アマゾンレジストリサービス社、XN--ECKVDTC9D (.ポイント) ゾーンに対する DNS 運用規定

第 0.2 版

目次

1　はじめに

本文書「XN--ECKVDTC9D (.ポイント)ゾーンに対する DNSSEC 運用規定」（DPS）は、XN--ECKVDTC9D (.ポイント)ゾーンの DNSSEC 運用に関するアマゾンレジストリサービス社の方針および運用を説明するものである。

1.1　概要

DPS の目的は、アマゾンレジストリサービス社により管理される XN--ECKVDTC9D (.ポイント)ゾーンに対する DNSSEC に関連する運用情報を提供することである。本文書は IETF ドメイン名システム運用（DNSOP）ワーキンググループにより提案された DPS フレームワークに従う。

1.2　文書名および識別

XN--ECKVDTC9D (.ポイント)ゾーンに対する DNSSEC 運用規定（XN--ECKVDTC9D (.ポイント) DPS）
バージョン：0.2
利用可能日：ルートゾーン委任の日
発効日：ルートゾーン委任の日

1.3　コミュニティおよび適用性

XN--ECKVDTC9D (.ポイント) DNSSEC サービスに関する期待される役割および責任を伴う利害関係者を以下に説明する。

1.3.1　ゾーンマネージャ

アマゾンレジストリサービス社が XN--ECKVDTC9D (.ポイント)ゾーンマネージャである。

1.3.2　ゾーンアドミニストレータ

Neustar が XN--ECKVDTC9D (.ポイント)ゾーンアドミニストレータである。

1.3.3　サーバオペレータ

Neustar が唯一のサーバオペレータである。

1.3.4　レジストリ

アマゾンレジストリサービス社が XN--ECKVDTC9D (.ポイント)ドメイン名登録のレジストリオペレータである。DNS サービスの一部として、アマゾンレジストリサービス社は自社の登録機関に DNSSEC サービスを提供し、登録機関は自社の登録者にこれらのサービスを提供する。レジストリは ZSK および KSK キーの組み合わせを用いてゾーンにサインする。KSK キーの DS 記録（単数／複数）はルートゾーンにおいて登録され利用可能となるが、これはルートと XN--ECKVDTC9D (.ポイント)

レジストリ間の信頼関係を維持するため DNSSEC 対応レゾルバを有効化する。

1.3.5 登録機関

レジストリは XN--ECKVDTC9D (.ポイント)ドメイン名登録システムの登録機関にサービスを提供する。登録機関は自社の登録者に対するドメインを登録、維持するため、レジストリとの契約上の取引関係を有する。登録機関は XN--ECKVDTC9D (.ポイント)ゾーンにおける DS 記録を含むドメイン情報を設定する。

1.3.6 登録者

登録者は XN--ECKVDTC9D (.ポイント)登録機関を通してレジストリに登録された XN--ECKVDTC9D (.ポイント)ドメインの所有者である。登録者により選択された登録機関または DNS プロバイダは、登録ドメインに対する DS 記録を提供する責任を有する。レジストリへのこれらの記録の提出を通して、レジストリから登録者の権限サブゾーンへの信頼関係を確立することができる。

1.3.7 XN--ECKVDTC9D (.ポイント)ゾーンキーサイニングキーオペレータ

Neustar が XN--ECKVDTC9D (.ポイント)ゾーンキーサイニングキーオペレータである。Neustar は XN--ECKVDTC9D (.ポイント)ゾーンのキーサイニングキー（KSK）を作成し、KSK を使用し XN--ECKVDTC9D (.ポイント)キーセットにサインする責任を有する。またプライベートキーを確実に作成、保管し、KSK の公的な部分を分配する責任を有する。

1.3.8 ルートゾーンゾーンサイニングキーオペレータ

Neustar が XN--ECKVDTC9D (.ポイント)ゾーンサイニングキーオペレータである。Neustar は XN--ECKVDTC9D (.ポイント)ゾーンのゾーンサイニングキー（ZSK）を作成する機能を行い、ZSK を使用し XN--ECKVDTC9D (.ポイント)ゾーンファイルにサインする責任を有する。

