セコムIS研究所
Intelligent Systems Laboratory

フィッシング詐欺の対策

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

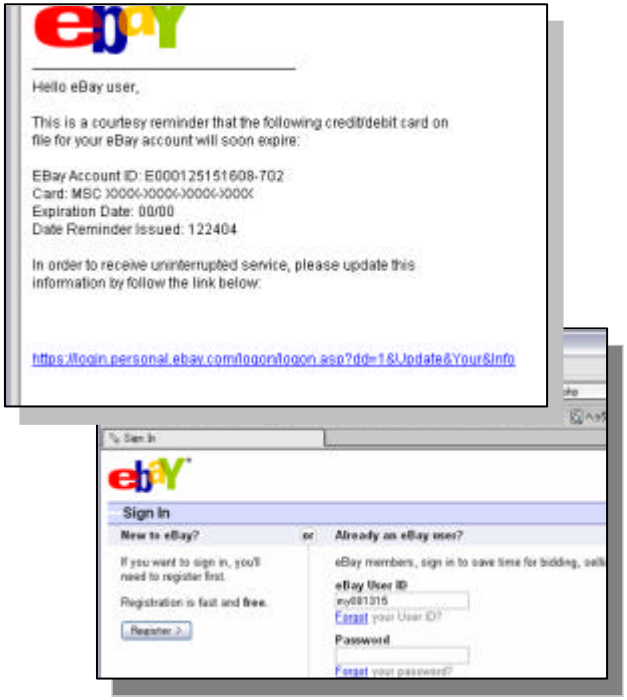
正規のサイトを偽装したり、不正に情報を詐取するツールを自動ダウンロード・インストールすることで情報を取得する。
例）金融機関のサイトを偽装し、アカウント情報を詐取する

