

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)

HITACHI
Inspire the Next

| 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

> GO

> 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 > HS03-008

> 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

 > お問い合わせ

- soft-security@itg.hitachi.co.jp

 > 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

2004.01.06更新

Verisign CAルート証明書 期限切れ問題の説明

(1)Javaに組み込まれているVerisign CAルート証明書 期限切れ問題の説明

対策	製品名	更新日
HS03-008-01	Cosminexus	2003.12.25
HS03-008-02	HP-UX, AIX 5L, Sun J2SE	2003.12.25

Sun Microsystems社からアナウンスがありました通

り、J2SE(Java™ 2 Platform、Standard Edition)にインストールされているVerisign社証明書のうち、Class2, 3の証明書が日本時刻で2004/1/8 8:59に失効します。このため、失効する証明書しかインストールしていないJ2SE環境を利用する場合、SSL接続できなくなる等の問題があります。

ただし、Internet Explorer、Netscape等のブラウザのSSL通信(https)は該当しません。

問題点の詳細は、Sun Microsystems社の以下のサイトを参照し

てください。

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57436-1>



(2)オラクル製品に組み込まれているVerisign CAルート証明書 期限切れ問題の説明

題の説明

対策	製品名	更新日
-	オラクル製品	2004.01.06

オラクル製品の一部コンポーネントにあらかじめ含まれているVerisignの認証局ルート証明書の一部が、日本時間2004年1月8日に有効期限を迎えます。

これに伴い、この証明書を使用してSSL通信を行っている場合、問題が起こる可能性があります。

詳細は[オラクル社サポートページ](#)を参照してください。

更新履歴：

- 2004.01.06 : オラクル製品の問題を追加しました。
- 2003.12.25 : 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](#)

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)

HITACHI
Inspire the Next

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

> GO

> 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 > HS03-008-01

> 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

2003.12.25更新

HS03-008;

Javaに組み込まれているVerisign CAルート証明書 期限切れ問題の説明

Cosminexusの対策

1. 影響範囲

Cosminexusに同梱しているJ2SEは、サーバサイドのプログラムを実行させます。

したがってVerisign社から「SSL Server Certificate」を入手し、SSL認証を行っている場合で、サーバ環境上で実行されるJavaアプリケーション(ServletやEJB)がSSL通信を利用していると、SSL通信ができなくなる可能性があります。

2. 対象製品と対策

Cosminexusが使用するJavaの提供元は、対応プラットフォーム及びバージョンによって異なっておりますので、プラットフォーム及びバージョン対応に対策を実行し、有効期間を延長した新しい証明書を組み込んでください。

形名	対象	製品名	適用OS	対策パッチ		更新日
					ダウンロー	

	バージョン		適用手順	ド		
P-2443-1C54	05-05	Embedded Cosminexus Server Version 5	HS03-008-01-a	cacerts.exe		
P-2443-1B54	05-00, 05-01, 05-05	Cosminexus Studio Version 5				
P-2443-1D54	05-00, 05-01, 05-05	Cosminexus Application Server Version 5				
P-2443-1F54	05-00, 05-01, 05-05	Cosminexus Developer Version 5				
P-24Z4-1A44	04-00, 04-01	Cosminexus Studio - Web Edition Version 4	Windows			
P-24Z4-1B44	04-00, 04-01	Cosminexus Studio - Standard Edition Version 4				
P-24Z4-1D44	04-00, 04-01	Cosminexus Server - Web Edition Version 4				
P-24Z4-1K44	04-00, 04-01	Cosminexus Server - Standard Edition Version 4				
P-24Z4-1A34	03-00, 03-01, 03-02, 03-05	Cosminexus Studio - Web Edition				
P-24Z4-1B34	03-00, 03-01, 03-02, 03-05	Cosminexus Studio - Standard Edition			HS03-008-01-b	cacerts.exe
P-24Z4-1C34	03-00, 03-01, 03-02, 03-05	Cosminexus Studio - Enterprise Edition				
P-	03-00, 03-	Cosminexus Server -				

