情報セキュリティ報告書

平成 24 年 5 月

公正取引委員会

目　次

はじめに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1

１　平成 23 年度の総括 ・・・・・・・・・・・・・・・・・・・・・・・・・2

２　本報告の基本情報・・・・・・・・・・・・・・・・・・・・・・・・・・3

３　情報セキュリティ対策の枠組み・・・・・・・・・・・・・・・・・・・5

４　平成 23 年度の重点事項 ・・・・・・・・・・・・・・・・・・・・・・8

５　情報セキュリティ対策の実施状況
５．１　自己点検結果・・・・・・・・・・・・・・・・・・・・・・・・・10
５．２　情報システムごとの状況・・・・・・・・・・・・・・・・・・・・12
５．３　教育・啓発・・・・・・・・・・・・・・・・・・・・・・・・・・13
５．４　調達・外部委託・・・・・・・・・・・・・・・・・・・・・・・・14
５．５　その他取り組んだ事項・・・・・・・・・・・・・・・・・・・・・14

６　情報セキュリティに関する障害・事故等報告・・・・・・・・・・・・15

７　情報セキュリティ対策に関する平成 24 年度の計画 ・・・・・・・・15

おわりに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・16

はじめに

平成 23 年度に実施した各種情報セキュリティ対策の具体的な内容をとりまとめ，情報セキュリティ報告書を作成しました。公正取引委員会においては，本報告書に記載したとおり，平成 23 年度には，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らず，また，緊急に対応が必要な重大な課題も発生していません。

しかし，情報セキュリティを取り巻く環境は常に変化しており，不正アクセスや不審メールによる攻撃等，情報セキュリティに対する脅威は増加する状況にあります。公正取引委員会においても，特段の被害はなかったものの，平成 23 年度中には，実際に，新型のウイルスが添付された不審メールを受信する事例が発生しています。これらの状況から，公正取引委員会が使用するシステムについても，常に，これらの脅威に対して十分な対策を採ることが必要不可欠な状況となっています。

そこで，公正取引委員会では，情報セキュリティに対する脅威への対応策を常に見直すとともに，全職員に対する情報セキュリティに関する最新情報の提供や，情報セキュリティに関する教育内容の充実を図ることによって，情報セキュリティ対策を万全なものとするための対策を講じております。

今後も，公正かつ自由な競争を促進して，一般消費者の利益を確保するとともに，我が国経済の健全な発達を図るという，公正取引委員会の役割を十分に果たすため，情報セキュリティ対策の充実に努めてまいります。

最高情報セキュリティ責任者
（官房総括審議官）
松尾　勝

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

（ア）職員による情報セキュリティ対策の実施状況の改善

職員による情報の取扱いに係るセキュリティ対策の実施状況を改善することに重点的に取り組みました。

この結果, 職員の情報セキュリティ対策の実施状況に改善が見られましたが, まだ十分ではない部分もあることから，引き続き，職員への教育等を通じて，情報セキュリティ対策の実施状況の改善を図っていきます。

（イ）標的型メール攻撃への対策

政府機関等に対するメールを利用した攻撃が増大していることを受け, その対策として，全職員への注意喚起及び訓練の実施に重点的に取り組みました。

今後も，職員への教育，訓練等を通じて，継続的に対策を採っていきます。

イ　情報セキュリティ対策の実施状況の自己点検結果

全職員を対象とした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。）を実施した結果，ほとんどの項目において適切に情報セキュリティ対策が実施されていましたが, 一部に情報セキュリティ対策の実施が十分ではない項目が見受けられましたので, 引き続き, 情報セキュリティ対策の実施状況の改善に努めていきます。

ウ　情報システムごとの状況

平成 23 年度の重点検査については，内閣官房情報セキュリティセンター（以下「ＮＩＳＣ」という。）の指定する検査項目を内部調査した結果，公正取引委員会の全ての公開用ウェブサーバ及び電子メールサーバについて最高の評価（実施率 100%）となりましたので，同結果をＮＩＳＣに報告しました。引き続き，適切な情報セキュリティ対策に努めていきます。

エ　教育・啓発

情報セキュリティ対策に関し，全職員を対象とした e-ラーニング研修を実施したほか，管理職員及び新規・中途採用職員に対しては，これに加えて集合研修も実施しており，さらに，情報セキュリティに係る最新の参考情報を，随時，イントラネット等を通じて全職員に対して提供しています。これらの研修等を通じて，情報セキュリティに対する全職員の理解を深めるように努めています。

