

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](#) > HS02-006

2003.07.07更新

SNMPに関するセキュリティ問題の説明

2002.02.12に米国CERT/CCからSNMPに関するセキュリティ問題 ([Advisory CA-2002-03](#))が公表されました。

これは、ネットワーク機器などの管理に広く利用されているプロトコル SNMP(Simple Network Management Protocol) のバージョン 1 の実装の多くに、SNMP パケットを適切に処理できない場合のあることが発見されたもので、ネットワーク機器のほか、Unix 系 OS や Windows, およびこれらの OS 上で動作する SNMP ソフトウェアで問題がある可能性があります。結果として、サービス運用妨害 (denial-of-service, DoS) 攻撃を受けたり、第三者がネットワーク機器の管理者権限を取得する恐れがあります。

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。なお、弊社開発 OS である HI-UX/WE2 の OS 本体には、SNMP デーモン(サービス)の機能が含まれていないため、本問題には該当いたしません。

[> 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](#)

■影響がある製品 (情報更新日：2002.09.04)



| 対策 | 製品名 | 適用OS | 更新日 |
|-------------|------------------------------------|--|------------|
| HS02-006-01 | JP1/Cm2/Network Node Manager | HP-UX, Solaris, Windows | 2002.09.04 |
| HS02-006-02 | JP1/Cm2/Extensible Agent | Windows | 2002.06.07 |
| HS02-006-03 | JP1/Cm2/Extensible SNMP Agent | HP-UX, Solaris, AIX, Linux, Tru64, HI-UX/WE2 | 2002.06.07 |
| HS02-006-04 | JP1/Cm2/SubManager | HP-UX, Solaris, AIX, HI-UX/WE2, Windows | 2002.05.29 |
| HS02-006-05 | JP1/Cm2/Hierarchical Agent | HP-UX, Solaris, Windows | 2002.05.10 |
| HS02-006-06 | Hitachi Directory Server Version 2 | HP-UX | 2002.04.10 |

- Solaris, HP-UX, Windows, Linux, AIX
- Oracle DataBase
- UnixWare 7 メディアキット(CALDERA)
- iPlanet Directory Server, iPlanet Web Proxy Server
- IntranetWare, NetWare

(上記製品については、対策パッチが提供されております。詳細はベンダ各社のWebサイトを参照下さい。なお、AIXについてはIBM社より問題がある旨の連絡がありましたので、影響がある製品として報告いたします。)

- SCO UnixWare2.1J PE, SCO UnixWare2.1J AS

(SCO UnixWareについては、御使用のお客様全てに、対応に関する連絡をさせていただいております。)

上記製品の対策パッチ適用が完了するまでは、お客様のシステムにおいて以下のいずれかの対策を実施いただくことを推奨いたします。

1. 不要な SNMP サービスを停止する。(SNMP でシステムの監視等を行っている場合は利用できなくなります。)
2. 許可していないホストからの SNMP アクセスを禁止する。
(例. UDPポート : 161,162を遮断する)
3. 各ベンダのWebサイトを参照し, 対策パッチが提供されている場合は適用する。

[ベンダ各社のWebサイト]

- [マイクロソフト](#)
- [Hewlett Packard](#)

[注意] HP-UXの対策パッチを適用する場合の注意事項は[こちら](#)を参照ください。

- [Sun Microsystems](#)
- [Red Hat Linux](#)
- [TurboLinux](#)
- [MiracleLinux](#)
- [International Business Machines, Corp.](#)
- [日本オラクル](#)
- [iPlanet\(Sun Microsystems\)](#)
- [ノベル株式会社](#)
- [CALDERA](#)

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

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 > HS02-006-01

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

JP1/Cm2/Network Node Manager の対策

JP1/Cm2/Network Node Managerにおいて、SNMP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。つきましては、該当する対策パッチを提供させていただきますので、入れ替えをお願いいたします。

[注意事項]

