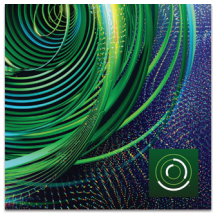
Adobe Marketing Cloudとセキュリティ



目次

アドビとセキュリティ

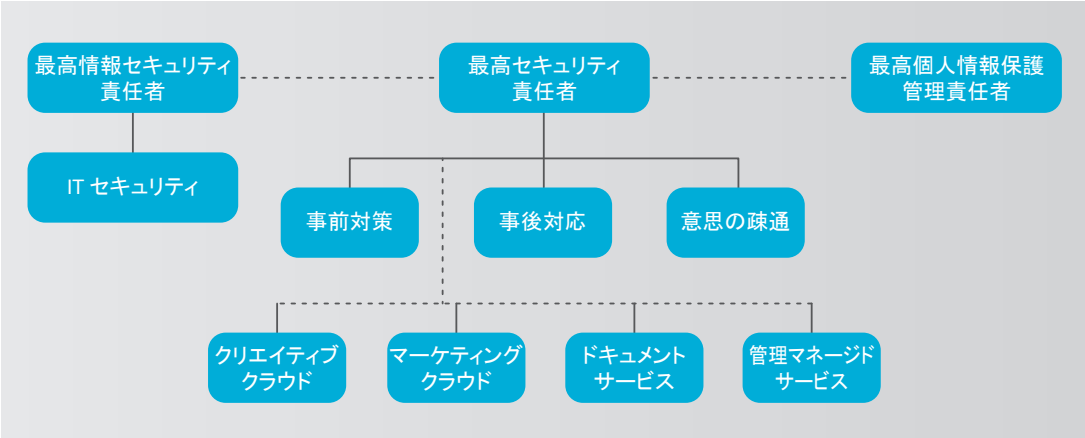
アドビにとって、デジタルエクスペリエンスにおけるセキュリティは最優先の課題です。社内のソフトウェア開発プロセスやツールに対する厳格で統一のとれたセキュリティ対策から、部門の枠を超えたインシデント対応チームに至るまで、アドビはセキュリティのすべての側面において事前対応型で、迅速かつ正確であることを目指しています。さらに、パートナー、研究者および他の業界団体と協力して、最新のセキュリティのベストプラクティスやトレンドを理解し、提供する製品およびサービスに継続的にセキュリティ対策を組み込んでいます。

このホワイトペーパーでは、Adobe Marketing Cloud におけるユーザーエクスペリエンスやデータのセキュリティを向上するために、アドビが実装する事前対応型アプローチおよび手順について説明します。

組織

製品やサービスのセキュリティに対する取り組みの一環として、アドビは最高セキュリティ責任者（CSO）の下にすべてのセキュリティ活動を統合しています。CSOのオフィスで、すべての製品・サービスのセキュリティ戦略と企業全体にわたるAdobe Secure Product Lifecycle（SPLC）の実装について統括しています。

CSOはまた、Adobe Secure Software Engineering Team（ASSET）も管理します。ASSETは、セキュリティのエキスパートが集まった専任のチームです。Adobe Marketing Cloud のデジタルマーケティング情報セキュリティチーム（DMIST）をはじめ、アドビ製品のセキュリティおよび運用を担う部門のコンサルタントとしての役割を担っています。ASSETの研究者は、各アドビ製品のセキュリティおよび運用を担当するチーム部門と協力して、製品やサービスに適切なレベルのセキュリティを実装します。その上、チームに開発、導入、運用、インシデント対応に繰り返し実行できる、わかりやすいプロセスのセキュリティベストプラクティスについてアドバイスします。



