STIG Viewer 2.x User Guide

Version 1, Release 7

July 2020

Developed by DISA for the DoD

内容

注意

この資料は、下記 URL の
“https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_STIGViewer_2-11_Linux.zip”に含まれる” U_STIG-_Viewer_2-x_User_Guide_July_2020.pdf”について、コンカレント日本株式会社で機械翻訳を用いて資料を作成しました。

ここに掲載している法令等の日本語訳文は、参考に供するための資料です。正確な内容については、原文による正式の文言をご確認ください。この資料の利用により生じた損害について、コンカレント日本株式会社は、一切の責任を負いません。

本資料の原文は改正される可能性があるので、その動向に注意を要することを付け加えておきます。

紹介

STIG Viewer バージョン 2.x は、以前の DISA ツール (STIG Viewer 1.2) の代わりとなります。このユーザー ガイドの目的は、2.x のナビゲーションとユーザーの視点からの機能の説明を支援することです。

DoD/DISA STIG Viewer について

DoD/DISA STIG Viewer ツールは、1 つ以上の XCCDF (拡張可能な構成チェックリスト記述形式) で書式設定された SCG を、人間が読みやすいわかりやすい形式で表示する機能を提供します。これは、DoD用にDISAによって開発され、公開されたSSTIと互換性があります。STIG Viewer の目的は、STIG コンテンツへのアクセスを容易にする直感的なグラフィカル ユーザー インターフェイスを提供し、現在の SCG を表示する方法 (Web ブラウザでスタイル シートを使用) では利用できない追加の検索および並べ替え機能を提供することです。STIG Viewerでは、次の機能を使用して追加機能もサポートしています。

- チェックリストの作成時に複数の SSTI をインポートして使用できます。
- 1 つまたは複数の XCCDF STIG ファイルを個別にロードします。
- Zip 圧縮された STIG パッケージから XCCDF STIG ファイルを抽出します。
- ユーザー構成データとインポートされた SSTI の現在のセットを格納するシステム上にローカル データ キャッシュを作成します。これにより、STIG Viewerが起動するたびに、ロードされた最後の SSTI セットの再ロードが可能になります。
- Viewerのオプションメニューからローカルデータキャッシュを削除します。STIG Viewerでは、一度に作成できるローカル データ キャッシュは 1 つだけです。
- 複数の XCCDF STIG ファイルを解凍し、zip 圧縮された STIG パッケージを持つ 1 つまたは複数のフォルダーを含む .zip ファイルから読み込むことができます。STIG Viewerは、ドリルダウンしてすべての XCCDF ファイルを見つけてロードします。この操作にはローカル データ キャッシュが必要なため、すべての XCCDF ファイルがローカル フォルダに展開されます。

- 脆弱性 ID、STIG ID、ルール ID、CCI、またはグループ/ルール名で STIG 要件/脆弱性のリストを並べ替えます。

- 1 つ以上のキーワードに基づいて、ロードされたすべての STIG ファイルを検索またはフィルタします。すべてのフィールドまたは個々のフィールドを検索し、STIG 要件/脆弱性のフィルター処理されたリストを返します。
  - 検索は、ルールタイトル、STIG ID、脆弱性ID、ルールID、重大度、またはCCIに制限される場合もあります。

- CCI 参照が STIG 要件に含まれている場合は、CCI データを表示します。

- 他のプログラム(WebブラウザやMicrosoft Word)で使用するために選択されたSTIGデータを印刷またはエクスポートします(HTMLおよびRTFファイル形式)。
  - 印刷/エクスポートされたデータは、Viewerの中央ペインに表示される要件のリストに基づいて作成され、出力は各要件を含むテーブルとしてフォーマットされます。

- 自動レビュー SCAP (セキュリティ コンテンツ自動化プロトコル) または XCCDF 結果をチェックリストにインポートし、自動結果をチェックリストに入力します。レビューの手動部分を完了し、自動化された結果に追加できます。

- チェックリストを.CSV ファイルとしてエクスポートします。
  注意: DISA は、最初に Java で STIG Viewer を開発し、Oracle Java 8 Java ランタイム環境 (JRE) で使用するために単一の JAR ファイルとして提供しました。Java 11 のリリースに伴う Java ライセンスおよび配布の変更により、DISA は Oracle JRE を必要としない ZIP ファイルにスタンドアロン STIG Viewer アプリケーションを提供するようになりました。これにより、アプリケーションは、既存のワークフローに対する中断を最小限に抑えて、Windows、Linux、および macOS を実行する 64 ビット X86 システムで実行できます。これにより、プログラムは現在ログインしているユーザーのアクセス許可レベルで実行されます。

- STIG Viewerは、ネットワーク接続を開いたり、使用したりしません。

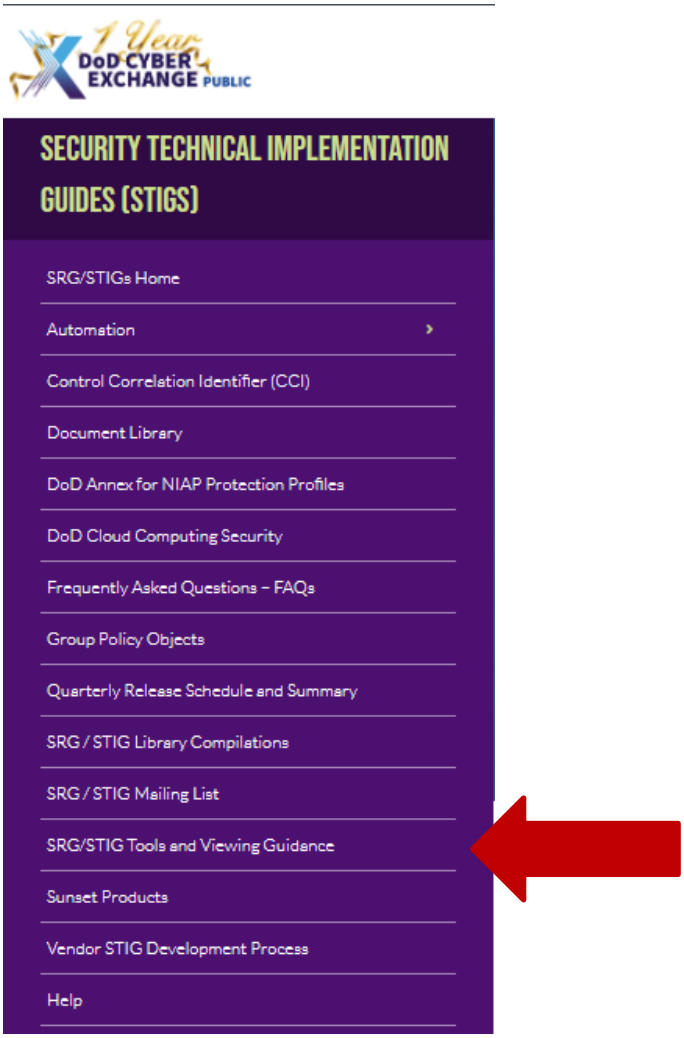
- Java は、ログインしているユーザーのローカルディレクトリにローカルデータキャッシュを作成します。これは、オペレーティング システムごとに異なる場所です。
  - Windows 10 の下では、これは次のディレクトリにあります:
    %USERPROFILE%\AppData\Local\STIGV_AppData
  - Linuxの下では、これは次のディレクトリにあります。
    $HOME/ STIGV_AppData/
    $HOME/.stigviewer.STIGViewer/
  - ローカル データ キャッシュをクリアすると、Java はフォルダとローカル データ キャッシュの両方を同時に削除します。

- STIG Viewerへの入力は、XML ファイルに含まれる XCCDF です。STIG Viewerは、他の種類のファイルを拒否します。STIG Viewerは、DISA が DoD 用に作成した XCCDF フォーマットの SSTI に最適化されています。

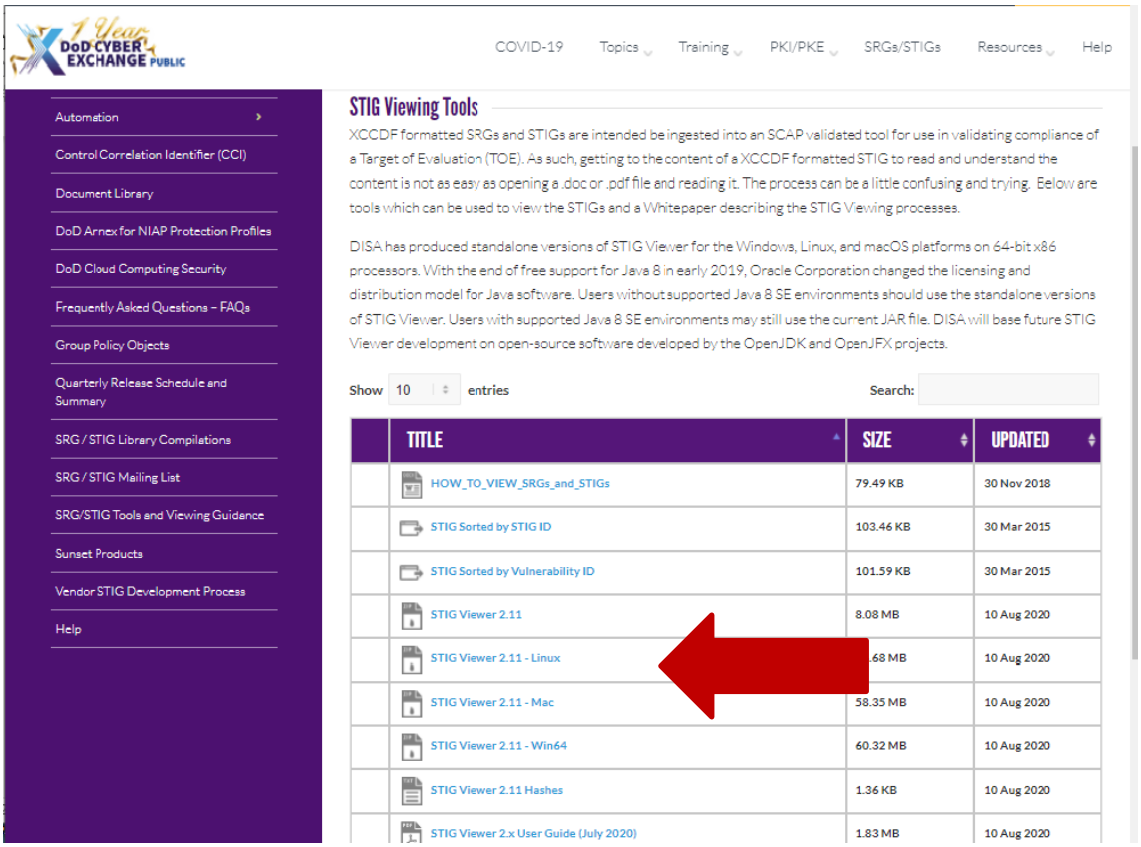
1. STIG Viewer 2.X のインストールと実行

1.1 Java JAR STIG Viewer のインストール

1. サイバーエクスチェンジ https://public.cyber.mil/ のウェブサイトから STIG Viewer 2.x ZIP ファイルをダウンロードします。SRG/SMG >> SRG/STIG ツールと表示ガイダンスに移動します。



