「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に対する意見募集の結果一覧

意見募集期間：平成29年1月26日(木)から同年2月16日(木)まで　　20件

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
1	Ⅲ.5.5	24	－	重要インフラ事業者に対する実行方法についての記載について以下の通り意見を述べる。 ・現在各会社でセキュリティ教育が経営層の指揮によってなされているが、会社の垣根を越えて、 重要インフラに対するセキュリティの重要性を改めて共有する機会を設けたほうが良いのではないか。 理由としてはオリンピック・パラリンピックを3年後に控え、様々な企業がそれぞれのインフラでかかわることになる。 例を挙げると、道路交通、鉄道などについていえば、鉄道会社と高速道路、一般道路それぞれにかかわる会社に関する、ITのセキュリティが連携することで、一つのインフラが危機にあったときに、他のインフラでカバーできるのではないだろうか。	御意見のとおり、重要インフラ事業者等や関係者間において、サイバーセキュリティに係るリスクやサイバー攻撃等に係る情報を共有することは重要です。第３次行動計画に掲げた「リスクマネジメント」について、第４次行動計画(案)では「リスクマネジメント及び対処態勢の整備」としており、各重要インフラ事業者等がその機能保証のため、内部統制を強化し、主体的かつ自立的に対処態勢を整備することが求められていますが、同時に「リスクコミュニケーション及び協議」も推進することとしています。この取組は、重要インフラ事業者等がステークホルダーとの間においてリスクに関する役割や責任の分担等に係る合意形成を行い、重要インフラサービスの提供に関して期待される責任を果たす上で重要です。それぞれの重要インフラ事業者等が各セプターやセプターカウンシル、分野横断的演習等を利活用して、各関係主体と協力しつつ、情報・意見交換の充実を図ることとしています。	なし
2	不明	－	－	重要インフラの情報セキュリティ対策について、情報セキュリティインシデントはほぼ例外無く情報通信インフラを利用して脅威が拡大することから、情報通信分野の企業には独自の責任ある対応が求められると思うが、その視点が盛り込まれていない。重要インフラセキュリティ対策において脅威の大本を無害化するためには攻撃発信元特定のための法執行機関への協力や積極的なマルウェア感染拡大防止等が不可欠であるが、情報通信事業者は責務を果たすことができる立場にありながら、通信の秘密教条主義から、その役割を担っているとは言い難い。諸外国の事例等についてもまとめるとともに、通信の秘密教条主義から脱した現実的な情報通信事業者の責務について提言を望みます。	第４次行動計画（案）では、第３次行動計画と同様に、「情報セキュリティ対策は、重要インフラ事業者等が自らの責任において実施するものである」ことを基本的な考え方としており、「Ⅳ．関係主体において取り組むべき事項」においても、「重要インフラ事業者等」については「自主的な対策として期待する事項」を示しています。 なお、重要インフラ事業者（情報通信）は、これまでも関係機関と協力して、マルウェア感染に係る利用者への注意喚起等の取組を行ってきています。	なし
3	Ⅰ.1 Ⅲ.5.6	1 26	全国銀行協会	「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）（以下、行動計画（案）という。）から「OT（ITを利用した制御システム等の運用技術）」という用語が使用されている（1頁）。また、各関係主体における人材育成について「OTの管理部門（中略）においても情報セキュリティ対策が要求される」との記述がある（26頁）。この用語を使用した背景と定義（制御技術そのものを指すのか、制御技術および技術を使ったシステムの運用まで指すのか等）をご教示いただきたい。	重要インフラ事業者等を取り巻く環境は、情報通信技術(IT)の活用が進展し、制御システム等の運用技術(OT)とも融合して広く実装されつつある一方 、情報セキュリティ対策を講じるべき防護対象が拡大・複雑化し、影響の範囲や程度を想定することが困難化している状況にあります。こうした背景を踏まえ、本行動計画では、機能保証の考え方に基づき「重要インフラサービスの安全かつ持続的な提供」を実現することを重要インフラ防護の目的の中で明確化しました。当該目的を果たすためには、重要インフラ事業者等にあっては、様々な役割や能力を持つ人材が組織横断的に連携し、情報セキュリティ対策に当たることが必要となります。 P.1脚注に記載のとおり、本行動計画においては「ITを利用した制御システム等の運用技術」を「OT」と表記していますが、P.26の「OTの『管理部門等』」については、上記背景を踏まえ、運用技術自体の管理に限らず、運用技術を用いた制御システムの管理、運用、保守等を担う部門も含めて、機能保証の考え方に基づき連携が必要となるOTに関わる部門を表す概念として整理しています。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
