ＩD管理とコンテンツ ID

1．ユビキタスネットワーク社会の進展とデジタル識別子

インターネットはビジネス及び社会生活の両面において，国民に大きな利便・恩恵をもたらす生活の必需品となっており，その先には，「ユビキタスネットワーク社会」と呼ばれる，便利で豊かな時代の到来が期待されている．[UJAP] このようなユビキタスネットワーク社会の構築においては，“(デジタル) ID”が重要な鍵を担っている．ここで，“ID”の表す内容（フルネーム）としては，Identity (同一性), Identification (同一性の確認)，及び Identifier（識別子/識別符号；対象の同一性を示す記号類）がある．ユビキタスネットワーク社会を安心・安全な社会とするためには，ID にまつわる技術的・社会的課題を解決すると共に，社会的コンセンサスを形成していく必要がある．

インターネットを利用したビジネスの進展に伴い，“Identity Management”[IMSP04]（ID 管理）が注目されている．ビジネスプロセスや社会活動の多くの部分がインターネット等のサイバー世界で行われるようになってきたのに伴い，Identity Management のための一群の管理情報の抽象概念は次第に拡張され，現在では“Digital Identity”と総称されることもある．Identity Management を適切に行うことにより，ビジネスや社会活動の効率化とコスト削減に結びつく．

Identity Management において通常用いられるものが，“Identifier”である．Identifier（識別子）の代表的な例は，ユーザ ID である．ユーザ ID に限らず，文字を用いた長い名称等より，管理対象に対応する短い番号や記号を用いた方が，データ処理及び通信による授受は容易であることは明らかである．この識別子自体，Identity Management における管理情報，すなわち Digital Identity の一部でもある．

ところで，このような識別子は，人だけに使われる訳ではない．コンテンツやサービス，モノ，さらには場所等にも使われる．これらの対象についても，識別のための管理情報が存在する．それらの情報は，“属性情報”や“メタデータ”と呼ばれる．適切に付与された識別子を適切に用いることにより，これらの対象に関する効率的な処理を行うことができる．(図-1)

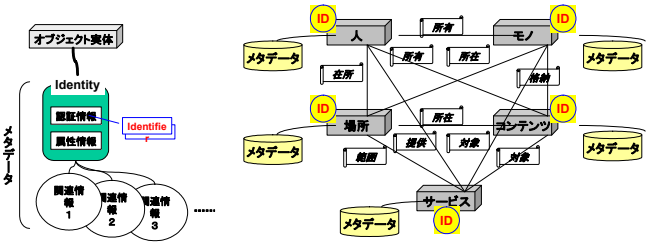

図-1　デジタル ID の概念と相関

このようにして，サイバー世界では，人，デジタルコンテンツ，サービス，モノ，場所等のオブジェクトに付与された識別子がシステム相互間で授受され，各システムにおける識別子対応の管理情報を用いて所定の処理が行われることになる．(図-2) このような世界においては，セキュリティ，データの一貫性，ユーザの利便性，プライバシー等の技術的・社会的課題がある．

