Orchestrating a brighter world NEC

NEC Express5800 / NX7700x シリーズ
NIST SP 800-193 対応 ホワイトペーパー

第 1.2 版

2025 年 3 月 31 日

日本電気株式会社

目次

1. はじめに

本書は、NEC Express5800 および NX7700x シリーズにおける 米国国立標準技術研究所(NIST: National Institute of Standards and Technology)が発行した「NIST Special Publication 800-193 Platform Firmware Resiliency Guidelines」（以後、NIST SP 800-193）への対応状況を説明した資料になります。

補足

NEC では、「NIST Special Publication 800-193 Platform Firmware Resiliency Guidelines」の内、「shall(必須)」の項目をすべてサポートすることで、NIST SP 800-193 に準拠としています。

※ 本書に掲載されている会社名、商品名、サービス等の名称は、各社の商標または登録商標です。
※ 本書に掲載されている内容は、変更される可能性があります。 詳細は「更新履歴」ご参照ください。

2. NIST SP 800-193 について

本ガイドラインは、米国国立標準技術研究所(NIST)によって提供される IT セキュリティのガイドラインで、プラットフォームのファームウェアが信頼できる状態であることを保証する手段を提供しています。

このガイドラインでは、以下の 3 つの重要なセキュリティ原則を提供しています。このセキュリティ原則は、信頼の基点（RoT）と信頼の連鎖（CoT）という 2 つのプロセスに基づいています。

2.1. セキュリティ原則

NIST SP 800-193 では、以下の 3 つの重要なセキュリティ原則が提供されています。

- **保護（Protection）**
  ファームウェア(*1)や重要なデータ(*2)の完全性を保つために、改ざんから保護されることを保証する仕組み

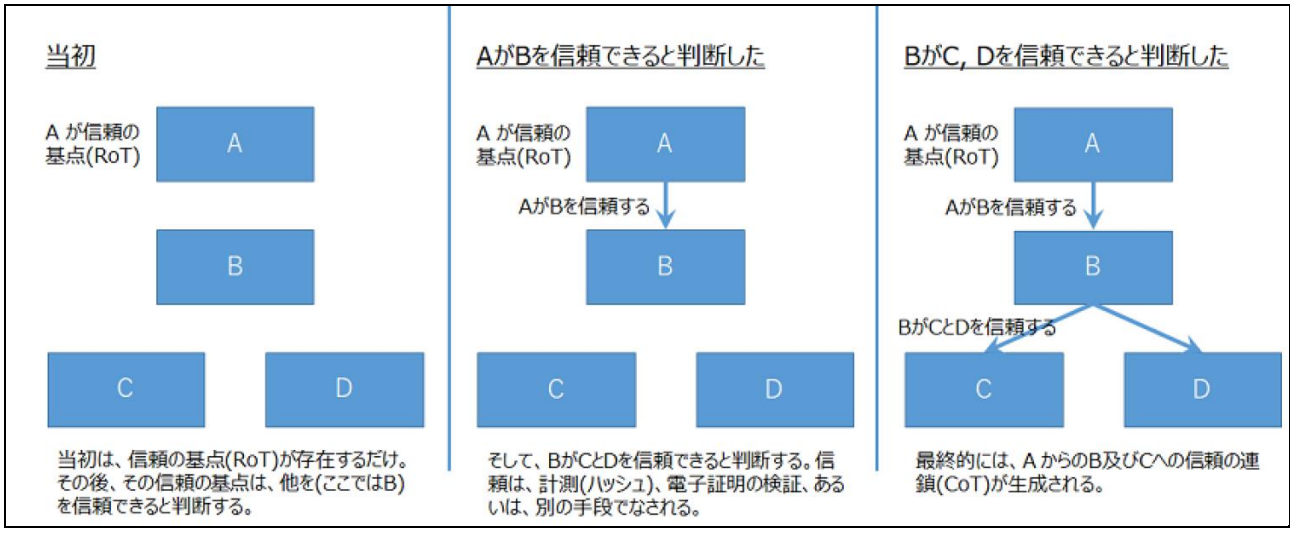
- **検知（Detection）**
  ファームウェア(*1)や重要なデータ(*2)が改ざんされていた場合、検知・通知・記録する仕組み

- **復旧（Recovery）**
  ファームウェア(*1)や重要なデータ(*2)が改ざんされたことを検知し、完全性のある状態に復旧するための仕組み

*1: サーバに搭載されたファームウェア
*2: OS の起動にかかわるハードウェア設定情報 等

2.2. 信頼の基点（RoT）と信頼の連鎖（CoT）

NIST SP 800-193 のセキュリティの仕掛けは、信頼の基点（RoT)の基に成り立っています。Rot から信頼の連鎖(CoT)が開始されることで、すべての要素が信頼できると判断されます。



