CommandCenter Secure Gateway (CC-SG) Release 7.0 リリースノート

はじめに

このリリースノートは、CommandCenter Secure Gateway (CC-SG) の 7.0 に関する重要な情報が記載されています。

Release 7.0 の内容：Release 6.2 の全ての機能に加え、新機能の追加と修正を含みます。

ファームウェア並びにこのリリースノートで言及される全てのドキュメントおよびファイルは、以下の URL から入手できます。

http://www.raritan.com/jp/support/product/commandcenter-secure-gateway

Release 7.0 の新機能およびアップデート

Release 7.0 に含まれる機能強化およびアップデートは以下のとおりです。

1. Java 非依存の接続クライアント「Desktop Admin Client for Windows」
2. CC-SG による DKX3 ユーザーステーションのログイン認証
3. Servertech 製 PDU「CDU1」「PRO2」について SNMP によるリモート電源操作をサポート
4. VMware 6.5 をサポート
5. 最新のセキュリティ対応および信頼性の向上
6. TLS v 1.2 に対応
7. SSH サーバーのアップデートによる鍵長 512 bit 未満の認証の使用禁止
8. コードサイニング証明書の更新
9. CC-SG WS-API の拡張　※API で使用するセキュリティ証明書をアップデートする必要あり
10. サードパーティー製サービスプロセッサである DRAC7 & 8 (KVM & 電源) の対応強化
11. PowerIQ 連携のパフォーマンス向上とセキュリティ強化
12. 新しい Java とブラウザに対応したセキュリティ強化

重要なおしらせ

・Release 7.0 は、既にエンジニアリングサポートが終了した Dominion KX II (DKX2-xxx) に対応する最終リリースとなります。
・仮想アプライアンスが Release 7.0 へアップグレードする場合、4GB 以上のメモリと 40GB の追加ディスクが必要です。　※詳細は「CC-SG 7.0 Upgrade Guide」を参照してください。
・一部の CC-SG ハードウェアアプライアンスは、ハードウェアスペックが非対応であるため、Release 7.0 をご利用することができません。
・Mobile KVM Client (MKC) は廃止されました。今後リリースされる Dominion KX III では、HTML KVM Client (HKC) を機能拡張することにより、Apple 社の iPhone と iPad にて利用できる予定です。
・CC-SG Web Services API を利用するためには、新しいセキュリティ証明書をインストールする必要があります。

製品ドキュメントの更新

・本リリースにより、以下のドキュメントが更新されました。（英語版のみ）

・CC-SG 管理者ガイド、ユーザーガイド、オンラインヘルプ

・CC-SG 7.0 アップグレードガイド（ファームウェアアップグレードに関する詳細説明）

・CC-SG 仮想アプライアンス向けクイックセットアップガイド（ライセンスサーバー無し向け）

・CC-SG WS-API プログラミングガイド

7.0 へのアップグレードパス

6.0、6.1、6.2 をご利用の場合、直接 7.0 へのアップグレードが可能です。
その他のアップグレードにつきましては、CC-SG のタイプ（「ハードウェアアプライアンス」と「仮想アプライアンス」のいずれか）、ライセンスによって異なります。

1. ハードウェアアプライアンス（CC-SG V1 および E1）

・CC-SG 5.x をご利用の場合、はじめに 6.0 へアップグレードしてから、7.0 へアップグレードする必要があります。
・CC-SG 3.x および 4.x をご利用の場合、5.0 → 6.0 → 7.0 といったアップグレード手順となります。
・**以下のハードウェアアプライアンスは、7.0 へアップグレードすることはできません。**
CC-SG-V1-A, CC-SG-V1-1（2009 年以前のモデル）, CC-SG-E-0

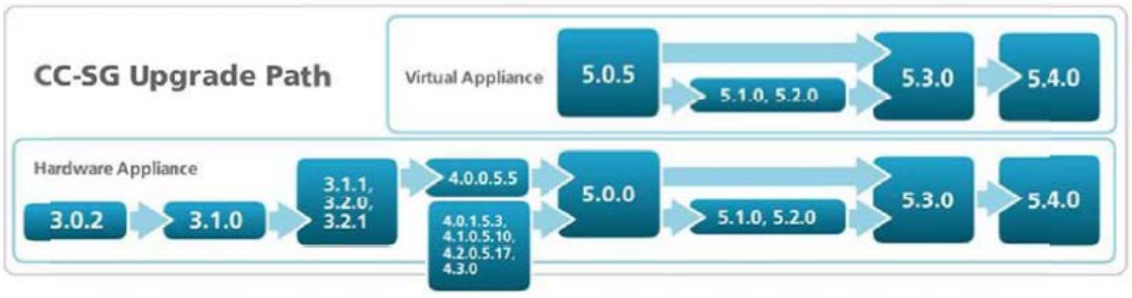
2. 仮想アプライアンス －ライセンスサーバー無し（5.3／5.4）

・CC-SG 5.3／5.4 をご利用の場合、6.0 → 7.0 といったアップグレード手順となります。

3. 仮想アプライアンス －ライセンスサーバーあり（5.0.5／5.1／5.2／5.3／5.4）

1）5.0.5／5.1／5.2 をご利用の場合、5.3 へ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必要分取得し、当該ライセンスサーバーから移行する必要があります。ラリタンのサポート窓口へご連絡いただき、新たなライセンスファイルを所得してから、CC-SG ライセンスマネージャーにて新しいライセンスを必要分アップロードしてください。ライセンス認証を再び行った後、CC-SG 6.0 へアップグレードが可能となります。
3）上記手順完了後、6.0 から 7.0 へアップグレードが行えます。

