

# Web 改ざん検知

---

Web 改ざん検知は、お客様が作成、管理されているウェブサイトが安全であることを確認するためのサービスとなります。診断対象のドメインと URL を登録することにより、Web 改ざん診断が実行され、マルウェアが検出された場合は、ご登録いただく管理者様にアラートメールが送信されます。

診断するページ数により、5段階のプランを提供しております。

- Web 改ざん検知サービス 100 ページ(URL 5 個、5 ドメイン) (無料オプション)
- Web 改ざん検知サービス 300 ページ(URL 5 個、5 ドメイン)
- Web 改ざん検知サービス 1000 ページ(URL 10 個、10 ドメイン)
- Web 改ざん検知サービス 2000 ページ(URL 10 個、10 ドメイン)
- Web 改ざん検知サービス 3000 ページ(URL 10 個、10 ドメイン)

## お申し込み方法



## Web 改ざん検知の管理画面へのログイン

### 1 Web 改ざん検知の管理画面へのログイン

Web 改ざん検知の管理画面ログインページの URL にアクセスします。

Web 改ざん検知の管理画面 URL : <https://www.gred.jp/saas/cpi>

ユーザ ID とパスワードを入力してログインします。

お知らせ

- 2016年11月09日 [アプリケーションメンテナンスのお知らせ](#)
- 2016年11月01日 [「重要」検索機能のお知らせ](#)
- 2016年09月30日 [定期システムメンテナンススケジュールのお知らせ](#)
- 2016年06月30日 [定期システムメンテナンススケジュールのお知らせ](#)
- 2016年05月18日 [アプリケーションメンテナンスのお知らせ](#)

過去の一覧を見る

メンテナンスおよび障害情報

- 2016年03月31日 [アラートメール送信サービス再開について](#)

過去の一覧を見る

ログインしてください。

ユーザーID

パスワード

ログイン状態を保存する

ログインする

[パスワードをお忘れの場合はこちらをクリック](#)

1-3 件 (全 3 件) 検索するタイトル  検索する

監視中 [www. \(http://\)](#)

ホーム

監視状態

レポート作成

監視内容の設定

監視結果

2016年11月23日 15:58

warning

再チェックする

2016年10月

日	月	火	水	木	金	土
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

2016年11月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

期間を選択してください

今日の検知結果確認

今日の検知結果はまだありません

最新のクロスドメイン検知リスト

最新の検知URLのリストをダウンロード

※ユーザ ID とパスワードは、管理者様へ別途メールで案内しております。

## 2 基本情報の変更

画面上部のリンクから変更できます。

### ユーザー管理

ユーザー管理	
新しいユーザーを追加します	
名前	<input type="text"/>
ログイン用メールアドレス	<input type="text"/>
アラート用メールアドレス	<input type="text"/>
アラートメール	<input checked="" type="radio"/> 受け取る <input type="radio"/> 受け取らない
アクセスの権限	<input type="checkbox"/> ウェブ解析 <input type="checkbox"/> CPI <input type="checkbox"/> www.kddi-webcommunications.co.jp <input type="checkbox"/> www.scalable.jp
<input type="button" value="追加する"/>	
ユーザーの編集	
<input type="button" value="変更する"/>	

新しいユーザーを追加できます。以下の項目を入力して追加ボタンをクリックしてください。

- **名前**  
名前の文字数は1文字以上128文字以下で指定してください。
- **ログイン用メールアドレス**  
受け取る／受け取らないを選択してください。
- **アクセスの権限**  
追加するユーザーへのアクセス権限を付与することができます。
- **アラート用メールアドレス**
- **アラートメール**

登録済みのユーザー情報を変更される際は、ユーザーの編集より変更をお願いいたします。

## ユーザー情報の変更

### ユーザー情報の変更

ユーザー情報を変更します。 **3**

ユーザID(ログインID):	<input type="text"/>
アラート用メールアドレス:	<input type="text"/>
ご担当者名(お名前):	<input type="text"/>
週間レポートメール通知:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アラートメール通知:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

\*ユーザID (ログインID) は変更できません。

以下を変更できます。

- アラート用メールアドレス
- 名前
- 週間レポートメール
- アラートメール

ID は変更することができません。

# ログアウト

Web 改ざん検知の管理画面からログアウトします。

## 3 ウェブ解析タブ

Web 改ざん検知の管理画面のウェブ解析画面で、お客様のウェブサイトのウェブ解析状況を確認することができます。

画面左側のリンクより、各項目をご確認いただけます。



## ホーム

Web改ざん検知の最終結果、カレンダー表示の診断結果をご確認いただけます。

最終結果の欄に表示されている再チェックするのボタンをクリックしますと、解析が実行されます。

カレンダー上で解析結果をご確認いただけます

- 「OK」：マルウェアが見つかりませんでした。
- 「！」：解析中に問題が見つかりました。「！」マークをクリックすると、問題の詳細画面が表示されます。

### ※問題が見つかった際の注意

"ウェブページに、未確認のクロスドメインスクリプトを発見しました。"

**問題が見つかりました**  
2010年10月17日 15:38

[http://18.aqtracker.com/asp/aq\\_tag2.js](http://18.aqtracker.com/asp/aq_tag2.js)



ウェブページに、未確認のクロスドメインスクリプトを発見しました。クロスドメインスクリプトとは、自社サイト以外のドメインにあるスクリプトを実行させるようなコードが自社のサイトに記述されているという事です。スクリプト自体を確認し、正常なものである場合には「[クロスドメインの許可設定](#)」メニューにて許可してください。このスクリプトを記載した覚えがない場合にはウェブサイトの改ざんが発生している恐れがあります。その場合にはただちに該当HTMLを確認して、修正を行ってください。また許可設定を行うと、今後「警告」のメッセージ等が表示されなくなります。必要な場合には「[クロスドメインの許可設定](#)」メニューにて許可設定を削除すると、以降、再び警告を発するようになります。クロスドメインスクリプトの許可機能のON/OFFは「[クロスドメインの許可設定](#)」から行えます。

### ウェブページにクロスドメインスクリプトを検知しました！

このメッセージは、自社サイト以外のドメインにあるスクリプトを実行させるようなコードが自社のサイトに記述されているということです。

スクリプト自体を確認し、正常なものである場合には「クロスドメインの許可設定」メニューにて許可してください。

### TOP ページの見た目が変化した可能性を検知

このメッセージは、TOP ページの見た目が変化した可能性を発見した時に送信されます。

### 実行ファイルのマルウェア類似挙動の可能性を検知

このメッセージは、監視対象ページにある実行ファイルが、マルウェアと類似した動きをしていることを発見した時に送信されます。

## 解析履歴

解析日	解析完了時間	解析結果	ページ数
2010年10月17日	15:39	クロスドメインスクリプトが存在します	906
2010年10月16日	15:40	クロスドメインスクリプトが存在します	906
2010年10月15日	15:40	クロスドメインスクリプトが存在します	905
2010年10月15日	14:42	クロスドメインスクリプトが存在します	905
2010年9月10日	03:37	問題はありませんでした	95
2010年9月9日	21:38	問題はありませんでした	95
2010年9月9日	15:33	問題はありませんでした	95
2010年9月9日	09:33	問題はありませんでした	95
2010年9月9日	03:33	問題はありませんでした	95
2010年9月8日	21:32	問題はありませんでした	95
2010年9月8日	15:33	問題はありませんでした	95
2010年9月8日	09:32	問題はありませんでした	95
2010年9月8日	03:32	問題はありませんでした	95

解析日、解析完了時間、解析結果、ページ数をご確認いただけます。

## レポート作成

### レポートの作成

レポートを表示する期間を選択してください。 

 解析履歴の保存期間は1年間です。

2016 年 11 月 >> 2016 年 11 月 

---

CLICK TRACK VIEW  2016年11月24日 10:08

### GREED Web改ざんチェック レポート

○ 解析対象ドメイン: http://www.

