Monthly Research

機械学習のセキュリティ技術応用

株式会社ＦＦＲＩ
http://www.ffri.jp

Agenda

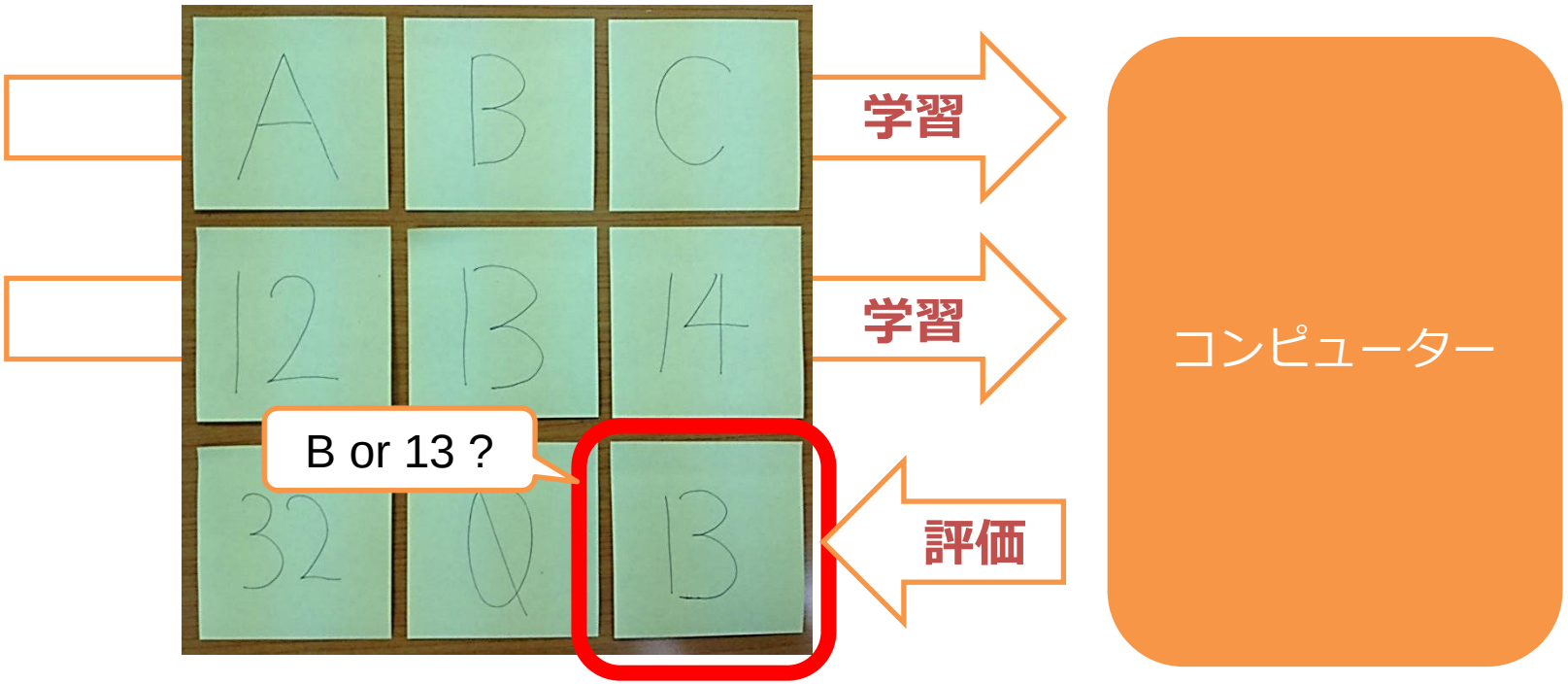
1. はじめに
2. 機械学習概要
   - 機械学習とは
   - 機械学習を取り巻く環境
   - 機械学習の種類
   - 代表的なソフトウェア実装
3. 機械学習に基づいたマルウェア検知
   - 機械学習に基づいたマルウェア検知
   - 試作の概要
   - 学習用/評価用データ
   - Cuckoo Sandbox
   - Jubatus
   - 評価結果
   - その他応用の可能性
4. まとめ
5. 参考資料

