

したがって Subject フィールド等において UTF-8 で許される範囲の多バイトコードを使用することができます。しかし実装を容易にするために、また国際的な互換性に配慮して、基本領域では多バイト文字コードを使用しないこととします。さらに RFC2459 であらかじめ定義されている拡張領域で、subjectAltName 以外のフィールドでは多バイト文字コードを使用しないこととします。また subjectAltName 拡張フィールド、および後述する RFC2459 で定義されていない拡張フィールドで多バイト文字コードを用いる場合は UTF-8 を使用することとします。

3-3. 公開鍵証明書の基本領域

3-3-1. version

version フィールドの値は 2 とします。これは X509 version 3 に準拠していることを示します。

3-3-2. serialNumber

公開鍵証明書のシリアル番号です。証明書発行局の中で一意で、再使用しません。

3-3-3. signature

signature フィールドには証明アルゴリズムの OID を格納し、ISO TS 17090 および日本の電子署名法に関連した「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」では次の 6 つのアルゴリズムが示されています。

1. md5WithRSAEncryption (1.2.840.113549.1.1.4)
2. sha1WithRSAEncryption (1.2.840.113549.1.1.5)
3. dsa-with-sha1 (1.2.840.10040.4.3)
4. ecdsa-with-sha1 (1.2.840.10045.4.1)
5. sha-1WithEsignEncryption (0.2.440.5.5.3.4)
6. md5WithEsignEncryption (0.2.440.5.5.3.3)

暗号技術の進歩により、新しいアルゴリズムが開発される可能性はあり、また既存のアルゴリズムに欠点が発見される可能性があります。したがってこのガイドラインではアルゴリズムを規定しません。しかし現時点での互換性を考えれば、少なくとももっとも広く用いられている上記の 2 は実装しておくことが推奨されます。

3-3-4. issuer

Issuer フィールドには証明書発行者の名前が入ります。名前は Directory Information Tree を使用することとされており、ISO TS17090 ではディレクトリのエントリとして CountryName, LocalityName, OrganizationName, OrganizationUnitName,

CommonName を挙げています。この中で CountryName, と CommonName は必須です。このツリー構造の名前は証明書発行局が一意に特定できる必要がありますが、証明書発行局の一意性は X509 の規定上は補償する手段がありません。したがって互換性を考慮する範囲で運用上、一意になるように定める必要があります。また再利用してはいけません。CountryName は国名が入りますが、この属性は必須とし、ISO の 2 文字の国名識別子を用いることとします。日本は JP です。LocalityName, OrganizationName, OrganizationUnitName はいずれもオプションですが、このいずれか 1 つまたはいずれかの組み合わせで、証明書発行局を一意に特定できる名前を格納します。CommonName は必須で、証明書発行局のポリシーを示す文字列を格納しますが、その先頭に"MD-HPKI-XX-"を付加するものとします。"XX"は"01"です。これはこの証明書がこのガイドラインに準拠していることを示します。またこのガイドラインが改定された場合には準拠している証明書の"XX"の値が変わります。

3-3-5. validity

公開鍵証明書の有効期間です。終了期限が 2049 年末までの場合は UTCTime 形式で表示し、グリニッジ標準時を使用します (YYMMDDhhmmssZ)。分単位までの表示も許されませんが、2050 年以降と変化を少なくする意味で秒単位まで表示することとします。2050 年以降は GeneralizedTime 形式を使用します。(YYYYMMDDhhmmssZ)

