今後のCRYPTREC活動

2003年5月22日

経済産業省

目次

目次

１．今後のCRYPTRECの活動目的及び活動内容（１）

１．１．活動目的

暗号技術及び暗号関連技術の評価等を通じて、電子政府等の安全性及び信頼性の確保に貢献すること。

１．２．活動内容

CRYPTRECは、2003年度以降、以下の活動を行う。なお、今後、新たに必要と考えられる事案が生じた場合には、その都度、暗号技術検討会において具体的な活動内容を検討していくものとする。

（１）電子政府推奨暗号の監視

（２）電子政府推奨暗号の安全性及び信頼性確保のための調査・検討
　　（イ）暗号アルゴリズム等を主な対象とする調査・検討
　　（ロ）暗号実装関連技術を主な対象とする調査・検討

（３）電子政府推奨暗号リストの改訂に関する調査・検討

（４）暗号モジュール評価基準の作成

１．今後のCRYPTRECの活動目的及び活動内容（２）

１．３　活動の具体的内容

（１）電子政府推奨暗号の監視

電子政府推奨暗号に選定された各暗号の安全性等についての情報収集や評価を行い、必要に応じて修正情報の周知やリストからの削除等の電子政府推奨暗号リストの変更を行う。

（２）電子政府推奨暗号の安全性及び信頼性確保のための調査・検討

（イ）暗号アルゴリズム等を主な対象とする調査・検討　暗号アルゴリズムや素因数分解問題等の数論的問題の困難性を主な対象とする調査及び検討を行う。

（ロ）暗号実装関連技術を主な対象とする調査・検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

（３）電子政府推奨暗号リストの改訂に関する調査・検討

将来の電子政府推奨暗号リストの改訂（新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄）のために必要な調査及び検討（電子政府における暗号利用状況調査等）を行う。その際、総務省、経済産業省及び行政情報システム関係課長連絡会議との連携を図ることにする。

（４）暗号モジュール評価基準の作成

暗号モジュール評価基準及び試験基準を作成する。

目次

２．１．今後のＣＲＹＰＴＲＥＣ体制

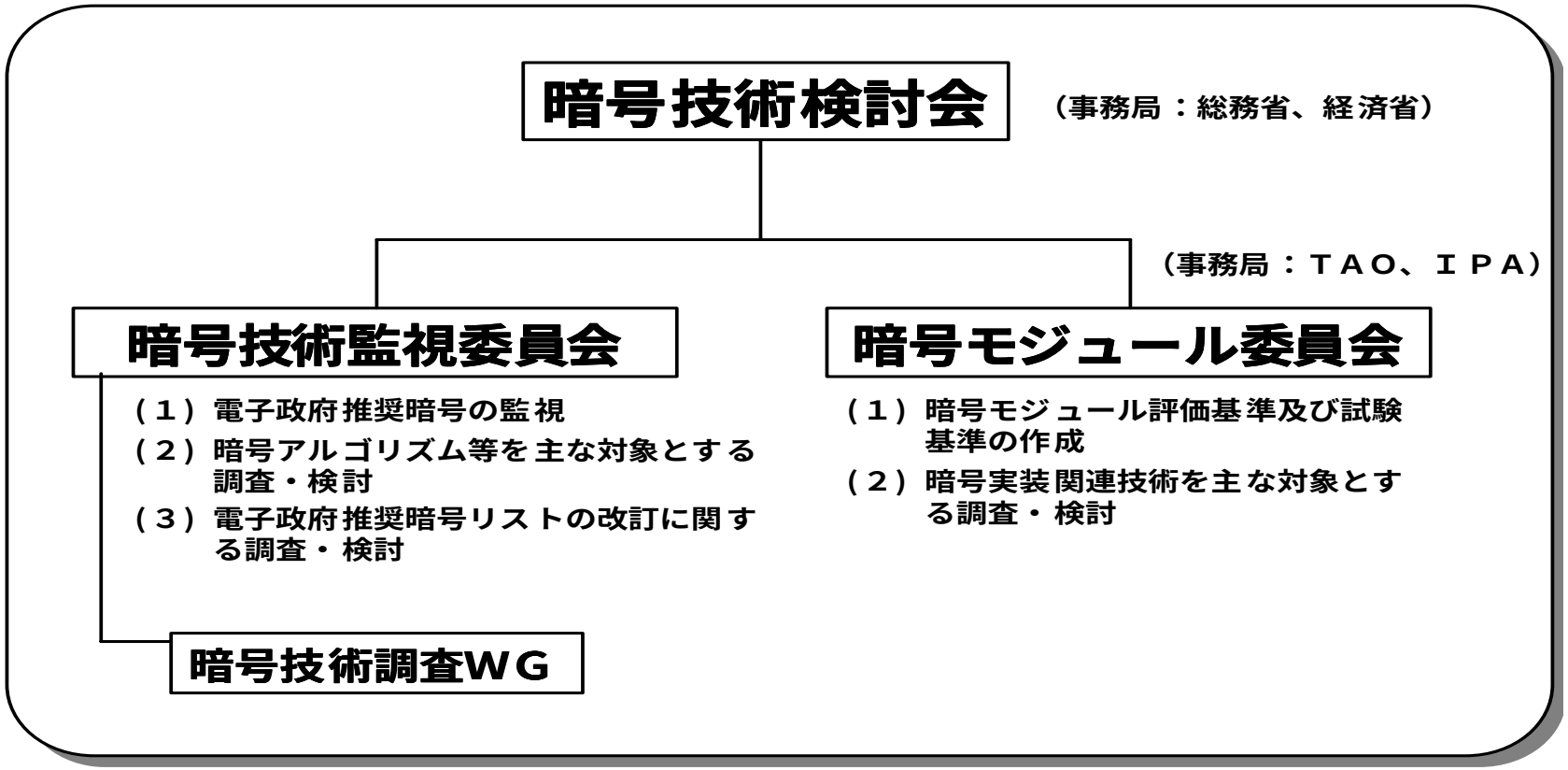
２００３年度以降、当面のＣＲＹＰＴＲＥＣの体制として、暗号技術検討会は存続し、暗号技術検討会の下に「暗号技術監視委員会」及び「暗号モジュール委員会」を設置する。

