NISC National Information Security Center

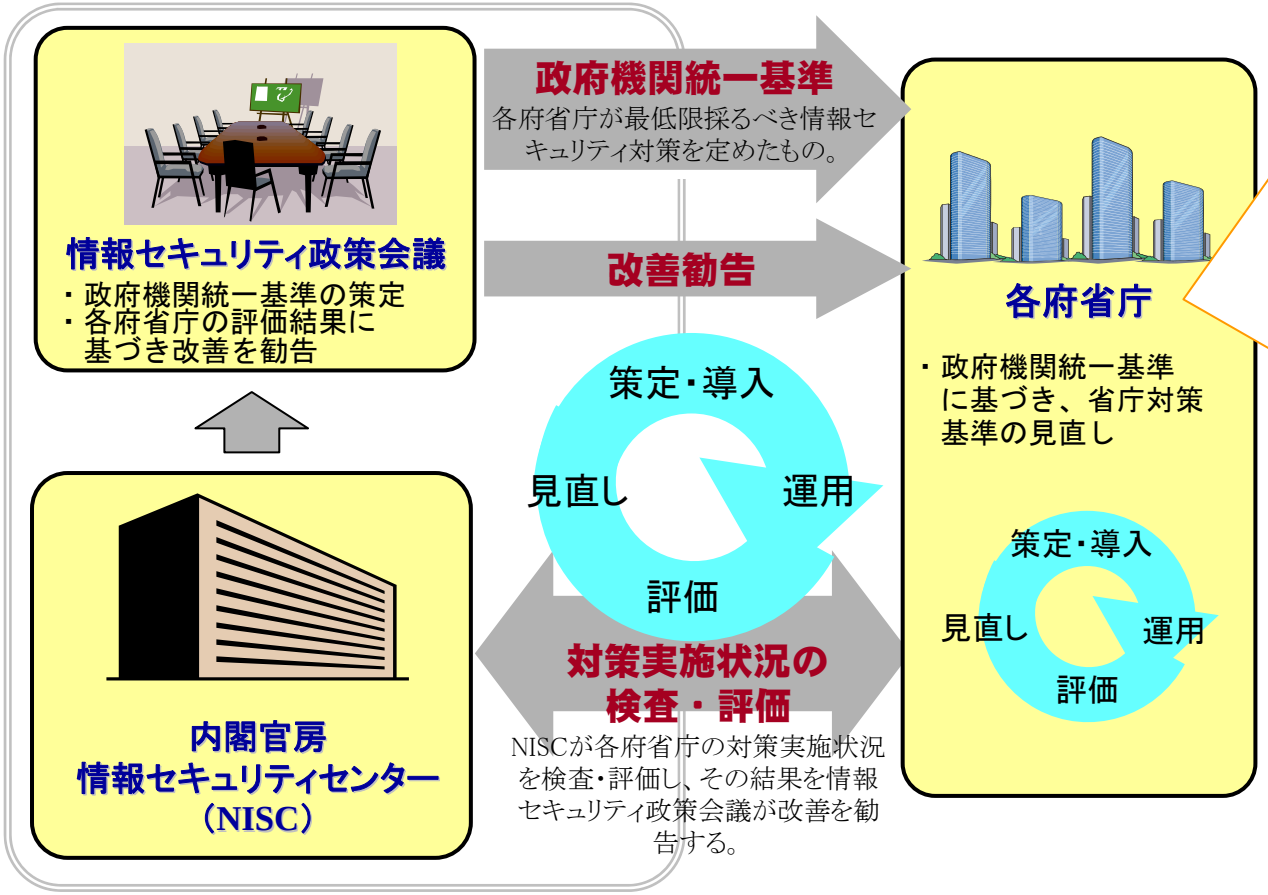
政府機関総合対策の現状について

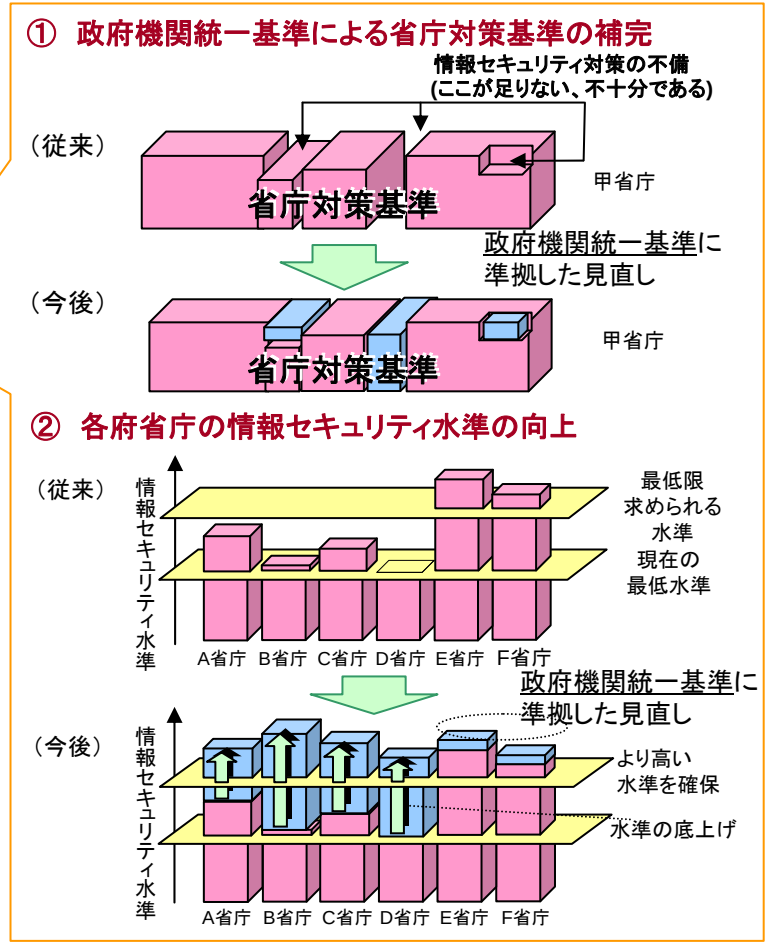
平成20年7月25日
内閣官房情報セキュリティセンター（NISC）

資料4－1

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」**を策定。
○ 各政府機関は本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」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

