金融機関のセキュリティ対策の動向について

平成19年2月14日
(財) 金融情報システムセンター
監査安全部
吉田　晃憲

1．FISCご紹介

2．FISCガイドラインの位置付け

3．「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」

4．「金融機関等におけるコンティンジェンシープラン策定のための手引書」

1. FISCご紹介

FISCご紹介

- FISC＝THE CENTER FOR FINANCIAL INDUSTRY INFORMATION SYSTEMS
- 金融機関･生損保･証券･コンピュータメーカー等の出捐により大蔵省（当時）の外郭団体として設立（１９８４年11月）

  ２０００年7月1日より金融庁の所管
- 金融情報システムに関連する諸問題について、金融機関等の協力をもとに総合的な調査研究を行い、金融情報システムの安全性確保のための施策を推進し、金融情報システムの円滑な発展に貢献することを目的としています。
- 会員　６５２機関（2007年1月末日現在）が、FISCの会員としてその活動をサポートしています。一方、FISCでは調査研究の成果を「金融情報システム白書」、機関誌「金融情報システム」の出版をはじめ、ホームページ、講演会、セミナー等様々な活動を通じて、会員に提供しています。

FISCご紹介

- **調査研究活動**

(1) 金融機関等のコンピュータシステム
(2) 電子決済･電子マネー
(3) ICカード
(4) 資金･証券決済システム
(5) リスク管理
(6) 個人情報保護

FISCご紹介

- **金融情報システムに関する自主基準（ガイドライン）策定**

  FISCは、会員企業や学識経験者等の皆様の協力を得て、金融情報システムの安全性確保や金融業務の安定的遂行のための自主基準を策定しています。これらは、金融機関や、金融機関に情報システムを提供するコンピュータメーカー等で広く用いられています。

（1）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

（初版1985.12　第７版 2006.03、第7版追補2007.03予定）

（2）金融機関等におけるコンティンジェンシープラン策定のための手引書

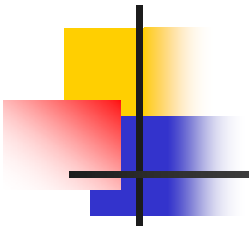
（初版1994.01　第３版2006.03）

（3）金融機関等のシステム監査指針

（初版1987.07　第2版2000.07　第3版2007.03予定）

（4）金融機関等におけるセキュリティポリシー策定のための手引書

（初版1999.01）



2．FISCガイドラインの位置付け

「金融機関等ｺﾝﾋﾟｭｰﾀｼｽﾃﾑの安全対策基準」

システム化に内在するリスク

①障害時の影響の広域化･深刻化

②プライバシー･企業機密の侵害

③コンピュータ犯罪

金融機関等に対する社会的要請

①安定したサービスの提供

②信用秩序維持

③技術的貢献

財団法人金融情報システムセンターにおいて金融機関等のコンピューターシステムの安全対策の**共通的なよりどころ**として策定

FISC安全対策基準

金融、保険、証券、クレジット等の金融業務を営む業界（金融機関等）の各社においては、

「本基準が安全対策を講ずるうえで業務内容に即した指針となること、各社がコンピュータシステムの状況等に即し漸次実施しうる内容となっていること等を勘案し、**各社が本基準を参考にしながら適切な安全対策を実施することが期待される。**」

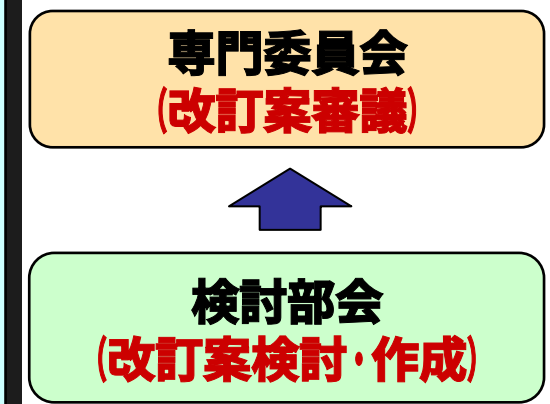
（「ガイドライン」であり、強制力はない。また、ＦＩＳＣによる「適合性評価認定」制度のようなものはない。）

