重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（案）に関するパブリックコメントの結果一覧　　（別紙）

No.	御意見の要旨	御意見に対する主な考え方
はじめに　関係		
1	■　はじめに関して。 ・　サイバー関係について、国民の安全が害された場合に、その対処について、国家としてもきちんとしてその国民の対処を支援するなどのことが必要なことを明示すべきであり、国民の安全と、国家の安全とを直ちに結びつけ、国家の安全保障の問題としてばかりとらえ、それについての、積極的役割というような記載をすべきではない。	法第１条の法目的に係る規定において「そのサイバーセキュリティが害された場合に国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機のサイバーセキュリティを確保する重要性が増大していることに鑑み」とあり、こうした観点から、政府が本法に基づき積極的に役割を発揮していくことは必要だと考えております。基本方針「はじめに」の記載はこうした旨を記載したものです。
第１章　重要電子計算機に対する特定不正行為による被害の防止に関する基本的な事項　関係		
2	第１章第３節（１）「政府内の連携と総合調整」に関して、以下の点を意見として申し上げます。 〇NCOの能動的な総合調整機能について 本方針案では、国家サイバー統括室（NCO）が司令塔として能動的に総合調整を行うことが明記されており、政府全体の施策を一体的に進める姿勢を評価いたします。 〇主務省庁の役割の明確化と能動性について 一方で、関係省庁の役割分担が不透明であり、主務省庁の能動的な関与が読み取りづらい印象を受けます。 例えば資産登録については省令で詳細を定めることになっておりますが、各事業者からの情報待ちではなく、主務省庁がデファクトスタンダードを整理・提示するなど、能動的に対応することが不可欠です。 〇三位一体の推進体制について サイバー対処能力強化法の円滑な運用には、NCOの総合調整機能に加え、主務省庁のリーダーシップ、そして事業者の現場対応力が三位一体となって進められることが必要です。 この点を、基本方針においてより明確に位置づけていただきたいと考えます。	基本方針第１章第３節に記載のとおり、内閣府を始めとした関係行政機関等は、政府一体となって法に基づく事務又は関連する施策が実施されるよう相互に緊密に連携協力してまいります。また、官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要であるため、関係機関・団体との連携に努めてまいります。関係省庁の役割については、それぞれ施策の内容に応じて、基本方針の各章に記載しております。
3	能動的サイバー防御(ACD)の実行にあたって、政府は着実な情報保全がなされている形で平時から効率的に民間のITインフラに対する攻撃データ等の収集・活用を行うべき。（第5章 第2節 （３）｜ 28頁 L.24～32 または 第2章第2節（１）｜ 10項 L.26～30） 令和4年12月に閣議決定し公表された国家安全保障戦略において、ACDを実施するための3つの措置の一つにアクセス・無害化措置がある。国民生活もしくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機へのサイバー攻撃を未然に防ぐためには、平時より民間企業特に特定社会基盤事業者のITインフラに関する構成情報やセキュリティ対策情報、当該ITインフラがサイバー攻撃され得る侵入ポイント、当該ITインフラに対する実際の攻撃情報等を効率的に収集、分析すること、また平常の状態をあらかじめ把握しておくことが必要不可欠である。特にITインフラに対する実際の攻撃情報は攻撃アクター／攻撃インフラを特定しアクセス・無害化措置を実施する上では必須であるため、民間企業において観測した当該攻撃データを国家サイバー統括室（NCO）が収集・分析し警察及び防衛省・自衛隊が活用するとともに、情報提供元の民間企業へフィードバックを行うなど情報活用のためのエコシステムを作るべきと考える。なお、その際に新設される協議会において、NCOが収集した情報の分析を行うためにアドホックもしくはタスクフォース的に攻撃情報の分析・議論ができる民間企業と連携を深めることを期待する。 これら情報の収集及び活用にあたっては、政府のみならず情報の共有を受ける民間企業においてもいわゆるセキュリティ・クリアランス等の制度の活用を念頭に確実な情報保全がなされている者のみが参画できる形にしなければならないことに留意されたい。また、高度な潜伏型攻撃に関する早期検出を可能とするため、政府と特定社会基盤事業者における事業者協定の範囲において、平時のオペレーションをヒアリングしてその状態を定期的に政府が把握するべきと考える。	基本方針第１章第３節⑵に記載のとおり、官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要であるため、関係機関・団体との連携に努めてまいります。頂いた御意見は、今後の制度設計・運用における参考といたします。
4	〇該当：基本方針（案）p7「政府が率先して情報を提供し官民双方向での情報共有を促進するなど、官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要である。」との記載部分 〇意見内容：当該箇所について「政府が率先して情報を提供し、脆弱性に関して国内外で公開される情報の集約や早期対応へのアラートを含む情報等について官民双方向での情報共有を促進するなど、官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要である。」との修正を提案します。 〇理由：サイバーセキュリティの確保において、日々発見される脆弱性に対する対応は対策の根幹となるため、JVNの活用やベンダーからの直接情報登録など、官民双方向での情報共有の促進に含まれる脆弱性対策情報の集約、重要度に応じた対策の促進が極めて重要であるため、具体的な内容を例示し、その実行を確実にすることが必要です。	脆弱性情報の集約や共有に関しては、基本方針第５章第２節⑹イにおいて、関係省庁・関係機関による脆弱性関連情報の取扱いについては、官民連携を強化し、政府が集約した情報を整理・分析し率先して民間事業者等に対し提供するという、本法による官民連携の強化に係る規定やその趣旨に基づき、政府が本法に基づく官民連携に係る事務を着実かつ効果的に実施できるよう、関係する告示・ガイドラインの必要な見直しを行う旨を記載しております。
5	■　第１章第３節「政府内及び事業者間との連携と総合調整」の箇所に関して。 ・情報を守るという場合に集中と分散のバランスが必要と考える。国家が全てを集中して集めてするシステムの問題点等をきちんと意識してなされなければならない。	頂いた御意見は、今後の制度運用における参考といたします。
6	■　第１章第４節「通信の秘密の尊重」の箇所に関して。 あたりまえのことについて全体的なこととして記載をしているが，この記載がないよりはましということも一応考えられるが、一方個々の各規定でこのことが徹底されているとはいえない。各規定各場面の中でこのことが突き詰められ、基本的にはできないことできるとする場合の、厳しい要件が、具体的に明示されていなければならない。各通信の秘密の侵害が問題となるような場面がでてくるなかで、通信の秘密の尊重ということを、日々検証するシステムが必要と考える。	基本方針第３章第３節⑴に記載しているとおり、本法に基づく通信情報の利用に係る制度では、法第４章から第７章までに規定する通信情報の取得及び取扱いに係る各種の手続や条件、制限等の規律が適切に遵守されることにより、通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることが確保される制度となっています。基本方針に則り、全ての関係職員は、これらの規律を厳格に遵守し、適正に業務を行うことを徹底してまいります。
7	■　第１章第４節「通信の秘密の尊重」の箇所に関して。 「関連業務に携わる通信情報保有機関における全ての関係職員は、通信情報を取り扱うに当たってはこの点について十分な認識を持ち、通信の秘密を尊重しつつ厳格にその業務に取り組むことを徹底する。」とあるが、方針として十分ではない。通信の秘密の侵害が問題となるような場面を例示し、それに対してどのような対応をすることで通信の秘密の尊重を全うするのかについての具体的指針を示すべきである。	同上

8	重要電子計算機、特定重要電子計算機と用語が混在している。これはもう少し整理を求めたい。 なお、何が重要電子計算機の具体例となるのか。何が特定重要電子計算機の具体例となるのか。何が特定重要設備の具体例となるのか。これらは具体的な例を示していただきたい。例えばガバメントクラウド自体は何になるのか？ガバメントクラウドを構成するインフラストラクチャーは何になるのか？ 本稿意見者は法学的知識を持ち合わせていないため、これらの一意の解釈が極めて原文では困難であったことを追記しておく。	「基本方針において使用する用語は、法において使用する用語の例による」（はじめに）としており、重要電子計算機及び特定重要電子計算機は、それぞれ法第２条第２項及び第３項により規定されるものを指します。これらの定義の考え方については、基本方針第１章第５節⑴の記載のとおりであり、今後、その具体範囲については、その内容も踏まえて、政省令等の策定を通じて明確化を図ってまいります。
9	P8.１行目 重要電子計算機の範囲を政令で定めるとありますが、各省の省令で分野毎に定められるということでしょうか。また、重要電子計算機の届出は所管省庁、あるいは内閣府のどちらでしょうか。重要電子計算機の範囲を決めるにあたり、製造ベンダーの意見も踏まえて検討頂きたい。	重要電子計算機については、法第２条第２項第１号、第２号及び第３号それぞれの規定に基づき政令で定めた上で、必要に応じ、省令等で明確化してまいります。政省令等の策定にあたっては、パブリックコメントといった必要な手続を経て、事業者からも御意見を伺いながら検討を進めてまいります。 特定重要電子計算機の届出は、法第４条第１項及び第２項の規定により、特別社会基盤事業者の所管省庁に届け出られ、当該所管省庁は内閣府に通知することとされています。
10	P８.５行目 「重要情報」の定義を明確にして頂きたい。	「重要情報」は、法第２条第２項第１号に定義があり、日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）第１条第３項に規定する特別防衛秘密、特定秘密の保護に関する法律（平成25年法律第108号）第３条第１項に規定する特定秘密、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和５年法律第54号）第27条第１項に規定する装備品等秘密又は重要経済安保情報保護活用法第３条第１項に規定する重要経済安保情報である情報をいいます。
11	P8 19~20行目 重要情報を保有する装備品製造等事業者に該当する場合は、重要電子計算機を所有していると見做される可能性があり、特定社会基盤事業者にも該当する可能性があるということでしょうか。	特定社会基盤事業者は、経済安全保障推進法第50条第１項に規定する特定社会基盤事業者をいい、その該当性は（重要電子計算機の所有の有無にかかわらず）同法に基づき判断されるものです。
12	全体 経済安全保障推進法でいう「特定重要設備」と、サイバー対処能力強化法に基づく基本方針でいう法第2条第2項第２号でいう「特定重要電子計算機」の関係が不明確だと思います。関係性を明示して頂きたい。	特定重要電子計算機については、特定社会基盤事業者が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、経済安全保障推進法に規定される特定重要設備の機能が停止し、又は低下するおそれがあるものと法第２条第２項第２号に規定されており、特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム等が該当します。その詳細は、基本方針第１章第５節⑴に記載のとおり、事業者の御意見を伺いながら、政省令等の策定を通じて明確化を図ってまいります。頂いた御意見は、今後の制度設計における参考といたします。
13	「P.8　特定重要電子計算機の定義について」：特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム（クラウドサービスを含む。）等と記載があり、現行の記載ではすべてのシステムと捉えることも可能と思いますので、より具体的な該当システムの定義を連携いただきたく存じます。	同上
14	電子計算機の区分としては、大きく基幹系・業務系・一般向け公開システムなどで分けられるが、重要電子計算機の範囲は、法目的の確実な実現を図るため、このすべての区分が対象となるべき（第1章 第5節（１）｜ 8頁 L.11～18） 民間企業においてインシデントが発生した際に、報道などでは「企業単位」でサイバー攻撃被害が周知され、特定重要設備への攻撃でなくても社会的な混乱・影響は大きい。サイバー対処能力強化法における「国民生活もしくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機へのサイバー攻撃を未然に防ぐ」という目的を鑑みると、特定社会基盤事業を提供するための特定重要設備が含まれるような基幹系システムのみならず、予約サイトや一般ユーザが契約変更するサイトのような一般向け公開システムや、営業秘密を扱ったり財務・経理処理を行ったりする業務系システムにおけるインシデントにおいても政府への報告対象とすべきと考える。 以上を踏まえ、本基本方針においては、「特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム（クラウドサービスを含む。）等」が重要電子計算機と記載されているが、当該文中の「等」に含まれる範囲について、より明瞭に記載をすべきと考える。	同上
15	＜対象＞8ページ 14～16行目　具体的には、特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム（クラウドサービスを含む。）等が該当する。 ＜意見＞特定重要設備と接続されている電子計算機でも、特定重要設備と当該電子計算機が外部と隔離された領域内で構成されているものはサイバーセキュリティが害されるおそれはないため、その旨を明らかにしていただきたい。	特定重要設備と接続されず、情報のやり取りができない情報システムについては、特定重要電子計算機の対象から外れることとなりますが、その具体的な範囲については、政省令等の策定を通じて明確化を図ってまいります。
16	4頁の「第１節 本法による各種措置を行うこととなった背景・経緯」において「社会全体のデジタル化やサプライチェーンの複雑化が進展」と表現がありサプライチェーンを見える化も重要な背策と認識するところ。 現状における本件の対象について、日本銀行が対象であることが「特定社会基盤事業者として指定した者」に記載がなく分かり辛いため、同等の対応を実施していることを広く周知する観点で、もう少し分かり易く対象であることを明示いただきたい。	日本銀行は、経済安全保障推進法に規定する特定社会基盤事業者には該当しませんが、法第２条第２項第１号ホの政令で定める法人に規定上含まれ得ます。当該政令で定める法人については、基本方針第１章第５節⑴の考え方を踏まえ、検討を行ってまいります。

