依拠当事者規約 ー Key Manager

依拠当事者規約は、Symantec Corporation（注）（以下「シマンテック」といいます）の Symantec Managed PKI Key Manager（以下「キーマネージャー」といいます）を利用して発行された Digital ID（以下「証明書」といいます）の使用を規律するものです。証明書はこの依拠当事者規約（以下「本規約」といいます）の URL（https://www.symantec.com/about/profile/policies/repository.jsp）を指し示すことによる引用と証明書の使用は当該 URL の条件に従うことを記述する項目を含みます。

（注）「Symantec Corporation」は、米国デラウェア州法人であり、アメリカ合衆国 94043 カリフォルニア州マウンテンビュー、エリスストリート（350 Ellis Street, Mountain View, California）に主たる事業所を有する Symantec Corporation 及びその完全子会社（株式会社シマンテックを含む）を意味する。

お客様が証明書の有効性を検査されるとき、あるいは証明書をダウンロードし、又はそのステータスを検証する為に証明書の破棄及びその他情報についてのシマンテックのデータベース（以下「リポジトリ」といいます）にアクセス若しくは使用されるときには、必ずその前にこの依拠当事者規約をお読み下さい。お客様がこの依拠当事者規約の条件に合意されない場合には、お客様は証明書に依拠すること、あるいは証明書をダウンロードし、又はそのステータスを検討する為にシマンテックのリポジトリを使用することはできません。

本規約は、お客様が証明書の調査若しくは証明書に含まれる公開鍵に対応する秘密鍵により生成されたデジタル署名を検証する照会を提出した時、又はお客様がシマンテックのリポジトリ若しくは証明書に関連するウェブサイトで提供される情報若しくはサービスをその他の目的で使用し若しくはそれに依拠した時に効力を生じます。

証明書を発行する発行機関（以下「IA」といいます）は、キーマネージャーを利用して加入者の為にその秘密鍵を生成し、当該秘密鍵のバックアップを行います。従って、IA は加入者が秘密鍵のアクセスを喪失する事態が発生した際に、当該加入者の秘密鍵を回復することが出来ます。尚、IA は合法的な業務上の理由がある場合、当該加入者の許可を得ることなく加入者の秘密鍵を回復することが有り得ます。当然、発行機関は、お客様あるいはその他の方が加入者に送付した暗号化メッセージを復号することが可能となります。お客様が加入者に送付する暗号メッセージに対するプライバシーを期待される場合には、このことを念頭において頂かなければなりません。キーマネージャーが適切に導入されると、キーマネージャーにより実現されるシマンテックの鍵回復サービスはかなりの利益をお客様に提供します。一方、仮にキーマネージャーの管理機能が不正に使用された場合、発行機関は、お客様が加入者に送られたメッセージが手元にあればそれを解

読することも出来ます。又、デジタル署名及び暗号に対してシングル鍵ペアーが導入される場合、発行機関は、回復された秘密鍵を利用して加入者に成り代わってお客様あるいはその他の方に送るメッセージにデジタル署名を付すことも出来ます。お客様は本規約の以下の規定をご了承することにより、上記についてもご承知頂くことになります。

お客様は、お客様がどの程度証明書の中の情報に依拠することを選択するかに関して決定できるための、十分な情報へのアクセスを有していることを認められるものとします。より詳細に解説する資料として、シマンテックのリポジトリ（https://www.symantec.com/about/profile/policies/repository.jsp）をご覧ください。お客様は、お客様の責任において証明書に含まれる情報に依拠するかどうかを決定されるものとします。お客様は、シマンテックリポジトリの使用及び証明書への依拠は、シマンテックの Certification Practice Statement（以下「CPS」といいます）（改正されたものを含みます）によって規律され、同 CPS は、引用により本規約に組み込まれることを認め、合意されるものとします。CPS は、インターネット上でリポジトリ https://www.symantec.com/about/profile/policies/repository.jsp において公表されています。また CPS の修正も、シマンテックのリポジトリ https://www.symantec.com/about/profile/policies/repository.jsp に掲載されています。証明書の有効性を検査しデジタル署名を検証するに必要な方法は、CPS の第 8 節に含まれています。

本規約において、加入者とは、シマンテックの証明書の対象でありかつそれを発行された人を意味するものとします。

お客様が加入者であり、シマンテックが NetSure® Protection Plan（https://www.symantec.com/about/profile/policies/repository.jsp）により保護されている証明書をお客様に発行した場合には、第 1 条ないし第 4 条（下記参照）の制限的保証、保証の否認、及び責任の制限は適用されず、かかる証明書については NetSure® Protection Plan の制限的保証、保証の否認及び責任制限が適用されます。デモ用、無料、及びテスト用証明書は、NetSure® Protection Plan で保護されません。より詳しい情報につきましては、NetSure® Protection Plan をご覧下さい。

お客様が NetSure® Protection Plan で保護される加入者でない場合には、下記の第 1 条ないし第 4 条がお客様に適用されます。

第 1 条

CPS の § 9.6.1 は、制限的保証について規定しています。CPS の § 9.6.1 に明示的に規定される場合を除き、発行機関及びシマンテックは、商品性の保証、特定目的への適合性の保証、及び提供

する情報の正確性の保証を含むあらゆる種類の保証及び義務から免責され、さらに過失又は相当な注意を払わなかったことから生ずるあらゆる責任からも免責されます。

第 2 条

いかなる場合も、発行機関又はシマンテックは、いかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任も負わず、また、いかなる逸失利益、データの損失、又は証明書、デジタル署名、若しくは本規約で提供され若しくは目的とされるトランザクション若しくはサービスの使用、配信、ライセンス、履行、不履行、若しくは利用不可能から生じ若しくはそれに関連する他の間接、付随的若しくは懲罰的損害についても責任を負わないものとします。このことは、当該発行機関若しくはシマンテックの何れか又はその双方が当該損害の可能性を知っていた場合でも同様です。

第 3 条

お客様を含めて全ての当事者に対する発行機関及びシマンテックの責任の総額は、下記の表に記載される当該証明書について適用される賠償額の上限を超えないものとします。

第 4 条

特定の証明書に関する全ての当事者に対する全ての発行機関及びシマンテックの責任の総額は、当該証明書に関連するあらゆるデジタル署名及びトランザクションの総額について、下記の額を超えない額に限定されるものとします。

	責任の上限
クラス 1	100 米ドル
クラス 2	5,000 米ドル
クラス 3	100,000 米ドル

本規約中の規定又はその適用について、その理由を問わずまたその程度を問わず無効又は強制不可能であると認められた場合、本規約の残りの規定（無効又は強制不可能な規定の他の人又は状況への適用）は、無効又は強制不可能であることにより影響されないものとし、当事者の意図を合理的に実行する方法で解釈されるものとします。

お客様は、本規約により、証明書に含まれる公開鍵に対応する秘密鍵の盗難又は他の形式での

危殆化の可能性があることを、そして、盗難又は危殆化した鍵が文書へのデジタル署名の偽造に使用される可能性があることを知らされるものとします。秘密鍵保護に関する情報として、https://www.verisign.com/repository/PrivateKey_FAQ/index.html をご覧下さい。

お客様は、証明書の調査若しくは証明書の破棄状況を確認する照会を提出されることにより、又は他の目的で証明書に関するシマンテックのリポジトリ若しくはウェブサイトが提供する情報若しくはサービスを利用し若しくは依拠することにより、本規約の条件を知り、それを承諾されたことを示されたものとします。もし同意されないときには、照会を提出しないで下さい。