



XDI/XRI Primer

(株)野村総合研究所 インターネット事業部
個人情報保護チーム 崎村夏彦
(Certified Risk Manager)
(XDI.ORG副理事長)

❖ RSAの定義

- 企業セントリックな見方
- デジタルな身元情報
- デジタル身元情報は永久的なものではありません。たとえば、社員が新規採用されるとそのデジタル身元情報が作成され、社員が退職するとそのデジタル身元情報は退職日をもって失効します

❖ NRIの定義

- 現代社会では「私」に関する情報、すなわち個人情報があちこちに散在する。クレジット会社には「私」の購買履歴、区役所には「私」の住民登録、勤務先には「私」の健康保険の情報があるといった具合である。「私」であることを同定でき、それをデジタル情報として保管したものは「デジタルアイデンティティ」と呼ばれる。
- ただし、「私」は人にかぎらず、組織、物、概念でも良い。

❖ RSAの定義

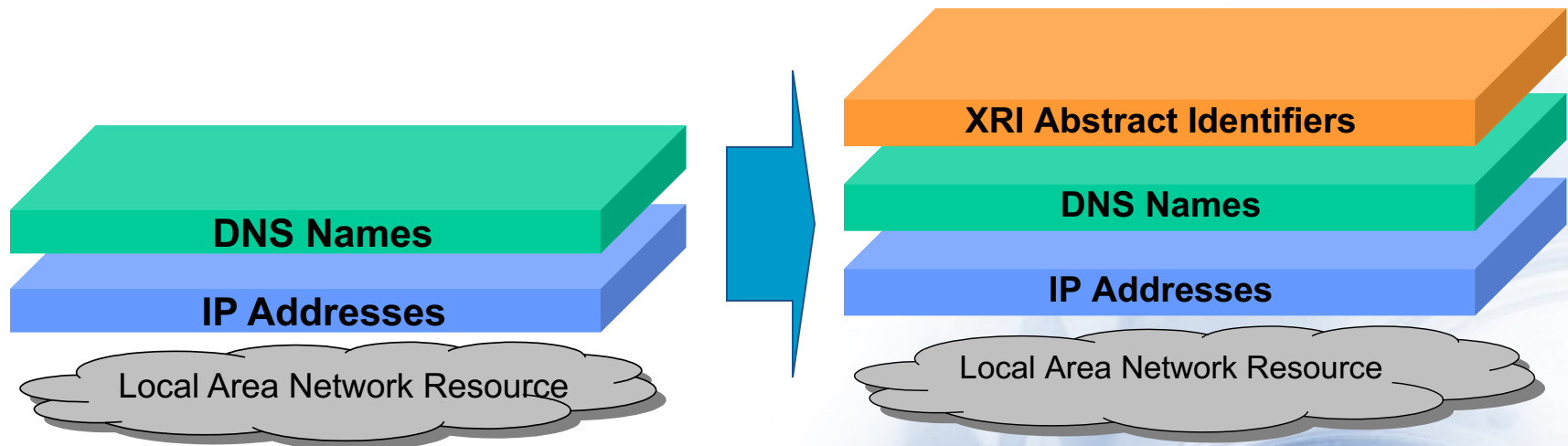
- デジタル身元情報の作成から廃棄に至るまでの全過程を維持管理できることであり、併せて電子的なリソースへのアクセスに関する組織のポリシーが遵守されるようにすること

❖ NRIの定義

- デジタルアイデンティティの作成から廃棄に至る全過程を管理し、その指し示す電子的リソースへのアクセスに関して、アイデンティティオーナーのポリシーが遵守されるようにすること

- ❖ 安定して指し示すことが出来ないものを管理対象には出来ない。
- ❖ たとえば、2者間の契約は、その2者と、契約自身、および契約が指し示す事象や物を、時を越えて指し示すことが出来なければ成立しない。
- ❖ 現実の社会では、人やモノの存在と物質的安定性がそれを担保している。
- ❖ ネットワーク上では、実体が無いから、これに変わるものが必要
- ❖ 長期間安定している人・物・概念とそれらの属性の識別子＝Identifierが必要
- ❖ IP Address, DNS name, URI いずれもこの要求を満たさない

現在の2階層から、抽象レイヤーを入れた3階層モデルに組み替える必要



XRIの目的は、こういった要件を満たす、
Abstract Identifier の syntax と resolution
mechanism を定義すること。