- 以下の対策パッチの適用に合わせ、各ベンダが本SNMP問題に関する対策パッチを提供している場合は、該当する対策パッチを適用する必要があります。各ベンダのホームページよりダウンロードしていただきますようお願い申し上げます。

なお、HP-UX以外は以下の対策パッチとの適用順序に制限はありません。(どちらを先に適用しても構いません)

HP-UXの場合、JP1/Cm2/Network Node Manager の対策パッチの適用手順にしたがってください。

- 06-71 以降のバージョンでは対策済みです。

> 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

| 形名 | 対象バージョン | 適用OS | 対策パッチ | | 吸収予定バージョン | 更新日 |
|-------------|----------|--------------|----------|------------------------|-----------|------------|
| | | | 適用手順 | ダウンロード | | |
| P-2442-6164 | 06-51~ | Windows 2000 | HS02-006 | P-2442-6164_0651SD.exe | 06-51 | 2002.04.25 |
| P-2442-6264 | 06-51-/A | Windows NT | -01-a | (1,213,416byte) | -/B | |
| P-1B42-6161 | 06-51 | HP-UX | HS02-006 | P-1B42-6161_0651SB.tar | 06-51 | 2002.05.29 |
| P-1B42-6261 | | | -01-b | (3,870,720byte) | -/A | |
| P-9D42-6161 | 06-51 | Solaris | HS02-006 | P-9D42-6161_0651SA.tar | 06-51 | 2002.05.29 |
| P-9D42-6261 | | | -01-c | (5,187,072byte) | -/A | |
| P-2442-6194 | 05-20~ | Windows NT | HS02-006 | P-2442-6194_0520SK.exe | 05-20 | 2002.09.04 |
| P-2442-6294 | 05-20-/F | | -01-d | (2,256,064byte) | -/G | |
| P-1B42-6111 | 05-20~ | HP-UX | HS02-006 | P-1B42-6111_0520SH.tar | 05-20 | 2002.09.04 |
| P-1B42-6211 | 05-20-/E | | -01-e | (5,519,360byte) | -/F | |
| P-9D42-6111 | 05-20~ | Solaris | HS02-006 | P-9D42-6111_0520SC.tar | 05-20 | 2002.09.04 |
| P-9D42-6211 | 05-20-/E | | -01-f | (4,632,064byte) | -/F | |

※本対策パッチには、前提となる関連パッチはありません。

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。
- 2002.09.04：バージョン 05-20 のセキュリティ問題対策パッチの提供を開始しました。

- 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

> 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 > HS02-006-02

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

JP1/Cm2/Extensible Agent の対策

JP1/Cm2/Extensible Agentにおいて、SNMP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。つきましては、該当する対策パッチを提供させていただきますので、入れ替えをお願いいたします。

[注意事項]

- 以下の対策パッチの適用に合わせ、マイクロソフト社が提供しております本 SNMP 問題に関する Windows の修正プログラムを適用する必要があります。マイクロソフト社のホームページよりダウンロードしていただきますようお願い申し上げます。
- なお、以下の対策パッチとの適用順序に制限はありません。(どちらを先に適用しても構いません)

・日本語版

| 形名 | 対象バー | 適用OS | 対策パッチ | | 更新日 |
|----|------|------|-------|--|-----|
| | | | 適用 | | |
| | | | | | |

> 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

| | ジョン | | 手順 | ダウンロード | |
|-------------|----------|--------------|----------|------------------------|------------|
| P-2442-6A64 | 06-50～ | Windows 2000 | HS02-006 | P-2442-6A64_0650SA.exe | 2002.04.25 |
| | 06-50-/A | Windows NT | -02-a | (28,296byte) | |
| P-2442-5A94 | 05-20～ | Windows 2000 | HS02-006 | P-2442-5A94_0520SA.exe | 2002.04.25 |
| | 05-20-/G | Windows NT | -02-b | (28,296byte) | |



