新機能：
Sophos Cloud Native Security

環境、ワークロード、アイデンティティを網羅する
マルチクラウドセキュリティのカバレッジを実現

SOPHOS
Cybersecurity delivered.

単一の統合クラウド セキュリティ ソリューション

ホスト、コンテナ、ストレージサービス、Infrastructure as Code などのクラウドテクノロジーへの移行は、組織が可視性を高めて、構成ミス、マルウェア、ランサムウェア、侵害などから保護する必要があることを意味しています。

Sophos Cloud Native Security は、可視性を提供するために必要なツールを統合し、クラウド環境を堅牢で侵害を阻止します。また、迅速な復旧を実現します。Sophos Cloud Native Security は、Amazon Web Services、Microsoft Azure、Google Cloud Platform で利用できる単一の統合ソリューションで、Sophos Cloud Optix と Sophos Intercept X Advanced for Server XDR を組み合わせています。

Sophos Central コンソールの単一管理画面では、マルチクラウド脅威の検出、インシデントの優先的な検出、自動的に接続されたセキュリティイベントを活用して、脅威の調査と対応時間をすべて一ヵ所で最適化することができます。

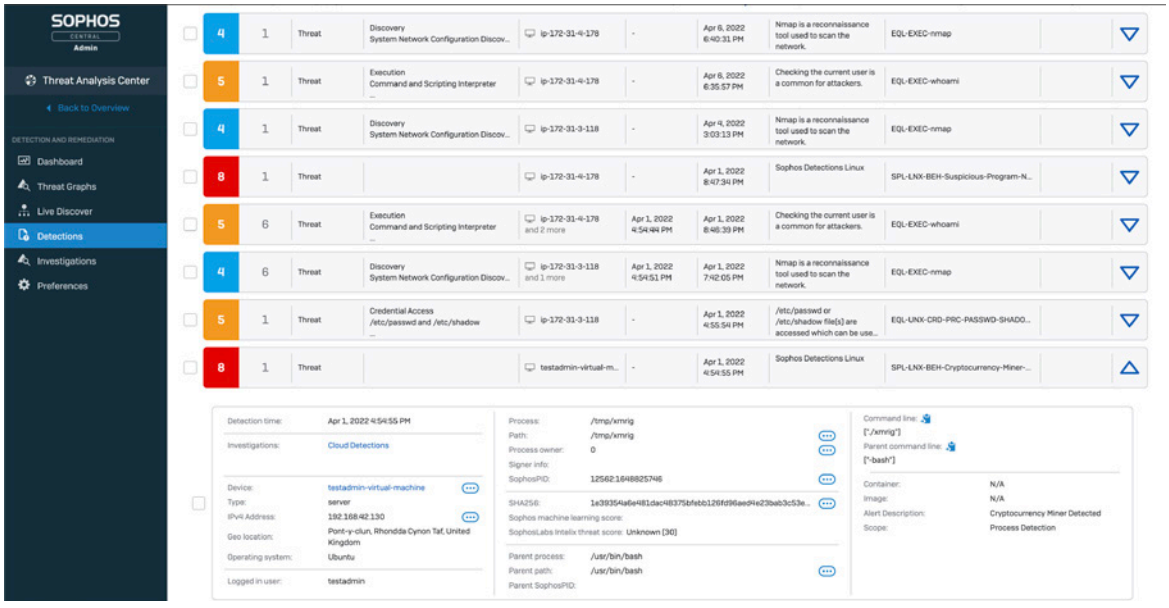
ソフォスサーバー保護機能の今後の進化

ソフォスは、パブリッククラウドでサーバーのワークロードを保護するために、信頼性の高い Windows 保護機能を拡張し、クラウドで最も普及している OS の 1つである Linux の展開を保護することに成功しました。

今年初めに、クラウドワークロード向けソフォスサーバー保護機能では、Linux とコンテナに関する機能が大幅に進化しました。これには、高度な Linux セキュリティインシデントを発生時に特定するための新しい動作とエクスプロイトのランタイム脅威保護が追加されました。

Sophos Cloud Native Security は、お客様のインフラストラクチャとデータを保護に必要なワークロード保護機能を提供し、クラウドの進化に合わせて対応します。