オ　調達・外部委託

情報処理業務を外部委託によって行う場合には，調達仕様等に含めるべき事項を示した規程や，情報の保護に関する誓約書のひな形を作成するなど，必要な情報セキュリティ水準を確保できるように取り組んでいます。

カ　情報セキュリティに関する障害・事故等の報告

昨年６月に，外部から当方の職員宛てにメールが送付され，当該メールに添付されていた，不正プログラムが組み込まれたファイルを職員が開封するという事案がありましたが，他の端末への感染，情報流出等の被害はありませんでした。

公正取引委員会では，不審なメールを受信した際の対応について研修の機会等を通じ，職員に対して繰り返し周知しており，メールを利用した攻撃に対しては，前述ア（イ）で示したように，重点的に対策を採っていきます。

（２）平成 24 年度の目標

公正取引委員会では，以下の目標に重点的に取り組むことによって，情報セキュリティレベルの更なる向上を図っていきます。

ア　平成 23 年度の自己点検において，十分に情報セキュリティ対策が実施されていなかった項目について，職員にその実施を促すため，研修資料の見直しや職員が実施すべき対策の周知を行っていきます。

イ　メールを利用した攻撃への対策として，職員への不審メール情報の発信，教育，訓練等の対策を採っていきます。

２　本報告の基本情報

（１）公正取引委員会の概要

公正取引委員会は，公正かつ自由な競争を促進することにより，一般消費者の利益を確保するとともに，国民経済の民主的で健全な発達を促進するため，独占禁止法及び下請法の厳正かつ的確な運用に努めています。

具体的な業務としては，私的独占，価格カルテル，入札談合，不公正な取引方法等の違反行為を排除し，さらに，これらの行為を行った事業者に対して課徴金の納付を命じるほか，競争政策に関する調査・研究・提言，経済・事業活動の実態調査，株式取得・会社の合併等に係る届出の受理，下請法違反行為の排除等を行うとともに，競争政策に関する国際的連携の強化にも努めています。

公正取引委員会において構築・運用している主な情報システムは，以下のとおりです。

ア　公正取引委員会内ネットワーク（共通システム）

業務遂行に当たり基盤となるインフラ系システムで，職員に対して電子メール，電子ポータル，電子掲示板，ファイル共有等の機能を提供しています。

イ　審決等データベース

独占禁止法に係る審決等データを蓄積・保存するとともに，国民の皆様の活用に資するため，検索機能を備えて公開しているシステムです。

ウ　公正取引委員会ホームページ

公正取引委員会の活動について，国民の皆様に情報発信していくためのシステムです。

（２）本報告の対象となる期間

本報告の対象となる期間は，平成 23 年４月１日から平成 24 年３月 31 日までです。

（３）本報告の対象となる組織

本報告の対象となる組織は，公正取引委員会です。

（４）本報告の対象となる情報

本報告の対象となる情報は，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（以下，両基準を併せて「政府統一基準」といいます。）の対象となる情報であって，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です。

（５）本報告の責任部署

本報告の責任部署は，公正取引委員会事務総局官房総務課です。

（６）公正取引委員会の定員数

本報告の対象となる公正取引委員会の定員数は 804 人（平成 24 年３月末現在）です。

（７）情報システム関係予算額

公正取引委員会において運用している情報システムに関する予算総額は，143,038 千円（平成 23 年度）です。

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

ア　公正取引委員会では，政府統一基準に基づき，平成 18 年３月に「公正取引委員会情報セキュリティポリシー」（以下「セキュリティポリシー」といいます。）を策定し，実施してきました。

また，セキュリティポリシーに定められた遵守事項を運用するための手順として，「情報取扱手順書」，「情報の格付及び取扱制限に関する規定」等のセキュリティポリシー関連規程を策定しています。

イ　今年度は，政府統一基準が改定されたことを受けて，規定内容を改定後の政府統一基準に準拠させるべく，セキュリティポリシー及びその関連規程の内容を見直し，改定しました。

