資料３

サイバーセキュリティ政策の評価等について

資料３－１　サイバーセキュリティ政策の評価等について

※資料３－２　平成 26 年度　サイバーセキュリティ政策の評価等の実施方針

※は、サイバーセキュリティ戦略本部決定案。

サイバーセキュリティ政策の評価等について

資料３－１

サイバーセキュリティ政策に係る年次報告

○ サイバーセキュリティ戦略本部は、「サイバーセキュリティ戦略」（平成25年6月10日情報セキュリティ政策会議決定）に対応する**「サイバーセキュリティ政策の評価等の基本方針」**（平成26年1月23日情報セキュリティ政策会議決定）に基づき、**「平成26年度サイバーセキュリティ政策の評価等の実施方針」**及び**「サイバーセキュリティ政策に係る年次報告」**を策定・公表する。

○ 当該年次報告の結果を踏まえ、新たなサイバーセキュリティ戦略の下、平成27年度のサイバーセキュリティ政策に係る年次計画やその評価方針を定める。

【 サイバーセキュリティ戦略本部】

サイバーセキュリティ戦略
H25/06/10　情報セキュリティ政策会議決定

毎年策定

計画（ Plan ）

サイバーセキュリティ 2014
H26/07/10　情報セキュリティ政策会議決定

対応

実施（ Do ）

サイバーセキュリティ政策の評価等の基本方針
H26/01/23　情報セキュリティ政策会議決定

毎年策定

平成26年度　サイバーセキュリティ政策の評価等の実施方針
今回　サイバーセキュリティ戦略本部決定(予定)

評価（ Check ）

サイバーセキュリティ政策に係る年次報告
H27/06　サイバーセキュリティ戦略本部決定（予定）

改善（ Act ）

新たなサイバーセキュリティ戦略

- サイバーセキュリティ 2015（仮称）
- サイバーセキュリティ政策の評価等の基本方針（仮称）
- 平成27年度　サイバーセキュリティ政策の評価等の実施方針（仮称）

資料３－２

平成 26 年度　サイバーセキュリティ政策の評価等の実施方針

（平成２７年２月１０日
サイバーセキュリティ戦略本部決定案）

サイバーセキュリティ戦略本部（以下「本部」という。）は、「サイバーセキュリティ政策の評価等の基本方針」（平成 26 年１月 23 日情報セキュリティ政策会議決定）に基づき、「サイバーセキュリティ戦略」（平成 25 年６月 10 日情報セキュリティ政策会議決定。以下「戦略」という。）及び「サイバーセキュリティ 2014」（平成 26 年 7 月 10 日情報セキュリティ政策会議決定。以下「年次計画」という。）に基づく内閣官房及び各府省庁の取組につき、以下のとおり、評価指標に基づくデータの把握及び評価、補完調査、分析等（以下「評価等」という。）を実施するものとする。

１　評価等の対象

本部は、戦略及び年度計画に基づき設定した「サイバーセキュリティ政策領域」（表１）を対象として、評価等を実施するものとする。

表１　　サイバーセキュリティ政策領域

１　「強靭な」サイバー空間の構築
- ① 政府機関等における対策
- ② 重要インフラ事業者等における対策
- ③ 企業・研究機関等における対策
- ④ サイバー空間の衛生
- ⑤ サイバー空間の犯罪対策
- ⑥ サイバー空間の防衛

２　「活力ある」サイバー空間の構築
- ① 産業活性化
- ② 研究開発
- ③ 人材育成
- ④ リテラシー向上

３　「世界を率先する」サイバー空間の構築
- ① 外交
- ② 国際展開
- ③ 国際連携

４ 推進体制等

2　評価等の視点

本部は、脅威やリスクが常に変化し続けるサイバーセキュリティ分野の特性を考慮しつつ、施策の実施主体や対象の特性を勘案のうえ、「結果（アウトプット）を測る視点」と「成果（アウトカム）を測る視点」から、総合的に評価等を実施するものとする。

