平成 27 年度第 1 回仙台市情報化推進会議情報セキュリティ専門委員会　議事録

1　日　時　　平成 27 年 7 月 29 日（水）13:00～14:30

2　会　場　　仙台市役所　本庁舎 2 階　第四委員会室

3　出席者

（1）各委員

林隆史委員長，石井夏生利委員，金谷吉成委員，佐藤昌志委員，舘田あゆみ委員

（2）事務局

大槻まちづくり政策局長，日下情報政策部長，渋谷情報政策課長，桝川文書法制課長，佐藤情報システム課長，久米井セキュリティ対策係長，伊藤主査，佐藤主事，小田嶋主事（記）

4　議事内容等

（1）開会

（2）局長挨拶

近年インターネットを介したサイバー攻撃の脅威が増大している。セキュリティの対応次第では組織そのものが無能集団と言われ，全否定される例を目の当たりにしている。こうした中，マイナンバー法が施行され，来年の 1 月には共通番号の利用が開始される。今後のセキュリティ対策に関しては，これまで過剰と思われていた対策についても，踏み込んでいかなければいけない時期に来ていると考えている。委員の皆様から厳しいご意見を頂戴し反映することで，仙台市が情報化の先進となれるようにしていきたい。

（3）委員長指名報告

仙台市情報化推進会議設置要綱第 7 条第 6 項に基づき，情報化推進会議の曽根座長の指名により林委員が委員長に就任。

（4）委員長挨拶

仙台市のセキュリティ対策については，資料を見る限り高いレベルにあると思う。しかし局長挨拶でのとおり，さらに高みを目指したいとの事なので，この会議を通して役に立てればと思う。

（5）議事

①平成 26 年度仙台市情報セキュリティ対策改善取組結果について（資料 1）

（事務局（渋谷課長）より資料及び以下の補足について説明）

- 情報セキュリティ点検は，平成 25 年度から，これまでの点検にリスク分析の考え方を取り入れた形で実施している。取組結果については，資料に示した通り。

・ 「未改善課題あり」の課数が減少したにもかかわらず，翌年度の自己点検で「課題あり」の課数が再び増加するという傾向がある。職員の意識を維持する為には，情報セキュリティ点検を継続し，職員への意識付けが必要と考えている。
・ 情報システム監査は，情報システムを所管している課を対象としたもので，「訪問調査・技術監査」後に改善取組の事後確認を行う「フォローアップ」を行った。取組結果については，資料に示した通り。
・ 訪問調査の結果より，情報システム監査の取り組みが安定運用のための点検と改善の契機になっていることが確認できたことから，今後も継続することで，情報システムにおけるセキュリティ対策の PDCA サイクルを機能させていきたいと考えている。
・ 職員向け情報セキュリティ研修については，表１のアンケート結果のとおり，職員から「研修が役立つ」という評価を受けており，一定の成果が出ていると考えられる。

②平成 27 年度仙台市情報セキュリティ対策改善取組について（資料２）

（事務局（渋谷課長）より資料及び以下の補足について説明）

・ 情報セキュリティ点検，情報システム監査，情報セキュリティ研修を引き続き行っていく。情報システム監査の来年度以降の選定方法については検討している（資料 4 で説明）。
・ 情報セキュリティポリシーの見直しの検討は，今年 3 月に国から「地方公共団体における情報セキュリティポリシーに関するガイドライン」が示されたことから，本市においてもこのガイドラインに基づきセキュリティポリシーの見直しを検討する。

（各委員からの主な質問・意見は以下のとおり）

（金谷委員）　情報セキュリティ点検について，平成 26 年度と比較して平成 27 年度の対象が 2 か所減ったのは課公所が 2 か所減ったということか。また 422 課のうち 290 課公所は何も課題がでなかったということでよいか。

（事務局）　そのとおり。

（金谷委員）　取り組み結果でほぼすべての課題を改善しているのはすばらしいことである。昨年と比べてもセキュリティに関する自己点検結果の課題がそれほど多く出なかったということは，庁内にセキュリティの取り組みについての意識が浸透してきて，よりセキュアな運用ができているということであり，よいことである。

（金谷委員）　図 2 の「不審な電子メールの取扱い」について，課題は解決しているようだが，実際の対策は難しい場合がある。特に標的型メールは最新の状況を踏まえて引き続き対応を検討すべきである。