暗号技術監視委員会の下に「暗号技術調査ＷＧ」を設置する。

従来の暗号技術評価委員会は暗号技術監視委員会に発展的に再編することとする。また、公開鍵暗号評価小委員会及び共通鍵暗号評価小委員会は暗号技術調査ＷＧに再編することとする。

2. 今後のCRYPTREC体制（2）

今後のCRYPTREC体制図



2. 今後のCRYPTREC体制（3）

２．２．暗号技術検討会

暗号技術検討会（「検討会」）は、電子政府推奨暗号リストに掲載された暗号技術の監視、関連する調査研究、及び、暗号技術の危殆化や暗号プロトコル等その他暗号技術の評価・利用等に関する事項について、総合的な観点から検討を行う。また、電子政府等のセキュリティの確保のため、政府のセキュリティ関係機関等との連携、調整を図る。

２．３．暗号技術監視委員会

暗号技術監視委員会（以下、「監視委員会」）は検討会の下に設置される。監視委員会は、数名の有識者等により構成され、安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行うとともに電子政府推奨暗号リストの改訂に関する調査・検討を行う。なお、監視委員会の日常業務を行う監視要員をTAO／通信総合研究所（CRL）（両機関は2004年4月に統合予定）及びIPAに配置する。

２．今後のCRYPTREC体制（４）

２．４．暗号技術調査WG

（１）暗号技術調査WG（以下、「調査WG」）は、電子政府推奨暗号リストの変更案等の作成、及び電子政府推奨暗号に関する暗号アルゴリズム

を主な対象とする具体的な調査・検討に際して監視委員会を支援することを目的として、監視委員会の下に設置される。

（２）調査WGは、監視委員会委員、従来の暗号技術評価委員会委員、共通鍵暗号評価小委員会委員及び公開鍵暗号評価小委員会委員等を元に構成される。これらのWGメンバーは、共通鍵暗号評価グループ及び公開鍵暗号評価グループに区分される。監視委員会は、事案の性質に応じて、共通鍵暗号評価グループ及び／または公開鍵暗号評価グループを召集し、調査WGを開催する。調査WGは、監視委員会に対して電子政府推奨暗号リストの変更案等の作成に関する専門的助言を行う。

（３）その他、調査WGは、監視委員会の要望により事案に応じて開催され、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする具体的な調査・検討（電子政府における暗号利用状況調査等）を行い、監視委員会に対して専門的な助言を行う。

