LDAP 署名と LDAP チャネルバインディング有効化の影響製品一覧

目次

本情報は掲載日時点の情報です。今後の状況によっては変更する場合がありますのでご注意願います。

Hitachi Command Suite

品名	形名	バージョン	対応状況
Hitachi Command Suite ・Hitachi Automation Director ・Hitachi Compute Systems Manager ・Hitachi Device Manager ・Hitachi Global Link Manager ・Hitachi Replication Manager ・Hitachi Tiered Storage Manager ・Hitachi Tuning Manager	全形名	全バージョン	StartTLS を使用する設定で対処可能。

※1：Hitachi Configuration Manager はストレージ製品側の外部認証連携機能もしくは外部認可連携機能の使用の有無により影響を受ける可能性があるため、対処方法の詳細はストレージ製品側の同機能についての情報を参照してください。

影響内容	HCS 製品内で、認証や認可機能が正しく動作しなくなります。その結果、製品の個々の機能も不正な権限での動作となり適切に動作しなくなります。 次のすべての条件に該当する場合、本現象が発生する可能性があります。 (1) HCS 製品が外部認証連携機能または外部認可連携機能を使用して、ノンセキュアなプロトコル(LDAP プロトコル)で Active Directory に接続している。 (2) Microsoft 社のセキュリティアドバイザリーADV190023 に記載されているセキュリティ強化(LDAP 署名および LDAP チャネルバインディングが有効化)がされている。
対処方法	外部認証連携機能もしくは外部認可連携機能に、セキュアなプロトコル(StartTLS)を使用してください。詳細は製品マニュアルを参照してください。 Hitachi Command Suite システム構成ガイド 4.7 外部認証サーバと外部認可サーバの登録 http://itdoc.hitachi.co.jp/manuals/3021/30219008E0/DMSJ0109.HTM 5.5.11 Hitachi Command Suite 共通コンポーネントのトラストストアーへの証明書のインポート http://itdoc.hitachi.co.jp/manuals/3021/30219008E0/DMSJ0189.HTM 5.5.12 LDAP ディレクトリサーバのサーバ証明書の条件 http://itdoc.hitachi.co.jp/manuals/3021/30219008E0/DMSJ0190.HTM

JP1/Automatic Operation

品名	形名	バージョン	対応状況
JP1/Automatic Operation	全形名	10-50 以降	StartTLS を使用する設定で対処可能。

影響内容	JP1/AO にて Active Directory 連携を使用している場合、Active Directory のユーザにて認証が正しく動作しなくなります。 次のすべての条件に該当する場合、本現象が発生する可能性があります。 (1) 外部認証サーバ連携にてを使用して、Active Directory に接続している。 (2) Microsoft 社のセキュリティアドバイザリーADV190023 に記載されているセキュリティ強化(LDAP 署名および LDAP チャネルバインディングが有効化)されている。
対処方法	外部認証サーバ連携にて、セキュアなプロトコル(startTLS)を使用するよう設定を変更してください。 設定手順等の詳細情報は、日立サポートサービス お客様専用ページより、以下の情報発信を参照願います。 JP1/AO Active Directory と連携する場合の注意事項 https://www.hitachi-support.com/product/jp1/yobou/v12/jp1te12033.html

JP1/Base

品名	形名	バージョン	対応状況
JP1/Base	P-2A2C-6LCL	12-00 以降	LDAPS での AD 連携により対処可能。
	P-2A2C-6LBL	11-00 以降	
	P-2W2C-6LA4	10-00 以降	
	P-242C-6L94 P-2A2C-6L94 P-282C-6L94 P-2D2C-6L94	09-00 以降	
	P-2A2C-6L84 P-282C-6L84 P-2D2C-6L84	08-50 以降	
	P-242C-6L84	08-11 以降	

