資料 2-3

平成 25 年度　サイバーセキュリティ政策の評価等の実施方針（案）

平成 26 年1月　　日
情報セキュリティ政策会議決定

情報セキュリティ政策会議（以下「政策会議」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　日政策会議決定。）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 2013」（平成 25 年6月 27 日政策会議決定。以下「年度計画」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

政策会議は、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

政策会議は、リスクや脅威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、内閣官房及び各府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、政府機関統一基準群[1]に基づき、対策実施状況報告書等をもとに客観的な評価を行い、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2次行動計画」[2]に基づく施策の成果検証等をもとに評価を行い、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

政策会議は、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。

内閣官房情報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 「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における政府機関統一管理基準及び政府機関統一技術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管理基準（平成 24 年度版）」及び「政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版）」を指す。

2 平成 21 年2月3日政策会議決定、平成 24 年4月3日改定。

⑴ 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。

⑵ 補完調査

NISC は、⑴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。

⑶ 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	サイバーセキュリティ政策内容	評価に当たり考慮すべき状況
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	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	・外部の脅威（標的型攻撃等）から重要な情報資産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状況。 ・政府機関統一基準群の改定状況。 ・認証ガイドラインに基づく助言等の実施状況。
	多様化する就労形態等への対応の強化	・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。 ・重要な情報の提供におけるSNSの利用への対応。 ・可搬記憶媒体（USBメモリ等）の情報セキュリティ対策の強化。 ・複合機等のセキュリティ対策の強化。
	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。 ・最高情報セキュリティアドバイザー等連絡会議の審議状況。 ・各府省庁におけるPDCAサイクルの適正性等を確認するための枠組みの構築状況。
	CSIRT等との連携強化や訓練等による対処態勢の構築・強化	・政府機関におけるCSIRT体制の機能の維持・向上の状況。 ・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。 ・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。 ・サイバー攻撃の主体・方法等に関する情報収集・分析の実施状況。 ・サイバー攻撃に対する各種訓練及び研修の実施状況。 ・脆弱性検査の実施状況。 ・標的型メール攻撃に係る教育訓練の実施状況。 ・各府省庁の情報システム運用継続計画の運用及び維持・改善策定状況。
	政府横断的な情報収集・分析システム(GSOC)の充実・強化	・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。 ・政府情報システムの統合・集約化の進捗状況
	電子メールに係る成りすまし防止等の対応強化	・電子メール利用における送信ドメイン認証技術やDKIM等の暗号技術の導入状況。
	安全な暗号利用の推進	・移行指針に規定する要件への適合状況。
	情報通信技術の利用環境変化に伴う情報セキュリティの確保等	・「政府情報システム管理データベース」の整備状況。 ・「政府共通プラットフォーム」における情報セキュリティ確保方策の検討状況。 ・クラウドサービスの利用状況。（通信利用動向調査：総務省） ・クラウドサービスを利用しない理由。（通信利用動向調査：総務省） ・スマートフォンの利用状況。（情報セキュリティの脅威に対する意識調査：情報処理推進機構） ・スマートフォンに必要だと思うセキュリティ対策。（情報セキュリティの脅威に対する意識調査：情報処理推進機構） ・ウィンドウズXP等のサポート終了問題への対応状況。
	政府機関情報システムに情報セキュリティ対策が適切に組み込まれるための方策	・「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の各府省庁における活用・普及状況。

