第7章 認証情報の応用

内容

- IP アドレスの認証で可能となるサービス
- IP 指定事業者と認証
- 応用サービス、ビジネス例

7. IP アドレス認証の応用

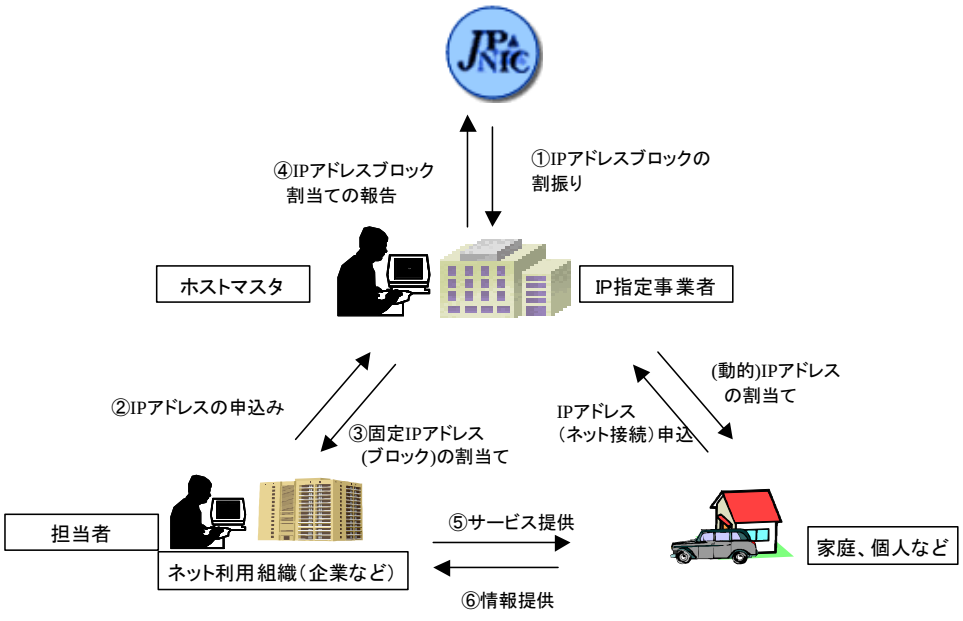
本章では、IP アドレスを認証することにより展開できる可能性のあるサービスを考え、そのサービスを応用したビジネスや事業のイメージを示す。なお、今回提示するビジネスや事業は、採算性や法や社会制度的な実現上の課題、制約等については考慮せずに考えたものである。

7.1　IP アドレスの認証で可能となるサービス

7.1.1.　現行の IP アドレス申請のプロセスと課題

企業（組織）や個人が所有する情報通信機器をインターネットに接続し、ネットワークサービスを提供（あるいは享受）したい場合、インターネットに接続する機器に特定の IP アドレスを設定しなければならない。

この IP アドレスは各人が勝手に設定するのではなく、一般には接続する ISP を通じてアドレス値を入手することになる。国内では、特定の IP アドレスが得られるまでの流れは図 7-1 のようになっている。



参考：JPNICホームページ：IPアドレスの申請
（http://jpnic.jp/ja/ip/ipguide-u.html#o1）

図 7-1　現行の IP アドレスに関わるプロセス

インターネットを利用するサービスのニーズは年々高まっており、それに応じて IP アドレスの申請も膨大な件数となっている。

このため、図 7-1 に示された各プロセスでは、作業量や利便性の点で IP アドレスの申請や承認に関する重要な情報をインターネットを通じてやりとり（送受信）されていることが多い。

ところで、現行の手続きでは、この申請や発行に関する情報の送受信を通常の電子メールシステムを通じて行っており、送信者の詐称などのリスクが残っている。このため、業務運用やシステム技術でこのリスクに対応していくことが必要である。

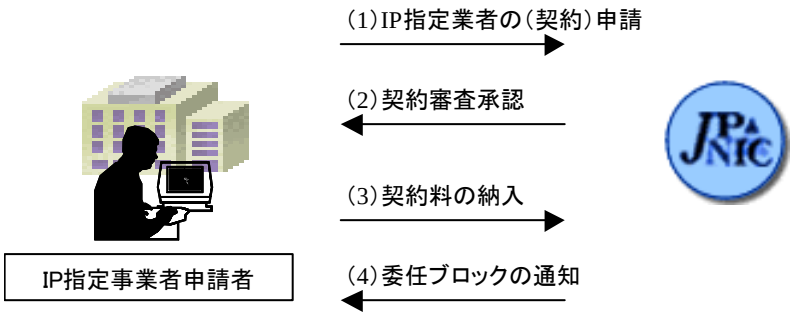
本節では、図 7-1 の中の各 2 者間で行われる情報のやりとり（プロセス）をさらに詳細に分析し、その中で判明した課題について、現行のセキュリティ上の課題と電子認証技術を使用することによって解消可能か考察する。

合わせてそうした課題が解消されることにより、これまで実施できなかったサービス（またはこれから実施可能となるサービス）について示してみたい。

7.1.2.　JPNIC と IP 指定事業者間における課題と認証

図 7-1 の①および④で示したように、JPNIC と IP 指定事業者間では、IP アドレスブロックの割り振り時、また自社やネット利用組織（ユーザ）に IP アドレスを割り当てた際に IP アドレス情報のやりとりが発生する。

「IP アドレスブロックの割振り」は IP 指定事業者になろうとする事業者（申請者）が JPNIC と契約した時点で初めて行われるものである。契約締結までの主な情報の流れは図 7-2 のようになる。



参考:JPNICホームページ:IPアドレス管理指定事業者について
（http://jpnic.jp/doc/jpnic-00117.html）

図 7-2　IP アドレス指定事業者となるまでのプロセス

現行の方式では、図 7-2 の（1）の過程で、IP 指定事業者になろうとする申請者は JPNIC に必要な文書（表 7-1）を電子メールおよび書面（郵送）で提出する。なお、この過程では対面確認までは必要とされていない。

直接の対面がないため、申請を行った者が本当にその組織の者と安易に判断することは危険ではあるが、2 章の表 2-21 中の 6、7 などその組織でないと入手が困難な文書があり、かつ契約料の納入がブロック割振りよりも先であるため、契約時点で IP 指定事業者が詐称されることは考えにくい。

ところが契約が済んだあとに、割り当て報告や登録内容の変更を通知する場合でも、現行の手続きでは電子メールベースで情報を交換している。

この過程で、悪意をもった者が IP 指定事業者の送信者を詐称し、内容の変更と偽って技術連絡窓口、事務連絡窓口等を通知してくるようなことがないとも限らない。仮にこの通知の段階で不正が発見できなかった場合、以後、詐称した者により虚偽の IP アドレスの割り当て情報が JPNIC に通知されてしまうリスクがある。

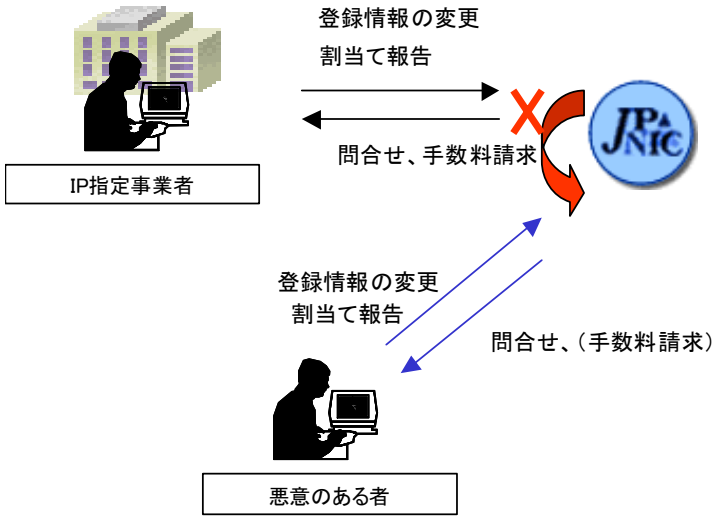


図 7-2　IP 指定事業者の詐称

こうした事態を回避するためには、JPNIC に割り当て報告や変更の連絡を行なう IP 指定事業者の担当者（以下、ホストマスタと呼ぶ）が確かにその本人であり、また連絡の文書が確実にその組織に割り当てられた IP アドレスが設定された情報通信機器から配信されたものであることを確実に示せる（確認できる）仕組みが必要である。

具体的には図 7-3 のようなホストマスタとその組織の情報通信機器（クライアント）を認証する方式が考えられる。

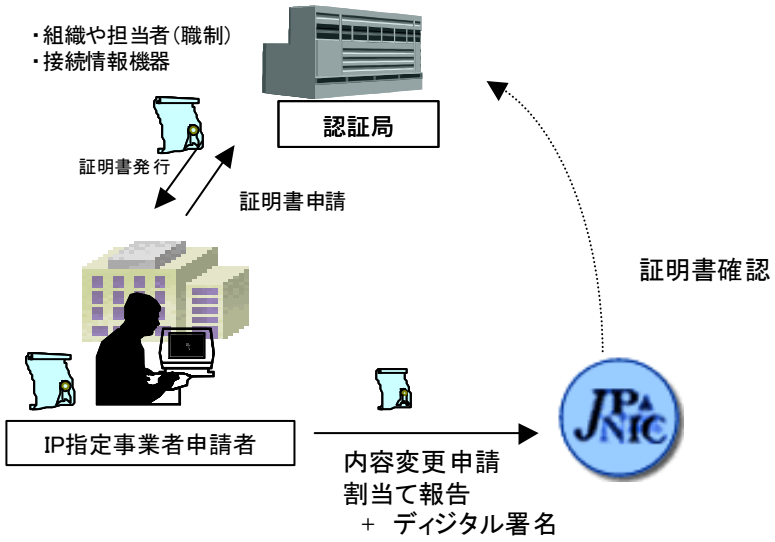


図 7-3　IP 指定事業者の認証方式

この方式が実現すると、次のようなネットワークサービスが可能となる。

- IP 指定事業者、または情報通信機器との安全なメッセージ交換サービス
- IP 指定事業者（ホストマスタ）の実在性や IP アドレス使用の真正についての一般または特定者への通知サービス

ただし、この方式では送信するメッセージ（文書、コンテンツ）の内容の真正性までは判断できない。つまり、ホストマスタが故意やミスにより割り当て情報を本来と異なる内容で記述してしまった場合などでも内容は誤ったままの状態で JPNIC には通知されてしまうことになる。これを回避するためには、割り当てた先の組織（企業等）からも割り当てについて確認が得られるような仕組みを考える必要がある。これについては 7.1.3 で示したい。

7.1.3.　IP 指定事業者とネット利用組織間の認証

図 7-1 の②および③で示したように、IP 指定事業者とインターネットを利用してサービスを実施しようとする組織（企業）との間でも接続の申込みや割り当てた IP アドレスに関する情報のやりとりが発生する。

IP 指定事業者は、図 7-4 のように通常は申込を受けた後、自社のネットワーク設備と申込者のネットワーク設備とを接続するため、申込者に出向き作業を実施する。これにより申込者が実在することや接続するルータ等は確認できる。

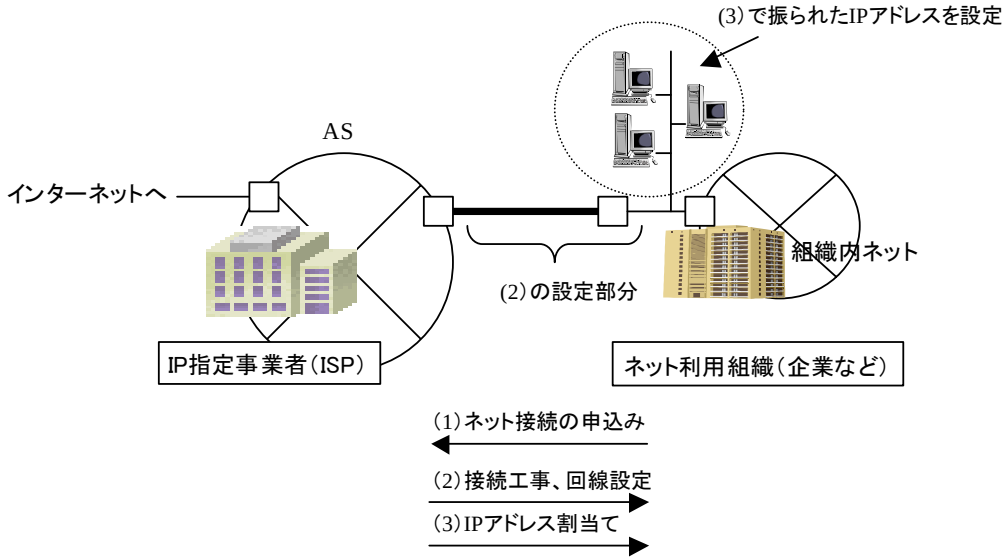


図 7-4　IP アドレス割り当ての一般フロー

ところで、ネット利用組織の IP アドレスの割り当て情報は図 7-1 の④のように IP 指定事業者が JPNIC にネットを通して報告するようになっている。④の情報は、電子メールのテキストで送信されており、ネット利用組織がその情報を確認したかは受信側（JPNIC）では不明である。このため、前述したようにホストマスタのミスや故意によって間違った割り当て情報が報告され、データベースに登録され、whois システム等を通じて外部に公開されてしまうようなリスクがある。

