資料4

安全対策基準(第９版)の改訂概要

平成29年12月20日

公益財団法人　金融情報システムセンター

安全対策基準（第９版）改訂までの流れ

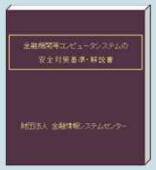
これまでの安全対策基準の改訂について

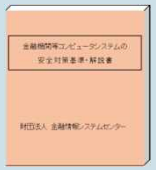
■『金融機関等コンピュータシステムの安全対策基準・解説書』（以下、安全対策基準という）は、昭和60年に初版が発刊された後、ＩＴの進展や新たなサービスの登場など、金融機関等を取り巻く環境の変化に応じ、改訂を行ってきた。

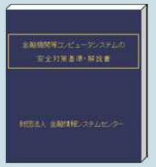
■直近では、クラウドサービスの利用及びサイバー攻撃対応等に関する有識者検討会を開催し、その検討結果を第８版追補改訂（平成27年6月発刊）に反映している。

■発刊以来、安全対策基準は、金融機関等の情報システムの安定運用に寄与してきたものの、多様化する基幹業務系以外のシステムに対し、安全対策を一律に実施するのではなく、リスクに応じて安全対策が策定されるよう、安全対策基準の改訂を行うこととした。

昭和60年度	・・・	平成23年度	平成25年度	平成27年度	平成29年度（予定）
初版発刊		第８版	第８版追補	第８版追補改訂	第９版
決済オンライン化に伴い、主に勘定系システムの安全対策に関する自主基準として策定	ＩＴの進展、新たなサービスなど状況の変化に応じ、安全対策基準の改訂を実施		大震災への対応、Ｗｅｂ化の進展、クラウドサービスの利用、サイバー攻撃対応を踏まえた改訂を実施		安全対策に対する考え方の見直し＝リスクベースアプローチの導入