○ 解析期間: 2016年11月~2016年11月

○ 解析結果: 問題なし

	2016									11月
改ざんを通知した回数										0
貴社のウェブページ数(平均)										42

### 解析結果詳細

指定された期間には詳細情報はありません。



期間を指定して、レポートを作成できます。

レポートには以下が表示されます。

- ・ 解析対象ドメイン
- ・ 改ざんを通知した回数
- ・ 解析期間
- ・ 貴社のウェブページ数
- ・ 解析結果
- ・ 解析結果詳細

レポート作成後、レポートを印刷することも可能です。

## 解析内容の設定

### 解析内容の設定

[▶ 現在の利用状況一覧を見る>>](#)

#### 基本設定



[▶ 監視のON/OFFと基本設定](#)

#### 除外設定



[▶ ホワイトリスト](#)  
[▶ 除外URL](#)

#### クロスドメイン設定



[▶ クロスドメイン検知](#)

#### オプション



[▶ GRED証明書](#)  
[▶ 改ざん検知機能](#)

[ ウェブ解析開始URL・ウェブ解析対象ドメインを変更されたい際にはサポートまでお問い合わせください ]

Web 改ざん検知の解析内容の設定画面です。

[現在の利用状況一覧を見る>>](#) をクリックすると現在の設定を確認することができます。

ウェブ解析開始URL	http://www.cpi.ad.jp/
ウェブ解析対象ドメイン	cpi.ad.jp
ウェブ解析対象階層	無制限です
除外URL設定	利用していません
クロスドメイン設定	利用中です
クロスドメイン許可	9 個のURLが設定されています
オプション機能	利用していません



## 基本設定

基本設定	
監視のON/OFF	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
メニュータイトル	<input type="text"/> (全角20文字 半角40文字) ※ページ上部の「ウェブ解析」タブの下に表示される部分です。
ウェブ解析対象階層の指定	<input type="checkbox"/> 階層目まで ※何も記入しなければ「無制限」です。

[変更する](#)

## 除外設定

### [ ホワイトリスト ]

ホワイトリスト	
このリストに設定したURLは解析ページ数としてカウントされますが必ず「OK」という結果になります。最大10個まで指定する事が可能です。 	
ホワイトリストに登録したいURL	<input type="text" value="http://"/>

[登録する](#)

**ホワイトリストに登録されているURL**  
登録されているホワイトリストはありません

このリストに設定した URL は解析ページ数としてカウントされますが必ず「OK」という結果になります。最大10個まで指定する事が可能です。

### [ 除外 URL ]

除外URL	
除外URLは、パス（ディレクトリ）指定を最大10個まで設定することができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。 	
除外URLに登録したいパス（ディレクトリ）	<input type="text" value="http://"/>

[登録する](#)

**除外URLリスト**  
登録されている除外URLはありません

除外 URL は、パス（ディレクトリ）指定を最大10個まで設定することができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。

## クロスドメイン検知

### クロスドメイン検知

異種ドメイン以外のスクリプト(クロスドメインスクリプト)が発見された場合に警告を行います。  
ここでは、安全なクロスドメインスクリプトに対して警告しないように、自社のドメイン以外に利用しているスクリプトのドメインを許可リストに設定しておくことができます。

クロスドメインスクリプトの検知機能  有効  無効

[適用する](#)

#### 許可リスト：クイック登録

最近のチェックで見つかったクロスドメインスクリプトから、許可リストに登録できます。

すべてチェック

[https://](#)

[登録する](#)

#### 許可リスト：追加

許可リストにクロスドメインスクリプトが使用種のドメイン名、もしくはホスト名が登録できます。

許可リストに登録したいクロスドメイン  [登録する](#)

#### 許可リスト：編集

現在登録しているクロスドメインスクリプトの一覧です。登録している項目を削除することもできます。

すべてチェック

[削除する](#)

クロスドメインスクリプトの許可設定を行います。

ウェブ解析機能では、改ざんによって意図しないドメインのスクリプトがウェブページに埋め込まれた場合に「警告」を行います。


このリストにて、自社のドメイン以外に利用しているスクリプトのドメインを設定しておくことによって、解析結果の「！」表示を「Safe」に変更します。

## オプション

### [ gred 証明書 ]

### GRED証明書シール

最新検査日 12月30日

 GRED Web改ざんチェックをご利用の方に提供しているWebサイト用の証明書シールです。下記のタグをページ内のGRED証明書のシールを表示させたい部分に挿入して下さい。※証明書のタグはお客様ごとに異なります。

[証明書の検証ページを見る](#)

gred セキュリティサービスをご利用の方に無償で提供している証明書です。

表示されているタグをページ内の gred シールを表示させたい部分に挿入してください。

## [ 改ざん時切り替え機能 ]

### 改ざん時切り替え機能

gredがチェックを行なったページに改ざんが見つかった場合、お客様のWebサイトの訪問者にgred内のメンテナンスページを表示することができます。**HTMLのタグのすぐ後**に下記のタグを挿入して下さい。

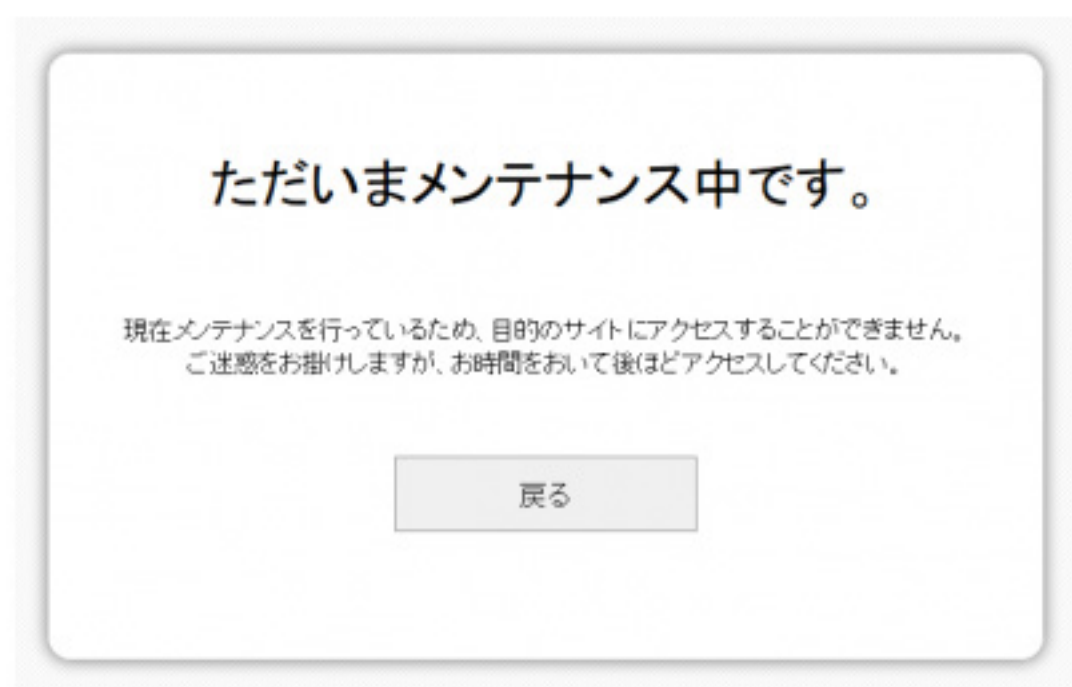
※パラメータにredirect\_uriを指定することでメンテナンスページのURLを独自に設定することが可能です。

[メンテナンスページを見る](#)

#### 切り替え機能の設定

上記のタグを一度挿入しておけば、切り替え機能の設定が下記より変更できるので、htmlの編集の手間が省けます。万が一弊社サービスで誤認により不正サイトとして検知されWebサイトがメンテナンス画面に切り替わっても、「無効」にすれば切り替え機能が解除され、通常通りページが表示されます。