FISCガイドライン策定手順

FISC会員企業と有識者から構成される専門委員会と検討部会（WG）において、改訂内容を検討・審議する。

・メンバー

- 都銀、地銀、信託、第二地銀、信用金庫、信用組合、労金連、農林中金、商工中金、生保、損保、証券、クレジット
- コンピュータメーカー、システムインテグレータ、通信会社
- 日本銀行
- 弁護士、大学の研究者
- 金融庁（オブザーバー）



FISCガイドラインの位置付け

金融庁　金融検査マニュアル（改訂案）
「オペレーショナル・リスク管理態勢の確認検査用チェックリスト（案）」

（別紙2）

Ⅰ．経営陣によるシステムリスク管理態勢の整備・確立状況

【検証ポイント】

・検査官は、システムリスクの**管理態勢に問題が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、「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」（財団法人金融情報システムセンター編）等**に基づき確認する。

（別紙2）

Ⅲ．個別の問題点

3．防犯・防災・バックアップ・不正利用防止

（5）コンティンジェンシープランの策定

（iii）コンティンジェンシープランの整備にあたっては、**「金融機関等コンティンジェンシープラン（緊急時対応計画）策定のための手引書」（財団法人金融情報システムセンター編）**を参照しているか。

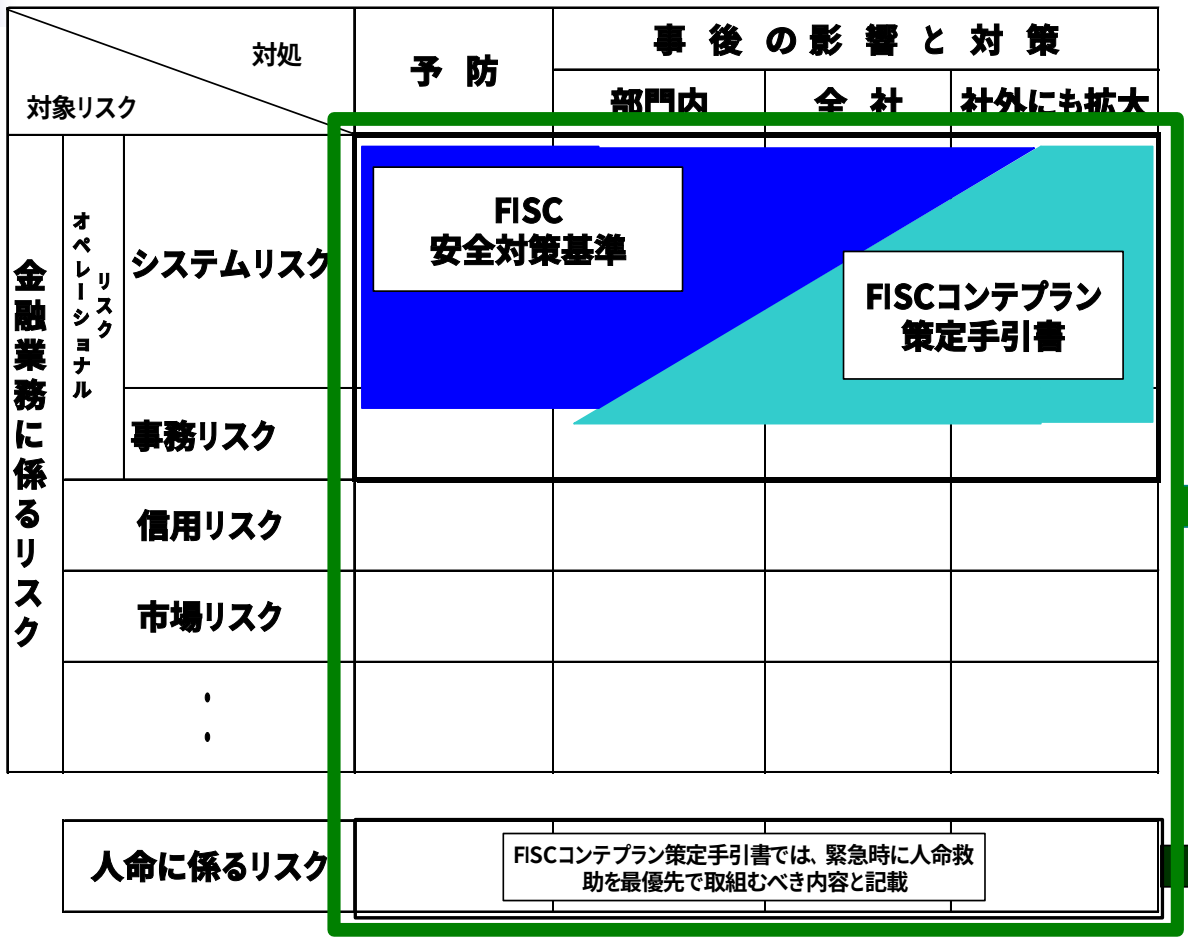
FISCガイドラインの位置づけ

重要インフラにおける「安全基準等」

金融	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 金融機関等におけるコンティンジェンシープラン策定のための手引書 金融機関等におけるセキュリティポリシー策定のための手引書

（平成18年11月27日　重要インフラ専門委員会　第7回会合）

FISCガイドラインの位置づけ



BCP(Business Continuity Plan):
BCPとは、潜在的損失によるインパクト(影響)の認識を行い実行可能な継続戦略の策定と実施および事故発生時の事業継続を確実にする継続計画である。事故発生時に備えて開発、編成、維持されている手順および情報を文書化した事業継続の成果物である。

3．FISCガイドライン
「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」