（金谷委員）　今後の取り組みとしては，情報セキュリティ点検，情報システム監査，情報セキュリティ研修の 3 本柱でやっていくことになると思うが，新たな対策についても検討してみてほしい。例として電子メールの予防訓練等が挙げられる。始めのうちは 7～8 割の人がメールを開封してしまうかもしれない。また真面目な人ほど引っかかる傾

向がある。しかし，それを通じてリスクがあるということを認識させることが重要である。

（金谷委員）　図 3 の「スタンドアロンパソコンのウイルス対策」について，自己点検後の改善報告で未改善課題が残っていたが，その後の追跡調査で改善したのはなぜか。

（事務局）　改善した事例として，調査後に廃棄したもの，庁内 LAN 用端末へ運用を変更したもの，新たにウイルス対策ソフトを導入したものなどがある。

（金谷委員）　システム上ウイルス対策ができないものもあると思われる。例えばそもそもウイルス対策ソフトが提供されていないようなシステム，なんらかの事情でアップデートできないシステム，インターネットから完全に隔絶していてウイルスのパターンファイルは月 1 回しか実施できないシステム等。いろいろな事情があると思うので，事情に応じてうまく対応をしてほしい。しかし今回の結果で 0 になったのは，適切な対策ができているということでよいことであると思う。

（金谷委員）　訪問調査の結果について，優良事例を紹介するのはよい取り組みである。「情報セキュリティ課題・対策事例集」でも改善例・優良事例をかなり紹介しており，どう対策すればよいかがわかりやすい。優良事例，危険な事例を集めて職員に周知していくのは有効なので，今後も継続してほしい。

（金谷委員）　予算措置を含めた対策が必要というのはまさしくその通りである。セキュリティは守られているというのが当たり前になってきていて，点検を行った結果が，予算措置の権限のある所まで効果が見えづらい。セキュリティの確保には，人・もの・金・情報・時間というものが必要になってくる。予算措置を含めたという文言はこの点を踏まえており，よい表現である。

（金谷委員）　リスク評価にはぜい弱性の認識だけでなく，脅威の認識も必要になってくる。脅威は日々変わっていて，例えば外部からの攻撃で新たな手法が開発されて新たな脅威になることがある。ぜい弱性の認識だけでなく，脅威の認識，つまり最新の情報を適切に集める努力もしてもらいたい

（金谷委員）　図 4 では自己点検を 68 システム対象として実施し，その結果 54 システムに課題が見つかったということでよいか。

（事務局）　そのとおり。

（金谷委員）　図 5 について，平成 25 年度と平成 26 年度の未改善課題ありの 56 システムは同一のものか。

（事務局）　同一のものとは限らない。平成 25 年度と平成 26 年度では，調査対象のシステム数が違い，対象システムも全く同じではない。また質問数も変更している。

（金谷委員）　恒常的に課題が減らせないシステムがあるということではないのか。

（事務局）　恒常的に課題が減らせないシステムもある。

（金谷委員）　技術面の課題には改善が難しいものも確かに存在する。その場合はリスク軽減策として多層防御の取り組みをするように強く働きかける必要がある。例えば「セキュリティパッチの適用」,「無停電電源装置（UPS）の管理」,「管理者 ID の運用管理（サーバ OS 用）」,「情報システムの稼働監視」等は改善が難しいことが図 5 からわかる。これらについては例外措置を手続きとして定めて，CISO からの承認を認めて，多層防御を含めた形でリスクの軽減に努めていくようにしていくべきである。また，課題に

関しては見えてきた後での対応が重要となる。

（金谷委員）　訪問調査の結果について，簡易なパスワードを設定していた事例や，バックアップの取得結果を確認していない事例があったとのことだが，これ以外にもいくつか課題は見受けられたと思う。「仙台市情報セキュリティ対策改善取組報告書（概要版）」でも管理者のパスワード変更が行われていない事例，実施手順が運用と合っていない事例があったとのことだが，特に管理者のパスワードを変更していない点は深刻な問題なので，訪問調査の結果を受けてフォローアップをしっかり行ってほしい。

