Monthly Research

ブラウザへの新しい攻撃と新しい対策

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

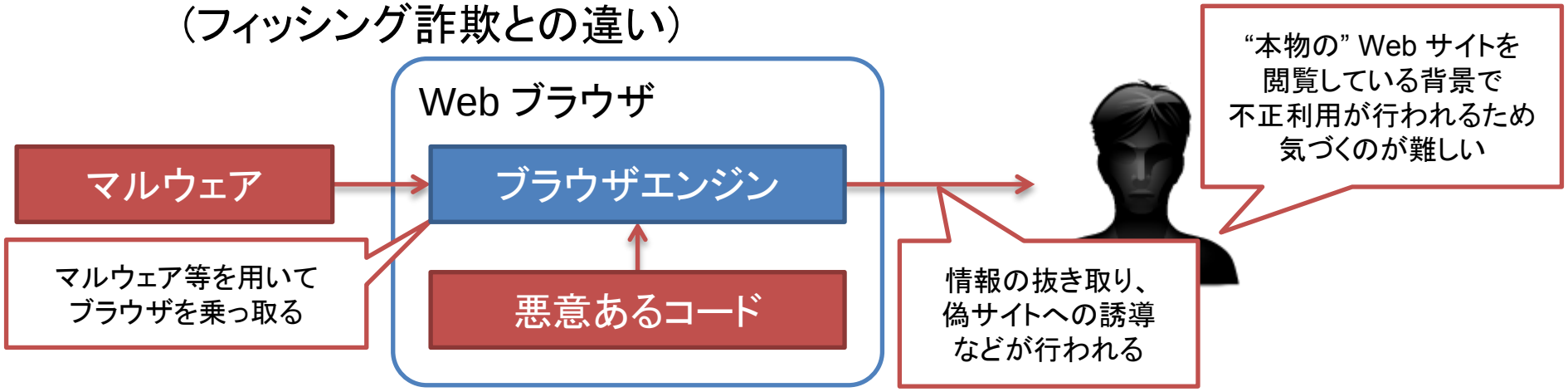
Ver2.00.01

ブラウザを取り巻く変化

- ブラウザから情報を盗み取るための新しい攻撃
  - フィッシングやキーロガーなどの手法からの進化
    ⇒ Man in the Browser (MITB) 攻撃
- 外部からの脆弱性攻撃への新しい対策
  - ブラウザのような大きなコードベースは脆弱性を生みやすい
    ⇒ ブラウザのプロセス分離