はじめに

- 本書では、始めに機械学習の概要について説明し、その後具体的な応用例として機械学習に基づいたマルウェア検知について紹介する。
- 著者は、セキュリティ研究者であり機械学習の専門家ではない。本書は、あくまで機械学習のセキュリティ技術への応用について考察、紹介するものである。
- 本書に記載のマルウェア検知の取り組みは、機械学習の応用例を示すことを目的とした試作のひとつである。

機械学習とは

- コンピューターになんらかの学習をさせることで、その経験に基づいた予測や推定をさせる手法・技術
- 人工知能に関する研究がベースとなっている



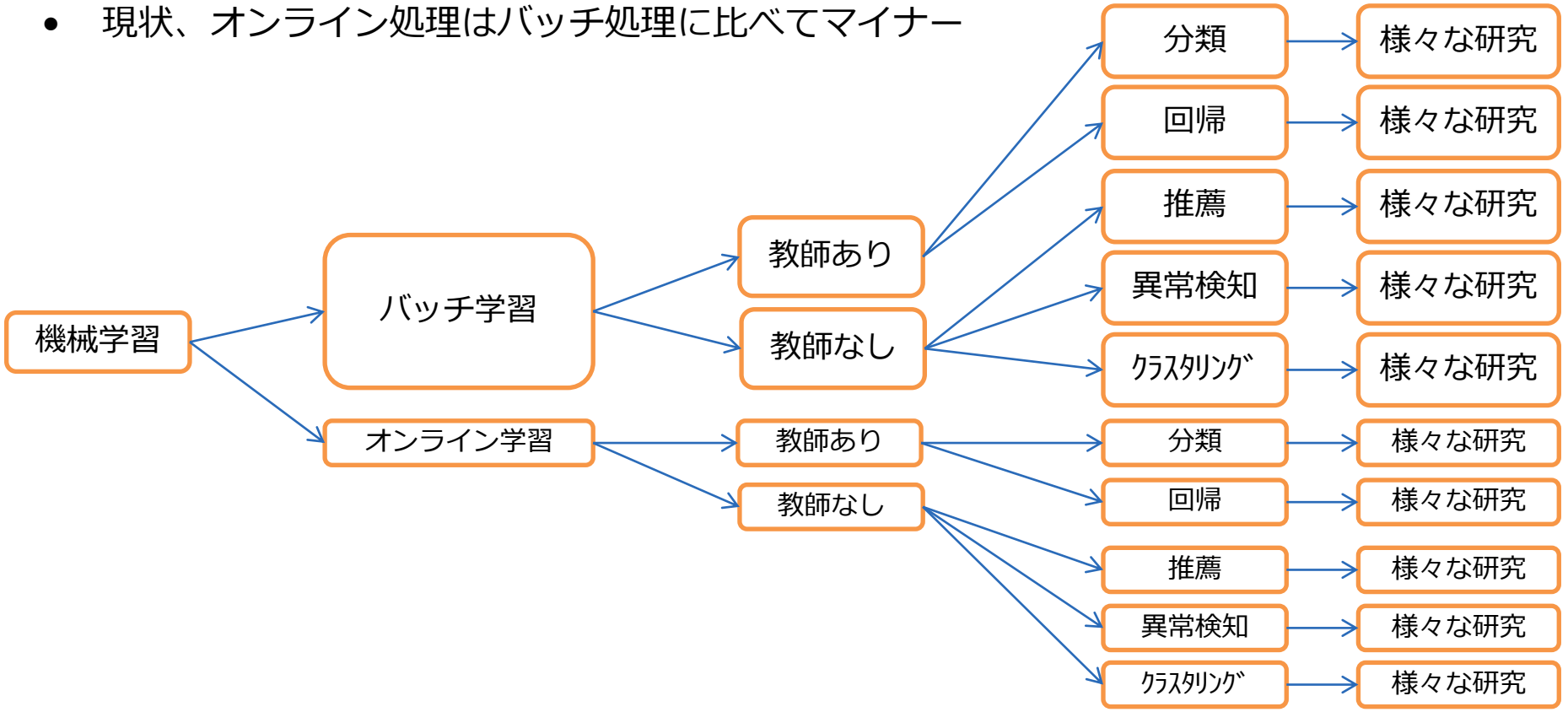
機械学習を取り巻く環境

- 近年、大量のデータから有益な情報を見出すビッグデータ解析が注目されている
  - Webを中心としたECやオンラインゲーム、BI（Business Intelligence)等
  - 今後M2M等の進展により更なるデータの増加が見込まれる

