別紙２

『テレワークセキュリティガイドライン（第４版）』（案）に対する意見の募集に対して提出された意見及びそれらに対する総務省の考え方（案）

（意見募集期間：平成 30 年 2 月 14 日～平成 30 年 3 月 15 日）

提出意見：5 者
　法人：1 者
　　（株式会社ソリトンシステムズ）
　個人：3 者
　　（個人 A～個人 C）
　提出者不明：1 者

【第一章　テレワークにおける情報セキュリティ対策の考え方】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見１　マルウェアの感染経路として、偽メールだけでなく、正規の相手先がマルウェア感染している場合についても考慮すべきである。	考え方１	
○　P.6 マルウェアの脆弱性に「偽メールに添付された」とあるが、正規の相手先がマルウェアに感染した場合にもウイルス付きのメールが添付される場合もあり、それを考量した表現にした方がよいのではないか。 【個人 A】	図中の限られた面積の中での例示につき、マルウェアに感染した相手から送られるメール等も意図して送られるものではないことから「偽メール」と総称して表現しております。	無
意見２　専門家登録制度として「情報処理安全確保支援士制度」を加えるべきではないか。	考え方２	
○　P.7 「【コラム】 中小企業の情報セキュリティ対策を支援する取組」に、一定の専門知識を備えた専門家登録制度として「情報処理安全確保支援士制度」を加えるべきではないか。 【提出者不明】	ご指摘をもとに、コラム内で情報処理安全確保支援士制度と IT コーディネータ制度について紹介するとともに、巻末の参考リンク集にも関連記述を追加いたしました。	有

意見３　「クラウド型アプリ形式」は、「クラウド型アプリ方式」変更してはどうか。	考え方３	
○　P.9 の表の行タイトル 「クラウド型アプリ形式」は、「クラウド型アプリ方式」が良いと考えます。 修正理由：他の名称との統一性を考えて。 【個人 B】	ご指摘を踏まえ、「クラウド型アプリ方式」に修正いたします。	有
意見４　テレワークのパターンとして、「セキュアブラウザ方式」や「アプリケーションラッピング方式」についても記載すべきではないか。	考え方４	
○　P.9 「テレワークの方法に応じた対策の考え方」項に対する意見 本項において、４種類のパターンに分類されたテレワークの方法が記載されている。 それら４種を、「テレワーク端末に電子データを保存しない」という要件を踏まえ、実現するためのツール(アプリケーション)での技術手法により分類すると、パターン１と２で記載されている「リモートデスクトップ方式」と「仮想デスクトップ方式」は、一般的にいわれる「画面転送型」であり、テレワークを実現するための技術方式の分類としては非常に偏っていると考える。 「画面転送型」以外の方式で「テレワーク端末に電子データを保存しない」という要件を踏まえると、「セキュアブラウザ方式」や「アプリケーションラッピング方式」というものも技術方式として存在しており、これらの方式を用いたテレワーク環境を実現している企業団体も増えてきている。いずれの方式も、テレワーク端末において、利用する電子データ(情報)を端末内に保存出来ないようにし、情報の外部流出を抑制することができる。 「セキュアブラウザ方式」では、特別な Web ブラウザを用い、利用端末内へのファイルのダウンロードや印刷、画面ショット取得、Web 参照履歴・キャッシュ保存を制限する(利用するデータ領域を仮想的に分離することで、利用端末内にデータを残さない仕組みも含む)。この場合、利用可能なシステムは Web サイトに限定されるが、業務利用されるシステムの大半は Web 化(クラウドアプリケーションも含む)	ご指摘を踏まえ、テレワークの方法に「セキュアブラウザ方式」と「アプリケーションラッピング方式」の２種類を追加し、それぞれの方法についての説明を追記するとともに、パターンが６種類となったことに伴い、ガイドライン全体にわたってパターンに関する記述の調整を行いました。	有

が進んでいることから、業務利用に対し必要十分である。また、「画面転送型」と比較した場合に、安価にテレワーク環境を用意でき、コストメリットもあることから、採用が進んでいる。 「アプリケーションラッピング方式」では、利用端末内のアプリケーション(文書作成ツール、Web ブラウザ等)に対し、端末内のコンピュータリソース(記憶媒体、プリンタ、レジストリ等のシステムリソース)へのアクセスを一時的(データ利用時のみ)に制御し、利用するデータ領域を仮想的に分離することで、利用端末内にデータを残さないことができる。先の「セキュアブラウザ方式」と同様に安価にテレワーク環境の用意が可能なことや、利用端末内のアプリケーションの自由度が高いことから注目されている方式である。 なお、どちらの方式においても、テレワーク端末から、利用システムへの経路制御(アクセス制御)やアクセスログの記録・保存も重要であることから、専用のゲートウェイ装置を経由(ユーザ・端末認証)させ、これらを実現する方法も存在する。 このような、近年の技術動向を踏まえ、本案に記載されている４種類のパターンに加え、「セキュアブラウザ方式」や「アプリケーションラッピング方式」等の、利用端末内部リソースの一時的(データ利用時のみ)な仮想隔離を行い「テレワーク端末に電子データを保存しない」という要件を満たす方式についても記載すべきである。 【株式会社ソリトンシステムズ】		
意見５　リモートデスクトップ方式であっても、クライアント PC にデータをコピーできる可能性がある点を記載すべきではないか。	考え方５	
○　P.9 パターン１リモートデスクトップ方式の説明で、「テレワーク環境で利用する端末に電子データは残りません」との記載があるが、リモートデスクトップ先からリモートデスクトップを実行するライアント側の PC にデータをコピーすることが可能であり、適切な表現とは言えないのではないか。 【個人 A】	ご指摘のとおり、原案は厳密には適切ではない表現となっていたことから、当該箇所を次の通り修正します。「テレワーク環境で利用する端末に電子データを残さないようにすることができますので、」	有