3-3-6. subject

Subject には証明書の所有者の名前が入ります。名前は Directory Information Tree を使用することとされており、ISO TS17090 ではディレクトリのエントリとして CountryName, LocalityName, OrganizationName, OrganizationUnitName, CommonName, SurName, GivenName, e-mail を挙げています。この中で CountryName は必須で、3-3-3 と同様の国名コードを格納します。日本は JP です。また CommonName は必須で、所有者がヒトである場合、電子署名法に適應するためには所有者の氏名（ローマ字表記）を含む必要があります。同様に所有者が法人である場合、法人名（ローマ字表記）を含む必要があります。また CommonName の値は同じ証明書発行局の発行する証明書の中で対象を一意に示すものとします。同姓同名の可能性があるので、氏名に資格登録番号のような ID 番号を付加することが求められます。対象が一意に決まるということは CommonName に同じ値を再利用するのは証明書の更新を行う場合だけということです。LocalityName, OrganizationName, OrganizationUnitName はオプションで使用目的を規定しません。SurName はオプションですが存在する場合は日本の姓名の「姓」に相当する値を格納します。GivenName はオプションですが存在する場合は日本の姓名の「名」に相当する値を格納します。E-mail はオプションですが、存在する場合は電子メールアドレスを 1 つ格納します。

3-3-7. subjectPublicKeyInfo

証明書所有者の公開鍵のアルゴリズム識別子と公開鍵を格納します。アルゴリズム識別子は OID で指定します。ISO TS 17090 および日本の電子署名法に関連した「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」では次の4つのアルゴリズムが示されています。

1. RSAEncryption (1.2.840.113549.1.1)
2. DSAEncryption (1.2.840.10040.4.1)
3. Ecdsa (1.2.840.10045.2.1)
4. ESIGNEncryption (0.2.440.5.5.3.7)

署名アルゴリズムと同様で、このガイドラインではアルゴリズムを規定しません。しかし現時点での互換性を確保するために、少なくとももっとも広く用いられている上記の1は実装しておくことが推奨されます。

3-3-8. issuerUniqueIdentifier

このフィールドは使用しません。

3-3-9. subjectUniqueIdentifier

このフィールドは使用しません。

3-4. 公開鍵証明書の一般的な拡張領域(RFC2459)

3-4-1. authorityKeyIdentifier

証明書発行局の公開鍵証明書を厳密に識別するための情報を格納します。keyIdentifier, authorityCertIssuer, authorityCertSerialNumber の3つのサブフィールドからなりますが、本ガイドラインでは keyIdentifier だけを使用します (ISO TS17090)。keyIdentifier は証明書発行局の公開鍵を SHA-1 ハッシュした値とします。AuthorityKeyIdentifier フィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3-4-2. subjectKeyIdentifier

証明書所有者の公開鍵を厳密に識別するための情報を格納します。所有者公開鍵を SHA-1 ハッシュした値を格納します。このフィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3-4-3. keyUsage

所有者公開鍵の使用目的を示すフィールドです。データはビットストリングで、

<code>digitalSignature</code>	(0)
<code>nonRepudation</code>	(1)
<code>keyEncipherment</code>	(2)
<code>dataEncipherment</code>	(3)
<code>keyAgreement</code>	(4)
<code>keyCertSign</code>	(5)
<code>CRLSign</code>	(6)
<code>EncipherOnly</code>	(7)
<code>DecipherOnly</code>	(8)

以上の9つが RFC2459 で定義されています。それぞれの属性は RFC2459 を参照してください。このフィールドは必須で、かならず値が必要です。また保健・医療・福祉分野で、Subject が人や組織の場合で法的に有効な署名に用いる場合は `nonRepudation` 以外のビットをオンにしないこととします。またそれ以外の署名に用いる場合も `digitalSignature` と `nonRepudation` 以外のビットをオンにしないこととします。(電子署名法)

3-4-4. `extendedKeyUsage`

`keyUsage` 以外の公開鍵の使用目的を示します。subject が人または組織で、`keyUsage` で `nonRepudation` または `digitalSignature` を指定した場合、このフィールドを使わないことが推奨されます。(電子署名法)

このフィールドはオプションです。

3-4-5. `privateKeyUsagePeriod`

証明書発行局の公開鍵証明書以外では使用しません。このフィールドはオプションです。

3-4-6. `certificatePolicies`

証明書発行局の証明書発行ポリシーの OID を格納します。このフィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3-4-7. `policyMappings`

