# 平成 23 年度情報セキュリティ報告書

平成 24 年５月

内閣法制局

# はじめに

近年めざましい進歩を続けている情報通信技術（ICT）により、インターネットや情報システムの利便性が向上する一方で、サイバー攻撃、不正アクセス、ウィルス感染やフィッシングサイトからの情報漏えいなどのリスク・脅威は増大しています。また、平成２３年度には、政府及び関係機関に対するサイバー攻撃事態等が発生しており、これらの脅威に適切に対応するため、日常的に利用するシステムの情報セキュリティ対策の重要性がますます高まってきています。

内閣法制局では、政府機関の一員として情報セキュリティ水準を高めるため、全職員を対象とした情報セキュリティ教育の実施、情報セキュリティ対策実施状況の確認のための自己点検の実施、内閣官房情報セキュリティセンターから送付される不審なメールに関する情報のイントラネットの掲示板への掲示及びメールによる注意喚起のための全職員への周知等の取組を実施してまいりました。

また、情報システムの対策としては、保有している情報システム（LAN 端末を含む。）の重点検査を実施し、安全性の確保に努めてまいりました。

平成２４年度以降も、リスク・脅威への対策や職員向け教育の充実を図り、引き続き情報セキュリティの維持・向上に努めてまいります。

最高情報セキュリティ責任者
（内閣法制局総務主幹）
北川　哲也

## １ 平成２３年度の総括

### (1) 平成２３年度の評価

#### ア　平成２３年度の重点事項

情報セキュリティ対策のうち、情報セキュリティ教育について、情報漏えいをはじめ遵守すべき事項に関する、教育資料の充実を図り、職員の理解を深めるための教育を行うこと。

#### イ　情報セキュリティ対策の実施状況の自己点検結果

平成２３年度の自己点検については、平成２２年度同様に内閣法制局の全職員を対象とし、文書のライフサイクルに的を絞って実施した。自己点検の結果からは、おおむね適切に実施されており、また、平成２３年度の課題として挙げた格付等についても改善されていることが認められた。

しかしながら、十分に実施されていない事項も僅かながら見られたところであり、なお改善の余地があるものと考える。

#### ウ　情報システムの情報セキュリティ対策状況

内閣法制局が保有する情報システム（内閣法制局 LAN システム、法令審査支援システム）のサーバ及び端末等に関しては、適宜セキュリティパッチを実施しており、万全な情報セキュリティ対策を講じている。

また、Web サーバについては、ASP サービスを利用しているが、委託先に対してはセキュリティ対策が講じられていることを確認している。

今後もこの状態を維持できるよう情報セキュリティの適切な対策の実施に努める。

#### エ　教育・啓発

内閣法制局では、全職員に対し、情報セキュリティ教育を実施している。教育用の資料は、内閣官房情報セキュリティセンター（以下「NISC」という。）が作成した資料を参考に内閣法制局用に作成したものを使用している。平成２２年度から、遵守すべき事項について、ポイントを絞った理解しやすい資料を作成し、教育に活用しており、平成２３年度はその資料に昨年度の改善すべき点を追加したものを、教材として同教育を実施した。同教育の資料等については、イントラネットに掲載し、いつでも閲覧できる体制としている。

また、NISC から送付される「不審メール情報」についても、イントラネットへの掲載と併せて、全職員へ注意喚起のためメールにより周知を図っている。平成２３年度は全職員が、NISC が実施したメールの取扱い訓練に参加し、メール開封時の注意喚起を実施した。

#### オ　調達・外部委託

内閣法制局では、情報システムの調達や外部委託に際し、委託先の情報セキュリティ水準を確保するため、内閣法制局情報セキュリティポリシー（管理基準編）及び同（技術基準編）（以下「内閣法制局情報セキュリティポリシー」

という。）に基づき、調達仕様書の入札適合条件などに情報セキュリティに関する社内規程及び管理体制が整備されている事実を証明するようにと記載内容に盛り込んでおり、その証明により、委託先の情報セキュリティ対策の実施状況を確認している。