- すべてを保護。クラウド、データセンター、ホスト、コンテナ、Windows、または Linux。
- エージェントまたは Linux 用 API 経由の軽量な Linux/Windows ホスト保護により、パフォーマンスとアップタイムを確保します。
- カーネルモジュールを導入せずに、実行時に Linux およびコンテナの高度なセキュリティインシデントを特定します。
- Windows ホストとリモートワーカーをランサムウェア、エクスプロイト、未知の脅威から保護します。
- アプリケーションの管理、構成のロック、重要な Windows システムファイルへの変更の監視を行います。
- Extended Detection and Response (XDR) を使用して、脅威の調査と対応を効率化し、イベントの優先順位付けと関連付けを行います。



Sophos Central コンソールで Sophos XDR Linux ランタイムの脅威を検出した例。

クラウドワークロード保護展開オプション

Sophos Central の管理 – この軽量 Linux エージェントは、セキュリティチームに、Windows および Linux の振る舞い、エクスプロイト、マルウェアの脅威を 1ヵ所で調査および対応するために必要な重要な情報を提供します。ホストを監視するこの展開オプションにより、チームはソフォスソリューションを単一画面で管理し、脅威ハンティング、修復、管理間をシームレスに移動できます。

API の統合 - Sophos Linux Sensor は、パフォーマンスに合わせて微調整された、柔軟性の高い展開オプションです。この Sensor は、API を使用して、ホスト環境またはコンテナ環境でのリッチランタイム脅威検出と既存の脅威対応ツールを統合します。これは、特定のセキュリティユースケースを満たすために必要なランタイム動作検出のみを含んだカスタムルールセットを作成する、より高いレベルの制御を提供します。

Sophos Linux Agent に加え、Sophos Linux Sensor は次の機能を提供します。

- その他の検出: アプリケーションやシステムの悪用を目的とした追加検出にアクセス
- 設定とチューニング: デフォルト検出の許可リストとブロックリストを変更するオプション
- リソースのチューニング: ホストリソースの使用率を最適化するための設定オプション

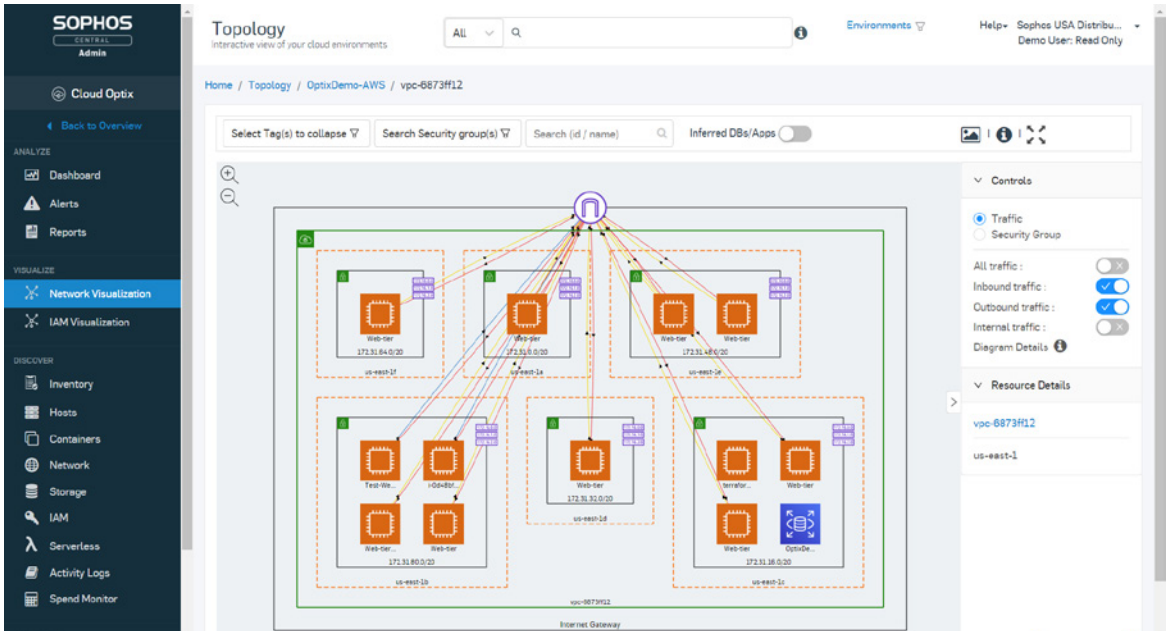
必要な保護の詳細

AWS、Azure、GCP 環境全体における攻撃対象領域の削減は、クラウドワークロードの脅威の保護と検知にとどまりません。そのため、ソフォス Cloud Native Security では、セキュリティツールキットを 1つのツールに統合して、クラウドセキュリティポスチャ管理、Kubernetes セキュリティポスチャ管理、Infrastructure as Code セキュリティ、クラウドインフラエンタイトルメント管理、クラウド支出監視などを行います。