影響内容	JP1/Base の認証サーバにおいて Active Directory サーバと連携してユーザ認証を行っている場合、LDAP 署名/LDAP チャネルバインディング有効化後に Active Directory サーバとの接続に失敗します。そのため認証情報を Active Directory サーバで管理している JP1 ユーザ（DS ユーザや連携ユーザ)はログインできなくなります。
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。JP1/Base 側の設定については、ディレクトリサーバ連携定義ファイルの PORT、SSL パラメーターを以下のように設定してください。 ・"SSL"=dword:00000001 ・"PORT"=dword:0000027C なお、ディレクトリサーバの接続先ポート番号をデフォルト値（636）から変更している場合は、変更したポート番号を 16 進数で指定してください。 設定方法の詳細につきましては、ご使用のバージョンの製品マニュアルをご参照ください。 JP1/Base 運用ガイド ディレクトリサーバ連携定義ファイル（Windows 限定）

JP1/Base の認証サーバを前提としている製品

■JP1/Audit Management - Manager、JP1/NETM/Audit – Manager

品名		形名	バージョン	対応状況
JP1/Audit Management - Manager		全形名	V10～V11 のすべて	JP1/Base の対処方法を参照。
JP1/NETM/Audit - Manager		全形名	V8～V9 のすべて	
影響内容	JP1/Audit Management の JP1/Base の認証サーバにおいて Active Directory サーバと連携してユーザ認証を行っている場合、JP1/Base の認証機能でエラーが発生してログインができないなどといった影響があります。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Automatic Job Management System 3、JP1/Automatic Job Management System 2 [Manager/Agent/View]

品名		形名	バージョン	対応状況
JP1/Automatic Job Management System 3 – Manager [Manager]		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
JP1/Automatic Job Management System 3 - Manager		全形名	V9～V10 のすべて	
JP1/Automatic Job Management System 3 – Manager [WebConsole]		全形名	V11～V12 のすべて	
JP1/Automatic Job Management System 3 - Agent		全形名	V9～V12 のすべて	
JP1/Automatic Job Management System 3 - Agent Minimal Edition		全形名	V11～V12 のすべて	
JP1/Automatic Job Management System 3 – View [View]		全形名	V11～V12 のすべて	
JP1/Automatic Job Management System 3 – View		全形名	V9～V10 のすべて	
JP1/Automatic Job Management System 2 - Manager		全形名	V8 のすべて	
JP1/Automatic Job Management System 2 - Agent		全形名	V8 のすべて	
JP1/Automatic Job Management System 2 - View		全形名	V8 のすべて	
影響内容	対象製品の JP1/Base の認証サーバにおいて Active Directory サーバと連携してユーザ認証を行っている場合、JP1/Automatic Job Management System 3 - View や JP1/Automatic Job Management System 3 - Web Console で JP1/Automatic Job Management System 3 - Manager にログインする際などに、JP1/Base の認証機能でエラーが発生してログインができないなどといった影響があります。 認証サーバが使用できないと、エージェントホストでのジョブ実行もできないため、JP1/Automatic Job Management System のシステム全体に影響を与えることになります。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Automatic Job Management System 3 - Definition Assistant

品名		形名	バージョン	対応状況
JP1/Automatic Job Management System 3 - Definition Assistant		全形名	09-10～V12のすべて	JP1/Base の対処方法を参照。
影響内容	接続先の JP1/Automatic Job Management System 3 - Manager で使用している JP1/Base の認証サーバにおいて Active Directory サーバと連携してユーザ認証を行っている場合、JP1 ユーザの認証ができず、操作に失敗します。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Automatic Job Management System 3、JP1/Automatic Job Management System 2 - Web Operation Assistant

品名		形名	バージョン	対応状況
JP1/Automatic Job Management System 3 - Web Operation Assistant		全形名	V9～V10 のすべて	JP1/Base の対処方法を参照。
JP1/Automatic Job Management System 2 - Web Operation Assistant		全形名	V8 のすべて	
影響内容	JP1/Automatic Job Management System 3 - Web Operation Assistant または JP1/Automatic Job Management System 2 - Web Operation Assistant の前提製品である JP1/Base の認証サーバで、Active Directory サーバと連携してユーザ認証を行っている場合に、Web ブラウザからのログインに失敗します。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Automatic Operation

