

公認内部監査人



Certified
Internal
Auditor

■ Part III ②

Business Knowledge for Internal Auditing
内部監査のためのビジネス知識



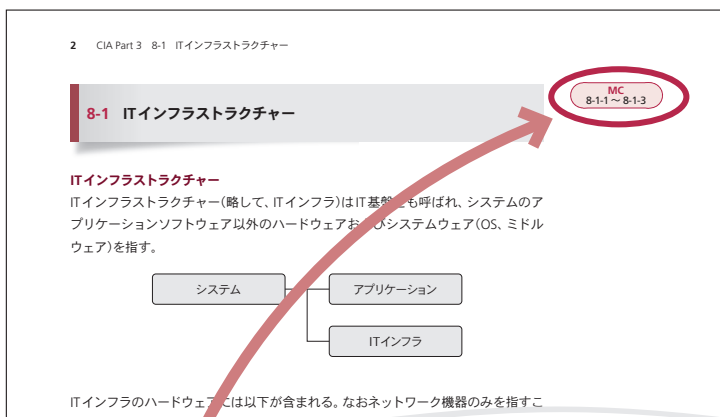
本書について

本テキストは、CIA 試験の出題範囲を基に、CIA 試験対策上重要な論点及び関連する内部監査の専門職の実施の国際フレームワーク(The International Professional Practices Framework; IPPF)の内容を取り入れ、受講生の皆様が理解しやすいように構成しています。

テキスト・MCカードの特徴

テキスト

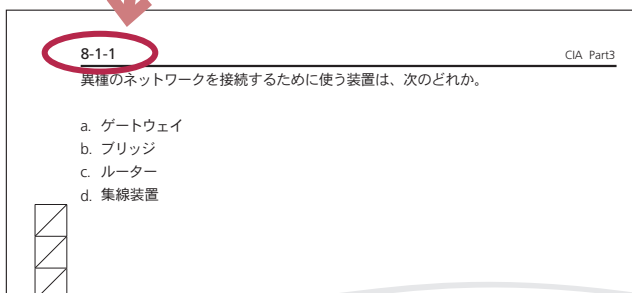
本テキストの最大の特徴は、CIA 試験の問題を解くために習得すべき知識を、短時間で学習できる小さなユニットに分けて解説している点にあります。また、各ユニットに結び付く MC 問題を、タイトルの横に明示してあります。



テキストを読み、eラーニングやライブ講義を視聴した後は、時間を空けずに該当問題を解くことで、そのつど早めに知識を定着させることを心がけて下さい。

MCカード

CIA 試験合格のために取り組んでおくべき問題を厳選して掲載してあります。また、可能な限り、誤答の選択肢についても解説を加えています。



誤答の選択肢についても、それが誤答となる理由をしっかりと検討しましょう。そうすることで、本試験での応用力・得点力が大きく改善します。

間違えた問題、理解が不十分であると感じる論点については、テキストの該当ユニット、及び関連講義に戻り、一つ一つ弱点を減らして行きましょう。

本書の使い方

■用語解説アイコン
(下記参照)

AZ
表面利率は表示された利率

■トピックタイトル
そのユニットで学ぶトピックのタイトルです。

■MCカード問題番号
ユニットに結び付くMCカードの問題番号です。

11-2 GAAPの構成要素 (2)会計原則

論点
原則には以下の4つの原則がある。

取得原主義	資産や負債を客観的に評価する原則	ある原価
収益認識	履行義務が満たされた時点で収益を認識する。	評価方法
収益費用の対応の原則	収益の獲得の過程で発生した費用は、関連する収益に対応させる。	
完全開示の原則	財務諸表はその利用者が意思決定を行う上で十分な情報を提供しなければならない。	

■例アイコン
(下記参照)

e.g.
販売費と一般管理費の按分

■補足アイコン
(下記参照)

完全開示の原則
財務諸表を

■豊富な図解
視覚的に理解することで学習時間を大幅に短縮できます。

■論点
重要学習ポイントについては論点タイトルが表示されています。

■豊富な図解
視覚的に理解することで学習時間を大幅に短縮できます。

額面レート > 実効利率
元本 = \$100,000
額面レート < 実効利率

社債の券面額と発行価格が元 (premium) 発行
社債の券面額と発行価格が元本 (discount) 発行

発生主義の原則
利益

発生原価
未消費の原価
消費された原価
費用
次期以降の費用
収益

アイコンについて



補足
本文に記載されていること
の背景等を知ること
により理解が深まります。



用語
本文記載の専門用語
について説明しています。



参照
具体例でイメージを持つ
ことにより、概念を自分
なりに理解できます。

CONTENTS

8

ITインフラストラクチャー
_____ 1

2	8-1	ITインフラストラクチャー
4	8-2	ネットワーク (1)対象地域による分類
6	8-3	ネットワーク (2)プロトコルによる分類
8	8-4	ネットワーク (3)情報処理方法による分類
12	8-5	音声通信
13	8-6	ITに関わる内部監査部門の役割
16	8-7	職務の分離

9

ITコントロール・
フレームワーク、
災害復旧 _____ 21

22	9-1	ITコントロール
24	9-2	ITコントロールの分類
25	9-3	ITコントロール・フレームワーク
32	9-4	情報システムの構築による影響
34	9-5	データ処理方法
36	9-6	アプリケーション統制 (1)入力
38	9-7	アプリケーション統制 (2)処理
41	9-8	アプリケーション統制 (3)出力
42	9-9	不測事態対応計画
46	9-10	バックアップ

10

情報セキュリティ _____ 49

50	10-1	ITに係るリスク
53	10-2	情報セキュリティとサイバー・セキュリティ
56	10-3	全般統制 物理的コントロール
58	10-4	全般統制 論理的コントロール
61	10-5	インターネットセキュリティ
65	10-6	データの保存に係るセキュリティ
67	10-7	情報の保護
72	10-8	データ保護法令
74	10-9	最新のテクノロジーとセキュリティへの影響

11

財務会計 _____ 79

80	11-1	GAAPの構成要素 (1)前提
81	11-2	GAAPの構成要素 (2)会計原則
82	11-3	GAAPの構成要素 (3)制約
83	11-4	損益計算書
87	11-5	貸借対照表と株式持分計算書
89	11-6	現金
90	11-7	売掛金
92	11-8	棚卸資産
98	11-9	有形固定資産
100	11-10	無形資産
101	11-11	現在価値
104	11-12	社債
107	11-13	リース
110	11-14	有価証券
115	11-15	収益認識 原則と例外
124	11-16	連結財務諸表、持分法

12

財務(ファイナンス) ____ 137

138	12-1	短期ファイナンス (1)日数計算
140	12-2	短期ファイナンス (2)比率計算
141	12-3	短期ファイナンス (3)在庫管理
146	12-4	短期ファイナンス (4)金利計算
151	12-5	長期投資の意思決定 (1)現在価値を考慮しない
155	12-6	長期投資の意思決定 (2)現在価値を考慮する
160	12-7	長期資金調達 (1)株主資本コスト
166	12-8	長期資金調達 (2)負債コスト
167	12-9	長期資金調達 (3)加重平均資本コスト
174	12-10	長期ファイナンスの比率分析 (1)レバレッジ分析
177	12-11	長期ファイナンスの比率分析 (2)株式に対する分析
178	12-12	株主資本利益率(ROE)

