

## 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

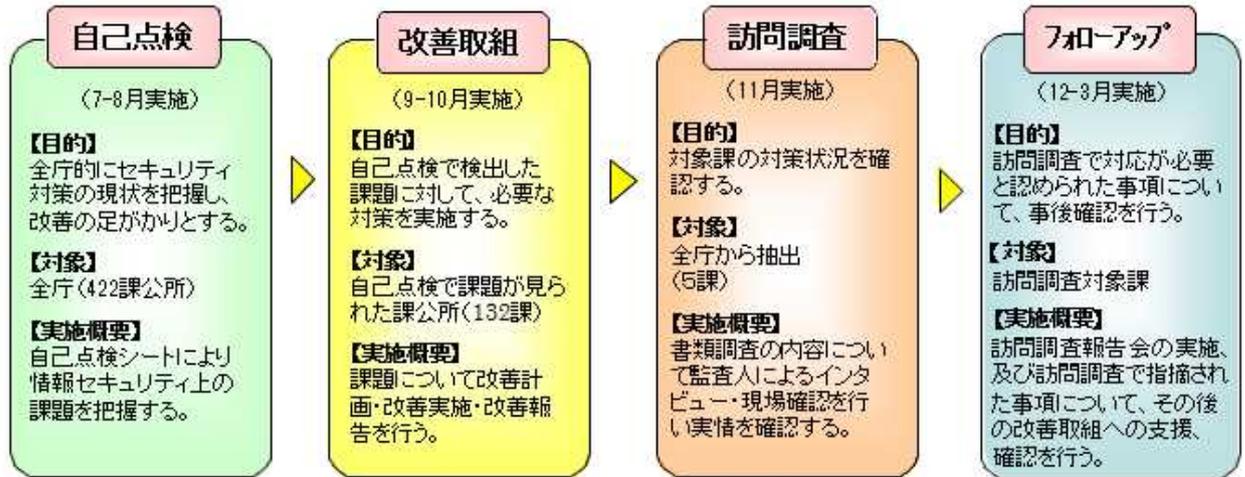
平成 18 年度から助言型監査を導入し、情報セキュリティ点検や研修、リスク分析及び情報システム監査を実施してきた。平成 26 年度仙台市情報セキュリティ対策改善取組の状況（以下「改善取組状況」という。）は、以下のとおりである。

### 1 情報セキュリティ点検

#### (1) 実施内容

自己点検により自課の情報セキュリティの現状及び課題を確認した。（図 1）

図 1 情報セキュリティ点検の流れ



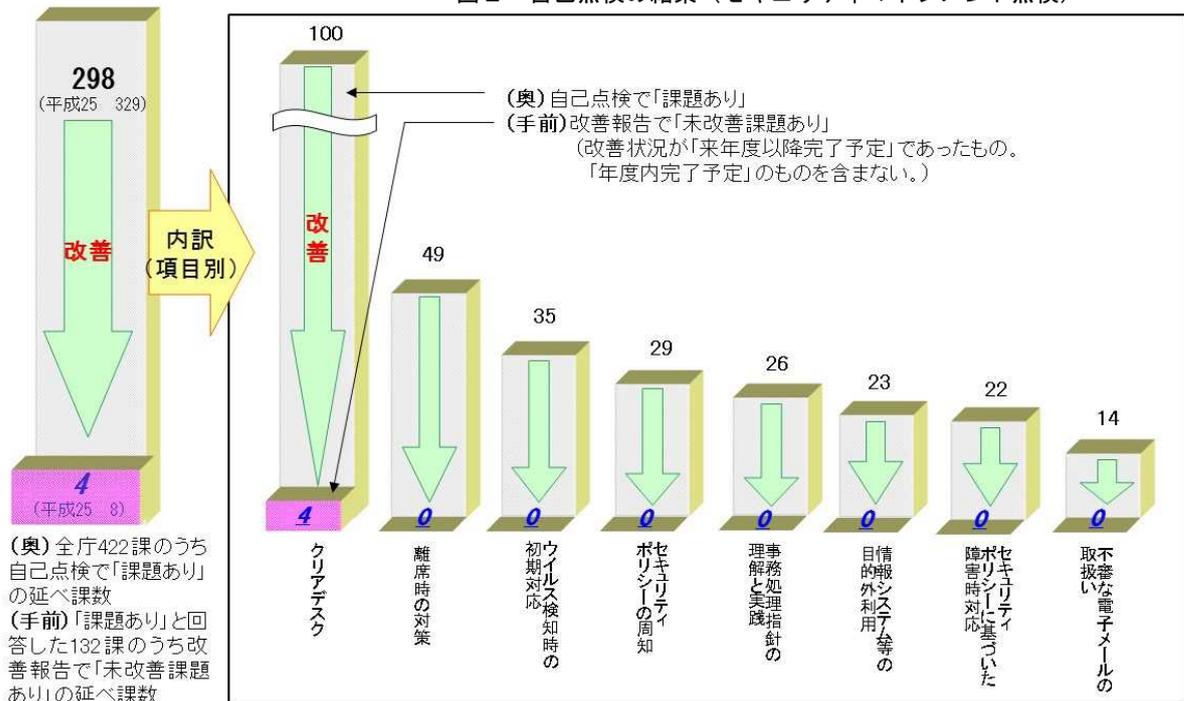
#### (2) 取組み結果

##### ① 自己点検の結果

(セキュリティマネジメント点検)

