

# ソフトウェア製品セキュリティ情報

## Software Vulnerability Information

ソフトウェア事業部 (Software Division)

| ホーム | 製品&amp;サービス | &gt;&gt; セキュリティ |

▶ 英語ページへ

**HITACHI**  
 Inspire the Next

日立サイトの検索 by Google

&gt; GO

&gt; 詳細な検索

ホーム &gt; 製品セキュリティ情報 &gt; ソフトウェア事業部セキュリティ情報 &gt; HS05-002

2005.01.31更新

## JP1/VERITAS Backup Execバッファオーバーフロー攻撃 に関するセキュリティ問題

### ■ 影響がある製品

対策	製品名	適用OS	更新日
HS05-002-01	JP1/VERITAS Backup Exec VERITAS Backup Exec	Windows	2005.01.31

### ■ 問題の説明

2005.01.17, VERITAS社TechNoteにてBackup Exec 8.x および 9.x におけるスタック上のバッファオーバーフローに対する脆弱性を利用し、遠隔地から不正に任意のコードが実行される危険性についてが公表されました。

上記の製品のバックアップサーバにおいて、外部から悪意のあるユーザによるバッファオーバーフロー攻撃を受けることで、任意のコマンドを実行することができてしまう脆弱性があります。

&gt; トップ

 ▼ What's New
 

- > お知らせ
- > 御参考 (警告情報など)

&gt; ソフトウェア製品セキュリティ情報

&gt; セキュリティ対応機関へのリンク

 > お問い合わせ  
[soft-security@itg.hitachi.co.jp](mailto:soft-security@itg.hitachi.co.jp)

個人情報保護ポリシーにご同意頂ける場合のみ、上記アドレスをご利用下さい。ご同意頂けない場合には、お問い合わせに回答できない場合があります。

なお、入力頂いた個人情報は本ポリシーに従って適切に管理し、問合せ対応のためにのみ使用します。第三者への個人情報の提供、預託、開示は法令に基づく場合を除いて行いません。

お問い合わせへの回答後、個人情報は当社が責任を持って適切に廃棄いたします。

&gt; 日立および他社の商品名称に関する記述

## 更新履歴：

- 2005.01.31：このセキュリティ情報ページを新規作成および発信しました。



- 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に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、当ホームページで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。
- 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。
- 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。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

 [ページトップへ](#)

## ソフトウェア製品セキュリティ情報

Software Vulnerability Information

ソフトウェア事業部 (Software Division)

| ホーム | 製品&amp;サービス | &gt;&gt; セキュリティ |

&gt;&gt; 英語ページへ

HITACHI  
Inspire the Next

日立サイトの検索 by Google

&gt; GO

&gt; 詳細な検索

ホーム &gt; 製品セキュリティ情報 &gt; ソフトウェア事業部セキュリティ情報 &gt; HS05-002-01

2005.01.31更新

HS05-002;

JP1/VERITAS Backup Execバッファオーバーフロー攻撃に関するセキュリティ問題

JP1/VERITAS Backup Execの対策

JP1/VERITAS Backup Exec, VERITAS Backup Execに次のセキュリティ上の問題があることが判明しました。

バックアップサーバにおいて、外部から悪意のあるユーザによるバッファオーバーフロー攻撃を受けることで、任意のコマンドを実行することができてしまう脆弱性があります。

つきましては、下記に従い回避策または対策をお願いします。

## [影響範囲]

JP1/VERITAS Backup Exec, VERITAS Backup Execのバックアップサーバの問題です。リモートエージェント側のサーバでは発生しません。

## [該当形名・バージョン]

対象となる日立製品と、これに対応するVERITAS社製品は以下のとおりです。

製品名	形名	対象バージョン	VERITAS社製品名/ バージョン	更新日

&gt; トップ

 > What's New
 

- > お知らせ
- > 御参考（警告情報など）

&gt; ソフトウェア製品セキュリティ情報

&gt; セキュリティ対応機関へのリンク

&gt; お問い合わせ

[soft-security](#)
[@itg.hitachi.co.jp](mailto:@itg.hitachi.co.jp)

個人情報保護ポリシーにご同意頂ける場合のみ、上記アドレスをご利用下さい。ご同意頂けない場合には、お問い合わせに回答できない場合があります。

なお、入力頂いた個人情報は本ポリシーに従って適切に管理し、問合せ対応のためにのみ使用します。第三者への個人情報の提供、預託、開示は法令に基づく場合を除いて行いません。

