Z-PROXY Server V2
ユーザーズガイド

（第 2.05 版）

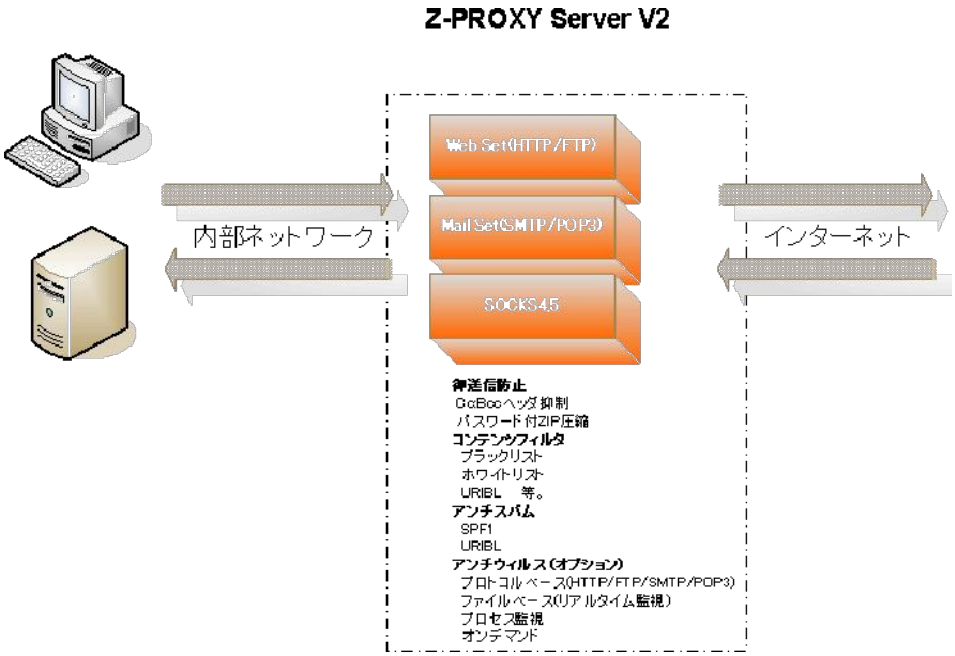
注意） 本マニュアルは、お買い上げいただいた製品をお使いになるコンピュータにインストールする方法や、「Z-PROXY Server」の各設定について説明をしています。本マニュアルに掲載されていない「Z-PROXY Server」の機能については、オンラインヘルプおよびインターネットサイトを、ご参照ください。

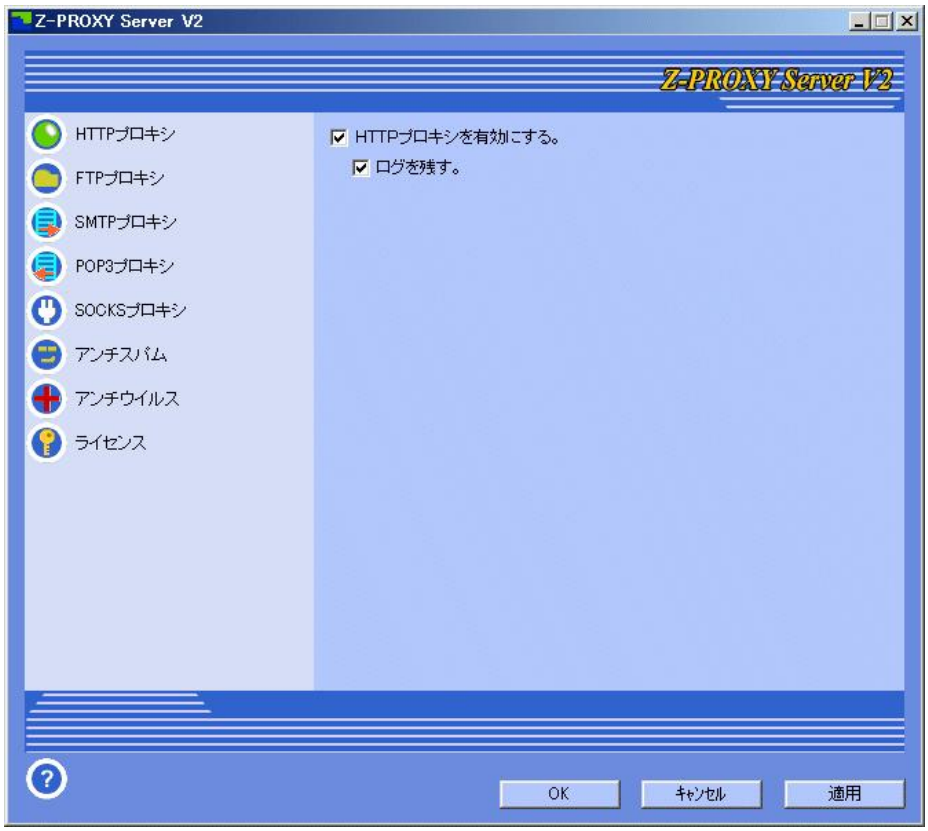
本ガイドをお読みになる前に

本ガイドをお読みになる前に、お使いのコンピュータで「Windows 2000 Server」/「Windows Server 2003(SBS2003)」/「Windows Server 2008」 のいずれかが正常に動作し、TCP/IP プロトコルが正しく機能していることをご確認ください。

「Z-PROXY Server V2」について

「Z-PROXY Server V2」は、Web/Mail/SOCKS4,5 プロキシ環境を構築する為のソフトウエアです。
プロキシ環境を構築することにより、メール誤送信対策対や、「プライバシーマーク」取得時に必要な、アクセスログ取得環境の構築、未成年向けのコンテンツフィルタサーバ、などにご利用いただけます。
導入コストやランニングコスト削減にも貢献可能なソフトウエアです。





[主な機能]

[コンテンツフィルタ機能]

HTTP 監視

付属する禁止ワード・ブラックリスト・ホワイトリストによる管理や、PICS（セルフレイティング）・未成年向け検索サイトへの参照URL問合せ・SURBL 問合せ先設定によるブロック機能を搭載したコンテンツフィルタとして危険なサイトのアクセスから利用者を守ります。

[アンチスパム機能]

SMTP 監視

付属するURIBL問合せ、キーワード一致、送信ドメイン認証（SPF1）等で通過時のメールのスパム判定を行うSMTPプロキシとして機能し、スパム判定されたメールには題名へのタグ挿入を行えます。

また、設定により暗号化された通信（SMTP Over SSL/TLS, STARTTLS）での送信メールを本プロキシサーバ内で解析判定が可能です。**※1**

POP3 監視

付属する URIBL 問合せ先設定で各ユーザ毎のメール受信時にスパム判定を行う POP3 プロキシとして機能し、スパム判定されたメールには題名へのタグ挿入を行えます。

また、設定により暗号化された通信（SMTP Over SSL/TLS, STARTTLS）での送信メールを本プロキシサーバ内で解析判定が可能です。**※1**

[プロキシ機能]

HTTP プロキシ

任意のアドレス:ポートで接続可能な HTTP プロキシサーバとして機能します。

上流にあるプロキシへのフォワード設定も可能で、特定の HTTP サーバアドレスとポートを指定することで「リバース・プロキシ」として WEB 本体側の改ざんリスク軽減や負荷分散が行えます。

プロキシ接続時の認証機能（Basic 認証）にて利用者毎の認証ID・パスワード設定が可能です。

認証情報の参照は、LDAP サーバまたは、独自のアカウント登録のいづれかを選択可能です。

FTP プロキシ

任意のアドレス:ポートに接続可能な SMTP プロキシサーバとして機能します。

アクティブモード、パッシブモード及び、FTP over HTTP(ブラウザ使用時)通信に対応しています。

SMTP/POP3 プロキシ

任意のアドレス:ポートに接続可能な SMTP/POP3 プロキシサーバとして機能します。

設定によりクライアント・プロキシ間のプレーン通信をプロキシ・サーバ間では暗号化通信（SMTP/POP3 Over SSL/TLS, STARTTLS）への変換や、クライアント・プロキシ間での暗号化通信（SMTP/POP3 Over SSL/TLS, STARTTLS）をプロキシ・サーバ間ではプレーン通信への変換が可能です。**※1**

SOCKS プロキシ （Full Set ライセンス時）

任意のアドレス:ポートに接続可能な SOCKS プロキシサーバとして機能します。

[メールアーカイブ機能]

SMTP プロキシ型アーカイブ機能

SMTPプロキシとして既存のメールサーバの前段に設置することで、暗号化通信でない通過メールを任意の指定フォルダ内に日単位のMailDIR形式で保管し、「情報漏えい」に備えたメールアーカイブとしてメール保管し監査時に利用することが可能です。

暗号化された通信（SMTP Over SSL/TLS, STARTTLS）についても設定により通過メールの保管が可能です。**※1**

保管されたメールは、別売のKSearch等、MailDIR 形式を検索可能なソフトを使って、監査時の検索、閲覧が可能になります。

[メール誤送信対策]

SMTP プロキシ型アーカイブ機能

SMTP プロキシとして既存のメールサーバの前段に設置することで、リッスン IP:ポート単位の指定により添付付メールを自動暗号化（パスワード付 ZIP 圧縮）し送信することが可能です。

[アンチウイルス機能] ※アンチスパムオプションをインストール時のみ

オンデマンド・ウイルススキャン機能

スキャンさせたいドライブ、フォルダ、ファイルに対し「デスクトップ上のアイコンへドラッグ＆ドロップ」を行うか、「マウスの右ボタンクリックで表示されるメニュー」にてウイルススキャンの実行が行えます。

実行中のプロセス監視機能

実行中のプロセス（プログラム）及び、スタートアップ用レジストリ、フォルダに登録されたプログラムについて定期的にウイルスチェックによる監視を行えま

す。

リアルタイム監視機能

指定したドライブやフォルダへのファイル書込み、変更状態を検出し対象となるファイルについてウイルスチェックによる監視を行えます。
USB メモリを対象ドライブとして監視することも可能です。

HTTP 監視 (Web Set 又は Full Set ライセンス時)

任意のアドレス:ポートで接続可能な HTTP プロキシサーバとして機能し、アクセス対象の各データについてウイルスチェックによる監視を行えます。
使用ブラウザには、HTTP プロキシサーバ経由での接続設定を行う必要があります。

FTP 監視 (Web Set 又は Full Set ライセンス時)

任意のアドレス:ポートで接続可能な FTP プロキシサーバとして機能し、アクセス対象の各データについてウイルスチェックによる監視を行えます。
使用クライアントには、FTP プロキシサーバ経由での接続設定を行う必要があります。

SMTP 監視 (Mail Set 又は Full Set ライセンス時)

任意のアドレス:ポートに接続可能な SMTP プロキシサーバとして機能し、送信メールについてウイルスチェックによる監視を行えます。
設定により暗号化された通信(SMTP Over SSL/TLS, STARTTLS)での送信メールを本プロキシサーバ内で解析判定が可能です。※1
使用クライアントには、SMTP プロキシサーバ経由での送信設定を行う必要があります。

POP3 監視 (Mail Set 又は Full Set ライセンス時)

任意のアドレス:ポートに接続可能な POP3 プロキシサーバとして機能し、受信メールについてウイルスチェックによる監視を行えます。
設定により暗号化された通信(POP3 Over SSL/TLS, STARTTLS)での受信メールを本プロキシサーバ内で解析判定が可能です。※1
使用クライアントには、POP3 プロキシサーバ経由での送信設定を行う必要があります。

※1 本プロキシ内での SMTP/POP3 over SSL の解析及び実行は IPv4 アドレスのみ可能です。

ソフトウェア使用許諾契約書

重要:本ソフトウェアは、以下条項にご同意いただいた場合にのみご使用いただけます。
本ソフトウェアを使用された場合は下記条項にご同意いただけたものとさせていただきますので、下記条項を充分お読みの上ご使用ください。

本ソフトウエアは、著作権法および著作権に関する条約をはじめ、その他の無体財産権に関する法律ならびに条約によって保護されています。本ソフトウエアは許諾されるもので、販売されるものではありません。

本ソフトウェアについて

・本ソフトウェアは、株式会社ケイ･テックが著作権を有する Windows サーバ上でプロキシサーバ機能を実現するソフトウエア「Z-PROXY Server V2」等を搭載しています。
・株式会社ケイ･テックは、当社の著作権に基づき、お客様に対し、以下の条件の下、日本国内において本製品を使用することを許諾します。

使用許諾

・お客様がご利用される1台のサーバ OS 上のみで使用することを条件に、日本国内のみにおいて、本ソフトウェアを使用する権利をお客様に対して非排他的に許諾します。お客様のこの権利は一切譲渡できないものとします。
・お客様は、コンピュータのRAM等の一次メモリーに本ソフトウェアを読み出す場合、あるいはコンピュータのハードディスク等の固定メモリーに組み込む場合のいずれであっても、使用権の許諾が必要な「使用」とみなされ、そのメモリーを有するサーバ毎に使用許諾を受ける必要があります。
・お客様は、保存の目的に限り本ソフトウェアのコピーを一部作成すること、又はオリジナルをバックアップもしくは保存用にのみ保持して本ソフトウェアをハードディスクに組み込むことができます。

著作権

・本ソフトウェアは、株式会社ケイ・テックが著作権を有する製品であり、著作権及びその他の知的財産権に関する法律によって世界的に保護されています。
・お客様はこの使用許諾契約書に定める態様で本ソフトウェアを使用する権利を許諾されたに過ぎず、本ソフトウェアに関し、その他いかなる権利も明示的又は黙示的に付与されたわけではありません。
・お客様は、本ソフトウェア及びマニュアルを第三者へ賃貸、貸与、販売又は譲渡できないものとし、かつ、本ソフトウェア及びマニュアルに担保権を設定することはできないものとします。
・お客様は、本ソフトウェアについてリバース・エンジニア、逆コンパイル又は逆アセンブルできないものとします。

有効期間

・本契約はお客様が本ソフトウェアをコンピュータ・ハードディスクへ最初にインストールした時から有効になり、本契約の規定に従って解除される場合を除き、ライセンス及びサポートサービス証書記載のサポート終了日をもって終了するものとします。
・但し、お客様は、別途提示するライセンス及びサポートサービスの更新料を事前に支払うことにより本契約の有効期間を1年間延長できるものとし、以後も同様とします。

保証及び責任の限定

・本ソフトウェアのメディア及び本製品マニュアルに物理的瑕疵が発見された場合は、本契約の発効日から90日間に限り、当該メディア及びマニュアルを無料交換いたします。但し、交換したメディア、マニュアルに対しては、交換前の保証期間が適用されるものとします。
・前項に明示される場合を除き、本ソフトウェアもしくはマニュアル及びサポートサービスに関していかなる保証も行いません。
・本ソフトウェアもしくはマニュアルの機能及びサポートサービスがお客様の特定の目的に適合すること保証するものでなく、また、本ソフトウェア及びマニュアルの物理的な紛失･盗難･事故及び火災･地震･第三者による行為その他の事故、お客様の故意又は過失･誤用その他異常な条件下での使用に起因するお客様の損害、本ソフトウェアの不具合、本ソフトウェア又はマニュアルが第三者の権利を侵害しないことにつき、いかなる保証も致しません。
・お客様が期待する成果を得るための本ソフトウェアの選択導入はお客様の責任とさせて頂きます。
・お客様の改造改変に起因して本ソフトウェアに何らかの障害が生じた場合、該当障害に関しいかなる責任も負わないものとします。