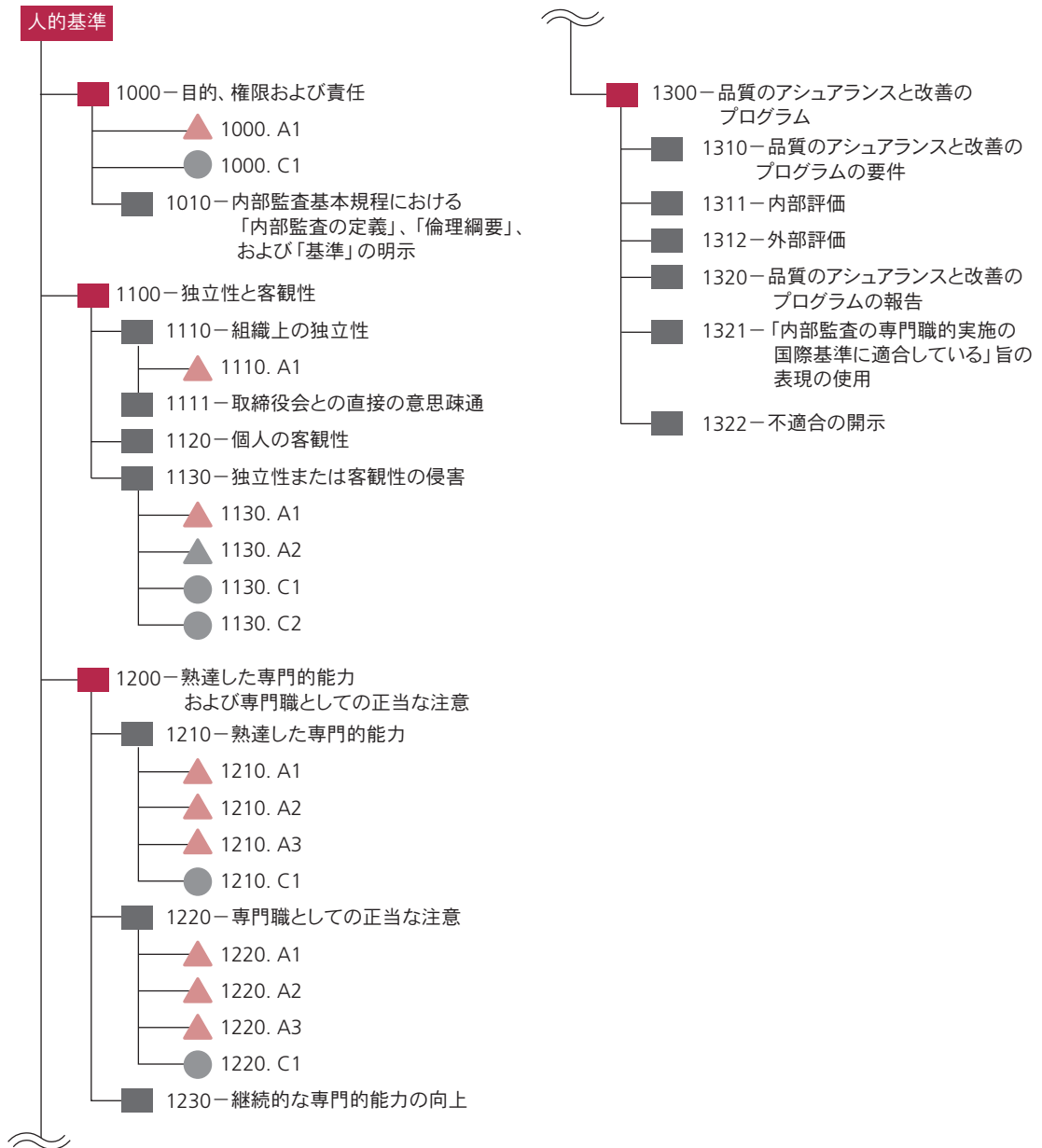
13

管理会計 _____ 183

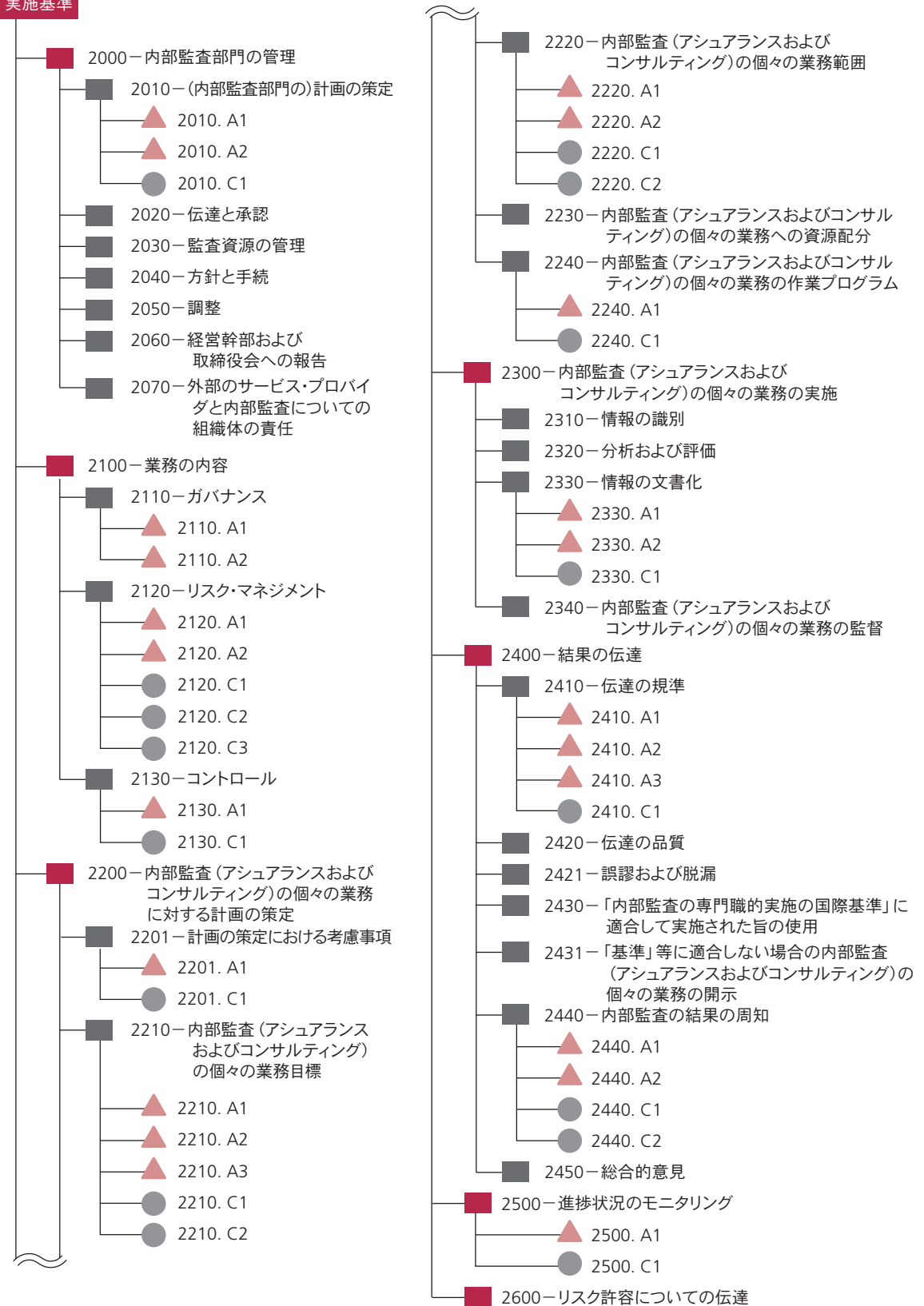
184	13-1 原価の分類
187	13-2 原価計算の流れ
189	13-3 製造間接費の配賦
193	13-4 活動基準原価計算(ABC)
197	13-5 個別原価計算
200	13-6 総合原価計算 (1)概論
201	13-7 総合原価計算 (2)加重平均法
203	13-8 総合原価計算 (3)先入先出法
205	13-9 CVP分析 (1)前提条件
207	13-10 CVP分析 (2)基本公式
210	13-11 CVP分析 (3)安全余裕率
211	13-12 直接原価計算
215	13-13 増分原価分析
218	13-14 基本予算
219	13-15 固定予算と変動予算
221	13-16 標準原価計算
224	13-17 責任会計
226	13-18 移転価格

Index _____ 230

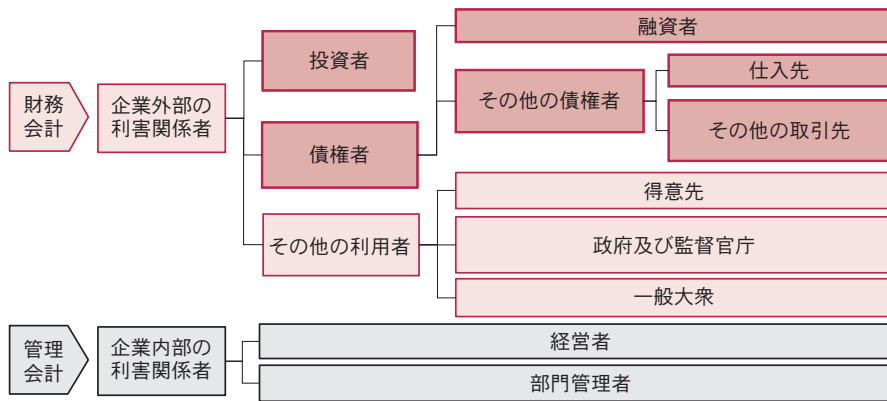
内部監査の専門職的实施の国際基準



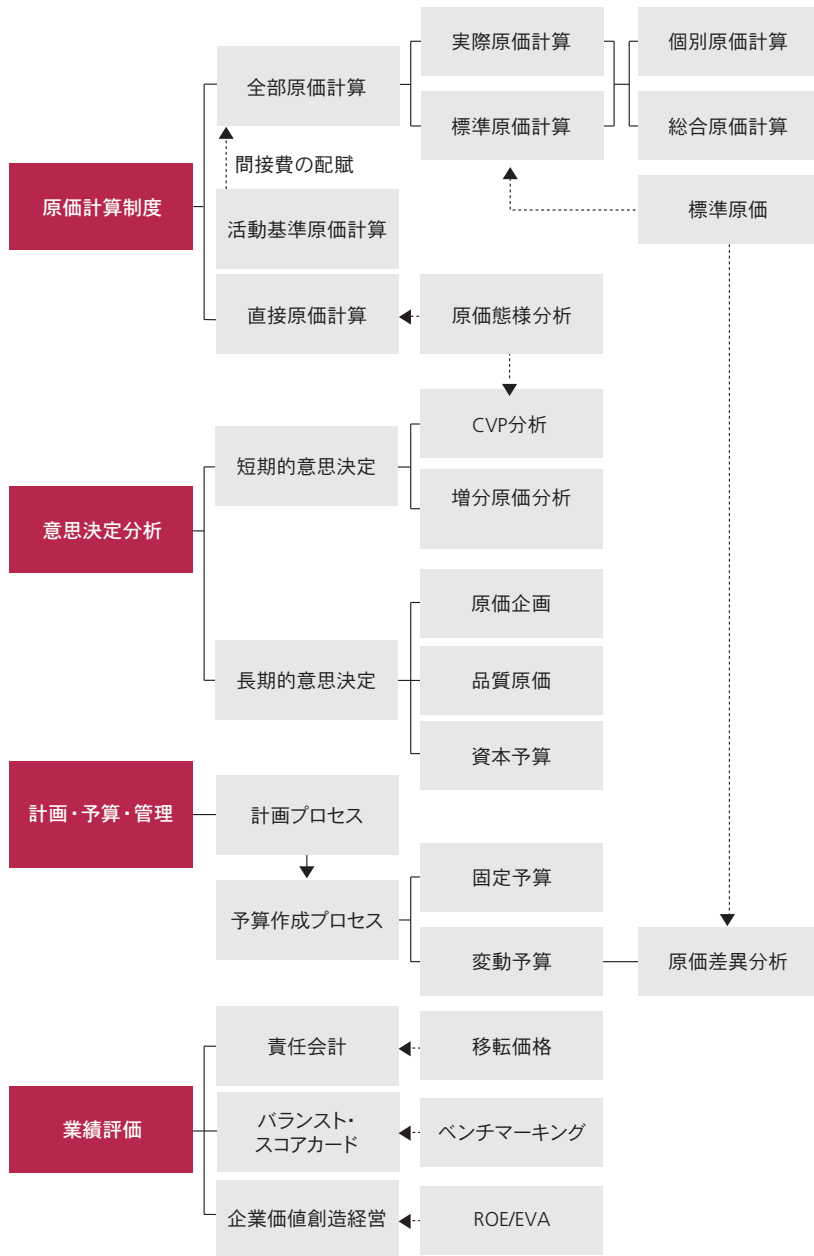
実施基準



〈財務会計と管理会計〉



〈主な管理会計〉



Part 3 コースシラバス

			ページ
第5回	Chapter 8	ITインフラストラクチャー	2
	Chapter	ITコントロール・フレームワーク、災害復旧	5
	9-1 ~ 9-8		41
第6回	Chapter	ITコントロール・フレームワーク、災害復旧	42
	9-9 ~ 9-10		5
	Chapter 10	情報セキュリティ	78
第7回	Chapter	財務会計	79
	11-1 ~ 11-11		5
			103
第8回	Chapter	財務会計	104
	11-12 ~ 11-16		5
	Chapter	財務(ファイナンス)	150
第9回	Chapter	財務(ファイナンス)	151
	12-5 ~ 12-12		5
			182
第10回	Chapter	管理会計	183
	13-1 ~ 13-8		5
			204
第11回	Chapter	管理会計	205
	13-9 ~ 13-18		5
			229



Chapter 9 Contents

□ 9-1	ITコントロール	22
□ 9-2	ITコントロールの分類	24
□ 9-3	ITコントロール・フレームワーク	25
□ 9-4	情報システムの構築による影響	32
□ 9-5	データ処理方法	34
□ 9-6	アプリケーション統制 (1)入力	36
□ 9-7	アプリケーション統制 (2)処理	38
□ 9-8	アプリケーション統制 (3)出力	41
□ 9-9	不測事態対応計画	42
□ 9-10	バックアップ	46

9-1 ITコントロール

ITコントロール

- a) IPPFでは、ITのコントロール手段を以下のように定義する。

定義 アプリケーション、情報、インフラストラクチャーおよび人といった、情報技術(IT)の基盤にかかる全般的および技術的なコントロール手段を提供するだけでなく、経営の管理やガバナンスを支援するコントロール手段。

ITコントロールは、ビジネスに係るコントロールの自動化と、情報技術(IT)そのもののコントロールという2つの要素がある。この定義は、ITコントロールが全ITインフラストラクチャーに対する全般的かつ技術的なコントロールを提供すると同時に、ビジネスマネジメントとガバナンスに対する支援を担うことを示している。

- b) IIAの発行するGTAG 1「ITコントロール」では、より具体的に、ITコントロールを以下のように説明している。

ITコントロールは、情報および情報サービスの信頼性にアシュアランスを提供する。ITコントロールは組織体が技術(テクノロジー)を利用するのに伴うリスクの軽減に寄与するプロセスである。

上記の説明から分かるとおり、基本的には、ITコントロールは関連するリスクを考慮して適用される。一方、特定のシステムかプロセスに限定されることなく、企業全体に影響を与え得る全般的リスクに対応するコントロールや全てのITインフラストラクチャーに適用される、基本的なレベルのウイルス予防策(IT hygiene)のようなコントロールを「ベースラインITコントロール(baseline IT controls)」と呼ぶ。

ITに関わるインターナル・コントロール

組織体の経営者は、ITプロセスがビジネスの目標に貢献し、競争上の利点になっていることについての保証を得る必要がある。組織体は、組織体のITが不正またはコンピュータ・ネットワーク上の攻撃(サイバー攻撃)等のリスクを軽減することを可能にすることについて保証を得る必要がある。株主等の利害関係者は、組織体のITの運用が信頼し得るものであることを求める。

