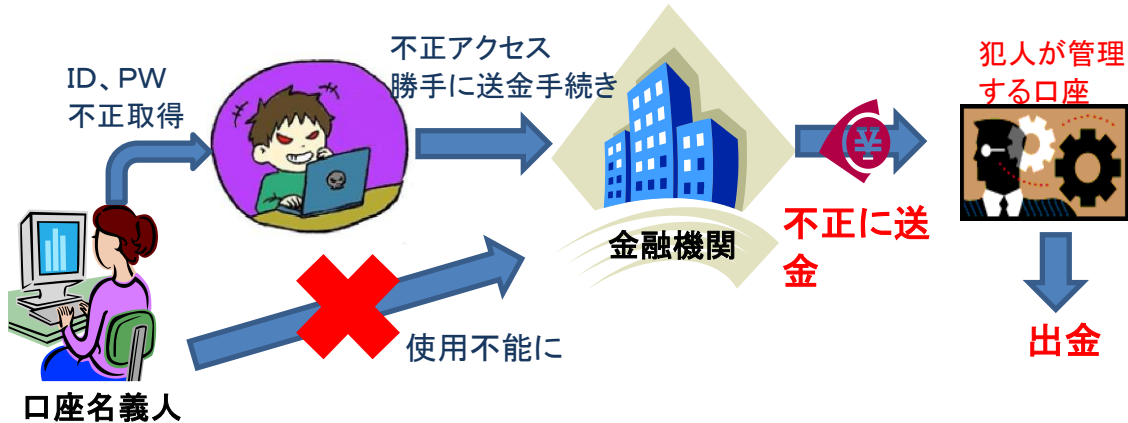


## インターネットバンキングによる不正送金被害増加中

### 1 インターネットバンキング不正送金事案とは

都市銀行や地方銀行等の金融機関が行っているサービスであるインターネットバンキングを悪用した犯罪で、インターネットバンキング用のID・パスワードを不正に取得したうえで、不正アクセスして、他人名義の銀行口座へ不正送金する事案



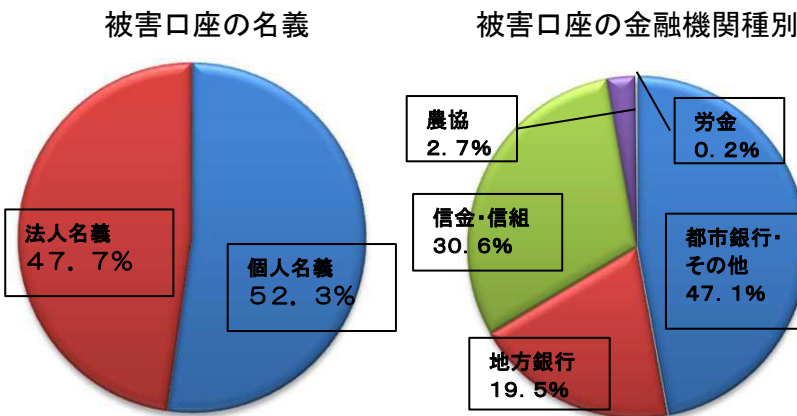
### 2 インターネットバンキング不正送金発生状況

#### ① 過去5年間の不正送金発生状況

	平成23年	平成24年	平成25年	平成26年	平成27年
発生件数	165件	64件	1315件	1876件	1495件
被害額(円)	約3億800万	約4800万	約14億600万	約29億1,000万	約30億7,300万

