Tenable Vulnerability Management スキャン調整ガイド

最終更新日: 2024 年 4 月 5 日

目次

はじめに

次のガイドでは、Tenable Vulnerability Management (旧 Tenable.io) スキャン設定の各側面について説明します。また、スキャンを高速化したり、より多くのデータを含めたりするなど、目的に応じてそれらの各側面を調整する方法についても説明します。

注意: 使用するスキャンテンプレートによっては、説明されている設定の一部を調整できない場合があります。高度なネットワークスキャンテンプレートおよび高度なエージェントスキャンテンプレートを使用すると、説明されている設定の各評価タイプに該当するものをすべて調整できます。

目次

ヒント: *Tenable Vulnerability Management スキャン調整ガイド* は、英語版と日本語版があります。

考慮事項

スキャン設定は脆弱性管理のスキャン時間とパフォーマンスに重要な役割を果たしますが、他の変数がスキャン時間とパフォーマンスに影響を与える可能性があります。次の表は、スキャン時間とパフォーマンスを改善しようとする際に考慮すべき各変数を説明しています。

変数	スキャン時間への影響	影響の説明
スキャン設定	高	スキャン設定により、スキャンの深度が決まります。一般に、スキャンの深度が深くなると、スキャン全体にかかる時間も長くなります。スキャンの深度を計画する際は、次のことを考慮してください。 • Tenable Vulnerability Management はどんな種類のポートスキャンを実行しているか • Tenable Vulnerability Management はどのポートをスキャンするか • どんな脆弱性をスキャンするか • 認証スキャンを実行しているか • マルウェアチェック、ファイルシステムチェック、設定監査などを行うか Tenable 提供のテンプレートを使用して、ターゲットを絞ったチェックと包括的なチェックの両方を実行できます。カスタムポリシーを作成して、設定可能なすべてのポリシー設定をカスタマイズすることもできます。
利用可能なスキャナーリソース	高	ネットワークスキャンで同時に評価できる IP アドレスの数は、次の 2 つの要素に大きく依存します。 • スキャンジョブに利用可能な Nessus スキャナーの数 • 内部 Nessus スキャナーが利用可能なリソース これらのいずれかまたは両方の要素を増やすことが、同時に行われる評価の速度および全体のスキャン時間を改善するための一番の早道です。しかし、大規模エンタープライズネットワークには多くの場合、これらのリソースをある最大値以上に増やすことを妨げるインフラまたは技術上の制約があります。

		Nessus スキャナーが、可能な限り[ハードウェア要件]を満たすようにしてください。最小要件*を超える*と、スキャナーはより多くのターゲットをより速く評価できます。 **注意:** 一部のクラウドスキャナー設定は変更できません。
評価のタイプ	中	環境内にある資産を評価するために利用できるさまざまなオプションがあります。正しいスキャン設定は環境によって異なります。所属している企業の資産または環境に最も効率的なスキャン設定を構築してください。例 • スキャナーに対してローカルでないリモートシステムには、Agents を使用する • クラウドが提供する仮想マシンには、[ネイティブのクラウド評価テクノロジー]を使用する
稼働ホストの数	中	稼働していないホストのスキャンは、稼働しているホストのスキャンよりも時間がかかりません。関連するホストの数が少ない IP アドレスの分布は、ホストの数が多い IP アドレスの分布よりもスキャン時間が短くなります。 特定のスキャンジョブのユースケースに応じて、IP の全範囲をスキャンするか、特定の IP をターゲットにするかを選択できます。詳細については、[一般]を参照してください。
ターゲット設定	中	ネットワークサービスがほとんど公開されていないロックダウンされたシステムのスキャンは、複雑なターゲットの設定に比べて時間がかかりません。たとえば、ウェブサーバー、データベース、ホスト侵入防止ソフトを搭載した Windows サーバーは、Windows 11 ワークステーションよりもスキャンに時間がかかります。
ターゲットとスキャナーの距離	中	Tenable では、スキャナーをターゲットの近くに配置し、最小のレイテンシで接続することを推奨しています (詳細については、次の Tenable ブログ記事を参照してください)。レイテンシは、スキャナーとそのターゲットとの間で交換されるすべてのパケットに付加的に影響します。ネットワークレイテンシと同時実行のプラグインチェックが、最も大きな影響を与えることが多いです。 例 • ルーター、VPN、ロードバランサー、ファイヤーウォールを経由してスキャ

		ンを行うと、開いているはずのポートがブロックされたり、閉じたポートに自動応答したりして、スキャン結果の忠実度に影響を与えることがあります。 • 単一のネットワークインフラの背後にある多数のホストをスキャンすると、スキャナーとホストの間の大量のセッション交換により、装置の負荷が増大する可能性があります。
曜日と時間	低	多くの環境では、インフラの負荷が高くなる期間があります。これらの時間帯を外して評価をスケジュールすると、スキャンのパフォーマンスが向上する場合があります。
ターゲットとなるリソース	低	スキャンターゲットに利用可能なリソースも、スキャン時間に影響を与える可能性があります。一般公開されているシステム(負荷のあるシステム)の方が、利用されていないバックアップシステムよりも、スキャンに必要な時間は長くなります。

センサーの選択

Tenable Vulnerability Management では、Tenable のクラウドスキャナー、Nessus スキャナー、Nessus Agents の 3 つのセンサータイプのいずれかでスキャンできます。

ネットワーク外部の資産をスキャンする必要がある場合は、クラウドスキャナーの使用を Tenable は推奨しています。クラウドスキャナーは Tenable によって管理され、企業で維持管理する必要がありません。詳細は、クラウドセンサーを参照してください。

ネットワーク内の資産は、Nessus スキャナーか Tenable Nessus Agents のいずれかでスキャンすることができます。次の表では、Nessus スキャナーと Nessus Agent によるスキャンの主な違いについて説明します。

Nessus スキャナー	
長所	短所
• Tenable Nessus スキャナーはネットワーク全体をスキャンできますが、Tenable Nessus Agents は Nessus Agent がインストールされている資産のみをスキャンします。 • Tenable Nessus スキャナーを使用すると、外部およびリモートのセキュリティチェックを実行できます。 • Tenable Nessus Agents とは異なり、Nessus スキャナーは、ポートスキャニングなどの機能を通じて、ネットワークの「外からの視点」を提供します。認証情報を使用して設定すると、Nessus スキャナーはネットワークの「中からの視点」も提供できます。	• Tenable Nessus Agents とは異なり、Nessus スキャナーの認証情報は手動で更新する必要があります。そのため、企業が認証情報を適宜更新しない場合、アクセス許可とログインの問題が発生する可能性があります。 • 通常、Nessus スキャナーでのネットワークスキャンは、Tenable Nessus Agents で個々の資産をスキャンするよりも時間がかかります。
Tenable Nessus Agents	
長所	短所
• Tenable Nessus Agents はターゲット資産に直接インストールされるため、Tenable Nessus スキャナーとは異なり、管理された認証情報を	• Tenable Nessus Agents はネットワークチェックを実行するように設計されていません。そのため、エージェントス

