

## 情報セキュリティ監査実施報告書

この情報セキュリティ監査実施報告書は令和 7 年度に実施した戸田市情報セキュリティ監査支援業務委託のうち情報セキュリティ外部監査（以下「外部監査」という。）、情報セキュリティ内部監査（以下「内部監査」という。）及び情報セキュリティ自己点検（以下「自己点検」という。）の実施結果を報告するものである。

それぞれの結果は下記のとおりである。

### 記

#### 1 外部監査及び内部監査における判定基準

外部監査及び内部監査では、監査項目ごとに下表で示す判定基準を基に監査対象のセキュリティ対策状況を判定した。

「監査の判定基準」

評価	成熟度判定	分類基準
適合 「○」	レベル 4 (評価事項)	レベル 3 の対策が継続的に実施されており、さらに積極的な改善活動がなされている。
	レベル 3	情報セキュリティポリシー等の基準を満たしており、標準的で適切な状態である。
不適合 「×」	レベル 2	情報セキュリティポリシー等の基準に対し、対策漏れがあり改善の余地がある。
	レベル 1	情報セキュリティポリシー等の基準に対し、場当たり的で対策不足のため改善が必要である。
	レベル 0	情報セキュリティポリシー等の基準に対し、必要な対策が実施されていない。又は認識されていない。

## 2 情報セキュリティ外部監査

監査中期計画に基づき、次の3つの手法で外部監査を行った。なお、監査対象は毎年変更して行っている。

### (1) サーバ機器等の技術的セキュリティ診断の結果

外部ネットワークに接続できないエリアにあるサーバを診断した結果、早急な改善を要するような緊急度の高い脆弱性は確認されなかった。しかし、システムへの影響度はさほど高くないものの、セキュリティ上改善が望まれる事項がいくつか検出されている。検出された課題については、可能な限り対応することが望まれるが、リスクが顕在化する条件に対して、対応することでシステムの動作に不具合が生じる可能性や改善にかかる費用等を加味し、総合的に検討した上で導き出された対策を実施することが望まれる。

### (2) 市職員への標的型攻撃を想定したメール訓練の結果

巧妙化する標的型攻撃メールを疑似的に再現した訓練メールを送信した結果、不信メールとして扱うべきところを正規のメールと認識してしまい、一部の職員が開封した。

訓練後に行ったアンケートでは、多くが標的型攻撃メールの対策を理解していることが確認された。また、不審メールを受信した際の対応や、不審な点に気付くためのポイントを再確認でき、訓練として有効だったとの回答が得られた。

昨今の標的型攻撃メールは、AIなどを使用して自然な文書が作られてきており、偽装のテクニックが年々向上している。そのため、今後も全体的な研修や標的型攻撃メール訓練を定期的に行い、注意喚起を継続することが望まれる。

### (3) 情報資産のセキュリティ対策状況確認の結果

例年行ってきた情報の取扱いや情報システムの管理の適切性、個人情報保護法及び番号法で求められる対策について、規程や法令等を遵守できているか否かの確認を行った。確認結果は成熟度モデルを参考にして数値化し、4.00点満点中3.00点以上を合格点とした。

その結果、確認した範囲の対策レベルの平均は、2.89点であり、昨年度と概ね同様の数値となった。いずれの検出も直ちに情報漏えい等の事故に発展する様な問題ではないが、事故が発生した際に説明責任を果たせなくなる懸念があった。

検出した課題については、全て改善の計画がなされ、かつその多くは今年度中に改善、又は改善予定であることが確認できた。事故の予防対策強化のため、今年度の課題及び改善方法を庁内に水平展開し、対策を促すことを推奨する。

## 3 情報セキュリティ内部監査

### (1) 内部監査の概要

戸田市の情報セキュリティ内部監査は、職員が監査員となって、外部監査の対象所属を除いた課所等（支所や保育園を含む）を対象に、平成17年度から3カ年で一巡する計画で実施されている。令和5年度からは7巡目が開始され、今年度も外部監査の一部と同じ項目について確認を行った。監査員への教育では、昨年同様に内部監査員の理解度向上を目的として事前学習時間を設

け、かつ判定の精度を向上させるための具体的な検出内容の事例紹介を行った。確認結果は外部監査と同様に成熟度モデルを参考にして数値化し、4.00 点満点中 3.00 点以上を合格点とした。

#### (2) 内部監査の結果

確認した範囲の対策レベルの平均は 3.00 点（前年度 3.12 点）と昨年度より低下したが、一昨年度以前と比較すると向上していることが確認できた。

更にセキュリティ対策を推進するために、今年度の課題及び改善方法を庁内に水平展開し、対策を促すことを推奨する。

### 4 情報セキュリティ自己点検

#### (1) 自己点検の概要

毎年、市の全職員を対象に情報セキュリティ自己点検を実施し、集計した結果から情報セキュリティ対策の浸透状況を継続的に確認している。なお、点検内容は、毎年少しずつ変更している。

#### (2) 自己点検の結果

市全体の遵守率は 96.1%（昨年度：95.2%）となり、昨年度より 0.9%向上した。低下した項目よりも向上した項目の方が多いため、全体の遵守率を押し上げている。

更にセキュリティ対策の認識を定着させるために、今後も継続的な周知と点検を行っていくことが望まれる。

以上