IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NIST SP800シリーズに見る BCPとContingency Planning

2006年2月1日

独立行政法人　情報処理推進機構

研究員　菅野　泰子

http://www.ipa.go.jp/security/

本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. **BCP/BCMをめぐる議論**
3. NIST SP800シリーズと
   FISMA導入プロジェクト
4. SP800-53 推奨セキュリティ管理策
5. SP800-34 IT緊急時対応計画

   Contingency Planning Guide for Information Technology Systems
   (ITシステムのための緊急時対応計画ガイド)　(January 2004)

はじめに：BCP/BCMをめぐる議論 (1)

BCP/BCMの重要性

- 企業経営の重要課題としてBCM（事業継続管理）が優先順位を上げてきている
- そこで、最初に各組織がBCP（事業継続計画）を策定することが推奨される
- サプライチェーンを構成する全企業でBCPを構築する必要がある
- BCPは、リスクの種類を問わず、重要業務を継続するという目的意識で策定される
- BCPは計画であり、それを組織内に浸透させ活用するためのBCMが必要である

社会的影響度

災害、事件・事故発生時の影響度の違いにより対応が異なる

- 国家安全保障レベル
- 重要インフラやライフライン
- 政府、自治体関係
- 民間企業（大企業、中小企業、IT関連企業、ITユーザ企業等々）

事業継続業務の優先度

- 組織において、全ての業務・事業の停止リスクへの対応は現実的ではない
- 継続業務の優先順位付けが必要。これは、重要な経営判断である

はじめに：BCP/BCMをめぐる議論 (2)

事業継続にかかわるリスクは多種多様である

- リスクに応じ対応が異なるため、全リスクを視野に入れてBCPを策定するのは難しい
  - 自然災害：地震、津波、雪害、雪崩、台風、洪水,旱魃、飢饉、伝染病 (SARS、鳥インフルエンザ)
  - 人為的：　偶発的：火事、交通事故、ガス爆発、水や空気の汚染、停電、通信障害
  - 意図的：テロ (サイバーテロ、生物・化学兵器の使用) 、戦争、暴動、ストライキ、犯罪、放火、電磁波
  - (NFPA 1600:2004　Annex A　(Explanatory Material)　を参照)
- 国際規格では、多くのリスクに適用できるよう共通の枠組みを提供をしている
- 実際にBCPを策定する際には、想定リスクを特定するほうが現実的
- 様々な業種業態に応じ、想定リスクが異なるため、具体的な策定例がほしい
  - 【経済産業省】事業継続策定ガイドライン　http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf
  - ケーススタディ：大規模システム障害、セキュリティインシデント、情報漏えい・データ改ざん
  - 【内閣府】事業継続ガイドライン 第一版　http://www.bcijapan.jp/documents/guideline01.pdf
  - 事業継続計画の文書構成モデル例　http://www.bousai.go.jp/MinkanToShijyou/shiryou4.pdf
  - 日本では最大の自然災害リスクである地震を想定リスクとして、社内の取組みをスタートさせることを推奨

BCPにおけるIT-BCPの重要性

- 産業や政府活動、国民生活の多くが情報システムや情報通信に依存している
- よって、BCPにおける情報及び情報システムの扱いは重要である = IT-BCPは重要
- 但し、IT-BCPを組織全体のBCP/BCMと連携させて考える必要がある。

本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. BCP/BCMをめぐる議論
3. **NIST SP800シリーズと FISMA導入プロジェクト**
4. SP800-53 推奨セキュリティ管理策
5. SP800-34 IT緊急時対応計画

   Contingency Planning Guide for Information Technology Systems
   (ITシステムのための緊急時対応計画ガイド) (January 2004)

NIST SP800シリーズの中のIT-BCP関連文書

NIST : National Institute of Standards and Technology （米国国立標準技術研究所）

緊急時対応計画

SP800-34 Contingency Planning Guide for Information Technology Systems
（ITシステムのための緊急時対応計画ガイド） (June 2002)

インシデント対応

SP800-61 Computer Security Incident Handling Guide (January 2004)
（コンピュータインシデント対応ガイド）

SP800-83 Guide to Malware Incident Prevention and Handling (November 2005)
（不正プログラムインシデント防止・対応ガイド）

推奨管理策

SP800-53 Recommended Security Controls for Federal Information Systems (February 2005)
連邦政府情報システムにおける推奨セキュリティ管理策

セキュリティ分類

FIPS 199 Standards for Security Categorization of Federal Information and Information Systems (February 2004)
連邦政府の情報および情報システムに対するセキュリティ分類基準

監査（自己監査と第三者監査）

Draft SP800-26 Rev1, Guide for Information Security Program Assessments and System Reporting Form (August 15, 2005)
(SP 800-26 Security Self-Assessment Guide for Information Technology Systems (November 2001))
ITシステムのためのセキュリティ自己アセスメントガイド

Draft SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems (July 15,2005)
連邦政府情報システムにおけるセキュリティ管理策アセスメントガイド

リスクマネジメント

SP800-30 Risk Management Guide for Information Technology Systems (July 2002)
ITシステムのためのリスクマネジメントガイド

NIST文書などの翻訳・調査研究プロジェクト

http://www.ipa.go.jp/security/publications/nist/index.html
http://www.nri-secure.co.jp/news_alert/report/nist/nist_report.html

NIST :
National Institute of Standards and Technology
米国国立標準技術研究所

SP800シリーズ:
SP=Special Publications
NIST CSD (Computer Security Division)
が発行するITセキュリティ関係のガイドライン
NIST CSD: http://csrc.nist.gov/

FIPS:

Federal Information Processing Standards
米国商務長官の承認を受けて、NISTが公布した情報技術関連の連邦政府基準

シリーズNo.(原文発行年月)	タイトル	掲載(予定)
SP 800-26 ※ (2001年11月)	ITシステムのためのセキュリティ自己アセスメントガイド Security Self-Assessment Guide for Information Technology Systems	2005年8月
SP 800-33 (2001年12月)	ITセキュリティのための基本テクニカルモデル Underlying Technical Models for Information Technology Security	2005年8月
SP 800-35 (2003年10月)	ITセキュリティサービスガイド Guide to Information Technology Security Services	2005年8月
SP 800-42 (2003年10月)	ネットワークセキュリティテストにおけるガイドライン Guideline on Network Security Testing	2005年8月
SP 800-50 (2003年10月)	ITセキュリティの意識向上およびトレーニングプログラムの構築 Building an Information Technology Security Awareness and Training Program	2005年8月
SP 800-55 (2003年07月)	情報技術システムのためのセキュリティメトリクスガイド Security Metrics Guide for Information Technology Systems	2005年8月
SP 800-61 (2004年01月)	コンピュータインシデント対応ガイド Computer Security Incident Handling Guide	2005年8月
SP 800-64 (2004年06月)	情報システム開発ライフサイクルにおけるセキュリティの考慮事項 Security Considerations in the Information System Development Life Cycle	2005年8月
[更新 05/12/28] SP 800-34 (2002年06月)	ITシステムのための緊急時対応計画ガイド Contingency Planning Guide for Information Technology Systems	2005年11月
NEW! SP 800-30 (2002年07月)	ITシステムのためのリスクマネジメントガイド Risk Management Guide for Information Technology Systems	2006年1月
SP 800-53 (2005年02月)	連邦政府情報システムにおける推奨セキュリティ管理策 Recommended Security Controls for Federal Information Systems	2006年2月

FISMA導入プロジェクト (FISMA Implementation Project)

FISMA：連邦情報セキュリティマネジメント法)

