カプセル化コンテンツの動向と展望

櫻井 紀彦
NTT **サイバースペース研究所**
sakurai@dq.isl.ntt.co.jp

ネットワークを用いたディジタル情報の流通が盛んになるにつれ，情報提供側の意図に従った範囲での利用ができる仕組みが求められるようになってきている．特にその扱いに「保護」・「利用範囲の限定」が要求される情報として，Privilege（例えば著作権を考慮すべきコンテンツ），Privacy（個人の情報），そしてKnowledge（ノウハウ・知識）がその例としてあげられる．本論文では，これらの情報をハンドリングする上で注目されている，Object の概念を拡張したカプセル化コンテンツについてその技術的動向を展望する．

Trends and Prospects about Secure Container Technology

Norihiko Sakurai
NTT Cyber Space Laboratories

Recently, more and more information is transferred, distributed, and exchanged through the network. It includes privileged materials such as copyrighted creations, privacy, business intelligence, etc. that should be protected from improper use. 'Secure Container' technology is one of the most promising technique to achieve sufficient protection stood together with flexible distribution. In this paper, I report the current status, then give the prospect, about the technology.

1．はじめに

インターネットが急速に世界中に浸透し，さらにパーソナルコンピュータや携帯端末の普及により，ネットワークを通じたディジタル情報の流通を，誰もが手軽に行える環境が整いつつある．これらの動きは，情報の活用という観点からみると，以下の大きなパラダイムシフトが生じたと捉えることができる．

① クローズな世界からオープンな世界へ

例えば自からの企業内のデータをある目的で共有するようなクローズな企業系内での情報の活用から，自らの所有する情報だけでなく，インターネットに発信されているさまざまな人々が築いた情報の海の中から，自分の目的に合わせて情報収集するような，オープンないわば社会系での情報の活用が行われるようになった．

②多様なメディアのディジタル化

メディア処理技術の発展も伴って，写真・絵画や音楽，映像などの多種多様な資産が，ディジタル化され，ネットワークを流通するようになった．

③ 経済的価値がある情報の流通へ

ディジタル化された音楽，美術品など，それ自身に経済的価値のある情報（以下ディジタルコンテンツ）を，ネットワークを通して必要とする人々に売買したり，さらにはこれらを結合・加工し付加価値をつけることにより，新たなビジネスが形成されはじめてきた．

これらの情報は，社会的資産としてより多くの人に利用してもらうことを期待するものであるが，その利用に関しては，何らかの権利【**Privilege**】を伴うもの（例えば著作権に基づく利用報酬を得ることなど）であり，発信者による何らかの意図が正確に反映されて，一層の流通の活性化が図れるものであることが通常である．

④ 開示範囲を保証した情報の提供の必要性

一方，医療・教育各種サービスのネットワーク化に伴い，個人がサービスを享受するために必要最小限の個人情報をネットワークを通してサービス主体へ提供することも必要になってきた．個人情報は，より適切なサービスを受けるために，サービス本来の目的

に対しては開示が必須ではあるが，他人に見られたり，本来の目的以外に使用されることは許しがたい性質をもつ情報，つまり【Privacy】の保護が必要な情報である．

また，近年，企業内の知識の集約を図り生産性を高めるための Knowledge Management の考え方が提案され，さらに将来的には SOHO（Small Office Home Office）の進展においても，その知識（ノウハウ的なもの）をいかに上手に運用していくかが重要な課題となっている．これらの知識【Knowledge】は，外部に発信して意味があるものの，その利用状況は発信者の意図に従った管理が要望されるものになっている．さらにこれらの知識情報は受け手によってその価値・扱い方が異なってくるという特徴がある．

2．カプセル化技術

本論文ではこれらの **Privilege**・**Privacy**・**Knowledge** のキーワードに代表されるような，何らかの形で社会に発信することが必要なものの，その利用に関しては，発信者の意図を保証することが重要な情報の流通・管理に関して，

「ディジタルデータとその利用方法を一体として，それを情報(*1)のハンドリングの単位として扱う考え方」に基づき考察を進めていく．

この考え方は，実はいわゆるオブジェクト指向の考え方[Atkinson1989]そのものであるが，各ディジタルデータにメソッドをそれぞれ適切にバインドしカプセル化し，カプセルがそれを利用する環境に移動し，メソッドにより内包データの管理を実行するなど，その自律性を重視したものである(*2)．

3章以降において，このカプセル化された情報による Privilege, Privacy, Knowledge データのハンドリングに関する現状の技術動向・課題について述べる．

