jNOTARY BusinessCA

ＴＡＡ証明書ポリシ

Version 1.0

株式会社　日本電子公証機構

改訂履歴

Version	日付	変更内容
1.0	2012.4.1	初版作成

目次

1 はじめに

1.1 概要

jNOTARY BusinessCA TAA 証明書ポリシ（Certificate Policy:以下、「本 CP」という）は、株式会社日本電子公証機構（以下、「jNOTARY」という）が運用する jNOTARY BusinessCA(以下、「本 CA」という)にて発行する TAA(TimeAssessmentAuthority)用証明書（以下、「証明書」という）の利用目的、適用範囲、申請者手続きを示し、証明書に関するポリシを規定するものである。なお本 CA の運用維持に関する諸手続については jNOTARY BusinessCA 運用規定（Certification PracteiceStatement:以下、「CPS」という）に規定する。

jNOTARY は、認証局として本 CA の鍵管理、申請者に対する証明書発行、失効等の認証サービス（以下、「本サービス」という）を提供する。

1.2 文書の名前と識別

本 CP の正式名称は「jNOTARY BusinessCA TAA 証明書ポリシ」という。
本 CP の識別子（OID）は 0 2 440 200148 2 2 5 です。本 CP は証明書にも公開されている場所が記載される。

1.3 コミュニティと適応可能性

1.3.1 本 CP の適用範囲

本 CP は、本 CA により実施される証明書発行及び失効業務に適用されます。本 CA より発行される証明書には、全て本 CP が適用される。

1.3.2 認証局(CA)

本 CA は、登録局（以下、「RA」という）と発行局（以下、「IA」という）から構成され、jNOTARY により運用される。証明書の発行、失効、失効情報の開示および保管等の統制、管理を行う。

1.3.3 発行局(IA)

本 CA において発行は IA によって行われる。IA は本 CPS に従い証明書の発行処理、失効処理および失効リスト（以下、「CRL」という）の発行処理を行う。

1.3.4 登録局(RA)

本 CA において登録は RA によって行われる。RA は証明書申請者となる個人、組織、団体からの証明書発行、失効等の要求に対して実在性の確認、本人性確認、運用規定の審査

等を行う。

1.3.5 申請者

申請者とは、自ら鍵ペアを生成し、本 CA からの証明書の発行を受ける組織または団体の代表者（または代表権を有するもの）をいう。

1.3.6 申請担当者

申請担当者とは、申請者から任命、委任または委託を受けたものであり、jNOTARY との窓口になる担当者をいう。

1.3.7 利用者

利用者とは、本 CA が発行した証明書を信頼して利用する者をいう。

1.4 証明書の使用方法

利用者は当該証明書の信頼性を本 CA の証明書によって検証することができる。

1.5 ポリシ管理

1.5.1 CP を管理する組織

本 CP の維持・管理は、jNOTARY が行う。

1.5.2 連絡先

本 CP に関する問い合わせは、電話、FAX、電子メールにて問い合わせを受け付けます。

[問い合わせ先]

窓口：株式会社日本電子公証機構　jNOTARY BusinessCA サービス窓口

住所：〒130-0013　東京都墨田区錦糸二丁目 14 番地 6 号　エニイビル

営業日：月曜から金曜日（祝日と年末年始の 12 月 30 日～1 月 5 日を除く）

受付時間：午前 10 時から午後 5 時

電話：03-5819-3871

電子メール：info@jnotary.com

1.5.3 CP 承認手続

本 CP は、jNOTARY の認証局検討委員会による承認のもと、作成および変更がなされ、リポジトリに公開される。

2．公表とリポジトリの責任

2.1 リポジトリ

CPS に規定する。

2.2 証明書情報の公開

CPS に規定する。

2.3 公開の時期および頻度

CPS に規定する。

2.4 リポジトリへのアクセスコントロール

CPS に規定する。

3．識別と確認

3.1 名前

3.1.1 名前の種類

証明書の発行者の名前と発行対象である申請者の名前は、X.500 の識別名（DN:Distinguished Name）形式に従い設定する。

3.1.2 意味のある名前の必要性

申請者の識別は、意味のある名前を用いる。証明書に記載される主体者名は、組織または団体に適切な範囲で関連したものでなければならない。

3.1.3 申請者の匿名性または仮名性

証明書に記載される主体者名に匿名や仮名は使用しない。

3.1.4 名前の一意性

証明書に記載される主体者名は、本 CA の発行した全ての証明書において一意とする。

3.1.5 認識、認証および商標の役割

商標使用の権利については、商標保持者に留保されるものとるす。本 CA は、必要に応じて、商標保持者に対して、商標に関する出願等の公的書類の提出を求めることがある。