（金谷委員）　技術監査の結果について，いくつかのシステムにぜい弱性が見つかった点や，パスワードが平文でやりとりされていた点などがあったが，特に外部接続しているものについてはセキュリティ上問題がある。これは，技術監査で得られた結果に基づいて粛々と対応していく必要がある。また，サポートが切れた PC やサーバについて，どうしても残さなければならず継続して使い続けるものは，慎重な対応が必要となる。

（金谷委員）　情報システム監査の結果が PDCA のきっかけになっているのはよいことなので，今後も継続して取り組んでほしい。

（金谷委員）　平成 27 年度のセキュリティ対策改善取組については，平成 26 年度と同様の取り組みを行っていくということでよいか。

（事務局）　そのとおり。

（金谷委員）　情報セキュリティ点検，情報システム監査についてそれぞれの訪問調査・技術監査が平成 26 年度と比較して 1 ヶ月遅れたのは，審査対象の抽出が大変だからということか。

（事務局）　抽出から監査までの期間が短いと，監査対象課で対応ができなくなってしまうため，余裕をもって対応してもらえるように期間を空ける予定である。

（金谷委員）　システム監査の対象が平成 26 年度と比べて 86 システムに増えたのはなぜか。

（事務局）　対象数については，いろいろな工夫をして選んだのと，受託業者からこのぐらいの数でやってもよいのではと提案があったので決定した。

（金谷委員）　これは全システムの約 4 割程度になる。すべてのシステムが 2～3 年に 1 度は監査対象となるのか。

（事務局）　総システム数は 210 であるが，自己点検の対象は重要なシステムから 161 システムを選んでいる。

（金谷委員）　何年経っても対象とならないシステムがあるということか。

（事務局）　1 度も対象とならないシステムも出てくる。

（金谷委員）　その点についてはどう考えているのか。

（事務局）　規模の大きなシステムで，複数課で利用するシステムを重要なシステムとして考えており，まずはそこを中心に監査をやっていくべきと考えている。市民への影響が小さいものや，一つの課で利用している小さいシステム等は後回しにしている。

（金谷委員）　重要度の高いシステムからやっていくという取り組みはよいが，いずれは小さいシステムでも 1 回は監査の対象としてほしい。きちんとしたセキュリティ対策を隅々まで広げていくことが重要である。

（金谷委員）　情報セキュリティ研修について，情報管理者から一般職員まで隅々にわたり対象としているのは，よい取り組みである。しかし 4 月に入庁した新任職員に対して，9

月に実施するのは遅いのではないか。

（事務局）　資料に記載はしていないが，4 月に新規採用職員向けのセキュリティ研修を実施している。

（金谷委員）　実施しているなら，1 行だけでもよいので記載してほしい。

（金谷委員）　情報セキュリティポリシーの見直しの検討について，総務省ガイドラインの改正内容は仙台市のセキュリティポリシーに影響を及ぼしているのか。

（事務局）　モバイル端末，複合機の取扱い，標的型メールの項目等については影響があるので改正を検討している。

（金谷委員）　新しい課題は今後も出てくるので，しっかりと情報収集をして取り組んでいってほしい。

（舘田委員）　全体的に去年より重大なリスクが減っている印象を受けた。対策への取り組み効果が表れているのだと思う。平成 18 年度から監査を導入しているとのことだが，自己点検で課題ありとなる件数は年々減ってきているのではないか。

（事務局）　確実に減ってきている。

（舘田委員）　経年変化について簡単にまとめると，どれぐらい効果があるのか，また定着している効果が見られるので，やってみてほしい。ここ 1～2 年見ただけでも課題が減っているので，効果を実感するうえでも経年変化があってよいと思う。

（舘田委員）　自己点検の質問内容は毎年変更しているのか。

（事務局）　年々少しずつ変更させている。特に平成 25 年度からはリスク分析の考え方も取り入れて大きく変更した。

（舘田委員）　セキュリティのリスクはどんどん変わってきているので，その取り組みは今後も実施してほしい。

（舘田委員）　自己点検は情報システムのみが対象なのか。それ以外の全般的な点検も行っているのか。

（事務局）　全般的な点検を行っている。

（舘田委員）　訪問調査の結果について， 優良事例を取り入れるのはよいことである。セキュリティ対策は後ろ向きでよいイメージがないが，前向きなメッセージを出すことで取り組んだ人のモチベーションをあげることができるので今後も継続するべきである。例えば交通事故ゼロ○ヵ月継続中というように，セキュリティ事故ゼロ○ヵ月継続中というようなメッセージの発信の仕方でもよいと思う。今このようなよい事例が続いていますというようなメッセージの発信の仕方がよい。