第２章　当事者協定の締結に関する基本的な事項　関係		
17	他の事業者の参考とするため及び手続の透明性を確保するため、当事者協定を締結した事業者名及びその当事者協定を公表することとすべき。	現時点で当事者協定の締結について公表を行うことは予定していませんが、協定当事者となる事業者に対しては、事前に協議等の場を通じて協定の締結に必要な情報提供を十分に行ってまいります。
18	当事者協定の位置づけおよび締結対象範囲に関する考え方について 重要電子計算機に対する不正な行為による被害の防止に関する法律（以下、「法」という。）は、当事者協定(法11条、12条）の相手方として「特別社会基盤事業者」および「特別社会基盤事業者以外の事業電気通信役務の利用者」を対象としており、特別社会基盤事業者に限定されない広い主体との締結を予定していると解される。 しかし、「当事者協定の締結の推進に当たっての考え方」（基本方針案p10）における記述は、特別社会基盤事業者を中心とした協定締結の推進に重点が置かれているように受け取れる。しかしながら、特別社会基盤事業者に該当しない事業者であっても、サイバー攻撃を受けた場合には社会・経済活動へ重大な打撃を与え得る。例えば、近時の大手飲料企業や電子商取引事業者に対する攻撃が、当該事業者の活動を困難とし、我が国の物流・消費行動に広汎な影響を与えたことは記憶に新しい。 また、法17条、32条および33条に基づく媒介中通信情報（法2条6項1号）の取得は、電気通信事業者の協力を前提として成立する制度である。しかしながら、近年の通信暗号化の急速な進展により、通信経路における機械的情報の取得自体が技術的に困難となりつつある。 とりわけ、DNS over HTTPS（DoH）・DNS over TLS（DoT） によるDNSクエリの秘匿化や、Encrypted Client Hello（ECH）によるTLSハンドシェイク情報（従来SNIとして可視であった情報）の暗号化は、通信事業者が経路で取得可能な機械的情報を著しく縮小させており、これらの措置に依拠する枠組みの持続可能性に疑問を投げかけている。 他方、当事者協定に基づく通信情報の提供は、協定当事者が管理する当事者管理通信情報（法2条6項2号）の提供を受けるものである。これは通信経路で暗号化される「前」あるいは復号された「後」の情報を対象とできるため、こうした暗号化技術の普及による影響を回避し得る、中長期的に実効性の高い枠組みである。 したがって、幅広い事業者をサイバー攻撃の脅威から守ると同時に、制度全体の実効性を中長期的に確保する観点から、特別社会基盤事業者に該当しない事業者との協定締結（法12条）についても、法11条に基づく協定と並行して推進する姿勢を打ち出すことが望ましいと考える。	基本方針第２章では、「特別社会基盤事業者」及び「特別社会基盤事業者を除く事業電気通信役務の利用者」を合わせて「特別社会基盤事業者等」と記載しており、利用者についても特別社会基盤事業者とあわせて当事者協定の締結の推進を図ることとしています。頂いた御意見は今後の参考とさせていただきます。
19	弊社は、貴府のサイバー対処能力強化法の施行及び省令制定を含む、特定不正行為による被害の防止に向けた活動を支持いたします。次の点について確認させていただきたく存じます。 「第２章 第２節 (2)当事者協定の締結についての推進方策」において、内閣府において、当事者協定の標準的な項目及びその内容を示したひな型を事前に作成し、協議に際して当事者協定を締結しようとする者がこれを参照できるようにしておくことを検討される旨の記載がございます。また、本法第11条にて、内閣総理大臣は、協定に基づき、特別社会基盤事業者を通信の当事者とする通信情報の提供を受け、個別分析情報を提供する旨が規定されています。 上記において、特定重要電子計算機の所有者が当該特定重要電子計算機の供給者である場合（いわゆるASPサービスやクラウドサービスのような形態である場合）、当該サービスを利用する特別社会基盤事業者のみならず、電気通信事業者でない電子計算機等供給者が通信情報を管理している等により、当該通信情報の提供について利害を有する場合がございます。この場合、以下の点について確認させて頂けますと幸いです。 (1)特別社会基盤事業者の単独の判断／作業で通信情報を提供することが困難な場合、当事者協定に、当該特定重要電子計算機の電子計算機等供給者を加えることができるでしょうか。 (2)電子計算機等供給者が当事者協定に含まれない場合、当該通信情報に当該特定社会基盤事業者以外の情報が含まれる可能性があることから、特別社会基盤事業者による通信情報の提供について、電子計算機等供給者より異議を述べる機会が与えられるべきではないでしょうか。 (3)提供が求められる通信情報に、当事者協定の当事者である特別社会基盤事業者以外の事業者に関する通信情報が不可分に／不可避的に含まれる場合、当該通信情報に係る他の全事業者との間で内閣府が当事者協定を締結することが現実的でないことも想定されます。この場合には、通信情報を管理している（電気通信事業者でない）電子計算機等供給者との間で当事者協定を締結することも考慮・明記頂けますと幸いです。 (4)⊞記(2)(3)の通信情報について、当事者協定の当事者である特別社会基盤事業者が他事業者の通信情報に接することがないよう、当該特別社会基盤事業者からの依頼により、（電気通信事業者でない）電子計算機等供給者より直接に内閣総理大臣に通信情報の提供を行うことも許容して頂きたく存じます。上記(2)(3)のような状況もあると想定されるところ、通信の秘密等への十分な配慮の一環として、柔軟な通信情報の提供方法がありうる点を基本的な方針にても明記して頂くのが良いと考えます。	(1)について 法第11条は、内閣総理大臣、特別社会基盤事業者及び同条第３項の電気通信事業者以外の者が協定に加わることを排除するものではなく、個別具体的な事情に照らし、例えば特別社会基盤事業者がその使用する設備の運用を他の事業者に委託しているような場合において、国が通信情報の提供に向けた調整を当該他の事業者を交えて行うことが円滑であると認められるようなとき等には、当該他の事業者が協定に加わることもあり得ると考えられます。 (2)から(4)までについて 当事者協定により提供を受ける通信情報には、特別社会基盤事業者と当該特別社会基盤事業者以外の他方当事者との通信に係るものが含まれる場合があるところです。法においては、(2)における御指摘の手続を経ることや当該他方当事者を協定当事者に含めることとはしていませんが、基本方針第３章第３節⑴に記載しているとおり、法第４章から第７章までに規定する通信情報の取得及び取扱いに係る各種の手続や条件、制限等の規律が適切に遵守されることにより、通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることが確保される制度となっています。 なお、(4)における御指摘の「（電気通信事業者でない）電子計算機等供給者」が行う業務及び特別社会基盤事業者との関係並びに「提供」の具体的な手法が必ずしも明らかではありませんが、御指摘の「電子計算機等供給者」が通信の一方当事者の地位になく、また、媒介中通信情報を管理する法第11条第３項の電気通信事業者でもない場合において、御指摘の「電子計算機等供給者」が通信情報の内容を確認し、協定当事者である特別社会基盤事業者の通信とそれ以外の者の通信とを区別して提供を行う行為は、通信の秘密に対する新たな制約となり得るものであり、法との整合性も含め、慎重な検討が必要であると考えられます。
20	該当箇所：第２章第２節⑵ 当事者協定の締結についての推進方策 意見：当事者協定については、内閣府と特別社会基盤事業者その他の事業電気通信役務の利用者（協定当事者）との間で協定（当事者協定）を締結することとなっているが、実際に通信役務の利用者個人から通信情報の利用に関する同意を得ることは困難と考えるため、電気通信事業者が利用者から非難を受けることがないよう、対応の指針を政府側から示していただくことを要望する。 また、通信の一方の当事者である事業者が内閣府との間で協定を締結することをもって、「通信当事者の有効な同意のある場合」として通信の秘密を侵害しない、との整理がなされていると理解しているが、この点、基本方針案へ明記すべきと考える。 協定で合意する範囲についても、適切かつ合理的な運用を要望する。	当事者協定は内閣府と協定当事者との間で締結する任意のものであり、内閣府は、できる限り丁寧にその締結に向けた協議を行うなど基本方針の記載に則り適切な制度の運用を図ってまいります。なお、当事者協定に基づく通信情報の利用を含め、法に基づく通信情報の利用による通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることについての考え方は、基本方針第３章第３節⑴に記載をしています。

21	○前文：弊社は、「重要電子計算機に対する不正な行為による被害の防止に関する法律」に関する「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」（案）の趣旨に深く賛同いたします。本基本方針（案）における官民連携をさらに円滑かつ効果的に推進するための弊社意見を、以下の通り提出させていただきます。今後のご検討において、ご参考としていただければ幸いです。 ○当事者協定に関して 当事者協定締結事業者が任意で提出を求められる情報には、当該事業者がベンダー等の外部から入手した情報が含まれる可能性があります。そのため、当事者協定締結事業者に対して、以下の事項を周知徹底いただくことを希望します。 ・政府への情報提供前に、原則として情報入手先に事前に十分な周知・協議を行うこと。 ・守秘義務がある情報が政府提出情報に含まれないよう、提出前に十分に確認すること。	頂いた御意見は今後の運用における参考といたします。
22	当事者協定によるクラウドサービス事業者からの通信情報の提供については、責任共有モデルに基づき、クラウドサービス事業者の管理範囲に限定されるべきと考える。 当事者協定の締結についても、協定を締結しないことによる不利益が生じないこと、また、協定の内容が事業者の技術的・契約的制約を十分に考慮するなど任意であることを実質的に担保する仕組みが必要ではないか。	当事者協定の締結は、法律上あくまでもこれを締結しようとする者の判断に基づく任意のものであり、内閣府は、できる限り丁寧にその締結に向けた協議を行うなど基本方針の記載に則り適切な制度の運用を図ってまいります。
23	P.12-13の選別後通信情報の例外により利用される情報について、利用後の廃棄に関するルールは政省令・ガイドラインで定められる予定でしょうか？	通信情報保有機関は、法第23条第４項第１号の規定に基づく他目的利用により選別後通信情報を利用する場合であっても、他目的利用をしない場合と同様に法第25条等の規定に従い選別後通信情報を消去することになります。その他の関係機関における他目的利用については、例えば、通信情報保有機関との間で事前に取り交わす書面の中で廃棄等の取扱いについても定めることが想定されます。
24	P12　17行目 「他目的利用」とは例えば何か、例示を示して頂きたい。	「他目的利用」としては、例えば、サイバー攻撃の動向について知見を有する民間のセキュリティ会社等に選別後通信情報を提供し、分析を依頼するといった利用が想定されます。
25	他目的利用における犯罪捜査との関係の明確化について 「当事者協定に基づく他目的利用に関する配慮事項」（基本方針案p13）は、法23条に基づき、選別後通信情報の他目的利用が認められる範囲について、法やこれに関する政府答弁よりも謙抑的に捉え、犯罪捜査目的は当該法目的に含まれないため許容されない、との解釈を示しているものと拝察する。 もっとも、本法の目的（法1条）は「特定不正行為による被害の防止」である。他方、不正アクセス禁止法や刑法上の電子計算機損壊等業務妨害罪・不正指令電磁的記録に関する罪などは、まさに本法が対象とする「特定不正行為」（法2条4項各号）そのものを禁圧するものであり、本法の「被害の防止」という目的と実質的に合致すると解される。したがって、選別後通信情報の利用が、法目的に適合する範囲、すなわちこれらの罪名に係るサイバー犯罪の捜査についてもなお制限されるのか否か、刑事訴訟法や国際捜査共助に基づく強制処分や捜査関係事項照会との優劣関係をいかに整理するのかについて明確化が必要であると考える。 なお、重大なサイバー攻撃に関与した個人・団体に対しては、多国間の法執行協力を通じて刑事訴追、経済制裁などのいわゆる「懲罰的抑止」を図るのが通例である。仮に我が国が提供可能な情報が、選別後通信情報に関する法23条の解釈・運用により刑事訴追目的で一切使用できないこととなれば、我が国は国際的な法執行協力の枠組みから事実上脱落し、結果としてわが国のサイバー防御能力そのものを低下させる恐れがあると考える。 以上の通り、国際的法執行協力への実質的な参加可能性を確保することが、法目的（1条）を達成する上で不可欠であるから、基本方針において解釈が示されることを強く要望する。	基本方針に記載のとおり、本法に基づく他目的利用には犯罪捜査のための選別後通信情報の利用は含まれ得ないものと考えております。また、他の法律に基づき選別後通信情報の提供を求められた場合については、基本方針第３章第３節⑸に記載した方針に則り、適切かつ適正な取扱いをしてまいります。
第３章　通信情報保有機関における通信情報の取扱いに関する基本的な事項　関係		
26	重要電子計算機に対する不正行為を防止するために利用する通信情報について、第1章第2節1の（ア）当事者協定、及び（イ）外外通信目的送信措置等により、国外から国外への通信、及び国外と国内の通信、国内から国内への通信情報を分析対象とすると理解してよろしいでしょうか。重要電子計算機に対する不正行為を防止するためには、国外から国外への通信は元より、国外と国内の通信及び国内から国内への通信情報についても分析対象とする必要があると考えます。また同様に、第2章第2節（1）では、「重要電子計算機に対する国外通信特定不正行為による被害を防止する」とありますが、重要電子計算機に対するサイバー攻撃は国内からも発生することは充分に考えられるため、本制度の効果的かつ効率的な運用を図るため、国外通信特定不正行為と並んで国内通信特定不正行為についても分析対象とすべきと考えます。	当事者協定に基づき取得した通信情報については外内通信（国外から国内への通信）を、外外通信目的送信措置、特定外内通信目的送信措置又は特定内外通信目的送信措置に基づき取得した通信情報についてはそれぞれ外外通信（国内を経由し伝送される国外から国外への通信）、外内通信又は内外通信（国内から国外への通信）をその分析の対象とすることとしています。また、国内から国内への通信情報については、立法時点でサイバー攻撃関連通信の99.4%が国外から行われているというデータがあることを踏まえ、法では利用の対象外としています。
27	通信情報の利用と通信の秘密の尊重 ・本法が憲法第21条第2項によって保障された通信の秘密を最大限に尊重しなければならないという原則に基づき、以下の点を要請します。 電気通信事業者への協力負担への配慮：我々は、同意なく通信情報を利用する措置（外外通信目的送信措置など）が、電気通信事業者の協力を得て政府の責任の下で実施される極めて公益性の高い措置であることを理解しています。しかしながら、政府に対し、協力の負担が過度なものとならないよう十分な配慮を行うこと、ネットワーク運営への支障を回避するための対策を十分に検討すること、並びに通信利用者の利便性の低下やコスト負担を防ぐことを徹底して要請します。さらに、電気通信事業者が政府からの情報開示要求を拒否できる「正当な理由」の例について、当該情報の提供が当該事業者の顧客やエンドユーザーとの契約上またはプライバシー上の義務と矛盾する場合を含めるよう要請します。 ・機械的情報の厳格な限定：分析の対象となる「機械的情報」の範囲は、通信の本質的な内容を伝達しうるものではない情報に厳格に限定される こと、また、この範囲が適切な手続きを経た上で規定される ことを要請します。	電気通信事業者への協力負担への配慮に関する御意見については、基本方針の記載への賛同の御意見として承ります。法第20条に規定する「正当な理由」に該当する場合については、電気通信事業者からの要請も踏まえつつ、法の趣旨に則り適切な運用を図ってまいります。 機械的情報の厳格な限定に関する御意見については、基本方針の記載への賛同の御意見として承ります。
28	該当箇所：第３章第２節⑵ 電気通信事業者の協力 意見：諸外国では、協力する事業者に対する金銭的補償が行われていることから、日本でも同様の措置を講じることが妥当だと考えているが、現状の基本指針案では「配慮」の具体的な内容が不明瞭であるため、下記下線の通り追記すべきと考える。 『くわえて、内閣府は、通信ユーザの利便性低下やコスト負担が生じるようなことも避けられるよう、協力する事業者に対する金銭的補償を行うなど、配慮することとする。』	現時点で、かかる配慮の具体的な内容について予断を持って基本方針に記載をすることは困難ですが、頂いた御意見も参考にしつつ、配慮の具体的な内容の検討を行ってまいります。
29	第3章第2節（2）では、内閣府が設置する受信用設備に通信事業者から通信情報が送信されることになっており、その後、取得した通信情報を選別して内閣府及び通信情報保有機関にて分析が実施されると理解しますが、通信の秘密を守る施策として、通信事業者から内閣府へ、あるいは内閣府から通信情報保有機関への通信情報の送信にあたっては強固な暗号化が施されるべきであり、HNDL（Harvest Now, Decrypt Later）攻撃への対策も考慮した量子暗号通信の実装を規定するべきと考えます。	頂いた御意見は今後の運用における参考といたします。

