別紙１

「サイバーセキュリティ対策情報開示の手引き（案）」に提出された意見及び
その意見に対する情報開示分科会の考え方
（意見募集期間：令和元年 5 月 18 日～令和元年 6 月 6 日）

提出意見：３者
　法人：１者

　個人：２者
　　（個人 A,B）

【総論】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見１　企業に対してサイバーセキュリティ対策を促すよりも先に政府がサイバーセキュリティ対策を強化するべきではないのか。	考え方１	
○　「総務省サイバーセキュリティ統括官室」が提唱している内容では、企業に対して、サイバーセキュリティ対策を導入では、「運用及び管理」での監督する側の「知識（ノウレッジ）」及び「技能（テクニック）」から成る「能力（プラクティック）」を向上する為に、当初では、「国家主権側（官公庁側）」に対し、サイバーセキュリティ対策を導入する事が必要と、私は考えます。 【個人 A】	貴重なご意見として今後の参考とさせていただきます。	無
意見２　日本政府のサイバーセキュリティ対策が不十分で社会に混乱を起こすような問題が生じた場合、日本政府が責任を負うべきである。	考え方２	
○　日本国における企業がサイバーセキュリティ対策を怠り、社会に混乱を招いても、日本政府の責任を逃れる為には、政策を高度化し、企業に対し、監督を促し、企業が「問題（トラブル）」が起きれば、企業側を見捨てる方法が望ましいと、私は考えます。国家主権側が国民主権側の企業に対して、サイバーセキュリティ対策の教育を施すと無駄な財政コストが掛かるので、国家側は、国民側に対し、サイバーセキュリティ対策の監督を施し、国	貴重なご意見として今後の参考とさせていただきます。	無

民側の企業が問題が起きれば、企業側を自業自得として、「破産（バンクラプト）」しても、企業側を見捨てる事が望ましいと、私は考えます。要するに、日本政府がサイバーセキュリティ対策が不十分で、社会に混乱を起こす様な「問題（トラブル）」が生じれば、日本政府に自業自得として、責任を負わす事が望ましいと、私は考えます。 【個人 A】		
意見３　「手引き」の中で模範的なプライバシーポリシーの具体例および、該当社名を挙げていただきたい。	考え方３	
○　「手引き」の中で、（１）　どういうプライバシーポリシー（個人情報等の取り扱い方について説明した文書。通常はウェブサイト上に掲載。）が望ましいのか（２）　模範的なプライバシーポリシーの社名を挙げていただきたい。手引き（案）の第６ページに「企業側がより一層個人に対する説明責任を果たし・・・利用者の理解及び認識を高め」ていくことの重要性が記載されている。そうすると、狭い意味のサイバーセキュリティに限らず、広く、個人情報の取り扱い方の開示方法についても、手引きでご指南頂くことが望ましいように思われます。個人の理解や認識を高まるべく、説明を丁寧にしようとすれば、長いポリシーとなってしまい、かえって消費者の方にご迷惑をおかけしてしまいます。他方、短く簡潔であろうとすると、IT リテラシーがあまりない方にとっては、「自分の個人情報がどのように取り扱われるのかがよくわからない」というご不満を抱く原因になります。そこで、ぜひ手引きにて、どのような記載ぶりが望ましいのか、また、具体的にはどの会社のプライバシーポリシーの記載がよくできているのか（或は、すぐれたプライバシーポリシーの記載例）を教えていただけると幸いです。【個人 B】	本手引きはあくまで民間企業のサイバーセキュリティ対策に係る情報開示に関する手引きとして作成しているものであり、広く個人情報の取扱い方の開示方法全体まで対象とすることは予定しておりません。	無
意見４　情報処理の促進に関する法律を尊重し「情報処理安全確保支援士」の関与を前提とした手引きを作成することが望ましいのではないか。	考え方４	
○　【全体意見】 現在、情報システムを抜きした企業経営は困難であることから、サイバーセキュリティリスクは IT リスクではなく経営リスクととらえるべきであり、実際に、米国ＳＥＣの Form10-K（日本における有価証券報告書に相当）においては、サイバーセキュリティに関する情報開示が求められている。 これについて、米国と同様、日本においても、サイバーセキュリティインシデントの内容によっては、企業価値が大幅に毀損され、株主、投資家、そして株式市場全体への悪影響をも与えうる状況となっていると考える。 また、2019 年度現在、	本手引きに対する賛同の意見として承ります。 なお、「情報処理安全確保支援士」の資格を有する人材の関与については、同資格のほかにも様々なサイバーセキュリティ関連の資格が存在す	有

日本の投資環境における外国人投資家の割合は約6割となっており、米国で企業価値の構成要素として「サイバーセキュリティ対策」が取り上げられている状況であるにも関わらず、日本がこれに取り組まないことは、日本企業に対する投資価値の低下（＝株価の低下）にもつながる重要な問題であるとの認識は、情報処理安全確保支援士会設立準備会も共有しているものであり、今回の手引きが作成されることそのものについては極めて有益であると考えている。しかし、サイバーセキュリティ対策情報の開示に際して、各企業単体のガバナンスとしての取組で留まるのではなく、「情報処理の促進に関する法律　第6条」において、サイバーセキュリティの確保を支援する役割を定められている「情報処理安全確保支援士」による各企業におけるサイバーセキュリティ対策への参加や、開示情報に対する第三者としての意見表明について記載されていないという点について、１　情報処理の促進に関する法律と整合性が取れていない、２　開示された情報の真正性について投資家等が確認できない、といった観点から、情報処理の促進に関する法律を尊重し「情報処理安全確保支援士」の関与を前提とした手引きを作成することが望ましいと考えるが、そうした場合、本書について大部分の改稿を要するため、情報処理の促進に関する法律との整合性については次回改定時における重要検討課題とするとともに、当面の対応として以下の部分に対する修正を行うことを提言する。 〈P15〉 ３　資源（予算、人員等）の確保 サイバーセキュリティリスクへの対策を実施するための資金確保と「情報処理安全確保支援士といった」サイバーセキュリティ人材の確保を実施する。 〈P19〉 ２　表現真正性 ●開示資料について、情報処理安全確保支援士による評価意見の記載を検討する。 【情報処理安全確保支援士会設立準備会】	ることから、同資格を有する人材のみではなく、広くサイバーセキュリティ関連の様々な資格を有する様々な人材の知見等を活用することが適当であると考えます。 頂いた御意見の趣旨を踏まえ、以下のとおり、本手引きの本文を修正させていただきます。 〈P15〉 ３　資源（予算、人員等）の確保 サイバーセキュリティリスクへの対策を実施するための資金確保と「情報処理安全確保支援士などのサイバーセキュリティ関連の資格を取得した」サイバーセキュリティ人材の確保を実施する。	