企業における
内部統制の実践とIT

2007年1月18日

日本ヒューレット・パッカード株式会社
個人情報保護対策室　室長
チーフ・プライバシー・マネージャ
佐藤　慶浩

2007/1/18 版

講師略歴 (http://yosihiro.com/profile/)

佐藤　慶浩　（さとう よしひろ）
日本ヒューレット・パッカード株式会社　個人情報保護対策室　チーフ・プライバシー・マネージャ
併任
- 内閣官房 情報セキュリティセンター（www.bits.go.jp/） 内閣参事官補佐(2004/7/15～)
- 情報処理推進機構（www.ipa.go.jp/）セキュリティセンター　非常勤研究員(2000/12～)

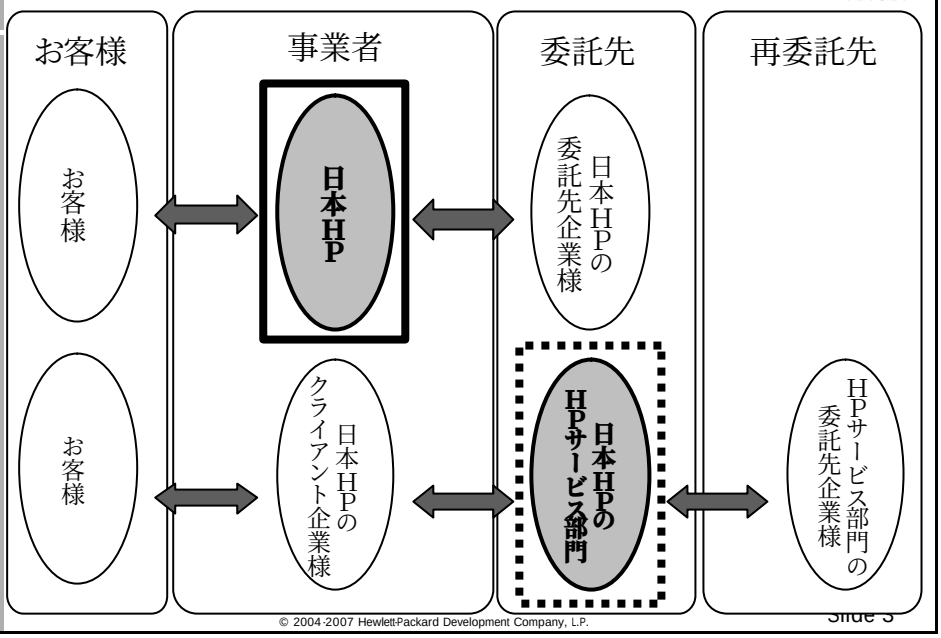
略歴
1990 年、日本ヒューレット・パッカード(株)入社。
2004 年6月、個人情報保護対策室長に着任。
2004 年11月、ヒューレット・パッカードのプライバシー・オフィスに所属し、日本のチーフ・プライバシー・マネージャとして全社施策の推進にあたる。

委員等
- 情報処理学会（www.ipsj.or.jp/） 正会員(1998～)
- NPO 日本ネットワークセキュリティ協会（www.jnsa.org/） 理事(2000/4～2004/5)
- 金融情報サービスセンター（www.fisc.or.jp/）セキュリティポリシー研究会 委員(2001～)
- ISO/IEC JTC1 国際標準セキュリティ委員会 委員(2001～)
- 杉並区住民基本台帳ネットワークシステム調査会議（www.city.suginami.tokyo.jp/）技術専門委員(2002/7～)
- 情報ネットワーク法学会（www.in-law.jp/）理事(2002/5～)
- 経済産業省　セキュリティホールに関する法律の諸外国調査委員会　委員(2003)
- 総務省　セキュアOSに関する調査研究会　構成員(2003/4～2004/3)
- 情報処理推進機構（www.ipa.go.jp/）情報システム等の脆弱性情報の取り扱いに関する研究会　委員(2003～)
- セキュアOSと基盤ソフトウエアに関する研究会（secure-os.yosihiro.com/） メンバー(2003～)
- 内閣官房 情報セキュリティ対策推進室 セキュアOS検討委員会 委員(2003～)
- NPO オープンソースデベロップメントラボ（www.osdl.jp/） Enterprise Linux for Public Sector ワークショップ メンバー(2004/2～)
- NPO デジタル・フォレンジック研究会(www.digitalforensic.jp/) 理事(2004/8～)
- 経済産業省 e-文書法 検討委員会委員(2004/11～)
- 経済産業省 個人情報保護ガイドラインQ＆A集検討会 委員(2005/4～)
- 日本情報処理開発協会 ISMS技術専門部会 委員(2006/5～)

Slide 2

2007/1/18 版

日本HPの 2つの立場



Slide 3

2007/1/18 版

Section 404 of the SOX -- Management Assessment of Internal Controls -- CEOs must establish and maintain "an adequate internal control structure and procedures for financial reporting." HP is required to report on its assessment of the effectiveness of internal controls and procedures for financial reporting as of the end of the reported year.

