**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５回）**
**議事概要**

**１．開催日時：平成２１年2月２７日（金）　１０：００～１２：００**
**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、小松構成員、佐々木構成員、中尾構成員、満塩構成員、**
**（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**
**（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）**
**国税庁長官官房古賀情報技術室長（代理）**
**厚生労働省大臣官房統計情報部企画課佐々木情報企画室長**
**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) 検討スケジュール等の見直しについて**
**(3) 保証レベルとリスク評価の考え方**
**(4) ガイドラインの内容案について**
**(5) 閉会**

**５．資料**
**＜配布資料＞**
**資料１　　セキュリティ分科会のスケジュールの見直しについて（案）**

資料２－１　『電子政府認証ガイドライン検討報告書』における保証レベルとリスク評価の考え方
資料２－２　リスク評価の進め方について
資料２－３　電子署名・認証の保証レベルについて
資料３　ガイドラインの内容案について

＜席上配布資料＞
参考資料１　セキュリティ分科会（第４回）議事概要

６．議事概要：

○ 冒頭、辻井主査より、検討スケジュールの見直し等について説明が行われた。

・ 本分科会のガイドラインは３月末に取りまとめる予定であったが、次回会合では中間取りまとめに留め、最終的なとりまとめは９月末とすることとした。他方、ユーザビリティ分科会のガイドラインは、平成 22 年度予算要求への検討スケジュールを考慮し、予定どおり 3 月末に取りまとめることとした。
・ セキュリティとユーザビリティのガイドラインを１つにまとめる予定であったが、スケジュールに差があるため２つのガイドラインに分けることとし、また、各々の内容に矛盾が生じないようにするため内容を調整することとした。
・ これらの内容について、次回開催の親会にて決定する予定。

○ 事務局より資料１、資料２－１及び資料２－２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。

・ 幾つもの方式が分散して、それぞれ違うものを使わなければならなくなると使い勝手が悪くなる。個別のリスク評価を行った後、トータルコストやユーザビリティの観点からの補正のプロセスは必要。
・ セキュリティ以外も含めて、トータルでどのように設計するかについては、コンサル等のディシジョンにゆだねられているため、判断基準がバラバラになるのではないか。トータルでのディシジョンに向けて、セキュリティ分科会でガイドラインの対象とする範囲がどこまでで、その先にどのような論点があるかの線引きが重要。
・ 低い保証レベルを要求する手続に入った後、高い保証レベルを要求する手続に入る時に、新たな認証を要求するような仕組みは技術としては存在するが、仕様を決める際には対象システム固有の問題も考慮しなければならない。保証レベルと実装の話は区別して考える必要がある。
・ リスクの影響度の詳細定義も必要であるが、リスクの影響度と保証レベルのマトリックスの作り方によって結果は幾らでも調整出来てしまうので、マトリックスの作り方には特に力を入れるべき。

・ 最終的な実装の問題に答を出すためにも、まずは電子政府サービスのリスク評価を行うための基準を整備するべき。その上で何が足りないか考え、その部分についての参考や指針となる資料を作成していく。

○ 資料２－３「電子署名・認証の保証レベルについて」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。

・ 保証レベルを決めた後、実装を決めるためにはコストやユーザビリティについても考える必要があるため、その部分に対するガイドなり、もう１段階工夫を考える必要があるのではないか。

・ 実装について考えると、認証だけでなく署名についても保証レベルを考えることが重要。その際、認証と署名で別々に保証レベルを定義するとともにその間のリンク付けをするのか、もしくは認証と署名を合体させた保証レベルを定義するのかについては非常に難しい論点。署名については、否認ではなく、改ざん防止という観点でレベル分けを考えることになると思うが、法的な話を踏まえた論点の整理が必要。

・ 認証の保証レベルについては、国際標準の議論がスタートしたばかり。２月に開催されたＩＴＵ－Ｔ ＳＧ１７会合では、ニュージーランド、米国 Telcordia Technologies 社（旧ベルコア）、米国政府からＩＴＵ－Ｔ勧告 X.eaa（Entity Authentication Assurance）の作成に向けた文書が入力されており、次回は６月中旬にフランスで議論が行われる予定。他方、ＩＳＯでも同じもの（WD29115）を踏まえ、５月中旬に北京で議論される予定。

○ 資料３「ガイドラインの内容案について」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。

・ 後々、ガイドラインをどのように適用していくのかについて整理が必要となる。どこまで整理出来るのかは、トータルでのデザインや実装についての検討をどこまで進められるかに依存するため、今後の議論の状況を見ながら整理を行う。

・ 分かりにくい分野であるため、ユーザーズガイドのようなものが必要ではないか。また、一番単純な評価方法を示すため、適用事例等を入れるべきではないか。

・ 仮にデファクトスタンダードを無視した国際標準が出来上がったとすると、政府調達の現場では国際標準に合わせるために相当なコストが発生する。

・ そのような事態を回避するために、国際標準の役割を考える必要がある。また日本から積極的に国際標準に対して何か発信するべきではないか。出すのであれば、次の会合で日本から文書を入力するのがタイミングとしてベストであり、スモールグループを作って議論してはどうか。

・国際標準は、概念の統一や、国際競争力を高めるという観点にはつながるが、政府に適用するガイドラインという観点では、逆にコンパクトな規模を対象としたものの方が現場には有用。また、自国で実践しているガイドラインがあれば、国際標準への提案が可能だが、

**日本はまだガイドラインも無い状況なので、提案は難しいのではないか。**

**以上**