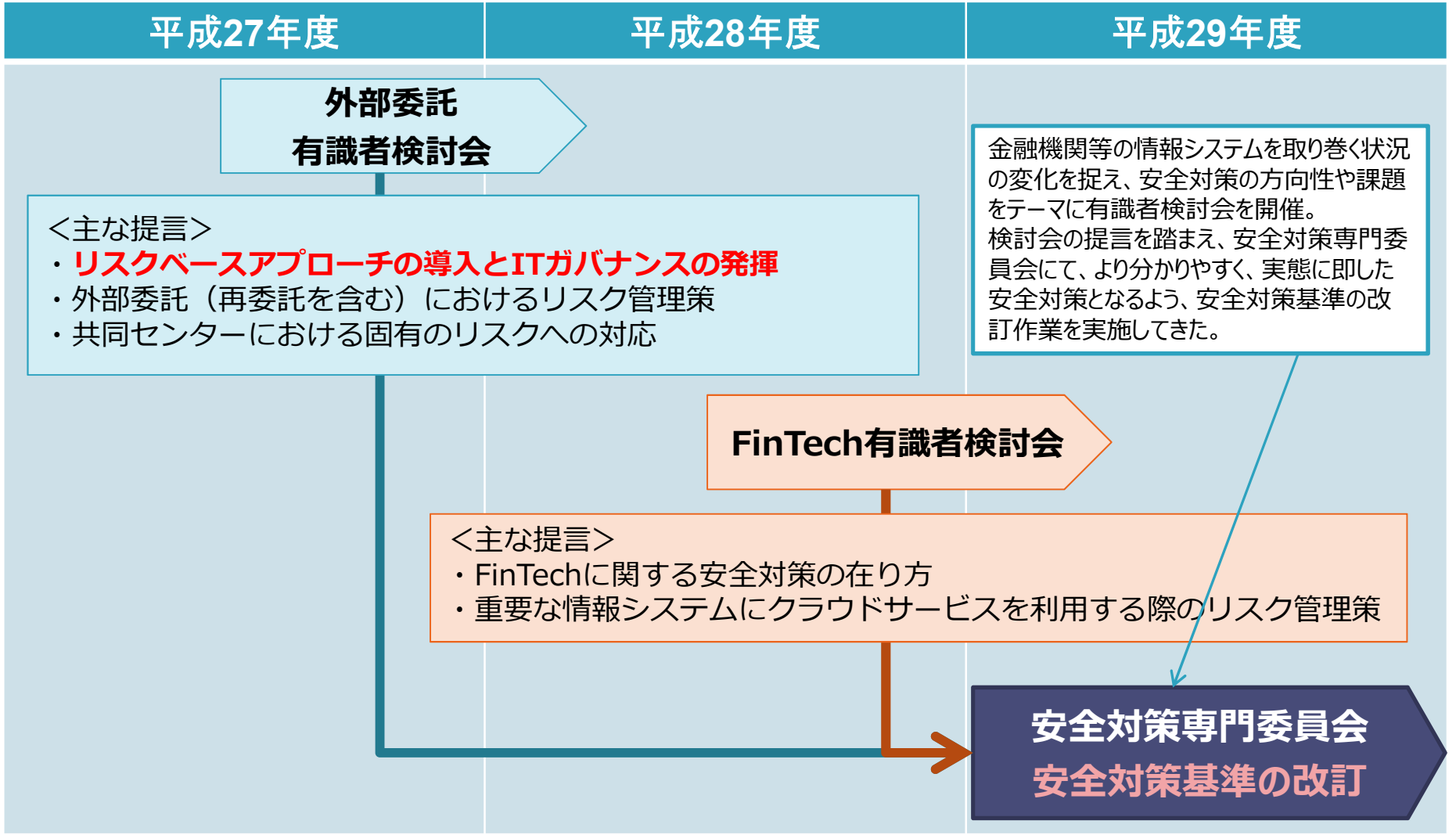




安全対策基準（第９版）改訂までの流れ

有識者検討会の提言を踏まえた安全対策基準の改訂

外部委託に関する有識者検討会及び、FinTechに関する有識者検討会の提言内容を安対基準改訂に反映。



安全対策基準（第９版）改訂の概要

改訂のポイント

各検討会における提言内容の反映箇所は次のとおり。

改訂に向けた提言

外部委託に関する有識者検討会

- ◆ リスクベースアプローチの導入とITガバナンスの発揮
- ◆ 委託先（再委託先を含む）におけるリスク管理
- ◆ 共同センターにおける固有のリスクへの対応

FinTechに関する有識者検討会

- ◆ FinTechに関する安全対策の在り方
- ◆ 重要な情報システムでクラウドサービスを利用する場合のリスク管理策
- ◆ 「オープンAPI」における安全対策の在り方
- ◆ 今後の安対基準改訂の考え方

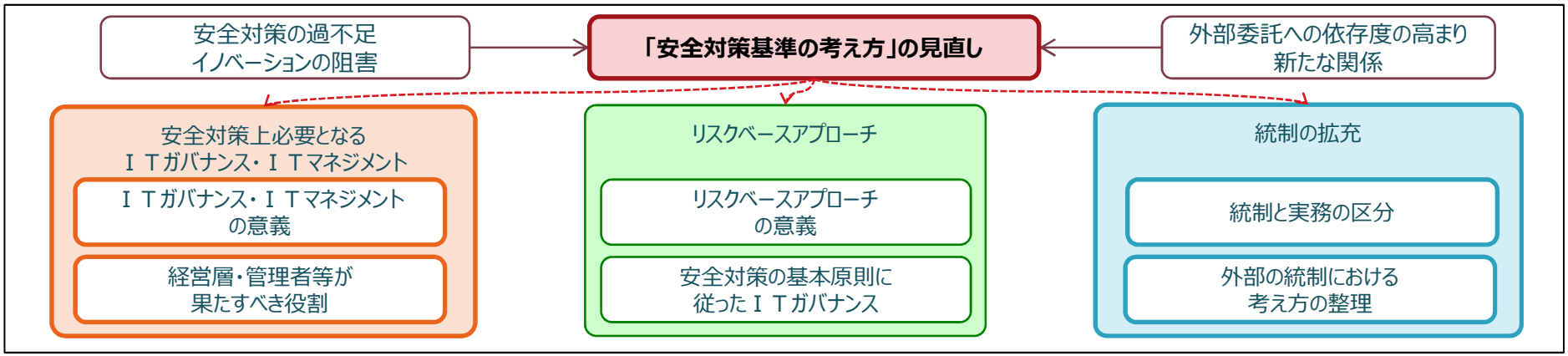
提言内容を安対基準（第９版）に反映

- リスクベースアプローチ導入に伴う改訂
  - 「金融情報システム」の分類
  - 「基準の分類」の設定
  - 「必須対策」の設定
- 外部の統制基準の整理
  - 外部の統制に関する整理
  - 外部委託基準とクラウド基準の整理・統合
  - 共同センター固有基準の新設
- 基準構成の変更・基準の分類
  - 新基準構成
  - 基準の並び替え
- 読みやすさの対応
  - 様式の再定義
  - 語尾の曖昧さ排除