- ビッグデータ解析の手法としての機械学習
  - 蓄積された膨大なデータを分析し、未来を予測する
  - 業界、領域毎に技術の浸透度、活用度は異なる
  - セキュリティ業界での活用はまだこれから

機械学習の種類

- 「機械学習」は、様々なテーマ、手法を包含した総称
- 大雑把には下記のように分類される
- 現状、オンライン処理はバッチ処理に比べてマイナー



機械学習の種類

- バッチ学習/オンライン学習
  - バッチ学習：蓄積したデータを一括で処理する（データが全て揃っている）
  - オンライン学習：逐次データを処理する（データが随時到着する）

  ⇒　リアルタイム性の違い

- 教師あり/教師なし
  - 教師あり：正解が存在するデータで学習する
    例）学習結果(りんご＝果物)に基づいてトマトが野菜か果物か判断する(分類)
    学習結果(駅からの距離/家賃)に基づいて物件Xの家賃を推定する(回帰)
    学習結果(人=哺乳類, 鮪=魚類)に基づいて鯨に類似したものを推薦する(推薦)
  - 教師なし：正解が存在しないデータで学習する
    例）似た者同士をグルーピングする(クラスタリング)
    普段と違う正常でないデータを発見する(異常検知)

  ⇒　取り扱う問題の違い

代表的なソフトウェア実装

- 「分類」、「クラスタリング」等を行う具体的な手法は、主に学術界(#)において日々研究がなされており、様々な手法が存在する（本書では言及しない）

- 実際に利用可能なフレームワーク、ライブラリは下記の通り（一例）
  - Hadoop
    - Hadoop自体は機械学習の仕組みは持たないが、MapReduceをベースとした3rd partyの機械学習フレームワークが複数存在
  - Apache Mahout
    - 上記 3rd partyライブラリの代表格。バッチ処理によるクラスタリング、分類等をサポート
  - Jubatus
    - オンライン機械学習向け分散処理フレームワーク（後述）
  - その他ライブラリ
    - Libsvm - http://www.csie.ntu.edu.tw/~cjlin/libsvm/
    - dlib ml - http://dlib.net/ml.html
    - Shark - http://shark-project.sourceforge.net/

