大統領府
行政管理予算局
ワシントンD.C. 20503

局長

2003年12月16日

M-04-04

各省庁および政府機関長官各位への覚書

発: Joshua B. Bolten
局長

件名: **連邦政府機関向けの電子認証にかかわるガイダンス**

政府は、市民および事業者の書類手続きを削減し、市民への対応時間を、週単位から分単位に向上することを約束している。これらの目標を達成するためには、市民がインターネットを使用して政府のサービスにすばやく簡単にアクセスできる必要がある。本ガイダンスは、紙の代わりにインターネットを使用してオンラインで実施される政府のサービスを対象としている。政府のオンライン・サービスの安全性と、プライバシー保護を確実にするためには、何らかの本人確認あるいは認証が必要である。

本ガイダンスは、合衆国法典第44編第3504条、1998年政府事務書類制限法 (GPEA: Government Paperwork Elimination Act) **に基づいて行政管理予算局** (OMB：Office of Management and Budget、**以下、OMBと称す**) **が発行したガイダンスを更新するものであり、合衆国法典第44編第36章の電子政府法** (E-Government Act) **の第203条を施行するものである。本ガイダンスはまた、電子認証電子政府構想** (E-Authentication E-Government Initiative) **の成果としての活動および米国国立標準技術研究所** (National Institute of Standards and Technology、**以下、**NIST**と称す**) **が発行した最新の標準を反映している。本ガイダンスの作成にあたり、**OMB**は各政府機関の最高情報責任者** (CIO) **と緊密に連携し、それぞれの意見を取り込んでいる。**

本ガイダンスでは、特定の電子的なトランザクションへのアクセスを対象とした認証 (**または電子認証**) **の分野における現行の方法や、政府全体としての標準の必要性を考慮するとともに、各政府機関が電子的なトランザクションに関わる認証の必要性を決定するのを支援する。本ガイダンスでは、政府が横断的に一貫したアプローチを採ることを確実なものとするために、各政府機関に対し、電子的なトランザクションについての「電子認証リスクアセスメント」を実施するように指示している** (**別添**A**参照**) **。また、連邦政府のサービスにオンラインでアクセスするための明確に理解できる基準を国民に対して提供する。別添**B**は、本ガイダンスの初期の版に対して寄せられたパブリックコメントについてまとめたものである。**

本ガイダンスに関する質問は、下記まで連絡されたい。
行政管理予算局 (Office of Management and Budget)
情報政策技術部 (Information Policy and Technology Branch)
政策アナリスト (Policy Analyst)
Jeanette Thornton
電話: (202) 395-3562
FAX: (202) 395-5167

電子メール: eauth@omb.eop.gov

別添

別添A: **連邦政府機関向けの電子認証に関わるガイダンス**
別添B: **パブリックコメントとそれらに対する対応の概要**

別添A

連邦政府機関向けの電子認証に関わるガイダンス

セクション1: **序説**
セクション2: **保証レベルおよびリスクアセスメント**
セクション3: **クレデンシャルサービスプロバイダの信頼性の評価**
セクション4: **認証プロセスの実装**
セクション5: **ガイダンスの発効日**

1. 序説

1.1. 概要

本ガイダンスでは、認証プロセスが適切なレベルの保証を与えることを確実なものとするために、各政府機関に対し、新規および既存の電子的なトランザクションを見直すことを要求している。本ガイダンスでは、認証を必要とする電子的なトランザクションにおける身元保証について4つのレベルを規定し、説明する。保証レベルは、連邦政府機関に代わってクレデンシャルサービスプロバイダ（Credential Service Providers、以下、CSPと称す）を評価するための基礎となる。本文書は、各政府機関が電子政府における認証の必要性を決定するのを支援する。各政府機関の業務プロセスのオーナーは、保証レベルおよびそれらを提供するための戦略を明らかにする主要な責任を負っている。この責任は、電子認証システムにも及ぶ。

政府機関は、2.3項で説明する次の手順を使用して保証レベルを決めるものとする。

1. 電子政府システムのリスクアセスメントを実施する。
2. 明らかにされたリスクを、適用可能な保証レベルに割り当てる。
3. 電子認証の技術ガイダンスに基づいて技術を選択する。
4. 実装したシステムが、要求されている保証レベルを達成していることを検証する。
5. 技術更新の必要性を判断するためにシステムを定期的に再評価する。

1.2. 適用範囲

- 本ガイダンスは、政府の業務を電子的に実施することを目的とする連邦政府機関の情報技術システム（すなわち電子政府）の利用者のリモート認証に適用する。一般に、認証においてはコンピュータや他の電子装置を含めるが、本ガイダンスではサーバの認証や他の機器の認証、およびネットワーク構成要素の認証は対象としない。

- 本ガイダンスの目的は、各政府機関が、認証プロセスの各ステップに対応するリスクを特定し分析することの支援である。認証プロセスには、身元証明、クレデンシャルの処理、技術管理および運営管理、記録維持、監査ならびにクレデンシャルの使用が含まれる（ただし、これらに限定されない）。プロセスの各ステップは、目標とする保証レベルと技術との全体の適合性に影響する。

- **本ガイダンスは、**OMB**通達** (Circular) A-130『**連邦情報リソースの管理** (Management of Federal Information Resources)』**の付録**II「**政府事務書類制限法** (Implementation of the Government Paperwork Elimination Act (GPEA)) **の実装」を補足するものである。**

