資料3

NISC National Information Security Center

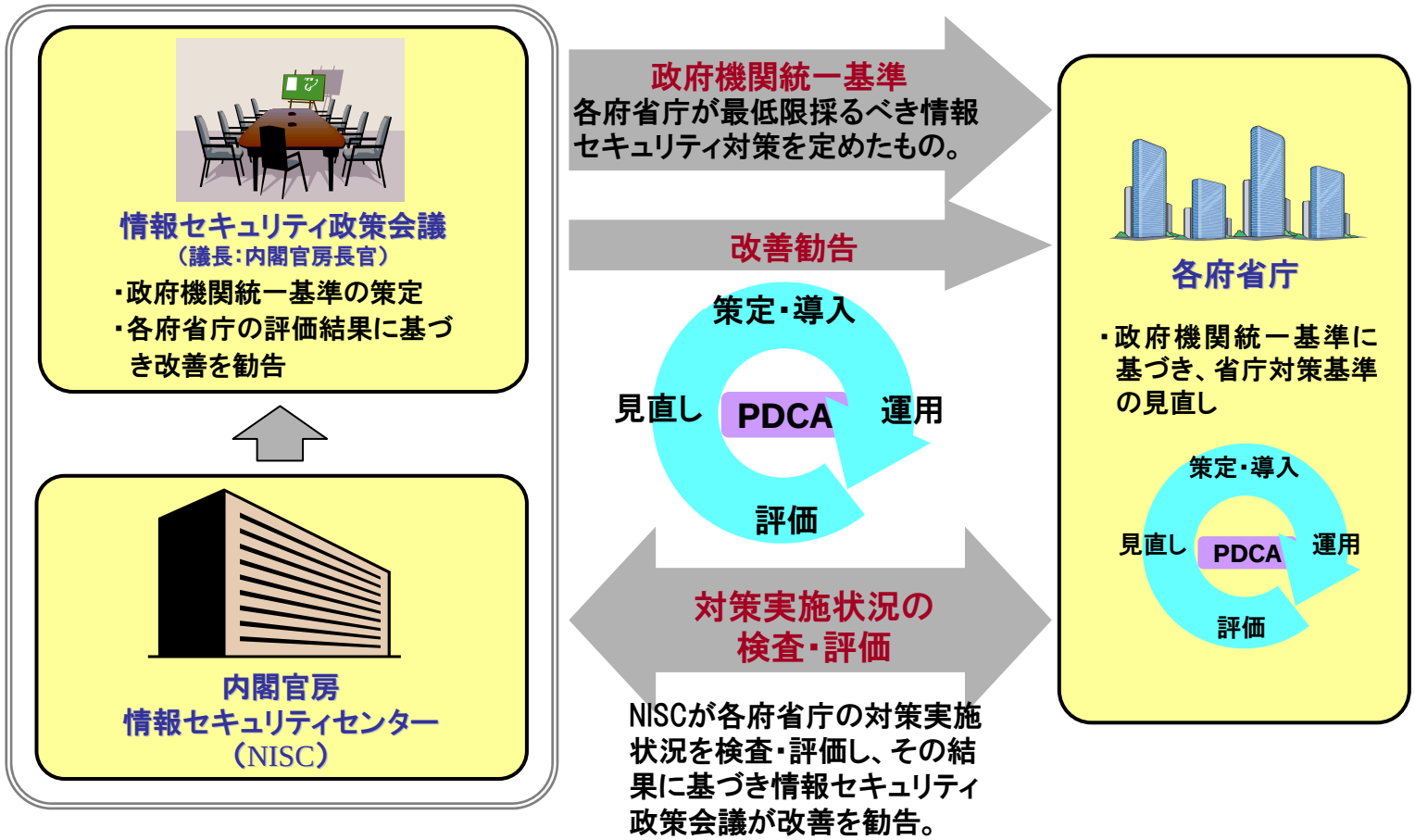
政府機関における情報セキュリティ対策の現状について

平成20年9月4日

内閣官房情報セキュリティセンター（NISC）

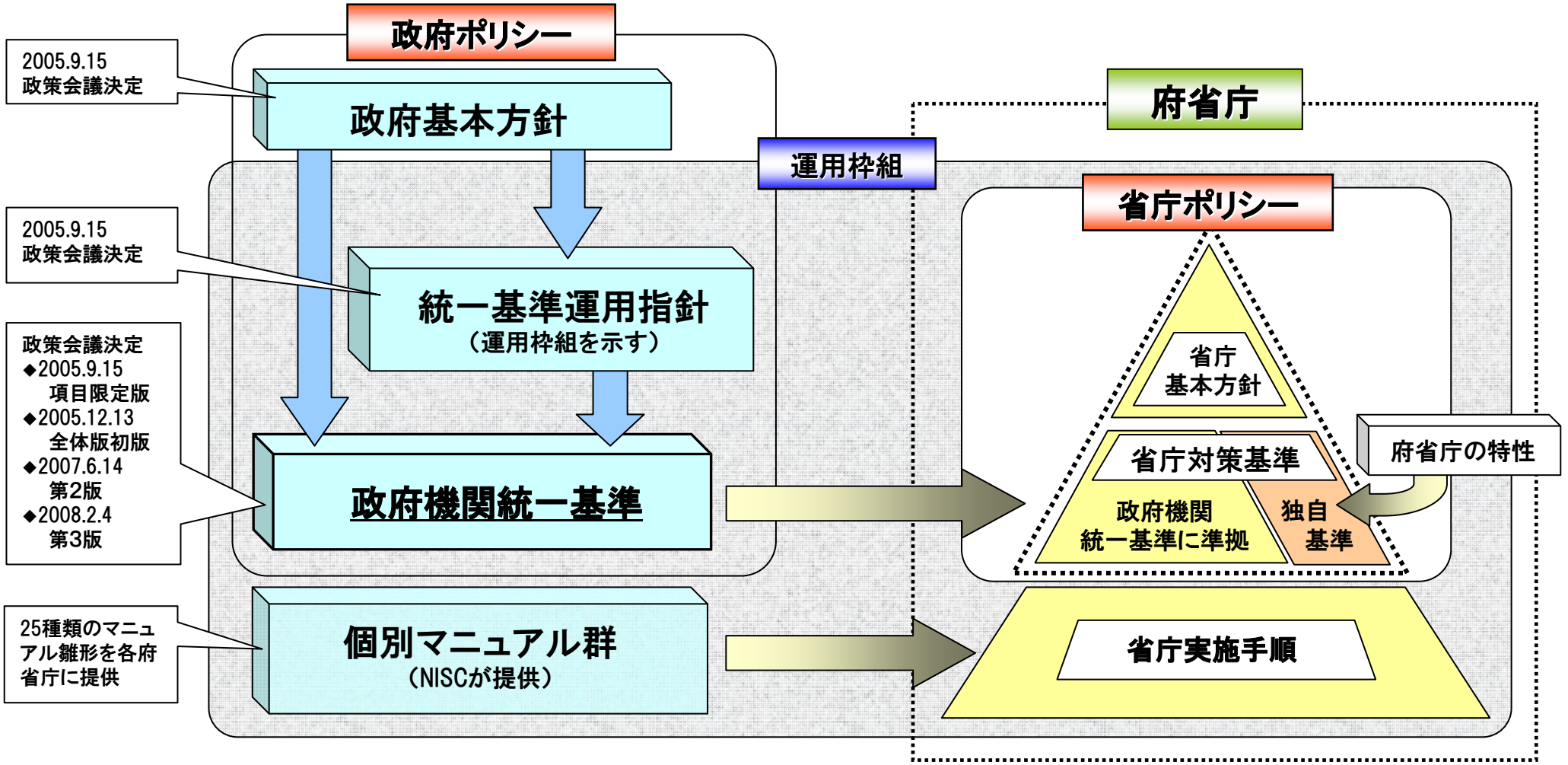
政府機関の情報セキュリティ対策の枠組み

- 政府機関全体としての情報セキュリティ水準の向上を図るため、各省庁が守るべき最低限の対策基準として、「政府機関の情報セキュリティ対策のための統一基準」（政府機関統一基準）を策定。
- 各政府機関は統一基準を踏まえて対策を実施し、内閣官房情報セキュリティセンターが対策実施状況を検査・評価。その結果に基づき、情報セキュリティ政策会議が改善を勧告。



