

# 情報共有における認証・認可機能構成の一考察

宮木 一郎† 関 良明‡ 富士 仁‡ 平田 真一‡ 板倉 征男†

†情報セキュリティ大学院大学

〒221-0835 横浜市神奈川区鶴屋町 2-14-1

‡日本電信電話株式会社 NTT 情報流通プラットフォーム研究所

〒180-8585 東京都武蔵野市緑町 3-9-11

E-mail:

mgs075510@iisec.ac.jp , {seki.yoshiaki, fuji.hitoshi, hirata.shinichi}@lab.ntt.co.jp,  
itakura@iisec.ac.jp

あらまし： 近年、情報の電子化が浸透し、通信インフラの進展を受けて情報共有を行う環境が整備されてきた。また、製造業界や医療業界等では、作業の専門性の進化と共に作業の分業化が進んでおり、異なる組織間で必要な情報を共有する需要が高まってきている。そこで、本論文では、異なる組織間で情報共有を行う際に、集中的に認証・認可機能を提供する情報管理センタ（情報提供者と参照者の間で情報を仲介するエンティティ）のリスクに着目し、その低減対策を考察する。具体的には、情報提供者が認証・認可機能を有する構成の提案を行う。

## A Study on Constitution of Authentication and Authorization Functions in Information Sharing Systems

Ichiro Miyaki†, Yoshiaki Seki‡, Hitoshi Fuji‡, Shinichi Hirata‡, Yukio Itakura†

† Institute of Information Security

Tsuruyacho 2-14-1, Kanagawa-ku, Yokohama, 221-0835 Japan

‡ NTT Information Sharing Platform Laboratories, NTT Corporation

3-9-11 Midoricho, Musashino, Tokyo, 180-8585, Japan

E-mail: mgs075510@iisec.ac.jp , {seki.yoshiaki, fuji.hitoshi, hirata.shinichi}@lab.ntt.co.jp,  
itakura@iisec.ac.jp

Abstract: Recently, demand that shares necessary information with special evolution of work between organizations that advance the division of labor of work, and are different has risen in the manufacturing field and the medical treatment industry. Then, when information is shared between different organizations, it pays attention to the risk at the information management center (entity that mediates information among the informer and those who refer) that offers the attestation and the authorization function in a concentrated manner, and the decrease measures are considered in this thesis. Concretely, it proposes the composition where the informer has the Authentication and Authorization Functions.

### 1. はじめに

近年、情報の電子化とインターネットを中心

とする通信インフラの整備に伴い、多くの情報がネットワーク上でやり取りされるようになった。その反面、社会問題として、エレベータ

の保守問題[1]や、ガストープの発火問題[2]に見られるように必要な情報が共有されないことから、適切な対応が行われず問題を大きくしている事例が発生している。

そこで、情報共有が必要となるシーンを想定し、そこから課題を見出し、安全に情報共有を行うことができる仕組みについて検討を行う。

2章で提案する情報共有の要件を整理し、その要件の事例をあげて検証を行う。3章では、要件に対する課題を設定し、関連研究について述べる。4章では、設定した課題に対して関連研究を踏まえた提案を行う。

## 2. 情報共有の必要性と要件

「電子・電機業界における電子タグを利活用したトータルトレーサビリティ実証実験」[3]では、情報共有の必要性が説明されている。

製造事業者は、製品の製造を行ったあとに、販売店を通して消費者に製品が販売する。販売された製品は、製品を保守する保守事業者により製品の故障対応や定期メンテナンスが行われる。製品が一定期間使用された後に、消費者は製品を破棄処分し、製品の一部がリサイクル事業者によって再利用される。このようにひとつの製品が、複数の事業者によって異なる目的で取り扱われ、製造情報、保守情報を共有しておかないと製品に対して適切な対応ができないケースが出てくる[3]。前述の実証実験[3]では、システム的に、情報提供者と参照者の間で情報を仲介するエンティティ（以後、情報管理センタという）が必要であると述べられている。

この内容を踏まえると、情報管理センタは、各情報提供者から情報を預かり、情報を参照する者が誰であるかを特定し（認証）、その後どの情報にアクセスできるかを判断（認可）する機能を有する。また、複数の組織間で情報を共有することから、異なる組織に所属する属性の異なるユーザのために、開示範囲が異なる複雑なアクセス制御が情報共有の要件となる。