この事態を回避するためには、IP 指定事業者から JPNIC へ IP アドレス割り当て情報が報告される際に、申込みを行った組織（企業）による内容の承認（保証）も合わせて行われればよい。

認証技術を使用してこれを実現する例を図 7-5 に示す。IP 指定事業者は申込みを行った組織から割り当て内容が正しいことを承認するディジタル（電子）署名付きの文書をもらい、JPNIC に更に自らの署名を付与して割り当て報告を行なうというものである。

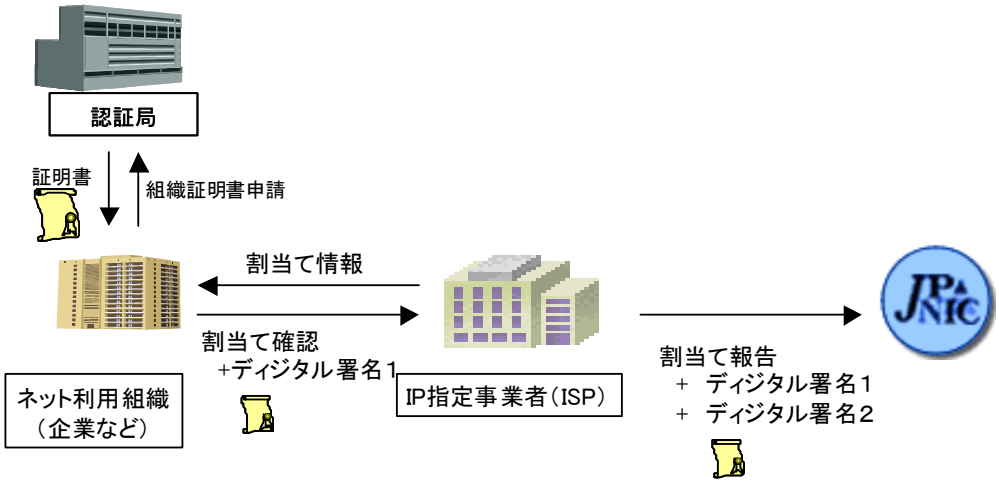


図 7-5　ネット利用組織（ユーザ）の認証方式

この認証の方式をとることにより、IP 指定事業者が配信するネット利用組織の IP アドレス割り当てに関する情報は非常に信頼性の高いものになり、以下のようなネットワークサービスが可能になる。

・割り当て先（ネット利用組織）またはその情報通信機器との安全なメッセージ交換サービス

・割り当て先（ネット利用組織）やユーザネットワークの実在性についての一般または特定者への通知サービス

ところで、現行では、IP アドレスブロックの割り当て時に IP 指定事業者が JPNIC に報告する内容は 2 章表 2-6 に示した事項となっている。

JPNIC の「IP アドレス割り当て報告申請フォーム（ユーザネットワーク用）」（http://jpnic.jp/doc/jpnic-00889.html）によれば、表 7.2 中のうち、b. [ネットワーク名]、B. [network-plan]については表 7-1 のような内容を記述することになっている。

表 7-1　割り当て時に行なう報告項目詳細

b. [ネットワーク名]	このネットワークを表す、意味のある任意の文字列を記入する。 ネットワーク名には、ネットワークが割り当てられる組織に関連のある名前を指定する。 また、英大文字，数字，"-" (ハイフン) のみを用いて 12 文字以内で記述する。複数のネットワークアドレスが同じネットワーク名を持つことも可能。 ネットワーク名は、インターネットレジストリの整合性チェックなど、主として管理目的に使用される。
B. [network-plan]	新規に構築するネットワークの詳細情報をサブネット毎に以下のフォーマットで記入する。ただし、プライベートアドレスを用いて構築する部分については記入しない。 address : ネットワークアドレス 申請時に割り当てるアドレスが確定していない場合には、 代わりに 10.0.0.0 からを使用して記入する。 mask : サブネットマスク connect : YES、NO または PART YES : インターネット接続する NO : インターネット接続しない PART: パートタイム接続(たとえばダイヤルアップ接続など)の場合 n0 : そのサブネットの直後のホスト数 n1 : そのサブネットの 6 カ月後のホスト数 n2 : そのサブネットの 1 年後のホスト数 remark : ネットワークの使用組織、用途(目的)を記入する。 日本語(全角)、英語(半角)表記が可能。 例) ・division：経理、総務、開発、販売、情報システム、 計算機センター、東京 NOC、大阪 AP HQ,Branch,R&D,Marketing,Sales support-group,customer-svc ・purpose ：バックボーン、サーバ、ダイヤルアップ LAN、WAN、ネットワーク R&D-network,HQ-net dial-up,dialup-ports,servers,point-to-point

このようにネット利用組織は、現行でも IP 指定事業者および JPNIC に対しては、割り当て先の組織や IP アドレスが振られるネットワークの用途（目的）について、ある程度の情報を示すことになっており、その一部は一般向けにも公開されている。(B. [network-plan]の情報は公開対象外)

ただし、以下の項目についてこの情報の中には含まれておらず、JPNIC や IP 指定事業者を含め、ネットワーク利用組織以外の者がこうした情報を得たい場合は、直接組織の担当者等と交渉の上で入手するしかない。

・割り当てた各 IP アドレスに情報通信機器が接続されアクティブな状態であるか（あるいは予備としてプールされているか）

・割り当てた各 IP アドレスに接続した情報通信機器の内容（用途やサービス）

・割り当てた各 IP アドレス接続先の情報通信機器の設置場所、位置

今後、ネットワークサービスがより高度化、複雑化する中で、B. [network-plan]を含め、上記のような情報を組織外に示す必要が出ることは十分に考えられる。担当者の手を逐一煩わすことなく、ネットワークを通じて信頼性の高い情報を示せるような仕組みがあれば、これまで実現できなかったような新しいネットワークサービスやビジネスに多いに利用されるのではないだろうか。

認証技術を利用する仕組みとしては図 7-6 のように図 7-5 の手順で登録する内容(項目）を拡張して、前述した情報を含めて認証を取る方式が考えられる。

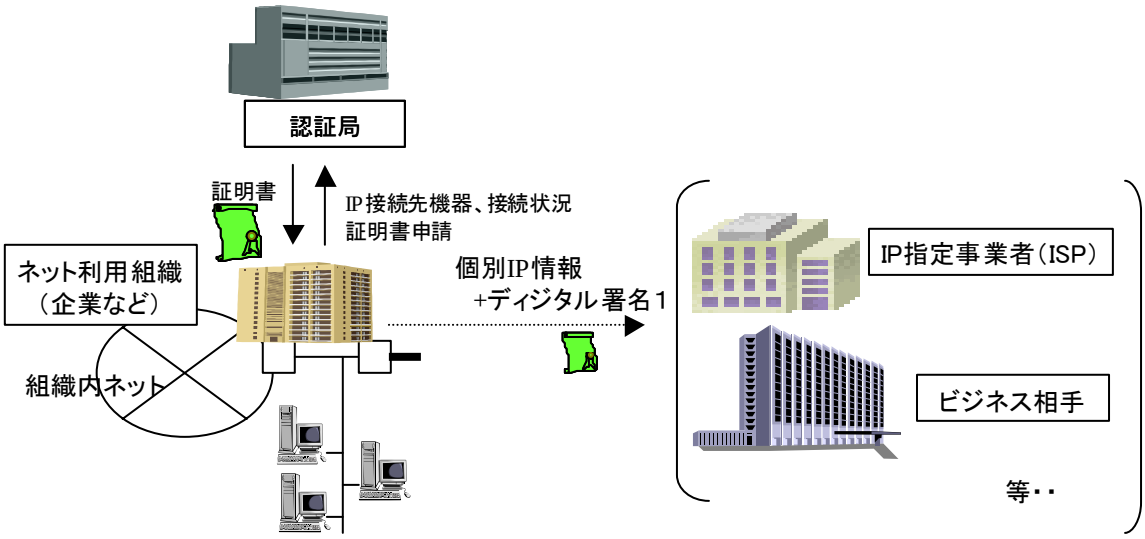


図 7-6　IP アドレス利用先の認証

この認証の方式をとることにより、前述したサービスに加え、以下のようなネットワークサービスが可能になる。

・割り当て先（ネット利用組織）のインターネット接続ネットワークの利用（計画）所についての一般または特定者への通知サービス

・割り当て先（ネット利用組織）の IP アドレス接続先機器の内容、設置場所についての一般または特定者への通知サービス

・割り当て先（ネット利用組織）の IP アドレス利用状況（使用、未使用）についての一般または特定者への通知サービス

7.1.4.　ユーザネットワークにおける IP アドレスの割り当てルールの新設

7.1.3 に示したように、ネット利用組織に割り当てられた IP アドレスの利用についての情報を必要に応じて外部者が入手できることで新しいネットワークサービスが出現する可能性がある。

ところで、この仕組みを利用して、特定の目的・用途や地域に割り当てられた IP アドレスに向けたネットワークサービスを行なうこと考えると、サービス提供者は IP アドレスの利用内容（証明）を確認するのに図 7-6 に示した認証局と通信を行なう必要がでてくる。もし、サービスが大規模な処理を必要とするような場合、逐一通信を行なうようなことでは機能として成り立たないことになる。このため、IP アドレス自体に特定の用途や接続場所等の意味が込められているようにする必要がある。

現行の IP アドレスの割り振り方式には、特定のアドレスブロックについて接続する情報通信機器の用途等を限定するルールはない。もし、ユーザネットワークで情報通信機器に IP アドレスを割り当てる際に、ユーザ共通の割り当てルールがあり、ルールに則った割り当てが一斉に行われ、加えて 7.1.3 の認証も行うことが可能となるならば、更に特定の IP アドレス（接続情報通信機器）に向けたネットワークサービスが可能となろう。

