ファクトリコンピュータNIST対応モデルについて（NIST SP800-193準拠）

2025年3月

日本電気株式会社
インフラ・テクノロジーサービス事業部門　コンピュート統括部

セキュリティ対策の必要性

従来のOSセキュリティ機能やウイルス対策ソフトでは防げないセキュリティ脅威として、
BIOSの改ざんがあります。
本体が利用不能になる、機密情報が盗まれる、ランサムウェアに感染させられるなどの
被害が考えられ、また復旧も困難で制御が永続的に乗っ取られる危険があります。

こういった脅威から守り安心してお使いいただくために、
高セキュリティ機能を搭載したモデルをご用意しています（NIST SP800-193に準拠）。
BIOSへの攻撃から保護し、万が一改ざんがおこなわれた場合はこれを検知しLEDで通知。
さらにバックアップのBIOSへ自動復旧をおこない、ログに記録したうえで
通常通り起動させることが可能です。

© NEC Corporation 2025

市場背景

- 企業・組織等が受けたサイバー攻撃の件数や被害金額は世界的に増加傾向
  インフラや製造、物流などの制御システム領域でも年々セキュリティ脅威が増加

※出展：IPA「情報セキュリティ白書2024」2024

- Microsoft社の調査(2021)では83%の企業が過去２年間にFWへの攻撃を経験
  被害企業はSWよりHWやFWのセキュリティをより重視し投資増加させる傾向

※出展：Microsoft「Security Signals」2021
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWPStZ

- FWの1つであるBIOSのセキュアブートを乗っ取る「UEFIブートキット」が台頭
  OSの起動プロセスを完全に制御、高い権限でマシンを秘密裏に操作される脅威

※出展：ESET「「BlackLotus」 UEFIブートキット：
いま、そこにある現実の危機」2023
https://www.eset.com/jp/blog/welivesecurity/blacklotus-uefi-bootkit/

© NEC Corporation 2025

主なセキュリティ対策

NIST対応モデル　Windows対応　Linux対応　両OS対応

Application

OS

BIOS

Hardware

ウイルス侵入や不正ソフトウェア動作防止

脅威　・ネットワークや外部機器経由でのウイルス感染
・不正ソフトウェア実行によるデータ改ざん

対策　Microsoft Defender
Unified Write Filter
SolidProtect
readonly

脆弱性対応

脅威　・BIOS脆弱性を付いた不正操作

対策　BIOS/MEFWアップデート

不正アクセス防止

脅威　・悪意ある利用者による不正操作

対策　BIOSパスワード
HDDパスワード
USB無効化
Microsoft Defender
セキュアブート

データ持ち出し防止

脅威　・USB機器経由のデータ漏洩
・HDD持ち出しによるデータ盗難

対策　HDDパスワード
USB無効化
Microsoft Defender
セキュアブート

BIOS改ざん防止（保護・検知・復旧）

脅威　・BIOSブート不正乗っ取り
・高い権限でマシン不正操作

対策　***ECチップ追加、NIST SP800-193準拠***

© NEC Corporation 2025

BIOS改ざんリスクについて

■ BIOS改ざんの危険性

- OS起動前のため「セキュアブート」や「OSセキュリティ機能」、「ウイルス対策ソフト」では防御・検知できない
- 改ざんされると**復旧が困難、制御が永続的に乗っ取られる**危険性あり

■ BIOS改ざんされた場合の影響

- 利用不能になる、機密情報が盗まれる、ランサムウェアに感染させられるなど、「装置運用や企業自体に**深刻な被害**」を与える可能性あり

BIOS改ざんへの対策機能を実装した、NIST対応モデルをご用意

© NEC Corporation 2025

NIST SP800-193に準拠したセキュリティ対策　1/2

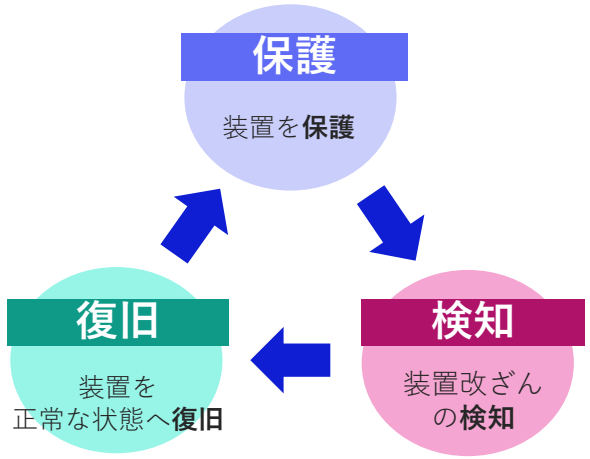
■ NIST SP800-193に準拠したセキュリティ対策

NIST SP800-193はコンピュータ（FC、PC、サーバ等）の電源を入れた際、
最初に動くファームウェア（BIOSなど）を守るためのガイドラインです。

原則/プロセス

3つの ＜**原則**＞と、２つの＜**プロセス**＞を定義

＜**原則**＞



＜**プロセス**＞

RoT(Roots of Trust)

