平成23年度情報セキュリティ報告書

平成24年５月

警察庁

はじめに　～最高情報セキュリティ管理者からのメッセージ～

飛躍的な発展を続ける情報通信技術は、あらゆる分野で活用され、インターネットを始めとする情報システムは今や我々の生活に欠かせないものとなっています。

警察においても、限られた警察力をより効果的に発揮するため、数多くの情報システムを導入しています。中には24時間稼働しているシステムも多く、大規模災害時等でも止まることがないよう諸対策を施し、可用性の確保にも力を入れています。その一方で、システムのぜい弱性を狙った攻撃やコンピュータ・ウイルス等の脅威は、情報システムの導入が進めば進むほど増大し、一たび情報の流出や情報システムに障害等が発生した際の影響は、計り知れないものがあります。

警察庁では、犯罪捜査や運転免許に係る個人情報等を保有していることから、情報システムの適正な運用に努めるとともに、情報セキュリティの確保を図るため、「警察情報セキュリティ訓令」を始めとする規程を定めており、平成23年度は次の対策に重点を置いて取り組んできました。

- 標的型メール攻撃に係る取組
- 証跡の取得項目の拡大

本報告書は、警察庁において平成23年度に実施した情報セキュリティ対策の状況等を取りまとめたものです。

平成23年度に情報セキュリティに関する重大な障害・事故等は発生しておりませんが、引き続き情報セキュリティの確保に万全を期すため、諸対策の継続・強化に努めてまいります。

最高情報セキュリティ管理者
（警察庁情報通信局長）
佐野　淳

第１　本報告書の目的

警察庁は、長官官房と五つの局、二つの部から成る内部部局と、三つの附属機関、九つの地方機関により構成されており、広域組織犯罪に対処するための警察の態勢、犯罪鑑識、犯罪統計等、警察庁の所掌事務について都道府県警察を指揮監督している。

また、警察庁の情報システムでは、これら業務に係る犯罪情報や運転免許に関する情報等の機密性の高い情報を多く取り扱っており、この情報の流出、漏えい等が発生すると、国民に対して多大な損害を与えることになることから、これを防ぐため、警察庁では、各種の情報セキュリティ対策を講じている。

