公認内部監査人(CIA)
Part III／第5回

※アビタスCIA本講座講義資料のため、MUFG CIA受験対策講座の実施回と異なります。

Abitus

Part 3 コースシラバス

			ページ
第1回	Chapter 1	戦略	1 〜 44
第2回	Chapter 2 Chapter 3	業績測定方法 組織行動	45 〜 90
第3回	Chapter 4 Chapter 5	リーダーシップ 組織構造とビジネス・プロセス	91 〜 142
第4回	Chapter 6 Chapter 7	データアナリティクス アプリケーションおよびシステム・ソフトウェア	143 〜 195

Part 3 コースシラバス

			ページ
第5回	Chapter 8 Chapter 9-1 ～ 9-8	ITインフラストラクチャー ITコントロール・フレームワーク、災害復旧	2 ～ 41
第6回	Chapter 9-9 ～ 9-10 Chapter 10	ITコントロール・フレームワーク、災害復旧 情報セキュリティ	42 ～ 78
第7回	Chapter 11-1 ～ 11-11	財務会計	79 ～ 103
第8回	Chapter 11-12 ～ 11-16 Chapter 12-1 ～ 12-4	財務会計 財務(ファイナンス)	104 ～ 150
第9回	Chapter 12-5 ～ 12-12	財務(ファイナンス)	151 ～ 182
第10回	Chapter 13-1 ～ 13-8	管理会計	183 ～ 204
第11回	Chapter 13-9 ～ 13-18	管理会計	205 ～ 227

8-2　ネットワーク　(1)対象地域による分類

論点　ネットワーク

ネットワークとは、複数のコンピュータや端末を通信回線によって接続し、相互に情報を交換するシステムである。より厳格には以下のように定義される。

定義　ネットワークとは、プリンタのような2つ以上のコンピュータが情報や資源を共有するための接続又は経路の配置である。

ネットワークの対象地域による分類

ネットワークを対象地域で分類すると、LAN(local area network; 構内情報通信網)と、WAN(wide area network; 広域通信網)に大別することができる。LANは、同じ建物の中などにあるコンピュータやプリンタなどを接続して、データを伝送するネットワークであり、WANは本社－支社間など地理的に離れた地点にあるコンピュータ同士を接続して、データを伝送するネットワークである。

a) PAN(personal area network)

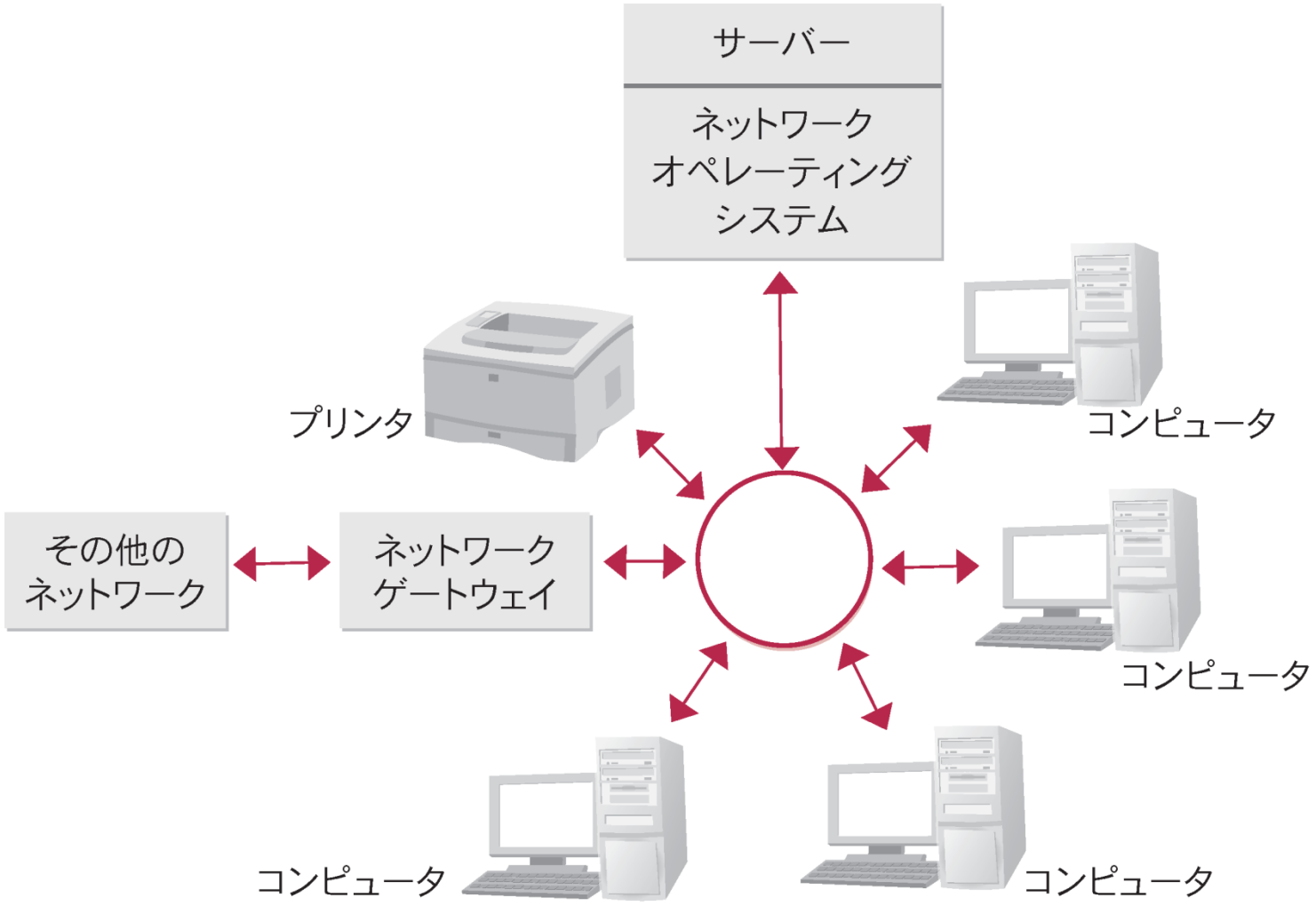
個人が使うコンピュータ機器の間等、狭い領域の通信に使用される。

b) LAN(local area network; 構内情報通信網)

定義 LANとは、一つ又は近接する複数の建物などの限定された地域を範囲とした、専用伝送路による電気通信網である。

LANの主たる特徴は以下の通り。

1） 限定された地域内に設置されていること。
2） パソコンやワークステーションを相互に接続すること。
3） LANの設備は利用者が自ら設置する私設ネットワークであること。
4） 伝送速度が高速であること。


サーバー
ネットワーク
オペレーティング
システム
プリンタ
コンピュータ
その他の
ネットワーク
ネットワーク
ゲートウェイ
コンピュータ
コンピュータ
コンピュータ

