



---

## オーストラリア政府電子認証枠組

### 公開草案

本文書は、オーストラリア政府の電子認証枠組の公開草案です。オーストラリア政府情報管理局は、この草案に対するご意見を2004年5月21日まで募集いたします。

ご意見送付先:

[agaf@agimo.gov.au](mailto:agaf@agimo.gov.au), 又は電話 02 6271 1317

## はじめに

企業と政府間のオンライン取引は、ますます普及している。オーストラリアの企業は様々な分野で政府機関と交渉する機会が多い。これは、一般的な問合せ、各種申請や支払、入札、政府委託業務と多岐にわたる。

企業は、インターネットや電話ベースのサービスなど、電子環境、デジタル環境を介して政府機関と交渉することが多くなっている。これは、企業にとっても政府にとってもメリットがある。例えば、24時間サービス、サービス待ち時間の短縮、政府との間のペーパーレス化、手続の合理化などがそれである。企業は、用紙の記入、企業支援プログラムの申込、取引の請負、納税申告など、政府に対してなすべき多くの事務処理を今ではオンラインで行なうことができる。

企業はオンライン取引の便益を享受している。

電子商取引やオンライン取引の量は急速に増えている。オーストラリア統計局の最近の統計によると、2002-03年に、オーストラリアの485,000の企業（全企業の71%）がインターネットを使用しているという。企業のインターネット収益は、243億ドルで、前年度の113億ドルから急増している。<sup>1</sup> インターネットを介して受注した企業数は前年度に比べ倍増した。2002-03年に、

- 71%の企業がインターネットを使ってオンラインで政府サービスにアクセスした。
- 21%の企業がインターネットを使ってオンラインで納税申告書を提出した。
- 28%の企業がインターネットを使ってオンラインで支払をした。
- 42%の企業がインターネットを使って租税関連の情報やサービスを求めた。
- 35%の企業がインターネットを使って規制に関する情報を求めた。及び
- 26%の企業がインターネットを使って雇用に関する情報を求めた。<sup>2</sup>

---

<sup>1</sup> オーストラリア統計局、*Business Use of Information Technology 2002-03*, 8129.0、2004年3月17日、p.3

<sup>2</sup> 同書、p.12

2003年4月に発行された「電子政府の便益研究」<sup>3</sup>では電子政府サービスのユーザとしての企業及び個人の意識調査をしている。政府とのオンラインでの取引により、企業がコスト面でも意思決定面でも改善したと認識していることが分かった。

ただし、企業も政府もこれらの取引が信頼しうるといふ保証を必要とする。

オンラインで取引する場合、互いの身元や表明の正当性が完全に保証されることが必要となる場面がある。この表明は、一連の属性（身元、職業的資格、又は人が特定の取引を行なう権限を与えられていること、など）に関連することが多い。資金や機密情報が関与する場合、保証の必要性は特に高くなる。身元やその他の属性の場合、表明の正当性の確立過程は、**企業認証**の重要な要素である。

大まかに言って、企業認証は、下記のうちの両方又はいずれか一方に依存する。

- パスワードやPIN（個人識別番号）のような企業が知っているもの
- スマートカードやトークンのような企業が有するもの

各関係者の請求を認証しないリスクは高いことが多い。

ユーザの正しい認証が行なわれない場合、資金の移転、モノの未承認発注、データの改ざんなどの事態が発生する可能性がある。認証は、信頼を支え、電子商取引における信頼性を築き、電子商取引の重要な要素となる。

デジタル取引、電話ベースの取引が複雑になるにつれ、「なりすまし」（偽ウェブサイト）や身分詐称の影響が深刻になり、企業や政府へのリスクが高まり、そのリスクに曝される機会も増える。政府も企業も、このような取引に関するリスクを評価し、アクセスや認証に関する適切な手順と解決策を実施する必要がある。

