平成18年3月修了
博士(学術)

個の情報管理による企業価値評価モデル

A Proposal of New Enterprise Valuation Model Based on Personal Information Management

高知工科大学大学院　工学研究科　基盤工学専攻

学籍番号　1056022

中川　喜博

Yoshihiro　Nakagawa

平成18年3月修了
博士(学術)学位論文

個の情報管理による企業価値評価モデル

A Proposal of New Enterprise Valuation Model Based on Personal Information Management

平成17年12月1日

高知工科大学大学院　工学研究科　基盤工学専攻

学籍番号　1056022

中川　喜博

Yoshihiro Nakagawa

～ 目　次 ～

第1章　序論

第2章　個人情報管理システムの構築

第3章　個人情報管理を基本とした新しい経営モデル（PRM）の提唱

第4章　PRMモデルの実践と検証

第5章　結論

はじめに

企業は人材という人“個”で成り立つ．病院は，患者単位の“個”のプロジェクトで成り立つ．しかし，現時点では“個”から構築する経営理論及び“個”の情報管理システムが存在しない．

筆者は本論文で正確なこの課題を解決すべく研究し，新たな“個”を主眼においた経営理論を論じた．また，解決に至る過程においてプライバシー工学（※）と命名し初めて定義する“個”の認証理論を導いた．更に，ビジネス実証の検証として起業工学の創造による理論化，並びに具現化を行った．

筆者は，企業価値を算出する為基幹システムにおいて“個”の証明で使用する電子署名の公開鍵認証基盤（PKI：Public Key Infrastructure）は，より高度なセキュリティーを必要とするシステムには不適であると判断した．これは，インターネットと端末間の送受信内容を保障するPKIには，本人の真正証明不全の技術的な問題（1）が存在する． このPKIの脆弱性を克服するバイオメトリクスがあるが，この認証技術で利用する個人認証の生体識別認証データー自体が，究極のプライバシー情報の個人情報である．筆者はこのPKIの問題を解決する為，従来には存在しない15の機能の必然性を明らかにした．それは，本人識別情

※プライバシー工学：2000年特許出願，2005年5月オフィスオートメーション学会で概念を発表．
学会レフリーより“Privacy Engineering”の言葉自体は定義も利用もされていないが，一部米国で情報登録時における意の文献がある．との指摘を頂いた．しかし筆者が提唱するのは，プライバシー情報の制御を意図する．

（1）地方公共団体による公的個人認証サービス制度の創設について，「地方公共団体による公的個人認証サービスのあり方検討委員会」報告書，本人が電子署名を行ったと推定，総務省自治行政局自治政策課，14年2月28日，42P－43P，http://www.soumu.go.jp/s-news/2002/pdf/020228_3a.pdf

報である個人情報を集中管理する情報センター(IDC:インターネット Data Center)を活用する事で, 自己の重要情報を自己コントロールするシステムである. すなわち, 認証するデーターの真正性を保持しつつ, 匿名性を維持し認証強度により段階的な開示を可とするデーター技術を筆者が全く新たな着想と構想について, プライバシー工学の研究をまとめたものである.

そして, このIDCビジネスのアプリケーション技術の核になる経営管理は, 戦略情報システム・経営分析システム・統合業務パッケージなど, 戦略的活用により, 経営環境及び仕事のスタイルに変革をもたらした. しかし筆者は, 経営分析手法自体は, 旧態依然のままであり財務会計中心の域を出ていない. そこで, 最先端の情報技術を駆使する事を前提とする, 次世代の多視点による経営評価と価値評価理論事確立と実現する技法を, 筆者が世界に先駆けて考案した. それは, 新たな計数理論を数値化と可視化する技術であり, 変化の流量を人工知能による評価, 更にシュミュレーションの先行計数予測で明確化する, そして技術と評価経営手法の進化を可能とさせる統合連携システムである. この科学的に捉えた, 相関分析法(多視点相関の時間軸を含む四次元ベクトルで企業・事業の価値と評価を可能にする技術のPRM(パーソナル・リソース・マネージメント)の研究をまとめた.

最後に, これらの技術を具現化できる新規事業のビジネス展開として, 一生涯の個人情報を集中管理する銀行機能を備えた電子医療カルテの情報統合管理センターを考察した. 本稿は, ユビキタスと広域災害にも対応可能とする, 新たな高信頼情報管理と新たな認証ビジネスの創出を, 筆者が全く新たな着想と構想の研究をまとめたものである.

筆 者

内 容 梗 概

本論文は，筆者が富士通株式会社通信研究部門などにおいて，情報通信プロトコルの設計と情報セキュリティーに関して行った研究，人工知能の知識データーベース構築に関して行った研究，ナレッジマネジメントの研究，プロジェクトマネージメントの研究を基にしたものである．更に，高知工科大学にと米国スタンフォード大学において，起業工学に基づく企業経営とインターネット上の情報保護について，国際的な視野と標準化を踏まえた理論の確立と，ビジネスへの実務展開に基づく工学的研究をまとめとした．

更に，2000年には本研究の具現化に向けて，世界最先端電子カルテを導入予定とする高知県医療情報センターと，医療IDC（医療情報銀行）の構想を議論した．更には，2003年7月2日，日本政府のIT戦略本部によって，e-Japan戦略Ⅱの先導的な取り組み7分野の内の，医療分野（認証基盤整備，電子カルテのネットワーク転送・外部保存の容認）と全く同じ構想である．それは，本人識別情報である個人情報を集中管事する情報センター（IDC:Iインターネット Data Center）を活用する事で，自己の重要情報を自己コントロールするシステムである．

これは，認証するデーターの真正性を保持しつつ，匿名性を維持し認証強度により段階的な開示を可能にした．この技術を新規事業の展開として，一生涯の個人情報を集中管理する銀行機能を備えた電子医療カルテの情報統合管理センターを考察した．本稿は，ユビキタスと広域災害にも対応可能とする，新たな高信頼情報管理と新たな認証ビジネスの創出を検討する．

また，病院経営の切り口で考察した時，患者毎の“個”のプロジェクトをナレッジマネジメントによる知識共有に対して，知的生産性の向上と知的触発の拡大を図る為オープン・ネットワークであるインターネットを活毎したグループウェアの研究を進めている．その一環として，インターネットによる業務システムの適用について分析を進めてきた．その結果，従来のIDCは，e

ーコマースや業務アプリケーションに限らずオープン・ネットワークが必要とする新たな経営理論に基づく経営支援システムと不特定アクセスによる利用者の特定や，分散ネットワークの性質による集中システム運用への適用条件が欠落している事などが明らかになった．更に，従来の経営理論に基づく大雑把な把握やインターネットの長所のみで構築したシステムは実用性が無く，金融ビジネスなどの確実性を要求するシステムには適用できない．本論文では，このシステム欠損を解明すると共に，IDCによって課題解決のキーとする研究により，次世代コンピュータネットワークの基本設計による経営理論と情報基盤の確立の結果により，具体的な適用計画を目的とする．

この医療IDCの実現化の最重要のキーポイントは，本人の認証と個人情報を集中管理する認証を必須の装備事する事にある．そして，この各個人毎に自己情報毎自己コントロールを可能にするプライバシー技術を確立させた．医療の他に行政IDC／金融IDCなど，計り知れない多くの新たな事業が派生する可能性を示唆する．

本論文は，5章に分けて構成するが，以下各章毎に順を追ってその内容の梗概を述べる．

第1章　序論

1．1　緒言

研究の背景と狙いに，旧来より主流である情報システムについて述べる．本章では，インターネット接続によるコンピュータシステムについて“個人”の視点から観察した．

1．2　背景

その情報ネットワークの変化によって，経営管理システムや業務の連携システムが，情報ナレッジマネジメントへと進み企業が保有する知的資産価値の企業価値基準の見方と評価方式に変化が見る考察を述べる．

1．3　マーケティングの考察

利用形態が従来の代理店販売などからe－businessや直接購買に見る様に，企業専用から顧客直接へと変化の傾向の考察を述べる．

1．4　これまでの研究の概況

インターネット利用問題の正確な状況把握と，不特定多数を前提にした個人情報保護のオープン･ネットワーク上の統合システム化に関して，本研究の目的と意義を明らかにさせた．

1．5　本研究の目的と意義

IDCで利用するＡＳＰについて，ホスティングサービス財務会計からのバランスシートなどや，キャッシュフローだけの会計主義による経営分析システムの問題について正確な把握を行った．また，戦略情報システムに関しても最近の状況について概説し，本研究の目的と意義を明らかにさせた．

第2章　個人情報管理システムの構築

2．1，個人情報保護の社会的ニーズ

情報保護のキーとなる本人認証が，現在の技術では実用的とする公開鍵方式と，電子署名の認証の欠点による運用未着手の理論的な問題調査を行い，工学的に情報の流れと認証方法を研究し問題を明らかにした．

2．2，個人情報認証構想の提案

前節の調査研究より，筆者が地球的規模の情報ネットワークの基礎基盤に向けて，ビジネスモデルとして基本特許を権利化した，全く新たな発想と構想による情報セキュリティーの確立理論を提案した．

2．3，個人情報認証の技術設計と基本運用設計仕様

前節の個人情報認証(IICA)の構想実現の為工学的な運用技術について実際の運用システム基本設計水準まで研究して, 技術仕様書として具現化への検証を行った.

第3章　個人情報管理を基本とした新しい経営モデル(PRM)の提唱

3.1 統合データーベースのコンテンツ

本章では旧来主流であった, 財務会計からのバランスシートとキャッシュフローだけの会計主義による経営分析システムの問題について, 正確な把握と戦略情報システムに関しても最近の状況について概説し, 本研究の目的と意義を明らかにさせた. 企業価値分析が可能とする資産収益性や投資収益性などの経営計数に基づく経営に役立てる理論的な問題調査を行い, 工学的に情報の分析方法を研究し問題を明らかにした.

3.2 次世代の経営評価理論(新構想)

本章では第1章と第2章の調査研究より, 効率性の高い事業体に変革する為起業家アプローチ導入の必要性と, 全く新たな発想と構想による経営分析の確立理論を考案した.

3.3 M&Aの次世代評価手法(新手法)

評価毎位の機能別(IP)及び分析のPRM連携機能を, 顧客が選択した機能毎に企業価値評価を構築してIDCとして提供する方法と装置

3.4 次世代の経営システム

構想と理論を具体化する為企業の現在の正当な価値を評価する必要性と, 今後の将来性に関する価値基準を戦略的な観点から評価させる技術の確立と企業の価値評価を, コンピュータシステムで企業の経営資源全体を統合した視点で行う

事より解決する相関モデルについて考察した.

3．5　結論

前節で確立した評価理論を経営分析のツールとして, 一般的な企業と事業体への国際的な範囲で適応が可能な全く新しい工学的手法に関する経営システムを述べた. また, 中期及び長期事業計画に関して, 望ましい企業と事業体の望ましい具体的な実現に向けて技術的に確立を前提とする為, 進化を前提にするイノベーションを可能にするPRMシステムの実現について述べた.

第4章　PRMモデルの実践と検証

4．1　緒言

結論ナレッジマネジメントによる知識共有を, 知的生産性の向上と知的触発の拡大を図るグループウェアの研究より, インターネットによる業務システムの適用について実験と分析を進めた結果, 従来のIDC(インターネット Data Center)は, e－コマースや業務アプリケーションに限らずオープン・ネットワークが必要とする不特定アクセスによる利用者の特定や, 分散ネットワークの性質による集中システム運用への適用条件が欠落している事などを明らかにした.

4．2　ビジネスへの適応

2章の技術と本章の解決法を特許明細として特許として権利化した. この権利を資本提供を行い起業を行った. 事業内容として次世代のICカード認証基盤についての取り組みについて述べた.

4．3　医療IDCへの応用

本人識別情報である個人情報を集中管理する情報センター(IDC:インターネット Data Center)を活用する, 自己の重要情報を自己コントロールするシステムの実

施例を考察した. 認証するデーターの真正性を保持しつつ, 匿名性を維持し認証強度により段階的な開示の可能技術を新規事業の展開として, 一生涯の個人情報を集中管理する銀行機能を備えた電子医療カルテの情報統合管理センターを考察した. ユビキタスと広域災害にも対応可能とする新たな高信頼情報管理と新たな認証ビジネスの創出について述べた.

4. 4 コンテンツ配信への応用

“個”へのデジタルコンテンツの配信を行う際のプライバシー制御と本人確認を行うビジネスを考察した. 更に配信確定時の著作権管理システムについて述べた.

第5章　結論

システムの利用者が, パッケージやシステムの固定仕様通りの操作と内容からの脱却手法として, 個人情報認証局(PICA)と個別経営管理システム(ERM)が価値あるものである評価について述べた. また, 実用化についての考察より, ビジネスとしての価値と方向性についても評価した.

第1章　序論

1．1　緒言

企業価値を高める為，企業の社員“個”が様々な業務経験で得た専門知識やノウハウを，会社全体で一元管理し，社員同士の情報交換の為ネットワークを構築及び，専門知識や重要情報の共有化を図り，会社組織の中の情報流通を密にして企業の競争力を高める経営手法について研究した．その結果，個人や部門に偏在する知的資産を電子文書にし，社員や協力会社，専門家等との連携の中で問題解決及び，商品開発等に共同で取り組むチームによる新しい仕組みが必要と考え，企業を構成する“個”を本研究による独自の理論による評価の積み上げにより，精度の高い価値分析が可能になる事を明らかにした．

この企業価値評価の経営理論はインターネットの利用を前提にしている．それは，多数の人が時間的あるいは地理的な制約が無く，大量かつ様々な形態の情報を入手し発信する事が可能である．

しかし，この理論を完成する前に極めて重要な問題を解決しなければならない．その問題とは，インターネット社会特有の“個”の証明と保護の問題が生じ，その影響が非常に早く広範囲に及ぶ特徴によるものである．現実に一般の消費者が電子取引により，その消費者個人の購買行動等の個人情報が電子データーとして蓄積する事による漏洩，改竄，悪用などの事件は既に多発している．その結果，ネットワーク上で授受する個人や企業の重要データーへのセキュリティー対策が極めて重要な課題となる．非対面であっても，より確実に本人を認証する指紋，顔，声紋やサイン，バイオメトリクス認証などと組み合わせた，個人情報データーの集中管理と保護と認証を行う統合化したネットワークシステムの利用のみがIT社会の実現を果たし，それ以外は分散管理の問題の為に実現が不可能と考える．これらの企業情

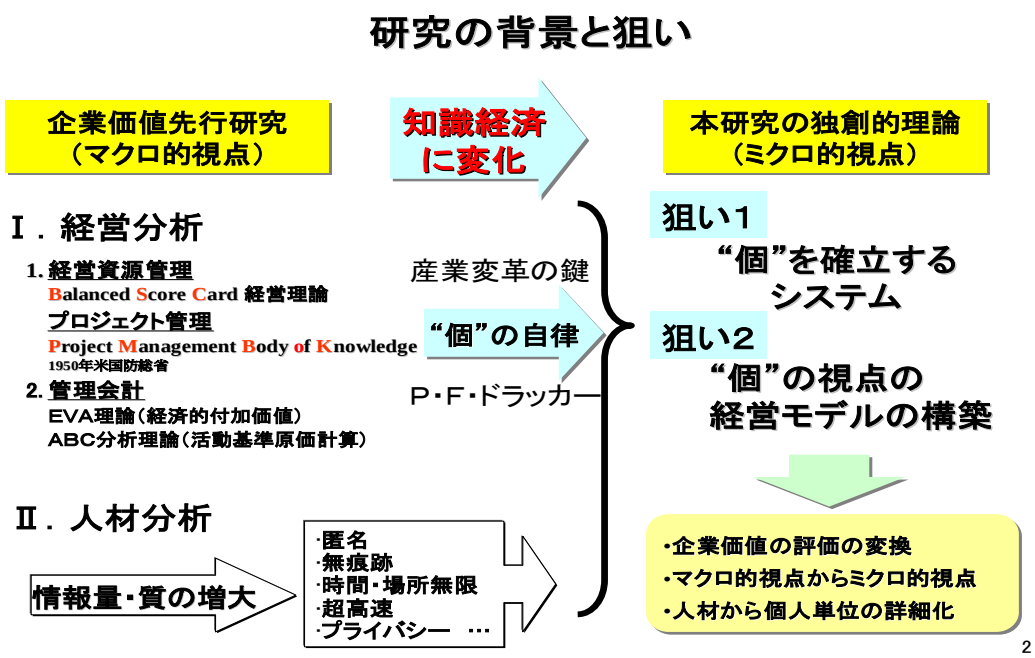
報としての“個”のデーター管理の問題に対処する為は，インターネット上の個人情報保護を，本理論を具現化するシステムとして第一の研究とした．

第二の研究として，前述の技術を基盤とした経営の情報工学的なシステム理論を論じる．従来の分析単位の集計中心によるアナログ理論では，企業評価システムとして完成できない課題に取り組んだ．経営に関する統合プラットホームとするため，全く新たな理論を必要とした．経営資源の相関関係の知識に対する人工知能的な推論によって，どこまで推察ができるかなどの神業的な経験知識を構築し，デシジョンマネジメント支援を行う．また，これらは単に一般企業だけが対象では無い．例えば，地方自治体の行財政改革を推進する手法として，活動基準で細分化した行政サービスの効果と，評価を明らかにする事が可能になる．これにより，行財政運営の効率化と再構築（リエンジニアリング）を実現するための判断基準として，評価システムとして活用できる理論を導いた．

1．2 背景

“個”の確立した経営理論の展開やシステムを定義するのは極めて困難である．

一般企業，公益団体の事業や企業価値評価は，情報技術革新に伴う戦略的事業経営判断と管理技法において，戦略情報システム・経営分析システム・統合業務パッケージなどの活用により，経営手法や環境及び仕事のスタイルに変革をもたらした．しかし，経営分析の手法自体は旧態依然のままであり，財務会計が中心の域を出ていない．また，事業主や株主が，新規事業・ベンチャー・研究開発投資・Ｍ＆Ａなどの，不確実性が高いビジネスプランなどに対し，戦略的経営判断と投資を可能にする事業価値評価の理論の確立は必須であると考えた．



筆者の理論は，第一の研究としたインターネット上での“個”の確立が基盤となる．

一般には，ネットワークの不正アクセスなどの防止手段においては，ICカードやPKI（公開鍵）認証での導入を検討している．しかし，これらは使用推定者の予測と端末を判別する＜本人見なし認証と端末認証＞であり従来，企業内でのみで利用が限定したネットワークを前提とした考案と開発したシステムの流用にほかならない．国際的にも，国の公的機関を対象とした個人情報保護法を制定しているなどの動きはあるものの，これら工学的な検証は一切成していない．

『個人情報』とは，通産省，日本工業規格が定めたJIS Q 15001(2)の定義によると，個人に関する，住所，氏名，年齢，生年月日，性別，電話番号，会員ID，Eメールアドレス，銀行口座番号，クレジットカード番号，各種アンケート回答等の情報であって，情報に含む氏名，生年月日その他の記述又は個人別に付した番号，記号その他の符号若しくは音声，

---

(2) JISQ15001 個人情報保護に関するコンプライアンス・プログラムの要求事項 Requirements for compliance program on personal information protection http://www.jisc.go.jp/app/pager?id=26738

画像により個人を識別できるものである．（ある情報のみでは特定の個人を識別できないが，他の情報と容易に照合でき，それにより個人を識別できる当該情報を含む）としている．いわゆる「個人識別情報」であり，インターネット利用者のWeb Browserが発信する環境変数の内容が個人を特定するものであれば個人情報とするなど．（IPアドレス，Browserとバージョン，直前のWebサイト履歴）特にJIS Q15001では，機微の個人情報として下記の情報収集自体をも禁止している．

1） 人種，民族，身体・精神障害，犯罪歴その他社会的差別の原因となる事項

2） 門地及び本籍地（所在都道府県に関する情報を除く）

3） 信教（宗教，思想及び信条），政治的見解及び労働組合への加盟

4） 保健医療及び性生活

5） デモへの参加その他の政治的権利行使に関する事項

また，一般に12歳～15歳までの年齢以下を対象に子供と定義し，個人情報の収集に際して保護者の同意を得るべきとしている．

これらの“個”の確立において「個人識別情報」は，その取扱いについて基本的な原則を確認する事ができるとしても具体的に取り決める事は困難である．インターネットの普及に伴い，様々な個人情報がネットワークを介して収集と利用を行っている．

(1) 個人情報の売買

個人情報を商品として取引し利用している．個人の氏名・住所・電話番号等などの個人を識別する情報は，インターネットで検索可能な個人の照会サービスを利用する事により，ネットワーク上で直接検索又は入手できる．

(2) 公共

電気・電話・水道・ガス・プロバイダなど，様々な公益設備の公益設備の利用に対して個人情報を提供する必要がある．住民基本台帳と同等に収集・蓄積・管理する個

人情報は膨大である. 公共的設備提供機関から深刻な漏洩事故が発生している.

(3) 信用情報機関

会社役員･個人など所得収入について, 消費者調査を行っている消費者調査機関がマーケッティングで活用する. インターネットでクレジットカードを利用すると,「消費者情報」も収集する.

(4) 金融

キャッシュ･クレジットカード番号は, 個人の信用情報が付帯して決済する. インターネット･バンギング等が存在する. それらのサービスの利用には, 取引関連の情報に詳細な個人情報を授受する. また, ネット上で様々なインターネット･ショッピング(電子商取引)の決済手段としてクレジットカードを利用してネットワーク上で授受している.

(5) 社会保障番号

米国では, 一般的な個人の本人確認の有効な認証･識別手段である. そのため社会保障関連情報がネットワーク上で流通している.

(6) 社内

従業員の個人情報もネットワークを介して授受している. リクルート･退社ネットワーク勤怠･給与･人事考課･利用状況･電子メールの内容等の監視が行われている.

1) 電子政府(E－Government)

電子政府実現の電子化の推進においては, 行政のインターネット化のレベルが企業の国際競争力, 国力, 個人の生活に密接に影響をおよぼす. しかし筆者は, インターネット等のオープン･ネットワークを通じてのオンライン申請等を前提としたシステム構築になっていないと考える. つまり, 情報としての大半が電子データーをフロッピーディスク等の保存媒体に記

録した形で提出する形でのフロッピー申請を認めるものが前提である.(3)

各国の行政機関が持つ住民基本台帳の“個”の情報の基礎的名前, 住所, 性別, 生年月日)情報は, 最新で極めて正確である. よって, マーケッティングの与信に活用する民間企業にとって非常に有益な情報である. これらの情報は, 国の行政機関において個人情報保護法により個人情報を保護しているが, 実際にプライバシー侵害が発生している. 行政サービスにおける行政のインターネット化は, 従来の紙ベースの行政とのインターフェイスを電子化, データーベース化, インターネット化する. ビジネスプロセスの革新, 新しい価値の創造を当然伴うものと考えるべきである.

行政サービスの電子化については『公開鍵方式による電子認証』の利用可否が現在の最大の課題であると考える. この電子政府の基本は行政手続のインターネット化で,

1. 電子申請･届出
2. 電子調達
3. 情報公開

を行うものである. 従来, これらの手続の大多数は役所の窓口で, フェイス･ツー･フェイスで紙を介して行われてきた. そして, 役所の窓口では, 申請等を行う人の本人確認が重要な位置を占めていた.

しかし筆者は, インターネットを介し, これらの“個”の確立手続を行う電子政府においては, 本人確認が非常に重要な要素となっており, 電子認証が電子政府構築への最重要課題と考える. 世界に先立つ最先端の技術として, 個人情報保護と電子認証を統合する制度と共に, 情報処理などの管理保全などの安全対策を考慮した『個人情報認証』が必須となるに伴い, オープン化に向けてセキュリティー手順の公開と機能の標準化を行う必要がある為である.

個人情報の管理強化への危惧より, 国民総背番号制への嫌悪感が非常に根強いが, 住

---

(3)『行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律』昭和63年12月16日法律第95号平成元年10月1日施行
www. isc. meiji. ac. jp／～sumwel__h／doc／codeJ／pubdata. htm

民基本台帳法の改正で，住民票コードが利用できる様になった．しかし筆者は，統一的なコードとしての使用は，慎重な取扱いが必要な為状の法令及びシステムでは困難である．氏名，住所，性別，生年月日の基本情報から個人を容易に識別し特定する事が可能である為ある．

インターネットを利用した電子商取引が急速に普及しつつあるが，オープン・ネットワークを利用した取引環境においては，セキュリティーの確保が重要となり，送信するデーターの秘匿問題の他，第三者による情報の改竄を防止し，通信相手を確認する方策が，安全な取引を行う上で重要な課題となっている

当事者が対面して書面により行う従来の“個”の確立とは異なり，デジタル情報により作成するデーターは，第三者により改竄がしてもその痕跡が残らない．また，不特定多数者間の非対面で行われる取引においては，第三者が不正に本人に成り済ました場合でも相手方を確認する有効な方法が無く，取引自体を後になって否認するおそれもある為新たな対応策が必要になる．

1．3 マーケティングの考察

現在のビジネスは，“個”が確立する顧客のあらゆる情報を収集し，マーケティングに活用するのは，経営戦略の常套手段である．その顧客の情報を効率的に収集，管理，共有し，マーケティングに活用する仕組みがCRM（Customer Relationship Management）である．しかし現在は，実際の店舗だけでなくインターネット上のオンライン取引など，顧客との接点の場が増えている．また，顧客のニーズ多様化により効率的に顧客の“個”の情報を収集し，管理する仕組みが重要となるが，数多くの個人情報を取り扱う為，“個”の情報保護の問題が発生すると考える．

カードを発行する銀行機関やカード会社には，クレジットカード詐欺の件数増加を防止する為，インターネット上の“個”の信用分析・価値評価システムや“個”の証明する仕組みが必

要と考える.

1) OECD8原則(4)

1980年9月23日に我が国など29カ国が加盟する経済協力開発機構(OECD)が『プライバシー保護と個人データーの国際流通についてのガイドラインに関する理事会勧告』(OECD8原則)を採択している. この中ではOECDの8原則の下, 各国で制定している個人情報保護法などのグローバルスタンダードに沿った管理方法でなければならないとしている.

収集制限の原則(適法・公正な手段によりかつ児童生徒(保護者)に通知又は同意を得て収集)

個人データーの収集には, 制限を設けるべきであり, いかなる個人データーも, 適法かつ公正な手段により, かつ適当な場合には, データー主体に知ら占め又は同意を得た上で, 収集するべきである.

データー内容の原則(データーは利用目的に沿ったもので, かつ正確, 完全, 最新であるべき)

個人データーは, その利用目的に沿ったものであるべきであり, かつ利用目的に必要な範囲内で正確, 完全であり最新なものに保たれなければならない.

目的明確化の原則(収集目的の明確化及びデーター利用と収集目的の両立)

個人データーの収集目的は, 収集時よりも遅く無い時点において明確化しなければならず, その後のデーターの利用は, 当該収集目的の達成又は当該収集目的に矛盾しないで, かつ, 目的の変更毎に明確化した他の目的の達成に限定するべきである.

---

(4)『OECD RECOMMENDATION CONCERNING AND GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA O. E. C. D. Document C(80)58(Final), October 1, 1980』
www. cpsr. org／cpsr／privacy／privacy__international／international__laws／1980__oecd__privacy__guidelines. txt

利用制限の原則（目的外利用の禁止）

個人データーは,『目的明確化の原則』により明確化した目的以外の目的の為, 開示利用その他の使用に供するべきでは無いが, 次の場合はこの限りでは無い.

