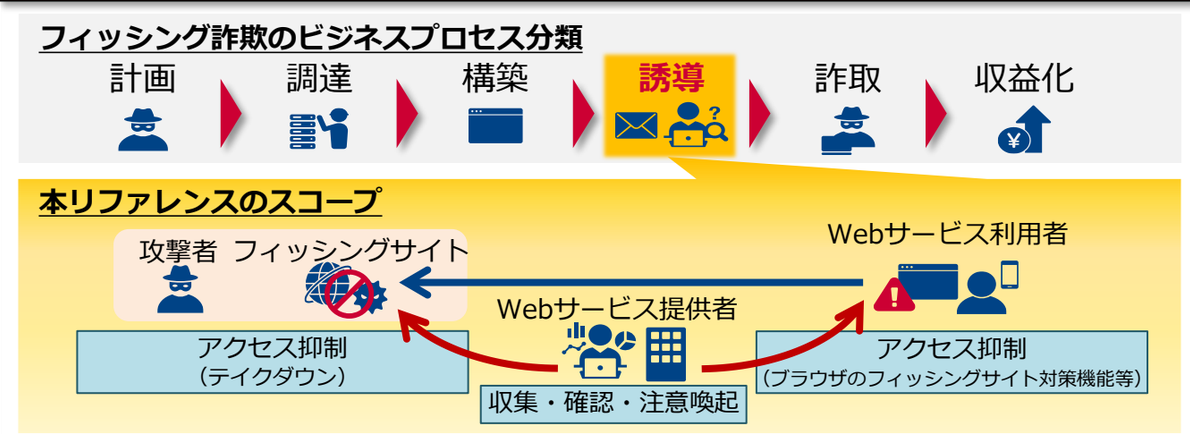
Webサービス提供者のためのフィッシング対応実務リファレンス（概要）

昨今のフィッシングに関連する被害の増加を受け、フィッシングメール/SMSのばら撒き後に利用者を守るような対策をWebサービス提供者が早期に講じるための参考情報（手順、留意点 等）をまとめたリファレンスである。

本リファレンスの想定読者、スコープ等

想定読者	フィッシングで騙られる企業や組織のCSIRT/SOCの担当者 （基礎的なネットワークやセキュリティの知識を前提とする）
スコープ	「フィッシング詐欺のビジネスプロセス分類」※の「誘導」段階におけるフィッシングメール/SMSのばら撒き後のフィッシング対策 （フィッシングサイトの収集、確認、アクセス抑制、注意喚起）
特徴	• 実用性を重視し、具体的なツール名や事例を交えて説明 • 初心者向けの基本的な対策に加え、既存で対策を講じるWebサービス提供者向けに高度な事例や手法まで紹介

「フィッシング詐欺のビジネスプロセス分類」と本リファレンスのスコープ



※：「フィッシング詐欺のビジネスプロセス分類」（https://www.antiphishing.jp/news/collabo_20210316.pdf）

本リファレンスの内容

章タイトル	記載内容（概要）
1. はじめに	フィッシング**対策が求められる背景**やリファレンスを読む際の**前提となる情報**（ターゲット、スコープ、注意事項 等）に加え、被害を抑制するためには3～6章で紹介する一連の対策（収集、確認、アクセス抑制、注意喚起）が必要である旨を説明する。
2. フィッシング攻撃の実態	適切な対策を検討する上で把握すべきフィッシング攻撃の実態について、昨今のフィッシングサイトに見られる**特徴的な事例や攻撃手法（クローキング 等）**、**Webサービス利用者のアクセス実態**の事例を紹介する。
3. 自社を騙るフィッシングサイト情報の収集	自社を騙るフィッシングサイト情報を収集する手法として、**SNS**や**サポートセンターの問い合わせ情報**、**インテリジェンスサービス**の活用などを**難易度順に**紹介する。正規サイトやサーバー証明書に関するログなどを活用した**高度な手法**も紹介する。
4. 自社を騙るフィッシングサイトの状態確認	収集したフィッシングサイトの稼働状況を確認するために、**ツールを活用する簡易な方法**から、**検証端末（PC／モバイル）を活用する方法**に加え、運用の留意点及び**クローキングを回避**する観点での推奨事項も紹介する。
5. 自社を騙るフィッシングサイトへのアクセス抑制	稼働確認したフィッシングサイトへのアクセスを抑制するために、**ブラウザのフィッシングサイト対策機能**（Google Safe Browsing 等）への報告や**テイクダウン**依頼の**具体的な手順や留意事項**、自動化を実現するための**APIを活用した高度な手法**を紹介する。
6. Webサービス利用者への注意喚起・啓発	被害発生を早急に周知し注意を促す観点で、3～5章の対策（収集、確認、アクセス抑制）に加えてWebサービス利用者に向けた**効果的な注意喚起のポイント**を紹介する。実際に公開された**注意喚起文の優良事例**を具体例として複数紹介する。
7. より効果的な対策に向けて	3～6章の対策をより効果的なものとする観点で、有償サービスの活用を含む**体制準備のポイント**を説明する。被害最小化の観点から、「誘導」段階に留まらない対策の参考情報や、想定読者へのメッセージとして**組織を超えた情報連携**の必要性なども説明する。
8. Appendix	参考情報として、クローキングの実例、テイクダウン依頼における依頼先事業者ごとの対応状況をまとめた「テイクダウン実施コスト効率一覧表」、本リファレンスの特に重要な要素を抜粋した資料などを掲載する。