上の図は、LANの一モデルであるが、LANにより、電子メールの交換、ファイルの共有、プリンタの共有、及びデータベースの共有が簡単にできる。サーバーは、データファイルやプログラムを保存しそれらをネットワーク利用者のために提供する。また、ネットワークゲートウェイが、LANと公設データネットワークを接続することで外部のネットワークとの情報交換も可能になる。

c) MAN（metropolitan area network; 都市内情報通信網）

LANの領域を広げたもの。同一都市内の近接オフィス数箇所をグループ化したものがこの例である。

d) WAN（wide area network; 広域通信網）

地理的に広範囲に広がる地点にあるコンピュータ同士を接続してデータのやり取りを行う。国や大陸全体に展開されることもしばしばである。

8-4　ネットワーク　(3)情報処理方法による分類

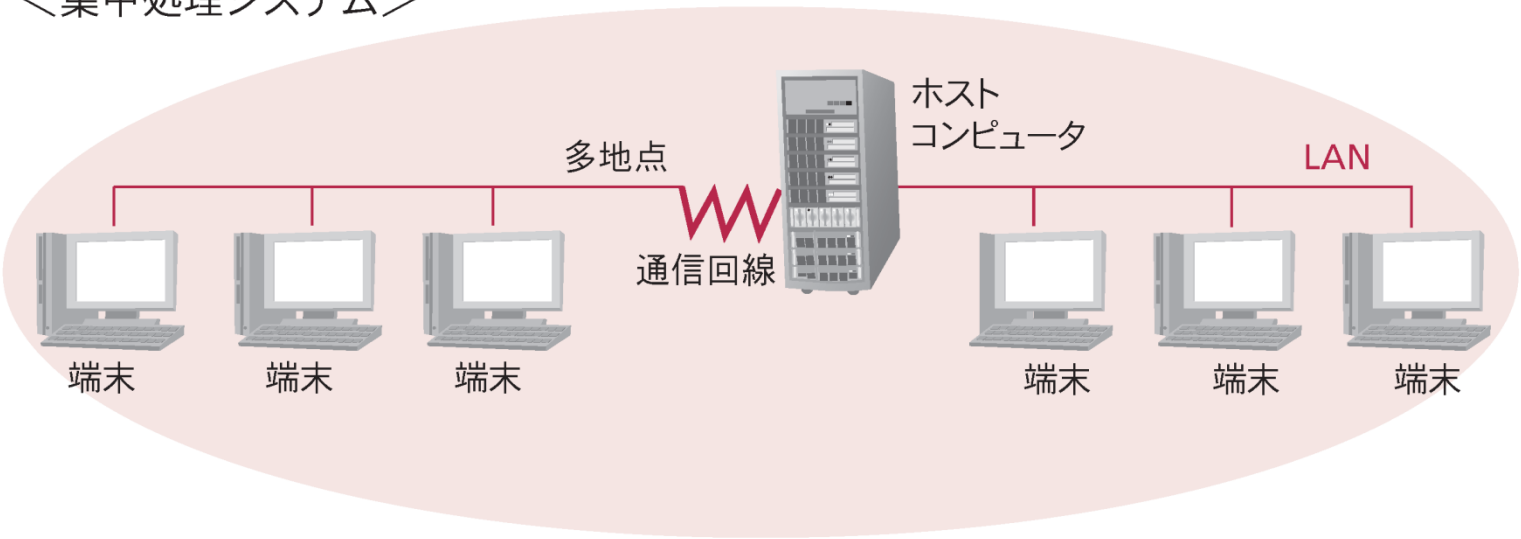
コンピュータ・ネットワーク

今日、コンピュータ単体で処理業務を行うことはほとんどなく、処理業務はネットワーク内のコンピュータによって行われる。

a) 集中処理

一台の大きなコンピュータによって処理することを、集中処理という。集中処理では、1 ヶ所で一元的にデータ処理を行うので、データはリアルタイムに更新できるが、ホストコンピュータの機能障害により、全システムがダウンする。

＜集中処理システム＞



集中処理システム

問題点

ホストコンピューターへの負担は重い

→ 障害回復計画が重要

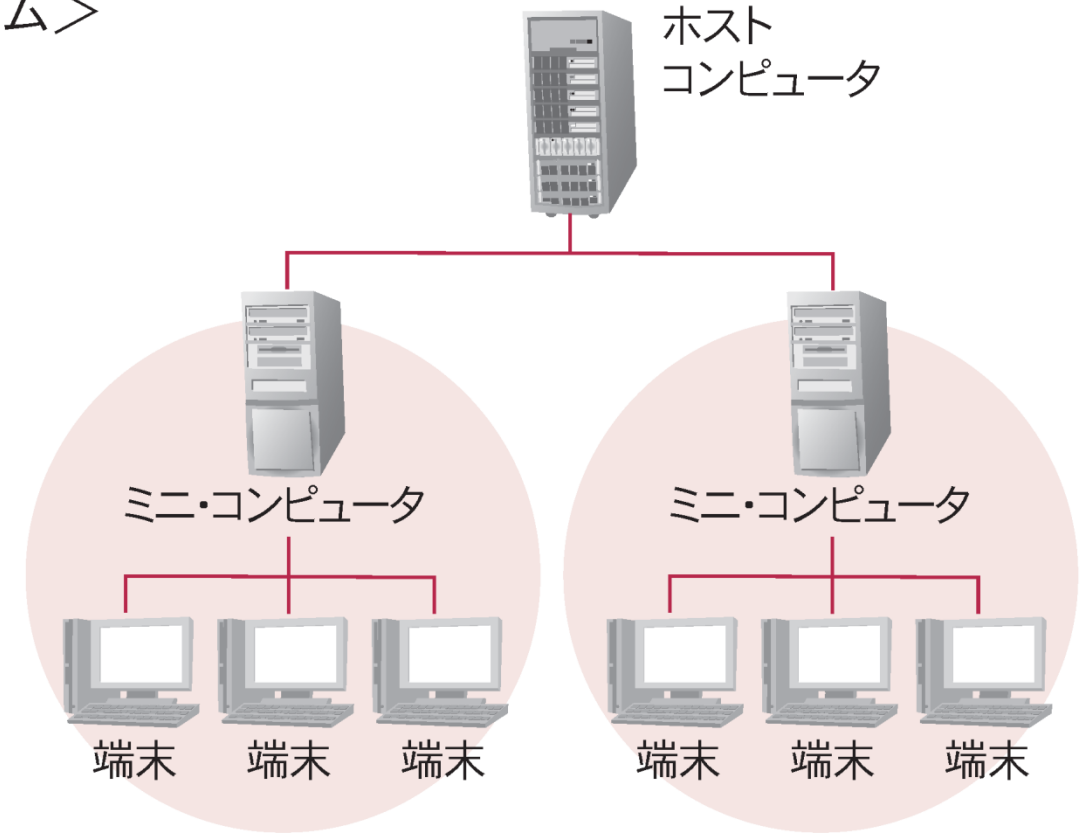
利点

機密保護やセキュリティの確保、運用管理が容易

b）分散処理

LAN等の通信網によって接続された複数のコンピュータが処理を分散するシステムを分散処理という。分散処理システムでは、個々の利用者のニーズは小型コンピュータで対応でき、ホストコンピュータへの負荷も比較的小さい。

