# Dell CloudIQによるサーバーのサイバーセキュリティの強化

## 概要

お客様から良い評判が得られるように組織がかける時間は数年におよぶことがありますが、サイバーセキュリティ関連のインシデントが発生するとその評判は数分で台無しになります。サイバーセキュリティ チームとサーバー管理者は、社内のあらゆるツールを駆使してインフラストラクチャを強化する必要があります。ここでは、すべての Dell PowerEdge のお客様が知っておくべき Dell CloudIQ の機能についてご紹介します。

この Direct from Development（DfD）Tech Note では、CloudIQ に組み込まれている PowerEdge サーバー向けサイバーセキュリティ機能について説明します。

CloudIQ は、Dell インフラストラクチャの製品ポートフォリオを対象とした、クラウド AI/ML ベースのモニタリングおよび予測分析アプリケーションです。CloudIQ は、セキュアな Dell IT クラウドにホストされています。正常性、パフォーマンス、テレメトリーを収集して分析し、リスクを特定して、問題を迅速に解決するためのアクションを提示します。

## 作成者

**Mark Maclean**
テクニカル マーケティング エンジニアリング

**Kyle Shannon**
製品管理

バージョン 1.1：2022 年 7 月

## はじめに

Dell CloudIQが提供するサイバーセキュリティ機能は、現在、Dell PowerEdgeサーバーもサポートしています。お客様のサーバー チームは、CloudIQに組み込まれているサイバーセキュリティ機能を使用することで、評価プランと呼ばれるポリシーを構築できます。この評価プランは、すぐに使用できるさまざまな「クリックして選択する」構成基準テストを使用して構築されます。この構成設定および値のリストは、Dellのベスト プラクティスとNIST（アメリカ国立標準技術研究所）のサイバーセキュリティフレームワークに基づいています。

## 迅速に成果を上げるためのアプローチ

的確なセキュリティ構成設定と適正な値を理解し、適切なスキルを備えているスペシャリストであれば、サーバー構成プロファイル「SCP」を構築し、それをiDRACまたはOME構成テンプレート機能と直接組み合わせて使用することで、サーバー構成を設定できます。一方、CloudIQにはこれよりはるかに迅速かつ規範的な方法が用意されています。この方法を使用することで、Dellの推奨設定と推奨値に基づいて構築されたサイバーセキュリティ評価ポリシーを実装できます。CloudIQは、サイバーセキュリティ プロセスをさらに合理化するために、複数のOMEインスタンスを集約し、複数の場所にあるサーバーを1つの統合ビューで表示することが可能です。組織によっては、構成コンプライアンスとセキュリティ管理が分離されていることを示すために、OMEとCloudIQの両方を使用する場合があります。


図1 サイバーセキュリティのステータス サマリー（CloudIQの概要ページ）

CloudIQの概要ページにある上記のサイバーセキュリティ タイルには、リスク レベルをまとめたステータス ビューが表示され、リスク カテゴリーごとのシステムの数と検出された問題の合計数が示されます。リスクは、重大度とサーバーあたりの問題の数によって決定されます。たとえば、高リスクの問題が1つ以上あるサーバーは高リスクに分類されます。高以外のリスクが6つ以上あり、そのうちの少なくとも1つが中程度の問題の場合、そのサーバーも高リスクとして分類されます。

## リスクの迅速な特定

システム リスク ダッシュボードは、ポリシーが適用されているすべてのサーバーを分類し、各サーバーを専用のカードに表示します。カードには、サイバーセキュリティのリスク レベル ステータスも表示されます。これにより、お客様はアクションに優先順位付けを迅速に行い、問題の解決にかかる時間を短縮できます。

