リリースノート（参考資料）

AdRem NetCrunch 12

AdRem NetCrunch 12 リリースノート

NetCrunch は AdRem Software が開発し所有する監視ソフトウェアである。
株式会社情報工房は日本における総販売代理店である。

[20220809]

目次

1. 本資料について

本資料では、AdRem NetCrunch バージョン 12.1.1.6459 日本語版（以下 12）について記しております。

2. NetCrunch 12 の新機能/変更点/修正点

NetCrunch 12 での新機能、変更点、修正点について記載いたします。

2.1. バージョン 12.1.1.6459

- アクティブアラートビュー – 任意のカスタマイズが可能なりました
- アトラスビューステータス – IP ネットワークを含む任意のアトラスビューのステータスを表示
- カスタマイズ可能な物理的セグメントマップ – 物理的セグメントマップのレイアウトをカスタマイズできるようになりました
- ノードタブのカスタマイズ可能なビュー – ノードビューをカスタマイズして保存
- マウスの右クリックでグラフィカルエディタのポップアップメニューに使用可能なオプションを表示
- IP Tools –「タイムアウト」および「試行回数」オプションに「SNMP スキャナー」を追加
- ライブインターフェイスステータスから MAC アドレスをクリップボードにコピーできるようになりました
- ノードアイコンウィジェット – 新しいオプションの「クリア」、「ライトテキストとクリア」、「ダークテキスト」を追加
- 並べ替え可能なノードタイルビューを追加
- パスワードリセットに関する問題を修正
- 刷新されたネットワークサービスステータスウィンドウ – 各サービスのステータス、応答時間、可用性を表示
- SNMP 設定ファイル – SNMP エンジンパラメータは「engine.cfg.yaml」を使用してカスタマイズが可能になりました
- 設定メニュー – 全ての設定が NetCrunch メニューから利用できるようになりました
- シェイプシャドウ – 色を変更して中央に配置できる新しいオプションを追加
- アクティブアラートと監視の問題のステータスダッシュボードセクションを関連するビューと接続しました
- 監査ログ/アクティビティ – ユーザーの構成アクティビティを別の暗号化されたデータベースに保存
- クラウドサービスノード – 単一のクラウドサービス（Azure、Amazon AWS、Google、その他のサービス）を監視
- ダークモード – ステータス、トップチャート、アラート、ノードなどの多くのウィンドウに追加
- デバイスコンフィグ管理 – 組み込みエディターと YAML にカスタムプロファイルを追加できます

- デバイスコンフィグ管理 – スイッチ、ルーター、ファイアウォールなどの様々なデバイスの構成変更を監視および保存
- トレンドとイベントのエクスポート – NCCLI コマンドラインユーティリティを使用して、NetCrunch からトレンドとイベントをエクスポートできます
- Extended Discovery Exclusions – 特定のアドレススペースを除外設定できます
- GrafCrunch – Grafana のバージョン 7.x に基づいてアップグレードされました
- グラフィカルビュー – 完全にインタラクティブで、デスクトップと Web コンソールで利用できる新しい現代的なエディターを追加
- ハードウェアビュー – Windows ノードのメモリ量、CPU 数/種類、ストレージ情報などの Windows マシンからのデータを表示
- アクセスプロフィール管理の向上 – 64 プロフィールに制限されなくなりました
- アクティブアラートビューの向上 – アラートソース列を提供
- 自動化された全画面表示の向上 – Web コンソールに移動
- イベントの詳細ウィンドウの向上 – 特定のアラートに関連する全てのタイプの操作が表示
- イベント詳細ウィンドウの向上 – あらゆる種類のしきい値を正確に視覚化
- トレンドビューアの向上 – 新しいバージョンでは、より多くの種類のグラフを使用でき、最小、最大、平均の線を表示するための追加オプションを追加
- インタラクティブグラフウィジェット – データの時間間隔に応じて自動的に更新されます。ユーザーはトレンドビューアまたは特定のノードメニューを簡単に開くことができます
- インタラクティブウィジェット –全てのウィジェットはインタラクティブであり、根本原因分析のために簡単にドリルダウンできます
- インターフェース監視 – リモートプローブが SNMP とインターフェースの監視をサポート
- 制限しきい値 – 指定された期間にわたって値を収集し、制限を超えた場合にユーザーに通知
- 監視依存関係マネージャー – 全ての監視依存関係を簡単に確認できます
- 監視依存関係マネージャー – 要素のドラッグアンドドロップが可能になりました
- 監視依存関係マネージャー – プローブとリモートアドレス空間をサポート
- 監視依存関係の再スキャンが可能になりました
- 監視プローブ – 分離されたネットワークを監視するためにリモートで使用することや NetCrunch サーバーの追加の監視エンジン
- ターゲット監視 – 関連する全てのモニターを 1 か所で検索し、必要に応じて新しいノードを作成できます
- ノードトラフィックビューを使用すると、データをよりクリーンな方法で表示し、通信者のリストを検索
- NetCrunch サーバーダッシュボード – 現在の NetCrunch の負荷と状態にすばやくアクセスでき、過去 7 日間のリソース使用履歴を表示
- 物理的セグメントマップ – 通常のマップと同じように、特定のポイントで簡単にドラッグおよびズームができます。
- 最近のセクション – 最後にクリックされた 5 件の検索結果を含む検索フィールドを表示
- 概要ダッシュボードを向上 – ダークモードをサポート
- トップチャートの向上 – ダークモードをサポート
- ルーティングマップの向上 – 検索及びナビゲート、ズーム、ドラッグをサポート

