政府機関の情報セキュリティ対策のための統一基準群の改定について（概要）

資料1-1

昨今の政府機関等を対象とした標的型攻撃等への対応、情報技術や利用環境の変化を踏まえた対応、調達時におけるセキュリティ要件の確保やリスク分析の確実な実施等の観点から、統一基準群の規定を見直し

○新たな脅威等への対応

標的型攻撃等に備えた体制の整備、災害時の継続的な運用の確保

＊障害・事故等の発生に備えた体制の整備や他の組織との情報共有に関する規定を追加

＊管理者権限の適切な管理（パスワード等）を行うための規定を追加

＊省庁対策基準と情報システム運用継続計画との整合的運用を確保するための規定の見直し

○情報技術・利用環境の変化への対応

共通基盤システムの適切な運用、区域における対策の明確化

＊政府の共通基盤システムの適切な情報セキュリティマネジメントに関する事項の追加

＊情報を取り扱う区域のクラス区分毎の対策に関する規定を追加

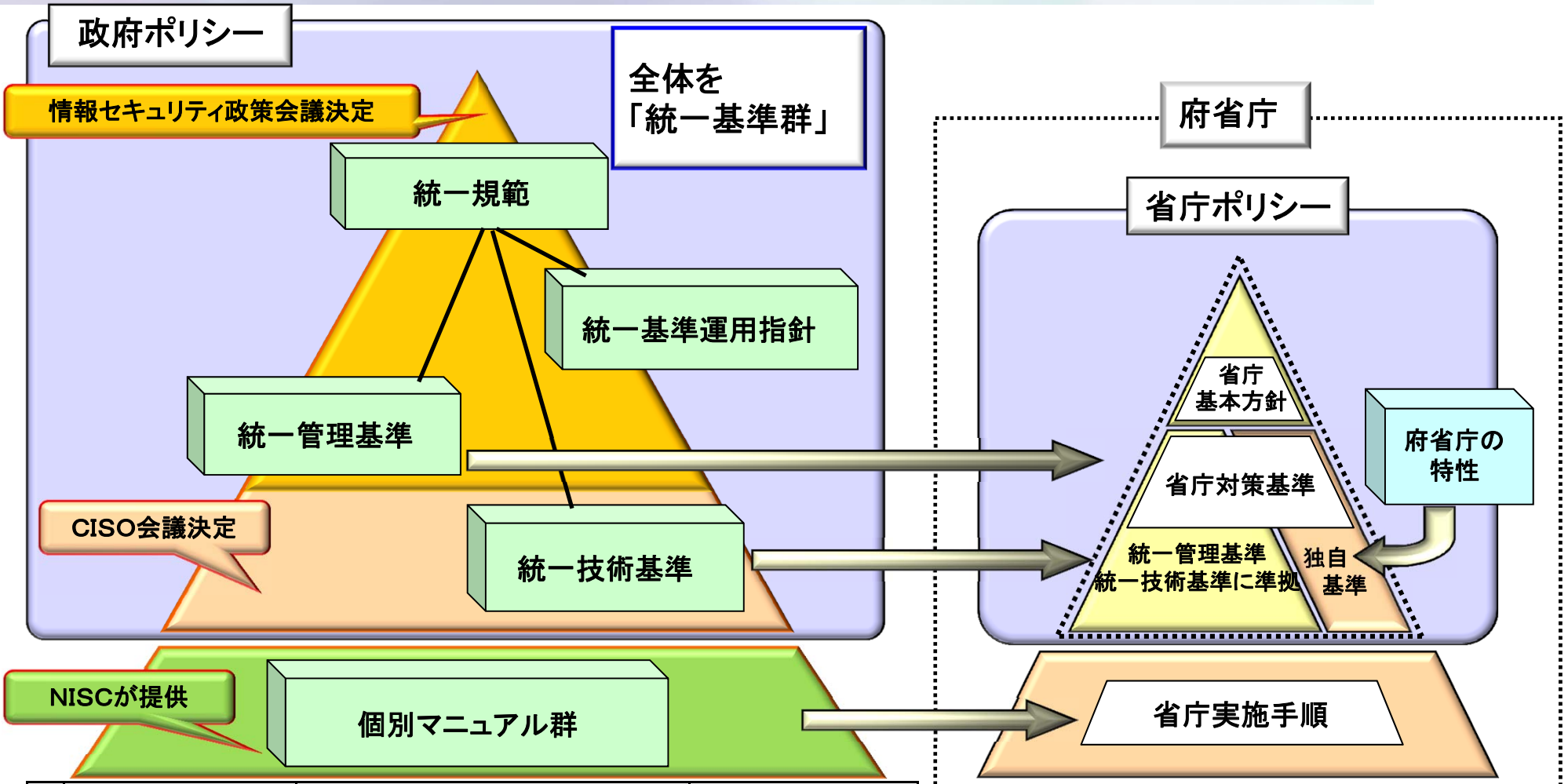
○基準運用の実効性の向上

調達時におけるセキュリティ要件の確保、リスク分析の実効性を確保

＊情報システムの調達時におけるセキュリティ要件を確保するための措置を追記

＊遵守事項の枠組みを変更し、全ての遵守事項について、各府省庁における確実なリスク分析の実施

政府機関統一基準群の構成について　（参考）



	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

※　統一技術基準については、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決裁を分離し、より機動的な運用を可能としている。