経営ガイドラインVer3.0（案）パブリックコメントで寄せられた御意見に対する考え方

整理番号	御意見の概要	御意見に対する考え方
1	>対策の推進はサプライチェーンに参加する中小企業を含む全ての企業の経営者の責務 他一か所に中小企業という文言が出てくる。本文書中での中小企業とは、中小企業基本法に定義される中小企業ということで良いか。 誰が読んでも一意となるよう確実に定義願う。 また、上記文章は、ともすれば大企業のことが記載ないため誤解を招くと思料する。 ここは 「対策の推進はサプライチェーンに参加する、大企業、中小企業といった企業の規模を問わず、全ての企業の経営者の責務である。」 というような文言のほうが適切と本稿意見者は思料する。	御意見を踏まえ、意図を明確に伝える観点から当該箇所を「対策の推進はサプライチェーンに参加する、企業規模の大小を問わない全ての企業の経営者の責務」に修正いたします。
2	1ページ 「サイバーセキュリティ経営ガイドラインの背景と位置づけ」をなぜ薄い青色で記載するのか？ 青色ならまだしもなぜ薄い青色なのか？ 「サイバーセキュリティを包含するリスクマネジメントの必要性 」の黒色はタイトルだから太字で強調するのはいいが、 しかし本文をなぜ薄い黒色で記載するのか？ 「タイトル」と「本文」でフォントの種類が違って見えるがどうなのか？ 適切なフォントが使われていない。 アルファベットが太字になっているのはなぜか？ ローマ数字の4ページの「指示６ ： PDCA サイクルによるサイバーセキュリティ対策の継続的改善 」では「PDCA」の箇所だけ太字だが、これはそれが大事だから太字で強調されているのか、不適切なフォントを使っているからアルファベットだけが太字になっているのか分からなく紛らわしい。 ページの表記も１２３４(機種依存文字でこのフォームで使えない。ローマ数字のことです) １２３４となぜ繰り返しているのか？ １２３４５６７８ではないのか？	御意見を踏まえ、フォントの統一及びページ番号の見直し等の修正を行いました。その他の御意見につきましては、今後の参考にさせていただきます。
3	サイバーセキュリティを是非とも確固たるものにしてほしいです。 昨今の中国共産党からと思われるサイバー攻撃の脅威は、恐るべきものだと感じています。 日本は、自国の企業で開発した技術を盗用され、人民解放軍の軍事に扱われるなどといった、恐ろしい情報もネットをはじめとする各方面で言われています。 ロシアのウクライナへの軍事侵攻が起こっている今、中国の台湾進攻も現実味を帯びています。 科学技術の流出はもちろん、外国への土地の売却なども、可能な限り辞めて頂きたいと思っています。 どうぞよろしくお願いいたします。	引き続き、サイバーセキュリティに関する施策を実施してまいります。
4	技術情報管理認証制度を盛り込んではいかがでしょうか。 経済産業省が推進している制度と存知でおります。 PマークやISMSとは違う形で、公的な情報管理基準の指針になるかと思います。 というか基準（ガイドライン）がないのは、大きな問題かと感じます。	御意見を踏まえ、サイバーセキュリティ経営の重要10項目のうち指示9の対策例として「ISMS等のセキュリティマネジメント認証を取得していることがより望ましい。」と記載している箇所への脚注として、「ISMS認証を取得していない場合でも、例えば、技術情報管理認証を取得していることを確認することなどが考えられる。 」を追記いたします。
5	非常に重要なガイドラインを細心の注意の上で見直し、改善していただき、そのご尽力に敬意を表します。	引き続き、サイバーセキュリティに関する施策を実施してまいります。
6	以前から、本ガイドラインの対象は、いわゆる「会社」と呼ばれる企業を対象にしている。しかし、「サイバーセキュリティ基本法」の「重要社会基盤事業者」や、「重要インフラ」と呼ばれる14分野を網羅できる記載にすべきではないか。あるいは、これらの14分野と、本ガイドラインとの関係等を明確に記載すべきではないか。 特に本ガイドラインの主担当でもある「経済産業省サイバーセキュリティ課」はデマケ等にとらわれることなく、広い視野で本邦のサイバーセキュリティに関してのガイドラインを適切に公表することを期待しています。	本ガイドラインにつきましては、「重要社会基盤事業者」及び「重要インフラ」に限られず、幅広い企業を対象として想定しておりますところ、御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
7	非常に些細な点ですが、今回のコメント募集の対象の文書は、*しおり無し*のPDFで公開されている。せめて、しおり付きのPDF、できたら複雑な検索が可能なWordでの提供もあることが望ましい。この部分ができていないと、電子的とかデジタルとかがしっかり理解されていない組織による作成と思われてしまう。例えば、ある国では国民の電子での可読性をあげるためにＰＤＦでの公開をやめているとの話も聞いたことがある。そのとおりだと思います。現在、公開されているV2.0は、しおり付きのＰＤＦで公開していただいているのに、今回のコメント対象の案は、しおりがない。 本来、V3.0への更新なので、変更箇所を適切に理解したいため、Wordの変更履歴機能を使ってのWord版も参考としてあることが当然であるのでないかと感じる。	サイバーセキュリティ経営ガイドラインVer3.0の公開にあたっては、しおり付きのPDF形式で公開予定です。そのほかいただいた御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
8	II(2)において「自社のサイバーセキュリティ確保に関する責務を全うするには･･･」と記載されている。サプライチエーンを示したいのかと思いますが、現在の記載だと片方側だけの記載になってしまっている。自社のサイバーセキュリティを確保するためだけではなく、他社のサイバーセキュリティを確保するために自社がリスクになる責任が存在する。V2.0(前版)では、両方を示す記載になっていたが、今回の案では片方になってしまったと認識される記載になってしまっている。	御意見を踏まえ、「自社のサイバーセキュリティ確保に関する責務を全うするには、ビジネスパートナーや委託先等」と記載している箇所を「サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等」に修正するとともに、後述の解説において自社が他社にとってのリスクとならないための責任に関する内容を追記いたします。
9	II(3)において、「サイバーセキュリティ対策の効果を高めるため･･･」と記載されている。「効果を高めるため」ではなく、「サイバーセキュリティを確保するため」には、コミュニケーションが必須であるような記載にしたほうがいいのではないか。	御意見を踏まえ、当該箇所を「効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要」に修正いたします。
10	「III. サイバーセキュリティ経営の重要１０項目」において、「これらは、単に指示すればよいのではなく、組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが求められる。」と記載されている。脚注1にも記載があるように、経営者等の「指示」には、前記の「組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮」が含まれている。下記のように変更したほうがいいのではないか。「これらの指示とは、組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮すること含まれる。」	御意見を踏まえ、当該箇所を「これらは、単なる指示ではなく、組織のリスクマネジメントの責任を担う経営者が自らの役割としてリスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが含まれる。」に修正いたします。
11	全体を通して、「製造業」の場合のその製造製品に関するサイバーセキュリティに関する記載が不足しているように思える。ＩＴ機器以外の製造業の製品においても、コンピュータを搭載している製品が多く存在する。本書は、「製造業」に特化すべきではないが、それを網羅する記載であるべき。例えば、「指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」において、「事業に用いる･･･自組織におけるサイバーセキュリティリスクを識別させる。」と自社で使うものしかリスクの対象にしていない記載になってしまっている。別な例として「指示６ PDCA サイクルによるサイバーセキュリティ対策の継続的改善」において、「リスクの変化に対応し、組織としてのリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえたPDCA サイクルを運用させる。」と記載されている。ここで「リスク」及び「リスク対策」が自社だけを示す記載になってしまっている。製造業者の製品のサイバーセキュリティを考慮した場合は、「リスク」は製品を購入した組織に存在して、その対策は、その組織と自社との共同作業になる。ここでは、「組織としての」の言葉がないほうが、より広い領域を対象にできるのではないか。	御意見を踏まえ、ご指摘の箇所についてそれぞれ以下のとおり修正いたします。 指示４：「自組織におけるサイバーセキュリティリスク」→「自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスク」 指示６：「組織としてのリスク対応」→「組織や事業におけるリスク対応」
12	本書で示す「サイバーセキュリティ」、「サイバーセキュリティリスク」を明確に定義したほうがいいのではないか。「サイバーセキュリティ基本法」で「サイバーセキュリティ」の用語を定義しているが、情報セキュリティの中のサイバーだけのような定義になってしまっている。ISO/IECTS 27100:2020 Information technology-Cybersecurity-Overview and Conceptsで定義されているsafeguarding of people, society, organizations and nations from cyber risks 等を参考に情報セキュリティとは、セキュリティに対する視点や関心の違いであると記載したらどうかと思います。情報セキュリティは、情報、情報システムのセキュリティを確保すること。サイバーセキュリティは、サイバーリスクから会社、組織、人、国家の安全を確保すること。その上で、サイバーリスクを企業(事業体)への脅威で定義したらどうかと思います。主な脅威は、事業が継続できなくなること。	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
