資料2

サイバーセキュリティ政策の評価に係る基本方針（案）

平成 27 年　　月　　日
サイバーセキュリティ戦略本部決定

サイバーセキュリティ戦略本部（以下「本部」という。）がサイバーセキュリティ政策を総合的かつ効果的に推進するため、サイバーセキュリティ政策の評価に係る基本方針を以下のとおり定める。

１　評価の目的

政府におけるサイバーセキュリティ政策に関する取組状況を毎年度点検し、必要な見直しを実施することによって、サイバーセキュリティ政策を着実に推進することを図るとともに、政府の取組状況について国民への説明責務を果たすことを目的とする。

２　評価の対象

評価の対象は以下のとおりとする。

(1)　サイバーセキュリティ戦略（平成 27 年９月４日閣議決定。以下「戦略」という。）に基づく年次計画で定められた施策
(2)　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
(3)　重要インフラ事業者等における対策のうち、「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。平成 27 年５月 25 日サイバーセキュリティ戦略本部改訂。以下「行動計画」という。）に関連する対策

３　評価の実施方法

(1)　戦略に基づく年次計画で定められた施策

戦略に照らした評価の視点（別添）から、年度末時点の達成度合いを毎年度評価する。評価にあたっては、サイバー空間を取り巻く脅威やリスクは常に変化し続けることから、年度末時点における脅威やリスクの状況変化も考慮する。

(2)　政府機関統一基準群に関連する対策

本部が実施する監査やその他の政府機関統一基準群に基づく点検の結果に応じて評価する。

---

[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。

(3)　行動計画に関連する対策

行動計画に基づく施策の成果検証等の結果に応じて評価する。

4　評価結果の活用

本部は、３で定めた評価を実施した結果、サイバーセキュリティ政策に関する課題等が確認された場合は、次年度の年次計画へ改善事項を反映する等、必要な対応を関係府省庁の協力を得つつ実施する。

5　評価結果の公表

本部は、サイバーセキュリティ上の特性に配慮しつつ、３で定めた評価の結果を年次報告として取りまとめ、公表する。

1. 経済社会の活力の向上及び持続的発展

1.1. 安全な IoT システムの創出

- IoT に係る事業におけるセキュリティ・バイ・デザインの推進状況。
- 経済社会への影響が大きい大規模な IoT 事業における横断的なセキュリティ対策に必要な企画・立案・総合調整（関係府省庁及び産学官の連携を含む）の実施状況。
- IoT のセキュリティに係る総合的なガイドラインや基準の整備状況。
- 利用者に着実に対策が行き届くような仕組み（社会的還元の道筋等の明確化）の検討、構築、活用に関する取組状況。
- IoT のセキュリティ対策に特に重要な技術開発・実証事業の実施状況。

1.2. セキュリティマインドを持った企業経営の推進

- ステークホルダーからサイバーセキュリティに関する取組が正当に評価される仕組みや財務面で有利となる仕組みの構築、情報開示を含むガイドライン等による啓発活動の実施状況。
- キャリアパスを考慮した長期的な人材育成や人事評価の在り方についての検討、経営層に訴求する取組の展開状況。
- インシデント情報共有のためのプラットフォーム構築等、情報共有網の拡充に関する取組状況。

1.3. セキュリティに係るビジネス環境の整備

- 中小企業等におけるセキュリティが確保されたクラウドサービスの普及に関する取組状況。
- 政府系ファンドの活用や、共同研究開発の促進、研究開発成果を活用したベンチャー企業の育成等の取組状況。
- 著作権法におけるリバースエンジニアリングに関する適法性の明確化等、制度見直しについての検討状況。
- 国際的な標準規格や評価・認証制度の相互認証への枠組み作りに関する取組状況。
- ASEAN 諸国等における必要な制度整備の支援、普及啓発活動等の実施状況。

2. 国民が安全で安心して暮らせる社会の実現

2.1. 国民・社会を守るための取組

- 脆弱性関連情報の収集やサイバー攻撃等観測システムの連携・強化に関する取組状況。
- 攻撃を受けた端末の利用者に対する注意喚起、感染による被害を未然に防ぐ方策の検討及び実施状況。
- 訪日客向けインターネット通信環境におけるセキュリティ対策の検討状況。
- 「サイバーセキュリティ月間」を始めとする、普及啓発活動の取組状況。
- インターネット利用における悩みや不安の相談に応じる活動の取組状況。
- 不正プログラム解析の技術力向上、インターネット観測高度化等の取組状況。
- 通信履歴の保存に関する取組の推進状況。