MC
9-1-1 ~ 9-1-3



原語

ITのコントロール手段：
Information Technology
Controls



原語

GTAG:
Global Technology
Audit Guide
GTAGについてはUnit
9-3で学習する。



インターネットを利用しているある企業のネットワーク・システムのファイアウォールはベースラインITコントロールの例である。
ITセキュリティ・コントロールに適用されるベースラインの例としては、VISAのカード保有者情報セキュリティプログラム(Cardholder Information Security Program ;CISP)のDigital Dozenとインターネット・セキュリティ・センターのFundamental fiveがある。



ITに関わるインターナル・コントロール

ITに関わるインターナル・コントロールの目的は、以下の項目を含む。

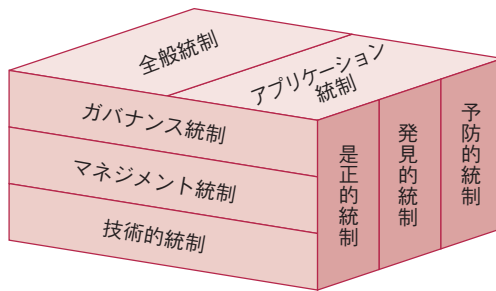
- 資産の保全
- 情報が利用可能であり、信頼性があり、かつ適切に規制されていることの確保
- ユーザーが実行した機能に対して説明責任を維持すること
- 顧客ID、およびプライバシーの保護
- 従業員の保護
- データおよびシステムの信憑性、インテグリティの維持
- 経営者に自動化されたプロセスがコントロールされていることを確信させること
- 全ての自動化されたおよびユーザーが着手したトランザクションにおける監査証跡の提供

9-2 ITコントロールの分類

ITコントロールの分類

IT環境におけるコントロールを考える際に、しばしば全般統制及びアプリケーション統制の2つに分類して考える。全般統制とは、企業の統制環境が安定的に、よく管理されることを保証するために設計される。人事管理や障害回復計画は、全般統制に含まれる。一方、アプリケーション統制は、取引におけるデータの入力、処理、出力統制等、アプリケーション・システムの特定の機能に関連する統制を指す。

GTAG 1では、全般統制とアプリケーション統制を含め、ITコントロールを次の3つの側面から分類している。



Source: Global Technology Audit Guide 1: Information Technology Controls (IIA)

〈ITコントロールの分類〉

全般統制	人事管理、障害回復計画等、企業の統制環境が安定的によく管理されることを保証するために設計される統制。
アプリケーション統制	入力、処理、出力統制等、アプリケーション・システムの特定の機能に関連する統制。
ガバナンス統制	ITに関わるセキュリティ方針の策定、規準の評価等、取締役会、監査委員会等が(最高経営者と協議しながら)責任を持つ監視的な性質を持つ統制。
マネジメント統制	重要な資産、機密データ、及び組織構造や物理的統制等を含む運用に対するリスクを軽減する統制。取締役会と執行役員との協力が求められる。
技術的統制	ガバナンス統制及びマネジメント統制が有効に機能するために、整備されていなければならない統制。システム・ソフトウェア、システム開発等のコントロールが含まれる。
予防的統制	望ましくない事象が発生するのを抑止する統制。
(例)	ファイアウォールの利用、論理的アクセス・コントロール
発見的統制	発生した望ましくない事象を発見する統制。
(例)	エラー・レポートのレビュー
是正的統制	発見的統制によって発見された不適切な事象を修正する統制。
(例)	エラー修正、業務継続

AZ

原語
 全般統制: General control
 アプリケーション統制: Application control
 ガバナンス統制: Governance control
 マネジメント統制: Management control
 技術的統制: Technical control
 予防的統制: Preventive control
 発見的統制: Detective control
 是正的統制: Corrective control

9-3 ITコントロール・フレームワーク

MC
9-3-1 ~ 9-3-10

ITコントロール・フレームワークの選択

ITコントロール・フレームワークの選択に際しては、コントロールに責任を負っている多数の従業員によって活用されるため、組織体全体への便益の提供という要素を考慮する。コントロール・フレームワークは、COBITのような公式なモデル又は、口頭で伝達され行動に反映される形式の両方を取り得、組織体の広範囲に適用が可能である。但し、全てのビジネスタイプ、又は全てのITを含有するフレームワークはない。

- a) COSO
COSOとは、トレッドウェイ委員会支援組織委員会(Committee of Sponsoring Organizations of the Treadway Commission)の略称であり、国際的なコントロールのフレームワークを提供している。
- b) COBITフレームワーク
COBIT(Control Objectives for Information and related Technology; COBIT)は、組織体が必要とする情報を提供するITを適切に管理するための標準を含む、ITガバナンスとコントロールの指導的なフレームワークである。COBITは、ISACA、及びISACAの研究機関であるITガバナンス協会(IT Governance Institute; ITGI)によって1996年に初版が発行され、2005年には第4版(COBIT 4.0)が、2007年にはCOBIT 4.0のアップデート版であるCOBIT 4.1が発行され、さらに2012年には第5版(COBIT 5)が発行されている。

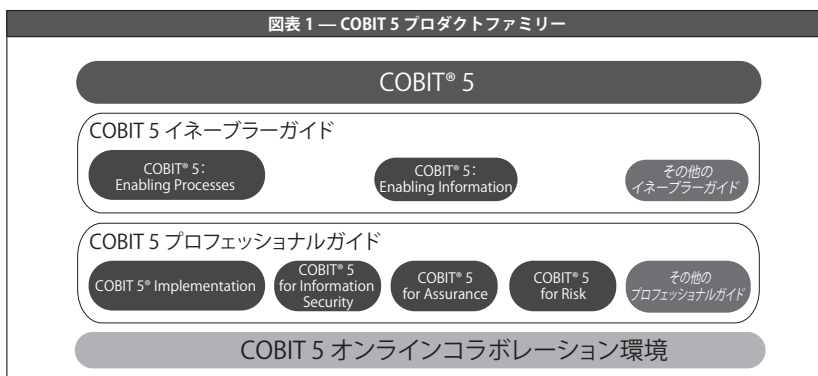
COBIT 5 フレームワークは、後述の5つの基本的な原則に基づいており、その原則から派生する形で、事業体のITガバナンスとITマネジメントを実現するイネーブラーについて説明するさまざまな指針が存在する(イネーブラーについての解説は省略する)。



COSOの国際的なコントロールの詳細についてはPart1のUnit 7-3から7-5を参照。

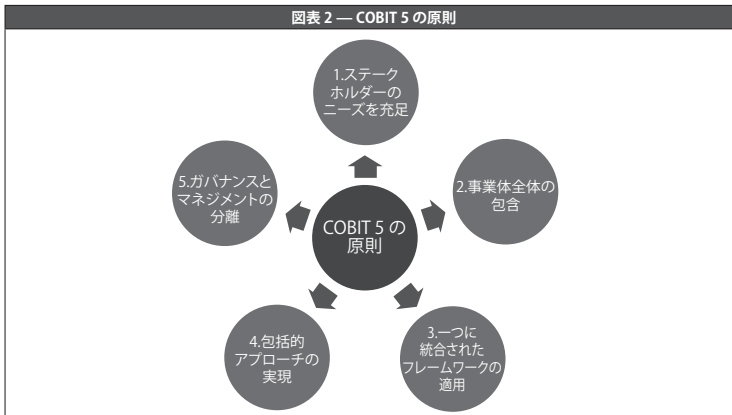


イネーブラー(Enabler):
本フレームワークによれば、「ある事柄が機能するか否かについて、個々に、かつ集合体として、影響を及ぼす要因」とされている。



Source: COBIT 5

5つの基本原則は、以下の通りである。



Source: COBIT 5

1) 原則1：ステークホルダーのニーズを充足

企業は、ステークホルダー(利害関係者)に対する価値を生み出すために存在している。そしてそれらの価値は、効果の実現と、リスクやリソース活用の最適化とのバランスを保つことで実現される。

COBIT 5は、ITを使った事業価値の創出をサポートするために、必要なすべてのプロセスと、その他のイネーブラーを提供する。企業毎にその目的は異なるため、企業はCOBIT 5を企業が扱うビジネスの背景に合わせてカスタマイズすることができる。

2) 原則2：事業体全体の包含

COBIT 5は企業のITガバナンスを、企業のガバナンスに統合する。

i) COBIT 5は、企業内部のすべての機能とプロセスをカバーする。すなわち、COBIT 5は「IT機能」のみにフォーカスするものではなく、情報とそれに関わる技術を、他の資産と同様に企業の全員が関与すべき資産として扱う。

ii) COBIT 5は、すべてのITに関わるガバナンスとマネジメントのイネーブラーを、企業全体に渡る包括的なものとして捉えている。すなわち、企業が保有する情報とそれらに関連するITについてのガバナンスおよびマネジメントに係る、社内外のあらゆるものとあらゆる人々を含む。

3) 原則3：一つに統合されたフレームワークの適用

IT関連の標準やベストプラクティスは数多く存在し、それぞれがITアクティビティの一部に関わるガイダンスを提供している。COBIT 5は、その関連する標準やフレームワークと高いレベルで整合を図っており、それがCOBITを企業のITガバナンスとITマネジメントに関わる包括的なフレームワークへと押し上げている。

4) 原則4：包括的アプローチの実現

企業のITガバナンスとITマネジメントを効率的かつ効果的なものとするためには、いくつかの互いに影響し合う構成要素を考慮した、包括的なアプローチが必要である。

COBIT 5は、組織のITに係る全般的なガバナンスとマネジメントシステムの導入を支援するために、一連のイネーブラーを定義している。COBIT 5フレームワークは、以下の7つのカテゴリーのイネーブラーを定義している。

- － 原則、ポリシーおよびフレームワーク
- － プロセス
- － 組織構造
- － 文化、倫理および行動
- － 情報
- － サービス、インフラストラクチャおよびアプリケーション
- － 人材、スキルおよび遂行能力

5) 原則5：ガバナンスとマネジメントの分離

COBIT 5フレームワークは、ガバナンスとマネジメントの間に明確な区別を設けている。

この2つの分野は、それぞれ異なる種類のアクティビティを含み、異なる組織構造を必要とし、異なる目的を持つ。

COBIT 5におけるガバナンスとマネジメントの主要な区別は以下のとおりである。

i) ガバナンス

ガバナンスとは、ステークホルダーのニーズや条件、選択肢を評価し、優先順位の設定と意思決定によって方向性を定め、合意した方向性と目標に沿ってパフォーマンスや準拠性をモニターすることで、企業の目標がバランスを取って、合意の上で決定され、達成されることを保証するものである。

ほとんどの企業において、取締役会の議長のリーダーシップのもと、取締役会がガバナンス全体の実行責任を負う。特に大きく複雑な企業では、特定のガバナンスの実行責任は、適切なレベルの、特定の組織構造に割り当てられることがある。

ii) マネジメント

マネジメントとは、企業の目標の達成に向けてガバナンス主体が定めた方向性と整合するようにアクティビティを計画、構築、実行し、評価することである。

ほとんどの企業において、最高経営責任者(CEO)のリーダーシップのもとに、経営幹部がマネジメントの実行責任を負う。

c) ISO/IEC 27000

ISO/IEC 27000シリーズは国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定するISMSに対するベストプラクティスを提供する。

ISMSとは情報セキュリティマネジメントシステム(Information Security Management System)の略称である。企業は多くの情報資産(機密情報や業務データなど)を保有しているが、当該情報資産を適切に保護するためにセキュリティ管理を行う仕組みのことをISMSと呼ぶ。

ISMSの基本的な考え方は、組織の情報資産を分類し、リスク評価を行い、必要なセキュリティ対策を決定し、それに基づいた対策の運用を行うことである。一時的な対策ではなく、継続的な情報セキュリティレベルの向上を図るために、PDCAサイクルの確実な実行およびその管理運用体制の構築が求められている。

d) eSAC (Electronic Systems Assurance and Control)