13	ガイドライン案拝見しました。 ２４ページに記載の　”ISMS 等のセキュリティマネジメント認証を取得していることがより望ましい。”　とありますが、これらのＭＳ取得を促す文言に ”技術情報管理人証制度（TICS）”の記述も検討いただきたいです。 ご検討をお願いいたします。	御意見を踏まえ、当該箇所への脚注として、「ISMS認証を取得していない場合でも、例えば、技術情報管理認証を取得していることを確認することなどが考えられる。 」を追記いたします。

整理番号	御意見の概要	御意見に対する考え方
14	・該当箇所 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策　（P24） ・系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等が SECURITY ACTION13を実施していることを確認する。なお、ISMS 等のセキュリ ティマネジメント認証を取得していることがより望ましい。 ・意見内容 上記の対策例にサプライチェーンの委託先等の情報管理状況を確認するための認証制度として経済産業省の「技術情報管理認証制度」も追加していただきたく。 ・理由 弊社は中小企業事業者ですが、ISMSより負担が少なくかつサイバーフィジカルの情報セキュリティ対策に「技術情報管理認証制度」を利用しようとしております。 しかしながら、サプライチェーン上流にこの制度の認知度が低いため認証取得のアピール効果が不明です。 国の定める情報セキュリティの認証制度なので、ぜひ、サイバーセキュリティ経営ガイドラインに記載いただきたく （出典）経済産業省ホームページ https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html	御意見を踏まえ、当該箇所への脚注として、「ISMS認証を取得していない場合でも、例えば、技術情報管理認証を取得していることを確認することなどが考えられる。 」を追記いたします。
15	指示９につきまして、意見申し上げます。 昨今のサイバーセキュリティのインシデントとして、委託先等のサプライチェーン全体の状況把握を経営者が必ずしも出来ていないと考えております。 特に委託先が外国企業である場合、法令が日本とは異なるケースが多く、例えば中国に委託先がある場合、機密情報管理についてどこまでガバナンスが効果的に出来るのかが重要課題と認識しております。グローバルとの一言で限定はせず、地政学的にどこの国が委託先としてリスクが高いのかを日本国として明確に指針を出すべきと考えます。	御意見を踏まえ、「対策を怠った場合のシナリオ」に「委託先選定に際して地政学リスクや自然災害等のリスクを考慮しなかった結果、想定外の事業停止に追い込まれる。」を、「対策例」に「委託先選定にあたっては、コストや体制、技術力のみでなく、環境リスク（自然災害やパンデミック等）、地政学リスク（テロや政治的な不安等）及び経済リスク（ 経済危機や原料の価格変動等）の影響を考慮する。」をそれぞれ追加いたします。
16	以下の2点について、どちらかというと文章構成への内容になりますが、意見を提出させていただきます。 「指示７：インシデント発生時の緊急対応体制の整備」 「指示８ インシデントによる被害に備えた事業継続・復旧体制の整備」 現在のサイバー攻撃の被害などを見ると、攻撃者の組織化する攻撃にインシデントを避けることは難しく、BCPを含めた内容も企業の存続に影響する内容として重要であり、10の指示のうち2項目をあてていることも、その内容にも分量などの制約がある中で妥当性があると思います。 ただし、個人的には10の指示の7~8番目にインシデントへの対応が位置していること自体に少し違和感があります。 というのも、企業経営に限りませんが日々の日常業務のようなものと、インシデント発生時のような緊急事態はかなり性質も違うと思っています。また、セキュリティベンダーの緊急対応の技術者も、それ以外の技術者とかなりスキル特性やパーソナリティが異なると認識しています。つまり、かなりセキュリティの中でもかなり特殊な分野であり、それを実施する人材、やり方、お金の掛け方なども他と大きく異なると考えています。 ＜章構成の変更について＞ そのため、構成としては指示１～３のような対策を行う体制準備・戦略的なものはまず別枠とします。そして、指示４～６のような具体的な対策の実装。指示９のような守るべき対象をサプライチェーン全体へ拡大すること。指示１０の（何事にも重要な）コミュニケーションを平常時の対策とします。 その上で、非常時のインデント対応としてやることを（指示７～８の部分）として纏めるようにすると個人的にはより良いと感じました。 ＜変更のメリット＞ このような構成自体の変更を行う事で、企業経営者やセキュリティ担当者に大きく３つの分野（以下の項目）でやらなければならないことを意識づけられると思います。これが、この変更のメリットです。 ［企業のセキュリティ対策に必要な3つの分野］ （1）体制整備・戦略的なこと全般 （2）攻撃（BCP等も含む）を受けにくする対策、より堅固な対策への恒常的施策 （3）それでも防ぐことが出来なかったインシデントへの緊急対応	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
	上記のように、３つの分野毎に結構やらなければならない事やその特性が大きく異なっていると私は感じています。そして、特性が異なるので対応する人のタイプも同様に異なります。 [役割と特性毎の担当者の特性] (1)戦略的に体制整備などの大枠を作る人　⇒経営企画的な人が適合 (2)具体的なセキュリティ対策を実行する人　⇒IT技術や攻撃手法に詳しい人 (3)インシデント等の緊急対応をする人　⇒行動と判断が迅速にできる人 ＜まとめ＞ 現在のセキュリティ対策はどうしても(2)のIT技術や攻撃手法に詳しい人が中心となる傾向が高いと思っています。もちろん、攻撃者の技術が高まっている現状ではそれは理にかなっていると思われます。 ただし、経営者はそういう特性の方をCISO等に就任させることで対策が終わったような錯覚を受けると思うのです。そのため、(1)のような事業部門などとの関係性が深く、そのような部門に組織的な指示ができる部門の方と技術力偏重の特性を持つ(2)の人がタッグを組む形態が望ましいと考えています。これができれば、(1)の人は経営に近いので、現在よりも「サイバーセキュリティ経営」と呼べるものに近いものが出来ると感じています。 それがわかる構成になっていれば、ガイドラインを見た人が、そういう組織体制にすることで「サイバーセキュリティ経営を実現するのか！」という理解をしてくれる可能性が高まり、私の考える理想形に少し近づくのではと考えています。 なお、(3)の緊急対応をする人というのは、それとは別の特殊部隊に近い印象を持っています。ただ、一般的なCSIRTメンバには荷が重いと個人的に思っていますし、そういう要員を社内に定常的に置くのも厳しいと思っています。そのため、ここは事前に緊急対応に強い経験値のある技術者が多数居る外部ベンダーとの事前の体制整備が重要と個人的には考えていますが、政府のガイドラインにそれを記載するのは少し問題があると思われるので、平常時の対策をしている人とは別に特性の違う緊急対応という特殊ミッションに対応する人が必要になるというくらいの表現が良いのではないでしょうか？ （あくまで個人意見として）意見募集に対する私見を述べさせていただきました。 宜しくお願い致します。	
17	経済産業省が中心となって推進されている「サイバーセキュリティ経営ガイドライン」 の作成・更新は、サプライチェーンに参加する中小企業等を含む民間事業者や、その経営とIT活用を支援する立場の私どもにとって、あるべき（目指すべき）姿の指標となるものであり、大変重要な取り組みであると認識しております。 さて、このたびの改訂にあたり、以下一点のみコメントさせて頂きます。 ■該当箇所P23～24 3.4.サプライチェーンセキュリティ対策の推進 における「対策例」として、経済産業省など国が制定した情報管理の認証制度である「技術情報管理認証制度（TICS）」を追記し、特に各業界のサプライチェーンに参加する中小企業への取得を推奨すべきであると考えます。 【追記案】 ・重要な技術情報等の流出防止を適切に管理する「技術情報管理認証制度（TICS）※」の認証を取得していることがより望ましい。 ※国が策定した基準に基づき国の認定を受けた機関による情報管理の認証制度です。 https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html 以上、どうぞよろしくお願いいたします。	御意見を踏まえ、サイバーセキュリティ経営の重要10項目のうち指示9の対策例として「ISMS等のセキュリティマネジメント認証を取得していることがより望ましい。」と記載している箇所への脚注として、「ISMS認証を取得していない場合でも、例えば、技術情報管理認証を取得していることを確認することなどが考えられる。 」を追記いたします。
19	該当箇所 ページII　下から二つ目の〇　及び　ｐ６「（１）の解説三つ目のポツにおける「経営者としての責務である」との記述について 意見内容 「サイバーセキュリティに関する残留リスクを許容水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である」との記述を、「エンタープライズレベルの残留リスクの許容水準を判断し、エンタープライズレベルでの残留リスク総量を水準まで低減させること、その一要因として対策の実施を通じたサイバーセキュリティに関する残留リスクを織り込むことは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。」といった内容に修正すべきと考えます。 理由 まさに、本案文で「サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった場合には、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。このため、サイバーセキュリティリスクを多様な経営リスクの中での一つとして位置づけ、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）を任命するとともに、経営者自らがリーダーシップを発揮して自社の組織や事業におけるリスクを把握した上で、それに応じた対策の推進を主導することが必要」とあるように、多様な経営リスクの中の一つとして位置づけられるべきものと考えます。	御意見を踏まえ、「サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバ ーセキュリティに関する残留リスクを許容水準まで低減することは、企業として 果たすべき社会的責任であり、その実践は経営者としての責務である。」と記載している箇所を、「サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必要な費用）と位置付けることが重要である。直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、サイバーセキュリティリスクを経営リスクとして織り込み、サイバーセキュリティリスクを把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。」に修正いたします。

