平成２３年度　情報セキュリティ報告書

平成２４年５月

法　　務　　省

目　次

第１　はじめに

１　最高情報セキュリティ責任者からのメッセージ

法務省では，進展著しい情報通信技術を積極的に導入・活用し，国民の皆様の重要な資産・財産情報である登記情報，国民生活の安全・安心に欠かせない刑事関連情報，適正な出入国管理を行うための情報等の電子化を進め，行政サービスの質の向上や業務の最適化・効率化に努めてまいりました。

一方，情報通信技術や電子化された情報に対する脅威は，多様化・高度化・複雑化しており，経済活動や社会生活の多くの場面において情報通信技術への依存が高まるにつれ，サービスの停止や情報の漏えい等の情報セキュリティに関する事案が与えるインパクトも大きくなっています。

特に，法務省が取り扱う情報の性質を考慮すれば，情報セキュリティに関する事案が発生した場合には，平穏な市民生活や円滑な経済活動を脅かし，国民の安全・安心な社会の形成を目指す，法務行政の遂行に著しい支障を来すことは言うまでもありません。

法務省では，このような事態を招かないようにするとともに，万が一，発生した場合には，その影響を最小限にとどめることができるように，情報セキュリティ対策の実施状況を把握・評価して，その維持・改善を行う各取組を一連の流れとするマネジメントサイクルを体系的かつ継続的に実施しています。

このマネジメントサイクルにおける各取組の内容・成果等は，この情報セキュリティ報告書において，国民の皆様に毎年確認していただくことになりますが，より実効性のあるマネジメントサイクルの確立及び情報セキュリティの更なる向上に取り組み，より充実した内容・成果等を報告できるよう努めてまいります。

平成２４年５月１６日

最高情報セキュリティ責任者

（法務省大臣官房長）

黒　川　　弘　務

２　平成２３年度の総括

(1)　平成２３年度の評価

平成２３年４月２１日，「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」が，情報セキュリティ政策会議において分冊・改訂されたことを踏まえ，法務省においても昨今の情報セキュリティに係る問題意識や技術的・環境的な変化に対応するため，省庁対策基準及び省庁対策基準に規定された対策内容を具体的に実施するための要領等の一部改正に取り組みました。

また，情報セキュリティ対策の教育・意識啓発に係る取組として，「情報セキュリティ月間」に本省に勤務する課室等情報セキュリティ責任者を対象とした集合研修を実施したほか，自己点検結果の正確性向上のため，自己点検に関する監査の対象を地方官署に勤務する職員まで拡大し，省内全体の情報セキュリティ対策の強化に取り組みました。

加えて，情報処理業務を外部委託する際の調達仕様書に盛り込む情報セキュリティ対策について，必要かつ十分な記載か，最高情報セキュリティアドバイザー等による指導・助言を行いました。

(2)　平成２４年度の目標

平成２４年度は，これまでの取組に加えて，役割に応じた情報セキュリティ対策の教育を実施することや同教育を通じて得た知識・技術等を習得させるための訓練として，平成２３年度，試行的に実施した「標的型メール攻撃の対応訓練」を本省内に拡大し，更に開封時の初動対応・報告まで含めた訓練を実施することについて検討しています。

第２　報告の基本情報

１　法務省の概要

私たちが社会生活を営んでいくためには，ルールが必要です。親子・兄弟等の親族関係の整理・登録や，家に安心して住むことができること，頼んだ材料が手に入れられることなどが，きちんとルール付けられていなければなりません。また，他人を傷つけるような行為，物を盗むような行為をした人がきちんと処罰されることも，この社会を保つために欠かせない仕組みです。

法務省は，このような社会における基本的なルールを定めるとともに，そのルールが守れるような司法の基本的な仕組みや，刑罰を受けた人の社会復帰を援助するための制度，登記・公証のような権利の実現を助ける制度の運営に携わっています。また，出入国が適切に行われるようにすること，人権が尊重されるよう努めたりすること，さらに，社会の安全を守るために必要な調査等を行うことなども，法務省の大事な仕事です。

法務省では，これらの業務を円滑かつ効率的に遂行し，国民の安全・安心な社会を支える根幹として，行政の情報化を図り，以下の情報システムについては，最適化計画を策定の上，情報システムの運用コスト等の削減や業務処理時間の削減を図っているところです。

