Windows 8 セキュリティ
AppContainerによるSandbox

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver 2.00.01

AppContainer概要

- Windows 8から導入されたサンドボックス
- 新たな “AppContainer”によって実現されている
- Windows Store Appは原則AppContainerで動作する
- ファイルアクセスや他プロセスへのアクセスなどが制限される

これまでのアプリとの違い

- Windows Store Appはこれまでデスクトップアプリと動作環境が大きく異なる
- 制限が多く、隔離された環境となりセキュリティ面でも大きく向上している

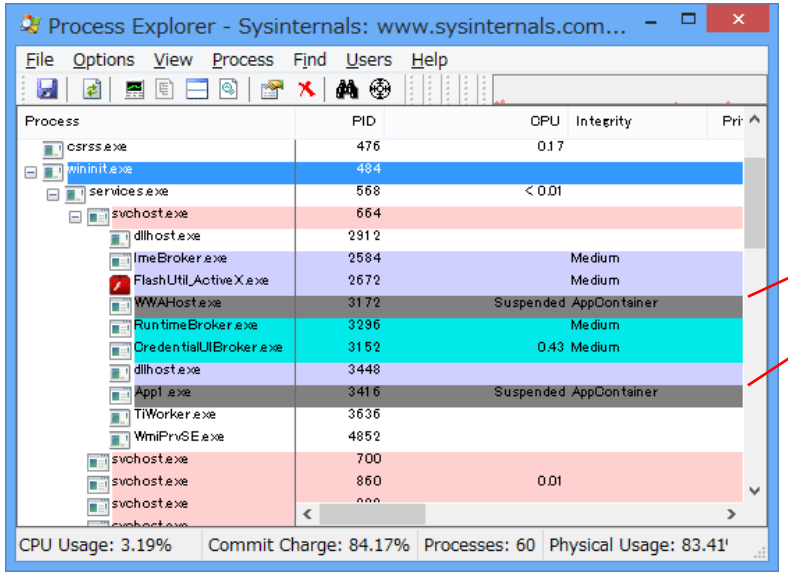
	Windows Store App	Desktop App
Integrity Level	Low	Medium
AppContainer	On	Off
Kernel Object	各アプリごとの名前空間	セッション内で共有

/AppContainer コンパイラオプション

- AppContainerとして動作するPEに適用されるフラグ
- Windows Store AppのEXEに適用される
- PEに新たなオプション
  - PEのDLL Characteristicsに新たな値が定義された模様
    - Windows Store AppのPEのDLL Characteristicsはフラグ0x1000がオン
      （2010年のPEの仕様では予約済みとされている値）

