

パブリック・コメントにおける提出意見と回答

1. パブリック・コメントの実施概要

実施期間:平成17年2月28日(月)～3月11日(金)

掲載場所:経済産業省ホームページ

意見提出方法:電子メール、Fax、郵送

提出意見

意見提出件数 :24件

意見提出者数:6者

(内訳:IT関係業界団体:2、経済団体:1、消費者団体:1、企業:2)

意見の内容

(1)情報セキュリティ対策ベンチマーク :7件

(2)情報セキュリティ報告書モデル :3件

(3)事業継続計画策定ガイドライン :11件

(4)その他 :3件

2. 提出意見と回答

(1)情報セキュリティ対策ベンチマーク関係

(2)情報セキュリティ報告書モデル関係

(3)事業継続計画(BCP)策定ガイドライン関係

(4)その他

(1)情報セキュリティ対策ベンチマーク関係

	該当文章	意見	回答
1	資料1、P13、3.1.概要	P13の冒頭に記されている「簡易なリスク分析」という用語は分かりにくいいため、簡単な説明を行うべき。	御指摘を踏まえ、「簡易なリスク分析」を「これら(企業の業態や保有する情報資産等)の属性」に修正します。
2	資料1、P14、3.1.(2)企業分類	上記部分の最下行にある「(参考 参照)」は、「(参考 参照)」に修正すべき。	御指摘のとおり修正致します。
3	資料1、P16～17「望まれる水準」	「望まれる水準」は、企業の業務内容・IT依存度といった内的要因だけでなく、社会全体のネットワーク化の更なる進展といった外的要因によっても変動していくものであるため、「望ましい水準」を層別に決めるのは適当ではなく、企業自らが設定すべき。	企業自身の目標は本来企業自らが設定すべきものではありませんが、「高水準のセキュリティレベルが要求される層」であるにもかかわらず、低いレベルにとどまる企業がある等の現状(アンケート結果)を踏まえれば、現時点においては、「望まれる水準」の設定が必要と考えております。
4	資料1、P27～28、6.2.セルフチェックと連動するリスク定量化ツールの提供	情報セキュリティ対策ベンチマークに盛り込まれた予防措置を講じても万全ではないことから、「あるリスクに対してはこのレベルの対策が必要」という合理的な情報セキュリティ対策水準を算定するため、リスクに関する定量的指標について官民共同で検討すべき。	御指摘の通り、情報セキュリティ対策ベンチマークだけでは十分ではなく、技術的対策等も重要であると考えております。 なお、資料1の27～28ページに記載しているとおり、情報セキュリティ対策ベンチマークに係るリスク定量化ツールについては、今後検討していきたいと考えております。
5	資料1、P27～29、6.2.関係機関・業界に求められる取り組み	対策ベンチマークの内容は、環境の変化等に応じて変化していくものであるため、当該内容の見直し・更新のための体制が必要ではないか。	資料1の27ページにおいて、施策ツールの普及促進活動、普及状況の把握も含めたフォローアップ、内容の改訂等の取組みの必要性を記載しておりますが、当該取組みの中で今後検討していきたいと考えております。
6	資料2、A1-25ページ、2.(1)回答企業の分類	回答企業分類に掲載のある数式について、数式に設定する変数値を明らかにすべき。	御指摘を踏まえ、標準偏差等の変数値を記載致します。
7	資料3、P7、質問項目4、5	対策ベンチマークアンケート調査における質問項目4(公益性)と質問項目5(社会的重要度)は漠然としており、今後改善が必要ではないか。	資料1の27ページにおいて、施策ツールの普及促進活動、普及状況の把握も含めたフォローアップ、内容の改訂等の取組みの必要性を記載しておりますが、当該取組みの中で今後検討していきたいと考えております。

(2)情報セキュリティ報告書モデル関係

	該当文章	意見	回答
1	資料1、P20、4.3.(2)ステークホルダーにとっての効果	情報セキュリティ報告書の公表は、情報セキュリティ担当者の社内での業績アピールのみならず、全従業員にとっても効果がある旨を強調すべき。	御指摘の趣旨を踏まえ、(情報セキュリティ報告書の公表は)従業員の情報セキュリティに対する意識・理解を高める効果もある旨を記載致します。
2	資料1、P28、6.2. 第三者機関による情報セキュリティ報告書格付け	対策ベンチマークによる評価結果の延長線上に、第三者機関による情報セキュリティ報告書の格付けがある等、両者の連続性について記述すべき。	情報セキュリティ報告書の格付けは第三者機関が独自の視点・評価軸を持って行うものであり、その評価方法や成果について現段階で予断を与えるような記述を行うことは適当ではないと考えます。
3	資料1、P28、6.2. 第三者機関による情報セキュリティ報告書格付け	情報セキュリティ対策等の内容を公表することは困難な場合が多く、情報セキュリティ報告書による格付けを実施しても、企業の情報セキュリティ対策レベルを正確に評価することは困難であることに留意すべき。	