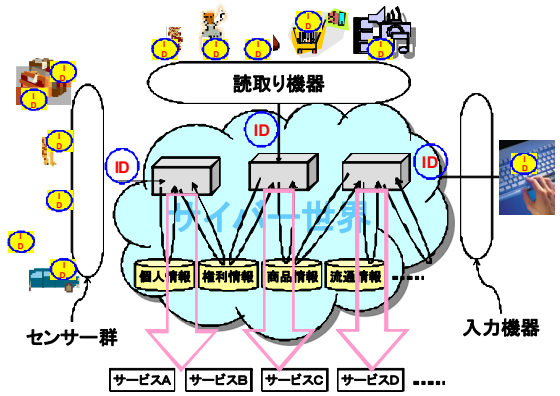

図-2　デジタル ID とサイバー世界のイメージ

2．デジタル識別子とその役割

ここでは，デジタル識別子を，実世界及びサイバー世界に存在するさまざまなオブジェクトに対して付与され，サイバー世界における種々の活動

のための使用される識別コード，と定義する．共通の認識の下に規定されたデジタル識別子を用いることにより，サイバー世界における活動の効率が高くなる．すなわち，サービスや地域共通に，高々数百ビット，あるいは数十文字のコードを指定することにより，世界中のどのコンピュータでも種々のオブジェクトを特定できる．そして，そのコードをキーにしてデータベースを検索することにより，必要な属性情報や関連情報等を容易に得ることができる．

(1) デジタル識別子の具備すべき条件　デジタル識別子に関しては，その識別対象や用途によって多少異なるものの，その具備すべき条件を，概ね以下の５つに整理できる．[ITSEC]

①グローバル環境でのユニーク性（Uniqueness）→デジタル識別子において最も重要な要求条件は，グローバルな利用環境を想定したときのユニーク性である．異なるコンテンツや異なる人に同じ値の識別子が重複して付与されていると，コンテンツの流通管理や課金処理がうまく機能しないことは明らかである．もちろん，限られたドメインにおいてのみ使用されることが明らかなものであれば，そのドメイン内でのみユニークであればよい．しかしながら，サイバー世界ではネットワークを通じて瞬時に世界中に情報伝達が行われ，そこでの活動は一般的にボーダーレスである．したがって，言語やシステム等の壁を越えてグローバルスケールでのユニーク性をどう担保するかが課題となる．そのために最もよく行われている方法は，所定の登録機関が集中的に識別子の発行を管理・運用することである．この機関を，RA（Registration Authority）と称する．通常，RA は，公的機関，あるいは公的機関から委任を受けた機関が運営する．

②永続性（Persistency）→識別対象オブジェクトは長期間，ものによっては半永久的に存続するものであるから，その識別子にも，対象オブジェクトのライフサイクル以上の永続性が要求される．この“永続性”という言葉には数多くの意味合いが含まれるが，代表的なものとしては以下のような項目が挙げられる．

i) 識別子が時間的に変化するもの（例えば，URL）に依存していないこと

ii) 発行者及び発行監督者の財政的基盤が健全であること

③識別子からのロケーション可解性（Resolvability）→ここでいうロケーションには，識別子の対象オブジェクトそのものと，対象オブジェクトのメタデータ（属性情報，関連情報等）との２種がある．識別子は，単に対象オブジェクトのユニーク性を証明するだけのものではなく，そのオブジェクト実体や，オブジェクトのメタデータ（属性情報，関連情報等）にアクセスするためのキーとしての機能を持つことにより，利便性が大幅に向上する．このように，識別子から実体やさまざまな情報等のロケーションを得る仕組みをレゾリューション（Resolution）という．特に，サイバー世界において電子商取引等のビジネスや電子政府/自治体等の社会活動が盛んになりつつある昨今の状況では，オンラインによるインタラクティブなレゾリューションサービスの提供は，Digital Identity のためのインフラとして極めて重要な要求条件となる．

④オブジェクト実体との不可分性（Inseparability）→人やモノのように，オブジェクト実体がリアル世界に存在する場合と，デジタルコンテンツのように，サイバー世界に存在する場合とがある．リアル世界にオブジェクト実体が存在する場合には，その識別子だけがサイバー世界に引き渡される．この場合に重要なことは，オブジェクト実体と識別子との対応関係を認証することである．一方，サイバー世界にオブジェクト実体が存在する場合には，オブジェクト実体とその識別子とが不可分の状態であること，すなわち，オブジェクト実体から識別子の切り離しが容易にはできないことが重要な要求条件となる．このとき注意すべきことは，デジタルコンテンツのように，デジタルネットワークばかりとは限らず，プリントアウトや画面表示といったアナログドメインを経由する流通経路も考えられるということである．また，著作権等の種々の重要情報との関連付けが行われている識別子を削除しようとする故意の攻撃も想定する必要がある．

