どの技術等情報にアクセスしたか（アクセス

ら、いつ、どの重要技術の情報にアクセスしたか（アクセス履歴）のログを取得し、管理するものとする。	履歴）のログを取得し、管理するものとする。
（３）情報システム全体における対策 　電子情報である重要技術の情報を保有する民間企業が使用する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）を使用しないものする。	（３）情報システム全体における対策 　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）を使用しないものする。
オペレーティングシステム（OS）及びソフトウェアによる制御を無効にできるシステムユーティリティソフトウエア（システム横断的に影響を与えるソフトウエア。）の使用については、情報システム及びそのセキュリティの維持・管理に必要なものを除き、可能な限り限定するものとする。	オペレーティングシステム（OS）及びソフトウェアによる制御を無効にできるシステムユーティリティソフトウエア（システム横断的に影響を与えるソフトウエア。）の使用については、情報システム及びそのセキュリティの維持・管理に必要なものを除き、可能な限り限定するものとする。
情報システムのOS、基本ソフトウェア、アプリケーションソフトなどは、可能な限り最新のものにアップデートするとともに、ウィルス対策ソフトウェアなどのセキュリティソフトを必ず導入し、当該セキュリティソフトは、可能な限り最新のものを利用するものとする。	情報システムのOS、基本ソフトウェア、アプリケーションソフトなどは、可能な限り最新のものにアップデートするとともに、ウィルス対策ソフトウェアなどのセキュリティソフトを必ず導入し、当該セキュリティソフトは、可能な限り最新のものを利用するものとする。
情報システムは、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う等により、悪意あるコードから保護するものとし、情報システムを構成するサーバー、パソコン等の通信機器について、一週間以上電源の切られた状態にある場合には、再度の電源投入時に同じ措置をとることを推奨する。	情報システムは、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、フルスキャンを行う等により、悪意あるコードから保護するものとする。

情報システムには、原則として、業務に必要のないソフトウェアのインストールを禁止するものとする。	情報システムには、原則として、業務に必要のないソフトウェアのインストールを禁止するものとする。
（４）情報システムの保守・点検 信頼できる第三者による情報システムの保守及び点検を行う場合であって、電子情報である重要技術の情報に関わる場合には、重要技術情報管理責任者の指示の下で、電子情報である重要技術の情報を他の記録媒体に移す等の処置を実施するか、又は重要技術の情報を保有する民間企業の従業員等が保守及び点検業務に立ち会って作業を監視することができる状況で行わせるものとする。	（４）情報システムの保守・点検 信頼できる第三者による情報システムの保守及び点検を行う場合であって、電子情報である技術等情報に関わる場合には、技術等情報管理責任者の指示の下で、電子情報である技術等情報を他の記録媒体に移す等の処置を実施するか、又は従業員等が保守及び点検業務に立ち会って作業を監視することができる状況で行わせるものとする。
また、第三者による情報システムの保守及び点検に当たって、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ものとする。	また、第三者による情報システムの保守及び点検に当たって、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ものとする。

個人情報のお取扱いについて

本公募は、経済産業省の業務委託を受けて三菱総合研究所が実施するものです。提案書にご記入の個人情報のお取り扱いについては、下記のとおり適切に管理いたしますので、ご同意の上、提案書をご提出ください。

1.個人情報の取扱いに関する弊社の基本姿勢	三菱総合研究所は、2003年1月8日にプライバシーマークの付与･認定を受けております。 ご提案者の個人情報は、弊社が定める「個人情報保護方針」に則り、適切な保護措置を講じ、厳重に管理いたします。
2.ご提案者の個人情報の利用目的	ご提案者の個人情報は、本事業の公募及び諸連絡のために利用させていただ きます。それ以外の目的で個人情報を利用する場合は、改めて目的をお知らせし、同意を得るものといたします。
3．ご提案者の個人情報の提供	ご提案者の個人情報については、当該プロジェクトの業務委託元である以下の組織に、以下の目的により提供を予定しています。 提供先　：経済産業省 提供する目的　：　本事業及び諸連絡 提供する個人情報の項目： 氏名、勤務先、所属、役職、電話番号、FAX、メールアドレス 提供の手段又は方法：手渡し
4．ご提案者の個人情報の委託	ご提案者の個人情報は、外部委託事業者に個人情報を取扱う業務を委託する予定はありません。
5．ご回答者の個人情報の利用終了後の措置（個人情報の保管期間）	当該契約終了後、弊社が責任をもって廃棄いたします。
6.個人情報に関するご連絡先	①　個人情報保護管理者：株式会社三菱総合研究所 代表取締役常務　松下岳彦 （連絡先:03-5157-2111、E-mail:privacy@mri.co.jp） ②個人情報の取扱いに関するご連絡先、苦情・相談窓口 ※開示、訂正、利用停止等のお申し出は、下記窓口までご連絡ください。 株式会社三菱総合研究所　広報部 電話：03-6705-6004　FAX：03-5157-2169 E-mail：prd@mri.co.jp　URL： http://www.mri.co.jp/request/

◆弊社の「個人情報保護方針」「個人情報のお取扱いについて」をご覧になりたい方は http://www.mri.co.jp/privacy_guide/privacy.html をご覧下さい。又、ご請求いただければお送り致します。

お問合せ番号：PMS000317