(a) データー主体の同意がある場合, 又は,

(b) 法律の規定による場合

安全保護の原則（合理的安全保護措置による紛失･破壊･使用･修正･開示等からの保護）

個人データーは, その紛失若しくは不当なアクセス･破壊･使用･修正･開示等の危険に対し, 合理的な安全保護措置により保護しなければならない.

公開の原則（データー収集の実施, 方針等の公開並びにデーターの存在, 利用目的, 管理者等の明示）

個人データーに係る開発, 運用及び政策については, 一般的な公開の政策が取無ければならない.

個人データーの存在, 性質及びその主要な利用目的と共に, データー管理者の識別, 通常の住所をはっきりさせる為手段が容易に利用できなければならない.

個人参加の原則（自己に関するデーターの所在確認及び異議申立ての保証）

個人は次の権利を有する.

(a) データー管理者が自己に関するデーターを有しているか否かについて, データー管理者又はその他の者から確認を得る事.

(b) 自己に関するデーターを,

- 合理的な期間内に,
- もし必要なら, 過度にならない費用で,
- 合理的な方法で, かつ,
- 自己に分かりやすい形で,
- 自己に知らしめる事.

(c) 上記(a)及び(b)の要求が拒否した場合には, その理由が与える事及びその様な拒否に対して異議を申し立てる事ができる事.

(d) 自己に関するデーターに対して異議を申し立てる事, 及びその異議が認めた場合には, そのデーターを消去, 修正, 完全化, 補正させる事.

責任の原則(管理者の諸原則実施の責任(個人情報管理者・窓口の明確化))

データー管理者は, 上記の諸原則を実施する為措置に従う責任を有する.

OECDの8原則は, プライバシー保護と個人データーの国際流通との調和を目的としたものであるが, その勧告附属文書において示した国内適用の8原則は, その後の我が国でも個人情報保護の制度化の基準となっているものである.

2) 個人信用情報

金融関連情報として特に最近では, インターネット・バンギング又は実体的な店舗を有さずにネット上にのみ存在する銀行等が設立している. それらのサービスを利用する際には, 取引関連の情報のみならず, 詳細な個人情報がネットワークを介して遣り取りする事になる. また, ネット上で様々なオンライン・ショッピング(電子商取引)の利用が可能になるにつれ, 決済手段としてはクレジットカードが利用しているが, カード番号は決済手段としてのみならず, 個人信用情報自体もネットワーク上でやり取りしている.

個人信用情報を取り扱う信用情報機関は, 信用報告のみならず, 趣味趣向や個人の経済活動に関する情報を収集して分析を行う消費者調査も行っている. 個人識別情報としては, 個人の氏名・住所・社会保障番号・生年月日等が表示する. また, 破産宣告を受けた情報や, 訴訟が提起しているといった情報も同時に表示する. 更に, これらの情報を収集した機関も明示する.

1．4　これまでの研究の考察(論注4，5，6，7，8)

1) ITの技術的インフラに関する問題

インターネット取引の発達に伴い，電子的な決済が一般化する為電子認証は，取引の当事者間での認証，電子メールにおける相手方個人の認証など電子商取引における安全性や信頼性を確保する為認証の効力，銀行やクレジット系の取引決済時の認証，認証の責任，認証システムの機能についてより高度化する必要がある．電子商取引の国際化に伴い，決済も各国間で連携して，実施する為電子決済に関するグローバル標準のシステムや制度化が不可欠である．認証する機関，公に認めた機関，業界で認めた機関で認証を一元化する事により，認証するデーターの正確さと履歴，公正を基本とするデーターセンターを設置する事により，これらの問題は容易に解決する．つまり，個人情報認証のシステムが認めない陳腐化した真性の無いデーターとした情報は情報価値が無く，また，分散したデーターベースの情報も管理できない事による問題を含んでいる．

生涯の個人情報を管理する為，認証情報管理センター，健康情報管理センターに向けた，銀行機能を備える電子医療カルテを考察した時，ユビキタスと広域災害にも対応する新たな認証ビジネスと新たなプライバシー技術を融合するプライバシー工学の創出を考えた．

セキュリティーという，従来の暗号等による情報保護が主体の概念とは画一する．インターネット上で必要となる利用者の特定や，分散ネットワークの性質を加味した集中方式により，システム上の欠落を補完する．また，全く適用できなかった金融ビジネスなどにも確実性が要求できる．更に，生体認証データーは変更できない本人情報として漏洩や紛失できない等への認証データーの管理問題も解決する．生涯のプライバシー情報を管理する認証情報管理の高信頼性情報管理システムに向けた，情報銀行を備える電子医療カルテを考察した時，ユビキタスと広域災害等にも対応できる新たな認証ビジネスとプライバシー技術を融合する，プライバシー工学が必要である．従来のセキュリティー概念の，暗号による情報保護が主体とは画一する．筆者が考案したのは，インターネット上で必要となる利用者の特定や分

散ネットワークの性質を加味し，集中方式によりシステム上の欠落を補完する．また，全く適用不可としてきた金融ビジネスにも確実性が要求できる．更に，変更できない生体認証データーの漏洩や紛失抑止処理等により，認証データー自体の管理問題を解決する，ワンタイム情報の機能を考案した．

また，医療電子カルテの開示など，医療情報の共有化などの法整備が進む事は容易に推察する．その場合に検査情報などの，“個”の確立した情報に関して，個人識別型定義を取った場合のそれ自身では個人を識別できないが，他の情報と照合する事により個人を識別する事ができる情報である．これらは，ＡＳＰなどのデーターセンターで，今まで医院･病院の実施記録として保管していた医療情報を管理する事を前提にする必要がある．つまり，“個”の確立した情報としてレントゲン･ＭＲＩ･ＣＴなどの検査データーを病院から個人に管理を移す事を個人情報認証が可能にする事についての研究の必要性を示唆している．

2） 集中方式のデーター統合

インターネットと中高速インターネットアクセスの普及に伴って拡大が期待するデジタルコンテンツ市場は，オンラインゲーム，オンライン音楽配信，オンライン出版など数兆円の市場規模になると予想する．これらのデジタルコンテンツの管理や著作権管理の問題などを含め，ｅ－コマースや業務アプリケーションに限らずオープン･ネットワークが必要とする不特定アクセスによる利用者の特定や，分散ネットワークの性質による集中システム運用への適用に関する絶対必要条件の欠落が明確になった．

更に，旧来のインターネットの長所のみで構築したシステムは実用性が無く，金融ビジネスなどの確実性を要求するシステムには適用できない事も現実化している．現在，国･地方を通じて行政情報化を進展しようとしているが，新しい情報化の進展に伴い個人情報の保護に関する適切な処置が不可欠である．更に，市場の拡大とニーズも要求している．“個”の確立

した情報に関して個人情報認証のシステムに統合し，分散化した各種情報についても危険分散を除き，集中方式を取る必要がある．それによるシステム構築費やデーター管理，セキュリティー管理などのコストメリットは激減すると考える．

ネットワーク上を流れるデーターのプライバシーは，許可していない第三者による情報そのものへのアクセスを禁止し，情報の盗聴や改竄，本人やユーザーに成り済ました不正情報の作成やその配布を防止する事である．この為は，「認証」という作業が必要になる．例えば，パスワードによるログオンは“本人又は関係者のみ知る”とした知識認証の一方法である．しかし筆者は，今までのハッカーなどの解読手口などを参考にするまでも無く，一般には下記の様に容易なものが設定している．

例えば，ID所有者の個人情報から類推できるものとして，

- IDそのもの
- ハンドルネーム
- 自分の名字や名前，旧姓，誕生日
- 配偶者や子供の名前，旧姓，誕生日
- 自分のイニシャル
- 免許証の番号，自動車のナンバー
- 会社の名前，電話番号，部署名
- 自宅の番地，自宅の電話番号
- 学校名
- ペットの名前
- アマチュア無線のコールサイン
- パソコンの機種
- 参加フォーラム名
- 趣味

- 従業員番号, パスポートの番号,

等がある.

課題1　Easy Password

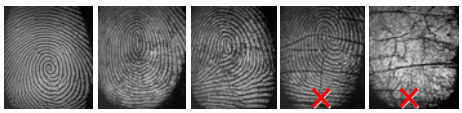
― 公知・忘却・簡便で推定も容易 ―

1.	ID	11.	Post name of company
2.	Handle name	12.	House number
3.	Family name	13.	School name
4.	Former name	14.	Pet name
5.	Consort and child's name	15.	Call sign of amateur radio
6.	Birthdays	16.	Participation forum name
7.	Initial	17.	Hobby
8.	Number of license certificate	18.	employee number
9.	Number of cars	19.	Passport
10.	Telephone number	20.	Simple password

6

課題2　人工指・他人受理・本人拒否率

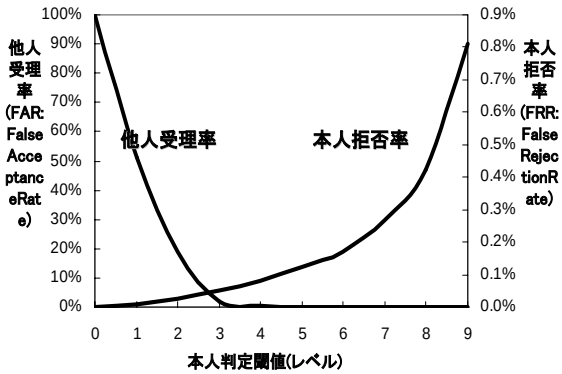
―生体認証は万人を特定できない ―



(1)指を奥に置きすぎている
(2)指を手前に置きすぎている
(3)指がセンサーの右側にずれている
(4)指の押し方が弱い
(5)指が立っている

(1)指が乾きすぎている
(2)汗が多すぎる
(3)指紋が磨耗している

□:指紋の中心
○:特徴点
\:隆線方向



7

課題3　Contact less Palm Vein Authentication
ー手の反り･角度･開き方で認識できない　ー

- ✓ The near-infrared ray is distributed evenly without contact
- ✓ The vein patterns can be extracted and matched regardless of various hold-up patterns
- ✓ The false rejection rate is the probability of the rejection of the properly registered individuals.
- ✓ The false acceptance rate is the probability of the false authentication of non-registered individuals

Contact less palm vein sensor

Near-infrared vein pattern

Vein Pattern

*In case that three palm profiles are used in registration, and one extra retry is allowed in verification

[8] 富士通㈱参考

一般に定義付けた「認証」の意は，電子的なメッセージの受信者が，送信者を識別し，メッセージの信憑性を確認するプロトコルの事をいう．

旧来，認証の為プロトコルは，秘密鍵暗号，又はＲＳＡ･公開鍵暗号のデジィタル署名（電子署名）」である．認証は，ＣＡ（Certification　Authority）が通信相手の真正性を証明するである．

ＰＫＩ（Public－Key　Infrastructure）の第1ステップはネットワークの使用に先立ってユーザーを確認する認証システムを設立する事が必要である．

1. 本人認証

   申請者側の認証

   行政側の認証

2. 電子文書の真性確保
3. 電子文書の到達確認
4. 手数料の納付方法

しかし筆者はデジィタル証明書の安全性は劣る. 即ち, 明確な証明書になっていない. ユーザーの確認情報例えば名前, 公開鍵, ユーザーのデジィタル署名が記録している. 証明書はデジィタル文書で中央ディレクトリに記録管理している. 証明書の正当性をチェックするプロセスはユーザーから確認できない.

3) 公開鍵方式による電子認証

PKIとは, (Public Key Infrastructure 公開鍵基盤) の事で, 証明書／公開鍵暗号の技術によって実現する, 暗号化や認証, 本人確認を行うセキュリティー基盤である.

ヨーロッパの民話の「長靴を履いた猫」. この物語は, 貧乏な若者が唯一遺産としてもらった猫が, 長靴を履く事で人間と同等に立ち振る舞い, 人の良い王様を騙す為百姓に嘘をつかせ, 人食い鬼の居城を乗っ取る為鼠に姿を変えさせて食べてしまう. そして若者を, カラバ侯爵として洗脳してお姫さまと結婚させ, 自分も貴族になるというもの. 現在, キャッシュカード詐欺にたとえるまでも無く, この民話は今日の日本でも生きているから不思議である.

この様な欺きのテクニックは, 行政やビジネスには使えない. つまり, u－Japanに求めている情報の正確性と秘匿性は信頼性工学の未成熟の結果, 極めて重大な国際社会問題になっている. 更に, インターネットにおける信頼性工学の意義を突き詰めると, 暗号を主体とした情報保護のセキュリティー工学の範疇では, 個人を特定できない大きな欠点がある事が判明している. 即ち, この欠点を解決する新たな定義として, プライバシー工学という『自己の情報制御による高信頼の情報を確実に担保する為能力と仕組み』が必要になる.

4) これからのPKI

本論のインターネットと端末間の送受信内容を保障する電子署名の公開鍵認証基盤は, この本人認証の仕組みとして, 本人しか知りえないであろうPINコード (知識認証) と, 本人し

か持ち得ないであろうICカード(持物認証)に基づいている. 現在, 国際的にもこのPKIが多く採用され普及活動が行われている. 更に次世代への技術適用動向は, 日本の金融機関が挙って静脈認証システムを採用している. 未だ技術的には, 未完であり本人拒否率と他人受け入れ率の問題がある.

筆者の体験で考察すると, この静脈認証の致命的な欠点は, 手のひらや指の角度や距離によって, 認証エラーの本人拒否により, 静脈認証ICカードの返却を余儀なくされた. この問題解決は技術研鑽により, 数年後にはパターン認識も完成されるであろう.

これらの本人真正不全を解決するバイオメトリクスは, 生体識別認証データーは高度のプライバシー情報である(5). このPKI問題を, 本人識別情報であるプライバシー情報を集中管理する情報センター(IDC: インターネット Data Center)で, 自己の重要情報を自己コントロール(5)により解決する. すなわち, 認証するデーターの真正性を保持し, 匿名性を維持し認証強度により段階的な開示を可能にした. この技術の応用として, 一生涯のプライバシー情報を集中管理する銀行機能を備える電子医療カルテの情報統合を考察し, ユビキタスと広域災害に対応可能となる, 新たな高信頼情報管理の具現化を検討した.

この医療IDCは, 2000年から筆者が国際学会や経済産業省に提言書などで提案した. その結果, 海外などで評価と支持を受け日本政府のe－JapanⅡの重点プロジェクト(6)と同機能である. 広域電子カルテを集中管理する当該ビジネスモデル基本特許(7)は, この提言前に筆者が発明者として日本特許庁に登録済みである.

医療IDCの, より高度なセキュリティーを必要とするシステムに, 現在の電子署名の公開鍵認証基盤は, 不適である. これは, インターネットと端末間の送受信内容を保障するだけ

---

(6) e－Japan 重点計画－2003, Ⅱ. 先導的取り組みによるIT 利活用の促進, 1. 医療, 日本国内閣「高度情報通信ネットワーク社会推進戦略本部, http://www.kantei.go.jp/jp/singi/it2/kettei/030808honbun.pdf

(7) 特許第3520365号 2000－330949(10／30, 2000), 情報通信システム, 出願者, 高知工科大学, 発明者, 中川喜博, IPC:G06F 15／00, 日本

のPKIには，本人真正証明不全の技術的な問題が存在する為ある．このPKIの脆弱性を克服する為バイオメトリクスがあるが，この認証技術で利用する個人認証の生体識別認証データー自体が究極のプライバシー情報であり，個人情報である．

5）認証データーの集中管理

本人識別情報である個人情報を集中管理するIDCを活用する事で，自己の重要情報を秘匿レベルに応じて自己コントロールするシステムである．即ち，認証するデーターの真正性を保持しつつ，匿名性を維持し認証強度により段階的な開示を可能にした．この技術を新規事業の展開として，一生涯の個人情報を集中管理する銀行機能を備えた電子医療カルテの情報統合管理センターを考察した．そして，ユビキタスと広域災害にも対応可能とする，新たな高信頼情報管理が必要不可欠である．

1．5．研究の目的と意義

会社組織の中の知的資産を“個”の社員が様々な業務経験で得た専門知識やノウハウを，会社全体で一元管理，“個”の価値評価の集大成が会社の価値評価にもなる企業の競争力を高める新たな経営手法の理論とシステムの必要性は容易に導く事ができる．この新しい企業価値評価の経営手法により，商品・システム開発・業務効率化の面で短期化・低コスト化への社員の問題解決能力が向上できる．この“個”を明確に認識するメカニズムが必要と考える．

PKI(8)は，確実な“個”の本人確認ができない．この重大問題の原因は，本人の推定状

(8) Information Management — PKI Guidance, ITS & PKI Sector, Treasury Board of Canada Secretariat, Example Risk Levels, E—Signature Types, and Retention Methods and Practices, March 31, 2002, http://www.cio—dpi.gc.ca/pki—icp/guidedocs/mngt—gestion/mngt—gestion04__e.asp#__Toc13556737

態のままでの承認が，PKIシステムの前提になっているからである．そのため，PKIの相互認証によって信頼関係を構築するインターネット社会の基盤になり得ていないと考えた．この欠陥とは，ICカードとPINコード（パスワード）を各個人による完全保管が前提であり，偽造や盗難には全く対処できない事にある．本人確認については，旧来の金融システムの磁気カードとパスワードから余り進歩していない．

PKI利用の主たる目的は，電子署名とシステム利用者の厳密認証及び，伝送路の暗号化である．従来の銀行キャッシュカードの様な，ID／パスワードの代替技術として秘密鍵や証明書及び，それらを格納するICカードを用いてインターネット上に構築するPKIによって暗号化したセキュアな伝送路を確立しただけである(9)．なお，電子認証は，公開鍵証明書への電子署名による信頼の連鎖だけで電子認証は実現しており，広範な電子認証においてPKIを代替可能な技術は現時点では存在していない(10)．バイオメトリクスなどの重要な個人識別情報を，入出力装置のICカードや携帯電話，PC等の移動体に格納する事は，情報漏洩につながる危険性がある．この対策として，盗難・スキミング・忘却のリスクから防御するシステムが必要であると考えた．現在，本人の真正認証ビジネスとして，生体認証を利用したユビキタス環境における携帯電話，PDAなどのモバイル端末や電子サイン，電子パスポート，運転免許証のICカード化の本人判定装置がある．

しかし，この本人判定装置に個人の生体情報を照合データーとして格納しなければならない．また，照合完了や端末認証の通信データストリームを流す偽装置の存在が重要問題であると考える．従来，これらの手続の大多数は窓口で，フェイス・ツー・フェイスで紙を介し

---

(9) 情報セキュリティ総合戦略，～世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と 総合的な安全保障向上～，経済産業省，2003 年10月10 日，9P－12P，63P－64P，http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_body.pdf

(10) 電子署名・認証ハンドブック【パーソナルユース編】，(財) 日本品質保証機構電子署名認証調査センター，3P，http://www.jqa.jp/11it/pdf/hb_p.pdf

て行われてきた. しかし, インターネットを介してこれらの手続を行う電子政府においては, 本人確認が非常に重要な要素となっており, 個人認証が電子政府構築への最重要課題である(11).

1) 主体となる“個”の意義

新たな企業価値評価における社員評価の“個”の扱いにおいて, オープン・ネットワークにおける認証極めて重大な欠点は, 本人確認について非対面で通信データーの遣り取りを行う事である. 筆者はこのPKIの重大な欠点と課題は, 他人がPKIに本人として認証局に登録する“成り済まし”など, 以下の5つと考える.

- 成り済まし
- 生体認証データーのプライバシー
- 信頼パス複雑化と有効性検証
- 秘密鍵の秘匿
- 信頼破壊時の即時対応

現在の技術では, 認証局で発行する認証については, 認証データーのみを, 本人推定者からの到達を証明させる事に限定している. また, 本人推定者からの認証データーについて, 慎重に到達の経由ルートを確認する技術理論と方法のみに, 依拠していた. この様な既存の技術では, 受信側は受信の内容が送信者本人のもので, 真正かどうかが判断できない. 閉じたネットワークでは, ID, パスワード等は, 当事者間での事前の合意がある場合のみ, 本人確認の有効な手段となる. しかし, インターネットでは, データー送付者と本人を結び付ける技術が確立していない. 更に, 事前の合意の無い第三者にとっては, 誰がデーター送信者であるかを認

---

(11) Information Management － PKI Guidance, ITS & PKI Sector, Treasury Board of Canada Secretariat, Example Risk Levels, E－Signature Types, and Retention Methods and Practices, March 31, 2002, http://www.cio－dpi.gc.ca／pki－icp／guidedocs／mngt－gestion／mngt－gestion04__e.asp#__Toc13556737

識する手段となるものは無く，成り済ましには電子認証でも認識できない．つまり，別の人が成り済まして偽りのデーターをやり取りしていても，受信側は本人かどうかの区別が付かない．

そこで，データーの改竄を防止する為，データーを送信した人が本人である事を証明すると同時に，真正の個人情報を保護する為技術として，電子認証と個人情報の正確なデーターが必要である．成り済ましの行為を防止する為，個人を証明する証明書とその真正データーの組み込み技術が基本的に要求する．更に，この証明書の登録･管理を行い，身元の保証と，個人情報を保護し，データーの有効性を担保する機能が必須と確信した．

以上を整理すると，筆者が提案しようとする個人認証局の構想において，次の問題解決のアプローチが，不可欠である．

第1は，セキュリティポリシー

第2は，セキュアなシステム構築

第3は，セキュリティマネジメント　である．

第2章　個人情報管理システムの構築

2．1．個人情報保護の社会的ニーズ

本論文の構想は前章の欠点を補うだけでなく保護すべきデーターと管理については従来の紙の管理を一元管理などにおいて凌ぐなどの点を含み筆者が構想を重ね完成したその構想をビジネスモデル基本特許として権利化した．(12)

現状の技術と理論では当事者間での本人確認は，前章まで問題提起し論じた様に，非対面でデーターの遣り取りを行う事による決定的な限界がある．つまり，本人と見なする者からデーターが来た事を慎重に確認する技術に留まっている．それにより，自分の知らない所でデジィタル署名が簡単に契約できる様になる為，社会混乱に陥る事は容易に想定できる．

本論文で定義する個人情報認証（データーセンター）は，通常の認証と下記の点で大きく異なる．

- 個人情報の銀行機能を持つデーターセンターとして，インターネットなどのネットワーク上で利用するＥＣ（エレクトロ・コマース）など，個人の情報を必要とする場合に認証と，データーの提供機関となる．
- データー提供方法も“個”毎に公開レベルを設定できるとして，必要に応じた最低限の公開方法として柔軟性を持たせるのである．

本構想自体，筆者がその構想と概念を発明し，1998年より実現性への考察を開始した．その後の完成度も加えこの筆者によるプライバシー工学の構想について以下に記述する．

---

(12) 特許第3520365号　2000－330949（10／30，2000），情報通信システム，出願者，高知工科大学，発明者，中川喜博，IPC：G06F　15／00，日本

(論注1) オフィスオートメーション学会　Vol．25No．3　PKIの重大欠陥による新ビジネスの創出　―個人情報と認証情報を銀行機能集中管理へ―　(16年10月掲載)

(論注2) 映像情報メディア学会　新しい個人情報認証局システムの開発，投稿

2．2 個人情報認証構想の考案

本構想は，各種インターネットを活用して各種認証手続を行うにあたり，

- 個人情報データーの管理保全
- 個人情報保護データー認証の統合

を特徴とした『個人情報認証』という管理局が従来の紙と実印の世界から開放し，学校･医療現場などの保護すべき情報の運用をするものである．

全世界の研究技術者の過ちは，認証について，認証で認証データーのみのデーターを発行するかの理論と方法に基づいていた為ある．個人情報銀行の役割として，証明書の登録･発行･更新･失効とユーザーが承認したデーターの提供を行い，ユーザーの保証と保護を行う．

個人が個人情報認証に対して設定する，個人情報保護レベルと提供承認のアクションは，携帯電話などのモバイル端末の形態がある．また，個人情報認証は政府のデーターセンターの様な大規模なものでは無く，会社単位の様に個々に閉じたサーバーの運用も対象とする．

また，別の人が成り済まして偽りのデーターをやり取りしていても受信側は，本人かどうかの区別が付かない．この問題点のデーターの改竄を防止する為，データーを送信した人が本人である事を証明すると同時に真正の個人情報を保護する為技術として電子署名とその対象とする正確なデーターが必要である．

ナリスマシの行為を防止する為，個人を証明する証明書とその真正データーを統合する技術が今回の目的である．

この証明書を登録･管理を行い，身元を保証し，個人情報を保護する機関が個人情報認証にあたる．この構想自体，どの国も無く機能自体が新しい．つまり，認証だけ行うシステムは存在しているが，認証と多種多量のデーターを組み合わせた認証システムは存在しない．

本発明の特徴は，情報公開手順，公開方法，許可した認証の方法を登録しておける，という点にあり，新機能の効果

- 使いやすい　公開手順が明確

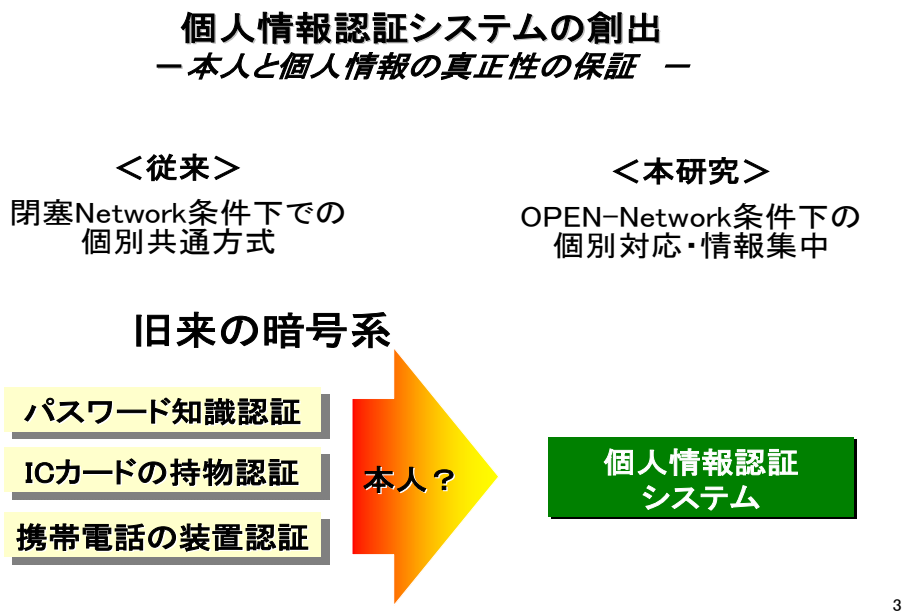
- 速い　　認証管理で性能を保証
- 省資源　　一元管理
- 高信頼　　連携設備バックアップセンタ
- 安全性　　セキュリティーシステム
- 確実性　　本人確認手続

従来，これらの手続の大多数は役所の窓口で，フェイス･ツー･フェイスで紙を介して行われてきた．そして，役所の窓口では，申請等を行う人の本人確認が重要な位置を占めていた．

しかし，インターネットを介し，これらの手続を行う電子政府においては，本人確認が非常に重要な要素となっており，個人認証が電子政府構築への最重要課題となっていた．

1） 個人情報認証の新構想

閉じたネットワークでは，ID，パスワード等は，当事者間での事前の合意がある場合，本人確認の有効な手段である．しかし，インターネットでは非対面でのデーター送付者を結び付ける技術的な枠組みが未だ確立していない．事前の合意の無い第三者にとっては，誰がデーター送信者であるかを認識手段となるものでは無い．成り済ましには電子認証でも認識できない．



各種行政手続を行うにあたり，個人情報保護と電子認証を統合する制度と共に，情報処理などの管理保全などの安全対策を考慮した『個人情報認証』が必須となる．またそれに伴い，セキュリティー手順と機能の標準化を行う必要がある．これら要件を満たすインターネットを介して，情報通信を可能とする下記の様なシステムの存在が必要となる．

個人情報認証システムの概要

保管する個人情報の例としては，行政の住民基本台帳及び給与の他に，保険証券，法的文書，医療文書などが主な対象として校区，青少年育成に関する履歴など個人に関するものが対象となる．つまり，インターネット内のシステムで個人情報が必要な場合，個人情報認証にその公開基準と認証を提示してサイトに提出する様になる．この個人情報認証は，個人情報データーの正式な提供機関であり，データーと認証と同一又はペアとして発行して，個人情報の正当性を保証する．これらは，ＯＥＣＤの８原則に従って管理運用する必要があり，以下の機能は必須条件である．

① 本人承認のデーター

インターネットは基本的に要求応答型のシステムである．よって，利用者は，Webサイトと情報のキャッチボールを行いながら次々と新しい情報を得る．利用者の提供する情報は匿名性が高く犯罪の温床になっており，公的機関で利用する場合は真正と擬似の切り分けを明確に行う必要がある．

しかし，インターネットを普段利用する場合，使用する個人情報に関しては真正のデーター流出抑止が前提であり，故意に個人の偽り情報をシステムで判断して送るなどの対応が必須条件になる．つまり，個人を特定しないデーターを利用者個人はその提供するデーターについて，当然了解していなければならない．また，児童子供に関しての承認行為は，児童本人とその監督責任を持つ保護者が承認する．

例えば，

⑴ 児童の氏名についてはその児童本人の氏名では無く学校側で一律に定めたドラエモンやポケモンのキャラクタ名などの一般的な氏名，

⑵ 児童の住所については，児童本人の住所では無く学校の所在地の様なアクセ

ス可能な住所

⑶ 児童の生年月日については児童本人の生年月日では無く学校側で一律に定めた生年月日などである.