整理番号	御意見の概要	御意見に対する考え方
20	#章立て ３．１．サイバーセキュリティリスクの管理体制構築 指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定 #ページ9 #資料内の具体的な記載内容 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整 合を取ったセキュリティポリシーを策定する。 #意見内容 "7ページで「対策の推進はサプライチェーンに参加する中小企業を含む全ての企業の経営者の責務である。」と述べているため、本書は幅広い中小企業の経営者も対象としているものと理解しています。 残念ながら、セキュリティポリシーという言葉を見て、どのようなものを用意すれば良いのか分からない経営者も多く存在することが予想されます。 そのため、セキュリティポリシーは、具体的にどのようなものであるというものの示すURLを注釈として用意するのがよろしいかと存じます。 URLの例 https://www.jnsa.org/result/2016/policy/ https://www.ipa.go.jp/security/keihatsu/sme/guideline/	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
21	#章立てサイバーセキュリティ経営ガイドライン・概要　I．企業リスクマネジメントの一部としてのサイバーセキュリティ #ページI　#資料内の具体的な記載内容 ----v3.0---- サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。 ----v2.0---- また、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、IT を利活用して企業の収益を生み出す上でも重要な要素となる。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。 #意見内容 v2.0 「セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。」のようにまずコストではない点をストレートに表現した方が経営者向けにはより伝わりやすいと思いました 例）セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。	御意見を踏まえ、「サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバ ーセキュリティに関する残留リスクを許容水準まで低減することは、企業として 果たすべき社会的責任であり、その実践は経営者としての責務である。」と記載している箇所を、「サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必要な費用）と位置付けることが重要である。直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、サイバーセキュリティリスクを経営リスクとして織り込み、サイバーセキュリティリスクを把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。」に修正するとともに、投資の意味するところに関する脚注を追記いたします。
22	提出意見： #章立て 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 #ページ 15 #資料内の具体的な記載内容 ゼロトラストモデルに基づく対策を講じる際には、境界防御の効果が期待できないことを踏まえた認証等の強化を図るとともに、インシデントの予兆の段階で即時の検知と対象ができるような仕組みや体制を整備する。 #意見内容 7ページで「対策の推進はサプライチェーンに参加する中小企業を含む全ての企業の経営者の責務である。」と述べているため、本書は幅広い中小企業の経営者も対象としているものと理解しています。 先ず、中小企業の経営者には「ゼロトラストモデル」という言葉は通じないものと考えます。 そのため、「ゼロトラストモデル」を端的に解説するURLを注釈として用意する必要があるものと存じます URLの例 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
23	＜ページ数＞ II ＜項目＞ I. 企業リスクマネジメントの一部としてのサイバーセキュリティ ＜記載内容＞ さらに、被害が深刻な場合の事業停止や新たな脅威に対処するための予算措置等の経営判断も要求され、担当者への丸投げは許されるものではない。 ＜コメント＞ CISOに丸投げするケースが言及されていますが、外部ベンダーにセキュリティ関連業務を丸投げしているケースもあると考えます。（XX会社にアセスメントしてもらっているから安心など）外部委託自体は悪ではありませんが、外部ベンダーへの丸投げ体質に関しても、被害が深刻な場合等の経営判断能力を奪う要因となるため、ここで言及していただき、強く牽制することが望ましいと考えます。 文案： さらに、被害が深刻な場合の事業停止や新たな脅威に対処するための予算措置等の経営判断も要求され、担当者への丸投げは許されるものではない。また、外部ベンダーに委託する場合であっても、委託する内容に関して自らが説明責任を有することを忘れてはならない。	当該箇所は経営者に対して自覚を求める意図で記載しており、外部委託に関する内容を記載することで経営者へのメッセージが伝わりにくくなるおそれがあることから、原案のとおりとさせていただきます。
24	#章立て 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 #ページ 15 #資料内の具体的な記載内容 ゼロトラストモデルに基づく対策を講じる際には、境界防御の効果が期待できないことを踏まえた認証等の強化を図るとともに、インシデントの予兆の段階で即時の検知と対象ができるような仕組みや体制を整備する。 #意見内容 7ページで「対策の推進はサプライチェーンに参加する中小企業を含む全ての企業の経営者の責務である。」と述べているため、本書は幅広い中小企業の経営者も対象としているものと理解しています。 中小企業は、即時検知や体制の部分で対応することが困難であるため、本文だけでは絵に描いた餅のように受け止められる恐れがあります。 そのため、本文に体制がない組織に向けて「仕組みや体制の整備が難しい組織は、これらを支援するサイバーセキュリティお助け隊等の中小企業向け施策を活用する。」といった文章を追記し、24ページに掲載している注釈「中小企業を対象に、サイバーセキュリティに関する「見守り」「駆付け」「保険」をまとめて提供するサービス 」を追加するのが良いと考えます。	御意見を踏まえ、当該箇所への脚注として「自組織のみで仕組みや体制の整備が難しい組織の場合、これらを支援する『サイバーセキュリティお助け隊』等の中小企業向け施策を活用することが考えられる。詳細については付録B（サイバーセキュリティ対策に関する参考情報）を参照のこと。」を追記いたします。
25	#章立て ３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進 指示１０ サイバーセキュリティに関する情報の収集、共有及び開示の促進 #ページ 25 #資料内の具体的な記載内容 JPCERT コーディネーションセンターにインシデントに関する情報提供を行い、必要に応じて調整を依頼する。 #意見内容 当該窓口情報にリーチするURLが掲載されていないため、URLを注釈に掲載することを提案します。 参考URL https://form.jpcert.or.jp/	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
26	#章立て　サイバーセキュリティ経営ガイドライン・概要 #ページ　II　#資料内の具体的な記載内容 ----v3.0---- サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。 ----v2.0---- また、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、IT を利活用して企業の収益を生み出す上でも重要な要素となる。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。 #意見内容 「サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが」の記載は、正しいが、これを記載することで経営者が及び腰になってしまう可能性があると考えます。 v2.0の記載である「IT を利活用して企業の収益を生み出す上でも重要な要素となる」のような前向きな記載の方が良いのではないかと感じました。 文案： サイバーセキュリティ対策への投資は、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠であるとともにIT を利活用して企業の収益を生み出す上でも重要な要素である。また、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。	御意見を踏まえ、「サイバーセキュリティ対策への投資による直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、対策の実施を通じてサイバ ーセキュリティに関する残留リスクを許容水準まで低減することは、企業として 果たすべき社会的責任であり、その実践は経営者としての責務である。」と記載している箇所を、「サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必要な費用）と位置付けることが重要である。直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、サイバーセキュリティリスクを経営リスクの一環として織り込み、その観点からサイバーセキュリティリスクを把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。」に修正するとともに、投資の意味するところに関する脚注を追記いたします。