カ　情報セキュリティに関する障害・事故等の報告

内閣法制局では、情報セキュリティに関する障害・事故等は発生していない。

(2) 平成２４年度の目標

内閣法制局では、今後、更なる情報セキュリティレベルの向上を目指すこととし、重点的に取り組むべき目標を以下のとおりとする。

ア　全職員の更なる情報セキュリティに対する意識向上のために、情報セキュリティ教育の内容の充実を図ること。

イ　文書のライフサイクルについて、情報セキュリティ教育の資料に盛り込むなど、情報セキュリティレベルの底上げを図ること。

## ２　報告の基本情報

(1) 内閣法制局の概要

内閣法制局の主な業務は、法律問題に関し内閣並びに内閣総理大臣及び各省大臣に対し意見を述べるという事務（いわゆる意見事務）並びに閣議に付される法律案、政令案及び条約案を審査するという事務（いわゆる審査事務）である。

意見事務は第一部で、審査事務は第二部、第三部及び第四部で行っている。

なお、人事、予算、会計等の官房的事務は長官総務室で行っている。

内閣法制局では、効率的に日常の業務が実施できるような下記の情報システムを構築・運用し、行政の効率的かつ着実な遂行に努めている。

ア　内閣法制局 LAN システム

職員が業務遂行に利用する LAN 回線、ソフトウェア及びハードウェアといった内閣法制局の情報処理の基盤となる情報システム

イ　法令審査支援システム

法令案の形式的事項について多様な項目の点検を実施し、法令案における誤り及びそのおそれのある箇所を指摘・表示する情報システム

(2) 対象とする期間

平成２３年４月１日から平成２４年３月３１日まで

(3) 対象とする組織

内閣法制局

(4) 対象とする情報

政府機関の情報セキュリティ対策のための統一基準群（以下「政府統一基準」という。）で対象とする情報であって、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報

(5) 本報告書の責任部署

内閣法制局長官総務室総務課

## ３ 情報セキュリティ対策の枠組み

(1) 情報セキュリティ対策に関する文書体系

内閣法制局では、政府統一基準に基づき、情報セキュリティ対策の基本方針及び情報セキュリティ対策基準として、内閣法制局情報セキュリティポリシーを定めている。また、内閣法制局情報セキュリティポリシーに定められた遵守事項を運用していくため、以下のような規程等を整備している。

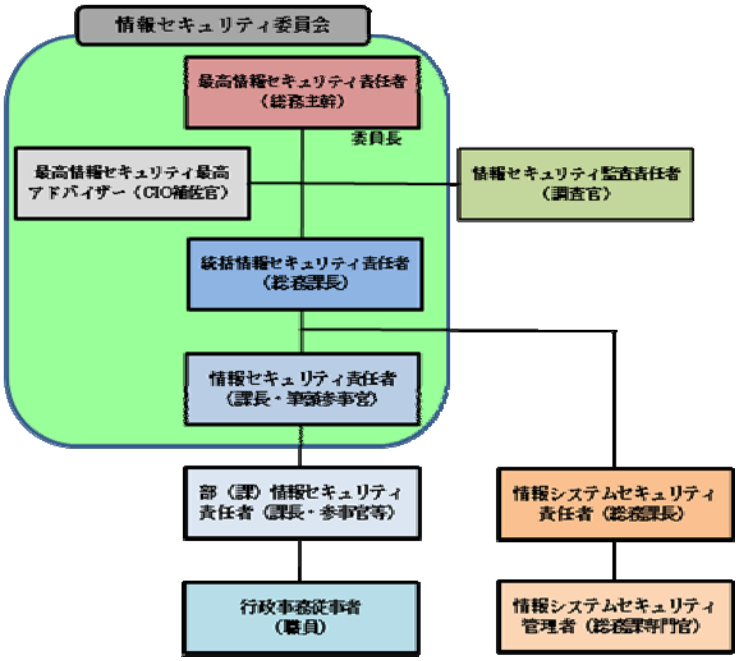
ア　人事異動等の際に行うべき情報セキュリティ対策実施規程
イ　例外措置手順書
ウ　障害等対応手順書
エ　情報セキュリティ監査実施手順書
オ　情報の格付及び取扱制限に関する規程
カ　情報取扱手順書
キ　情報システムにおける情報セキュリティ対策実施規程