情報セキュリティに関する文書の策定、実装、運用を行うことにより、情報及び情報システムのセキュリティを強化することを米連邦政府機関に義務付け

"Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

--- **Federal Information Security Management Act of 2002 (*Title III of the E-Government Act*)**

NISTのFISMA導入プロジェクト

目的：連邦政府の情報セキュリティ強化に寄与する (FISMAへの準拠)

フェーズI： FISMA関連のセキュリティ基準 (FIPS) およびガイドライン(SPシリーズ) の開発
(1-2の文書を残し、ほとんど完成)

フェーズII：セキュリティサービスプロバイダ認定プログラムの開発 (2006年より開始)

フェーズIII：セキュリティ・ツール検証プログラムの開発 (開始時期未定)

Flagship Standard：FIPS199 (FIPS: Federal Information Processing Standards)

組織や組織の資産に対する脅威の影響度を算定し、影響度により各情報システムを低・中・高に分類するための基準。 低位・中位・高位に分類することにより、情報セキュリティ対策の優先順位を明確にし、各レベルに応じた管理策を選択 → **セキュリティ対策コストの適正化**

FIPS/SPシリーズ: 政府、民間を問わず、セキュリティ担当者にとって有益な文書群

FISMA導入プロジェクト
リスクマネジメントフレームワーク(RMF)

開始点

(FIPS199/SP800-60)

セキュリティ分類

情報資産に対する潜在的な脅威の影響度に基づき、情報システムを低位・中位・高位に分類する。

(FIPS200/SP800-53)

セキュリティ管理策の選択

情報システムを保護するための最低限のセキュリティ管理策を低位・中位・高位の分類に応じて選択する。

(SP800-37)

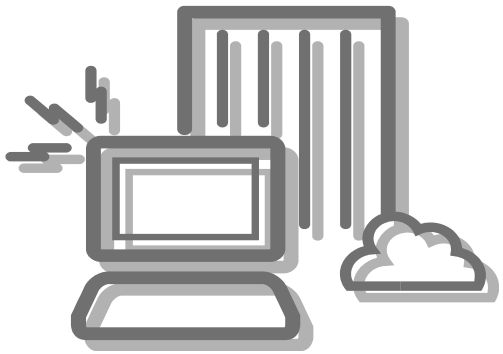
セキュリティ管理策実施状況の監視

セキュリティ管理に影響を及ぼす情報システムへの変更を継続的に監視し、管理策の有効性を評価する。

(SP800-53/
FIPS200/SP800-30)

選択したセキュリティ管理策の微調整

リスクアセスメントを行い、組織の状況、求められる脅威への対策および、政府機関それぞれに特有な要件に基づく最低限の管理策を調整する。



(SP800-37)

システムの運用認可

政府機関の業務や資産、人員へのリスクを判断し、容認可能な場合は、情報システムの運用を承認する 。

(SP800-18)

セキュリティ管理策の文書化

システムセキュリティ計画において、情報システムのセキュリティ要件の概要を提供し、計画・実施されるセキュリティ管理策を文書化する 。

(SP800-70)

セキュリティ管理策の導入

新／旧情報システムにおいて、セキュリティ管理策を導入する。
(セキュリティ構成管理チェックリストも導入)

(SP800-53A/SP800-26/
SP800-37)

セキュリティ管理策の評価

セキュリティ管理策がどの程度まで正しく導入され、意図した通りに運用され、セキュリティ要件に見合う成果を上げているかを判断する。

本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. BCP/BCMをめぐる議論
3. NIST SP800シリーズと
   FISMA導入プロジェクト
4. **SP800-53 推奨セキュリティ管理策**
5. SP800-34 IT緊急時対応計画

   Contingency Planning Guide for Information Technology Systems
   (ITシステムのための緊急時対応計画ガイド)　(January 2004)

SP800-53 推奨セキュリティ管理策

Recommended Security Controls for Federal Information Systems (February 2005)

IPA

シリーズNo.	タイトル	翻訳掲載予定
SP 800-53	**連邦政府情報システムにおける推奨セキュリティ管理策** Recommended Security Controls for Federal Information Systems **第2章:セキュリティ管理策の選択と特定に関連する基本概念** 管理策の分類（管理策の構成と分類）、共通管理策と最低限の管理策 管理策の有効性評価、維持管理 **第3章　セキュリティ管理策の選択と特定のためのプロセス** 組織のリスクマネジメントとベースライン管理策の選択、管理策の補正 **付録：管理策の選択、特定に関する詳細な情報を提供** 定義及び用語、セキュリティレベル低・中・高それぞれの情報システムに対する最低限の管理策一覧、管理策の基本カタログ、他の標準の管理策への対応表	2006年4月予定
SP800-53 **Annex 1**	連邦政府情報システムにおける推奨セキュリティ管理策 **セキュリティレベル低における必要最低限の管理策** Recommended Security Controls for Federal Information Systems Minimum Security Controls/Low Baseline	2006年4月予定
SP800-53 **Annex 2**	連邦政府情報システムにおける推奨セキュリティ管理策 **セキュリティレベル中における必要最低限の管理策** Recommended Security Controls for Federal Information Systems Minimum Security Controls/Moderate Baseline	2006年4月予定
SP800-53 **Annex 3**	連邦政府情報システムにおける推奨セキュリティ管理策 **セキュリティレベル高における必要最低限の管理策** Recommended Security Controls for Federal Information Systems Minimum Security Controls/High Baseline	2006年4月予定

SP800-53の管理策ーファミリ、クラス、識別子

クラス*	ファミリ	識別子
管理	リスクアセスメント	RA
管理	計画	PL
管理	システムおよびサービスの調達	SA
管理	認証、認可、およびセキュリティアセスメント	CA
運用	人的セキュリティ	PS
運用	物理的および環境的な保護	PE
運用	緊急時対応計画 (Contingency Planning)	CP
運用	構成管理	CM
運用	保守	MA
運用	システムおよび情報の完全性	SI
運用	記録媒体の保護	MP
運用	インシデント対応 (Incident Response)	IR
運用	意識向上および訓練	AT
技術	識別および認証	IA
技術	アクセス制御	AC
技術	監査および責任追跡性	AU
技術	システムおよび通信の保護	SC

17のファミリと163の管理策

(管理策、補足ガイダンス、管理強化策)

CP-1 緊急時対応計画の方針と手順

管理策
補足ガイダンス
管理強化策

CP-2 緊急時対応計画

CP-3 緊急時対応訓練

CP-4 緊急時対応計画のテスト

CP-5 緊急時対応計画の更新

CP-6 代替格納拠点

CP-7 代替処理拠点

CP-8 電気通信サービス

CP-9 情報システムのバックアップ

CP-10 情報システムの復旧と再構成

* 各ファミリに含まれる管理策の主な特性に基づいて管理・運用・技術のクラスに分類されているが、セキュリティ管理策の多くは複数のクラスに関連付けることができるため、クラス分けは便宜的なもの。

【参考】ISO/IEC17799の管理策(BCP関連)

IPA

ISO/IEC 17799:2005

- Security policy
  セキュリティ基本方針
- Organizing information security
  情報セキュリティのための組織
- Asset management
  資産の管理
- Human resources security
  人的資源のセキュリティ
- Physical & environmental security
  物理的及び環境的セキュリティ
- Communications & operations management
  通信及び運用管理
- Access control
  アクセス制御
- Information systems acquisition, development and maintenance
  システムの取得、開発及び保守
- **Information security incident management**
  情報セキュリティインシデントの管理
- **Business continuity management**
  事業継続管理
- Compliance
  順守

11の管理領域と133の管理策

(管理策、実施の手引き、関連情報)