⑤他識別子との相互運用性（Interoperability）→

識別子体系は，本来，世界で統一された共通のものであることが望ましい．これは，その目的である，処理の効率性やユーザの利便性の観点からも，当然のことである．しかしながら，特に最近規定された識別子については，世界の多くの団体により独立に，あるいは連携を図りつつも独自に，標準化作業が行われている．それらの活動と成果は，各団体の関連業界におけるビジネス上の特徴を反映している場合が多く，世界で唯一の識別子体系にまとまることは考えにくい．したがって，複数の識別子体系の共存が必要となる．具体的には，オブジェクトの利用局面に応じて，他体系の識別子が付与されているオブジェクトに対して，その識別子を参照する仕組みが必要となる．識別子やメタデータの交換によく利用される XML（eXtensible Markup Language）ベースの文書においては，当該識別子を規定した機関のロケーション情報（URI; Uniform Resource Identifier）を記述することにより，複数機関で規定された識別子の混在を可能としている．これは，名前空間（Namespace）と呼ばれる．[XMLNS]

(2) デジタル識別子の種類　グローバル環境でこそ威力を発揮するデジタル識別子であるため，その標準化は必須である．ここでは，オブジェクトの種類ごとに，グローバル環境で運用されている主なデジタル識別子をリストアップする．

①ネットワークアドレス→電話番号(固定, 携帯)，MAC アドレス, IP アドレス，ドメイン名, URL（URI）
②人→メールアドレス，住民基本台帳番号，OpenID
③コンテンツ→コンテンツ ID，DOI（Digital Object Identifier），ISAN（International Standard for Audiovisual Number）等[CIDS][ITSEC]
④サービス→GUID（Global Unique ID)，UUID（Universally Unique Identifier）
⑤モノ→JAN（Japanese Article Number）等のいわゆるバーコード（商品コード)，Auto-ID やユビキタス ID 等の RFID
⑥場所→RFID

(3) デジタル識別子の利用　さまざまなデジタル識別子を用いることにより，サイバー世界において，高度なサービスを効率よく実現することができる．

①オブジェクト管理→商品の在庫管理，受発注管理，及び，これらの管理により集められたデータによる売れ筋商品や需給予測等の分析から，サプライチェーン管理（SCM; Supply Chain Management）や電子データ交換（EDI; Electronic Data Interchange）へと発展している．
②流通状況把握→いわゆる「トレーサビリティ」[DIDR]等のように，個々の対象商品一つずつをそのライフサイクルに亘って個別に管理する．
③レゾリューション→オブジェクトあるいはその情報にアクセスすることを目的に，ある識別子から別の識別子に変換することを表す．人やモノ，コンテンツ等のデジタル識別子の場合には，その識別子からオブジェクト実体あるいはオブジェクトに関する属性情報等（メタデータ）の所在を示すアドレス（URL 等）を得るために，レゾリューションが用いられる．[PCID]
④ディレクトリ・サービス（Directory Service）→インターネット上に散在する多くの資源（データやサーバ，ユーザ等）に関する情報を提供するサービス．レゾリューションと組み合わせたディレクトリ・サービスでは，まず，レゾリューションによりデジタル識別子から対応するディレクトリのアドレスを得た後，そのアドレスにアクセスすることにより，当該オブジェクトに関する権利情報や製品情報を入手する仕組みとなっている．

3．コンテンツ ID の概要

“コンテンツ ID”は，流通するコンテンツを特定するために，一意に付けられるデジタル識別子である．デジタルコンテンツに対しては，その内容や権利関係の情報，さらには流通に関する情報等の種々の属性を記述したメタデータが存在するが，コンテンツ ID により，このメタデータをも一意に特定することができる．[PCID]