IIAが、eビジネスに関わるシステムの管理環境を評価するための枠組みとして作成したガイドラインである。

eSAC が対象としている範囲は以下の3領域である。

- 開発、運用、メンテナンスを含むライフサイクル全体
- マネジメント、組織、エンジニアリングのそれぞれの活動を含む組織全体
- システム、ソフトウェア、ハードウェア、人的要因、テストエンジニアリング、システム管理、運用、メンテナンスとの相互作用

eSACでは、情報セキュリティは単なるIT技術の問題だけでなく、ビジネスの問題でもあるという認識が示され、人々の認識と行動、トレーニング、そして特にマネジメント層のセキュリティ意識を抛り所とする企業文化について言及しなければならないとしている。



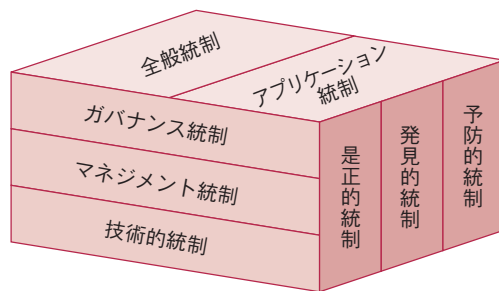
国際電気標準会議
(International
Electrotechnical
Commission; IEC) :
電気及び電子技術分野
の国際規格の作成を行
う国際標準化機関であ
る。

〈eSACが掲げているコントロール目標〉

可用性	情報、プロセス、サービスが必要な時に利用可能であることを保証すること
能力	システム処理を確実にかつ適正な時間で完了させる能力を保有していること
機能性	ユーザーのニーズを満たす機能、応答性、使いやすさを備えていること
保護性	不正なアクセスや使用から、ハードウェアやソフトウェア、データが保護されていること
説明性	システム処理が正確に完了したことを保証するために、個人の役割、行動、責任が明確にされていること

e) GTAG (Global Technology Audit Guide)

ITコントロールは、複数の異なる視点から分類することが可能である。IIAの発行する“Global Technology Audit Guide”では以下のモデルを提示している。



Source: Global Technology Audit Guide 1: Information Technology Controls (IIA)

GTAGは、コントロール・フレームワークではないが、主として内部監査部門長、監査委員会、経営者層向けに提供される、ITマネジメントとIT監査についての国際的なガイドである。

f) ITIL (Information Technology Infrastructure Library)

ITILとはITサービス提供時に必要となる業務プロセスのベストプラクティス集である。企業の情報システム部門やアウトソーシング事業者が、情報システムの利用者に対して高品質のシステム運用サービスを提供する際の規範となる。ITILはコントロール・フレームワークではないが、多くのIT企業が準拠している規範である。

ITILは7つの書籍で構成されており、中期的なサービスの管理手法を記述した「サービスデリバリー」と日々のIT運用手法を記述した「サービスサポート」の2つの書籍がその中核をなす。その他、ITILを組織に導入する際の目標設定から診断などの方法論を説明した「サービスマネジメント導入計画立案」やビジネス環境における課題としてパートナーシップやサプライヤー管理などを説いた「ビジネスの観点」などがある。



GTAG(Global Technology Audit Guide)は、コントロール・フレームワークではないが、組織体が適切なフレームワークを選択することを支援する。

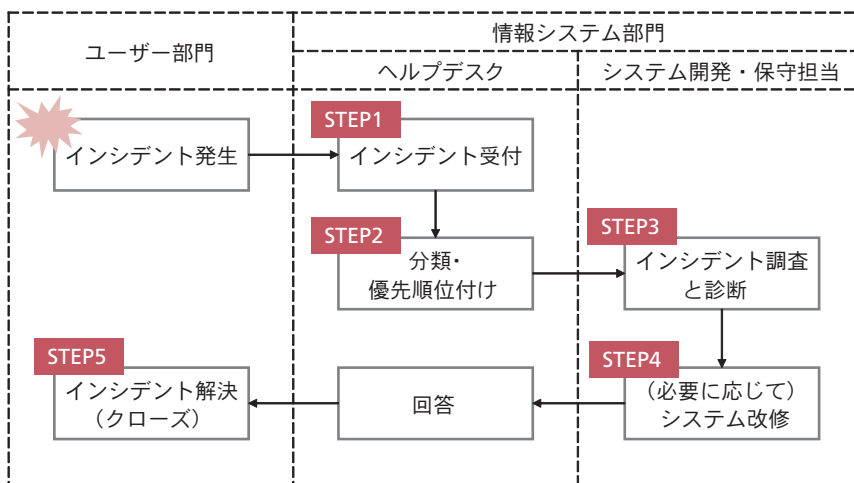
参考

インシデント

ITサービスマネジメントにおけるインシデントとは、情報システム部門が提供するITサービスがシステムの不具合や故障などにより、サービスの質や利便性が損なわれかねない状況を指す。インシデントには、ユーザーがITサービスに対して不満足な状態であることも含まれる。

インシデント管理

インシデント管理は、概ね以下のステップで実施される。



STEP1：インシデント受付

電話やメール等でインシデントの発生連絡を受け付ける。インシデントの発生箇所はユーザー部門の場合が多いが、システム部門内で発生することもある。受け付けたインシデントはヘルプデスクにて記録される。

STEP2：分類・優先順位付け

受け付けたインシデントは、インシデントの種類毎に分類され、対応の優先度を決める。インシデントにはシステムの不具合やウィルス感染に関する連絡だけでなく、単なるPCの基本操作に関する質問やプリンタの不具合なども含まれており、多くの種類が存在するため、種類別に分類した上で、対応の優先度(緊急度)を決定する。

なお、単なるPCの基本操作に関する質問などは、ヘルプデスクで回答し、インシデントをクローズする。

STEP3 : インシデント調査と診断

システムの不具合に関するインシデントなどはヘルプデスクだけで解決できないため、システム開発・保守担当など技術部門にエスカレーションし、インシデントの原因を追求する。

また、インシデントの原因と緊急度を鑑みて根本対応を行う。なお、インシデントの原因が根深く根本対応に時間がかかる場合や緊急度が高い場合などには、一時的な対応である暫定対応が行われることがある。

STEP4 : (必要に応じて)システム改修

インシデントがシステムの不具合に関するインシデントである場合、システム改修が必要になる場合がある。この場合、変更管理プロセスに則ってシステム改修が行われる。

STEP5 : インシデント解決(クローズ)

顧客であるユーザー部門にインシデントに対する回答を連絡し、インシデント管理をクローズする。1つのインシデントを解決することで別のインシデントが発生することもあるが、その場合は別のインシデントとして扱う。

9-4 情報システムの構築による影響

MC
9-4-1～9-4-2

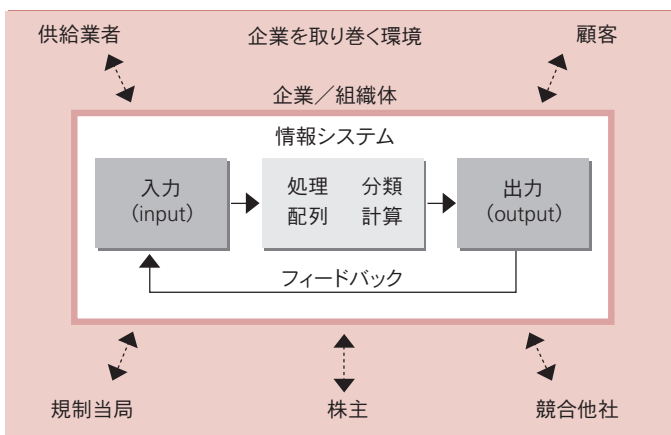
論点 情報システム

情報システムとは、組織体または社会の活動に必要な情報の収集、処理、伝達に関わる仕組みである。

定義 情報システムとは、組織体の意思決定、調整、統制、分析、及び視覚化することを支援するために、情報を収集、処理、記憶、及び伝達するための要素が相互に関連している仕組みである。

情報システムとは、コンピュータに関わるものばかりではない。広義の情報システムには、手作業で記帳する帳簿等のような、コンピュータに関わらないものも含まれる。しかし、本書においては、コンピュータに関わる情報システムを“情報システム”として解説を行う。

- a) 情報システムの3つの重要な要素が組織に必要な情報を生み出す。



情報システムの3つの要素とは、入力、処理、及び出力である。入力では、組織内外より生のデータを収集し、処理では入力された生のデータをより意味のある形へ転換する。出力では、処理された情報を、利用者へ配信をすると共に、入力が正しかったかどうかを評価するためにフィードバックを行う。

情報技術にかかわる用語はほとんどカタカナ表記であるため、必要に応じて原文を表示している。CIA試験ではカタカナと英語の併記で問われる。

情報とは、事実である生のデータを人間にとって有意義、かつ有用な形式に変更したものを意味する。一方データ(data)とは、組織内外で発生している事象を人間が理解できるように形に体系化する以前の事実の連続のことである。

情報システムの構築による影響

情報システムの構築は企業に様々な影響を及ぼすが、従来のマニュアル処理との比較におけるコンピュータ処理による影響をまとめると以下の通りである。

- a) 監査証跡を追跡することが難しくなる場合がある。コンピュータによって随時処理が更新されるため、取引証跡が非常に短い時間、かつコンピュータが読める形式でしか残らない。
- b) コンピュータは、同じ処理命令に対して統一した処理を行うことができるため、事務的なミスを減らすことができる。従って、高度な計算を伴う業務を大量に処理することが可能である一方、プログラミングエラーが発生した場合、同じ条件下の全ての取引処理に誤りが発生する。
- c) 多くの人が分担して行っていた職務が、コンピュータによって集中処理することが可能になるため、従来の職務の分離の概念が適用されなくなる。また、コンピュータにアクセスが可能な個人が、複数の業務内容にアクセス可能になるため、新たなコントロールが必要になる。
- d) 承認されていない者によるデータへの不正アクセスや、証拠を残さずにデータが改竄されるリスクは、紙で書類を作っている環境よりもコンピュータを利用している環境の方が高く、潜在的な不正の可能性がある。
- e) 情報システムは多様な分析ツールや、適時に報告書を提供することが可能であるため、経営者にとって企業の活動のレビューや監督がしやすくなる。



監査証跡：
監査証跡とは、情報システムに関する事象の発生から最終結果に至るまでの過程を追跡することを可能にする仕組みのことである。

9-5 データ処理方法

データ処理方法

データ・ベース内のデータが更新されるタイミングは、データ処理の方法によって異なる。

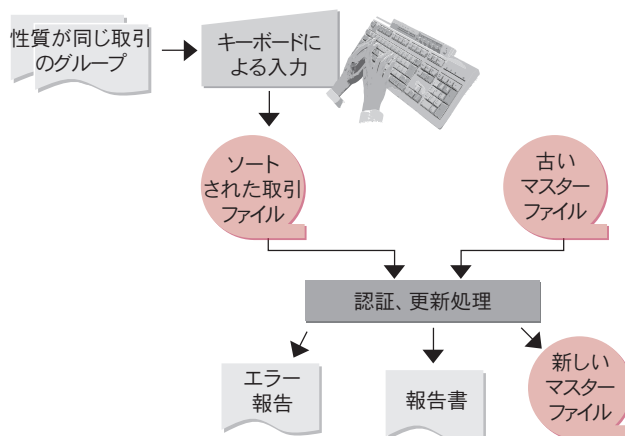
論点

バッチ処理とオンライン・リアルタイム処理

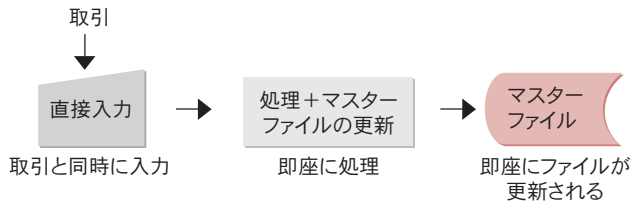
バッチ処理とオンライン・リアルタイム処理は以下の特徴を持つ。

バッチ処理	性質を同じくする取引等の蓄積されたデータを一括処理する方法
オンライン・リアルタイム処理	データが発生する部門等にコンピュータにつながった端末があり、データが発生するつど直接データを入力し、即座に処理する方法