- **本ガイダンスは、「認可」には直接適用されない。認可は、認証が行われた後の特定の身元に対して「許可される」活動を対象とする。認可に関わる判断は、業務プロセスオーナーの権限の範囲内にあり、そうあり続けるべきである。**

- **本ガイダンスは、「署名の意思」、すなわち政府機関が電子署名として認証クレデンシャルを使用することに関わる事項は対象としない。電子署名の詳細については、**GPEA**の実装に関わる**OMB**ガイダンス** [1] **および公法**106-229「**国際商取引および国内商取引における電子署名法** (Electronic Signatures in Global and National Commerce Act)」[2] **を参照のこと。**

- **本ガイダンスでは、どの技術を実装すべきかについては特定しない。商務省の米国国立標準技術研究所** (NIST) **では、補足的な電子認証技術ガイダンスを現在作成している。政府機関は、そのガイダンスを用いることにより、ここに説明する分析プロセスに基づき、適切な技術を決定することができるであろう。**

- **本文書は、特定の個人または主体に対して合衆国もしくはその政府機関または職員に対抗するいかなる権利も与えるものではなく、そのような権利を支持するためにも使用してはならない。**

1.3. **概要**

本文書は、政府機関に対し電子的な認証 (**電子認証**) **に関するガイダンスを提供する。米国学術研究会議** (National Research Council) **のレポート「そこを通るのはだれ？プライバシーというレンズを通して見た認証** (Who Goes There? Authentication Through the Lens of Privacy)」[3]**では、電子認証を、情報システムに対し電子的にユーザの識別情報に関する信用を確立するプロセスと定義している。そのレポートでは、個人認証を、特定の識別情報が特定の個人を表していることについて、了解されているレベルの信頼性を確立するプロセスと定義している。**

認証においては、認証対象者のクレデンシャルの信頼性に基づいて個人の身元を確認することが中心となる。「認可」は、個人に許可されるユーザ権限を明確にすることが中心となる。

政府のサービスを電子的に (**つまり、電子政府を**) **成功裏に実装するためには、連邦政府機関は、それぞれのトランザクションについて、要求される保証のレベルを明らかにしなければならない。これは、それぞれのトランザクションについてリスクアセスメントを行うことで達成する。リスクアセスメントにおいては、以下のことを明らかにする。**

a) **リスク**

b) **それらが発生する可能性の高さ**

---

[1] **OMB 覚書** (Memorandum) M-00-10、**2000 年 4 月 25 日、** http://www.whitehouse.gov/omb/memoranda/m00-10.html

[2] **OMB 覚書** (Memorandum) M-00-15、**2000 年 9 月 25 日、** http://www.whitehouse.gov/omb/memoranda/m00-15.html

[3] **2003 年 3 月 31 日、**http://www.nap.edu/books/0309088968/html/

OMB通達 (Circular) A-130『連邦情報リソースの管理 (Management of Federal Information Resources)』には、連邦政府機関が各情報システムに関わるリスクを特定して軽減する戦略を立案し、更新しなければならないと記載されている。本ガイダンスは、各政府機関が、特定されたリスクを対応する保証レベルへ割り当てることを支援する。

GPEAガイダンスのセクション5では、電子政府のトランザクションおよびシステムを計画し、実装するにあたって政府機関が考慮すべきリスク要素の詳細を示している。本文書では、以下を通じ、電子認証プロセスの実装方法を各政府機関に提示することによって、セクション5を詳細化する。

- リスクアセスメントに関するプロセスの概略説明
- 身元保証の4つのレベルの説明
- 適切なレベルの身元保証を決定する方法の説明

1.4. 適用範囲

連邦政府機関のすべてのトランザクション [4] が認証を必要とするわけではない。しかし、本ガイダンスでは、当事者 (個人の利用者、事業者または政府の主体) が誰であるかにかかわりなく、認証を「必要とする」すべてのトランザクションを対象とする。

本ガイダンスの対象とならないトランザクションには、合衆国法典第44編第3542条 (b) (2) で定義された「国家的セキュリティシステム (national security systems)」に関係するトランザクションが含まれる。さまざまなレベルの保証を必要とする電子的プロセスを有する民間組織ならびに州、地方および部族政府は、必要に応じてこれらの標準の使用を検討してもよい。

個人認証には次の2つのタイプがある。

a) 身元の認証:個人固有の身元の確認。
b) 属性の認証:個人が特定のグループ (退役軍人、米国市民など) に属することの確認。

属性の認証は、特定の個人が特定の属性を有することについて、了解されているレベルの信頼性を確立するプロセスである。属性が、利用者の識別情報に結び付いていない場合、その属性は「匿名クレデンシャル」(4.2項にて詳細を説明する) であるとみなされる。属性の認証については本文書においては特には取り上げていないが、政府機関は特定の状況においては「匿名クレデンシャル」を受け付けてもよい。

2. 保証レベルおよびリスクアセスメント

2.1. 保証レベルの説明

本ガイダンスでは、電子政府トランザクション向けの識別情報認証の4つの保証レベルを説明する。それぞれの保証レベルは、利用者がその身元を示す識別情報 (この文脈においては、ク

---

[4] 本文書の目的のため、トランザクションを「利用者と、業務またはプログラム上の目的を支援するシステムとの間の個別の独立した事象」と定義する。

レデンシャル [5] を提示したことについての政府機関の確信の程度を示す。この文脈においては、保証とは、1) クレデンシャルの発行対象者の身元を確立するための「審査プロセス」の信頼性の程度、および、2) そのクレデンシャルを使用する個人が、当該クレデンシャルの発行対象となった個人であることの信頼性の程度、と定義する。

