説明資料1

NISC National Information Security Center

# 政府におけるセキュリティ対策

内閣官房情報セキュリティセンター

平成23年9月7日

# 情報セキュリティ政策の枠組みと推進体制

**内閣官房を中心に関係省庁も含めた横断的な体制を整備**

## 高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　内閣特命担当大臣（科学技術政策）
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（8人）

（事務局）
**内閣官房IT担当室**
室長（官房副長官補（内政））

## 情報セキュリティ政策会議　（2005年5月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　内閣府特命担当大臣（科学技術政策）
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣
民間有識者（６人）

閣僚が参画

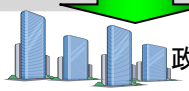
- CISO等連絡会議
- 重要インフラ専門委員会
- 技術戦略専門委員会
- 普及啓発人材育成専門委員会

（事務局）
**内閣官房情報セキュリティセンター（NISC）**
センター長（官房副長官補（安危））
副センター長（内閣審議官）２名
内閣参事官　６名
情報セキュリティ補佐官（アドバイザー）３名

**重要インフラ所管省庁**
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）

**その他の関係省庁**
その他
文部科学省（セキュリティ教育）　等

重要インフラ事業者　等



政府機関（各府省庁）

協力

協力
4省庁
- 警察庁（サイバー犯罪の取締り）
- 総務省（通信・ネットワーク政策）
- 経済産業省（情報政策）
- 防衛省（国の安全保障）

企業　2　個人

# 内閣官房における情報セキュリティ政策の流れ


各省における試行錯誤 | サイバー攻撃への対応を中心とした対策実施時期 | IT障害への対応も含めた総合的な対策基盤づくりの推進 | サイバー攻撃事態発生を念頭、新たな環境変化対応、能動的情報セキュリティ対策「事故前提社会」への対応力強化など成熟した情報セキュリティ先進国へ向けた取組み

## 対策推進の枠組み

約1箇月で組織を立ち上げ

基本戦略

**【基本戦略】**

**国民を守る情報セキュリティ戦略**
（2010.5.11 情報セキュリティ政策会議決定）

**第１次情報セキュリティ基本計画**
（2006.2.2 情報セキュリティ政策会議決定）

**第2次情報セキュリティ基本計画**
（2009.2.3 情報セキュリティ政策会議決定）

**【年度計画：情報セキュリティ20xx】**

※ 基本戦略に基づき策定する年度計画

SJ2006 | SJ2007 | SJ2008 | SJ2009 | 情報セキュリティ2010 | 情報セキュリティ2011 | 2012 | 2013

政府機関対策

情報セキュリティポリシーに関するガイドライン
（2000.7 情報セキュリティ対策推進会議決定）

**政府機関の情報セキュリティ対策のための統一基準（第１～3版）**
（2005.12.13 情報セキュリティ政策会議決定）

**政府機関統一基準（第4版）**
（2009.2.3 情報セキュリティ政策会議決定）

**政府機関統一基準群**
（2011.4.21 情報セキュリティ政策会議決定）

重要インフラ対策

重要インフラのサイバーテロ対策に係る特別行動計画
（2000.12 情報セキュリティ対策推進会議決定）

**重要インフラの情報セキュリティ対策に係る行動計画**
（2005.12.13 情報セキュリティ政策会議決定）

**重要インフラの情報セキュリティ対策に係る第2次行動計画**
（2009.2.3 情報セキュリティ政策会議決定）

基本戦略

政府

## 組織体制

内閣官房情報セキュリティ対策推進室（2000.2設置）

① **内閣官房情報セキュリティセンター**（2005.4 設置）

② **情報セキュリティ政策会議**（2005.5 設置）

③ **GSOC**（2008.4 運用開始）

# 情報セキュリティ対策推進会議について

情報セキュリティ政策会議

情報セキュリティ対策推進会議（CISO等連絡会議）

審議・検討・助言

情報セキュリティ対策推進会議を改組（目的及び構成員）
平成22年7月22日　情報セキュリティ政策会議決定

●目的　関係行政機関の最高情報セキュリティ責任者（CISO）等相互の緊密な連携の下、政府機関における情報セキュリティ対策の推進を図る。

●構成員　議長　内閣官房副長官（事務）
副議長　内閣危機管理監
構成員　各府省庁のCISO（官房長クラス）等

●主な検討事項等
・統一技術基準の改定
・各府省庁の情報セキュリティ報告書の報告等
・対策実施状況報告、重点検査等の報告及び評価
・政府機関における暗号移行指針の策定及びその実施
・最高情報セキュリティアドバイザー等連絡会議の設置・運営
・その他政府機関の情報セキュリティ政策に係る事項