アドビのセキュリティ組織

DMISTマネージャーは、コントロールの作成、手順の実装、インシデント対応の調整およびAdobe Marketing Cloudの監査の管理を行います。

DMISTは、適切な管理、技術および物理的なコントロールを確実に実装して顧客データへの不正アクセスを防止します。DMIST セキュリティチームのメンバーは、Information Systems Security Certification Consortium, Inc（ISC）²® が付与する世界的に認められた民間のセキュリティ資格である Certified Information Systems Security Professional（CISSP®）を取得し、定期的に継続します。メンバーは、3 年ごとにその資格を更新します。DMISTセキュリティチームのメンバーは、リスクと脆弱性の管理、ネットワークセキュリティ、モニタリング、監査、コンプライアンスおよびアプリケーションセキュリティといった広範なセキュリティ分野を専門としています。

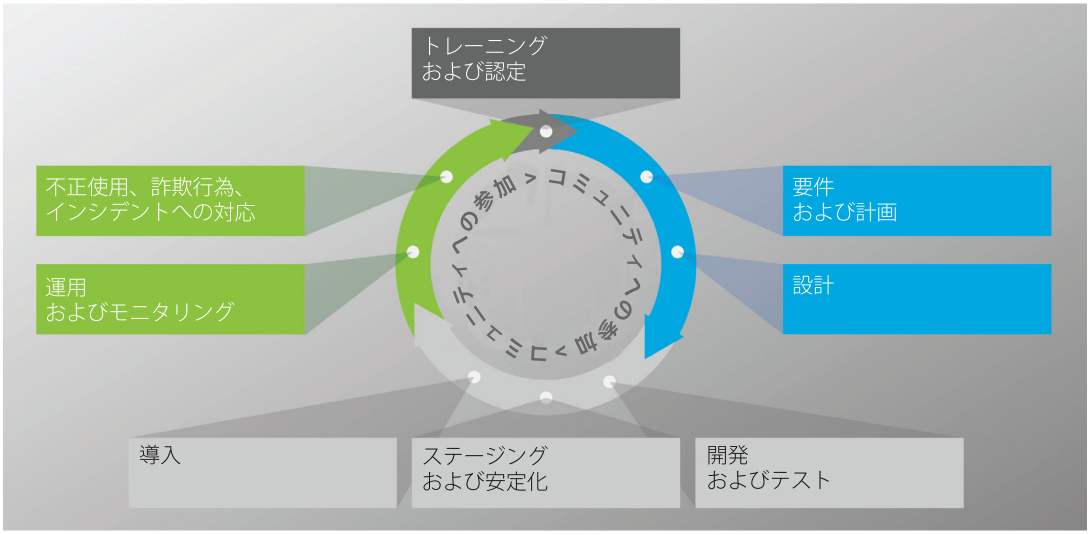
製品開発

他のアドビ製品およびサービスの組織と同様に、Adobe Digital Marketing組織ではAdobe Software Product Lifecycle（SPLC）プロセスを使用します。ソフトウェア開発のベストプラクティス、プロセスおよびツールにおよぶ数百もの特定のセキュリティコントロールを厳選したAdobe SPLCは、設計や開発から品質保証、テストおよび導入に至るまで、製品ライフサイクルのすべての段階に組み込まれます。特定のSPLCガイダンスでは、詳細なリスク評価に基づいて製品やサービスごとに細かく推奨されています。Adobe SPLCは、継続的なコミュニティ活動によって補完され、技術、セキュリティプラクティス、脅威の展望に変化が生じても、常に最新状態が保たれるようになっています。

Adobe Secure Product Lifecycle

Adobe SPLCコントロールには、それぞれのAdobe Marketing Cloudサービスに応じて、次のようなベストプラクティス、プロセス、ツールの一部またはすべてが含まれています。