必要としません。 • Nessus スキャナーとは異なり、Tenable Nessus Agents の地理的な配置について心配する必要はありません。 • 一般に、Tenable Nessus Agents で個々の資産をスキャンする方が、ネットワーク全体をスキャンするよりもはるかに高速です。 • エージェントはインターネットにアクセスできるため、Tenable Nessus Agents は資産データを収集して Tenable Vulnerability Management に送信できます。つまり、Tenable Nessus Agents を使用すると、企業ネットワークに接続されていない資産をスキャンできます。	キャンのみを実行する場合、特定のプラグイン項目はチェックできません。 • Tenable Nessus Agents は、DB サーバーへのログイン、デフォルトの認証情報の試行、トラフィック関連の情報抽出など、リモート接続を必要とするセキュリティチェックを実行できません。 • Tenable Nessus スキャナーとは異なり、Tenable Nessus Agent スキャンは Tenable Nessus Agent がインストールされていない資産をスキャンできません。

最終的には、環境やビジネス要件に最適なセンサーを使用することを Tenable は推奨します。多くの場合、さまざまなシステムの種類やネットワークの部分に対して、エージェントとネットワーク評価の両方を使用する必要があります。エージェントスキャンの利点と制限の詳細については、*Nessus Agent ユーザーガイド*の利点と制限を参照してください。

スキャンテンプレートの選択

Tenable Vulnerability Management には、さまざまなビジネスニーズに対応したスキャナーと Nessus Agent のスキャンテンプレートが各種用意されています。Tenable Vulnerability Management のスキャンテンプレートには、4 つのカテゴリ(脆弱性スキャン、設定スキャン、戦術スキャン、インベントリコレクション)があります。ユーザーインターフェースで Vulnerability Management スキャンを作成すると、Tenable Vulnerability Management のスキャンテンプレートがすべて表示されます。

次のスキャンテンプレートカテゴリをクリックして、説明を表示します。特定のスキャンテンプレートの詳細については、スキャンテンプレートを参照してください。

> **注意:** クラウドスキャナーまたは Nessus スキャナーを使用するように Nessus スキャナーテンプレートを設定できます。

脆弱性スキャン

Tenable では、所属する企業の標準的な日常のスキャンニーズのほとんどで、脆弱性スキャンテンプレートを使用することを推奨しています。Tenable Vulnerability Management の特に注目すべき脆弱性スキャンテンプレートには以下のものがあります。

- 高度なネットワーク/エージェントスキャン - Tenable Vulnerability Management が提供する最も設定しやすいスキャンタイプです。このスキャンテンプレートを、特定のポリシーと一致するように、または特定の資産を検索するように設定できます。これらのテンプレートのデフォルト設定は基本的なネットワーク/エージェントスキャンと同じですが、追加のオプションを設定可能です。

  > **注意:** 高度なスキャンテンプレートを使うと、Tenable Vulnerability Management のエキスパートは、高速または低速チェックといったカスタム設定によって詳細なスキャンを行えますが、設定を誤ると、資産の停止やネットワークの過負荷が引き起こされる場合があります。高度なテンプレートは注意深く使用してください。

- 基本的なネットワーク/エージェントスキャン - Tenable Vulnerability Management のデフォルトのプラグインをすべて有効にしたシステムのスキャンには、このテンプレートを使用します。これは、脆弱性を見つけるためにシステムをすばやく簡単にスキャンできる方法です。

- 認証パッチ監査 (Nessus スキャナーのみ) - 認証情報付きのこのテンプレートを使用して、スキャナーがホストに直接アクセスし、ターゲットホストをスキャンし、欠落しているパッチ更新を列挙できるようにします。

- ホスト検出 (Nessus スキャナーのみ) - このスキャンを起動して、ネットワーク上のホストと該当する関連情報 (IP アドレス、FQDN、オペレーティングシステム、開いているポートなど) を確認します。ホストのリストを取得した後、各脆弱性スキャンでターゲットにするホストを選択できます。

  Tenable では、Tenable Nessus Network Monitor などのパッシブネットワーク監視のない企業がこのスキャンを毎週実行し、ネットワーク上の新しい資産を検出することを推奨しています。

  > **注意:** 検出スキャンによって特定された資産は、ライセンスに対してカウントされません。

設定スキャン

Tenable では、設定スキャンテンプレートを使用して、ホスト設定が各種業界標準に準拠しているかどうかをチェックすることを推奨しています。設定スキャンは、*コンプライアンススキャン*と呼ばれることもあります。コンプライアンススキャンが実行できるチェックの詳細については、脆弱性管理スキャンのコンプライアンスおよび脆弱性管理スキャンの SCAP 設定を参照してください。

タクティカルスキャン

Tenable は、タクティカルスキャンテンプレートを使用して、特定の脆弱性または脆弱性のグループをネットワークでスキャンすることを推奨しています。

タクティカルスキャンは軽量でタイムリーなスキャンテンプレートであり、特定の脆弱性に対して資産をスキャンするために使用できます。Tenable では、Tenable Vulnerability Management タクティカルスキャンライブラリを頻繁に更新し、一般に関心のある最新の脆弱性を検出するテンプレートを追加しています。

インベントリコレクション (Nessus Agent のみ)

標準の Tenable Nessus Agent 脆弱性スキャンとは異なり、インベントリ収集テンプレートは Tenable の Frictionless Assessment テクノロジーを使用して、より高速なスキャン結果を提供し、スキャンのシステムフットプリントを削減します。エージェントベースのインベントリスキャンは、ホストから基本情報を収集し、それを Tenable Vulnerability Management にアップロードします。その後、Tenable Vulnerability Management は、Tenable がカバレッジをリリースする際に、不足しているパッチおよび脆弱性に対して情報を分析します。これにより、ターゲットホストのパフォーマンスへの影響が軽減されると同時に、アナリストが最新パッチの影響を確認する時間を減らすことができます。詳細については、Tenable 提供の Nessus Agent テンプレートを参照してください。

設定

スキャンに使用するスキャンテンプレートを選択した後、いくつかの設定により、スキャン設定のパフォーマンスを調整できます。続くトピックでは、スキャン設定の各セクション(設定、認証情報、コンプライアンス、プラグイン)と、スキャンのパフォーマンスを最大化するための設定方法について説明します。

> **注意:** 選択するスキャンテンプレートによっては、説明されている設定やセクションの一部を表示できない場合があります。たとえば、ほとんどのスキャンテンプレートでは、プラグインファミリーを設定できません。

スキャン設定は、スキャンの機能、パフォーマンス、スキャン時間に大きく影響します。設定を使用して、Tenable Vulnerability Management がスキャンを起動するタイミングと頻度、検出オプション、デバッグ機能、評価方法、パフォーマンスオプション、その他のスキャン動作を設定します。Tenable Vulnerability Management は、設定を 5 つのカテゴリ(*基本*、*検出*、*評価*、*レポート*、*詳細*)に分類します。

スキャン設定の中には、情報提供を目的としたものや、スキャンパフォーマンスに影響を与えないものがあります(名前、説明、通知設定など)。このセクションでは、スキャンパフォーマンスに*影響する*すべての設定と、スキャンパフォーマンスを向上するための調整方法について説明します。

