

# Ask the Experts

Day 2 運用 : Cisco HyperFlex  
(Day2 Operations : Cisco Hyperflex)

2024年6月18日



# Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

## 免責

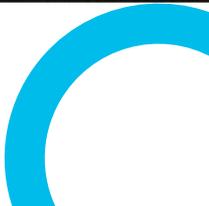
この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

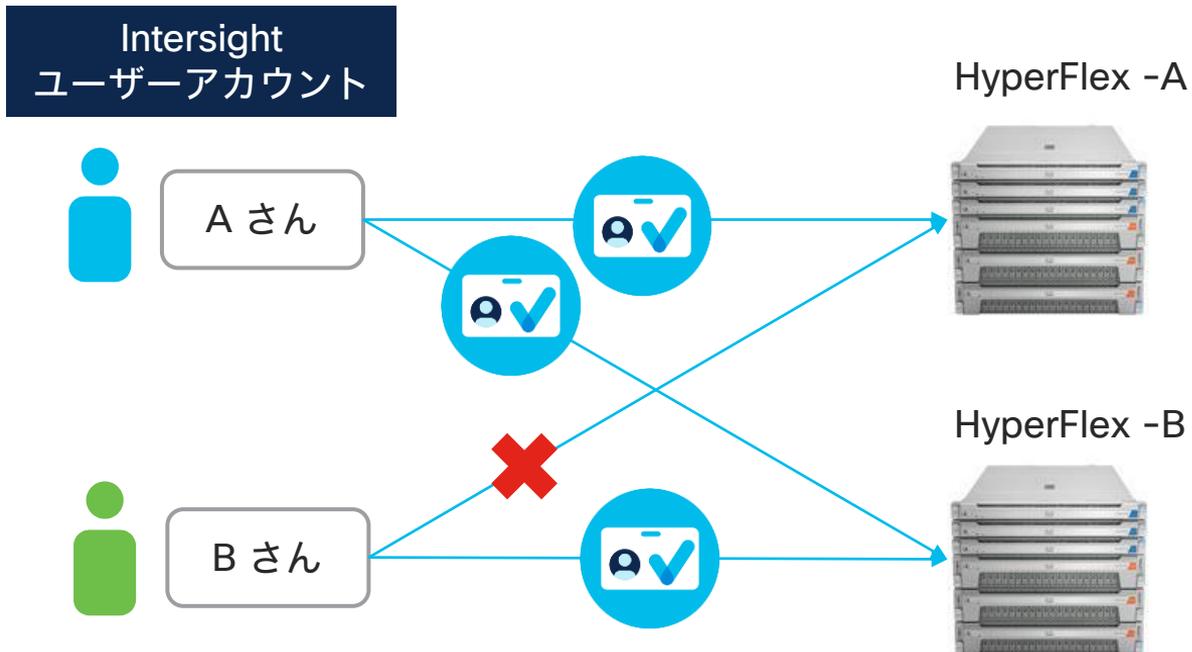
# アジェンダ

- 01 アクセス権限の管理 (Intersight)
- 02 障害予防
  - ・ハードウェア互換性リスト(HCL)
  - ・アドバイザリ機能
- 03 障害対応
  - ・ Proactive RMA
  - ・ Connected TAC
  - ・ ログ取得機能 (マニュアル)
- 04 フィードバック機能