2.2. 重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し状況。
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進状況。
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制の整備状況。
- 制御系システムについて、国際標準に即した第三者認証制度の活用等の推進状況。

2.3. 政府機関を守るための取組

- サプライチェーン・リスクへの対応を始めとした企画・設計段階からのセキュリティ確保を盛り込む取組の推進状況。
- ペネトレーションテストを始めとした検査の実施状況。
- GSOC の検知・解析機能の強化及びインターネット接続口の集約状況。
- CSIRT の体制強化及びインシデント発生に備えた訓練・演習の実施状況。
- 定期的な自己点検及び第三者視点からのマネジメント監査の実施状況。
- 独立行政法人や府省庁と一体となり公的業務を行う特殊法人等における対策の強化状況。

3. 国際社会の平和・安定及び我が国の安全保障

3.1. 我が国の安全の確保

- 外国政府機関との情報共有を含む情報収集・情勢分析機能の強化状況。
- 対処機関における人材育成・確保、最新技術の導入・習得、研究開発等を含む諸制度の見直し等の検討状況。
- カウンターサイバーインテリジェンスに係る取組の推進状況。
- 先端技術に関与する組織における意識啓発、監視・対処能力の向上、調達物品・サービスに関する調査・確認、官民の情報共有等の実施状況。
- 政府と社会システムを担う事業者間における双方向の情報共有。
- 自衛隊の任務保証に関連する主体との連携状況。

3.2. 国際社会の平和・安定

- 国際法の適用に関する議論（国際会議等）への参画状況。
- サイバー犯罪条約の拡大、国際捜査共助等の国際連携の強化状況。
- 国際的な連絡体制の構築、連絡演習等の実施状況。
- サイバー空間における国際テロ組織の活動等に関する情報収集・分析状況。
- 各国へのキャパシティビルディングの取組状況。
- 国際場裡で活躍し得る、質の高い国際的な人材の育成状況。

3.3. 世界各国との協力・連携

- 日・ASEANにおける国際会議や共同プロジェクト等の枠組み、相手国のニーズを踏まえたキャパシティビルディングの実施状況。
- 日米におけるサイバー関連施策やサイバー攻撃に関する情報の共有・活用、事案への対処に際しての連携、先端的技術分野における共同プロジェクト等の実施状況。
- 欧州諸国との平素からの情報共有・活用、共同訓練、先端的技術分野における共同プロジェクト等の実施状況。
- 中南米、中東アフリカ諸国とのパートナーシップの構築状況。

４．横断的施策

4.1. 研究開発の推進

- 各省庁におけるサイバー攻撃検知・防御力向上等に資する研究開発施策の取組状況。
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含めた領域の研究との連携、融合領域における研究の促進状況。
- 暗号研究等、コア技術を育む基礎研究への取組状況。
- 総合科学技術・イノベーション会議等、産学官が連携した総合的な研究開発において今回のサイバーセキュリティの研究に特に重要な目標への取組状況。

	4.2. 人材の育成・確保 ・ 産学官連携による人材育成のための実践的な演習の取組状況。 ・ 技術的な能力とともに、法律や経営学、組織経営等に必要な知識を併せ持つハイブリッド型人材の育成に関する取組状況。 ・ 初等中等教育段階における情報モラルや論理的思考力等の教育状況。 ・ 海外からの参加者を集めた競技イベントの実施状況。 ・ 実践的な能力を適時適切に評価できる資格制度や標準的なスキル基準の整備、キャリアパスの構築に関する取組状況。
5．推進体制	
	・ 高度セキュリティ人材の民間登用等による NISC の対処能力の強化状況。 ・ サイバー空間における脅威情報の収集・分析機能に関する我が国全体としての強化状況。 ・ 政府機関、独立行政法人、セキュリティ事業者等が協力して大規模なサイバー攻撃へ対処するための体制整備状況。 ・ 2020 年東京オリンピック・パラリンピック競技大会に向けた専従 CSIRT の整備に係わる検討状況。