# アクセス制御のための機械可読サービスポリシー文書

佐藤 周行 † 谷本 茂明 ‡ 金井 敦 §

† 東京大学
schuko@satolab.itc.u-tokyo.ac.jp

‡ 千葉工業大学
shigeaki.tanimoto@it-chiba.ac.jp

§ 法政大学
yoikana@hosei.ac.jp

**あらまし** アクセス制御では，アクセス先のサービスポリシーのチェックが必要であるが，従来，アクセス時のロジックに組み込まれることなく，利用者に提示して同意を得る，または事前の契約等でのチェックの中で行うなど，メタなプロセスとして実現されることが普通であった．本論文では，利用側の判断ロジックをあらかじめ提示することを前提とし，サービスポリシーを機械処理可能な状態でアクセス先から得，評価することで一連の処理を自動化するための，機械可読・機械処理可能な形式でのサービスポリシー文書を定義することを試みる．具体例として電子証明書の CP/CPS, プライバシーポリシーをあげ，XML のスキームを提案する．
Keywords: アクセス制御, サービスポリシー, XML

# XMLed Service Policy Documents for Access Control

SATO Hiroyuki† TANIMOTO Shigeaki‡ KANAI Atsushi§

†The University of Tokyo
schuko@satolab.itc.u-tokyo.ac.jp

‡Chiba Institute of Technology
shigeaki.tanimoto@it-chiba.ac.jp

§Hosei University
yoikana@hosei.ac.jp

**Abstract** Access control inherently requires verification of service policies of peers. However, this kind of verification is usually performed in the form of out-of-band ways such as user's explicit giving consent, and offline contracts. In this paper, we propose XMLed service policy documents that clients automatically verify by obtaining from a peer. CP/CPS for digital certificates and privacy policies are given as two examples of XMLed policy documents whose schemes are defined in this paper.
Keywords: access control, service policies, XML

## 1 はじめに

組織の提供するサービスについてのポリシー文書の重要性が急速に高まりを見せている．サービスポリシーに限らず，関連するプライバシーポリシーやセキュリティポリシーを加えると，現在では，サービス開始時にはなんらかのポリシーの提示がなされているのが普通になった．現在のネット環境では，アクセス先の信頼度が問題にされはじめており，消費者が納得できるような形でサービスポリシー他を提示することの重要性は今後ますます高まると考えられる．

特にアクセス制御では，アクセス先のサービスポリシーのチェックが必要であるが，従来，ア

クセス時のロジックに組み込まれることなく，利用者に提示して同意を得る，または事前の契約等でのチェックの中で行うなど，メタなプロセスとして実現されることが普通であった．代表的な形としては，ソフトウェアのインストール時に使用許諾条件を示し，それに同意することがインストールの条件になる，またはあらかじめ Web 上でサービスポリシーを提示しておくことなどが広く行われている．

しかし，サービス形態の多様化や消費者の要求の多様化，また消費者のリテラシーの幅などにより，この形には様々な問題が指摘されている．一つは「同意の有効性」に疑問がつくケースがみられることである．大部の契約書を見せて，クリックを迫るようなインタフェースの有効性は前から問題にされている．対抗して「自明なものを表示しない」「標準的なものを標準的な形式で提供する」ことは，対人間の効果にフォーカスしたものであり，必要なことを必要なだけ記述することを目的にはしていない．さらに，消費者が，対費用効果を考え，サービスメニューの多様化を求めるようになった．利用者が，特殊な条件をサービスの際に要求することもこれに含まれる．サービスの提供レベルに段階をつけて，プライシングに反映させることは普通に行われてきた．電子証明書の CA でも，現在は主に EV と WTCA の二つの認定レベルが存在する．WTCA はさらに組織認証とドメイン認証の区別が存在するが，現在では CA の CP/CPS を確認することでしか区別できない．

これら，サービスの提供レベルの差を保証するのが監査である．上記の電子証明書の CA の認定プログラムが独立監査を必須としているのは監査が認定に本質的であることを示している．さらに，US ICAM による IdP の 4 レベルモデルの策定も，レベル 2 以上は外部/独立監査を必須にしている．監査は，レベルが一つだけのもの（e.g. ISMS, プライバシーマーク）でも要求されている．ただし，認定業務の中でも，業界の自主基準で運用しているものもあり，独立監査が必ずしも要求されていないものもある．

