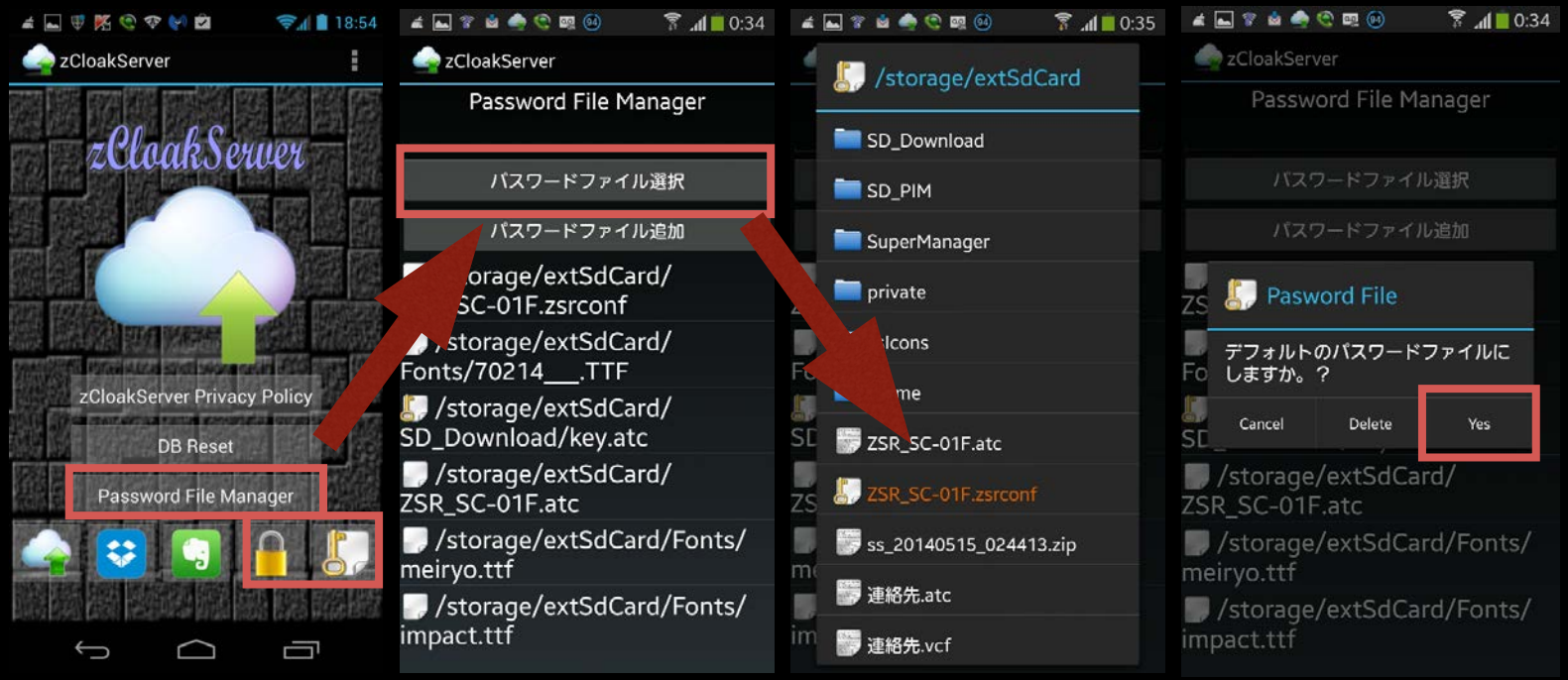
zCloakServer
暗号運用マニュアル

通話録音アプリzSuperRecorder＋zCloakServer

パスワードキーファイルの登録

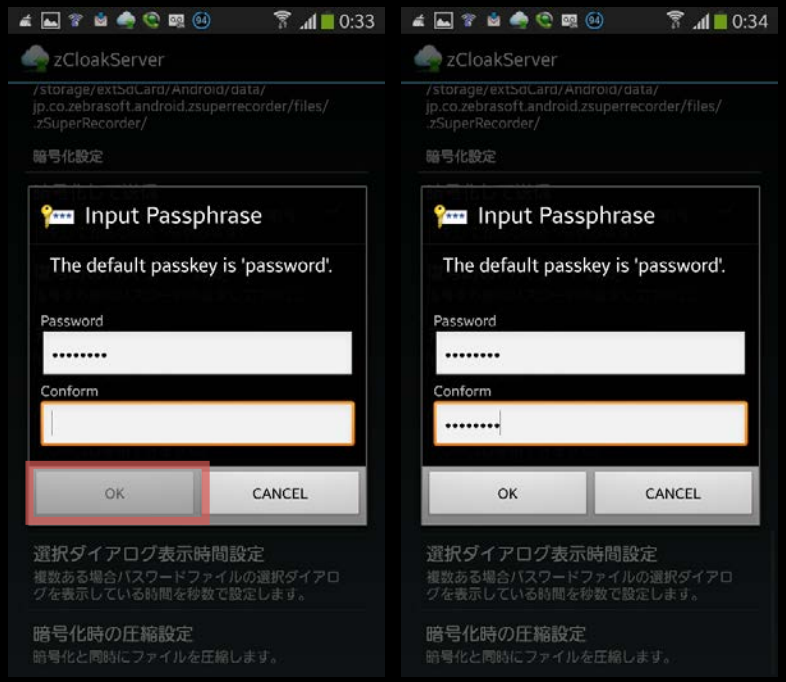


■zCloakServerで予めパスワード様のキーファイルを登録します。
平文パスワードより取り扱いは楽な上に、キーファイルが無いと復号出来ないので極めて高度な暗号ファイル管理が出来る様になります。
また、キーフィルは幾つでも登録出来るので暗号内容や共有先で切り替えて利用する事が可能です。

※キーファイルとは、平文のパスワード文字列の代わりにファイルのハッシュキーをパスワードとして入力して運用します。
単純な平文のパスワードよりも意味不明なコードになるので手入力するのも大変です。
また、ファイルの中身等でも同一ハッシュコードは取得出来ないので色々と活用方法が広がります。
例えば、あるテキストファイルをキーファイルにしていて、暗号化後、テキストのファイル名を変えておいたり、中身に1文字追加したりしてキーファイルとして共有先に送る事で、そのままでは復号出来ません。