- 製品チーム向けのセキュリティトレーニングと認定
- 製品の健全性、リスク、脅威の展望に関する分析
- 安全なコーディングガイドライン、ルール、分析
- Adobe Marketing CloudセキュリティチームがOpen Web Application Security Project（OWASP）の最も重大な Webアプリケーションのセキュリティ上の不具合TOP10と、CWE/SANS の最も危険なソフトウェアエラー TOP25 に対処できるようにするためのサービスロードマップ、セキュリティツールおよびテスト方法
- 包括的なセキュリティアーキテクチャのレビューと侵入テスト
- 脆弱性を引き起こす可能性がある既知の不具合を解消するためのソースコードレビュー
- ユーザー生成コンテンツの検証
- 静的および動的なコード分析
- アプリケーションとネットワークのスキャン
- 安全かつ順応性の高いレビュー、対応計画、開発者向け教材のリリース準備



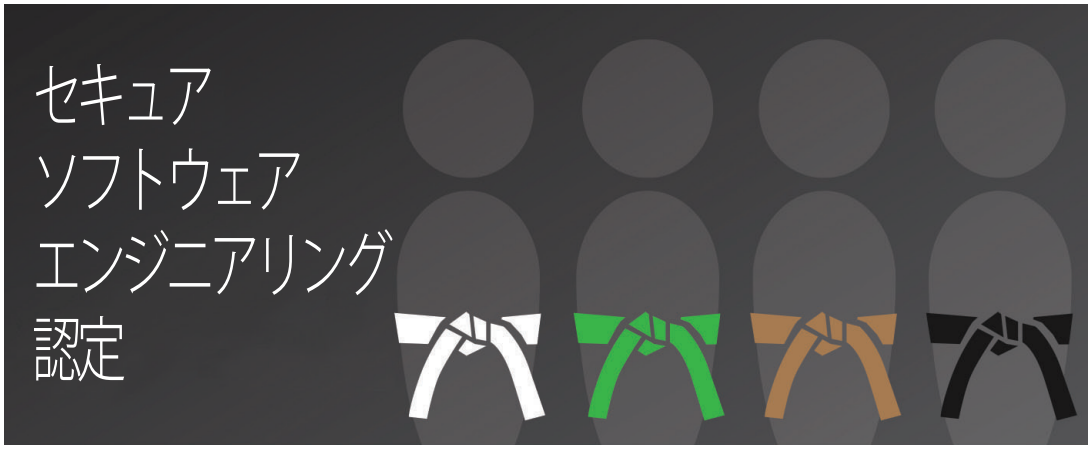
Adobe Secure Product Lifecycle（SPLC）

生産および開発環境
アドビでは、技術的なコントロールを使用して、稼働しているシステムへのネットワークレベルおよびアプリケーションレベルでのアクセスを制限し、セグメント化された開発と生産環境を維持します。従業員は開発や生産システムにアクセスするための特定の権限を付与されます。また、アドビでは、Adobe Digital Marketing環境で取られたアクションに対する説明責任を果たすために、主要なシステムのアクセスログを作成し、維持およびレビューしています。

トレーニング

アドビのソフトウェアセキュリティ認定プログラム
アドビでは、開発チームに対して継続的なセキュリティトレーニングを実施し、企業全体でセキュリティの知識を向上し、アドビ製品およびサービスの包括的なセキュリティ向上を図っています。アドビのソフトウェアセキュリティ認定プログラムに参加した従業員は、セキュリティプロジェクトを修了することで様々な認定レベルに到達します。

プログラムには4つのレベルがあり、それぞれに色つきの「帯」（白、緑、茶、黒）が指定されています。白および緑のレベルは、コンピューターベースのトレーニングを修了すると達成されます。さらに上位の茶帯および黒帯のレベルは、数ヶ月または1年にわたる実務経験を伴うセキュリティプロジェクトを修了する必要があります。茶帯および黒帯を獲得した従業員は、製品チーム内のセキュリティチャンピオンおよびエキスパートになります。新しい脅威に対応し、ソフトウェア言語を反映するためにトレーニングは毎年更新されています。



アドビのソフトウェアセキュリティ認定プログラム

Adobe Marketing Cloudセキュリティチームでは、年に1回と必要時に、部門レベル（ネットワークオペレーション、エンジニアリング、クライアントサービスなど）でより具体的なセキュリティトレーニングが実施されます。

