ガードエクスプレス

操作説明書

有限会社メディアテック

http://www.guardexpress.com

～　目次　～

１．はじめに

ガードエクスプレスは社内ネットワークからの情報漏洩対策に有効なフォレンジックサーバ用プログラムです。
ネットワーク内のすべての通信データを常に記録・保存することで内部の不正行為を抑止し、万一漏洩が発生した場合は漏洩者の特定証拠保全に威力を発揮します。
日本版 SOX 法や新会社法で要求されている「IT による内部統制」や情報漏洩対策として、「抑止」「監査」「証明」「記録」「証拠保全」に威力を発揮します。

１－１．導入の為の動作環境

弊社が推奨する「メールエクスプレス」動作環境については、下記をご参照ください。

ＯＳ	Windows2000/XP/Vista/Server
ＣＰＵ	CPU：Pentium 2.0GHz 以上推奨
メモリ	2.0GB 以上推奨
ＨＤＤ	250GB 以上推奨

「ガードエクスプレス」導入の前に NET Framework 3.5 を WindowsUpdate からインストールして下さい。

１－２．インストール

ダウンロードしたZIPファイルを展開し、その中のSetup アイコンをクリックするとインストールが始まります。完了するとデスクトップにショートカットが作成され、ダブルクリックするとライセンスDIALOG が現われるので‘同意’ボタンを押すとプログラムが開始されます。
プログラムをダウンロードして試用された後、製品版をご購入される場合はユーザー登録と認証キーが必要になります。
登録するにはE-mail(sales@guardexpress.com)又はFax(0185-89-5572)でプロダクトID と連絡可能な電話番号をお知らせ下さい、こちらから電話で確認を取らせて頂いた後に認証キーと御請求書をお送り致します。

１－３．バージョンアップ

登録ユーザーは当社ホームページから最新バージョンを自由にダウンロードしてバージョンアップを行うことが出来ます、重大なバグ修正などが行われた時はE-mail等でお知らせいたします。

２．プログラム起動

プログラムの起動後何らかの操作を行う場合は目的に応じて管理ユーザーまたは閲覧ユーザーでログインして下さい。ログイン前は何の操作もできないようになっています。

２－１．ログイン

２－２．操作パネル

[運転モード]
起動時は“PROGRAM.INI”で設定されたモードで起動されます。
起動後のモードの変更は管理ユーザーでログインしている場合のみ可能です。
モードが自動の場合はスケジュールに従って開始／停止が行われます。

[開始／停止]
開始・停止ボタンは手動モードでのみ操作可能です。

[監視／総検出アドレス数]
監視中のアドレス数と検出された総アドレス数が表示されます、ライセンスによって最大監視可能数が制限される為この２つの値は異なる場合があります。

[監視プロトコル]
現在監視対象となっているプロトコルが表示されます。

[DISK 使用率]
キャッシュの未処理件数とログフォルダの使用率が表示されます。
キャッシュの未処理件数が常に大きな値になっている場合はシステム設定値“PROGRAM.INI”を調整する必要があります。

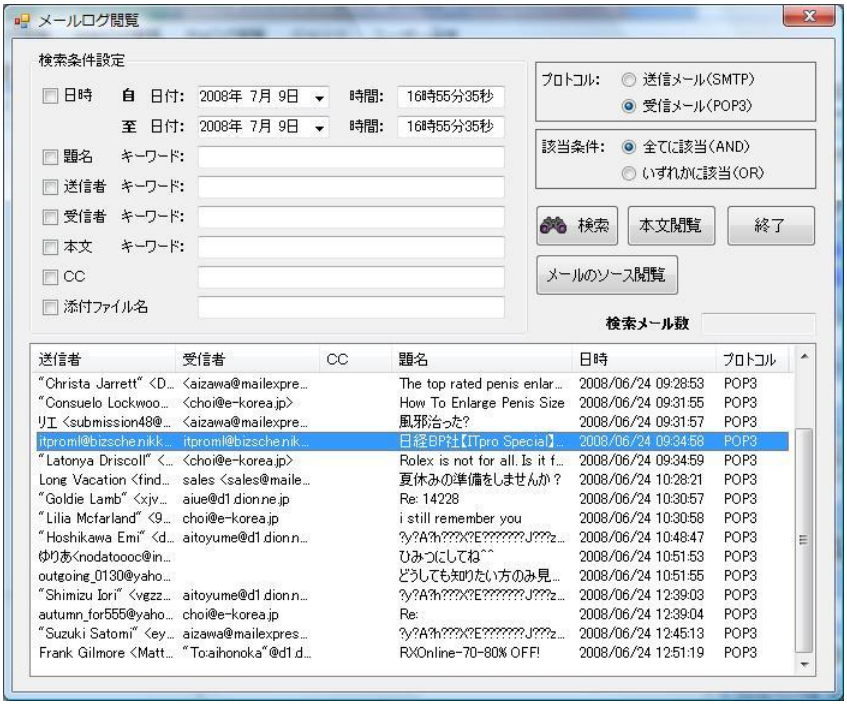
[ユーザー権限]
現在ログイン中のユーザー権限を表示します、ログインしていない状態では空白になっています。