（佐藤委員）　情報セキュリティ点検について，改善課題の数がいったん減少しても次の年に再び増加してしまうのは意識の問題と記載があるが，例えば「スタンドアロンパソコンの盗難防止対策」や「USB メモリへの重要性分類の表示」，「廃棄予定のフロッピーディスクの保管と廃棄」等の項目は意識の問題だけではないように思われる。そこの理由を踏み込んで調査した方がよい。聞き方に問題がある可能性もある。システム監査についても同様で，1 年経過したら課題が増えてしまう原因を追究してみるべきだと思う。

（事務局）　毎年続けるのは重要だが，マンネリ化してしまう問題もある。自己点検では問題なかった項目が，実際の訪問調査で課題として発覚することもある。これについて

の対策は今後の課題であると考えている。

（佐藤委員）　しっかりと課題を挙げてきているというところは，ごまかしていない証拠でもあるかもしれない。

（佐藤委員）　訪問調査の結果について，多くの課題が検出されたとあるが，自己点検でカバーできなかった課題が新たに出てきたのであれば，翌年度の自己点検に反映させるべきである。

（佐藤委員）　技術面の課題について，リスク低減策を実施してリスクをコントロールしている所管課が増加しているのはよいことである。やりにくいことをやっていくよりも，自ら考え工夫してリスクを低減するほうが実効性があるケースもある。よい取り組みがあれば広く紹介していくべきである。

（佐藤委員）　標的型メールの訓練については，社内でも取り組んでおり，年々開封率は下がってきているが 0 にはならない。それはしょうがないが，重要なのは，問題が起きた時にどう対処するかであり，それを確認しておくことに意味がある。多少費用はかかるが効果はあるので検討してみてほしい。

（佐藤委員）　セキュリティポリシーの見直しについて，仙台市はマイナンバーの対応はすでに済んでいるのか。

（事務局）　まだできていない。しかし現在のセキュリティポリシーはある程度，国からのガイドラインに沿って作られている。マイナンバー法に対応するだけであれば，遵守法令の中にマイナンバー法を入れるだけで足りるのではないかと考えている。

（佐藤委員）　マイナンバーの保管を誰が取得してどう管理するか，情報が漏れた時の対応をどうするか等のルールはどう策定するのか。

（事務局）　個別のシステムの対応は，実施手順で担当者やセキュリティ対応について記載している。セキュリティポリシーではなくその下の位置づけでシステムごとに作ってもらう事を想定している。

（石井委員）　システム監査の結果について，自己点検の結果で恒常的対策がとれていないものがあったが，特定個人情報保護評価との関係で気にしなければいけない事はあるか。

（事務局）　今回のセキュリティ監査に関しては特にない。

（石井委員）　今回の調査は社会保障や税に関係しないシステムなのか。

（事務局）　社会保障や税に関係するシステムも調査対象であったが，問題はなかった。

（石井委員）　外部に業務を委託する場合，委託先で情報が漏えいする可能性があるが，その対策について補足説明をしてほしい。

（事務局）　外部委託審査会という仙台市独自の取り組みを実施している。個人情報を取り扱う情報システム処理に関しては，依頼課で現地調査等をして調査票を作成してもらい，それが基準を満たしているか審査している。この取り組みにより，外部での情報漏えいに対する対策はできていると考える。

（石井委員）　何がきっかけで外部委託審査会を始めたのか。

（事務局）　過去に委託先で情報漏えいがあり，それをきっかけに始めた。

（石井委員）　審査の内容はマイナンバーの特定個人情報保護評価とは重複するのか。

（事務局）　重複する部分がある。特定個人情報保護評価は，個人のプライバシーや権利，利益に重大な影響を及ぼす事案について，新たに特定個人情報を取得する際に求められ

ているが，特に重大なものについてはその取得の前にパブリックコメントや第三者機関による点検が必要となる。本市は個人情報保護審議会という別の審議会で点検を経た上で，情報を持つという仕組みをとっている。

