CallManager 認証満了および削除

目次

概要

この資料は **CertExpiryEmergency を**受け取るところ Cisco Unified CallManager （ CM ）における問題を記述したものです: 実時間監視 ツール（ RTMT ）クライアントからの**認証終止** EMERGENCY_ALARM アラーム メッセージは問題に、ソリューションを提供し。

前提条件

要件

Cisco は 9.x によって CM バージョン 6.x の知識があること、そして推奨しますシステムことを:

- Domain Name System （ DNS ） 設定を持っていません。 これは資料の簡単にするためにされますが、多くのシステムに設定される良いそれがあります。
- 期限切れ、再生する必要があるまたは切れることになっている認証を持っています認証。

  注: システムの IP アドレスはホスト名か IP アドレスを変更した後**生成する新しいですか再生**コマンドを入力する場合重要ではありません。

使用するコンポーネント

この文書に記載されている情報は管理 ページとの Cisco CM サーバに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

問題

CertExpiryEmergency を受け取ります: CM の RTMT からの**認証終止 EMERGENCY_ALARM** アラーム メッセージ:

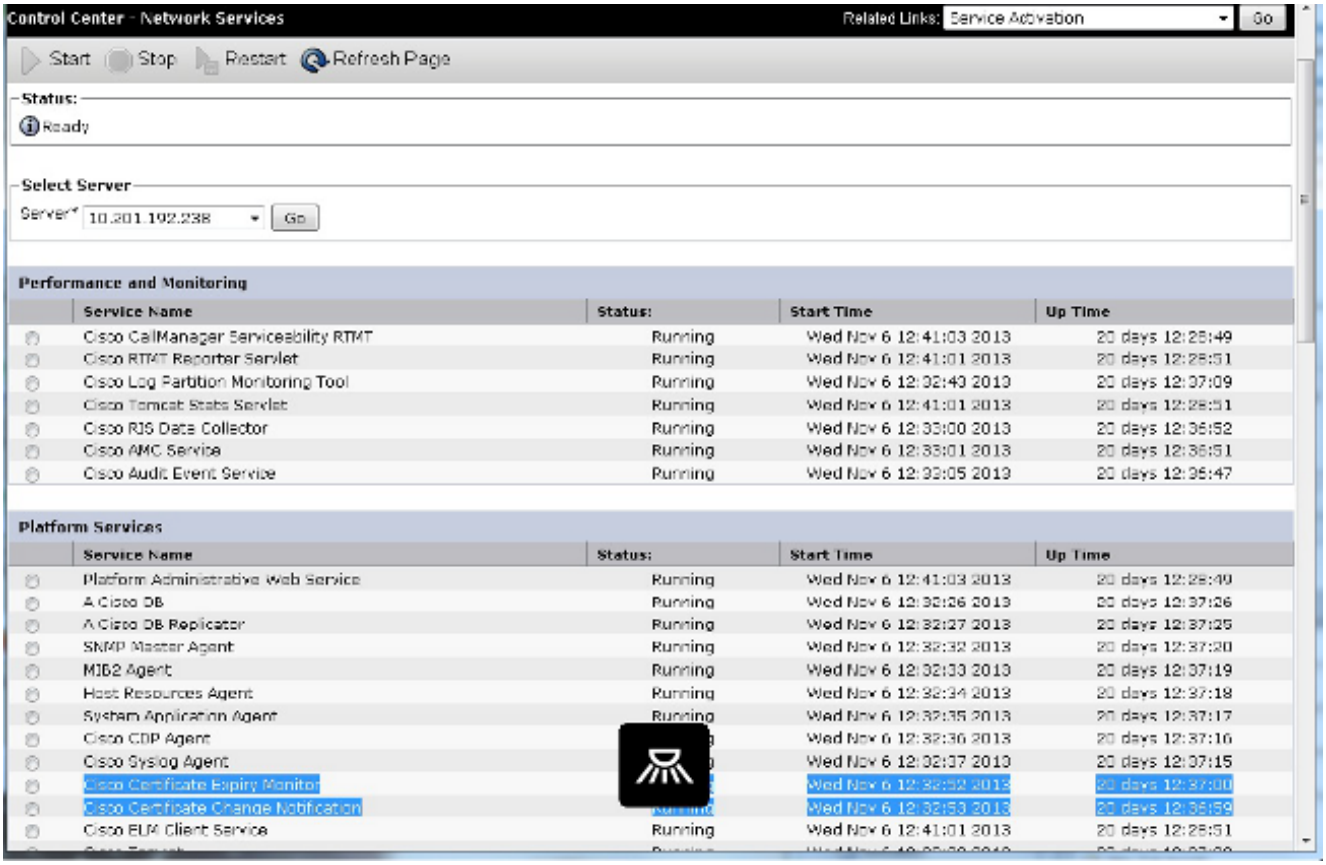
```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor Cluster ID:Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 630: Jul 30 17:00:00.353 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CallManager-trust Type:trust-cert Expiration:Fri Dec 28 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 631: Jul 30 17:00:00.354 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CAPF-trust Type:trust-cert Expiration:Fri Dec 28 12:14:4 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI
```