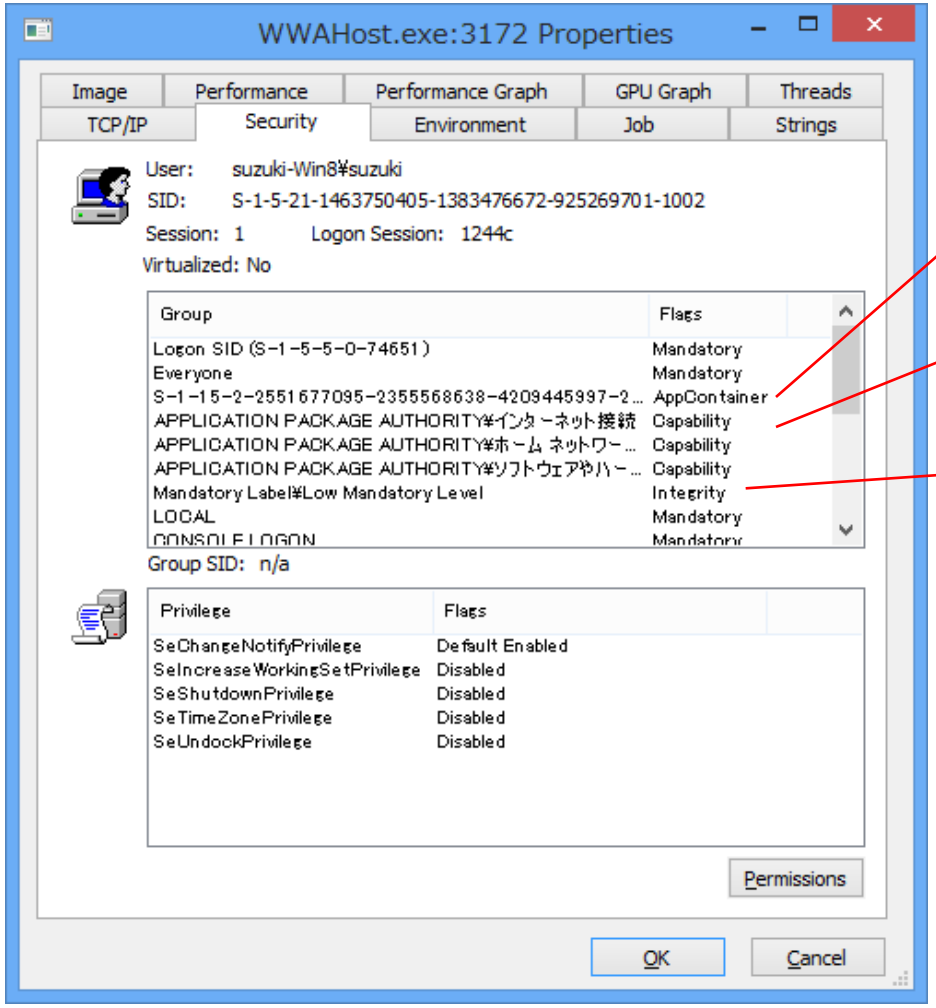
AppContainerのアクセストークン

- Process Explorer
  - Windows Store AppのIntegrity LevelはAppContainer
- Windows SDKのヘッダファイル
  - AppContainerに対応するIntegrity LevelのSIDは存在しない
  - AppContainerは既存のLow, Medium, Highといったintegrity Levelとは別の仕組み
- AppContainerプロセスのIntegrity Level
  - SECURITY_MANDATORY_LOW_RID (Low)と同じ
- プロセストークンに新たな値
  - Windows 8より、GetTokenInformation APIで取得できる値に"TokenIsAppContainer"が追加された



