



はじめに

この章は、次の項で構成されています。

- [今回のリリースでの新機能](#) (1 ページ)
- [AsyncOS 12.0 と以前のリリースでの Web インターフェイスの比較](#) (9 ページ)
- [Cisco コンテンツ セキュリティ管理の概要](#) (15 ページ)

今回のリリースでの新機能

ここでは、AsyncOS for Cisco Content Security Management のこのリリースにおける新機能と拡張機能について説明します。

表 1: AsyncOS 12.0 の新機能

機能	説明
レポート、隔離、およびトラッキングのための新しい Web インターフェイス	

機能	説明
	<p>アプライアンスには、現在、次を検索および表示するための新しい Web インターフェイスがあります。</p> <ul style="list-style-type: none"> • 電子メール レポート。次のカテゴリに基づいて [レポート (Reports)] ドロップダウンから電子メール レポートを表示できます。 <ul style="list-style-type: none"> • 電子メール脅威のレポート • ファイルおよびマルウェアのレポート • 接続およびフローのレポート • ユーザ レポート • フィルタのレポート <p>詳細については、「中央集中型の電子メールセキュリティ レポートの使用」の章を参照してください。</p> <ul style="list-style-type: none"> • スパム隔離 <ul style="list-style-type: none"> • スпамやスパムの疑いがあるメッセージを、Web インターフェイス ページの [隔離 (Quarantine)] > [スパム隔離 (Spam Quarantine)] > [検索 (Search)] で表示および検索できるようになりました。 • セーフリストやブロックリストに追加されたドメインを、Web インターフェイスの [隔離 (Quarantine)] > [スパム隔離 (Spam Quarantine)] > [セーフリスト (Safelist)] または [ブロックリスト (Blocklist)] ページで表示、追加、および検索できます。 <p>詳細については、「スパム隔離」の章を参照してください。</p> <ul style="list-style-type: none"> • ポリシー、ウイルスおよびアウトブレイク隔離。ポリシー隔離、ウイルス隔離、およびアウトブレイク隔離は、Web インターフェイスの [隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [検索 (Search)] ページで表示および検索できます。詳細については、「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の章を参照してください。 • メッセージトラッキング。メッセージまたはメッセージのグループは、検索条件に応じて Web インターフェイスの [トラッキング (Tracking)] > [検索 (Search)] ページから検索できます。詳細については、「メッセージのトラッキング」の章を参照してください。 <p>重要 • アプライアンスで AsyncOS API が有効になっているこ</p>

機能	説明
	<p>とを確認してください。</p> <ul style="list-style-type: none"> デフォルトで、<code>trailblazerconfig</code> はアプライアンスで有効になっています。 <ul style="list-style-type: none"> 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。 また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。 <code>trailblazerconfig</code> が無効になっている場合は、[管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] で設定された AsyncOS API ポートがファイアウォールで開きます。デフォルトの AsyncOS API HTTP/HTTPS ポートは 6080/6443 です。
<code>trailblazerconfig</code> CLI コマンド	<p><code>trailblazerconfig</code> コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。</p> <p>(注) デフォルトで、<code>trailblazerconfig</code> の CLI コマンドはアプライアンスで有効になっています。<code>help trailblazerconfig</code> コマンドを入力すると、インラインヘルプを参照できます。</p> <p>詳細については、trailblazerconfig コマンドを参照してください。</p>
アプライアンスでの機密情報の暗号化	<p>CLI で <code>adminaccessconfig > encryptconfig</code> サブコマンドを使用して、アプライアンスの機密情報の暗号化を設定できます。</p> <p>(注) デフォルトでは、暗号化はアプライアンス上で無効になっています。</p>
メッセージトラッキング機能拡張	<p>メッセージの「Reply To」ヘッダーに基づいてメッセージを検索できるようになりました。</p> <p>詳細については、メッセージのトラッキングを参照してください。</p>