マルチクラウドの可視性、ガバナンス、コンプライアンスを実現

単一のコンソールで、AWS、Azure、GCP、Kubernetes、Infrastructure as Code、Docker Hub 環境全体にエージェントレスの可視性と修復ツールを使用することで、効率性を高めます。

- オンデマンドのアセットインベントリやエクスポート可能なネットワークトポロジの可視化により、全体像を把握できます。
- Azure Advisor、Azure Sentinel、AWS Security Hub、Amazon GuardDuty、AWS CloudTrail、AWS IAM Access Analyzer、Amazon Detective、Amazon Inspector、AWS Systems Manager、AWS Trusted Advisor などのクラウド プロバイダー セキュリティ サービスを単一のビューで統合します。
- ソフォスのワークロード保護エージェントとファイアウォールの自動アセット検出と可視化機能が、シャドー IT を防止します。
- ホスト、コンテナ、Kubernetes、サーバーレス、ストレージおよびデータベース サービス、ネットワーク セキュリティグループ全体の構成リスクの防止および修復を行います。
- 自動的にお客様の環境にマッピングされるポリシーにより、セキュリティとコンプライアンス基準を継続的に監視および維持し、監査対応レポートにより数週間の労力を節約します。CIS Foundations Benchmark、ISO 27001、EBU R 143、 FEDRAMP FIEC、GDPR、HIPAA、PCI DSS、SOC2、ソフォス ベスト プラクティスを含むポリシーです。
- 単一の画面に複数の AWS および Azure サービスのクラウドコストを並べて把握できるようにして可視性を高め、無駄な支出を削減します。クラウドプロバイダーのコストを最適化するための推奨事項をソフォスより受信、または AWS Trusted Advisor や Azure Advisor サービスと統合することができます。
- 警告による疲弊を軽減し、リスク評価と色分けされた警告を使用して、迅速な解決と重要な問題を効率的に検出し、詳細な修正手順を表示します。