27	#章立て 指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善 #ページ 17-18 #資料内の具体的な記載内容 サイバーセキュリティリスク管理に関する KPI を定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する。KPI としては、リスク対応に関するパフォーマンスの評価の観点から、次のような指標が考えられる。 対策をしなかった場合の被害額 #意見内容 被害額を算出する手法について、対象読者は思い至らないものと考えますため、その手法に関わる解説URLを注釈に掲載するのがよろしいかと存じます。 URL例 https://www.j-cic.com/reports.html 取締役会で議論するためのサイバーリスクの数値化モデル	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
28	「付録A~F」に関しては実務上かなり参考となるものが紹介されており、大変ありがたいものであると感じました。 しかし、それぞれの「指示」の「具体的な対策」などにおいて「付録A~F」が紹介された際に、付録のリンクが記載されていないため、情報に対してのアクセシビリティが低い構成となっておりました。 忙しい経営者や経営者から指示を受けた担当者が効率よく情報にアクセスするために、「付録A~F」を紹介する際には付録のリンクも記載していただくことが望ましいかと考えます。	御意見は、付録A～Fの改訂に当たって参考にさせていただきます。
29	#章立て ３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進 指示１０ サイバーセキュリティに関する情報の収集、共有及び開示の促進 #ページ 25 #資料内の具体的な記載内容 ・IPA に対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいてマルウェア情報や不正アクセス情報の届出をする。 #意見内容 当該窓口情報にリーチするURLが掲載されていないため、URLを注釈に掲載することを提案します。 参考URL https://www.ipa.go.jp/security/outline/todokede-j.html	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
30	#章立て 指示６ PDCA サイクルによるサイバーセキュリティ対策の継続的改善 #ページ 18 #資料内の具体的な記載内容 サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じた公表、又はサプライチェーン関係者への個別の開示等に取り組む。 #意見内容 ここに掲載されている情報開示手段への記載について、認知度が低く、その必要性が遡及されていないものと考えます。 総務省から提示されている「サイバーセキュリティ対策情報開示の手引き」を注釈URLとして掲載しつつ、世の中としてそのような動きになっていることを重ねて示すよう文面を調整するのがよろしいかと考えます。 参考URL https://www.soumu.go.jp/main_content/000630516.pdf	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
31	#章立て ３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進 指示１０ サイバーセキュリティに関する情報の収集、共有及び開示の促進 #ページ 25 #資料内の具体的な記載内容 ・IPA や一般社団法人 JPCERT コーディネーションセンター等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に活かす。 #意見内容 当該情報にリーチするURLが掲載されていないため、URLを注釈に掲載することを提案します。 参考URL https://www.ipa.go.jp/security/announce/alert.html https://www.jpcert.or.jp/vh/top.html https://www.jpcert.or.jp/at/2022.html	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
32	#章立て サイバーセキュリティ経営ガイドライン・概要 #ページ II #資料内の具体的な記載内容 多様化するサプライチェーン上のサイバー攻撃の起点は広く拡散しており、大企業等と直接の取引がない中小企業であっても、サプライチェーンを通じた間接的 なつながりがある全ての企業において、自然災害等のリスクに加えて、サイバー攻撃等によるリスクを考慮したリスクマネジメントが求められている。 #意見内容 「サプライチェーンを通じた間接的なつながりがある全ての企業において、」と記載があるが、結局のところ全ての企業で、サイバー攻撃等によるリスクを考慮したリスクマネジメントが求められていることが伝えたいことだと理解しました。本記載だと、一部の中小企業の経営者は、無関係であると読み取る方もいると考えました。 #文案 多様化するサプライチェーン上のサイバー攻撃の起点は広く拡散しており、大企業等と直接の取引がない中小企業であっても、把握できていない間接的なつながりがある可能性があるため、全ての企業において、自然災害等のリスクに加えて、サイバー攻撃等によるリスクを考慮したリスクマネジメントが求められている。	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
33	#章立て ３．３．インシデント発生に備えた体制構築 指示７ インシデント発生時の緊急対応体制の整備 #ページ 19 #資料内の具体的な記載内容 緊急時において、被害を最小限に抑えるための迅速対応の態勢を確立するため、以下を実施できるような対応体制（CSIRT）を構築する。 #意見内容 CSIRTの構築についての情報にリーチする手段が掲載されていないため、読み飛ばされる可能性を懸念します。 CSIRT構築に関わるURLを注釈に掲載することを提案します。 参考URL https://www.nca.gr.jp/ https://www.nca.gr.jp/ttc/wtda.html	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
34	該当箇所：　指示5で記載している「サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。」の機能追加に関する提案です。 意見内容：　防御をすり抜けても発症を防止する仕組みの予防を保護対策に含め、防御・予防・検知・分析の仕組みの構築を提案します。 理由：　最近のサイバー攻撃、特にランサムウェアは格段に高機能化しており、防御をすり抜けたマルウェアの活動を検知・分析する時間の余裕がなくなっています。「防御」フェーズと「検知」フェーズの間に「予防」フェーズを取り入れることによって、インシデント化してビジネスが止まってしまう前に予防的な措置をとることが可能になります。本提言は経団連の「NISTのCSF改定案に対する意見」(https://www.keidanren.or.jp/policy/2022/045.html)でも記載されております。	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
35	該当箇所：　指示9で記載されているサプライチェーン全体の状況把握および対策に関するご提案 意見内容：　サプライチェーン全体の中で最低限取るべきサイバーセキュリティ対策ならびに優先順位を明示して頂くことにより、自社システムのビジネス規模、役割、責任範囲を鑑みてセキュリティ対策投資の割合と優先順位が設定できます。 その優先順位はエンドポイント→クラウド→ネットワークであり、対処すべき仕組みは防御→予防→検知→分析とすることが望ましいと考えます。 理由：　企業規模によっては十分なサーバーセキュリティ対策費用が確保できず、防御・検知・分析する仕組みの全てを構築する資金や人的リソースを確保出来ないことが想定されます。一方で防御をすり抜けるケースが多発していることも鑑みると、防御・予防・検知・分析の仕組み(提案1)を参照しながら、最低限とるべき対策の指針と優先順位を提示することでサプライチェーン全体を俯瞰した方策の実効性を高めることに繋がると考えております。 参考資料：経団連サイバーセキュリティ経営宣言 2.0(https://www.keidanren.or.jp/policy/2022/087.html)	御意見は、サイバーセキュリティ経営ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
36	該当箇所：　ＰＩＩ、下線部の「サイバーセキュリティに関する残留リスクを許容水準まで低減する」の記載 意見内容：　許容水準について具体的に記載している項番を明示する目的で、参照すべき指示(例、指示4)の記載を提案します。 理由：　本書がセキュリティ対策に関する経営ガイドラインであり下線部は特に重要な記述であるため「残存リスクの許容水準」を経営者に理解していただく必要があります。指示4に記載しているサイバーセキュリティリスクの把握と対策計画の策定、そして提案1、提案2で記述した最低限の対策や優先順位を関連づけることで残留リスクの把握と許容水準を具体化できるものと考えております。	御意見をもとに、脚注としてサイバーセキュリティ経営の重要10項目のうち指示４を参照すること、及び許容可能水準のとして業界ガイドラインや取引先の要請などを参照すべきことを追記いたします。
37	独立行政法人情報処理推進機構（IPA）が当該ガイドラインをベースとして「サイバーセキュリティ経営可視化ツール」を提供しておりますが、Ver3.0の公開に合わせて「サイバーセキュリティ経営可視化ツール」も更新して頂けると有難いです。「サイバーセキュリティ経営可視化ツール」の更新の予定についてご教示ください。	IPAにおいて年度内に経営ガイドラインの改訂に伴う可視化ツール（Excel版）の更新を予定しております。
38	pl サイバーセキュリティ経営ガイドラインVer3.0 の策定にあたって 文中で「中小企業の情報セキュリティ対策ガイドライン」を紹介しておりますが、参考URLを示したほうが良いと思います。	御意見をもとに、付録B（サイバーセキュリティ対策に関する参考情報）への参照情報を追記いたします。
39	p3 １．１．サイバーセキュリティ経営ガイドラインの背景と位置づけ (4) 本ガイドラインの位置付け 「各種ガイドラインやフレームワークと間に」とありますが、「各種ガイドラインやフレームワークとの間に」の誤記ではないでしょうか。	御意見のとおり、修正いたします。

整理番号	御意見の概要	御意見に対する考え方
40	p.6 2．経営者が認識すべき３原則（1） 解説に「社外とのオンラインでのコミュニケーション」とありますが、 近年ではテレワークの普及に伴い社内でのオンラインコミュニケーションも増加しています。 「社内外のオンラインでのコミュニケーション」としてはいかがでしょうか。	御意見のとおり、修正いたします。