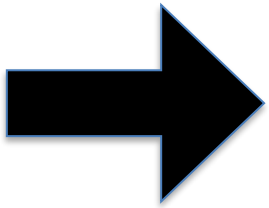
＜分散処理システム＞



分散処理システム

問題点

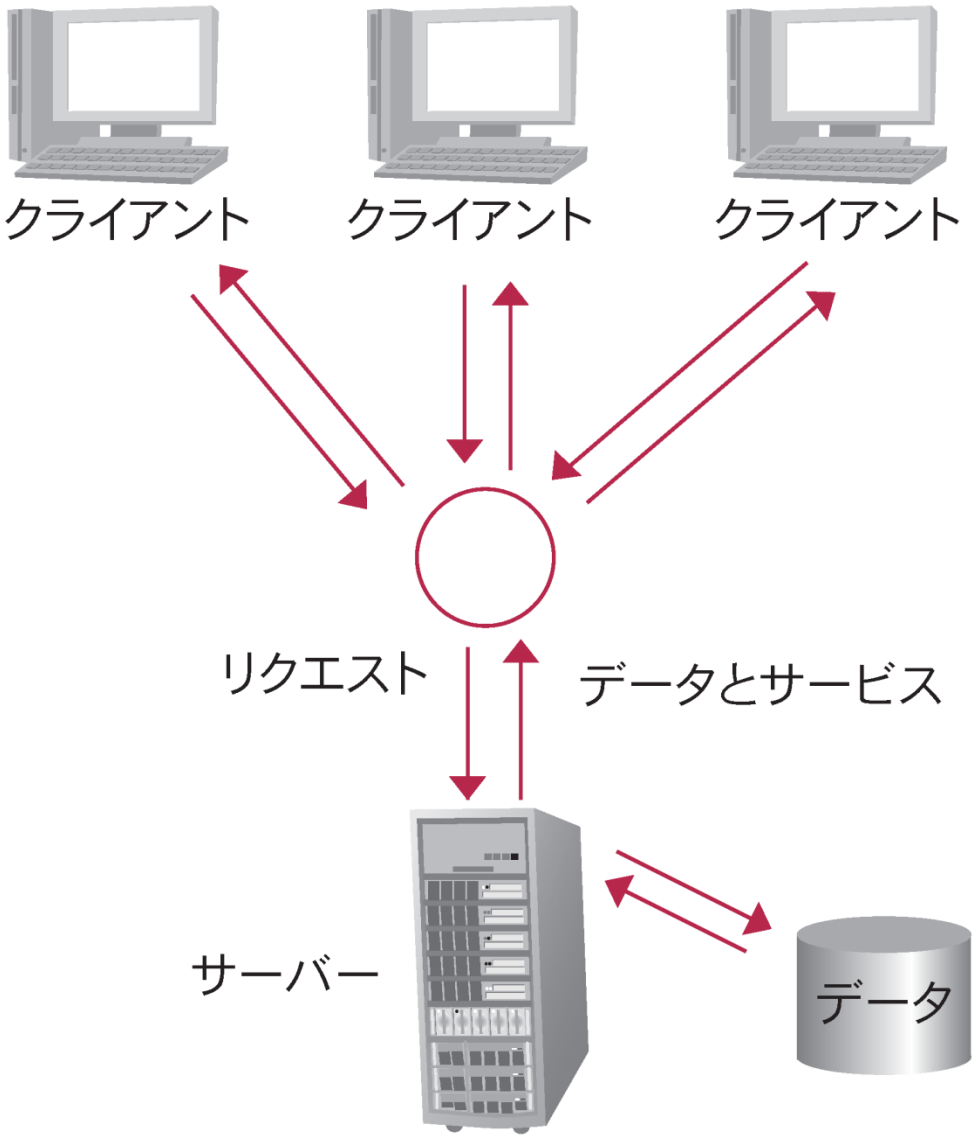
モニタリングがしづらい



アクセス統制が重要

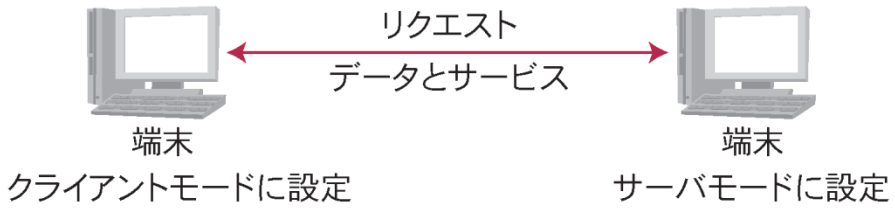
c)　クライアント・サーバー処理（client/server processing）

クライアント及びサーバーという役割を持つコンピュータによって処理を分散しているシステムを、クライアント・サーバー処理システムという。クライアントはサーバーに対してサービスをリクエストし、処理の結果を受け取る。サーバーはファイル管理、印刷制御等を、クライアントの要求に応じて行う。一般に、サーバーはクライアントよりも高性能なコンピュータを用いる。


クライアント
クライアント
クライアント
リクエスト
データとサービス
サーバー
データ

d)　ピアツーピア処理(peer-to-peer processing)

ピアツーピア処理においては、それぞれのパソコンは互いにクライアントとサーバーの役割を受け持つが、専用のサーバーを用意せず、対等の立場で処理業務を共有する。専用サーバーを必要としないため費用もあまりかからず、小規模なLANでプリンタ等を接続するのに向いている。



Key Point

分散処理、集中処理の利点、リスクは？

8-6　ITに関わる内部監査部門の役割

ITに係るリスク・マネジメント

ITに係るリスク・マネジメントとは、リスクを識別し、評価し、許容できるレベルまで軽減するプロセスと定義される。

論点 ITに係るリスクのマネジメント

経営幹部や経営管理者の責任で

ITに係るリスク・マネジメントは通常以下のプロセスを踏む。

情報資産の評価	組織体が価値を置く全ての情報資産を識別する
脅威の評価	情報資産に影響を与え得る有害な事象の発生可能性を識別する
脆弱性の評価	情報資産の全ての弱点とその重度を識別する
リスクの判定	情報資産に対するリスクを評価し優先順位を付ける
リスクに対する決定	情報資産に対するリスクを許容するか、移転するか、軽減策をとるかについて決定する **リスク対応の決定**

a）「基準」では、内部監査人がリスク・マネジメントプロセスの有効性の評価及び改善に貢献することを要求している。また、アシュアランス業務については、以下の通り情報システムのリスク評価についても明示している。

「基準」2120：リスク・マネジメント；「基準」2120.A1

内部監査部門は、リスク・マネジメント・プロセスの有効性を評価し、リスク・マネジメント・プロセスの改善に貢献しなければならない。(2120)

内部監査部門は、以下の各事項に関わる組織体のガバナンス、業務および情報システムに関するリスク・エクスポージャー(リスクに曝されている度合い)を評価しなければならない。

- 組織体の戦略目標の達成状況
- 財務および業務に関する情報の、信頼性とインテグリティ
- 業務とプログラムの有効性と効率性
- 資産の保全
- 法令、方針、定められた手続および契約の遵守(2120.A1)

b） IT環境の中でCAEが考慮すべき層は、ITマネジメント、技術的インフラストラクチャー、アプリケーション、外部との接続である。CAEは監査資源が各層に適切に配分されることを確保しなければならない。

有効なITコントロールの指標

ITコントロールの必要性は、情報資産の保護だけでなく、コストのコントロールから競争力の維持、及び法規制へのコンプライアンスまで様々である。

ITコントロールに関する内部監査部門の役割

「基準」2130では、コントロールに関する内部監査部門の役割について、以下のように規定している。

「基準」2130：コントロール

内部監査部門は、コントロール手段の有効性と効率性を評価し、継続的な改善を進めることにより、組織体が有効なコントロール手段を維持することに役立たなければならない。

GTAG-1

GTAG-1では、ITコントロールに係る内部監査人の役割として次の項目を挙げている。

- ITインターナル・コントロールに関する問題について、監査委員会や経営幹部に対して助言する。
- 監査対象領域および監査計画にITが含まれていることを確実にする。
- 監査部門に資源と優先順位を割り当てる際に、ITリスクが考慮されていることを確実にする。
- 内部監査部門が必要としているIT資源を定義する(監査スタッフの専門的な教育訓練を含む)。
- 各々の監査について、監査計画がIT問題を考慮にいれていることを確実にする。
- 監査対象部門と連携し、何を知りたいのか、何を知るべきなのかを決定する。
- ITリスクの評価をする。
- 信頼性があり、検証できる証拠の構成要素を決定する。
- 全社レベルのITコントロールの監査を実施する。
- IT全般統制の監査を実施する。
- ITのアプリケーションコントロールの監査を実施する。
- 専門的かつ技術的なITコントロールの監査を実施する。
- ITの有効かつ効率的な利用による、監査手続を支援する。
- システム開発またはシステム分析活動の際に、コントロールがどのように導入され、または回避されるのかを理解している熟達者として活動する。
- 既知の、及び文書化されたITリスクを最小化する、正式な活動の実施をモニタリングし検証することを支援する。