# アクセス制御管理 (Intersight RBAC 機能)

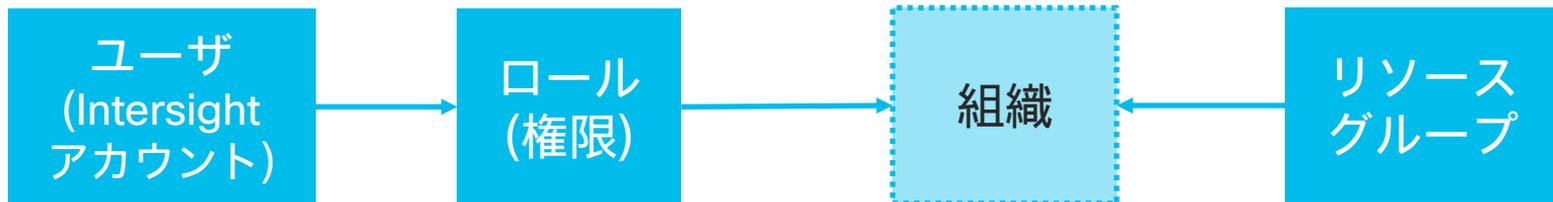


# アクセス制御管理



# アクセス制御管理（組織とロール）

ロールベース アクセス コントロール（RBAC）



<定義済みのロール>

- Account Administrator
- Read-only
- Device Technician
- Device Administrator
- **HyperFlex Cluster Administrator**
- Server Administrator
- User Access Administrator

<組織>

ロールとリソース  
グループの組み合わせ

<リソースグループ>

管理対象のグループ化



# 障害予防

- ・ハードウェア互換性リスト (HCL)



# ハードウェア互換性リスト(HCL)

## 概要

ハードウェア互換性リストとは、シスコ(パートナー)でテストおよび検証されたリスト(ハードウェアとソフトウェアの組み合わせにおける動作保証)

- ハードウェア : UCS Manager / CIMC から情報を取得
- ソフトウェア : OS に導入されたモジュールによって情報を取得

The screenshot displays the HCL Validation page in the UCS Manager interface. The page is divided into two main sections: Details and HCL Validation. The Details section shows the HCL Status as 'Validated' and a button for 'Get Recommended Drivers'. The HCL Validation section shows three categories of compliance, all marked as 'Validated': Server Hardware Compliance, Server Software Compliance, and Adapter Compliance. Below this, a table lists the validated items with columns for Model, Hardware Status, Software Status, Firmware Version, Driver Protocol, and Driver Version. The table contains three rows of data.

Model	Hardware Status	Software Status	Firmware Version	Driver Protocol	Driver Version
Cisco Boot optimized M.2	Validated	Validated	2.3.17.1014		
Cisco 12G Modular Raid C	Validated	Validated	51.10.0-3612	lsi_mr3	7.718.02.00-1vmw.703
Cisco(R) LOM X550-T2	Validated	Validated	0x80001514-1.823.2	ixgben	1.11.4.0-10EM.700.1.0.

# ハードウェア互換性リスト(HCL)

## 概要

### 1 Server Hardware Compliance Validated

Server Model  
**HX220C-M5SX**

CPU  
**Intel(R) Xeon(R) Platinum 8160 CPU @ 2.10GHz**

Server Firmware Version  
**4.2(3g)**

### 2 Server Software Compliance Validated

OS Vendor  
**VMware ESXi**

OS Version  
**7.0.3 3**

### Server Software Compliance Incomplete

**i** Missing Operating System information. Learn

OS Vendor

-

OS Version

-

### 3 Adapter Compliance Not Listed

**!** Incompatible component firmware and driver for one or more components. Learn more at [Help Center](#)

🔍 Add Filter

4 items found

10

per page

<<

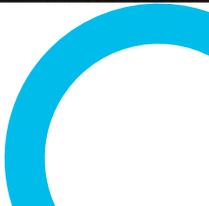
1

>>



Model	Hardware Status	Software Status	Firmware Version	Driver Protocol	Driver Version
Cisco(R) LOM X550-T2	<span>Validated</span>	Validated	0x800016F7-1.826.0	ixgben	1.12.3.0-1OEM.700.1.0.15843807
Intel MLOM Quad Port 1Gb RJ45 NIC	<span>Validated</span>	Validated	0x80000E78-1.826.0	igbn	1.9.1.0-1OEM.700.1.0.15843807
Intel i350 Quad Port 1Gb Adapter	<span>Validated</span>	Validated	0x800011A4-1.826.0	igbn	1.9.1.0-1OEM.700.1.0.15843807
Cisco 12G Modular Raid Controller with 2GB cache (max 16 drives)	<span>Validated</span>	Incompatible Driver	51.19.0-4532	lsi_mr3	7.718.02.00-1vmw.703.0.20.19193900

