別紙２

「『テレワークセキュリティガイドライン（第３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
（意見募集期間：平成 25 年２月４日～同年３月５日）
【意見提出：５件】

| No. | 提出された意見 | 総務省の考え方 |
|---|---|---|
| 1 | 次に掲げる用語を用語集に加えるべきだと思います。<br>１．アクセスポイント（第５ページ）<br>２．定義ファイル（第１４ページ）<br>３．ミドルウェア（第２２ページ）<br>４．パッチ（第２４ページ）<br>５．ウイルス、ワーム及びトロイの木馬の違い（第３２ページ）<br>【個人】 | ご指摘のとおり、以下の内容を用語集に追記いたします。<br>【追記内容】<br>アクセスポイント：端末からインターネットに接続する際に中継を行う機器で、端末とは無線で、インターネットとは有線で通信を行うもの。<br>定義ファイル：ウイルスやワーム等の特徴を収録したファイルのこと。ウイルスやワーム等を検出する際に使われる。<br>ミドルウェア：ＯＳとアプリケーションの中間的な処理を行うソフトウェア。<br>パッチ：ソフトウェアを改善・改良するためのプログラムで、修正箇所についてのみ記述されたもの。<br>ウイルス、ワーム、トロイの木馬：悪意のあるソフトウェアの一種。 |
| 2 | WIFI のルータを使用したネットワークについての記述が抜けています。セキュリティの観点からも記述すべきと思います。<br>【個人】 | ご指摘のとおり公共の場所で使用可能な公衆無線ＬＡＮ（Ｗｉ－Ｆｉ）は、適切な暗号化をしないと情報漏洩等の危険を伴いますので、「勤務者１１」の解説に以下のとおり追記いたします。<br>【追記内容】<br>・・・可能性があります。公衆無線ＬＡＮ（W |

| | | |
|---|---|---|
| | | ｉ－Ｆｉ）を利用する際にも特に注意が必要です（※）。機密情報かどうかに・・・<br><br>（※）詳細については、総務省「無線 LAN を安心して利用するための手引書」<br>http://www.soumu.go.jp/main_sosiki/joho_tsusin/security.html<br>を参照してください。 |
| 3 | 電気機械メーカーにて、長年コンピュータ・システムを企画設計していたＯＢとして提言させて頂きます。本ガイドラインは、３版にもなるというところで言うのもなんですが、廃刊にすべきと思います。以下、その理由について述べます。まず、情報セキュリティ対策は、テレワークという限定は無く、コンピュータシステム全体の問題であり、情報セキュリティ対策をするのは、自社の扱う情報の「機密性」、「完全性」及び「可用性」を損なう脅威分析を行え、なお且つ、コンピュータシステムを熟知しているプロの情報システム管理者です。今や、非常に頭の良い連中が、システムの脆弱性を見つけ攻撃してくる新たなウイルスが次々と現れ、プロと言う人々でも苦労している状態です。素人がガイドラインを読んだ程度で手出しできるものではありません。そして情報セキュリティ対策の基本は、「ルール、人、技術のバランス」などではありません。脅威分析結果から得られた「格付け対策」です。参考までに、基本となる３レベルを紹介します。最上位）盗まれないように隔離する。第２位）盗まれても中身が読めないように暗号化などする。第３位）盗まれたり改ざんされたら証拠が残るようにする。この３レベルで、ハードウェア、ソフトウェア、人の対策をしていくのです。なお、膨大ではありますが、内閣官房情報セ | このガイドラインは、情報セキュリティ全体に関して網羅的に記載している訳ではなく、テレワークを対象にして、セキュリティ上の留意点をとりまとめたものです。<br>セキュリティに対して技術的対策を実施するには対策を実施する人材の育成や対策を行うに当たってのルール整備が併せて重要であり、そのような観点からまとめた本ガイドラインは必要なものと考えます。 |