代表例はICML- http://icml.cc/2013/

機械学習に基づいたマルウェア検知

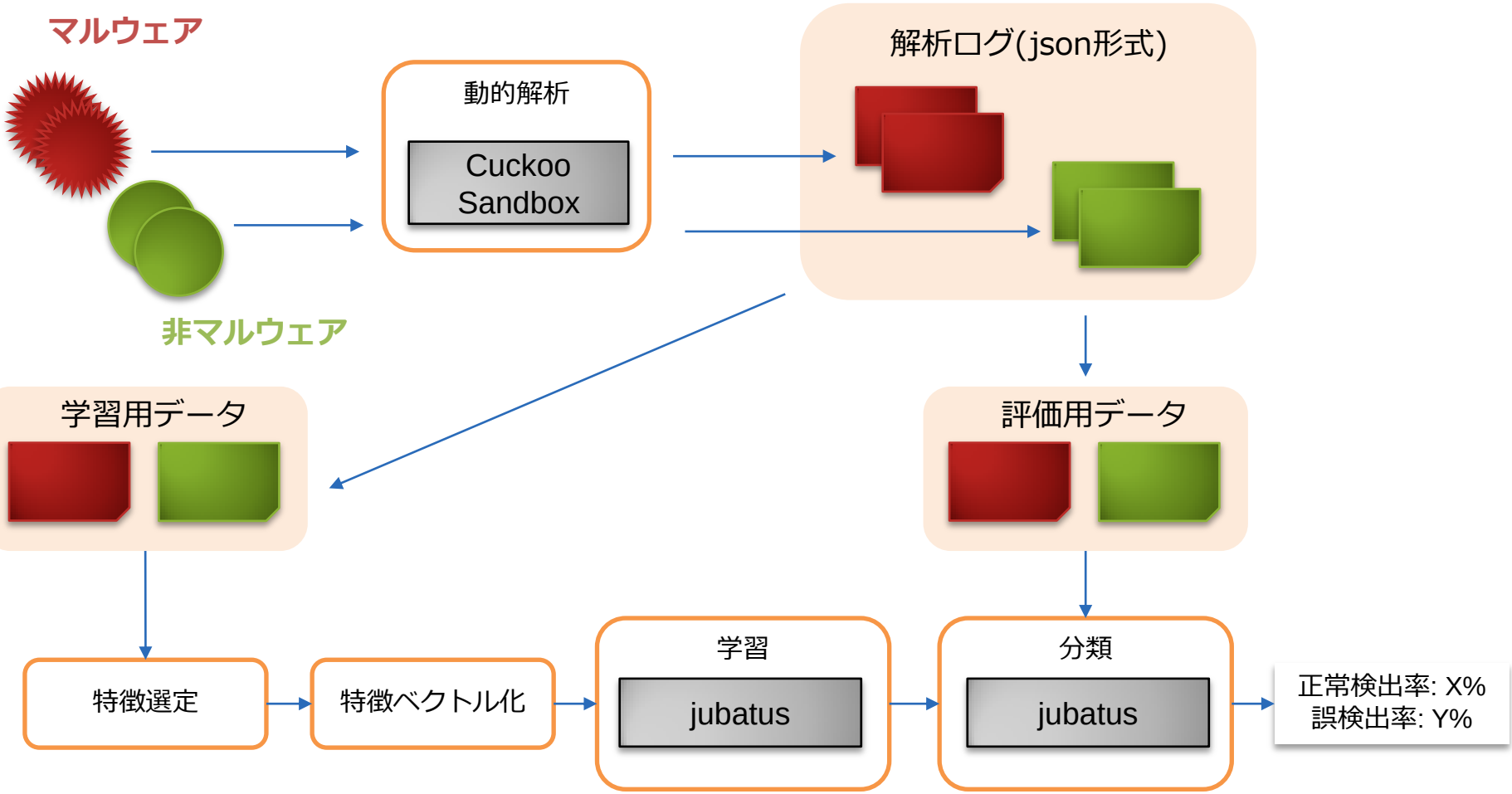
- 「分類」に基づいたマルウェア検知の仕組みを試作

- 主な工程は下記の通り
  1. マルウェア、非マルウェアについて学習用、評価用のデータを用意

  2. 学習用データから特徴を選定し、特徴ベクトル化(データ化)する
     - 当該領域に属する専門家の仕事(知識、経験に基づいて選定)
     - 本試作では、Cuckoo Sandboxの解析結果からAPIログ等を抽出、加工

  3. 抽出した特徴ベクトルにラベル(正解)を付けて学習を実施
  4. 評価用データから同様に特徴ベクトルを抽出し、分類を実施
     - 機械学習フレームワークとしてJubatusを利用

試作の概要


マルウェア
非マルウェア
動的解析
Cuckoo Sandbox
解析ログ(json形式)
学習用データ
評価用データ
特徴選定
特徴ベクトル化
学習
jubatus
分類
jubatus
正常検出率: X%
誤検出率: Y%

学習用/評価用データ

- マルウェア / 2641件（学習用：1320 / 評価用：1321）
  - 直近6ヵ月間の最新マルウェアからランダムサンプリング
  - metascan(#)を利用し、10社以上のアンチウイルス製品で検出率を調査
    ⇒　平均検出率：約30%、最高検出率：約60% (2013年4月時点)