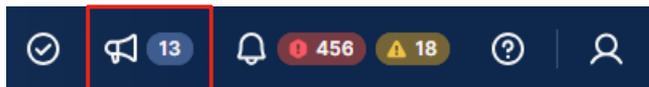
# 障害予防 ・アドバイザリ



# アドバイザリ

## 機能概要

- アドバイザリ機能は3つの情報を提示  
セキュリティアドバイザリ、Field Notice、End of Life (EoL)
- 有償ライセンスが必要 (Intersight Essentials 以上)



### Advisories

**Security Advisories** | Field Notices | End of Life Advisories | Acknowledged

• Advisories for affected devices only are listed here. For a complete list of advisories and more information, see [Help Center](#)

\* All Security Adviso... @ +

🔍 Add Filter

4 items found 10 per page 1 of 1

Description	Severity	CVEs	Affected Devices	Last Update
<a href="#">Cisco Integrated Management Controller Multiple Remot...</a>	Critical	CVE-2020-3470	1	Nov 18, 2020 5:00 PM
<a href="#">Cisco FXOS and NX-OS Software Cisco Discovery Proto...</a>	Medium	CVE-2022-20625	2	Mar 1, 2022 6:35 PM
<a href="#">Cisco FXOS and NX-OS Software Cisco Discovery Proto...</a>	High	CVE-2022-20824	2	Aug 24, 2022 5:00 PM
<a href="#">Cisco Integrated Management Controller GUI Denial of S...</a>	Medium	CVE-2021-34736	2	Oct 20, 2021 5:00 PM

# アドバイザリ

## 脆弱性情報(CVE) の概要

### Intel 2023.3 IPU - BIOS and Processors Advisories

**Details**

Severity  
High

ID  
Intel 2023.3 IPU - BIOS and Processors Advisories

CVEs  
CVE-2022-37343, CVE-2022-44611, CVE-2022-38083, CVE-2022-27879, CVE-2022-43505, CVE-2022-40982, CVE-2023-23908, CVE-2022-41804, CVE-2022-36392, CVE-2022-38102, CVE-2022-29871

Published  
2023年8月8日 09:00

Last Update  
2023年8月8日 09:00

Base Score  
7.2

**General**

Intel 2023.3 IPU - BIOS and Processors Advisories

**Summary**

Potential security vulnerabilities in the BIOS firmware or Intel® Processors for Cisco UCS M4, M5 and M6 generation of servers may allow escalation of privilege, information disclosure or denial of service. Cisco is releasing software updates to mitigate these potential vulnerabilities.

**Details**

To learn more about this security vulnerability, the affected products, and other details, see:  
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00813.html>  
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00783.html>  
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html>  
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00836.html>  
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00837.html>

Affected Devices (5)

Advisories for the devices are processed every 3 hours. If you update the device, it can take up to 12 hours for the updated status to be displayed for the device. For more info see [Help Center](#)

5 items found 10 per page 1 of 1

Name	Type	Model / Type	Firmware / Version
CS-FI6248-infra-1	Server	UCSC-C220-M5SX	4.1(3i)
CS-FI6248-infra-2	Server	UCSC-C220-M5SX	4.1(3i)
CS-FI6248-infra-3	Server	UCSC-C220-M5SX	4.1(3i)
C220-WZP22060AWK	Server	UCSC-C220-M5SX	4.2(3e)
CS-FI6454-IMM-1	Server	UCSC-C220-M5SX	4.2(3e)

Workarounds/Solutions

There are no workarounds that address this vulnerability.

Fixed Releases

Below firmware releases and later versions have fixes for the above mentioned vulnerabilities.

**UCS Servers Operating in Intraight Managed Mode**

# アドバイザリ

## Field Notice 概要

### FN74071

**Details**

ID  
FN74071

Published  
2023年12月13日 09:00

Last Update  
2023年12月13日 09:00

### General

Cisco Hyperflex Potential All Paths Down conditions in presence of stale disk mirror clean requests or Reduce Resync - Workaround Provided

**Summary**

Cisco HyperFlex Data Platform (HXDP) Software Releases 5.0(2a), 5.0(2b), 5.0(2c), and 5.0(2d) include software defects that may result in data unavailability or, in rare cases, data loss. The impact of these two bugs is typically triggered by a cluster maintenance event or an event such as drive failure.