4つの保証レベルは次のとおりである。

- レベル1: 主張された識別情報の有効性についてほぼ、あるいはまったく信頼性がない。
- レベル2: 主張された識別情報の有効性についてある程度の信頼性がある。
- レベル3: 主張された識別情報の有効性について高い信頼性がある。
- レベル4: 主張された識別情報の有効性についてきわめて高い信頼性がある。

2.2. リスク、潜在的影響および保証レベル

本ガイダンスでは、認証エラーに関連するリスクのみを対象とするが、NIST Special Publication 800-30『ITシステムのためのリスクマネジメントガイド（Risk Management Guide for Information Technology Systems）』では、連邦政府の情報システムにおいてリスクを管理するための一般的な方法論を推奨している。加えて、ほかの手段によるリスクマネジメント（ネットワークのアクセス制限、侵入検知およびイベント監視など）も、より高いレベルの認証保証に対する必要性を低減するのに役立つ場合がある。

潜在的影響の分類:利用者が主張する識別情報について妥当なレベルの保証を決定するためには、政府機関は潜在的なリスクを評価し、それらの影響を最小限に抑える対策を特定する必要がある。より悪い結果を招く可能性のある認証エラーについては、より高い保証レベルが必要となる。業務プロセス、ポリシーおよび技術がリスクの低減に役立つ場合がある。認証エラーによるリスクは、次の2つの要素の関数である。

a) 潜在的な害または影響
b) そのような害または影響が生じる可能性の高さ

害および影響には、次のような分類が含まれる。

- 不便、苦痛もしくは地位または評判に対する打撃
- 財務上の損失または政府機関の賠償責任
- 政府機関の活動計画または公共の利益に対する害
- 機密情報の無許可の公開
- 身の安全
- 民事上または刑事上の法律違反

---

[5] クレデンシャルを、「認証トランザクションにおいて検証者に対して提示されたときに検証される対象物」と定義する。

電子的なトランザクションに要求される保証レベルは、連邦情報処理規格 (FIPS: Federal Information Processing Standard) 199『連邦政府の情報および情報システムに対するセキュリティ分類規格(Standard for Security Categorization of Federal Information and Information Systems)』に説明されている潜在的影響の値を使用し、上記のそれぞれの分類について潜在的な影響を評価することによって決定される。3つの潜在的影響の値は、次のとおりである。[6]

- 低位の影響
- 中位の影響
- 高位の影響

次項では、それぞれの分類の潜在的影響を定義する。注:認証エラーが、特定の分類おいて測定可能な結果をもたらさない場合には、そこには影響は「存在しない」ものとする。

認証エラーの潜在的影響の決定

「不便、苦痛もしくは地位または評判に対する打撃」の潜在的影響:
- 低位 — 最悪の場合、限定的かつ短期間の不便、苦痛または任意の当事者の当惑。
- 中位 — 最悪の場合、深刻かつ短期間または限定的かつ長期間の不便、苦痛または任意の当事者の地位または評判に対する打撃。
- 高位 — 深刻または長期間の不便、苦痛または任意の当事者の地位または評判に対する打撃 (通常は、特に深刻な影響のある状況や多くの個人に影響する状況のために用意されている)。

「財務上の損失」の潜在的影響:
- 低位 — 最悪の場合、任意の当事者の回復不能で軽微または若干の財務上の損失、もしくは最悪の場合、政府機関の軽微または若干の賠償責任。
- 中位 — 最悪の場合、任意の当事者の深刻で回復不能な財務上の損失、もしくは政府機関の深刻な賠償責任。
- 高位 — 任意の当事者の壊滅的で回復不能な財務上の損失、もしくは政府機関の深刻または壊滅的な賠償責任。

「政府機関の活動計画または公共の利益に対する害」の潜在的影響:
- 低位 — 最悪の場合、組織の運営または資産もしくは公共の利益に対する限定的な悪影響。限定的な悪影響の例としては以下が考えられる。(i) 組織が「著しく」低下した効率で主要な機能を実施せざるを得ず、その状態が継続する、業務能力の劣化。(ii) 組織の資産または公共の利益の軽微な損害。
- 中位 — 最悪の場合、組織の運営または資産もしくは公共の利益に対する深刻な悪影響。深刻な悪影響の例としては以下が考えられる。(i) 組織が「大幅に」低下した効率で主要な機能を実施せざるを得ず、その状態が継続する、業務能力の大幅な劣化。(ii) 組織の資産または公共の利益の重大な損害。
- 高位 — 組織の運営または資産もしくは公共の利益に対する重大または壊滅的な悪影響。重大または壊滅的な悪影響の例としては以下が考えられる。(i) 組織が主要な機能の1つ以上を実施できず、その状態が継続する、業務能力の激しい劣化または喪失。(ii) 組織の資産または公共の利益の際立った損害。

---

[6] 本文書の目的のため、該当しない影響の値は、害の分類に該当する場合がある。

「機密情報の無許可の公開」の潜在的影響:

- 低位 — 最悪の場合、許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の限定的な公開に起因する、FIPS PUB 199に規定されている「低位の影響」をもたらす機密性喪失。
- 中位 — 最悪の場合、許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の公開に起因する、FIPS PUB 199に規定されている「中位の影響」をもたらす機密性喪失。
- 高位 — 許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の公開に起因する、FIPS PUB 199に規定されている「高位の影響」をもたらす機密性喪失。