❖ [xri-requirements-and-glossa...](#)

- <http://www.oasis-open.org/apps/org/workgroup/xri/download.php/2523/xri-requirements-and-glossary-v1.0.doc>
- いろいろ書いてあるが、要は：
 - 長期間安定したIDと、短期で使い捨てに出来るIDとを組み合わせたい
 - もちろん、名前解決して、物理的な場所に到達して値を取得したい
 - 人にも物にも抽象的概念にもIDを振りたい
 - リソースだけでなく、リソースの属性にもIDを振りたい
 - 一つのIDを、異なるコンテキストで評価することによって、違う値を取り出すことができるようにしたい
 - バージョンコントロールしたい(特に同期をするために重要)
 - 最初から国際化を考えておこう
 - デリゲーションを可能にし、できるだけ分散化できるようにしよう
 - セキュリティとプライバシーを最初から考えておこう

- 人や物だけでなく、その属性までも識別子でポイントし、RESTスタイルでメタデータおよびデータにアクセスできること。
- それにあたってはアクセスコントロールが可能なこと。
- アクセスコントロールは、契約法上意味がある「契約」として結ばれること。(これによって、国境をまたがった取引でも可能になる。)
- データをリクエストするときには、契約案を提示し、契約締結によってデータが取得できる形とすること。
- 契約締結に当たっては、事前にルールを設定しておき、自動契約も可能であること。
- 自動契約ができなかった場合には、契約リクエストを個人に対して提示することができること。
- この契約リクエストは、個人が読んでわかるような形にすること。
- 契約は、個人・法人に対してのみでなく、グループに対しても適用することができること。(multi-party contract)

- どうしても必要な場合以外は、個人を特定しないですむように、偽名ベースでの情報交換が可能であること。
- 逆に、実名性が必要である場合には、永続的かつ一意な識別子で互いをポイントできること。
- その識別子が指し示すデータの過去分にもアクセス可能であること。
- 各個人、法人、物に関しては、第三者による Certification の利用が可能であること。
- 各自の identity の運用レベルに関して、第三者による監査と certification が可能であり、その情報が利用可能で、これを使って自動契約が可能であること。
- 各 identity に関して、Reputation Service が利用可能で、これを使って自動契約が可能であること。

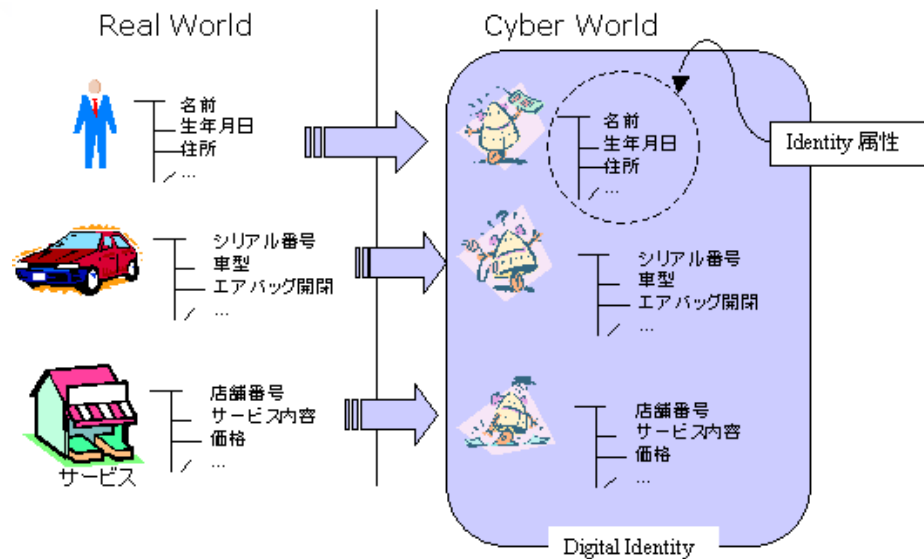
抽象的には...