切り替え機能設定    有効    無効



gred がチェックを行ったページに改ざんが見つかった場合、お客様の Web サイトの訪問者に gred 内のメンテナンスページを表示することができます。

HTML のタグのすぐ後に表示されているタグを挿入してください。

また、切り替え機能の有効／無効を設定することが可能です。

### ❗ 重要

Web 改ざん検知は、ウェブサイトのコンテンツを診断するサービスとなります。

マルウェアを削除したり、コンテンツが安全な状態になるようにサイトの内容を修正、改善するものではありません。

## 不正侵入検知（IDS/ADS）

---

不正侵入の検出（IDS）では、2,000種類のシグネチャを搭載し、多種多様なハッキングパターンを検知可能です。

不正侵入は3段階の危険度で分類され、ADSと連動することで不正侵入を防御します。

シグネチャは最新の状態に自動アップデートされるため導入後も安心してご利用いただけます。

また不正侵入からのディフェンス（ADS）でIDSが攻撃を検知した場合、攻撃元からのすべてのパケットを破棄するルールをファイアウォールに自動的に挿入し、リアルタイムで攻撃を阻止します。

※本サービスのご利用はご契約時に、別途専用ファイアウォールのお申し込みが必要です。

### ホワイトリスト登録について

不正侵入検知（IDS/ADS）ではお客様任意の接続元IPアドレスをホワイトリストに登録できます。（有償）

ホワイトリストに登録したIPアドレスは、不正侵入検知（IDS/ADS）の対象外となります。

ホワイトリスト登録をご希望の場合は、マイページのお問い合わせフォームまたはメール（管理先情報にご登録のメールアドレスから「[support@cpi.ad.jp](mailto:support@cpi.ad.jp)」）宛に『ご契約ドメイン（ご契約ID）とホワイトリストに登録されたいIPアドレス』をご明記のうえ、ご依頼ください。

# サポートについて

---

CPIにてサポート対象となる内容とサポート対象外とさせていただいている内容は以下のとおりです。  
ご不明な場合にはお問合せください。

## 目次

- 📄 サポート対象
- 📄 サポート対象外

## サポート対象

- コントロールパネルの操作、不具合について
- Web、FTP、メールなどのサーバーアクセス時のトラブル（障害など）
- CPI提供の各種サービスについて

※以下のサポート対象外の内容を除く

## サポート対象外

- プロバイダやお客様のローカルなネットワーク環境やパソコン環境について
- メールソフト、FTPソフトなどの設定や操作方法について
- データベース（MySQL、PostgreSQL）の操作方法について
- phpMyAdmin、phpPgAdminの操作方法について
- CMSインストーラーの各プログラムとphpBBとMovable Typeについて
- ホームページの作成方法（HTMLの記述方法など）について
- CPI提供以外のプログラムの動作や設定方法について
- 「.htaccess」「.htpasswd」の記述方法や動作について
- インターネット上でダウンロードしたプログラムの動作や設定方法について
- CPI提供のプログラムの編集方法について
- CPI提供のプログラムをお客様にて編集した場合の動作について
- スпамメールチェック機能の判定基準、判定結果について
- ウイルスチェック機能の判定基準、判定結果について
- スケジュール管理ツールの動作について
- ウェブメールの操作について
- アクセスログ分析の解析の方法について
- （どのようなルールで解析を行っているかについて）
- ログファイルの内容について

# 24/365 TEL &メールサポート

---

## ❗ 重要

こちらは有償オプションサービス「24時間365日TEL&メールサポート」をご契約いただきましたお客様のためのサービスとなります。オプションサービスをお申し込みいただいておりませんお客様につきましてはご利用がいただけませんのであらかじめご容赦くださいませ。  
お申し込みは[マイページ](#)より承ります。

## 目次

- 🔻 [ご利用いただけるお客様](#)
- 🔻 [受付方法](#)
- 🔻 [24時間365日TEL&メールサポートのサポート範囲について](#)
- 🔻 [ご注意](#)

## ご利用いただけるお客様

24時間365日TEL&メールサポートは以下のお客様からのお問い合わせに対してご回答を行っております。

- ご契約情報に登録されている管理担当者様

## 受付方法

専用の電話番号と、メールアドレスをご用意しております。  
ご連絡をいただく場合には、必ずドメイン名のご連絡をお願いいたします。  
ご契約ドメイン名を確認させていただきましてからの対応となります。

## 24時間 365日 TEL & メールサポートのサポート範囲について

- コントロールパネル、マイページに関するお問い合わせ
- メールソフト、FTPクライアントの設定情報
- サービス仕様に関するお問い合わせ
- 障害・不具合に関するお問い合わせ

※内容によってはメールでお問い合わせをお願いする場合があります。

## ご注意

- 障害発生時は復旧作業を優先させていただくため、対応にお時間がかかる場合があります。
- ご契約やお支払いに関するお問い合わせは、翌営業日の対応となります。
- 調査や設定変更などの技術的なご依頼については、翌営業日の対応となる場合や対応できない場合があります。



# .htaccess の設定方法

---

ここでは、サーバーをご利用いただく際のヒントとして、よく利用される .htaccess の一般的な内容の一部のみを掲載しております。

他の運用方法もありますが、ウェブ構築関連の書籍やサイト等でご確認のうえ、設定してみてください。

.htaccess はウェブサーバーに対する制御を行うためのファイルです。

編集はテキストエディタ等で行っていただき、ファイル名を「.htaccess」（拡張子なし）で「html」以下の設定を適用させたいディレクトリにアップロードしていただくことで反映されます。

記述内容によっては、アクセスできなくなったり、サーバーに負荷がかかってしまう場合もございますので、作業時には記述内容や設定内容はお客様の自己責任の下、設定内容に十分ご注意ください。

ここに記載している内容は、一般的な設定内容となり、お客様のコンテンツにも依存することがございますため、技術サポート対象外となっております。

## ❗ 重要

.htaccess の各行の途中に「#」でコメントアウトするとエラーになります。  
コメントアウトされる場合は、行を分けて記述してください。

## 目次

- 🔍 シンボリックリンクを有効化する場合  
mod\_rewrite を利用する場合
- 🔍 リダイレクト（転送）設定する
- 🔍 表示順序の変更
- 🔍 エラーページの表示設定
- 🔍 アクセスを制御（拒否／許可）する
- 🔍 MIME タイプを定義する
- 🔍 SSI を「.shtml」の拡張子ではなく、「.html」で利用する方法

## シンボリックリンクを有効化する場合 mod\_rewrite を利用する場合

.htaccess ファイルに以下の記述をしますと、ご利用いただけます。

なお、シンボリックリンクのリンク元ファイルとリンク先ファイルが、お客様領域（同一ユーザー ID）内にあることが条件となります。

```
Options +SymLinksIfOwnerMatch  
RewriteEngine On
```

※上記のように必ず「+」記号をつけてください。

## リダイレクト（転送）設定する

サーバーでリダイレクトを有効化するには、以下の2行の記述が必要となります。

```
Options +SymLinksIfOwnerMatch  
RewriteEngine On
```

※上記のように必ず「+」記号をつけてください。

### 例1：www なしで接続があった場合に www ありの URL にリダイレクトする

```
Options +SymLinksIfOwnerMatch  
RewriteEngine On  
RewriteCond %{HTTP_HOST} ^example%.jp  
RewriteRule (.*) http://www.example.jp/$1 [R=301,L]
```

※URL に続く数字は、301 リダイレクト：恒久的なリダイレクト、302 リダイレクト：一時的なリダイレクトという意味です。運用に応じてステータスコードを変更してください。

## 例 2：ホームページに対して、http（通常の 80 番ポート）で接続があった場合に、強制的に https（SSL の 443 番ポート）での接続に変更する

```
Options +SymLinksIfOwnerMatch
RewriteEngine On
RewriteCond %{SERVER_PORT} !^443$
RewriteRule ^(.*)?$ https://www.example.jp/$1 [L,R]
```