「身の安全」の潜在的影響:

- 低位 — 最悪の場合、医療措置を必要としない軽症。
- 中位 — 最悪の場合、軽症が生じる中程度のリスクまたは医療措置を必要とする負傷が生じる限定的なリスク。
- 高位 — 深刻な負傷または死亡のリスク。

「民事上または刑事上の法律違反」の潜在的影響:

- 低位 — 最悪の場合、通常は法執行の対象とならないような性質の民事上または刑事上の法律違反のリスク。
- 中位 — 最悪の場合、法執行の対象となる可能性のある民事上または刑事上の法律違反のリスク。
- 高位 — 法執行の計画にとって特に重要とされている民事上または刑事上の法律違反のリスク。

保証レベルの決定:

リスクアセスメントから得られた影響のプロファイルを、以下の表1に示す各保証レベルに対応する影響のプロファイルと比較する。求められる保証レベルを決定するには、リスクアセスメントにおいて分析したすべての分類について、(後述のステップ2に示すように) その潜在的影響と同じかまたはそれを上回る影響プロファイルを見つけなければならない。

表1 — 各保証レベルにおける最大の潜在的影響

	保証レベルに対する影響プロファイル			
認証エラーの潜在的影響の分類	*1*	*2*	*3*	*4*
不便、苦痛もしくは地位または評判に対する打撃	***低位***	***中位***	***中位***	***高位***
財務上の損失または政府機関の賠償責任	***低位***	***中位***	***中位***	***高位***
政府機関の活動計画または公共の利益に対する害	***該当なし***	***低位***	***中位***	***高位***
機密情報の無許可の公開	***該当なし***	***低位***	***中位***	***高位***
身の安全	***該当なし***	***該当なし***	***低位***	***中位 高位***
民事上または刑事上の法律違反	***該当なし***	***低位***	***中位***	***高位***

政府機関は、潜在的影響の分析にあたって、2つ以上の失敗または2人以上の人に対する害がある可能性を含め、認証失敗の直接または間接の潜在的結果をすべて考慮しなければな

らない。潜在的影響の定義には、「深刻」、「軽微」など相対的な言葉が含まれており、それらの意味は状況によって異なる。政府機関は、これらの害の相対的な大きさを判断するにあたって、状況、ならびに影響を受ける人々または主体の性質を考慮すべきである。今後、政府機関がこれらの事項について実際的な経験を積むにつれて、これらの用語の意味もより明確になってくる。政府機関の活動計画または他の公共の利益に対する害の分析は、状況に大きく依存する。政府機関は、これらの事項について慎重に考慮する必要がある。

場合によっては（表1に示したように）、影響が複数の保証レベルに対応することがある。たとえば、表1を見ると、財務上の損失の中位のリスクは、保証レベル2および3に対応する。このような場合、政府機関はその状況を考慮して適切な保証レベルを決めればよい。

2.3. リスクアセスメントを使用した保証レベルの決定および認証ソリューションの選択

政府機関は、以下のステップを使用して適切な保証レベルを決定するものとする。

ステップ1: 電子政府システムのリスクアセスメントを実施する。政府機関がリスクアセスメントを実施するためのガイダンスとしては、OMBのGPEAガイダンスのA-130、セクション5およびNISTの既存のガイダンスが利用できる。リスクアセスメントにおいては、潜在的な害の相対的な深刻さ、および個人識別情報認証エラーが生じた場合に電子政府システムに関連して幅広い範囲の（任意の当事者に対する）影響が発生する可能性を評価する。

注:1つの電子政府システムであっても、複数の分類やタイプのトランザクションが存在する可能性があり、その場合は、全体のリスクアセスメントの中で個別に分析が必要となる。また、1つの電子政府システムであっても、複数の政府機関を横断する可能性がある。その場合、それぞれの機関の活動を個別に考慮する必要がある場合も生じる。

リスク分析は、ある程度までは主観的なプロセスであり、政府機関は、技術的な失敗、悪意のある第三者、国民の誤解、人的エラーを含むさまざまな要因に起因する害を考慮しなければならない。政府機関は、それぞれの業務プロセスにどのような潜在的な害が対応するかを判断するために、幅広いシナリオを考慮しなければならない。この分析を行うにあたっては、範囲が狭すぎるよりは広すぎるほうがよい。一度リスクを明らかにしたら、特定のリスクが生じる可能性を低減することで、そのリスクを軽減するために、業務プロセスを調整する方法が存在する可能性もある（ステップ 4を参照）。

ステップ2: 明らかにされたリスクを、該当する保証レベルに割り当てる。リスクアセスメントは、2.2項の潜在的影響の分類に従ってまとめるものとする。

必要な保証レベルを決定するために、政府機関はまず認証技術に関係なく、トランザクションプロセス固有のリスクを明らかにすべきである。続いて、政府機関は明らかになったすべての潜在的影響に対応できる最低限のレベルの認証を選び、潜在的影響の分類の結果を認証レベルに対応付ける。つまり、潜在的影響の5つの分類がレベル1に該当し、潜在的影響の1つの分類がレベル2に該当する場合、そのトランザクションに必要なのは、レベル2の認証である。たとえば、医療処置の際に利用者の電子的な身元識別情報/クレデンシャルの誤使用によって深刻な怪我または死亡のリスクが生じる場合、他に引き起こされる結果がたとえ軽微であったとしても、レベル4の欄のリスクプロファイルに割り当てる。