改訂履歴および改訂ポイント

■**初版策定（1985年12月、基準項目数：226）**

金融機関等のコンピュータシステムの共通的なよりどころとして、 FISCにおいて金融業界の意のもとで策定

■**改訂第2版（1991年2月、基準項目数：252）**

①本部・営業店の防犯対策 ②無人運転/自動運転の対策 ③顧客データの保護 ④暗証番号・パスワード等が他人に知られないための対策 ⑤端末機器の安全対策 ⑥パッケージ導入時の安全対策 ⑦コンピュータウイルスに対する対策

■**改訂第3版（1998年7月、基準項目数：272）**

①ｾｷｭﾘﾃｨﾎﾟﾘｼｰ/ｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝの策定 ②ｸﾗｲｱﾝﾄｻｰﾊﾞｰ・ｼｽﾃﾑの安全対策 ③オープンネットワーク利用時の安全対策（不正アクセス対策等） ④顧客情報管理厳正化（帳票の取扱、システムの廃棄等） ⑤蓄積データ／伝送データの漏洩防止（重要なデータの暗号化） ⑥電子的価値の保護（ICカード等の耐タンパー性、暗号化） ⑦バックアップセンターの保有 ⑧コンピュータウイルス等に対する防御・検知・復旧方法

■**改訂第4版（2000年7月、基準項目数：295）**

①アウトソーシングの安全対策 ②インストアブランチの安全対策 ③コンビニATMの安全対策 ④デビットカードの安全対策 ⑤オープンネットワークを利用した金融サービスの安全対策 ⑥電子メールの利用時の安全対策 ⑦不正取引の検知（マネーロンダリング対策、カード不正使用対策）

改訂履歴および改訂ポイント

■**改訂第5版（2001年9月、基準項目数：297）**

①アウトソーシング活用時のセキュリティポリシーのあり方　②コンティンジェンシープランの位置付け　③金融機関等の合併等に伴う対応　④インターネットを利用した金融サービスの多様化に伴う対応　⑤カードの多様化に伴う対応（ICカード等）　⑥システムの24時間運転に伴う対応　⑦他業態からの新規参入等に伴う対応⑧ハイテク犯罪への対応（ホームページ改ざん等）

■**改訂第6版（2003年10月、基準項目数：299）**

①経営層の関与について見直し　②安全対策基準の対象システムに資金決済システムを追加　③コンティンジンシープランにおけるバックアップの考え方を整理　④アウトソーシングの安全対策強化　⑤**サイバーテロに関する記述追加**　⑥設備関連最新技術反映　⑦事故・犯罪対策強化　⑧関連ガイドライン等の取り込み

