「テレワークセキュリティガイドライン（第５版）」（案）に対する意見募集の結果

意見募集期間：令和３年２月15日～同年３月５日

提出意見数：20件（法人：３件、個人・匿名17件）（提出意見数は意見提出者数としています。）

No	該当箇所／意見	意見に対する考え方	修正有無
	第２章　２．組織の立場に応じた重要な役割　(1) 経営者の役割		
01	（意見） 「事業の効率的かつ健全な発展」という観点から、マネジメントやカルチャーについても言及し、本当の意味でテレワークを推進する立場にたったガイドラインとするべきである。 （理由） 経営者の役割として、「事業の効率的かつ健全な発展と、当該事業に影響を及ぼすセキュリティリスクへの対応という両側面」と言及がある（13頁）ものの、実施すべき事項の１０項目すべてがセキュリティに関する内容となっている。総務省の所管の範囲内で作成されていることは理解するが、「事業の効率的かつ健全な発展」の観点も反映するべきではないか。 （参考１）内閣官房から最近出た基礎データ（内閣官房・経済産業省「内閣 コロナ禍の経済への影響に関する基礎データ」によれば、米国では在宅勤務の方が生産性が高いと答えている人は41.2%、日本では在宅のほうが生産性が低いと答えている人が92.3%となっている。日本では光インターネットが普及しているにもかかわらず、上記の結果が出ることを考えると、技術での解決だけではこの差は埋まらないと推測される。 （参考２）マッキンゼーの報告書（2020年3月「A blueprint for remote working: Lessons from China」）では、マネジメントとカルチャーを変えなければならないと主張している。8つの洞察のうちセキュリティとテクノロジーの指摘は2つか3つ程度で、それ以外はマネジメントとカルチャーの指摘である。 （参考３）Harvard Business Review（2020年11月3日「リモートワークとは朝から晩までビデオ会議をすることではない」）では、Gitlabという企業が紹介されている。同社は、完全リモートで業務を行う2000人の社員が在籍し、急成長している企業である。テレワークで重要なのは、社員の自由度の尊重や、仕事のやり方をアジャイルなテック企業のマネジメントを取り入れることであると指摘されている。 冒頭の「事業の効率的かつ健全な発展」という観点で、国内でも多くのマネジメントやカルチャーの指摘がなされている。ぜひこういった点への言及をいただき、本当の意味でテレワークを推進する立場に立ってガイドいただきたい。 【一般社団法人新経済連盟事務局】	本ガイドラインは、第１章３．に記載のとおり「テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針」として策定するもので、記載内容もこれに沿ったものとなっており、原案通りとします。 なお、テレワーク推進は重要な課題であることから、総務省としてテレワーク総合情報サイト（https://telework.soumu.go.jp/）を開設しているほか、関係省庁とも連携しつつその推進に取り組んでいます。	無
	第２章　２．組織の立場に応じた重要な役割　(1) 経営者の役割		
02	p13などにセキュリティポリシー（基本方針）とありますが、最近は「セキュリティポリシー」とは言わずに、「基本方針」というようになっていると思います。 同じくp13に「セキュリティ責任者を定める」とありますが、責任者とともに「セキュリティ対応組織」を定めることも必要と思います。 【個人09】	「セキュリティポリシー」の呼び方に関する御意見については、本ガイドラインでは「セキュリティポリシー（基本方針）」と記載し、いずれの言葉になじみのある読者に配慮していることから、原案通りとします。 「セキュリティ対応組織」に関する御意見については、組織体制に関して「予算や人員の確保」として記載済みであることから、原案通りとします。	無
	第２章　２．組織の立場に応じた重要な役割　(3) テレワーク勤務者の役割　＜パスワードの管理＞		
03	「パスワードは、第三者に推測されにくい複雑なものを用いる」となっていますが、具体的な基準を示した方がいいと思います。 例えば、小さな中小企業とNPO向け情報セキュリティハンドブック」には、推奨パスコード基準が示されています。	パスワードの複雑性要件については、利用するシステムや利用環境により要件が異なること、及び多要素認証の利用有無によっても異なることから、原案通りとします。	無

	【個人09】	なお、内閣官房内閣サイバーセキュリティセンターが発行する「小さな中小企業とNPO向け情報セキュリティハンドブック」においても一律な基準が設定されているわけではなく、p.114以降に詳細にパスワードの複雑性について記載がなされています。	
	第２章　２．組織の立場に応じた重要な役割　(3) テレワーク勤務者の役割　＜適切なテレワーク環境の確保＞		
04	テレワークで脆弱になりがちなのは、作業を行う「テレワーク環境」であるため、テレワーク環境のネットワークセキュリティや物理セキュリティについては、独立した節を設けて説明すると、より理解が進むと考えます。 例えば、自宅のインターネット回線の利用を許可する場合は、自宅のルーターや無線LANなどをセキュアに設定する必要があるなどが挙げられます。 また、業務を行う場所の物理セキュリティの確保も必要であると考えます。 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、自宅でのセキュリティ対策等について追記します。	有
	第２章　３．クラウドサービスの活用の考え方　(1) クラウドサービスとは		
05	クラウドサービスの例に「グループウエア」も示してはどうでしょうか。 【個人09】	本ガイドラインに記載するクラウドサービスは代表的なものの例にすぎないことから、原案通りとします。 なお、グループウェアは複数サービスのパッケージとしても解されることから例示として適当でないと考えます。	無
	第２章　３．クラウドサービスの活用の考え方　(2) テレワークにおけるクラウドサービスの有効性		
06	最終段落の、無償、安価なクラウドサービスにおけるセキュリティ機能の制限や、利用状況等のデータをマーケティング情報として活用される恐れがあるといった記載については、セキュリティ観点の内容のため、(2)の③よりも、次の(3)テレワークへのクラウドサービス活用の考慮事項において注意喚起すべきと考えます。 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、該当箇所の記載位置を変更します。	有
	第２章　３．クラウドサービスの活用の考え方　(3) テレワークへのクラウドサービス活用の考慮事項		
07	テレワーク下では、つい気が緩んで、あるいは他人の目という抑止力がないことで、気軽に個人でクラウドサービスを使い始めることが考えられます。許可されていないPCやスマートフォンを業務に活用したり、許可されていないクラウドサービスを活用したりするシャドーITについて記載いただきたいと考えます。 クラウドサービス利用時のルール徹底（申請/許可制）を明記すべきです。 【株式会社ブロードバンドセキュリティ】	御意見は「クラウドサービス活用」に関する考慮事項ではないこと、及びシャドーITに関しては第５章２．において記載済みであることから、原案通りとします。	無
	第２章　３．クラウドサービスの活用の考え方　(3) テレワークへのクラウドサービス活用の考慮事項		
08	どのようにすればクラウドサービスの信頼性を確認できるのか具体的に書かれていません。認証取得状況や、セキュリティポリシーの確認、ホワイトペーパーなどで確認する等の具体的な確認方法について明記すべきです。 【株式会社ブロードバンドセキュリティ】	クラウドサービスの選定に関する具体的な確認方法については第５章１．において第三者認証等による方法を記載済みであることから、原案通りとします。	無
	第２章　３．クラウドサービスの活用の考え方　(3) テレワークへのクラウドサービス活用の考慮事項		
09	クラウドサービスで提供されるセキュリティコンポーネントや監視、アラートツールが適切に使用されていないことによるセキュリティ事故が増加しています。したがって、それらの積極的な活用と適正な維持についても言及することが求められます。特に、クラウドサービスの改定等により機能の追加、変更が生じた場合は、必ずリリースノートを確認し、影響範囲を認識の上、各種コンポーネントの設定を適切に見直すといった内容を明記すべきです。 【株式会社ブロードバンドセキュリティ】	アクセス権限等の確認の必要性については第５章９．に記載済みであることから、第２章は、原案通りとします。 なお、第５章９．に記載済みの部分において、御意見を踏まえ、継続的な設定見直し等について追記します。	有