機能	説明
AsyncOS 12.0 for Cisco Eメールセキュリティアプライアンスの新機能のサポート	<p>セキュリティ管理アプライアンスの [レポート (Reporting)] ページで、次のレポートを表示できるようになりました。</p> <ul style="list-style-type: none"> • 外部脅威フィード レポート • 送信者ドメインのレピュテーション レポート <p>詳細については、新しい Web インターフェイスの電子メール レポート ページの概要を参照してください。</p> <p>これで、DANE の成功および DANE 障害シナリオでの送信 TLS 接続の概要を表示できるようになりました。詳細については、<i>AsyncOS 12.0 for Cisco Email Security Appliances ユーザ ガイド</i> またはオンラインヘルプにある「SMTP DNS-based Authentication of Named Entities」セクションを参照してください。</p> <p>次のメッセージイベントを使用して、セキュリティ管理アプライアンスの [メッセージトラッキング (Message Tracking)] ページでメッセージを検索できるようになりました。</p> <ul style="list-style-type: none"> • 外部脅威フィード レポート • 送信者ドメインのレピュテーション レポート • DANE 障害

機能	説明
[高度なマルウェア防御 (Advanced Malware Protection)]レポートの拡張機能	<p>[高度なマルウェア防御 (Advanced Malware Protection)]レポートページには、次の拡張機能が追加されています</p> <ul style="list-style-type: none"> • 新しいセクション-[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)]セクションは、[カスタム検出 (Custom Detection)]に分類される、AMP for Endpoints コンソールから受信したブラックリスト ファイル SHA の割合を表示します。 <p>AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイルSHA の脅威名は、レポートの[着信マルウェア脅威ファイル (Incoming Malware Threat Files)]セクションで[シンプルカスタム検出 (Simple Custom Detection)]として表示されます。</p> <ul style="list-style-type: none"> • 新しいセクション-[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)]セクションは、[カスタム検出 (Custom Detection)]に分類されるしきい値設定を基にしてブラックリスト ファイル SHA の割合を表示します。 • レポートの[詳細 (More Details)]セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブラックリスト追加ファイル SHA のファイル トラジェクトリ詳細を表示できます。 • 新しい判定 - ファイルの分析後に、ファイルに動的なコンテンツが存在しないときの新しい判定[低リスク (Low Risk)]が導入されました。判定の詳細は、レポートの[AMPにより渡された受信ファイル (Incoming Files Handed by AMP)]セクションに表示されます。 <p>「[高度なマルウェア防御 (Advanced Malware Protection)]ページ」を参照してください。</p>

機能	説明
Web レポートおよびトラッキングのための新しい Web インターフェイス	<p>アプライアンスには、現在、次を検索および表示するための新しい Web インターフェイスがあります。</p> <ul style="list-style-type: none"> • Web レポート <p>次のカテゴリに基づいて [レポート (Reports)] ドロップダウンから Web ベースのレポートを表示できるようになりました。</p> <ul style="list-style-type: none"> • 一般的なレポート • 脅威レポート <ul style="list-style-type: none"> • [Web トラッキング (Web Tracking)] <p>検索条件に応じて Web トランザクションを検索できます。セキュリティ管理アプライアンスで、[Web] ドロップダウンをクリックし、[トラッキング (Tracking)]>[Web トラッキングの検索 (Web Tracking Search)] ページを選択します。</p> <p>重要</p> <ul style="list-style-type: none"> • アプライアンスで AsyncOS API が有効になっていることを確認してください。 • デフォルトで、trailblazerconfig はアプライアンスで有効になっています。 <ul style="list-style-type: none"> • 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。 • また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。 • trailblazerconfig が無効になっている場合は、[管理アプライアンス (Management Appliance)]>[ネットワーク (Network)]>[IP インターフェイス (IP Interfaces)] で設定された AsyncOS API ポートがファイアウォールで開きます。デフォルトの AsyncOS API HTTP/HTTPS ポートは 6080/6443 です。 <p>詳細については、「中央集中型 Web レポートおよびトラッキングの使用」の章を参照してください。</p>


