JPAAWG 2026 / LIGHTNING TALK

OSSを用いた
標的型攻撃メール訓練基盤の内製化

今回お話しすること

- OSSの選定
- 送信方法の選定
- インフラの選定
- ？
- 安全に利用するための工夫

01 / TOOL SELECTION

標的型攻撃メール訓練向けOSSを比較

要件：CSVでメールアドレス・氏名・部署を取り込み、差し込みとクリック記録を行う。

	FIRST CHOICE Gophish v0.12.1 / 2022	AIが提案 →	SELECTED Phishing Club v1.44.0 / 2026
基本要件	CSV・差し込み・クリック記録		CSV・差し込み・クリック記録
部署	専用項目なし Position （役職）を代用		Department を標準装備
更新状況	最新公開版は2022年 既知脆弱性の修正版は未公開		2026年も 新しいバージョンを公開

必要な機能 ＋ 現在も更新が続いていること で選択。

出典：Gophish v0.12.1 ／ CVE-2024-55196 ／ CVE-2026-39904 ／ Phishing Club v1.44.0

02 / DELIVERY SERVICE

配信サービスが王道。それでも使わなかった

Amazon SES | **SendGrid** | **Mailgun**

利用条件

模擬フィッシングは審査・制限の対象になり得る。SendGridはセキュリティテスト用途を禁止。

標準は共有IPアドレス

他の利用者も同じIPアドレスを使用。GWSのメール許可リストには不適。

料金目安（USD・2026年11月確認）

	Amazon SES	SendGrid	Mailgun
無料枠	$200クレジット 新規AWS・6か月 SESにも利用可	100通／日 60日間の無料トライアル	100通／日 Freeプラン
1通換算	$0.0001 従量課金	約$0.0004 Essentials 50kを満額利用	$0.0015 Basic 10kを満額利用
固定IPアドレス	$24.95／IP 月額＋送信料	$89.95〜 Pro・月額／1個含む	$90〜 Scale・月額／1個含む

送信元と誘導先サイトを、固定IPアドレス付きクラウドVMに集約。

出典：SES FAQ・料金 ／ SendGrid Policy・料金 ／ Mailgun料金

03 / CLOUD PLATFORM

どちらもTCP/25を制限。違いは解除までの手順

当初案：固定IPアドレス付きクラウドVMから、GWSの受信MXへ直接配送。



Google Cloud

Compute Engine

外向きTCP/25を
標準で制限

一部は低リスク判定で自動解除
利用者向け申請手順は明示なし

AWS

Amazon EC2

外向きTCP/25を
標準で制限

解除申請フォームと
手順が明示

解除までの手順が見えるため、AWSを選択。

出典：Google Cloud：SMTP（port 25）traffic ／ AWS：Remove the restriction on port 25　※ Azureも選択肢でしたが、選定時には失念していました。