※契約プランによっては、独自 SSL をご契約いただいておりますと、SSL サーバー証明書はご利用いただけません。

上記例は、[www.example.jp] というコモンネームで SSL サーバー証明書を取得していることを前提とした説明です。

## 例 3：特定のディレクトリ（例：aaa）に対するアクセスを、別のディレクトリ（例：bbb）にリダイレクトする

```
Options +SymLinksIfOwnerMatch
RewriteEngine On
Redirect permanent /aaa/ http://www.example.jp/bbb/
```

## 例 4：転送元に対するアクセスを、すべて転送先のトップページにリダイレクトする

```
Options +SymLinksIfOwnerMatch
RewriteEngine On
RedirectMatch 301 .* http://www.example.jp/
```

## 例 5：携帯電話の振り分け設定

```
Options +SymLinksIfOwnerMatch
RewriteEngine On

# docomo
RewriteCond %{HTTP_USER_AGENT} DoCoMo
RewriteRule ^$ http://example.jp/i/index.html [R]

# SoftBank
RewriteCond %{HTTP_USER_AGENT} SoftBank
RewriteRule ^$ http://example.jp/s/index.html [R]

# au
RewriteCond %{HTTP_USER_AGENT} UP.Browser
RewriteRule ^$ http://example.jp/au/index.html [R]

# Android
RewriteCond %{HTTP_USER_AGENT} Android
RewriteRule ^$ http://example.jp/android/index.html [R]

# iPhone
RewriteCond %{HTTP_USER_AGENT} iPhone
RewriteRule ^$ http://example.jp/iphone/index.html [R]

# iPad
RewriteCond %{HTTP_USER_AGENT} iPad
RewriteRule ^$ http://example.jp/ipad/index.html [R]
```

※.htaccess では、各モバイル機器ごとの振り分けルールのみ設定します。  
振り分け先のコンテンツについては、別途ご用意ください。

## 表示順序の変更

index から始まるファイルについて、サーバーでの優先順位（読み込み順）は、以下の通りです。（上から優先順位の高い順）

- ①index.html
- ②index.shtml
- ③index.cgi
- ④index.html
- ⑤index.htm
- ⑥index.php

### 例：index ファイルの読み込み順を変更する

※DirectoryIndex の後に、表示させる順で記述してください。

以下の設定例の場合、index.html よりも先に index.cgi を探して表示します。

```
# index ファイルの読み込み順の変更
DirectoryIndex index.cgi index.html
```

## エラーページの表示設定

エラーページは独自のページを用意することが可能です。

### 例：独自のエラーページを作成して、エラー時に表示する

```
# エラーコード401: Authorization Required (認証失敗)
ErrorDocument 401 /error/401.html
```

※ローカル URL (=自サイト内の絶対パスで表現されるもの) である必要があります。

または

```
ErrorDocument 401 '<html><head><meta http-equiv="Refresh" content="0;url=http://example.jp/error/401.html">
</head></html>'

# エラーコード403: Forbidden (閲覧権限が無い)
ErrorDocument 403 /error/403.html

# エラーコード404: Not Found (ページが見つかりません)
ErrorDocument 404 /error/404.html

# エラーコード500: Internal Server Error (サーバ内部エラー)
ErrorDocument 500 /error/500.html
```

※URL は表示させたいエラーページのアドレスに置き換えてください。

※上記の例は、エラーページのファイルをドキュメントルート (html) 直下に「error」という名前のディレクトリ配下に置いている場合です。

※.htaccess ファイルは、ドキュメントルート (html) 直下に置いてください。

※アクセス集中を表す 503 エラー (Service Temporarily Unavailable) につきましては、サーバー側で制御しているため、お客様にて変更いただけません。ご了承ください。

## アクセスを制御（拒否／許可）する

HP へのアクセスを制御する場合は、1 行目に優先順位を指定する必要があります。  
通常、以下のように設定します。

- 一部のアクセス元のみを拒否する場合 → 許可を優先
- 一部のアクセス元のみを許可する場合 → 拒否を優先

### 例 1：IP アドレス（192.0.2.1）からの接続のみを許可する

```
# IP アドレス（192.0.2.1）からの接続のみを許可する場合
order deny,allow
deny from all
allow from 192.0.2.1
```

※IP アドレス（192.0.2.1）は、設定したい IP アドレスに置き換えてください。

### 例 2：IP アドレス（192.0.2.1）からの接続以外を許可する

```
# IP アドレス（192.0.2.1）からの接続以外を許可する場合
order allow,deny
allow from all
deny from 192.0.2.1
```

※IP アドレス（192.0.2.1）は、設定したい IP アドレスに置き換えてください。

## MIME タイプを定義する

サーバーにアップロードしたファイルの扱い方を定義します。

### 例 1：PHP 以外の拡張子を PHP として処理する

```
# .htm や .html ファイルを拡張子のままではなく、 php として処理
AddHandler x-httpd-php528 .htm .html
```

※AddType による設定はご利用いただけません。

### 例 2：サーバーでデフォルト MIME タイプとして定義されていない MIME タイプを追加する

```
# pdf ファイルと jpeg ファイルをMIMEタイプとして定義
AddType application/pdf .pdf
AddType image/jpeg .jpeg
```

※上記は設定例です。

実際には定義する必要がない場合や、定義してもサーバーの仕様上、ご利用いただけない MIME タイプもありますが、設定ファイルの詳細は案内していないため、設定のうえお試しください。

## SSI を「.shtml」の拡張子ではなく、「.html」で利用する方法

.htaccess ファイルに以下の記述をしますと、ご利用いただけます。

```
AddOutputFilter INCLUDES .html
```



# .htaccess とは

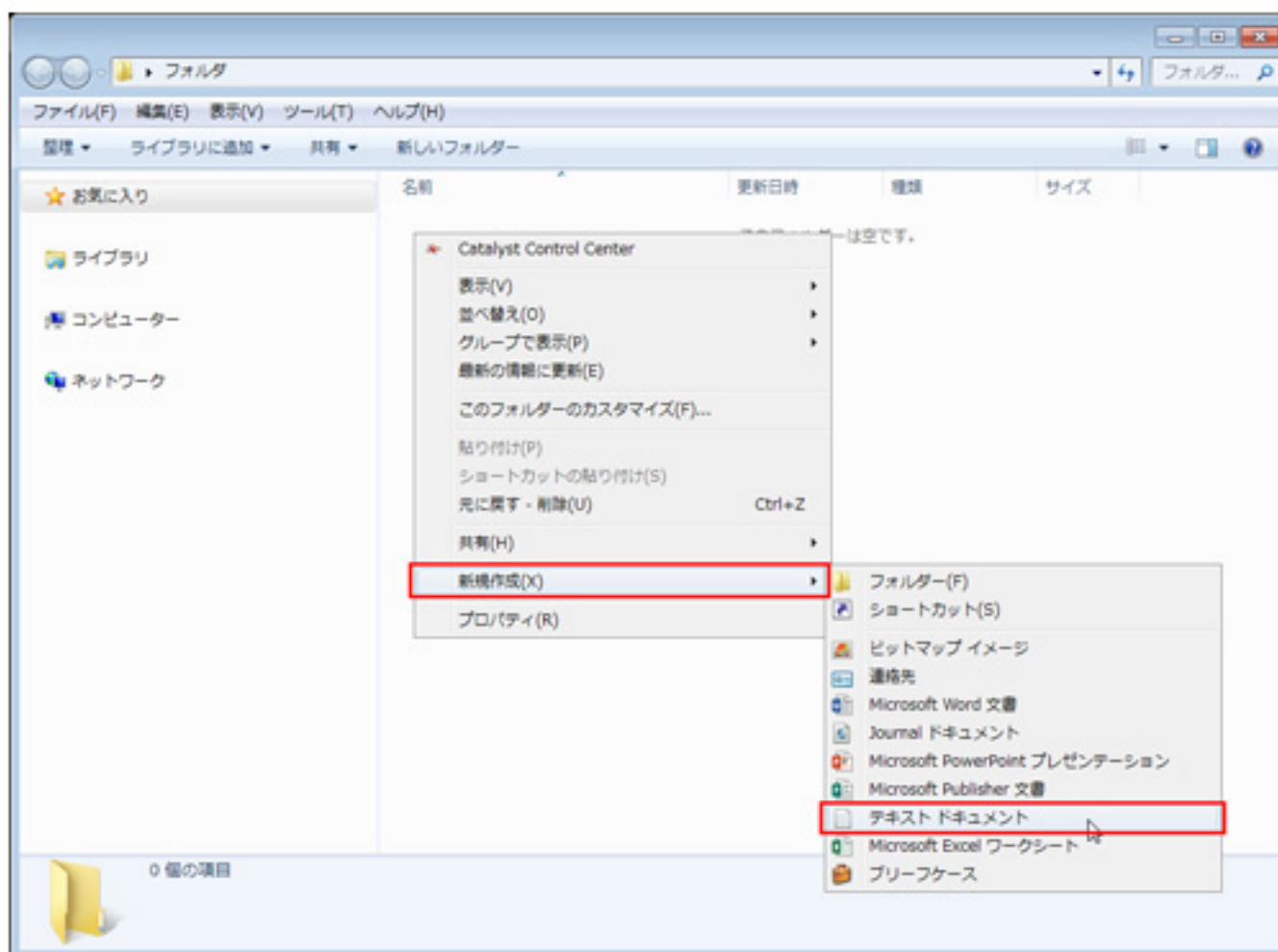
htaccess を利用すると、ウェブサーバーの設定を変更することができ、アクセス制限、ユーザーの認証 (ユーザー名とパスワードを入力)、リダイレクトなどが利用できます。