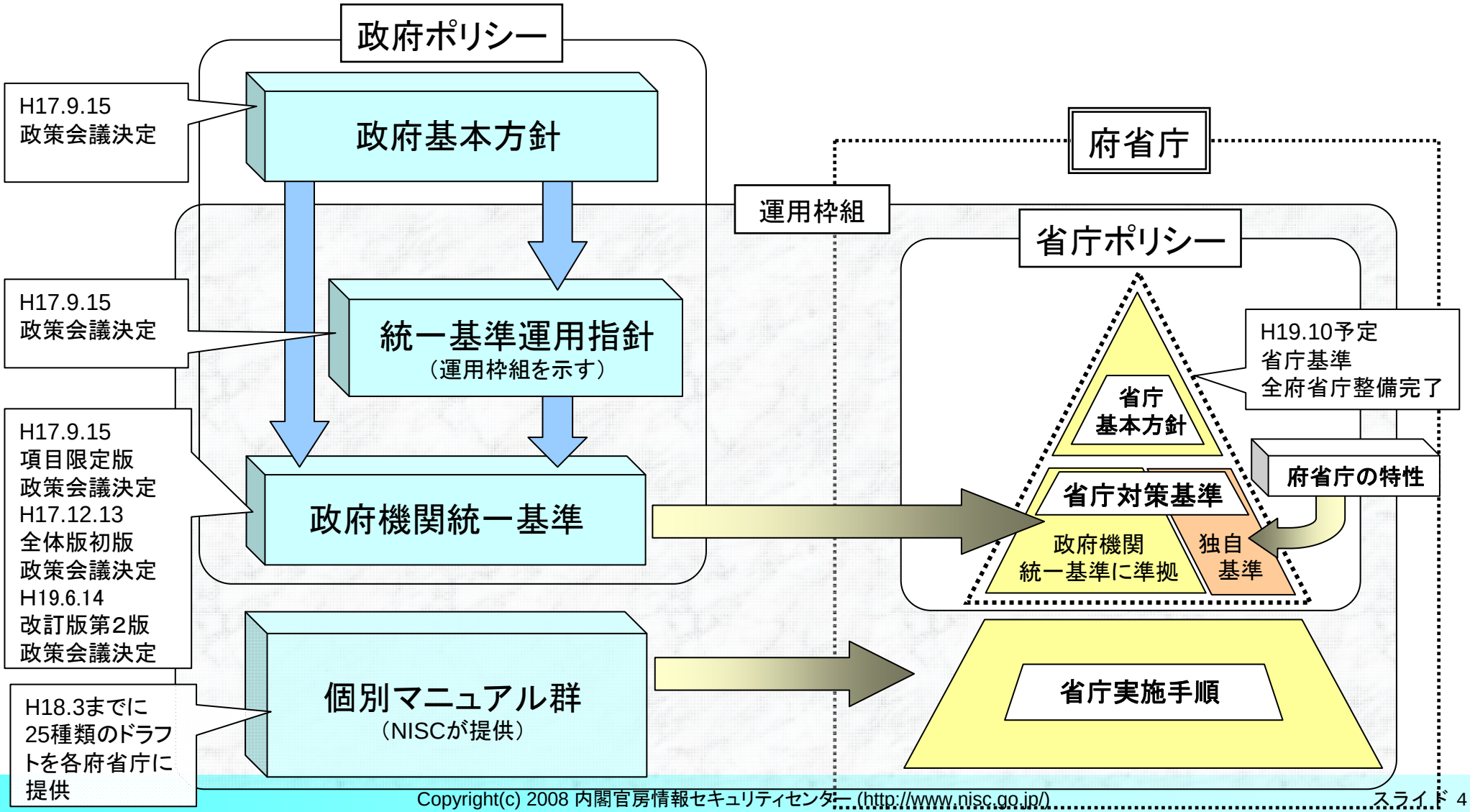
第5部　情報システムの構成要素についての対策
- ○ 安全区域
- ○ アプリケーション（共通、電子メール、ウェブ）
- ○ 電子計算機（共通、端末、サーバ）
- ○ 通信回線（共通、庁内、庁外）

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）

政府機関の情報セキュリティ対策の枠組み

○政府全体としての情報セキュリティ水準の向上を図るため、「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。(平成17年9月策定)



政府機関全体としての総合的な評価の運用

➢ 毎年度の対策実施状況報告により、政府機関における情報セキュリティ対策の実施状況を把握・分析。

➢ さらに、相互に補完する「情報セキュリティマネジメントの評価」と「情報セキュリティ対策実施状況の評価」の双方の評価指標を設定し、併用。

情報セキュリティ対策実施状況の総合評価
＜実施率（スナップショット）＞

政府機関統一基準の基本遵守事項の中でも重要な項目に着目し、重点検査を実施して、対策実施率を定量的に評価

A	X＝100%	● 経年度比較を行い、水準の維持や改善の進捗を把握する。
B	80%≦X＜100%	
C	60%≦X＜80%	● 経年度比較を行い、改善の進捗を把握する。 ● 改善を勧告する場合がある。
D	X＜ 60%	

情報セキュリティマネジメントの総合評価
＜マネジメント評価＞

政府機関における情報セキュリティマネジメントがPDCAサイクルの各段階で確実かつ効果的に行われているかを評価

★★★ 政府内外を問わず模範となる先進的な取り組みを実践している。	● 参考にすべき優れたプラクティスをベストプラクティス等として公表し、各府省庁での取り組みを促進する。
★★ 政府機関の模範となる工夫が見られる。	
★ おおむね適切に行われている。	● 統一基準で求めている水準の対策は行われている

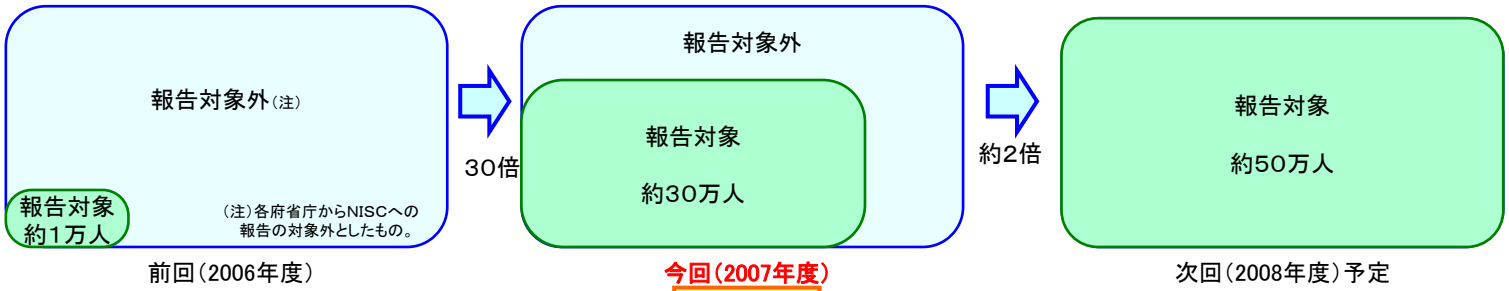
政府機関の対策実施状況報告（2007年度）の概要

1　対策実施状況報告の実施目的

政府機関の情報セキュリティ対策は、「2009年度初めには、すべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指す」（第1次情報セキュリティ基本計画）ことが目標とされている。
この**目標を達成するため、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**。

