資料４

「限定提供データに関する指針（改訂案）」及び「秘密情報の保護ハンドブック（改訂案）」に対する主な御意見及びそれに対する考え方

平成６年１月 29 日

Ⅰ.「限定提供データに関する指針（改訂案）」について

項目	御意見	御意見に対する考え方
１．総論	● 基本的に法改正に伴う指針の修正であり、修正案に賛成する。今後、適宜、必要に応じて当該指針の見直しを行っていただくことを希望する。	● 御意見ありがとうございます。今後も適宜、必要に応じて本指針の見直しを図ってまいりたいと考えております。
２．改訂内容の記載について	● P6「(法第 19 条第１項第８号) 令和５年改正後の法第 19 条第１項第９号」と改正前と改正後との条項を記載していますが、改正後の最新の条項だけを記載したほうがいいのではないかと思います。	● 御指摘を踏まえ、限定提供データに関する規定の創設時の条文が参照できるよう、「法第 19 条第１項第８号」の記載は残しつつ、注釈として改正後の最新条項である「第 19 条第１項第９号」に言及することとしました。
	● 限定提供データ指針改訂案 16 頁において、営業秘密及び限定提供データの「両制度による保護の可能性を見据えた管理を行うことが期待される。」という改訂案が示されているところ、各企業においては、まさにそのような管理体制の具体的内容を知りたいという要望があることから、今後、当該管理に関するガイドブック等が策定されるべきである。 当該策定の際には、当連合会としても協力を惜しむものでない。	● 御指摘のありました管理体制の具体的内容につきましては、本指針の今後の見直しにおいて、情報管理の実務での状況等を勘案しながら、明確化を検討してまいりたいと考えております。
	● 16 頁「営業秘密」の定義について、一つの考え方を示すものとして「営業秘密管理指針」の参照が例示され	● 利便性を高める観点から、御意見を踏まえて、注釈として「営業秘密管理指針」の URL

	ている。本「限定提供データに関する指針」(改訂案)は中小企業等も参考にするものであるので、利便性を高めるため、欄外等に「営業秘密管理指針」の URL（https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf）の掲載を図っていただくことを希望する。	（https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf）の記載を追記いたしました。
３．改訂内容以外の記載について	● 「限定提供データ」についてⅡ章で法の定義の解説がされている。この章または、付録等で、そもそも「限定提供データ」と「営業秘密」及び「著作権」との関係を「秘密管理性」、「公知性」等の特性との関係でわかりやすく図示した説明を含めて欲しい。	● 限定提供データと対比して取り上げるべき情報の範囲についての精査とともに、どのような観点から整理を行うのが適切かなど様々な論点が考えられることから、御指摘のあった意見につきましては、今後の改訂時の参考とさせていただきます。
	● P13「下記の認証に関する技術を単独若しくは複数組み合わせて使用することや、認証に関する技術に暗号化に関する技術 を 組み合せて使用することが考えられる。」と記載されている。⑴階層が１つの場合は、「若しくは」ではなく、「又は」を使うルールがある。⑵助詞の「や」は、or 若しくは and 又は and/or のどれを指すか不明確になるため、避けるべき。	● 御指摘の箇所については、認証に関する技術の使用、認証に関する技術と暗号化に関する技術を組み合わせての使用について、考えられる具体例として記載したものですが、その内容については誤解が生じる記載にはなっていないと考えており、原案のままとさせていただきます。
	● P13 の「対応する措置としては」から 14 頁の「②専用回線」までの説明は、現状の技術において、秘密管理性の具体的な例示であり、本内容のままだけでは秘密管理性の最低限の要求にもなっていない。指針ではなく、ガイドライン、ハンドブック等の望ましい対応であり、法的な要件の必須ではない記載ではないかと	● 限定提供データに関する指針では、立法時の議論・検討を踏まえて、各要件についての考え方をお示ししていますが、裁判例の蓄積等を踏まえて今後本指針の見直しを行う際には、御指摘の点も参考にして検討してまいりたいと考えております。