	第２章　４．ゼロトラストセキュリティの考え方　全般		
10	P22　修正依頼 現在：内部ネットワークにも脅威が存在しうる 修正後：内部ネットワークにも脅威が存在する 修正理由：「存在しうる」ではあくまで可能性を示唆しているにすぎず表現として弱い。また、ゼロトラストセキュリティの「決して信頼せず」とも意味に齟齬がある。明確に「存在する」とすることで、ゼロトラストセキュリティの考え方に沿う内容となる。 P22　修正依頼 現在：区別せず機器単位で、 修正後：区別せずユーザ、機器、データ、サービスなどの最小リソース単位で 修正理由：ゼロトラストセキュリティの考え方は、ネットワークから機器という形で粒度を細かすることではない。ユーザ、機器、データ、サービスなどすべてをリソースとして考え保護するものである。機器に限った表現は好ましくない。また、仮想化技術などを考慮すると、機器よりも細かい単位でのセキュリティ・制御・保護も必要なため、修正内容のような表現のほうが好ましい。 P22　修正依頼 現在：強固なユーザ認証と厳密なアクセス管理 修正後：強固なユーザ認証と厳密なアクセス管理及び認証・認可情報の一元管理 修正理由：強固なユーザ認証と厳密なアクセス管理を行うには、その前提として認証情報含むユーザ情報とアクセス管理を実施するためのアクセス権限情報が適切に管理されている必要がある。したがって、「及び認証・認可情報の一元管理」を追加した。 P22　修正依頼 現在：データ、機器等の資源 修正後：ユーザ、機器、データ、サービス等の資源 修正理由：前述の通り、ユーザやサービスも資源（リソース）として考えるのがゼロトラストセキュリティの考え方であるので、追加した。 P23　修正依頼 現在：一般従業員のアクセス権限や、対策に不備のあるPC等に対するアクセス権限については必要最小限に制限するといった動的なアクセス権制御による対策が重要になっています。 修正後：データやサービスへのアクセスを必要最小限かつ正当な権限を有する者のみに制限し、対策に不備のあるPCや不審な振る舞いのユーザ等によるアクセスついてはブロックするなどの静的および動的なアクセス権制御による対策が重要になっています。 修正理由：「一般従業員のアクセス権限」と「対策に不備のあるPC等に対するアクセス権限」だけを必要最小限に制限するという記述は誤解を生む。ここで言及されている、水平展開型の攻撃（ラテラルムーブメント）においては、特権ユーザや管理者ユーザなどの権限奪取および奪取した権限が必要以上に大きい（例えば関係ないファイルも暗号化できてしまうなど）ことのほうが問題であり、攻撃で利用される。 　また、「一般従業員のアクセス権限」（静的に割り当てるもの）と「対策に不備のあるPC等に対するアクセス権限」（コンテキスト・状況に応じて動的に変わるべきもの）をまとめて「動的なアクセス権制御」とするのは行き過ぎである。 　したがって、最小権限の原則（業務に必要最低限な権限しか割り当てないという考え方）と、コンテキスト・状況の変化に応じた動的なアクセス制御という形で修正を記載した。 P23　修正依頼 現在：データや機器を防御の中心 修正後：ユーザ、機器、データ、サービスなどの資源を防御の中心 修正理由：前述のように、データと機器だけが資源（リソース）ではない。また防御する対象として、ユーザやサービスなども明示するべきである。さらには、その前で言及されている「クラウドサービスの普及や自己所有の端末を業務に用いるBYOD	１点目については、内部ネットワークに脅威が存在するか否かは環境による（例：インターネット隔離環境等）ため、断定することは避ける趣旨から、原案通りとします。 ２点目については、御意見を踏まえ、機器（ハードウェア）に限る趣旨ではないことを明確にするため、「データ」を追記します。 ３点目については、ゼロトラストセキュリティの直接的な特徴ではないことから、原案通りとします。 ４点目については、ゼロトラストセキュリティの考え方には諸説あり、本ガイドラインは具体的な立場を説明しきるものではないことから、原案通りとします。 ５点目については、御意見を踏まえ、最小権限の原則と、動的アクセス権制御の双方について記載していることが明確な表現となるよう修正します。 ６点目については、上述の理由を総合し、「データや機器等」との表現に修正します。	有