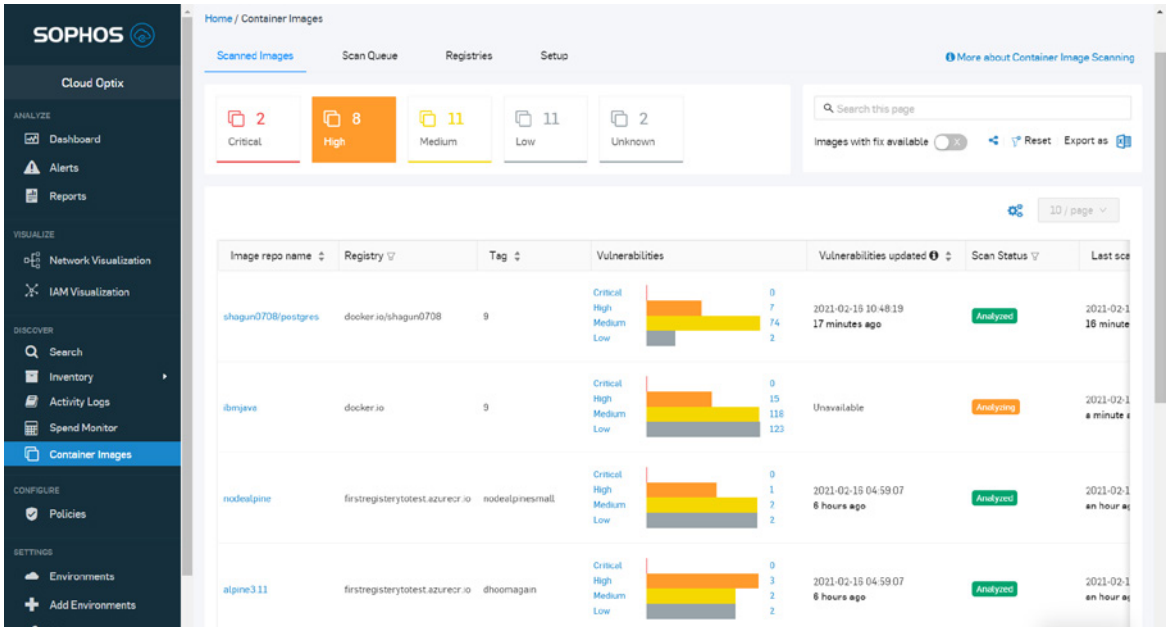


セキュリティ グループ分析による AWS 向けのソフォス ネットワーク トポロジの視覚化の例。

DevOps スピードを損なうことなくリスクを低減

開発パイプラインのどの段階であっても、統合されたセキュリティ構成とコンプライアンスチェックにより、高速でセキュアな開発を可能にします。

- Terraform、AWS CloudFormation、Ansible、Kubernetes、Azure Resource Manager テンプレートファイルの構成ミス、埋め込まれた機密情報、パスワード、キーを自動的に検出します。
- OS の脆弱性を持つコンテナの展開を防止し、利用可能な修正を特定します。Amazon ECR、ACR、Docker Hub レジストリ、Infrastructure as Code 環境、ビルドパイプラインにおけるイメージをサポートします。
- GitHub および Bitbucket とのシームレスな統合を行い、Sophos Central でオンデマンドスキャンの結果を受け取るか、REST API を使用して開発の任意の段階で Infrastructure as Code テンプレートをスキャンします。

