セコムIS研究所
Intelligent Systems Laboratory

フィッシング詐欺の手法

JPNIC・JPCERT/CC
セキュリティセミナー2005
「Webのセキュリティ」

2005年10月6日

セコム IS研究所 金岡 晃

フィッシング詐欺とは

セコムIS研究所 Intelligent Systems Laboratory

フィッシング詐欺とは

正規組織からの通知と見せかけてユーザを誘導し、秘密情報などの情報詐取を行い、最終的に金銭の詐取を行なうもの。主に金銭的な取引を行うウェブサイトへのログイン情報などを取得し、攻撃者が金銭的な利益を得ることを目的としている。

フィッシング詐欺の流れ

誘導

それらしい名称を用いたり、利用者が気づかないように設定変更を行い、情報詐取を目的とするサイトなどへ誘導する。
例）金融機関からを装ったメール

情報取得

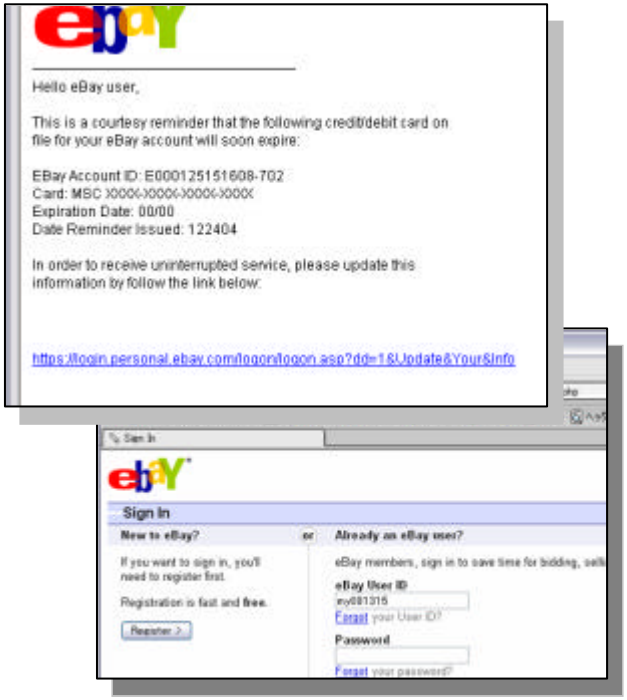
正規のサイトを偽装したり、不正に情報を詐取するツールを自動ダウンロード・インストールすることで情報を取得する。
例）金融機関のサイトを偽装し、アカウント情報を詐取する

