- Q 「仮想マシンではライセンスの取得はできません。」のメッセー ジが表示され、ライセンスが取得できない
- A1 PC を再起動します
- A2 サービスを再起動します
- A3 Windows の機能の[Hyper-V]のチェックを外します
- A4 「仮想化ベースのセキュリティを有効にする」を「無効」にしま
- A5 Windows セキュリティの「メモリ整合性」をオフにします

スタンドアローン版レブロのライセンスは仮想マシンを中継して取得することはできません。仮想マシンでライセンスを取得 しようとすると、「仮想マシンではライセンスの取得はできません。」のメッセージが表示されます。

以下は仮想マシンでない PC で該当のメッセージが表示される場合の対処法です。対処法ごとに、ライセンスの取得が行 えるかご確認いただき、改善しない場合は次の対処法をお試しください。また、ライセンスを取得した PC でレプロを起動す る際に、「仮想マシンが検知されました(H0051)」のエラーが表示される場合も同様の方法をご確認ください。



▼A1 PC を再起動します レブロを閉じ、PC の再起動を行います。

▼A2 サービスを再起動します

PC のスタートメニューの[すべて]をクリックし、[Windows ツール]をクリックします。

1		-	-			
	Q、アプリ、設定、ドキュメントの	0検索				
	すべて		< 戻る			
	W					
	Ŵ					
	Windows 11 ユーザーナ	۲F				
	Windows セキュリティ システレ					
	Windows ツール	Ν				
		~		J		
	「艹―ビフ]たおす	助します				
2		切しより。				
2	🐞 Windows ジール			- 🗆 X		
		ユリティ → Windows ツール	~ C Windows	ソールの検索 、 ク		
	整理 ▼			II • 🛯 🕄		
	Dev Home	📷 コマンド プロンプト	🗎 Fərî	ブのデフラグと最適化		
	🔩 iSCSI イニシエーター	🕺 コントロール パネル	(S) パフォ	ーマンス モニター		
	■ ODBC データ ソース (32 ビット)	■ コンピューターの管理	📼 7 7 4)	ル名を指定して実行		
	■ ODBC データ ソース (64 ピット)	 シンボーネントサービス シュードマー 		スモニター		
	Windows Media Player Legacy		1895-1 1815-1	トナスクトラノ 変統		
	Mindows PowerShell	システム構成	□-カ.	ル セキュリティ ポリシー		
	Mindows PowerShell (x86)	■ ステップ記録ツール	🏭 印度(の管理		
	A Windows PowerShell ISE	🔗 セキュリティが強化された Windows Defer	nder ファイアウォール 👝 回復	ドライブ		
	A Windows PowerShell ISE (x86)	@ タスク スケジューラ	49 文字	コード表		
	Windows Xモリ診断	NB タスク マネージャー				
	■ イベントビューアー	"■ディスク クリーンアップ				
	34 信の項目 1 信の項目を選択			≡ □	i i	
0	Sentinel LDK L	license Manage	ər」を選択し	ます。		
3	右クリックし、「再	記動をクリック	します。			
	0 #_V7					
		A 11 - T(H)				
	ファイカル(F) 操TF(A) 表示(V)					
						_
	S 9-EX (U-1))// O 9	-ビス (ローカル)		^		4.0.00
	Sentine	LDK License Manager	名前 ② Sensor Manitoring	Sonico	記明 データを	状態
	<u> +</u>	<u>)停止</u>	Sensor Service	Service	さまざま	実行・
	<u>9-670</u>	<u>) 共走回到</u>	Sentinel LDK Licen	se Manager	Manag	宝行。
	12111		Server		開始(S)	
	Manage	icenses secured by Sentinel	Shell Hardware Det	tection	一時停止(U)	
	LDK.		Smart Card		再開(M)	
			Smart Card Device	Enumeration Se	再起動(E)	
			SNMP トラップ		すべてのタスク	(K)
			Software Protection	n –	最新の検却に	重新(F)
			Spot Verifier SQL Server VSS Wri	ter		(۲) (۲.)
			the second		1110 = 2(0)	

※「Sentinel LDK License Manager」が見つからない場合、こちらの操作は不要です。

SSDP Discoverv

拡張 標準/ ローカル コンピューター のサービス Sentinel LDK License Manager を停止して開始します。 スタートアップの種類 手動 (トリガー開始) 手動 (トリガー開始) 。 カ(トリガー開始)

。 カ (トリガー開始) i (トリガー開始)