■**改訂第6版追補（2005年3月、基準項目数：301）**

個人情報保護法全面施行に伴い情報漏洩対策拡充、生体認証情報の管理追加

■**改訂第6版追補2（2005年12月、基準項目数：303）**

偽造・盗難キャッシュカード対策

■**改訂第7版（2006年3月、基準項目数：304）**

インターネットバンキング対策等

[参照法令等]
法令等～建築基準法、電気事業法、不正アクセス禁止法、労働者派遣事業法　預金者保護法　他
海外・国内規格等～BS7799　他
海外・国内ガイドライン等～FSA個人情報保護法ガイドライン・実務指針、全銀協ガイドライン　他
金融検査マニュアル　　等

(参考) インターネットバンキング利用状況

	金融機関数 （有効回答数）	サービス契約口座数 （有効回答数）
2004年3月	359 （ 464 ）	14,319,949 （ 299 ）
2005年3月	361 （ 456 ）	16,319,721 （ 256 ）
2006年3月	410 （ 478 ）	20,811,913 （ 312 ）

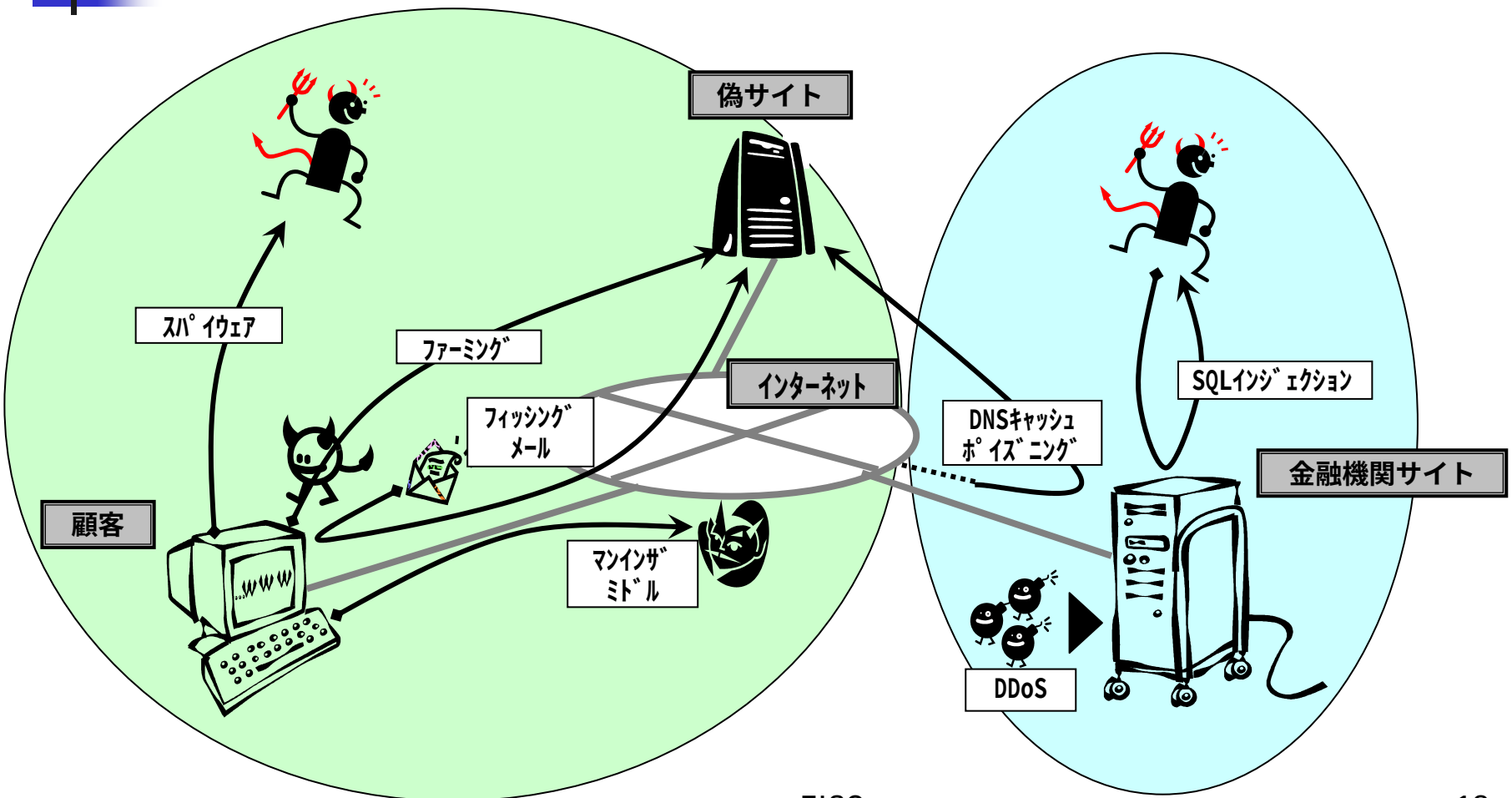
(FISC「金融情報システム白書」より)