したがって情報利用者に対し, 児童の氏名などの個人情報がそのまま提供せずに済み, 児童の個人情報を有効に保護できる一方, 児童は継続してインターネットが利用可能である. 個人情報認証(データーセンタ)で管理する個人情報については, 本人認証はパスワードを含めバイオメトリクスなどの生体認証などを行い, 自己情報の開示請求権・訂正請求権・目的外利用等の中止請求権の保障を可能とする必要がしなければならない.

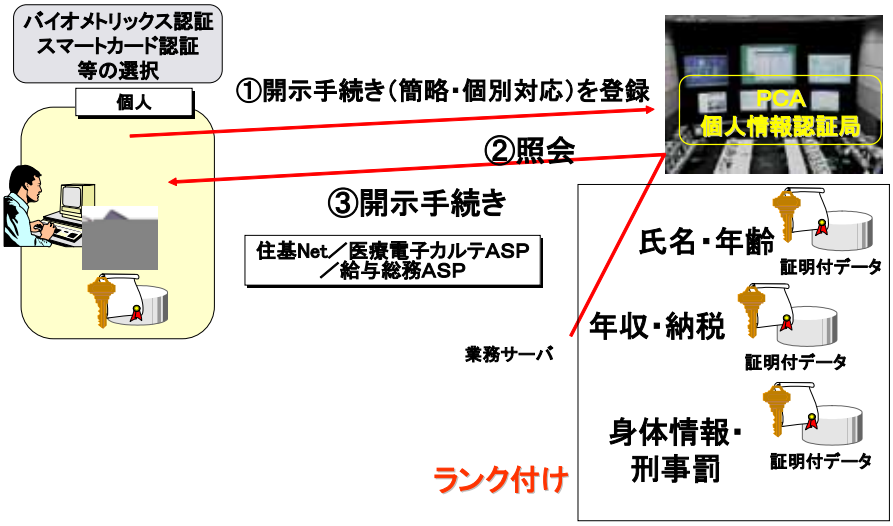
② 情報公開レベルの設定

個人情報のデーター提供方法は, 情報項目毎に対して段階的な公開レベルを設定できるとして, 必要に応じた最低限の公開方法として柔軟性を持たせる必要がある. 電子政府システムなどの公的機関で必要とするものでも, 個人情報認証には予め利用するシステム又は情報のシステムを管理する国家・地方公共団体毎に定めた個人情報保護条例などの公開基準のレベル毎に個人情報などを登録しておく必要がある. 地域行政サービスなど通常のインターネット利用には, 住民・自治体が定めるレベルを使用するなどの規則性が必要である.

つまり, 公開レベルを予め設定可能とする個人情報認証(データーセンタ)が必要である. 例えば, 個人情報認証は, 児童の氏名, 生年月日, 通学路, 保護者名, 保護者のクレジットカード名, 保護者の年収, などのある個人情報に対してその公開レベルを, 第一公開レベルないし第二公開レベルとして定めて, 情報セキュリティーの段階的な機能を要求する.

プライバシー技術②　複数の開示手続き

（情報開示手続きを秘匿レベル毎に設定）



- 第一公開レベルは，保護するべき内容が通常程度の個人情報として児童の氏名などである．ただし，ここでの児童の氏名は児童本人の氏名では無くドラエモンや鉄腕アトムといったキャラクタであって，児童本人を特定する事ができない情報である．
- 第二公開レベルは，保護するべき内容が中程度の個人情報として児童の年齢，通学路などである．第二公開レベルの場合は，保護者の事前の同意ないしは認知が必要なものである．
- 第三公開レベルは，保護するべき内容が高程度の個人情報として，保護者のクレジットカード名，保護者の年収などである．

③ 個人情報の保護教育

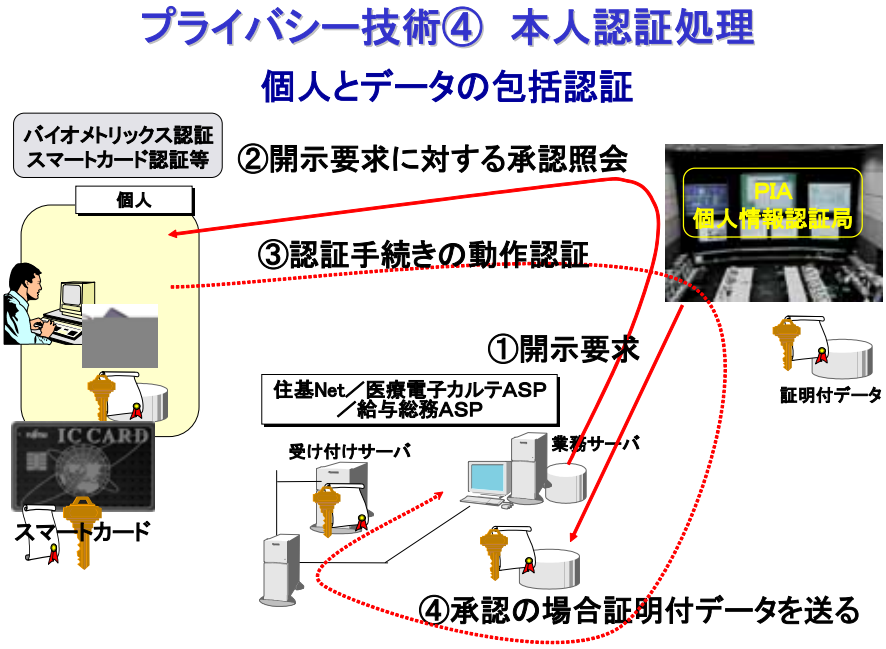
インターネットのシステムにおいては，児童･子供のみならず一般も含めて個人情報に対するセキュリティーの意識付け教育を十分に行う必要がある．その教育には，情報漏洩などのリスクなどに対して理解させる一般的な概念教育と利用学習中における具体的指導の方法がある．インターネット利用又は情報発信を行う中で，今まさに発信しようとする個人情報（実データー）を明示し，公開に際して想定するリスクを表示する機能を有する事

により，より具体的な体験学習をさせる事が必要である．

また，この様な個人情報が公開する事を情報提供側に対して警告を行う様にすると，児童はその警告に気づいて個人情報を不測に公開してしまう事を防止できる．この様な警告の機会を，児童生徒に提供する事により，巧みな手口によるWebサイトから逃げる術を学ぶ様になる．

④ 個人データー提供と認証

個人情報のデーターセンターとして，インターネットなどのネットワーク上で利用するインターネット試験・ECなど，個人情報を必要とする場合に認証と，データーの提供機関が必要である．一般にECなどの個人情報保護としては，企業内，企業間，企業消費者間，行政間，学校との間の取引等が挙げるが，各場面によって本人確認や個人情報認証，公証サービスのニーズも異なってくる．



この各場面において，認証・公証ニーズの要求レベル毎の個人情報データーと認証と共に，学校企業間ECにおける児童個人情報認証の運用基準作成，公証サービス実現の

為環境整備等を必要とする. 個人情報個人情報銀行の役割として, 証明書の登録･発行･更新･失効と児童生徒が承認したデーターの提供を行い, 個人情報データーの保証と保護を行う. 個人が個人情報認証に対して設定する, 個人情報保護レベルと提供承認のアクションは, 携帯電話などのモバイル端末の形態も考慮しなければならない.

また, 個人情報認証はデーターセンターの様な大規模なものでは無く, 学校単位の様に個々に閉じたサーバーの運用も考える.

⑤ 個人情報の保全と管理

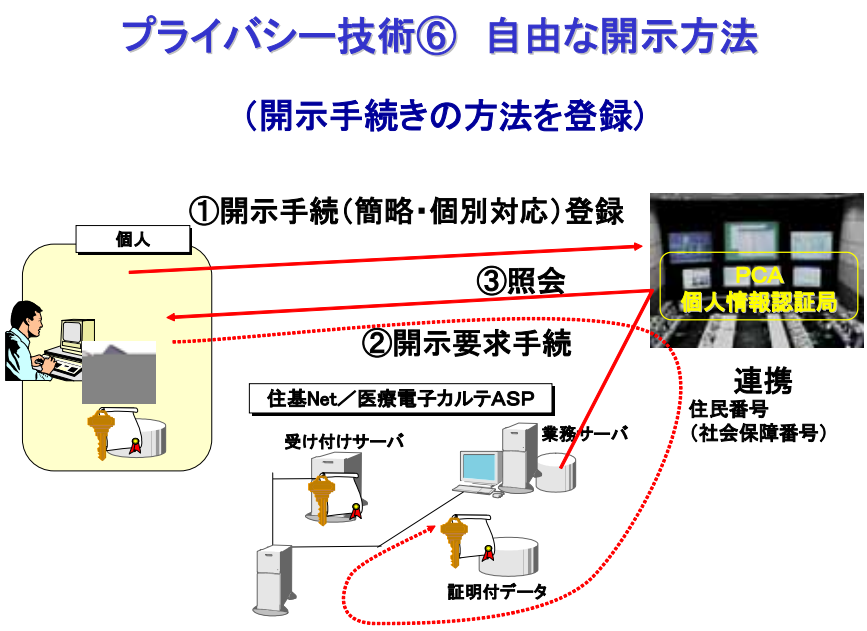
個人情報認証は, 個人情報保護システムを有するが, その機能には情報の自由な流通を促進させる為, 個人情報データーの保護と整合性の確保と, 明確な管理が必要である. ＯＥＣＤの8原則の下, 各国で制定している個人情報保護法などのグローバルスタンダードに沿った管理方法でなければならない. 教育機関で個人情報がどの様に収集･保管しているかを保護者･地域に対して公示する必要がある. これらの機能を十分に満たした, 個人情報を管理するシステムが必要である.

つまり, 学校事務の個人情報の適正な管理において児童学生の家庭これら家庭環境調査や連絡網･緊急連絡先に関する,『児童生徒の情報管理手順』などを教育委員会, 学校の単位で明確化する必要がある. よって, 教員は自宅などの児童生徒（保護者）承知しない個人のノートブックパソコン又は自宅など, 不特定の場所にデーターを保管できなくなる事を意識しなければならない.

また, これら個人情報の複製など利用範囲の拡大と削除･焼却にも最善の注意を必要とする.

⑥ 本人固有の情報公開手順

個人情報に関して，利用者に対して情報を公開する方法を予め本人が知っておく必要がある．



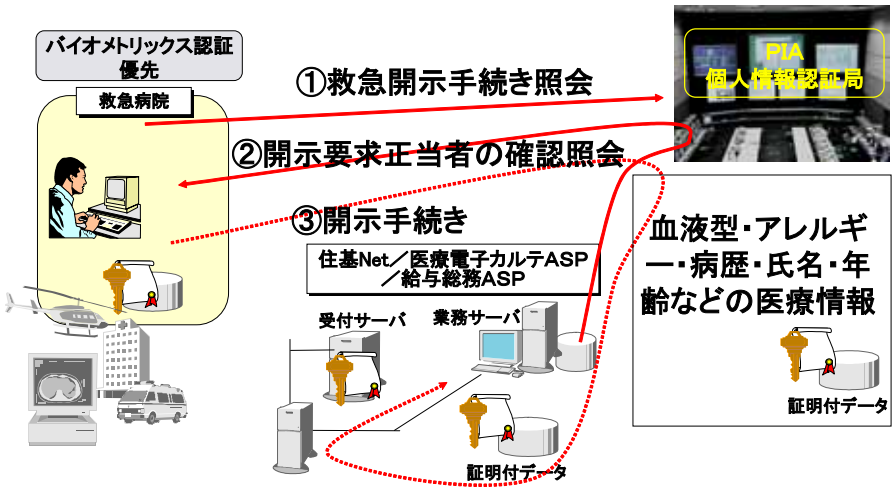
必要以外の個人情報については公開する必要も無く，提供する必要も無い．よって，必要最低限の公開を行う為は個人の事情による公開手順が必要になる．

⑦ 生命緊急時などの公開

個人情報のデーター提供方法は，本人の意識に関わらず身元確認を容易にし，生命維持に必要であれば，病歴，アレルギーなどの検査項目などの情報を得る事が必要である．

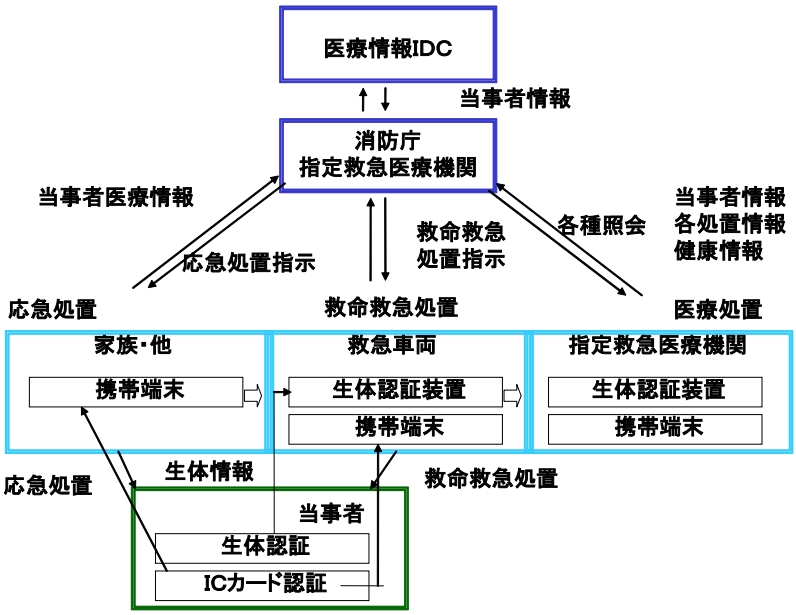
プライバシー技術⑦　緊急時の開示方法

（緊急時開示を本人が受諾済）



ただし，緊急時に本人が提供する意思を事前に確認しておく必要がある．

また，死亡などの身元確認なども同様である．

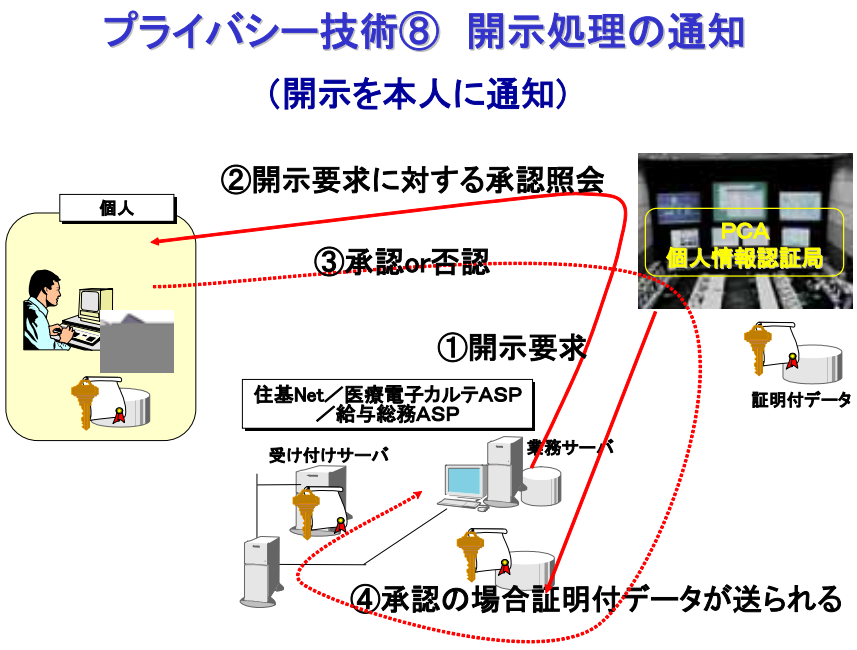


⑧ 公開時に本人に確認

本人が知らない内に個人情報を閲覧などの防止の為公開する場合はメールなどの通

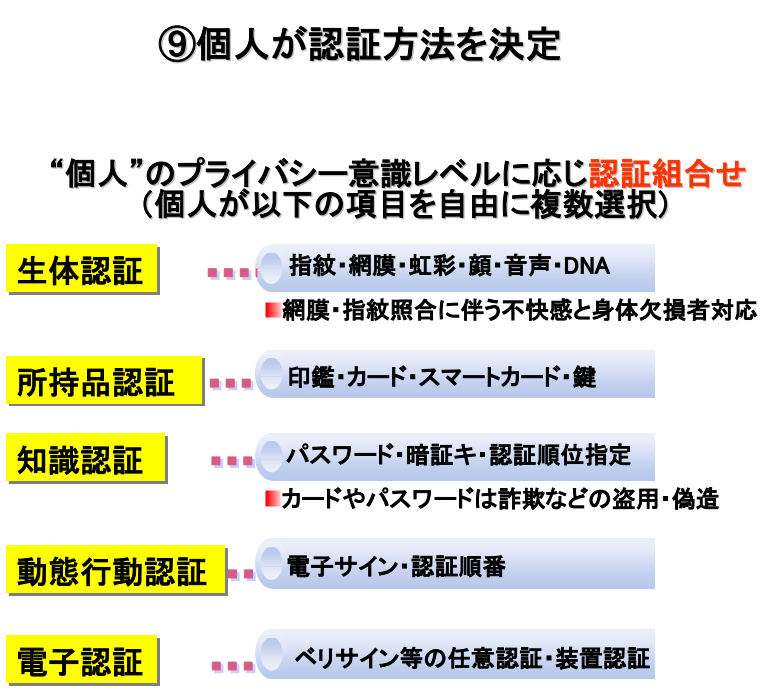
知により警告及び承認依頼を本人に出す機能が必要である.

ただし, 給与処理などの定期的な業務を始めとする安全性が確保した機関による個人が承認している場合は, 本人確認不要とする.



⑨ 個人が認証方法を許可

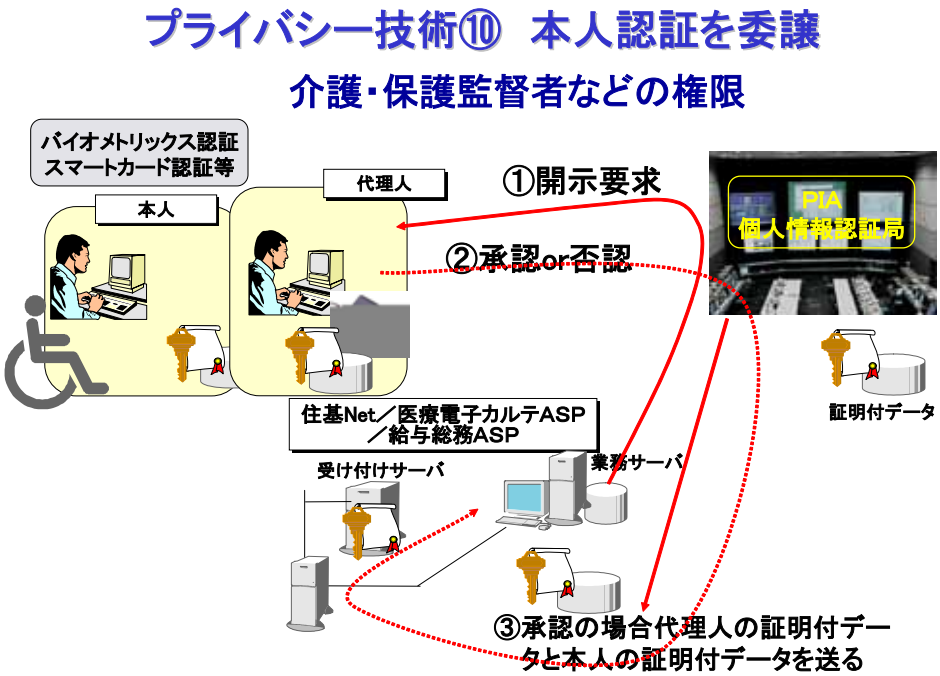
個人情報認証に対して, 本人である証明方法を定義する事を可能とする.



パスワードとIDカードのみで許可するセキュリティレベルと，バイオメトリックスを併用したセキュリティレベル認証などの個人の特性に合わして認証を行う事を可能にする必要がある．身体欠損などによる代替え処置を含め，公平な装置と安全性確保の為須である．

⑩ 個人情報の権限委譲

個人情報認証は，個人情報保護システムを有するが，その機能には幼児などの保護者を必要とするもの又は身体知能障害などの介護を必要として保護者が代理を行う場合など，個人情報に関する管理認証権限の委譲を行う事を可能としなければならない．



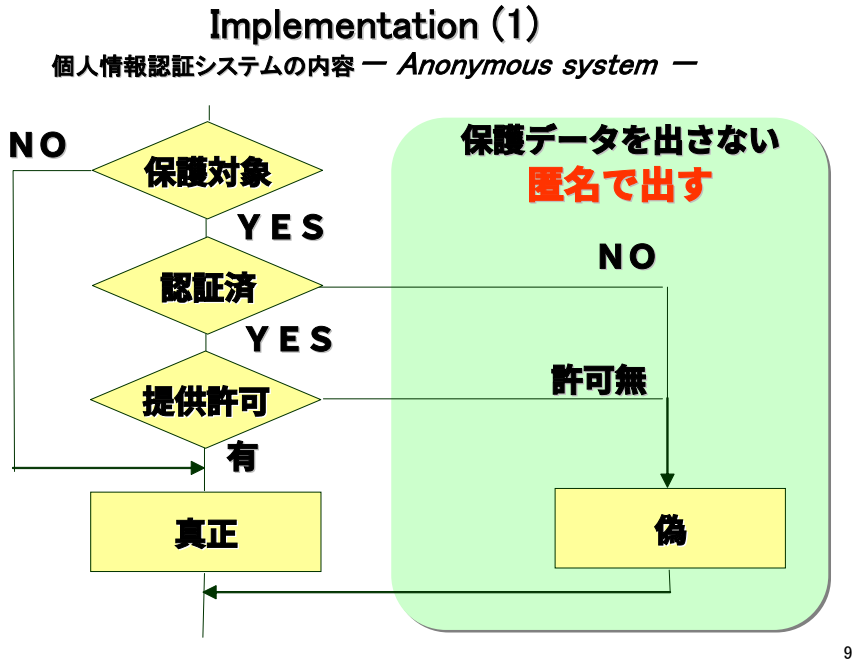
以上の機能を満たす個人情報認証が必要であり，文教・医療・自治体・企業・個人などの分野で実際の活用方法を探る．

2） 個人情報保護認証

前述を踏まえこれら要件を満たすインターネットを介して，情報通信を可能とする下記の様なシステムの存在が必要となる．

まず，パソコン単体などでの個別管理では無く，第三者が管理し，児童らの個人情報は，クラス単位，学校単位又は地域単位の団体でセキュリティー管理のシステムになる．例えば自治体が保有する11桁の住民票コードを付与する「改正住民基本台帳法」に基づく住民票データーと個人の認証を行う公的な個人情報認証（データーセンタ）の存在が必要となる．保管する個人情報の例としては，行政の住民基本台帳及び給与の他に，保険証券，法的文書，医療文書などが主な対象として校区，青少年育成に関する履歴など個人に関するものが対象となる．

つまり，インターネット内のシステムで個人情報が必要な場合，個人情報認証にその公開基準と認証を提示してサイトに提出する様になる．この個人情報認証は，個人情報データーの正式な提供機関であり，データーと認証と同一又はペアとして発行して，個人情報の正当性を保証する．



2．3 個人情報認証の技術設計と基本運用設計仕様

2000年に筆者が特許にて発表した完全独自仕様から現行のRAの機能を融合させた.

1) IICAの目的

個人情報認証(IICA:Individual Information Certification Authority)は, 個人情報認証による情報資源と情報基盤の安全な活用を支えるものである. IICAは認証方法に基づく個人情報データーと認証証明書を使う為部門や機関が必要な設備, 仕様, 指針を確立する. その目的は,

- 情報システムのセキュリティー
- 電子商取引
- 電子メールを含む安全な通信

にある.

IICAは機関の間だけでなく, 個人情報認証の他部門の出先機関, 自治体, 企業, 国民の間の安全な通信と商取引を支える. IICAは, 極秘では無いが取扱いに注意を要する応用プログラムにおける安全な通信と情報処理を容易にする.