	の活用等も進んで」というIT環境の変化を背景とすると、機器（スマホもPCもサーバもスイッチも機器である）として、サーバも含む形で表現するよりも、デバイス（スマホやPCなどコンピューティングリソースとしての最小単位のイメージ）として表現したほうが好ましい。物理サーバ単位で防御するのは、仮想化やクラウド技術が普及いた現在ではあまり意味をなさない（もう少し細かい単位で制御しないと無意味）。 【個人14】		
	第２章　４．ゼロトラストセキュリティの考え方　(1) ゼロトラストセキュリティとは		
11	二段落目の末尾に「機器単位のセキュリティ強化をうたった考え方を指します。」とありますが、ゼロトラストの考え方の根底にはクラウドシフトがあるため、「強固な利用者認証と厳密なアクセス管理による機器単位のセキュリティ強化」と記載いただきたいです。 【株式会社ブロードバンドセキュリティ】	ゼロトラストセキュリティの特徴として「強固な利用者認証と厳密なアクセス管理」を記載済みであることから、原案通りとします。	無
	第３章　全体　／　第３章　１．テレワーク方式の選定　(2) テレワーク方式の特性比較		
12	（意見） テレワークを実現するための方式選択（24頁）では、「アプリケーション」、「ネットワーク」、「クライアント」の３つの分野で分類すること提案する。すべての組み合わせはないものの、オンプレミスかクラウドか、VPNかゼロトラストか、BYODもできるPC/モバイルか各種技術で強化したものか、といった大括りで選択させ、その上でその他の技術の選択を階層的に分類しシンプルに理解させるべきである。 （理由） 第２章で、クラウドとゼロトラストを全面的に解説していることは高く評価するものの、第３章全体で、テレワーク方式として掲げた７項目のうちクラウドは一つ、ゼロトラストは方式としては取り上げていない。 また、この７つの分類はテレワークに関連する技術の羅列に留まっており、テレワークの方式を決めるための分類としては適切なものにはなっていない。一案として、テレワークを実現するための方式選択では、「アプリケーション」、「ネットワーク」、「クライアント」の３つの分野で分類し、全ての組み合わせはないものの、オンプレミスかクラウドか、VPNかゼロトラストか、BYODもできるPC/モバイルか各種技術で強化したものか、といった大括りで選択させ、その上でその他の技術の選択を階層的に分類しシンプルに理解させることが適切と考えられる。 27頁の特性比較では、安易に考えるとスタンドアロンが一番安全と判断したり、他の方式を選択して実はクラウドを考慮していないということが起きる可能性が想定される。上記のような考え方をすると26頁のフローチャートももっと分かりやすいものになると思われる。 【一般社団法人新経済連盟事務局】	ゼロトラストセキュリティはセキュリティ確保のための考え方であり、テレワーク方式の一つと考えることは適当ではないため、原案通りとします。 なお、テレワーク方式として「VPN方式」は記載済みであり、BYOD利用についても各方式の細分として記載済みです。	無
	第３章　１．テレワーク方式の選定　(2) テレワーク方式の特性比較		
13	注釈に ″端末やクラウド上でのデータ保存に関する制限の容易性や、テレワーク端末やテレワーク関連設備へのシステムアップデートの強制適用の容易性等を示します。″ との記載があるが、″どの方式が一番安全なのか（情報漏洩の可能性が低いのか）/コントロールしやすいのか″という視点を加味すべきかと思われます。 ″どの方式が一番安全なのか″と″コスト″　が　テレワークシステム導入起案時に　経営者から起案者　にまず聞かれることが多いと思うため、非常に重要な視点かと思います。 上記視点で７つの方式を検討すると、下記が妥当と考えます。 S：(4)セキュアコンテナ　(5)セキュアブラウザ 理由：・管理者がユーザに与える操作範囲を制限することが容易（(5)セキュアブラウザであればブラウザしか操作できない）なため、不正アクセスされてもＯＳ設定を変更できない。 ・不正アプリケーションをダウンロードしてもShell操作などを不可能にしておけば実行することができないため、感染リスクが	具体的にどのテレワーク方式が「安全」であるのかについては、管理主体の技術力や業務内容に依存するため一概に示すことはできないことから、原案通りとします。	無

	低い A：(1)VPN (2)リモートデスクトップ　(3)仮想デスクトップ 理由：(4)(5)よりもユーザ操作の自由度が高く、設定不備などで管理者の想定しない操作、不正プログラムの実行などが可能になってしまうリスクがある。 B：(6)クラウドサービス 理由：データ管理が別途必要だが、ノウハウの詰まったデザインパターンが確立してきており、セキュリティ専門者不在の会社であれば自営よりも高セキュリティ運用できる可能性が高い。 D：(7)スタンドアロン 理由：持ち出されている間はシステム上で統制できない "セキュリティ統制の容易性"にまとめるのではなく、別項目として　システムとしての安全性　のようなものを作っても良いかと思います。 【個人07】		
	第３章　１．テレワーク方式の選定　(2) テレワーク方式の特性比較		
14	p27 テレワーク方式の特性比較について - セキュリティ上の具体的なデメリットを表示した方がわかりやすいと思います - 「標準よりも」と記載がありますが、何が「標準」になりますが。 - S～Dの表示の仕方を変更した方がいいと思います。「優れている、劣っている」いう表現は、適切ではないと思います。メリットとデメリットを考えて、企業や組織がテレワーク方式を選べるようにした方がいいと思います。 【個人09】	テレワーク方式の特性比較については、方式を検討する際の一助とするため、一覧性を重視した記載としており、記載分量に限りがあることから、原案通りとします。 なお、各方式の特徴等の詳細については、第３章２．に記載済みです。	無
	第３章　２．テレワーク方式の詳細解説と考慮事項　(1) VPN方式		
15	VPN環境は、昨今攻撃のターゲットになっていることから、利用者だけでなくインフラを提供する立ち位置においても対策を記載しておく必要があると考えます。例えば、VPN装置のセキュリティ対策、外部からのアクセスを許容する内部環境のアクセス制御、利用時の認証に多要素認証を導入といった内容を含めることが必要です。 【株式会社ブロードバンドセキュリティ】	いずれの対策についても、VPN機器だけに限らず、インターネットに接続された機器・システム全般に言える話であり、第５章に記載済みであることから、原案通りとします。	無
	第３章　２．テレワーク方式の詳細解説と考慮事項　(4) セキュアコンテナ方式 **(5) セキュアブラウザ方式：セキュリティ考慮事項**		
16	セキュリティ考慮事項に記載されている　作業が制限される、というのは　導入前の仕様検討時に注意することであり、セキュリティ事項として記載されていることに違和感があります。 また、別の意見でも記載しましたが、作業が限定される、ということはデメリットであると同時に　管理者が使わせたい機能だけを提供できる（使わせたくない機能を制限できる）というメリットでもあると思います。 ユーザが実行ファイルをダウンロードしても実行できない、というのは　VDIなどでもできないメリットだと思います。 【個人08】	「セキュリティ考慮事項」の項目には、各方式特有のセキュリティ上の留意点のほか、各方式において特に留意すべき考慮事項について記載していることから、項目名を「考慮事項」とし、関連する記載を修正します。 また、御意見を踏まえ、利用アプリケーションが制限される点について、メリットとしても追記します。 なお、第３章について記載内容が明確となるよう全面的に見直しを図っています。	有
	第３章　２．テレワーク方式の詳細解説と考慮事項　(5) セキュアブラウザ方式		
17	P42のセキュアブラウザ方式のメリットとして「セキュアブラウザ上で動作させるアプリケーションは、手元端末内にインストールされたものを利用するため、インターネットの通信速度の影響を受けにくい」とありますが、動作させるアプリケーションは社内システムやクラウドサービスで提供されるアプリケーションソフトウェア、つまりはWebアプリケーションであると思われます。 手元端末内にインストールされたセキュアブラウザにおいて処理するデータは、社内システムやクラウドサービスから提供されるものであり、通信環境の影響を受けやすいと思われます。	御意見を踏まえ、リモートデスクトップ方式等に比べてインターネットの通信速度の影響が小さいという旨の表現に修正します。	有