・英語版

| 形名 | 対象バージョン | 適用OS | 対策パッチ | | 更新日 |
|-------------|---------|--------------|----------|------------------------|------------|
| | | | 適用手順 | ダウンロード | |
| P-2442-6A67 | 06-50 | Windows 2000 | HS02-006 | P-2442-6A67_0650SA.exe | 2002.06.07 |
| | | Windows NT | -02-c | (28,808byte) | |
| P-2442-5A97 | 05-20 | Windows NT | HS02-006 | P-2442-5A97_0520SA.exe | 2002.06.07 |
| | | | -02-d | (28,808byte) | |

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](#)

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](#) > HS02-006-03

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

JP1/Cm2/Extensible SNMP Agent の対策

JP1/Cm2/Extensible SNMP Agentにおいて、SNMP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。つきましては、該当する対策パッチを提供させていただきますので、入れ替えをお願いいたします。

[注意事項]

- 以下の対策パッチの適用に合わせ、各ベンダが本SNMP問題に関する対策パッチを提供している場合は、該当する対策パッチを適用する必要があります。各ベンダのホームページよりダウンロードしていただきますようお願い申し上げます。

なお、HP-UX以外は以下の対策パッチとの適用順序に制限はありません。(どちらを先に適用しても構いません)

HP-UXの対策パッチを適用する場合は[こちらの注意事項](#)を参照ください。

- 日本語版

[> 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](#)

| 形名 | 対象バージョン | 適用OS | 対策パッチ | | 更新日 |
|-------------|--------------------|-----------|-------------------|---|------------|
| | | | 適用手順 | ダウンロード | |
| P-1642-6A6 | 06-50 | HI-UX/WE2 | HS02-006 -03-a | P-1642-6A6_0650SA.tar (3,727,360byte) | 2002.03.15 |
| P-1B42-6A61 | 06-50 | HP-UX | HS02-006 -03-b | P-1B42-6A61_0650SA.tar (1,822,720byte) | 2002.03.15 |
| P-9142-6A61 | 06-50~ 06-50-/A | AIX | HS02-006 -03-c | P-9142-6A61_0650SA.tar (1,720,320byte) | 2002.03.15 |
| P-9D42-6A61 | 06-50 | Solaris | HS02-006 -03-d | P-9D42-6A61_0650SA.tar (1,239,040byte) | 2002.03.15 |
| P-9S42-6A61 | 06-50 | Linux | HS02-006 -03-e | P-9S42-6A61_0650SA.tar (1,413,120byte) | 2002.03.15 |
| P-9U42-6A61 | 06-50 | Tru64 | HS02-006 -03-f | P-9U42-6A61_0650SA.tar (1,525,760byte) | 2002.03.15 |
| P-1642-5A1 | 05-20~ 05-20-/B | HI-UX/WE2 | HS02-006 -03-g | P-1642-5A1_0520SA.tar (778,240byte) | 2002.05.29 |
| P-1B42-5A11 | 05-20~ 05-20-/C | HP-UX | HS02-006 -03-h | P-1B42-5A11_0520SA.tar (614,400byte) | 2002.05.29 |
| P-9142-5A11 | 05-20~ 05-20-/C | AIX | HS02-006 -03-i | P-9142-5A11_0520SA.tar (768,000byte) | 2002.05.29 |
| P-9D42-5A11 | 05-20~ 05-20-/D | Solaris | HS02-006 -03-j | P-9D42-5A11_0520SB.tar (2,088,960byte) | 2002.05.29 |
| P-9S42-5A11 | 05-20 | Linux | HS02-006 -03-k | P-9S42-5A11_0520SA.tar (512,000byte) | 2002.05.29 |

