Supported by Microsoft

Windows ストア アプリで ウイルスを作るには!?

わんくま同盟
BluewaterSoft 山本 康彦 (@biac)

Community OpenDay
Supported by Microsoft

コミュニティ 紹介

わんくま同盟


わんくま同盟コミュニティ紹介
わんくま同盟 名古屋勉強会
次回 2013/05/18

わんくま同盟って何？

- わんくま同盟は、コミュニティで活動している者たちの集団です。
- 縦の繋がりはなく、横の繋がりで成り立っています。
- ぜひご参加ください!!
- ノンジャンルです。開発者が多いです。
- 各自のスタイルで情報提供などをしています

- あなたも一緒に情報発信しませんか？

わんくま同盟

主な活動内容

勉強会

- http://wankuma.com/seminar/
- 東京・大阪・名古屋・福岡、ほか
- ほぼ毎週どこかで勉強会

ブログ

- http://blogs.wankuma.com/
- 主に開発系だけど、ノンジャンル

掲示板

- http://bbs.wankuma.com/
- C#とVB.NETの掲示板

わんくま同盟

勉強会について

- わんくま同盟の勉強会では、以下のスタイルでの勉強会を開催しています。
  - 1枠50分のセッション x 3～5セッション
  - 1人5分のLightningTalks x 3つ
  - Ustream中継＆ビデオ録画(後日公開)
- 名古屋勉強会は2007年12月に第1回開催。
- 名古屋勉強会では、biacさんによるTDD道場、TDDワークショップやパネルディスカッション等の独自企画にも取り組んでいます。

わんくま同盟

来週 !!

地下鉄鶴舞線
浄心駅 徒歩1分

次回勉強会情報

- わんくま同盟 名古屋勉強会 #27
- 日時：2013年5月18日(土) 13:50～18:20
- 場所：名古屋市西生涯学習センター(浄心)
- 参加費：無料
  - ★ TDD道場 (第15回) <biac>
  - ★ Windows ストア アプリの肝 ～ データ バインディングを極める! <biac>
  - ★ Team Foundation Serviceを使ってみる <You&I>
  - ★ 森理式 VSハッカソンのススメ <森理 麟>
  - ★ Visual Studio についてのパネルディスカッション
  - ★ 懇親会

スピーカー登壇希望者は随時募集中です！

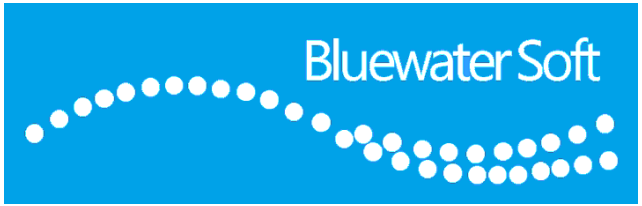
スピーカー 紹介

BluewaterSoft 山本 康彦 (@biac)

スピーカー紹介

biac (山本 康彦)
http://www.bluewatersoft.jp

- 1957: スプートニク以前に誕生
- 1983: 名古屋大学工学部(修士)卒
- HONDA R&Dで自動車設計
- 1994～ ソフトウェア業界
- 2012～ BluewaterSoft



スピーカー紹介

biac (山本 康彦)
http://www.bluewatersoft.jp

BluewaterSoft

本を書いたり

速攻入門 C# プログラミング
技術評論社、共著
2012/3

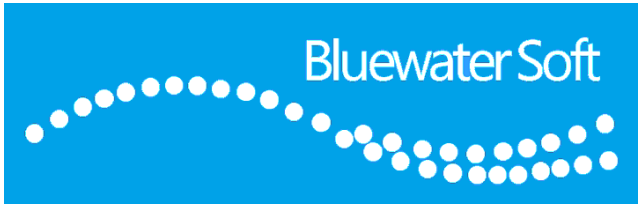
Windows 8 業務アプリ開発読本
技術評論社、共著
2013/3

C#でマルチスレッド プログラミング (仮題)

【近刊予定】

スピーカー紹介

biac (山本 康彦)
http://www.bluewatersoft.jp



記事を書いたり

WinRT/Metro TIPS
@IT ～ 連載中
http://www.atmarkit.co.jp/ait/subtop/features/da/ap_winrttips_index.html