	【個人11】		
	第３章　３．テレワーク方式の併用　(1) ローカルブレイクアウトとの併用		
18	「VPN方式は基本的に端末へのデータを許容しているため、データの保存ができないよう制限を設けた方が好ましいクラウドサービスはありません」という表現は、「VPN方式は基本的に端末へのデータ保存を許容しているため、クラウドサービス側でデータ保存を制限することによるセキュリティ上のリスク低減効果は期待できません。」とした方が明確になると考えます。 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、記載内容を明確化するよう修正します。	有
	第４章		
19	「第４章 テレワークセキュリティ対策一覧」の各対策の中には、テレワーク方式によっては実施不要のものもあると思います。７種類のテレワーク方式とセキュリティ対策のマトリクスで対策の要否が示されていると自社環境で何をする必要があるかが分かりやすくなると思います。 【個人06】	第４章の対策については、テレワーク方式によらず共通的に実施すべきものとして整理し、テレワーク方式に固有のセキュリティ考慮事項については第３章に記載しているため、原案通りとします。 なお、セキュリティ対策の具体化に当たっては、テレワークの実施形態により個別に異なるため、テレワーク実施者それぞれにおいて適切に判断されるべきと考えます。	無
	第５章　１．ガバナンス・リスク管理		
20	セキュリティポリシーや関連規程の見直し時に、「テレワーク勤務者に周知」するとなっていますが、「会社や組織全体」に周知した方がいいと思います。 【個人09】	第２章において、経営者や管理者についても、テレワークを実施する立場になった場合は「テレワーク勤務者」として取り扱う旨を記載していることから、原案通りとします。 なお、「会社や組織全体」とした場合、特に誰に対して訴求したい事項なのかが不明確になると考えます。	無
	第５章　３．脆弱性管理　＜セキュリティアップデートの実施＞		
21	2020年４月頃からテレワークの実施が急増した結果、その場しのぎの突貫作業で作られたテレワーク環境が2021年現在も放置されている。 最も多いパターンは急遽テレワーク用のリモートデスクトップを行うための端末を用意した結果、管理者権限の縛りをあまりにもきつくし過ぎたためOSのセキュリティパッチの適応が労働者自身の自宅にある回線では不可能で、企業に出社し社内LANに接続しないと出来ないような環境が作られている。 また、同じ原因で今日ではほぼ必須となったセキュリティ対策ソフト（ウイルスバスター等）のアップデートがリモートワークを自宅で実施する場合に不可能になったりしている。 前者は適切な権限設定が必要であるが、後者は社内LANのみを前提としたセキュリティ対策ソフトではなくスタンドアロンで稼働出来るセキュリティ対策ソフトの導入をさせる必要がある。 国内にセキュリティパッチの適応されていない端末が数十万単位で残存している可能性から何らかの対策を行わなければならない。 【個人01】	OSやソフトウェアのアップデートの必要性については記載済みであることから、原案通りとします。 なお、具体的なセキュリティアップデートの方法については、システム構成や管理方法により異なることから、一概に記載することは困難です。	無
	第５章　４．特権管理		
22	特権アカウントの操作等のログに関する記載がありません。不正アクセスを受けることで甚大な被害につながる恐れが高い特権アカウントは、認証履歴だけでなく、実行された操作についてもログを取得し、レビューする運用についても言及いただきたいと考えます。 【株式会社ブロードバンドセキュリティ】	特権ID（特権アカウント）に関するログレビューの重要性については、第５章10. において記載済みのため、第５章４. については、原案通りとします。 なお、特権IDに関するログについて、レビューだけでなく取得する必要性についても明確となるよう、第５章10.	有

		の記載を修正します。	
	第５章　５．データ保護　＜紙への印刷に関する統制＞		
23	データの印刷に関する内容が記載されておりません。テレワーク環境化で、コンビニエンスストア等の複合機、あるいは印刷のクラウドサービスを自己の判断で利用してしまうケースがあり、思わぬ情報漏えいの原因となりかねません。したがって、データの取り扱いの一つとして、紙への印刷に関する統制についても記載が必要です。 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、紙文書に対する情報の取扱方法について追記します。	有
	第５章　５．データ保護　＜機密性を有する情報の管理＞		
24	管理者E-3「テレワークで利用する機密性を有する情報について、保存場所を特定し、管理を行う。」において「管理」とは何を指すのかが曖昧ではないか。 情報が組織として特定できない場所に保管されることを防止する方策、及び何を意図してどのような「管理」を行うのかを具体的に補足していただきたい。また、4章の解説において明示いただきたい。（第4章においても当該の対策についての解説は見当たらなかった） 【個人03】	御意見を踏まえ、「管理する」という表現について、「機密性を有する情報を特定し、保存場所を把握する」という表現に内包されることから、修正します。	有
	第５章　５．データ保護　＜保存データの暗号化＞		
25	■意見１ １（１）該当箇所 ●対象ページ62ページ ●第5版(案)の内容　管理者Ｅ-８　発展対策 テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。 １（２）意見の内容 下記内容に変更いただけるよう、ご検討をお願い申し上げます。 ●変更案　発展対策 テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化やファイル単位の暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。 ●変更内容　「内蔵されるHDDやSSDの記録媒体レベルでの暗号化」の後に「やファイル単位の暗号化」を追加 ●変更理由　後述されている77ページの＜記録媒体の暗号化・廃棄＞の【管理者Ｅ-８】に記載されている「ファイルを強制的に暗号化」するという記載内容に合わせた方がよいと考えます。 ■意見２ ２（１）該当箇所 ●対象ページ：76ページ ●第5版(案)の内容：管理者Ｅ-８　発展対策 テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。 ２（２）意見の内容 下記内容に変更いただけるよう、ご検討をお願い申し上げます。 ●変更案　管理者Ｅ-８　発展対策 テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化やファイル単位の暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。 ●変更内容　「内蔵されるHDDやSSDの記録媒体レベルでの暗号化」の後に「やファイル単位の暗号化」を追加 ●変更理由　後述されている77ページの＜記録媒体の暗号化・廃棄＞の【管理者Ｅ-８】に記載されている「フ	意見１から意見３までについては、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を求めている趣旨は、端末の紛失・盗難時に記録媒体が取り外され、データが不正に解読されることをシステム的に防止するためであり、利用者によるファイル単位の暗号化についてはこの趣旨に合わないことから、原案通りとします。 意見４については、「文書管理システム」は「ファイル暗号化ソリューション」と同義で使用していますが、御意見を踏まえ記載を明確化するよう修正します。	有