詳細については、下記のオリジナルドキュメントをご参照ください。

NIST SP 800-193(Final)

https://csrc.nist.gov/publications/detail/SP 800-193/final

3. 対象機種

2024 年 9 月 30 日現在 NEC では、以下の機種が NIST SP 800-193 に準拠(*1)しています。
記載がない機種のサポート可否は、Express5800 シリーズは NEC ファーストコンタクトセンター(https://www.express.nec.co.jp/howto/question/contact.html)までお問い合わせください。
NX7700x シリーズは弊社営業までお問い合わせください。

3.1. Express5800 シリーズ

- R120j-1M
- R120j-1M (2nd-Gen)
- R120j-2M
- R120j-2M (2nd-Gen)
- R110k-1M
- R110k-1M (2nd-Gen)
- R110m-1
- T110k-M
- T110k-M (2nd-Gen)
- R120i-1M (*2)
- R120i-2M (*2)
- R32Ba-E2
- R32Ba-E2 (2nd-Gen)

3.2. NX7700x シリーズ

- A7012M-2
- A7010E-2
- A7010E-2c

(*1): ソフトウェアのアップデートが必要な場合があります。 詳細は、https://www.support.nec.co.jp/View.aspx?id=3140109677 に掲載されている「NEC Express5800 および NX7700x シリーズ NIST SP 800-193 準拠 運用構築手引き」ご参照ください。

(*2): NIST SP800-193 に準拠する運用環境の構築方法が他の機種と異なります。構築方法の詳細については、NEC ファーストコンタクトセンター(https://www.express.nec.co.jp/howto/question/contact.html)までお問い合わせください。

4. 用語集

用語	説明
Application Specific Integrated Circuit (ASIC)	一度製造されると機能の変更不可能な半導体集積回路です。
Baseboard Management Controller (BMC)	システムボードに内蔵されているハードウェア監視用コントローラです。
Chain of Trust (CoT)	一連の信頼できるものから成る信頼の連鎖を指します。最初の要素は一般的に最も信頼できるもの（RoT と呼ばれる）で、その後の各要素は前の要素によって検証され、信頼できると判断されます。
Chain of Trust for Detection (CTD)	CoT のプロセスの過程で実施されるファームウェアや重要データに破損・改ざんがないかを検出するプロセスのことを指します。
Chain of Trust for Recovery (CTDec)	CoT のプロセスの過程で実施されるファームウェアや重要データに破損・改ざんが検出された場合、復旧するプロセスのことを指します。
Chain of Trust for Update (CTU)	CoT のプロセスの過程で実施されるファームウェアの更新と重要なデータの変更を認証するプロセスのことを指します。
NEC iLO	3 章の対象機種に記載されたサーバに搭載されている BMC です。
Random Access Memory (RAM)	一時的にデータを格納するための揮発性メモリです。消去可能・書き換え可能であることが特徴で、電源を切るとデータは消失します
Read Only Memory (ROM)	永続的にデータを格納するための不揮発性メモリです。一度書き込むと普通は消去・書き換えができないことが特徴で、電源を切ってもデータは保持されます。
Root of Trust (RoT)	サーバ等のセキュリティにおいて最も信頼される部分のことで、NEC iLO 搭載機種においては、NEC iLO 内部の ASIC が RoT の役割を担っています。RoT はファームウェアや重要なデータが信頼できる状態から始まることを保証します。
Root of Trust for Detection (RTD)	RoT のプロセスの過程で実施されるファームウェアや重要データに破損・改ざんがないかを検出するプロセスのことを指します。
Root of Trust for Recovery (RTRec)	RoT のプロセスの過程で実施されるファームウェアや重要データに破損・改ざんが検出された場合、復旧するプロセスのことを指します。
Root of Trust for Update (RTU)	RoT のプロセスの過程で実施されるファームウェアの更新と重要なデータの変更を認証するプロセスのことを指します。

5. NIST SP 800-193 サポート状況

NEC Express5800 および NX7700x シリーズでの「NIST Special Publication 800-193 Platform Firmware Resiliency Guidelines」の「4. Firmware Security Guidelines for Platform Devices」で提示されている要件への対応概要を以下の表に示します。

