情報セキュリティに関する提言

平成２４年２月２４日

自　由　民　主　党

情報セキュリティに関する提言
３つのポイント

1. 我が国は、既に組織的なサイバー攻撃の脅威にさらされており、この状況をサイバー空間における「有事」とし、国家安全保障上の重要課題と位置付ける。
⇒ **政治主導**

2. 我が国の情報セキュリティ技術は、未だ世界最高峰には程遠く、現行目標（２０２０年）では、足下の有事に対処できないので、今後５年程度に目標を短縮し、国家安全保障の喫緊の課題として緊急に技術開発の予算措置を行い、世界最高峰の国産技術を育成する。 ⇒ **技術開発**

3. 安全保障に対する国家的な投資を呼び水として、高度な情報セキュリティ産業市場を創出し、民間に１０万人規模の新規雇用を生む。 ⇒ **産業創出**

これらの政策を具体化するとともに、それらを推進するために必要な法と組織体制の整備と予算措置を提言する。

目　　次

情報セキュリティに関する提言

はじめに

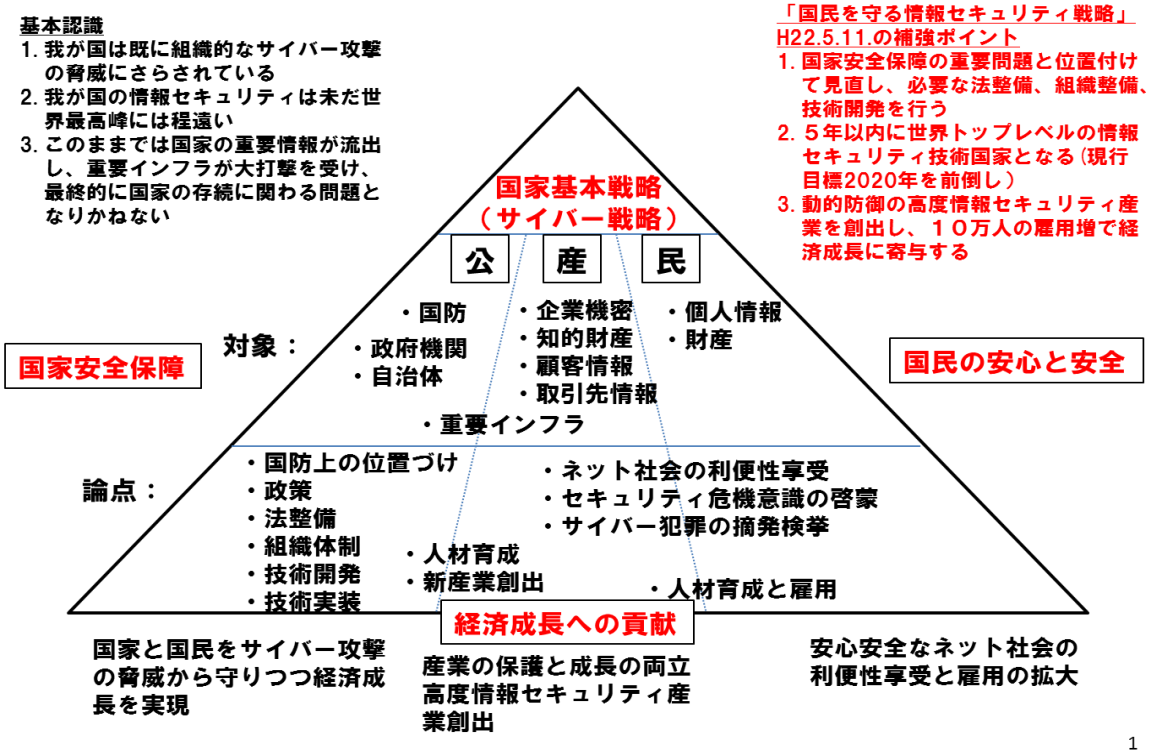
平成２３年、国会、行政機関、国家の重要な情報を扱う企業などがサイバー攻撃を受け、重要な情報が窃取されるという事態が発生した。平成 23 年米国がサイバー空間を第５の戦場と位置付けたように、今やサイバー攻撃は、国家安全保障上の重要問題であり、このまま放置すれば国家機関や国の重要インフラに深刻な打撃を受けかねない。

政府は、平成２２年に「国民を守る情報セキュリティ戦略」を策定したが、平成２３年に発覚した足下の状況を考えると、より国家安全保障上の位置づけを高め、情報セキュリティ確保のための体制を緊急に拡充整備するとともに、研究開発、人材育成、関連産業の活性化等の対策を速やかに実施し、２０２０年に世界最先端の「情報セキュリティ先進国」実現を目指す政府目標を前倒し、今後５年以内にこれを達成するべきである。

研究開発推進による高度な技術と人材育成の促進、高度な技術と人材による産業の活性化・起業の促進、産業の活性化による研究開発の更なる促進という好循環を形成することにより１０万人の新規雇用を創出して、世界最先端の情報セキュリティ大国を実現し、国家安全保障と成長戦略を同時に達成することを提言する。（資料１「情報セキュリティ政策に関する基本的な考え方」参照）

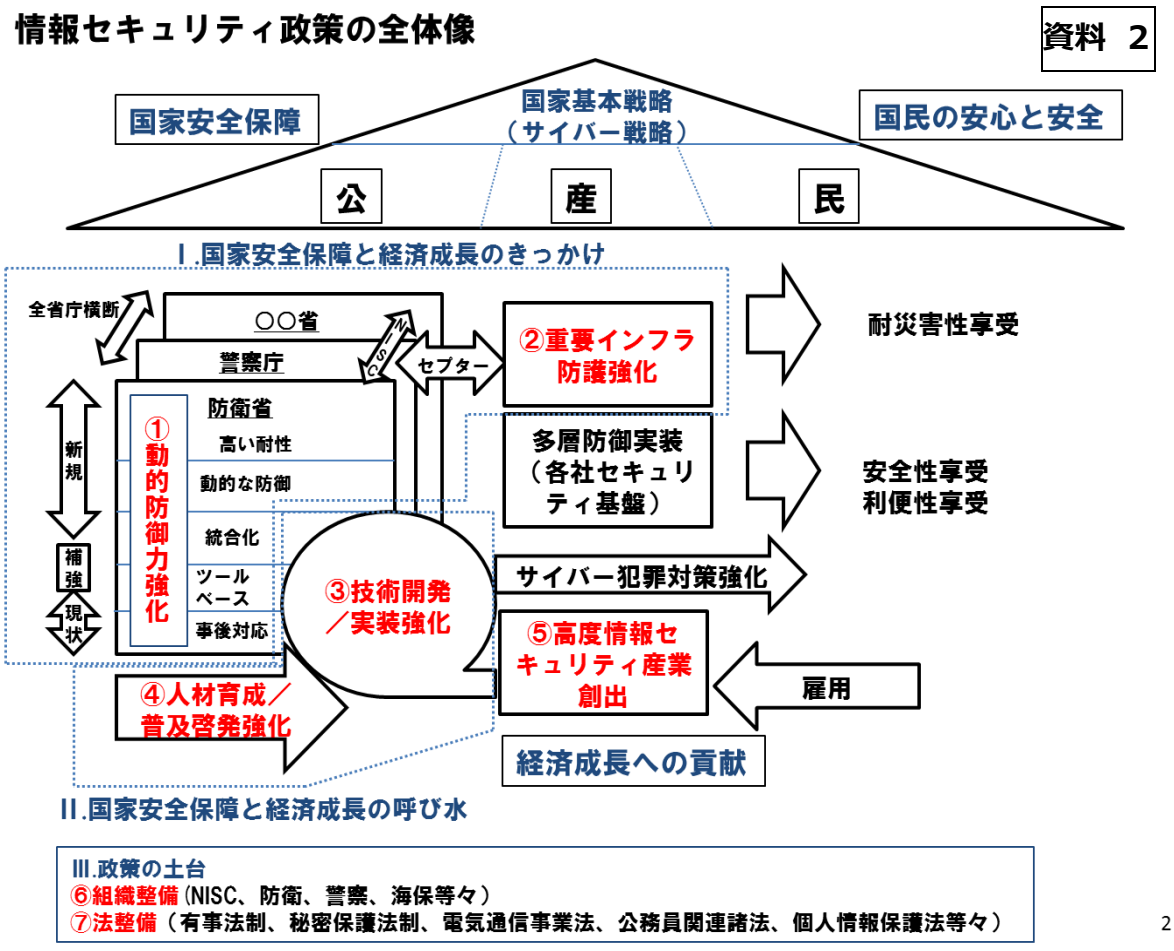
資料 1

情報セキュリティ政策に関する基本的な考え方



1

具体的には、「Ⅰ.国家安全保障と経済成長のきっかけ」として米国防総省並みの「①動的防御力強化」（少なくとも、防衛省、警察庁、海上保安庁）、米国土安全保障省並みの「②重要インフラ防護強化」により、我が国に世界最高レベルの情報セキュリティを実現する事で国家安全保障の強化と経済成長の象徴的なきっかけとする事。また、「Ⅱ.国家安全保障と経済成長の呼び水」としての「③技術開発／実装強化」、「④人材育成／普及啓発強化」を実施して、政策目標実現の呼び水を強化する事。さらに、以上を通じた「⑤高度サイバーセキュリティ産業創出」で１０万人の新規雇用を実現して経済成長へ貢献する事。そして、それらの実現に必要な「Ⅲ.政策の土台」として「⑥組織整備」と「⑦法整備」を行う事を申し入れる（資料２「情報セキュリティ政策の全体像」参照）。法整備に関しては、特に厳正にクラス分けされた情報の管理と運用に必要な秘密保護法制、サイバー攻撃という新たな国家的脅威に対処するために必要な有事関連法制／ガイドラインの整備が急務である。また、組織に関しては、関連する複数省庁間の調整機能の強化と高度な専門性を有する人材の政府における育成と民間からの採用をより積極的に拡大することが急務である。



