Cisco IOS Software Internet Key Exchange Vulnerability

Advisory ID: cisco-sa-20130327-ike

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ike/

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

Revision 1.1

Last Updated 2013 April 11 15:30 UTC (GMT)

For Public Release 2013 March 27 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアのインターネット キー エクスチェンジ（IKE）機能には、サービス拒否（DoS）を引き起こす可能性のある脆弱性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策がありません。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ike/

注：2013 年 3 月 27 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には、7 件のセキュリティ アドバイザリが含まれています。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ アドバイザリには、そのアドバイザリで詳述された脆弱性を修正する Cisco IOS ソフトウェア リリー

ス、および 2013 年 3 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェア リリースを記載しています。

個別の公開リンクは、次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

該当製品

IKE バージョン 2 (IKEv2) をサポートしておらず、IKE バージョン 1 (IKEv1) を使用するように設定されている Cisco IOS ソフトウェアの該当バージョンのソフトウェア イメージを稼働している場合、その Cisco IOS デバイスには脆弱性が存在します。

脆弱性が認められる製品

デバイスで Cisco IOS ソフトウェアの該当バージョンが稼働しているかどうかの確認

この脆弱性の影響を受けるのは、Cisco IOS ソフトウェアの 15.1GC、15.1T、15.1XB リリース トレインです。他の Cisco IOS ソフトウェア リリース トレインは、この脆弱性の影響を受けません。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、**show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Cisco IOS ソフトウェア バージョンが IKEv2 をサポートしているかどうかの確認

Cisco IOS ソフトウェアの バージョン 15.1(1)T で、一部プラットフォーム向けに IKEv2 のサポートを導入しました。IKEv2 をサポートするイメージがデバイスにあるかどうかを確認するには、デバイスにログインしてコマンドライン インターフェイス（CLI）から **show subsys | include ikev2** コマンドを実行します。出力に *ikev2 Library* が含まれる場合、このデバイスは IKEv2 をサポートしています。出力に *ikev2 Library* が含まれていない場合、このデバイスは IKEv2 をサポートしていません。次の例ではデバイスは IKEv2 をサポートしています。

```
ISR2900#show subsys | include ikev2
ikev2                Library     1.000.001
ikev2_cli_registry Registry 1.000.001
ISR2900#
```

次の例ではデバイスは IKEv2 をサポートしていません。

```
ISR2900#show subsys | include ikev2
ikev2                Library     1.000.001
ikev2_cli_registry Registry 1.000.001
ISR2900#
```

デバイスで IKEv1 が設定されているかどうかの確認

IKEv1 はいくつかの機能で使用しています。その中には、次のようなさまざまなバーチャル プライベート ネットワーク（VPN）が挙げられます。

- LAN-to-LAN VPN
- リモート アクセス VPN（SSL VPN は含まず）
- Dynamic Multipoint VPN（DMVPN）
- Group Domain of Interpretation（GDoI）

デバイスに IKEv1 が設定されているかどうかは、次の 2 つの方法で確認できます。

- 実行中のデバイスで IKE ポートが開いているか確認する
- デバイスの設定に IKEv1 機能が含まれているか確認する

実行中のデバイスで IKE ポートが開いているか確認する

デバイスに IKE が設定されているかどうかを確認する推奨方法は、 **show udp** CLI コマンドを実行することです。デバイスの UDP ポート 500、UDP ポート 4500、UDP ポート 848、UDP ポート 4848 が開いている場合、デバイスは IKE パケットを処理しています。

次の例では、IPv4 または IPv6 のいずれかを使用して、デバイスはUDP ポート 500 および UDP ポート 4500 で IKE パケットを処理するように設定されています。

```
ISR2900#show subsys | include ikev2
ikev2                Library     1.000.001
ikev2_cli_registry Registry 1.000.001
ISR2900#
```

