Solution overview

# WithSecure™ Cloud Protection **for Salesforce**

# 目次

# 1. 概要

WithSecure™ Cloud Protection for Salesforce は Salesforce プラットフォームが備えるネイティブなセキュリティ機能を補完するために設計された、クラウドベースのセキュリティソリューションです。

Salesforce との連携により、クラウドエコシステムでは一般的な Shared Responsibility（責任共有）モデルの下で、企業は以前よりも簡単にセキュリティの一部を担うことができます。WithSecure™ Cloud Protection は、システム全体のセキュリティ機能を補完し、企業のセキュリティ戦略をクラウドサービスに拡大するための優れた選択肢です。

WithSecure™ Cloud Protection for Salesforce は Salesforce の利便性を妨げることなく、Salesforce プラットフォームのユーザーが取り扱うファイル、URL、電子メールに由来するリスクを軽減するための、専用のセキュリティコンポーネントを提供します。またこのソリューションは、豊富なレポート、高度なセキュリティ分析、完全な監査証跡を提供し、インシデント対応を迅速かつ効率的に行ことができます。

Cloud Protection は、Salesforce とウィズセキュアの間でネイティブな Cloud-to-Cloud 統合を実現しており、セキュリティとリソースの面からも最適な選択肢です。

まず、サーバーやプロキシなどのミドルウェアの導入や保守、ネットワーク構成の変更にリソースを割く必要がありません。

さらに、Salesforce はすべての通信で HTTPS 暗号化を使用するため、CASB（Cloud Access Security Broker）のようなプロキシを使用するソリューションでは途中で暗号化を解除しなければならず、システム全体のセキュリティ強度が低下し、脆弱性が発生しやすくなります。

また、緊密な統合の結果、Salesforce AppExchange による簡便な導入が可能です。導入はわずか数分で完了し、コストと時間のかかる IT 関連の作業は不要です。

**WithSecure™ Cloud Protection for Salesforce には、次のようなメリットがあります：**

**クラウドの保護：**クラウドエコシステムで使用される責任共有モデルの一部を担うための理想的なソリューションであり、企業のセキュリティ戦略をクラウドサービスにも拡張できます。

**次世代のセキュリティ：**リアルタイム脅威インテリジェンス、スマートクラウドサンドボックスなど、単純なウイルス対策製品以上の機能を提供します。

**高度な分析：**豊富なレポート、高度なセキュリティ分析、完全な監査証跡により、Salesforce のコンテンツを 360 度全方向から可視化し、迅速かつ効率的なインシデント対応を実現します。

**Salesforce との共同開発：**このソリューションは Salesforce と共同で設計・開発されており、シームレスな統合と信頼性、優れたユーザーエクスペリエンスを保証します。

**Cloud-to-Cloud アーキテクチャ：**Salesforce とウィズセキュアのクラウド同士を統合しているため、ミドルウェアの導入や高価な IT 作業は必要ありません。

このソリューションは、Salesforce AppExchange からトライアル利用とダウンロードが可能です。



# 2. ウィズセキュアについて

ウィズセキュアは、ランサムウェアへの日和見感染から高度なサイバー攻撃まで、30 年以上に渡ってあらゆるものから企業やユーザーを守ってきたサイバーセキュリティのリーディングカンパニーです。

ウィズセキュアは全世界に 1,700 人の従業員を擁し、30 ヵ所の拠点でグローバルに事業を展開し、年間 2 億 1,300 万ユーロの売上げを上げています。

ウィズセキュアは、他のどの企業よりも多くヨーロッパのサイバー犯罪調査に参画しており、お客様に最高のセキュリティを提供するために、70 以上の業界パートナーやインターポールのような国際的なセキュリティ当局と緊密に連携しています。

日々、何百万人ものユーザーがウィズセキュアのソリューションによって保護されています。ウィズセキュアは数千社におよぶ信頼性の高いチャネルパートナーに加え、ボーダフォン、テレフォニカ、ユニティメディアなどの大手通信事業者を含む 200 社もの通信事業者とのネットワークを通じて、世界中のお客様にサービスを提供しています。

競合他社よりも優れた保護を提供するウィズセキュアの能力は、独立した業界の専門家やアナリストによるテストにより、毎年のように証明されています。

ウィズセキュアは、AV-Testからベストプロテクション賞を 6 度受賞しています。AV-Test および AVComparatives から複数回「Best Protection」および「Top-Rated」賞を受賞していることは、ウィズセキュアの保護レベルが一貫していることを証明しています。