.htaccess ファイルはテキスト形式のファイルであり、FTP ソフトなどでご利用のサーバーにアップロードして利用します。

## .htaccess の作成方法

本ページでは、php5.2.8 の PHP 情報 (phpinfo) をウェブ表示させる方法を例にご説明します

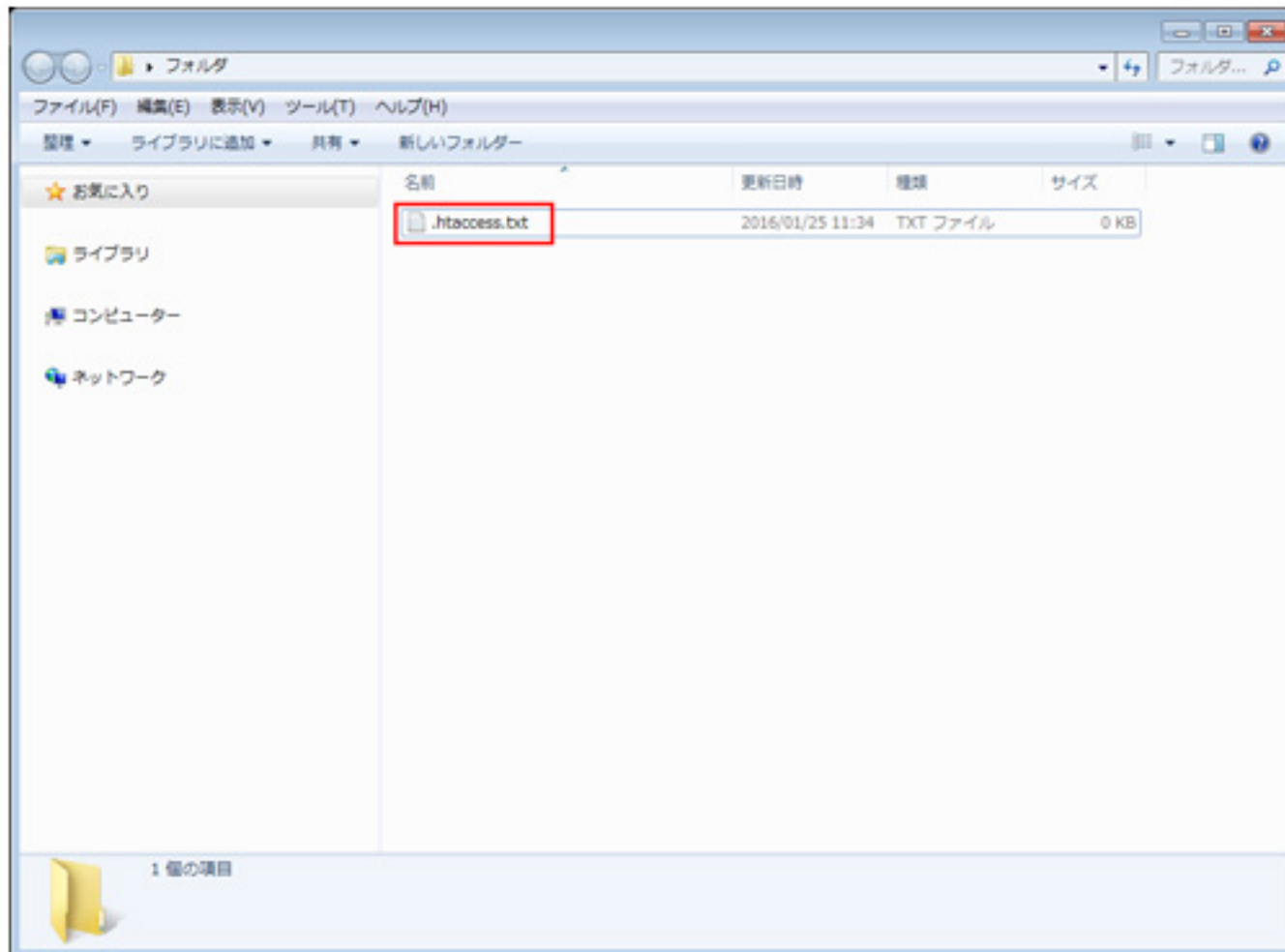
### 1 Windows 上でテキストファイルを新規作成します。



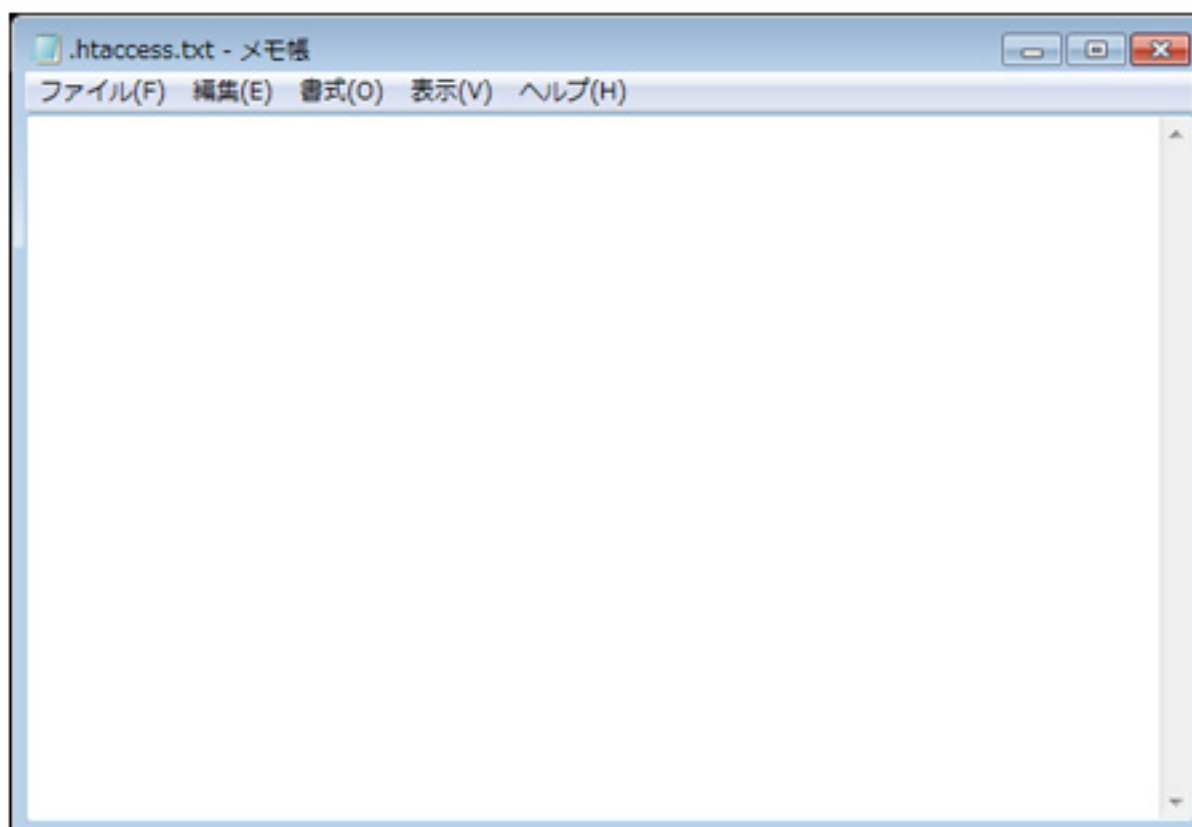
## 2 テキストファイルのファイル名を【.htaccess.txt】と入力して保存します。