２．５．暗号モジュール委員会

（１）暗号モジュール委員会は検討会の下に設置される。

（２）暗号モジュール委員会は、ISO/IEC等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。

（３）電子政府推奨暗号の安全性及び信頼性確保のための、主として暗号実装関連技術等を対象とする調査・検討を行う。

目次

３．電子政府推奨暗号の監視（１）

３．１．電子政府推奨暗号の監視の基本的考え方

今後、CRYPTRECは、電子政府推奨暗号の安全性及び信頼性を確保することを目的とし、継続的に暗号技術に関する情報を収集し、必要に応じて暗号の安全性を評価する電子政府推奨暗号の監視活動を行う。また、監視は、以下のような考え方に基づいて実施することとする。

（１）実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。

（２）電子政府推奨暗号の仕様変更は原則として認めない。

（３）電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

３．２．電子政府推奨暗号の監視の具体的内容

電子政府推奨暗号の監視は、調査研究、リストからの削除、修正情報の周知等からなる。それぞれの具体的内容は以下（１）～（４）のとおりとする。

（１）暗号技術調査・研究及びデータの蓄積

暗号技術に関する調査研究を実施し、国際標準化の動向等種々のデータを蓄積する。

（２）電子政府推奨暗号の削除

（イ）電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く攻撃を回避することが不可能であると判断される場合には、当該暗号をリストから削除する。

（ロ）電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く、パラメータの修正等の簡易な修正を行うことによって攻撃を回避することが可能であると判断される場合であっても、その方法等を記述した修正情報が当該暗号の仕様書の管理者より提案されない場合には、当該暗号をリストから削除する。

3. 電子政府推奨暗号の監視(3)

(3)電子政府推奨暗号に関する修正情報の周知

(イ)電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、電子政府推奨暗号の仕様変更ではなくパラメータの修正等の簡易な修正を実施することにより当該攻撃を回避することができると判断される場合には、当該修正方法を修正情報として周知する。

(ロ)(イ)の場合において、修正情報は仕様書の管理者から提案させることとし、監視委員会は、提案された修正情報を加味して当該電子政府推奨暗号の安全性評価を実施する。仕様書の管理者より修正情報の提案がなされない場合には、当該暗号をリストから削除する。

(ハ)監視委員会は応募暗号[10]以外の電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いとは判断していないにも関わらず、当該暗号に関する修正情報が仕様書の管理者により発行された場合であって(パラメータ修正等の簡易な修正に限る)、監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

10:応募暗号:電子政府推奨暗号のうち、以下のものを指す。(公開鍵暗号)ECDSA, RSA-PSS, RSA-OAEP, ECDH
PSEC-KEM(共通鍵暗号)CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000, MUGI, MULTI-S01

３．電子政府推奨暗号の監視（４）

（４）電子政府推奨暗号の追加

（イ）電子政府推奨暗号リストの改訂（新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄）が行われるまでは、電子政府推奨暗号の追加は例外的な扱いとする。

（ロ）電子政府推奨暗号リストに掲載されていない暗号が国際的に高い評価を得ている場合であって、暗号技術検討会が当該暗号を新たに評価することが必要と判断し、かつ、

評価の結果、暗号技術検討会が当該暗号を電子政府推奨暗号リストへ掲載することが適切と判断する場合には、当該暗号を電子政府推奨暗号リストへ追加する。

（ハ）電子政府推奨暗号リストへの追加を検討する場合には、「10年間は安心して利用できる」という観点から評価を行う。

（ニ）電子政府調達者より、電子政府推奨暗号リストに無い新たな用途及び当該用途に適した暗号の追加に関する要望がよせられた場合であって、かつ、暗号技術検討会としても当該用途の追加が適切と判断した上で、それに適した暗号の評価を実施し、その結果、適切な暗号を選定した場合には、当該用途及び当該暗号を電子政府推奨暗号リストへ追加することとする。

目次

4. 電子政府推奨暗号の監視の手順（1）

電子政府推奨暗号の監視の手順は、（１）監視委員会における情報収集、（２）監視委員会における情報分析、（３）監視委員会及び検討会における審議及び決定の３段階からなる。具体的には以下のとおりとする。

（１）監視委員会における情報収集

監視委員会において、電子政府推奨暗号の安全性に関する情報を迅速かつ円滑に入手するためには、監視委員会自らが情報収集を行うだけでなく、過去3年間のCRYPTREC活動によって形成された、暗号研究者とのネットワークを活用することが重要である。そこで、以下のように情報収集を行うこととする。

（イ）国内外の学会等への参加等を通じて暗号技術に関する情報（学術論文、発表原稿等）を収集する。
（ロ）暗号技術調査WGメンバー等との連絡体制を整備し、同メンバーから恒常的に情報提供を受ける。
（ハ）応募暗号については、原則として応募元から情報提供を受ける。
（ニ）その他一般からの情報提供も受ける。