デバイスの設定に IKEv1 機能が含まれているか確認する

Cisco IOS のデバイス設定に脆弱性があるかどうかを確認するには、管理者は IKE を利用する機能が少なくとも 1 つ以上あるかを確認する必要があります。これは、 **show run | include crypto map|tunnel protection ipsec|crypto gdoi** イネーブル モード コマンドを使用して確認できます。このコマンドの出力に、 *tunnel protection ipsec* または *crypto gdoi* のいずれかが含まれる場合、そのデバイスには IKE の設定が含まれます。このコマンドの出力に、 *crypto map* が含まれる場合、 *ipsec-isakmp* として暗号マップが設定されているかを確認します。次の例では、IKE が設定されたデバイスを示します。

```
router# show run | include crypto map|tunnel protection ipsec|crypto gdoi
crypto map CM 100 ipsec-isakmp
 crypto map CM
router#
```

脆弱性が認められない製品

IKEv2 をサポートする該当バージョンの Cisco IOS ソフトウェアが稼働しているシスコ デバイスは、IKEv1 が設定されているかに関わらず、影響を受けません。

次の製品は IKEv1 と IKEv2 両方をサポートしており、この脆弱性の影響を受けないことが確認されています。

- Cisco ASR 5000 シリーズ Small Cell Gateway
- Cisco Access Service Network（ASN）Gateway
- Cisco ePDG（ASR5000 で稼働）
- SAMI ベースの Wireless Security Gateway（WSG）
- Cisco NX-OS ソフトウェア
- Cisco ASA ソフトウェア
- Cisco AnyConnect
- Cisco CGR 1000 ルータ

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Cisco IOS ソフトウェアには、認証されていないリモートの攻撃者が DoS 状態を発生させる可能性のある脆弱性が含まれています。

この脆弱性は、該当するソフトウェアによる IKE パケットに対する検証が不適切であることに起因します。攻撃者は、IKEv1 を利用する機能が設定されたデバイスに特定の IKE パケットを送信することで、この脆弱性を不正利用できる可能性があります。不正利用が成功した場合、攻撃者はサービス拒否（DoS）状態につながるメモリ リークを引き起こす可能性があります。
この脆弱性によってデバイスが不正利用されていないかどうかを識別するには、古いバッファの内容を確認します。この脆弱性による影響を受けたデバイスは、 **Crypto IKE Dis user** でバッファ リークを示し、かつ **Crypto IK** でのバッファ リークが発生中であることを示します。次の例は、この脆弱性によってメモリ リークが発生しているシステムを示しています。

```
Router#show buffer leak

Header DataArea Pool Size Link Enc Flags Input Output User

49AB48C0 3F405384 Small 0 0 0 0 None None Init
49ABB8DC 3F4072C4 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABBD58 3F407604 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABC1D4 3F407944 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABC650 3F407C84 Middl 419 7 1 80 Gi0/0 None Crypto IK


Router#show buffer leak resource user
Resource User: Init count: 21
Resource User: Crypto IKE Dis count:      100
Resource User: EEM ED Syslog count: 10
Resource User: IP ARP Adjacen count: 1
```

ネットワークが現在不正利用されている場合、 **Crypto IKE Dis** のカウントが増加します。この脆弱性は、IPv4 または IPv6 のどちらによっても不正利用される可能性があります。この脆弱性を引き起こすのは、デバイス宛てのトラフィックだけです。デバイスを通過するトラフィックは無

関係です。

この脆弱性は、Cisco Bug ID CSCth81055（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-1144 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

<table>
<tr><th colspan="6">CSCth81055 - Cisco IOS Software Internet Key Exchange Vulnerability
Calculate the environmental score of</th></tr>
<tr><td colspan="6">CVSS Base Score - 7.8</td></tr>
<tr><td>Access Vector</td><td>Access Complexity</td><td>Authentication</td><td>Confidentiality Impact</td><td>Integrity Impact</td><td>Availability Impact</td></tr>
<tr><td>Network</td><td>Low</td><td>None</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="6">CVSS Temporal Score - 6.4</td></tr>
<tr><td colspan="2">Exploitability</td><td colspan="2">Remediation Level</td><td colspan="2">Report Confidence</td></tr>
<tr><td colspan="2">Functional</td><td colspan="2">Official-Fix</td><td colspan="2">Confirmed</td></tr>
</table>