なりすまし

詐取した情報を用いて、本人になりすます。
例）金融機関サイトへのログイン

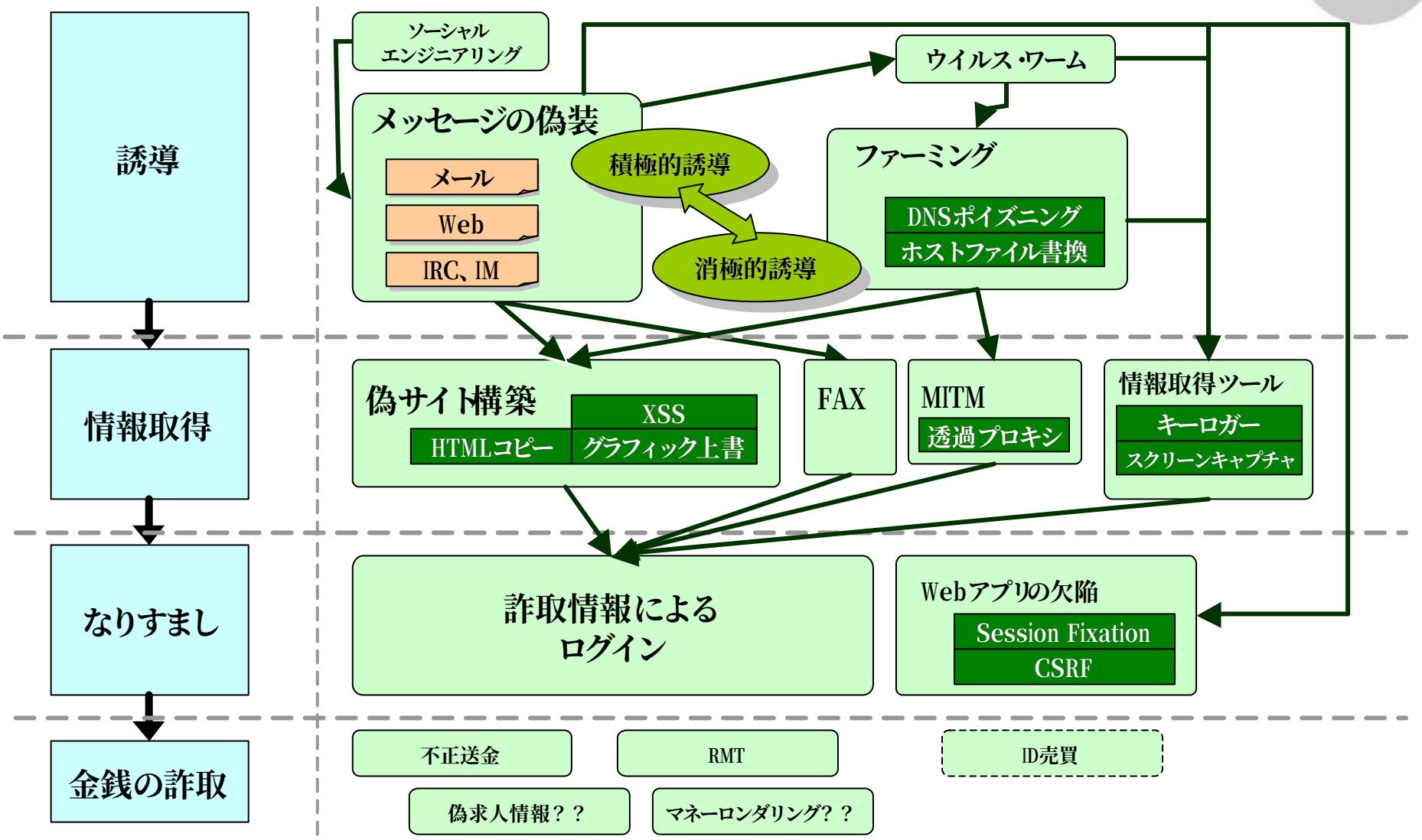
金銭の詐取

金銭的な利益を不正に得る。
例）不正送金、RMT（Real Money Trading）



フィッシング詐欺の全体像

Intelligent Systems Laboratory



セコムIS研究所
Intelligent Systems Laboratory

利用される技術

利用技術の拡大

○典型的な例
【誘導】メールの文面の偽装＋URLの見た目を偽装
【情報取得】HTMLコピーによる偽サイト

いまだ支配的ではある

発展

- グラフィック上書き
- ファーミング
- IMの利用

洗練

- ログインリダイレクト
- キーロガーの利用

典型的な技術

利用技術	*技術詳細*
ソーシャルエンジニアリング	文面の偽装
偽サイト構築	HTMLのコピー
	隠しフレーム
	グラフィック上書き
	右クリック偽装
メッセージの偽装	見た目の偽装
	サーバ側ソフトの脆弱性
	クライアント側ソフトの脆弱性
	グラフィックの上書き