「結果を測る視点」による評価は、年度計画の個々の施策がどのような結果をもたらしたのか、各年度における進捗状況を確認するものである。また、「成果を測る視点」による評価は、施策により実現した社会が戦略の目標、すなわち理想とする社会にどれだけ近づけたのか、戦略に照らして期間中の成果を確認するものである。

政府機関等における対策のうち、政府機関統一基準群[1]に関連する対策の具体的な実施状況については、同基準群に基づいた点検を踏まえた評価を行い、年次報告の一部として取りまとめるものとする。

重要インフラ事業者等における対策のうち、内閣官房及び重要インフラ所管省庁におけるサイバーセキュリティ対策の具体的な実施状況については、「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年５月 19 日情報セキュリティ政策会議決定）に基づく施策の成果検証等から評価を行い、年次報告の一部として取りまとめるものとする。

なお、政府機関等における対策、重要インフラ事業者等における対策については、必要に応じて各主体による調査等を実施し、これをもって評価等の仕組みとして活用するものとする。

3　評価等の方法

本部は、内閣官房及び関係府省庁の協力のもと、各施策の進捗状況や成果を確認するとともに、別添「サイバーセキュリティ政策領域における評価に当たり考慮すべき状況」を踏まえて評価等を実施するものとする。

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。）は、それに必要となる次の資料と年次報告の原案を取りまとめるものとする。

(1) 評価指標に基づくデータの把握及び評価

NISC は、内閣官房のその他の部局及び各府省庁の協力を得て、評価指標に基づくデータを把握し、その評価資料を取りまとめる。

(2) 補完調査

NISC は、(1)を実施することが困難な事項に関する状況を把握するため、内閣

[1]「政府機関の情報セキュリティ対策のための統一規範」、「政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針」、「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（いずれも平成 26 年5月 19 日情報セキュリティ政策会議決定）等を指す。