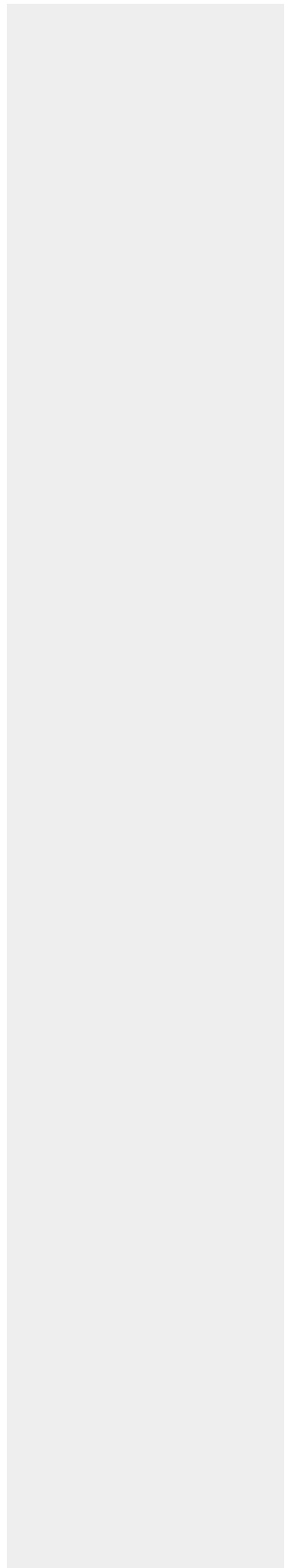


24Z4-1D34	01, 03-02, 03-05	Web Edition				
P-24Z4-1E44	03-00, 03-01, 03-02, 03-05	Cosminexus Server - Standard Edition				
P-24Z4-1F44	03-00, 03-01, 03-02, 03-05	Cosminexus Server - Enterprise Edition				
P-24Z4-1G34	03-00, 03-01, 03-02, 03-05	Cosminexus Management Server - Enterprise Edition				
P-1B43-1B51	05-02, 05-05	Cosminexus Application Server Version 5	HP-UX	HS03-008-01-a	cacerts.exe	
P-1B43-1B51	05-00	Cosminexus Application Server Version 5				
P-1BZ4-1S41	04-01	Cosminexus Server - Web Edition Version 4				
P-1BZ4-1T44	04-01	Cosminexus Server - Standard Edition Version 4				
P-1BZ4-1S31	03-00, 03-01, 03-02, 03-05	Cosminexus Server - Web Edition				
P-1BZ4-1T31	03-01, 03-02, 03-05	Cosminexus Server - Standard Edition				
P-1BZ4-1U31	03-01, 03-02, 03-05	Cosminexus Server - Enterprise Edition				
P-1BZ4-1V31	03-01, 03-02, 03-05	Cosminexus Management Server - Enterprise Edition				
P-		Cosminexus				

2003.12.25

HPのサイト(リンク切れ)

左記に含む



1M43-1B51	05-00, 05-05	Application Server Version 5	AIX	HS03-008-01-a	cacerts.exe
P-1MZ4-1E44	04-01	Cosminexus Server - Standard Edition Version 4		米国IBM のサイ トを参照	左記に含む
P-9DZ4-1D41	04-01	Cosminexus Server - Web Edition Version 4	Solaris	HS03-008-01-b	cacerts.exe
P-9DZ4-1E41	04-01	Cosminexus Server - Standard Edition Version 4			
P-9DZ4-1D31	03-00,03-01,03-02,03-05	Cosminexus Server - Web Edition			
P-9DZ4-1E31	03-01,03-02,03-05	Cosminexus Server - Standard Edition			
P-9DZ4-1F31	03-01,03-02,03-05	Cosminexus Server - Enterprise Edition			
P-9DZ4-1G31	03-01,03-02,03-05	Cosminexus Management Server - Enterprise Edition			
P-9S43-1B51	05-05	Cosminexus Application Server Version 5			

更新履歴：

- 2003.12.25 : Cosminexusの対策を公開しました。

- 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](#)

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)

HITACHI
Inspire the Next

| 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

> GO

> 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 > HS03-008-02

> 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

2003.12.25更新

HS03-008;

Javaに組み込まれているVerisign CAルート証明書 期限切れ問題の説明

HP-UX, AIX 5L, Sun J2SEの対策

1.影響範囲

使用されているJ2SEの使用目的によって、サーバサイドのプログラムの問題だけではなく、クライアント系の問題も発生いたします。発生する問題は各ベンダから提供される情報を参照してください。

2.HP-UX

【対象製品】

Java 2 Standard Edition for HP-UX 1.2.2.16とそれ以前

Java 2 Standard Edition for HP-UX 1.3.0.03とそれ以前(すべてのリリース)

Java 2 Standard Edition for HP-UX 1.3.1.11とそれ以前

Java 2 Standard Edition for HP-UX 1.4.0.05とそれ以前(すべてのリリース)

【対策】

以下のHPのサイトに記載されている方法により対策してください。

- VeriSign root certificate expiration notice

<http://www.hp.com/products1/unix/java/infolibrary/verisign.html>

- VeriSignルート証明書の有効期限について

<http://www1.jpn.hp.com/products/software/development/java/verisign.html> (リンク切れ)

- HP-UX搭載HP Java製品のルート証明書失効問題と対策方法のお知らせ

<http://www.hitachi.co.jp/Prod/comp/soft1/HP-UX/news/javacert.html> (リンク切れ)

H9000Vサポートサービスご契約のお客様は、お客様専用ホームページから2003年12月発行ニュース「製品情報」の「HP-UX搭載HP Java製品のルート証明書失効問題と対策方法のお知らせ」を参照し、対策をお願いします。

3.AIX 5L

【対象製品】

RT-11M11-130 AIX 5L V5.1 01-00以降

RT-11M11-230 AIX 5L V5.2 01-00以降

【対策】

以下の米国IBMのサイトに記載されている方法により対策してください。

<http://www-106.ibm.com/developerworks/java/jdk/security/>

EP8000サポートサービスご契約のお客さまは、お客さま専用ホームページ

「障害回避・予防のお願い」を参照し、対策をお願いします。

4.Sun J2SE

【対象製品】

- J2SE 1.4.2_02 以前のバージョン
- J2SE 1.4.1_05 以前のバージョン
- J2SE 1.4.0_04 以前のバージョン
- J2SE 1.3.1_09 以前のバージョン
- J2SE 1.3.0_05 以前のバージョン

・ J2SE 1.2.2_017 以前のバージョン

【対策】

以下のSunのサイトに記載されている方法により対策してください。

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57436-1>

また、日本語による対策手順の説明は、[HS03-008-02-a](#)を参照してください。

更新履歴：

- ・ 2003.12.25 : HP-UX, AIX 5L, Sun J2SEの対策を公開しました。

-
- ・ 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.