(2) 情報セキュリティ対策の推進体制

内閣法制局では、情報セキュリティ対策を推進するために、政府統一基準及び内閣法制局情報セキュリティポリシーに基づき、以下に示す体制を整備している（図１）。

ア　最高情報セキュリティ責任者
　内閣法制局の情報セキュリティに関する事務を統括
イ　情報セキュリティ委員会
　最高情報セキュリティ責任者を委員長とし、情報セキュリティに関する重要事項の審議を実施
ウ　情報セキュリティ監査責任者
　情報セキュリティ監査に関する事務を統括
エ　統括情報セキュリティ責任者
　最高情報セキュリティ責任者の補佐及び情報セキュリティ責任者の統括
オ　部（課）情報セキュリティ責任者
　部（課）内の情報セキュリティに係る事務を統括
カ　情報システムセキュリティ責任者
　所管する情報システムの運用管理の統括
キ　情報システムセキュリティ管理者
　情報システムごとの情報セキュリティの運用管理
ク　最高情報セキュリティアドバイザー
　情報セキュリティに関する専門的な助言

図１　内閣法制局における情報セキュリティ対策の推進体制




(3) 情報セキュリティ監査

内閣法制局では、局内の情報セキュリティ対策の改善に資する事を目的として、毎年度、情報セキュリティ監査を実施している。

ア 平成２３年度に実施した情報セキュリティ監査の内容

(ｱ) 内閣法制局情報セキュリティポリシーの政府統一基準への準拠性監査

内閣法制局情報セキュリティポリシーが、政府統一基準に準拠していることを確認する監査

(ｲ) 各種実施手順書の内閣法制局情報セキュリティポリシーへの準拠性監査

各種実施手順書が、内閣法制局情報セキュリティポリシーに準拠していることを確認する監査

(ｳ) 自己点検の適正性監査

情報セキュリティの自己点検結果が、内閣法制局における情報セキュリティ対策の実施状況を適切に反映していることを確認する監査

(ｴ) 例外措置の申請の監査

例外措置の申請に対して、内閣法制局情報セキュリティポリシー例外措置手順書に基づき適切な審査が実施されていることを確認する監査

イ 情報セキュリティ監査の結果

監査の結果、以下のとおり全体として重大な指摘事項はなく、高いレベルで情報セキュリティ対策が実施されていることが確認された。

(ｱ) 内閣法制局情報セキュリティポリシーの政府統一基準への準拠性に関する監査

政府統一基準が要求する事項を満たしていることが確認された。

(ｲ) 各種実施手順書の内閣法制局情報セキュリティポリシーへの準拠性に関する監査

各種実施手順書は、内閣法制局情報セキュリティポリシーで要求されている項目を満たしていることが確認された。

(ｳ) 自己点検の適正性に関する監査

自己点検結果は、監査時の調査票回答結果と整合性があり、適切に自己点検が実施されていることが確認された。

(ｴ) 例外措置の申請に関する監査

例外措置の申請は、該当するものがなかった。

## ４ 平成２３年度の重点事項

### (1) 目標

情報セキュリティ教育のうち、情報の格付及び取扱制限をはじめ遵守すべき事項について、職員の理解を深めること。

### (2) 実績及び評価

情報の格付及び取扱制限及び情報漏えいに関し、教育資料の充実を図り、職員に対して情報セキュリティ教育を実施した。数人に対してヒアリングを行った結果、他府省等から送付された資料等について、情報の格付及び取扱制限を遵守するようになったとの回答があり、一定の成果があったものと考えられる。

## ５ 平成２３年度における情報セキュリティ対策の実施状況

### ５．１ 内閣法制局情報セキュリティポリシーに関する自己点検結果

#### (1) 課題と対策

ア　自己点検について

情報セキュリティ対策の実施状況の自己点検（以下「自己点検」という。）は、対策基準の各遵守事項について各職員自らが実施状況を確認し、自己評価を行うものである。

自己点検の実施は、各職員が情報セキュリティに向き合う良い機会であり、自己点検を通じて、各職員の情報セキュリティに対する意識の醸成につながるものと考えている。

このような考えから、平成２３年度の自己点検は対象者を全職員とし、教育付き自己点検票をメールにて配布し、期間内（平成２３年１１月２２日～１２月９日）に提出してもらう方法で実施した。