- 非マルウェア / 1803件（学習用：893 / 評価用：910）

http://www.opswat.com/products/metascan

Cuckoo Sandbox - http://www.cuckoosandbox.org

- オープンソースのマルウェア動的解析システム
  - 仮想環境内でマルウェアを実行
  - 実行時のふるまいをモニタリング
  - VirusTotal連携、yara連携等
- 社内のマルウェア解析用ネットワークにシステムを設置、実行
  - 1検体当り90秒実行
- 解析ログ中に含まれるAPIログ等を抽出、加工し特徴ベクトル化

Cuckoo Sandboxの解析ログ(APIログ)


```
"calls": [
    {
        "category": "system",
        "status": "FAILURE",
        "return": "0xc0000135",
        "timestamp": "2013-02-28 12:03:49,478",
        "thread_id": "420",
        "repeated": 0,
        "api": "LdrLoadDll",
        "arguments": [
            { "name": "Flags", "value": "1242916" },
            { "name": "FileName", "value": "C:¥¥WINDOWS¥¥system32¥¥VB6JP.DLL" },
            { "name": "BaseAddress", "value": "0x00000000" }
        ]
    },
    {
        "category": "registry",
        "status": "SUCCESS",
        "return": "0x00000000",
        "timestamp": "2013-02-28 12:03:49,528",
        "thread_id": "420",
        "repeated": 0,
        "api": "NtOpenKey",
        "arguments": [
            { "name": "KeyHandle", "value": "0x00000058" },
            { "name": "DesiredAccess", "value": "1" },
            { "name": "ObjectAttributes", "value": "Registry¥¥MACHINE¥¥System¥¥Curre
        ]
    },
```

Jubatus – http://jubat.us/ja

- (株)Preferred Infrastructure、NTTｿﾌﾄｳｪｱｲﾉﾍﾞｰｼｮﾝｾﾝﾀが共同開発
- 現時点での最新バージョンは0.4.4(2013/06/21)
  - 1st リリースは、0.1.0(2011/10/26)
- ライセンスは、LGPL v2.1
- 分散処理に対応したオンライン機械学習フレームワーク
  - 継続的なマルウェアの収集、分析、モニタリング
  - サーバー増設によるスケールアウト
- 下記の機械学習をサポート
  - 分類/回帰/推薦/グラフマイニング/統計分析/異常検知
- C++/Python/Ruby/Java向けのSDKを提供

評価結果

- 正常検出率/誤検出率は、採用する特徴、特徴の加工方法、学習時のパラメータ等で変動
- 2013年6月時点における最良成績は下記の通り
  - 従来のパターンマッチング、ジェネリック検出等に対して高い検出率を確認
  - 理論上、1000ファイル当たり8件の誤検出が発生するため改善の余地が残る
- 誤差を考慮すると統計上、データ数が不十分であるため追加、継続検証が必要

マルウェア(件)	非マルウェア(件)	正常検出率(%)	誤検出率(%)
1321	910	94.5495	0.8791

(2013年6月時点)

その他応用の可能性

- データを確保することができれば様々な応用が可能
  - 分類 x マルウェア → マルウェア検知(本試作)
  - クラスタリング x マルウェア → マルウェアの家系分類、新種検出
  - 異常検知 x 通信データ → C&C通信検知
  - 異常検知 x 通信パターン → マルウェア感染検知
  - 異常検知 x 認証ログ → なりすまし検知、etc.

まとめ

- ビッグデータ解析の手法として機械学習が注目されている
- 機械学習をセキュリティ技術にも応用することが可能
  - 本格的な応用はこれから
- 一例としてマルウェア検知を試作
  - 課題は存在するものの従来技術に対して非連続的な可能性を確認
- マルウェア検知以外にも様々な応用の可能性が期待される

参考資料

- Jubatus
  - http://jubat.us/ja/
- 機械学習チュートリアル
  - http://www.slideshare.net/unnonouno/jubatus-casual-talks
- Automatic Analysis of Malware Behavior using Machine Learning
  - http://pi1.informatik.uni-mannheim.de/malheur/