監査の重要ポイントは（ガバナンスを含む）ポリシーと運用である．ここでいうポリシーは特に内部統制のためのポリシーである．この二つが正しく運用されていることが保証されてはじめて（対外的な）サービスポリシーの有効性が保証される．その意味で，サービスポリシーはその運用に対する監査と一体となって評価されるべきものである．

本論文では，上記監査によってサービスポリシーの精度が保証されているとしたうえで，サービスポリシーの流通と消費のスキームを考える．具体的には，ポリシー文書をプログラムで処理することを可能にして，大部なポリシーについても「有効な同意」の方法を提供し，さらに，プログラムで詳細にポリシーを解析することを可能にしてポリシーの細かい点の評価によるサービスの層化を可能にするものである．このために本質的な，ポリシー文書の機械可読形式による提供とその形式を提案する．具体例として電子証明書の CP/CPS, プライバシーポリシーをあげ，XML のスキームを提案する．

機械可読形式のポリシー文書の用意は従来のものでは P3P が先導的な役割を果たしてきた．これはプライバシーポリシーを対象とし，人間に対して有効に文書を提示するためのものに加え，プログラムが処理することを可能にして，様々な判断を行うことを目的とするものである．同じ P3P の中の Compact Privacy Policy では，プログラム（ブラウザ）に対してポリシー判断ができる形でプライバシーポリシーを送出することを提案している．我々は，これをサービスポリシーに一般化した形式を提案する．サービスにアクセスする際にサービスポリシーの（プログラムによる）評価をアクセス制御に含めることで，アクセス制御を拡張することができる．また．ユーザエージェント対 Web サーバに限定せず，サーバ間でポリシーを交換することを想定する．

本論文の構成は以下のとおりである．2 節では，機械可読形式ポリシー文書の形式の提案を行う．XML 要素と属性の標準語彙について論じる．3 節では，事例研究として RFC3647 に基づいた CP/CPS の XML 化と有力な企業が出しているプライバシーポリシーをもとにしてプライバシーポリシーの XML 化を試みる．4 節で

は関連研究を示し，5 節で結論を述べる．

# 2 機械可読形式ポリシー文書の形式

ポリシー文書は，プログラムによって処理・消費されることを前提として XML の DTD または XML スキーマを定める．特に DTD では，XML 要素の木構造と属性の様式を定めることが必要である．

## 2.1 方針 : 従来のポリシー文書との互換性

機械可読・機械処理可能化にあたり，従来のポリシー文書を復元できることは大前提である．以後の事例研究では，RFC3647 [2] とプライバシーポリシーをあげるが，これらはいずれも人間に理解されることを前提としてセクション構成等の文書構造を持っている．本論文の方針として，参考となる元文書の構造を自然に反映できる XML 木構造を構築することを考える．実は，属性に用いる標準的な語彙を定めることで，定められた語彙から構造付きの文書を復元できることは明らかである．しかし，ポリシーを定義するときには，定義する人間で従来の文書構造を参照することが自然であることから，上の方針を取ることにした．

さらに，できるだけ高い精度で元文書の（内容面での）復元ができることを方針とする．このためには，属性の定義において，ポリシーに必要な標準的な語彙を提案することも方針とした．

## 2.2 XML 要素の木構造

XML 要素は，機械可読化の対象としたポリシー文書のセクションヘッダと一対一に対応させる．さらに，木構造はセクション構造をそのまま踏襲することにする．これによって，方針の一つである元文書の復元可能性が，セクション構成については自明になる．

## 2.3 属性の標準語彙

標準語彙を定めることで，属性の種類を固定し，ポリシー文書の消費側に便宜を図ることができる．このためには DTD において ENTITY 型の宣言および各 ENTITY の定義が必要である．

しかし，利用シナリオがある程度想定できるサービス以外にこれを適用すると，将来の利用シナリオに対応できない．

本論文では，CDATA 型で属性定義をできるようにしているが，事例研究で見るようにその語彙をある程度標準化することを想定している．これを ENTITY (ENTITIES) 型に整理した形で提供することは今後の課題である．

