



Guard

ユーザ ガイド



Guard: ユーザ ガイド

発行日 火曜日, 12. 7 月 2016 バージョン 2.4.2.0

製作著作 © 2016-2016 OX Software GmbH , このドキュメントは OX Software GmbH の知的所有物です。

このドキュメントの全部または一部をコピーする場合、各コピーにこの著作権情報を明記する必要があります。このドキュメントの内容は細心の注意を払って編集されていますが、情報の誤りを完全に排除することはできません。OX Software GmbH、著者、および翻訳者は、記述の誤りとそれによって生じる結果について、いかなる責任も負うものではありません。このドキュメントで使用されるソフトウェアの名称およびハードウェアの名称は登録商標である可能性があり、無償での使用が保証されているものではありません。OX Software GmbH は原則的に、製造元によるつづりの表記に従います。このドキュメントでは（注釈を付記せずとも）ブランド名、商標、ロゴなどを使用していますが、（商標とブランド名に関する法律により、）これらのブランド名等を無償で使用できることを示すものではありません。

目次

1 このドキュメントについて	5
2 Guardの概要	7
3 使用説明Guard	9
3.1 セットアップGuard	10
3.2 メールやり取りを暗号化する	11
3.2.1 暗号化されたメールの閲覧	11
3.2.2 暗号化されたメールの送信	11
3.2.3 外部の宛先はどのように暗号化されたメールを閲覧するのか?	12
3.3 ファイルの暗号化	13
3.3.1 ファイルの暗号化	13
3.3.2 新しい暗号化ファイルの作成	13
3.3.3 暗号化ファイルを開く	13
3.3.4 暗号化ファイルのダウンロード	14
3.3.5 ファイルの復号	14
3.4 サインアウトGuard	15
3.5 Guard設定	16
3.5.1 Guardセキュリティ設定	16
3.5.2 PGP 暗号化設定	17
3.5.3 管理鍵	18
索引	21

1 このドキュメントについて

このドキュメントを活用するために理解しておくべき情報を次のトピックごとに説明します。

- [このドキュメントの対象読者](#)
- [このドキュメントに記載されている内容](#)
- [その他のドキュメント](#)

このドキュメントの対象読者

このドキュメントは、許可されていないアクセスに対し、メールやファイルを保護するための暗号化機能を使用するユーザを対象にしています。

このドキュメントに記載されている内容

このドキュメントは、次の情報が含まれます。

- [Guardの概要](#)では、Guardの概要について説明します。
- [使用説明Guard](#)では、Guardの使用方法について説明します。

このドキュメントでは、グループウェアの一般的なインストール方法と構成方法について説明します。ご利用のグループウェアのインストールバージョンならびに構成によっては、記載の方法と異なる場合があります。

その他のドキュメント

グループウェアに関する全般的な情報は、Groupwareのユーザ ガイドを参照してください。

2 Guardの概要

Guardは、メールおよびファイルを暗号化するグループウェアセキュリティコンポーネントの一つです。

- ユーザや外部の人とやりとりするメールを暗号化します。
- 単体ファイルを暗号化します。暗号化されたデータを他のユーザと共有します。
- セキュリティオプションを使用して、暗号化レベルを指定します。
- 暗号化されたデータをパスワードで保護します。また、パスワードリセット機能を使用して、パスワードを紛失しても暗号化ファイルを処理します。

3 使用説明Guard

Guardアプリケーションの使用方法を次のトピックごとに説明します。

- 基本設定を[適用](#)
- [メール](#)を暗号化
- [ファイル](#)を暗号化
- セキュリティ設定を[適用](#)

3.1 セットアップGuard


使う前にGuardの基本設定を適用しなければなりません。

- まず、Guard セキュリティパスワードを設定してください。そのパスワードはデータの暗号化と暗号化されたデータのデコードに使われます。
- 二番目のメールアドレスを入力します。このメールアドレスは、お使いの Guard セキュリティパスワードを忘れたときに使用します。これには、Guard セキュリティパスワードのリセット機能を使用します。新しいパスワードが送信されます。セキュリティ上の理由により、二番目のメールアドレスを設定しておくことを強くお勧めします。設定しなければ、新しいパスワードが最初のメールアドレスに送信されます。