(1) コンテンツ ID の形式とメタデータ　コンテンツ ID の形式とバインド方法を図-3 に，コン

テンツのメタデータを図-4 に示す．ID は，電子透かし等により，コンテンツに埋め込まれる．[CNLAN]

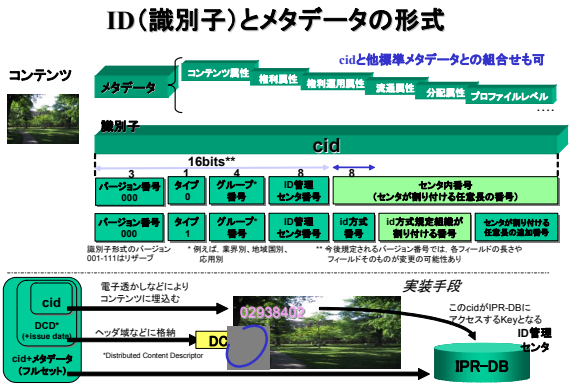

図-3　コンテンツ ID の形式とバインド方法

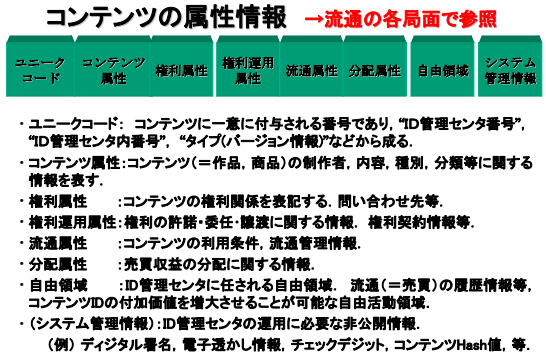

図-4　コンテンツのメタデータ

(2) コンテンツ ID の付与単位　コンテンツ ID の付与単位は，著作者あるいはコンテンツ流通をする人が，その流通を管理したい単位で，任意に決めることができる．例えば，映画の 1 作品全体に 1 つの ID を付与することも，シーンとかカットとか，個々の部分的なところにそれぞれ ID を付与することも可能である．また，コンテンツのモジュール，つまり部品に ID を付与し，その部品を集めた 1 つの作品に対してもさらに別の ID を付与することもできる．さらに，実際のコンテンツの流通を考えると，例えば DVD のようにパッケージとして流通させる場合や放送やインターネットで流す場合等，いろいろな流通経路がある．流通条件はこの経路ごとに異なるので，同じ作品でも，流通経路に応じて別の ID を付与するということも可能である．

(3) コンテンツ ID の運用　実際にコンテンツを保持する者が，コンテンツやその属性情報の管理のために“ID 管理センタ”を設置する．公的な認可登録機関として“レジストレーション・オーソリティ（RA）”を設け，ID 管理センタに対して RA からセンタ番号を重複なく発行する．各 ID 管理センタでは，このセンタ番号と内部管理の独自番号とを連結してコンテンツ ID を構成することにより，全体として，ユニークな番号が発行できる．この仕組みを図-5 に示す．