[表示／無し]
パケットのキャプチャリング状態を表示します、CPU のオーバーヘッドが大きいため必要のない時は無し(非表示)にして下さい。

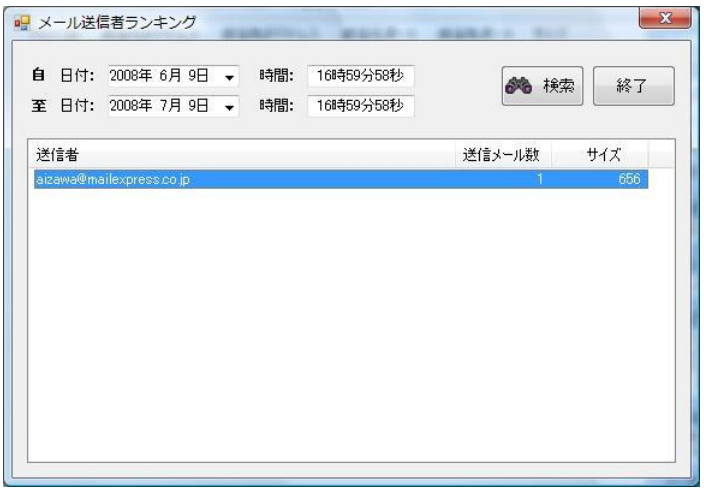
３．Mail ログ閲覧

メールログの検索と閲覧を行います。
ログの検索は様々な条件を指定することで効率よく行うことが可能です、検索フォルダ設定で設定されたフォルダが検索対象となります。

３－１．Mail ログ検索



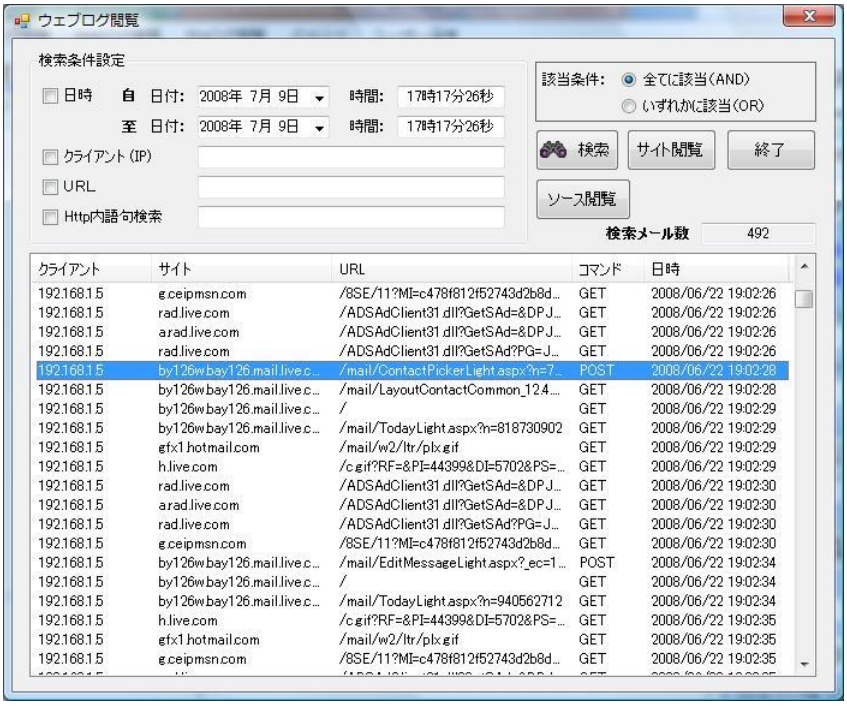
３－２．Mail 送信者ランキング



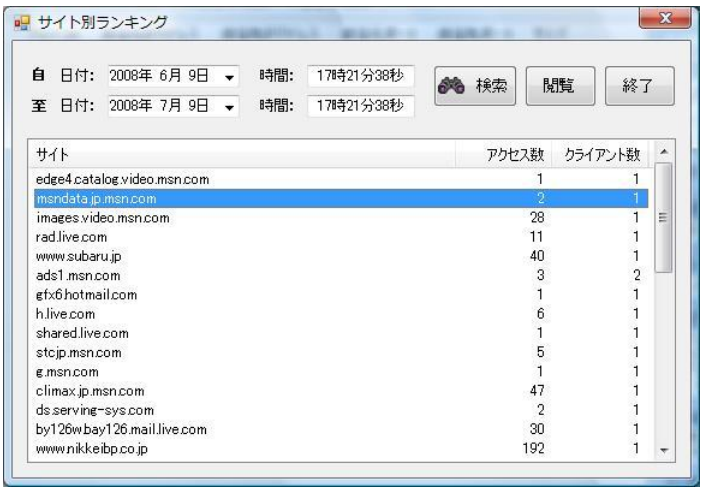
４．Web ログ閲覧

Web ログの検索と閲覧を行います。
ログの検索は様々な条件を指定することで効率よく行うことが可能です、検索フォルダ設定で設定されたフォルダが検索対象となります。