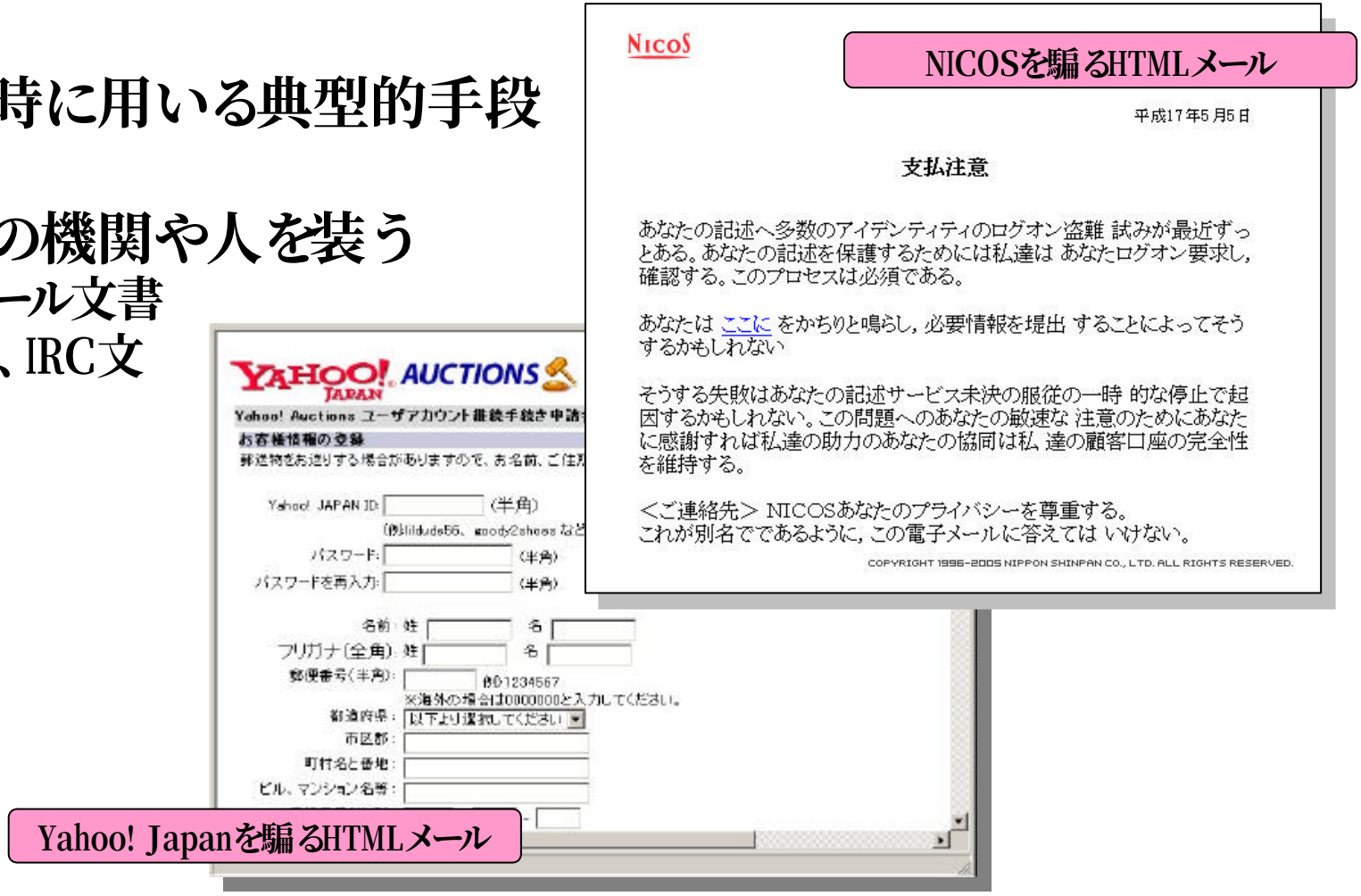
発展・洗練された技術

利用技術	*技術詳細*
ファーミング	DNSポイズニング
	ホストファイルの書換
	プロキシ情報の書換
情報取得ツール	キーロガー
	スクリーンキャプチャ
MITM（中間者攻撃）	透過プロキシ
	ログインリダイレクト
Webアプリの欠陥	XSS
	CSRF
	Session Fixation

利用技術：ソーシャルエンジニアリング

セコムIS研究所 Intelligent Systems Laboratory

- 誘導時に用いる典型的手段
- 正規の機関や人を装う
  - メール文書
  - IM、IRC文



利用技術：メッセージの偽装

セコムIS研究所 Intelligent Systems Laboratory

見た目の偽装：URL

典型的、で一番多い

- URLの表示と実際のリンク先
- ドメインの取得
  - ー まぎらわしいドメイン
  - ー 打ち間違えを意識したドメイン
  - ー IDN（国際化名）ドメイン
- ドメインの表示
  - ー ID/パスワードが入ったURL
  - ー IPアドレスでのURL表記
  - ー エンコードを変える

