

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3回）会合
議事概要

1. 開催日時：平成20年12月12日（金） 16:00～18:30

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、佐々木セキュリティ分科会主査代理、
荒木構成員、小松構成員、猿渡構成員、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 甲斐（代理）

セコム株式会社 I S 研究所 松本

凸版印刷 野村

野村総合研究所 崎村

（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情報セキュリティ対策室中村補佐（代理）

法務省民事局総務課堀補佐官（代理）

法務省民事局相澤商事課長

国税庁長官官房情報技術室藤田補佐（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佐々木補佐（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

経済産業省商務情報政策局情報経済課情報セキュリティ政策室下里係長

4. 議事次第

(1) 開会

(2) 電子署名の運用状況

(3) 電子署名及び認証業務に関する法律における「推定効」について

(4) ユーザインタフェースに関する技術動向

(5) 閉会

5. 資料

<配布資料>

- 資料 1-1 商業登記に基づく電子認証制度
- 資料 1-2 電子署名及び認証業務に関する法律の施行状況等について
- 資料 2 電子署名及び認証業務に関する法律における「推定効」について
- 資料 3-1 暗号アルゴリズム SHA-1 及び RSA 1024 に係る移行指針
- 資料 3-2 格納媒体の多様化ならびに技術動向について
- 資料 3-3 分散認証 (Web-SSO)

<席上配布資料>

- 参考資料 1 セキュリティ分科会 (第 2 回) 議事概要
- 参考資料 2 電子政府評価委員会 平成 19 年度報告書 (抄)
「参考資料 3 オンライン申請システムの利用に関するアンケート調査について」

6. 議事概要 :

- 資料 1-1 「商業登記に基づく電子認証制度」及び資料 1-2 「電子署名及び認証業務に関する法律の施行状況等について」説明が行われ、これらについて、以下のような質疑応答が行われた。
 - ・ 商業登記に基づく電子認証制度においては、利用の範囲に限定がないため、どのように利用されているかを把握することはできないが、電子入札を含め、広く利用されていると思われる。
 - ・ 電子署名法に基づく場合についても、社長が自然人として使っている法人利用かどうか、利用実態は把握していない。
- 資料 2 「電子署名及び認証業務に関する法律における「推定効」について」を説明。これについて、以下のような質疑応答が行われた。
 - ・ 印影がその人の実印で押印されたものであることが証明されれば、私文書の成立の真正が推定される。この推定を覆すに当たり、実印は厳重に保管しているのが社会的な常識であるので、裁判所の個々のケースごとの判断によるところではあるが、単に実印が盗まれたというだけでは、この推定を覆すことはできないのではないか。
 - ・ 秘密鍵の取扱いについての社会的な常識がどのようなものかによって裁判所の判断が変わってくると考えられる。秘密鍵が厳重に保管され、容易に配布されないものであることが社会的な常識であれば、当該秘密鍵を用いたことだけでその本人が秘密鍵を用いたという推定が働くと考えられるが、秘密鍵が容易にコピーされて配布され得るものであることが社会的な常識であれば、当該秘密鍵を用いたことだけの立証では不十分で、当該秘密鍵を用いたのは本人である

ことの立証が必要となると考えられる。

- ・ 「文書の成立の真正」と「文書の記載内容の真実性」とは別次元の問題である。例えば、作成名義人が見聞きしたものを報告する文書の場合には、作成名義人が本人であれば、当該私文書が真正に成立したといえるが、報告されている内容が真実であるとまではいえない。
- ・ 政府への申請・申告と推定効との関係を考えるに当たって、民事訴訟法における推定効を離れて、独自の推定効のようなものを議論することによりあまり実益はないのではないかと。申請書、申請内容が申請者の意思に基づくものかどうか争われたときに推定効が問題となる場合、これは正に民事訴訟法における推定効の議論そのものである。
- ・ 印影の偽造は電子署名の偽造よりはるかに容易にできる。民間では訴訟リスクを保険で対応することにより、ビジネスを展開している。医療などきわめてセンシティブな情報を扱う場合には、厳密な手続きが必要だと思うが、簡易な手続きまで行政官のリスク回避のために、厳密な手続きを国民に負わせている。利便性が落ちれば、利用されなくなって、何のためにやっているのか、となってしまう。総合的な判断により最適解を考えるべき。
- ・ 商業登記自体は、公文書であるが、民事訴訟法上、私文書と異なり、公文書がその方式及び趣旨により公務員が職務上作成したものと認めるべきときは、当該公文書は、真正に成立したものと推定することとされている。
- ・ 公文書については、厳密に言えば、タイムスタンプが必要で時刻認証がなければ原本性の保証はできない。
- ・ 電子署名をどこに使うかが問題。主な手続きについて、各省に電子署名を要する手続きについて、紙申請ではどの程度の本人確認、改ざん防止を行っているのか等についてアンケートを実施し事実確認をしているところ。取りまとめ次第、リスクの考え方を議論する。