以下の設定カテゴリをクリックして、各カテゴリの詳細と調整方法を確認してください。

基本

基本設定では、スキャンを実行するセンサー、センサーがスキャンするターゲット/資産、Tenable Vulnerability Management がスキャンを起動するスケジュールを選択します。これら 3 つの側面はすべて、スキャンの範囲とパフォーマンスに大きな影響を与えます。

設定	説明	調整のヒント
一般 (Nessus スキャナーテンプレートのみ)		
スキャナータイプ	ローカルの内部スキャナーとクラウド管理対象スキャナーのどちらでスキャンを実行するかを指定し、**スキャナー**設定の選択リストに、ローカルスキャナーとクラウド管理対象スキャナーのどちらを表示するかを決めます。	内部 Nessus スキャナーは、Tenable のクラウドスキャナーよりも常に優れたパフォーマンスと調整機能

		を提供できる可能性があります。
スキャナー	スキャンを実行するスキャナーを指定します。 スキャンするターゲットの場所に応じて、スキャナーを選択します。例 • リンクされたスキャナーを選択して、ルーティング不可能なIPアドレスをスキャンします。 **注意:** クラウドスキャナーの場合、自動選択は使用できません。 • 次の場合は、スキャナーグループを選択してください。 ◦ 複数のスキャナーの間でスキャンの負荷を分散し、スキャンスピードを上げる場合 ◦ スキャン設定でスキャナーの指定を更新する必要なしに、将来スキャナーを再構築して新しいスキャナーをリンクする場合 • ターゲットに対してスキャンのルーティングを有効にするには、**[自動選択]**を選択してください。	スキャナーグループをターゲットにして複数のスキャナーを使用すると、より短い時間でスキャンでき、スキャナーが応答しない場合にスキャナーをフェイルオーバーすることができます。
ネットワーク、ターゲットグループ、ターゲット、ターゲットのアップロード、タグ	スキャンを実行するホストを指定するには、ネットワーク、ターゲットグループ、ターゲット、ターゲットのアップロード、タグというさまざまなオプションを選択できます。	特定の資産をターゲットにすると、IP範囲またはCIDR表記をターゲットにするスキャンよりも早くスキャン結果が得られます。

スキャンウィンドウ	スキャンが自動的に停止するまでの時間枠を指定します。ドロップダウンボックスを使用して時間の間隔を選択するか、✎ をクリックしてカスタムのスキャンウィンドウを入力します。 **注意:** スキャン期間の時間枠はスキャンジョブにのみ適用されます。スキャンジョブが時間枠内で完了した後、またはスキャン期間の終了によりスキャンジョブが停止した後も、Tenable Vulnerability Management では最大 24 時間、スキャンジョブのインデックス作成が必要になる場合があります。このため、スキャン期間が過ぎても、スキャンが **[完了]** と表示されない場合があります。Tenable Vulnerability Management がスキャンのインデックスを作成し終わると、**[完了]** と表示されます。	スキャンウィンドウは、特殊な環境や保守作業期間にスキャンを制限する場合に役立ちます。
スキャンタイプ (Nessus Agent テンプレートのみ)		

スキャンタイプ	スキャンウィンドウまたはトリガーに基づいて、エージェントスキャンを実行するかどうかを指定します。
	
	• **スキャンウィンドウ** - 脆弱性レポートでエージェントがレポートを行う時間枠を指定します。ドロップダウンボックスを使用して時間の間隔を選択するか、✎ をクリックしてカスタムのスキャンウィンドウを入力します。
	
	ウィンドウスキャンは明示的に起動するか、特定の時間に起動するようにスケジュールする必要があります。
	
	• **トリガーによるスキャン** - エージェントがレポートを行うためのトリガーを指定します。ドロップダウンボックスで、次のトリガータイプから選択します。
	
	  • **Interval** - 各スキャン間の時間間隔 (時間) (たとえば、**12** 時間ごと)
	
	  • **ファイル名** - エージェントのスキャンをトリガーするファイル名。Tenable Vulnerability Management が[トリガーディレクトリ]でファイル名を検出すると、スキャンがトリガーされます。
	
	ヒント: 1 回のスキャンに複数のトリガーを設定すると、スキャ	

	ンはリストされた順序でトリガーを検索します(つまり、スキャンが1番目のトリガーで起動しない場合は、2番目のトリガーを検索します)。 **注意:** エージェントはトリガーされたスキャンを自動的に実行するため、管理者が起動したり、特定の時間に起動するようにスケジュールしたりする必要はありません。トリガーされたスキャンも、スキャン DB や UUID を生成しません。	
スケジュール		

頻度	Tenable Vulnerability Management がスキャンを開始する頻度を指定します。
	
	• **1度** – 特定の時刻にスキャンをスケジュールします。
	• **日単位** – 1~20 日ごとの特定の時刻にスキャンを行うようスケジュールします。
	• **週単位** – 1~20 週間ごとの特定の曜日と時刻にスキャンを行うようスケジュールします。
	• **月単位** – 1~20 か月ごとに、以下の指定に従ってスキャンを行うようスケジュールします。
	  • **月の特定の日** – 毎月、特定の日付の選択した時刻にスキャンが繰り返されます。たとえば、開始日を10月3日と選択した場合、翌月以降、毎月3日の選択した時刻にスキャンが繰り返し実行されます。
	  • **月の特定の週** – 毎月、特定の週の曜日にスキャンが繰り返されます。たとえば、開始日を月の第一月曜日にした場合、翌月以降、毎月第一月曜日の選択した時刻にスキャンが実行されます。
	
	注意: 毎月、同じ日時でスキャンするようスケジュールする場合、Tenable では、開始日を28日以前に設定することを推奨します。一部の月に存在しない日付(例: 29日)を開始日に選択した場合、Tenable Vulnerability Management
		Tenable は、ほとんどの種類の資産に対して、少なくとも週に2回フル脆弱性スキャンを実行することを推奨しています。

	は、それらの日にはスキャンを実行できません。 • **年単位** – 1 ~ 20 年ごとの特定の日時にスキャンの実行をスケジュールします。	
開始	スキャンを開始する正確な日時を指定します。 デフォルトでは、開始日はスキャンを作成する日付になっています。開始時間は、最も近い 30 分単位の時間になります。たとえば、2018 年 9 月 31 日の午前 9 時 12 分にスキャンを作成した場合、Tenable Vulnerability Management はデフォルトの開始日時を *2018 年 9 月 31 日の 9 時 30 分*に設定します。	
タイムゾーン	**[開始]** の値セットのタイムゾーンを指定します。	

詳細については、脆弱性管理スキャンの基本設定を参照してください。

検出

検出設定では、スキャン設定の検出関連機能 (ホスト検出、ポートスキャニング、サービス検出) を指定できます。

エージェントはリモートチェックやネットワークのスキャンを行えないため、検出設定は Nessus Agent スキャンテンプレートに対して制限されています。エージェントスキャンの WMI と SSH の設定のみを行えます。

