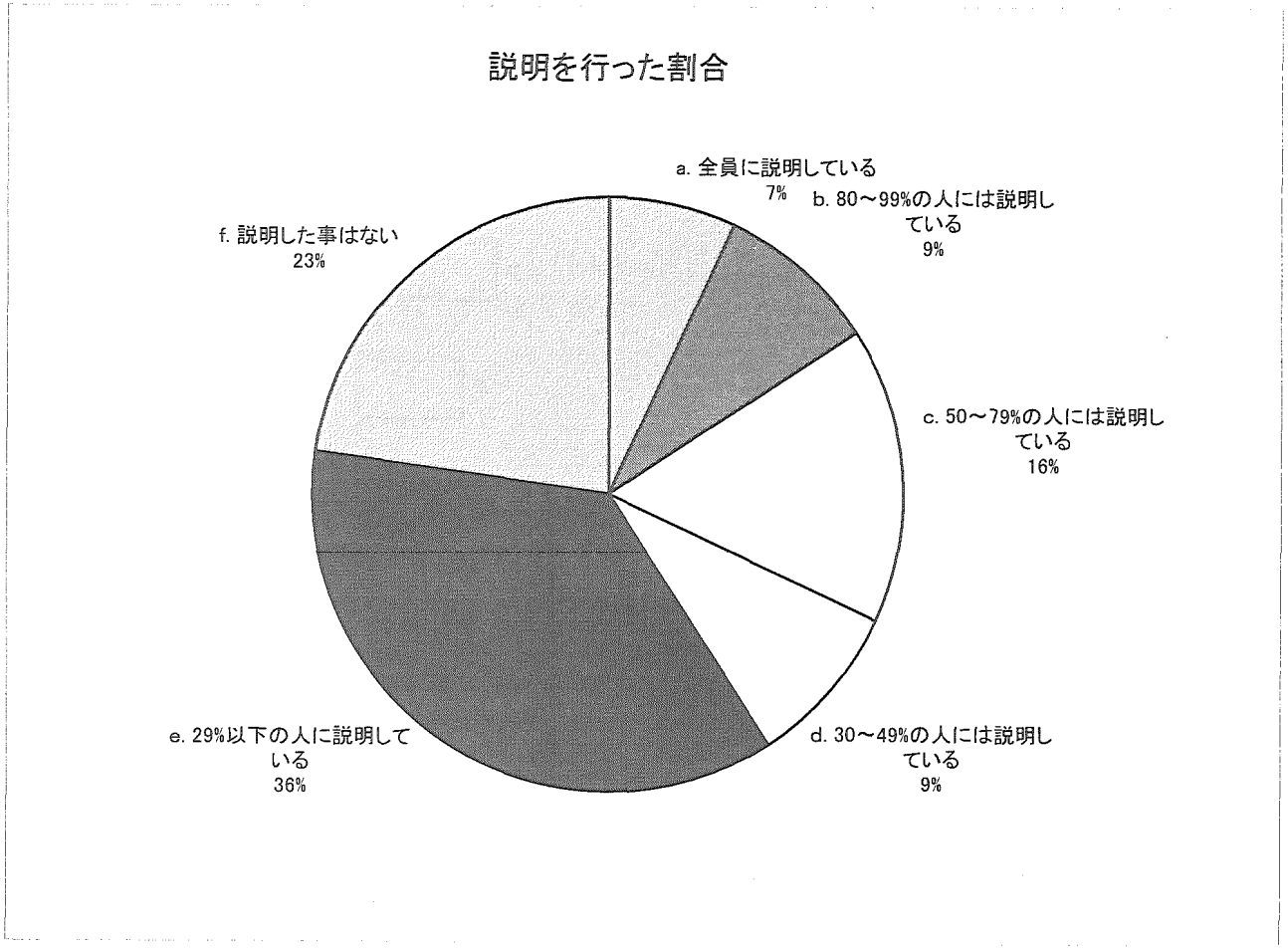
A-net ご利用に関するアンケート調査 集計結果

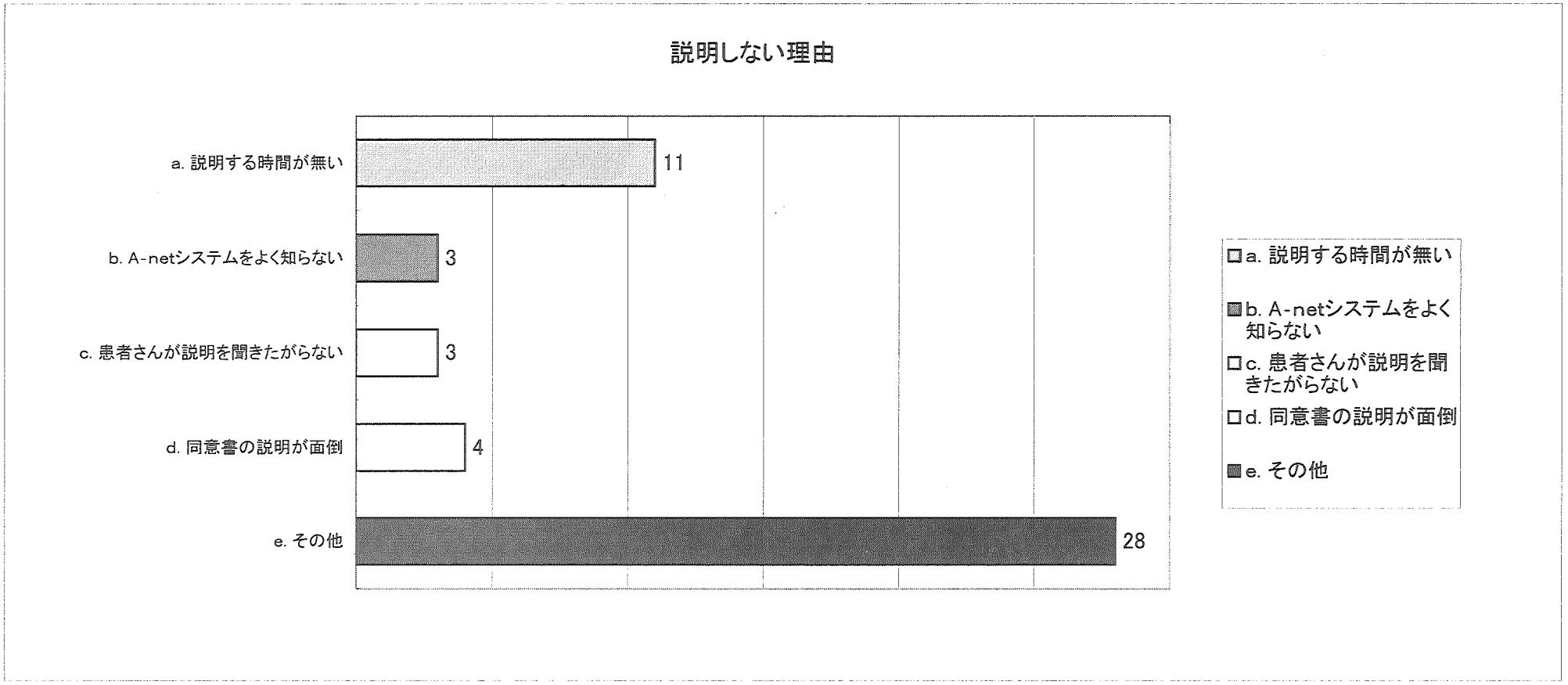


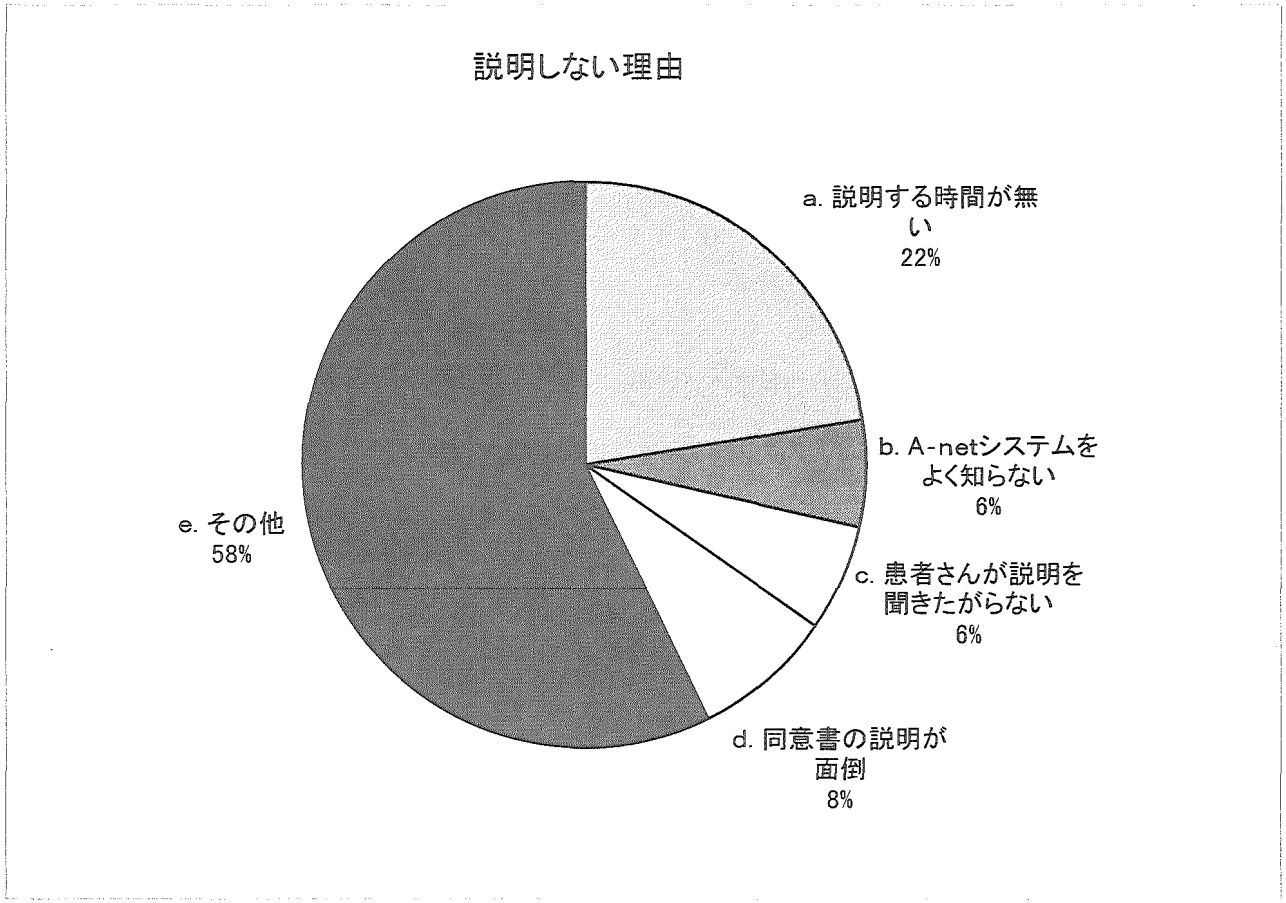
A-net ご利用に関するアンケート調査 集計結果

1. HIV患者診療について

④ 説明しない理由後ご回答ください【③でa.以外の方のみご回答ください】

質問項目	集計結果(人)
a. 説明する時間が無い	11
b. A-netシステムをよく知らない	3
c. 患者さんが説明を聞きたがらない	3
d. 同意書の説明が面倒	4
e. その他	28




説明しない理由
a. 説明する時間が無い
22%
b. A-netシステムをよく知らない
6%
c. 患者さんが説明を聞きたがらない
6%
d. 同意書の説明が面倒
8%
e. その他
58%

A-net ご利用に関するアンケート調査 集計結果

1-④ その他の意見

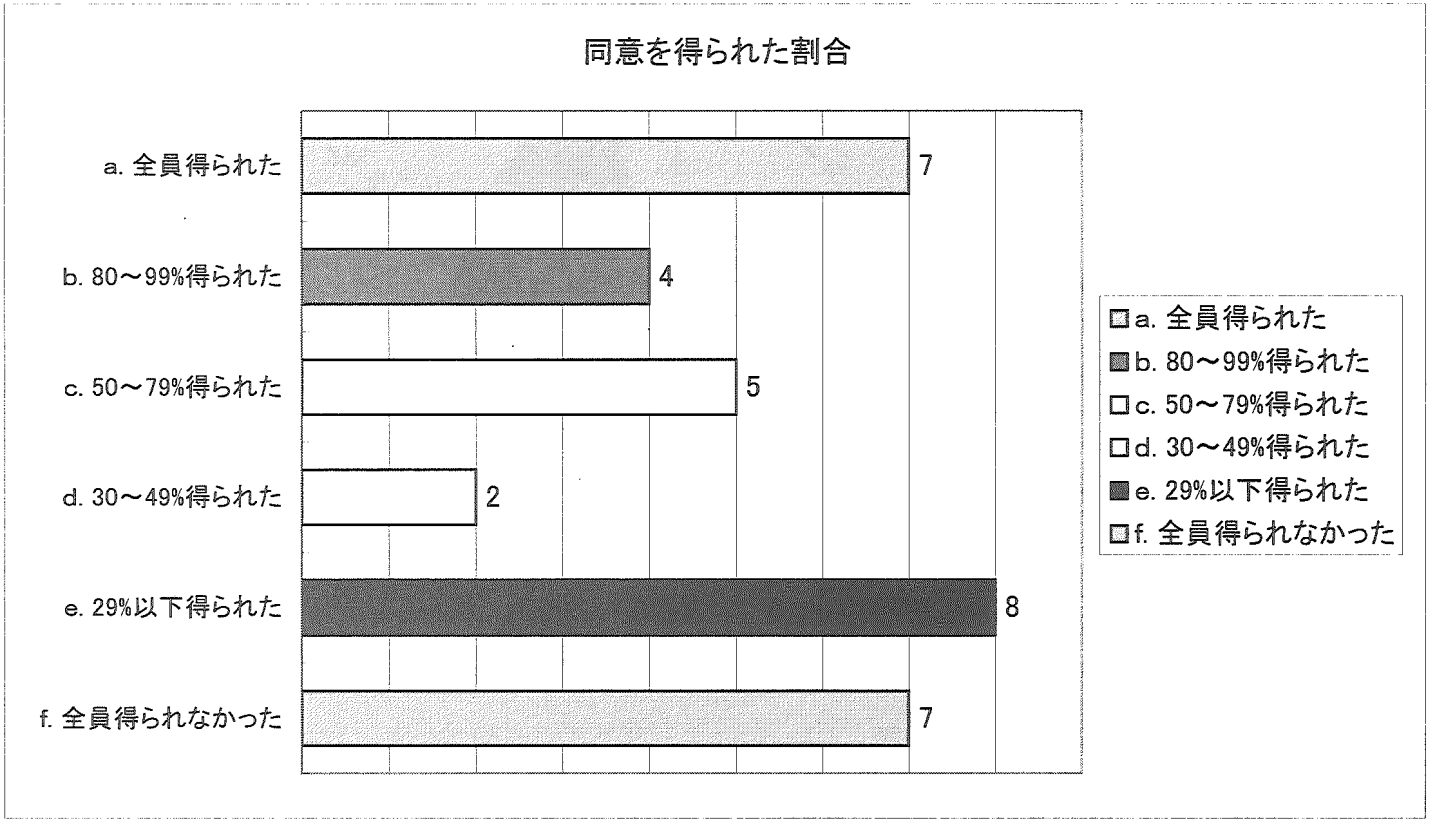
・入力するのは月に20人程度が限度だから。
・当初は説明したが希望者がいなかった。このため説明しにくくなった。
・医師が主に説明しているため、Nsｻｲﾄﾞとしては、転院になるなど病院を変わる際A-netに加入していない患者には、説明と同意を求める。
・多くの患者は当科のみを受診し、他の拠点病院を受診する機会がほとんど無い。その場合は、ﾈｯﾄﾜｰｸに参加する事である種のｾｷｭﾘﾃｨ上の不安を誘発する可能性があると考えるため。
・ほとんどの患者様が私がA-netに参加する前からの通院患者様なので、担当が変わった途端に説明し参加してもらうのがやりにくかったためです。
