DELL Technologies

ホワイトペーパー

強化されたiDRAC9のセキュリティ: ルート オブ トラストとBIOSライブスキャン

Dell EMC PowerEdgeサーバーのクラス最高峰のセキュリティを維持する、DRAC9 4.10.10.10および4.40.20.00の活用

概要

iDRAC9 4.10.10.10 (AMDプラットフォーム)および4.40.20.00 (インテル プラットフォーム)　では、サーバーの重要な領域へのマルウェア侵入リスクを軽減するための、強化されたルートオブトラスト（RoT）メカニズムが提供されています。また、インテルおよびAMDの新世代プラットフォームにおいて、システムに不正な変更が起きていないことを照合する確認機能が、BIOSスキャンという形で追加されています。

2021年6月

改訂

Date	説明
2020年4月	イニシャルリリース
2021年8月	インテル プラットフォームの追加

謝辞

著者:

- Aniruddha Herekar
- Arun Muthaiyan
- Doug Iler
- Murali Somarouthu
- Prashanth Giri

目次

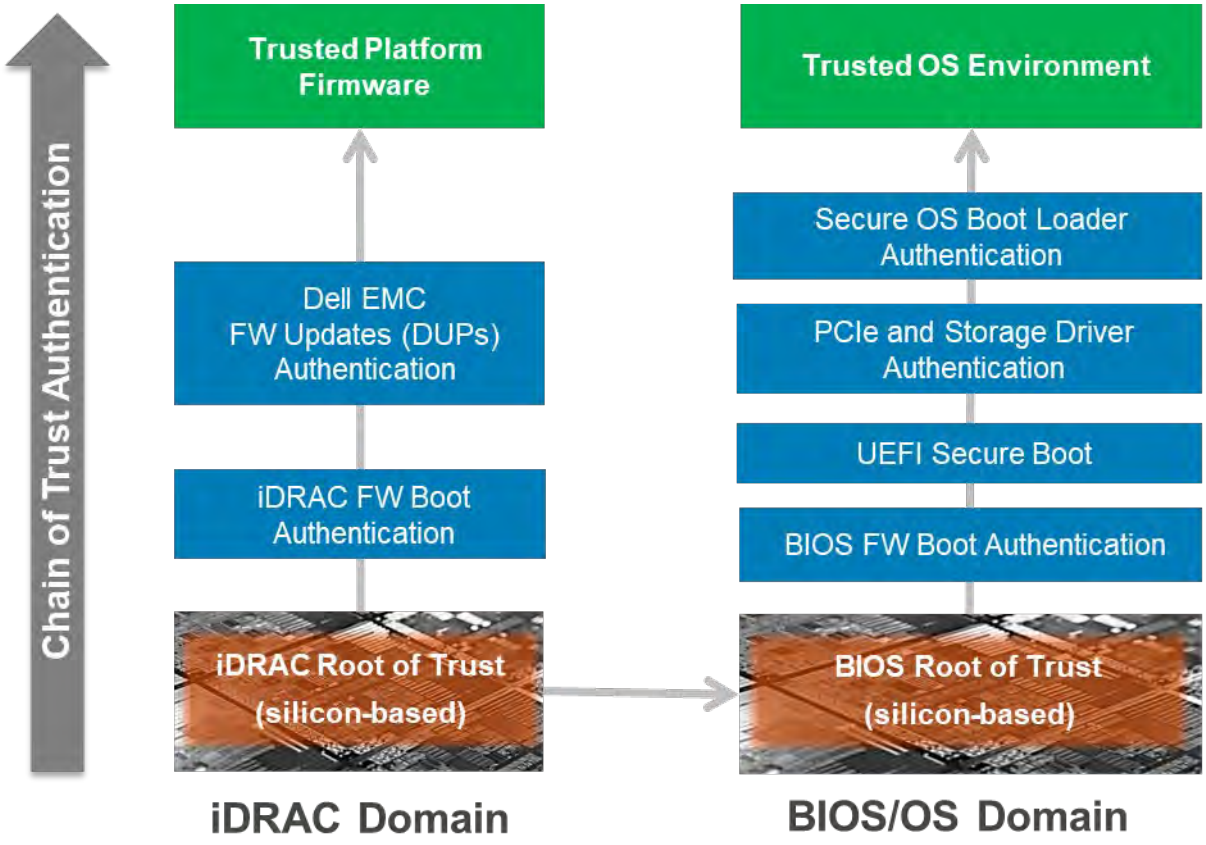
エグゼクティブサマリー

データセンター運用の成功には、セキュリティは不可欠な要素です。Dell EMCは、お客様に最も安全なソリューションを提供するために継続的にコードの改善を行うことをコミットしています。iDRAC9 4.10.10.10（AMDプラットフォーム）および4.40.20.00 (インテル プラットフォーム) のファームウェアリリースでは、ハードウェアベースのセキュリティ技術を活用してBIOSファームウェアの整合性を照合・確認できます。
さらに、スケジュールおよびオンデマンド機能としてのBIOSイメージのスキャンも利用可能になりました。このBIOSライブスキャン機能は、AMD "Rome"またはインテル"Ice Lake"搭載のPowerEdgeサーバーで利用できます。

