

「政府機関の情報セキュリティ対策の ための統一基準」について

2006年8月2日

内閣官房情報セキュリティセンター

NISC (National Information Security Center)

<http://www.nisc.go.jp/>

講演内容について

対象者:

政府機関統一基準全般に関心のある者

受講するための前提条件:

情報セキュリティの基本的知識

情報セキュリティポリシーの策定経験

統一基準とは

統一基準ができる前…

「政府機関における情報セキュリティ対策はどのようになっていますか？」というお問い合わせをいただいた際には、「各政府機関により対策内容が異なります。」という対応をしていました。

統一基準によって…

「各政府機関では統一基準に沿って情報セキュリティ対策基準を定めています。取り扱う情報等により、それ以上の対策基準を定めている機関もあります。」と回答できるようになりました。

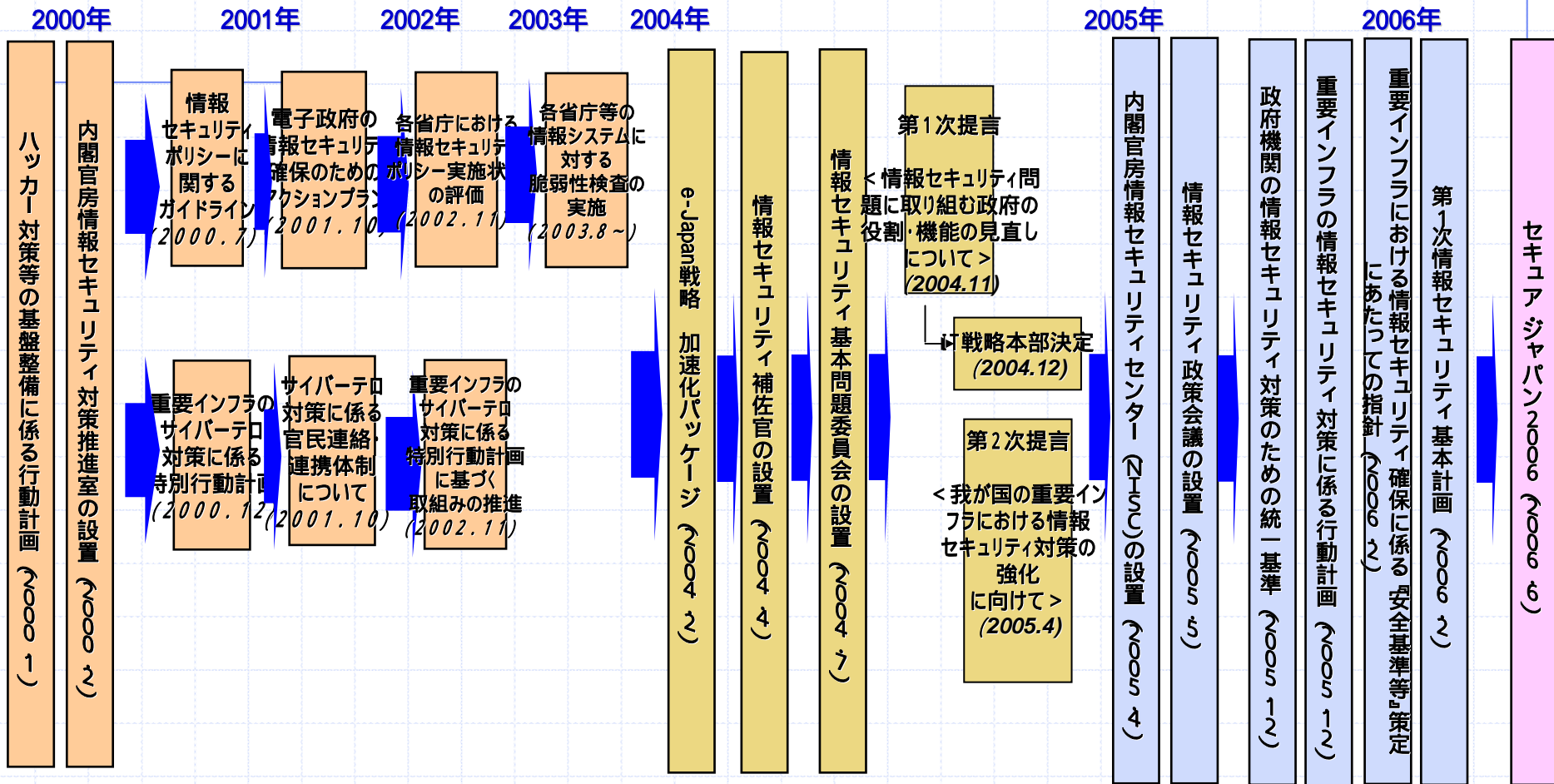
目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

現在までの内閣官房における情報セキュリティ政策の流れ



内閣官房の体制強化の変遷

2000年2月発足時 2001年1月

8名 → 9名

2004年7月

18名

2005年4月NISC設置時

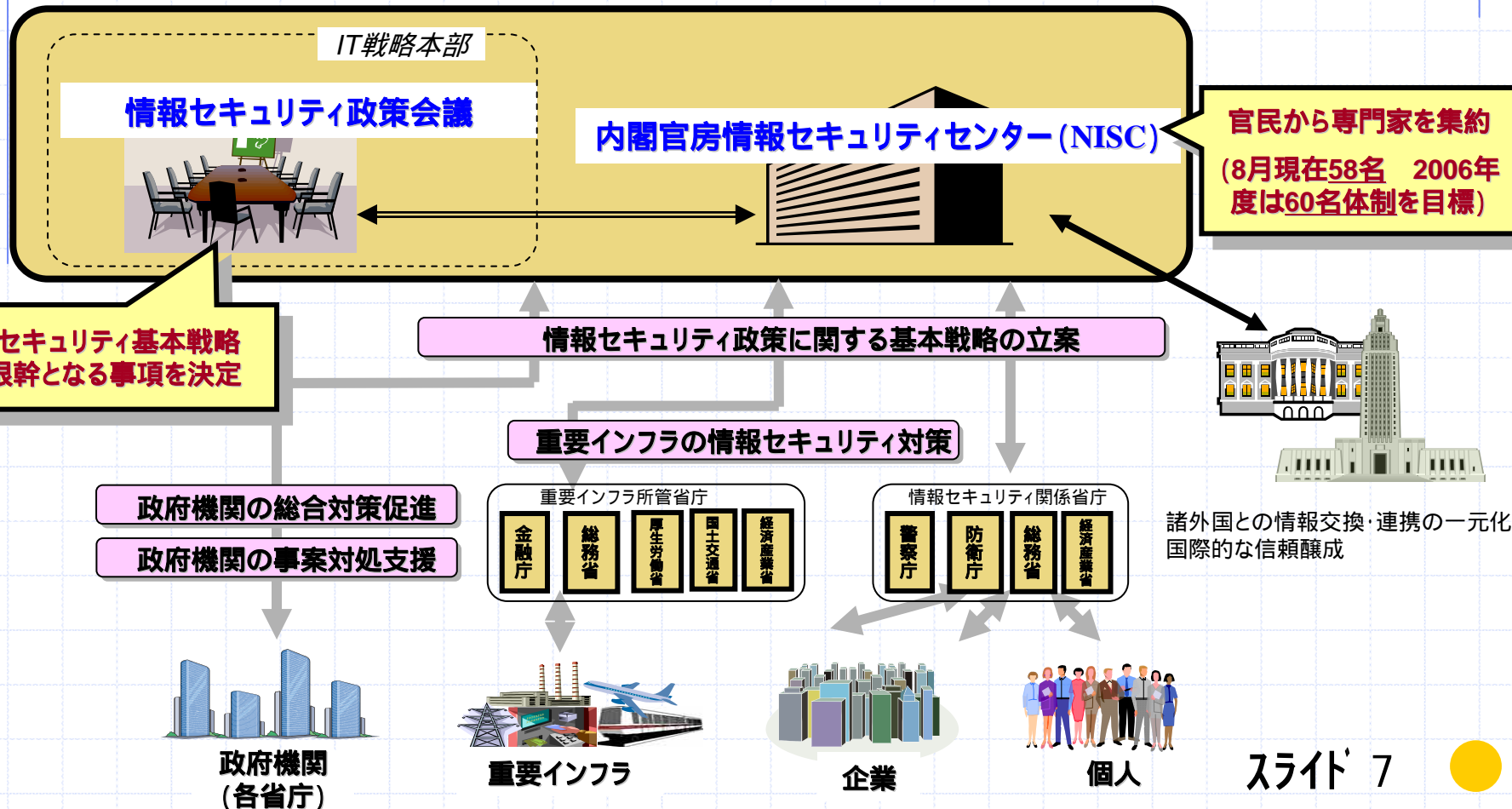
35名

2006年8月

58名

情報セキュリティ政策会議及び 内閣官房情報セキュリティセンター (NISC) の設置

- 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」(2004年12月7日IT戦略本部決定)を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備中。
 - **2005年4月25日、内閣官房情報セキュリティセンター (NISC; National Information Security Center) を設置。**
 - **2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」を設置。**



情報セキュリティ政策会議とは

情報セキュリティ政策会議の設置について

平成17年5月30日

高度情報通信ネットワーク社会推進戦略本部長決定

1 高度情報通信ネットワーク社会推進戦略本部令(平成12年政令第555号)第4条の規定に基づき、官民における統一的・横断的な情報セキュリティ対策の推進を図るため、高度情報通信ネットワーク社会推進戦略本部に、**情報セキュリティ政策会議(以下「政策会議」という。)**を置く。

2 政策会議の構成員は、次のとおりとする。ただし、構成員以外の国務大臣も必要に応じて会議に出席し、意見を述べることができる。

議長 内閣官房長官

議長代理 情報通信技術(IT)担当大臣

構成員 国家公安委員会委員長

防衛庁長官

総務大臣

経済産業大臣

情報セキュリティ対策に関し優れた見識を有する者であって高度情報通信ネットワーク社会推進戦略本部長から政策会議における審議に参画することを委嘱された者

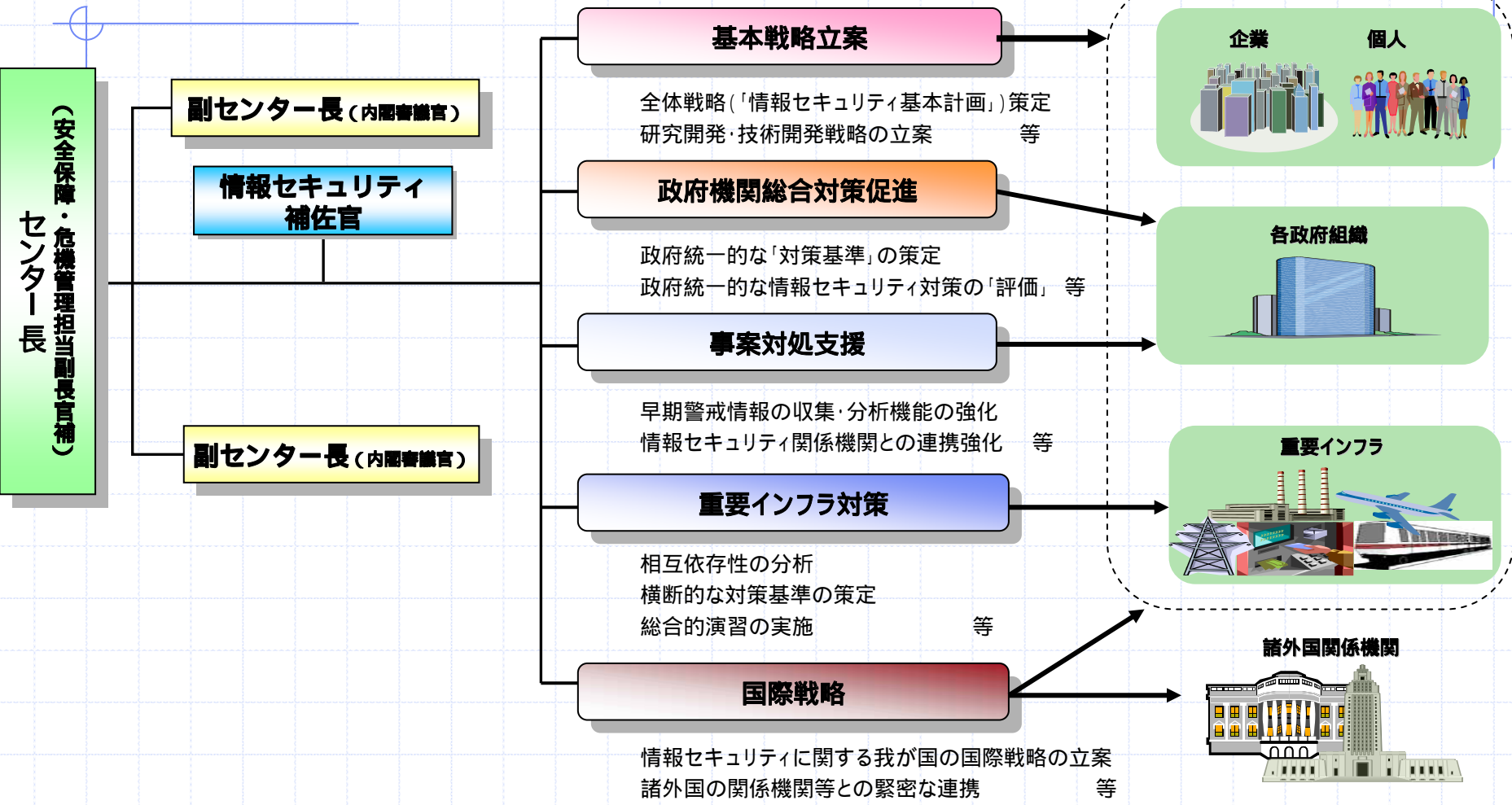
3 政策会議の庶務は、警察庁、防衛庁、総務省及び経済産業省の協力を得て、内閣官房において処理する。

4 前各項に掲げるもののほか、政策会議の運営に関する事項その他必要な事項は、議長が定める。

附 則

以上に伴い、情報セキュリティ対策推進会議を廃止する

内閣官房情報セキュリティセンター (NISC) の機能・体制



各府省庁による情報セキュリティ対策 平成12年～現在の状況

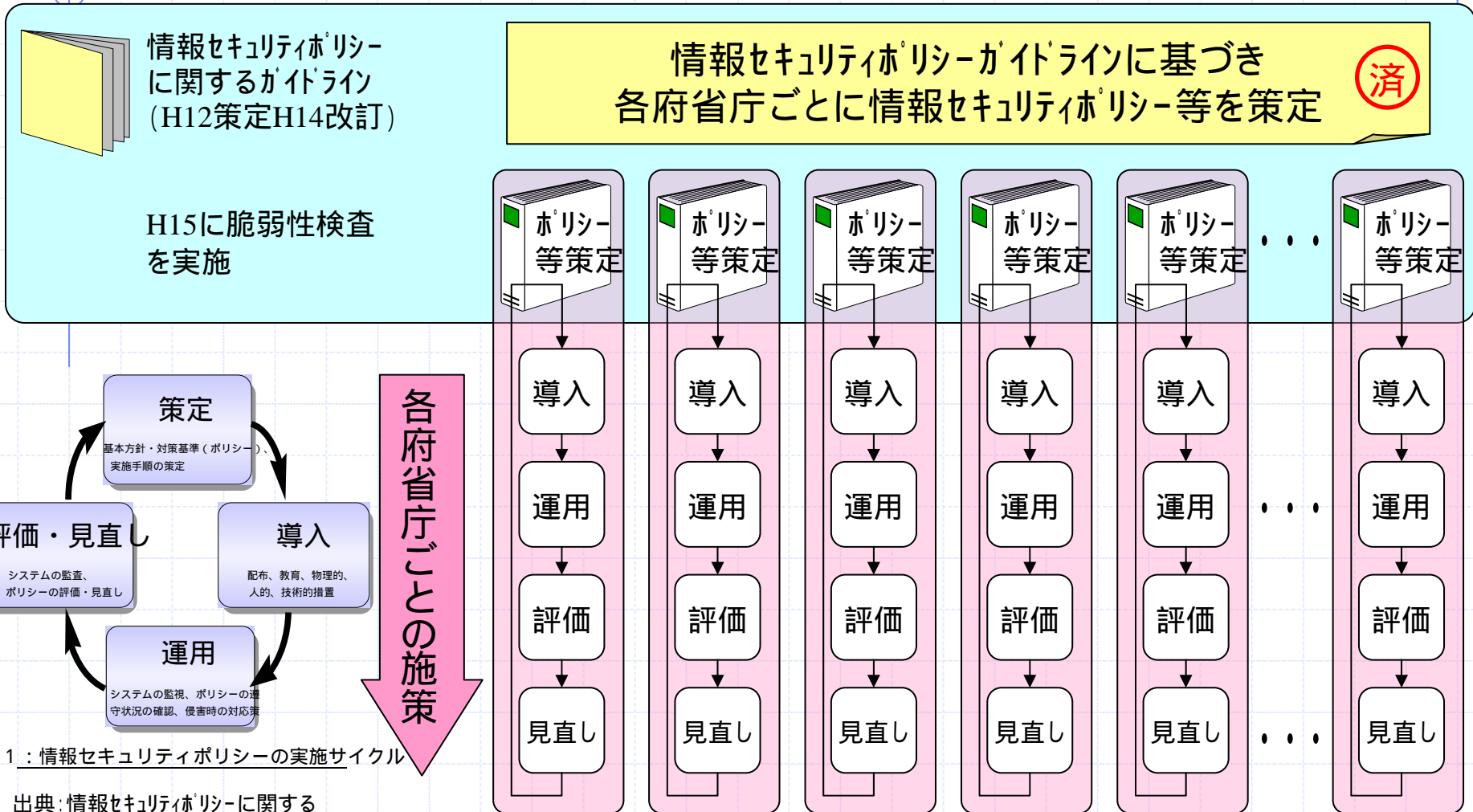


図1：情報セキュリティポリシーの実施サイクル

出典：情報セキュリティポリシーに関するガイドライン (H12策定H14改訂)