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

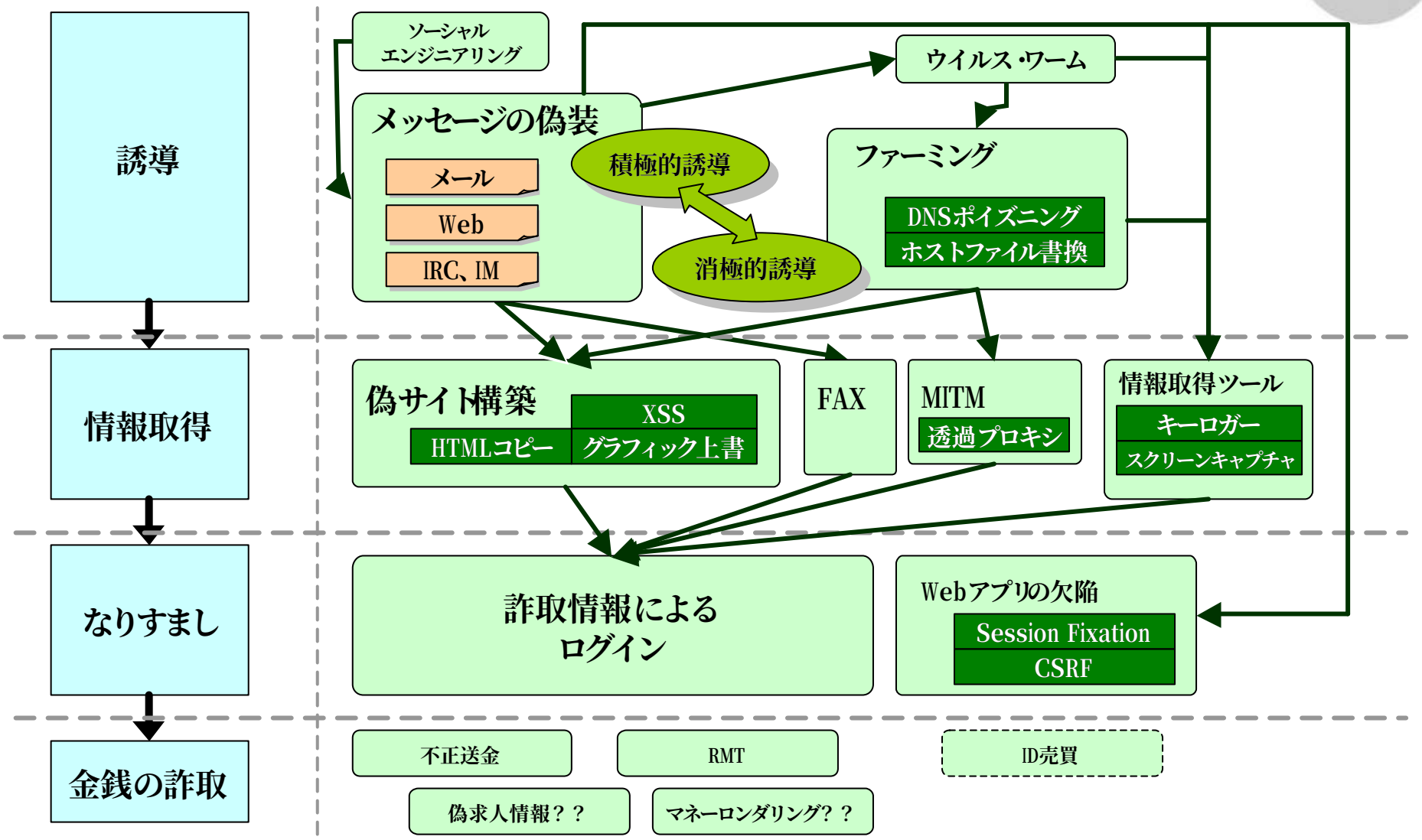
金銭の詐取

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



フィッシング詐欺対策 総論

セコムIS研究所 Intelligent Systems Laboratory

根絶手段は？

現状では、ない！

フィッシング詐欺は単一の問題により起こる事象ではなく、インターネットを中心として、さまざまな技術のや人間系の問題、組織体制など広範囲にわたるレイヤでの問題点が複合的にからみあったもの

「インターネットの信頼性」という根深い問題がある

→ 被害を極小化させる対策は存在する

対策の方向性

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する必要性

プレイヤー	技術の浸透度	予防
フェーズ	知識の浸透度	事後対応
レイヤ	体制の敷設度	

→ 現状で最適となる対策を選択

→ 短期間で見直す

プレイヤーごとの対策 :全体像

セコムIS研究所 Intelligent Systems Laboratory

	一般ユーザ		xSP	サービス提供エンド
	一般ユーザ	エンドユーザのシステム管理者	ネットワークオペレータ	Webアプリ開発者
予防	• 利用PCの安全性確保 — OS/ブラウザバージョン更新 — ウイルス対策ソフト導入 — パーソナルファイアウォール導入 • メール内容の確認 • フィッシング専用ツール利用 ・・・(a) • サービス提供組織独自ツール利用 ・・(a) • フィルタリングソフト/サービス利用 • フィッシング対応ブラウザ利用 ・・・(b) • 送信ドメイン認証対応メーラ利用 ・・(b)		• 管理サーバ/機器の脆弱性除去 • 提供サービスの定期検査 • 送信ドメイン認証対応 • 25番ポート送信ブロッキング • メールフィルタリングサービス • 登録業務の厳格化 ・・・(b)	• 管理サーバ/機器/Webアプリの脆弱性除去 • 適切なWebサイト表示 • Webサーバ証明書の適切な導入・利用 • サービス価値とバランスの取れたWebアプリ認証 • 顧客とのメッセージング方法の決定・周知・遵守 • 送信ドメイン認証対応 • 利用ドメインの統一 • ドメイン監視サービス利用
事後対応	• 「フィッシング110番」への連絡		• 窓口の設置、連絡体制の確立 • Bot化顧客対応 :報告、遮断	• 自社内での対応スキーム • 他者からの報告窓口の設置・周知

a) 一時的な利用を前提にするべき
b) 少し先の話

xSPが行なうべき対策