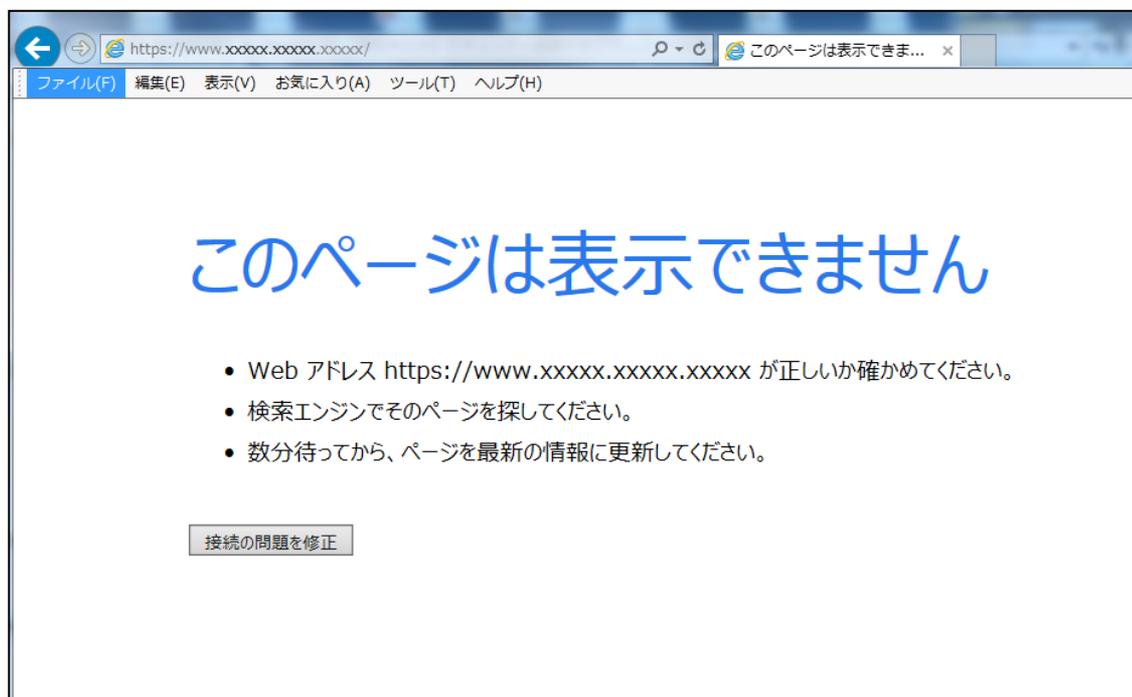


HTTPS通信が遮断される場合の対処（1/5）

以前アクセス可能だったWebページに2018年6月4日以降アクセスできなくなった場合、ゲートウェイ装置のファームウェアバージョンアップによる影響の可能性あります。

その場合、以下の手順に則りゲートウェイ装置の設定を変更することで再度アクセス可能にすることができます。

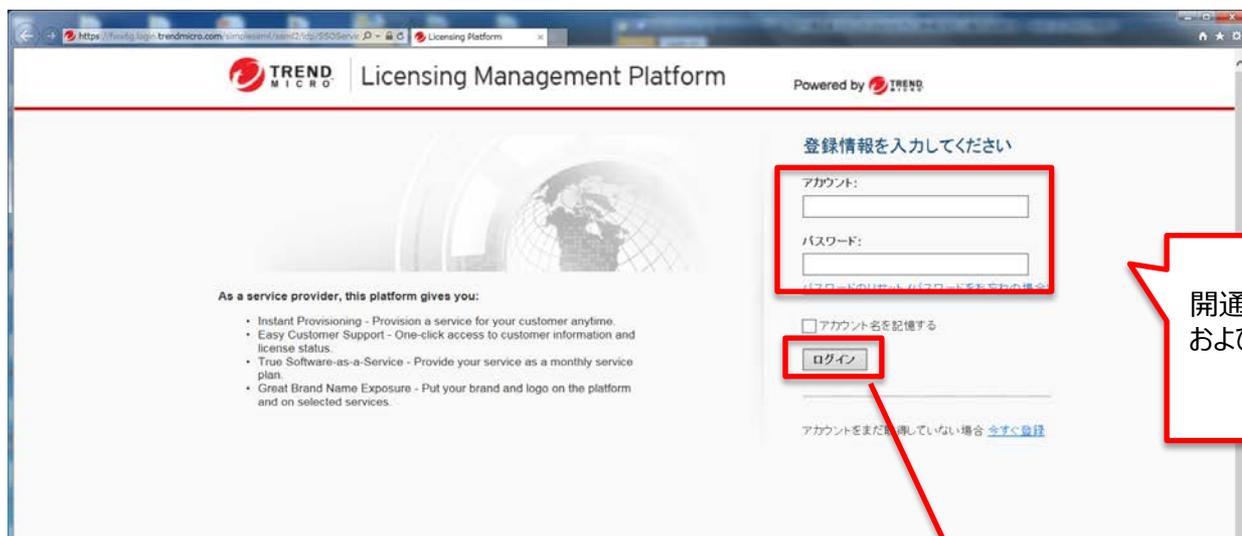
【ゲートウェイ装置で通信が遮断された場合のWebブラウザ表示イメージ（※）】



（※）本メッセージが表示される原因はURLの間違い、Webサーバー側の過負荷等複数考えられます。
ゲートウェイ装置のバージョンアップが原因だった場合のみ有効であることをご理解の上以下の手順を実施してください。