基本設定にはオプション2つあります。

- 初めて暗号化機能を使用するときに基本設定をセットアップする
- 初めて暗号化機能を使用する前に基本設定をセットアップする

初めて暗号化機能を使用するときに基本設定をセットアップする

1. フォルダツリー内のフォルダ名の隣の暗号化アイコン  をクリックし、メールの作成時、ファイルの暗号化時、または、新規ファイルのアップロード時で、暗号化機能を有効にします。
2. Guard セキュリティパスワードと二番目のメールアドレスを入力するよう、促されますので、データを入力します。

初めて暗号化機能を使用する前に基本設定をセットアップする

1. メニューバーの右側にある システム メニュー アイコン  をクリックします。メニューで、設定 の項目をクリックします。
2. サイドバーで、Guard セキュリティをクリックします。
Guardセキュリティ設定を初めて開くと、Guard セキュリティキーを作成ウィンドウが開きます。
3. パスワード フィールドで、データを暗号化するためのパスワードを入力します。
確認 フィールドで、同じパスワードを再度入力します。
4. 新しい二番目のメールを入力フィールドに、Guard セキュリティパスワードのリセット用の仮パスワードを受け取るためのメールアドレスを入力します。
5. OK をクリックします。

3.2 メールのやり取りを暗号化する


次のようなオプションの機能があります。

- 暗号化されたメールの閲覧
- 暗号化されたメールの送信
- 外部の宛先はどのように暗号化されたメールを閲覧するのか？

3.2.1 暗号化されたメールの閲覧

暗号化されたメールを閲覧するには、Guard セキュリティパスワードが必要です。暗号化されたメールの差出人は、追加のパスワードでメールを保護できます。

暗号化されたメールを閲覧する

1. 暗号化 アイコン  が付いたメールを選択します。詳細ビューで、セキュアなメールです。Guard セキュリティ パスワードを入力してください。 の通知が表示されます。
Guardを使用した時に Guard セキュリティパスワードを覚えるように設定した場合、メールが設定によって、すぐに表示されます。
2. Guard セキュリティパスワードを入力します。
セキュリティパスワードをGuardが記憶する期間を指定できます。これには、ログインを保持Guard を有効にします。一覧から目的の値を選択します。
3. OK をクリックします。内容がテキストで表示されます。
メールにファイルが添付されている場合、添付されたファイルの暗号化バージョンや復号されたバージョンを使う機能が表示されます。


注： 暗号化されたメールを使用している場合は、このメールに返信したり、転送のみできます。

3.2.2 暗号化されたメールの送信

次のようなオプションの機能があります。

- 暗号化されたメールの送信。差出人と宛先しかメールの内容を読めません。
警告： 暗号化されたメールの下書きを送信する場合は、下書き フォルダから送信されたと同時に削除されます。
- 署名付きのメールを送信。署名を付けることによって宛先は通信中のメール内容が変わったかどうかを判断することができます。
- 署名付きの暗号化されたメールの送信。

暗号化されたメールを送信する

1. メールアプリケーションの中でメールを作成してください。
作成ページで、右上の暗号化アイコンをクリックします。
件名下の **セキュリティ** をクリックすることもできます。暗号化を有効にする
宛先の横のアイコンは、メッセージがこの宛先に暗号化可能かどうかを示しています。アイコン上に
マウス ポインタを置くと、内容が表示されます。
2. 追加オプションを表示するには、**セキュリティ** をクリックします。次のオプションを起動できます。
メールの署名を可能にするために**サイン**を有効にしてください。
宛先のメールクライアントがPGPに対応しなくてもメールの内容が読めるようにするために**インライ
ン PGP** を有効にしてください。この場合はHTML形式のメールを送信することはできません。
メールの宛先が暗号化された返信を送るようには、公開鍵を添付ファイルで送ります。自分
の公開鍵を添付ファイルとして送信できます。これを行うには、**鍵**を添付を有効にします。
3. 暗号化送信をクリックします。
外部の宛先に送信するとき、**暗号化されたメールを開くときの注意事項 [12]** を外部の宛先に送信す
るためのウィンドウが表示されます。
最初の暗号化されたメールをこの外部の宛先に送ると、外部の宛先には公開鍵付きの添付が届きます。

3.2.3 外部の宛先はどのように暗号化されたメールを閲覧するのか？

グループウェアのユーザでない外部の宛先に、暗号化されたメールを送信することもできます。外部の宛先を追加するとき、Guardが公開鍵がこの宛先に利用可能かどうかを確認します。その結果により、Guardは暗号化されたメールの送信手順を変更します。

