

GIDEON

ユーザーズ
ガイド

GIDEON
AutoCrypto

The logo graphic consists of a blue triangle pointing up and to the right, and a dark grey triangle pointing down and to the right, overlapping the blue one.

for Linux

ギデオン

AutoCrypto 操作ガイド

目次	
第1章 管理GUI操作	4
1.1 管理GUI用サービス起動と停止	4
1.2 管理・設定画面のアクセス方法	4
1.3 ログイン	5
1.4 初期設定	7
1.5 TOP画面	10
1.6 全体設定	12
1.6.1 基本設定	13
1.6.2 承認	15
1.6.3 ID管理	17
1.6.4 ホワイトリスト	19
1.6.5 チェックリスト	21
1.6.6 ライセンス	22
1.6.7 SMTPサーバの設定	23
1.6.8 更新環境の設定	24
1.7 サポート画面	25
第2章 承認GUI操作	28
2.1 承認の流れ	28
2.2 承認GUI画面のアクセス方法	29
2.3 ログイン	30
2.4 承認操作	31
お問い合わせ	36

1.1 管理GUI用サービス起動と停止

[注意] 従来製品で管理GUIを起動されている場合はこの項目の操作は不要です。

管理画面を利用するためのサービスを起動するには、インストール後、root権限でログインし、以下のイタリック部分のコマンドを実行します。

```
# /usr/local/gwav/gwav-gui-control
==== GUI setting ====
  Use web-interface for anti-virus (Yes/No) [No]: y
Starting mini_httpd:                [ OK ]
Starting mini_httpsd:               [ OK ]
```

このサービスを停止するには、上記「*y*」に替わり「*n*」を入力します。

1.2 管理・設定画面のアクセス方法

クライアントPCから本製品がインストールされたシステムのGUI管理画面にアクセスします。WEBブラウザのアドレスバーで、以下のようにシステムのホスト名またはIPアドレスとポート番号(777)とサイト名(ac)を指定します。

<http://antivirus.gideon.co.jp:777/ac/>

※ホスト名がantivirus.gideon.co.jpの場合

セキュリティが気になる場合は、HTTPSでポート番号(999)を指定します。

<https://antivirus.gideon.co.jp:999/ac/>

※ホスト名がantivirus.gideon.co.jpの場合

※ お使いのWEBブラウザおよびファイヤーウォールで、上記のポート番号を許可するように設定してください。また上記ポートにアクセスするには、本製品インストール後に、前項に記した操作によりシステム上で必要スクリプトを実行し、ウェブサーバサービスを起動させておく必要があります。

1.3 ログイン

管理・設定画面にアクセスすると、画面1.1 ログイン画面が表示されます。既存製品にて初回のログインで設定したパスワードを入力します。パスワード入力後 [ログイン] ボタンをクリックします。



画面1.1

パスワードの変更

画面1.1 ログイン画面で既存のパスワードを入力して [変更] ボタンをクリックすると、画面1.2 パスワード入力画面が表示されます。

ここでパスワードを再設定します。(半角英数20文字以内)



画面1.2

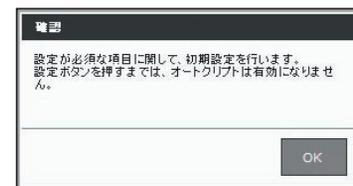
1.4 初期設定

初回ログインの際には画面1.3 使用許諾画面が表示されます。



画面1.3

この画面の記載条項をお読みいただき、承諾いただける場合は[承諾する]ボタンをクリックして、さらにポップアップして表示される画面1.4にて[OK]ボタンをクリックして初期設定画面(画面1.5)に進んでください。



画面1.4

初期設定

ライセンス設定
 お客様登録No.
 パスワード

利用メールアドレスのホスト名 (@含む)

<例>
 info@gideon.co.jpの場合: f@gideon.co.jpと登録

SMTPサーバの設定
 ホスト名 ポート番号
 認証方法
 ユーザー名 パスワード

本製品のライセンス設定です。ライセンス証に正しい認証してください。ライセンス証が存在しない場合は、そのまま利用下さい。試用版としてご利用いただける場合は、インストール後、必ず登録解除です。
 『全件設定/ライセンス』でも同様の設定が可能です。