・現在ｼｽﾃﾑのｾｷｭﾘﾃｨの都合上、外来診療場所以外にあるため使用しづらいと思います。
・主治医で無いから
・ﾃﾞｰﾀ入力の時間が取れない。
・医師が主に説明。複数の病院に通院必要な場合（second opinionなど）はNs側からも積極的に伝えている。
・利益が少ない。
・A-net構築以前の患者様で、当院のみの受診の患者様
・意義を感じない
・①「A-netができた」ということで施設参加はさせて頂いたものの、具体的に何をﾒﾘｯﾄとして参加を勧めるめきなのかが今一つ私どもの中で不明瞭であり、実際の活用にまで至っていません。もちろん概ねの意図やｼｽﾃﾑは理解していますが。②参加する患者さんがいても多忙すぎてﾃﾞｰﾀ入力をする時間が取れない現状があります。
・①説明の理解が十分得られないと判断した。精神疾患合併ケースなどは実施していない。②利用する医療社側にPtへﾒﾘｯﾄを説明するﾒﾘｯﾄが十分に感じられない
・診療時間が限られ、A-netでの診療までの時間が見出せない。
・現時点でのA-netは、一般のHIV感染者に対する診療上のﾒﾘｯﾄは少ない
・初期に同意が得られなかった例が多かったため。以後は併診や転院の可能性が無ければ説明していない。
・併診の機会が無いため
・説明する前に死亡、または1回だけの受信者のため。
・多施設に通院するということの可能性が低い患者が多いため。
・必要性を感じない。
・①患者さんに他院受診の希望が無い。②以前、ACC受診のため入力したが、利用されなかった。
・まだ実際に患者を診察していないため
・最初からﾌﾟﾗｲﾊﾞｼｰについて脅えている人、診察室にも知人が院内にいる時には入ってきたり。こういう人も田舎にはまだいます。