共有先で、ファイル名を戻したり、中身の文字を削除して保存し直す事で再度キーファイルとして利用する事が出来ます。

若しくは、特定の文章を決めておいてファイルに入力して保存したファイルをキーにしておく等と言った活用方法があります。
キーファイルを加工しておけば、万が一途中で搾取されても復号出来ないので極めて安全な運用が可能です。

平文パスワードの登録



■平文パスワードは最大32文字までで設定可能で、1文字から決定出来る様にしています。
2度同じパスワードを入力して一致しないと保存出来ないので間違い防止になります。

また、zCloakServerの場合、暗号化時にパスワードファイル選択画面から平文パスワード入力ダイアログを表示出来るのでパスワードファイルでの暗号化と平文パスワードでの暗号化が混在していても対応可能です。

zCloakServerのコンセプトとして、最後に選択したキーファイルや平文パスワードを登録するので、2回目以降は確認の入力で暗号化出来ます。
但し、平文パスワードの管理は利用者がちゃんと管理しないと後で忘れた場合解読出来なくなるので取り扱いはご注意下さい。

※複数のキーを用意して運用する場合、キーファイルでの管理の方が便利です。
平文パスワードで暗号化した場合、そのファイル単体を送ればパスワードさえわかっていれば簡単に復号可能です。