カ (遅延開始、トリ... カ (トリガー開始)

 \square

プロパティ(R)

ヘルプ(H)

●補足説明

スタートアップの種類が「自動」になっていない場合は、「自動」に変更してください。

Sentinel L	DK License Manage	er」を右クリックし、[プロ	コパティ]から	変更できます。
ぬ サービス				– o x
ファイル(F) 操作(A)	表示(V) ヘルプ(H)			
🗢 🔿 🔲 🖾 🧔	à 📑 🛛 📷 🕨 🔳 II IV			
🔍 サービス (ローカル)	◎ サービス (ローカル)	-		
	Sentinel LDK License Manager	名前	説明 状態	スタートアップの種類
		🍓 Sensor Monitoring Service	データを	手動 (トリガー開始)
	<u>サービスの停止</u> <u>サービスの再起動</u>	Sensor Service	さまざま… 実行中	手動 (トリガー開始)
		Sentinel LDK License Manager	Manag 実行中	
	説明:	Shared PC Account Manager	開始(3) 停止(0)	(1-57)-(用))(1)
	Manages licenses secured by Sentinel	Shell Hardware Detection	一時停止(U)	
		Smart Card	再開(M)	(トリガー開始)
		Smart Card Device Enumeration Serv	再起動(E)	(トリカー開始)
		SNMP トラップ	ナバスのクラカルハ	
		Software Protection	977(0)979(K)	/ (遅延開始、トリ
		Spot Verifier	最新の情報に更新(F)	(トリガー開始)
		SQL Server VSS Writer	プロパティ(R)	
		Car SSDP Discoverv	ヘルプ(H)	
	∖拡張√標準/			
選択した項目のプロパティ	ダイアログ ボックスを開きます。			

スタートアップの種類が「自動」以外の場合、「自動」に変更してください。

コーカル コンピューター) S	entinel LDK License Manager のプロパティ	×	
全般 ログオン 回	復 依存關係		
サービス名:	haspims		
表示名:	Sentinel LDK License Manager		
説明:	Manages licenses secured by Sentinel LDK.		
		,	
実行ファイルのパス: "C:¥Program Files (x86)¥Common Files¥Aladdin Shared¥HASP¥haspIms.exe" -	n	「自動」を選択します。
スタートアップの	自動	7	
裡規(上):			
サービスの状態:	実行中		
開始(<u>S</u>)	停止(① 一時停止(<u>P</u>) 再開(<u>R</u>)		
ここでサービスを開始す	「るときに適用する開始パラメーターを指定してください。		
開始パラメーター(M):			
	OK キャンセル 適用(/	<u>4</u>)	
上記の方法で	改善しない場合は、PC の再起動を行ってく	ださし	۱ _°





▼A4「仮想化ベースのセキュリティを有効にする」を「無効」にします

キーボードの Windows マーク+R で「ファイル名を指定して実行」を開きます。

0

1	「gpedit.msc」と入力し、[OK]をクリックします
	ファイル名を指定して実行 ×
	 実行するプログラム名、または開くフォルダーやドキュメント名、インターネットリソース名を入力してください。 名前(<u>O</u>): gpedit.msc
	OK 参照(B)

。 [ローカルコンピューターポリシー]-[コンピューターの構成]-[管理用テンプレート]-[システム]-[Device Guard]を開



「仮想化ベースのセキュリティを有効にする」を右クリックし、[編集]をクリックします。

← ⇒ 2 □ ≥ 2 □ ▼				
 ✓ ¹ システム 	📔 Device Guard			
> App-V	仮想化ベースのセキュリティを有効にする	設定		
> iscsi	<u>ポリシー設定</u> の編集 へ	 Windows Defender アプリケーション制御を展 個 仮想化ベースのセキュリティを有効にする 	開する	
Kerberos	· · · · · · · · · · · · · · · · · · ·		編集(E)	
LAPS	Windows Server 2016 以降または Windows 10 以降		フィルター有効(F)	
> Invet Logon OS ポリシー	説明:		フィルター オフション(O フィルターの再適用(E)))
> IN の後#2 > IN Windows タイムサービス	仮想化ベースのセキュリティを有		すべてのタスク(K)	
Windows ファイル保護 アクセス拒否アシスタンス	効にするかどうかを指定します。		ヘルプ(H)	