(*1) **増永[増永 1991]によると情報は「その受け手が知識の増加を引き起こすもの」として定義しており，本来その利用方法等を含んでいるものである．**

(*2) ディジタルデータと利用方法等のメソッドをカプセル化し，ネットワークを通して移動した先の環境においても自律的制御を行う機能単位を総称して，筆者は特に Active Object という呼び方をしている．

3．Privilege を伴うディジタルコンテンツ

社会的資産として価値を持つディジタルコンテンツは，MPEG 等の符号化技術と情報通信技術の進歩によって，扱える情報形態も文字情報から高品質の静止画像，音声，動画像へと広がり，ネットワークを用いた映画や楽曲の販売も試みられるようになった．しかしながら，ディジタル情報は複製が容易で劣化しないという特徴をもつため，一定の価値を持つ情報を流通する際には，不正な利用を防止し，知的所有権を保護する仕組みが不可欠であり，これらの保護を目的としたシステムが提案・実用化されている．

これらのシステムは大きく２つの特徴を持つ技術が基本になっている．

一つは電子透かし技術等を用いて，ディジタルコンテンツ自身に著作者情報を埋め込む技術である．この技術は，コンテンツの部分再利用などにおいても効力を発揮するが，基本的に不正な利用を防止するのではなく，不正利用が行われた時にその証拠として提示できるため，不正を抑止する機能であり，自動車の安全装置に例えるとシートベルトや剛性ボディのような Passive Safety 技術である．コンテンツ ID フォーラム(cIDf) [岸上 2000]の活動においても取り上げているように，コンテンツの流通促進のためには重要な技術であるが，本論文のターゲットからはやや外れるので，詳細は省略する．

これに対して，不正利用の発生自身を未然に防ごうとする，Active Safety 技術が開発されている．同様に自動車の安全装置に例えるとアンチロックドブレーキなどのしかけが相当する．Active Safety 技術と Passive Safety 技術は相互補完として組合せることにより最も効果を発揮する．

カプセル化を用いた Active Safety 技術として具体的な例としては以下のものがあげられる．

3.1 Active Safety を実現している例

⑴ Windows Media Rights Manager（WMRM）（Microsoft 社）[w1]

Windows Media Technology において，ディジタルメディアの安全な配布を行うシステムコンポーネントである．WMRM では，ディジタルコンテンツを暗号化し，これ対して別途ライセンスを供給することで，コンテンツ所有者の権利を保護するしくみ．ライセン

スには，コンテンツの復号キーのほか，コンテンツの使用開始／終了日時，使用回数，可搬記憶メディアへの出力許可等の条件を含めることができる．これらの条件は WMRM をサポートするプレイヤー（例：Windows Media Player）によってライセンスから読み出され，プレイヤーがそれに従って動作することを前提としている．

（2） MetaTrust Utility（InterTrust社）[w2]

MetaTrust Utility は InterTrust の DRM 技術と互換性のある製品の総称である．InterTrust は，自社で DRM 製品を提供する一方，その技術ライセンスを他企業に提供し，単一技術に基づくグローバルなフレイムワークを構築することを目指している．主要なコンポーネントは，DigiBox Container, Usage Rules, InterRights Point, Transaction Authority Framework の 4 つである．コンテンツ提供者は，保護の対象となるコンテンツに，その利用条件（Usage Rules）を添付して DigiBox Container に格納し利用者端末に配信する．利用者端末上に配備されている InterRights Point が Usage Rules を満たすことを確認した場合にのみ配布された DigiBox Container が開かれ内包されたコンテンツを利用できる．その一方で InterRights Point は Transaction Authority Framework システムと通信し，課金等に必要な情報を送信する．

⑶ RightsEdge (ContentGuard社) [w3]

ContentGuard は，もともと Xerox で研究開発が行われていた著作権保護技術だが，現在は Xerox からスピンオフし，Microsoft と Xerox の共同出資のもとで運営され，製品として"RightsEdge"というシステムを提供している．ContentGuard における処理の流れの概要は，まず提供者が Protection Toolkit を用いて，コンテンツから保護されたコンテンツと Rights Label を生成する．Rights Label はコンテンツに許可される権利とその条件，その他コンテンツに関する書誌情報等を記述したメタデータで，XrML（eXtensible rights Markup Language）というXML ベースの言語で記述されている．この Rights Label が RightsEdge Server に送られる一方，保護されたコンテンツはリポジトリーに保管される．利用者は，ネットワーク上の電子店舗などを通じて RightsEdge Server からライセンス（Rights Label から生成され，やはりXrML で記述されている）を購入するとともに，リポジトリーから対応するコンテンツを入手する．最後に，Activation Server からユニークな公開鍵ペアの秘密鍵を入手し，コンテンツの保護を解除して利用する．

