

セキュリティ情報（2008年8月20日）

日立ディスクアレイサブシステムにおけるSVPセキュリティホール （新規：MS08-041～051／更新：MS07-047、MS08-022、MS08-033、MS08-040）対策について

2008年8月20日

（株）日立製作所RAIDシステム事業部

1. 日立ディスクアレイサブシステムに対するセキュリティホール対策のお知らせ

Microsoft製品に対して、以下に示すセキュリティホールが公開されました。

【新規】

- MS08-041：Microsoft Access Snapshot ViewerのActiveXコントロールの脆弱性により、リモートでコードが実行される（955617）
- MS08-042：Microsoft Wordの脆弱性により、リモートでコードが実行される（955048）
- MS08-043：Microsoft Excelの脆弱性により、リモートでコードが実行される（954066）
- MS08-044：Microsoft Officeフィルターの脆弱性により、リモートでコードが実行される（924090）
- MS08-045：Internet Explorer用の累積的なセキュリティ更新プログラム（953838）
- MS08-046：Microsoft Image Color Management Systemの脆弱性により、リモートでコードが実行される（952954）
- MS08-047：IPsecポリシーの処理の脆弱性により、情報漏えいが起こる（953733）
- MS08-048：Outlook ExpressおよびWindowsメール用のセキュリティ更新プログラム（951066）
- MS08-049：イベントシステムの脆弱性により、リモートでコードが実行される（950974）
- MS08-050：Windows Messengerの脆弱性により、情報の漏えいが起こる（955702）
- MS08-051：Microsoft PowerPointの脆弱性により、リモートでコードが実行される（949785）

【更新】

- MS07-047：Windows Media Playerの脆弱性により、リモートでコードが実行される（936782）
- MS08-022：VBScriptおよびJScriptスクリプトエンジンの脆弱性により、リモートでコードが実行される（944338）
- MS08-033：DirectXの脆弱性により、リモートでコードが実行される（951698）
- MS08-040：Microsoft SQL Serverの脆弱性により、特権が昇格される（941203）

日立ディスクアレイサブシステムのSVPにおける、上記1～15の脆弱性の影響は下記の通りです。

- 本件は、Microsoft Access Snapshot Viewerの脆弱性により、リモートでコードが実行されるというものです。SVPはサブシステム管理専用装置であり、Microsoft Access Snapshot Viewerがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、Microsoft Wordの脆弱性により、リモートでコードが実行されるというものです。SVPはサブシステム管理専用装置であり、Microsoft Wordがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、Microsoft Excelの脆弱性により、リモートでコードが実行されるというものです。SVPはサブシステム管理専用装置であり、Microsoft Excelがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、Microsoft Officeフィルターの脆弱性により、リモートでコードが実行されるというものです。SVPはサブシステム管理専用装置であり、Microsoft Officeがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、Internet Explorerの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページまたは電子メールメッセージを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、Microsoft Image Color Management Systemの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施された画像ファイルを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
- 本件は、IPsecポリシーの処理の脆弱性により、情報漏えいが起こるというものです。SVPでは、IPsecを使用していません。このため、SVPでは本脆弱性の影響は受けません。

8. 本件は、Outlook ExpressおよびWindowsメールの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページまたは電子メールメッセージを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
9. 本件は、イベント システムの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、攻撃対象となるコンピュータにログオンし、特別な細工が施されたアプリケーションを実行する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
10. 本件は、Windows Messengerの脆弱性により、情報の漏えいが起こるといいます。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページまたは電子メールメッセージを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
11. 本件は、Microsoft PowerPointの脆弱性により、リモートでコードが実行されるというものです。SVPはサブシステム管理専用装置であり、Microsoft PowerPointがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。
12. 本件は、Windows Media Playerの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
13. 本件は、VBScriptおよびJScriptスクリプトエンジンの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
14. 本件は、DirectXの脆弱性により、リモートでコードが実行されるというものです。本脆弱性を攻撃者が悪用するには、特別な細工が施されたWebページまたは電子メールメッセージを表示させるように、SVP使用者（保守員）を誘導する必要があります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
15. 本件は、Microsoft SQL Serverの脆弱性により、特権が昇格されるというものです。SVPはサブシステム管理専用装置であり、Microsoft SQL Serverがインストールされることはありません。このため、SVPでは本脆弱性の影響は受けません。

よって、今回公開された脆弱性については特に対策の必要はありません。

2. 対象製品

Hitachi Universal Storage Platform V、Hitachi Universal Storage Platform H24000、Hitachi Universal Storage Platform VM、Hitachi Universal Storage Platform H20000、Hitachi Universal Storage Platform、Hitachi Universal Storage Platform H12000、Hitachi Network Storage Controller、Hitachi Universal Storage Platform H10000、SANRISE9980V/9970V、SANRISE9980V-e/9970V-e、SANRISE H1024/ H128

注：Hitachi Adaptable Modular Storage、Hitachi Workgroup Modular Storage、Hitachi Simple Modular Storage、SANRISE9500Vシリーズ、SANRISE 2000/2000-e/1000シリーズ、およびSANRISE H512/H48は影響を受けません。

3. Storage Navigatorのご使用について

Storage Navigatorのご使用については、Storage Navigator機能に限ったご使用であれば特に問題ありません。

クライアントPCを他の用途でもご利用されている場合、ご利用内容によっては今回の脆弱性の影響を受ける可能性があります。

詳しくはメーカーにお尋ねいただくか、以下のセキュリティサイトをご確認の上対応をお願い致します。

<http://www.microsoft.com/japan/>

本セキュリティホールに関する情報

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-041.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-042.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-043.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-044.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-045.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-046.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-047.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-048.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-049.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-050.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-051.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-047.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-022.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-033.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms08-040.msp>

本件に関する問合せ窓口

(株)日立製作所RAIDシステム事業部 販売推進本部 販売企画部

[問い合わせ先はこちら](#)

-
- *1 弊社では、セキュリティ対応に関して正確な情報を提供できるよう努力しておりますが、セキュリティ問題に関する情報は変化しており、当ホームページに記載している内容を予告なく変更することがありますので、あらかじめご了承ください。情報ご参照の際には、常に最新の情報をご確認いただくようお願いいたします。
- *2 当ホームページに記載されている製品には、他社開発製品が含まれております。これらのセキュリティ情報については他社から提供、または公開された情報を基にしております。弊社では、情報の正確性および完全性について注意を払っておりますが、開発元の状況変化に伴ない、当ホームページの記載内容に変更が生じることがあります。
- *3 当ホームページはセキュリティ情報の提供を目的としたものであり、法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして、弊社では責任を負いかねます。

[ページの先頭へ](#)