幹事会

最高情報セキュリティ・アドバイザー等連絡会議

平成22年12月27日　情報セキュリティ対策推進会議で設置

●目的　情報セキュリティ対策推進会議に対して、専門的な見地から審議、検討、助言等を行うとともに、各府省庁における知識・経験の共有を図る。

●構成員　各府省庁の最高情報セキュリティアドバイザー及び情報セキュリティ対策推進会議に参加する有識者

●主な検討事項等
・各府省庁が作成した情報セキュリティ報告書についての技術的な評価・助言
・政府機関における暗号移行指針に係る技術的な審議、検討、助言
・その他、政府機関の情報セキュリティ政策に係る事項の技術的な審議、検討、助言

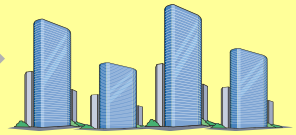
# 政府機関統一基準の策定・見直し

- **政府機関における情報セキュリティ対策のための統一的な基準**を策定し、政府全体の情報セキュリティ水準の向上を図る
- 各政府機関は本基準を踏まえて**対策を実施**し、**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において基準の見直しを決定**

**情報セキュリティ政策会議**
- 政府機関統一基準の策定
- 各府省庁の評価結果に基づき基準を見直し

**政府機関統一基準**
各府省庁が最低限採るべき情報セキュリティ対策を定めたもの。

**改善勧告**



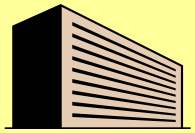