⑷ RightsShell （NEC社)[w4]

RightsShell は，コンテンツを暗号化し，その利用の際にチケットと呼ぶディジタルの利用券と組み合わせて使うことで不正な利用から著作物を守るコンテンツ配信システム．RightsShell では，コンテンツは暗号化され，利用形態毎の鍵（≒利用鍵）と合わせたカプセルとして提供される．カプセルの利用の際には，まず RightsShell クライアントを介してチケットサーバーからチケットを入手する．チケットには，契約条件とチケット鍵が含まれており，このチケット鍵と利用鍵からコンテンツの復号鍵が生成され，復号が行われる．復号されたコンテンツは RightsShell クライアントを介してブラウザー上で再生される．

⑸ Cryptlope/EMMS（IBM社） [w5]

IBM の Eelectronic Media Management System（EMMS）は，"Content Mastering Program", "Web Commerce Enabler", "Clearinghouse Program", "Content Hosting Program", "Player Software Development Kit" という5 つの主要製品で構成される，ディジタルコンテンツ流通の包括的なソリューションである．コンテンツ提供者は Content Mastering を用いて，暗号化／電子透かし処理のなされたコンテンツを "secure container" に格納して Content Hosting に格納するとともに，販促用のデータを Web Commerce Enabler によって構築された Web 店舗に送る．利用者は Web 店舗の販促用データを EMMS 対応 Player で再生する．利用者が購入のアクションを取ると，Player は対応する secure container を Content Hosting から取得するとともに，Clearinghouse に課金情報を送る．Clearinghouse は Player にライセンスを発行するとともに，課金情報をWeb 店舗や Content Hosting に転送し，課金処理を行う

EMMS の secure container としては，（明示的に記されてはいないが）同社の Cryptolope 技術が利用されているようである．Cryptolope は，一つのファイルの中に，（複数の）暗号化されたコンテンツ，それらのメタデータや復号鍵，契約条件，電子透かし／シグネチャ，電子公証書などが格納された複合ファイルで，Cryptolope 対応プレイヤーが，契約条件に基づくライセンスを受け取り，それに従って動作することでコンテンツの不正な利用を防止する．

他に RealSystem［w6］（RealNetwork 社）などは特にカプセル化はされていないものの ActiveSafty な機能を持つものもある．

これらのシステムは，カプセルに内包する機能と，利用者 PC 上に置く機能の機能分担により，例えば以下のような違いがある．

タイプ A. ．．．利用者環境に，カプセル構造を認識，暗号・復号が可能な信頼できるプレーヤやアプリケーションが存在し，カプセル内には利用条件とディジタルコンテンツが内包されるタイプ．

タイプ B．．．利用者環境には，カプセルを実行させるための最低限のコンテナのみが存在し，暗号・復号，コンテンツ表示手段（プレーヤ），利用条件の監視手段まですべてカプセル内に内包しているタイプ

(1)～(6)は，タイプ A であり，利用条件の検証をした後にネットワーク経由で別途送られてくる復号鍵により復号行う方式を採用しており，安全性の観点から優れているが，このセキュアなポイントをどのように広めていくかが課題になる．このタイプはコンテンツの配信の形式が定型化される場合に特に適する．下記に具体的に紹介する Matryoshka はタイプ B で利用者側に必要な機能はほとんどなく，自律性を重視するタイプで，復号鍵まで内包する場合には，オンライン接続を必要としない．このため広告など不特定多数のユーザに配布するようなシーンにも利用できる反面，復号鍵を内包する場合にはクラッキングなど安全性面では相対的に弱くなる．

3.2 カプセル化コンテンツの具体例

3.2.1 Matryoshka（NTT）の例

Matryoshka を例にとりその動作原理を具体的に説明する．Matryoshka とは，流通対象となる価値を持つコンテンツと，利用制約条件やコンテンツの説明等のコンテンツ関連情報と，カプセル全体の動作を統括し，利用制約条件に基づきコンテンツを実際に表現する機能；コントロールを有する単一の格納単位であり，それらを内包する実行ファイル形式で存在する．Matryoshka カプセルを実行すると，カプセル内のコントロールは，同じくカプセルに内包されているコンテンツ関連情報を読み込むとともに，実行環境をセンシングし，利用制約条件のチェックを行う．利用制約条件としては，利用者認証（端末限定），使用時間管理，使用期限管理，使用回数管理が可能になっている．条件が適合する場合，コントロールは履歴情報の更新処理を行った後に，制約条件に基づいてコンテンツを表示する．コンテンツ及びコンテンツ関連情報は通常暗号化処理がなされており，カプセルに内包されるコントロールのみが必要な暗号復号化処理等を行い，コンテンツの正常な表示ができるよう設計されている．このように Matryoshka カプセルは，コンテンツ自身に表現手段と利用制御機構を併せ持つことで，どの流通過程においても，自律的にコンテンツの保護を行うことが可能になっている．

