jamf

ホワイトペーパー

macOS セキュリティ インシデント対応 ガイド

サイバー攻撃やセキュリティ侵害が発生した際、被害の大きさや復旧時間の長さ、損失コストの大きさは組織がどれだけ効率的かつ効果的に対応できるかにかかっています。このようなプロセスはセキュリティインシデント対応と呼ばれ、IT 部門や情報セキュリティ部門が用意したセキュリティプログラムの成功を左右する重要な要素です。

大半の組織でセキュリティ上の脅威に対抗するための堅牢な対策が用意されていますが、サイバー攻撃やセキュリティ侵害が発生した時に備えて、ツールやワークフロー、ベストプラクティスを用意しておく必要があります。そして、組織で使用される Mac の台数が増える今こそ、Mac のセキュリティ対策を強化して組織を保護するときです。

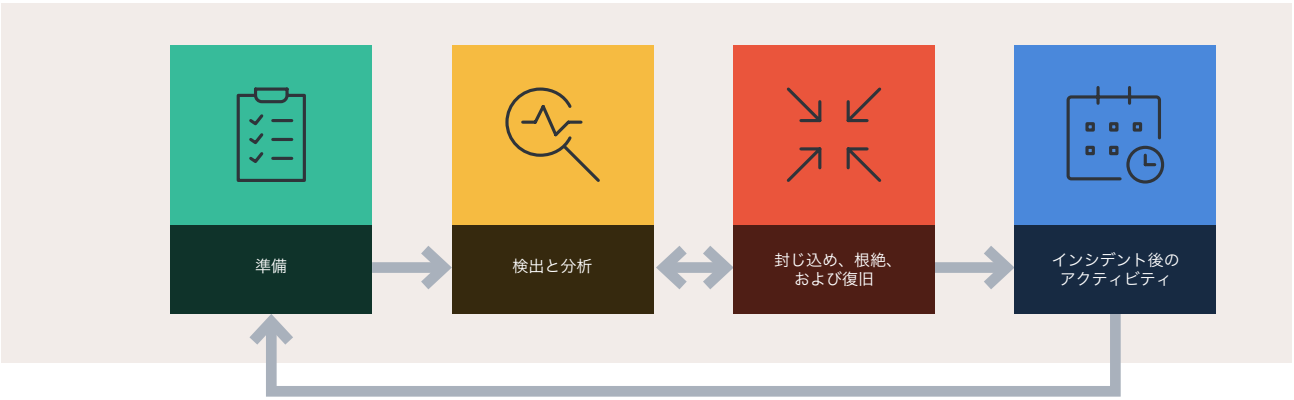
このホワイトペーパーでは 次のステップについて説明します

1. インシデントに備える
2. インシデントを検出して分析する
3. インシデントの封じ込め、根絶、復旧を行
4. インシデント後のアクティビティを監視する

攻撃の種類に応じて防御策

組織内で Mac の台数が増えるにつれ、Windows 中心のセキュリティソリューションで提供されているよりも強力な方法で組織内の Mac を保護することにフォーカスする必要があります。すべての Mac にセキュリティツールが組み込まれていますが、攻撃方法が変化して Mac の市場シェアが拡大したことで、Mac と組織のデータを保護するためのより優れた方法が求められています。一方、Mac のセキュリティソリューションをどのように活用しているかにかかわらず、インシデント対応は組織的かつ一貫した方法で進める必要があります。

アメリカ国立標準技術研究所（NIST）ではセキュリティインシデント対応の構成要素として以下の 4 つを定めています。



ステップ 1：インシデントに備える

ほぼすべての組織にとってセキュリティは最優先事項となっており、リモートワークの拡大に伴い、インシデントへの備えがますます重要になっています。IT 管理者はエンドポイントのセキュリティを最大限に高める必要があります。セキュリティを確保するにはエンドポイントを管理、監視してパッチを適用し、セキュリティ設定をする必要があります。これらを行うために、さまざまなツールが活躍します。

Jamf Pro に用意されたダッシュボードを利用すると、Mac デバイスの状態を常に評価しながら注意が必要なハードウェアを把握できます。特許技術を有するスマートグループ機能によって、IT 管理者は更新や再構成、パッチ適用が必要なデバイスを絞り込んでセキュリティを強化することが可能です。こうした作業は、IT 担当者がデバイスを直接操作しなくてもすべてリモートから実行可能で、自動化することもできます。