ステップ3: NISTの電子認証の技術ガイダンスに基づいて技術を選択する。保証レベルを決定した後、政府機関はNISTの電子認証技術ガイダンスを参照して、適切な技術要件を明らかにして実装すべきである。

ステップ4: 実装後、情報システムが必要な保証レベルを運用上達成していることを検証する。実装によっては、特定のリスクが生まれたり、複雑化したりする可能性があるため、最終的な検証を実施して、ユーザと政府機関の間のプロセスについて、必要な保証レベルがシステムにおいて達成されていることを確認すること。政府機関は、要求されているセキュリティ手順（例えば証明および認定）の一環として、認証プロセスがシステムの認証要件を満たすことを確認すべきである。

ステップ5: 技術更新の必要性を判断するために情報システムを定期的に再評価する。政府機関は、技術の変化や政府機関の業務プロセスの変化を受けて、身元識別情報認証の要件が引き続き有効であることを確実なものとするために、情報システムを定期的に再評価しなければならない。年次の情報セキュリティ評価義務は、そのための格好の機会を提供する。政府機関は、追加的なリスク軽減策を採用して、身元クレデンシャルの保証レベルを調整してもよい。身元クレデンシャルの保証レベルの要件を緩和すると、利用が可能な顧客の人数が増える可能性はあるが、政府機関は、それがシステムにとって適切な保証レベルを選択することに反しないことを確実なものとしなければならない。

2.4. 保証レベルおよびリスクプロファイル:説明および例

レベル1 — 主張された識別情報の信頼性がほぼ、あるいはまったくない。たとえば、レベル1のクレデンシャルを持つ人は、Webページ上の項目を後で参照できるように、ブックマークできる。

例:

- 電子的なトランザクションにおける個人によるフォームの送信は、次の場合にレベル1のトランザクションとなる場合。(i) すべての情報が、その個人から連邦政府機関に流れる、(ii) 送信に対して何も情報が公開されず、(iii) より上位の保証レベルの基準が適用されない場合。たとえば、ある個人がある公園の年間入園許可証を申請するとき（そして、そのトランザクションの金銭面については別の契約者が扱い、そのために別のトランザクションとして分析される場合）、連邦政府機関とのトランザクションは、最小限のリスクしか生じないため、レベル1として扱うことができる。

- 利用者が、カスタマイズされた「My.ED.gov」ページを作成することを許可する、自身の登録によるユーザIDまたはパスワードを合衆国教育省に提示する場合。IDまたはパスワードを不正に入手した第三者が、カスタマイズの内容から、該当する個人の個人情報または業務の情報を推測する可能性があるが、カスタマイズの程度が高くなければ、そのようなリスクはおそらく非常に低い。

- 利用者がwhitehouse.govのWebサイトでのオンラインディスカッションに参加する場合。ここでは名前および所在地以外の情報を明らかにすることを求められない。フォーラムが機密情報や個人情報を対象としたものでなければ、明白な固有のリスクはない。

レベル2 — 最終的には、信頼性とは、主張された識別情報が正確であることである。レベル2のクレデンシャルは、政府機関が身元識別のアサーション（アサーションの詳細は、連邦側の任意のアクションに先立って、独立に検証される）を最初に必要とする、国民との幅広い業務にとって適切である。

例:

- **利用者が、**Gov Online Learning Center（www.golearn.gov）**に登録する場合。サイトのトレーニングサービスは、適切なコースの教材を提示したり、利用者が報酬や昇進に関係する必要なトレーニングを修了していることを示したりするために、利用者の認証を行う必要がある。このトランザクションに対応する唯一のリスクは、第三者が成績情報を入手して、受講生のプライバシーまたは評判を害することである。政府機関がそのような害が軽微であると判断した場合、トランザクションはレベル2である。**

- **受給者が社会保障Webサイトを通じて自身の住所記録を変更する場合。このサイトでは、正しい資格保有者の住所が変更されることを保証するために認証が必要となる。このトランザクションには、不便が生じることについて低いリスクがある。支払い金額、口座の状態および変更の記録にかかわる公式の通知は、受給者の記録上の住所に送られるので、個人の秘密情報が不正に公開される中程度のリスクがある。政府機関は、不正な公開のリスクを鑑みて保証レベル2の認証が妥当かどうかを判断する。**

- **政府機関のプログラムクライアントが銀行口座、プログラムの資格または支払い情報を更新する場合。喪失または遅延があれば利用者に大きな影響がある。そのようなエラーは、利用者への支払いを遅延させる可能性があるが、通常は永久的な喪失という結果にはならない。個人の財務上の潜在的影響は低いが、積み重ねによって影響が中位になる可能性がある。**

- **政府機関の職員が、潜在的に機密な、個人顧客情報にアクセスできる場合。職員は、個別にシステムに対しレベル2の認証を行うが、技術的な管理策（仮想プライベートネットワークなど）によって、システムへのシステム上のアクセスを政府機関の構内に限定できる。構内へのアクセスは管理されており、システムのログには職員のアクセスのインスタンスが記録される。これよりも制約の少ない環境の場合、個人の機密情報への職員によるアクセスは、その情報の不正な公開について「中位」の潜在的影響をもたらすが、システムのセキュリティ対策によって全体のリスクが「低位」となる。**

レベル3 — レベル3は、主張された身元識別情報の確実性について高い信頼性が必要なトランザクションに適している。利用者は、レベル3のクレデンシャルを使用することで、追加の身元識別アサーション管理策の必要なしに、アクセスが限定されているWebサービスにアクセスできる。