これらの厳しい基準を満たすために、ウィズセキュアのソリューションは、ヒューリスティック脅威分析や行動脅威分析、WithSecure™ Security Cloud を介して提供されるリアルタイムな脅威インテリジェンスなど、さまざまな先駆的な技術を活用して、セキュリティに多層的なアプローチを適用しています。

1988年に設立されたウィズセキュアは、NASDAQ OMX Helsinki Ltd.に上場しています。

# 3. SHARED RESPONSIBILITY（責任共有）モデル

クラウドエコシステムのセキュリティに関しては、クラウドサービスプロバイダとその顧客が責任を分担するのが一般的です。

たとえば Salesforce は、認証、ルール、ユーザー権限、ロールなど、システムおよびアプリケーションレベルのセキュリティのさまざまな側面をカバーします。

一方で、エンドユーザーが Salesforce プラットフォームにアップロードしたファイルやリンクのセキュリティを確保するのは、すべての組織の責任です。

しかし組織は、パートナーや顧客などの外部ユーザーが Salesforce クラウドで使用し共有するコンテンツの安全性、アイデンティティやアクセス制御対策などの全体的なセキュリティレベルを保証することはできません。

さらに、多くの組織ではファイアウォールやその他のネットワークセキュリティ機能を介してクラウドアプリケーションへの直接アクセスを提供しているため、マルウェアやランサムウェア、悪意のあるリンクからの保護は、全面的にエンドポイントに委ねられていることが多いのです。

## Salesforce Cloud

### アプリケーションサービス

| | | | | |
|---|---|---|---|---|
| アイデンティティ シングルサインオン | パスワードポリシー | 2 要素認証 | ユーザーロール パーミッション | フィールド/Row Level セキュリティ |

### ネットワークサービス

| | | | | |
|---|---|---|---|---|
| HTTPS 暗号化 | ペネトレーションテスト | 高度な脅威の検知 | セキュア ファイアウォール | IP ログイン制限 |

### インフラサービス

| | | | | |
|---|---|---|---|---|
| セキュアデータセンター | バックアップ/災害復旧 | リアルタイム レプリケーション | サードパーティ証明書 | 顧客監査 |

+

## WithSecure™ Cloud Protection

コンテンツ：ファイルおよびリンクの保護

| | | | | |
|---|---|---|---|---|
| 脅威インテリジェンス サービス | マルチエンジン アンチウイルス | スマートクラウド サンドボックス | レポート/監査サービス | セキュリティ解析 サービス |

そのため、これらのリスクを軽減するためのセキュリティ対策を追加する必要があります。例えば、組織は以下のような対策を行う必要があります。

- Salesforce の Service Cloud を利用し、サービス/カスタマーケアチームを経由して行われる標的型攻撃を防止
- 組織のコミュニティクラウドでポルノやランサムウェアなどの好ましくないコンテンツや悪意のあるコンテンツが共有され、組織に悪影響を与えることを防止
- Sales Cloud や Chatter などで共有された悪意のある添付ファイルが組織内で拡散することを防止

WithSecure™ Cloud Protection for Salesforce は、これらのリスクを防ぐために特別に設計されています。Salesforce が本来持っているネイティブなセキュリティ機能を専用のセキュリティコンポーネントで補完し、クラウドエコシステムで使用されている責任共有モデルが想定するセキュリティの一部を組織が担当できるようにします。

# 4. ソリューション概要

WithSecure™ Cloud Protection for Salesforceは、Salesforce プラットフォームのネイティブセキュリティ機能を補完するために設計された、クラウドベースのセキュリティソリューションです。ユーザーがアップロードしたファイルや URL によって引き起こされるリスクを軽減するために、専用のセキュリティコンポーネントを提供します。

このソリューションは、ほとんどの Salesforce Cloud をサポートします。これにはSales Cloud、Community Cloud、Service Cloud などが含まれますが、それらに限定されません。また、このソリューションは以下の Salesforce エディションをサポートします：Professional、Enterprise、UnlimitedおよびDeveloper

WithSecure™ Cloud Protection for Salesforce は Salesforce のさまざまなクラウドとの間で最大の互換性と信頼性を実現するために、Salesforce と緊密に協力して設計・開発されました。

このソリューションは Cloud-to-Cloud アーキテクチャを採用しているため、プロキシのようなミドルウェアの導入あるいは管理、ネットワーク構成の追加は必要ありません。AppExchange から簡単に導入することができます。