企業, 一般国民, 個人情報認証の他機関, 及び自治体間の安全な通信の為は, 個人情報認証は重要な役割を担う. IICAは, 閉鎖的な個人情報認証共同体内だけの内向の通信及び情報システムの安全性確保に焦点を合わせているのでは無い. むしろ, その目的は, 全国及び世界との安全な情報アクセスと通信を個人情報認証ユーザーに対して提供する事にある. 併せて, 個人情報認証内部の安全な情報アクセスと通信を提供する. 個人情報認証の認証方法暗号使用の働きかけは, 一般的には, まず機関内部の緊急性の高い施策を直接支援する個々のアプリケーションから始まる. これら個人情報認証アプリケーションは, 各機関における効率性の向上や費用削減効果をもたらす. その様なIICAはそれ自身がより大きな地球規模の個人情報認証の一部を生かす. 通信ネットワークにおいては, 端末数

が増えればより有効性が増すが，それと同様に，個人情報認証の「信頼ネットワーク」は，より広範囲で地球規模の共同体との安全な通信とネットワークを許容する事で，より有効性が増す．

IICAの大きな課題は，個人情報認証技術を用いている個々の機関のプロジェクトを結合し，種々の民間ベンダーレベルから広範囲な相互信頼ネットワークに持っていく事にある．この実現には，個人情報認証全体は，事実上も，それら部分を併せたものより大規模になっている様になると考える．

2) 基本概念

個人情報の電子認証は，認証方法－認証手順ペアの概念に基づいている．個人情報の電子認証者は，他人に対して秘密にしておく一つの認証手順と，それに付随する認証方法を持ち，認証方法は公にする．

認証方法を与えられても，それから認証手順を見つける事はできない．個人情報の電子認証者は電子文書（メッセージないしFile）に自分の認証手順で認証する．信頼者は個人情報の電子認証者の認証方法を用いてこの認証の正当性を確かめる事ができる．個人情報の電子認証は次の三つの重要なセキュリティサービスを提供する．

- 内容の正当性確保（integrity）：認証した文書に対するいかなる変更も，認証正当性確認で不当とする．
- 成り済まし防止（secure non－repudiation）：個人情報の電子認証者だけが自分の認証手順を知っているので，個人情報の電子認証者だけにその認証ができる．
- 相手確認（authentication）：依頼者は，個人情報の電子認証者に対して要求を送る事により個人情報の電子認証者の身元確認ができる．個人情報の電子認証者は，その要求に対してある付加情報を付け（これにより何らかの攻撃を防ぐ），その要求と

併せて個人認証プロトコルの確認を行う．もし，依頼者が個人情報の電子認証者の認証方法でその認証が正しい事が確認できれば，依頼者に要求する個人情報が提供する．データー自体が送付する事により，個人情報の電子認証者により認証した事が分かる．

これらに加えて，認証方法技術は依頼者と個人情報の電子認証者に対して秘密性を提供する．依頼者は個人情報の電子認証者の認証方法によりメッセージを暗号化でき，それは個人情報の電子認証者だけが（自分の認証手順により）復号化できる．依頼者は，一時的に用いる個人情報を個人情報の電子認証者の認証方法で暗号化し，それを個人情報の電子認証者に送る事ができる．個人情報の電子認証者はそれを自分の認証手順で復号化できる．これにより，依頼者と個人情報の電子認証者は，Triple DES暗号Algorithmに基づく個人情報を使って，お互いの間のメッセージを暗号化できる．Triple DES暗号方式は，DESを3回繰り返す暗号方式で最も暗号強度は最高レベルに近いので極秘データーの暗号化に広く使用している．

認証方法証明書は電子文書であり，それには，少なくとも，使用者の名前と認証方法が記述して，認証機関（IICA：Individual Information Certification Authority）により個人情報の電子認証している．個人情報データーと認証証明書の目的は，使用者の名前と認証方法の信頼性を保って関係付ける事にある．依頼者は，そのIICAを信頼すると同時にそのIICAの認証方法を知っており，個人情報の電子認証者の個人情報データーと認証証明書上のIICAの認証を確認する事により，個人情報の電子認証者の個人情報データーと認証証明書から個人情報電子認証者の認証方法の信頼を持って確認できる．

更に，IICAには，登録機関（RA：registration authority），個人情報データーと認証証明書状態通知，管理機関（management authority）がある．登録機関（RA）はそれ自身では個人情報データーと認証証明書の発行は行わないが，IICAが個人情報データーと

認証証明書を発行する末端利用者の身元を登録する. 個人情報データーと認証証明書状態通知は, IICAの為, 信頼関係者の監査済み個人情報データーと認証証明書の状況情報を提供するインターネットサービスである.

個人情報認証により実現するセキュリティサービスは, 個人情報認証とセキュリティサービスを支援する情報サービス, 安全サービスである. 中心には核となる個人情報認証があり, それが個人情報データーと認証証明書を発行, 管理する. 一番目は, その個人情報データーと認証証明書を使う顧客で, 次は様々なセキュリティサービスを提供, 用意する様々なセキュリティー特化のサービス又は機関である. 一般的な情報･通信サービスは, 範囲外にあり, それらの中では, 必ずしもセキュリティーに特化するものでは無いが, セキュリティサービスに重要な幾つかの一般サービスを表している. 外側は, 核の個人情報認証や顧客, 機関, サービスにより実現するサービスを表している. 中心の個人情報認証は, 非機密･取扱注意のアプリケーションの為, 諸部門や関連機関により使われる認証方法個人情報データーと認証証明書を管理するIICA, RA, 個人情報データーと認証証明書状態通知, 及び管理機関からなる.

これら核となる個人情報認証は次の事を行う.

1. 認証方法個人情報データーと認証証明書の発行
2. 必要に応じ認証方法の失効
3. 個人情報データーと認証証明書の発行及び失効を行う為指針の確立
4. 後年の個人情報データーと認証証明書の有効性確認が必要である場合に備えた情報の保存

個人情報認証クライアントは, その個人情報認証が発行, 管理している認証方法個人情報データーと認証証明書を使い, 個人情報認証ユーザーにセキュリティサービスを提供する. 個人情報認証クライアントは, 個人情報データーと認証証明書に関して, 次の4つの基本的な役割を果たす.

1. 認証方法と認証手順ペアの生成
2. 個人情報の電子認証の生成
3. 個人情報の電子認証の検証
4. 認証手順管理(即ち, Triple DESAlgorithmによるセションないしメッセージについての合意ないし配布)

最初の機能, 即ち, 個人情報ペアの生成は, IICAないしRAでも行われる. しかし, 個人情報の電子認証の為クライアントによる個人情報生成は, このシステムの整合性の保持, 成り済ましの防止に役立つ. というのは, これにより, 個人情報の電子認証に使う認証手順はそのクライアントだけが持つ事になるからである. 残りの三つの機能は, クライアント間同士の直接の手順により, 認証方法に基づくセキュリティー手順の多様性を可能とするものである. これらのサービスには, 監査, 監査済みの対象・役割に基づくアクセス制御成り済まし防止サービス, 及び秘密保持がある.

数多くのサービスと機関がこの共通個人情報保護基盤を支え, クライアントはこれらサービスと機関からセキュリティサービスを受ける様になると考えている. サービスの全範囲は十分には明らかでなく, 未だ進化段階でもあるが, 次のものは含む様になると考えている.

- 電子公証:電子公証は, 公証人制度と類似のサービスを提供する. 公証人は, ある文書に対する信頼のおける日付を提示し, それにより, ある時点でそれが存在する事を示すと共に, 認証した文書の認証の信憑性をも証明する.
- 個人情報復旧機関:IICAは秘密保持の個人情報管理に使う認証手順のコピーを個人情報復旧機関(IIRA:Individual Information recovery agent)に委ねる. あるいは, 暗号化したメッセージを送るあるクライアントが, 一時的に暗号化に用いた個人情報をIIRAの認証方法で暗号化し, そのメッセージに含めるかもしれない. IIRAの目的は, 個人情報を無くした際に暗号化したデーターの復号化の許可, 管理監督, 法律面の強化である.

IICAと個人情報復旧は分離した方が良い様になると考えている. IICAが唯一秘密保持ないしアクセスする必要があるのは自分自身の認証手順だけであるのに対し, IIRAは大量のクライアント認証手順の保管, 保護, 及び注意深く制限したアクセスを提供する必要がある. IIRAは, その保持する利用者認証手順の分離的な制限を行い, それらの個人情報にアクセスするには二つ以上の機関の調整が必要な場合もあると考えている.

これは, 個人情報管理用の個人情報ペアのみに当てはまる. 即ち, 個人情報の電子認証に使う認証手順は通常, 個人情報データーと認証証明書保持者によって他の組織には決して漏らしてはならない.

- 書留配達機関:このサービスは, 書留便と類似の, 受け手の成り済まし防止のサービスである.
- このサービスにより, あるメッセージが場合によっては受取拒否や, そのメッセージを配達する.
- チケットデーター関:この機関は, データーないしシステムへのアクセスに使える暗号化した電子「チケット」を提供する. ここでは, 認証方法かTriple DES暗号のいずれかを使用し, 分散システムでのアクセス制御を集中管理する手段を提供する.
- また, 次の三つの情報ネットワークサービスは個人情報認証にとって特に重要である.
- レポジトリ:レポジトリは, 証明書や廃棄情報の様な他の関連情報の保持及び検索の為, インターネット公開アクセスシステムである. 事実上, 個人情報データーと認証証明書はそれをレポジトリにおく事により発行する. レポジトリには, 認証実行ステートメントも置く. IICAにおいては, 期待する正規のレポジトリはLDAP[RFC1777]を用いたディレクトリである.
- データーアーカイブ:アーカイブはIICAFile及び文書の長期保存を行う. IICAの寿命は比較的短い. しかし, 非常に古い文書上の認証の正当性を確認する事は重要

様になると考えている. IICAはその利用者認証の確認に必要な情報を保存する準備が必要だが, アーカイブにおいては, かなり後年の, 例えば数10年後に必要となるデーターを作り出す事が可能である.

- 名前付けと登録:分散環境においては, 多くの対象は一意の名前を持つ必要がある. この事は, セキュリティー対象物に対しても同様で, 例えば, 認証対象物や発行者は一意の名前が必要である.

3)個人情報認証サービス

個人情報認証は, 非極秘・取扱注意の個人情報認証の情報処理と国家情報基盤(NII)の使用に必要なサービスと設備を提供する. それには次のものも含む.

・個人情報の電子認証:

- 監査
- 正当性確認
- 成り済まし防止
- 通信セッション
- 電子メールメッセージ

IIRAにより拡張した場合は, 個人情報認証は暗号化データーに対する個人情報復旧サービスも提供する.

個人情報認証は, 安全な情報アクセス, 通信, メッセージング及びデファクト標準や公的セキュリティー標準に準じた主流の商業セキュリティー製品を使う企業ないし個人ユーザーとの電子商取引に必要なサービスと設備を提供する.

4) 個人情報認証データー構造

X．509 標準で定義している三つの基本データー構造がIICAで使使用する．即ち，個人情報データーと認証証明書(certificate)，相互個人情報データーと認証証明書ペア(cross certificate pair)，個人情報データーと認証証明書廃棄List(CRL：Certificate Revocation List)である．

5） 相互個人情報データーと認証証明書

複数のIICAはお互いに相互認証する事がある．それは，各々が他方に対して個人情報データーと認証証明書を発行し，その二つの個人情報データーと認証証明書をcross Certificate Pair と呼ばれる単一のディレクトリ属性で組み合わせるものである．crossCertificatePair属性は両方向の信頼チェインをサポートする．共通の「ルート」IICAから始まる信頼モデルでは無く，利用者に個人情報データーと認証証明書を発行したIICAから始まる信頼モデルにおいては，これらのペアが必要になる．

6） 個人情報認証経路Architecture

認証経路は，個人情報データーと認証証明書の連鎖である．その連鎖は，証明者によって信頼しているIICAの認証方法から始まる．認証経路のそれぞれの個人情報データーと認証証明書は，その前に証明する者の個人情報によって認証する．信頼団体は，その経路の中の個人情報データーと認証証明書中の認証を順番に証明していく事により，一つの認証の証明を行う．認証経路は，個人情報認証の必須のArchitecture構成要素である．認証経路の配置は様々な方法があり，その結果も異なる．

7） 認証及び認証経路

認証付き書類の認証は，個人情報データーと認証証明書中の認証方法で正当性確認がする．認証自身は，その書類に認証するのに使った認証方法の個人情報データーと認証証明書を特定はしない事に注意する．もし全ての個人情報データーと認証証明書の認証方法でその書類の認証が確認してなければ，その認証は確認できない．個人情報の電子認証者には，自分が信頼するIICAがある．そして，その認証方法を知っている．通常は，個人情報の電子認証者は，ある信頼できる「別の搬送方法」によってその個人情報を含む「自己認証した」個人情報データーと認証証明書を与えられているので，個人情報の電子認証者はこの認証方法を知っている．

依頼者は，異なるIICAが発行する個人情報データーと認証証明書を持っており，そのIICAの認証方法を個人情報の電子認証者は知らない．しかし，そのIICAは，個人情報の電子認証者が信用するIICAから個人情報データーと認証証明書を受けているかもしれないし，あるいは，個人情報の電子認証者が信用するIICAから始まって他のIICAに向かう個人情報データーと認証証明書の連鎖が存在し，最終的に依頼者の個人情報データーと認証証明書に到達するかもしれない．この様な連鎖は，認証経路と呼ぶ事にする．

そして，個人情報の電子認証者は，自分が知っているIICAの認証方法から始め，引き続く認証を確認し，最終的に依頼者の個人情報データーと認証証明書に到達する．IICAが他のIICA又はend－entityに出した個人情報データーと認証証明書による信頼関係トポロジーであるという事を理解しておく事が重要である．

8） 認証経路Architecture

IICAが個人情報データーと認証証明書を発行する際は，組織的で順序付けした方法を取る事もあれば，より柔軟で順序付けしていない方法を取る事もある．更に，現在のWeb Browser製品は，一般的な意味での認証経路処理方式を余り使わない，簡略化した「フラット」な個人情報認証のみが実装している．システマチックで順序付けした認証経路のトポロジ

ーは階層構造的であるが，より一般的なトポロジーは，相互認証したIICAのメッシュ構造である．

9） 階層構造

権威機関（Authorities）は，個人情報データーと認証証明書を出す「ルート」IICAの下に階層的に従属IICAを配置する．これらのIICAは，その階層内での下位のIICA又は利用者に個人情報データーと認証証明書を出してもよい．

階層構造個人情報認証では，全ての信頼集団はルートIICAの認証方法を知っている．どの個人情報データーと認証証明書も，ルートIICAからの個人情報データーと認証証明書の認証経路確認によって確かめる．個人情報の電子認証者は，IICA4 によって発行した依頼者の個人情報データーと認証証明書を確認し，次にIICA2 から発行したIICA4の個人情報データーと認証証明書を確認し，最後に，ルートであって個人情報の電子認証者がその認証方法を知っているIICA1 から発行したIICA2 の個人情報データーと認証証明書を確認する．

10） 個人情報認証Architecture

近い将来，機関において多かれ少なかれ個々のアプリケーションをサポートする為独立のIICAを設立する努力があると想定する．多くの場合，IICAの設立及び運営費用はその機関が果たすべきミッション，例えば，購買，許認可，外交等をサポートする何らかのアプリケーションから産み出している．そして，認証方法技術の適用は，その機関アプリケーションに直接寄与する事で正当化する．

また，別の場合では，一般利用者に対する個人情報データーと認証証明書の発行や個人情報の配送を容易に行う為民間のIICAサービスプロバイダを利用しており，その費用負担は，それら個人情報データーと認証証明書に依存する様々な機関のプロジェクトがいっ

ている. この様な個別の個人情報認証においては, より広範囲の個人情報認証規模のIICA については, 一般的にはほとんど考えられておらず, 既存のシステムでは統合的な運用やより広範囲の国家IICAの創造は容易では無い.

ユーザーが増えるほどネットワークは価値を増すという「メトカルフェの法則」は, 勿論個人情報認証にも当てはまる. ローカルな環境だけでなく, 全体, 国及び世界規模に信頼関係を増やすシステムに大きな利益がある事は明白である. ある個人情報認証における信頼関係は認証経路に沿って増えていく.

個人情報認証の大きな課題は, 様々な機関によって現在既に実装している個人情報データーと認証証明書を使う多くの, そして通常は極めて異なったシステムがあるという現実を踏まえて, それらの間に一貫した方法で認証経路を作り出し, 十分信頼性の高い広範な信頼関係を増やしていくかにある.

機関IICAや個人情報認証外のIICAの間にシステマチックな認証経路を提供するブリッジIICA (BIICA) を使う. 何らかの標準や要件に適合したIICAは, BIICAと相互認証を行う資格を持ち, それによって, より広範なないし国家IICAでの信頼関係の相互運用に必要な認証経路を得る.

時には, 機能的に劣るクライアントの認証経路処理の制限で, 相互運用性に混乱を来すかもしれないが, この様な認証経路の存在は, 広範な信頼関係の相互運用において必要な前提条件である.

第3章　経営管理分析理論

3．1　統合データーベースのコンテンツの提案(論注9)

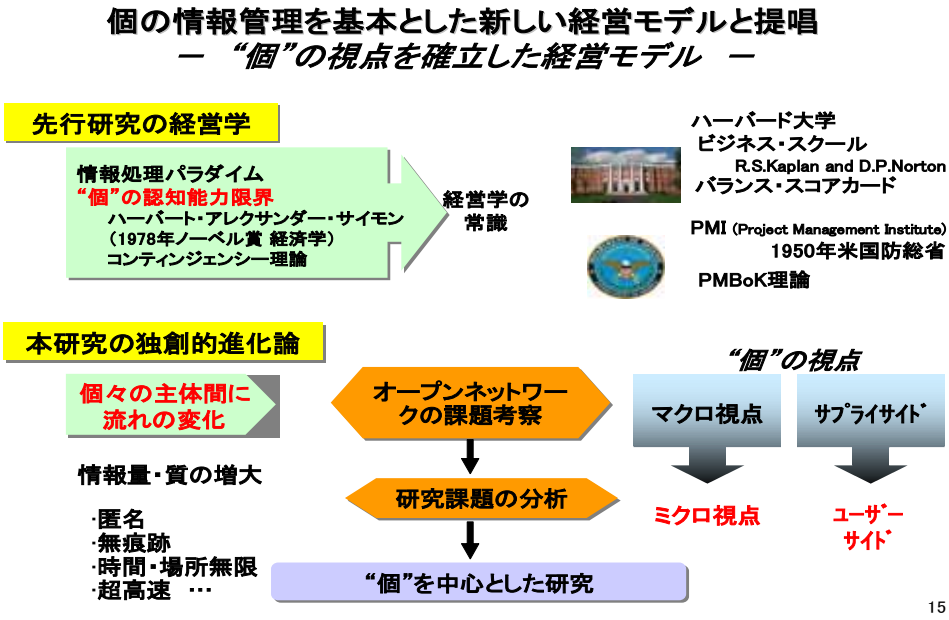
従来の製造業を中心とした資金，設備，土地などの有形資産経営から，知識経済という特許などの知的財産権の無形資産に基づく知識経営戦略へと企業経営の環境が変化している．この知的資産は，財務諸表には現れない．本論文では情報化時代の競争優位を獲得する為の新しい企業評価システムを提案する．

本論文で着目した点は，“個”の単位で管理する経営理論は存在しないばかりかその分析も実績も無い所に着目した．かつてはデーターとして極細すぎて管理もデーターの定義もできなかったと推測する．この“個”の単位で管理する企業価値評価は，情報技術革新に伴う戦略的事業経営判断と管理技法において，戦略情報分析･経営評価分析･統合業務評価単位などの活用により，経営環境及び仕事のスタイルに変革をもたらすと確信する．

新しい企業価値評価方法として以下を考えた．

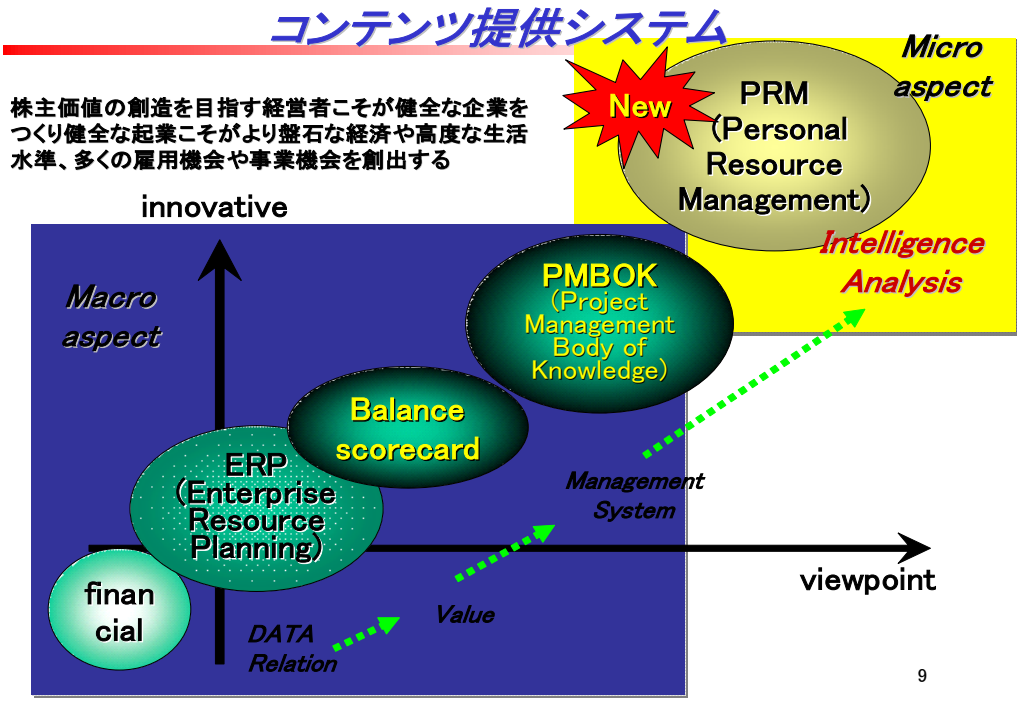
- 選択した目標が戦略を構成する相関関係が適切に対応できる
- 評価計数は最終的に“個”の計数にリンクする
- 事前的計数と事後的計数とに適切なバランスがとれている
- 業績評価の計数は企業価値に変化を起こすものである事

(論注9) 2001年8月24日　　電気通信学会，次世代ERPの構築について



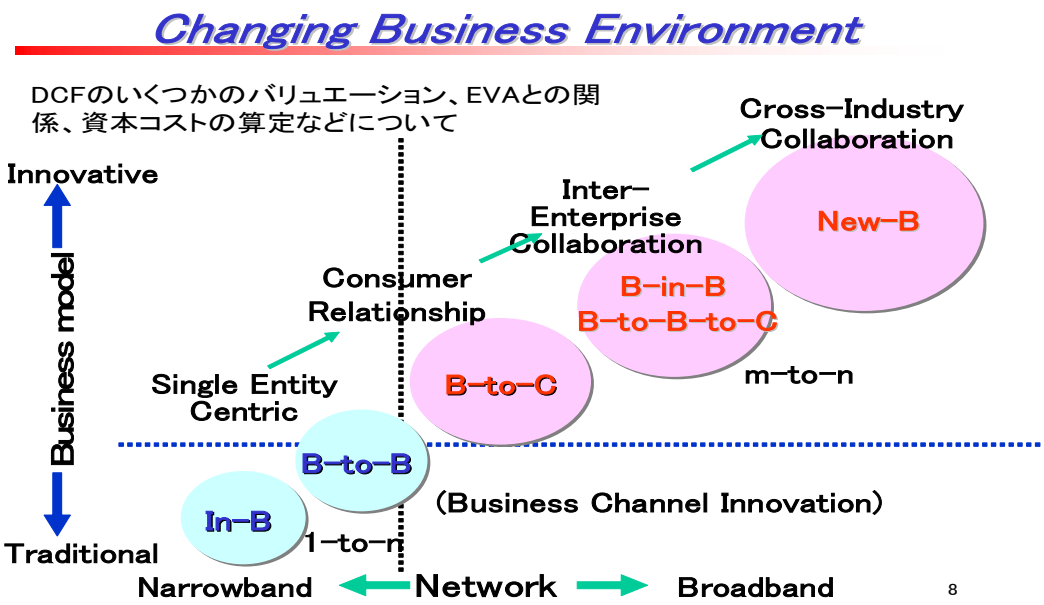
企業の価値評価は財務分析又は，評価分析は財務会計ばかり行われてきた．また評価については，将来業績予測として回帰分析などの統計的方法を用いて財務的な面を中心に分析評価している．しかし現状は，経営分析の手法自体は旧態依然のままであり，財務会計が中心である．経営者や株主が，戦略的経営判断と投資を可能にする事業価値評価の理論の確立が必要である．

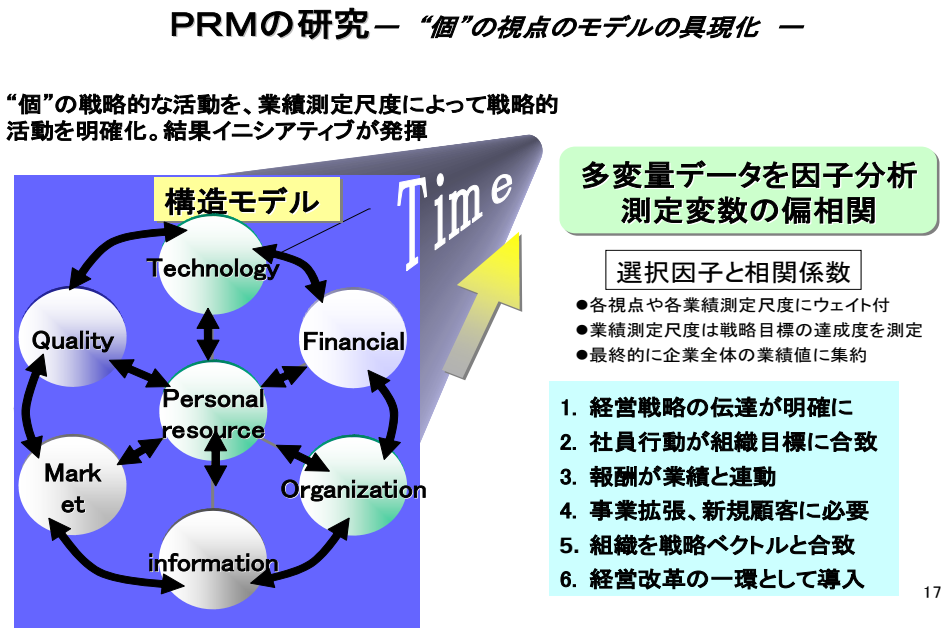
そこで，最先端の情報技術を駆使する事前提とする，次世代の多要素によるデジタルな経営評価と，価値評価理論の確立と，実現する技法を筆者が考案した．