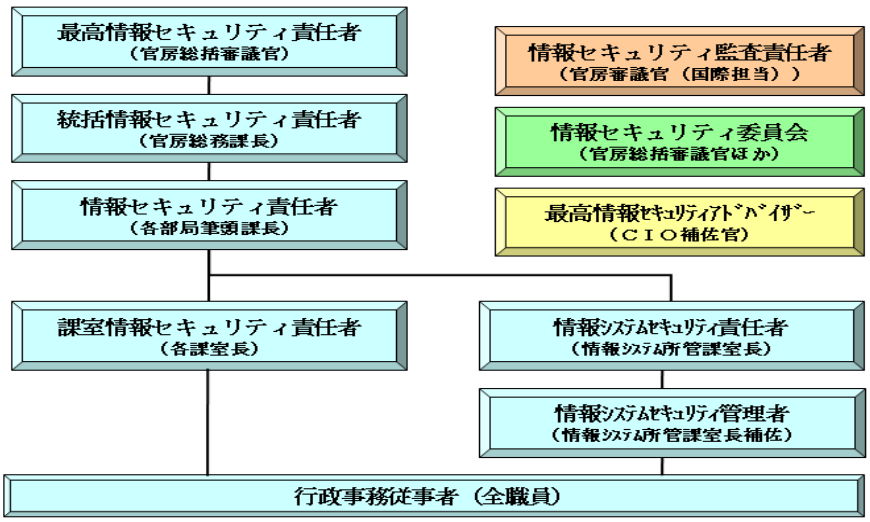
（２）情報セキュリティ対策の推進体制

ア　情報セキュリティ対策に係る組織体制

公正取引委員会では，図１に示すとおり，最高情報セキュリティ責任者の下，それぞれの職務に応じて情報セキュリティ対策に係る責任者を置いており，組織全体として情報セキュリティ対策に取り組んでいます。

また，情報システムの整備及び管理並びに情報セキュリティ対策に関し，十分な知識と経験を有する者を最高情報セキュリティアドバイザーの任に当たらせており，本報告書の作成を含め，公正取引委員会の情報セキュリティ対策に関する助言を得ています。

図１　情報セキュリティ体制



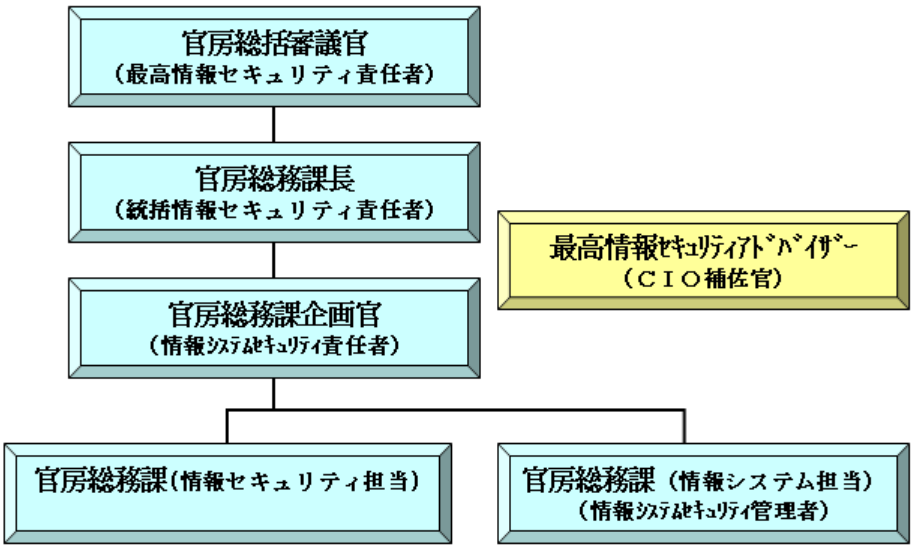
職 務	役 割
最高情報セキュリティ責任者	全組織における情報セキュリティ対策に関する事務の統括
情報セキュリティ監査責任者	情報セキュリティ監査に関する事務の統括
情報セキュリティ委員会	セキュリティポリシーを始めとする各種規程の策定等
最高情報ｾｷｭﾘﾃｨｱﾄﾞﾊﾞｲｻﾞｰ	情報セキュリティ対策への助言
統括情報セキュリティ責任者	情報セキュリティ責任者の統括，各種規程・手順等の整備
情報セキュリティ責任者	所管する単位における情報セキュリティ対策に関する事務の統括
課室情報セキュリティ責任者	課室における情報セキュリティ対策に関する管理事務の統括
情報ｼｽﾃﾑｾｷｭﾘﾃｨ責任者	情報システム毎の管理統括
情報ｼｽﾃﾑｾｷｭﾘﾃｨ管理者	情報システム毎の対策の実施
行政事務従事者	日常業務における情報セキュリティ対策の実施