**各府省庁**
- 政府機関統一基準に基づき、省庁対策基準の見直し

統一規範等

**情報セキュリティ対策推進会議（CISO等連絡会議）**

策定・導入 → 運用 → 評価 → 見直し → PDCA

統一技術基準



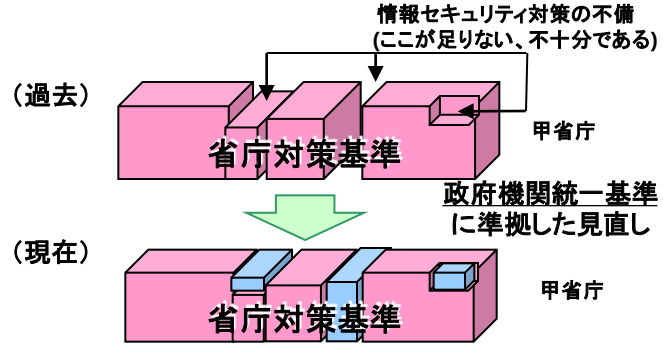
**内閣官房 情報セキュリティセンター（NISC）**

**対策実施状況の検査・評価**
NISCが各府省庁の対策実施状況を検査・評価し、その結果を踏まえ、情報セキュリティ政策会議等で基準の見直し等を決定する。

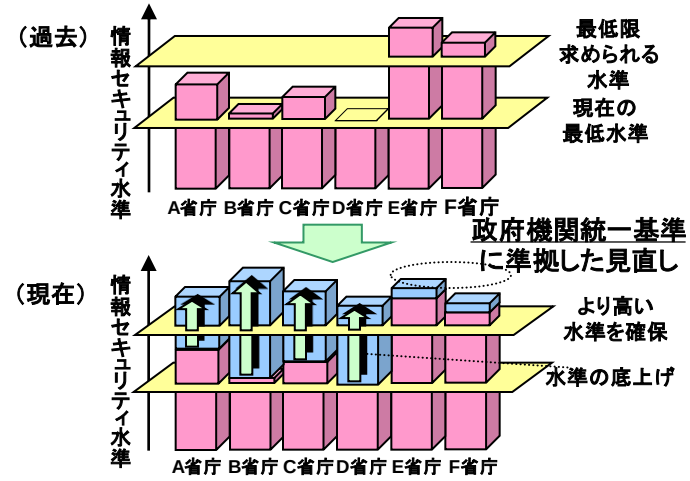
策定・導入 → 運用 → 評価 → 見直し → PDCA

＊対策の平準化・より高い水準への底上げ

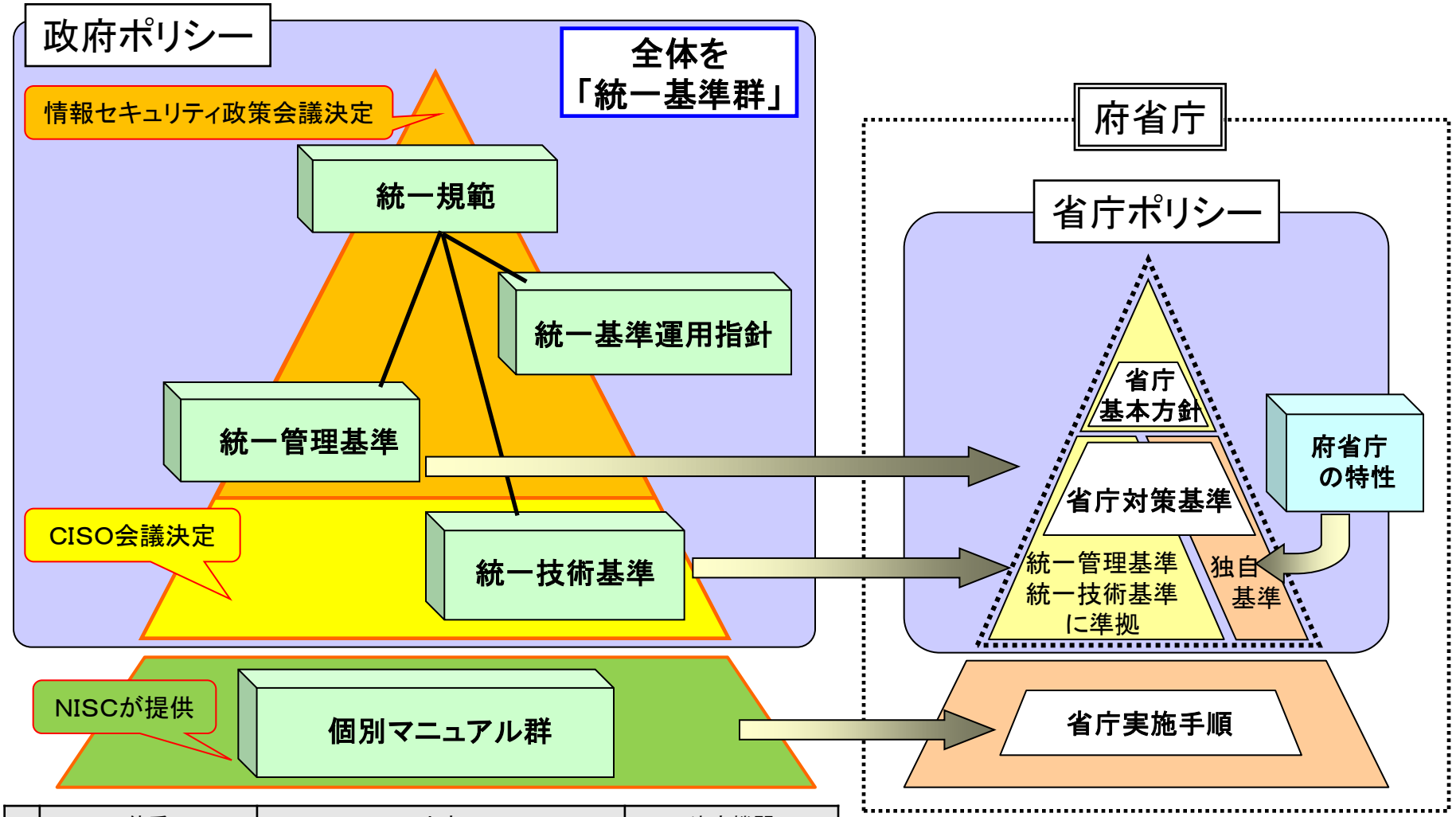
**① 政府機関統一基準による省庁対策基準の補完**




**② 各府省庁の情報セキュリティ水準の向上**



# 政府機関統一基準群と省庁対策基準との関係など




| | 体系 | 内容 | 決定機関 |
|---|---|---|---|
| 1 | 統一規範 | 情報セキュリティ基本方針 | 政策会議 |
| 2 | 統一基準運用指針 | 情報セキュリティマネジメントの指針 | 政策会議 |
| 3 | 統一管理基準 | 情報セキュリティポリシー （基本編） | 政策会議 |
| 4 | 統一技術基準 | 情報セキュリティポリシー （技術編） | CISO等連絡会議 |