証明書発行局の公開鍵証明書以外では使用しません。このフィールドはオプションです。

3-4-8. `subjectAltName`

証明書所有者の別名を格納します。多バイト文字コードの名前を使用する場合はここに格納します。このフィールドは必須ですが、クライアントが解釈できるかどうかは任意です。

3-4-9. issuerAltName

使用しません。

3-4-10. subjectDirectoryAttributes

証明書所有者の属性を格納できます。RFC2459 では一般的な目的で使用することは推奨されていませんが、後述の hcRole attribute に限って使用することとします。それ以外の attribute を含めてはいけません。

3-4-11. basicConstraints

証明書発行局の公開鍵証明書以外では使用されません。証明書発行局の公開鍵証明書では必須であり、値が必要です。

3-4-12. nameConstraints, policyConstraints

この2つのフィールドは証明書発行局の公開鍵証明書以外では使用されません。これらのフィールドはオプションです。

3-4-13. CRLDistributionPoints

CRL の発行点または参照点を示します。このフィールドは OCSP レスポンダを利用しない限り必須です。OCSP レスポンダを採用する場合は使用しません。互換性を考慮する場合、インターネット上で最も汎用的なプロトコルである HTTP をサポートするのが望ましいため、CRL を Web サーバに格納し、CRLDistributionPoints の値をその URL とすることを推奨します。また、ISO/TC215 では OCSP レスポンダ (authorityInformationAccess) について明確な規定がないため、本フィールドが必須になっていますが、OCSP レスポンダを採用する場合は本フィールドの代わりに authorityInformationAccess フィールドに OCSP レスポンダのアドレスを記載します。

3-4-14. authorityInformationAccess

CA に関する情報を取得する方法と場所を記載することができますが、このガイドラインでは OCSP (Online Certificate Status Protocol : RFC2560) レスポンダを使用する場合に OCSP レスポンダのアクセス方法とアドレスを記載します。それ以外の用途には使いません。このフィールドは OCSP レスポンダを採用していない場合は使用しません。

3-5 特別な (RFC2459 で定義されていない) 拡張領域

3-5-1 hcRole attributes

拡張フィールドの定義ではなく、subjectDirectoryAttributes の属性の 1 つとして保健医

療福祉分野で役割および職種などの属性を指定する目的で定義します。hcRole Attribute のフォーマットは ISO TC 17090 に準拠しますが、当分の間、国家資格である保健・医療・福祉分野の職名だけを使用し、Attribute の値は PrintableString で表現するものとします。なお、hcRole 属性自体の OID は ISO TC 17090 で定義されたものを使用します。今後、保健・医療・福祉分野のわが国の職種が体系的に定義され、OID を取得することが必要で、これらが整備された時点で hcRole の使用方法については再検討が必要と考えられます。

当面 HcRole で使用できる値

Medical Doctor	医師
Dentist	歯科医師
Pharmacist	薬剤師
Medical Technologist	臨床検査技士
Radiological Technologist	診療放射線技師
General Nurse	看護婦（士）
Public Health Nurse	保健婦（士）
Midwife	助産婦
Physical Therapist	理学療法士
Occupational Therapist	作業療法士
Orthoptist	視能訓練士
Speech Therapist	言語聴覚士
Dental Technician	歯科技工士
National Registered Dietian	管理栄養士
Certified Social Worker	社会福祉士
Certified Care Worker	介護福祉士
Veterinarian	獣医師
Emergency Medical Technician	救急救命士
Psychiatric Social Worker	精神保健福祉士
Care Manager	介護支援専門員

3-5-2 qualifiedCertificateStatements

証明する内容が公的に認められたものであることを示すための拡張フィールドで、ISO TS17090 で記載されています。しかし、Qualified Certificate 自体は RFC3039 で定義されており、単純に拡張フィールドを 1 つ追加するだけで実装するには無理がある。TS17090 の記載も不十分でこのままでは実装困難である。したがってこのガイドラインでは使用しないこととします。