・株式会社ケイ･テックはいかなる場合でも、お客様又は第三者に対し、特別・付随的又は派生的損害（逸失利益を含む）に関する責任を負わないものとします。
・本契約のもとで、理由の如何を問わず株式会社ケイ･テックがお客様又はその他第三者に対して負担する責任の総額は、本契約のもとでお客様が実際に支払われた対価を上限とします。

契約の解除

・株式会社ケイ･テックは原契約のいずれかが終了した場合は、有効期間の満了もしくは、別途書面にて指定する終了日をもって、本契約を解除することができるものとします。
・お客様が本契約に違反した場合、株式会社ケイ･テックは本契約を解除することができるものとします。この場合、お客様は、以後本ソフトウェア及びマニュアルを一切使用することができません。
・本契約が解除された場合、理由の如何を問わず、既に支払われた本ソフトウェアに関するライセンス対価は返還いたしません。
・本契約が終了するか又は解除された場合、お客様は、本ソフトウェア、マニュアル及びそのすべての複製物を返却するか又は破棄するものとします。

一般条項

・本契約は、日本国法に準拠するものとします。本契約に起因する紛争の解決については、東京地方裁判所を第一審の専属的合意管轄裁判所とします。
・お客様は、本ソフトウェア又はマニュアルを直接的、間接的を問わず、日本国、米国及びその他の国の全ての法律・規則（以下、輸出管理法という）に違反して輸出しないこと、また核兵器、化学兵器、生物兵器の拡散防止に関する規定を含む輸出管理法によって禁じられている用途で使用しないことを保証すると共に、それらの諸規制等を遵守しなくてはなりません。
・本契約は、本ソフトウェアの使用許諾に関し、本契約より前にお客様との間になされたすべての取り決めに優先して適用されます。

株式会社ケイ･テック

導入（インストール）

注意）

インストールの作業は、管理者権限のアカウントにログインして行って下さい。

使用しようとするIP,ポートを別のプログラムが使用中であったり、ファイアウォール設定などで塞がれていないことを確認してください。

Windows Vista/Windows Server 2008 への導入を行う場合。

Windows Vista/Windows Server 2008 では、Administrator アカウントであっても、User Account Control（UAC）が有効の場合、起動時に「管理者アカウントで起動」するようにしてください。

また、User Account Control（UAC）の解除することによっても、利用が可能です。

Windows Vista での User Account Control（UAC）の解除の方法。

1.Administrator 権限を持つアカウントでログインします。

2.コントロールパネル

→ クラッシック表示

→ ユーザアカウント

→ ユーザーアカウント制限の有効化または無効化

→ [ユーザーアカウント制御(UAC)を使ってコンピュータの保護に役立たせる]のチェックをはずします。

設定を行った後、再起動します。

3.再起動後、再び、Administrator 権限を持つアカウントでログインします。

1. ファイルをインストールする。

CDもしくは、ダウンロードした上記インストールプログラムを実行します。

インストールが開始されますと上記ダイアログが表示されますのでインストール先を指定してインストールを行います。

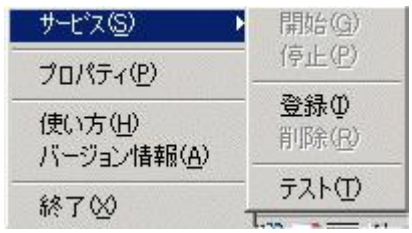
2. サービスプログラムのインストール。

インストールが完了するとデスクトップ上に設定アイコンが表示されるので、マウスでクリックし起動します。

タスクトレイにアイコンが常駐します。

タスクトレイ上のアイコンをマウスの右ボタンでクリックすると、メニューが表示されます。

サービス(P)



左ボタンでクリックすると、プロキシプログラムをサービスに登録・削除・開始・停止などを制御するメニューが表示されます。

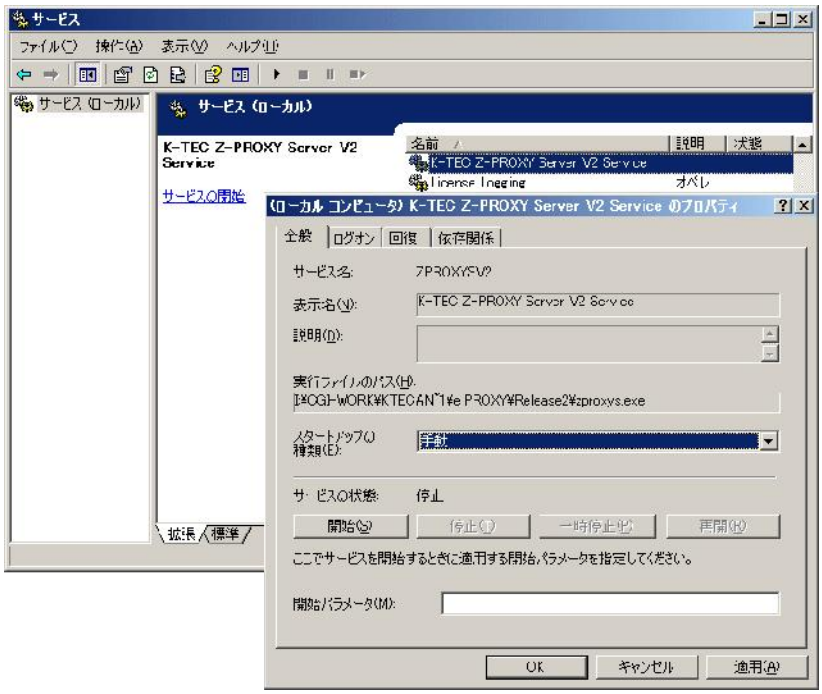
登録(I)

サービスの登録を行います。

クリックすると、登録された旨を示す TIPS 画面が表示されます。

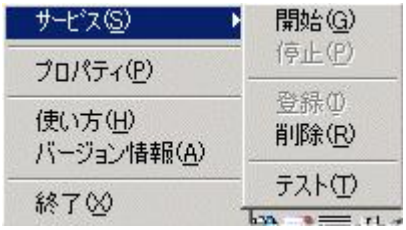
OS再起動時にプロキシプログラムが自動的に起動するため、サービス登録時に自動起動として登録が行われます。

OS再起動時に自動起動させたくない場合は、[管理ツール]の[サービス]から[K-TEC Z-PROXY Server V2 Service]のプロパティを開き[スタートアップの種類]を[手動]に変更してください。



開始(P)

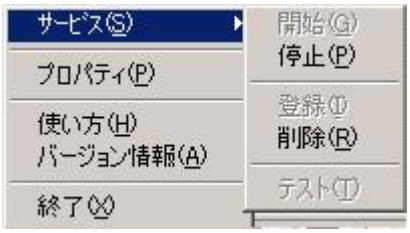
サービスの開始を行います。



クリックすると、サービスとして、プロキシプログラムが起動します。

停止(P)

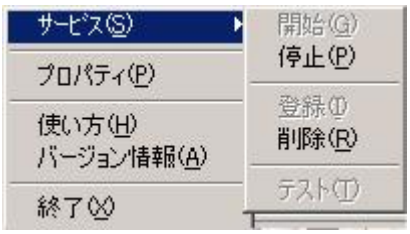
サービスの停止を行います。



クリックすると、サービスとして、プロキシプログラムが起動します。

削除(P)

サービスの削除を行います。



クリックすると、サービスから削除された旨を示す TIPS 画面が表示されます。

テスト(P)

サービスの登録後、サービスが停止状態で実行が可能です。

クリックすると、コマンドプロンプトからプロキシプログラムの起動を行い動作確認が行えます。

プロパティ(P)

左ボタンでクリックすると、監視対象を設定するダイアログが表示されます。

使い方(H)

左ボタンでクリックすると、このヘルプメニューが起動します。

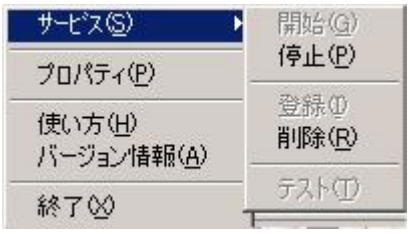
バージョン情報(A)

左ボタンでクリックすると、Z-PROXY Server V2 のバージョン情報が表示されます。

終了(X)

左ボタンでクリックすると、Z-PROXY Server V2 のタクストレイ常駐を終了します。

このとき、サービスとして起動している、プロキシプログラムは停止しません。



プロキシプログラムを停止するには、メニューの「サービス」から「停止」をクリックしてください。

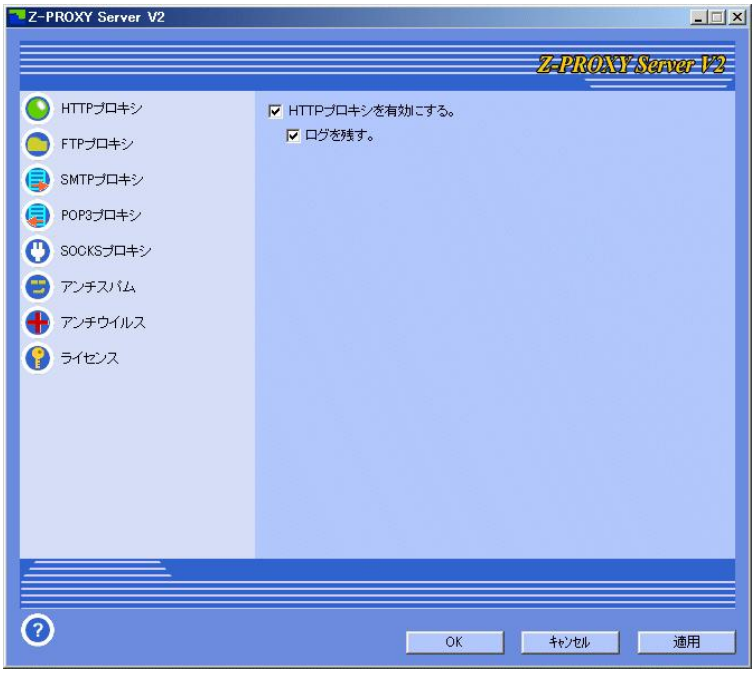
Z-PROXY Server V2 の操作

タスクトレイにアイコンが常駐しています。

タスクトレイ上のアイコンをマウスの右ボタンでクリックすると、メニューが表示されます。

表示されたメニューの「プロパティ(P)」を左ボタンでクリックすると、接続に必要な情報を設定するダイアログが表示されます。

表示されたダイアログの左側に表示されたメニューを選択すると、必要な設定内容が表示されます。



設定後[OK]ボタンを押し、サービスを再起動を行うことにより、変更された設定に従って監視処理が行われます。

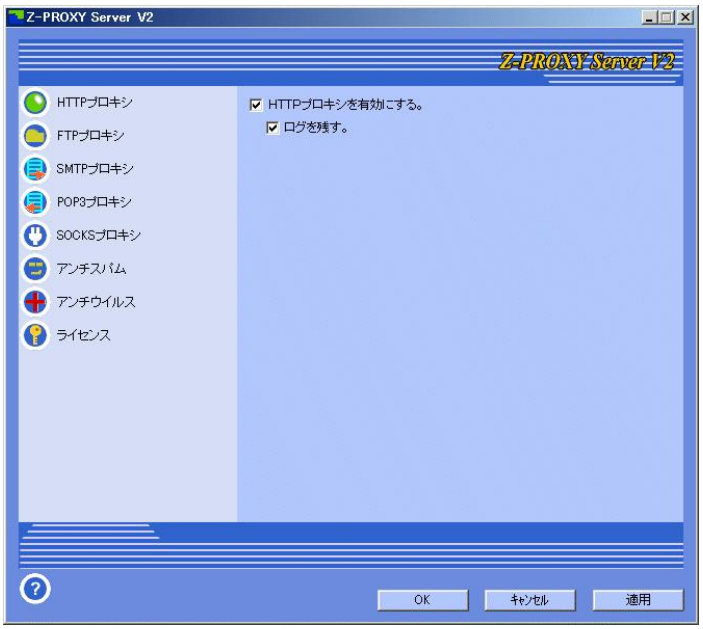
Z-PROXY Server V2 の設定

プロパティダイアログの起動

デスクトップに表示されたアイコン(Z-PROXY Server V2)を起動します。

タスクトレイ上のアイコンをマウスの右ボタンでクリックすると、メニューが表示されます。

表示されたメニューの「プロパティ(P)」を左ボタンでクリックすると、接続に必要な情報を設定するプロパティダイアログが表示されます。



HTTP プロキシ

HTTP プロキシサーバに関する設定を行う項目です。

FTP プロキシ

FTP プロキシサーバに関する設定を行う項目です。

SMTP プロキシ

SMTP プロキシサーバに関する設定を行う項目です。

POP3 プロキシ

POP3 プロキシサーバに関する設定を行う項目です。

SOCKS プロキシ

SOCKS プロキシサーバに関する設定を行う項目です。

アンチスパム

スパムチェックに関する設定を行う項目です。

アンチウイルス

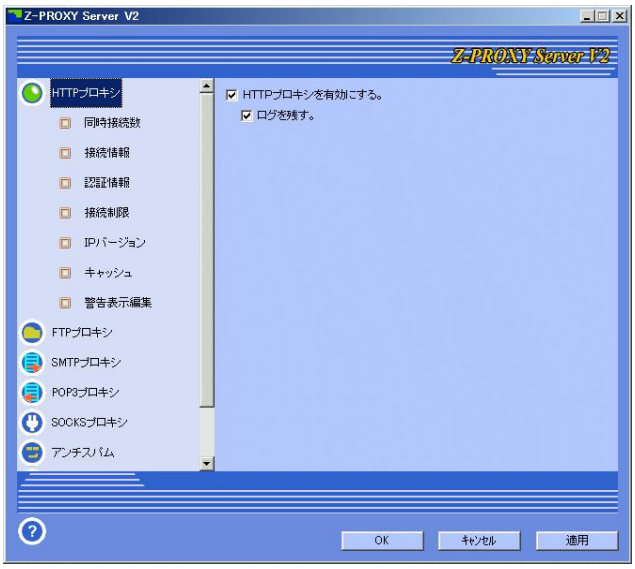
アンチウイルスに関する設定を行う項目です。

ライセンス

ライセンスの状態やライセンスキーの登録に関する設定ダイアログが開きます。

HTTPプロキシの設定

「HTTPプロキシ」をマウスでクリックすると、設定一覧が表示されます。



HTTP プロキシを有効にする。

チェックすると、任意のポートに設定した HTTP プロキシサーバ機能が利用可能になります。

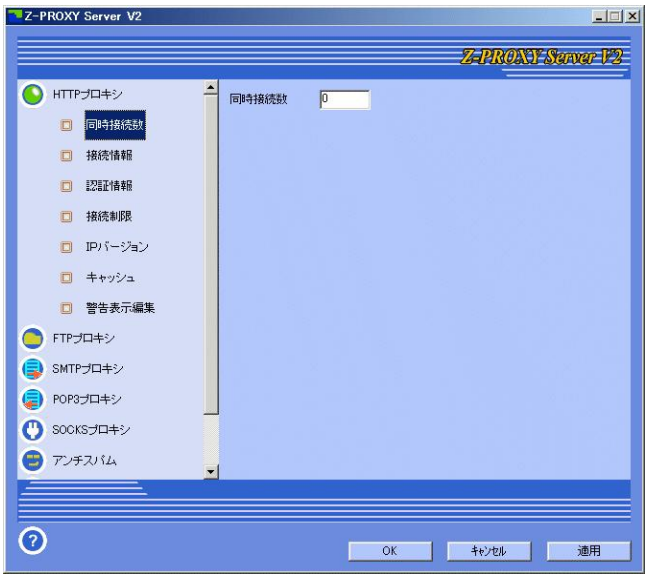
アンチウイルスオプションが追加インストールされている場合は、ウイルスチェックによる監視を行います。

https での通信時は、ウイルスチェックは行われません。

ログを残す

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

同時接続数



HTTP プロトコルセッションの同時処理数の上限を規定したい場合、1～65565の範囲で指定します。

0の場合は制限を行ないません。(デフォルト=0)