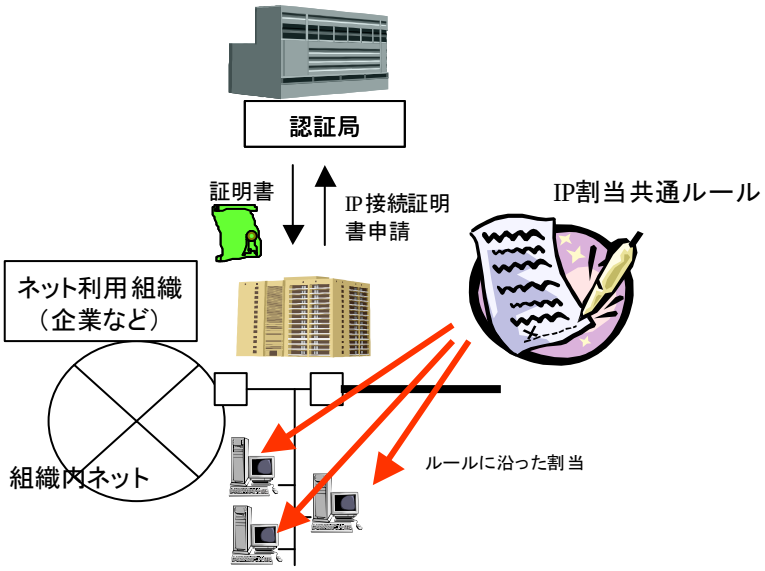


図 7-6　IP アドレスの利用別割り当て

7.1.5.　認証の対象と実現できるサービス

これまでの記述により、IP アドレスの付与や利用に関し、認証技術を用いることで既存の課題を解消したり、新たに出現する可能性のあるサービスがあることがわかる。

これまで挙げた認証の方式と可能性のあるサービスを表 7-2 に整理した。

表 7-2　IP アドレス認証により可能となるサービス例

No.	認証対象	可能になるネットワークサービス
A	IP 指定事業者担当者（ホストマスタ）およびクライアント	・IP 指定事業者、または情報通信機器との安全なメッセージ交換サービス ・IP 指定事業者（ホストマスタ）の実在性や IP アドレス使用の真正についての一般または特定者への通知サービス
B	ネット利用組織（担当者）	・割り当て先（ネット利用組織）またはその情報通信機器との安全なメッセージ交換サービス ・割り当て先（ネット利用組織）やユーザネットワークの実在性についての一般または特定者への通知サービス
C	ネット利用組織の IP アドレス接続機器の用途等	・割り当て先（ネット利用組織）のインターネット接続ネットワークの利用（計画）についての一般または特定者への通知サービス ・割り当て先（ネット利用組織）の IP アドレス接続先機器の用途、サービス内容、設置場所（地域）等の情報を一般または特定者へ通知するサービス ・割り当て先（ネット利用組織）の IP アドレス利用状況（使用、未使用）についての一般または特定者への通知サービス
D	割り当てルールに基づき設定した接続機器	（基本的にはCと同様）

次節では、こうしたサービスの組み合わせや応用により展開できる可能性のある応用サービスやビジネスの例を示し、実現に向けての要件や課題を考察してみたい。

7.2.　IP アドレス認証による応用サービス、ビジネス例

本節では IP アドレスを認証することにより新たに可能となるサービスやビジネスのアイデア例や実現に向けての課題点を表７-3 のように分類して示してみたい。

表 7-3　IP アドレス認証により可能となるサービス例

サービスタイプ	内容
既存通信事業補完型	現行の情報通信技術を使用して、安全性に課題のある既存のビジネス、サービスの部分を解決し、全体の信頼性を向上させるサービス。
高セキュア通信機能型	ISP などの通信事業者が、顧客のネットワークの安全を維持するために、通過するパケットに対するルートやフィルタリング機能を顧客のニーズや環境を考慮してより安全に高めるサービス。
新通信インフラ提案型	IP アドレスのブロック域に特定用途の意味を持たせることを前提に、実現できる可能性がある新しい通信サービス。

7.2.1.　既存通信事業補完型

ここでは、表 7-2 に示したＡ、Ｂを中心に JPNIC、IP 指定事業者、ネット利用組織間で認証技術によりインターネットを介して交換する情報の信頼が高まることを前提とした応用サービス、ビジネスを挙げてみたい。

7.2.1.1.　ネットワーク接続関連情報照会

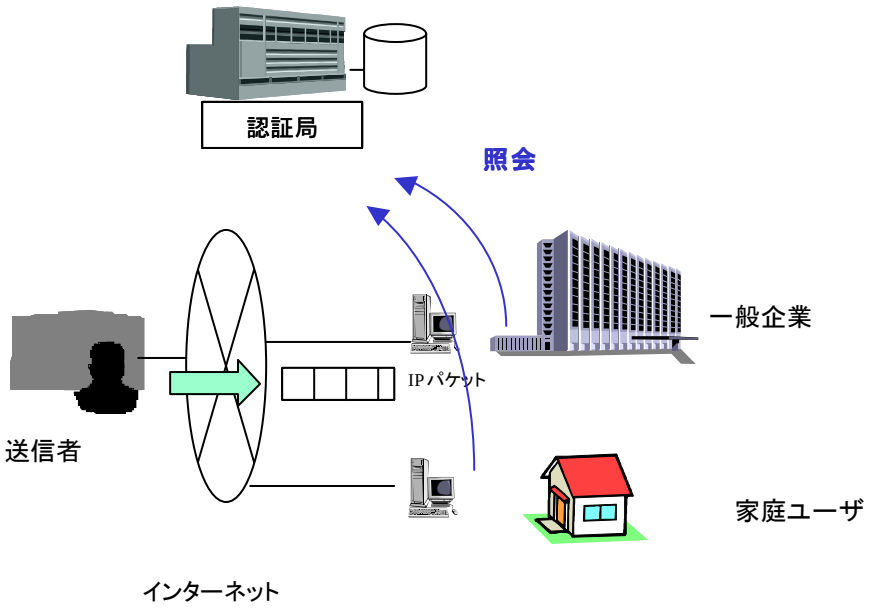


図 7-7　送信者（パケット）の確認イメージ

現在、インターネットを通じて通信を行なう際、相手先の IP アドレス（あるいはドメイン名）が正規に割り当てられた相手であるか、またその相手が信頼できる事業者なのかを確認するのは簡単ではない。現行で可能な一般的な手段は JPNIC が提供する whois システムにより IP アドレスの割り当て先を確認し、そこで得られた割り当て先の企業名等から必要に応じて別の信用調査機関（帝国データバンク等）が調査したその企業の事業に関する情報を参考にするというものである。ただし、前述したように現行の whois システム内に搭載されている情報は、信頼性と網羅性の点で十分ではない。また、ネットワーク事業の内容を調べるのに、わざわざ別の信用調査機関のサービスを利用するというのは業務上無理がある。

そこで、表 7-4 の A、B のサービスを応用し、IP アドレス割り当て範囲やその用途、またその組織自体に関する信頼性の高い（第三者により証明された）情報を必要に応じて企業や一般ユーザに提供するサービスが考えられる。

このサービスは、ネット利用組織から直接情報が得られる IP 指定事業者が手がけやすいと思われる。ただし、各事業者が保有している情報は自社の顧客のみであるため、そのままでは提供できる情報は限定されてしまう。そのため、全 IP 指定事業者から情報を集約する機関や、あるいは IP 指定事業者間で必要に応じて情報を提供し合えるようなシステムがあれば、利用者は 1 つの IP アドレス情報からワンストップで必要な情報を得ることができるようになるだろう。

7.2.1.2.　通信相手確認サービス

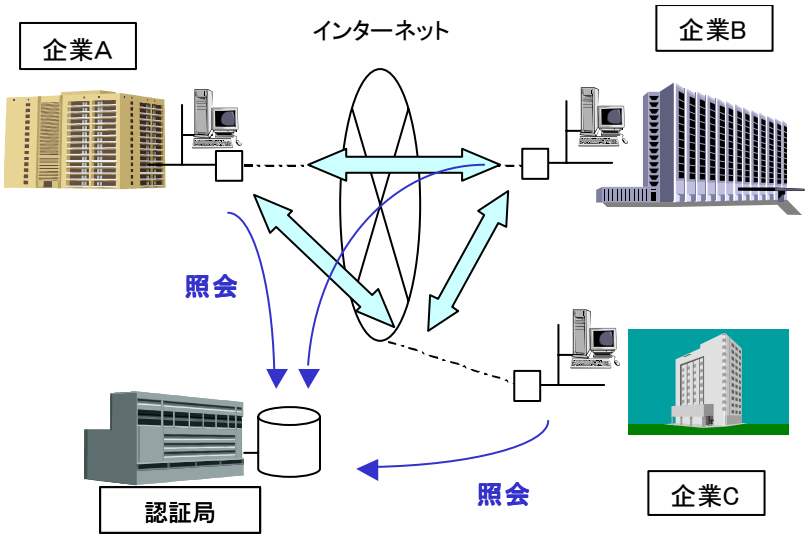


図 7-8　企業間通信サービスにおける相手先の確認イメージ

現在、異なる企業サイトのネットワークを安全に接続する方式として VPN（Virtual Private Network）が使用されることが多い。この場合、通信相手間では IP アドレスを含む使用する機器の環境を交換し、ルータやサーバに設定する必要がある。

企業内で事業所間を接続する場合や日頃付き合いの深い企業間の場合は、接続情報について信頼の高いものを得られるが、今後のネットワークビジネスの中で、多数の企業間を VPN のような形で結ぶような場合、相手先のネットワーク接続についてより信頼性の高い情報を簡易な方法で入手できることが求められる。

7.2.2.　高セキュア通信機能型

ここでは、表 7-4 の C を中心に認証技術を利用して、ネット利用組織がネット上で自組織に割り当てられた IP アドレス（接続された情報通信機器）の利用に関する情報を特定者または一般に通知できる、また特定のルールに則ってインターネットに接続する情報通信機器に IP アドレスが振られることを前提とした応用サービス、ビジネスを挙げてみたい。

7.2.2.1.　ネット利用組織の IP アドレス利用状況を考慮したルーティング

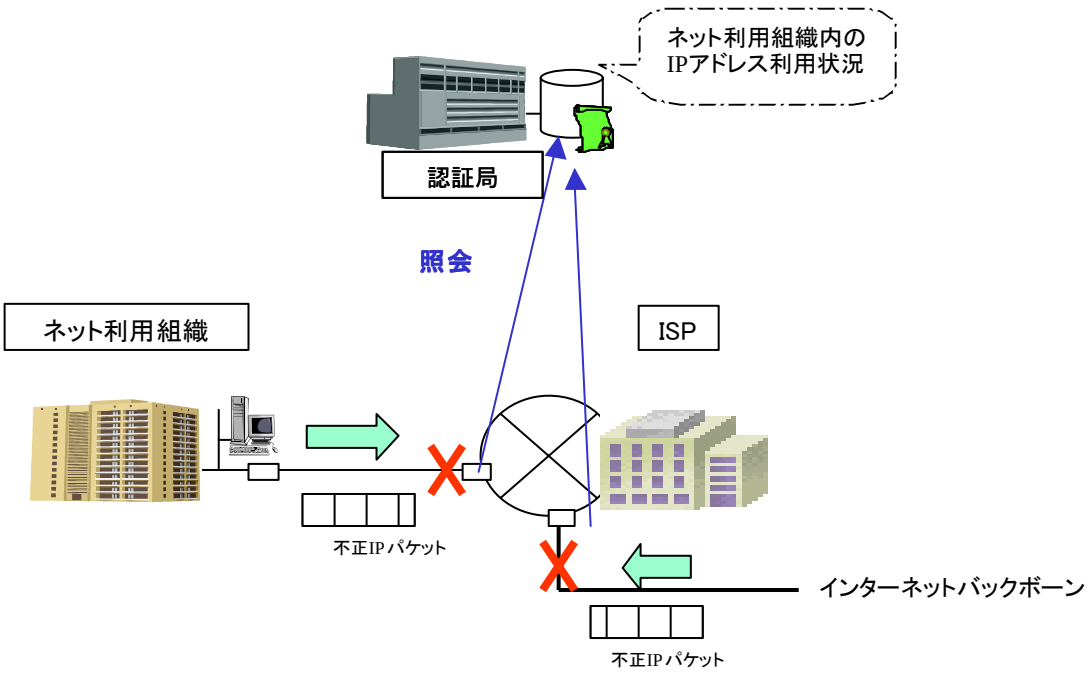


図 7-9　未使用 IP アドレスのパケットをブロックする

ネット利用組織から IP アドレス利用状況を確認できることにより、ISP では、ネット利用組織から AS に届くパケットのうち未使用であるはずの IP アドレスから発信されたものを選別（フィルタリング）できるようになる。また、ネット利用組織へ送信するパケットについても未使用 IP アドレスへ送信しているパケットを選出して IDS などに応用することが考えられる。