本報告書は、平成23年度の警察庁における情報セキュリティに係る取組等について、国民に対して広く周知することを目的としている。

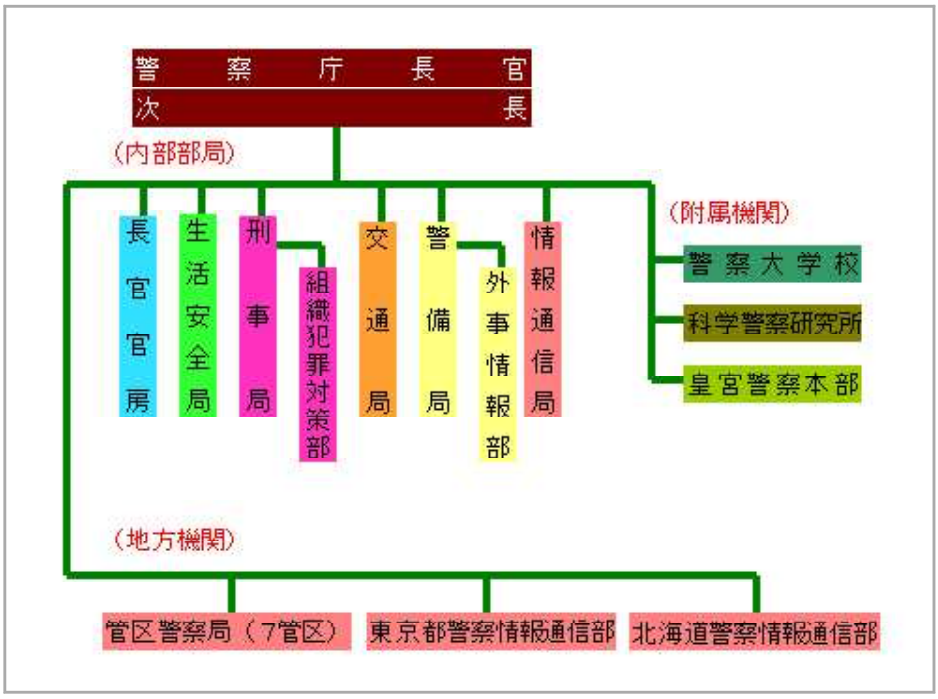

図１　警察庁の組織図

第２　情報セキュリティ対策の枠組み

１　情報セキュリティに係る文書体系

警察庁では、情報システム及び情報システムで取り扱われる情報に関して、体系的かつ網羅的な管理の基準及びそれを組織的に実施するための基本的事項を定めた「警察情報セキュリティに関する訓令」及びこれに基づいて定めた情報セキュリティに関する規程により構成される「警察情報セキュリティポリシー」により、情報セキュリティの維持を図っている。

警察情報セキュリティポリシーを構成する各規程については、情報セキュリティに関する情勢等を踏まえて随時見直しているところである。

２　情報セキュリティに係る管理体制

警察庁では、図２のとおり、最高情報セキュリティ管理者の下、内部部局、附属機関及び地方機関のそれぞれに情報セキュリティ管理者を、また、各所属に運用管理者を置き、情報セキュリティの維持のための体制を整備している。

また、各情報システムの整備を担当する所属の長をシステムセキュリティ責任者、また、維持管理を担当する所属の長をシステムセキュリティ維持管理者とし、情報システムの設計・整備から運用・維持管理まで、一連のライフサイクルを考慮した情報セキュリティ対策に取り組んでいる。

さらに、情報システムに係る情報セキュリティに関する監査の実施を統括する者として情報セキュリティ監査責任者を置き、情報セキュリティ対策の実施の徹底を図っている。

なお、情報セキュリティに関する重要事項については、最高情報セキュリティ管理者を委員長とし、各局部の庶務担当課長等を委員とする情報セキュリティ委員会において審議している。