3.2 新規の識別と認証

3.2.1 秘密鍵の所有を証明する方法

本 CA は、申請担当者から提出された証明書発行要求（Certficate Signing Request:以下、「CSR」という）の署名の検証を行い、それに含まれている公開鍵に対する秘密鍵で署名されていることを確認する。また、CSR のフィンガープリントを確認し、公開鍵の所有者を特定する。

3.2.2 組織または団体の認証

申請担当者は、証明書の発行申請時に、本 CA に以下の情報を提出しなければならない。

ａ．ビジネス CA TAA 証明書発行申込書
ｂ．証明書発行申込書に押印した会社代表印の印鑑登録証明書
ｃ．履歴事項全部証明書（商業登記簿謄本）
ｄ．CSR

本 CA は、以上の情報を用いて申請に誤りや欠落情報がないことを確認する。
ｂとｃに関しては、発行日から３ヶ月以内のものであること。

3.2.3 個人の認証

本 CA は、個人に対して証明書の発行は行わない。

3.2.4 申請担当者の権限の正当性確認

本 CA は、申請者となる組織または団体の申請担当者が、その組織または団体に関する情報の申請を行うための正当な権限を有していることを確認する。

3.3 更新申請時の識別と認証

3.3.1 通常の秘密鍵更新に伴う証明書申請時の識別と認証

本 CP「3.2 新規の識別と認証」と同様の手続による。

3.3.2 証明書失効後の秘密鍵更新に伴う証明書申請時の識別と認証

本 CP「3.2 新規の識別と認証」と同様の手続による。

3.4 失効請求時の識別と認証

本 CA は、証明書の取消申請を受け付けた場合、提出された申請者の情報をもとに、適正な要求であることを確認する。

4．証明書の運用要件

4.1 証明書発行申請

4.1.1 証明書発行申請を行うことができる者

証明書の発行申請は、発行申請を行う組織または団体の申請担当者が行うことができる。

4.1.2 登録手続および責任

申請担当者は、本 CA より事前に周知された手続きに従い、証明書の申請を行う。

申請担当者は、証明書の発行申請を行うにあたり、本 CP、CPS、その他本 CA より開示された文書の内容を承諾しているものとする。

申請担当者は､本 CA に対する申請内容が正確な情報であることを保証しなければならない。

4.2 証明書発行申請手続

4.2.1 識別と認証の手続

本 CA は､申請担当者からの発行申請に対し､受領した申請書類および CSR の真正性を、「3.2 新規の識別と認証」に基づき確認する。

4.2.2 証明書発行申請書の受理または却下

本 CA は、申請担当者からの申請に対し予め定められた審査手続きに従い、証明書の発行申請の諾否を決定し、その結果を申請担当者に通知する。

4.2.3 証明書発行申請の処理時間

本 CA は、申請担当者からの発行申請を承諾した場合、速やかに証明書を発行する。

4.3 証明書発行

4.3.1 証明書の発行時における CA の処理手順

本 CA は、申請担当者から提出された CSR の公開鍵に対し、本 CP「7.1 証明書プロファイル」に準じた内容で、本 CA の秘密鍵を用いて署名を付した証明書を発行する。

4.3.2 申請者に対する証明書発行通知

本 CA は、受け付けた申請に対する証明書の発行が完了した後、発行した証明書をフロッピーディスク等の外部記憶媒体に保管し、受領書とともに封緘したうえで、申請担当者と