14.1 Information security aspects of business continuity management
(事業継続管理における情報セキュリティの側面)

14.1.1 Including information security in the business continuity management process
(事業継続管理手続への情報セキュリティの組込み)

14.1.2 Business continuity and risk assessment
(事業継続及びリスクアセスメント)

14.1.3 Developing and implementing continuity plans including information security
(情報セキュリティを組み込んだ事業継続計画の策定及び実施)

14.1.4 Business continuity planning framework
(事業継続計画策定の枠組み)

14.1.5 Testing, maintaining and re-assessing business continuity plans
(事業継続計画の試験、維持及び再評価)

※日本語訳は暫定的な仮訳

SP800-53 付録F:セキュリティ管理策カタログ

CP-9　情報システムのバックアップ

管理策：

組織は、情報システムに含まれるシステムレベルの情報（システム状態情報を含む）を［*組織が定義した頻度*］でバックアップし、バックアップ情報をバックアップにふさわしい安全な立地場所に保管する。

補足ガイダンス：

情報システムのバックアップ頻度、および代替格納拠点へのバックアップ情報の転送速度**は**（そのように指定されている場合）、組織のリカバリータイムおよびリカバリーポイントの目標と整合が取れている。

管理強化策：

(1)組織は、記録媒体の信頼性と情報の完全性を保証するために、バックアップ情報のテストを*［組織が定義する頻度］*で行う。

(2)組織は、緊急時対応計画のテストの一環として、情報システム機能の復元時にバックアップ情報を選択的に使用する。

(3)組織は、オペレーティングシステムおよびそのほかのきわめて重要な情報システムソフトウェアのバックアップコピーを、運用中のソフトウェアとは同一の場所ではない、離れた場所にあるファシリティまたは耐火性容器に格納する。

低　CP-9	**中**　CP-9 (1)	**高**　CP-9 (1) (2) (3)

SP800-53 付録D：セキュリティ管理策一覧(抜粋)

管理番号	管理名	管理ベースライン		
		低	中	高
緊急時対応計画				
CP-1	緊急時対応計画の方針と手順	CP-1	CP-1	CP-1
CP-2	緊急時対応計画	CP-2	CP-2 (1)	CP-2 (1)
CP-3	緊急時対応訓練	**選択せず**	CP-3	CP-3 (1)
CP-4	緊急時対応計画のテスト	**選択せず**	CP-4 (1)	CP-4 (1) (2)
CP-5	緊急時対応計画の更新	CP-5	CP-5	CP-5
CP-6	代替格納拠点	**選択せず**	CP-6 (1)	CP-6 (1) (2) (3)
CP-7	代替処理拠点	**選択せず**	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	電気通信サービス	**選択せず**	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	情報システムのバックアップ	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	情報システムの復旧と再構成	CP-10	CP-10	CP-10 (1)
事故対応				
IR-1	インシデント対応の方針と手順	IR-1	IR-1	IR-1
IR-2	インシデント対応の訓練	**選択せず**	IR-2	IR-2 (1) (2)
IR-3	インシデント対応のテスト	**選択せず**	IR-3	IR-3 (1)
IR-4	インシデントの処理と対応	IR-4	IR-4 (1)	IR-4 (1)
IR-5	インシデントの監視	**選択せず**	IR-5	IR-5 (1)
IR-6	インシデントの報告	IR-6	IR-6 (1)	IR-6 (1)
IR-7	インシデント対応の支援	IR-7	IR-7 (1)	IR-7 (1)

FIPS199
SP800-60
各情報システムを低･中･高に分類

組織や組織の資産に対する脅威の影響度を算定し、影響度により低位･中位･高位に分類

低：限定的な悪影響
中：重大な悪影響
高：致命的又は壊滅的な悪影響

SP800-53
低･中･高のセキュリティレベルに応じ、管理策を選択

他の管理策とSP800-53の比較(BCP関連)
- SP800-53 付録G: セキュリティ管理策のマッピング(抜粋)

IPA

管理番号	管理名	ISO 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3
緊急時対応計画						
CP-1	緊急時対応計画の方針と手順	5.1.1, 10.4.1 14.1.1, 14.1.3 15.1.1	9.	---	COBR-1 DCAR-1	2.B.4.e(5) 6.B.1.a(1)
CP-2	緊急時対応計画	10.3.2, 10.4.1 10.8.5, 14.1.3 14.1.4	4.1.4, 9.1.1 9.2, 9.2.1 9.2.2, 9.2.3 9.2.10, 12.1.8 12.2.2	SC-3.1 SC-1.1	CODP-1 COEF-1	6.B.2.b(1)
CP-3	緊急時対応訓練	14.1.3 14.1.4	9.3.2	SC-2.3	PRTN-1	8.B.1
CP-4	緊急時対応計画のテスト	10.5.1, 14.1.5	4.1.4, 9.3.3	SC-3.1	COED-1	6.B.3.b(2)(b)
CP-5	緊急時対応計画の更新	14.1.3, 14.1.5	9.3.1, 9.3.3 10.2.12	SC-2.1 SC-3.1	DCAR-1	6.B.3.b(2)
CP-6	代替格納拠点	10.5.1	9.2.4, 9.2.5 9.2.7, 9.2.9	SC-2.1 SC-3.1	CODB-2	6.B.2.a(2) 6.B.3.a(2)(d)
CP-7	代替処理拠点	14.1.4	9.1.3, 9.2.4, 9.2.5, 9.2.7, 9.2.9,	SC-2.1 SC-3.1	COAS-1, COEB-1 COSP-1, COSP-2	6.B.3.a(2)(d)
CP-8	電気通信サービス	14.1.4	---	---	---	6.B.2.a(4)
CP-9	情報システムのバックアップ	10.5.1, 11.7.1	9.1.1, 9.2.6, 9.2.9, 9.3.1, 12.1.9	SC-2.1	CODB-1, CODB-2 COSW-1	6.B.1.a(2)
CP-10	情報システムの復旧と再構成	14.1.4	9.2.8	SC-2.1	COTR-1, ECND-1	4.B.1.a(4) 6.B.1.a(1) 6.B.2.a(3)(d)

ISO/IEC17799とSP800-53の比較(BCP関連)

(参考) SP800-53：セキュリティ管理策のマッピング

管理番号	SP800-53 管理名	ISO/IEC FDIS 17799:2004/11/28
CP-1	緊急時対応計画の方針と手順 Contingency planning policy and procedures	5.1.1 Information security policy document 10.4.1 Controls against malicious code 14.1.1 Including information security in the business continuity management process 14.1.3 Developing and implementing continuity plans including information security 15.1.1 Identification of applicable legislation
CP-2	緊急時対応計画 Contingency plan	10.3.2 System acceptance 10.4.1 Controls against malicious code 10.8.5 Business information systems 14.1.3 Developing and implementing continuity plans including information security 14.1.4 Business continuity planning framework
CP-3	緊急時対応訓練 Contingency training	14.1.3 Developing and implementing continuity plans including information security 14.1.4 Business continuity planning framework
CP-4	緊急時対応計画のテスト Contingency plan testing	10.5.1 Information back-up 14.1.5 Testing, maintaining and re-assessing business continuity plans
CP-5	緊急時対応計画の更新 Contingency plan update	14.1.3 Developing and implementing continuity plans including information security 14.1.5 Testing, maintaining and re-assessing business continuity plans
CP-6	代替格納拠点 Alternate storage	10.5.1 Information back-up
CP-7	代替処理拠点 Alternate processing sites	14.1.4 Business continuity planning framework
CP-8	電気通信サービス Telecommunications services	14.1.4 Business continuity planning framework
CP-9	情報システムのバックアップ Information system backup	10.5.1 Information back-up 11.7.1 Mobile computing and communications
CP-10	情報システムの復旧と再構築 Information system recovery and reconstitution	14.1.4 Business continuity planning framework