Process Explorerでは
Integrity LevelがAppContainerと表示される

AppContainerプロセスのアクセストークン情報



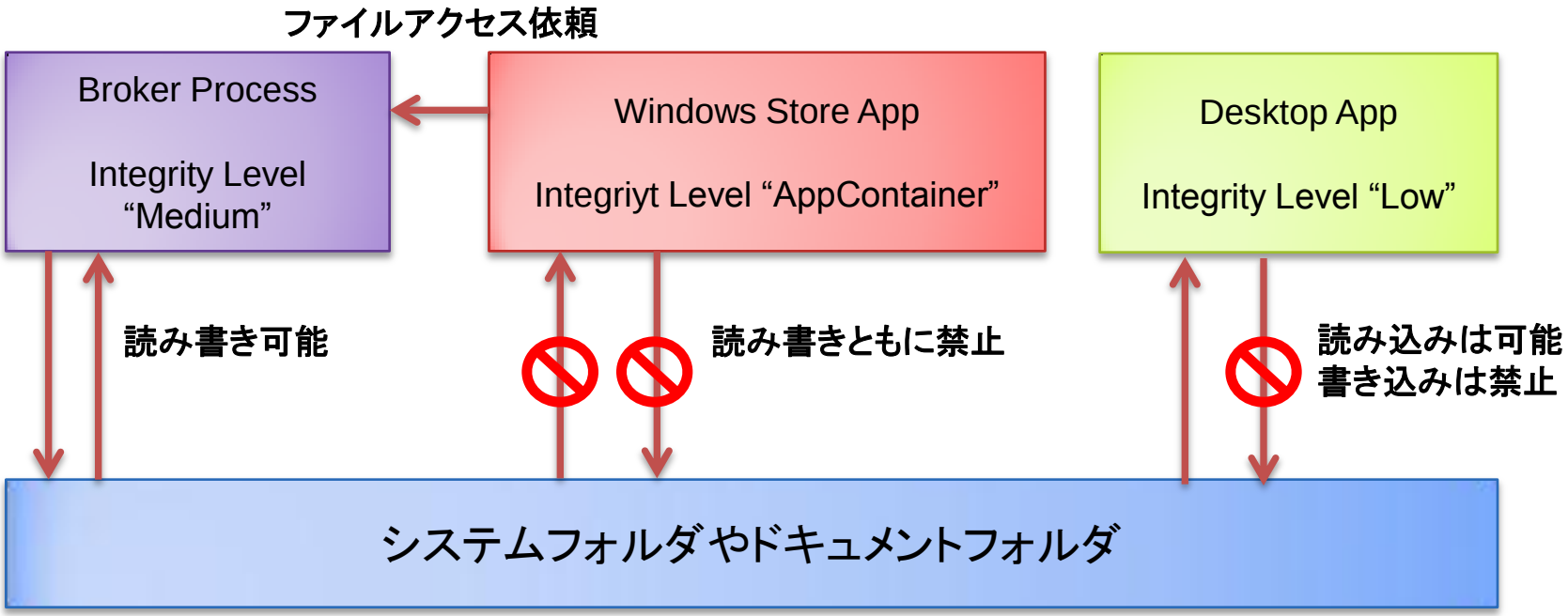
AppContainerを表すSIDが存在

CapabilityもSIDで表現される

Integrity Levelは “Low”

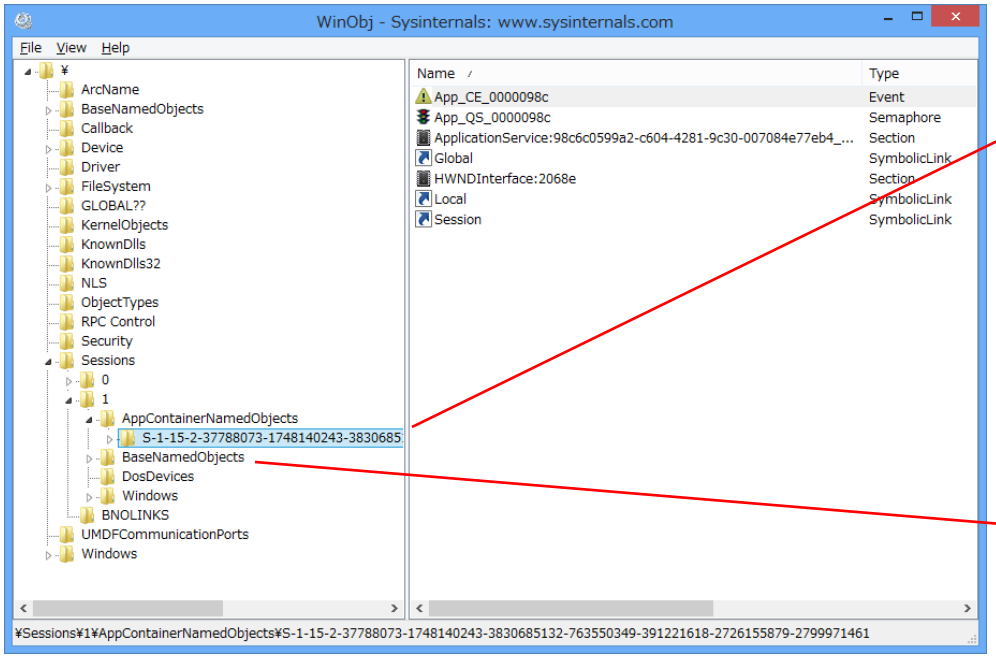
フォルダ・ファイルアクセス制限

- AppContainerからはシステムフォルダやドキュメントフォルダなどほとんどのファイルの直接の読み込みが禁止される
- ファイルアクセスは原則Runtime Broker経由(Capabilityによる制御)
- 今までのデスクトップアプリとは読み込みも禁止される点で大きく異なる
- アクセスするには、ALL APPLICATION PACKAGESグループに明示的にアクセス権を設定するなどの必要がある



