2011 年 3 月 23 日

マイポータル機能の開発に留意すべきこと

奈良先端科学技術大学院大学
情報科学研究科 教授
山口 英

1. マイポータル運営機関に対する監査強化が必須

マイポータルで提供される機能は、利用者からの情報保有機関に蓄積される個人情報へのアクセスを中継すること、そして情報保有機関に対する申請処理を中継することだ。このことから、マイポータルには、様々なセンシティブな個人情報が中継される。このため、マイポータル運営機関における情報漏洩、あるいは、職員による不正な情報取得が発生することは厳に避けなければならない。マイポータル運営機関における情報漏洩・情報不正取得対策の有効性等を確保するためには、運営組織自らが行う対策実施に加え、第三者監査により適切な対策実施の確認が必要になることは明らか。この監査では、(1)運営体制を評価するISMS的な静的なマネージメント監査、(2)マイポータル機能に対する第三者機関による実時間でのログ確保(運営機関によるログ改ざんへの対抗)と監査の実施、(3)マイポータル機能を実装するシステムのソースコードレベルでの検査・監査が必要である。マイポータル機関、およびその職員による個人情報の取得リスクを考慮し、国民に安心感を与えるためにも、さまざまな監査機能の実装が必要である。

3 月 4 日の意見書にも述べたが、マイポータル運営機関、情報連携基盤運用機関、および情報保有機関における情報不正取得、情報漏洩、ログ改ざん等のリスクは明確に存在し、過去の様々な行政機関における不祥事を勘案しても、発生しうるリスクである。これに対抗すべき合理的な機能実装は必須である。前回WGで提案した、第三者機関におけるログの集中管理は一つの解決方法である。行政機関における不正行為に対抗するための機構検討を早急に行うべきだ。

2. マイポータルの認証システムに対する想定リスクを明確にしろ

資料2, p1 には「住基ネット訴訟に係る最高裁判決に対応するためには、マイポータルにログインするための本人認証は、高いセキュリティレベルに対応

できる認証方法とするなど、個人情報保護の観点や情報の一元管理を回避する厳格な仕組みが必要であり」との説明がある。一般に、情報システムでの認証システムのセキュリティレベルを検討する場合、認証システムに対する想定リスクを明確にし、その想定リスクに応じて強度を設計することが一般的だ。最高裁判決は一つの達成目標を与えているが、合理的な対応を考えるためのリスクシナリオを与えているわけではない。

したがって最高裁判決が求める達成目標を勘案しつつ、適切な想定リスクを設定し、設定した想定リスクを広く公開して評価を求め、その上で合意された想定リスクに応じた認証強度を設計すべきだ。

現在の事務局による作業は、全く合理性が無い。

3. 実行する処理のレベルに応じた認証手段を提供すべき

本人確認を必要とする様々なサービスを考えた場合、実行する処理に応じた、異なる強度の認証手段を複数提供するのが当たり前になっている。押印を考えてみた場合、認印もあれば、実印を使う場合もあり、さらには印鑑証明を添付することもある。このような処理レベルに応じた複数手段提供は、我々の社会では普通になっている。また、現在の行政事務でも同じような考え方が導入されている。

しかし、マイポータルの検討では、最高強度の認証手段を提供すれば、それで全てが解決するという、あまりに安易な考え方に支配されている。このような最高強度の認証手段のみを提供して「これでよし」とする対応は、ユーザの利便性を阻害するリスクを高め、必要以上の費用負担を利用者に強いることになる。

対象とする申請プロセス、情報参照プロセスを精査し、処理レベルに応じた認証手段を提供することが必要だ。

以上。