(参考) 政府機関統一基準と ISO/IEC17799:2005, NIST SP800-53との対応

出典：内閣官房情報セキュリティセンター
政府機関統一基準とISO/IEC17799:2005等との対応について
http://www.bits.go.jp/active/general/pdf/rel2005_iso.pdf

管理番号	基本／強化	遵守事項 （2005年12月13日政策会議決定：NISD-K303-052）	ISO/IEC17799 :2005	NIST SP800-53
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				
6.3.2(1)(a)	基本	最高情報セキュリティ責任者は、府省庁におけるBCPの整備計画について統括情報セキュリティ責任者を通じ情報セキュリティ委員会が適時に知ることができる体制を構築すること。	14.1.1	CP-2
6.3.2(1)(b)	基本	統括情報セキュリティ責任者は、府省庁においてBCPの整備計画を把握した場合は、その内容を情報セキュリティ委員会並びに必要に応じて情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者に連絡すること。	14.1.1	CP-2
(2)BCPと情報セキュリティ対策の整合性の確保				
6.3.2(2)(a)	基本	情報セキュリティ委員会は、府省庁においてBCP又は省庁対策基準の整備計画がある場合には、BCPと省庁対策基準との整合性の確保のための検討を行うこと。	14.1.4	CP-2
6.3.2(2)(b)	基本	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁においてBCPの整備計画がある場合には、すべての情報システムについて、当該BCPとの関係の有無を検討すること。	14.1.2	CP-2
6.3.2(2)(c)	基本	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システムセキュリティ責任者及び課室情報セキュリティ責任者は、府省庁においてBCPの整備計画がある場合には、当該BCPと関係があると認めた情報システムについて、以下に従って、BCPと省庁対策基準に基づく共通の実施手順を整備すること。	14.1.3/14.1.5	CP-5
6.3.2(2)(c)(ア)	基本	通常時においてBCPと省庁対策基準の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。	14.1.3/14.1.5	CP-5
6.3.2(2)(c)(イ)	基本	事態発生時においてBCPと省庁対策基準の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定の整備を行うこと。	14.1.3/14.1.5	CP-5
(3)BCPと情報セキュリティ関係規程の不整合の報告				
6.3.2(3)(a)	基本	行政事務従事者は、府省庁においてBCPの整備計画がある場合には、BCPと情報セキュリティ関係規程が定める要求事項との違いなどにより、実施の是非の判断が困難な場合には、関係者に連絡するとともに、統括情報セキュリティ責任者が整備した障害等が発生した際の報告手順により、情報セキュリティ責任者にその旨を報告して、指示を得ること。	14.1.4	CP-2

本資料は、政府機関統一基準の各遵守事項について、国際的な規格であるISO/IEC17799:2005及び米国政府機関が作成した文書であるNIST SP800-53の管理策のうち関連性があると認められる箇所の項目番号を示したものです。
なお、政府機関統一基準については、政府機関における情報セキュリティに特化して作成されていることから、一方に含まれる事項に相対する他方の事項が存在しない場合があります。例えば、要員審査や雇用条件に関する対策について、ISO/IEC17799:2005では言及されていますが、政府機関においては国家公務員法等により別途規定されているため、政府機関統一基準の対象外になっています。

IT-BCPに関する更に詳細なガイドライン

SP800-53の管理策ファミリ CP(緊急時対応計画)、IR (インシデント対応) は、ITBCPに関する項目を網羅的に含んでいる。しかし、実際に組織の中で管理体制を確立し、維持継続するためには、**更に詳細なガイドラインが必要**。
さらには、**組織全体のBCMの中に、ITBCPを位置づける必要がある。**
SDLC (**システム開発ライフサイクル**:System Development Life Cycle **も考慮すべき。**

参照

IT緊急時対応計画

SP800-34 Contingency Planning Guide for Information Technology Systems
(ITシステムのための緊急時対応計画ガイド) (January 2004) 107 pages

インシデント対応

SP800-61 Computer Security Incident Handling Guide (January 2004) 148 pages
(コンピュータインシデント対応ガイド)
SP800-83 Guide to Malware Incident Prevention and Handling (November 2005)
(不正プログラムインシデント防止・対応ガイド) 101 pages

その他: SP800-12 An Introduction to Computer Security: The NIST Handbook (October 1995)
第11章 「Preparing for Contingencies and Disasters」

本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. BCP/BCMをめぐる議論
3. NIST SP800シリーズと
   FISMA導入プロジェクト
4. SP800-53 推奨セキュリティ管理策
5. **SP800-34 IT緊急時対応計画**

   Contingency Planning Guide for Information Technology Systems
   （ITシステムのための緊急時対応計画ガイド） （January 2004）

SP800-34: IT緊急時対応計画のポイント

1. **目的、範囲、対象とする読者 (誰が何のためにどのように利用するか明確)**
2. **IT緊急時対応計画と事業継続計画等各計画の位置づけ**
3. **緊急時対応計画とリスクマネジメントプロセス**
4. **緊急時対応計画とシステム開発ライフサイクル**
5. **緊急時対応計画策定プロセスにおける7つのステップ**
   (1)緊急時対応計画ポリシーステートメントの策定　(2)ビジネスインパクト分析の実施
   (3)予防対策の特定　(4)復旧戦略の策定　(5)IT緊急時対応計画の策定
   (6)テスト、訓練、演習の計画　(7)計画の保守
6. **豊富なテンプレートと付録 (計画管理ツールとしても利用可能)**
7. **技術的考慮事項と人的考慮事項**

SP800-34：目的、範囲、対象とする読者

IT緊急時対応計画：
緊急事態発生後の重要なITサービスの継続、復旧のための幅広い対策範囲を規定

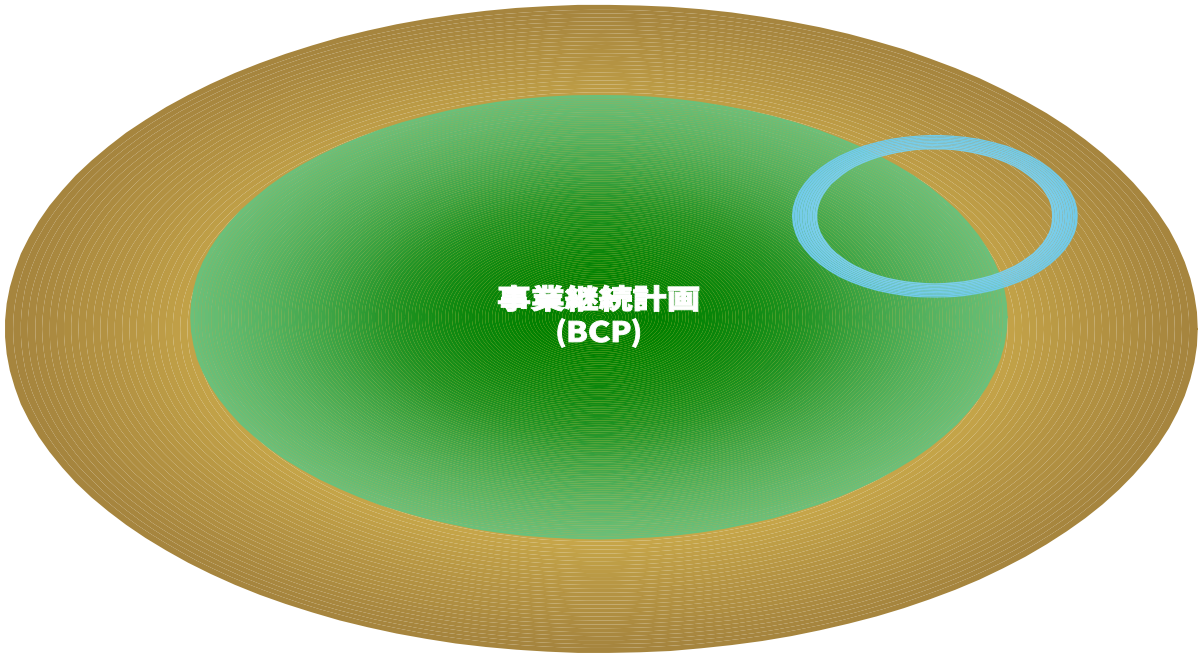
本ドキュメントの目的：
効果的な計画策定、保守を行うための基本的な原則および実施例を提示
IT緊急時対応計画策定のための、体系的で費用対効果の高いソリューションの提供

