

# 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; HS06-015

2006.09.08更新

## JP1/VERITAS Backup Exec for Windows Servers の RPC インターフェース・ヒープ・オーバーフローによる脆弱 性問題について

### ■ 影響がある製品

対策	製品名	適用OS	更新日
HS06-015-01	JP1/VERITAS Backup Exec	Windows	2006.09.08

### ■ 問題の説明

Symantec社 (旧VERITAS社) TechNoteにてSymantec Backup Exec for Windows Server : RPC インターフェース・ヒープ・オーバーフローによりアクセス権を持つユーザに特権昇格の可能性が公表されました。

上記の製品において、この脆弱性を利用した悪意のある第三者からの攻撃により、任意のコードを実行される可能性があります。

&gt; トップ

 > What's New
 

- > お知らせ
- > 御参考 (警告情報など)

 > ソフトウェア製品セキュリティ情報
 

- > 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:@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：



- 2006.09.08 : 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&サービス](#) | [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

[> 詳細な検索](#)[ホーム](#) > [製品セキュリティ情報](#) > [ソフトウェア事業部セキュリティ情報](#) > HS06-015-01

2006.09.08更新

HS06-015;

JP1/VERITAS Backup Exec for Windows Servers の RPC インターフェース・ヒープ・オーバーフローによる脆弱性問題について

## JP1/VERITAS Backup Execの対策

JP1/VERITAS Backup Execにおきまして、RPC インターフェース・ヒープ・オーバーフローによる脆弱性があることが判明しました。  
つきましては、下記に従い対策をお願いします。

### [影響範囲]

JP1/VERITAS Backup Execのメディアサーバ、および、リモートエージェントがインストールされているサーバすべてが対象となります。

(Symantec社、セキュリティ・レスポンスID: SYM06-014)

RPC インターフェースにおいて、ヒープ・オーバーフローの問題が発生するという報告を受けました。 Remote Agentsモジュールを適用されている環境（バックアップサーバ本体であるメディアサーバを含む）において、ユーザ入力の不適切な妥当性チェックと後処理によってオーバーフローが

[> トップ](#)[> What's New](#)[> お知らせ](#)[> 御参考（警告情報など）](#)[> ソフトウェア製品セキュリティ情報](#)[> セキュリティ対応機関へのリンク](#)[> お問い合わせ](#)[soft-security](mailto:soft-security@itg.hitachi.co.jp)[@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。

[> 日立および他社の商品名称に関する記述](#)

発生します。この脆弱性を悪用することにより、標的システムで任意のコードが実行され、ユーザ権限が昇格される恐れがあります。

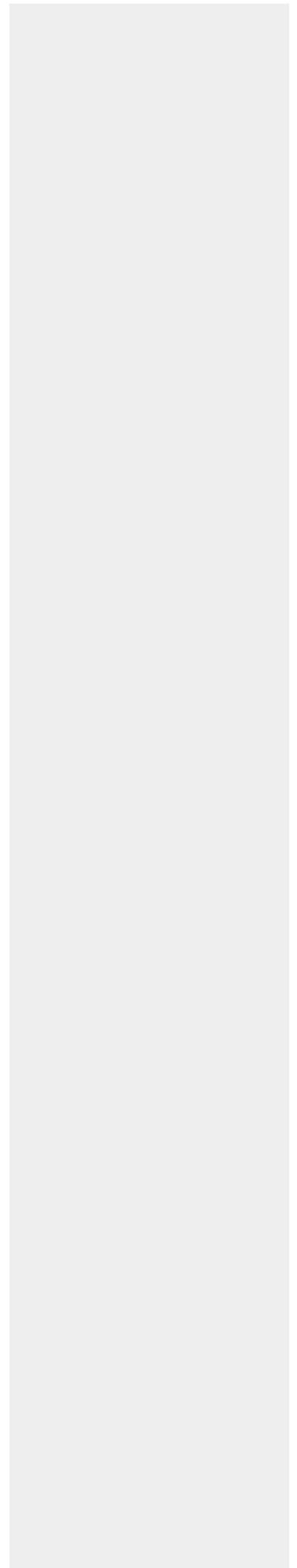


[該当形名・バージョン]