Matryoshka には，Active-X（Windows 専用）ベースの実装のものと，マルチプラットフォームでの動作をねらった Java による実装のものがある[阿部 2000]．

さらに，cIDf で定義されたコンテンツ ID を Passive Safety の機能である電子透かしとしてコンテンツに埋め込み，またそのコンテンツの属性や特徴量などでの検索を可能とし，そのコンテンツを利用者に提供する時には，許諾された利用条件とともにカプセル化を行う統合的なコンテンツ管理システムも実用化されてきている[西岡 2001]．

3.2.2 課題と展望

（1）コンテンツライフサイクルを通した管理の実現

ディジタルコンテンツは，加工・部分利用などの再利用を含め，コンテンツの生成，流通，利用，加工といったライフサイクルを一貫してその利用条件を継承・管理することが望ましい．

このためには，加工手段となるプログラムが，①そ

の一次コンテンツのそれぞれのカプセルに設定されている加工時の条件や加工後再利用される部分に関する利用条件を継承して，②加工生成された二次コンテンツの利用条件をこれに加えて設定し，③再度カプセルとして生成することが必要であり，その一連の処理を管理できる外部のサーバの存在を含め，この条件を正当に実行する編集環境が提供できるかが重要になる．

⑵ リソースを安全に提供するメカニズム

カプセル自身は利用者から見るとその内包している処理系が正当なものなのか，悪質なものなのかを容易に見分けることができない．このため安全にカプセルを利用するためには，カプセルが実行するための利用者リソースを限定することが必要になってくる．例えば[谷口 2001]では，カプセルと利用者サイトとの間で「契約に基づくリソース提供」が行われるメカニズムを提案している．

① まず，利用に先立ちカプセルと利用者サイトが，互いのリソースの利用条件に関する契約を取交わす

② 情報カプセルが実際に利用者サイト上で起動されると，相互に認証を行い，正規のリソース利用者であることを確認する

③ 情報カプセル実行中は，相手の要求に応じ，契約に則って互いにリソースを提供する．場合によっては，提供するリソースについて，その利用方法を継続的に監視し，不正な利用は事前に防止する

具体的には，利用者サイトの空間をパブリックリソースとプライベートリソースに分け，その空間間の移動（資源を割り当て）を管理する機構を提供することで実現を考えている．

4. Privacy情報のハンドリング

医療情報システム，福祉情報システムあるいは教育情報システムといった個人に密着したサービスがネットワークを介した広域情報サービスとして展開されるにつれて，個人の Privacy に関する情報の扱いはますます慎重になるべき重要な課題になってきている．Privacy 情報に関するカプセル化の重要性に関して，医療情報システムを例に考察する．

4.1 医療情報システムでの要求条件の例

⑴ 情報の開示制御

医療情報には，患者のプライバシーに関する情報が含まれており，診断情報のうち参照が認められた目的に対して，許可された情報のみが参照できるようにする必要がある．例えば，看護人や薬剤師が参照すべき情報は，個人の電子カルテ情報の内，主治医が検査項目や投薬の目的に記述した部分のみに限定して参照できるような，目的に対応した情報の開示が必要になる．このような要求条件に対し，共有するデータベースの項目のそれぞれに開示ポリシーを記述可能とし，そのポリシーを評価した結果，正しい目的として認証されたアクセス主体に対してのみ参照等を許す開示制御が実用化されている[山本 2000]．

⑵ 開示制御された結果読出された情報の保護

開示制御によりアクセス時点での正当な参照が行われたとしても，一旦読み出されたPrivacy情報が，開示制御の及ばない範囲に転々流通することを防止することが必要となる．この手段として，開示制御によって正しいと評価された目的の情報要求元に情報を送る場合にも，その開示ポリシーが評価可能なメソッドをバインドしたカプセルとして Privacy 情報を送ることが考えられる．カプセルは，正しい目的と認証されない処理系からアクセスされた場合に，不正アクセスとして Privacy 情報自身を消去し，本来の共有データベースに対して正当なアクセス権を持ったのちに参照するように要求する．またアクセス主体の履歴を取得していくことも可能である．

4.2 課題と展望

Privacy 情報は，

・情報が不正に漏洩してしまった場合の社会的影響が極めて大きい．

反面，個人の利便性向上の側面からは

・様々な社会サービスが電子化・NW化するにつれ，サービスを適切に享受するために，提供が必要．

と相反する問題があり，アクセス主体の目的を認証し，正当な場合のみ Privacy 情報を提供するといった制御が可能なカプセルは，有望な手段となる．

この時，各サービスは，カプセルに対して通信し

データを出入れすることが必要になるため，そのプロトコルの標準化や，アクセスの目的（AP の正当性）を認証するための手段が確立されていくことが課題となる.