解決策

CM アラーム メッセージ問題を解決するためにこのセクションで情報を使用して下さい。

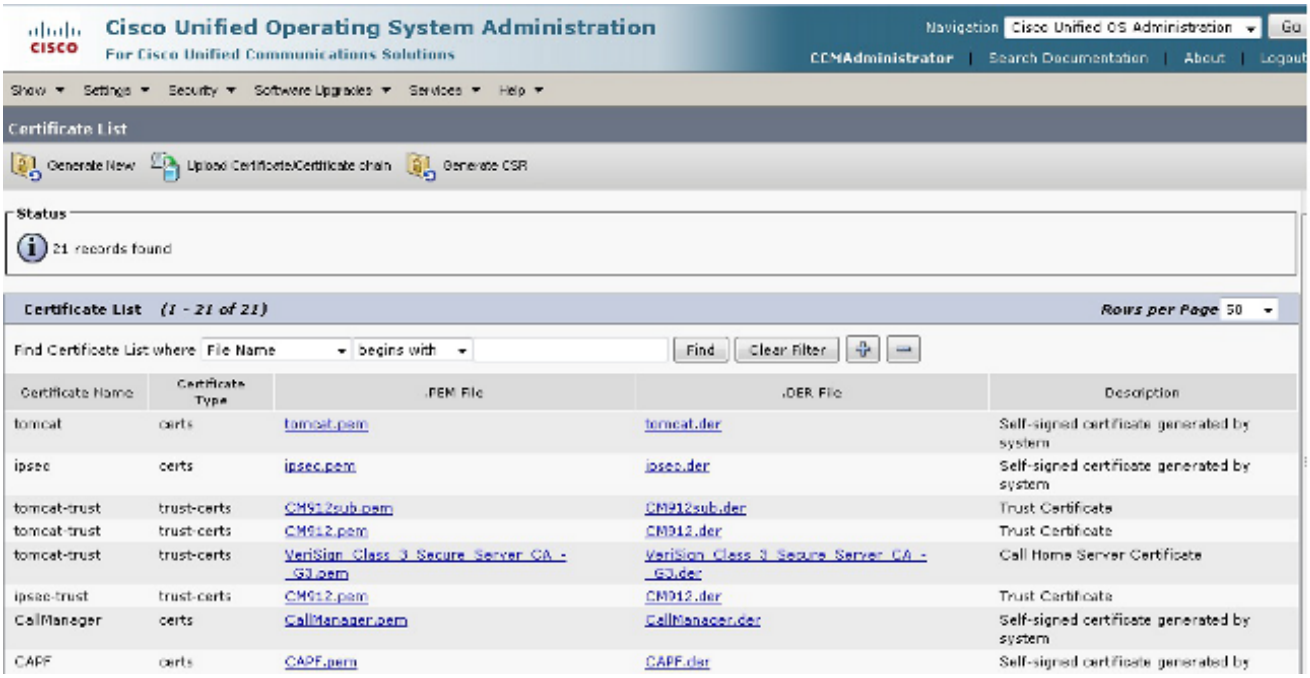
1. CM から統一されたサービサビリティ ページ GUI は **Tools > Control Center** に、**-ネットワークサービス** ナビゲート します。