接続先情報

接続情報をクリックすると、接続ポートの設定を行う為のダイアログ画面が表示されます。

接続情報の登録

[接続情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

接続先名称

接続先の名称を記入する欄です。

受信 IP・ポート

HTTP プロキシへ接続できる IP アドレス欄(固定:LOCALHOST)とポート欄(変更可能)です。

上位プロキシ・ポート

上位の HTTP プロキシがありフォワードしたい場合、その IP アドレスとポートを指定します。

フォワードしない場合は、上位プロキシ欄を空欄とします。

また、特定の HTTP サーバアドレスとポートを指定することで「**リバース・プロキシ**」として WEB 本体側の改ざんリスク軽減や負荷分散として利用が可能です。

接続情報の削除

リスト上の削除したい HTTP 接続情報を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい HTTP 接続情報を選択し、キーボードの[Delete] キーにて削除が行えます。

認証情報

認証情報をクリックすると、この HTTP プロキシへ接続する際に必要な認証 ID とパスワードの設定を行う為の画面が表示されます。

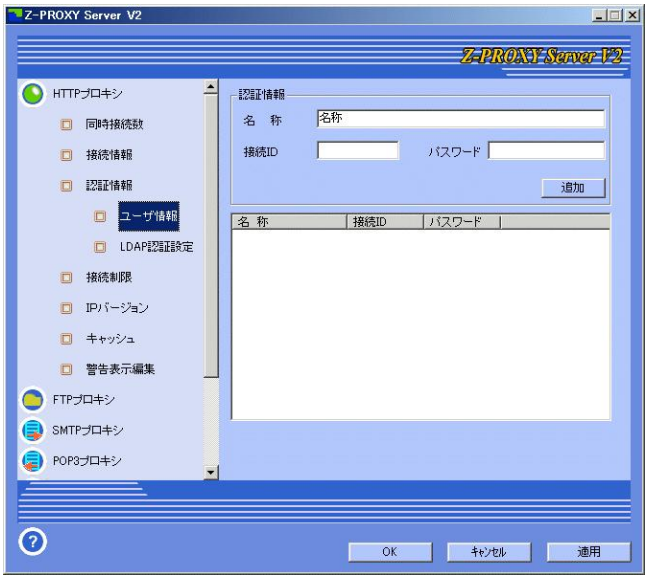
接続にはユーザ認証が必要

HTTP ブラウザの接続に HTTP 認証を必要としたい場合、チェックします。

利用するユーザ情報

Z-PROXY 内で独自管理するユーザ情報または、LDAP サーバ上のユーザ情報のどちらで利用するかを選択します。

ユーザ情報



Z-PROXY 内で独自管理するユーザ情報の管理や LDAP 選択時のユーザ情報の表示を行ないます。

認証情報の登録

[認証情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

名　　称

複数の認証 ID・パスワードを設定する場合の名称を記入する欄です。

接続 ID・パスワード

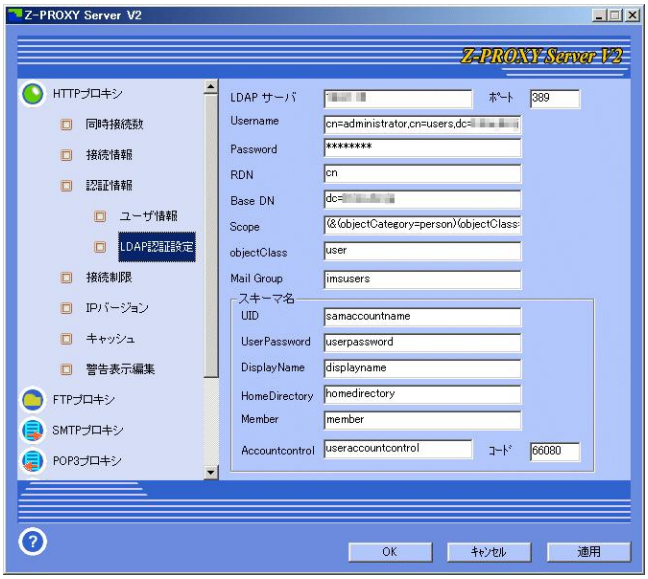
HTTP プロキシへ接続できる ID・パスワード欄です。

認証情報の削除

リスト上の削除したい HTTP 認証情報設定を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい HTTP 認証情報設定を選択し、キーボードの[Delete] キーにて削除が行えます。

LDAP 認証設定



LDAP サーバ上のユーザ情報の利用設定を行ないます。

アカウント登録・削除を行う場合は、LDAPサーバに付属する操作ツールをご使用ください。

詳細は、アクティブディレクトリ(AD)との接続例又は、OpenLADP との接続例を参照してください。

接続制限

接続アドレス編集

「接続アドレス編集」ボタンを押すことで表示されるメモ帳に接続元IPの接続許可範囲の設定を行います。

許可範囲以外からの接続には強制的に切断が行われます。

指定できる IP アドレスは、ワイルドカード及び、ネットマスクを使用でき、拒否 IP を指定する場合は、IP アドレスの記述に半角スペースを挟み'reject'と記入してください。

例）192.168.0.0～192.168.0.15 以外の IP からの接続を禁止する場合。

192.168.0.0/28

＊reject

禁止ワード

参照したページにここで指定した文字列が含まれている場合表示を禁止します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

ホワイトリスト編集

定義されたURLの参照には禁止ワードチェックをパスし、表示レスポンスを向上させたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

ブラックリスト編集

定義されたURLの参照を禁止としたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

URIBL編集

参照するURLのドメインをここで定義した、URIBLに問合せブラックリストとして掲載されている場合にURLの参照を禁止としたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

PICS-Label(セルフレイティング)

参照するページにMETAタグとしてPICS-Label項目が含まれている場合、以下で選択する表現範疇であるか否かの判定により、参照を禁止したい場合の設定です。

一般的に、未成年に対する閲覧制限を行ないたい場合に利用します。

未成年向け検索サイトへの参照URL問合せ

参照するURLについて、一般公開されている未成年向け検索サイトへURL検索を行い、この応答結果を利用したURLの参照の禁止を行ないます。

本設定は、上記「PICS-Label(セルフレイティング)」の有効時において、「簡易制限(小学生以下)」～「簡易制限(高校生以下)」が選択されている場合に自動的に有効になります。

また、本機能を利用することにより、コンテンツフィルタ用DBの更新不要で、常に最新の「未成年向けコンテンツフィルタ」として機能させることが可能になります。

IPバージョン

IPバージョンをクリックすると、IPv6での接続を行うなどの接続可能IPバージョンの選択を行なえます。

キャッシュ

キャッシュをクリックすると、HTTP プロキシキャッシュの設定を行えます。

キャッシュ有効期間(分)

HTTP プロキシ内でキャッシュした情報の有効期間を分単位で設定します。

0分とすると、キャッシュした情報は無効とされ、常にサーバの情報を取得に行きます。

キャッシュをクリアする

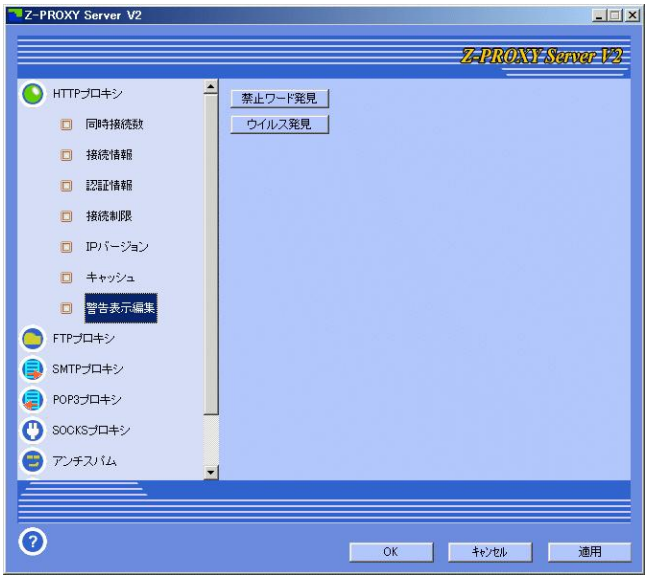
ボタンを押すとHTTP プロキシ内でキャッシュした情報の一括削除を行います。

キャッシュしないリンク

キャッシュ有効期間が設定されている場合に、特定のリンク先についてプロキシ内のキャッシュを利用したくない場合明示的にここに編集します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

警告表示編集



参照したページで禁止ワードが含まれる場合ブラウザに表示する HTML データを編集を行う場合、各ボタンをクリックし編集を行います。

ボタンをクリックすると、編集用のメモ帳が開きます。表示サンプルが含まれていますので、サンプルを参考に編集を行って下さい。

「ウイルス発見」ボタンは、アンチウイルス(オプション)機能がインストールされている場合に、参照したURL 内にウイルスが発見された場合ブラウザに表示する HTML データを編集を行います。

FTPプロキシの設定

「FTPプロキシ」をマウスでクリックすると、設定一覧が表示されます。

FTP プロキシを有効にする。

チェックすると、任意のポートに設定した FTP プロキシサーバ機能が利用可能になります。

アンチウイルスオプションが追加インストールされている場合は、ウイルスチェックによる監視を行います。

ログを残す

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

同時接続数

FTTP プロトコルセッションの同時処理数の上限を規定したい場合、1～65565の範囲で指定します。

0の場合は制限を行ないません。(デフォルト=0)

接続情報

接続情報をクリックすると、接続ポートの設定を行う為のダイアログ画面が表示されます。

接続情報の登録

[接続情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

接続先名称

接続先の名称を記入する欄です。

受信 IP・ポート

FTP プロキシへ接続できる IP アドレス欄(固定)とポート欄(変更可能)です。

接続先・ポート

FTP プロキシが接続する FTP サーバー名(IP アドレスでも可)欄とポート欄(変更可能)です。

接続先・ポート欄を空欄とすると、FTP Over HTTP での接続として利用されます。

公開 IP

インターネット上に公開している IP アドレス(グローバル IP)を設定します。

クライアントがインターネット上からパッシブモードで接続する際のデータセッションの接続 IP を認識する為に必要となります。

同一セグメント内での接続の場合は、空欄でも構いません。

接続情報の削除

リスト上の削除したい FTP 接続情報を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい FTP 接続情報を選択し、キーボードの[Delete] キーにて削除が行えます。

接続制限

接続制限をクリックすると、接続元IPの接続許可範囲の設定が行えます。

接続アドレス編集

「接続アドレス編集」ボタンを押すことで表示されるメモ帳に接続元IPの接続許可範囲の設定を行います。

許可範囲以外からの接続には強制的に切断が行われます。

指定できる IP アドレスは、ワイルドカード及び、ネットマスクを使用でき、拒否 IP を指定する場合は、IP アドレスの記述に半角スペースを挟み'reject'と記入してください。

例）192.168.0.0～192.168.0.15 以外の IP からの接続を禁止する場合。

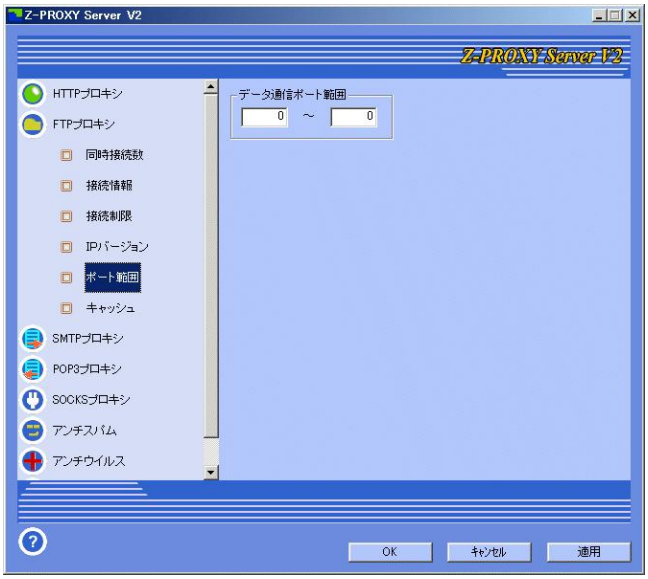
192.168.0.0/28

＊ reject

IPバージョン

IPバージョンをクリックすると、IPv6での接続を行うなどの接続可能IPバージョンの選択を行なえます。

データ通信ポート範囲



データ通信に使用されるポート範囲(1～65535)を指定します。

特定のポート範囲のみに限定したい場合に設定してください。

開始欄又は、終了欄が0の場合は、1～65535の全てが使用可能なポート範囲として利用されます。

キャッシュ

キャッシュ有効期間(分)

FTP プロキシ内でキャッシュした情報の有効期間を分単位で設定します。

0分とすると、キャッシュした情報は無効とされ、常にサーバの情報を取得に行きます。

キャッシュをクリアする

ボタンを押すとFTP プロキシ内でキャッシュした情報の一括削除を行います。

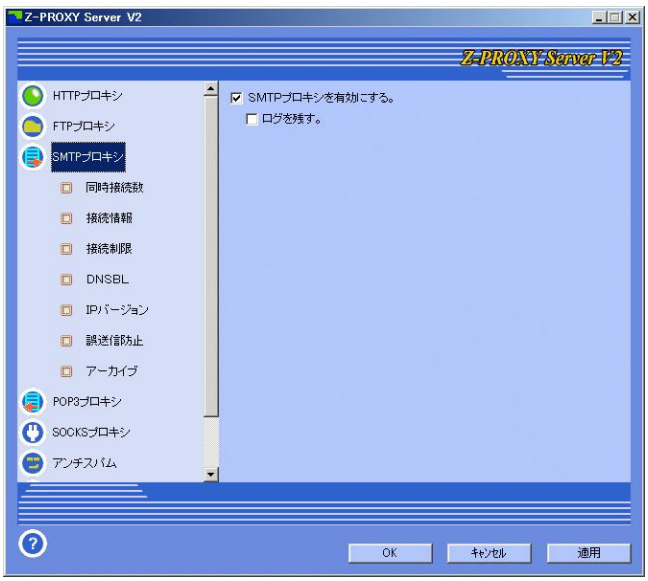
キャッシュしないリンク

キャッシュ有効期間が設定されている場合に、特定のリンク先についてプロキシ内のキャッシュを利用したくない場合明示的にここに編集します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

SMTPプロキシの設定

「SMTPプロキシ」をマウスでクリックすると、設定一覧が表示されます。



チェックすると、任意のポートに設定したSMTP用プロキシサーバが起動します。

SMTPプロキシを有効にする。

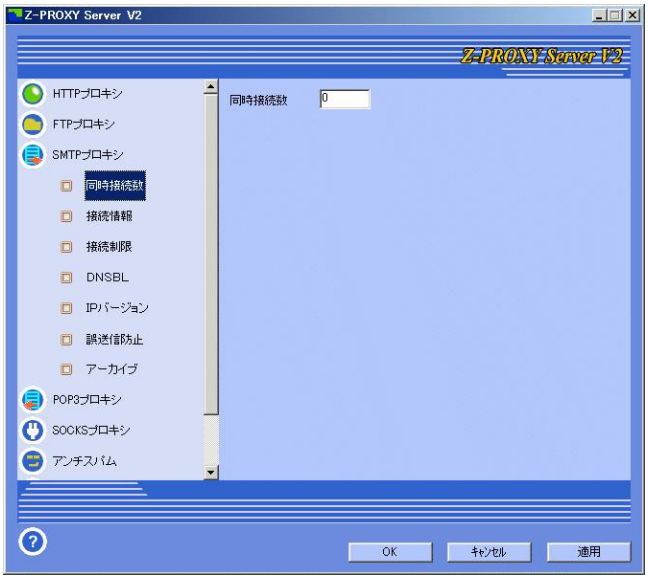
チェックすると、任意のポートに設定したSMTPプロキシサーバ機能が利用可能になります。