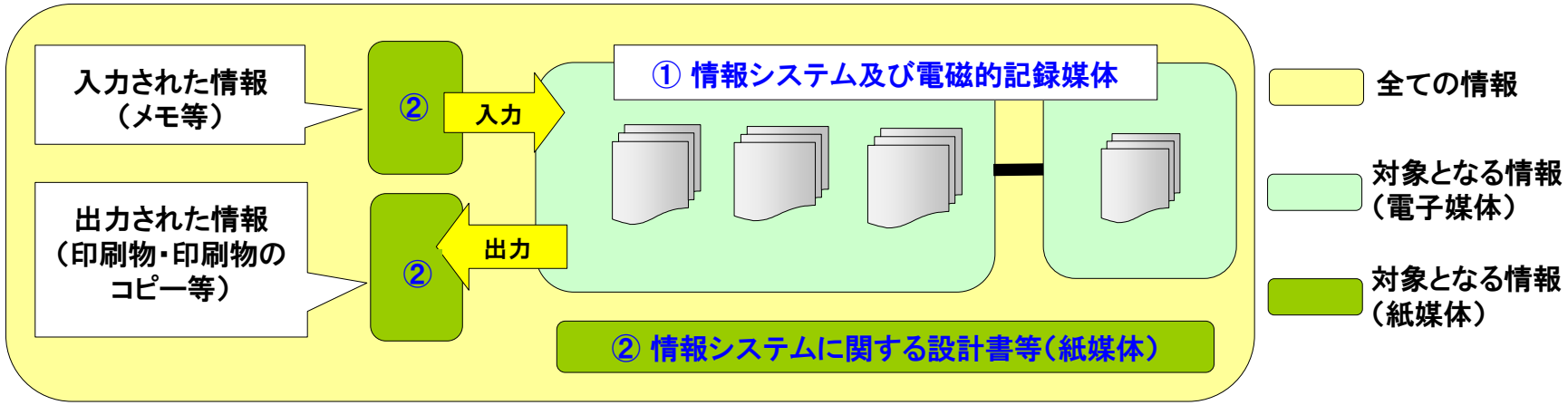
「政府機関統一基準」と各府省庁の情報セキュリティ対策基準

◆ 各政府機関は、政府機関統一基準を踏まえて自らの情報セキュリティ対策基準を整備。



政府機関統一基準の適用対象範囲

- 情報セキュリティポリシーにおいて対象となる情報は、
  - ① 情報システムの内部及び電磁的記録媒体に記録された情報
  - ② 情報システムに関係がある書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面及び情報システムに関する設計書等）。
- 上記以外の書類だけで保管されている資料等は対象とならない。



〔対象とならない情報の例〕

- 紙のみで保存されている情報
- 情報システムに入力する前の情報が書かれた紙媒体（メモ等）〔入力した時点で対象となる〕
- 情報システムから印刷物を出力後、情報システムから当該情報を削除した印刷物〔紙面全部を対象とする別途の文書管理規程により適切に管理されることを前提として、当該情報を削除した時点で本ポリシーの対象でなくなる。〕

現在、行政文書の大半はPC上で作成・処理されていることから、
事実上、殆どの行政文書が情報セキュリティポリシーの対象

「政府機関統一基準」の具体的な内容

第1部： 総則

第2部： 組織と体制の整備

- ○ 組織・体制の整備（各責任者等の権限と責務の明確化等）
- ○ 情報セキュリティ対策の教育
- ○ 情報セキュリティ対策の自己点検
- ○ 見直し
- ○ 違反と例外措置
- ○ 障害等の対応
- ○ 情報セキュリティ対策の監査

第3部： 情報についての対策

- ○ 情報の格付け
- ○ 情報の取扱い（利用・保存・移送・提供・消去）

第4部： 情報セキュリティ要件の明確化に基づく対策

- ○ 情報セキュリティ機能
  - 主体認証、アクセス制御、権限管理、証跡管理、情報保証、暗号・電子署名
- ○ 脅威対策
  - セキュリティホール対策、不正プログラム対策、サービス不能攻撃対策
- ○ 情報システムのセキュリティ要件
  - 情報システムの設計・構築・運用等