の間で手交するかまたは郵送により申請担当者宛に送付する。

4.4 証明書の受領

4.4.1 証明書の受領確認手順

申請担当者は、証明書の内容を確認し、問題が無いと判断した時点で、本 CA に対して受領書を送付しなければならない。本 CA は、受領書を受領した時点で証明書の受け入れの完了とする。なお、証明書の内容に誤りがあった場合、申請担当者は遅滞無くその旨を本 CA に連絡しなければならない。

4.4.2 他のエンティティに対する CA の証明書発行通知

本 CA は、他のエンティティに対して証明書の発行通知を行わない。

4.5 鍵ペアと証明書の用途

4.5.1 申請者の秘密鍵および証明書の用途

本 CA が発行する証明書および申請者が所持する秘密鍵の用途は、jNOTARY が提供しているサービスや、jNOTARY と契約関係にかる本 CA の申請者が提供しているサービスまたは製品に定めている用途に制限されている。本 CA が発行する証明書を、その他の用途に使用してはならない。

4.5.2 利用者の公開鍵および証明書の用途

利用者は、本 CP および CPS の内容について理解し、承諾した上で本 CA の証明書を使用し、本 CA が発行した証明書の信頼性を検証しなければならない。

4.6 証明書の更新

本 CA は、申請者の鍵ペアの更新を伴わない証明書更新を認めない。証明書を更新する場合、新たな鍵ペアを生成することとし、本 CP「4.7 鍵更新を伴う証明書の更新」に定める手続に従う。

4.7 鍵更新を伴う証明書の更新

4.7.1 鍵更新を伴う証明書の更新理由

更新を伴う証明書の更新は、証明書の有効期間が満了する場合または鍵の危殆化に伴い証明書の失効を行った場合に行われる。

4.7.2 新しい公開鍵の証明書申請を行うことができるもの

本 CP「4.1.1 証明書発行申請を行うことができる者」と同様とする。

4.7.3 鍵更新を伴う証明書更新申請の処理手続

本 CP「4.2 証明書発行申請手続」と同様とする。

4.7.4 申請者に対する新しい証明書の通知

本 CP「4.3.2 申請者に対する証明書発行通知」と同様とする。

4.7.5 鍵更新に伴い発行された証明書の受領確認手続

本 CP「4.4.1 証明書の受領確認手続」と同様とする。

4.7.6 他のエンティティに対する CA の証明書発行通知

本 CP「4.4.2 他のエンティティに対する CA の証明書発行通知」と同様とする。

4.8 証明書の変更

4.8.1 証明書を変更する場合

証明書の記載事項に変更が生じた場合、申請者は本 CA に対して速やかに変更に関する申請を行わなければならない。変更に伴う証明書の再発行手続は、証明書の失効および新規発行時の手続を持って行われる。

4.8.2 証明書の変更申請をすることができる者

本 CP「4.9.2 証明書失効申請することができる者」および「4.1.1 証明書発行申請を行うことができる者」と同様とする。

4.8.3 証明書の変更申請の手続処理

本 CP「4.9.3 失効申請手続」および「4.2 証明書発行申請手続」と同様とする。

4.8.4 申請者に対する新しい証明書の発行通知

本 CP「4.3.2 申請者に対する証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認手続

本 CP「4.4.1 証明書の受領確認手続」と同様とする。

4.9 証明書の失効および一時停止

4.9.1 証明書失効事由

申請担当者は、自らの判断に基づいて証明書の失効申請を行うことができる。ただし、次の事由が発生した場合、申請担当者は本 CA の証明書の失効申請を行わなければならない。

・証明書記載事項に変更があった場合
・秘密鍵が盗難、紛失、漏洩、不正利用等のより証明書の信頼性を喪失した可能性がある場合
・秘密鍵が危殆化し機密性が失われた場合またはその可能性がある場合
・証明書の内容、利用目的が正しくない場合
・証明書の利用を中止する場合

また、本 CA は、次の事由に該当すると判断した場合、申請担当者からの失効の有無に関わらず、証明書の失効ができるものとする。

・申請者が本 CP および CPS、契約、法律に基づく義務を履行していない場合
・jNOTARY が本サービスを終了する場合
・本 CA の秘密鍵が危殆化したまたはその恐れがあると判断された場合
・本 CA が失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効申請することができる者

