



特集

地方公共団体組織認証基盤（LGPKI）が発行する証明書について

地方公共団体組織認証基盤（以下「LGPKI」という。）では、職責証明書、利用者証明書、Webサーバ証明書、メール用証明書及びコードサイニング証明書の5種類の証明書を発行しています。

今月号では、LGPKIが発行する証明書について紹介します。

1 LGPKIが発行する証明書の種類について

LGPKIは、地方公共団体及びLGMAN-ASPサービス提供者^{※1}に対して証明書を発行します。発行する証明書は、主に次の目的で利用します（図-1）。

(1) 職責証明書

他の地方公共団体や、住民・企業等向けに発信する公文書への電子署名や、電子行政サービスを利用して地方公共団体が国などに提出する申請書への電子署名などに利用します。地方公共団体の職責者による電子署名が付与されていることから、職責者による公文書であることが確認できます。また、内容が改ざんされていないことが保証されます。

(2) 利用者証明書

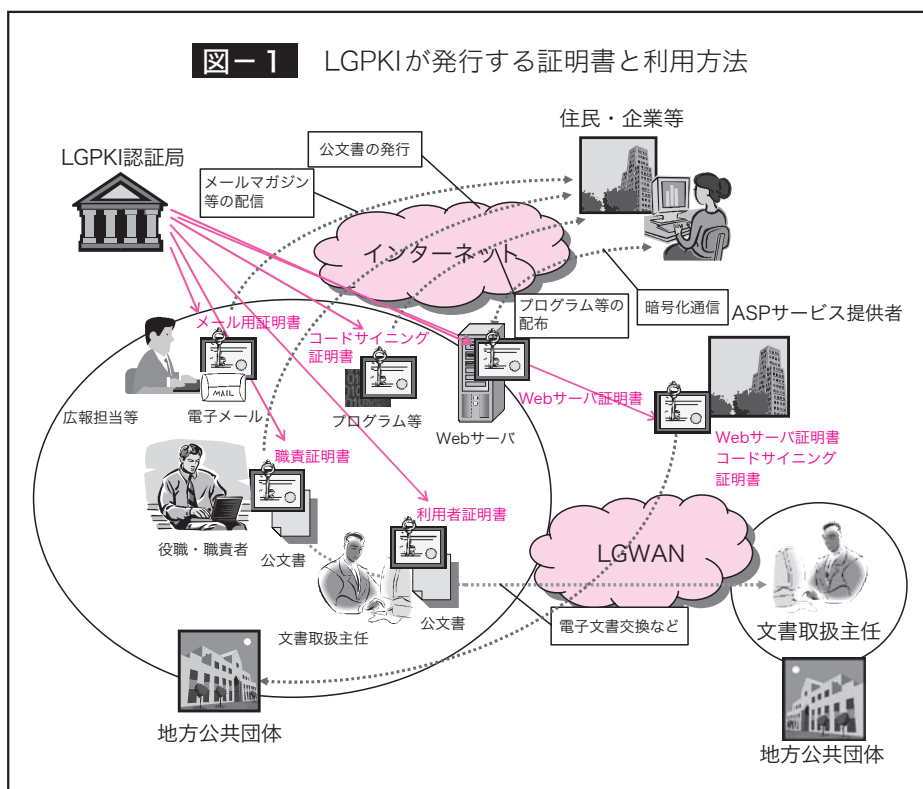
各種アプリケーションシステムを使用するための利用者認証や、電子署名及び暗号化通信として利用します。利用者認証によって、システムを利用する権限を持たない者からの不正操作を防ぐことがで

きます。また、電子署名により発信者が作成したメッセージであることと内容が改ざんされていないことが保証され、さらには、暗号化により送り先の相手のみのメッセージ閲覧が可能になります。

(3) Webサーバ証明書

地方公共団体のWebサーバと通信する住民・企業等、主にインターネット経由による各種電子行政サービスなどで通信される情報が読み取られないよう暗号化し、安全な通信を行うために利用します。