イ　情報セキュリティ対策に係る推進部署の体制

公正取引委員会における情報システム及び情報セキュリティ対策に係る推進部署の体制は，図２のとおりです。

官房総務課（情報セキュリティ担当及び情報システム担当）では，情報セキュリティに係る規程の策定や教育，情報システムの運営・管理とそのセキュリティ対策等の役割を担っています。

図２　情報セキュリティ対策に係る推進部署の体制



（３）監査等

ア　概要

公正取引委員会では，情報セキュリティ対策の改善のため，セキュリティポリシーの規定に基づき，毎年度，情報セキュリティ監査を実施しており，本年度については平成 24 年１月から３月にかけて実施しました。監査を実施する際には，監査の客観性を確保するため，情報セキュリティ対策の推進を担当する職員及び被監査部局の職員が監査の実施担当者とならないこととしています。

また，情報システムのセキュリティレベルの維持・向上のため，毎年度，情報システムに関する脆弱性検査を実施していますが，平成 23 年度は公開用ウェブページ等を検査対象とし，専門的な技術を有する外部事業者に委託して検査を実施しました。

イ　情報セキュリティ関係規程に係る準拠性監査

（ア）監査の対象

平成 24 年２月時点で，セキュリティポリシーの規定内容と政府統一基準の規定内容との整合性及びセキュリティポリシー関連規程の内容とセキュリティポリシーの規定内容との整合性を監査しました。

（イ）結果

セキュリティポリシーの規定内容が，政府統一基準の規定内容と整合性がとれていることを確認しました。

また，セキュリティポリシー関連規程の内容が，セキュリティポリシーの規定内容と整合性がとれていることを確認しました。

ウ　自己点検結果に関する監査

（ア）監査対象

平成 23 年 12 月に実施した自己点検の結果が，各職員の実際の情報セキュリティ対策の実施状況と合致しているかを確認し，自己点検結果の適正性を監査しました。

（イ）結果

職員の情報セキュリティ対策の実施状況と自己点検結果が合致していることを確認しました。

エ　情報システムの脆弱性検査

（ア）実施時期

平成 23 年 11 月 1 日から同月 18 日にかけて，公開用ウェブページの一部（外部からの入力を伴うページなど）等を対象に攻撃者が実際に用いる攻撃手法を用いて脆弱性検査を実施しました。

（イ）結果

公開用ウェブページについては，そのサーバの管理・運営を専門事業者に委託しており，同事業者は手順書を作成して適切なセキュリティ対策を実施していますが，今回の脆弱性検査においては，入力フォームを持つ複数のウェブページを対象に攻撃者が実際に用いる攻撃手法を用いて意図的な攻撃を重ねた結果，攻撃者による不正な情報取得に繋がる可能性のあるクッキー（注１）に係る問題等が確認されましたので，これらの脆弱性を解消すべく，セキュア属性（注２）を付与するなどの対処を実施しました。

（注１）　「クッキー」とは，ウェブサイトの提供者（ウェブサーバ）が，ウェブブラウザを通じて，ウェブサイトの訪問者のコンピュータに一時的に訪問者の各種データ（最後にサイトを訪れた日時，そのサイトの訪問回数等）を書き込む仕組みであり，訪問者が再度同じウェブサイトにアクセスした場合は，ウェブブラウザを通じてウェブサーバにクッキーのデータが送信され，ユーザ識別等に利用されます。

（注２）　「セキュア属性」とは，暗号化通信以外の通信の場合には，クッキーのデータをウェブサーバに送信しないようにする設定を指します。

4　平成 23 年度の重点事項

（１）職員による情報セキュリティ対策の実施状況の改善

ア　重点事項

昨年度に実施した自己点検では，職員の情報セキュリティに係る対策項目（注）の平均実施率は 95.5%となり，おおむね適切に実施されていましたが，対策項目ごとに実施状況を見ると，情報の保存方法等の一部の項目について，実施状況が十分とは言えない項目も認められる結果となりました。この結果を受けて，職員による情報の取扱いに係る情報セキュリティ対策の実施状況を改善するための取組に重点的に取り組みました。

（注）政府統一基準等で定められた情報セキュリティに係る遵守事項を指します。

イ　取組内容

（ア）情報セキュリティ対策の周知

全職員に向けて，昨年度の自己点検の全体結果を周知するとともに，情報セキュリティ対策の実施が十分ではない項目について，改めて職員が実施すべき対策を周知しました。

（イ）研修資料の内容の見直し

全職員向けの情報セキュリティ対策に係る研修資料において，職員が実施すべき情報の取扱いに係る情報セキュリティ対策について重点的に解説するとともに，職員が実施すべき対策を端的にまとめた資料も加え，職員の理解向上を図りました。

