

セキュリティ情報（2004年7月20日）

SANRISE9900V/2000シリーズにおけるTCPプロトコルの脆弱性対策について

2004年7月20日
(株)日立製作所RAIDシステム事業部

1. SANRISE9900V/2000シリーズに対するTCPプロトコルの脆弱性のお知らせ

インターネット等で広く利用されているTCPプロトコルの脆弱性に関して、下記の情報が公開されました。

1. NISCC Vulnerability Advisory 236929
Vulnerability Issues in TCP
2. JPCERT/CC
TCP プロトコルに潜在する信頼性の問題 Potential Reliability Issue in TCP

弊社のSANRISE9900V/2000シリーズにおける、上記脆弱性の影響は下記の通りです。

1. SANRISE9900V/2000シリーズは、TCPプロトコルを搭載しておりますが、通常の構成/運用では、この脆弱性の影響は受けません。

よって、上記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

SANRISE9980V/9970V、SANRISE9980V-e/9970V-e、SANRISE H1024/ H128、SANRISE 2000/2000-e シリーズ、およびSANRISE H512/H48

3. Remote Console Storage Navigatorのご使用について

Remote Console Storage Navigatorのご使用については、Remote Console 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。

NISCC

<http://www.uniras.gov.uk/vuls/2004/236929/index.htm>

JPCERT/CC

<http://www.jpCERT.or.jp/at/2004/at040003.txt>

更新履歴

- 2004年7月20日 調査中を対策不要情報に更新
- 2004年4月28日 NISCCに基づく情報に訂正
- 2004年4月23日 新規情報掲載

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す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。