○　法務省情報ネットワーク（共通システム）

○　登記情報システムの業務・システム

○　地図管理業務の業務・システム

○　検察業務の業務・システム

○　矯正施設被収容者処遇関連情報の管理及び生活維持管理業務・システム

○　更生保護情報管理業務の業務・システム

○　出入国管理業務の業務・システム

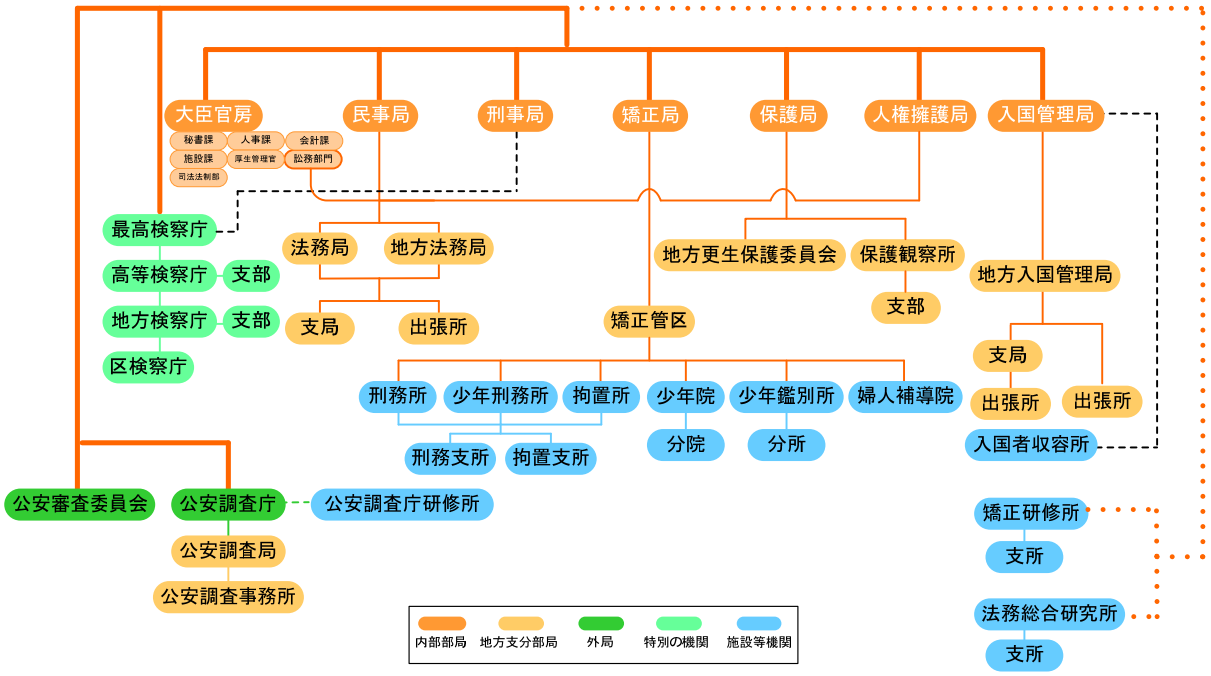
２　報告の対象期間

平成２３年４月１日から平成２４年３月３１日まで

3　報告の対象組織

「本省部局等」及び「所管各庁」

【対象組織図】



「本省部局等」とは，本省内部部局（大臣官房，民事局，刑事局，矯正局，保護局，人権擁護局，入国管理局），法務総合研究所，公安審査委員会及び公安調査庁を指します。

「所管各庁」とは，最高検察庁，高等検察庁，地方検察庁，区検察庁，法務局，地方法務局，矯正研修所，矯正管区，刑務所，少年刑務所，拘置所，少年院，少年鑑別所，婦人補導院，地方更生保護委員会，保護観察所，入国者収容所，地方入国管理局，公安調査局，公安調査事務所及び公安調査庁研修所を指します。

4　報告の対象情報

法務省の保有する情報（検討段階の情報を含む。）のうち，情報システム[1]内部又は外部電磁的記録媒体に保存された電磁的記録[2]，電磁的記録が記載された書面並びに情報システムの開発，構築，運用及び保守に関する設計書

1　情報システムとは，法務省管理の機器等で構成され，一定の目的のために機能する仕組みをいう。
2　電磁的記録とは，電子的方式，磁気的方式その他人の知覚によって認識できない方式で作られる記録であって，電子計算機による情報処理の用に供されるもの（画像，映像，音声を含む。）をいう。