セキュリティ認識トレーニング
アドビの従業員は、従業員オリエンテーションプロセスの一環としてセキュリティ認識トレーニングを修了しています。さらに、Adobe Digital Marketing に関係する従業員は、社内のセキュリティ認識セミナーや他の活動に参加し、組織および企業内の特定の役割にセキュリティが及ぼす影響への意識を高めます。

情報セキュリティポリシー

アドビは、ISO 27001 標準を枠組みとして使用し、企業全体にわたる広範な情報セキュリティポリシーを実装して、社内データと顧客データの両方を保護しています。次の各ポリシーは、管理承認プロセスを経ています。

- 一般的な情報セキュリティポリシー
- ネットワークセキュリティポリシー
- リモートアクセスと通信の運用ポリシー
- 電子通信ポリシー
- 制限されたアクセスの許可ポリシー
- ログインIDとパスワードに関するポリシー
- 業務行動規範

Adobe Marketing Cloud サービスでは、企業が次の追加ポリシーおよび手順を定義します。

- Adobe Digital Marketingデータ保護標準
- 認証標準
- 暗号化と安全な通信の標準
- データ上書き手順
- InfoSec情報セキュリティインシデントへの対応手順
- ライブネットワークアクセス手順
- 個人情報標準
- 物理セキュリティ標準
- 脆弱性管理標準

Adobe Marketing Cloudネットワーク

Adobe Marketing Cloudネットワークでは、データの収集、コンテンツの供給、レポート作成が行われるので、ネットワークセキュリティがとても大切になります。この目的のために、ネットワークアーキテクチャには、開発・生産環境のセグメント化、DMZ セグメント、強化された要塞ホスト、ユニークな認証など、業界標準のセキュリティ設計プラクティスが実装されています。

パスワード保護されたユーザーアクセス

Adobe Marketing Cloudサービスにアクセスするには、ユーザー名とパスワードを使った認証が要求されます。現在Adobe IDを使用しているサービスでは、SHA 256 ハッシュアルゴリズムをパスワードソルトおよび多数のハッシュの繰り返しと組み合せて使用します。アドビは継続的に開発チームと協力して、進化する認証標準に基づいて新しい保護を実装しています。

安全な管理

アドビは、Adobe Marketing Cloudサーバーを安全に管理できるようにアドビのオフィスからデータセンター施設に専用のネットワーク接続を導入しています。サーバーに対するすべての管理接続は、暗号化されたセキュアシェル（SSH）、セキュアソケットレイヤ（SSL）、仮想プライベートネットワーク（VPN）チャネルで行われ、リモートアクセスには常に二要素認証が必要です。信頼できないIPアドレスリストから接続が行われた場合、インターネットからの管理アクセスが許可されません。

ファイアウォールとロードバランサー

Adobe Marketing Cloudネットワークに実装されたファイアウォールは、許可されたポート（HTTP のポート80およびHTTPSのポート 443）を除き、すべてのインターネット接続を拒否します。ファイアウォールでは、ネットワークアドレス変換（NAT）も実行します。NATによって、サーバーに接続しているクライアントから、サーバーの実際のIPアドレスは秘匿されます。ロードバランサーは受信HTTP／HTTPS接続をプロキシーし、サービスを中断することなくネットワークで瞬時負荷スパイクを処理するリクエストに対応します。アドビは完全に冗長化されたファイアウォールとロードバランサーを実装しているため、1 つのデバイス障害がトラフィックフロー全体に波及することを防止しています。

ルーティングできないプライベートアドレス指定

アドビは、ルーティングできない IPアドレス（RFC 1918）を使用して、顧客データが格納されているすべてのサーバーを維持しています。Adobe Marketing Cloudのファイアウォール、NATと組み合わされたプライベートアドレスによって、ネットワーク上の個々のサーバーがインターネット上から直接アドレス指定されることを防ぎ、攻撃の潜在的な可能性を大幅に減らしています。