7.2.2.2.　特定用途割り当てを考慮したルーティング

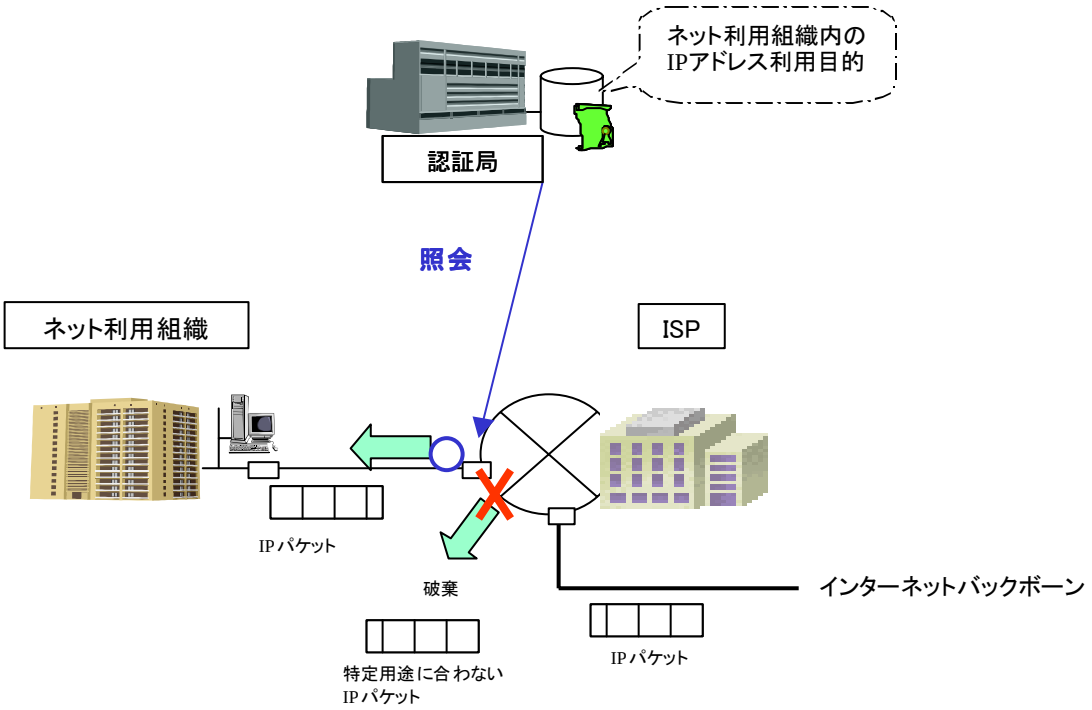


図 7-10　特定用途にマッチしない IP パケットのフィルタリング

ネット利用組織から使用する IP アドレスの接続機器の用途や場所を確認できることにより、ISP は、ルータを通過させるパケットについてその用途毎にポリシーを定めることが可能となり、新たなルーティングサービスを付加することが可能となる。

例えばネット利用組織向けに送信されたパケットについて、未使用の IP アドレスに送信された IP パケットや認証局に登録されていない IP パケットの場合は自動的に破棄する（通過させない）、パケット送信元と送信先の特定用途がマッチしている場合のみ通過させる、などが実施可能になる。

7.2.3.　新通信インフラ提案型

ここでは、表 7-4 の C、D を中心に、IP アドレスのあるブロック域を特定用途に割り当てるルールが確立され、ネット利用者が使用されている IP アドレスに接続されている機器の用途や場所が簡単に確認できるようになることを前提として、特定用途かつ不特定多数の IP アドレス先を対象とするネットワークサービスのアイデアを挙げる。

特定用途として地理的条件や利用者（年代、職業）等、様々な対象（セグメント）が考えられるが、ここでは次のように分類、整理を行なった。

（ア）学校・教育

（イ）街・地域

（ウ）家庭

（エ）公共・メディア

（オ）社会インフラ

（カ）医療

（キ）その他

なお、本アイデアの多くは JPNIC 内で組織されている「認証情報の応用専門家チーム」で検討の中から挙がったもので、現行の社会生活の中で不便、不安に感じる事象を中心に、ネットワーク社会の中で IP アドレスが認証できることにより社内生活が便利、安心になるようなサービスが示されている。なお、今回の検討については、あえて法制度や規制などによる実現難度は考慮していない。

次ページより、分類ごとに挙げられたアイデアを具体的に示してみたい。

7.2.3.1.　学校・教育

（1）　登下校時間通知サービス

【概要】

学童の交通事故を予防するためには、登下校の時間帯は車両よりも歩行者を優先する交通制御や車両への事前の情報提供が有効と思われる。小中学校などでは、行事や地域事情（天候や災害）により通常と異なる時間帯に登下校することがある。こうした場合に、通学地域内の IP アドレスを振られた情報通信機器向けに学校から登下校時間情報を配信すれば、情報を受けた各機器は以下のようなアクションを起こすことが可能となる。

-信号機

通学路の進行方向を優先（青の時間帯を長くする）する。

-車（カーナビ）

スクールゾーンを赤色等で強調表示し、多数の児童・生徒が通る可能性を警告する。

-携帯電話（メール、着メロ）

周辺注意のメールを受信する。また、専用の着信音で通知を行う。

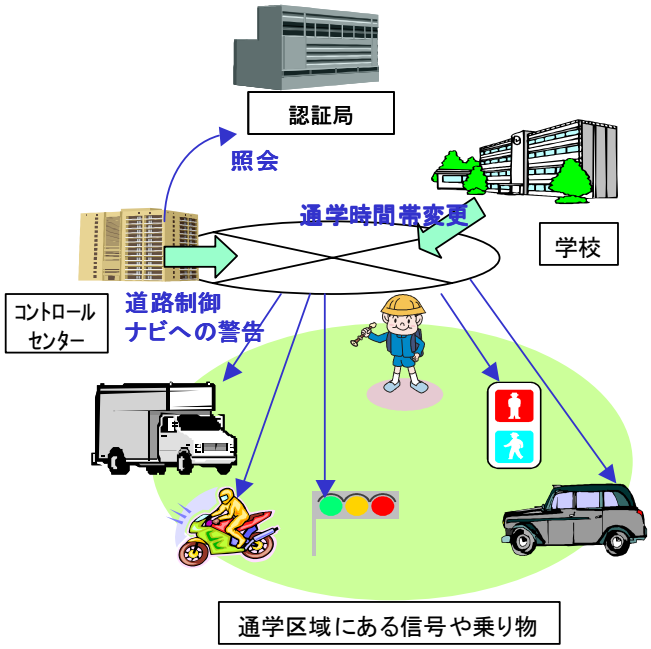


図 7-11　登下校時間通知サービス

【サービス対象者・ニーズ】

サービス提供元：

学校、自治体　[登下校の時間帯変更の注意を促したい]

サービス提供先：

家庭　[登下校の安全を高めたい]

【アプリケーションの機能・実現方式】

- 各種 GIS データへの通学路の設定機能
- 登下校時間帯入力（変更）機能
- 登下校変更時間の一斉配信機能

【認証方式・技術】

- 送信者が確実に学校からであることを確認する。
- 送信先を当該地域に限定する。

7.2.3.2.　街・地域

（1）　災害時の地域一斉連絡

【概要】

局所的な災害などが生じた場合、地域毎に、より細かな即時性の高い情報（ニュース）が配信される必要がある。地域向けの連絡手段としては現在 CATV による地域放送があるが、加入者は限られており、地域全域に情報を行き届けるための基盤となっているとは言いがたい。もし、情報通信機器の IP アドレスや認証情報の中に特定の地域に設置（接続）されていることを示す情報を含めることができれば、その地域の機器向けに一斉に緊急情報（信号）を配信することが可能となる。情報（信号）をキャッチした後の警告等の表示の仕方については情報通信機器ごとのアプリケーション仕様となるが、例えば次のようなことも可能となる。

-地域内の公園、商店街等のスピーカーによる緊急連絡

緊急情報を音声により周辺に伝える。

-家庭内の情報家電による緊急連絡

モニタによる文字や映像表示により住人に注意喚起を行なう。

-携帯電話、車等の通信機器による緊急連絡

音声や振動により、搭乗者へ注意喚起行なう。またモニタで詳細情報を表示する。

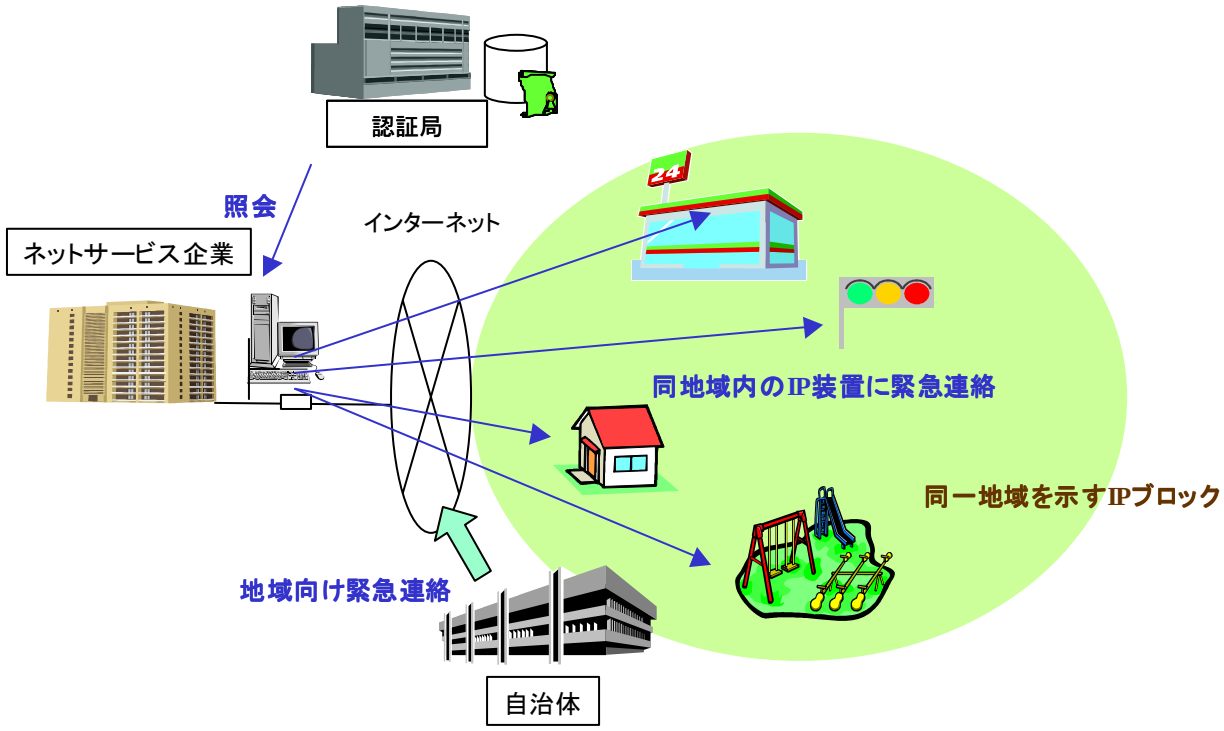


図 7-12　災害時の地域一斉連絡

【サービス対象者】

サービス提供元：

自治体、自治会　[災害時に正確な情報を迅速に地域に伝えたい]

サービス提供先：

住民　[災害時に多様な手段で情報を得たい、正確な情報を知りたい]

【アプリケーションの機能・実現方式】

・送信対象機器範囲確認機能

・対象機器向け情報一斉配信機能

・パケット経路変更、地域外パケットフィルタリング機能

【認証方式・技術】

・ 配信先の機器が該当地域に設置されたものであるか、IP アドレスブロック域や認証機関に登録された属性情報により確認する。

（2） 福祉用の地域連絡

【概要】

幼児や徘徊癖ある老人が自宅からいなくなってしまった際などに周辺地域に容姿や服装、連絡先などの情報を一斉配信し、支援を求めるサービス。また、1 人暮らしの人が近所への緊急の通知手段として使用するなど、様々な連絡用として応用できる可能性がある。