※被害額は、犯人が送金処理を行ったすべての額

#### ② 平成27年中における被害内訳



#### 被害状況の特徴

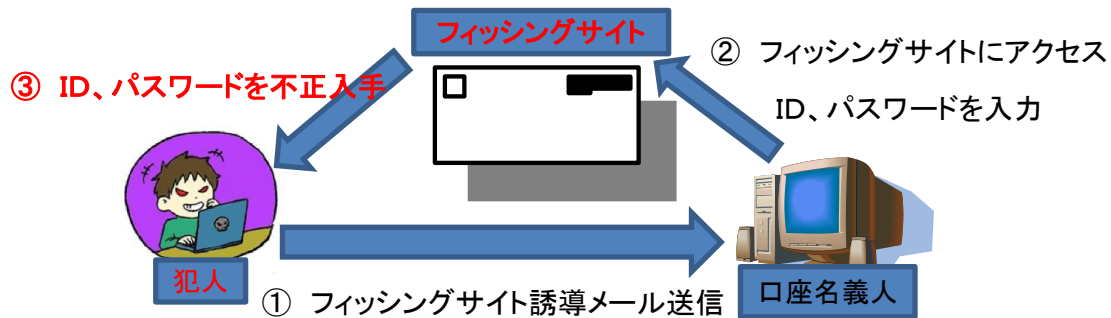
- 法人口座被害の増加により被害額が過去最悪を記録
- スマートフォン等にSMSを送信して偽サイトに誘導するフィッシングを初めて確認
- 信金・信組、農協・労金に被害が拡大
- 特に信用金庫の法人口座被害が急増
- 被害口座名義人の多くがセキュリティ対策未実施

法人口座の被害が急増しています。セキュリティ対策を徹底して下さい。



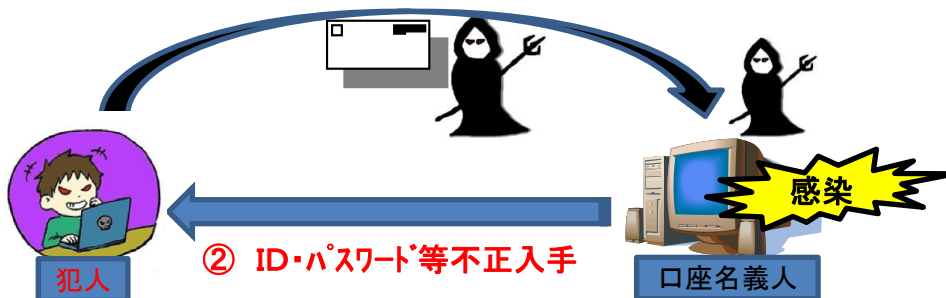
### 3 ID・PWの不正取得被害の主な態様

#### ① フィッシングサイトによる不正入手



#### ② 不正プログラム(ウイルス等)による不正入手

##### ① 不正プログラム添付メールの送信



### 4 利用者に講じて頂きたい対策

#### ① パソコンのOS、ソフトウェアを最新の状態に

ウイルスは、パソコンのOSやインストールされている各ソフトのぜい弱な部分を狙って侵入します。OSやソフトウェアは、常に最新の状態に更新しましょう。

#### ② ウイルス対策ソフトを導入

不正送金が行われた口座の名義人が使用しているパソコンを確認すると、インターネットバンキングのID・パスワード等を盗み取るウイルスに感染していることが多いです。

インターネットにアクセスするパソコンには、必ずウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新しましょう。

#### ③ フィッシングサイトに注意

電子メールにより、本物のウェブサイトと酷似したフィッシングサイトに誘導されないように、発信元に心当たりのない電子メールに注意しましょう。

金融機関のサイトへのアクセスは、かならずトップページからアクセスするようにして下さい。

また、金融機関が電子メールで口座番号や暗証番号、個人情報を問い合わせることはありません。もし、これらの情報の入力を求めるメールがあれば、それはフィッシングメールですので、入力を絶対にしないで下さい。

#### ④ ワンタイムパスワードなど金融機関が行っているセキュリティ対策を積極的に利用

不正送金被害を防止するためには、携帯電話のメールアドレスやトークン(ワンタイムパスワード生成器)を使ったワンタイムパスワードの利用が効果的です。

その他、金融機関が提供するセキュリティの高い対策がありますので、詳しくは口座を開設している金融機関に相談して、積極的に利用しましょう。

サイバー犯罪についての相談をお寄せ下さい。

大分市荷揚町4番35号

大分県警察本部生活安全部生活環境課サイバー犯罪対策室

Tell:097-534-2048