（金谷委員）　特定個人情報保護評価については，委託先のリスク対策について第三者委員会のほうで審査している。

（委員長）　他の自治体での第三者委員会に参加した経験からすると，1回だけの審議では足りないと感じる。1回だけでは細かい部分までの指摘が難しく，その部分から情報が漏れてしまう。手間がかかってしまうが，国が定めている公式なものでなくてもよいので，事前に点検をする機会を設けたほうがよい。

（石井委員）　他の自治体では，部会を別途設けて二段階で検討した上で，審議会に挙げて結論を出すところがある。対応は大変かもしれないが，会議としては中身があるものになる。

（委員長）　情報セキュリティ点検では，侵入されない，アタックされないというところの点検が主になっているが，ここ 1 年でセキュリティに関する状況はかなり悪化しており，以前は城壁の外をどうするかという所を見ていたが，今は城壁の中で暴れているものをどうするかというのがセキュリティ関係者の認識になっている。仙台市はせっかくここまで対策が進んでいるのだから，侵入された時にどうするかという点検をしていくべきである。例えば標的型メールは，ある組織に対してばらまいたあとで，ウェブページでアクセスした人が複数いても，そのうち 3 人目だけにウイルスを送り込むような，かなり手が込んだものになってきている。しかも細かく点検してやっとわかるようなものになってきている。今はどちらかというと，マルウェアが内部に入ってしまった後の対応を考えるべきであり，その中でどういう事が必要か考えたときに，課によって，または内部同士でどういう接続方法をしているかによって心配なところは違ってくると思う。そういった情報を点検の中で集めていくべきである。通常の IPS，ファイアウォールではどうしようもないのは事実であり，次世代型ファイアウォールにしても何を守らなければいけないのか，どれぐらい労力をかけるかという考えなしに買っても大変なだけである。しかし，点検の中にマルウェアが入ってしまった後にどうするかという項目を加えて，情報を集めていけば相当違ってくる。

（委員長）　インシデントが発生したときに誰に知らせて対応するかという点について，最近のマルウェアの事例としては，サイト内で一斉に配った後，マルウェアを潰しはじめると動作していなかったものが動き出すものや，すべてを一斉に潰すと情報を取るのをやめて中の情報をすべて消してしまうものなどがある。むやみに対応はせず，事例を収集する事が大事である。

（委員長）　情報システム監査の結果として，防御面での対策は進んでいるようだが，可用性についても対策を進めるべきである。セキュリティパッチは複雑化してきており，パッチをあてることでシステムが動作しなくなることもある。そういう観点も踏まえて「セキュリティパッチの適用」，「情報システムの稼働監視」の項目はもう少し点検したほうがよいかもしれない。

（委員長）　OECD8 原則にもあるとおり，今後は情報主体からの情報開示要求が多くなることが予想される。仙台市は意識が高い人が多いため，確認を求められた際に，本人確

認をどこまで行うのか，どこまで開示するのかが問題となる。ルールを慌てて決めるのはよくない。時間はまだあるので早めに検討を進めるべきである。

（金谷委員）　特定個人情報になると法定代理人からだけでなく任意代理人からの開示請求があるのでそこについても気を付けてほしい。

③セキュリティ障害について（資料３）

（事務局（渋谷課長）より資料及び以下の補足について説明）

（各委員からの主な質問・意見は以下のとおり）

（石井委員）　これらの障害に気付いたきっかけは何か。

（事務局）　（1）と（2）は市民からの問い合わせがきっかけで発覚した。（3）は担当課で検証していた際，icsca のポイント付与でおかしな点があり発覚した。（4）は（3）の結果から全部のプログラムを見直した際に発覚した。

（石井委員）　申し出があって発覚したものと，自分達で偶然気づいたもの，芋づる式に発覚したものということか。

（事務局）　そのとおり。

（金谷委員）　仙台市の取り組みは機密性に関する対策は徹底されているようで，その部分での事故が発生していないのは評価できる。完全性・可用性の部分では，最近 GIMA（中央官庁や裁判所などが利用する職員認証サービス）が止まった事故があったが，そのような事故が発生してしまうと業務に支障が出てしまうので，完全性・可用性についても意識を持ったうえでセキュリティ対策を実施してほしい。