（ウ）教育方法の見直し

今年度から，全職員向けの情報セキュリティ対策に係る e-ラーニング研修と自己点検を併せて行うこととしました。これにより，各職員が，自己点検によって十分に実施できていない対策を自ら見つけ出し，研修資料等によって，その実施すべき対策を繰り返し確認できるようにしました。

ウ　評価

平成 23 年度に実施した自己点検においては，全職員のうち，情報セキュリティの各対策を「実施」したと回答した職員の割合は 96.4 %となり，昨年度の 95.5%に比べて 0.9 ポイント上昇しました（自己点検結果の詳細は後述５．１参照。）。

しかし，まだ十分とは言えないことから，前記イ（ウ）の取組を継続した上で，引き続き，職員への教育などを通じて，実施状況の更なる改善に取り組みます。

（２）標的型メール攻撃への対策

ア　重点事項

政府機関等に対して，標的型メール攻撃（特定の組織及び個人等に向けてメールで不正プログラムを送り付ける攻撃）が増大していることを受け，緊急に取り組むべき事項として，全職員に対する注意喚起，対処方法の周知，訓練の実施等に取り組みました。

イ　取組内容

（ア）全職員への注意喚起

従来から，ＮＩＳＣから提供される「不審メール情報」を全職員に向けて情報発信し，注意を呼び掛けていますが，これに加えて，改めて全職員向けに「標的型メール攻撃」の攻撃手法等について説明し，注意を促すとともに，不審なメールを受け取った場合の対処方法等について，各種研修の機会等を通じて，繰り返し周知しました。

（イ）訓練の実施

当委員会は，ＮＩＳＣが政府機関を対象として平成 23 年 10 月から 12 月

に実施した標的型メール攻撃訓練に参加しました。

訓練は，全職員に対し，不審なメールを模擬した訓練用メールを２回送付し，当該メールに添付されたファイルを開いたり，リンク先にアクセスした場合には，教育用サイト（職員に不審なメールに添付されたファイル等を開いたことを気付かせ，不審なメールを見分けるポイントや対処方法等を解説した資料を掲載したサイト）に誘導するというものです。

全職員のうち，訓練用メールに添付されたファイルを開くか，リンク先にアクセスした職員の割合（開封率）は，訓練に参加した全機関の平均値よりもかなり低いものでした。また，１回目の開封率よりも，２回目の開封率の方が低くなっており，今回の訓練は，一定程度の効果があったものと評価できます。

ウ　評価

平成 23 年度に実施した標的型メール攻撃訓練においては，一定の効果を得ることができましたが，今後も，職員への不審メール情報の発信や教育，訓練等の充実を図り，継続的に標的型メール攻撃への対策を採っていきます。

５　情報セキュリティ対策の実施状況

５．１　自己点検結果

（１）平成 23 年度自己点検結果の状況

ア　対策実施状況の把握率

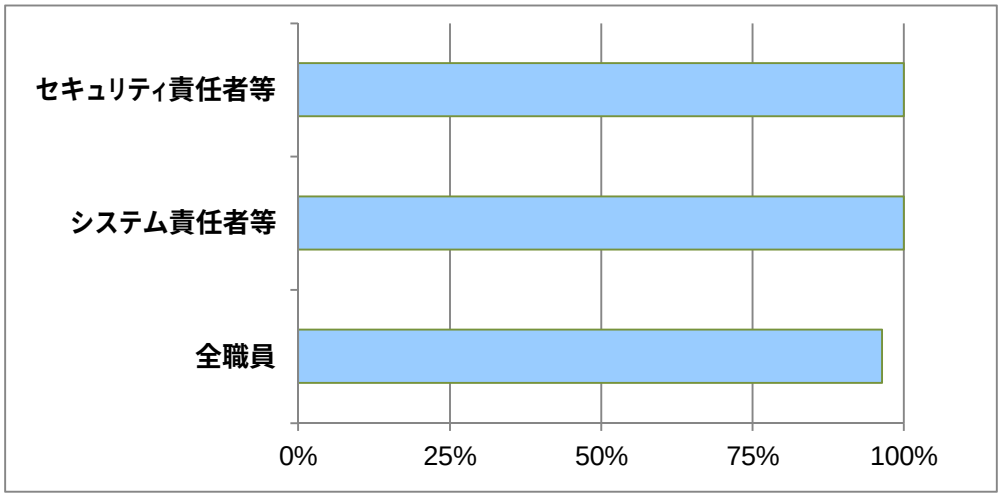
全職員のうち自己点検を実施した職員の割合（把握率）は，昨年に引き続き 100％を達成し，全職員のセキュリティ対策の実施状況を把握することができました。