3-6. 証明書廃棄リストプロファイル
RFC2459 に準拠します。

	CAの証明書	国家資格のSP	その他のSP	サービス受給者	医療機関(組織)	
version	C	C	C	C	C	
serialNumber	C	C	C	C	C	
signature	C	C	C	C	C	
issuer	C	C	C	C	C	
validity	C	C	C	C	C	
subject	C	C	C	C	C	
subjectPublicKeyInfo	C	C	C	C	C	
issuerUniqueID	N	N	N	N	N	
subjectUniqueID	N	N	N	N	N	
authorityKeyID	M	M	M	M	M	
subjectKeyID	M	M	M	M	M	
keyUsage	C	C	C	C	C	
extendedKeyUsage	N	O	O	O	O	
privateKeyUsagePeriod	O	O	O	O	O	
certificatePolicies	M	M	M	M	M	
policyMappings	M	N	N	N	N	
subjectAltName	M	M	M	M	M	
issuerAltName	N	N	N	N	N	
subjectDirectoryAttributes	N	C	O	O	O	
hcRole	N	C	N	N	N	ISO TS17090
basicConstraints	C	N	N	N	N	
nameConstraints	O	N	N	N	N	
policyConstraints	O	N	N	N	N	
CRLDistributionPoints	M	M	M	M	M	
authorityInformationAccess	O	O	O	O	O	
qualifiedCertificateStatements	N	N	N	N	N	ISO TS17090

C：必須でクライアントが解釈できることが必要。M：必須だがクライアントは解釈できるかどうかは任意。O：必須ではないが実装してもよい。N：使用しない。SP 専門職

4. 属性証明書のプロファイル

4-1. 全体的な方針

このガイドライン作成時点で属性証明書は RFC ではなく、IETF Internet draft で、draft-ietf-ac509prof-09.txt として参照可能です。このガイドラインではこの Internet draft に準拠することとします。このガイドラインで述べるのは原則として draft-ietf-ac509prof-09.txt で記述されている事項以外に日本の保健・医療・福祉分野で公開鍵基盤を用いるための制限や追加項目です。実装に際しては draft-ietf-ac509prof-09.txt を参照してください。

4-2. 文字コードセット

公開鍵証明書と同様に PrintableString、BMPString、UTF-8String を使用することができますが、Attributes 以外では多バイト文字コードを使用しないこととします。Attributes もできるだけ多バイト文字コードを使用しないことが推奨されます。

4-3. 属性証明書の基本的なフィールド

4-3-1. version

version フィールドの値は1です。これは v2 であることを示しています。

4-3-2. holder

holder は属性証明書の所有者を示します。draft-ietf-ac509prof-09.txt では baseCertificateID、entityName、objectDigestInfo の3つのオプションのうち、1つが存在することになっていますが、保健・医療・福祉分野では baseCertificateID だけを用いることとします。BaseCertificateID は保有者の PKC の issuer と serial number からなります。draft-ietf-ac509prof-09.txt では issuer UniqueIdentifier もオプションで使用可能ですが、このガイドラインでは使用しないこととします。BaseCertificateID を用いる場合、AC は常に PKC とペアで使用する必要があります。

4-3-3. issuer

属性証明書の発行者を示します。V1Form と V2Form があり、V2Form を用いることになっています。V2Form は issuerName、baseCertificateID、objectDigestInfo の3つのオプションから1つを選択することになっていますが、issuerName を使用することとします。issuerName のフォーマットは PKC の issuer と同じ形式です。すなわち、ディレクトリのエントリとして CountryName, LocalityName, OrganizationName,

OorganizationUnitName, CommonName が使用可能で CountryName, と CommonName は必須です。CountryName は国名が入りますが、この属性は必須とし、ISO の 2 文字の国名識別子を用いることとします。日本は JP です。LocalityName, OrganizationName, OrganizationUnitName はいずれもオプションですが、このいずれか 1 つまたはいずれかの組み合わせで、証明書発行局を一意に特定できる名前を格納します。