# 4.1 ファンクションダイアグラム

## 4.1.1 ファイル、URL、メール

WithSecure™ Cloud Protection は、Salesforce プラットフォームで使用されるすべてのファイル、リンク、および電子メールを常時監視します。

## 4.1.2 Salesforce Cloud

エンドユーザーが Salesforce を介してコンテンツを利用、アップロード、ダウンロードするたびに、トラフィックは WithSecure™ Security Cloud の特許取得済みの脅威分析および検知プロセスによって検査されます。

このソリューションは、ユーザーが感じる遅延を最小限に抑え、Salesforce の本来の使い勝手を維持できるように設計されています。

## 4.1.3 WithSecure™ Security Cloud

WithSecure™ Security Cloud は、コンテンツのリスクプロファイルに応じて段階的にコンテンツを分析する、多段階のコンテンツ分析を採用しています。さらに、高リスクであることが判明したファイルについては、ゼロデイマルウェア攻撃やその他の高度な脅威を防ぐために設計されたスマートクラウドサンドボックス技術による詳細な分析が行われます。

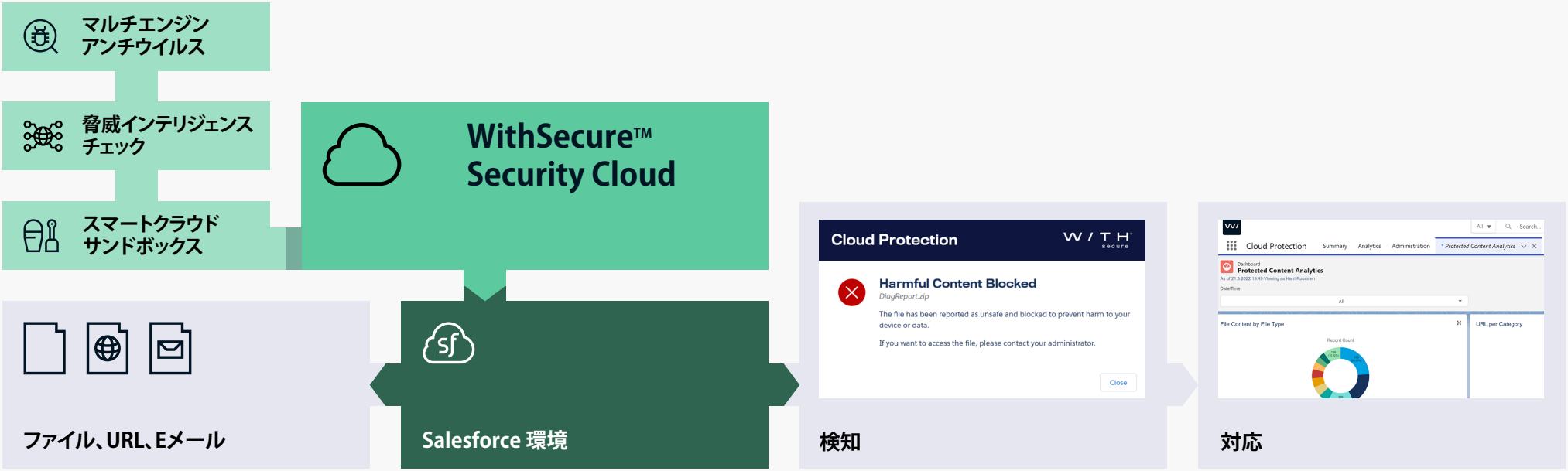
## 4.1.4 検知

有害または未許可と評価されたコンテンツは、自動的に削除またはブロックされます。エンドユーザーにはコンテンツがブロックされたことが通知され、次に何をすべきかがアドバイスされると共に、それ以上のアクセスはできなくなります。
そしてセキュリティアラートがソリューション管理者とセキュリティチームに送信されます。制限対象のコンテンツは、ファイルタイプや拡張子ごとにコンテンツフィルタリングポリシーで定義できます。例えば管理者は、.com、.exe、.bin、.bat などの実行ファイルをすべてブロックすることができます。

## 4.1.5 対応

システム管理者は、豊富なレポート、高度なセキュリティ分析、完全な監査証跡などにより、Salesforce を通じて発生した攻撃への対応や、未知の攻撃源からの攻撃の調査など、脅威への対応を容易に行うことができます。