各府省庁による情報セキュリティ対策 現在の「ポリシー等文書体系」

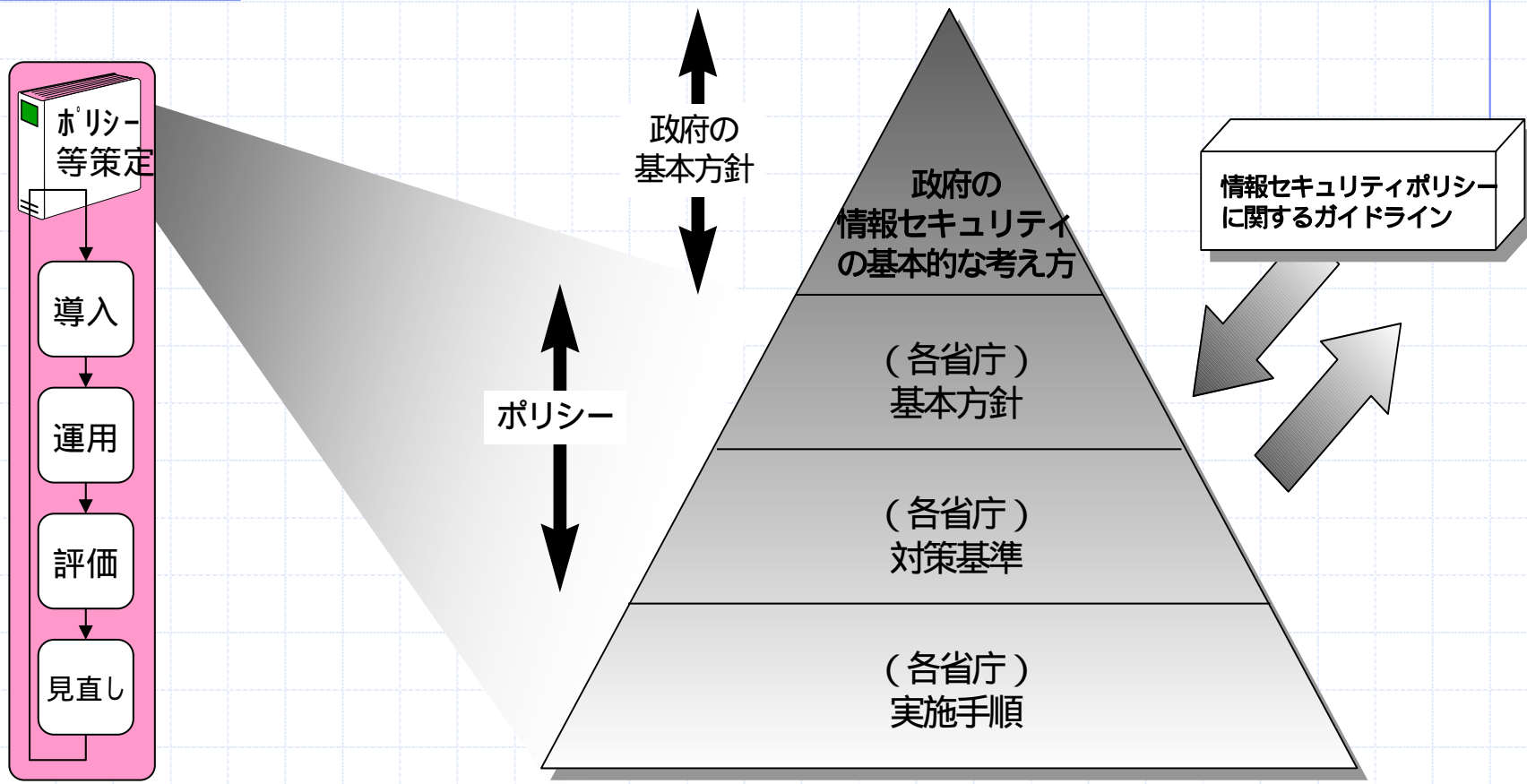


図2：ポリシーの位置づけ

出典：情報セキュリティポリシーに関するガイドライン(H12策定H14改訂)

各府省庁における 情報セキュリティ対策基準の状況

認識された課題:

「情報セキュリティポリシーに関するガイドライン」(平成12年7月)に基づき、各府省庁において「情報セキュリティポリシー」が策定され、運用されている。

各府省庁の情報セキュリティ水準の向上に一定の成果があったものの、具体的な対策の内容・水準については各府省庁それぞれで決めることとしているため、各府省庁で情報セキュリティ水準にばらつきがみられる。

周辺環境の変化:

政府機関に対するサービス不能攻撃(DoS攻撃)等、情報セキュリティに対するリスクは近年急速に増大している。

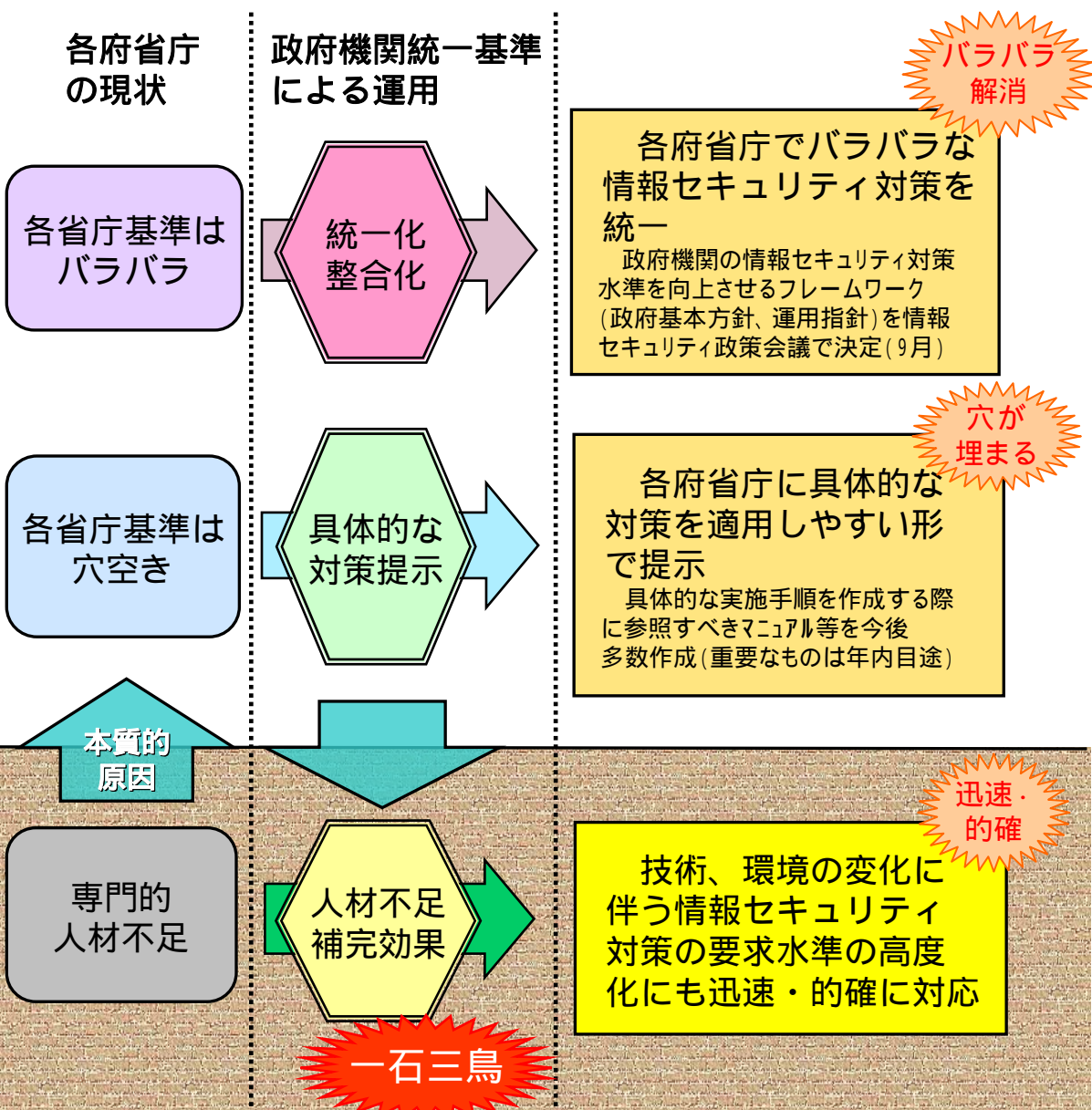
政府機関統一基準 の必要性・目的

情報セキュリティに対するリスクの高まりにより、政府全体として十分な情報セキュリティ水準の確保が必要。

「政府機関の情報セキュリティ対策における政府機関統一基準」を策定し、各府省庁の情報セキュリティ水準の斉一的な引き上げを図り、各府省庁が保有する情報の漏えい、改ざん、破壊を防止し、適正な行政サービスを継続して提供することをもって、国民の信頼を確保しようとするものである。

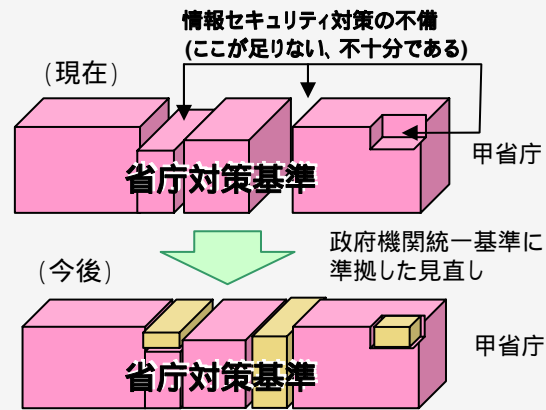
政府機関統一基準の策定の目的

世界最先端のIT(情報技術)国家にふさわしい情報セキュリティ水準を目指して、統一基準を運用

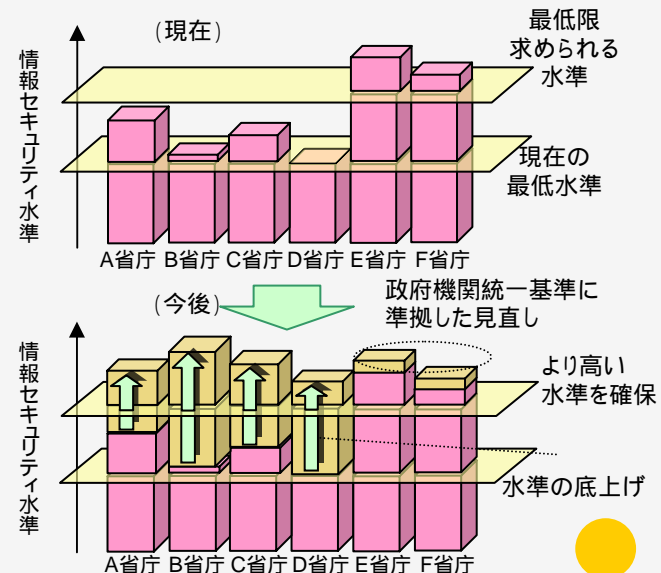


各府省庁の対策の統一化・整合化と水準の向上

政府機関統一基準による省庁対策基準の補完

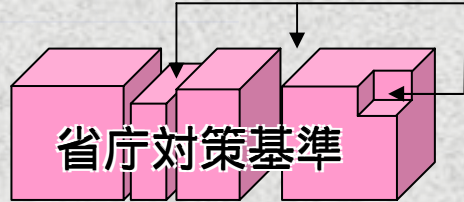


各府省庁の情報セキュリティ水準の向上



政府機関統一基準による省庁対策基準の補完

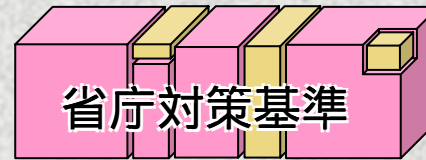
(現在) 情報セキュリティ対策の不備
ここが足りない、不十分である



甲省庁



(今後)

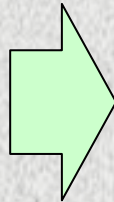
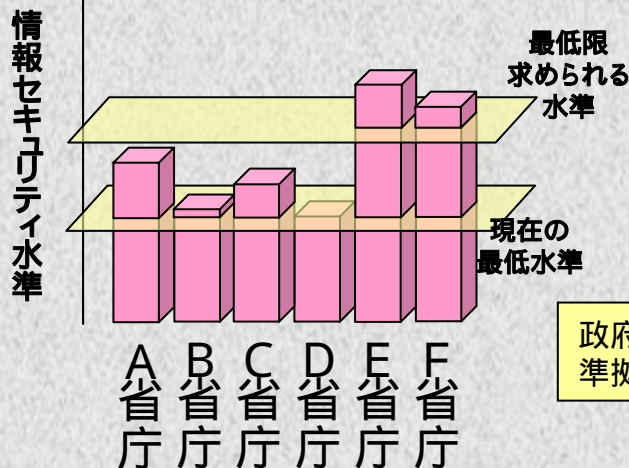


甲省庁

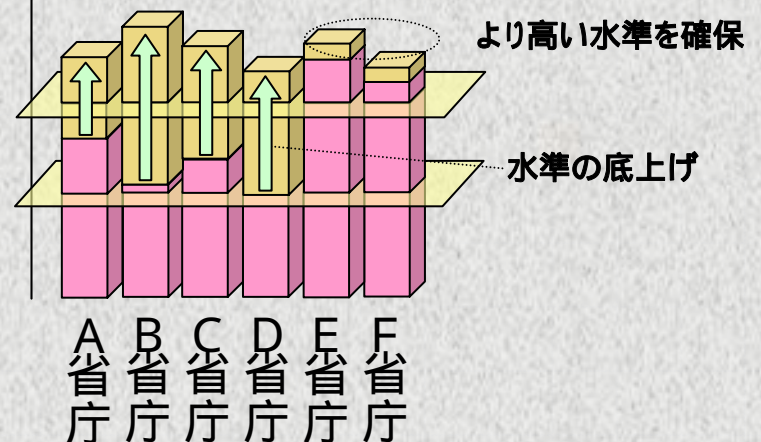
政府機関統一基準に
準拠した見直し

各府省庁の情報セキュリティ水準の向上

(現在)



(今後)

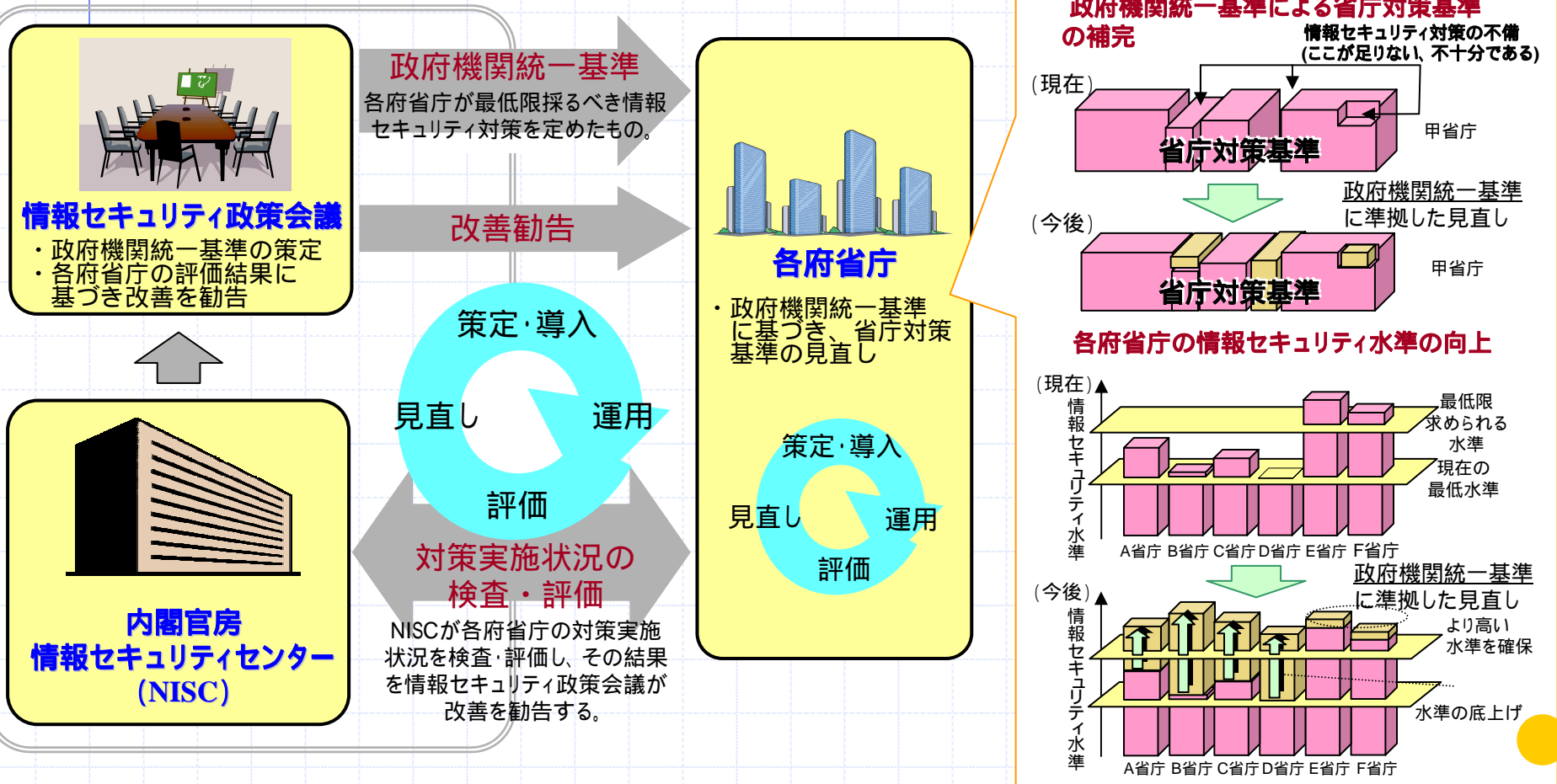


政府機関統一基準に
準拠した見直し

個別設計図としての「政府機関統一基準」

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の「個別設計図」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(NISC)**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**。