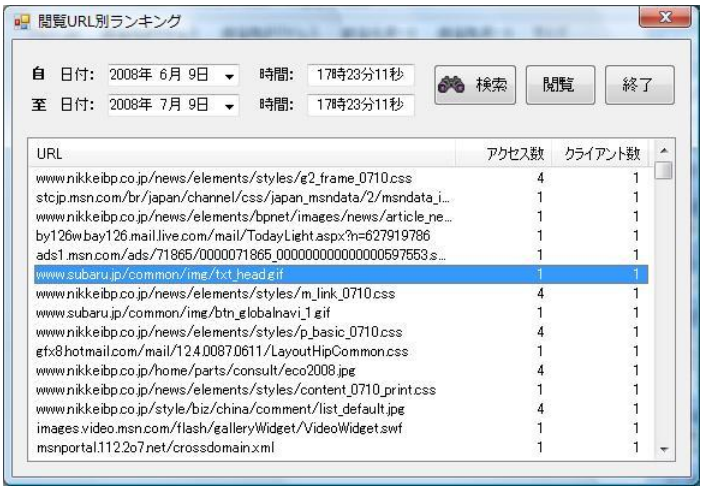
４－１．Web ログ検索



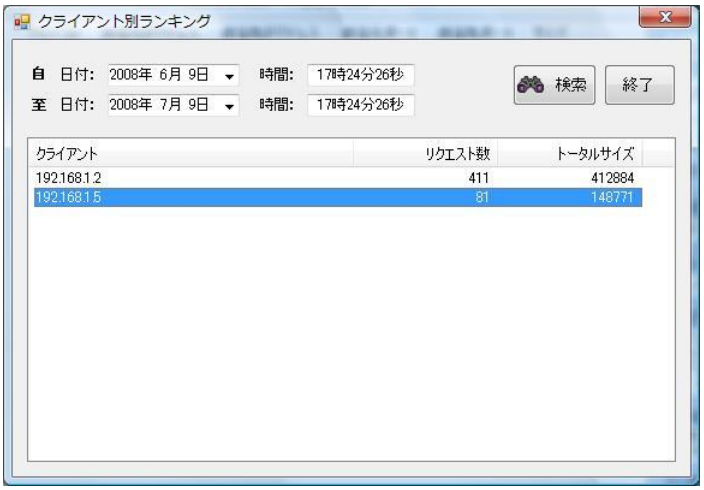
４－２．サイト別ランキング



４－３．閲覧 URL 別ランキング



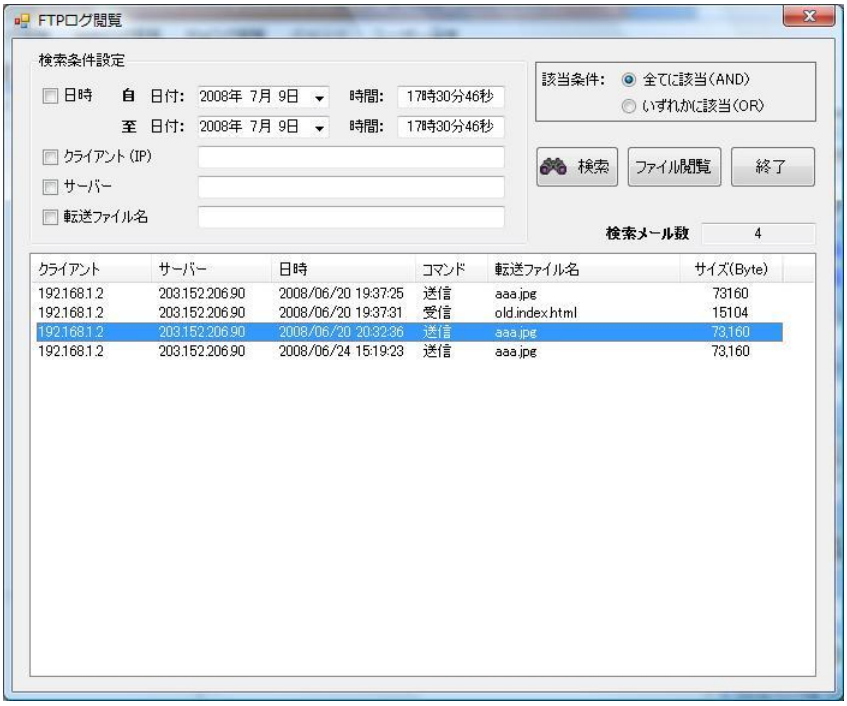
４－４．クライアント別ランキング



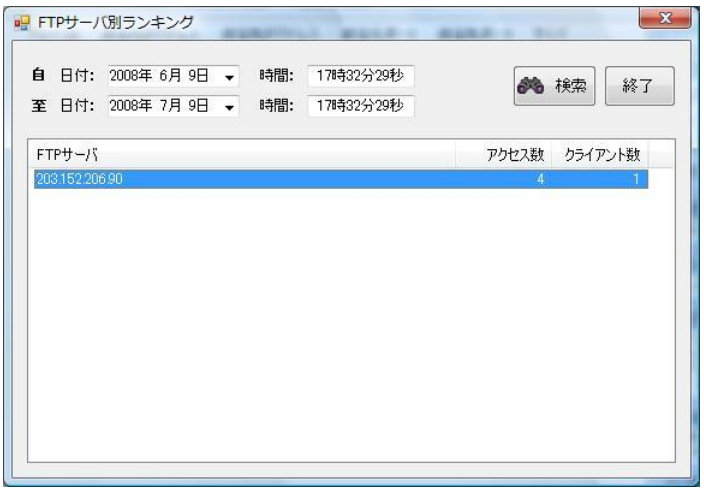
５．Ftp ログ閲覧

Ftp ログの検索と閲覧を行います。