## 2.4 ポリシー文書の消費

サービス受け入れに際し，アクセス元を評価する枠組として，オンラインでは Web ブラウザが電子証明書のルート証明書が証明書ストアに格納されているかどうかのチェック，アクセスフェデレーション内で．アクセス IdP が US FICAM の定める，RP の要求する LoA を取得しているかをアサーション内の記述でチェックする枠組がすでにある．これからもわかるように，従来の枠組は評価を第三者の認定を得ているかどうかに帰着させるのが一般的であった．提案の枠組は，これら認定とは独立にポリシーそのものを評価（消費）の対象とする．

ポリシー消費としては，人間の理解を前提とした文書への変換や条件を指示し，その条件にポリシー文書が適合しているかどうかの検証があげられる．具体的に [7] にユースシナリオをあげている．ここでは，ポリシーそのものを対象とした評価エンジンの構築を前提としている．

# 3 事例研究

## 3.1 電子証明書の CA の CP/CPS

### 3.1.1 元になるポリシー文書

CP/CPS は整備が進み，現在では書式が RFC3647 に準拠しているものがほとんどである．したがっ

て，RFC3647 のセクション構造をそのまま用いることにした．さらに，属性値については，セクション構成との関係で以下のことを観察した．

- 規定に対して Yes/No で決められるもの．(e.g. Rekey のセクションでは，Rekey を行うかどうかの規定をする必要があり，そのための属性は Yes/No で与えられる．)
- 規格で定めがあるもの．(e.g. 証明書の用途．たとえば以下のように定める)

```
<CertificatesissuedtoOrganizations
  issue="yes"
  usage="server:o:wildcard"/>

<CertificatesissuedtoIndividuals
  issue="yes"
  usage="client authentication:\
  code signing:smime:signing"/>
```

- 種類を列挙するもの．(e.g. 物理セキュリティのための方策．たとえば以下のように定める)

```
<PHYSICALCONTROLS>
<SiteLocationandConstruction
   type="slab to slab barriers:\
   electronic control access system:\
   alarmed dorrs and video monitoring:\
   security logging and audits:\
   card key access">
```

最初の二つについては ENTITY (ENTITIES) 型で属性を指定することは容易であることを確認して，その語彙と範囲の策定もも含めて将来の課題とし，まずは CDATA 型でこれらを指定することにした．

#### 3.1.2 DTD

DTD を抽出する際には，実際に運用されている CA の CP/CPS を参照して，属性の語彙を検討した．結果を [12] にあげ，本論文では，RFC3647 で定める 1 章と 2 章に対応する構造を図 1 に示す．DTD の規模は，要素数 285, 属性数 165 になった．

#### 3.1.3 XML 化の効用

電子証明書で採用されている Web トラストモデルに加えて，電子証明書の中で規定されている情報は有用であるが，それでも OV か DV かの区別やワイルドカードを許す証明書を発行するかどうかについては CP/CPS の記述を検証しなければならない．それらが評価の対象になる場合に，この機械可読・機械処理可能化が有効である．

### 3.2 プライバシーポリシー

#### 3.2.1 元になるポリシー文書

プライバシーポリシーは，プライバシーに関する現在の環境の急速な変化に対応するために一部の組織で本格的な整備が進められ，改訂の頻度も小さくない．プライバシーに関する認定制度として，日本ではプライバシーマーク [10] があり，JIS Q15001 [5] を根拠として JIPDEC が運用している．JIS Q15001 は，組織が収集保有するプライバシー情報を保護するための規格である．しかし，RFC3647 と異なり，JIS Q15001 の規程の各項を実現する項目の列挙という形で一般の組織でプライバシーポリシーが定められることは一般的ではない．

現在では，むしろ，利用者に対し，提供サービスにおいて，利用者のプライバシー情報の何をどう利用するかの説明，つまりサービスポリシーの一部としてのプライバシーポリシーが重要な部分であると理解されている．