１．緊急に行うべき対応策

◇ 今般の衆議院システムにおける ID、パスワード漏洩を教訓として、政府及び衆参両院はその情報システムにおいて、下記の取り組みを緊急に行うこと。

・情報システムに接続されている全ての端末におけるウイルスチェックを早急に行うこと。
・システムに接続されている全ての端末におけるウイルス対策ソフトの導入状況、更新状況を確認し、最新のウイルスパターンが導入されていることを徹底すること。
・システムに接続されている全ての端末における OS の更新状況を確認し、必要なパッチ等が当てられていることを徹底すること。
・ログインパスワードの定期的な更新を義務付け、一定期間にわたって更新されない端末は接続を切断すること。
・ワンタイムパスワード、生体認証等により安全度の高い本人確認の導入を早急に確立すること。
・衆参両院は全議員、全秘書に対する情報セキュリティ研修を早急に実施すること。
・衆参両院は、各院が被っている脅威に関する情報を、両院、行政府とともに共有して、迅速な対応に努めること。
・衆参両院は、攻撃発覚後に迅速かつ適切な対応を講じるため、責任の所在を明確にし、情報セキュリティ専門家を有効に配置すること。

◇　政府管轄下の全ての情報機器（端末、サーバ等）に的確なセキュリティポリシーの実装を早急に徹底させ、運用監視センター（SOC）の監視下におくこと。再来年度中に完成させ、個別省庁の SOC 構築が困難な場合は内閣官房情報セキュリティセンターの GSOC の監視下に置くこと。

◇　政府管轄下のネットワーク機能を持つ全ての複合機のセキュリティ機能を検査し、上記と同様に SOC の監視下に置くこと。機能を持たない複合機は早急に入れ替えること。

２．動的防御力強化

防衛省、警察庁、海上保安庁等直接的に国家安全保障に関わる国家機関に対して、米国防総省並みのサイバー攻撃に対する動的防御力を実現し、これを国家安全保障の強化と経済成長のきっかけとする。（資料３「①動的防御力強化のポイント」参照）

資料 3

①動的防御力強化のポイント

対応レベル	各組織の個別対応（現在対応中）		各組織の全体的な対応（例.米国防総省）		
米国防総省(DOD)のリスク/迅速性モデル	A.事後対応	B.ツールベース	C.統合化	D.動的な防御	E.高い耐性
対策の全体像	・発生後にとる対応 ・最低限のツール ・主に手作業	・断片的にツール導入 ・外部コンプライアンスとの適合	・ツールが入り口だけでなく出口も含めた情報システム全面に展開されている ・統合的なアーキテクチャに基づいた多層防御の統一セキュリティシステムが導入されている ・高度な予測機能がある ・サイバー攻撃を受けても即時に検知しログ解析で分析と対応ができる		・高度な予測機能 ・各種攻撃を受けていても通常の運用

日本　　米DOD

先ずはB.ツールベースの完備
全省庁の全端末（複合機を含む）／サーバにツールベースの対応を完備する
- **全端末／サーバへのセキュリティポリシー／ツールの導入**
- **全端末／サーバをGSOCの監視対象とする**
- **SOCを個別に構築運用できる省庁は、その個別SOCとGSOCを連携させる**
- **監視要員は十分にセキュリティを考慮して積極的に民間採用を行う（数千人規模）**

並行してD.動的防御の構築
国家安全保障を担う、防衛、警察、海保では、早急に米国防総省並みの動的防御力を実装する
- **来年度から設計開始**
- **再来年度以降、構築と運用開始**

3

◇　対象機関に対して当面必要なツールベースでの情報セキュリティを万全なものとすること。

◇　来年度から再来年度にかけて対象機関の全端末、サーバ、複合機等の機器に対してセキュリティポリシーを実装し、再来年度以降それらの全てに関して運用監視センター（SOC）での監視を実施する。独自の SOC が望ましいが、場合によっては、内閣官房情報セキュリティセンター（NISC）の運用監視センター（GSOC）を活用してもよい。

◇　数万人規模のサイバー部隊を有している国などへ適切に対処するため、情報セキュリティに関する高度な知見を有する者を数万人規模で補充し、抜本的に強化すること。その際、求める人材像を明確にし、セキュリティコンテストの優秀者や産業界で活躍している者も積極的に採用すること。

◇　対象機関の全体にわたり、未知の攻撃に対してもリアルタイムに防御することのできる統一情報セキュリティシステムとしての多層防御による「動的防御システム」を開発・導入すること。来年度から設計を開始し、再来年度以降に構築、運用を開始すること。

◇　ネットワーク監視センターの拡充などにより、監視機能を抜本的に強化すること。

◇　多層防御による統一的セキュリティシステム構造を備えた高い防御力を持つバックアップシステムの導入を行うこと。

◇　情報システム関連調達品の安全性を担保するため、調達段階において検査する仕組みを構築すること。

◇　サイバー攻撃を受けた際に反撃できる能力を確保するための制度設計、技術開発に取り組むこと。

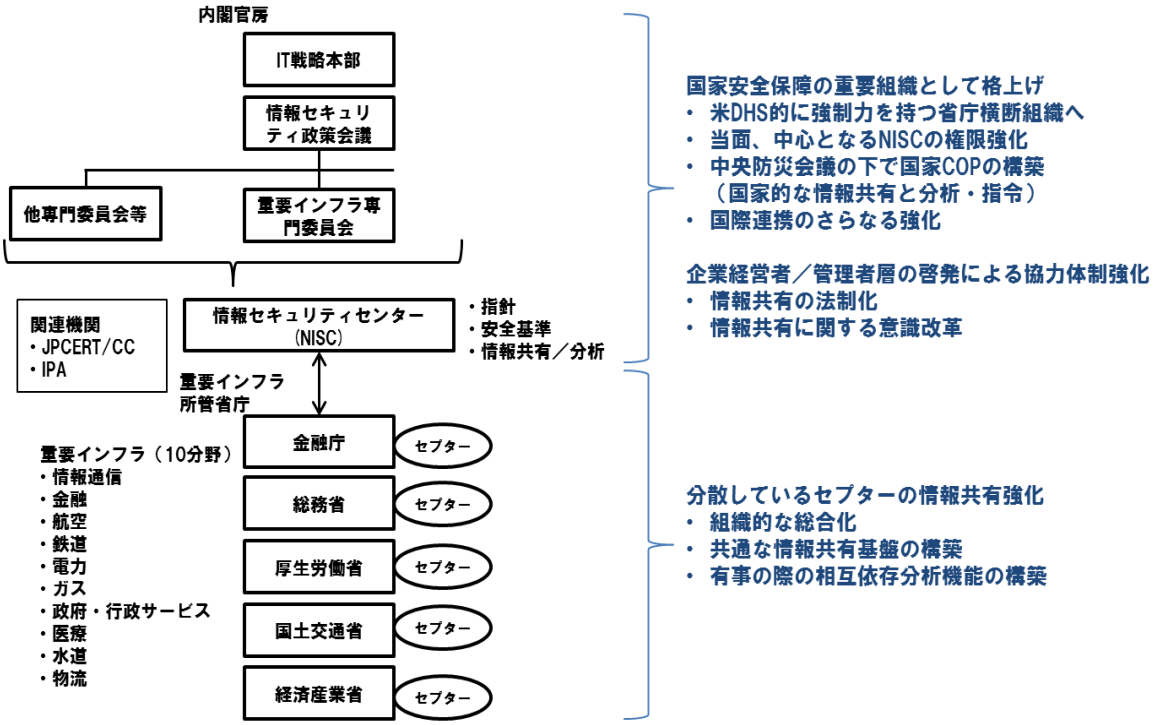
◇　以上の実現により、数千人規模の SOC 要員の雇用と、最先端情報セキュリティ技術の育成を図る。要員の雇用には、十分にセキュリティを考慮した上で、積極的に民間採用を行う。

３．重要インフラ防護強化

現在内閣官房情報セキュリティセンター（NISC）が中心となり、５つの重要インフラ所管省庁が協力している重要インフラ防護（CIP）に関して、国家安全保障上の情報セキュリティ強化と経済成長のきっかけとして、より強力な機能と体制を構築する。（資料４「②重要インフラ防護強化のポイント」参照）

資料 4

②重要インフラ防護強化のポイント



セプター：Capability for Engineering of Protection, Technical Operation, Analysis and Response
COP: Common Operation Picture