設定	説明	調整のヒント
ホスト検出		
リモートホストに ping	[オン] に設定すると、ホストがアクティブかどうかを確認するために、スキャナーはリモートホストの複数のポートに ping を送信します。追加のオプション **[全般設定]** と **[ping メソッド]** が表示されます。 [オフ] に設定すると、スキャン時にスキャナーはリモートホストの複数のポートに ping を送信しません。 **注意:** VMware ゲストシステムをスキャンするには、**[リモートホストの ping]** を **[オフ]** に設定する必要があります。	

応答しないホストのスキャン	Nessus スキャナーが ping メソッドに応答しないホストをスキャンするかどうかを指定します。このオプションは、PCI 四半期外部スキャンテンプレートを使用するスキャンでのみ使用できます。	
高速ネットワーク検出を使用 (リモートホストの Ping が有効な場合に利用可能)	無効になっている場合、ホストが ping に応答した際に Tenable Vulnerability Management は、誤検出を回避するために追加のテストを実行して、応答がプロキシやロードバランサーからのものでないことを確認します。これらのチェックは、特にリモートホストがファイヤーウォールで保護されている場合には時間が掛かります。 有効にすると、Tenable Vulnerability Management はこれらのチェックを行いません。	この設定によりスキャンの速度が上がる可能性がありますが、ターゲットの設定により、すべての環境で適切であるとは限りません。
Ping メソッド (リモートホストの Ping が有効な場合に利用可能)	センサーの ping メソッドを指定します。	ほとんどの環境で、Tenable はデフォルトの ping メソッドの使用を推奨しています。UDP を有効にすると、スキャン時間が大幅に増える可能性があります。詳細については、Ping タイプの順序/階層のコミュニティ記事を参照してください。
脆弱なデバイス	1 つまたは複数のスキャナーが検出する脆弱なデバイスを指定します。ネットワークプリンター、Novell NetWare ホスト、オペレーショナルテクノロジー (OT) デバイスのス	Tenable は、本番環境で脆弱

	キャンを有効にできます。	なデバイスをスキャンすることは、運用に影響を与える可能性があるため推奨していません。OT デバイスを評価する必要がある場合は、OT Security を使用して詳細な評価を実行することを検討してください。
ウェイクオン LAN	Wake-on-LAN (WOL) メニューでは、スキャンを実行する前に WOL マジックパケットを送信するホストを制御します。スキャンの前に起動するホストのリストは、1 行ごとに 1 つの MAC が記載されたテキストファイルをアップロードして指定できます。	
ポートスキャン		
スキャンされていないポートを閉じていると見なす	有効にすると、ポートが選択されたポートスキャナーでスキャンされていない場合 (たとえば、ポートが指定された範囲から外れている場合)、スキャナーはそのポートを閉じていると見なします。	
ポートのスキャン範囲	スキャンされるポートの範囲を指定します。 サポートするキーワードの値は以下のとおりです。 • [デフォルト] は、約 4,790 個のよく使用されるポートをスキャンするようにスキャナーに指示します。 • [すべて] は、ポート 0 を含む 65,536 個のポートをすべてスキャンするようにスキャナーに指示します。	ネットワーク内のローカルクロストラフィックを把握している場合は、この設定を調整して、ネットワーク上のア

	また、コンマ区切りのポートリストまたはポート範囲を使用して、カスタムリストを指定することもできます。たとえば、「21,23,25,80,110」または「1-1024,8080,9000-9200」と入力します。ポート 0 以外のすべてのポートをスキャンする場合は、「1-65535」と入力します。 ポートスキャンに指定したカスタム範囲は、**[ネットワークポートスキャナー]** 設定グループで選択したプロトコルに適用されます。 TCP と UDP の両方をスキャンする場合は、各プロトコルに固有の分割範囲を指定できます。たとえば、同じポリシーで TCP と UDP の異なる範囲のポートをスキャンする場合は、「T:1-1024,U:300-500」と入力します。 両方のプロトコルでスキャンするポートのセットを指定したり、プロトコルごとに個別の範囲を指定したりすることもできます。たとえば、「1-1024,T:1024-65535,U:1025」と入力します。	クティブリスニングサービスのみを含めることができます。ただし、未使用のサービスがスキャンで見逃される可能性があります。
SSH (netstat)	有効にすると、スキャナーは netstat を使用して、認証された SSH ベースのスキャンを実行しながら開いているポートを特定します。 さらに、スキャナーは次のように動作します。 • **[ポートのスキャン範囲]** 設定で指定されたカスタム範囲を無視します。 • **[スキャンされていないポートを閉じていると見なす]** 設定が有効な場合には、スキャンされていないポートを引き続き閉じていると見なします。 ポート列挙子 (netstat または SNMP) が正常に機能すると、ポート範囲は すべてになります。	
WMI (netstat)	有効にすると、スキャナーは netstat を使用して、ローカルマシンから開いているポートをチェックします。このオプションを使用するには、ターゲットへの WMI 接続を介して	

	netstat コマンドを実行できる必要があります。	
SNMP	有効にすると、スキャナーは SNMP の詳細を使用して、SNMP ベースのスキャンを実行しながら開いているポートを特定します。	
ローカルポートの列挙に失敗した場合にのみネットワークポートスキャナーを実行	ローカルポート列挙子が実行されると、その資産に対してすべてのネットワークポートスキャナーが無効になります。	
ローカルポートの列挙子が検出した、開いている TCP ポートを確認	有効にすると、ローカルポートエニュメレーター (WMI や netstat など) によってポートが検出された場合、スキャナーはリモートからもそのポートが開いていることを確認します。このアプローチは、何らかの形のアクセス制御 (TCP ラッパー、ファイヤーウォールなど) が使用されているかどうかを確認するのに役立ちます。	この設定を有効にすると、スキャン時間が長くなります。
TCP	内蔵の Tenable Nessus TCP スキャナーを使用して、完全な TCP 3 ウェイハンドシェイクを利用してターゲットの開いている TCP ポートを特定します。このオプションが有効になっている場合、**[ファイヤーウォールの自動検出をオーバーライド]** オプションも設定できます。	
SYN	内蔵の Tenable Nessus SYN スキャナーを使用して、ターゲットとなるホストの開いている TCP ポートを特定します。SYN スキャンは、完全な TCP 3 ウェイハンドシェイクを開始しません。スキャナーは、SYN パケットをポートに送信して SYN-ACK 応答を待機し、応答、または応答がないことに基づいてポートの状態を判断します。 このオプションが有効になっている場合、**[ファイヤーウォールの自動検出をオーバーライド]** オプションも設定できます。	SYN スキャンは、ネットワークトラフィックが少ないため、ほとんどの状況で TCP スキャンよりも効率的です。
ファイヤーウォールの自動検出を上書	この設定は、**[TCP]** または **[SYN]** のどちらかのオプションが有効になっている場合に有効化できます。	