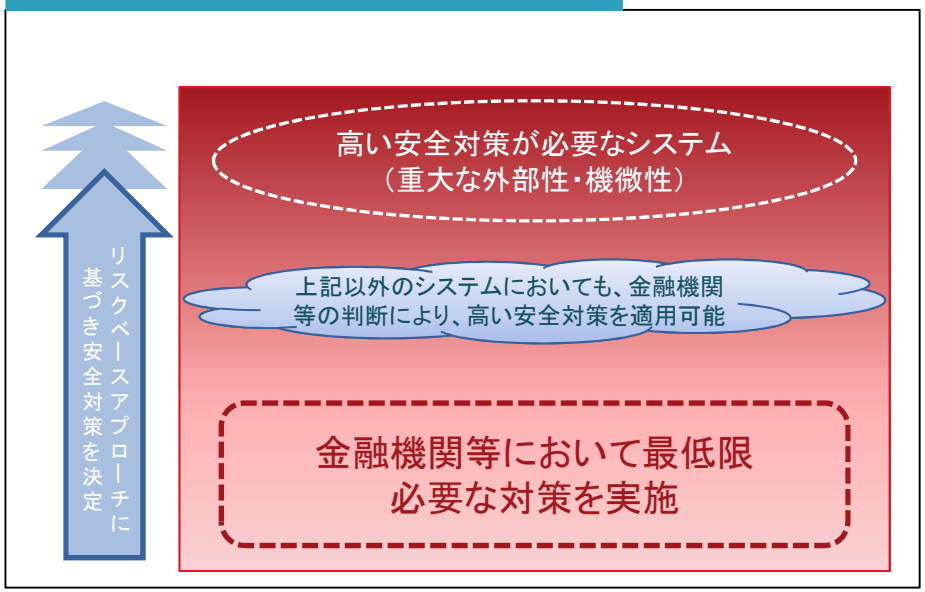
安全対策基準（第９版）改訂の概要

リスクベースアプローチ導入に伴う改訂

ITガバナンスの下、金融情報システムに対してリスク評価を実施し、リスク特性に応じた安全対策基準を適用。



基本原則に従った安全対策の考え方



金融情報システムの分類

「金融情報システム」

金融機関等が、業法等に基づき、顧客に商品・サービスを提供するために利用する情報システム

特定システム

金融情報システムのうち、重大な外部性を有するシステム（システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性があるシステム）や、機微情報（要配慮個人情報を含む）を有するシステム（機微情報（要配慮個人情報を含む）の漏えい等により顧客に広範な損失を与える可能性があるシステム）。

通常システム

特定システム以外の金融情報システム。なお、特定システムの一部について、リスクの影響が限定的である場合、特定システムから切り離し、「通常システム」とすることも可能。

安全対策基準（第９版）改訂の概要

「基準の分類」・「必須対策」の設定

ITガバナンスの下、金融情報システムに対して自らリスク評価を実施し、リスク特性に応じた安全対策基準を適用。

「基準の分類」の設定

基礎基準	特定システム、通常システムによらず、金融情報システムが最低限適用する基準
付加基準	「基礎基準」以外で、リスク特性に応じて追加・選択する基準 ※特定システムは適用する基準

「基礎基準」の選定にあたっての考え方

○統制・監査に関する基準
○顧客データの漏えい防止及びシステムの不正使用防止に関する基準
○コンティンジェンシープラン策定に関する基準
○システムの運行管理に最低限必要な基準

「必須対策」の設定

必須対策	基礎基準や付加基準において、「解説部分」で「必要である」と記載されている対策をすべて各基準の「必須対策」と位置付ける。
その他の対策	「解説部分」で「望ましい」と記載されている対策、例示されている対策は、すべてリスクベースアプローチによって選択的に適用されるものと位置付ける。