**CSWf98678:** All Paths Down (APD) may occur sometime after a drive is replaced. This bug can cause the following issues:

The cluster becomes inaccessible (APD) due to a Cisco HyperFlex file system process (storfs) crash. Node panic/outage might occur.

**CSWf34019:** A race condition during cache-to-persistent destaging may discard the data to be flushed. This bug can cause the following issues:

Multiple disks across multiple nodes may be retired. The cluster state can become CRITICAL, which stops cluster read/write activity.

**Details**

To learn more about this field notice, the affected products, and other details, see: <https://www.cisco.com/c/en/us/support/docs/field-notices/740/fn74071.html>

**Affected Devices (1)**

**i** Advisories for the devices are processed every 3 hours. If you update the device, it can take up to 12 hours for the updated status to be displayed for the device. For more info see [Help Center](#)

1 items found 10 per page 1 of 1

Name	Type	Model / Type	Firmware / Version
<a href="#">CS-HXDP-Cluster</a>	HyperFlex Cluster	Hybrid	5.0(2d)

1 of 1

**Workarounds/Solutions**

Cisco has enabled the remediation for this issue using 2 different methods. Intersight users are advised to use the Intersight API method for remediation. Non-Intersight users can use a tool that can be run on any affected cluster which corrects the configuration to address the issues. If the remediation fails to run, you will be directed to contact Cisco TAC. There is no expected down time or operational impact to the cluster from running this tool. Detailed procedure to remediate the affected clusters is documented in the field notice.

As a general best practice, Cisco recommends running a backup before making any cluster changes and scheduling a maintenance window to complete these types of activities. If you are running one of the affected software releases, Cisco

**Summary**

Details

Affected Devices (1)

Workarounds/Solutions

# アドバイザリ

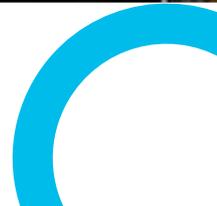
## EOS/EOSL 概要

### ucs-c-series-m5-eol-info

Details	General
<p>Status</p> <p><a href="#">Info</a></p> <p>ID</p> <p>ucs-c-series-m5-eol-info</p> <p>Type</p> <p>End of Life Announcement</p> <p>Last Update</p> <p>2023年5月2日 09:00</p> <p>Effective Date</p> <p>2023年5月1日 09:00</p>	<p>End-of-Life Announcement for the Cisco UCS M5 Rack Servers (C220 M5, C240 M5, C480 M5)</p> <p>Summary</p> <p>Cisco announces the end-of-sale and end-of-life dates for the Cisco UCS M5 Rack Servers (C220 M5, C240 M5, C480 M5). The last day to order the affected product(s) is October 30, 2023. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as per EoL bulletin.</p> <p>Details</p> <p>To learn more about this end of life advisory, the affected products, and other details, see: <a href="https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-m5-rack-server-c220-c240-c480-eol.html">https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-m5-rack-server-c220-c240-c480-eol.html</a></p> <p>End-Of-Life Milestones</p> <ul style="list-style-type: none"><li>● <b>End of Life Announcement Date - 2023年5月1日 09:00</b> The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.</li><li>● <b>End of Sale Date - 2023年10月30日 09:00</b> The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.</li><li>● <b>Last Ship Date - 2024年1月28日 09:00</b> The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.</li><li>● <b>End of Routine Failure Analysis Date - 2024年10月29日 09:00</b> The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.</li><li>● <b>End of New Service Attachment Date - 2024年10月29日 09:00</b> For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.</li><li>● <b>End of Service Contract Renewal Date - 2028年1月25日 09:00</b> The last date to extend or renew a service contract for the product.</li><li>● <b>Last Date of Support Hardware - 2028年10月31日 09:00</b> The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.</li></ul> <p>Affected Devices (8)</p>

## 障害対応

- ・ プロアクティブ RMA
- ・ Connected TAC



# サポート連携

- プロアクティブ RMA



- Connected TAC



# プロアクティブ RMA

## 自動実行のポイント

プロアクティブ RMA が動作するには、下記の障害時に実行されます

- メモリ  
障害コード : F0185 (DIMM 動作不能)
- ディスクドライブ  
障害コード : F1732 / F0181 (DISK 動作不良、不能)
- ファン  
障害コード(ラックサーバ) : F0484 / F0397 / F0794  
障害コード(ブレードサーバ) : F0484 / F0397