- SNMP ビューの向上 – 監視プローブによってサポートされる新しいエンジンをもたらします。ノードに書き込み可能な SNMP プロファイルがある場合、デバイスの SNMP データを簡単に変更できます
- [設定]タブ – 以前にトップメニューに配置されたすべての設定が含まれます
- ステータスダッシュボード – 特定のノードまたはアラートの概要をすばやく確認するための新しいツールチップを提供
- [タスク]タブ – 添付ファイルを使用して単純なタスクを追跡するための小さなユーティリティ
- 以下の監視センサーを追加、修正
  - AWS アラームセンサー – 最も重要な AWS アラームを追跡でき、監視を拡張して、データ不足などの状態について警告
  - AWS Auto Scaling センサー – Auto Scaling Group 内の変更を追跡し、グループインスタンスの複数の状態を監視
  - AWS Cost センサー – AWS サービスを使用するための予算と推定コストの使用を監視
  - AWS EBS センサー – 単一の EBS インスタンスによって使用されるパフォーマンスとリソースの観点から EBS を監視
  - AWS EC2 センサー – 利用可能な各 EC2 インスタンスリソースのネットワーク負荷、ディスク使用率、CPU 使用率を監視
  - AWS ELB センサー – ユーザーのアプリケーションの状態とそのパフォーマンスをリアルタイムで監視
  - AWS ElastiCache センサー – ElastiCache のパフォーマンスに関する監視
  - AWS SQS センサー – パフォーマンスとワークロードのパラメーターを監視して、キューの過負荷を回避し、多数の空の受信を検出
  - Azure API Management Services センサー – リクエストや使用率などの API メトリックに関する情報を提供
  - Azure CosmosDB センサー – サービスの可用性を監視し、可用性が低下したときにユーザーに警告
  - Azure Cost センサー – 予算の使用と Azure リソースの使用にかかる推定コストを監視
  - Azure Insights コンポーネントリソースセンサー – 分析ツールを提供するとともにパフォーマンスの異常を検出することで、ユーザーのライブアプリケーションを監視
  - Azure Kubernetes Cluster センサー – 管理対象クラスターのメトリックを収集して、ユーザーに通知
  - Azure Load Balancer センサー – バックエンドリソースやサーバーのグループ全体に負荷（受信ネットワークトラフィック）を均等に分散するのに役立ちます
  - Azure Logic Apps センサー – AzureLogicApps と呼ばれる Microsoft クラウドテクノロジーのパフォーマンスと動作を監視
  - Azure SQL DB センサー – Azure SQL DB で管理されているデータベースのパフォーマンスと動作を監視
  - Azure Server Farm センサー – Azure Monitor メトリックを使用して、Azure Server Farm リソースを監視
  - Azure Service Bus センサー – ServiceBus 名前空間に接続されているクラウド