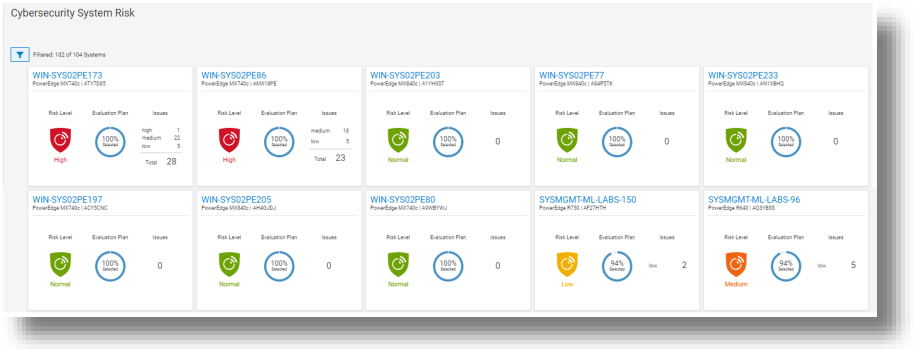


図 2 Cybersecurity System Risk（全システム ダッシュボード）

ダッシュボードに加えて、［Security Assessment］のステータスには、各サーバーの詳細情報が、逸脱したセキュリティ構成を望ましい状態に戻すための推奨アクションとともに表示されます。ドーナツ グラフには、選択されているルールの数が、特定のサーバーに割り当てられたリスク評価プランの総テスト数に対する割合として表示されます。

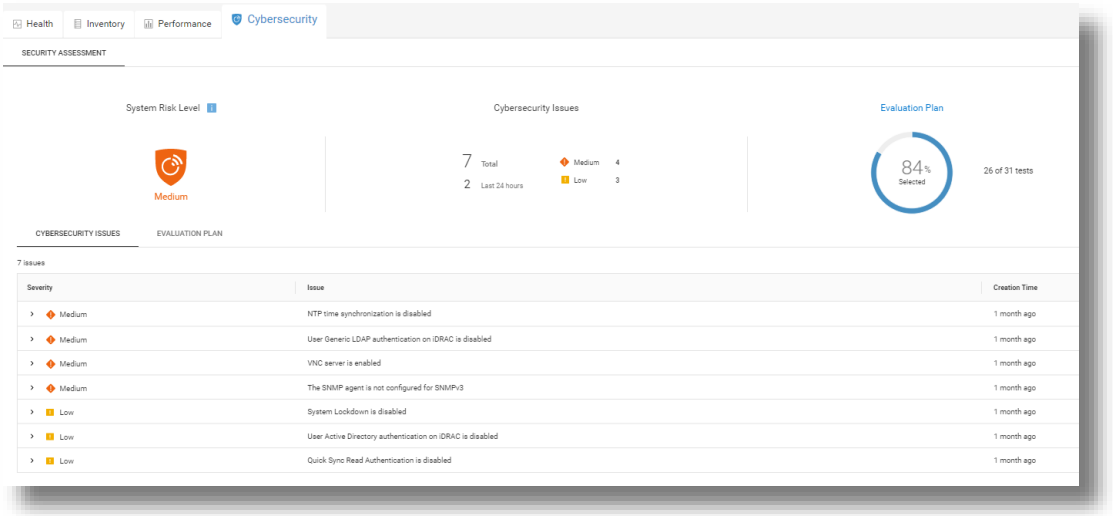


図 3　　サイバーセキュリティ リスクの詳細と推奨事項

［Cybersecurity］タブの［System Detail］ページには、評価プランとそのステータスに関する詳細情報が表示されます。ページの下部には、コンプライアンス違反の要素と対応処置の詳細が表示される［Cybersecurity Issues］と、プラン全体と各テストの選択ステータスが表示される［Evaluation Plan］という2つのタブがあります。