# プロアクティブ RMA

## 送付されるメール

From: sherholm@cisco.com  
To: XXXXXXXXXXX  
Cc: attach@cisco.com  
Subject: [Action Required] SR XXXXXXXXXXX : **Proactive RMA** for HX Drive in HX Cluster: XXXXXXXX, Triggered when disk in a HX cluster is in a hard black list and cannot be recovered. [Connected via Intersight]

Hello XXXXXX XXXXXX,

This email is to let you know that Cisco has received a fault message from your Cisco Hyperflex server connected by Cisco Intersight. The fault indicates a hard disk drive has failed and needs replacing. A TAC Case was created automatically (SR XXXXXXXXXXX) and draft RMA created to ship the replacement part. You need to open the RMA link to verify your shipping address and submit the RMA so the replacement part can be shipped out: [https://ibpm.cisco.com/rma/home/?RMANumber= XXXXXXXXXXX](https://ibpm.cisco.com/rma/home/?RMANumber=XXXXXXXX) If entitled a Cisco Field Engineer can be requested on the above RMA form to complete the replacement.

Note: If you have difficulty loading the link above, please contact Logistics Support Center at one of the following manners:

<https://www.cisco.com/c/en/us/buy/logistics-support-center.html>

More information about the failed part and the server in which it's installed:

Hyperflex Cluster Name: XXXXXXXX  
Server Hostname: XXXXX  
Server IP: XXXXXXXXXXX  
Server Serial Number: XXXXXXXXXXX  
Disk slot: 11  
Fault Description: Triggered when disk in a HX cluster is in a hard black list and cannot be recovered.

# プロアクティブ RMA

## 有効にする方法

設定

システム

アカウントの詳細

設定

アカウント名	JapanCSS
アカウントID	63762f907564612d33a290e4
アクセスリンク	https://63762f907564612d33a290e4.intersight.com/
	https://japancss.intersight.com/
Region	intersight-aws-us-east-1
作成時刻	2022年11月17日 21:56
Default Idle Timeout	30m
ユーザあたりの同時セッションの最大数	32 sessions
デフォルトセッションタイムアウト	16h
Audit Log Retention Period	48 Months
タグ	AutoRMAEm... tsumura@ci... AutoRMA Ture

アカウント設定の設定

Disabled

API Keys Maximum Expiration Time (Days) \* ⓘ

180

1 - 360

タグの設定

AutoRMAEmail tsumura@cis... ×

AutoRMA True × key:value形式でタグを入力します

キャンセル 設定

sherholm@cisco.com から送付されるメールを受信するメールアドレスを入力下さい

例1 : AutoRMA の送信先を [test@cisco.local](mailto:test@cisco.local) にする

AutoRMAEmail:test@cisco.local

例2 : AutoRMA の送信先を [test@cisco.local](mailto:test@cisco.local) と [group@cisco.local](mailto:group@cisco.local) の複数にする

AutoRMAEmail:test@cisco.local,group@cisco.local

# Connected TAC

## シスコサポート連携

The screenshot shows the Cisco Intersight Infrastructure Service interface. The main content area displays details for server C220-WZP23301041, which is marked as 'クリティカル' (Critical). The 'アクション' (Action) dropdown menu is open, listing various operations such as Power, System, Profile, and 'TACケースを開く' (Open TAC Case), which is highlighted with a red box. Other visible options include 'オペレーティングシステムのインストール', 'ファームウェアのアップグレード', 'IMCの起動', 'vKVMの起動', 'トンネリングされたvKVMの起動', 'Start Alarm Suppression', 'ライセンス階層の設定', and 'テクニカルサポートバンドルの収集'.

### Open TAC Case

Click Continue to open Cisco Support Case Manager(SCM) with details about your selection from Intersight.

Selected Server: C220-WZP23301041  
Serial Number: WZP23301041.