(参考) モバイルバンキング利用状況

	金融機関数 （有効回答数）	サービス契約口座数 （有効回答数）
2004年3月	275 （ 464 ）	13,166,454 （ 294 ）
2005年3月	367 （ 456 ）	15,515,919 （ 256 ）
2006年3月	390 （ 477 ）	19,073,220 （ 290 ）

(FISC「金融情報システム白書」より)

(参考) インターネットにおける犯罪例



セキュリティ対策例

サイバー攻撃とその対策

- ネットワークセキュリティ対策の強化
- 「重要インフラの情報セキュリティ対策に係る行動計画」（平成17年12月13日）

【運103】（参考）

（詳細は、FISC「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」（第7版）をご確認ください。）

セキュリティ対策例

システム構築

- 不正プログラムへの防御対策　【技49】
- セキュアプログラミング技法
⇒セキュアプログラミングを考慮しシステム構築　【技10】
- 不正プログラムの検知策や、その他システムの正当性を検証する対策
⇒アクセス履歴、資源管理、ライブラリ管理など　【技50】
- 不正プログラムによる被害時対策構築　【技51】

（詳細は、FISC「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」（第7版）をご確認ください。）

セキュリティ対策例

セキュリティ評価

- ファイアウォールのセキュリティ評価箇所
⇒外部ネットワーク側、内部ネットワーク側
- ペネトレーションテスト

【技43】

- WEBアプリケーションの監査（評価）を定期的あるいはシステム変更時に実施

【技49】

（詳細は、FISC「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」（第7版）をご確認ください。）

セキュリティ対策例

暗号化対策

- SSL暗号鍵長128ビット
- 技術の進歩により暗号は脆弱になること、より安全性の高い暗号方式の採用
- 2010年問題
- 「電子政府推奨暗号リスト」

【運29】（参考）

（詳細は、FISC「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」（第7版）をご確認ください。）

セキュリティ対策例

運用管理など

•修正プログラミングの適用タイミング
⇒外部ネットワークとの接続部分の機器については、
インターネットからの不正アクセスや攻撃を受ける
危険性を考慮し、速やかに適用

【運56】

•不正行為の対する既存の対応事例などを情報収集し、防御対策、検知対策の参考とする

【運103】

（詳細は、FISC「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」（第7版）をご確認ください。）

セキュリティ対策例

認証方式（その1）

金融庁「情報セキュリティに関する検討会」（2006年3～6月）
－対策のあり方－
•インターネットバンキングにおける認証方式については、個々の認証方式が、各種犯罪手口に対してどの程度の強度を有するかを検証した上で、選択すべき。

（リスク分析に基づく認証方式の選択）
（金融庁HPより引用）

セキュリティ対策例

認証方式（その2）

FFIEC（Federal Financial Institutions Examination Council、
連邦金融機関検査協議会）
2005年10月「Authentication in an Electronic Banking Environment」
⇒ 「記憶認証」「所持認証」「生体認証」

