Google Cloud

フィッシング詐欺から企業ブランドを守る

～VirusTotal と Web Risk API を使ったテイクダウンの方法を解説～

髙橋 悟史、ペイン ディヴィッド

Google Cloud
セキュリティ スペシャリスト

本日お話する内容

お話する内容

企業のブランドイメージに損害を与える フィッシングサイトの発見方法と、
セーフブラウジングによるアクセス停止方法

お話しない内容

従業員や、ユーザーがフィッシングサイトにアクセスすることを防ぐ方法

フィッシングの概要と
企業ブランドへの影響

フィッシング被害が増加

フィッシングとは
偽りのウェブサイトにユーザーを**誘導して**、**ID 情報**を盗んだり、**マルウェア**に感染させる手法

2021 年 はフィッシングの被害、ブランドの**悪用が増加**※1

誘導用のサイトや、誘導するためのメッセージが本物と見分けがつかない高度なものが増えており、被害が増えている

※1 フィッシング対策協議会のデータより

サイバー攻撃の最初のステップ

サイバー攻撃の

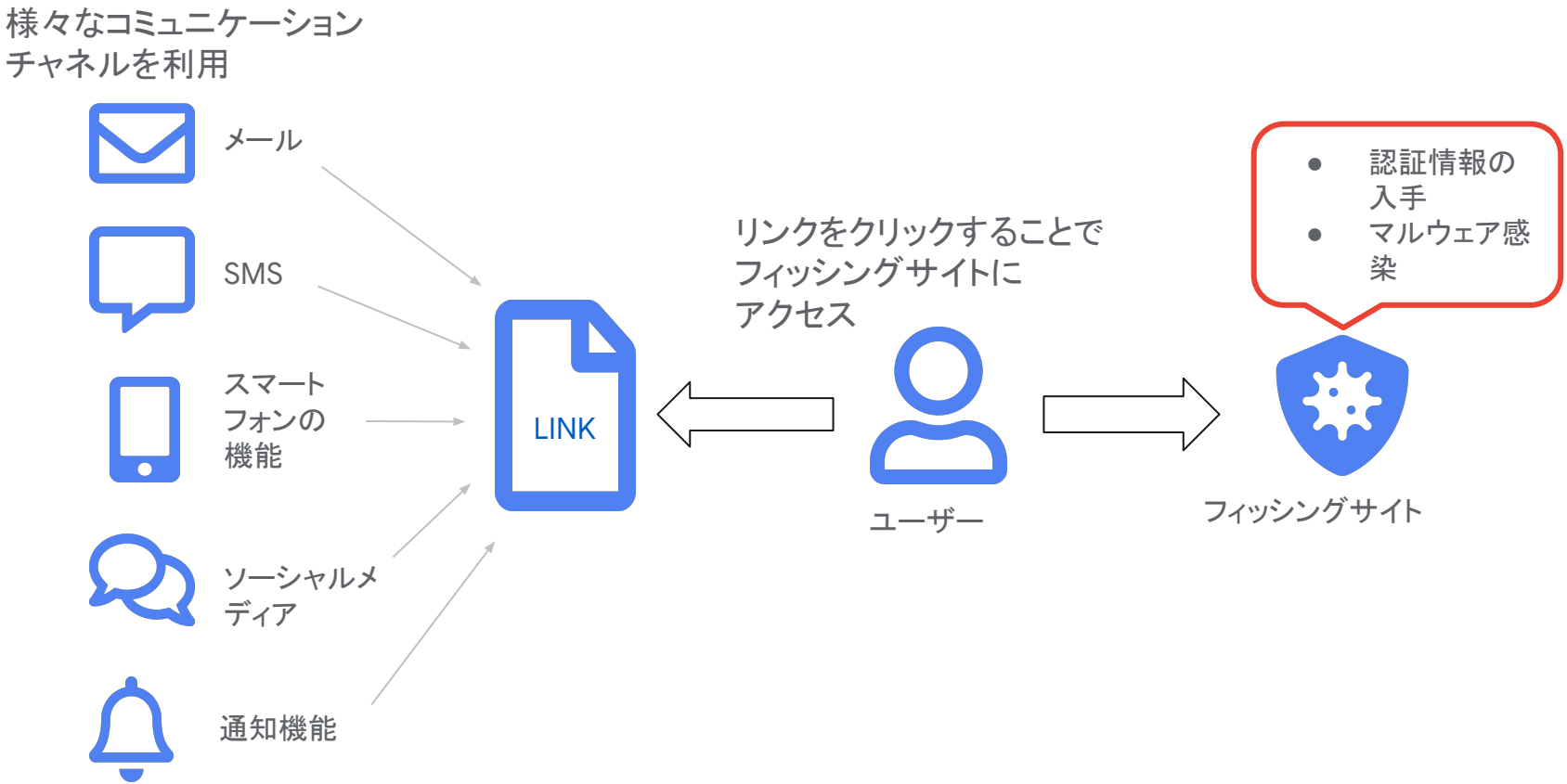
91% は

フィッシングメールから始まる[1]