## 2.1 製造業における具体的な事例

具体的に報告書で記載されている製造業のフロー[3]を分析し事例を示す。ここでは、製造業における製品の障害情報に着目し、利用シーンを洗い出し、障害情報の利用状況を整理する。

### (1) 製造事業者が利用するケース (①)

- (ア) 製品事業者が故障した製品を送付され修理を行う場合
- (イ) 製品事業者で故障した製品の障害解析を行う場合
- (ウ) 製品事業者で製品開発を行う上での前の製品の障害情報を元にフィードバックを行う場合

### (2) 保守事業者が利用するケース (②)

- (ア) 現場で製品の故障を修理する場合

### (3) リサイクル事業者が利用するケース (③)

- (ア) 製品のリユースする際に製品に起きている障害情報からリユースに耐えうるかを判断する場合

上記①～③について、製品のライフサイクルからみた流れの中の位置づけを図1に示す。

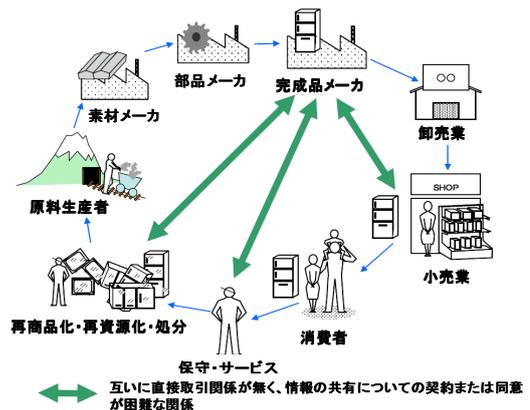


図1 障害情報の利用シーン[4]

「障害情報」に対して用途別にアクセスする情報の範囲を図2に示す。

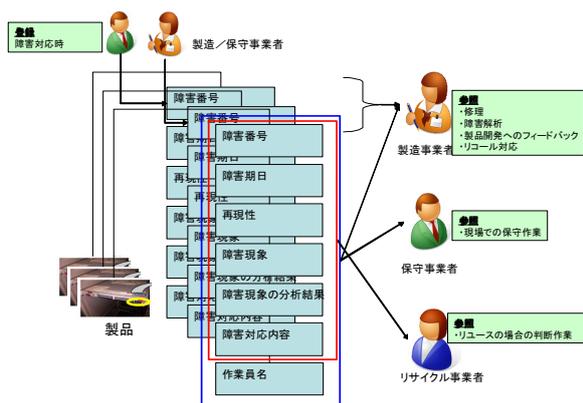


図 2 「障害情報」に対するアクセス

障害情報の中には、障害日付、再現性、障害現象、障害減少の分析結果、障害対応内容、作業員名が記載される。この情報において、保守作業を行う際には、過去の対応を聞くような場合に作業員名の記載を必要とするが、リサイクル事業者側にまで担当者名を見せる必要はない。よって、利用シーンと情報との突合せを行った結果として、「障害情報」を利用する目的とユーザの属性に応じて情報の参照範囲が異なることが分かる。

その結果、情報に対する複数の異なる組織に所属しユーザの属性に応じて複雑なアクセス制御が必要であることがわかる。

## 2.2 他の事例適用

医療業界における異なる組織を考えると、診療所、大学病院、専門家が他の病院、薬局があげられる。情報として患者情報と患者に関わる病歴を当てはめてみる。診療所から大学病院に紹介状を通して、今かかっている病気の診断をお願いする。大学病院では、レントゲンなどの画像診断を行う上で画像診断士のアドバイスを得るための専門家のいる大学病院に情報を開示する必要がある[5]。また、診断した結果から薬局はその指示に従い適切な薬を提供する。また、病気が治っても病気によっては、別の病気にかかった時に適切な対応を行ってもらうために前の病気の情報を診療所で知っ

ておく必要があると考えられる。よって、医療業界においても、複数の診療所や複数の大学病院等で情報共有するケースがあり、かつ用途に応じた情報に対するアクセス制御が必要であることがわかる。

## 3. 関連研究

2章で示した、情報管理センタでの機能を整理すると、情報管理センタでは、認証・認可の2つの機能を持つ。認証では、アクセスするユーザの認証とともにそのユーザの属性を保証する必要がある。認可では、異なる属性を持つユーザに応じて情報に対するきめ細かいアクセス制御を行う必要がある。