A-net ご利用に関するアンケート調査 集計結果

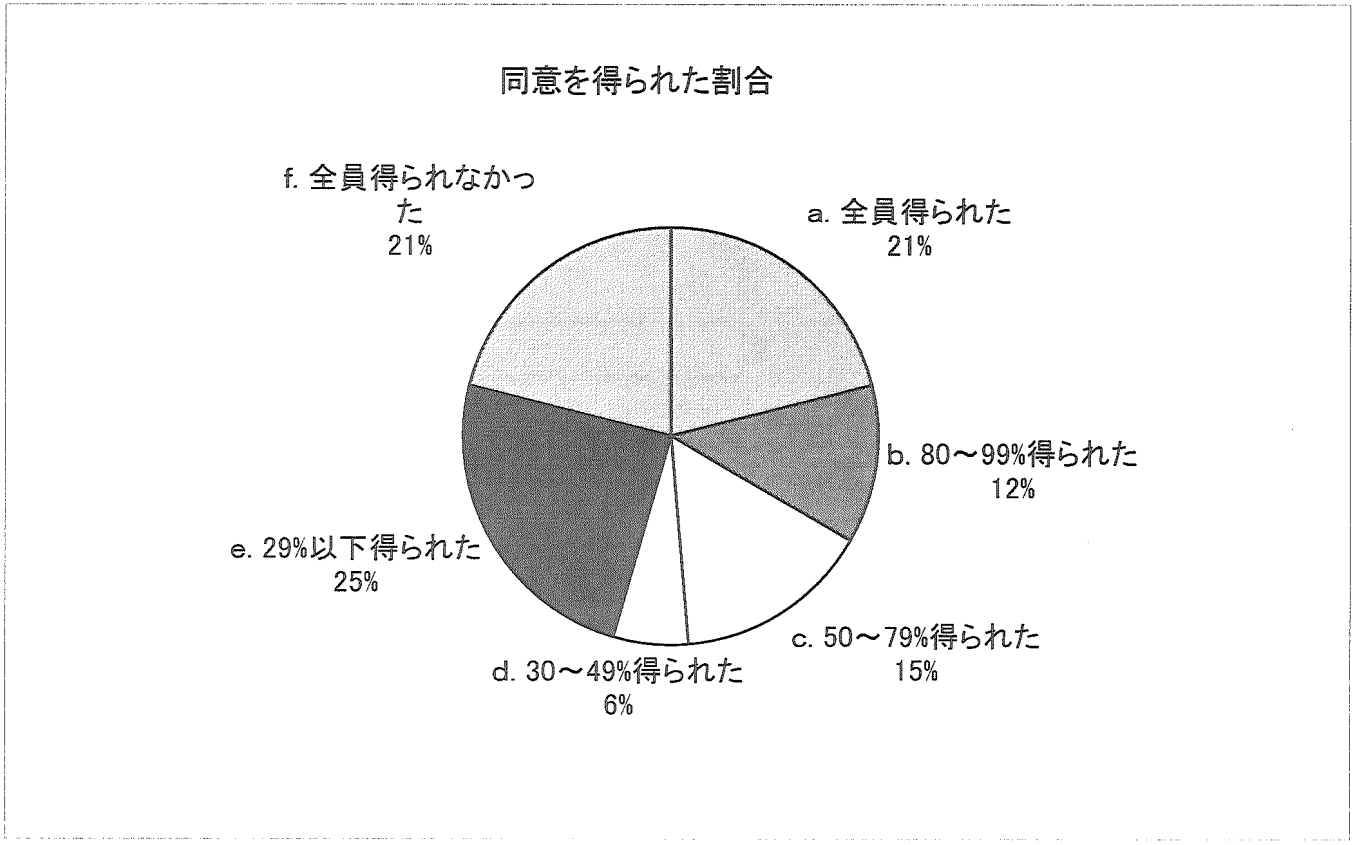
1. HIV患者診療について

⑤ A-net参加同意説明を行った患者の内、同意を得られた割合はどれ位ですか。

質問項目	集計結果(人)
a. 全員得られた	7
b. 80～99%得られた	4
c. 50～79%得られた	5
d. 30～49%得られた	2
e. 29%以下得られた	8
f. 全員得られなかった	7



