

# Connected Threat Defense Step by Step設定ガイド(IMSVA)

トレンドマイクロ株式会社



TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScan Web Security Suite、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro Mobile Security、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan Web Manager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンアップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おまかせハックアタック対策、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンアップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Airサポート、Connected Threat Defense、ホワイトクリーナー、Trend Micro Policy Manager、メールダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、およびTrend Micro Policy-based Security Orchestrationは、トレンドマイクロ株式会社の登録商標です。

# 製品名の表記について

本ドキュメントにおいては製品名等は以下のように表記します。

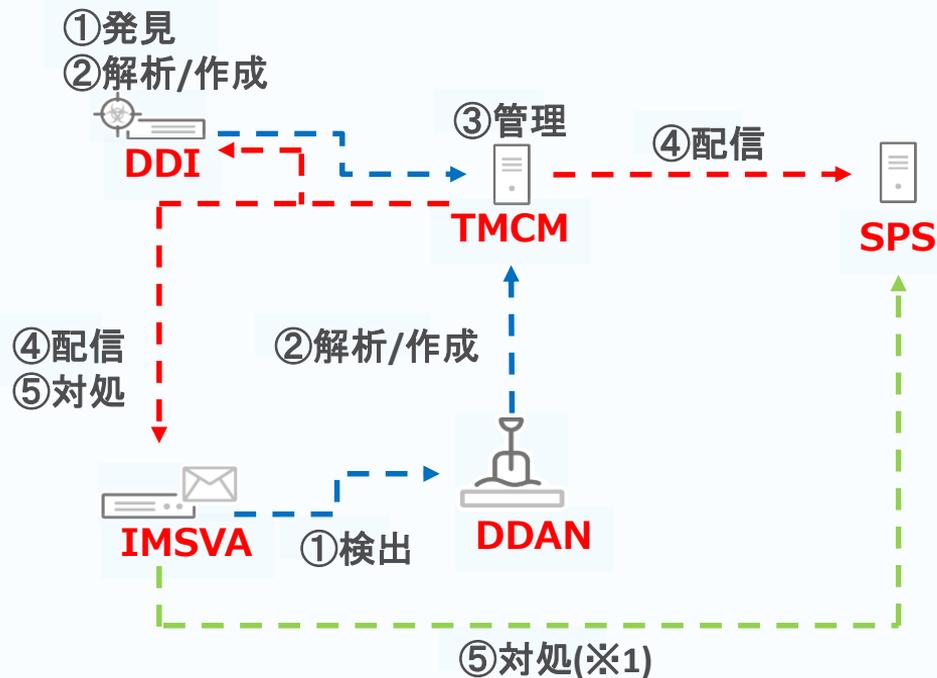
- Connected Threat Defense … 「CTD」
- Trend Micro Deep Discovery Analyzer … 「DDAN」
- Trend Micro Control Manager … 「TMCM」
- InterScan Messaging Security Virtual Appliance … 「IMSVA」
- Smart Protection Server … 「SPS」
- Trend Micro Deep Discovery Inspector … 「DDI」
- 不審オブジェクト[Suspicious Object] … 「SO」

# 本ドキュメントの目的

本ドキュメントはIMSV Aを中心としたCTDの設定に特化した資料となります。

CTDの製品間連携の設定をする必要があり、手順は複雑になりがちです。その手順をStep by Stepで解説し、順番通りに設定すればCTDに必要な連携設定は完了します。また、各画面におけるパラメータの解説はしておりませんので、必要に応じて各製品の管理者ガイド等を参照ください。

# 連携構成図



- ※1 不審オブジェクト(URL)の検出には、統合SPSまたはスタンドアロンSPSを参照します。
- ※2 DDIは必須コンポーネントで無いため、利用されていない環境では以降の設定は割愛ください。

# 目次

STEP0 事前準備	P6-P8
STEP1 TMCM-DDANを連携する	P9-P12
STEP2 TMCM-DDIを連携する	P13-P17
STEP3 TMCM-SPSを連携する	P18-P20
STEP4 IMSVA-SPSを連携する	P21-P26
STEP5 TMCM-IMSVAを連携する	P27-P31
STEP6 IMSVA-DDANを連携する	P32-P36

# STEP0 事前準備

---

# STEP0-1 DDANのAPIキーを取得する

1. DDANのWEBコンソールへアクセスします  
[https://\[DDAN IP or FQDN\]/pages/login.php](https://[DDAN IP or FQDN]/pages/login.php)
2. ログインします
3. [ヘルプ] - [バージョン情報] をクリックします
4. 以下の情報(APIキー)を控えます(以降、※1と記載)

現在の位置: ヘルプ > バージョン情報

④ 製品ライセンスの有効期限はあと49日で終了します。保護を継続するには、[新しいアクティベーションコードの入力](#)を行ってください。

### バージョン情報

---

**製品情報**

**Deep Discovery Analyzer**

フォームウェアのバージョン: 5.0.0.4480

**APIキー:** 9 [REDACTED] D0

CPU: Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz 16 cores  
取り付け済みのメモリ: 16 GB

Copyright © 2017 Trend Micro Incorporated. All rights reserved.