**府省庁は、省庁ポリシー等に基づき情報セキュリティ対策を実施**

※ 統一技術基準は、各府省庁において技術的対策を柔軟に講じられるよう統一基準との決裁の分離し、より機動的な運用を可能とする。

# 政府機関統一基準群の全体構成

## ◆統一規範

（1）目的及び対象
（2）政府機関の情報セキュリティ対策のための基本指針
（3）政府機関の情報セキュリティ対策のための基本対策

## ◆統一基準運用指針

政府機関統一基準及び技術基準の運用の枠組み
（1）政府機関統一基準及び技術基準の策定と各府省庁における情報セキュリティポリシーの見直し
（2）対策実施手順書の整備の支援
（3）対策実施状況の確認と評価に基づくPDCAサイクルの確立

## ◆統一管理基準

第1．1部　総則
第1．2部　組織と体制の整備
第1．3部　情報についての対策
第1．4部　情報処理についての対策
第1．5部　情報システムについての基本的な対策

## ◆統一技術基準

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

# NISC Webページ

**http://www.nisc.go.jp/**




・国民を守る情報セキュリティ戦略
・第2次情報セキュリティ基本計画
・情報セキュリティ20xx
・セキュアジャパン20xx
・20xx年度の情報セキュリティ政策の評価等