今回の自己点検の対象は、情報のライフサイクルに特化しており、項目数が６０から６と大幅に少なくなった。

イ　平成２２年度の自己点検の結果に基づく課題と対策

平成２２年度の自己点検の結果を見ると、把握率（自己点検の状況が把握で

きた者の割合）は 100%、実施率（把握された者のうち対策を実施した者の割合）は 98.6%と共に高い値となっている。しかしながら、実施率の十分でない項目として、情報の格付及び取扱制限の遵守が上げられており、それに関する事項を情報セキュリティ教育の資料に盛り込み、併せて情報漏えいの防止に関する事項ついても職員の理解を深めるため、情報セキュリティ教育を実施した。

(2) 平成２３年度自己点検の結果の状況

(ｱ) 把握率

前年度に引き続き、100%を維持している（表１）。

表１　把握率

| 対象年度 | 把握率 |
|---|---|
| 平成 22 年度 | 100% |
| 平成 23 年度 | 100% |

(ｲ) 実施率

役割別で見ると、部（課）長等及びシステム責任者については平成２２年度に引き続き 100%を維持し、行政事務従事者については若干、平成２２年度を下回る結果となっている（表２）。

表２　役割別の実施率

| 対象年度 | 部(課)長等注1 | システム責任者注2 | 行政事務従事者注3 |
|---|---|---|---|
| 平成 22 年度 | 100% | 100% | 98.6% |
| 平成 23 年度 | 100% | 100% | 98.4% |

注１　部（課）情報セキュリティ責任者　注２　情報システムセキュリティ責任者及び管理者　注３　職員

(ｳ) 到達率（政府統一基準に掲げられている各遵守事項について、一定の割合（100%、95%、90%）以上の者が対策を実施した事項の割合）

役割別で見ると、部（課）長等及びシステム責任者については、平成２２年度に引き続き 100%を維持している。行政事務従事者については、平成２２年度を下回る結果となっているが、平成２２年度と平成２３年度では、点検項目数が大幅に削減されているため、正確に比較することは難しい（表３）。

表３　役割別の到達率

【到達率：100】

| 対象年度 | 部(課)長等注1 | システム責任者注2 | 行政事務従事者注3 |
|---|---|---|---|
| 平成 22 年度 | 100% | 100% | 71.7% |
| 平成 23 年度 | 100% | 100% | 50.0% |

【到達率：95】

| 対象年度 | 部(課)長等注1 | システム責任者注2 | 行政事務従事者注3 |
|---|---|---|---|
| 平成 22 年度 | 100% | 100% | 98.3% |
| 平成 23 年度 | 100% | 100% | 100% |

【到達率：90】

| 対象年度 | 部(課)長等注1 | システム責任者注2 | 行政事務従事者注3 |
|---|---|---|---|
| 平成 22 年度 | 100% | 100% | 100% |
| 平成 23 年度 | 100% | 100% | 100% |

注１　部（課）情報セキュリティ責任者　注２　情報システムセキュリティ責任者及び管理者　注３　職員

(3) 総評

平成２３年度の自己点検の結果、把握率及び部（課）情報セキュリティ責任者及び情報システムセキュリティ責任者の実施率については、平成２２年度と同様に 100%を維持している。

また、行政事務従事者の実施率については僅かに下降しているが、平成２２年度の自己点検と平成２３年度の自己点検では、点検項目数が大幅に変更となり単純に比較できるわけではない。情報のライフサイクルのうち、情報の作成から保存までの間において一部未実施の職員がおり、それらの職員に対して情報の取扱いに関する意識を浸透させるためには、教育の徹底を図っていく必要があると考えている。

## ５．２ 情報システムの情報セキュリティ対策状況

(1) 目的

情報システムの情報セキュリティ対策は、情報システム上で取り扱う情報を守る上で重要なものである。情報システムに対するセキュリティ対策は、リスクの軽減を図るためには必須であり、必要な対策を実施する必要がある。

内閣法制局では、毎年度、政府統一基準で定められた遵守事項の実施状況に係る重点的な検査（以下「重点検査」という。）を実施している。

(2) 情報システムの対策状況

平成２２年度の重点検査において、全府省庁が、対象となる端末及びサーバ類に対する情報セキュリティ対策の実施率が 100%であったため､平成２３年度の重点検査の検査項目より削除されることとなった。今後もこの状態を維持するよう努める。また、web サーバに関しては、ASP サービスを利用しているため重点検査