---

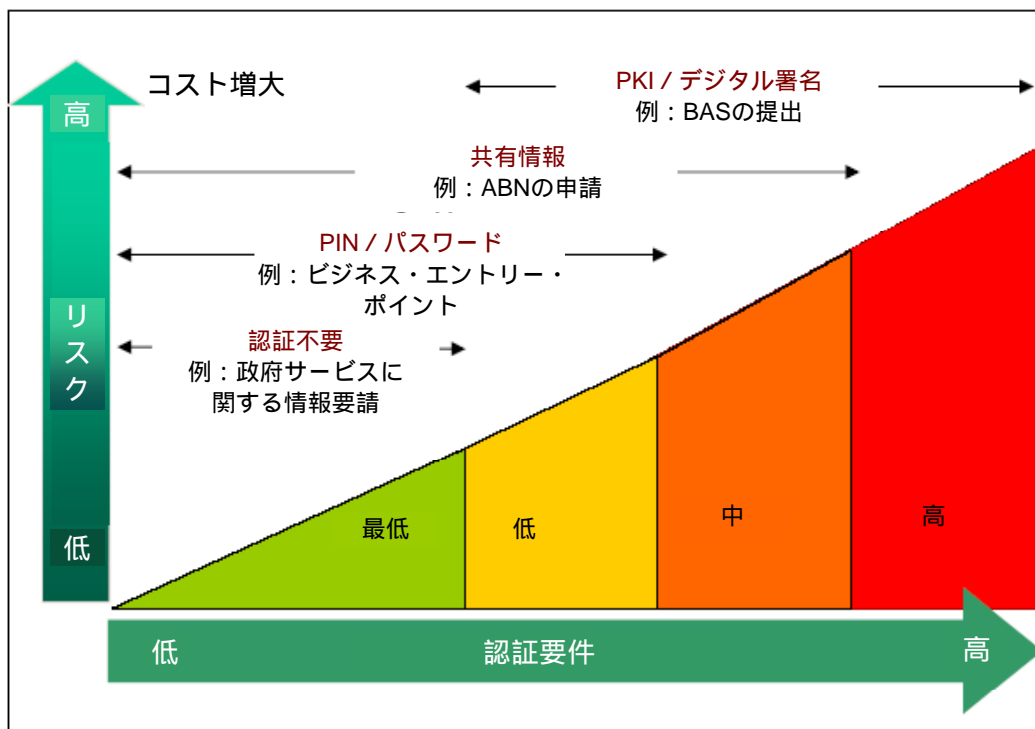
<sup>3</sup> 国立情報経済局、e-Government Benefits Study、2003年4月、p.8

AGAFは、政府  
認証に一貫し  
た方法を提供  
する。

政府は、認証について政府横断的な方法を定めるオーストラリア政府認証枠組 (AGAF) の実施に向けて取り組んでいる。オーストラリア政府は、リスクの関与度により、様々なタイプの取引に対し、様々な認証技術が必要だと認識している。オーストラリア政府機関が認証方法について意思決定する場合に、必ず一貫した方法が適用されるようにするのが、AGAFの趣旨である。AGAFは、オーストラリア政府機関が取引の際のリスクレベルに対応した認証手段を実施することを保証するものである。

図1 企業リスク及び認証要件は、企業にとっても政府にとっても、取引に潜むリスクが高くなるにつれて、認証レベルをいかに高めるべきかを示している。

図1: 企業リスク及び認証要件・技術の範囲



## オーストラリア政府認証枠組とは何か?

認証手段の選択に一貫した方法を採用することにより、オーストラリア政府は、

- 政府のオンラインサービスを使用する企業の経験や期待の一貫性を提供する。
- 有用で、安全で、プライバシーの侵害がない認証手段により支えられたオンラインサービスを提供することにより企業及び政府の中で信頼を築く。
- 一貫した、監査可能なリスク管理が行政全体の認証に適用されることを保証する。
- 企業がオンラインで安全に政府と取引し、政府が企業と取引するための単純で低コストの選択肢を提供する。

AGAFは、一貫性、信頼性、及びその費用効果を提供する。

AGAFは、国のIDシステムや個人又は商用情報・属性の中央レジストリを提案するものではない。

AGAFは、取引のリスクに対応する4レベルのリスクに関し、認証方法を提案する。各レベルの詳細については、別表Aを参照のこと。

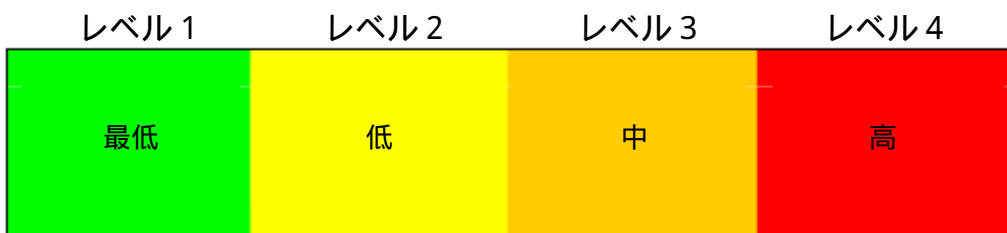
図2: オーストラリア政府のリスク保証レベル

レベル 1	レベル 2	レベル 3	レベル 4
最低リスク	低リスク	中リスク	高リスク
表明の信頼度に対する要件なし	表明に幾分かの信頼度	表明に中位の信頼度	表明に高い信頼度