1.3.9 リライングパーティー

リライングパーティーには、例えばゾーン内で名前をリゾルブするブラウザまたはホスト、DNS プロバイダ、ISP、DNSSEC プロトコルを使用して名前の確実なレゾリューションのために XN--ECKVDTC9D (.ポイント) DNSSEC サービスを使用またはそれに応答するあらゆるユーザーといった DNS レゾルバが含まれる。

1.4 仕様管理

1.4.1 仕様管理機関

XN--ECKVDTC9D (.ポイント) DPS のアドミニストレータはアマゾンレジストリサービス社である。

1.4.2 連絡先情報

アマゾンレジストリサービス社の代理の Neustar。アドレスは Reg-support@neustar.biz

1.4.3 仕様変更手順

DPS の内容は年 1 回または必要に応じてより頻繁に検討される。修正は既存の文書になされるか、新規文書として発行される。すべての修正は下記のレポジトリで利用可能となる。アマゾンレジストリサービス社は通知なしで修正を発行する権利を有する。

2 発行およびレポジトリ

2.1 DPS レポジトリ

DPS は NIC.XN--ECKVDTC9D (.ポイント)のアマゾンレジストリサービス社のウェブサイトにあるレポジトリで発行される。

2.2 キーサイニングキーの発行

KSK はルートゾーンで発行される。信頼関係は、信頼の頼みの綱としてのルートキーを使用することで得られる。

2.3 レポジトリへのアクセス制御

DPS は DPS レジストリへのアクセス、読み込みを行うすべての人々に対して公的に利用可能となっている。すべての変更要求は検討のためにアマゾンレジストリサービス社に提出されなければならない。DPS への承認されない変更を防止するために制御がなされている。

3 運用要件

3.1 ドメイン名の意味

ドメイン名は登録のために公的に利用可能となっている。特定の方針に違反する場合、レジストリが登録を削除または拒否する権利を有することがある。

3.2 子ゾーンに対する DNSSEC の有効化

XN--ECKVDTC9D (.ポイント)ゾーンから子ゾーンへの信頼関係は、子ゾーンのサイン済み DS 記録が XN--ECKVDTC9D (.ポイント)ゾーンで発行された時に確立される。信頼関係が確立された後、子ゾーンは有効化した DNSSEC となる。

3.3　子ゾーンマネージャの識別および認証

レジストリは子ゾーンマネージャと直接の関係を持たないため、子ゾーンマネージャを識別、認証しない。

3.4　委任署名者（DS）記録の登録

登録機関は自社の登録者の代理で DS 記録を含むドメイン登録データを設定、管理するためにレジストリに接続を行う。

3.5　プライベートキーの所有を証明する方法

レジストリは子権威ゾーンでプライベートキーの所有を立証しない。

3.6　DS 記録の削除

登録機関は登録機関が管理するドメインに対する DS 記録の削除をいつでも要求できる。登録機関からの有効な要求の受領後、レジストリはゾーンから DS を削除する。

4　設備、管理および運用制御

4.1　物理的制御

XN--ECKVDTC9D (.ポイント)レジストリは、ミッションクリティカルプラットフォームに期待される環境仕様のすべてを満たすまたは超えるデータセンター設備内に存在している。

4.1.1　立地および建設

XN--ECKVDTC9D (.ポイント)レジストリおよび DNSSEC サービスは、米国のバージニア州スターリングおよびノースカロライナ州シャーロットの複数の非常に豊富なデータセンターから運用される。設備の立地により、レジストリのすべての側面を効果的に運用し自然および人為的災害を防ぐために必要となる多様なネットワーク接続および適切なネットワーク能力がもたらされる。双方のデータセンターにおいて、暗号キーが FIPS 140-2 レベル 3 ハードウェアセキュリティモジュール（HSM）に保管される。