影響

この脆弱性の不正利用が成功した場合、サービス拒否（DoS）状態につながるメモリ リークを引き起こす可能性があります。メモリが使い果たされると、Cisco IOS デバイスはリロードを行うか応答不能になります。この状態から回復するには、電源をオフ/オンする必要があります。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the March 2013 Bundled Publication」列は、Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載されたすべての脆弱性を修正する最初のリリースを示します。可能な限り、最新のリリースにアップグレードすることを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication
There are no affected 15.0 based releases		
Affected 15.1-Based	First Fixed Release	Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication

Releases		
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	15.1(4)GC	15.1(4)GC1
15.1M	Not vulnerable	15.1(4)M6
15.1MR	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1MRA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	* See footnote Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1SVA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1SVC	Not vulnerable	Not vulnerable
15.1SY	Not vulnerable	15.1(1)SY1; Available on 24-MAY-13
15.1T	15.1(3)T	Vulnerable; First fixed in Release 15.1M
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based Releases	**First Fixed Release**	**Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication**
There are no affected 15.2 based releases		
Affected 15.3-Based Releases	**First Fixed Release**	**Bundle First Fixed Release for All Advisories in th March 2013 Bundled Publication**
There are no affected 15.3 based releases		

* Cisco 7600 シリーズのルータ用の最初の修正リリースは Cisco IOS ソフトウェア リリース 15.1(3)S5 で、2013 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載されます。Cisco 7200 および 7300 シリーズのルータ用の最初の修正リリースは Cisco IOS ソフトウェア リリース 15.1(3)S5a で、2013 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開に記載され 2013 年 4 月 15 日に公開を予定しています。

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、このアドバイザリで説明されている脆弱性の影響は受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、このアドバイザリで説明されている脆弱性の影響は受けません。

回避策

次の方法で、この脆弱性を識別できます。

Cisco IOS Embedded Event Manager（EEM）

脆弱性のある Cisco IOS デバイス上で、ツール コマンド言語（TCL）に基づく Cisco IOS Embedded Event Manager（EEM）ポリシーを利用すると、この脆弱性によって引き起こされたメモリ リークを識別して、検出することができます。このポリシーによって、管理者は影響を受けた処理がないか Cisco IOS デバイス上のメモリを監視することができます。Cisco IOS EEM がこの脆弱性による不正利用の可能性を検出すると、それに反応してポリシーがネットワーク管理者にアラートを送信し、それを受けて管理者は適宜、失われたメモリを復旧するためにデバイスのアップグレードまたはリロードを行うことを判断できます。例となるポリシーは、メモリのリークが継続し、EEM_IKE_BUFF_INCR_THRES に達したとき、かつ IKE バッファが EEM_IKE_BUFF_INCR_THRES 回リークしたときに syslog を送信する TCL スクリプトをベースとしています。IKE バッファが解放されると、カウンタはゼロからカウントを開始します。メモリ リーク syslog の生成後、スクリプトは再度初期化されます。TCL スクリプトは次のリンクの「Cisco Beyond: Embedded Event Manager（EEM）Scripting Community」からダウンロードできます。 https://supportforums.cisco.com/docs/DOC-30300/ 次にデバイスの設定例を示します。

```
Router#show buffer leak

Header DataArea Pool Size Link Enc Flags Input Output User

49AB48C0 3F405384 Small 0 0 0 0 None None Init
49ABB8DC 3F4072C4 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABBD58 3F407604 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABC1D4 3F407944 Middl 419 7 1 80 Gi0/0 None Crypto IK
49ABC650 3F407C84 Middl 419 7 1 80 Gi0/0 None Crypto IK


Router#show buffer leak resource user
Resource User: Init count: 21
Resource User: Crypto IKE Dis count:      100
Resource User: EEM ED Syslog count: 10
Resource User: IP ARP Adjacen count: 1
```

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

この脆弱性は内部脆弱性テストの一環で発見されました。

この通知のステータス：Final

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証を示唆するものでもありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有しま

す。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ike/

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.1	2013-April-11	Changed bundle first fix release data for 15.1SG.
Revision 1.0	2013-March-27	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。