4	Ⅲ.1.1	11	全国銀行協会	「内部統制」の一般的な定義に鑑みると、「内部統制を図るための取組」として、「ペネトレーション」が例示されている点には違和感がある。例えば、「ペネトレーションテスト」を独立して記述することを検討いただきたい。	内部統制の基本的要素として「ITへの対応」が含まれることから、ITへの適切な対応に欠かせない情報セキュリティ確保のための取組の一例としてペネトレーションテストを挙げていますが、御指摘を踏まえ、関係部分を以下のとおり修正します。 「対処態勢整備や内部統制の基本的要素としてのITへの適切な対応に欠かせない情報セキュリティ確保の意識~~を持った企業経営の強化に向けた内部統制を図る~~ための取組（※一例として、内部監査や、ペネトレーションテスト等が考えられる。）」	11
5	Ⅲ.2.2	14	全国銀行協会	当セプターの構成員は、内閣官房内閣サイバーセキュリティセンター（以下、「NISC」という。）から所管省庁および当セプター事務局を経由して提供されるサイバー攻撃等に関する情報のほか、JPCERTおよび金融ISAC（注）等からも同種の情報を得ている。 今後、本行動計画（案）にもとづき、更なる情報共有体制の強化が進められると、NISCから各セプター構成員に展開されるサイバー攻撃等に関する情報の数が多くなるものと考えられる。 一方、セプター構成員の立場に立つと、当セプターを含めた複数の先から展開されるサイバー攻撃等に関する情報に重複が生じた場合、不要な確認作業に労力を費やすおそれがある。 ついては、可能であれば、JPCERTおよび金融ISAC等の機関とも連携し、情報の重複等が極力発生しないような情報共有体制の構築について検討いただきたい。 （注）金融ISACはセプター構成員の一部が加盟。	御指摘のとおり、NISCが提供する情報と関係機関等から展開される情報に重複が生じる可能性がありますが、それだけ当該情報は分野横断的な影響等が懸念されるものであると考えられます。 情報共有体制の強化に向けては、関係主体間での連携を密に、各セプター事務局とも連携しつつ情報の峻別をはじめとした取組を進めてまいります。 また、御指摘のような効率的な情報共有体制の実現に向け、情報共有システムの整備にも取り組んでまいります。	なし
6	Ⅰ.4.3	6	内閣府SIP	本行動計画における重点的な取組方針 第４次行動計画案に示された通り、重要インフラ事業者等における先導的取組において、更に強化・推進していくことが重要である。特に、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する必要がある。このような重要インフラ事業者等における先導的取組の推進と他の分野への拡大を積極的に推進すべきである。	御意見のとおり、重要インフラの情報セキュリティ対策を強化・推進するためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第４次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
7	Ⅰ.4.4 表2	8	内閣府 SIP	表2 本行動計画における施策群と補強・改善の方向性等 5. 防護基盤の強化において、「〇セキュリティ・バイ・デザインの推進」に加え、セキュリティ・バイ・デザインを反映した「セキュリティ対策への長期的・継続的な投資」を加えるべきである。	御意見のとおり、重要インフラ事業者等がセキュリティ・バイ・デザインの考え方にのっとり、制御系機器・システム等の調達及び運用を行うためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第4次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
8	Ⅲ.2.2	14	内閣府 SIP	情報共有の更なる推進 第4次行動計画案に示された通り、情報共有体制の強化が重要である。 「共有すべき情報」の考え方について、ここに例示されている「システムの不具合等に関する情報」とは、現に運用中のシステムについての情報を念頭においていると見受けられるが、これに限らず、今後調達予定の機器についての情報も共有することが、重要インフラ防護に有効である。 一般に重要インフラ事業者が運用するシステムは規模が大きいため、調達すべき機器も数多い。調達する機器の選定にあたっては、セキュリティ強度が高いものを求めるとともに、セキュリティ強度が低いものは避けなければならない。この際、エビデンスに基づく非推奨製品や事故事例を共有してナレッジベースを構築することが、調達時のセキュリティ対策として有効である。 このようなナレッジベースの構築は、内閣官房、重要インフラ所管省庁、重要インフラ事業者が相互に協力・分担しながら推進すべきである。	御指摘のとおり、調達機器の脆弱性等に係る各種情報も極めて有用であり、既に関連する情報は情報セキュリティ関係機関等でも提供されているところです。今後の情報共有システムの整備にあたっては、御指摘のような情報の共有に向けた検討も進めてまいります。	なし