TCP/25制限の解除だけでは終わらなかった

用途に「社内向けのメール訓練」と書いて申請した。

01 TCP/25制限解除を申請

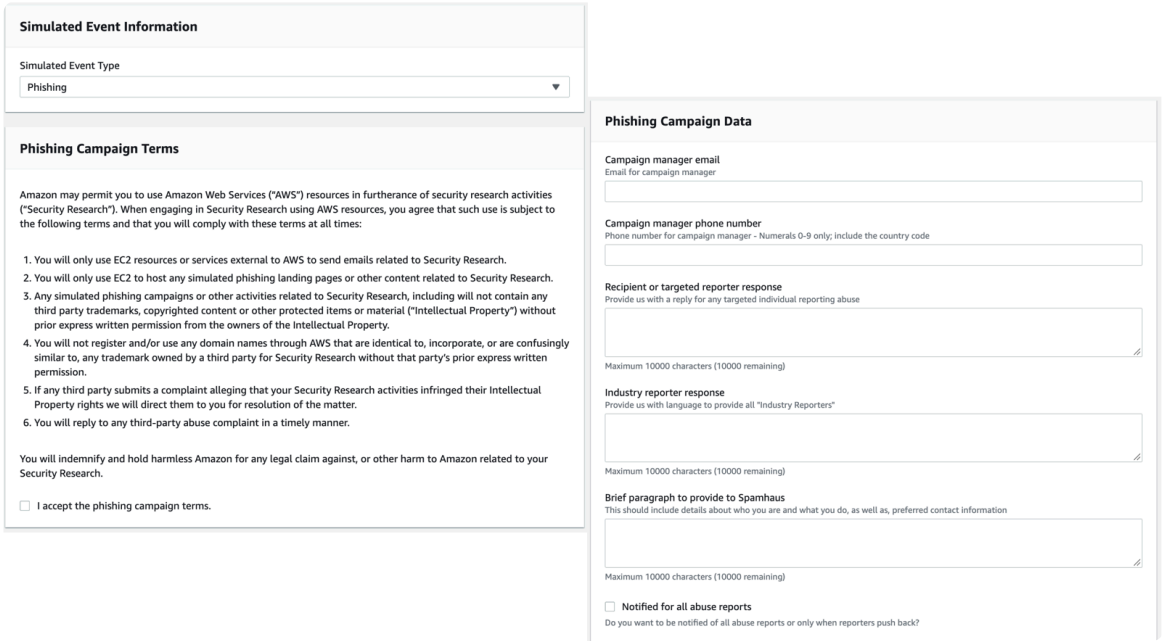
用途・送信量・迷惑メール対策を記載

02 別の事前承認へ

`Simulated Event Type` で `Phishing` を選択

03 入力・提出・承認待ち

長い記述欄＋緊急連絡先2名。承認後にTCP/25制限解除を再審査



Simulated Event Information

Simulated Event Type

Phishing

Phishing Campaign Terms

Amazon may permit you to use Amazon Web Services ("AWS") resources in furtherance of security research activities ("Security Research"). When engaging in Security Research using AWS resources, you agree that such use is subject to the following terms and that you will comply with these terms at all times:

1. You will only use EC2 resources or services external to AWS to send emails related to Security Research.
2. You will only use EC2 to host any simulated phishing landing pages or other content related to Security Research.
3. Any simulated phishing campaigns or other activities related to Security Research, including will not contain any third party trademarks, copyrighted content or other protected items or material ("Intellectual Property") without prior express written permission from the owners of the Intellectual Property.
4. You will not register and/or use any domain names through AWS that are identical to, incorporate, or are confusingly similar to, any trademark owned by a third party for Security Research without that party's prior express written permission.
5. If any third party submits a complaint alleging that your Security Research activities infringed their Intellectual Property rights we will direct them to you for resolution of the matter.
6. You will reply to any third-party abuse complaint in a timely manner.

You will indemnify and hold harmless Amazon for any legal claim against, or other harm to Amazon related to your Security Research.

☐ I accept the phishing campaign terms.

Phishing Campaign Data

Campaign manager email
Email for campaign manager

Campaign manager phone number
Phone number for campaign manager - Numerals 0-9 only; include the country code

Recipient or targeted reporter response
Provide us with a reply for any targeted individual reporting abuse

Maximum 10000 characters (10000 remaining)

Industry reporter response
Provide us with language to provide all "Industry Reporters"

Maximum 10000 characters (10000 remaining)

Brief paragraph to provide to Spamhaus
This should include details about who you are and what you do, as well as, preferred contact information

Maximum 10000 characters (10000 remaining)

☐ Notified for all abuse reports
Do you want to be notified of all abuse reports or only when reporters push back?

書かなければならないことが多く、大変でした。

出典：AWS Simulated Events policy　※ フォーム提出・自動返信受領済み。自動返信は承認ではない。

05 / OPERATIONS

TCP/25制限の解除を待たず、送信経路を切り替えた

実際の送信経路



GWSのメール許可リスト：ISPの固定グローバルIPアドレス

SMTPリレーは、EC2のElastic IPアドレスからのみ受付。

今回使用した送信経路。GWSのIP許可リストはトップレベル組織全体へ適用。

06 / DATA MINIMIZATION

送信後に、保持する属性を減らす

キャンペーンを開いたまま、計測に不要な氏名・部署を消せるか検証。

送信前

メールアドレス
＋ 氏名 ＋ 部署

全件送信後に氏名・部署を消去

→

計測中

メールアドレスを保持
氏名・部署は空

開封・クリックは同じ受信者へ記録できた ✓

送信済みメール、外部SMTP、既存バックアップ／エクスポートは別コピー。SQLiteの直接操作は行わない。

実機確認：Phishing Club v1.44.0の標準管理APIを使用。

07 / TAKEAWAYS

内製するなら、アプリの外側まで見る

01	選ぶ	必要な機能があり、現在も更新が続いているOSSを選ぶ。
02	確認する	ポート制限だけでなく、用途条件と申請期間を先に確認する。
03	減らす	送信後は、計測に不要な受信者属性を保持しない。

OSSを動かすだけでは、訓練基盤は完成しない。