Slide 4

2007/1/18 版

企業における内部統制

①性悪説だけでは企業は成り立たない
②性善説を前提とした対策
③性悪説を想定した対策
④性悪者を減らし、性善者を増やす環境
⑤外部委託って、内部？？？
⑥許容リスクは減らしていける？？？

2007/1/18 版

企業における内部統制　①

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する

2007/1/18 版

企業における内部統制 ②

性善説を前提とした対策とは・・・

- 『しなければならないこと』と『してはならないこと』を明確にしていること。
- それを守るべき者に教育していること。
- それを守るべき者が理解していること。
- それを守るべき者が、遵守することに同意していること。
- 同意した者の状況を確認していること。

これが、すなわち、ガバナンスが構築された状態。

- コーポレート～，IT～，フィナンシャル～ ・・・

Slide 7

2007/1/18 版

性善説を前提とした対策・・・

情報は活用するためにある

情報セキュリティ偏重の過度の情報保護は禁物
情報活用が、企業における情報保持の目的
情報保護は、目的達成のための条件であり義務であるが、目的ではない
情報活用と情報保護のバランスをはかる情報セキュリティ施策とすべき

ビジネスに貢献しない施策は要注意

コンプライアンス施策をROIで考えてはいけない
IT施策におけるTCO削減は避けれない
ビジネスに貢献するような、IT施策でなければ実効性は高まらない
セキュリティ対策のひとつは単純化。単純化はコスト低減になるはず
逆にコスト低減になっていないということは、複雑化をもたらしている危険信号
ITの最適化計画の中でコンプライアンス施策を設計し、業務に組み込むべき

Slide 8

2007/1/18 版

性善説を前提とした対策・・・

守れるルールだけが、守られる。

必ず遵守できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的に企業の内部統制レベルを向上することができる。
できることの他に、できれば望ましいようなルールを混在させて、「ルールは必ずしも守らなくても良い」という意識を持たれることは好ましくない。
具体的な遵守方法が十分検討されていないようなルールを設けることは論外。
ビジネスの要求に即したバランスを保つ、事前合意されたルールを設けることが重要。

性善説を前提。性悪説も想定。

性善説を前提とする。その上で、性悪説についても想定する。ことが重要。
性善説であれば、「ルールは守られる」というところから検討し始めることができる。
性悪説への対策は、ルールを守っている性善説の人達によって実施する。しかない。