4.1.2　物理的アクセス

Neustar は最高レベルのセキュリティおよびサービス可用性を提供するために非常に安全なデータセンターから運用を行う。設備への物理的アクセスはしっかりと制御されている。物理的セキュリティメカニズムにはセキュリティガード、閉回路 TV 監視ビデオカメラおよび侵入検出システムが含まれる。NOC は年中無休ですべての所在地へのアクセスを監視している。

HSM へのアクセスには少なくとも 2 つのキー、アドミニストレータおよびセキュリティ監査者が必要となる。キーのバックアップは PIN エントリーデバイス（PED）キーに保管され、2 時間耐火暗証番号金庫にロックされる。

4.1.3 電源および空調

各データセンターはバックアップ発電機およびバッテリ電源を含む複数の電源で運用される。各設備は温度および湿度を制御するために複数の空調ユニットを有する。

4.1.4 浸水

アマゾンレジストリサービス社および Neustar は浸水によるシステムへの損傷の影響を最小化するために予防措置を取っている。

4.1.5 火災予防および防止

アマゾンレジストリサービス社および Neustar は火災またはその他損傷をもたらす炎もしくは煙への露出を防止、沈静化するために予防措置を取っている。すべてのシステムは自動鎮火システムにより保護されている。

4.1.6 媒体保管

媒体保管および取り扱い手順は Neustar のデータ保護方針により定められている。

4.1.7 廃棄物処理

Neustar 情報セキュリティ方針および手順には、感度に基づいた古い材料の適切な処理に対するガイドラインが含まれる。手順には Neustar 敷地内の特別にマーク付けされたごみ箱内の堆積した古い紙情報も関係している（シュレッダにかけられる）。さらに電子データは確実に削除またはクリアされ、媒体は物理的に破壊される。もはや必要とされないハードディスクおよびバックアップテープは消磁される。

4.1.8 現場外バックアップ

バックアップソフトウェアがすべての重要なシステムのバックアップのために設置、利用され、定期的にバックアップ媒体が現場外に回される。さらにすべての重要なシステムのバックアップが、Neustarバックアップ方針に従い年2回のバックアップリカバリ試験のために確立したプロセスに統合される。

4.2 手順制御

4.2.1 信任を得た役割

Neustar は DNSSEC 管理および運用において、限定数の信任を得た役割を有する。役割は以下の通りである。

キーアドミニストレータ

- キーおよび DS 記録の作成
- キーロールオーバーイベントの管理

セキュリティ監査者

- セキュリティ監査を監督する
- 規則／手順が守られていることを確かなものとする

DNSSEC 役員

- コミュニティ会議およびワークショップに参加する
- DNSSEC 技術のエキスパート
- Neustar と外部パーティー間のコーディネータ

4.2.2 タスクごとに必要となる人の数

キーサイニングセレモニーおよび HSM 有効化には最低 2 人のキーアドミニストレータと 1 人のセキュリティ監査者が必要となる。

4.2.3 各役割に対する識別および認証

公認の職員のみが、XN--ECKVDTC9D (.ポイント) DNSSEC システムがあるデータセンターへの物理的アクセスを得ることが認められている。システムへのアクセスは上記で識別された役割を有するメンバーのみに与えられる。

4.2.4 任務の分離を必要とするタスク

任務の分離を必要とするタスクにはキー作成、実施および除去が含まれる。

4.3 職員制御

4.3.1 資格、経験および許可要件

従業員のみをセクション 4.2.1 で説明されている DNSSEC の役割に割り当てることができる。経験および資格はケースバイケースで評価されるが、一般的に DNS 運用とセキュリティ関連技術の詳細な知識が必要とされる。

4.3.2 経歴確認手順

経歴確認には申込者の資格、職歴、身元照会先、教育的経歴、その他その地位の任務に関するデータの検討が含まれる。

4.3.3　訓練要件

職員には DNSSEC の運用および管理における継続的な訓練が提供される。訓練は XN--ECKVDTC9D (.ポイント)特有の規則、手順および関連技術を含むがこれに限定されない。職員は DNSSEC ワークショップおよび会議に積極的に参加する。