アプリのメトリックを監視
・Azure Storage Account センサー – 潜在的なサービスの問題を検出し、コスト関連のサービスの使用状況を監視
・Azure Website センサー – AzureWebApps を使用してクラウドにデプロイされた Web アプリケーションの使用状況とパフォーマンスを監視
・デバイス構成センサー – Telnet または SSH プロトコルを使用したデバイス構成の監視とバックアップ
・Gitlab クラウドセンサー – GitLab クラウドリポジトリ内の特定のプロジェクトの最新のビルド/ジョブのステータスを監視
・Google Analytics Metrics センサー – Google Analytics ReportingAPIv4 と OAuth2 を使用して GoogleAnalytics ビューのいくつかの指標を監視
・Google Analytics のユーザーとセッションセンサー – GoogleAnalytics ダッシュボードに基づいてユーザーとセッションに関連する指標を測定
・Google ドライブセンサー – Google API と OAuth2 を使用して、Google ドライブの無料ストレージとゴミ箱のサイズを監視
・HPE 3PAR StoreServ センサー – ストレージオブジェクトの状態と使用率の統計を監視
・Microsoft365 サービスステータスセンサー – Microsoft 365 サービスの状態を監視し、一部のサービスが劣化または中断された状態にある場合に警告
・Microsoft クラウドアプリケーション – OneDrive センサー – OneDrive API を使用して OneDrive ストレージの使用状況を監視、承認のために OAuth2 を監視
・NetApp ONTAP センサー – NetApp ストレージコンポーネントの状態とパフォーマンスを監視
・NetApp SANtricity センサー – ストレージのポーリング、ボリューム、コントローラー、ドライブの現在のステータスなどの様々なパフォーマンスメトリックを収集、確認
・Palo Alto Firewall センサー – PaloAlto デバイスに構成された IPSec サイト間 VPN トンネルを監視
・SSL 関連のセンサー – NetCrunch が使用する Mozilla 証明書パッケージにデフォルトで含まれていない追加のルート証明書を許可します
・SSL 関連のセンサー – 指定したフォルダにカスタム証明書を追加できます
・Veeam Backup＆Replication – バックアップリポジトリの容量を監視し、リポジトリの使用可能なスペースが少ないかどうかをユーザーに通知
・Windows Hardware センサー – 構成の変更を追跡し、特定の変更をユーザーに通知
※古いインベントリモジュールの部分的な交換となります
・Zoom Account センサー – Zoom Account の実際の構成設定を読み取り、構成の変更を監視
・Zoom Operation Logs センサー – 毎月のアカウント全体で Zoom サービスの使用について確認できます
・Zoom Plans Usage センサー – 使用状況を監視
・Zoom Status センサー – Zoom サービスのステータスを監視

■ 以下の監視パックの追加、修正
・MeinbergLANTIME (SNMP)

・Atlantis ILIO (SNMP)
・Kentix
・Ruckus SmartZone (SNMP)
・Ruckus ZoneDirector (SNMP)
・Stormshield (SNMP)
・Eltek(SNMP) – バッテリー、ファン、整流器をチェックし、電圧、電流、温度に関する情報を収集
・GUDE Expert PDU Energy 8341 シリーズ(SNMP) – 凝縮の可能性や温度/湿度の変動などの環境問題について通知
・Hillstone Firewall(SNMP) – HillstoneFirewall からの複数のメトリックを監視します。IPSec 攻撃は、オンラインユーザー、ドロップされたパケットをカウント
・Hillstone Firewall – System (SNMP) – HA、ファン、電源に問題がある場合にアラームを発し、メモリ、CPU、アクティブなセッションの使用状況を通知
・APCATS(SNMP) – 入力/出力の周波数、電圧、電流、電力を監視
・APCNetBotzRack Monitor(SNMP) – 煙探知、温度が高すぎるなど、複数のイベントが発生したときに通知
・AVG Antivirus
・AVG Internet Security
・Adaware Antivirus
・Adaware Total Security
・AsustorDisk(SNMP) – 空き容量とディスク温度を監視
・AsustorSystem(SNMP) – プロセッサとメモリの使用率を確認します。システムと CPU の温度、ファン、およびネットワークに関する情報を収集
・AsustorUPS(SNMP) – バッテリーの状態、充電レベル、電圧を監視
・Avast Premium Security
・Axis Video(SNMP) – 障害やその他の望ましくないイベントについて警告
・BitDefender
・BitDefender Parental Control
・BullGuard Antivirus
・BullGuard Internet Security
・BullGuard Premium Protection
・Carel(SNMP) – 複数のメトリック(温度、ファン、湿度など)を監視
・Cisco UCS – PSU and Fan (SNMP) – ファン、ファンモジュール、PSU のステータスを確認
・Citrix Netscaler(SNMP) – CPU /メモリの使用量が多すぎるか、サーバー/クライアント接続が多すぎる場合にアラート
・Comodo Antivirus and Internet Security
・Comodo Endpoint Protection
・ESET
・Exchange 2016 – メールボックスマルチロールサーバーの主要な Windows サービスとパフォーマンスカウンターを監視
・F-Secure
・G Data Antivirus