基準の適用方法	基礎基準		付加基準	
	必須対策	その他の対策	必須対策	その他の対策
特定システム	○	△	○	△
通常システム	○	△	△	△

【凡例】○：適用　　△：選択的に適用

システム構成等の観点から適用する必要がない、あるいは適用できない場合には「必須対策」であっても適用は不要である（例えば、外部接続しないシステムについて、外部接続管理に関する安全対策の適用は不要である）。
また、「必須対策」には、「個人データを扱うシステムの場合には～することが必要である。」などのように、一定の条件の下において適用が必須である対策も含まれている点に留意する必要がある。

安全対策基準（第９版）改訂の概要

外部の統制の範囲

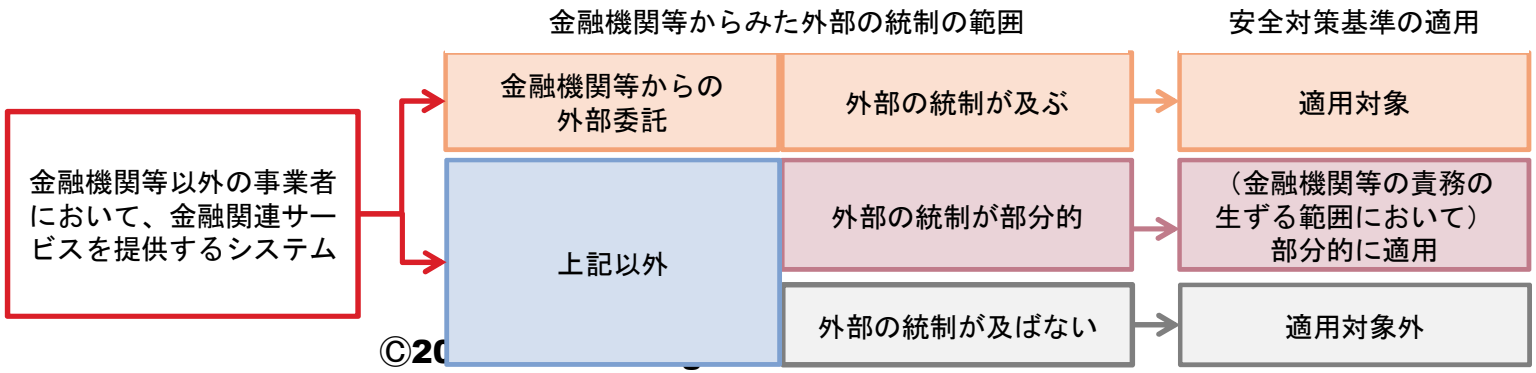
金融機関等以外の事業者が、金融関連サービスを提供する場合の安対基準の適用の考え方を整理。

外部の統制と安対基準の適用範囲の整理

用語の定義

金融サービス	金融機関等（銀行等の預金取扱金融機関、信託会社、証券会社、保険会社、クレジット会社等をいう（ただし、電子決済等代行業者などのFinTech企業等を除く））が業法等に基づき、顧客に提供するサービス
金融関連サービス	金融サービスを補完するため、金融機関等以外の事業者が提供するサービス

FinTech企業等の登場により、金融機関等以外の事業者が金融機関等の外部委託先とはならず、主導的に金融関連サービスを提供するケースが生じている。金融機関等による外部の統制が及ばないか、または部分的となる場合の安全対策基準適用方法の考え方を示した。



安全対策基準（第９版）改訂の概要

外部統制基準の整理

外部委託基準（運【87～90】）、クラウド基準（【運108～111】）及び、監査に関する基準（【運91】、【運112】）の内容を統合・整理し、クラウド固有基準と共同センターに関する基準を新設。

外部委託基準とクラウド基準の整理・統合　監査基準の整理・統合　クラウド固有基準の新設

第8版追補改訂（H27.6発刊）

	外部委託	クラウド
利用検討時	運87 運87-1	運108
契約締結時	運88	運109
運用時	運89 運90	運110
契約終了時	運90内	運111
監査	運91内	運112

第9版改訂案

	新基準番号	ポイント
利用検討時	【統20】	記載の重複・冗長を排除し再構成
契約締結時	【統21】	記載の重複・冗長を排除し再構成
運用・モニタリング時	【統22】 【統23】	・記載の重複・冗長を排除し再構成 ・データ漏洩防止基準「運110」は、【統21】へ統合。
契約終了時	–	【統21】へ統合
監査	【監1】	記載の重複を排除し、監1へ統合
クラウド固有	【統24】 （新設）	・クラウド固有のリスク管理策 （「クラウド拠点の把握」「監査権の明記」等）