「複数要素認証」「二要素認証」といった言葉だけが先行

- **認証方式によってリスクに対する耐性が異なる。**
- **こうしたリスクに対する耐性を分析した上で、適切な認証方式を採用する。**

【技35】（参考）（2007年3月、第7版追補改訂）

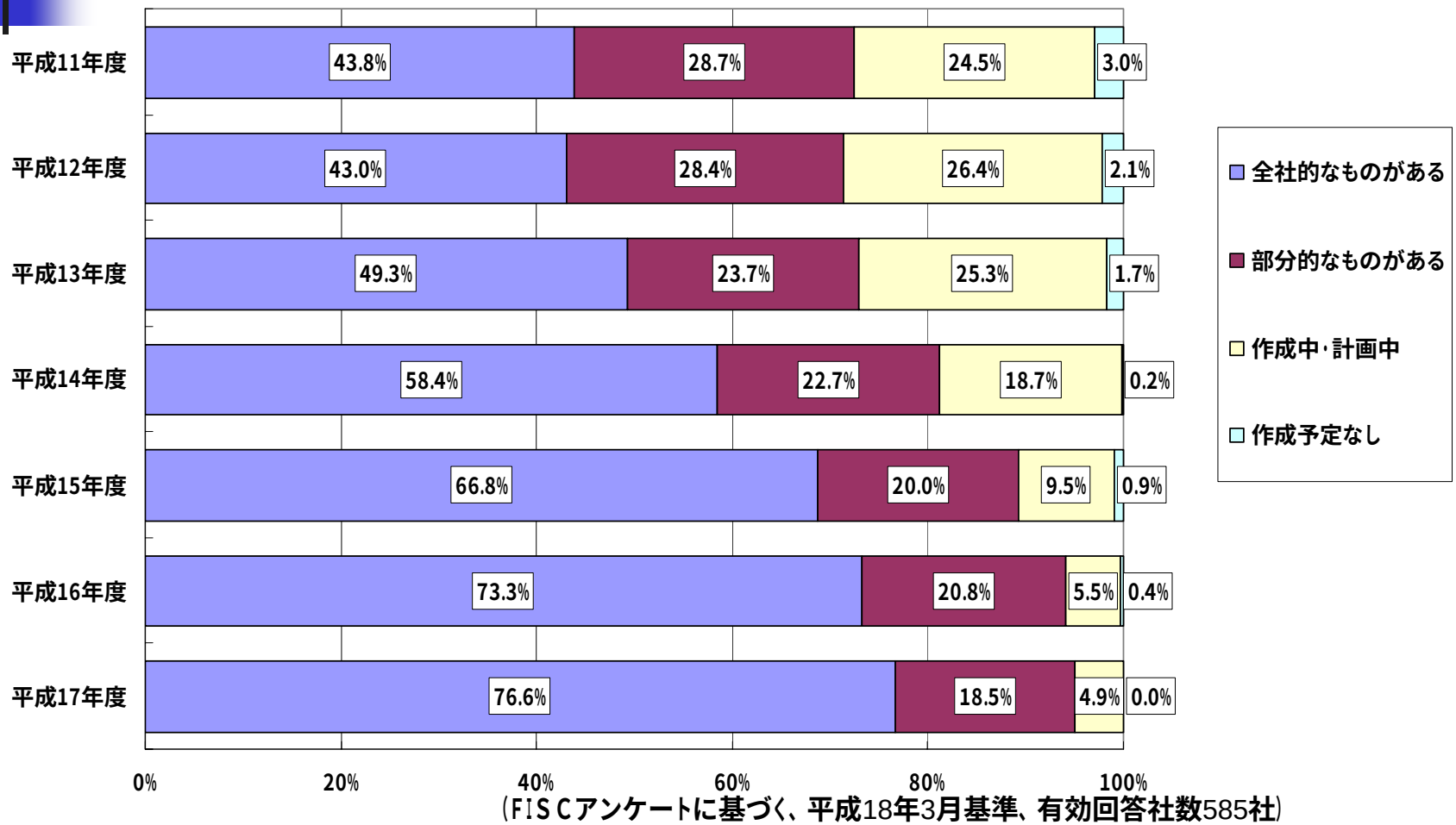
4．FISCガイドライン

「金融機関等におけるコンティンジェンシープラン策定のための手引書」

コンティンジェンシープランに盛り込まれる内容

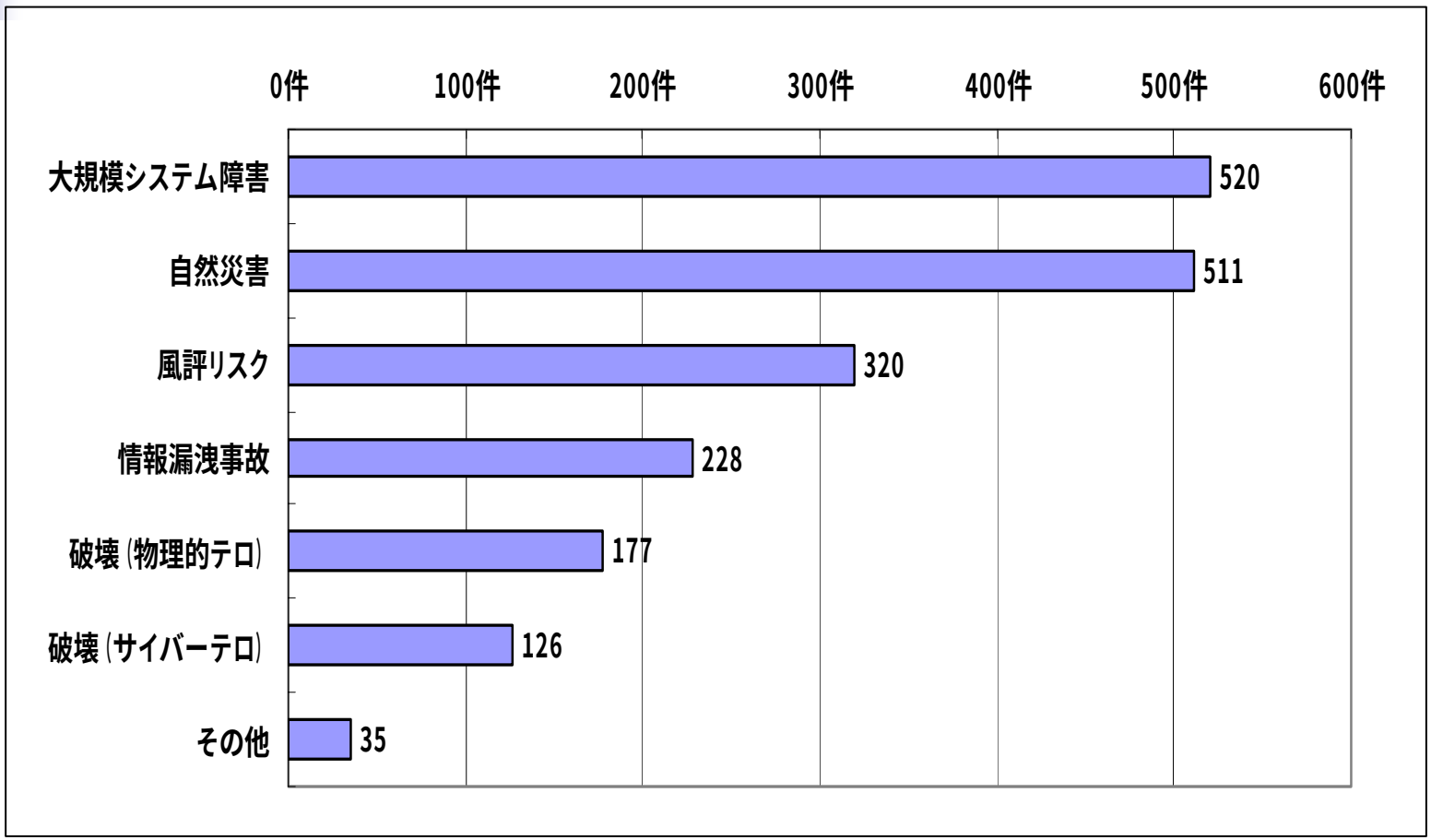
- 想定する緊急事態と被害
- 影響を受ける業務
- 業務の優先度
- 代替手段を用いた業務の継続方法
- 必要となるリソース
- 緊急時体制
- 緊急時行動計画（初期対応・暫定対応・復旧対応）
- 教育・訓練、維持管理方法

コンティンジェンシープラン策定状況



（FISCアンケートに基づく、平成18年3月基準、有効回答社数585社）

コンティンジェンシープラン策定時の想定リスク



（FISCアンケートに基づく、平成18年3月は有効回答社数555社、複数回答あり）

ご清聴ありがとうございました。