・G Data Internet Security
・G Data Total Security
・Janitza – 電圧、電流、周波数の測定値を監視し、有効/無効エネルギー、実電力/無効電力などのデータを収集
・Kaspersky Endpoint Security
・Kaspersky Home Products
・Kaspersky Security Center
・Kaspersky Small Office Security
・Linux – CPU(SNMP) – CPU 負荷を監視
・Linux – ディスク(SNMP) – ディスクユーティリティを監視
・Linux – メモリ(SNMP) – システムのメモリ使用率を監視
・Malwarebytes
・McAfee Total Protection
・Nasuni Filer – 統計(SNMP) – 送受信されたビット/秒、キャッシュ、接続されたクライアントの数を監視
・Nasuni ファイラー – システムヘルス(SNMP) – 更新、ライセンスの使用状況、温度、電源からのエラー、RAID を監視
・Nasuni Filer – ボリューム(SNMP) – ウイルス対策ポリシーの違反と状態について通知、ボリューム状態を監視
・Norton
・Panda Dome
・Pingdom
・Ruckus – システムヘルス(SNMP) – メモリ使用率または CPU 使用率が高いときにアラートを出します。サービスが無効になったときに通知
・SocomecModulysUPS(SNMP)は、環境、バッテリー、UPS の問題について通知、入力フェーズと出力フェーズを監視
・SocomecUPS(SNMP) – 入力/出力電流、周波数、電圧に関するデータを収集、バッテリーの問題について通知
・Sophos Endpoint Protection
・Sophos Home
・Trend Micro
・Tycon – 4 つのオンボードリレーの電圧と電流、デバイスの内部および外部温度を監視
・VIPRE
・Veritas Backup Exec Agent – 主要な Veritas Backup Exec Agent Windows サービスを監視
・Veritas Backup Exec Events – 特定の Veritas Backup Exec Windows イベントログイベントを監視
・Veritas Backup Exec Server – 主要な Veritas Backup Exec Server の Windows サービスを監視
・Veritas NetBackup Client – 主要な Veritas NetBackup Exec クライアントの Windows サービスを監視
・Veritas NetBackup Server – 主要な Veritas Backup Exec エージェントの Windows サービスを監視

・Webroot SecureAnywhere
・Windows Defender (2016-2019)
・ZoneAlarm
・eScan
・pfSense (SNMP) – ファイアウォールのパケットレートに関する統計を収集し、ドロップされたパケット数を監視
・Cybernetics iSAN Series Storage (SNMP) – CPU またはシャーシの温度が高いときにアラートを発生します。ディスク、電源、アレイの問題についても通知

- レポートジェネレーターが閉じられていない場合、システムリソースが枯渇する問題を修正
- **変更された主な機能**
  ・NetCrunch に内包されているコンパイル済み MIB 情報のソースデータ(MIB 定義のテキストファイル)が削除
  ※該当の MIB 定義を編集・再コンパイルする際には,、製造元サイトから[MIB Database Sources]ファイルをダウンロードし、インストールいただく必要があります。
- **削除された主な機能**
  ・IP ネットワークマップの[マップ]タブの削除
  ※V11 以前で[編集済みカスタムマップ]を使用している場合は引き続きご利用可能です。
  ・パフォーマンスビューの削除
  ※グラフィカルビューにより再作成が必要となります
  ・ノードの一覧のエクスポート
  ・Windows 機器のインベントリ機能の削除
  ※Windows ハードウェアコンフィグセンサーより代替可能です。
  ・ルーティングマップの外観オプションの削除
  ・Windows Server 2012R2 及び 8.1 へのインストール
  ・非推奨のアンチウイルスソフトウェアに関連する 44 個の古い監視パック