A-net ご利用に関するアンケート調査 集計結果

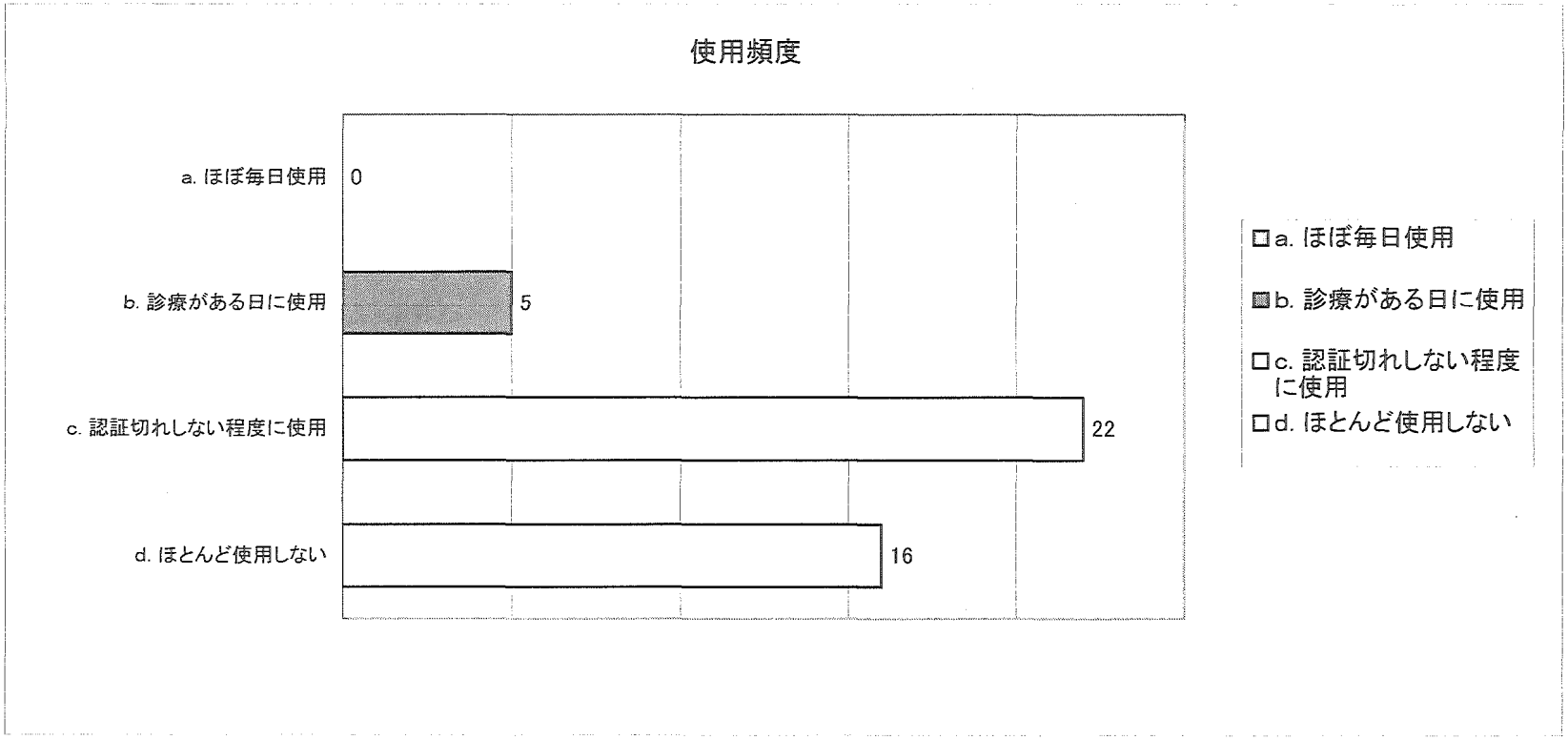


A-net ご利用に関するアンケート調査 集計結果

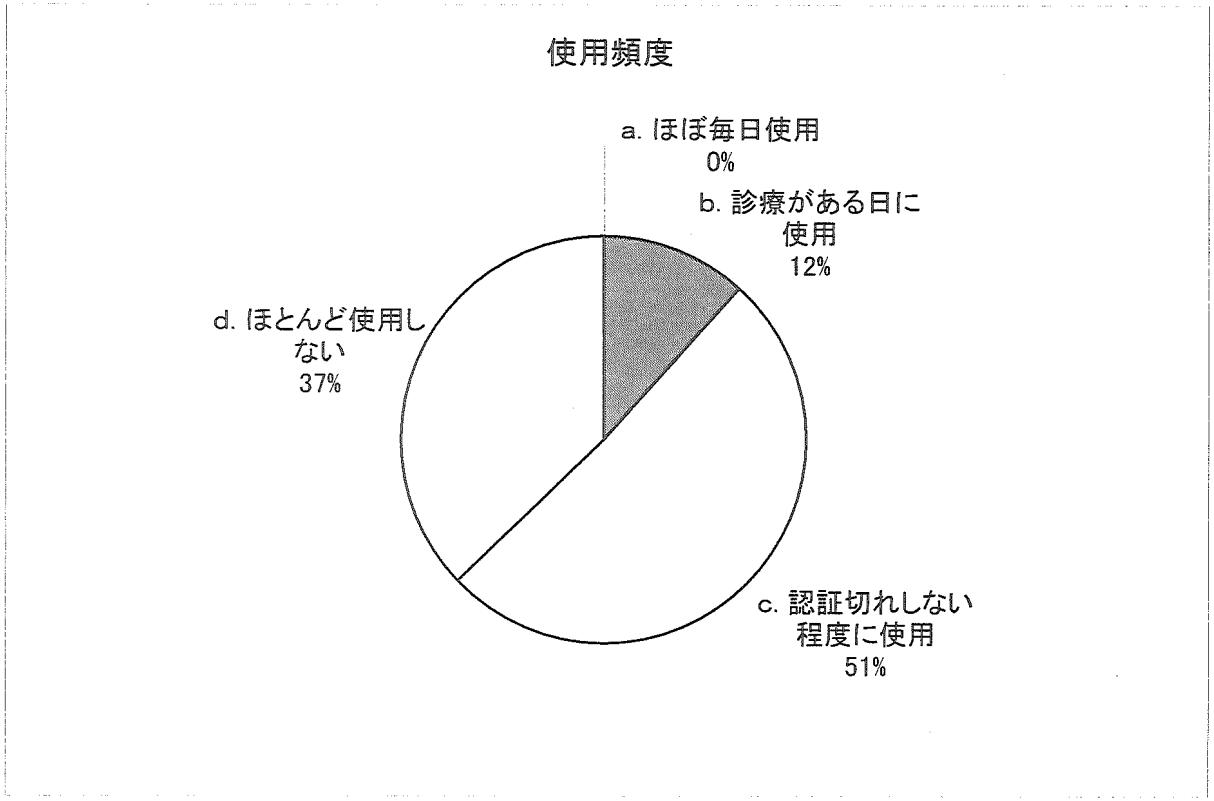
2. A－netについて

① A－netシステムをご使用になる頻度はどのくらいでしょうか。

質問項目	集計結果（人）
a. ほぼ毎日使用	0
b. 診療がある日に使用	5
c. 認証切れしない程度に使用	22
d. ほとんど使用しない	16



A-net ご利用に関するアンケート調査 集計結果

