平成 24 年度　電子入札コアシステム利用者会議･特別会員会議　議事要旨

日時：平成 25 年 1 月 25 日(金)13：30～15：00
場所：日本青年館ホテル　3 階　国際ホール

1. 議事次第

（1）開会
（2）主催者挨拶　（一般財団法人日本建設情報総合センター理事　坪香　伸）
（3）議事
　1）利用者会議・特別会員会議　合同開催の経緯
　2）コアシステム事業の状況について
　3）意見募集について
　4）暗号アルゴリズム移行スケジュールについて
　5）その他
（4）閉会

2. 配布資料

資料１　利用者会議・特別会員会議　合同開催の経緯
資料２　コアシステム事業の状況について
資料３　意見募集について
※資料４、資料５についてはセキュリティに関する事項を含むため公表は控えさせていただきます。

3. 参加者

区分	団体数	参加者数
中央省庁	5 団体	11 名
公社・機構	12 団体	13 名
都道府県	39 団体	53 名
市町村等	30 団体	35 名
コアコンソ会員	19 団体	28 名
業界団体	6 団体	7 名
合計	111 団体	147 名

※団体数及び参加者数には JACIC 関係者は含みません。

4. 会議概要

１）利用者会議・特別会員会議　合同開催について（資料１）

これまで、利用者会議と特別会員会議は別々に開催していたが、幅広く情報提供を行うことにより、事業がより一層、円滑に展開されると考えられるため、今年度は、利用者会議・特別会員会議を合同で開催することを説明した。

＜質疑応答等＞　特になし

２）コアシステム事業の状況について（資料２）

コアシステム事業の状況として、コアシステムの普及状況、平成 24 年度の事業活動、事業改善方針の実施状況等について説明した。なお、事業改善方針の「４）ユーザサポート」については、これまでの取り組みにより対応が完了したため措置済みとし、業務改善方針より削除することとした。

＜質疑応答等＞

茨城県：資料の P9、P10 のコアシステム普及状況において、当県の共同利用参加団体数が１７団体となっているが、現時点では行方市が運用中であるため１８団体となっているので訂正する。

また、コアシステムの機能充実、物品役務の強化に向けた要件定義、基本設計に関する意見募集はまだ行っているか。

事務局：現在要件定義を行っているところなので積極的に意見等をいただきたい

石川県：P6 の 2)処理速度等の性能向上に記載されている IC カードへのアクセス方法の変更とは具体的にどのようなことか。また、P7 の 5)情報セキュリティの強化のまた書きにある JRE 7 対応について update11 に対する注意喚起があったと記憶しているがその対応状況を教えてほしい。

事務局：IC カードへのアクセス方法の見直しとしては、毎回アクセスするような部分を効率化することで処理時間を時間短縮できると考えており、実際に対応を行う際は情報提供を行う。

また、JRE7 update11 の注意喚起については、重要なぜい弱性が 2 件あるところ、1 件しか対応されていないと指摘がされているが、現時点では、JRE7 update11 が最新版となっている。

これらの対応を行うためには認証局の対応が必要となる。JACIC では迅速にセキュリティ対応を行うこととしているため、コアシステム本体と LGPKI クライアントソフトについては JRE7 update11 の動作確認を実施し、コアコンソやサービスセンターの HP で動作確認が完了したことをアナウンスした。

なお、JRE7 update11 では、最初に利用した時にポップアップ画面が表示され、利用者側で許可するか判断を求められる。これらの操作についても HP にわかりやすく

掲載しているので、ご確認いただき質問等あれば事務局に連絡してほしい。

神奈川県：P6 の 2)処理速度の向上について IC カードのアクセスや DB 構造の見直しとあるが、LGPKI 専用クライアントソフト V2.1 やコアシステム V5.3 への反映はなされるのか。また、本県からの情報提供であるが、JER7 update11 についてコアシステムを利用する際に、時刻表示の時とコアマークの表示の時にポップアップが 2 回表示される。この時に同じ画面がピッタリと重なって表示されており、ひとつめの画面でボタンを押しても画面が消えないように錯覚する。また、場合によっては、どちらかの画面が別の画面の裏に入ってしまうとずっと残った状態になるので注意が必要。

事務局：IC カードのアクセスや DB 構造の見直しについて、LGPKI 専用クライアントソフト V2.1 やコアシステム V5.3 への反映は行わず、コアシステム V6 での対応とさせていただきたい。

JRE7 update11 で複数のポップアップがでるということについては、アクセスする URL 毎にポップアップがでるためそのような状態になることは確認している。