図-1 LGPKIが発行する証明書と使用方法



※1 C-7-2 総合行政ネットワーク ASP基本綱領に定めるLGMANにASPサービスを提供する日本国内の組織等。

また、Webサーバ証明書を搭載することで、Webサイトにアクセスした場合、当該Webサイトは地方公共団体が提供していることを保証することができます。

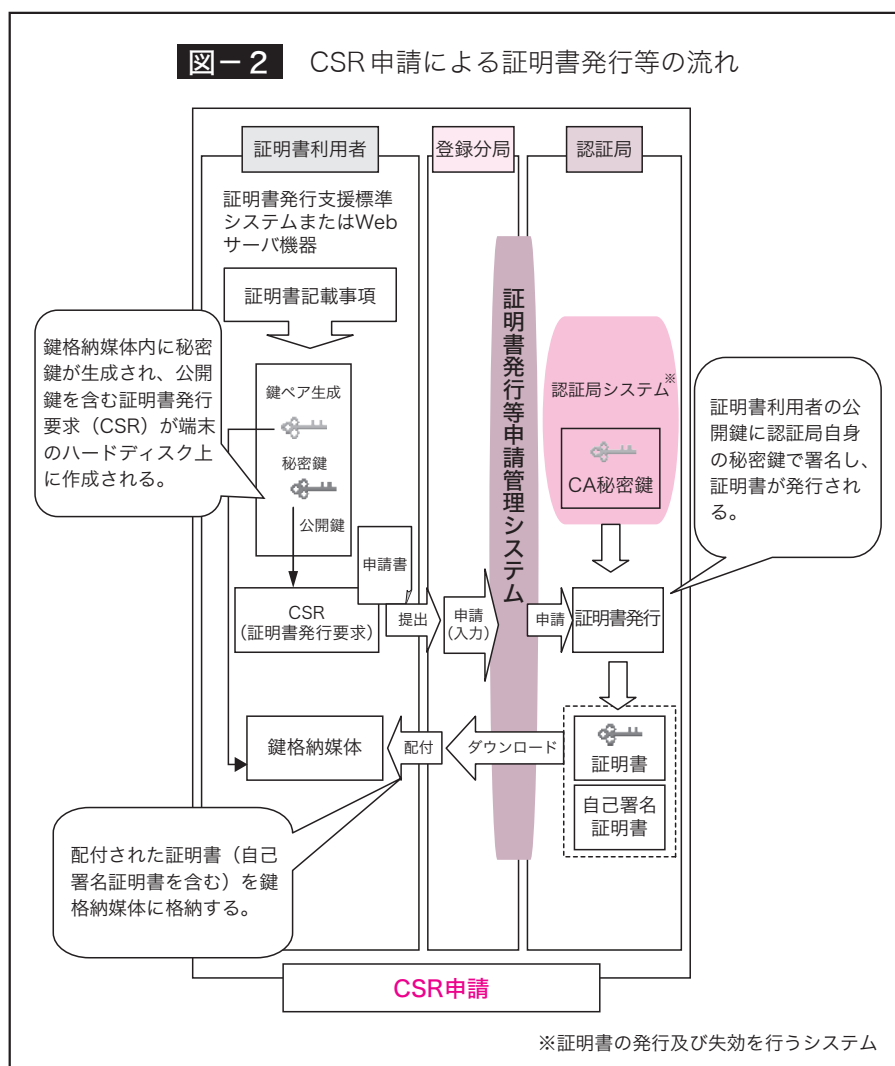
(4) メール用証明書

電子メールへの電子署名に利用し、住民・企業等向けに発信するメールマガジンなどで発信者が地方公共団体であることを保証するために利用します。電子署名により地方公共団体のメール発信者が作成したメールであること並びにメールの内容が改ざんされていないことを保証します。

(5) コードサイン証明書

地方公共団体が提供するプログラム等ソフトウェアへの電子署名に利用します。各種電子行政サービス用のプログラムなどを住民・企業等に配付する場合に電子署名を行い、提供者が地方公共団体であることを保証します。

図-2 CSR申請による証明書発行等の流れ



2 証明書の発行申請について

証明書の利用を希望する地方公共団体の職員（以下「証明書利用者」という。）は、CSR申請^{※2}または通常申請^{※3}のいずれかの方法により、証明書の発行申請を行います。申請方法は平成20年10月以降、CSR申請のみとなるため、本特集では、CSR申請について説明します。