3. 既知の問題

NetCrunch 12 での既知の問題について記載いたします。

3.1. その他

- Web アクセスを行った場合、マップを表示した際にレイアウトが崩れて表示される。
  回避方法:一度マップの[ノード]→[詳細]タブなどを表示したのち、再度[マップ]タブを表示する。
- WMI ツールのイベントログや、Windows イベントログ監視イベントで発生したイベントログのパラメータに表示される発生時刻が間違っている。
- SNMP プロフィールに SNMPv1 を使用した場合、値を収集できないことがある。
  回避方法:SNMPv2 を使用する。

4. よくある質問

NetCrunch について、よくある質問について記載いたします。

4.1. よくある質問および回答

- ノードの設定の[DNS 名]欄に日本語を使用できない。
  回答:バージョン 8 より仕様変更のため、使用できなくなりました。ファイルからノードの挿入を用いた場合やバージョンアップを行った場合、DNS 名に日本語を使用している場合、プロパティの変更を行うことができません。

- バージョン 6 からのアップグレード後、アラートのメールの件名に DNS 名が表示されない。
  回答:バージョン 7 より、イベントログの表示情報の仕様が変更されております。これにともない、デフォルトでメールのメッセージ定義に使用されている「$Common.AlertInfo」に含まれる情報が変更されました。DNS 名を表示するパラメータとして「$Properties.DisplayName」がございますので、メッセージ定義にこのパラメータの挿入をご試行ください。
  メッセージ定義の編集方法について、以下に例示いたします。
  1. メインメニュー→[監視]→[アラートメッセージ形式]を選択します。
  2. [アラートメッセージ形式]ウィンドウにて[メッセージ形式]を選択します。
  3. [email-txt]または[email]を選択します。
  4. 編集したいメッセージ定義に[パラメータの追加]からパラメータを挿入し、保存します。

- Admin のパスワードが分からない。
  回答:Admin のパスワードが分からない場合、nccli.exe を使用してパスワードをリセットすることができます。nccli.exe は、NetCrunch のインストールフォルダ内に用意されています。
  以下に手順を記載いたします。
  1. NetCrunch 搭載サーバーのコマンドプロンプトにて、以下のコマンドを実行します。
     nccli.exe reset-admin-password
  2. コンソールを起動すると、ユーザー名とパスワードの入力画面が表示されます。ユーザー名に Admin、パスワードは空欄に設定の上、[OK]をクリックします。
  3. [NetCrunch パスワードの変更]ウィンドウにて Admin のパスワードを設定の上、[OK]をクリックします。

■ NetCrunch から受信したメールが文字化けする。

回答:NetCrunch では、テキスト形式のメールの文字コードが「UTF-8」に設定されております。また、メールのヘッダー内に「MINE-Version:1.0」という表記が存在しないため、メーラーによっては MINE 形式と認識できず、文字化けする場合がございます。テキスト形式のメールが文字化けする場合、メーラー側で受信したメールを「UTF-8」で表示するか、NetCrunch が送信するメールを HTML 形式に変更することをご検討ください。

■ Windows イベントログの監視が行えない。

回答:NetCrunch のサービスの 1 つに、AdRem NetCrunch Server というサービスがございます。このサービスの起動ユーザーは、通常、ローカルシステムアカウントになっております。起動ユーザーがローカルシステムアカウントの場合、環境によっては、Windows イベントログの監視が行えない場合がございます。この事象を解消するには、起動ユーザーを変更する必要がございます。
以下に手順を記載いたします。
※Windows の操作については、OS や表示方法によって異なります。