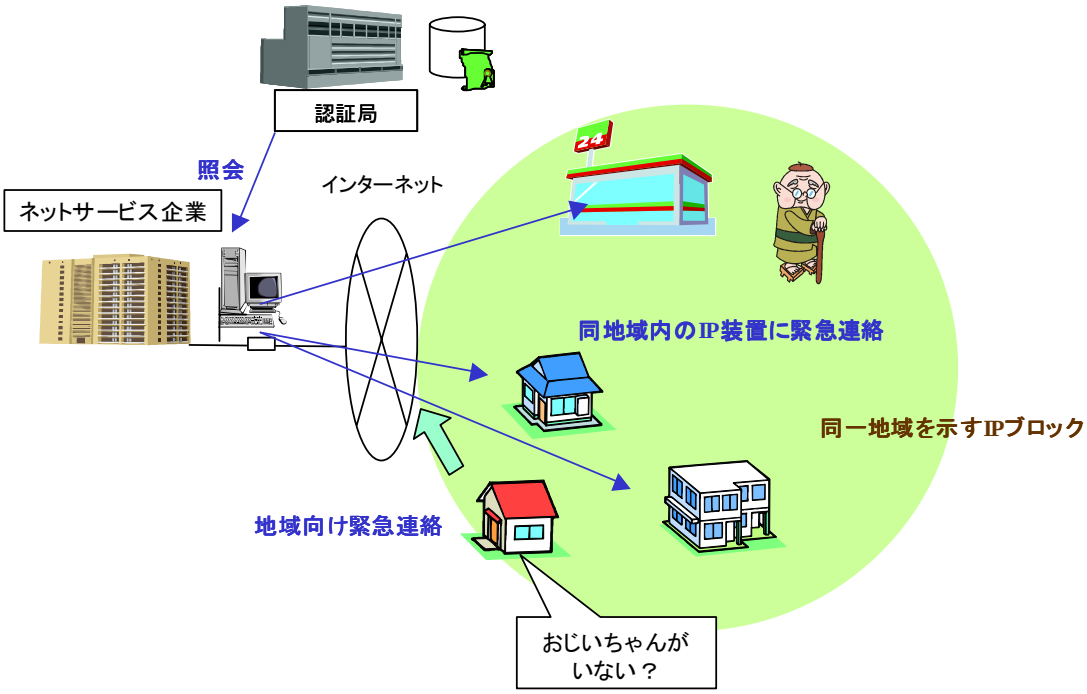


図 7-13　福祉用地域連絡

【サービス対象者・ニーズ】

サービス提供元：

自治体、自治会　[住民が安心して暮らせるサービスを提供したい]

サービス提供先：

介護の必要な家庭　[徘徊者を早く探し出したい]

【アプリケーションの機能・実現方式】

・送信対象機器範囲確認機能

・対象機器向け（警告）情報一斉配信機能

・パケット経路変更、地域外パケットフィルタリング機能

【認証方式・技術】

・ 配信先の機器が該当地域に設置されたものであるか、IP アドレスブロック域や認証機関に登録された属性情報により確認する。

7.2.3.3.　家庭

（1）　ペット認証サービス

【概要】

ペット（犬、猫等）の首輪などに小型情報通信機器を取り付け、ネットワークを通じてペットとの通信を可能にする、飼主や自治体（保健所）などによって実施するサービスである。IP アドレスブロックの中にペット用のアドレスブロックも用意する。

具体的なサービスとしては、以下のようなことが考えられる。

-GPS や地域に設置されたセンサーと組み合わせ、ネット上で猫などのペットの現在位置を確認する。また、他のペットの位置も確認できることより、ペットの集まりやすい場所や行動（なわばり）範囲などをネットから確認することができる。

-狂犬病の予防注射時期などを該当時期に保健所がペット向けに通知する。受信した小型情報通信機器にそれに合わせて発光する等の機能をつけると第三者にも認識が可能になる。

-小型情報通信機器を通じて音声や特殊音等により餌や注意の情報をペットに伝える。

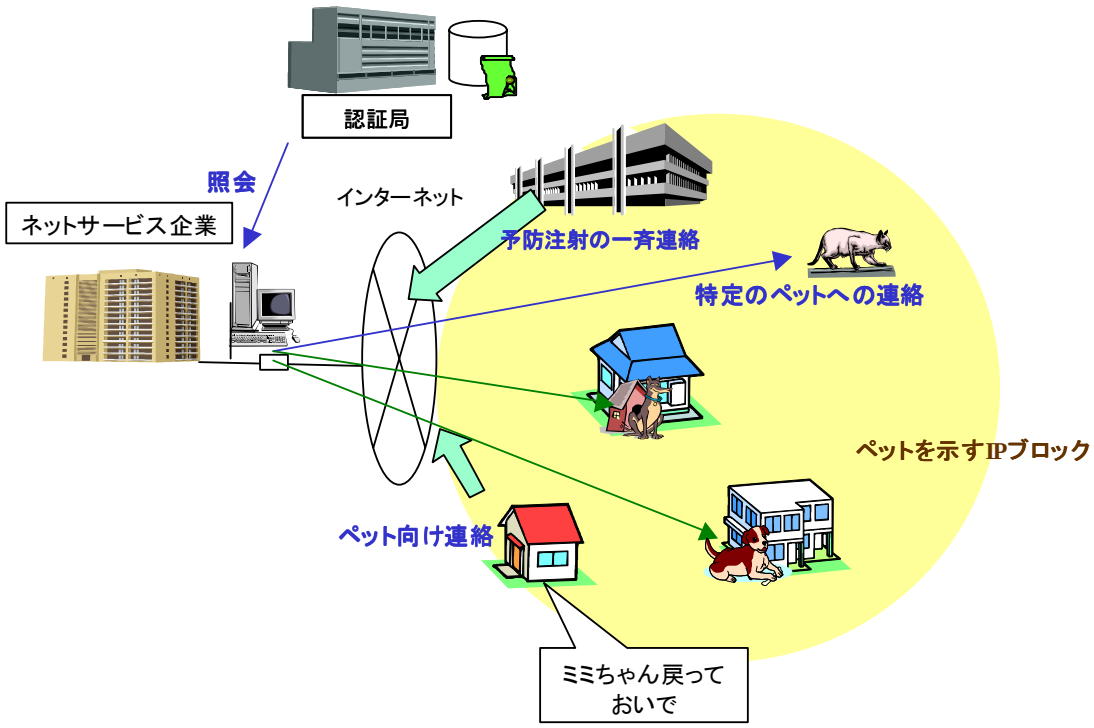


図 7-14　ペット用 IP アドレスブロックとその利用

【サービス対象者・ニーズ】

サービス提供元：

保健所、警備会社

[住民が安心して暮らせるサービスを提供したい、ペット飼主に注意を促したい]

サービス提供先：

ペットの飼主　[ペットの行動を把握したい、コミュニケーションを上げたい]

【アプリケーションの機能・実現方式】

・ペット位置確認機能

・飼主との通信機能

・アラート情報表示（光、音声）機能

【認証方式・技術】

・ ペット用の IP アドレスブロック域を使用する。認証機関に登録されたペットに関する情報より、飼育環境（飼主）を確認する。

（2）　（家庭外からの）家庭内機器・装置の遠隔サービス

【概要】

現在、身近な家電製品の中には、ネットワークに接続して家の外から遠隔で家電の操作を行なえるもの（ネット家電）が現れている。今後の家庭では、このような家電以外にも様々な電気機器や装置のネットワーク化が進んでいくと思われる。例えば、以下のような装置がネットワークに接続することにより、留守中でも通常と同じように家事が行えたり、家の中を警備するようなサービスが可能となる。

- 留守中に庭の植物へ天候の状況を見ながら散水を行なう、またペットへの餌の量をモニタ映像を見ながら調節する。
- 部屋内で侵入があった場合に、監視カメラ映像を警備会社や警察に転送する。また、モニタを見ながら遠隔で防犯インクなどを侵入者に噴射する。
- 車から降りずに車庫のシャッター操作（開閉）を行なう。また、旅行先などで遠隔で天窓を開閉し、部屋内の空気を入れ替える。

なお、こうしたサービスを行なうには、プライバシー保護の点からサービス提供範囲が限定され、確実に利用対象者だけの操作を受け付ける仕組みが必要である。

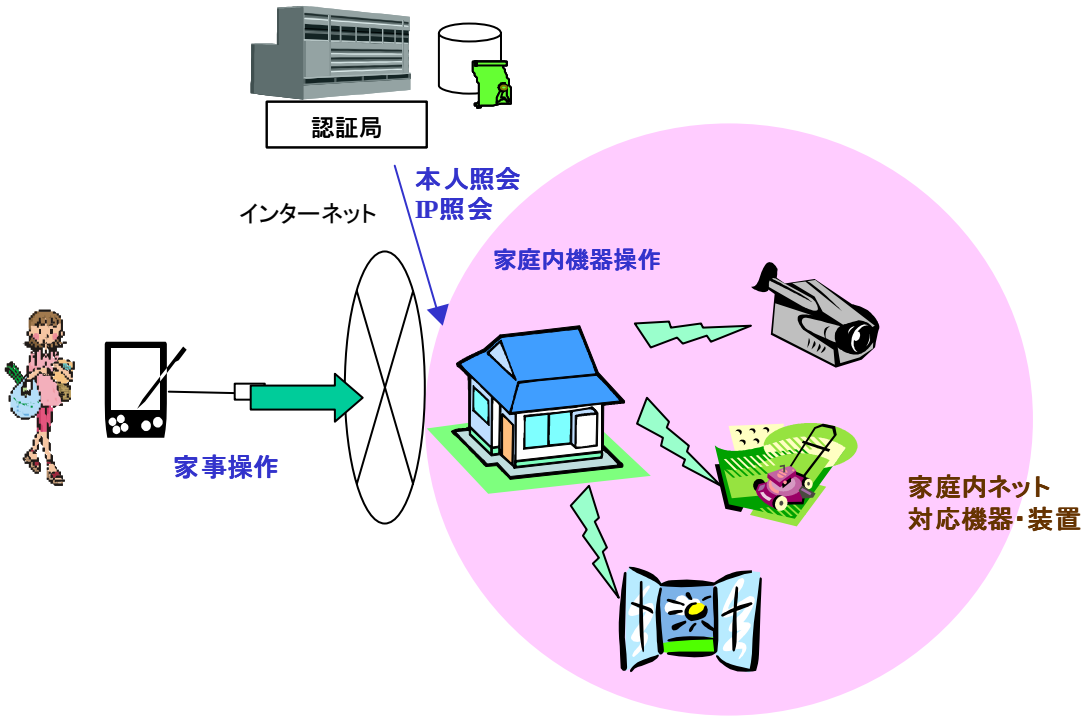


図 7-15　家庭内機器・装置の遠隔サービス

【サービス対象者・ニーズ】

サービス提供元：

警備会社、ハウジングメーカー

[住民が安心して暮らせるサービスを提供したい、付加価値の高い家を提案したい]

サービス提供先：

住人　[安心して旅行に出かけたい、生活をより一層快適にしたい]

【アプリケーションの機能・実現方式】

・遠隔操作者確認機能

・動作終了（状態）通知機能

【認証方式・技術】

・ 操作者自身の認証の他、操作先の情報通信機器が操作を許可する IP アドレスになっているか等、複数の認証により判定を行なう。

（3）　ネット家電を通じての緊急情報発信サービス

【概要】

住宅火災を防止するため、アイロンや電気ストーブなど発熱する家電について標準使用時間を大幅に越えてスイッチが入った状態になっている場合に、家人が不在やなんらかのトラブルがあったとみなしてマンションの管理人や隣の世帯、製造メーカーの保守部門などにネットを通じて警告情報を通知するようなサービスである。

また、逆に普段使用するはずの機器が一定時間全く使用されていないことを警告するようなサービスも考えられる。例えば、家族が別々に暮らしている場合や、老親と子供の世帯が別の場合などでは、直接電話などで連絡を取り合うのが億劫となる場合もある。この場合、遠隔で相手方の家庭内の機器利用がわかれば、普段通り生活していると推測でき、また、通常使用されるはずの機器が暫くの期間使用されていないような場合は、なんら異常があるとみなして関係者に通知を行なうようにすることも可能である。