CommonName は必須で、証明書発行局のポリシーを示す文字列を格納しますが、その先頭に "MD-HPKI-XX-" を付加するものとします。"XX" は "01" です。これはこの証明書がこのガイドラインに準拠していることを示します。またこのガイドラインが改定された場合には準拠している証明書の "XX" の値が変わります。

4-3-4. signature

属性証明書発行者の電子署名のアルゴリズムを示します。PKC の signature と同じです。

4-3-5. serialNumber

属性証明書のシリアル番号です。属性証明書発行局の中で一意の番号であり、再使用しません。

4-3-6. attrCertValidityPeriod

属性証明書の有効期間を示します。PKC の有効期間と同じ形式ですが、一般に短く設定されます。

4-3-7. attributes

attributeType と attributeValue からなり、1 つの属性証明書では attributeType はユニークです。つまり同じ attributeType の attributes は 1 つしか書けません。ただし 1 つの attributeType に対して attributeValue は複数あってもかまいません。attributeType は OID を用いますが、当面は draft-ietf-ac509prof-09.txt で定義されている attributeType だけを用いるものとします。attributeValue は UTF-8 string を用いることができますが、可能な限り多バイト文字は使用しないこととします。

attributeValue で汎用性のあるものは登録制にして、将来の OID 化に備える必要があります。

4-3-8. issuerUniqueID

属性証明書発行局を一意に指定する ID ですが、このフィールドは使用しません。

4-4 属性証明書の一般的な拡張フィールド

属性証明書には次の6つの拡張フィールドを使用することができます。ただし、すべてオプションで必須ではありません。したがって特定のドメインでいずれかの拡張フィールドを用いる場合はドメイン内で仕様の整合性をはかる必要があります。

4-4-1 Audit Identity

holder と Audit の対象者が異なる場合に使用することができます。これを用いる場合は値がなければいけません。

4-4-2 AC Targeting

属性証明書が有効な対象システムまたはプロトコルを指定します。このフィールドが存在し、クライアントが対象に含まれない場合、クライアントは属性証明書を拒否しなければなりません。このフィールドを使用する場合は値がなければいけません。

4-4-3 Authority Key Identifier

発行者の公開鍵の識別子を格納します。PKC の KeyIdentifier と同じです。値は空でもかまいません。

4-4-4 Authority Information Access

発行者の情報のアクセス方法とアドレスを指定します。このガイドラインでは OCSP レスポンダのアクセス方法とアドレスを指定する以外には使用しません。値は空でもかまいません。

4-4-5 CRL Distribution Points

証明書廃棄リストのアクセス方法を指定します。PKC と同様です。属性証明書の一般的な運用では有効期間を短く設定するために CRL を使用しなくてよい場合が多いことに注意してください。値は空でもかまいません。

4-4-6 No Revocation Available

証明書廃棄リストが存在しないことを示すフィールドで値は常に NULL です。このフィールドが存在すれば CRL はありません。

5. 証明書発行局の運用とポリシー

6. 証明書発行局連携

公開鍵証明書は証明書発行局 (CA) が複数ある場合、信頼性の連携を行うためには何らかの方法で CA 間の信頼性の伝達が必要になります。信頼性を伝達する方法には3つの方法

がよく知られています。1つ目は1つの Root CA から樹状に CA を配置し、基本的なポリシーを共有する方法です。このような証明書を受け取ったクライアントは証明書を Root CA の方向にたどり、信頼している Root CA に行き着けば、その証明書自体を信頼します。2つ目は Bridging CA を用いる方法で、Bridging CA はそれぞれの CA に対して証明書を発行します。Bridging CA が信頼できればそれが証明している CA はすべて信頼できるようになります。3つ目は Cross Certificate で、信頼性を伝達したい CA が相手の CA に証明書を発行します。相互に発行する場合があります。1つ目の方法は3つ目の方法の特殊な形と考えることもできます。いずれの方法にも欠点と長所があり、本ガイドラインでは特に規定したり推奨したりしません。実際に証明書連携が必要な場合が起こったときに改定の上、言及することとします。