このドキュメントでは、iDRACのルート オブ トラスト (RoT) とBIOSライブスキャン機能でどのようにサーバーのセキュリティが強化されるかを解説します。

1 イントロダクション

今日では、アップデートしたファームウェアやROM（Read Only Memory）さえもがハッカーの攻撃対象になります。ハッカーは、システムの変更・改ざんや悪意ある露出を行うための方法を見出そうとします。UEFIセキュアブートは、もちろんホストにセキュリティをもたらす効果的なメカニズムですが、いったんファームウェアが汚染されると、外部からの攻撃は回避できません。システムへ物理的なアクセスを得た悪意あるハッカーはBIOSのイメージを改ざんできます。改ざんされたBIOSコードはセキュリティの大きな脅威となり、またシステムは別の攻撃にも無防備な状態になります。インテルは、ブート時の整合性の脅威に対抗すべく、数年前の第4世代CoreプロセッサーでBoot Guardテクノロジーを投入しました。このルート オブ トラストは、システムをマルウェアによる改ざんから保護する、1回限りプログラム可能な読み取り専用キーに基づきます。Boot Guardを装備したシステムは、ブート イメージの暗号化ハッシュのデジタル署名と、プラットフォームの製造工場がシリコンに保存した署名とが一致することを、システム起動時に確認します。 正常に検証できる場合BIOSは、予定通り起動されます。検証に失敗した場合はBIOSイメージが汚染されていることを意味し、システムは起動できません。さらに、Boot Guardの認証メカニズムとは別に、iDRAC9がホスト起動時にBIOSイメージを検証するルート オブ トラストを提供します。BIOSイメージの検証が無事に完了した場合に、ホストは起動できます。iDRAC9は、サーバーの稼働中でもBIOSイメージを検証できます。これはオンデマンドでも、ユーザーが事前にスケジュールしたインターバルでも実行可能です。



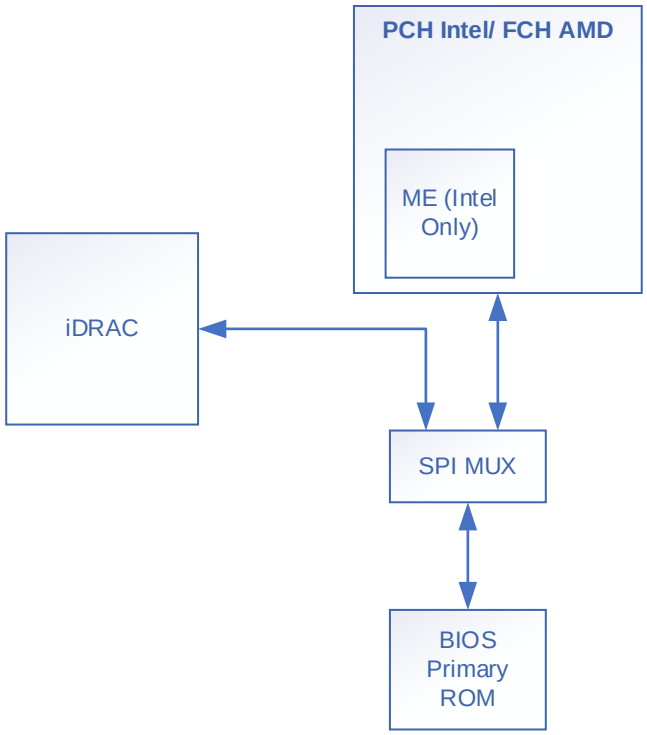
iDRAC9搭載のPowerEdgeサーバー内の、シリコンベースのルート オブ トラスト

2 Dell EMCのルートオブトラストとBIOSライブスキャン

2.1 ルートオブトラスト(RoT)