2　2007年度の報告の範囲

2007年度は、目標達成のための中間地点と位置づけ、**2008年度に全ての対象を報告することを明確化**するとともに、2007年度は**できるかぎり多くの対象に係る対策実施状況の報告を求めた（前年度比約30倍）。**
（2007年度の報告対象については組織の規模や繁忙期等に配慮し、各府省庁から事前に提示された対象範囲とした。）



3　報告の概要及び2008年度に向けた課題

報告の概要

- 政府機関全体で約30万人分の対策実施状況について報告があった。これを分析した結果、各府省庁が報告対象とした者のうち状況が把握できた者の割合を示す把握率は全府省庁平均で約93%、実施率は全府省庁平均で約93%、到達率については、100%の職員が実施した遵守事項の割合では約64%、90%の職員が実施した遵守事項の割合では約82%であった。
- 一定の成果が見られるが、なお不十分な点があり、第一次基本計画の最終年度に向けて、取り組むべき課題が依然として残っている

2008年度に向けた課題

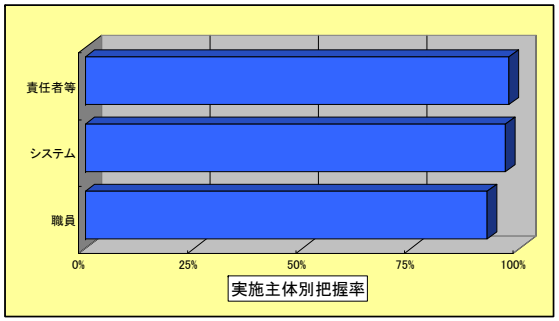
- 第1次基本計画の目標を達成するためには、政府全体として「情報セキュリティ対策の教育」、「格付け・取扱い制限に係る措置」、「情報システムの台帳整備」等の課題が残っている。これらのほとんどについては、前回（2006年度）からの課題でもあり、改善に向けた取組みを加速する必要がある。
- 一方、前回（2006年度）に課題とされた「安全区域内における職員識別の徹底」等については、各府省庁とも改善がみられている。
- 今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、NISCにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

政府機関の対策実施状況報告(2007年度)の評価結果【実施主体ベース】

1 把握率

全府省庁の平均把握率

93. 4%



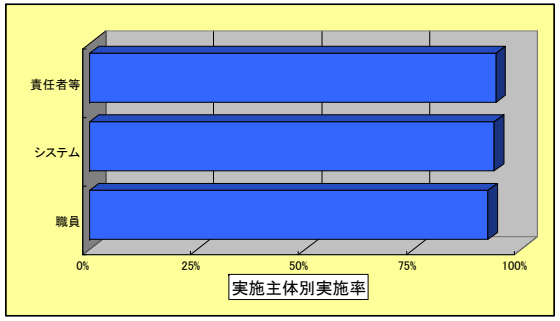
① 昨年度比で30倍と大幅に報告対象が増えた中、平均把握率は約93%となっており、多くの省庁では対策実施状況が把握できている結果であった。

② 来年度は全対象であること、今年度は対象を各省庁が事前に設定した範囲内であったこと、特に職員の把握率が低いことから、来年度に向け、把握率の改善手段をあらかじめ検討する必要がある。

2 実施率

全府省庁の平均実施率

93. 4%



③ 平均実施率は約93%となっており、責任者等が高く、システム担当、職員の順に低い結果であった。

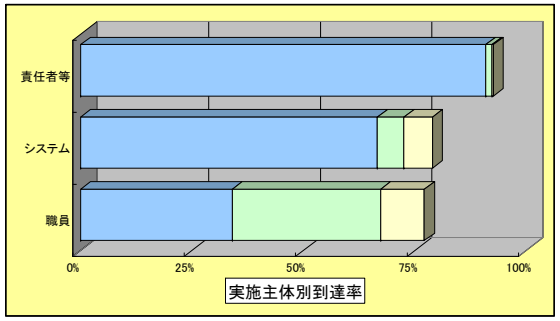
④ 情報セキュリティ対策について組織的な責務を果たすべき責任者等の実施率が100%に満たないことは問題であり、職員についても実施率が低い状態の改善が必要である。

3 到達率

全府省庁の平均到達率

100%実施した割合　:64. 1%
95%以上実施した割合:75. 8%
90%以上実施した割合:81. 7%

全対象者が対策を実施した遵守事項の割合
95%以上の対象者が対策を実施した遵守事項の割合
90%以上の対象者が対策を実施した遵守事項の割合



⑤ 到達率でみると、責任者等に比べシステム担当や職員が低くなる傾向が顕著に現れた。

⑥ これは職員については、日々の業務において日常的に実施しなければならない遵守事項が多いことから、責任者等やシステム担当と比して100%達成に困難な面があるためだが、万一の事故防止のためには日々の取り組みが重要であり、到達率向上の努力が必要である。
一方、責任者等やシステム担当については、日常的なものは少なく、早急に100%を達成する必要がある。

把握率:各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合
実施率:把握した者のうち、責務が生じた者に占める対策を実施した者の割合
到達率:把握した者のうち、責務が生じた一定の割合(100%、95%、90%)以上の者が対策を実施した遵守事項の割合

責任者等:最高情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者、情報セキュリティ監査実施者、統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者、許可権減車及び情報セキュリティ関係規程を整備した者

システム: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責任者を含む複数の者が主体となっているものを含む)、情報システムセキュリティ管理者及び権限管理を行う者

政府機関の対策実施状況報告（2007年度）の評価結果【遵守事項ベース】

政府機関全体の実施状況について特筆すべき遵守事項は次のとおり。

1　情報セキュリティ対策の教育

[統一基準2．2．1]