	思います。	
	● 当連合会は、2022年4月意見書5～6頁において、「指針（改訂案）45頁で、「限定提供データに係る不正競争によって『営業上の利益』を侵害される者は、原則として、『限定提供データ保有者』（法第2条第1項第14号、法第15条2項参照）になると考えられる。」という記載は、「『限定提供データ保有者』（法第2条第1項第14号、法第15条第2項参照）は、原則として、限定提供データに係る不正競争によって『営業上の利益』を侵害される者になると考えられる。」と修正するのが適切だと思われる。」と述べた。 この点については、今回の限定提供データ指針改訂案48頁でも修正はなされていない。 もっとも、本質的な問題としては、限定提供データ指針改訂案が、「誰がデータ保有者となるかについては、不正行為の対象とされたデータの管理にかかる具体的ビジネスモデル等によって事案ごとに決まる。」（同39頁）と解説しているものの、そもそも、「限定提供データ保有者」という定義規定に関する解説をしていないこと、及び「データ保有者」という用語に関する解説もしていないことに起因する問題と考えられる。 限定提供データ指針改訂案39～40頁及び49頁においても紹介されているように、データの利活用にお	● 2022年時のパブリックコメントにおいて、同趣旨の御意見を頂戴した際、当該御意見を踏まえ、 「限定提供データに係る不正競争によって『営業上の利益』を侵害される者に当たるのは、原則として、『限定提供データ保有者』（法第2条第1項第14号、法第15条第2項参照）であると考えられる。」 との修正を前回改訂時に既に行っております。 また、「限定提供データ保有者」の解説につきましては、今後の裁判例の動向や蓄積を踏まえて、次回の改訂に向けて、検討してまいりたいと考えております。

	いては複数主体が登場するものであるから、何をもって「データを保有」していると考えられるのか、「営業上の利益」を有していれば「データ保有者」なのか、電磁的管理を施している者が「データ保有者」なのか等、今後の情報管理に関する実務及び技術の推移を踏まえながら限定提供データ保護制度の趣旨に照らして次回改訂時に充実した議論が行われることを期待する。	
4．その他	● パブコメの文書が Word の変更履歴(いわゆる red version)で提供され、変更箇所が、既存のドキュメントとの対応でわかりやすくなっていると思います。しかし、最低限 PDF で公開するのであれば、可読性を高めた“しおり付き PDF”で開示すべきだと思います。さらにレビューをしやすくするためには、Word で提供されるとワイルドカード検索なども有効に活用できると思います。さらに、Word の変更履歴付きで提供されることにより、変更を見たい場合、変更後の文書を見たい場合など切り替えてみることができ、レビューの質、速度を向上できる可能性があると思います。	● いただいた御意見については、今後のパブリックコメントの募集に際して、参考にさせていただきます。
	● 「営業秘密管理指針」と本パブコメ対象の「限定提供データに関する指針」と 2 つの指針があり、両方とも根拠法として不正競争防止法と同じ法を根拠としているにもかかわらず、各企業は両方を確認しないとい	● 営業秘密と限定提供データは、保護客体・不正競争行為がそれぞれ別のものとして規定されており、また、法律上、両者の保護は重複しないものと規定されております。このため、その法的保護を受ける上

	けない。新しい限定提供データに関して議論した結果であることは、認識はできますが、使用者である企業は両方を合わせて考えないといけない。両方を合わせて、同じ部分、異なる部分とを明確に記載した指針とすべきではないかと思います。	での措置等を解説する指針について、別個独立のものとして作成・公表しても、事業者にとって支障はないものと考えております。ただし、指針、ハンドブックなど解説書が多岐にわたっている中で、今後の各種資料を抜本的に改訂する際には、いただいた御意見を参考にさせていただきます。
	● 本パブコメの対象ではないかもしれませんが、不正競争防止法に関する文書は、経済産業省等から、営業秘密管理指針、今回の限定提供データに関する指針、ハンドブック、手引き、等の関係をもう少し整理した上で、Web ページ上で公開すべきではないかと思います。	● 御指摘のとおり、経済産業省において作成・公表している不正競争防止法に関する資料は複数あるところ、その公表に際しては、事業者、制度利用者の皆様にとって分かりやすい形での情報提供に向けて、御指摘の点も踏まえ、対応してまいりたいと考えております。
	● 限定提供データ指針改訂案は、秘密情報ハンドブック改訂案と比して、近時の AI として利活用されている生成 AI に関する言及は見当たらない。しかし、近時、AI を利活用する場合、そのモデルによっては、「取得したデータを使用して得られる成果物」（限定提供データ指針改訂案 24 頁）が「取得したデータと実質的に等しい場合や実質的に等しいものを含んでいると評価される場合」（同頁）もあると考えられる。 AI に関する今後の技術趨勢及び議論を踏まえて、次回改訂時に充実した議論が行われることを期待する。	● いただいた御意見については、AI に関する今後の技術趨勢及び議論を注視しつつ、次回改訂時の参考にさせていただきます。