30	該当箇所：第３章第３節⑴ 通信の秘密等への十分な配慮 意見：電気通信事業者が、自身が当事者ではない通信情報の取得に関し、内閣府に協力する場合について、通信の秘密の侵害にあたらないことの法的な整理を明確に基本方針案へ記載いただくことを要望する。	法第20条の規定に基づく電気通信事業者の協力について、内閣府が、法に規定しているものを除き、追加的に通信の秘密を制約し得るような内容の協力を求めることは想定されません。
31	* 違憲：本法は、憲法が私たちの権利として明記している「通信の秘密」を根本から侵害するものであり、本法に基づく方針の制定そのものに反対である。「方針」の基本的な立場は、政府や民間企業などが通信情報をより幅広く利用できるような制度的枠組の構築を目指すために、通信の秘密を国家の政策目標に従属させて可能な限り狭く限定しようとするものであって、憲法が保障する「通信の秘密」の権利を根底から侵害する。この原則的な立場を表明した上で、以下、具体的に問題を指摘する。 * 利用者個人の権利無視：「方針」は、通信の当事者、通信サービスを利用する個人でありまたコンテンツ――文字、画像、動画、コンピュータ・プログラム等形式を問わない――の制作者でもある利用者個人の権利を無視している。また通信事業者は、メタデータも含めて、意図した相手(受信者)のみが通信情報にアクセス・利用できるように送受信に責任をもち、利用者の許可なく政府に通信情報を提供することは憲法上許されない。従って協定を結ぶこと自体が、通信の当事者の権利を侵害することになる。通信情報のコンテンツ作成主体はサービスの利用者(通信の当事者)である。通信事業者は、通信情報の送受信を媒介・管理するのみであり、所有権等を有さない。政府に至っては、通信サービスの媒介・管理者でもなければ通信情報の所有権者でもない。通信情報は通信の当事者である個人に帰属するものであり、通信情報の保護の法的制度的枠組は、通信の秘密はもとより、思想信条の自由や出版の自由など基本的人権の根幹に関わる。方針は、この権利の枠組を否定するものである。 ** 令状主義：通信情報は通信の当事者である利用者個人に帰属するものであることから、憲法35条が明記する「侵入、捜索及び押収を受けることのない権利」によって保護されるものである。「方針」は、通信情報の収集について裁判所の令状を要件としていない。監理委員会は裁判所のような中立的な司法機関ではない。むしろ通信の当事者の権利を弱めることに加担しかねない組織である。当事者の許可なく外国を含む政府や政府を介した民間による通信情報の利用は明らかな憲法違反である。本「方針」では、司法の役割への言及が一切みられないことも含めて、通信の秘密に関する権利侵害を制度化するものである。「方針」では、アクセス・無害化についても司法の介入を認めていない。これは、裁判所の令状に基づいてアクセス・無害化を執行し米国の事例よりもさらに後退している。私達はアクセス・無害化措置そのものに反対であるが、最も侵襲性が高く、令状は必須の条件である。 ** 情報開示、異議申し立て：「方針」は、通信情報の提供や利活用を通信事業者、政府省庁、民間事業者の間の問題としてのみ取り上げている。通信の当事者個人は、自分の情報でありながら、意図しない第三者に利用されていることすら知らされない。どのような通信情報が、どのような理由・目的で通信事業者から政府等に提供されたのかについて、知る権利がある。「方針」には知る権利への言及がない。また、通信情報の提供・利用について、間違いや冤罪といえる場合の救済の道がなく、通信当事者が異議申し立てを行う制度的な枠組もない。 ** 個人が特定可能な場合への歯止めがない：「方針」では、通信情報を個人が特定されないように加工処理するかの文言が多くみられるが、「分析の対象となる機械的情報に対して他の情報と照合しない限り特定の個人を識別できないようにする非識別化措置を講ずる」(p.17)とある。機械的情報に限らず収集情報を他の情報と照合することは禁じられておらず、結果として個人が識別可能であることを容認しており、歯止めがない点は、認められない。 ** 外国政府への情報提供と人権侵害の問題：「方針」は「同意によらずに通信情報を利用する措置（外外通信目的送信措置等）」で、外国における当事国の同意や了承のない情報収集活動を認めている。これは、日本によるスパイ活動を制度化する枠組であり認められない。この規定は、国内法、国際法、当事国の国内法にも抵触しかねず、日本政府や通信事業者が深刻な人権侵害の加害者になりうる規定であって、容認できない。 *「方針」の必要性への疑問：サイバー攻撃が深刻な事案となる問題を私たちは認識している。しかし、その多くは、警察や自衛隊も含む政府の治安機関によらなくても解決可能であり、私たちの基本的人権を大幅に制約しなければならないこととは言えず、「方針」のような枠組は必要性がない。	本意見募集は、「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針　（案）」について、御意見を募集するものです。 なお、基本方針第３章第３節⑴に記載しているとおり、法に基づく通信情報の利用は、それが令状によるものでなくとも、当該利用による通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることが確保される制度となっています。また、ここに記載しているとおり、その利用の対象は、自動選別によって不正な行為に関係があると認めるに足りる機械的情報（通信の当事者の意思の本質的な内容を理解することができないと認められる情報。基本方針第１章第５節⑵参照。）のみに限られます。くわえて、基本方針第３章第３節⑸に記載しているとおり、通信情報の利用に関する事務の実施においては、通信情報保有機関は、個人情報の保護に関する法律（平成15年法律第57号）を始めとする他法令を適切に遵守する必要があります。
32	「方針」では、通信情報の提供や利活用が通信の当事者個人を無視する枠組になっている。自分の情報でありながら、意図しない第三者に利用されても知らされない。どのような通信情報が、どのような理由や目的で通信事業者から政府等に提供されたのかについて、個人には知り確認する権利がある。また、その提供・利用情報が間違っている場合にも異議申し立てできない。 そもそも、裁判所の令状なしに個人の通信情報を政府が取得することは　令状主義に反し、通信の秘密を保障する憲法に違反する。	本意見募集は、「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針　（案）」について、御意見を募集するものです。 なお、基本方針第３章第３節⑴に記載しているとおり、法に基づく通信情報の利用は、それが令状によるものでなくとも、当該利用による通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることが確保される制度となっています。
33	方針案と、方針案の前提の「能動的サイバー防御」などを定めた重要電子計算機に対する不正な行為による被害の防止に関する法律は、憲法の通信の秘密等の権利を侵害するものなので、反対です。私たちの個人情報である通信内容が政府によって集められることは、人権侵害です。かつ、令状もなく集められるとしたら、令状主義にも反するもので、司法における人権保護を根幹から揺るがしています。	同上
34	P18　21行目～28行目 「提供用選別後情報」、「選別後通信情報」のイメージが具体的につかないため、例示をして頂きたい。	「提供用選別後情報」については、サイバー通信情報監理委員会との協議等を踏まえ、その基準を内閣府令で定めることとしており、現時点でその具体の例をお示しすることは困難です。また、「選別後通信情報」については、これを選別するための措置である自動選別について第３章第３節⑴に、選別後通信情報を構成する「機械的情報」の考え方について第１章第５節⑵に記載しているとおりです。

第４章　情報の整理及び分析に関する基本的な事項　関係		
35	特定重要計算機の届け出や、インシデント報告が、企業に過度な負担とならない配慮が必要。例えば、インシデントの報告はスピード重視で最低限の報告に留める初報と、調査がひと段落ついた後の続報の2回が現実的。インシデント対応に注力するためにも、報告稼働の軽減が重要である。（国家を背景とするサイバー攻撃を受けた場合、調査には1か月以上かかる）	特定重要電子計算機の届出や特定侵害事象等の報告を求めるにあたっては、基本方針第４章第２節に記載のとおり、特別社会基盤事業者の負担にも配慮し、合理的な制度設計・運用となるよう努めてまいります。
36	基本方針（案）p.21で言及されている特定重要電子計算機の届出の考え方に賛同する。制度の目的を踏まえ、届出対象となる特定重要電子計算機については、システムの実態や機器の分類等に応じて丁寧に整理し、明確なガイダンスを示すことを期待する。	特定重要電子計算機の届出を求める内容については、基本方針第４章第２節⑴に記載のとおり、特定重要電子計算機の機器の分類ごとに整理してまいります。
37	1.サイバー脅威の増加に対する日本政府の取り組みを支持する。しかしクラウドの扱いについては今後の検討課題とされている項目が多く、今後、クラウドサービスの以下の技術的特性を十分に考慮した制度設計を求める。 a. 責任共有モデル： クラウドサービスでは、責任共有モデルの考え方に基づき、クラウドサービス事業者が管理するインフラストラクチャー層（物理インフラ、ネットワーク、ハイパーバイザー等）と、顧客が管理するアプリケーション・データ層が明確に区分されている。 b. 利用形態の多様性： クラウドサービスには多様な利用形態があり、それぞれで管理範囲や責任分担が異なる。そのため、利用形態ごとに適切な基準を設定することが、実効性のある制度運用につながると考える。 c. 既存の国際的なセキュリティ認証： クラウドサービス事業者は、ISO 27001、SOC2、ISMAP等のセキュリティ認証を既に取得しており、第三者による厳格な監査を経ている。これらの既存認証を活用することで、新たな監査や届出の重複を避け、効率的な制度運用が可能となると考える。 2.第5節「重要電子計算機の定義の考え方」において、「特定重要設備と接続され、一定の情報のやり取りが可能な情報システム（クラウドサービスを含む。）（8頁目14－16行目）」がそれに該当するとされているが、その規模は膨大であり、かつ形態も多様であることから、実行力ある制度設計のため、省令で今後定められるとされる範囲の明確化においてクラウドサービス事業者へ意見を反映させるよう配慮してほしい。特に、責任共有モデルの考え方を踏まえ、クラウドサービス事業者と特定社会基盤事業者それぞれの管理範囲を明確にした上で、実効性のある範囲設定を行う、また、今後の具体化プロセスにおいて、クラウドサービスの技術的特性を十分に考慮した制度設計を要望する。 3.特定重要電子計算機の届出について、特別社会基盤事業者の負担に配慮するという考え方を支持する（21頁22行目-22頁16行目）。クラウドサービス利用時の届出は、サービス名、利用形態、用途等の基本情報に限定し、クラウドサービス事業者が既に取得している国内や欧米主要国で確立されているセキュリティ認証や国際標準（ISO27001、SOC2、ISMAP等）を活用することで、詳細な技術情報の届出を省略できる仕組みとすることを要望する。省令における詳細においては、その実情をふまえ、既存認証の活用により事業者の負担軽減と、過度な技術情報開示によるセキュリティリスクの回避が可能となる制度設計を要望する。 4.特定侵害事象等の報告については（22頁17行目）、クラウドにおける顧客データへのアクセスは制限されており、また、顧客との契約上の守秘義務を負っている。そのためクラウドサービス事業者による通信情報の包括的な取得・提供は技術的に困難である。「特定重要電子計算機の機能がクラウドサービス上で実装されている場合の考え方については、クラウドサービスの利用形態ごとに整理する。（23頁1行目）」という考え方を支持する。クラウドサービス事業者はグローバルネットワークの膨大な情報を扱うため、事象の明確な基準が設定されない場合、大量の低精度データが報告されかねない。今後具体化が必要な論点にある通り利用形態により責任範囲が異なるため、具体的な取得・提供の方法について、実務的な協議の機会を設けていただきたい。 6.記録保持期間の合理化については、現行の記録保持要求は無期限に近い運用となっており、特別社会基盤事業者に過度な負担を強いることとなる。リスクベースアプローチに基づく合理的な保持期間への見直しを強く要望する。	特定重要電子計算機の届出や特定侵害事象等の報告を求めるにあたって、特別社会基盤事業者がクラウドサービスを利用している場合には、頂いた御意見も参考にしつつ、また、関係事業者の御意見も伺いながら、その実情も踏まえた制度設計・運用となるよう努めてまいります。
38	特定重要電子計算機の機能がクラウドサービス上で実装されている場合、クラウドサービスそのものの理解やサイバー攻撃に対する耐性を理解していただくことが重要である。２４項２５－２８行目において、クラウドサービス事業者のニーズも含めることで、クラウドを利用している民間事業者のニーズを踏まえることが可能になると考える。	同上
39	電気通信事業者がクラウドサービスを利用しているケースがある。 今後の論点になるが、その場合の責任共有モデルの考え方について整理が必要である。	頂いた御意見は、今後の制度設計・運用における参考といたします。
40	p.21-23 第4章 第1節、第4章 第2節(1)(2) 「基本的な考え方」や「報告等情報の収集の考え方」において、特別社会基盤事業者については、「過度な負担とならないように」などと明記されています。一方、第1章第2節で、「全てのステークホルダがサイバーセキュリティ対策の一翼を担い、サイバー攻撃対応のエコシステムを官民横断で構築する」とあるように、本施策の目的を達成するためには、特別社会基盤事業者はもちろん、一翼を担う「供給者」の負担についても配慮し、本施策が官民全体で効果的に機能することが重要であると考えます。 特別社会基盤事業者と同様、供給者の負担への配慮についても、基本方針として記載いただけないでしょうか。	御指摘を踏まえ、第4章第1節「基本的な考え方」における「特別社会基盤事業者の負担にもよく留意しつつ」に、脚注として「特別社会基盤事業の負担も踏まえた制度設計・運用とすることで、当該事業者から協力が求められる電子計算機等供給者等の負担の軽減にも資すると考えられる」旨を追記します。
41	弊社は、基本的方針（案）の趣旨に深く賛同いたします。本基本方針（案）における官民連携をさらに円滑かつ効果的に推進するための弊社意見を、以下の通り提出させていただきます。今後のご検討において、ご参考としていただければ幸いです。 〇特定重要電子計算機の届出関連 基本方針において、「特定重要設備と接続され、一定の情報のやり取りが可能な情報システム（クラウドサービスを含む。）等」が特定重要電子計算機に該当し得るとされている点について、「接続される」の定義によっては、極めて膨大な数の届出および更新届出が必要となるおそれがあります。特別社会基盤事業者が契約するSaaSは契約数が多く、入れ替わりの頻度も一定程度高いのが実態です。 この膨大な届出は、届出に関与する特別社会基盤事業者およびベンダー、並びに届出情報を管理分析する政府機関の双方にとって、非効率かつ過度な負担を生じさせる可能性があります。そのため、届出を要する特定重要電子計算機は真に必要なものに限定されるよう、特別社会基盤事業者およびそのベンダーも含めた官民での双方向の議論が今後実施されることを期待します。 また、届出において、特別社会基盤事業者及びそのベンダーの営業秘密やセキュリティ関連情報など、過度に詳細な情報の開示が要求されることがないよう要望いたします。 上記の観点から、「特定重要電子計算機の届出を求めるに当たっては、特別社会基盤事業者の負担にも配慮する。」との記載について、「特定重要電子計算機の届出を求めるに当たっては、特別社会基盤事業者および関連するベンダー等の負担にも配慮する。」との記載への変更を希望します。	同上

42	弊社は、基本的方針（案）の趣旨に深く賛同いたします。本基本方針（案）における官民連携をさらに円滑かつ効果的に推進するための弊社意見を、以下の通り提出させていただきます。今後のご検討において、ご参考としていただければ幸いです。 〇特定侵害事象等の報告関連 重要特定侵害事象等の発生時における政府への迅速かつ的確な報告は、官民一体での対応を行う上で極めて重要です。特に初動対応時においては、第一線で被害防止・軽減にあたる関係事業者の現場への負荷は可能な限り最小限となるように配慮しつつ、必要なタイミングで真に必要な情報共有を実施できることが重要と考えます。 基本方針案において、「特定侵害事象等の報告内容については、不確実な内容も含めて報告時点で判明した事項を記載すれば速報として足りることとする等、タイミングに即して特別社会基盤事業者にとって過度な負担とならないよう設定する。」と記載いただいておりますが、多くの特定侵害事象等への対処に主体的に関与するベンダーにとっても過度な負担とならないよう配慮いただくことを要望します。その観点で、「特別社会基盤事業者及びそのベンダー等にとって過度な負担とならないよう設定する。」などと基本方針案の記載も修正されることを希望します。	同上
43	[該当箇所：第１章第５節、第４章第２節（１）]＜特定重要電子計算機の届出＞ 方針案では、日本における特別社会基盤事業者のレジリエンス強化を目的とした官民連携の促進策の一環として新たに導入される、特別社会基盤事業者が使用している特定重要電子計算機の届出義務について説明がされています。特定重要電子計算機には重要設備だけでなく、クラウドコンピューティングサービスを含む情報システムも含むとされています。特定重要電子計算機の対象範囲については、来年公布予定の政令・省令で詳細が定められると理解していますが、特定重要電子計算機の指定に際しては、リスクベース・アプローチを採用し、特別社会基盤事業者が提供する重要役務の継続的な提供に不可欠な特定のシステムに焦点を当て、特別社会基盤事業者が使用するその他の重要でないシステムは指定対象としないことを求めます。 方針案の第4章第2節(1)で述べられているように、特別社会基盤事業者が使用する機器の数を考慮すると、届出は膨大となり、手続きに多大な時間を要すると予想されます。本方針を実現可能なものとするためには、高度なコンピューティングシステムを導入する特別社会基盤事業者、また、届出を管理する政府機関の負担を最小限に抑えることが重要です。この点において、クラウドコンピューティングサービスの対象範囲を、特別社会基盤事業者のテナントのうち重要機能を支えるサービスに絞り込むことを推奨します。 本方針が関連するステークホルダーにおいて効果的に実施されるためには、合理的な制度設計が必要であり、この点において、個別事業者向けの専用設計品等に関しては届出を不要とすることや、機器更新等の重要電子計算機の変更に伴う届出の負担を配慮した方針案の考え方を我々は支持します。 また、本法及び方針案に沿い、クラウドサービスプロバイダーではなく、特別社会基盤事業者によって直接さまざまな対策が継続的に実行されるようにすることも重要です。 そして、届出手続においては、過度に詳細な情報の開示を義務付けることは避けるべきです。特に、企業秘密やシステム・セキュリティー関連情報など、供給者が特別社会基盤事業者と共有することが困難な情報を収集することを特別社会基盤事業者に求めないことが重要です。	特定重要電子計算機の届出を求めるにあたっては、基本方針第４章第２節⑴に記載のとおり、特別社会基盤事業者等の負担にもよく留意しつつ、実情に応じた合理的な制度設計・運用となるよう努めてまいります。頂いた御意見はその参考といたします。
44	該当箇所：第１章第５節⑴ 重要電子計算機の定義の考え方 意見：官民連携を強化し、我が国全体のサイバーセキュリティ能力の向上を図ることの重要性は理解する。 一方で、日々多様なサイバー攻撃が多数発生しており、各社のサイバーセキュリティ部門も日常対応に相当のリソースを割いている現状を踏まえると、効果的なセキュリティ強化のためには、まずは優先度の高い領域に注力して取り組むことが重要である。 実際、昨年度5月より開始された経済安全保障推進法に基づく届出対応においては、事業者側でも相当な工数を要している状況にある。制度対応に過度な負担が生じ、結果として日常的なサイバーセキュリティ対応が手薄になるような事態は避けるべきである。 また、設備に関する情報は、通常、外部には公開されない極めて機微な情報である。万が一それらの情報が漏洩した際は、これまで攻撃者が入手できなかった内部情報を提供する結果となり、かえってセキュリティリスクを生じさせるおそれがある。したがって、提出を求める情報についても、目的達成に真に必要な範囲に限定するべきである。 優先度の高い領域として、具体的に指定すべき重要電子計算機は、基本方針案で示された「サイバー攻撃を受けた場合に、国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれがあるような一定のもの」との考え方を踏まえ、例えば電気通信事業分野においては、電気通信事業の役務の安定的な提供に影響を及ぼし、国家や国民の安全を損なう事態を生ずるおそれがある機器とするのが適当と考える。そのため、機器の登録範囲は、電気通信事業としての通信サービスの安定提供に必要不可欠な機器＝「商用に供する設備」に限定すべきと考える。 また、「特定重要電子計算機の届出情報に関しては、内閣府が横断的に管理し、例えば脆弱性情報や特定侵害事象等の報告情報との照合など、必要な整理・分析を行った上で、特別社会基盤事業者に対して、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施するために活用する」という目的を踏まえると、一の事業を守るのではなく国全体の重要インフラ事業を守ることに資する取組みであると理解している。この目的においていち早くインシデント情報や脆弱性情報を収集・展開すべきは外部から攻撃を受けるアタックサーフェスであること、また、通信事業者の場合、ネットワークの性質上、「特定重要設備と接続され、一定の情報のやり取りが可能な情報システム」はあらゆる機器が該当してしまい、そのすべてを届出することは現実的ではないことからも、最もリスクが高いアタックサーフェスに特化して指定すべきと考える。	同上

