資料 3-2

「情報セキュリティ２０１２」の骨子案

１　最近の環境変化

⑴　本格的なサイバー攻撃の発生と深刻化
- 標的型攻撃の拡大と深刻化
- インターネット以外の環境における脅威の顕在化
- 意図的なサイバー攻撃の実施　等

⑵　社会経済活動の情報通信技術への依存度の更なる高まりとリスクの表面化
- スマートフォン等の本格的な普及と脆弱性を利用した攻撃の表面化
- ソーシャル・ネットワーク・サービス（SNS)、クラウドコンピューティング等の普及、IPv6 への移行　等

⑶　新たな技術革新に伴う新たなリスクの出現
- M2M（Machine To Machine）[1]環境の出現　等

⑷　重大なＩＴ障害のリスク回避に向けた取組の必要性の高まり
- 東日本大震災に伴う事業継続計画(BCP)上の問題の顕在化
- 集積された個人情報の侵害や漏えいに対する国民の不安の増大　等

⑸　諸外国による取組の強化
- 諸外国による安全保障面を含む情報セキュリティへの取組の強化
- サイバー空間における国際連携のための様々な取組　等

２　基本方針

「国民を守る情報セキュリティ戦略」（2010 年度～2013 年度の４カ年計画）で示された基本的考え方、及び、最近の環境変化と関連施策の実施状況を踏まえた以下の視点の下、施策を重点化して取りまとめる。なお、「情報セキュリティ 2011」の基本方針に示された「『サイバー空間』についての基本的考え方」を踏襲する。

①　国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化

②　スマートフォン等の本格的な普及に伴うリスクの表面化に対応する安全・安心な利用環境の整備

③　国際連携の強化

---

[1] M2M（エムツーエム、Machine-to-Machine の略）とは、ネットワークに繋がれた機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムを指す。例としては、各種センサー・デバイス（情報家電、自動車、自動販売機、建築物、スマートフォン等）を、ネットワークを通じて協調させ、エネルギー管理、施設管理、経年劣化監視、防災、福祉等の多様な分野のサービスを実現するなど。