なお，自己点検を実施する際には，今年度から，回答をワンクリック方式による選択制にし，集計を自動化させることで，各職員の記入作業及び集計作業の迅速化を図りました。

イ　セキュリティ対策の実施率

セキュリティ対策の実施率を，各職員のセキュリティ対策上の役割別に示すと下図のとおりであり，セキュリティ責任者等及びシステム責任者等では，全ての対策項目についてセキュリティ対策を実施しており，100％を達成しました。また，全職員（セキュリティ責任者等，システム責任者等を含む。）を調査対象とした場合でも，全ての対策項目で 90％以上となっており，全体として 96.4％と高い割合を示しました。

図３　役割別の実施率

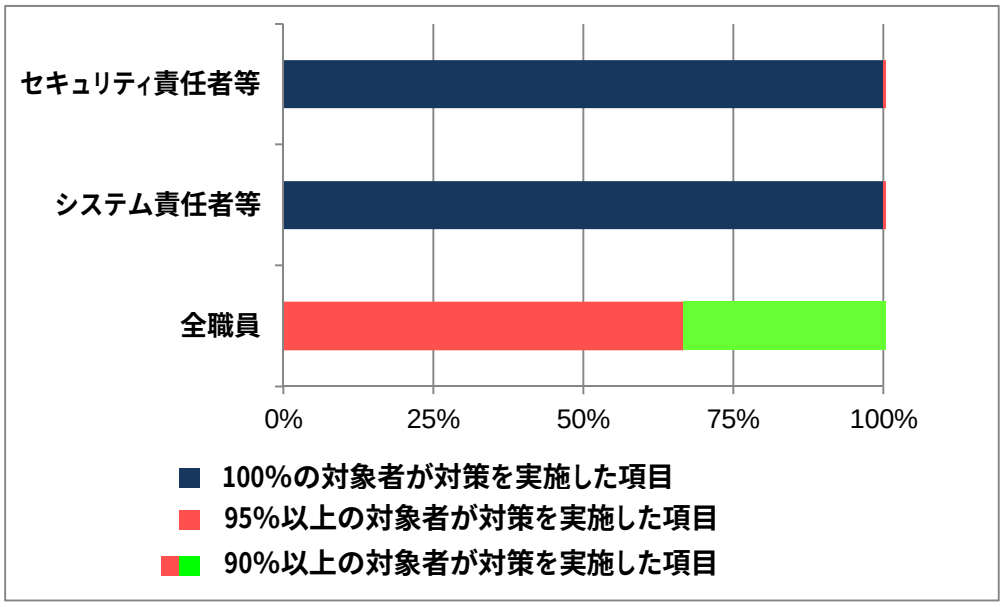


ウ　セキュリティ対策の到達率

実施率が一定の割合（100%，95%以上又は 90%以上）に到達した対策項目の割合（到達率）を，各職員のセキュリティ対策上の役割別に示すと下図のとおりの結果となりました。

セキュリティ責任者等及びシステム責任者等のみを調査対象とした場合，全項目について到達率が 100%でしたが，全職員（セキュリティ責任者等及びシステム責任者等を含む。）を調査対象とした場合では，全項目について，到達率 90%以上となりましたが，到達率 95%以上の項目は全体の 66.7%程度にとどまり，到達率 100%の項目はありませんでした。

図４　役割別の到達率



（２）総評

セキュリティ責任者等及びシステム責任者等を対象とした点検では，昨年度に引き続き，情報セキュリティ対策の実施率・到達率ともに 100％を達成することができましたので，今後も，この水準を保つよう努力していきます。しかし，全職員を対象とした点検では，情報セキュリティ対策の実施率・到達率ともに，昨年度よりも着実に改善しているものの，いまだ対策の実施状況が十分とは言えない項目もありました。全職員に対する情報セキュリティ対策の更なる周知及び教育が必要と考えられます。

（３）自己点検の結果に基づく改善指示等の状況

全職員に向けて，自己点検の結果とともに，今回の点検で情報セキュリティ対策の実施が十分ではないことが判明した一部の項目について，全職員が情報セキュリティ対策の重要性を認識し，当該対策を実施することとなるよう，改めてセキュリティ対策として実施すべき内容を具体的に文書にして，全職員に向けて周知するなどの措置を採りました。