45	＜対象＞ 22ページ 3～6行目　特別社会基盤事業者自らが直接管理していない特定重要電子計算機に係る届出については、その特別社会基盤事業者の対応に係る負担の大きさにもよく留意しつつ、実情に応じた合理的な制度設計・運用となるよう努めることとする。 ＜意見＞ (1)第三者が特定重要電子計算機を管理し、複数の特定社会基盤事業者が利用している場合、同一内容を複数の特定社会基盤事業者から届出を行うのは事業者、政府双方にとって負担であり、メリットもないことから、当該ケースにおいては特定重要電子計算機を管理する第三者から直接届出を行う運用を検討いただきたい。 (2)特定重要電子計算機の届出においては、経済安全保障推進法でも届出を行っており、同情報の活用についても検討いただきたい。また、経済安全保障推進法に関する届出はe-Govを使用しているが、本法に基づく特定重要電子計算機の届出、インシデント報告要領について、経済安全保障推進法と平仄をあわせる形で検討いただきたい。	同上
46	＜対象＞ 23ページ 16～19行目　また、特別社会基盤事業者自らが直接管理していない特定重要電子計算機に係る特定侵害事象等の報告については、その情報の取得可能性やその特定重要電子計算機に係る管理の実情にもよく留意しつつ、合理的な制度設計・運用となるよう努めることとする。 ＜意見＞ 第三者が特定重要電子計算機を管理し、複数の特定社会基盤事業者が利用している場合、同一内容を複数の特定社会基盤事業者から届出を行うのは事業者、政府双方にとって負担であり、メリットもないことから、当該ケースにおいては特定重要電子計算機を管理する第三者から直接届出を行う運用を検討いただきたい。	同上
47	P21　21行目 「横断的」に管理をするとはどういう管理か。誰がどのタイミングでどこの情報にアクセスしたのか、管理のトレースができるようにして頂きたい。	特定重要電子計算機の届出は、法第４条第１項及び第２項の規定により、特別社会基盤事業者の所管省庁に届け出られ、当該所管省庁は内閣府に通知することとされており、これを脆弱性情報の提供等に活用するため、今後整備するシステムの下で、内閣府において横断的に管理します。頂いた御意見は今後の制度運用の参考といたします。
48	P21 27行目 「個別事業者向けの専用設備品等」とは、汎用品でなくインデント製品であれば届出の対象外という理解でよいでしょうか。個別事業者向けの専用品の定義を明確にして頂きたい。また、対象外とする理由は何かご教示頂きたい。	特定重要電子計算機の届出情報は、特別社会基盤事業者に対する脆弱性情報の提供等のために活用するため、個別事業者向けの専用設計品等に関しては届出不要とします。届出義務の対象範囲については、今後、政省令等の策定を通じて明確化を図ってまいります。
49	P22 7行目 「既設特定重要電子計算機」とは、タイミングは納入時、運転時など様々起算点が考えられることから定義が必要ではないかと考えます。	頂いた御意見は今後の制度設計における参考といたします。
50	弊社は、貴府のサイバー対処能力強化法の施行及び省令制定を含む、特定不正行為による被害の防止に向けた活動を支持いたします。弊社は、本法の主旨に基づく適切な対応を通じて、貴府及び関係省庁における本法の円滑な施行に貢献させていただく所存です。つきましては、次の点について確認させていただきたく存じます。 「第４章 第２節 (1)特定重要電子計算機の届出の考え方」において、既設特定重要電子計算機について施行後6月の経過措置が規定されています。また、施行後6月の間に新たに導入する特定重要電子計算機であって、既設特定重要電子計算機と一体として運用するものについては、既設特定重要電子計算機と同一時期に届出を行うことが適当であると考えらえる旨の記載がございます。 この同一時期の意味は、例えば、いずれも施行後6月以内で、既設特定重要電子計算機との一体運用が予定されている新たな特定重要電子計算機の届出準備がn月に完了し、既設特定重要電子計算機の届出準備がn＋2月に完了するという前提で考えた場合（又はこれらの前後が逆の場合）、(1)両届出をn月に前倒して行う必要があるという意味か、(2)両届出の準備が完了するn＋2月に行うことで良いという意味か、いずれが正しいでしょうか。	施行後６月以内に新たに導入される特定重要電子計算機（既設特定重要電子計算機と一体として運用するもの）については、施行後６月以内の既設特定重要電子計算機の届出と同一時期に届出を行うことが認められる、という趣旨になります。このため、御質問のn+2月が施行後６月以内であれば、(2)でよいということになります。
51	[該当箇所：第４章２節（２）、第５章第２節、第５節]＜侵害事象（インシデント）の報告＞ 方針案の第4章第2節(2)では、特定重要電子計算機に影響を及ぼすおそれがある特定侵害事象について、特別社会基盤事業者に報告を求める新たな義務についての考え方が示されています。方針案において、報告様式の統一化や官民連携基盤による報告窓口の一元化等、影響を受けるステークホルダーの負担軽減を図る考え方が示されていることを我々は高く評価しています。特別社会基盤事業者と政府双方にかかる追加的な作業負担を最小化し、恩恵を最大化する侵害事象（インシデント）報告要件の在り方を今後も継続的に模索することを推奨します。特別社会基盤事業者に課される義務は、重要なITサービスを提供している事業者に直接的・間接的に影響を及ぼす可能性があります。 この点において、サイバー侵害事象報告要件に関し、国内では省庁横断的に、国際的には新たな国際的動向と整合させる方向性が方針案において示されていることを歓迎します。多くの大規模なサイバーセキュリティインシデントが分野横断的・国境横断的な性質を持つことを踏まえれば、日本政府の制度が他の主要法域の制度と整合すればするほど、国内企業も多国籍企業も、より調和した、効果的かつ迅速な対応ができるようになります。その目的は、日本にある企業に独自のコンプライアンス義務を課すことではなく、重大な侵害事象を迅速に特定・緩和して被害を最小化することであるべきです。 特に、サイバーセキュリティ侵害事象が「報告対象」であるか否かを判断するためのリスクベースの閾値を設定する際には、産業界のパートナーや関連するステークホルダーと緊密に連携することを推奨します。報告対象となるサイバー侵害事象は、重大な損害をもたらし、企業の重要な機機能の提供能力を損なう実際のサイバー侵害事象のみが含まれるように狭く定義する必要があります。侵害事象が疑われる場合や、単にリスクを伴ったり、危険にさらしたり、もしくは、その他の方法でサイバー侵害事象が発生する可能性を高める場合等は含まれないようにするべきです。この点において、ファイアウォール等のインターネットとの接続点となる機器については、平時から大量の攻撃性通信をブロックしており、そのような事象まで含めて一律に報告を求めると、特別社会基盤事業者に過度な負担を強いることが方針案において認識されていることを高く評価します。 また、報告義務の開始および関連する時間軸は、特別社会基盤事業者が報告義務の対象となった侵害事象を認識した（すなわち、判断した）時点とすべきです。方針案において、明確に侵入を検知した後の事象のみを対象とする方向性が示されていることを我々は支持します。特別社会基盤事業者が侵害事象に遭遇したという疑いまたは確信に基づいて義務を課すべきではありません。この点は、本法第５条において規定されている「特定侵害事象の原因となり得る事象」を今後、定義する上で特に重要となります。最近公表された、「官民連携の強化に向け今後具体化が必要な論点」においては具体的な事象の痕跡を認知した場合に報告を求める対応とする考えが示されています。侵害事象報告制度を実用的かつ効果的にするために、「痕跡」とみなされる範囲を絞りこむことを推奨します。	特定侵害事象等の報告を求めるにあたっては、基本方針第４章第２節⑵に記載のとおり、特別社会基盤事業者等の負担にもよく留意しつつ、実情に応じた合理的な制度設計・運用となるよう努めてまいります。 また、御意見の趣旨を踏まえ、協議会に関しては、「協議会の構成員による自発的な相互の情報提供・意見交換等を活性化させていく」と修正します（基本方針第６章第２節）。 特定侵害事象等の報告を求める範囲については、基本方針第４章第２節⑵に記載のとおり、報告を行う事業者において判断を迷うことがないよう、既存のフレームワークも参考に、設定します。その際、例えばファイアウォール等のインターネットとの接続点となる機器については、平時から大量の攻撃性通信をブロックしており、そのような事象まで含めて一律に報告を求めると、特別社会基盤事業者に過度な負担を強いることとなるため、例えば明確に侵入を検知した後の事象のみを対象とするなど、官民での有効な対処及び事業者の負担の観点から適切に報告範囲を設定します。 また、報告の期限についても、基本方針第４章第２節⑵に記載のとおり、諸外国での同様の報告手続を設けている国の例や、官民で有効な対処を行う観点も踏まえて期限を設定します。 頂いた御意見は、その制度設計の参考といたします。

52	[該当箇所：第４章２節（２）、第５章第２節、第５節]＜侵害事象（インシデント）の報告＞ 方針案では、報告の期限について「諸外国での同様の報告手続きを設けている国の例や、官民で有効な対処を行う観点も踏まえて期限を設定することとする」と記されています。政府が様々な国際基準を参照していることを我々は高く評価します。報告対象侵害事象に該当すると事業者が判断した後でも、侵害事象の性質を理解するのには時間がかかることがよくあります。多くの場合、企業は簡易な通知を迅速に提供できるものの、米国の重要インフラ向けサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act、CIRCIA）のように 72 時間以下にならない基準を課すことで、特別社会基盤事業者は、１） 侵害事象の理解と対応に集中し、２）政府にとって有用な報告を提出する時間を確保することができます。企業の限られたリソースをインシデント対応からコンプライアンス義務にシフトさせることは逆効果です。企業は、政府関係者に可能な限り最新の情報を確実に提供することに尽力しています。そのため、速報を提出するための十分な時間を設けることを強く推奨します。	同上
53	[該当箇所：第４章２節（２）、第５章第２節、第５節]＜侵害事象（インシデント）の報告＞ 特定侵害事象等の報告内容については、不確実な内容も含めて報告時点で判明した事項を記載すれば速報として足りることとするという考え方が方針案では示されています。速報に必要な情報を政府が詳しく定義する過程においては、特別社会基盤事業者が把握している１） 悪意のある行為者についての情報（戦術、手法、手順を含む）、２） 脆弱性（どのように悪用されたかを含む）、３） 影響を受けた情報および情報システム、といった情報に限定すべきです。特別社会基盤事業者が供給者から収集した侵害事象報告情報は、特別社会基盤事業者の従業員、その産業を所管する省庁や内閣府など、関連組織の幅広い主体と共有される可能性があることを考慮し、こうした情報には企業秘密や機密性の高い専有情報が含まれるべきではありません。	同上
54	p.23 16-19行目 特別社会基盤事業者自らが直接管理していない特定重要電子計算機については、特別社会基盤事業者からの特定侵害事象の報告は不要で、電子計算機の供給者側からの報告のみで充足できるようにしていただきたい。もし両者の報告が必要となるのであれば、両者間の情報の紐づけ連携をどう行うか（報告の順番や付番等）が重要となる認識であり、その方式をご教示いただきたい。	同上
55	○報告要件の整合性と調和 コンプライアンス負担の軽減と対応時間の短縮のため、EUのNIS2における72時間初期通知モデル、オーストラリアの2024年サイバーセキュリティ法に基づく72時間報告要件、または米国で導入予定の72時間インシデント報告要件など、主要な規制枠組みと報告期限・内容を整合させるべきです。特に留意すべきは、これらの各枠組みには、インシデントのトリアージおよび対応活動において、インシデントの範囲や規模に関するその他の関連事実が特定された場合に備えた、フォローアップ報告に関する規定が含まれている点です。 提出される報告の内容に関しては、内容を標準化し、機械可読とすべきです。報告テンプレートはMITRE ATT&CKやVERISなど広く採用されているフレームワークに対応し、相互に防御することを可能にする脅威関連要素を特に重視するとともに、必要不可欠な場合を除き被害者を特定する観測可能な要素の範囲を限定すべきです。項目を例示すると次のとおりです：攻撃ベクトル、戦術・手法、侵害の兆候（例：ドメイン、IPアドレス、ファイルハッシュ）、影響を受けたシステムと機能的影響、既知の最も早い発生時刻と滞留時間、連絡先。 テンプレートは中核部分で業界を問わない設計としつつ、関係省庁や業界専門家による審査を経た業界固有の付属文書を許可し、明確な事例を示して曖昧さを軽減すべきです。重要な点として、事実を確認した後に適時に更新が行われる場合、初期データが不完全であったことを理由に事業者が不利益を被るべきではありません。 ○結果指標と実際の運用影響を伴うインシデントに焦点を当てる 対象範囲と報告の基準に関しては、重要性と対象ネットワークにおけるインシデントの確定を重視した政策を採用すべきです。報告対象となる「特定セキュリティインシデント」は、システムまたはデータの機密性、完全性、可用性の実際の損失または侵害をもたらす確定した事象、あるいは運用上の安全性や回復力に重大な影響を与える事象と定義されるべきです。対照的に、スキャン・プロービング・ネットワークエッジで遮断された汎用攻撃・セキュリティ関連性のない偶発的停止など日常的なバックグラウンド・ノイズは対象外とすべきです。これらの基準を明確化し、対象コンピュータ／ネットワークシステムを侵害する個別インシデントに焦点を当てることで、対応者や当局の負担軽減、「アラート疲労」の防止、報告エコシステムの分析的シグナルを高めることが可能となります。	同上
56	該当箇所：第４章第２節⑵ 特定侵害事象等の報告の考え方 意見 サイバー攻撃は軽微なものを含めると日々多数検知しており、その全てを報告することは現実的ではないため、特定重要設備の稼働や役務提供に実際に影響を与えたもののみを対象とすることを要望する。 また、同じ報告を複数求められることのないよう、既存のルールとの整合性・統合を図っていただきたい。 インシデント報告の期限については、有識者会議の資料には欧米主要国の例も参照しながら設定（速報：12~72時間、確報：1ヶ月程度）と記載されているが、調査期間に相応の時間を有する（場合によっては1ヶ月以上要する）ケースもあるため、期間設定は考慮いただくよう要望する。	同上