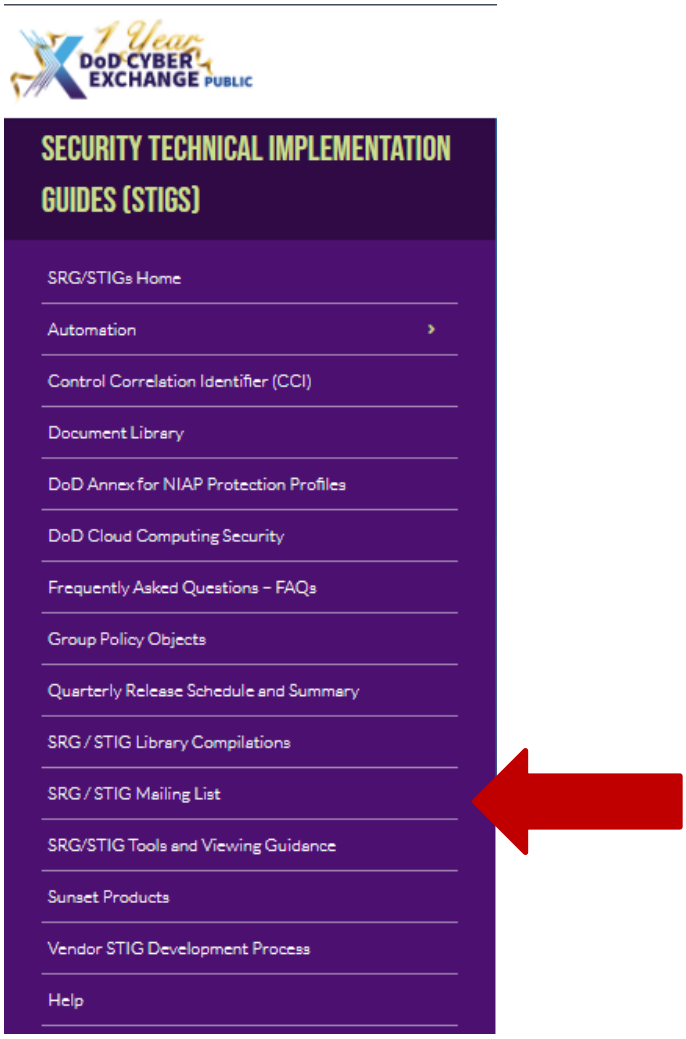
2. STIG Viewer バージョン 2.x を右クリックします。



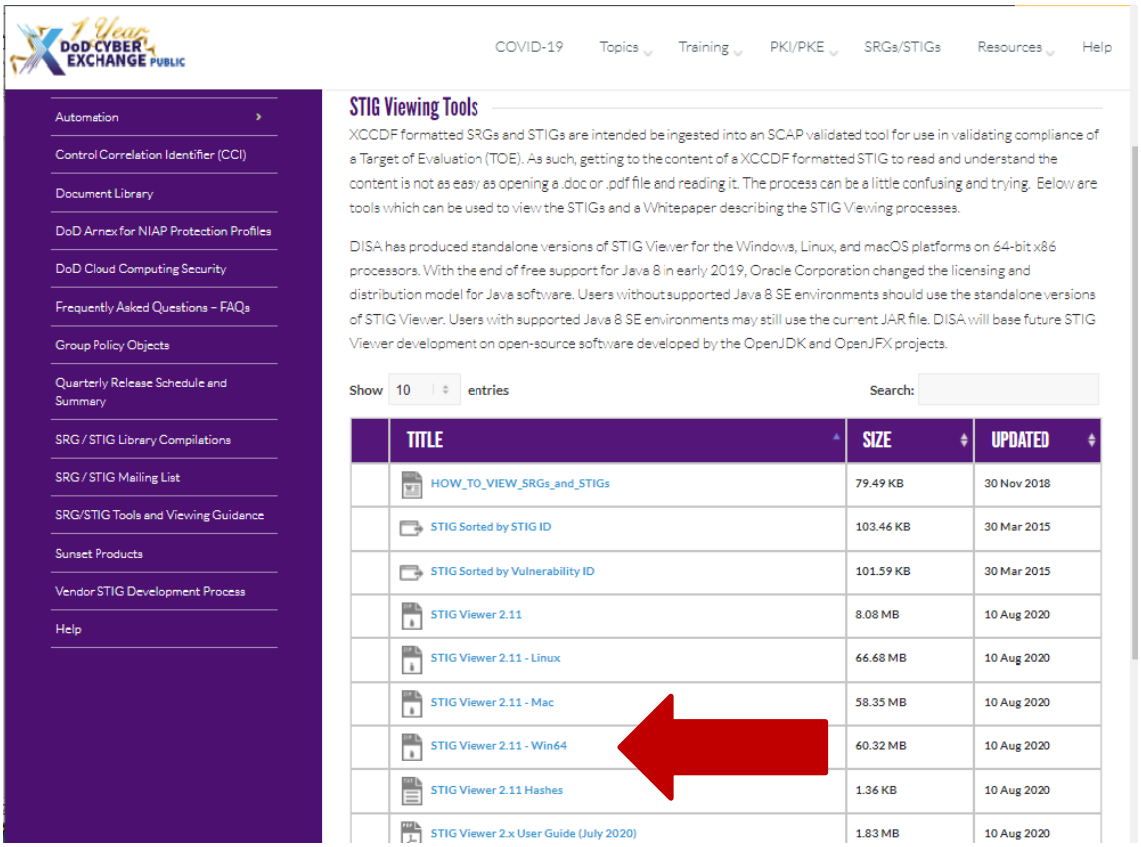
3. [ファイルの保存] をクリックして、STIGViewer2.x.zipとしてコンピュータに保存します。JAR ファイルを ZIP ファイルから直接実行するか、または後で実行するために任意の場所に抽出します。

1.2 スタンドアロン STIG Viewer のインストール

1. サイバーエクスチェンジのウェブサイトから STIG Viewer 2.x スタンドアロンの ZIP ファイルをダウンロードします。SRG/SMG >> SRG/STIG ツールと表示ガイダンスに移動します。



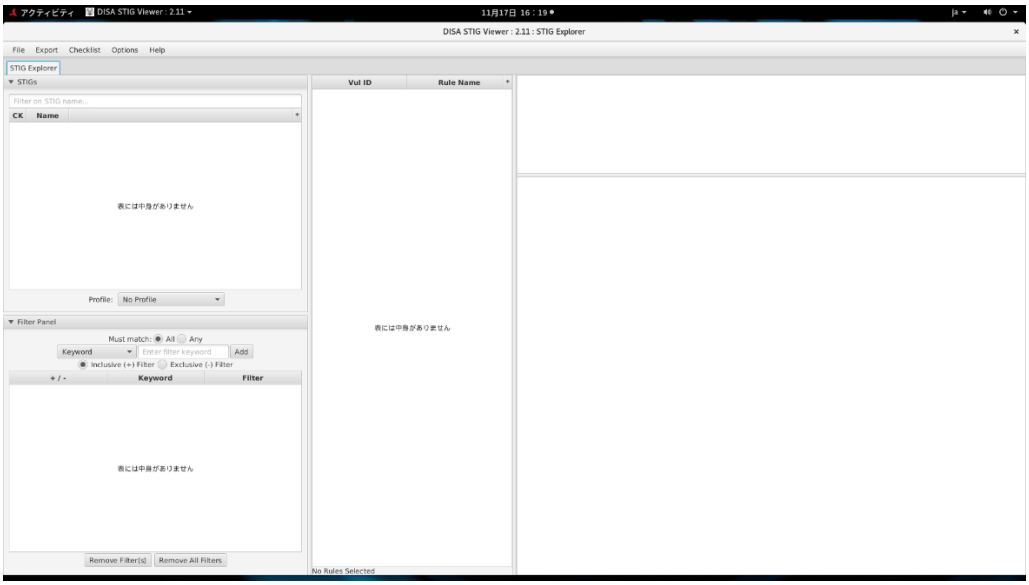
2. STIG Viewer バージョン 2.x (Windows) を右クリックします。



3. [ファイルの保存] をクリックして、STIGViewer2.x-Win64.zipとしてコンピュータに保存します。Windows 以外の ZIP ファイルは"Win64" を "Linux" または "Mac" に置き換えます。ZIP ファイルのすべての内容をローカル ハード ディスクに抽出します。スタンドアロン アプリケーションは ZIP ファイル内からは実行されません。Linux スタンドアロン STIG Viewer を実行するには、GLIBC 2.14 以降が必要です。これは、アプリケーションが RHEL 6 で実行されないことを意味します。