品名		形名	バージョン	対応状況
JP1/Automatic Operation		全形名	V10～V12 のすべて	JP1/Base の対処方法を参照。
影響内容	JP1/Automatic Operation の外部認証連携で JP1/Base の認証サーバを使用しているかつ、JP1/Base の認証サーバで Active Directory サーバーと連携してユーザー認証を行っている場合、JP1/Automatic Operation へのログインができなくなります。			
対処方法	外部認証連携で JP1/Base の認証機能を利用する場合は、JP1/Base に記載している対処方法にて対処してください。			

■JP1/Integrated Management 2、JP1/Integrated Management

品名		形名	バージョン	対応状況
JP1/Integrated Management 2 - Manager		全形名	V12 以降	JP1/Base の対処方法を参照。
JP1/Integrated Management 2 - View		全形名	V12 以降	
JP1/Integrated Management – Manager		全形名	V8～V11 のすべて	
JP1/Integrated Management - View		全形名	V8～V11 のすべて	
影響内容	対象製品の JP1/Base の認証サーバにおいて Active Directory サーバと連携してユーザ認証を行っている場合、JP1/Integrated Management - View や統合オペレーションビューアで JP1/Integrated Management - Manager にログインする際などに、JP1/Base の認証機能でエラーが発生してログインができないなどといった影響があります。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/IT Desktop Management 2 - Manager

品名		形名	バージョン	対応状況
JP1/IT Desktop Management 2 - Manager		全形名	11-10～V12 のすべて	JP1/Base の対処方法を参照。
影響内容	JP1/IT Desktop Management 2 - Manager のマネージャセットアップで「JP1/Base を使用してユーザ管理する」を選択した場合、JP1/Base の認証機能でエラーが発生してログインができないなどといった影響があります。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Navigation Platform、JP1/Integrated Management - Navigation Platform

品名		形名	バージョン	対応状況
JP1/Navigation Platform		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
JP1/Integrated Management - Navigation Platform		全形名	V10 のすべて	
影響内容	ユーザ認証を利用している環境でナビゲーション プラットフォームを運用し JP1/Base の認証サーバを使用しているかつ、JP1/Base の認証サーバで Active Directory サーバーと連携してユーザ認証を行っている場合、JP1/Navigation Platform へのログインができなくなります。			
対処方法	ユーザ認証方式を JP1 認証モードのままとする場合は、JP1/Base に記載している対処方法にて対処してください。			

■JP1/NETM/DM Manager

品名		形名	バージョン	対応状況
JP1/NETM/DM Manager		全形名	08-10～V10のすべて	JP1/Base の対処方法を参照。
影響内容	JP1/NETM/DM Manager のインストール時に「JP1/Base を使用してユーザ管理する」を選択した場合、JP1/Base の認証機能でエラーが発生してログインができないなどといった影響があります。			
対処方法	JP1/Base に記載している対処方法にて対処してください。			

■JP1/Operations Analytics

品名		形名	バージョン	対応状況
JP1/Operations Analytics		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
影響内容	JP1/Operations Analytics にて JP1/Base の認証機能との連携を行っている場合かつ、JP1/Base の認証サーバで Active Directory サーバと連携してユーザ認証を行っている場合、該当ユーザでログインができなくなります。			
対処方法	JP1/Base の認証機能との連携を行っている場合は、JP1/Base に記載している対処方法にて対処してください。			

■JP1/Performance Management - Manager

品名		形名	バージョン	対応状況
JP1/Performance Management – Manager [Manager]		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
JP1/Performance Management - Manager		全形名	V8～V10 のすべて	
影響内容	JP1/Performance Management にてユーザ認証モードを JP1 認証モードにしている場合(PFM 認証モードの場合は非該当)、かつ，JP1/Base の認証サーバで Active Directory サーバと連携してユーザ認証を行っている場合、JP1/Performance Management - WebConsole のログインができなくなります。			
対処方法	(1) ユーザー認証方式を PFM 認証モードにする。 (2) ユーザー認証方式を JP1 認証モードのままとする場合は、JP1/Base に記載している対処方法を実施する。			