統一基準による情報セキュリティ対策の実施

(緊急度の高い対策中心)

17年度内サイクル

旧ガイドライン
(平成12年)

内容充実・項目追加

(9月)

政府機関統一基準
(2005年項目限定版)

各府省庁の当初状態
実態調査
…(12月までに)

(12月)

各府省庁基準改定
状況検査
…(3月までに)

ファーストラック作業

標準的年度サイクルの実施

項目を追加充実

政府機関統一基準
パブリックコメント実施

政府機関統一基準
(2005年12月版(全体版初版))

標準的年度
サイクルの開始

セキュリティ対策に関する
検査を複数年にわけて
順次実施

策定・導入

見直し

運用

評価

策定・導入

見直し

運用

評価

個別マニュアル群の整備

対策の
具体化の
切り札

基準を適用する
具体的基準

緊急性の高い項目
について作成(12月)

個別マニュアル群

充実

項目追加

継続的に
追加・更新

中長期的なセキュリティ 対策の強化・検討

最適化計画とは、
総務省行政管理局
が中心となって推進
しているシステム
刷新計画

最適化計画対象の
政府共通システム
の開発との連携

最適化計画で新たに開発
(導入)するシステムの
セキュリティ機能を明確化

セキュリティ強化に
資する新規システム
(機能)の導入検討と
その実現

(検討例)

IPv6、生体認証
セキュアOS…

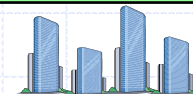
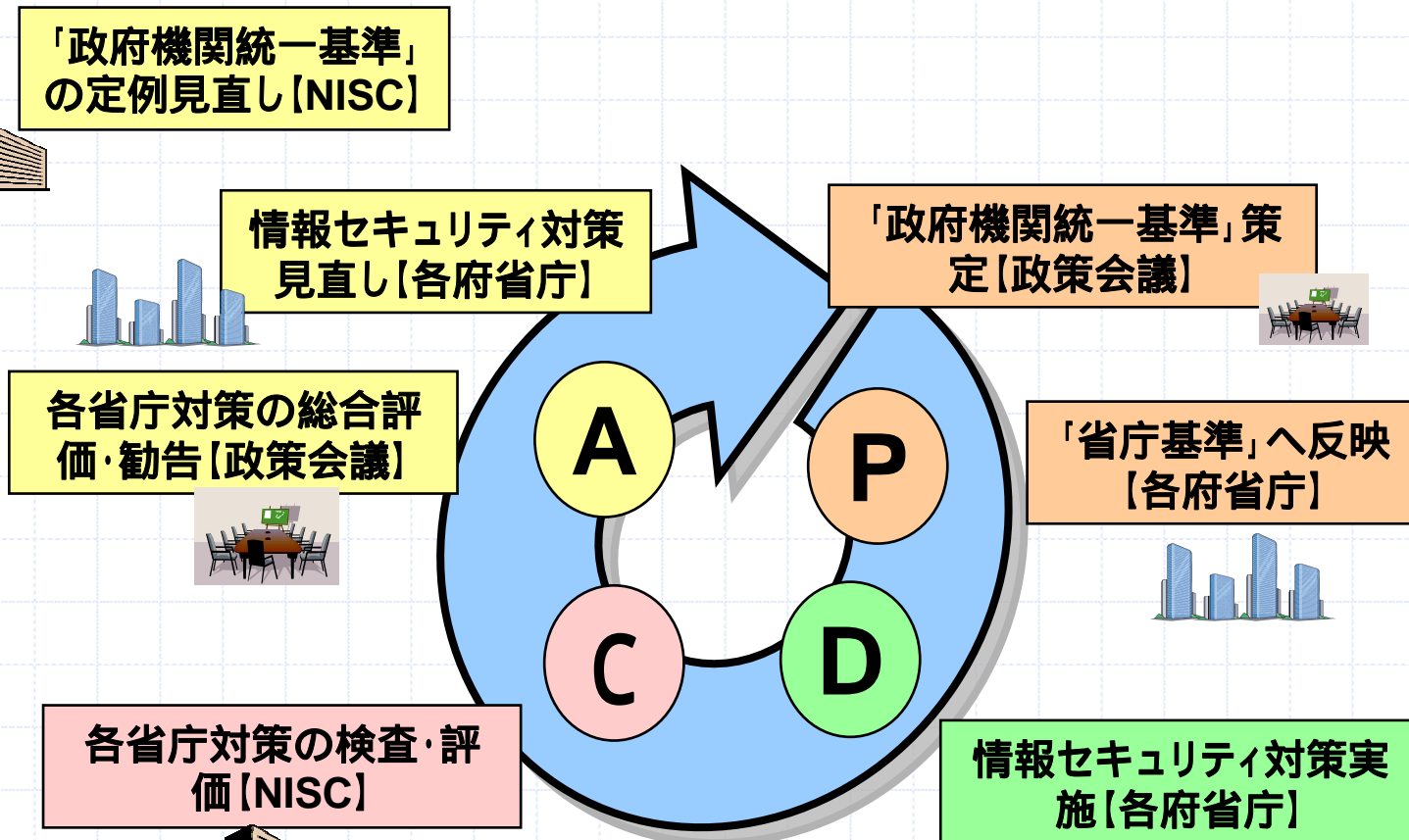
17FY

18FY

19FY

世界最先端のIT(情報技術)国家にふさわしい情報セキュリティ水準の実現

「政府機関統一基準」に基づく PDCAサイクル



目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答



2 . 1

政府機関統一基準 文書群体系の説明

政府機関統一基準文書群の策定

基本問題委員会提言等において、「政府統一安全基準」等を定めると記載しているものは、具体的には「**政府機関統一基準文書群**」を定めることをいい、以下の文書群のことである。

政府機関の情報セキュリティ対策の強化に関する基本方針
政府機関の情報セキュリティ対策における政府機関統一基準
の策定と運用等に関する指針
政府機関の情報セキュリティ対策のための統一基準
統一基準適用個別マニュアル群

これを指す

については、補足等するための解説書等がある。

政府機関統一基準文書群の 略称

政府機関の情報セキュリティ対策の強化に関する基本方針

政府基本方針

政府機関の情報セキュリティ対策における政府機関統一基準
の策定と運用等に関する指針

統一基準運用指針

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

統一基準適用個別マニュアル群

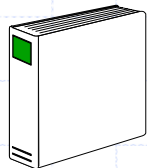
個別マニュアル群

～ については以下のWebページで公開

<http://www.nisc.go.jp/active/general/kijun01.html>

については公開予定(2006年8月以後)

政府機関統一基準の 文書番号 K303



政府機関統一基準

正式名称：「政府機関の情報セキュリティ対策のための統一基準」

略称：「政府機関情報セキュリティ対策統一基準」

「政府機関統一基準」

文脈上問題なければ、「統一基準」も使用可

文書を特定する場合：「NISD-[K303](#)-052」

→ NISD: National Information Security Documents

→ K303: 政府機関統一基準のための固定番号

→ 052: 版番号 (2005年度の第2版の意)

文書番号: NISD-K303-052

政府機関統一基準の全体構成

- 第1部 総則
- 第2部 組織と体制の構築
- 第3部 情報についての対策
- 第4部 セキュリティ要件の明確化に基づく対策
- 第5部 情報システムの構成要素についての対策
- 第6部 個別事項についての対策



2 . 2

政府機関統一基準の内容説明

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第1部の構成

第1部 総則

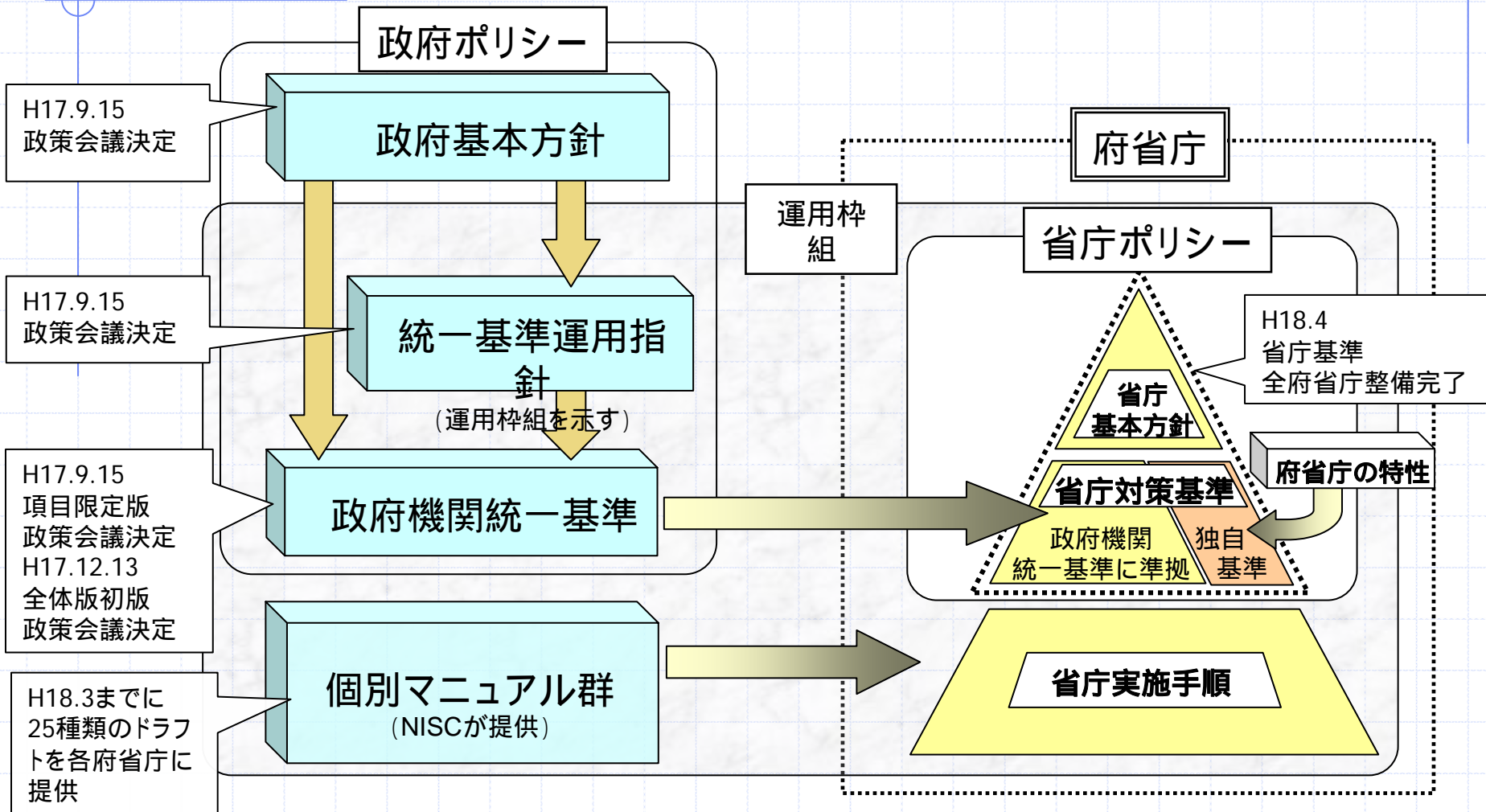
1.1.1 本統一基準の位置付け

1.1.2 本統一基準の使い方

1.1.3 用語定義

第1部 総則

1.1.1 本統一基準の位置づけ

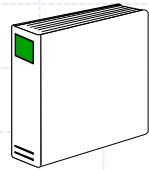


政府機関統一基準 現行ガイドラインとの関係

「現行のガイドライン(「A省ポリシー(例)」を含む。)」のうち、各府省庁が実施すべき具体的な対策に該当する部分は、これを抽出し、必要な追加、削除、修正を行った上で「政府機関統一基準」に盛り込んだ。

他方、各府省庁がセキュリティポリシーを策定する上での手続き及び考え方に関する部分は、「統一基準運用指針」として再構成した。

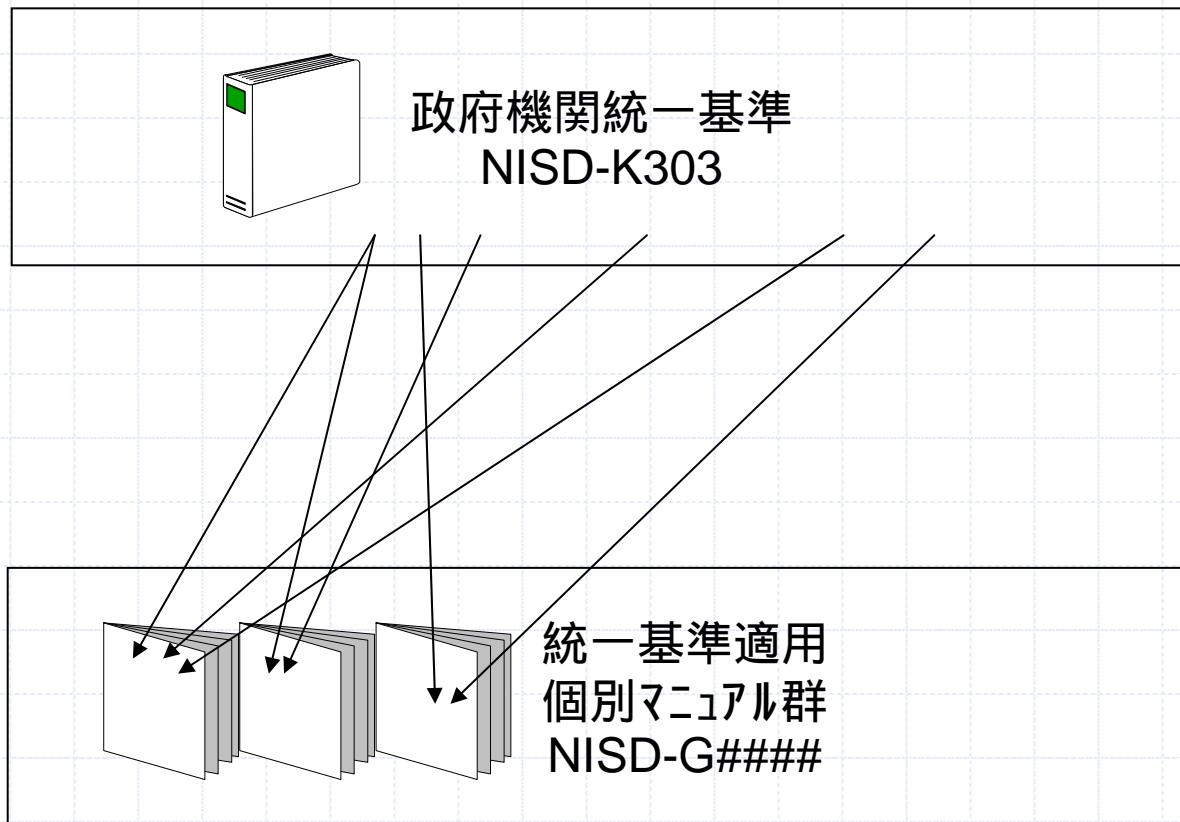
政府機関統一基準の 項目群構成



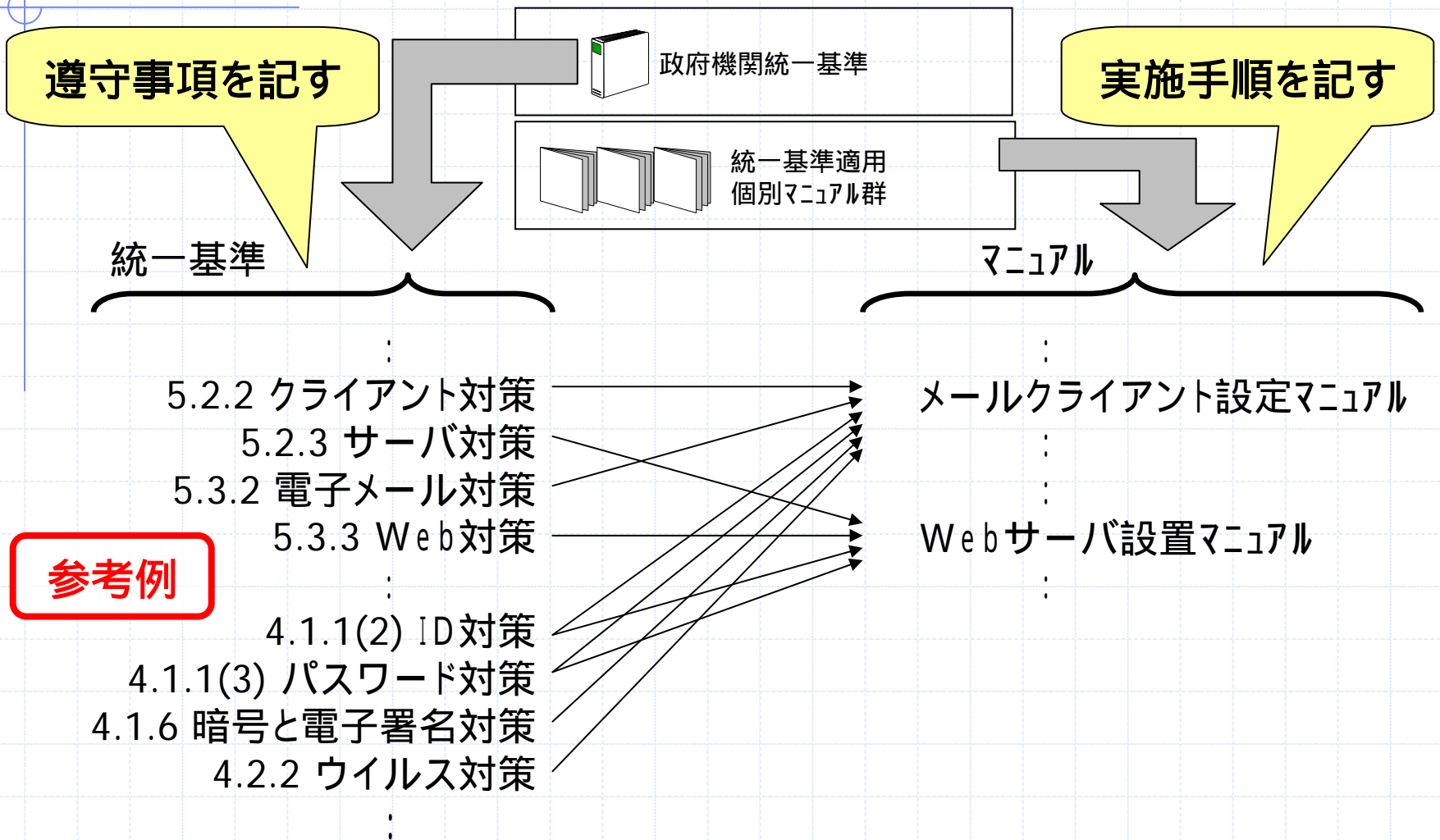
政府機関統一基準
NISD-K303-052

- 第1部 総則
- 第2部 組織と体制の構築
- 第3部 情報についての対策
- 第4部 セキュリティ要件の明確化に基づく対策
- 第5部 情報システムの構成要素についての対策
- 第6部 個別事項についての対策