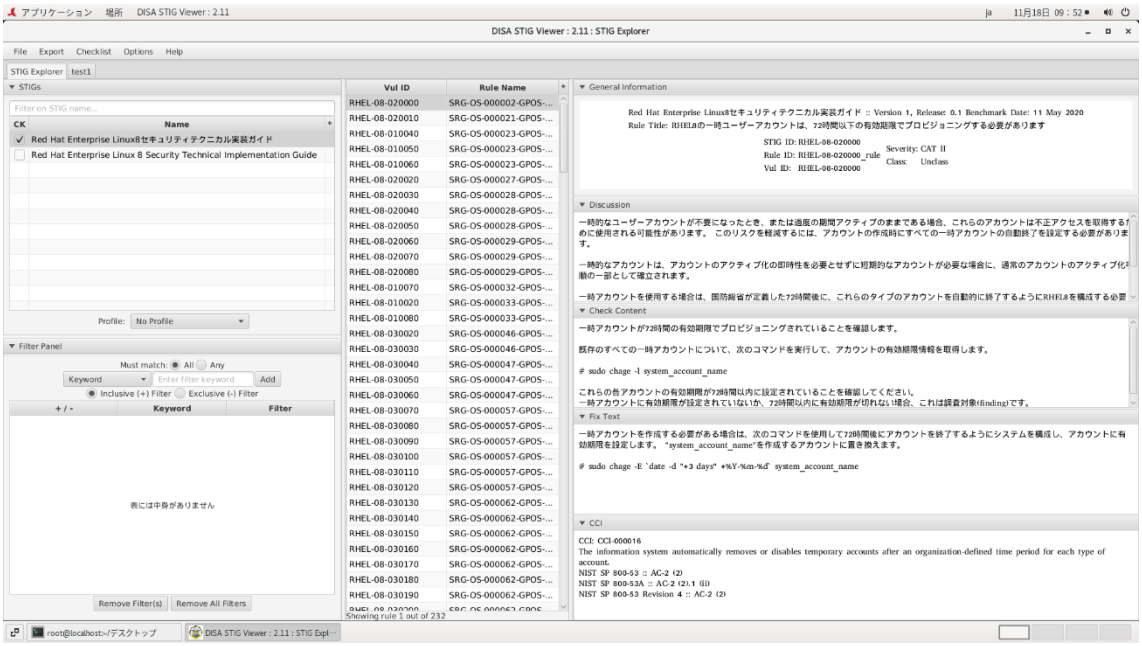
1.3 STIG Viewer を開く

1. STIGViewer2.x.jarをクリックして、Java JAR STIG Viewerを起動します。バンドルされた STIGViewer バッチ スクリプト ファイル (Windows の場合は "STIGViewer.bat" と macOS および Linux の場合は "STIGViewer" を使用して、スタンドアロン STIG Viewerをコマンド ラインから起動します。STIG Viewer のスタンドアロン バージョンをアプリケーション ファイアウォールで実行する方法については、ローカル システム管理者に問い合わせてください。起動時に空の STIG Viewerは次のようになります。

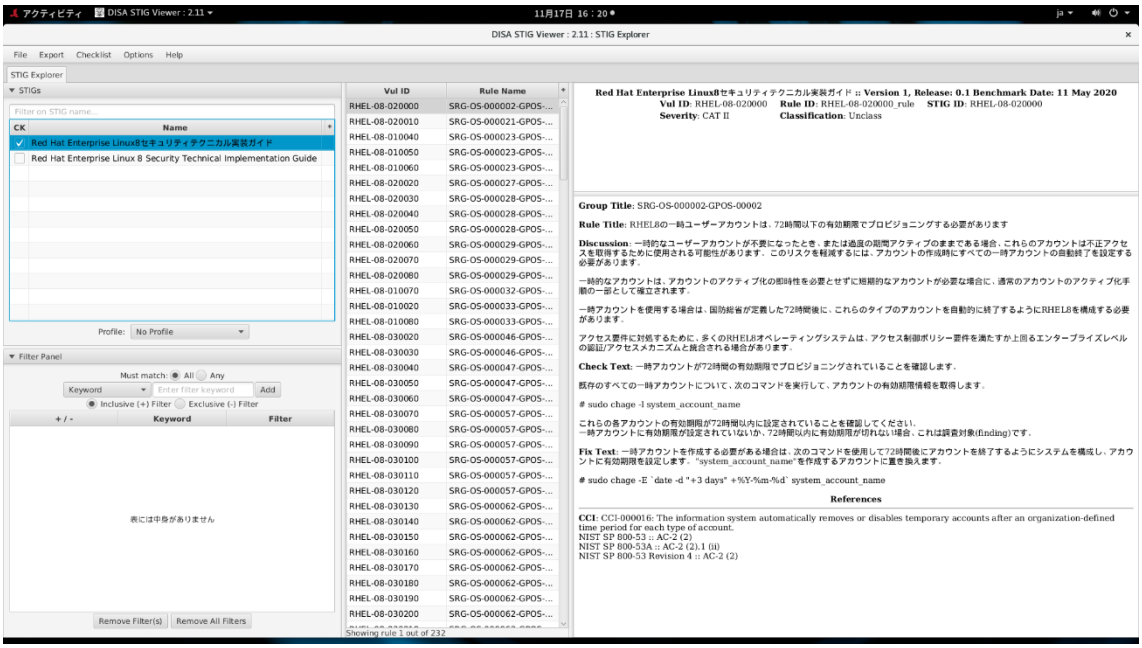


2. STIGがSTIGViewerにロードされると、設定によって外観が決まります。

SV 2.x Classic light:



Light theme:



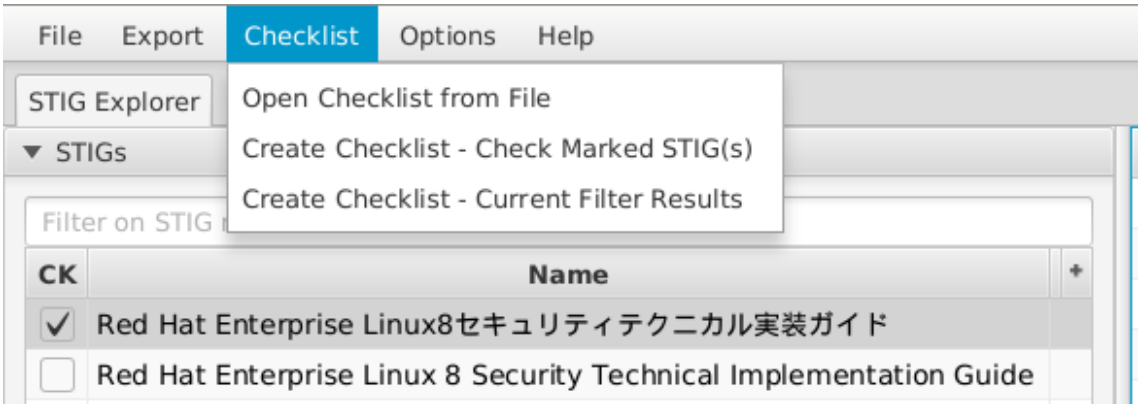
3. Viewerには、3つの主要な列があります。
   - 左側列: STIG名称とFilters
   - 中央列: 脆弱性(Vulnerability) ID 情報
   - 右側列: 脆弱性(Vulnerability)の詳細情報

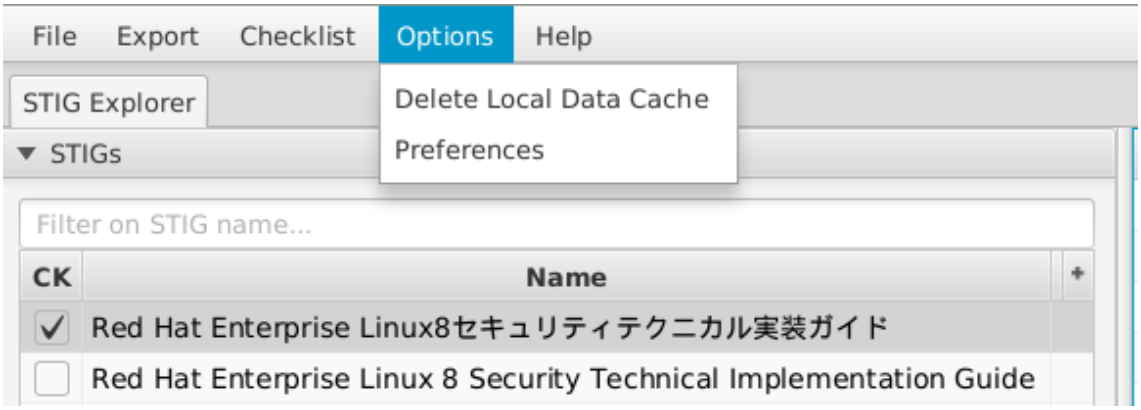
4. Classic themesでは、左右の列にはそれぞれ折りたたみ可能なセクションがあります。各セクション ラベルの左側にある小さな矢印をクリックすると、セクションが展開または折りたたまれるのが切り替わります。折りたたむセクションが多いほど、互いのセクションが高く開きます。縦方向の区切り線は、サイズを調整するためにスライドします。
   - 左側列ラベル: STIGS, Filter Panel
   - 右側列ラベル: General Information, Discussion, Check Content, Fix Text, CCI,その他
5. 非Classic themesでは、右の列の様々なセクションが2つにマージされます。

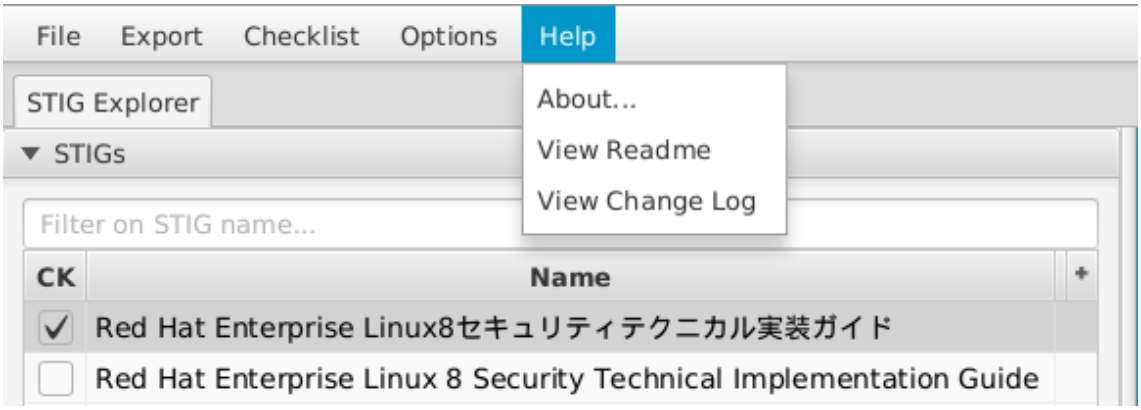
6. 上記のLight themesに加えて、同様のDark themesもあります。

1.4 STIG Viewer メニューバー

1. STIG Viewerメニューバーには、File、Export、Checklist、Option、および Help の5 つのドロップダウンメニューがあります
   各メニューの選択項目を以下に示します。




File
Export
Checklist
Options
Help
Delete Local Data Cache
Preferences
STIG Explorer
STIGs
Filter on STIG name...
CK
Name
Red Hat Enterprise Linux8セキュリティテクニカル実装ガイド
Red Hat Enterprise Linux 8 Security Technical Implementation Guide