2007/1/18 版

企業における内部統制 ③

性悪説を想定した対策とは・・・

- 性善説を前提とした対策を実施している人達に担ってもらう。
- いかなる、規則や教育も、この領域では不毛となる。

2007/1/18 版

不正行為の類型

許可されていない者による不正行為（通称：外部犯）

- 無許可の行為　　悪意あり
  - 技術面：アクセス制御による防御・多重の防御

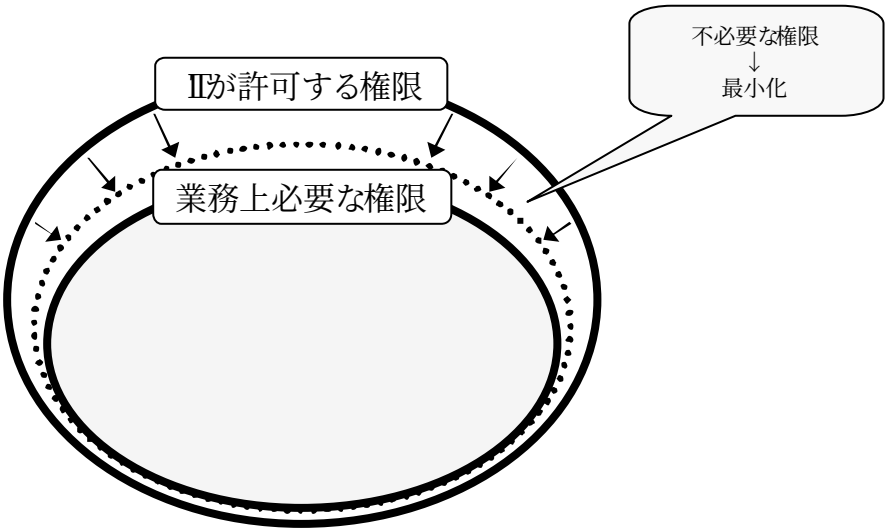
許可された者による不正行為（通称：内部犯）

- 誤操作・過失　　悪意なし
  - 誤操作を軽減する設計
  - 啓発、教育、訓練
- 権限の悪用　　悪意なし　悪意あり
  - 運用面：許可する権限の最少化
  - 技術面：監視による抑止効果
  - 技術面：アノマリ・アクセス（非通常行動）の検出

Slide 11

2007/1/18 版

権限の悪用 ・許可する権限の最小化



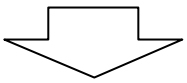
Slide 12

2007/1/18 版

企業における内部統制 ④

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する



性悪者を減らし、性善者を増やす環境

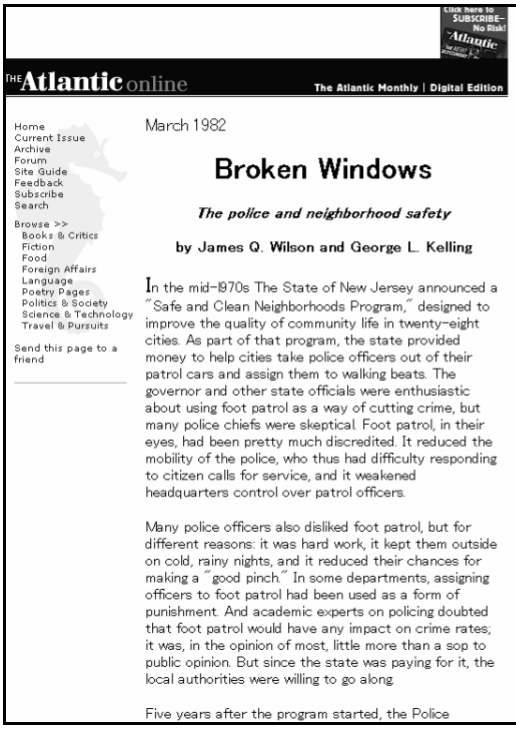
2007/1/18 版

性悪者を減らすための環境作り

ブロークン・ウインドウズ理論

Broken Windows Theory
March 1982, Atlantic Online

※一例であり、これを画一的に、あるいは一意に推奨するということではありません。



THE Atlantic online — The Atlantic Monthly | Digital Edition

Home
Current Issue
Archive
Forum
Site Guide
Feedback
Subscribe
Search

Browse >>
Books & Critics
Fiction
Food
Foreign Affairs
Language
Poetry Pages
Politics & Society
Science & Technology
Travel & Pursuits

Send this page to a friend

March 1982

Broken Windows

The police and neighborhood safety

by James Q. Wilson and George L. Kelling

In the mid-1970s The State of New Jersey announced a "Safe and Clean Neighborhoods Program," designed to improve the quality of community life in twenty-eight cities. As part of that program, the state provided money to help cities take police officers out of their patrol cars and assign them to walking beats. The governor and other state officials were enthusiastic about using foot patrol as a way of cutting crime, but many police chiefs were skeptical. Foot patrol, in their eyes, had been pretty much discredited. It reduced the mobility of the police, who thus had difficulty responding to citizen calls for service, and it weakened headquarters control over patrol officers.

Many police officers also disliked foot patrol, but for different reasons: it was hard work, it kept them outside on cold, rainy nights, and it reduced their chances for making a "good pinch." In some departments, assigning officers to foot patrol had been used as a form of punishment. And academic experts on policing doubted that foot patrol would have any impact on crime rates; it was, in the opinion of most, little more than a sop to public opinion. But since the state was paying for it, the local authorities were willing to go along.

