

CC4U(CSC版)におけるセキュリティ対策

CC4U(CSC版)におけるセキュリティ対策まとめ

1. 利用者の悪意のない誤操作によるセキュリティ確保
 - ① 「ゲストOS」の全画面実行(Kioskモード)のみとし、「ホストOS」の画面には入れません。
 - ② 「ゲストOS」の画面キャプチャは、「ホストOS」できません。
 - ③ 「ゲストOS」と「ホストOS」間で、ファイルとテキスト、および全てのデータはコピーアンドペーストはできません。
 - ④ 「ゲストOS」から「ホストOS」経由で、印刷することはできません。
 - ⑤ シリアル接続、USB接続などの外部接続周辺機器は、接続できません。

2. 利用者の興味からくる操作に対するセキュリティ対策
 - ① USBメモリを丸ごとコピーしてもUSBのデバイスIDをMokaFive 管理サーバで登録しているため、使えないようになっています。(よって、Windows XP Embeddedのライセンス管理にもなり、マイクロソフト社がEmdeddedをUSBに搭載して出荷しても良いと認めた唯一のしくみになります。)
 - ② 「ゲストOS」を仮想化するソフトウェアのVMwareは、完全にMokaFiveで制御されており、利用者は動作環境の変更ができません。
 - ③ 「ゲストOS」と「ホストOS」間の通信は、NAT(ネットワークアドレス変換)接続されており、VPNは「アプリケーション(APP)」とCSCサーバで終端されています。またCC4Uは、プライベートアドレスを割り当てているため、利用者はその間のデータを操作することはできません。

3. OS、アプリケーションS/Wの不具合に対するセキュリティと対策
 - ① 「ゲストOS」と「APP(アプリケーション)」は、カプセル化されており独立した環境となっていますので、一般に「ホストOS」上の他のアプリケーションS/W(ウイルスもこの1種です)から直接の影響を受けることはありません。
 - ② 「ゲストOS」と「APP(アプリケーション)」は、「ホストOS」よりも特権レベルが低く、「ゲストOS」と「APP(アプリケーション)」の不具合によって「ホストOS」やH/Wが、破壊されることはありません。
 - ③ 「ホストOS」にウイルスがいた場合は、「ゲストOS」にウイルスが感染する可能性があります。しかし、CC4Uでは「ゲストOS」にWindows XP Embeddedを使用しており、ウイルスに感染しても、その書き込み保護機能を使うため、再起動を行うと元のきれいな状態に戻ります。つまりハードウェアシンクライアントと同じセキュリティレベルです。
 - ④ 万一、CC4Uに害を与えるウイルスが発見されて、その対策を行う必要が生じた場合は、仮想化ソフトウェア(VMware、MokaFive)や「ゲストOS」、「APP(アプリケーション)」を通信機能を用いて一括アップデートできる機能を備えています。

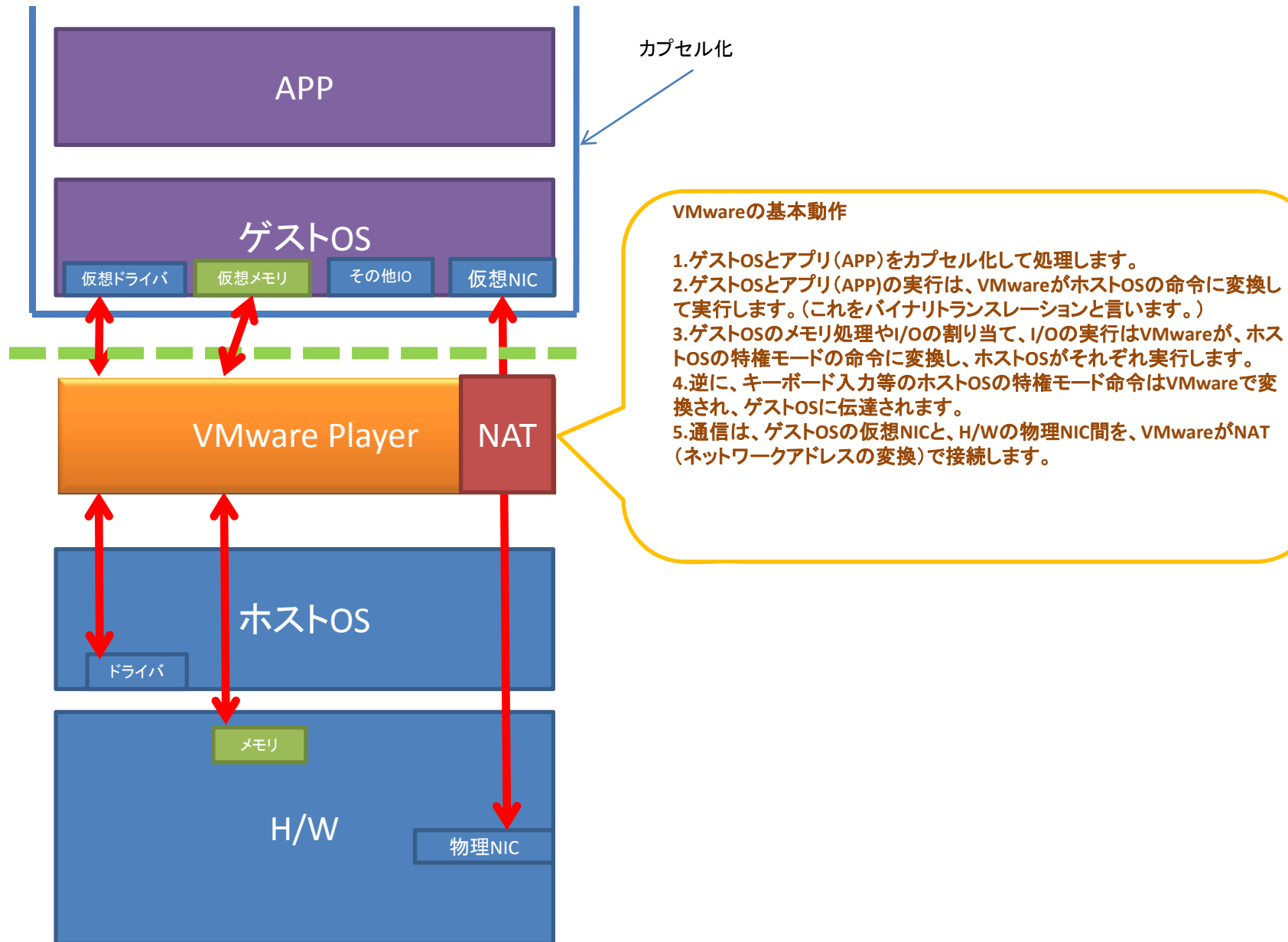
4. H/Wの動作に対するセキュリティ対策
 - ① 「ゲストOS」から「ホストOS」のI/Oを動作させる場合の対策は、上記1のとおりです。
 - ② キーロガーについては、VMwareで影響を受けにくくしています。