５　報告の担当部署

大臣官房秘書課情報管理室情報政策第二係

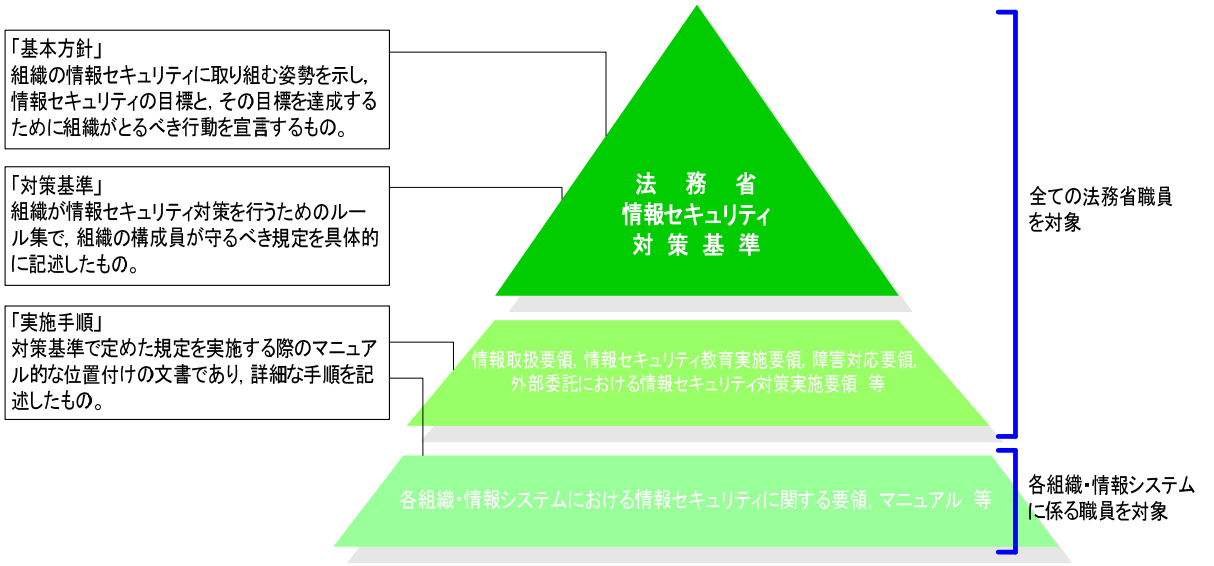
第３　情報セキュリティ対策の枠組み

１　情報セキュリティ対策に関する文書体系

法務省では，「政府機関の情報セキュリティ対策のための統一基準[3]」（平成１７年１２月１３日情報セキュリティ政策会議決定）に準拠した「法務省情報セキュリティ対策基準」（平成１８年４月２７日事務次官決定。以下「法務省基準」という。）及び同基準に規定された対策内容を具体的に実施するための要領等を整備し，法務省における情報セキュリティ水準の維持・向上を図っています。

なお，法務省基準と同基準に規定された対策内容を具体的に実施するための要領等を併せて，「情報セキュリティ関係規程」と総称しています。

【文書体系概略図】



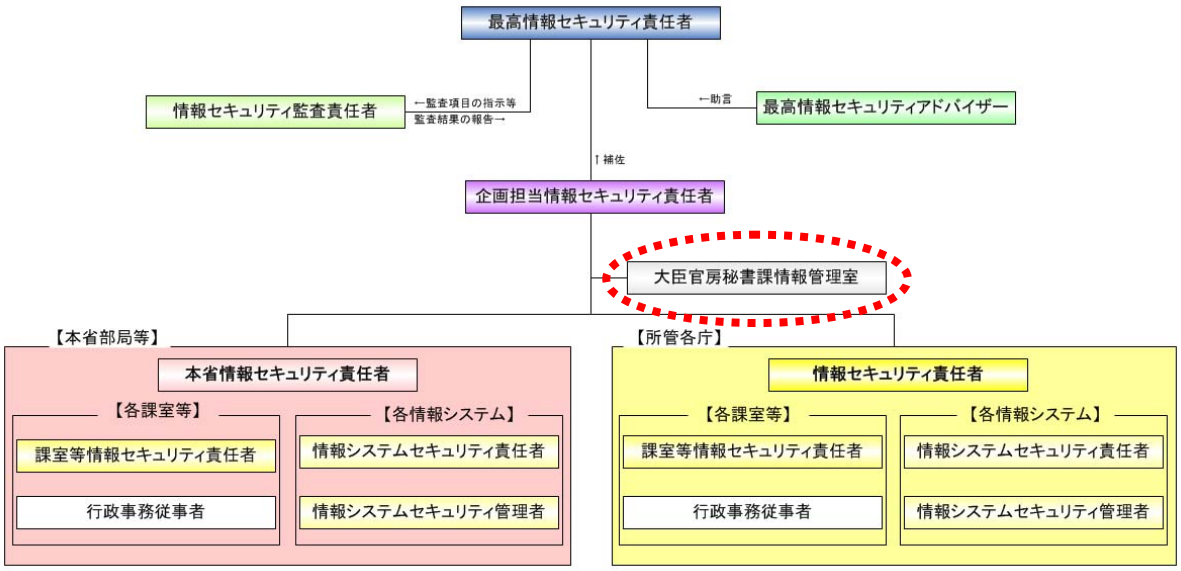
２　情報セキュリティ対策の推進体制

(1)　情報セキュリティ対策に係る組織体制

法務省では，次の組織・体制により情報セキュリティ対策を推進しています。

[3] 平成２３年４月２１日，「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」に分冊することが情報セキュリティ政策会議において決定された。

【推進体制概略図】



○　法務省情報セキュリティ委員会

法務省の情報及び情報システムにおける情報セキュリティ対策の推進に関する事務を総括する。最高情報セキュリティ責任者（大臣官房長）を委員長とし，「電子政府構築計画」（平成１５年７月１７日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）に基づき，法務省における情報化を総合的かつ計画的に推進するために設置された「法務省情報化推進会議」の各委員（本省情報セキュリティ責任者）により構成されている（平成２３年度は３回開催）。