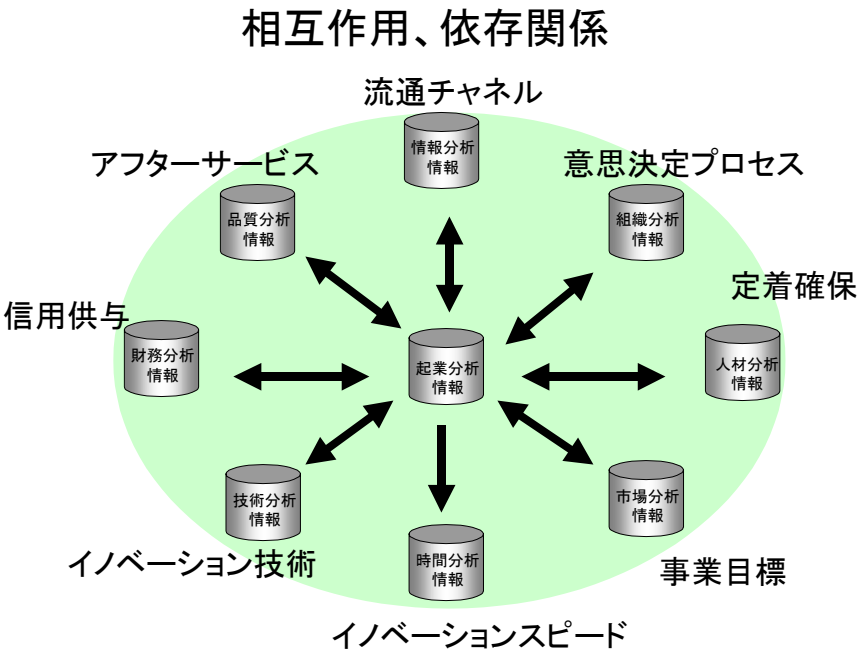
この科学的に捉える相関分析法（多要素相関に時間軸を加える次元ベクトルの企業・事業価値の評価）は，新たな変化の増減量をデジタルで捉え，人工知能により評価する技術でリスクやリターンを定量的に評価し，計数理論を数値化と可視化，更にシュミュレーションの先行計数予測で明確化する．

ＩＴ技術を前提とし，動態評価など全く新たな経営評価理論で，評価経営手法の進化を可能とさせる統合連携分析である．





8つの評価要素単位で構成する特徴を持ち，新しい理論で定量化するデーターは，全てがお互いに関連性を持つ為知的資本形成活動に着目した評価の価値連鎖がフルメッシュで関係付けを行う．



その相関させる要因は，事業目標，戦略，プロジェクトマネージメント，是正と再構築である．そして，この企業実態の把握は，情報の活用や評価が，従来の枠組みとは明らかに異なる事ある．この企業実態の把握は，情報の活用や評価が，従来の枠組みとは明らかに異なる事である．

① 時間

情報技術と処理能力を最大限に活用する経営分析において，各分析単位の時系列マイルストーンの変化量を定量化したベクトルで表記し，活動のスピードとそれらを基にしたシュミュレーション分析と先行計数と傾向などを評価する．(13)

(13) 付加価値の源泉，Hermann Simmon/Yoo,, ilHwa, , 69p-192p5章時間資源, , 洋経済新報社

時 間

時 間	
	スピード
	計 画 構 築
	現 在
	未 来
	短 期 計 画
	中 期 計 画
	長 期 計 画
	生 産 性
	変 化
	目 標
	事 業 目 標

等・・・

①時間　基本的な要素として重要 （スピード戦略）

各分析単位の時系列マイルストーンの
変化量を定量化したベクトルで表記

情報技術と処理能力を最大限に活用する経営分析において、
活動のスピードとそれらを基にしたシュミュレーション分析と
先行指標と傾向などを評価する。

企業内でERPパッケージの導入で資源最適化は、
Supply Chain ⇒ **量的な観点**
IT ⇒ **価格面**
（企業間の最適化、動的化、タイムリー）

企業間で取引きされる金額 ⇒ 単価 × 数量×時間（スピード）

時間軸の最適化を全面に打ち出した
サービス、ビジネスは無い

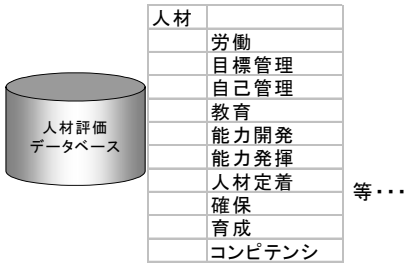
② 人材

個人の能力を，より高度な知識を身に付け高める手段と適応する能力を数値化し評価する．また，その能力をグループや組織に移転して，更に大きな能力にしていく育成能力も含み，コンピテンシなどを段階的な数値化を行い評価する．(14)

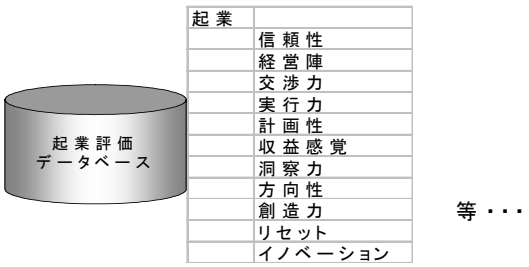
---

(14) マーケティングマネージメント，John a.. Howard，93p-94p 動機付け測定方法，KENPAKUSHA

人材



（起 業 ）



② 人材

HRM（ヒューマン･リソース･マネジメント／人材管理）

経営者能力･営業力･企画力･実行力･目標

個人の能力を、より高度な知識を身に付け高める手段と適応する能力を数値化し評価する。また、その能力をグループや組織に移転して、更に大きな能力にしていく育成能力も含み、コンピテンシなどを段階的な数値化を行い評価する。

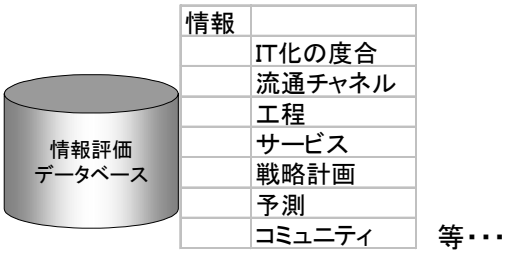
人材教育や人材確保での問題

·クローズ型雇用からオープン型雇用への雇用形態の変化
·企業内教育から自己投資への人材教育の変化
·年功中心から能力･業績中心への給与システムの変化E−**成長を決めるのは資産の大きさではなく、技術と人材**

③ 情報

情報共有と収集環境を含めた能力と情報の活用力を評価する．また，知識を組織やグループに移転，知識を移転する為情報技術の活用と知識共有件数などを評価する．

情報



③ 情報

KM（ナレッジマネジメント／知識管理）
情報ガバナンス・情報リテラシー

情報共有と収集環境を含めた能力と情報の活用力を評価する。また、知識を組織やグループに移転、知識を移転するための情報技術の活用と知識共有件数などを評価。

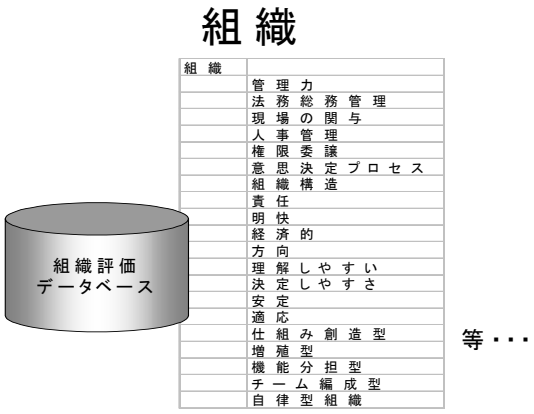
- ビジネス戦略を結びつける。
- 業務プロセスを結びつける。
- 文化を結びつける。
- 行動を結びつける。
- 物理的オフィス環境を結びつける。

知識ライフサイクル

1. 生成
2. 蓄積
3. 加工（整理、知識化）
4. 利用
5. 廃棄
6. 管理・運用（KM）
7. 表出化
8. 連結化
9. 内面化
10. 共同化
11. 人 → 人、知識
12. 知識 → 人、知識

④ 組織

仕事やもの，心に対する価値観を均一にし，チームが個人を助け成就させる組織力を，新たな評価基準を作成して評価する．また，個人のアイデアを掘り起こす段階，実現する段階で，開発力，開発工数と一般的な生産性基準からの効率と高職位者の，イニシアティブの度合いを評価する．



④ 組織

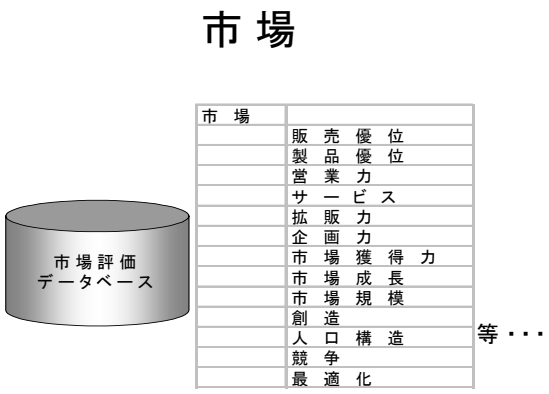
財務管理・法務・総務・経営者・人事
危機管理・IT化・意思ﾌﾟﾛｾｽ

仕事や物、心に対する価値観を均一にし、チームが個人を助け成就させる組織力を、新たな評価基準を作成して評価。個人のアイデアを掘り起こす段階、実現する段階で、開発力、開発工数と一般的な生産性基準からの効率と高職位者の、イニシアティブの度合いを評価する。

1. ビジネスの遂行には、組織力と行動力（体力）と知力が必要
2. 組織力を活かして1＋1＝3の仕事をする
3. 積極的に情報交換を行う
4. 商品の融通を行う
5. 個人を助け、思いを成就させる
6. 個人がアイデアを醸成し、ビジネスを企画するための蓄積結果）グループ全体でロスを無くす（組織力の強化、活用）

⑤ 市場

今後の伸び，市場の大きさは，競合関係，顧客絞り込み，新規顧客獲得，顧客分析，市場分析，マーケット分析，クレーム処理件数，顧客情報の戦略的情報活用範囲と市場優位戦略へのイノベーションなどを評価する．



⑤ 市場

市場獲得性・市場成長性・市場規模
販売優位性・製品優位性・実用性

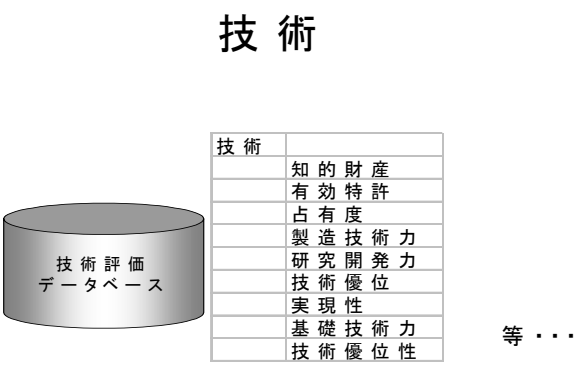
顧客絞り込み、新規顧客獲得、顧客分析、市場分析、マーケット分析、クレーム処理件数、顧客情報の戦略的情報活用範囲と市場優位戦略へのイノベーションなどを評価する。

- ·次世代の商品
- ·ビジネスを伸ばす
- ·多方面に興味
- ·顧客
- ·ビジネスの優位性

マーケットに対し、経営の状態、ポジション

⑥ 技術

技術そのものとその技術を使ったビジネス展開の事業コンセプトや，有効特許の件数など知的財産を含め，着想･構想･設計･開発などの技術革新力と，創造性･管理運営能力･技術力を補完する能力と，差別的特徴のある技術力などを評価する.



⑥技術（知的財産）

知的所有権占有度･製造／技術優位性･実現性･研究開発力

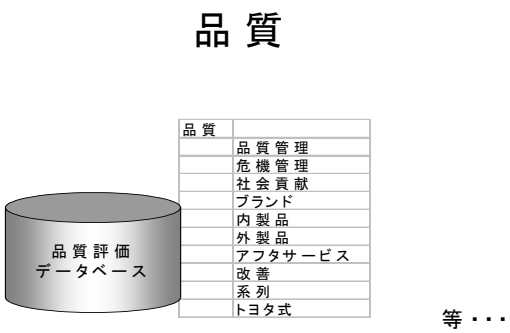
有効特許の件数など知的財産を含め、着想･構想･設計･開発などの技術革新力と、創造性･管理運営能力･技術力を補完する能力と、差別的特徴のある技術力などを評価。

競争優位の技術を活かす

発明(の技術)が「出願時点」において背景技術レベルより判断。
革新的な発明：所謂基本発明(特許)、若しくは既存技術の延長ではなく従来の 技術レベルから飛躍した革新的な技術に関する発明。また、従 来技術の延長上にあっても、発明による改良部位が著しく広範 囲に及ぶもの
改良発明～従来との差が大～：
A. 発明による改良部位が広範囲に及ぶもの。
B. 発明による改良部位が製品の主要部に関するもの。
C. 社外より(高い)評価を得ている場合

⑦ 品質

シックスシグマなどの適応有無と，生産からサービスまでミクロ単位の品質管理と，コスト削減率の積み上げなどに対する監査項目とその回数，是正件数などの改善率を評価する．



⑦ 品質

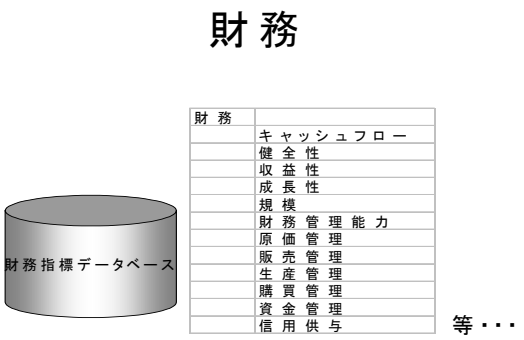
シックスシグマなどの適応有無と、生産からサービスまでミクロ単位の品質管理と、コスト削減率の積み上げなどに対する監査項目とその回数、是正件数などの改善率を評価する。

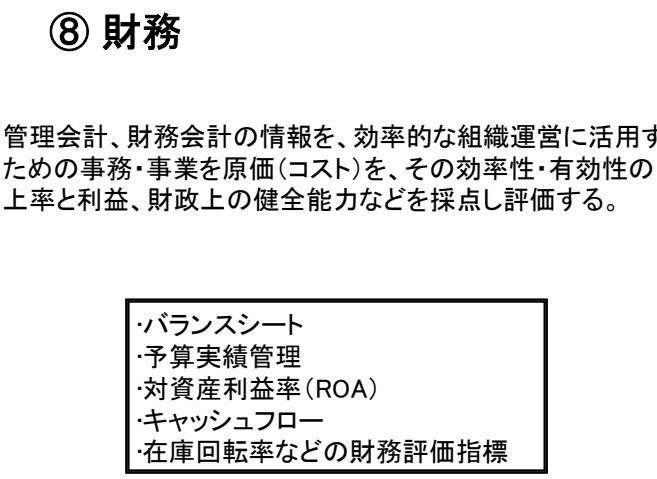
標準インタフェースの決まり方が，市場で多数派となったインタフェースが事実上の業界標準（デファクト・スタンダード）として追認されていく。

「マルコム・ボルドリッチ賞」という経営品質賞の選考基準を参考
商務長官マルコム・ボルドリッチの提唱による「顧客の視点から企業を見直す」

⑧ 財務

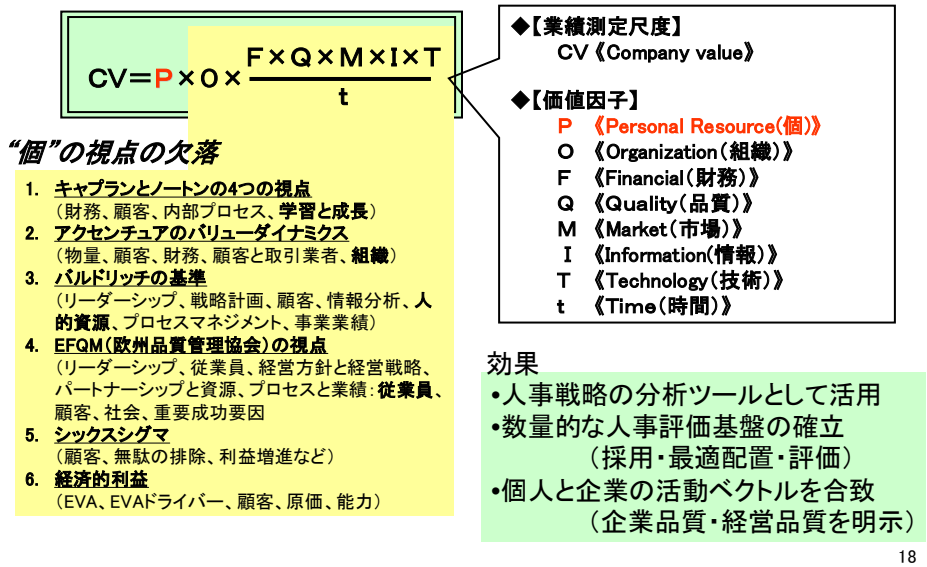
資金繰り, 管理会計, 財務会計の情報を, 効率的な組織運営に活用する為事務･事業を原価（コスト）を, その効率性･有効性の向上率と利益, 財政上の健全能力などを採点し評価する.





経営の情報工学的な分析構築において, 従来の分析単位の集計中心によるアナログ理論では, 企業評価分析として完成できない. その為に, 全く新たな理論を必要とした.

― “個”の視点を中心とする業績測定尺度に関する考察 ―



人工知能の推論では，バランスシートからどこまで推為ができるかなどの神業的な経験知識を構築し，デシジョンマネジメント支援を行う．また，これらは単に一般企業だけが対象では無い．

例えば，地方自治体の行財政改革を推進する手法として，活動基準で細分化した行政サービスの効果と，評価を明らかにする事が可能になる．これにより，行財政運営の効率化と再構築（リエンジニアリング）を実現する為，判断基準としての評価分析として活用できる．

日本には，カンバン方式や高信為性運動などの推進する手法として，KJ法，ブレーストーミング，データー中心の業務分析（コア・データーンスとそれ以外の業務を分離）などがある．

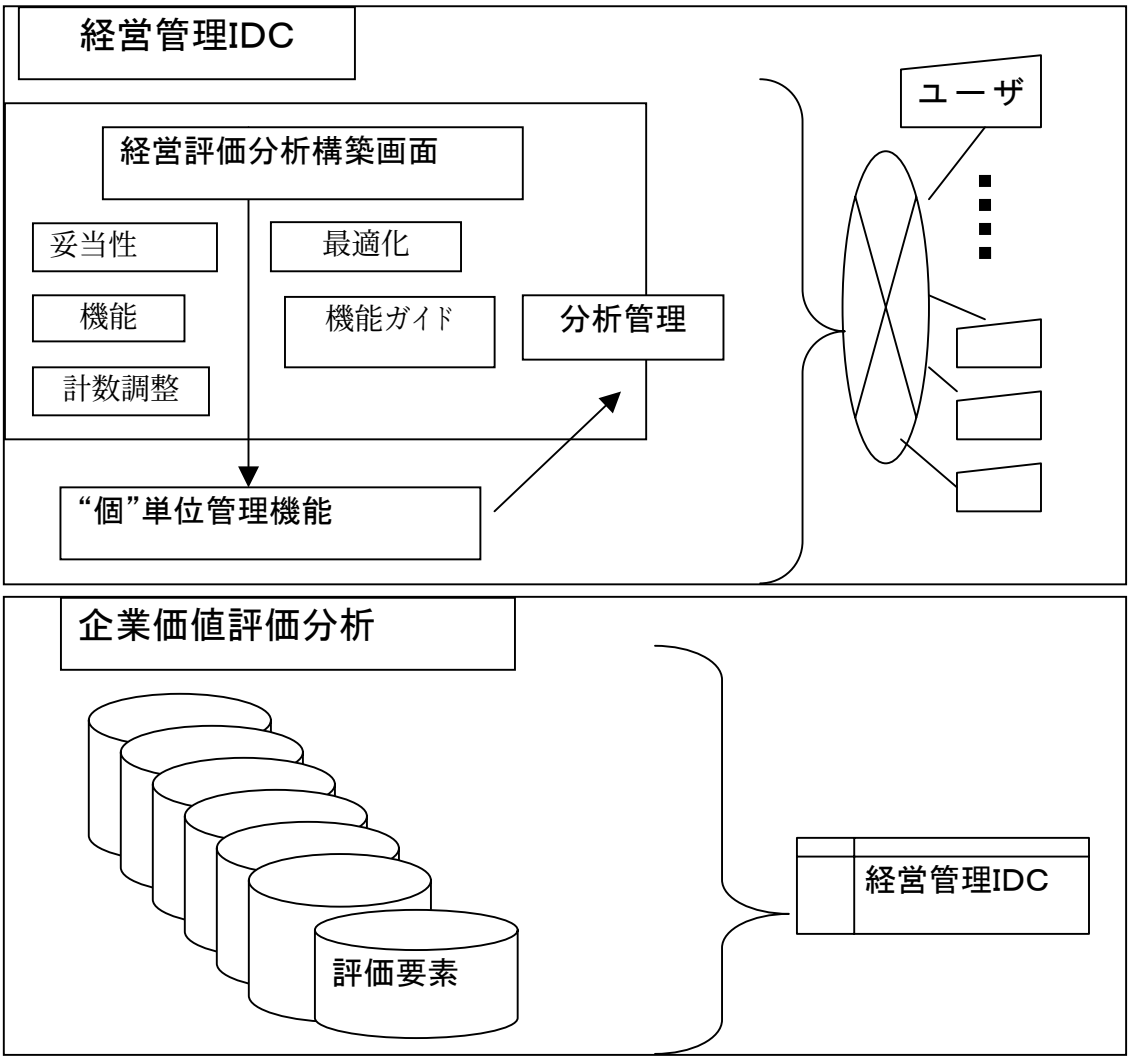
この企業価値の把握は，情報の活用や評価が，従来の枠組みとは明らかに異なる事である．

戦略を実際の計数に落とし込むプロセスが大切で自分たちがどういう為織にしたいのか，その為に何をするのかという事を計数化する．

3．2， 次世代の経営評価理論(新構想)

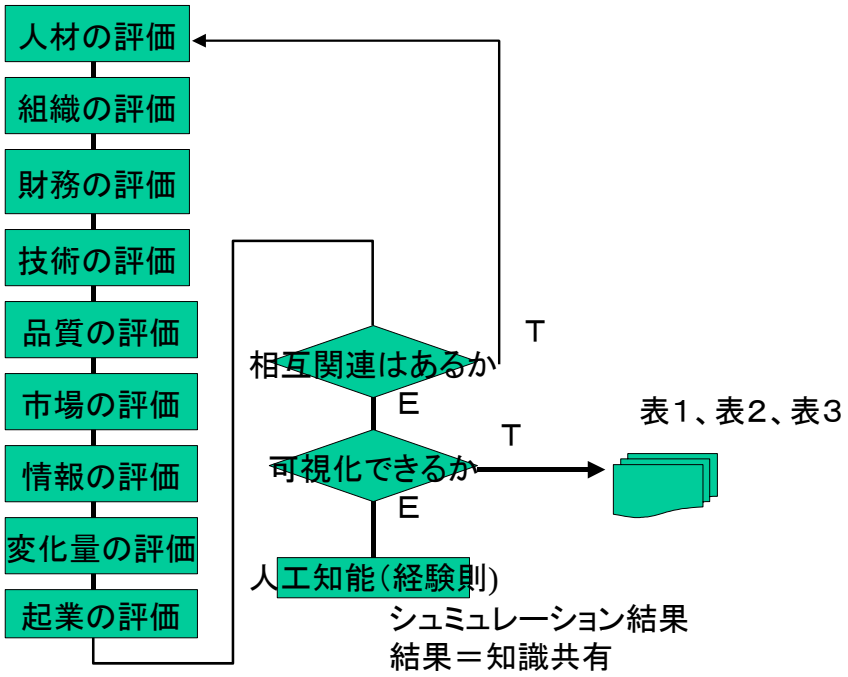
分析機能と個別構成分析をIDCによって提供する方法と分析のPRM連携を,“個”が選択した機能毎企業価値評価を構築してIDCとして提供する方法の分析が

1. IDCのデーターによって,必要とする分析の連携機能を”個”の識別に従ってデーターIDC分析
2. 分析機能の選択契約に”個”の識別によってPRMのカスタム構成を可能にする”個”のインターフェイスを備えたIDCを提供する.



経営管理IDCはインターネットサイトの1つの構成要素であり，これに対して”個”のは例えば”個”の所要のPRM連携機能によって特定のPRMを構成する．

一般的にIDCはより大きなインターネットサイトのサブセットである．経営管理IDCでは”個”の評価すべき分析機能を選択する事ができる．特定の分析機能を選択する際に，”個”のが特定の分析機能に対する分析機能情報に向かい，その分析機能を企業価値評価を構築し，企業価値評価を構築した分析機能の機能を問い合わせ，その分析機能を分析定義設定し，ここに説明している様な他のアクションを取る事ができる能力を経営管理IDCは”個”の管理分析に提供する．”個”による特定種類の分析の選択，”個”が企業価値評価を構築した分析を分析定義設定ができた場合，IDCアプリケーションが制御する機能に向けられる．



”個”の構成マシーンすなわち”個”の構成PRMを作る際に使用する経営管理IDCの構成を以下に説明する．

このIDC”個”のインターフェイスが含まれており，このインターフェイスはインターネッと通してPRMを分析構成し，その機能を問い合わせ，それを分析定義設定完了できる利点を持っ

ている. 個別の評価要素関係付け機能には, ”個”の固有の経営評価分析構築画面, 評価単位”個”の評価要素関係付け機能, 分析管理及び評価要素が含まれている. この評価要素は”個”の固有の経営評価分析構築画面, 評価単位”個”の評価要素関係付け機能, 及び分析管理に情報を提供する. “個”の固有の経営評価分析構築画面には, 機能モジュール, 機能ガイド, 計数調整モジュール, 妥当性(または相対性)警告モジュール, 及び分析最適化モジュールが含まれている.

“個”の固有の経営評価分析データーの様々なモジュールは, 以下で更に詳細に説明する様に評価要素からのデーターにより駆動する.

経営管理IDCには, ”個”の固有の経営評価分析構築画面, 評価単位”個”の評価要素関係付け機能及び分析管理用のスマートプロセスが含まれており, これらは全て評価要素により駆動される. 従来のIDCの”個”の固有の分析構築情報画面は”個”に対してPRM分析のIDC設計開始画面から選択した分析を提示し, 全ての利用可能なPRM連携機能を含んでいる. 本発明の経営管理IDCの”個”の固有の経営評価分析は評価単位”個”の評価要素関係付け機能及び分析管理にも追加され, したがって, ”個”の固有の経営評価分析の評価単位”個”の評価要素関係付け機能と分析管理に追加されている. 本質的に”個”の固有の経営評価分析構築画面全体が評価要素により駆動される. “個”の固有の経営評価分析構築画面, 評価単位”個”の評価要素関係付け機能及び分析管理はそれぞれ提供分析選択機能の一部であり, 評価要素により駆動される.

例えば以下で更に説明する様, 評価単位”個”の評価要素関係付け機能に関して, IDCの”個”により評価単位”個”の評価要素関係付け機能中に構成され配置した特定分析と結合される付加的な分析最適化情報を提供する事できる.