政府機関統一基準と 個別マニュアルの関係



政府機関統一基準と個別マニュアルの関係



第1部 総則

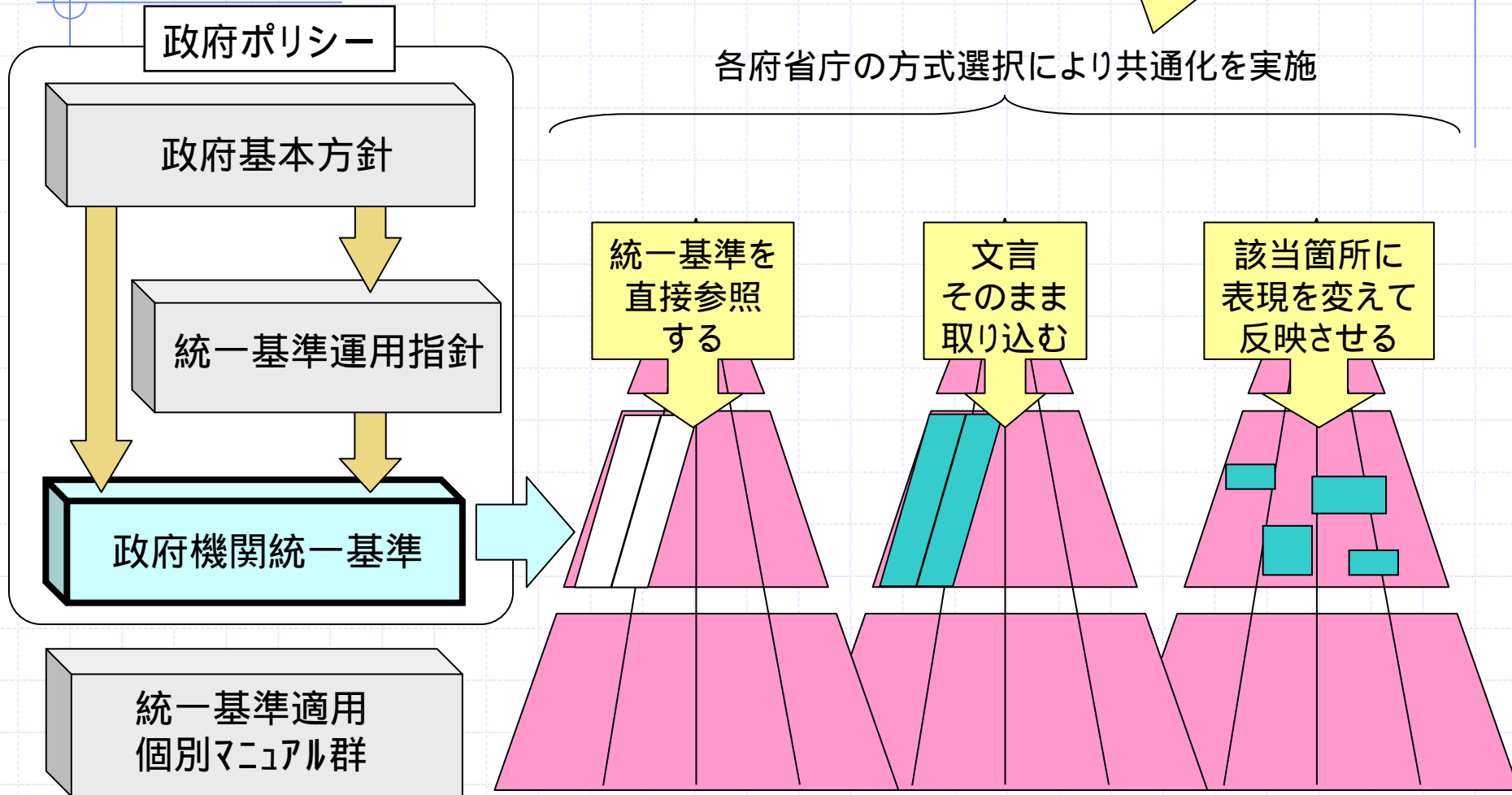
1.1.2 本統一基準の使い方

(1) 統一基準と省庁対策基準との関係

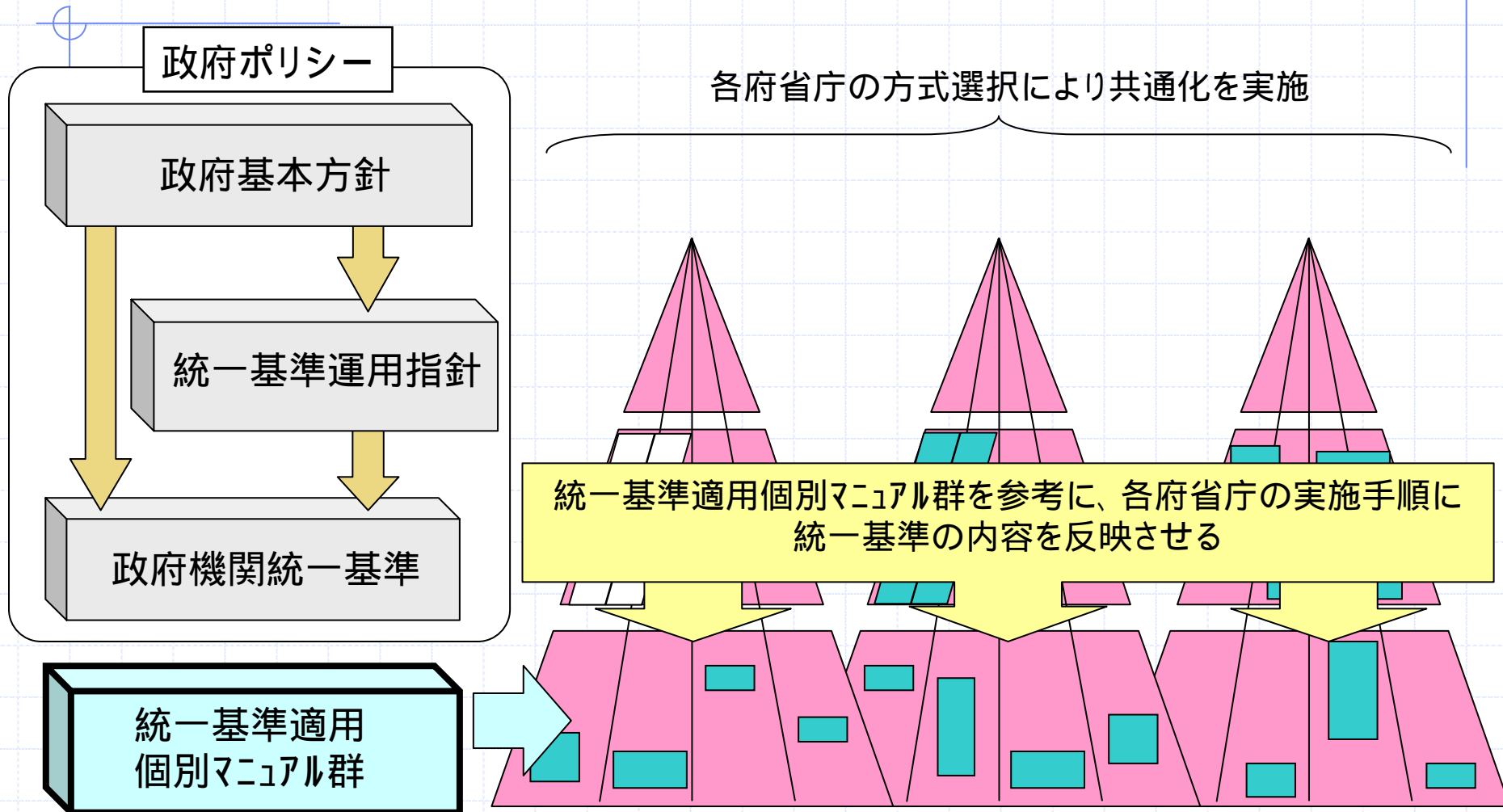
以後のスライドにて説明

政府機関統一基準 各府省庁基準への反映

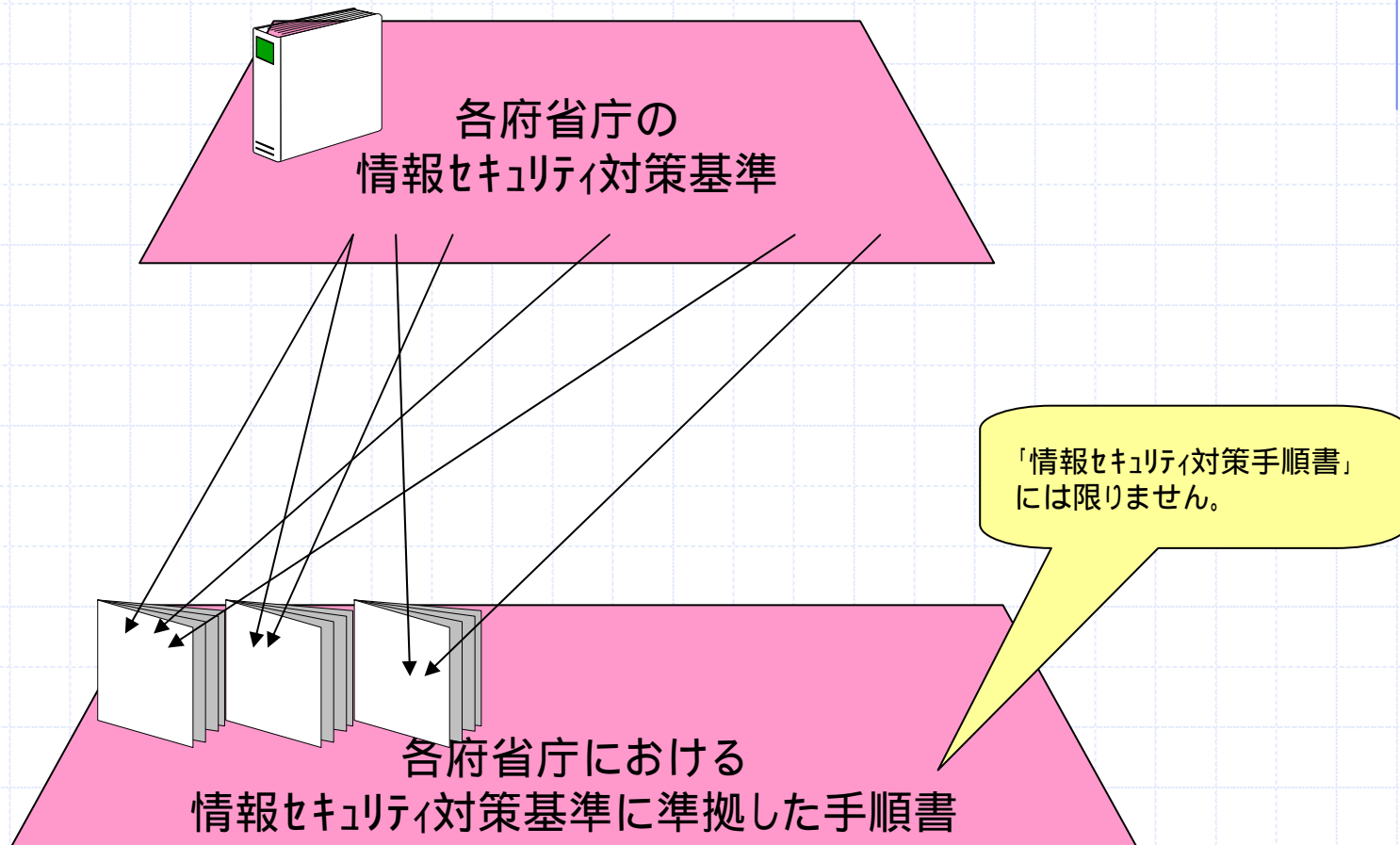
「統一化」というより「共通化」



政府機関統一基準 各府省庁実施手順への反映

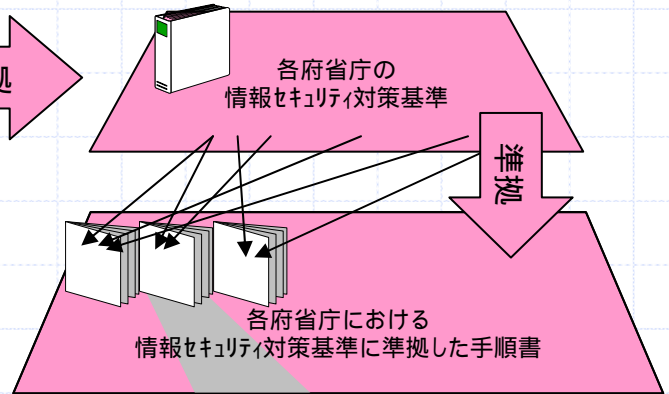
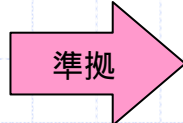


各府省庁における情報セキュリティ 対策基準とそれに準拠した手順書



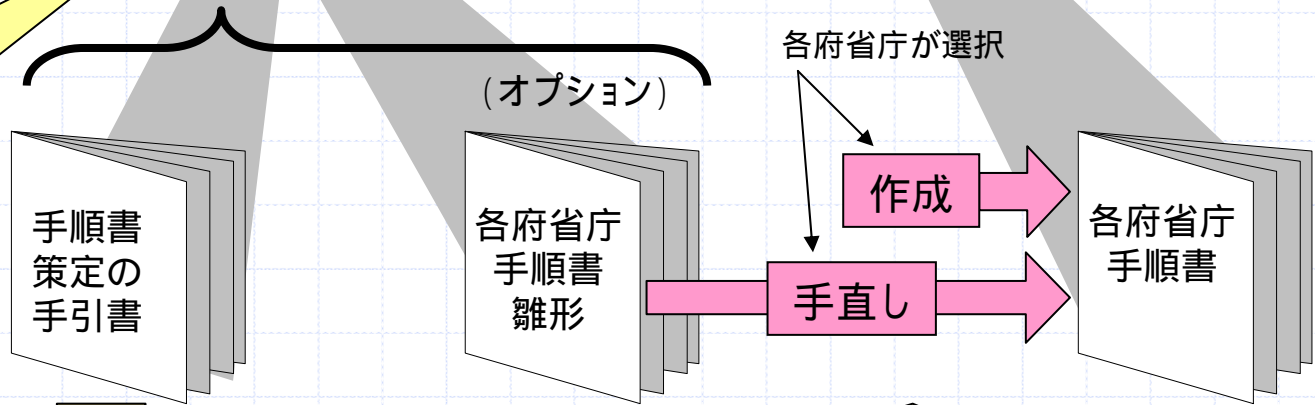
統一基準適用個別マニュアル群

政府機関統一基準



統一基準適用
個別マニュアル群

NISCは、「作成及び手直し手引書」及び「雛形」を整備する。

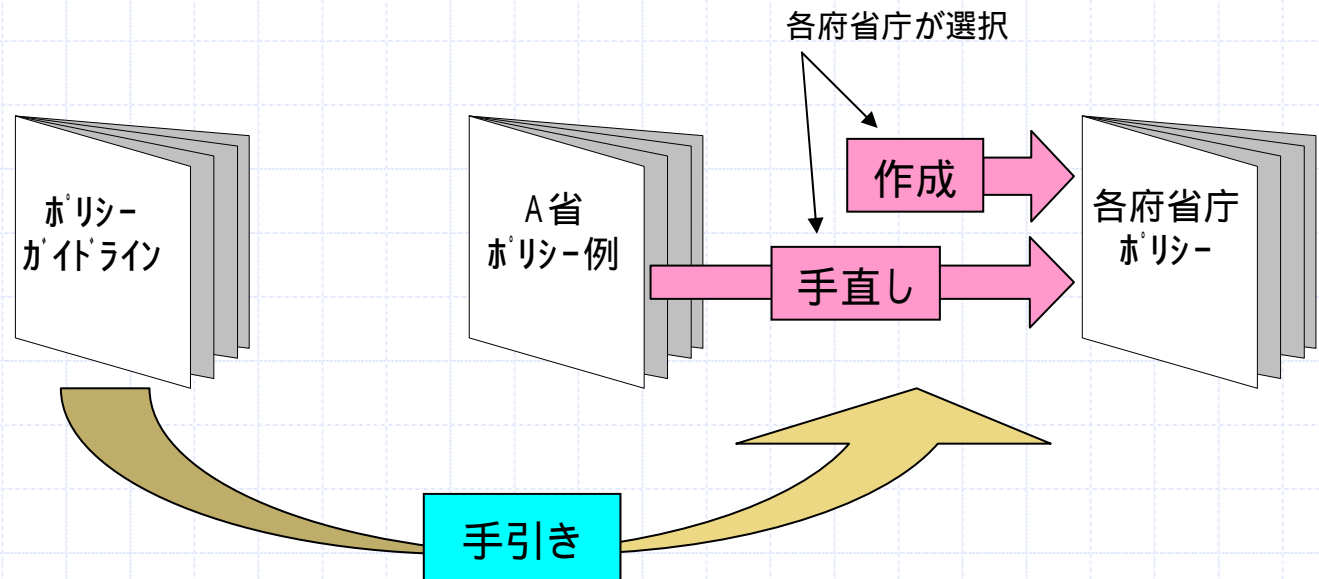


作成及び手直し
手引き



(参考)