機能	説明
メトリックバー ウィジェット	<p>[メトリックバー (Metrics Bar)]ウィジェットを使用すると、[高度なマルウェア防御 (Advanced Malware Protection)]レポート ページで Cisco Threat Grid アプライアンスによって実行されるファイル分析のリアルタイム データを確認できます。</p> <p>詳細については、[高度なマルウェア防御 (Advanced Malware Protection)] ページを参照してください。</p>
[HTTPSレポート (HTTPS Reports)] ページ	<p>[HTTPSレポート (HTTPS Reports)]レポート ページの各 HTTP/HTTPS トラフィックのクライアント側とサーバ側の接続に基づいて、HTTP/HTTPS トラフィックの総合計と暗号のサマリーを確認できます。</p> <p>詳細については、中央集中型 Web レポートおよびトラッキングの使用を参照してください。</p>
スマート ソフトウェア ライセンシングのサポート	<p>スマート ソフトウェア ライセンシングを使用すると、Cisco Email Security Appliance のライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager (CSSM) でアプライアンスを登録する必要があります。CSSMは、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。</p> <p>注意 アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ライセンシングモードにロールバックすることができなくなります。</p> <p>詳細については、スマート ソフトウェア ライセンシングを参照してください。</p>
Cisco Threat Response ポータルへのアプライアンスの統合	<p>Cisco Threat Response ポータルにアプライアンスを統合すると、Cisco Threat Response ポータルで次のアクションを実行することができます。</p> <ul style="list-style-type: none"> • 組織内の複数のアプライアンスからメッセージ トラッキングのデータを確認します。 • メッセージ トラッキングで検出された脅威を特定、調査、および修正します。 • 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。 • ポータルで脅威をドキュメント化して調査を保存し、ポータル内の他のデバイス間で情報を共有します。 <p>詳細については、ネットワークと IP アドレスの割り当てを参照してください。</p>



機能	説明
Web トラフィック タップ ポリシー	<p>Cisco コンテンツ セキュリティ管理 アプライアンスでは、現在、Web トラフィック タップ ポリシーを設定できます。Web トラフィック タップ ポリシーは、Web セキュリティ アプライアンスを通過するなどの Web トラフィックをタップするかに基づいて、定義できます。</p> <p>セキュリティ管理 アプライアンスで Web トラフィック タップ ポリシーを設定するには、Web セキュリティ アプライアンスで Web トラフィック タップ機能を有効にする必要があります。</p> <p>[Web 概要 (Web Overview)] レポート ページには、[Web トラフィック タップのステータス (Web Traffic Tap Status)]、[Web トラフィック タップのサマリー (Web Traffic Tap Summary)]、[タップされた HTTP/HTTPS トラフィック (Tapped HTTP/HTTPS Traffic)]、および [タップされたトラフィックのサマリー (Tapped Traffic Summary)] のセクションが含まれるようになりました。Web レポートの概要を参照してください。</p>
Cisco Web セキュリティ アプライアンス 用 AsyncOS での Office 365 Web サービス外部 URL カテゴリ機能のサポート	<p>このリリースでは、Cisco Web セキュリティ アプライアンス 用 AsyncOS での Office 365 Web サービス外部 URL カテゴリ機能をサポートします。</p> <p>詳細については、中央集中型 Web レポートおよびトラッキングの使用を参照してください。</p>




AysncOS 12.0 と以前のリリースでの Web インターフェイスの比較

次の表は、新しい Web インターフェイスの以前のバージョンとの比較を示しています。

表 2: 新しい Web インターフェイスの以前のリリースとの比較


Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
Web インターフェイスへのアクセス	セキュリティ管理 アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。詳細については、 レガシー Web インターフェイスへのアクセス を参照してください。	-

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディング ページ	セキュリティ管理アプライアンスにログインすると、[メールフロー概要 (Mail Flow Summary)] ページが表示されます。	アプライアンスにログインすると、[システムステータス (System Status)] ページが表示されます。
製品ドロップダウン	[製品 (Product)] ドロップダウンで、E メールセキュリティアプライアンスと Web セキュリティアプライアンスを切り替えることができます。 詳細については、 インタラクティブレポートページの使用 を参照してください。	[電子メール (Email)] または [ウェブ (Web)] タブを使用して、E メールセキュリティアプライアンスと Web セキュリティアプライアンスを切り替えることができます。
レポートドロップダウン	[レポート (Reports)] ドロップダウンで、E メールセキュリティアプライアンスと Web セキュリティアプライアンスのレポートを表示できます。 詳細については、 インタラクティブレポートページの使用 を参照してください。	[レポート (Reporting)] ドロップダウンメニューで、E メールセキュリティアプライアンスと Web セキュリティアプライアンスのレポートを表示できます。
管理アプライアンスタブ	セキュリティ管理アプライアンスで  をクリックして、[管理アプライアンス (Management Appliance)] タブにアクセスします。	レポート、メッセージトラッキング、隔離の有効化と設定、ネットワークアクセスの設定、およびシステムステータスの監視を実行できます。
マイレポートページ	セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [レポート (Reporting)] > [マイレポート (My Reports)] を選択し、[マイレポート (My Reports)] ページにアクセスします。	既存のレポート ページのチャート (グラフ) と表を組み合わせて、レポートダッシュボードをカスタマイズできます。