- 宛先に公開鍵がある場合：
 - メッセージはこの鍵で暗号化されて送られます。宛先は、自分の秘密鍵のついたメッセージを閲覧できます。
 - 宛先が暗号化された返信を送るようには、公開鍵を添付ファイルで送ります。添付ファイルはpublic.asc.となります。宛先は、この鍵を自分のメールクライアントにインポートできます。
- 宛先に公開鍵がない場合：
 - 外部のユーザがすでにゲストアカウントを持っている場合、ユーザはゲストアカウントのログインページにリンク付きのメールを受け取ります。ログインすると、ゲストページで暗号化されたメールを読むことができます。ユーザはこのページから暗号化された返信を送信できます。
 - ゲストアカウントがない場合は、ゲストアカウントを作成されます。ガイドラインが添付されたメールと自動作成されたパスワードを外部の宛先に送信します。ユーザはさらにゲストページにリンク付きのメールを受け取ります。ゲストページでは、自動で作成されたパスワードでログインします。その後、自分のパスワードを作成できます。
 - グループウェア構成によって、ゲストアカウントメールは設定日数を過ぎると削除されます。削除されたメールを利用できるように、ゲストページにリンクのはったメールには、暗号化されたメールに添付ファイルがついています。添付ファイルはencrypted.asc.です。この添付ファイルはゲストページでアップロードしたり、閲覧できます。

3.3 ファイルの暗号化

次のようなオプションの機能があります。



- ファイルの暗号化
- 新しい暗号化ファイルの作成
- 暗号化ファイルを開く
- 暗号化ファイルのダウンロード
- ファイルの復号

3.3.1 ファイルの暗号化

ファイルの暗号化時には、そのファイルの最新バージョンのみが暗号化されます。その他のすべてのバージョンは削除されます。

ファイルを暗号化する

警告: ファイルの暗号化時には、そのファイルの最新バージョン以外のすべてのバージョンが削除されます。過去のバージョンを維持するには、ファイルの暗号化前に保存してください。

1. ドライブアプリケーションの1つまたは複数のファイルを選択します。ツールバーの**アクション** アイコンをクリックします。メニューで **暗号化** をクリックします。
種類バーの右側の**アクション**アイコンを使うこともできます。メニューで **暗号化** をクリックします。
2. ファイルが複数のバージョンを含む場合、**ファイルを暗号化**ウィンドウが表示されます。ファイルの暗号化と過去のすべてのバージョンの削除を確定するには、**OK** をクリックします。
ファイルのバージョンは1つしかない場合は何も求められずに暗号化されます。

3.3.2 新しい暗号化ファイルの作成

ローカル ファイルを暗号化した上でアップロードすることによって、新しい暗号化ファイルを作成できます。

新しい暗号化ファイルを作成する


1. ドライブアプリケーションで、フォルダツリーのフォルダを選択します。
注: オブジェクトを作成する権限のあるフォルダを開いてください。
2. ツールバーで、**新規** をクリックします。**ローカルファイルを追加および暗号化** をクリックします。
3. **更新ファイル**ウィンドウの1つまたは複数のファイルを選択します。
開く をクリックします。表示エリアには現在の進行ステータスが表示されます。
処理をキャンセルするには、表示エリアの右側下にある**ファイル詳細** をクリックします。**読み込み進行** ウィンドウで、ファイル名横の**キャンセル** をクリックします。

ヒント: お使いのオペレーティング システムのデスクトップからファイルをドラッグし、**ドライブ アプリケーション** ウィンドウの上部にドロップすることでも、新しい暗号化ファイルを作成できます。

3.3.3 暗号化ファイルを開く

暗号化されたファイルを開き、閲覧できます。ファイルは、サーバ上で暗号化されたままになります。



暗号化されたファイルを開く

1. ドライブ アプリケーションで、表示エリアの暗号化ファイルを選択します。ツールバーで、ビューアイコン  をクリックします。
2. セキュリティパスワードを入力ウィンドウが開きます。Guard セキュリティパスワードを入力します。セキュリティパスワードをGuardが記憶する期間を指定できます。これを行うには、パスワードを記憶を有効にします。一覧から目的の値を選択します。
OK をクリックします。