３）意見募集について（資料３）

これまでは、アンケート調査によりコアシステムに関する意見要望を募ってきたが、平成 24 年度より意見募集のホームページを新設し、年間を通じて意見要望を募ることを説明した。

なお、意見要望の募集結果は、年末締めとし利用者会議等で報告することとした。

＜質疑応答等＞　特になし

４）暗号アルゴリズム移行スケジュールについて（資料４）

暗号アルゴリズム移行の全体のスケジュールについて、政府機関の暗号アルゴリズム移行指針の改定により当初予定していた「2014 年度早期」から「2014 年 9 月下旬以降、早期に」とされたことや、電子入札システム提供者、利用者の視点の違いによる移行スケジュール等の説明を行った。

＜質疑応答等＞　特になし

茨城県：茨城県では旧暗号の IC カードを有効期限内は使いたいと考えている。しかし、内部で検討しても良くわからなかったので IC カードの取り扱いついていくつか確認したい。

① 現行の旧暗号の IC カードと暗号アルゴリズムが代わった新暗号の IC カードとは別物なのか？

② フェーズ１の期間中は旧暗号の IC カードしか使えず、新暗号のカードは使えないのか？

③ フェーズ２では旧暗号の IC カードの有効期限が残っていても使えなくなるのか？

事務局：IC カードの発行は JACIC が行っているものではないので、当方で聞いている情報を提供する。

① 旧暗号の IC カードと新暗号の IC カードは、見た目は同じでも中に格納される鍵の長さが異なるので別々のカードとして発行される。

② フェーズ１の期間中は旧暗号の IC カードしか発行されない。また、新暗号の IC カードはフェーズ２になってから発行される。フェーズ２に切り替わる１日前でも旧暗号の IC カードが発行されると聞いている。

③ 旧暗号の IC カードの利用については、フェーズ２の期間に入っても利用できると聞いている。ただし、フェーズ３になると利用できなくなるので、フェーズ３の開始時期が利用期限といえる。

資料の備考欄に書いてあるように「検証」について、フェーズ１は旧暗号アルゴリズムのみ、フェーズ２は新旧暗号アルゴリズム、フェーズ３は新暗号アルゴリズムのみとなっているのでフェーズ２の間は旧暗号の IC カードが利用できると聞いている。

茨城県：9 月に暗号移行が行われる際に、7 月にカードの期限を迎えた時に長期のカードを購入するか、短期間のものを購入して次年度に新暗号版を購入するのがよいか相談したい。

事務局：JACIC から回答することは難しいので、適切な時期にその時の状況を踏まえて、それぞれの認証局に相談いただきたい。

広島市：P15 の 7 に「暗号移行フェーズの設定を行うことができる」となっているが、これは総務省からのフェーズ２開始のアナウンスを受けて切り替える（システム上の設定をその時に行う）というイメージでよいか。

事務局：切り替えは日付を設定している定義ファイルを持つようになっており、その日付を過ぎたらフェーズ２として動くようになるので、ある日に設定の切り替え作業を行うものではない。ただし、この設定日については暗号の切り替えが１日行われるものではないので、事前にフェーズ２で動くように設定することでスムーズに移行が行われるものと考えている。

広島市：受注者の画面にコメントが表示された場合、問合せについては広島市で対応することとなるが、認証局の対応時期に関係すると思われる。これはコアシステム側で画面にコメントを表示する機能が用意されているので各自治体の判断で設定してくださいというものと考えてよいか。表示される画面で受注者側に更新を促す場合、対応が開始できる時期があると思われるが。

事務局：各民間認証局は、来年度の早期にモジュールを出す予定なので、その時点から対応可能と考えてよい。メッセージは古いクライアントソフトが使われていることを明

示するので、その時点で各自が利用している認証局に確認すれば新しいクライアントソフトを入手できるようになっている。

広島市：切り替え日はいつごろを設定することが望ましいのかアドバイスしてほしい

事務局：現在のモジュールは平成２６年４月１日を設定しているが、ゴールデンウィークや6月に設定しておき、揃って切り替える考えもある。ただし、日付を各団体で設定いただくか、コアシステムとしてリリース時に組み込むかは、影響度合いなどを検証していないので、正会員と相談して良い方法を検討したいと思う。

文部科学省：P16 の暗号アルゴリズム移行スケジュールにおいて、暗号モジュールは V5.1 から順次提供されることとなっており上期中（９月まで）には出されると思うが、最初の V5.1 用モジュールはいつ提供されるのか。