| | | |
|---|---|---|
| | キュリティセンターが基準書や、解説書などを公開していますので読まれることをご提案致します。　以上<br>【個人】 | |
| 4 | P.5 図１<br>脅威：重要情報の盗聴<br>　他と比べて細かく、整合性が取れていない<br>重要情報の盗聴→通信情報の盗聴<br><br>P.10　（クラウドサービスの利用について）<br>・・・以下のことに注意して利用すべきです。<br>クラウド上に重要情報を置く危険性が書かれていない。<br>クラウドを利用するということは、『社内設置のサーバの管理を委託』するのと同じリスクがある。<br>・クラウド事業者が信頼できるか。　システム管理者であれば、情報を閲覧できる場合がある。内部統制が整っているか。<br><br>P.13～<br>全般的に経営者（陣）の責任・関与が弱い。<br>システム管理者は実務を実施すべきだが、その決定は経営者が行う。<br>また、システム管理者は決定に必要な情報を提供する義務を負う。<br>上記について、<br>経営者はルールを決める<br>システム管理者はルールを決める情報を提供、ルールが守られるように運用する | 特に重要な情報については、特段の対策が必要と考えられることから、「重要情報」と記載したものです。従って原案のとおりといたします。<br><br>ご指摘を踏まえて、（クラウドサービスの利用について）に以下の内容を追記します。<br>【追記内容】<br>・クラウド事業者の提供するクラウドサービスを利用する場合、データを預けることになりますので、クラウド事業者が信用に足る事業者かどうかに注意する必要があります。<br><br>経営者はルールの策定等に責任を持ってあたる必要があり、責任や関与が小さいということはありません。<br>また、システム管理者は、経営者がルールを策定する際に必要となる情報を提供する点については、ご指摘を踏まえて、「管理者１」の解説に以下のとおり追記いたします。 |

| | | |
|---|---|---|
| | 勤務者はルールを遵守する<br>というのが明確に書かれていると、判りやすい。<br>【提出者不明】 | 【追記内容】<br>　また、経営者がルールを決める際に必要な情報を提供します。 |
| 5 | ＜全体複数ページ＞<br>　以下の記述は表現を整理し、本ガイドラインが示す内容の重み付けを明確にして頂きたい。<br>「必要があります」「心がけます」「ようにします」「検討すべきです」「検討して下さい」「検討します」「よいでしょう」「重要です」「してください」<br>（意見提出の理由）<br>・様々な本書の内容が、どの程度の重要度、優先度であるのか、実装する際には必須なのか任意なのか、多様な文の帰結は複数の解釈を惹き起こす恐れがあります。<br>・本ガイドが示す、重要度や優先度、任意／必須が分かるような表現に整理すると良いと思います。 | 　テレワークの実施環境やその場の状況等により、実施すべき対策は異なると考えられます。本ガイドラインの運用に当たっては、そうした個別の事情に応じ、重要と考えられる対策を実施していただきたいと思います。 |
| | ＜全体複数ページ＞<br>「～し」、「～して」や「～など」、「～等」表記にブレがあります。<br>（意見提出の理由）<br>　読みやすく、統一感がでるため修正が望ましいと思います。 | 　ご指摘のとおり修正いたします。 |
| | ＜４ページ　３段落目＞<br>　以下の記述は記述表現の再考をして頂きたい。<br>「JISQ27002 規格における考え方をベースとしています。ただし、本ガイドラインはこの規格の完全な遵守を求めるものではなく～」 | 　本ガイドラインは、ＪＩＳにおいて求められている事項かどうかにかかわらず、重要と考えられるものをまとめたものです。 |

| | | |
|---|---|---|
| | （意見提出の理由）<br>・本ガイドラインにて示される具体例（例「私物利用の場合～企業から端末を貸与するほうが望ましいと考えられます」など）が、JISQ27002（実践のための規範）を越えたものも含まれていると思います。規格の完全遵守を求めないとしてもJISQ27002との整合性につき、本ガイド利用者に誤解を与える恐れがあります。<br>・JISQ27002に基づく例示と、それ以外の例示を明示的に分けると不要な誤解を与えにくくなると思います。<br><br>＜７ページ　（「人」について）＞<br>　記述の5行目「ルールが守られているかどうかを確認するのが難しい」を、「ルールが守られているかどうかを企業・組織が確認するのが難しい」と役割を担う団体を追記することを検討して頂きたい。<br>（意見提出の理由）<br>　人の役割を記述している箇所なので、役割を担う対象をはっきりさせると読みやすさが増すと思います。<br><br>＜８ページ 表1代表的な例＞<br>　項目名「代表的な例」を「代表的なテレワーク作業例」に変更してはいかがでしょうか。<br>（意見提出の理由）<br>　テレワーク形態と対策を論じている箇所のため、「例」の文字に関わる対象を記載しないと、「対策例」を読み間違える恐れがあります。 | ご指摘のとおり修正いたします。<br><br>ご指摘のとおり修正いたします。 |