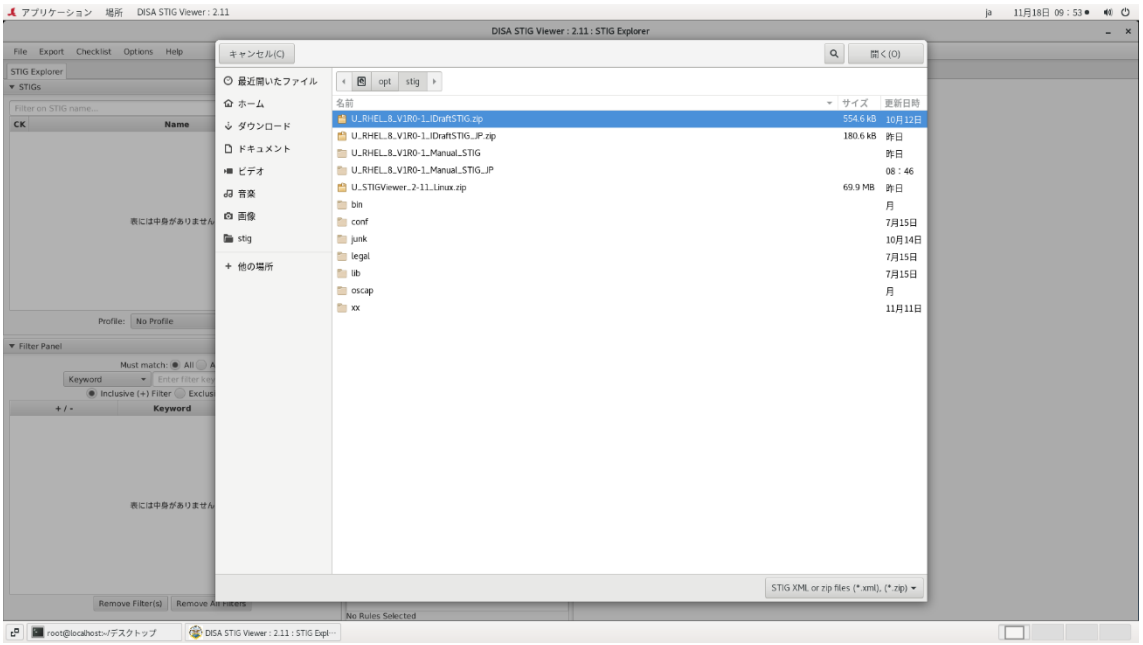

File
Export
Checklist
Options
Help
About...
View Readme
View Change Log
STIG Explorer
STIGs
Filter on STIG name...
CK
Name
Red Hat Enterprise Linux8セキュリティテクニカル実装ガイド
Red Hat Enterprise Linux 8 Security Technical Implementation Guide

2 STIG をロードする

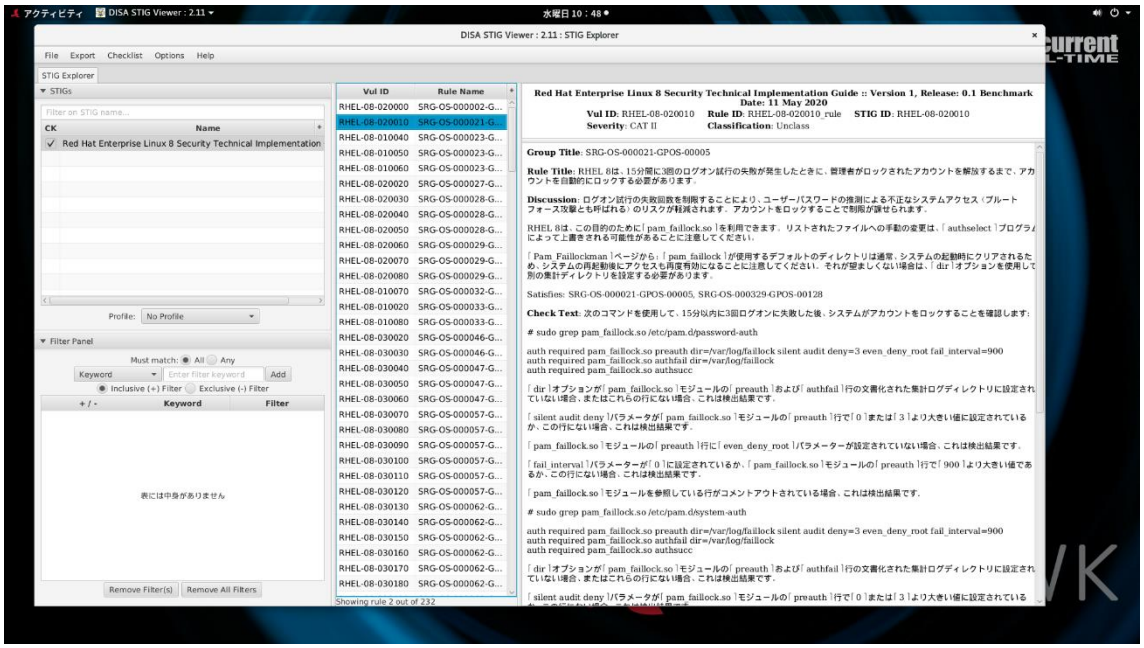
Cyber Exchange Web サイトからダウンロードされた STIG は、.zip 形式であり、STIG ビューアにロードされます。 STIG ビューアはすべての STIG を同じ方法で処理します。 このガイドは、すべてのテクノロジーに適した一般的な手順を提供します。

1. STIG Viewerメニューバーから、[File]-[Import STIG] を選択します。

2. 読み込む STIG.zipファイルを選択し、[開く]ボタンをクリックします。この例は、Linux STIG を示しています。

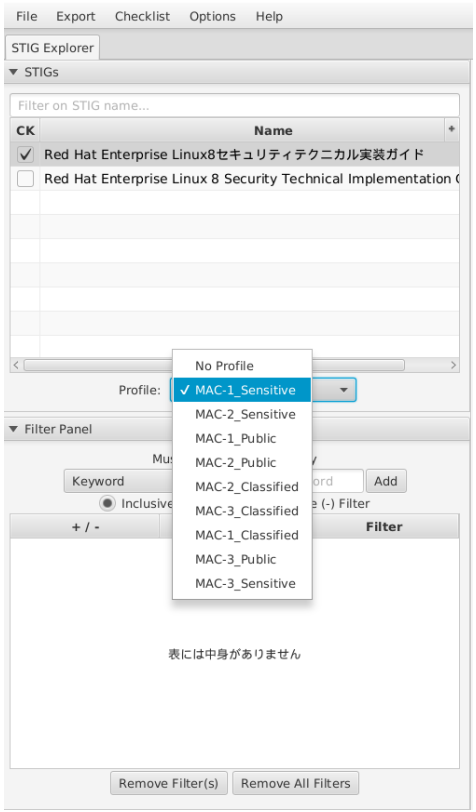


3. STIG Viewerは STIG がロードされたことを示します。
4. 複数のSTIGがロードされている場合は、STIGリストを右クリックして、[Check All]オプションを表示できます。 このオプションは、キーワード検索を行うときに役立ちます。 さらに、ショートカットCtrl + Aを使用すると、リスト内のすべてのSTIGが強調表示されます。