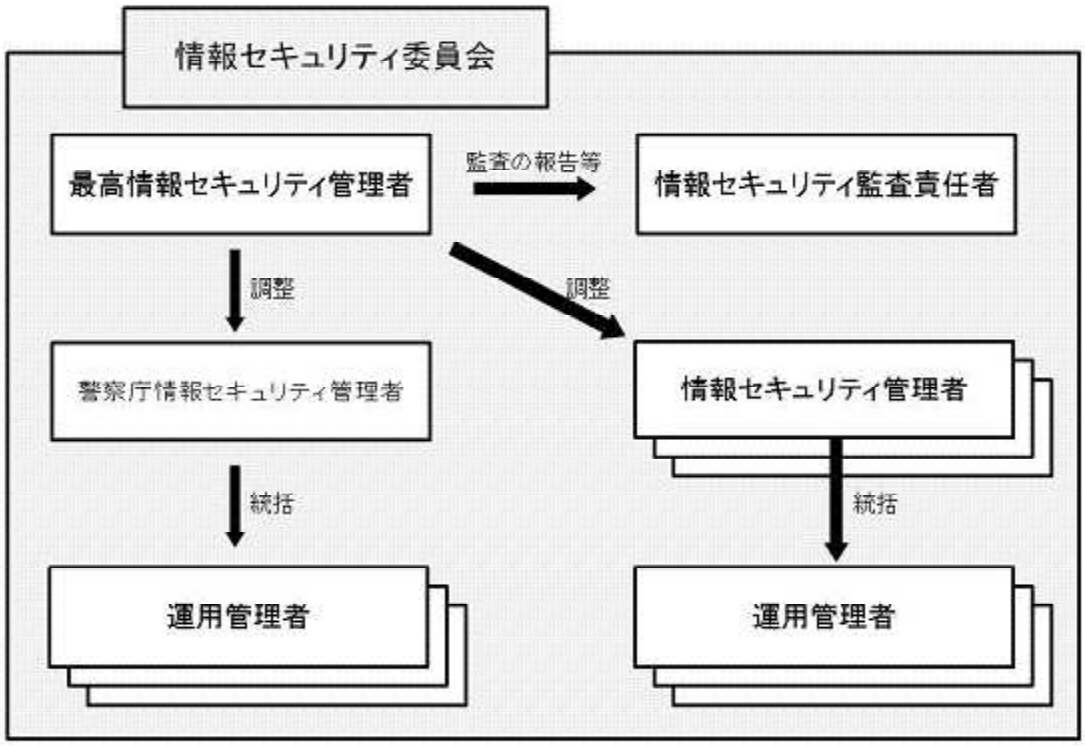

図２　情報セキュリティに係る管理体制

３　特異事案発生時の連絡体制

警察庁では、国民生活又は警察活動に重大な支障が生じ得る情報セキュリティに関する障害、事故等（以下「特異事案」という。）が発生した場合の措置要領を定めている。その概要は次のとおりである。

○　職員は、特異事案を認知した場合は、当該職員が属する機関の情報セキュリティ管理者に速やかにその概要を報告する。あわせて、被害の拡大を防止するための一時的な措置を講じる。

○　報告を受けた情報セキュリティ管理者は、警察庁情報セキュリティ管理者に速やかに報告する。このとき、警察庁情報セキュリティ管理者は、当該事案の種別に応じて、関係する所属の長に連絡する。

○　情報セキュリティ管理者は、関係するシステムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者と緊密に連携し、当該事案の原因調査及び再発防止策を講じ、その内容を警察庁情報セキュリティ管理者に報告する。

第３　警察庁における情報セキュリティ対策

１　庁舎管理

庁舎出入口にセキュリティゲートを設け、身分証を持たない者の入館を禁じるとともに、警備員による常時警戒を行うことで、不審者の立入りを防止している。

２　個人所有のパソコンの業務使用禁止

公用パソコンを１人１台整備し、個人所有のパソコンの業務使用を禁止している。

３　ネットワークの分離

警察以外の機関と電子メールの送受信を行うための外部ネットワークと、警察情報を作成したり警察内部の電子メールを送受信したりする内部ネットワークとを完全に分離し、要機密情報は内部ＷＡＮシステムでのみ取り扱うこととしている。これにより、警察情報を窃取等するための外部からの攻撃は不可能になっている。

４　外部記録媒体の取扱い

(1)　自動暗号化機能

平成19年に、各情報システムにおいて外部記録媒体に情報を保存する際に自動的に暗号化する機能を具備させた。これにより、万が一、外部記録媒体を紛失した際にも、警察以外の機関には当該外部記録媒体に保存された情報を読み取ることができない。

(2)　外部記録媒体の利用制限措置

外部記録媒体による情報漏えいを防止するため、平成19年に、許可なく外部記録媒体を利用できなくするための技術的措置を講じた。これにより、電子計算機から要機密情報を持ち出す際には、上司がパソコン上で許可手続を行う必要がある。