第5部： 情報システムの構成要素についての対策

- ○ 安全区域
- ○ アプリケーション（共通、電子メール、ウェブ）
- ○ 電子計算機（共通、端末、サーバ）
- ○ 通信回線（共通、庁内、庁外）

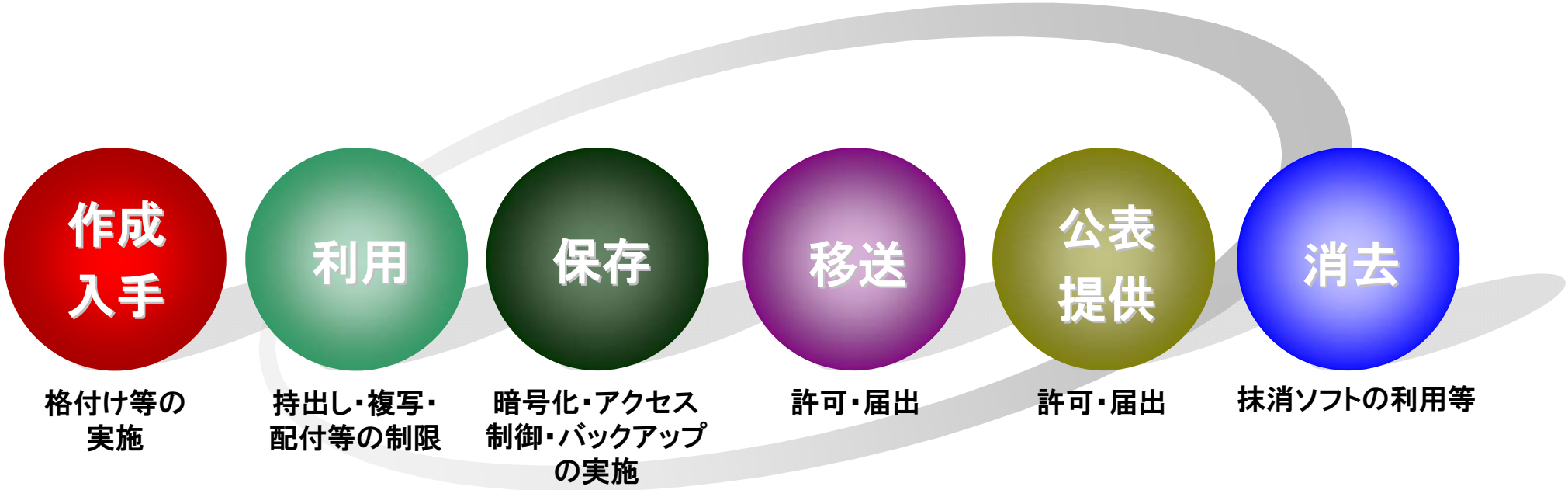
第6部： 個別事項についての対策

- ○ 機器等の購入
- ○ ソフトウェア開発
- ○ 府省庁支給以外の情報システム（私物PC等）による情報処理の制限
- ○ 外部委託
- ○ 府省庁外での情報処理（情報の持ち帰り等）の制限
- ○ その他

対策レベル： 「***基本遵守事項***」（必須の対策事項）と「***強化遵守事項***」（重要なシステムにおいて必要性を判断して取り入れる対策事項）

「情報についての対策」(第3部)の具体的な内容

- すべての情報は、作成・入手された後に、利用、保存、移送、公表・提供などの取扱いを受けた後に、最後に消去される。これを情報のライフサイクルと呼ぶ。
- 情報に対するセキュリティ対策は、このライフサイクルのそれぞれの段階において発生する脅威に対して行うことになる。



情報の格付けと取扱制限とは

- 情報の作成者又は入手者が、当該情報の重要性や講ずべき情報セキュリティ対策を他の者に認知させ、明確化するための手段が「格付け」と「取扱制限」。
- 「政府機関の情報セキュリティ対策のための統一基準」に準拠する、全ての府省庁の情報セキュリティポリシーにおいて、作成・入手した情報には「格付け」及び「取扱制限」を付記することを規定。

格 付 け

- 情報の重要性や価値等を主体的にランク付けすること。
- 情報を作成又は入手し管理を開始する前に、機密性、完全性、可用性の観点から（書面については機密性のみ）定義に基づいて決定。