官房のその他の部局及び各府省庁の協力を得て補完調査を実施し、その資料を取りまとめる。

補完調査の実施に当たっては、各々の取組の性質及びこれを取り巻く環境が異なることなどを十分に考慮し、柔軟に対応するものとする。

(3) 分析

NISC は、必要に応じて、評価指標に基づくデータ、評価の結果及び補完調査の結果に基づき必要な分析を行い、その資料を取りまとめる。

別添　サイバーセキュリティ政策領域における評価に当たり考慮すべき状況

サイバーセキュリティ政策分野・施策内容			評価に当たり考慮すべき状況
1「強靱な」サイバー空間の構築			
①政府機関等における対策			
1）情報及び情報システムに係る情報セキュリティ水準の一層の向上			
【情報の重要度等に応じた政府機関における統一的な仕組みの強化】			
	（ア）	業務・情報の特性に応じた対策の重点実施のための枠組みの構築・運用	・重要な業務・情報を守るために必要な情報セキュリティ対策を計画的・重点的に実施するための枠組みの構築・運用状況 ・各府省庁の対策推進計画の策定状況
	（イ）	政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し	・各府省庁の情報セキュリティポリシーの見直し状況
【多様化する就労形態等への対応の強化】			
	（ク）	政府機関におけるスマートフォン等の情報セキュリティ対策の強化	・各府省庁における私物のスマートフォン等を外出先やテレワーク等で業務利用する際の情報セキュリティ対策の実施手順の作成に係る支援の状況
【政府横断的な情報システムの対策強化等】			
	（コ）	複数の府省庁で共通的に使用する政府情報システム基盤の運用管理に関する体制等の整備	・政府情報システムの統合・集約化の進捗状況
	（サ）	社会保障・税番号制度に対応した情報セキュリティ対策	・社会保障・税番号制度に係る情報セキュリティ対策の検討状況
【情報システムにおけるサプライチェーン・リスク等への対応強化】			
	（セ）	調達時における対策の推進	・サプライチェーン・リスクへの対応に関する情報収集・共有等の取組状況
	（ツ）	運用・管理を委託している情報システムの情報セキュリティ対策の強化	・クラウドコンピューティングを含む運用・管理を外部に委託している政府機関の情報システムについて、情報セキュリティを確保するための取組の推進状況
【独立行政法人、地方公共団体等における対策の強化】			
	（ノ）	独立行政法人等における情報セキュリティ対策の推進	・独立行政法人等における情報セキュリティ対策の実施状況
2）サイバー攻撃への対処態勢の充実・強化			
【GSOCの抜本的強化】			
	（ア）	政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の運用による緊急対応能力の向上	・サイバー攻撃等に関する情報収集・分析結果等の情報共有の実施状況
	（イ）	サイバー攻撃事態への対処に資する情報の集約・共有の充実	・サイバー攻撃事態への対処に資する情報の集約・共有等の実施状況
【CYMATとCSIRT等との連携強化や訓練等による対処態勢の構築・強化】			
	（ウ）	情報セキュリティ緊急支援チーム（CYMAT）要員等への訓練による対処能力の向上	・サイバー攻撃に対する各種訓練及び研修の実施状況
	（エ）	CSIRT等の体制の整備及び連携の強化	・政府機関におけるCSIRT体制の機能の維持・向上の状況
	（キ）	大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等	・大規模サイバー攻撃事態等発生時の初動対処に係る訓練等の実施状況
【人材の確保・育成】			
	（シ）	採用時における情報セキュリティ関連素養の確認	・公務員採用時における情報セキュリティ関連素養の確認に関する要請の状況及び当該要請を踏まえた対応状況
	（セ）	人事ローテーションの工夫	・人事ローテーションの工夫の検討の状況
	（ソ）	優秀な外部人材の活用	・外部人材の活用状況
3）その他			
	（ア）	情報セキュリティガバナンスの機能強化に向けた取組	・情報セキュリティ対策推進会議（CISO等連絡会議）の審議状況
②重要インフラ事業者等における対策 【安全基準等の整備及び浸透】、【情報共有体制の強化】、【障害対応体制の強化】、【リスクマネジメント】及び【防護基盤の強化】については、「重要インフラの情報セキュリティ対策に係る第3次行動計画（平成26年5月19日情報セキュリティ政策会議決定）」に記載の方法により評価を実施する。			
【その他の施策】			
	（ノ）	制御機器等の評価・認証スキームの確立支援	・制御システムセキュリティの国際標準、評価・認証スキーム策定への参画状況
	（ハ）	制御システムセキュリティの国際標準に基づく評価・認証機関設立	・制御システムセキュリティの評価・認証機関の設立

③企業・研究機関等における対策

【中小企業等における対応強化】

(イ)	中小企業における情報セキュリティ対策の底上げ	・中小企業における情報セキュリティ投資を促進するための関連税制の利用促進等の施策推進状況
(エ)	個人情報漏えい等防止のための対策	・個人情報の保護に関する法律のガイドラインの改正及び個人情報漏えい対策の普及啓発状況
(オ)	技術・営業秘密保護に関する官民の情報共有	・技術・営業秘密保護のための取組の実施状況

【事業等のリスクの開示】

(カ)	上場企業における事業等のリスクとしての開示の検討	・上場企業における情報セキュリティに関する事項について事業等のリスクとしての開示に向けた検討状況
(キ)	セキュリティエコノミクスに関する対応	・企業などの組織にとって最適な情報セキュリティ対策への投資や対策のレベルを評価する仕組みに関する検討状況