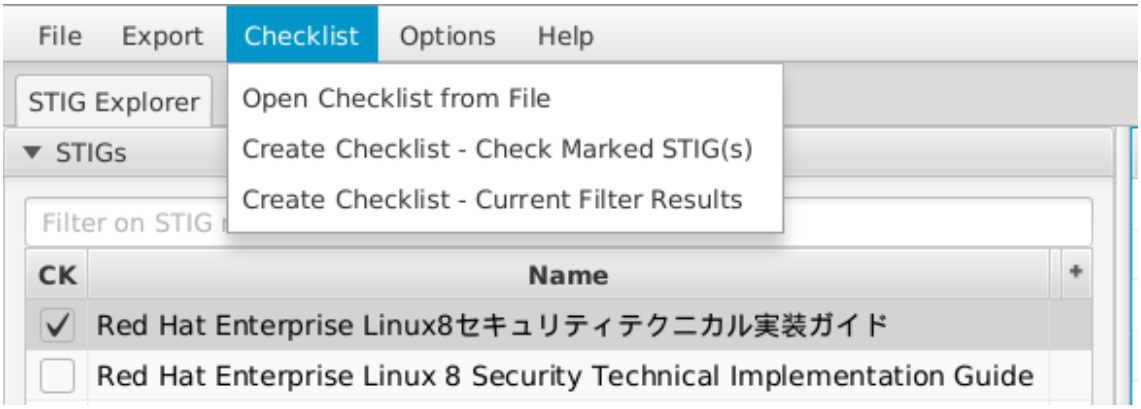


2.1 STIG からチェックリストを作成する

1. [Profile]ドロップダウンをクリックし、チェックリストとレビュー対象のアセットの [MAC/Classification]を選択します。

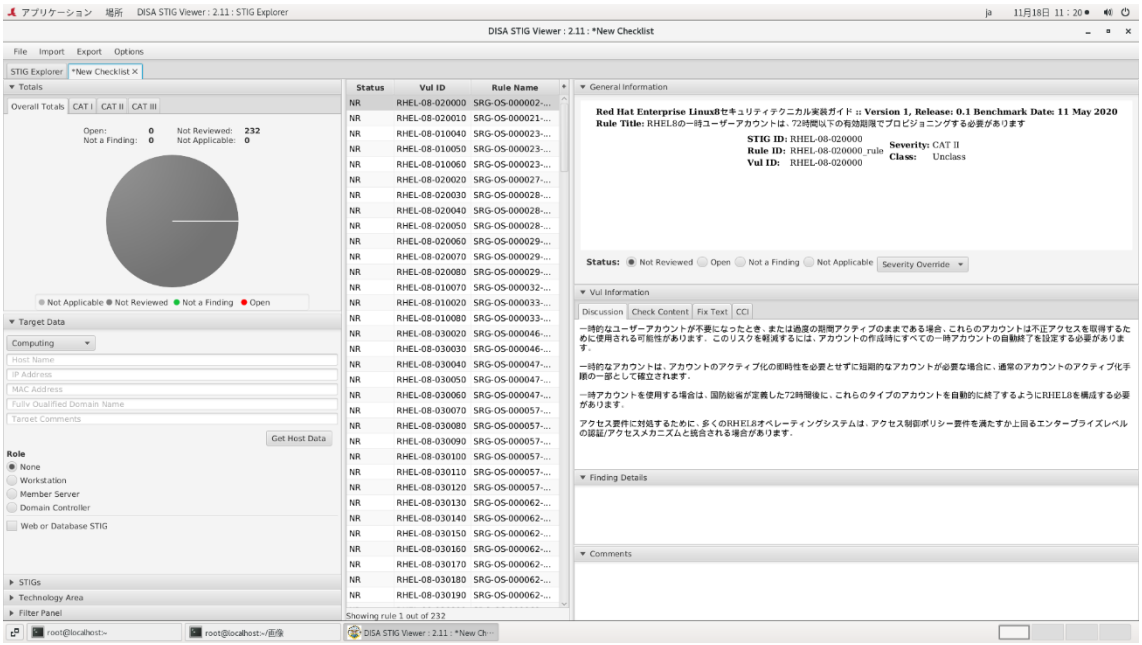


2. STIG の横にある [CK] チェックボックスをオンにし、メニュー項目の[Checklist]>> [Create Checklist – Check Marked STIG(s)] をクリックします。



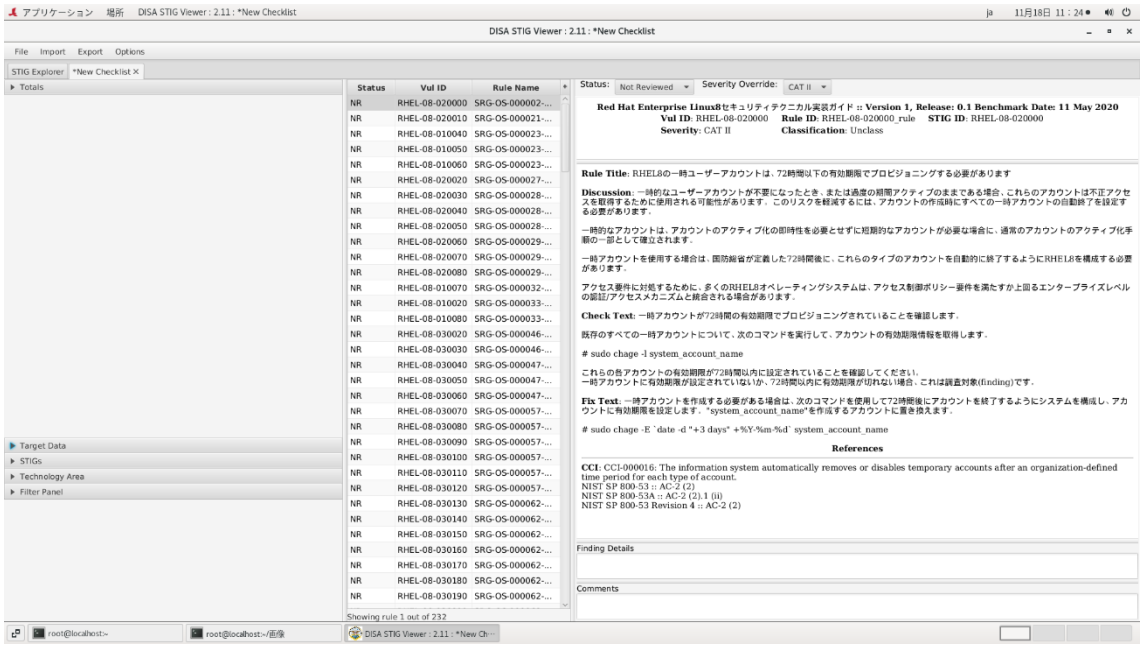
3. [Checklist]>>[Create Checklist – Current Filter Results] を選択して、フィルタされた結果からチェックリストを作成します。

4. [Checklist]タブが開き、STIG のチェックリスト情報が選択されます。



5. Checklistタブの列は STIG タブ列とは異なります。
   - 左側列: Totals, Target Data, STIGs, Technology Area, and Filter Panel
   - 中央列: チェックリストの脆弱性
   - 右側列: General Information, Vuln Information, Finding Details, Comments

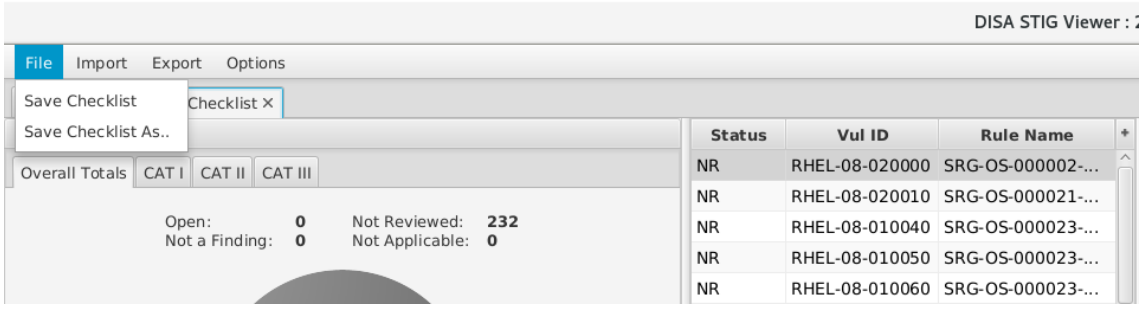
注:これらは、[Option] メニューの [Preferences] から[SV 2.x Classic Light]ビジュアルスタイルオプションを選択した場合のタブです。 右側の列セクションを折りたたむには、チェックリストを作成する前にLight themeに変更します。 すべてのセクションを表示するには、一部を折りたたんでください。 すべてのセクションが折りたたまれたビューについては、以下を参照してください。



2.2 Checklist タブ - メニューの選択

2.2.1 File メニュー

[File] メニューでは、チェックリストを保存したり、新しいファイル名/場所を使用してチェックリストを保存したりできます。

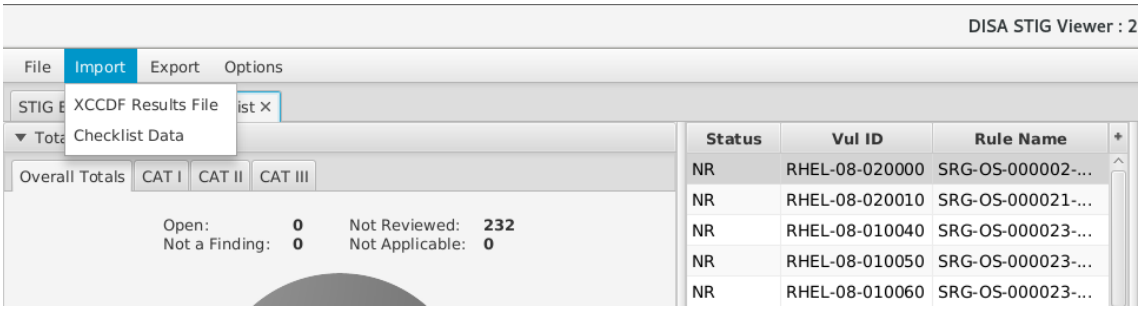


2.2.2 Import メニュー

[Import]メニューのオプションを使用すると、XCCDF結果ファイルまたはチェックリストデータをインポートできます。 XCCDF結果ファイルは、拡張子が.xmlのファイルで、SCCツール（https://cyber.mil/stigs/scap/）などのSCAP準拠ツールを使用したスキャンの結果が含まれています。

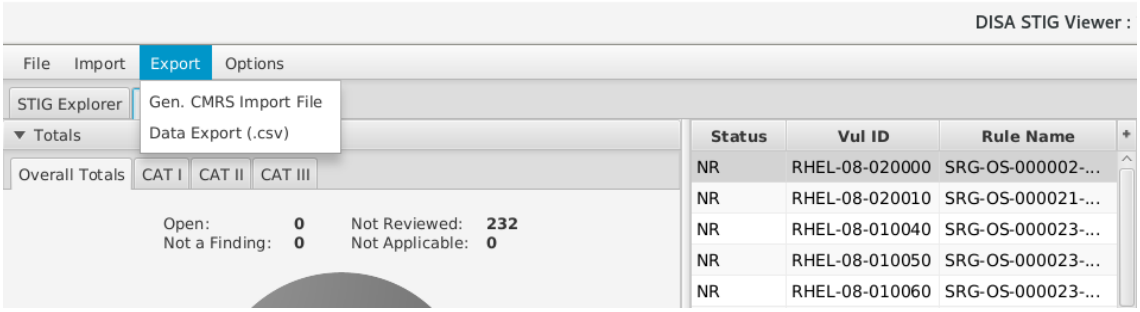
[Import] メニューには、以前に保存した STIG Viewer チェックリスト ファイル (.ckl) をインポートする機能も含まれています。最近更新されたルールの結果は、ルール ID が変更されるため、インポートされません。

インポートが完了したら、手動チェックである残りの未確認 (NR) ルールに対処します。チェックリストを完了するには、NR ステータスのすべての項目を適切なステータスに設定してください。



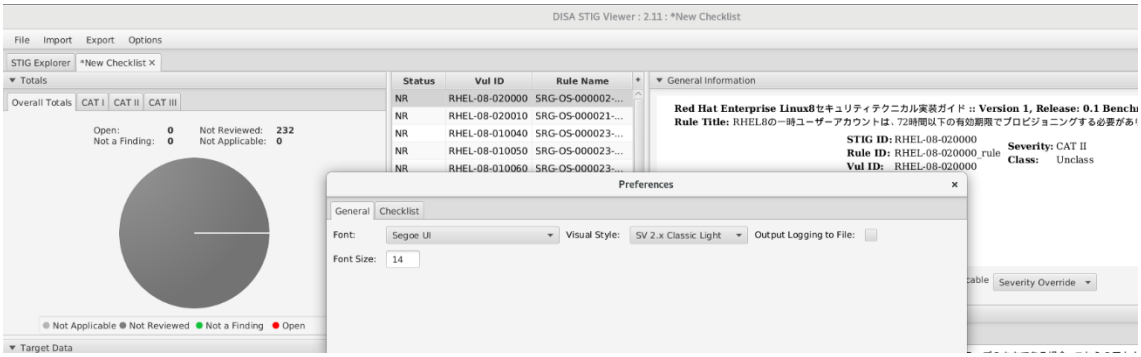
2.2.3 Export メニュー

[Export]メニューには、チェックリストデータをレポート用の一般的な CMRS インポート ファイルにエクスポートする機能があります。チェックリスト データを Excel スプレッドシート (.csv) にエクスポートすることもできます。