Dell EMCはセキュリティを非常に重要視しており、悪意あるBIOSの改ざんに対抗するため、Boot Guardテクノロジーを最新のPowerEdgeサーバーで採用しています。iDRAC9搭載のDell EMC PowerEdgeサーバーでは、まずiDRACが最初に「信頼の連鎖」による認証に基づき起動して、次にBIOSの整合性が検証されます。iDRACは、ハードウェアベースのセキュリティテクノロジーの役割も果たします。AMDシステムでは、iDRAC9はSPIおよびAMD Fusion Controller Hub(FCH)を経由してプライマリーBIOS ROMにアクセスし、RoTプロセスを実行します。インテル システムでは、iDRAC9はSPIおよびインテルPlatform Controller Hub (PCH)を経由してプライマリーBIOS ROMにアクセスし、RoTプロセスを実行します。

iDRAC9はRoT処理を行うため、BIOSプライマリーROMに直接アクセスします。これはセキュリティブロック、ホストイニシャルBootBlock、どちらの場合もです。



iDRACによるBIOSイメージROMへのアクセス

次の条件下で、iDRAC9がBIOSをリカバリーします。

1. BIOSの整合性チェックに失敗した。
2. BIOSセルフチェックに失敗した。

3. RACADMコマンド利用時に以下のコマンドを使用した
    a. RACADM command:
    racadm recover BIOS.Setup.1-1

2.1.1 サポートされるプラットフォームとiDRACのバージョン

Table 1 プラットフォーム、iDRACバージョン、サポートされる機能

プラットフォーム	サポートされるiDRAC9のバージョン	機能
R6525, C6525	3.42.42.42以上	ホスト起動時のBIOS整合性検証
R6525, C6525, and R7525	4.10.10.10 以上	ホスト起動時のBIOS整合性検証とBIOSイメージのライブスキャン
第15世代インテルXCC搭載プラットフォーム: PowerEdge R650、R750、MX750cほか	4.40.20.00 以上	ホスト起動時のBIOS整合性検証とBIOSイメージのライブスキャン

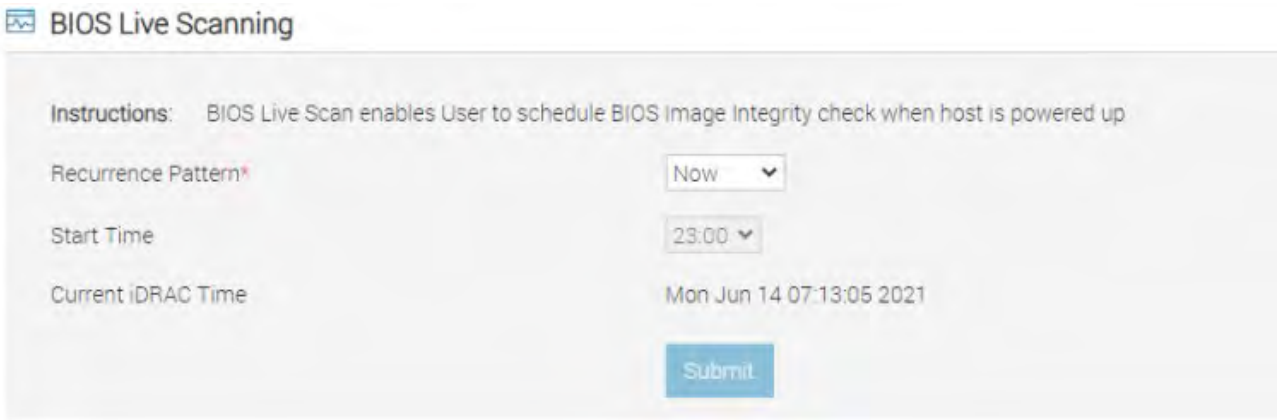
注意: iDRAC9によるハードウェアRoTならびにBIOSライブスキャン機能は、インテルおよびAMD搭載の第15世代プラットフォームのみでサポートされます。詳細は、iDRAC9のリリースノートでご確認いただけます。