4

◇　NISC を中心とする CIP 関連機関（重要インフラ１０分野の各セプターを含む）を国家安全保障上の重要な機関として格上げする。将来的には米国土安全保障省のような省庁横断で強制力を持つ組織とすること。（組織整備として後述）

◇　重要インフラ１０分野の各セプターに共通な情報共有基盤を再来年度までに構築すること。

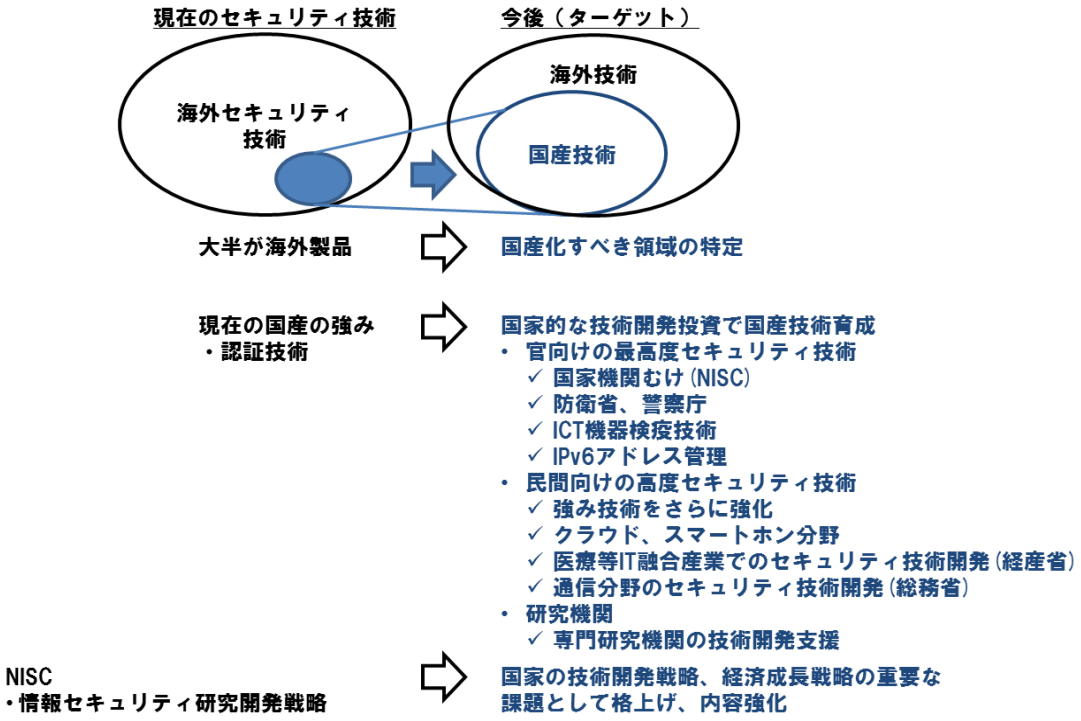
◇　重要インフラ１０分野において有事の相互依存分析機能を、再来年度までに構築すること。

４．情報セキュリティ技術研究開発と実装の強化

国家安全保障の強化と経済成長の呼び水として、情報セキュリティ技術開発と実装の強化を行う。これにより、５年以内に世界最高水準の情報セキュリティ技術保有国となり、この分野であらたに１０万人の雇用を創出させる。（資料５「③技術開発／実装強化のポイント」参照）

③技術開発／実装強化のポイント

資料 5



◇　情報セキュリティ研究開発を国家安全保障、経済成長戦略及び科学技術政策における重要課題として位置づけ、重要な領域での国産技術育成を図ること。

◇　特に、国家安全保障に直接関わる防衛省、警察庁、海上保安庁等において、世界最高水準の情報セキュリティ技術を育成し、その中で特定の対象技術に関しては官での調達を前提とした技術開発を行い、国産技術の育成を強力に推進すること。

◇　情報セキュリティ研究開発戦略（平成23年7月情報セキュリティ政策会議）を推進するため、研究開発予算を大幅に拡充すること。

◇　特に、情報システム内のデータ保護を強化するための技術、クラウドコンピューティングのセキュリティ技術、スマートフォンのセキュリティ技術、サイバー攻撃の解析・追跡技術、情報システム機器の検疫技術など、情報セキュリティ確保の上で重要となる技術開発を強力に推進すること。

◇　世界レベルの研究開発を加速するため、産官学それぞれの研究者･技術者・組織が組織の壁を越えて結集する最先端の情報セキュリティ研究開発拠点及び情報セキュリティに関する脆弱性･安全性評価に関する専門家集団が結集する情報セキュリティ評価拠点を形成し高度情報セキュリティ産業の創出に寄与すること。これらの拠点の整備・運用のため、１０００億円の取り崩し型基金を設置すること。

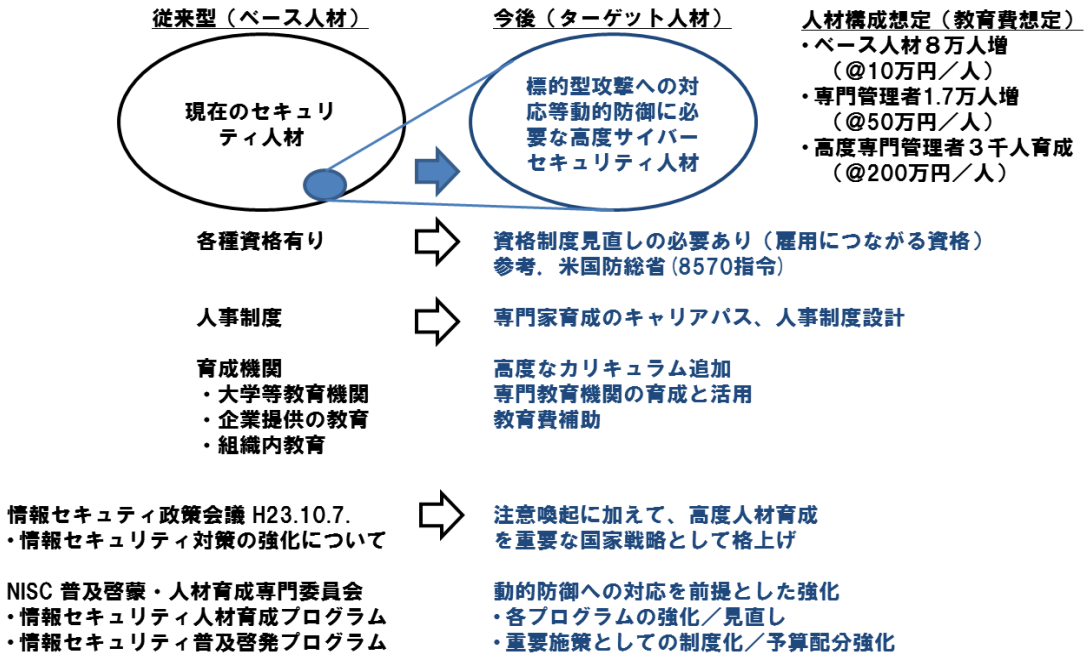
◇　IT 融合産業創出をはじめとして IT を利用するすべての研究開発領域において情報セキュリティに配慮した IT 投資・研究開発を行うこと。これを確保するため、内閣官房は総合科学技術会議と連携した確認を行うこと。

５．情報セキュリティ人材育成と普及啓発強化

国家安全保障の強化と経済成長の呼び水として、情報セキュリティ技術開発／実装の強化とともに、この分野で１０万人の新規雇用を創出するための人材育成を行う。（資料６「④人材育成／普及啓発強化のポイント」参照）

資料 6

④人材育成／普及啓発強化のポイント



6

（１）大学・大学院教育の充実

◇　専門分野でグローバルに活躍できる人材、技術的基盤を有して情報セキュリティだけでなくリスク・マネジメント及びリスク評価もできる人材を育成するため、大学・大学院では、情報セキュリティに関する基礎知識を徹底的に教え、産学連携による実践的な教育を実施すること。

◇　マネジメントと情報セキュリティ技術の知見を融合できる人材を育成するため、経済学、経営学などと数理科学、情報学、ソフトウェア科学、電子通信工学等の両面に関する理論と実務教育のバランスに配慮した体系的なカリキュラムを確立すること。

◇　社会人が最先端の理論と実務を体系的に学べるよう、社会人学生の履修も想定したカリキュラムを確立すること。

◇　情報セキュリティ人材に求められる知識を体系的に学べるカリキュラムを修めた人材に対しては、情報セキュリティ技術経営等の新しい学位を授与すること。
◇　情報セキュリティ人材に求められる知識を体系的に学べるカリキュラムを設けている大学・大学院に対しては、当該カリキュラムを一層充実させるため、重点的に運営費交付金等を交付すること。
◇　情報セキュリティ対策を習得するためには、実践的な訓練が必要であるため、産学連携により、模擬訓練ができる環境を設置すること。

（２）初等中等教育の改革

◇　初等中等教育における全教員及び全管理職を対象とした情報セキュリティ研修等を実施し、初等中等教育における情報セキュリティ教育の質を抜本的に向上すること。
◇　初等中等教育において情報セキュリティが適切に教育されているか定期的に確認すること。
◇　高等学校の必履修科目である「情報」を大学入試センター試験の出題科目とすること。