情報セキュリティポリシーに関するガイドライン



第1部 総則

1.1.2 本統一基準の使い方

(2) 適用対象範囲

(a) 情報

以後のスライドにて説明

(b) 行政事務従事者

『(b)本統一基準は、行政事務従事者のうち、情報及び情報システムを取り扱う者に適用される。なお、本統一基準中、特に断りがないものを除き、「行政事務従事者」とは、**情報及び情報システムを取り扱う行政事務従事者**をいう。』

(c) 府省庁

以後のスライドにて説明

政府機関統一基準 の適用対象範囲

適用対象範囲：

情報システムに格納されている情報

情報システムに関係がある以下の情報

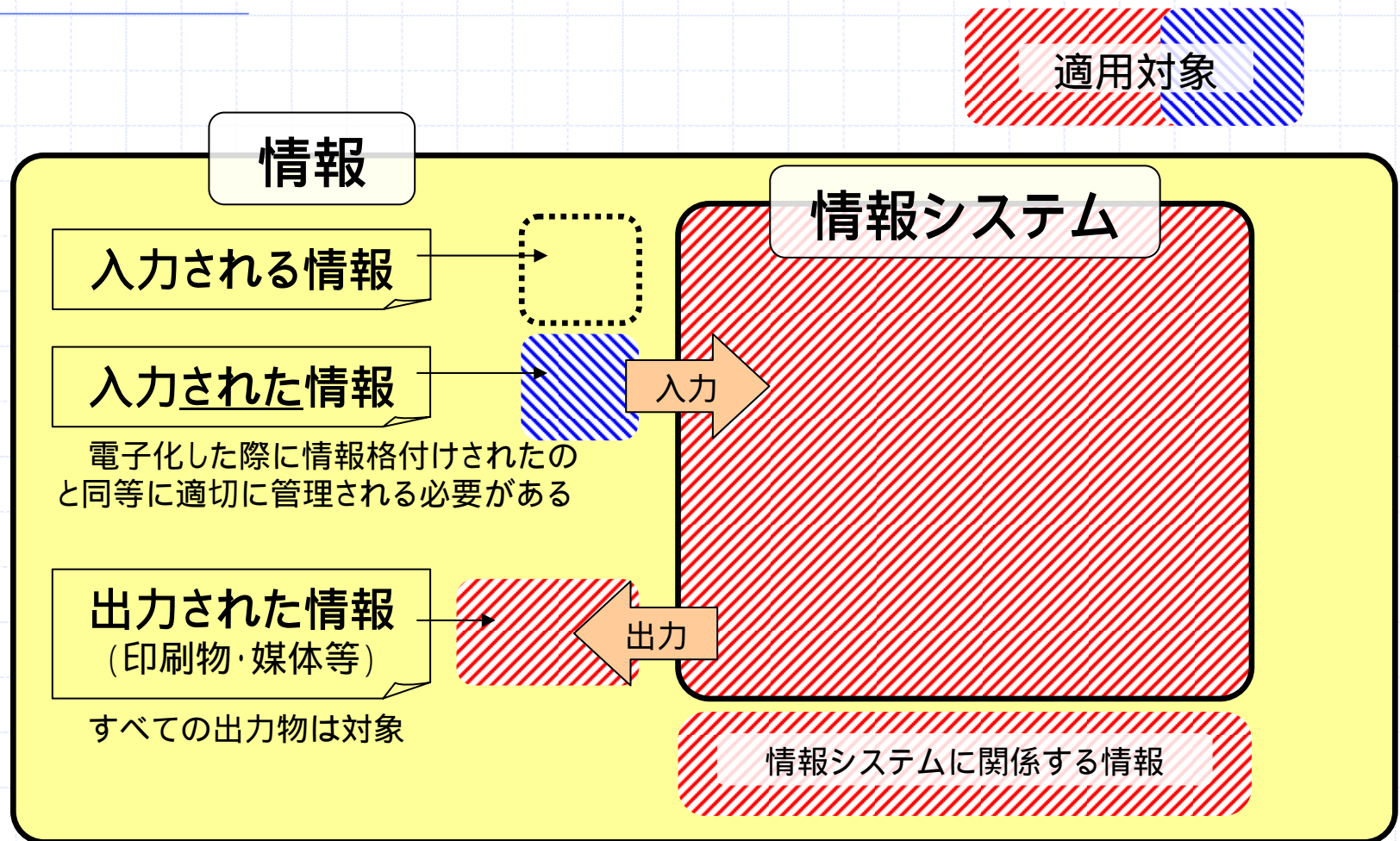
紙に記載された情報

情報システム外部の電磁的記録媒体に記録された情報

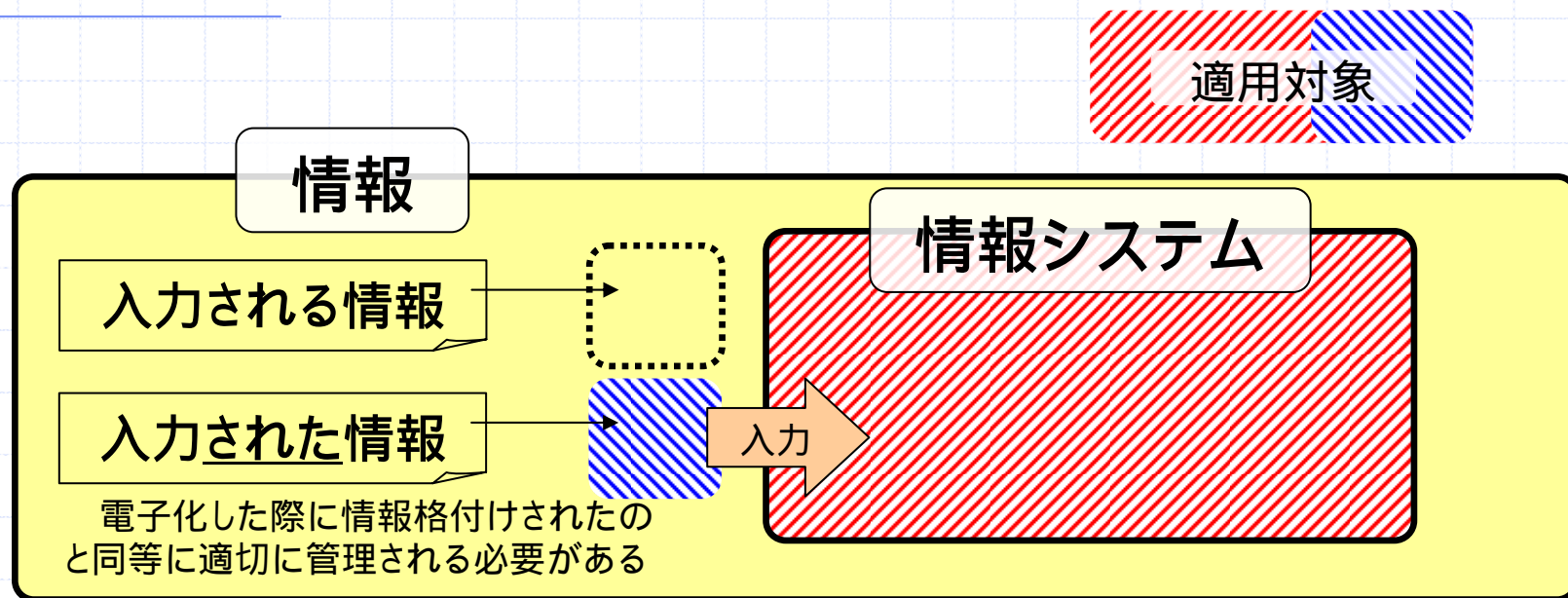
「情報」、「情報システム」及び「これらを取り扱う者」の相互関係を明確にし、守るべきものは「情報」という視点から全体を構成する。なお、この「情報」には、情報システムに関係がある限り、紙に記載された情報や情報システム外部の電磁的記録媒体に記録された情報を含めるものとする。

「各府省庁の情報システム及びその運用に関する安全基準の策定に係る基本方針について」
平成16年7月26日情報セキュリティ対策推進会議幹事会 より

政府機関統一基準 の適用対象範囲



政府機関統一基準 の適用対象範囲



情報システムに入力されるまでの情報は、すべて対象外。
情報システムに入力され、それが情報格付けされた時点をもって、その情報は、情報セキュリティ対策基準の定めと同等の安全管理措置が講じられる必要がある。
紙などの非電子の情報については、本統一基準とは別途の規程等により、適切に管理される必要があるが、それについては、本基準の定めるところではない。
情報システムに入力するまで安全管理措置が講じられていなかった情報が、入力の際の格付けによって管理が必要になる場合、それは本基準が追加の管理要件を求めているのではなく、本来必要であったことが、本基準により明確になっただけだと考えられる。

政府機関統一基準 の適用対象範囲

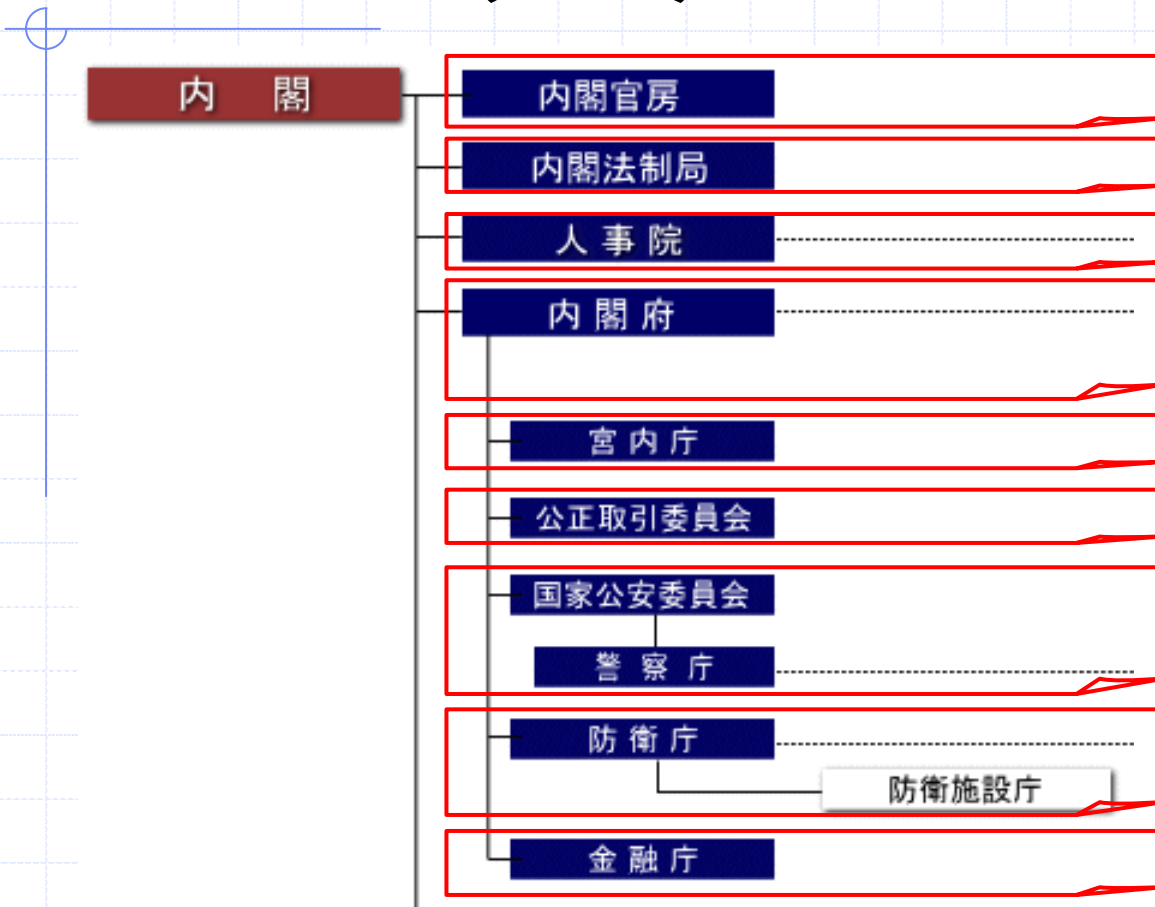
本統一基準だけで、すべての情報セキュリティ対策を網羅する
のではない。

国家公務員倫理規程による
守秘義務の適用範囲

各府省庁の定める
情報セキュリティ対策基準の範囲

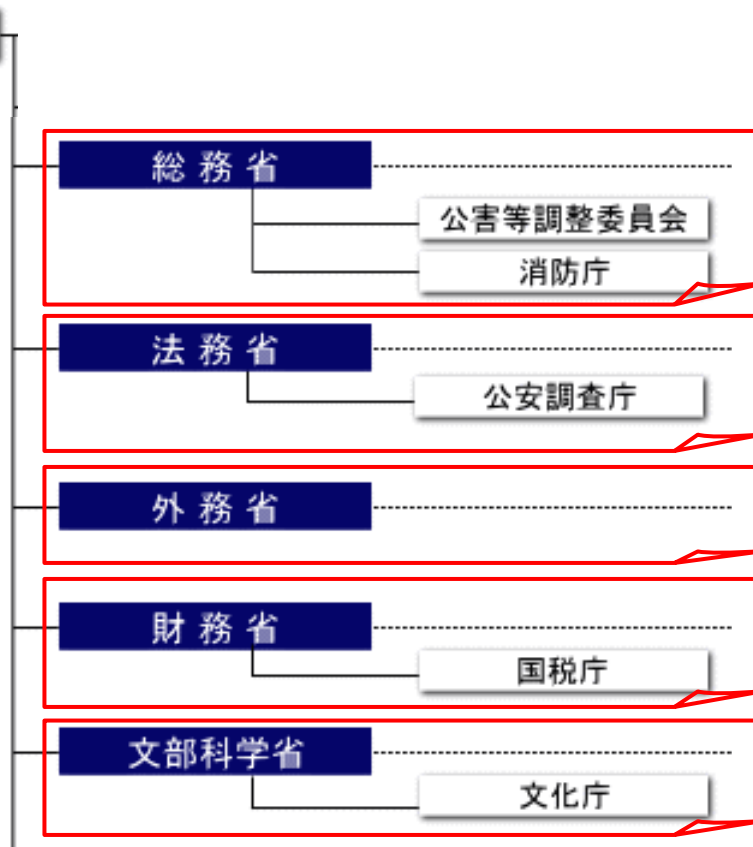
政府機関統一基準の適用範囲

府省庁 (1/3)



府省庁 (2/3)

内閣



省に付属する庁等を情報セキュリティポリシーおよび対策基準で、どのように包含あるいは従属させるかは、各省の判断によるが、その関係を明確にしておかなければならない。

府省庁 (3/3)

内閣



省に付属する庁等を情報セキュリティポリシーおよび対策基準で、どのように包含あるいは従属させるかは、各省の判断によるが、その関係を明確にしておかなければならない。

第1部 総則

1.1.2 本統一基準の使い方

(3) 全体構成 『部、節及び項の3つの階層によって構成される。』

第 X 部

X.Y 節

X.Y.Z 項

趣旨(必要性)

~~ 趣旨説明文 ~~

遵守事項

(1)

(a) ~~ 遵守事項本文 ~~

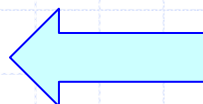
解説: ~~ (a) の解説文 ~~

(b) ~~ 遵守事項本文 ~~

解説: ~~ (b) の解説文 ~~

(2)

解説文は
「統一基準解説書」
にだけ記載



政府機関統一基準の全体構成

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策
第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

主たる対象者

統括

全従事者

情報システム
関係者

(各事項による)

政府機関統一基準の全体構成

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策
第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

概ねの頻度

年次

日常業務

情報システムの
ライフサイクル
毎・段階毎

(各事項による)

第1部 総則

1.1.2 本統一基準の使い方

(4) 対策項目の記載事項

統一基準に記載のとおりです。

(5) 対策レベルの設定

『(a)「**基本遵守事項**」は、保護すべき情報とこれを取り扱う情報システムにおいて、**必須として実施**すべき対策事項』

『(b)「**強化遵守事項**」は、特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、**必要と認められるときに選択して実施**すべき対策事項』