今後も，職員によるセキュリティ対策の実施状況の改善に向けて，更なる周知及び教育の充実に努めていきます。

５．２　情報システムごとの状況

（１）課題と対策

情報システムの重点検査は，政府統一基準に準拠した対策が実施されているかを確認するためにＮＩＳＣが実施する調査であり，公正取引委員会はＮＩＳＣが配布する調査票に基づき，平成 23 年 10 月１日時点のウェブサーバ及び電子メールサーバの状況について内部調査を実施しました。

内部調査の結果，公正取引委員会が管理するすべてのウェブサーバ及び電子メールサーバにおいて情報セキュリティ対策（政府統一基準における遵守事項）の実施率が 100％でしたので，これをＮＩＳＣに報告しています。

（２）情報システムの対策状況

公正取引委員会の公開用ウェブサーバ及び電子メールサーバの運用・管理は，専門の事業者に委託しており，同事業者は手順書を作成して，当該手順書に基づき運営・管理しています。内部調査の結果，両サーバともに不正プログラム対策，不正アクセス対策，情報保護対策及びサーバ管理の対策の実施率が 100％でした。

（３）総評

公正取引委員会では情報セキュリティレベルの維持・向上に努めており，重点検査については，平成 20 年度以降，公開用ウェブサーバ及び電子メールサーバの全てについて，実施率 100%となっており，平成 23 年度においても内部調査の段階では実施率 100%となっています。

今後も適切な情報セキュリティ対策を実施し，情報セキュリティレベルの維持・向上に努めていきます。

５．３　教育・啓発

（１）教育

情報セキュリティ対策を確実に実行していくためには，公正取引委員会の全職員が，公正取引委員会の情報セキュリティ対策を十分に理解する必要があります。このため，全職員を対象として，情報セキュリティ対策に係る研修を継続的に実施していくことが大切です。

公正取引委員会では，毎年度，情報セキュリティ対策に係る研修の計画を策定しており，当該研修計画に基づいて，e-ラーニング研修，集合研修及びテレビ会議システムを用いた研修を実施しています。

平成 23 年度に実施した情報セキュリティ対策に係る研修の主な内容は，以下のとおりです。

ア　新規及び中途採用者向け研修

新規及び中途採用者を対象とした集合研修において，情報セキュリティ対策に係る研修を実施しました。

イ　全職員向け e-ラーニング研修

全職員を対象に e-ラーニングによる情報セキュリティ対策に係る研修を行いました。研修終了後には，理解度確認テストを実施し，職員の理解度を把握するとともに，あらかじめテスト問題の解説を作成し，職員が回答後に解説を見ることができるようにして，職員の理解度向上を図りました。

ウ　管理職員向け研修

全管理職員を対象として，職員を管理・指導する立場にある管理職員が，情報セキュリティ対策の中で担う役割をテーマとして，最高情報セキュリティアドバイザーを講師とする集合研修を実施しました。

エ　ＩＴ基礎研修

職員に情報セキュリティを含む基本的なＩＴ知識（独立行政法人情報処理推

進機構が実施する国家試験である「ＩＴパスポート試験」相当のもの）を習得させることを目的として，最高情報セキュリティアドバイザーを講師とする集合研修及びテレビ会議システムを用いた研修を実施しました。

（２）実施手順等の参照の容易化

全職員が利用するイントラネット上に，情報セキュリティ関係規程やこれまでの情報セキュリティ関係の研修資料等を掲載し，職員がいつでもこれらを参照して利用することができるようにしています。また，情報セキュリティ対策に係る各種の最新の情報についても同サイトに掲載し，随時，職員に情報発信しています。

（３）ひやり事例を含む障害等の事例の共有

いわゆる「ひやり事例」を含め，公正取引委員会の外部で発生した事故や障害等の事例を収集し，全職員向け e-ラーニング研修及び管理職員向け集合研修の資料に使用するなどして，職員に対する注意喚起を行っています。

５．４　調達・外部委託

情報処理業務を外部委託によって行う場合には，情報セキュリティを確保する観点から，業務を委託する者が契約等により，適切に委託先による業務の遂行を管理する必要があります。

公正取引委員会では，情報処理業務を外部委託によって行う際に課室情報セキュリティ責任者等が行う手続や，情報セキュリティの観点から調達仕様に含めるべき事項を示した手順書を作成しています。また，情報セキュリティ対策や個人情報保護の観点から，委託先に提出を求める情報の保護に関する誓約書のひな形も作成し活用しています。