	ファイルを強制的に暗号化」するという記載内容に合わせた方がよいと考えます。 ■意見３ ３（１）該当箇所 ●対象ページ：77ページ ●第5版(案)の内容：＜記録媒体の暗号化・廃棄＞ ３（２）意見の内容 下記内容に変更いただけるよう、ご検討をお願い申し上げます。 ●変更案　＜端末および記録媒体のデータ暗号化・廃棄＞ ●変更内容　「記録媒体」を「端末および記録媒体」に変更し、「暗号化」を「データ暗号化」に変更 ●変更理由　暗号化される対象は、記録媒体に限らず、テレワーク端末内の記憶媒体または、それに保存されているファイルなどのデータであるという観点をタイトルに明記した方がよいと考えます。 ■意見４ ４（１）該当箇所 ●対象ページ：77ページ ●第5版(案)の内容： ○ 端末管理ツールを導入し、テレワーク端末やUSBメモリ等の記録媒体の自動暗号化を行ったり、文書管理システムでファイルを強制的に暗号化して保存したりすることで、テレワーク勤務者が意図的に設定を変更できないようにすることも重要です。【管理者Ｅ-８】 ４（２）意見の内容 下記内容に変更いただけるよう、ご検討をお願い申し上げます。 ●変更案 ○ 端末管理ツールを導入し、テレワーク端末やUSBメモリ等の記録媒体の自動暗号化を行ったり、文書管理システムやファイル暗号化ソリューションなどでファイルを強制的に暗号化して保存したりすることで、テレワーク勤務者が意図的に設定を変更できないようにすることも重要です。【管理者Ｅ-８】 ●変更内容　「文書管理システム」の後に「やファイル暗号化ソリューションなどで」を追加 ●変更理由　ファイルを強制的に暗号化するシステムは、文書管理システムに限らず、ファイル暗号化機能を持つ他のソリューションも存在すると考えます。 【匿名02】		
	第５章　６．マルウェア対策　＜EDR＞		
26	（「テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、隔離やシステム停止といった迅速な対応が行えるようにする。」との記載部分） （意見内容） 当該部分について「テレワーク端末にEDR（Endpoint Detection and Response）ソリューションを導入し、未知のマルウェアを含めた不審な挙動の検知及びOSやドライバなどのシステムの動作及びファイルやレジストリへの読み書きに関連するログの取得を行って、疑義端末の隔離やシステム停止及び検証や復旧作業といった迅速な対応が行えるようにする。」との変更を提案します。 （理由） EDRの効果は、一般的なアプリケーションに関連するログだけではなく、OSやドライバなどのシステムの動作及びファイルやレジストリへの読み書きに関連するログを取得することで、悪意あるソフトウェアによる秘匿を回避し、併せてこれらのログを取得して分析し続けることによって（１）疑義端末を早期に発見し当該疑義端末の隔離やシステム停止を自動的に行うこと、及び（２）当該ログを利用して過去にさかのぼったインシデント分析を可能とすることによりインシデント発生後の検証や復旧作業を迅速化すること、が両立することにあります。	御意見を踏まえ、隔離やシステム停止だけでなく検証や復旧作業までの対応も考慮するため、対策事項について、「隔離やシステム停止といった迅速な対応が行えるように」という部分を「マルウェア感染後の対応を迅速に行えるように」と修正します。 また、EDRに関してはコラムにもその詳細を記載していますが、御意見を踏まえその内容も修正します。	有

	そのため「OSやドライバなどのシステムの動作及びファイルやレジストリへの読み書きに関連するログ」との文言でEDRの効果を得るために必要なログの種類を明示し、各組織に周知する必要があります。また、原案はEDRによって得られる（１）及び（２）の効果のうち（１）の効果を明示しているため（２）の効果を明示することを提案します。 【ヴイエムウェア株式会社】		
	第５章　６．マルウェア対策　＜EDR＞		
27	（「EDRを導入することで、未知のマルウェアを含めた不審な挙動の検知や、検知した情報に基づく自動的な対応が可能になります。」との記載部分） （意見内容） 当該部分について「EDRを導入しOSやドライバなどのシステムの動作及びファイルやレジストリへの読み書きに関連するログを取得することで、未知のマルウェアを含めた不審な挙動の検知や、検知した情報に基づく自動的な疑義端末の隔離やシステム停止及び検証や復旧作業といった迅速な対応が可能になります。」との変更を提案します。 （理由） EDRの特徴である自動的な対応を行うためには、OSやドライバなどのシステムの動作及びファイルやレジストリへの読み書きに関連するログを取得することが必要です。EDRの如く称しつつも自動的な対応に十分でない一部のログのみを取得するケースが散見されることから、本ガイドラインによって各組織にEDRの効果を得るために取得する必要があるログの種類を明示し、その周知を図るため、変更を提案します。 【ヴイエムウェア株式会社】	御意見を踏まえ、EDRに関するコラムにおいて、取得・分析するログに関する記載を脚注として追記します。	有
	第５章　７．通信の保護・暗号化　＜エンドツーエンド暗号化＞		
28	管理者E-2において「エンドツーエンドで常時暗号化されているもののみ利用を許可する」について、その確認方法を明示または例示できないか。サービスやアプリにおいて、「エンドツーエンドで常時暗号化」されているか否かを自ら確認することは、提供・開発事業者への確認も含めて至難ではないかとも思われる。 【個人04】	御意見を踏まえ、エンドツーエンドで暗号化が担保されたサービスの参考となるよう、米国国家安全保障局（NSA）が公表している資料を追記します。 なお、エンドツーエンドでの暗号化について、個別に示すことは困難なことから、サービス利用者自身において、サービス内容をよく確認したり、必要に応じてサービス提供事業者に確認したりすることが必要です。	有
	第５章　８．アカウント・認証管理		
29	P83　修正依頼　＜適切な管理ルールの設定＞内の記載 現在：利用者認証に一定回数した場合 修正後：利用者認証に一定回数失敗した場合 修正理由：たんなる記載ミス、コピペミス。「失敗」を書き忘れている。 【個人14】	御意見のとおり修正します。	有
	第５章　８．アカウント・認証管理　【コラム】パスワードの管理方法		
30	マスターパスワードの活用という内容で、一定の固定値と可変値を組み合わせる方式が解説されています。この方法を用いても、万が一固定値部分のマスターパスワードが漏えいした場合は、総当たり攻撃によるパスワード特定を受けるリスクが高まることになります。また、本ガイドラインにより適切でない考え方が浸透してしまう恐れがあることから記載すべきでないと考えます。他例として記載されているパスフレーズあるいは、多要素認証を積極的に用いる方向にすることがより本質的なセキュリティ強化策となります。 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、マスターパスワードを記載する趣旨について脚注で追記します。	有
	第５章　９．アクセス制御・認可　／　第６章　３．アクセス権限の設定不備		