5. Knowledge情報のハンドリング

Knowledge 自身，情報価値の高いものであり，企業での知識の共有，SOHO 等におけて個人から知識を発信する様なビジネスの形成等において，Privilege 情報や Privacy 情報と同様に，利用条件や開示範囲などの制御が重要である．さらに Knowledge に特徴的なものとして，利用者毎にその知識に対する重要度や重視する知識の関連性が異なることが考えられる．このため，他の情報と同様にカプセル化されて管理された場合に，それらのカプセル内情報の集合が利用者の重要度等に応じて構造化されていく要求が考えられる．またカプセルとして保全された情報から必要な情報を検索することも考えられる．カプセルの集合に対して，オブジェクト間通信を使ったカプセル内の情報間の類似性・関連性を評価し，リンクを張っていくことにより，カプセル情報間の整理を行う研究が進んでいる［難波 2000］.

6. まとめ

Privilege のあるディジタルコンテンツ，Privacy 情報，Knowledge を例にあげ，カプセル化技術の動向と課題をまとめた．今後の情報化社会におけるキーとなるこれらの情報のハンドリングそれぞれにおいて，内包する情報の利用条件を監視しながら，正当な情報の利用を可能とするカプセルは，提供者にとっても利用者にとっても，相互に安全性と利便性を与えるものとなることが期待できる．また，本稿では触れなかったが，例えば，Smile による同期制御を内包したカプセル[木俵 1997]に代表されるような，より豊かな表現手段としてしての応用方法もあり，今後のコンテンツ流通システム等を考えていく上で「オープンな社会系での情報ハンドリング」の基本単位として扱われていくと考える.

参考文献

[Atkinson1989] Atkinson,M. 他："The Object-Oriented Database System Manifesto," DOOD'89, pp.40-57, 1989

［増永 1991］増永: "リレーショナルデータベース入門," サイエンス社, 1991

[谷口 1999] 谷口, 森賀, 久松, 櫻井: "マルチメディア情報ベースとその格納単位 Matryoshka", 情処 DICOMO シンポジウム, 1999

[加賀美 2000]加賀美, 森賀, 塩野入, 櫻井: "コンテンツ流通における自律管理を目的としたカプセル化コンテンツ Matryoshka", 情処研報 DPS 97-18, 2000

[谷口 2000] 谷口, 阿部, 塩野入, "Java を用いた動画配信用著作権保護カプセル", 情処研報 DPS 98-6, pp.31, 2000

[阿部 2000]阿部, 谷口, 塩野入: "Java を用いた動画配信カプセルの実装", 情処 DPS ワークショップ, 2000

[西岡 2001] 西岡, 大竹, 瀬尾: "コンテンツ流通情報管理機構の実現", 情処研報 DPS 102-14, 2001

[岸上 2000] 岸上, "電子化知的財産とコンテンツ ID", 情処研報 EIP 11-1,2000

[谷口 2001] 谷口, 難波, 塩野入, "情報カプセル流通における利用者システム保護", 情処研報 DPS 101-18, 2001

[山本 2000] 山本, 寺西, 梅本："医療情報システムにおける情報開示制御方式", 情処研報 DPS 100-4, 2000

［難波 2000］難波, 谷口, 塩野入, 櫻井: "カプセル間通信による情報カプセル整理機構の検討", 情処 DPS ワークショップ, 2000

[木俵 1997] 木俵, 田中, 上原:"版権管理のための Java による画像データカプセル化", 情処研報 DBS 111-11, 1997

参考 WWW home page

[w1] Windows Media Rights Manager ：
http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp

[w2] MetaTrust Utility
http://www.intertrust.com/main/metatrust/index.html

[w3]RightsEdge (ContentGuard)
http://www.contentguard.com/

[w4] RightsShell
http://www.digigacha.com/setumei/index.html

[w5] Cryptlope/EMMS
http://www.ibm.com/software/cryptolope/
IBM Software : Security : Cryptolopes : Overview
http://www.ibm.com/software/emms/
IBM Software: Database and Data Management: IBM Electronic Media Management System

[w6]RealSystem ：*RealNetworks.com - RealSystem iQ*
http://www.realnetworks.com/realsystem/