証明書の失効申請は、失効申請を行う組織または団体の申請担当者が行うことができる。

4.9.3 失効申請手続

証明書の失効申請手続は、本 CA に対して証明書失効の関する必要な情報を郵送することで行われる。ただし、緊急を要する場合や上記の方法による要求ができな場合、代替策として、電子メールによる申請も可能である。

4.9.4 失効申請の猶予期間

秘密鍵が危殆化した場合を除く失効申請は、失効を希望する１０営業日前までに、本 CA に行わなければならない。ただし、秘密鍵が危殆化またはそのおそれがある場合は、当該問題を発見後、速やかに失効申請を行わなければならない。

4.9.5 CA の失効申請処理の許容時間

本 CA は、有効な失効申請を受け付けてから２営業日以内に証明書の失効を実行する。

4.9.6 利用者の失効確認要求

利用者は、本 CA により発行された証明書を信頼し、利用する前に、CRL を確認するこ

とにより証明書が失効されていないことを確認しなければならない。

4.9.7 証明書失効リストの発行頻度

CRL は、１日１回新たな CRL が発行される。

4.9.8 証明書失効リストの発行の最大遅延時間

CRL は、証明書の発行および失効を行ってから、１営業日以内の新たな CRL を発行し、リポジトリに公開する。

また、本 CA は CRL とともに失効理由を示す情報をリポジトリに公開する。

4.9.9 証明書の一時停止

本 CA は、証明書の一時停止を行わない。

5．物理的、手続き的、要員的なセキュリティ管理

5.1 物理的管理

CPS に規定する。

5.2 手続上の管理

CPS に規定する。

5.3 人事上のセキュリティ管理

CPS に規定する。

5.4 セキュリティ監査の手順

CPS に規定する。

5.5 記録の保管

CPS に規定する。

5.6 鍵の切り換え

CPS に規定する。

5.7 信頼性喪失や災害からの復旧

CPS に規定する。

5.8 認証業務の終了

CPS に規定する。

6．技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

CPS に規定する。

6.2 CA 秘密鍵の保護

CPS に規定する。

6.3 鍵ペア管理のその他の側面

CPS に規定する。

6.4 コンピュータのセキュリティ管理

CPS に規定する。

6.5 セキュリティ技術のライフサイクル管理

CPS に規定する。

6.6 ネットワークセキュリティ管理

CPS に規定する。

7．証明書と CRL のプロファイル

7.1 証明書のプロファイル

本 CA が発行する証明書が、X.509 フォーマット証明書形式により作成される。
表「7-1 基本証明書領域」に示すフィールドを用いる。

表「7-1 基本証明書領域」

フィールド	説明
Version（バージョン番号）	証明書フォーマットのバージョン番号
SerialNumber（シリアル番号）	CA 内で一意の番号
Signature（署名アルゴリズム）	本サービスで用いられる電子署名のアルゴリズム
Issuer（発行者名）	発行者情報（jNOTARY の情報）
Validity（有効期間）	証明書有効期間の開始と終了*1
Subject（申請者名）	申請者情報
SubjectPublicKeyInfo（申請者公開鍵情報）	申請者の公開鍵情報と公開鍵データ
Extensions（拡張領域）	証明書拡張領域

*1 有効期間は 6 年 1 ヶ月

7.1.1 バージョン番号

本 CA が発行する証明書の X.509 フォーマットのバージョン番号は、Version3 である。

7.1.2 証明書拡張領域

本 CA が発行する証明書は、X.509 証明書拡張フィールドを使用する。
表「7-2 証明書拡張領域」に示すフィールドを用いる。

表「7-2 証明書拡張領域」

フィールド	説明
authorityKeyIdentifier（機関キー識別子）	CA の公開鍵のハッシュ値
subjectKeyIdentifier（サブジェクトキー識別子）	申請書の公開鍵のハッシュ値
keyUsage（キー使用法）	鍵の用途
CertificatePolicies（認証ポリシ）	OID および CPS の URL
CRLDistributionPoint	CRL の配布場所