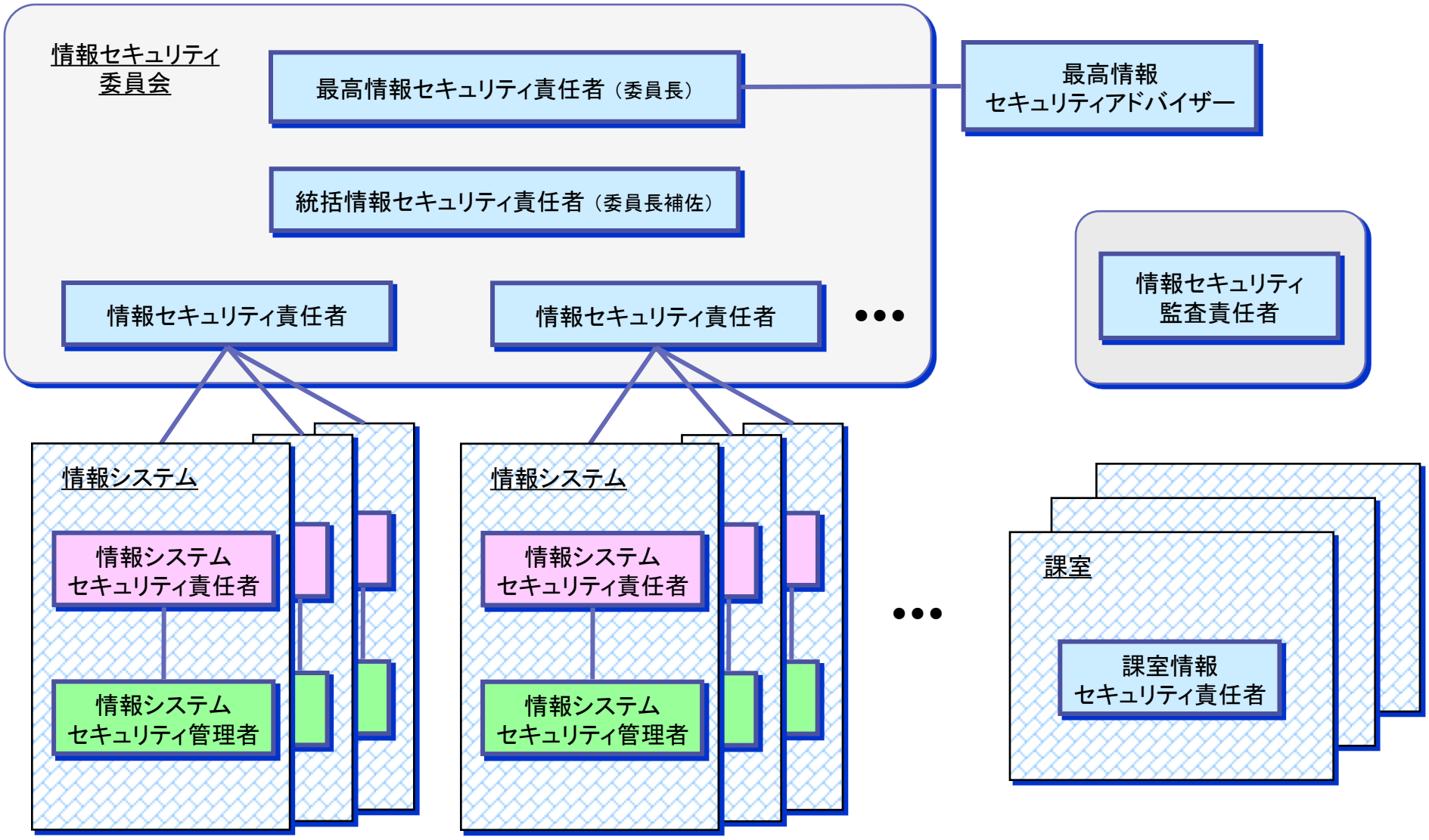
他

・統一規範
・策定と運用等に関する指針
・統一管理基準
・統一技術基準
・同 各解説書
・同関連のファイル掲載
（旧版の統一基準、新旧対照表）
・個別マニュアル群

他

情報セキュリティ政策会議の会議資料が掲載されている。
（会議終了後、ほぼ当日中）

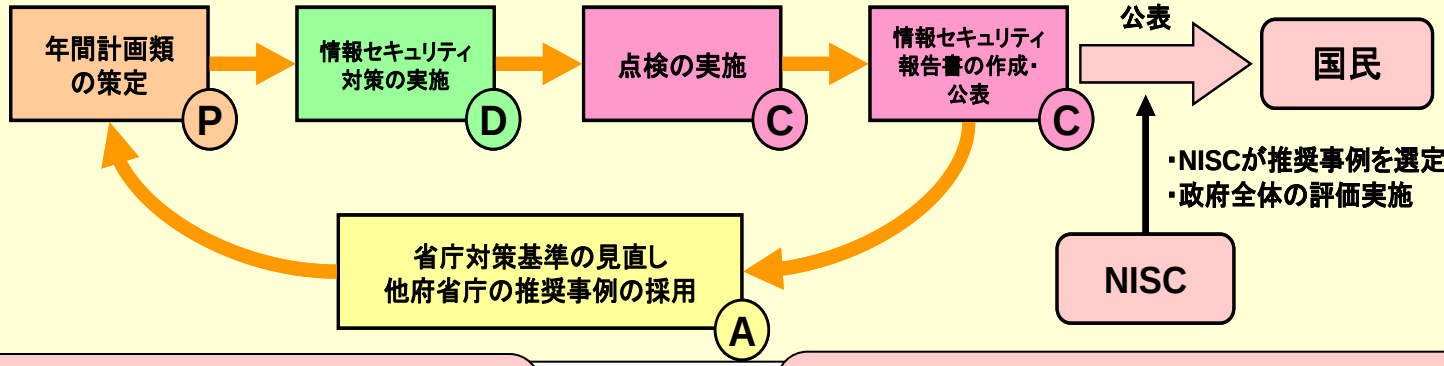
# 組織・体制イメージ図


情報セキュリティ
委員会
最高情報セキュリティ責任者（委員長）
最高情報
セキュリティアドバイザー
統括情報セキュリティ責任者（委員長補佐）
情報セキュリティ
監査責任者
情報セキュリティ責任者
情報セキュリティ責任者
●●●
情報システム
情報システム
セキュリティ責任者
情報システム
セキュリティ管理者
情報システム
情報システム
セキュリティ責任者
情報システム
セキュリティ管理者
●●●
課室
課室情報
セキュリティ責任者