■JP1/Service Support、JP1/Integrated Management - Service Support

品名		形名	バージョン	対応状況
JP1/Service Support		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
JP1/Integrated Management - Service Support		全形名	10-10 以降	
影響内容	JP1/Service Support で JP1/Base の認証機能を使用しているかつ、JP1/Base の認証サーバで Active Directory サーバーと連携してユーザー認証を行っている場合、JP1/Service Support へのログインができなくなります。			
対処方法	JP1/Base の認証サーバを使用したログイン認証 利用する場合は、JP1/Base に記載している対処方法にて対処してください。			

■JP1/SNMP System Observer、JP1/Cm2/SNMP System Observer

品名		形名	バージョン	対応状況
JP1/SNMP System Observer		全形名	V11～V12 のすべて	JP1/Base の対処方法を参照。
JP1/Cm2/SNMP System Observer		全形名	V9～V10 のすべて	
影響内容	SSO コンソールのログインにおいてユーザ認証方式を JP1 認証方式にしている場合(SSO 認証方式の場合は非該当)、かつ、JP1/Base の認証サーバで Active Directory サーバと連携してユーザ認証を行っている場合、SSO コンソールでの参照・設定・運用を行うことができません。			
対処方法	(1) ユーザー認証方式を SSO 認証方式にする。 (2) ユーザー認証方式を JP1 認証方式のままとする場合は，JP1/Base に記載している対処方法を実施する。			

JP1/Data Highway

品名	形名	バージョン	対応状況
JP1/Data Highway - Server	全形名	10-50 以降	LDAPS での AD 連携により対処可能。
JP1/Data Highway – Server Starter Edition			

影響内容	JP1/DH - Server にて Active Directory 連携を使用している場合、Active Directory のユーザにて認証が正しく動作しなくなります。その結果、次の現象が発生します。 ●「認証システム設定」メニューから認証システムの接続確認を実施したときにログイン認証失敗エラーとなる（接続確認は代表ユーザでログインした場合のみ実施できる機能です)。 ●JP1/DH - Server にログインしようとしたときにログイン失敗エラーとなりログインができない。 ●データ送受信コマンドを実行したときにログイン失敗エラーとなりコマンド実行に失敗する。 次のすべての条件に該当する場合に本現象が発生する可能性があります。 (1) 「認証システム設定」メニューから認証システム名を選択し「編集」をクリック ● 「LDAP 認証システム編集」画面において、以下が設定されている。 ➢「基本」タブ−「サーバタイプ」に「Active Directory」が設定されている ➢「ディレクトリサーバ／認証方式」タブ−「ディレクトリサーバ設定」において、プロトコルに「ldap」が設定されている (2) 「認証ルール設定」−「認証ポリシー定義」で上記の認証システムが適用されているユーザが JP1/DH - Server にログインする。
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 「認証システム設定」メニューから認証システム名を選択し「編集」をクリックします。表示される「LDAP 認証システム編集」画面において、LDAPS(LDAP over SSL)を使用するように設定を変更してください。詳細は製品マニュアルを参照してください。 JP1/Data Highway - Server 管理者ガイド 3.5.6　認証システム設定(※) (2)　認証システムを編集する 【V12】http://itdoc.hitachi.co.jp/manuals/3021/30213D4300/HB440061.HTM 【V11】http://itdoc.hitachi.co.jp/manuals/3021/30213B4420/HB440061.HTM 【V10】http://itdoc.hitachi.co.jp/manuals/3021/3021314220/H1420068.HTM ※バージョン 10 の場合は「3.5.5　認証システム設定」

	【注意】連携する Active Directory サーバが自己署名の証明書を使用している場合は、当該証明書を JP1/DH - Server の Java のキーストアにインポートする必要があります。詳細は製品マニュアルを参照してください。 JP1/Data Highway - Server 構築・運用ガイド 5.3.4　ルート証明書の登録 【V12】http://itdoc.hitachi.co.jp/manuals/3021/30213D4100/HD410118.HTM 【V11】http://itdoc.hitachi.co.jp/manuals/3021/30213B4220/HB420117.HTM 【V10】http://itdoc.hitachi.co.jp/manuals/3021/3021314020/H1400111.HTM