ポータルを提供する企業では，プライバシー情報を利用した広告を含む様々なビジネスを展開するのが一般的であり，プライバシーポリシーを適切な粒度で開示することで展開ビジネスの正当性を主張するとともに，利用者の安心を得ることができる．しかし，プライバシー情報の収集利用にそれほど興味を示さず，結果としてプライバシーポリシーがごく簡単になっている組織も存在する．さらに，利用者に対して ID を提供するサービスでは，他のサービスに対して ID を含む個人情報をどのような形式で提供するかについての規程が必要になる．

```
<!ELEMENT CPCPSrfc3647 ((INTRODUCTION, PUBLICATIONANDREPOSITORYRESPONSIBILITIES,
     IDENTIFICATIONANDAUTHENTICATION, CERTIFICATELIFE-CYCLEOPERATIONALREQUIREMENTS,
     FACILITYMANAGEMENTANDOPERATIONALCONTROLS, TECHNICALSECURITYCONTROLS,
     CERTIFICATECRLANDOCSPPROFILES, COMPLIANCEAUDITANDOTHERASSESSMENTS,
     OTHERBUSINESSANDLEGALMATTERS))>
<!ATTLIST CPCPSrfc3647
name CDATA #REQUIRED
>
<!ELEMENT INTRODUCTION (#PCDATA | OVERVIEW | DOCUMENTNAMEANDIDENTIFICATION |
            PKIPARTICIPANTS | CERTIFICATEUSAGE | POLICYADMINISTRATION |
            DEFINITIONSANDACRONYMS)*>
<!ELEMENT OVERVIEW (#PCDATA)>
<!ELEMENT DOCUMENTNAMEANDIDENTIFICATION (#PCDATA)>
<!ATTLIST DOCUMENTNAMEANDIDENTIFICATION
name CDATA #IMPLIED
>
<!ELEMENT PKIPARTICIPANTS ((CertificationAuthorities, RegistrationAuthorities,
            Subscribers, RelyingParties, OtherParticipants))>
<!ELEMENT KEYPAIRANDCERTIFICATEUSAGE ((SubscriberPrivateKeyandCertificateUsage,
      RelyingPartyPublicKeyandCertificateUsage))>
<!ELEMENT SubscriberPrivateKeyandCertificateUsage (#PCDATA)>
<!ATTLIST SubscriberPrivateKeyandCertificateUsage
type CDATA #IMPLIED
>
<!ELEMENT RelyingPartyPublicKeyandCertificateUsage (#PCDATA)>
<!ATTLIST RelyingPartyPublicKeyandCertificateUsage
type CDATA #REQUIRED
>
<!ELEMENT POLICYADMINISTRATION ((OrganizationAdministeringtheDocument, ContactPerson,
       PersonDeterminingCPSuitabilityforthePolicy, CPApprovalProcedure))>
<!ELEMENT OrganizationAdministeringtheDocument (#PCDATA)>
<!ATTLIST OrganizationAdministeringtheDocument
name CDATA #REQUIRED
>
<!ELEMENT ContactPerson (#PCDATA)>
<!ATTLIST ContactPerson
name CDATA #REQUIRED
>
<!ELEMENT PersonDeterminingCPSuitabilityforthePolicy EMPTY>
<!ELEMENT CPApprovalProcedure (#PCDATA)>
<!ELEMENT DEFINITIONSANDACRONYMS EMPTY>
```

図 1: 機械可読 CP/CPS の Introduction と Publication and Repository Responsibilities の章を定める DTD の一部

以上，プライバシーポリシーは，企業のビジネス形態によって規定のされ方が大きく変わり，特定の 1 個の ISO (JIS) や RFC のような規格はなじまないと考えることができる．

以上を考え，ここではポータルサービスを提供する代表的なネット企業（複数）の提示するプライバシーポリシーから関連する部分を抽出することにした．

なお，ID を提供するサービスは，現在アクセスフェデレーションの形で一般的になっていて，このサービス形態を想定したプライバシーポリシーの検討は重要である．これについては今後の課題としたい．

### 3.2.2 DTD

プライバシーポリシーの XML 化では先行例として P3P [3] があり，本論文と目的と手段を共有している．本論文では，P3P の定義とは独立に，現在採用され公開されているプライバシーポリシーから DTD を作ることにした．