- a) バッチ処理は、売掛金の1日分の回収額の計算や、月1回の給与計算等、処理のタイミングが業務上決まっていて、データが揃ってから処理するものに適する。従ってバッチ処理では、取引データは特定の期間取引ファイルに蓄積され、定期的に企業の常設ファイルであるマスターファイルを更新する時に使われる。



- b) オンライン・リアルタイム処理は、在庫の問い合わせや航空機座席予約システムのように、データが発生するごとに個々に処理しなければならないものに適する。従って、オンライン・リアルタイム処理では、マスターファイルは常に更新されている。



9-6 アプリケーション統制 (1)入力


コンピュータシステムのセキュリティ(アプリケーション統制)

コンピュータ・システムに対するセキュリティのうち、特定のソフトウェア・アプリケーションに関わる統制をアプリケーション統制という。

論点

アプリケーション統制

アプリケーション統制とは、アプリケーション・システムにおける取引及びデータに関する統制である。データの入力、処理、出力の際に、エラーや反則的な事象の発生が予防、発見、又は修正されるように設計、導入されるコントロールである。

 アプリケーション統制については、ほとんどがカタカナ名称となるため、原文を表示している。CIA試験では、カタカナ、もしくはカタカナと英語の併記で問われる。

全般統制との関係

全般統制はアプリケーション統制が継続的に有効に機能していることを担保する。

アプリケーション統制は誤ったデータがシステムに入力されないようにするなどの統制であり、個々のアプリケーションソフトウェアの機能として実装される。すなわちアプリケーション統制とはプログラムである。

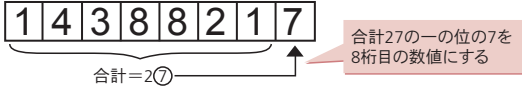
本番環境に正しいプログラムが登録されている限り有効なアプリケーション統制は継続して機能することになるが、プログラムの本番登録について適切な手続が整備されていないような状況下においては、いつ何時そのプログラムが変更や削除されているかは不明である。すなわち有効でない全般統制の下では、いつアプリケーション統制が無効化されてもおかしくはない。

このためアプリケーション統制は、有効な全般統制の下で機能する統制と言える。


入力の有効性の統制(コントロール)

入力統制は、入力されたデータが妥当であることを保証し、誤ったデータを排除することを目的とする。

予め記録された入力 (preprinted form)	予めフォーム上の場所とフォーマットが割り当てられる。
(例)	特定のID番号の入力をさせるためにその文字(数字)の数だけ空欄を設けておく。

チェック・ディジット (check digit)	数学的に計算がされた数値をデータに付加することにより、元のデータが改竄されていないか、別のデータにすりかわっていないかを確認する。
(例)	<p>8桁の銀行口座の8桁目を、口座番号の上7桁の合計の一の位とする。口座番号の入力の度にコンピュータが8桁目を計算し、入力された8桁と比較する。</p> 
限界チェック (limit check)	データは予め設定された数値を超過できない。
(例)	給料支払額が4,000ドルを超えてはならないと設定した場合、支払額が4,000ドルを超えた場合にはデータは拒絶され、更なる検証/承認が必要となる。
メニュー・ドリブン・ インプット (menu driven input)	入力に際して、オペレータに適切な範囲での答えを選ばせるもの。
(例)	画面表示の一覧表から科目名を選択する。
フィールドチェック (field check)	特定のデータフィールドに、受け入れられるキャラクターのタイプを制限する統制方法。
(例)	試験の得点欄には数値のデータのみ入力できる。
バリディティ・チェッ ク(validity check)	入力されるデータは、有効なデータのみを許可する統制である。
(例)	フィールドに性別を数字で入力させる。 1：男、2：女、それ以外のは受け付けない。
ミッシング・データ・ チェック (missing data check)	入力データ上で、ある種のデータの不備を探す統制。
(例)	従業員の所属部門番号が抜けていたら、エラーメッセージが出る。
フィールド・サイズ・ チェック (field size check)	正確なキャラクターの数を要求する統制。
(例)	7桁の入力を要するフィールドで、それ以下、それ以上の桁が入力された場合にエラーメッセージが出る。
ロジック・チェック (logic check)	入力の論理的でない組み合わせを受入れないようにする統制方法。
(例)	65歳以下の人は、特定の社会保障給付を受けられないにもかかわらず、年令欄にそれ以下の年令がインプットされ、給付の申告があったような場合、エラーメッセージが出る。

9-7 アプリケーション統制 (2)処理

 論点 処理プロセスにおけるコントロール

処理プロセスにおけるコントロールの主要な目的は、良質な監査証跡に寄与することである。処理プロセスにおけるコントロールは、データ・ファイルに対するコントロールと処理コントロールに分類される。

データ・ファイルに対するコントロール	正当な処理のみがデータに対して行われることを保証する。
処理コントロール	累積されるデータの完全性及び正確性を保証する。

処理に関するコントロールにおいても、入力のコントロールで使われる手法を用いて信頼性のチェックが加えられる。主な処理プロセスにおけるコントロールの手法には以下がある。

a) データ・ファイルに対するコントロール

前後イメージ報告
トランザクションの処理の前後のデータを保存、報告することで、前後のイメージの比較が可能となる。これにより、トランザクション処理がコンピュータ記録に与えた影響を追跡する。
エラー報告の保守及び取扱い
全てのエラーが適切に照合され、修正が適時的に行なわれるようコントロールを設立する。
原始証憑の保存
原始証憑を適切な期間保存し、臨機応変に検索、検証できるようにしておく。また、必要に応じ、コントロールされた環境下で証憑を破棄する。
内部及び外部ラベリング
これらラベルは、適切なデータが使用されることを保証する。
正しいバージョンの使用
正しい処理を行なうために、正しいバージョンのファイルの使用は不可欠である。
データ・ファイル・セキュリティ
不正にアプリケーションに侵入しデータ改竄などを試みる、承認を受けていないユーザーのアクセスを防止する。



内部監査人は、一部例外を除いて、最新バージョンのファイルが使用されていることに関心を頂く。

個別チェック
個々の文書を、コンピュータが作成した文書のリストと照合する。
トランザクション・ログ
すべてのトランザクション入力(日付、時間、IDおよび端末の所在情報など)はトランザクション・ジャーナルにコンピュータによって記録される。この詳細リストは監査証跡として役立つ。
ファイル更新及び保守に関する承認
ファイル更新、保守のために適切な承認を必要とすることにより、保存されたデータの正確性、および最新性が保たれていることが保証できる。

b) 処理コントロール

冗長性チェック (redundancy check)	本来は必要のないビットを、各データ・セグメントの末尾に追加することにより、伝送上のエラーを検知する。冗長性チェックの手法として、パリティチェックや巡回冗長検査(CRC)、ハミング符号などがある。								
(例)	<p>パリティチェックとは送信するビット列に対して、パリティビットと呼ばれる検査用のビットを付加することで、データが誤っていることを検知する。</p> <p>例えば、偶数パリティと呼ばれる場合は、送信するデータのビット列とパリティビットに含まれる1の数が偶数になるようにパリティビットを付加してデータを送信する。</p> <div style="text-align: center;"> <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px 5px;">0</td> <td style="padding: 2px 5px;">1</td> <td style="padding: 2px 5px;">0</td> <td style="padding: 2px 5px;">0</td> <td style="padding: 2px 5px;">1</td> <td style="padding: 2px 5px;">1</td> <td style="padding: 2px 5px;">0</td> <td style="padding: 2px 5px;">1</td> </tr> </table> ↓ </div> <p style="text-align: center;">送信するデータ パリティビット</p> <p>これにより、受信者側は送られてきたデータを確認し、1の数が偶数にならなければ、データの伝送にエラーがあったと判断できる。</p>	0	1	0	0	1	1	0	1
0	1	0	0	1	1	0	1		
コントロール・トータル (control total)	入力されたデータフィールドの合計額を処理されたデータの合計額と照合する。								
(例)	金融機関等では、受け付けた小切手の金額はコンピュータ用にコード化されるのだが、コンピュータ上で正当に処理されているかの確認が必要である。コントロール・トータルとは、100、又は200等のまとまった小切手の合計金額値をコンピュータに記憶しておき、一枚一枚の小切手を処理した後の合計金額と比較する方法である。								



巡回冗長検査
(Cyclic Redundancy Check; CRC):
送信するデータを特定の式で除した余りを、送信するデータに付加する方法である。
ハミング符号:
送信するデータに検査・訂正用のビットを付加する方法である。

冗長性チェックなどをハードウェアで実装すると「ハードウェア統制」と呼ばれる。



コントロール・トータル
(control total)は、入力の有効性の統制手法にも使われる場合もある。

ハッシュ・トータル (hash total)	総従業員の社会保障番号の算術的合計値など財務的には全く意味のない、統制のためだけにとる統計値のことである。又、処理したレコード数をカウント(record count)して統制に利用することもある。
(例)	販売システムから会計システムに転送されたデータを検証する場合、財務的には意味のない、商品コードの合計額で照合する。
ラン・トゥー・ラン・トータル (run-to-run totals)	前の工程で集計したデータと次の工程で集計したデータとの値を照合する。アプリケーション処理の段階でデータを検証することが出来る。

9-8 アプリケーション統制 (3)出力

出力の有効性の統制

- 1) 出力統制は、ユーザーに送信したデータが一貫し、安全な方法で表示され、形式が整えられ、配布されていることを保証する。出力統制には、処理結果の妥当性の確認という側面と、出力されたデータの利用と配布についてのコントロールという側面がある。前者については、データの突合やエラーレポートに示された項目の追跡等が有効であり、後者については承認された人以外がその出力データを読むことがないように、リストを作成し、そのデータにアクセスした従業員の記録を採っておく方法などがある。
- 2) 主な出力統制には以下のものがある。

- 換金性、機密性、重要性がある書類の受渡記録の管理、および安全な場所での保管。
- 出力帳票の配布。
出力帳票は予め承認された配布媒体(パラメータ)を用いて配布される。オペレーション担当は出力の完了および配布がスケジュール通り行なわれているかを調査し、また配布前には配布記録をとらなければならない。
- 合計突合および照合。
データ処理アプリケーション・プログラムの出力は、定期的にコントロール・トータルと突合をしなければならない。
- 出力エラーの取扱い。
アプリケーション・プログラムの出力に含まれるエラーの報告および管理のための手続が確立されていなければならない。
- 出力伝票の法規制を遵守した保存方針確立、及び保存期間の厳守。
- 機密保持を必要とするような帳票の受領記録の検証。

処理統制と出力統制の違い

処理統制と出力統制の大きな違いは人手による統制(マニュアル統制)が存在するかどうかである。

システムにより自動化されたチェック機能などシステム内で完結している統制は処理統制であるが、この処理統制を利用して(単なるシステム操作ではなく)人が内容の妥当性チェックなどを行う場合など、自動で出力されたレポートを人がチェックするような統制は出力統制である。

9-9 不測事態対応計画

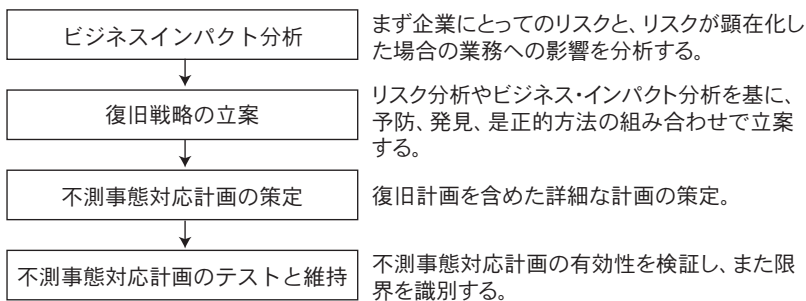
事業継続計画、不測事態対応計画の構築

ビジネスの中断は自然災害、事故または意図的な犯罪行為によって発生する。ビジネスの中断は重大な財務上および業務上の損害をもたらすことがある。ビジネスの成功にITの活用が不可欠な今日、コンピュータ・システムの中断についても十分な準備が必要である。