2. クラスタのサーバすべての **Cisco 認証終止モニタ**および **Cisco 認証 変更通知** サービスを停止して下さい:



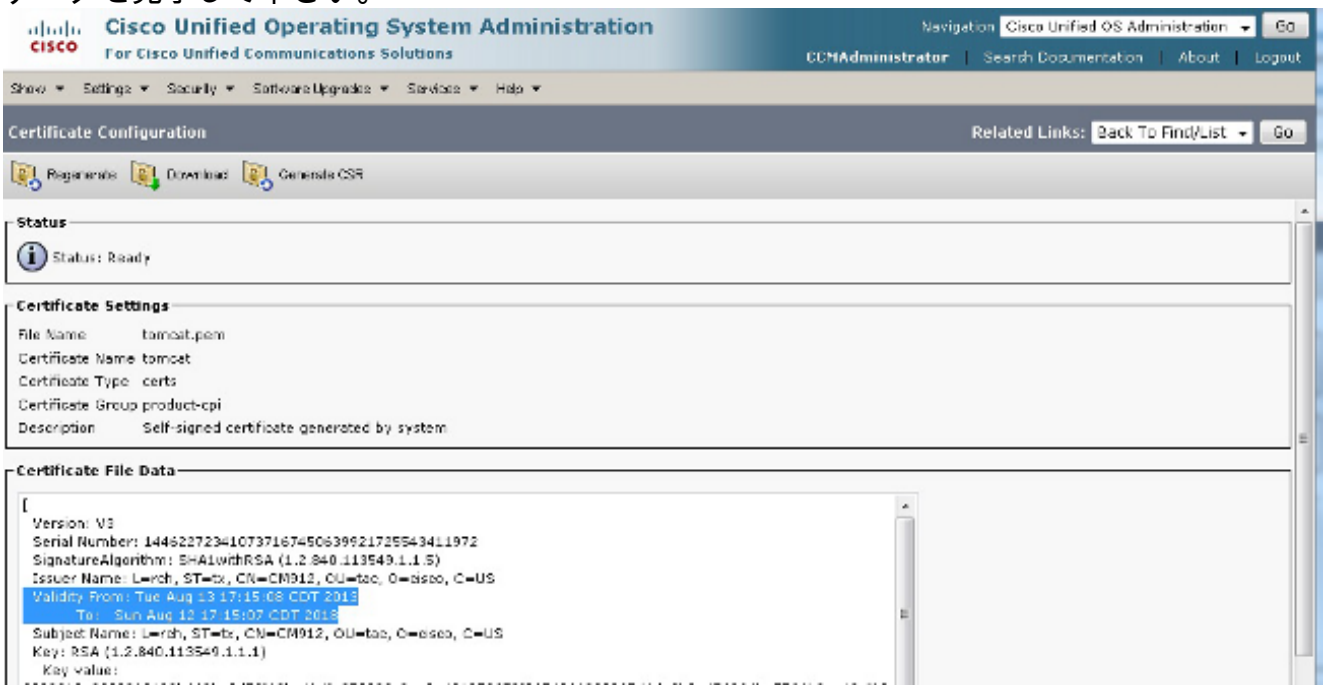
3. Operating System （ OS ） 管理 GUI から、この画面 表示は**セキュリティ > Certificate Management** にナビゲート し:

4. 特定のサーバの認証すべてを表示するために『Find』 をクリック して下さい:

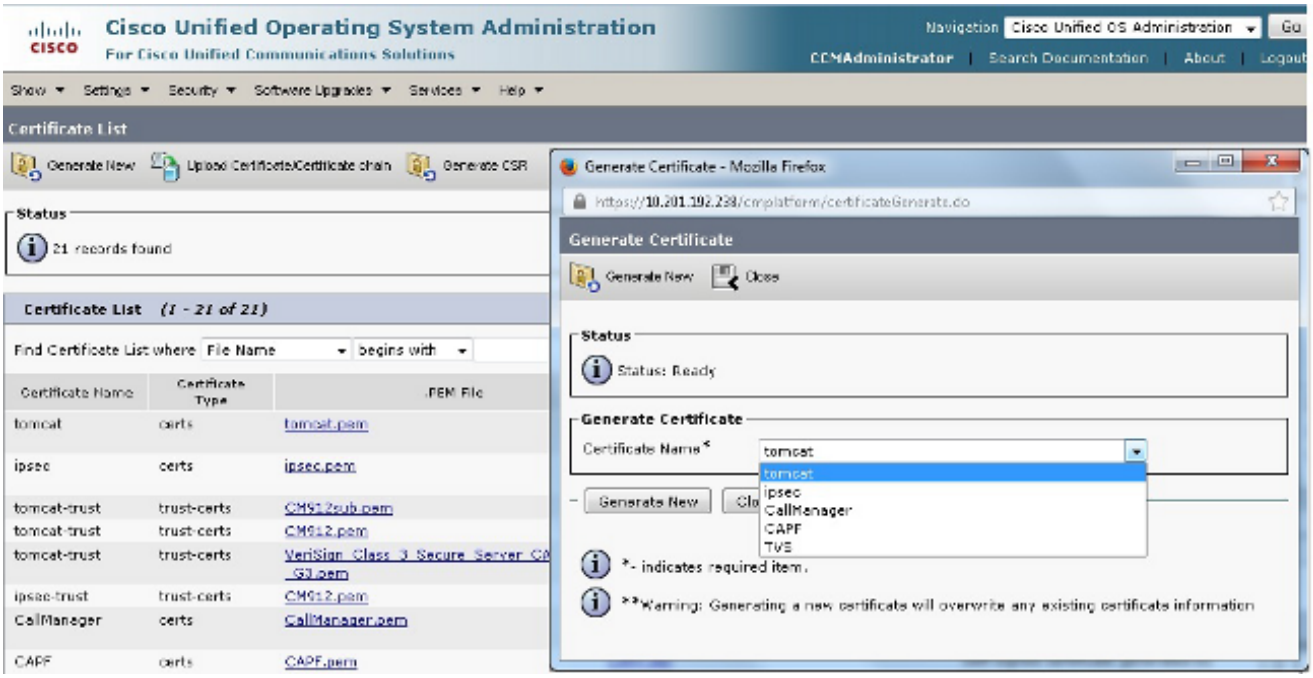


5. 認証（Tomcat 認証この場合）をクリックし、次のイメージで強調表示されるように日付を、見て下さい。 Tomcat 認証に関しては、サーバが **CCMAdmin ページ** ログインのためにサード パーティ 認証を使用するかどうか確認して下さい。 ブラウザからのページにログインするときこれをチェックできます。

   注: それがサード パーティ 署名入り認証である場合、CCMAdmin Web GUI 認証 Ciscoサポート コミュニティ技術情報をアップロードする CUCM を参照し、Tomcat 再生成の後でステップを完了して下さい。