Ⅱ.「秘密情報の保護ハンドブック（改訂案）」について

項目	御意見	御意見に対する考え方
１．総論	● AI を活用する際の留意点、経済安全保障推進法施行後の留意点等の環境の変化に対応したタイムリーな改訂が含まれ、また多くのコラム等についても追記がなされており、企業だけではなく大学に対しても情報管理の重要性について注意喚起する修正になっており、修正案に賛成する。なお、今後、当該ハンドブックの改訂について普及を図るにあたり、中小企業や大学関係者にもわかりやすい簡易版の説明資料を作成いただくことを希望する。また、今後も、適宜、必要に応じて当該ハンドブックの見直しを行っていただきたい。	● 御意見ありがとうございます。御意見を踏まえて、主な改訂箇所について整理した資料を作成し、これとともに周知・啓発に努めてまいりたいと考えております。なお、大部にわたる本ハンドブックを利用する上での導入となるてびき・要点をまとめた「秘密情報の保護ハンドブックのてびき」も作成・公表しており、この資料も紹介・併用しながら、営業秘密の管理・保護に関する啓発につとめるようにいたします。 また、今後も適宜、必要に応じて本ハンドブックの見直しを図ってまいりたいと考えております。
２．改訂内容の記載について	● 非常に重要な「生成 AI」に関して追加することは賛成です。しかし、主に管理すべきは、外部の生成 AI でかつデータの利活用が管理されていないものであり、必要以上に生成 AI に関して利活用を躊躇してしまう記載は避けるべきだと思います。外部の AI においても、その AI サービス提供者との間で、入力したデータの他への利活用をしない旨の契約、運用が保証されれば、外部の生成 AI においても、効果的に利活用すべき。	● 総論にあたる冒頭において、生成 AI の活用を通じた利便性などの効用にも言及することとし、その利用・活用への萎縮がないよう配慮いたしました。なお、その他の箇所につきましては、漏えい防止に向けた具体的な対策・措置に関する注意事項であることから、原案のままとさせていただきます。
	● 今般の生成 AI ブームを踏まえて、秘密情報ハンドブ	● 従前の AI を利用したツールを含め、AI に関する今

	ック改訂案において全般的に生成 AI に関する記述の加筆案が示されていることについては評価するが、例えば、生成 AI でない従前の AI を利用した文書系ツールの利用による文書記載内容の漏えいリスクについては従来から指摘がなされてきたところであり、単に「生成 AI」に絞った追記とすべきかについては、検討を要する。 「生成 AI を含む新たなツール」(秘密情報ハンドブック改訂案 129 頁) という記載もあるが、例えば、「生成 AI を含む新たなツール」には、従前の AI を利用した文書系ツール及びチャットボット ((生成) AI が搭載されているのか否か利用者において判然としない場合もある)等があることについても付記すべきである。 また、秘密情報ハンドブック改訂案への生成 AI に関する追記にあたり「社外に流出・公開等されてしまう可能性」(秘密情報ハンドブック改訂案 27 頁) 等の記載が多用されているが、そもそも「生成 AI を含む新たなツール」を利用して入力した情報を「社外」の者がアクセスできるようになることを認識していない企業等も散見されるから、より具体的な記載が望ましい。	後の技術趨勢及び議論を注視しつつ、いただいた御意見については、次回改訂時の参考にさせていただきます。
	● P2「1-1 目的及び留意点等」において、「(本書と限定提供データに関する指針との関係)」が記載されてい	● 御指摘の箇所は、平成 30 年に限定提供データ制度が導入されたことに伴い、限定提供データに関する指