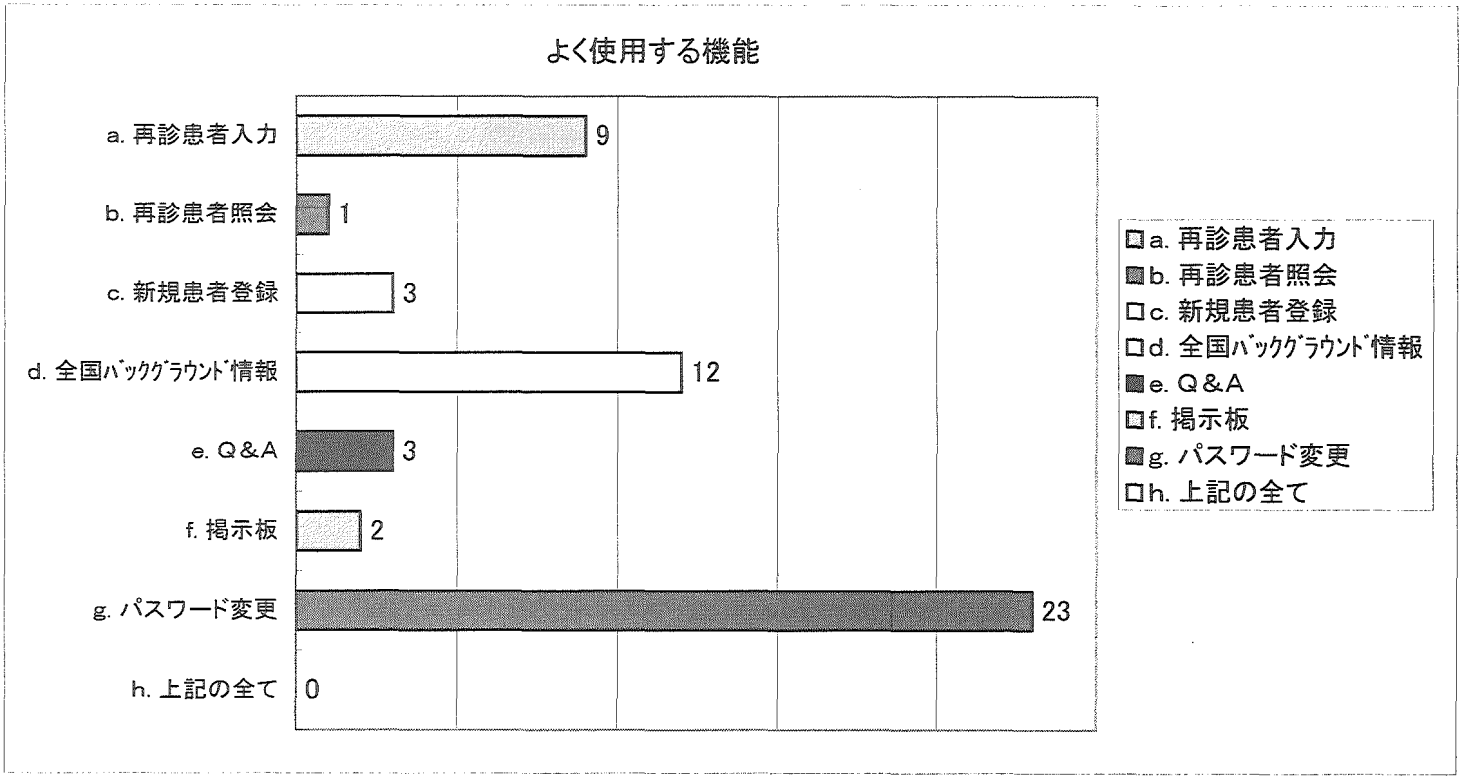


A-net ご利用に関するアンケート調査 集計結果

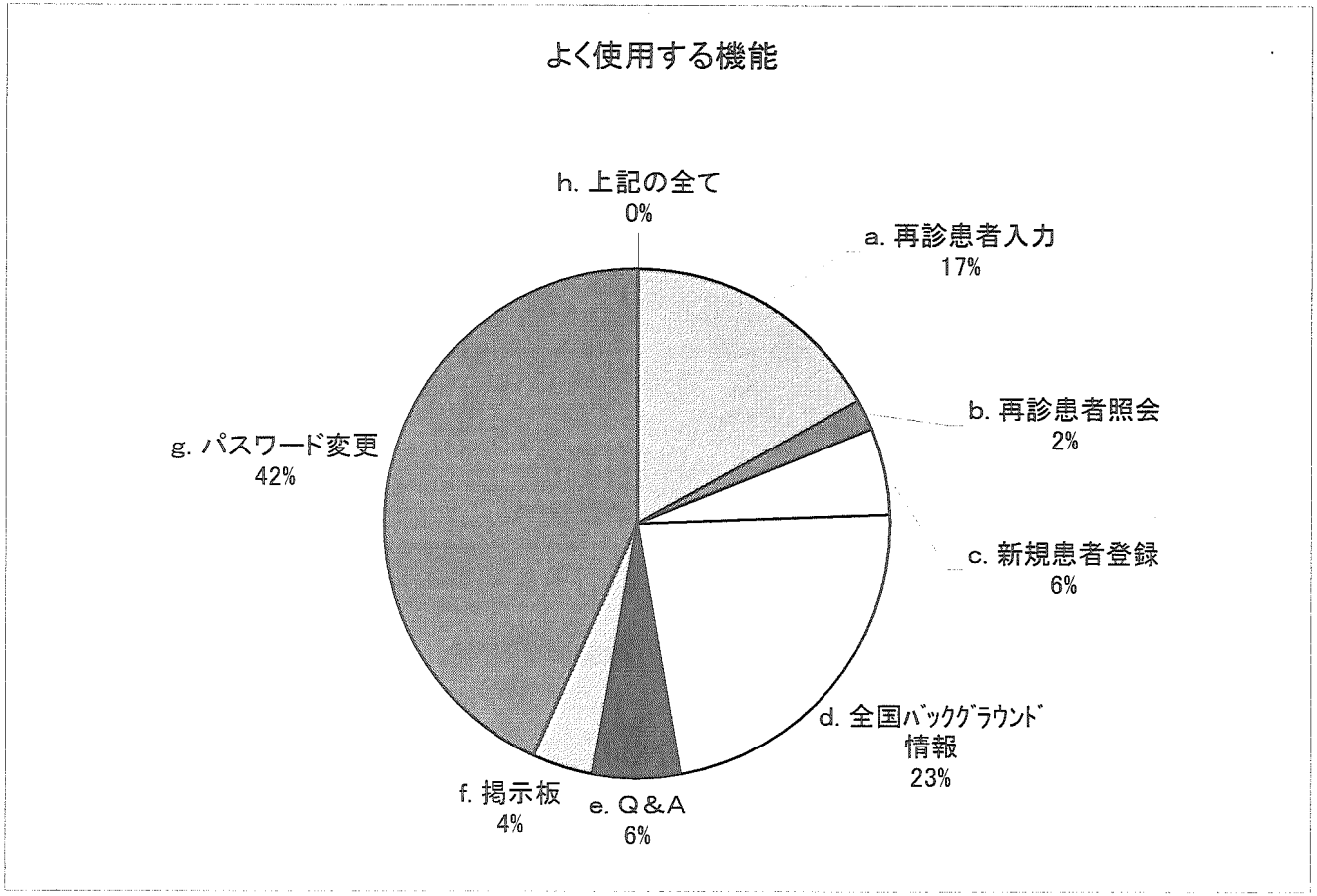
2. A－netについて

② よく使用する機能は何でしょうか。(複数選択可)【①でd.以外の方のみご回答下さい】

質問項目	集計結果(人)
a. 再診患者入力	9
b. 再診患者照会	1
c. 新規患者登録	3
d. 全国ﾊﾞｯｸｸﾞﾗｳﾝﾄﾞ情報	12
e. Q&A	3
f. 掲示板	2
g. パスワード変更	23
h. 上記の全て	0