41	p.6 2．経営者が認識すべき３原則（2） 解説に「システム管理等の委託先等」との表現が2回出てきますが、先日の大阪急性期・総合医療センターの事例では、給食委託事業者がランサムウェアの侵入口になったと報道されています。 システムに関する業務委託以外であってもリスクが生じることを強調するために、単に「委託先等」、もしくは「機密情報を取り扱うあらゆる委託先等」などとしてはいかがでしょうか。	御意見をもとに、当該箇所を「システム管理等を含むあらゆる委託先等」に修正いたします。
42	p.7 2．経営者が認識すべき３原則（2） 2014年のSQLインジェクション脆弱性が原因でクレジットカード情報が漏洩した事件や、近年の尼崎USB紛失事件など、関連企業に対する損害賠償訴訟の事例などを交えながら、サプライチェーン全体の危険性を訴求した文書にした方がより説得力が増すのではないでしょうか。	御意見をもとに、当該箇所に脚注を追加するとともに、付録B（サイバーセキュリティ対策に関する参考情報）に被害例の紹介に関する関連情報を追記いたします。
43	p.10 指示２ サイバーセキュリティリスク管理体制の構築 ガイドライン全般にわたり、グローバルな事業展開に対する目配りが不足しているように見受けられます。 海外においては、セキュリティに関する法律や制度が日本とは異なることによるリスクがあり、それに対応する必要があることを、対策例に追記してはいかがでしょうか。 例えば、GDPR（の「72時間ルール」）、中国サイバーセキュリティ法など。	御意見をもとに、サイバーセキュリティ経営の重要10項目のうち指示４における対策例に「サイバーセキュリティリスクの把握にあたっては、自組織のみならず、サプライチェーン全体を通じたリスクを対象とするとともに、サイバー攻撃以外のリスクとして偽情報、機械学習における誤判断、海外での法令違反等も考慮する。」を追記いたします。
44	p.13 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 対策例の「リスクの洗い出し」の例として、「自社での過去の事故事例や、類似する他社事例の分析」を追加してはいかがでしょうか。	御意見のとおり、修正いたします。
45	p.14 3．2．サイバーセキュリティリスクの特定と対策の実装 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 リスク移転策として「クラウドサービスの利用」と記載がありますが、クラウドサービスならリスクを完全に移せる、という誤解を招く可能性があるため「※責任範囲をよく吟味する必要がある。」等の注釈をいれてみてはいかがでしょうか。 ※サイバー保険についても同様のことが言えるかと思います。	御意見を踏まえ、当該箇所に脚注として「クラウドサービスの利用及びサイバー保険の加入のいずれも、自社が負うリスクをゼロにするものではなく、それぞれの効果と責任範囲を把握した上で実施を検討する必要がある」を追記いたします。
46	p.15 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 No8とも関連しますが、昨今クラウドサービスの設定不備による情報漏洩事故が多発してますので、対策例として以下の一文を追記してはいかがでしょうか。 -クラウドセキュリティ診断を実施して、クラウドのセキュリティ設定の不備の検出、および対処を行う。	御意見をもとに、当該箇所に脚注を追加するとともに、付録B（サイバーセキュリティ対策に関する参考情報）にクラウドサービスのセキュリティ対策に関する関連情報を追記いたします。
47	p.17 指示６ PDCAサイクルによるサイバーセキュリティ対策の継続的改善 対策を怠った場合のシナリオに、「経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。」に対応するものがありません。 以下のようなシナリオを追加してはいかがでしょうか。 ----- 定期的な報告等を受けておらず、経営者自身がリスクや問題を把握できていない場合、現場では予算や人材の不足を理由に対策が疎かにされるおそれがある。	御意見をもとに、当該箇所に「定期的な報告等を受けておらず、経営者自身がリスクや問題を把握できていない場合、適切なセキュリティ対策が実施されず、サイバー攻撃を受けるおそれがある。」を追記いたします。

整理番号	御意見の概要	御意見に対する考え方
48	p.18 指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善 No8,9と関連しますが、昨今の時代背景も考慮し、「脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービス」に限定せず、 「脆弱性診断・ペネトレーションテストやクラウドセキュリティ診断、情報セキュリティ監査等の外部サービス」としてはいかがでしょうか。	御意見をもとに、当該箇所を「目的に応じた脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービス」に修正いたします。
49	p.23 指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策 自社が委託元である場合だけでなく、逆の観点、すなわち委託先となる場合についても触れてはいかがでしょうか。 例えば、「他社から業務委託等を受ける場合には、契約時に委託元と合意したセキュリティ要求を遵守する必要や責任がある」など。	御意見をもとに、サイバーセキュリティ経営の重要10項目のうち指示 9 における対策例に「他社から業務委託等を請ける場合には、契約時に委託元と合意した情報の取扱いなどのセキュリティ関連の要求事項を遵守する。」を追記いたします。
50	p.24 指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策 対策例に、「緊急時に備え、委託先に起因する被害に対するリスクマネーの確保として、委託先に対してサイバー保険への加入を推奨する。」とありますが、 「リスクマネー」という単語を用いるのは妥当でしょうか？ 「回収不能となるリスクがある投資資金」といった意味であるため、ガイドラインで意図した意味合いになっていないように思われます。	御意見を踏まえ、「委託先に起因する被害に対するリスクマネーの確保として」と記載していたものを「委託先に起因する被害に対する補償手段の確保として」に修正いたします。
51	（該当箇所） P.6 2. (1) 1ポツ （意見） 「・・・、対策 の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減 することは、経営者としての責務である。」の「許容水準まで低減」はあたかも一般的な水準が存在するかのようにも受け取れるので、「自社が受容可能とする水準まで低減」と記載することをご提案いたします。 （理由） 前段で、「サイバーセキュリティ対策は企業活動におけるコストや損失を減らすための必要不可欠の投資である」とありますように、リスク低減対策とリスク受容の関係は各企業の戦略になりますので、一般的な水準(妥当であったとしても)を達成すればそれで良いという誤解を与えてしまうのではないか、懸念されますため。	御意見をもとに、当該箇所を「自社が許容可能とする水準まで低減」に修正いたします。
52	（該当箇所） P.7 2.(2) 3ポツ （意見） 「・・・、自社のみならず、サプライチェーンのビジネスパートナーやシステム管理等の委託先等、サプライチェーン全体を俯瞰し、総合的なセキュリティ対策を徹底することが必要である。」の「サプライチェーン全体を俯瞰」は、主語がサプライチェーンの頂点の企業である立場を連想させるので、「サプライチェーンの一端を担う企業として全体を意識し」と記載することをご提案いたします。 （理由） サプライチェーンの頂点以外の企業、上流・下流、企業の大小に関係なくサプライチェーン問題を意識して取り組んで頂くことが必要だと考えられますため。	御意見を踏まえ、当該箇所を「サプライチェーンの一端を担う企業として全体を意識し」に修正いたします。
53	（該当箇所） P6 2.(1) 2ポツ （意見） 以下の通り""の箇所を追記することをご提案いたします。 「サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった場合には、 "個人情報保護法違反による罰則や人命への影響が発生する可能性があるため" 企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。」 （理由） 個人情報保護法および人命への記載を追記することにより、迅速かつ適切な対応の必要性が伝わりやすいと考えられますため。	御意見を踏まえ、当該箇所を「サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった場合には、人命への影響や法令違反が発生する可能性があるため、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。」に修正いたします。

整理番号	御意見の概要	御意見に対する考え方
54	（該当箇所） P6 2.(2) 1ポツ （意見） 以下の通り""の箇所を追記することをご提案いたします。 「デジタル技術の業務利用が普及した環境において、サプライチェーンには在来形の部品調達などの形態や規模にとどまらない、クラウドサービスの利用、 "モバイルデバイスやモバイルアプリの利用、" 情報を扱う機器の保守や情報を記録した媒体の廃棄のような、デジタル環境を介した外部とのつながりの全てが含まれ、かつこれらのつながりは時と共に刻々と変化するなど非定型である。」 （理由） デジタル環境の活用を前提とする場合、モバイルデバイスやモバイルアプリに対するセキュリティ対策も必要となるためサプライチェーン全体として目配りの対象として明記することが望ましいと考えられますため。	御意見を踏まえ、当該箇所を「デジタル技術の業務利用が普及した環境において、サプライチェーンには在来形の部品調達などの形態や規模にとどまらない、クラウドサービスやモバイルデバイスの利用、 情報を扱う機器の保守や情報を記録した媒体の廃棄のような、デジタル環境を介した外部とのつながりの全てが含まれ、かつこれらのつながりは時と共に刻々と変化するなど非定型である。」に修正いたします。
55	（該当箇所） P21 対策を怠った場合のシナリオ 1ポツ （意見） 以下の通り""の箇所を追記することをご提案いたします。 「重要な業務が適切な時間内に復旧できないことで、企業経営および "顧客や取引先等" に致命的な影響を与えるおそれがある。 」 （理由） 指示8ではサプライチェーンを含めたインシデントによる被害を取り扱っているため、対策を怠った際の影響範囲として顧客や取引先等を含めることが望ましいと考えられますため。	御意見を踏まえ、当該箇所を「重要な業務が適切な時間内に復旧できないことで、顧客における重大な被害、さらには自社の経営に致命的な影響を与えるおそれがある。 」に修正いたします。