ターゲッティングされた攻撃は検知するのが難しい

Source: Enterprise Phishing Susceptibility and Resiliency Report, Cofense

フィッシングサイトへの誘導



スピア型 フィッシング

高橋 悟史様、

RSA カンファレンスへのご参加ありがとうございます。
ご参加の記念品として、T シャツをお送りしています。添付のフォームに記入してお送りください。

RSA カンファレンス事務局

お客様各位、

システムを入れ替えるために、パスワードの変更を皆様にお願いしています。
リンク先のサイトからパスワードの変更をお願いします。

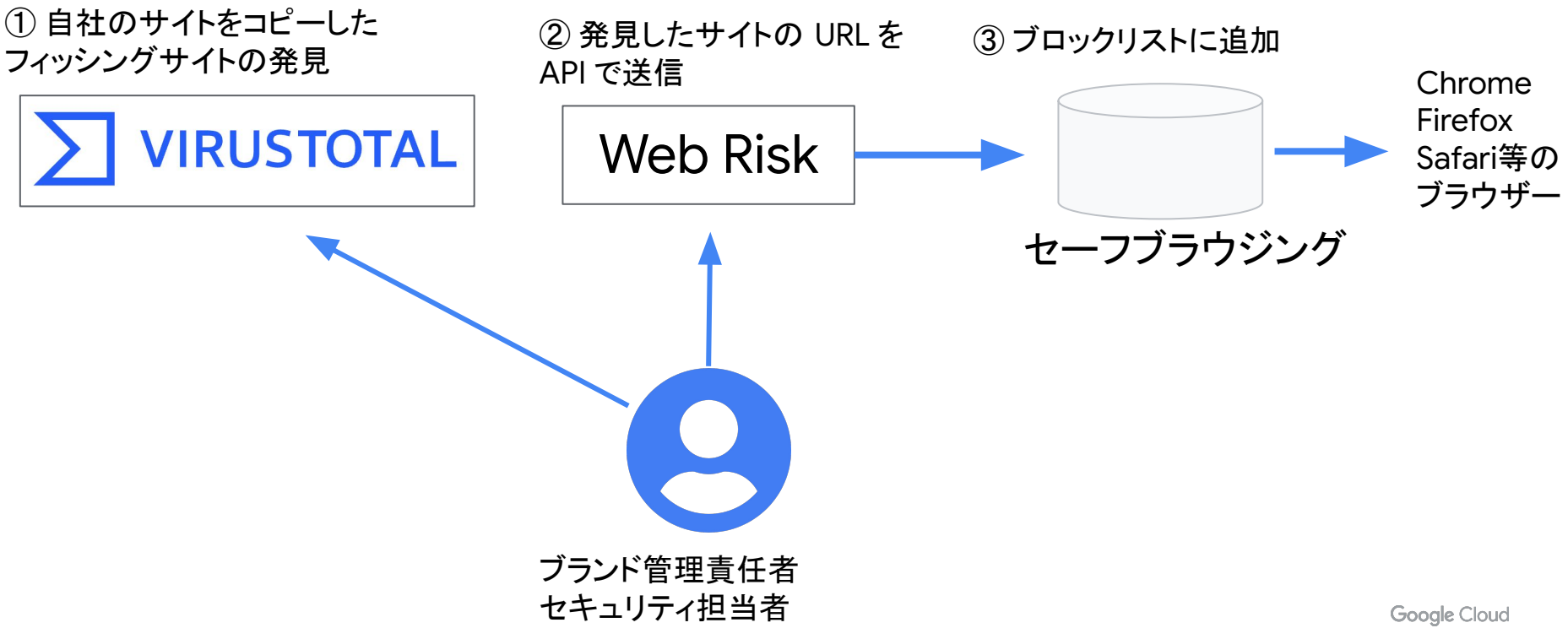
よろしくお願いします
EC サイト ABC

フィッシングサイトの例

- サイトのコンテンツは簡単にコピー出来る
- 見分わけるのが困難なサイトの作成が可能

VirusTotal と Web Risk による フィッシングサイトの発見と セーフブラウジングの 拒否リストへの追加

ソリューションの全体像



世界最大の
クラウドソース
脅威インテリジェンス

30 億以上
ファイル
圧縮ファイルを含めて500億

10 億以上
分析報告
サンドボックス

200 万
ファイル分析
（毎日）

232 カ国
グローバル

200 万
ユーザー
月間平均

50 億以上
URLs
1 日あたり 6 百万 URL 分析

30 億以上
ドメイン

50 億以上
pDNS

70+ アンチウイルス

70+ URL データベース

15+ サンドボックス

20+ ルール
(YARA, SIGMA, IDS)