C#で始めるテスト駆動開発入門
CodeZine
http://codezine.jp/article/corner/446

Metro スタイル・アプリの開発者が知るべき3つのこと
@IT 2012/3
http://www.atmarkit.co.jp/fdotnet/chushin/readyforwin8app_01/readyforwin8app_01_02.html

スピーカー紹介

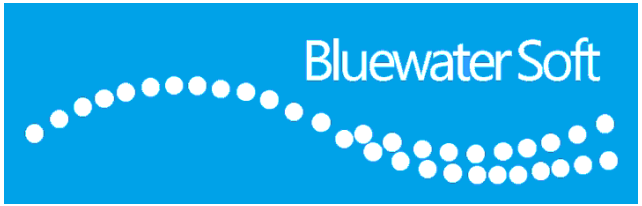
biac (山本 康彦)
http://www.bluewatersoft.jp

BluewaterSoft

アプリを作ったり

スピーカー紹介

biac (山本 康彦)
http://www.bluewatersoft.jp



講師やったりしてます

C# / VB.NET による
Windows 8 アプリ開発入門

2013/7/11～12
名古屋ソフトウェアセンター

http://www.nagoya-sc.co.jp/ap/seminar?m=1&key=10734

スピーカー紹介

biac (山本 康彦)
http://www.bluewatersoft.jp

BluewaterSoft

昨年のCOD、そして…

Windows ストア アプリで ウイルスを作るには!?

・ウイルス、というかマルウェアを作る
・ところでウイルスって何?

広義のウイルス＝マルウェア、狭義のウイルス、スパイウェア …

広義のウイルス＝マルウェア (Malicious + Software)

狭義のウイルス

・自己伝染機能
・潜伏機能
・発病機能

あまり見かけなくなった

スパイウェア

ユーザーの情報を盗み出す
・キー入力
・ファイルの内容
・通話内容
・位置情報
…etc

「カレログ」
2011 Android

バックドア

＝遠隔操作(RAT)

「遠隔操作事件」
2012 Windows

アドウェア

・悪質な広告，詐欺
・広告から
マルウェアを導入

「BadNews」
2013 Android

Windows ストア アプリとして、マルウェアを作れるか?

- 「狭義のウイルス」は、まず不可能
  自由なファイルの読み書きが出来ない(後述)ので、
  自己伝染機能を実装できない。

- スパイウェア等は…!?
  作れるんじゃないのかな?

これが本セッションのテーマ

順番に考えていこう

Windows ストア アプリで ウイルスを作るには!?

- マルウェアのコードが書けただけでは、役に立たない
- マルウェアが実際に「活躍」しなきゃ!

Community OpenDay

Supported by Microsoft

「役に立つ」マルウェアとは?

- 役に立つ機能を実装する
  * 欲しいモノが手に入る / 出来る
  * ユーザーに気付かれない / 騙せる
- バラ撒く
  * 多くの / 特定のユーザーに行き渡らせる
- 身元を隠す
  * バラ撒いた人物が分からないように

Windows ストア アプリで ウイルスを作るには!?

- そもそも論として… …
- 狙うデータはどこにある?

Community OpenDay

Supported by Microsoft

Windows ストア アプリのアーキテクチャ思想: Device + Service

複数デバイスで
シームレスなUX

↓

データはクラウドに

デバイス側に
めぼしい獲物がいない!

Windows ストア アプリで ウイルスを作るには!?

- ユーザーに気付かれないように 何か悪いことをするには?

Community OpenDay
Supported by Microsoft

こっそり動かしたい!

継続的な監視をしたい
・GPS情報
・キーロガー
・通信内容傍受

そういうマルウェアは、常時稼働していなければ!!

できねぇ… orz

- 他のアプリに切り替えらえると、中断される
  http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/Hh770837.aspx
- バックグラウンド タスクは、最短で15分に1回、最長2秒間だけ
  http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/hh977056.aspx

こっそりファイルに
アクセスしたい!