	ます。そこで、「など限定提供データにも活用可能な内容も含まれており、その管理について参考になるものと考えられます。」と記載されています。2 つの指針と本書との関係をもう少し丁寧に記載すべきかと思います。限定提供データでも参考になると記載されていますが、これ自体は間違いではないですが、営業秘密にも参考になる記載があるとか、営業秘密と限定提供データとの両方に参考になるとかの記載にしたほうが誤解しにくいのではないかと思います。現状の記載では、本書が営業秘密を主としたハンドブックであり、限定提供データには参考にはなるが、それを主に記載していないとよめてしまう。さらに、すると、限定提供データのハンドブックがどこかに存在することを推定してしまう。2 つの指針(本来 1 つにすべきですが)は、法的な条件のみにして、本ハンドブックは、営業秘密、限定提供データ、その他のデータを企業が管理するために、必須ではないが、参照できるような位置付けにして(そのようになっているのかもしれませんが)、それを明確に記載すべきではないかと感じます。	針について従来参考情報扱い（枠囲い）で追加された記載であったが、2023 年の法改正で限定提供データの保護範囲について整理がなされたこと、また限定提供データ制度が導入されて５年が経過し、営業秘密管理指針と同様に本文扱いとすることが適切との観点から、従来の記載内容を踏襲しながら、今回の法改正内容を踏まえた技術的な整理を行ったものであり、内容面で不明瞭・誤解が生じるとは考えていないことから、原案のままとさせていただきます。
	● ハンドブックの転職・独立は、転職・独立起業が良いのではないでしょうか？	● 御指摘を踏まえ、「転職・独立・起業」と修正いたしました。
	● Ｐ4 脚注 4 がリンク切れしているようです。	● 脚注のリンク先を以下に修正いたしました。 https://www.meti.go.jp/shingikai/mono_info_ser

		vice/ai_shakai_jisso/pdf/20220128_1.pdf
	● 6ページの枠線内の8行目「あてはまる」と、同12行目「当てはまる」とは、どちらかに字句を統一したほうがよい。	● 御指摘を踏まえ、文書内での平仄の観点から、「あてはまる」に修正いたしました。
	● 6ページの枠線内の1行目「大学・研究機関など」の「など」には、大学・研究機関以外の何が含まれるのか？	● 御指摘の箇所に関係するその他の組織としては、例えば高等専門学校があてはまると考えております。
	● P19 「(顧客の個人情報、受託やライセンス、M&Aにおける交渉（事前協議を含む。） 等の他社との契約等により限定的に開示された営業情報 ・限定提供データ等)」と記載されていますが、言葉の係り方がわかりにくくなっています。さらに、助詞の“や”は、andなのかorなのか不明になりやすいのでJISでは避けるべきとされています。「受託やライセンス」と「M&A」との関係、最後の「営業情報・限定提供データ等」はその前のどこまでを示しているか。 (変更案)(顧客の個人情報、受託若しくはライセンス又はM&Aにおける交渉（事前協議を含む。）等の他社との契約等により限定的に開示された営業情報 ・限定提供データ等)	● 御指摘の点を踏まえ、明確化の観点から19頁の記載を以下のとおり修正いたしました（20 頁も同旨修正)。 「(顧客の個人情報、受託契約・ライセンス契約・M&A交渉におけるNDA等の他社との契約等により限定的に開示された営業情報・限定提供データ等)」
	● P21脚注13がリンク切れしているようです。	● 脚注のリンク先を以下に修正いたしました。 https://www.jnsa.org/ikusei/01/02-02.html
	● P.37	● 御意見を踏まえて、記載を修正いたしました。

	コラム３　外国から狙われる企業の秘密情報 〇意見内容 ３（通常の）経済・学術活動（に見せかけた）を通じ秘密情報の窃取 ↓ ３（通常の）経済・学術活動（に見せかけた）を通じ「た」秘密情報の窃取 〇理由 「た」が不足していると思われます。	
	● P42 脚注 21 がリンク切れしているようです。	● 脚注のリンク先を以下に修正いたしました。 https://www.npsa.gov.uk/trusted-research-academia
	● 今次改正により「日本国内において管理されている」営業秘密に関する国際的な侵害事案における民事訴訟の手続が明確化されたこと（同法第 19 条の 3）を紹介する秘密情報ハンドブック改訂案 135 頁で、「管理」の説明として「サーバに蔵置」という新しい用語が見受けられるが、物理サーバ及び仮想サーバそれぞれに応じて「管理」に該当し得る例を解説すべきである。	御指摘の点を踏まえ、わかりやすさ、明確化の観点から 135 頁の記載を以下のとおり修正いたしました。 「これにより、日本国内において保有・管理されている営業秘密だけでなく、海外に所在するサーバに保存されている営業秘密についても、海外での侵害行為（海外に所在する物理サーバや仮想サーバからの取得行為等）に対し日本の不正競争防止法に基づいて保護を受けることが可能となりましたが、この保護を受ける上で、日本国内で管理体制を敷いていること（例：ID・パスワードの設定