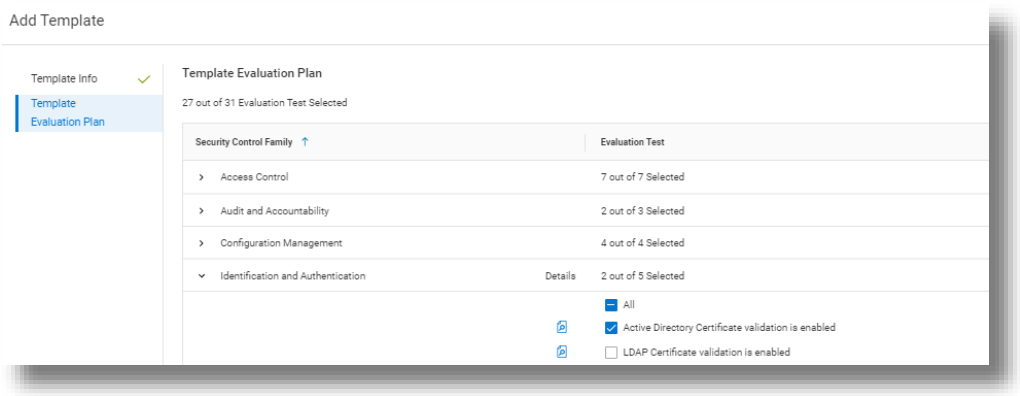


図 4 テストの選択

CloudIQ ユーザーは、サイバーセキュリティのステータス サマリーが記載されたダイジェスト E メールを毎日受け取ることもできます。

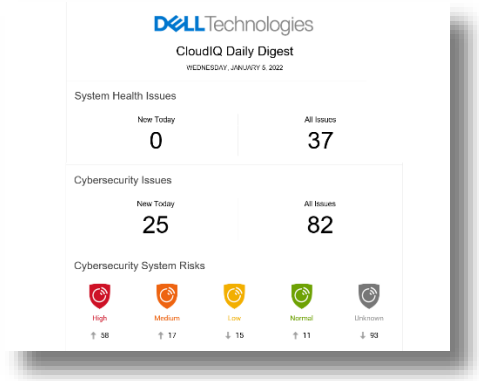


図 5 CloudIQ から毎日配信されるダイジェスト E メール

## 有効化とセキュリティ

ご想像のとおり、CloudIQには管理者アカウントおよびユーザー アカウントに関するさまざまなセキュリティ アクセス制御が組み込まれており、アカウントの作成およびレポート生成を制御できます。CloudIQには、サイバーセキュリティ管理者とサイバーセキュリティ ビューアーという2つのサイバーセキュリティ ロールが組み込まれています。これらのロールは、CloudIQ管理者権限を持つアカウントから割り当てることができます。

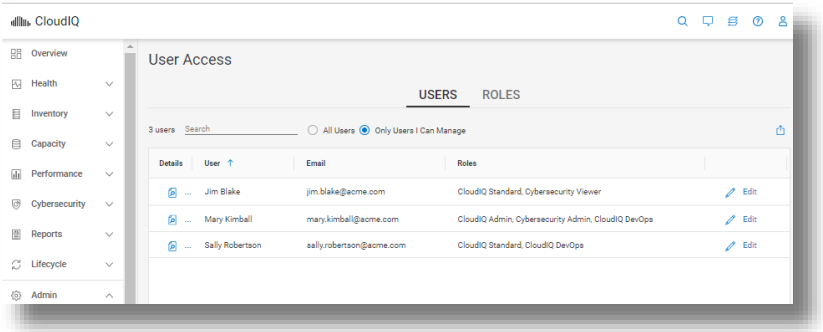


図 6 RBAC のセットアップ

CloudIQ内でPowerEdgeのサイバーセキュリティをサポートするには、CloudIQプラグイン1.1以降を有効にして、OpenManage Enterpriser 3.9以降を実行している必要があります。すべてのサーバーがDell ProSupportの対象である必要があり、OMEによってすでに検出されている必要があります。