2.2.4 Optionメニュー

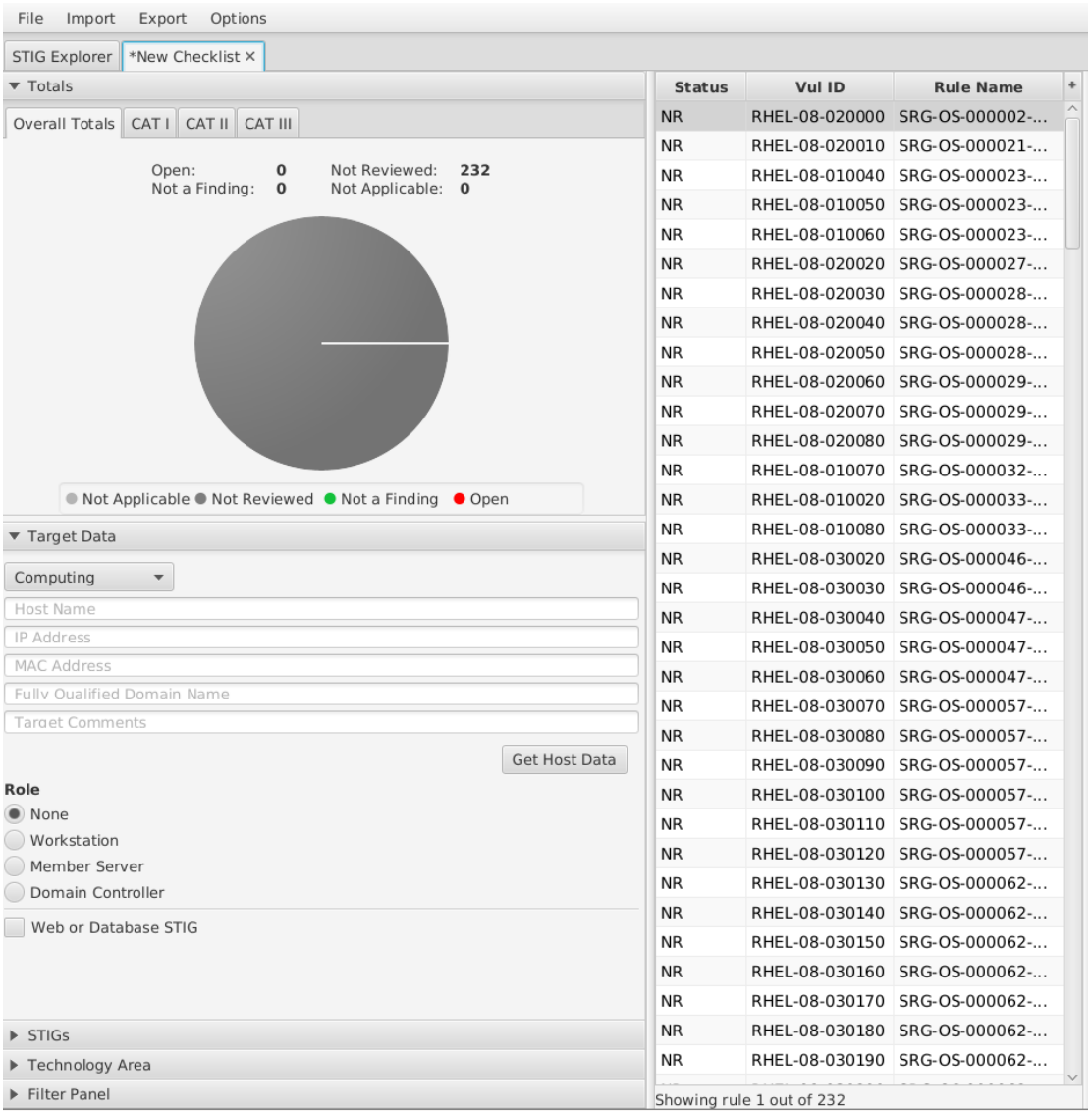
[Option]メニューには、フォントサイズ、表示スタイル、およびチェックリストのテキストの色を変更するための設定が用意されています。表示スタイルオプションには、Light themesとDark themesの両方が含まれ、STIG とチェックリストの両方の右側の列のセクションの外観が含まれます。

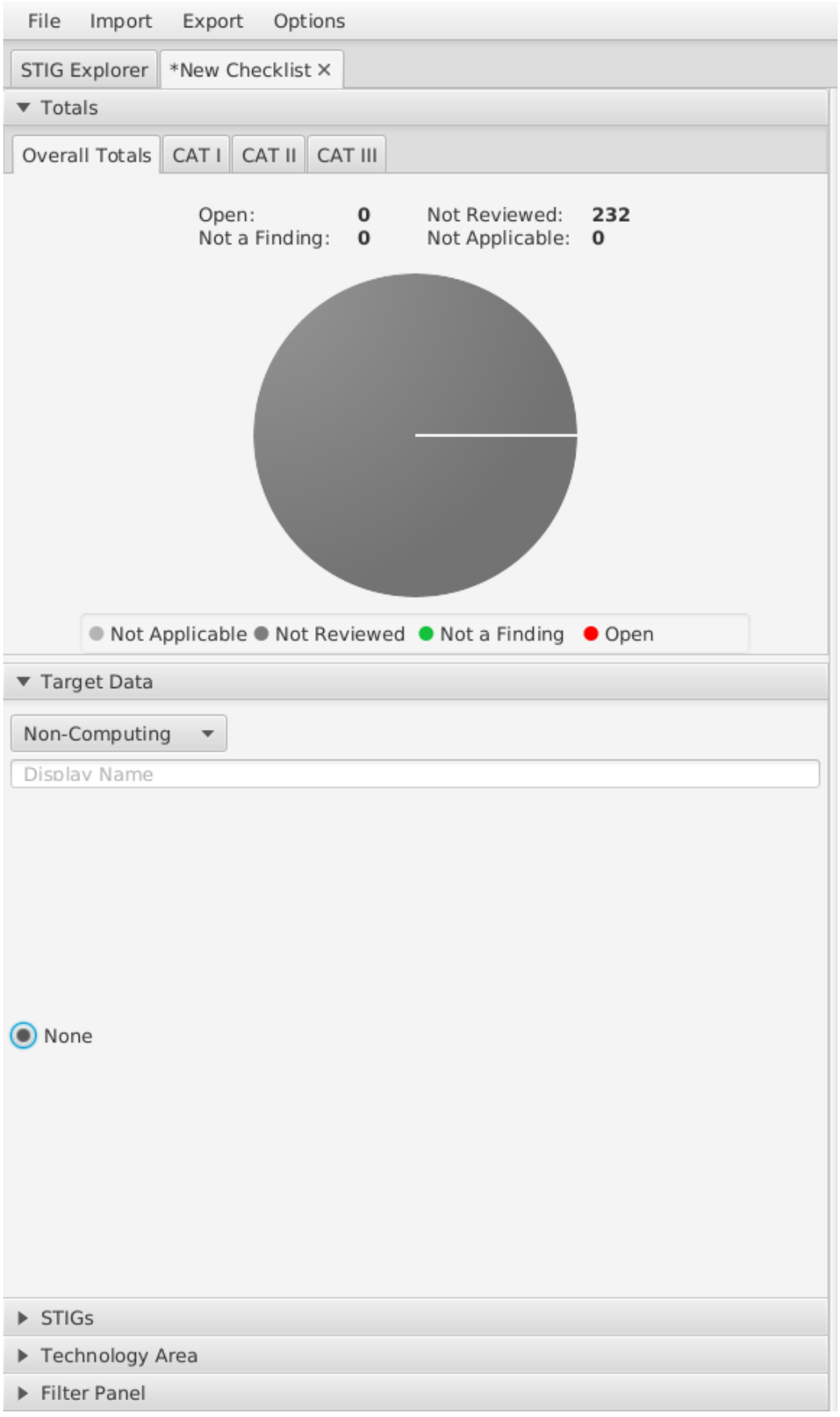


3. Checklist セクション

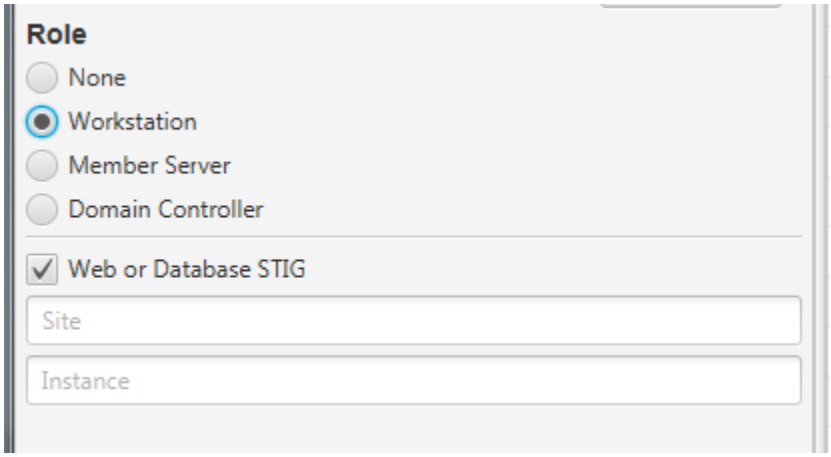
3.1 Checklist – Target Data セクション

1. [Checklist – Target Data]セクションでは、STIGアセットを識別します。上部のドロップダウンボタンを使用して、[Computing]と[Non-computing]を切り替えることができます。Computingアセットに関しては、確認対象のアセットのHost Name, IP Address, と MAC Addressを入力します。[Target Comments] のすべてのアセットにコメントを追加することもできます。Non-computingアセットの場合は、アセットの名前のみを入力します。
   注:使用しているコンピュータがアセット対象でない限り [Get Host Data] ボタンをクリックしないでください。クリックすると、使用しているコンピュータの情報が [Computing] フィールドに入力されます。



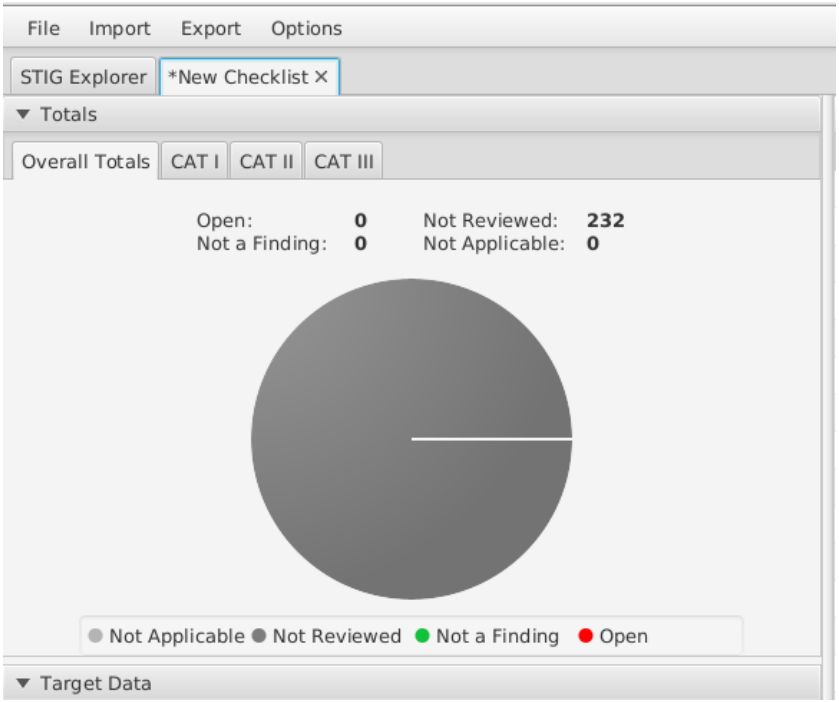


2. [Role]のサーバタイプラジオボタンを選択します。[Web or Database STIG] ボックスをクリックすると、サイト名とインスタンス名のフィールドが表示されます。



