平成 23 年 10 月 28 日

自由民主党　政務調査会
IT 戦略特別委員会

情報セキュリティ対策に関する申入れ

1. 今般の衆議院システムにおける ID、パスワードの漏えいを教訓として、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なうこと。
   －システムに接続されているすべての端末におけるウィルスチェックを直ちに行なうこと。
   －システムに接続されているすべての端末におけるウィルス対策ソフトの導入状況、更新状況を確認し、最新のウィルスパターンファイル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すべての端末における 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変更を義務付け、一定期間にわたって変更されてい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認すること。
   －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緊急に実施すること。

2. 政府は、国家としての安全保障、外交、国民の安心・安全の観点から現在の方針を見直し、至急「国家セキュリティ基本戦略(仮称)」の形で再構築して、2012 年 3 月を目途に国民に公表すること。

3. 政府は、「国家セキュリティ基本戦略(仮称)」の検討に際し、米国国土安全保障省を参考に省庁横断で強力な権限を持つ組織(例えば、NSC 又は国家セキュリティ庁)の早期創設を目指し、重要インフラ防護の体制を強化すること。

4. 内閣官房情報セキュリティセンターは、総務省、経産省、警察庁等と協働し、現在の官民における情報システムを対象として、情報セキュリティの観点からのリスク評価、サイバー空間の内外情勢分析、有効な対策について 2011 年末を目処に早急にとりまとめ、政府機関、地方自治体、重要インフラ企業、その他防衛調達等の政府との契約関係を持つ企業に提供すること。

5. 防衛省は、2011 年末を目処に、防衛調達に関わる企業等における情報管理、保秘管理について実効的な対策を実施すること。さらに対策の実施状況を検証し、改善を促す枠組みを、2012 年 3 月末を目処に防衛調達に関係する企業と協力して創設・運用すること。

6. 警察庁は、ハイテク犯罪、サイバー犯罪の拡大防止、抑止を実現するために、捜査能力の向上と国際捜査態勢の整備を進めること。ただし、わが国の経済状況が厳しい環境であることから、徒に民間組織の負担を増やすような協力要請や情報提供要請は厳に慎むべき。また、サイバー犯罪者・集団を迅速に把握・捕捉できる世界最先端の技術開発を来年度予算から実施し、同時に必要な体制整備を開始すること。

7. 防衛省、警察庁、海上保安庁は、米国国防総省の統合的なセキュリティ・アーキテクチャーを参考に、来年度予算から統合アーキテクチャーの導入と運用体制の整備及び内部統制の仕組みの実現を開始すること。

8. 政府は、2012 年 3 月末を目処に、重要インフラにおけるサイバー攻撃の可能性を評価・検証すること。さらに、2012 年 6 月末を目処に、重要インフラ防衛のためのアクションプランを立案し、直ちに実施すること。

9. 政府は、国会に対して、サイバー空間におけるリスク分析、内外情勢分析、諸外国の政策動向を定期的（半年に 1 回）に報告すること。

10. 政府は、現在不定期開催となっている情報セキュリティ政策会議を 3 ヶ月毎に定期開催し、対策の適時適正性を管理し、また、状況認識の共有、状況に応じた適切な政策を実施すること。会議が取り扱う政策については、経済政策と安全保障政策の両方を含むこと。

11. 政府は、重要インフラ事業者間でのリスク情報、対策情報の円滑な流通を実現するために、平成 24 年度から既存の情報収集分析共有機能（各重要インフラ事業分野における CEPTOAR や JPCERT/CC 等の CSIRT）の強化を行い、さらに制御システムセキュリティに代表される新たなリスクに対応するための施策の前倒し実施を行うこと。

12. 民間における情報セキュリティ対策の強化を実現するために、政府は情報セキュリティ関連の技術開発投資の強化、情報セキュリティ関連産業の育成、さらに、情報セキュリティ対策に資する人材育成の強化策（奨学金の創設等を含む）を立案し、平成 24 年度中に政策実施に着手すること。

13. 日本国内にはグローバルな IT 企業が多数存在し、専門的な人材と技術・ソリューションが民間に存在することから、政府は一連のセキュリティ対策、重要インフラ防護対策の推進に際して、官の中で閉じることなく、積極的に民間のノウハウと活力を取り入れ、オールジャパン体制で推進する事を強化すること。

14. サイバー攻撃のような国境を越えた犯罪に対処するため、政府はサイバー対策及び重要インフラ防護に関して、国際的な連携をより一層強化すること。

15. セキュリティは最も弱いところから破られるため、サイバーセキュリティの強化のためには省庁個別の対応ではなく、横断的、統合的なガバナンスが求められる。このため政府は、政府 CIO、CTO、CSO（チーフ・セキュリティ・オフィサー）を設置し、セキュリティリスクに対応する政府の責任の所在を明確にすること。

16. 国民が安全・安心に IT のメリットを享受することができる高度情報通信ネットワーク社会の実現を目標に、政府は 2012 年 3 月を目処に新たな IT 政策の方針を策定し、強力な IT 政策を実施すること。特に、セキュリティが課題となって IT 化が遅れていた医療、介護、労働、雇用、教育、電子政府について、従来の政策を見直し、抜本的な政策を構成すること。また、IT 化の推進による社会全体でのコスト削減を政策評価指標とし、わが国が真に強い IT 先進国になるための政策を実施すること。