このソフトウェアは著作権法および国際条約により保護されています。この製品の全部または一部を無断で複製したり、無断で複製物を頒布すると、著作権の侵害となりますのでご注意ください。

[サードパーティのライセンス情報](#)

# STEP0-2 TMCMのサービスURLとAPIキーを取得する

1. TMCMのWEBコンソールへアクセスします

[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)

2. ログインします

3. [運用管理] - [不審オブジェクト] - [配信設定] をクリックします

4. 以下の情報(サービスURL、APIキー)を控えます(以降、※2と記載)



TREND MICRO Control Manager™ ユーザ名: root

★ ダッシュボード ディレクトリ ▼ ポリシー ▼ ログ ▼ レポート ▼ アップデート ▼ 運用管理 ▼

### 配信設定

Control Managerは仮想アナライザとユーザ指定の不審オブジェクトを統合し、それらを管理下の製品と他社のソリューションに送信します。

#### トレンドマイクロの管理下の製品の設定

不審オブジェクトを管理下の製品に送信します。 [詳細情報](#)  
次の設定を使用します:

サービスURL: 1 [REDACTED]

APIキー: 00 [REDACTED].2E

HP TippingPointの設定

# STEP1 TMCM-DDANを連携する

---

# STEP1-1 DDANをTMCMへ登録する

1. TMCMのWEBコンソールへアクセスします

[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)

2. ログインします

3. [運用管理] - [管理下のサーバ] をクリックします

4. [サーバの種類]からDeep Discovery Analyzer を選択します

5. [追加]をクリックします

# STEP1-1 DDANをTMCMへ登録する

6. 以下のパラメータを入力し、[保存]をクリックします

プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理管理] - [設定] - [プロキシ設定]を事前に設定する必要あり

DDAN WEBコンソールのURLを入力

TMCM上での表示名を入力(任意)

DDAN WEBコンソールのログイン情報を入力

# STEP1-1 DDANをTMCMへ登録する

## 7. TMCMに登録されたことを確認します



管理下のサーバ

サーバの種類: Deep Discovery Analyzer

追加 | 表示の更新 | プロキシの設定 | クラウドサービスの設定 | ディレクトリ管理

サーバ	表示名	製品	接続タイプ	最新のレポート	処理
<a href="https://10.0.100.11">https://10.0.100.11</a>	DDAN	Deep Discovery Analyzer 5.8	手動	2018/06/13 07:55 am	 

レコード: 1 - 1 / 1 | ページ 1 / 1 | 10 / ページ

日時が表示されて  
いれば正常に登  
録が完了している

# STEP2 TMCM-DDIを連携する

---

# STEP2-1 DDIをTMCMへ登録する

1. DDIのWEBコンソールへアクセスします

[https://\[DDI IP or FQDN\]/](https://[DDI IP or FQDN]/)

2. ログインします

3. [管理] - [統合製品/サービス] - [Control Manager] をクリックします

# STEP2-1 DDIをTMCMへ登録する

## 4. 以下のパラメータを入力し、登録をクリックします

プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理] - [システム設定] - [プロキシ]を事前に設定する必要あり

The screenshot shows the 'Control Manager' registration page. It includes sections for connection status, connection settings, server settings, bidirectional port transfer, proxy settings, and synchronization of out-of-sync objects. Red boxes and arrows highlight specific fields: the 'Entity Display Name' field (DDI), the 'Server Settings' section (port 443, HTTPS checked, admin user), the 'Proxy Settings' section (checkbox for proxy server), and the 'Synchronization of Out-of-Sync Objects' section (checkbox checked, API key field).