31	P63、P86、P96 修正依頼　管理者I-3 基本対策 現在：データに対するアクセス制御に際して、保存するフォルダのアクセス権限設定やファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御する。 修正後：データに対するアクセス制御に際して、保存するフォルダのアクセス権限設定やファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御する。また、アクセス制御設定にミスや漏れ、消し忘れなどがないか、余計な権限を付与してないか等を定期的にチェックして確認する。 修正理由：前述の通り、アクセス権限設定は付与するときでなく見直しも必要なため。 P96　修正依頼 現在：アクセス権限の適切な設定が行われていない場合、不正アクセスや情報漏えいにつながるおそれがあります。メンテナンス作業等でアクセス権限を変更する際は、不必要な許可ルールが誤って追加されていないか、また、既に必要のなくなった許可ルールが残留していないか等の観点で入念にチェックを行い、必要最小限のアクセス権限設定が行われるようにすることが重要です。 修正後：アクセス権限の適切な管理（付与・見直し・更新・削除）が行われていない場合、不正アクセスや情報漏えいにつながるおそれがあります。メンテナンス作業等でアクセス権限を変更する際は、不必要な許可ルールが誤って追加されていないか、また、既に必要のなくなった許可ルールが残留していないか等の観点で入念にチェックを行い、必要最小限のアクセス権限設定が行われるようにすることが重要です。また定期的に設定内容をチェックし設定ミスや更新・削除忘れなどがないかを確認することも重要です。 修正理由：「アクセス権限の適切な設定」とすると、アクセス権限を”与える”ときに適切に設定すべきと理解される恐れがある。アクセス権を与えないとシステムが利用できないので、アクセス権限の付与（申請・承認なども含む）は早く処理を終わらせるというプレッシャーの中で行われるため、怠慢（必要性を判断せず承認）、ミス（本来与えるべきよりも大きな権限をとりあえず与える）などが発生しがちである。また、システムが使えないという不都合な状態となるため、アクセス権の”付与”作業が忘れられることはない。（忘れられるとシステムにアクセスしたい人が困る。）。一方、アクセス権の見直し・更新・削除は行わなくても、一義的に困る人がいないので放置されがちである。この放置がセキュリティ上の脆弱性となる。”付与”の際に適切に実施することが大事なのではなく、アクセス権限のライフサイクル全体において適切に管理することが大事なので、修正案のように記載した。また、監査的な意味で定期的な設定内容のチェック（アクセス権限の棚卸）も追記した。 全体： 資料全体を通して、設定や制御に関する記載は充実しているが、見直しやチェック、確認、監査などの視点が不足している印象を受けた。特に今回のパンデミックのように想定しない自体が発生した場合には、「まずはテレワーク実施できる状態にする」ことが優先されるため、一時的にはセキュリティ上は脆弱な状態が発生する。例えば、とりあえず管理者権限与えた。とりあえず、全ユーザ同じパスワードを設定した。多要素認証は導入しないでVPN機器利用に踏み切った。などは容易に想像できる。それ自体はビジネスの継続のためには致し方ない部分もあり、一時的にはリスク許容・受容することも理解はできる。 一方で、”一時的”として、許容したリスクが放置される場合も多い。実は設定の不備などよりも、リスクを放置してしまうという情報セキュリティ体制やガバナンスの不備などのほうが結果としてリスクを大きくしてしまうことになるということをどこかに記載していただきたい。 そのうえで、個別の対策に関しても、見直しやチェック、確認、監査などの視点を踏まえて追記・修正などをご検討いただきたい。 非常に丁寧に読者を想定して記載されているこの資料であるが、テレワーク導入時に一度、セキュリティチェックのために一度といった利用のされ方を想定されいるのではなく、定期的な見直しの際にも活用できるものとなっているので、その部分を強調するためにも、見直しやチェック、確認、監査などの視点も強調してもらいたい。 最後に執筆頂いた方々、とてもいい資料をありがとうございます。 【個人14】	御意見を踏まえ、第５章においてアクセス権限設定等の継続的な見直しについて解説を追記するとともに、第６章において「設定が行われていない場合」を「設定やその管理が継続的に行われていない場合」とし、権限付与作業のみに限られない趣旨を明確するよう修正します。	有
	第５章　13. 教育		
32	テレワーク等オフィス外での業務には、情報漏えいや端末のウイルス感染などリスクが潜みます。テレワーク	セキュリティ対策の実施状況の把握に関しては記載済み	有

	におけるセキュリティリスクを把握し、その低減を目的とした教育を行なう必要があると考えます。 教育を効果的に行うためには、事前にテレワーク勤務者に対してセキュリティ意識調査を行うことが推奨されます。テレワーク勤務者のセキュリティに対する理解度/認識状況を把握することで、より効果的な教育が可能となります。また、調査を通じて、企業のセキュリティルールの不足事項の有無も可視化することができます。 【株式会社ブロードバンドセキュリティ】	でしたが、研修・周知の実施と混在した記載となっていたため、記載内容を整理し、修正します。	
	第５章　13. 教育		
33	テレワークの場合、オフィスに出社して業務を行なうときに比べ、他の社員の目がなくなり、私物PCやHDDが存在しやすくなるなど、特に物理的なセキュリティ対策がとりにくくなっています。内部不正を起こす意思を持つ人が、悪意ある行動をとれないよう、スキを見せない（「機会」を与えない）ためには、内部不正を防止する技術的対策が重要ですが、限界があります。内部不正の発生を防ぐため、「動機」や「正当化」を低減する教育や啓発の実施が必要です。 【株式会社ブロードバンドセキュリティ】	セキュリティ教育に関連して、内部不正対策に関する教育についても重要であることから、脚注により追記します。	有
	用語集　シンクライアント		
34	シンクライアント専用端末も存在するため、以下の説明のほうがより適切だと考えます。 「利用者のクライアント端末に必要最小限の処理をさせ、ほとんどの処理をサーバ側に集中させたシステムアーキテクチャ全般のこと。または、そのようなシステムアーキテクチャで使われるように機能を絞り込んだ専用のクライアント端末のことをいう場合もある。」 【株式会社ブロードバンドセキュリティ】	御意見を踏まえ、より明確かつ簡易な表現に修正します。	有
	全般		
35	「テレワーク」だと「テレワ」の段階で「テレルワ（照れるわ）」と聞き間違いをするので、「リモートワーク」を使ってほしいです。 【個人05】	政府内において「テレワーク」という表現が一般的であること（例えば厚生労働省においては「テレワークの適切な導入及び実施の推進のためのガイドライン」を策定しています。）から、原案通りとします。 なお、米国NIST等の海外機関においても「telework」を一般的に用いているものと認識しています。	無
	全般		
36	PPAP対策について 会社員です。 パスワード付き圧縮ファイルを禁止しても、ファイル共有サービスのURLとパスワードを同じメールで送られたりしているので、セキュリティの機密性が保たれていないケースが身近でも起きております。 しかも、先様が客先であるなど、問題を指摘しずらい場合があります。 添付ファイルにパスワードをつけるのも、ファイル共有サービスを利用するのも、情報漏洩対策としての機密性が重要になりますので、その目的を果たせるように、総務省様からも呼びかけをぜひお願い申し上げます。 【個人10】	いわゆるPPAPについては、原案においても第２章３．(1)中の注釈において「セキュリティ対策としての効果が疑問視されている状態である」と記載しておりましたが、御意見を踏まえ、内容を追記した上でコラム（第５章７．内）として記載します。	有
	全般		
37	記載が無かったが、記載を行うべき事について、記述しておく。 電子メールについては、ISP等が電子メールのTLSによる保護（SMTPoverTLS、STARTTLS）に対応しているものを用いる事が重要である事について、記述されたい。そうでないと、使用しているISP等の間で平文で電子メールの送受信がされてしまう（情報漏洩してしまう事態である。）。（利用者とその利用者が契約しているISP等のサーバとの通信のSMTP、POPのみがTLSで保護されているだけの事も多いので注意が必要である。Gmailなどからその ISP等の事業者のメールサーバがTLSでの保護に対応しているかどうか確認を行ってみる事が推奨される。）	御意見を踏まえ、POP/SMTP over TLS等の重要性について追記します。	有