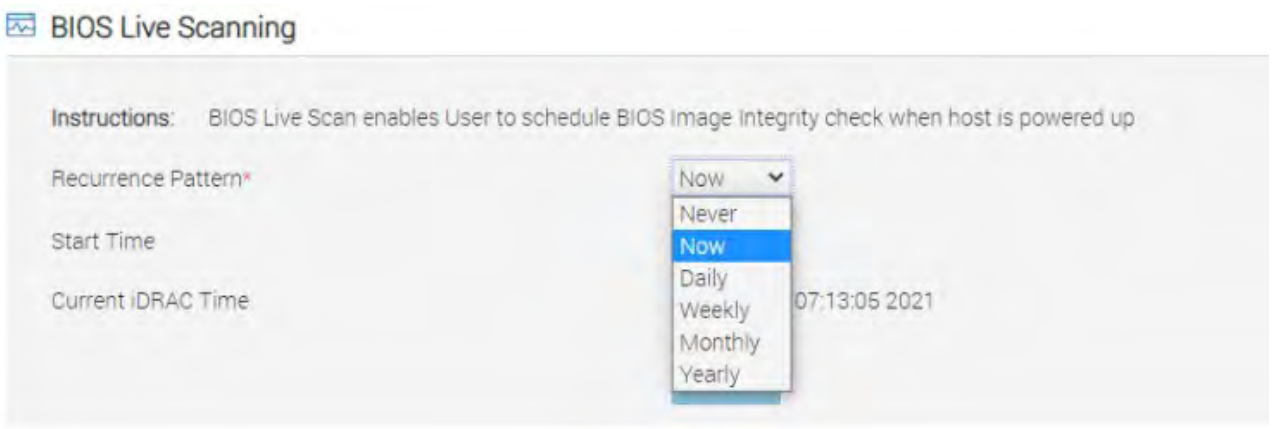
2.2 BIOSライブスキャン

BIOSライブスキャンは、ホストの電源が入っている状態で、プライマリーROMにあるBIOSイメージの整合性と信頼性を検証します。BIOSライブスキャンはPOSTのプロセスではありません。この機能は、iDRAC9 4.10.10.10（AMDプラットフォーム）および4.40.20.00 (インテル プラットフォーム) 以上で、iDRAC Datacenterライセンスが適用された場合に利用できます。このオペレーションには管理者権限もしくは“Execute Debug Commands”コマンドを使えるデバッグ権限が必要です。スキャンのスケジューリングはiDRAC UI、racadm、Redfishインターフェースで可能です。

2.2.1 iDRAC ユーザーインターフェースを使ったスキャンのスケジュール

下記のイメージはBIOSライブスキャンを実行する方法の複数の選択肢を示します。





iDRAC UIでのBIOSライブスキャン.

2.2.2 RACADMインターフェースを使ったスキャンのスケジュール

Usage: racadm biosscan -s <start-time>

#racadm help biosscan

Racadm biosscan -- Performs BIOS Live Scanning

Usage:
racadm biosscan -s <start-time>
-s <start-time>
  0 - Never schedule. Deletes existing jobs
  1 - Schedule Now
  2 - Schedule Daily
  3 - Schedule Monthly
  4 - Schedule Yearly

Usage Examples:
- To perform BIOS scan now:
  racadm biosscan -s 1

2.2.3 Redfishインターフェースを使ったスキャンのスケジュール

1. 最初に**“Get”**コマンドを打ち、求められたらユーザーネームとパスワードを入力

   https://<IP address>/redfish/v1/Systems/System.Embedded.1/Bios

2. 以下の2通りの方法でBIOSライブスキャンを起動するためのPOSTオペレーションを実行できます
   - POSTでの空のペイロードから**今すぐスキャンするジョブを設定**

https://<IP address>/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning

- POSTにて (**https://<IP address>/redfish/v1/JobService/Jobs**) を入力し具体的なスケジュールをboyd内で指定

i. To schedule scanning Now (immediately)

```
{
        "Payload":{
                "TargetUri":
                 "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
        }
}
```

ii. 1日一度のスキャンをスケジュール

```
{
        "Payload":{
                "TargetUri":
                "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
        },
        "Schedule": {
                "RecurrenceInterval": "P1D"
        }
}
```

iii. 月に一回のスキャンをスケジュール

```
{
        "Payload":{
                "TargetUri":
                 "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
        },
        "Schedule": {
          "EnabledDaysOfMonth":[24]     (Day of the date from which you prefer to schedule monthly)
        }
}
```

iv. 年に一回のスキャンをスケジュール

```
{
        "Payload":{
                "TargetUri":
                 "/redfish/v1/Systems/System.Embedded.1/Bios/Actions/Oem/DellBios.RunBIOSLiveScanning"
        },
        "Schedule": {
                                        "RecurrenceInterval": "P365D"
        }
}
```

システムおよびiDRACの最新リリースに関するさらなる詳細はこちらから

www.dell.com/poweredgemanuals

iDRAC 製品マニュアル	www.dell.com/idracmanuals
DRAC サポートサイト	www.dell.com/support/idrac

注意: Dell Technologiesは iDRACファームウェアや他のファームウェア（BIOS、ネットワークカード、その他）を最新のバージョンにアップデートすることを推奨しています。ファームウェアを最新バージョンにアップすることはこのホワイトペーパーにあるようなセキュリティ面のメリットをご享受いただけます。

3 結論

最高レベルのセキュリティを維持することは、今日の世界では不可欠です。一方で悪意のある活動を行う側も、先進テクノロジーを駆使して進化しており、それがシステムのセキュリティの大きな課題となっています。iDRAC9の4.10.10.10以上のバージョンでは、BIOSの整合性チェックと平常時のBIOSライブスキャン機能の両方が提供されています。iDRAC9は、インテルおよびAMD搭載の最新のPowerEdgeにおいて、ホストシステムのBIOSブートプロセスが安全であることを確実なものとします。.