侵入検知

アドビは侵入検知システム（IDS）センサーをAdobe Marketing Cloudネットワークの重要なポイントに導入し、不正なネットワークアクセスを検知してセキュリティチームに警告しています。セキュリティチームは、警告を確認してセキュリティ侵害の兆候がないか、ターゲットにされたプラットフォームを調べることで侵入通知を追跡します。アドビでは、すべてのセンサーを定期的に更新し、適切に動作しているかどうかモニタリングしています。

サービスモニタリング
アドビは、Adobe Marketing Cloudネットワーク上のすべてのサーバー、ルーター、スイッチ、ロードバランサーおよびその他の重要なネットワーク機器を年間365日24時間休みなくモニタリングしています。Adobe Network Operations Center（NOC）は様々なモニタリングシステムから通知を受け取り、即座に問題の修正を試みたり、その問題を適切な関係者に報告します。さらに、複数の第三者たる企業と外部モニタリング契約を結んでいます。

データのバックアップ
主要なAdobe Marketing Cloud製品ラインナップの各製品の顧客データは、スナップショットを使用して毎日バックアップされます。各スナップショットは、最大 7 日間保存されます。バックアップ手順を組み合せることで、短期バックアップからの迅速なリカバリーとデータのオフサイト保護が実現されます。

変更管理
アドビは変更管理システムを使用し、変更をスケジュール化することで、リソースの依存関係を共有するチーム間でのやり取りを増やしたり、保留中の変更を関係者に通知したりします。さらに、変更管理システムを使用して、ネットワークトラフィックが多くなる期間に重ならないように保守による機能の一時停止をスケジュール設定します。

パッチ管理
Adobe Marketing Cloud組織内のホストコンピューターへのパッチ配信を自動化するために、アドビ社内のパッチおよびパッケージリポジトリーと業界標準のパッチおよび構成管理を使用します。ホストの役割と保留中のパッチの重要性に応じて、アドビは導入時と定期的なパッチスケジュールでホストにパッチを配信します。必要に応じて、短期間予告で緊急パッチをリリースおよび導入します。

アクセスコントロール
管理ツールにアクセスできるのは、アドビのイントラネット内の認定ユーザーまたはVPN接続作成の複数要素の認証プロセスを完了したリモートユーザーのみです。さらに、アドビは監査のためにすべてのAdobe Marketing Cloudプロダクションサーバーの接続を記録しています。

フォレンジック分析
アドビは、すべての画像取り込み、証拠の安全な保持および分析過程の管理記録などのフォレンジック分析プロセスに準拠しています。さらに捜査または起訴が必要な場合、アドビは法的機関と協力することもあります。

リスクおよび脆弱性管理

監査
アドビでは、内部監査を実施しています。また、Adobe Marketing Cloudネットワーク上に実装されたポリシー、手順およびコントロールに対する追加チェックとして、第三者と協力してセキュリティ監査を実施しています。これらの監査は、企業レベル、製品レベル、または確認された特定の脅威に対して実行されます。

侵入テスト
アドビでは、認可された第三者たるベンダーと協力して侵入テストを実行します。これによって、潜在的なセキュリティ脆弱性を発見し、アドビ製品およびサービスの全体的なセキュリティを向上しています。ベンダーは、業界のベストプラクティスに従ってテストを実行します。当該第三者から提供されたレポートを受け取り次第、アドビはこれらの脆弱性を文書化し、共通脆弱性評価システム（CVSS）などの業界標準のベストプラクティスに従った社内プロセスを使用して深刻度と優先度を評価し、軽減策や修復計画を作成します。お客様は、書面での要求により秘密保持契約の下で、使用したテスト方法と結果の概要を示したテスト完了通知を当該第三者から受け取ることができます。

