５．今回の不正アクセスに対する対応と、今後の対策について

システム会社での再発防止策

・被害にあった機器の入れ替え
・被害該当箇所のセキュリティの再設定（管理者 ID・パスワードを強度の高いものに変更、該当外部機器のポート閉鎖）
・新たなセキュリティシステム「Acronis Cyber Protect」を導入、24 時間のフル監視を行う。

弊社からシステム会社へ、下記の再発防止策を実施するよう指示

・委託業務にて使用するサーバーのメンテナンス計画及び実績をシステム会社にて毎月記録し、１か月に１度、弊社へ報告すること。
・システム会社にて新たに導入したセキュリティソフトによるサーバーの常時監視を実施すること。
・セキュリティソフトによる状態報告をシステム会社で確認すること。
　また、状態報告は１か月に１度、弊社へ報告すること。
　ただし、エラーなど問題が発生した場合は、直ちに弊社に連絡を行うこと。

弊社社内での再発防止策

・弊社社内での個人情報保護に関わるルールの周知徹底