図3 は、様々な種類のリスクレベル、認証カテゴリー、認証方法を示す。使用する認証手段の種類を決定する場合に政府機関が履行する3つのステップを概略する。

### 図3: AGAF

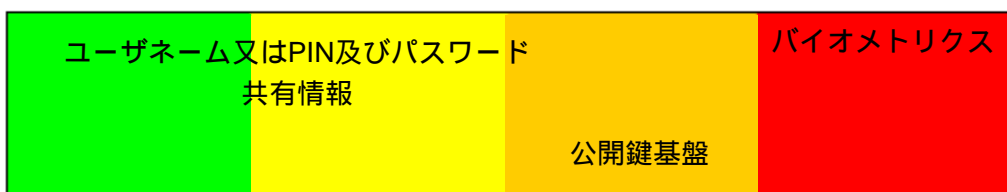
#### ステップ1：取引のリスク



#### ステップ2：認証の対象は何か？



#### ステップ3：認証手段



取引に潜むリスクレベルを評価した後、政府機関は、取引における信頼性を保証するために何を認証すべきかを検討する。これが決まると、適切な認証手段が選択されよう。

図3は、低リスク取引には、ユーザネームやパスワードなどの低レベル認証を使用することを示す。高機密又は高リスクの取引は、公開鍵基盤などの高レベル認証手段を要する。例えば、

- 政府プログラムに関する情報を求めるオンラインでの単純な問合せによって成立するリスクは最低レベルなので、認証は要さない。
- モノやサービスに対するオンラインでの支払には、通常、企業の属性（有効なクレジットカード等）が認証されることが必要となる。買主又は売主の身元についての情報が虚偽である場合、虚偽情報の受領者にとって中程度のリスクが成立する。従って、ユーザネームやパスワードなど、中位の保証を要求する適切な認証方法が適用される。
- 租税局に対し、四半期営業損益計算書を提出する。この場合、人が事業体を代表して取引する権限を与えられているという保証の必要性は、中程度から高程度である。財務データが第三者に傍受又は改ざんされれば、相当の損害が生じうるというリスクがある。公開鍵基盤のような高保証認証法が使用される。

図3に示すように、認証技術は、全リスクレベルに対応できる。PINやパスワード並びに公開鍵基盤は、全リスクレベルに対応する認証を提供する。

ただし、企業は、自身のシステムのセキュリティ全般は、適切な認証方法、適切で最新のウィルス保護ソフトウェアやファイアウォールを有するか否かに掛かっていることを認識すべきである。

## 現状

現在、オンラインサービスのユーザの大半は、認証にユーザネーム/パスワードの方法を採用している。環境が複雑になるに従い、リスクに曝される度合は誰にとっても高くなる。従って、オーストラリア政府は、様々なリスクレベルに対応しうる多数の認証法が使用できるオンライン認証の方法を実施する必要がある。

認証手段を選択する場合、企業に対する影響が考慮される。

AGAFは、リスクが低い場合、企業が時間のかかる認証手続の制約を受けないことを確保する。

AGAFは、政府機関が特定の認証技術の採用を決定する助けとなる指針を提供する。また、その決定に至った経緯を企業側が理解する助けにもなる。政府機関がある技術に決めるときに考慮した事項には次の事項が含まれる。

- 表明が、実際は虚偽であるのに、認証されて受け入れられる場合、発生する潜在的危害
- 技術の使用に影響を及ぼす法的、公共政策的問題（プライバシーを含む）
- 技術が企業側に広く理解され、利用されているか否か
- 必要な認証手順に参加する企業の意欲
- 認証技術を支持する基盤、サービス及び解決策の可用性と信頼性
- 技術が企業クライアント及びオーストラリア政府に与える財政的影響並びにこれが受け入れられるか否か
- 技術のマイナスの影響は、利点によって正当化されうるか否か

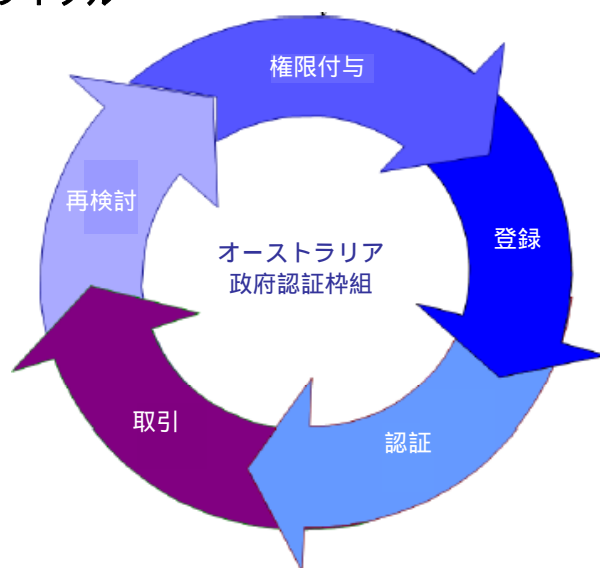
別表B は、現在、政府で行われている種類のオンライン取引及び使用されている認証技術を概略する。

## 企業が政府との交渉でとるべきステップは何か?

認証が必要とされる環境で取引を行なうために、企業は、任命された担当者が会社を代表して政府と取引できるように、アクセス及び認定手順を確立しなければならない。特に、企業は下記のことを履行しなければならない。