3.3.4 暗号化ファイルのダウンロード

暗号化ファイルをローカルにダウンロードし、閲覧または編集できます。ファイルは、サーバ上で暗号化されたままになります。


暗号化されたファイルをダウンロードする

1. ドライブ アプリケーションで、表示エリアの暗号化ファイルを選択します。ツールバーで、ビューアイコン  をクリックします。
注: ポップアップで、ダウンロード をクリックすると、ダウンロードされたファイルが暗号化されたままになります。
2. セキュリティパスワードを入力ウィンドウが開きます。Guard セキュリティパスワードを入力します。セキュリティパスワードをGuardが記憶する期間を指定できます。これを行うには、パスワードを記憶を有効にします。一覧から目的の値を選択します。
OK をクリックします。
3. ビューアのアクション アイコン  をクリックします。復号されたファイルをダウンロード をクリックします。

3.3.5 ファイルの復号

ファイルを復号すると、ファイルの暗号を解除できます。

ファイルを復号する


1. ドライブ アプリケーションで、表示エリアの暗号化ファイルを選択します。ツールバーのアクションアイコン  をクリックします。メニューで、暗号化を削除 をクリックします。
2. セキュリティパスワードを入力ウィンドウが開きます。Guard セキュリティパスワードを入力します。Guard セキュリティパスワードを記憶する期間を指定できます。これを行うには、パスワードを記憶を有効にします。一覧から目的の値を選択します。
OK をクリックします。

3.4 サインアウトGuard

グループウェアを閉じずに Guard からサインアウトできます。サインアウト後に暗号化されたメール、ファイル、フォルダを開くには、Guard セキュリティパスワードを再度入力します。

注：この機能は、暗号化されたメールやファイルを開いたときにパスワードを記憶を有効にしたときのみ、適用されます。

Guardからサインアウトする：

1. メニューバーの右側にある システム メニュー アイコン  をクリックします。
2. メニューで、サインアウトをクリックします。

3.5 Guard設定

次のようなオプションの機能があります。


- Guardセキュリティパスワードを管理するには、[Guardセキュリティ設定](#)を使用します。
- 安全なメールを送信するための初期設定を変更するには、[PGP 暗号化設定](#)を使用します。
- [PGP鍵](#)を管理することができます

3.5.1 Guardセキュリティ設定


次のようなオプションの機能があります。

- Guard セキュリティパスワードを**変更**
- Guardセキュリティパスワードを失った場合、Guardセキュリティパスワードを**リセット**することで一時Guard セキュリティパスワードを要求できます。
- 二番目のメールアドレスを **変更**


Guardセキュリティパスワードの変更方法

1. メニューバーの右側にある **システム メニュー アイコン**  をクリックします。メニューで、**設定** の項目をクリックします。
2. サイドバーの**Guardセキュリティ**をクリックします。
3. パスワードの下の**現在のセキュリティパスワード**の入力フィールドに今までデータの暗号化に使用してきたパスワードを入力します。
新しい**セキュリティパスワード**の入力フィールドにこれからデータの暗号化に使用したいパスワードを入力します。
新しい**セキュリティパスワードを確認**フィールドに再度入力してパスワードを確認します。
4. **セキュリティパスワードを変更**をクリックします。

Guardセキュリティパスワードのリセット方法：

1. メニュー バーの右側にある **システム メニュー アイコン**  をクリックします。メニューで、**設定** の項目をクリックします。
2. サイドバーの**Guardセキュリティ**をクリックします。
3. **セキュリティパスワードをリセット**をクリックします。新しいパスワードが二番目のメールアドレスに送信されます。
二番目のメールアドレスを入力していない場合は、新しいパスワードが一番目のメールアドレスに送信されます。
4. この新しいパスワードが現在の Guard セキュリティパスワードとなります。すぐにこのパスワードを**変更**してください。


暗号化されたパスワードのリセット用二番目のメールアドレスの変更方法

1. メニューバーの右側にある **システム メニュー アイコン**  をクリックします。メニューで、**設定** の項目をクリックします。
2. サイドバーの**Guardセキュリティ**をクリックします。
3. **二番目のメールアドレス**の下の**現在のセキュリティパスワード**を入力フィールドにデータの暗号化に使用しているパスワードを入力します。
新しい**二番目のメール**を入力フィールドに、Guard セキュリティパスワードのリセット用の仮パスワードを受け取るためのメールアドレスを入力します。
メールの変更をクリックします。

3.5.2 PGP 暗号化設定

PGP 暗号化設定は、メール作成時に利用可能な規定の設定を指定します。新規メール作成時、初期設定の調整をメール送信前に行えます。

PGP の暗号化設定を変更する

1. メニュー バーの右側にある **システム メニュー アイコン**  をクリックします。メニューで、**設定** の項目をクリックします。
2. サイドバーで、**Guardセキュリティ**を選択します。**詳細設定**をクリックします。
3. **PGP 暗号化設定**下の設定を変更します