（３）産官学の人材が交流する回転ドア型キャリアパスの実現

◇　米国防総省指令８５７０を参考に既存の資格制度を見直し、我が国にも世界最先端の情報セキュリティに関する資格制度を設け、これを産官学共に資格取得の推進を行うこと。
◇　特に、上記資格保有者に関しては、国家機関が運用監視センター（ＳＯＣ）を中心に、積極的に採用すること。
◇　情報セキュリティに関する最先端の情報が集約される行政機関・研究開発機関、最先端の実践的な経験ができる監視サービス・情報セキュリティ企業等を相互に経験できるキャリアパスの形成を行うこと。
◇　内閣官房情報セキュリティセンター、独立行政法人情報処理推進機構、独立行政法人情報通信研究機構等に情報セキュリティに関する高度人材を集め、高度情報セキュリティ人材育成のセンター機能を実現すること。
◇　内閣官房情報セキュリティセンター等においては、特定任期付職員等の制度を活用し、高度な専門性を有する情報セキュリティ人材を活用すること。

（４）グローバル人材及びカリスマ人材の発掘・育成

◇　情報セキュリティの分野で世界的に通用し、国際的な議論をリードできる人材を育成すること。

◇　情報セキュリティキャンプやセキュリティコンテスト等の取り組みにより、セキュリティ分析、侵入検査、脆弱性の発見などに長けたカリスマ的な人材を発掘し、育成すること。
◇　政府主催のハッカーコンテストを実施し十分に魅力的な表彰をするとともに、コンテストの優秀者について政府で積極的に登用すること。

（5）国民各界各層に対する普及啓発

◇　情報セキュリティ上のリスクは、被害者となる恐れがあることはもちろんのこと、不正なプログラムに感染することで意図せずに加害者になってしまうこともある。情報セキュリティに係る取組を、一般常識、マナー、あるいは社会的習慣として広く国民全体に定着させるため、細やかな普及啓発活動を行うこと。

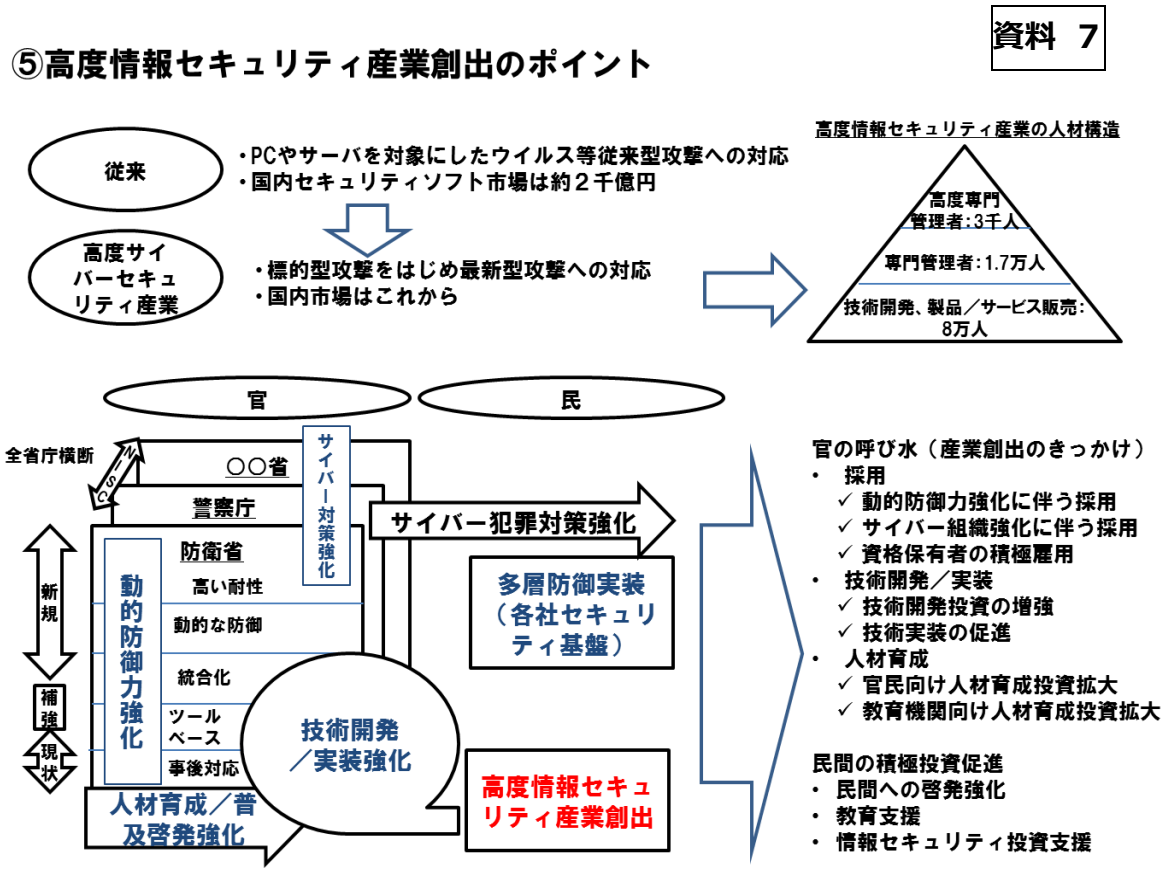
（6）経営者層の意識改革

◇　情報セキュリティ対策は、経営の根幹にかかわる重要な問題であるが、経営層マターではないという認識が大半である。情報セキュリティ対策の重要性、情報セキュリティ人材の育成・確保の重要性等について、政府関係機関から経営者層へ直接訴えかけるなどにより、経営者層の意識改革を促すこと。

６．高度情報セキュリティ産業の創出

国家安全保障の強化を経済成長に結びつけるため、以上の政策を強力に推進して、世界最高水準の高度な情報セキュリティ産業を創出する。（資料７「⑤高度情報セキュティ産業創出のポイント」参照）

資料 7



◇　世界最高水準の情報セキュリティ産業を育成し、起業の促進と新たに 10 万人の雇用を創出すること。

◇　新たな情報セキュリティ技術の開発促進及び国家安全保障等の観点から、政府は国産の新技術を率先して導入すること。併せて日本のベンチャー企業からも積極的に調達すること。

◇　各府省庁等は調達段階において調達品の安全性を確認する仕組みを構築すること。

◇　各省庁等から送信される電子メール等には全て電子署名を導入し、安全性の確保と電子署名事業の普及・拡大を図ること。

◇　各府省庁等は、情報セキュリティに配慮した調達を行うため、情報セキュリティに配慮した調達計画を作成すること。調達の制度化は別途実施すること。

◇　内閣官房は、各府省庁等の情報システム関連予算について情報セキュリティに配慮された要求及び執行となっているか監視すること。このため、情報セキュリティセンターの増員と専門チームの設置を行うこと。

◇　防衛産業や政府の重要な情報を扱う企業等においては、国の情報セキュリティ対策と同程度の対策が講じられるよう、契約段階から必要な情報セキュリティ特約等を課すこと。調達時の情報セキュリティの法制化を別途検討すること。

◇　標的型攻撃（不審）メールに対する訓練等様々なセキュリティ対策訓練を積極的に実施し、それを提供する事業の育成・発展を支援すること。

◇　グローバル市場の獲得に向け、日本発の国際標準を大幅に拡大すること。そのための予算、要員を確保すること。

◇　スマートフォンのセキュリティ確保に関するガイドラインを策定すること。

◇　クラウドコンピューティングのセキュリティ確保に関するガイドラインを策定すること。

◇　情報セキュリティ対策を実効あるものとするため、クラウド事業者等の情報サービス企業においては情報セキュリティに関する資格保有者を必ず置くことの義務化を検討すること。