1. NetCrunch のコンソールおよびコネクションブローカーを終了します。
2. Windows のスタートメニューから、[NetCrunch サーバーの停止]を選択します。
3. Windows のタスクマネージャーの[プロセス]タブにて、「AdRem NetCrunch Server」または「NCServer.exe」が存在しないことを確認します。
4. Windows のスタートメニューから、[コントロールパネル]→[管理ツール]→[サービス]を選択し、サービスツールを起動します。
5. [サービス]ウィンドウ上にて、[AdRem NetCrunch Server]を右クリックし、[プロパティ]を開きます。
6. [AdRem NetCrunch Server のプロパティ]ウィンドウの[ログオン]タブにて、[アカウント]を選択し、[アカウント]と[パスワード]を設定します。[アカウント]は、[参照]ボタンから設定を行います。
   ※Administrators 権限のローカルユーザーまたは NetCrunch の Windows 監視ドキュメントの条件を満たしたドメインユーザーを設定します。
7. Windows のスタートメニューから、[NetCrunch サーバーの開始]を選択します。
8. Windows のタスクマネージャーの[プロセス]タブにて、「AdRem NetCrunch Server」または「NCServer.exe」が存在することを確認します。
9. NetCrunch のコンソールを起動します。
10. 監視対象の Windows ノードを右クリック→[ノードの設定]を選択します。
11. 新しく開いたウィンドウの[監視]タブの[Windows]の項目の右側にある歯車のアイコンをクリックします。

12. [Windows]ウィンドウの[認証プロフィール]の項目で[編集]をクリックします。
13. [認証プロフィール]ウィンドウにて、[ユーザー名]と[パスワード]を設定します。すでに[ユーザー名]などが設定されている場合は、設定をいったん消去し、再度設定します。
14. [OK]をクリックし、各ウィンドウを閉じます。

※手順[10.]から[14.]は、各 Windows ノードに対して設定する必要がございます。
※AdRem NetCrunch Server の起動ユーザーの変更後、監視問題が発生する場合がございます。手順[14.]まで実施いただき、各 Windows ノードの認証プロフィールの設定後、監視間隔以上の時間監視問題が解消されない場合は、弊社サポートセンターまでお問い合わせください。

■ CSV ファイルからノードを追加する際、名前を設定して追加した。当初はノードのキャプションにはホスト名が表示されていたが、いつの間にか名前の表示が消えていた。
回答:CSV ファイルから追加したノードの名前が名前解決できないものである場合、ノードの設定にある[DNS 名]欄に名前が反映されません。この場合、[DNS 名]欄が空欄となり、空欄のまま設定を保存しますと、ノードのキャプションに表示されていた名前が削除されます。ノードの設定を編集する際には、[DNS 名]欄を再設定していただく必要がございます。
[DNS 名]欄を使用する以外にノードに名前を設定する方法としては、[表示名]欄とフィールドを使用する方法が考えられます。[表示名]欄を設定しますと、任意の名前をノードのキャプションに反映することができます。また、フィールドに設定することで、メール通知などのメッセージのパラメータを使用することができます。

■ トレンドデータ、イベントデータのテキスト出力方法が解らない。
回答: トレンドデータ、イベントデータをエクスポートする場合、nccli.exe を使用してエクスポートすることができます。nccli.exe は、NetCrunch のインストールフォルダ内に用意されています。
※バージョン 12 ではタイムゾーンが UTC を採用されております。そのため、JST - 9 時間の時間が表示されております。

以下に使用方法の例を記載いたします

nccli.exe export-trend -node <node> -counter <counter> -from <fromDate> [-to <toDate>]
パフォーマンスデータを CSV ファイルにエクスポートできます。

コマンドパラメータ (export-trend):

オプション	説明
-node	ノード名、アドレス ID
-counter	カウンタパス。

	例:Processor(_Total)¥% Processor Time
-from	開始日。 例: 01/31/2022 or 2022-01-31
[-to]	終了日 (オプション). パラメータが指定されていない場合、プログラムは 1 日のデータのみをエクスポートします。
[-file]	出力ファイル名 (フルパス)。 デフォルト <アトラスデータフォルダ>¥TrendExport

nccli.exe export-events -node <node> -from <fromDate> [-to <toDate>] [-file <fileName>] [-output <dataFormat>]
イベントデータを CSV または JSONL ファイルにエクスポートできます。CSV ファイルはフラット形式であり、イベントパラメータを含めることはできません。

:

コマンドパラメータ(export-events)

オプション	説明
-node	ノード名、アドレス、ID
-from	開始日。 例: 01/01/2022 or 2022-01-01
[-to]	終了日 (オプション). パラメータが指定されていない場合、プログラムは 1 日のデータのみをエクスポートします。
[-file]	出力ファイル名 (フルパス)。 デフォルト <アトラスデータフォルダ>¥TrendExport
[-output]	出力データ形式。 CSV(デフォルト)または JSONL。 プログラムは、イベントパラメータを JSONL 形式にのみエクスポートできます。