インシデントへの対応および通知

新しい脆弱性と脅威は日々進化しているため、アドビはできる限り迅速に対応して新しく発見された脅威を軽減するよう努力しています。アドビは、US-CERT、Bugtraq、SANS などの業界全体の脆弱性アナウンスリストの利用に加え、主要なセキュリティベンダーが発行する最新のセキュリティ警告リストも利用します。

公表された脆弱性がAdobe Marketing Cloudネットワークを攻撃した可能性がある場合、DMIST セキュリティチームがカスタマイズした共通脆弱性評価システム（CVSS）のスコアを生成して、適切な脅威レベルおよび優先度を特定します。その後、Adobe Marketing Cloud 組織内の適切なチームに脆弱性を伝え、軽減に向けての取り組みを調整します。

インシデントへの対応
Adobe Marketing Cloudを含むアドビのクラウドベースサービスでは、セキュリティコーディネーションセンター（SCC）でインシデントへの対応や意思決定、外部モニタリングを一元的に管理し、全機能の一貫性と問題の迅速な解決を実現します。

アドビの製品やサービスで問題が発生した場合、SCCは関連するアドビ製品のインシデント対応チームおよび開発チームと連携して、次の実績あるプロセスを使用してできるだけ早く問題を特定、軽減、解決します。

- 脆弱性の状態評価
- プロダクションサービスにおけるリスクの軽減
- セキュリティが侵害されたノードの検疫、調査、破棄（クラウドベースのサービスのみ）
- 脆弱性のための修正プログラムの開発
- 問題を阻止する修正プログラムの展開
- 動作のモニタリングと解決策の確認
- 根本原因を特定して解消するフォレンジック分析の実行

アドビのホスティング場所

物理施設のセキュリティ
アドビが所有またはリースするホスティング施設にあるすべてのハードウェアは、物理的に不正アクセスから保護されています。Adobe Marketing Cloudのプロダクションサーバーが設置されているすべての施設には、専任の現場セキュリティ担当者が 24 時間常駐しており、これらの担当者は施設に入るための証明書を持つ必要があります。アドビは、データセンターにアクセスするためには暗証番号またはバッジ型証明書（場合によっては両方）を運用するように求めています。認可されたアクセスリストに表示された担当者のみが施設に入ることができます。一部の施設ではトラップを使用して、不正な人物が認可された担当者の後ろについて施設に入ることができないようにしています。

ビデオ監視
Adobe Marketing Cloudのプロダクションサーバーが設置されているすべての施設では、ビデオ監視を行ってポイントアクセスの出入りを最小限モニタリングする必要があります。アドビは、データセンター施設に対し、機器への物理アクセスをモニタリングするように求めています。問題が発生すると、ビデオログを確認してアクセスを特定します。

火災抑制
すべてのデータセンター施設では、空気サンプリング、即応型の煙探知システムを使用し、火災の最初の兆候が見られた時点で施設担当者に警告する必要があります。さらに、各施設にダブルインターロック方式の予作動式ドライパイプスプリンクラーシステムを設置して、煙探知機が起動したり熱が検知されたりしなければ、サーバー領域に放水されないようにしています。

コントロールされた環境
すべてのデータセンター施設は、温度湿度コントロールや液体検知を含め、環境的にコントロールされている必要があります。アドビは、完全に冗長構成の冷暖房換気空調（HVAC）システムを備え、24時間体制の施設チームにより、発生する可能性のあるあらゆる環境問題に対応できる体制を整えるように求めています。環境パラメータが定義された値から外れると、環境モニターがアドビと施設のネットワークオペレーションセンター（NOC）の両方に警告を発します。

バックアップ電源
独立した配電器からの複数の電力供給によって、アドビが所有またはリースするすべてのデータセンター施設に継続的に電力を供給できます。アドビでは、主要電源からバックアップ電源に自動的に移行することとされており、この移行はサービスを中断することなく行われます。また、各データセンター施設にあらゆるレベルで発電機やディーゼル燃料契約などの冗長性を維持するよう求めています。さらに、各施設では負荷をかけて発電機を定期的にテストして機器の可用性を確認します。