全府省庁の平均実施率

84．2%

遵守事項	実施率
(1)教育の実施	84．1%
(2)教育の受講	84．8%

遵守事項別実施率

①毎年度1回以上実施すべき教育の計画策定や着任・異動後3ヶ月以内に実施すべき教育の計画策定が不十分。
　計画がなされていても受講状況の把握や未受講者への受講指導の徹底が不十分。

②職員による教育受講が不十分である。

2　格付け・取扱い制限に係る措置

[統一基準3．2．1～3．2．6]

全府省庁の平均実施率

89．7%

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

③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である。

④　情報の移送、情報の提供時において、管理者に対して行うべき許可申請、届出が不十分である。

3　情報システムの台帳整備

[統一基準4．3．1(5)]

全府省庁の平均実施

77．9%

⑤　情報システムが扱う情報や当該情報の格付けを含む事項を記載した情報システムの台帳整備が不十分。

4　安全区域内における職員識別の徹底

[統一基準5．1．1(4)]

全府省庁の平均実施率

93．2%

⑥　安全区域内における職員識別の徹底については、昨年度は課題とされたが、昨年に比べ、安全区域内の職員識別の徹底について改善がみられる。

○　今後、教育の実施など十分進んでいない遵守事項について各省庁はその改善に努めるとともに、NISCにおいてはその実施状況をフォローし、必要な協力を行う必要がある。

（参考1）報告対象範囲

2007年度は、2008年度に全対象を報告対象とするためのロードマップとして位置づけ、組織の規模や事務繁忙期等に配慮し、各府省庁から事前に提示された範囲を報告対象とした。

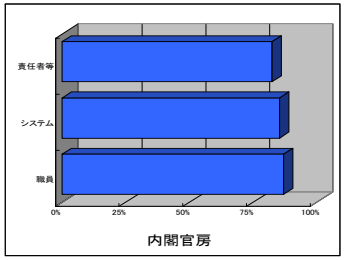
	2007年度の把握率	2007年度に報告対象とした範囲		2008年度の報告対象範囲
		職員	情報システム	
内閣官房	78.2%	すべて対象	すべて対象	すべての職員・すべての情報システムが報告対象
内閣法制局	100%	すべて対象	すべて対象	
人事院	100%	すべて対象	すべて対象	
内閣府	91.4%	本府（地方支分部局を除く）：すべて対象	すべて対象	
宮内庁	100%	係長相当職以上で単独でパソコンを使用する職員	前回対象4情報システム類型（※）	
公正取引委員会	96.7%	本局：課室長級以上及び各課室総括担当職員 地方機関：課室長級以上及び総務課職員	前回対象4情報システム類型＋主要情報システム	
警察庁	100%	本庁内部部局：すべて対象 附属機関及び地方機関：課長相当職以上	前回対象4情報システム類型＋インターネットに接続された情報システム	
金融庁	100%	課長補佐相当職以上	前回対象4情報システム類型＋主要情報システム	
総務省	93.6%	すべて対象	すべて対象	
法務省	100%	本省（外局含む）：すべて対象 所管各庁：本省課室長相当職以上	本省において所管しているすべての情報システム	
外務省	100%	すべて対象（ただし、在外公館の現地職員は除く）	前回対象4情報システム類型＋主要情報システム＋その他要保護情報を扱う情報システム	
財務省	100%	本省（外局含む）：すべて対象 地方機関（税関、国税局、財務局）：すべて対象 地方機関（税務署）：各署統括官（課室長相当職）以上	前回対象4情報システム類型＋主要情報システム	
文部科学省	56.4%	係長相当職以上	前回対象4情報システム類型＋主要情報システム	
厚生労働省	80.4%	本省（外局含む）：すべて対象 地方機関等：政令職以上	すべて対象	
農林水産省	100%	本省：すべて対象 地方出先機関：一部対象外	すべて対象	
経済産業省	95.9%	行政職俸給表（一）における6級以上（指定職含む）	すべて対象	
国土交通省	100%	本省（外局含む）：課室長以上 地方機関：本省課室長相当職以上	前回対象4システム類型＋主要情報システム	
環境省	83.8%	すべて対象	すべて対象	
防衛省	98.8%	すべて対象	すべて対象	

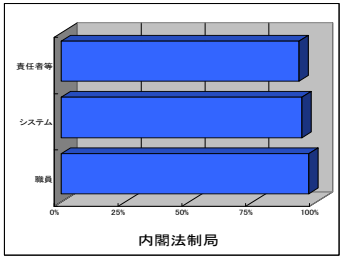
把握率：各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合

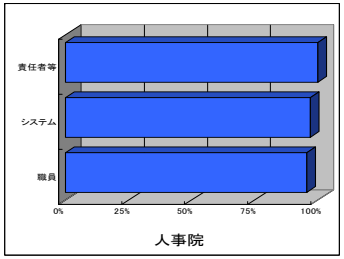
（※前回対象4情報システム類型：電子申請システム、文書管理システム、府省庁LANシステム、最適化対象システム）