ここで登録したホスト名が含まれるメールアドレスのみが宛先化対象となります。
 『全件設定/チェックリスト』でも同様の設定が可能です。

本製品がメールを送信する際に利用するSMTPサーバの設定です。
 『全件設定/SMTPサーバ』でも同様の設定が可能です。

画面1.5

初期設定画面では次の項目を設定します。

[注意] ここで設定する項目は製品利用開始後にも管理GUIから設定可能です。

ライセンス設定

本製品のライセンス設定を行います。ライセンス証書の記載に従い、お客様登録No.とパスワードを入力してください。

なお、すでにギデオン製品がインストールされている場合は本項目に表示されている情報からの変更は不要です。

利用メールアドレスのホスト名

本製品をご利用いただくメールアカウント、或いはドメインを限定される場合はこの項目に登録してください。

なお、この項目を登録しない場合は全ての送信メールが処理対象となります。また、この項目に設定した内容は他のギデオン製品機能(アンチウイルス、アンチスパムなど)には影響がありません。

SMTPサーバの設定

本製品がメールを送信する際に利用するSMTPサーバの設定です。

SMTPサーバのホスト名(或いはIPアドレス)、ポート番号、認証が必要なら認証方法と認証ユーザー名/パスワードを登録してください。

なお、すでにギデオン製品がインストールされている場合は本項目に表示されている情報からの変更は不要です。

1.5 TOP画面

「TOP」タブをクリックすると、画面1.6が表示されます。



画面1.6

[再読み込み]ボタン :

暗号化ログ、状況や監視イベントの表示を最新にする場合にクリックします。

[ログアウト]ボタン :

管理GUIから再度ログイン画面に戻る場合にクリックします。

動作状況 :

ONはサービス稼働中、OFFはサービス停止中です。動作状況表示ボタンをクリックすると、動作切り替えウインドウがポップアップし、サービスのON/OFFを切り替え可能です。

●**暗号化ログ** (画面1.6 上段部分)

メール暗号化を行った日時、メール暗号化のID、送信元アドレス、暗号化ファイ

ル名などの情報をログに出力します。

なお、表の各項目名(No.、日時、AUTOCRYPTO-ID、From、送信)の部分をクリックすると、項目別に表をソートすることが可能です。

[自動更新]ボタン :

このボタンをクリックすると、ボタンの色が **自動更新** と変化し、10秒ごとにログ表示を更新します。

[ダウンロード]ボタン :

このボタンをクリックすると、リアルタイム監視ログをcsv形式でダウンロードすることができます。

●**暗号化ログファイル** (画面1.6 下段部分)

ここでは暗号化処理の詳細ログを表示します。

1.6 全体設定

画面1.6上段左部の[全体設定]ボタンをクリックすると、画面1.7がポップアップウィンドウとして表示されます。

この画面では暗号化ファイルの名称、解凍パスワード、承認方法、暗号化対象のメールアドレスなどを設定します。

画面1.7

設定項目の詳細を以下にご案内します。

1.6.1 基本設定

[全体設定]ボタンをクリックした直後、あるいは[基本設定]タブを選択することにより表示される画面1.4上で、暗号化ファイル名の名称、解凍パスワードの形式、暗号化を行うメールを自動選択するフィルタの設定が行えます。

1.6.1.1 暗号化ファイル名

暗号化した後の添付ファイル名の形式を設定します。

ファイル名の設定では以下のマクロが利用できます

- \$(filename) メール内の最初のファイル名
- %Y 現在の西暦年(4桁)
- %y 現在の西暦年(下2桁)
- %m 現在の月(2桁)
- %d 現在の日(01~31)
- %H 現在の時(00~23)
- %M 現在の分(00~59)
- %S 現在の秒(00~59)
- %% 文字

<例>

現在日時が2012年1月4日9時30分の場合

%Y%m%d%H%M.zip → 201201040930.zip

1.6.1.2 暗号化ファイルパスワード

暗号化ファイルのパスワードを設定します。

「暗号化ファイルパスワード」の欄には固定の文字列、および\$(1)~\$(16)というマクロを利用して設定します。

<例>

「gideon\$(10)」と設定した場合

パスワード名: gideon(任意の10桁の文字列)

また、「マクロで展開されるランダムな文字集合の種類」の欄では文字列を英数のみにするか、或いは英数記号にするかを選択できます。

1.6.1.3 パスワード通知メールの件名

パスワード通知メールの件名を固定の文字列、および\${subject}というマクロを利用して設定します。

<例>

「[パスワード] \${subject}」と設定した場合

パスワード記述メールの件名: [パスワード](送信したメールの件名)