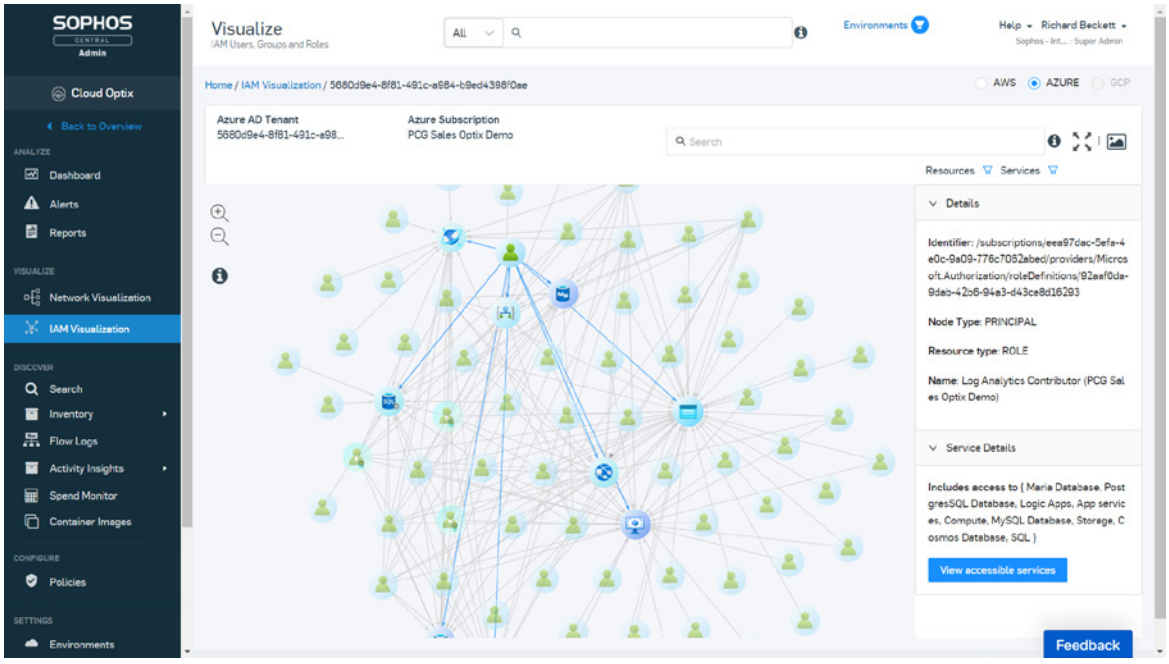


ソフォス コンテナ イメージスキャンの脆弱性評価結果の概要の例。

最小権限の原則を適用

マルチクラウド環境全体にクラウド インフラストラクチャ エンタイトルメント管理で最小限の権限の実装をソフォスが支援することで、ID が悪用される前に管理します。

- すべてのアイデンティティは、それぞれのタスクに必要なアクションのみを実行できるようになります。
- 通常とは異なるユーザーのアクセスパターンや場所を特定し、認証情報の不正使用や盗難を識別します。
- 環境へのアクセスに使用される、使われず、管理されず、古くなった、Microsoft Azure IAM ロールを浮き彫りにします。
- 複雑に絡み合った AWS IAM ロールを可視化し、IAM ロールに対する過剰な権限の付与を素早くハイライトして防止します。
- SophosAI を活用して、AWS 環境のユーザー動作におけるリスクの高い異常を結びつけて、セキュリティ侵害を防止します。

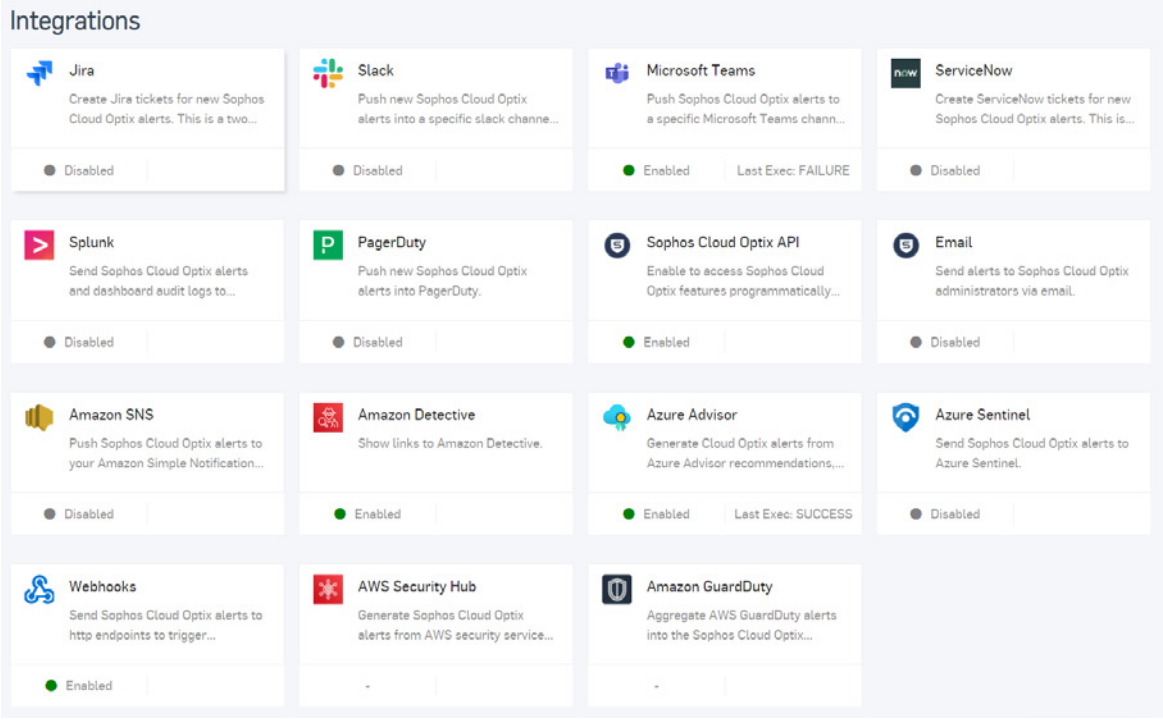


Microsoft Azure 向けの Sophos IAM 可視化の例。

SecOps を効率化し、コラボレーションを強化

クラウド環境のセキュリティポスチャ警告を、たったの数回のクリックで、一般的な SIEM、コラボレーション、ワークフロー、DevOps ツールと統合し、組織全体の俊敏性を向上させます。

- IT 管理担当: Splunk、Azure Sentinel、PagerDuty と統合し、セキュリティおよびコンプライアンスイベントの通知を即座に受け取れるようにします。
- コラボレーションツール：Slack、Microsoft Teams、Amazon SNS (Simple Notification Service) にクイック通知を送信し、トピックに関するコラボレーションを行うことができます。
- ワークフロー管理：Sophos Central から JIRA や ServiceNow のチケットを作成し、標準ワークフローにアラート対応を組み込んで、チケットの重複を回避します。



