報道資料

平成 24 年 10 月 26 日

内閣官房情報セキュリティセンター（NISC）

情報セキュリティ対策推進会議第８回会合の開催について

本日、「情報セキュリティ対策推進会議」（議長：竹歳内閣官房副長官）の第8回会合が開催されました。概要は以下のとおり。

政府機関の暗号アルゴリズム(SHA-1 及び RSA1024)に係る移行指針の改定

「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成 20 年 4 月 22 日情報セキュリティ政策会議決定）を改定。

主な改定点は、以下のとおり。

- 各認証基盤との調整結果を踏まえ、切替時期を見直し
  - (1) 新たな暗号方式による電子証明書の発行開始時期
    「2014年度早期」⇒「2014年9月下旬以降、早期に」
  - (2) 従来の暗号方式による電子証明書の検証（有効性の確認）終了時期
    「2015年度早期」⇒「2015年度末までに」 ただし、発行済み電子証明書の有効期間が残存し、やむを得ない場合は、「2019年度末まで」可

政府機関における情報セキュリティ対策に係る取組の推進

本年9月中旬に発生した政府機関等に対するサイバー攻撃について報告があり、昨今の状況を踏まえた政府機関における情報セキュリティ対策として、以下の取組の推進を要請。

- 昨今の状況を踏まえ、早急に対応すべき措置
  - (1) 各府省庁において管理する情報システム（ウェブサイト）等の再点検
  - (2) 障害・事故等の発生に備えた体制（CSIRT 等）の充実強化
  - (3) 平素からの情報収集の強化と情報共有の徹底
- なりすまし防止のための対策技術（送信ドメイン認証）等の更なる導入の促進
- 政府機関の情報セキュリティ担当者の人材育成

（詳細については別添資料参照）

【本件に関する問い合わせ先】
内閣官房情報セキュリティセンター（NISC）
内閣参事官　三角　育生
電話　03－3581－3959

※ 本会合の会議資料等は、内閣官房情報セキュリティセンターのホームページに公表しております。
http://www.nisc.go.jp/conference/suishin/index.html

政府機関の暗号アルゴリズムに係る移行指針の改定概要

1　経緯

①電子政府システム（入札・申請等）において電子署名等のために広く使用されているSHA-1及びRSA1024と呼ばれる暗号方式の安全性の低下が指摘

②より安全な暗号方式（SHA-256及びRSA2048）への移行が必要であることから、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を策定

（H20年4月22日　情報セキュリティ政策会議決定）

2　政府機関における移行に向けた準備スケジュール

- 各府省庁が保有する情報システムの新たな暗号方式への対応時期　⇒「2013年度末まで」
- 新たな暗号方式による電子証明書の発行開始可能時期　⇒「2014年度早期」
- 従来の暗号方式による電子証明書の検証（有効性の確認）終了可能時期　⇒「2015年度早期」