IT監査の実施

簡単！IT監査の例

- IDの作成、削除が適切に行われているか
- ITシステム導入前のテストを行っているか
- ITシステムの入力と承認が分離されているか

8-7　職務の分離

職務の分離

職務の分離とは、一般的に取引の承認、記録、及び保管をそれぞれお互いから独立したものに担当させることで、相互にチェックできる体制を構築し、不正や誤謬を防止するコントロールである。

IT環境においても職務の分離という概念は非常に重要である。以下では組織内における職務の分離と情報システム部門内での職務の分離の2つの観点から考える。

a) 組織内における職務の分離

情報システム部門は利用部門(ユーザー部門)から独立していなければならい。利用部門とは、情報システムを利用する部門を指す。

利用部門は情報システムに記録された取引データの内容に責任を有し、情報システム部門は情報システムの安定稼働やデータの完全性などを担保することで利用部門のシステム利用をサポートする責任を有している。
情報システム部門はその責任を果たすべく、アプリケーション統制などを回避できるシステム権限を保持している。利用部門とシステム部門が分離されていない場合、情報システム内のデータがアプリケーション統制を通じて登録されたデータ、すなわち承認された正規のデータであるか否かの判断が難しくなり、情報システムのデータの信頼性が低下することに繋がる。このため両者は明確に分離されなければならない。

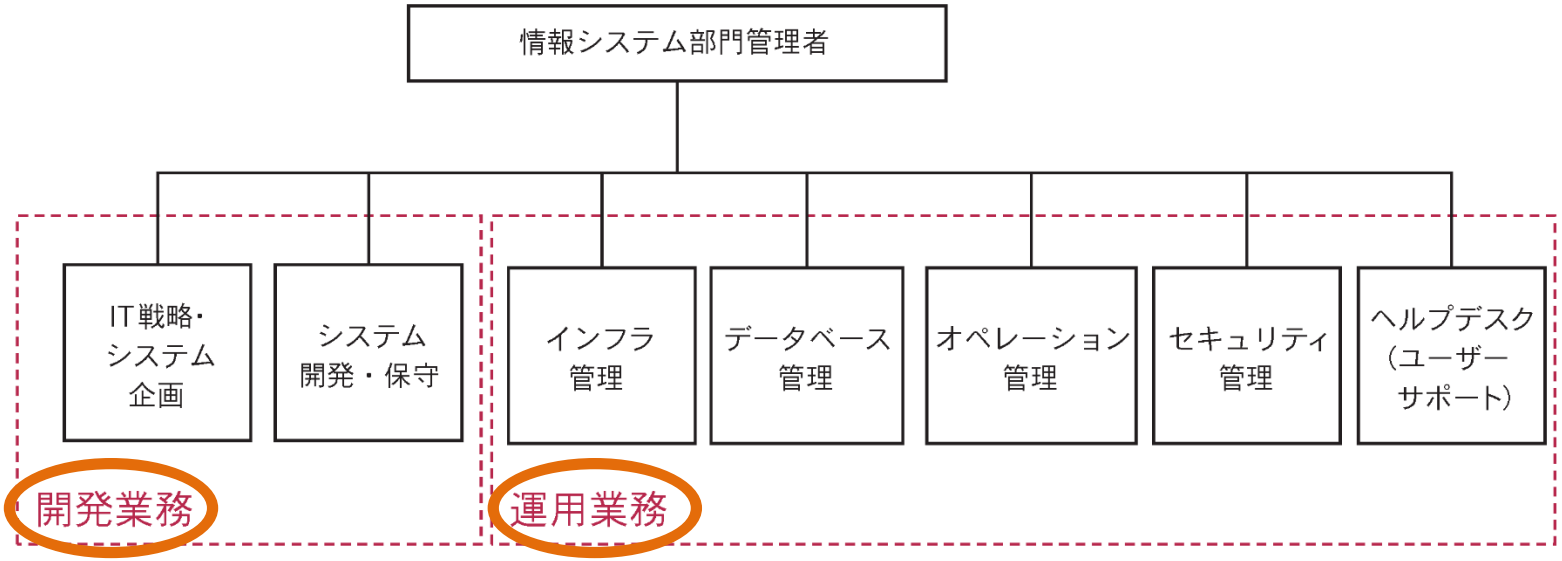
この組織内における職務の分離を達成させるためには、企業内で次のような機能設計が必要である。

1） 全てのシステム取引は、利用部門によって着手され、承認されなければならない。
2） 既存のシステムの変更、及び新規システムの導入は利用部門からの公式な文書での承認が必要である。
3） データ処理中に発見された間違いの修正については、エラーログに掲載の上、特定の利用部門に修正について問い合わせをしなければならない。

b) 情報処理部門内での職務の分離

情報システム部門はアプリケーション統制を回避できる高権限を有しており、適切に職務の分離がなされないと、無制限のデータアクセスを許してしまい、個人による不正が行われる可能性がある。このため、情報システム部門内の不正リスクを減らす目的で、少なくとも開発業務と運用業務の担当（または部門・グループ）を分離することが必須となる。

以下は、情報システム部門の主な機能である。



ポイント：開発者と運用を分離して、開発者には本番環境に触れさせないようにする

〈情報システム部門の主な機能と役割〉

情報システム部門管理者	情報システム部門の責任者。大規模な組織では最高情報責任者（Chief Information Officer; CIO）が配置される。
IT戦略・システム企画	最新のIT情報を収集し、組織のIT戦略を立案する役割を担う。
システム開発・保守	アプリケーション・システムの開発、保守（既存システムの変更を含む）を担う。
インフラ管理	ネットワークや関連機器の管理、サーバーなどのハードウェアの管理及びオペレーティングシステムの管理を担う。ネットワーク機器の管理だけを総務部門などに切り出している組織もある。

データベース管理	データベースの監視・メンテナンスなどのデータベースの管理業務を担う。データベースの完全性を担保する責任がある。
オペレーション管理	情報システムのジョブスケジューラの監視など、情報システムの日常業務を担う。
セキュリティ管理	システム・オーナーから委任されたセキュリティの導入・維持の役割を担う。セキュリティ対策ソフトの導入やアップデートを行う。
ヘルプデスク	利用部門(ユーザー部門)からの問い合わせ対応を担う。パソコンの不具合やソフトの簡単な使い方などの対応は行うが、高度な内容の問い合わせに対しては情報システム部門内の関連部署にエスカレーションする。

〈その他の機能等〉

システム・アナリスト	利用者のニーズに基づいてシステムを設計し、設計文書を作成する。
プログラマー	アナリストが作成した文書を基にプログラミングする。
品質保証	品質保証の担当者は通常、品質管理、及び品質保証の２つの業務を担当する。
Web マスター	Web サイトのデザイン、開発、維持・管理を担当する。
媒体管理 （ライブラリアン）	コンピュータ及びディスクに保存しているすべてのプログラム、データファイルの記録、発行、受領及び保護を担う。インフラ管理のうちプログラムとデータに特化した表現。