き	有効になっている場合、この設定は自動ファイヤーウォール検出をオーバーライドします。 この設定には、次の3 つのオプションがあります。 • **積極的な検出を使用**: ポートが閉じているように見える場合でもプラグインの実行を試みます。このオプションは、本番環境のネットワークでは使用しないことをお勧めします。 • **ソフト検出を使用**: リセットが設定される頻度を監視する機能とダウンストリームのネットワークバイスで制限が設定されているかどうかを確認する機能を無効にします。 • **検出機能を無効化**: ファイヤーウォール検出機能を無効にします。	
UDP	このオプションは、Tenable Nessus のビルトイン UDP スキャナーを使用して、ターゲット上の開いている UDP ポートを特定します。 プロトコルの性質により、ポートスキャナーが開いている UDP ポートとフィルタリングされている UDP ポートの違いを見分けるのは通常は不可能です。	UDP ポートスキャナーを有効にすると、スキャン時間が大幅に増加し、信頼できない結果が生成される可能性があります。できれば、代わりにローカルポート列挙オプションを使用することを検討してください。
サービス検出		
すべてのポートをプローブしてサービス	有効にすると、スキャナーは、**[ポートのスキャン範囲]** オプションで定義されているように、開いている各ポートをそ	

を見つける	のポートで実行されているサービスにマップしようとします。 **警告:** まれに、プロービングによって一部のサービスが中断され、予期しない副次的な影響が生じることがあります。	
SSL/TLS/DTLS サービスを検索	SSL/TLS サービスの検索時に、スキャナーがターゲットとなるホストのどのポートを検索するかを指定します。 この設定には、次の2 つのオプションがあります。 • **既知の SSL/TLS ポート** • **すべての TCP ポート**	CRL チェックを有効にすると、スキャン時間が長くなります。

詳細については、脆弱性管理スキャンの検出設定を参照してください。設定済みの検出スキャンテンプレート設定の詳細については、設定済みの検出設定を参照してください。

評価

評価セクションでは、スキャンが脆弱性を識別する方法と、センサーが特定する脆弱性を設定できます。これには、マルウェアの特定、総当たり攻撃に対するシステムの脆弱性の評価、ウェブアプリケーションの感染性が含まれます。

設定または設定グループ	説明	調整のヒント
一般		
通常の精度のオーバーライド	場合によっては、欠陥が存在するかどうかを Tenable Vulnerability Management がリモートで判断できません。パラノイアレポートが **[誤検知の可能性を表示]** に設定されている場合、リモートホストに影響を与えるか疑いがある場合でも、欠陥が都度報告されます。反対に、パラノイアの設定が **[誤検知の可能性を回避]** になっていると、リモートホストに関する不確実性の要素があるときには、Tenable Vulnerability Management は欠陥を一切報告しません。これら 2 つの設定の中間の場合は、この設定を無効にします。	
徹底的なテストの実行 (ネット	さまざまなプラグインの動作が増加します。たとえば、SMB ファイル共有を調べる場合、プラグインは 1 つではなく 3 つのディレ	この設定を有効にする

ワークが中断したり、スキャン速度に影響が及んだりする可能性があります)	クトリレベルを深く分析します。そのため、状況によってはネットワークトラフィックと分析の負荷が増加する可能性があります。より徹底的に行うことにより、スキャンによる影響は大きくなり、ネットワークが中断する可能性が高くなりますが、より有用な監査結果を得られる可能性も高くなります。	と、スキャン時間が長くなります。
アンチウイルス定義の猶予期間(日):	ウイルス対策ソフトウェアチェックの遅延の日数 (0 ~ 7) を設定します。ウイルス対策ソフトウェアチェックのメニューで、ウイルス対策の署名が期限切れになった場合に報告されるまでの猶予期間を Tenable に指定できます。Tenable のデフォルト設定では、署名の期限が切れた場合、どれほど前に更新が利用可能になったか(数時間前など)を考慮しません。このオプションでは、期限切れと報告されるまでの期間を最大 7 日間まで設定できます。	
SMTP	(Nessus スキャナーテンプレートのみ) スキャン設定で SMTP テストを有効にできます。	
総当たり (Nessus スキャナーテンプレートのみ)		
ユーザーから提供された認証情報だけを使用する	場合によっては、Tenable でデフォルトアカウントと既知のデフォルトパスワードをテストに使用できます。その場合、試行が連続で無効になる回数が多すぎると、オペレーティングシステムまたはアプリケーションでセキュリティプロトコルがトリガーされ、アカウントがロックされる可能性があります。Tenable がこのようなテストを実行しないよう、この設定はデフォルトで有効になっています。	
デフォルトアカウントをテストする (低速)	Oracle ソフトウェアの既知のデフォルトアカウントをテストします。	
SCADA (Nessus スキャナーテンプレートのみ) *これはレガシー設定であり、ほとんどの環境で変更すべきではありません。OT Security を使用して、SCADA システムを評価できます。*		
Modbus/TCP コ	Modbus は、1 の機能コードを使用して Modbus 子のコイルを	

イルアクセス	読み取ります。コイルはバイナリ出力設定を表し、通常はアクチュエーターにマッピングされます。攻撃者はコイルを読み取ることができるため、システムをプロファイルし、書き込みコイルメッセージを介して変更するレジスタの範囲を特定できます。	
ICCP/COTP TSAP アドレス指定の脆弱性	ICCP/COTP TSAP アドレス指定メニューは、可能な値を試すことにより、ICCP サーバー上の接続指向トランスポートプロトコル(COTP)トランスポート サービスアクセスポイント (TSAP) の値を決定します。	
ウェブアプリケーション (Nessus スキャナーテンプレートのみ)		
ウェブアプリケーションのスキャン	有効な場合、Nessus はウェブアプリケーションレベルのチェックを有効にします。	この設定は、ウェブアプリケーションを実行しているネットワークサービスのスキャンする場合に便利です。Tenable は、クロスサイトスクリプティングや SQL インジェクションなどの一般的なウェブアプリケーションの脆弱性をスキャンするために、Tenable Web App Scanning モジュールを使

		用することを推奨しています。詳細については、Tenable Web App Scanningスキャンの概要を参照してください。
Windows		
SMB ドメインに関する情報をリクエストする	有効にすると、ローカルユーザーの代わりにドメインユーザーが照会されます。	
ユーザー列挙メソッド	ユーザー検出に適した数のユーザー列挙メソッドを有効にできます。	
マルウェア		
マルウェアのスキャン	ターゲットホストでマルウェアをスキャンするためのポリシーを設定します。残りのマルウェアオプションを表示するには、この設定を有効にします。	
DNS 解決を無効にする	このオプションをオンにすると、Tenable はクラウドを使用してスキャン結果を既知のマルウェアと比較することができなくなります。	
カスタム Netstat IP 脅威リスト	検出する既知の不良 IP アドレスのリストを含むテキストファイルです。 ファイルの各行は、IPv4 アドレスで始める必要があります。オプションとして、IP アドレスの後にコンマを追加してその後に説明を続けると、説明を追加できます。コンマ区切りのコメントに加えて、ハッシュ区切りのコメント (# など) も使用できます。	