平成 25 年度に比べ課題や未改善課題は減少しているが、クリアデスクについては、他の調査項目と比較するとまだ未改善の課が残っており、根気強く対策を継続することが必要である。（図 2）

図 2 自己点検の結果（セキュリティマネジメント点検）

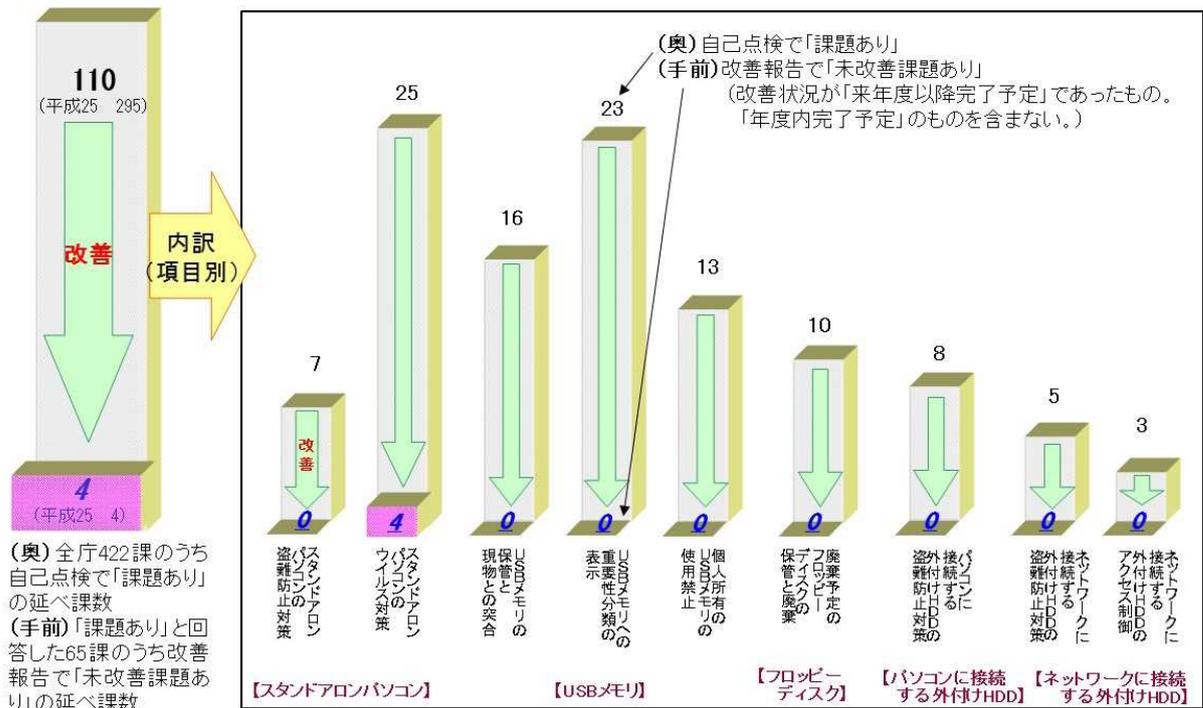


(リスク対策状況点検)

各課で保有する主要な情報資産の動向を把握できるようになった。

また、平成 25 年度と同様にスタンドアロンパソコンのウイルス対策で未改善課題があったが、追跡調査の結果、全て改善していることを確認した。(図 3)

図 3 自己点検の結果 (リスク対策状況点検)



② 訪問調査の結果

自己点検では課題なしと判断していたが、訪問調査で「USBメモリの保管と現物との突合」、「USBメモリへの重要性分類の表示」などの課題を確認した。

一方、USBメモリの保管方法の工夫により現物の有無確認を容易にして紛失を防止する対策が実施されている事例、スタンドアロンパソコン向けのウイルス対策ソフトの導入や定義ファイル更新作業の当番制及び作業記録の作成により、ウイルス対策が確実に実施されている事例などの優良事例を確認した。