**Control Manager**  
Deep Discovery InspectorとControl Managerとの間の通信を設定します。

接続ステータス  
Control Managerサーバ登録ステータス: 登録されていません

接続設定  
サーバアドレス: [REDACTED]  
エンティティ表示名\*: DDI

Control Managerサーバ設定  
サーバの完全修飾ドメイン名IPアドレス\*: [REDACTED]  
ポート\*: 443  HTTPSを使用して接続する  
Webサーバ認証:   
ユーザ名: admin  
パスワード: [REDACTED]

双方向通信ポート転送  
 双方向通信ポート転送を有効にする  
IPアドレス: [REDACTED]  
ポート: [REDACTED]

プロキシ設定を使用  
 プロキシサーバを使用して接続する

不審オブジェクトの同期  
 不審オブジェクトをControl Managerと同期する  
APIキー: [REDACTED] 2E

登録 接続テスト キャンセル

TMCM上での表示名を入力(以降、※3と記載)

TMCMの接続情報に合わせて設定

チェックし、「※2>APIキー」を入力

# STEP2-1 DDIをTMCMへ登録する

## 5. TMCMに登録されたことを確認する

### Control Manager

Deep Discovery InspectorとControl Managerとの間の通信を設定します。

**接続ステータス**

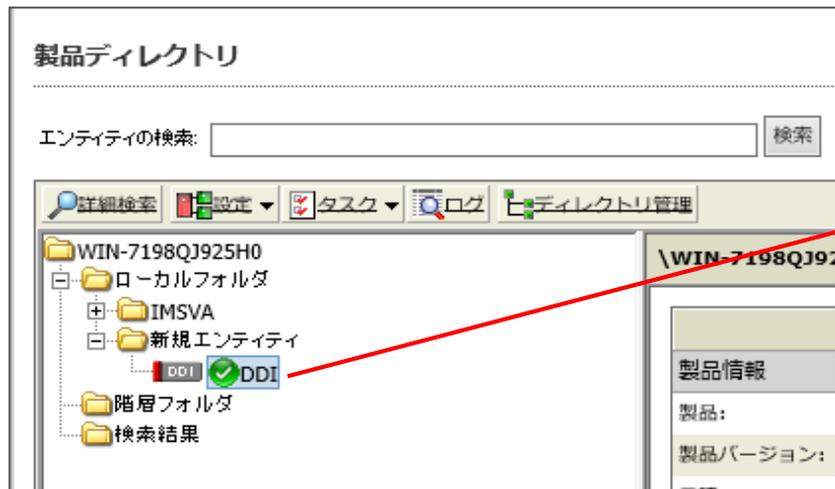
登録済みControl Managerサーバ: **10.0.2.10-100**

最終接続ステータス: 2018年06月14日 08時03分58秒

日時が表示されて  
いれば正常に登  
録が完了している

# STEP2-2 DDIがTMCMへ登録されたことを確認する

1. TMCMのWEBコンソールへアクセスします  
[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)
2. ログインします
3. [ディレクトリ] - [製品] をクリックします
4. ディレクトリツリーを展開します
5. ディレクトリツリー下に「※3」が登録されていることを確認します



※3の表示を確認し、  
緑アイコンが表示され  
ていれば正常に登録  
が完了している

# STEP3 TMCM-SPSを連携する

---





# STEP4 IMSVA-SPSを連携する

---

# STEP4-1 IMSVAにSPSを登録します

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [ポリシー] – [Smart Protection] – [ローカルソース] をクリックします

4. 追加をクリックします

# STEP4-1 IMSVAにSPSを登録します

5. 以下のパラメータを設定し、保存をクリックします

プロキシサーバを介してアクセスする必要がある場合はチェックする

Smart Protection

[ローカルソース]→[Smart Protection Serverの追加]

Smart Protection Server

Smart Protection Serverのアドレスを確認するには、サーバのコンソールを開き、[概要] 画面を参照してください。

サーバ: [localhost]

例: server.us.trendnet.org、10.1.1.1、または2001:db8:10ffae:44f2

ファイルレビュテーションポート: 443

SSLを有効にする

Webレビュテーションポート: 5274

プリファレンス: 10

プロキシ設定

有効

プロキシタイプ: HTTP

プロキシサーバ: [ ]

プロキシポート: [ ]

ユーザー: [ ]

パスワード: [ ]

保存 キャンセル 接続テスト

SPSのIP or FQDNを設定する

SPS側の設定に沿って設定ください

SPS側の設定に沿って設定ください

# STEP4-1 IMSVAにSPSを登録します

## 6. 正常に登録出来たことを確認します

Smart Protection

セキュリティリスク検索 Webレピュテーションサービス **ローカルソース**

Smart Protection Serverリスト

追加 削除 インポート エクスポート

<input type="checkbox"/>	Smart Protection Serverのアドレス	ファイルレピュテーション	Webレピュテーション	プリファレンス
<input type="checkbox"/>	XXXXXXXXXX	✓	✓	10