# 情報セキュリティ報告書の概要

## ■ 情報セキュリティ報告書の目的

各府省庁の最高情報セキュリティ責任者が中心となり、自ら問題意識を持って、自組織の情報セキュリティ対策の取組状況を国民へ公表し、各府省庁の参考となるベストプラクティスを共有するなどの取組を通じて、能動的に情報セキュリティ対策の改善を図る仕組みを各府省庁において実現する。




## 全府省庁への導入スケジュール

**【平成21年度】**

- 情報セキュリティ報告書専門委員会において、情報セキュリティ報告書作成のためのガイドラインを検討し、決定。
- 総務省及び経済産業省において、試行的に情報セキュリティ報告書21年度試行版を作成。

**【平成22年度 】**

- 全府省庁において、情報セキュリティ報告書を試行的に作成（公表は任意）。

**【平成23年度（予定）】**

- 全府省庁において、情報セキュリティ報告書を作成し、公表。

## 平成22年度の情報セキュリティ報告書について

**【実施状況】**

1. ４月中に全ての府省庁において、情報セキュリティ報告書案を作成
2. ４月28日に開催された最高情報セキュリティアドバイザー等連絡会議において、各府省庁が作成した報告書案に対する助言及び推奨事例候補を推薦
3. アドバイザー会議による助言を踏まえ、各府省庁において必要な見直しを行った上で平成22年度の報告書として決定
4. 報告書については、５月31日に開催されたCISO等連絡会議において報告
5. 年次報告（評価書）については、７月８日に開催された情報セキュリティ政策会議において報告し、公表

# 政府機関における情報セキュリティに係る年次報告（平成22年度）の概要

各府省庁
情報セキュリティ報告書

各府省庁のCISOが、省内における**年間の情報セキュリティ対策の取組状況等**について**取りまとめた報告書**

→ CISO等連絡会議に報告（平成23年5月31日）

平成22年度は、試行的に作成。 平成23年度より公表予定

**政府機関における情報セキュリティに係る年次報告（平成22年度）**

各府省庁の情報セキュリティ報告書をCISO等連絡会議において**評価した報告書**

→ CISO等連絡会議にて決定（平成23年5月31日）

年次報告については、平成22年度より公表

## 年次報告の概要

### 国内外における情報セキュリティに関する動向

- ○ サービス不能攻撃等、**サイバー攻撃の増加**
- ○ **標的型メール攻撃の増加・巧妙化等**
- ○ **情報の流出**
- ○ 情報システムの**障害・事故等の発生**
- ○ ネットワーク**環境の進化等に伴うリスクの増加**
- ○ **東日本大震災**に伴う情報システムに関連した**事故等の発生**

### 政府機関の取組

- ○ **CISO等連絡会議・最高情報セキュリティアドバイザー等連絡会議**の設置及び開催
- ○ **情報セキュリティ報告書**を試行的に作成
- ○ **政府機関統一基準群**の整備
- ○ 公開ウェブサーバに対する**脆弱性検査**の実施
- ○ 政府機関から発信する**電子メールに係るなりすましの防止**
- ○ 政府職員に対する**教育・意識啓発の推進**