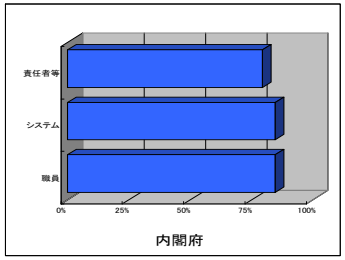
（参考2）各府省庁の対策実施状況報告（2007年度）の集計結果

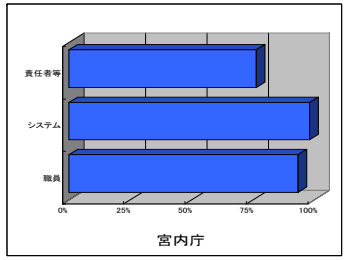
○ 実施率

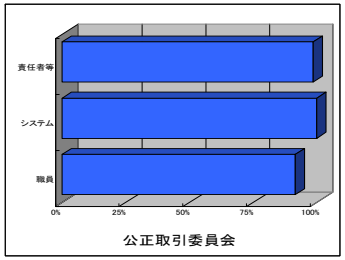


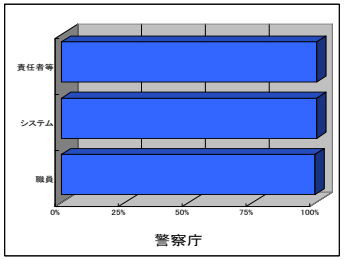


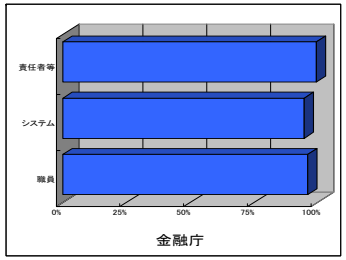


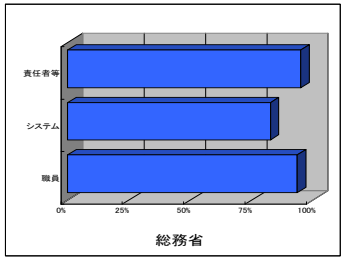


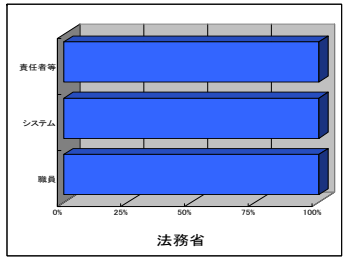


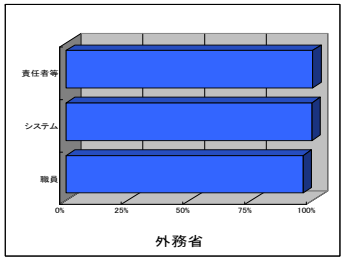


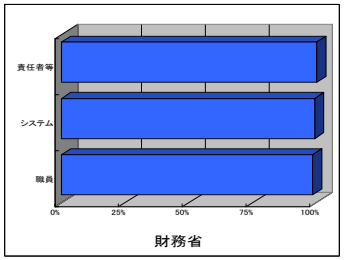


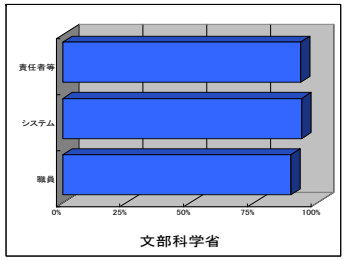


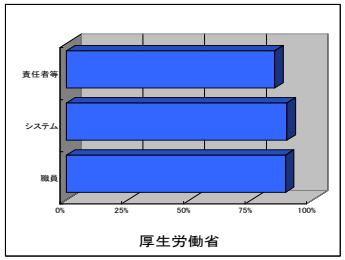


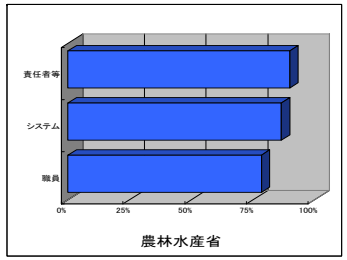


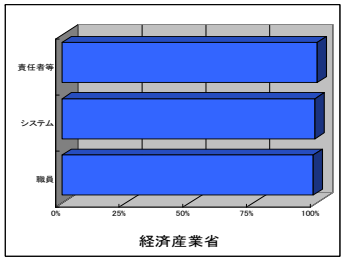


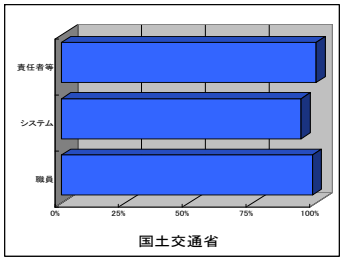


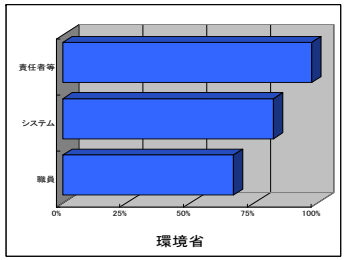


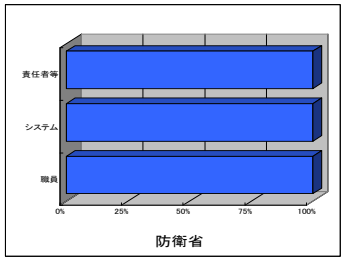


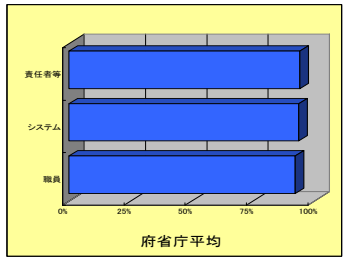








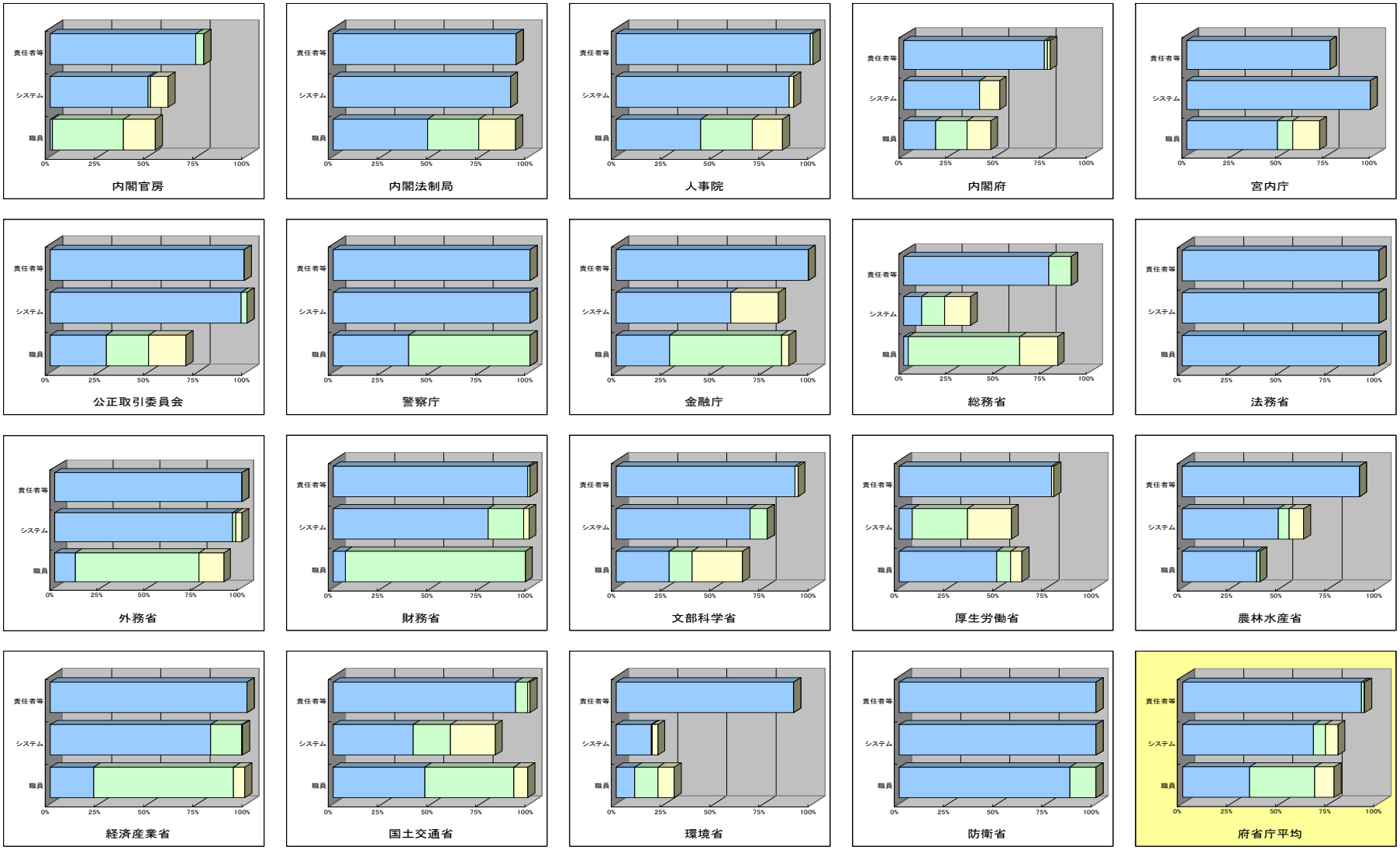




実施率：把握した者のうち、責務が生じた者に占める対策を実施した者の割合

（参考2）各府省庁の対策実施状況報告（2007年度）の集計結果

○ 到達率



全対象者が対策を実施した遵守事項の割合
95%以上の対象者が対策を実施した遵守事項の割合
90%以上の対象者が対策を実施した遵守事項の割合

到達率：把握した者のうち、責務が生じた一定の割合（100%、95%、90%）以上の者が対策を実施した遵守事項の割合

「政府全体のPDCAサイクル」のための各省検査及び評価
～端末・ウェブサーバに関する重点検査（2007年度）

重点検査の項目

端末に関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・主要APのパッチ等の適用状況 ・アンチウイルス対策ソフトの運用状況
情報保護対策	・モバイルPCの暗号化機能の運用状況
端末管理	・端末の物理的対策状況

ウェブサーバに関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・WEBサーバAPのパッチ等の適用状況等
不正アクセス対策	・不正アクセス対策状況
情報保護対策	・利用者に対する権限管理等の実施状況
サーバ管理	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況