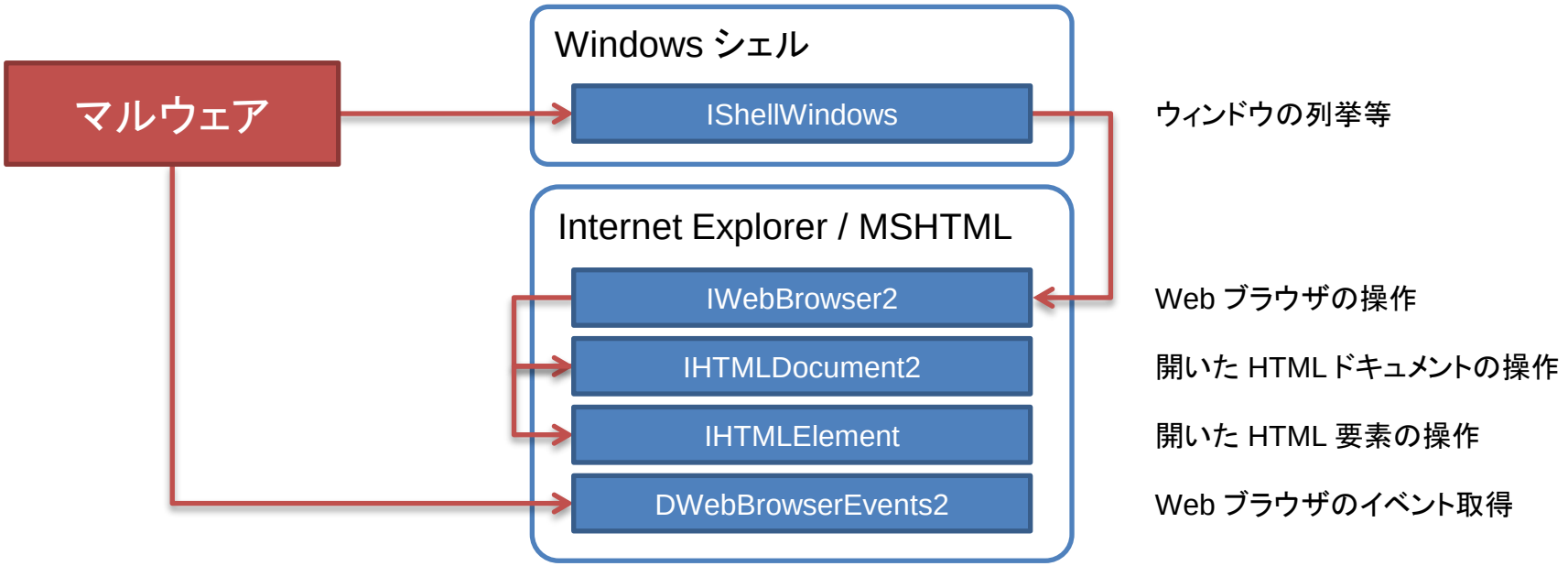
Man in the Browser (MITB) 攻撃

- マルウェア等によってブラウザを乗っ取ることによって、認証情報を盗むなどの攻撃の総称
- 金融詐欺に悪用される新しい手法となりつつある
  - ブラウザの正しいセッションに便乗して不正操作を紛れ込ませる（キーロガー等による古典的な ID 窃盗との違い）
    - オンラインバンクにおける二要素認証をも回避する
  - “本物の” Web サイトの表示内容をマルウェアによって置き換える（フィッシング詐欺との違い）



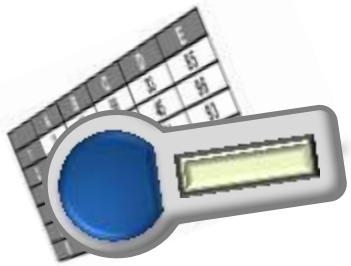
MITB 攻撃の例

- DCOM コンポーネントの利用
  - 外部プロセスから Internet Explorer 等の COM コンポーネントを開く
  - 開いたコンポーネントから IE を操作する
    - 操作のためのインタフェースは（元々正当な理由のために）公開されている