57	弊社は、基本的方針（案）の趣旨に深く賛同いたします。本基本方針（案）における官民連携をさらに円滑かつ効果的に推進するための弊社意見を、以下の通り提出させていただきます。今後のご検討において、ご参考としていただければ幸いです。 〇特定侵害事象等の報告関連 「報告を行う事業者において判断に迷うことがないよう、サイバー攻撃に用いられる戦術等を体系化した既存のフレームワークも参考に、その報告を求める範囲が明確となるよう設定する。」との記載に賛同し、各特別社会基盤事業者がベンダーから入手して報告すべき情報についても、範囲、粒度、及びタイミング等に関する規定の表現や運用について、明確な設定を期待します。規定に曖昧さが残る場合、特別社会基盤事業者からベンダーに対して念のため多めに情報を要求するという事態が発生し、結果として情報共有過程の末端に存在するベンダーの負担が制度設計時の想定を遥かに超えて増大するおそれがあります。 基本方針案において、報告形式の標準化や報告窓口の一元化による報告者の負担軽減をご検討いただいていることを歓迎します。数多くの業種の特別社会基盤事業者にサービスを提供しているクラウド事業者としては、これらに加えて、特別社会基盤事業者がベンダーから入手すべき情報報告内容が、特別社会基盤事業者の業種に関わらず統一されることを期待します。顧客の業種ごとに異なる報告内容が必要となった場合、ベンダーの対応が煩雑化し、初動対応中のセキュリティ部署にとって大きい負荷となるおそれがあります。 報告対象の設定について、特定重要設備そのもの以外については、例えば明確に侵入を検知した後の事象のみ対象とするなど、民間の負担軽減も考慮した設定とするという基本方針の記載に賛同します。 特定侵害事象等の報告期限について、「同様の報告手続きを持つ他国の事例に基づき、また効果的な官民対応の必要性を考慮して設定される」べきとの基本方針案の記載に賛同いたします。 本制度における特定侵害事象等の報告枠組みでは、ベンダーから特別社会基盤事業者の報告義務のために提供した情報は、特別社会基盤事業者の従業員や各関係省庁を含む関連の幅広い関係者にアクセス可能となることが想定されます。情報にアクセスできる人数が増えるほど情報の他への漏洩リスクが高まることを踏まえると、情報の性質に応じた適切な情報共有の経路や制度の選択も重要と考えます。本報告制度において、特に特別社会基盤事業者がベンダーから入手すべき内容には、営業秘密や機密性の高い情報が含まれないことを要望いたします。 特定侵害事象等報告により提出された情報に脆弱性情報等を含みうるため、政府内での厳格な取扱の実施を要望します。特に以下の点について考え方をお示しいただけますとありがたく存じます。また、具体の制度設計において、特別社会基盤事業者経由で情報を提出するベンダーに対してもステークホルダーとして綿密な意見交換を実施いただくことを要望します。 ・政府内のアクセス制限（重要経済安保情報の取扱い業務を許可された正職員（民間出向除く）など） ・情報公開請求の開示対象外の整理 ・他の関係機関と共有する基準の厳格な運用（匿名化された分析のみの共有等）	同上
58	P.22の特定侵害事象等の報告に関して、「特定重要設備の機能が低下するおそれが特に大きいもの」については、セキュリティ担当者が報告対象の事案をもれなく把握できるよう政省令・ガイドラインにおいて分かりやすい基準や業種別の事例を設けていただきたいです。また、基準や事例の策定に当たっては、報告対象件数が過大にならないよう、事業者からのヒアリングを行っていただきたいです。現時点で、政省令を検討するに当たっての事業者へのヒアリングの予定又は実績がありますでしょうか？	特定侵害事象等の報告を求める範囲については、基本方針第４章第２節⑵に記載のとおり、報告を行う事業者において判断を迷うことがないよう、既存のフレームワークも参考に、設定します。 政省令の検討にあたっては、従前から特別社会基盤事業者との意見交換を行ってきておりますが、事業者の御意見も伺いながら、事業者の実情にもよく留意しつつ検討を進めてまいります。
59	クラウドサービスの利用への対応とプロバイダーの負担軽減 クラウドサービスが本法の対象となり得ることを踏まえ、以下の明確化と配慮を要請します。 ・クラウドサービスプロバイダーの役割の明確化：本法（サイバー対処能力強化法）自体にはクラウドサービスへの言及はありませんが、基本方針（案）では、特別社会基盤事業者の特定侵害事象の報告義務の文脈において、当該事業者が使用する「特定重要電子計算機」に加えて、その機能がクラウドサービス上で実装されている場合は、クラウドサービス等の情報システムについても侵害事象の報告を求める範囲を明確に設定する、と記載されています。この場合、当社の理解では、特別社会基盤事業者は、当該関連するクラウドサービスを含む特定重要電子計算機に関連する特定侵害事象の発生などを報告しなければならないということになります。基本方針（案）における定義の拡大によって、特定重要電子計算機の機能をホストしていると見なされるクラウドサービスを含むあらゆる情報システムが負う義務が、特別社会基盤事業者の上記の報告義務を支援することに限定されることをご確認ください。 ・円滑な報告の支援： 我々は、機能がクラウドサービス上で実装されている場合に、「特定侵害事象」の報告に関するアプローチを様々なクラウドサービスの利用形態に基づいて整理するという方針を支持します。この「クラウドサービスの利用形態」とは、IaaS、PaaS、SaaSのような異なるクラウドサービスモデルを意味するのでしょうか。さらに、被害組織の負担軽減と政府の対応迅速化の観点から、統一的な報告様式および報告窓口の一元化の調整を促進するという方針を支持します。我々は、保護を奨励するために、報告の期限を明確化すること、報告の対象となる重大性の閾値を定義すること、そして企業に強力な法的責任の保護（免責）を提供することを政策として要請します。	特定侵害事象等の報告義務については、法第５条の規定により、特別社会基盤事業者が特定侵害事象等の発生を認知したときに報告することを求めています。こうした規定の下、特別社会基盤事業者がクラウドサービスを利用している場合には、頂いた御意見も参考にしつつ、実情も踏まえた制度設計・運用となるよう努めてまいります。「クラウドサービスの利用形態」とは、主に、IaaS、PaaS、SaaSといった形態を想定しておりますが、今後、実情も踏まえて検討を進めてまいります。
60	p.23 第4章 第2節(2) 「特定侵害事象の報告の考え方」で、「政府として把握したい事象についての目安をより抽象的に設定し～」とありますが、これは、p.22「その報告を求める範囲が明確になるよう設定する」との記述と一見矛盾しているように読めてしまうと思います。この「抽象的」の意図としては、「把握したい事象について細かい項目を明確化すると報告する側の負担になるため、抽象的にする」との理解で合っていますでしょうか？もしそうであれば、 ・「報告を求める範囲」と「政府として把握したい事象」は何れも「具体的に(明確に)設定」する。（特に義務として求める範囲は明確にする） ・ただし、「政府として把握したい事象」については、できる範囲で報告すればよい。 ということがわかる記載に修正していただけないでしょうか。	「政府として把握したい事象についての目安をより抽象的に設定し～」の部分については、その報告を求める範囲が明確になるよう設定する、法第５条の規定による「特定侵害事象等の報告」とは別に行う情報収集に関する記載です。この旨が明確となるよう、「このため、法第５条の規定に基づく特定侵害事象等の報告の範囲とは別に、政府として把握したい事象についての目安をより抽象的に設定し～」と修正します。
61	p.22.22-32行目 不正な通信を検知した場合に報告を行うという基準は、金融庁の監督指針にて金融機関に対して示されている、金融機関におけるサイバー攻撃発生時の報告基準と異なっていると思料する。そのため、このケースはNCOのみ、このケースは金融庁とNCO両方、といったような報告先の違いにより混乱が発生する可能性があると思料する。報告の基準は異なっていても、報告窓口が統一されているのが望ましいと思料する。	基本方針第４章第２節⑵に記載のとおり、サイバー攻撃に係る被害組織の負担軽減と政府の対応迅速化を図る観点から、関係行政機関で緊密な連携を図りつつ、特定侵害事象等の報告と他の法令に基づく報告の様式の統一化に加えて、官民連携基盤による報告窓口の一元化について所要の調整を進めてまいります。

62	インシデント報告の方式として、自動化／省力化での報告を主流とし、政府でアプリケーションやポータル等を準備し、多くの情報を入力せずにシステム上で各社の報告が受け取れるよう整備するべき。（第4章 第2節（２）｜ 23頁 L.22～27 及び 23頁 L.11～13） 令和7年10月に国家サイバー統括室は、サイバー攻撃による被害発生時のインシデント報告様式の統一というインシデント報告における事業者負担軽減策を実施したこと及び今後官民連携基盤による報告窓口の一元化を進めると表明していることを歓迎する。この点について、さらに迅速なインシデント報告を実現するためには、その方式として自動化／省力化での報告を主流として進めることを提案する。加えて、機械的な共有を行うにあたって、収集・整理・分析を効率的に行うことを目的として政府が受け取るデータ形式の統一化を図ることも重要であると考える。	頂いた御意見は、今後の制度設計・運用における参考といたします。
63	政府が収集する情報（通信情報や、基幹インフラ企業の特定重要計算機情報、インシデント報告など）は、目的に照らし適切な範囲とすべき。それらの情報が漏洩した場合、日本全体が危機となる。対策に必要な情報の収集・活用は必要であるが、政府に機微情報が集中すると攻撃対象となりうる事のリスクも考慮し、真に必要な情報に限って収集して頂きたい。収集した情報はセキュリティ対策に万全を期して管理して頂きたい（暗号化・分散保管など）	法第４条の規定による特定重要電子計算機の届出情報や法第５条の規定による特定侵害事象等の報告情報を含め、本法に基づき政府が収集する情報は機密性の高い情報も含まれることから、法の規定及び基本方針に則り安全管理措置を講じてまいります。また、その情報提供にあたっては、法第43条の規定に則り、また基本方針第５章第４節に記載のとおり、事業者の権利利益の保護に十分に配慮します。頂いた御意見は今後の制度運用における参考といたします。
64	○民間パートナーからのインシデント情報の責任ある利用 基本方針は、サイバー防衛に必要なデータを機械的・自動的に分離することを可能とするデフォルトの自動フィルタリングや、サイバー通信情報監視委員会による独立した検査など、機密情報を保護するための重要な措置を講じています。政府が高価値かつタイムリーな分析を行えること確保しつつ、信頼と参加を最大化するため、私たちは、重要なインシデント情報を公表・開示から保護している他の国際的なインシデント報告制度のベストプラクティスを反映した、明確で原則に基づく枠組みを制度化することを推奨します。 第一に、目的限定は明示的かつ狭くすべきです（第2章第3条第2項「他目的利用に関する配慮事項」、第5章第4条「情報提供にあたって必要な配慮（権利・利益の保護）」）。民間パートナーからの通信情報及びインシデント報告は、重要コンピュータ・ネットワークへの損害の防止、軽減、修復、並びに当該システムの復旧の支援にのみ使用されるべきです。「他目的利用」での使用は、提供当事者からの個別ケースごとの書面による明示的同意を条件とし、かつ本法で規定されたサイバーセキュリティ目的に拘束されるものとすべきです。 第二に、匿名化をデフォルトとすることです。報告主体及び利用者の権利・利益を保護しつつ広範な価値を有する分析を引き出すため、政府は共有可能な脅威要素（例：TTP、侵害の兆候、攻撃者インフラ識別子）の収集・分析を優先し、防御行動に厳密に必要な場合を除き、被害者を特定可能な観測データの収集を避けるべきです。 第三に、相互性とフィードバックループを保証すべきです。提供者は、自身の提出物と集約データセットから導出された、タイムリーで実用的な匿名化された助言（アドバイザリー）を受け取る必要があります。これには、観測された事象を既知のTTP（戦術・技術・手順）にマッピングし、活動中の攻撃者インフラを特定し、セクター関連コンテキストと推奨される緩和策を提供することが含まれます。 第四に、強固なセキュリティガバナンスは信頼の基盤です。フィルタリング後の通信情報と報告データを扱う中央リポジトリは、ISO共通基準など広く採用されている国際的枠組みに準じた中程度の影響基準を満たすか、またはそれを上回るセキュリティ管理を実施し、継続的監視と定期的かつ独立した評価を行うべきです。 最後に、標準化されたテンプレートの利用を通じて予測可能性を確保し同意を得るべきです。基本方針が当事者間合意のモデルを提供しようとする意図を有していることは極めて有意義です。これらのテンプレートでは、対象となる情報のカテゴリー、適用されるフィルタリングと匿名化処理、利用目的、アクセスと保持の管理、必要に応じて「他の目的」へのオプトインを可能とする仕組みを明確に規定すべきです。	同上
65	[該当箇所：第４章２節（２）、第５章第２節、第５節]＜侵害事象（インシデント）の報告＞ 方針案第5章第5節で述べられているように、侵害事象に関連する情報は、漏えいした場合に悪用される可能性があり、本法に基づく政府の情報取得等に対する国民の信頼を損なうおそれがあることから、公表前に適切な措置を講じるべきです。情報取扱者の特定、研修の実施、保管庫の施錠等の物理的な安全管理措置、電子ファイルのアクセス制御等の技術的な安全管理措置の確保といった組織的な安全管理措置を講じるという方針案の考え方を我々は支持します。 政府は、上記のサイバー侵害事象報告で得られた情報を、一般市民に情報公開を義務付ける法律や政策から保護し、サイバー侵害事象報告から収集した匿名化された分析結果のみを他のサイバーセキュリティ関係者と共有すべきです。これにより、企業が情報を共有する際の障壁が低減され、企業被害のさらなる拡大の可能性が低減され、他の企業のサイバーセキュリティが改善されます。	同上
66	重要電子計算機や特定重要電子計算機の構成に係る情報は、経営上の重要情報であり、攻撃のターゲットとなり得ると考える。本データベースの構築・運用に当たっては、構成、アクセスコントロール、監視など、十分に高いセキュリティを具備することが必須である。	同上
67	該当箇所：第５章 第５節 安全管理措置 意見：届出情報や協議会の中で共有した情報の中には、通常、外部には公開されない機微な情報も含まれるため、万が一漏洩した際には、かえってサイバー攻撃のリスクを高める恐れがある。そのため、収集した情報が不要になった時点で削除することや、報告の際にはExcelファイルをメールで送付するような方法ではなく、セキュリティを確保できるシステムを活用するなど、情報漏洩を防ぐ仕組みの整備が必須と考える。	同上
68	脅威情報の共有には被害企業を特定できる情報が含まれることがあり、法的保護がない場合、クラウドサービス事業者は顧客からの守秘義務違反や、競合他社からの独占禁止法違反で訴訟を受けるリスクがある。そのため、政府提供の情報に基づき防御措置を実施し、それが事業者に影響を与えた場合、クラウドサービス事業者を民事訴訟から保護する免責規定が必要である。	同上
69	P23 11行目 「特に重要な事業者」でいう「特に」の基準は分野毎に省令で定められるのでしょうか。	政省令に委任されている事項ではないため、政省令における規定は想定しておりません。