○　最高情報セキュリティ責任者

法務省における情報セキュリティ対策のための体制の整備に関する事務を統括する。

○　最高情報セキュリティアドバイザー

最高情報セキュリティ責任者に対し，情報セキュリティ対策のための体制の整備及び最高情報セキュリティ責任者が特に求める事項に関する助言を行う。

○　情報セキュリティ監査責任者

法務省における情報セキュリティ対策に関する監査事務を統括する。

○　本省情報セキュリティ責任者

本省部局等及び所管各庁における情報セキュリティ対策に関する事務を統括する。

○　企画担当情報セキュリティ責任者

最高情報セキュリティ責任者を補佐し，情報セキュリティ対策のための体制の整備に関する事務を担当する。

○　情報セキュリティ責任者

所管各庁における情報セキュリティ対策に関する事務を統括する。

○　情報システムセキュリティ責任者

情報システムの開発，構築，運用及び保守の各段階を通じて，当該情報システムのセキュリティ対策に関する事務を統括する。

○　情報システムセキュリティ管理者

情報システムセキュリティ責任者を補佐し，当該情報システムのセキュリティ対策に関する事務を担当する。

○　課室等情報セキュリティ責任者

課室等における情報セキュリティ対策に関する事務を担当する。

○　大臣官房秘書課情報管理室

法務省における情報セキュリティ対策のための体制の整備に関する事務を処理する。

(2)　情報セキュリティ対策に係る推進部署の体制

法務省における情報セキュリティ対策の推進・総合調整等の役割を担う部署は，大臣官房秘書課情報管理室情報政策第二係になります。

情報政策第二係は，「法務省基準」に基づく情報セキュリティ対策の実施，法務省情報セキュリティ委員会において決定された事項又は情報セキュリティ政策会議において決定された事項等の周知，省内の情報セキュリティ対策に係る取組の取りまとめ等の事務を所掌しています。

なお，体制は，情報管理室長１名，室長補佐（情報政策担当）１名及び情報政策第二係２名の計４名が担当しており，平均業務経験年数は２年３か月です（平成２４年３月３１日現在）。

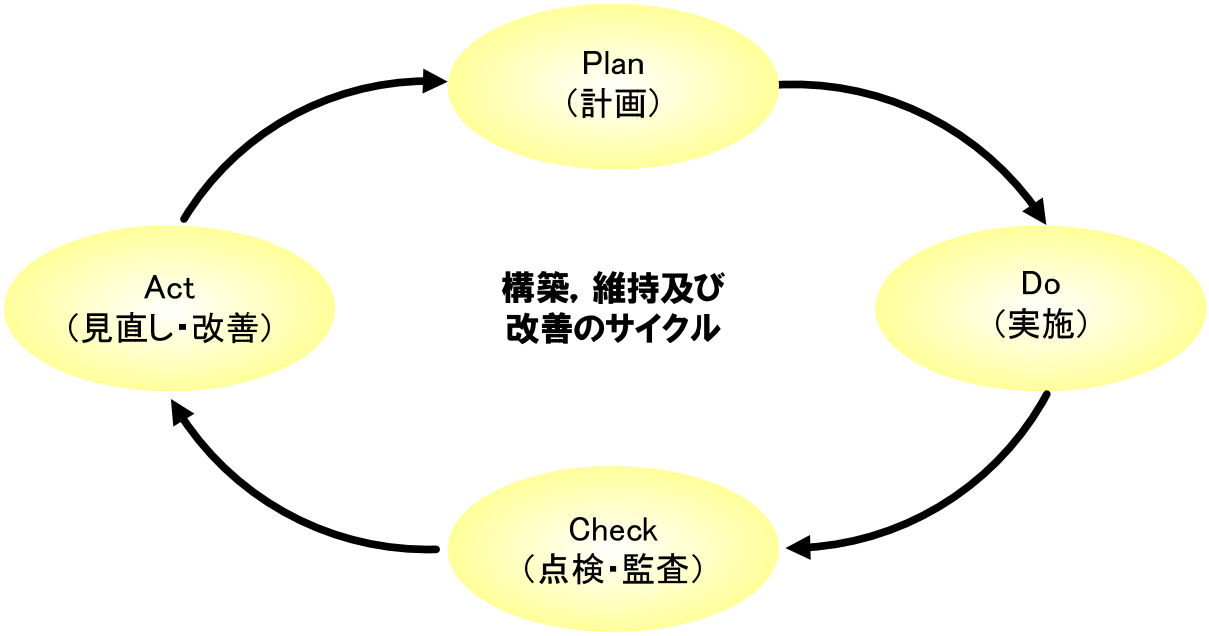
３　情報セキュリティ対策のマネジメントサイクル

情報セキュリティ対策は，一度実施すれば終了するものではなく，常に積極的な対策を講じなければ，新たな脅威に対応できない側面があるため，環境の変化

に合わせて絶えず，見直しと改善が求められます。

法務省では，情報セキュリティ対策における目標達成レベルを継続的に維持・改善するため，ＰＤＣＡの手法を取り入れ，Ｐｌａｎ（計画）―Ｄｏ（実施）―Ｃｈｅｃｋ（点検・監査）―Ａｃｔ（見直し・改善）というマネジメントサイクルを繰り返し実施しています。

ＰＤＣＡサイクルは，以下の各フェーズからなります。



【Ｐｌａｎフェーズ】

問題を整理し，目標を立て，その目標を達成するための計画を立てます。

【Ｄｏフェーズ】

目標と計画をもとに，実際の業務を行います。

【Ｃｈｅｃｋフェーズ】

実施した業務が計画どおり行われて，当初の目標を達成しているかを確認し，評価します。

【Ａｃｔフェーズ】

評価結果をもとに，業務の改善を行います。

４　情報資産台帳の整備と活用

「電子政府推進計画」（平成１８年８月３１日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）及び法務省基準に基づき，新たに情報システムを整備した場