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。

論点　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

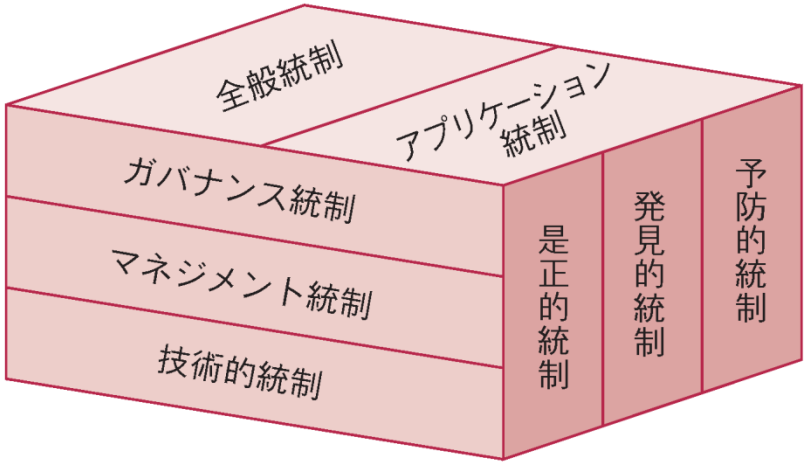
完全性

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統制のあるべき姿

〈ITコントロールの分類〉

1 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。
2 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。
3 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。
4 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。

5 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。
6 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
7 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
8 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

ITコントロールの分類

① 組織全体のITシステムに関わる統制

② ITを通して行われる、個別取引に関する統制

③ 取締役会の責任（監視）

④ 経営幹部や各部門長の責任（運用）

⑤ IT部門の責任（開発）

⑥ 未然防止

⑦ 適時発見

⑧ 修正

9-3　ITコントロール・フレームワーク

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とり得、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。