A-net ご利用に関するアンケート調査 集計結果

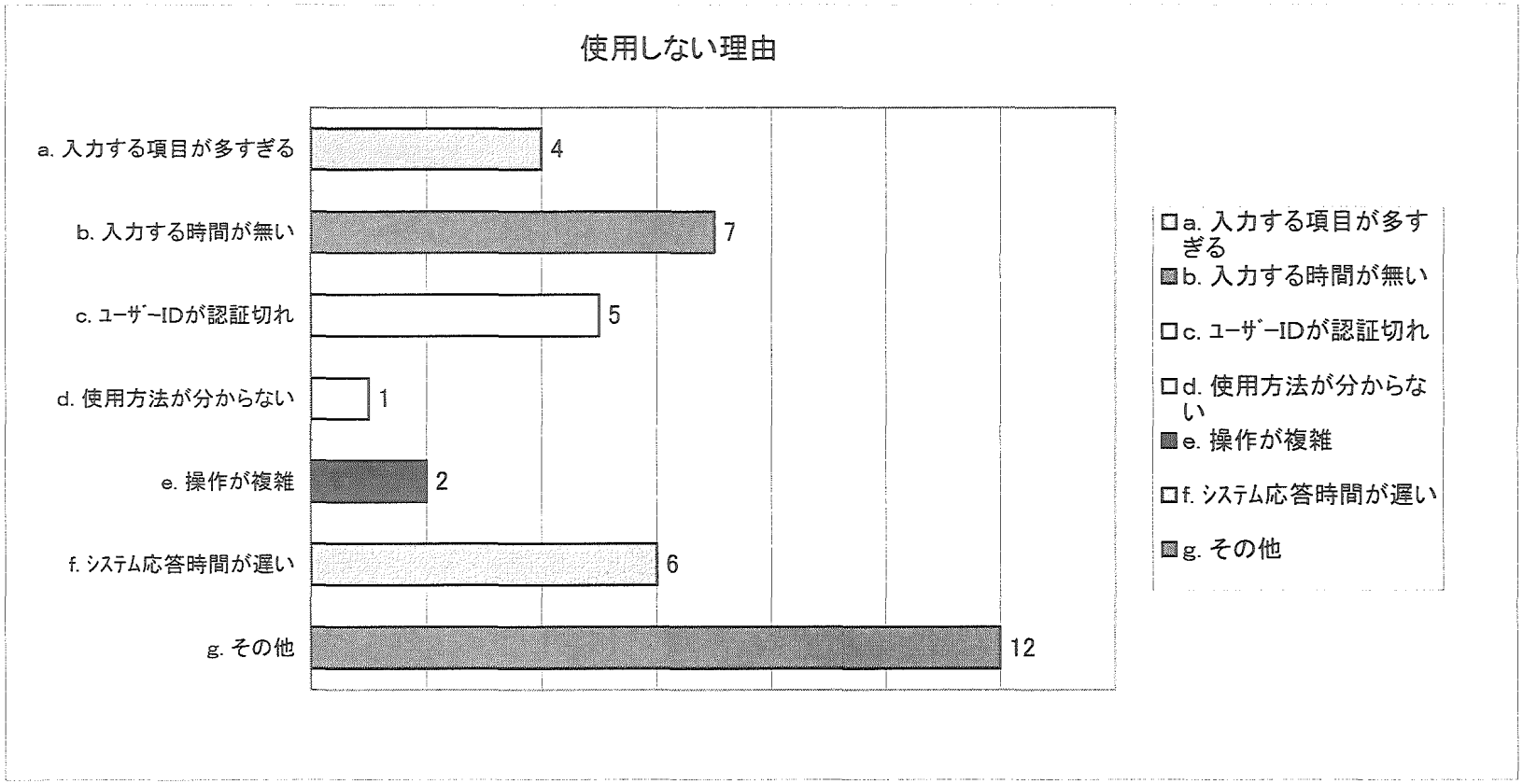


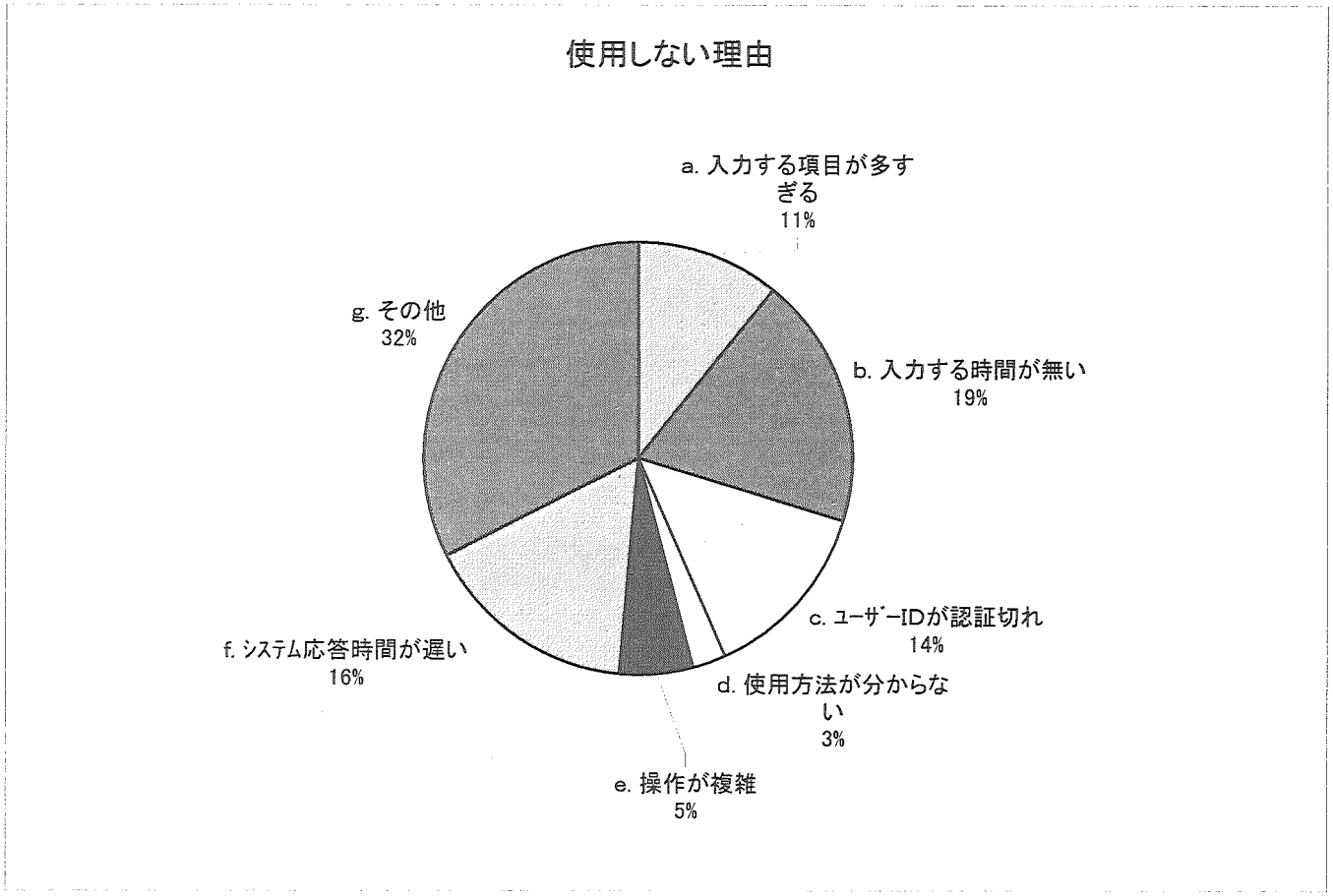
A-net ご利用に関するアンケート調査 集計結果

2. A－netについて

③ 使用しない理由を教えて下さい(複数選択可)【①でd.の方のみご回答下さい】

質問項目	集計結果(人)
a. 入力する項目が多すぎる	4
b. 入力する時間が無い	7
c. ユーザーIDが認証切れ	5
d. 使用方法が分からない	1
e. 操作が複雑	2
f. システム応答時間が遅い	6
g. その他	12




使用しない理由
a. 入力する項目が多すぎる
11%
b. 入力する時間が無い
19%
c. ユーザーIDが認証切れ
14%
d. 使用方法が分からない
3%
e. 操作が複雑
5%
f. システム応答時間が遅い
16%
g. その他
32%

A-net ご利用に関するアンケート調査 集計結果

2-③ その他の意見

・複数施設にまたがって診察を受ける可能性のある患者さんはほとんど無く、院内のﾃﾞｰﾀﾍﾞｰｽで十分と考えているため。
・当院では現時点で電子ｶﾙﾃの計画はなく、使用する利点が無い。
・患者の個人ﾃﾞｰﾀについては、病院の端末で各種の出力ができる。一方、A-netでは患者本人のﾃﾞｰﾀさえ印刷できない設定になっている。患者にとって目に見えるﾒﾘｯﾄが無い。
・現在私は診療をしていない。
・相談したその場所で入力できないのは大きい。
・今の所患者さんへの説明をしていません。その他の利用(統計利用)については興味ある項目がありません。
・当科外来に端末が無いため、使用が困難
・院内でﾃﾞｰﾀ管理システムがあり、それを転記するﾒﾘｯﾄが感じられない。看護情報ｼｽﾃﾑがあり、A-netに入力すると入力が重複となる。
・医師・患者へのﾒﾘｯﾄが少ない。
・あまり必要を感じない
・診療日に入力できないので後日入力すると日付が入力日受診になってしまうが、訂正の仕方を知らないため。
・現在通院中の患者に登録社がほとんどいないため