・英語版

| 形名 | 対象バージョン | 適用OS | 対策パッチ | | 更新日 |
|-------------|---------|-------|-------------------|---|------------|
| | | | 適用手順 | ダウンロード | |
| P-1B42-6A62 | 06-50 | HP-UX | HS02-006 -03-l | P-1B42-6A62_0650SA.tar (1,822,720byte) | 2002.06.07 |

| | | | | | |
|-------------|-------|---------|-------------------|---|------------|
| P-9142-6A62 | 06-50 | AIX | HS02-006 -03-m | P-9142-6A62_0650SA.tar (1,720,320byte) | 2002.06.07 |
| P-9D42-6A62 | 06-50 | Solaris | HS02-006 -03-n | P-9D42-6A62_0650SA.tar (1,239,040byte) | 2002.06.07 |
| P-9U42-6A62 | 06-50 | Tru64 | HS02-006 -03-o | P-9U42-6A62_0650SA.tar (1,525,760byte) | 2002.06.07 |
| P-1B42-5A12 | 05-20 | HP-UX | HS02-006 -03-p | P-1B42-5A12_0520SA.tar (614,400byte) | 2002.06.07 |
| P-9142-5A12 | 05-20 | AIX | HS02-006 -03-q | P-9142-5A12_0520SA.tar (768,000byte) | 2002.06.07 |
| P-9D42-5A12 | 05-20 | Solaris | HS02-006 -03-r | P-9D42-5A12_0520SA.tar (2,088,960byte) | 2002.06.07 |

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.

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

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 > HS02-006-04

> 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

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

JP1/Cm2/SubManager の対策

JP1/Cm2/SubManagerにおいて、SNMP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。つきましては、該当する対策パッチを提供させていただきますので、入れ替えをお願いいたします。

[注意事項]

- 以下の対策パッチの適用に合わせて、各ベンダが本SNMP問題に関する対策パッチを提供している場合は、該当する対策パッチを適用する必要があります。各ベンダのホームページよりダウンロードしていただきますようお願い申し上げます。

なお、HP-UX以外は以下の対策パッチとの適用順序に制限はありません。

(どちらを先に適用しても構いません)

HP-UXの対策パッチを適用する場合は[こちらの注意事項](#)を参照ください。

| 形名 | 対象バー | 適用OS | 対策パッチ | | 更新日 |
|----|------|------|-------|--|-----|
| | | | 適用 | | |
| | | | | | |

| | ジョン | | 手順 | ダウンロード | |
|-------------|-----------------------|----------------------------|----------|------------------------|------------|
| P-2442-6B64 | 06-51 | Windows 2000 Windows NT | HS02-006 | P-2442-6B64_0651SA.exe | 2002.04.19 |
| P-2442-6C64 | | | -04-a | (37,768byte) | |
| P-2442-6D64 | | | HS02-006 | P-2442-6B64_0651SB.exe | |
| P-1642-6B6 | 06-51 | HI-UX/WE2 | HS02-006 | P-1642-6B6_0651SA.tar | 2002.04.19 |
| P-1642-6C6 | | | -04-c | (3,727,360byte) | |
| | | | HS02-006 | P-1642-6B6_0651SB.tar | |
| P-1B42-6B61 | 06-51 | HP-UX | HS02-006 | P-1B42-6B61_0651SA.tar | 2002.04.19 |
| P-1B42-6C61 | | | -04-e | (1,822,720byte) | |
| P-1B42-6D61 | | | HS02-006 | P-1B42-6B61_0651SB.tar | |
| P-1B42-6E61 | | | -04-f | (624,640byte) | |
| P-9142-6B61 | 06-51 | AIX | HS02-006 | P-9142-6B61_0651SA.tar | 2002.04.19 |
| P-9142-6C61 | | | -04-g | (1,720,320byte) | |
| | | | HS02-006 | P-9142-6B61_0651SB.tar | |
| P-9D42-6B61 | 06-51 | Solaris | HS02-006 | P-9D42-6B61_0651SA.tar | 2002.04.19 |
| P-9D42-6C61 | | | -04-i | (1,239,040byte) | |
| P-9D42-6D61 | | | HS02-006 | P-9D42-6B61_0651SB.tar | |
| P-9D42-6E61 | | | -04-j | (747,520byte) | |
| P-2442-5B94 | 05-20-/A~ 05-20-/B | Windows NT | HS02-006 | P-2442-5B94_0520SA.exe | 2002.05.10 |
| P-2442-5C94 | | | -04-k | (37,768byte) | |
| P-2442-5D94 | | | HS02-006 | P-2442-5B94_0520SB.exe | |
| P-1642-5B1 | 05-20-/A | HI-UX/WE2 | HS02-006 | P-1642-5B1_0520SA.tar | 2002.05.29 |
| P-1642-5C1 | | | -04-m | (778,240byte) | |
| | | | HS02-006 | P-1642-5B1_0520SB.tar | |
| P-1B42-5B11 | 05-20-/A | HP-UX | HS02-006 | P-1B42-5B11_0520SA.tar | 2002.05.29 |
| P-1B42-5C11 | | | -04-o | (614,400byte) | |
| P-1B42-5D11 | | | HS02-006 | P-1B42-5B11_0520SB.tar | |
| P-1B42-5E11 | | | -04-p | (706,560byte) | |
| P-9142-5B11 | | | HS02-006 | P-9142-5B11_0520SA.tar | |