Key Point: **組織のITガバナンスとマネジメントの成熟度を評価するのに役立つフレームワーク**

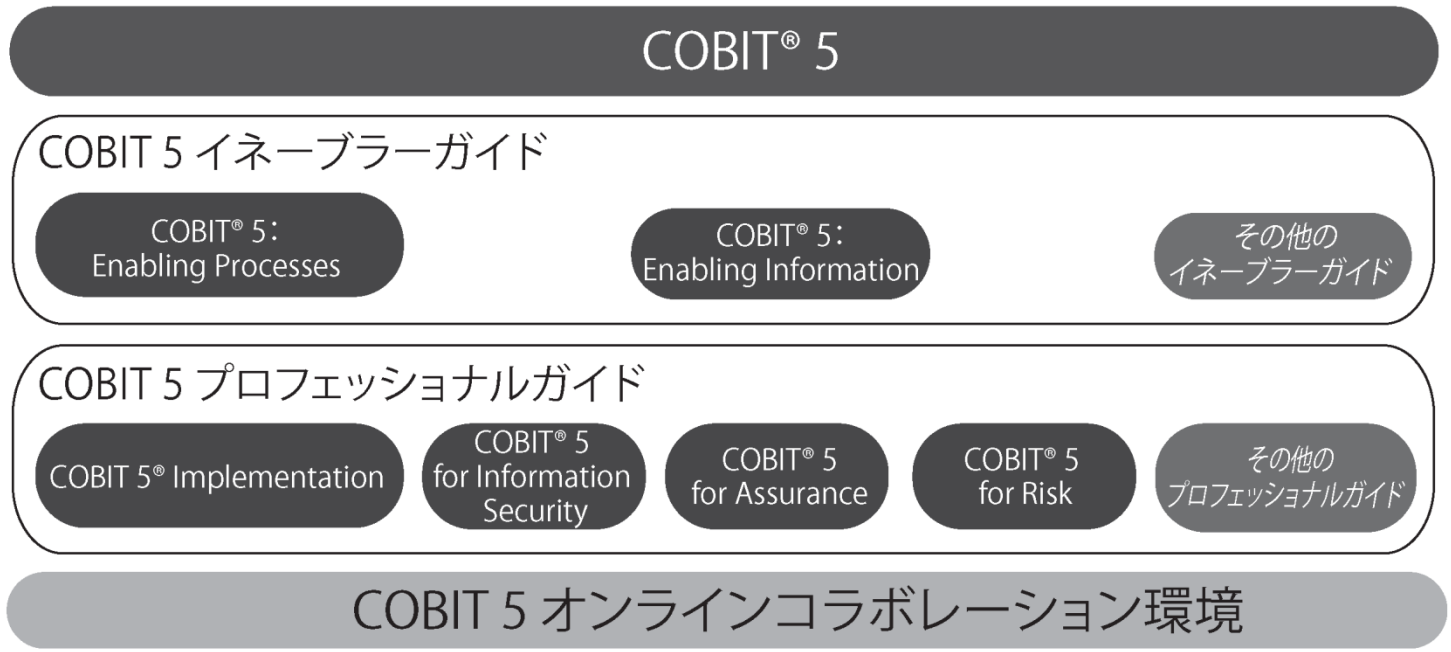
ル・[illegible]のフレームワークを提供している。

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)。

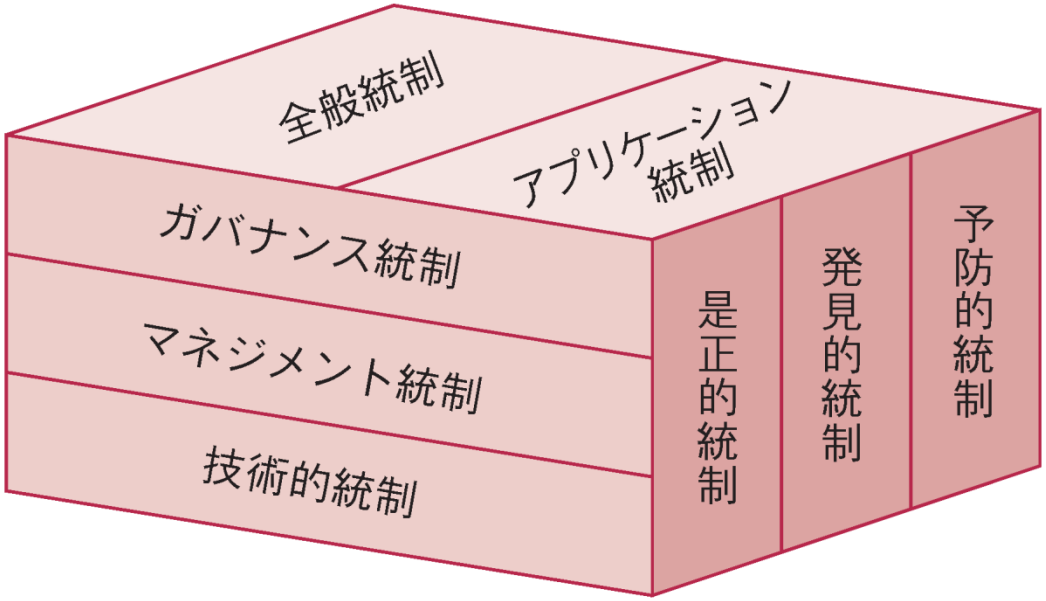
図表 1 — COBIT 5 プロダクトファミリー



Source: COBIT 5

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

IT監査のガイダンス

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。

9-4　情報システムの構築による影響

論点　情報システム

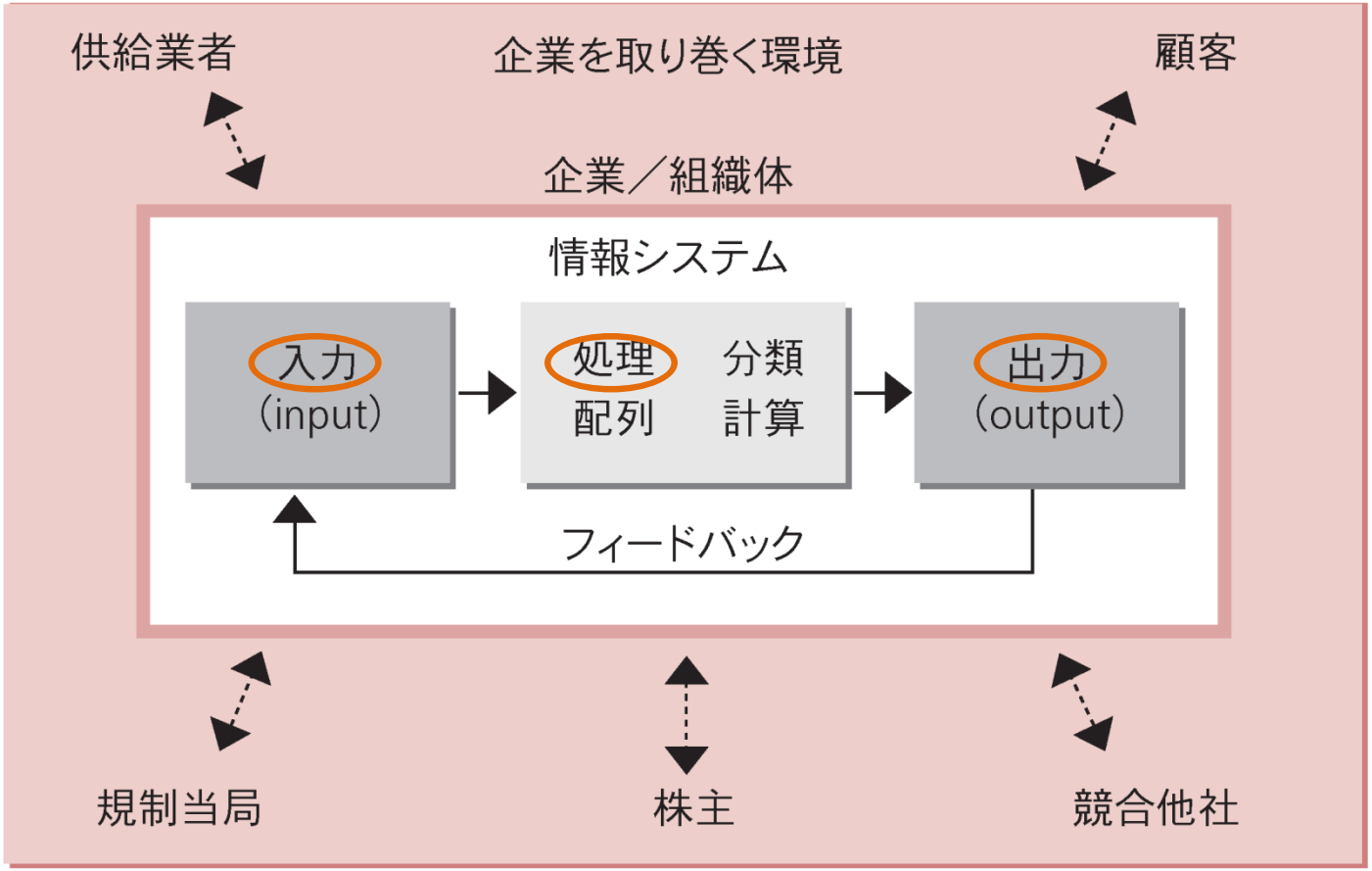
情報システムとは、組織体または社会の活動に必要な情報の収集、処理、伝達に関わる仕組みである。

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。

3要素

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。

IT化がICや、内部監査に与える影響

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。

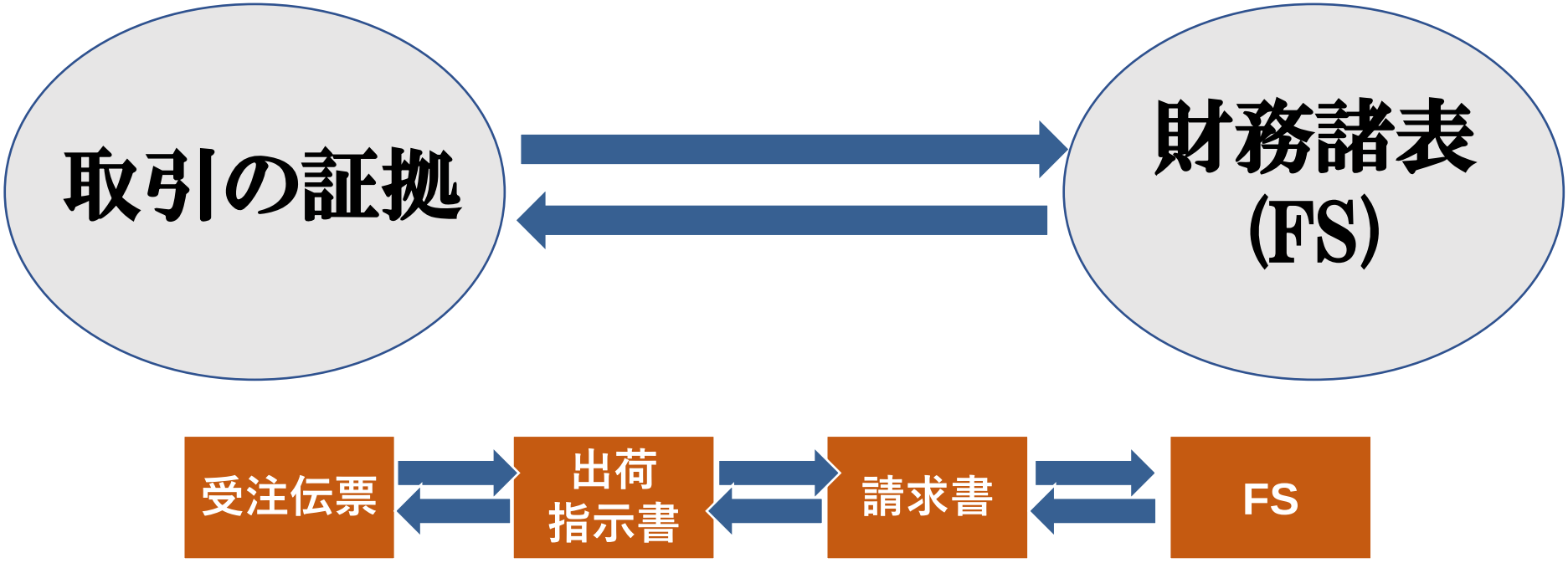
c) 多くの人が分担をして行っていた職務が、コンピュータによって集中処理することが可能になるため、従来の職務の分離の概念が適用されなくなる。また、コンピュータにアクセスが可能な個人が、複数の業務内容にアクセス可能になるため、新たなコントロールが必要になる。

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(Audit Trail)