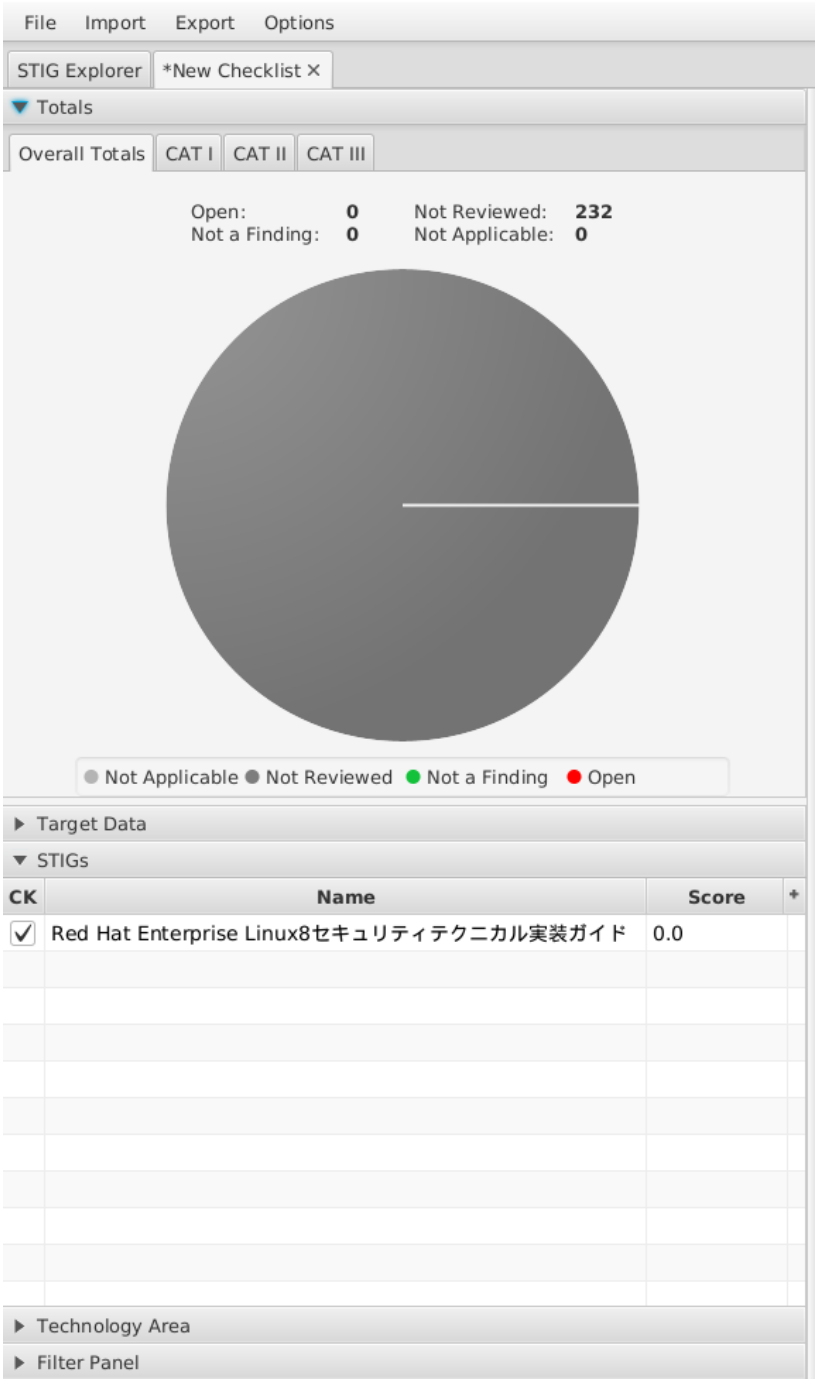
3.2 Checklist – Totals セクション

[Checklist Totals] セクションには、各脆弱性ステータスの個々のCAT I、II、およびIIIの合計数と、[Overall Totals]のタブが含まれています。



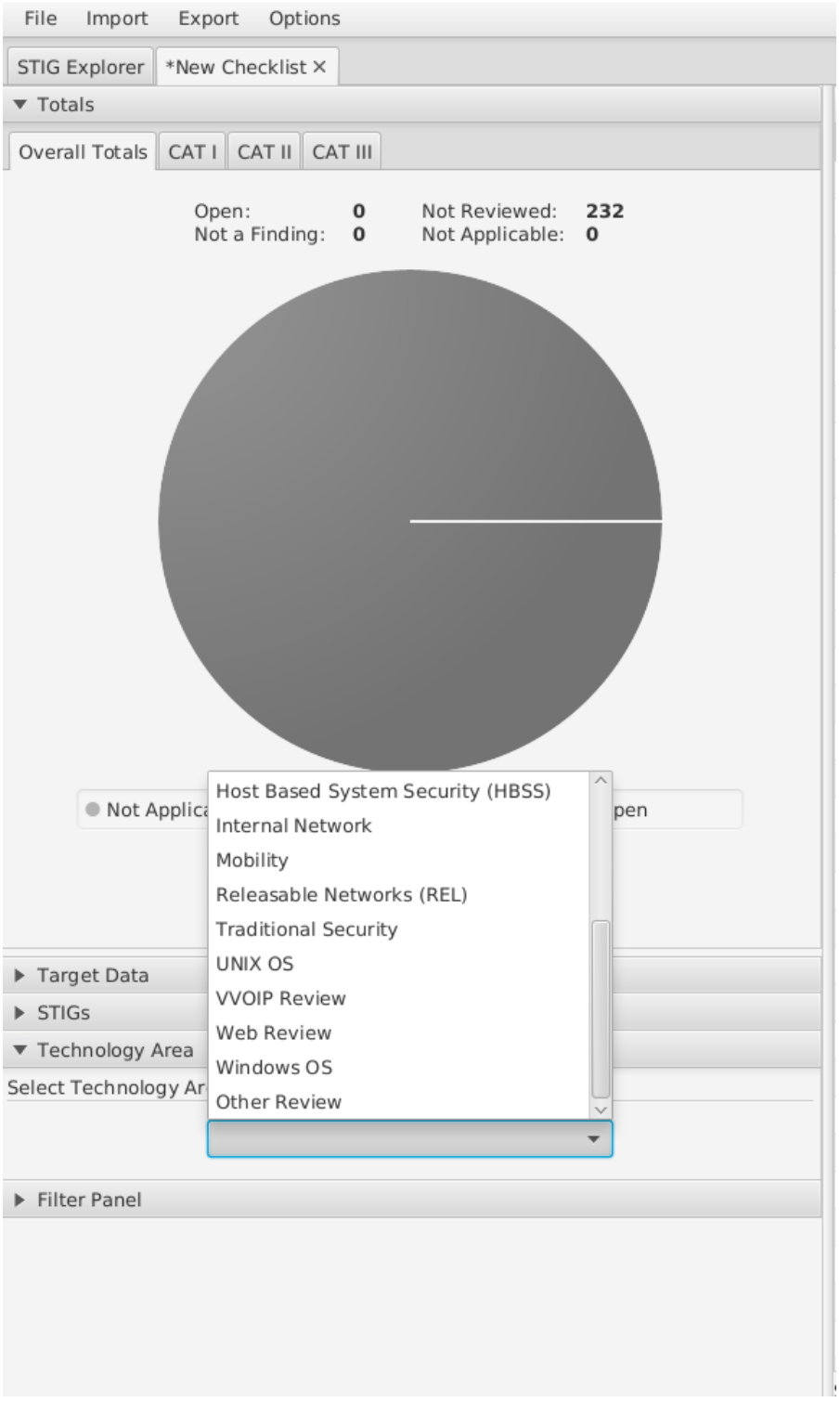
3.3 Checklist – STIGs セクション

STIGsセクションには、このチェックリスト内のSTIGのタイプが含まれています。 1つのチェックリストタブに複数のSTIGを含めることができます。



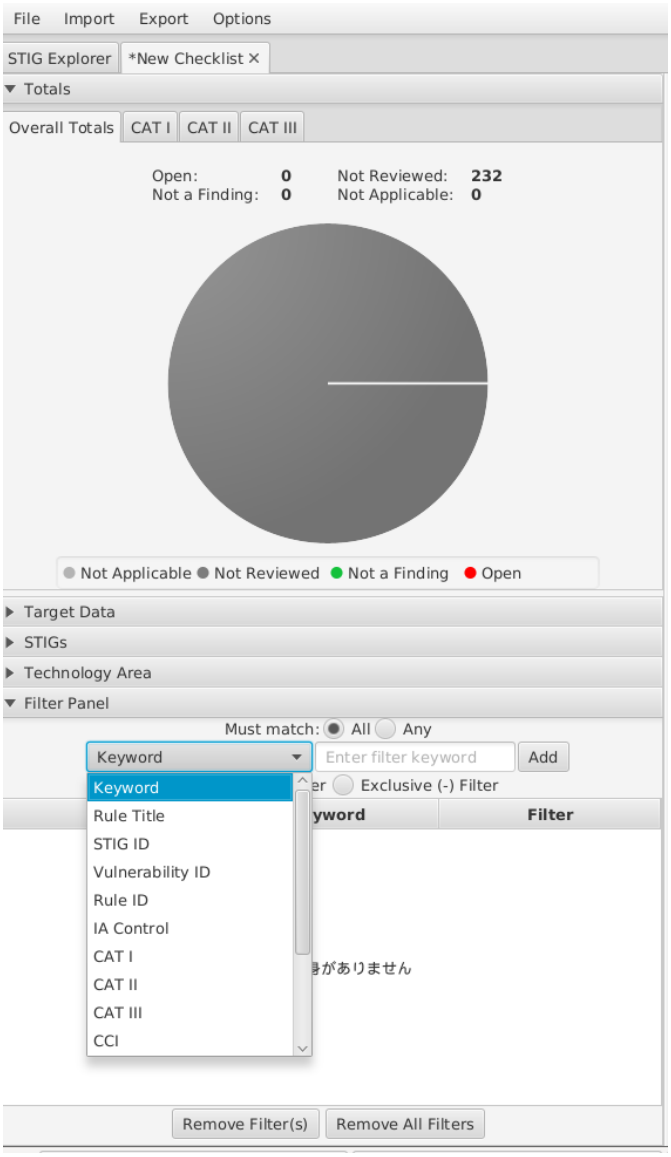
3.4 Checklist – Technology Area セクション

[Technology Area]セクションには、レビュー対象のアセットに対して特定のテクノロジを選択するためのテクノロジドロップダウン リストが含まれています。