4.3.4　再訓練頻度および要件

再訓練は必要に応じて提供されケースバイケースで行われる。

4.3.5　ジョブローテーション頻度およびシーケンス

本文書では適用なし。

4.3.6　無許可行為への制裁

本文書では適用なし。

4.3.7　契約職員要件

本文書では適用なし。

4.3.8　職員に提供される文書

DNSSEC 関連活動に参加するすべての職員には、サービスを統率する運用手順、規則および方針を含む文書が提供される。

4.4　監査ロギング手順

4.4.1　記録されるイベントの種類

XN--ECKVDTC9D (.ポイント)レジストリは以下を含むイベント（誰が、何を、いつ）に関するすべての必要な情報をログする。

- DNSSEC サービスがあるデータセンターへのアクセス
- サーバおよび HSM へのアクセス
- ファイルおよびファイルシステムへの修正
- キー運用：
  - キー作成／削除およびキーのライフサイクルに関するその他イベント
  - DS 記録の作成およびルートゾーンへの提出

4.4.2 プロセスログの頻度

監査ログは XN--ECKVDTC9D (.ポイント) DNSSEC サービスの運用整合性を確かなものとするため定期的な間隔で監視される。異常イベントは DNSSEC セキュリティ監査者によるさらなる調査のためにフラグされる。

4.4.3 監査ログ情報の保有期間

レジストリログは少なくとも 3 カ月間オンラインで保持される。古いほうのログは最長 5 年間保管、アーカイブされる。

4.4.4 監査ログの保護

監査ログへのアクセスは、無許可閲覧、修正、削除またはその他改ざんからファイルを保護するため公認の職員のみに利用可能である。監査ログはプライベートキーの整合性を損なうために使用されうるいかなる情報も含まない。

4.4.5 監査ログバックアップ手順

監査ログはオフライン保管システムに事前に定められた間隔でバックアップされる。これらのアーカイブへのアクセスは公認の DNSSEC の職員によってのみ要求、閲覧できる。

4.4.6 監査収集システム

レジストリは重要なイベントの監査ログへのロギングを自動化するソフトウェアおよびアプリケーションを利用する。システムレベルロギングに従い、アプリケーションログが記録され保管される。

4.4.7 イベント起因問題に対する通知

本文書では適用なし。

4.4.8 脆弱性評価

脆弱性の自動および手動評価は部分的に監査ログの監視によりなされる。レジストリ職員も参加しコミュニティの他のメンバーとセキュリティ関連情報を共有する。

4.5 侵害および災害リカバリ

4.5.1 事故および侵害取り扱い手順

事故および侵害が検出された場合は、争点の範囲が決定される。キーが侵害された場合、緊急キーロールオーバーが直ちに開始される。レジストリは KSK および ZSK 双方に対して緊急ロールオーバー方針を有している。

4.5.2 破損した演算リソース、ソフトウェアおよび／またはデータ

レジストリはリソース、ソフトウェアおよび／またはデータ破損の場合に備えてバックアップシステムおよびフェイルオーバーサイトを有する。争点の性質により、レジストリリカバリ計画に従い適切なアクションが取られる。

4.5.3 エンティティのプライベートキーの侵害に関する手順

レジストリの KSK の侵害の場合、以下の手順が取られる。

- 新規 KSK を作成、有効化する、またはすでにレジストリゾーンにあるプレビュ KSK を有効化する。有効化の一部として、DNSKEY セットが再署名される。
- 侵害されたキーの DS 記録をルートゾーンの新規 DS 記録と交換する。
- 除去するのに十分安全となった後、すぐにレジストリのゾーンにおける侵害された KSK を取り消し、その後除去する。