アンチウイルスオプションが追加インストールされている場合は、ウイルスチェックによる監視を行います。

ログを残す

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

同時接続数



SMTPプロトコルセッションの同時処理数の上限を規定したい場合、1～65565の範囲で指定します。

0の場合は制限を行ないません。(デフォルト=0)

接続情報

接続情報をクリックすると、接続ポートの設定を行う為のダイアログ画面が表示されます。

接続情報の登録

[接続情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

接続先名称

接続先の名称を記入する欄です。

トンネル

この接続で、暗号化通信(SMTP over SSL/TLS)等をプロキシ内で解析しないでそのままトンネルさせる場合にチェックします。

なお、本設定の通信はトンネリングされるのみでスパムチェックは行われません。

受信IP・ポート

SMTP プロキシへ接続できる IP アドレス欄(固定)とポート欄(変更可能)です。

接続元との通信に暗号化を行う。

この接続で、接続元(SMTP クライアント等)と本プロキシ間に暗号化通信(SMTP over SSL/TLS)を行う場合にチェックします。

この設定では、暗号化を行う為の証明書と秘密鍵が必要になります。

STARTTLS

この接続で、接続元(SMTP クライアント等)と本プロキシ間の平文ポートを利用し、STARTTLS 命令以降を暗号化通信(SMTP over SSL/TLS)を行う場合にチェックします。

この設定では、暗号化を行う為の証明書と秘密鍵が必要になります。

「接続元との通信に暗号化を行う。」と「STRATTLS」は排他的に選択が可能です。

・証明書

証明書(PEM 形式)の記載されたファイルをフルパスで指定します。

隣にある「参照」ボタンを押すと保管されているファイルの選択設定が可能です。

・秘密鍵

秘密鍵(PEM 形式)の記載されたファイルをフルパスで指定します。

隣にある「参照」ボタンを押すと保管されているファイルの選択設定が可能です。

注) 本プロキシ内での SMTP over SSL/TLS の解析及び実行は IPv4 アドレスのみ可能です。

接続先・ポート

SMTP プロキシが接続する SMTP サーバー名(IP アドレスでも可)欄とポート欄(変更可能)です。

接続先との通信に暗号化を行う。

この接続で、本プロキシと接続先(SMTP サーバ等)間に暗号化通信(SMTP over SSL/TLS, STARTTLS)を行う場合にチェックします。

注) 本プロキシ内での SMTP over SSL/TLS の解析及び実行は IPv4 アドレスのみ可能です。

STARTTLS

この接続で、接続先(SMTP サーバ等)と本プロキシ間の平文ポートを利用し、STARTTLS 命令以降を暗号化通信(SMTP over SSL/TLS)を行う場合にチェ

ックします。

「接続先との通信に暗号化を行う。」と「STRATTLS」は排他的に選択が可能です。

注）本プロキシ内での SMTP over SSL/TLS の解析及び実行は IPv4 アドレスのみ可能です。

接続時 IP

接続先へ接続する際に使用するIPアドレスを設定します。

マシン上に複数のIPアドレスが設定されている場合、デフォルトのIPで接続しますが、デフォルト以外のIPアドレで接続を行いたい場合に設定します。

空欄の場合はデフォルトのIPアドレスとなります。

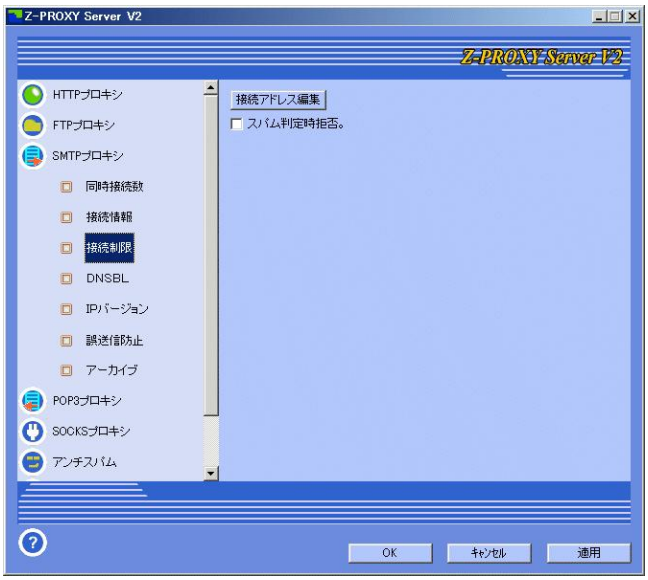
接続情報の削除

リスト上の削除したい SMTP 接続情報を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい SMTP 接続情報を選択し、キーボードの[Delete] キーにて削除が行えます。

なお、暗号化通信（SMTP over SSL/TLS）では、通信はトンネリングされるのみでスパムチェックは行われません。

接続制限



接続制限をクリックすると、接続元IPの接続許可範囲の設定が行えます。

接続アドレス編集

「接続アドレス編集」ボタンを押すことで表示されるメモ帳に接続元IPの接続許可範囲の設定を行います。

許可範囲以外からの接続には強制的に切断が行われます。

指定できるIP アドレスは、ワイルドカード及び、ネットマスクを使用でき、拒否 IP を指定する場合は、IP アドレスの記述に半角スペースを挟み'reject'と記入してください。

また、無条件にメールをスルーさせる場合は、IP アドレスの記述に半角スペースを挟み'pass'と記入してください。

例）192.168.0.0～192.168.0.15 以外の IP からの接続を禁止する場合。

192.168.0.0/28

＊ reject

例）192.168.0.5 からの送信は無条件にスルーさせる場合。

192.168.0.5 pass

スパム判定時拒否。

スパムチェックが有効で、スパムと判定されたメールを通過させたくない場合にチェックします。

DNSBL

接続元IPアドレスをDNSブラックリストで参照し、ブラックリストに存在する場合、接続を強制的に切断します。

問合せ先編集

問合せたいDNSBLサイトを記述します。

記述方法は1行1サイトとして複数記述可能ですがあまり、問合せサイトを複数記述するとレスポンスに影響が出ますの注意が必要です。

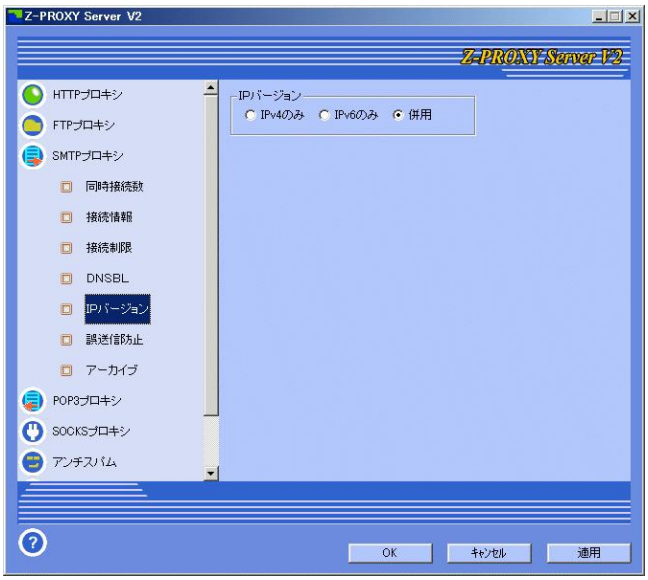
ホワイトリスト編集

DNSBLサイトへの問合せが不要な接続元IPを1行1IPアドレスとして記述します。

例）210.xxx.xxx.123 からの接続はDNSBLサイトへの問合せが不要な場合。

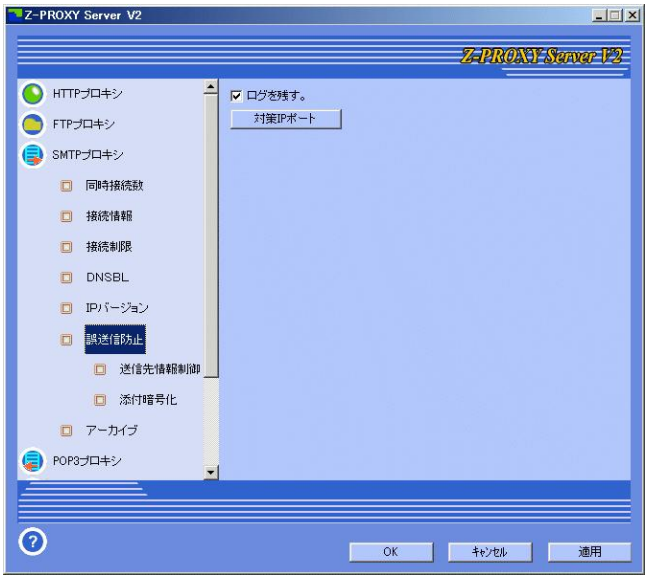
210.xxx.xxx.123

IPバージョン



IPv6での接続を行いたい場合などに接続可能IPバージョンを選択します。

誤送信防止機能



詳細ボタンを押すと、添付付メールを自動暗号化（パスワード付 ZIP 圧縮）したメールとして送信する設定を行うダイアログが表示されます。

ログを残す。

パスワード付 ZIP 圧縮の処理状況を記録します。

ログは環境変数"ALLUSERSPROFILE"

└ Z-PROXY

└ mail2ziplog

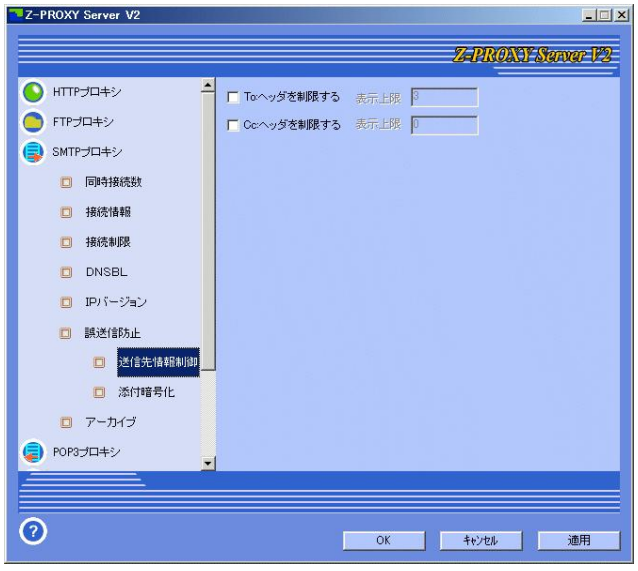
に記録されます。

対策 IP ポート

ボタンをクリックすると処理対象となる'リッスンIP:ポート' の指定を列挙する為、メモ帳が開きます。

対象となる'リッスンIP:ポート' 設定し保存してください。

送信先情報制御



BCC で送信すべき送信先アドレスを To:ヘッダや Cc:ヘッダに誤って記載して送信した場合に、To:ヘッダや Cc:ヘッダの記載から削除するための設定です。

To:ヘッダを制限する

To:ヘッダ欄について'表示上限'で指定したアドレス数を超える送信先アドレスを削除する場合にチェックします。

表示上限

ここで指定したアドレス数を上限に、To:ヘッダ情報を加工します。

Cc:ヘッダを制限する

Cc:ヘッダ欄について'表示上限'で指定したアドレス数を超える送信先アドレスを削除する場合にチェックします。

表示上限

ここで指定したアドレス数を上限に、Cc:ヘッダ情報を加工します。

添付暗号化

添付ファイル付メールに対しパスワード付 ZIP 圧縮を行い保護する為の設定です。

圧縮対象

添付付メールをメール丸ごとパスワード付圧縮を行なうか、含まれる添付ファイルを検出してファイルのみをパスワード付圧縮を行なうかを選択します。

メール全体

メール全体を丸ごとパスワード付圧縮を行い添付ファイルとして送信します。メールの本文は「メールメッセージ」で設定した内容が利用されます。

ファイル毎

含まれる添付ファイルを検出してファイルをパスワード付圧縮を行ないます。メールの構造は変わりません。

MIME 形式で構成される添付メールが対象となります。

分割されたメールや TEXT 形式内に uuencode 形式や hexbin 形式のデータを貼り付けたメールは処理されません。

圧縮ファイル拡張子

パスワード付 ZIP 圧縮されたメールは通常拡張子が'ZIP'となりますが、送信先サーバのポリシーにより、拡張子が'ZIP'を含んだ添付メールが拒絶されるような場合、ここで指定した拡張子に意図的に置換えた添付ファイル名として送信させる場合に設定します。

付加パスワード

ここで設定した任意の文字列最大7桁＋内部生成コード5桁を使ったパスワードをパスワード付 ZIP 圧縮に利用します。

SMTP サーバ設定(パスワードメール送信用)

SMTP

パスワードメールを送信する為の SMTP サーバを指定します。

ポート

パスワードメールを送信する為の SMTP ポートを指定します。

送信元アドレス

パスワード通知メールに利用するエンベロープの送信元の指定を行ないます。

送信元

添付付メールを送信した時点でのエンベロープの送信元を利用します。

アドレスを指定

右の入力欄に指定したメールアドレスを利用します。(空白可。)

送信先アドレス

パスワード通知メールの送信先の指定を行ないます。

送信先のまま

添付付メールの送信先へ送信します。

送信元へ返信

送信元へ送信し、添付付メールの送信先へは送信しません。

本メールを受けた後、改めてパスワードを送信先へ送信することで、添付メール送信先への誤送信が無いか二重チェックが可能になります。

IP バージョン

SMTP サーバの接続に利用する IP バージョンを指定します。

SMTP 認証

SMTP 認証を行う。(PLAIN のみ)

SMTP 認証を行いメール送信する場合にチェックします。

ID

SMTP 認証用 ID を設定します。

パスワード

SMTP 認証用パスワードを設定します。

メールメッセージ

パスワード付 ZIP 圧縮されたメールを添付したメールの本文として、ここで記載した文章が利用されます。

パスワードメールメッセージ

パスワードを通知するメールの本文として、ここで記載した文章が利用されます。

メールアーカイブ

SMTP プロキシを通過したメールを以下で指定するフォルダ内に日単位のフォルダを作成し、MailDIR 形式で順次保管しする為の設定です。

メール経路での情報漏えいなどの監査を実施際にメールデータの保管は欠かせなません。

メールを保管する

チェックすると以下の項目に指定したフォルダ内に日単位(20090716)といったフォルダを作成し1日単位のメールデータを順次保管します。

検索ソフトの実行パス

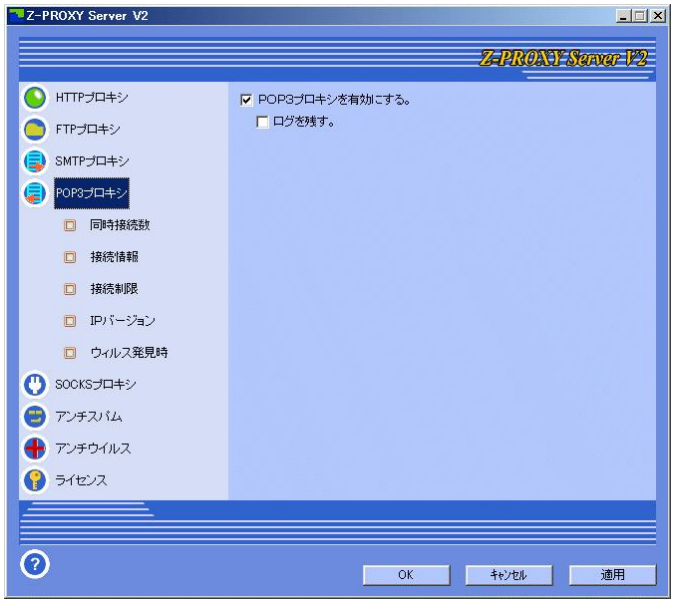
MailDIR 形式で保管されたメールデータを検索するツールKsearch(別売)を起動したい場合、インストールしたフォルダをフルパスで設定します。