サーバ側脆弱性を利用した偽装

MTAの脆弱性、設定ミス：From行の偽装

クライアント側脆弱性を利用した偽装

HTMLメールにおけるステータスバーのリンク先情報（OE、Eudora）

その他

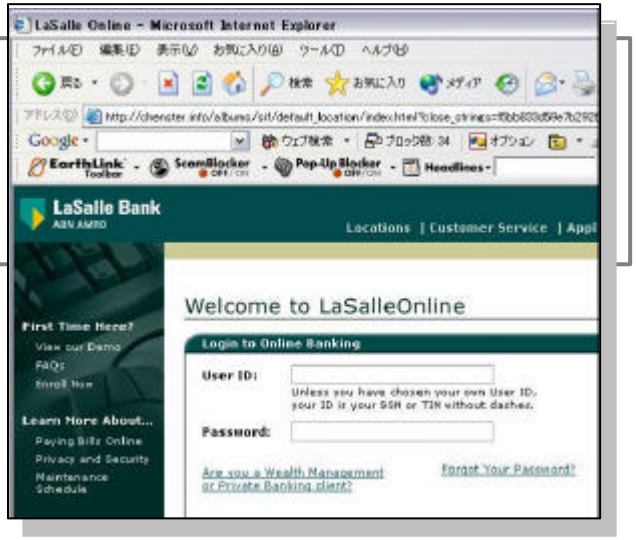
短縮化URLサービス：TinyURLなど

利用技術 :偽サイトの構築

セコムIS研究所
Intelligent Systems Laboratory

HTMLのコピー

- 正規サイトのHTMLをコピーして偽サイトで使う
  - 容易に同じ概観を作成可能
  - 画像は直接リンクまたはローカル保存で利用



見た目の偽装

- アドレスバー、鍵マーク、ゾーンに別のそれらしいグラフィックを上書き
  - JavaScript、VBScript、Javaなどを利用
- 右クリックの別実装
  - 「プロパティ」での偽装発覚を逃れたり
- ポップアップの偽装
  - 実際のブラウザ情報やWebアプリのように
- SSL証明書詳細やセキュリティセッティング偽造

入力情報の確認

- 正規サイトへログイン情報を送信、確認
- クレジットカード番号の内容チェック
  - 最初の数桁 :カード会社
  - 最後の4桁 :チェックディジット

隠しフレーム

フレームにより正規サイトと偽装サイトを表示。偽装サイト非表示、正規サイト非表示の双方で利用される

利用技術 :ファーミング

セコムIS研究所 Intelligent Systems Laboratory

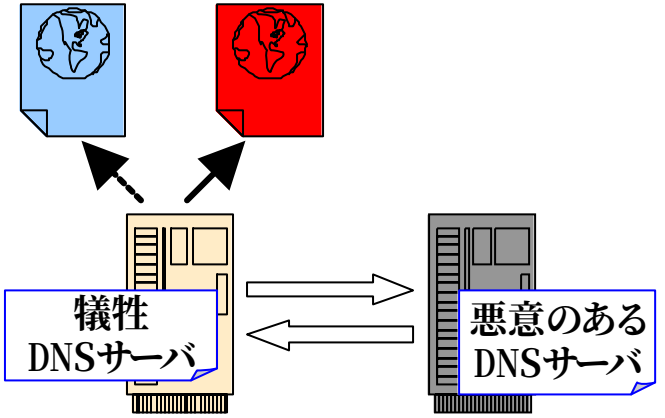
ファーミングとは

正しいURL接続を偽サイトにつなげること。DNSのキャッシュを悪用したり、PCやサーバが保持するホスト情報を改ざんすることで実現する

DNSキャッシュポイズニング

- 甘い設定を持つDNSを突き、DNSサーバのキャッシュ情報を改ざんする
  - 悪意のあるDNSサーバへクエリを発行させる
  - 悪意のあるDNSサーバはクエリを返すと同時に、関係ない回答も行う
  - 「関係ない回答」を甘い設定のDNSが受け取ることで汚染される