		など）が必要なことから、営業秘密を海外に所在するサーバに保存している場合には、これらを意識して取り組むことが重要となります。」
	● 今次改正について説明する秘密情報ハンドブック改訂案 146 頁で「①産業スパイなど営業秘密を不正手段で取得した者（第 2 条第 1 項第 4 号）」と追記する改訂案が示されているが、平成 27 年の制度導入当初から、「産業スパイ」に対象を限っていたものではなく、同号の不正取得行為があたかも「産業スパイ」並みに不正な場合に限られるかのような誤解も生じかねない。 よって、「産業スパイ」は削除することが望ましい。	● 御指摘の箇所については、営業秘密を不正手段で取得した者（第 2 条第 1 項第 4 号）の例として分かりやすいものをあげたものであり、記載ぶり（「例えば」と明記）からこれに限定されるとの誤解はないと考えており、原案のままとさせていただきます。
	● 秘密情報ハンドブック改訂案 147 頁で「警告書を受け取ること等により営業秘密の不正取得・不正開示に関する経緯を事後的に知った場合であって」と追記する改訂案が示されているが、実務においては、どのような内容の警告書であれば事後的悪意とすることができるのかという点が問題である。単に警告さえすれば（受け取らせさえすれば）事後的悪意にできるかのように読める記載については、転職の自由及び人材の流動化という時勢に鑑みても、より明確かつ適切な記載を検討すべきである。 同様に、秘密情報ハンドブック改訂案 149～150 頁にかけて「転職者により営業秘密の持ち出し等を理由と	● どのような内容の警告書であれば事後的悪意とすることができるのかという点につきましては、今後の裁判例の動向や蓄積を踏まえて、次回の改訂に向けて、その記載ぶりを検討してまいりたいと考えております。 また、149～150 頁については、改正後の第 5 条の 2 の運用・実務の状況などを踏まえて、次回改訂時の参考にさせていただきます。

	する警告や訴えの提起等がなされた場合には」と追記する改訂案が示されているが、①「警告」の段階と「訴えの提起」の段階とでは、転職前に勤務していた企業の秘密情報が社内に持ち込まれた可能性の程度も異なる上、②実務においては、「同人が社内に持ち込んだ情報」が何なのか明確に分からない中で社内調査を行わなければならない場合もあり、また、③「その内容によっては当該情報を削除」したくても「当該情報」の外延が不明であったり、混入していて「削除」できなかったりする場合もあることから、追記するのであれば、場合分けをしたり、実務上の問題点も紹介するなど、より記載を充実化すべきである。	
３．改訂内容以外の記載について	● P.31 （１）ルール化の必要性とその方法 箇条書き３つ目 〇意見内容 「クラウド上に置く際のアクセス権限を適切に設定すること等」と記載がありますが、アクセス権限だけでなく、下記のような認証やユーザ管理などにも触れるのはいかがでしょうか。 ・多要素認証を採用するなどといった認証強度 ・不要なアカウント/権限の削除 ・定期的な設定のチェック。※Salesforce の事故受けて	● 対策方法の拡充を図る観点から、御意見を踏まえて、御指摘の手法についてもある旨を注釈に追記いたしました。

	○理由 適切なアクセス制御の実現のためにはアクセス権限の設定だけなく、制御の前提となる適切なアカウント管理についても重要であると考えられるためです。	
	● P. 33 （２）秘密情報の取扱い等に関する社内の規程の策定 囲み線内の最後の箇条書き ○意見内容 の保存が可能な場合、端末の内蔵記憶装置の号化やデータのリモートワイプの対策強化） ↓ の保存が可能な場合、端末の内蔵記憶装置の「暗」号化やデータのリモートワイプの対策強化） ○理由 誤記と思われます。	● 御意見を踏まえて、記載を修正いたしました。
	● P. 34 （２）秘密情報の取扱い等に関する社内の規程の策定 ページ内箇条書き２つ目 ○意見内容 セキュリティ確保のためのルール（クラウドサービスで用いるパスワードについて他の用務で用いるパスワードとの共用を避けるなどの厳格な管理、データの共有範囲の限定等）を定めて ↓	● 対策方法の拡充を図る観点から、御意見を踏まえて、記載を修正いたしました。

	セキュリティ確保のためのルール（多要素認証の設定、パスワードの使いまわしを避ける、データの共有範囲の限定、不要なアカウント/権限の削除等）を定めて 〇理由 多要素認証などについても近年のセキュリティ対策では基本的な対策となっていると考えられるためです。	