共同センター固有基準の新設

第9版改訂案

	新基準番号	ポイント
共同センター固有	【統25】 （新設）	・共同センター固有のリスクに対する安全対策 （緊急事態発生時における「時間性」の問題）

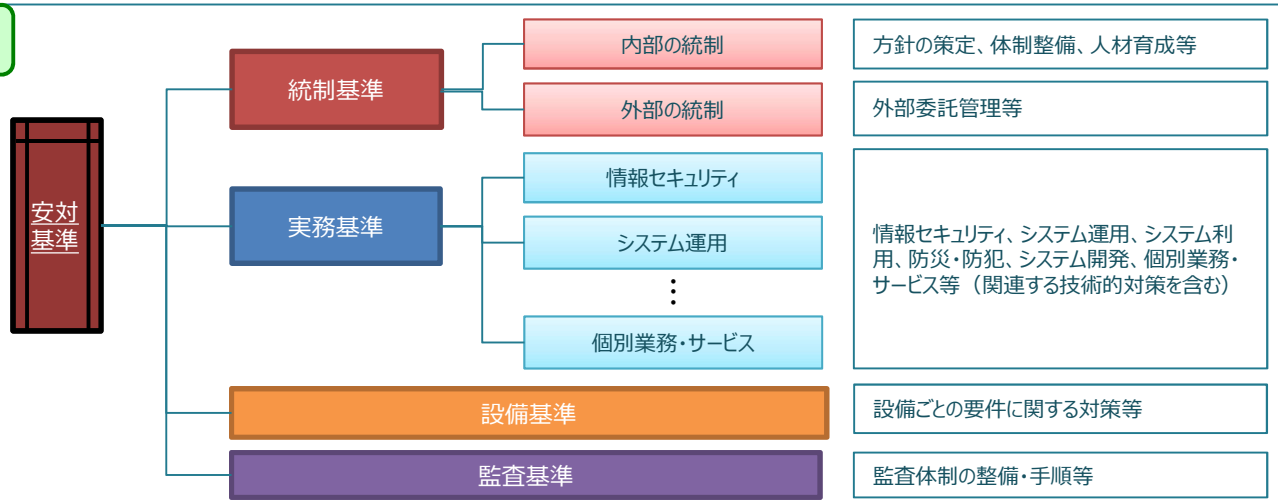
安全対策基準（第９版）改訂の概要

基準構成の変更

基準の構成を「統制基準」「実務基準」「設備基準」「監査基準」に変更。

金融機関の経営層はITガバナンスを発揮していくことが求められ、また、金融機関等においては外部委託やサービス利用への依存度が高まる中、安対基準は統制面での対策を拡充していくことが求められる。これらの要求に応えていくには、安対基準において、**統制面の対策を明示的に示す**ことが有効。

新基準構成



基準項目の並べ替え

基準項目（大項目・中項目・小項目）をシステム共通の視点・利用者の視点に沿って変更。

これまでの基準項目の構成は、基幹業務系システムにおける安全対策を効果的に実施することを前提としていたが、情報システムが多様化し、外部委託やサービス利用への依存度が高まる中、金融機関等はもちろん、FinTech企業等の新たな利用者にとっても、利用しやすい構成へ変更。