7.1.3 名前の形式

本 CA が発行する各種の証明書に含まれる識別名には、ITU-T X.500 識別名 DN が用いられます。

7.1.4 名前の制約

証明書の記述に使用する言語は英語です。本 CA の名称、申請者の属性も英語（ローマ字等）で表記されます。

7.2 CRL プロファイル

本 CA が発行する CRL は、X.509CRL フォーマット形式で作成される。
表「7-3 CRL 基本領域」に示すフィールドを用いる。

7-3 CRL 基本領域

フィールド	説明
Version（バージョン番号）	CRL フォーマットのバージョン番号
Signature（署名アルゴリズム）	本サービスで用いられる電子署名のアルゴリズム
Issuer（発行者名）	CRL 発行者情報（jNOTARY の情報）
ThisUpdate（更新日）	CRL 発行日時
NextUpdate（次回更新予定日）	CRL の次回更新予定日時
RevokedCertificates（失効リスト）	失効となった証明書の情報

7.2.1 バージョン番号

本 CA は、ITU-T Recommendation X.509 バーション２である。

7.2.2 CRL 拡張

本 CA が発行する X.509CRL 拡張フィールドを使用する。
表「7-4 CRL 拡張」に示すフィールドを用いる。

7-4 CRL 拡張

フィールド	説明
AuthorityKeyIdentifier（機関キー識別子）	CA 公開鍵のハッシュ値
CRL Number	CRL 発行番号

8．準拠性監査

8.1 監査の頻度

CPS に規定する。

8.2 監査の身分と資格

CPS に規定する。

8.3 監査人と被監査対象との関係

CPS に規定する。

8.4 監査対象

CPS に規定する。

8.5 監査指摘事項への対応

CPS に規定する。

8.6 監査結果の報告

CPS に規定する。

9 他の業務上および法的問題

9.1 料金

料金体系については、別途定める。

9.2 財務的責任

jNOTARY は、本サービスの提供にあたり、十分な財務的基盤を維持するものとする。

9.3 機密保持

9.3.1 機密情報の範囲

本 CA が保持する個人および組織の情報は、証明書、本 CP および CPS の一部として明示的に公表されたものを除き、機密保持対象として扱われる。jNOTARY は、法の定めている場合および申請者による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。

9.3.2 機密情報保持対象外の情報

証明書および CRL に含まれる情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持の対象外とする。

・jNOTARY の過失によらず知られた、あるいは知られるようになった情報
・jNOTARY 以外の出所から、機密保持の制限無しに jNOTARY に知られた、あるいは知られるようになった情報
・jNOTARY によって独自に開発された情報
・開示に関して申請者のよって承認されている情報

9.3.3 機密情報の保護責任

本 CA が保持する機密情報を、法の定めによる場合および申請者による事前の承諾を得た場合に開示することがある。その際、その情報を知りえたものは、契約あるいは法的な制約によりその情報を第三者に開示することはできない。

9.4 個人情報の保護

本 CA が取得する個人情報は、本 CP「9.3 機密保持」のとおり機密情報として取り扱う。また、本 CA は、個人情報に関する法律または関連する法令および jNOTARY が一般に公開している個人情報保護方針を遵守する。

9.5 知的財産権

jNOTARY と申請者間で別段の合意がされない限り、本サービスにかかわる情報資料および情報データは、次に示す当事者の権利に属するものとする。

申請者証明書　　: jNOTARY に帰属する財産である。
CRL　　: jNOTARY に帰属する財産である。
申請者の秘密鍵　　: 秘密鍵は、公開鍵と対になる秘密鍵を所有する申請者に帰属する財産である。
申請者の公開鍵　　: 公開鍵は、対になる秘密鍵を所有する申請者に帰属する財産である。
本 CP および CPS　: jNOTARY に帰属する財産である。

9.6 表明保証

9.6.1 CA の表明保証

jNOTARY は、本 CP および CPS の規定した内容を遵守して申請者に関する審査、証明書の登録、発行、失効を含む認証サービスを提供し、CA 秘密鍵の信頼性を含む認証業務の信頼性を確保する。