1.6.1.4 最大サイズ

暗号化する際のメールの最大サイズをMbyte単位で設定します。このサイズを超えたメールは暗号化を行いません。

1.6.1.5 非暗号化対象メールのフィルタ設定

「非暗号化サブジェクト」の欄に指定した文字列に、メールの件名が前方一致した場合、添付ファイルの暗号化を行いません。

また「非暗号化行」の欄に指定した文字列にメール本文中の『行』が完全一致した場合、暗号化を行いません。

1.6.2 承認

画面1.7上で、「承認」タブを選択することにより表示される画面1.8上で、承認モードとデフォルトテンプレートを設定します。



画面1.8

1.6.2.1 承認モードの選択

パスワード通知メールを送信する際の承認の要否と承認を誰が行うかのモードをラジオボタンにより次の3つから選択します。

- 1) 承認なしモード(パスワード送信を10秒後に自動で行います)
- 2) 自己承認モード(パスワード送信の許可を、自分自身で行います)
- 3) 承認依頼モード(パスワード送信の許可を、『承認者』にお願いします)

[注意] 1)以外のモードを選択した場合は後述のID登録を行わないとパスワード通知メールが送信されませんのでご注意ください。

1.6.2.2 デフォルトテンプレート

承認されたパスワード通知メールは、本テンプレートの内容に従ってメール本文を作成し、送付します。

ただし、『承認ID管理』にて設定された個別テンプレートが存在する場合には、そちらを優先して利用します。

本テンプレートには、以下のマクロを利用することができます。

- ・ `#{password}` 暗号化ファイルのパスワード
- ・ `#{from}` 送信者(envelope from)
- ・ `#{subject_decode}` 元メールの件名
- ・ `#{date}` 元メールの時刻
- ・ `#{message-id}` 元メールのMessage-Id
- ・ `#{filename}` 暗号化ファイルのファイル名
- ・ `#{md5}` 暗号化ファイルのMD5値
- ・ `#{autocrypto-id}` 製品が付加するID

<テンプレート設定例>

```

いつもお世話になっております。ギデオンです。

下記のメールでお送りしました添付ファイルの
開封パスワードをお知らせ致します。

パスワード:#{password}

よろしく御願ひ申し上げます。

-----送信済メール-----

From:      #{from}
Subject:   #{subject_decode}
Date:      #{date}

+-----+
株式会社 ギデオン
〒2230056横浜市港北区新吉田町3382-7
TEL045-590-1216 FAX045-590-1217
E-mail: info@gideon.co.jp
URL: http://www.gideon.co.jp/
    
```

1.6.3 ID管理

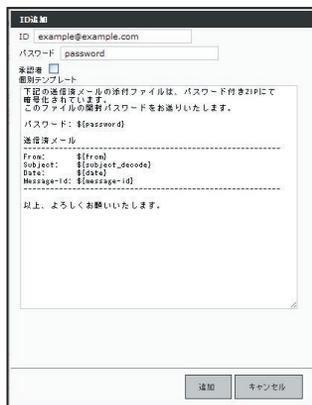
画面1.7上で、[ID管理]タブを選択すると、画面1.9が表示されます。この画面上では承認や個別テンプレートを利用するためのID、承認GUIアクセスのためのパスワード、利用するテンプレート登録と承認依頼のための『承認者』を指定できます。



画面1.9

1.6.3.1 ID追加

[追加]ボタンをクリックすると、画面1.10が表示されます。画面1.10上で承認が必要なメールアドレス、後述の承認GUIへのログインパスワード、『承認者』の指定を設定します。



画面1.10

また、同画面上ではパスワード通知メールのテンプレートを個々に設定できます。ここで個別テンプレートを設定した場合、デフォルトテンプレートより優先して利用されます。個別テンプレートでは、デフォルトテンプレートと同様に、以下のマクロを利用することができます。

- ・ \${password} 暗号化ファイルのパスワード
- ・ \${from} 送信者(envelope from)
- ・ \${subject_decode} 元メールの件名
- ・ \${date} 元メールの時刻
- ・ \${message-id} 元メールのMessage-Id
- ・ \${filename} 暗号化ファイルのファイル名
- ・ \${md5} 暗号化ファイルのMD5値
- ・ \${autocrypto-id} 製品が付加するID

1.5.3.2 承認ID編集

ID管理の表中の各行をクリックすると、画面1.10が表示され、ID追加と同様に設定内容を編集できます。

1.6.4 ホワイトリスト

画面1.7上で、[ホワイトリスト]タブを選択すると、画面1.11が表示されます。この画面上で指定した送信元や送信先のメールアドレスを含むメールに対してはメール暗号化を行いません