## PowerEdge サイバーセキュリティ評価プランのテスト要素

次の表に、各テスト基準と、それらが属するテスト プラン ファミリーの詳細を示します。

| ファミリー | 名称 |
|---|---|
| システムと通信 | IPMI over LAN インターフェイスが無効 |
| システムと通信 | IPMI Serial over LAN が無効 |
| システムと通信 | 仮想コンソールの暗号化が有効 |
| システムと通信 | 仮想メディアの暗号化が有効 |
| システムと通信 | 自動検出が無効 |
| システムと通信 | iDRAC の vLAN 機能が有効 |
| システムと通信 | iDRAC Web サーバーの TLS 1.2 または TLS 1.3 が有効 |
| システムと通信 | iDRAC Web サーバーの HTTP リクエストが HTTPS リクエストにリダイレクトされる |
| システムと通信 | 仮想コンソールのプラグイン タイプが有効 |
| システムと通信 | iDRAC が専用 NIC を使用している |
| システムと通信 | iDRAC Web サーバーの TLS 1.2 または TLS 1.3 が有効 |
| アクセス制御 | IP ブロックが有効 |
| アクセス制御 | VNC サーバーが無効 |
| アクセス制御 | SNMP エージェントが SNMPv3 用に構成されている |
| アクセス制御 | サーバーに対する Quick Sync 読み取り認証が有効 |
| アクセス制御 | SSH が無効 |
| アクセス制御 | iDRAC でのユーザー汎用 LDAP 認証が有効 |
| アクセス制御 | iDRAC でのユーザーActive Directory 認証が有効 |
| 構成管理 | USB ポートが無効 |
| 構成管理 | Telnet プロトコルが無効 [1] |
| 構成管理 | System Lockdown が有効 |
| 構成管理 | BIOS POST からの iDRAC の構成が無効 |
| 監査と説明責任 | NTP 時刻同期が有効 |
| 監査と説明責任 | NTP が保護されている |
| 監査と説明責任 | リモート Syslog が有効 |
| システムと情報の整合性 | ローカル構成が有効、ホスト システムでの iDRAC 構成が無効 |
| システムと情報の整合性 | セキュア ブートが有効 |
| ID と認証 | パスワードの強力な保護のスコアが最小 |
| ID と認証 | LDAP 証明書の検証が有効 |
| ID と認証 | Active Directory 証明書の検証が有効 |
| ID と認証 | 256 ビット以上を使用した iDRAC Web サーバーSSL 暗号化 |
| ID と認証 | iDRAC Web サーバー - SCEP が有効 |
| | |

1. iDRAC ファームウェア リリース バージョン 4.40.00.00 以降では、Telnet 機能が iDRAC から削除されます

## まとめ

CloudIQは一般的なITチーム メンバーとは異なり、食事をしたり、睡眠を取ったり、休日に出かけたりする必要がありません。そのため、組織はCloudIQ Cybersecurityポリシーを利用して、コンプライアンス違反のサーバーを継続的に監視することができます。CloudIQに組み込まれているサイバーセキュリティ機能により、お客様は、事前定義済みのテストの自動化やステータスの可視化を通じて、サーバー セキュリティの提供を迅速化できます。これにより、サイバーセキュリティ チームが適用する必要があるガバナンスと制御を維持しながら、サーバー管理者高いレベルの柔軟性が得られます。CloudIQは、サーバーのサイバーセキュリティとシステム正常性のステータス、および幅広いDellインフラストラクチャポートフォリオを1つの便利なクラウドベースのポータルにまとめて表示することで、リスクをさらに軽減し、ITの生産性を向上させます。

## 参考資料

Dell.com：CloudIQに関する製品情報、デモ ビデオなど

ブログ：インテリジェントなクラウドベースのモニタリングによるサーバー サイバーセキュリティの管理

ビデオ：PowerEdgeサーバー用のDell CloudIQ Cybersecurityポリシーの構築および追跡

技術情報ページ：OpenManage Enterprise CloudIQプラグイン

Dellのその他のサイバーセキュリティ関連ソリューション