取引の発生源(証拠)から、成果物(財務諸表)までの道筋、またはその逆



9-5　データ処理方法

データ処理方法

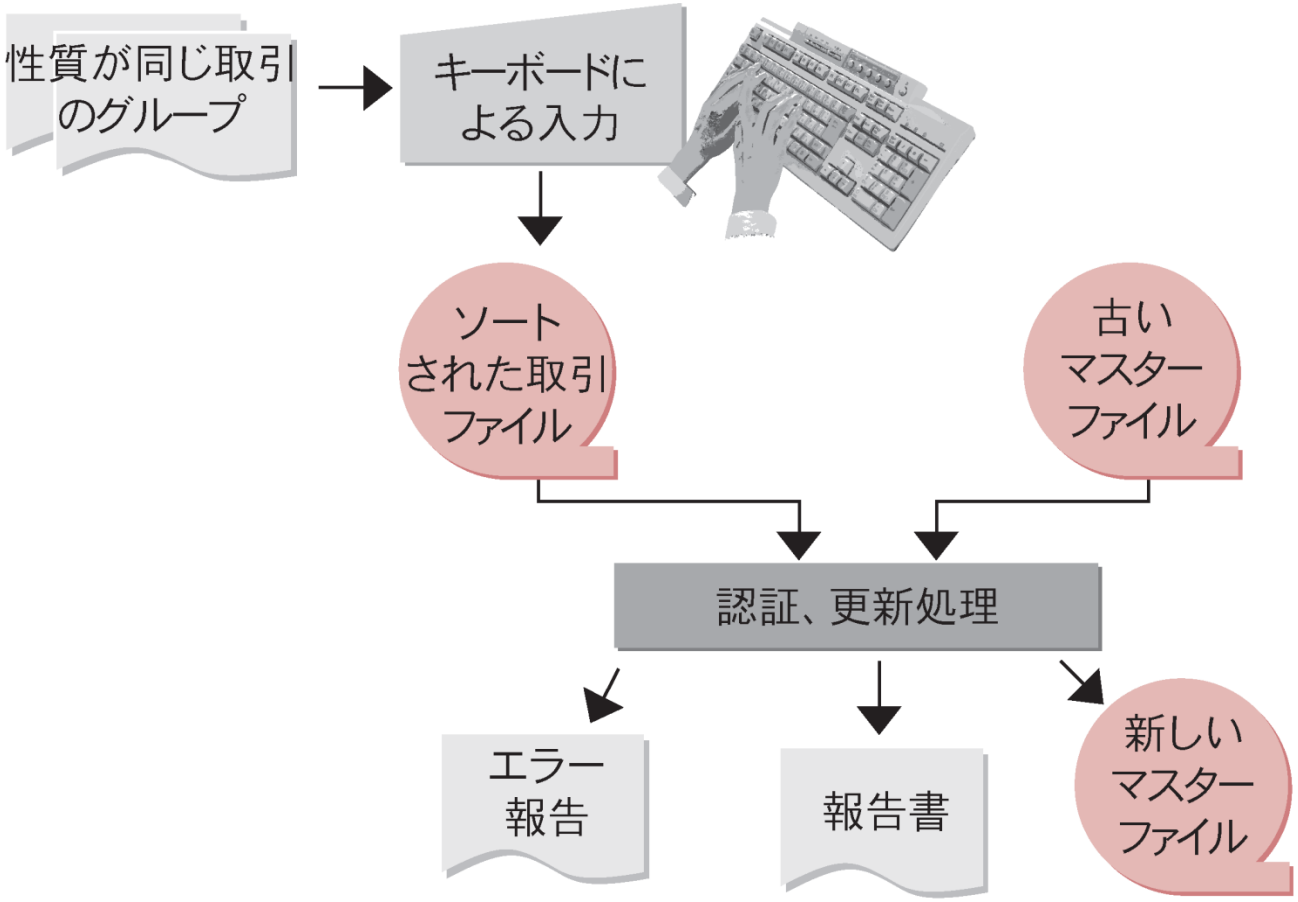
データ・ベース内のデータが更新されるタイミングは、データ処理の方法によって異なる。

論点　バッチ処理とオンライン・リアルタイム処理

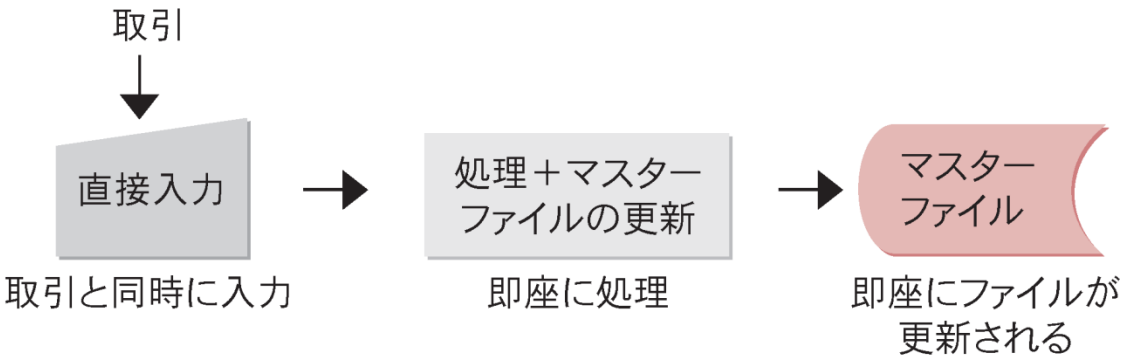
バッチ処理とオンライン・リアルタイム処理は以下の特徴を持つ。

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。


性質が同じ取引のグループ
キーボードによる入力
ソートされた取引ファイル
古いマスターファイル
認証、更新処理
エラー報告
報告書
新しいマスターファイル

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。



バッチ処理

比較的簡単に、監査証跡(Audit Trail)を得る事が出来る。

OLRT処理

監査証跡(Audit Trail)は得づらい。

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。

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。

全般統制との関係

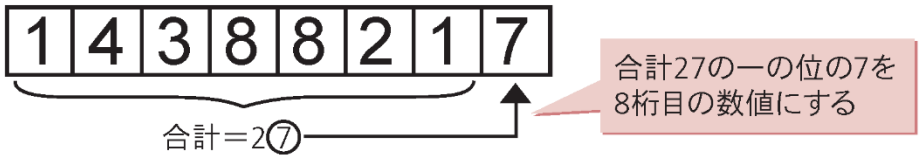
全般統制はアプリケーション統制が継続的に有効に機能していることを担保する。

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)　エディットチェック=入力統制

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かめる。
(例)	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。 
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、それ以外のものは受け付けない。
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。

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　処理履歴
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。