	注意： Tenable は、テキストファイル内のプライベート IP 範囲を検出しません。	
既知の不正な MD5 ハッシュのリストを指定する	既知の不正な MD5 ハッシュをさらに指定する、1 行に 1 つの MD5 ハッシュを含むテキストファイル。 任意でハッシュの説明を含めることもできます。その場合は、ハッシュの後にコンマを追加し、続けて説明を入力します。ターゲットのスキャンで一致するものをセンサーが見つけた場合に、スキャン結果に説明が表示されます。コンマ区切りのコメントに加えて、ハッシュ区切りのコメント (fop など) も使用できます。	
既知の正しい MD5 ハッシュのリストを指定する	既知の正しい MD5 ハッシュをさらに指定する、1 行に 1 つの MD5 ハッシュを含むテキストファイル。 任意で各ハッシュの説明を含めることもできます。その場合は、ハッシュの後にコンマを追加し、続けて説明を入力します。ハッシュの説明を入力すると、ターゲットのスキャンで一致するものをセンサーが見つけた場合に、スキャン結果に説明が表示されます。コンマ区切りのコメントに加えて、ハッシュ区切りのコメント (# など) も使用できます。	
ホストファイル許可リスト	Tenable は、システムホストファイルに侵害の兆候がないかチェックします (例：侵害された Windows システム (ホストファイルチェック) というタイトルのプラグイン ID 23910)。このオプションを使用すると、スキャン中に Tenableに無視させる IP とホスト名のリストを含むファイルをアップロードできます。通常のテキストファイルの行ごとに 1 つの IP と 1 つのホスト名 (ターゲット上のホストファイルと同じ形式) を含めます。	
Yara Rules (Yara ルール)	スキャンに適用される YARA ルールを含む .yar ファイルです。1 回のスキャンでアップロードできるファイルは 1 つのみであるため、すべてのルールを 1 つのファイルに含めてください。詳細は、yara.readthedocs.io を参照してください。	Tenable は、PE および ELF サブモジュールで定義されたもの

		を含め、ハッシュ機能を除くすべての YARA 3.4 ビルトインキーワードをサポートしています。Tenable 製品は Yara Imphash チェックをサポートしていません。
ファイルシステムのスキャン	有効にすると、Tenable はホストコンピューターのシステムディレクトリとファイルをスキャンできます。 **警告:** 10 台以上のホストを対象としたスキャンでこの設定を有効にすると、パフォーマンスが低下する可能性があります。	この設定を有効にすると、スキャン時間が長くなります。
Windows のディレクトリ([ファイルシステムのスキャン] が有効な場合に利用可能)	特定の Windows ディレクトリおよびユーザープロファイルのファイルシステムのスキャンを有効にします。	
Linux のディレクトリ([ファイルシステムのスキャン] が有効な場合に利用可能)	特定の Linux ディレクトリのファイルシステムのスキャンを有効にします。	
MacOS のディレクトリ([ファイルシステムのスキャン]	特定の macOS ディレクトリのファイルシステムのスキャンを有効にします。	

が有効な場合に利用可能)		
カスタムディレクトリ([ファイルシステムのスキャン]が有効な場合に利用可能)	マルウェアファイルスキャンでスキャンするディレクトリをリストするカスタムファイル。1 行につき 1 つのディレクトリをリストします。ルートディレクトリ(C://など)をリストしたり、変数(%Systemroot% など)を使用したりすることはできません。	
データベース(Nessus スキャナーテンプレートのみ)		
検出された SID を使用する	有効にすると、少なくとも 1 つのホスト認証情報と 1 つの Oracle データベース認証情報が設定されている場合、スキャナーはホスト認証情報を使用してターゲットのスキャンを認証してから、ローカルでの Oracle システム ID (SID) の検出を試行します。次に、指定された Oracle データベース認証情報と検出された SID の使用の認証を試行します。 スキャナーがホスト認証情報を使用してターゲットのスキャンを認証できないか、ローカルで SID を検出しない場合、スキャナーは Oracle データベース認証情報の手動で指定された SID を使用して Oracle データベースを認証します。	

詳細については、脆弱性管理スキャンの評価設定を参照してください。設定済みの評価スキャンテンプレート設定の詳細については、設定済みの評価設定を参照してください。

レポート

レポート設定は、スキャン設定に対して作成できるスキャンレポートの冗長性とフォーマットに影響を与えます。レポート設定は、スキャンのパフォーマンスには影響しません。ただし、Tenable では組織のニーズに合わせて確認し設定することを推奨しています。詳細については、脆弱性管理スキャンでのレポート設定を参照してください。

詳細

詳細セクションでは、より一般的な設定、パフォーマンスオプション、デバッグ機能を設定できます。

設定	説明	調整のヒント

一般設定 (Nessus スキャナーテンプレートのみ)		
安全なチェックを有効化	有効にすると、リモートホストに悪影響を及ぼす可能性のあるすべてのプラグインが無効になります。	Tenable は、本番環境でこの設定を無効にすることを推奨していません。プラグインにより、サービスやターゲットがクラッシュする可能性があります。ただし、この設定を無効にすると、攻撃を受けている可能性が高いシステム (インターネットに接続しているシステムなど) について、より多くのインサイトが提供される場合があります。
スキャン中に反応しなくなるホストのスキャンを停止する	有効にすると、ホストの無応答状態が検出された場合に Tenable はスキャンを停止します。この状況は、スキャン中にユーザーがPCをオフにした場合、サービス拒否プラグイン後にホストが応答を停止した場合、またはセキュリティメカニズム (IDS など) がサーバーへのトラフィックのブロックを開始した場合に発生することがあります。通常これらのマシンでスキャン	

	を継続すると、ネットワーク全体に不要なトラフィックが送信され、スキャンが遅延します。	
ランダムに IP アドレスをスキャンする	デフォルトでは、Tenable は IP アドレスのリストを順番にスキャンします。このオプションを有効にすると、Tenable は IP アドレス範囲内のホストのリストをランダムな順番でスキャンします。通常、このアプローチは大規模なスキャンでネットワークトラフィックを分散するのに役立ちます。	
検出された SSH の免責メッセージを自動的に受け入れる	有効にすると、認証スキャンが免責事項要求のある FortiOS ホストに SSH 経由で接続を試みる場合に、スキャナーが免責事項要求の了承に必要なテキスト入力を行い、スキャンを継続します。	
複数のドメイン名からなるターゲットを並列にスキャンする	無効になっている場合、ホストに負荷を掛けないよう、Tenable は単一の IP アドレスに解決される複数のターゲットを 1 つのスキャナーが同時にスキャンしないようにします。代わりに Tenable スキャナーは、IP アドレスがスキャナー上の同じスキャンタスクまたは複数のスキャンタスクに複数回現れた場合、IP アドレスのスキャンを順番に実行します。スキャン完了までの時間が長くなる可能性があります。 有効になっている場合、Tenable スキャナーは、1 つの IP アドレスに解決される複数のターゲットを同じスキャンタスク内で、または複数のスキャンタスクにまたがって同時にスキャン可能です。スキャンの完了までの時間は短くなりますが、ホストに負荷が掛かり、タイムアウトや不完全な結果になる可能性があります。	
認証スキャンするホストに一意の識別子を作成する	有効にすると、スキャナーは認証スキャンに使用する一意の識別子を作成します。	
信頼できる CA	スキャンで信頼できると見なされる CA 証明書を指定します。これにより、Tenable Vulnerability Management 環境の脆弱性であるプラグイン 51192 を発生させることなく、SSL 認	