→ 実際の事例を後述



hostsファイルの書換

PCやサーバがローカルに保持しているホスト情報ファイルを改ざんする

プロキシ悪用

他のキャッシュ汚染

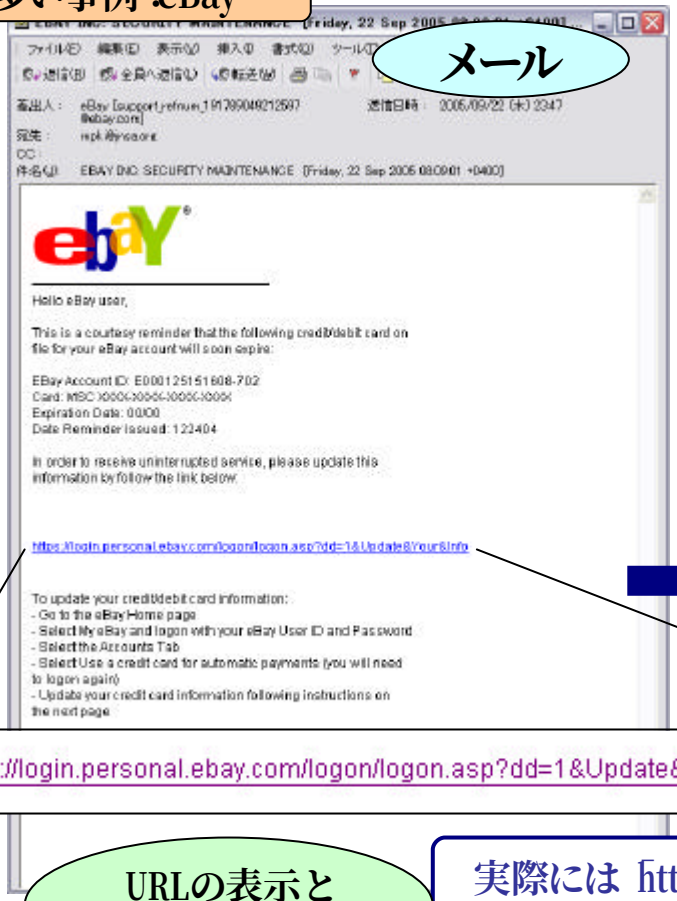
ウイルス・ワーム感染

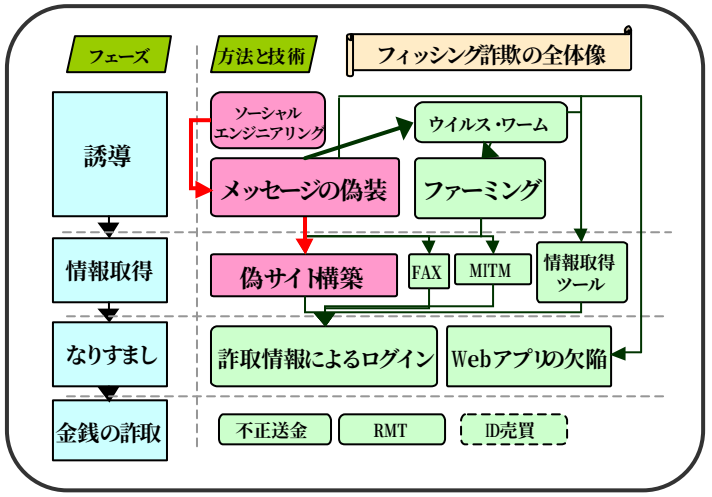
フィッシング事例 :eBay

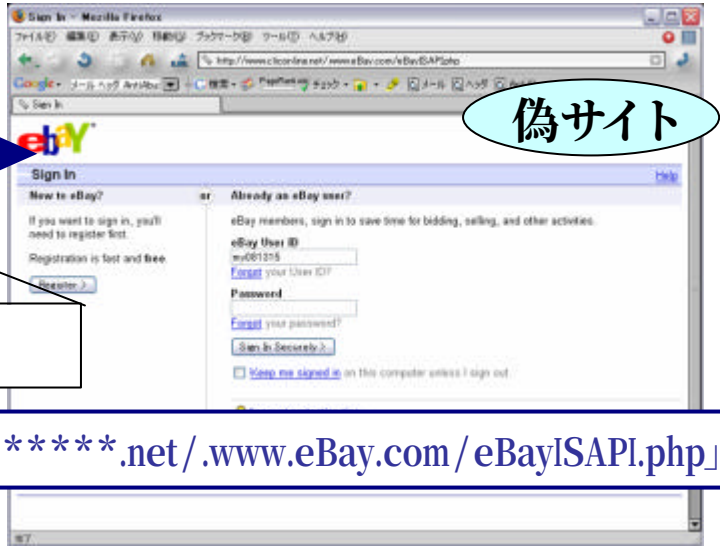
セコムIS研究所
Intelligent Systems Laboratory

一番多い事例 :eBay

メール







偽サイト

https://login.personal.ebay.com/logon/logon.asp?dd=1&Update&Your&Info

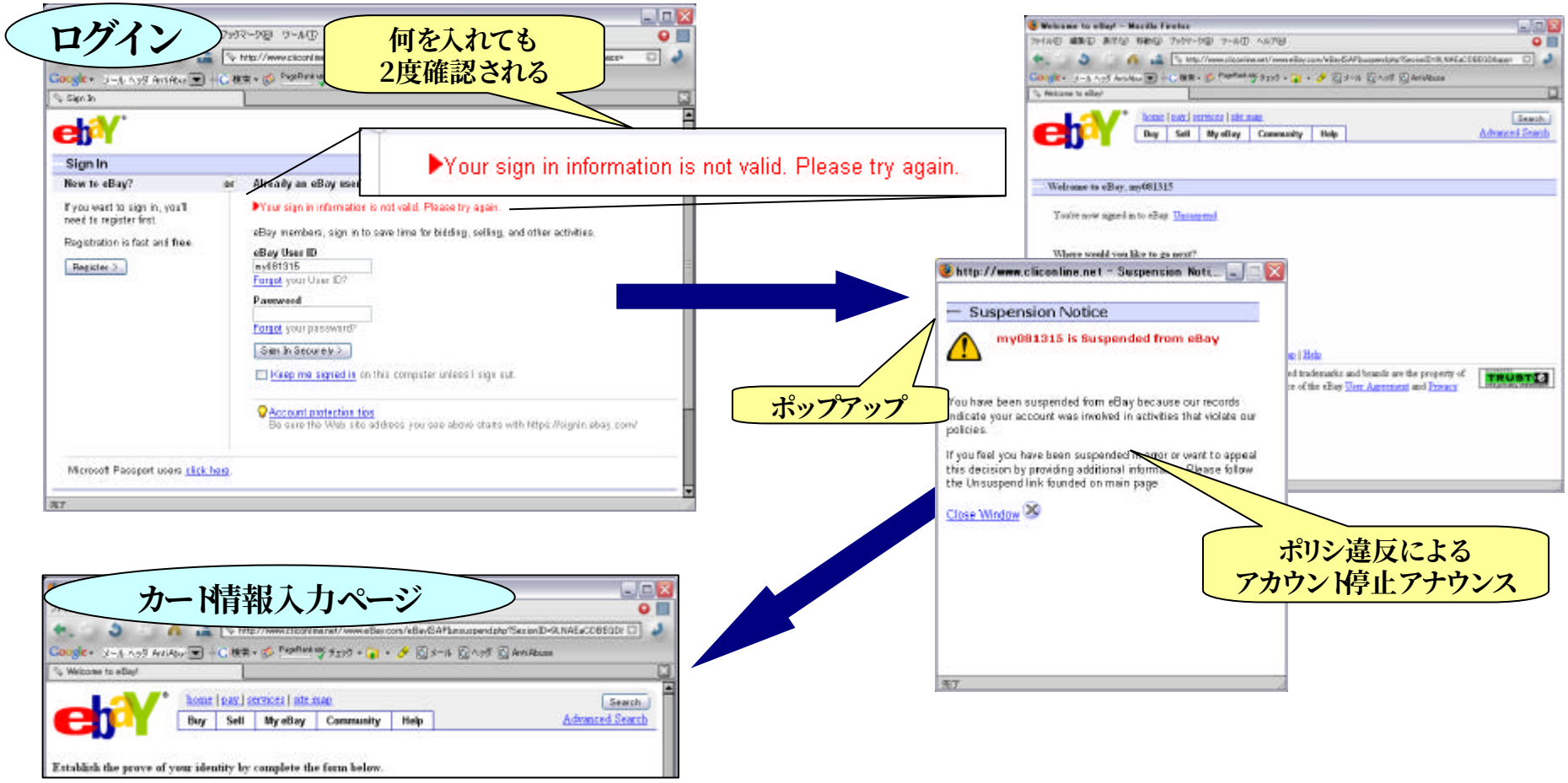