モジュールが提供されてから発注したいと考えているが、暫定予算等の関係から時期によっては後回しにできるかを検討したい。

P18 に記載されている JRE 6 のサポート切れに伴う JER 7 への切り替えについて保守業者から GPKI ラッパーの JRE 7 対応予定が分かれば教えてほしいと問い合わせがあった。

JRE 6 の有償サポートを受けることで延長されるので問題ないのであれば良いが、JRE 7 対応を実施する際に必要となるため提供されるのか、わかれば教えてほしい。

事務局：V5.1 用暗号移行対応モジュールのリリースは、6 月末を予定している。GPKI については、現時点では情報がないので別途確認するようにしたい

福岡県：P21 のコアシステムのサポートについて、本県は現在 V5.1 を利用しており、H28 年度まで使う予定となっている。V5.1 は H26.5 までがサポート期間となっているが、H26 年度末まで JRE 等のサポートを受けることはできないか。また、それ以降も要望により延期されるということにならないか。

事務局：V5.1 のサポートは H26.5 までとなっている。これは V5.1 で利用している JDK5.0 がオラクルの有償サポートを含めても H26.5 までとなっているためであり、セキュリティパッチ等を受けセキュリティが担保される期間を示している。

しかし、その後の H26 末まで色が変えてあるのはコアシステムで一番影響がある AP サーバのサポート期限が H27.3 までとなっているためである。なお、これは現時点における製品のセキュリティ対応スケジュール期間であり延長等も考えられる。

コアシステムでは、これまでもメーカーによる製品のサポート期限を過ぎたものであっても、セキュリティ対応はできないものの問合せ等は受けている。

暗号移行後は全ての利用団体が V5.1 以降となるので、引き続き問合せ等については対応し、期限については別途調整する。

福岡県：動作確認についても継続されるのか？

事務局：Java が更新された場合の動作確認は行えないが、問合せを受けた際に再現テスト等は行うようにする。

福岡県：H26 年度末以降の Java の更新等は対象外となるのか。

事務局：メーカーからは、それ以降に更新版は提供されないとされているが、緊急対応等でパッチ等が提供される場合がある。このような時は動作確認を行うようにする。

愛知県：フェーズ２と IC カードの話がでていたが、私の認識では、LGPKI の場合はフェーズ２で旧暗号の IC カードが利用できる。しかし、一度ロックしてしまうと再発行は新暗号のみとなるため新暗号の IC カードも対応しておく必要がある。

このため、先ほどの日付の定義ファイルを設定する際にゴールデンウィークや 6 月とされた場合、その時点からフェーズ２となるためカードの運用に影響がでる可能性がある。

事務局：現時点における H26 年度の想定スケジュールは、①６月（仮）コアシステムフェーズ２設定→②９月下旬（仮） GPKI 新暗号 IC カード発行開始→③９月下旬（仮） LGPKI 新暗号 IC カード発行開始→④１０月（仮） 民間認証局新暗号 IC カード発行開始となっている。③までの期間に LGPKI の IC カードが PIN ロックしても、再発行は現行暗号となると思われる。しかし、③以降に PIN ロックした場合は、ご指摘どおり、新暗号の IC カードが再発行されると思われる。これらの扱いは認証局によって異なると思われるので、各認証局から情報収集し、コアシステム関係者に情報提供していくこととしたい。

都市再生機構：P16 の暗号アルゴリズム移行スケジュールについて、当機構はスケジュールに沿って実施できるか自信が持てていないところ。暗号モジュールの適用規模を見極めるための情報提供をお願いしたい。また、スケジュールのバーチャートで年度内となっているが、フェーズ２の開始が H26.9 となっており、このバーチャートの必要性がどの程度必須なのか教えてほしい。また、前回のブロック会議で暗号移行に関する模式図を提示していたので更新版をお願いしたい。

事務局：暗号アルゴリズムの移行について質問をいただいているが、非常に複雑かつ政府等の対応も関係しており、各団体の対応も様々であるため、わかりやすい資料を準備して HP やブロック会議等で提供し引き続き質問等を受けつけていくようにしたい。

５）その他（資料５）

電子入札コアシステムに関する以下の情報提供を行った。

① コアシステム v5.3 の提供について

② コアシステム v5.1 及び v5.2 で使用する Java SE について

③ コアシステム v5.0 への暗号モジュール提供を行わないことについて

④ コアバージョンと動作確認対象ミドルウエアの対応

＜質疑応答等＞　特になし

以上