こうしたサービスでも機器間や特定の相手の通信で確実に通信したい相手か確認できる必要があり IP アドレス認証の仕組みが活用できるものと思われる。

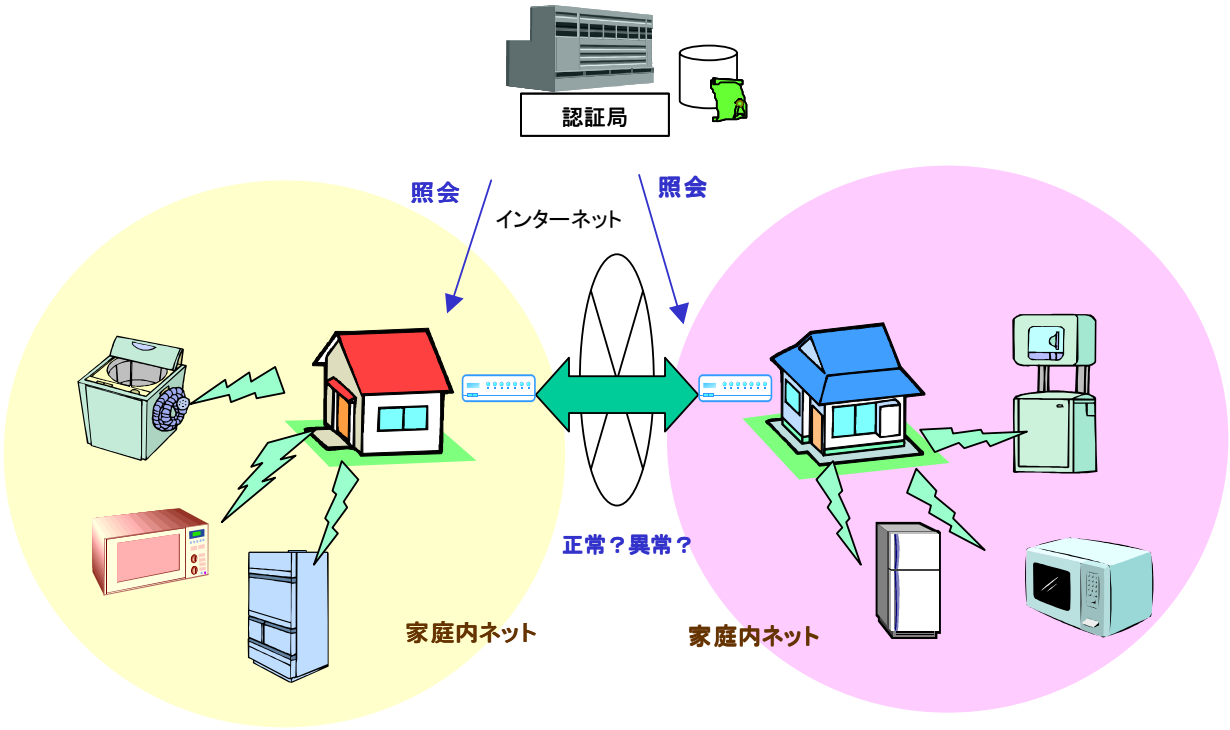


図 7-16　家庭内機器を通した家庭間緊急連絡サービス

【サービス対象者・ニーズ】

サービス提供元：

家電メーカー、警備会社、自治会

[住民が安心して暮らせるサービスを提供したい、付加価値の高い製品を販売したい]

サービス提供先：

住人（マンション等）[安心して外出したい、離れた家族の様子を知りたい]

【アプリケーションの機能・実現方式】

・送信相手登録機能

・送信条件設定（異常、正常）機能

・異常時リモート対応機能（スイッチオフ等）

【認証方式・技術】

・ 通信し合う機器自体の認証、また異常時の緊急措置を実行できる権限があるか判定を行なう。

（4）　幼児・児童玩具向け通信サービス

【概要】

今後、幼児・児童を対象とした玩具でもインターネットに接続機能を備えるものが急増してくると思われる。こうした玩具からアクセス要求があった場合、幼児・児童からということが予め認識できれば、不適切なサイトへのアクセスやコンテンツの受信を ISP 側で止めることができる。

このサービスの実現には、玩具に割り当てる IP アドレスブロックの中に幼児・児童用の機器ということがわかるような仕組みがあるとよいだろう。

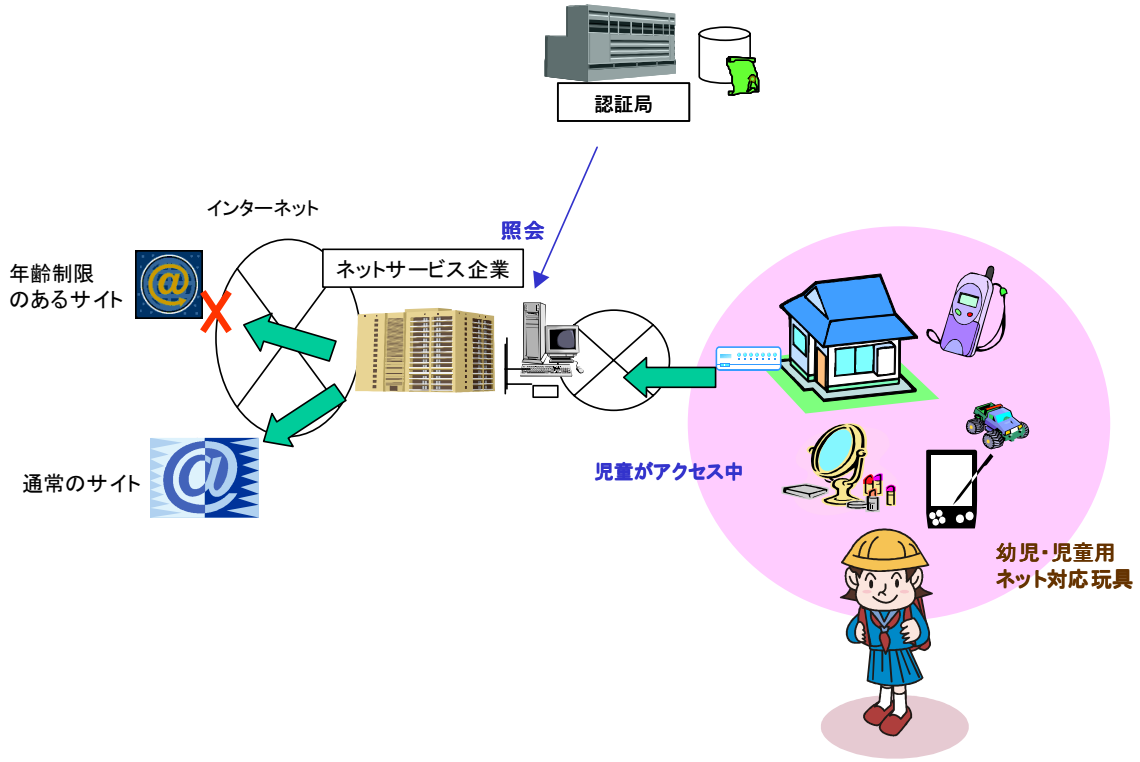


図 7-17　幼児・児童向け通信サービス

【サービス対象者・ニーズ】

サービス提供元：

ＩＳＰ、ＷＥＢサイト　[資格のある利用者のみアクセスを受け付けたい]

サービス提供先：

玩具メーカー、家庭　[子供に年齢制限のあるサイトにアクセスさせたくない]

【アプリケーションの機能・実現方式】

・送信先機器属性判定機能

・条件外パケットフィルタリング機能

【認証方式・技術】

・ 玩具に割り振られた IP アドレスブロック等により機器を操作する者の年代を判定する

7.2.3.4.　公共メディア

（1）　電子書籍への閲覧制限サービス

【概要】

公共や学校図書館ではスペースの関係で蔵書を大幅に増やすのは難しい状況にあり、電子書籍に対する関心が高まっている。ただし、電子書籍を購入した場合、現在、貸し出しの扱いは難しい。電子的なコピーが自由にできるのでは著作権上問題であり、また公共図書館内など特定の場所に設置された PC でしか閲覧できないのでは利用しづらく普及は見込めないだろう。インターネットを通じた利用方法についても大きな課題である。

もし、購入する際にその電子書籍が利用できる範囲を予め特定でき、利用する PC がその条件にマッチしていることが認証できればこの課題を解決することができる。

例えば、学校図書館の場合は、利用された PC がその学校内に設置された PC または生徒（児童）の携帯型 PC であれば、閲覧期限付きで電子書籍のコピーや閲覧が可能になるといったものである。同様に公共図書館の場合は地域住人の家に設置された PC または地域住人が常時使用する PC であるかが認証できれば、同じく閲覧期限付きで電子書籍のコピーや閲覧を可能とする。

これらの仕組みを実現するのに IP アドレスに地域ブロックや学校ブロックを割り当てや IP アドレス認証は効果のあるものと思われる。

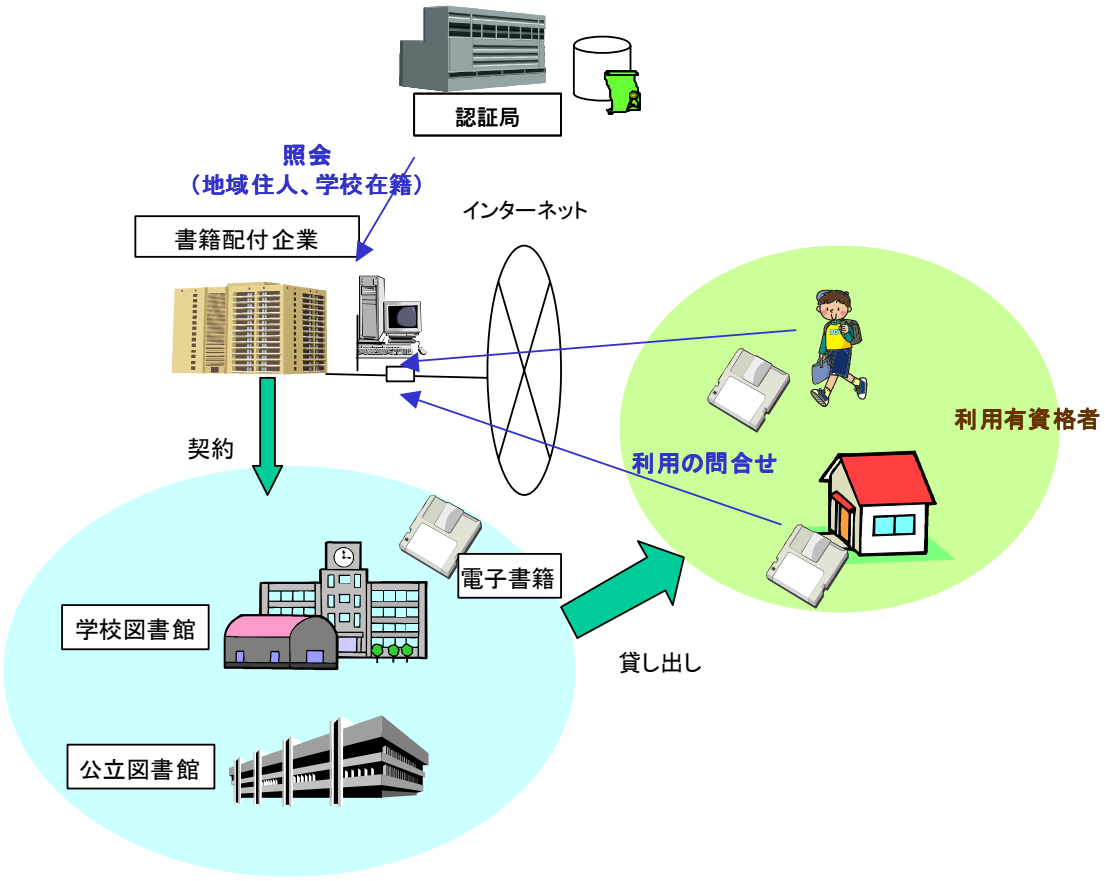


図 7-18　電子書籍の利用者認証サービス

【サービス対象者・ニーズ】

サービス提供元：

学校図書館、公共図書館　[蔵書数を増やしたい、管理費を下げたい]

サービス提供先：

（学校）生徒、地域住民　[最新の書籍を読みたい、書籍を持ち歩きたくない]

【アプリケーションの機能・実現方式】

・電子書籍利用資格確認機能

・電子書籍使用期限設定機能

・不正閲覧（資格外、期限外）防止機能

【認証方式・技術】

- 電子書籍使用時に、割り振られた IP アドレスから設置場所（地域）、施設（学校、図書館）の利用資格を判断する。
- 電子書籍使用時に、ネットワークを通じて IP アドレス認証局に登録されている利用者の情報（住所、所属先）から使用資格を判断する。

（2）　ネット投票サービス

【概要】

現行の選挙や住民投票は、投票場所や投票の時間帯が限られているため、当日の急な都合によっては投票に行くことが難しい場合がある。また、障害を持つ人が投票場に出向くことも現実的には難しい問題が多い。