❖ 任意のサービス間で

- 互いに認証をして
 - パーミッションベースで
 - 任意のデータの交換を行い
 - そのログを残す
- システム

❖ Digital Identity の例

- 自然人(個人のネット上でのエージェント)
- 法人(法人のネット上でのエージェント)
- 物(車などのネット上での表現)
- サービス



- ❖ **Identity**の数は莫大になる。したがって、分散データベースで無ければならない。
- ❖ 永続的識別子を渡すことは、プライバシーリスクになる可能性がある。そのため、できるだけ流したくない。偽名を受け取って、その存在や信用を証明するサービスが必要である。
- ❖ 識別子は国際化されていなければならない。
- ❖ 識別子は**URI**であれ。
- ❖ 得られたデータは、(スキーマ拡張の必要が無い)一定のフォーマットで **envelope** されていること。
- ❖ これにあたり、ボキャブラリとしての抽象識別子が整備されること。

❖ 適切な識別子(Identifier)を使い分け、そのマッチングの許可に注意を払えば、個人情報マーケティング他にはそれほど必要ないはずだ！

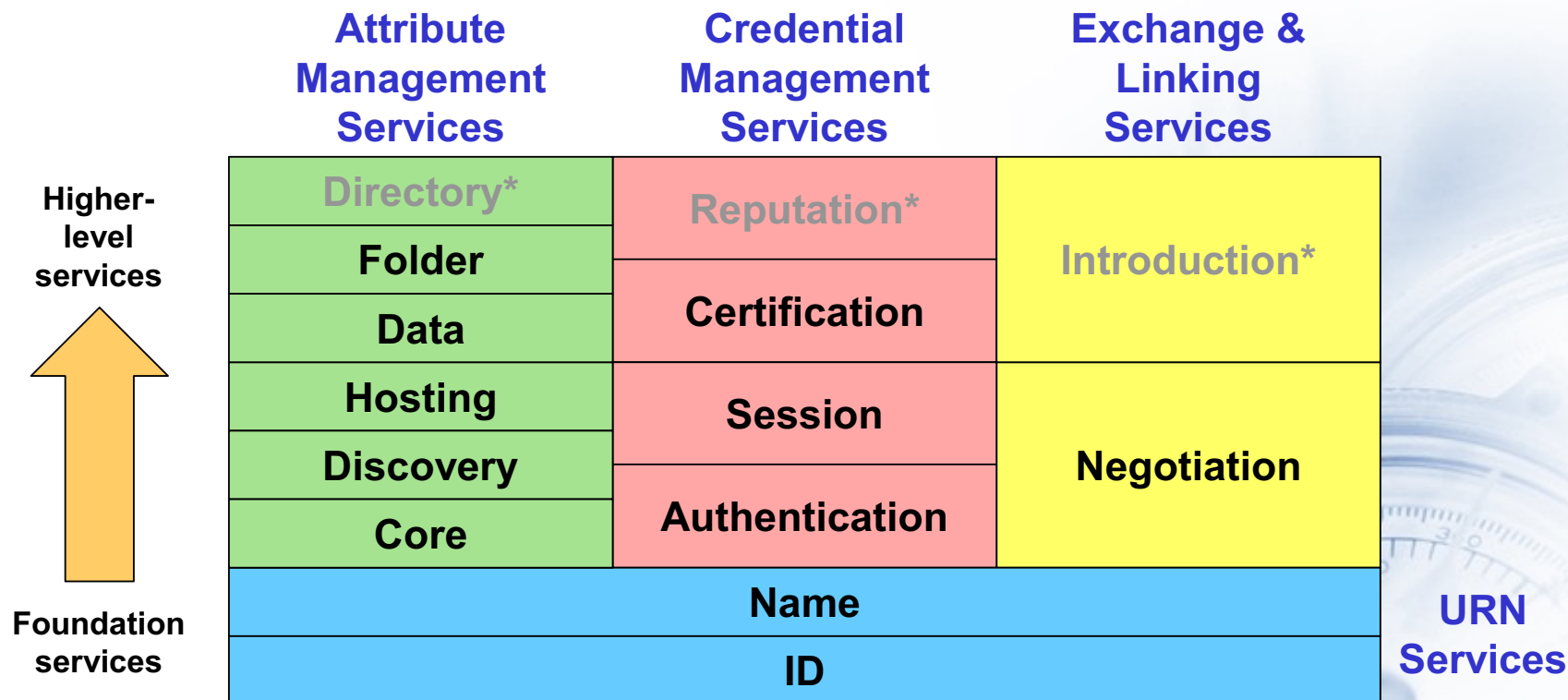
識別子	実名性	仮名性	匿名性
永続性	本名など	ペンネーム	
一時性		その場限りの ニックネーム	