CSRとは、証明書利用者自身が鍵ペアを生成し、

公開鍵や証明書記載事項などを含むデータに基づき、証明書発行を認証局に対して要求するためのデータです。CSR申請では、証明書利用者は証明書発行申請書及びCSRを提出し、登録分局^{※4}に証明書発行申請を行います。次項の2（1）のとおり必要な環境を整備し、2（2）から2（3）までの手順に従い登録分局に申請を行います。登録分局における審査が完了した後、2（4）のとおりLGWANポータルサイト上にある「証明書発行等申請管理システム（CIRS）」を用いてオンラインで申請を行います（図-2）。

※2 Certificate Signing Requestの略。証明書利用者自身が鍵格納媒体に鍵ペア（公開鍵暗号方式における公開鍵とそれに対応する秘密鍵の対）を生成する申請方法。

※3 鍵格納媒体ごと郵送し、認証局（LGWAN運営主体）で鍵ペアを生成する申請方法。

※4 認証局から証明書の発行等申請の受付及び審査業務の一部を委任され、地方公共団体内に整備する体制。

(1) 証明書利用者側で必要な環境について

証明書利用者は登録分局への証明書発行申請にあたって、証明書発行申請書及びCSRを準備します。CSRを作成するためには、証明書を格納する鍵格納媒体（コードサイニング証明書のみUSBトークンも利用可能）が必要であり、作成は「証明書発行支援標準システム」を使用^{※5}して行います。

また、鍵格納媒体にICカードを使用する場合は、通常申請に必要な機器等に追加して、「LGWAN用ICカードフォーマット」及び「LGWAN用ICカードドライバソフトウェア（バージョンB00以上）」が必要です。

ア 「LGWAN用ICカードフォーマット」について

「LGWAN用ICカードフォーマット（以下「フォーマット」という。）」とは、ICカード内のデータを消去し（以下「フォーマット処理」という。）、CSRの作成を可能にするソフトウェアです。なお、未使用のICカードについても、CSRを作成するためにはフォーマットを使ってフォーマット処理を行う必要があります。フォーマットの調達にあたっては、「F-1-1-3 総合行政ネットワーク接続仕様書（資料編）」^{※6}に記載された事業者の製品のみを調達の対象とします。

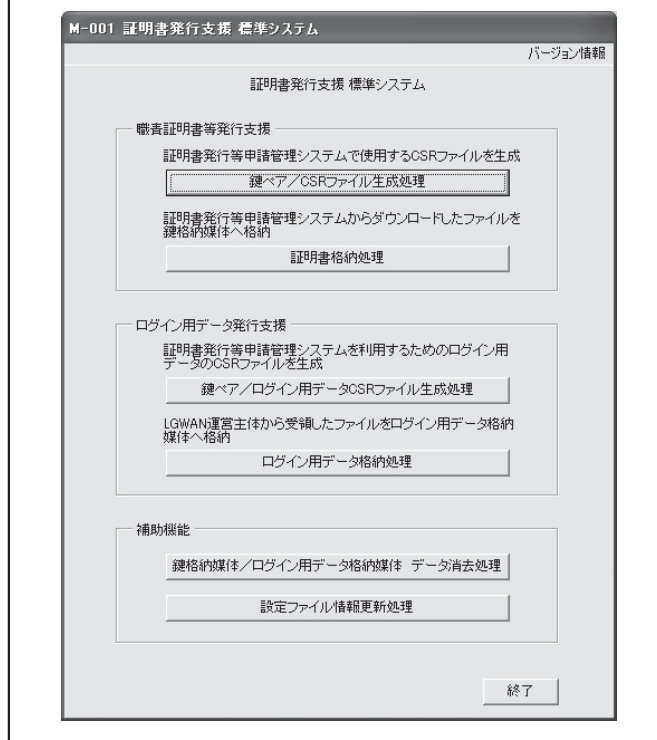
イ 「LGWAN用ICカードドライバソフトウェア」について

「LGWAN用ICカードドライバソフトウェア」とは、ICカードを動作させるために端末にインストールする必要があるドライバソフトウェアです。CSRを作成するためには、バージョンが「B00」以上のソフトウェアが必要です。なお、フォーマットと同様の方法で調達します。