４．電子政府推奨暗号の監視の手順（２）

（２）監視委員会における情報分析

監視委員会は、（１）により収集された情報を分析し、電子政府推奨暗号の削除等を検討すべき事態が発生しているか否か判断する。その結果、監視委員会が電子政府推奨暗号の削除等を検討すべき事態が発生していると判断する場合には、事案に応じて、暗号技術調査ＷＧの共通鍵暗号評価グループおよび／または公開鍵暗号評価グループ・「集し、暗号技術調査ＷＧを開催する。ただし、監視委員会が、電子政府推奨暗号の削除等を直ちに行うべき事態が発生していると判断する場合は、その緊急性に応じた対応を実施する。

4. 電子政府推奨暗号の監視の手順（3）

（3）監視委員会及び検討会における審議及び決定

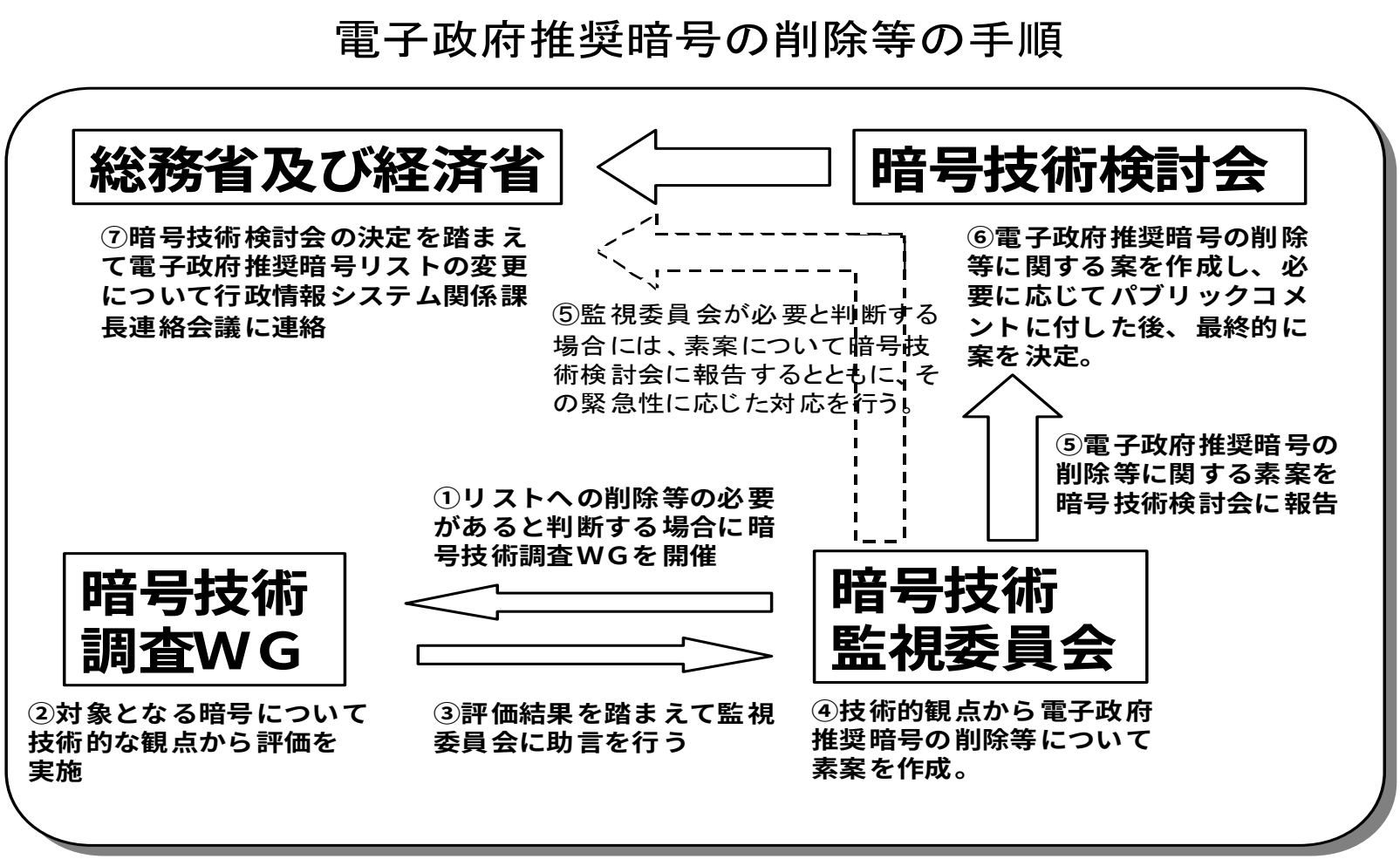
（イ）暗号技術調査WGは、技術的観点から、監視委員会に対して助言を行う。なお、暗号技術調査WGは、応募元等より修正情報の提供を受け、同修正情報を加味した暗号の安全性評価も行う。