ログの検索は様々な条件を指定することで効率よく行うことが可能です、検索フォルダ設定で設定されたフォルダが検索対象となります。

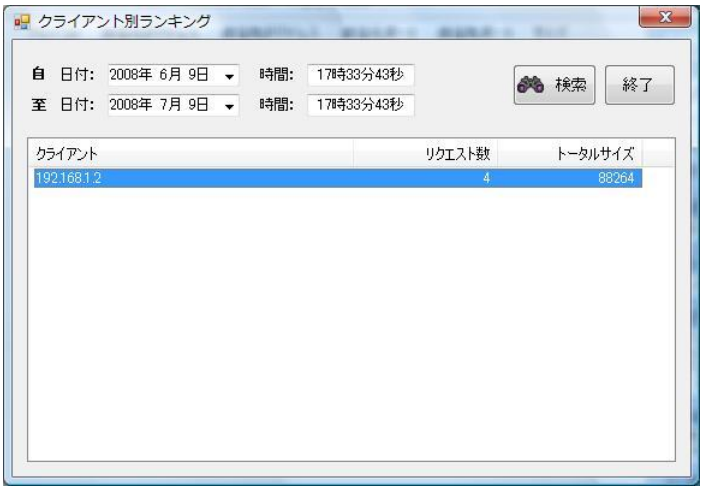
５－１．Ftp ログ検索



５－２．Ftp サーバ別ランキング



５－３．クライアント別ランキング



６．環境設定

導入後、最初に行う必要があります。
ネットワーク設定、スケジュール設定、ログフォルダ設定、検索フォルダ設定、ポート番号設定の順で全ての項目を確認して下さい、基本的な設定はデフォルト値として設定されていますので変更する項目のみを設定し直して下さい。