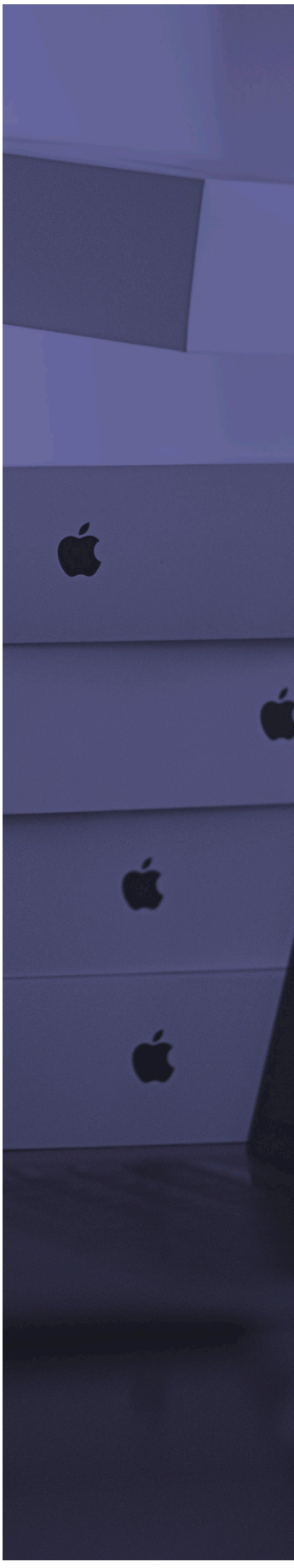
デバイスで起きていることを把握するために、Mac に特化したエンドポイントセキュリティソリューションである Jamf Protect ではプロセス情報とファイル情報とともにその他の行動分析を収集します。こうした情報をリアルタイム分析と事後分析に役立てることで、悪意のあるアクティビティを検出してアラートを生成します。以下の点に注目してください。

- Jamf Protect の脅威検出機能では、マルウェアとアドウェアを自動的にブロックおよび隔離します。望ましくない特定のソフトウェアを制限したい場合は、Jamf Protect 内で署名や開発者の TeamID などで定義することができます。
- macOS に対する一般的な攻撃パターンは Jamf Protect に組み込まれたアナリティクスによって検出されます。検出メカニズムが適切にリスクを軽減できるように、アナリティクスは MITRE ATT&CK® フレームワークにマッピングされていて、高い信頼性で攻撃ベクトルに対応します。
- Jamf Protect は検出した攻撃に関連するさまざまなレベルのデータを収集するため、脅威検出時にはすべてのプロセス、ユーザ、グループ、そしてバイナリ情報を確認することができます。
- データとアラートは Jamf Protect から SIEM に送信できます。さらに、macOS 統合ログのログデータを直接 SIEM や他のシステムに送信可能です。
- 多くの攻撃で対応方法が共通しているため、Jamf Pro を使って望ましい対応方法や修復方法を設定および自動化することができます。
- Jamf Pro では、スマートグループで範囲を指定してポリシーと構成プロファイルを配布することで、インシデント対応中に追加の対応ワークフローを自動的にトリガーしたり手動で実行したりすることができます。

ポリシーと構成プロファイルによって以下のことが可能になります。

ネットワークの分離	ダメージの封じ込めが必要な、積極的な攻撃を受けている可能性があるデバイスを隔離します。
ペナルティボックス	信頼されていないユーザーが社内リソースにアクセスできないようにします。
デバイスのロック	疑わしいアクティビティを調査している最中にユーザーがデバイスを使えないようにします。
オブジェクトの削除	望ましくないアプリケーションやプラグイン、ファイルをデバイスからリモートから削除します。
デバイスの隔離	インシデント対応の一環としてデバイスを直接操作する必要があり、リモートからでは復旧できない場合、IT 担当者がデバイスを操作できるようになるまでデバイスの隔離を行います。
カスタムのスクリプトやコマンドの実行	スクリプトとコマンドを活用して、デバイスを直接操作せずにデータやデバイス情報をリモートから復旧します。
エンドユーザーへのカスタムメッセージの送信	試みられた攻撃や組織のポリシー、ベストプラクティスなどの情報を直接エンドユーザーに伝えます。
デバイスの復旧	デバイスを初期化する必要がある場合、リモートから macOS とアプリケーションの再デプロイを実行します。

ステップ 2：インシデントを検出して分析する



セキュリティ部門は、攻撃を示すイベントのアラートを受け取ることができますが、それでも積極的に注意を払っていく必要があります。また、準備や防止策が整っている場合でも、最良の防御策を攻撃が突破することを想定して準備を整えておかなければなりません。

感染しているアプリケーションをエンドユーザーが誤ってダウンロードしてしまった場面を想像してみてください。そのタイミングこそエンドポイントセキュリティソリューションが威力を発揮するときです。セキュリティインシデントが発生してその影響がまったくわからないときは、関連する情報を集めて脅威を分析し、被害を受けたデバイスを隔離してさらなる感染を阻止する必要があります。

インシデントの調査中は、セキュリティ部門は常に詳細を把握しなければなりません。これを実現するために、通常は SIEM や他のログ集約システムでさまざまなシステムやデバイスからログを集めます。調査や監査を実施しているときには、社内の Mac デバイスに何が起きているかを完全に把握して、必要な情報を見ることができます。