9	Ⅲ.4	18	内閣府 SIP	リスクマネジメント及び対処態勢の整備 第4次行動計画案に示された通り、「リスクアセスメントの結果を踏まえた適切な対処態勢が整備されること」が必要である。この「適切な対処態勢」に加えて、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、経営層が率先して中長期的な「セキュリティ対策投資計画への反映」が重要である。	御意見のとおり、重要インフラ事業者等において「適切な対処態勢」を整備するには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第4次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
10	Ⅲ.5.1	23	内閣府 SIP	重要インフラに係る防護範囲の見直し 第4次行動計画案に示された通り、「サプライチェーンを含めた「面としても防護」を確保する」ことが重要である。 上述のような、製品そのもののセキュリティ強度の評価を共有することに加え、その製品のサプライチェーンが信頼できることを確認するための技術や制度について検討を深めることが必要である。	御指摘の事項については、「面としての防護」に向けて取り組むにあたり、重要な要素のひとつであると考えます。現行の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）」においては、本編「Ⅲ6.1.5(2)」に関連して「同対策編」の「Ⅱ1.5(2)」に、サプライチェーンリスクへの対応に関する記述をしていますが、当該指針を2017年度に改定する必要があり、サプライチェーンが信頼できることを確認するための技術の動向等について考慮すること等を記載したいと考えています。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
11	Ⅲ.5.4	25	内閣府 SIP	セキュリティ・バイ・デザインの推進 第４次行動計画案に示された通り、「システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの考え方を関係主体が共通の価値として認識することを促していく」ことが重要である。特に、設備規模が大きいことに加え、その設備寿命が永い重要インフラにおいては、設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する必要がある。	御意見のとおり、重要インフラ事業者等がセキュリティ・バイ・デザインの考え方にのっとり、制御系機器・システム等の調達及び運用を行うためには、必要な経営資源の確保等について中長期的な視点で検討されることも必要であると認識しています。このため、御意見を踏まえ、第４次行動計画案のⅢ章「5.5.経営層への働きかけ」④に、以下を追記します。 「なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。」	25
12	Ⅲ.5.8	26	内閣府 SIP	規格・標準及び参照すべき規程類の整備 第４次行動計画案に示された通り、規程類を整理することが重要である。 対策の実効性を持たせるためには、セキュリティ要件を定めた規程類を整理するだけでなく、重要インフラ事業者が日常的に参照している（重要インフラの安定運用に向けた）ガイドライン等に直接要件を追記していくことが重要である。	各重要インフラ分野における、ガイドラインを含む安全基準等の策定・改定に当たっては、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第4版)」が活用されています。重要インフラ事業者等が日常的に参照している重要インフラサービス提供に係る既存のガイドライン等に、当該指針を踏まえた情報セキュリティに関する事項を追記することで、実効性の向上が期待できる場合は、そのようにしていただくべきと考えます。	なし
13	Ⅳ.5. (5)	33	内閣府 SIP	Ⅳ. 関係主体において取り組むべき事項（P33） 5. 重要インフラ事業者等の自主的な対策として期待する事項 (5)「防護基盤の強化」に関する対策 「〇4 制御系機器・システムの第三者認証制度の認証を受けた製品の活用を検討。」に加え、「設備更改時における重要インフラ設備のセキュリティ対策強化と、既存設備のための付加的なセキュリティ対策強化を、計画的に推進する。」を追記すべきである。	御意見のとおり、重要インフラ事業者等において設備のライフサイクルも勘案した計画的なセキュリティ対策を講じることが必要であると認識しています。こうした取組については、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に実施することが重要であると考えています。このため、第４次行動計画案のⅣ(ローマ数字の４)章の「5.(5)「 防護基盤の強化」に関する対策」の⑤として、以下の項目を追加します。 「情報セキュリティ対策に関する各取組に必要な予算・体制・人材等の経営資源を計画的に確保、配分。」	33