### 各府省庁における対策の実施状況

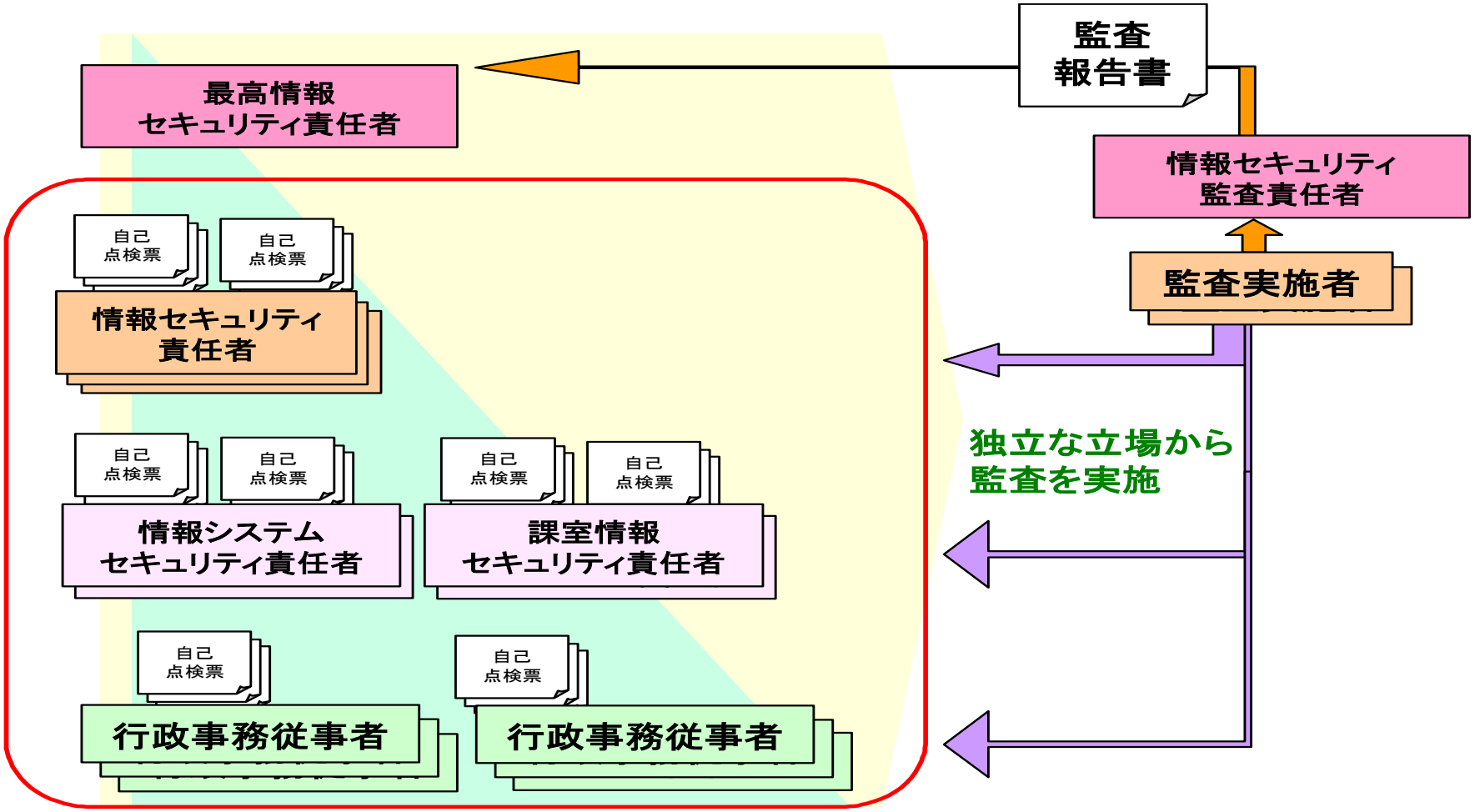
- ○ 政府機関全体の**実施率**は、**98．9%**
- ○ **情報の取扱い**に関する項目（**94%**）など、年々改善の努力がなされてきてはいるが、**更なる改善**が望まれる。

### 情報セキュリティに関する動向を踏まえた課題

- ○ 東日本大震災等を踏まえた情報システムの**業務継続能力の強化**
- ○ **標的型メール攻撃への対応**
- ○ **新たな技術**に対する**情報セキュリティ対策の強化**
- ○ **安全な暗号利用**の促進
- ○ **情報流出防止**への取組