【情報セキュリティガバナンスの確立】

(ク)	情報セキュリティガバナンス確立の促進	・「セキュリティガバナンス協議会」の活動状況
(ケ)	企業における情報セキュリティ対策の支援	・情報セキュリティ報告書モデルの普及状況
(サ)	企業における電子署名利活用の普及促進	・電子署名利活用の普及促進
(ス)	CISO等の設置促進	・企業におけるCISO等の普及促進状況
(セ)	組織の緊急対応チームの普及、連携体制の強化	・CSIRTの普及や国内外の組織内CSIRT との間における緊急時及び平常時の連携の強化、標的型攻撃への対処を念頭においた運用の普及、連携に関する状況
(タ)	内部の不正行為によるセキュリティインシデント防止の検討	・内部者の不正行為によるセキュリティインシデント防止方策に関するガイドラインの普及浸透状況
(チ)	経営層向けセミナーの開催等	・経営層向けセミナーの開催状況

【教育機関における取組の強化】

(ト)	地方公共団体の教育関係部門における情報セキュリティに関する取組の推進	・各地域で情報教育を推進する中核的な役割を担う指導主事等を対象とした研修の実施状況

【その他】

(ニ)	個人情報保護法の見直し	・個人情報保護法の見直しに関する検討状況

④サイバー空間の衛生

【普及啓発】

(ア)	新たな情報セキュリティ普及啓発プログラムの策定	・「新・情報セキュリティ普及啓発プログラム」の策定とそれを踏まえた関係施策等の進捗状況 ・「情報セキュリティ社会推進協議会」の設置及びその活動状況
(ウ)	「サイバーセキュリティの日」の取組の推進	・「情報セキュリティ月間」及び「サイバーセキュリティの日」における普及啓発活動の実施状況
(キ)	国際連携を活用した国内外における普及・啓発活動の実施	・情報セキュリティ国際キャンペーンの実施状況
(ケ)	各種メディア等を通じた普及・啓発の推進	・情報セキュリティに関するポータルサイト等のコンテンツ及びアクセスの状況 ・インターネット安全教室開催数（経済産業省）、e-ネットキャラバン開催状況（総務省、文部科学省） ・普及啓発ロゴマークの利用状況
(コ)	情報セキュリティに関する事故事例等に関する普及啓発の推進	・事故事例等の収集実績
(サ)	無線LANの情報セキュリティ確保の推進	・無線LANのセキュリティ対策、情報漏えい対策等の推進

【インシデントの認知・解析機能の向上】

(タ)	サイバー攻撃の予兆の早期把握と情報収集・分析の強化	・サイバー攻撃高度解析機能の整備、対応調整支援、予兆の早期把握と情報収集・分析の強化状況
(チ)	サイバー攻撃事案の実態解明に係る情報収集・分析等	・サイバー攻撃事案の実態解明に係る情報収集・分析状況
(ツ)	新しい脅威・攻撃の分析・共有	・新しい脅威・攻撃の分析・共有状況
(テ)	コンピュータセキュリティ早期警戒体制の強化	・インシデント報告関連件数（JPCERT/CC インシデント報告対応レポート） ・コンピュータウィルス届出状況（IPA） ・コンピュータ不正アクセス届出状況（IPA） ・脆弱性関連情報の届出状況（IPA）
(ナ)	サイバー攻撃事前防止・早期対策に向けた取組の推	・サイバー攻撃予知・即応技術の研究開発の状況

【ソフトウェアの脆弱性への対応】

(ノ)	脆弱性関連情報届出受付制度の運営及び脆弱性関連情報の提供	・ソフトウェア脆弱性に関する情報収集・提供の実績（JPCERT/CC、脆弱性関連情報届出受付制度、脆弱性対策情報データベース）等
(ヘ)	組込み機器の脆弱性対策の推進	・組込機器の脆弱性対策の検討状況