本 CP および CPS に規定された保証を除き、jNOTARY は、明示的あるいは暗示的に、もしくはその他の方法を問わず、一切の保証を行わない。

9.6.2 申請者の表明保証

本 CA の申請者は、以下の義務を負う。

・本 CA に、真性者が把握できる範囲で正確かつ完全な情報を提供する。当該情報に変更があった場合は、その旨を速やかに本 CA に通知する。
・危殆化から自身の秘密鍵を保護する。
・証明書の使途は本 CP および CPS に従うものとする。
・申請者が、証明書に記載の公開鍵に対応する秘密鍵が危殆化した、またはそのおそれがあると判断した場合や、登録情報に変更があった場合、申請者は本 CA に証明書の失効を速やかに要求すること。
・申請担当者が異動、退職等で変更になる場合は、新しい申請担当者を本 CA に速やかに連絡しなければならない。

9.6.3 利用者の表明保証

本 CA のサービス利用者は、以下の義務を負う。

・本 CA が発行する証明書を信頼し、本 CP および CPS に規定されている本 CA が意図する目的のみに証明書を使用すること。

・証明書を信頼しようとするときは、リポジトリ内の CRL に含まれる失効情報を取得して、証明書が失効していないことを確認する。
・証明書を信頼しようとするときは、当該証明書の有効期間を確認し、有効期間内であることを確認すること。
・本 CA が発行した証明書を信頼しようとするときは、当該証明書が本 CA の証明書によって署名検証できることを確認すること。
・本 CA の証明書を信頼して利用する際、本 CP および CPS の規定されている利用者として責任を負うことに合意すること。

9.7 保証の制限

jNOTARY は、本 CP「9.6.1 CA の表現保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害または派生的損害に対する責任を負わず、また、いかなる逸失利益、データ紛失またはその他の間接的もしくは派生的損害に対する責任を負わない。

9.8 責任の制限

本 CP「9.6.1 CA の表明保証」の内容に関し、次の場合、jNOTARY は責任を負わないものとする。

・jNOTARY に起因しない不正使用ならびに過失等により発生する一切の損害
・申請者または利用者が自己の義務の履行を怠ったために生じた損害
・申請者または利用者のシステムに起因して発生した一切の損害
・jNOTARY、申請者または利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
・申請者が契約に基づく契約料金を払っていない間に生じた損害
・jNOTARY の責に帰することのできない事由で証明書および CRL の公開された情報に起因する損害
・jNOTARY の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
・証明書の使用に関して発生する取引上の債務等、一切の損害
・現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
・天変地異、地震、噴火、火災、津波、水害、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止を含む業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、申請者および利用者には、jNOTARY および関連する組織等に対する損害賠償責任および保護責任が発生する。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅延、不履行のうち、証明書申請時に申請者が本 CA に最新かつ正確な情報を提供しなかったことに起因するもの、または各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような申請者および利用者のミス、怠慢な行為、各種行為、履行遅延、不履行等の各種責任が含まれる。

9.10 改訂

9.10.1 改訂手続

jNOTARY は、本 CP の内容変更に際して、変更した CP をリポジトリ上に掲載することにより、申請者および利用者に対して変更の告知を行う。

9.10.2 通知方法および期間

本 CP を変更した場合、速やかに変更した本 CP をリポジトリに掲載することにより、申請者および利用者に対しての告知とする。

9.11 紛争解決手段

本 CA のサービスの利用に関して、jNOTARY に対して訴訟、仲裁を含む法的またはその他の解決手段に訴えようとする場合、jNOTARY に対して事前にその旨を通知するものとする。

9.12 準拠法

本 CA、申請者および利用者の所在地にかかわらず、本 CP および CPS の解釈、有効性および本サービスにかかわる紛争については、日本国の法律が適用される。

9.13 雑則

9.13.1 完全合意条件

jNOTARY は、本サービスの提供にあたり、自らのポリシおよび保証ならびに申請者または利用者の義務等を本 CP、CPS および契約によって包括的に定め、これ以外の口頭であろうと書面であろうとを問わず、いかなる合意も効力を有しないものとする。