この機能を情報管理センタで集中的にすべて保持する場合、情報管理センタにおける情報漏洩リスクは非常に大きい。たとえば、情報管理センタにおける内部犯行による脅威や情報が集中することによる外部犯行の脅威が考えられる。

そこで、ここでは情報管理センタにおける情報漏洩リスクの中でも、情報管理センタの運用者が権限もないままに情報を参照できてしまうリスクに着目し、その低減を検討する。そのために、情報管理センタの認証・認可のそれぞれに関する関連研究を以下に記述する。

### 3.1 認証

認証として複数の異なる事業体と情報管理センタとの関係を考えて、Liberty Allianceでの認証情報を複数のグループ間で紐付けて制御する方式が考えられる。ただし、ユーザ認証そのものは規定されておらずIDとパスワードを用いたり証明書を用いたりすることができる。また、ユーザの属性情報に関しては、ID-WSF を利用することで属性流通させることができる[6]。

他に、証明書を利用してユーザ認証し、属性証明書をを用いてユーザの属性を保証する方式

もある[7]。属性証明書は公開鍵証明書と同様に、X.509 規定に準拠しているが、アクセス制限を行うために必要な個人の属性情報(名前、所属、部署、役職など)を含んでいるものである。

### 3.2 認可

認可に関する技術としては、コンテンツ流通や著作権管理において情報に対するアクセス制御を実現しており、情報を保護するという観点から類似の技術として着目した。著作権管理の著書[8]によると、情報の保護は、暗号機能によって情報を守りユーザに提供される。提供されたユーザは、その情報を解くために鍵を入手する場合とあらかじめ保存しておいた鍵を用いて鍵を導出する場合があります、その鍵を使用してその情報を復号する[4]。また、アクセスポリシーに従った細かな制御をデータ単位で行いたい場合は、著作権管理の論文[9]で示すようにコンテンツ管理情報と呼ばれるアクセスポリシーをカプセル化し、独自アプリケーションを用いて実現している。また、コンテンツ流通における論文[10]では、インターネット上の外部認証センタを用いて、必要な権限を入手することで情報へのアクセス制御を実現している。

## 4. 認証・認可の融合提案とその評価

### 4.1 提案

関連研究から、認証および認可のそれぞれに応じた技術的な解決案が提案されているが、個々が独立したものとして存在しているため、ここでは設定した課題に対して双方を融合した提案を行いシステムとしてリスク低減のための対策について提案する。

図 3 に今回のアプローチ方法について説明する。(1)は、認証と認可を情報管理センタで集中して行うモデルであり、情報提供者側のシステムとは独立して存在する。(2)は、認可の部分のみを情報提供側で行うモデル、(3)は、認証のみを情報提供側で行うモデルである。関連研究

から認証・認可の双方を同等に扱って評価したものはないため、ここでは、(2)の方向性と(3)の方向性を融合した(4)を提案する。(4)は、認証・認可を情報提供側で両方とも制御できるようにしたものである。

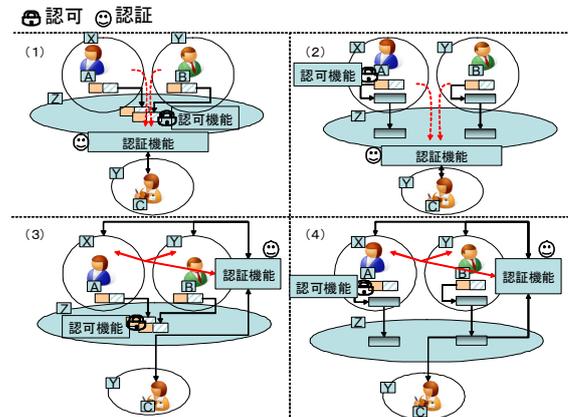


図 3 認証・認可における提案モデル

(4)について、3章で示した関連研究を加味し、以下に(2),(3)における技術的な方式を示す。

- 認証 1 : ユーザ認証は PKI 等を利用し、ユーザの属性を保証する方式として第三者機関である属性認証局を利用する方式
- 認証 2 : ユーザ認証は PKI 等を利用し、ユーザの属性は、ID-WSF を用いた形で実現する方式
- 認可 1 : 情報管理センタで預かった情報を自ら暗号化し、情報に対する保護は情報管理センタで行う方式
- 認可 2 : 情報提供者が、情報そのものに対して保護する方式