例:

- **特許弁理士が合衆国特許商標局に対し、機密の特許情報を電子的に提出する場合。不適切に開示された場合、競合相手が競争上優位に立てることになる。**

- ある供給業者が、大規模な政府調達について、一般調達局の契約担当官に対する口座を維持している場合。潜在的な財務上の損失は大きいが、重大または壊滅的ではないので、レベル4は適切ではない。

- 第一対応者が、インシデントを報告し、運営上の情報を共有し、対策活動をコーディネートするために、災害管理報告Webサイトにアクセスする場合。

- 政府機関の職員または委託業者が、リモートシステムを使用して、潜在的に機密な、個人顧客情報へのアクセスする場合。当該職員は、アクセスが限定されている連邦政府の庁舎で作業をする。これによってコンピュータへの物理的なアクセスは限定されるが、システムトランザクションはインターネット経由で行われる。職員が機密の個人情報を入手できることによって、不正な公開について中位の潜在的影響がもたらされる。

レベル4 — レベル4は、主張された身元識別情報の確実性について非常に高い信頼性が必要なトランザクションに適している。利用者は、レベル4のクレデンシャルを提示することで、追加の身元識別アサーション管理策の必要なしに、身元を主張して、アクセスが限定されているWebリソースにアクセスできる。

例:

- 法執行官が、犯罪歴が格納されている法執行データベースにアクセスする場合。不正なアクセスがあれば、プライバシーの問題が発生したり捜査が妨げられたりする可能性がある。

- 復員軍人援護局の薬剤師が規制医薬品を調剤する場合。薬剤師は、資格のある医師が処方したものであることの確実な保証が必要である。薬剤師は、処方箋の検証と、処方された量に基づく薬剤の正しい調剤ができなかった場合、刑事責任を問われる。

- 政府機関の捜査官が、リモートシステムを使用して、潜在的に機密の個人顧客情報へアクセスする場合。捜査官は、自身のノートPCをクライアントの現場、個人宅または職場で使用して、さまざまな接続を通ってインターネット経由で情報にアクセスする。捜査官が機密の個人情報にアクセスできることで、不正な公開については中位の潜在的影響しかもたらさないが、捜査官のノートPCの脆弱性および安全でないインターネットアクセスが全体のリスクを高める。

2.5. リスクの範囲および要素

保証レベルを判断するときに必要なリスクアセスメントの要素の1つは、電子的に伝送された情報の否定（または否認）である。OMBのGPEAガイダンスのセクション9cにおいては、そのような情報について利用者の是認を得るようにすることで、リスクをいかに最小に抑えるかを計画すべきだと述べている。OMBのGPEA実装手順およびガイダンスのセクション8cには、否認の発生可能性を最小限にすることに関するガイダンスが含まれている。

OMBのGPEAガイダンスでは、適切に実装された技術は、身元識別の認証について、手書きの署名よりも高い信頼性を提供できると述べている。しかし逆に、電子的なトランザクションによって、刑事上および民事上の法律違反に関連するリスクまたは害が大きくなる（そして、その

救済を複雑化させる）可能性がある。司法省の『連邦政府機関向けの電子プロセス実装ガイド（Guide for Federal Agencies on Implementing Electronic Processes）』[7]では、電子政府にまつわる法的な課題について論じている。法的な必要性および執行上の必要性が認証システムの設計に影響を与える可能性がある。また、特定のシステム管理文書の作成および維持を伴うこともある。

法的な問題は、政府機関にとって政策上大きな課題となる可能性がある。政府機関は、トランザクションに対して保証レベルを割り当てるとき、こうした問題を考慮すべきである。リスクアセスメントにおいては、以下に関して、違法な活動およびプロセスの失敗の潜在的な影響を含めるべきである。

- 政府機関の執行の優先順位
- 政府機関の計画上の利害
- 国家安全、環境および経済市場など、より広い公共の利害

一部の害（財務上の損失や個人情報の公開など）については、それぞれの保証レベルのところで説明しており、その他は政府機関の活動計画上の利害に依存する。リスク分析プロセスは、必然的に大きく状況に依存し、各政府機関はそれぞれのシステムが独自のリスクをもたらさないか考慮すべきである。

リスク分析では、刑事上および民事上の法律違反ならびに政府機関の活動計画または公共の利益に対する害に関連付けられるリスクを検討することで、これを取り込む。政府機関は、この影響を判定するにあたって、それぞれの弁護士事務所と適切に協議すべきであることに留意されたい。このリスクアセスメントを行い、プロセスを設計するとき、政府機関は自身の活動計画に影響を与えうる単独の行為および行動パターンを考慮すべきである。たとえば、機密情報が政府機関のWebサイトから入手できる場合、政府機関は、リスクアセスメントの際に、単独の行為およびそのような行動のありうるパターンを検討するのがよい（合衆国法典第18編第1029条および1030条）。

また、政府機関はリスク軽減管理策を強化することで、身元クレデンシャルへの依存を低減してもよい。たとえば、政府機関の業務プロセスが身元アサーション保証レベル3の対象である場合、システム管理策、つまり“二次レベルの認証”活動を増やすことで、レベル2のクレデンシャルを受け付けるようにプロファイルを緩和できる（セクション2.3、ステップ5を参照）。