14	別紙3	56	S&J株式会社	別紙３ 情報連絡における事象と原因の類型 「発生した事象」のうち「上記につながる事象」は、「未発生の事象」の「予兆・ヒヤリハット」に含まれるべきと考えられます。理由は、「2.2 情報連絡の仕組み」に記載されている「予兆・ヒヤリハットやシステムの不具合に係る法令等で報告が義務付けられていない事象を報告する場合」において、「上記につながる事象」が含まれるかどうかがあいまいな解釈ができてしまうためです。また、より「予兆・ヒヤリハット」の目的を明確にするためには、「マルウェアが添付された不審メールの受信」は省くべきと思われます。 私の「未来投資会議構造改革徹底推進会合「第４次産業革命（Society5.0）・イノベーション」会合 （第４次産業革命）（第２回） 配布資料」の資料１０におけるP.7にヒヤリハットの事例が記述されています。	別紙３では、「上記につながる事象」の例として実際にマルウェアの感染等が確認されたことをもって「発生した事象」と整理するとともに、情報連絡の対象であることを明確化しています。また、「マルウェアが添付された不審メールの受信」それ自体は「未発生の事象」であり、原案のとおりとします。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
15	別添	44	S&J株式会社	「別添：情報連絡・情報提供について」の「1. システムの不具合等に関する情報」 「予兆・ヒヤリハットに関する情報」の報告について記述されているが、そもそも、このような事象を検知できるシステムと体制が無ければならないことを明記すべきです。言い換えれば、検知しなければ報告しなくてもいい、ということにならないようにしなければならない、ということです。	重要インフラ事業者等に対しては自らの責任において、予兆・ヒヤリハットに限らず情報セキュリティ全般についてその実施や対策を実装するための環境整備を求めており（p32）、御指摘の箇所はその取組から得られた情報の共有を促すことを意図していますので、原案のとおりとします。	なし
16	Ⅰ.3	3	特定非営利活動法人日本ネットワークセキュリティ協会	施策の「安全基準等の整備及び浸透」にある現状の課題として、 「自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である」 とあるが、施策としては、指針や基準の浸透しかなく、実務的に有効なCheck（確認）がなされているかの策がない。 確実に推進するための、具体的な取り組みを明示いただきたい。	情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものであり、 政府機関は、重要インフラ事業者等による情報セキュリティ対策のPDCAサイクルの定着化等に必要な支援を行います。 具体的な支援策としては、従前から、安全基準等の浸透状況等調査により、重要インフラ事業者等の情報セキュリティ対策の取組状況等を把握し、施策の改善に活用するなどしておりますが、これに加え、指針に記載されたPDCAプロセスのさらなる明確化や、Check（確認）に係る観点の整理（「4.2.5 モニタリング及びレビューの推進」）等を実施します。	なし
17	別紙1	50	電気事業連合会	P50の別紙1　対象となる重要インフラ事業者等と重要システム例に関して、電力分野については、対象となる重要インフラ事業者等の記載を見直してはどうか。 今後、電力システム改革の過程で会社が分割される際に、様々な会社形態が考えられ、場合によっては発電事業等を行わない持株会社がセキュリティ統括の役割を担う可能性もあるため、現行案の範疇を尊重しつつ、このようなケースを考慮して「一般送配電事業者、主要な発電事業者　等」とするべきではないか。	御指摘のとおり、修正いたします。	50
18	Ⅰ.4.4 表2	7	石油化学工業協会	「第4次行動計画(案)」の7ページ 表2「本行動計画における施策群と補強・改善の方向性」に、第3次行動計画からの主な補強・改善の方向性として「情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点からサービス維持レベルを関係法令等において具体化するなど、制度的枠組みを適切に改善する取組を継続的に実施」との記述がある。 重要インフラ事業者は「サイバーセキュリティ基本法」に則って自主的に取組んできているところである。法制化の検討に際しては、初めから法制化ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提である。対象となる事業者へのサイバー攻撃による障害の影響の大きさと、これに対応するための事業者の負担に十分に配慮されたい。 また同表2の「情報共有体制の強化」に関して、情報は単に収集するだけでなく、有効に活用することこそが肝要と考える。サイバーインシデントの増加に伴って情報共有すべき関係先も増えており、窓口の一本化など効率化も望まれる。情報共有体制が有効かつ効率的に機能するような仕組み作りをお願いしたい。	御指摘の「制度的枠組みを適切に改善する取組」は、法制化のみを念頭に置いたものではありません。重要インフラを取りまく環境は分野により様々であると考えられ、技術の進展等により重要インフラサービスの形態そのものが変化するケースのほか、サービス形態は変わらなくても、コスト削減や利便性の向上等を目的としてサービスの提供に必要なシステムが大きく変わるケースもあると考えられます。御指摘のとおり重要インフラ分野毎の事業特性等を踏まえつつ、法制化も含めた制度見直しの検討を行い、その結果、必要と判断された場合に法制化を実施すべきと考えられます。 また、御指摘のような有効かつ効率的な情報共有体制の実現に向け、関係主体間で連携した情報共有システムの整備に取り組んでまいります。	なし