	証に自己署名証明書を使用することができます。	
パフォーマンスオプション (Nessus スキャナーテンプレートのみ)		
ネットワーク輻輳の検出時にスキャンを減速させる	有効にすると、Tenable は、送信パケットが多すぎてネットワークパイプが限界に近づいていることを検出できます。ネットワーク輻輳を検出すると、スキャンを調整して輻輳に対応し、緩和します。輻輳が緩和されると、Tenable は自動的にネットワークパイプ内の使用可能なスペースを再び使用しようとします。	
Linux カーネル輻輳検出を使用する	この設定を有効にすると、Tenable は Linux カーネルを使用して、送信パケットが多すぎてネットワークパイプが限界に近づいていることを検出します。検出すると、Tenable はスキャンにスロットルをかけて輻輳状態を緩和します。輻輳状態が緩和すると、Tenable は自動的にネットワークパイプ内の使用可能なスペースの再使用を試みます。	
ネットワークタイムアウト (秒単位)	プラグイン内で特に指定されていない場合に、Tenable がホストからの応答を待機する時間を指定します。低速接続でスキャンしている場合、この値を高い秒数に設定しても構いません。	この設定の値を大きくすると、タイムアウトに関係するすべてのチェックに影響するため注意が必要です。スキャン時間が桁違いに長くなる可能性があります。
ホストごとの同時チェックの最大数	Tenable スキャナーが 1 つのホストに対して同時に実行するチェックの最大数を指定します。	Tenable では、この設定を調整する際にスキャンターゲットのパフォーマンスを

		監視することを推奨しています。
スキャンごとの同時ホストの最大数		この設定の値を大きくするとスキャン時間が短縮されますが、Nessus スキャナーの負荷が増加します。Nessus スキャナーで利用可能なリソースとスキャンされるシステムの数によりますが、特定の時点以降、この設定を増やすとスキャナーは能力以上のことをしようとするため、スキャンが遅くなる可能性があります。
各ホストで同時に実行できる最大 TCP セッション数	単一ホストに対して確立された TCP セッションの最大数を指定します。 この TCP スロットリングオプションは、SYN スキャナーが送信する 1 秒あたりのパケット数も制御し、その数は TCP セッション	

	の 10 倍になります。たとえば、このオプションが 15 に設定されている場合、SYN スキャナーは最大で毎秒 150 パケットを送信します。	
各スキャンで同時に実行できる最大 TCP セッション数	スキャンされるホストの数に関係なく、各スキャンタスクで確立される TCP セッションの最大数を指定します。 Windows ホストにインストールされたスキャナーの場合、正確な結果を得るには、この値を 19 以下に設定する必要があります。	
Unix の検索コマンドオプション		
ファイルパスを除外	Unix システムで find コマンドを使用して検索する、すべてのプラグインから除外するファイルパスのリストを含むプレーンテキストファイルです。 ファイルでは、Unix の find コマンド -path 引数で許可されているパターンごとにフォーマットされた、1 行ごとに 1 つのファイルパスを入力します。詳細については、find コマンドのマニュアルページを参照してください。	
ファイルシステムを除外	Unix システムで find コマンドを使用して検索するすべてのプラグインから除外するファイルシステムのリストを含むプレーンテキストファイルです。 ファイルでは、Unix の find コマンド -fstype 引数でサポートされるファイルシステムの種類を使用して、1 行ごとに 1 つのファイルシステムを入力します。詳細については、find コマンドのマニュアルページを参照してください。	
ファイルパスを含める	Unix システムで `find` コマンドを使用して検索する、すべてのプラグインから含めるファイルパスのリストを含むプレーンテキストファイルです。 ファイルでは、Unix の `find` コマンド `-path` 引数で許可されているパターンごとにフォーマットされた、1 行ごとに 1 つのファイルパスを入力します。詳細については、`find` コマンドのマニュアルページを参照してください。	

	ファイルパスを含めると、プラグインで検索される場所が増えるため、スキャンの継続時間が延びます。対象はできるだけ明確に指定してください。 **ヒント: [ファイルパスを含める]** と **[ファイルパスを除外する]** に同じファイルパスを含めないようにしてください。結果はオペレーティングシステムによって異なる場合がありますが、この競合によってファイルパスが検索から除外される可能性があります。	
デバッグ設定 **注意:** Tenable は、本番環境でデバッグ設定を有効にすることを推奨していません。デバッグ設定は大量のデータを生成し、全体的なスキャン時間とパフォーマンスに影響を与える可能性があります。Tenable は、この設定を常に使用するのではなく、特定のデバッグインスタンスにのみ使用することを推奨します。		
常に SSH コマンドを報告する	有効にすると、Tenable はホストで SSH を介して実行されるすべてのコマンドのレポートを、マシンで読み取り可能な形式で生成します。報告されたコマンドは、プラグイン 168017 の下に表示されます。 **注意:** プラグイン 168017 を無効にすると、この設定が正しく機能しません。	
プラグインのデバッグを有効化	プラグインからの利用可能なデバッグログをこのスキャンの脆弱性出力へ添付します。	
デバッグログレベル	デバッグログステートメントの冗長性と内容を制御します。	Tenable サポートが特に指示しない限り、デバッグログレベルを **レベル 3:** に設定してください。
起動されたプラグインを列挙	スキャン中に Tenable が起動したプラグインのリストを表示します。プラグイン 112154 のスキャン結果でリストを表示できます。	

	注意: プラグイン 112154 を無効にすると、この設定が正しく機能しません。	
監査証拠説明の詳細度	プラグイン監査証跡の詳細度を制御します。 次のオプションがあります。 • **監査証跡なし** - (デフォルト) Tenable はプラグイン監査証跡を生成しません。 • **すべての監査証跡データ** - スキャンにプラグインが含まれなかった理由を監査証跡に含めます。 • **スキャンエラーのみ** - スキャン時に検出したエラーのみを監査証跡に含めます。	
スキャン開始のシフト (Nessus Agent テンプレートのみ)		
最大遅延 (分)	(Agents 8.2 以降) 設定されている場合、エージェントグループ内の各エージェントは、指定された時間の値 (分) を最大値とするランダムな時間、スキャンの開始を遅らせます。同時に開始しないようにすることで、仮想マシン CPU などの共有リソースを使用するエージェントの影響を低減できます。 設定した最大遅延時間がスキャンウィンドウを超過する場合、Tenableは、スキャンウィンドウがクローズする最低 30 分前にエージェントがスキャンを開始するよう、最大遅延時間を短縮します。	この設定は、共有インフラ (仮想ホストなど) でリソースの過剰使用を防ぐのに役立ちます。
コンプライアンス出力設定		
コンプライアンスの最大出力長 (KB)	ターゲットから返される各コンプライアンスチェック値の最大出力長を制御します。コンプライアンスチェック値がこの設定の値より大きい場合、Tenable Vulnerability Management は結果を切り捨てます。 **注意:** コンプライアンススキャン処理が遅い場合、この設定の値を小さくして処理速度を向上させることを推奨します。	