次の設定が利用できます。

メールの作成時に暗号化をデフォルトにする

新規メールをデフォルトごとにPGPで暗号化するかどうかを指定する

送信メールヘサインの追加をデフォルトにする

新規メールをデフォルトごとにPGPで暗号化するかどうかを指定する

PGP の上級機能を有効にします。

鍵管理などの PGP 機能を表示するかどうかを設定できます。

新規メールにインライン PGP 使用をデフォルトにする

この設定を表示するには **PGP の上級機能を有効にします**というチェックボックスを有効にします。


PGP 暗号化がインラインで行えるかどうかを指定します。宛先のメールクライアントがPGPサポートされていない場合はこの設定だけを使用してください。メッセージは読むことができます。この場合はHTML形式のメールを送信することはできません。

3.5.3 管理鍵

暗号化されたメッセージの送受信には、管理鍵の機能は基本的には必要ありません。この機能は以下の要件については使用可能です

- ローカルメールクライアントなどの他のメールクライアントでGuard PGP鍵を使用したい。
- PGPアプリケーションからのPGP鍵がある。その鍵を Guard で使用したい。
- 外部パートナーの公開鍵を持っている。この外部パートナーからの暗号化されたメッセージを鍵サーバーにアクセスせずに読むために、パートナーの公開鍵を Guard にインポートしたい。
- 受信者が鍵サーバーにアクセスせずに暗号化されたメッセージにアクセスして読むために、受信者に自分の公開鍵を提供したい。

自分の鍵を管理するページを開ける方法：

1. メニューバーの右側にある **システム メニュー アイコン**  をクリックします。メニューで、**設定** の項目をクリックします。
2. サイドバーで、**Guardセキュリティ**項目を選択します。**詳細設定**をクリックします。
PGP の上級機能を有効にしますを有効にします。

このページでは、次の要素があります。

- **Guard の既定設定を変更するオプション**
- **あなたの鍵セクション**。秘密と公開 PGP 鍵を管理する機能が含まれます。
既存の鍵はあなたの**鍵リスト**下に表示されます。鍵リストには2つの鍵があります。
 - **マスター鍵**特に、この鍵はメールの署名に使用されます。
 - **サブ鍵**この鍵は、メールおよびファイルの暗号化および復号化に使用されます。
マスター鍵とサブ鍵の違いは、PGP暗号化技術の特徴の1つです。各マスター鍵およびサブ鍵には、公開鍵と秘密鍵があります。目的に応じて、Guardは自動でそれぞれの鍵を使用します。
- **公開鍵セクション**。あなたまたは他のユーザと共有している公開鍵を表示。ユーザの公開鍵がこのリストに表示されている場合、このユーザに暗号化して送信したメールを復号することができるのみならず

次の機能が利用できます。

- **自分の公開鍵をダウンロードする**
- **メールごとに自分の公開鍵を送信する**
- **ローカル鍵をアップロードしたり、新しい Guard 鍵を作成して既存の鍵に新しい鍵を追加する**
- **鍵を現在の鍵に変更する**
- **鍵の詳細を表示する**
- **鍵を削除する**
- **自分の秘密鍵をダウンロードする**
- **鍵にメールアカウントを追加する**
- **外部パートナーの公開鍵をアップロードする**

自分の公開鍵のダウンロード方法：

1. 設定で鍵を管理するページを開けます。
2. Click on **あなたの鍵**の下にある**自分の公開鍵**をクリックします。

メールごとに自分の公開鍵を送信する方法：

1. 設定で鍵を管理するページを開けます。
2. **あなたの鍵**の下にある**公開鍵をメールする**をクリックします。

新しい鍵を自分の鍵に追加する方法：

1. 設定で鍵を管理するページを開けます。
2. あなたの鍵の下にある **+** 鍵リスト横の追加アイコンをクリックします。鍵の追加 ウィンドウが開きます。
3. 次のようなオプションの機能があります。
 - 秘密鍵の追加には、**秘密鍵をアップロードする**をクリックします。秘密鍵を含むファイルを選択してください。秘密鍵のアップロードウィンドウが開きます。
新しい鍵のアップロードには、Guard セキュリティパスワードを入力してください。新しい鍵用の新しいパスワードを入力します。
 - 公開鍵の追加の場合、**公開鍵のみを追加する**をクリックします。公開鍵を含むファイルを選択してください。
 - 新しい鍵ペアを作成する場合は、**新しい鍵を作成する**をクリックします。セキュリティ鍵作成ウィンドウが開きます。
新しい鍵用のパスワードを入力します。パスワードを確認してください。
新しい鍵にはマスター鍵と該当するサブ鍵があります。
新しい鍵はあなたの鍵リストの一番上に入力されます。新しい鍵が現在の鍵になります。