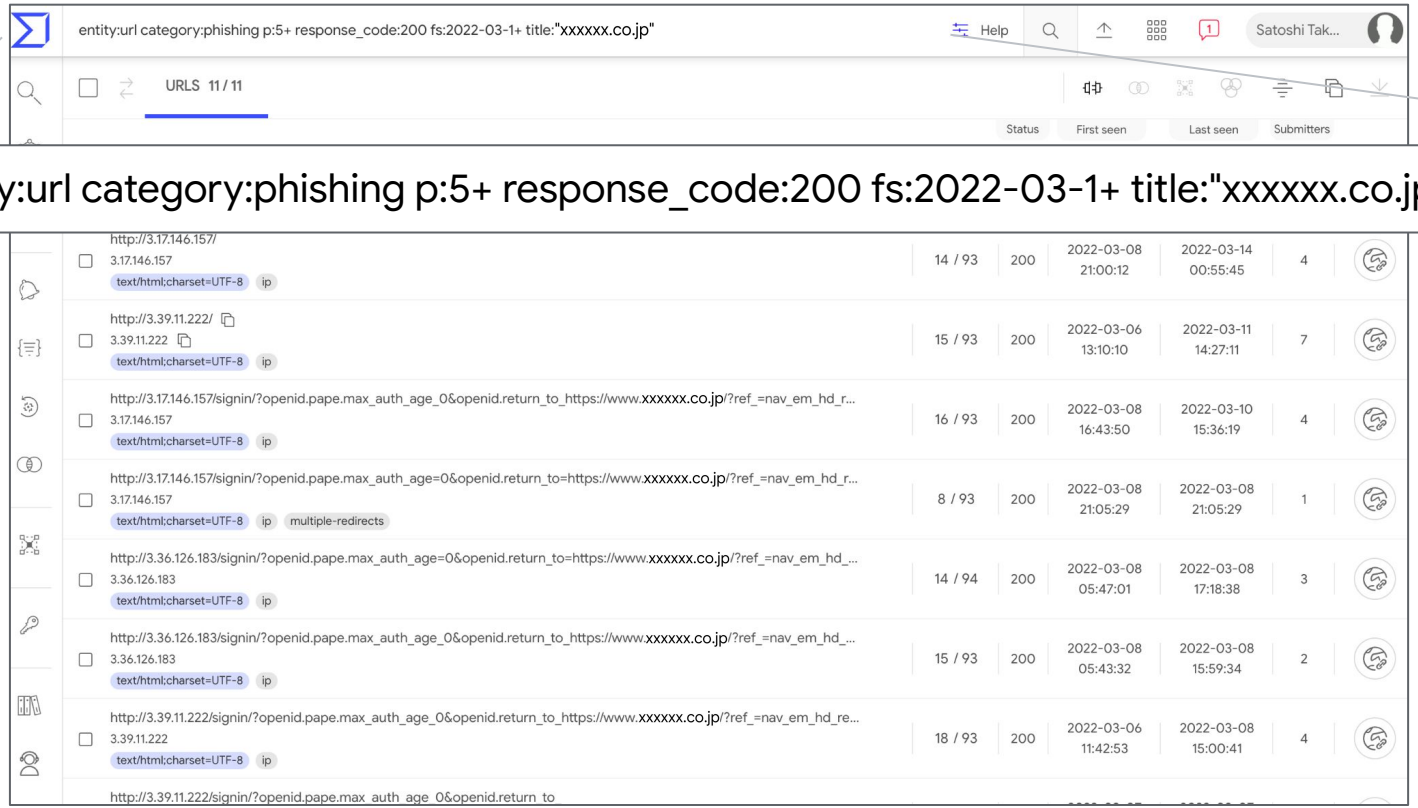
VirusTotal

パブリックサービス

ファイルをアップロードして、70 以上もの
アンチウィルスソリューションから
セカンドオピニオンを得ることが出来る

www.virustotal.com

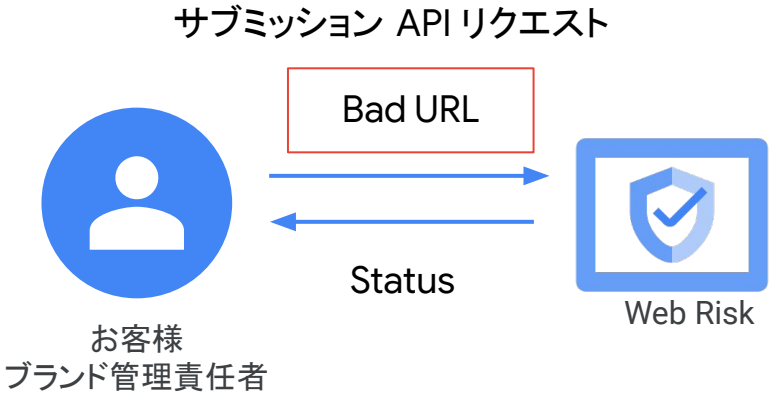
VirusTotal はファイル、URL、IP アドレス、ドメイン名などの条件で マルウェアや悪性サイトを見つけて分析するためのツール



entity:url category:phishing p:5+ response_code:200 fs:2022-03-1+ title:"xxxxxx.co.jp"

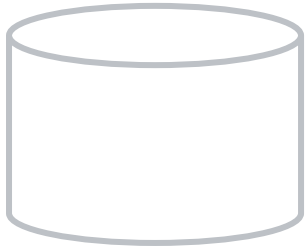
発見したフィッシングサイトのセーフブラウジングの拒否リストへの追加：Web Risk

- 4 種類の API
- サブミッション API は お客様管理者が URL 情報を送信して、セーフブラウジングの拒否リストの更新を依頼する



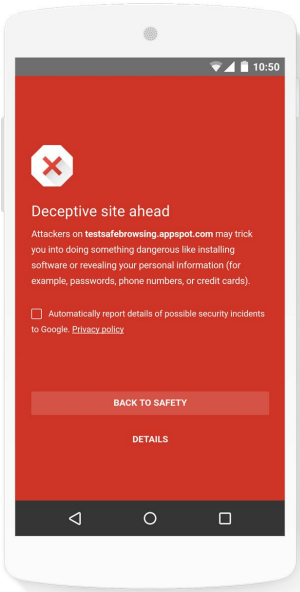
参照: https://cloud.google.com/web-risk/docs/quickstart

Google セーフブラウジング



safebrowsing.google.com

このサイトは安全か？



40 億台以上のデバイスを保護

Google Chrome
Firefox
Safari 等

[Google Safe Browsing]

Thank you.

Google Cloud