アドビのオフィス

アドビは世界中にオフィスがあるため、次のプロセスと手順を企業全体に実装してセキュリティの脅威から企業を保護します。

物理的なセキュリティ

アドビのすべてのオフィス所在地では、現地の警備員を採用して敷地を 24 時間体制で保護しています。アドビの従業員は、建物にアクセスするためのキーカード型IDバッジを携帯しています。訪問者は正面入口から入り、受付で署名して一時的な訪問者IDバッジを掲示します。訪問者には常に従業員が同伴します。サーバー機器、開発マシン、電話システム、ファイルサーバーとメールサーバーおよびその他のデリケートなシステムは環境コントロールされたサーバールームに常時設置されており、そのサーバールームには認可されたスタッフメンバーのみがアクセスすることができます。

ウイルス対策

アドビでは、送受信されたすべての企業電子メールをスキャンして既知のマルウェアによる脅威をスキャンしています。

アドビの従業員

従業員による顧客データへのアクセス

アドビでは、認可された適切な従業員のみが顧客データにアクセスできます。役割ベースのアクセスを使用し、特定のジョブ機能に基づいてデータへの従業員アクセスを制限します。アドビでは、業務上正当なアクセスであると書面で承諾を受け、身元調査を通過した後にのみ、Adobe Marketing Cloudネットワークにアクセスできます。アドビは、アクセス権限と職責変更を定期的に確認します。

身元調査

アドビは、雇用目的で身元調査レポートを取得します。アドビが通常調べるレポートの内容および範囲には、適用される法令で許可される範囲において、学歴、職歴、犯罪歴などの裁判記録の照会と同僚や友人による身元保証が含まれます。これらの身元調査要件は、システムを管理したり顧客情報にアクセスしたりすることになる米国の新規の正社員に適用されます。米国の新規の派遣社員には、アドビの身元調査ガイドラインに従って適切な派遣会社を通して身元調査要件が課されます。米国以外では、アドビの身元調査ポリシーと適切な現地法に従って特定の新入社員について身元調査を行います。

従業員の退職

従業員がアドビから退職する場合、従業員の上司が退職届を提出します。承認されると、アドビの人事担当が電子メールワークフローを開始して関係者にその従業員の退職日までに特定の処理を行うように通知します。アドビが従業員を解雇する場合は、人事担当が従業員の退職日時を示した同様の電子メール通知を関係者に送信します。

アドビの企業セキュリティ担当は次の処理のスケジュールを設定して、従業員の退職日にその従業員がアドビの機密情報ファイルやオフィスにアクセスできないようにします。

- 電子メールアクセスの削除
- リモートVPNアクセスの削除
- オフィスおよびデータセンターのバッジの無効化
- ネットワークアクセスの終了

要求に応じて、上司はアドビのオフィスまたは建物から退職する従業員に警備員を同伴させることができます。

顧客データの機密保持

アドビは、顧客データのセキュリティを重視し、顧客データを常に機密情報として扱います。お客様との契約で許可されている場合を除き、アドビはお客様の代わりに収集した情報を使用しません。詳細は、アドビのプライバシーポリシー（http://www.adobe.com/jp/privacy/policy.html）を参照してください。アドビのプライバシーポリシーに記載されている場合または Adobe Marketing Cloudサービスを使用する企業から要求された場合を除き、アドビは顧客データを共有しません。

まとめ

本ホワイトペーパーで説明したセキュリティの事前対応型アプローチと厳格な手順によって、Adobe Marketing Cloudデータをセキュリティ保護しています。厳格な社内ソフトウェア開発プロセスおよびツールから部門の枠を超えたインシデント対応チームに至るまで、アドビはデジタルマーケティングデータのセキュリティを重要視しています。

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

12/13