検索ソフトの起動

上記で指定した検索ソールを起動したい場合、このボタンをクリックします。

POP3プロキシの設定

「POP3プロキシ」をマウスでクリックすると、設定一覧が表示されます。



POP3 プロキシを有効にする。

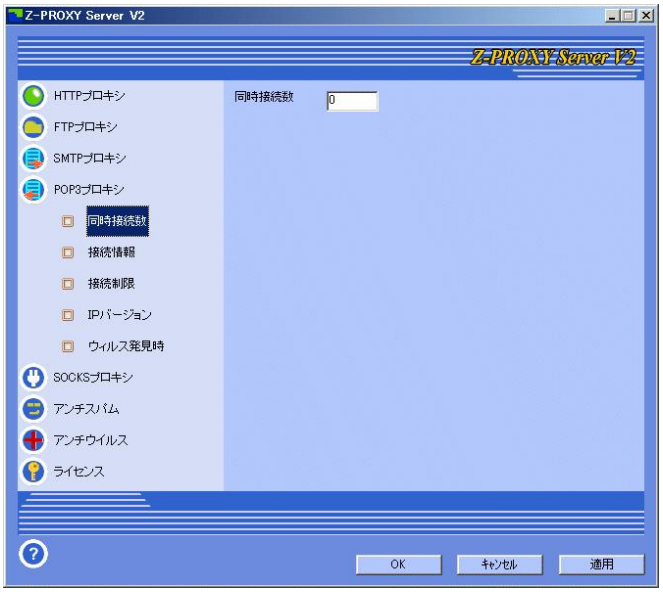
チェックすると、任意のポートに設定した POP3 プロキシサーバ機能が利用可能になります。

アンチウイルスオプションが追加インストールされている場合は、ウイルスチェックによる監視を行います。

ログを残す

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

同時接続数



POP3 プロトコルセッションの同時処理数の上限を規定したい場合、1～65565の範囲で指定します。

0の場合は制限を行ないません。(デフォルト=0)

接続情報

接続情報をクリックすると、接続ポートの設定を行う為のダイアログ画面が表示されます。

接続情報の登録

[接続情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

接続先名称

接続先の名称を記入する欄です。

トンネル

この接続で、暗号化通信(POP3 over SSL/TLS)等をプロキシ内で解析しないでそのままトンネルさせる場合にチェックします。

なお、本設定の通信はトンネリングされるのみでスパムチェックは行われません。

受信 IP・ポート

POP3 プロキシへ接続できる IP アドレス欄(固定)とポート欄(変更可能)です。

接続元との通信に暗号化を行う。

この接続で、接続元(POP3 クライアント等)と本プロキシ間に暗号化通信(POP3 over SSL/TLS)を行う場合にチェックします。

この設定では、暗号化を行う為の証明書と秘密鍵が必要になります。

STARTTLS

この接続で、接続元(POP3 クライアント等)と本プロキシ間の平文ポートを利用し、STARTTLS 命令以降を暗号化通信(POP3 over SSL/TLS)を行う場合にチェックします。

この設定では、暗号化を行う為の証明書と秘密鍵が必要になります。

「接続元との通信に暗号化を行う。」と「STRATTLS」は排他的に選択が可能です。

証明書

証明書(PEM 形式)の記載されたファイルをフルパスで指定します。

隣にある「参照」ボタンを押すと保管されているファイルの選択設定が可能です。

秘密鍵

秘密鍵(PEM 形式)の記載されたファイルをフルパスで指定します。

隣にある「参照」ボタンを押すと保管されているファイルの選択設定が可能です。

注) 本プロキシ内での POP3 over SSL の解析及び実行は IPv4 アドレスのみ可能です。

接続先・ポート

POP3 プロキシが接続する POP3 サーバー名(IP アドレスでも可)欄とポート欄(変更可能)です。

接続先との通信に暗号化を行う。

この接続で、本プロキシと接続先(POP3 サーバ等)間に暗号化通信(POP3 over SSL/TLS)を行う場合にチェックします。

注)本プロキシ内での POP3 over SSL/TLS の解析及び実行は IPv4 アドレスのみ可能です。

STARTTLS

この接続で、接続先（POP3 サーバ等）と本プロキシ間の平文ポートを利用し、STARTTLS 命令以降を暗号化通信（POP3 over SSL/TLS）を行う場合にチェックします。

「接続先との通信に暗号化を行う。」と「STRATTLS」は排他的に選択が可能です。

注）本プロキシ内での POP3 over SSL/TLS の解析及び実行は IPv4 アドレスのみ可能です。

接続時 IP

接続先へ接続する際に使用するIPアドレスを設定します。

マシン上に複数のIPアドレスが設定されている場合、デフォルトのIPで接続しますが、デフォルト以外のIPアドレで接続を行いたい場合に設定します。

空欄の場合はデフォルトのIPアドレスとなります。

接続情報の削除

リスト上の削除したい SMTP 接続情報を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい SMTP 接続情報を選択し、キーボードの[Delete] キーにて削除が行えます。

なお、暗号化通信（POP3 over SSL/TLS, STARTTLS）では、通信はトンネリングされるのみでスパムチェックは行われません。

接続制限

接続アドレス編集

「接続アドレス編集」ボタンを押すことで表示されるメモ帳に接続元IPの接続許可範囲の設定を行います。

許可範囲以外からの接続には強制的に切断が行われます。

指定できる IP アドレスは、ワイルドカード及び、ネットマスクを使用でき、拒否 IP を指定する場合は、IP アドレスの記述に半角スペースを挟み'reject'と記入してください。

例）192.168.0.0～192.168.0.15 以外の IP からの接続を禁止する場合。

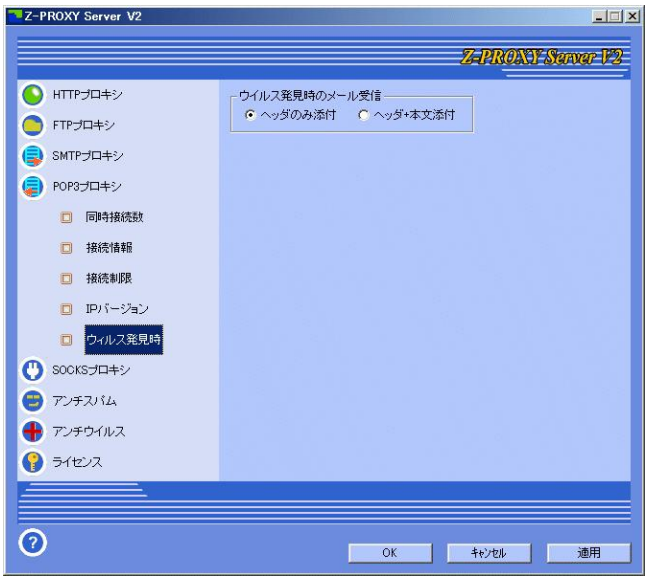
192.168.0.0/28

＊ reject

IPバージョン

IPv6での接続を行いたい場合などに接続可能IPバージョンを選択します。

ウイルス発見時



アンチウイルスオプションが追加インストールされている場合は、ウイルス発見時のメールの受信データを"ヘッダのみ"の受信か、"本文を添付ファイルとして加工"したものを受信するかの加工方法をここで指定します。

SOCKSプロキシの設定

「SOCKS プロキシ」をマウスでクリックすると、設定一覧が表示されます。

SOCKS(v4／v5)を有効にする。

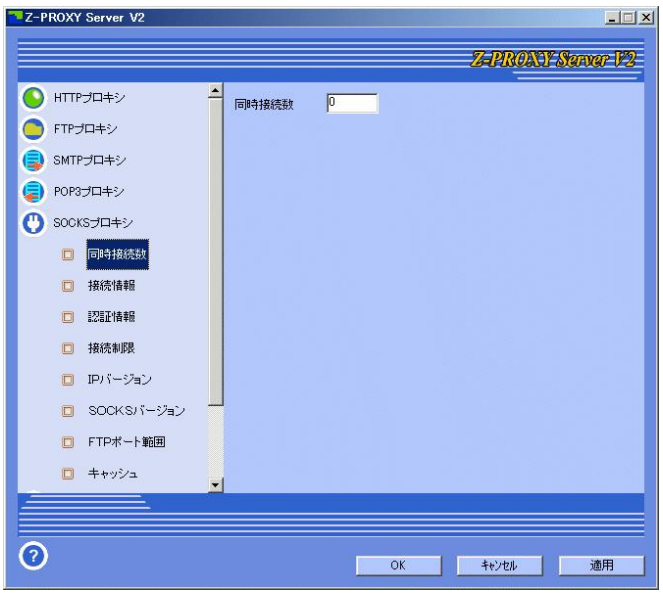
チェックすると、任意のポートに設定した SOCKS サーバ機能が利用可能になります。

アンチウイルスオプションが追加インストールされている場合は、ウイルスチェックによる監視を行います。

ログを残す

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

同時接続数



SOCKS プロトコルセッションの同時処理数の上限を規定したい場合、1～65565の範囲で指定します。

0の場合は制限を行ないません。(デフォルト＝0)

接続情報

接続情報をクリックすると、接続ポートの設定を行う為のダイアログ画面が表示されます。

接続情報の登録

[接続情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

接続先名称

接続先の名称を記入する欄です。

受信 IP・ポート

HTTP プロキシへ接続できる IP アドレス欄とポート欄(変更可能)です。

接続時 IP

インターネット上に公開する場合のグローバル IP を指定する欄です。

LAN内での公開の場合は、"空白"若しくは、"受信 IP"と同一にします。

接続情報の削除

リスト上の削除したい HTTP 接続情報を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したい HTTP 接続情報を選択し、キーボードの[Delete] キーにて削除が行えます。

認証情報

認証情報をクリックすると、この SOCKS による HTTP プロトコルへ接続する際に必要な認証 ID とパスワードの設定を行う為の画面が表示されます。

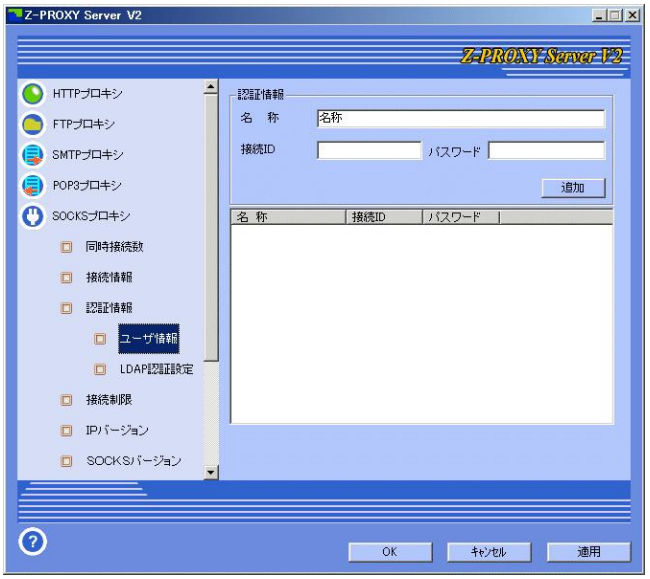
接続にはユーザ認証が必要

HTTP ブラウザの接続に HTTP 認証を必要としたい場合、チェックします。

利用するユーザ情報

Z-PROXY 内で独自管理するユーザ情報または、LDAP サーバ上のユーザ情報のどちらで利用するかを選択します。

ユーザ情報



Z-PROXY 内で独自管理するユーザ情報の管理や LDAP 選択時のユーザ情報の表示を行ないます。

認証情報の登録

[認証情報]に囲まれた、各項目を設定し、[追加]ボタンを押すと下段のリストに追加されます。

名　　称

複数の認証 ID・パスワードを設定する場合の名称を記入する欄です。

接続 ID・パスワード

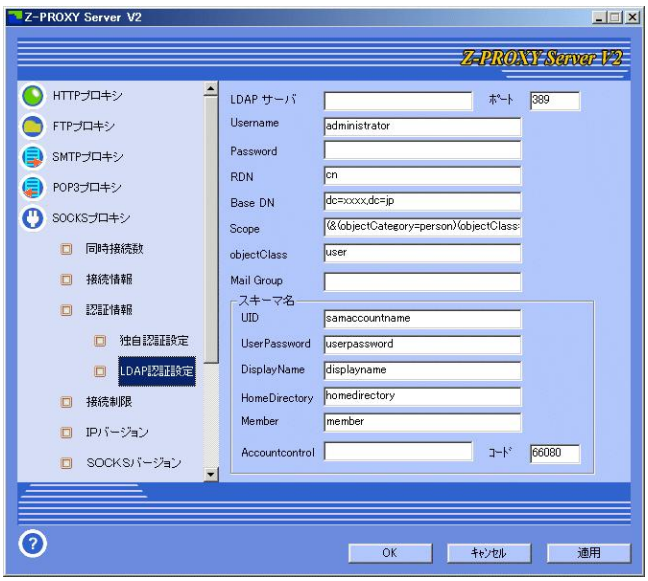
HTTP プロキシへ接続できる ID・パスワード欄です。

認証情報の削除

リスト上の削除したい HTTP 認証情報設定を選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとリストから削除が行えます。

または、リスト上の削除したいHTTP認証情報設定を選択し、キーボードの[Delete] キーにて削除が行えます。

LDAP 認証設定



LDAP サーバ上のユーザ情報の利用設定を行ないます。

アカウント登録・削除を行う場合は、LDAPサーバに付属する操作ツールをご使用ください。

詳細は、アクティブディレクトリ(AD)との接続例又は、OpenLADP との接続例を参照してください。

接続制限

接続制限をクリックすると、接続元IPの接続許可範囲、「ホワイトリスト」、「ブラックリスト」等の設定が行えます。

接続アドレス編集

「接続アドレス編集」ボタンを押すことで表示されるメモ帳に接続元IPの接続許可範囲の設定を行います。

許可範囲以外からの接続には強制的に切断が行われます。

指定できる IP アドレスは、ワイルドカード及び、ネットマスクを使用でき、拒否 IP を指定する場合は、IP アドレスの記述に半角スペースを挟み'reject'と記入してください。

例）192.168.0.0～192.168.0.15 以外の IP からの接続を禁止する場合。

192.168.0.0/28

＊ reject

ホワイトリスト編集

定義された URL の参照には無条件にパスし、表示レスポンスを向上させたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

ブラックリスト編集

定義された URL の参照を禁止としたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

URIBL編集

参照するURLのドメインをここで定義した、URIBLに問合せブラックリストとして掲載されている場合にURLの参照を禁止としたい時に設定します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