すべての情報に必須

取扱制限

- 情報を取扱う際の制限事項。
- 機密性、完全性、可用性の観点から「複製禁止」、「持出禁止」、「再配布禁止」、「暗号化」、「読後廃棄」などを決定。

情報に応じて任意

【機密性】情報へのアクセスを許可された者だけがこれにアクセスできる状態を確保すること。
【完全性】情報が破壊、改ざん又は消去されていない状態を確保すること。
【可用性】情報へのアクセスを許可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

政府機関統一基準における格付けの分類基準

◆ 政府機関統一基準で示す「機密性」、「完全性」、「可用性」の格付けの分類基準は以下のとおり。

格付け		分類基準	（該当する情報の例）
機密性	3	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報	特定の職員だけが知り得る状態を確保する必要のある情報で秘密文書に相当するもの
	2	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報	職員だけが知り得る状態を確保する必要がある情報（職員のうち特定の職員だけが知り得る状態を確保する必要がある情報を含む）
	1	機密性2情報又は機密性3情報以外の情報	公表・公開又はそれを前提として作成した情報及び職員以外が知り得ても問題のない情報（公表・公開しても問題のない情報）
完全性	2	行政事務で取り扱う情報（書面を除く）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報
	1	完全性2情報以外の情報（書面を除く）	事故があった場合でも業務の遂行に支障がない情報
可用性	2	行政事務で取り扱う情報（書面を除く）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報
	1	可用性2情報以外の情報（書面を除く）	滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報

政府機関の対策実施状況について(2007年度)

- 政府機関全体としての情報セキュリティ対策を推進する観点から、各府省庁の対策の実施状況をNISCにおいて把握。
- 2007年度に政府機関全体で約30万人の職員の対策実施状況についての報告を分析した結果、政府全体として「情報セキュリティ教育の実施」、「格付け・取扱い制限に係る措置」、「システム台帳の整備」等の課題が残っていることが判明。これらのほとんどについては、2006年度からの課題でもあり、改善に向けた取組みを加速することが必要。

◇格付け・取扱い制限に係る措置の実施状況

格付け・取扱い制限に係る措置の平均実施率

89. 7%

遵守事項全体の平均実施率

93. 1%

遵守事項	実施率
(1)情報の作成と入手	87. 3%
(2)情報の利用	96. 6%
(3)情報の保存	87. 7%
(4)情報の移送	86. 3%
(5)情報の提供	90. 6%
(6)情報の消去	96. 5%

遵守事項別実施率

① 情報の作成と入手時において、情報の格付けの実施や格付けの明示等の実施が不十分

② 情報の移送、情報の提供時において、管理者・責任者に対して行うべき許可申請、届出が不十分

各府省庁の文書管理規則、個人情報保護法と政府機関統一基準等について

情報セキュリティに関連する制度	各府省庁の文書管理規則及び情報公開基準等	政府機関統一基準	個人情報保護法
根　拠	情報公開法等	情報セキュリティ政策会議決定	個人情報保護法
目　的	・行政文書の適正な管理の確保 ・事務の適正かつ能率的な遂行 ・情報公開法の適正かつ円滑な運用等	・政府機関全体の情報セキュリティ対策の強化・拡充	・行政機関における個人情報の取扱いに関する基本的事項を定める
主な対象	・行政文書（行政機関の職員が職務上作成し、又は取得した文書、図画及び電磁的記録であって、当該行政機関の職員が組織的に用いるものとして、当該行政機関が保有しているもの）	・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 ・情報システムに関係がある書面に記載された情報（情報システムから出力した情報等）	・保有個人情報（行政機関の職員が職務上作成し、又は取得した個人情報であって、当該行政機関の職員が組織的に利用するものとして、当該行政機関が保有しているもの（情報公開法第2条第2項に規定する行政文書に記録されているものに限る）
情報等の取り扱いに係るルールの内容	・各府省庁の文書管理規則の定めるべき行政文書の分類、作成、保存、廃棄等の手続きの要件を定める ・情報公開の開示基準 ↓ 各府省庁の情報公開法に基づく処分に係る審査基準等で具体化	・情報の作成・入手、利用、保存、移送、公表・提供、消去にかかわるルール ↓ 各府省庁の情報セキュリティポリシーで具体化	・個人情報保護における、従事者の義務、利用目的の特定、利用及び提供の制限、提供を受ける者に対する措置要求等 ↓ 各府省庁の個人情報保護管理規程で具体化

各府省庁内に同趣旨あるいは関連したルールが併存