個人情報

リスク低減情報

❖ 1991以来のXNSの活動を引き継ぐ形で開始

- XNS ver.1.0 を開始点に



* Not defined in XNS 1.0 specifications

- ❖ まずは、Identifier に焦点
- ❖ 最終的には、XNSを大幅に簡単化することを目標
- ❖ Visa International, AMD, Cordance, Epok, NRI, NuStar, Gemplusなどが主立って活動
- ❖ その他のメンバー: IBM, Novel, EAN International,, TSO, XNSORG
- ❖ <http://www.oasis-open.org/apps/org/workgroup/xri/>

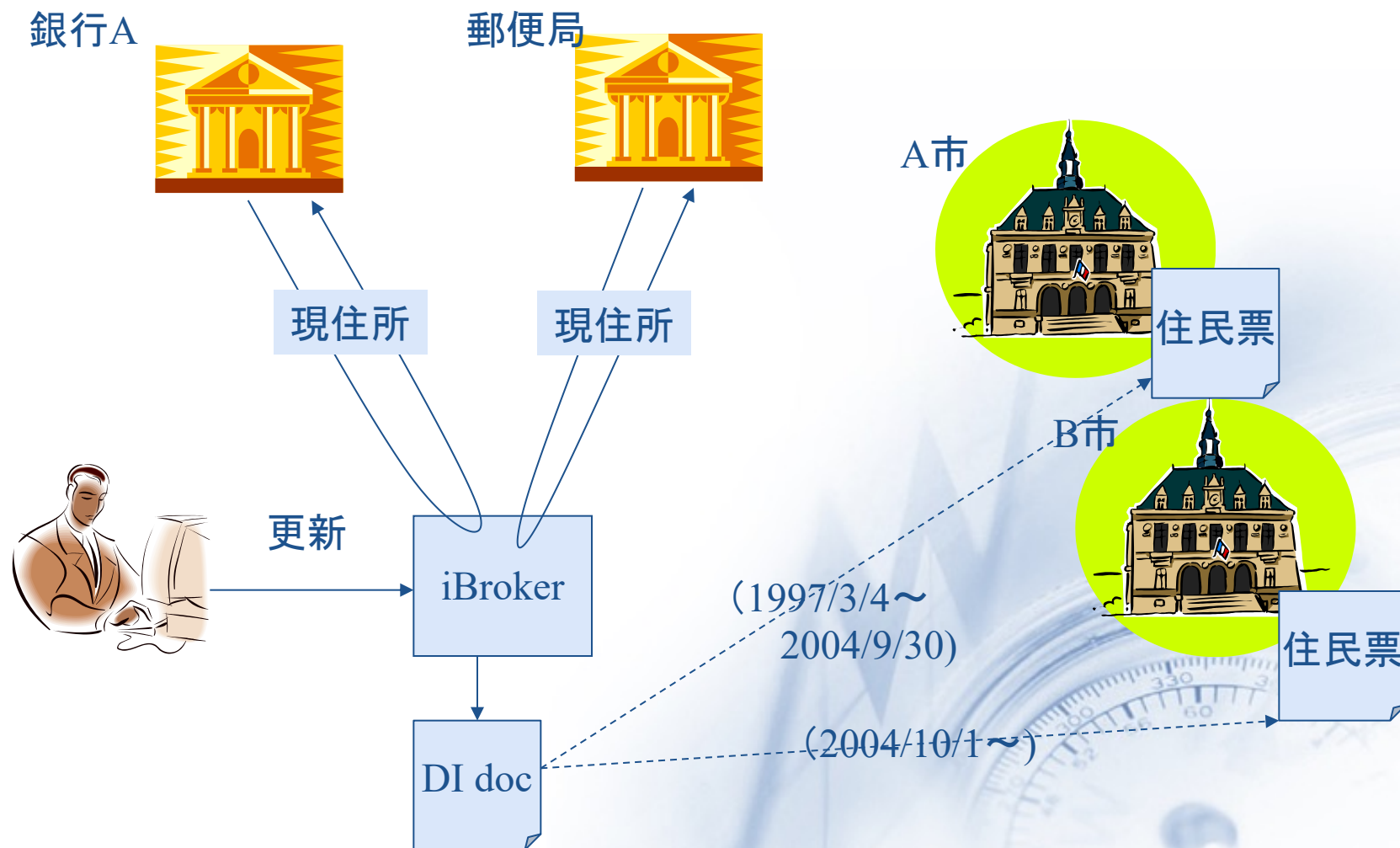
- ❖ xri:@NRI/(+employee)/崎村夏彦/(+phone)
- ❖ =西谷昌樹
- ❖ =Drummond_Reed
- ❖ xri:(urn:oasis:spec:2040)/(+index)
- ❖ xri:=(http://www.my-
website.com)/favorites.html