### 4.2 評価

4.1 で示した認証・認可のそれぞれを組み合わせたものを案として列挙する。この場合、認証 1,2 に加えて認証を情報管理センタで行う 3 通りと、認可 1,2 に加えて情報管理センタで認可を行う場合でかつ情報そのものを保護しない (ACL を用いたアクセス制御を行う) の 3 通りを組み合わせると 9 つのパターンが考えられる。

表 1 考えられるパターン

モデル	項番	認証	認可	説明
(1)	①	/	/	情報管理センタで認証・認可機能を持ち集中型で管理する。
(2)	②	/	1	共有情報は、情報管理センタが保護する。
	③	/	2	共有情報は情報提供者が保護する。
(3)	④	1	/	認証は、第三者機関で行う
	⑤	2	/	認証は、情報提供者側で行う
(4)	⑥	1	1	認証は、第三者機関で行い共有情報は、情報管理センタが保護する。
	⑦	1	2	認証は、第三者機関で行い、共有情報は情報提供者が保護する。
	⑧	2	1	認証は、情報提供者側で行い情報管理センタとの共有は、Liberty を用いて行い、情報管理センタが保護する形で対応する。
	⑨	2	2	認証は、情報提供者側で行い情報管理センタとの共有は、Liberty を用いて行い、共有情報は情報提供者が保護する。

脚注：斜め線：情報管理センタで実施

①～⑨に関して、リスク低減の程度を、情報管理センタに対して評価する。軸としては、情報漏洩リスクの低減を評価するにあたって、情報そのものの使用範囲（可用性）が劣ってしまえば、本来の情報を共有し活用することに反するためここでは、可用性と情報漏洩リスクで検証する。<sup>1</sup> 以下に評価 3 軸を定義する。

軸 1：可用性を示し、情報管理センタで利用可能、どこでも利用可能の 2 段階で評価する。

軸 2：情報漏洩リスクとして、認証・認可に利用するユーザ情報（ユーザが持つ属性情報を含む）

が情報管理センタでの情報の状態に応じて評価する。ユーザ情報の状態として、情報管理センタでそのものを保持する場合と第三者機関で保持する場合と情報提供者が保持する場合が考えられる。情報管理センタに限ってみると、ユーザ情報をまったく持たない場合が最も良いが、第三者機関で保持する場合は、システム全体としてリスクを第三者機関に負わせていることとなるため、情報提供者に保持させ、認証機能を実現することが望ましいことがわかる。

軸 3：情報漏洩リスクとして、共有情報が情報管理センタでの情報の状態に応じて評価する。共有情報の状態として、平文として情報管理センタで保持すると情報管理センタの管理者に対しては、権限がなくても参照されるリスクがある。情報に対して何らかの保護を実施する場合でも、情報管理センタでその保護を行う場合は、一旦情報提供者から平文で情報の提供を受けるため、一時的にも情報管理センタの管理者が参照できるリスクがある。よって、情報に対して、情報提供者が情報を保護することができれば、情報管理センタの管理者が、情報に対して参照するリスクが低減できると考えられる。

ユーザ情報と共有情報のそれぞれの情報漏洩リスクと可用性をあわせて 3 軸にしたものを図 4 に示す。縦軸をユーザ情報の情報漏洩リスクとし、上向きになるほどリスクが低くなるように表現した。横軸は、共有情報の情報漏洩リスクをあらわし、ユーザ情報と同様にリスクを表現する。奥行軸を可用性とし手前にくるほど可用性が高いと表現する。

<sup>1</sup> C.I.A. (Confidentiality, Integrity, Availability) の観点から見ると完全性も含める必要があるが、ここでは、情報に対する情報漏洩リスク（機密性）に着目し完全性については対象外で評価する。