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
有効なレポートデータページ	セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [レポート (Reporting)] > [有効なレポートデータ (Reporting Data Availability)] を選択し、[有効なレポートデータ (Reporting Data Availability)] ページにアクセスします。	データを表示、更新およびソートして、リソース使用率と電子メールトラフィックの問題点に対するリアルタイムの可視性を提供できます。
レポートのスケジュール設定とアーカイブ	セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] を選択し、レポートをスケジュールします。 セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archive Reports)] を選択し、レポートをアーカイブします。	セキュリティ管理アプライアンスで、[メール (Email)] > [レポート (Reporting)] > [スケジュールされたレポート (Scheduled Reports)] ページを使用してレポートをスケジュールすることができ、[メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archived Report)] ページを使用してレポートをアーカイブすることができます。
レポートの概要ページ	セキュリティ管理アプライアンスの [メール レポートの概要 (Email Reporting Overview)] ページの新しい Web インターフェイスが、[メールフロー概要 (Mail Flow Summary)] ページとして設計し直されました。[メールフロー概要 (Mail Flow Summary)] レポートページには、受信および送信メッセージに関する傾向グラフや要約テーブルが表示されます。	セキュリティ管理アプライアンスの [メール レポートの概要 (Email Reporting Overview)] ページに、お使いの E メールセキュリティアプライアンスからのメールメッセージアクティビティの概要が表示されます。[概要 (Overview)] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
高度なマルウェア防御レポートページ	<p>[レポート (Reports)]メニューの[高度なマルウェア防御 (Advanced Malware Protection)]レポートページでは、次のセクションを使用できます。</p> <ul style="list-style-type: none"> • [概要 (Overview)] • [AMP ファイル レピュテーション (AMP File Reputation)] • [ファイル分析 (File Analysis)] • [ファイル レトロスペクション (File Retrospection)] • [メールボックスの自動修復 (Mailbox Auto Remediation)] 	<p>セキュリティ管理アプリケーションの[メール (Email)]>[レポート (Reporting)]ドロップダウンメニューには次の[高度なマルウェア防御 (Advanced Malware Protection)]レポート ページがあります。</p> <ul style="list-style-type: none"> • [高度なマルウェア防御 (Advanced Malware Protection)] • [AMP ファイル分析 (AMP File Analysis)] • [AMP判定のアップデート (AMP Verdict Updates)] • [メールボックスの自動修復 (Mailbox Auto Remediation)]
アウトブレイクフィルタ ページ	<p>新しい Web インターフェイスの[アウトブレイク フィルタリング (Outbreak Filtering)]レポートページでは、[過去 1 年間のウイルスアウトブレイク (Past Year Virus Outbreaks)]および[過去 1 年間のウイルスアウトブレイクの概要 (Past Year Virus Outbreak Summary)]を使用できません。</p>	<p>[メール (Email)]>[レポート (Reporting)]>[アウトブレイクフィルタ (Outbreak Filters)]ページには、[過去 1 年間のウイルスアウトブレイク (Past Year Virus Outbreaks)]および[過去 1 年間のウイルスアウトブレイクの概要 (Past Year Virus Outbreak Summary)]が表示されます。</p>

