CommandCenter Secure Gateway (CC-SG) Release 6.0.0.5.14

Release Notes v4

はじめに

このリリースノートは、CommandCenter Secure Gateway(CC-SG)の最新リリースに関する重要な情報が記載されています。本文書全体と本リリースに関連するユーザーマニュアル等をお読みください。

リリース6.0.0.5.14では、(1) 2014年4月リリースの6.0.0の機能を網羅し　(2) Open SSL ハートブリードセキュリティ脆弱性に対応（3）その他の機能の追加と修正を図りました。

リリース6.0.0.5.14のファームウェアならびにこのリリースノートで言及されるすべてのドキュメントおよびファイルは**http://www.raritan.com/support/commandcenter-secure-gateway/**で入手できます。

リリース6.0のファームウェアは、最新の保守契約とともにCC-SGをご使用のお客様へ提供されます。

最新の製品マニュアル

本リリースにより、以下の CC-SG のドキュメントが更新されました。

- CC-SG Administrators Guide, User Guide & Online Help
- CC-SG 6.0 Upgrade Guide(ファームウェアアップグレードに関する詳細説明)
- Quick Setup Guide for CC-SG Virtual Appliance - No License Server
- CC-SG WS-API Programming Guide

新機能およびアップデート（リリース6.0.0.5.14）

CC-SG リリース 6.0.0.5.14 に導入されている機能およびアップデートは以下の通りです。

1. **OpenSSL ライブラリのハートブリード脆弱性対策**

   CC-SG で使用している OpenSSL 暗号化ソフトウェアライブラリの「ハートブリード」セキュリティ脆弱性対策。脆弱性からの回復は、セキュリティ専門家と相談のうえ、新しい SSL 証明書のインストールやパスワードの変更といった適切な対応を実施してください。

2. **CC-SG　E1　アプライアンスのオーバーヒート LED 点灯エラー**

   フロントパネルの CPU オーバーヒート LED が誤作動により点灯するエラーを解消しました。

3. **リモート IPMI アクセス**

   CC-SG E1 アプライアンス LAN ポート経由でのリモート IPMI アクセスをセキュリティの観点からブロックしました。

新機能およびアップデート（リリース6.0）

CC-SG リリース 6.0 に導入されている機能およびアップデートは以下の通りです。

3. **Dominion KX III 対応**

   高性能 KVM-over-IP スイッチの最新機種、Dominion KX III(DKX3-xxx)に対応しています。CC-SG 6.0 では、Dominion KX II(DKX2-xxx)は継続してサポートされますが、第一世代機種の Dominion KX のサポートは終了しました(下記参照)。

4. **Java 7 対応**

   最新の Java 7 Runtime Environment(7u51 まで)のサポートにより、セキュリティの向上を図りました。リリース 6.0 では Java 6 はサポート対象外となり、Java 8 については本バージョンでは正式にサポートされておりません。サポート対象バージョンは、互換性マトリックス（Compatibility Matrix）を参照してください。

5. **第一世代 Dominion KX スイッチのサポート終了**

   Dominion 第一世代機種 Dominion KX (DKX-xxx)、KSX (DKSXxxx)、KX-101 (DKX-101)および Paragon、 IP-Reach (IPR-xx)はサポート対象外となります。 これらの機種は販売終了品およびサポート終了品のため、**第一世代の製品を CC-SG の管理下から外して第二世代以降の製品に交換した後、リリース 6.0 にアップグレードしてください。**

6. **第一世代 Dominion クライアントのサポート終了**

   第一世代の MPC(KVM)、RRC(KVM)および RC(シリアル)クライアントはサポート対象外となります。KVM-over-IP は、Windows ベースの Active KVM Client(AKC)または Java ベースの Virtual KVM Client(VKC)を、シリアルについては Raritan Serial Client(RSC)をお使いください。

7. **Flexera lmadmin および lmgrd ライセンスサーバー(CC-SG バーチャルアプライアンス使用)は、サポート対象外に**

   CC-SG バーチャルアプライアンスに関し、CC-SG 6.0 では Flexera の lmadmin や lmgrd ライセンスサーバーはサポート対象外となり、外部ライセンスサーバーが不要となります。ライセンスサーバーをお使いの場合、ラリタンにご連絡頂き新たなライセンスファイルを取得して、当該ライセンスサーバーから移行する必要があります。CC-SG 6.0 へのアップグレードには、再ライセンス認証が必要です。ラリタンまでご連絡いただき、CC-SG ライセンスマネージャーを使って、新しいライセンスをアップロードしてください。