| | | |
|---|---|---|
| | ＜８ページ　表１代表的な例、シンクライアント型＞<br>　説明文を下記のような表現に変更してはいかがでしょうか。<br>「テレワーク端末をシンクライアントとして使い、社内システム内のデータを参照したり編集する」<br>（意見提出の理由）<br>　パターン①と②の作業例は、情報取得方法を記載しています。パターン③の作業例は、接続説明になっています。<br>説明のパターンを統一すると IT が苦手な方が、より読みやすくなると思います。 | 　ご指摘を踏まえて、以下のとおり修正いたします。<br>【修正内容】<br>　テレワーク端末から社内システムに接続し、社内システム内の電子データを手元にコピーせずに閲覧や編集を行う |
| | ＜８ページ　パターン①（オフライン持ち出し型）＞<br>　3 行目「社内システムへのアクセスにインターネットを使わなければ」を、「インターネットを使って社内システムへアクセスして、参照したデータをテレワーク端末に格納しなければ」のように変更してはいかがでしょうか。<br>（意見提出の理由）<br>「インターネット」、「社内システム」、「データ」の関係性がはっきりすると、 IT が苦手な方が、より読みやすくなると思います。 | 　参照したデータをテレワーク端末に格納するのはパターン②に該当します。パターン①は参照したデータをテレワーク端末に格納するか否かに関わらず、社内システムへのアクセスにインターネットを使わない場合を指すことから、原案のとおりといたします。 |
| | ＜１０ページ　（自社にふさわしいテレワークの方式の検討）＞<br>　後半の段落「私物利用の場合」のガイドラインを別枠で追記することの検討をお願いします。<br>（意見提出の理由）<br>　セキュリティガイドライン 34 か条は、会社が完全にコントロール可能な会社貸与の設備を主としていると考えます。私物の設備へ規制することは | 　私物利用の場合のセキュリティ対策については、２３ページに記載しております。 |

<table>
<tr>
<td></td>
<td>難しいので、私物規制の要件が別にまとまっていると IT が苦手な方の理解が深まると思います。<br><br>＜１０ページ　３段落＞<br>　以下の記述は記述表現の再考をして頂きたい。<br>「私物利用の場合～企業から端末を貸与するほうが望ましいと考えられます」<br>（意見提出の理由）<br>　結論は理解出来るものの、根拠が不明確であると思います。<br><br>＜１１ページ　１段落目＞<br>　以下の記述は記述表現の再考をして頂きたい。<br>「～テレワーク用の一種の「穴」を空ける」<br>（意見提出の理由）<br>・「ポートに穴を開ける」という表現は、 SE 職レベルで使用されるものの本ガイドの利用者レベルに合っているか不明と思います。<br>・漢字表記の訂正「空ける」→「開ける」<br><br>＜１４～３０ページ　テレワークセキュリティ対策 34 か条　テレワークセキュリティ対策 34 か条の解説＞<br>　たとえば次表のような形で「テレワークセキュリティ対策 5 か条」あるいは「テレワークセキュリティ対策 16 か条」にまとめられないでしょうか？<br><table><tr><td>テレワークセキュリティ対策 5 か条</td><td>経営者</td><td>管理者</td><td>勤務者</td></tr></table></td>
<td>　ご指摘を踏まえて、以下のとおり修正いたします。<br>【修正内容】<br>　「私物利用の場合、・・・企業から端末を貸与する という選択肢も考えられます。」<br><br>　ここで使用している「穴」という言葉は、職場内に設置したサーバに、テレワーク先からアクセスする場合のイメージをわかりやすく解説するために用いていることから、原案のとおりといたします。<br>　また、漢字表記については、両論あるようですので、ひらがな表記にいたします。<br><br>　ご指摘を踏まえ、「テレワークセキュリティ対策のポイント」との記載に修正いたします。</td>
</tr>
</table>

| | | | | |
|---|---|---|---|---|
| (ア)情報セキュリティ保全対策の大枠 | 1～3 | 1～3 | 1～3 |
| (イ)悪意のソフトウエアに対する対策 | | 4～8 | 4～8 |
| (ウ)端末の紛失・盗難に対する対策 | | 9 | 9～10 |
| (エ)重要情報の盗聴に対する対策 | | 10 | 11～12 |
| (オ)不正侵入・踏み台に対する対策 | | 11～15 | 13～16 |

（意見提出の理由）

内容は非常に良く判りやすいのですが、「34 か条」と言われると読み下す上でも身構えるものがあります。「34 か条の解説」を読むと、大項目(ア)～(オ)の 5 項目に分類されており、中項目(青色の表)の 16 項目も経営者・管理者・勤務者の立場の違いはあれ、基本的な対策の主旨は同じだと考えます。