HTTPS通信が遮断される場合の対処 (2/5)

開通時に送付したメールに記載のURL (https://clp.trendmicro.com/Dashboard?T=fWX6g) にアクセスし、アカウント名・パスワードをご入力いただくことによりLicensing Management Platform (LMP) にログインすることができます。ログイン後、画面右側の「コンソールを開く」をクリックしていただくことにより、Cloud Edge Cloud Console (CECC) にログインすることができます。



サービスプラン名	製品/サービス	シート/ユニット	ライセンス種別	開始日	有効期限	アクション
【体験版】CloudEdge 50	Cloud Edge 50	5シート	体験版	2018/05/22	2018/06/21 (残り31日)	コンソールを開く

● 有効期限内 ⚠ 間もなく期限切れ ✖ 有効期限切れ

HTTPS通信が遮断される場合の対処 (3/5)

CECCにログイン後[ポリシー]の[許可/ブロックリスト]をクリックし、許可リストに[URLの追加]を行います。

The screenshot displays the CECC web interface. At the top, a navigation bar includes 'ダッシュボード', 'ゲートウェイ', 'ポリシー', '分析とレポート', and '管理'. The 'ポリシー' menu is highlighted with a red box. Below it, a sidebar lists various policy objects, with '許可/ブロックリスト' highlighted in a red box. The main content area shows the '許可/ブロックリスト' management screen, with the '許可リスト' tab selected. A red box highlights the '追加' button, and an arrow points to a dropdown menu where 'URLの追加' is selected. Another red box highlights the 'URLの追加' button in the dropdown menu. A third red box highlights the '許可リスト' tab. Two callout boxes provide instructions: one pointing to the '許可/ブロックリスト' menu item and another pointing to the 'URLの追加' button.

[ポリシー]から[許可/ブロックリスト]に進みます。

[許可リスト]で[URLの追加]を実施します。

HTTPS通信が遮断される場合の対処 (4/5)

[許可するURLの入力]欄にアクセス可能なWebサイトのURLを記載し、[保存]をクリックします。
なお、むやみにURLを追加するとセキュリティホールになりかねませんので、必要なURLのみ許可設定を実施してください。

許可するURLの追加/編集

許可するURLは安全であると見なされます。この設定はURLフィルタルールよりも優先されます。URL文字列の先頭または最後に、ワイルドカードとしてアスタリスク (*) を使用できます。

許可するURLの入力

xxxx.xxxx/

ゲートウェイグループの選択

すべてのゲートウェイ

ゲートウェイグループを指定する

保存 キャンセル

アクセス可能なWebサイトのURLを入力します。

「*」はワイルドカードで下記のように用います。

「https://xxxx.xxxx/*」

↓

「https://xxxx.xxxx/」で始まるURLを許可

「*xxxx.xxxx/*」

↓

「xxxx.xxxx/」を含むURLを許可

入力が完了したら
[保存]をクリックします。

HTTPS通信が遮断される場合の対処 (5/5)

[すべて配信]をクリックし、正常に処理が完了しましたらログアウトします。

以上の手順でアクセス可能にならない、または不明点がございましたら「セキュリティおまかせサポートセンタ」（電話番号は開通時のメールに記載）にご連絡ください。

The screenshot displays the Trend Micro Cloud Edge management interface. At the top, there is a navigation bar with tabs for 'ダッシュボード', 'ゲートウェイ', 'ポリシー', '分析とレポート', and '管理'. Below this, a notification bar indicates that settings have been updated and prompts the user to click 'すべて配信' to reflect changes. The main content area is divided into several sections. On the left, there is a sidebar with a 'すべて配信' button and a 'ゲートウェイ配信ステータス' section showing a green checkmark and the text 'Cloud Edge_01'. In the center, there is a '許可/ブロックリスト' section with a table of whitelisted URLs. The table has columns for '名前', '種類', and 'ゲートウェイグループ'. The table contains the following entries:

名前	種類	ゲートウェイグループ
.apple.com/	URL	すべて
.google.com/	URL	すべて
.trendmicro.com/	URL	すべて
.trendmicro.org/	URL	すべて
download.windowsupdate.com/	URL	すべて
update.microsoft.com/	URL	すべて
windowsupdate.com/	URL	すべて
windowsupdate.microsoft.com/	URL	すべて
xxxx.xxxx/	URL	すべて
cloudedge50-p.activeupdate.trendmicro.com/activeupdate	URL	すべて