”個”はインターネットを通し, コンピュータ装置を使用して経営管理IDCにアクセスする事ができる. 本発明のIDCプリケーション及び分析は, 機能選択モジュール, 機能モジュール, 妥当性警告モジュール, 稼動遅延表示モジュール, 分析最適化モジュールを含むIDCプリケー

ションを提供する．更に分析最適化モジュールはメッセージを提供するが，このメッセージは，特定の構成において選択すべき推薦ＰＲＭ連携機能の分析最適化情報又はメッセージとしてもここでは言及され，例えばどのＰＲＭ連携機能が他のＰＲＭ連携機能よりも好ましいかなどが含まれている．

分析過負荷遅延又は稼動遅延表示モジュールに関して，分析過負荷遅延表示又はアイコンは，特定の選択したＰＲＭ連携機能及び／又はＰＲＭ連携機能の組合せが稼動遅延となるとの表示を”個”に提供し，遅延に対するある時間量の表示を更に含んでいてもよい．言い換えると，稼動遅延表示又はアイコンは，特定の選択ＰＲＭ連携機能又は複数のＰＲＭ連携機能が稼動遅延となる事の事前通知を”個”に提供する．この実施形態の稼動又は分析過負荷遅延表示又はアイコンは，特定のＰＲＭ連携機能を選択した結果として生じる潜在的な稼動遅延の事前又は早期表示を”個”に提供する利点を持っている．

有効な分析ＰＲＭ連携機能の”個”の選択を更に教育し又は援助する為付加的な用法も認識されている．ＰＲＭ連携機能推薦／テキストメッセージは提供ＰＲＭ評価単位分析機能評価要素中のエントリから得られる．

言い換えると，妥当性の強化は1つ又は他の理由ために1以上のＰＲＭ連携機能に相対性が無い場合にこれを”個”に知らせる．

妥当性の強化には組み込み論理が含まれており，これは”個”により組み立てられた特定の構成をチェックし，選択したＰＲＭ連携機能を特定の構成に対して同時に組み立てる事できるか否かを示す．2つの以上のＰＲＭ連携機能に相対性が無い場合には，ここで更に詳細に説明する様1つの実施形態では，妥当性強化はＰＲＭ連携機能に相対性が無い事すメッセージを返す．

ＩＤＣは，少なくともここで説明した拡張機能の範囲内でできるだけ広く，データーベース，そ

の企業価値評価を構築，及びＩＤＣを企業価値評価を構築可能な様に様観点から示した．ＩＤＣは，ＩＤＣにより”個”のが誰であるか識別した事よってデーターベースにより駆動される．このＩＤＣ及び”個”のインターフェイスは従来のＩＤＣの欠点を解消する利点を持っている．従来のＩＤＣは，本発明のＩＤＣに関してここで説明した様に企業価値評価を構築可能では無かった．従来のＩＤＣの焦点は，“適切な機能で適切な分析機能を得る事ができるか？”であった．従来のＩＤＣにおいて分析がいったん選択されると，全ての”個”に対して分析構成は同じであった．従来のＩＤＣのバックエンドには企業価値評価を構築は無かった．更に，従来のＩＤＣにおいて”個”の固有の分析構築情報画面がしていた事には何らかの妥協もあった．

このＩＤＣ及び”個”のインターフェイスは，”個”の固有の分析構築情報画面から分析構成まで，提供ＰＲＭ評価単位の拡張した企業価値評価を構築の観点を持っている．本発明のＩＤＣ及び”個”のインターフェイスは，サービスとして”個”の固有の分析構築情報画面が伝える事ができるもの，拡張機能セットとして”個”の固有の分析構築情報画面が伝える事ができるものに更に改善による機能ＵＰを加えた．全体的に見て，この方法及び装置は改善による機能ＵＰしたＩＤＣを提供する．ＩＤＣには，特定の分析機能の選択契約に対する所定のビューを発生させる単一のＩＤＣが含まれており，これは”個”の毎更に企業価値評価を構築する事できる．

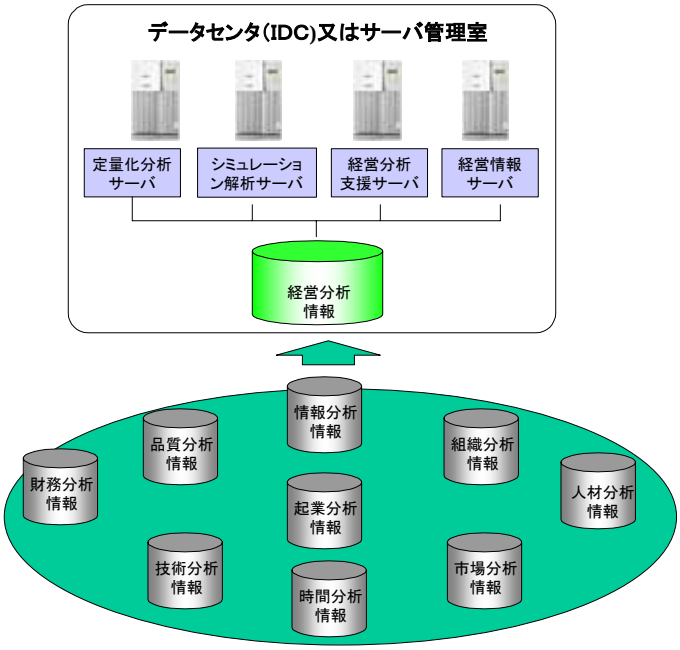
しかしながら，ＩＤＣは多くの異なる”個”に対して多くの異なる提供ＰＲＭ評価単位の様相を持っている．しかしながら本質的に同じコアのＩＤＣであり，各”個”に対して企業価値評価を構築可能であり，更にデーターベースにより駆動される．

したがってＩＤＣの企業価値評価を構築は，ここで説明した様な追加した拡張機能に関連して改善による機能ＵＰした利点を持っている．

3．3　M&Aの次世代評価手法(新手法)

分析機能と個別構成分析をIDCによって提供する方法及び装置

評価毎位の機能別(IP)及び分析のPRM連携機能を，顧客が選択した機能毎に企業価値評価を構築してIDCとして提供する方法と装置



この実施形態に関して，経営管理IDCはインターネットサイトの1つの構成要素であり，これに対して”個”のは例えば”個”の所要のPRM連携機能によって特定のPRMを構成しようとする．

一般的にIDCはより大きなインターネットサイトのサブセットである．

経営管理IDCでは”個”の分析機能を選択する事ができる．

特定の分析機能を選択する際に，”個”のが特定の分析機能に対する分析機能情報に向かい，分析機能を企業価値評価を構築し，企業価値評価を構築した分析機能の機能を問い

合わせ，その分析機能を分析定義設定し，ここに説明している様な他のアクションを取る事ができる能力を経営管理IDCは”個”に提供する．

”個”の構成マシーンすなわち”個”の構成PRMを作る際に使用する経営管理IDCの構成を以下に説明する．ここで説明している様プログラミングコード及び機能は技術的によく知られているプログラミング技術を使用して実現する事できる．

評価要素により駆動される”個”の固有の経営評価分析構築画面の観点が図示されている．例えば以下で更に説明する様，評価単位”個”の評価要素関係付け機能に関して，IDCの”個”により評価単位”個”の評価要素関係付け機能中に構成され配置した特定分析と結合される付加的な分析最適化情報を提供する事できる．

”個”のはインターネットを通し，経営管理IDCにアクセスする事ができる．分析最適化推薦モジュールにより経営分析最適化が分析最適化メッセージを提供できる様になる．分析最適化推薦モジュールは情報タイプ伝達モジュールであり，IDCアプリケーションに伝達する．カスタムPRMの構成中に”個”によりなされる特定の選択に応答して，分析最適化推薦モジュールにより特定のメッセージが呼び出される．したがって，IDCプリケーションは分析最適化メッセージと共に，メッセージを含む事ができる．

経営管理IDCは，”個”による組み立てられた構成の妥当性を評価するモジュールを更に含む．

妥当性（または相対性）警告モジュール34は，特定の分析に対して選択したPRM連携機能が正しく無い場合が発生した事示す妥当性メッセージを”個”に提供する．

特定の分析に対して選択したPRM連携機能が構成した分析の稼動に悪影響を与える場合には警告メッセージが発行され，”個”のがそれによってPRM連携機能を修正できる様なる．

妥当性の強化には組み込み論理が含まれており，これは”個”により組み立てられた特定の構成をチェックし，選択したPRM連携機能を特定の構成に対して同時に組み立てる事できるか否かを示す．2つの以上のPRM連携機能に相対性が無い場合には，ここで更に詳細に説明

する様1つの実施形態では，妥当性強化はＰＲＭ連携機能に相対性が無い事すメッセージを返す．

計数調整モジュールと異なり，ＰＲＭ連携機能相対性警告は可能性ある非相対性を説明するテキストメッセージを伴う．提供ＰＲＭ評価単位分析機能評価要素中の警告テキストのエントリを通して，他の分析ＰＲＭ連携機能と潜在的に相対性を持たないものとしてＰＲＭ連携機能は人手で識別される．他には，特定のＰＲＭ連携機能が第2のＰＲＭ連携機能の選択を必要とするので，追加ＰＲＭ連携機能を選択しなければならず，選択しなければ分析は組み立てる事できず，不確定な稼動遅延となる．

“個”の組立て分析の妥当性は経営管理ＩＤＣの一部における”個”の分析定義設定完了の応諾しないこれらの分析定義設定完了は，以前に達成可能であったものよりもかなり低いパーセンテージに下がる様有効に処理される．この実施形態に関して，2つのタイプの妥当性が意図されている．

積極的な妥当性は構成のＰＲＭ連携機能の積極的なクロスチェックであり，問題が検出した時には問題の発生を示す．更に，ＰＲＭ連携機能との特定の非相対性を示すメッセージを表示する事ができる．分析管理には，評事単位”個”の評価要素関係付け機能と”個”の固有の経営評価分析構築画面との間の企業価値評価を構築レベルを持つ経営管理ＩＤＣの企業価値評価を構築可能な部分を含んでいる．これらの特別な”個”の一人では決してないとして”個”のを認識する様経営管理ＩＤＣはセットアップされていない．以前の同様な分析では，”個”には全て一体となったフォームが提示され，複数の入力，情報，及び複数の履歴ＰＲＭ連携機能に対するテキストメッセージがある全て一体となったフォームを完成させなければならず，これは”個”のを更に混乱させる傾向があった．

全て一体となったフォームでは，テキストメッセージやフォームに書き入れる為インストラクションの応諾などにより”個”のはすぐに混乱する様なる．

“個”のが入っている提供PRM評価単位を知る事により，経営管理IDCはその提供PRM評価単位に適切な分析管理を提示する．”個データービジネスIDCに入っている場合，分析管理はパーソナル利用PRM連携機能プランやパーソナル利用データー入力を表示したり提示したりせず，ビジネス利用情報を提示したり，ビジネス利用入力を要求する．したがって，分析管理は，”個”のが入っている特定の提供PRM評価単位に関連している情報及び要求される入力のみを提示する利点を持っている．“個”のが家庭／パーソナル利用為めのPRMを分析定義設定する家庭の消費者である為経営管理IDCが決定した場合には，分析管理は，家庭／パーソナル利用の為のPRMを分析定義設定する家庭の消費者に無関係な情報を提示するのを避ける利点を持っている．“個”のが入っている特定の提供PRM評価単位に直接関係していない全ての履歴PRM連携機能は，所定の”個”に提示しない．この開示にしたがった分析構成拡張機能は関係の無い分析構成PRM連携機能，すなわち特定の”個”の又は分析機能の選択契約に関係の無いPRM連携機能を全てクローズする．

分析構成に関して，従来のIDCに対して新しい提供PRM評価単位を作る際に分析構成を企業価値評価を構築する必要がある度に，新しいオブジェクト又は分析構成ページを作る必要があった．分析管理はデーターベースにより駆動される．すなわち，経営管理IDCに他の分析機能の選択契約追加すべき必要がある場合には，新しい分析機能の選択契約が以前規定した”個”の分析構成とどの様に異なるかを規定する共通の構成要素が規定される事より，アプリケーションが分析機能の選択契約の分析管理をすぐに作る事ができ，開発者は巻き込まれない．企業価値評価を構築可能な分析管理を発生させて多くの”個”にズに合わせる為ツールセットが提供される．

更に分析構成に関して，この経営管理IDCの分析管理には，従来のIDCの1つのサイズが全てに適合する分析構成と対照的に企業価値評価を構築可能な拡張機能が含まれている．

例えば，分析管理に対して，家庭の分析定義設定者は何らかのビジネス利用情報や入力に対して認識したり，これを受けたりする必要は無い．

この様なビジネス利用情報又は入力は，家庭の分析定義設定者に阻害要因として作用し，家庭のオンライン分析定義設定者の家庭分析定義設定経験を損なう．一般的に家庭のオンライン分析定義設定者はビジネス利用の用語や条件を読み通したく無い．所定の分析機能の選択契約に対して阻害要因として作用すると考えられるものが，特定分析機能の選択契約の経営管理IDCから有効に取り除かれる．

稼動PRM連携機能及び履歴PRM連携機能も企業価値評価を構築可能である．基礎を成す原理の1つは，ビジネス対パーソナル提供PRM評価単位の識別である．

提供PRM評価単位はビジネス用（すなわちビジネス”個”の専用）又はパーソナル用（パーソナル”個”の専用）として識別する事ができる．この方法では，分析管理を企業価値評価を構築する能力が組み込まれているので，分析管理は，恐らくどこでも，選択した分析機能の選択契約から，分析管理の”個”のスペクトに無関係なものを取り除く方法を識別する事ができる．

同様にまた更に重要な事，分析管理はパーソナル”個”に対して避ける．経営管理IDCの分析管理はパーソナル”個”に会社名を聞かず，したがって，この様になっていなければ正しい分析構成フォームを完成させていないと思うかもしれない”個”の混乱を避ける事ができる．

この経営管理IDCは”個”の分析定義設定完了がオンラインでされる事より獲得される効率を維持する利点を持っている．

パーソナル対ビジネス間の混乱に対する可能性が存在している場合には，経営管理IDCはこの様な何らかの混乱を最小にする為企業価値評価を構築を含む利点を持っている．すなわち，経営管理IDCは”個”の特にパーソナル”個”のを混乱させるものを避ける事できる．例えば，所定の分析機能の選択契約によって，履歴PRM連携機能，稼動PRM連携機能，オンラインフォームを完成させる際のインストラクション用の”個”のへのメッセージが企業価値評価を構築に組み込む．

経営管理IDCの他の構成要素には，ビジネス”個”に対して，どのタイプのビジネスに”個”のが入っているかについての質問が含まれているので，更に援助が必要とされる時に，オンライン分析定義設定に続いて，”個”のは適切なハンドリングセールス力に適切にルーティングされる．

パーソナル”個”のは，どのタイプのビジネスに”個”のが入っているかを聞くページに出会う必要は無い．

分析管理毎評価要素中に規定されているものは，分析管理の企業価値評価を構築可能な構成要素の一部である．この構成要素には，IDC提供者のどの部署を分析管理に対して提供できるかを含んでいる．経営管理IDCがビジネス”個”に自己を規定してもらう為方法として，従業者の規模の指定を使用する事できる．経営管理IDCには，所定の提供PRM評価単位に対して許容可能なPRM連携機能としてこれらの3つのビジネスタイプ／規模がそれぞれ規定されているビジネス提供PRM評価単位を作る能力が含まれている．

この経営管理IDCは，特定の”個”のが誰であるか識別（例えばどの分析機能の選択契約に入っているか）すると，経営管理IDCは無関係のPRM連携機能及び部署を取り出し，その”個”の用のPRM連携機能として”個”に対してそれらを提示しない．経営管理IDCが誰であるかを知っている”個”に対して有効なPRM連携機能のみを有するものとして，所定の”個”に対する分析管理が規定される．この選択は，連邦政府の”個”に対する分析管理から有効に取り出される．すなわち，所定の分析管理が1つの有効な部署のみを持つとして規定されている場合には，”個”のが分析構成を始める時に1つの部署は部署の選択を表示しない様IDC及び提供分析選択機能用のコードが書かれる．複数の部署がある場合にのみ，選択が分析管理において表示される．すなわちこれが，この開示によってこの経営管理IDCに組み込まれる企業価値評価を構築した分析管理の1つの観点である．

所定の”個”に関連しない情報（すなわち，その情報がその所定の”個”にとって意味を成さない）は，”個”のが誰であるかについての経営管理IDCの理解に基づいて，その”個”には提

示しない. 言い換えると, ”個”のが誰であるかについての経営管理IDCの理解に基づいて, これは”個”に対して意味を成さず, 混乱や, あるいは時間や不便さをもたらすだけである事が分かる.

したがって経営管理IDCは, 各分析機能の選択契約に対して, 分析管理を可能な限り企業価値評価を構築可能な様にする組み込み能力を持っている.

特定の分析機能の選択契約に属している”個”のが識別されると, ”個”のは所定の”個”に特有な提供PRM評価単位を獲得する.

分析機能の選択契約は特定の会社, 組織又は個人に関係しており, したがって多くの分析機能の選択契約がある. 提供PRM評価単位の差異の一部は, 経営管理IDCのどの部分を”個”のが見始めるかを”個”の固有の経営評価分析構築画面が決定する事である. PRM分析のIDC提供PRM評価単位が”個”に見せるのはどの分析機能であるかを規定する. “個”の固有の経営評価分析構築画面は, 所定の分析内において”個”のが見る事できるのがどのPRM連携機能であるかを決定し, 分析最適化PRM連携機能, 許容されているPRM連携機能などを決定する.

経営管理IDCに到達する為どのリンクを”個”のが実行したかによって, ”個”のは特定の分析機能の選択契約に入っているものとして識別される. すなわち, ”個”のが入っているのがどの分析機能の選択契約であるかを経営管理IDCに知らせる埋め込み識別子がリンクに含まれている. 最初のページは特定タイプの分析機能の選択契約の例であり, 割引機能は秘密のものであり, 情報はパスワード保護されている. 提供PRM評価単位へのリンクを持つページはパスワード保護されている. 各所定の”個”の分析機能の選択契約を識別すると, 経営管理IDCは所定の”個”の分析機能の選択契約に基づいて動作する. したがって, 各分析機能の選択契約に対する経営管理IDCの表示は全て異なる.

“個”の固有の経営評価分析構築画面中の計数調整モジュールに関して, 経営管理IDC中にPRM連携機能を設定し, 所定の分析機能の選択契約に対する計数調整モジュールを起動

する．分析最適化は経営管理IDCの他の拡張機能である．経営管理IDCの分析最適化はより高価なPRMを”個”に提供する可能性を提供する．これは，分析最適化メッセージが経営管理IDCに組み込まれている場合である．

IDCのIDC提供における分析最適化メッセージの存在は改善による機能UPである．経営管理IDCに対するIDCのIDC提供は”個”の固有の経営評価分析構築画面と評価単位”個”の評価要素関係付け機能を含んでいる．

このIDCには，”個”の固有の分析構築情報画面と評価単位”個”の別構築分析に追加されている拡張機能セットが有効に含まれている．このIDCは，信頼性，性能，保守の観点から有効にアップグレードされている．更に，このIDCには可能な限り強くする改善による機能UPが含まれている．最後に，先に説明した様分析最適化は企業価値評価を構築可能である．

分析構成には，従来のIDCの1つのサイズが全てに適合する分析構成とは対照的に企業価値評価を構築可能な拡張機能も含まれている．このIDCは，全ての分析機能の選択契約に対して企業価値評価を構築可能な”個”の提供PRM評価単位となる様拡張されている．

“個”の固有の分析構築情報画面には4つの新しい拡張機能，すなわち標準的な提供PRM評価単位の表示に対する追加構成要素が含まれている．評価単位”個”の別構築分析には新しい拡張機能が含まれている．分析構成は新しい企業価値評価を構築拡張機能を備えている．

IDCの各バージョンには，所定の分析機能の選択契約に対して必要な様この様ものを変更させる能力（例えば分析過負荷フラグ）が含まれている．したがってこの追加構成要素は所定の分析機能の選択契約毎提供PRM評価単位により全て企業価値評価を構築可能である．

端から端まで，IDC経験が有効に改善による機能UPされる．IDCは，少なくともここで説明した拡張機能の範囲内でできるだけ広く，データーベース，その企業価値評価を構築，及びIDCを企業価値評価を構築可能な様にする観点から示した．IDCは，IDCにより”個”のが誰

であるか識別した事よってデーターベースにより駆動される．このＩＤＣ及び”個”のインターフェイスは従来のＩＤＣの欠点を解消する利点を持っている．

3．4　次世代の経営システム

企業などの価値評価は，財務を中心としたシステム又は，分析システムであった．また評価についても，コンサルタント企業や格付企業や銀行やリース企業が行うなど，将来業績予測として回帰分析などの統計的方法を用いて，財務的な面が中心に分析し評価していた．

しかし，これから起業する企業（例えば社内プロジェクトレベル）での企業評価の評価方法をそのまま一般の企業やグループ企業（例えば多国籍企業レベル）に適用できないという欠点があった．

また，経営分析の手法もまた旧態依然のままで，財務会計が中心の域を出ておらず，基本でき経営の資源自体の評価が全くできていない．

事業主や株主が，新規事業・ベンチャー・研究開発投資・Ｍ＆Ａなどの，不確実性の高いビジネスプランなどに対し，戦略的経営判断と投資を可能にする，本来の成長分析を行うべきである．事業の価値評価ができない為に，不確実性が極めて高いビジネスになっている．

しかしこれらは本来，手作業による各分野の関連の発見，多量データーの分析など経験と勘とに頼る必要がある．この様な欠点を解決するＩＴ技術を駆使する事，可能になる可視化技術とモデリング方法による，企業評価システム及びプロセスを提供する．

1）価値評価の相関モデル

企業の価値評価を，コンピュータシステムで企業の経営資源全体を統合した視点で行う事より解決する．相関モデル（多資源相関に時間軸を加える次元ベクトルの企業・事業価値の評

価)は, 新たな変化の増減量をデジタルで捉え. また, 人工知能により評価する知的財産で, リスクやリターンを定量的に評価し, 計数理論を数値化と可視化, 更にシミュレーションの先行計数予測で明確化させる.

この相関モデルによる分析手法などにより, 価値を予測する「可視化手段」と, 可視化と人工知能による評価技術でリスクやリターンを定量的に経営評価の改善方法を導き出す「経営分析支援手段」と, シミュレーション機能により, デジタルな経営評価による「先行計数予測手段」を備えたシステムを構成する.

これら三つの手段は, 随時, 学習用データ(種々の企業変数や地域データなど)を入力して学習を行う事より種々の条件や種々の変数に対応できる様に構成して格納する.

そして, 評価対象とする企業の関連データーと動態評価情報の8つの評価資源単位(人材・財務・知的財産・情報・市場・戦略・組織・時間)で構成する特徴を持ち, 全てがお互いに関連性を持つ為, フルメッシュで関係付けが行われる. その相関させる要因は, 事業目標, 戦略, プロジェクトマネージメント, 是正と再構築である. 所望の価値評価や変化量の予測などを出力する事できる. つまり, 以下の4つの機能が個人毎に使い易い形でサービス提供する事必要である

- 企業活動の資源を中心にした8つのデーターベースからなる構造を持ち, 相関関係値によって企業活動の分析と知識データーベースを活用する人工知能などの推論エンジンによりアドバイスを行う. また, 時間軸などの変化の絶対値から正ベクトルの値を持つ尖度の算出により, 経営の正確な傾向を把握する事できる経営マネージメントシステム.
- IDCのデーターによって, 必要とするシステムの連携機能をユーザーの識別に従って提供できるASP方式のシステム.
- システム機能の選択契約にユーザーの識別によってERMのカスタム構成を可能にする. また, そのユーザーインターフェイスを備えたASPシステム.

- IDCが効率的に顧客要求するシステム機能について，ERMシステムのメンテナンスを容易にする為のシステム構成を持つASPシステム.

この様なシステムを用いる事より，客観的で正確な企業評価を自動的に行うと共に，これから起業するビジネスプランや，大企業のいずれの企業評価も的確に実行する事可能になる.

2) 通信システム機能(論注20)

IDCに不可欠な超高速フォトニック・ネットワークの実現を図る為幹線系，アクセス系及びノード系の各要素技術を光領域で高品質・効率的に行う技術が必要とした.

旧来，構内ネット網でしか構想もできなかったMEGA容量の通信容量から，複数GIGA容量の通信プロトコルに対応する，新たな通信専用制御システムは本構想の実現については必須である. メタル通信からオプティカル通信への対応による多重ルーティングを行う機能と，セキュアなIDCの構築とセキュリティーを整え，不特定多数に対応させる，IDC専用通信システムを考案した. 実際の適用するインターネットゾーンにあるシステムとの高速かつ大量データー連携の実現の為，インターネットゾーンとの直結のファイアウォールと一体になった通信専用制御システムの下記機能を必要要件とした.

(a) ネットワーク不正利用防止装置

インターネットTCP／IPプロトコルで，相互が定めた内部用(通信装置間専用でマッピング)IPアドレスの同期を取りながら変換する装置を組み込む事で，汎用機器環境でも利用者を限定する.

論注20 平沼赳夫経済産業大臣，第1種包括役務取引(情報処理技術)の許可.
中川喜博研究内容による，(BIT－U－GL－02－100003，BIT－U－GL－02－100004)
審査許可請求:光伝送通信技術及び光ルーティング技術と交換
【米国スタンフォード大学へ最先端技術の輸出】
申請者:(2002年12月24日 富士通株式会社)
申請者:(2003年1月8日 橋本大二郎高知工科大学理事長)

(b) ネットワーク負荷削減装置

インターネットTCP／IPプロトコルで，種別と容量と優先によって専用フィールドに変換する装置を組み込む事，ルータの負荷削減と効率を図る事できる．また，通信データー種別によるパケットサイズ最適化を行う事帯域の効率的な使用ができる．

(c) 通信幹線の自動最適化システム

TCP／IPプロトコルで，幹線の入り口において通信種別に応じたスプール（buffering機能）を持たせて送受信する事より幹線の通信混雑（輻輳）を緩和させる効果により，負荷削減とスループットの効率化を図る．

(d) IPV6のユーザー認証通信システム

インターネットTCP／IPプロトコルのIPV6に，ユーザー認証サーバーより認証コードを受取，認証パラメータを通信フレームに組み込む事成り済ましの防止ができる．

(e) ルーティング情報管理システム

ユーザ拠点～通信制御装置間を，一つのIDCルーティング通信制御装置にまとめ，管理対象の全ての拠点間を接続するルーティング情報の最適化と経路についてのセキュリティーを動的に管理する．また，上位で管理する仮想ルータ機能を持つ．

(f) ルーティングのセキュリティーシステム

従来のゲートウェイ，ルーティング情報は公開用として，そのテーブルに対応する独自のセキュリティネットワークテーブルを設ける事より，容易な進入を防ぎ，ネットワーク外部からの不適切なアクセスは隣接を含め動的にもルーティング情報を更新させない．

(g) IDC専用拡張ヘッダーによる通信システム

インターネットTCP／IPプロトコルで，新たなIDC専用の拡張ヘッダを定義してセキュリティー，過負荷の帯域保証性能，IDC相互認証連携の3つの機能を備える事より，極度の集中が予想されるIDCなどに対応する．

(h) 限定範囲にて個人認証局の許可した通信システム

インターネットTCP／IPプロトコルIPV6に，ユーザー認証サーバーより認証コードを受取，認証パラメータを組み込む．認証の組み込みの無いパケットは破棄される．

(i) 限定範囲にて組織及び個人認証局の許可したルーティングを管理する装置

管理対象ドメイン間において，ルーティングテーブルの管理を，認証局を通じて認証コードを付加してセキュリティー動作を保証する．又は，認証局自体に管理させて，緊急時など動的変更などの必要が発生した場合，セキュリティレベルに応じてルーティング情報の変更や透過パケットを定義する．

(j) 障害発生源を探査する探査パケットと通過情報を収集と送信するネットワーク装置

ゲートウェイ又はルータの前にIDC（親），ユーザ（子）の通信制御装置を組み込み，独自に定義した探査パケットを通過する毎に，LOGと資源情報などを送信元に送付する．

(k) 発信元を特定させる追跡パケットと戻り情報の収集と送信するネットワーク装置

発信元不明や，誤りなどを調査する為追跡パケットを送信できる構造を持ち，通過する探査パケット情報の戻り情報についてのレポートを管理側に通過する監視装置から直接に収集元に，送信する事最終の収集可能先までの状態を把握し，発信源を特定する事できる．

3．5 結論

“個”を中心とした企業価値評価と企業分析において重要な事は「業績に結びつく行動」は，“個”によってあるいは立場によって“個”ごとに異なる点にある．

前節で確立した評価理論を経営分析のツールとして，企業評価や価値評価分析の部分を除く一部は個人の評価コンピテンシマネージメントに通ずると考える．（一般に，コンピテンシマ

ネージメントは「高い成果を上げている人に特徴的な能力」と言う.）例えば, この“個”の技術に関する特徴的能力を育成によって高い成果を上げる事ができる. この“個”のコンピテンシに対して重要なコンピテンシをコア・コンピタンスという. 具体的にはビジネスの土台となる通信, 情報, デバイスあるいはシステムなどの技術である. 本論文の企業価値評価の理論はこれらのコンピテンシに対しても適用できる.