コンピュータ（FC、PC、サーバ等）のセキュリティにおいて最も信頼される部分。
FCではECチップが RoTの役割を担う。
※EC （Embedded Controller）チップは信頼の根源として機能
　RoTはBIOS含むファームウェアなどが信頼できる状態から始まることを保証

CoT(Chain of Trust)

一連の信頼できるものから成る信頼の連鎖。
最初の要素はRoT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。

© NEC Corporation 2025

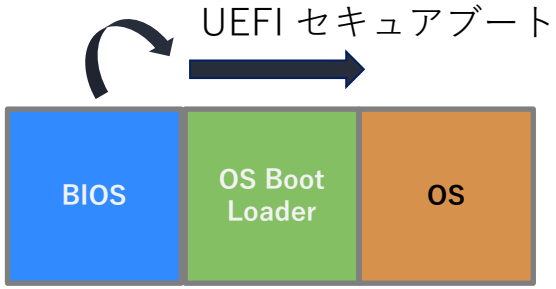
NIST SP800-193に準拠したセキュリティ対策　2/2

コンピュータのBIOS**保護**、改ざん**検知**、**復旧**をNIST SP800-193に準拠した
セキュリティファームウェア(FW)で実現

- **保護**：BIOSアップデート時、書換不可のECチップを起点に、不正な更新ではないことを検証。
- **検知**：BIOS起動時、書換不可のECチップを起点に、BIOSの改ざん有無を検証。
- **復旧**：改ざん検知時、自動復旧。BIOSが信頼できることを担保。

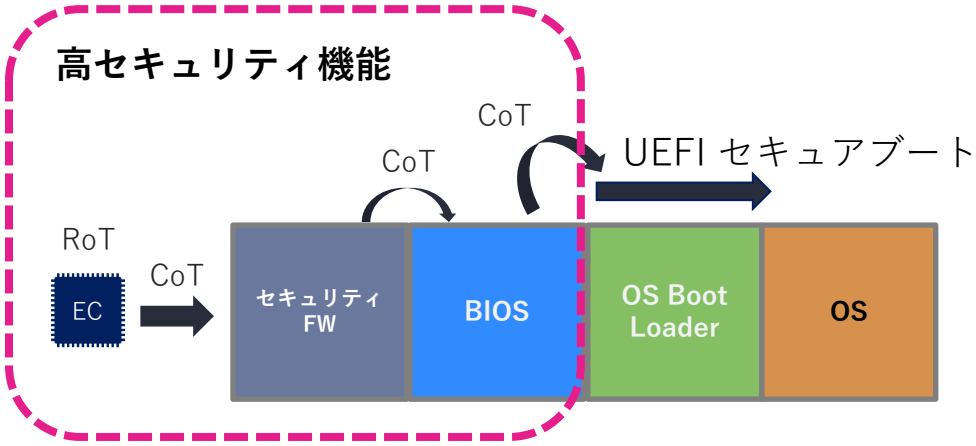
従来の装置起動シーケンス

・セキュアブート機能で不正な起動を防止できるが
BIOSが正しい状態であることが前提



NIST対応モデルの装置起動シーケンス

・ECチップを起点にBIOSの改ざん有無を検証
・改ざん検知時は自動復旧させ正常にOS起動



© NEC Corporation 2025

BIOS改ざん検知・復旧

- BIOS改ざんを検知後、LEDで通知し即時復旧開始
- 約5分で復旧完了、改ざん検知・復旧情報をログに記録のうえ通常通り起動

© NEC Corporation 2025

NIST対応製品について

■ 対応製品

シリーズ	型番	概要
省スペース	FC-E20W-NS	Xeon E-2278GEL (8コア/16スレッド) NIST対応モデル(標準(国内仕様))
省スペース	FC-E20W-NL	Xeon E-2278GEL (8コア/16スレッド) NIST対応モデル(保守期間延長(国内仕様))

注：フリーセクションで選択できるプリインストールOSは以下の通りです

- Windows 10 IoT Enterprise 2016 LTSB (64bit 日本語)
- Windows 10 IoT Enterprise 2019 LTSC (64bit 日本語)
- Windows 10 IoT Enterprise 2021 LTSC (64bit 日本語)

© NEC Corporation 2025

（参考）NISTとは / NIST SP800とは

- **NIST**：National Institute of Standards and Technology (米国国立標準技術研究所)
  - 科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関
  - NIST内には情報技術に関する研究をおこなっているITL(Information Technology Laboratory)あり ITLは情報技術に関してAIやセキュリティ等の研究も実施、各種文書を発行
  - **NIST SP 800シリーズ**はその中のガイドラインの一つ

ITL Publications

- Computer Security Resource Center
- Information Technology Laboratory (ITL) Patent Policy - Inclusion of Patents in ITL Publications
- Federal Information Processing Standards (FIPS)
- NIST Special Publication 800-series General Information(SP 800)
  コンピュータセキュリティ関係のレポート。セキュリティに関し、幅広く網羅しており政府機関、民間企業を問わず、セキュリティ担当者にとって有益な文書
- NIST Special Publication 1800-series General Information
- ITL Bulletin
- ITL Newsletter
- NIST Special Publication 500 Series
- Searchable NIST Publication Database

© NEC Corporation 2025

\Orchestrating a brighter world