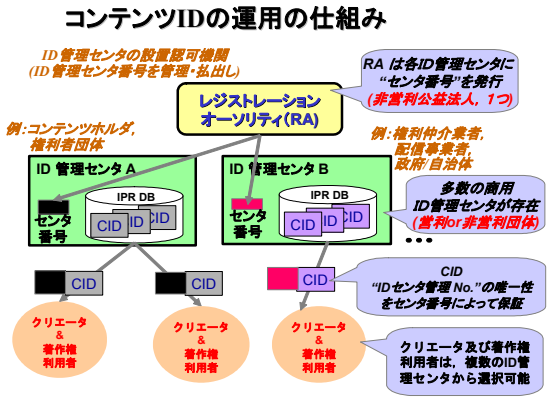

図-5　コンテンツ ID の運用の仕組み

(4) コンテンツ ID レゾリューション　コンテンツ ID からメタデータの所在場所を知るための“コンテンツ ID レゾリューション”では，コンテンツに ID が付与され，例えば電子透かしによりその ID が埋め込まれて流通している状況において，利用者が入手したコンテンツから取得したコンテンツ ID をサーバに渡すと，その ID に対応する属性情報が登録されているデータベースのロケーション（URL）が返却されるため，そこにアクセスすることにより，種々の情報を入手することができる．このイメージを図-6 に示す．コンテンツ ID レゾリューションの応用として，コンテンツを媒介としてサービスに誘導することも可能となる．[SVSI]

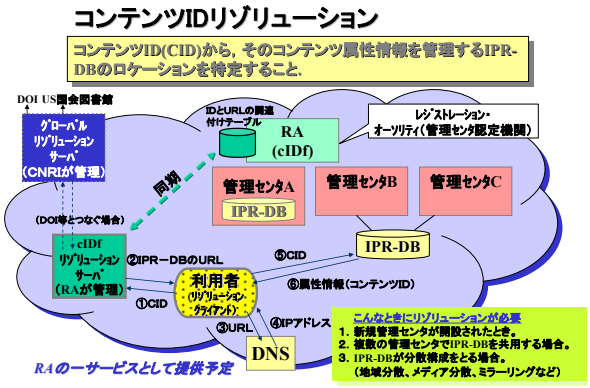

図-6　コンテンツ ID レゾリューション

(5) コンテンツ ID の標準化　　コンテンツ ID の仕様は，1999 年～2007 年にかけてコンテンツ ID フォーラム（cIDf）において策定され，その一部は，ISO MPEG-21 等にも採用されている．cIDf は既に解散しているが，現在は，NPO 法人ブロードバンドアソシエーション（http://www.npo-ba.org/）が cIDf 仕様及び RA を引き継いでいる．

4．社会基盤としてのデジタル ID の課題

デジタル ID を活用したユビキタスネットワーク社会は，豊かで便利な生活をもたらしてくれるものと期待されている．しかし，一方では，そのような社会における，セキュリティやプライバシーに関する懸念や不安も指摘されている．これらの懸念や不安を解消し，安心・安全で便利な社会を持続させるために，技術的に，社会的に，あるいは運用上で解決すべき課題は多い．また，それらの各課題は，相互に深く関わっている．

(1) 技術的課題　　セキュリティとプライバシーに関わる問題の解決が必要である．

①ID のオブジェクトへのバインド技術→デジタル識別子の具備すべき条件の一つとして述べたように，デジタル識別子とオブジェクト実体との不可分性を保証する技術は，非常に重要である．人に対する識別子の場合には，バイオメトリックス認証を使用することができる．[BIOM] デジタルコンテンツに対する識別子の場合には，コンテンツファイルのヘッダ域への格納，電子透かし（Watermarking），電子指紋（Fingerprinting）等の技術があるが，それぞれ一長一短がある．[DCAJ]

②個人情報開示制御技術→消費者は，得られる利益に応じて個人情報の開示範囲を決定するのが普通であり，さまざまな条件に応じて，開示してもよいと考える個人情報を設定でき，その結果として作成される開示制御テーブルに基づいた情報の提供が行われることが望ましい．

③レゾリューション拒否技術→ID から対応する情報の場所を引くレゾリューションを許容するか否かを消費者により制御することができれば，プライバシーの問題が解決される可能性がある．その実現方法の一つとして，米国で導入された電話勧誘拒否登録制度“Do-Not-Call Registry” [DNCR]と同様のものが考えられる．

④オブジェクト認証技術→人が本人であることや，モノやコンテンツが本物であること等を証明することは，非常に難しい．人のように，あらかじめそのオブジェクトを特徴づけるデータ（DNA や指紋等）が登録されていれば，比較的容易に証明可能である．デジタルコンテンツの場合には，『ワンウェイ・ハッシュ』と呼ばれる技術を用いて，その特徴データを抽出することができる．