	● コラム３　外国から狙われる企業の秘密情報 ① １　リスク低減のための措置 〇意見内容 箇条書きに下記を追加するのはいかがでしょうか。 「保有するアプリケーション/システムに対する定期的な脆弱性診断やペネトレーションテストを実施する。」 〇理由 システムに潜むリスクを脆弱性診断やペネトレーションテストの実施によって攻撃される前に特定し、インシデントにつながる脆弱性を管理することが必要なためです。 ② １　リスク低減のための措置 最後の箇条書き 〇意見内容 〇 近年のランサムウエアの流行に対抗するためには「,」データの ↓ 〇 近年のランサムウエアの流行に対抗するためには「、」データの 〇理由 「,」ではなく「、」が正しいと思われます。 ③ １　リスク低減のための措置＞最後の箇条書き 〇意見内容	● ①②④については、御意見を踏まえて、記載を修正いたしました。 ③については、御意見を踏まえて、わかりやすさの観点から、記載内容が分かりやすくなるよう、以下のとおり修正いたしました。 「近年のランサムウェアの流行に対抗するため、情報窃取被害によるリスク低減を図る観点から自組織で保管する重要データを暗号化する。」 また、バックアップの取得については、「３　インシデント発生時の適切な対処・回復」に記載しておりますが、御意見を踏まえて、わかりやすさの観点から「３　インシデント発生時の適切な対処・回復への備え」と項目名を修正いたしました。

	近年のランサムウエアの流行に対抗するためには,データの暗号化が必要となると考えられます。 ↓ 近年のランサムウエアの流行に対抗するためには、システムの暗号化被害に備えたバックアップの取得が必要となると考えられます。 〇理由 ランサムウェアの典型的な攻撃は、システムを暗号化して復号と引き換えに身代金を要求するものであるため、有効な対策はバックアップ等によって不正な暗号化に備えることを対策としてはいかがでしょうか。 ④　2　インシデントの早期検知 箇条書き１つ目 〇意見内容 〇 サーバ等における各種ログを確認する。 ↓ 〇 サーバやPC、ネットワーク機器等における各種ログを確認する。 〇理由 ユーザーが操作するPC等から収集できるログもインシデント対応に重要な場合があるため、「サーバ以外のログにも目を向ける必要がある」という点で「等」にまとめるのではなく、少し具体的な名称を追加してはいかがでしょうか。	

	● P.56 ３－４ 具体的な情報漏えい対策例 （１）従業員等に向けた対策 ２「持ち出し困難化」に資する対策 【書類、記録媒体、物自体等の持出しを困難にする措置】 ｃ．電子データの暗号化による閲覧制限等 ・意見内容 電子データにおいて「閲覧」以外の情報漏えいに繋がる可能性のあるすべての操作を制限するための文言の追記 ・理由 電子データの持出しにつながる操作は閲覧だけではなく、印刷やコピー&ペーストなども同様である。 故に暗号化による閲覧制限だけではなく、閲覧権を持つ従業員等に対してもデータ単位で閲覧、編集、印刷、コピー&ペースト等の利用権限を設定し、最小の権限でデータを利用させるようにすることが望ましい。 またこの暗号化した電子データを参照するためには管理サーバーによる認証を受けることが必要となるシステムが望ましい。	● 対策方法の拡充を図る観点から、御意見を踏まえて、御指摘の手法についてもある旨を注釈に追記いたしました。
	● P.59 【秘密情報の複製を困難にする措置】 ｊ．私物の USB メモリや情報機器、カメラ等の記録媒	● 対策方法の拡充を図る観点から、御意見を踏まえて、記載を修正いたしました。

	体・撮影機器の業務利用・持込みの制限 下から2つ目の箇条書き 〇意見内容 機器の利用制限を行うことのほか、EDR（Endpoint Detection and Response）の導入などするなど内部不正モニタリングシステムを活用し ↓ 機器の利用制限を行うことのほか、EDR（Endpoint Detection and Response）やNDR（Network Detection and Response）等の導入で社内ネットワーク全体の不審な挙動や異常を検知し 〇理由 近年のIT環境はエンドポイントが増加しており、EDRのみではなくNDRを活用したネットワーク全体での監視の重要性が増していると考えられます。 ● P.67 ｏ．PCやネットワーク等の情報システムにおけるログの記録・保存とその周知 箇条書き4つ目 〇意見内容 マルウェア対策機能、不正サイトへの接続をブロックする機能等を利用することや、EDRを導入し、エンドポイントにおける不審な挙動や異常を検知し、 ↓	

