

電子政府ガイドライン作成検討会 セキュリティ分科会(第6回)
議事概要

1.開催日時:平成21年3月23日(月) 18時00分~20時00分

2.場 所:内閣府別館9階会議室

3.出席構成員:

辻井セキュリティ分科会主査、

荒木構成員、岩下構成員、宇賀構成員、小松構成員、佐々木構成員、中尾構成員、満塩構成員、
須藤座長、大山構成員、遠藤構成員

(オブザーバー)(敬称略)

安心・安全インターネット推進協議会/日立製作所システム開発研究所 洲崎

セコム株式会社IS研究所 松本

NTT情報流通プラットフォーム研究所 高橋、坂本

(参加府省)

総務省行政管理局長屋行政情報システム企画課長

総務省行政管理局行政情報システム企画課北川調査官

総務省自治行政局地域政策課中垣内補佐(代理)

総務省自治行政局井上地域情報政策室長

総務省自治行政局市町村課村山専門官(代理)

総務省情報流通行政局情報流通振興課新井情報セキュリティ対策室長

法務省民事局総務課堀補佐官(代理)

法務省民事局杉浦補佐官(代理)

国税庁長官官房上斗米企画課長

厚生労働省大臣官房統計情報部企画課情報企画室野中補佐(代理)

厚生労働省労働基準局労働保険徴収課江口係長(代理)

社会保険庁総務部総務課澤田情報企画調整室長

経済産業省商務情報政策局情報経済課三角情報セキュリティ政策室長

4.議事次第

(1) 開会

(2) リバティ・アライアンスの取り組みについて

(3) セキュリティ分科会中間報告案について

(4) 閉会

5. 資料

< 配布資料 >

資料1 リバティ・アライアンスの取り組みについて

資料2 セキュリティ分科会の検討状況(案)

< 席上配布資料 >

参考資料1 セキュリティ分科会(第5回)議事概要

6. 議事概要:

資料1「リバティ・アライアンスの取り組みについて」について、NTT情報流通プラットフォーム研究所の高橋プロジェクトマネージャー及び坂本主任研究員から説明が行われ、以下のような質疑応答が行われた。

- ・ IAF (Identity Assurance Framework)は、米国発の流れであり、OMB M-04-04 や SP800-63 の規定するレベル自体にはまだ議論があるものの、これらのフレームワーク自体はヨーロッパ、オセアニア、その他の国も積極的に参加しており、グローバル化に向かっている。ITU や ISO での議論についても反映させていく予定。また、SAML の設計思想には、信頼関係の構築の一環として、署名を打つことなど、否認防止の必要性について最初から含まれている感じである。
- ・ ID-WSF (Identity Web Services Framework) は同意に基づくアイデンティティに対する属性情報の交換を安全にする仕組みであるが、これはユーザから属性情報提供の許可を得ることにより、ユーザの正当な代理人であるということを保証する意味で、サービス提供者が IdP (アイデンティティ提供者) からアクセス鍵を受け取り、ユーザの属性情報を使用できるというもの。実用化については、実験段階。
- ・ IdP の実施組織は政府系が多いが、第三者(民間)がやるモデルを試行している国もある。EU 加盟国は、域内のどこにいても同じサービスが受けられるようデータベースの相互アクセスができるようにしたい事情があり、SAML2.0 のような枠組みを必要としている。
- ・ アイデンティティ連携の保証レベルは、金融、医療など高いレベルが必要とされる分野の場合は、規制により基準なりが求められ民間のみではできなかった。それらお墨付きのものと連携することにより民間のビジネスにすることを目指したもの。
- ・ SAML2.0 のシングルサインオンの特徴として、仮名を使ったアカウント連携があるが、一般的な民間サービスを想定しており、そのまま匿名サービスを前提としていない行政サービスに使えるモデルであるかは疑問だが、官民連携する場面ではこのようなモデルが有用な場合もあるのではないか。
- ・ 電子認証ガイドラインを作っている国と SAML による連携をしている国の相関が高い。シングルサインオンができるようになるためには電子認証ガイドラインのようなガイドラインが重要である。

資料2「セキュリティ分科会の検討状況(案)」、資料2:別紙1「認証の保証レベルの考え方」、同:別紙2「重点手続再点検の状況(中間報告)」、同:別紙3「リスク評価の考え方」及び同:別紙4「今後の検討事項について」について説明が行われ、以下のような質疑応答が行われた。

- ・ 対象のシステム別にトータルとしての保証レベルをクリアした上で、対策をどうとるのは総合判断となるものであり、このままの進め方で良いのではないか。
- ・ 保証レベルのあり方、実装については、各府省庁にまかせるのではなく、次世代電子行政サービス基盤等検討プロジェクトチームとの連携をとりつつ、整理するべき。
- ・ 登録、発行・管理といったIDマネジメントは、IDの信頼性の観点から、認証に限った話ではないので、広い範囲で考えるべきである。
- ・ 今後の検討事項について、ユーザビリティ向上の観点からの実現上の課題は、ユーザビリティ分科会と調整をしながらになるが、認証基盤のユーザビリティは、セキュリティ分科会でやることになっている。シングルサインオン等の認証における使い勝手は、今後当分科会で検討することになる。
- ・ 小手先の議論ではなく、システム側でセキュリティの要素を含めた安定的な挙動を保証してくれるディペンダブル・コンピューティングという枠組みで社会システムを捉えることが必要であるが、まずは電子署名を含めた認証とセキュリティを考えるのが当分科会の使命である。
- ・ セキュリティ分科会は、各府省庁が十分な検討を行うためのわかりやすいインデックスをガイドラインの形で与えることを第一義とし、将来ビジョンも多少入れることになる。
- ・ リスク評価の進め方としては、手続きごとに、なりすまし・改ざんなどによる影響の洗い出し
影響の程度の判定 保証レベルの仮導出 仮導出した保証レベルの検証 に戻る、
のサイクルを何度か回し、適宜見直しをしながら、適切なレベル感を探っていく。

以上