| | | | | | |
|-------------|-----------------------|---------|-------------------|---|------------|
| P-9142-5C11 | 05-20-/A | AIX | -04-q HS02-006 | (768,000byte) P-9142-5B11_0520SB.tar | 2002.05.29 |
| | | | -04-r | (1,024,000byte) | |
| P-9D42-5B11 | 05-20-/A~ 05-20-/B | Solaris | HS02-006 | P-9D42-5B11_0520SA.tar | 2002.05.29 |
| P-9D42-5C11 | | | -04-s | (2,088,960byte) | |
| P-9D42-5D11 | | | HS02-006 | P-9D42-5B11_0520SB.tar | |
| P-9D42-5E11 | | | -04-t | (716,800byte) | |

※対策パッチは、両方とも適用してください。

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.

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

> 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 > HS02-006-05

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

JP1/Cm2/Hierarchical Agent の対策

JP1/Cm2/Hierarchical Agentにおいて、SNMP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。つきましては、該当する対策パッチを提供させていただきますので、入れ替えをお願いいたします。

[注意事項]

- 以下の対策パッチの適用に合わせ、各ベンダが本SNMP問題に関する対策パッチを提供している場合は、該当する対策パッチを適用する必要があります。各ベンダのホームページよりダウンロードしていただきますようお願い申し上げます。

なお、以下の対策パッチとの適用順序に制限はありません。(どちらを先に適用しても構いません)

| 形名 | 対象バージョン | 適用OS | 対策パッチ | | 更新日 |
|----|---------|------|-------|--------|-----|
| | | | 適用手順 | ダウンロード | |
| | | | | | |

- > 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

| | | | | | |
|-------------|--------------------|----------------------------|-------------------|---|------------|
| P-2442-6Y64 | 06-51~ 06-51-/A | Windows 2000 Windows NT | HS02-006 -05-a | P-2442-6Y64_0651SA.exe (51,440byte) | 2002.04.05 |
| P-1B42-6Y61 | 06-51 | HP-UX | HS02-006 -05-b | P-1B42-6Y61_0651SA.tar (92,160byte) | 2002.04.12 |
| P-9D42-6Y61 | 06-51 | Solaris | HS02-006 -05-c | P-9D42-6Y61_0651SA.tar (337,920byte) | 2002.04.12 |
| P-2442-6Y94 | 05-21 | Windows NT | HS02-006 -05-d | P-2442-6Y94_0521SA.exe (49,464byte) | 2002.05.10 |
| P-1B42-6Y11 | 05-21 | HP-UX | HS02-006 -05-e | P-1B42-6Y11_0521SA.tar (81,920byte) | 2002.05.10 |
| P-9D42-6Y11 | 05-21 | Solaris | HS02-006 -05-f | P-9D42-6Y11_0521SA.tar (296,960byte) | 2002.05.10 |

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.