鍵を現在の鍵にする：

あなたの鍵リストに複数のマスター鍵とサブ鍵がある場合にこの機能が使用できます。この後、現在の鍵が暗号化に使用されます。


1. 設定で鍵を管理するページを開けます。
2. あなたの鍵リストの中で、**現在の下の鍵の横にあるチェックボックス**をクリックします。マスター鍵を現在の鍵に変更するときに、対応するサブ鍵に現在のもの、またはその逆に印が付けられます。

鍵の詳細を表示する：

鍵の詳細を表示できます。鍵の詳細は、PGP知識のあるユーザには特に必要です。


1. 設定で鍵を管理するページを開けます。
2. 種類バーの右側で、**詳細アイコン**  をクリックします。鍵の詳細ウィンドウが開きます。鍵の署名を見るには、**署名**をクリックします。

鍵を削除する

1. 設定で鍵を管理するページを開けます。
2. 種類バーの右側で、**削除アイコン**  をクリックします。秘密鍵の削除ウィンドウが開きます。
3. 次のようなオプションの機能があります。
 - 秘密鍵を無効にするには、**無効**をクリックします。
秘密鍵用のパスワードを入力します。必要であれば、鍵を無効にする理由を選択します。
無効をクリックします。
 - 秘密鍵を削除するには、**削除**をクリックします。
秘密鍵用のパスワードを入力します。
削除 ボタンをクリックします。
マスター鍵を削除すると、対応するサブ鍵も削除されます。


秘密鍵のダウンロード方法：

注意：秘密鍵をご自分のローカルマシンにダウンロードするのは、安全上のリスクを生じる可能性があります。他の誰もご自分の秘密鍵にアクセスできないことを確認してください。


1. 設定で鍵を管理するページを開けます。
2. 種類バーの右側で、**ダウンロードアイコン**  をクリックします。

鍵にメールアカウントを追加する：

追加のユーザIDを鍵に追加すると、鍵を複数のメール アカウントに使用できます。

1. 設定で鍵を管理するページを開きます。
2. 種類バーの右側で、編集アイコン  をクリックします。ユーザID追加ウィンドウが開きます。
3. ユーザID名を入力します。この鍵に使用したいメールアドレスを入力します。
鍵のパスワードを入力してください。
OK をクリックします。

外部パートナーの公開鍵のアップロード方法：

1. 設定で鍵を管理するページを開きます。
2. 種類バーの右側で、追加アイコン  をクリックします。公開鍵を含むファイルを選択してください。

索引

シンボル

- ×Guard, 7
- サイン アウト
 - パスワードの変更, 15
- ドキュメント, 5
- パスワードのリセット, 16
- パスワードの変更, 16
- ファイルの暗号化, 13
- ファイルを復号する, 14
- メールのやり取りを暗号化する, 11
- 新しい暗号化ファイルを作成する, 13
- 暗号化
 - ファイル, 13
 - 新しい暗号化ファイルの作成, 13
- 暗号化されたメール
 - 外部の宛先へのアクセス, 12
 - 拒否する, 11
 - 読む, 11
 - 送信する, 11
- 暗号化する
 - メールのやり取りを, 11
- 暗号化ファイル
 - ダウンロード, 14
 - 復号, 14
 - 開く, 13
- 暗号化ファイルをダウンロードする, 14
- 暗号化ファイルを開く, 13

G

- Guard, 9
 - PGP 暗号化設定, 17
 - サインアウト, 15
 - セキュリティ設定, 16
 - セットアップ, 10
 - 管理鍵, 18
 - 設定, 16
- Guard Guard PGP 設定
 - PGP の上級機能を有効にします, 17
 - メール送信の署名付きをデフォルトにする, 17
 - 新規メールにインライン PGP 使用をデフォルトにする, 17
- GuardGuard PGP 設定
 - メール作成時に暗号化をデフォルトにする, 17
- Guard設定
 - パスワードのリセット, 16
 - パスワードの変更, 16