（石井委員）　（機密性に関する）事故が発生していないかどうかはわからない。気づいていないだけである。

（佐藤委員）　個人情報の流出に関する事故だけでなく，システムの障害すべてをセキュリティ障害として報告してもらっているのか？

（事務局）　そのとおり。

（佐藤委員）　4 件だけしか障害が発生していないのか。

（事務局）　公表するほど大きい障害は 4 件だけである。

（金谷委員）　去年，仙台市は USB メモリの紛失問題があったが，その後の対策のおかげでよくなったように見受けられる。しかし気づいていないだけで探せば問題はある。しっかりと検知をして見つけたら遮断する。遮断してその後に追跡する。そういう所まで対応できる体制を整えておく必要がある。職員が個人の端末を使って情報の送受信をする場面なども想定されるが，いろいろな所でいろいろな使われ方がされているので，見つかっていないリスクはあるのではと思う。

（石井委員）　マイナンバーが始まった際に情報提供ネットワークシステムを使用するが，（1）（2）のように間違った情報を照会者に送ってしまう危険性はあるのか。

（事務局）　データ自体が間違っていた場合には，その危険性はある。

（石井委員）　マイナンバー制度との関連では，（1）（2）については気を付けた方がよい。

（委員長）　システム開発に関して，地方公共団体は発注する際，テストは受託者側がやるという意識がある。情報システムの費用算出の際に，テスト項目については，国が出

しているガイドラインを含めて，不当に少ない場合がある。本来はコーディング 1 に対してテストは 10 ぐらいの労力が必要で，テストにも労力をかけなければいけない。コーディングはわかりやすいのでお金をかけやすいが，テストにお金をかけていない場合がある。テストのやり方・報告の結果，その評価等について業者に委託する場合，また内製のソフトの場合でも誰が担当するかは検討しなければいけない。

（舘田委員）　受注者側としてテストはもちろん実施しているはずである。自治体も一緒に参加してチェックをして問題ないように対応はしていると思うが，ものすごいケースがあるため，想定外のトラブルは起こってしまう。ありとあらゆるケースすべてに対応するのは難しい。発注者も受注者もお互いに責任はあるが，トラブルの原因の多くは，仕様漏れが多い。費用はかかるが仕様の細かい部分まで確認をしていくべきである。

（金谷委員）　すべてのリスクに対応するのは難しい。リスク評価をし，リスクをすべてなくすのが理想だが，それは難しいので，リスクの低いものは問題が起こってから改善をしていくというやり方も一つの手である。

（舘田委員）　問題が発生した際，その情報を組織の上に上げる仕組みが重要である。

（委員長）　　システムを発注する際に，システム作成前に行う業務分析の時間が足りないことが多い。発注してから 1 年（理想は 1 年半）はテスト期間として，仕様の検証期間として考えておくべきである。これは 3 年目以降の運用保守以上の費用をみておいたほうがよい。結果的にはよいシステムの作成につながる。

④その他の庁内セキュリティ対策について（資料４）

（事務局（渋谷課長）より資料及び以下の補足について説明）

（各委員からの主な質問・意見は以下のとおり）

参考資料 3　USB メモリのセキュリティ対策の結果について

（金谷委員）　昨年度の一番大きな話題であり，しっかり対策していることが伺える。本数については，だいぶ減ったがまだ多い印象を受ける。

（事務局）　　必要最小限の数を全庁に照会し，情報政策課で調達している。

（金谷委員）　対策前の本数について，資料 4 では 3,982 本となっているのに対し，参考資料 3 では 4,766 本となっている。本数が違うのはなぜか。

（事務局）　　事前に送付した資料については数字を修正している。対策前の本数は，企業局を含めると 4,766 本になるが，企業局を除くと 3,982 本になる。対策後の 1,199 本も企業局を除いた数値となり，企業局を含めると数は増える。

（金谷委員）　今後もさらに取り組みを続けていくのが望ましい。

（委員長）　　USB メモリを使用した後の取扱いはどうしているのか。

（事務局）　　データを消去して，保管庫で施錠管理するようにしている。

（金谷委員）　USB メモリの運用ルールはあるのか。

（事務局）　　共通実施手順で取決めしている。

（佐藤委員）　それは USB メモリについてだけでなくデータ持ち出し全般に関してのルールということなのか。

（事務局）　　そのとおり。

（佐藤委員）　暗号化 USB メモリはデータが強制的に暗号化されるものなのか。

（事務局）　強制的に暗号化される。既存 USB のメモリを回収し，暗号化 USB メモリを調達をして配布するところまで一括して情報政策課で行っており，暗号化 USB メモリの種類は基本的に 1 つしかない。それ以降については，各課で調達することになるが，暗号化するものに限っている。