画面1.11

タイプ指定には以下があり、メールアドレスかメールアドレスの『@』以降を記述できます。

- from= envelope fromと一致
- to= envelope toと完全一致
- to*= 複数のenvelope to中、1つでも一致

<例>

- ・ @example.comが含まれるenvelope fromは暗号化しない。
from=@example.com
- ・ info@example.jpが唯一のenvelope toの場合は暗号化しない。
to=info@example.jp
- ・ 複数への宛先送信中、1つでもadmin@example.jpが含まれた場合は暗号化しない。
to*=admin@example.jp

[オートクリプト機能を利用しているMTAがsendmailの場合の注意事項]

外部メール配信に関しては、メールアドレスをそのままホワイトリストに記述していただいて構いません。

しかし、本製品が導入されているサーバ宛のメールアドレスを指定する場合には、ホスト部分を@localhostに変更してください。

具体的には、example.comにオートクリプト機能が導入されている場合、to=user@example.comではなく、to=user@localhostと記述します。

to*についても同様です。

1.6.5 チェックリスト

画面1.7上で、[チェックリスト]タブを選択すると、画面1.12が表示されます。この画面上で記述されたアドレスがenvelope fromに含まれる場合に暗号化を行います。



画面1.12

1行内にメールアドレス、もしくはメールアドレスの『@』以降を記述します。記述がない場合は、全てのメールが暗号化対象となります。

<例>

- ・ info@example.com、もしくは@example.jpが後方一致するアドレスのみ暗号化する。
info@example.com
@example.jp

1.6.6 ライセンス

画面1.7上で、[ライセンス]タブを選択することにより表示される画面1.13上で、ユーザ登録時に発行された「お客様登録No.」と「パスワード」を入力します。

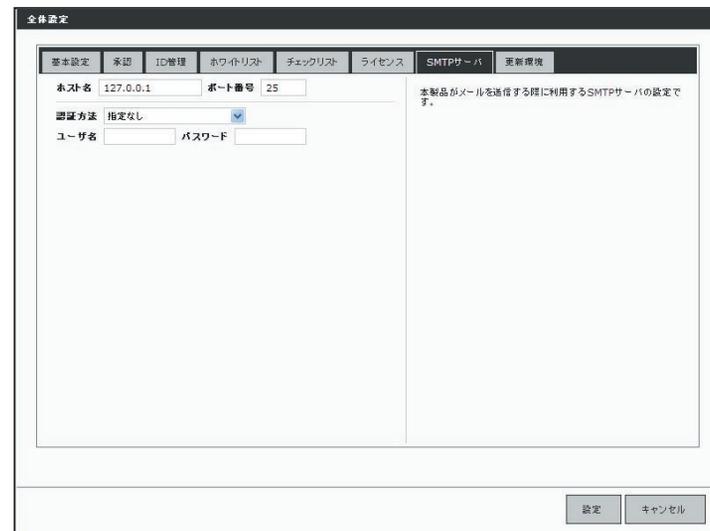


画面1.13

1.6.7 SMTPサーバの設定

画面1.7上で、[SMTPサーバ]タブを選択することにより表示される画面1.14上で、通知メールなどを送信するために使うメール(SMTP)サーバとメールサーバ利用に認証が必要であれば、認証方法、認証ユーザ名とパスワードを指定します。

ホスト名については、例えば、自社の正式なメールサーバ名(FQDN)が、mail.domain.jpであればそのメールサーバ名を指定します。また、メールサーバ内に本製品をインストールした場合は「127.0.0.1」で構いません。