ユーザーの重要なファイルを、
こっそり読み取ってどこかに送信
したり、ネットにバラ撒きたい

- 自由にアクセスできるのは、画像フォルダなどの一部だけ

http://msdn.microsoft.com/ja-jp/library/windows/apps/hh967755.aspx

- その他の場所は、ユーザー操作が必須

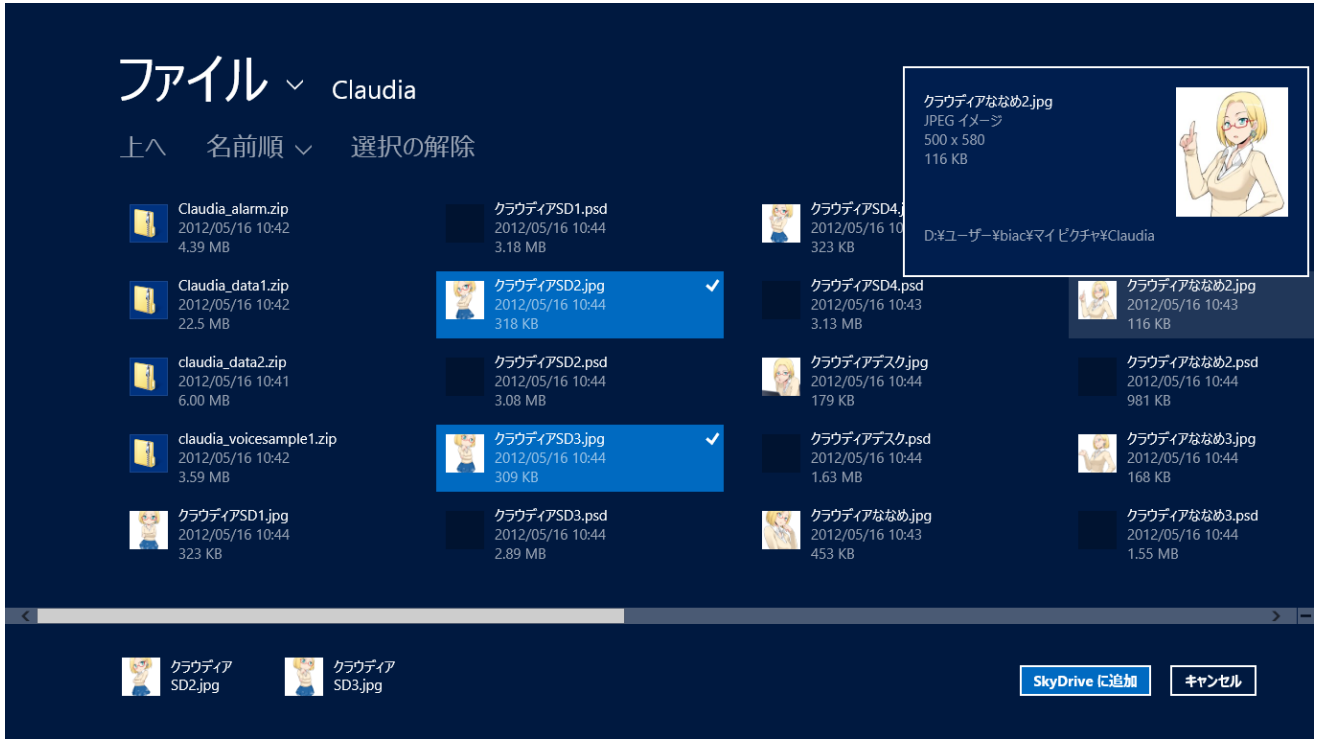
http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/hh771180.aspx

《 ファイル オープン ピッカー 》 例: SkyDrive アプリからローカルフォルダー

とあるフォルダーで、ファイルを2つ選択したところ。

特別に許可された場所以外のファイルへのアクセスは、このようにユーザーの操作を必要とする。

ぬぅ…
いやマテ、
Win32 がある!!



Win32 APIを使えば
ファイル読み書き自由だぜ!

WinRT/.NET Framework のAPIでは
ファイルアクセスできないなら、
Win32 API を叩けばいいのよ～♪

よ し よ し …
ストアに出してやろう!