対象となる日立製品と、これに対応するSymantec社（旧VERITAS社）の製品は以下のとおりです。

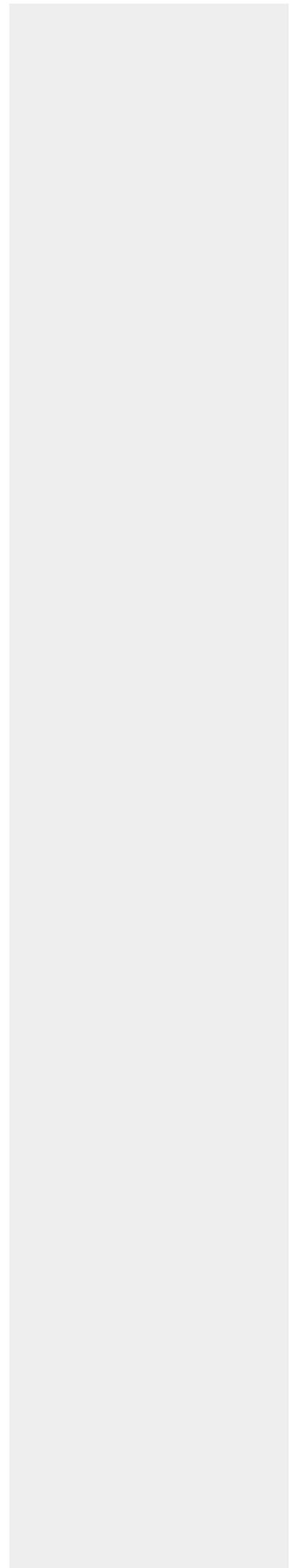
製品名 (注1)	形名	対象 バー ジヨ ン	適用OS	Symantec社（旧 VERITAS社）製品 名/バージョン	更新日
JP1/VERITAS Backup Exec 10d for Windows Servers	RT-1V25-K4W110	07-60		Symantec Backup Exec 10d (10.1) for Windows Servers rev. 5629	2006.09.08
		07-61		Symantec Backup Exec 10d (10.1) for Windows Servers rev. 5629	2006.09.08
	RT-1V25-K4WL10	07-60		Symantec Backup Exec 10d (10.1) for Windows Servers rev. 5629	2006.09.08
		07-61		Symantec Backup Exec 10d (10.1) for Windows Servers rev. 5629	2006.09.08
			07-60		Symantec Backup Exec 10d Windows リモー

	RT-1V25-K4WC10			トエージェント (CAL)1ライセンス	
		07-61		Symantec Backup Exec 10d (10.1) for Windows Servers rev. 5629	2006.09.08
JP1/VERITAS Backup Exec 10.0 for Windows Servers	RT-1V25-K3W110	07-52		VERITAS Backup Exec 10.0 for Windows Servers revision5520	2006.09.08
		07-51		VERITAS Backup Exec 10.0 for Windows Servers revision5484 SP1	2006.09.08
		07-50		VERITAS Backup Exec 10.0 for Windows Servers revision5484	2006.09.08
		07-52		VERITAS Backup Exec 10.0 for Windows Servers revision5520	2006.09.08
	RT-1V25-K3WL10	07-51		VERITAS Backup Exec 10.0 for Windows Servers revision5484 SP1	2006.09.08
		07-50		VERITAS Backup Exec 10.0 for Windows Servers revision5484	2006.09.08
	RT-1V25-K3WC10	07-52	Windows	VERITAS Backup Exec 10.0 Windows リモー トエージェント (CAL) 1 ライ	2006.09.08



	RT-1V25-K3WA10	07-51
	RT-1V25-K3WA20	07-50
JP1/VERITAS Backup Exec 9.1 for Windows Servers	RT-1V25-K2W110	07-01
		07-00
	RT-1V25-K2WL10	07-01
		07-00
	RT-1V25-K2WC10	07-01

センス	
VERITAS Backup Exec 10.0 Windows リモ トエージェント (CAL) 1 ライ センス	2006.09.08
VERITAS Backup Exec 10.0 Windows リモ トエージェント (CAL) 1 ライ センス	2006.09.08
VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	2006.09.08
VERITAS Backup Exec 9.1 for Windows Servers revision4691	2006.09.08
VERITAS Backup Exec 9.1 for Windows Servers revision4691 SP1	2006.09.08
VERITAS Backup Exec 9.1 for Windows Servers revision4691	2006.09.08
VERITAS Backup Exec 9.1 Windows リモ トエージェント (CAL) 1ライセ ンス	2006.09.08
VERITAS Backup	



		07-00	Exec 9.1 Windows リモートエージェント (CAL) 1ライセンス	2006.09.08
	RT-1V25-K2WC20	07-01	VERITAS Backup Exec 9.1 Windows リモートエージェント (CAL) 3ライセンス	2006.09.08
		07-00	VERITAS Backup Exec 9.1 Windows リモートエージェント (CAL) 3ライセンス	2006.09.08

(注1) JP1/VERITAS Backup Exec 9.0 for Windows Serversは、フルサポートが終了しておりますので、最新バージョンにバージョンアップまたは下記の暫定回避策の実施をお願いいたします。

#### [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、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  
Symantec社（旧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.symantec.com/region/jp/avcenter/security/content/2006.08.11.html>

## [暫定回避方法]

この脆弱性に対して下記暫定回避策があります。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

リモート・アクセスを信頼できるシステムや認証されたシステムのみに制限します。

## 更新履歴：

- 2006.09.08 : JP1/VERITAS Backup Exec for Windows Servers の RPC インターフェース・ヒープ・オーバーフローによる脆弱性問題について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.