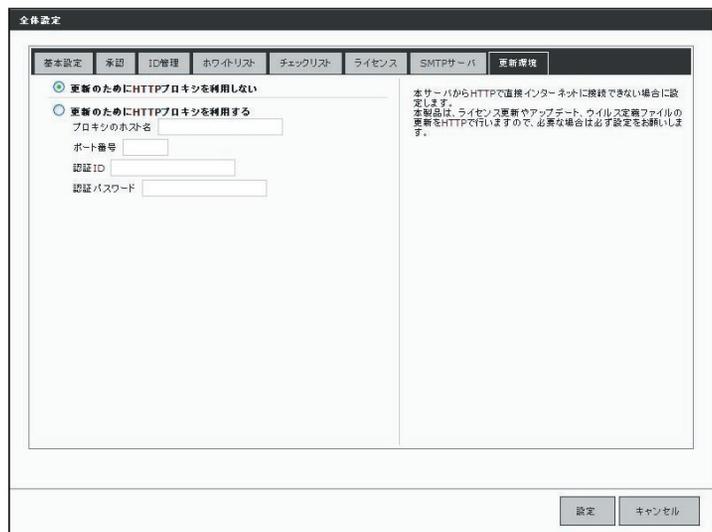
画面1.14

1.6.8 更新環境の設定

画面1.7上で、[更新環境]タブをクリックすると、画面1.15が表示されます。

本製品は外部HTTPサイトにアクセスすることで、モジュールおよび定義ファイルを更新します。特定のHTTPプロキシサーバを経由しないと外部のURLにアクセスできない場合には、「更新のためにHTTPプロキシを使用する」を選択してください。

「プロキシのIPアドレス」「ポート番号」は必須項目です。
「ID」「パスワード」が設定されている場合には、それぞれ入力が必要です。



画面1.15

1.7 サポート画面

「サポート」タブをクリックすると、画面1.13が表示されます。



画面1.16

「再読み込み」ボタン :

稼働状況やウイルス定義ファイル更新ログの表示を最新にする場合にクリックします。

「ログアウト」ボタン :

管理GUIから再度ログイン画面に戻る場合にクリックします。

最新のバージョン情報

製品モジュールとアンチウイルスエンジンの定義ファイルの現在のバージョンが表示されます。

製品モジュールの[手動更新]ボタン :

[手動更新] ボタンをクリックすると、その時点で最新のモジュール(修正パッチモジュール、アップデートモジュールなど)の取得を行います。既に更新済みの場合は新たに更新されません。

自動更新の頻度は、初期設定では1日1回の更新に設定されています。緊急対策が必要な場合は手動更新を行ってください。

稼働状況

1時間おきに実施される製品稼働チェックの結果が表示されます。

ウイルス定義ファイル更新ログ履歴

1時間おきにウイルス定義ファイル更新動作の結果が表示されます。但し、配布元サーバが更新されていないなどの理由で定義ファイル配布元サーバと製品内にダウンロードされている定義ファイルが同一の場合の更新動作については表示されませんのでご了承下さい。

ウイルス定義ファイルの[手動更新]ボタン

[手動更新] ボタンをクリックすると、その時点で最新の定義ファイルの取得を行います。既に更新済みの場合は、新たに更新されません。

自動更新の頻度は、1時間毎に設定されています。緊急対策が必要な場合は手動更新を行ってください。

自己承認モード、或いは承認依頼モードを選択した場合、承認GUI画面からパスワード通知メールの送信承認の操作を行えます。

本章では承認の流れと承認GUIの操作方法をご案内します。

2.1 承認の流れ

自己承認モードと承認依頼モードでそれぞれの承認の流れは次の通りです。

[自己承認モード]

添付ファイル付きメール送信
↓
送信先に添付ファイルが暗号化されたメールが届く
↓
送信元ID(メールアドレス)で承認GUIにログインし、『送信』ボタンをクリック
↓
送信先にパスワード通知メールが届く

[承認依頼モード(承認される場合)]

添付ファイル付きメール送信
↓
送信先に添付ファイルが暗号化されたメールが届く
↓
送信元ID(メールアドレス)で承認GUIにログインし、『承認依頼』ボタンをクリック
↓
承認者に承認依頼メールが届く
↓
承認者ID(メールアドレス)で承認GUIにログインし、『承認する』ボタンをクリック
↓
送信先にパスワード通知メールが届く

[承認依頼モード(承認されない場合)]

添付ファイル付きメール送信
↓
送信先に添付ファイルが暗号化されたメールが届く
↓
送信元ID(メールアドレス)で承認GUIにログインし、『承認依頼』ボタンをクリック
↓
承認者に承認依頼メールが届く
↓
承認者ID(メールアドレス)で承認GUIにログインし、『承認しない』ボタンをクリック
↓
送信元に非承認メールが届く

2.2 承認GUI画面のアクセス方法

個々のクライアントPC、或いはスマートフォンやタブレットなどのモバイルデバイスから承認GUI画面にアクセスします。WEBブラウザのアドレスバーで、以下のようにシステムのホスト名またはIPアドレスとポート番号(777)とサイト名(approve)を指定します。