7. 時刻認証機構

7-1. Time Stamp Protocol (RFC3161)について

診療情報の大部分は法的に保存義務があり、また証拠性が求められます。一連の情報は時系列にしたがって因果関係や従属関係があることが多く、時刻および時系列は重要です。したがって信頼できる時刻情報を情報に付属させることは重要で、そうすることによって証拠性や証明力の増加が期待できます。信頼できる時刻情報を付加することを時刻認証と呼びます。時刻認証の方法はいくつか存在し、信頼性が説明できるものであればどれを利用してもかまいませんが、PKI の応用として Time Stamp Protocol (RFC3161)があります。これは Time Stamp Authority を用い、クライアントから送られる情報のハッシュを含むリクエストに対して、時刻情報を付加し、署名をおこなって返すサービスで、Time Stamp Authority さえ信頼できれば構築も容易であり、十分な信頼性を持つものです。本ガイドラインでは TSP の使用を推奨します。

RFC3161 にはいくつかの選択可能なオプションがあり、実装の仕方によっては互換性のない Time Stamp Token ができます。したがって本ガイドラインでは推奨する選択を含めて TSP の詳細を定めることとします。

7-2. TSA の公開鍵証明書

TSA の公開鍵証明書の形式は本ガイドライン 3 章に従いますが、3-4-4 の extendedKeyUsage フィールドは必須で、その値は id-kp-timestamping (OID: 1.3.6.1.5.5.7.3.8) です。

7-3. ハッシュアルゴリズム

ハッシュアルゴリズムは SHA-1 と MD5 を採用し、SHA-1 はかならず実装しなければなりません。

7-4. nonce は使用することとし、64 ビットの乱数を使用することとします。

7-5. タイムスタンプ要求メッセージおよび応答メッセージでは extensions フィールドは使用しないこととします。

7-6. タイムスタンプ応答メッセージで、accuracy フィールドは必ず存在するものとします。Accuracy は 1 秒以下でなければなりません。accuracy の値は実測値ではなく、1 秒としてもかまいません。

7-7. タイムスタンプ応答メッセージで、ordering フィールドは必ず存在し、値は true です。言い換えれば Timestamp Authority は時刻情報だけで順番が確定できるように応答メッセージを作成する必要があります。

7-8. 伝送方法

RFC3161 ではタイムスタンプメッセージの伝送方法は規定されていませんが、このガイドラインでは少なくとも http をサポートすることを推奨します。インターネットのような汎用経路を通過する場合は SSL/TLS を用いることを推奨します。

8. 権限管理への応用例

「日本における HIV 診療支援ネットワークの確立に関する研究」へのご協力をお願い

HIV 診療支援ネットワークシステム(A-net)が構築されて3年を経過いたしました。現在まで、最高水準の情報技術と運用を行ってきましたので、プライバシー漏洩等の事故は全く起きていません。そこで、今後システムを研究面等におきましても、さらに有効活用していただくためのご意見として、一般的に個人の医療や福祉についての情報の保護のあり方につきまして、みなさまにご意見をいただければと思います。

この調査は厚生労働省厚生科学研究費によって行われる調査です。この調査の結果は、全体の統計数値として集計されますので、個別の回答につきまして、外部に漏れることは一切ございません。また、この調査にご協力いただかなくても、一切不利益を生じることにはございません。また、途中で撤回もご自由です。

どうかご協力をよろしくお願いいたします。

平成14年2月

日本における HIV 診療支援ネットワークの確立に関する研究班

主任研究者 国立国際医療センター 内科・情報システム部 秋山 昌範

分担研究者 立教大学コミュニティ福祉学部 高橋 紘士

国立国際医療センター エイズ治療・研究開発センター 岡 慎一

調査票

この調査票については各質問の（ ）のところに回答のしかたが記載されています。あてはまる回答の番号にひとつだけ○をしていただく質問と、あてはまる回答の番号にすべていくつでも○をしていただく質問があります。また、あてはまらない場合には自由に回答を文章で記入していただく場合もあります。また最後の質問では自由にご意見を記入していただく欄もあります。

