

検証委員会からご指摘頂いた事項

1. 不正アクセス事案および発覚後の対応が遅れたことに関する原因分析

不正アクセス事案に対する原因として、①情報保護の体制が不十分であったこと、②ProjectWEB に対する人員・予算の制約等からセキュリティの強化・管理に手が回らなかったこと、③不正アクセスを直ちに検知する体制が整っていなかったこと、④各テナントの管理に係る事項の多くがテナント管理者に委ねられていたこと、のご指摘を頂きました。

また、発覚後の対応の遅れの原因として、①個別プロジェクトのインシデントとの前提で対応していたこと、②属人的運用やログ管理不適切により ProjectWEB の構造の把握に時間を要したこと、③ProjectWEB のシステムの性質につき共通認識が乏しく被害可能性のある情報の重要性・業務影響の想定が困難だったこと、④セキュリティインシデントに対応する体制が効果的に機能しなかったこと、⑤セキュリティインシデントにおける迅速な対応を阻害する風土や準備不足があったこと、⑥顧客先等への対応姿勢が適切でなかったこと、が指摘されています。

こうした事態を招いた真因の分析として、①ProjectWEB が当初想定されていたよりも幅広い環境や目的でなし崩し的に利用され、ProjectWEB の性質や利用状況に沿った取扱いがなされていなかったこと、②富士通の組織体制が縦割りの傾向にあり、それを反映して社内システムの管理が全社一元的あるいは中央集権的になされていなかったこと、③業務上の利便性やコスト削減の意識から情報管理やセキュリティが優先されない場合があったこと、④インシデント対応において主体的に先手を打とうとする姿勢が十分でなかったこと、のご指摘を頂きました。

2. 検証委員会による再発防止の提言

以上の原因分析での指摘事項および富士通における再発防止策の検討・実施状況を踏まえ、報告書では、以下の再発防止策の提言を頂きました。

- (1) 社内 IT システム等におけるセキュリティの充実
- (2) 不正アクセスや脆弱性を直ちに検知し、即座に対応する組織の整備
- (3) 社内 IT システムの一元管理及び各システムの位置付けの明確化
- (4) セキュリティ意識の全社への貫徹に向けた教育・意識付けの徹底
- (5) 関係当局とのコミュニケーションの充実等
- (6) 情報管理やセキュリティを業務上の利便性やコスト削減に劣後させない風土醸成
- (7) インシデント発生時における社内外への情報伝達の改善
- (8) その他富士通において更に検討すべき事項（風土改善等）