の対象外となっているが、委託業者に対しては、重点検査で行うべきセキュリティ対策と同レベルの対策が取られていることを確認している。

## ５．３ 教育・啓発

### (1) 教育

#### ア　教育計画の策定、教育の企画等

情報セキュリティ対策を職員一人一人が着実に取り組んでいくためには、内閣法制局情報セキュリティポリシーの内容、関係規程類にある具体的な事項を各職員が理解して、日々実践していくことが大切である。そのためには、各職員に対して情報セキュリティ教育を実施していくことが必要である。

内閣法制局では、毎年度、係長級以下の職員には職員研修の際に、課長補佐級以上の職員には法令整備会議の際に、それぞれ一定の時間を確保して情報セキュリティ教育を実施している。

#### イ　教育教材について

内閣法制局が情報セキュリティ教育で使用している教材は、NISC が作成・配布したものを参考にして、内閣法制局の職員の教育用として作成した教材を使用している。平成２２年度に、遵守すべき事項について、ポイントを絞った理解しやすい資料を作成し、平成２３年度用に追加をしたものを教材として実施した。

#### ウ　教育受講状況の管理

内閣法制局では、係長級以下の職員が対象の職員研修及び課長補佐級以上の職員が対象の法令整備会議の際に情報セキュリティ教育を実施しており、その時の受講状況を把握して管理している。また、理解度については、自己点検の結果により確認している。

### (2) 情報セキュリティ関係資料のイントラネットへの掲載

情報セキュリティ関係規程類やNISC から送付される「不審メール情報」等についても、イントラネットへの掲載と併せて全職員にメールを送信して周知している。

## ５．４ 調達・外部委託

### 外部委託先の管理

情報システム開発等の業務を外部に委託して実施する際には、内閣法制局と同等の情報セキュリティ水準を委託先に求め、確保する必要がある。

このため、内閣法制局では、内閣法制局情報セキュリティポリシーに基づき、調達仕様書や契約書などの記載内容により、委託先の情報セキュリティ対策の実施状況を確認するなど、委託先の管理を実施している。

## ６　情報セキュリティに関する障害・事故等報告

内閣法制局では、情報セキュリティに関する障害・事故等は発生しなかった。

## ７ 情報セキュリティ対策に関する平成２４年度の計画

平成２４年度は、平成２３年度に続き情報セキュリティ対策に関する自己点検及び監査を実施するとともに、情報システムの重点検査を実施する。

また、平成２３年度の自己点検の結果を踏まえ、情報のライフサイクルをはじめ情報セキュリティ教育に関する資料の充実を図る。

## おわりに　～最高情報セキュリティアドバイザーのメッセージ～

情報セキュリティに対する脅威は年々増大しています。その要因としては、情報化の進展により重要な情報が様々に電子化された情報資産として取り扱われ蓄積されてきていること、情報技術の進展により情報資産への攻撃手法が高度化、多様化していること、さらに政府機関はその性格上攻撃目標として狙われる可能性が高いこと等が挙げられます。

内閣法制局は、政府機関の中でも組織的には小規模で情報システムも大規模なものは保有しておりませんが、法令関連情報、人事・会計情報等重要な情報資産を保有しており、それらのセキュリティを確保するためにリスクに見合った対策を実施しております。

今年度は教育、自己点検、情報システムの重点検査及び監査等、情報セキュリティの維持、向上に向けて着実な活動を展開してきました。さらに標的型攻撃対策の一つとして、メールの取扱いの訓練や不審メールに対する職員への注意喚起等へも取り組みました。結果としてセキュリティ障害・事故がゼロであったこと、監査結果が良好であったことは評価できます。ただ、今年度重点的に実施された情報サイクルに関する行政事務従事者向けの自己点検結果から情報の取扱いの実施がまだ十分でないと思われますので、人的セキュリティの改善が今後の課題と認識します。

今後は、計画、実施、監査・点検、見直しという情報セキュリティマネジメントのPDCAサイクルを着実に回す中で、今年度の活動から得られた課題への対策を組み込み、セキュリティレベルを継続的に改善させることが重要と考えます。

最高情報セキュリティアドバイザーとしては、内閣法制局の実状に合ったアドバイスを適切に提供し、当局のセキュリティレベルの更なる向上に貢献する所存であります。

最高情報セキュリティアドバイザー（内閣法制局 CIO 補佐官）
川合 浩司