56	該当箇所 ３．２．サイバーセキュリティリスクの特定と対策の実装　 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 「対策例」から暗号化についての記述 意見内容 「営業秘密や機微性の高い技術情報、個人情報などの重要な情報については暗号化や電子署名など、情報を保護する仕組みや、改ざん検知の仕組みを導入する。」 　上記記述に対し、暗号化の定義を明確化 理由 一般的に機密情報の暗号化保護というとパスワードにより解除できるシステムを想定される方が多くいると思われます。しかし、パスワード設定は ・一定の桁数以上でないと容易に解析可能であること ・使い回しを避け、ファイル毎に個別のパスワードを設定する必要があるが、それを実行するには運用への負荷が大きいこと ・暗号化する、しないが個人の判断に委ねられ、組織として情報の管理と共有ができないこと ・ファイル利用のために復号する必要があり、通常の平文と同じ保護のかからない状態に戻ってしまうこと などから、適切なデータ保護の手段とならない可能性があります。それ故、例えば ・個人情報保護法の表現に従い、高度な暗号化（電子政府推奨暗号化技術の使用、暗号鍵の適切な管理等）等による秘匿化を行う ・パスワードに頼らない暗号化技術を用いる ・機微情報へのアクセスを必要な者のみに制限し、またアクセス可能な者も任意に復号し持ち出せないよう常時暗号化する仕組みを導入する。 などの表現を加え定義を明確化することで、経営者がより実効性のある暗号化を選択できるようにするのがよいと考えます。	御意見はを踏まえ、暗号化に関する脚注を加えるとともに、付録E（用語の定義）の改訂に当たって関連情報を追記いたします。
57	・該当箇所 １．はじめに １．１．サイバーセキュリティ経営ガイドラインの背景と位置づけ (1)サイバーセキュリティを包含するリスクマネジメントの必要性 ・意見内容 過失・内部不正への言及 ・理由 現行の「サイバーセキュリティ経営ガイドラインVer2.0」 「付録E 用語の定義」 （4） サイバーセキュリティ サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。 上記の定義からサイバーセキュリティリスクにはサイバー攻撃、過失、内部不正のすべてのリスクを含むと解釈しますが、該当箇所では特にサイバー攻撃について言及しており、その他のリスクにスコープが当たっていないように感じられます。 特に内部不正による漏洩は損害額も大きくなりやすく、事業経営にも直結します。 経営層が組織として内部統制の構築と強化を実行することで対策していくべき問題であることを喚起する必要があると考えます。	御意見は、付録E（用語の定義）の改訂に当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
58	意見１ ＜該当箇所＞ P9の指示1の対策例3点目 ＜意見内容＞ 「セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。」の文言を、「セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。なお、対外的に公開するセキュリティポリシーは付録のセキュリティポリシー例に則ったものとする」に修正し、付録にセキュリティポリシーの例示を載せてはどうか。 ＜理由＞ ステークホルダーに企業のサイバーセキュリティに対する姿勢を示すためには、ある程度項目・内容が統一されていた方が、ステークホルダー側の理解も進み、企業も他社との比較により、自社のセキュリティポリシーが十分かどうかを把握し、対策することでサイバーセキュリティに対する好循環が生まれると考えるから。	御意見をもとに、当該箇所に脚注を追加するとともに、付録B（サイバーセキュリティ対策に関する参考情報）に関連情報を追記いたします。
59	意見２ ＜該当箇所＞ p11 対策例4点目 ＜意見内容＞ 「事業の現場業務の遂行の過程でセキュリティ対策に配慮する必要がある人材を対象に」は「全従業員に」でよいのではないか。 ＜理由＞ p6の(1)1項目に記載の通り、現代の多くの企業は企業活動のあらゆる部分をデジタル環境に依存している。このような状況で、「セキュリティ対策に配慮する必要がある人材」は一部の人に限定されるべきではなく、すべての従業員がセキュリティ対策を意識することが必要であると考える。限定的な記載をしてしまうと、従業員へのセキュリティ教育の浸透を遅らせる懸念もあるため、ガイドライン上は対象を広くすべきである。	御意見を踏まえ、当該箇所を「セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門等のあらゆる業務に従事する人材に、「プラス・セキュリティ」知識・スキルの習得を促す。」に修正いたします。
60	意見３ ＜該当箇所＞ P13の指示4の対策例 ＜意見内容＞ 「サイバーセキュリティに関する最新情報の収集」および「最新情報の参照先」を対策例に追記してはどうか ＜理由＞ 企業のサイバーセキュリティ対策としてはリスク管理体制やインシデント発生後の対応などサイバー攻撃を想定した包括的なセキュリティ計画を立てることが重要であると捉えている。一方で、サイバー攻撃の手段は一様ではなく、かつ時々刻々と攻撃手段がアップデートされ、計画策定段階で最新の情報を踏まえることが重要である。したがって、指示10の「サイバーセキュリティに関する情報の収集、共有及び開示の促進」だけでなく、計画策定段階である指示4でも『サイバーセキュリティに関する最新情報の収集』をガイドラインの対応例などに明記しても良いと考える。また、企業がどこから最新情報を入手すればよいか分からないことも想定されるため、政府（または政府推奨）の情報源を指定または策定してもらえると企業も活用しやすいと考える。（例えば、『IPAが公開している「〇〇（情報源）」を参照してもらうとよい』といった感じで）	御意見をもとに、当該箇所に脚注を追加するとともに、付録B（サイバーセキュリティ対策に関する参考情報）に脅威に関する情報源情報を追記いたします。
61	意見４ ＜該当箇所＞ P15の指示５の対策例1点目 ＜意見内容＞ 「クラウドサービスを利用する際には、クラウドサービスにおいて提供されるセキュリティ機能を考慮した選定を行い」の文言を「クラウドサービスを利用する際には、付録のチェックリストを参考にし、クラウドサービスにおいて提供されるセキュリティ機能を考慮した選定を行い」といったように修正し、付録にクラウドサービス選定の際のチェックリスト（またはクラウドサービス選定時の参考情報）を添付してはどうか。 ＜理由＞ 企業のセキュリティ対策を万全にしていても、クラウドサービス側のしっかりとしたセキュリティ対策が講じられていないと、企業のセキュリティ対策も万全とは言えなくなるため、クラウドサービス選定には注意が必要である。一方で、企業としてはクラウドサービス選定の際にどのような注意をすべきなのか分かり兼ねる場合もあるため、ガイドラインにクラウドサービス選定の際の注意点（チェックリスト）を含めてもよいと考える。	御意見をもとに、当該箇所に脚注を追加するとともに、付録B（サイバーセキュリティ対策に関する参考情報）にクラウドサービスのセキュリティ対策に関する関連情報を追記いたします。
62	【提出意見の背景となる考え方・全体像について（協力をベースとしたセキュリティ向上の規範としての本文書の意義を支持）】 　デジタル時代の日本の国際競争力の強化において、日本におけるセキュリティレベルを向上させ、国際的にも通用する「信頼」を確実にすることが不可欠です。そのためには、B2C,B2Bを問わず社会のすべてのステークホルダーがサイバーセキュリティの当事者として協力しあうことが必要と考えます。その中でもメインプレイヤーである民間企業の役割は大きく、サプライチェーンにつながるすべての企業の経営者が共有すべき規範として、本経営ガイドラインは有効です。従って、協力をベースとしたセキュリティ向上のためにこの文書を支持します。 　前書きにてVer. 2 .0以降の環境の大きな変化について、６点、リストアップ頂いていますが、国内に閉じないサプライチェーン、委託受託関係の増大と多様性を前提としていることがわかると、よりこの文書の効果が高くなると存じます。	御意見を踏まえ、「サプライチェーンを介した」と記載している箇所を「国内外のサプライチェーンを介した」に修正いたします。

整理番号	御意見の概要	御意見に対する考え方
63	1．P.I　「サイバーセキュリティ経営ガイドラインVer.3.0の策定にあたって」 ランサムウェアの被害の説明～確認と重要性の強調提案 ランサムウェアの被害について取上げて頂いたことを支持します。更に経営者に経営リスクとしての実感を持ってもらうために、企業の事業活動の停止だけでなく、暗号化されシステムが長期間使えなくなること、事前に窃取された開示されたくない情報を晒すと脅され得ること、犯罪集団に身代金を支払わざるを得なくなること、これによる取引先への損害、レピュテーションリスクなど、サイバーセキュリティへの取組は信用問題である点も言及して頂ければ理解されやすいと存じます。	御意見を踏まえ、ランサムウェアに関する脚注を加えるとともに、付録E（用語の定義）の改訂に当たって関連情報を追記いたします。
64	地政学的リスクにつきましても、おそらく意図されているように存じますが、明示した方がより実感を持ってもらえると存じます。	御意見を踏まえ、本書において扱うリスクの例に地政学リスクを追加し、サイバーセキュリティ経営の重要10項目のうち指示4、指示9及び指示10の対策を怠った場合のシナリオ、対策例等に反映いたします。
65	P.2　「本ガイドラインの対象者と責任」 支持と確認 インシデント事例を見ると、海外子会社から入られて攻撃を受けている例が多くみられます。今回は明示されておりませんが、海外子会社に対するガバナンスについても、この文意に含まれると解釈できるでしょうか？できれば明示的に言及頂ければ効果的かと存じます。	御意見を踏まえ、経営者が認識すべき３原則（２）及びサイバーセキュリティ経営の重要10項目のうち指示9において、「国内外の拠点、ビジネスパートナー」が対象であることを示す追記を行うことでグローバル展開時のリスクも考慮に含めるべきことを明確化いたします。
66	P.6　2．経営者が認識すべき３原則　（１）明確化の検討提案 セキュリティは経営課題として重要なリスクマネジメントであり、（絶対を求めるのではなく）「残留リスクを許容水準まで低減することは経営者の責務である」、と明示されたことは、日本のセキュリティの特殊性を是正する観点からもとても重要だと支持させて頂きたいと存じます。日本の企業はセキュリティとはリスク回避と考え守りのセキュリティになりがちであり、データ活用も躊躇しがちですが、この明示によって、少し理解が進むと存じます。	本ガイドラインの改訂方針に関する肯定的意見として承ります。