※特定の古い CC-SG へアップグレードが必要な場合は、以下のアップグレードパスをご参照ください。



アップグレードに関する追加情報

仮想アプライアンス：
・4GB のメモリが必要です。
・7.0 へアップグレードする前に仮想マシンに 40GB の HDD を追加する必要があります。

ハードウェアアプライアンス：
・CC-SG V1 もしくは E1 は 7.0 へのアップグレードが可能ですが、CC-G1 以前はアップグレードできません。また、以下の旧製品は、アップグレード対象外です。

- CC-SG-V1-A
- CC-SG-V1-1（2009 年以前のモデル）
- CC-SG-E-0

その他：
・アップグレードを実施する際には、アップグレード前と後でそれぞれバックアップを実施してください。もし、段階アップグレードの場合は、その都度実施するようにしてください。
・ご利用の構成によっては、CC-SG 以外のラリタン製品のアップグレードが必要になる事があります。
CC-SG 7.0 のサポート対象デバイスの一覧は、「互換性マトリックス」（Compatibility Matrix）を参照してください。管理対象となる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。
・アップグレード手順の詳細については、CC-SG 7.0 アップグレードガイドを参照してください。
・ご不明点は、ラリタンのサポート窓口までお問い合わせください。

特記事項および制限事項

1. 3.0 は、セキュリティの問題により初期状態では無効となっています。古い機器との接続のために、有効にすることは可能です。
2. TLS1.0 は、以下のラリタン製品を利用する場合に必要です。

   KX2 v2.7, KSX2 v2.7, LX v2.7, KX2-101v2 v3.7

3. Java 非依存の HTML KVM とシリアルクライアントは、Proxy モードでは動作しません。
4. KVM およびシリアルクライアントの電源制御を行なう場合は、ラリタン製 PX シリーズの PDU を D2CIM-PWR を介して Dominion 製品に接続する必要があります。
5. ブラウザで Java を無効にして HKC を自動的に起動するためには、「コントロールパネル」に用意された「Java」をクリックして「Java コントロール・パネル」を起動して、「セキュリティ」タブの「ブラウザおよび Web Start アプリケーションで Java コンテンツを有効にする」のチェックボックスを解除します。

6. VMware の Web Viewer を使用するためには、証明書をインストール必要があります。

7. 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ができません。今後のアップデートで修正見込みです。

8. IPv6 の利用：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。

・Admin Client は、IPv6 環境で Firefox 6 ～12 を使用することはできません。回避策として、ユーザー証明書のインストールが挙げられます。詳細は管理者ガイドをご参照ください。

・IPv6 環境で VNC を使用する場合、Real VNC サーバーの設定において「Prefer On」を選択してください。

・IPv6 環境における制限事項は、管理者ガイドを参照ください。

9. Windows 7 用の VNC および RDP のインターフェースを追加する場合、ICMPv4 と ICMPv6 を Windows Firewall で許可してください。

10. CC-SG 経由で iLO3 の 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 社のアップレットに署名が無いため発生します。

11. サポート対象外の Java のバージョンは、v6 と v7 となります。組み込み型サービスプロセッサのバージョンによっては、最新の Java へのアップデート対応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」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「例外サイト・リスト」を使用してください。

12. RSA リモートコンソールは、JRE1.6.0_10 以降を使用する場合、CC-SG から起動することができません。IBM から回避策が掲示されていますので、ご参照ください。

http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396

13. ASS-256bit 暗号化を有効にする場合、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 JCE Unlimited Strength Jurisdiction Policy ファイルをインストールしてください。

14. CC-SG は無料試用版ライセンスで動作する ESXi の仮想ノードに対する管理と接続はできません。

15. VMware クライアントを利用する場合、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。

16. DRAC5 をターゲットとしてアクセスする場合、SSH 同時接続数は 4 つに制限されます。

17. 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未対応の場合、電源制御のためにグレースフルシャットダウンの操作を実行すると、「graceful shutdown not supported」（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。

18. SNMPv3 オプションおよび MGSOFT MIB Browser を使用する場合、「Authentication Passphrase」（認証パスワード）と「Privacy Passphrase」（個別パスワード）は異なるものでなければなりません。

このように設定されていない場合、CC-SG が SNMP トラップを送信しても、ブラウザの情報は反映されません。

19. CC-SG の HTML ベースの Access Client では、Chrome バージョン 45 以降および Edge ブラウザからインバンドインターフェースを起動することはできません。インバンドインターフェースを使用する予定の場合、少なくとも他のブラウザをご使用になることをお勧めします。インバンドインターフェースでこれらのブラウザを使用する必要がある場合は、Java ベースの CC-SG Admin Client を使用してインバンドインターフェースにアクセスしてください。ただし、iLO、DRAC、RSA は起動しません。