URLの表示と
実際のリンク先

実際には「http://www.******.net/.www.eBay.com/eBayISAPI.php」

フィッシング事例：一般事例

セコムIS研究所
Intelligent Systems Laboratory

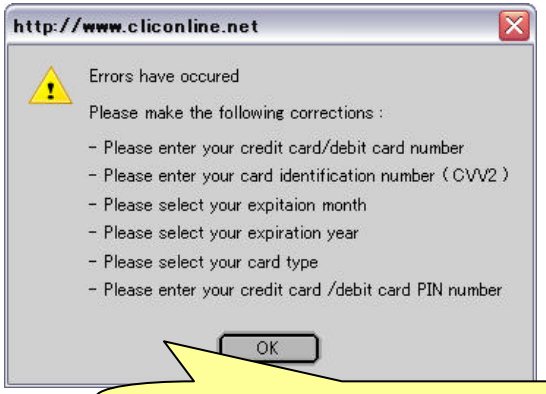
一番多い事例：eBay



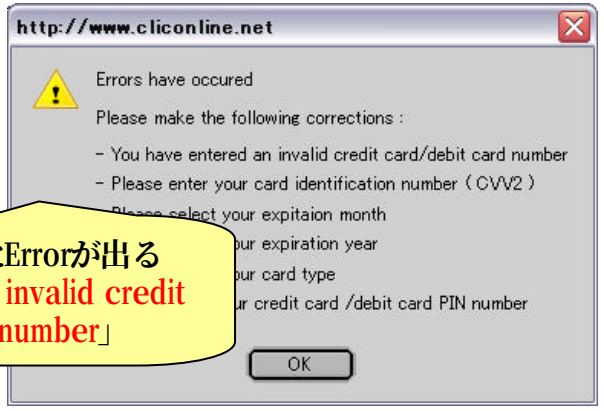
フィッシング事例：一般事例

セコムIS研究所 Intelligent Systems Laboratory

一番多い事例：eBay



空欄でSubmitすると
カード情報の部分でErrorが出る



適当なカード番号だとErrorが出る