No.	箇所	頁	団体名	御意見	御意見に対する考え方	修正
19	別紙2	54	石油化学工業協会	「第4次行動計画(案)」の別紙2「重要インフラサービスの説明と重要インフラサービス障害の例」で、化学分野に係る法令、ガイドラインとして「石油化学分野における情報セキュリティ確保に係る安全基準」が制定されているので、これに改めていただきたい。	御指摘のとおり、修正いたします。	54
20	Ⅰ.4.4 表2 Ⅲ 2.1	7 13	日本化学工業協会	化学セプター（主要石油化学事業者）が供給するサービスは、ポリエチレン、ポリプロピレン、塩化ビニル等国民生活に幅広く使用されている財を構成する主要部材の一つである。従来から、かかるサービスの供給途絶に備えた対応としては、供給するサービスが部材の供給であり、地域を越えた代替供給が可能であることを踏まえ、緊急時の事業者間の融通や緊急時を想定した余裕を持った製品在庫等により必要な備えを進めてきているところである。 一方、本行動計画案において重要インフラサービスとして位置づけられているセプターの供給するサービスは、化学を除けば、地域を越えた代替供給が困難なものであり、また、関連する業法により事業者に対して供給責任を負わせているものである。 一方、化学セプターの存立する産業基盤においては、化学的、物理的にリスクを内在する物質を、多くの場合高温、高圧で処理するものであり、同様のプロセスを扱う他製造業と同様に、サイバー攻撃による施設の安全の確保に重点を置いた対策が必要であり、かかる観点から従来からNISCと定期的に情報交換を行い、その対策の継続的な改善を進めているところである。これらの状況を政府においてはご理解頂き、各事業者において適切な対応がとられることが促進されるような方策をとっていただきたいと考えている。 なお、「4.4本行動計画における施策群と補強・改善の方向性等」の表２中の「１．安全基準等の整備及び浸透」において、情報セキュリティ対策を関係法令等における保安規制として位置付ける、とあるが、サービス供給継続の観点から保安規制としてセキュリティ対策を位置付けるのは必ずしも適切ではないと考えられる。保安規制としてセキュリティ対策を位置付けるのであれば、物理的な安全、保安の確保の観点から別途の視点で審議を尽くすべきと考えるところ、「保安規制として位置付けること」の部分を削除していただきたい。 また、サイバー攻撃情報の報告を法的に義務付けたとしても、そのことにより、事業者における対応の促進が図られるとは考えられず、それよりもむしろ、従来から行われているIPAやNISC、事業者相互間の情報共有・交換を一層充実させることにより、事業者の自主的な対応を促すことが、セキュリティ対策の向上に資するのではないかと考えられる。したがって、はじめから規則や法規制ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提であると考える。 また、「Ⅲ. 計画期間内に取り組む情報セキュリティ対策」の「2.1 本行動計画期間における情報共有体制」に、24時間365日体制による迅速かつ効率的なサーバー攻撃に関する情報共有の実現に向け、内閣官房と重要インフラ事業者等の間のホットライン構築とあるが、報告時刻については、実効性ある現実的な方策にすべきと考えられる。	「安全」が確保されるということも、事案の性質に応じて、機能保証の重要な要素であると考えています。御指摘を踏まえ、関係部分を以下のとおり修正します。 「安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、」 なお、御指摘の「情報セキュリティ対策を関係法令等における保安規制として位置付ける」ことについては、「制度的枠組みを適切に改善する取組」の一例として挙げているものであり、法制化のみを念頭に置いたものではありません。重要インフラを取りまく環境は分野により様々であると考えられ、技術の進展等により重要インフラサービスの形態そのものが変化するケースのほか、サービス形態は変わらなくても、コスト削減や利便性の向上等を目的としてサービスの提供に必要なシステムが大きく変わるケースもあると考えられます。御指摘のとおり重要インフラ分野毎の事業特性等を踏まえつつ、法制化も含めた制度見直しの検討を行い、その結果、必要と判断された場合に法制化を実施すべきと考えられます。 また、御指摘のとおり、ホットライン構築に向けては報告タイミングも含め実効性ある現実的なものとなるよう情報共有システムの整備・運用に取り組んでまいります。	7,12,28,30