- iDRAC9とインテルBoot Guardの大きなメリットは、万一BIOSイメージが感染した際のリカバリ能力です。
- ホスト側のルーオブトラスト(RoT)は、ホストBIOSが改ざんや不正アクセスにあった場合にそれを早期に検知しリスクを最小化することで、システムのブートプロセスの安全性を確実にします。
- ホストシステムが稼働中であっても、BIOSイメージを繰り返し検証できるプロセスを持つことで、起こり得るセキュリティの脅威からシステムを保護します。
- 決められたスケジュールに基づきBIOSイメージの整合性をスキャンするメカニズムにより、たとえ稼働中のホストであっても、もしBIOSが改ざんた場合でもお客様がそれを認知できます。
- スキャン結果が失敗した場合はLED表示やイベントログへの反映など優れた、アラートメカニズムがあります。
- 悪意あるソフトウェアが起こし得る、潜在的なダメージをシステムのブート時に軽減します。

A トラブルシューティング

1. iDRACにログインすると、iDRACによるBIOSの検証が失敗した旨のシステムイベントログ（SEL）が上がっているが、ホストシステムは起動できている。

    - これはiDRACによるHW RoTの機能の一貫です。BIOSイメージの検証に失敗した場合でも、iDRACは健全なBIOSイメージを引き出してきてリカバリ オペレーションを行います。

2. ホストは正常に起動しOSが立ち上がったにもかかわらず、タイムアウトによりネットワーク接続が検知できない。

    - BMCがHW RoTプロセスを始められない場合、その状態を自己検知するメカニズムがシステムに備わっています。その場合、システムはセーフモードで起動します。

3. BIOSイメージの整合性チェックの失敗により起動が行われず、それにより行われたBIOSリカバリーも失敗した場合は、以下のいずれかの手法でBIOSを手動でリカバリーします。

    - 任意のiDRACインターフェース（例：iDRAC UI）を用いてBIOSのDell Update Package（DUP）をアップロード
    - 当ドキュメントの第2セクションで解説されているRACADMのBIOSリカバリーコマンドを実施

B 用語集

用語	説明
BIOS	Basic Input/ Output System、またはシステムBIOS、ROM BIOS
FCH	Fusion Controller Hub
iDRAC	Integrated Dell Remote Access Controller
LED	半導体素子の一種で、電流を流すと発光するダイオード。発光ダイオードと呼ばれる。
ME	インテル マネジメント・エンジン
OS	オペレーティングシステム
PCH	プラットフォーム・コントローラー・ハブ：周辺I/O制御用プロセッサーとしていくつかのデータパスを管理し、インテル製CPUの機能のサポートする役割を果たす。
POST	Power-On Self-Test
ROM	Read Only Memory
RoT	Root of Trust
UEFI	Unified Extensible Firmware Interface

C 技術サポートおよび各種リソース

Dell.com/support はお客様のニーズを最優先に考え、日々サービスとサポートを提供をしています。

C.1 関連情報

ドキュメント（リンク）	内容
https://github.com/corna/me_cleaner/wiki/Intel-Boot-Guard	Intel Boot Guard
https://edk2-docs.gitbooks.io/understanding-the-uefi-secure-boot-chain/secure_boot_chain_in_uefi/intel_boot_guard.html	UEFI Secure Boot Chain - Intel Boot Guard の理解
https://2016.zeronights.ru/wp-content/uploads/2017/03/Intel-BootGuard.pdf	Safeguarding（安全防護対策）のための ルートキット：Intel BootGuard
http://www.uefi.org/specifications	UEFI 仕様詳細
https://downloads.dell.com/solutions/dell-management-solution-resources/Secure%20Boot%20Management%20On%20DellEMC%20PowerEdge%20Servers.pdf	DELL EMC PowerEdgeサーバーにおける セキュアブート管理
https://blog.dellemc.com/en-us/hardware-root-trust/	ハードウェア ルート オブ トラストとは？