（ロ）監視委員会は、暗号技術調査ＷＧの助言を踏まえて、電子政府推奨暗号の削除等を実施するか否かについて素案を作成し、暗号技術検討会に報告する。

（ハ）暗号技術検討会は、総合的な観点から当該素案を審議し電子政府推奨暗号の削除等に関する案を作成する。同案が電子政府推奨暗号リストに変更を加えるものである場合、総務省及び経済産業省はパブリックコメントに付し、その結果を暗号技術検討会に報告する。暗号技術検討会は、パブリックコメントの結果を踏まえて、電子政府推奨暗号の削除等に関する案を決定する。

（ニ）暗号技術検討会の決定に基づいて電子政府推奨暗号リストの変更を行った場合、総務省及び経済省は、電子政府推奨暗号リストの変更について行政情報システム関係課長連絡会議等に連絡する。

4. 電子政府推奨暗号の監視の手順(4)



目次

５．電子政府推奨暗号リストの改訂（１）

５．１．基本的認識

（１）電子政府推奨暗号は、現時点において、今後10年間は安心して利用できるという観点から選定された暗号である。

（２）しかし、暗号に対する解析や攻撃の技術や手法はますます高度化しており、電子政府推奨暗号は常に危殆化の危険にさらされている。一方、新たな暗号の開発も進んでおり、今後、安全性や実装性に優れた新しい暗号の出現が期待されるところである。

（３）そこで、危殆化した暗号の削除や新しい暗号の選定等により電子政府推奨暗号リストを一定期間毎に改訂することが望ましい。

（４）改訂を実施する際に、仮に公募を実施する場合は、公募のアナウンス（公募開始時期、公募期間、評価期間、新リスト発表時期等の公表）から新リストの策定まで、5年程度の期間をかけることが望ましい。

5. 電子政府推奨暗号リストの改訂（2）

５．２．基本的考え方

リストの改訂作業の具体的な実施内容については、電子政府の導入状況及び電子政府推奨暗号の監視状況を考慮しつつ、然るべきタイミングで検討を行うこととする。なお、リスト改訂作業の実施方法としては、現在のところ、以下のような検討事項が想定されるところである。

（想定される検討事項）
（イ）公募の要否
（ロ）リスト項目（技術分類等）の見直し
（ハ）項目別の掲載暗号数
（ニ）評価基準、評価方法

また、改訂作業の具体的な開始時期については、2003年度以降に暗号技術検討会において検討の上決定するが、改訂作業の完了及び新リストの決定は、遅くとも10年後の2013年までとする。なお、仮に公募を実施するとした場合は、5年程度の期間をかけることが望ましいと考えられることから、遅くとも2008年3月頃には公募のアナウンスを行うことが望ましい。

目次

6. 暗号モジュールに関する検討

（1）電子政府の安全性及び信頼性を確保するためには、暗号技術レベルの安全性だけでなく暗号技術の実装の安全性を確保する必要があり、この観点から暗号モジュールの安全性評価基準を作成することが急務である。

（2）他方、暗号モジュールの安全性評価基準に関しては、米国が自国の政府調達基準であるFIPS140-2のISO/IEC化を提案しており、暗号モジュールの安全性評価基準を我が国において作成するにあたっては、ISO/IEC等における議論を注視していく必要がある。

（3）このような状況を踏まえて、検討会の下に暗号モジュール委員会を設置する。暗号モジュール委員会は、ISO等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。

（4）なお、暗号モジュール委員会は、暗号技術監視委員会と連絡をとりつつ、電子政府推奨暗号の安全性及び信頼性確保のための暗号実装関連技術を主な対象とする調査・検討を併せて行うこととする。

7. ご静聴ありがとうございました。

http://www.meti.go.jp/policy/netsecurity/

経済産業省
情報セキュリティ政策室
北浦　康弘

kitaura-yasuhiro@meti.go.jp
Tel : 03-3501-0397
Fax: 03-3501-6639