Five years after the program started, the Police

凶悪犯罪を未然に防止することはできるか？

情報セキュリティの重大違反を防止することはできるか？

人が業務を遂行しており、人が違反する
→違反を低減させるにはどうすればよいかについても考える。

2007/1/18 版

ブロークン・ウインドウズ理論

第 1段階
　落書きが放置されていると罪悪感が薄れやすくなる
第 2段階
　軽犯罪が多発し治安が悪くなる
第 3段階
　警察の監視がないと判断され、より凶悪な犯罪者が寄り付く
第 4段階
　犯罪がエスカレートし凶悪犯罪が発生する
対策
(1)落書きを徹底的に消す
→警察や住民の監視があるというメッセージ
→軽い気持ちで罪を犯す人が減少する
(2)軽犯罪の取締りを強化する
→小さな犯罪も許さないという姿勢をアピール
→犯罪を起こそうと思う人間は近づかない
→凶悪犯罪は低減する

Slide 16

2007/1/18 版

企業における内部統制 ④

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する

↓

性悪者を減らし、性善者を増やす環境

↓

性善者が増えれば・・・

Slide 17

2007/1/18 版

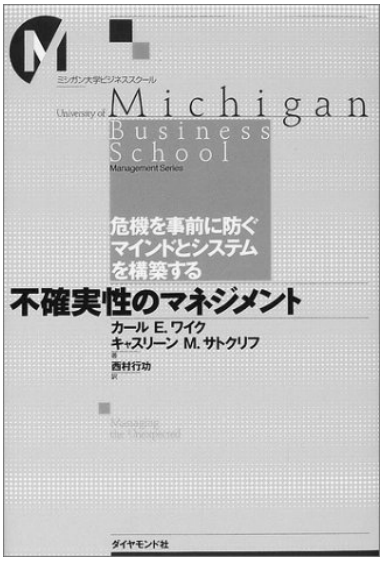
想定外事象への対応に関する

参考図書

Managing Unexpected

不確実性のマネジメント

出版 :ダイヤモンド社



Slide 18

2007/1/18 版

企業における内部統制 ⑤
外部委託先って、内部？？？

Slide 19

2007/1/18 版

委託関係において
あってはならないこと

委託関係において、発注者が安全管理措置を具体的に示さず、結果責任としての賠償責任だけをリスク転嫁することは、健全な社会を形成するとは思われない。

リスクの転嫁の連鎖だけが発生する
- 具体策がないまま見積もりをする
- 適正にするところは費用が高くなる
- 適当に対応するところは費用が安くなる
- 発注者としての具体策がないため、費用以外での評価ができない

リスクが潜在化するだけ
- 結果責任だけを押し付けると、自社の周囲に粗悪業者が蔓延し、事故が発生するその日まで、リスクが温存される危険性が高まる。

Slide 20

2007/1/18 版

委託関係において配慮すべきこと

委託発注者は、一次的な事業責任者である。

発注者は、自身の安全管理措置を具体的に定めて徹底する。
発注者は、安全管理措置を発注時に具体的に示す。
受注者は、指示された措置に必要な対策を具体的に設計し、必要な費用を見積もる。
双方が、対策に必要な運用体制を確立する。

