電子署名法研究会（平成２８年度第４回）
議事要旨

日時：平成２９年３月１４日（火）　１５時００分～１７時００分
場所：経済産業省別館１階１１４各省庁共用会議室

構成員

電子署名法研究会構成員（敬称略）
　手塚構成員、大澤構成員、長尾構成員、永田構成員、佐々木構成員、松本鋭一構成員、
　松本泰構成員、宮内構成員、茗原構成員
WG 構成員（敬称略）
　佐藤雅史構成員、西山構成員、濱口構成員、政本構成員、宮崎構成員、山岸構成員

議題

（１）電子署名法との関連整理について
（２）リモート署名構成図の修正について
（３）リモート署名検討の論点
（４）その他

議事概要

　事務局より「電子署名法との関連整理について」、「リモート署名構成図修正内容」、「リモート署名検討の論点」の説明が行われた。各構成員等からの意見、質疑は以下の通り。

（１）　電子署名法との関連整理について

・　符号や物件の適正な管理は、法３条の括弧書きによる要件ではなく「本人による」という要件にかかわるものである。括弧書きは、直前の「電子署名」を制限するものであって、「本人による電子署名」を定義しているわけではないという解釈が多いのではないかと思う。括弧書きは、「符号や物件を適正に管理すれば本人しかできない」性質を持つ仕組（署名方式等）を使うことが要件であって、符号や物件が実際に適正に管理されていることが要件なのではない。そのため、適正な管理の方法については、法３条括弧書きとの関係で論じる必要はなく、法３条本文の「本人による」という要件との関係をわかりやすく表現するのがよい。例えば、“法３条にある「本人による」が認められるためには、少なくとも〇〇を実施しておかなければならないと考える”というような流れでまとめるとよいのではないか。
・　p44 の文章では、「ログを記録する」とあるが、ログを記録することが本人によ

る電子署名であることを担保するものではない。ログと本人によるということの関係の解釈は明言できないので書き方に注意すべきである。

- 「(1) 署名鍵の管理・利用について」は、法３条に関する記載であることがわかるように修正すべきである。
- 「(2) 署名鍵の生成・送付について」は、施行規則６条３号、３の２（利用者が作成する場合）、３の２（利用者がリモート署名事業者に依頼する場合）との関連を説明すべきである。
- 双方について、想定している問題点を記載すると、何のための記載か分かりやすいだろう。
- サイバー関係の保険対象はまさに議論しているところである。保険については、リスク移転策の一つにはなるが、どの範囲を対象とするかの具体化まで整理を行っていないのであれば、今回の検討内容に「保険」という言葉は使用しない方がよいだろう。
- 「リモート署名利用者の管理下」とあるが、適切な表現でない。具体的に記載するか、“利用者の意思に基づき／従って適切な管理がされている”等の記載がよいのではないか。

（２）リモート署名構成図の修正について

- Hash 値生成機能、SCM 活性化機能、署名フォーマット構築機能を点線で括っている意図は何か。
- 利用者確認の結果を受ける機能として、Hash 値生成機能、SCM 活性化機能、署名フォーマット構築機能を点線で囲った。
- 利用者認証機能、利用者情報機能、利用者情報 DB の通っている線の意図は何か。
- 相互に関連していることを表現している。
- そうであれば、利用者認証機能、利用者情報機能、利用者情報 DB も同様に点線で囲うべきだろう。
- SCM-C が、SCM 活性化機能を通過（スルー）しているように見える意図は何か。
- 誤りである。
- 同様に署名検証機能もリポジトリから矢印が通過しているので修正が必要だろう。

（３）リモート署名検討の論点

- 図４．１のプレイヤ同士をつなぐ線の意味がよく分からない。
- 図４．２の（２）リモート署名のモデルの CSP 吹き出しの２ポツ目「IdP」の文章は記載しない方がよい。「IdP」は、詳細説明のときに登場させる方が適切である。

・ 4.1.3「プレイヤの役割」の前に、4.3「リモート署名のライフサイクルと処理フェーズ」を記載した方がよい。

（4）その他

・ 本日の議論を踏まえて整理すると、電子署名法研究会としては、今まで議論してきたリモート署名と電子署名法との関連や、リモート署名を実施する際の検討ポイントが主題となるため、それらを前に出すように章構成の変更した方がよい。
・ いろいろな箇所で出ている「意志」を「意思」に修正。
・ また、「SCM-C」と「PIN」の使い分けを明示すること。
・ 「リモート署名事業者」の方が読み手にとって第三者に委託することのイメージがつきやすく分かりやすい。
・ リモート署名提供者が、Remote Signature となっている。違和感があるので修正した方がよい。
・ Remote Signer も日本語と対応していないため、検討した方がよい。
・ 表 4-12 の wrap 鍵と Unwrap 鍵は共通鍵系なのか公開鍵系なのか。wrap 鍵と Unwrap 鍵と同じものであるなら、それが分かるように修正した方がよい。
・ 「鍵生成時に鍵の属性を考慮に入れて生成を行う必要がある。」という文章があるが、「鍵の属性」とは何を意味するのかを説明する必要がある。「鍵属性管理」も同様である。
・ 「復号に利用する鍵は暗号対象鍵と同等の暗号強度を持つことが望ましい。」とあるが、鍵が強度を持つという表現は適切でないので修正する必要がある。
・ 4.5「登録フェーズ」に、電子認証ガイドラインと無理矢理対応づけられているので違和感ある。この章までの用語の定義も引用しているガイドラインと本報告書では異なるので、ガイドラインを参照していることを簡単に書き、引用箇所を参考として記載すればよい。
・ 表 4-9 や 4-10、4-11 も同様である。
・ 表 4-8 に「アサーション」が出ているが、以降にアサーションは出てない。この表自体も不要ではないか。
・ 「7.2 構成員」の表 7-1、7-2 に「後日修正予定」とあるが、修正する内容は何か。
・ 五十音順に並び替える作業である。

お問合せ先
商務情報政策局 サイバーセキュリティ課
電話：０３－３５０１－１２５３
FAX：０３－３５８０－６２３９