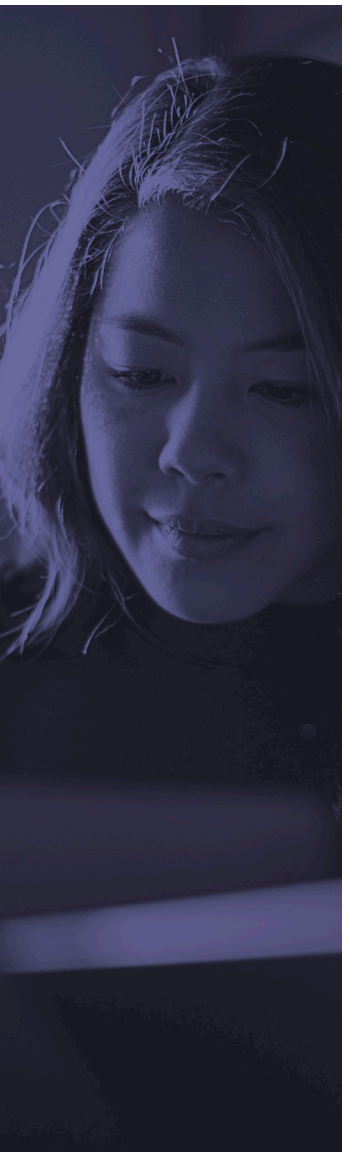
ステップ 3：インシデントの封じ込め、根絶、復旧を行う

ネットワーク内で攻撃が発生している時には時間が最も重要です。まず、攻撃を阻止し他のシステムに攻撃が拡大するのを防ぐ必要があります。準備が整っているため、関連するプロセスは Jamf Protect によってブロックされますが、一目ではわかりにくい他の攻撃者が足掛かりを築くところまで根絶できるわけではありません。アクティビティベースのアラートに対応するときに被害を最小限に抑えるため、Jamf Protect ではスマートグループ機能やすべてのモバイルデバイス管理（MDM）および Jamf Pro のコマンドを活用します。対応の自動化の例としては、次のようなものがあります。

- ネットワーク上のマシンを隔離して管理インフラストラクチャとしか通信できないようにする。
- クラウドや社内リソースへのアクセスを減らす。
- デバイスで悪意のあるアクティビティが発生していることをエンドユーザーに知らせて、さらなるアクションが実行されないようにする。

デバイスの安全が確保されて攻撃を止めたら、IT 部門とセキュリティ部門はデバイスで何が起きたかを詳しく調査して、他のスクリプトやバイナリ、バックドア、新しい認証情報、新たなリスクが残っていないかを確認します。Jamf を使うと部門で以下のことを実行できます。

- 隔離されたバイナリを調査のために取得する。
- 検出したバイナリやその他のファイルを削除する。
- 新たにインストールされたアプリケーションを特定する。
- 新しいローカルユーザーアカウントを特定する。



Jamf によって攻撃が緩和されても、その後デバイスを信頼済み状態に戻す必要があります。Jamf Pro のポリシーとスマートグループを活用して以下を実行することで、負荷を増やさずに環境をクリーンアップできます。

- カスタムのスクリプトやコマンドを実行してセキュリティ設定をリセットする。
- カスタムメッセージをエンドユーザーに送って追加のヘルプリソースに誘導する。
- デバイスに macOS を再デプロイして必要なアプリケーションを再インストールする。

ステップ 4：インシデント後のアクティビティを監視する

Jamf Protect は、インシデント発生時に IT 部門とセキュリティ部門へ通知をし、何が起きたかを正確に分析できるツールを提供します。Windows の世界では封じ込めや根絶、復旧のプロセスを組織に合わせて用意するのが一般的ですが、Jamf ではこうした機能を Mac にもたらすことで、次にセキュリティインシデントが発生したときに、Apple のやり方に従った形で部門で対応して修復することができます。

インシデント発生後：

- Jamf Protect は監視を継続して、新たな脅威やアクティビティが発生したときに通知します。
- Jamf Protect アナリティクスをカスタマイズして拡張し、自社の IT 部門や情報セキュリティ部門が特定して絞り込んだ新たな標的型の脅威に対応することができます。
- また、特定した脅威のバイナリ情報をカスタムのブロックリストに追加することで社内の Mac デバイス全体を保護します。
- 攻撃対象になったエンドユーザーは業務上の情報セキュリティ教育を受講して再認定を受けます。

今すぐ Mac のセキュリティ強化を始めましょう

セキュリティインシデントを適切に評価して攻撃に対する潜在的な脆弱性を判断するために、Jamf Pro と Jamf Protect を組み合わせることで、社内の Mac デバイスに対して実行される無数の攻撃を監視、ブロック、検出し、これらに対応します。

感染しているアプリケーションをエンドユーザーがダウンロードしたり、スピアフィッシングやランサムウェア攻撃が発生しても、あらかじめ用意された修復方法があることで、必要な対応を行いハードウェアやソフトウェア、組織のデータを保護できます。

Jamf のセキュリティインシデント対応機能のデモをぜひご覧ください。

Jamf Protect デモをリクエスト