8. **iLO4 に対応**

   HP の統合サーバー管理システム iLO4 に対応しています。

9. **Chrome ブラウザおよび Internet Explorer 11**

   Chrome ブラウザおよび Internet Explorer 11 を CC-SG でお使いいただけるようになりました。

10. **レポート機能により、CC-SG ファームウェア アップグレードの失敗を通知**

    万一、CC-SG のアップグレードに失敗すると、CC-SG の診断コンソールに「ファームウェアのアップグレードに失敗しました」と表示されます。ユーザーには、アップグレードに失敗した理由とともに、推奨されるアクションが提示されます。

11. **セキュリティを強化**

    OS、Apache および OpenSSH バージョンのアップデート、新しい Verisign 証明書の取得、CC-SG Super User Password の長さ設定、SSL 証明書のキー長を 2048 ビットに増加など、多種多様なセキュリティの脆弱性への対策を図り、セキュリティを強化しました。

12. **CC-SG API のアップデート**

    デバイス管理サービスの getDevice()機能で、DeviceData wsdl ファイルが変更されました。デバイスのモデルおよび portCount に新しいフィールドが 2 つ追加されました。ポートカウントは、KVM、シリアル、電源、アウトレットといったフィーチャーポートの数を表しています。詳細については、API ガイドを参照してください。

バージョン 6.0.0.5.14 へのアップグレードパス

CC-SG のバージョン 6.0.0.5.14 へのアップグレードパスは、CC-SG のタイプ(バーチャルアプライアンスまたはハードウェア)およびライセンスのタイプによって、以下のように異なります。

1.ハードウェアアプライアンス(CC-SG V1 および E1)

- 5.x CC-SG バージョンはすべて、CC-SG 6.0.0.5.14 に直接アップグレードできます。

- 3.x および 4.x バージョンは、下図に示すように、先にバージョン 5.0 にアップグレードしてから CC-SG 6.0 にアップグレードする必要があります。

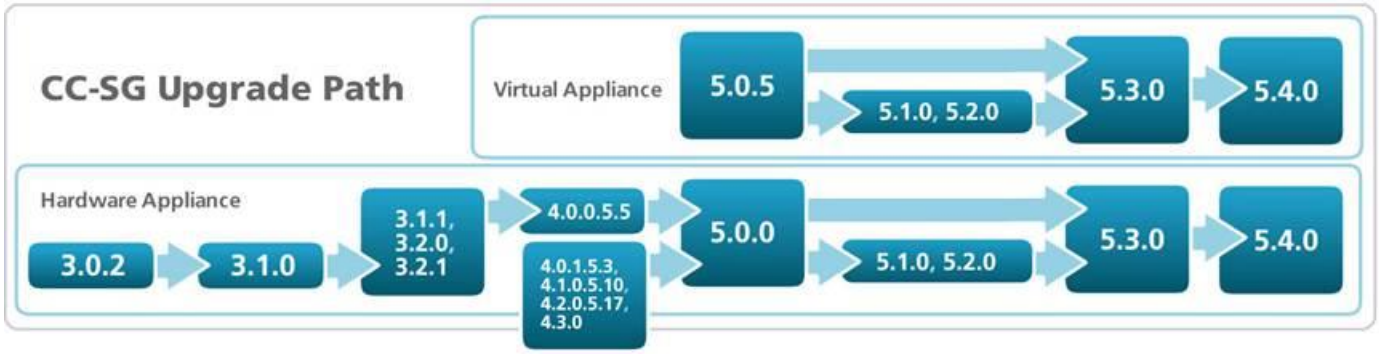
2.バーチャルアプライアンスーライセンスサーバーなし(バージョン 5.3 および 5.4)

- 5.3 または 5.4 からバージョン 6.0.0.0.5.14 に直接アップグレードできます。

3.バーチャルプライアンスーライセンスサーバーあり(バージョン 5.0.5、5.1、5.2、5.3、5.4)

1) バージョン 5.0.5、5.1、5.2 は、バージョン 5.3 にアップグレードする必要があります。
2) CC-SG 6.0 は Flexera lmadmin や lmgrd ライセンスサーバーをサポートしていないため、新しいライセンスファイルを(1 つまたは複数)取得して、当該ライセンスサーバーから移行する必要があります。ラリタンのテクニカルサポートまでご連絡いただき、新たなライセンスファイルを取得してから、CC-SG ライセンスマネージャーを使って新しいライセンス(1 つまたは複数)をアップロードしてください。再ライセンス認証を行ったあと、CC-SG 6.0.0.5.14 へのアップグレードが可能となります。
3) 上記手順が完了後、バージョン 5.3 または 5.4 からバージョン 6.0.0.5.14 に、直接アップグレードできます。