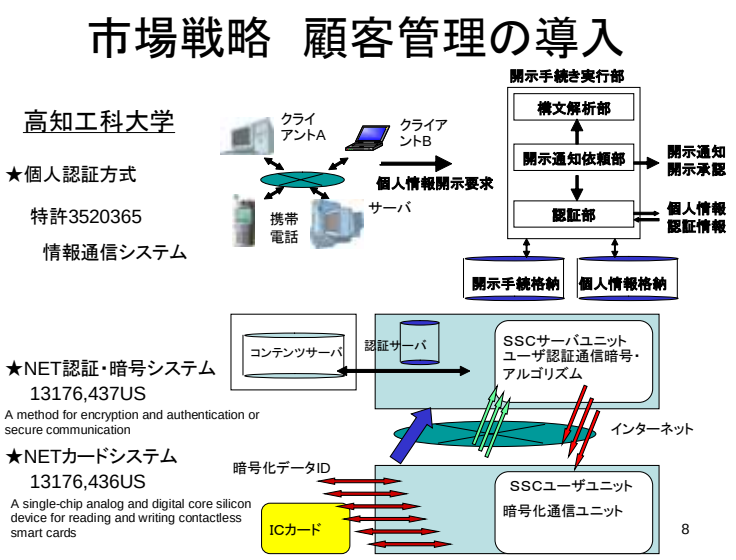
一般的な企業と事業体への国際的な範囲で適応が可能な全く新しい工学的手法に関する経営システムとして, 中期及び長期事業計画に関して, 望ましい企業と事業体の望ましい具体的な実現に向けて技術的に進化をしなければならない.

個人あるいは組織の重要な本論の企業価値評価分析方法は時間や時代と共に変化している. 毎週あるいは 四半期単位で本論文の企業価値評価方式でチェックする事が必要である.

第4章 PRMモデルの実践と検証

4．1 緒言 (論注1)

過去には，『端末認証で本人認証』とする，誤った過去の認識が研究の基本であった．その結果，携帯電話決済や銀行キャッシュカードシステムが社会的な重大問題となり，生体認証システムの導入が必然になったのは未だ記憶に新しい．この本人認証には，生体情報･所持品情報･知識情報･動態情報の様々なプライバシー情報の利用が必須になる．更に個人の高度認証や電子カルテ保存の為には大容量のデーターを利用する．そ為ため，保証するプライバシー情報と高度の管理方法による高信頼性による情報流通システムが必要になる．



更に今の課題として，近年の生体認証付銀行ICカードは，中に生体の静脈情報を保存し，持ち運びする方式を採用している．暗証番号4桁は，銀行キャッシュIDカードの中（F1F2F3F4様式）に格納して端末側で暗証番号の確認をしていたがその後，暗証番号はセンター照会に変更になった．IT技術者は，銀行キャッシュカードをIDカードリーダで読み込み，忘却した暗証番号を調べたりする事も容易に行っていた．

筆者は，この様な端末機だけの確認によるセキュリティー技術の概念では，ICカードや本人認証が一般化する将来，頭打ちであると考える．

(論注9) 4章全て 2004年11月27日 ICOA国際学会，Proposal of a new Concept on Personal Information and new Certificate Authority

プライバシー情報は毎個人毎の条毎と利用場面の条件毎の活用を前提にして，個人の意思を確認しながら，秘匿と公開する為の個々の技術が必要である．IT技術は，インターネット接続する地球上の利用者を相手にする為，ネットワークに流れる本人固有のプライバシー情報の制御を確実に行う必要があり，その為に独立したプライバシー技術の確立が必須であると考えた．このプライバシー技術は国際的にも，情報保護を主体とするセキュリティー分野から派生する研究分野として位置付けるのが一般的である．

しかし筆者は，自由な視点や技法の捉え方が，今後は困難であると考える．即ち，前者は施設･装置や暗号などによる完全秘匿を前提にするものである．これに対し後者は，漏洩などを踏まえ認証情報などのプライバシー情報の提供や委託により『必要な情報のみ活用』を前提とする．この両者の大きく異なる点は，後者は事象や個人の意思により，情報のコントロールを行う事ある．これ以外の相違については，以下の全く別の観事と視点の考察による高度な高信頼性の情報流通が必要になる．筆者はこれをプライバシー工学とした．

1) プライバシー情報の流通

情報活用を前提に秘匿するシステムは，国際的に通用する常識的なシステムポリシーが必須である．また，職員の興味での検索や漏洩，住民閲覧公開の運用ではプライバシーを守る事ができない．

本人識別情報であるプライバシー情報を集中管理する情報センター（IDC：インターネット Data Center）を活用する事，自己の重要情報を自己コントロールするシステムである．すなわち，認証するデーターの真正性を保持しつつ，匿名性を維持し認証強度により段階的な開示を可能にした．新たな高信頼

情報管理の具現化を検討した. バイオメトリクスなどの重要な個人識別情報を, 暗号化しているとはいえ入出力装置のICカードや携帯電話, PC等の移動体に格納する事, 直接や間接の情報漏洩につながる危険性がある. この対策として, 盗難・スキミング・忘却のリスクから防御するシステムが必要であると考えた. 現在, 本人の真正認証ビジネスとして, 生体認証を利用したユビキタス環境における携帯電話, PDAなどのモバイル端末や電子パスポート, 運転免許証のICカード化の本人判定装置がある. しかし, この本人判定装置に個人の生体情報を照合データーとして格納しなければならない.

また, 認証照合完了信号やワンタイムパスワードなどの端末認証の通信データストリームを流す擬態装置の存在自体が重要問題であると考える.

2) プライバシー通信システム機能

これらの社会的な課題から, 解決を具現化する為に, 費用, 機能性, 合法性の3つのバランスを考慮し, 筆者が提案するのは下記の三点である.

- プライバシー情報の一元管理化

認証できる正確な情報を集中管理する. 管理効率と修正更新による整合性を確保する.

- 割符を利用する情報分散(ワンタイム情報)

提供する情報単体では意味不明を基本とする. 情報を活用する時点で, 常に利用照会を行い, 正確な情報となる. 更にワンタイムの割符となる情報を得る事情報利用回数が一度のみに制限する.

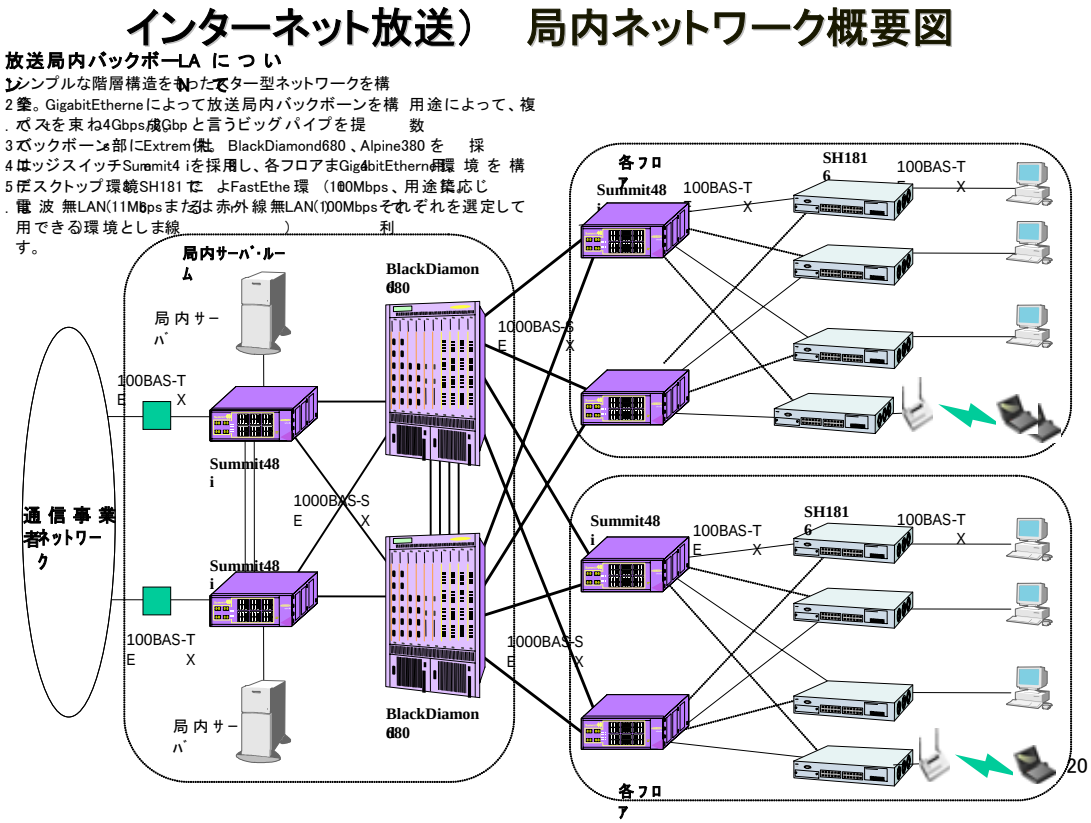
- IP／V6拡張機能の個人認証付ヘッダ

通信パケットの先頭に個人認証付の情報を付加してプライバシー通信機能を確保する. 情報プライバシーIDCに不可欠な超高速フォトニック・ネットワークの実現を図る為, 幹線系, アクセス系及びノード系の各要素技術を光領域で高品質・効率的に行う技術である.

4. 2 ビジネスへの適用(論注11, 12)

電子政府及び金融，医療情報センターの情報基盤の根幹を乗っ取る事，以外と簡単にできる．悪意ある第三者は，成り済ましや電子証明書が簡単に開設できる認証局又は，擬似ホームページを必ず利用する．そのため，個々のユーザー自身が，インターネットに対してセキュアなセキュリティー構築を行う事，運用管理作業項目の洗出し能力不足と，個人のセキュリティー理解不足の為不可能である．

現状の電子政府などは，偽認証局及び認証システム基盤を含め，他人が本人であるとして認証局に登録する事よる“成り済まし”には，全く成す術が無い．この課題の対策は，本システムにおける個人データーの中央集中化した管理アーキテクチャを開発し，機能的に動作させる事解決する事できる．個人毎のＰＣに重要なプライバシー情報を管理させるのでは無く，銀行の貸し金庫以上のセキュリティーが高い環境を低コストで，災害に強く監視体制も整備した拠点ＩＤＣを銀行の様に利用する事解決できると考える．

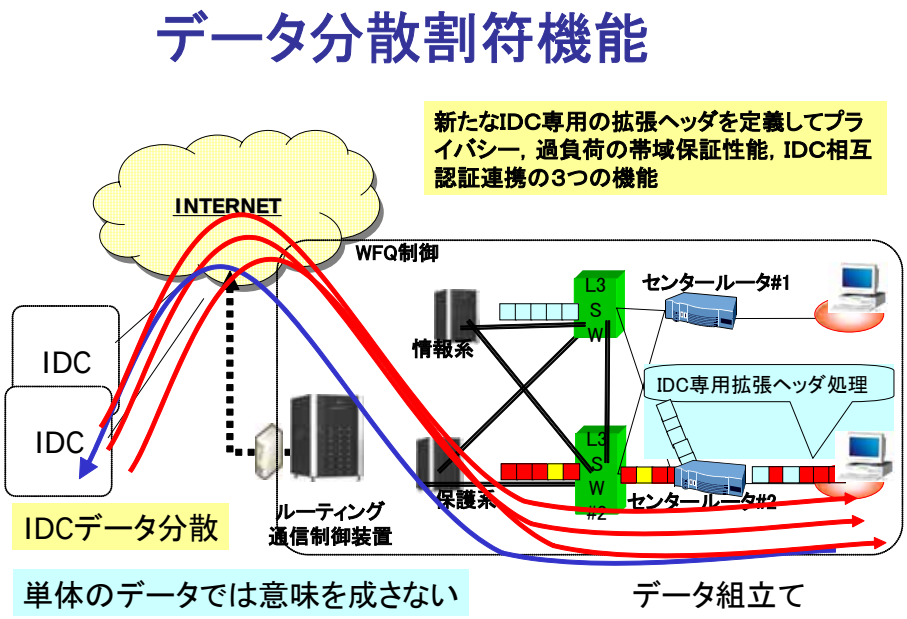


個人データーの中央集中化にあたっては，個人認証局にプライバシー情報を守る為の新

たなアーキテクチャを必要とする．個人認証局の基礎基盤は，公的認証機関としての個人データーの提供に関する機能，プライバシー情報を管理する機能とプライバシー情報の様々な提供を拒否する機能を持つ，基本アーキテクチャを開発する事可能にした．この個人が個々の情報をコントロールする事できる，アーキテクチャを前提にする全く新たなシステム基盤を提起するものである．本構想の特徴は，情報公開手順，公開方法，許可した認証の方法を登録しておけると言う点にある．

1）割符を利用する情報分散（ワンタイム情報）

旧来，構内ネット網としても構想もできなかった多拠点間を，Tera容量の光通信プロトコルに対応する新たな光通信専用制御システムは，本構想の実現では必須である．

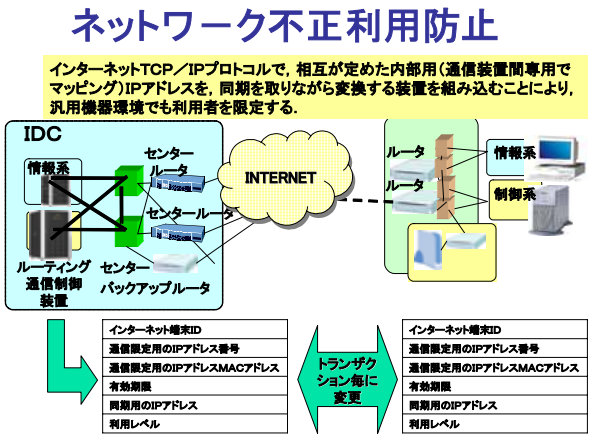


メタル通信からオプティカル通信への対応による多重ルーティングを行う機能と，セキュアなIDCの構築とセキュリティーを整え，不特定多数に対応させるIDC専用通信システムを考案した．実際の適用するインターネットゾーンにあるシステムとの高速かつ大量データー連携の実現の為に，インターネットゾーンとの直結のファイアウォールと一体になった通信専用制御シス

テムの下記機能を必要要件とする.

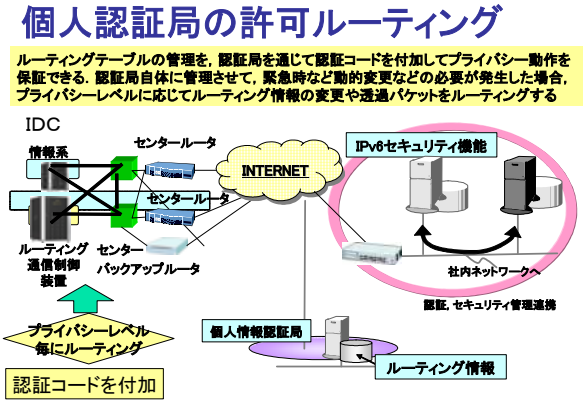
(a) ネットワーク不正利用の防止

インターネットTCP／IPプロトコルで，相互が定めた内部用（通信装置間専用でマッピング）IPアドレスを，同期を取りながら変換する装置を組み込む事より，汎用機器環境でも利用者を限定する.



(b) 組織及び個人認証局の許可ルーティング

管理対象ドメイン間において，ルーティングテーブルの管理を，認証局を通じて認証コードを付加してセキュリティー動作を保証できる．認証局自体に管理させて，緊急時など動的変更などの必要が発生した場合，セキュリティレベルに応じてルーティング情報の変更や透過パケットをルーティングする.

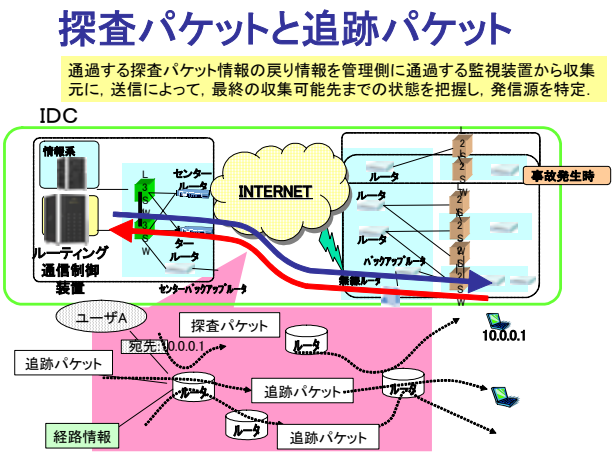


(c) 障害源の探査パケットと通過情報の収集送信

ゲートウェイ又はルータの前にIDC（親），ユーザ（子）の通信制御装置を組み込み，独自に定義した探査パケットを通過する毎に，Logと資源情報などを送信元に送付する.

(d) 発信元特定の追跡パケットと戻り情報の収集

発信元不明や，誤りなどを調査する為の追跡パケットを送信できる構造を持つ．通過する探査パケット情報の戻り情報についてのレポートを管理側に通過する監視装置から直接に収集元に，送信する事によって，最終の収集可能先までの状態を把握し，発信源を特定する事ができる．

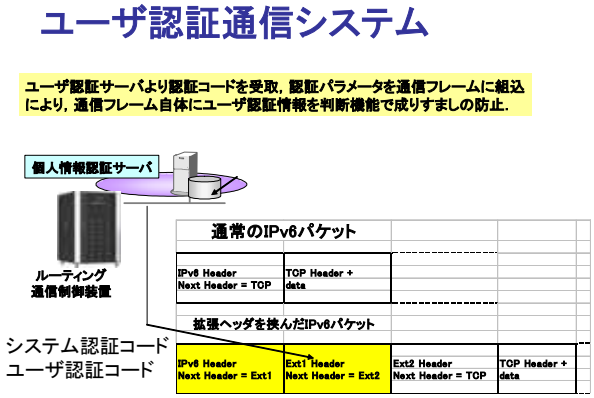


2) IP／ヘッダ張機能の個人認証付ヘッダ

プライバシー情報の認証済手続が完了した場合にIP／V6の拡張ヘッダに認証済みコードを埋め込み，受信側に受け取る．

(a) IDC専用拡張ヘッダによる通信システム

インターネットTCP／IPプロトコルで，新たなIDC専用の拡張ヘッダを定義してセキュリティー，過負荷の帯域保証性能，IDC相互認証連携の3つの機能を備える事より，極度の集中の予想するIDCなどに対応する．



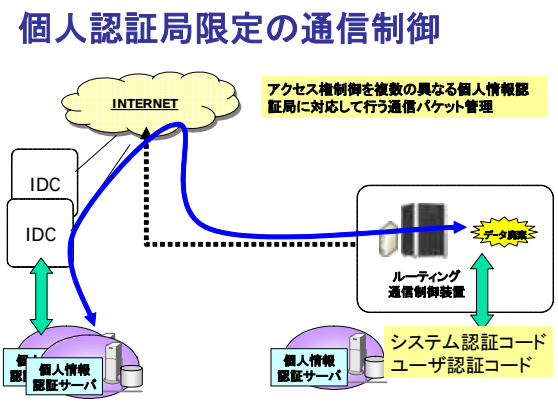
(b) IPV6のユーザー認証通信システム

インターネットTCP／IPプロトコルのIPV6に，ユーザー認証サーバーより認証コードを受取，

認証パラメータを通信フレームに組み込む事より，通信フレーム自体にユーザー認証情報を判断機能で成り済ましの防止ができる．

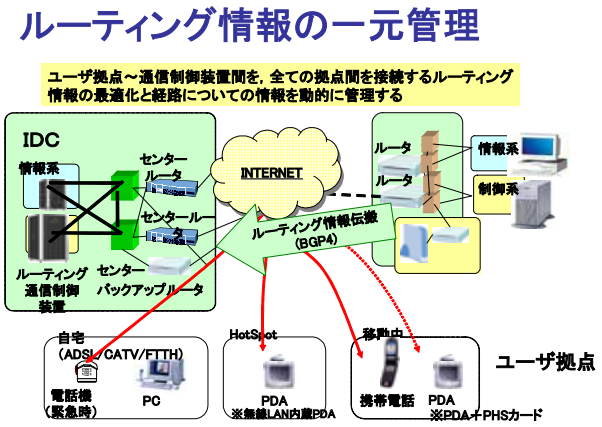
(c) 個人認証局の許可した通信システム

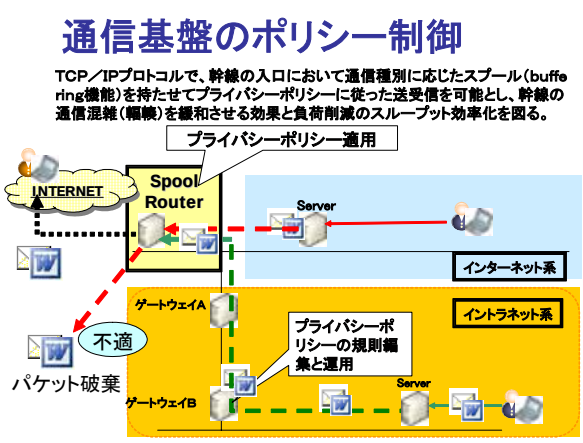
インターネットＴＣＰ／ＩＰプロトコルＩＰＶ６に，ユーザー認証サーバーより認証コードを受取，認証パラメータを組み込む．認証の組み込みの無いパケットは破棄する機能を持つ．



(d) ルーティング情報の一元管理

ユーザー拠点～通信制御装置間を，一つのＩＤＣルーティング通信制御装置にまとめ，管理対象の全ての拠点間を接続するルーティング情報の最適化と経路についての情報を動的に管理する．更に，上位で管理する仮想ルータ機能を持つ．





(e) ルーティングのプライバシー管理

従来のゲートウェイ，ルーティング情報は公開用として，そのテーブルに対応する独自のセキュリティネットワークテーブルを設ける事より，容易な進入を防ぎ，ネットワーク外部からの不適切なアクセスは隣接を含め動的にもルーティング情報を更新させない機能を持つ．

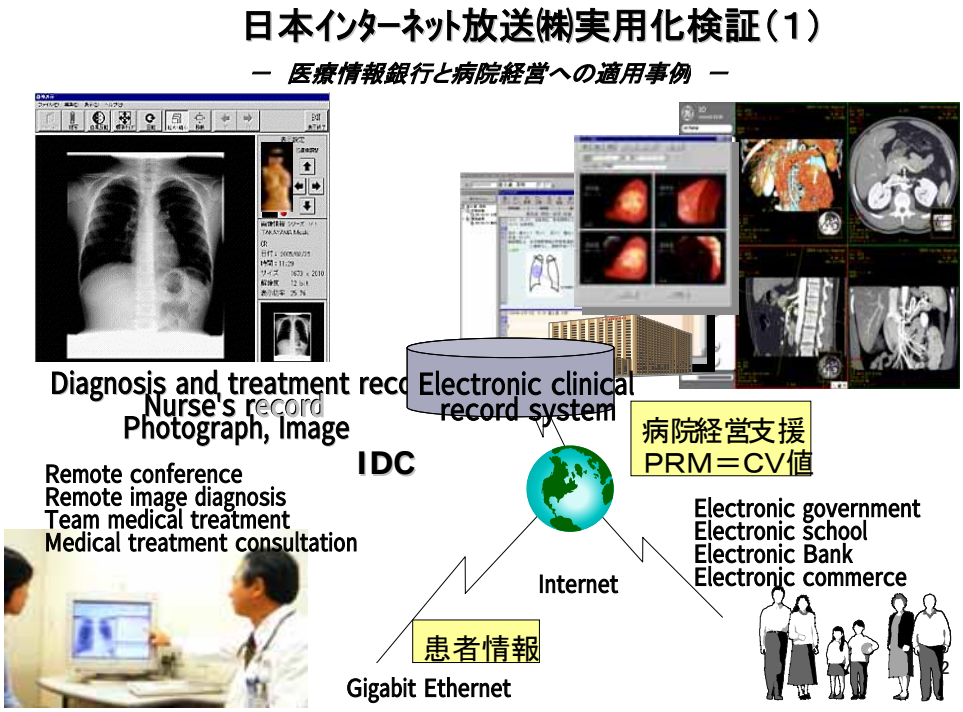
本論は，ワンタイム情報という新たな言葉を定義した．ワンタイム情報とは，利用について1度だけの限定使用が可能な情報を意味する．そのため，ネットワーク上で情報が漏洩しても，分散情報として独り歩きできず，何時までも利用する事無い．欠点はアクセスの度毎に割符を照会と同時に，ダウンロードの必要がある為トラフィックが増大する．

プライバシー工学では，プライバシー情報はパーソナル・コンピュータ単体の個別管理では無く，第三者が管理して，地域単位のＩＤＣでデーター集中化するセキュリティー管理システムの配下におく．電子政府が保有するプライバシー情報の認証を行う公的な個人認証局（ＩＤＣ）が主体である．市町村には，認証システムを安定運営する事，それに伴う責任が生じる為，（ＡＳＰ：アプリケーション　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）方式を電子政府・医療・業務の統合化整備や広域的な運営に導入する等の対応が可能なＩＤＣ運用とする．プライバシー工学は，複数の情報を元にした確実な本人認証を行う為に，プライバシー情報自体を本人による情報公開などのコントロール権を持たせて集中管理し，保護する．例えば，個人が電子政府内を含め，一切の開示を拒否する項目であれば，個人認証局からは情報提供する事，本人が亡くなった後も一切できない．