ウ 「証明書発行支援標準システム」について

職責証明書、利用者証明書、メール用証明書及びコードサイニング証明書のCSR作成や、発行

図-3 証明書発行支援標準システム画面（例）



した証明書の鍵格納媒体への格納などに使用するシステムです。

「証明書発行支援標準システム」(図-3)は、LGWANポータルサイト^{※7}からダウンロードします。

エ その他

登録分局へ作成したCSRを提出する際、CSRを格納するフロッピーディスクが必要になります。また、登録分局から配付される証明書の格納時にも使用します。

(2) CSRの作成

証明書利用者は、主に次の流れで環境を整備し、CSRの作成を行います。

ア 証明書発行支援標準システムを端末にインストール

イ 格納媒体がICカードの場合

※5 Webサーバ証明書を除く（Webサーバ証明書の場合は、Webサーバ等機器の機能でCSRを作成します）。

※6 F-1-1-3 総合行政ネットワーク接続仕様書（資料編）(<http://center.lgwan.jp/library/index.html#F-1-1-3>)

※7 K-3-3 証明書発行支援標準システムプログラム及びインストール手順書 (<http://center.lgwan.jp/library/index.html#K-3-3>)

①ソフトウェアのインストール(フォーマット、
LGWAN用ICカードドライバソフトウェア
のバージョンアップ)

②フォーマットでICカードをフォーマット処
理

ウ 証明書発行支援標準システムを使用して鍵ペ
ア及びCSRを作成

(3) 登録分局への提出

作成したCSRは、フロッピーディスク等に格納し、

証明書発行申請書とあわせて登録分局に提出します。

(4) 認証局への申請及び証明書の配付

登録分局は、審査等の必要な手続きを行い、問
題がない場合には、「証明書発行等申請管理システ
ム(CIRS)」を用いて、認証局(LGWAN運営主体)
に発行申請を行います。