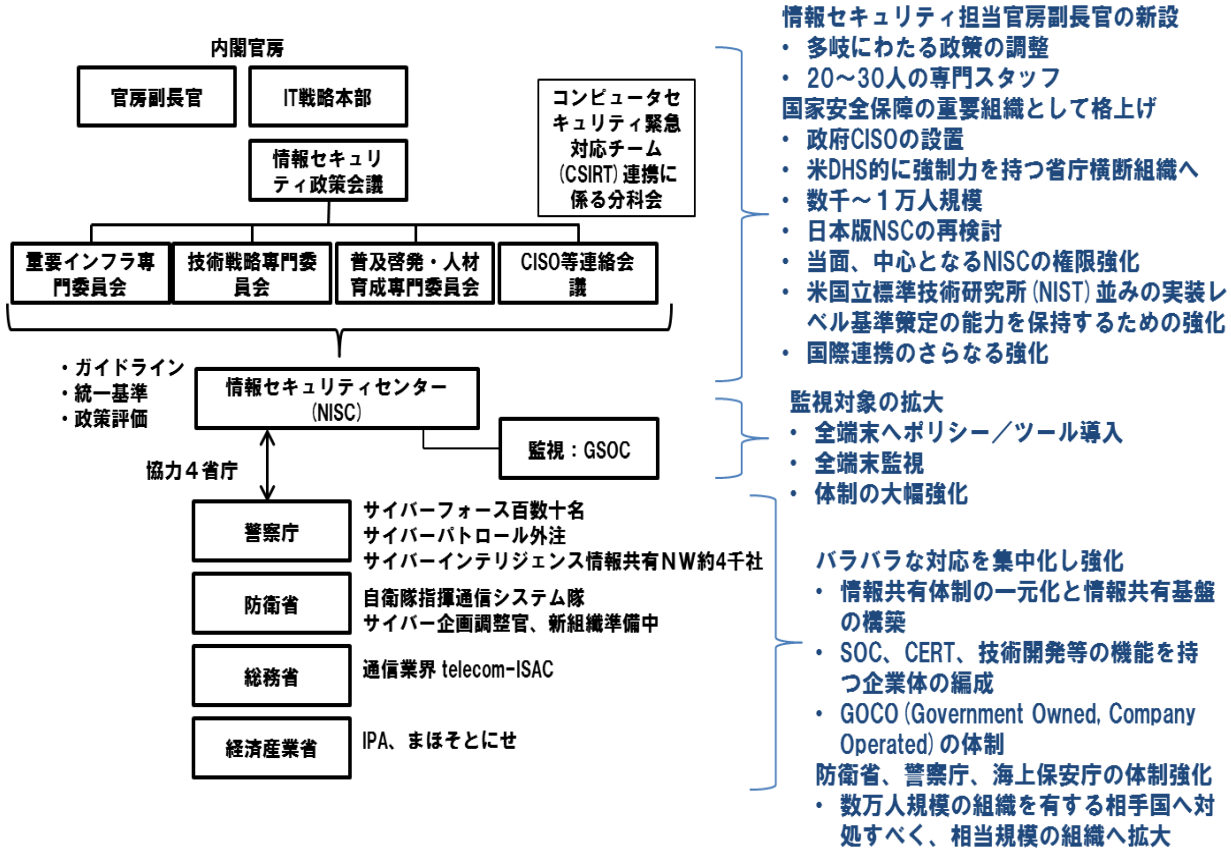
◇　情報セキュリティ投資を促進するため、情報セキュリティ投資に対する減税・免税の措置を抜本的に拡充すること。

７．政府機関等の強化、組織整備

政策を実現するにあたり、政府の関連機関を大幅に強化、整備する。（資料８「⑥組織整備のポイント」参照）

資料 8

⑥組織整備のポイント



（１）情報セキュリティ政策調整役としての官房副長官機能の新設

◇　国家安全保障、産業政策、外交等多岐にわたる情報セキュリティに関する政策を関連省庁間で調整する政策調整役としての官房副長官（政務）を新設すること。

◇　当該官房副長官には、20～30 名の専門スタッフを付すること。

（２）政府 CISO 等

◇　政府として情報を集約し、一元的に対処するため、政府 CISO (Chief Information Security Officer)を新たに設置すること。

◇　政府部内で攻撃発覚後に迅速かつ適切な対応を講じるため、政府部内の情報セキュリティ専門家、情報セキュリティ担当者を組織化し、組織的な「新しい官民連携モデル」の確立を目指すこと。

（3）内閣官房情報セキュリティ関係機関の機能強化

◇　サイバー攻撃に対し確実かつ速やかな対応を可能とするため、内閣官房の組織を強化すること。
◇　将来的には、米国土安全保障省のような組織横断で強制力のある組織をめざし、来年度からその検討を開始すること。

（4）政府の情報システムに係るセキュリティの抜本的強化

◇　現在、各府省庁が独自に構築し、調達しているインターネットへの接続環境を抜本的に見直し、接続点を少数のゲートウェイに絞り込み、緊急時（有事）の代替ネットワーク環境を整備する等セキュリティの強化を図ること。
◇　政府機関情報システムの 24 時間監視を行っている GSOC について、新たな脅威に対応するため、機能を大幅に拡充するとともに、監視対象を「go ドメイン」全体にまで拡大すること。
◇　特に、政府管轄下の全ての情報機器（端末、サーバ、複合機等）を GSOC と連携した個別省庁の SOC にて監視できる体制を再来年度までに構築すること。その際、個別省庁の SOC が現実的に構築できない場合は GSOC の監視下におくこと。そのため、GSOC の予算と要員を大幅に増強すること。

（5）国家公務員試験の改革

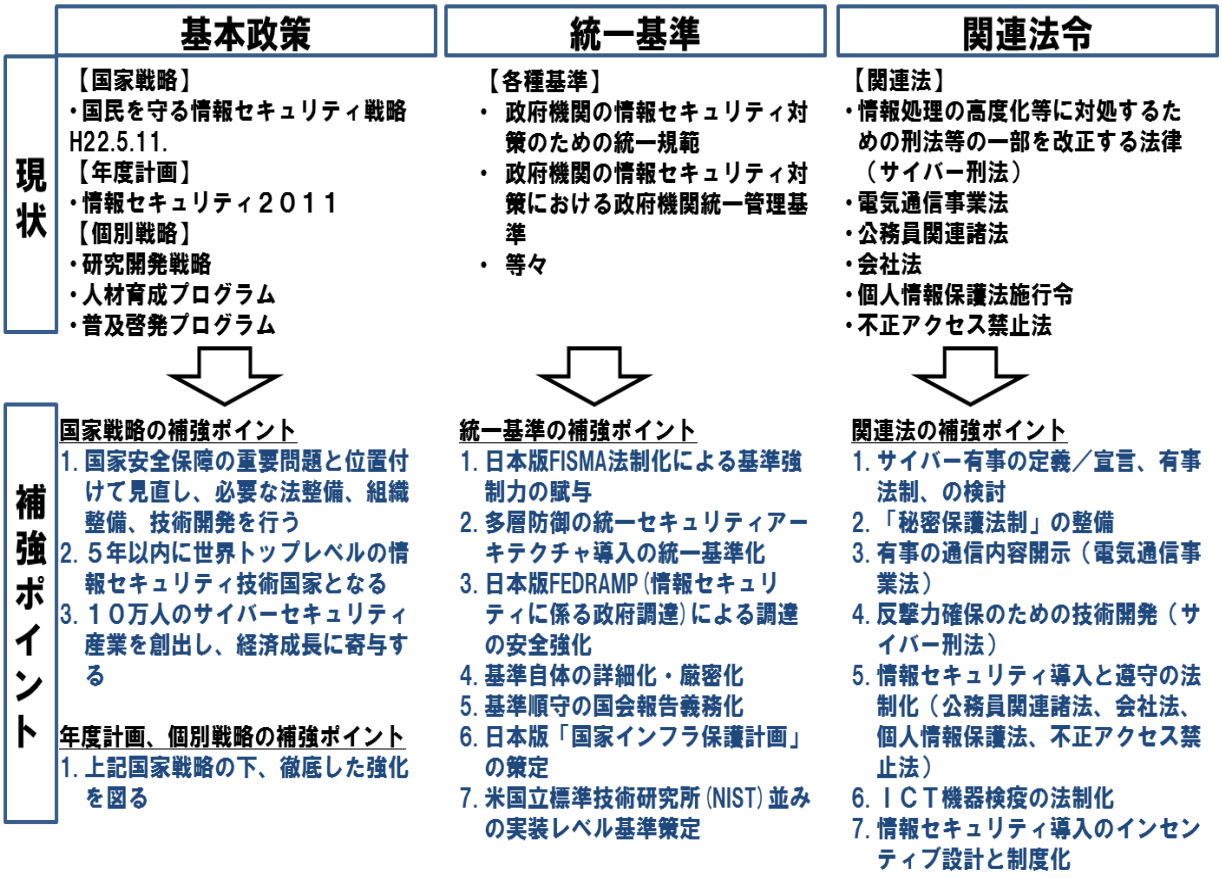
◇　国家公務員試験において情報セキュリティに関する問題を出題し、情報セキュリティに関する知見を備えている者を採用すること。

８．法整備とガイドラインの整備

政策を実現するにあたり、必要な法整備やガイドラインの整備を行う。（資料９「⑦法整備のポイント」参照）

資料 9

⑦法整備のポイント



9

（１）有事法制の補強

◇　国家機関及び、軍事関連企業に対するサイバー攻撃に関して、「有事」である事の定義を行うこと。既に米国は、平成２３年に第５の戦場と定義している。

（２）秘密保護法制の整備

◇　政府が持つ情報（文書とデジタル情報の全て）を厳格にクラス分けし、適正に運用するための「秘密保護法制」を整備すること。

◇　将来的には、この「秘密保護法制」を基に情報セキュリティに関する技術開発や調達を行うべく関連法制、ガイドラインを整備すること

（３）国家戦略の補強修正

◇　平成２２年閣議決定された「国民を守る情報セキュリティ戦略」に関して平成２３年に発覚した足下の状況を考慮して新たに次の３点を補強すること。
・情報セキュリティを国家安全保障上の重要問題として明確に位置づけること。
・２０２０年までに世界最高水準の情報セキュリティ技術保有国となるという目標を今後５年以内と前倒しすること
・情報セキュリティを経済成長に結びつけるために、高度情報セキュリティ産業を創出して１０万人の新規雇用増を目標とすること。