(2) 社会的課題　　技術面で取り組む必要があるが，社会のコンセンサスが最も重要である．

①監視カメラ/センサー等による監視型社会→安全とプライバシーとのトレードオフ，バランスの問題である．

②個人情報の管理→個人情報に関する消費者の最大の懸念は，それが，いつ，誰に対して，どのように提供されるか分からない，ということである．

③プライバシー保護→ガイドラインは，技術と法制度に裏打ちされることにより，実効性が高まる．

④スパムメール→デジタル ID の悪用による迷惑行為である．フィルタリングに加え，“Sender ID” 等の抜本的技術も議論されている．[SNDRID]

(3) 運用上の課題　関係者の協調が望まれる．また，運用者には公平性・透明性が求められると共に，利用者にも応分の負担が求められる．

①標準化→普及促進のために，また，利用者が後で困らないように，産官学連携による標準化が望まれる．また，対象によっては，国家戦略の観点から，官主導の標準化活動も重要である．

②ID 登録機関（Registration Authority）→グローバル環境でユニークな，全世界の共有資源としてのデジタル ID を実現するためには，その付与方法を統一的に定め，運用する必要がある．

参考文献

[BIOM] 瀬戸洋一: “バイオメトリクス技術の国際標準化に対する産業界の取り組み”, 情報技術標準化フォーラム講演資料, http://www.itscj.ipsj.or.jp/forum/seto.pdf （2003 年 7 月 18 日）

[CIDS] 山下博之，他 : “コンテンツ識別子標準の動向とコンテンツ流通サービス”，画像電子学会誌，Vol. 30，No. 5，pp. 532-539，2001 年 5 月．

[CNLAN] 山下博之 : “次世代の認証技術 : 利用状況を把握するコンテンツ ID による認証, ”COMPUTER & NETWORK LAN, 2004 年 9 月号，pp.30-35，オーム社.

[DCAJ] “コンテンツ不正利用等監視・追跡技術の利用とその法的課題に関する調査研究報告書”，DCAJ 15-CC-L，（財）デジタルコンテンツ協会(DCAj)，2004 年 3 月．

[DIDR] 國領二郎+日経デジタルコアトレーサビリティ研究会: “デジタル ID 革命”，日本経済新聞社, 2004 年 1 月 23 日．

[DNCR] National Do Not Call Registry: http://www.donotcall.gov/ (2004 年 7 月 23 日)

[IMSP04] Duncan A. Buell and Ravi Sandhu: “Identity Management”, IEEE Internet Computing, Vol. 7, No. 6, Nov. / Dec., 2003, pp. 26 – 52.

[ITSEC] 片方善治監修: “IT セキュリティソリューション体系”，上巻 7.1 節，（株）フジ・テクノシステム，2004 年 4 月 5 日．

[PCID] 安田浩，安原隆一監修: “ポイント図解式 コンテンツ流通教科書”，（株）アスキー，2003 年 7 月 2 日．

[SNDRID] “Sender ID ホームページ”: http://www.microsoft.com/japan/mscorp/safety/technologies/senderid/default.mspx

[SVSI] 山下博之，他 : “連携シナリオ"流通に基づく P2P サービス仲介に関する一考察, ” インターネットコンファレンス 2003 講演，2003 年 10 月 28 日．(http://www.internetconference.org/ic2003/PDF/paper/yamashita-hiroyuki.pdf)

[UJAP] “「ユビキタスネット社会の実現に向けた政策懇談会」中間とりまとめ”，総務省，http://www.soumu.go.jp/s-news/2004/040701_1.html （2004 年 7 月 1 日）

[XMLNS] Tim Bray, et al., Namespaces in XML, 1999, W3C Recommendation, http://www.w3.org/TR/REC-xml-names （日本語訳 : JIS TR X 0023:1999）