詳細については、脆弱性管理スキャンの詳細設定を参照してください。設定済みの詳細スキャンテンプレート設定の詳細については、設定済みの詳細設定を参照してください。

脆弱性管理スキャン設定の詳細については、スキャン設定を参照してください。

認証情報設定

> **注意：** Tenable Nessus Agent スキャンの認証情報を設定する必要はありません。Tenable Nessus Agents は資産に直接インストールされるため、ローカルセキュリティチェックに必要なアクセス権をすでに持っています。

スキャンの認証情報設定により、組織の資産をスキャンするために Nessus スキャナーが持つ認証情報が決まります。Nessus スキャナーの認証情報（*認証スキャン*と呼ばれる）を提供することで、大規模なネットワークをスキャンすると同時に、アクセスするためにさらに認証情報が必要なローカルレベルでのエクスポージャーをスキャンできるようになります。個別のスキャン、スキャンテンプレート、グローバルな Tenable Vulnerability Management レベル（*管理された認証情報*と呼ばれる）の 3 つの異なるレベルで、認証情報をスキャナーに割り当てることができます。

一般に、スキャナーに認証情報を追加すると、より多くの資産を認証できるようになりますが、最終的にはスキャンターゲットと環境に依存します。ただし、スキャンにさらに時間がかかる可能性があります。

完全な認証スキャン完了には、より長い時間がかかる可能性があります。ただし、これは他のスキャン設定と評価されるターゲットによって異なります。一般に、完全な認証スキャンが推奨されます。これは、作成されるネットワークオーバーヘッドが少なく、リスクの特定と優先順位付けに役立つ情報が最大 10 倍多く返されるためです。

認証情報が機能するには適切な権限が必要です（詳細については、*Nessus ユーザーガイド*の Nessus 認証情報を使用したチェックを参照してください）。認証情報管理のために追加のセキュリティコントロールを提供することもできます（詳細については、スキャン認証情報を保護する方法：概要のブログ記事を参照してください）。

スキャン認証情報設定の詳細については、脆弱性管理スキャンの認証情報を参照してください。

コンプライアンス設定

コンプライアンスセクションでは、コンプライアンスチェック(監査とも呼ばれる)をスキャン設定に追加できます。コンプライアンスチェックにより、ホストがどのように設定されているか、さまざまな業界標準に準拠しているかどうかをスキャンで検出できます。Tenable の事前設定済みのコンプライアンスチェックを使用することも、カスタマイズした監査項目を作成してアップロードすることも可能です。

認証スキャンと同様に、コンプライアンスチェックを追加すると、スキャンでより多くのデータを生成できるようになりますが、そうすると全体のスキャン時間が長くなる可能性があります。

一般に、ほとんどの権限ベースのコンプライアンスチェック(たとえば、CIS や DISA からのベースライン)は、全体的なスキャン時間に大きな影響を与えません。ただし、ファイルコンテンツのチェックを有効にする監査は、ターゲットファイルシステムを検索して指摘されたパターンを探すため、通常はスキャン時間に大きな影響を与えます。

スキャンコンプライアンス設定の詳細については、脆弱性管理スキャンのコンプライアンスを参照してください。

プラグイン設定

プラグインセクションでは、スキャン設定のプラグインファミリーを有効または無効にできます。プラグインファミリーを有効または無効にすると、スキャンでどのセキュリティチェックを実行するか、または実行しないかが決まります。プラグイン設定は、スキャンが返すデータの量、およびスキャンの実行にかかる時間に大きな影響を与える可能性があります。一般に、多くのプラグインファミリーを有効にしてスキャンを行うと時間がかかりますが、多くのスキャンデータが生成されます。少ないプラグインファミリーを有効にしたスキャンは短時間で行えますが、生成されるスキャンデータは少なくなります。

スキャナーは各ターゲットに対して適切なプラグインとファミリーを自動的に実行し、各システムがスキャンされると適切なプラグインが決定されます。一般に、プラグインファミリーを広範にわたって無効化したり、デバイスごとに異なるプラグイン設定を使用してターゲットを絞ったスキャンポリシーを作成したりすることは不要で、リスクの誤認につながる可能性があるため、Tenable では推奨していません。

スキャンプラグイン設定の詳細については、脆弱性管理スキャンのプラグインを設定するを参照してください。

スキャン起動タイプ

スキャンに余計な時間がかかる原因としてよくあるのが、ターゲットを不必要に再スキャンしてしまうことです。完全な「標準」スキャンの起動に加えて、Tenable Vulnerability Management では、同じスキャン設定を使用してターゲットのより小さなサブセットをスキャンする、*カスタム開始*スキャンと*ロールオーバー*スキャンの 2 つの代替方法があります。

スキャン起動タイプ	説明
起動(標準)	通常、スキャンを起動すると、Tenable Vulnerability Management はスキャン設定で設定したターゲットのスキャン設定を起動します。 詳細は、脆弱性管理スキャンを起動するを参照してください。
カスタム開始	スキャン設定で設定されたターゲットに対してスキャンを起動する代わりに、**カスタム開始**を選択して、単一のターゲットまたはターゲットのリストをスキャンできます。Tenable は、フルスキャンを起動する前に、このオプションを使用して少数のターゲットに対してスキャン設定をテストすることを推奨します。 詳細は、脆弱性管理スキャンを起動するを参照してください。
ロールオーバーを起動	ロールオーバースキャンを起動すると、Tenable Vulnerability Management が以前にスキャンしていないターゲットに対してのみスキャンが実行されます。これは、割り当てられたすべてのターゲットを調べる前にスキャンが終了した次のような場合に発生します。 • ユーザーがスキャンを手動で停止した時 • スキャン期間の設定により、スキャンがタイムアウトした時 • スキャナーがスキャンタスクを中止するか、適切に初期化しなかった時 ロールオーバースキャンにより、すべての資産を完全にカバーするスキャンを完了できます。また、ロールオーバー機能を使用すると、ネットワークに影響を与える大規模なスキャンも分割して実行することができます。 詳細は、ロールオーバースキャンを起動するを参照してください。

その他のヒント

- **スキャンの重複を回避する** – 組織で、複数のスキャンが同じホストを不必要にスキャンするよう設定されている可能性があります。そのようなスキャンにより、重複したスキャンおよび資産データが作成される場合があります (*スキャン重複*とも呼ばれます)。これは大抵、組織が認証スキャンと非認証スキャンの設定を別々に使用して同じ資産をスキャンする場合に発生します (この場合、組織は資産に対して認証スキャンを行うだけで、認証スキャンと非認証スキャンで見つかるデータの両方を取得できます)。

  スキャン設定をレビューして、複数のスキャン設定で同じ脆弱性データを発見するために同じ資産をスキャンしていないことを確認するようおすすめします。

  > **注意:** 場合によっては、エージェントと非認証ネットワークスキャンを同じターゲットで実行することが効果的なこともあります。

- **ネットワーク設定に基づいて効果的な評価を行えるようにスキャンを設定する** – 最も効果的な方法で評価を行いたい場合、多くのシステムを同時にスキャンすることは必ずしも最善とは限りません。効果的な評価方法を決定するには、さまざまなネットワーク要因を考慮する必要があります。詳細については、パフォーマンスとリソース使用量のためのネットワーク評価の調整のブログ記事を参照してください。