接続先プロトコル設定

SOCKS 経由で各種のプロトコルをポート単位で規定して利用可能にするための指定を行います。

例）ポート番号 10080 を HTTP プロトコルで接続可能にする場合。

10080,0,0,http

http,ftp,smtp,pop3 のデフォルトポート以外でこれらのプロトコル(http,ftp,smtp,pop3)を使用する場合は、プロトコルを明示しておく必要があります。

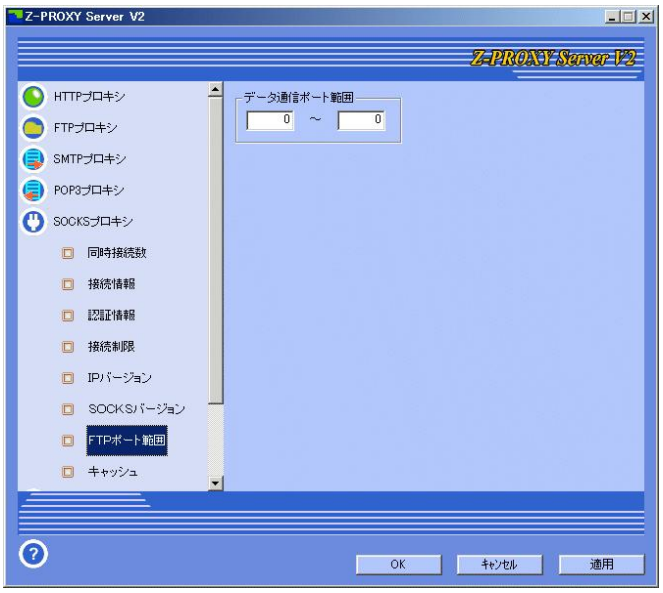
IPバージョン

IPバージョンをクリックすると、IPv6での接続を行うなどの接続可能IPバージョンの選択を行なえます。

SOCSKバージョン

処理対象とするSOCKSのバージョンを選択します。

FTPデータ通信ポート範囲



データ通信に使用されるポート範囲(1～65535)を指定します。

特定のポート範囲のみに限定したい場合に設定してください。

開始欄又は、終了欄が0の場合は、1～65535の全てが使用可能なポート範囲として利用されます。

接続先プロトコル設定

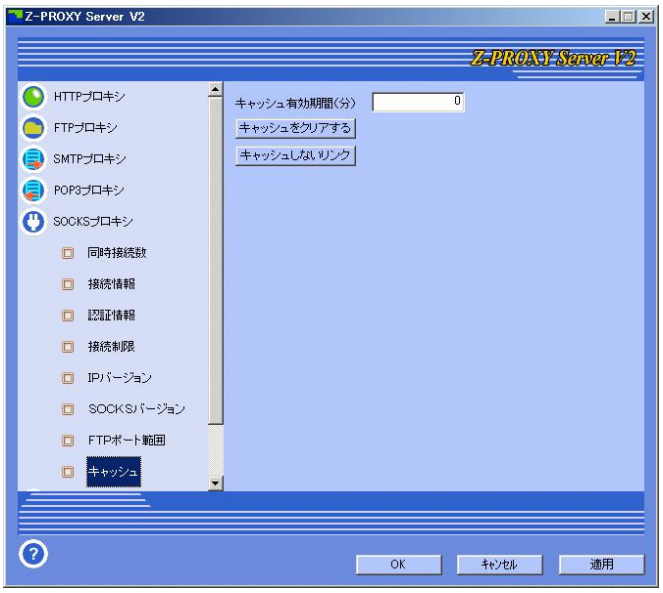
SOCKS 経由で各種のプロトコルをポート単位で規定して利用可能にするための指定を行います。

例)ポート番号 10080 を HTTP プロトコルで接続可能にする場合。

10080,0,0,http

http,ftp,smtp,pop3 のデフォルトポート以外でこれらのプロトコル(http,ftp,smtp,pop3)を使用する場合は、プロトコルを明示しておく必要があります。

キャッシュ



キャッシュをクリックすると、SOCKS 経由の(HTTP,FTP)用キャッシュの設定を行えます。

キャッシュ有効期間(分)

SOCKS プロキシ内で(HTTP,FTP 用)キャッシュした情報の有効期間を分単位で設定します。

0分とすると、キャッシュした情報は無効とされ、常にサーバの情報を取得に行きます。

キャッシュをクリアする

ボタンを押すと SOCKS プロキシ内で(HTTP,FTP 用)キャッシュした情報の一括削除を行います。

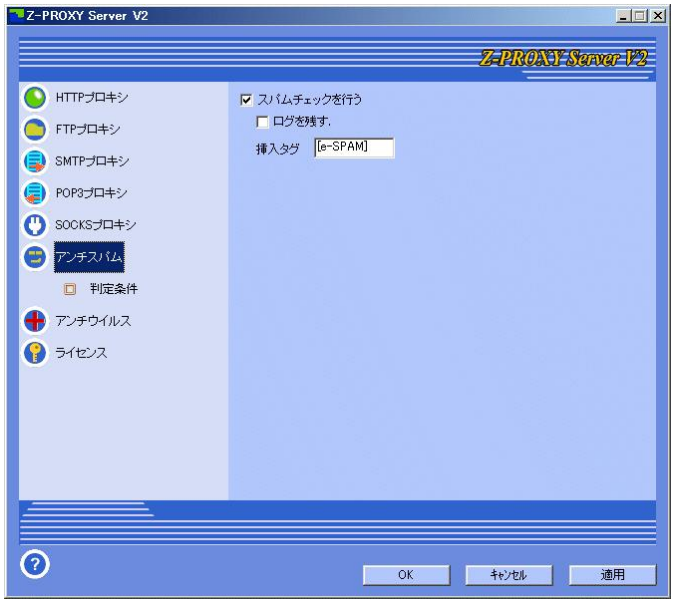
キャッシュしないリンク

キャッシュ有効期間が設定されている場合に、特定のリンク先についてプロキシ内のキャッシュを利用したくない場合明示的にここに編集します。

ボタンをクリックすると、編集用のメモ帳が開きます。編集方法は開いたメモ帳に記載されていますので、サンプルを参考に編集を行って下さい。

アンチスパムの設定

「アンチスパム」をマウスでクリックすると、設定一覧が表示されます。



スパムチェックを行う

SMTP プロキシ又は、POP3 プロキシをメールが通過する際、メール内に含まれる URL を抽出し、SURBL ボタンで設定した SURBL サイトリストのブラックリストに含まれていないか問合せします。

ブラックリストに含まれる URL を含むメールには、「題名ヘッダ」の先頭に「挿入タグ」で指定したタグ（文字列）を挿入し、メールクライアント側に受信させます。

ログを残す

チェックした結果をログとして残す場合にチェックします。デフォルト:オフ

挿入タグ

URIBLサイトへの問合せの結果ブラックリストに含まれる URL が発見された場合、そのメールの「題名ヘッダ」の先頭にここで指定した文字列を挿入し、メール受信時の振分けに使用します。

判定条件

スパムと判定する条件設定を行います。

キーワード

メール本文中の文字列でスパムと判定したい場合にボタンをクリックしキーワードを指定します。

URIBL

問合せたいURIBLサイトリストの編集を行う場合にボタンをクリックし、URIBLサイトを指定します。

日付ヘッダの異常

メールに含まれる送信日付が異常と思われる日付を示している場合にスパム判定としたい場合チェックします。

送信ドメイン認証(SPF1)不一致

SMTP プロキシに対して送信ドメイン認証(SPF1)で不一致な送信に対してスパム判定としたい場合チェックします。

ホワイトリスト

このファイルへは、送信ドメイン認証（SPF1）での判定をスキップさせたい接続Pアドレスを設定します。

アンチウイルス(アンチウイルスオプションが必要です。)

注意)

アンチウイルス機能をご利用になるためには、アンチウイルスオプションをダウンロードし本プログラムインストールフォルダにインストールする必要があります。

「アンチウイルス」をマウスでクリックすると、設定一覧が表示されます。

アンチウイルスエンジンを起動する。

チェックすると、アンチウイルスオプションの利用を有効にします。

ログを残す

アンチウイルスエンジンの動作についてログを残す場合にチェックします。デフォルト:オフ

データ更新

アンチウイルスデータベースを定期的に更新する為の設定です。

データ更新間隔

アンチウイルスデータベースを更新する間隔を設定します。デフォルト:1時間

ログを残す

アンチウイルスデータベースの更新ログを残す場合にチェックします。デフォルト:オフ

更新はプロキシサーバを使用する。

プロキシサーバー経由でアンチウイルスデータベースを更新する場合にチェックします。デフォルト:オフ

チェックボックスがオンした場合は、接続するプロキシサーバー(IP)アドレスとポート番号を設定してください。

プロセス監視

実行中のプロセス監視

チェックすると、実行中のプロセス(プログラム)及び、スタートアップ用レジストリ、フォルダに登録されたプログラムについて定期的にウイルスチェックによる監視を行えます。

ログを残す。

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

リアルタイム監視

リアルタイム監視

チェックすると、指定したドライブやフォルダへのファイル書込み、変更状態を検出し対象となるファイルについてウイルスチェックによる監視を行います。

複数のドライブを監視する場合は、";"(セミコロンで区切り)記載が可能です。

例)"A:"ドライブと"C:"ドライブを監視する場合 → "A:¥;C:¥"

ログを残す。

監視した結果をログとして残す場合にチェックします。デフォルト:オフ

対象ドライブ

監視したいドライブを直接入力設定します。

ここでの、設定は未接続のUSBドライブを直接指定することも可能で、接続が行われた時点で監視が開始されるようになりますが、監視開始後の自動開放は出来なくなります。

複数のドライブを監視する場合は、";"(セミコロンで区切り)記載が可能です。

例)"A:"ドライブと"C:"ドライブを監視する場合 → "A:¥;C:¥"

監視先設定

ボタンを押すと、監視を除外するフォルダを選択可能な、フォルダツリーダイアログが表示されます。

監視の除外は、該当するフォルダのチェックをオフとして、[OK]ボタンを押してダイアログを閉じてください。

除外する拡張子

監視から除外するファイルの拡張子の設定を行いときボタンをクリックし、表示されたメモ帳に拡張子を登録し保存することで除外対象として登録します。

ウイルス発見時

「ウイルス発見時」をマウスでクリックするとウイルス発見時のメール通知に関する設定をダイアログ画面が開きます。

メールで通知する。

ウイルス発見時にメールで通知するか否かを指定します。

チェックすると、以下に指定した内容に従ってメール通知を行います。

SMTP サーバー

通知に使用する SMTP サーバーを指定します。

ポート

SMTP サーバーのポート番号を指定します。(デフォルト 25)

SSL で通信

SMTP への送信で SSL による通信を行う場合に指定します。

送信元アドレス

通知メールの送信者アドレスを指定します。

送信者名

通知メールの送信者名を指定します。

SMTP 認証で送信(PLAIN のみ)

送信する場合に SMTP 認証を行う場合に指定します。(PLAIN 方式での認証でのみ利用できます。)

ユーザ名

SMTP 認証で使用するユーザーID を指定します。

パスワード

SMTP 認証で使用するパスワードを指定します。

通知先指定

通知を行いたい送信先アドレスを指定します。

送信先アドレス

送信先アドレス欄に指定したアドレスに通知を行います。

複数送信先を指定する場合は、","(半角カンマ)で区切りを入れると可能になります。

また、本欄へ変数名(&TO,&FROM)を指定しますと変数名に従い通知を行います。

変数名

&TO ウイルスの発見されたメールの TO:ヘッダに記載された最初のアドレスに通知します。

&FROM ウイルスの発見されたメールの FROM:ヘッダに記載された最初のアドレスに通知します。

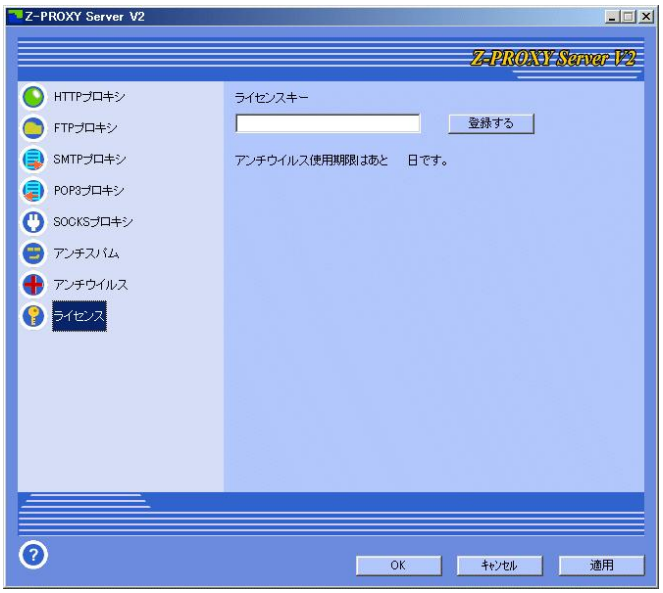
例) xxx1@abc.jp と メールの送信手順で送られた RCPT TO:のアドレスへ通知する場合

xxx1@abc.jp,&RCV または、 &RCV,xxx1@abc.jp

先頭の記述アドレスがメールの TO:ヘッダに以降のアドレスは CC:ヘッダに記録されます。

ライセンス

「ライセンス」をマウスでクリックするとライセンスの状態やライセンスキーの登録に関する設定ダイアログが開きます。

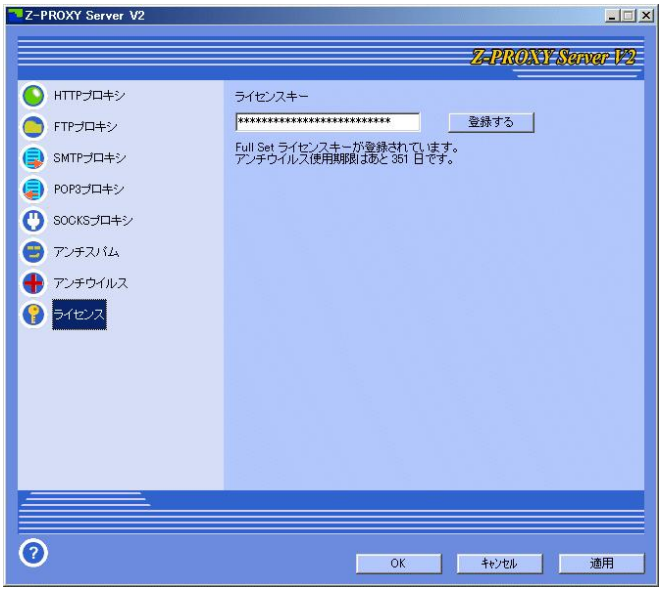


「Z-PROXY Server V2」 は、ライセンス未登録のままの場合、実行開始から30日間を試用期間として設定されています。

ライセンスが未登録のまま、試用期間を経過すると処理が停止しますので、ご注意ください。

継続してご使用になる場合は、年間ライセンスを取得いただき、以下の手順にてライセンスキーを登録いただくことで、ご使用が可能となります。

ライセンスキー入力欄がから、ライセンスキーを入力し、「登録する」ボタンを押しライセンスを登録してください。



正しいライセンスキーが入力され、再表示させると、「使用期限はあと nnn 日です。」のメッセージが表示されるようになります。

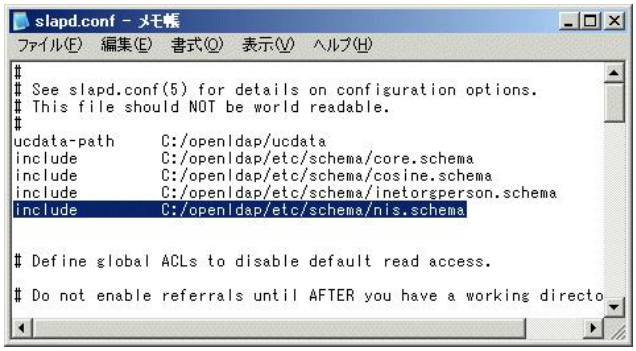
HTTP プロキシ認証の設定

OpenLDAP との接続例

1. OpenLDAP 側の設定

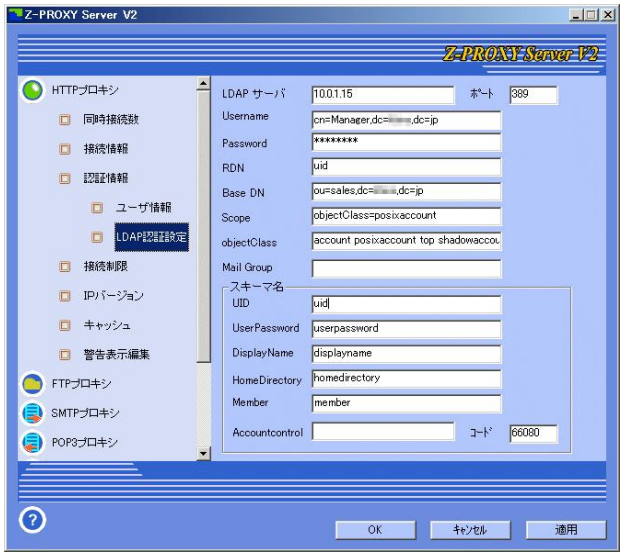
Open LDAP をユーザーアカウントとして、posixaccount を利用可能にするには、nis.schema を Open LDAP 側の設定(slapd.conf)に記載しておく必要があります。