今回提案する DTD のセクション立てを図 2 のように定める．

属性の値については，参考にしたポータル企業で具体的にあげられていた語彙を収集した．XML 要素 InformationYouGiveUs と LogInformation の属性 type と when に使われた値をその例として以下ににあげる．この標準化については今後の作業としたい．

**InformationYouGiveUs**

type=”name:email:phone:creditcard”

when=”registration”

**LogInformation**

type=”queries:phonelog:ipaddress:
eventinformation:owncookies”

when=”atservice”

DTD の規模は要素数 25，属性数 27 になった．

### 3.2.3 XML 化の効用

プライバシーポリシーは，利用者の同意のプロセスを本質的に含み，また改訂の頻度が高いので，ポリシーの理解の補助のためのプログラムによる処理は有用である．利用者に表示することを目的とするなら，P3P 対応文書への変換，Standard Label [6] 対応文書への変換等が考えられる．また，利用者側にとって不適切な規程を含むものをフィルタリングすることにも使用できる．

## 4 関連研究

ポリシーを機械可読・機械処理可能にし，プログラムによる判断を可能にすることを目的としているものには P3P[3]，さらに P3P Compact Policy がある．ブラウザプラグインに対するガイドラインが [4] で提案されている．ごく初期には，プラグインも提供されていたことが観察できる（e.g. IE 6.0 までに対する Privacy Bird plugin）．

本論文は，プライバシーポリシーについては目的と手段を P3P と共有する．組織の内部統制が強調される現在，サービスポリシー規程一般にこれを拡張するのは意味がある．本論文で述べた事例研究の他に，クラウド SLA の XML 化を検討したものとして [9] がある．

規程のテンプレートとしては電子証明書に対する RFC3647[2] が標準例である．Kantara の Standard Label[6] は，プライバシーポリシーについて，表示の正規化を意図している．また，日本においても，政府部内で情報セキュリティ対策のための規程群の統一基準を示す動きがある [11].

ポリシーとその運用は認定制度と深い関係がある．電子証明書については，各 CA は RFC3647 に準拠した CP/CPS を定めながら，WTCA[8] や EV[1] の定める評価基準に従って運用を行うことでそれぞれの認定を得ている．また，日本では JIPDEC の運用するプライバシーマーク [10] の認定基準が JIS Q15001[5] になっている．