緑アイコンで成功しています

# STEP4-2 ファイルレピュテーションを設定する

1. [ポリシー] – [Smart Protection] – [セキュリティリスク検索] をクリックします
2. 以下のパラメータを設定し、保存をクリックします

こちらを選択し、STEP4-1で設定した、SPSを指定します

Smart Protection

セキュリティリスク検索 Webレピュテーションサービス ローカルソース

検索方法

従来型スキャン ⓘ

スマートスキャン - ファイルレピュテーションサービス ⓘ

Trend Micro Smart Protection Network ⓘ

Smart Protection Server ⓘ

Smart Protection Serverを [Smart Protection]→[ローカルソース] で設定します。

Trend Micro Smart Protection NetworkまたはSmart Protection Serverに接続できない場合は従来型スキャンに切り替える

保存 キャンセル

# STEP4-3 Webレピュテーションを設定する

1. [ポリシー] – [Smart Protection] – [Webレピュテーション] をクリックします
2. 以下のパラメータを設定し、保存をクリックします

こちらを選択し、STEP4-1で設定した、SPSを指定します

Smart Protection

セキュリティリスク検索 Webレピュテーションサービス ローカルソース

Webレピュテーションサービス

Trend Micro Smart Protection Network  
グローバルプロキシ認証資格情報は、[管理]→[プロキシ] で設定します。

Smart Protection Server

Smart Protection Serverに接続できない場合はTrend Micro Smart Protection Networkに切り替える

Smart Protection Networkへの外部クエリを実行しない

Smart Protection Serverを [Smart Protection]→[ローカルソース] で設定します。

注意: Smart Protection Serverを選択する場合は、この製品Q&A記事を参照して、トレンドマイクロでテストされていないURLを評価し、そのURLにTime-of-Clickプロテクションのスマートフラグを付けるようSmart Protection Serverを設定する方法について確認してください。

保存 キャンセル

# STEP5 TMCM-IMSVAを連携する

---

# STEP5-1 IMSVAをTMCMへ登録する

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)

2. ログインします

3. [管理] - [管理 > IMSVA設定] - [接続] - [Control Managerサーバ] をクリックします

# STEP5-1 IMSVAをTMCMへ登録する

## 4. 以下のパラメータを設定し、保存をクリックします

TMCM上の  
表示名(以降  
、※4と記載)

チェックする

認証が必要で  
あれば設定しま  
す

チェックする

チェックする

接続ステータス  
bka-ctdmsva01.oka.com 登録されていません

Control Managerサーバの設定  
IMSVAをControl Managerで管理するには、Control Manager MCPエージェントを有効にして、すべてのControl Managerサーバの設定項目を入力してください。

全エージェントを登録解除

MCPエージェントを有効にする  
サーバ: [ ]  
通信プロトコル:  
 HTTPポート: [80]  
 HTTPSポート: [443]

Webサーバ認証:  
ユーザ名: [admin]  
パスワード: [ ]

プロキシ設定  
 プロキシを有効にする  
プロキシのタイプ: [HTTP]  
プロキシサーバ: [ ]  
ポート: [ ]  
ユーザ名: [ ]  
パスワード: [ ]

不審オブジェクトリストの設定  
 不審ファイルリスト [ ]  
同期間隔: [5] 分  
前回の同期: [該当なし]  
 不審URLリスト [ ]

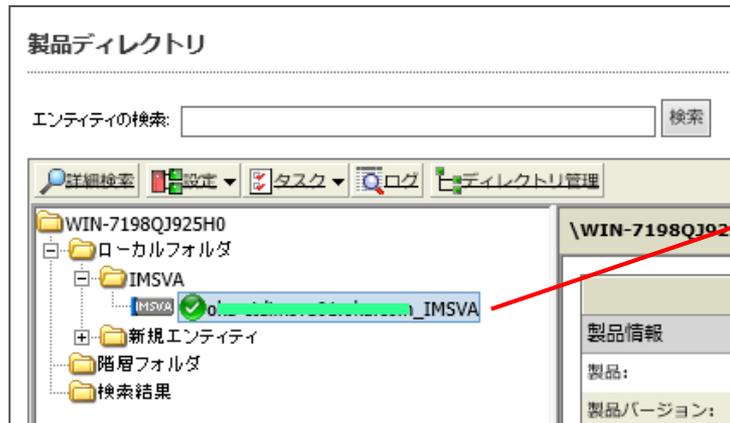
保存 キャンセル

TMCMのIP or  
FQDNを記載す  
る

プロトコル及び  
ポート番号を指  
定します

# STEP5-2 IMSVAがTMCMへ登録されたことを確認する

1. TMCMのWEBコンソールへアクセスします  
[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)
2. ログインします
3. [ディレクトリ] - [製品] をクリックします
4. ディレクトリツリーを展開します
5. ディレクトリツリー下に「※4」が登録されていることを確認します