	【その他】		
	(マ)	スパムメール対策の強化	・スパムメール対策の状況
	(ミ)	暗号・認証技術等を用いた通信プロトコルの利用による安全な通信環境の実現	・暗号・認証技術等を利用した通信プロトコルの安全性評価、情報提供の状況
	(ム)	IPv6ネットワークのための情報セキュリティ検証環境の構築	・IPv6普及・高度化推進協議会等における検討・推進状況
⑤サイバー空間の犯罪対策			
	【サイバー攻撃対策等の強化】		
	(ア)	サイバー攻撃対策に係る態勢等の強化	・サイバー犯罪の検挙状況(サイバー空間をめぐる脅威の情勢について:警察庁)
	(イ)	日本版NCFTAの創設に向けた検討	・日本版NCFTAの創設、サイバー空間の脅威への対処に関する産学官連携の推進状況
	(オ)	サイバー犯罪の被害防止対策の推進	・情報セキュリティに係る政府系ウェブサイト(サイバー犯罪対策、@Police)における広報啓発の実施状況
	(カ)	不正アクセス禁止法の適正な運用を始めとした不正アクセス防止対策の推進	・不正アクセス行為の発生状況(不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況:国家公安委員会、総務省、経済産業省)
	(キ)	フィッシング対策協議会	・フィッシング対策協議会の活動状況
	【事後追跡可能性の確保】		
	(コ)	ログの保存の在り方の検討	・関係事業者における通信履歴等に関するログ保存の在り方、捜査への利用の在り方についての検討状況
	(サ)	デジタルフォレンジックに係る取組の推進	・デジタルフォレンジックに係る体制等の強化、不正プログラム解析のための体制等の強化及び調査研究の状況
	【人材育成等による体制強化】		
	(ス)	サイバー防犯ボランティア育成の推進	・サイバー防犯ボランティアの育成状況
	【その他】		
	(セ)	スマートフォンの安全利用のための環境整備	・青少年に対する有害環境対策の検討・実施状況、取締りの強化と情報発信の推進状況
⑥サイバー空間の防衛			
	【自衛隊等の態勢の強化】		
	(ア)	サイバー情報収集装置の整備	・サイバー情報収集装置の整備状況
	(イ)	次期サイバー防護分析装置のシステム設計等	・次期サイバー防護分析装置のシステム設計等の進捗状況
	(エ)	防衛情報通信基盤(DII)の整備	・防衛省情報通信基盤(DII)の整備状況
	【国家レベルのサイバー攻撃への対応の強化】		
	(ス)	国家レベルのサイバー攻撃への対応の強化	・外国政府等の関与が疑われる国家レベルのサイバー攻撃への対応強化の進捗状況
2「活力ある」サイバー空間の構築			
①産業活性化			
	(ア)	M2Mにおける情報セキュリティの確保に関する検証等の推進	・M2Mにおける情報セキュリティの研究開発の進捗状況
	(イ)	スマートコミュニティ普及等に資する高セキュアな半導体デバイスの研究開発等の推進	・スマートコミュニティ・スマートグリッドにおける情報セキュリティの研究開発の進捗状況
	(ウ)	新たな情報流通形態に対応した情報秘匿・認証・改ざん防止技術の研究開発	・クラウド等の新たな情報流通形態に対応するため、必要な情報秘匿及び認証を両立するための研究開発の進捗状況
	(エ)	省リソースデバイスにおける情報セキュリティ技術の研究開発	・省リソースデバイスにおける情報セキュリティ技術の研究開発の進捗状況
	(ケ)	国際的なルールに基づくセキュリティ製品の貿易の推進	・複合機や制御システム等の貿易で日本製品が不当な扱いを受けることが無いよう、国際標準化や評価・認証の国際相互承認等に参加
	(コ)	自動車に係る情報セキュリティの確保	・自動車の制御システムに関するセキュリティ上の諸問題についての調査・対策等の検討状況
②研究開発			
	(ア)	「情報セキュリティ研究開発戦略 」の研究開発の推進	・「情報セキュリティ研究開発戦略」の見直し状況
	(ウ)	標的型攻撃の対策技術に関する研究開発	・サイバー攻撃の解析・検知技術、標的型攻撃の対策技術の研究開発進捗状況
	(オ)	新世代ネットワーク基盤技術に関する研究開発	・次世代ネットワーク技術の研究開発進捗状況
	(ケ)	サイバーセキュリティ研究基盤の構築	・サイバーセキュリティ研究基盤「NONSTOP」の運用状況 ・「サイバー攻撃対策総合研究センター(CYREC)」の整備や研究開発の進捗状況
	(ツ)	サイバー攻撃の解析・検知に関する研究開発	・標的型攻撃等の新たなサイバー攻撃への対策技術に関する研究開発の進捗状況
	(ト)	制御システムセキュリティに関する研究開発	・制御システムのセキュリティ検証方法及び評価・認証方法に関する研究開発の進捗状況