論点 ITに関わる不測事態対応計画

ITに関わる不測事態対応計画(contingency planning)とは、自然災害等により組織体にとって重要な機能を持つコンピュータ・システムや通信サービスが遮断された場合、どのように復旧するか計画立案を含め、業務リスクを軽減させるように設計されたプロセスである。

a) 不測事態対応計画の一連の流れは以下の通り。



ビジネスインパクト分析(BIA)によって以下の点が明らかになる。

- 事業継続計画の対象となる重要業務の特定
- 業務継続・復旧の優先順位付け
- 目標復旧時間と目標復旧ポイントの設定

ビジネスインパクト分析を行うことの主目的は、有事の際に復旧を優先する業務の選定とその目標復旧時間の決定にある。

まず優先的に復旧させる業務の選定は、「有事」を想定することから始まる。まず環境面からの分析として、対象業務に関係する建物や電気・ガス・水道といった社会インフラにおける被害想定と業務への影響を検討する。



基本的な概念を共通とする「事業継続計画」の用語は複数ある。事業継続計画「Business continuity planning (BCP)」がより一般的かつ包括的な概念であり、BCPは通常、災害復旧計画(Disaster Recovery Planning(DRP))を伴う。ここでは事業継続計画と不測事態対応計画を同義として説明する。



原語
ビジネスインパクト分析:
Business Impact Analysis;
BIA



目標復旧時間:
どれだけ早く業務を再開できるか
目標復旧ポイント:
どの時点までデータを復元できるか

次に業務面からの分析として、業務を行う際の最低条件を整理し、想定被害下における停止業務を洗い出す。このうち、業績に与える影響やCSR等の観点から優先順位付けを行い、優先的に復旧させる業務を選定していくことになる。

また、洗い出された業務について目標復旧時間と目標復旧ポイントを定め、これを達成できるように対策(予防・代替手段など)を検討していくことになる。

〈システムに関する不測事態対応計画時の指標〉

目標復旧時間(RTO)	事前に定めたレベルにシステムが復旧するまでの時間。業務の重要度に応じて設定する。
目標復旧時点(RPO)	データの復旧を保証する時点。RPOが1時間であれば、システム停止の1時間前までのデータが復旧される。
目標復旧レベル(RLO)	目標復旧時間の経過後に、システムが復旧するレベル。

AZ

原語
目標復旧時間：
Recovery Time
Objective; RTO
目標復旧時点：
Recovery Point
Objective; RPO
目標復旧レベル：
Recovery Level
Objective; RLO

AZ

原語
耐故障コンピュータ・システム：
fault-tolerant
computer system
可用性コンピュータ：
High-availability
computing

b) 耐故障コンピュータ・システム、可用性コンピュータ

耐故障コンピュータ・システムとは、継続して中断されないサービスを提供するために、ハードウェア、ソフトウェア、及び電源装置の構成要素を重複して搭載しているコンピュータ・システムである。オンライン取引処理を必要とする航空会社や金融機関等は、100%の稼働率を確保するために伝統的に耐故障コンピュータ・システムを利用してきた。

可用性コンピュータも、耐故障コンピュータ・システム同様、バックアップのハードウェア資源を搭載しており、アプリケーションとシステムの可用性を最大化するように設計されている。ただ、可用性コンピュータは、障害が発生した際に即座に回復するためのシステムである一方で、耐故障コンピュータ・システムが利用可能な状態を継続するシステムであり、“回復させる時間”という概念がないという点において異なる。

c) 障害回復計画に使われる技術

1) フェイルソフト(fail soft)

システムの一部に障害が発生した際に、故障した箇所を破棄、切り離すなどして障害の影響が他に及ぶのを防ぎ、最低限のシステムの稼働を続けるための技術。

2) ミラーリング(mirroring)

サーバーの全てのプロセス及び取引をバックアップサーバーへ複製しておき、主たるサーバーの機能障害が起きた際に、バックアップサーバーが引き継ぐ。

d) 不測事態対応計画に対応する設備

不測事態に対応する設備体制には以下がある。

1) ホット・サイト

障害が発生した場合に、適合性のあるコンピュータ機器があり、瞬時にもしくは数時間以内に業務が再開できる体制のことである。

2) コールド・サイト

障害が発生した場合に、コンピュータを設置する場所のみ確保されているが、実際にコンピュータ等は運びこむ必要がある。

3) ウォーム・サイト

ホット・サイトとコールド・サイトの間に位置する。基礎的なインフラは提供されているが、通常はコンピュータ設備を欠く。ウォーム・サイトは、緊急導入のためのコンピュータがすぐに取得できることを前提としているが、他の設備をそろえるには、数日あるいは数週間かかる場合がある。

4) 相互援助協定

同等の装置あるいはアプリケーションを保持する2つ以上の組織間で結ばれる協定であり、参加者は災害等が発生した場合に、互いにコンピュータを使用する時間を提供することを約束する。低コストであるが、装置構成の差により、効果的に運用するためには頻繁なプログラム変更が必要となる。

不測事態対応計画の内部監査

不測事態対応計画の実効性を検証するための内部監査手続として以下の方法が考えられる。

- a) 不測事態対応計画の内容を、定期的に机上レビューしていることを確認する。
- b) 不測事態対応計画の内容を理解していることを確認すべく、担当者にインタビューする。

上記手続からもわかるように、システムを完全に復旧できなかった場合のことや、一時的に業務が停止することへの影響を勘案して、実際にシステムを停止させて計画通りに復旧できるかどうかを検証するような手続は通常行わない。


参考

情報システムは重要度によって以下のように分類することができる。

システムの分類	説明
クリティカル (critical)	この分類にあてはまる機能は、同一の能力を持つシステムに置き換えなければ実行不可能である。手動による方法では重要なアプリケーションの代替にはならない。中断に対する許容度は非常に低い。従って中断によるコストは非常に高い。
バイタル (vital)	この分類にあてはまる機能は、短期間であれば手作業で実行可能である。中断に対する許容度はクリティカル・システムの許容度よりも高い。よって機能がある時間(通常5日以下)で復旧されれば幾らかコストは低くなる。
センシティブ (sensitive)	この分類にあてはまる機能は、許容できるコストの範囲内で、長期間において手作業で実施可能である。手作業で実施される過程においては、通常は難しい手順が発生するため、追加の要員が必要になる。
ノン・センシティブ (nonsensitive)	この分類にあてはまる機能は、より長い期間中断させられることもあり、復旧される場合においても、ほとんど、または全くコストを掛けることは無い。また中断前の状態にまで回復させることも無い。

Source: ISACA Review Manual 2007

9-10 バックアップ

人的ミスを含む様々なトラブルからデータやプログラムを守るために、定期的にバックアップを取得することが有効である。なおバックアップ媒体は本番環境とは別の媒体を使用するが、安価な磁気テープが採用されることが多い。

バックアップの方法

a) フルバックアップ

システムの本番環境にある全てのデータやプログラムを保存する方法。1回のバックアップにすべての内容が含まれているため、障害発生時には直前のバックアップだけで元の状態に戻せるメリットがあるが、バックアップ媒体の容量を多く使用してしまうデメリットがある。

b) 差分バックアップ

前回のフルバックアップ以降に作成、変更されたデータやプログラムのみを保存する方法。障害発生時はフルバックアップと差分バックアップの両方を用いて元に戻すことになり手間がかかるが、バックアップ媒体の容量を抑えられるメリットがある。

週次でフルバックアップ、日次で差分バックアップを取得しているケースが多い。

世代管理


バックアップ媒体を複数本用意することで世代管理を行うことができる。例えば週次でフルバックアップ、日次で差分バックアップを取得している場合、1週間分のバックアップ媒体を3セット用意することで、3世代管理(本番環境を含めると4世代管理)が可能となる。

世代管理を行うことで、復元できるデータが直前だけでなく、世代数分まで戻ることが可能となる。

バックアップ媒体は本番環境がある場所と同じ場所に保管しておく、火災や地震などが発生した場合、本番データとバックアップデータの両方を喪失してしまうリスクがある。このため、バックアップ媒体は地理的遠隔地に保管することが推奨される。これをオフサイト保管という。多くの場合、1世代を直近世代用、1世代をオフサイト保管用、1世代をオフサイト保管地との輸送に充てたテープローテーションを行うことが多い。

データ廃棄時の留意点

データセキュリティの重要な側面として、削除したデータが完全に消去され、第三者によって復元ができないようになっているかを確認することがある。特に機密情報については、特別なファイル消去ソフトウェアや消磁、物理的破壊等の方法を取ることが検討されるべきである。



メディア・サニタイズ
メディアに記録されたデータをどのような手段でも読み取れないようにすること。具体的にメディアを物理的に破壊することや意味の無いデータで上書きしてしまう作業を指す。



Chapter 10

情報セキュリティ

Chapter 10 Contents

□ 10-1	ITに係るリスク	50
□ 10-2	情報セキュリティとサイバー・セキュリティ	53
□ 10-3	全般統制 物理的コントロール	56
□ 10-4	全般統制 論理的コントロール	58
□ 10-5	インターネットセキュリティ	61
□ 10-6	データの保存に係るセキュリティ	65
□ 10-7	情報の保護	67
□ 10-8	データ保護法令	72
□ 10-9	最新のテクノロジーとセキュリティへの影響	74

10-3 全般統制 物理的コントロール

物理的コントロール

物理的コントロールは、物理的アクセス・コントロール、環境の危険に対するコントロール、及び自然災害からの保護を含む。

物理的アクセス・コントロール

アクセス・コントロールの観点から情報資産を大別すると、物理的アクセス・コントロール(施設の施錠管理など、物理的な管理でコントロールする方法)が対象とする情報資産と論理的アクセス・コントロール(システム上のアクセス権限をコントロールする方法)が対象とする情報資産に分類される。

このうち物理的アクセス・コントロールは、コンピュータ機器、ファイル、書類のある施設には権限のある者以外のアクセスを禁止する。警備員の採用や、写真入のIDカードの携帯を義務付けるほか、カードキー等の方法がある。

物理的アクセス・コントロールの例

- a) カード
特定のIDカードの保有者を入室権限者とみなす方法。IDカードを紛失しても当該IDカードの失効手続を行うことでカードリーダ自体の更新は不要であるため、後述の「鍵」より優れている。
- b) 鍵
鍵の保有者を入室権限者とみなす方法。鍵を紛失した際は、ドアの鍵を更新する必要があるため、紛失時の経済的損害が大きい。
- c) 生体認証
静脈や指紋などを利用して、入室権限者を識別する方法。静脈や指紋などは変わることのない情報であるため、個人の特定が絶対的である。しかし静脈情報や指紋情報は最上位の個人情報であり、これらのデータが流出すると回復できないというデメリットがあるため、強固なセキュリティ対策の実施が必須となる。
- d) キーパッド(コード入力)
数字の組み合わせなどのパスコードを知っている者を入室権限者とみなす方法。入室権限者の変更があればパスコードを変更する必要があるため、入室権限者の変動が激しい場合は適用に向かない。

環境的コントロール

コンピュータ・システムが安定的に稼働し続けるためには、コンピュータルームの管理も重要である。

a) 温度・湿度管理

コンピュータルームには多くのサーバーが設置されるため高温になりやすい。またコンピュータは湿度に弱いため、一般的にコンピュータ室には能力の高いエアコンを設置する。なおサーバールーム内の温度を一定にするために大型扇風機を設置する例もある。

b) 電源管理

コンピュータは電気で動く。通常、電源は停電の一種である瞬断が発生する。また停電発生時においてもシステムを正常終了させるためには一定期間システムの稼働を支える電源が必要である。これらの対応策として、無停電電源装置(UPS)を設置する。