<http://antivirus.gideon.co.jp:777/approve/>

※ホスト名がantivirus.gideon.co.jpの場合

セキュリティが気になる場合は、HTTPSでポート番号(999)を指定します。

<https://antivirus.gideon.co.jp:999/approve/>

※ホスト名がantivirus.gideon.co.jpの場合

※ お使いのWEBブラウザおよびファイヤーウォールで、上記のポート番号を許可するように設定してください。

2.3 ログイン

承認GUI画面にアクセスすると、画面2.1のログイン画面が表示されます。ここで先に管理GUIから登録しておいた承認IDとパスワードを入力した上で、[ログイン]ボタンをクリックしてログインを行います。

※PCのブラウザからアクセスした場合



画面2.1

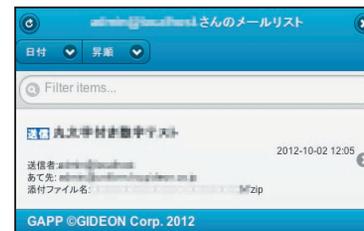
※スマートフォンのブラウザからアクセスした場合



画面2.2

2.4 承認操作

承認GUI画面にログインすると、画面2.3の承認待ちパスワード通知メールリストが表示されます。



画面2.3

画面2.3上でリスト右部にある▶をクリックすると、選択されたメールについて、自己承認モードの場合は送信承認画面、承認依頼モードの場合は承認依頼画面が表示されます。

[自己承認モードの場合]



画面2.4

画面2.4上でパスワード通知メールの送信を承認する場合は[送信]ボタンをクリックしてください。

続いて画面2.5のメール送信の確認画面が表示されますので、ここで [はい] を選択すると指定された宛先にパスワード通知メールが送信されます。



画面2.5

また、パスワード通知メールの送信を承認しない場合は[削除]ボタンをクリックすると、パスワード通知メールは送信されず、破棄されます。

[承認依頼モードの場合]



画面2.6

画面2.6上でパスワード通知メール送信の承認処理を承認者に依頼をする場合は[承認処理を依頼]ボタンをクリックしてください。

続いて画面2.7の承認依頼確認画面が表示されますので、ここで複数の承認者が登録されている場合はプルダウンメニューより承認依頼先IDを選択して [はい] をクリックすると指定された承認者に承認依頼メールが送信されます。



画面2.7

承認依頼メールを受け取った承認者は承認者IDで承認管理GUIにログインすると、画面2.8の承認待ちリストが表示されます。



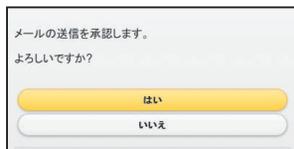
画面2.8

承認者は画面2.8上でリスト右部にある「承認」をクリックすると、選択されたメールについて、画面2.9のパスワード通知メール送信承認画面が表示されます。



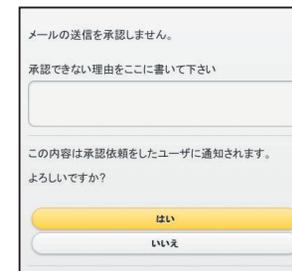
画面2.9

画面2.9上で承認者が承認する場合は[承認する]ボタンをクリックし、引き続き、画面2.10の承認確認画面が表示されますので、ここで[はい]を選択するとパスワード通知メールが送信先に送付されます。



画面2.10

一方、画面2.9上で承認者が承認しない場合は[承認しない]ボタンをクリックし、引き続き、画面2.11の非承認確認画面が表示されますので、ここで承認できない理由を記載した上で[はい]を選択すると、非承認通知メールが送信元に送付されます。



画面2.11

お問い合わせ

■ お問い合わせ

株式会社 ギデオン

〒223-0056横浜市港北区新吉田町3382-7

<http://www.gideon.co.jp/>

●サポートセンター(技術のお問合せ)

E-mail: sp@gideon.co.jp TEL 045-590-3655

●インフォメーションセンター(その他のお問合せ)

E-mail: info@gideon.co.jp TEL 045-590-1216

受付時間/9:00～17:00(祝祭日を除く、月～金)

ギデオン AutoCrypto
操作ガイド

2012年10月5日 初版発行

発行所 株式会社ギデオン

〒223-0056

神奈川県横浜市港北区新吉田町3382-7

<http://www.gideon.co.jp/>

本誌からの無断転載を禁じます。

乱丁、落丁はお取替え致します。上記発行所までご連絡下さい。

Copyright(c)2012 GIDEON Corp.

Printed in Japan