= 記号などは省略形で、実際には、

xri://authority.subauth/path/to/the/resource のような、uri
の形式を取る。

- 抽象的概念用のネームスペースを持っている。例 : +email, +love
- 国際化を当初より想定。UTF-8 というのみならず、Language Identifier, Font Identifier を持っており、それでコンテキスト切り替えをやることにより、マルチリンガル対応が可能
- 無制限 Federation : =sakimura.sato.suzuki は、sakimura ネームスペースでのsatoの実体を持つネームスペースの中のsuzuki を指す。
- 各データが識別子を持っている
- 他のスキームを取り込むことが出来る
 - 例 : (<http://www.cimbalom.org/>).player

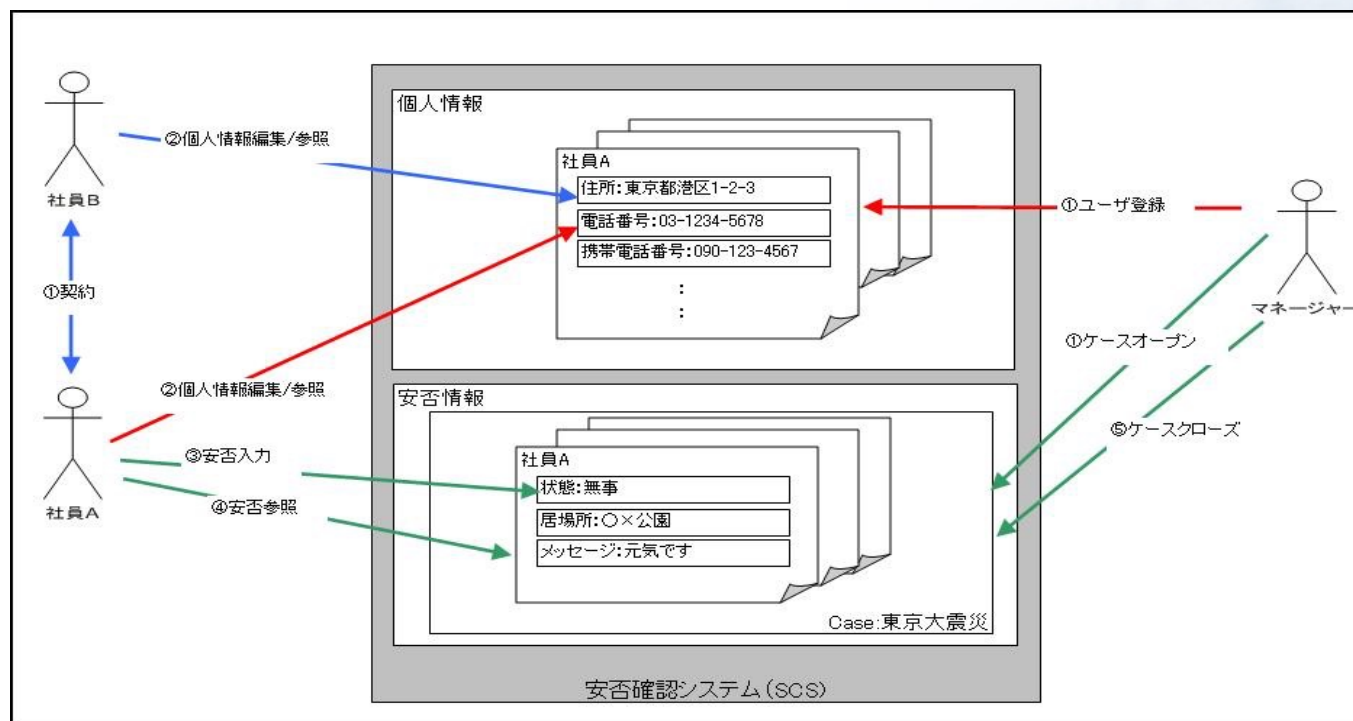
利用例：住所変更(DAB)







