

# 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](#) > HS02-001

2003.07.07更新

## Sun Java Runtime Environmentにおける Bytecode Verifier の脆弱性に関するセキュリティ問題 及び Sun Java VMにおける HttpURLConnection の脆弱性に関するセキュリティ問題の説明

2002.04.03に米国Sun Microsystems, Inc. からJava Runtime Environment における Bytecode Verifier の脆弱性に関するセキュリティ問題 (Bulletin 218)及び, Java VMにおける HttpURLConnection の脆弱性に関するセキュリティ問題 (Bulletin 216)が公表されました。

Java Runtime EnvironmentのBytecode Verifierに脆弱性が確認された問題については, この脆弱性により, 信頼されていないアプレットを悪用することで, 高位者権限を取得することができてしまいます。

脆弱性を悪用することにより, サンドボックスと呼ぶJavaアプレットのアクセス範囲を制限する機構を回避することができるため, ユーザの計算機上でJava アプレットを悪用した不正な操作が可能となるおそれがあります。

Java Runtime Environmentに脆弱性が確認された問題については, この脆

[> 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](#)

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](#)

弱性により、ユーザがプロキシサーバを使用している環境で、悪質なJavaアプレットにより脆弱性を悪用された場合、プロキシサーバへのアクセス要求ならびに応答をモニタすることができてしまいます。

脆弱性を悪用することにより、インターネット接続にあたり、プロキシサーバを介した構成で使用している場合、悪質なJavaアプレットにより脆弱性を悪用することで、攻撃者が望む送信先などにユーザ情報を転送することが可能となるおそれがあります。

弊社ソフトウェア事業部より提供している製品について、本問題の影響がある製品を以下に示します。

■影響がある製品 (情報更新日：2002.06.07)

対策	製品名	適用OS	更新日
HS02-001-01	System Manager - Management Console Version 2.0 02-20以降	Windows	2002.06.07
	System Manager - Management Console Version 3.0 03-44-/A以前		

更新履歴：

- 2003.07.07：このセキュリティ情報ページをリニューアルしました。

- 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

**HITACHI**  
Inspire the Next

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](#)

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](#) > HS02-001-01

2003.07.07更新

HS02-001;

Sun Java Runtime Environmentにおける Bytecode Verifier の脆弱性に関するセキュリティ問題 及び Sun Java VMにおける HttpURLConnection の脆弱性に関するセキュリティ問題の説明

## System Manager - Management Console の対策

System ManagerのオプションPPであるSystem Manager - Management Consoleにおいて、JRE(Java 2 Runtime Environment)に関するセキュリティ上の問題があることが判明しました。本件は、System ManagerのWeb管理コンソールのために使用しているJREの問題です。コンソールサービスはWeb管理コンソールの機能を包含しておりますので、JREをアンインストールし、コンソールサービスを使用するようにお願いいたします。また、Web管理コンソールをご使用になる場合は、対策版03-50への入れ替えをお願いいたします。

### 1. JREの影響範囲

System Manager - Management Console製品に含まれるJREをインストールすると、JREの脆弱性に関する問題が発生します。

[> 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](#)

なお、System Manager - Management Consoleをインストールした  
 だけでは、JREはインストールされません。System Manager -  
 Management ConsoleのCD-ROMから手動でインストールした場合  
 にのみ、JREの脆弱性に関する問題が発生します。

## 2. 該当するJREを含むSystem Manager - Management Consoleのバージョン一覧

製品名	形名	対象バージョン
System Manager - Management Console Version 2.0	P-2418-3124	02-20 02-30
System Manager - Management Console Version 2.0 Upgrade	P-2418-312U	02-30-/A
System Manager - Management Console Version 3.0	P-2418-3134	03-00 03-00-/A 03-10 03-20 03-30
System Manager - Management Console Version 3.0 Upgrade	P-2418-313U	03-30-/A 03-31-/A 03-40 03-42 03-44-/A

## 3. 回避方法

System Manager - Management ConsoleのCD-ROMからインストールしたJREを、[アプリケーションの追加と削除] でアンインストールしてください。

この場合、System Manager - Management ConsoleのWeb管理コンソールを使用することができなくなりますので、コンソールサービスをご利用ください。コンソールサービスではWeb管理コンソールの機能を包含しております。

また、Web管理コンソールをご使用になる場合は、脆弱性の問題が

対策されたJREを含んでいるSystem Manager - Management Consoleのバージョン03-50(2002年5月発行済み)をご使用願います。

#### 4. 注意事項

System Manager - Management Console以外の製品がJREを使用している場合、JREをアンインストールすると他の製品に影響を与える可能性がありますので、JREのアンインストールには充分ご注意ください。この場合は、他の製品で動作確認済みの脆弱性の問題が対策されたJREを使用する必要があります。

#### 更新履歴：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

- 
- 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.