設問の指示にしたがって、回答いただくようお願いいたします。

この場でご記入いただける場合は、封筒を用意して封をして所定の箱に投函ください。

また、お持ち帰りいただいて、この調査票を郵送していただいても結構です。封筒には返送先を印刷してあります。また料金別納郵便になっていますので、切手をはらずに、このまま投函していただいても結構です。

また、回答いただくご意思がない場合は調査票をそのまま封筒に入れて、お返しいただくかそのまま、破棄していただいても結構です。

返送先は

〒352-8558埼玉県新座市北野1-2-26立教大学コミュニティ福祉学部高橋紘士研究室です。

それではよろしくお願いいたします。

I あなたの基礎属性について伺います。(あてはまる答えの番号に1つだけ○をつけてください)

1 あなたの性別をお答え下さい。

1 男 2 女

2 あなたの年齢は次にあてはまる回答の記号でお答え下さい。

1 20歳未満 2 20歳台 3 30歳台

4 40歳台 2 50歳台 3 60歳台以上

3 あなたのこの病院への通院してからの年数をお答え下さい

1 1年未満 2 1年以上2年未満 3 2年以上～3年未満

4 3年以上5年未満 5 5年以上

4 身体障害者手帳をお持ちですか

1 持っている 2 申請するつもりである

3 申請する気持ちはない 4 身体障害者手帳発行の対象にならない

5 感染の経路

1 血液製剤による 2 それ以外

II 「HIV診療支援ネットワーク (A-net)」について

1 あなたは、現在治療を受けるにあたって「HIV診療支援ネットワーク (A-net)」が活用されているのを御存じでしたか。(ひとつだけ○)

- 1 よく知っている 2 なんとなく知っていた 3 あまり知らなかった
4 まったく知らなかった

2 あなたは主治医の先生からこの「HIV診療支援ネットワーク (A-net)」の利用についての説明を受けましたか。(ひとつだけ○)

- 1 詳しく説明を受けた 2 説明を受けたがその内容はあまりはっきりしなかった
3 説明を受けたかどうか分からない 4 説明は受けなかった

3 あなたはHIV診療支援ネットワーク (A-net)にあなたの診療の記録としてどのような項目は記載されているか御存じですか。(ひとつだけ○)

- 1 詳しく項目まで知っている 2 ある程度は知っている 3 あまり知らない
4 まったく知らない

III HIV診療情報ネットワークのデータ記載事項をめぐる意見

あなた、次のような情報項目がHIV診療情報ネットワークに入力され利用されることについてどのようなお考えですか

1 あなたの姓名 年齢、居住地などの個人を識別する情報 (ひとつだけ○)

- 1 登録して当然である 2 登録するのはやむを得ない
3 できれば登録してほしくない 4 まったく登録してほしくない

2 あなたの病名 症状、経過情報 血圧等のバイタルサインの情報 (ひとつだけ○)

- 1 登録して当然である 2 登録するのはやむを得ない
3 できれば登録してほしくない 4 まったく登録してほしくない

3 あなたの検査結果についての情報 (ひとつだけ○)

- 1 登録して当然である 2 登録するのはやむを得ない
3 できれば登録してほしくない 4 まったく登録してほしくない

4 あなたの薬剤の使用状況についての情報 (ひとつだけ○)

- 1 登録して当然である 2 登録するのはやむを得ない
3 できれば登録してほしくない 4 まったく登録してほしくない

5 あなたの福祉サービス利用についての情報 (ひとつだけ○)

- 1 登録して当然である 2 登録するのはやむを得ない

- 3 できれば登録してほしくない 4 まったく登録してほしくない

6 それでは全体として病気や診療にかかわる情報をデータとして登録し活用することについてどうお考えになりますか、当てはまるものすべての番号に○をつけてください。

- 1 自分が質のよい診療に必要なことである
- 2 医学の研究を発展させるうえで必要なことである
- 3 医師どうしの情報連携がすすみ、誰でもどこでも質の高い医療を受診することができるようになる
- 4 従来のやりかたよりも自分の診療の情報がきちんと保護されるようになる
- 5 かえって情報が洩れる可能性が増えるとおもう
- 6 医師のために役に立つかもしれないが患者には何も利益がない