③人材育成

(ア)	「新・情報セキュリティ人材育成プログラム」の推進	・「情報セキュリティ人材育成プログラム」の策定とそれを踏まえた関係施策等の進捗状況
(ウ)	情報セキュリティに関する教育における産学連携の促進	・PBL（課題解決型学習）等の実践教育を推進する産学連携のネットワークの構築状況
(オ)	情報セキュリティに係る競技会・演習等の実施	・セキュリティキャンプ、セキュリティコンテスト等の開催支援状況
(カ)	横断的キャリアパス・モデルの普及、人材育成計画の策定促進	・キャリアパスモデルの普及促進
(キ)	スキル、資格、教育プログラム等の整理	・共通キャリア・スキルフレームワークの普及促進
(ケ)	情報セキュリティに関する国家試験の改善	・情報セキュリティに関する資格制度の検討状況
(タ)	情報セキュリティ監査知識を有する人材の育成等の促進	・情報処理技術者試験（情報セキュリティスペシャリスト試験、システム監査技術者試験等）の合格者数
(ツ)	制御システムセキュリティに係る人材育成	・制御システムセキュリティセンター（CSSC）テストベッド施設を活用した、制御システムセキュリティ人材の育成状況
(テ)	政府機関等による民間セキュリティ人材の一時的受入れ	・政府機関等による民間セキュリティ人材の一時的受入れ、優秀な外部人材の活用状況

④リテラシー向上

【初等中等教育段階における取組】

(ア)	初等中等教育段階における情報に関する教育	・初等中等教育段階における情報モラル教育の実施状況 ・教員のセキュリティリテラシー向上、教員のICT活用指導力の状況（学校における教育の情報化の実態等に関する調査：文部科学省） ・e-ネットキャラバン開催状況（総務省、文部科学省）

【高齢者層などリテラシーの強化が必要とされる層における対策】

(イ)	情報セキュリティ・サポーターの育成・活用	・情報セキュリティ・サポーターの育成・活用状況
(ウ)	情報セキュリティ相談窓口の充実	・情報セキュリティ相談窓口の機能充実

【スマートデバイスへの対応】

(エ)	スマートフォン等による安心・安全な無線LANの利用の推進	・無線LANへのオフロード促進状況
(カ)	スマートフォン等におけるフィルタリングの在り方の検討	・スマートフォン等のセキュリティ対策、利用者情報保護、フィルタリング等の導入状況
(ク)	ソーシャルメディアの利用に係る情報セキュリティ確保方策	・SNS利用にかかるセキュリティの確保の検討、個人情報保護の状況

3「世界を率先する」サイバー空間の構築

①外交

【基本的な価値観を共有する国等との多角的なパートナーシップの構築・強化】

(ア)	ハイレベルによる戦略的な取組の強化	・ハイレベルによる戦略的な取組状況

【従来の国際法の適用に関する検討の深化】

(イ)	サイバー空間に関する国際的な規範作りへの参画等	・サイバー空間における国際法の適用に関する検討、国際的な規範作りへの参画状況
(ウ)	「国際安全保障の文脈における情報及び電気通信分野の進展」に関する政府専門家会合への政府専門家の派遣等による安全保障分野での国際議論への参画	・同会合でのサイバー空間における国際法の適用に関する検討状況等