＜１６及び２４ページ　枠内＞

以下の記述は記述表現の再考をして頂きたい。

「記録媒体（USB 等）

（意見提出の理由）

「USB 等」→「USB メモリ等」

ご指摘のとおり修正いたします。

| | | |
|---|---|---|
| | ＜１７、１９～３０ページ　セキュリティガイドライン 34 か条の表番号＞<br>14～16 ページに掲載している表番号と同じ表現にすることをご検討願います。<br>（意見提出の理由）<br>14～16 ページの表では、1から通し番号ですが、後述の解説では、役割に番号を設定した表現になっています。<br>番号を ID として必要な箇所を探すときに、本体と参照先の番号表現が違うと、読み違えることがあります。<br><br>＜２３ページ　不正改造の説明箇所＞<br>「俗に「脱獄化」や「root 化」とも呼ばれます。」→「端末の「root 化」や「脱獄」などと呼ばれる行為があります」<br>（意見提出の理由）<br>脱獄は（端末を root 化した後の）行為なので「脱獄化」ではないと考えます。<br><br>＜２３ページ　（ウ）端末の紛失・盗難に対する対策＞<br>勤務者 9 の事項に対する、管理者へのガイド追加の検討をお願いします。<br>（意見提出の理由）<br>解説ページの構成は、<br>管理者の決めた対策を勤務者が実施する流れになっています。その流れを踏まえて、管理者は勤務者の使用する原本の所在管理を確認するための対照ガイドが必要と考えます。 | 後述の解説だけを読む場合にも、実施すべき対策だけでなく実施する主体もわかるように配慮した記載にしています。従って、原案のとおりといたします。<br><br>ご指摘のとおり修正いたします。<br><br>テレワークにおいて情報資産を持ち出すことは業務の一部として勤務者が日常的に行うことであり、個別のルールを策定し、それに従うのではなく、テレワークの実施に当たり策定する情報セキュリティポリシー等、全体としてのルールに従うものと考えます。従って、原案のとおりといたします。 |

| | | |
|---|---|---|
| | ＜２３、２４ページ　（ウ）端末の紛失・盗難に対する対策＞<br>テレワーク利用端末（特に BYOD 端末）を廃棄する際のルール（「パソコンの廃棄・譲渡時のハードディスク上のデータ消去に関するガイドライン」等）を記載していただけるとよいと考えます。<br>（意見提出の理由）<br>対策しない場合、重要情報を削除しただけのテレワーク/BYOD 端末が中古品として出回り、データサルベージを目的とした第三者に渡る可能性がありえます。また、P23 にも BYOD の記載がありますがテレワークと （持ち込みの）BYOD は両輪で進む可能性が高く、シャドーIT 問題の対策として、BYOD 端末の持ち込みに関しても台帳での管理を啓蒙していただけるとよいかと考えます。 | ご指摘を踏まえて、「管理者９」及び「勤務者１０」の解説を以下のとおり修正いたします。<br>【追記内容】<br>＜システム管理者＞<br>・・・状態かどうかを確認できるため便利です。<u>また、私物端末を利用する場合においても、同様に台帳等を整備することは有効と考えられます。</u><br><u>さらに、テレワークで使用した端末や USB メモリ等を廃棄・譲渡する場合、データをゴミ箱フォルダに捨てたり、ゴミ箱フォルダを空にするだけではデータは完全に削除されるとは限らない点に注意する必要があります。消去専用ソフトウェアを使用したり、ハードディスクを物理的に破壊したりする等の対策が必要です。</u><br>＜テレワーク勤務者＞<br>・・・できれば端末を一緒に持ち運ぶようにするほうがよいでしょう。<br><u>また、テレワークで使用した私物端末や USB メモリ等を廃棄・譲渡する場合にも、上記＜システム管理者＞で記載した事項に注意する必要があり、勤務者自身が行うのではなくシステム管理者が確実に実施することが望ましいと考えられます。</u> |