- ❖ 社員の住所や個人携帯電話番号、メールアドレス等の個人情報を事前に登録する
- ❖ 平時において個人情報へアクセスする(社内連絡システムとしての利用を想定)には本人との事前契約を必要とする
- ❖ 災害発生時、マネージャーはケース(災害ごとに設定)をオープンする
- ❖ ケースオープン後、社員は安否情報を入力する。また、契約の有無によらず他ユーザの個人情報、安否情報にアクセスできるようになる
- ❖ ケースクローズ後はマネージャのみ安否情報の参照が出来る



❖ GCS (Global Context Symbols)

- 人間の可読性向上のために、XRIでは識別子の論理的コンテキストをあらわすための記号を持っている。

Symbol Character	Authority Type	Establishes global context for
+	General public	管理責任を負うAuthorityのない一般的概念に対応するIDであることを表す。例: 愛
=	Person	自然人をあらわすIDであることを示す。
@	Organization	法人に代表される、団体をあらわす記号。
\$	OASIS XRI Specification	メタデータをあらわすための特殊識別子であることを示す。OASIS標準で定義される。例: 言語、バージョン、型、クエリなど。
*	User-relative	Authorityが現在のユーザーに相対的に定義される識別子であることを示す。Spec の 3.2.6.節を参照
!	XRI author	人間の可読性のためのコメントとしての識別子。機械による処理では無視される。

❖ クロスリファレンス

- 括弧 () で囲む。中に入るストリングは、“.”で始まらなければならない。
(URIとの混乱を避けるため)
- フルスキーム表示の場合はもちろんその限りではない。

❖ セルフリファレンス

- 概念を表し、それ自体はリゾルブできないことを現すのにも、クロスリファレンスのシンタックスを利用する。
- 例: xri:(+user-friendly)

❖ パス

- URI 同様、“/” で階層を切り、“?”, “#” または、文字列の終わりでパスは終了する。
- URIでは、パスはOpaqueパートとして取り扱われるが、XRIでは、2種類に分けて処理される。
 - Reassignable Identifier: “.” で区切る。
 - Persistent Identifier: “:” で区切る。
 - Dot あるいは Colon セグメント以外は、Opaqueセグメントとして文字列を取り扱う。

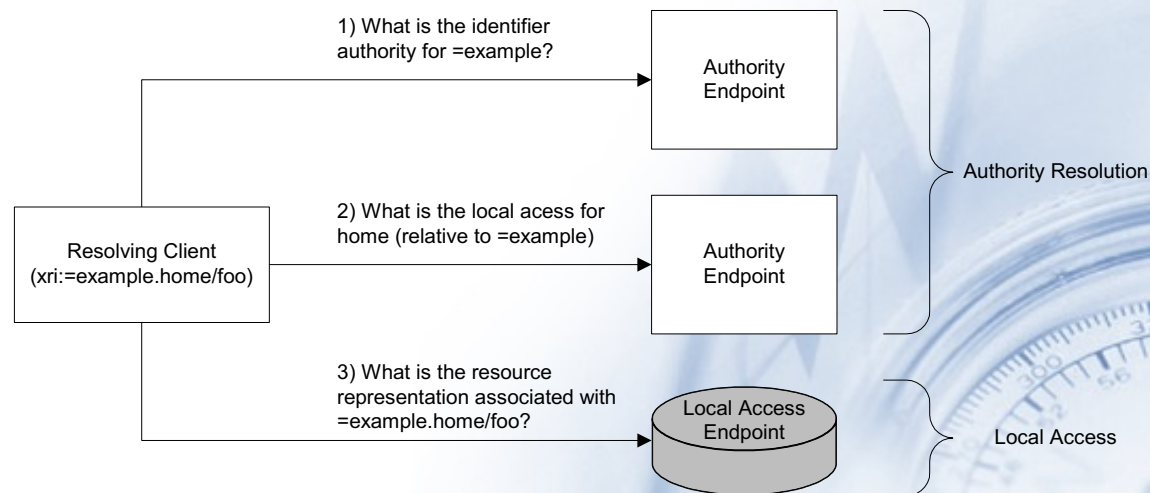
= 崎村夏彦 / (+phone) / (+work)