ポリシーを機械可読・機械処理可能にしたうえでの利用シナリオとそのトラストモデルが [7] で論じられている．

```
<!ELEMENT PrivacyPolicy (Introduction, RequestedData,Purpose,AdditionalTerms,
                         AccessToPII,Redistribution,InformationSecurity,
                         Enforcement,Change)>
<!ELEMENT Introduction (#PCDATA)>
<!ELEMENT RequestedData (InformationYouGiveUS,InformationWeGetatService)>
<!ELEMENT InformationYouGiveUS EMPTY>
   <!ATTLIST InformationYouGiveUS type CDATA>
   <!ATTLIST InformationYouGiveUS when CDATA>
<!ELEMENT InformationWeGetatService (DeviceInformation,LogInformation,LocationInformation)>
<!ELEMENT DeviceInformation (#PCDATA)>
   <!ATTLIST DeviceInformation type CDATA)>
<!ELEMENT LogInformation (#PCDATA)>
   <!ATTLIST LogInformation type CDATA)>
   <!ATTLIST LogInformation when CDATA)>
<!ELEMENT LocationInformation (UniqueApplicationNaumber,LocalStorage,
                               CookiesAndAnonymousIdentiifers)>
<!ELEMENT UniqueApplicationNaumber (#PCDATA)>
   <!ATTLIST UniqueApplicationNumber when CDATA>
<!ELEMENT LocalStorage (#PCDATA)>
   <!ATTLIST LocalStorage type CDATA>
   <!ATTLIST LocalStorage when CDATA>
<!ELEMENT CookiesAndAnonymousIdentiifers (#PCDATA)>
   <!ATTLIST CookiesAndAnonymousIdentiifers type CDATA>
   <!ATTLIST CookiesAndAnonymousIdentiifers when CDATA>
<!ELEMENT Purpose (#PCDATA)>
   <!ATTLIST Purpose type CDATA>
<!ELEMENT AdditionalTerms (Transparency,InformationShare)>
<!ELEMENT Transparency (#PCDATA)>
   <!ATTLIST Transparency type CDATA>
<!ELEMENT InformationShare (#PCDATA)>
<!ELEMENT AccessToPII (#PCDATA)>
   <!ATTLIST AccessToPII access CDATA>
   <!ATTLIST AccessToPII correct CDATA>
   <!ATTLIST AccessToPII delete CDATA>
   <!ATTLIST AccessToPII fee CDATA>
<!ELEMENT Redistribution (WithConsent,WithDomainAdm,ExternalProcessing,Legal)>
<!ELEMENT WithConsent (#PCDATA)>
   <!ATTLIST WithConsent type CDATA>
   <!ATTLIST WithConsent cond CDATA>
<!ELEMENT WithDomainAdm (#PCDATA)>
   <!ATTLIST WithDomainAdm type CDATA>
<!ELEMENT ExternalProceesing (#PCDATA)>
   <!ATTLIST ExternalProcessing type CDATA>
   <!ATTLIST ExternalProcessing cond CDATA>
<!ELEMENT Legal (#PCDATA)>
   <!ATTLIST Legal jurisdiction CDATA>
<!ELEMENT InformationSecurity(#PCDATA)>
   <!ATTLIST InformationSecurity usertype CDATA>
   <!ATTLIST InformationSecurity vendortype CDATA>
<!ELEMENT Application (#PCDATA)>
   <!ATTLIST Application incltype CDATA>
   <!ATTLIST Application excltype CDATA>
<!ELEMENT Enforcement (#PCDATA)>
<!ElEMENT Change (#PCDATA)>
   <!ATTLIST Change type CDATA>
```

図 2: プライバシーポリシーの DTD

## 5 結論

本論文では，機械可読形式ポリシー文書の形式の提案を行った．XML で記述することにし，XML 要素と属性の標準語彙について考察した．さらに事例研究として RFC3647 に基づいた CP/CPS の XML 化と有力な企業が出しているプライバシーポリシーをもとにしてプライバシーポリシーの XML 化を試みた．この 2 つの例は，規程のテンプレートがデファクトで存在する分野と，しない分野である．前者については，XML 要素の規定は自然にできることがわかった．さらに，標準語彙の策定のためには，できるだけ多くの記述を反映するために，現在存在する規程類の収集も重要であることがわかった．

今後は，多くの例の収集による DTD の精密化とともに，利用シナリオを具体的に提示して，提案した枠組の有効性を示すことが課題である．

## 参考文献


[1] CA/Browser Forum: Guidelines For The Issuance And Management Of Extended Validation Certificates, version 1.5.0, 2014.

[2] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.: Internet X.509 Public key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, 2003.

[3] Cranor, L, Langheinrigh, M., Marchiori, M., Presler-Marshall, M., Reagle, J.: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendatation, 2002.

[4] Cranor, L.: P3P 1.1 User Agent Guidelines, W3C Working Draft, 2003.

[5] JIPDEC: JIS Q15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン, 2006.

[6] Kantara: The Standard Information Sharing Label, http://standardlabel.org/v/0.4, 2012.

[7] SATO, H., TANIMOTO, S., KANAI, A.: A Policy Consumption Architecture that enablesDynamic and Fine Policy Management, Proc. 3rd ASE International Conf. CyberSecurity 2014.

[8] Sheehy, D., Greene, M., Lundin, M., Ward, Jeffrey: Trust Service principles and Criteria for Certification Authorities, version 2.0, 2011.

[9] 横谷 百合, 金井 敦, 谷本茂明, 佐藤周行: ダイナミックなクラウド選択のための SLA の XML 化に関する提案, 2014-DPS-158(47), 2014.

[10] http://privacymark.jp/ (LAD: 2014/08/21)

[11] http://www.nisc.go.jp/active/general/kijun26.html (LAD: 2014/08/21)

[12] http://www-sato.cc.u-tokyo.ac.jp/PKIproject/sample3647-x.dtd