67	関連して、海外の会社は、デジタル活用で打って出るにあたり信用を得るための「攻めのセキュリティ」に取組んでいますので、Ver.2.0にあった、ITを利活用して企業の収益を生み出す上でもセキュリティが重要な要素となることも、残して頂くのが良いのではないかと存じます。	御意見を踏まえ、御指摘の箇所に「サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）」である旨を追記し、解説全体の内容の調整をいたします。
68	経営リスクマネジメントとしての取組を強調されることは重要であり、支持します。一方、日本企業には2000年代からプライバシーマークなどの認証を取得し、「認証を持っているから大丈夫」と安心して、形骸化した運用をしつつ時代遅れの対策を継続している所も少なくないように思います。リスクマネジメントは脅威の変化に応じて不断の見直しを要求するものであることに言及し、セキュリティの脅威が大きく変わったことを踏まえ、形骸化していないか、実質的な再点検を促す記述があると、より効果的かと存じます。	御意見を踏まえ、サイバーセキュリティ経営の重要10項目のうち指示４の対策例に、「リスクマネジメントは脅威の変化に応じて不断の見直しを要求するものであり、自組織におけるリスクとその対応方策が形骸化していないか、定期的な確認を行う。」を追記いたします。
69	P.6　2．経営者が認識すべき３原則　（２）明確化の検討提案 前述のとおり、海外の会社の脆弱性から被害に遭うことがありますので、サプライチェーンがグローバル化していることにも留意し、海外の委託先やネットワークでつながる顧客に対しても目配りすることについて、注意を促されると、より効果的かと存じます。	御意見を踏まえ、当該箇所を「サプライチェーンとしてつながる国内外の拠点、ビジネスパートナーやシステム管理等を含むあらゆる委託先等においてサイバー攻撃への対策が不十分であった場合、それらのセキュリティが弱い組織を踏み台にしたサイバー攻撃による重要情報の流出等、サプライチェーン全体の機能が停止するのみならず、自社にも甚大な被害をもたらす等の問題が生じうる。」に修正いたします。
70	指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定（p.13） 【賛同】「対策を怠った場合のシナリオ」の改定（以下の記述）に賛同します。 「・サイバーセキュリティリスクは企業の事業内容や組織形態によって異なる。自社のサイバーセキュリティリスクのアセスメントを行うことなく、他社の事例やベンダからの提案などを参考に実態にそぐわないリスク対応計画を策定した場合、未対策のリスクによる事業の中断や機密情報の漏えいなど、経営上許容できない損失が発生するおそれがある。」	本ガイドラインの改訂方針に関する肯定的意見として承ります。
71	指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築（p.15-p.16） 対策例にある、「・自社内で対策実施に必要なスキルを有する人材を確保できない場合は、専門サービスを提供する外部事業者を活用する。」について 【お願い】前段のセキュリティの取り組みの記述及び後述される「情報セキュリティサービス基準適合サービスリスト」に対応し、「サービスの選定」ではなく、「情報セキュリティサービスの選定」に統一頂きたい。	御意見を踏まえ、当該箇所を「自社内で対策実施に必要なスキルを有する人材を確保できない場合は、専門の情報セキュリティサービス等を提供する外部事業者を活用する。」に修正いたします。
72	指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築（p.15-p.16） 対策例にある「・従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。」について 【質問】従業員に対する教育に関する記述が減ったのは、指示7と指示８の演習の記述を重視したためでしょうか。	Ver2.0改訂後、新たに付録F『F)サイバーセキュリティ体制構築・人材確保の手引き』を作成し、教育関連の内容を当該付録に集約しております。

整理番号	御意見の概要	御意見に対する考え方
73	指示６ PDCA サイクルによるサイバーセキュリティ対策の継続的改善（p.17-p.18） 対策例にある「・サイバーセキュリティリスク管理に関するKPI を定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する。KPI としては、リスク対応に関するパフォーマンスの評価の観点から、次のような指標が考えられる。」について 【お願い】例示されている指標の5項目が業種・業界、企業規模、情報システム基盤により、大きく異なると考えられ、KPI（Key Performance Indicator）として適切な例示なのか、またはKGI（Key Goal Indicator）が示されているのか、ご確認頂きたい。	例示については条件に応じて適切な指標が異なってくるところ、御意見も踏まえ、読者の誤解を生じさせぬよう「KPI としては、リスク対応に関するパフォーマンスの評価の観点から、次のような指標が考えられる。」と記載していたものを「KPI としては、リスク対応に関する組織内パフォーマンスの評価の観点から、次に例示するような指標が考えられる。」に修正いたします。
74	指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策（p.24） 対策例にある「緊急時に備え、委託先に起因する被害に対するリスクマネーの確保として、委託先に対してサイバー保険への加入を推奨する。」について 【お願い】サイバー保険の活用は、法人組織におけるセキュリティ意識の醸成やインシデント対応の重要性を訴求するだけではなく、インシデント発生時の初動対応に係る初期費用の支払いを補填できるなど、幅広い効果をもたらすものと理解しています。 反面、サイバー保険は、この文章が意図するほどの広範囲の補償は行われておらず、調査費用等が負担されることが一般的で、復旧費用や損害賠償への対応は補償の範囲外となっていますので、サイバー保険の活用については、各事業者により選択できるものであると考えています。よって、文章の意図に合わせた修正が必要ではないかと考えます。 尚、リスクマネーという言葉の意味（リスクをとって高いリターンを狙う短期の資産運用を行う資金。）は、この文中に使用することが適切であるかどうかは再検討頂ければと思います。 更に、「委託先に対してサイバー保険への加入を推奨する」という書き方は、発注者側として委託先にサイバー保険の加入を要求するように読み取れますが、委託先への要求もあるとは思いますが、まずは自衛策の1つとして自社で保険を掛けることが重要ではないかと考えます。そこで、この一文については、本来の意図に合わせた書き換えが必要であると思います。	御意見を踏まえ、当該箇所を「緊急時に備え、委託先に起因する被害に関する補償手段の確保として、委託先に対してサイバー保険への加入を推奨する。」に修正するとともに、サイバー保険に関する脚注を追記いたします。
75	指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策（p.24） 対策例にある「・サプライチェーンにおけるサイバーセキュリティ対策を担保する手段として、第三者による評価検証結果を活用する。」について 【お願い】第三者による評価検証結果を活用する、というのは、自社が評価を受けてアピールするのか、取引先を評価するのかどちらの意味か、また、活用して対策を担保する、という意味がちょっと分かりにくく思います。 また、評価検証結果についても「助言型」では不十分であるというように読み取れますが、ここでは「保証型」を意図していますでしょうか。	ここではサプライチェーンにおけるセキュリティ対策が意図したとおりに措置されているかどうか等を担保する手段の一つとして、保証型に限定されない第三者による評価検証結果を活用していくことを意図しておりますところ、御意見を踏まえ、「（認証制度の活用、助言型外部監査の実施等）」を追記いたします。
76	- 該当箇所 経営者が意識すべき3原則：サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要 - 内容 「セキュリティが弱い組織を踏み台にしたサイバー攻撃による重要情報の流出等」により「自社に被害が出る」ことを強調する記述となっているが、後述の「サイバーセキュリティ経営の重要10項目：指示9」とも連動する様に「自社が加害者になる」点も含めた記述として欲しい。 - 理由 「経営者の責任」として、自社を守るという観点も重要だが、法令遵守などを含め「社会に迷惑を掛けない」という観点も非常に重要であり、自社の責任の範囲内で留まる話ではない（有事の際に自社だけの被害に留まらない）ことを強く意識すべきと考えている。	御意見を踏まえ、「サプライチェーンとしてつながる（中略）問題が生じうる。」の記載に続けて「また、自社の対策不十分が原因である場合、自社がサプライチェーンの他企業にとっての加害者の立場になる。」を追記いたします。
77	- 該当箇所 経営者が意識すべき3原則：関係者との積極的なコミュニケーションが必要 - 内容 例えば「セキュリティチェックシート」の様なものを定期的に依頼するなどの「継続的に実施が出来る具体的な取り組み例」を示し、それをきっかけにコミュニケーションを図ることを勧奨する記述として欲しい。 - 理由 「サイバーセキュリティ経営の重要10項目：指示9」と繋がる部分も有るが「情報共有」勧奨の単語のみ、或いは「スポットでの確認（例：契約時・購買時・宣言の有無確認など）」に留まっている一方で「情報共有」或いは「コミュニケーション」はきっかけ、或いは「アジェンダ」の様なものが存在しないと生まれないものだと考えている。	御意見は、付録A（サイバーセキュリティ経営チェックシート）の改訂に当たって参考にさせていただきます。

整理番号	御意見の概要	御意見に対する考え方
78	- 該当箇所 経営者が意識すべき3原則：関係者との積極的なコミュニケーションが必要 - 内容 「関係者」の中に「サイバーセキュリティ経営の重要10項目：指示10」に記載が有る様なIPA、JPCERT/CC、商工会議所などはもちろん、セキュリティ関連事業者なども含めた記述として欲しい。 - 理由 「経営者」はどこまで行っても「セキュリティのプロフェッショナル」ではなく、その意味では「よく分からないもの」のリスクだけを背負ってリーダシップを発揮することは難しいと考えており、また実態として「意識・ヤル気」は有り「丸投げ」する気は無いけれども「相談したい」という様に考えている経営者が多いことを考えると「相談先」の例として、幾つかの機関を挙げておいて頂きたいと考えている。 経営者に「全てを背負わせず」に社会としての「セーフティネットが存在する」ことを示したいと考えている。 セキュリティ市場の活性化にも繋がると考えている。	御意見を踏まえ、当該箇所を「このときの関係者には、社内であればCIO等のセキュリティ担当者のみならずセキュリティ対策を実施すべき担当者を含み、社外ではサイバーセキュリティ関連情報を扱うIPA、JPCERT/CC、商工会議所等などはもちろん、セキュリティ関連製品・サービスの事業者等を含む。」に修正するとともに、サイバーセキュリティ経営の重要10項目のうち指示10の対策例についても、「IPA や一般社団法人 JPCERT コーディネーションセンター等による脆弱性情報など の注意喚起情報を、自社のサイバーセキュリティ対策に活かす。」と記載していたものを「IPA や一般社団法人 JPCERT コーディネーションセンター等による脆弱性情報などの注意喚起情報や、セキュリティ関連製品・サービスの事業者等とのコミュニケーションを、自社のサイバーセキュリティ対策に活かす。」に修正いたします。
