資料10

2007 年 12 月 12 日
富士通株式会社
黒川 博昭

第 15 回情報セキュリティ政策会議への意見書

情報セキュリティは政府機関・重要インフラ・企業といった主体に関係なく大変重要であり、共通的な要素も多く、民間で取り組んでいる内容もふまえ、以下にコメントさせて頂きます。

1．政府機関の情報セキュリティ対策について

今回報告された電子メールサーバの重点検査は、大変良い取り組みであると思います。その対応策について各府省庁より報告されていますが、情報漏えいのリスクの低減とサーバの管理コストの低減の観点からサーバ集約を進めるべきであると思います。

① 全府省庁のサーバ台数は約 1900 台ですが、府省庁システムのユーザ数に対し多いと思われます。IT の進展・メール利用の拡大によって、台数が増えたのだと想定されます。IT 技術・(組織・人を含めた)システムの運用環境等は時間と共に必ず変化します。したがって、適切なタイミングで政府の全体最適の観点から見直し改善すべきです。

② メールサーバ群は各府省庁内外のネットワークで繋がっていると思います。その際、1台でもセキュリティ対策に不備があると、そのサーバが踏み台となり他サーバに影響を及ぼし、情報漏えいやシステムダウン等様々なリスクが顕在化します。管理台数が多いと当然のごとく管理する人の数もコストも増えます。メールサーバのリスクの低減と管理工数・コストの低減の観点からサーバ集約を進めるべきであると思います。

2．セキュリティ・バイ・デザイン[SBD]の取り組みについて

情報システムの開発にあたっては、システムで実現したい事(要件)を定義しなければ正しいシステムの設計・開発はできません。セキュリティ・バイ・デザインは、情報システムにセキュリティ機能を正しく組み込むためのルールだと考えます。各府省庁がシステムを開発する時、そのデザインルールにしたがって、システムの企画段階から、セキュリティを意識して定義することが求められます。その事により、各府省庁のシステムのセキュリティレベルが均質となり、強化されます。

また、一般に、各府省庁は、発注者として、情報システムで実現したい事を定義して発注する能力と、納入物をきちんと定義と比べて評価する検収能力を備える必要があります。そして、セキュリティ機能については、専門家(第三者)によりチェックを受ける事、もしくは、考慮すべき事項の標準化・共通化を政府として進める事が重要です。このことは、各府省庁のセキュリティの透明性・効率性の観点からも有効です。

更に、セキュリティの確保に向けて、開発から運用段階までを考慮し、以下の点について検討することも期待します。

① 企画・要件定義の段階において、点検リストを作成することは、情報システムの調達仕様を明確にし、(例えば、要件定義の漏れが見つかった際の対応等)下流工程における発注者と開発事業者のそれぞれの責任の明確化のために有効であると考えます。

② 設計開発段階において、開発事業者は情報セキュリティに関する実装を含め固有の開発手順を有していることが普通です。したがって、発注者は固有手順に関して、情報セキュリティ機能の実装を含め、正しいシステム開発が正しい手順で行われているか専門家により確認することも必要です。

③ 運用・保守の段階において、発注者と事業者間で契約を交わし、新たな脅威の発生に対し即時に対応できるように、予算上の仕組みを構築することが必要と考えます。

3. 次期情報セキュリティ基本計画(仮称)検討に向けた取り組みについて

IT は中小企業や個人等国民生活の隅々まで浸透し重要なインフラになっています。IT にはセキュリティ対策が不可欠です。その際、我が国の IT の進展を考えると、情報セキュリティ人材の不足、情報セキュリティ対策費用の増加は必ず起きると思います。特に、中小企業等の IT 活用は、セキュリティについて事業規模にあった費用で保証される必要があります。そのため、SaaS(Software as a Service)などの新しい IT サービスの活用形も検討しておく必要があります。

いずれにしても、高齢化社会の到来等の社会構造の変化や、IT を多用する社会生活、自動車における ITS(Intelligent Transport Systems)の活用等、IT 技術の進展による変化が必ず起きます。同時に、人材資源の限界も意識する必要があります。

したがって、現在、第一次情報セキュリティ基本計画を進めていますが、上記をふまえて、現在のセキュリティリスクやその対策コストと実現性を可視化した上で、今後のわが国の情報セキュリティの全体最適の観点から議論を展開頂きたいと思います。

以上