2007/1/18 版

委託先への誤った管理

- 委託先にプライバシーマーク認証取得を指示する

→愚の骨頂

- 委託先にISMS認証取得を指示する

→誤解されやすい

事業者として、社外への丸投げ体質は許されない。

委託はリスク転嫁策のように思われるが、事故発生後のことを考えれば、それが正しくないことは、すぐにわかること。

さらに、自社内の現場での責任意識・危機管理意識の希薄化を招くため、むしろ、百害あって一利なし。

2007/1/18 版

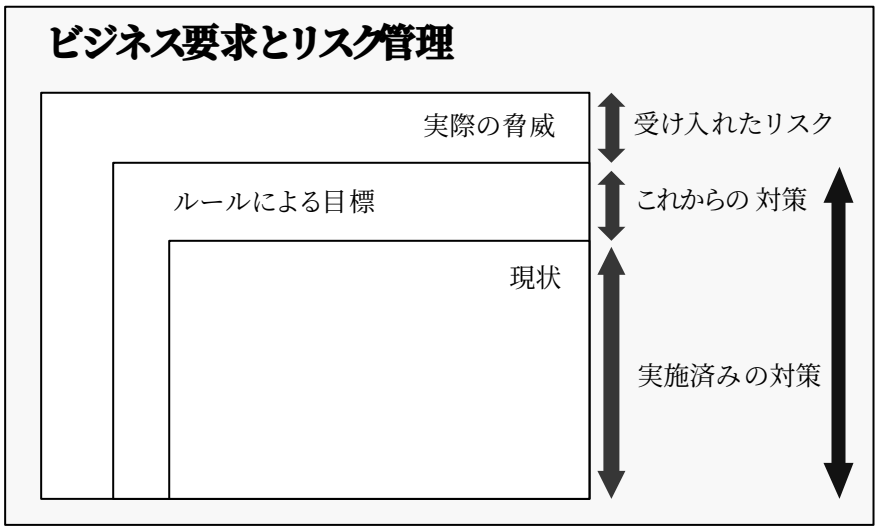
企業における内部統制 ⑥

許容リスクは減らしていける？？？

Slide 23

2007/1/18 版

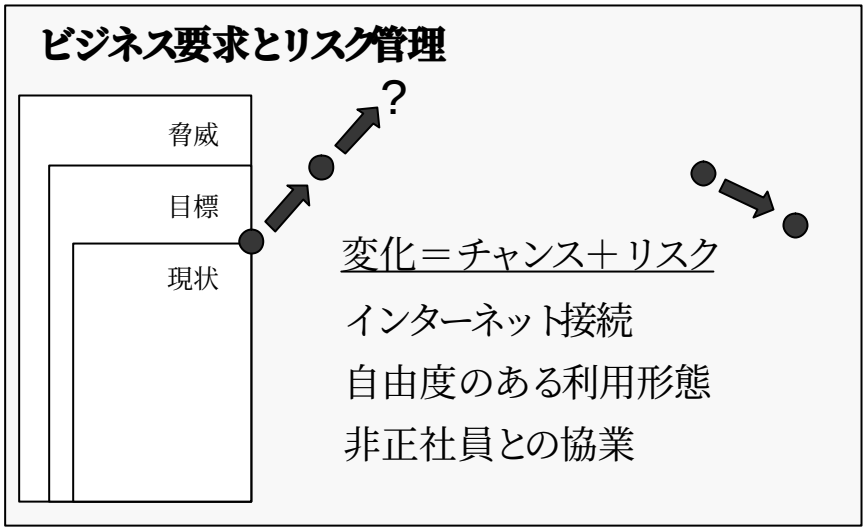
最低基準ではなく適正基準
「何ができるかより、何をしないか」



Slide 24

2007/1/18 版

最低基準ではなく適正基準
「何ができるかより、何をしないか」



Slide 25

2007/1/18 版

Section 409 -- Real Time Disclosure -- mandates that companies must disclose on a rapid and current basis "material changes in the financial condition or operations of the [company], in plain English, which may include trend and qualitative information."

Slide 26

2007/1/18 版

徹底する？？？

- 「徹底」という言葉は、その瞬間までを評価することにしか使えない
- 事故が起きるまでは「徹底」できており、事故が起きた瞬間に「徹底」できていなかったことになるだけ
- 対策の文脈において、「徹底」とはその時点の状態を表現するだけの言葉でしかない

- 「徹底する」という言葉には、何の期待も信頼も置けない

by 佐藤慶浩

2007/1/18 版

可視化（見えるようにすること）

- ちゃんとやっていても、やっていることをわかってもらえなければ、見てもらえなければ意味がない。
- 全数対策工数は、サンプリング対策工数より多い。少ない工数を選ぶのは得策か？
- 最低限のサンプリング基準を達成することは、ビジネスに貢献するのか？

- すべてを可視化できることは、ビジネスに貢献する。
  - Customer chain, Supply chain, Financial chain
- 企業規模による処理の多少はITの限界に達していない。
  - 10人なら処理できて、10万人なら処理できない？？？

2007/1/18 版

アダプティブ・エンタープライズの実現方法 ～4つの設計指針～

シンプル化
- 要素数の削減
- カスタマイズの低減
- 変更の自動化

+

標準化
- 標準技術と標準インタフェースの採用
- 共通アーキテクチャの適用
- 標準プロセスの導入

+

モジュール化
- 単純構造に分割
- 再利用可能な構成要素を作成
- 論理的なアーキテクチャの導入

+

統合化
- ビジネスとITの連携
- 企業内外でのアプリケーションとビジネスプロセスの結合

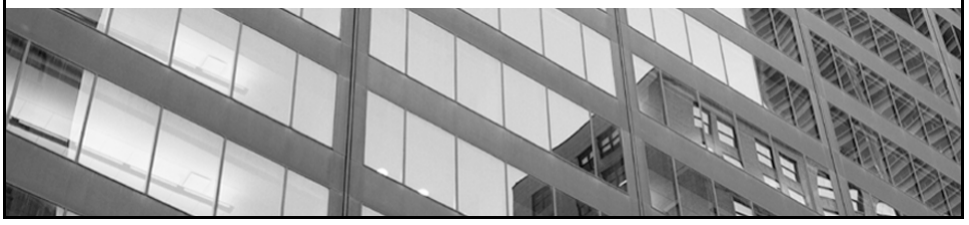
一貫した適用:
- ビジネスプロセス
- 情報
- アプリケーション
- インフラストラクチャ