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

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 > HS02-006-06

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

Hitachi Directory Server Version 2 (HP-UX版) のSNMP

エージェントに含まれる問題について

Hitachi Directory Server Version 2のHP-UX版が、2002.02.12に米国CERT/CCで公表されたSNMPに関するセキュリティ問題(Advisory CA-2002-03)に該当することがわかりました。

(Hitachi Directory Server Version 2は、ディレクトリサーバへの操作の統計情報を収集するSNMPエージェントを含みます。)

ただし、Hitachi Directory Server Version 2のAdministration Serverで、SNMP関係の設定をしていない場合は、SNMPエージェントは起動されていませんので、この問題には該当しません。

またWindows版の場合はOSのSNMPマスタエージェントを利用しますので、本製品はこの問題に該当しません。SNMPを利用する設定になっている場合には、[マイクロソフト](#)の修正プログラムを適用してください。

HP-UX版 Hitachi Directory Server Version 2のSNMPマスタエージェントは、

HITACHI
Inspire the Next

日立サイトの検索 by Google

> GO

> 詳細な検索

> 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。

> 日立および他社の商品名称に関する記述

"/opt/hitachi/DirectoryServerV2/plugins/snmp/magt/magt"です。

ps コマンドで Hitachi Directory Server Version 2のSNMPマスターエージェントの存在を調べてください。

入力例

```
ps -ef | grep magt
```

出力例

```
root 13622 13600 0 22:13:03 pts/tb 0:00 grep magt
root 5938 1 0 Apr 5 ? 1:04 /opt/hitachi/
DirectoryServerV2/
plugins/snmp/magt/magt
/
```

Hitachi Directory Server Version 2のSNMPエージェントを起動し運用されている場合は、以下のいずれかで対処いただくようお願いいたします。

1. SNMPアクセスは、許可したホストからのアクセスを除いて禁止してください。
2. 外部ネットワークの第三者からSNMPアクセスを受ける可能性があるシステムにおいて、Hitachi Directory Server Version 2のSNMPマスターエージェントを起動している場合は、以下手順で停止してください。

停止方法

```
kill -TERM <magtのPID>
```

[補足]

- Hitachi Directory Server Version 2には、自動起動スクリプトにSNMPマスターエージェントを登録する処理はありません。
- 自動起動スクリプトに
"/opt/hitachi/DirectoryServerV2/plugins/snmp/magt/magt"
を登録している場合は、当該登録を削除いただきますようお願いいたします。



SNMPによる収集情報に替わる、Hitachi Directory Serverの稼動情報について

Hitachi Directory Server Version 2では、製品に含まれている

Administration Serverで、ディレクトリサーバのキャッシュ利用状況、コネクション接続数などの稼動情報を参照できます。

本問題への対処としてSNMPマスタエージェントを停止した場合、SNMPマネージャ製品からの監視ができなくなってしまうますが、Administration Serverからの稼動情報参照で代替頂きますよう、ご検討をお願いいたします。

- Hitachi Directory Server Version 2の稼動情報参照手順

Administration ServerのTOP画面から、稼動状態を参照したいサーバインスタンスを選択しボタンを押します。このとき、サーバインスタンスが停止している場合は、起動してください。

Hitachi Directory Server の稼動情報は、画面上部に表示されるボタンのうち Server Status ボタンを押すと参照できます。左のフレームから以下のリンクを選択して参照してください。

- ディレクトリサーバの状態監視画面
- データベース状態監視画面

- HP-UXでのAdministration Serverの起動方法

1. /opt/hitachi/DirectoryServerV2/start-adminコマンドをスーパーユーザで実行します。

Administration Serverのプロセスが開始されます。

2. ブラウザから、`http://<サーバホスト名>:<ポート番号>`を指定します。

ユーザ名とパスワードの入力を促すダイアログが表示されます。

3. 管理者のユーザIDとパスワードを指定します。 Administration

Serverが起動します。

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。

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](#) > HS02-006-hpux_attention

2003.07.07更新

HS02-006;