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
スパム隔離 (管理ユーザおよびエンドユーザ)	<p>新しい Web インターフェイスで [隔離 (Quarantine)] > [スパム隔離 (Spam Quarantine)] > [検索 (Search)] をクリックします。</p> <p>エンドユーザは、URL (<a href="https://example.com:<https-api-port>/eq-login">https://example.com:<https-api-port>/eq-login) を使用してスパム隔離にアクセスできます。</p> <p>example.com はアプライアンスホスト名で、<https-api-port> はファイアウォールで開いている AsyncOS API HTTPS ポートです。</p>	-
ポリシー、ウイルスおよびアウトブレイク隔離	<p>新しい Web インターフェイスで [隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] をクリックします。</p> <p>新しい Web インターフェイスでは、[ポリシー、ウイルス、およびアウトブレイク隔離 (Policy, Virus and Outbreak Quarantines)] のみを表示できます。</p>	アプライアンスでは、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。
隔離内のメッセージに対するすべてのアクションの選択	複数 (またはすべて) のメッセージを選択し、削除、遅延、リリース、移動などのメッセージアクションを実行できます。	複数のメッセージを選択して、メッセージアクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
拒否された接続	拒否された接続を検索するには、セキュリティ管理アプリケーションで、[トラッキング (Tracking)] > [検索 (Search)] > [拒否された接続 (Rejected Connection)] タブをクリックします。	-
クエリ設定	セキュリティ管理アプリケーションでは、メッセージトラッキング機能の [クエリ設定 (Query Settings)] フィールドは使用できません。	メッセージトラッキング機能の [クエリ設定 (Query Settings)] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージトラッキングデータ	セキュリティ管理アプリケーションで  をクリックして、[メール (Email)] > [メッセージトラッキング (Message Tracking)] > [有効なメッセージトラッキングデータ (Message Tracking Data Availability)] を選択し、[有効なメッセージトラッキングデータ (Message Tracking Data Availability)] ページにアクセスします。	アプリケーションの欠落データインターバルを表示することができます。
メッセージの追加詳細の表示	[判定チャート (Verdict Charts)]、[最後の状態 (Last State)]、[送信者グループ (Sender Groups)]、[送信者 IP (Sender IP)]、[SBRIS スコア (SBRIS Scor)]、[ポリシー一致 (Policy Match)] の詳細など、メッセージの追加の詳細を表示できます。	-

Web インターフェイス ページ または要素	新しい Web インターフェイス	レガシー Web インターフェイス
判定チャートと最後の状態の判定	判定チャートに、アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	メッセージの添付ファイルとホスト名は、セキュリティ管理アプライアンスのメッセージの [メッセージの詳細 (Message Details)] セクションには表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細 (Message Details)] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、SBRIS スコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、SBRIS スコア、およびポリシー一致の詳細は、セキュリティ管理アプライアンスの [メッセージの詳細 (Message Details)] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、SBRIS スコア、およびポリシー一致は、メッセージの [メッセージの詳細 (Message Details)] セクションには表示されません。
メッセージの方向 (受信または送信)	メッセージの方向 (受信または送信) は、セキュリティ管理アプライアンスのメッセージトラッキング結果ページに表示されます。	メッセージの方向 (受信または送信) は、メッセージトラッキング結果ページには表示されません。

Cisco コンテンツ セキュリティ管理の概要

AsyncOS for Cisco Content Security Management には次の機能が統合されています。

- 外部スパム隔離：エンドユーザー向けのスパム メッセージおよび疑わしいスパム メッセージを保持しており、エンドユーザーおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 集約ポリシー (Centralized Policy)、ウイルス (Virus)、アウトブレイク隔離 (Outbreak Quarantines)：これらの隔離および隔離内に隔離されたメッセージを複数の E メールセ

セキュリティアプライアンスから管理するための単一のインターフェイスを提供します。隔離されたメッセージをファイアウォールの背後に保存できます。

- **中央集中型レポートिंग (Centralized reporting)** : 複数の E メールおよび Web セキュリティアプライアンスからの集約データに関するレポートを実行します。個別アプライアンスで使用できる同じレポート機能を、セキュリティ管理アプライアンスでも使用できます。
- **中央集中型トラッキング (Centralized tracking)** : 単一のインターフェイスを使用して、メールメッセージを追跡すること、および複数の E メールおよび Web セキュリティアプライアンスにより処理された Web トランザクションを追跡することができます。
- **Web セキュリティアプライアンスの中央集中型構成管理 (Centralized Configuration Management for Web Security appliances)** : 簡易性および一貫性のため、複数の Web セキュリティアプライアンスを対象にポリシー定義とポリシー導入を管理します。



(注) 中央集中型の電子メール管理、または E メールセキュリティアプライアンスの「クラスタリング」にセキュリティ管理アプライアンスは含まれません。

- **中央集中型アップグレード管理 (Centralized Upgrade Management)** : 単一のセキュリティ管理アプライアンス (SMA) を使用して、複数の Web セキュリティアプライアンス (WSA) を同時にアップグレードできます。
- **データのバックアップ (Backup of data)** : レポートデータ、トラッキングデータ、隔離されたメッセージ、安全な送信者とブロックされた送信者のリストなど、セキュリティ管理アプライアンスのデータをバックアップします。

1 台のセキュリティ管理アプライアンスからのセキュリティ操作を調整することも、複数のアプライアンス間に負荷を分散させることもできます。