政府機関は、電子記録の取扱いについて米国国立公文書館（National Archives and Records Administration、以下、NARAと称す）が発行しているすべての関係ガイダンスに従うことが期待されている。本ガイダンスでは、実装上の課題をセクション4.1でさらに詳しく取り上げる。

3. CSP（Credential Service Providers）の信頼性の評価

身元クレデンシャルは、電子的なトランザクションにおいて自分の身元を示すために使用されるので、クレデンシャルの信頼性のレベルを評価することが重要である。CSPは、政府機関または非政府機関であり、電子クレデンシャルの発行や、場合よっては維持もする。これらの組織は、本ガイダンスで説明している保証レベルに照らして公式の評価を完了しているものとする。

---

[7] http://www.usdoj.gov/criminal/cybercrime/eprocess.pdf

CSPの発行および維持のポリシーは、その電子認証プロセスの信頼性に影響を与える。したがって、電子認証構想（E-Authentication Initiative）においては、CSPが値する最高保証レベルを政府が判定するための評価プロセスを作成する。たとえば、CSPが保証レベル3のプロセスおよび技術の要件をすべて満たす場合、利用者は、そのCSPによって提供されるクレデンシャルを使用して、保証レベル1、2および3を必要とするトランザクションに対して自身を認証できる。

4. 認証プロセスの実装

4.1. 電子認証プロセス

身元識別情報の検証から、クレデンシャルの発行、厳密に管理されている安全なアプリケーションにおけるそのクレデンシャルの使用、記録および監査に至るまで、認証プロセスの各ステップは、選択された保証レベルに影響を与える。保証レベルが最も低いステップによって、他のステップが危険にさらされる可能性がある。プロセスの各ステップは、他のステップと同じ程度に強く堅牢でなければならない。政府機関は、強力な身元識別情報検証、強力なクレデンシャルおよび堅牢な管理（強力な保管および監査のプロセスを含む）を通じて最高レベルの身元識別保証を達成する。ただし、最良の認証システムは、設計およびテストが綿密に行われた利用者および政府機関のソフトウェアアプリケーションが結実したものである。現在策定中の連邦政府機関の横断的な認証を可能にするプロセスは、完成すれば実装のために公開される。

利用者の身元確認に必要なクレデンシャルのレベルを決定するために、政府機関は、業務アプリケーションがクレデンシャルをどのように処理するのかを理解する必要がある。政府機関は、電子認証（および認可）プロセスの各ステップの要件を明らかにしなければならない。これには次のステップが含まれる。

- 最初の登録
- 引き続く申請のための政府機関への来訪
- 身元クレデンシャルの検証
- トランザクション管理
- 長期的記録管理
- 定期的システムテスト
- 一時停止、失効、再発行
- 監査

それぞれのステップは、電子認証技術ガイダンスにおいて説明されている。これらのステップの責任は、業務プロセスオーナー、指定政府機関、または政府横断的な権威機関にある。

4.2. 匿名クレデンシャルの使用

身元識別とは異なり、匿名クレデンシャルは、認証を既知の個人識別情報と関連付ける必要がないとき、属性の評価に使用してもよい場合がある。プライバシー保護のためには、誰が政府と通信を行っているのかを知る必要性と、その利用者のプライバシー権とのバランスをとることが重要である。これには、各個人に対して確約したとおりの利用目的でのみ情報を使用す

ることを含む。場合によっては匿名性を保つことが望ましく、以下を認証するだけで十分なことがある。

- 利用者が特定のグループに所属している
- 利用者が、そもそも情報を提供または作成した本人である。
- 利用者が、特定の仮名を使用する権利を与えられている。

これらの匿名クレデンシャルは、用途が限られており、個別的に実装されるものとする。人によっては、匿名クレデンシャルと身元クレデンシャルの両方を持っている場合がある。一般に、匿名クレデンシャルはレベル1およびレベル2に対してのみ適切である。

4.3. 情報共有およびプライバシー法

認証プロセスを開発するとき、政府機関は利用者の身元確認に関連する情報の収集と格納について、セキュリティを管理するための要件を満足しなければならない。2002年制定の電子政府法のセクション208では、電子情報システムおよび収集について、プライバシーへの影響評価を実施することを政府機関に義務付けている。これには、国民がアクセスする電子情報システムに認証技術を追加したときに評価を行うことも含まれる。プライバシーへの影響評価に関する追加情報については、OMBガイダンス [8] を参照されたい。

ほとんどの電子認証プロセスは、次の情報を取得する。

- 電子政府のサービスを使用する個人/事業者/政府に関する情報
- 利用者の電子的なクレデンシャル（つまり、公開鍵証明書、ユーザ識別子、パスワード、個人識別番号PINの何らかの組み合わせ）
- クレデンシャルの検証方法を含め、ユーザ認証に関連付けられるトランザクション情報
- 監査証跡/セキュリティ情報

認証プロセスが、プライバシー法によって保護されている情報（政府機関が個人の名前または他の識別子を使用して取り出す個人に関する情報であり、そのため、政府機関のプライバシー法記録体系において維持されている情報）を取得する場合、政府機関はかかる情報についてプライバシー法を遵守しなければならない。

認証データは、無断の開示または変更から保護されなければならない。プライバシー法では一般に、登録利用者が記録システムに維持されている自身の情報にアクセスしたり、その修正を要請したりできることを要求している。記録のシステムからの情報は、プライバシー法および他の該当する法律に従う場合を除き、共有すべきではない。