範囲：
ITシステムの運用に影響を及ぼす各種のインシデントに適用できる計画原則について概略を説明。短期の中断をもたらすインシデントから、長期的影響を及ぼす災害までを対象。
次の一般的なIT処理システムに対する緊急時対応計画原則を説明。
・デスクトップコンピュータやポータブルシステム　・サーバー　・メインフレーム　・分散システム
・ウェブサイト　・ローカルエリアネットワーク (LAN)　・ワイドエリアネットワーク (WAN)

対象とする読者
・IT運用、保守を担当するシステム管理者、ITビジネスを手がけるマネージャー
・情報システムセキュリティ担当者・責任者
・ 組織のITセキュリティ活動の開発、導入、保守を担当するスタッフ
・システムエンジニアおよび設計者　・ITシステムのユーザ等

連邦政府だけでなく、民間または商業組織にも利用可能

SP800-34：BCPプロセス全体における IT緊急時対応計画の位置づけ



説明

施設

IT

ビジネス

特に重要

SP800-34：BCPプロセス全体における IT緊急時対応計画の位置づけ

IPA

計画名	目的	範囲
事業継続計画（BCP）	必要不可欠な業務を継続しながら、重大な中断状態から復旧する手順を提供する。	ビジネスプロセスを扱う。ITについては、ビジネスプロセスのサポートに関するもののみを扱う。
事業復旧（再開）計画（BRP）	災害発生後、迅速に事業運営を回復する手順を提供する。	ビジネスプロセスを扱う。IT特化ではなく、ITについては、ビジネスプロセスのサポートに関するもののみを扱う。
運用継続計画（COOP）	組織において必要不可欠かつ戦略的な機能を代替サイトで最大30日間継続させるのに必要な手順や設備を提供する。	最も重要な組織のミッションのサブセットを扱う。通常は本社レベルに向けて策定される。ITには特化しない。
サポート継続計画/ IT緊急時対応計画	主要なアプリケーションまたは汎用サポートシステムを復旧する手順や能力を提供する。	IT緊急時対応計画と同様、ITシステムの中断を扱い、ビジネスプロセスには特化しない。
緊急時コミュニケーション計画	要員および一般人に現状を報告する手順を提供する。	要員と一般人とのコミュニケーションを扱い、ITには特化しない。
サイバーインシデント対応計画	悪意のあるサイバーインシデントの検知、対応、その影響の低減のための戦略を提供する。	システムおよびネットワークに影響を及ぼすインシデントに対する情報セキュリティ対策を重視する。
災害復旧計画（DRP）	代替サイトでのサービス提供能力の復旧を促進する詳細手順を提供する。	ほぼ、ITに特化している。影響が長期にわたる大規模災害に限定される。
人員緊急時計画（OEP）	物理的な脅威に対し、生命への危険および傷害の発生を最小化し、資産を損害から保護するため、調整された手順を提供する。	特定施設に関連する人員および資産を重視する。ビジネスプロセスまたは、ITシステムの機能性には特化しない。

注：IT緊急時対応計画とその関連計画については、一般的な定義はまだ無く、SP800-34では、
IT緊急時計画に関する共通理解の基盤を提供するために、各計画の目的と範囲について説明している。

SP800-34：緊急時対応計画とリスクマネジメントプロセス

- リスクマネジメント：リスクを特定し、コントロールし、低減するための幅広い活動
- リスクはゼロにはならない → 残存リスクに対応できる緊急時対応計画を策定
- リスクは変化する → 緊急時対応計画の継続的な保守、テスト、レビューが必要

リスクマネジメントプロセスの要素としての緊急時対応計画

リスクマネジメントに関するSPシリーズ文書

SP800-30 Risk Management Guide for Information Technology Systems
ITシステムのためのリスクマネジメントガイド
【リスクアセスメントの実施方法と、適切な技術的、管理的、運用的管理策を選択する方法について、詳細なガイダンスを提供している。】

SP800-34：IT緊急時対応計画と想定する脅威

ITシステムに対する脅威

自然の脅威 - 台風（ハリケーン）、竜巻、洪水、火災など
人的脅威 – 操作ミス、妨害行為、悪意のあるコードの埋め込み、テロ攻撃等
環境的脅威 – 機器故障、ソフトウェアエラー、通信ネットワークの切断、停電等

SP800-34 IT緊急時対応計画の対応する脅威

上の脅威のうち、サイバー攻撃（サービス拒否、ウイルスなど）への対応については取り上げない。同様に、本ドキュメントでは、不法侵入、サービス拒否攻撃、悪意のあるロジックの注入などのサイバー犯罪に対するコンピュータフォレンジック分析による証拠保存に関連する、インシデント対応についても記述していない。
（これらの種類の対応には、IT緊急時対応計画の対象範囲外の内容が含まれているため。）

インシデント対応に関するSPシリーズ文書

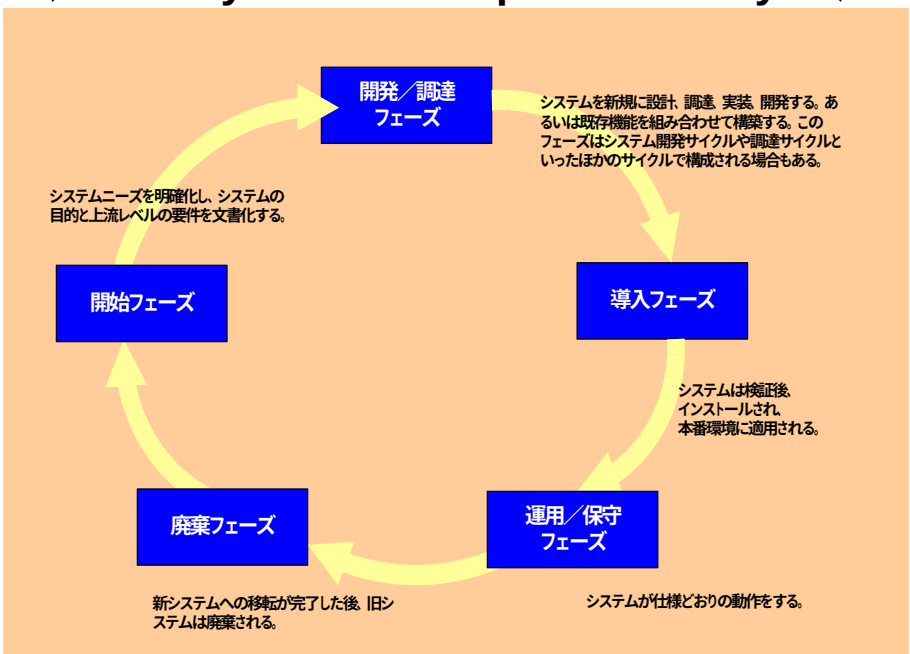
SP800-61 Computer Security Incident Handling Guide (January 2004)
（コンピュータインシデント対応ガイド）