また長期的な停電が発生しても稼働が求められるコンピュータ・システムがある場合は、自家発電装置の設置が必要となる。

c) 消火設備

サーバーは発熱するため、温度管理が適切でないと発火する可能性がある。また災害等によりサーバールームが被災し、消火を必要とする場合も考えられる。このような事態に備えて消火器が設置されるが、消火器は通常の粉末消火器ではコンピュータ・システムに粉末が詰まり使用できなくなるため、二酸化炭素消火器の設置が必要である。なお当然であるが、コンピュータルームにはスプリンクラーの設置は厳禁である。



原語
無停電電源装置：
Uninterruptible Power
Supply; UPS

10-4 全般統制 論理的コントロール

MC
10-4-1 ~ 10-4-16

論理的コントロール

論理的コントロールは、ソフトウェアを利用して論理的な規則によってアクセス等の検討をする。

論理的アクセス・コントロール

論理的アクセス・コントロールは、アクセス権限のある利用者を識別するシステムである。論理的アクセス・コントロールでは、無権限者のアクセスを回避し、承認された者に対してシステムを利用できる権限の範囲を与える。

組織体にとって最も重要な資産の一つであるデータへの効果的なセキュリティ・システムは以下のような保証を提供する。

- a) 権限のある利用者のみデータへアクセスできること
- b) アクセスのレベルはその必要性に応じていること
- c) データの修正には完全な監査証跡が残ること
- d) 未承認のアクセスは拒絶され、アクセスを試みたことが報告されること



アクセスレベル：
各部署によってアクセスできるデータが限られている。顧客対応に無関係な部署は、顧客データにアクセスすることは出来ない。

論理的アクセス・コントロールの例

a) ユーザー認証

1) パスワード認証

ユーザー ID などの識別情報とパスワードの組み合わせが一致する場合に、アクセスしようとしている者を正当な本人であると見なす方法である。パスワードにはユーザーが文字列を指定している場合もあれば、トークンなどで自動生成したコードを利用する場合もある。パスワードは秘匿性を高める必要があるため、ユーザーが文字列を指定する場合は、他人に推測されにくいパスワードにすることやパスワードを解析されにくいように一定以上の桁数や英数字混在などの複雑なパスワードにすることが推奨される。



アカウントが乗っ取られたり、パスワードが流出した事実があれば、パスワードの変更が必要になるが、そのような事実がなければ、パスワードのパターン化につながるため定期的なパスワード変更は不要である。



論点 パスワード認証のセキュリティ強化

パスワード認証のセキュリティ強化のために以下のような機能が実装されることがある。

- 1) 一定回数以上パスワードを間違えるとアクセスできない。
 - 2) 過去に使用したパスワードは利用できない。
- アカウントの乗っ取りは、マシンによるパスワードの総当たり試行が多いことから、上記 1) の機能は、セキュリティ強化に特に有用である。

2) 端末認証

特定の端末のみにアクセスを限定することで、端末からのアクセスは正当なアクセスであるとみなす方法である。端末の利用者が正当な本人であるかどうかは端末への物理的・論理的なアクセス・コントロールで担保される。

3) 2段階認証

上述のパスワードは複数の認証場面で使いまわされることにより、1つが漏えいすると芋づる式に他の認証も突破されてしまう脆弱性を持っていた。このためパスワード単独での認証では限界があることから、パスワード認証に加えて、セキュリティコードなどによる認証を行う2段階認証が誕生した。

たとえば、システムにアクセスする時にパスワードだけでなく、メールで送られた数字を入力させることで、正当な本人であることを確認する。

4) コールバック

社外からのコンピュータへのアクセスを承認された従業員のみ制限する方法である。まず、従業員が会社のコンピュータ・システムを電話で呼びだし、ユーザー名、パスワードを入力する。システムは一度遮断され、その従業員がアクセスを許可された者であることが識別されると、システムが自動で利用者へ通信を行う。

b) ユーザー ID 管理

1) ユーザー ID の棚卸

ユーザー ID などの識別情報は常に最新の状態になっている必要がある。どれほど強固な認証の仕組みを実装していても、かつて権限者であった者が異動や退職などで無権限者になったにもかかわらず、ユーザー ID が付与されたままであれば十分なアクセス・コントロールが実現できているとは限らない。このためセキュリティ担当者を採用し、常にユーザー ID が最新化されている状況を担保することが望まれる。

c) 事後監視・その他

1) アクセス・コントロール・ソフトウェア

機密データの不正な改竄などを防止する機能を含むソフトウェア。ユーザー識別および認証の適用やログの記録を含む。

2) 監査ロギング

全てのアクセス試行を、その成功失敗にかかわらず記録しセキュリティ管理者に報告する機能(アクセス・コントロール・ソフトウェアの機能にも含まれる)。

3) 自動ログオフ機能設定

一定の時間操作をしないと自動的に接続が切られるという設定。

10-6 データの保存に係るセキュリティ

MC
10-6-1 ~ 10-6-4

データストレージ

1つの記憶装置にデータを保管していると、当該データが破壊された場合、復旧が不可能になる。サイバー攻撃とその防御策は互いに「いたちごっこ」の関係にあり、完全防御は不可能であることを前提にすると、1つの記憶装置にデータを保管すること自体がリスクとなる。このため多くの企業では複数の記憶装置にデータを保管している。

a) ミラーリング

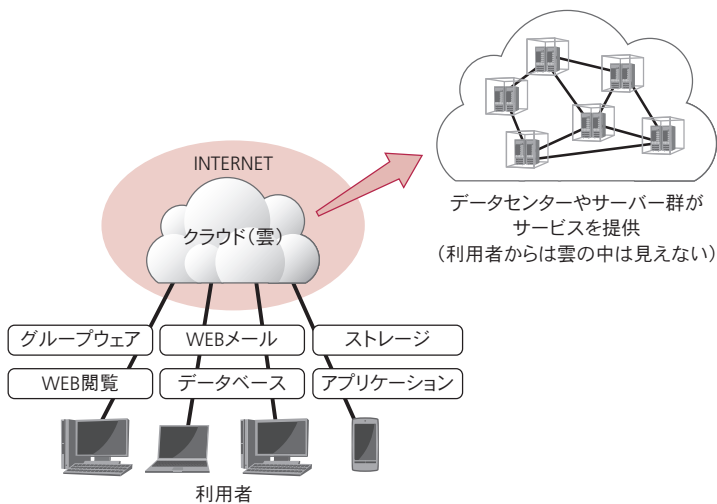
1つのデータを同時に2つ以上の記憶装置に記録する方式をミラーリングという。これにより片方の記憶装置に記録されているデータが破壊されたとしても、もう片方のデータで復旧することが可能となる。

b) バックアップ

磁気テープなど、本番環境のストレージ以外にバックアップとしてデータを退避させることで、データ破壊が発生した際に復旧することが可能となる。

クラウド・コンピューティング

クラウド・コンピューティングとは、インターネット上に拡散したコンピューティング資源を活用して、利用者(ユーザー)に情報サービスやアプリケーションサービス等を提供する、というコンセプトのことである。



クラウド・コンピューティングを利用したバックアップ

従来のコンピュータ・ネットワークでは、ネットワークはデータやメッセージ等が通過する経路という役割しか持たず、計算や情報処理を行う主体はあくまでも手元のコンピュータ(エンドノード)であった。

クラウド・コンピューティングにおいては、前出のイラストにあるように、サービスの提供者は大規模なデータセンターなどに多数のサーバーを用意し、遠隔からネットワークを通じてソフトウェアやデータ保管領域を利用できるようなシステムを構築し、ユーザーに提供する。ユーザーはパーソナルコンピュータやブラウザ、インターネット接続環境等の最低限のネットワーク接続環境を用意するのみでよい。

クラウド・コンピューティングを利用した場合、データのバックアップはこのクラウド上に送られることになる。

クラウドサービスの利点・欠点

クラウドサービスの利用者は最低限のネットワーク接続環境を用意するのみでサービスを利用できる。すなわち、サーバー群の導入など多額の設備投資を回避することが可能であり、またその調達や設定にかかる工数を短縮することが可能となる。

しかしながら、クラウドサービスにも欠点がある。

クラウドサービスへの接続環境に障害が発生するとクラウドサービス自体が利用できなくなる。また必ずしもクラウドサービス提供者の情報セキュリティの水準が、自社の情報セキュリティの水準を上回るとは限らない。さらに、データが保管されている場所が自国と異なる場合、データ保管国の法的規制に影響を受けるカントリーリスクがある。

これらの欠点があることも承知したうえで、サービスの検討を行うことが必要である。

10-7 情報の保護

MC
10-7-1 ~ 10-7-14

情報の保護

情報の重要性が高まれば高まるほど、機密性は高まる。

情報セキュリティ対策を実施する際に維持することが求められる要素の1つに機密性が含まれているように、情報が権限のない者に漏れないようにすることは、情報セキュリティを考える第一歩と言える。

eSACモデルによるITビジネスアシュアランス目標

eSACとはIIAが、eビジネスに関わるシステムの管理環境を評価するための枠組みとして作成したガイドラインである。

eSACではITビジネスアシュアランスの目標として、以下の5つが挙げられており、そのうちの1つに情報の保護に関する事項が含まれている。




eSACについては、Unit 9-3参照。

可用性 (Availability)	情報、プロセス、サービスが必要な時に利用可能であることを保証すること
能力 (Capability)	システム処理が確実にかつ適正な時間で完了する能力を保有していること
機能性 (Functionality)	ユーザーのニーズを満たす機能、応答性、使いやすさを備えていること
保護性 (Protectability)	不正なアクセスや使用から、ハードウェアやソフトウェア、データが保護されていること
説明性 (Accountability)	システム処理が正確に完了したこと保証するために、個人の役割、行動、責任が明確にされていること

マルウェア(Malware)

マルウェアはシステムの破壊目的よりも金銭的利益を目的とするものが多い。コンピュータ・システムへ侵入し、パスワードや財務データを収集するなどの犯罪が増加し続けている。マルウェアには以下のようなものがある。

 マルウェア(Malware): Malicious software (悪意のソフトウェア)を組み合わせて創られた造語である。

ワーム (worm programs)	利用者のディスクの空き容量やメモリがなくなるまで、自己増殖により破壊活動を行う。インターネットが普及するにつれ、電子メールなどを介して高速で自己増殖するものが出現している。
トロイの木馬 (Trojan horse)	正当なプログラムのコピー等外側からは他のもののように見えるが、無害なプログラムと利用者を信じ込ませてコンピュータへ侵入し、攻撃的手段によって、データ消去やファイルの外部流出などの破壊活動を行うプログラムのことである。トロイの木馬は単独の複製能力は持たないが、実行されるとより悪質なソフトウェアのインストールを可能にする等の影響がある。
論理爆弾 (logic bomb)	プログラムに特定の条件(特定の日、システム操作等)がそろった場合不正プログラムが作動する仕組みで、システム攻撃を開始する。
バックドア (back door)	通常の認証を回避し、不正侵入をするための裏口。(Wormによってもインストールされ得る。)

マルウェアに対するコントロール


マルウェアに対してはアンチウイルスソフトウェアによる検知、修復を通じて、感染前の状態に戻すことができる。ただし毎日のように新しいウイルスが誕生している現在においては、常に最新のウイルス定義にアップデートしておかなければマルウェアに対するコントロールとしては不十分である。

また、アンチウイルスソフトウェアは感染直前・又は感染後のコントロールとして有効であるが、そもそも感染させない、すなわち事前のコントロールを具備することも重要である。