合又は情報システム用機器等に変更が生じた場合には，検収後速やかに，情報資産台帳を作成又は更新することとしており，法務省の保有する情報システムの整備状況をリアルタイムに把握することを目指し，情報システムの予算要求・調達又は情報セキュリティ対策の実施に役立てていきたいと考えています。

第４　平成２３年度の重点事項

１　重点的に取組を行った事項

政府全体の「情報セキュリティ月間」を利用し，本省内に勤務する課室等情報セキュリティ責任者を対象とした集合研修を実施しました。平成２３年度は，内閣官房情報セキュリティセンターから講師を招いて，最新の脅威についての講義のほか，最高情報セキュリティアドバイザーによる標的型メール攻撃の仕組みについての講義を実施しました。

また，地方官署に勤務する職員の情報セキュリティ対策や機器等の情報セキュリティ対策の実施状況をより正確に把握し，自己点検結果の正当性を高めることを目的に，これまで本省内に勤務する職員を対象に実施していた自己点検に関する監査（執務室における情報セキュリティ対策の実施状況）を地方官署に勤務する職員まで拡大しました。

これは，法務省は，中央省庁の中でも組織規模が比較的大きく，所管する業務も多岐にわたっていることから，地方官署に勤務する職員の情報セキュリティ対策や保有する機器等の情報セキュリティ対策について，より適切に実施状況を把握するため，自己点検に関する監査の対象を拡大したものです。

２　重点的な取組に対する評価

昨今の情報セキュリティ上の脅威は，多様化・高度化・複雑化しており，機器等又はネットワークのセキュリティ対策を強化し，多層的に防御する必要があります。機器等又はネットワークのセキュリティ対策は，予算が逼迫した状態にあるものの，機器の設定変更，機能追加又は機能改修，及び最新機器の導入等により，一定のレベルまで計画的な対策を講じることができます。

一方，職員による情報の紛失（漏えい）や情報の誤送信・誤廃棄等の不適切な取扱いは，繰り返し職員を教育することや情報セキュリティに対する意識啓発を

行ったとしても，完全に職員の行動を規制することは困難です。

これまでにも，セルフチェック方式により情報セキュリティ対策の自己点検を実施し，行政事務従事者が情報セキュリティ関係規程に準拠した運用を行っているか確認してきましたが，法務省基準に定める遵守事項は非常に項目が多いため，自己点検を実施する職員の負担が大きいことや概要的な点検とならざるを得ないなどの問題を抱えていました。

そのため，平成２３年度は，自己点検の点検項目を大幅に集約するとともに，自己点検に関する監査の対象を，地方官署に勤務する職員まで拡大しました。これにより，地方官署において情報セキュリティを維持する新たなスキームが形成されたこと，監査実施者の経験に基づく知識の向上が図られること，被監査者に対する意識啓発につながることなどの効果が生じることを期待しています。

第５　情報セキュリティ対策の実施状況

１　教育・啓発

法務省では，毎年，企画担当情報セキュリティ責任者が全ての行政事務従事者を対象にした「年度教育計画」を企画・立案し，同計画に基づいて情報セキュリティ対策の教育を実施することとしています。

平成２３年度に実施した情報セキュリティ対策の教育の概要は，次のとおりです。

【教育の目的】

法務省基準に規定する行政事務従事者の遵守事項を再確認させ，行政事務における情報の適正な取扱いの徹底を図り，もって，法務省内の情報セキュリティ対策水準の維持・向上に努めることを目的としました。

【教育資料の整備】

全ての職員が活用できる内容とし，情報のライフサイクルに従ったフェーズごとの対策が理解できるよう整理しました。

情報セキュリティ対策の教育効果を高めるために，教育用コンテンツや構成等の見直しを毎年行うとともに，重要な事項については繰り返し周知・徹底を図るよう，バランスをとりながら教育資料を作成することに留意しました。

また，教育担当者の理解を深めるために，より詳細かつ技術的な事項を記述した（各責任者の視点等も含む。）補足資料を参考配布したほか，教育資料等に関するアンケート調査を実施しました。

なお，平成２４年度から役割に応じた教育を実施するために，全ての職員を対象としたテキスト，情報セキュリティ責任者及び課室等情報セキュリティ責任者向けテキスト並びに情報システムセキュリティ責任者及び情報システムセキュリティ管理者向けテキストをそれぞれ整備することを計画しています。

【実施期間】

平成２３年５月１０日（火）から同９月３０日（金）まで

【教育担当者】

本省情報セキュリティ責任者又は情報セキュリティ責任者が指名した者

【教育受講状況】

本省情報セキュリティ責任者は，所管する地方支分部局及び施設等機関における教育の受講状況を取りまとめ，企画担当情報セキュリティ責任者に報告することとしており，当該報告を受けた企画担当情報セキュリティ責任者が，法務省全体の教育受講状況を最高情報セキュリティ責任者及び法務省情報セキュリティ委員会に報告しています。

また，正当な理由なく情報セキュリティ教育を受講しない行政事務従事者に対しては，本省情報セキュリティ責任者が，課室等情報セキュリティ責任者をして，教育の受講を勧告することとしています。