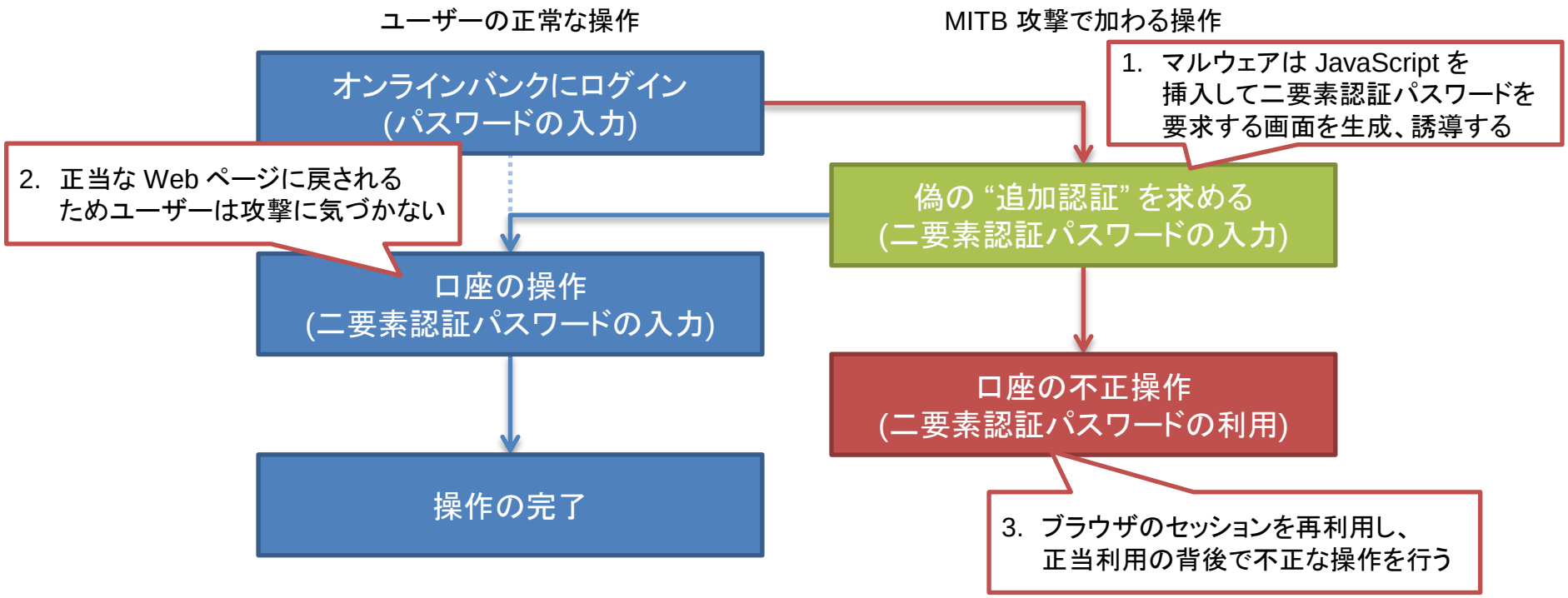
Operation High Roller

- 2012年に発生した大規模な金融詐欺
  - 米国やヨーロッパ諸国が主要な対象に
  - 2ヵ月間で最大で20億ユーロの被害が発生（およそ 2,000億円）
- マルウェアと MITB 攻撃の組み合わせによって“二要素認証”を回避
  - 二要素認証: オンラインバンクのアカウントとは別に再利用の難しいパスワードや暗証番号を求める認証方式
    - カード式の乱数表
    - ハードウェアトークンによるワンタイムパスワード
  - 二要素認証はユーザーの ID とパスワードのみを盗む古典的な金融詐欺として有力な手法だと考えられている



Operation High Roller における MITB 攻撃

- MITB 攻撃を利用して偽サイトを生成、誘導
  - 挿入した JavaScript を用いて本物のサイトを書き換える
  - 盗んだ認証情報を基に不正操作を紛れ込ませる