	その事についての注意喚起を行い（※1)、インターネット上の他のメールサーバとの間で、TLSによる保護が行われた形での電子メールの送受信が可能なISP等の事業者を選ぶ事が望ましい旨の記述を行うようにしていただきたい。 また、送信者についての保証と内容の正当性の保証のために、電子署名の利用を励行するような記述を行っていただきたい。 電子メールの利活用については、ICT技術の利用に際して重要なものであるはずであるが、総務省自身が疎かにしていたりもするように、日本の社会において、電子メールについてのそのセキュリティについては、何故か、依然として、疎かな状況である。 Webページにおいて、アカウントや取引等に関係する重要な通信がなされる場合は、SSL/TLS（今日ではほぼTLSの利用のみであろうが。）で保護されたHTTPSプロトコルを用いるように、事務に関係する電子メールについては、TLSで保護されたSMTPプロトコルの通信（SMTPoverTLS、STARTTLS）で行われるべきであるが、総務省は、自身の組織についての戒めの意も含めて、電子メールについてのTLSでの保護の重要性について、社会に注意喚起を行っていただきたい。 本当に、この様なガイドラインにおいて、電子メールの保護についての重要性が示されていないのは、困った事なのであるが、国は、個人情報保護・業務重要情報保護・サイバーセキュリティについての保護を、本当に、事業者に行わせたいのであれば、電子メールについての保護のために、TLSでの保護（SMTPoverTLS、STARTTLS）が基本として常時行われる様な事業者を選択するように、推奨されたい。（その様な推奨の社会への提示が行われる事により、日本国内のISP等事業者も、電子メールの役務について、TLSでの保護を行っていく傾向が出てくるであろう。総務省は、牽引役としての役割がある事を自覚し、日本のICT分野周辺が健全に発展していくよう、電子メールについての保護が行われる重要性について、ガイドライン等で都度示していっていただきたい（TLSによる電子メールの保護が一般的でない現状、都度、その重要性を提示する事が、重要かつ必要である。）。） ※1 「Webページ等の閲覧に用いられているHTTPプロトコルは平文でのやり取りがなされるものであり、重要な通信はSSL/TLSによる保護がなされたHTTPSプロトコルで行われる事が盗聴・改竄対策として重要となるが、電子メールの送信に用いられているSMTPプロトコルもまた平文でのやり取りがなされるものであり、個人情報保護やサイバーセキュリティを考えると、HTTPSと同様に、電子メールは素のSMTPプロトコルをSMTPoverTLSやSTARTTLSの利用によってのTLSでの保護がなされた形での通信がなされるようにすべきである。」、等の記述によって。 【個人15】		
	全般		
38	全体的に「セキュリティ」という言葉が使用されていますが、「サイバーセキュリティ」もしくは「情報セキュリティ」とすべきではないでしょうか。 【個人09】	本ガイドラインにおいては、固有名詞等で用いる場合、及び一般的になじみが深い「情報セキュリティ関連規程」として使う場合以外は、原則として「セキュリティ」と表記を統一しています。 なお、一部に表記揺れがあったことから修正します。	有
	全般		
39	アプリケーションの記述で、アプリケーションが全てブラウザアクセスするとは限らないので、インストールが必要なソフトウェアと、利用するアプリケーションの定義を明確にしたほうがよいと思われます。 （例えば、テレワークでよく利用するMicrosoft Teamsはインストールするソフトウェアであり、バックエンドではWebアクセスするアプリケーションでもあります。） 【個人11】	本ガイドラインにおいて「アプリケーション」は、アプリケーションソフトウェアを指し、インストールの有無や、ブラウザアクセス利用の有無で線引きされるものではありません。 なお、一部にソフトウェア・OS・アプリケーションの用語の表記揺れがあったことから修正します。	有
	全般		
40	下記の通り、不自然な表現がありましたのでご報告いたします。 1. p.83、「＜適切な管理ルールの設定＞」の7行目 誤：利用者認証に一定回数した場合 正：利用者認証に一定回数失敗した場合 2. p.107、「(2)テレワークセキュリティへの示唆」の 4行目 誤：不適切な設定がないかを確認するしたり 正：不適切な設定がないかを確認したり 3. p.113、項目「ローカルブレイクアウト」	御意見のとおり修正します。	有

	誤：データセンターを介さずに、インターネットへの直接アクセスするネットワーク構成のこと。 正：データセンターを介さずに、インターネットに直接アクセスするネットワーク構成のこと。 なお、内容については第４版に比べて的確な構成であり、現状に即して情報が盛り込まれていると思います。 【個人02】		
	全般		
41	中小企業におけるテレワークのセキュリティ面からの実現性についてのコメントです。 インターネット回線を外部から引き込むにあたって、事故を防ぐ意味で工担免許保持者もしくは管理下にある者が工事することには賛成です。 事業所のルーターの交換、及び設定の変更には工担の免許が必要だと認識していますが、以下はそれが正しいとしてコメントします。 中小企業において、システム担当者に工担の資格を取らせるのは現実的ではありません。情報システムのプロではあっても、回線引き込み工事のプロではないので、小売業や卸問屋のシステム担当者に工担の資格を取らせるのは無理があります。 ここで、セキュリティの問題が発生した場合、ルーター機器の交換にも、セキュリティ設定の変更にも、毎回工担資格をもった業者に発注しなければなりません。次の工担試験を待つには長すぎますし、問題発生が深夜の場合、業者を呼ぶこともままならず、セキュリティ上の脆弱性を放置したままとなり、被害が拡大する可能性があります。 ACL1行更新するのにも業者を呼ばないといけないのかと考えると、非現実的です。 上記の問題に関して、工担免許なしで、どこまで対策が可能なのか、記載していただけないでしょうか？ 【個人13】	工事担任者を要しない工事は、電気通信事業法関係法令※で規定しているものであり、その解釈を記載することは本ガイドラインの趣旨と異なることから、原案通りとします。 ※工事担任者規則（昭和60年郵政省令第28号）第３条及び昭和60年郵政省告示第224号（工事担任者を要しない端末機器の接続の方式を定める件）	無
	全般		
42	テレワークを実施するにあたり、労務管理の観点から利用時間の制限について網羅すべきと考えます。 厚生労働省のテレワークにおける適切な労働管理のためのガイドラインでも、テレワークは労働者が使用者と離れた場所で勤務をするために相対的に使用者の管理の程度が弱くなる恐れがあることから、長時間労働を招く可能性を示唆しています。そこでテレワークにおける長時間労働を防ぐ手法の一つとしてシステムのアクセス制限を挙げています。 例えば深夜、休日はアクセスできないように設定することで長時間労働を防ぐことが有効になる観点からシステムのアクセス制限も機能として考慮すべき、と考えます。 【個人11】	本ガイドラインは、第１章３．に記載のとおり「テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針」として策定するもので、記載内容もこれに沿ったものとなっており、原案通りとします。	無
	全般		
43	僭越ながら、標記につきまして一切の対価なく一個人かつ一市民として御意見とお伺いを申し上げます。人々の生命、心身の健康、生活、尊厳、権利、プライバシー、個人情報等が守られ、人々が早期に救済されますよう、御検討のほど、よろしくお願いいたします。関連する様々な問題を解決、改善する一助になれば、幸いに存じます。 ◇　御提案事項１　テレワーク時の働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等の保護の明記のお願いとそのお伺い 本文では、主に、組織がその組織自身の情報資産を保護するために、特に、その組織で働く方に情報資産の取扱方法等について注意を喚起する趣旨で述べられた記載が多いように感じておりますが、テレワーク時の働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等の保護については、ほとんど全く触れられていないように存じます。相手の同意もなく、或いは、相手が嫌がっているのにもかかわらず、無遠慮にプライバシーに立ち入り過ぎること、個人情報等を収集すること等には、大きな問題があるのではないでしょうか。テレワーク時にプライバシーが侵害された方、テレワーク時に個人情報等が無断で同意もなく取得されてしまった方等にとっては、精神的苦痛、犯罪行為等の被害等も受ける恐れがあるのではないでしょうか。ハラスメント防止（セクシャルハラスメント、パワーハラスメント等）、安全配慮、犯罪防止等のため、各事業所の各組織で働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等を積極的に保護すべく取り組むことも重要ではないでしょうか。ハラスメント（セクシャルハラスメント、パワーハラスメ	本ガイドラインは、第１章３．に記載のとおり「テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針」として策定するもので、記載内容もこれに沿ったものとなっており、原案通りとします。 なお、例えば労務管理等については厚生労働省においては「テレワークの適切な導入及び実施の推進のためのガイドライン」を策定しています。 また、アクセシビリティの確保及び動画コンテンツに対する要望については、今後の参考とさせていただきます。	無