(3)　個人所有の外部記録媒体の利用禁止措置

平成22年に、職員が上司の許可を受けて外部記録媒体を利用する場合であっても、公用の外部記録媒体以外の利用を不可能とする技術的措置を講じた（図３を参照。）。

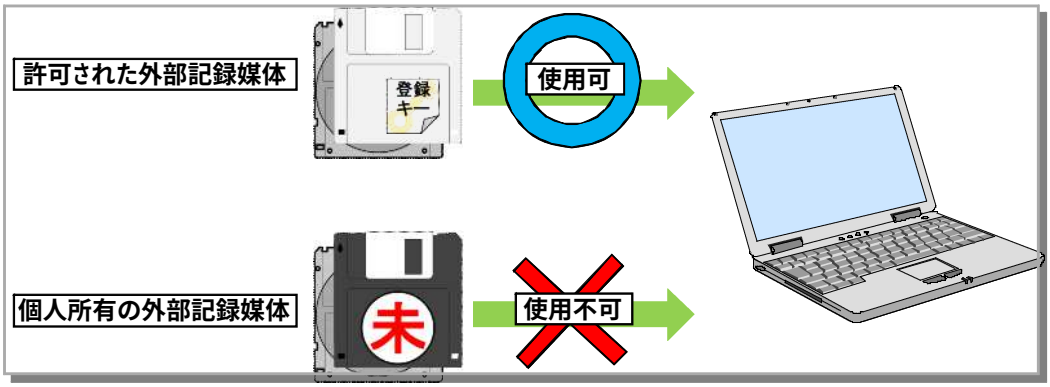

図３　無許可の外部記録媒体の利用を技術的に禁止するソフトウェア

第４　平成23年度の取組

１　標的型メール攻撃に係る取組

昨今、行政機関等において標的型メール攻撃によるウイルス感染事案が発生したことを受け、外部との電子メールの送受信を行っている職員を対象に、標的型メール対処訓練を実施した。本訓練を通して、全職員にメールを不用意に開封することでウイルス感染が起こり得ることを周知し、注意を呼びかけた。

２　証跡の取得項目の拡大

情報漏えいを防止する観点から、内部ネットワークについて、従来取得してきた外部記録媒体の証跡に加え、ファイル操作、印字等の証跡等新たに取得する項目を追加した。

３　情報セキュリティに係る教育

(1)　学校教育の実施

警察では、職員に対し、上級の幹部として必要な知識、技能、指導能力及び管理能力を習得させるための教育訓練等を行う機関として､警察大学校を設置している。警察大学校では、様々な課程を設け、警察の各分野における高度な教育を行っており、その中で情報セキュリティに対する理解を深められるよう講義を行った。

特に、情報セキュリティについて指導する者を育成するための課程を設け、警察情報セキュリティポリシーにおける規定事項、情報セキュリティに関する技術、特異事案発生時の対応等について、実践的な訓練を交えて講義を行った。

(2)　教育資料の作成

警察情報セキュリティポリシーに係る職員及び運用管理者の理解を促すために、警察情報セキュリティポリシーにおけるそれぞれの責務等について解説する資料を作成し、配布した。

(3)　情報処理能力検定

警察職員の情報処理に関する知識及び技能の修得意欲を高め、その能力の普及及び向上に資するため、情報処理能力検定を受験させている。初級を端末を操作する職員、中級を各所属の指導員、上級をシステム開発要員と位置付け、業務に応じて各級を受験するよう推奨している。

4　異動期における対策

異動期においては、通常期に増して情報管理の徹底が必要となることから、職員が利用している端末からの不必要な情報の削除及びその確認、新規採用者への情報セキュリティに関する教育の実施等、具体的な指示を行い、これに係る手順等をまとめた資料を作成した。

5　情報セキュリティの維持の実施状況の自己点検

(1)　概要

職員の情報セキュリティに対する理解の醸成を図るため、毎年度、情報セキュリティの維持の実施状況の自己点検を実施している。

平成23年度は、警察庁情報セキュリティ管理者が、役割ごとに警察情報セキュリティポリシーに規定されている遵守事項の実施状況を点検できる点検票を作成して、全ての職員及び情報セキュリティに係る各管理者等に対して配布し、各々が当該点検票を用いて実施した。その後、警察庁情報セキュリティ管理者は点検票を収集し、その内容を確認した。

(2)　結果

全ての職員及び情報セキュリティに係る各管理者等が自己点検を実施し、全ての者が、役割ごとに警察情報セキュリティポリシーに規定されている遵守事項を全て遵守していることを確認した。今後もこの水準を維持するため、継続的に情報セキュリティに関する教育を実施していく必要がある。