1. **権限付与**—企業は単数又は複数の担当者を選任し、会社を代表してオンラインで取引し、特定の政府アプリケーションにアクセスする権限を彼らに与える。
2. **登録**—企業は、担当者を政府機関に登録し、彼らが適切な認証手順を使って取引できるようにする。
3. **認証**—企業代表者の取引する権利は、PINやパスワードなどの認証手段を使って確認される。政府機関は、代表者が特定のアプリケーションにアクセスする権限を有していることを確認することができる。
4. **取引**—企業の代表者は、政府とオンラインで取引を進める。
5. **再検討**—企業は、通常の業務に即して、権限付与された担当者を再検討し、その担当者が企業から権限付与された者としての職務を続けるべきであることを確認する。

図4: 企業認証サイクル



企業の登録や認証に係る手順は、各政府機関の要件によって異なる。一般に、企業に課せられる要件は、リスクが高くなるに従い、厳しくなる。これは、企業と政府の両方にとって防御策となる。管理上の問題として、企業は、企業の委任システムの一環として、政府のオンラインアプリケーションへの従業員のアクセス権の記録簿を維持しなければならない。

### 認証手段

オーストラリア政府が提供するオンラインサービスには、企業及び政府にとって様々なリスクレベルが絡み、様々な認証手段が必要とされる。企業及び政府が負担する費用を最小限にしながら、最も適した効果的な方法を選択するのが重要な鍵となる。この枠組が提案する様々な種類の認証技術を表1に記載する。

表 1: 認証手段

<p><b>共有情報</b> (チャレンジ/ レスポンス・システムとも称される)</p>	<p>認証を希望する企業ユーザは、取引に係る政府機関による一連の質問に答える。その質問は正当なユーザのみが知る情報に関するものとする。その情報は特定の機関と企業との間でのみ共有される。情報は次の3種類からなる。</p> <ul style="list-style-type: none"> <li>• 記録された固定データ (例、生年月日)</li> <li>• 可変データ (例、最後の支払、受領、請求の日・額)</li> <li>• 具体的に設計された共有秘密情報 (ユーザが機関に一連の質問及び回答を提供した場合)</li> </ul> <p>リスクレベル: 最低から中</p> <p>企業に対する予想される影響: 担当者は、提供した情報について記録をとり、安全に保管する。</p> <p>現行の政府アプリケーション: オーストラリア企業番号用のアプリケーション</p>
<p><b>ユーザネーム/ パスワード</b></p>	<p>認証は、企業ユーザがユーザネームとパスワードを提出することで成立する。このパスワードは一機関にのみ有効である。企業は、他機関で同じパスワードを使用することはできない。</p> <p>リスクレベル: 低から中- ただし、特にそれが共有情報など他の認証手段と併用される場合、更に高リスクアプリケーションで広範囲に使用されるようになっている。</p>

	<p><b>企業に対する予想される影響:</b> 担当者は、ユーザネーム / パスワードの記録を取り、これを安全に保管する。</p> <p><b>現行の政府アプリケーション:</b> 税関申告や支払、ジョブネットワークによる取引、ビジネスビザ、特許出願、ビジネス・エントリー・ポイント、センターリンクによる取引</p>
<p><b>ワンタイムパスワード</b></p>	<p>ワンタイムパスワードは、アプリケーションやサービスにアクセスするたびに独自の異なるパスワードが生成されるシステムである。これにはユーザネームと適合する独自のパスワードを生成するハードウェアデバイスが使用される。企業は、事前登録して、ユーザネーム及びハードウェアデバイスを発行される。ユーザがワンタイムパスワードで保護されたウェブサイトに入ると、デバイス上に表示された直近のパスワードが問われる。機関は、どのパスワードがその時に当該ユーザに有効であるか知っている。同期されたパスワードは、周期的に変わる。</p> <p><b>リスクレベル:</b> 中から高</p> <p><b>企業に対する予想される影響:</b> 担当者は、ハードウェアデバイスを防御して、絶対に紛失や盗難にあわないことを確保しなければならない。コストは高くなる可能性がある。</p> <p><b>現行の政府アプリケーション:</b> 国会議員はワンタイムパスワードを使用する。</p>

<p><b>公開鍵基盤 (PKI)</b></p>	<p>PKI は、ユーザが自らの本人性を認証し、公開鍵暗号法を使用して情報を安全かつ内密に交換することを可能にする技術及び手続である。<sup>4</sup> これを実現するために、秘密鍵、公開鍵、及びデジタル証明書が認証局 (CA) と呼ばれる信任された第三者機関を介して取得される。<sup>5</sup></p> <p>認証局は、公開鍵をデジタル証明書に関連づけ、鍵保有者の身元を保証する。次に、登録局が企業ユーザから適切なレベルの身元証拠を収集する。</p> <p>企業ユーザには、誰でも見ることができる公開鍵、及び送信者の真正性及び送られた情報のデータ完全性を証明するために情報を暗号化する秘密鍵が発行される。企業ユーザは、自らの秘密鍵を使って署名した情報を送信する。受信者は、当該企業の公開鍵でデータを確認することによってメッセージを検証する。メッセージが改ざんされている場合、又は第三者がユーザのふりをしている場合、受信者は、それが暗号化されているときには、読むことも、署名を認証することもできない。これは、PKI採用企業とPKI採用政府機関との間に流れる情報が高度の否認防止性(いずれの当事者も送受信の事実を否認できないことを意味する)を有することを保証する。また、その情報が暗号化されている場合解読できず、不正に改ざんすることもできない。</p> <p>PKI 認証証明物は、多数の政府機関で使用可能であるが、今のところ企業ユーザにとって高コストである。</p> <p>“Gatekeeper”は、政府に提供される又は政府が採用するPKIサービスにおける信頼性を評価するための政府の方策である。認証局及び登録局用のGatekeeper認定手順は、Gatekeeper 認定デジタル証明書の使用に関わる全員に高度の確度と信頼性を提供する。オーストラリア企業番号デジタル署名証明書 (ABN-DSC) は、企業と政府間の使用が意図されている。オンライン取引を実施するためにPKIの利用を意図するオーストラリア政府機関は、Gatekeeper の認可を受けたPKI機能やサービスを使用しなければならない。</p>
---------------------------	--