(3) 事業継続計画(BCP)策定ガイドライン関係

	該当部分	意見	回答
1	資料7、P3、1.2.(2) 図表2 事業中断の原因	図表2「業務中断の原因」に、財団法人日本情報処理開発協会(JIPDEC)「わが国における情報セキュリティの実態—情報セキュリティに関する調査」集計結果—」35ページ、36ページ「Q18 過去1年間に発生したシステムダウンの原因」に関する統計を使用すべき。	図表2は、情報システムへの依存増大に伴い、情報システムの障害が事業継続に及ぼす影響が大きくなっていることを、他の要因と比較しながら示すためのものです。御指摘のJIPDECの統計は、システムダウンの原因に係るものであって、システムダウンが事業継続に及ぼす影響を他の要因と比較しているものではないため、現在の図表2が適当と考えます。
2	資料7、P7、1.3.(5) 周辺領域・関連法規制	BCPとITIL (Information Technology Infrastructure Library) や米国企業改革法(SOX法)などの関係について記載すべき。	BCPとITIL及びSOX法の間には一定の関係があることは認識しておりますが、BCPと関連する事象を網羅することは困難であるため、今回のガイドラインでは現時点で比較的浸透している、BCPとの関係性の高いものに絞らせていただきました。
3	資料7、P12	図表番号5が3、4の前に来ている(通番の誤り)。	御指摘のとおり、修正致します。
4	資料7、P12、2.3.(1) ビジネスインパクト分析	原案では、リスク分析がBIA(Business Impact Analysis)の手段であるかのように読めるが、リスク分析はBIAの前提条件を整理・確認するためのものであることを明確にすべき。	御意見を踏まえ、リスク分析とBIAを明確に区別する方向で修正致します。
5	資料7、P13、2.3.(1) 目標復旧時間の設定	目標復旧時間(RTO)の設定に関して、ビジネス部門の役員の同意を得る等の設定手順についての記述を追加すべき。	御意見を踏まえ、設定手順に係る記述を追加致します。
6	資料7、P15、2.4.(2) テスト<BCP>のテスト検証項目>	システム障害訓練に限らず、ビジネス部門の参加も含めた総合訓練も加えるべき。	御意見を踏まえ、BCP総合訓練に係る記述を追加致します。
7	資料7、BCPガイドライン全般	BCPに関して、優先的に策定すべき業種や策定期限を提示すべき。	一般的に言って、社会的影響力の大きな業種においては、BCPを策定する必要性が高いと思われますが、優先的に策定すべき業種や策定期限を一律に設定するのではなく、BCPの概念自体の認知度向上を図りつつ、各企業の自律的・継続的な取組みを促していくことが重要と考えます。
8	同上	BCPの策定状況について定期的にフォローアップする仕組み・方策について検討すべき。	資料1の27ページにおいて、施策ツールの普及促進活動、普及状況の把握も含めたフォローアップ、内容の改訂等の取組みの必要性を記載しておりますが、当該取組みの中で今後検討していきたいと考えております。
9	同上	企業がBCP策定を公表することを推奨する仕組み・方策について検討すべき。	資料1の27ページにおいて、施策ツールの普及促進活動、普及状況の把握も含めたフォローアップ、内容の改訂等の取組みの必要性を記載しておりますが、当該取組みの中で今後検討していきたいと考えております。
10	同上	本ガイドラインに即した事業継続計画を策定し、実装することに対するインセンティブ(補助金や税制優遇措置など)について検討すべき。	BCPの策定は各企業が自らの利益を守り、企業価値を高めるために自律的・継続的に行っていただくべきものであり、補助金の付与や税制優遇措置などは現時点では予定しておりません。
11	同上	基幹システム、データプロセッシングのみでなく、平時・復旧時におけるバイタル・レコード(基幹文書・重要文書)マネジメントも重要である。	御指摘を踏まえ、23ページ3.4.(3)の脚注として、バイタル・レコード・マネジメントに係る記述を追加致します。

(4) その他

	該当文章	意見	回答
1	資料1、P2～3、1.2.企業や組織の情報セキュリティ対策の現状認識	個人情報の漏えいは「企業の責任」であることを明確にすべきであり、消費者に対しての十分な情報提供・啓発も引き続き行うべき。また、事故発生時に情報流出経路をトレースできるような仕組みについても記述すべき。	個人情報を取り扱う企業の責任については、本年4月に完全施行される個人情報保護法で明記されておりますが、これに加えて、当省としては、個人情報保護ガイドラインの策定やセミナー等を通じて、企業に対する啓発活動を行っているところです。また、消費者への情報提供・普及活動に関しても、政府として引き続き取り組んでまいりたいと考えます。なお、事故発生時のトレースに係る御指摘を踏まえ、事業継続計画策定ガイドライン(資料7)40ページに、情報システムの使用状況やアクセス状況の監視に係る記述を追加致します。
2	資料1、P11～12、2.3.情報セキュリティガバナンスの確立に向けた施策ツール	「事業継続計画策定ガイドライン」と「情報セキュリティ対策ベンチマーク」及び「情報セキュリティ報告書モデル」の関係について記述すべき。	御指摘の趣旨を踏まえ、「事業継続計画策定ガイドライン」が後2者に間接的に関係する旨の記述を追加致します。
3	資料1、P11～12、2.3.情報セキュリティガバナンスの確立に向けた施策ツール	情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインを社会に普及させる際には、規制等の強制的な手法によるのではなく、広報活動を充実させる等、企業への周知徹底を図るような手法を検討すべき。	資料1報告書の26～30ページで記載している「各主体に求められる取組み」を着実に実施することにより、企業への周知徹底と積極的な取組みを促すとともに、こうした取組みを支援・促進する環境を関係機関・業界及び政府が整備していきたいと考えております。