6　情報システムにおける情報セキュリティ対策の検査

(1)　概要

情報システムにおける情報セキュリティ対策の徹底のため、毎年度、情報システムにおける情報セキュリティ対策の実施状況の検査を行っている。

平成23年度は、情報システムを構成する機器のうち、情報セキュリティを確保する上で重要な端末装置、ウェブサーバ及び電子メールサーバを対象にして検査を行った。主な検査項目は、次のとおりである。

ア　端末装置

(ｱ)　不正プログラム対策

ＯＳ及び主要なアプリケーションのセキュリティパッチの適用、ウイルス対策ソフトの導入等

(ｲ)　盗難防止対策

セキュリティワイヤーの導入、保管庫の施錠管理等

(ｳ)　暗号化機能の導入

ハードディスクに記録する情報の自動暗号化機能の導入等

イ　ウェブサーバ

(ｱ)　不正プログラム対策

ＯＳ及びアプリケーションのセキュリティパッチの適用、ウイルス対策ソフトの導入等

(ｲ)　アクセス管理

利用者及び管理者権限のアクセス管理の徹底

(ｳ)　通信の暗号化

遠隔保守における通信経路の暗号化

(ｴ)　情報のバックアップ

ウ　電子メールサーバ

(ｱ)　不正プログラム対策

ＯＳ及びアプリケーションのセキュリティパッチの適用、ウイルス対策ソフトの導入等

(ｲ)　アクセス管理

利用者及び管理者権限のアクセス管理の徹底

(ｳ)　通信の暗号化

インターネット経由の通信経路の暗号化

(ｴ)　情報のバックアップ

(2)　結果

検査により、端末装置、ウェブサーバ及び電子メールサーバに係る全ての検査項目について、必要な対策が実施されていることを確認した。今後もこの水準を維持するため、継続的に各種対策を実施していく必要がある。

7　情報セキュリティ監査

(1)　概要

情報セキュリティ対策の実施状況を確認し、対策の徹底を図るとともにその効果を高めていくために、毎年度、情報セキュリティ監査（以下「監査」という。）を実施している。

平成23年度の監査計画については、情報セキュリティ監査責任者が、情報セキュリティ委員会の審議を経た上、最高情報セキュリティ管理者の承認を得て策定した。当該計画に記載された監査の内容は、次のとおりである。

ア　関係規程に関する準拠性の監査

警察情報セキュリティポリシー及びこれに関する規程が、「政府機関の情報セキュリティ対策のための統一基準群」に準拠していることを確認するもの。

イ　情報流出事案防止対策等の実施状況の監査

情報流出事案防止対策、情報セキュリティに関する教育、情報セキュリティ侵害事案への対応等の実施状況が適切に実施されていることを確認するもの。

ウ　自己点検の妥当性の監査

情報セキュリティの維持の実施状況の自己点検の結果が妥当であることを確認するもの。

エ　警察庁運転免許証認証局の監査

警察庁運転免許証認証局が適切に運用管理されていることを確認するもの。

オ　例外措置の適用申請及び許可状況の監査

警察情報セキュリティポリシーの例外措置の適用申請について、定められた手続によって適切に管理されていることを確認するもの。

(2)　結果

監査を実施した結果、各システムの情報セキュリティ対策は良好であり、情報セキュリティ侵害事案を想定した訓練の実施、毎月の情報セキュリティに関する教育の実施等、積極的な取組がみられたが、情報流出事案防止対策等の実施状況において軽微な改善を要する事項が見られた。

監査終了後、監査報告書を最高情報セキュリティ管理者に提出するとともに、改善を求める事項、検討を要する事項等を、情報セキュリティ委員会の審議を経て決定し、対象部署の長に指示した。指示を受けた対象部署の長は、当該指示の内容を踏まえ、速やかに必要な措置をとり、その結果を最高情報セキュリティ管理者に報告することとされている。