		社会保障・税番号制度に対応した情報セキュリティ対策の検討	・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。
		地方公共団体、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。 ・独立行政法人における送信ドメイン認証技術導入の進捗状況。
		人材の確保・育成	・人事ローテーションの工夫の検討の状況。 ・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。 ・外部人材の活用状況。 ・政府機関における情報セキュリティ教育の実施状況。
		対処態勢の整備	・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。
	②重要インフラ事業者等における対策	新たな行動計画の策定	・「重要インフラの情報セキュリティ対策に係る第2次行動計画」の見直し、次期行動計画策定の進捗状況。
		リスク評価手法に基づく対策の重点化	・政府機関等による施策の検証における安全基準等の整備及び浸透状況。 ・共通脅威分析において実施した検討項目件数。 ・環境変化への対応における情報発信やリスク・コミュニケーションの現状。
		情報共有体制の深化・拡充	・セプターの強化、セプターカウンシルの活動状況。 ・情報共有体制における共有情報の動向。 ・重要インフラ事業者等の取組の検証における検証レベルを逸脱したIT障害等の発生状況。
		重要インフラ障害に対する連携対応能力の強化	・分野横断的演習における参加規模と参加者の意向。
		制御システムに関する情報セキュリティ上の課題への対応	・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。評価・認証機関の設立。
		重要インフラ分野における国際連携の推進	・「MERIDIAN」への参画、連携実績。
		訓練等による対処態勢の強化	・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。
	③企業・研究機関等における対策	中小企業に対する情報セキュリティ対策支援	・中小企業を指導する立場にある者等を対象としたセミナー等の開催状況。 ・個人情報保護、技術・営業秘密保護のための取組の実施状況。
		事業等リスクの開示	・上場企業における事業等のリスクとしての開示の検討状況。 ・セキュリティエコノミクスに関する対応状況。
		情報セキュリティガバナンスの確立	・「セキュリティガバナンス協議会」の活動状況。 ・ 企業における情報セキュリティ監査制度の活用、企業における情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークの活用状況、取引相手における情報セキュリティ対策実施状況の確認状況、CC認証取得製品の導入状況。 ・「情報システム・モデル取引・契約書」の活用状況。 ・ 電子署名利活用の普及促進。 ・ 企業におけるCISO、CSIRT等の設置状況。 ・ 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の検討。 ・ 経営層向けセミナーの開催状況。

		・情報セキュリティトラブルの重要性に対する認識（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（リスク分析）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（セキュリティポリシーの策定）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（情報セキュリティ報告書の作成）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（事業継続計画（BCP）の作成）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（全体的なセキュリティ管理者の配置）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（部門ごとのセキュリティ管理者の配置）（情報処理実態調査：経済産業省） ・情報セキュリティ対策状況（内部統制の整備強化）（情報処理実態調査：経済産業省） ・情報セキュリティの対策状況（ISO/IEC15408認証取得製品導入）（情報処理実態調査：経済産業省） ・情報セキュリティ対策状況（外部専門家による常時セキュリティ監視）（情報処理実態調査：経済産業省） ・情報セキュリティ対策状況（内部によるシステム監査）（情報処理実態調査：経済産業省） ・情報セキュリティ対策のセキュリティ向上以外の効果の推移（情報処理実態調査：経済産業省）
	個人情報保護の見直し	・個人情報保護法の見直し進捗状況。
④サイバー空間の衛生	普及啓発	・「情報セキュリティ普及・啓発プログラム」の見直し進捗状況。 ・「サイバーセキュリティの日（仮）」の新設。「情報セキュリティ月間」の充実。 ・各種メディアを通じた普及啓発の推進。 ・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） ・事故事例等の収集実績。 ・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	・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。 ・サイバー攻撃事案の実態解明に係る情報収集・分析状況。 ・標的型攻撃等、新しい攻撃の分析・共有状況。 ・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）
	ソフトウェア脆弱性への対応	・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）、IPA「icat」等。 ・制御システムに係る脆弱性ハンドリング体制の改善、組込機器の脆弱性対策の推進状況。
	安全・安心なサイバー空間の実現	・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。 ・IPv6普及・高度化推進協議会等における検討・推進状況。 ・スパムメール対策の状況。 ・SOC事業者間等における情報共有の状況。