「You have entered an invalid credit card/debit card number」

適切な（？）カード番号が入力されると、
正規のeBayサイトへリダイレクトされる

国内フィッシング事例 :YAFOO!

セコムIS研究所 Intelligent Systems Laboratory

日本初の摘発・有罪

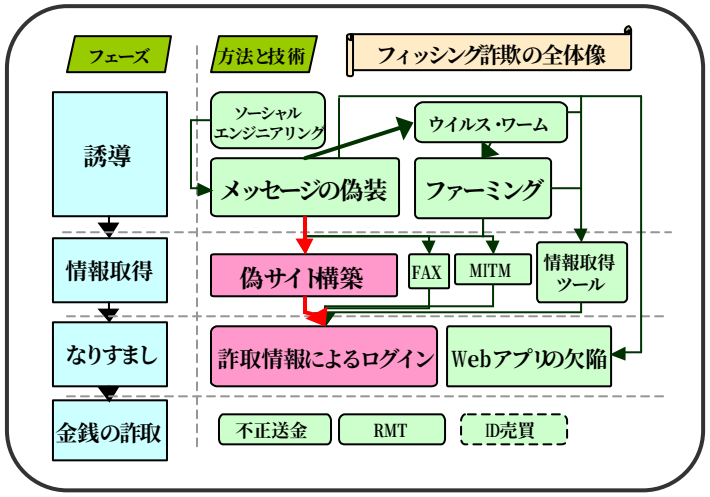
・2005年2月
「Yahoo! JAPAN」に似せたWebサイトが開設される

本物と間違えてアクセスしたユーザの
ID/パスワードを窃取。
窃取したID/パスワードでログイン、
メールを見るなどする

ヤフーは著作権法違反で
被害届を提出

・2005年6月
著作権法違反と不正アクセス禁止法違反の疑いで
開設者を逮捕

・2005年9月
有罪判決 :懲役1年10月、執行猶予4年
(求刑 :懲役2年)