JP1/IT Desktop Management 2、JP1/IT Desktop Management、Hitachi IT Operations Director

品名	形名	バージョン	対応状況
JP1/IT Desktop Management 2 - Manager	P-2642-78A4	10-50 以降	TLS を使用して AD と通信することにより対処可能。
JP1/IT Desktop Management 2 - Manager	P-2A42-78BL	11-00 以降,11-01 以降,11-10 以降,11-50 以降,11-51 以降	
JP1/IT Desktop Management 2 - Manager	P-2A42-78CL	12-00 以降	
JP1/IT Desktop Management 2 - Operations Director	P-2A42-7KBL	11-01 以降,11-10 以降,11-50 以降,11-51 以降	
JP1/IT Desktop Management 2 - Operations Director	P-2A42-7KCL	12-00 以降,12-10 以降	
Hitachi IT Operations Director	P-2642-8554	04-50 以降	
JP1/IT Desktop Management - Manager	P-2642-7394	09-50 以降,09-51 以降	SSL を使用して AD と通信することにより対処可能。
JP1/IT Desktop Management - Manager	P-2642-73A4	10-00 以降,10-01 以降,10-02 以降,10-10 以降	

影響内容	次の機能で Active Directory と連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に、Active Directory に接続できなくなります。 ・Active Directory に登録されている機器を探索する
対処方法	SSL または TLS を使用して Active Directory と連携するように設定してください。 設定手順を以下に示します。 ・管理画面の[設定]-[他システムとの接続]-[Active Directory の設定]で接続先の Active Directory を設定する際、「SSL」または「TLS」のチェックボックスをオンにする。 設定方法の詳細につきましては、ご使用バージョンの製品マニュアルを参照ください。 JP1 Version 12　JP1/IT Desktop Management 2 導入・設計ガイド 付録A.4　パラメーター一覧 (19)　Active Directory の設定のパラメーター JP1 Version 12　JP1/IT Desktop Management 2 構築ガイド 4.4.1　Active Directory と接続するための情報を設定する手順

品名	形名	バージョン	対応状況
JP1/IT Desktop Management 2 – Manager[アセットコンソール]	P-2642-78A4	10-50 以降	LDAPS での AD 連携により対処可能。
JP1/IT Desktop Management 2 – Manager[アセットコンソール]	P-2A42-78BL	11-00 以降,11-01 以降,11-10 以降,11-50 以降	
JP1/IT Desktop Management 2 – Manager[アセットコンソール]	P-2A42-78CL	12-00 以降,12-10 以降	

影響内容	次の機能で Active Directory と連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に、Active Directory に接続できなくなります。 ・アクセス定義ファイルを使用してディレクトリ情報取得 ・ログイン認証
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 LDAPS で連携する場合の手順を以下に示します。 ・アクセス定義ファイルを使用してディレクトリ情報取得を行う場合 組み込み関数$LDAPACS の CONNECT 関数の PORT 引数に 636 を指定してください。 ・ログイン認証の場合 Asset Console のセットアップの[ディレクトリサーバ連携]のポート番号に 636 を指定してください。 設定方法の詳細につきましては、ご使用バージョンの製品マニュアルを参照ください。 JP1 Version 12　JP1/IT Desktop Management 2 - Asset Console アクセス定義ファイル作成ガイド 5.　アクセス定義ファイルに記述する組み込み関数 $LDAPACS（ディレクトリ情報へのアクセス関数） JP1 Version 12　JP1/IT Desktop Management 2 - Asset Console 構築・運用ガイド 7.3.6　ディレクトリサーバ連携の設定

JP1/Navigation Platform

品名	形名	バージョン	対応状況
JP1/Navigation Platform	P-292C-4PCL	全バージョン	対策 VR 発行予定('20/7 未)。 対策 VR の適用により対処可能。
JP1/Navigation Platform for Developers	P-292C-4VCL		