上記の特定のバージョンのアップグレードが必要な場合は、下図を参照してください。（図はバージョン 5.4 まで）



アップグレードに関する追加情報

CC-SG バーチャルアプライアンスは、お使いの仮想マシンにセカンドハードディスクを増設してからアップグレードする必要があります。

CC-SG V1 または CC-SG E1 は 6.0.0.0.5.14 へのアップグレードが可能ですが、それ以前の CC-G1 ユニットではできません。

アップグレード手順の前後に、お使いの CC-SG のバックアップをとってください。

お使いの他のラリタン製品のアップグレードが必要な場合もあります。サポート対象デバイスの一覧は、CC-SG 互換性マトリックスを参照してください。管理対象ラリタン製品のアップグレードについては、CC-SG 管理者ガイド（Administrators Guide）を参照してください。

アップグレードの手順に関する詳しい説明は、CC-SG 6.0 アップグレードガイドを参照してください。

ご不明な点がある場合は、ラリタンまでお問い合わせください。

特記事項および制限事項

1. Microsoft RDP クライアントは、CC-SG ブックマーク経由で起動することはできません。今後のアップデートで修正します。

2. IPv6：CC-SG を IPv4/IPv6 デュアルスタックモードで使用する場合は以下の点にご注意ください。
   - Administrators Client は、Firefox6、7、8、9、10、11、12 を使用している場合は IPv6 ネットワークで起動することはできません。ユーザー証明書のインストールなどにより回避することができます。詳細は管理者ガイドを参照してください。
   - IPv6 ネットワークで VNC を使用する場合は、Real VNC サーバー設定で[Prefer On](オンを選択)を選択してください。
   - IPv6 の Static Route(静的ルート)を追加する場合は、以下にご注意ください。
     1. CC-SG を再起動すると、値は保持されません。
     2. IP フェイルオーバが発生すると、値は保持されません。
   - IPv6 で使用できない特長や機能については、管理者ガイドを参照してください。
3. Windows 7 用の VNC および RDP インタフェースを追加する場合は、ICMPv4 と ICMPv6 が Windows 7 のファイアウォールで許可されていることを確認してください。
4. CC 経由で iLO3 KVM アプリケーションを起動すると、「セキュリティ保護されていないコンテンツをロードしますか」という警告が表示され、これを承認する必要があります。これは、HP アプレットに署名がないために発生します。
5. サポート対象 JRE バージョンは、Java 7 JRE 1.7 Update 51 までです。サポート対象外のバージョンには、1.7.0_11 および 1.7 update 9-bo5 が含まれます。組込み型サービスプロセッサのバージョンによっては、最近の Java の変更に合わせてアップデートされていないものがあるため、その場合は Java セキュリティレベルを低めに設定するか、Java コントロールパネルのセキュリティタブにある Exception Site List(例外サイトリスト)をお使いください。
6. [Bookmark Node](ノードをブックマークに設定)機能は、Internet Explorer バージョン 8(IE8)を使用する場合はサポートされません。
7. RSA リモートコンソールは、JRE 1.6.0_10 以上を使用する場合は CC-SG から起動することはできません。IBM からこれを回避する方法が提供されています。以下 URL からご確認ください。
   http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&Indocid=MIGR-5080396.
8. AES 256 暗号化を有効にする場合は、CC-SG からのロックアウトを回避するため、必ずクライアント PC またはデバイスに管轄ファイルをインストールしてください。
9. VMware Viewer および Firefox バージョン 3.6.x は互換性がありません。
10. CC-SG では、無料試用版のライセンスを使用する ESXi 仮想ノードの管理またはアクセスはできません。
11. VMware をクライアントとして使用する場合、シングルマウスモードは Windows または Linux のターゲットサーバーでは機能しません。
12. DRAC5 ターゲットにアクセスする場合の同時 SSH セッションの最大数は 4 です。
13. お使いの DRAC のバージョンがグレースフルシャットダウンに対応してしない場合、電源制御のためにグレースフルシャットダウン操作を実行すると、「グレースフルシャットダウンはサポートされていません」というメッセージが表示されます。
14. SNMPv3 オプションおよび MGSOFT MIB Browser を使用する場合、認証パスワードとプライバシーパスワードは異なるものでなければなりません。CC-SG はトラップを送信しますが、ブラウザはこれを無視します。