医療用公開鍵基盤ガイドライン　ドラフト　v006　Feb. 5

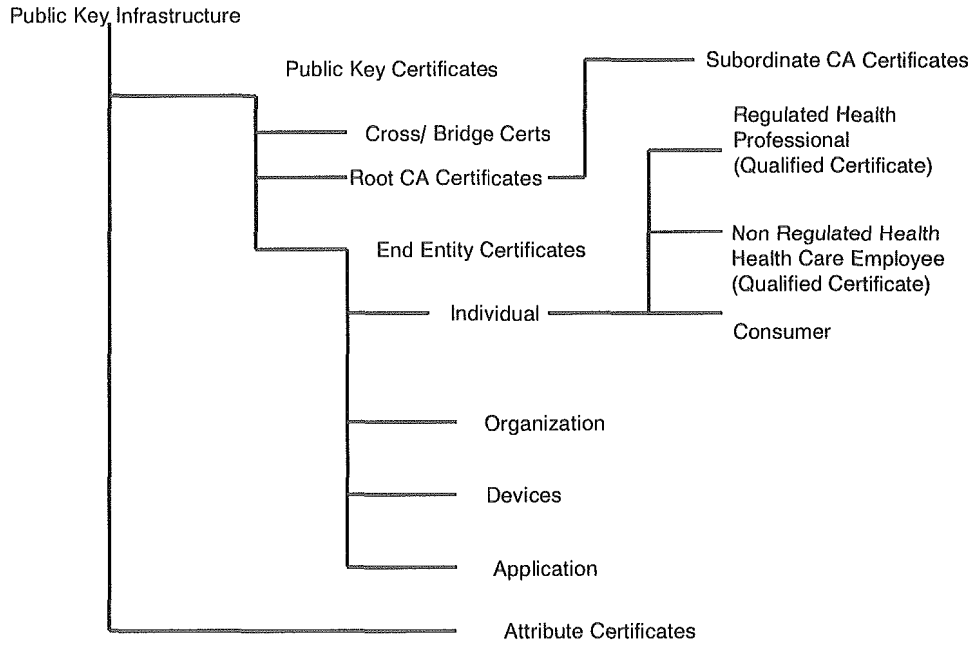
１．保健・医療・福祉分野と公開鍵基盤

２．基本的な方針と注意点

２－１．医療とＰＫＩ

ITU-T X.509 で規定される公開鍵基盤(PKI)を医療で用いる場合、その目的はいくつか考えられます。ISO-TS 17090 には以下の図が示されています。

Figure 1 – Health Care Certificate Types



この中で End Entity Certificates の Individual、Organization、それから Attribute Certificates は適応分野で運用や証明書の型式をある程度定めることが必要になります。このドキュメントは主にこれらの証明書の保健・医療・福祉分野で用いる場合の運用と証明書型式について、主に技術的な観点からガイドラインを示しています。Device や Application に PKI を用いる場合、保健・医療・福祉分野で特別に考慮することはなく、また SSL/TLS や PKI-VPN のように各方面で応用されている例があり、それらを参考にすればよいでしょう。

２－２．電子署名と完全性

End Entity Certificates の中で Individual、つまり医療従事者や患者などのサービス受給者に証明書を発行する場合と、Organization、つまり医療機関や保健者などの組織に証明書を発行する場合、その用途はいくつか考えられます。

用途の１つ目は「署名」で、これには法律や規則で定められている署名・捺印を電子的に行う場合と、法律や規則で定められてはいないが、情報作成・編集の責任者を明確にするために行う場合があります。また電子署名は通常，署名の対象となる情報のダイジェストに対して行われますので、もとの情報の完全性（真正性）の保証のための１つの手段としての意味がありますが、完全性については後であらためて取り上げます。法律や規則で定められている場合はわが国では「電子署名法」に準拠した証明書と署名方法が必要です。電子署名法では電子署名に用いる証明書は署名の目的のためだけに用いることが定められていますので、署名に用いる証明書およびそのペアの署名鍵は他の用途に用いてはいけません。法律・規則で定められていない署名に同じ証明書や署名鍵を用いるかどうかは、運用で定めなければなりませんが、今後の連携医療の発展を考えると、あまり狭い範囲だけで通用する証明書を用いることは推奨されません。また証明書の数が増えるとそれだけ運用に負担がかかりますので、法的に有効な署名と同じものを用いると良いでしょう。

２－３．資格認証

保健・医療・福祉分野では情報を扱う人の資格や役割が重要な場面が多くあります。PKIで資格や役割をあらわすためには２つの方法があります。１つは公開鍵証明書に資格や役割を示すフィールドを定義して使う方法で、もう１つは属性証明書を使う方法です。この２つの方法にはそれぞれ特徴があり、使い分けを工夫する必要があります。属性証明書は公開鍵が含まれていなくて、通常は短い有効期間で使用します。また公開鍵がないために署名との関連付けは属性証明書自体ではできませんので、対応する公開鍵証明書を一緒に用いる必要があります。

属性証明書と公開鍵証明書の使い方を検討するためにＡ病院の内科外来を担当するＸ医師が紹介されて受診した患者の過去の診療記録について紹介元のＢ医療機関に問い合わせる場合を考えてみます。Ｘ医師はＢ医療機関に対して問い合わせ書を作成して送りますが、Ｂ医療機関は問い合わせて来た人の身元や属性を確認することなしに、患者情報を返送することはできません。Ａ病院の内科に患者を紹介したことはわかっていますので、問い合わせて来た人がＡ病院の内科担当の医師であることを確認すればよいことになります。

２－３－１．公開鍵証明書による資格認証

最初に公開鍵証明書だけですべての属性を証明する場合を考えてみます。この場合証明書にはＸという人で、医師であって、Ａ病院の従業員で、内科外来担当であることが記載されることになります。そしてこの証明書はＢ医療機関で信頼できるものであると判断さ

れなくてはいけません。したがって証明書の発行者はＢ医療機関が信頼できる組織が発行したものである必要があります。Ａ病院が大阪にあり、Ｂ医療機関が東京であることもありえますし、それ以外の医療機関とも同様な場合が起こりうることを考えると、事実上日本中ですべての医療機関から信頼される組織が証明書を発行する必要があります。

仮に財団法人医療情報システム開発センター（MEDIS-DC）が証明書を発行すると仮定します。MEDIS-DC はＸが医師であることは厚生労働省に問い合わせることで理論的には確認することが可能です。またＡ病院が存在することも地方自治体等に問い合わせることで確認できます。これらは手間ではありますが、仕組みをうまく作れば現実にも可能でしょう。Ｘ医師がＡ病院に勤務していることも保険医登録情報などを用いればなんとかできるかも知れません。しかしＸ医師が内科外来担当であることはＡ病院に問い合わせる以外に確認の方法がありません。証明書発行の要請があるたびにその医療機関に勤務形態を確認しなければなりませんので、証明書発行の運用は複雑になります。これは証明内容に責任を持つ組織が 1 つの証明書に対して多数存在するための複雑さです。また、もし発行したとしても内科外来担当から救急外来担当に変わった場合や、Ａ病院からＢ病院に転勤した場合には証明書を廃棄して、新しい証明書を発行しなければなりません。電子証明書は単なるファイルですので、いくつでもコピーできます。したがって電子証明書そのものをすべて廃棄することは不可能ですので、証明書廃棄リスト（CRL）を発行し、証明書を使う人は常に最新の CRL を参照して、その証明書は廃棄されていないかどうかを確認する必要があります。転勤や担当部署の変更は全国的に見れば日常的に起こっていますので、大量の CRL が常に存在することになり、PKI 全体の運用に大きな負担になります。

つまり医療で必要なすべての属性を 1 つの公開鍵証明書に盛り込むことは現実には不可能といえます。複数の公開鍵証明書を組み合わせて使う方法も考えられますが、もとの情報と証明書を関連付けるためには電子署名を行う必要があり、公開鍵証明書の数だけ電子署名を重ねる必要があります。そのため電子署名の順序など複雑な取り決めをしなければなりませんし、CRL が大量に発生する問題は解決できません。

２－３－２．属性証明書による資格認証

属性証明書は技術的には公開鍵証明書の簡略版であり、比較的簡単に発行できますし、通常は数時間～数日といった短期間で無効になるようにしますので、資格や役割の変更があっても CRL を発行する必要性はほとんどありません。一方、属性証明書には公開鍵がありませんので、電子署名と直接対応付けることはできません。公開鍵証明書と組み合わせて用いる必要があります。つまり属性証明書で資格認証を行うということは、公開鍵証明書を属性証明書の使い分けを考えることにほかなりません。

２－３－１の公開鍵証明書だけで資格認証を行う場合にうまくいかない理由は証明内容に責任を持つ組織が複数存在することと、CRL が大量に発生することでした。従ってこれらの障害を取り除くことができるような属性証明書と公開鍵証明書の使い分けを考えれば