３　主な施策

⑴　大規模サイバー攻撃事態への対処態勢の整備等

〇初動対処態勢の充実

・サイバー攻撃等対処に係る企画機能の強化（防衛省）

・陸自電算機防護システムの整備等（防衛省）

・重要インフラに対するサイバーテロ対策に係る官民連携の強化（警察庁）

〇訓練の実施

・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（内閣官房及び関係府省庁）

〇国際的な情報収集

・諸外国の関係機関等とのサイバー攻撃に係る情報の共有を通じた対処能力の向上（内閣官房及び関係府省庁）

〇高度解析機能の整備

・攻撃手法が複合化・複雑化するサイバー攻撃を高度解析する枠組みの検討（総務省及び経済産業省）

・サイバーテロの予兆の早期把握と情報収集・分析の強化（警察庁及び法務省）

⑵　政府機関等の基盤強化

〇政府機関における態勢の強化

・CSIRT 等の体制の整備及び連携の強化（内閣官房及び全省庁）

・国の重要な情報を扱う企業等の情報セキュリティ対策の推進（内閣官房及び全府省庁）

〇職員を対象とした訓練、システムへの検査等の充実

・標的型攻撃に係る教育訓練の実施（内閣官房及び関係府省庁）

・公開ウェブサーバに対する脆弱性検査の実施（内閣官房及び関係府省庁）

〇GSOC の能力充実

・政府横断的な情報収集・分析システム（GSOC）の運用による緊急対応能力の向上（内閣官房及び全府省庁）

〇複数の府省庁で共通使用するシステムの運用管理体制等の整備

・複数の府省庁で共通的に使用する基盤となる情報システムの運用管理体制等整備（内閣官房及び関係府省庁）

〇社会保障・税番号制度への対応

・社会保障・税番号制度及び国民 ID 制度に対応した情報セキュリティ対策の検討（内閣官房及び関係府省庁）

⑶　重要インフラの基盤強化

〇行動計画を踏まえた指針の見直し

・「重要インフラの情報セキュリティに係る第２次行動計画」の改定（内閣官房）

〇セプターカウンシル等の情報共有体制の強化

・セプターの強化及び訓練（内閣官房）

〇重要インフラ分野での国際連携の強化

・MERIDIAN 等を通じた国際連携推進（内閣官房、総務省及び経済産業省）

〇共通脅威分析、分野横断的演習を通じた対策の向上

・共通脅威分析の実施（内閣官房）

・分野横断的演習の実施（内閣官房及び重要インフラ所管省庁）

〇個別分野におけるサイバー演習

・通信、電力、ガス等の個別分野におけるサイバー演習（総務省及び経済産業省）

⑷ 標的型攻撃に対する官民連携の強化

〇政府機関、企業等における対応の強化と連携、情報共有態勢の構築

・官民のサイバー攻撃情報共有ネットワーク及び関係団体間の情報連携（内閣官房、警察庁、総務省及び経済産業省）

⑸ 脅威の高度化・多様化への対応

〇スマートフォンの情報セキュリティ上の課題への対応

・スマートフォンにおけるセキュリティ確保の推進（総務省及び経済産業省）

・スマートフォンの情報セキュリティ対策の強化（内閣官房及び全府省庁）

〇クラウド化、IPv6 に対応した情報セキュリティ確保方策

・社会基盤としてのクラウドのセキュリティ（総務省及び経済産業省）

・災害に備えたクラウドへの移行等の促進（総務省）

〇制御系システムにおける情報セキュリティの強化

・制御システムのセキュリティに係る検証施設の構築、情報セキュリティ標準に関する国際標準化の推進及び評価・認証制度の整備（経済産業省）

〇M2M 環境における情報セキュリティの在り方の検討

・M2M 環境における情報セキュリティの在り方の検討（内閣官房、総務省及び経済産業省）

⑹ 研究開発、人材育成の推進

〇研究開発等の充実

・イノベーション創出を支える情報基盤強化のための新技術開発（文部科学省）

・標的型攻撃の対策に関する技術開発（総務省）

・情報セキュリティ研究開発戦略の推進（内閣官房、総務省、文部科学省、経済産業省及び防衛省）

〇人材育成の充実

・内閣官房情報セキュリティセンターや独立行政法人等を活用した人材育成（内閣官房、総務省及び経済産業省）

⑺ 情報セキュリティ産業の振興

〇総合的な情報セキュリティ産業振興策の推進

・情報セキュリティ産業の振興策の検討（内閣官房、総務省及び経済産業省）

⑻ 国民・利用者保護の強化

〇継続的な普及・啓発の推進

・スマートフォンの情報セキュリティ対策に係る普及啓発（内閣官房、総務省及び経済産業省）

〇「情報セキュリティ月間」のさらなる充実

・「情報セキュリティ月間」の充実（内閣官房及び関係省庁）

・「国際連携情報セキュリティ意識啓発週間」（仮称）の実施（内閣官房及び関係省庁）

〇情報システム障害等による社会混乱の防止

・情報システム等の安全性・信頼性に関する利用者への品質説明力の強化（経済産業省）

⑼ 制度整備

〇サイバー空間の安全性・信頼性を向上させる制度の検討

・サイバー刑法の円滑な施行（法務省）

・サイバー犯罪条約の締結に向けた準備（外務省）

〇改正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

・不正アクセス防止対策の強化（警察庁、総務省及び経済産業省）

〇各国の情報セキュリティ制度の比較検討

・各国のセキュリティ法制度の調査（内閣官房）

⑽ 国際連携の強化

〇米、欧州諸国、ASEAN 等との国際連携の強化

・情報セキュリティ政策に関する二国間政策対話の強化（内閣官房及び関係府省庁）

・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（内閣官房、総務省及び経済産業省）

・サイバー攻撃に関する国際的な情報収集ネットワーク構築・研究開発（総務省）

・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（経済産業省）

〇国際的な議論への積極的な参画

・サイバー空間に関する国際規範作りへの参画（内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省）

・サイバー空間に関するブダペスト会議や「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歩」に関する国連政府専門家会合等の国際会議への参画（内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省）