※ご利用の環境によっては、ファイル名の先頭にドットが存在するとファイルが保存できない場合がございます。

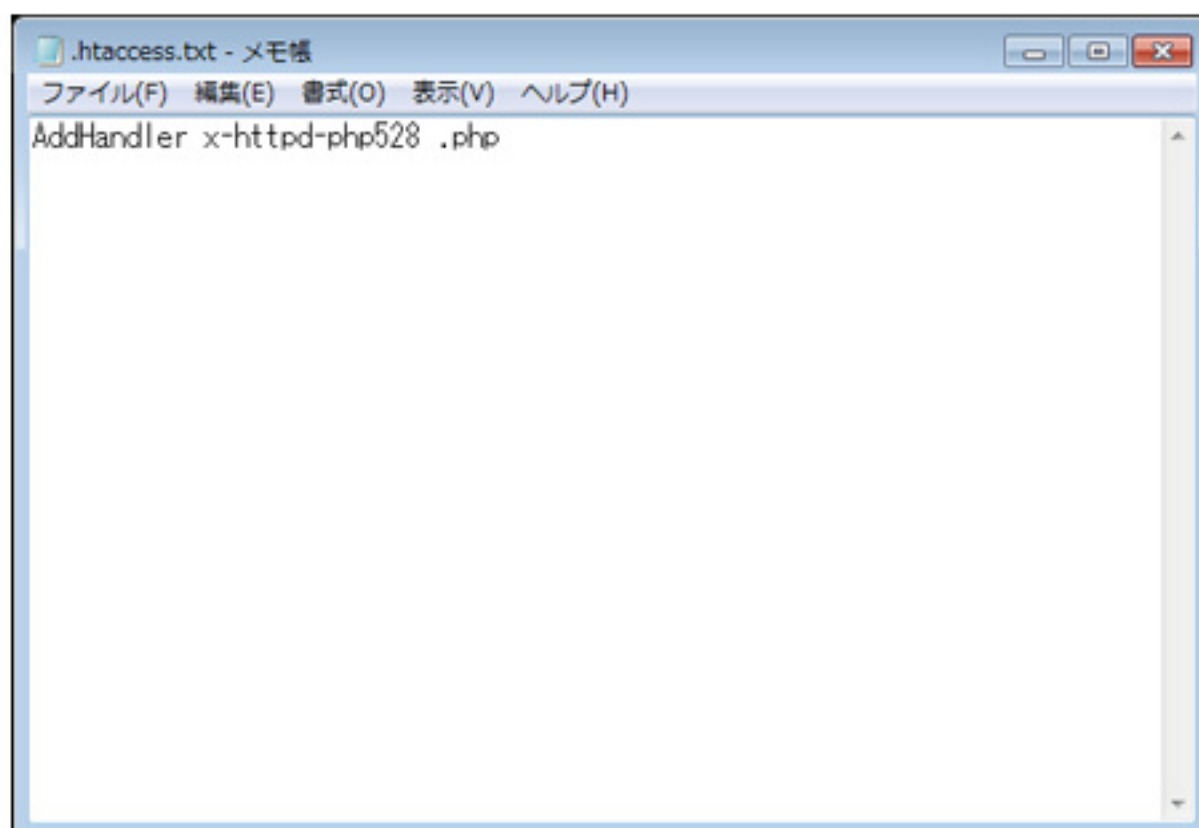
※ファイルの拡張子が表示されない場合は、Windowsのエクスプローラーの「ツール」 - 「フォルダオプション」 - 「表示」タブ - 「詳細設定」 - 「登録されている拡張子は表示しない」のチェックをはずしてください。



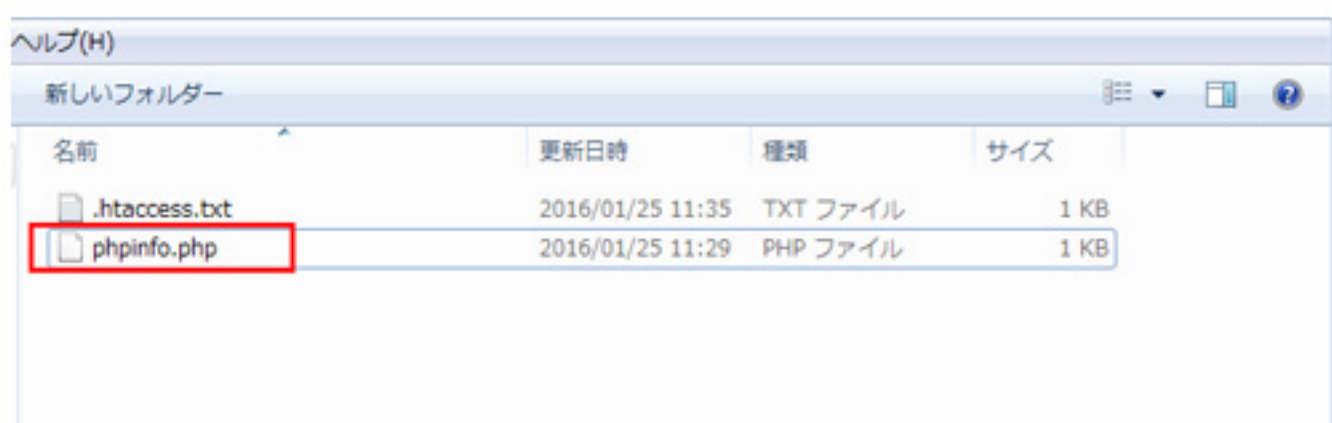
## 3 作成したテキストファイルを、テキストエディタで開きます。例では Windows のメモ帳を利用します。