③ まとめ

書類調査の結果、「セキュリティマネジメント点検」については、課題や未改善課題は平成 25 年度に比べて減少しているが、「クリアデスク」については、他の調査項目と比較するとまだ未改善の課が残っている。職員への継続的な周知と課全体での定期的な整理整頓の実施（日常業務での対策）が効果的だが、収納スペースの確保に起因する課題等に対しては、予算措置を含めた課及び局での対策（環境面での対策）が必要である。

また、「リスク対策状況点検」については、具体的な対策の実施状況の確認により、どのような未対策のせい弱性が多いか等の具体的な課題が明確になった。

なお、改善報告において「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は「課題あり」の課数が再び増加するという傾向がある。情報セキュリティ対策の推進においては、職員の意識を維持・向上を図り、一過性の対策としないための継続的な意識付けが必要である。

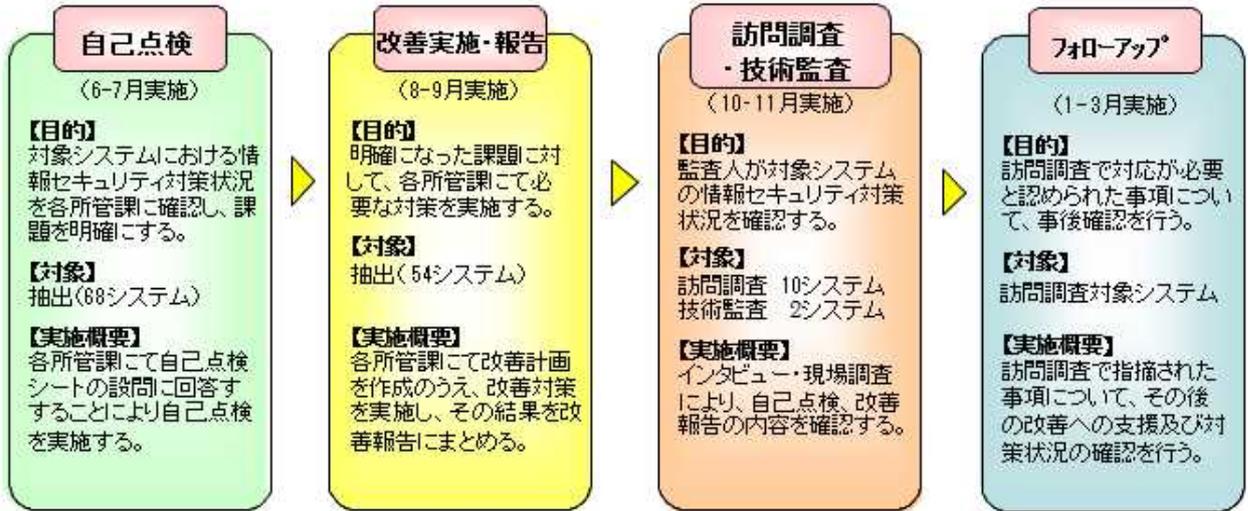
## 2 情報システム監査

### (1) 実施内容

複数の課公所で使用されている情報システムや個人情報等の重要な情報を取扱う情報システムに対して運用にかかる自己点検を行い、その中の10システムについては訪問によるシステム運用面からの調査も行った。また、2システムを選定し、訪問調査に加え技術監査を実施した。

(図4)