SP800-83 Guide to Malware Incident Prevention and Handling (November 2005)
（不正プログラムインシデント防止・対応ガイド）

SP800-34：緊急時対応計画とシステム開発ライフサイクル(SDLC)

緊急時対応計画は主に運用/保守段階フェーズの活動に関連するが、緊急時対策をSDLC のすべての段階で考慮することで、コスト削減や運用負荷軽減に寄与できる

システム開発ライフサイクル
(SDLC：System Development Life Cycle)



開始フェーズ：
新ITシステムの企画に際し、緊急時対応計画の要件を考慮する

開発/調達フェーズ：
緊急時対応策は、運用要件を反映する

導入フェーズ：
緊急時対応策を検証、テストする

運用/保守フェーズ：
- 緊急時対応計画手順を包含する訓練と意識向上プログラムを整備する
- 定期的にバックアップを実施して、オフサイトに保存する。
- 必要に応じた緊急時対応計画の保守・更新

廃棄フェーズ：
既存システムを撤去し、別のシステムに交換する場合も、緊急事態について考慮する

システム開発ライフサイクルに関するSPシリーズ文書

SP800-64　Security Considerations in the Information System Development Life Cycle
(情報システム開発ライフサイクルにおけるセキュリティの考慮事項)

NIST CSD SDLC Web http://csrc.nist.gov/SDLCinfosec/　　Information Security in the SDLC Brochure

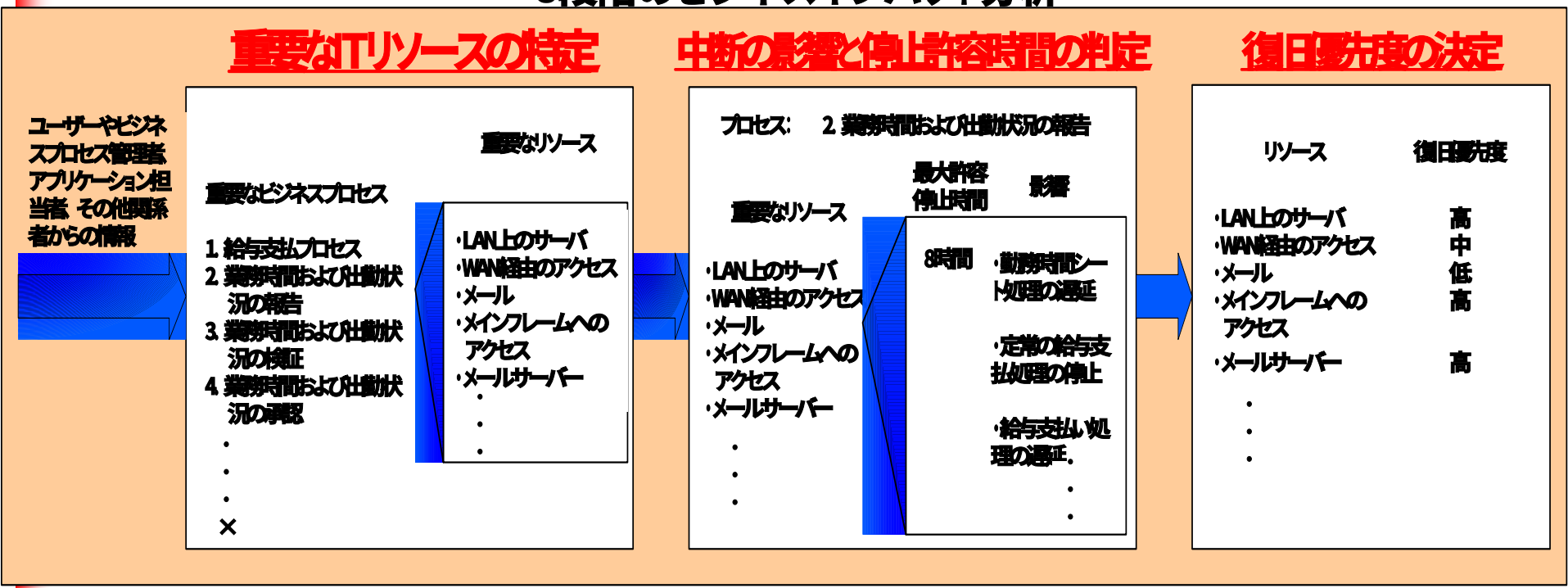
SP800-34：緊急時対応計画策定プロセス 7つのステップ

1. 緊急時対応計画ポリシーステートメントの策定	・緊急時対応計画に 対する法令、規定 の要求事項の特定 ・緊急時対応目標の定義とフレームワークや責務の確定 ・ポリシーの承認・公表
2. 事業影響分析の実施	【緊急時対応要件と優先度の決定】 ・重要なITリソースの特定 ・中断の影響と停止 許容時間の判定 ・復旧優先度の決定
3. 予防対策の特定	・コントロールの導入 ・コントロールの維持
4. 復旧戦略の策定	・復旧手段の特定 ・システムアーキテ クチャへの統合
5. 緊急時対応計画の策定	【IT緊急時対応計画の中核 】 ・復旧戦略の文書化 (対応組織・役割・責任・手順等) ・緊急時対応の詳細ガイダンス
6. テスト、訓練、演習の計画	・テスト目的の明確化 ・テスト合格基準の作成 ・テスト実施により得た教訓の文書化 ・教訓の計画への反映 ・担当者教育
7. 計画の保守	・レビューおよび 更新計画 ・更新の際の内部／外部組織と の調整 ・計画の配布管理 ・変更点の文書化

SP800-34：事業影響分析

ビジネスインパクト分析（ステップ 2）

3段階のビジネスインパクト分析



ビジネスインパクト分析は、緊急時対応計画プロセスにおける主要なステップ
緊急時対応計画コーディネーターは、システム要件、プロセス、および相互依存関係を特定し、緊急時対応要件と優先度を決定することを可能にする。
分析結果は、運用継続計画、事業継続計画、事業復旧計画の分析と戦略策定にも利用

SP800-34：
付録B：ビジネスインパクト分析例とテンプレート

IPA

ビジネスインパクト分析例

モデル：50人のユーザに対応するLANを備えた小規模オフィス
在庫管理や主要なリソースの管理、電子メールやオフィスアプリケーションの利用

ビジネスインパクト分析テンプレート

ユーザがITシステムのビジネスインパクト分析を行う際に役立つように設計。カスタマイズ可能。

予備システム情報

組織:	事業影響分析実施日:
システム名:	事業影響分析 連絡担当窓口:
システムマネージャの連絡先（連絡担当窓口）:	
システムの詳細: 【システムの目的および、システム図を含むアーキテクチャの説明】	
A. システム連絡担当窓口の特定	役割
内部関係者 【システムを使用またはサポートする組織内の人員、職位または事務所を特定する。またシステムとの関連性を明記する】	
・ ・	・ ・
外部関係者 【システムを使用またはサポートする組織外の人員、職位または事務所を特定する。またシステムとの関連性を明記する】	
・ ・	・ ・
B. システムリソースの特定【システムを構成する具体的なハードウェア、ソフトウェア、およびその他のリソースを特定する。数量とタイプも含める】	
ハードウェア ・ ・	
ソフトウェア	