影響内容	Active Directory 連携で認証に失敗します。
対処方法	今後発行予定の対策バージョンを適用してください。 対策バージョンを適用できない場合は、Microsoft 社情報※に従って、LDAP 署名および LDAP チャネルバインディングを無効化してください。 ※本文の「3．LDAP 署名および LDAP チャネルバインディングの設定変更方法」を参照してください。

JP1/NETM/Asset Information Manager

品名	形名	バージョン	対応状況
JP1/NETM/Asset Information Manager	P-2642-1N84	08-50, 08-51, 08-52	LDAPS での AD 連携により対処可能。
JP1/NETM/Asset Information Manager	P-2642-1N94	09-00, 09-01, 09-10, 09-11, 09-12, 09-50	
JP1/NETM/Asset Information Manager	P-2642-1NA4	10-10	

影響内容	次の機能で Active Directory と連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に、Active Directory に接続できなくなります。 ・アクセス定義ファイルを使用してディレクトリ情報取得 ・ログイン認証(09-12 以降)
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 LDAPS で連携する場合の手順を以下に示します。 ・アクセス定義ファイルを使用してディレクトリ情報取得を行う場合 組み込み関数$LDAPACS の CONNECT 関数の PORT 引数に 636 を指定してください。 ・ログイン認証の場合 Asset Information Manager のセットアップの[ディレクトリサーバ連携]のポート番号に 636 を指定してください。 設定方法の詳細につきましては、ご使用バージョンの製品マニュアルを参照ください。 JP1/NETM/Asset Information Manager アクセス定義ファイル作成ガイド 5. アクセス定義ファイルに記述する組み込み関数 $LDAPACS（ディレクトリ情報へのアクセス関数） JP1/NETM/Asset Information Manager 設計・構築ガイド 5.3.6 ディレクトリサーバ連携の設定

JP1/NETM/DM Manager

品名	形名	バージョン	対応状況
JP1/NETM/DM Manager	P-2642-1184	08-50, 08-51, 08-52	LDAPS での AD 連携により対処可能。
	P-2A42-1184		
JP1/NETM/DM Manager	P-2642-1194	09-00, 09-01, 09-10, 09-12, 09-50, 09-51	
	P-2A42-1194		
JP1/NETM/DM Manager	P-2W42-11A4	10-10	

影響内容	LDAP 署名/LDAP チャネルバインディング有効化後に、dcmadsync.exe コマンドによるディレクトリ情報取得が失敗するようになります。 Asset Information Manager Limited の次の機能で Active Directory と連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に、Active Directory に接続できなくなります。 ・ログイン認証(09-12 以降)
対処方法	dcmadsync.exe コマンドでディレクトリ情報を取得する際、Active Directory と LDAPS(LDAP over SSL)で接続するようにしてください。 LDAPS で接続するには、dcmadsync.exe が使用するパラメタファイルの「PORT」タグに 636 を指定してください。 パラメタファイルについては、ご使用の製品マニュアルを参照ください。 JP1/NETM/DM 運用ガイド 1 3.4.4 パラメタファイルの作成 Asset Information Manager Limited のログイン認証機能をご使用の場合は、Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 LDAPS で連携する場合の手順を以下に示します。 ・Asset Information Manager Limited のセットアップの[ディレクトリサーバ連携]のポート番号に 636 を指定してください。 設定方法の詳細につきましては、ご使用バージョンの製品マニュアルを参照ください。 JP1/NETM/DM 構築ガイド 10.2.4 ディレクトリサーバ連携の設定

