情報セキュリティ対策ロードマップ（俯瞰図）

SAMPLE

※報告書の一部を抜粋

	優先度：極高 重要性・緊急性が共に高い	優先度：高 重要性は低いが緊急性は高い	優先度：中 重要性は高いが緊急性は低い	優先度：低 重要性・緊急性共に低い
マネジメント対策領域	**【M-1-01】個人情報保護関連規程類等の見直し（1-1,1-4）** ・プライバーポリシーの見直し、情報主体への開示・訂正・利用停止・削除などに係わるプロセスの策定・見直しなど、2022年4月の個人情報保護法に対応した個人情報保護関連規程類、個人情報の取り扱いに係わる業務フロー・手順の整備・見直しを早急に実施する。	【M-2-01】情報セキュリティポリシーの策定（1-1） ・情報セキュリティに係わる基本的な考え方を示した情報セキュリティポリシー文書を策定する。 ・策定にあたっては、社内規程、およびISO27000シリーズなどの情報セキュリティに係わるグローバルスタンダード等を考慮する。	【M-3-01】情報セキュリティ推進体制の整備（1-2） 【M-3-02】重要情報（重要情報資産）の棚卸（1-4,1-5） 【M-3-03】情報管理基準の策定（1-4, 2-3）	【M-4-01】リスク管理基準の策定（1-3） 【M-4-02】情報資産管理基準の策定（1-5） 【M-4-03】媒体管理基準の策定（1-6） 【M-4-04】人的セキュリティ管理基準の策定（1-7） 【M-4-05】業務委託管理基準の策定（1-8） 【M-4-06】教育・訓練計画の策定（1-9） 【M-4-07】点検・監査計画の策定（1-10） 【M-4-08】セキュリティ区画基準の策定（2-1） 【M-4-09】入退室基準の策定・実装／実施（2-2）
システム（技術的）対策領域	**【S-1-01】マルウェア対策の実装・実施（3-6,4-2）** ・社員等が業務上使用する端末にはマルウェア対策機能が標準実装されているものの、現在のセキュリティ動向を踏まえると必ずしも十分とは言えない。 ・CISが推奨するセキュリティ設定を行うとともに、マルウェア対策ソフトを導入して、増大する脅威に対応することを推奨する。 **【S-1-02】バックアップ／リストアの実施・実装（4-6）** ・システム・データのバックアップ・リストアの実装・実施に係わる方針・ルールの策定する。 ・AWS RDSが提供する「DBインスタンス暗号化」の有効化によるバックアップデータの暗号化、RDS以外に保存されている重要情報のバックアップ取得および必要に応じたオフライン保管の実施を推奨する。	【S-2-01】パスワード強度（複雑性）の強化（3-3） ・情報主体に提供しているパスワード設定機能において設定可能なパスワード強度（複雑度）を高めることを推奨する。 ・インターネットの安全・安心ハンドブック（NISC）、CIS ・Password Policy Guide、NIST SP800-63などのガイドライン等を参考に強度（複雑性）の見直しを検討する。 【S-2-02】信頼できる時刻ソースとの同期（3-5） ・セキュリティ監視機能を用いたシステムに対する不正アクセスを確実に検知するとともに、万が一、不正アクセス等を受けた歳に被害の状況・原因等を的確に把握するためにも、すべてのシステム環境において信頼できる時刻ソースと同期する。 【S-2-03】セキュリティ監視機能の実装・実施（3-5） ・生成するログの決定、取得、見直しおよび監視機能の実装、不正アクセス・改ざんの検知・防止機能の実装・実施に係わる方針・ルールを定め、これらの機能を実装・実施する。 ・必要に応じて、SOCサービスの利用も検討する。 ・脆弱性診断において指摘しているAWS環境におけるログの取得、アラートの設定等への対処も検討する。	【S-3-01】NWセキュリティ対策の明文化（3-1,3-2） 【S-3-02】ID管理、識別・認証ルールの明文化（3-3） 【S-3-03】アクセス制御条件の設定・実装（3-4） 【S-3-04】重要情報（データ）の暗号化（4-1） 【S-3-05】システム故障対応機能の実装（4-5） 【S-3-06】システム故障対応ルールの明文化（4-5）	【S-4-01】システムセキュリティエンジニアリング基準の策定・実施（4-1,4-2） 【S-4-02】システム開発環境管理基準の策定（4-3） 【O-4-03】システム維持管理ルールの明文化（4-4）
運用対策領域	【凡例】 XXXX：開発・構築等が必要な対策 XXXX：ルール・手順等の策定が必要な対策	【O-2-01】脆弱性対応ルールの策定・実施（5-2） ・脆弱性対応プロセス（認識プロセス、分析プロセス、対応プロセス）を踏まえて、脆弱性対応ルールを策定する。 ・特に、分析プロセスにおける収集する脆弱性情報に対する対応基準（CVSSなどを用いた重大度／優先順位付けのための基準）を定め、これに基づいて対応および対応状況管理を実施する。	【O-3-01】インシデント対応ルールの策定・実施（5-1） 【O-3-02】事業継続計画の策定・実施（5-3）	