

セキュリティ情報（2007年2月16日）



SANRISEシリーズにおけるSVPセキュリティホール (新規：MS07-005～016／更新：MS06-058) 対策について

2007年2月16日
(株) 日立製作所RAIDシステム事業部

1. SANRISEシリーズ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】

- MS07-005：ステップ バイ ステップの対話型トレーニングの脆弱性により、リモートでコードが実行される (923723)
- MS07-006：Windowsシエルの脆弱性により、特権が昇格される (928255)
- MS07-007：Windows Image Acquisitionサービスの脆弱性により、特権が昇格される (927802)
- MS07-008：HTMLヘルプの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 (928843)
- MS07-009：Microsoft Data Access Componentsの脆弱性により、リモートでコードが実行される (927779)
- MS07-010：Microsoft Malware Protection Engineの脆弱性により、リモートでコードが実行される (932135)
- MS07-011：Microsoft OLEダイアログの脆弱性により、リモートでコードが実行される (926436)
- MS07-012：Microsoft MFCの脆弱性により、リモートでコードが実行される (924667)
- MS07-013：Microsoftリッチエディットの脆弱性により、リモートでコードが実行される (918118)
- MS07-014：Microsoft Wordの脆弱性により、リモートでコードが実行される (929434)
- MS07-015：Microsoft Officeの脆弱性により、リモートでコードが実行される (932554)
- MS07-016：Internet Explorer用の累積的なセキュリティ更新プログラム (928090)

【更新】

- MS06-058：Microsoft PowerPointの脆弱性により、リモートでコードが実行される (924163)

弊社のSANRISEシリーズのSVPにおける、上記1～13の脆弱性の影響は下記の通りです。

- 本件は、ステップ バイ ステップの対話型トレーニングの脆弱性により、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。
- 本件は、Windowsシエルの脆弱性により、特権が昇格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、攻撃対象の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。
- 本件は、Windows Image Acquisitionサービスの脆弱性により、特権が昇格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、攻撃対象のコンピュータにローカルでログオンし、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。
- 本件は、HTMLヘルプの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 Data Access Components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 Malware Protection Engine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、本脆弱性の影響を受けるアプリケーション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 OLEダイアログの脆弱性により、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。

8. 本件は、Microsoft MFC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、Microsoft リッチエディットの脆弱性により、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。
10. 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。
11. 本件は、Microsoft Office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。
12. 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。
13. 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。

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、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、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/ms07-005.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-006.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-007.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-008.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-009.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-010.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-011.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-012.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-013.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-014.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-015.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms07-016.msp>

<http://www.microsoft.com/japan/technet/security/bulletin/ms06-058.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](#)

[サイトの利用条件](#) | [個人情報保護に関して](#) | [商品名称について](#) | [更新履歴](#)

© Hitachi, Ltd. 1994, 2022. All rights reserved.