<sup>4</sup> 「鍵」とは、暗号化及び復号化するための暗号アルゴリズムを使用した文字列である。

<sup>5</sup> Gatekeeperの認可を受けた認証局及び登録局に関する完全なリストについては、[www.agimo.gov.au/infrastructure/gatekeeper/accreditation](http://www.agimo.gov.au/infrastructure/gatekeeper/accreditation) を参照のこと。

	<p><b>リスクレベル:</b> 低から高、ただし、現在、PKIは、高コストであることから、主として高リスク取引に使用されている。</p> <p><b>企業に対する予想される影響:</b> 特別のソフトウェアが必要となろう。鍵及び証明書が活性化する前に従業員は本人性立証をしなければならないだろう。コストはさまざまだろう。</p> <p><b>現行の政府アプリケーション:</b> 防衛、ヘルスケア関係の事業者用システム、医薬品給付システム、ATOビジネス・ポータル、及び営業損益計算書(BAS)の提出その他の企業取引に使用される電子商取引インターフェース</p>
<p><b>バイオメトリクス</b></p>	<p>指紋、手、虹彩スキャン、声紋などがユーザの識別に使用される。生体(バイオメトリック)識別子は、トークンやスマートカードの所有者を示すためのパスワードと同様に使用できる。</p> <p><b>リスクレベル:</b> 中から高</p> <p><b>企業に対する予想される影響:</b> 関係者が身体的属性を快く登録し、このデータセキュリティに信頼を置く必要があるだろう。</p> <p><b>現行の政府アプリケーション:</b> なし。ただし、商用又は休暇でビザなしの訪米を希望するオーストラリア国民は、2004年末までにパスポートに生体識別子を含めなければならない。また、税関及び出入国管理事務所は、“Smartgate”を試験している。これは、国際線乗客及び乗員のための生体顔認識システムである。</p>

### 将来の認証

リスクが高くなれば、認証は更に重要になる。

現在、官民共に、オンラインサービスの大半のユーザは、単純なユーザネームとパスワードにより認証されている。高保証認証プロトコルを必要とする取引は、市場活動の中で僅かな部分しか占めていない。「なりすまし」(偽ウェブサイト)や身分詐称などの行為が深刻な影響をもたらしているところから、これが長期的にどの程度持続可能なものかは、分からない。詐欺的行為が更に広がり、深刻になったり、取引が複雑になると、更に厳格な認証策が必要となろう。政府及び企業は、高まるリスクの評価に基づいて認証レベルを引き上げる準備が必要である。

したがって、政府も企業も、上昇するリスクに対応する準備をしなければならぬ。

個々のリスクの性質によってこの必要を満たすことができる多様な認証手段及び取引がなされる広範な環境がある。政府が企業と取引するために必要な方法を現在考えていること、その認証手段が各取引のリスクレベルに即すことは、関係者全員の利益にかなう。

この方法は、海外の進展とも合致している。

AGAFは、諸政府が企業と政府間の電子的やり取りの普及を促進する相互信頼の構築に向けて取り組んでいる国際的な流れと一致している。この傾向は加速度的に進んでおり、最近の国際合意書には電子取引の国際相互認証についての言及が含まれている。これは、商業文書の迅速な処理や確実性の促進に対する国際的通商要件に対応する。オーストラリアはまだこの案の実施には至っていないが、貿易相手国の中の2カ国（シンガポールと米国）との取引を準備中である。APEC諸国や他の貿易相手国との間でも進展が見られる。

## 結論

AGAFにより、政府は認証要件を簡素に保つことができる。

AGAF案は、将来、オンラインで提供されるサービスが増えるに従い、オンラインサービスの企業ユーザの認証方法を多少手直しする必要があるだろうと認識している。政府機関がAGAFを採用することにより、企業は単純なもしくは低リスクの取引のために面倒で高コストの認証手順を実行しなくてもよくなり、政府が企業に自らの認証をさせる場合、現実的かつ一貫した姿勢が確保されるだろう。同様に、企業は、その商行為に適したレベルの認証を決定するために、AGAFに概略されたリスク管理技術を利用することができる。