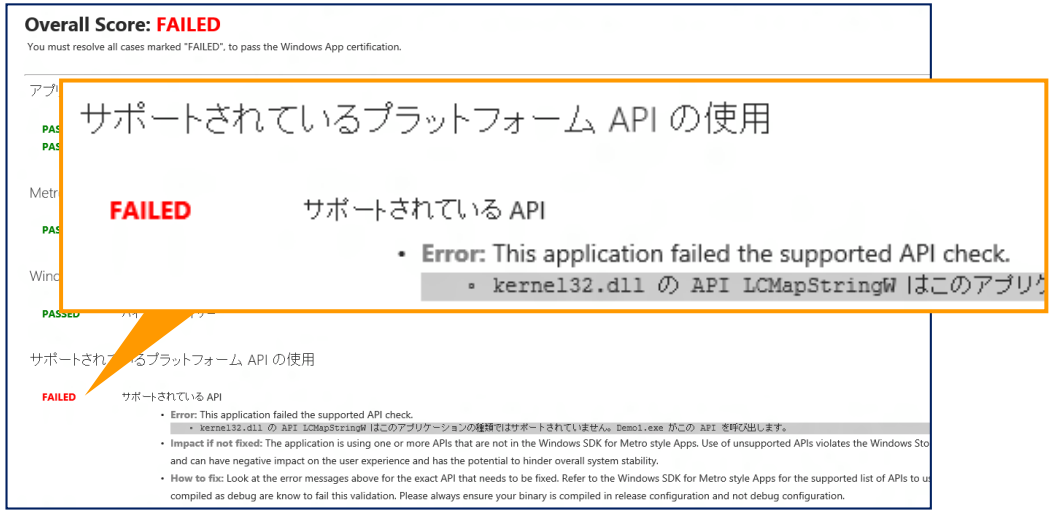
- Win32 and COM for Windows Store apps
  http://msdn.microsoft.com/ja-jp/library/windows/apps/br205757
- ん!?
  上に載ってないAPIも動くじゃん。
- やった! ファイル読み書きが自由に出来る!!

開発者用
簡易チェック ツール

ストアで審査に使ってるチェックツールよりは甘いでしょうが、**WACK** (Windows App Cert Kit, Windows アプリ検証キット) が提供されています。
WACKに通らないようでは、ストアの審査は絶対に通りません。

ダメぢゃん… orz

- 前ページのリストに無いAPIを使っていると…



じゃ、アドレス帳を
狙ってやるか!

メアドを抜ければ、カネになるぜ!

アドレス帳データを扱うAPIはあるし～♪

- Windows.ApplicationModel.Contacts名前空間

http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/windows.applicationmodel.contacts.aspx

- え? 列挙できね～っ!?
  ユーザーの選択が必須!

http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/JJ152724%28v=win.10%29.aspx

《 連絡先ピッカー 》 例: メッセージング アプリから People アプリの連絡先

Peopleアプリの連絡先を表示したところ。

この連絡先ピッカーでユーザーに選択してもらうと、そのメアド等がアプリで取得できる。

こっそりは
ムリぽ… orz

せめて夜中に印刷して
困らせてやるくらいは!!

PC用のプラットホームで印刷できないなんて、ありえな～い♪

バックグラウンド タスクで、夜中に用紙が尽きるまでムダな印刷をしてやんよ!

- PrintManagerオブジェクトに指示すりゃいいんだよね♪
- え? 印刷にも、ユーザーの操作が必須!?

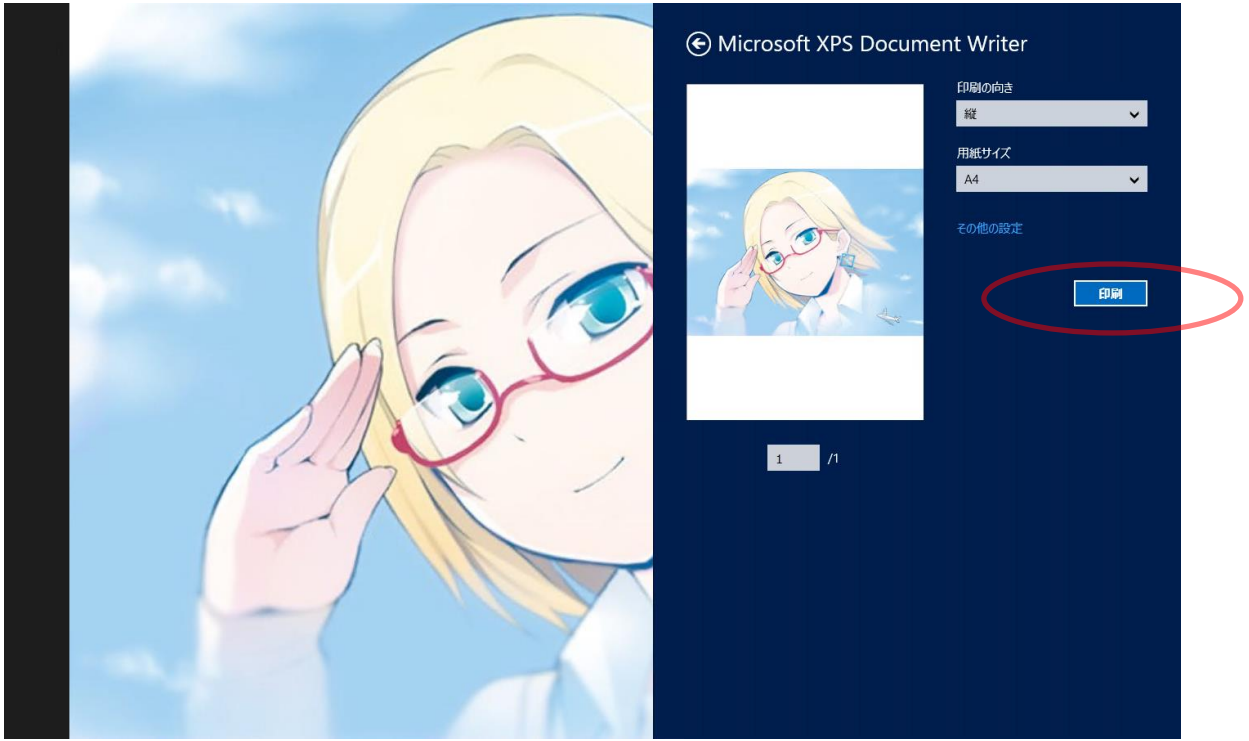
http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/hh849591.aspx