A. システム連絡担当窓口の特定・役割
B. システムリソースの特定
C. 重要な役割の特定
D. 重要な役割とリソースの対応
E. 中断の影響と許容可能な中断時間の特定
A. リソースの復旧優先度の設定

SP800-34：予防対策の特定と復旧戦略の策定

予防対策の特定（ステップ 3）

システムの種類および構成によって利用できる予防対策は多様

共通する対策例：

定期的なバックアップ、バックアップ電力、防火システム、火災および煙検知器　・水や煙センサー
バックアップメディア、耐火性・耐水性コンテナ、・緊急時マスターシステムシャットダウンスイッチ
暗号鍵管理などの技術的なセキュリティコントロールや最小権限によるアクセスコントロール

復旧戦略の策定（ステップ 4）

1) **バックアップ手法**：データの重要性と更新の頻度に応じバックアプ手法を定める
オフサイト施設、ベンダー選択の際の考慮点

2) **代替サイト**：長期にわたる代替施設でのシステム運用が必要な場合を考慮
種類：専用サイト、内部または外部組織との相互契約によるもの、賃貸による商用施設
契約により代替サイト運用の場合に契約に最低限記載すべき内容
分類：コールドサイト、ウォームサイト、ホットサイト、モバイルサイト、ミラーサイト

3) **機器交換**：プライマリサイトが利用できなくなった場合、必要な装置を代替拠点に搬送

4) **役割と責任**：緊急時対応計画コーディネーターが、適切なチームを編成して戦略を導入する

5) **コストの考慮事項**：対処可能な要員と利用可能な予算枠で、効果的に導入されることを確認

SP800-34：テスト、訓練、演習、計画の保守

IT緊急時対応計画の策定（ステップ 5）　（後述）

テスト、訓練、演習の計画（ステップ 6）

テスト、訓練、演習は、緊急時対応能力を実行可能とするのに重要

テストで検証されるべき領域（テスト目標と合格基準の設定）

・代替プラットフォームでのバックアップメディアからのシステム復旧
・復旧チーム間の共同作業　・内部および外部との接続性
・代替装置の使用によるシステム性能　・通常業務の復旧　・通知手順

演習の基本的スタイル：　クラスルーム演習と機能演習（シュミレーションとウォーゲームを含む）

訓練が必要な事項：

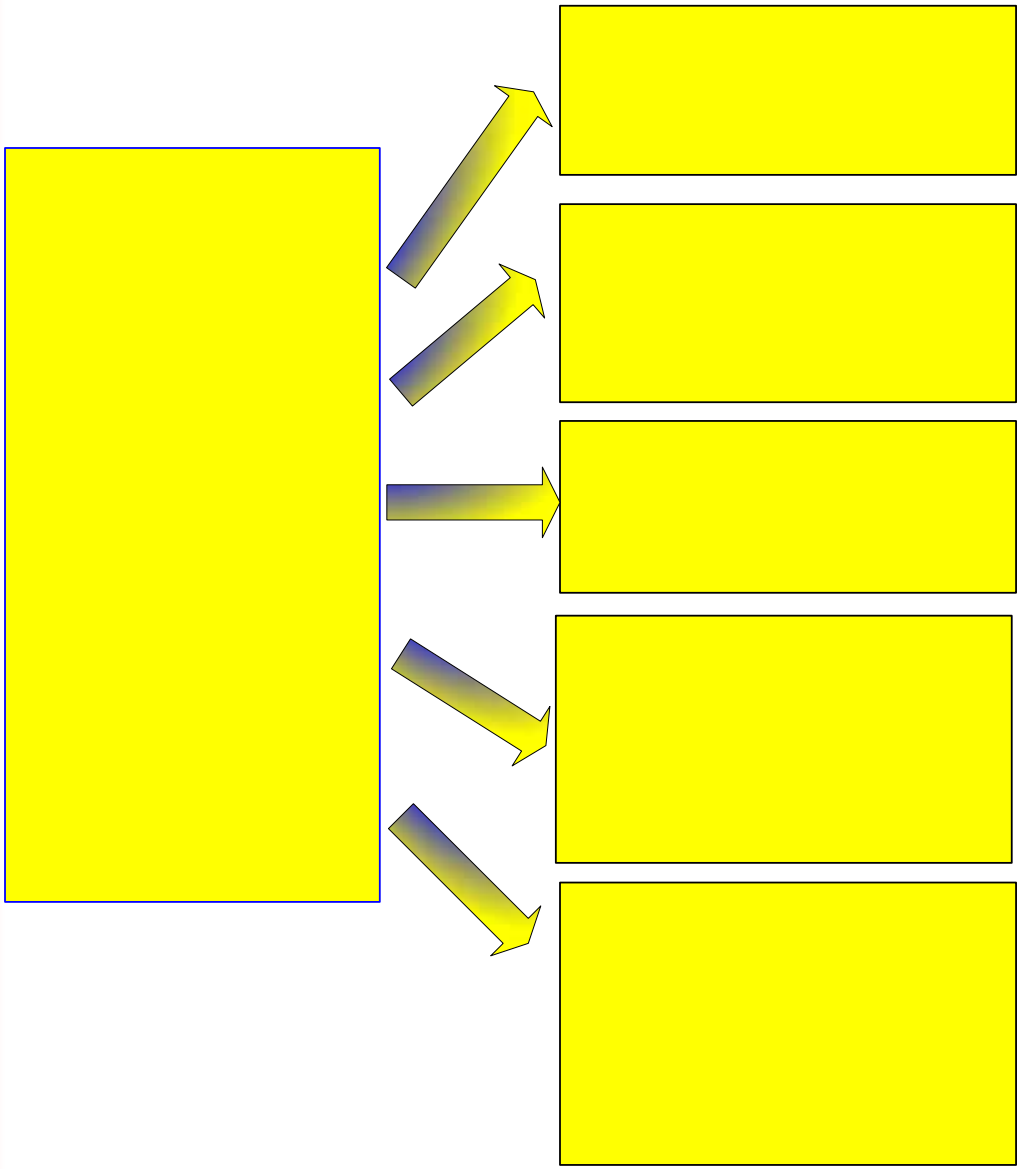
・計画の目的　・チーム間の共同作業およびコミュニケーション　・報告手順
・セキュリティ要件　・チーム固有のプロセス（通知/実行、復旧、再構築フェーズ）
・各自の責任（通知/実行、復旧、再構築フェーズ）

各自の復旧手順がマニュアルがなくても実行できるレベルまで訓練する
（災害発生後の数時間、紙や電子媒体の計画が入手できない事態に備えるため）

計画の保守（ステップ 7）

組織の変更管理プロセスの一部として、緊急時対応計画を定期的にレビューし更新し、
新しい情報の文書化を行う。

SP800-34：緊急時対応計画の策定



付録A：IT緊急時対応計画のフォーマット例

1. はじめに
1.1 目的
1.2 適用範囲
1.3 範囲
1.3.1 計画の原則
1.3.2 想定条件
1.4 参照/要件
1.5 変更の記録
2. 運用のコンセプト
2.1 システムの説明およびアーキテクチャ
2.2 後継者の指定
2.3 責任
3. 通知および実行フェーズ
4. 復旧措置
5. 通常業務への復帰
5.1 並行処理
5.2 計画の終了
6. 計画の付録
    - 要員の連絡先リスト
    - ベンダーの連絡先リスト
    - 機器および仕様
    - サービスレベル契約と同意覚書
    - IT作業標準
    - 事業影響分析
    - 関連する緊急時対応計画
    - 緊急時管理計画
    - 人員緊急時計画
    - 運用継続計画

SP800-34：緊急時対応計画の技術的考慮事項

(策定のプロセス・フレームワークを補完するITシステムに関する情報)