MITB への対策 / まとめ

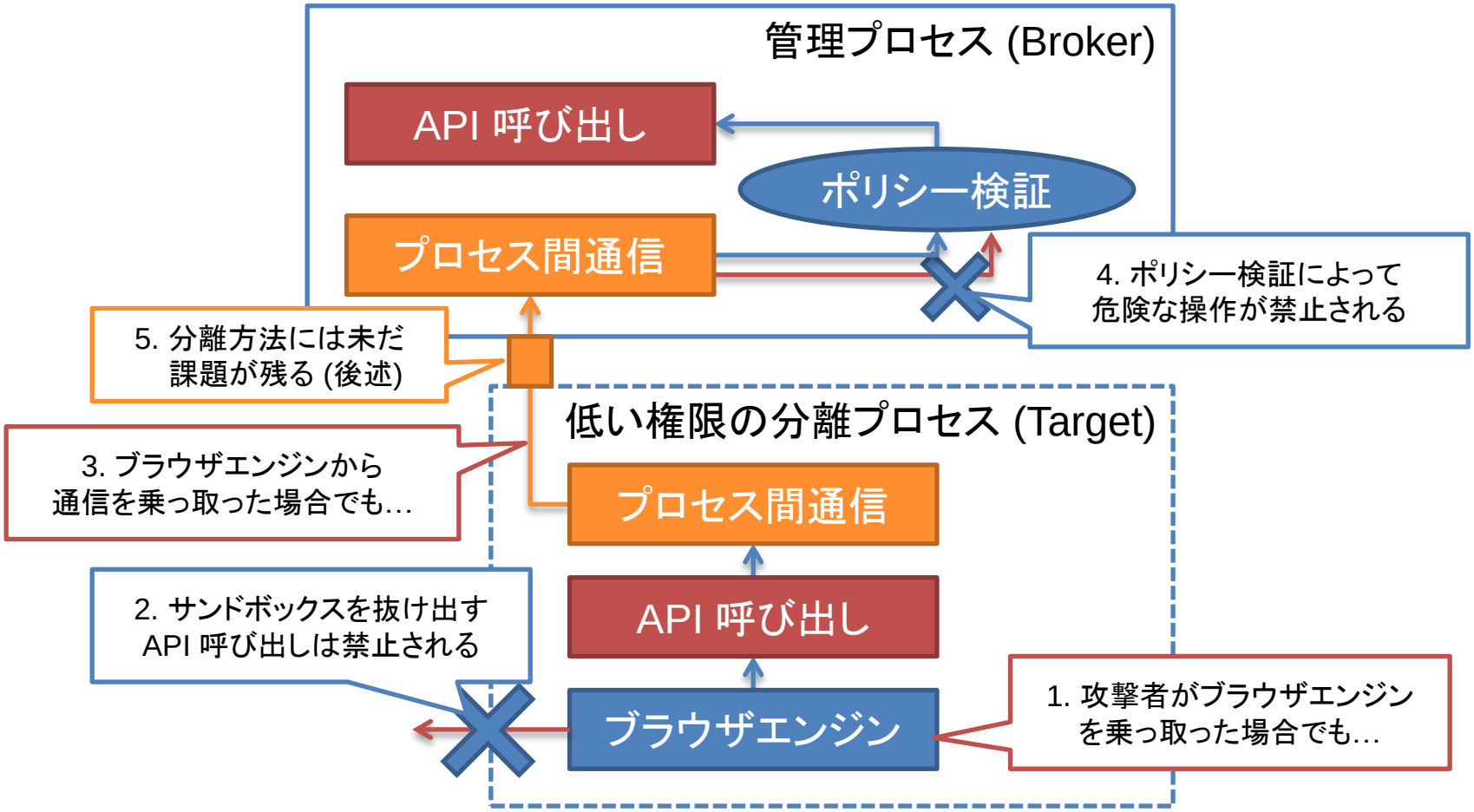
- ユーザー側で気づくことは難しい
  - URL が本物である上に、攻撃者のスキルも向上しつつある
- セキュリティ製品によるフックの防止
  - Rootkit などによって妨害を受けない限り、
    MITB 攻撃を発見することは（技術的には）比較的容易
  - 一部の統合セキュリティ製品におけるブラウザ保護の利用
- より堅牢な保護手法とより良いユーザーへの通知が必要とされる
  - FFRI においては対策手法を研究開発中

新しい対策: ブラウザのプロセス分離

- ブラウザエンジンやサードパーティーのプラグインは
  常に攻撃の危険にさらされてきた
  - 経験則: 大きく複雑なコードほど潜在的なバグや脆弱性は多い
  - ブラウザエンジンは複雑なデータを扱う巨大なプログラム
- 攻撃される危険性の大きいブラウザエンジンの一部を
  権限の低い別プロセスとして分離する
  - “サイトを見ただけで感染する” 種類の脆弱性攻撃を最小化
  - 実装例:
    - Microsoft Internet Explorer (Windows Vista 以降)
    - Google Chrome
    - Safari (ver.5 以降)

※ Firefox も最近のバージョンでプロセス分離を実装したが、現状ではセキュリティ上の効果が小さいため除外した。

ブラウザのプロセス分離とサンドボックス化



※ 参考: http://www.chromium.org/developers/design-documents/sandbox/

プロセス分離への攻撃と課題 / まとめ

- 経験則: 大きく複雑なコードほど潜在的なバグや脆弱性は多い
  - 課題: 現状では、分離したプロセス間で比較的
    大きく複雑 (かつ重要) なデータをやり取りする
    - 攻撃: プロセス分離メカニズムの突破 (CVE-2012-1846)
    - 攻撃: 不十分なセキュリティ分離の悪用 (CVE-2011-3084)
  - ブラウザの実装によってこの手法が強化されると予想される
    (セキュリティとパフォーマンスのバランス)

- 課題があるとはいえ、最新のセキュリティ機構である
  プロセス分離はブラウザへの脆弱性攻撃の影響を
  最小化するために十分働いていると考えられる