（金谷委員）　暗号化の復号はどのように行うのか。

（事務局）　USB メモリを挿入した際に，復号パスワードを入力するものを使用している。

（金谷委員）　暗号化パスワードの管理については別途規定を定めているのか。

（事務局）　運用で一定の文字を組み合わせてパスワードを設定してもらうように取決めしている。

（委員長）　持ち出した USB メモリをどの PC に接続したか記録は残しているか。

（事務局）　どの PC に接続したかは記録していない。

（委員長）　マルウェア等を感染して持ってくる可能性があるため，対応できるなら，どの PC に接続したかも管理するべきである。

（事務局）　持ち出しについては，台帳で管理している。

（委員長）　マルウェアに感染したと判かった場合，その PC に接続した USB メモリは全部疑うべきで，その際に必要な情報となる。業務に差し支えない程度に検討してみてほしい。

（石井委員）　パスワードの更新について，更新時期の取決めはあるのか。

（事務局）　定期的に更新するように取決めしているのみである。基本的には年に 1 回や人事異動の際に行うものであると思うが，各課の運用次第である。

（金谷委員）　課で共通のパスワードを使用しているのか。

（事務局）　パスワードは各課別々であり，固体ごとの設定は各課の運用次第である。

（金谷委員）　場合によっては異動後も USB メモリが使える可能性があるということか。

（事務局）　変更していなければあり得る。しかし施錠管理されているので，その点は問題ないと考える。

（石井委員）　参考資料 3 について，利用実態調査の用途のうち「バックアップ用（約 21%）」とあるが，かつてはバックアップとして使用していたのか。

（事務局）　庁内 PC データのバックアップとして使用していた。しかし運用上問題があるため，禁止した経緯がある。

参考資料 4　情報システム監査の実施方法について

（金谷委員）　監査対象をローテーションするのは対象課にとって事前準備が可能なので，よい取り組みである。しかし総システム数 206，重要システム数 161 に対し，仮に訪問調査の対象を 10 システムとして 5 年サイクルで回すとしたときに，計 50 システムとなる。残りの 150 システムについては適宜追加・入れ替えをするとの事だが，万遍なく調査はしづらくなってしまう。その対応はどう考えているのか。

（事務局）　訪問調査と技術監査に関しては，重要なシステムのみを対象としている。重要システムの定義としては，求められる可用性の面で一週間以上止まったら業務に影響が生じるものを選んでいるのが現状。本来は 1 日で影響が出るものを重要システムとするべきだとは思うが，現状はこの大きなくくりの中で対象のシステムを選定するこ

とにしている。その中で選定したものについては順番に自己点検をしていこうと考えている。訪問調査や技術監査についても新たに作るシステムや，重要になってくるシステムが出てくると思うので，入れ替えは検討している。

（金谷委員）　訪問調査については，重要なシステムに重点を置くのはよいと思うが，自己点検はなるべく多くのシステムを網羅できるように抽出・選定をしていってほしい。

（金谷委員）　インフラ系のシステムも監査の対象に含まれるのか。

（事務局）　　インフラ系のシステムは調査の対象としていない。

（委員長）　　システムの数を減らすことはできないのか。むやみに統廃合するわけにはいかないが，減らしていかないと今後管理が大変になる。

（事務局）　　今年度から最適化推進室を設置した。システムの最適化を行うが，情報資産のスリム化を目指すとともに，内容の近いシステムは更新の時を見据えて統合を目指すようにしている。

（委員長）　　構築当時は便利だと思って作成したシステムでも，現在は内容が近いシステムがあると思う。そういうものは共通で使えるようにして，管理の対象を減らした方がよい。

（委員長総括）　仙台市のセキュリティ対策は全般的に進んでいると感じた。しかし，さらに上の対策を目指しているとのことなので，今回の議論の内容を踏まえてさらに対策を進めて，全国の模範となるようになっていただきたい。

（以上の議事について，委員会としての承認を得た。）

（６）その他

特になし。

（７）閉会

－　以上　－