⑤サイバー空間の犯罪対策	サイバー攻撃対策等の強化	・「サイバー攻撃特別捜査隊」、「サイバー攻撃対策官」、「サイバー攻撃分析センター」等の設置。「サイバーフォースセンター」の技術力向上。 ・日本版NCFTAの創設、サイバー攻撃に関する産学官連携の推進状況。 ・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） ・フィッシング対策協議会の活動状況。 ・サイバー犯罪の検挙状況（サイバー犯罪の検挙状況等について：警察庁） ・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。
	事後追跡可能性の確保	・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。 ・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	・サイバー防犯ボランティアの育成状況。
	スマートフォン利用者を狙ったサイバー犯罪への対処	・アプリのチェックの仕組みの充実、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	・サイバー防衛隊(仮称)の進捗状況。 ・サイバー攻撃対処の能力・態勢強化の進捗状況。
	国家レベルのサイバー攻撃への対応強化	・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	スマートコミュニティ・スマートグリッドの普及	・M2Mにおける情報セキュリティの検討会・研究開発の進捗状況。 ・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検討会・研究開発の進捗状況。 ・パーソナルデータ等を利活用した新サービスの開発・育成状況。 ・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。
	クラウドコンピューティングの普及	・安心・安全なクラウド利用環境の実現に向けたガイドライン策定、国際標準化に向けた取組の状況。 ・SaaS利用に伴う外部への支払い費用。（情報処理実態調査：経済産業省） ・SaaS利用に関するSLAの状況。（情報処理実態調査：経済産業省） ・クラウドサービスを利用しない理由。（通信利用動向調査：総務省）
	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、評価・認証の国際相互承認等に参加。 ・セキュリティ製品の政府調達における在り方の検討状況。
	安全な電子商取引の推進	・BtoB EC（企業間電子商取引）市場規模について（我が国情報経済社会における基盤整備）。（経済産業省） ・EtoC EC（消費者向け電子商取引）市場規模について（我が国情報経済社会における基盤整備）。（経済産業省）

②研究開発	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。 ・「研究開発戦略」及び「研究開発ロードマップ」に記載されている重要分野の研究開発の進捗状況。 ・サイバー攻撃の解析・検知技術、標的型攻撃の対策技術、次世代ネットワーク技術等の研究開発進捗状況。
	研究開発拠点等の整備	・「サイバー攻撃対策総合研究センター（CYREC）」整備の状況。 ・サイバーセキュリティ研究基盤「NONSTOP」、制御システムセキュリティ評価・認証テストベッド施設の整備状況。
③人材育成	人材育成プログラムの改定	・「情報セキュリティ人材育成プログラム」改定の進捗状況。
	セキュリティ人材の育成	・大学等における情報セキュリティ教育の実績、産学連携（最新情報の提供、共同研究、マッチング、インターンシップ等）の実績。 ・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。 ・ITスキル標準、キャリアパスモデル、スキルフレームワークの普及促進。 ・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。 ・情報処理技術者試験の改善検討状況。
	専門家の育成	・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。
	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。
④リテラシー向上	初等中等教育段階における取組	・学習指導要領の改定等による、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）
	高齢者層等における対策	・情報セキュリティ・サポーターの育成・活用状況。 ・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	・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。 ・無線LANへのオフロード促進状況。
	ソーシャルメディアへの対応	・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	多角的なパートナーシップの構築・強化	・ハイレベルによる戦略的な取組状況。 ・米国、欧州諸国、ASEAN各国等との各種国際会合、関係構築状況。
	国際規範作りへの参画	・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。
②国際展開	ASEAN地域との連携強化	・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）。

		国際連携による普及・啓発活動	・情報セキュリティ国際キャンペーンの実施状況。
		サイバー攻撃事前防止・早期対策	・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。
		ビジネス環境整備、企業の国際展開の促進	・セキュリティマネジメント導入支援、ノウハウ提供状況。 ・技術研修、セミナーの開催状況。 ・国際標準化への参画、CC認証等における国際協調状況。 ・政府調達ルールの見直し、電子商取引、個人情報保護への対応。
	③国際連携	サイバー犯罪対策における国際連携	・サイバー犯罪に関する情報交換、最新捜査手法の習得、職員交流等の状況。 ・国際捜査共助の状況。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	・国際会議等への参画状況。 ・海外CSIRT等との情報共有、連携状況。
		インターネット国際接続の冗長化	・海外接続ケーブルの複数ルート化、帯域増強の状況。
4 推進体制等			
		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。 ・GSOC抜本強化に向けた検討状況。 ・外部専門家の登用及び活用状況。
		NISCの窓口機能の強化	・各府省庁に対するサイバーセキュリティ・コンサルティングの状況。 ・対外広報、情報発信等の状況。 ・関係府省庁、関係機関・会議、重要インフラ事業者等とのサイバー攻撃に関するインシデント情報等の共有範囲、件数の拡大状況。
		サイバーセキュリティに関する国際戦略の策定	・「サイバーセキュリティ国際連携取組方針」の策定。