レジストリの ZSK の侵害の場合、以下の手順が取られる。

- 新規 ZSK を作成、有効化する、またはすでにレジストリゾーンにあるプレビュ ZSK を有効化する。有効化の一部として、すべての署名が再署名される。
- 署名が期限切れとなった後、すぐにレジストリのゾーンから侵害された ZSK を除去する。

4.5.4 取引継続性および IT 災害リカバリ能力

レジストリは完全に運用可能なバックアップ／フェイルオーバーサイトを維持する。災害の場合、フェイルオーバー／バックアップサイトが DNSSEC 運用を引き継ぐ。

4.6 エンティティの終了

レジストリが終了した場合、レジストリの完全な協力を得て秩序だった変換が行われる。

5 技術的セキュリティ制御

5.1 キーペアの作成および設置

5.1.1 キーペアの作成

KSK および ZSK のキーペアが、年 1 回または必要に応じてより頻繁に生じるサイニングセレモニーの間に作成される。一般的に計画されたキーロールオーバーサイクルにより、数カ月の XN--ECKVDTC9D (.ポイント) DNSSEC サービス運用を認めるため、セレモニーの間に十分なキーペアが作成される。キー作成は FIPS 140-2 レベル 3 ハードウェアセキュリティモジュールにおいて公認の職員により行われる。

5.1.2 パブリックキーの配送

レジストリ KSK および ZSK により使用されるパブリックキーは、レジストリの DNSKEY リソース記録セット（RR セット）の一部として利用可能である。その他の手段により分配されることはない。

5.1.3 パブリックキーパラメータ作成および品質確認

パブリックキーの立証は定期的に行われる。

5.1.4 キー使用の目的

キーはレジストリのゾーンにおける署名作成のために使用され、その他の目的のために使用されることはない。

5.2 プライベートキーの保護および暗号モジュールエンジニアリング制御

5.2.1 暗号モジュール標準および制御

ZSK および KSK は FIPS 140-2 レベル 3 ハードウェアセキュリティモジュール内で作成、保管される。

5.2.2 プライベートキーの複数人による制御

キー作成の間、少なくとも 2 人の DNSSEC キーアドミニストレータの公認メンバーが存在していなければならない。

5.2.3 プライベートキーのエスクロー

XN--ECKVDTC9D (.ポイント)ゾーンのプライベートキーはエスクローされない。

5.2.4 プライベートキーのバックアップ

プライベートキーは FIPS140-2 準拠 PCMCIA カードでバックアップされ、現場外で 2 時間耐火暗証番

号金庫に保管される。

5.2.5　暗号モジュールでのプライベートキーの保管

本文書では適用なし。

5.2.6　アーカイバルプライベートキー

プライベートキーはフェイルオーバーの場合のバックアップサイトを除き保管目的でアーカイブされることはない。

5.2.7　暗号モジュールへ／からのプライベートキーの移動

HSM で作成された ZSK および KSK は暗号化された形式でバックアップサイトに移動される。

5.2.8　プライベートキーを有効化する方法

プライベートキーは、セキュリティ監査者の立ち会いのもと PIN をハードウェアセキュリティモジュールに供給するキーアドミニストレータによって有効化される。

5.2.9　プライベートキーを無効化する方法

プライベートキーはシステムのシャットダウンにより無効化される。

5.2.10　プライベートキーを破壊する方法

KSK および ZSK プライベートキーは再度使用できないような方法でシステムから取り除かれる。

5.3　キーペア管理の他の側面

5.3.1　アーカイバルパブリックキー

旧式のパブリックキーはアーカイブされない。

5.3.2　キー使用期間

KSK は約 1 年プラス発行および無効化を含む移行のための期間の間レジストリのゾーンにおいて有効であり続ける。ZSK によりサインされた多数の署名によって、ZSK は約 3 カ月プラス発行および無効化を含む移行期間の間有効であり続ける。レジストリは必要に応じてこれらの期間を変更できる。