(6) 評価の方法

統一基準に記載のとおりです。

第1部 総則

1.1.3 用語定義

統一基準に記載のとおりです。

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第2部の構成

第2部 組織と体制の構築

2.1 導入

2.1.1 組織・体制の確立

2.1.2 役割の分離

2.1.3 違反と例外措置

2.2 運用

2.2.1 情報セキュリティ対策の教育

2.2.2 障害等の対応

2.3 評価

2.3.1 情報セキュリティ対策の自己点検

2.3.2 情報セキュリティ対策の監査

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

第2部 組織と体制の構築

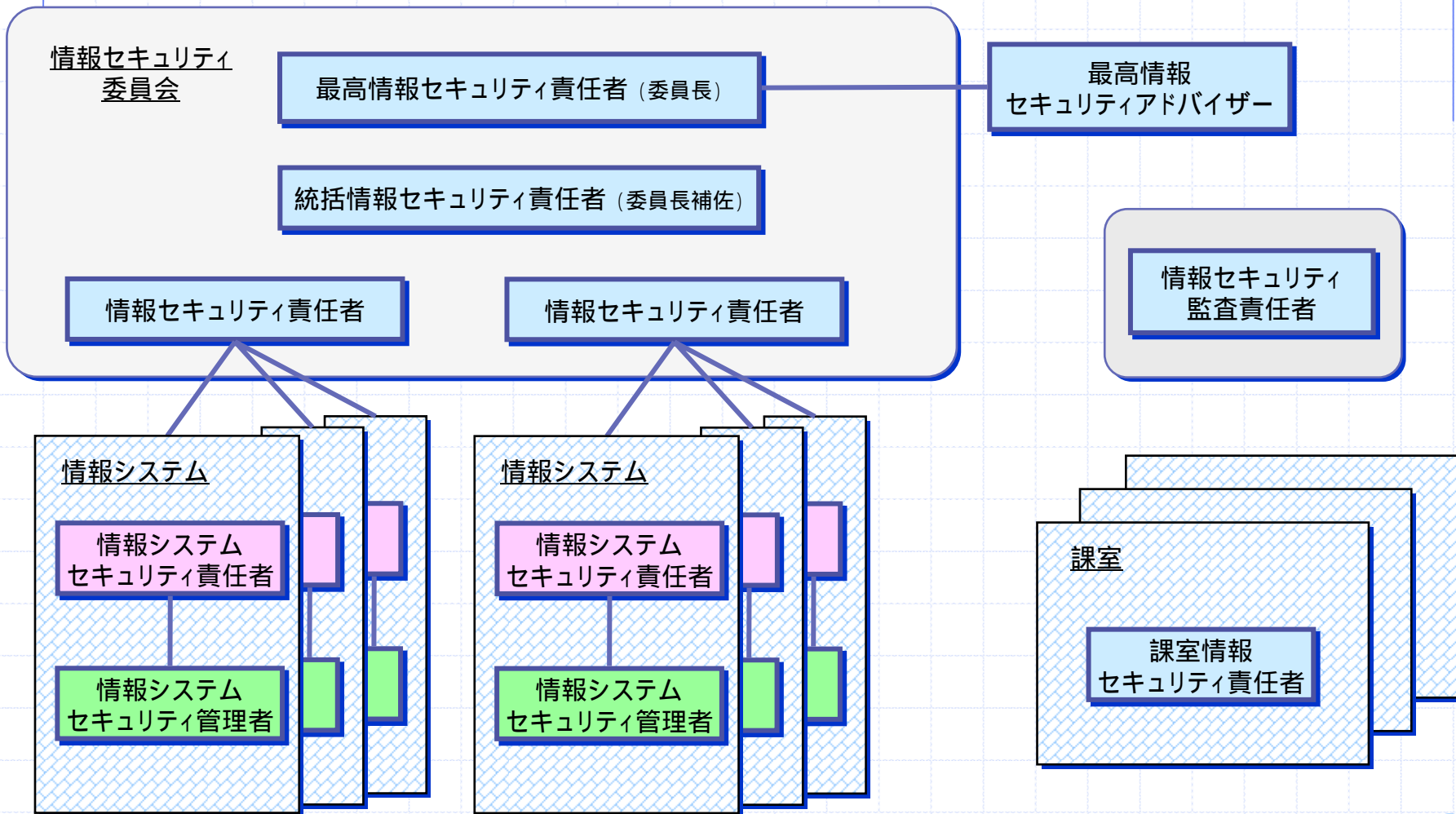
2.1 導入

2.1.1 組織・体制の確立

次スライドにて説明

統一基準解説資料 別添資料

A.1.1 組織・体制イメージ図



第2部 組織と体制の構築

2.1 導入

2.1.2 役割の分離

- 『
- (a) 情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。
 - (ア) 承認又は許可事案の申請者とその承認者又は許可者
 - (イ) 監査を受ける者とその監査を実施する者

概説：承認又は許可する役割の者自らが、申請をする場合には、その申請について自らが承認又は許可することはできない。その場合には、同じ承認又は許可をする役割を担う他者に申請し、承認又は許可を得る必要がある。

』

第2部 組織と体制の構築

2.1 導入

2.1.3 違反と例外措置

『

趣旨

政府において情報セキュリティを継続的に維持するためには、万一違反があった場合に、定められた手続きに従って、適切に対応する必要がある。

また、情報セキュリティ関係規程の適用が行政事務の適正な遂行を著しく妨げる等、情報セキュリティ関係規程の規定とは異なる代替の方法を採用し、又は規定を実施しないことを認めざるを得ない場合についても、あらかじめ定められた例外措置のための手続きにより、情報セキュリティを維持しつつ柔軟に対応できるものでなければ、当該規程の実効性を確保することが困難となる。

』

第2部 組織と体制の構築

2.1 導入

2.1.3 違反と例外措置

(1) 違反への対応

統一基準に記載のとおりです。

(2) 例外措置

統一基準を参照しながら説明

第2部 組織と体制の構築

2.1 導入

2.1.3 違反と例外措置

(2) 例外措置

- 『(f) 最高情報セキュリティ責任者は、**例外措置の適用審査記録の台帳を整備**し、例外措置の適用審査記録の参照について、情報セキュリティ監査を実施する者からの求めに応ずること。』

府省庁における、すべての例外措置について、随時回答できる状態にしておく必要があります。

第2部 組織と体制の構築

2.2 運用

2.2.1 情報セキュリティ対策の教育

啓発<教育<訓練

毎年度最低1回 & 着任時3ヶ月以内の受講
人は現在の自分の立場で理解するため、同じ内容であっても受講済み教育の再受講が効果的である。

受講状況の管理

未受講者への受講勧告

受講状況の組織としての把握

受講義務の明示(本人の責任)

受講支援(上司の義務)

基本的な遵守事項を実践することも大切

第2部 組織と体制の構築

2.2 運用

2.2.2 事故及び障害の対応

事前準備 = 体制、報告手順、対応手順、緊急連絡網の整備

(強化事項: 府省庁外からの通報も想定)

事前準備に基づく、計画内対応と**計画外対応**

One stop & **Non-stop**

= 窓口設置 & **無期限待機防止**

原因調査、再発防止策立案と**実施支援**

準備した内容を**周知**することは大切

第2部 組織と体制の構築

2.3 評価

2.3.1 情報セキュリティ対策の自己点検

2.3.2 情報セキュリティの監査

後で詳しく説明します。

第2部 組織と体制の構築

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

- 『 (a) 情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認められた場合にはその見直しを行うこと。』
- 『 (b) 行政事務従事者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行うこと。』

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第3部の構成

第3部 情報についての対策

3.1 情報の格付け

3.1.1 情報の格付け

3.2 情報の取扱い

3.2.1 情報の作成と入手

3.2.2 情報の利用

3.2.3 情報の保存

3.2.4 情報の移送

3.2.5 情報の提供

3.2.6 情報の消去

情報のライフサイクル

第3部 情報についての対策

3.1.1 情報の格付け

- 『
- (a) 情報セキュリティ委員会は、行政事務で取り扱う情報について、機密性、完全性及び可用性の観点による当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること。
- 』

「重要度」のような単一観点ではなく、三つの観点を区別して対策を講じる。

機密性、完全性、可用性の3つの観点

「格付け」の基準

「取扱制限」の基準

「格付け」及び「取扱制限」を明示する手順

← 次のスライドで紹介

← 3.2.1 で紹介

すべての行政事務従事者は、各府省庁の定めた、これらの「基準」と「手順」により「格付け」と「明示」をしなければならない。

「格付け」と「取扱制限」 (Classification と Marking)

格付け	分類基準	取扱制限

政府共通の指定

必須の指定

段階的な指定

格付けによって、本統一基準に含まれる遵守事項が選択されて対策内容が定まる。

各府省庁個別の指定

任意の指定

無段階の指定

取扱制限の指定によって、各府省庁が定める「取扱制限」基準により対策内容が決まる。

「格付け及び取扱制限」を指定するための判断を

誰が 指定判断者 (統一基準において指定実施者は情報の作成・入手者)

どのように 判断基準、方法

実施するののかについてを、

各府省庁が「格付け及び取扱制限の基準」に含めて定める。

統一基準解説資料 別添資料

A.1.2 情報の格付け一覧 (1 / 3)

機密性による情報の格付け

格付け	分類基準	取扱制限
機密性3情報	秘密文書に相当する機密性を要する情報	例) 複製禁止 再配付禁止 暗号化必須
機密性2情報	秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としない情報	
機密性1情報	機密性2情報又は機密性3情報以外の情報	

統一基準解説資料 別添資料

A.1.2 情報の格付け一覧 (2 / 3)

完全性による情報の格付け

格付け	分類基準	取扱制限
完全性2情報	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	例) 年 月 日まで保存
完全性1情報	完全性2情報以外の情報	

統一基準解説資料 別添資料

A.1.2 情報の格付け一覧 (3 / 3)

可用性による情報の格付け

格付け	分類基準	取扱制限
可用性2情報	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	例) 1時間以内復旧
可用性1情報	可用性2情報以外の情報	

第3部 情報についての対策

3.1.1 情報の格付け

1.1.3 用語定義より

『

- ・ 「要機密情報」とは、機密性2情報及び機密性3情報をいう。
- ・ 「要保全情報」とは、完全性2情報をいう。
- ・ 「要安定情報」とは、可用性2情報をいう。
- ・ 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。

』

→ 要機密情報、要保全情報、要安定情報のいずれか。

第3部 情報についての対策

3.2.1 情報の作成と入手

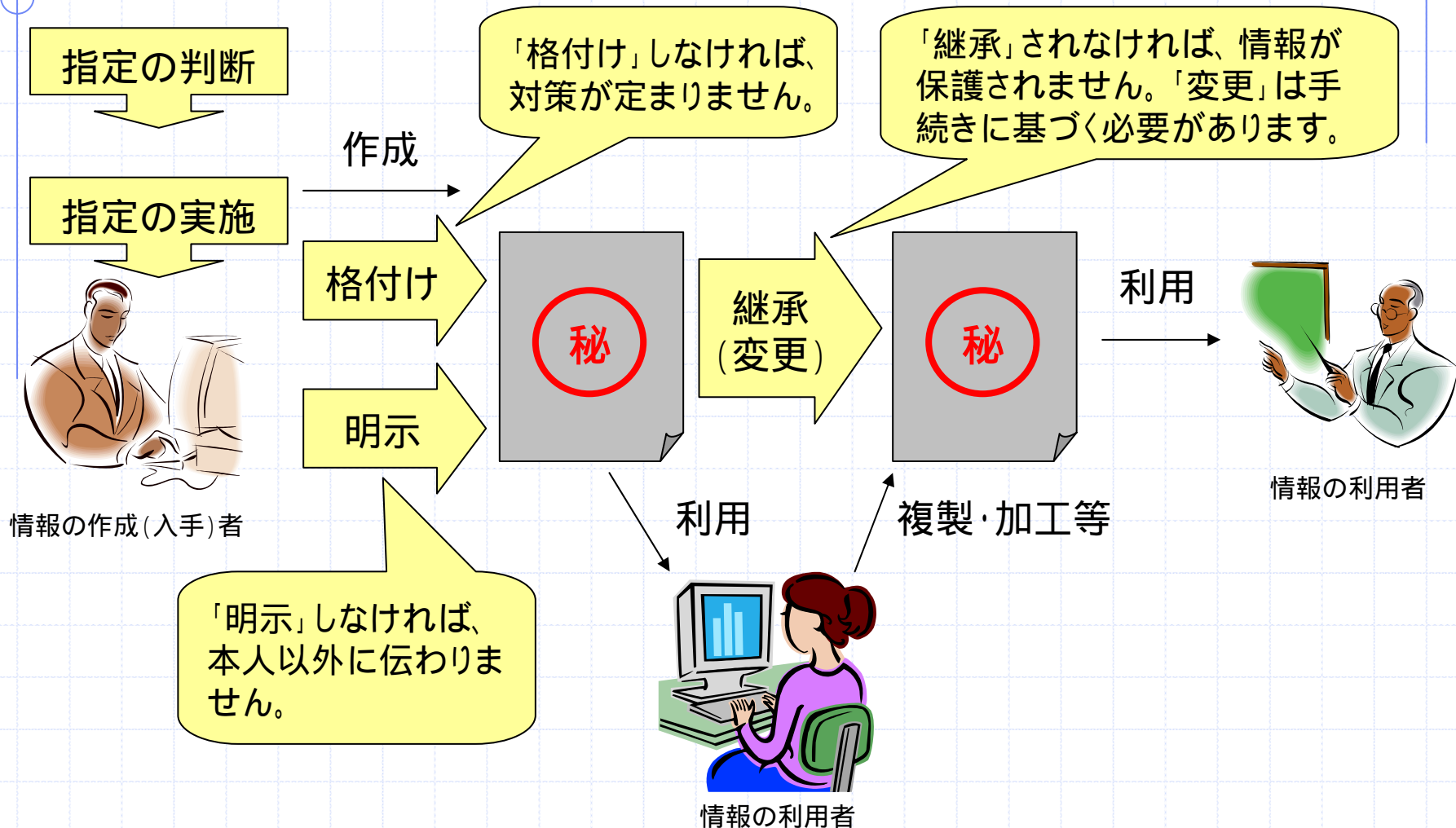
- (1) 業務以外の情報の作成又は入手の禁止
- (2) 情報の作成又は入手時における格付けの決定と取扱制限の検討

必ず格付けを実施

必要性を必ず検討し、必要に応じて取扱制限を指定

- (3) 格付けと取扱制限の明示
- (4) 格付けと取扱制限の継承
- (5) 格付けと取扱制限の変更

情報の格付け(及び取扱制限)



第3部 情報についての対策

3.2.1 情報の作成と入手

3.2.1 (3)格付けと取扱制限の明示

1.1.3 用語定義より

『「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。』

第3部 情報についての対策

3.2.2 情報の利用

(1) 業務以外の利用の禁止

(2) 格付け及び取扱制限に従った情報の取扱い

(3) **要保護情報**の取扱い

【基本遵守事項】

- (a) 持ち出し禁止
- (b) 放置禁止
- (c) 複製制限
- (d) 再配布制限

【強化遵守事項】

- (e) 機密性3情報の格付け期間の明記
- (f) 機密性3情報の連番採番と記録

第3部 情報についての対策

3.2.3 情報の保存

(1) 格付けに応じた情報の保存

【基本遵守事項】

- (a) アクセス制御
- (b) 外部記録媒体の管理
- (c) 入出力書面の管理
- (d) 暗号化
- (e) 電子署名
- (f) バックアップ
- (g) バックアップ

(2) 情報の保存期間

【基本遵守事項】

- (a) 保存と消去

第3部 情報についての対策

3.2.4 情報の移送

(1) 情報の移送に関する許可及び届出

- (a) **機密性3**情報 **許可**を得る
- (b) **機密性2**情報 **届け出**る

(2) 情報の送信と運搬の選択

- (a) **送信と運搬**の選択

移送 = 送信 | 運搬

(3) 移送手段の選択

- (a) 移送(送信又は運搬) **手段**の選択

(4) 書面に記載された情報の保護対策

(5) 電磁的記録媒体に記録された情報の保護対策

- 【基本】(a-b) パスワード設定の必要性、暗号化の必要性
- 【強化】(c) 暗号化 + 情報分割 + 複数経路

第3部 情報についての対策

3.2.5 情報の提供

(1) 情報の公表

【基本遵守事項】

- (a) 機密性1 情報であることを確認
- (b) 付加情報の考慮

(2) 他者への情報の提供

【基本遵守事項】

- (a) 機密性3 情報 許可を得る
- (b) 機密性2 情報 届け出る
- (c) 提供先における適切な取り扱い措置
- (d) 付加情報の考慮

第3部 情報についての対策

3.2.6 情報の消去

(1) 電磁的記録の消去方法

【基本遵守事項】

- (a) 廃棄する時 復元が困難な状態にする
- (b) 再利用する時 復元が困難な状態にする

【強化遵守事項】

- (c) 廃棄に限らず 要機密情報を復元困難な状態にする

(2) 書面の廃棄方法

【基本遵守事項】

- (a) 廃棄する時 復元できない方法を用いる

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第4部の構成

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.1 主体認証機能

4.1.2 アクセス制御機能

4.1.3 権限管理機能

4.1.4 証跡管理機能

4.1.5 保証のための機能

4.1.6 暗号と電子署名(鍵管理を含む)

4.2 情報セキュリティについての脅威

4.2.1 セキュリティホール対策

4.2.2 不正プログラム対策

4.2.3 サービス不能攻撃対策

4.3 情報システムのセキュリティ要件

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

遵守事項の構成

情報セキュリティについての機能

- (a) を行う必要性の有無を
検討すること。
- (b) 必要性があると
認めた情報システムには、
を行う機能を設けること。
- (c) 必要性があると
認めた情報システムには、
をすること。
- (d) ……