意見６　リモートデスクトップ方式であっても、クライアントPCにデータをコピーできる可能性があるため、パターン１とパターン４は同等のセキュリティ対策が必要ではないか。	考え方６	
○　P.11 パターン４（会社のPCの持ち帰り方式） 「４種類のパターンの中で最も厳格な情報セキュリティ対策を端末に対して行う必要がある」との記載があるが、前述のとおりパターン１リモートデスクトップ方式でもPCにデータをコピーを可能することは可能であるので、パターン１とパターン４は同等のセキュリティ対策が必要ではないか。 【個人A】	パターン４は、PCへのデータのコピー以外にも移動中の盗難・紛失等のリスクも考慮する必要があるなど、パターン１と比較してリスクの高い方式であることから、原案のとおりといたします。	無
意見７　テレワーク中にクラウドサービスに接続する際の、ファイアウォールの設定の記述を変更した方が良いのではないか。	考え方７	
○　P.13 「オフィス内に設置したサーバにテレワーク先からのアクセスを許可する場合、インターネットとの接続地点に設置するファイアウォールにテレワーク用の一種の「穴」をあける必要がありますが、これは攻撃に悪用される恐れがあり、注意深く設定しなければなりません。オフィス内のサーバをクラウドサービスに移行することでこうした「穴」をあける必要がなくなり、」 との記載があるが、クラウドサービスに接続するためにサーバに「穴」を空ける必要はあるので表現を変えた方が良いのではないか。 【個人A】	当該箇所における「穴」は外部から内部へのアクセス手段を意味する表現ですので、読者にその意味を明確に伝えるため、当該箇所を次の通り修正いたします。 「オフィス内に設置したサーバにテレワーク先からのアクセスを許可する場合、インターネットとの接続地点に設置するファイアウォールにおいて、外部から内部にアクセスするための一種の「穴」をあける必要がありますが、これは攻撃に悪用される恐れがあり、注意深く設定しなければなりません。オフィス内のサーバをクラウドサービスに移行することでこうした「穴」をあける必要がなくなり、」	有

【第三章　テレワークセキュリティ対策の解説】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見８　文章を以下のように修正してはどうか。	考え方８	
○　P.23 「9 ページに示したいずれの方法でも設定できますが、上述のように機密情報の持ち出しにはリスクが大きいので、テレワークで機密情報を扱う必要がある場合は、「リモートデスクトップ方式」や「仮想デスクトップ方式」にした上で、利用者に応じたアクセス制限を行うことで、機密情報を保護しつつ利用することが可能となります。」 ★上記部分を以下に修正する案を提案します。 「前述のテレワークの方法で示したいずれの方式を選択しても、情報資産に対するアクセス制限を行なうことは可能ですが、上述のように、機密情報の持ち出しには大きなリスクを伴ないます。 テレワークで機密情報を扱う必要がある場合には、「リモートデスクトップ方式」や「仮想デスクトップ方式」を採用した上で、資産情報の重要度と利用者の権限に基づく、適正なアクセス制御を行なうことで、機密情報の保護と利用の両立が可能になります。」 修正理由：原案の趣旨を踏まえた上で、主語述語などを補う推敲を行なったものです。 【個人 B】	ご指摘の趣旨を踏まえ、次の通り修正いたします。 「前述のテレワークの方法で示したいずれの方式を選択しても、情報資産に対するアクセス制限を行うことは可能ですが、上述のように、機密情報の持ち出しには大きなリスクを伴います。 テレワークで機密情報を扱う必要がある場合には、「リモートデスクトップ方式」や「仮想デスクトップ方式」を採用した上で、情報資産の重要度と利用者の権限に基づくアクセス制限を行うことで、機密情報の保護と利用の両立が可能になります。」	有
意見９　第三者の視線にさらされることが望ましくない情報を編集する場合、第三者に覗かれる恐れのある環境でのテレワークは禁ずるべきではないか。	考え方９	
○　P.45 「第三者の視線にさらされることが望ましくない情報を編集せざるを得ない場合は、あらかじめ企業のロゴを外したり、重要情報の書かれている部分の背景を文字と同じ色にして見えなくする等により、多少覗かれても実害がないようにすることも検討すべきです。」	ご指摘を踏まえて次のように修正いたします。「こうした環境においては、第三者の視線にさらされることが望ましくない情報の閲覧や編集は避けるべきです。あらかじめこうし	有

との記載があるが、そのような環境ではテレワークは行わないとした方が良いのではないか。 【個人 A】	た環境での作業が避けられないとわかっている場合は、資料から固有名詞などの機密情報を除いておくことで、漏えい時の被害を限定的にするなどの対策が考えられます。」	

【その他】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見１０　LINE とスマートフォンについての記述の追加を求めるもの。	考え方１０	
LINE とスマートフォンについての記述を追加されたい。 注意喚起が不十分であると考える。 【個人 C】	SNS 及びスマートフォンの安全な使い方に関する注意喚起につきましては、テレワーク目的に限定せずに幅広く啓発する必要があることから、本ガイドラインの対象外と考えます。	無