5.4　有効化データ

5.4.1　有効化データの作成および設置

HSM の有効化には、セキュリティ監査者の立ち会いのもと PIN を PIN エントリーデバイスに供給するキーアドミニストレータが必要となる。

5.4.2 有効化データの保護

キーアドミニストレータは自身の PIN および PED を保護し守る責任を有する。アクセスは必要に応じて取り消しまたは修正することができる。

5.5 コンピュータセキュリティ制御

DNSSEC サービスのすべての構成要素には、特定の運用を行うためのアクセスおよび能力を与えられた様々な公認の職員が含まれる。これらのアクセスおよび運用は監査ログにログ、記載される。規則からの逸脱または悪意ある試みはさらなる調査のために監視、記録される。

5.6 ネットワークセキュリティ制御

DNSSEC サービスのすべての運用は、Neustar のデータセンター内で主催、実施される。これらは複数の層の物理的ネットワーキング保護により保護される内部ネットワークである。ネットワークはネットワークおよび物理的セキュリティ方針に従い確保される。

5.7 タイムスタンピング

DNSSEC サービスにより使用されるすべてのタイムスタンプは UTC であり、NTP（ネットワークタイムプロトコル）サーバを使用して同期される。

5.8 ライフサイクルの技術的制御

5.8.1 システム開発制御

DNSSEC サービスのすべての構成要素はデプロイの前に厳格な開発ガイドラインに従う。これらの厳格なガイドラインにより確実かつ高品質で再生可能な結果が確かなものとなる。

5.8.2 セキュリティ管理制御

レジストリは、自身のサーバ上のあらゆるソフトウェア変更を監視し、公認の職員により検証されるよう日報を作成するためのメカニズムを有する。

5.8.3 ライフサイクルのセキュリティ制御

レジストリは、フィードバックおよびコミュニティ主導の最高の運用に基づき自身の制御を改善し続ける。ソフトウェアまたはセキュリティ方針および手順へのあらゆる変更は、デプロイの前に評価、試験、承認される。

6　ゾーンサイニング

6.1　キーの長さおよびアルゴリズム

レジストリの KSK および ZSK 双方共に RSASHA256 である。KSK は 2048 ビット、ZSK は 1024 ビットである。

6.2　認証済みの存在の否定

レジストリは RFC 4034 に規定されている通りに NSEC 記録を使用し存在の否定を認証する。

6.3　署名フォーマット

XN--ECKVDTC9D (.ポイント)ゾーンの記録に対する署名フォーマットは、RFC 5702 で規定されている RSA/SHA-2 である。

6.4　ゾーンサイニングキーロールオーバー

XN--ECKVDTC9D (.ポイント) ZSK は 3 カ月ごとにロールオーバーされる。

6.5　キーサイニングキーロールオーバー

XN--ECKVDTC9D (.ポイント) KSK は 12 カ月ごとにロールオーバーされる。

6.6　署名有効期間および再署名頻度

署名は ZSK および KSK によりサインされた署名双方に対して 30 日間有効である。署名の再署名は期限切れの約 7 日前に行われる。

6.7　ゾーンサイニングキーセットの検証

ZSK はサイニングセレモニーの間に作成され、明確に定められた手順のセットに従う。作成されたパブリックキーおよびそのメタデータは、自動立証ツールの他のセットによってさらに検証される。

6.8　リソース記録の検証

レジストリはゾーン内のすべてのリソース記録のオンライン検証を定期的に行う。またゾーン内ですべてのリソース記録を記録し、すべての署名を立証する。

6.9　リソース記録 TTL

DNSKEY、DS およびそれらの対応するリソース記録署名（RRSIG）の TTL は 518400 に設定される（6 日）。NSEC およびそれらの対応する RRSIG の TTL は 86400 である（1 日）。TTL は必要に応じて将来変更できる。

7　適合性監査

適切な手順が常に守られ手順が正確に実施されていることを確かなものとするため、保持されたログおよびその他関連情報を使用して監査が行われる。

7.1　エンティティ適合性監査の頻度

監査はレジストリによって、または第三者へ外部委託されている技術的レジストリサービスの場合は、このような第三者サービスプロバイダによって少なくとも年 1 回行われる。