◇　毎年度の年度計画策定に際しては、上記を考慮した現実的な計画とすること。

（４）政府統一基準の補強

◇　内閣官房情報セキュリティセンター（NISC）のガイドライン遵守を個別省庁の自主性に委ねるのではなく、米国連邦情報セキュリティマネジメント法（FISMA）のように強制力を持たせる法整備を行うこと。

◇　政府調達に際しての統一的な情報セキュリティのガイドラインを強化し、その遵守に強制力を持たせるべく法制化すること。

◇　NISC の各種ガイドラインを遵守しているかどうかについて毎年国会での報告義務をもたせること。

◇　現在 NISC がコーディネートしている重要インフラ防護をより強化するために必要な、日本版の「国家インフラ保護計画」を策定し、関係省庁や、産業界の関与に強制力を持たせる法整備をおこなうこと。

◇　NISC の制定する各種基準／ガイドラインをより、高度化、精緻化し、米国立標準技術研究所のようなレベルに達するために、NISC の増強、必要な標準技術機関の創設を検討すること。

（５）関係機関の増強に関する法整備

◇　NISC、防衛省、警察庁、海上保安庁など特別に情報セキュリティ施策を強化する機関に対して、その組織整備や予算獲得が優先的に行われるべく必要な法整備を検討すること

（６）情報窃盗罪（仮称）の創設

◇　いわゆる情報横領、情報窃盗に関する処罰のあり方について、政府全体としての論点の整理・検討を行うこと。

（7）情報セキュリティ導入と遵守の法制化

◇　情報セキュリティ導入とその遵守に関して、公務員関連諸法、会社法、個人情報保護法、不正アクセス禁止法などの全般でどのように法制化すべきかを検討すること。

（8）通信事業者における情報セキュリティ対策

◇　不正な通信である蓋然性が高い場合、通信事業者から利用者に対して不正な通信である蓋然性が高いことを注意喚起できるよう、所要の規則・ガイドラインを策定すること。

◇　不正な通信が実施された蓋然性が高い場合、国の行政機関が通信事業者に対して通信内容の開示を請求できるよう、所要の規則・ガイドラインを策定すること。

（9）インターネットサービスプロバイダにおける情報セキュリティ対策

◇　インターネット利用者の身近な存在であるインターネットサービスプロバイダからその利用者に対し、情報セキュリティ対策の必要性及び対策の実施を定期的に呼びかけるよう、所要の規則・ガイドラインを策定すること。

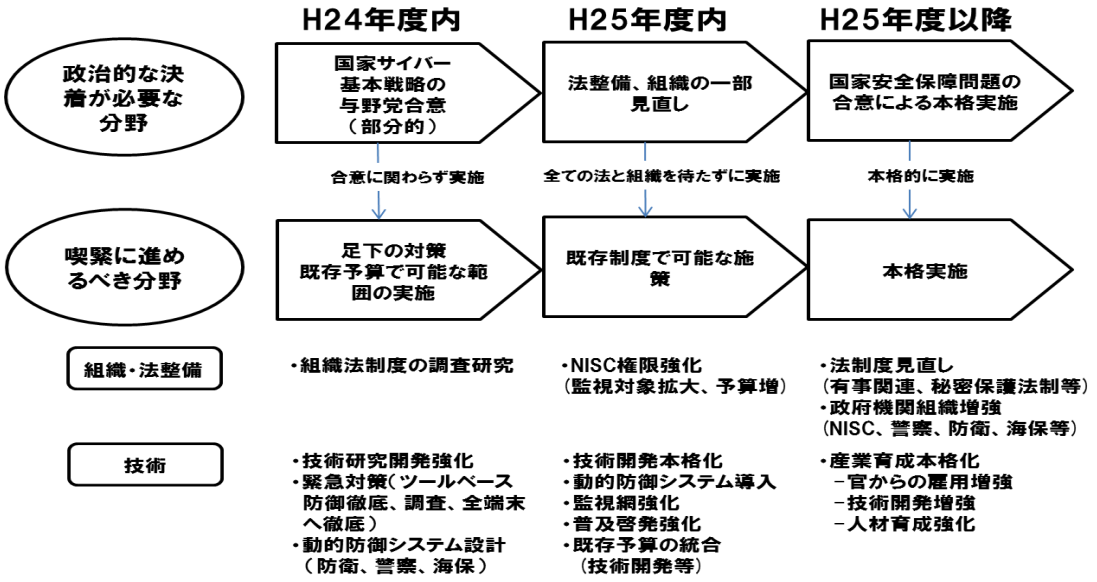
◇　インターネットサービスプロバイダがその利用者に対し、標的型攻撃（不審）メールに関する訓練を適切に実施するよう所要の規則・ガイドラインを策定すること。

◇　インターネットサービスプロバイダの情報セキュリティサービスの強化を図るため、所要の規則・ガイドラインを策定すること。併せて、高度情報セキュリティ認定サービスプロバイダ等の指定を検討すること。

９．政策実現に向けての工程

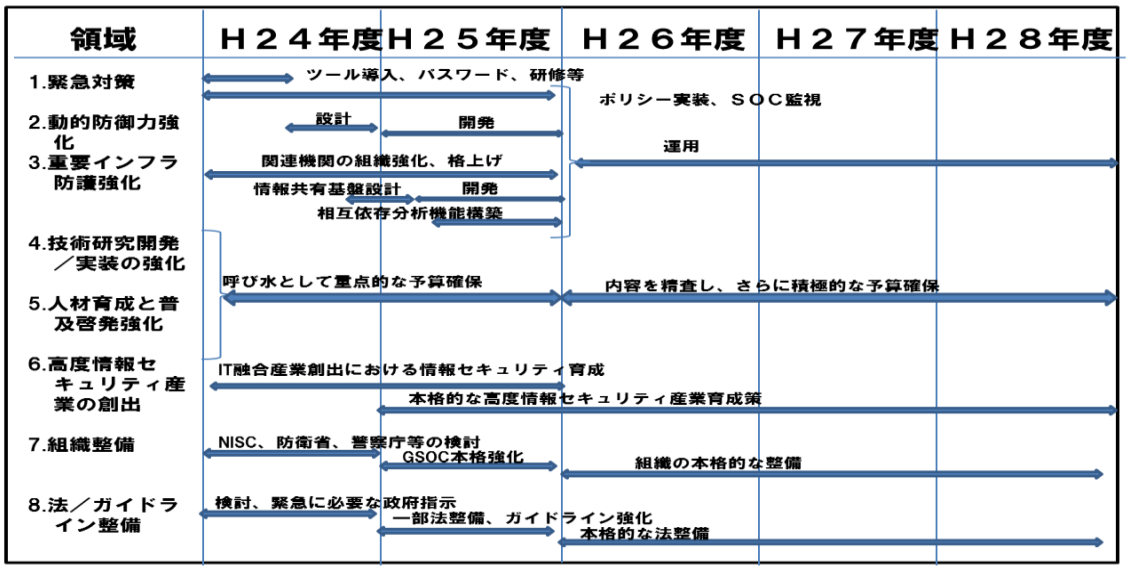
政策実現のための工程は平成２４年度、２５年度を組織や法整備を本格展開するための準備期間として、研究開発や動的防御力強化など既存制度で可能な部分から着手する。法整備を待たなければならない政策については平成２５年度以降に本格実施を目指す。（資料１０「実現に向けた流れ」、資料１１「情報セキュリティ政策工程表」参照）

実現に向けた流れ　　**資料　１０**



10

情報セキュリティ政策工程表　　**資料　１１**



11

◇　緊急対策の予算を平成２４年度で確保すること。

◇　情報セキュリティ研究開発の推進に直ちに着手し、研究開発の推進を呼び水として、情報セキュリティ人材育成及び情報セキュリティ産業の活性化を推進すること。

◇　このため平成２４年度及び平成２５年度の予算において、情報セキュリティ研究開発関連予算を重点的に確保すること。

◇　動的防御強化に関しては、対象省庁の既存情報セキュリティ対策予算を融通または、増額して平成２４年度に設計に着手すること。

◇　重要インフラ防護に関しては、平成２４年度は組織強化等の検討を行い、遅くとも平成２５年度から本格的に情報共有基盤と相互依存分析機能を構築すること。

◇　高度情報セキュリティ産業創出については、平成２４年度はＩＴ融合産業創出の中での重要ファクターとして取り組み、平成２５年度以降本格的な産業育成策を実施すること。

◇　内閣官房情報セキュリティセンター（ＮＩＳＣ）によるＧＳＯＣの監視対象拡大とそのための増員は、平成２５年度から本格的に着手すること。

◇　ＮＩＳＣ、防衛省、警察庁、海上保安庁の情報セキュリティ機能強化に必要な組織整備は、平成２４年度から着手し、平成２５年度以降本格化させること。

◇　必要な法やガイドラインの整備／強化は平成２４年度から検討を開始し、平成２５年度以降順次実現すること。

１０．予算関連

情報セキュリティに関してはこれまで国家的な危機感が薄く、その予算措置も各省庁で数億円から数十億円程度であった。今回の申し入れは、これを国家安全保障上の重要問題と位置付けるため、一気に全体で１～２千億円規模まで増額すべきことを提言する。これは防衛予算の一部と考えれば、妥当なレベルと思われる。