第8版追補改訂

・勘定系システムを前提とした構成
・作業の流れをイメージ（入退室管理・・・・）した構成

⇒

第９版改訂案

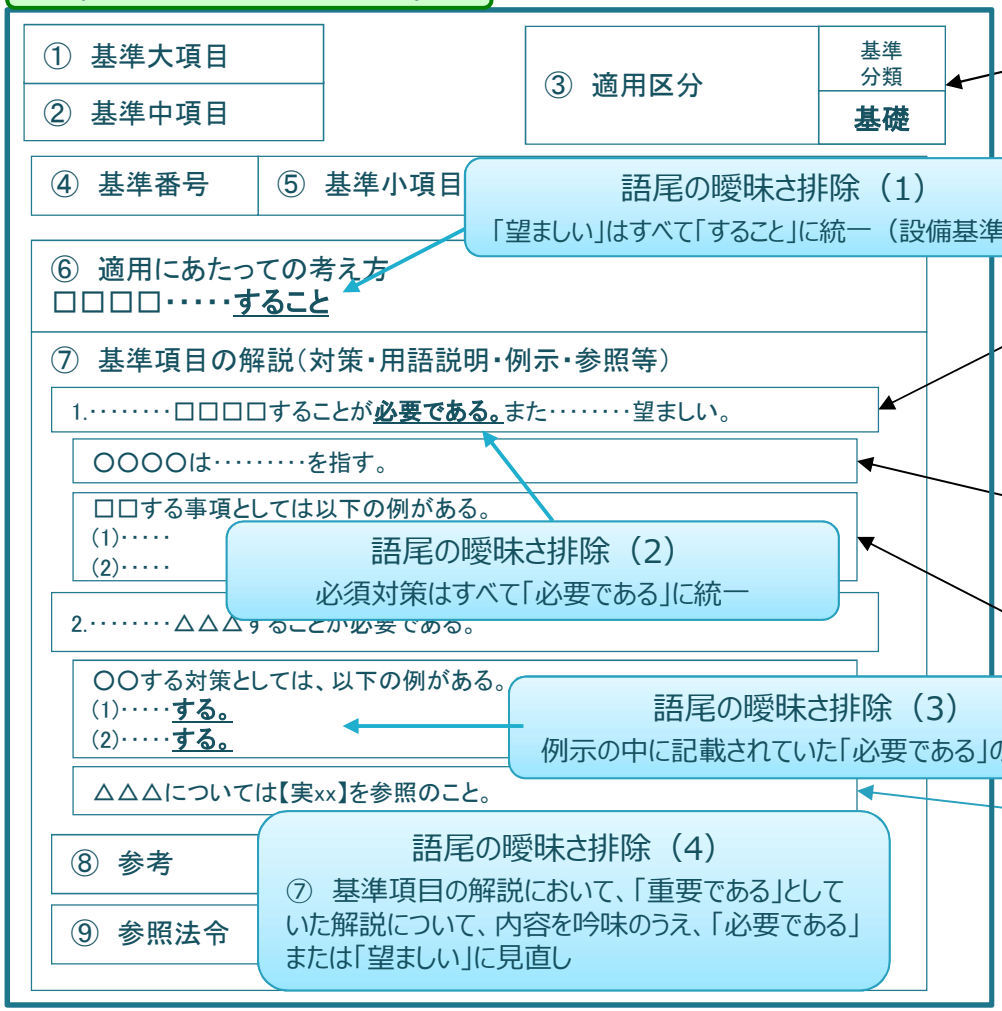
・様々なシステムを想定した構成
・利用者の目的（セキュリティ対策・・・・）をイメージした構成

安全対策基準（第９版）改訂の概要

読みやすさの対応（記述様式の再定義・標準化）

「読みやすさの向上」を目的とし、様式、記述ルールを再定義するとともに、基準本文（主に解説部分）の変更を実施。

様式・記述ルールの再定義



【基準分類】
基礎基準・付加基準のいずれであるかを表示する。
（設備基準にはない）

【対策】
実施する「対策」を記載する。

- 「～必要である」 ・・・必須対策
- 「～可能である」 ・・・必須対策に対する代替策
- 「～望ましい」 ・・・選択可能な対策（ベストプラクティス）
- 「～考えられる」 ・・・選択可能な対策

※番号は「対策」のみに付され、例示、用語説明は、関連する「対策」の下に記載している。

【用語説明】
基準中で使用される用語についての説明を記載する。

【例示】
対策に対する具体的な実施方法等を記載する。
例示の内容は、リスク特性等に応じて選択可能な対策となる。
（例示以外の方法等を選択することも可能）

【参照】
対策に関連する基準番号を記載する。

安全対策基準（第９版）改訂の概要

改訂版安対への移行措置

安全対策基準適用における経過的措置を掲載。

（参考）安全対策基準適用における経過的措置について

第9版改訂は、それ以前の改訂と異なり、安全対策基準の適用の考え方から抜本的に変更を行うことから、安全対策基準を使用する金融機関等においては、社内規程の見直しや、場合によっては組織体制等の見直しが発生するなど、その影響が大きいことが予想される。

そのため、現状で安定的に運営されている金融情報システムについては、従来どおりの取扱いを継続することとし、所要の社内体制や規程等の整備を行ったうえで、システムの更改時や新システムの導入時に、変更後の安全対策基準を適用するなど、順次移行を図ることとする。