(a) で必要性があると判断された情報システムに対して、(b) 以後の遵守事項を適用する。

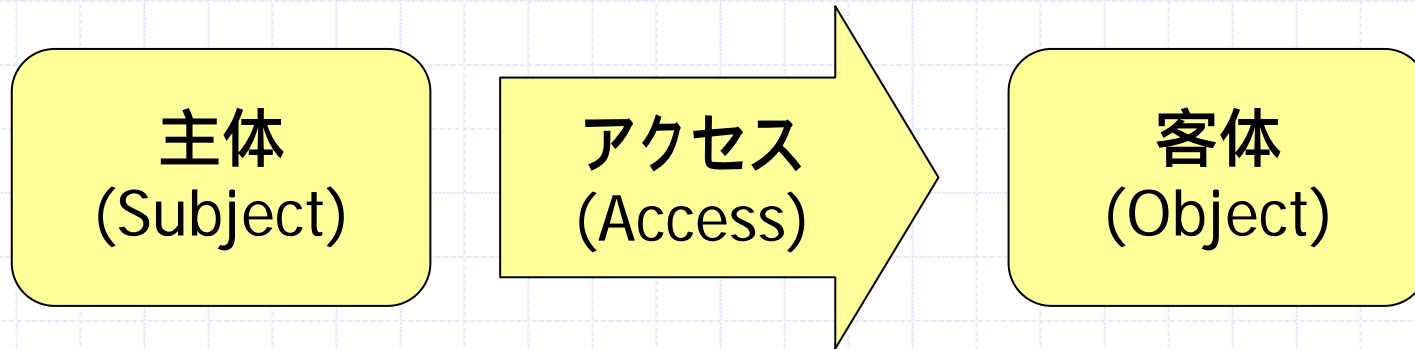
K303-052

1.1.3 用語定義 より

- ・「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。
- ・「識別」とは、情報システムにアクセスする主体を特定することをいう。
- ・「識別コード」とは、識別するために、情報システムが認識するコード(符号)をいう。代表的な識別コードとして、ユーザIDが挙げられる。
- ・「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本統一基準における「主体認証」については、公的又は第三者による証明に限るものではない。
- ・「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
- ・「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。

4.1 に出てくる用語解説： 主体 (Subject) と客体 (Object)

主体 が 客体 に アクセス する。

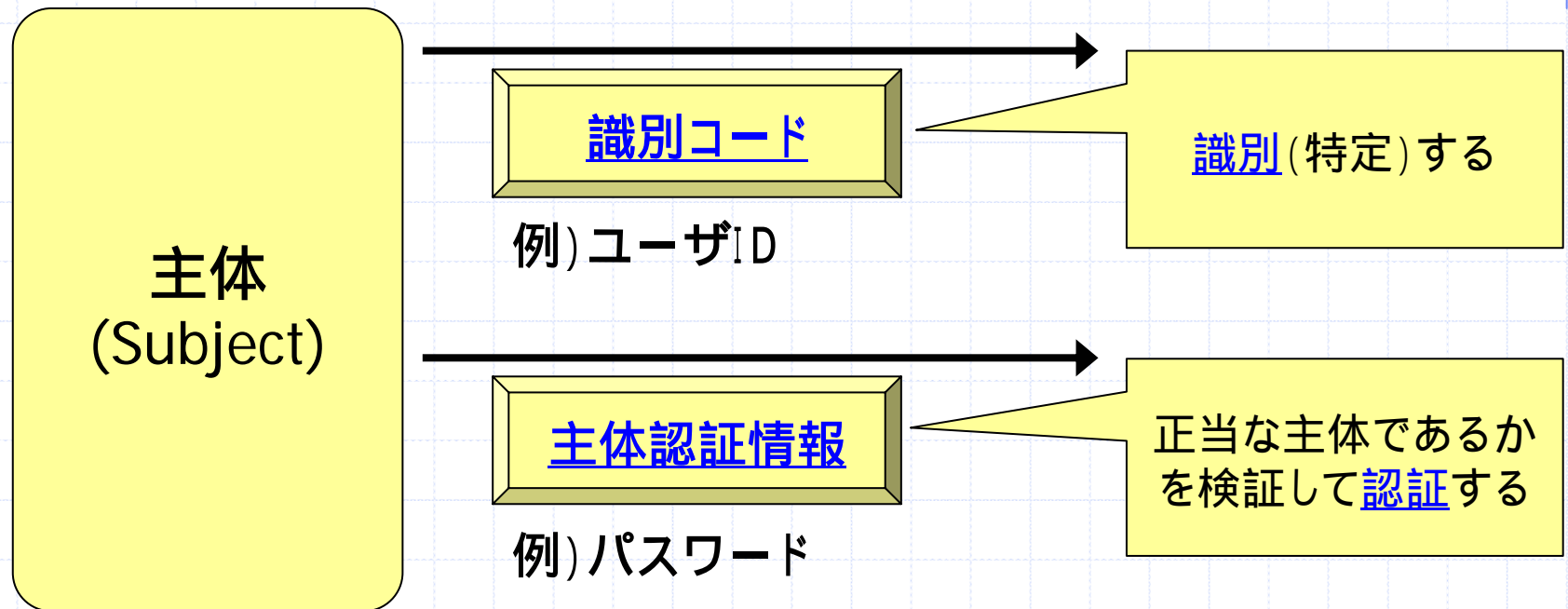


例) 人が情報にアクセスする。
プログラムがデータにアクセスする。
人がプログラムにアクセスする。

アクセスするものが「主体」、アクセスされるものが「客体」

4.1 に出てくる用語解説： 主体(Subject) と 認証(Authentication)

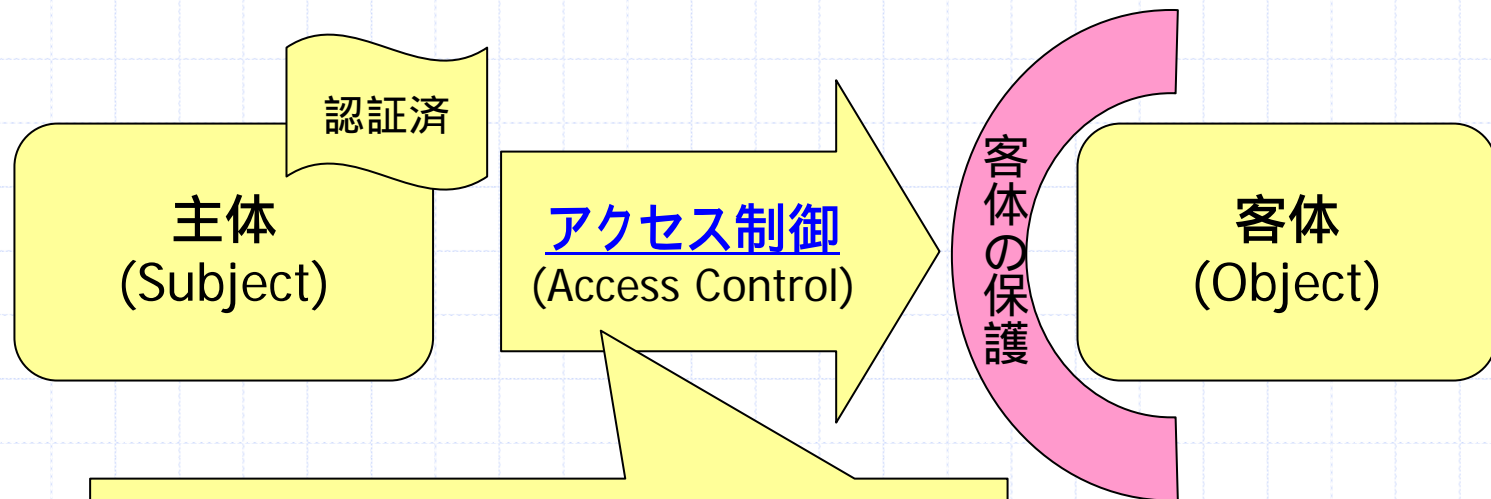
主体 を 認証(Authenticate) する。



本統一基準における「主体認証」は、第三者による認証に限らない。
(第三者を伴わない認証も含める。) 用語説明を参照

4.1 に出てくる用語解説： アクセス制御(Access Control)

主体から客体への アクセス制御 をする。



主体が客体へのアクセスをしようとしたときに、それが許可されたものであるかを確認して、そのアクセスを制御する。

認証なしで、アクセス制御することもできます。
例) アクセスのためのパスワードだけを設定する場合など。
誰が？いつ？どこから？どうやって？ 何にアクセスするか。

K303-052

1.1.3 用語定義 より

- ・「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、1つの識別コードは1つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況などを考慮して、1つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードとをいう。
- ・「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、磁気テープカードやICカード等がある。
- ・「複数要素(複合)主体認証(multiple factors authentication / composite authentication)方式」とは、知識、所有、生体情報などのうち、複数の方法の組み合わせにより主体認証を行う方法である。
- ・「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。
- ・「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

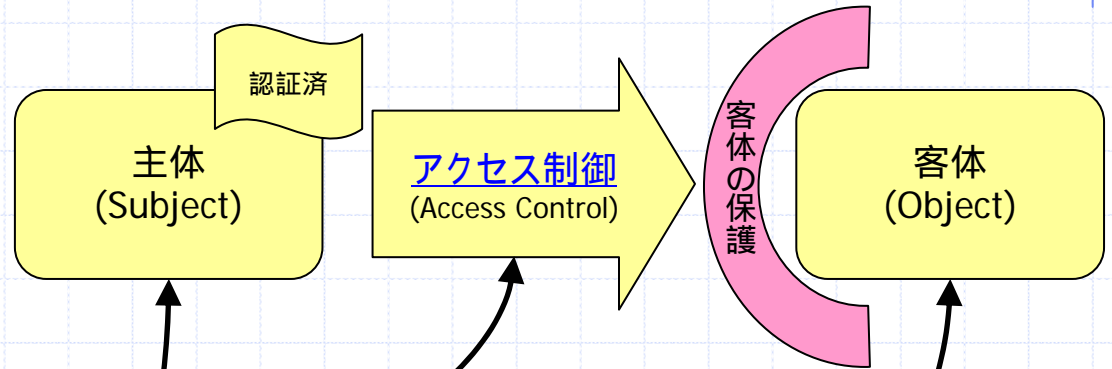
4.1.5 保証

4.1.4 証跡管理
(Auditing)

4.1.3 権限管理
(Administration)

4.1.2 アクセス制御
(Access Control)

4.1.1 主体認証
(Authentication)



K303-052

1.1.3 用語定義 より

『

- ・「**権限管理**」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
- ・「**付与**」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。

』

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.5 保証

4.1.4 証跡管理
(Auditing)

4.1.3 権限管理
(Administration)

4.1.2 アクセス制御
(Access Control)

4.1.1 主体認証
(Authentication)

管理



第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

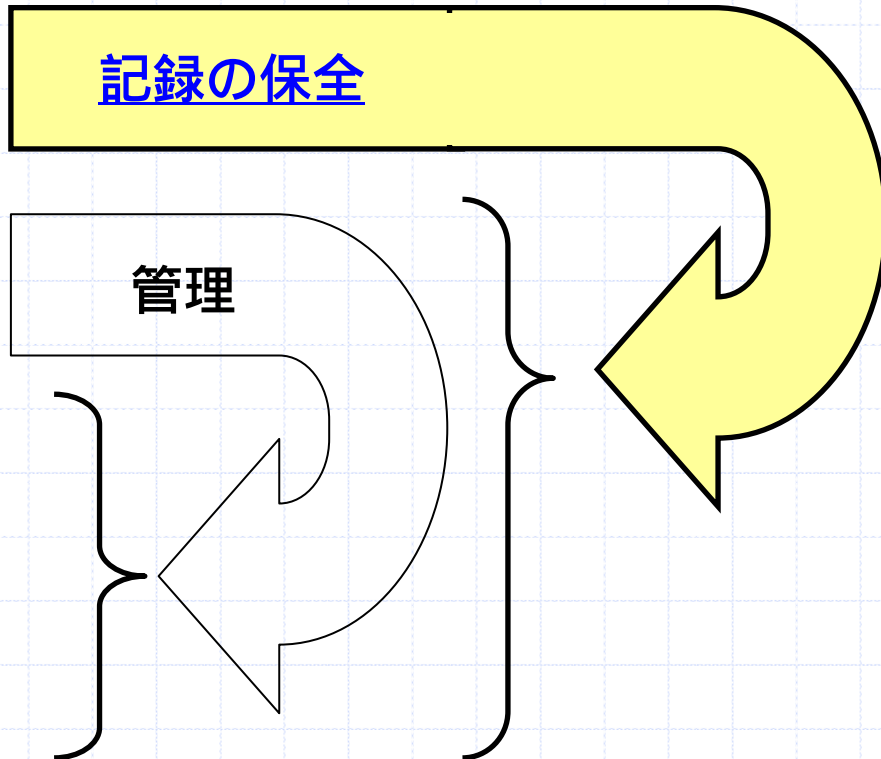
4.1.5 保証

4.1.4 証跡管理
(Auditing)

4.1.3 権限管理
(Administration)

4.1.2 アクセス制御
(Access Control)

4.1.1 主体認証
(Authentication)



K303-052

1.1.3 用語定義 より

次のスライドを参照

- ・「強制アクセス制御 (MAC: Mandatory Access Control)」とは、主体が客体に設定したアクセス制御について、その設定の継承を情報システムが強制的に行う方式をいう。強制アクセス制御の機能を備えた情報システムでは、主体が客体を保護すべき対象とした場合には、アクセスを許可された者であっても、それを保護すべき対象ではないものとすることはできない。すなわち、主体が設定したアクセス制御の継承は、任意ではなく強制されることになる。
- ・「最小特権機能」とは、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。

統一基準解説資料

4.1.2 アクセス制御

『

用語解説

アクセス制御方式やセキュリティに配慮したOSに関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮したOSを活用した情報システム等に関する調査研究」を参照のこと。

http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf

』

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

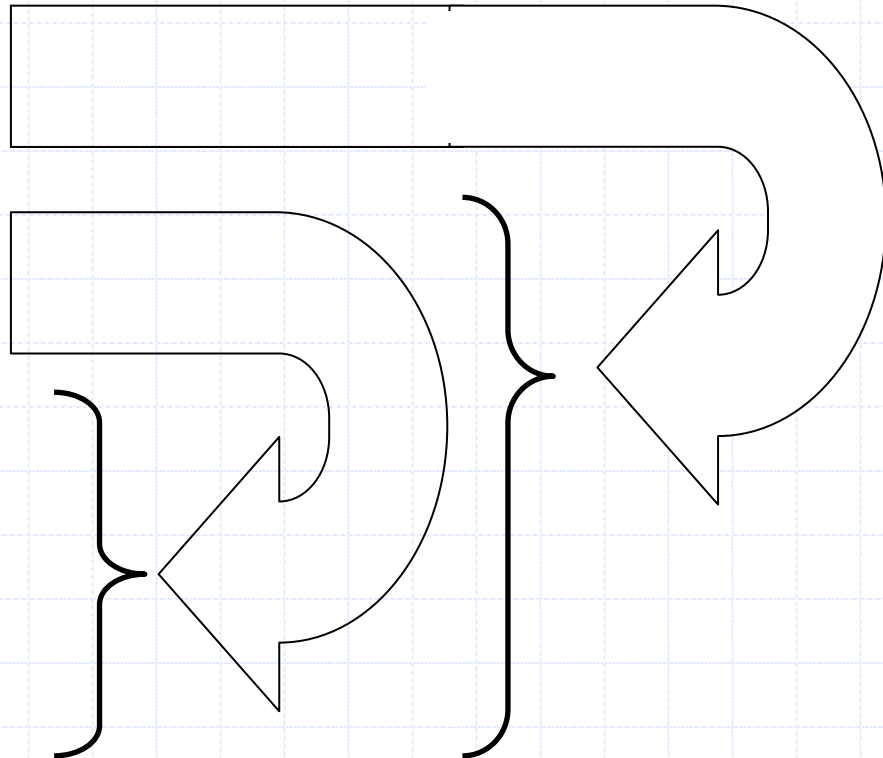
4.1.5 保証

4.1.4 証跡管理
(Auditing)

4.1.3 権限管理
(Administration)

4.1.2 アクセス制御
(Access Control)

4.1.1 主体認証
(Authentication)



第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.6 暗号と電子署名

4.1.1 ~ 4.1.5 とは独立した機能検討

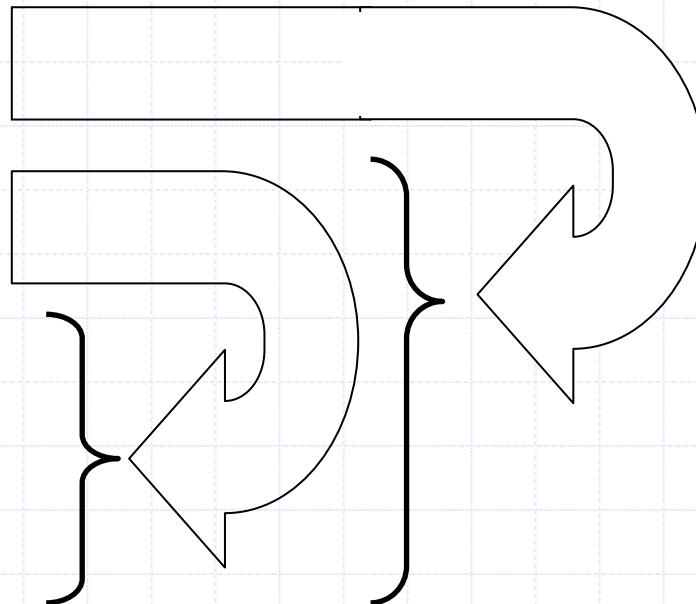
4.1.5 保証

4.1.4 証跡管理
(Auditing)

4.1.3 権限管理
(Administration)

4.1.2 アクセス制御
(Access Control)

4.1.1 主体認証
(Authentication)



統一基準 K303-052 第4部の構成

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.1 主体認証機能

4.1.2 アクセス制御機能

4.1.3 権限管理機能

4.1.4 証跡管理機能

4.1.5 保証のための機能

4.1.6 暗号と電子署名(鍵管理を含む)