3.5 Checklist – Filter Options セクション

[Filter Options]セクションでは、Keyword, Rule Title, STIG ID, Vulnerability ID, Rule ID, Severity, CCI, または Statusで脆弱性をフィルター処理できます。 基準を満たすまたは満たさない脆弱性を見つけるには、[Inclusive Filter]または[Exclusive Filter]ラジオボタンを選択します。 [Must match：All]または[Must match：Any]を使用して複数のフィルターを組み合わせ、すべてのフィルターが一致するか、任意のフィルターがそれぞれ一致するようにします。 フィルタをクリアするには、[Remove Filter(s)]または[Remove All Filters]ボタンを選択します。



3.6 Checklist – General Information セクション

1. 中央の列で選択した脆弱性の右側の列に[General Information]セクションが表示されます。

2. [Status] ラジオボタンを選択して、脆弱性をOpen (調査対象), Not a Finding (調査対象外), またはNot Applicable (適用外)として識別します。脆弱性テキストの色もステータスを反映するように変更されます。

3. ステータスの重大度をダウングレードまたはアップグレードする必要がある場合は、[Severity Override]ドロップダウンをクリックします。 ポップアップボックスが表示され、オーバーライドに必要な調整テキスト(CAT I,CAT II,CAT III)を入力します。

4. 複数の脆弱性チェックを選択するには、最初の選択をクリックしてから、後続の選択を Shift キーを押しながらクリックします。Ctrl+ A キーを押すか、右クリックして [Select All] を選択して、すべての脆弱性を選択します。

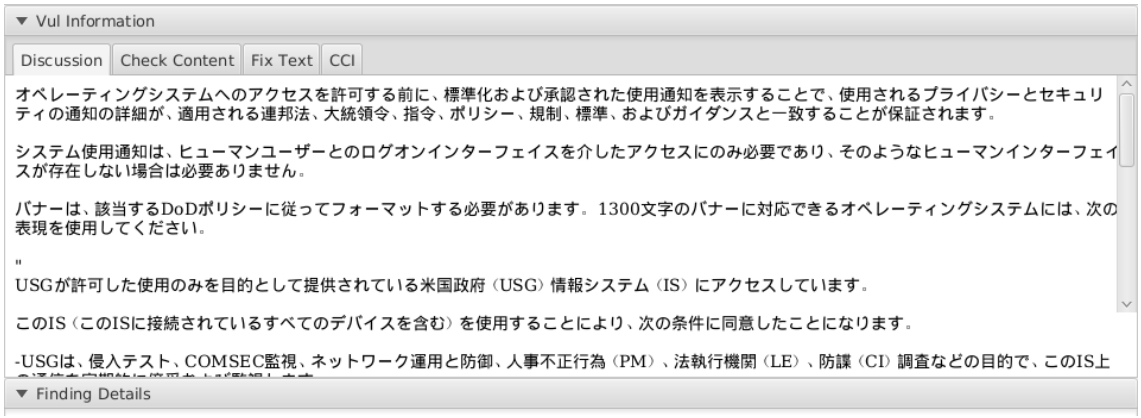
5. 選択したすべてのチェックに設定する[Status]ラジオボタンまたはドロップダウンメニューオプションを選択します。

6. 1 つ以上のチェックのステータス選択のステータスラジオボタンとドロップダウンメニューオプションに加えて、4 つのステータスのそれぞれにショートカットキーがあります:
   - "R" または "r" は選択したチェックを“Not Reviewed”.としてマークします。 (調査していない)
   - “O”または”o”は、選択したチェックを“Open”とマークします。 (調査対象)
   - “N”または”n”は、選択したチェックを“Not A Finding”とマークします。 (調査対象外)
   - “X”または”x”、選択したチェックを“Not Applicable”.とマークします。 (適用外)

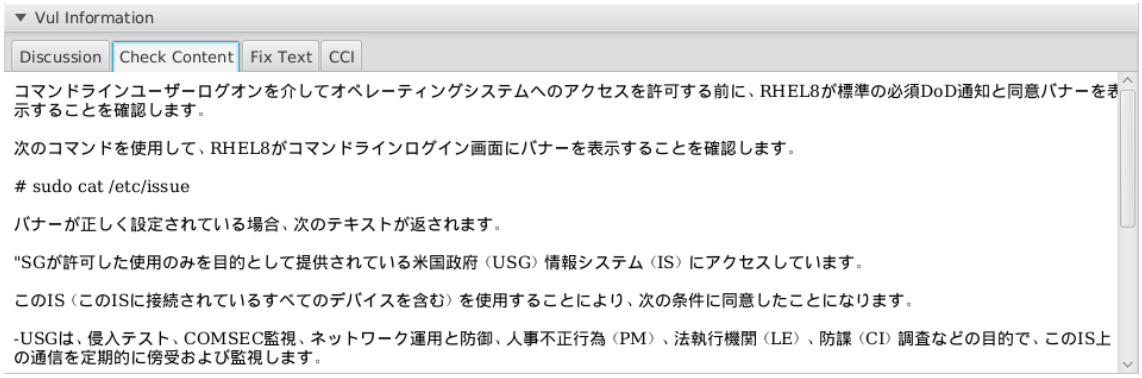
3.7 Checklist – Vuln Information セクション

クラシックスタイルの[Vuln Information]セクションには、中央の列で選択した脆弱性に関連する5つのタブがあります(LightとDark themeスタイルには以下のタブはありません)。

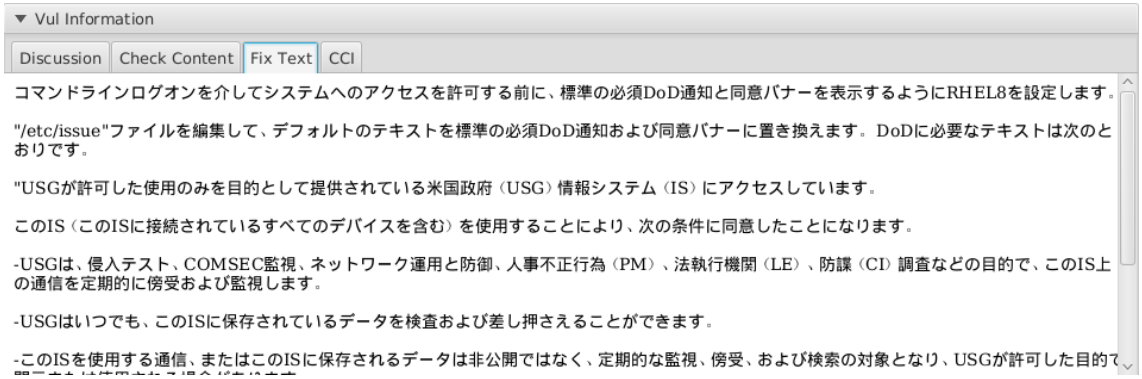
- [Discussion] タブ – チェックの簡単な説明



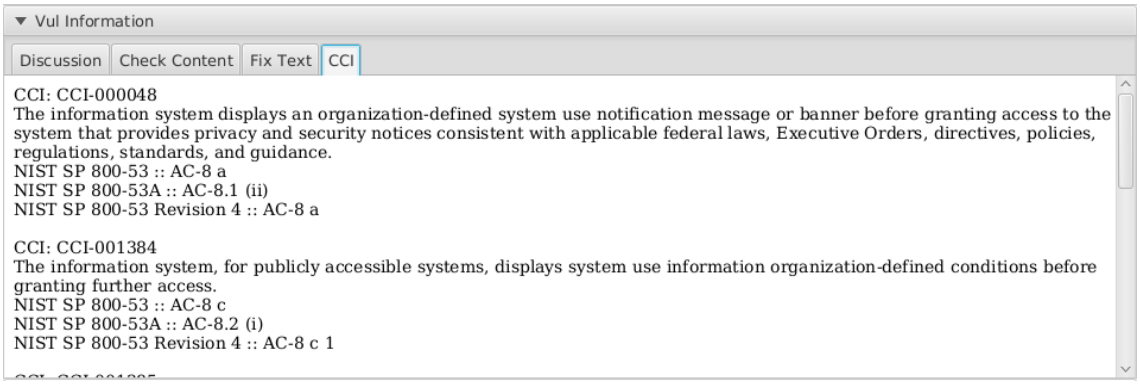
- [Check Content] タブ – 調査項目を確認するための手順について説明します (自動ベンチマークには、このタブや手動による確認手順は含まれません)。



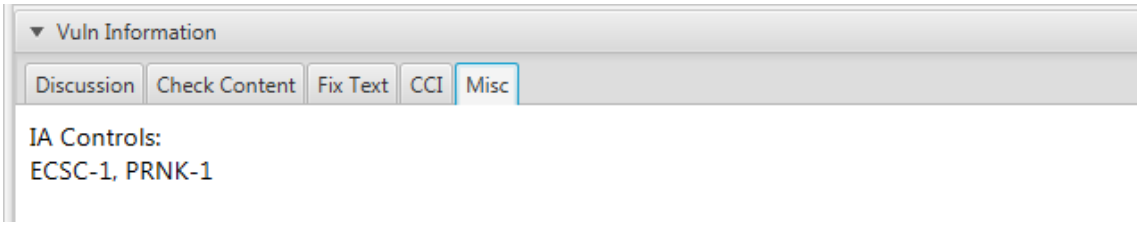
- [Fix Text] タブ – 調査項目の確認結果がOpen（調査対象）であった場合に修正する方法を説明します



• CCI タブ – 調査項目およびNIST SP 800-53 リファレンスに関する CCI 情報を提供します。



• [Misc] タブ – 調査項目用の IA コントロールを提供します (該当する場合にのみ表示されます)



3.8 Checklist – Finding Details セクションと Comments セクション

レビュー担当者からの詳細とコメントを記録するには、[Finding Details] セクションと [Comments] セクションを使用します。右クリックして[Paste Text]を選択して、[Paste as Finding Details]または[Past as Comments]を一括で貼り付けます。