キャンセル Continue

### Support Case Manager

Open a new support case / Takeshi Tsumura (tsumura@cisco.com)

OPEN NEW CASE  
Products & Services

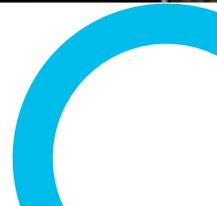
1  
Check Entitlement

リクエストのタイプ

障害解析  ハードウェア交換(RMA)  その他のお問い合わせ

## 障害対応

- ・ログ取得機能 (マニュアル)



# ログ取得機能 (マニュアル)

## 概要

The screenshot displays the Cisco Intersight web interface for a server named C220-WZP23301041. The server is marked as 'Critical' (クリティカル). The interface is divided into several sections: '概要' (Overview), '運用' (Operations), 'サーバ' (Server), and '詳細' (Details). The 'サーバ' section is active, showing a list of servers with columns for 'スレッド' (Thread) and 'ID'. The '詳細' section shows the server's health status as 'Critical' (クリティカル) and provides various configuration options. The 'プロパティ' (Properties) section shows the server's name, IP address, and serial number. The 'アクション' (Actions) menu is open, listing various operations such as Power, System, Profile, and Tech Support Bundle Collection. The 'Tech Support Bundle Collection' option is highlighted with a red box, and a red arrow points to a notification banner at the top right that reads 'Tech Support Bundle Collection started'.

# ログ取得機能 (マニュアル)

## 概要

Cisco Intersight システム

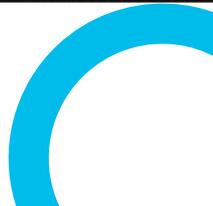
### テクニカルサポートバンドル

テクニカルサポートバンドル

テクニカルサポートバンドルの追加

ダウンロード	シリアル	PID	デバイス...	ステータス	ファイルサイズ	理由	最終更新
<input type="checkbox"/>	FDO22232S60	UCSC-FI-6332-1...	Fabric Intercon...	CollectionInPro...	0 bytes		1分前
<input type="checkbox"/>	WZP24241EDD	UCSC-C220-M...	Rack Server	Completed	12.78 MiB		2024年2月8日 1...
<input type="checkbox"/>	WZP24241EDD	UCSC-C220-M...	Rack Server	Completed	12.38 MiB		2024年1月19日 ...
<input type="checkbox"/>	WZP24241EDD	UCSC-C220-M...	Rack Server	Completed	12.27 MiB		2024年1月16日 ...
<input type="checkbox"/>	WZP22060AWK	UCSC-C220-M...	Rack Server	Completed	19.53 MiB		2023年12月22...
<input type="checkbox"/>	FDO2308007F	UCSC-FI-6454	Fabric Intercon...	Completed	310.00 MiB		2023年12月22...
<input type="checkbox"/>	FDO2308007F	UCSC-FI-6454	Fabric Intercon...	Completed	307.73 MiB		2023年12月22...
<input type="checkbox"/>	WZP22060AWK	UCSC-C220-M...	Rack Server	Completed	19.82 MiB		2023年12月1日 ...
<input type="checkbox"/>	WZP24241EDD	UCSC-C220-M...	Rack Server	Completed	10.07 MiB		2023年6月29日...
<input type="checkbox"/>	WZP24241EDD	UCSC-C220-M...	Rack Server	Completed	9.78 MiB		2023年6月12日...