クラウドセキュリティポスチャ管理の警告を管理するための一般的なソフォスの統合ソリューションの例。

チームを強化するパートナーシップ

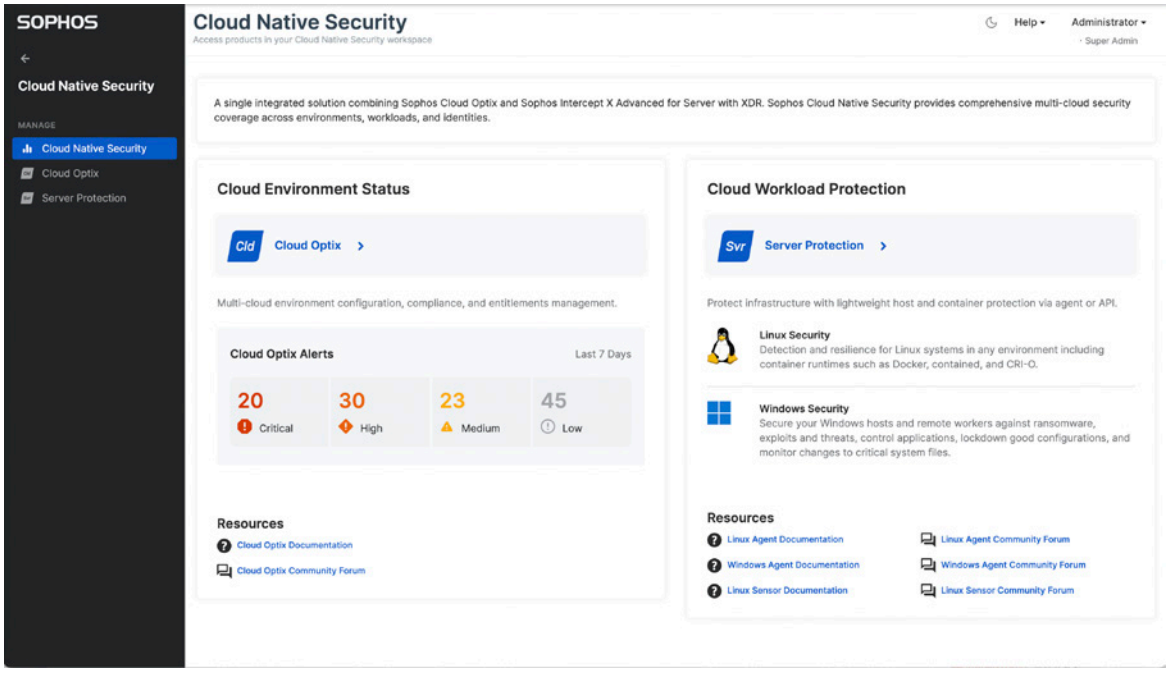
セキュリティチーム、ソフォスパートナーの支援、または Sophos MTR (Managed Threat Response) サービスを使用して 24時間年中無休で監視や対応を行うことができます。

Sophos MTR は、Sophos Cloud Native Security を補完するのに最適です。この MTR (Managed Threat Response) サービスは、お客様と連携して、お客様の環境を年中無休で監視し、潜在的な脅威に対応し、感染の痕跡を検索します。いつ、どこで、なにが、どのように、なぜ起きたのかなどのイベントに関する詳細な分析を提供し、高度な脅威がデータやシステムを標的にするのを防ぎます。

Sophos Cloud Native Security の利用状況

この新しい統合パッケージは、すべてのお客様が利用でき、Intercept X Essentials for Server、Intercept X Advanced for Server、および Intercept X Advanced for Server with XDR からにアップグレードが可能です。

Sophos Central 内で有効にすると、左側のナビゲーションに新しい「CNS」項目が表示されます。これは、Sophos Cloud Optix と Intercept X Advanced for Server with XDR 製品へのアクセスを提供する新しい Cloud Native Security の概要ダッシュボードにリンクしています。



Sophos Central 管理コンソールの Sophos Cloud Native Security ダッシュボードの例。

無償評価版

無償評価版の登録 (30日間)
sophos.com/ja-jp/cloud

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-07-06 JA (DD)