（前提として完全性は同等とする）

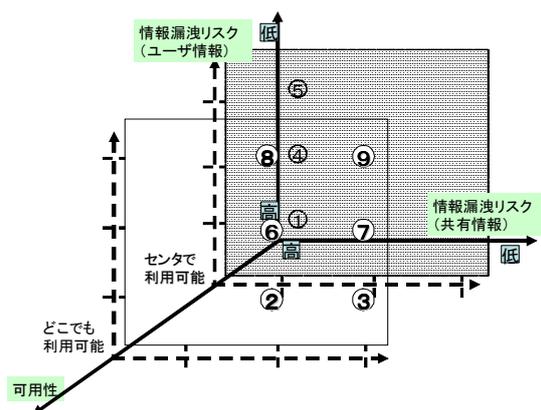


図 4 情報管理センタのリスク評価

図 4 により、可用性として前面に出ている側が、可用性として高くその中で情報における情報漏洩リスクの最も低いものを考えると⑨が最もすぐれているといえる。

## 5. まとめ

情報共有を行う上で、最近の社会問題になっている事例をあげ、異なる対等な組織間で情報を共有するために必要な要件を仮定した。また、そのようなシーンが、製造業や医療業界で適用可能な要件であることを確認できた。また、情報管理センタの機能として、認証・認可機能に着目し、情報管理センタが担う情報漏洩リスクを、可用性を失わずに低減することが可能かについて検討した。その結果、認証・認可を融合させた形で実現することの意味を、情報漏洩リスクと可用性の3軸で評価し、適切な考え方を導き出すことができた。

また、製造業における事例からもわかる通り、今回の想定要件の中で、異なる属性に応じて情報に含まれているデータに対して詳細なアクセス制御を実現する必要が不可欠であり、暗号技術で詳細な形で保護せずに最終的には独自アプリケーションを用いるケースが多い。そこで、情報に対するアクセスポリシーをそのままの条件で暗号化を施すことができれば、独自アプリケーションに頼らず情報に対して暗号機能のみを用いた保護が可能となる。このような

高機能暗号が、現在 ABE (Attribute Based Encryption) [11]に代表されるように、属性に応じた暗号化が可能な技術が出てきており、十分適用できるのではないかと考えられる。今後は、認証・認可機能を融合した形でのシステム提案をより具体的に行い、認証・認可のそれぞれに適用する技術の親和性についての検討や高機能暗号を用いたきめ細かなアクセス制御を実現し、最終的には、提案されたシステムが、従来のシステムと比較して技術的に優位であることを検証する必要がある。

## 【参考文献】

- [1] 国土交通省：「エレベータの保守業者等に関する実態調査」の結果について、  
[http://www.mlit.go.jp/report/press/house05\\_hh\\_000114.html](http://www.mlit.go.jp/report/press/house05_hh_000114.html)
- [2] 経済産業省：長期使用製品安全点検制度  
[http://www.meti.go.jp/product\\_safety/producer/shouan/07kaisei.html](http://www.meti.go.jp/product_safety/producer/shouan/07kaisei.html)
- [3] 社団法人 電子情報技術産業協会：平成 17 年度エネルギー使用合理化 電子タグシステム開発調査事業 「電子・電機業界における電子タグを活用したトータルトレーサビリティ実証実験」,(2006)
- [4] 次世代電子商取引推進協議会：平成 19 年度 情報共有基盤整備報告書,(2008).
- [5] エム・イー振興協会：医療機器システム白書 2008～2009,(2008).
- [6] Susan Landau, Sun Microsystems : Liberty ID-WSF Security and Privacy Overview Version: 1.0,  
[http://www.projectliberty.org/resource\\_center/specifications/liberty\\_alliance\\_id\\_wsf\\_2\\_0\\_specifications\\_including\\_errata\\_v1\\_0\\_updates](http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates)
- [7] 独立行政法人情報処理推進機構セキュリティセンタ：PKI 関連技術解説”  
<http://www.ipa.go.jp/security/pki/>
- [8] 今井秀樹, 五十嵐達治, 遠藤直樹, 川森雅仁, 古原和邦, 三瓶徹, 中西康浩：ユビキタス著作権管理技術’ 東京電機大学出版局, PP.13-32,(2006).
- [9] 加賀美 千春, 森賀 邦広, 塩野入 理, 櫻井 紀彦：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, マルチメディア通信と分散処理, 97-18, コンピュータセキュリティ, PP.8-18(2000).
- [10] 関 亜紀子, 亀山 渉：コンテンツ循環における権利継承の自動化, 情報処理学会論文誌, Vol.48, No5, pp.1952-1964,(2008).
- [11] V. Goyal, O. Pandey, A. Sahai, and B. Waters : Attribute-based encryption for fine-grained access control of encrypted data., In Proceedings of the 13th ACM conference on Computer and Communications Security (CCS 2006), PP. 89-98,(2006).