70	該当箇所：第４章第２節⑴ 特定重要電子計算機の届出の考え方 意見：現在、多くの事業者ではベンダから脆弱性情報を有償で入手し、自社の取り組みとして脆弱性対応を実施している状況である。能動的サイバー防御により、国をあげて日本全体のサイバーセキュリティ強化を図るという観点からは、現在は個社ごとに対応している情報収集の取り組みについて、国として取りまとめを行い、外国の政府等から提供を受けた情報、地政学的情勢等の攻撃の目的や背景に関する情報等、民間では収集が難しい情報など、事業者のサイバー対処能力強化につながる情報を提供いただくことを期待する。 また、特定重要電子計算機の届出等で得た情報等を用いて、実際にどの程度被害防止や早期対応に資する情報提供が行われたのか、被害防止のために効果的な情報が提供されているのかどうか、一定期間経過後に検証・評価を行うことが重要であると考える。	情報の作成にあたっては、基本方針第４章第３節⑴に記載のとおり、民間事業者のニーズもよく踏まえつつ、政府だからこそ取得や、整理・分析が可能な情報を基とした情報の作成に努めてまいります。また、情報提供後も、基本方針第５章第４節に記載のとおり、情報提供を受けた者からのフィードバック等を踏まえて、情報提供の在り方についても不断に改善を図ってまいります。
71	P21　5行目 その他の手法によりとは例えば何でしょうか。「経済安全保障推進法（基幹インフラ役務の安定的な提供の確保に関する制度）」で事業者が所管省庁に届け出た情報も情報の整理分析源の一つとして取り扱われるのか、他国からのインテリジェンス情報も含まれるのでしょうか。	その他の手法により収集される情報については、例えば、国内の関係機関や外国の政府等から提供を受けた情報、行政機関の端末における監視・分析データ等の行政機関が保有する情報が考えられます。
72	P25　20行目 内閣府は、重要電子計算機に対する特定不正行為による被害の防止に効果的な総合整理分析情報を作成するとありますが、「特定重要設備」に対する特定不正行為に関する情報は内閣府の分析対象からは除外されるという理解でよいでしょうか。	重要電子計算機のうち、法第２条第２項第２号に該当する特定重要電子計算機には、特定重要設備の一部を構成するものが含まれるため、内閣府の整理・分析の対象に含まれます。
73	基本方針（案）では、「種々の情報のデータベース化等による整理や、各種の情報間の照合等の分析を行う」と言及されている。本データベースの構築に当たっては、発見された脆弱性情報を元に効率的かつ迅速な対応を可能とする仕組みが必要と考える。ICT分野では、特定の製品を元に、顧客毎に異なる製品として提供するケースがあるため、製品間の関係性に着目し、発見された脆弱性の影響範囲を特定できるようなデータベースの設計を検討すべき。 また、ICT製品は頻繁な改版が実行されることを前提として、本データベースには、製品のサービスインの時点の構成からサービス終息までのライフタイムを通したバージョンコントロールを行う、CMDB (Configuration Management Database)の機能を持たせることが有効と考える。	頂いた御意見は、今後の制度設計・運用における参考といたします。
74	P21　18行目、P26　6行目　第5節　事務の委託に対する考え方 事務の一部の委託について、委託する相手は「重要経済安保情報保護活用法」で規定する適正評価（セキュリティクリアランス）を実施すべきと考えます。	頂いた御意見は今後の制度運用における参考といたします。
第５章　総合整理分析情報の提供に関する基本的な事項　関係		
75	P21 15行目 「重要電子計算機の被害防止に効果的な情報」とは具体的には何でしょうか。	例えば、サイバーセキュリティの実務の専門家が求める技術情報や経営層の判断に必要となる攻撃の目的や背景等に関する情報、政府が把握した公表前の脆弱性情報等が考えられます。
76	■　第５章第２節「総合整理分析情報等の提供先云々」の箇所に関して ・「外国の政府等に対する情報提供」ということに関して、はじめに述べたように安全に関する議論と、国家の安全に関する議論については、きちんと分けて考えられなければならない。国民の安全に関する問題については基本外国との広い連携等が必要な場合があると考えられる。国民の安全の問題を直ちに国家の安全という問題にすり替えられることがなりように、また、国家の安全が国民の安全と切り離されたり、対立的にならないように考えなければならない。	頂いた御意見は、今後の参考といたします。
77	P25　13行目 「提供用総合整理分析情報」は、重要経済安保情報保護活用法でいう「重要経済安保情報」との関係、違いは何でしょうか。	提供用総合整理分析情報は、本法第39条に規定されており、選別後通信情報を含まず秘密を含み得るものです。重要経済安保情報は、重要経済安保情報保護活用法第３条第１項に規定されており、重要経済基盤（重要なインフラや物資のサプライチェーン）に関する一定の情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを指します。
78	国の安全保障にかかわる機微な情報を扱うことを勘案し、いわゆるセキュリティ・クリアランス制度の活用も念頭に置きながら官民の情報共有により得られた情報は、日本のインテリジェンスベンダー育成に活用すべき。（第5章 第2節（３）｜ 29頁 L.8～11 または　第6章 第5節 ｜ 37頁 L.10～13） 原案の29頁 L.3においては、「提供用総合整理分析情報を提供する」とあるが、サイバー対処能力強化法第二十九条及び第四十五条 3項を見ると、提供用総合整理分析情報のみならず「その他情報」つまり提供用選別後情報等の共有が想定されているところ、記載を「提供用総合整理分析情報等を提供する」等に修正いただきたい。 加えて、提供用総合整理分析情報は、原案37頁L10.～13にあるように日本のいわゆるセキュリティ・クリアランスを取得したサイバー脅威インテリジェンスベンダー向けにMISP等のオープンソース・ソフトウェア（OSS）プラットフォームで機械的に提供するなど、具体的な情報の活用方法について民間事業者と検討し、民間事業者にとって情報の活用がしやすい形で官から民へ提供されることを期待する。	御意見を踏まえて「提供用総合整理分析情報等を提供する」と修正します。後段の御意見は、今後の参考といたします。
79	P27 第５章２節 重要情報を保有する装備品製造等事業者に該当する場合で、かつ特定社会基盤事業者に該当しない場合は、政府から情報提供はされないのでしょうか。	特定社会基盤事業者に該当しない、重要電子計算機を使用する者に対しても、重要電子計算機の被害の防止のため、情報提供を行います。
80	官⇒民で配布されることが期待される情報とは、戦略的インテリジェンス情報などの事業者のChief Information Security Officer（CISO）が自社内に警戒指示を出せるような情報や、戦術的インテリジェンス情報などの現場で脆弱性対応に即座に活用できるような情報を共有することを期待する。（第5章 第2節（３）｜ 29頁 L.1～7 または　第5章 第3節 ｜ 35頁 L.15～20） 原案へは本趣旨の記載があり歓迎する。一方で、原案該当部分は「サイバーセキュリティの実務を担う専門家が求める技術情報に限らず（中略）適切なタイミングで積極的に提供する」と記載があり、どのように提供がなされるかという提供方法について明記がされていない。今後どのようなデータ形式が現場で使いやすいか等民間企業と意見交換をしながら実効性のある形で政府から民間企業へ情報提供がなされるよう制度が運用されることを期待する。	頂いた御意見は、今後の制度運用における参考といたします。
81	p.30 第5章 第2節など 本法や第5章第2節などで、「内閣府は総合整理分析情報を（重要）電子計算機の使用者に提供」とありますが、「（重要）電子計算機(特定重要電子計算機以外)の使用者」は届出義務がありませんので、対象となる電子計算機をどのように把握をするのかを明記していただけないでしょうか？	第５章第２節⑸の「電子計算機を使用する者に対する周知等」においては、周知等用総合整理分析情報を公表や協議会等を通じた情報提供等により周知することを想定しておりますので、その旨が分かるよう修正します。
82	官民連携及び情報提供の強化 電子計算機及び関連機器の供給者として、我々は、重要電子計算機への被害を防止するため、内閣府または関係省庁が公表に先立って脆弱性情報を迅速に提供するという方針を支持します。我々は、脆弱性情報の提供に際して、その機密性と緊急性を考慮し、適切な情報提供と情報管理を確保するための努力を行うこと、および本法に基づく官民連携に関連する行政事務を効果的に遂行するために、関連する告示やガイドラインの見直しを行うことを要請します	基本方針第５章第２節⑹イに記載のとおり、脆弱性情報の提供に当たっては、その秘匿性や緊急性も踏まえて、適切な情報提供・情報監理に努めてまいります。また、脆弱性関連情報の取扱いについても、基本方針第５章第２節⑹イに記載のとおり、本法に基づく官民連携の強化に係る規定やその趣旨に基づき、関係する告示・ガイドラインの必要な見直しを行います。

83	「P30 ？電子計算機等供給者に対する情報提供等、脆弱性情報に係る情報提供 イ 脆弱性情報に係る情報提供」：脆弱性情報の提供に当たっては、受け取った特別社会基盤事業者が効率的に処理が行えるよう、システム的に処理可能な統一プロトコルで提供することは検討しないでしょうか。	頂いた御意見は今後の制度運用にあたっての参考といたします。脆弱性情報の提供に当たっては、基本方針第５章第２節⑹イに記載のとおり、情報の提供を受けた者がその対策を行うことができるよう、適切な情報提供に努めてまいります。
84	[該当箇所：第４章第３節（１）（２）、第５章第２節（４）（５）（６）]<脆弱性の公表と脆弱性対応の強化> 方針案第4章第3節(1)では、特定重要電子計算機の届出、脆弱性、特定侵害事象等の報告等、種々の情報を内閣府が収集し、データベース化等による整理や、各種の情報間の照合等の分析を行うことで、サイバー攻撃の予防措置や重要電子計算機を防護する組織（民間事業者を含む）における戦略的な意思決定・判断に効果的に活用できるようにすると説明しています。また、内閣府から当該情報（「総合整理分析情報」）の提供を受けた行政機関が、必要に応じて当該情報を加工し、関係機関・関係者と共有することで、情報受領者が具体的な措置を講じることを促すとしています。しかし、当該情報が公表されていない場合、情報共有はサイバーセキュリティに実質的なプラス効果をもたらさず、悪用される機会を増やす可能性があります。そのため、政府内での情報の発信に安全策を講じ、遅延させることを推奨します。また、方針案第5章第2節（6）において所管省庁からの要請を受けた際に電子計算機等供給者が講じなければならない「必要な措置」については、その要請が確認された脆弱性に焦点を当て、体系化された情報開示の慣行に沿った形で、その脆弱性に見合った適度な範囲にとどまるようにすることを強く推奨します。さらに、第5章第2節(4)では、政府が特定した公表前の脆弱性情報が、守秘義務および安全管理措置を課せられる協議会の構成員である特別社会基盤事業者と共有されると記されています。しかし、どのような公表前脆弱性情報が想定されているのか、また政府がどの主体から当該情報を取得するつもりなのかは不明確です。提案されている制度の運用意図をより的確に理解するためには、情報の範囲および取得・共有プロセスに関する一層の明確化が望まれます。さらに、方針案第5章第2節(5)では、マルウェア感染等により一般利用者の通信機器を利用して攻撃が行われることが増加していることを踏まえ、脅威情報に必要な加工を行った上で、重要電子計算機を使用する者に限らず、特定不正行為に用いられるおそれのある電子計算機を使用する者にも周知のために政府が情報を提供し得ると記されています。本措置の意図には賛同するものの、特に脆弱性に対するパッチが未提供の場合、政府が脆弱性を公に早期に開示するのは避けるよう求めます。ソフトウェアやハードウェアの脆弱性は避けられるものではありませんが、多くの場合、独立したセキュリティ研究者によって特定されています。そのため、このようなコンピューティングシステムのベンダーが、特定された脆弱性に関する第三者からの報告を処理するための手順を維持することが不可欠となります。この点に関して、情報セキュリティコミュニティは、「協調的脆弱性開示」（coordinated vulnerability disclosure、CVD）と呼ばれる一連の手順を開発しました。これは、ベンダーが第三者の利害関係者と協力し、一般への潜在的なリスクを軽減するのを支援するものです。すべての CVD 要件は、既存の国際的に認められた標準規格である ISO/IEC 29147 および 30111 に準拠する必要があります。CVD の指針は、脆弱性を修正できるベンダーに直接報告し、ベンダーが根本的な脆弱性を軽減するためのパッチを開発、テスト、展開する機会が得られるまで公開を延期することで、セキュリティが最大限に保護されるというものです。この基本原則を具体化するため、ソフトウェアベンダーは、第三者からの脆弱性報告に対応するための CVD プログラムを維持しています。これは、悪意のある攻撃者が未修正の脆弱性を悪用してシステムに侵入するリスクを最小限に抑える方法です。したがって、特定された脆弱性、特に特別社会基盤事業者が使用する重要なコンピューティングシステムに関連する脆弱性が検証され、確実に修正されるまで、公表されないようにすることを我々は政府に強く求めます。また、セキュリティ研究者、顧客、あるいは政府によって発見されたものであるかどうかに関わらず、新たに発見された脆弱性の報告をコンピューティングシステムベンダーが容易に受け取れるよう、ベンダーに対し、脆弱性開示ポリシーの公表を奨励します。脆弱性開示ポリシー は、特に製造業者が日本国外に所在する場合、所管大臣が製造業者に連絡を取り、脆弱性情報を共有する方法を提供するため、所管大臣にとっても有益です。製造業者が新たに発見された脆弱性を可能な限り迅速に是正できるよう、関係者が新たな脆弱性を内密に直接ベンダーに報告することを奨励するような方針とすべきです。	脆弱性情報の提供にあたっては、例えば、公表前の脆弱性情報については守秘義務の下での提供を行うなど、基本方針第５章第２節⑹イに記載のとおり、その情報の秘匿性も踏まえ、適切な情報管理に努めてまいります。また、関係省庁・関係機関による脆弱性関連情報の取扱いについては、基本方針第５章第２節⑹イに記載のとおり、本法に基づく官民連携の強化に係る規定やその趣旨に基づき、関係する告示・ガイドラインの必要な見直しを行い、見直した告示・ガイドラインに基づき取り扱うこととなります。頂いた御意見は今度の制度設計・運用の参考といたします。
85	弊社は、貴府のサイバー対処能力強化法の施行及び省令制定を含む、特定不正行為による被害の防止に向けた活動を支持いたします。弊社は、本法の主旨に基づく適切な対応を通じて、貴府及び関係省庁における本法の円滑な施行に貢献させていただく所存です。つきましては、次の点について確認させていただきたく存じます。 「第５章 第２節 (6) ア 電子計算機等供給者に対する情報提供等」において、重要電子計算機における脆弱性を悪用した特定不正行為による被害の防止のため、内閣府又は電子計算機等の供給を行う事業の所管省庁は、必要に応じて、公表前の脆弱性情報をその重要電子計算機の供給者に対して迅速に提供する旨の記載がございます。 「公表前の」とあることから、この脆弱性情報には、提供用総合整理分析情報に相当する情報（周知等用総合整理分析情報よりも秘匿性の高い情報）も含まれ得るものでしょうか。もし含まれる場合、当該提供用総合整理分析情報の提供を受けるためには、本法第45条に基づく協議会の構成員として加わることが必須になるでしょうか。	御理解のとおり、提供される脆弱性情報の秘匿性によっては、提供用総合整理分析情報に該当する可能性があります。提供用総合整理分析情報に該当する場合には、法第45条の規定により、協議会の構成員に提供することとなります。
86	P30 10行目～ ア 電子計算機等供給者に対する情報提供等 ここで提供される情報と、重要経済安保情報保護活用法でいう「重要経済安保情報」との関係、違いは何でしょうか。また、受け取った情報の廃棄時期・方法についてはどう考えればいいのでしょうか。受け取った情報に対して生じる義務は具体的に何でしょうか。	重要経済安保情報については前述のとおりです。法第42条第１項の規定により脆弱性に関する周知等用総合整理分析情報等の提供を受けることだけをもって、電子計算機等供給者に義務が生じることはありません。なお、基本方針第５章第２節⑹アに記載のとおり、サイバーセキュリティ基本法（平成26年法律第104号）に電子計算機等供給者の責務が規定されており、また、本法には、電子計算機等の供給を行う事業の所管省庁は、必要に応じ、電子計算機等供給者に必要な措置を講ずるよう要請することができる旨が規定されています。受け取った情報の管理等については、今後の制度設計・運用の中で検討します。
87	p.30 15-26行目 電子計算機の供給者が必要な措置を講じることができない、もしくは講じようとしないケースがあった場合に、当該電子計算機の利用者に対して当該電子計算機の利用を控えるような要請が発生することが有りうるのか。例えば、海外の供給者に対しては協力が得られにくいことも考えられ、このようなケースで特定社会基盤事業者側に発生する影響を理解したい。	御指摘の措置要請に関する記載は、法第42条第２項の規定によるものであり、同項の規定により特別社会基盤事業者に対し措置要請が行われることはありません。他方で、特別社会基盤事業者については、法第40条第１項の規定により、特別社会基盤事業者の所管省庁から、周知等用総合整理分析情報の提供を受けた者は、同条第２項の規定により、同情報を活用して、特定重要電子計算機に対する被害の防止のために必要な措置を講ずるよう努めなければならないこととされており、基本方針第５章第２節⑷に記載のとおり、例えば、提供される脆弱性情報が、特別社会基盤事業者の役務提供上重大なものと認められる場合等には、内閣府と所管省庁における緊密な連携の下で、所管省庁において適切な措置の実施を求めることがあります。なお、法第42条第２項の規定による電子計算機等供給者に対する措置要請も含め、同条第１項から第５項までの規定は、同条第６項の規定により、国外に所在する電子計算機等供給者が国内に所在する者に対し電子計算機等の供給を行った場合について、適用することとされています。