4．3　医療IDCへの応用

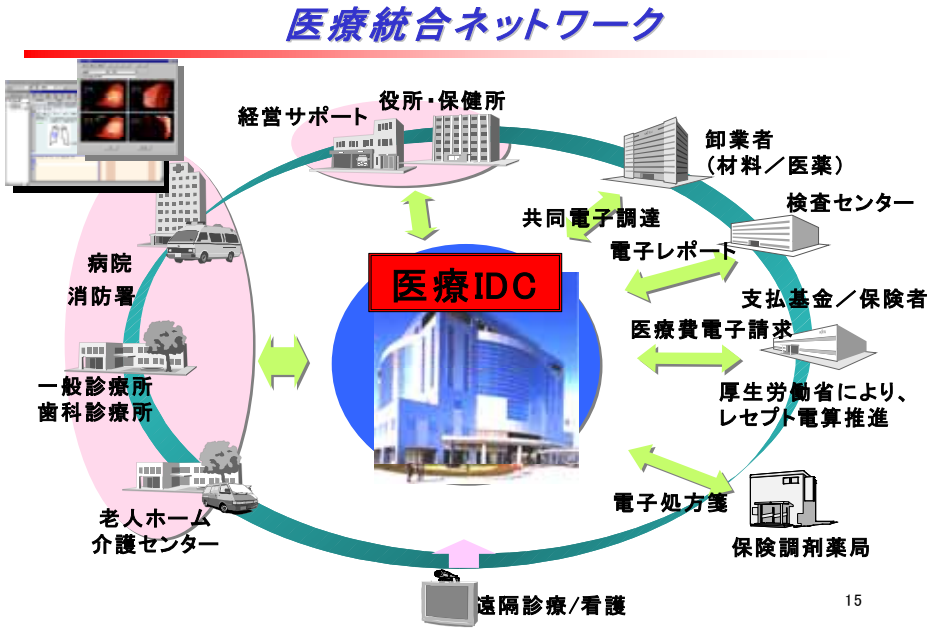
我が国の医療環境は，人口の少子高齢化と医療進歩に伴う医療費の増加に対し，様々な医療費抑制施策が講じており，各病院は医療の公共的使命，役割を果たしつつ経営改善と病院間競争に打ち勝つサービスの向上に努力を求めている．

こうした厳しい状況の中で，病院情報システムは従来の仕事の延長線での各部門業務の効率化だけでなく，情報を中心に院内の人と物と金の流れを抜本的に見直し，病院機能を飛躍的に向上させるシステムが求めている．



医療電子カルテに関しては，病院間のデーターの送受信においてのみ，インターネットの利用検討が始まっている．本構想の個人認証局は，セキュリティーを確立し，安全を確保すべく検討を開始した．特に，医療などの患者データーは最重要な個人情報とする観点から，漏洩，改竄，盗聴など，絶対にあってはならない．本構想の個人認証局の患者データーは，医療機関間のインターネット通信において『あらゆる診療関係情報（診療録，検査報告

書，検査レポート，看護記録，紹介状，診断書，画像，心電図，脳波，PET，MRI／MRA，CT等）を対象に電子化したもの』を指す．本来，治療費を支払う患者自身のもので，患者個人が検査と治療データーの管理責任を負い，データーの開示と提供のコントロールを行う事が望ましい．また，本構想の個人認証局のデーターは，患者と医師が治療に向けて情報開示とコラボレーションを行う為のものであり，医療技術向上と医師と患者のDecision making supportの為のKnowledge Managementとして活用できる．また，救急医療に関しては，移動体との通信はもとより，患者の関係者への速やかな連絡と保護者確保に至るまで，該当する個人情報は非常に重要でしかも大量に扱う事できる．



重要な情報の保護は，IDCでの集中管理が最も効率的である事を示した．しかし，電子取引のビジネスモデルとしての今のデジタル証明書及び認証技術には，偽の認証局と本人の確実な認証が不完全な問題があり，現時点の技術のまま，見切り発車する事，非常に危険である．現在，本人の真正認証は，ICカードなどの携帯移動体に個人の生体情報を照合データーとして格納しなければならない．また，バイオメトリクス照合完了済や端末認証データーの不正通信データストリームを流す偽装置への課題が重要問題と考える．

現行のシステム技術においては，個人情報の中央集中化は文化の違いにより非常に困

難を極めると予想する. 既に住民票をコード化しているスウェーデン, フィンランドの北欧とは異なり, 米国, 日本, 韓国, カナダなどは容易に個人の情報を国には預ける事はしないと予測する. よって, 保護手続による確実な手続を必要とするが, 国民が自己の情報を預ける事安心感を与える本構想の個人認証局の明確なシステムが無ければ, 電子政府への前進はあり得ない. また, 電子政府などのセキュリティポリシーやインターフェイスとしては, セキュリティー保持に必要な水準と利便性について, 各国の要求水準の決定理由を明確にするなどの, セキュリティマネジメントを行う国際的な調整機関が必要と考える.『電子政府の基礎基盤』とは, 個人情報認証基盤の事であり, 電子認証への早急な対応と解決によって, 各国が推進する電子政府の国際標準化にも必要と考える. また, 国際社会のIT革命へ向かう為に, 本構想によって解決すべき課題であると考える.

更に, インターネットの長所のみで構築したシステムは実用性が無く, 金融ビジネスなどの確実性を要求するシステムには適用できない. 本論文では, このシステム欠損を解明すると共に, IDCによって課題解決のキーとする研究により, 次世代コンピュータネットワークの基本設計による情報基盤の確立の結果と, 具体的な適用計画を目的とする.

病院の規模に関係なく, 診療所大規模病院では, アウトソーシング型になりＡＳＰで対応する. 住民本人のカルテ情報をどこでも引き出す事が可能で, 病－病連携, 病－診連携が可能となり情報の共有化が医療の質の向上を目指し, 情報開示への対応を行う. 病院毎に又は, 全ての病院が電子カルテシステムの構築を必要とせず, 容易利用を可能とする. 今後は保健･医療･福祉･介護の情報システムを地域の, 市町村への展開が必要としている.

IT, コンピュータ関連のビジネスは厚生労働省には無く, まして情報化戦略は無に等しい. 医療保険制度の改革, 患者意識の変革, 社会環境の変化等, 昨今の医療を取り巻く環境がますます厳しくなる中で, 良質な医療の効率的な提供と, 患者サービス向上の為に, 事務のIT化と経営方法の改善とが病院の重要テーマである.

会社経営の手法を医療に持込み, 医療改革を行った場合の効果について研究する. 戦

略経営管理ソリューション「SMS（Strategic Management Solution）」は，病院経営管理に関わる様々題を最新の管理手法や最先端の起業工学を用いて解決するソリューションである．経営管理に関わる収益管理，リスク管理，コスト管理が全て含まれる必要があり，評価を行う研究により，病院経営管理と医療財政に大いに貢献する．

非営利の医療，教育や，公団などの特殊法人の事業は，国の定めた枠組みに沿って事業を進めてきた．経営分析手法自体は，旧態依然のままで可視化した程度であり，効果的な医療経営の分析は行えない．

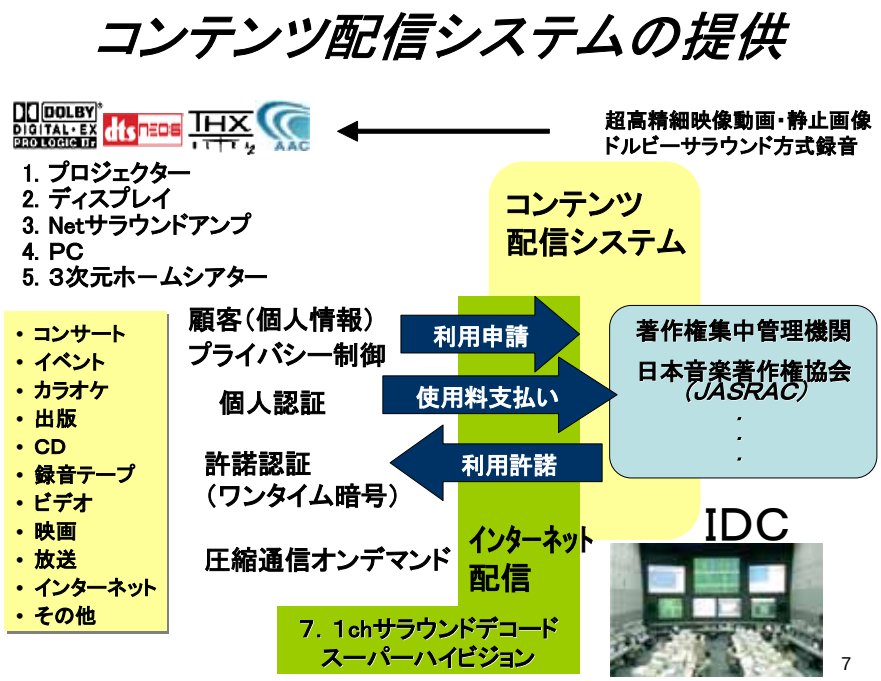
そこで，次世代の多視点による経営評価と価値評価理論の確立と実現する技法を，考案する必要がある．それは，新たな計数理論を数値化と可視化する技術であり，変化の流量を人工知能による評価，更にシュミュレーションの先行計数予測で明確化する，技術と評価経営を可能とさせる統合連携システムになるはずである．重要な点は，状況が変化する中で分析形態も変化しなければならない．変化する状況について，独立してサービス及びシステムを創造（起業家精神）させながら対応させる機能が必要である．

経営手法でデジタルに可視化する仕組みの試行と開発した評価法の組込みに相当する医療に関する新たな評価･管理法の開発を使った．　ＩＤＣで利用する病院経営のＡＳＰについて，ホスティングサービス財務会計からのバランスシートなどや，キャッシュフローだけの会計主義による経営分析システムの問題について正確な把握を行った．企業の実態の把握する事，自分の健康状態を知るのと同じである．節税とか，銀行からいかに融資を引き出すかなど，財務会計ばかりが行われてきた事が改善できる．

4．4　コンテンツ配信への応用

ＩＤＣで利用する病院経営のＡＳＰについて，ホスティングサービス財務会計からのバランスシートなどや，キャッシュフローだけの会計主義による経営分析システムの問題について正確な把握を行った．企業の実態の把握する事は，自分の健康状態を知るのと同じである．この為の会計が管理会計と言われるが，日本ではこれまで，節税とか，銀行からいかに融資を引き出すかなど，財務会計ばかりが行われてきた．つまり，企業などの価値評価は，財務を中心としたシステム又は，分析システムであった．また評価についても，コンサルタント企業や格付企業や銀行やリース企業が行うなど，将来業績予測として回帰分析などの統計的方法を用いて，財務的な面が中心に分析され評価されていた．

しかし，これから起業する企業（例えば社内プロジェクトレベル）での企業評価の評価方法をそのまま一般の企業やグループ企業（例えば多国籍企業レベル）に適用できないという欠点があった．



また，経営分析の手法もまた旧態依然のままで，財務会計が中心の域を出ておらず，基

本的な経営の資源自体の評価が全くできていない. 事業主や株主が, 新規事業･ベンチャー･研究開発投資･M＆Aなどの, 不確実性の高いビジネスプランなどに対し, 戦略的経営判断と投資を可能にする, 本来の成長分析を行うべきである. 事業の価値評価ができない為に, 不確実性が極めて高いビジネスになっている.

しかしこれらは本来, 手作業による各分野の関連の発見, 多量データーの分析など経験と勘とに頼る必要がある. この様な欠点を解決するIT技術を駆使する事で, 可能になる可視化技術とモデリング方法による, 企業評価システム及びプロセスを提供する. 企業の価値評価を, コンピュータシステムで企業の経営資源全体を統合した視点で行う事により解決する. 相関モデル（多資源相関に時間軸を加える次元ベクトルの企業･事業価値の評価）は, 新たな変化の増減量をデジタルで捉え. また, 人工知能により評価する知的財産で, リスクやリターンを定量的に評価し, 計数理論を数値化と可視化, 更にシミュレーションの先行計数予測で明確化させる.

この相関モデルによる分析手法などにより, 価値を予測する「可視化手段」と, 可視化と人工知能による評価技術でリスクやリターンを定量的に経営評価の改善方法を導き出す「経営分析支援手段」と, シミュレーション機能により, デジタルな経営評価による「先行計数予測手段」を備えたシステムを構成する.

これら3つの手段は, 随時, 学習用データ（種々の企業変数や地域データなど）を入力して学習を行う事により種々の条件や種々の変数に対応できる様に構成して格納する.

そして, 評価対象とする企業の関連データーと動態評価情報の8つの評価資源単位（人材･財務･知的財産･情報･市場･戦略･組織･時間）で構成する特徴を持ち, 全てがお互いに関連性を持つ為, フルメッシュで関係付けが行われる. その相関させる要因は, 事業目標, 戦略, プロジェクトマネージメント, 是正と再構築である. 所望の価値評価や変化量の予測などを出力する事ができる. つまり, 以下の4つの機能が個人毎に使い易い形でサービス提供する事が必要である.

① 企業活動分析方法，企業活動ＤＢ構築方法それに使用する分析シート及び企業活動管理システム

② 企業活動の資源を中心にした8つのデーターベースからなる構造を持ち，相関関係のプロット値によって企業活動の分析と知識データーベースを活用する人工知能などの推論エンジンによりアドバイスを行う．また，時間軸などの変化の絶対値から正ベクトルの値を持つ尖度の算出により，経営の正確な傾向を把握する事ができる経営マネージメントシステム．

③ システム機能とユーザー識別に従う個別構成システムとＡＳＰ提供の方法とその装置

④ ＩＤＣのデーターによって，必要とするシステムの連携機能をユーザーの識別に従って提供できるＡＳＰ方式のシステム．

⑤ 統合システムのカスタム構成を可能とする個別対応システム

⑥ システム機能の選択契約にユーザーの識別によってＥＲＭのカスタム構成を可能にする．また，そのユーザーインターフェイスを備えたＡＳＰシステム．

⑦ 統合システムのメンテナンスを容易にする個別構成システムとＡＳＰ提供の方法と装置

⑧ ＩＤＣが効率的に顧客要求するシステム機能について，ＥＲＭシステムのメンテナンスを容易にする為のシステム構成を持つＡＳＰシステム．

この様なシステムを用いる事により，客観的で正確な企業評価を自動的に行うと共に，これから起業するビジネスプランや，大企業のいずれの企業評価も的確に実行する事が可能になる．

第5章　　結 論

業績評価(過去), 保有能力評価(現在)と戦略能力評価(未来)より, 工学的な経営分析又は, 企業分析を行う手法を考案した. 8つの戦略要素のバランスを取りながら企業価値を分析しながら強力に推進できる. また本論は, ワンタイム情報という新たな言葉も定義した.

プライバシー工学では, プライバシー情報はパーソナル・コンピュータ単体の個別管理では無く, 第三者が管理して, 地域単位のIDCでデーター集中化するセキュリティー管理システムの配下におく. 電子政府が保有するプライバシー情報の認証を行う公的な個人認証局(IDC)を主体とする. 市町村には認証システムを安定運営する事と, それに伴う責任が生じる為, (ASP:Application Service Provider)方式を電子政府・医療・業務の統合化整備や広域的な企業経営に導入する等の対応が可能なIDC運用を可能にしなければならない. (15)

プライバシー工学は, 複数の情報を元にした確実な本人認証を行う為に, プライバシー情報自体を本人による情報公開などのコントロール権を持たせて集中管理し, 保護する. 例えば, 個人が電子政府内を含め, 一切の開示を拒否する項目であれば, 個人認証局からは情報提供する事は, 本人が亡くなった後も一切できない. また, 光増幅技術の目覚ましい進展や多波長光源, 分波器等の光部品の特性向上に支えられ, 新たな光通信技術として, point－to－pointの適用だけでは無く, 多重化信号処理を行うノード装置にフォトニック・ネットワークを利用するであろう. このネットワークは, 波長多重技術をベースとして, 大容量な情報伝送能力により, 神経網としての役割を担うものと期待する. 本論文では, その構成要素となる光ルータ, 光ADM, 光ノードの活用を前提にしたプライバシー情報のネットワー

---

(15) e－Japan 重点計画－2003, Ⅱ. 先導的取り組みによるIT 利活用の促進, 1. 医療, 日本国内閣「高度情報通信ネットワーク社会推進戦略本部, http:／／www. kantei. go. jp／jp／singi／it2／kettei／030808honbun. pdf

クオペレーションの概要を報告した. 個々の大容量データーを, 大規模トランザクションでプライバシー情報を保護する光統合ネットワークは, 波長多重伝送システムと光ルーティング装置や各種光デバイス技術の進展により実現化する. 経済的で発展性のあるプライバシー制御システムが完成しつつあり, 今後の幅広い発展を期待する.

また, ネット流出した情報を, 一度のみ有効とし, 以後無効にするプライバシー工学も実用できる.

最新の情報処理技術を活用し, このデーターをいかにタイムリーに検索, 抽出できるかが経営情報を把握するにあたり重要である. システムで収集した収入データーが判り易く, 活用し易い形式で本研究のデーターベース化と企業価値分析法により患者一人を単位とするプロジェクトとする管理への移行を強く求めるものである. (16)

電子政府の実現の為には, 基盤技術 (Network, セキュリティー, 電子認証, データーベース等) と共に, 電子化に対応した制度・法令等 (登記, 印鑑, 印紙等) の整備も必要となる. これら, 制度, 基盤技術, サービスが一体となって発展する事, より質の高い電子政府が実現されると考え, 技術だけでなく制度面の改革もかなりの面で必要性を感じた.

また, 個人情報認証局などのSystemにより, これからの児童生徒の個人情報は, インターネットを介して特定されずに済む一方で, インターネットを介して情報通信が可能となる.

例えば, 学校の教育現場において多数設置されたパーソナル・コンピュータを, 使用する児童により当該児童本人やその児童の周囲の保護者本人に関する情報が不測に電気通信網を介して公開されずに済み, 個人情報を極めて効果的に保護する事できるからである. これらは, 機械的にほぼ完璧に個人情報を保護する事が可能である.

---

(16) 付加価値の源泉, Hermann Simmon/Yoo,, ilHwa, , 21p-137p3章考える経営, , 洋経済新報社

しかし,「完璧」というSystemは存在しない.

絶えず技術進歩が著しい分野であるインターネット技術は, 技術進歩により常に見直しが必要である. それにも増して, この様なリスクに対する人への教育と制度が今後必要不可欠になる.

つまり, 児童生徒と教員の教育に関して, IT専任講師と教育委員会及び校内のセキュリティー管理者の育成である. これは, 情報教育教科制度における教員育成カリキュラムに情報セキュリティー分野における学士, 修士の必須教科とする必要性がある.

これらは, 今の教師と生徒の教育世代間の格差を是正し先輩後輩の循環教育を促進させる. また, これらのインターンシップ制度に採用される学生が選別される為, 将来就職活動においても, ITの基準を満たしている事暗黙に認定され, 優秀な生徒学生の雇用にも非常に有効になると考える.

本論文で記載した筆者による新構想が, 我が国法制度及び国際法制度上, 適用されるか否かは関知しない事は言うまでも無い.

参 考 文 献

(2) JISQ15001 個人情報保護に関するコンプライアンス・プログラムの要求事項Requirements for compliance program on personal information protection http://www.jisc.go.jp/app/pager?id=26738

(3)『行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律』昭和63年12月16日法律第95号平成元年10月1日施行
www.isc.meiji.ac.jp/~sumwel_h/doc/codeJ/pubdata.htm

(4)『OECD RECOMMENDATION CONCERNING AND GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA O.E.C.D. Document C(80)58(Final), October 1, 1980』www.cpsr.org/cpsr/privacy/privacy_international/international_laws/1980_oecd_privacy_guidelines.txt

(5) 情報セキュリティー総合戦略, ～世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上～, 経済産業省, 2003年10月10日, 9P－12P 63P－64P, http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_body.pdf

(6) e－Japan 重点計画－2003, Ⅱ. 先導的取り組みによるIT 利活用の促進, 1. 医療, 日本国内閣「高度情報通信ネットワーク社会推進戦略本部, http://www.kantei.go.jp/jp/singi/it2/kettei/030808honbun.pdf

(7) 特許第3520365号 2000－330949(10/30, 2000), 情報通信システム, 出願者, 高知工科大学, 発明者, 中川喜博, IPC:G06F 15/00, 日本

(8) Information Management－PKI Guidance ITS & PKI Sector, Treasury Board of Canada Secretariat, Example Risk Levels, E－Signature Type

s, and Retention Methods and Practices, March 31, 2002, http:／／www. cio－dpi. gc. ca／pki－icp／guidedocs／mngt－gestion／mngt－gestion04__e. asp#__Toc13556737

(9) 情報セキュリティー総合戦略, ～世界最高水準の「高信頼性社会」実現による経済･文化国家日本の競争力強化と総合的な安全保障向上～, 経済産業省, 2003年10月10日, 9P－12P, 63P－64P, http:／／www. meti. go. jp／policy／netsecurity／downloadfiles／Strategy__body. pdf

(10) 電子署名･認証ハンドブック【パーソナルユース編】, (財) 日本品質保証機構電子署名認証調査センター, 3P, http:／／www. jqa. jp／11it／pdf／hb__p. pdf

(11) Information Management － PKI Guidance, ITS & PKI Sector, Treasury Board of Canada Secretariat, Example Risk Levels, E－Signature Types, and Retention Methods and Practices, March 31, 2002, http:／／www. cio－dpi. gc. ca／pki－icp／guidedocs／mngt－gestion／mngt－gestion04__e. asp#__Toc13556737

(12) 特許第3520365号 2000－330949(10／30, 2000), 情報通信システム, 出願者, 高知工科大学, 発明者, 中川喜博, IPC:G06F 15／00, 日本

(13) 付加価値の源泉, Hermann Simmon／Yoo, PilHwa, 169p－192p5章時間資源, 東洋経済新報社

(14) マーケティングマネージメント, John a. Howard, 93p－94p動機付け測定方法, KENPAKUSHA

(15) e－Japan 重点計画－2003, Ⅱ. 先導的取り組みによるIT 利活用の促進, 1. 医療, 日本国内閣「高度情報通信ネットワーク社会推進戦略本部, http:／／www. kantei. go. jp／jp／singi／it2／kettei／030808honbun. pdf

(16) 付加価値の源泉, Hermann Simmon／Yoo, PilHwa, 121p－137p3章考える経

営, 東洋経済新報社

謝 辞

本論文を結ぶにあたり, 本研究の開始から終了までの間, 終始, 懇切な御指導と御鞭撻を賜った高知工科大学大学院教授加納剛太博士に衷心から深く感謝の意を表すと共に, 本研究をまとめるに際し, 有益な議論と御指導を賜った高知工科大学大学院教授情報システム工学科清水明宏博士, 起業家コース長冨澤治博士, 起業家コース平野真博士, 馬場敬三博士, 小林和彦博士, 長尾高明博士, そして大阪大学大学院工学研究科教授濱口智尋博士, また, 本論文の特許戦略について助言と御指導を頂いた, 東京大学先端技術研究センター教授玉井克哉博士, 経営理論の展開方法に長年ご指導を頂いた米国スタンフォード大学のRichard B. Dasher教授には厚く感謝の意を表します.

また, 本研究について発表を許可し, 始終御指導と御鞭撻を頂いた, 香川大学大学院教授最所圭三博士に心から御礼申し上げます.

富士通株式会社高島章副会長には, 本研究についてあらゆる面で前向きな遂行と発明に関する国際学会国内学会発表と, その研究成果に関する活用許可と権利の便宜を頂き厚く感謝の意を表します.

最後に, 高知工科大学大学院教授 故) 渡部宏邦博士には起業工学の集大成を教授頂き, 日本インターネット放送株式会社の設立の基となりました. ここに厚く感謝の意を表します.

2005年12月1日

筆 者

本 研 究 の 業 績 一 覧

- 論文

(論注1) 中川喜博単著:オフィスオートメーション学会 Vol. 25No. 3 PKIの重大欠陥による新ビジネスの創出

―個人情報と認証情報を銀行機能集中管理へ― (16年10月掲載)

(論注2) 中川喜博単著:映像情報メディア学会 新しい個人情報認証局システムの開発, 投稿

- 国際学会講演

(論注3) 2004年11月27日 中川喜博単著:ICOA国際学会, Proposal of a new Concept on Personal Information and new Certificate Authority

- 学会講演

(論注4) 2000年8月20日 中川喜博単著:プライバシーマークにおける監査業務の教育

(論注5) 2000年8月20日 中川喜博単著:個人情報保護の監査と報告書について

(論注6) 2000年12月2日 中川喜博単著:教育システム情報学会(旧CAI学会)個人情報保護システムの機能に関する考察

(論注7) 2000年12月2日 中川喜博単著:インターネットにおける学習教材の問題

(論注8) 2000年11月20日 中川喜博単著:ビジネスモデル特許国際出願と適応構想について

(論注9) 2001年8月24日 中川喜博単著:電気通信学会, 次世代ERPの構築について

(論注10) 2003年6月27日 中川喜博単著:映像メディア学会, 新しい個人情報認証

局システム

(論注11) 2004年1月27日　中川喜博単著:四国エンジェルスフォーラム, 医療IDCの事業化について

(論注12) 2004年1月27日　中川喜博単著:四国エンジェルスフォーラム, 起業の要点と意識改革討論会(パネラー)

- 特許登録

(論注13) 特許第34. 20364. 号, 2000－330949(10／30,　2000),　通信装置, 出願者, IPC:　G06F　14. ／00, :2001－64. 44. 4(12／27,　2001), 個人情報管理装置,　特許権者:学校法人高知工科大学, 発明者:中川喜博, 加納剛太,　IPC:　G06F　13／00,　日本国特許庁

- 国際特許出願

(論注14) 公開特許:Patent アプリケーション 09／836222(4／18, 2001), INDIVIDUAL INFORMATION MANAGING DEVICE, apply: Fujitsu Ltd. 100%, invent: NAKAGAWA Yoshihiro, IPC: G06F 14. ／00, G06F 1／00, G06F 12／14, USA

- 国内特許出願

(論注15) 公開特許 アプリケーション 2000－330949(10／30, 2000),　TELECOMMUNICATIONS SYSTEM,　apply: Kochi University of Technology,　invent: KANO Gota,　NAKAGAWA Yoshihiro,　IPC: G06F 14. ／00

(論注16) 公開特許2001. 64. 44. 4(12／27, 2001),　INDIVIDUAL INFORMATION MANAGEMENT DEVICE,　apply: Kochi University of Technology,　invent: KANO Gota,　NAKAGAWA Yoshihiro,　IPC: G06F 13／00

(論注17) 公開特許2000－271924. (9／7, 2000), Patent public presentation: PAT. 2002－ 82909 (3／22, 2002), INFORMATION MANAGEMENT PROVISION and INFORMATION MANAGEMENT SYSTEM, apply: 富士通株式会社 100%, invent: 中川喜博, IPC: G06F 14. ／00, G06F 1／00, G06F 12／14

(論注18) 公開特許2000－397492(12／27, 2002), PERSONAL INFORMATION MANAGEMENT PROVISION apply: 富士通株式会社 100%, invent: 中川喜博, IPC: G06F 14. ／00

- 経済産業省

(論注19) 提言書2000年12月14日　中川喜博単著:個人認証基盤の構築(個人情報認証局構想について提言書)

(論注20) 平沼赳夫経済産業大臣, 第1種包括役務取引(情報処理技術)の許可.

中川喜博研究内容による, (BIT－U－GL－02－100003, BIT－U－GL－02－100004)

審査許可請求:光伝送通信技術及び光ルーティング技術と交換

【米国スタンフォード大学へ最先端技術の輸出】

申請者:(2002年12月24日 富士通株式会社)

申請者:(2003年1月8日 橋本大二郎高知工科大学理事長)