- 4 テキストファイルの1行目に、「AddHandler x-httpd-php528 .php」と入力し、改行をしてファイルを保存します。



- 5 PHPの実行のテスト用に、サンプルプログラムを作成します。ファイル名は【phpinfo.php】とします。

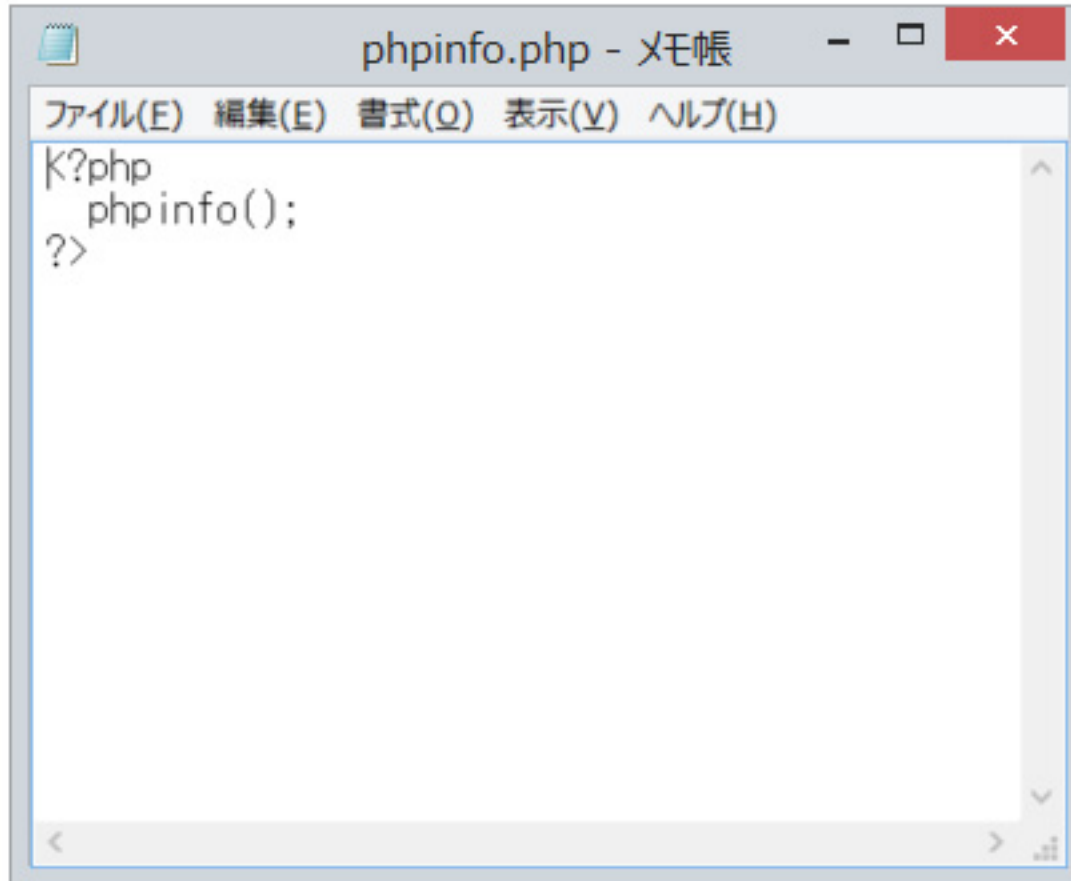


## 6 phpinfo.php ファイルをメモ帳で開きます。

下記のように

```
<?php  
phpinfo();  
?>
```

と入力してファイルを保存します。



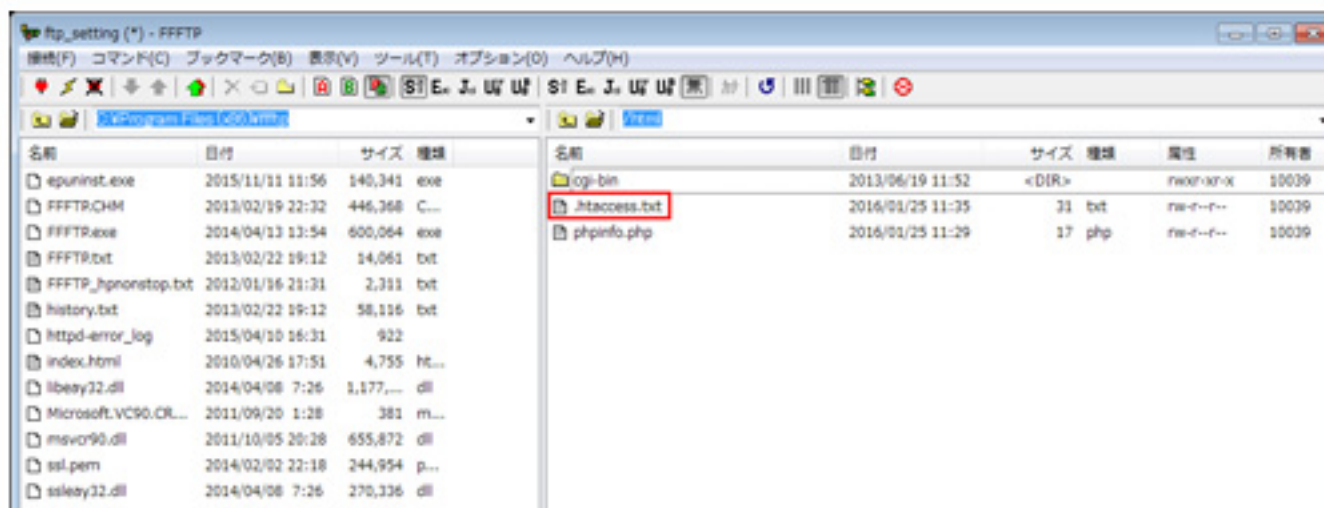
## 7 FTP ソフトを利用して、ファイルをサーバーへアップロードします。

例では、html ディレクトリ内に作成した

.htaccess.txt

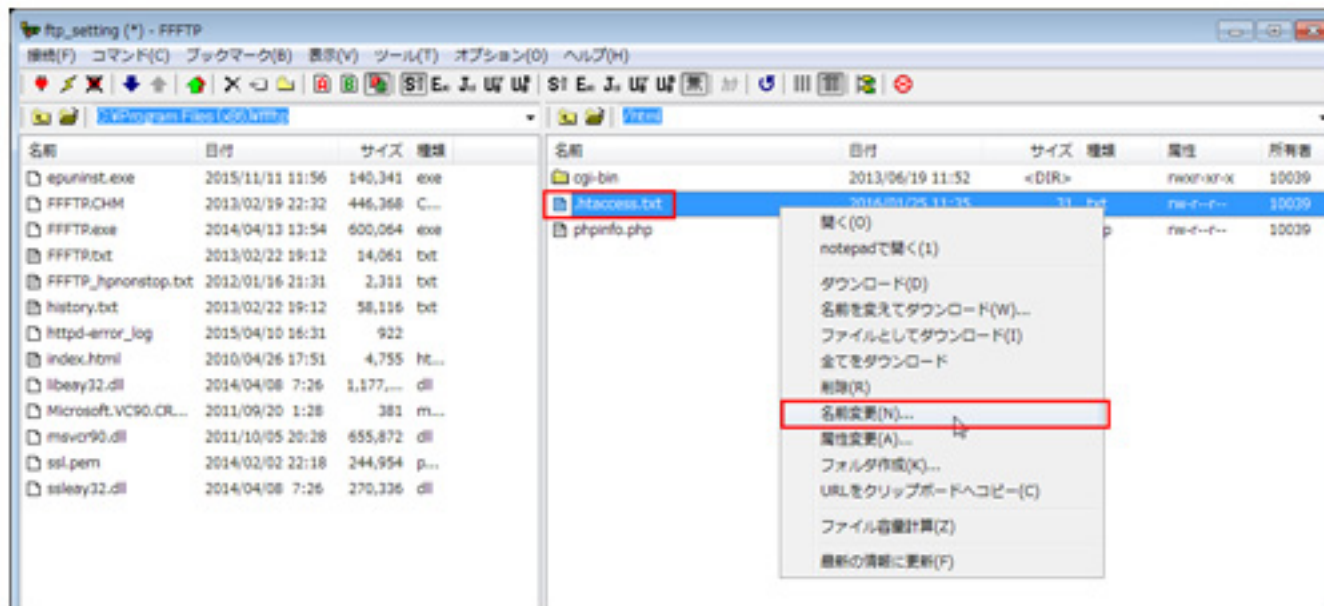
phpinfo.php

の2ファイルをアップロードしました。



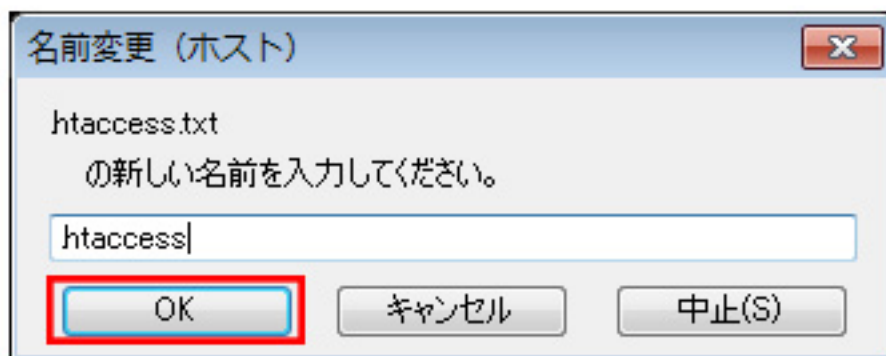
8

.htaccess.txt ファイルをマウスで選択し、「名前変更」をクリックします。



9

ファイル名を .htaccess へ変更して OK ボタンをクリックします。



10

ブラウザで PHP プログラムのファイルにアクセスすると、PHP のプログラムが動作して、phpinfo() の実行結果が表示されます。

PHP Version 5.2.8	
System	FreeBSD z105secure.ne.jp 5.4-RELEASE FreeBSD 5.4-RELEASE #0: Thu Apr 8 20:28:58 JST 2010 root@z105secure.ne.jp:/usr/src/sys/0805/compile/CP1.085
Build Date	Apr 8 2010 22:45:31
Configure Command	./configure '--disable-debug' '--disable-pv' '--enable-calendar' '--enable-cli' '--enable-discard-path' '--enable-evil' '--enable-ftp' '--enable-gd-jis-compat' '--enable-gd-native-ttf' '--enable-mbregex' '--enable-mbstring' '--enable-soap' '--enable-sockets' '--enable-zend-multibyte' '--enable-zip' '--with-bz2' '--with-config-file-path=/usr/local/etc/php.conf.5.2.8' '--with-curl' '--with-freetype-dir=/usr/local/lib' '--with-gd' '--with-gettext' '--with-iconv=/usr/local/include' '--with-imap-ssl' '--with-imap=/usr/local/lib' '--with-jpeg-dir=/usr/local/lib' '--with-libxml-dir' '--with-mcrypt' '--with-mhash' '--with-mysql=/usr/local/mysql' '--with-mysqli=/usr/local/mysql/bin/mysql_config' '--with-openssl' '--with-pdo-mysql=/usr/local/mysql' '--with-pdo-pgsql=/usr/local' '--with-pdo-sqlite' '--with-pgsql=/usr/local' '--with-png-dir=/usr/local/lib' '--with-popt' '--with-xmllib' '--with-xsl' '--with-zlib' '--without-pear' '--prefix=/usr/local'
Server API	CGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php.conf.5.2.8
Loaded Configuration File	/usr/local/etc/php.conf.5.2.8/php.ini
Scan this dir for additional ini files	(none)
additional ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	22060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	disabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, sslv2.3ls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.conv.*, bzip2.*, zlib.*

# 日本語ドメイン

---

## 日本語ドメインのご利用について

ドメインをご利用するにあたっての注意事項や制限事項について説明します。

CPI ではドメインを ASCII 文字（半角の英数字や「-」ハイフンなどの文字）に変換した Punycode (ピュニコード) を利用してご提供いたします。

お申込みやお問い合わせの際は、Punycode をご用意ください。

Punycode は始めや途中に「xn--」という文字列があります。

例

ドメイン名例.jp ⇔ xn--eckwd4c7cu47r2wf.jp

参考：

Punycode について

<http://jprs.jp/glossary/index.php?ID=0051>

日本語ドメイン名を Punycode に変換するためのサイト

<http://punycode.jp/>