	マルウェア対策機能、不正サイトへの接続をブロックする機能等を利用することや、EDR（Endpoint Detection and Response）やNDR（Network Detection and Response）等の導入で社内ネットワーク全体の不審な挙動や異常を検知し、 ○理由 近年のIT環境はエンドポイントが増加しており、EDRのみではなくNDRを活用したネットワーク全体での監視の重要性が増していると考えられます。 ● P.68 ｏ．PCやネットワーク等の情報システムにおけるログの記録・保存とその周知 箇条書き5つ目 ○意見内容 企業内での場合と異なり物理的な視認性の確保が困難なことから、テレワークに伴うログを記録して、安全に保存するようにします。 ↓ 企業内での場合と異なり物理的な視認性の確保が困難なことから、テレワークに伴うログをPC管理ツール等を活用して記録し、安全に保存および収集をするようにします。 ○理由 PC上に保管されるログは改ざんされたり、ログ取得	

	を無効化されたりする可能性が考えられます。 単純にログを保存するのではなく、PC 管理ツールと呼ばれるようなもので安全に保管し、必要に応じて管理サーバーへのログ送信が必要ではないかと考えられます。	
	● P.91（改訂前 P.82） 取引先の管理能力の事前確認 　取引先の決定に当たっては、当該相手方が秘密情報を適切に管理し、かつ、自社からの情報管理に係る要請に適切に対応できる能力を有するか否かを、事前調査や、ISMS(情報セキュリティマネジメントシステム)などの基準・認証・資格などを参考としつつ、事前に確認することが重要です。 ↓ 省略 「事前調査や、プライシーマーク、ISMS（情報セキュリティマネジメントシステム)、CBPR などの基準」 （コメント） プライバシーマークと、CBPR の追加を提案します。 ● 改訂案）91 頁「取引先の管理能力の事前確認」の部分 「ISMS（情報セキュリティマネジメントシステム）などの基準・認証・資格など」の部分。 〇意見内容 ISMS に加え「プライバシーマーク」及び「APEC CBPR	● 御意見を踏まえて、関係機関・関係団体にも確認の上、今回の改訂版の公表までに修正いたします。

	ないしグローバル CBPR（越境プライバシールール)」を加えることを要望します。 ○理　　由 本ハンドブック案は、「情報漏えいのリスク」についての管理体制整備、「プライバシー・人権を保護するための個人情報保護法等の法的要求を満足できる組織体制の構築」(160 頁、163 頁）等について解説するものです。これらの体制構築・確認にあたり、既に普及しているプライバシーマーク制度や、経済産業省や個人情報保護委員会が推奨している CBPR システムの参照が有効であると考えられるため、当該システムに基づく認証に言及していただきたいと考えます。	
	● P.112 ｆ．ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート 1 行目 ○意見内容 例えばファイアーウォールや IDS/IPS とウェブサーバーの間に ↓ 例えばファイアーウォールや IDS/IPS と「ウェブサーバ」の間に ○理由 他のページに合わせて「サーバ」としてはいかがでし	● 御意見を踏まえて、記載を修正いたしました。

	ょうか。	
	● P.161 6-1　漏えいの兆候の把握及び疑いの確認方法 （１）漏えいの兆候の把握 箇条書き４つ目 〇意見内容 AI 等の最新技術を組み入れたモニタリングシ「ム」テム ↓ AI 等の最新技術を組み入れたモニタリングシ「ス」テム 〇理由 「システム」の誤記と思われます。	● 御意見を踏まえて、記載を修正いたしました。
	● P.228 秘密情報管理に関する各種ガイドライン等 について 以下の認証に関する適合評価基準等の追加を提案します。 ・プライバシーマーク ・CBPR ● （改訂案）228 頁「(参考資料４）秘密情報管理に関する各種ガイドライン等」の部分 〇意見内容	● 御意見を踏まえて、関係機関・関係団体にも確認の上、今回の改訂版の公表までに修正いたします。