【二国間・多国間の協議・対話等の継続・拡大】

(エ)	サイバーセキュリティ政策に関する二国間対話の強化	・各国とのサイバー協議等の開催状況
(カ)	多国間の枠組み等における国際連携・協力の推進	・多国間の枠組み等への参画状況

【日米安保体制を基軸とした米国との協力の深化】

(キ)	サイバー空間における米国との協力の深化	・日米協力の進展状況

②国際展開			
【ASEAN地域等とともに成長できる関係の構築】			
	(ア)	日・ASEAN情報セキュリティ政策会議の推進による日・ASEAN関係の連携強化	・日・ASEAN情報セキュリティ政策会議等の開催状況 ・ASEAN各国との連携強化の状況（意識啓発、技術協力、サイバー連絡演習、人材育成等）
	(イ)	日・ASEAN のサイバー犯罪対策協力の促進	・サイバー犯罪対策能力構築支援の実施状況
	(エ)	APECにおける情報セキュリティ分野の連携推進	・研究開発や意識啓発等の連携推進状況、CSIRT構築・支援の活動状況
	(オ)	海外の組織内CSIRTの構築・運用支援	・CSIRT構築・支援の活動状況
	(カ)	各国における対外・対内調整を担うCSIRTの体制強化の支援及び連携の強化	・インシデント対応業務の支援状況及び連携強化状況、各国CSIRTとの連携状況
	(キ)	ASEANのビジネス環境整備（ISMS等）	・ベンチマーク等のツールの技術提供と導入の支援実施状況
	(ク)	サイバー攻撃事前防止・早期対策に向けた取組の推	・サイバー攻撃予知・即応技術の研究開発の状況
	(ケ)	アジア太平洋地域等での早期警戒情報の共有促進	・サイバー攻撃予知・即応技術の研究開発、インターネット定点観測（TSUBAME等）のプロジェクトの状況
	(コ)	途上国向け研修・セミナー等の開催	・動向、技術、政策等に関する研修やセミナーの開催
	(サ)	途上国に対する技術援助の推進（サイバー犯罪対策のための刑事司法制度整備）	・二国間又は多国間の枠組みを活用した技術援助活動の推進状況
	(シ)	ソフトウェア開発のアウトソーシング先国等におけるセキュアコーディングセミナーの実施	・コーディング手法に関する技術セミナーの実施状況
【日本企業の国際展開の促進】			
	(ス)	情報セキュリティ分野での国際標準化への参画	・国際標準化への参画状況
	(セ)	脆弱性対策に関する国際標準化活動等への参画	・国際標準化への参画状況
	(ソ)	Common Criteria（ISO/IEC15408）における国際協調	・CC認証等における国際協調状況
	(チ)	制御システムセキュリティに関する国際支援	・各国への働きかけ、協力関係の構築状況
	(ト)	個人情報の保護に関する国際的な取組への対応	・個人情報保護に係る国際会議等への対応状況
③国際連携			
【サイバー犯罪対策における連携】			
	(ア)	サイバー攻撃に関する諸外国関係機関との連携の強	・サイバー攻撃に関する情報交換の状況
	(イ)	サイバー犯罪の取締りのための国際連携の推進	・サイバー犯罪に関する情報交換、最新捜査手法の習得、職員交流、国際捜査共助等の状況
	(ウ)	中央当局制度を活用した国際捜査共助の迅速化	・国際捜査共助の状況
	(エ)	サイバー犯罪条約普及への参画	・サイバー犯罪条約普及への参画状況
【情報共有・信頼醸成措置の推進】			
	(オ)	国際会議等への参加を通じた連携の強化	・国際会議等への参画状況
	(カ)	諸外国とのCSIRT間連携の強化	・海外CSIRT等との情報共有、連携状況
	(キ)	国際的な窓口機能の強化を通じた各国との連携	・国際的な窓口機能の構築状況
4 推進体制等			
	(ア)	NISCの機能強化	・「サイバーセキュリティセンター（仮称）」への改組に向けた検討状況