IV 情報保護と情報利用について

1 一般に医師が患者さんの治療から得られた様々な情報を研究に活用することについて様々な意見があります。あなたはこれらの意見をどのようにお考えになりますか

意見1 医師が自分の（患者）の治療によって得られたデータを研究に利用するのは、病気への科学的知識を増し、治療方法の発展など医学の進歩に貢献できるから、当然のことである。

（ひとつだけ○）

- 1 そう思う 2 どちらかといえばそう思う 3 あまりそうは思わない
4 まったくそうは思わない

意見2 医師が自分の（患者）の治療によって得たデータを研究に利用することによって、最新の治療方法の利用することができるようになるなど、自分の治療に役立つことになる

（ひとつだけ○）

- 1 そう思う 2 どちらかといえばそう思う 3 あまりそうは思わない
4 まったくそうは思わない

意見3 医師が自分の（患者）の治療によって得たデータを研究に利用するのは、医師が研究成果の発表し学会等での評価を得ることを目的とした医師の研究に役立つだけである。

（ひとつだけ○）

- 1 そう思う 2 どちらかといえばそう思う 3 あまりそうは思わない
4 まったくそうは思わない

V 医療や福祉のサービスの現場では様々な職種の人々が従事しています。これらの人々の個人情報保護についての意識についてあなたはどのようにお感じになっていきますか、御意見をお聞かせ下さい

1 つぎのような職種の人々が職務上得られた情報を他に洩すことの可能性についてどうお考えですか（ひとつだけ○）

1-1 医師

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-2 看護婦

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-3 臨床検査技師

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-4 薬剤師

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-5 コンピュータの運用を行う技術者

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-6 病院での受け付け支払いを担当する職員

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-7 病院等で様々な生活や療養上の相談を受ける医療ソーシャルワーカー

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-8 行政の福祉窓口担当者

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-9 社会福祉施設の職員

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-10 在宅介護を行うホームヘルパー

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-11 ボランティア

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

1-12 地域の民生委員

1 しばしばある 2 時々ある 3 稀だがある 4 ない 5 まったくない

2 これらの人々が情報の漏洩を行わないようにするための仕組みや制度がきちんと整備されている

ると思いますか（ひとつだけ○）

2-1 医師

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-2 看護婦

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-3 臨床検査技師

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-4 薬剤師

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-5 コンピュータの運用を行う技術者

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-6 病院での受け付け支払いを担当する職員

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-7 病院等で様々な生活や療養上の相談を受ける医療ソーシャルワーカー

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-8 行政の福祉窓口担当者

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-9 社会福祉施設の職員

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-10 在宅介護を行うホームヘルパー

- 1 きちんと整備されている 2 どちらかというと整備されている
3 あまり整備されていない 4 まったく整備されていない

2-11 ボランティア

- 1 きちんと整備されている 2 どちらかという整備されている
3 あまり整備されていない 4 まったく整備されていない

2-12 地域の民生委員

- 1 きちんと整備されている 2 どちらかという整備されている
3 あまり整備されていない 4 まったく整備されていない

3 あなたの病気にかかわる情報が他に洩れるかもしれないとおもったことはありますか
(ひとつだけ○)

3-1 診療室の治療の場で

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-2 病院の受け付けの場で

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-3 病院の医療ソーシャルワーカーやコーディネーターなどの相談窓口で

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-4 薬局等で薬を受け取るところで

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-5 検査をおこなうところで

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-6 病院の受け付け支払い窓口で

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-7 福祉サービスの窓口で

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある
3 洩れたのではないかと思ったことがある 4 洩れたと思う

3-8 福祉サービスを利用するとき

- 1 そのようなことは全くない 2 もしかしたら洩れるかもしれないと思ったことがある