本人認証やユーザ情報認証の状況は進化している。したがって、オーストラリア政府は、これからの認証の必要に関し、引き続き企業と協調して取り組むつもりである。

## 別表 A

### AGAFのリスク保証レベル

<b>レベル 1 – 最低リスク</b>
<p>レベル1の認証は、実際は虚偽であるのに真実と受け取られた表明から、<b>最小損害</b>が発生すると思われる電子政府取引に適している。この損害は下記の事態を引き起こす可能性がある。</p> <ul style="list-style-type: none"><li>• 誰かに最小の不便をかける。</li><li>• 個人の安全へのリスクはない。</li><li>• 個人的、商業的機密情報の第三者への開示はない。</li><li>• 誰かに最小の金銭的損失を与える。</li><li>• 誰の地位や評判も傷つけない。</li><li>• 誰にも苦痛を与えない。</li><li>• 政府機関のシステムやその業務履行能力に対する脅威はない。</li><li>• 重大な犯罪を幫助することも、その発覚を妨げることもしない。</li></ul>
<b>レベル 2 – 低リスク</b>
<p>レベル2の認証は、実際は虚偽であるのに真実と受け取られた表明から、<b>軽度の損害</b>が発生すると思われる電子政府取引に適している。この損害は下記の事態を引き起こす可能性がある。</p> <ul style="list-style-type: none"><li>• 誰かに軽度の不便をかける。</li><li>• 個人の安全へのリスクはない。</li><li>• 個人的、商業的機密情報の第三者への開示はない。</li><li>• 誰かに軽度の金銭的損失を与える。</li><li>• 誰かの地位や評判に軽度の損傷を与える。</li><li>• 誰かに軽度の苦痛を与える。</li><li>• 政府機関のシステムやその業務履行能力に対する脅威はない。</li><li>• 重大な犯罪を幫助することも、その発覚を妨げることもしない。</li></ul>
<b>レベル 3 – 中リスク</b>
<p>レベル3の認証は、実際は虚偽であるのに真実と受け取られた表明から、<b>中程度の損害</b>が発生すると思われる電子政府取引に適している。この損害は下記の事態を引き起こす可能性がある。</p> <ul style="list-style-type: none"><li>• 誰かに相当な不便をかける。</li><li>• 個人の安全へのリスクはない。</li><li>• 個人的、商業的機密情報の第三者への開示がある。</li><li>• 誰かに相当な金銭的損失を与える。</li><li>• 誰かの地位や評判に相当の損傷を与える。</li><li>• 誰かに相当の苦痛を与える。</li><li>• 政府機関のシステムやその業務履行能力に中程度の脅威を与える。</li><li>• <b>重大な犯罪を幫助する可能性やその発覚を妨げる可能性がある。</b></li></ul>
<b>レベル 4 – 高リスク</b>
<p>レベル4の認証は、実際は虚偽であるのに真実と受け取られた表明から、<b>重大な損害</b>が発生すると思われる電子政府取引に適している。この損害は下記の事態を引き起こす可能性がある。</p> <ul style="list-style-type: none"><li>• 誰かに重大な不便をかける。</li><li>• 個人の安全へのリスクがある。</li><li>• 個人的、商業的機密情報の第三者への開示がある。</li><li>• 誰かに重大な金銭的損失を与える。</li><li>• 誰かの地位や評判に重大な損傷を与える。</li><li>• 誰かに重大な苦痛を与える。</li><li>• 政府機関のシステムやその業務履行能力に重大な脅威を与える。</li><li>• 重大な犯罪を幫助する可能性やその発覚を妨げる可能性がある。</li></ul>

## 別表 B

### 事例 1

#### オーストラリア企業番号の申請- 共有情報

オーストラリア企業番号 (ABN) は、11桁の識別子であり、オーストラリア租税局その他の政府機関との取引を円滑化するものである。

企業は、セキュリティ及びプライバシーを確保するため、セキュア・ソケット・レイヤ (SSL) を使ってオンラインでABNを申請することができる。新たな申請がなされる度に独自の参照番号が生成される。企業が申請書を保存し、後で完成させようとする場合、この参照番号を記憶しておかなければならない。企業は、次にパスワードを指定する。租税局は申請者に対し、申請者の又は共同事業者の身元証拠を提供するよう求める。

租税局は、申請者が提供した情報と政府機関に検証用として存在するデータ (例えば、オーストラリア証券投資委員会 (ASIC) によるオーストラリア会社登録番号 (ACN)) とを比較する。

ABNが発行されれば、企業は、租税局が発行するデジタル証明書 (公開鍵基盤機構) を使って、各種情報にアクセスしなければならない。

認証及び租税局が使用するセキュリティプロトコルに関する更なる情報は、[www.abr.gov.au](http://www.abr.gov.au) に掲載されている。