JP1/Network Node Manager i、JP1/Cm2/Network Node Manager i

品名	形名	バージョン	対応状況
JP1/Network Node Manager i	P-8242-82CL	12-00	LDAPS での AD 連携により対処可能。 (Linux、HP-UX、Solaris 版は対処要。Windows 版 NNMi は対処不要)
JP1/Network Node Manager i	P-8242-82BL	11-50, 11-10, 11-00	
JP1/Network Node Manager i Advanced	P-8242-83BL	11-50, 11-10, 11-00	
JP1/Cm2/Network Node Manager i	P-8242-82A1	10-50, 10-10, 10-00	
	P-1J42-82A1		
	P-9D42-82A1		
JP1/Cm2/Network Node Manager i Advanced	P-8242-83A1	10-50, 10-10, 10-00	
	P-1J42-83A1		
	P-9D42-83A1		
JP1/Cm2/Network Node Manager i	P-9W42-8291	09-50	
	P-1J42-8291		
	P-9D42-8291		
JP1/Cm2/Network Node Manager i Advanced	P-9W42-8391	09-50	
	P-1J42-8391		
	P-9D42-8391		

影響内容	Linux、HP-UX、Solaris 版 JP1/Network Node Manager i (NNMi)で Active Directory サーバと LDAP で連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に Active Directory サーバとの LDAP 接続に失敗し、NNMi へログインできなくなります。
対処方法	Linux、HP-UX、Solaris 版 NNMi へのログインについて、Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 NNMi 側の設定については、NNMi のセットアップガイドの「12. NNMi と LDAP によるディレクトリサービスの統合」(バージョン 12 の場合)を参照ください。 12. NNMi と LDAP によるディレクトリサービスの統合 http://itdoc.hitachi.co.jp/manuals/3021/30213E0200/NNMS0214.HTM

JP1/NNMi、JP1/Cm2/NNMi を前提としている製品

■JP1/Integrated Management 2、JP1/Integrated Management - Event Gateway for Network Node Manager i

品名		形名	バージョン	対応状況
JP1/Integrated Management 2 - Event Gateway for Network Node Manager i		全形名	V12 のすべて	JP1/NNMi の対処方法を参照。
JP1/Integrated Management - Event Gateway for Network Node Manager i		全形名	09-50～V11 のすべて	
影響内容	09-50 以降の JP1/Network Node Manager i、JP1/Cm2/Network Node Manager i で Active Directory サーバと LDAP で連携している場合、JP1/Network Node Manager i, JP1/Cm2/Network Node Manager i への接続に失敗し NNMi インシデントを取得できません。			
対処方法	JP1/Network Node Manager i、JP1/Cm2/Network Node Manager i に記載している対処方法にて対処してください。			

■JP1/SNMP System Observer、JP1/Cm2/SNMP System Observer

品名		形名	バージョン	対応状況
JP1/SNMP System Observer		全形名	V11～V12 のすべて	JP1/NNMi の対処方法を参照。
JP1/Cm2/SNMP System Observer		全形名	09-50～V10 のすべて	
影響内容	09-50 以降の JP1/Network Node Manager i、JP1/Cm2/Network Node Manager i で Active Directory サーバと LDAP で連携している場合，JP1/SNMP System Observer、JP1/Cm2/SNMP System Observer が使用できません。			
対処方法	JP1/Network Node Manager i、JP1/Cm2/Network Node Manager i に記載している対処方法にて対処してください。			

JP1/Service Support

品名	形名	バージョン	対応状況
JP1/Integrated Management - Service Support	P-242C-8F94	09-50 以降	LDAPS での AD 連携により対処可能。
	P-242C-8FA4	10-00 以降	
JP1/Service Support	P-2A2C-8FBL	11-00 以降	
	P-2A2C-8FCL	12-00 以降	
JP1/Integrated Management - Service Support Starter Edition	P-242C-8LA4	10-10 以降	
	P-2A2C-8LBL	11-00 以降	
JP1/Service Support Starter Edition	P-2A2C-8LCL	12-00 以降	
JP1/Integrated Management - Service Support Advanced Edition	P-242C-8UA4	10-50	