また、アカウントの登録・削除は OpenLDAP 側で行う必要があります。



2. Z-PROXY Server V2 側の設定

Z-PROXY Server V2 が Open LDAP へ接続を行う為の設定内容は以下の通りとなります。



Proxy 認証には LDAP サーバのアカウントを使用する。

LDAP サーバのアカウントをプロキシ認証に使用するときチェックします。

LDAP サーバ

接続先の LDAP サーバーのアドレスを指定します。

例)192.168.1.12

ポート

接続先の LDAP サーバーのポート番号を指定します。

例)389

UserName

接続先時のユーザーID を指定します。

例)cn=<接続 ID>,dc=<組織名>,dc=&国(jp)>

Password

接続先 ID のパスワードを指定します。

例)secret

RDN

相対識別名となる名称を指定します。

例)uid

Base DN

検索の開始位置を示す DN を指定します。

例)ou=<部署名>,dc=<組織名>,dc=&国(jp)>

Scope

検索する階層レベルの範囲を指定します。

例)objectClass=posixaccount

objectClass

エントリの大枠を規定する形式を指定します。

例) account posixaccount top shadowaccount

Mail Group

エントリの大枠を規定する形式を指定します。

Open LDAP の場合は設定不要です。

スキーマ名

以下の各データベースの構造名称を指定します。

UID

ユーザ ID のスキーマ名を指定します。

uid

UserPassword

パスワードのスキーマ名を指定します。

userpassword

DisplayName

表示名のスキーマ名を指定します。

displayname

HomeDirectory

ホームディレクトリのスキーマ名を指定します。

homedirectory

Member

メンバのスキーマ名を指定します。

member

Accountcontrol

Active Directry 接続時のアカウントの状態のスキーマ名を指定します。

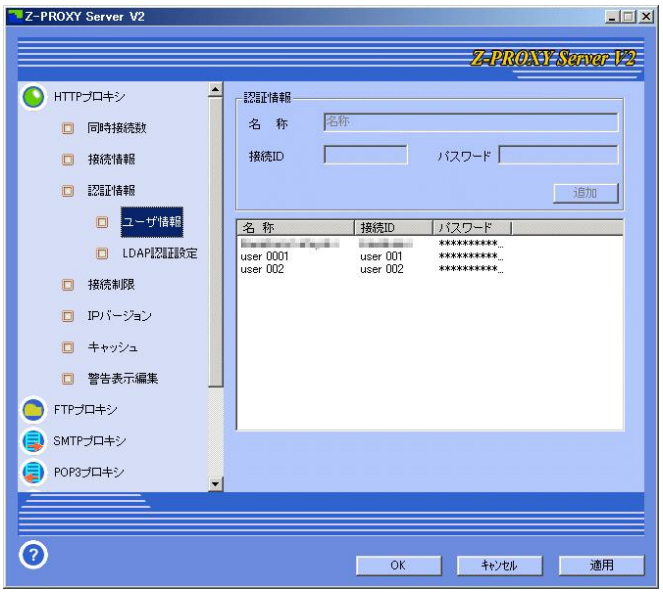
Open LDAP の場合は設定不要です。

コード

上記、Accountcontrol で Active Directry 接続時のアカウント作成時の値を指定します。

Open LDAP の場合は設定不要です。

設定後、[認証情報設定]ダイアログを起動し、既に登録済みのアカウントが表示されれば、設定完了です。



[サービス]の再起動を行うと機能が有効になります。

アクティブディレクトリ(AD)との接続例

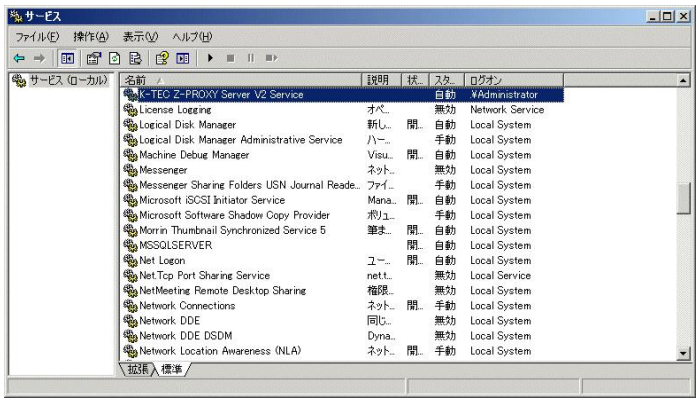
1. アクティブディレクトリ(AD)側の設定

アクティブディレクトリ(AD)側の設定は特にありませんが、アカウントの登録・削除はアクティブディレクトリ(AD)側で行う必要があります。

2. Z-PROXY Server サービスログオンアカウントの変更

アクティブディレクトリ(AD)側と接続する為に、サービスのログオンアカウントを"Administrator"権限のアカウントとして設定変更を行う必要があります

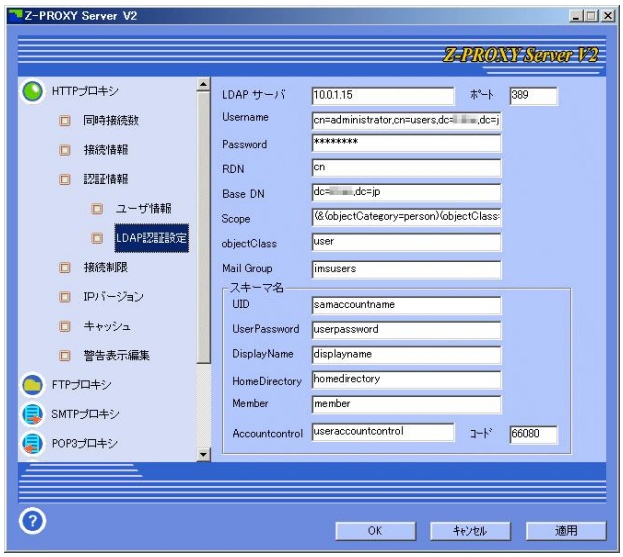
設定変更を行うには、[スタート]→[管理ツール]→[サービス]を選択し、表示されたサービスの一覧から**[K-TEC Z-PROXY Server V2 Service]**のプロパティを開き、[ログオン]タブを選択します。



[ログオン]項目の[アカウント]ボタンを選択し、"Administrator"権限のアカウントとパスワードを登録して下さい。

3. Z-PROXY Server V2 側の設定

Z-PROXY Server V2 側がアクティブディレクトリ(AD)へ LDAP プロトコルで接続を行う為の設定内容は以下の通りとなります。



Proxy 認証には LDAP サーバのアカウントを使用する。

LDAP サーバのアカウントをプロキシ認証に使用するときチェックします。

LDAP サーバー

接続先のアクティブディレクトリ(AD)サーバーのアドレスを指定します。

例)192.168.1.15

ポート

接続先のアクティブディレクトリ(AD)サーバーのポート番号を指定します。

例)389

UserName

接続先時のユーザーID を指定します。

例)cn=<接続 ID(administrator)>,cn=users,dc=<組織名>,dc=<国(jp)>

Password

接続先 ID のパスワードを指定します。

例)secret

RDN

相対識別名となる名称を指定します。

例)cn

Base DN

検索の開始位置を示す DN を指定します。

例)cn=users,dc=<組織名>,dc=&国(jp)>

Scope

検索する階層レベルの範囲を指定します。

例)(&(objectCategory=person)(objectClass=user)(memberof=cn=imsusers,cn=users,dc=<組織名>,dc=<国(jp)>))

objectClass

エントリの大枠を規定する形式を指定します。

例) user

Mail Group

エントリの大枠を規定する形式を指定します。

例) imsusers

スキーマ名

以下の各データベースの構造名称を指定します。

UID

ユーザ ID のスキーマ名を指定します。

samaccountname

UserPassword

パスワードのスキーマ名を指定します。

userpassword

DisplayName

表示名のスキーマ名を指定します。

displayname

HomeDirectory

ホームディレクトリのスキーマ名を指定します。

homedirectory

Member

メンバのスキーマ名を指定します。

member

Accountcontrol

Active Directry 接続時のアカウントの状態のスキーマ名を指定します。

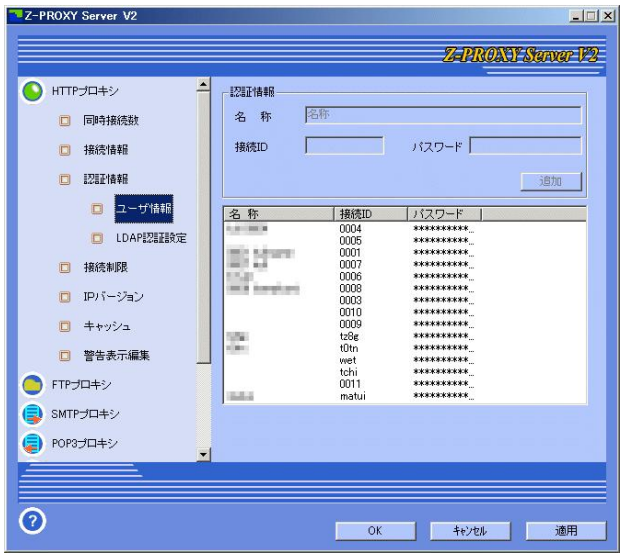
useraccountcontrol

コード

上記、Accountcontrol で Active Directry 接続時のアカウント作成時の値を指定します。

66080

設定後、[認証情報設定]ダイアログを起動し、既に登録済みのアカウントが表示されれば、設定完了です。



[サービス]の再起動を行うと機能が有効になります。

指定ファイルをウイルススキャンするには

本機能はオプションです。

アンチウイルスオプションが追加されている必要があります。

指定ファイルをウイルススキャンするには、以下の2種類の方法から選択して実施します。

1. タスクトレイに常駐しているアイコンのメニューから実施する場合。

タスクトレイ上のアイコンをマウスの右ボタンでクリックすると、メニューが表示されます。

表示されたメニューの「スキャン(S)」を左ボタンでクリックすると、「リアルタイム監視」で指定した対象ドライブについて一括スキャンを開始します。

監視しないフォルダの指定がされている場合は、この指定に準じてスキャンが行われます。

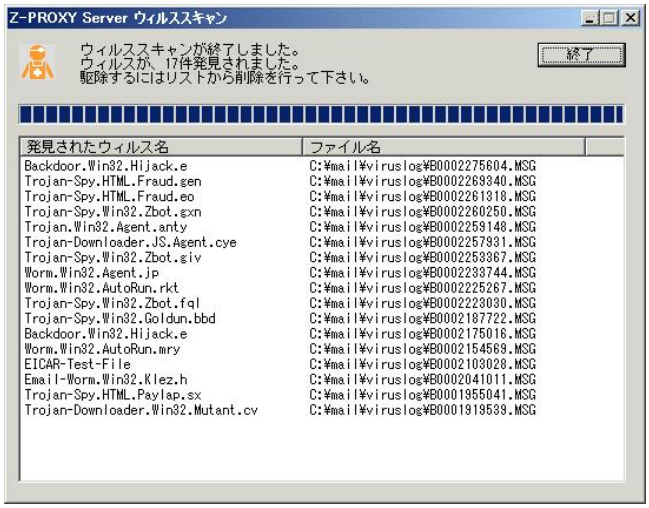
2. 任意のドライブ、フォルダ、ファイルのみをスキャンする場合。(オンデマンド・ウイルススキャン)

スキャンさせたいドライブ、フォルダ、ファイルに対し「デスクトップ上のアイコンへドラッグ＆ドロップ」を行うか、「マウスの右ボタンクリックで表示されるメニュー」を選択することでスキャンを開始します。

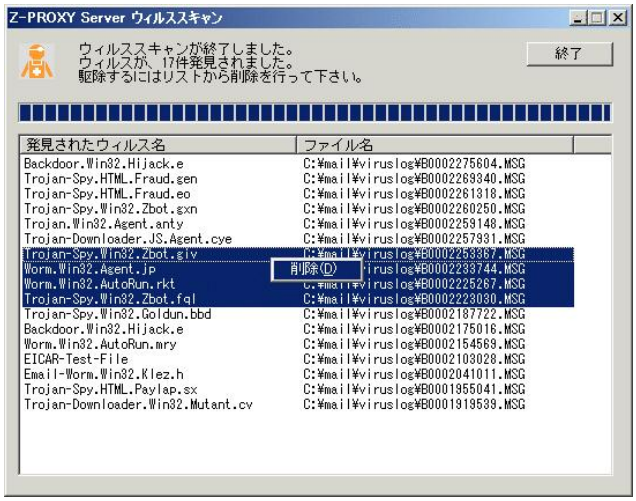
監視しないフォルダの指定は、無視され全ての階層のスキャンが行われます。

ドライブ単位でのウイルススキャン実行例	フォルダ単位でのウイルススキャン実行例	ファイル単位でのウイルススキャン実行例
		

ウイルススキャン結果(発見例)



ウイルススキャン結果(削除方法)



発見されたウイルスを削除するには、リスト上の削除したいファイルを選択し、右ボタンをクリックすると、[削除]のポップアップメニューが表示されるので選択するとファイル毎、削除が行われます。

または、リスト上の削除したいファイルを選択し、キーボードの[Delete] キーにて削除が行えます。

使用フォルダ＆レジストリ

【使用フォルダ】

環境変数"ALLUSERSPROFILE"