なお，平成２３年度における受講状況は，約９８．９％であり，正当な理由なく情報セキュリティ教育を受講していない行政事務従事者はおりません。

【教育の効果測定】

教育した内容の浸透度・理解度を確認するため，これまではチェック形式による確認をしていましたが，平成２３年度から質問形式に変更したことで，より理解度を正確に確認することができたと考えています。

２　自己点検の結果

最高情報セキュリティ責任者を始めとする全ての行政事務従事者において，法務省基準に基づく情報セキュリティ対策の実施状況を確認するため，職員自らが

自己点検を行いました。

自己点検の集計結果は，次のとおりです。

【法務省全体の実施率】

１００％（実施人数／全体の人数）

【総評】

情報セキュリティ対策の自己点検について，網羅的な点検から重点的な点検として点検項目を絞ったことにより，職員の負担軽減を図り，実施率１００％の点検が実施できたものと考えています。

平成２４年度も，自己点検に関する監査の対象拡大・監査における質問（ヒアリング項目）の充実を図り，引き続き高い実施率を維持するよう努めます。

３　情報システムの対策実施状況の検査の結果

内閣官房情報セキュリティセンターが指定する検査項目について，平成２３年１０月１日現在における，公開用ウェブサーバ及びメールサーバの情報セキュリティ対策の実施状況を検査しました。

検査項目及び検査結果は，次のとおりです。

【公開用ウェブサーバ】

○　検査項目

・　サーバの保有台数の調査

・　サーバの運用に関する検査／調査

ＨＴＴＰ通信を行うサーバにおける脆弱性に関する調査，大量のパケット送信型のサービス不能攻撃への対策の状況，ＯＳの最新化の状況（パッチ適用（アップデート）の状況），ウェブサーバアプリケーションの最新化の状況（パッチ適用（アップデート）の状況）

○　実施率

１００％（実施台数／全体の台数）

【メールサーバ】

○　検査項目

・　サーバの保有台数の調査

・　サーバの運用に関する検査／調査

ＯＳの最新化の状況（パッチ適用（アップデート）の状況），電子メールサーバアプリケーションの最新化の状況（パッチ適用（アップデート）の状況）

○　実施率

１００％（実施台数／全体の台数）

【総評】

公開ウェブサーバ及びメールサーバで稼動するアプリケーションの脆弱性を狙った攻撃から情報システムを保護するため，引き続き，高い実施率が維持できるよう努め，より高いレベルで情報セキュリティ水準が維持できるよう，脆弱性を修正するプログラム等が公開されてから適用するまでの期間を短縮することや適用頻度を見直すことについて検討したいと考えています。

４　調達・外部委託

(1)　調達におけるセキュリティ要件の策定

法務省では，「情報システムに係る政府調達の基本指針」（平成１９年３月１日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）に基づき，情報システムに係る調達を実施していますが，セキュリティ要件の策定については，外部の支援業者を調達して企画・設計を行う場合や法務省情報化統括責任者（ＣＩＯ）補佐官の助言等を受けて企画・設計を行う場合等，様々な方法により行われています。

「情報セキュリティを企画・設計段階から確保するための方策（ＳＢＤ：Security By Design）に係る検討会」において策定された「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」が公開されたことを受け，今後は，情報システムを新規構築する場合に限らず，企画・設計段階の業務要件を変更する場合等についても，セキュリティ要件を策定する必要があるため，同マニュアルを活用するなどして，情報セキュリティ水準の維持に努めていきます。

(2)　外部委託先の事業者に求める情報セキュリティ対策

外部委託先の事業者に求める情報セキュリティ対策は，省内の情報システムに係る業務について責任を持って統括する体制（プロジェクト・マネジメン

ト・オフィス（ＰＭＯ））による調達仕様書の妥当性確認に付随して，「外部委託における情報セキュリティ対策実施要領」（平成１８年１０月１３日企画担当情報セキュリティ責任者決定）に従って，調達仕様書に盛り込むべき情報セキュリティ対策の有無及び同対策の内容等について確認し，最高情報セキュリティアドバイザー等から必要な助言を行いました。

また，平成２３年度は，今後，クラウドサービス等を利用する機会が増えることを想定し，「クラウドサービス等を利用する際の留意事項」を盛り込むなどして，同要領の一部改正も実施しています。

５　監査

(1)　監査の概要

情報セキュリティ対策の監査として，情報セキュリティ監査責任者が企画・立案した平成２３年度情報セキュリティ対策の監査計画書に基づき，「情報セキュリティ関係規程に関する準拠性・適合性監査」，「自己点検に関する監査」及び「その他の監査」をそれぞれ実施しました。

平成２３年における監査の実施内容は，次のとおりです。

【情報セキュリティ関係規程に関する準拠性・適合性監査】

法務省基準及び同基準に規定された対策内容を具体的に実施するための要領等が，上位の文書に準拠し，又は適合しているかの確認を行いました。

「法務省基準」は，「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」との準拠性を確認しています。

【自己点検に関する監査】

自己点検結果のとおり，情報セキュリティ対策を講じているか実地に点検対象者を確認し，自己点検結果の正当性を確認する作業を行いました。

監査の対象は，全ての本省情報セキュリティ責任者並びに一部の課室等情報セキュリティ責任者，情報システムセキュリティ責任者，情報システムセキュリティ管理者及び行政事務従事者ですが，今年度は，執務室における情報セキュリティ対策の実施状況の確認を充実させる目的で，監査対象を拡大し，地方官署に勤務する職員まで監査を実施しました。