影響内容	JP1/Service Support で Active Directory サーバと連携してユーザ認証を行っている場合、LDAP 署名/LDAP チャネルバインディング有効化後に Active Directory サーバとの接続に失敗し、JP1/Service Support にログインできなくなります。
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 JP1/Service Support 側の設定については、以下のように設定してください。 （1）JAAS 対応ユーザ管理定義ファイル（hptl_jp1_imss_ua_conf.properties）で LDAPS 接続する設定をします。 ・java.naming.provider.url.0 の設定で LDAP サーバの URL を LDAPS に変更してください。 以下に変更例を示します。 【変更前】java.naming.provider.url.0=ldap://ldap-server:389 【変更後】java.naming.provider.url.0=ldaps://ldap-server:636 なお，636 は LDAPS のポート番号です。使用しているポート番号がこの番号と異なる場合は使用しているポート番号を設定してください。 ・hptl_jp1_imss_ua_conf.properties に下記定義を追加してください。 com.cosminexus.admin.auth.ldap.attr.password.0=unicodePwd （2）証明書を登録します。 ・作成したデジタル証明書を，Active Directory がインストールされているサーバ（LDAP サーバ）に登録します。 デジタル証明書の作成，登録方法については，Active Directory のドキュメントを参照してください。 ・認証局（CA）の証明書を，JP1/Service Support に登録します。

	認証局の証明書の JP1/Service Support への登録は，付属する keytool を使用して実行できます。 keytool の実行例を次に示します。 なお，表記の都合上，複数行にわたっていますが，実際は一行で記述します。 "JP1/SS パス¥uCPSB¥jdk¥jre¥bin¥keytool.exe" -import -alias cakey -file C:¥temp¥cacer.cer -trustcacerts -keystore "JP1/SS パス¥uCPSB¥jdk¥jre¥lib¥security¥cacerts" なお，キーストアのデフォルトパスワードは「changeit」です。 コマンドの最後に信頼するか聞かれるので「y」を入力してください。 （3）設定を反映します。 JP1_SS コマンドプロンプトから jsschauthorityserver コマンドを実行し， JP1/Service Support サービスを再起動すると，設定が反映されます。 コマンド例：jsschauthorityserver -ldap AD

JP1/VERITAS NetBackup

品名	形名	バージョン	対応状況
JP1/VERITAS NetBackup 8.2	RT-1V25-LC0M40	12-00 以降	LDAPS での AD 連携により対処可能。
JP1/VERITAS NetBackup 8.1	RT-1V25-LB0M40	11-50 以降	
JP1/VERITAS NetBackup 8.0	RT-1V25-LA0M40	11-10 以降	
JP1/VERITAS NetBackup 7.7	RT-1V25-L90M40	11-00 以降	

影響内容	NetBackup または OpsCenter で Active Directory サーバと LDAP で連携している場合、LDAP 署名/LDAP チャネルバインディング有効化後に Active Directory サーバとの LDAP 接続に失敗し、LDAP 認証を使用しているユーザは Java 管理コンソール（OpsCenter の場合はブラウザ）でログインできなくなります。
対処方法	Active Directory と LDAPS(LDAP over SSL)で連携するように設定してください。 NetBackup または OpsCenter 側の設定については、製品マニュアルを参照ください。 ■NetBackup の場合 Veritas NetBackup™ Commands Reference Guide https://www.veritas.com/content/support/en_US/doc/15263389-132009154-0/v132458849-132009154 ■OpsCenter の場合 Veritas NetBackup™ OpsCenter Administrator's Guide https://www.veritas.com/content/support/en_US/doc/27537447-127427700-0/v83450486-127427700

更新履歴

日付	内容
2019/12/16	新規作成
2019/12/24	アドバイザリ ADV190023 の更新に伴い、更新プログラムのリリース時期を 「2020 年 3 月」に変更。
2020/2/10	・次の対象製品を追加。 - JP1/Data Highway - JP1/IT Desktop Management 2、JP1/IT Desktop Management、Hitachi IT Operations Director - JP1/Navigation Platform - JP1/NETM/Asset Information Manager - JP1/NETM/DM Manager - JP1/Service Support - JP1/Base の認証サーバを前提としている製品 - JP1/NNMi、JP1/Cm2/NNMi を前提としている製品 ・アドバイザリ ADV190023 の更新に伴い、タイトルを変更。

- 以上 -