Slide 29

参考資料

http://yosihiro.com/business

http://yosihiro.com/go/blog



2007/1/18 版

http://yosihiro.com/go/blog

Slide 31

2007/1/18 版

内閣官房情報セキュリティセンター
政府機関情報セキュリティ統一基準

http://www.nisc.go.jp/active/general/kijun01.html

- **政府機関の情報セキュリティ対策のための統一基準（2005年12月版［全体版初版］）解説書**

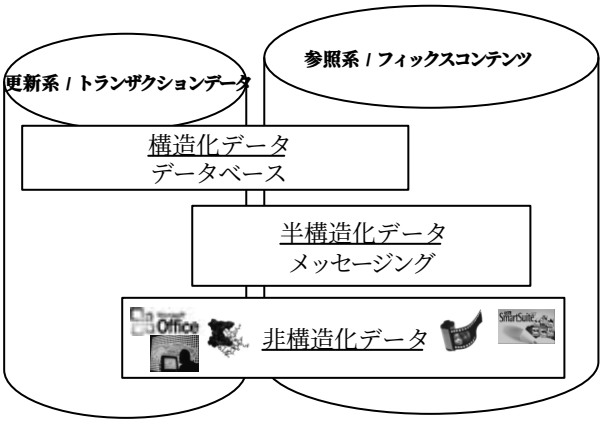
Slide 32

2007/1/18 版

データ特性の考察

2007/1/18 版

データの構造化度合いとデータ増加傾向



データ量がますます増加するのは、管理が複雑なデータタイプ。

活用によってビジネス加速にもつながるデータ。

現在	企業情報の15%	企業情報の85%
今後	年に61%で増加	年に92%で増加

2007/1/18 版

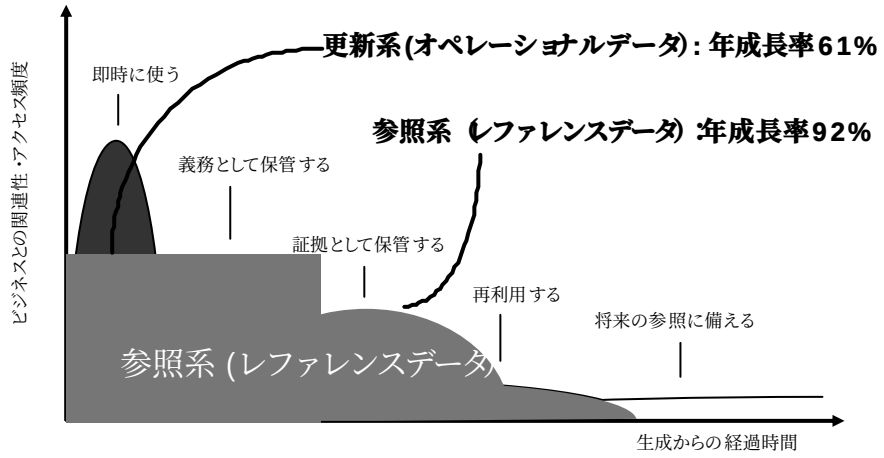
データの構造化度合いと特徴

	構造化データ	半構造化データ	非構造化データ
呼称	オペレーショナルデータ トランザクションデータ	フィックスコンテンツ レファレンスデータ	
環境	DB, DWH, EDI環境	メッセージング環境	WEB, ファイルサーバ環境
データ	Oracle、SQLServer、DB2 等のRDBで管理されているデータ	E-Mail/インスタントメッセージの本文、メールアドレス、件名	オフィス文書、音声・画像イメージビデオ、HTML等のファイル
管理の単位	データは、テーブル単位、テーブルの中のデータも、カラム数や、項目、数値か文字等で管理。管理しやすい。	本文・アドレス・件名単位データ間の関連性、返信/転送などの関係を踏まえて、データを選別しながら管理することが難しい。	ファイル単位の管理
一般的な管理状況	時間経過に応じてバックアップ、アーカイブ、世代管理	個人管理に依存したQuota 管理/データ管理	Webサイト/プログラムファイル等は、ネーミングルール、更新管理、バックアップ管理等 Office文書は、企業によって管理レベルがまちまち、バックアップ・容量管理 等

Slide 35

2007/1/18 版

データの活用目的と活用頻度の変化



Source: Jan Möller, Ministry of Transport, NL

Slide 36