よいことになります。公開鍵証明書は基本的には公開鍵が誰のものか証明するものです。この「誰」に対して責任を持つ組織が単純であり、「誰」があまり変化しなければ公開鍵証明書の運用は単純になり、それ以外の属性を属性証明書で証明すればよいことになります。このような「誰」の定義には2つの場合を考えることができます。

1つ目は個人や法人といった人格を「誰」として扱う場合です。このような公開鍵証明書に対する署名は個人「実印」や法人の「公印」に相当します。証明に責任を持つ組織は住民票情報を管理している地方自治体や法人登記または医療機関登録を管理している組織になります。これは電子政府計画で整備されつつあり、制度的な問題は別として技術的には比較的容易に運用可能です。先の例で言えばXさんとA病院、B医療機関がそれぞれ公開鍵証明書を1つもつことになります。Xさんが医師であること、A病院の勤務医であること、内科外来担当医であることはすべて属性証明書で運用することになります。この方法ではCRLはほとんど発生しませんし、属性証明書を証明内容ごとに複数使うことにすれば、証明内容に対する責任組織も単純です。ただし一般には属性証明書は有効期間が短いものですので、しばしば必要になる医師の資格を示す属性証明書もその都度、発行を要求しなければなりません。医師の資格に責任を持つのは厚生労働省ですから、たとえ地方自治体に業務を委託するとしても医師資格属性証明書の要求は多数が集中することになり、運用上の負荷になる可能性があります。医師のような公的資格は変更が極めて少ないので、属性証明書の有効期間を長くすることも考えられます。しかしこの場合は少ないとはいえ、資格喪失などがありますので、属性証明書のCRLの発行を考えなければなりません。CRLの発行はそれほど難しいことではありませんが、属性証明書を使うシステムがすべてCRLを検索しなければならなくなり、実装上の負荷になる可能性があります。また属性証明書は公開鍵証明書に関連付ける必要がありますが、属性証明書の有効期間が公開鍵証明書の有効期間を超えることはできないために、公開鍵証明書の有効期間が残り少なくなっている場合などは属性証明書の有効期間を変えなければならず、発行自体も複雑になります。

2つ目は公的な資格を含めた個人を「誰」として扱う場合です。法人や組織は一つ目の場合と同じです。先の例では「医師であるXさん」を公開鍵証明書で資格認証し、「A病院の勤務医」、「A病院の内科医外来担当医」を属性証明書で資格認証します。この場合は運用がもっとも単純になります。公的資格はほとんど変化しませんので、CRLの発生は少なく、証明内容の責任の所在も単純で明確です。唯一の問題はXさんが医師として署名する場合と、個人として署名する場合に証明書や署名鍵を使い分ける必要があることですが、あまり大きな問題にはならないでしょうし、心情的にはかえって好まれるかも知れません。公的資格には「医師」のような国家資格や「保険医」のような地方自治体に対する登録資格があり、現在の管理体制では責任の所在が異なる以上は証明書を分ける必要がありますが、これは制度的な整備や「保険医」の属性証明を医療機関や医師会などに委任することで、解決することが可能です。

このガイドラインはPKIを保健・医療・福祉分野に応用するための技術的な指針ですの

で、運用面の断定はしていませんが、公的な資格を公開鍵証明書で運用し、それ以外の属性は属性証明書で運用することを推奨しています。またその前提で証明書の形式などを規定しています。また当面は国家資格だけを公的な資格としてガイドラインに取り入れています。これは制度的な整備などが整えば改定される可能性があります。

２－４．暗号化

PKI は暗号化に用いることもできます。PGP や S/MIME でも暗号化を行うことができます。アプリケーションやライブラリも数多く存在し、また保健医療福祉分野で特別な要素もありませんので、PKI を暗号化に用いること自体は簡単です。しかしただ１つ注意しなければならないことは、法的に有効であることが求められる署名に用いる証明書や署名鍵は暗号化に使ってはいけないということです。また保健医療福祉分野の情報は利用できなければ意味がありません。暗号化によって万が一にも利用性が阻害されることがないように注意する必要があります。通信途中のような一時的な暗号化は問題がありませんが、データベースそのものを暗号化するような場合は、事故などがおこっても必要なときに速やかに復号できる必要があります。

２－５．電子保存の真正性と長期にわたる署名の確認

PKI は公開鍵暗号を基礎においていますが、公開鍵暗号の安全性は時間的に有限とされています。例えば 1024 ビットの RSA 暗号を用いる場合は１年程度の安全期間を前提に運用されることが多いでしょう。単純な情報交換やある時点での資格認証には問題がありませんが、保存された情報の署名の有効性を長期にわたって確認する必要がある場合には問題が生じます。法的に保存が義務付けられた情報は３～５年、あるいはそれ以上の間、真正性を保って保存しなければなりません。１年の寿命の公開鍵暗号を用いる場合、公開鍵が作成され証明書が発行された直後に署名を行っても、その署名が確認できる、つまり PKI で真正性が保証されるのは高々１年です。したがって PKI を利用して電子保存の真正性を求める場合は工夫が必要です。

１つは署名そのものの有効期間を延長する方法です。簡単に言えば有効期間が切れる前に新しい署名鍵と公開鍵証明書を作成し、再署名します。この方法は単純ですが、署名者ごとに署名の有効期間を管理し、再署名を依頼する必要があり、個別に再署名する限り、ほとんど不可能と考えてよいでしょう。システムで自動的に再署名する方法も考えられますが、署名鍵をシステムがアクセスできる必要があり、事実上不可能です。

２つ目は署名の確認者を置く方法です。例えばすべての署名は有効期間が１ヶ月以上ある書名鍵および公開鍵証明書を用いて行うことと決めておき、すべての署名を一ヶ月に一度確認します。そして有効であった署名のなされた情報のリストを作り、そのリストに確認者が署名を行います。これを確認済みリストとし、さらに確認者の署名の有効期間が過ぎる前に確認済みリストの署名確認を行い、そのリストを作成し、署名を行います。これを

何度か繰り返せば一定期間の真正性は確認者に信頼性のもとに保証されます。

２つ目の方法の応用として、確認リストを作成した時点で機能上および運用上で改ざん不可能な媒体（例えば第三者が監査可能な金庫保管したCD-ROMなど）に固定して厳重に管理することも可能です。

いずれにしても単純に電子署名をしたから長期の保存の真正性が確保されるとかんが得てはいけません。

２－６．タイムスタンプ

電子署名によって署名時点での真正性が証明可能であり、また前節にのべたような工夫を行えば一定期間の真正性も確保できると説明しましたが、保健医療福祉分野の場合、情報が作成された時刻や、順番が重要です。虫垂炎と診断した時点と虫垂炎の手術を行った時点がこの順か、逆の順かで大きく意味が変わってきます。したがって一般に保健医療福祉分野では電子署名を行った時刻が大変重要で、信頼性のある時刻情報を付加する必要があります。訴訟等で証明力を確保しようと思うと、時刻の信頼性は第三者にとっても信頼できるものでなければなりません。本ガイドラインでも第７章でタイムスタンプについて述べていますが、基本的にはすべての署名にタイムスタンプがあることが求められます。

第三者に信頼される時刻情報を付加するためにはタイムスタンプ発行局は保健医療福祉機関から独立した信頼できる第三者機関（Trusted Third Party：TTP）が行うことが理想ですが、しっかりした監査によって信頼性が説明可能であれば、保健医療福祉機関内部やそのグループ内に置くことも可能です。

３．公開鍵証明書と証明書失行リストのプロファイル

３－１．全体的な方針

保健・医療・福祉分野での公開鍵証明書プロファイルはITU-T X.509推奨規格第３版に準拠するものとします。すなわちRFC2459に規定されているプロファイルに従うものとします。ITU-T X.509推奨規格はRFC2459以外にもISO/IEC9594-8として登録されていますが、このガイドラインで参照した文書はRFC2459です。このガイドラインではRFC2459自体にも触れていますが、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を中心に記載しています。実装に際してはRFC2459を参照してください。また原則としてISO TS 17090に準拠しています。

３－２．文字コードセット

名前などの文字コードセットは RFC2459 で PrintableString, BMPString および UTF-8String を使用することが定められています。(2003 年以降は UTF-8String のみ。)

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,