その後、認証局から証明書が発行されたら、登録
分局は、証明書利用者に対して証明書を格納したフ
ロッピーディスク等を配付します(図-4)。

図-4 証明書発行支援標準システムを利用した申請から配付までの手順

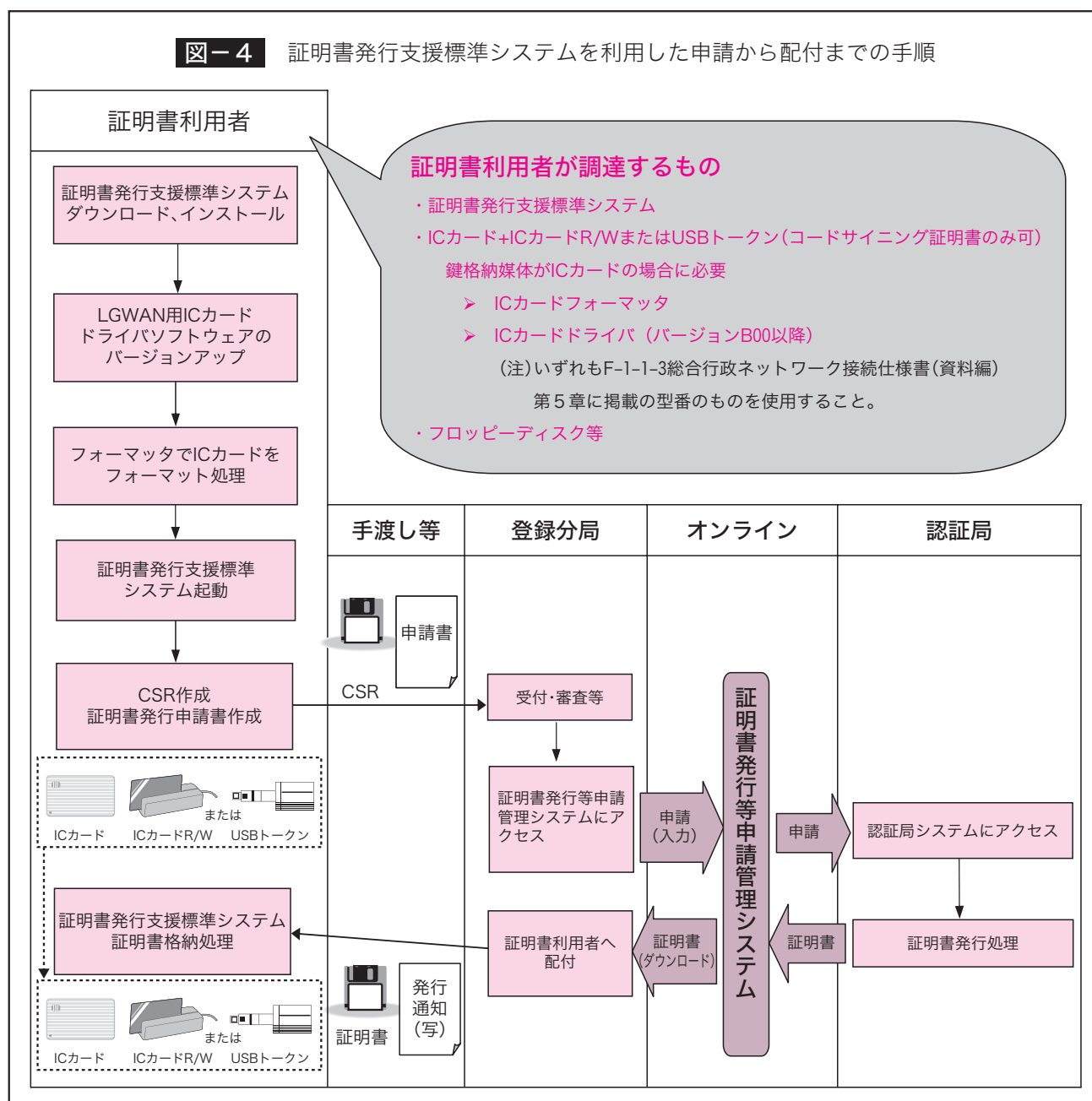
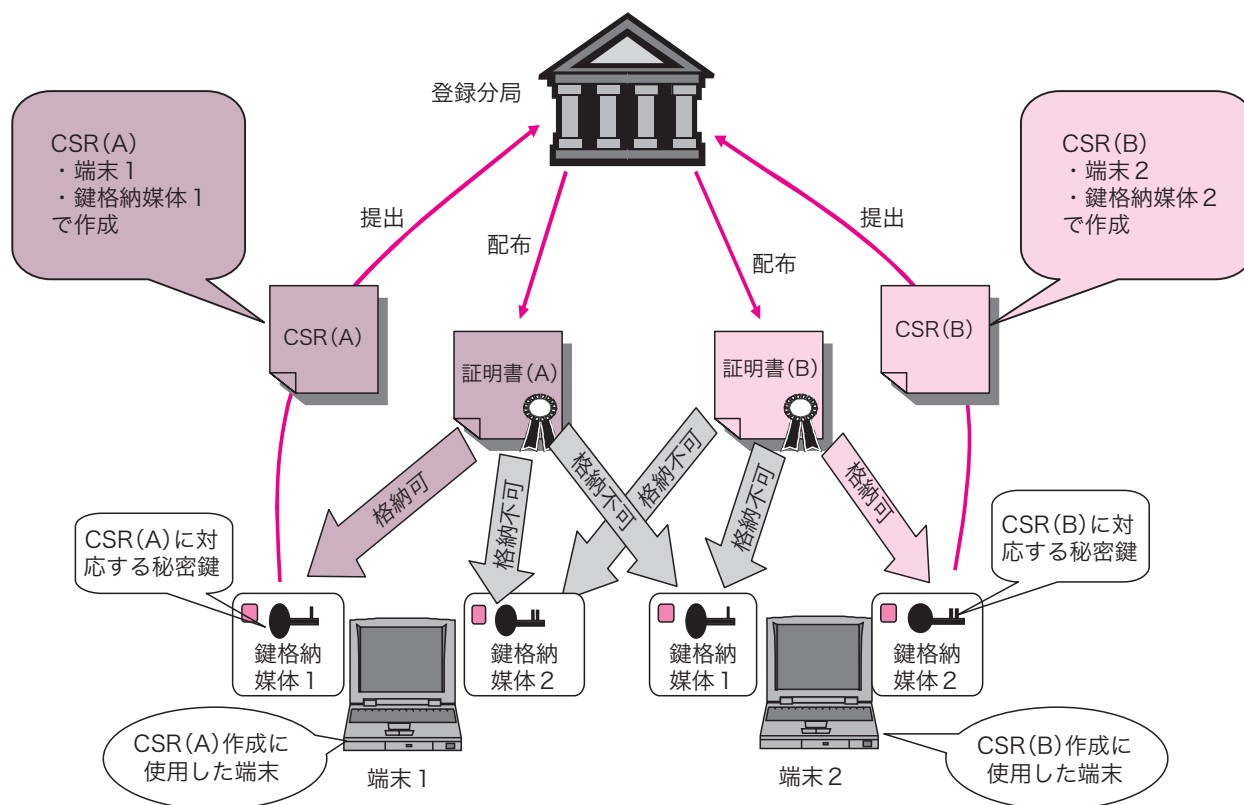