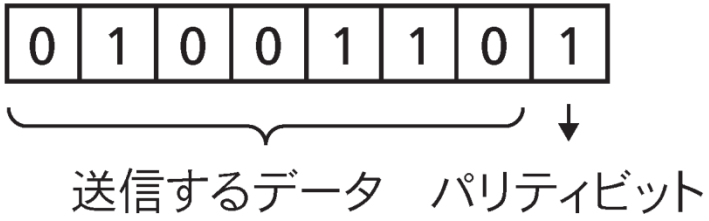
b) 処理コントロール

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）

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。

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。



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。

合計する事に意味のある数字を合計してチェックする

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。

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。

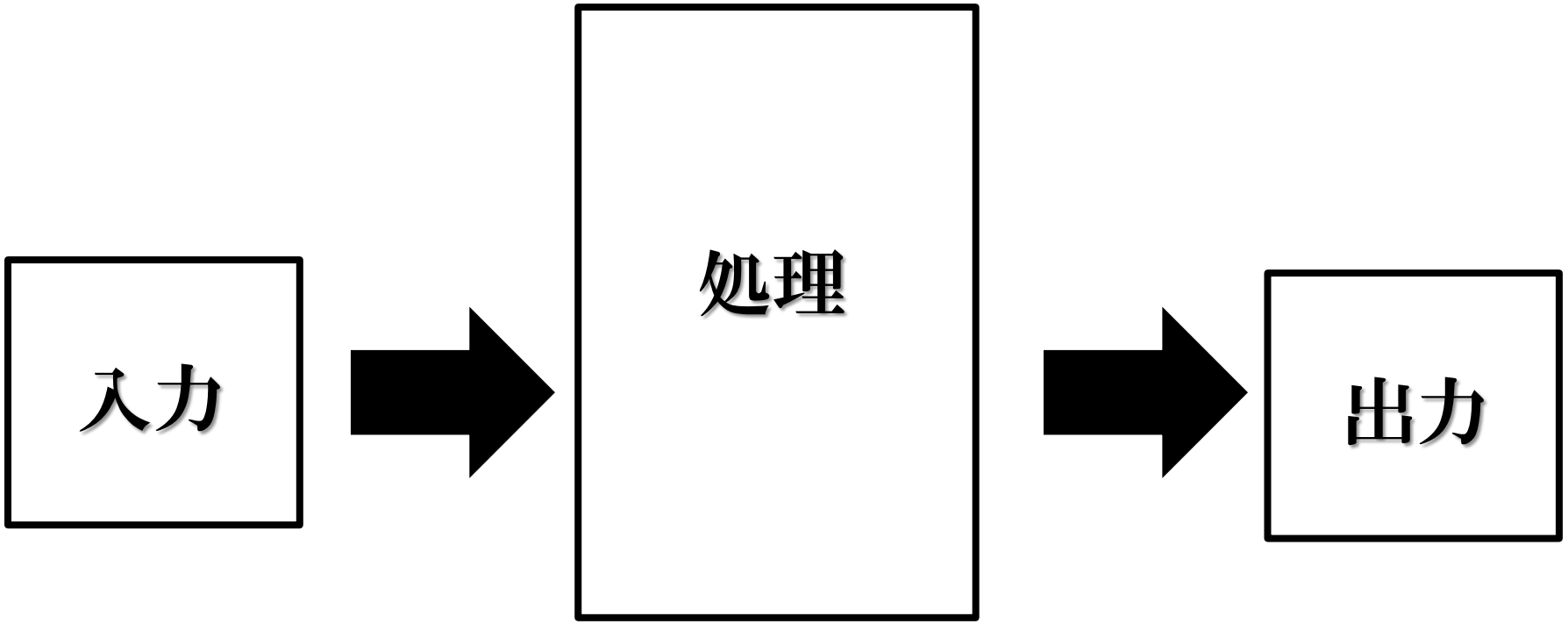
- 換金性、機密性、重要性がある書類の受渡記録の管理、および安全な場所での保管。
- 出力帳票の配布。
  出力帳票は予め承認された配布媒体(パラメータ)を用いて配布される。オペレーション担当は出力の完了および配布がスケジュール通り行なわれているかを調査し、また配布前には配布記録をとらなければならない。
- 合計突合および照合。
  データ処理アプリケーション・プログラムの出力は、定期的にコントロール・トータルと突合をしなければならない。
- 出力エラーの取扱い。
  アプリケーション・プログラムの出力に含まれるエラーの報告および管理のための手続が確立されていなければならない。
- 出力伝票の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

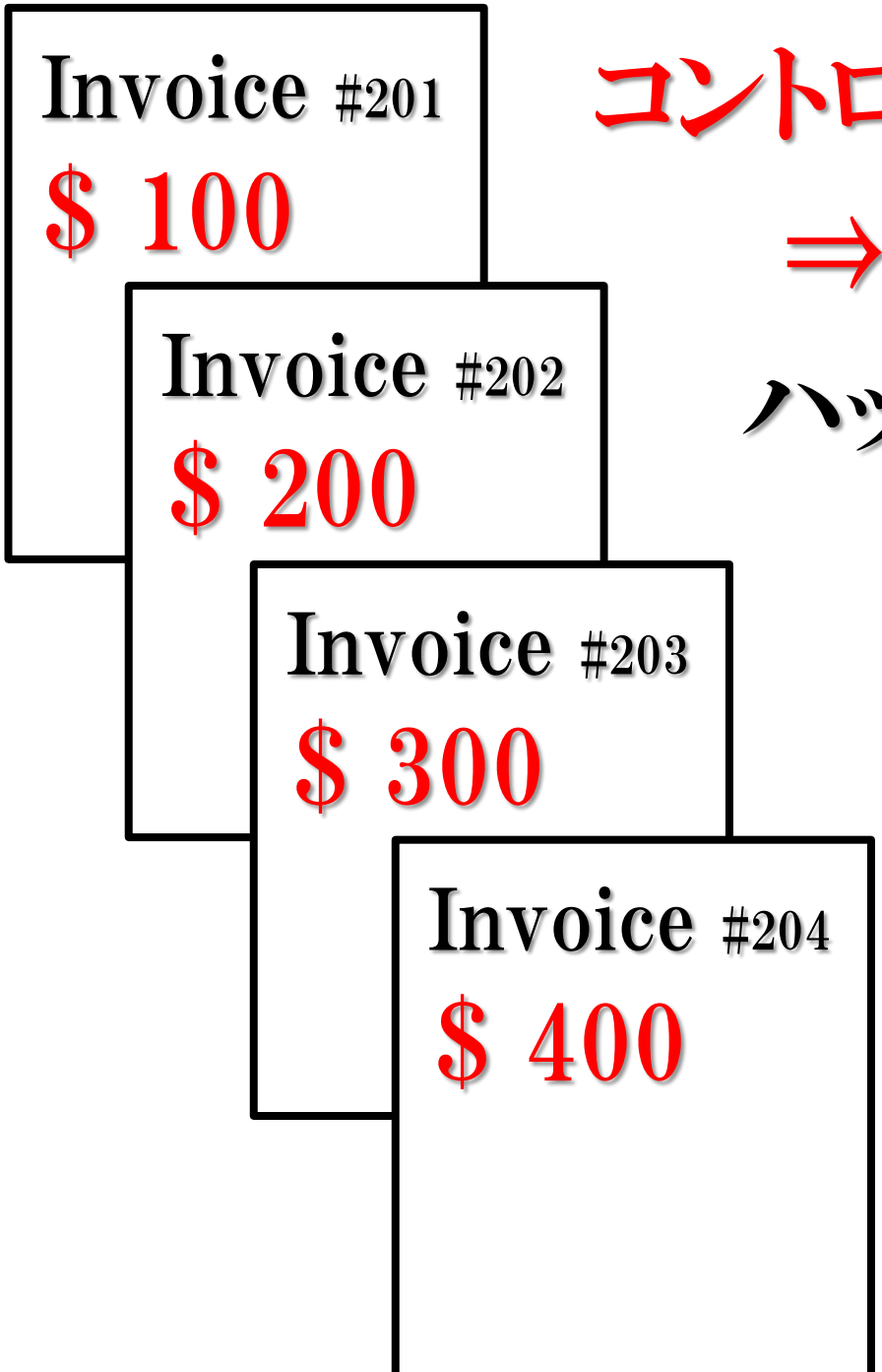
処理統制と出力統制の違い

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。

IT





コントロールトータル

⇒$1,000

ハッシュトータル

⇒810

レコードカウント

⇒4

参考図書

栢木先生のITパスポート教室

技術評論社

著:栢木　厚

IT学習の注意点

- 言葉や用語の意味をおさえる
- IT化されたことによるIC、内部監査に与える影響
- 監査の視点からのITリスクとIT統制

本日の論点

- ネットワーク
- ITリスクとIT統制

Chapter 8

◎ 4, 6,

△ 3, 5

Chapter 9

◎ 2, 4, 9, 10

Key Point

PC5台、プリンター2台、モバイル端末7台を保有する小企業が使うと思われるネットワークは？

A: LAN
B: MAN
C: PAN

Key Point

接続やルーターを管理する部門は？

A: ネットワーク管理部門
B: オペレーション部門
C: システム開発部門