### 例 2

#### ビジネス・エントリー・ポイント- ユーザーネーム/パスワード- SSL

ビジネス・エントリー・ポイント(BEP) は、オーストラリアの中小企業界のためのオンライン政府資源である。これは企業に対し、起業、税務、許認可や規制について広範なサービスや情報を与えると共に、納税や許認可申請などの重要なオンライン取引も可能にする。

BEPのトランザクション・マネージャ機能は、ユーザがサイトにいる間、セキュア・ソケット・レイヤ (SSL)暗号化により保護される。SSLに基づく認証手順は、あるサーバが本当に正当なサーバであるかを確認するために公開鍵暗号化及びデジタル署名を使用する。それは、ユーザを認証するものではない。いったん、サーバが認証されると、クライアント及びサーバは、両者が交換する情報を暗号化するために対称鍵暗号の技術を使う。異なるセッション鍵が各取引に使用され、ハッカーがメッセージを解読できないようにする。企業は、BEPにアクセスするのにユーザーネーム/パスワードを使用する。

認証及びBEPで使用されるセキュリティプロトコルに関する更なる情報は、[www.business.gov.au](http://www.business.gov.au) に掲載されている。

### 事例 3

#### セキュアネット医療電子署名局(HeSA) 医療PKI

セキュアネットHeSA 医療PKI は、オーストラリアの医療部門に公開鍵基盤(PKI) を提供する。PKI は、インターネット上で医療関係の情報の送受信に使用され、患者情報の危殆化が発生しないことを確保する。

自身のデジタル鍵及び証明書の取得に関心のある医療提供者は、医療電子署名局 (HeSA)を通して登録する必要がある。

HeSAは、次の2種類の証明書を提供する。

- 「個人」証明書は、ある人が電子的にメッセージを暗号化し、他の証明書加入者と交換することを可能にする。これはまた、電子署名を個人レベルで行なうことを可能にし、それによって、情報を送信する人の本人性に関し高レベルの確実性が与えられる。
- 「ロケーション」証明書は、同一ロケーションにいる多数の人がメッセージを暗号化し、署名し、他の証明書加入者と交換することを可能にする。ロケーション証明書を使用したメッセージの署名は、メッセージが発行されたロケーションを確認するが、どの個人が発行したかは確認しない。

すべての加入者は、次の2組の鍵ペアを受領する。

- 認証及びデータ完全性のための秘密認証鍵及び公開認証鍵。送信者は、自身の秘密認証鍵を使用してメッセージにデジタル署名をする。一方、メッセージの受信者は、いったんメッセージを受信すると、送信者のデジタル署名を検証するために公開認証鍵を使用する。
- 電子メッセージの秘密保持を保護するための秘密守秘鍵及び公開守秘鍵。送信者は、メッセージを送信する前に、受信者の公開守秘鍵を使って暗号化する。一方、受信者は、自身の秘密守秘鍵を使用して、受信したメッセージを解読する。
- デジタル鍵及び証明書を登録するには、すべての申請者はHeSA のウェブサイトアクセスして登録申請をするが、この手続にはユーザID / パスワード方式が使用される( ABNの申請とほぼ同じ)。申請者は、一連の質問に回答し、HeSA が証明書発行の手配をするために必要な情報を提供する。登録手続きを完成させるために、すべての申請者は、申請手続き中に指示されるところに従い、身元証明関連の文書のハードコピーを提出しなければならない。

認証及びHeSAで 사용되는セキュリティプロトコルに関する更なる情報は、 [www.hesa.com.au](http://www.hesa.com.au) に掲載されている。

## 別表 C

用語集: AGAF – 企業のための概略	
用語	定義
属性	<p>事業体の性格。事業体には人又は組織が含まれる。</p> <p>人の属性には、人の性、年齢層、資格（登録弁護士など）、他事業体の代理人として行為する資格が含まれる。企業の属性には、ASIC会社登録番号、オーストラリア企業番号等が含まれる。</p>
認証	<p>宣言や主張の信頼性において一定レベルの信頼度を達成するために宣言や主張を検証する手順。</p>
バイオメトリクス	<p>バイオメトリック技術は、個人を識別するために生理的、行動的な特徴を利用する。例えば、虹彩スキャン、網膜スキャン、顔スキャン、指スキャン、掌形認証、声検証及び動的署名検証などがある。</p>
企業から政府(B2G)	<p>企業と政府間のオンライン取引。</p>
認証局 (CA)	<p>デジタル証明書を発行し、その内容を保証し、そのような事業を行なうことを政府に信託され、その旨の保証及びある程度の補償さえ提供することのある組織。</p>
チャレンジレスポンス	<p>ユーザが質問（「チャレンジ」）に対し正しい回答（「レスポンス」）を与えるまで、ユーザのアクセスを許さないシステムの認証技術。</p>
信用証明物	<p>物理的又はデジタルに存在する文書や物であって、宣言や主張の認証過程の中でこれを裏付ける。</p> <p>例えば、本人確認文書やトークンなど。</p>
暗号法	<p>平文を「暗号文」に変換することにより、権限付与されていない受信者には理解できない平文を提供する、及びこの暗号化された「暗号文」を理解できる形に戻すための原則、手段、方法に関する研究分野。</p>
復号化	<p>暗号化がなされる前の「平文」形式を回復するための暗号文の暗号変換。暗号化及び暗号法も参照。</p>