《 印刷コントラクト 》 例: Photos アプリから印刷

Photosアプリから、デバイス チャームを開いて、プリンタを選択したところ。

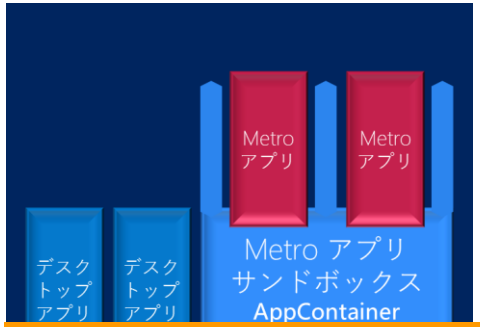
印刷コントラクトが出している右側のフライアウトで、ユーザーが [印刷] ボタンをタップしないと、印刷は始まらない。

カンベンして… orz



動いているデスクトップ アプリと通信すれば!

ガチガチのサンドボックス。



そこまでやるか… orz

- プロセス間通信 不可!
  Windowハンドルも
  取れない!
- Localhost へのループ
  バック接続も禁止

※ デバッグ時はOK
http://www.moonmile.net/blog/archives/3414

かくなる上は、
動的に実行ファイルを!

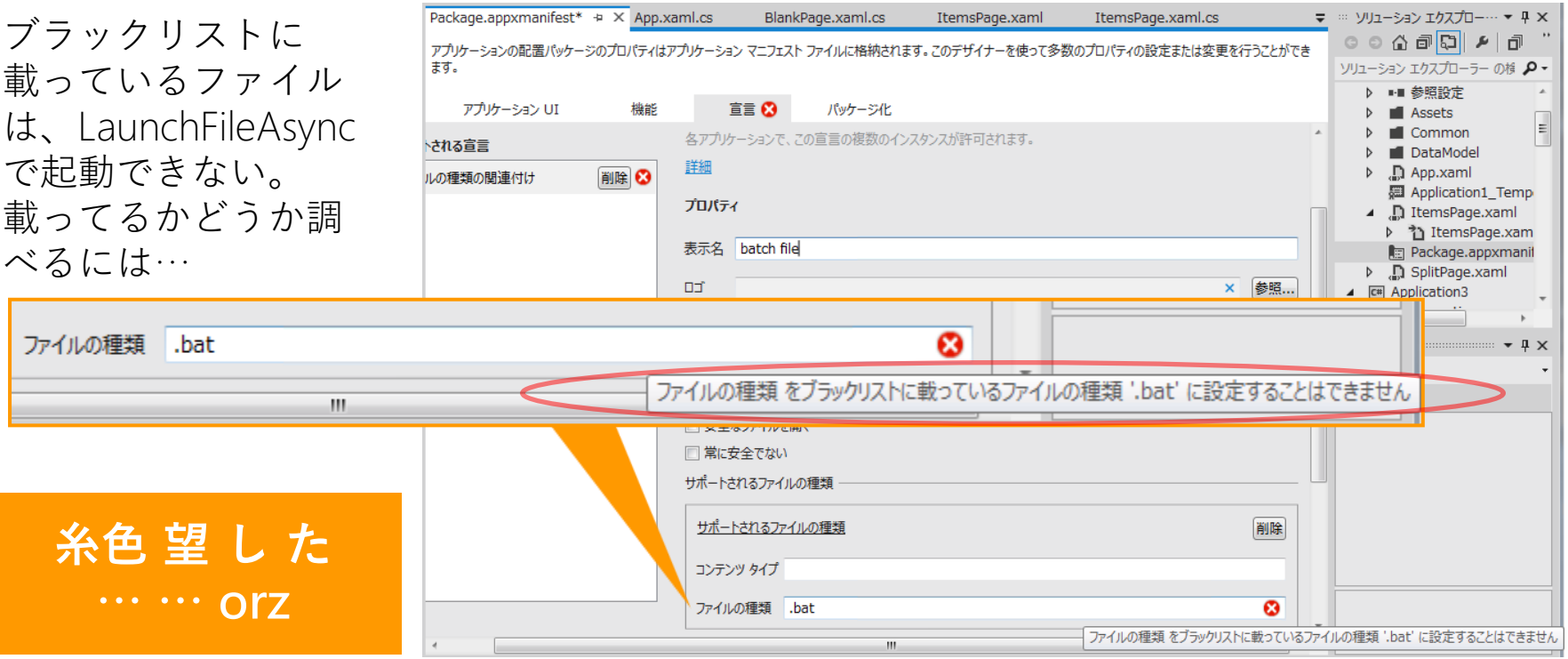
プロセスを直接起動することはできないけれど…

実行ファイル (exe, bat, ps1 等) として書き出して、 LaunchFileAsync で動かしてやれば♪

- LaunchFileAsyncメソッドは実行ファイルを起動できない