SNMPに関するセキュリティ問題の説明

HP-UXのSNMP対策パッチを適用する場合の注意事項

JP1/Cm2 製品のインストール環境へ、HP-UX の本 SNMP の対策パッチをはじめとする、OV EMANATE Agent へのパッチを適用する場合、HP-UX提供のSNMPとJP1/Cm2提供のSNMPが異なるため、適用の順序などに制約があります。以下のJP1/Cm2製品が該当します。具体的な適用の順序などは、製品毎に異なります。

- JP1/Cm2/Extensible SNMP Agent(以降 JP1/Cm2/ESA)
- JP1/Cm2/SubManager
- JP1/Cm2/Network Node Manager (以降 JP1/Cm2/NNM)

1. JP1/Cm2/Extensible SNMP Agentの場合

JP1/Cm2/ESAのアンインストール後にHP-UXのSNMP対策パッチを適用し、その後にJP1/Cm2/ESAを再インストールする（定義情報はそのまま引き継がれます）。

[> 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](#)

[注意事項]

JP1/Cm2/ESAがインストールされている間は、JP1/Cm2/ESA提供のSNMPが優先され、HP-UXが提供しているSNMPは起動しません。

ただし、JP1/Cm2/ESAをアンインストールすると、HP-UXが提供しているSNMPが起動するようになります。

JP1/Cm2/ESAを使用する場合は、JP1/Cm2/ESAを再インストール後にJP1/Cm2/ESAのSNMPに関するセキュリティ問題対策パッチを必ず適用してください。対策パッチを提供していないバージョンのJP1/Cm2/ESAをご使用の場合は、許可していないホストからのSNMP アクセスを禁止する等の対策を行ってください。

2. JP1/Cm2/SubManagerの場合

次の(a)か(b)のいずれか一方の方法を適用します。

(a) HP-UXのSNMP対策パッチを直ちには適用しない方法

- JP1/Cm2/SubManagerのSNMPに関するセキュリティ問題対策パッチを適用します。

対策パッチを提供していないバージョンの

JP1/Cm2/SubManagerをご使用の場合は、許可していないホストからのSNMP アクセスを禁止する等の対策を行ってください。

この時点では、HP-UXのSNMP対策パッチは適用しません。

- その後、JP1/Cm2/SubManagerの使用を中止してJP1/Cm2/SubManagerのアンインストールを行った後、HP-UXはそのまま使用し続ける時に、HP-UXのSNMP対策パッチを適用します。

この時、JP1/Cm2/SubManagerをアンインストールした後にHP-UXのSNMP対策パッチを適用します。

(b) HP-UXのSNMP対策パッチを直ちに適用する方法

- JP1/Cm2/SubManagerをアンインストール後にHP-UXのSNMP対策パッチを適用します。
その後、JP1/Cm2/SubManagerを再インストールします。ただし、JP1/Cm2/SubManagerの定義情報やデータベースなどは削除されるため、はじめから構築をやり直す必要があります。
- JP1/Cm2/SubManagerを再インストールした後は、必ずJP1/Cm2/SubManagerのSNMPに関するセキュリティ問題対策パッチを適用します。
対策パッチを提供していないバージョンのJP1/Cm2/SubManagerをご使用の場合は、許可していないホストからのSNMPアクセスを禁止する等の対策を行ってください。

[注意事項]

JP1/Cm2/SubManagerの場合、HP-UXのSNMP対策パッチを適用するにはJP1/Cm2/SubManagerをいったん削除してからパッチを適用する必要がありますが、この場合、JP1/Cm2/SubManagerの定義情報やデータベースなども削除され、はじめから構築をやり直す必要があります。このことが問題となる場合は、上記(a)の方法を適用してください。問題とならない場合には、上記(b)の方法を適用することをお奨めします。

なお、JP1/Cm2/SubManagerがインストールされている間は、JP1/Cm2/SubManager提供のSNMPが優先され、HP-UXが提供しているSNMPは起動しません。

ただし、JP1/Cm2/SubManagerをアンインストールすると、HP-UXが提供しているSNMPが起動するようになります。

3. JP1/Cm2/Network Node Managerの場合

JP1/Cm2/Network Node Managerの対策パッチの適用手順にした

がってください。

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。