4 「無効」を選択し、「適用]をクリック後、[OK]をクリックします。

	- 0
🛅 仮想化ベースのセキュリティを有効にする	前の設定(P) 次の設定(N)
○ 未構成(<u>C</u>) コメント: ○ 有効(E)	
● 無効(型) サポートされるバージョン:	Windows Server 2016 以隋または Windows 10 以降
オプション:	\J µ ⊅:
プラットフォームのビキュリティ レベルモ 重用す コードの基合性に対する 伝承化 ベースの停留 いEFI メモリ 屈性 ラーブルモ要求する Centential Guard の構成 Machine Identity Isolation Configuration ビージョン ための構成	2 使意心へつのをキュリ・毛索加にするかどうかを指定します。 使意心へつのをキュリ・モストロン・パイパーで見ていていた。 できなっア・トラング・ビスターと、「「「「「「「」」」、 になせるファードのも変であり、オワンクにしている、発展さき用いです。 になせるファードのも変であり、オワンクとしている。発展さき用いです。 しての整合性というないのであり、オワンクとしている。 しての整合性というないであり、かっち、モートラードを要信します。 この整合性というない、かっち、モートラードを要信します。 この整合性というないであり、かっち、モーションドを要信したす。 の参加ですれたいがくれていた。 いうないではないたいであり、このまた、このまう、モーションド・ になったいたいたいた。 このないたいたいたいた。 このないたいたいたいた。 このないたいたいたいた。 このないたいたいたいた。 このないたいたいたいため、 になったいたいたいため、 していたいたいたいため、 のきたいたいたいため、 のきたいたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたいため、 このないたちか、 このないたちか、 このないため、 このないため、 このないため、 このないため、 このないたちか、 このないため、 このないため、 このないたちか、 このないたちか、 このないため、 このないたちか、 このなり、

●補足説明

2

改善しない場合は、[Device Guard]で、「Windows Defender アプリケーション制御を展開する」/「ビジネス向けアプリコントロールの展開」も同様に「無効」にします。

📋 Device Guard			
Windows Defender アプリケーション制御	設定	状態	
を展開する	🔤 Windows Defender アプリケーション制御を展開する	未構成	
<u>ポリシー設定</u> の編集	三 仮想化ハースのセキュリティを有効にする	木備成	
必要条件: Windows Server 2016 以降または Windows 10 以降			
説明: Windows Defenderアプリケーション制 御の展開			
このポリシー設定を使用すると、コード整 合性ポリシーをコンピューターに展開し ステムのコンピューターでの実行を許可す		_	
10.201721-9-00美行を計刊9			

▼A5 Windows セキュリティの「メモリ整合性」をオフにします PC のスタートメニューの[すべて]をクリックし、[Windows セキュリティ]をクリックします。

Q アプリ、設定、ドキュメントの検索		
すべて		< 戻る
W		
Windows 11 ユーザーガイド		
Windows セキュリティ システム	La la	
Windows 7-70	÷	



「デバイスセキュリティ」より「コア分離」の[コア分離の詳細]をクリックします。 3 ← 😐 デバイス セキュリティ \equiv お使いのデバイスに組み込まれているセキュリティです。 Ŵ 0 🗈 コア分離 コア分離は、Windowsカーネルを保護することでデバイスを安全に保つのに役立ちま 9 コア分離の詳細 (y) ٥ 📮 セキュリティ プロセッサ トラステッド ブラットフォーム モジュール (TPM) と呼ばれるセキュリティ プロセッサにより、 お使いのデバイスに追加の暗号化が提供されています。 ÷ セキュリティ プロセッサの詳細 88 🕼 セキュア ブート ŝ

٨	「メモリ整合性」を「オフ」にします。
4	Windows thaultr X
	← ≡
	〇 コア分離
	お使いのデバイスで使用可能な、仮想化ベースのセキュリティを使用するセキュリティ機 能です。
	Xモリ整合性
	攻撃によって悪意のあるコードが高セキュリティブロセスに挿入されるのを防ぎます。
	▲ メモリ整合性はオフです。お使いのデバイスは脆弱な状態にある可能性が 無視 あります。
	 オフ 評価価報
	この機能を使用するには、メモリの整合性を有効にする必要があります。
	カーネル モード ハードウェア強制スタック保護:
	カーネル モードメモリ内のリターン アドレスを置き換えて有害なコードを起動する攻撃を

●補足説明

ネットワーク版レブロのライセンスの場合は、仮想マシンでもライセンスの取得が可能です。弊社で動作確認を行ったサービス・ソフトは弊社 HP の「レブロのリモート対応について」をご参照ください。