これらは，全職員が利用するイントラネット上に掲載し，職員がいつでも参照できるようにしており，職員がこれらに基づいて，調達・外部委託業務を実施することによって必要な情報セキュリティ水準を確保できるようにしています。

５．５　その他取り組んだ事項

公正取引委員会の内部規程である文書取扱規程及びセキュリティポリシーの両規程において，秘密文書の管理方法について定めていることから，これを整理・統合することについて検討しています。

６　情報セキュリティに関する障害・事故等報告

昨年６月に，公正取引委員会の職員宛てに，当該職員と業務上やり取りのあった団

体職員を装ったメールが送付され，当該メールに添付されていた，不正プログラムが組み込まれたファイルを開封するという事案がありました。公正取引委員会では，速やかに当該ファイルを開いたパソコンをＬＡＮから隔離するなどの対策を実施するとともに，職員への周知及びＮＩＳＣへの情報提供を行いました。ＮＩＳＣによれば，当該ファイルには，特定の３つのサイトに誘導するプログラムが組み込まれており，発見時点では大手ウイルス対策ベンダーのウイルス対策ソフトでは検出できないものであったとのことです。公正取引委員会では，その後もログ解析を行い，不正プログラムの活動を注視していましたが，特定の３つのサイトに誘導された通信は発見されず，本件による情報流出等の被害はなく，また，他の端末へのウイルス感染もありませんでした。

このような標的型メール攻撃への対策として，前述４（２）で示した取組を重点的に行ってきましたが，今後も職員への教育，訓練等を通じて，継続的に対策を採っていきます。

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，セキュリティポリシーにおいて毎年度実施することとしている情報セキュリティ対策に係る教育，自己点検及び監査を実施するとともに，以下の事項に取り組むこととします。

ア　平成 23 年度の自己点検の結果，十分に情報セキュリティ対策が実施されていなかったことが判明した項目について，職員にその実施を促すため，研修資料の見直しや職員が実施すべき対策の周知を積極的に行います。

イ　標的型メール攻撃への対策として，職員への不審メール情報の発信，教育，標的型メール攻撃訓練等の対策を積極的に行います。

ウ　引き続き，定期的に情報システムに係る脆弱性検査を実施し，情報セキュリティレベルの維持・向上に努めます。

おわりに

公正取引委員会では，政府統一基準に準拠して必要な情報セキュリティ対策を講じています。情報セキュリティ対策で重要な役割を果たすのは人であるとの観点から，毎年，新規採用者への情報セキュリティ教育，全職員向け及び管理職向けの情報セキュリティ研修等を行っています。また，その研修等での理解向上とともに，その実施状況についての自己点検とフィードバックを行い，ＰＤＣＡサイクルを回しています。

平成 23 年度は，平成 22 年度に比べて自己点検結果と全職員向け情報セキュリティ研修後の理解度確認テスト結果が共に改善されています。公開用ウェブサーバ及び電子メールサーバについては，ＮＩＳＣの指定する検査項目の全てにおいて，最高の評価（実施率 100％）を得ています。また，標的型メール攻撃対策では，全職員に対して繰り返しの周知を行い，標的型メール訓練において，全機関の平均値よりもかなり低い開封率であったことより，全般として情報セキュリティ意識が向上していると理解できます。

他方，昨年６月に外部から当方の職員宛てのメールで，不正プログラムが組み込まれた添付ファイルが送付され，当該添付ファイルを職員が開封する事案がありましたが，事後の適切な対応により，情報流出がないことが確認できました。また，公開用ウェブページの脆弱性検査において，発見された脆弱性を解消すべく対処したことにより，実際の被害は出ておりません。このように事故対応や問題発生防止対応を適切に行ったことについては，今後の参考として活用すべき点だと考えます。

今後は，更にセキュリティレベルを高めるため，新たな脅威（標的型メール攻撃等）を前にして，引き続き情報セキュリティ意識を維持・向上させるとともに，今後改定が予定されている政府統一基準に沿って対策を強化し，着実に情報セキュリティ対策を実施していくことが重要であると考えます。また，公正取引委員会は，留置された情報システムや電子データの調査を行う機会が増加すると考えられますので，留置された情報システムや電子データからのコンピュータウイルス感染防止のための対策にも引き続き努めていく必要があると考えます。

公正取引委員会最高情報セキュリティアドバイザー
（公正取引委員会ＣＩＯ補佐官）
三枝　文仁