## ドメインで実現可能な事項

日本語ドメインでウェブサイトを公開することができます(URL： <http://<ドメイン名>/>)

## 制限事項

ドメインの取得代行および管理維持は行っておりません

ドメインではメールサービスをご利用いただけません。

CPI サービスにおいては日本語ドメインを Punycode で管理をしております。そのため、各機能のドメイン表記は Punycode となります。

FTP 接続時もドメインをご利用可能ですが、FTP クライアントソフトによって、ドメインへの対応状況が異なりますのでご注意ください。

SSL サーバー証明書はご利用いただけません。そのため、`https://<ドメイン名>/` のような URL はご利用いただけません。

Get a File (ファイル転送サービス) はご利用いただけません。

日本語ドメインは種類を問いませんが、トップレベルドメインが日本語の場合はご利用いただけません。

## お問い合わせの際は Punycode をお知らせください

弊社ではドメイン名を Punycode で取り扱います。

レンタルサーバーのお申込みやお問い合わせいただく場合は、お客様のドメイン名を ASCII 表現に変換した Punycode をご用意ください。

## ドメイン名でご利用可能なソフトウェア

下記情報は参考情報となり、すべての動作を保証するものではありません。オペレーティングシステムや、クライアントソフト、ご利用のPC環境により動作が異なる可能性がございますのでご注意ください。

### 【FTP クライアント】

オペレーティングシステム	FTPクライアント	バージョン	接続先への入力設定値		
			IPアドレス	ftp.punycode (ピュニコード)	ftp. 日本語ドメイン名
Windows 7	FFFTP	1.98g	○	○	○
	NextFTP	4.94.02	○	○	○
	filezilla	3.11.0.1	○	○	○
	Cyberduck	4.7	○	○	×
	WinSCP	5.1.7	○	○	×
MacOS 10.6.8	fetch	5.6	○	○	×
	filezilla	3.8.1	○	○	×
	Cyberduck	4.6.5	○	○	×
MacOS 10.9.2	filezilla	3.10.3	○	○	○



## 【SFTP】

オペレーティングシステム	SFTP クライアント	バージョン	接続先への入力設定値		
			IP アドレス	punycode	日本語ドメイン
Windows 7	WinSCP	5.1.7	○	○	×
	filezilla	3.11.0.1	○	○	×
	Cyberduck	4.7	○	○	×
MacOS 10.6.8	filezilla	3.8.1	○	○	×
	Cyberduck	4.6.5	○	○	×
MacOS 10.9.2	filezilla	3.10.3	○	○	×

## 【WebDAV】

オペレーティングシステム	WebDAV クライアント	バージョン	URL への入力値	
			punycode	日本語ドメイン
Windows 7	teamfile	2.1.141.1421	○	×
	cyberduck	4.7	○	×
	carotdav	1.11.15	○	×
MacOS 10.6.8	MacOS 標準機能	サーバーへ接続	○	×

## CHM-0Z と CHM-1Z のサーバー環境の確認方法

---

お客さまのご利用されているサーバープランのご確認方法です。

	CHM-11Z	CHM-01Z
ウェブサーバー名 (主契約サーバー)	faXXXX.secure.jp	chzXXXX.secure.jp
ご提供開始	2017年11月15日(水) 15時以降	2017年11月15日(火)15時以前 新規のお申込み受け付けは終了いたしました。

## 確認方法

サーバー名はコントロールパネルにて確認することができます。



The screenshot shows the 'Control Panel' interface for a server. The URL is 'fd1953001.secure.jp'. The main content area is divided into 'Information' and 'Category' sections. The 'Information' section includes a list of recent updates and a 'Shortcuts Menu' with a 'Home' button. The 'Category' section lists various management tools like 'お告知情報', 'メール', 'FTP/ファイル管理', '制作ツール', 'ソフトウェア', 'ログ管理', 'サポート', and '機能一覧'. On the right side, there is a 'お客様のご利用状況' (Customer Usage Status) section with a red box highlighting the following information:

プラン名	マナーサポートプラン CHM-11Z
サーバ名	N195240001.jp
IPアドレス	211.3.134.41

Below this, there is a 'ディスク使用状況' (Disk Usage Status) section with a pie chart showing the usage of 'ウェブ' (13,065MB), 'メール' (13,759MB), and 'データベース' (18,008MB).

プラン名 [ ]  
サーバ名 [ ] secure.jp  
IPアドレス [ ]

こちらでサーバー名をご確認いただけます。

CHM-Zは2017年11月15日(水)の機能強化に伴い、お申込みの時期により提供されるサーバーの機能や仕様が変更となりました。

CHM-Zのオンラインヘルプでは、CHM-01Z、CHM-11Zの両方のサーバー環境の説明を記載しております。お客様がご利用のサーバー環境がどちらであるかをご確認するにあたり、上記表を参考にしてください。