図4 情報システム対象の監査の流れ

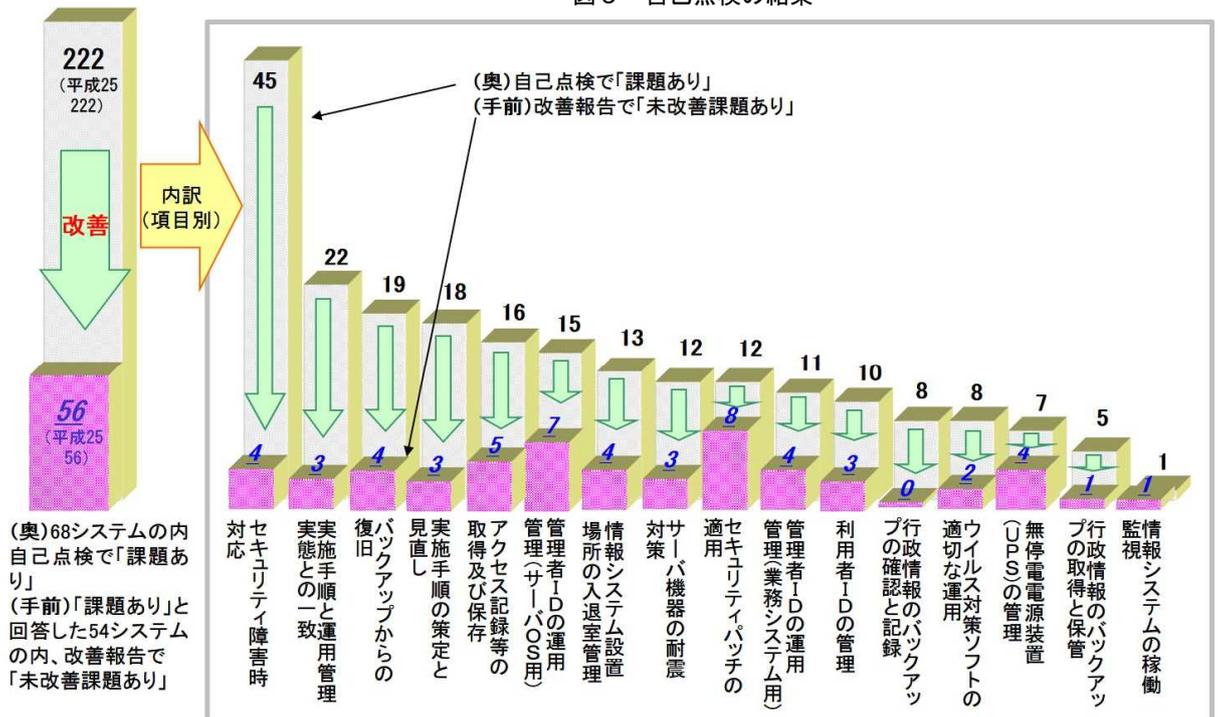


### (2) 取組み結果

#### ① 自己点検の結果

自己点検及び改善報告の結果から、情報システムにおける情報セキュリティ対策では、技術面の課題には改善が難しいものがあり、運用面の課題は速やかに改善されるという傾向がある。改善が困難な技術面の課題の一つである「セキュリティパッチの適用」については、「適用できない理由」の確認と並行して、本当に適用できないのであればリスク低減策の実施状況を確認して、情報セキュリティリスクの低減を推進した。(図5)

図5 自己点検の結果



## ②訪問調査の結果

訪問調査では、情報システムの形態、規模、接続するネットワーク、保有する行政情報などの個別の状況を把握したうえで、対象システムの運用管理状況を点検し、簡易なパスワードが設定されていたり、バックアップの取得結果を確認していないため失敗を検知できないなどの見落とし又は認識不足と判断した多くの課題を検出した。検出した課題については、情報システムの運用管理実態にあった具体的な改善提案を行い、改善への取組みを支援した。

## ③技術監査の結果

診断ツールによるサーバ・機器診断と Web アプリケーションのぜい弱性診断を実施した。1 システムでは、いくつかのぜい弱性を検出したが、庁内 LAN の内側からのアクセスに限定していることと、複数の対策による多層防御が機能しているため、対策の必要性は低いと判断した。他の 1 システムでは、インターネットに公開されているサーバの 1 台に、サポートが終了した OS が使用されている緊急度の高いぜい弱性を検出した。

また、他の公開サーバ上で動作する Web アプリケーションからも対策が必要なぜい弱性を検出した。

## ④まとめ

書類調査の結果、運用面の課題について速やかに改善が実施されているが、技術面の課題については、システム上の制約、保守契約、費用面等の理由で改善が進みにくい状況であるが、このような技術面の課題については、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システム所管課が増加している。

技術監査では、庁内 LAN に接続しているシステムとインターネットに公開している情報システムに対して、診断ツールによるサーバ・機器診断と Web アプリケーション診断を実施した。診断結果ではいくつかの課題を検出しているが、2 システムとも明確なセキュリティパッチの適用方針があり、課題の改善についても適切な対応が実施された。

訪問調査では、情報システム監査の取組みが、情報システムの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。このような取組みを継続することで、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。

### 3 情報セキュリティ研修

職責別に以下の表のとおり実施した。

研修のアンケートでは、全ての研修において、「非常に役立つ・役立つ」と回答した職員が8割以上であった。

表1 職員向け情報セキュリティ研修

研修コース	参加人数	アンケート結果
局区情報管理者研修	28名	—
情報管理者＋副情報管理者（講義）	167名	非常に役立つ・役立つ 89%
情報管理者（演習）	67名	非常に役立つ・役立つ 97%
一般職員（基礎編）	271名	非常に役立つ・役立つ 85%
一般職員（応用編）	109名	非常に役立つ・役立つ 83%

### 4 外部委託審査会等

情報システム処理に伴う個人情報に係る外部委託に関するガイドラインに基づき、個人情報の保護を図るため、受託者の個人情報保護対策が適切かつ十分にとられているかを審査する「外部委託審査会」を開催。また、受託者を対象とした「個人情報セキュリティ研修」を継続して開催している。

平成26年度審査件数 234件

平成26年度個人情報セキュリティ研修受講者数 315人（6回 185事業者）

以上