・府省庁の調査に基づく結果
・平成19年3月末時点

総合評価	端末			ウェブサーバ		
	H18		H19	H18		H19
内閣官房	B	▶▶	B	B	▶	B
内閣法制局	C	▶▶	B	B	—	B
人事院	C	▶▶▶	A	B	▶▶	B
内閣府	C	▶▶▶	B	C	▶▶	B
宮内庁	D	▶▶▶▶	A	C	▶▶▶	A
公正取引委員会	C	▶▶▶	A	A	—	A
警察庁	D	▶▶▶▶	A	B	▶▶	A
金融庁	B	▶▶	B	B	▶	A
総務省	C	▶▶▶	B	B	▶	B
法務省	D	▶▶▶▶	B	C	▶▶▶	B
外務省	D	▶▶▶▶	A	B	▶▶	B
財務省	C	▶▶	B	B	▶▶	B
文部科学省	C	▶▶▶	A	B	▶▶	A
厚生労働省	D	▶▶▶	B	B	▶	B
農林水産省	C	▶▶▶	A	B	▶	A
経済産業省	C	▶▶▶	A	B	▶	A
国土交通省	D	▶▶▶	B	C	▶▶	B
環境省	B	▶	B	B	▶▶	A
防衛省	C	▶▶▶	B	B	▶▶	A

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x=100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

上昇率	上昇率	上昇率	上昇率	上昇率	上昇率
▶▶▶▶ x＞ 40%	▶▶▶ x＞ 30%	▶▶▶ x＞ 20%	▶▶ x＞ 10%	▶ x＞ 0%	— x= 0%

「政府全体のPDCAサイクル」のための各省検査及び評価
～電子メールサーバに関する重点検査（2007年度）

重点検査の項目

電子メールサーバに関する重点検査項目	
不正プログラム対策	・OSのセキュリティパッチ適用状況（アップデートの状況） ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況） ・電子メールコンテンツに対する不正プログラム対策の状況
サーバ管理	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況 ・時刻同期機能の動作
不正アクセス対策	・不正中継対策の状況
情報保護対策	・電子メールの受信に係わる利用者に対する認証等の実施状況

・府省庁の調査に基づく結果
・平成19年9月末時点

総合評価	電子メールサーバ	（参考）端　末	（参考）ウェブサーバ
	平成19年9月末	平成19年3月末	平成19年3月末
内閣官房	B	B	B
内閣法制局	B	B	B
人事院	A	A	B
内閣府	B	B	B
宮内庁	B	A	A
公正取引委員会	B	A	A
警察庁	A	A	A
金融庁	A	B	A
総務省	B	B	B
法務省	B	B	B
外務省	B	A	B
財務省	A	B	B
文部科学省	A	A	A
厚生労働省	A	B	B
農林水産省	A	A	A
経済産業省	A	A	A
国土交通省	B	B	B
環境省	A	B	A
防衛省	A	B	A

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x＝100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