※4の表示を確認し、  
緑アイコンが表示され  
ていれば正常に登録  
が完了している

# STEP5-3 TMCM上のIMSVA情報にログイン情報を登録する

1. TMCMのWEBコンソールへアクセスします

[https://\[TMCM IP or FQDN\]/webapp/login.aspx](https://[TMCM IP or FQDN]/webapp/login.aspx)

2. ログインします

3. [運用管理] - [管理下にサーバ] をクリックします

4. [サーバの種類] からInterScan Messaging Security Virtual Appliance を選択します

5. 「※4」の登録を確認後、処理をクリックします

サーバ	表示名	製品	接続タイプ	最新のレポート	処理
<a href="https://[redacted]">https://[redacted]</a>	[redacted]	InterScan Messaging Security Virtual Appliance 9.1	自動	2018/06/14 03:15 pm	

# STEP5-3 TMCM上のIMSVA情報にログイン情報を登録する

6. IMSVAのWEBコンソールの認証情報を設定し、保存をクリックします

サーバの編集

**サーバ情報**

サーバ:   
例: http(s)://<サーバ名>:ポート番号

表示名:

製品: InterScan Messaging Security Virtual Appliance 9.1

---

**認証**

ユーザ名:

パスワード:

---

**接続**

接続にプロキシサーバを使用する

保存      キャンセル

# STEP6 IMSVA-DDANを連携する

---

# STEP6-1 IMSVAへDDANを登録する

1. IMSVAのWEBコンソールへアクセスします  
[https://\[IMSVA IP or FQDN\]:8445/console.imss](https://[IMSVA IP or FQDN]:8445/console.imss)
2. ログインします
3. [管理] - [ポリシー] - [仮想アナライザ] - [サーバ管理] をクリックします
4. [追加] をクリックします
5. パラメータを設定し、保存をクリックします。

チェックする

DDAN IP or  
FQDNを記載  
する

仮想アナライザ

[サーバ管理] -> [サーバの追加]

仮想アナライザサーバ

有効

サーバ:

例: server.us.trendnet.orgまたは10.1.1.1

ポート:

APIキー:

プリファレンス:

保存 キャンセル

※1を記載する

# STEP6-2 仮想アナライザへの送信設定をする

1. IMSVAのWEBコンソールへアクセスします

[https://\[IMSV A IP or FQDN\]:8445/console.imss](https://[IMSV A IP or FQDN]:8445/console.imss)

2. ログインします

3. [管理] - [ポリシー] - [仮想アナライザ] - [仮想アナライザ設定]をクリックします

チェックする

DDAN IP or  
FQDNを記載  
する

仮想アナライザ

[サーバ管理] -> [サーバの追加]

仮想アナライザサーバ

有効

サーバ:

例: server.us.trendnet.orgまたは10.1.1.1

ポート:

APIキー:

プリファレンス:

保存 キャンセル

※1を記載する

# STEP6-2 仮想アナライザへの送信設定をする

## 4. パラメータを設定し、保存をクリックします。

チェックする

仮想アナライザ

仮想アナライザの設定    サーバ管理

メールメッセージを仮想アナライザに送信 ⓘ

セキュリティレベルの設定

仮想アナライザがメッセージのリスクレベルを評価した後、IMSVAが以下に設定されたセキュリティレベルに基づいて指定された処理をメッセージに対して実行します。

高    不審な動作を示しているすべてのメッセージに処理を適用する

中    不正プログラムである可能性が中程度から高いメッセージに処理を適用する

低    不正プログラムである可能性が高いメッセージにのみ処理を適用する (推奨)

タイミングの設定

分析の最長時間:    1800 秒 (値の範囲:300-1800)

データベース切断設定

IMSVAの管理データベースの接続が切断されると、次の処理が実行されます。

仮想アナライザへのメッセージ送信の停止

仮想アナライザの検索除外に指定された処理の実行

仮想アナライザのプロキシ設定

プロキシを有効にする

プロキシのタイプ:    HTTP

プロキシサーバ:    \_\_\_\_\_

プロキシサーバポート:    8080

ユーザー名:    \_\_\_\_\_

パスワード:    \_\_\_\_\_

保存    キャンセル

プロキシサーバを介してアクセスする必要がある場合はチェックする

※[管理]-[プロキシ]を事前に設定する必要あり

