NISC National Information Security Center

指針の継続的改善について（2010年度分析・検証結果）

２０１１年6月

内閣官房 情報セキュリティセンター（NISC）

１）「指針の継続的改善」の分析・検証におけるアプローチ

○2010年度については、指針本編の改定（５月）、指針対策編の策定（７月）を実施済である。
○今回の分析・検証においては、次の4つのアプローチから検討が必要な課題を抽出し、指針への反映要否を判断した結果、 2010年度内は指針の更なる改定は実施しないこととしたい。

◆分析・検証における４つのアプローチ

①定常的なIT障害等の発生状況の分析：
2010年度に発生したIT障害の事例から、得られた教訓をどのように指針に反映するか。

②関連文書の検証：
情報セキュリティ対策に関連する文書等をどのような観点で指針に盛り込んでいくか。

③社会的条件（環境）の変化の検証：
技術面、経営面、法制面及びその他の社会的動向の観点から重要インフラの情報セキュリティ対策に及ぼす変化に対して、指針ではどのように反映していくか。

④行動計画に基づく施策の成果：
第2次行動計画に基づき、取り組んできた施策の成果をどのように反映するか。

2）「指針の継続的改善」の分析・検証結果

○以下の分析・検証結果より、現段階で、指針の改定が必要な項目はないと判断した。

①定常的なIT障害等の発生状況の分析

（1）ガンブラー

・「Webサイト改ざん」と「Web感染型ウイルス」を組み合わせて、多数のパソコンをウイルスに感染させようとする攻撃手法。2009年12月頃から日本の大手企業のウェブサイトにおいて改ざん被害が拡大している。

（2）Stuxnet

・シーメンス社の制御用アプリケーションWinCC/Step7をターゲットにしたマルウェアで、感染するとPLC（Programmable Logic Controller）制御が書き換えられる。USBメモリ経由でも感染する。現段階では、具体的なシステムへの影響は未判明で、重要インフラへの実害は報告されていない。

＜分析・検証結果＞

- ガンブラーについて、外部のセキュリティ機関の分析によると、手法は新しく、感染も広範囲に渡ったが、既存の情報セキュリティ対策（利用ソフトウェアのアップデート、アンチウイルスソフトウェアの導入、外部ネットワークからのアクセス制限等）を行うことで対応できる。
- Stuxnetについて、外部のセキュリティ機関の分析によると、手法は新しく、複雑であるが、既存の情報セキュリティ対策（制御系ネットワークの分離、媒体の管理、不正アクセスの監視等）を行うことで対応できる。

②関連文書の検証

●以下の文書を検証

・「オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン」（各府省情報化統括責任者(CIO)連絡会議第41回会合決定）

- 左記関連文書の中の「認証方式の保証レベルに係る対策基準」にある対策（ウイルスソフトの導入や通信内容の暗号化等）は、指針の4つの柱「エ　情報システムについての対策」、重点項目「イ　情報漏洩防止のための対策」に明記している。

③社会的条件（環境）の変化の検証

●以下の動向の変化を検証

・IPv4アドレス枯渇（2011/2）　・クラウドコンピューティング

- IPv4アドレス枯渇については、指針の重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に、IPv6への移行を明記している。
- クラウドコンピューティングについては、以下の共通脅威分析の項を参照。

④行動計画に基づく施策の成果

●共通脅威分析は「クラウドコンピューティング」をテーマに分析

●CIIREX2010では、大規模通信障害を想定した演習を実施

- ●クラウドコンピューティングの分析では、運用・管理上の懸念点等はあったが、重要システムとしての導入は現時点で将来課題であり、安全基準等に反映すべき項目はなかった。
- ●演習結果から見出された気付きは、ほとんど運用上の課題であり、安全基準等の見直しを要するものはなかった。