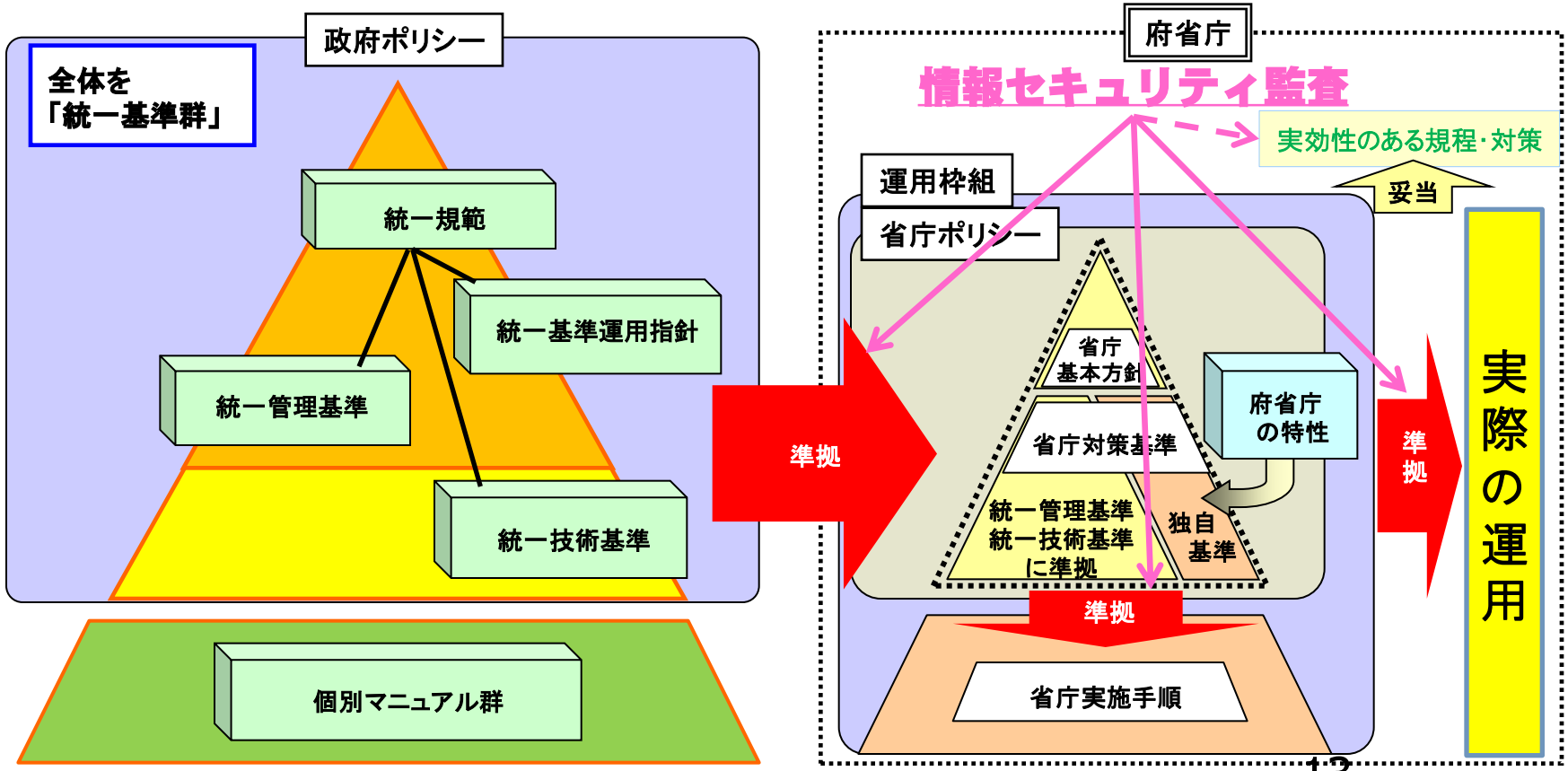
# 情報セキュリティ監査（監査の概要）

- 各府省庁は、**政府機関統一管理基準 1.2.3.2 情報セキュリティ対策の監査**を遵守し、自らのPDCAサイクルを適切に運用することが求められる。



# 情報セキュリティ監査（監査の目的・位置付け）

| | | |
|---|---|---|
| 必須 | 準拠性監査 | ■ 省庁対策基準が政府機関統一基準群に準拠しているか<br>■ 実施手順が省庁対策基準に準拠しているか<br>■ 情報セキュリティ対策の運用が情報セキュリティ関係規程に準拠しているか |
| 推奨 | 妥当性監査 | ■ 情報セキュリティ関係規程が実効性のあるものになっているか<br>■ 情報セキュリティ対策が妥当であるか、有効に機能しているか |



# 情報セキュリティ監査（規程）

**政府機関の情報セキュリティ対策のための統一規範**

***（監査）***

**第十条**　各府省庁は、省庁基準が統一規範に準拠し、かつ実際の運用が省庁基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。

***（情報セキュリティ報告書）***

**第十一条**　各府省庁は、自己点検及び監査の結果を反映した情報セキュリティ報告書を毎年度作成し、公表しなければならない。報告書の構成、細目は別に定める。

2　各府省庁は、作成した情報セキュリティ報告書に基づいて省庁基準を見直し、必要な措置を講じなければならない。