5. デジカメ、筆記などに対するセキュリティ対策
 - ① 対応しておりません。

各要素のセキュリティの役割

| 項目 | Windows XP Embedded | VMware Player | MokaFive Player | CSC(簡単VPN) |
|--|---------------------|---------------|-----------------|------------|
| 1. 利用者の悪意のない誤操作によるセキュリティ確保 | | | | |
| 「ゲストOS」の全画面実行(Kioskモード)のみとし、「ホストOS」の画面には入れません。 | | | ○ | |
| 「ゲストOS」の画面キャプチャは、「ホストOS」できません。 | | | ○ | |
| 「ゲストOS」と「ホストOS」間で、ファイルとテキスト、および全てのデータはコピーアンドペーストはできません。 | | | ○ | |
| 「ゲストOS」から「ホストOS」経由で、印刷することはできません。 | | | ○ | |
| シリアル接続、USB接続などの外部接続周辺機器は、接続できません。 | | | ○ | |
| 2. 利用者の興味からくる操作に対するセキュリティ対策 | | | | |
| USBメモリを丸ごとコピーしてもUSBのデバイスIDをMokaFive管理サーバに登録しているため、使えないようになっています。 | | | ○ | |
| 「ゲストOS」を仮想化するソフトウェアのVMwareは、完全にMokaFiveで制御されており、利用者は動作環境の変更ができません。 | | | ○ | |
| 「ゲストOS」と「ホストOS」間の通信は、NAT(ネットワークアドレス変換)接続されており、VPNは「アプリケーション(APP)」とCSCサーバで終端されています。またCC4Uは、プライベートアドレスを割り当てているため、利用者はその間のデータを操作することはできません。 | | ○ | | ○ |
| 3. OS、アプリケーションS/Wの不具合に対するセキュリティと対策 | | | | |
| 「ゲストOS」と「APP(アプリケーション)」は、カプセル化されており独立した環境となっていますので、一般に「ホストOS」上の他のアプリケーションS/W(ウイルスもこの1種です)から直接の影響を受けることはありません。 | | ○ | | |
| 「ゲストOS」と「APP(アプリケーション)」は、「ホストOS」よりも特権レベルが低く、「ゲストOS」と「APP(アプリケーション)」の不具合によって「ホストOS」やH/Wが、破壊されることはありません。 | | ○ | | |
| 「ホストOS」にウイルスがいた場合は、「ゲストOS」にウイルスが感染する可能性があります。しかし、CC4Uでは「ゲストOS」にWindows XP Embeddedを使用しており、ウイルスに感染しても、その書き込み保護機能を使うため、再起動を行うと元のきれいな状態に戻ります。つまりハードウェアシンクライアントと同じセキュリティレベルです。 | ○ | | | |
| 万一、CC4Uに害を与えるウイルスが発見されて、その対策を行う必要が生じた場合は、仮想化ソフトウェア(VMware、MokaFive)や「ゲストOS」、「APP(アプリケーション)」を通信機能を用いて一括アップデートできる機能を備えています。 | | | ○ | |
| 4. H/Wの動作に対するセキュリティ対策 | | | | |
| キーロガーについては、VMwareで影響を受けにくくしています。 | | ○ | | |

VMwareの仕組み(概要)



CC4U(CSC版)の仕組み(概要)