4.2 情報セキュリティについての脅威

4.2.1 セキュリティホール対策

4.2.2 不正プログラム対策

4.2.3 サービス不能攻撃対策

4.3 情報システムのセキュリティ要件

第4部 情報セキュリティ要件の明確化に基づく対策

4.2 情報セキュリティについての脅威

情報システムが、各項で想定している脅威について確認し、影響を受ける場合には、その項の遵守事項を適用してください。

影響を受けるおそれが全くなければ適用不要です。

4.2.1 セキュリティホール対策

4.2.2 不正プログラム対策

ウイルス等への対策

4.2.3 サービス不能攻撃対策

想定している脅威

統一基準 K303-052 第4部の構成

第4部 情報セキュリティ要件の明確化に基づく対策

4.1 情報セキュリティについての機能

4.1.1 主体認証機能

4.1.2 アクセス制御機能

4.1.3 権限管理機能

4.1.4 証跡管理機能

4.1.5 保証のための機能

4.1.6 暗号と電子署名(鍵管理を含む)

4.2 情報セキュリティについての脅威

4.2.1 セキュリティホール対策

4.2.2 不正プログラム対策

4.2.3 サービス不能攻撃対策

4.3 情報システムのセキュリティ要件

第4部 情報セキュリティ要件の明確化に基づく対策

4.3 情報システムのセキュリティ要件

4.3.1 情報システムのセキュリティ要件

- (1) 情報システム計画・設計
- (2) 情報システムの構築・運用・監視
- (3) 情報システムの移行・廃棄
- (4) 情報システムの見直し

情報システムの
ライフサイクル

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第5部の構成

第5部 情報システムの構成要素についての対策

5.1 施設と環境

5.1.1 電子計算機及び通信回線装置を設置する安全区域

5.2 電子計算機

5.2.1 電子計算機共通対策

5.2.2 端末

5.2.3 サーバ装置

5.3 アプリケーションソフトウェア

5.3.1 通信回線を介して提供するアプリケーション共通対策

5.3.2 電子メール

5.3.3 ウェブ

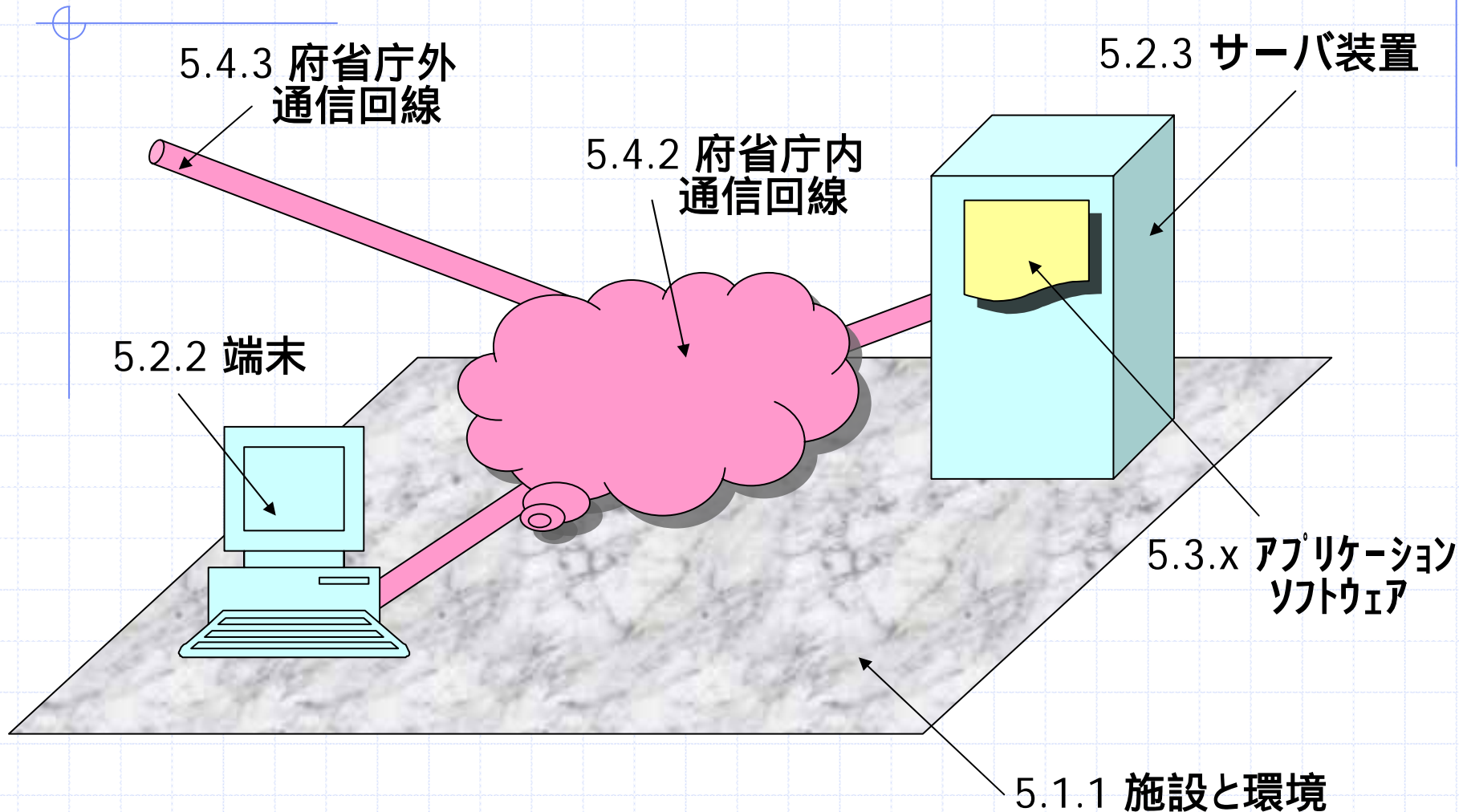
5.4 通信回線

5.4.1 通信回線共通対策

5.4.2 府省庁内通信回線の管理

5.4.3 府省庁外通信回線との接続

統一基準 K303-052 第5部の構成



第5部 情報システムの構成要素についての対策

5.1 施設と環境

5.1.1 電子計算機及び通信回線装置を設置する安全区域

- (1) 立入り及び退出の管理
- (2) 訪問者及び受渡業者の管理
- (3) 電子計算機及び通信回線のセキュリティ確保
- (4) 安全区域内のセキュリティ管理
- (5) 災害及び障害への対策

第5部 情報システムの構成要素についての対策

5.2 電子計算機

5.2.1 電子計算機共通対策

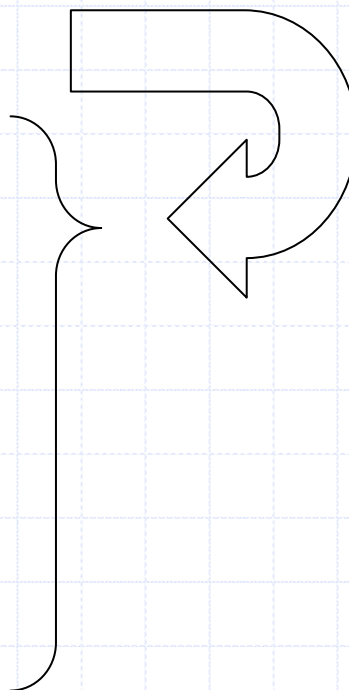
- (1) 電子計算機の設置時
- (2) 電子計算機の運用時
- (3) 電子計算機の運用終了時

5.2.2 端末

- (1) 端末の設置時
- (2) 端末の運用時

5.2.3 サーバ装置

- (1) サーバ装置の設置時
- (2) サーバ装置の運用時



第5部 情報システムの構成要素についての対策

5.3 アプリケーションソフトウェア

5.3.1 通信回線を介して提供するアプリケーション共通対策

- (1) サービスの導入時
- (2) サービスの運用時

5.3.2 電子メール

- (1) 電子メールの導入時
- (2) 電子メールの運用時

5.3.3 ウェブ

- (1) ウェブの導入時
- (2) ウェブの運用時

第5部 情報システムの構成要素についての対策

5.4 通信回線

5.4.1 通信回線共通対策

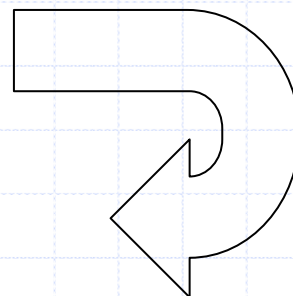
- (1) 通信回線を構築時
- (2) 通信回線を運用時
- (3) 通信回線の運用終了時

5.4.2 府省庁内通信回線の管理

- (1) 府省庁内通信回線を構築時
- (2) 府省庁内通信回線を運用時

5.4.3 府省庁外通信回線との接続

- (1) 府省庁内通信回線を府省庁外通信回線との接続時
- (2) 府省庁外通信回線と接続している府省庁内通信回線の運用時



2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

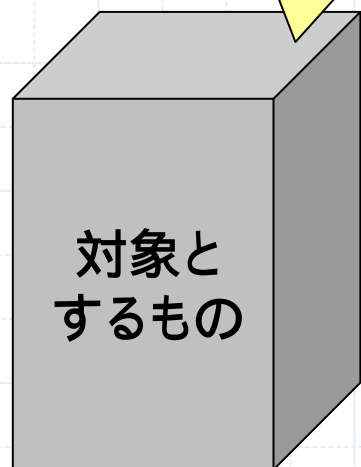
第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052

第4部 と 第5部 の関係

対象とするものごとに複数の部節にある遵守事項を適用しなければなりません。



第4部
の
遵守事項

第5部
の
遵守事項

第6部
の
遵守事項

適用しなければならない遵守事項と、適用しない遵守事項があります。

統一基準 K303-052

第4部 と 第5部 の関係

第4部 セキュリティ要件の明確化に基づく対策

セキュリティ機能の必要性及びセキュリティ脅威の影響を確認し、必要な事項を適用する。

全項目の遵守事項を確認する。

対象とするものに何が必要かによって遵守事項が決まる

情報システムのライフサイクルに応じた事項を適用する。

該当する見出し項目の遵守事項を確認する。

対象とするライフサイクルによって遵守事項が決まる

第5部 情報システムの構成要素についての対策

当該システムの種類を確認し、該当すれば適用する。

該当する見出し項目の遵守事項を確認する。

対象とするものがどんな種類かによって遵守事項が決まる

2.2

政府機関統一基準の内容説明

第1部 総則

第2部 組織と体制の構築

第3部 情報についての対策

第4部 セキュリティ要件の明確化に基づく対策

第5部 情報システムの構成要素についての対策

第6部 個別事項についての対策

統一基準 K303-052 第6部の構成

第6部 個別事項についての対策

6.1 調達・開発にかかわる情報セキュリティ対策

6.1.1 機器等の購入

6.1.2 外部委託

6.1.3 ソフトウェア開発

6.2 個別事項

6.2.1 府省庁外での情報処理の制限

6.2.2 府省庁支給以外の情報システムによる情報処理の制限

6.3 その他

6.3.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止

6.3.2 事業継続計画(BCP)との整合的運用の確保

第6部 個別事項についての対策

6.1 調達・開発にかかわる情報セキュリティ対策

6.1.1 機器等の購入

- (1) 府省庁内における情報セキュリティ確保の仕組みの整備
- (2) 機器等の購入の実施における手続の遵守

第6部 個別事項についての対策

6.1 調達・開発にかかわる情報セキュリティ対策

6.1.2 外部委託

- (1) 府省庁内における情報セキュリティ確保の仕組みの整備
- (2) 委託先に適用する情報セキュリティ対策の整備
- (3) 外部委託先の選定における手続の遵守
- (4) 外部委託の実施における手続の遵守
- (5) 外部委託終了時の手続の遵守

第6部 個別事項についての対策

6.1 調達・開発にかかわる情報セキュリティ対策

6.1.3 ソフトウェア開発

- (1) ソフトウェア開発体制の確立時
- (2) ソフトウェア開発の開始時
- (3) ソフトウェアの設計時
- (4) ソフトウェアの作成時
- (5) ソフトウェアの試験時

第6部 個別事項についての対策

6.2 個別事項

6.2.1 府省庁外での情報処理の制限

いわゆる、モバイルコンピューティングについての対策です。

- (1) 安全管理措置の整備
- (2) 許可及び届出の取得及び管理
- (3) 安全管理措置の遵守

統一基準解説書を参照してください。

第6部 個別事項についての対策

6.2 個別事項

6.2.2 府省庁支給以外の情報システムによる情報処理の制限

いわゆる、私物の業務使用についての対策です。

- (1) 安全管理措置の整備
- (2) 許可及び届出の取得及び管理
- (3) 安全管理措置の遵守

統一基準解説書を参照してください。

私費に限らず、府省庁が支給していない物、例えば、出向者が出向元から支給されている物を含むため、「私物」とはせずに、「府省庁支給以外の～」としている

第6部 個別事項についての対策

6.3 その他

6.3.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止

(1) 措置の整備

(a)

『解説：府省庁外の情報セキュリティ水準の低下を招く行為の防止に関して、統括情報セキュリティ責任者が、規定を整備することを求める事項である。』

府省庁外の情報セキュリティ水準の低下を招く行為としては、例えば、以下のものが挙げられる。

- ・府省庁のウェブのコンテンツを利用するために、ブラウザのセキュリティ設定の下方修正を明示的に要求する行為
- ・府省庁のウェブにより実行形式のファイル(Windowsの場合、「.exe」ファイル)を提供(メールに添付する場合も同様)する行為
- ・府省庁のウェブにより署名していない実行モジュール(JavaアプレットやWindowsのActiveXファイル)を提供する行為
- ・府省庁からHTMLメールを送信する行為

なお、後者の2つについては、利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある行為である。』

(2) 措置の遵守

第6部 個別事項についての対策

6.3 その他

6.3.2 事業継続計画 (BCP) との整合的運用の確保

- (1) 府省庁におけるBCP整備計画の把握
- (2) BCPと情報セキュリティ対策の整合性の確保
- (3) BCPと情報セキュリティ関係規程の不整合の報告



目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

3.1

統一基準作成時の配慮事項

- 構造・体系化した全体構成
- 遵守内容の重複を許容
- 遵守事項の主体者(主語)を明記
- 遵守事項の実施内容(述語)を単純化
- 主体者は、セキュリティ対策での役割(帽子)としている
- 組織上の役職(椅子)は、全員を表す「行政事務従事者」のみ
- 「課室情報セキュリティ責任者」に「課長」(椅子)を想定している
- が、それ以外はすべて役割(帽子)としている
- 実施内容は具体的なものを原則
- 具体性の度合いは、共通化現実性と方策限定の必要性に応ずる
- 逐条解説文による補足説明

3.2

政府機関としての事項

作業の委任

現実の実施者よりも高い役職者が主体者の場合あり

規程文書決済者が唯一

第1部、2～3部、4～6部で分割してもよい

リスク・エスカレーションの不在

手続きの整備を求めているが、現場管理職によるエスカレーションでもよい

監査室不在

監査規程との整合に言及していない

未定稿は行政文書ではない

未定稿について言及していない

事務部門以外は別途強化遵守事項あり

行政事務と著しく異なる業務については別途の基準を検討

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

4. 政府機関以外での活用方法について

DO

情報セキュリティ対策体制の検討

情報の対象の検討

格付け・取扱制限表、明示の定義の検討

定義用語の検討

一括置換(の右側は参考例)

「行政事務」 「業務」

「行政事務従事者」 「社員」

「機密性1情報」 「非機密情報」

「機密性2情報」 「社外秘情報」

「機密性3情報」 「極秘情報」

節・項の取捨選択

強化遵守事項の取捨選択

4. 政府機関以外での活用方法について

DO NOT

部・節・項構成を変更しない

第7部を新設して追加する

別規程を設け、統一基準対応規程については、事務部門など適合する部門だけを対象とする

統一基準との対応関係を管理するのもよい

追加事項、懸念事項についてはパブコメで意見提出

主語をセキュリティ体制上の役割(帽子)以外にしない

帽子の任命部分で吸収させる

述語を統合しない

解説部分の追記をなるべく検討する

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

5. その他

標識と運転席(サインポスト&コックピット)

- ・府省庁基準による有言実行を構築(実行状況の把握)
- ・基準文書の記述により対策実施が担保
- ・実効性に問題があれば、基準文書を改訂して改善

アクセルペダル + 走行速度メーター

メーターが建前ならば、横並び対策になる

走行速度メーターと標識による指示

区別して構築

タクシーなら安心とは必ずしもならない

5. その他

フラクタルなPDCA

- ・年度計画
- ・情報のライフサイクル
- ・情報システムのライフサイクル
- 日常的な全員参加型のリスク判断
- ・情報:情報の格付け
- ・情報システム:必要性の判断
- 日常的な全員参加型の自己点検
- ・情報(第2～3部):教育理解度の再確認としての自己点検
人ごとに集計
- ・情報システム(第4～5部):オンタイム・チェックリストとしての自己点検
システムごとに集計

5. その他

専任監査者ではなくてもできる監査領域の拡大

- ・ 遵守事項実施状況の判断は主体者自身による情報提供を前提
- ・ 専任監査者は、妥当性・実効性の確認を優先
- ・ 自己点検作業が多大な印象があるかもしれないが、その分、監査は容易

目次

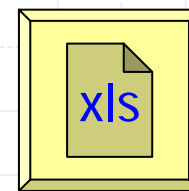
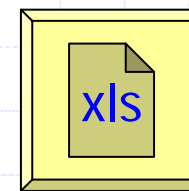
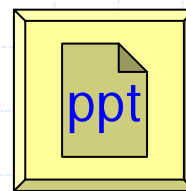
1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

6. 自己点検と監査の概略

自己点検

各遵守事項についての主体者自身による自己点検

- ・遵守性の自己申告



監査

全遵守事項及びその他についての主体者以外による確認

- ・統一基準と府省庁基準、関連規程の準拠性の確認
- ・自己点検結果の妥当性の確認
- ・重点検査による実効性の確認

統一基準単独では、監査以外については遵守性を重視

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答