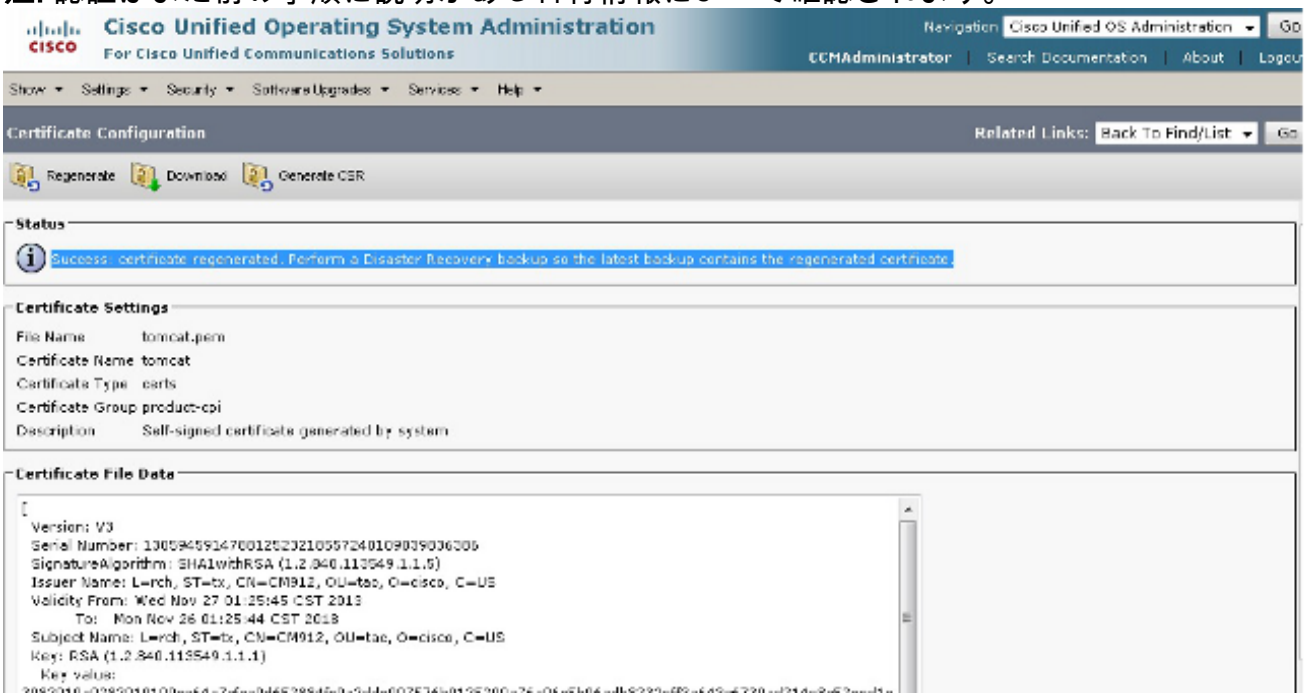


6. パブリッシャの**証明書管理** ページにナビゲート して下さい。 見つけ、**tomcat.pem ファイルを**クリックし、それから再生をクリックして下さい:



7. そのノードの Tomcat サービスを再開し、CLI をノードに開き、**utils サービス再始動 Cisco Tomcat** コマンドを入力するため。 認証が生成されれば認証が現在であることを確認するために、メッセージはポップアップします。

   注: 認証はまた前の手順に説明がある日付情報によって確認されます。



8. Tomcat 認証を再生するためにクラスタのサブスクライバのそれぞれのためのこのプロセスを完了して下さい。

CUCM バージョン 8.x および それ 以降のための認証再生

Cisco Unified Communications Manager （ CUCM ）バージョン 8.x および それ 以降のための期限の 切れた 認証を再生するためにこのセクションで情報を使用して下さい。

注: サービスを再開し、プロセスの電話をリブートする必要があるので、正常な営業時間後

に認証を再生して下さい。

CAPF

認証局（CA）プロキシ 機能（CAPF）再生成に関しては、クラスタがセキュア クラスタ モードにないようにして下さい: **クラスタ セキュア モード**のための CM 管理Webページおよび検索からの **System > Enterprise Parameters** にナビゲート して下さい。 値が **0** である場合、クラスタはセキュア クラスタ モードにありません。 値がゼロ以外数である場合、クラスタはセキュア モードにあり、CTL ファイルをアップデートするために Certificate trust list （CTL） クライアントを使用して下さい。

