第２回　地方公共団体における情報セキュリティ対策の向上に関する研究会
議事概要

１．開催日時：平成 26 年 12 月 16 日（火）10：30 ～ 12：00

２．開催場所：ＮＥＣ本社ビル　2Ｆ　242 会議室

３．出席者

＜座長＞

佐々木　良一（東京電機大学未来科学部教授）

＜構成員＞

今井　建彦（仙台市まちづくり政策局情報政策部長）
大高　利夫（藤沢市総務部参事兼ＩＴ推進課長）
古保里　学（福岡県企画・地域振興部情報政策課情報企画監）
高橋　邦夫（豊島区政策経営部情報管理課長）

＜オブザーバ＞

石川　家継（地方公共団体情報システム機構情報化戦略部次長）

＜事務局＞

増田　直樹（総務省自治行政局地域情報政策室長）
須藤　正喜（総務省自治行政局地域情報政策室理事官）
大井　芳泰（総務省自治行政局地域情報政策室係長）
日本電気株式会社

４．議題

・情報セキュリティポリシーに関するガイドラインの改定案について
・情報セキュリティ監査ガイドラインの改定案について

《外部委託（クラウドサービス等）について》

○　クラウドサービスについて高度なセキュリティ対策が必要ということであるが、具体例がないため「高度な」という表現のみでは、内部で運用する場合と外部委託しサービスとして利用する場合のリスクの違いがわかりにくい。

○「庁舎外への機器の設置」についてクラウドサービスの「国際的な情報セキュリティの第三者認証」の具体例を追記してほしい。

《外部委託（サプライチェーンリスク等》

○　サプライチェーンの定義が必要。電気・ガス等は含まずソフトウェアの構成要素の中の部分に特化しているのであれば、それを明記すべき。

○　ICT サプライチェーンを構成して提供されるサービス（ASP サービス等）は今後増えてくると思われる。サービスの裏に様々な関係者が関与しており、セキュリティのコントロールが及びにくいため、どのような注意を払い契約をすれば良いかを明記すべき。

《ネットワークの利用》

○　公衆無線ＬＡＮについて公式に設定した通信網以外は原則禁止ということを明記すべきではないか。

○　タブレットから基幹業務にアクセスする仕組みを今後検討している団体についても考慮すべきではないか。

○　基幹系業務すべてを外に持ち出すわけではなく、十分な対策を施し、必要なものだけを限定して持ち出すということが明確にできる書き方ができると良いのではないか。

○　アクセス記録等のログを残し、定期的なモニターや監査をきちんと行うと明記することで、基幹系のネットワークへアクセスする場合に対応する手はある。

《標的型攻撃について》

○　標的型攻撃に関して、メールのセキュリティについても注意事項等明記すべき。
技術的対策の記載だけではなく、人的対策についても記載すべきではないか。

○　メールのセキュリティに関しては、事後対策としてログの確認についても記述が必要である。

《監査手順準備について》

○　セルフチェック、内部監査、外部監査という一連の流れの中で、このガイドラインは

どこで使うか位置づけを記載するとよい。実際に実行に移せるレベルで記載されてあるガイドラインになるとよい。

《フォローアップ監査》

○　現行の監査ガイドラインは、フォローアップ監査に関しての記載が少ない。フォローアップ監査に力を入れることで PDCA が回ると思われる。

《監査の品質について》

○　監査の品質確保について具体的にどのように「良い監査」と評価すればよいか。また、品質の話が出てくる理由として、安かろう悪かろうという監査をしないために、という前提を記載したほうが良い。

○　職員の気づかない事項を指摘してくれる監査等は有効であるため、監査の実績が重要。