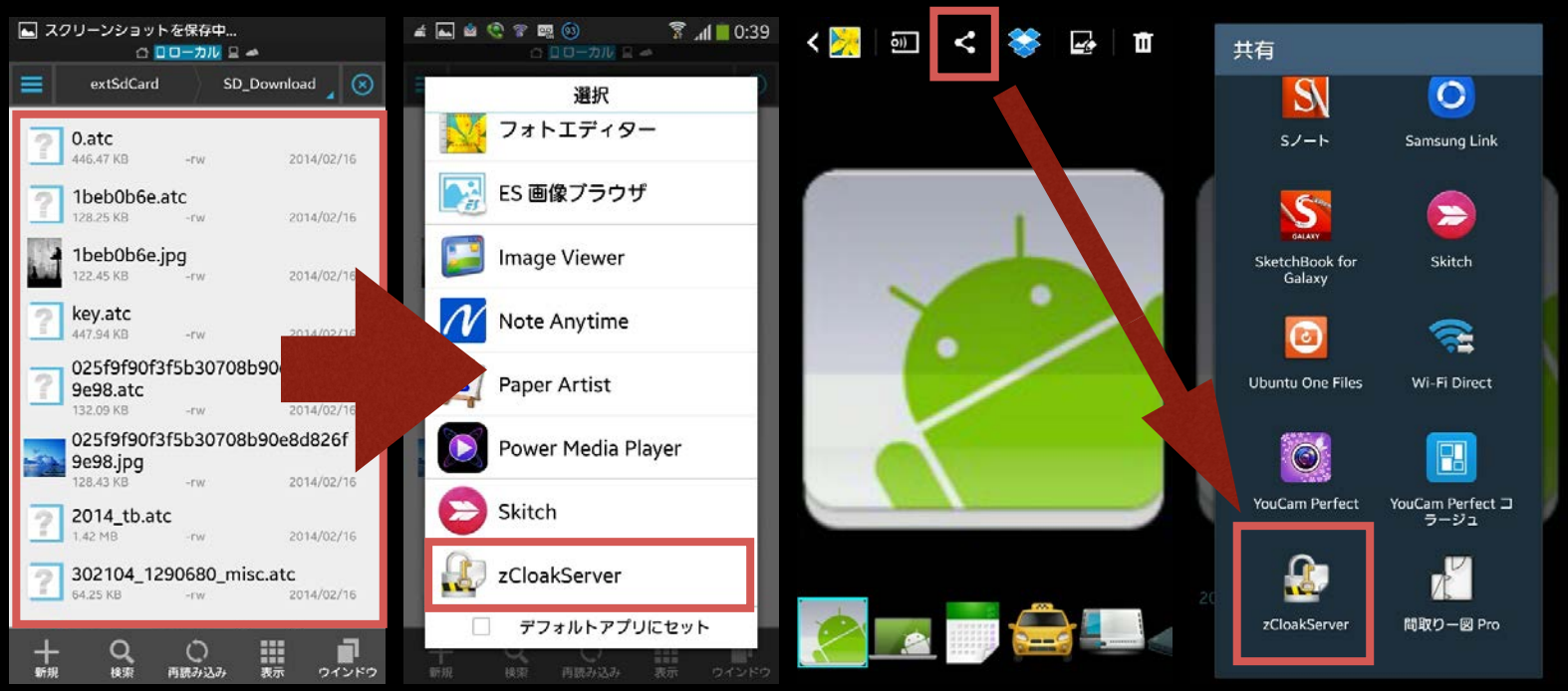
通話録音ファイルの暗号化

■zSuperRecorderの通話録音ファイルが暗号化される流れ
通常に通話を録音し、終話後設定している保存形式で音声ファイルが端末の指定フォルダーに保存されます。
すると、zCloakServerが反応して、複数暗号ファイルリストを表示するので、どのキーファイルを使うかタップで選択します。
そのまま放置するとデフォルトのキーファイル（鍵アイコンのあるファイル）で暗号化を実施します。

暗号化中は通知エリア上で進捗情報が確認出来るプログレスバーと暗号化しているファイル名を確認する事が可能です。

暗号化が終了すると、zCloakServer側の設定によりますが、暗号元ファイルを削除してzSuperRecorderのファイルリストに暗号化したファイルを登録しなおします。
暗号化したファイルもアイコンで確認することが出来、そのままタップすると自動的に復号して再生プレイヤーを表示します。
暗号化していることを意識する必要も無く、簡単に暗号化ファイルを取り扱えます。
また、複数キーファイルが登録されていてでデフォルトのキーファイルで復号出来ない場合に登録しているキーファイルリストを表示するので、該当のキーファイルに切り替えて復号可能です。
また、キーファイルでは無く、平文のパスワードで復号する場合、予め設定しているパスワードに切替て復号します。

通常ファイルの暗号化



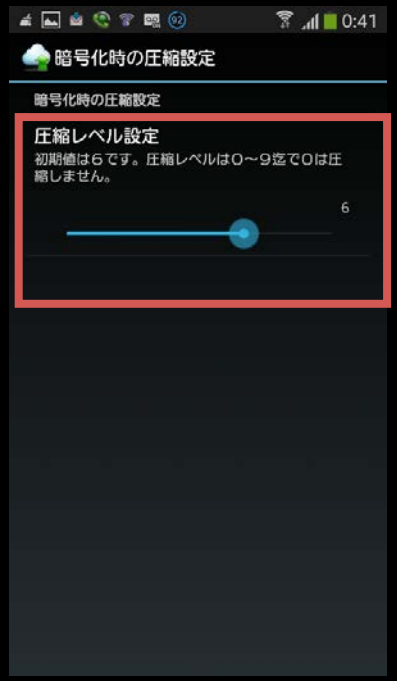
■通常のファイルを暗号化する場合
zCloakServerにはファイルマネージャ画面を用意していないので、他のファイルマネージャアプリなどファイルを選択出来るアプリを利用して一般のファイルを暗号化若しくは復号する事が可能です。