カーネルオブジェクトの分離

- カーネルオブジェクトツリーに、各Windows Store App専用のディレクトリが作成される
  - AppContainerNamedObject
    - S-1-15-2-XXXX.... （一つ目のAppContainerのSID）
    - S-1-15-2-YYYY.... （二つ目のAppContainerのSID）
- デフォルトでデスクトップアプリが作成する同一セッション内のオブジェクトへのアクセスは制限される
- Windows Store Appがデスクトップアプリの持つオブジェクトに対して操作することができない（攻撃できない）
  （＊ALL APPLICATION PACKAGEグループに対するアクセス許可を明示的に設定するなどでアクセス可能）

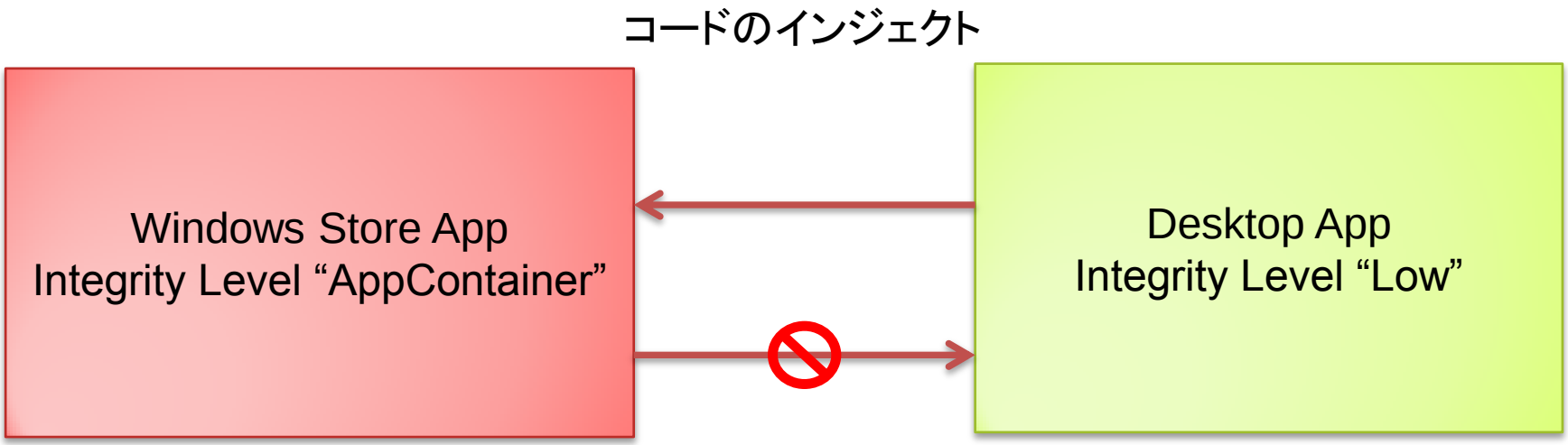


AppContainerのオブジェクト名前空間
AppContainerから名前を指定して
オブジェクトの作成、オープンを行う場合
こちらが参照される

セッションのオブジェクト名前空間
デスクトップアプリから名前を指定して
オブジェクトの作成、オープンを行う場合
こちらが参照される

プロセスメモリアクセス制限

- AppContainerからは通常のデスクトップアプリプロセスへのメモリアクセスはできない（読み書きともに不可）
- 逆（デスクトップアプリ→Windows Store App）のメモリアクセスは可能
  - Windows Store App型のIEなどへのコードインジェクションは可能



Internet Explorer 10

- Windows Store App型のInternet Explorer 10はAppContainerで動作
- これまでIntegrity Level “Low”として動作していたプロセスがAppContainerとして動作している
- 脆弱性攻撃を受けた際の被害が大きく抑えられる

まとめ

- Windows Store Appは制限の大きいサンドボックス環境で実行される
- 今までの、Integrity Level “Low” よりも更に強い制限
- Windows Store Appが攻撃され乗っ取られた場合でも、システムへの影響はかなり低く抑えられる
- デフォルトではWindows Store Appからデスクトップアプリへの侵入はできない（Sandboxの実装に脆弱性がない限り）
- Windows Store App型のIEはAppContainerとして動作する
  - IEの脆弱性を突いた攻撃が成功してもできることが限られている
  - ただし、デスクトップアプリなどからマルウェアに感染した場合、MITBなどの攻撃を受ける可能性はまだ存在する