（H21年2月3日　情報セキュリティ政策会議決定）

3　移行指針の改定概要

- 切替時期について各認証基盤との調整結果を踏まえ、以下のとおり改定

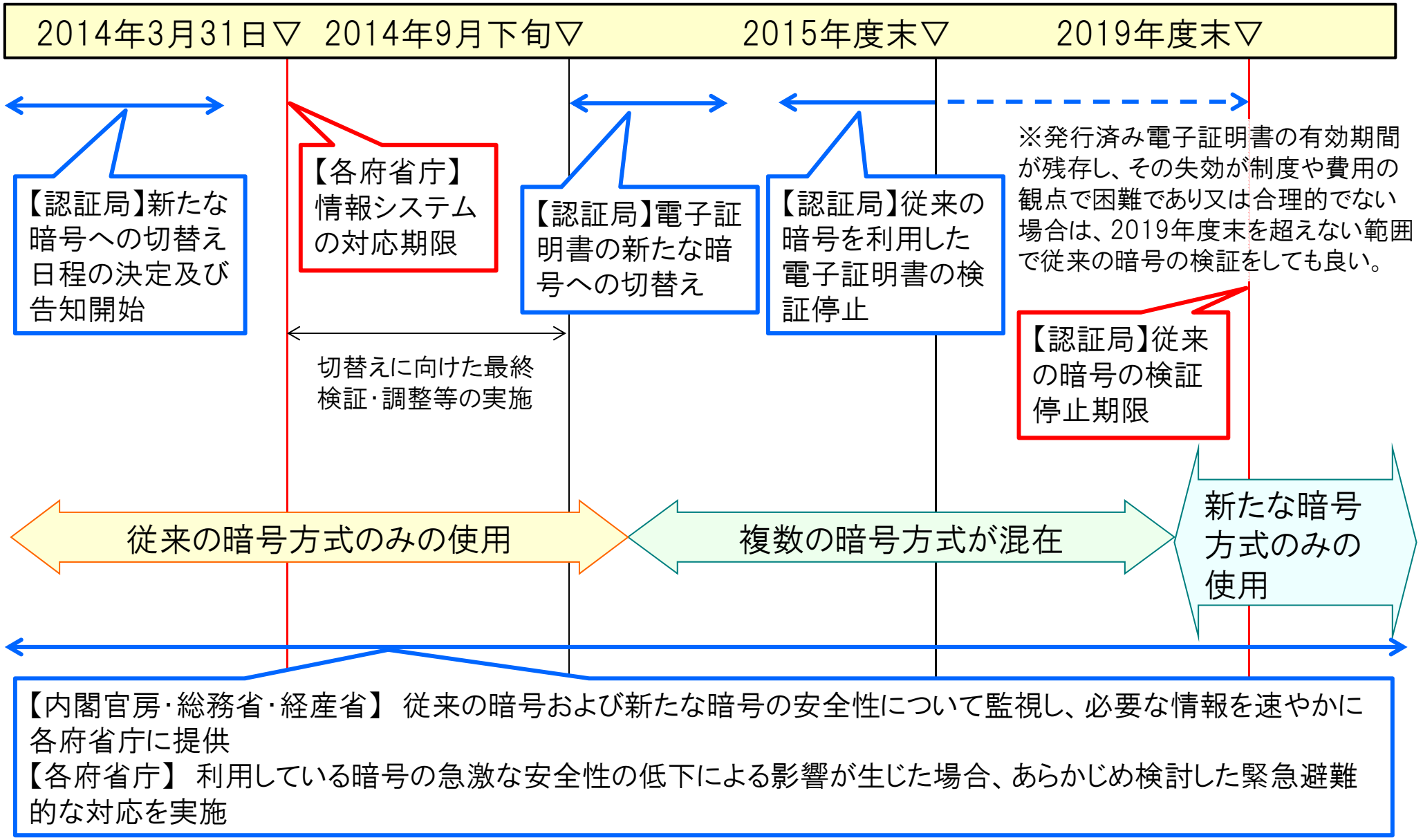
  政府認証基盤及び電子認証登記所が発行する電子証明書については、

  a.「2014年9月下旬以降、早期に」新たな暗号方式に切替

  b.「2015年度末までに」従来の暗号方式によって発行された証明書の検証を終了

  ただし、発行済み電子証明書の有効期間が残存し、やむを得ない場合は、「2019年度末まで」検証可

（参考）政府機関における暗号移行スケジュール



本年９月中旬の我が国政府機関等に対するサイバー攻撃

攻撃事案

○ 攻撃予告
- 9/13以降、ネット上にて我が国の政府機関等のシステムに係る脆弱性等の情報収集、攻撃の呼びかけ等
- 9/19以降、攻撃の呼びかけは急速に沈静化

○ 関連が疑われる障害の概要
- ウェブサイトの閲覧障害
  総務省統計局、政府インターネットテレビ（内閣府）等のウェブサイトが一時閲覧しづらい状態になったが、いずれも現在は閲覧が可能な状態
- ウェブサイトの改ざん
  裁判所、文化庁等のウェブサイトが改ざんされ、一部は復旧、その他は復旧に向け作業中
  （原因が判明している事案は、全て既知の攻撃手法によるものであり、高度な手法は見当たらず）

CISO等連絡会議幹事会（9/25）において、各府省庁等に対し下記の対応措置を要請

対応措置

1. 各府省庁等において管理する情報システム等の再点検
2. 障害・事故等の発生に備えた体制の充実強化
3. 平素からの情報収集の強化と情報共有の徹底

政府機関等における情報セキュリティ対策の点検・実施について

昨今の状況

本年９月をはじめ、昨今、政府機関等における情報システムの**ウェブサイトが外部からの攻撃**によって、**改ざん**されたり、**一定の間、閲覧困難**となるといった事案が顕在化

〔想定される脅威〕

○情報システムの機能障害により、国民生活や社会経済上必要な**サービスの停止**

○重要な**情報の漏えいや改ざん**

昨今の状況を踏まえ、早急に対応すべき措置

＊本年9月25日　幹事会において各府省庁に要請

1．各府省庁において管理する情報システム等の再点検

⇒**ウェブサイト**（**外部委託等**により構築・運用しているものを**含む**）に対しては、**既知の脆弱性を衝いた攻撃手法**が見受けられることから、以下の事項を中心に点検・実施

