Cloudflare Area 1とGoogle Cloud：

統合クラウドメールセキュリティと先制フィッシング対策

業界の課題：

マルウェアを使わないビジネスメール詐欺（BEC）やアカウント乗っ取り型詐欺、インサイダー（内部関係者）の脅威など、今日の高度なフィッシング攻撃は、従来のセキュアメールゲートウェイやメール認証では検知することが困難です。

ソリューション：

Cloudflare Area 1 メールセキュリティサービスは、先見的にウェブを巡回してフィッシングキャンペーンを発見し、その早期発見とメールのコンテキスト分析技術により、被害が発生する前に受信箱をフィッシング攻撃から保護します。

Area 1はGoogle Cloud Platform上に構築されており、わずか数分でデプロイでき、最高水準の徹底したフィッシング対策セキュリティレイヤーを提供します。

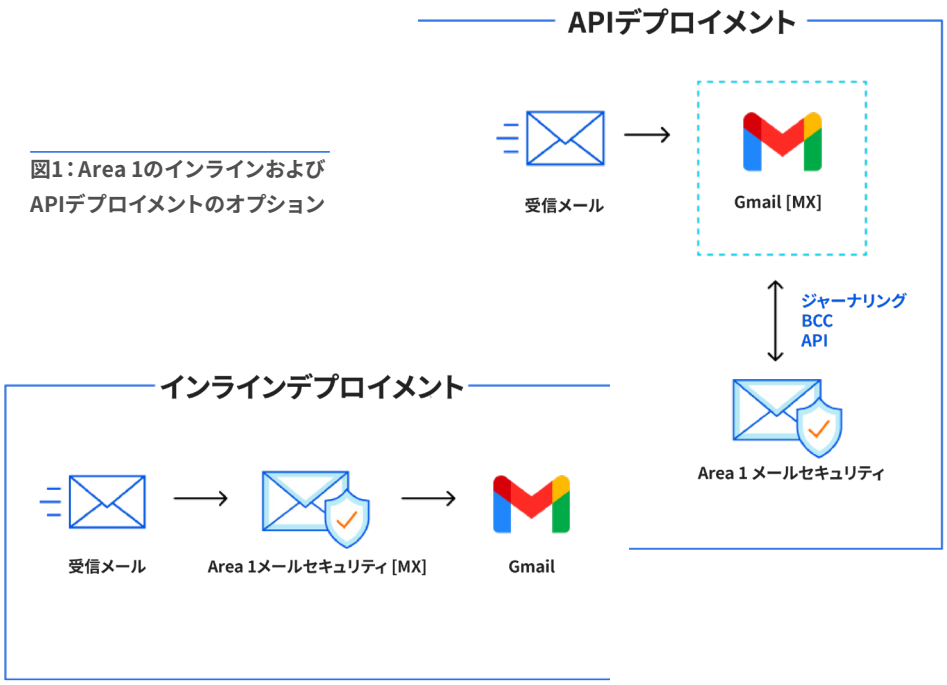

図1：Area 1のインラインおよびAPIデプロイメントのオプション

最もよく使われるクラウドアプリケーションであるメールを標的とした最新の攻撃から防御します。

フィッシング、BEC、メール詐欺などの高度な脅威を先制して阻止します。

Cloudflare Area 1とCloudflareリモートブラウザ分離の統合で、マルチチャンネルの脅威を分離・防止します。

SPF/DKIM/DMARCを回避するために攻撃者が使用する、侵害されたアカウントやドメイン、新規ドメイン、類似ドメイン、近接ドメインを発見することができます。

Cloudflare Area 1を選ぶ理由：

先制的なセキュリティ

攻撃サイクルの初期段階でフィッシングを止めるため、早期に攻撃者のインフラストラクチャと攻撃メカニズムを特定します。

包括的な保護

メール攻撃のあらゆるタイプ（URL、ペイロード、BEC）、ベクトル（メール、Web、ネットワーク、マルチチャンネル）、チャンネル（外部、内部、信頼できるパートナー）をカバーします。

コンテキスト分析

BEC、ベンダーメール詐欺、その他の高度な脅威を捕らえる先進的な検知テクニック（言語分析、コンピュータビジョン、ソーシャルグラフほか）を活用します。

継続的な保護

メールがユーザーの受信箱に到着する前、転送中、到着した後と、複数の脅威防御層で多層防御態勢をとります。

なぜCloudflare Area 1＋Google Cloudなのか：

- **運用効率の向上** — 従来のセキュアなメールゲートウェイを最新のクラウドファーストアーキテクチャに置き換えることで、複雑さを軽減します。
- **シームレスで柔軟な導入ー完全な柔軟性のあるArea 1サービスを5分以内に**デプロイし、アンチスパム、DLP、暗号化、アーカイブなど、Google Cloudのネイティブ機能とシームレスに統合します。
- **簡素化されたSaaSセキュリティ** ー 統合されたArea 1クラウドメールセキュリティに加え、Cloudflare Zero Trustプラットフォームは、クラウドアクセスセキュリティブローカー（CASB）機能をGoogleを提供しています。データ漏えいやコンプライアンス違反を容易に防止し、組織全体のデータ損失、フィッシング、ランサムウェア、シャドーIT、横移動などを阻止するワンストップショップを手に入れることができます。

ケーススタディ：S&P100の消費者向けパッケージ商品のリーダー企業は、クラウドメールの脅威からエグゼクティブとユーザーを保護

お客様の課題	Cloudflare Area 1を選んだ結果
• Google Workspaceと既存のセキュリティインフラをすり抜ける脅威 • シニアエグゼクティブや役員を狙ったBEC攻撃 • ITチームは、メールセキュリティのルールやブロックリストを常に調整するために、時間とリソースを費やしています	• 1年以内に800万件以上の標的型攻撃をブロックしました • ITチームは取締役会向けに、より優れたメールセキュリティの指標とレポートを提供できるようになりました • 生産性の向上とサイバーセキュリティリスクの大幅な低減を実現しました

Cloudflare Area 1によるGmailフィッシング対策の強化については、こちらからカスタムリスク評価をご依頼ください。