79	- 該当箇所 サイバーセキュリティ経営の重要10項目：指示4 - 内容 リスク把握、リスクの洗い出し方法として「CPSFの参照」を勧奨しているが「可視化ツール」「5分自社診断」などの方が現実的なケースも存在すると思われるので、そちらの記述もお願いしたい。 - 理由 中小企業のほとんどでCISOなどが設置されておらず、経営者、或いは兼任で社員が対処していることが多い実態を考えると、より簡単に分かり易い方法で「自社状況」の把握を勧奨した方が良いと考えている。	御意見を踏まえ、当該箇所を「付録B に示す「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」及び「サイバーセキュリティ経営可視化ツール」等」に修正するとともに、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
80	- 該当箇所 サイバーセキュリティ経営の重要10項目：指示5　対策を怠った場合のシナリオ - 内容 サイバー攻撃を防げず、発生した場合に事業継続に影響する可能性が有ることはもちろん、2次被害など、自社だけに留まらず社会全体に影響を与える可能性が有ることを記載して欲しい。 - 理由 サイバー攻撃数が増加し、かつ攻撃の対象や手法が多様化している現状において、攻撃被害が自社だけに留まらず、社会全体に対して影響を与える可能性が有ることを、ここでも強調していただきたい。 例えば、会員制のECサイトを用いてサービスを提供している会社であれば、会員情報が漏えいした場合に自社で不正利用される可能性があることは当然だが、同じID・PWを利用している一般消費者が多いという実態から鑑みても、他社に対するリスト型攻撃に発展し、被害の範囲は社会全体に波及する可能性が有る。自社にしか迷惑が掛からないという表現のままではサイバー攻撃に対する対策は進まず、社会全体として取り組む課題であることを認識してもらうためにも、記載した方が良いと考える。	御意見を踏まえ、当該箇所を「指示４を通じて明らかにされたサイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃を防げず、発生した場合の事業継続に影響する可能性があるのみならず、個人情報の漏えいや他社に対するサイバー攻撃への発展など社会全体に影響を与える可能性がある。」に修正いたします。
81	- 該当箇所 サイバーセキュリティ経営の重要10項目：指示5　対策例 - 内容 IPAが公表している『安全なウェブサイトの作り方（https://www.ipa.go.jp/files/000017316.pdf）』や『セキュリティ実装 チェックリスト』を参考に、セキュリティを考慮したWebサイトの制作を行うべき旨、並びにWeb Application Firewall（WAF）導入を対策の一つとして追加していただきたい。 - 理由 サイバー攻撃被害の実態の1つとして、DDoS攻撃や不正アクセスによるWebアプリケーションの改竄事例など、Webサイトがきっかけ・対象となっていることが多いにもかかわらず、ITリテラシーの高くない経営者であればあるほど「サイバー攻撃＝ウイルス感染のみ」というイメージが強く、PCなどのデバイスやBEC（ビジネスメール詐欺）への対策にばかり目が行きがちとなっている。自社が保有しているWebサイトに対策が必要だと認識していない経営者が多い現状を変えるためにも、自社のWebサイトも攻撃の対象、或いは他社に被害を与える踏み台になり得ることを明示していただきたいと考えている。 また、SQLインジェクションやクロスサイトスクリプティング（XSS）などを起因とした被害がいまだに多く発生している現状に対し、脆弱性を検出・対処するだけでなく、Web Application Firewall（WAF）の導入によりリスクを低減することを対策方法の1つとして明示することが、被害減少に繋がるのではないかと考えている。	御意見は、付録B（サイバーセキュリティ対策に関する参考情報）の改訂に当たって参考にさせていただきます。
82	- 該当箇所 サイバーセキュリティ経営の重要10項目：指示9 - 内容 「対策例」に加害者とならない為の例も挙げて欲しい。例えば、改竄された請求書の貼付けによるBEC（ビジネスメール詐欺）被害の誘発や、Webサイト改竄による個人情報の漏洩誘発など。 - 理由 「加害者にもなり得る」記載が有る一方で「対策例」に当該事項に関する対策事例が触れられていない。	御意見を踏まえ、付録B（サイバーセキュリティ対策に関する参考情報）に加害者とならない為の例をまとめた情報源を掲載するとともに、「加害者となるおそれもある」の箇所の脚注で付録Bの情報源を参照するようにいたします。

整理番号	御意見の概要	御意見に対する考え方
83	- 該当箇所 サイバーセキュリティ経営の重要10項目：指示10 - 内容 「対策例」として、サーバ提供事業者やWebサイト制作事業者などとの密な連携を記載して欲しい。 - 理由 特に中小企業の場合、何かインシデントが生じた際には当該事業者を頼るケースが多く、当該事業者にはその際に得た情報を「インシデント情報収集機関」へ連携していくことを促していくことで、社会全体としてサイバー攻撃被害を「もっと身近なもの」にしていく動きが必要だと考えている。 根本的に「サイバー攻撃被害」が身近な例として挙がって来ない為、何処まで行っても「対岸の火事」として、サイバー攻撃対策を実施しない企業（経営者）が大多数であると考えている。	御意見を踏まえ、対策例に「サーバ提供事業者やWebサイト制作事業者など、自社事業に関わる外部の事業者等と日常からサイバーセキュリティ関連情報の共有等に関して積極的な連携を行う。」を追記いたします。
84	1.グローバルな視点の追加 今次改定案では全編を通じて、「国境を越えたサイバーセキュリティリスク・対策」といった観点がやや希薄ではないか。「経団連サイバーセキュリティ経営宣言2.0」にも現状認識を示しているとおり、取引先や海外子会社等のサプライチェーンを経由したサイバー攻撃が増加傾向にある中、サプライチェーン全体を俯瞰したサイバーセキュリティ対策の強化にあたっては、グローバルな視点を盛り込むことが不可欠ではないか。	御意見を踏まえ、経営者が認識すべき３原則（２）及びサイバーセキュリティ経営の重要10項目のうち指示9において、「国内外の拠点、ビジネスパートナー」が対象であることを示す追記を行うことでグローバル展開時のリスクも考慮に含めるべきことを明確化いたします。
85	2.多様な経営リスクにおける位置づけの敷衍 「経営者が認識すべき3原則」の一つとして、「・・・サイバーセキュリティリスクを多様な経営リスクの中での一つとして位置づけ、・・・」（6頁）と記載されているが、企業が実行に移すにあたっては、例えば以下のように、より具体的に踏み込んだ内容とする必要があるのではないか。 ➢どのような経営リスクと同列に扱うべきか（例：為替変動、天変地異、エネルギー価格高騰　等） ➢どのような粒度で判断すべきか（例：IT系・OT系を峻別して考えるべきか、ランサムウェアとDDoS攻撃を同列で扱うべきか　等） ➢対策を推進する際に、経営者として何を判断すべきか（例：リソース配分の優先度　等） ここまで踏み込んで記載したうえで、別途「手順・ツール」で具体的なツールを提示することによって、経営ガイドラインの実効性が高まるのではないか。	御意見をもとに、それぞれ以下のように修正いたします。 （経営者が認識すべき３原則（１）の解説） 文中で「多様な経営リスク」と記載している箇所を「多様な経営リスク（例：自然災害、地政学的事象、為替や原料価格の変動　等）」に修正いたします。 （サイバーセキュリティ経営の重要10項目のうち指示４の対策例） 文中で「リスク源」と記載している箇所を「リスク源（例：CPSFの添付Bに記載されている「システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染、正規ユーザによる内部不正」等）に修正いたします。 （概要Ⅲ冒頭の説明） 「単に指示すればよいのではなく、組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが求められる。」と記載している箇所を「単なる指示ではなく、組織のリスクマネジメントの責任を担う経営者が自らの役割としてリスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが含まれる。」に修正いたします。
86	3.「事業継続」に関する記述の追加 事業サイドと情報システム・セキュリティ担当者の間の日常のコミュニケーションが重要であるという認識を踏まえ、「経営者が認識すべき3原則」の（3）の記述（Ⅲ頁）を以下のとおり変更しては如何。 変更前：「・・・社内の関係者（CIO等セキュリティ担当者、事業担当責任者等）にサイバーセキュリティ対策に関する情報開示を行うことなどで・・・」 変更後：「・・・社内の関係者（CIO等セキュリティ担当者、事業担当責任者等）にサイバーセキュリティ対策に関する情報開示や事業継続に関して定期的な検討を行うことなどで・・・」	御意見を踏まえ、「社内の関係者（CIO 等セキュリティ担当者、事業担当責任者等）にサイバーセキュリティ対策に関する情報開示を行うことなどで」と記載していたものを「社内の関係者（CIO 等セキュリティ担当者、事業担当責任者等）に事業継続に加えてサイバーセキュリティ対策に関する情報開示を行うことなどで」に修正いたします。
87	4.「サイバー保険」に関する記述の追加 指示４および指示９にサイバー保険の活用を推奨する記載があるが、サイバー保険のカバー範囲が必ずしも被害の全体でないこと、国家レベルの攻撃の場合は戦争扱いとなり、被害に対する補償が支払われない可能性があることを注記する必要があるのではないか。	御意見を踏まえ、指示９における「緊急時に備え、委託先に起因する被害に対するリスクマネーの確保として、委託先に対してサイバー保険への加入を推奨する。」と記載されている箇所を「緊急時に備え、委託先に起因する被害に対する補償手段の確保として、委託先に対してサイバー保険への加入を推奨する。」に修正するとともに、サイバー保険に関する脚注を追記いたします。