88	p.31　第5章 第４節 「～インシデントに係る情報を提供した事業者に対して政府からフィードバックを行うこと等により、政府に対して情報提供を行った事業者に対して、政府から積極的にフィードバック等を行い、～」については、同じ内容が繰り返されているので、以下のように修正してはいかがでしょうか。 「～インシデントに係る情報を提供した事業者に対して政府から積極的にフィードバック等を行い、～」	御意見を踏まえて、「～インシデントに係る情報等を提供した事業者に対して政府から積極的にフィードバック等を行い、～」と修正します。
89	インシデント報告を行った事業者は、一定程度の減責・免責がされる、対応についての政府からの実質的な補填が出るなど、事業者側にメリットが出るようにすべき。 （第4章 第2節（２）｜ 23頁 L.22～27） インシデント報告は法律に定められた義務ではあるものの、特定社会基盤事業者へは通常の企業よりもその対応分の負担が増加する。従って、インシデント報告を行った事業者においては、一定程度の減責・免責がされる、インシデント対応についての政府からの実質的な補填が出るなど事業者側に何らかのメリットが出るようにすべきであると考える。一例として、不正アクセス禁止法においては、都道府県公安委員会による援助を行うことが定められており、米国においても国土安全保障省及びサイバーセキュリティ・インフラセキュリティ庁が重大インシデントと宣言するケースにおいては、金銭的な補助を含む援助等を行うというCyber Response and Recovery Fundというものを設立するよう法律で定められている。また、特定社会基盤事業者以外の事業者においても、サイバー対処能力強化法におけるインシデント報告義務を負うわけではないものの、個人情報保護法等の法令に基づくインシデント報告義務は引き続き負うこととなる。その際、特定社会基盤事業者や政府のセキュリティ対策に寄与する情報を含むインシデント報告をおこなった者等、一定の基準以上を満たすインシデント報告に対しても同様のメリットを検討することで、特定社会基盤事業者に限らず民間から政府への自発的なインシデント報告が加速すると考える。	頂いた御意見は、今後の制度設計・運用における参考といたします。基本方針第５章第４節に記載のとおり、官民の情報共有がより活発となるよう、インシデントに係る情報等を提供した事業者に対して政府から積極的にフィードバックを行うこと等に取り組んでまいります。
90	我が国の国産事業者が中心となり、国内にデータがとどまる形でサイバー脅威情報の官民における活用サイクルができる制度を作るべき（第5章 第2節（３）｜ 29頁 L.8～11） サイバー対処能力強化法及び同整備法における官民連携については、民から官へのインシデントの報告や官から民へのサイバーセキュリティ関連情報の提供等、官民における情報(データ)の流通が大きな柱の一つである。それら流通するデータは安全保障に関するデータであるため、国産事業者が中心となり我が国の司法管轄権の及ぶ範囲にデータが留まるような制度及び情報通信基盤の下で扱われなければならないと考える。 加えて、官民における積極的な情報の流通がなされ、そのような情報を基にした政府におけるアクセス・無害化オペレーションの高度化がなされるために、民間事業者が国家サイバー統括室(NCO)をはじめとする政府機関への情報提供を行うインセンティブを感じるような制度設計が必須であると考える。 例えば、インシデント報告を行った際に一定程度減責・免責されることや、実質的な補填が政府から出ることや、新たに作られる協議会において情報共有を行うことでNCOや関係府省庁で独自の追加分析がなされフィードバックされるなどが挙げられる。	同上
91	政府機関としては、情報提供を受けた場合は秘密情報の確実な削除等により、その提供者が不利益を被ることがないようにされたい（第4節 ｜ 32頁 L.2～9） 民間企業から政府へのインシデントの報告情報、通信事業者から政府が受け取る通信情報、当事者協定に基づく特定社会基盤事業者から政府が受け取る情報及び協議会を通じて民間企業から政府が受け取る情報には、例えばITインフラの構成情報やアンチマルウェアソフトの検知名、被害範囲等が含まれ得る。一つの情報だけでは秘密が暴露しない場合でも複数の情報が重なり状況証拠が積み重なることで秘密情報が意図せず漏洩してしまう可能性もあることを念頭に、秘密情報の確実な削除等により情報提供者が不利益を被ることがないように留意されたい。	頂いた御意見は、今後の制度運用における参考といたします。基本方針第５章第４節に記載のとおり、政府に情報提供した事業者が不利益を被らないよう、事業者等の権利利益の保護に十分に配慮してまいります。
92	P27　26行目 事務の一部の委託について、委託する相手は「重要経済安保情報保護活用法」で規定する適正評価（セキュリティクリアランス）を実施すべきと考えます。	頂いた御意見は今後の制度運用における参考といたします。

第６章　協議会の組織に関する基本的な事項　関係		
93	P34　19行目～ 現在のサイバーセキュリティ協議会は廃止になるとのことですが、現在の協議会構成員のCISTAへのアクセスはどうなるのでしょうか。	今後の協議会の設計・運用の中で、その取扱いも含めて検討いたします。
94	該当箇所：第６章第１節 基本的な考え方 意見：「被害防止のために必要な情報に関する資料の提出の求めがあった場合における対応等が必要となる」という点について、事業者におけるセキュリティ対策やシステム構成、顧客との契約関係など、外部への提供が難しい、あるいは提供することで新たなリスクを生じ得るものも含まれる可能性がある。そのため、制度の運用にあたっては、情報の性質や機微性に応じて、提出の範囲や方法を柔軟に判断できる仕組みとすることが望ましい。こうした柔軟性を確保することにより、事業者側の協力がより円滑に進み、結果として制度全体の実効性向上にも資するものと考える。	頂いた御意見は、今後の協議会の設計・運用における参考といたします。
95	重要電子計算機や特定重要電子計算機の構成においては、外資系企業の製品・サービスが使用されているケースもあるため、協議会にはこれらの外資系企業の参画が必須である。外資系企業が積極的に本情報共有に関与できる仕組みやセキュリティクリアランス制度との関係の整理、海外政府からの情報共有等も含め、実効的な体制や仕組みを実現することが重要と考える。	同上
96	該当箇所：第６章 協議会の組織に関する基本的な事項 第４節 協議会の構成員　（P36） 意見：新たに設置される協議会では、「セキュリティ対策を行うベンダ」（以下、サイバーセキュリティ事業者）の参加も想定されています。そこで、サイバーセキュリティ事業者が協議会を通じて得た情報の自社サービスへの活用の意義や有効性についても議論し、許容される用途を基本方針に明記していただくことを要望します。 理由： １．具体的には、協議会を通じて共有される攻撃初期の情報（TTPsやIoC等）は、被害者が特定される情報を除去した形でサイバーセキュリティ事業者に共有されることを期待します。サイバーセキュリティ事業者がその情報を自社のセキュリティサービスに組み込むことによって、協議会に参加していない広範な企業・組織への被害拡大を防ぐことが期待できます。例えば、サイバーセキュリティ事業者がセキュリティ監視サービスに検知ルールを組み込んだり、脅威ハンティングのルールとして利用したりすることで、同様の攻撃手法による被害の拡大を防ぐことが期待できます。 ２．基本方針の検討過程においては、そのような活用も念頭にあると推測されますが、基本方針に明記いただくことで、サイバーセキュリティ事業者としては協議会を通じて得た情報の事業活用の是非について懸念を持つことなく、自信をもって進めることができます。 ３．また、協議会に参加するサイバーセキュリティ事業者のセキュリティサービスに共有された脅威情報を組み込むことによって、サイバーセキュリティ事業者から協議会及び協議会参加者へのフィードバックも期待できます。このフィードバックを通じて、共有すべき情報の種類・内容・時期などの精度を高めていくことが可能になると考えます。情報を共有する側としても、共有した情報に対する評価（役に立ったか、立たなかったか）がなければ、継続的に情報共有を行うモチベーションは維持されにくくなります。 ４．協議会を通じてサイバーセキュリティ事業者に共有される脅威情報を、サイバーセキュリティ事業者の事業で利用できるようにすることは、海外セキュリティベンダーに対して国産セキュリティベンダーを差別化する要因にもなると考えます。海外セキュリティベンダーはグローバル規模の観測網を通じて得られた膨大な脅威情報をもとにセキュリティサービスを展開していますが、我が国固有のシステムや脅威というものも存在します。協議会に参加するサイバーセキュリティ事業者が協議会を通じて共有される情報を事業に活用する明確な道筋を示すことで、我が国のサイバーセキュリティ事業者の育成にも資するものと考えます。	御指摘の点も含め、協議会の運用の詳細については、今後、サイバー関連事業者とも意見交換をしながら、具体化の検討を進めてまいります。
97	P37　10行目～ 11行目の「同法」とは重要経済安保情報保護活用法のことでしょうか。「セキュリティ・クリアランス制度を活用して」とありますが具体的にどのように活用するか明確にして頂きたい。例えば、協議会の構成員は同法における適正評価を受けた者に限るという意味でしょうか。	「同法」とは、重要経済安保情報保護活用法を指します。この点を明確にするため、記載を修正します。 重要経済安保情報については、必要に応じて協議会の構成員が取り扱えるようにするため、同法に基づくセキュリティ・クリアランス制度を活用するものであり、協議会の構成員となるために、適正評価といった重要経済安保情報を取り扱うための手続きを求められることはありません。このため、協議会の構成員は同法における適正評価を受けた者に限られるものではありません。 その上で、協議会の具体的な設計・運用に関しては、今後、検討を進めてまいります。
98	p.37 10-14行目 セキュリティ・クリアランス制度は施行されて間もない仕組みであり、取得に相応の期間を要すると想定している。協議会に参加するために、当該クリアランス取得に関してどのような対応が必要なのか、協議会のスタート時期を含むタイムラインと共にご提示いただきたい。	同上
99	■　第６章第５節「安全管理措置」の箇所に関して 「重要経済安保情報についても、必要に応じて適切な情報管理の下で協議会の構成員が取り扱えるようにするために、同法に基づくセキュリティ・クリアランス制度を活用して、協議会の構成員への情報提供を行う。このため、当該制度の活用に向けた調整を進める。」とあるが、重要経済安保情報については、広汎無限定になる恐れが強い概念であり、これと、セキュリティ・クリアランスを組み合わせ広く用いることについては、セキュリティ・クリアランス＝適性評価＝身辺調査は、調査対象者に留まらず、その家族等まで国籍、犯罪歴、精神疾患、飲酒の程度、借金の有無等まで調査することとなっており、調査対象者及びその家族等のプライヴァシーの権利などの基本的人権を侵害する恐れの強い、深刻な問題を持つ制度であることをきちんと理解をした制度設計でなければならないものである。思想・信条に関する事項の調査をすることももちろん許されない。上記「」書き部分は削除されるべきである。	重要経済安保情報については、重要経済安保情報保護活用法に基づき、適切に取り扱います。