(4. 1 章) Roots of Trust

本章では基本的な信頼の起点(RoT)と信頼の連鎖(CoT)においての保護、検出、回復の動作について記されたガイドラインが定義されています。

要件	対応内容
4.1.1 Roots of Trust (RoT) and Chains of Trust (CoT)	NEC iLO(マネジメントコントローラ)の ASIC にて Roots of Trust(RoT)を実現しています。この NEC iLO の ASIC を起点として RoT を開始し、信頼の連鎖(CoT)を実施します。
4.1.2 Root of Trust for Update (RTU) and Chain of Trust for Update (CTU)	ファームウェアのアップデートは RoT で検証済みの NEC iLO ファームウェアによって、署名検証を実施してからアップデートが実施されます。また署名検証には、FIPS186-4 に準拠したアルゴリズムを使用しています。
4.1.3 Root of Trust for Detection (RTD) and Chain of Trust for Detection (CTD)	NEC iLO の ASIC を起点として RoT を開始し、信頼の連鎖(CoT)を実施します。その過程でファームウェアコードおよび重要データの改ざん・破損を検出します。
4.1.4 Root of Trust for Recovery (RTRec) and Chain of Trust for Recovery (CTRec)	ファームウェアコードおよび重要データの改ざん・破損を検出した場合、各ファームウェアや重要データの復旧を行います。

(4.2 章) Protection

本章ではファームウェアや重要データの一部は改ざんされた場合、プラットフォームの完全性が保持されないため、ファームウェアと重要なデータの保護についてのガイドラインが定義されています。

要件	対応内容
4.2.1 Protection and Update of Mutable Code	各種ファームウェアは、FIPS 186-4 や NIST SP 800-57 に準拠したデジタル署名が付与されており、デジタル署名を用いた検証が実施されます。この検証は、OS 上で実行されるソフトウェアがアクセスできないメモリ領域で実行しており、セキュアな検証を行います。
4.2.2 Protection of Immutable Code	一部のファームウェアが、書き込み不可ストレージに格納されています。このストレージは書き込み不可から設定変更はできません。
4.2.3 Runtime Protection of Critical Platform Firmware	ファームウェアを RAM 上に展開する場合、OS 上で動作しているソフトウェアからアクセス不可となるように設計されています。
4.2.4 Protection of Critical Data	一部の重要データは不揮発性ストレージ上に保存されており、OS 上のソフトウェアからはアクセスできないように保護されています。その他のアクセス可能な重要データは、標準的な I/F を通じてのみアクセスすることを許可しています。

(4.3 章) Detection

本章ではファームウェアや重要なデータを実行前に改ざんされていないか検証する、また改ざんされている場合、改ざんの通知・記録を実施するためのガイドラインが定義されています。

要件	対応内容
4.3.1 Detection of Corrupted Code	重要データやファームウェアイメージが破壊されたとしても、RTD の破損・改ざん検出能力に影響はありません。またデジタル署名の検証により破損・改ざんを検知した場合、ログの記録、および通報が可能です。また自動的に復旧プロセスが開始されます。
4.3.2 Detection of Corrupted Critical Data	重要データを使用する前に検証を実施します。もしこのチェックが失敗した場合、クリティカルデータはデフォルト値に復元されます。また検証失敗時の動作としてログの記録、通報機能もサポートしています。

(4.4 章) Recovery

本章ではファームウェアや重要なデータの破損を検知した場合の復旧や、管理者が手動でファームウェアや重要データの復旧を実施するためのガイドラインが定義されています。

要件	対応内容
4.4.1 Recovery of Mutable Code	ファームウェアは不揮発性ストレージ上に保存されており、OS 上のソフトウェアからは直接アクセスできないように保護されています。 デジタル署名を用いた検証でファームウェアの破損・改ざんが検出された場合、各種ファームウェアの復旧を実行し、ログの記録、通報を行います。また復旧時においても、常にイメージの検証を行うことで、正しく認証されたイメージのみが復旧されます。
4.4.2 Recovery of Critical Data	重要データは OS 上のソフトウェアがアクセスできない領域に管理されています。万が一、重要データの破損・改ざんが検出された場合、RoT と CoT のプロセスにおいて、検出・復旧処理が行われることから、重要データの改ざんする攻撃に対抗できるように設計されています。

更新履歴

版数	日付	更新内容
1.0	2024/8/30	初版
1.1	2024/9/30	対象機種に以下の機種を追加しました。 Express5800 シリーズ 　R110k-1M (2nd-Gen) / T110k-M (2nd-Gen) / R120i-1M / R120i-2M NX7700x シリーズ 　A7012M-2 / A7010E-2 / A7010E-2c
1.2	2025/3/31	対象機種に以下の機種を追加しました。 Express5800 シリーズ 　R32Ba-E2 / R32Ba-E2 (2nd-Gen)