もし、ネットワークを通じた安全な投票の仕組みがあれば、出先や投票場に行きにくい住民でも手軽に投票することが可能になる。安価なコストでネット投票が実現できれば、これまでの投票に加え、アンケート調査も兼ねた各種の投票サービスが登場する可能性がある。

ネット投票の仕組みとしては、投票時に個人やその属性の認証に加え、投票する機器の設置場所や形態、発信する IP アドレス等を予め特定させるようにすれば、なりすまし等不正を防ぐ手立てを増やすことができよう。

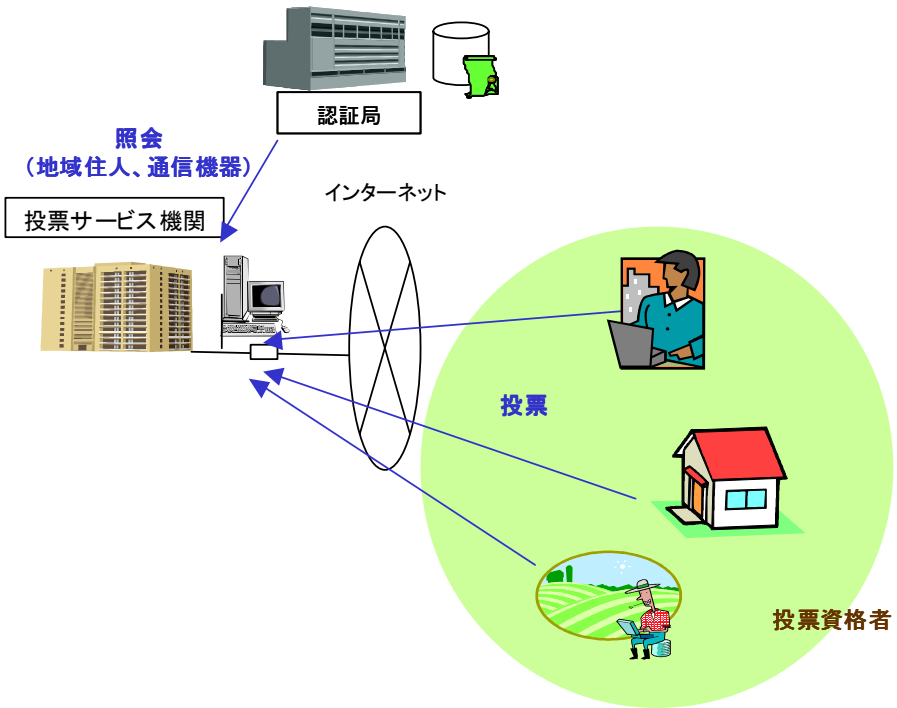


図 7-19　ネット投票サービス

【サービス対象者・ニーズ】

サービス提供元：

自治体　[投票コストを下げたい、民意を知る機会を多くしたい]

サービス提供先：

住民（選挙人）　[投票手段を増やしたい]

【アプリケーションの機能・実現方式】

・投票資格確認機能

・ネット投票機能

・投票結果分離機能（投票者と投じた内容を切り離す機能）

・集計結果提示機能

【認証方式・技術】

・ 投票時に、個人の認証他、投票機器に割り振られた IP アドレスから設置場所（地域)、形態（PC、携帯電話、キオスク端末、等）などからその投票に対する資格の有無や投票集団属性を判断する。

7.2.3.5.　社会インフラ

（1）　緊急時交通制御サービス

【概要】

緊急車両（パトカー、救急車、消防車等）は発進時に道路を優先的に通過できることになっているが、通行車両はサイレンの音や光により緊急車両の存在を認知するため、両端への待避などの行動は遅れがちとなる。また、緊急車両は信号が赤の場合でも交差点を通過するが、非常に危険を伴うためできるだけ緊急車両の動きに合わせて信号制御がされる方が望ましいといえる。

現在車両や交通インフラの IT 化が急速に進展しており、情報通信環境が十分に整い車両間や周辺の交通インフラと通信できるようになる日も遠くないと思われる。このような環境が整備された場合、車両や交通インフラへの IP アドレスの特定域の割り当て、認証は非常に重要になると思われる。前述の緊急車両の場合、GPS 技術と組み合わせることにより、通過道路の信号などの制御装置の IP アドレスブロックに対して進行意思（情報）を一斉配信することができる。各信号はその情報を受取り、適切に点灯時間をコントロールし、緊急車両を安全かつ短時間で現場に誘導することが可能となる。また同時に、周辺の車両（IP アドレスブロック）に対し、通過の意思を一斉配信することで、カーナビゲーションシステムや携帯電話などを通して、緊急車両が近づくことを早い時期に周辺に知らせることが可能となる。

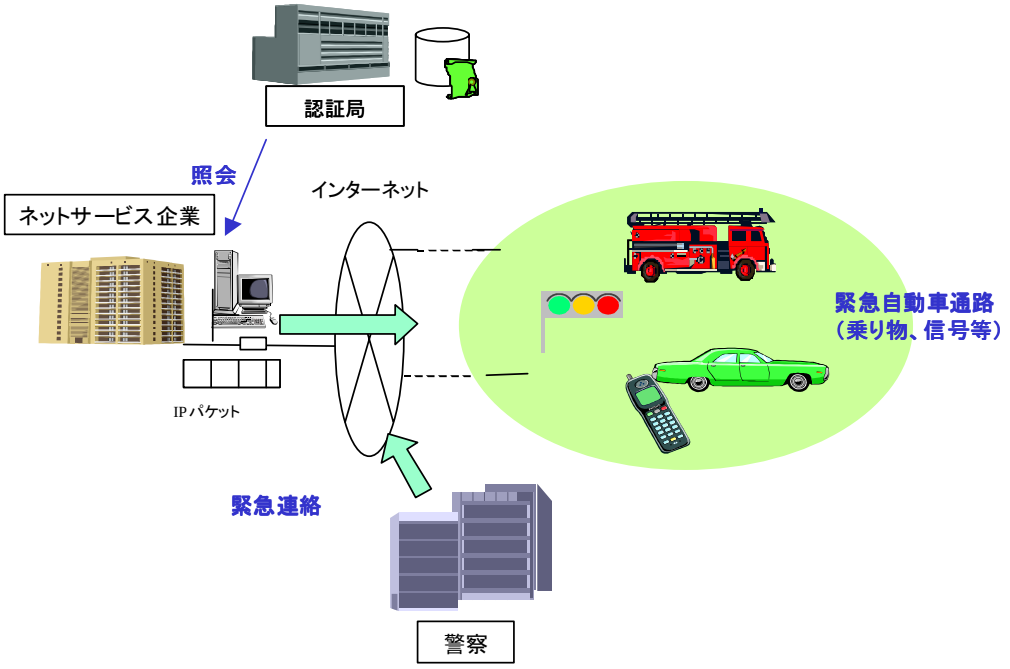


図 7-20　緊急時交通制御サービス

【サービス対象者・ニーズ】

サービス提供元：

公共基盤　[緊急情報を早く、確実に周辺に伝えたい]

サービス提供先：

警察・消防署（緊急車両）　[現場に早く、安全に到着したい]

【アプリケーションの機能・実現方式】

・緊急情報適正範囲ブロードキャスト機能

・緊急情報発信者確認（認証）機能

・緊急情報受信（表示）機能

【認証方式・技術】

- 緊急情報受信側で、発信者が確かに緊急情報を発信できる相手かどうかを IP により確認（認証）する。
- 発信側では、車両用として割り振られ、かつ自分から半径 200 メートル以内などに限定した IP アドレス域に緊急情報を一斉に配信する。

7.2.3.6.　医療

（2）　医療用 IP 閉域サービス

【概要】

医療用の情報は、当事者や許可のある者以外には絶対に渡ることがない仕組みが必要である。特にネットワークを通じた医療情報の交換には十分な配慮が必要がある。

こうした機密性を要するネットワークのセキュリティを高めるのに専用の IP アドレスブロックを設け、同時に認証を実施するのは効果的な方法である。例えば、医療用に使用される情報通信機器に特定の IP アドレスブロックが割り当てられた場合、ＩＳＰなどがパケットをチェックし、データ域が暗号化されていない場合は通過させない、というようなサービスが可能になる。また、通信相手について IP アドレスブロックや認証情報から不適切な相手かどうかを判別するようなサービスも考えられる。また、適切な送信相手に対しては、経路や優先度により同じ IP アドレスブロック内で閉域のネットワーク化が期待でき、レントゲン情報などは非常に大量のデータ容量を必要とするような場面での高速通信サービスが期待できる。

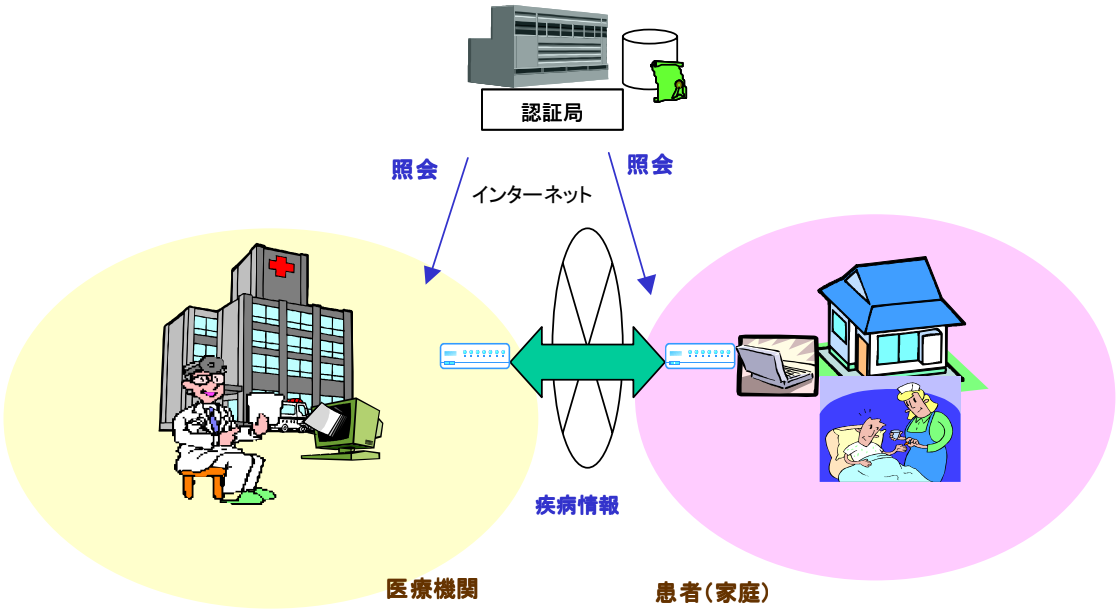


図 7-21　医療用 IP 閉域サービス

【サービス対象者・ニーズ】

サービス提供元：

ISP　[送受信相手が適切な所であるか確認したい]

サービス提供先：

医療機関　[医療情報を安全に送受信したい、大量の情報を高速に送りたい]

【アプリケーションの機能・実現方式】

・送受信先（属性）確認機能

・パケット暗号化確認機能

・医療機関閉域ネット（一種の VPN）構成機能

【認証方式・技術】

・ 医療情報の送信先、受信先について正規の相手かどうかを IP アドレス認証により確認する。また、送信先を特定の IP アドレスブロック域が振られた相手のみに限定し、不必要な発信を回避する。

（3）　家庭医療機器のネット対応

【概要】

高齢化社会を迎える中、家庭内で疾病を予防し、また病状を早期発見することは今後益々求められていくことになろう。近年では体温計、血圧計などの家庭用医療機器もディジタル化、高機能化が進んでおり、本人や家族が計測した場合でも信頼あるデータ値が得られるようになっている。

今後、これらの家庭内医療機器においても通信機能が標準装備されるようになった場合、地域の医療機関と連携して、複数の医療機器を定期的な自己計測することにより、リアルタイムで自分の健康度合いのチェックや医療機関からの助言が受けられるサービスが可能となる。また、老人や健康不安を持つ人には、一定の計測を越えたり、一定期間の入力がない、等の条件により自動的に医療センターに通知が行き、生存確保や急病対処の連絡を行なうようなサービスも考えられる。