政府機関の情報セキュリティマネジメントの総合的評価

- 情報セキュリティ・ベストプラクティス

★★ 省内ネットワークを活用した職員の支援
・eラーニングシステム　・実施手順等の運用 — 総務省 / 経済産業省

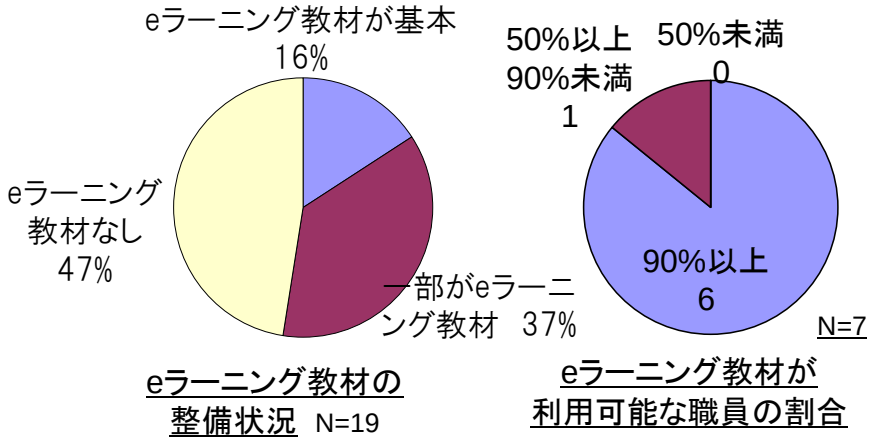
★★ 幹部職員の下で全庁一体となった対策の推進 — 警察庁

★★ 外部委託における情報セキュリティの確保 — 外務省 / 防衛省

・ 政府機関の模範となるプラクティス(★★)は「計画」及び「周知」を中心に44件。
・ 政府内外を問わず模範となる先進的な取り組み(★★★)は見られなかった。

- 各府省庁の体制等の調査結果
・ 情報セキュリティ担当者(常任)の職員に占める割合:
2%超=4府省庁、0.5%以下=7府省庁
・ 情報セキュリティ担当者(常任)の平均経験年数:
1年～3年が中心
・ eラーニング導入は府省庁全体では部分的:
「eラーニング教材が(一部でも)ある」=10府省庁

※eラーニング:コンピュータネットワークなどを活用して教育を行うこと



eラーニング教材の整備状況 N=19

eラーニング教材が利用可能な職員の割合

電子政府の情報セキュリティを企画・設計段階から組み込むための方策（SBD）の推進

今後、電子政府の取組みが本格化し、我が国政府・行政の活動基盤がITへの依存度を高めていく中で、情報セキュリティの確保は不可欠。

ITの利活用と情報セキュリティは車の両輪

【参考】電子政府の取組みの本格化の動き（例）

【平成20年第6回経済財政諮問会議における福田総理コメント】
・・・　利便性、それから、役所の無駄を省くという一石二鳥を政府のIT化で実現しようとすることなのだが、これは随分、時間がかかっている。前から言っていて、なかなか実現しない。・・・是非、岸田臨時議員を中心に頑張っていただきたい。・・・

【「IT政策ロードマップ」中間報告（平成20年4月22日　IT戦略本部）中の記述】
・・・　オンライン利用率50%という当初の目標の着実な達成に向け、当面のオンライン利用拡大策を着実に進めるとともに、従来までの発想を大きく転換し、次世代の電子行政サービスの実現に向けた取組みを従来にないスピード感をもって、抜本的に強化する。・・・

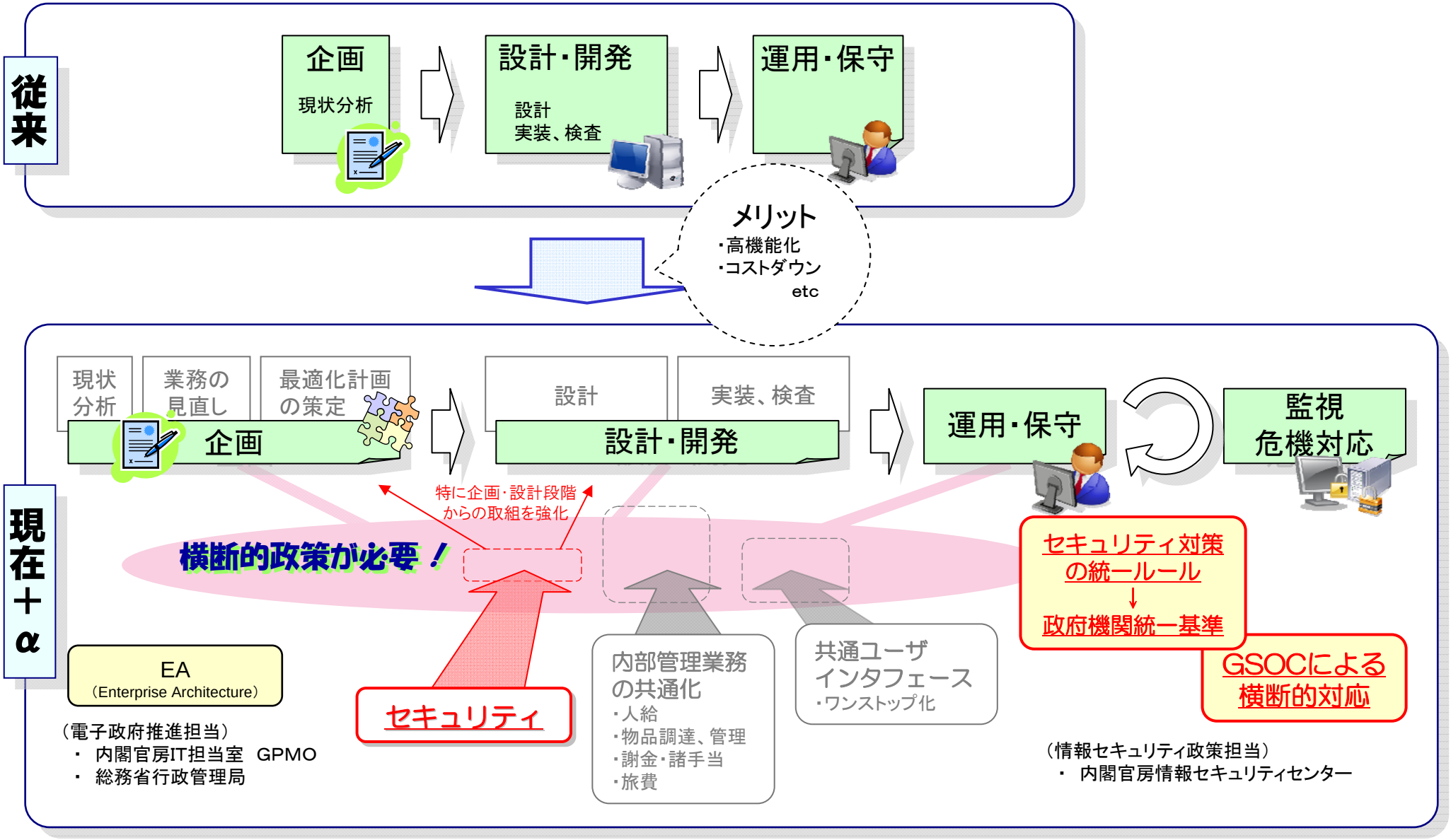
システム構築段階からセキュリティを取り入れた電子政府の企画・設計を行うための方策としてSBDを推進