注: 詳細については IP Phone セキュリティおよび CTL（証明書信頼リスト） Ciscoサポート コミュニティ技術情報を参照して下さい。

1. パブリッシャから、証明書管理 ページにナビゲート して下さい。
2. **CAPF.pem ファイルを**開き、再生をクリックして下さい。 **これは**認証を更新し、2 つの新しい信頼ファイルを作成します: 1 つは CM 信頼であり、他は CAPF 信頼です。
3. サービサビリティ ページから、**ツール > 機能 サービス**へのナビゲート。
4. CAPF サービスが**機能 サービス**の下でアクティブになる場合、サービスを再開して下さい。 CAPF サービスがアクティブにならない場合、再始動は必要ではないです。
5. **ツール >** サービサビリティ ページからの**ネットワークサービス**にナビゲート し、信頼確認サービス（TV）サービスを再開して下さい。
6. **ツール >** サービサビリティ ページからの**機能 サービス**にナビゲート し、ノードを規定 し、TFTPサービスを再起動して下さい。
7. サービスが再開されたら、更新済識別信頼リスト（ITL）ファイルを取得できるように電話をリブートして下さい。
8. 証明書管理 ページに戻り、2 つの古い信頼ファイルを削除して下さい。 これらはエラー出力から受け取った 2 つの切らされた信頼ファイルです。 新しい認証に **CAPF.pem ファイルと**一致するシリアル番号があります。
9. 各サブスクライバのための前の手順を完了して下さい。

IPSec

インターネット プロトコル セキュリティ（IPSec）認証はディザスタ リカバリ失敗（DRF）マスターおよびローカルに影響を与えます、バックアップと復元機能を取扱う。

1. パブリッシャの OS 管理 ページへのナビゲート。
2. **セキュリティ > Certificate Management** にナビゲート し、**IPSEC.pem ファイルを**クリック

して下さい。

3. 信頼ファイルをアップデートするために**再生を**クリックして下さい。

4. 認証が再生したことサーバをリブートして下さい。 各サービスが後あらゆる認証のあらゆる再生成/アップデート再開する必要があったのでこれが必要となります。 ただし全体のノードをリブートする、IPSec にサービス再始動機能が以外ありません。 他の認証がアップデートされることを/再生する必要がある場合すべてのステップを完了し、次にノードをリブートして下さい結局認証が処理された。 これはサーバが truststore でアップデートされるすべての認証を持つようにおよびきちんと読取るようにします。

CM

1. パブリッシャの OS 管理 ページへのナビゲート。

2. 証明書管理 ページにナビゲート し、『Find』 をクリック し、**CallManager.pem ファイルを**クリックし、それから再生をクリックして下さい**。**

3. **ツール >** サービサビリティ ページの**機能サービス**にナビゲート し、指定されたノードを見つけ、Cisco CM サービスを再開して下さい。

4. サービサビリティ ページから、**ツール > ネットワークサービス**にナビゲート し、TV サービスを再開して下さい。

5. サービサビリティ ページから、**ツール > 機能 サービス**にナビゲート し、ノードを規定 し、CM および CTI サービスを再開して下さい。

6. 更新済 ITL ファイルを取得できるように電話をリブートして下さい。

7. 各サブスクライバのための前の手順を完了して下さい。

TVS

1. パブリッシャの OS 管理 ページへのナビゲート。

2. **セキュリティ > Certificate Management** にナビゲート し、『Find』 をクリック し、**TVS.pem ファイルを**クリックし、それから再生をクリックして下さい**。**

3. サービサビリティ ページから、**ツール > ネットワークサービス**にナビゲート し、TV サービスを再開して下さい。

4. サービサビリティ ページから、**ツール > 機能 サービス**にナビゲート し、ノードを規定 し、TFTPサービスを再起動して下さい。

5. 更新済 ITL ファイルを取得できるように電話をリブートして下さい。

6. 各サブスクライバのための前の手順を完了して下さい。

認証を削除して下さい

認証を削除するとき、以前に述べられたサービスが停止すること、そして確認して下さい現在実際に期限切れ使用されないし、ではないことを削除する認証ことを。

また削除の後でそれを保存することができないので、認証内の情報すべてを常にチェックして下さい。