このようなサービスにおいては、送信データが確かにその患者のものであり、指定された機器が正常な動作状態の下で送ったことを確認する仕組みが必要になる。

IP アドレス認証と特定ブロック域の割り当てはこのような場面においても有効な方法であると思われる。

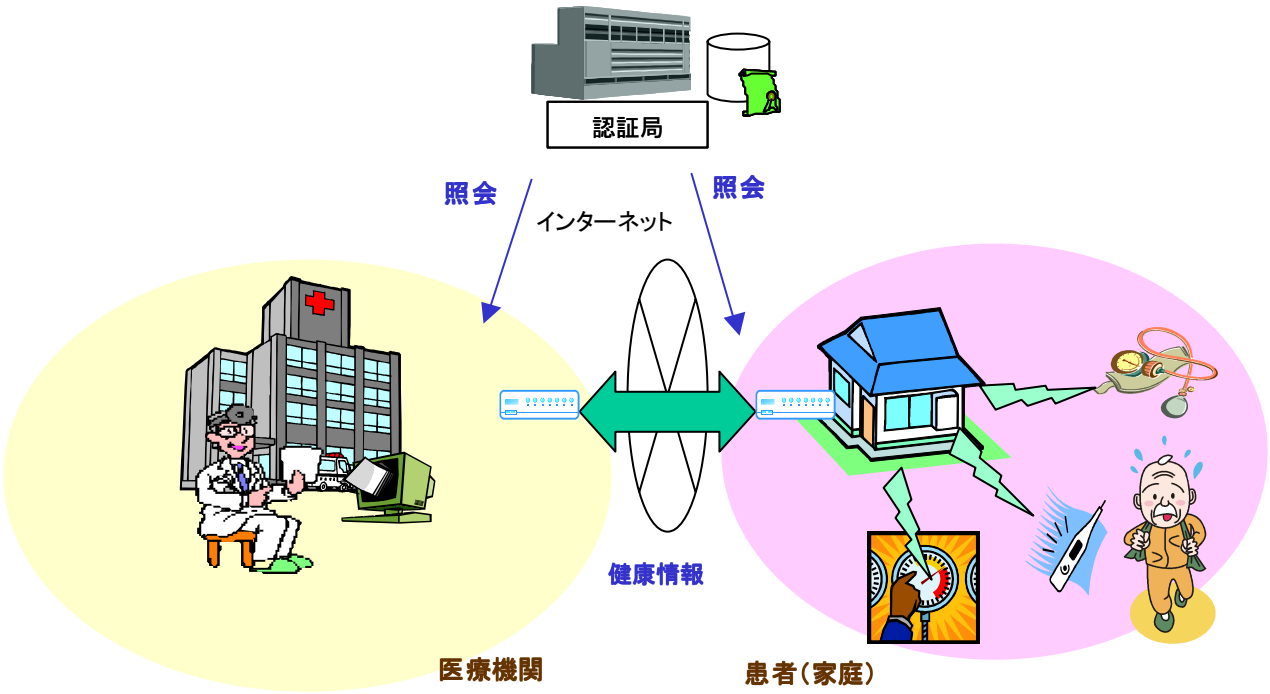


図 7-22　家庭用医療機器のネット対応イメージ

【サービス対象者・ニーズ】

サービス提供元：

医療機関、家庭医療機器メーカー[患者の最新の健康状態を総合的に知りたい]

サービス提供先：

住民（高齢者、病人など）　[健康状態を知りたい、担当医に現状を通知したい]

【アプリケーションの機能・実現方式】

・家庭内医療機器情報登録機能（初期および正常状態の登録）

・計測データ送信機能

・計測データ受信（相手先確認）機能

【認証方式・技術】

・ 計測データの送信先、受信先について正規の相手かどうかを IP アドレス認証により確認する。また、送信先を特定の IP アドレスブロック域が振られた相手のみに限定し、不必要な発信を回避する。

7.2.3.7.　その他

（1）　ライフスタイル集計サービス

【概要】

一般者の行動や購買活動を調べる方法として様々なマーケティング手法があるが、これは携帯型の情報通信機器を利用して行なうサービスである。携帯型の情報通信機器を街中に設置されたセンサーで認証し、特定のセグメント（年代や性別）の人の行動を集計、分析するものである。収集の段階では、IP アドレス情報自体は渡されず　IP アドレス認証用として付随登録されている年代や性別などのみがカウントされる。参加者は、情報通信機器だけを持ち歩くだけで、報酬（調査謝礼）を得ることができる。

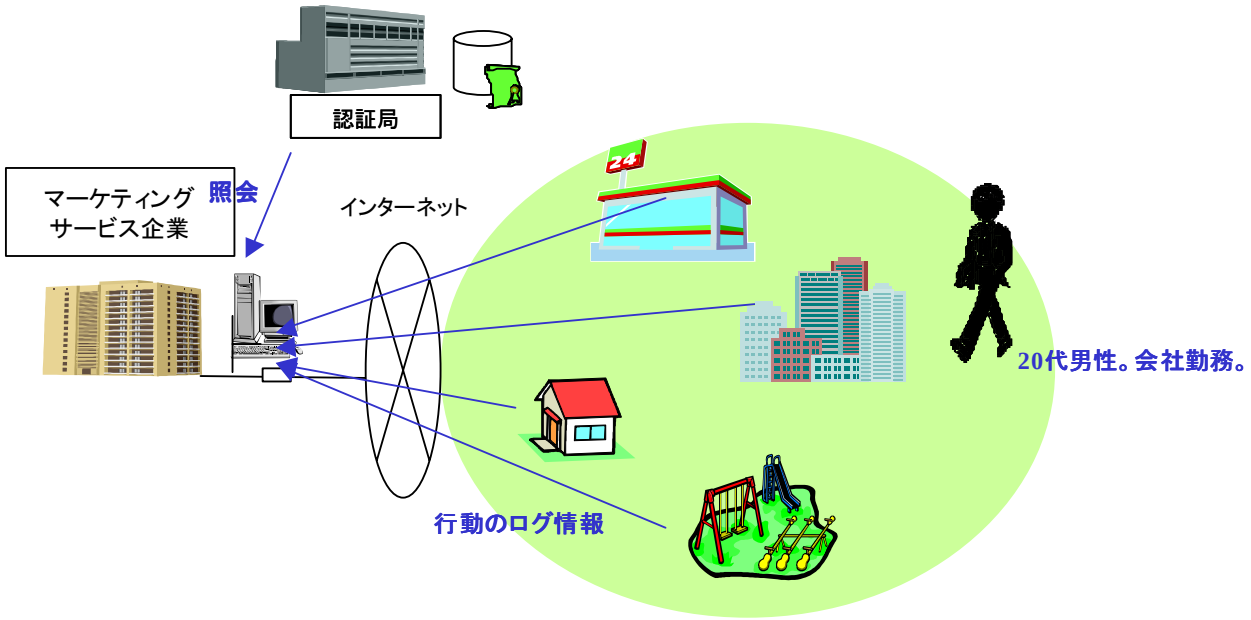


図 7-23　ライフスタイル集計サービス

【サービス対象者・ニーズ】

サービス提供元：

マーケティング会社、大手メーカー　[消費者行動をより正確に知りたい]

サービス提供先：

一般消費者　[労せず報酬を得たい]

【アプリケーションの機能・実現方式】

・携帯機器情報登録機能（初期および正常状態の登録）

・受信 IP 機器の利用者情報確認機能

・セグメント別行動情報集計・分析機能

【認証方式・技術】

・　センサーにより認識された IP アドレスをもとにその機器の利用者のマーケティングに関係するセグメント情報（年代や性別等）を確認する。

（2）　特定移動体向け情報配信サービス

IP アドレスの認証や IP アドレスブロックから移動体が判別できるようになることで次のようなサービスが実施できる可能性がある。

・安全情報についての車体間およびパトロールセンターへの通信（前後方の運転手の異常予測）
・別の移動体への自分の位置の通知
（電車が近づいていることを車側が事前に確認できるなど）

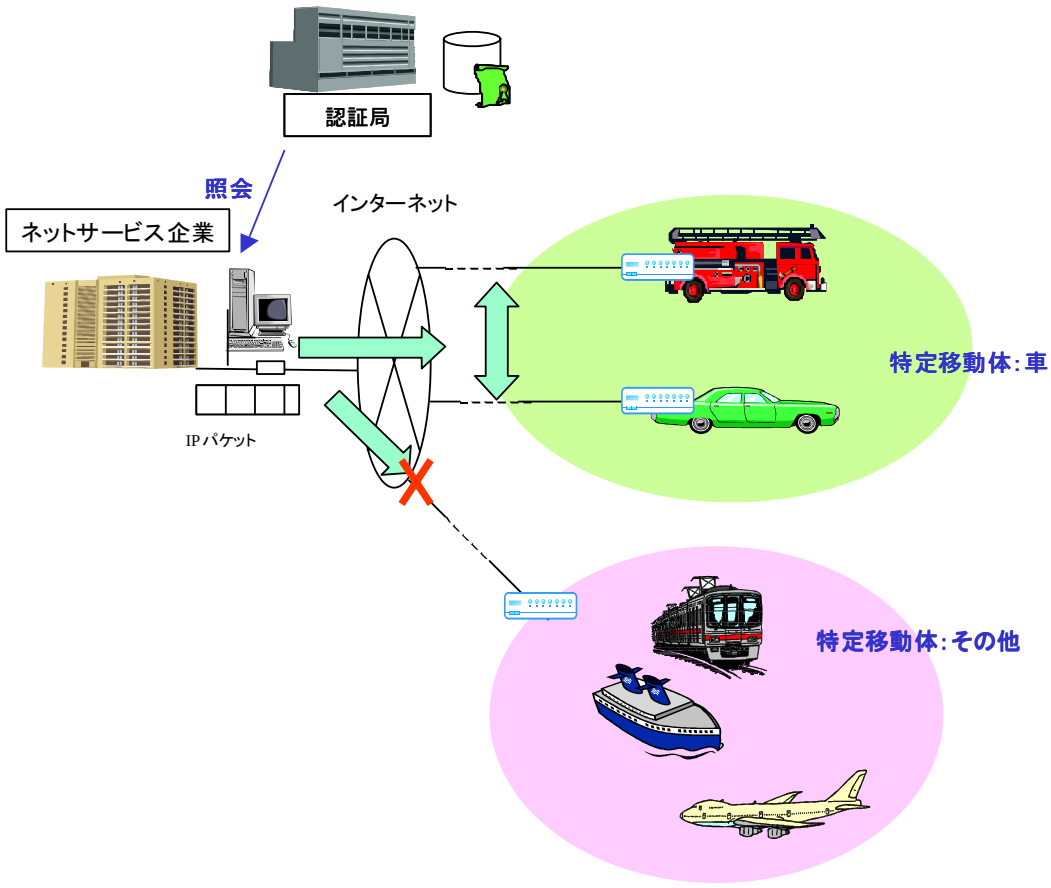


図 7-24　特定移動体向け情報配信サービス

【サービス対象者・ニーズ】

サービス提供元：

交通センター、警察　[最新の交通情報を提供し、安全性を高めたい]

サービス提供先：

各種移動体　[安全に通行したい、事故を防ぎたい]

【アプリケーションの機能・実現方式】

・通信相手（送信、受信）選別（認証）機能

・情報送信機能

【認証方式・技術】

・ IP アドレスブロックや自分の場所の情報をもとに、周辺の同じ移動体からの情報や地域特有の情報を認識する。

7.3.　まとめ

本章では、IP アドレスを認証することにより新たに展開できる可能がある情報通信サービスやビジネスのアイデアを探り、既存通信事業補完型、高セキュア通信機能型、新通信インフラ提案型に分類し、整理を行なった。本章に挙げたようなアイデアを実際に実現するには、技術的な問題から社会法制度の改正まで様々な障壁があるが、いずれも公共性の高いサービスであり、いくつかのアイデアについては実現に向けて今後詳細検討する価値があるものと思われる。

アイデアを検討する中で、現在の業務の中のセキュリティ面が弱い部分を補完するようなビジネス、サービスの展開はもちろんのこと、IP アドレス自体に特定の用途を持たせることができれば、従来では技術上やコスト上で実現が難しかったビジネス、サービスが短期、低コストで実現できる可能性がある。

実際に認証局を設立して、サービスを具現化する際には本章で挙げたようなビジネス、サービスをいずれ行なえるようにすることも視野に入れ、各種技術仕様を検討していくとよいであろう。