基本操作は、ファイラーにもよるとは思いますが、暗号化したいファイルをタップすると、そのアプリに関連付けられた共有メニューが表示されるので、zCloakServerは名前より、ほぼ一番最下行に表示されるので、zCloakServerの暗号化アイコンである、鍵とファイルのアイコンをタップすると、暗号ファイルリストが表示されるので、使いたいキーファイルを選択するか、平文パスワード入力に切り替えて暗号化して下さい。

また、ギャラリーアプリ等に有る共有メニューにもおそらく最下行にアイコンが表示されていると思うので選択する事で暗号メニューを表示します。

拡張子が「atc」だった場合、自動的に復号として扱うようにしています。

暗号化時のオプション機能



■暗号化時にファイルを圧縮する事が可能です。
初期値の暗号レベルは「６」に設定しています。
ファイルの種類によっては圧縮効果のあるファイルや効果の無いファイルもありますが、少なくとも暗号化時に付加される情報を圧縮して元のファイルよりは小さくする事がかのうですが、「０」に設定した場合、圧縮機能が機能しないので、付加する情報分、元のファイルよりも容量は大きくなります。

圧縮レベルは１～９迄で、10分間録音したWAV形式のファイルが約5MB程あったのですが、圧縮レベル６で暗号化したら約2.3MBまで圧縮することが出来ました。
他に、既に圧縮されているAMR形式やMP3等の録音ファイルは圧縮レベルを上げてもほとんど効果はありません。

圧縮における暗号化速度や復号速度などはほとんど影響はありません。
但し、非力なスマホでの暗号化、復号なので、10MBを超える様なファイルの暗号化はかなり時間がかかりますので大体5MB程度のファイルを暗号化する場合にzCloakServerは有効です。

zCloakServer暗号化運用総括

Google PlayStoreにも色々と暗号化アプリは登録されています。
有料アプリ等は1000円を超える物もありました。
一応に、アプリの性質上ファイルマネージャ的な画面を持ち、アプリ自体でファイルを選択して暗号化するとか復号するとかを選ぶ様なものが一般的でした。
アタッシェケース for Androidも同様にファイルマネージャ系のアプリですが、共有メニュー等で他のアプリからファイルを受け取る機能を実装していました。

そこで、zCloakServerは基本性質上、zSuperRecorderの録音ファイルをCloudへ送信するオプションアプリで、情報漏洩などの観点より、極めてプライベートな情報である通話録音こそ暗号化して守る必要があると思い、パソコン等では定番のアタッシェケース for Windows互換の暗号化であれば、活用の幅が広がりより便利に利用出来ると思い、互換の暗号化機能を実装しています。
パソコン版のアタッシェケースはWindows、Mac、Linuxで利用可能で、Windows以外はjava版のアタッシェケース for javaを利用します。

zCloakServerで暗号化したファイルはパソコン版のアタッシェケースで復号出来ますし、その逆も問題ありません。
パスワードファイルでの暗号/復号に双方向で対応しています。

この暗号化を施したファイルをCloudに送信する事で、非常に安全な通話ログ管理が実現します。
通常、キーファイルで暗号化したファイルをDropboxやEvernoteに送信しておき、キーファイルはDropbox等に別に置いておくか、USBメモリーなどに別に保管しておきます。
個人的には復号が必要な時にDropboxの特定のフォルダーにアップロードしてパソコン版のアタッシェケースで復号する様にして、普段はDropboxから削除しておきます。
キーファイルは何時でもキーファイルマネージャの共有機能からDropboxやメールを選択して簡単に送信出来るようにしているので再生が必要な時以外は復号する事が無いので単にバックアップしている状態になります。

復号が必要な時のみ、キーファイルを送信すれば良いので、過去のログがいくら残っていても極めて安全な暗号化状態なので万が一漏洩しても意味の無いファイルでしかありません。

Windows版 アタッシェケースホームページより抜粋すると「暗号化アルゴリズムには、2000年10月にアメリカ政府標準技術局（NIST）によって、 次世代暗号化標準 AES（Advanced Encryption Standard）として選定された“Rijndael（ラインダール）”を採用。」とあり、極めて高度な暗号化ファイルが作成されるので安心してCloudを活用する事が可能になります。

zCloakServer単体での利用も可能なので他の暗号化アプリと比較しても使い勝手においては類を見ないUIで簡単に暗号/復号ソリューションを利用出来ると思います。（パスワードファイルに対応しているアプリはほとんどありませんでした。）

https://play.google.com/store/apps/details?id=jp.co.zebrasoft.android.zcloakserver

ZEBRASOFT tamayan

アンドロイドアプリ *Developer*