【以下のような効果で電子政府の情報セキュリティ確保に貢献】

- 必要なセキュリティ要件が企画・設計段階から適切に検討され、後の工程においてセキュリティ上の抜け穴が生ずるおそれを無くす。
- 適切な調達仕様が示されることにより、調達プロセスにおいてベンダーと的確な意思疎通が可能となる。
- 構築が進んだシステムに対して後追い的にセキュリティ対策を講ずるよりもコスト的に優しく、使い勝手の面でも無理をかけない。

電子政府構築との連携

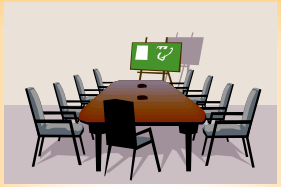
（国民本位の安全で使いやすい電子政府構築）



電子政府における安全な暗号の利用

電子政府における安全な暗号の利用に関する現在の体制

情報セキュリティ政策会議



内閣官房
情報セキュリティセンター

決定

決定

基本遵守事項
として使用を明記

政府機関統一基準

注意喚起等を
踏まえ指針を決定

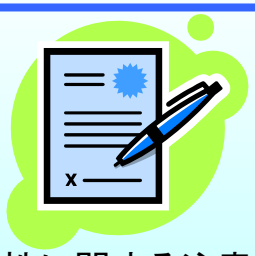
暗号移行指針（※）

暗号技術検討会
（総務省・経済産業省）

CRYPTREC
Cryptography Research and Evaluation Committees

評価・検討

電子政府推奨暗号リスト



安全性の
監視・調査

安全性に関する注意喚起
（「SHA－1の安全性に関する見解」等）

※:「政府機関の情報システムにおいて使用している暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月22日情報セキュリティ政策会議決定）

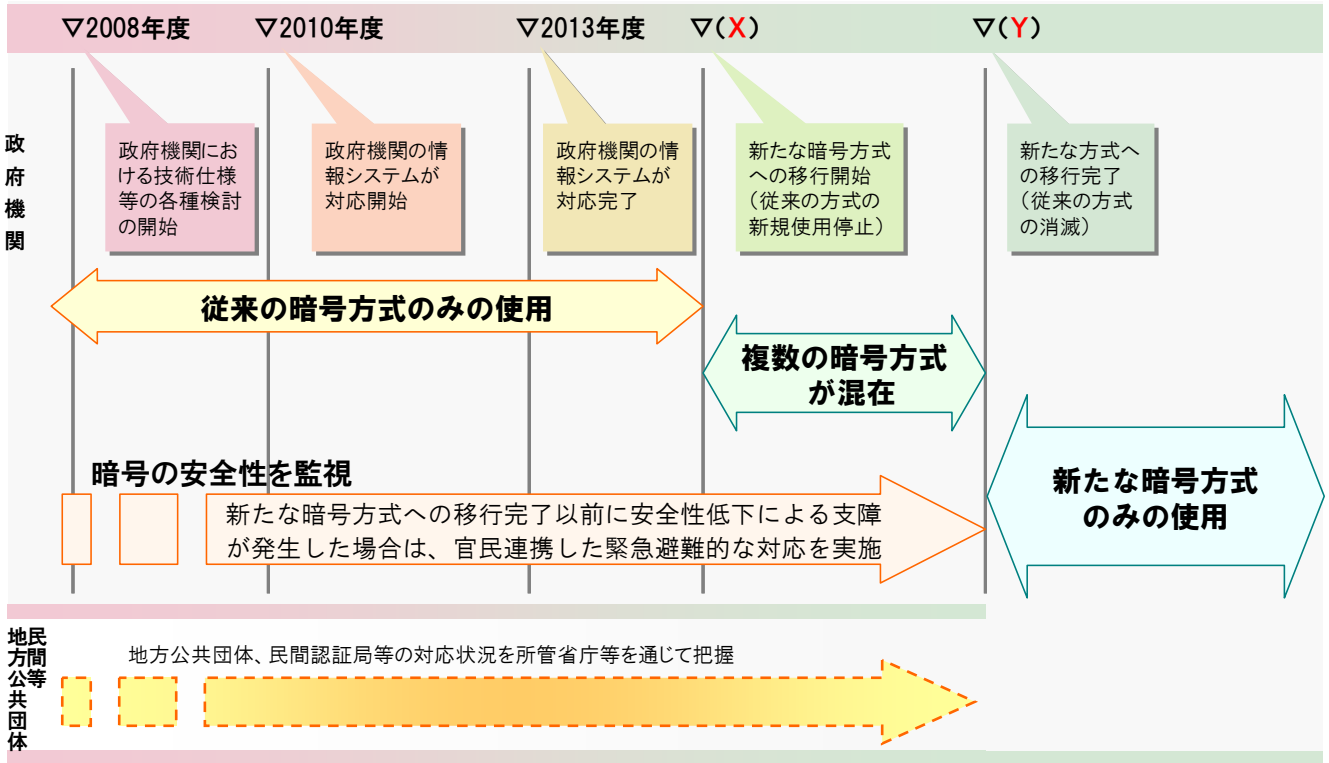
電子政府における安全な暗号の利用

「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」の決定

①電子政府システムでは、電子署名等のために暗号が使用されており、SHA-1及びRSA1024と呼ばれる暗号方式を広く使用。
②しかし、このSHA-1及びRSA1024は、安全性の低下が指摘されており、より安全な暗号方式への移行が必要。
③より安全な暗号方式への移行にあたっては、情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため、政府統一的な移行指針を策定することが必要。

「新たな暗号方式としてSHA-256及びRSA2048を採用すること」などを規定した移行指針を情報セキュリティ政策会議において決定

移行指針に基づく暗号方式の移行スケジュール



（X, Y）：関係機関との調整を図りながら、2008年度中に時期を検討

（参考）
米国では**期限を決めて対応する方法**を採用し、2010年末以降、政府機関において、SHA-1の新規使用を停止する方針。
しかし、SHA-1が2010年に危殆化するかどうかは専門家の間でも意見がわかれる。
このため本指針は、**暗号の安全性低下の状況を監視しながら対応する方法**とし、政府が暗号の安全性を監視し、安全性低下が早まった場合は、緊急避難的な対応を実施（コンテンジェンシープランの発動）。