結果の概要は、次のとおりである。

ア　関係規程に関する準拠性の監査

警察情報セキュリティポリシー及びこれに関する規程に関し、「政府機関の情報セキュリティ対策のための統一基準群」と対比して内容の整合性を確認することにより、適切に準拠していることを確認した。

イ　情報流出事案防止対策等の実施状況の監査

面接調査、実地調査等により、情報流出事案防止対策等が、おおむね適切に実施されていることを確認したものの、軽微な改善を要する事項が見られた。

ウ　自己点検の妥当性の監査

面接調査により自己点検の結果との相違の有無を確認し、自己点検が適正に実施されたことを確認した。

エ　警察庁運転免許証認証局の監査

外部の事業者が実施した「府省認証局監査基準作成ガイドライン」の準拠性監査及びぜい弱性監査の報告書を確認し、警察庁運転免許証認証局が適切に運用管理されていることを確認した。

オ　例外措置の適用申請及び許可状況の監査

例外措置の適用審査記録の台帳を確認し、例外措置の適用申請について定められた手続により適切に管理されていることを確認した。

8　障害・事故等への対応

平成23年度においては、重大な障害・事故等は発生していない。特異事案発生時の措置要領の定めるところにより、迅速な対応に努めており、勤務時間外及び休日における連絡系統図等連絡網を適正に管理し、特異事案発生時の対応に備えた。

第５　平成24年度における取組の方針

１　継続した取組

これまで実施している基本的な対策は、既知の脅威への対応や情報セキュリティ意識の底上げに有効であることから、情報セキュリティに関する指導・教育、自己点検、重点検査及び監査を継続して行うこととする。

２　情報セキュリティ対策に関する平成24年度の計画

継続した取組に加え、きめ細かな対策を行うことにより一層の情報セキュリティの確保を図るため、各級の管理者に対する教育等を行い、組織全体の情報セキュリティレベルを更に高める。特に、情報セキュリティ監査を例年よりも実地を重視したものとし、更なる強化を図る。

また、変遷する社会情勢に対応するための警察活動の変化、情報通信技術・サービスの多様化、「政府機関における情報セキュリティ対策のための統一基準群」等の改正を踏まえ、警察情報セキュリティポリシーの見直しを行う。

おわりに　～最高情報セキュリティアドバイザーからのメッセージ～

犯罪は、24時間365日途切れることなく発生し、これに対峙するため捜査指揮や効率的な捜査を支援する情報システムは警察業務にはなくてはならないものとなっており、一旦、システム障害等が起こるとその影響は計り知れません。また、警察は多くの個人情報等を保有しているため、その管理を徹底する必要があります。

このため、警察職員は警察情報セキュリティポリシーを遵守し、これら情報システムを様々な脅威から守り、情報流出等の防止を図っています。日々生まれてくる新たな脅威にどのように対応していくべきか、我々は日々議論し、知恵を出し合いながら対策を練っています。

情報セキュリティ対策には、「これで大丈夫。」という終わりはなく、新たな攻撃手法や巧妙化する手口等に対し、現在執っている対策で十分なのか、それとも更なる対策が必要なのかを検討・評価し、必要に応じて改善する、いわゆるＰＤＣＡサイクルを繰り返し回し、課題解決に向けた取組を継続していく必要があります。

平成23年度も端末、ウェブサーバ、電子メールサーバ等に対して重点的に検査を実施しました。また、個々の職員に対しても自己点検を引き続き行い、情報セキュリティに対する意識の向上を図りました。さらに、年度計画に基づく情報セキュリティ監査及び警察庁運転免許証認証局の監査を行いました。

このような基本的な取組を継続するとともに、監査による確認を的確に行い、一層の情報セキュリティの確保に努めていく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
（警察庁情報通信局情報管理課長）
羽室　英太郎