└ Z-PROXY

- ├ cash　　プロキシでの一次作業フォルダ
- ├ httpcache　HTTP プロキシでのキャッシュデータ保管フォルダ
- ├ ftpcache　FTP プロキシでのキャッシュデータ保管フォルダ
- ├ spamenglog　スパムチェック用ログフォルダ
- ├ httplog　　ＨＴＴＰプロキシ用ログフォルダ
- ├ ftplog　　ＦＴＰプロキシ用ログフォルダ
- ├ smtplog　　SMTP プロキシ用ログフォルダ
- ├ pop3log　　POP3 プロキシ用ログフォルダ
- ├ sockslog　　ＳＯＣＫＳプロキシ用ログフォルダ
- ├ mail2ziplog　パスワード付圧縮ファイル化処理用ログフォルダ
- ├ white.db　　ＨＴＴＰプロキシ用ホワイトリストファイル
- ├ black.db　　ＨＴＴＰプロキシ用ブラックリストリストファイル
- ├ http.ini　　ＨＴＴＰプロキシ用接続情報ファイル
- ├ http-old.ini　ＨＴＴＰプロキシ用接続情報ファイル（変更前バックアップ）
- ├ http-auth.ini　ＨＴＴＰプロキシ用認証情報ファイル
- ├ http-auth-old.ini　ＨＴＴＰプロキシ用認証情報ファイル（変更前バックアップ）
- ├ http-dnsbl.db　ＨＴＴＰプロキシ用ＤＮＳＢＬファイル
- ├ ftp.ini　　ＦＴＰプロキシ用接続情報ファイル
- ├ ftp-old.ini　ＦＴＰプロキシ用接続情報ファイル（変更前バックアップ）
- ├ ftp-auth.ini　ＦＴＰプロキシ用認証情報ファイル
- ├ fttp-auth-old.ini　ＦＴＰプロキシ用認証情報ファイル（変更前バックアップ）
- ├ smtp.ini　　SMTP プロキシ用接続情報ファイル
- ├ smtp-old.ini　SMTP プロキシ用接続情報ファイル（変更前バックアップ）
- ├ smtp-con.ini ＳＭＴＰ接続制限用アドレス編集ファイル
- ├ smtp-conbl.ini ＳＭＴＰ接続ＤＮＳＢＬ問合せサイト編集ファイル
- ├ smtp-conwl.ini ＳＭＴＰ接続ＤＮＳＢＬ問合せ不要（ホワイトリスト）ＩＰ編集ファイル
- ├ pop3.ini　　POP3 プロキシ用接続情報ファイル
- ├ pop3-old.ini　POP3 プロキシ用接続情報ファイル（変更前バックアップ）
- ├ pop3-con.ini ＰＯＰ３接続制限用アドレス編集ファイル
- ├ socks.ini　　ＳＯＣＫＳプロキシ用接続情報ファイル
- ├ socks-old.ini　ＳＯＣＫＳプロキシ用接続情報ファイル（変更前バックアップ）
- ├ socks-con.ini ＳＯＣＫＳ接続制限用アドレス編集ファイル
- ├ socks-auth.ini　ＳＯＣＫＳプロキシ用認証情報ファイル
- ├ socks-auth-old.ini　ＳＯＣＫＳプロキシ用認証情報ファイル（変更前バックアップ）
- ├ socks-ptl.ini　ＳＯＣＫＳプロキシ接続先プロトコル対応ファイル
- ├ socks-ptl-old.ini　ＳＯＣＫＳプロキシ接続先プロトコル対応ファイル（変更前バックアップ）
- └ socks-dnsbl.db　ＳＯＣＫＳプロトコルでのＨＴＴＰ接続時用ＤＮＳＢＬファイル

- ├ mail2zip　　パスワード付 ZIP 圧縮処理用作業フォルダ
- ├ mail2ziplog パスワード付 ZIP 圧縮処理用ログフォルダ
- ├ ziped-message.txt　　ZIP 圧縮処理用添付メッセージ（本文メール用）
- ├ ziped-pw-message.txt　ZIP 圧縮処理用添付メッセージ（パスワードメール用）
- └ mime.ini　　ZIP 圧縮処理用 MIME 名から拡張子の引き当てテーブル

【使用レジストリ】

■作業ルートフォルダ指定

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ workenv　　(文字列) デフォルト:ALLUSERSPROFILE

■メール通知関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ SmtpSend　　(DWORD) 通知フラグ 0:しない,1:する
└ SmtpSMTPServer　(文字列) 送信先サーバー
└ SmtpPort　　(DWORD) 送信先ポート デフォルト:25
└ SmtpSendaddr　(DWORD) 送信先指定　0:送信先を指定,1:送信元へ送信,2:両方に送信
└ SmtpTo　　(文字列) 送信先アドレス
└ SmtpFrom　　(文字列) 送信元アドレス
└ SmtpFromName　(文字列) 送信元名称
└ SmtpAuth　　(DWORD) ＳＭＴＰ認証フラグ 0:しない,1:する
└ SmtpID　　(文字列) ＳＭＴＰ認証ＩＤ
└ SmtpPassword　(文字列) ＳＭＴＰ認証パスワード
└ SmtpSSL　　(DWORD) ＳＳＬ送信フラグ 0:しない,1:する

■自動更新関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ Timeout　　(DWORD) 更新間隔（時間）
└ LogEnabled　　(DWORD) ログ記録 0:しない,1:する
└ ProxyServerUsed　(DWORD) プロキシサーバーを使用する 0:しない,1:する
└ ProxyServerName　(文字列) プロキシサーバーアドレス
└ ProxyServerPort　(DWORD) プロキシサーバーポート

■監視対象関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ http (DWORD) ＷＥＢ操作（ＨＴＴＰ） 0:しない,1:する
└ httplog (DWORD) ＷＥＢ操作（ＨＴＴＰ）のログ 0:しない,1:する
└ cwflog (DWORD) 禁止ワード検査のログ 0:しない,1:する
└ cwfshtmlbuffer (DWORD) 禁止ワード検査時のＨＴＭＬ読み込みバッファサイズ デフォルト300(KB)
└ cwfshtmlcharset (文字列) 禁止ワード検査時のデフォルトキャラクタコード sift_jis
└ ftpp (DWORD) ＷＥＢ操作（ＦＴＰ） 0:しない,1:する
└ ftplog (DWORD) ＷＥＢ操作（ＦＴＰ）のログ 0:しない,1:する
└ smtp (DWORD) メール送信（ＳＭＴＰ） 0:しない,1:する
└ smtplog (DWORD) メール送信（ＳＭＴＰ）のログ 0:しない,1:する
└ pop3 (DWORD) メール受信（ＰＯＰ３） 0:しない,1:する
└ pop3log (DWORD) メール受信（ＰＯＰ３）のログ0:しない,1:する
└ socks (DWORD) ＳＯＣＫＳ 0:しない,1:する
└ sockslog (DWORD) ＳＯＣＫＳのログ 0:しない,1:する

■HTTP/1.1 Keep-Alive 操作

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ httpkeepalive (DWORD) 0:常に無効（デフォルト） 1:HTTP/1.1のとき有効

■ヘッダ操作関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
|
└ smtpaddheader (DWORD) SMTP用Recieved:ヘッダ挿入の有無 0:しない 1:挿入する（デフォルト）
|
└ httpaddheader (DWORD) HTTP用X-Forwarded-For:,Remote-Host-Wp:,Forwarded:,Via:ヘッダの挿入の有無（デフォルト値=14 Via:ヘッダ無し）

ヘッダ＼bit	3	2	1	0
X-Forwarded-For:	1	-	-	-
Remote-Host-Wp:	-	1	-	-
Forwarded:	-	-	1	-
Via:	-	-	-	1

※１ もし、ヘッダを挿入しない場合 httpaddheader = 0
※２ もし、Via:ヘッダのみ挿入する場合 httpaddheader = 1
※３ もし、Forwarded:ヘッダのみ挿入する場合 httpaddheader = 2
※４ もし、Remote-Host-Wp:ヘッダのみ挿入する場合 httpaddheader = 4
※５ もし、X-Forwarded-For:ヘッダのみ挿入する場合 httpaddheader = 8
※６ もし、Forwarded:/Remote-Host-Wp:ヘッダの２ヘッダ挿入する場合 httpaddheader = 6
※７ もし、Forwarded:/Remote-Host-Wp:/X-Forwarded-For:ヘッダの３ヘッダ挿入する場合 httpaddheader = 14
※８ もし、Via:/Forwarded:/Remote-Host-Wp:/X-Forwarded-For:ヘッダの４ヘッダ挿入する場合 httpaddheader = 15

といった具合で設定します。

■誤送信防止対策関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ M2ZLog (DWORD) ログの取得 0:しない,1:する
└ M2ZUniqPW (文字列) 付加パスワードの任意文字列（半角英数字で最大７桁まで）
└ M2ZEtend （文字列）ZIP拡張子
└ M2ZIPversion (DWORD) IPバージョン 0:IPv4 1:IPv6
└ M2ZSmtp (文字列) SMTPサーバアドレス
└ M2ZSmtpPort (DWORD) SMTPサーバポート
└ M2ZESmtp (DWORD) SMTP認証の有無 0:無し,1:有り
└ M2ZSmtpAuthID (文字列) SMTP認証用ＩＤ
└ M2ZSmtpAuthPW (文字列) SMTP認証用パスワード
└ M2ZToHead (DWORD) To:ヘッダ制限の有無 0:しない,1:する
└ M2ZToHeadCount (DWORD) To:ヘッダ表示上限数
└ M2ZCcHead (DWORD) Cc:ヘッダ制限の有無 0:しない,1:する
└ M2ZCcHeadCount (DWORD) Cc:ヘッダ表示上限数
└ M2ZLevel (DWORD) 圧縮時のパスワードの生成方法オプション 0:自動生成 1:固定生成 2:生成しない
└ M2ZUnitZIP (DWORD) メール単位か添付毎のパスワード圧縮かの指定 0:メール 1:添付毎
└ M2ZEnvTo (DWORD) エンベロープの送信先条件 0:送信先のまま 1:送信元へ返信
└ M2ZEnvFromType (DWORD) エンベロープの送信元条件 0:送信者 1:指定アドレス
└ M2ZEnvFromAddr (文字列) エンベロープの送信元が指定アドレスの場合アドレス情報

■スパムチェック関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ spamcheck (DWORD) 実行の有無 0:しない,1:する
└ spamtag （文字列）挿入タグ
└ spamenglog (DWORD) スパムチェックのログ 0:しない,1:する
└ spamdate (DWORD) 日付ヘッダ異常によるスパム判定の有無 デフォルト値＝０：0:しない,1:する
└ spamspf1 (DWORD) 送信ドメイン認証（ＳＰＦ１）によるスパム判定の有無 デフォルト値＝０：0:しない,1:する

■チェックファイルサイズ上限

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ scanmaxsizehigh (DWORD) スキャン対象のファイルサイズ上限（上位32bit）デフォルト=0
└ scanmaxsizelow (DWORD) スキャン対象のファイルサイズ上限（下位32bit）デフォルト=0

■キャッシュ関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ httpcacheexpire (DWORD) HTTP キャッシュ有効期間（分）デフォルト0分
└ ftpcacheexpire (DWORD) FTP キャッシュ有効期間（分）デフォルト0分
└ sockscacheexpire (DWORD) SOCKS キャッシュ有効期間（分）デフォルト0分

■ソケット接続リトライ回数

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ httpconrtynum (DWORD) HTTP プロキシでのソケット接続失敗時のリトライ回数 デフォルト：10回
└ ftpconrtynum (DWORD) FTP プロキシでのソケット接続失敗時のリトライ回数 デフォルト：10回
└ smtpconrtynum (DWORD) SMTP プロキシでのソケット接続失敗時のリトライ回数 デフォルト：10回
└ pop3conrtynum (DWORD) POP3 プロキシでのソケット接続失敗時のリトライ回数 デフォルト：10回
└ socksconrtynum (DWORD) SOCKS プロキシでのソケット接続失敗時のリトライ回数 デフォルト：10回

■無通信タイムアウト関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ httpcltime (DWORD) クライアントからの受信タイムアウト時間 デフォルト：30000(ms)
└ httpsvtime (DWORD) サーバからの受信タイムアウト時間 デフォルト：30000(ms)
└ httpsslcltime (DWORD) 暗号化トンネリング時のクライアントからの受信タイムアウト時間 30000(ms)
└ httpsslsvtime (DWORD) 暗号化トンネリング時のサーバからの受信タイムアウト時間 30000(ms)
└ httpipverstion (DWORD) IPバージョン 0:IPv4,1:IPv6,2:併用
|
└ smtpcltime (DWORD) クライアントからの受信タイムアウト時間 デフォルト：30000(ms)
└ smtpsvtime (DWORD) サーバからの受信タイムアウト時間 デフォルト：30000(ms)
└ smtpsslcltime (DWORD) 暗号化トンネリング時のクライアントからの受信タイムアウト時間：30000(ms)
└ smtpsslsvtime (DWORD) 暗号化トンネリング時のサーバからの受信タイムアウト時間：30000(ms)
└ smtpipverstion (DWORD) IPバージョン 0:IPv4,1:IPv6,2:併用
|
└ pop3cltime (DWORD) クライアントからの受信タイムアウト時間 デフォルト：30000(ms)
└ pop3svtime (DWORD) サーバからの受信タイムアウト時間 デフォルト：300000(ms)
└ pop3sslcltime (DWORD) 暗号化トンネリング時のクライアントからの受信タイムアウト時間：30000(ms)
└ pop3sslsvtime (DWORD) 暗号化トンネリング時のサーバからの受信タイムアウト時間：30000(ms)
└ pop3ipverstion (DWORD) IPバージョン 0:IPv4,1:IPv6,2:併用
|
└ sockscltime (DWORD) クライアントからの受信タイムアウト時間 デフォルト：60000(ms)
└ sockssvtime (DWORD) サーバからの受信タイムアウト時間 デフォルト：600000(ms)
└ socksssslcltime (DWORD) 暗号化トンネリング時のクライアントからの受信タイムアウト時間：60000(ms)
└ socksssslsvtime (DWORD) 暗号化トンネリング時のサーバからの受信タイムアウト時間：60000(ms)
└ socksipverstion (DWORD) IPバージョン 0:IPv4,1:IPv6,2:併用

■FTP データポート範囲関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ ftpportstartrenge (DWORD) FTP データポート下限 デフォルト＝0
└ ftpportendrenge (DWORD) FTP データポート上限 デフォルト＝0
└ socksportstartrenge (DWORD) SOCKS 用 FTP データポート下限 デフォルト＝0
└ socksportendrenge (DWORD) SOCKS 用 FTP データポート上限 デフォルト＝0

■FTP 用(IPv6⇔IPv4 接続変換時)コマンド変換関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ ftpcmdconvert (DWORD) IPv6⇔IPv4 変換時に PORT⇔EPRT,PASV⇔EPSV を変換して送信する 0:する 1:しない デフォルト＝0

■HTTP 用 PICS-LABEL(セルフレイティング)フィルタ関連

HKEY_LOCAL_MACHINE
└ SOFTWARE
└ KTEC
└ Z_PROXY_SERVER
└ pics_use (DWORD) PICS-LABEL によるフィルタリングを有効にする 0:無効 1:有効 デフォルト＝0
└ pics_nude (DWORD) ヌード表現に関するフィルタレベル 0～4 0デフォルト＝0
└ pics_sex (DWORD) 性的表現に関するフィルタレベル 0～4 0デフォルト＝0
└ pics_violence (DWORD) 暴力的表現に関するフィルタレベル 0～4 0デフォルト＝0
└ pics_language (DWORD) 言語的表現に関するフィルタレベル 0～4 0デフォルト＝0
└ pics_other (DWORD) その他表現に関するフィルタレベル 0～3 0デフォルト＝0
└ pics_communication (DWORD) コミニュケーション関連に関するフィルタレベル 0～2 0デフォルト＝0

株式会社 ケイ･テック