図-5 証明書格納処理の組み合わせについて

CSRを作成した鍵格納媒体・端末にしか、その証明書は格納できない



○端末1を使い鍵格納媒体1に証明書(A)の格納ができる。

×端末2では鍵格納媒体1に証明書(A)の格納ができない。

また、CSR作成時の鍵格納媒体に対応する証明書以外を格納することはできない。

(鍵格納媒体1に証明書(B)を格納、鍵格納媒体2に証明書(A)を格納することはできない。)

3 証明書の格納について

登録分局から証明書が配付されたら、証明書利用者は、証明書発行支援標準システムを使い、証明書を鍵格納媒体に格納する処理を行います。

証明書を鍵格納媒体に格納する際は、「CSRを作成した鍵格納媒体」及び「CSR作成時に使用した端末」を用いて証明書を格納する必要があります。CSR作成時に使用していない端末や、CSRと証明書の組み合わせが一致しない場合などは、証明書を格納することができませんので、組み合わせを間違えないよう注意してください(図-5)。

4 今後について

証明書発行申請の方法については、通常申請を終了し、平成20年10月以降はすべて、CSR申請に統一する計画となっています。そのため、現在、通常申請のみを行っている場合は、今後の証明書発行申請に向けて本特集の2(1)(2)で記述した環境の整備を行っていただきますようお願いします。

また、「証明書発行支援標準システム」については、CSR申請への統一化に伴い、複数の鍵ペア・CSRの連続生成など、利便性向上のための機能改修を今年度事業で行っているところです。

LGPKI 登録分局設置状況 (平成20年 8 月 6 日現在)

	都道府県	市区町村				都道府県	市区町村		
		登録分局 設置数 (A)	団体数 (B)	設置率 (A/B)			登録分局 設置数 (A)	団体数 (B)	設置率 (A/B)
1	北海道	154	180	85.6	25	滋賀県	21	26	80.8
2	青森県	39	40	97.5	26	京都府	22	26	84.6
3	岩手県	35	35	100.0	27	大阪府	39	43	90.7
4	宮城県	27	36	75.0	28	兵庫県	41	41	100.0
5	秋田県	23	25	92.0	29	奈良県	39	39	100.0
6	山形県	35	35	100.0	30	和歌山県	27	30	90.0
7	福島県	49	59	83.1	31	鳥取県	15	19	78.9
8	茨城県	44	44	100.0	32	島根県	17	21	81.0
9	栃木県	31	31	100.0	33	岡山県	27	27	100.0
10	群馬県	38	38	100.0	34	広島県	19	23	82.6
11	埼玉県	70	70	100.0	35	山口県	20	20	100.0
12	千葉県	56	56	100.0	36	徳島県	24	24	100.0
13	東京都	59	62	95.2	37	香川県	16	17	94.1
14	神奈川県	33	33	100.0	38	愛媛県	18	20	90.0
15	新潟県	29	31	93.5	39	高知県	34	34	100.0
16	富山県	15	15	100.0	40	福岡県	65	66	98.5
17	石川県	19	19	100.0	41	佐賀県	20	20	100.0
18	福井県	15	17	88.2	42	長崎県	23	23	100.0
19	山梨県	25	28	89.3	43	熊本県	40	48	83.3
20	長野県	76	81	93.8	44	大分県	18	18	100.0
21	岐阜県	40	42	95.2	45	宮崎県	25	30	83.3
22	静岡県	37	41	90.2	46	鹿児島県	42	46	91.3
23	愛知県	61	61	100.0	47	沖縄県	41	41	100.0
24	三重県	22	29	75.9	合計		1,685	1,810	93.1

LGWAN-ASP サービス接続／登録状況 (平成20年 8 月 6 日現在)

< サービス提供者の分類 >

・アプリケーション及びコンテンツ	登録	167件	・ホスティング	接続	94件
・通信	登録	152件	・ファシリティ	登録	176件

※接続／登録済のLGWAN-ASPサービス提供者のリストは、下記URLに掲載しております。

<http://www.lasdec.nippon-net.ne.jp/cms/15,0,41.html>