  http://msdn.microsoft.com/ja-jp/library/windows/apps/xaml/hh779671.aspx
- .docにして、Wordのマクロとか
  ……もダメですか

《 ブラック リスト 》 例:ファイルの種類の関連付け設定

ブラックリストに
載っているファイル
は、LaunchFileAsync
で起動できない。
載ってるかどうか調
べるには…



糸色 望 し た
… … orz

ユーザーに気付かれないように何か悪いことをするには?

- ローカルは、ほぼムリ
  ファイルI/O、プロセス間通信、デバイス操作 …ユーザー操作抜きでは手も足も出ない
- インターネット アクセスは自由
  遠隔操作で掲示板に書き込むマルウェアなら作れそう
- あとは、騙せばいいのよ～♪

  ユーザーを騙して、Webメールのアクセス権を貰うとか、いろいろ…
- そんなこんなで、作れたとしましょう♪

Windows ストア アプリで ウイルスを作るには!?

・ストアの審査をかいくぐって
マルウェアをバラ撒くには?

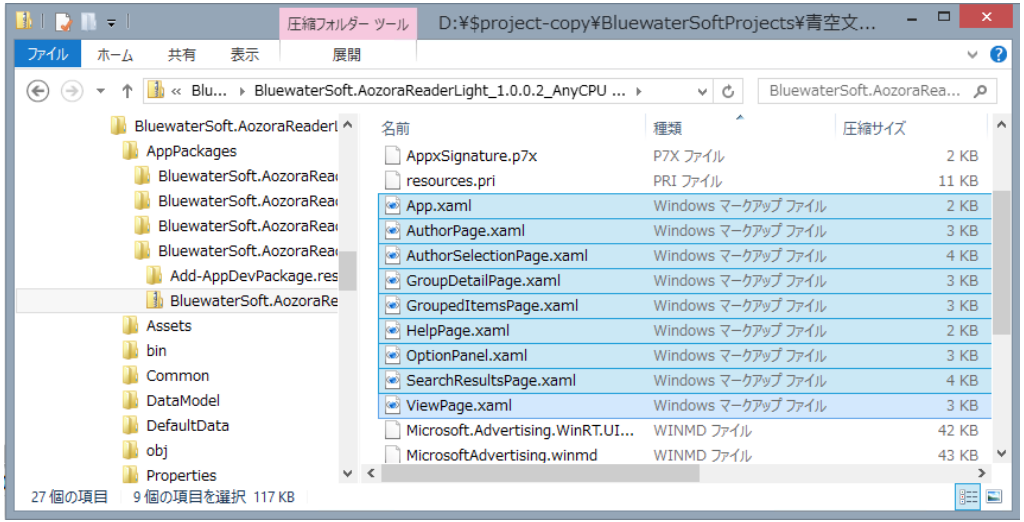
ストアの審査を
かいくぐるには?