	ISMS に加えプライバシーマーク（JIS Q 15001）、APEC 及びグローバル CBPR 認証の解説を加えることを要望します。 〇理　　由 本ハンドブック案は、「情報漏えいのリスク」についての管理体制整備、「プライバシー・人権を保護するための個人情報保護法等の法的要求を満足できる組織体制の構築」（160 頁、163 頁）等について解説するものです。これらの体制構築・確認にあたり、既に普及しているプライバシーマーク制度や、経済産業省や個人情報保護委員会が推奨している CBPR システムの参照が有効であると考えられるため、当該システムに基づく認証に言及していただきたいと考えます。	
	● P.228 秘密情報ハンドブック改訂案 187 頁以下の参考資料２についても、情報の利用態様の変化（例えば、CD が使われることは少なくなった一方で、クラウドサーバを利用することが多くなった等）を踏まえた参考例に改訂し、スタートアップ及び中小企業等において参照しやすい参考例とすべきである。なお、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号）」（同頁）は廃止されたので該当記載は削除すべきである。	● いただいた御意見については、次回改訂時の参考にさせていただきます。 また、御意見を踏まえて、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号）」に関する記載を削除いたしました。

	● 参考資料 5（P. 235～） 特にスタートアップ企業等においては人材が流動化しており競業避止義務契約が締結されることも少なくないことから、秘密情報ハンドブック改訂案 237 頁以下の裁判例紹介も適宜、アップデートすべきである。	● いただいた御意見については、今後の参考にさせていただきます。
4．その他	● 2 章かその前に、保有する情報の把握・評価、秘密情報の決定において、不正競争防止法の営業秘密、限定提供データ、著作権上で保護されるもの、個人情報保護法など情報、データの分類とそれに関係する法などが図示して説明があるといいのではないかと思いました。	● 御指摘の点については、今後の改訂時の参考にさせていただきます。
	● ①企業における情報管理は、不正競争防止法等の法令ごとに行うものではなく、また、サイバーセキュリティ、技術情報流出及び輸出管理などのリスクごとに行うものでもなく、あらゆる法令及び実務を踏まえて横断的に行われるものである。 ②そこで、サイバーセキュリティに関して、コラムの記載（秘密情報ハンドブック改訂案 125 頁）にとどまらず、経済産業省が発行するサイバーセキュリティ経営ガイドライン（秘密情報ハンドブック改訂案 230 頁）との異同及び関係についてもより詳しく紹介されることを希望する。 ③同様に、技術情報管理についても、コラム（秘密情	● ②③④については、今後の改訂の際に検討してまいりたいと考えております。 ⑤については、本ハンドブック末尾において、「秘密情報の保護ハンドブックのてびき」及び「秘密情報の保護・活用事例集」に言及する資料を、別途添付いたします。

	報ハンドブック改訂案 141 頁）として紹介するのみならず、秘密情報ハンドブック改訂案で紹介する対策案と技術情報管理認証制度の基準との異同、並びに当該認証制度のために経済産業省が案内している自己チェックリスト及び活用ガイドとの具体的な併用（活用）方法についても紹介されることを希望する。 ④また、外為法コンプライアンスについては、特に大学等において取り組まれているところ、秘密情報ハンドブック改訂案 44 頁において「大学・研究機関に勤務している教員・研究者など」に関する加筆をするのであれば、外為法との交錯点についても、より詳しく紹介されることを希望する。 ⑤あわせて、「秘密情報の保護ハンドブック」の内容を分かりやすく紹介した資料として「てびき」が、また、秘密情報管理の事例集として「秘密情報の保護・活用事例集」が発行されていることについて、秘密情報ハンドブック改訂案においても紹介し、「秘密情報の保護ハンドブック」が企業等においてより活用されることを期待する。	
	● P179 からの「情報漏えい対策一覧」は、自社での対策を検討する際のチェックリストとしても有効ではないかと思います。その利活用をしやすくするために、Excel、Word 等の書式で提供していただけるといいのではないかと思います。	● 御指摘を踏まえて、利用者の利便性の観点から、「情報漏えい対策一覧」及び「各種契約書等の参考例」について、Word ファイルでも提供するようにいたします。

	● P187 各種契約書等の参考例などはWordで提供されると利活用しやすいのではないかと思います。	
	● パブコメの文書が Word の変更履歴(いわゆる red version)で提供され、変更箇所が、既存のドキュメントとの対応でわかりやすくなっていると思います。しかし、最低限 PDF で公開するのであれば、可読性を高めた“しおり付き PDF”で開示すべきだと思います。さらにレビューをしやすくするためには、Word で提供されるとワイルドカード検索なども有効に活用できると思います。さらに、Word で提供されることにより、変更を見たい場合、変更後の文書を見たい場合など切り替えてみることができ、レビューの質、速度を向上できる可能性があると思います。	● いただいた御意見については、今後のパブリックコメントの募集に際して、参考にさせていただきます。