デジタル証明書	<p>下記の事項を行なう認証局が署名した電子文書。</p> <ul style="list-style-type: none"> <li>鍵保有者及び鍵保有者が代表する事業体を識別する。</li> <li>鍵ペアの公開鍵を特定することにより、鍵保有者を鍵ペア（公開鍵及び秘密鍵）に結びつける。及び</li> <li>証明書プロファイルに要求される全ての情報を含めなければならない。</li> </ul>
デジタル署名	印刷文書のための手書き署名と同様に、電子文書のための電子署名。当該署名は、ある名の人とその署名が付された文書を書いたか、その文書に同意したことを表明する、偽造不可能なデータである。
電子政府	政府機関が他の事業体と交渉する場合の電気通信ベースツールのアプリケーション。
暗号化	データの元の意味が知られたり、使用されたりすることを防ぐために平文データをその元の意味を隠す形式（暗号文）にする暗号変換。復号化及び暗号法も参照。
事業体	認証される組織又は人。法人、トラスト、退職年金基金、社団法人などが含まれる。
身元証拠 (EOI)	身元に関する宣言や主張の認証において裏付けとなる証拠。
Gatekeeper 認定	政府使用のためのPKIシステムの認定。認証局又は登録局が公表されているGatekeeper 認定基準を満たしているという根拠に基づいて与えられる認定。
ハードトークン	スマートカードのような物理的な認証デバイス
本人認証	宣言や主張の信頼性において一定レベルの信頼度を達成するために、特定の事業体がある身元を適切に使っているという宣言や主張を検証する手順。
本人確認文書	手書き文書や印刷文書、又はそれと同等の電子形態のもの、例えば、出生証明書、旅券、運転免許、雇用主発行のビル・セキュリティ・カード等。
鍵	メッセージを暗号化又は復号化するために使用されるデータ要

	素
否認防止性	事業者がある特定の宣言や主張を否認又は否定する可能性を排除されている状態。
ワンタイムパスワード	ユーザが自身の認証を行なうたびに新たなパスワードが必要となる認証方式。これは通常、アプリケーションが評価されるたびに、入力するための独自のパスワードを生成するハードウェアの使用によって達成される。
パスワード	ユーザ又はITアドミニストレータに選ばれた任意の文字列であって、ユーザがログオンしようとするときに、ユーザを認証するために使用される。  個人識別番号(PIN)も参照。
個人識別番号(PIN)	人がユーザネームを使用する権利を有するという宣言や主張の認証において裏付けのために使用される文字列。  パスワードも参照。
PKI	公開鍵基盤を参照。
秘密鍵	事業者を代表して電子的にメッセージに署名するために使用される暗号鍵ペアのうちの秘密コンポーネント。
公開鍵	事業者を代表して電子的にメッセージに署名するために使用される暗号鍵ペアのうちの公開可能なコンポーネント。
公開鍵暗号法	鍵ペアと呼ばれる2つの関連する鍵が関与する暗号法の一形式。鍵ペアのうち的一方(秘密鍵)は所有者だけが知っているはずであり、他方(公開鍵)は、誰でも知ることができる。
公開鍵基盤(PKI)	情報交換の安全な方法。IDや文書やメッセージの暗号化に、PKIでは「公開鍵及び秘密鍵」方式を用いる。公共システム上で人や組織の本人性を認証するデジタル証明書を発行する認証局から始められる。
登録	後続の認証過程を簡単にするための一連のステップから構成される過程。
登録局(RA)	認証局(CA)に代わり登録手続を行う事業者。
リスク管理	脅威、脆弱、リスクが評価され、コストと便益との間の調和が

	求められる過程。
共有情報	正当なユーザだけが答えることのできる一連の質問。例えば、母親の旧姓。
スマートカード	識別又は金銭取引に使用される、マイクロプロセッサ及びメモリ内蔵型クレジットカード様デバイス。読取機にかけると、中央コンピュータとデータのやりとりをする。
ソフトトークン	コンピュータに格納されている認証デバイス。
トークン	ある法的事業体から別の法的事業体に発行され、第三者の事業体がある程度の信頼を置く認証デバイス。トークンは、偽造して当該事業体を騙そうとする試みを困難にするためにセキュリティ機能を備えていることが多い。  例えば、「アイデンティティカード」(特に「写真ID」)、及びスマートカード。
ユーザID	ユーザネームを参照。
ユーザネーム	コンピュータシステムにアクセスするために使用される名前。通常、ITアドミニストレータから、ユーザに発行される文字列。
値	属性を参照。