SP800-34では、7種類のプラットフォームに対し推奨する緊急時対応計画について これらのシステムに共通する戦略と手法を提供

7種類のプラットフォーム

- **デスクトップコンピュータ およびポータブルシステム**
- **サーバー**
- **ウェブサイト**
- **ローカルエリアネットワーク**
- **ワイドエリアネットワーク**
- **分散システム**
- **メインフレームシステム**

例：ウェブサイトの緊急時対応策

- ウェブサイトの文書化
- ウェブサイトの適切なコード化、プログラミング
- セキュリティポリシーおよびコントロール との適合
- サポートインフラストラクチャの対応計画の考慮
- 負荷分散の導入
- インシデント対応手順との適合

注：スーパーコンピュータおよび無線ネットワーク向けの緊急時対応計画については触れていないが、ここで述べる原則の多くはこれらのシステムに対しても適用される。

注2：ここで示す情報は、あるITシステムにはあてはまらない可能性もあるため、必要に応じシステムに固有の緊急時対応要件に合致するように修正する必要がある。

SP800-34：緊急時対応戦略の要約

緊急時対応計画での考慮事項	1	2	3	4	5	6	7
システム、設定、およびベンダー情報の文書化	×	×	×	×	×	×	×
各ユーザーに対するデータのバックアップの奨励	×						
適切なコード化、プログラミング、および文書化			×				
緊急時対応策とセキュリティポリシーとの整合性維持	×	×	×	×	×	×	×
緊急時対応策とセキュリティ管理策との整合性維持	×	×	×	×	×	×	×
サポートインフラストラクチャの緊急時対応の考慮			×			×	
ホットサイトと相互補完契約に関する考慮							×
インシデント対応手順への適合			×				
ベンダーとの調整				×	×	×	×
ベンダーとのSLAの設定					×		×
PC上のデータの保存に関するガイダンスの提供	×						
ハードウェア、ソフトウェア、および周辺機器の標準化	×	×				×	
オフサイトでのバックアップメディアの保管	×	×					×
オフサイトでのバックアップの保管	×	×					
緊急時対応策	**1**	**2**	**3**	**4**	**5**	**6**	**7**
システム、アプリケーション、データのバックアップ	×	×					
コンポーネント間の相互運用性の確保	×	×					
単一障害点の特定				×	×		
イメージディスク	×						
重要なコンポーネントでのフォールトトレランスの導入		×					×
負荷分散の導入		×	×				
重要なコンポーネントにおける冗長性の実装	×	×		×	×		×
ストレージソリューションの導入		×					×
リモートアクセスと無線テクノロジーの統合				×			
監視				×			
データの複製		×					×
代替ハードディスクドライブの使用	×						
無停電電源装置の使用	×	×					×

緊急時対応計画での考慮事項では、緊急時対応策を補完する技術的要件または要素を取り上げる。

1. デスクトップコンピュータおよびポータブルシステム
2. サーバー
3. ウェブサイト
4. ローカルエリアネットワーク
5. ワイドエリアネットワーク
6. 分散システム
7. メインフレームシステム

緊急時対応策は技術的な基盤の上に作成され、緊急時対応戦略を導入するために使用される。

SP800-34：
付録D：緊急時対応計画における人的考慮事項

IPA

生命の安全等の「人的考慮事項」は最重要課題

IT緊急時対応計画は、人員緊急時計画、事業継続計画、緊急時コミュニケーション計画などの各計画と整合性をとる必要がある。
特に壊滅的なイベントを想定する場合には、以下の点を十分に考慮する。

- **人員緊急時計画：人員の安全性と撤退計画、退去手順、安否確認手順・方法**
  定期的な避難訓練、退避の際の人員確認の手順
- **地域の消防署、警察署、レスキュー組織との連携：事前の関係構築**
- **コミュニケーション計画: 組織内での内部伝達と外部関係者への伝達窓口や手順**
- **人員の福利厚生：深刻な状況下では、人的問題への対処が、事業再開よりも優先**
  避難所、就業場所、人材調達、災害後の悲嘆へのカウンセリング

参考URL(米国)：
人員の安全性と撤退計画： www.gsa.gov, www.fema.gov , www.americanredcross.org
連邦従業員援助プログラムに関する情報: www.opm.gov/ehs/Eappage.htm
非営利団体の災害時支援情報: www.americanredcross.org/services/disaster
緊急時対応計画および管理: www.contingencyplanning.com
障害復旧研究所インターナショナル (Disaster Recovery Institute International) : www.dr.org
障害復旧ジャーナル (Disaster Recovery Journal) : www.drj.com
国家非常事態管理局: www.nemaweb.org

まとめ

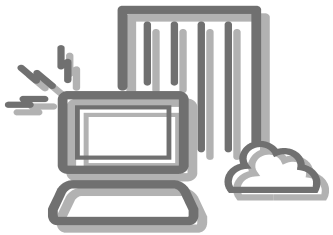
IPA

(FIPS200/ SP800-53)
セキュリティ管理の選択

開始点 (FIPS199/ SP800-60)
セキュリティの分類

(SP800-37)
セキュリティ管理策実施状況の監視

(SP800-53/ FIPS200/SP800-30)
選択したセキュリティ管理の調整



(SP800-37)
システム運用の承認

(SP800-18)
セキュリティ管理策の文書化

(SP800-70)
セキュリティ管理策の導入

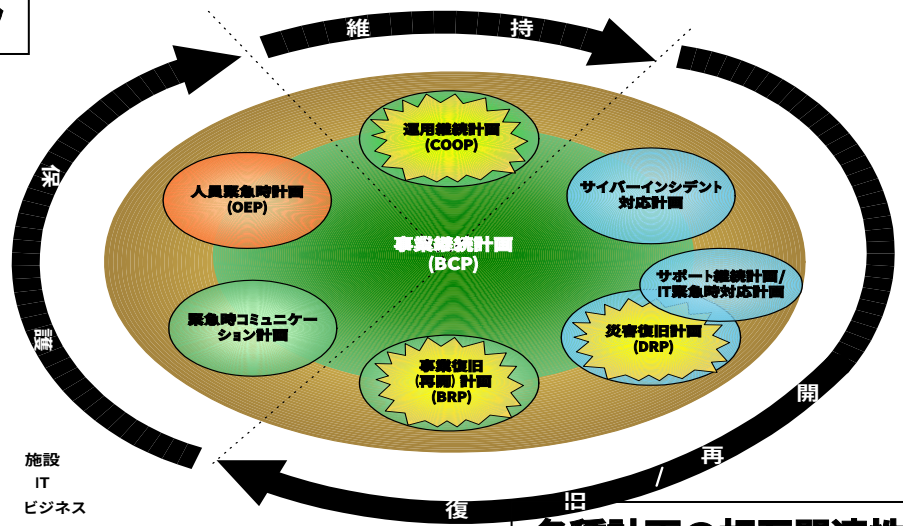
(SP800-53A/SP800-26/SP800-37)
セキュリティ管理策の評価

FISMA　リスクマネジメントフレームワーク

FIPS199　セキュリティ分類
SP800-53　管理策の選定
SP800-34　IT緊急時対応計画
SP800-61　インシデント対応

事業継続は、情報セキュリティ対策において重要な対策項目である

IT-BCPを組織全体のBCP/BCMとどう連携させるか、どのように位置づけて機能させるかを考えることで、BCPへの理解や取組みが進む。



各種計画の相互関連性

独立行政法人　情報処理推進機構
セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
　文京グリーンコートセンターオフィス１６階
ＴＥＬ　０３（５９７８）７５０８　　ＦＡＸ　０３（５９７８）７５１８
電子メール　isec-info@ipa.go.jp
ＵＲＬ　http://www.ipa.go.jp/security/