	ント等）の予防、防止等のため、組織で懸命に働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等が保護されるよう、働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等の保護が組織内で真正面に取り組まれるように、本文でも十分に記載すべきではないでしょうか。当ガイドラインとしては、テレワーク時の働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等のプライバシー、個人情報等もきちんと保護対象として明記し、どのような点に注意するか、その方法等について、詳説し、適切に保護されるとよいのではないでしょうか。 　例えば、テレワーク時のカメラ（ＰＣ、スマートフォン、デジタルカメラ、デジタルビデオカメラ等）での動画、写真等の撮影（不同意の無断撮影、不同意の無断録画、盗撮を含む。）、私物、オンライン会議時の自宅の部屋の風景、自宅のＰＣ等のＩＰアドレス、自宅で使用しているインターネット回線業者名等には、労働者、管理職、その御家族、その御関係者、求職者等のプライバシー情報、個人情報等も含まれる可能性がございます。退職後、異動後もテレワーク時のＩＰアドレス、動画、写真等、様々な個人情報、プライバシー情報等が期限の定めなく保管される恐れもございます。また、退職後、異動後も、そのテレワーク時の情報が悪用され、ハッキング等のサイバー攻撃、嫌がらせ、犯罪行為、報復等の被害を受ける恐れもございます。また、採用選考時には、引用文献１にあるように、「採用選考時に配慮すべき事項」等を含む様々な配慮を要する内容もあり、慎重に情報を取り扱う必要があると存じます。求職者、派遣労働の応募者、フリーランス等の請負業務、準委任業務等の受託者等の履歴書、職務経歴書、エントリーシート、適性試験、面接での様々な回答、オンライン面接時の自宅の風景等には、求職者のプライバシー、個人情報等も含まれる恐れもあると存じます。基本的に、テレワーク時は、様々な関係者へのプライバシー、個人情報等に対する慎重な配慮、事前の体制作り等が必要であると存じます。 　また、働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等に対するハラスメント防止（セクシャルハラスメント、パワーハラスメント等）、安全配慮、犯罪防止等のため、個人情報保護法、不正競争防止法、労働契約法、労働施策総合推進法、男女雇用機会均等法、育児・介護休業法、職業安定法、労働安全衛生法、労働基準法等の法令等、関係するガイドライン等に十分に配慮されたガイドラインにした方がよいのではないでしょうか。また、これらの法令等の名称、ガイドライン等に当ガイドラインが配慮されていること、準拠文献、出典等を当ガイドラインの本文でも、明記することも理解が深まり、よいのではないでしょうか。働く方（労働者、管理職、役員等）、その御家族、その御関係者、求職者等の肖像権、知的財産等への配慮についても当ガイドラインで明記した方がよいのではないでしょうか。 引用文献１　厚生労働省．（令和2年）．事業主啓発用パンフレット：公正な採用選考をめざして（令和2年度版）．参照日　令和3年3月5日，参照先　https://www.mhlw.go.jp/www2/topics/topics/saiyo/dl/saiyo-01.pdf 引用文献２　厚生労働省．（no date）．公正な採用選考について．参照日　令和３年３月５日，参照先 https://www.mhlw.go.jp/www2/topics/topics/saiyo/saiyo.htm ◇　御提案事項２　働く方（労働者、派遣労働者、フリーランス等の請負業務、準委任業務等の受託者、管理職、役員等）、その御家族、その御関係者に対するテレワーク時の不正競争防止法の営業秘密の取扱いへの注意喚起について 　御提案事項１でも触れましたが、本文において、働く方（労働者、派遣労働者、フリーランス等の請負業務、準委任業務等の受託者、管理職、役員等）、その御家族、その御関係者に対するテレワーク時の不正競争防止法の営業秘密の取扱いへの注意喚起がほとんどないように存じました。働く方（労働者、派遣労働者、フリーランス等の請負業務、準委任業務等の受託者、管理職、役員等）、その御家族、その御関係者は、不正競争防止法の営業秘密の取扱いのため、どのような点に注意すべきか、どのような対策を講ずるべきか等をしっかりと、分かりやすく明記し、多くの方が理解できるようにした方がよいのではないでしょうか。 ◇　御提案事項３　障がいをお持ちの方にも分かりやすいガイドライン作りへの御配慮について 　もう既に十分に御配慮いただいているのかもしれませんが、当ガイドラインを健常者の方だけではなく、障がいをお持ちの方にも広く当ガイドラインを御理解していただけるように、様々な御配慮をいただけるとよいのではないかと存じました。例えば、ソフトウェアを活用した、点字翻訳へのしやすさの向上、自動音声での文字の読み上げ等にも利用できるような御配慮もあるとよいのではないかと存じました。 ◇　御提案事項４　テキスト以外に動画コンテンツ等で情報発信することについて 　もし可能でございましたら、テキスト以外に動画コンテンツでの情報発信等も御実施していただけますと、より多くの方がより関心を持って、効果的に学習ができ、より広くより速く理解が促進する可能性もあるかもしれませんので、併せて、御検討のほど、よろしくお願いいたします。 【個人12】		
	その他（意見募集期間）		
44	本件の意見募集期間を30日未満としたのはなぜですか？ 【匿名01】	本件は行政手続法（平成５年法律第88号）に基づく意見公募対象ではないため、意見提出期間を30日以上と定めた同法第39条第３項の規定は適用されません。	無

※意見提出以外の部分についても誤植修正及び文意の明確化のため修正を実施しています。