お問い合わせへの回答後、個人情報は当社が責任を持って適切に廃棄いたします。

&gt; 日立および他社の商品名称に関する記述

JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01	VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	2005.01.31
		07-00	VERITAS Backup Exec 9.1 for Windows Servers revision4691	2005.01.31
	RT-1V25-K2WL10	07-01	VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	2005.01.31
		07-00	VERITAS Backup Exec 9.1 for Windows Servers revision4691	2005.01.31
JP1/VERITAS Backup Exec 9.0 for Windows Servers	RT-1V25-K1W110	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	2005.01.31
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	2005.01.31
	RT-1V25-K1WL10	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	2005.01.31
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	2005.01.31
	RT-1V25-K1WU10	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	2005.01.31
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	2005.01.31
	RT-1V25-	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	2005.01.31

	K1WU20	06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	2005.01.31
	RT-1V25- K1WU30	06-73, 06-74	VERITAS Backup Exec 9.0 for Windows Servers revision4454	2005.01.31
		06-72	VERITAS Backup Exec 9.0 for Windows Servers revision4367	2005.01.31
JP1/VERITAS Backup Exec for Windows NT/Windows 2000 V8.6	RT-1V25- ANTAS126	06-70	VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3878	2005.01.31
	RT-1V25- ANTAS130			2005.01.31
	RT-1V25- ANTSR104			2005.01.31
	RT-1V25- ANTSR105			2005.01.31
	RT-1V25- YNTSR104			2005.01.31
VERITAS Backup Exec for Windows NT/Windows 2000 V8.6	RT-1V25- 3NTSR104	08-60	VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3808 または VERITAS Backup Exec for Windows NT/Windows 2000 V8.6 revision3878 (注1)	2005.01.31
	RT-1V25- 3NTSR105			2005.01.31
	RT-1V25- 3NTSR114			2005.01.31
	RT-1V25- ZNTSR104			2005.01.31
	RT-1V25- 3NTAS126			2005.01.31
	RT-1V25- 3NTAS130			2005.01.31
VERITAS Backup Exec for Windows	RT-1V25- 2NTAS860	08-50	VERITAS Backup Exec for Windows NT/Windows 2000	2005.01.31
	RT-1V25- 2NTAS890			2005.01.31

NT/Windows 2000 V8.5	RT-1V25- 2NTSR720	V8.5	2005.01.31
----------------------	----------------------	------	------------

(注1) 対応するVERITAS社製品のrevision番号は、revision3878かrevision3808のいずれかです。いずれかは、Backup ExecのGUIを立ち上げ、[ヘルプ] - [バージョン情報] により確認してください。

#### [回避策]

バックアップ保護するサーバをFirewallの内部で使用する。もしくは、IPフィルタリングする。

#### [対策]

- サポートサービスをご契約されているお客様  
JP1/VERITASサポートサービスのホームページで、詳細の対策手順を説明していますので、参照し対策をお願いします。
- サポートサービスをご契約されていないお客様  
VERITAS社の以下のホームページを参照し、対策をお願いします。

<http://www.veritas.com/jp/support/shared/technotes/J273419/J273419.htm>

(注2)revisionやService Packの適用は、バックアップサーバおよびリモートエージェント側のサーバの両方で必要です。

#### ダウンロード先 (英文)

##### 9.1 Service Pack

1 : <http://seer.support.veritas.com/docs/267180.htm>

##### 9.1.4691 Hotfix

40 : <http://seer.support.veritas.com/docs/273420.htm>

##### 9.0 revision

4454 : <http://seer.support.veritas.com/docs/258718.htm>

9.0 Service Pack

1 : <http://seer.support.veritas.com/docs/267151.htm>

9.0.4454 Hotfix

30 : <http://seer.support.veritas.com/docs/274298.htm>

8.6 revision

3878 : <http://seer.support.veritas.com/docs/241038.htm>

8.60.3878 Hotfix

68 : <http://seer.support.veritas.com/docs/273850.htm>

更新履歴 :

- 2005.01.31 : JP1/VERITAS Backup Execのバッファオーバーフロー攻撃に関するセキュリティ問題の情報を公開しました。

- 
- 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に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、当ホームページで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。
  - 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。
  - 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。

- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

 [ページトップへ](#)

[！サイトの利用条件！](#) [！個人情報保護ポリシー！](#) [！日立について！](#)

©Hitachi, Ltd. 1994, 2008. All rights reserved.