| | | |
|---|---|---|
| | ＜２５ページ　２～４行目＞<br>　以下の記述は削除、または記述表現の再考をして頂きたい。<br>「従業員が客の出入りを常時チェックしている店の中のように、置き引きしにくい場所であれば画面をロックするだけでも構いませんが」<br>（意見提出の理由）<br>　この条件でも置引きは発生します。本ガイドがこの条件であれば「画面ロックのみ」を推奨するように読み取れてしまうと思います。 | 　ご指摘を踏まえて、該当箇所を削除いたします。 |
| | ＜２５ページ　(エ)重要情報の盗聴に対する対策＞<br>　勤務者 11 の事項に対する、管理者へのガイド追加の検討をお願いします。<br>（意見提出の理由）<br>　解説ページの構成は、<br>管理者の決めた対策を勤務者が実施する流れになっています。その流れを踏まえて、管理者は勤務者の実施している対策の種類や性質について、確認することを記述した対照ガイドが必要と考えます。 | 　勤務者１１の事項については、業務の一部として勤務者が日常的に行うことであり、個別のルールを策定し、それに従うのではなく、テレワークの実施に当たり策定する情報セキュリティポリシー等、全体としてのルールに従うものと考えます。従って、原案のとおりといたします。 |
| | ＜２５ページ　管理者 10 と勤務者 12 のガイド＞<br>　管理者 10 が定めた点検ルールに対して、勤務者が実施することの事項を勤務者ガイドに追加することをご検討ください。<br>また、勤務者 12 の事項、第三者との共有環境での対策実施に対する、管理者のガイドを追加する検討をお願いします。<br>（意見提出の理由）<br>　管理者 10 の定めたルールを受けて、勤務者 12 で対策を実施することを、つなが | 　「管理者１０」については、全般にかかわる事項ですので、「管理者２」の解説に移します。<br>　また、勤務者１２の事項については、業務の一部として勤務者が日常的に行うことであり、個別のルールを策定し、それに従うのではなく、テレワークの実施に当たり策定する情報セキュリティポリシー等、全体としてのルールに従うものと考 |

| | | |
|---|---|---|
| | りで読み取ることが難しいです。<br>・点検についてのガイド<br>・第三者との共有環境で作業するときのガイド<br>　ガイドを上記のような 2 項目に分けると、管理者と勤務者それぞれの重要事項についての理解が深まるものと考えます。<br><br>＜２６ページ　８～１０行目＞<br>　以下の記述は削除、または記述表現の再考をして頂きたい。<br>「あらかじめ企業ロゴを外したり、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などにより、多少覗かれても実害がないようにすることも」<br>（意見提出の理由）<br>・「企業ロゴを外す」ことの実害防止効果が不明（ロゴを外せば実害が無いか）と思います。<br>・背景と同色にして文字を見えなくした状態は例示として実現性や利便性が低いと思います。<br><br>＜３０ページ　下から３行目＞<br>　以下の記述は削除、または記述表現の再考をして頂きたい。<br>「『この人のいつものメールの書き方と違う』と思ったら、そのメールを開かずに隔離することを心がける」<br>（意見提出の理由）<br>・「書き方の違いに気付く」には、直前にメールを開くため、実践困難と思います。 | えます。従って、原案のとおりといたします。<br><br>　これは例示として挙げており、その場の状況に応じて適宜の対応が必要です。<br><br>　ご指摘を踏まえて、該当箇所を削除いたします。 |

| | | |
|---|---|---|
| | ・「書き方の違い」を開封前に「件名（タイトル）」で判断することを提案している場合、直接的な表現にしたほうが良いと思います。<br><br>＜３１ページ　用語集＞<br>「マルウェア」はありますが、「ウィルス」や「ワーム」がありません。<br>（意見提出の理由）<br>P5 や P21 で「ワーム」が出てきますが、読み手にマルウェアの説明を必要とするのであれば「ウィルス」や「ワーム」も必要と考えます。あるいは全般に「マルウェア」と置き換えてもよいかと思います。<br><br>＜３１ページ　用語集＞<br>「シンクライアント」の説明として「ほとんどの機能やリソース管理をサーバ側で行い、クライアント側では最低限の処理しか行わない」旨の表記の追加が望ましい。<br>（意見提出の理由）<br>サーバ側のデータを参照・編集できるという旨がかかれており重要なシンクライアントの定義が漏れていると考えます（単なるネットワーク端末との区別がつきづらいと思います）。<br>【日本ユニシス株式会社】 | ご指摘を踏まえて、「ウイルス」、「ワーム」を用語集に追記いたします。追記内容は、意見 No.１に記載のとおりです。<br><br>８ページ表１の「代表的な例」の「シンクライアント型」に関するご意見に対して回答した内容を踏まえて、以下のとおり修正いたします。<br>【修正内容】<br>シンクライアント<br>・・・を接続することで、遠く離れた社内システムに接続し、社内システム内の電子データを手元にコピーせずに閲覧や編集を行うことができるサービスにおける、・・・ |