また，一部の情報システムセキュリティ責任者及び情報システムセキュリティ管理者については，外部の事業者を調達の上，自己点検に関する監査を実施しました。

【その他の監査】

「法務本省内ＬＡＮシステム」のサーバ装置，通信回線装置及びウェブアプリケーションに対する情報システム監査（助言型監査）を，外部の事業者を調達し，実施しました。

「法務本省内ＬＡＮシステム」は，法務本省内における効率的な行政事務遂行のため構築し，本省と所管各庁を接続する法務省情報ネットワーク，霞が関ＷＡＮ，インターネット等の各種ネットワークを中継する機能を提供するとともに，国民等利用者向けサービスである法務省ホームページ等の基盤として稼動する重要な情報システムであることから，毎年，情報システムの脆弱性監査を受けています。

(2)　監査結果等

監査の結果全般としては，緊急に改善を図る必要のある事実は認められず，おおむね適正に運用されているとの結果となりました。

しかし，「情報セキュリティ関係規程に関する準拠性・適合性監査」においては，より準拠性・適合性を確保し得る規定の仕方等について検討することが望ましい部分について，情報セキュリティ監査責任者から助言意見を付しています。当該情報セキュリティ関係規程については，平成２４年度以降の監査において，その改善状況等の確認を行います。

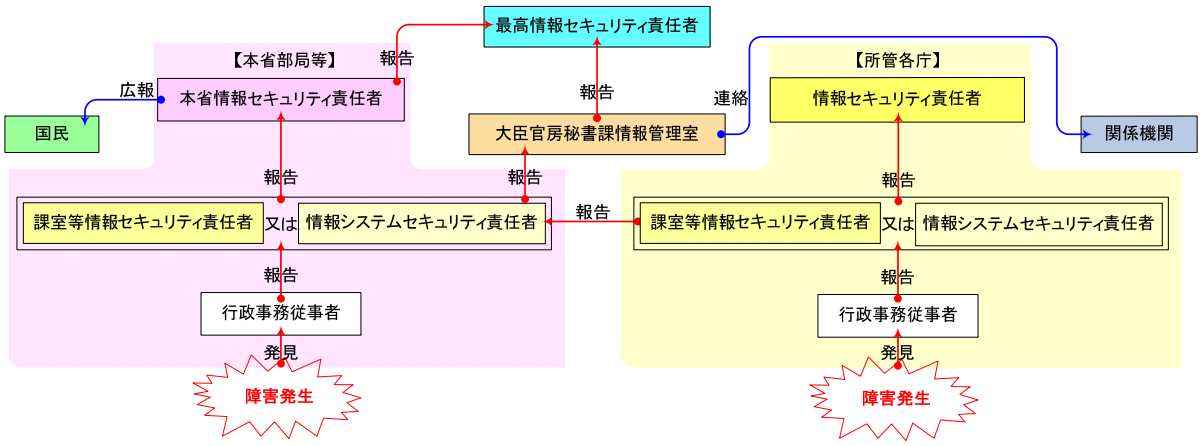
また，「自己点検に関する監査」のうち，本省情報セキュリティ責任者及び課室等情報セキュリティ責任者並びに行政事務従事者を対象とした監査においては，特段の指摘事項はありませんでしたが，情報システムセキュリティ責任者及び情報システムセキュリティ管理者を対象とした監査において，外部委託事業者から，より適切に情報システムの運用等を図るために推奨される事項が報告されています。平成２４年度においては，情報システムの運用管理を担当する係と監査の実施を担当する係が連携し，報告された内容について整理・検討した上で，対応することとします。

第６　情報セキュリティに関する障害・事故等

１　情報セキュリティに関する障害・事故等の把握

所管各庁で障害・事故等が発生した場合の行政事務従事者から最高情報セキュリティ責任者への報告経路は，①行政事務従事者→②情報システムセキュリティ責任者又は課室等情報セキュリティ責任者（所管各庁）→③情報システムセキュリティ責任者又は課室等情報セキュリティ責任者（本省部局等）→④本省情報セキュリティ責任者及び大臣官房秘書課情報管理室→⑤最高情報セキュリティ責任者となります。

【障害・事故等発生時の報告経路】



２　障害・事故等の概要，それに対する対応等

平成２３年度，法務省では３件の情報セキュリティに関する障害が発生しました。いずれも情報が流出した事実は確認されていませんが，事案を発生させたことについて深く反省し，既に関係機関等において注意喚起するとともに再発防止策を講じています。

今後，情報システムによる行政サービスの安定的な提供を目指し，法務行政の信頼性の向上に努めてまいります。

以下は３件の事案概要等になります。

○　１件目

【概要】

事故者は，平成１９年１月ころから平成２２年９月ころにかけ，①自己所有のＵＳＢメモリに職務上の情報を保存して庁舎外に持ち出し，②貸与を受けた法務省管理のＵＳＢメモリの適正な管理を怠り，同ＵＳＢメモリを紛失し，③