審査では動作しないように時限式にでもしておいて、あとは見つからないようにいかに巧妙にコーディングするか、です♪

敵さんは、WACKより高精度な解析ツールを使ってることも忘れずに。
(自動セキュリティ検査に1時間以上)

バラ撒き成功♪

- 隠し画面なんかを XAML で作ってると間違いなく見つかる。
  ↓パッケージの中身、XAMLは丸見え



Windows ストア アプリで ウイルスを作るには!?

Community OpenDay

Supported by Microsoft

・自分の身元を隠すには?

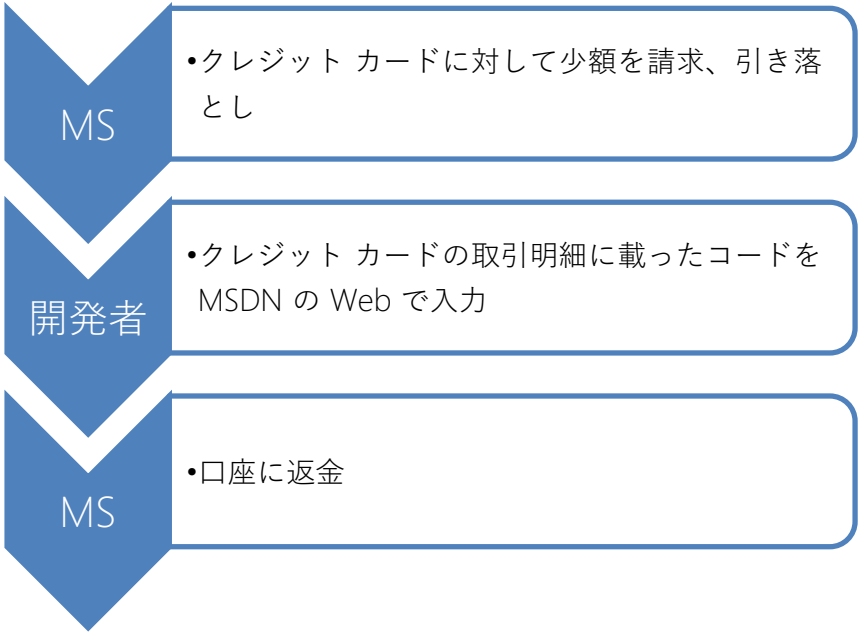
自分の身元を隠せるか?

- マルウェアが露見したときに、犯人が分からないようにしなくては!!
- しかし、開発者登録には、本人名義のクレジットカードが必要

http://msdn.microsoft.com/ja-jp/library/windows/apps/jj863494.aspx#verifying_accounts

日本で、身元を隠して銀行口座を開くのは無理ゲー … orz

アカウントの検証
(無償キャンペーンの場合)



Windows ストア アプリで ウイルスを作るには!?

Community OpenDay

Supported by Microsoft

・まとめ

まとめ

立ちはだかる3つの壁

1. (ウォール・マリア)
   プラットホームの制限
2. (ウォール・ローゼ)
   ストアの審査
3. (ウォール・シーナ)
   身元の保証

安全で安心

- 従来のWindowsとは
  異次元

  Windows reimagined

- 代償は、開発者の苦労
  でも、理由が分かれば
  苦労し甲斐があるよね♪

参考URL

いかに安全で安心な Windows ストア アプリのエコシステムを Microsfot は築こうとしているのか

- MSDN Blogs:
  信頼できる Metro スタイル アプリを提供する
  http://blogs.msdn.com/b/b8_ja/archive/2012/05/25/metro-trustworthy.aspx
- TechNet Blogs:
  Windows 8 セキュリティ特集 #5
  Windows ストア アプリ
  http://blogs.technet.com/b/jpsecurity/archive/2012/11/29/3535394.aspx

ご清聴ありがとうございました