7.2　監査者の身元および資格

適合性監査はセキュリティ監査、セキュリティツール、DNS および DNSSEC の能力を有する独立したセキュリティコンサルティング会社によって行われる。

7.3　監査者の信頼者に対する関係

監査を行う責任を有する監査者は可能な場合レジストリおよび／またはレジストリサービスプロバイダの外部の者となる。

7.4　監査の対象テーマ

監査の範囲は、キー管理運用、インフラストラクチャ／行政管理、KSK および ZSK、署名ライフサイクル管理、運用開示を含み、監査期間中に生じたイベントの検討を含む。

7.5　不備の結果として取られるアクション

監査中に重大な異常が発見された場合は、妥当であればレジストリおよび／またはレジストリの外部委託されたサービスプロバイダが直ちに通知を受け、影響を受ける者によって是正措置計画が作成され、実施される。

7.6　結果の伝達

各監査の結果は、妥当であれば監査の完了後 30 日以内にレジストリおよび／またはレジストリの外部委託されたサービスプロバイダに書面による報告書で提供される。

8　法的事項

8.1　料金

委任署名者リソース記録の受領、サイニングおよび発行または DNSSEC に関連するその他機能に料金が発生することはない。

8.2　金銭的な責任

アマゾンレジストリサービス社は、本 DPS の下で発行された署名の不適切な使用に対し金銭的な責任を負わない。

8.3 取引情報の機密性

8.3.1 機密情報の範囲

以下の記録は機密およびプライベートなものとして保持されるものとする(機密／プライベート情報)。

- プライベートキーおよびこのようなプライベートキーをリカバーするために必要な情報
- 将来発行されることになるキーセットの署名
- 取引記録（取引の完全な記録および監査証跡の双方）
- Neustar により作成または保持された監査証跡記録
- Neustar により作成された監査報告書（このような報告書が保持される範囲まで）またはそれらの個々の監査者（社内または公的）（このような報告書が公知となるまで)。
- 危機管理計画および災害リカバリ計画
- Neustar ハードウェアおよびソフトウェアの運用を制御するセキュリティ手段ならびに DNS キーの管理

8.3.2 機密情報の範囲内にない情報

パブリックキーのような Neustar により運用されるドメインのデータベースに関する情報およびその他ステータス情報は公的なものである。

8.3.3 機密情報を保護する責任

適用なし。

8.4 個人情報のプライバシー

8.4.1 プライベートなものとして扱われる情報

適用なし。

8.4.2 プライベートなものとみなされない情報の種類

適用なし。

8.4.3 プライベート情報を保護する責任

適用なし。

8.4.4 司法または行政手続きに関する開示

アマゾンレジストリサービス社は、アマゾンレジストリサービス社が召喚状、質問状、自白要求および文書作成の要求のような民事裁判または行政処分における開示手続き中に、司法、行政またはその他法的手続きに対して誠意を持って開示が必要であると考える場合、機密の／プライベートな情報を開示する権利を有する。

8.5 責任の限度

アマゾンレジストリサービス社は本書に基づく自社の義務の自社の履行に由来する金銭的損失または間接損害もしくは障害から発生する損失に対して責任を有しない。その他責任は明示黙示を問わず受け入れられない。

8.6 期間および終了

8.6.1 期間

DPS はアマゾンレジストリサービス社レポジトリにおける発行と共に有効となる。本 DPS への修正はアマゾンレジストリサービス社レポジトリにおける発行と共に有効となる。

8.6.2 終了

本 DPS はその時々に修正され新版に取って代わられるまで有効であり続ける。

8.6.3 紛争解決条項

DNSSEC 参加者間の紛争は、当事者間の適用可能な合意における条項に従い解決されるものとする。

8.6.4 準拠法／管轄

本 DPS は米国ワシントン州の法および管轄に従うものとする。