他の職員の識別コードを使用して，サーバに不正アクセスしたものである。

【原因】

事故者の情報の取扱いに対する意識が低かったことによるものである。

【対応】

事故者が保有する情報を回収し，情報流出の防止を図った。

【情報セキュリティ関係規程】

法務省管理以外の外部電磁的記録媒体に情報を保存することは原則禁止されている。

【再発防止策】

該当庁において，情報の管理を徹底するよう職員研修を実施し，注意喚起を行った。

○　２件目

【概要】

事故者は，平成２３年１０月ころ，モバイルパソコンにおいて作成した文書を出力し，同文書をキャリーバッグに入れて帰庁したところ，同文書が紛失していることに気が付いたものである。

【原因】

事故者が同文書の存在について確認・注視することを怠ったものによる。

【対応】

移動経路を検索したほか，遺失物等について関係機関に照会を行った。

【情報セキュリティ関係規程】

要機密情報が記載された書面を運搬するときは，郵送等を利用するに当たっては，これを親展とするなどし，携行するに当たっては，当該書面を封筒又は書類鞄等に収納し，盗難又は置忘れ等の防止に努めることが規定されている。

【再発防止策】

情報の取扱いを一層慎重に行うよう関係職員を指導した。

○　３件目

【概要】

事故者は，平成２３年１２月，使用権限のないＩＤ・パスワードを使用して内部のネットワークに不正アクセスし，閲覧が許可されていないファイルを閲

覧したものである。

【原因】

事故者の情報セキュリティに関する意識が低かったことによるものである。

【対応】

証跡を確認し，情報の持ち出し又は漏えいがないか確認した。

【情報セキュリティ関係規程】

情報及び情報システムの取扱いに当たっては，行政事務遂行上の必要性に留意することが規定されている。

【再発防止策】

情報セキュリティ関係規程の遵守のほか，電磁的記録に対するアクセス制御，保存場所又は保存方法等，適正な管理について，所管各庁に注意喚起文書を発出した。

第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，これまでの取組に加えて，役割に応じた情報セキュリティ対策の教育を開始すること，及び同教育を通じて得た知識・技術等を習得させるための訓練を情報システムごとに実施することを計画しています。

情報セキュリティ対策は，情報セキュリティを担当する職員や情報システムの関係職員のみが実施するものではなく，情報及び情報システムを取り扱う全ての職員が実施するものです。

また，情報セキュリティ対策は，情報及び情報システムを取り扱う全ての職員が，職制及び職務に応じて与えられている権限と責務を理解した上で，負うべき責務を全うすることで実現されることから，それらの権限と責務の正確な理解が情報セキュリティ対策の適正な実施に欠かせない条件となります。

したがって，平成２４年度は，①全ての行政事務従事者向けのテキスト，②情報セキュリティ責任者及び課室等情報セキュリティ責任者向けのテキスト，③情報システムセキュリティ責任者及び情報システムセキュリティ管理者向けのテキストをそれぞれ整備し，情報セキュリティ上の役割に応じて与えられている権限と責務を理解させる内容の教育を開始します。

加えて，平成２４年度は，情報セキュリティ対策の教育を通じて得た知識・技術等を習得させるための訓練を，情報システムごとに実施することを考えていま

す。

なお，平成２３年度は１１４名の職員を対象として「標的型メール攻撃の対応訓練」を試行的に実施しましたが，平成２４年度はその対象を拡大することに加え，更に開封時の初動対応・報告まで含めた訓練を実施することについて検討しています。

第８　結び

法務省においては，多様化・高度化・複雑化が進む情報セキュリティ上のリスクに対して，ＰＤＣＡサイクルの手法を用いた情報セキュリティマネジメントサイクルを体系的かつ継続的に実施することで，省内全体の情報セキュリティ水準の維持・向上に取り組んでいます。

法務省の組織規模・組織構成，取り扱う情報の性質等を考慮すれば，情報セキュリティガバナンスの強化として，地方官署における情報セキュリティ対策の実施状況を確認する仕組みが不可欠であると考えており，平成２３年度，自己点検に関する監査の対象範囲を地方官署まで拡大できたことに対しては，一定の効果が期待できると評価しています。

一方，情報セキュリティを取り巻く環境の変化は著しく，引き続き省内において情報セキュリティを担う体制の強化や各情報システムの対策実施状況をリアルタイムで確認できる仕組みの構築，インシデント対応部隊・情報セキュリティ監査実施部隊の整備等，課題が残されていると認識しています。

さらに，平成２３年度は３件の情報セキュリティに関する障害が発生・発覚したことを再認識し，二度と同種同様の事案が発生しないよう機器等の情報セキュリティ対策に加え，職員による情報の取扱いの徹底，運用面における情報セキュリティ対策，情報セキュリティポリシーの充実等を図っていきたいと考えています。

最高情報セキュリティアドバイザーとしては，情報セキュリティを企画・設計段階から確保するための方策（SBD: Security By Design）の観点を踏まえ，調達仕様書の妥当性確認時に，セキュリティ要件定義が必要かつ十分か確認するなどして，法務省の情報及び情報システムを保護するために，必要な助言・提案を行いたいと思います。

平成２４年５月１６日

最高情報セキュリティアドバイザー

（法務省ＣＩＯ補佐官）

大　成　　宣　行