６－１．ネットワーク設定

キャプチャーデバイス

キャプチャーを行うネットワークカードを選択して下さい。

監視対象プロトコル

監視を行うプロトコルを選択して下さい、必要のないプロトコルを監視対象から外すことでDISK容量を節約できます。

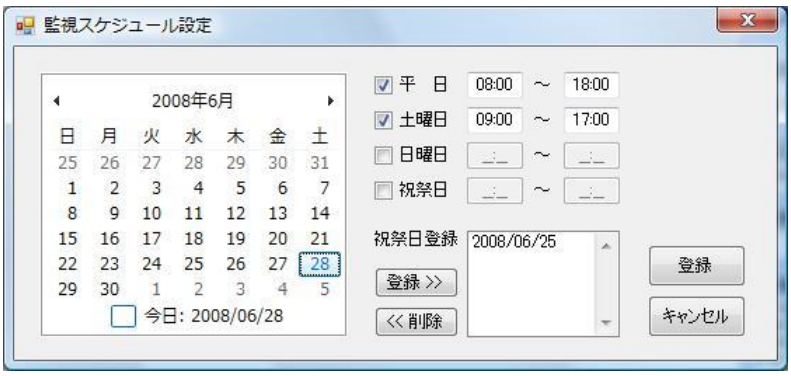
監視対象アドレス

監視対象とするIPアドレスを4つのグループで指定することが出来ます。またチェックを全て外すことで全てのIPアドレスを監視対象とする事が出来ますが、無駄な監視を行わない為にもチェックを指定することをお勧めします。

除外IPアドレス

自PCのキャプチャーデバイスに割り当てられたアドレスは監視対象から外す事が出来ます。また除外IPアドレスは監視対象アドレスで指定した範囲内に有っても監視対象から外されます。

６－２．スケジュール設定



平日、土曜日、日曜日、祝祭日

チェックの付いた日の指定された時間帯が監視の対象となります（自動モードの場合）。

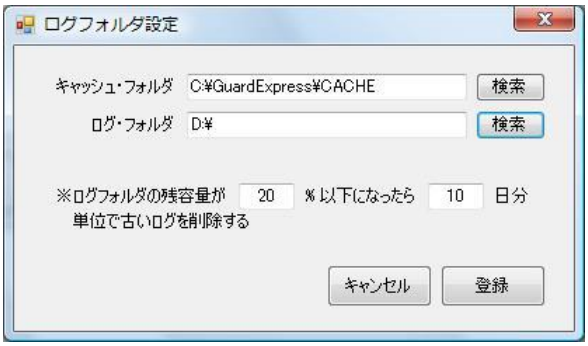
祝祭日登録

祝祭日の年月日をあらかじめ登録します。ここで登録された日は祝祭日のチェックがオフの場合は監視対象から外され、オンの場合は監視対象となります。

カレンダー

祝祭日を登録する際に使用します。

６－３．ログフォルダ設定



キャッシュ・フォルダ

キャプチャされたパケットが一時的に保管されるフォルダです、通常はデフォルトの設定で使用して下さい。

ログ・フォルダ

解析されたパケットがログとして保管されるフォルダです、通常は大容量のHDDなどを指定します。

ログフォルダの残容量

ログフォルダの残容量が少なくなった場合に容量を確保するため古いログを削除しますが、その際の条件を設定します。

６－４．検索フォルダ設定

ログ・フォルダ

ログフォルダ設定で指定されているフォルダが表示されます。検索対象とする場合はチェックをオンにします。

検索フォルダ１、２

バックアップしたDVD,Blu-rayディスク等をマウントした状態で検索を行う場合などに指定します。

６－５．ポート番号設定

HTTP

HTTPのポート番号を2種類指定できます、通常はデフォルトのままで使用して下さい。

POP3,SMTP

POP3,SMTPのポート番号を指定します。SMTPは2種類指定できます。

FTP,FTP-Data

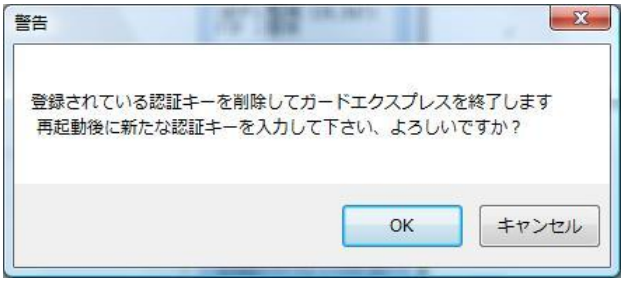
FTPのポート番号を指定します。パッシブモードにも対応しています。

６－６．プロダクト ID

このメニューは有料版でのみ表示されます。
プロダクト ID の参照と認証キーの再登録が可能です、認証キー再登録はライセンスのアップグレードの時などに使用されます。

[プロダクト ID 参照]

[認証キー再登録]



７．ユーザー設定

管理ユーザー、閲覧ユーザーの登録を行います。
登録は管理ユーザーのみが行うことが出来ます、システムに最低１人の管理ユーザーが必要です。
インストール直後はデフォルトで“admin”ユーザーが登録されています、パスワードも“admin”です。

７－１．ユーザー登録

７－２．パスワード変更