○ 資料 3-1 「暗号アルゴリズム SHA-1 及び RSA 1024 に係る移行指針」を説明。これについて、以下のような質疑応答が行われた。

- ・ 安全性の問題を考えると、例えば、RSA2048 より RSA3072 の方がより安全であるが、あえて RSA2048 を採用したのは、ここ何年かで製品化され、入手しやすいものという観点からである。

○ 資料 3-2 「格納媒体の多様化ならびに技術動向について」を説明。

○ 資料 3-3 「分散認証 (Web-SSO)」を説明。これについて、以下のような質疑応答が行われた。

- ・ 例にあるA社は、ユーザー側で署名をするのではなく、A社認証サーバで署名する。ボタンを押すことが一種の契約行為で、トークン確認をして本人を限定。ログを残し監査等に供することにより、一定の否認防止の状況を作っている。
- ・ 連携認証の場合、どちらがどこまでやったのかの証拠を残す必要がでてくる。また、どのレベルの認証が必要かのポリシーが必要。

- ・ SAML と OpenID の技術的互換性確保は、双方のコミュニティで密接にやっており、難しくないだろう。そのためアシュアランス・フレーム・ワーク、認証レベルの互換性確保、をきちんとやらなければという話になっている。リバティも OpenID もアシュアランス・レベルとして SP800-63 を参照していく傾向であり、5 レベル(4 レベルとそれ未満のレベル)が標準になっている印象を受けている。
- ・ 暗号の危殆化については、ライブラリの実装が広く行われているものでないと民間で採用してもらえないので、それを許容しつつ、高レベルのものを推奨している。

○ その他

- ・ 電子署名と一括りに言っているが、実際には法的な拘束力を持つものと持たないものがあり、使い分けるための用語を検討すべき。
- ・ 危殆化の話があったように、継続的にリスクの見直しをする必要があり、過信的に電子署名なら良いという流れはまずい。厳密にするとところと逆に利便性を高めるところと適用範囲を整理していくのが方向性ではないか。
- ・ 当分科会でのガイドライン検討では、本人の確認などのセキュリティ技術として ID/パスワードや電子署名など様々な技術の順序立てを整理、サービスの内容によりどの程度のセキュリティがふさわしいか議論し、サービス運用側が選択できるようにするところまでか。
- ・ 基本的にはそうだと思うが、さらに組織間のデータベース連携によりワンストップサービスが実現した際のセキュリティはどうあるべきか、官官、官民の場合について、決済系も含めて、合理的な段階数でレーティングすべきである。
- ・ 紙による申請がオンライン申請になるというだけでは、社会的インパクトもニーズもない。行政側がもつ様々な情報をお互いにやりとりしあい、個人情報、年金、税金、医療、福祉等々の情報に自分だけが自分のプライバシーを守りながら普通にアクセスできる、ワンストップで利用できるといったサービスが今後は大事。
- ・ 今年度のタスクとして、分類の基準の考え方を示すというはあるが、これまでの議論で長期に戦略的に考えなければいけないことが明らかになっている。例えば、官民連携のポータルを立ち上げた場合、民間サービスの本人確認との連携をどう行うのか。決済系をどうするのか。やるべきものと、できないものを、戦略をもって検討すべき。
- ・ 環境が異なれば、行動も異なるので、これまでの環境では使われなかったオンライン申請も環境が変われば使われるかもしれない。したがってシミュレーションはデータに基づいて完璧にやらないといけない。また、自治体によってやり方が違うものを政府と連携しないといけないので、このあたりの調整も必要になる。
- ・ 分科会でのタスクは与えられた期間でやりつつ、大きいことも同時に考えながら常にループで議論を進めていかないとけない。

以上