---

[8] OMB 覚書 M-03-22、http://www.whitehouse.gov/omb/memoranda/m03-22.html

4.4. 費用対便益の考察

ほかの資本購入と同様に、電子認証の実装にあたっては費用と便益を考慮する必要があり、そのため『資本計画ガイド（Capital Programming Guide）』[9] によって費用便益分析が要求される。また、必要な保証レベルを、費用および選択したソリューションの業務、ポリシーおよび技術的要件の負担と釣り合うようにすることも重要である。

一般に含まれる便益：

- トランザクション速度の向上
- パートナー参加の増加および顧客満足の向上
- 記録維持の効率性改善およびデータ分析の機会
- 職員の生産性向上および最終成果物の品質向上
- 国民に対する情報にかかわるより大きな便益
- セキュリティの向上
- 機密性が高い情報に対する広範なセキュリティ

一般に含まれる費用：

- アプリケーション設計のための初期投資
- 技術の調達
- テスト
- 機能実装の配備
- 長期の保守

場合によっては初期投資が小さく、長期の保守費用が高いことがある。したがって、システムのライフサイクル全体に渡って費用を評価することが重要である。認証エラーは、政府機関および国民にとって大きな費用となることがある。これらの費用は、セクション2に規定したリスク分析によって明らかになり、どのような費用便益分析にも含めるべきである。

負担は、次の2つの要素で構成される。

a) 連邦政府に属さない主体に課される費用
b) 費用見積もりでは捉えられないが、技術ソリューションによって各主体に課される時間的要求

負担が過多のシステムは、非連邦政府の主体によるシステムの使用に影響し、期待された便益および投資回収率が減少する可能性がある。特定の保証レベルの技術ソリューションの費用または負担が大きすぎる場合、政府機関は要求保証レベルを引き下げて、同等の保証レベルを達成するために管理策の実施または業務プロセスの調整を行うことを検討すべきである。このようなリスク軽減の方法で費用を受容できるレベルまで引き下げられない場合、政府機関は、電子認証システムにかかわる構想を再考する必要があるかもしれない。

---

[9] OMB 覚書き A-11、Supplement, http://www.whitehouse.gov/omb/circulars/a11/cpgtoc.html

保証レベルが高いほど、クレデンシャルの費用も高くなる可能性がある。クレデンシャルの数を最低限にすることで費用を削減できる。リスクアセスメント、費用および便益の評価に関する追加情報については、GPEAガイダンスのセクション3を参照されたい。電子認証の技術ガイダンスでは、保証レベルに対応するためのさまざまな代替方法を提示しており、認証の費用を各政府機関が抑えるのに役立つ可能性がある。

5. ガイダンスの発効日

政府機関は、ユーザ認証を必要とするすべての既存のトランザクションおよびシステムを、2005年9月15日までに、記述されている保証レベルのいずれかに分類しなければならない。政府機関は、これを次の順番で行うべきである。

- 「主要（major）」と分類されたシステムは、2004年12月15日までに完成させなければならない。
- 新規の認証システムは、システム設計の一環として、NISTが発行する最終的な電子認証技術ガイダンスが完成してから90日以内に分類を始めるべきである。

選択された保証レベルは、政府機関のWebサイト、官報、その他の手段（たとえば、要求に応じて）を通じて一般に入手可能になっていなければならない。政府機関のアプリケーションの保証レベルは、電子認証構想に従い、国民がアクセスできる中心的な場所に掲載される。

2004年より、政府機関は電子政府法の第202(g)条によって義務付けられているOMBへの年次の電子政府活動報告（E-Government Act Reports）に、本ガイダンスの実装の進捗を報告することを求められる。

別添B

パブリックコメントとそれらに対する対応の概要

2003年7月11日に、一般調達局は行政管理予算局OMBと連携して「連邦政府機関のための電子認証政策案（Draft E-Authentication Policy for Federal Agencies）」を、官報通達[68 FR 41370]に掲載した。

ガイダンスの案に対して、連邦政府機関、技術ベンダ、その他の組織を代表する47件のコメントが寄せられた。最終的なOMBガイダンスの策定にあたっては、すべてのコメントを考慮した。ガイダンスへのコメントは、電子的なトランザクションを実装するときに政府横断的な電子認証のガイダンスに各政府機関が従うこと、またリスクアセスメントを実施することを義務付ける要件の確立に寄与した。以下の段落は、コメントおよびわれわれの対応の全般的なグループ分けをまとめたものである。

<u>コメントと対応</u>

コメントは、次の3つに分類できた:1. 認証ガイダンスの必要性、費用および考え方に対する全般的なコメント、2. ドキュメントの特定セクションに限定したコメント、および 3. 編集または書式にかかわるコメント。全体として、約1/3のコメントが取り込まれ、大幅な改訂および再編成となった。

コメントの半分はセクション2「保証レベルおよびリスクアセスメント」に関するもので、ガイダンスの明確化を求めるものが中心だった。ガイダンス全体が大幅に改訂されたが、もっとも改訂が大きかったのは本セクションである。改訂の内容としては、保証レベルの説明の改善およびあいまいな命名規則の排除、適切な保証レベルを判断するための方法の明確化のほか、認証エラーに対する潜在的な影響、および事例の正確性の確保が含まれる。適用範囲のセクションを改善し、混乱しやすい用語を定義し、一貫性を向上するためにガイダンスの見直しを行った。また、最近発行されたNISTの標準（FIPS 199）および該当する法に合わせてガイダンスを改訂しました。さらに、法的正確性の確保のためにもガイダンスに改訂を加えた。