予算措置案（1）

資料 １２

		年度					単位:億円
所管	項目	2012	2013	2014	2015	2016	備考
NISC主導（全省庁）	全省庁セキュリティポリシー実装	100	100	10	10	10	端末30万台、全サーバ、通信機器にセキュリティポリシーを実装し、セキュアで監視可能な状況の設計と構築。既存の各省庁情報セキュリティ予算を活用し、必要に応じて増額。40万台×5万円、その後運用経費
	全省庁セキュリティツール実装	30	30	3	3	3	端末30万台、全サーバ、通信機器にエンドポイントセキュリティ・検疫・暗号化等を施す費用。既存の各省庁情報セキュリティ予算を活用し、必要に応じて増額。エンドポイントセキュリティ:5、エンドポイント検疫:5、エンドポイント暗号化:15、情報漏洩検出:15、情報漏洩遮断:15、諸経費:5
	GSOCの全省庁端末監視		100	100	100	100	全端末／サーバを対象に、リアルタイム監視。警察庁、防衛省には個別SOCを構築し、GSOCと連動して運用。
	全省庁文書コンテンツ保護	20	20	2	2	2	文書等コンテンツのセキュリティシステム導入。既存の情報セキュリティ予算を活用し、必要に応じて増額。
	全省庁重要データベース保護		50	50	10	10	統合IDレポジトリシステム導入、DBファイアウォール、DB権限分離、暗号化、統合ログ監視システム導入
	全省庁複合機対策	50	25	10	10	10	全省庁の複合機4千台を想定。調査分析・設定:1、機器入替2千台×2百万円:40、ログサーバ等管理機器導入運用:2、教育:4、諸経費:3、構築後運用
	サイバー攻撃対策演習強化	5	10	10	10	10	全端末／サーバを対象に定期的にサイバー攻撃に対する演習を実施
	技術開発及びサイバーセキュリティ産業創出	1000					産官学情報セキュリティ研究開発拠点整備及び、高度情報セキュリティ産業創出。1000億円の取り崩し型基金
	官向けセキュリティ技術開発	50	100	100	100	100	国家機関を最高度のセキュリティで守るための集中的な技術開発。例. 動的防御に必要な要素技術、IPv6アドレス管理技術、ICT検疫気機器技術等々。上記基金活用を検討。
	官の高度人材育成	5	5	5	5	5	動的防御を運用できる官の人材育成。高度専門管理者5百人、専門管理者2千人、高度知識保有者1万人を5年間で育成
	公的資格制度制定	5	5	5	5	5	米国防総省の資格制度(8570指令)を想定し新たな国家セキュリティ資格制度を制定し、運用
	公的資格専門教育補助		5	5	5	5	公的資格の専門教育を民間に拡大するための補助。民間人材を官で積極採用。
	国際連携のさらなる強化	5	5	5	5	5	サイバーセキュリティの国際連携をさらに強化

12

資料 １３

予算措置案（２）

		年度					単位:億円
所管	項目	2012	2013	2014	2015	2016	備考
NISC主導（CIP関連省庁）	官・民間の啓発強化	5	5	5	5	5	情報セキュリティ及び重要インフラ防護(CIP)に関する普及・啓発活動の強化
	CIP情報共有基盤の構築	5	50	10	10	10	重要インフラ防護(CIP)各セプター間での情報一元管理・共有基盤の設計・開発・運用
	CIP国家COP構築		50	10	10	10	CIPの運用に必要なCOP(Common Operation Picture)の構築、統合災害対策システムとして運用
	CIP相互依存分析機能構築		10	5	5	5	重要インフラの相互依存関係を分析し、災害に際してリアルタイムに分析、指令をできる機能の構築
衆参両院	ツールベース防護強化	5	5	1	1	1	高強度認証、メールフィルタリング、エンドポイント管理、ログ管理、侵入防御システム等のツール実装と運用
防衛省	統合セキュリティシステム導入	30	300	100	100	100	米国防総省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用。有事を想定したバックアップシステムの構築・運用。
	サイバー防衛組織の増強	50	300	300	300	300	数千人規模の組織増強
	国際連携のさらなる強化	5	5	5	5	5	同盟国との国際連携のさらなる強化
警察庁	統合セキュリティシステム導入	20	300	100	100	100	米国防総省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用。有事を想定したバックアップシステムの構築・運用。有事を想定したバックアップシステムの構築・運用。
	サイバー犯罪対策組織の増強	50	300	300	300	300	数千人規模の組織増強
	国際連携のさらなる強化	5	5	5	5	5	サイバー犯罪に関する国際連携のさらなる強化
海上保安庁	統合セキュリティシステム導入	5	10	10	5	5	米国防総省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用
経産省	IT融合産業における情報セキュリティ強化予算	50	100				動的防御を可能とする既存技術の高度化、各種ハード機器との融合技術、IT融合産業における高度セキュリティ技術開発等(IT融合産業創出予算内)
	高度情報セキュリティ産業育成		100	200	200	200	
	高度セキュリティ人材育成	25	25	25	25	25	高度専門管理者3千人、専門管理者1.5万人を5年間で追加育成
文科省	セキュリティ人材育成補助	10	10	10	10	10	教育機関で高度セキュリティ知識保有者7万人を5年間で追加育成
	セキュリティ教育設備投資補助	10	10	10	10	10	人材育成に必要な設備投資の補助
総務省	全国自治体セキュリティ実装補助			300	300	300	全国の自治体中央官庁に準ずるツール導入・運用のための補助
	セキュリティ技術開発	100	100	100	100	100	動的防御を可能とする通信技術(プロトコル、機器等)の開発
	年度合計	1645	2140	1801	1756	1756	

13

◇　政策実現のための予算措置としては、平成２４年度に１６４５億円程度を見込むがこの内１０００億円は技術開発（及び産業創出）のための取り崩し型基金であり、他の技術開発関連予算はこの取り崩しが可能となる。

◇　また、平成２４年度の技術開発と動的防御強化を除く多くの項目は既に概算要求されている各省庁の予算項目をやりくりする形で実現可能な範囲と思われる。

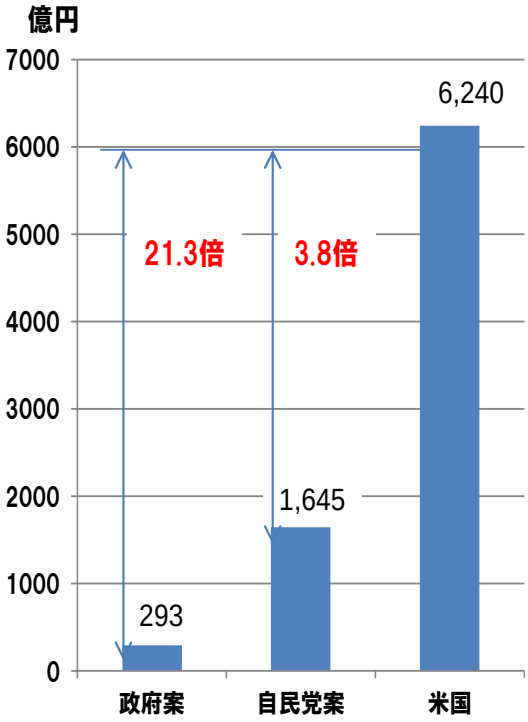
◇　動的防御強化に関しては、対象省庁の既存情報セキュリティ対策予算を融通または、増額して、平成２４年度に設計に着手すること（再掲）

◇　国家安全保障の強化と経済成長を共に実現するために平成２５年度以降に毎年度２０００億円前後の積極的な予算計上を行う。
（資料１２、資料１３「予算措置案」参照）

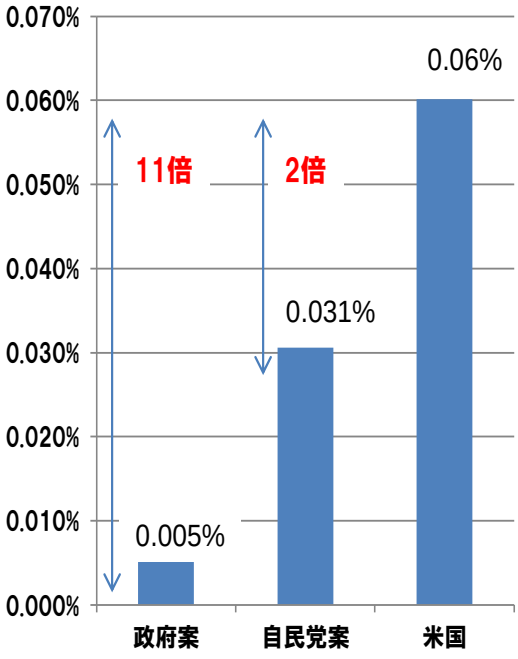
平成２４年度情報セキュリティ関連予算(想定値)比較

米国と比較して日本は比較にならない程の低さ。自民党案は逼迫する財政事情を考慮し、また本格的な積極投資の初年度としてGDP比で米国の半分程度からスタート。

平成24年度
情報セキュリティ関連予算
総額(想定値)比較



平成24年度
情報セキュリティ関連予算
総額GDP比率(想定値)比較



注:

- **為替レートは1ドル=78円と想定**
- **GDPはIMFの2011年予測値ベース**
- **政府案、米国の総額想定は次頁**

日米の平成２４年度情報セキュリティ関連予算(想定値)

政府案の平成２４年度情報セキュリティ関連予算概要予測

項目		億円
情報セキュリティ重点関連予算*1	大規模サイバー攻撃事態への対処体制の整備等	4.9
	GSOCの運用	6.5
	国民生活を守る情報セキュリティの強化	66.9
	国民・利用者保護の強化	1.7
	国際連携の強化	0.5
	技術戦略の推進(人材育成)	0.1
	情報セキュリティに関する制度整備	0.1
	災害時に強靭な情報通信システムの構築	0.4
	「ニューディペンダビリティ」の確保	3.2
情報セキュリティ研究開発投資*2		48.6
防衛省、情報セキュリティ基盤強化*3		60.0
その他(サイバーフォース、関連技術開発等の推定)		100.0
	合計	292.8

*1 出所:NISC集計

*2 2010年度予算、出所:2011年度情報セキュリティ研究開発戦略

*3 出所:防衛省概算要求資料

2012年度　米国情報セキュリティ関連予算概要 予測

省	項目	億ドル
DHS*1	政府NW防御	2.34
	情報セキュリティ・アセスメント	0.41
	人材育成	0.25
	各省連携(DHS,DOD,NSA)	0.01
	情報セキュリティ研究開発投資	2.31
DOD	情報セキュリティ(全IT予算366の8%*2と想定)	29.28
	サイバー軍(サイバー・コマンド) *3	32.00
	ナショナル・サイバー・レンジ*4	5.00
DOJ/FBI	情報セキュリティ(全IT予算30の8%*2と想定)	2.40
その他		6.00
	合計*5	80.00

*1 出所:DHS2012予算要求

*2 出所:IDC Government Insights report

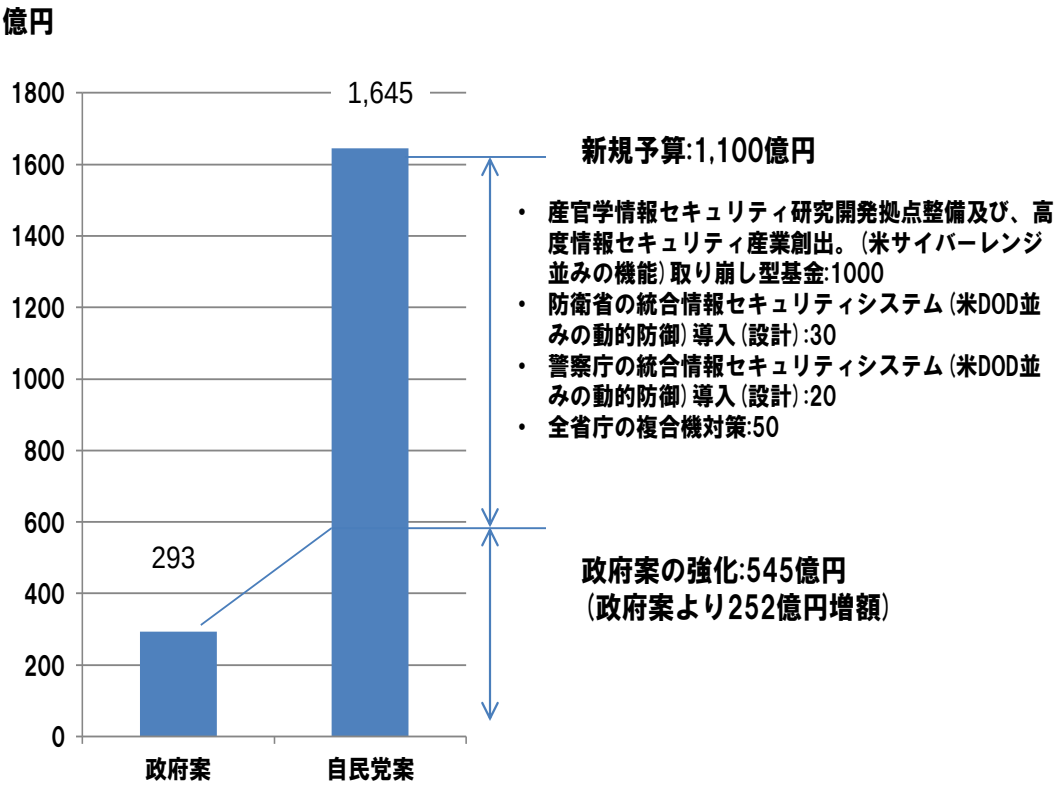
*3 出所:JETRO/IPAニューヨークだより

*4 2011年度と同額と想定

*5 出所:マカフィ社

平成24年度情報セキュリティ関連予算
政府案と自民党案の比較

自民党案は政府案を大幅に増強するとともに、米国のレベルに追い付くためのスタートとしての新規予算を提案。



平成 24 年度情報セキュリティ関連予算

自民党案:政府案への新規予算

所管	項目	億円	備考
NISC主導 （全省庁）	全省庁複合機対策	50	全省庁の複合機4千台を想定。 調査分析・設定：1 機器入替2千×2百万円：40 ログサーバ等管理機器導入運用：2 教育：4 諸経費：3 構築後運用
	技術開発及びサイバーセキュリティ産業創出	1000	産官学情報セキュリティ研究開発拠点整備及び、高度情報セキュリティ産業創出。 1000億円の取り崩し型基金
防衛省	統合セキュリティシステム導入	30	米国防省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用。 有事を想定したバックアップシステムの構築・運用。
警察庁	総合セキュリティシステム導入	20	米国防省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用。 有事を想定したバックアップシステムの構築・運用。
	新規合計	1100	

平成24年度情報セキュリティ関連予算
自民党案：政府案の増強項目

所管	項目	億円	備考
NISC主導（全省庁）	全省庁セキュリティポリシー実装	100	端末30万台、全サーバ、通信機器にセキュリティポリシーを実装し、セキュアで監視可能な状況の設計と構築。既存の各省庁情報セキュリティ予算を活用し、必要に応じて増額。40万台×5万円、その後運用経費
	全省庁セキュリティツール実装	30	端末30万台、全サーバ、通信機器にエンドポイントセキュリティ・検疫・暗号化等を施す費用。既存の各省庁情報セキュリティ予算を活用し、必要に応じて増額。エンドポイントセキュリティ:5、エンドポイント検疫:5、エンドポイント暗号化:15、情報漏洩検出:15、情報漏洩遮断:15、諸経費:5
	全省庁文書コンテンツ保護	20	文書等コンテンツのセキュリティシステム導入。既存の情報セキュリティ予算を活用し、必要に応じて増額。
	サイバー攻撃対策演習強化	5	全端末／サーバを対象に定期的にサイバー攻撃に対する演習を実施
	官向けセキュリティ技術開発	50	国家機関を最高度のセキュリティで守るための集中的な技術開発。例. 動的防御に必要な要素技術、IPv6アドレス管理技術、ICT検疫気機器技術等々。上記基金活用を検討。
	官の高度人材育成	5	動的防御を運用できる官の人材育成。高度専門管理者5百人、専門管理者2千人、高度知識保有者1万人を5年間で育成
	公的資格制度制定	5	米国防総省の資格制度（8570指令）を想定し新たな国家セキュリティ資格制度を制定し、運用
	公的資格専門教育補助		公的資格の専門教育を民間に拡大するための補助。民間人材を官で積極採用。
	国際連携のさらなる強化	5	サイバーセキュリティの国際連携をさらに強化
NISC主導（CIP関連省庁）	官・民間の啓発強化	5	情報セキュリティ及び重要インフラ防護（CIP）に関する普及・啓発活動の強化
	CIP情報共有基盤の構築	5	重要インフラ防護（CIP）各セプター間での情報一元管理・共有基盤の設計・開発・運用
衆参両院	ツールベース防護強化	5	高強度認証、メールフィルタリング、エンドポイント管理、ログ管理、侵入防御システム等のツール実装と運用
防衛省	サイバー防衛組織の増強	50	数千人規模の組織増強
	国際連携のさらなる強化	5	同盟国との国際連携のさらなる強化
警察庁	サイバー犯罪対策組織の増強	50	数千人規模の組織増強
	国際連携のさらなる強化	5	サイバー犯罪に関する国際連携のさらなる強化
海上保安庁	統合セキュリティシステム導入	5	米国防総省並みの動的防御を可能とする統一されたセキュリティシステムの設計・開発・運用
経産省	IT融合産業における情報セキュリティ強化予算	50	動的防御を可能とする既存技術の高度化、各種ハード機器との融合技術、IT融合産業における高度セキュリティ技術開発等（IT融合産業創出予算内）
	高度セキュリティ人材育成	25	高度専門管理者3千人、専門管理者1.5万人を5年間で追加育成
文科省	セキュリティ人材育成補助	10	教育機関で高度セキュリティ知識保有者7万人を5年間で追加育成
	セキュリティ教育設備投資補助	10	人材育成に必要な設備投資の補助
総務省	セキュリティ技術開発	100	動的防御を可能とする通信技術（プロトコル、機器等）の開発
強化合計		545	