①改ざんの原因となる可能性が高い基盤ソフトウェアの**脆弱性情報を確認**

②**アップデートやパッチ適用等**が適切に行われていない場合は、速やかに対応

＊所管する重要インフラ事業者や独立行政法人、特殊法人、国立大学法人等に対しても同様

2．障害・事故等の発生に備えた体制の充実強化

⇒インシデント等の発生に際し、迅速かつ的確に対応するため、各府省庁において**CSIRT等の機能を有する体制**を早急に**整備**

3．平素からの情報収集の強化と情報共有の徹底

⇒NISCへの情報連絡と他の府省庁へのNISCからの情報提供の徹底（再確認）

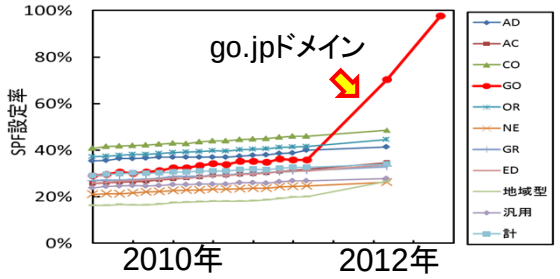
メールアドレスを詐称されないための対策の推進

電子メールの送信元について、なりすましを防止するための対策の一環として
DNSサーバへのSPFレコードの記載等を推進

これまでの主な取組

- 本省、外局、地方支分部局、独立行政法人等において、送信側SPFの導入を推進
- 外局を含む**第3レベルドメイン（xxx.go.jp）**について、**送信側SPFの設定をほぼ完了**
  （H24年3月31日現在　第3レベルドメインで**設定率　97．4%**）

主な取組内容
①DNSサーバにSPFレコードを記載
（メール送信を行わないものについては、その旨記載）
②利用していないgo.jp ドメインについては、廃止



今後の主な取組

- **送信側におけるSPF対策の推進**
  ⇒**第4レベル（yyy.xxx.go.jp）以上の政府ドメイン**についても、DNSサーバへのSPFレコードの記載を徹底
- **受信側におけるSPF対策の推進**
  ⇒メールサーバ等の更新時期に合わせて、**受信側SPF機能を導入**
  ⇒SPF判定結果を**メール受信者が一目で分かるような周知方法（件名に「meiwaku」等）の検討**
- **SPF以外の対策技術の導入検討**
  ⇒暗号技術を利用する、**より強固な対策技術DKIM**のSPF対策との併用　等

＊DKIM（DomainKeys Identified Mail）：電子署名を利用した電子メールの送信ドメイン認証技術の一つ

政府機関の情報セキュリティ担当者の育成等に関する事例の概要

政府機関の情報セキュリティ担当者の育成等の参考となるよう、内閣官房情報セキュリティセンターにおいて、事例を整理。

情報セキュリティ担当者に係る人事ローテーション等の工夫

○専門的知識を有する者を情報セキュリティ担当とし、その後、係長、補佐へ計画的に登用

○通常2年の人事異動を、情報セキュリティ担当者については、長期化

○システム関連部門経験者に、独法等のセキュリティ関連部門や別の部門のセキュリティ業務を担当させるなど人事異動に配慮

○職員を国内外の情報セキュリティ関係大学院等へ留学

外部人材の活用

○専門資格を有する外部人材を任期付で採用し、最長5年に渡って担当させる。任期中の勤務状況が優れている者は、内部選考を経て常勤化

○官民交流法により、高度な知識と豊富な経験を有する外部人材を採用

○公募により、民間セキュリティ人材を期間業務職員として採用

○セキュリティ監視・管理等を行う業務を外部委託し、委託先職員が省内に常駐

公務員採用時における情報セキュリティ関連素養の確認

○採用面接時に、ITパスポート、情報セキュリティ等の資格の有無を確認

○官庁訪問者に記載させる面談カードにITに関する資格等を取得しているか記載させるとともに面談の場において確認

○採用面接において、情報セキュリティに関する常識について質疑応答

職員全体の意識啓発と能力の底上げ

○全職員に対し、e-ラーニングによる情報セキュリティ対策にかかる研修を実施

○新規採用者、中途採用者、管理職向けに情報セキュリティに関する研修を実施

法律家の活用

○情報セキュリティに詳しい法学者や弁護士を懇談会等の委員に委嘱

○別の部署で採用している弁護士と必要に応じ連携