評価・見直しに関する対策基準

１．趣旨

本文書では、「岡山理科大学情報セキュリティポリシー」（以下、ポリシー）の運用実態の把握、情報セキュリティの診断等により、情報セキュリティに対する脅威、脆弱性を洗い出し、その対策を検討し、ポリシーに反映させるために、情報セキュリティポリシーの評価や見直しについて記述する。

２．ポリシー運用実態

最高情報セキュリティ責任者は、ポリシーの運用実態を把握するため、情報セキュリティ委員会、ネットワーク委員会に対し、次のような措置を求めなければならない。

2.1 ポリシー運用実態等の把握

全学ネットワーク運用管理責任者はネットワーク委員長と連携し、ネットワーク委員会を定期的および必要に応じて臨時的に開催し収集した情報を分析・整理した上で、情報セキュリティ委員会に報告しなければならない。情報セキュリティ委員会は、この報告、ならびに、情報セキュリティ委員を通じて得られた全学におけるポリシーの運用実態に基づいて、定期的および必要に応じて随時検討し、ポリシーの不完全さを認識しなければならない。

2.2 利用者の意見

部局情報セキュリティ委員は、各部局の教職員および学生からポリシー遵守に関する意見を収集し、情報セキュリティ委員会に報告しなければならない。

2.3 情報セキュリティ診断

全学ネットワーク運用管理責任者はネットワーク委員長と連携し、情報システムの安定性、機密性ならびに犯罪・事故予防の観点から情報システムに対する情報セキュリティ診断を実施すべきである。その結果をネットワーク委員会において情報セキュリティ診断として取りまとめ、情報セキュリティ委員会に報告しなければならない。

診断過程で重大なセキュリティの脆弱性が発見された場合は、緊急避難措置をとるとともに、ネットワーク委員と情報セキュリティ委員にその事実を速やかに連絡しなければならない。

2.4 情報セキュリティ監査

最高情報セキュリティ責任者は、監査を実施し、各部署が法令ならびにポリシーおよびこれに関連する規程・基準等を遵守しているか運用実態を把握すべきである。その結果を情報セキュリティ監査結果として取りまとめ、情報セキュリティ委員会に報告しなければならない。

2.5 セキュリティ対策費

情報セキュリティ委員会は、情報セキュリティ対策に要した直接的経費を把握しなければならない。これには、情報処理センターが不正アクセス等の検出のために購入した装置（ハードウェア、ソフトウェア、ソフトウェアのバージョンアップを含む）や外注したセキュリティ診断およ

び監査などに要した費用が含まれる。
　情報セキュリティを維持し続けるため、経費を正しく見積もり、予算措置をとらなければならない。

３．セキュリティレベル向上策
　最高情報セキュリティ責任者は、ポリシーに添った対策がどの程度実施されているかを評価するとともに、セキュリティレベルの向上に必要な措置を講じるため、情報セキュリティ委員会を年１回以上開催しなければならない。

3.1 ポリシーの更新
　情報セキュリティ委員会は、上記２．の結果に基づき、ポリシーの実効性を少なくとも年１回評価し、必要な部分を見直して内容の変更および実施時期の決定を行い、よりセキュリティレベルの高い、かつ、遵守可能なポリシーに更新しなければならない。

3.2 情報セキュリティ計画および予算案の作成・評価
　全学ネットワーク運用管理責任者は、評価・見直しの結果を踏まえ、ネットワーク委員会の審議を経て、次年度の情報セキュリティ計画およびそれに必要な予算案を作成しなければならない。情報セキュリティ委員会は、これらの計画や予算案を評価しなければならない。

3.3 報告義務
　最高情報セキュリティ責任者は、大学協議会ならびに教授会に評価・見直しの結果を報告しなければならない。さらに、その要約を全学の構成員に提示しなければならない。

４．施行期日
　本対策基準は、平成１６年１１月１日より施行する。