↑
個人であることをあらわす

↑
筆者の再割当可能アドレス

↑
電話という概念だが、
はリゾルブ可能
相対的に

- ❖ **XRI**は複数のリゾリューションメカニズムを持ちうる。
- ❖ **Ver.1.0** の **spec** では、**HTTP**を利用した一つのリゾリューションのみを提示している。
- ❖ 原則的には、左から右へ評価してゆく



- ❖ @a.b.c のようなアドレスを左から順番に評価すると、それぞれに対して、Identifier Authority Descriptors が返される。これを手がかりにして、次のレベルの評価を行い、繰り返して、最終結果に到る。

```
<IdentifierAuthority xmlns="xri:$r.s/IdentifierAuthority">
  <Resolved>.foo</Resolved>
  <NextAuthority>
    <URI>http://xri.example.com</URI>
    <URI>https://xri.example.com</URI>
  </NextAuthority>
  <LocalAccess>
    <Service> xri:$r.a/X2R</Service>
    <Type>application/rddl+xml</Type>
    <URI>http://xri.example.com</URI>
  </LocalAccess>
  <LocalAccess>
    <Service> xri:$r.a/X2R</Service>
    <Type>image/jpeg</Type>
    <URI>http://pictures.xri.example.com</URI>
  </LocalAccess>
  <Mapping>xri:@:1:2:3</Mapping>
</IdentifierAuthority>
```

❖ 例: `xri:=example.home.base/foo.bar`

- “=” が、`http://equals.xns.org/xri-resolve` だとすると:
- “**=example**” の解決
 - GET <http://equals.xns.org/xri-resolve/.example>
 - 200 OK HTTP/1.1
 - Content-Type: `application/xriad+xml`
 - Expires: `Fri, 7 Nov 2003 19:43:31 GMT`
 -
 - `<IdentifierAuthority xmlns="...">`
 - **`<NextAuthority>`**
 - **`<URI>`**
 - **`http://xri.example.com/xri-resolve/`**
 - **`</URI>`**
 - **`</NextAuthority>`**
 - `<LocalAccess>...</LocalAccess>`
 -
 - **`</IdentifierAuthority>`**

GET ://xri.example.com/xri-resolve/.home

200 OK HTTP/1.1

Content-Type: application/xriad+xml

If-Modified-Since: Fri, 31 Oct 2003 19:43:32 GMT

<other HTTP headers>

<IdentifierAuthority xmlns="...">

<NextAuthority>

<URI>

http://xri.home.example.com/xri-resolve/

</URI>

</NextAuthority>

<LocalAccess>...</LocalAccess>

...

</IdentifierAuthority>

- ❖ XRIは、もともと XNSプロジェクト (www.xns.org) から発生したTCで、スタートポイントは、XNS ver.1.1 を基にしている。そのうち、識別子文法の部分と、そのリゾリューションの部分抜き出して、改善したのがXRIである。
- ❖ XNSのビジョン：
 - 人・物・概念に識別子を与え、互いに識別することを可能にする。
 - 識別子は、実名、仮名、匿名を使い分けられるような体系になっていなければならない。
 - そのためには、永続的識別子と、複数の一時的識別子を持ち得なければならない。
 - それぞれのIdentity同士のデータの交換は、「契約」に基づいて行われ、この「契約」がアクセスコントロールを担う。
 - (Contract law の「契約」を使うのは、国境を越えた取引を行うためである。)
 - 「契約」に当たっては、互いの身元を保証してくれるCertification サービスが必要となることもあろう。
 - また、たとえ「契約」に基づいていても、破る人が出てくるだろう。そのためには、そのような人・組織に情報を渡さないようにする目安として、Reputation サービスを設立する。
- ❖ したがって、XRIだけでは道半ばで、「契約」に基づくセキュアなデータ交換プロトコルが必要である。⇒ eXtensible Data Interchange (XDI) TC の準備中。


```
<resource>
  <xri>+phone.number</xri>
  <xri>+:(@:A4B6/:18)</xri>
  <resource>
    <xri>+work</xri>
    <xri>+:(@:A4B6/:465)</xri>
    <xri>:3</xri>
    <resource>
      <xri>$v/:1</xri>
      <xri>$v.d/2003-01-12T12:13:14Z </xri>
      <data>04-206-544.0947 x1234</data>
    </resource>
    <resource>
      <xri>$v/:2</xri>
      <xri>$v.d/2003-08-30T11:05:55Z </xri>
      <data>04-206-626.8833</data>
    </resource>
  </resource>
</resource>
```