# フィードバック機能

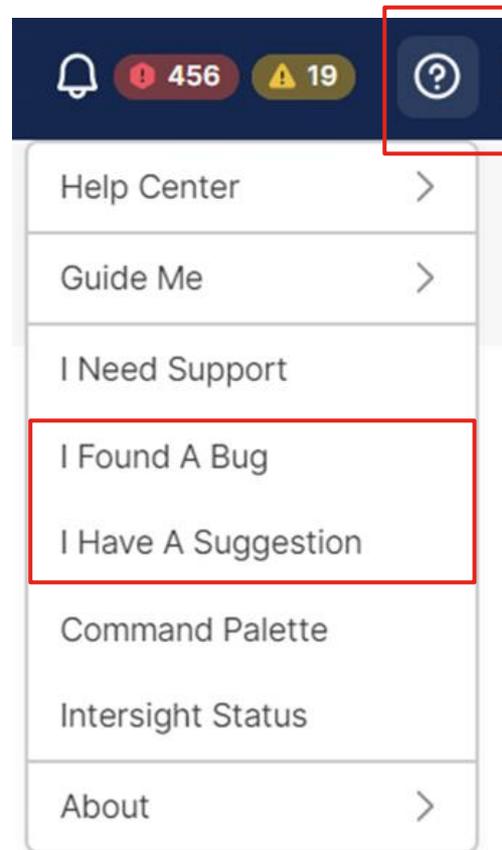


# ユーザーフィードバック

## 概要

Intersight にはフィードバック機能があります。  
右上のハテナマークをクリックしてください

- I Need Support  
シスコサポートに連絡する機能  
(サポートケースを開きます)
- I Found A Bug  
バグを報告する機能
- I Have A Suggestion  
機能改善や、新機能追加など  
皆様のご意見を投稿する機能





## デモ#1: Connected TAC



## デモ#2: アクセス制御管理 (RBAC)

# 覚えておくべき重要なポイント



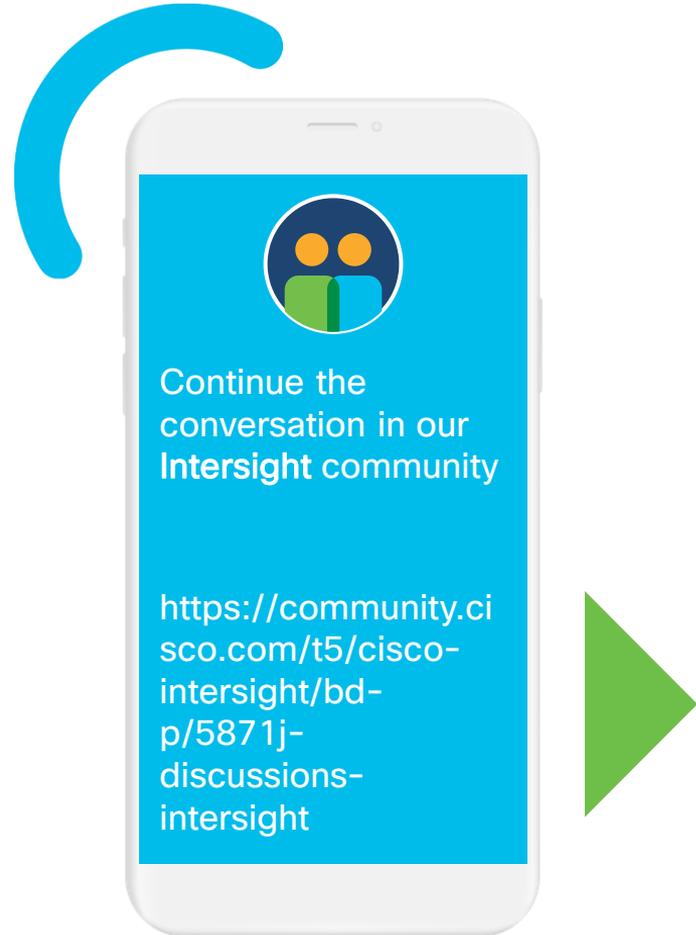
- 01 Intersight は、アクセス制御が可能です。  
定期的に権限の見直しを行ってください
- 02 障害予防には2つの機能があります  
・ハードウェア互換性リスト  
・アドバイザリ機能
- 03 障害対応の自動化にはプロアクティブ RMA です。  
機能を有効にする事を忘れないでください
- 04 Connected TAC 機能により、障害対応にかかる時間を短縮することができます
- 05 皆様のご意見をフィードバック下さい。  
製品の改善 / 新機能追加を出来るだけ実施します

# Resources

Ask the Experts リンク集: Cisco Hyperflex

<https://community.cisco.com/t5/-/-/ta-p/4478213>

※本日の ATXs 以外のリソースリンクも確認できます。



# Cisco コミュニティサイトについて



日本語サイトがあります！  
言語設定を変えるだけ。

- ・ わからない事
  - ・ 知りたい事
- 日本語でご質問下さい！

日本語コミュニティサイト  
<https://community.cisco.com/t5/japan/tkbc-p/japanese-community>