第７章　その他重要電子計算機に対する特定不正行為による被害の防止に必要な事項　関係		
100	■　第７章第１節「制度及び基本方針の見直しに関する事項」の箇所に関して 「法附則第７条は、政府は、附則第１条第４号に掲げる規定の施行後３年を目途とし、特別社会基盤事業者による特定侵害事象等の報告、重要電子計算機に対する特定不正行為による被害の防止のための通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとしている。」とあるが、通信情報の取得について、どのような情報をどのような理由によって取得したかを具体的に検討すべきであること、検討の結果、その取得が不必要ないし有害であった場合には当該取得事案を一般・抽象化し、取得を禁ずるルールを明示する見直しを行うべきであること、を明記すべきである	頂いた御意見は今後の参考といたします。
101	アクセス・無害化措置について、各施策との連携にしか触れられていない。 参議院の附帯決議で示されているように、その適正性を担保するための記録の保存及び事後的検証、国際法上許容されることの担保するための外務大臣による検討、深刻な外交問題につながる懸念に留意して国際法上の整理を明確化等についても具体的に記載する必要がある。	基本方針は法第３条第２項各号に掲げる事項について定めるものであり、警察官職務執行法（昭和23年法律第136号）等を根拠とするアクセス・無害化措置については、法と関係する部分について記述しているものです。
102	■　第７章第３節「アクセス・無害化措置との連携」の箇所に関して 能動的サイバー防御ということで、内閣官房警察防衛省自衛隊等ということについての前のめりの記載は、冒頭で述べた国民の安全をいうことは題目のみとなり、でこれと別に国家の安全というものが、前に出て、かつ、外国というものについては、一般的外国でなく、敵国かどうかという概念が、つきまとってしまっているものである。攻撃されそうであれば攻撃をするなどということは一方でサイバー問題の安全保障保障の重要性をいうのであれば、宣戦布告をしているとみられる恐れがあることは自覚しなければならない。あくまで国民の安全という部分に限定して考えていかなれけれならない。	基本方針は本法に基づき定めるものであり、重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）において導入されるアクセス・無害化措置に係る制度そのものに対する御意見は本意見募集と直接関係するものではないと考えられますが、御意見として承ります。
基本方針全般		
103	サイバー攻撃は日々激化しており、能動的サイバー防御の必要性や、基本方針で記載されている内容の重要性について賛同する。 能動的サイバー防御は日本として新たな試みであり、官民双方にとって有益な取り組みとしていくべき。日々進化するサイバー攻撃に対して、新たに考慮すべきことも出てくる。継続的に官民で意見交換し、精査していくことが重要であり、また枠組みについても不断の見直しが必要。 いずれにしても、この仕組みを機能させていくためには、企業がメリットを感じ、積極的に取り組むことができる環境づくりが必要。我々としては我が国のサイバー対処能力強化に向け真摯に取り組んでいく考えだが、皆が同じ思いをもって取り組めるよう、理解の浸透を図っていただきつつ、意味のある取り組みとなるよう推進していただきたい。	官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要です。このため、制度設計・運用にあたっては、民間事業者と継続的に情報交換を行い、また、社会経済構造の変化等にも留意しつつ、不断に検証し必要な見直しを行います。 基本方針第１章第２節に記載のとおり、法に基づく各般の施策については、全てのステークホルダーが当該施策によるサイバーセキュリティ対策の一翼を担うとともに、そのメリットを実感できるサイバー攻撃対応のエコシステムを、官民を横断して構築することを目指さなければならないと考えております。このため、本法に基づく措置に関する周知・広報を含め、基本方針に則り、適切かつ適正な制度運用に努めてまいります。
104	日本国民の生活に直接のダメージを及ぼす可能性の高いもの、例えば電力・水道・ガス・通信・金融・交通などは、攻撃されてからの対応では、後手後手にまわってしまい、対処が間に合わないなどとなってしまうかもしれないので、平素より常に監視を続け、攻撃される前、もしくは攻撃され始めた瞬間に対応できるよう環境を整えておくことが、必要不可欠だと考えます。	頂いた御意見は今後の参考とさせていただきます。基本方針に記載のとおり、攻撃の高度化等、サイバー攻撃の態様は変化していくことが想定されること等から、政府としては、特別社会基盤事業者による特定侵害事象等の報告のほか、法第45条第１項に規定する協議会等も活用しながら、柔軟な情報収集を行ってまいります。
105	官民(特別社会基盤事業者、供給者などを含む)がそれぞれ役割を果たし、制度が効果的に機能するよう、特定不正行為による被害防止措置を講じる場合など、対応にあたっての事業者と供給者の責任分界やコスト負担などの考え方について基本方針に明記していただけないでしょうか。 例えば、特定侵害事象の報告、被害防止措置は特別社会基盤事業者の義務ですが、その際に双方の適切な責任、負担を考慮して「供給者に対して過度な要請を行わない」、「対応に関する適正な価格転嫁」などが必要と考えます。	特別社会基盤事業者と電子計算機等供給者の責任分界や費用負担等の関係性については、個々の状況も踏まえた民間事業者同士の契約関係等によるものであるため、政府として言及することは差し控えますが、一般論としては、独立行政法人情報処理推進機構及び経済産業省が公表する情報システム・モデル取引・契約書も参考にしつつ、取引等が行われれることが期待されます。
106	本方針（案）が示すとおり、「サイバー攻撃により国家・国民の安全が害され、又は国民生活・経済活動に多大な影響が及ぶことを防ぐ」ことは、我が国にとって喫緊の課題であり、サイバーセキュリティ対策の抜本的強化は不可欠です。当社としても、こうしたサイバーセキュリティの確保と国民生活・経済活動の安定のために政府が積極的に役割を果たすという方針に賛同いたします。 能動的サイバー防御に係る制度は、国家安全保障上の意義を有すると同時に、通信の秘密やプライバシーなど国民の基本的人権にも関わる極めて繊細な仕組みです。したがって、制度の具体的運用にあたっては、政府が一貫して主体的な責任を負い、その判断と説明の下で実施されることを明確にし、関係事業者に対して不当な批判や誤解が及ばないよう実務面での配慮を徹底していただきたいと考えます。 また、政府におかれては、制度の理念や目的、運用の仕組みや状況を国民に対して分かりやすく発信し、可能な限り透明性を高め、社会全体として制度の意義を理解し支える環境を醸成するための周知・啓発活動を継続的に実施していただくようお願い申し上げます。 さらに、今後策定される内閣府令についても、国民の権利保護や企業活動への影響に十分配慮し、パブリックコメントにとどまることなく、事業者を含む関係者との実質的かつ継続的な協議・調整を経て、事業者にとって過度な負担とならず、真に実効性のあるものとして制定・運用されることを要望いたします。	頂いた御意見は、今後の制度設計・運用における参考といたします。基本方針に記載のとおり、本法に基づく措置について必要な周知・広報を行うとともに、特定重要電子計算機の詳細等については、事業者の御意見も伺い、その負担にも留意しつつ、合理的な制度設計となるよう努めてまいります。
107	日々巧妙化、高度化するサイバー攻撃に対応するため、能動的サイバー防御の必要性や、今回取りまとめていただいた基本方針に記載されている内容の方向性・重要性について賛同いたします。その上で、官民双方にとって能動的サイバー防御を、有益かつ継続的な取組とするため、対応する企業に過度な負担とならないよう、配慮をお願いいたします。 また、重要インフラの停止等につながるおそれのある電子計算機の届出範囲や内容、政府と企業の間で締結する当事者協定、報告が必要なインシデントの範囲や報告期限、情報共有および対策に関する協議会等についての詳細は、今後、政省令の策定タイミングで具体化されるものと認識しております。 そのタイミングにて、官民で密に意見を交換し、企業からの意見も十分踏まえた上で、詳細な制度設計をお願いいたします。	同上
108	弊社は、基本的方針（案）の趣旨に深く賛同いたします。本基本方針（案）における官民連携をさらに円滑かつ効果的に推進するための弊社意見を、以下の通り提出させていただきます。今後のご検討において、ご参考としていただければ幸いです。 〇全般的な要望 本方針案に記載されている目的を達成するため、検討過程における官民の十分な双方向の意見交換の継続的な実施を日本政府に強く希望いたします。 特に、「サイバー対処能力強化法の施行等に関する有識者会議第３回（2025年10月30日）資料３『官民連携の強化に向け今後具体化が必要な論点』」に記載されている通り、クラウドサービスへの適用に関しては、今後の考え方の整理が必要な事項が多数残されていると理解しております。特別社会基盤事業者の制御系システムに関わるクラウド事業者に限らず、特別社会基盤事業者にサービス提供するIaaS、PaaS、SaaSの各事業者との意見交換は、官民双方にとって極めて有益であると考えます。	同上

その他		
109	サイバーセキュリティ分野は、一度のミスが国家的損失につながる極めて繊細な領域であると同時に、とびぬけて優秀な人材の創造性が国家の安全を支える分野でもある。本法の制度設計においては、こうした技術者の創造性と倫理を尊重し、信頼と誇りをもって協力できる環境の整備を強く求めたい。 プログラムは単なる命令の羅列ではなく、書き手の思想・美学・作風がにじみ出る創作物です。とくにハッカー文化においては、コードの構造や命名、処理の流れに"筆跡"が現れ、誰が書いたかを見抜けるほどの個性が宿ります。こうした技術者のコードや知見は、著作物に近い"精神的成果"であり、通信の秘密と同様に守られるべき知的な人格権であると考えます。 制度の信頼性は、制度そのものの中身だけでなく、それを運用する人材の質と育成環境にかかっています。ホワイトハッカーの教育においては、防御技術はもちろんですが、さまざまな攻撃者視点を含む実戦的な演習が不可欠です。優秀な人材ほど形式的・防御偏重の教育や現場では自身が育たないと考えるため、海外や民間に流出します。制度の中で活躍でき、際限なく技術向上できる育成環境、職場が必要である。 官民連携の枠組みも、単なる情報提供や報告義務にとどめず、技術者同士が学び合い、育ち合う"育成の場"として設計されるべきです。協議会や当事者協定においては、個別分析情報の提供だけでなく、実戦形式の攻防演習や独自のトラップなど、教育支援を通じて、協定当事者が"育つ"制度となるよう工夫していただきたい。とくに地方自治体や中小事業者も参加できるよう、柔軟で実効性ある支援体制が求められる。 地方自治体や中小事業者が単なる「支援対象」ではなく、国家のサイバーセキュリティにおける"起点"にもなり得る存在であることを強く認識すべきである。 近年のサイバー攻撃では、攻撃者が直接政府機関を狙うのではなく、セキュリティ対策が脆弱な地方自治体や中小事業者を踏み台として侵入し、そこから政府機関や重要インフラに波及する事例が増加している。 とくに、クラウドサービスや外部委託、メール連携などを通じて、地方の端末や中小事業者のネットワークが政府系システムと接続されている場合、攻撃者にとっては"入口"として極めて魅力的な標的となる。一見すると小規模な侵害が、結果として国家的な情報漏えいや機能停止につながる可能性がある。 このような構造的リスクを踏まえれば、地方自治体や中小事業者に対する支援は「善意の配慮」ではなく、「国家防衛の一環」として位置づけるべきである。 制度設計においては、こうした主体が"弱点"にならないよう、実効性ある教育・演習・支援体制を整備し、技術的にも人的にも"育てる"視点が不可欠である。 また、情報提供や協定締結においても、地方や中小事業者が「情報を受け取るだけ」の立場ではなく、現場からの知見や異変の報告が政府機関の防御力を高める"逆流型のセキュリティ"として機能するよう、双方向の仕組みを整備していただきたいです。 また、制度の運用にあたっては、通信の秘密や技術者の創造性を尊重し、大事な技術の拡散を防ぐことも柔軟にして欲しい事です。 また、協力するセキリュティ業者には(外資系なら特に)、丁寧な対話を通じて信頼を築きつつ、透明性と説明責任を確保していただきたい。 本法の目的は、日本国家と日本国民の安全を守ることにあります。制度と人材の両方に敬意と慎重さをもって向き合う必要があります。技術者の創造性を尊重し、守り育てる制度こそが、真に強いサイバーセキュリティの土台になると信じています。	基本方針第１章第２節に記載のとおり、法に基づく各般の施策については、全てのステークホルダーが当該施策によるサイバーセキュリティ対策の一翼を担うとともに、そのメリットを実感できるサイバー攻撃対応のエコシステムを、官民を横断して構築することを目指さなければならないと考えております。このため、本基本方針に則り、適切かつ適正な制度運用に努めてまいります。
110	全体　重要インフラ・基幹インフラに対する政府のサイバーセキュリティ施策の全体像 ・重要インフラ事業者、基幹インフラ事業者、またこれらの事業者に設備・サービスを提供するベンダーは、経済安全保障推進法（基幹インフラ役務の安定的な提供の確保に関する制度）、サイバーセキュリティ基本戦略、重要インフラのサイバーセキュリティに係る行動計画、重要インフラ統一基準、サイバー対処能力強化法、重要経済安保情報保護活用法全てに関わると理解しています。これら法律、戦略が個別にあるように見えており、全体像とそれぞれの戦略、法律の関係が分かりにくいので全体像を示して頂きたい。 ・例えば、イギリスではNPSAが、Critical National Infrastructure（CNI）として13分野で 、アメリカではCISA が16分野指定されているが国としての定義は一つであり、民間企業からみても分かりやすいと考えます。日本も定義を統一してはいかがでしょうか？	頂いた御意見は今後の参考といたします。
111	方針案における「特定重要電子計算機に対する不正行為の防止」および「官民連携体制の強化」の趣旨に賛同いたします。当社は、国内外の公共・民間分野においてストレージ基盤を提供しており、ランサムウェアやサプライチェーン攻撃などに対する耐性確保の観点から、特にデータ層の安全性と可用性を重視した設計を提案しています。本意見書では、今後の制度運用における技術的視点から三点申し上げます。 第一に、特別社会基盤事業者および関係行政機関における「データ保全・復旧の強靭化」です。サイバー攻撃は侵入防止だけでなく、データの改ざん・暗号化・消去を伴うケースが増加しています。これに備えるためには、攻撃後も改ざんされない状態でデータを保持し、迅速に復旧できる仕組みが不可欠です。具体的には、ストレージレイヤにおける不可改ざんスナップショット（Immutable Snapshot）や論理的隔離バックアップ（SafeMode等）の導入を制度的に推奨いただくことで、攻撃発生時の被害最小化と行政継続性の確保が期待できます。これらの仕組みは、既に複数の政府・自治体・重要インフラで運用実績があり、官民共通のベースラインとして適用可能です。 第二に、官民間の「情報共有・分析基盤」におけるストレージの信頼性向上です。フォレンジック分析や通信情報の提供・保管では、証跡の完全性と再現性が重要となります。データが後から改ざんされないこと、また分析時に正確な原本を再構築できることが求められます。当社では、エンドツーエンドの整合性チェック（End-to-End Checksum）および多層暗号化を備えたアーキテクチャにより、長期保存と再利用の双方を安全に実現する技術を提供しています。こうした「検証可能なデータ保全」の考え方を、今後の特別社会基盤事業者や自治体クラウドのセキュリティ評価基準に含めることを提案いたします。 第三に、サプライチェーンの透明性と信頼性確保です。特定重要電子計算機の防護においては、機器製造・ファームウェア更新・暗号鍵管理に至るまで、信頼できる供給経路が前提となります。当社では、製造から納入までの全工程において署名付きファームウェア、TPM/UEFI Secure Boot、KMIP対応暗号鍵管理を実装しており、ハードウェアレベルでの改ざん検知および安全な運用が可能です。こうしたセキュア・サプライチェーンの概念を、特別社会基盤事業者認定基準の一部として明示いただければ、官民双方の責任分界がより明確になると考えます。 総じて、サイバー攻撃対策はネットワーク境界の強化だけでなく、「最後に残るデータそのものを守る」視点が極めて重要です。Pure Storageは、国内の公共クラウド・プライベートクラウド・オンプレミスを問わず、可用性99.9999%以上の永続ストレージ基盤を提供しており、官民データの保全・復旧を支える技術的基盤として貢献できると確信しています。本方針の具体化に際し、データ保全層における安全・可用・持続的な仕組みの明確化をお願い申し上げます。	同上
112	国産のプラットフォームやアプリが無い状態で海外産のそれらを使っている状況でどのような方策を練ったとて絵に描いた餅でしかないでしょう 日本には世界に先んずる第一人者が居るのですからその叡知を活用しないでどんな方法を講じたとて防ぐことは不可能かと	本意見募集と直接関係するものではないと考えられ、参考の御意見として承ります。

113	一般の 公務員組織でなく、官房機密費なとで問題になっている 内閣官房の管轄にするのは、おかしいのではないか?国民に 活動を秘密にする気なのか? 「通信の秘密の保護」などを謳っているが、これでは 何も保障できないではないか。管轄を経済産業省などに 変えるべきである。 また、あまりに特権か強過ぎる組織であるにも関わらず、 政府側の乱用 (国民監視、選挙操作など) に対する歯止めが 全く法文化されていない。 これでは やりたい放題ではないか。初歩の思想からの 作り直しを求める。	本意見募集は、「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針 （案）」について、御意見を募集するものです。 なお、基本方針第３章第３節⑴に記載しているとおり、法に基づく通信情報の利用は、それによる通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度にとどまることが確保される制度となっています。
114	執行者の国籍要件を日本国籍に定めてください。警察官、自衛官だけで執行するとは限らないでしょう。国籍要件は必須です。帰化間もない者も参加できないようにしてください。帰化後10年以降など年数を設けるべきです。同時に、執行者を選ぶ者の国籍要件も必要です。外部専門者に委託するのはいいのです。その必要はあると考えます。ですがどこにいくらで委託しているか、国民がいつでも確認できるようにして欲しいです。 日本の通信はほとんど全てNTTの通信網を利用しています。重要電子計算機に対する不正な行為による被害の防止に関する法律はNTTの通信網が日本の管理下にあって初めて正しく機能します。今はNTT法により、NTT株の外資の割合が抑えられていますが、仮にNTT法がなくなり外資の割合が増えた場合、重要電子計算機に対する不正な行為による被害の防止に関する法律でいくらサイバー攻撃を防ごうとしても意味がなくなります。合わせてNTT法を残し、NTTの通信網を外国から守ってください。	法に基づき政府の事務の委託を受けることができる者（受託者）については、法第72条第１項及び第２項の規定により、独立行政法人情報処理推進機構その他当該事務について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができる法人を政令で定めることとされています。このため、基本方針に基づき、今後、政令で受託者を定めてまいります。なお、受託者の役員・職員又はこれらの職にあった者は、同条第４項の規定により、正当な理由がなく当該委託に係る事務に関して知り得た秘密の漏えい・盗用をしてはならないこととされており、これに違反した者には罰則が設けられています。 後段の御指摘については、本意見募集と直接関係するものではないと考えられ、参考の御意見として承ります。

※略称
経済安全保障推進法：経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）
重要経済安保情報保護活用法：重要経済安保情報の保護及び活用に関する法律（令和６年法律第27号）