事前のコントロールには、差出人不明の電子メールの添付ファイルを開かない等の利用者教育のほかに、組織が承認していないソフトウェアのインストール制限やウイルスの感染経路の一つであるUSBメモリなどを系統的に使用不可能にするなどが挙げられる。

様々な攻撃

現在のコンピュータ・システムは不正アクセスやコンピュータ・ウイルスなどの脅威にさらされている。悪意を持って他人のコンピュータのデータやプログラムを盗聴、改ざん、破壊などをするクラッカーと呼ばれる者が、インターネットなどのネットワークを通じて外部から様々な攻撃を仕掛けてくる。なおハッカーとはコンピュータに精通した人々に対する尊称であり、クラッカーとは区別される。

 ハッカーとクラッカーを区別しない場合もある。すなわち、悪意で他人のコンピュータのデータやプログラムに対する攻撃を行う者を、ハッカーということもある。

- a) ランサムウェア(Ransomware)
身代金要求型ウイルスとも呼ばれるコンピュータ・ウイルスであり、感染するとハードディスクなどを暗号化した上でロックし、解除するための金銭を要求するコンピュータ・ウイルスである。多くの場合、金銭を支払っても解除されない。
- b) ソーシャルエンジニアリング(Social engineering)
権限のある利用者などから心理的な策略によってパスワードなどのセキュリティ上重要な情報を入手することである。例えば、IDカードを忘れたと偽って借りること、役職を偽って(他人になりすまして)アクセス方法を聞きだすこと等がある。
- c) フィッシング(phishing)
正規のWebサイトや電子メールを装って、ユーザーからパスワードなどの情報を入手する手口。銀行のネットバンキングなどは金銭に直結するWebサイトであるため、フィッシングの標的になりやすい。
- d) DoS攻撃(Denial of Service attack)
サービスの可用性を侵害することを目的とした攻撃である。一斉にデータを送信することによりネットワーク上のトラフィックを増大させ、一時的にサービスのレスポンスを著しく悪化させる攻撃である

不正コピー

コンピュータ・システムの領域において複製は容易に実行可能である。ソフトウェアも同様に複製が可能であり、ソフトウェアの製造元が了解していない複製は不正コピーと呼ばれ、使用許諾契約(ソフトウェアのライセンス契約)上の違反行為となる。

ソフトウェアのライセンス契約は、組織体とソフトウェアの製造元との間での契約であり、多くの場合、ソースコードのライセンスを組織体が購入しない限り、ソースコードを解明するためにソフトウェアの逆コンパイルあるいは逆行分析(リバース・エンジニアリング)を行うことを明確に禁止している。

なお、バックアップ対象にプログラムが含まれていることが多い今日においては、障害回復のためにバックアップとしてソフトウェアのプログラムをコピーすることの合意が使用許諾契約上に明記されていることが望ましい。


 参考

サイバー・セキュリティ関連用語

APT 攻撃 (Advanced Persistent Threat)	特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃。
アドウェア (Adware)	無料で使える代わりに広告を表示するソフトウェア。アドウェアがマルウェアのような動きをする場合がある
ブートセクタ感染型ウイルス (Boot virus)	ブートとはコンピュータを起動し利用可能にするプロセスである。ブート領域に感染することによりコンピュータを起動不能に追い込むウイルスである
ボットネット (Botnet)	サイバー攻撃により乗っ取った多数のコンピュータで構成されるネットワークのこと
クリックジャッキング (Clickjacking)	ソーシャルメディア上の「いいね!」ボタンなどのクリック可能なコンテンツの下にハイパーリンクを隠し、クリックするとマルウェアのダウンロードや他のウェブサイトへ個人情報の送信などが実行されるサイバー攻撃。
クリプトジャッキング (Cryptojacking)	携帯端末やコンピュータを乗っ取り、ビットコインなどの暗号通貨のマイニング(発掘)行為に加担させるサイバー攻撃。暗号通貨にはマイニングと呼ばれる次のチェーンを計算することで入手可能なものがあるが、計算には多くのCPUなどのITリソースを必要とすることから、近年増加傾向にある。
DDoS 攻撃 (Designated denial-of-service attack)	多量のマシンから1つのサービスに、一斉にDoS 攻撃を仕掛けること
マクロウイルス (Macro virus)	Microsoft Officeのマクロ機能を悪用したコンピュータ・ウイルス
マルバタイジング (Malvertising)	不正広告とも呼ばれ、Web 広告からのマルウェア感染のこと
メモリ常駐型ウイルス (Memory-resident virus)	主にメインメモリに感染するウイルス。メインメモリ上に感染することによりアンチウイルスソフトウェアでの駆除が困難になる
パッチ (Patch)	バグ修正や機能変更を目的として既存プログラムを修正するプログラムのこと
ペネトレーションテスト (Penetration test)	検証対象のシステムに対して、想定される攻撃シナリオを複数用意し、実際に攻撃を行い、侵入または検証対象のデータの奪取ができるかどうかを検証するテスト。

ファーミング (Pharming)	不正なスクリプトによってインターネットの閲覧者を偽のWebサイトに誘導し、不正に個人情報を得るフィッシング詐欺の類似手法
セッションハイジャック (Session hijacking)	通信を乗っ取り、本人に代わって「なりすまし」ログインを行うサイバー攻撃。本人変わってログインすることで、ログイン先の機密情報などを盗んだり、不正送金などを行う。
スパム (Spam)	一斉にばらまかれる迷惑メール
スプーフィング (Spoofing)	インターネット上で他人になりすまし、情報盗用などを行うこと。スプーフィング(なりすまし)には、メールの発信元のアドレスや名前を偽装するメールスプーフィング、偽のIPアドレスを用いてサーバーに侵入を試みるIPスプーフィング等がある。
スパイウェア (Spyware)	ユーザーに知られることなく情報収集することを目的とした不正なプログラム
デマウイルス (Virus hoax)	存在しないウイルスを存在するかのように装う詐欺
ゼロデイ攻撃 (Zero-day attack)	システムに脆弱性が見つかり、修正プログラムが適用される日(これをOne Dayと呼ぶ)よりも前の攻撃のこと

10-9 最新のテクノロジーとセキュリティへの影響

BYOD(Bring your own device)

私的デバイスの業務利用のこと。従来は情報漏洩リスクを危惧して私的デバイスの業務利用を禁止する企業が多かった。しかしながら、スマートフォンをはじめとした携帯端末の高性能化によりセキュリティ強化が可能になったことを背景に、常に持ち運んで使い慣れた私的デバイスを業務利用した方が効率的であることが増えたため、BYODを導入する企業が増えた。

BYODを導入する際、企業は以下のことを検討する必要がある。

- a) 私的デバイスを使用する際の基本的なルールの制定
- b) 私的デバイス自体のセキュリティ対策
- c) 紛失・盗難時の対応
- d) 退職時のデータの削除方法

リモートワイプ

携帯端末を紛失した際、遠隔操作により全てのデータを削除(破壊)することで携帯端末から情報を抜き取ることを防止する技術のこと。BYODが広がった背景にはリモートワイプ技術の発展がある。

リモートワイプは遠隔操作によるデータの削除技術であって、工場出荷状態に戻すといった初期化の技術ではない。最近では特定のデータのみを削除することも可能になってきている。

スマート・デバイス(Smart Device)

あらゆる用途に使用可能な情報機器の総称。スマートフォンやタブレットに限らず、個人の健康関連データを測定するウェアラブル機器やネットワーク接続された家電なども含む。スマート・デバイスは一つのOS上で様々なアプリケーションソフトウェアが稼働し、ネットワークとも常時接続していることが多いため、端末単体のセキュリティ対策として、認証やウイルス対策、暗号化、紛失・盗難対策などの実施が必要となる。

IoT(Internet of Things)

一般的にモノのインターネットと訳され、家電などの様々なモノがインターネットに接続され、情報交換することで、相互に制御する仕組み。例えば、レコーダーをネットワーク接続することで家の外からのテレビ番組の録画や、個人の健康関連データを測定するウェアラブル機器から情報を収集し統計分析が実現できる。IoTにおいてもネットワーク接続に関連するセキュリティ対策(認証やウイルス対策、暗号化など)が求められる。

クラウド・コンピューティング

クラウド・コンピューティングでは、VPNなどの専用回線を用いたセキュリティ対策などを行う必要があるが、アプリケーション・ソフトウェアやデータが保管されているサーバーなどのセキュリティ対策は、クラウドサービスの提供者のセキュリティ水準に依存することになる。このため、クラウド・コンピューティングを利用するには、クラウドサービス提供者のセキュリティ水準が、自社が定めるセキュリティ要件を満たすかを検討し、必要に応じてセキュリティの見直しを要求する必要がある。

ブロックチェーン

ブロックチェーンとは分散型ネットワークによるデータベースである。ブロックと呼ばれるデータ単位を、ネットワークを通じて鎖のように連結していくことで全体のデータを構成する技術であり、ビットコインの中核技術として利用されている。ブロックには前のブロックのリンク情報が含まれており、このリンクを辿ることでチェーンを構成している。各ブロックの管理は分散されたサーバーで行われているため、全てのブロックのデータを一度に改ざんすることはできない仕組みとなっており、たとえデータの改ざんが発生しても、他のブロックとの整合性を失うため、即時に発見され、修復されることになる。

RPA(Robotic Process Automation)

主にパソコン上での作業を自動化し、またその作業を監視するツール。元々はシステム開発時におけるテストにおいて、大量のテストデータの投入を行う際に利用されていたツールである。RPAは人間のパソコン上での作業を記録した上で、繰り返すことや事前に定められた時刻にその処理を実行することができる。なお記録した作業については加工することが可能であるが、極力コーディング作業を必要としないようなユーザーインターフェース(UI)が開発される傾向にある。RPA導入によって単純作業の自動化が可能となるため、作業の効率化が進むが、承認行為などをRPA化することは厳禁である。



コーディング：
処理をプログラミング言語で記録することを指す。



ユーザーインターフェース：
(User Interface; UI):
システムと人との間で情報をやりとりするための仕組みの総称。ソフトウェアの画面使用のこと。

AI(Artificial Intelligence)

人工知能のことであり、ディープラーニング(深層学習)と呼ばれる技術の発明によって、近年脚光を浴びている技術である。ディープラーニングとは多層化のニューラルネットワークによる機械学習手法であり、これまでのコンピュータが苦手とした情報の取捨選択による重要知識の蓄積(情報の最適化)を、人の神経細胞を模した構造(これを多層化ニューラルネットワークと呼ぶ)で実現している。

セキュリティの観点からはAIは以下の3つの検討領域がある。

a) AIからのセキュリティ

AIは必ずしも正しい結果を提供してくれるわけではない。例えば、自動運転をサポートするAIの場合、危険に直面した際に経済的損失と人命のいずれを優先して回避行動をとるのかについて、正しい結果を導くための十分な機械学習が必要となる。

b) AIのセキュリティ

AI自身がハッキング等を受けることに対するセキュリティを考慮する必要がある。

c) AIによるセキュリティ

AI自身をセキュリティ対策の一つとして活用する方法で、例えばDoS攻撃を受けていることの自動検知及び対処などの活用が可能である。















CIA

テキスト Part 3-2

2005年11月10日 初版第1刷発行

2021年10月1日 第9版発行

編者：三輪 豊明

発行：株式会社アビタス

Abitus

〒151-0053

東京都渋谷区代々木2-1-1

新宿マインズタワー 15F

03-3299-3222 (phone)

03-3299-3777 (facsimile)

<https://www.abitus.co.jp>

Material from "The International Professional Practices Framework (IPPF)"

Copyright © by The Institute of Internal Auditors · 247 Maitland Avenue · Altamonte Springs,
Florida 32701-4201 U.S.A.,

are reprinted and translated with permission.

本書の内容の一部または全部の無断複写、無断転載、及び無断転売を禁止します。

2021 Abitus, Inc. All rights reserved.