インパクト

社会的なインパクト

法律
- 著作権法違反
- 不正アクセス禁止法違反

ニュース
- TVのニュース番組でも報道される

→ 技術的なインパクトは薄い

国内フィッシング事例：ネットバンキング

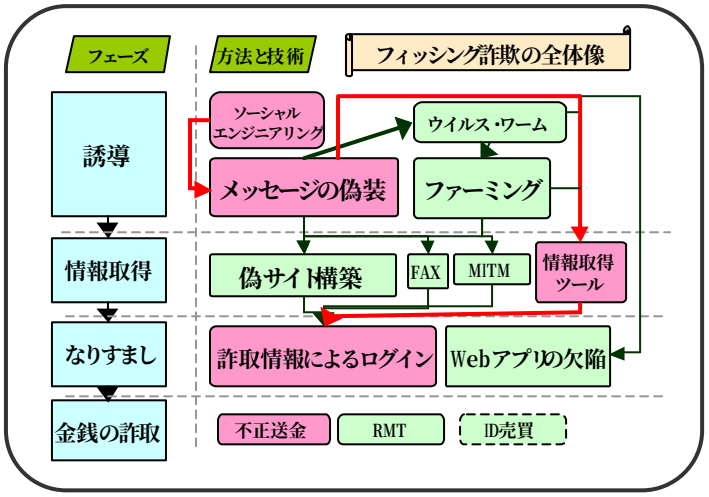
セコムIS研究所 Intelligent Systems Laboratory

スパイウェアによる不正送金被害

・2005年7月
　スパイウェアによる不正取引が発生
　　:イーバンク銀行、ジャパンネット銀行、みずほ銀行

ログインに必要な情報をスパイウェアで収集

3行で9件、合計約940万円の被害



実はフィッシング詐欺？

*あくまで記事と状況から推測したものです

通販顧客を装ったメール	苦情文面＋該当商品画像ファイルと見せかけたスパイウェア添付
↓	
スパイウェアのインストール	添付スパイウェアを実行、インストール
↓	
ログイン情報の窃取	キーロギングや、HTTP/HTTPS通信の盗聴　→　犯人へ送信
↓	
ログイン、不正送金	

ファーミング関連事例：DNSポイズニング

セコムIS研究所 Intelligent Systems Laboratory

米国SANSレポート

"March 2005 DNS Poisoning Summary"
http://isc.sans.org/presentations/dnspoisoning.php

2005年2-3月にわたり起こったDNSポイズニング事例のレポート

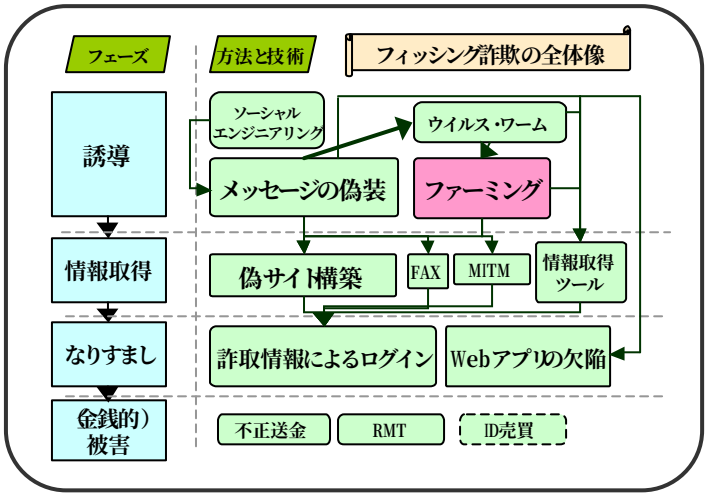
対象プラットフォーム

- Windows NT4/2000 DNSサーバ → 初期設定に問題があり、DNSキャッシュポイズニングが可能
- Symantecの特定製品 → 製品のバグにより、DNSキャッシュポイズニングが可能

2つのケース

- リダイレクト先にスパイウェア → 汚染DNSサーバ数 3
- リダイレクト先は処方薬販売サイト → 汚染DNSサーバ数 2

1304のドメインが汚染
800万弱のHTTPアクセス
その他：FTP・IMAPのログインなど



ファーミングの脅威

"Black Ops of TCP/IP 2005"
Dan Kaminsky @ BlackHat 2005

250万台のDNSサーバ

- 潜在的な脆弱性：23万台
- 確実に汚染可能：13000台

フィッシング対策 概要

セコムIS研究所 Intelligent Systems Laboratory

考え方

さまざまなプレイヤーがさまざまなフェーズ・レイヤで対処を考慮しなければならない

- xSP、（ターゲット）企業、一般ユーザ
- メール/Web
- 予防と事後対応

根絶する解は現状ではないと言っていい → 下地はできつつある

対策概要

現状の最適解（ベストプラクティス）を適用 → 短い期間での見直し

「対策編」へつづく