以下は、このソリューションが Salesforce Cloud に補完的なセキュリティを提供するプロセスのハイレベルな概要です。



# 4.2 File Protection

WithSecure™ Cloud Protection は、ウイルス、トロイの木馬、ランサムウェア、その他の高度なマルウェアを検出してブロックするために、独自の多階層構造のセキュリティプラットフォームを採用しており、従来の技術と比較して、はるかに優れた保護を提供します：

- 広範囲に特徴、パターン、傾向を検出し、未知のマルウェアの亜種であっても、より信頼性の高い正確な検出を可能にします。
- 数千万ものセキュリティクライアントから収集したリアルタイムな脅威インテリジェンスを活用することで、新たに出現し急速に拡散する脅威に対し、迅速かつ優れた保護を提供します。
- エミュレーションにより、難読化技術を使ったマルウェアの検出を可能にします。

ウィズセキュアの特許取得済みのスキャンロジックと Salesforce プラットフォームとのシームレスな統合により、ユーザーがファイルをアップロードしたりダウンロードしたりする際に、透過的な脅威検知プロセスを確実に適用します。

## 4.2.1 Upload Protection

ユーザーが Chatter、Salesforce Files または Attachments にファイルをアップロードするたびに、多階層の分析プロセスがバックグラウンドで起動します：

**初期分析**

ファイルのチェックサム（SHA1）が計算され、ファイルの内容やメタデータとともに Salesforce Cloud 内の脅威検知キャッシュに保存されます。チェックサムは既存の脅威検知キャッシュに保存されているものと比較され、ファイルが以前に解析されたことがあるかどうかを確認します。これによりクラウドへのアクセスが減少し、ユーザーエクスペリエンスをさらに向上させることができます。脅威検知結果は定期的に更新され、期限切れの結果は自動的にクリアされるため、最新の情報を維持することができます。キャッシュから解析結果が利用可能な場合は、自動的にそれを使用します。

**脅威インテリジェンスチェック**

キャッシュに結果が見つからない場合は、SHA-1 チェックサムについて WithSecure™ Security Cloud を介して脅威インテリジェンスのチェックが行われます。このサービスはファイルの安全性評価、拡散度および可能性のある脅威を返し、悪意のあるファイルを自動的にブロックします。

システムは設定に応じて、悪意のあるファイルを元のファイルが削除された理由を説明する .txt ファイルで置き換えるか、悪意のあるファイルへのそれ以上のアクセスを単にブロックします。

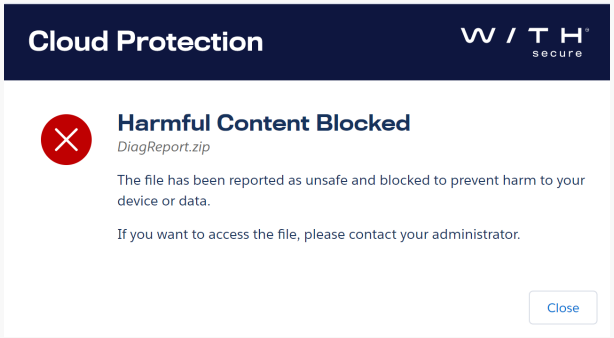
**マルチエンジンアンチウイルス**

ファイルのレピュテーションが不明な場合、コンテンツは WithSecure™ Security Cloud にアップロードされ、さらなる脅威分析が行われます。ファイルは、マルウェア、ゼロデイエクスプロイト、および高度な脅威のパターンを見つけるために、複数の補完的なマルウェア対策エンジンによる詳細な分析を受けます。この段階の分析プロセスでは、WithSecure™ Labs が収集した脅威インテリジェンスデータと機能をフルに活用します。

**コンテンツフィルタリング**

Cloud Protection アプリケーションは脅威分析を実行する前に、ソリューションの設定で定義されたファイルタイプまたは拡張子の制限リストに対してファイルをチェックします。ファイルがリストの拡張子またはファイルタイプのいずれかに合致した場合、アプリケーションはそのファイルをブロックします。管理者へは、通知設定に従ってセキュリティアラートが送信されます。

コンテンツフィルタリングにより、組織はユーザーが不適切なコンテンツや危険なコンテンツをアップロードすることを防ぐことができます。例えばマルウェアを拡散させるリスクを最小限に抑えるために、Cloud Protection では Salesforce Cloud にアップロードされた実行ファイル（EXE、COMなど）やスクリプト（VBS、PS1など）をブロックするように設定することができます。




### スマートクラウドサンドボックス

システムは最適化された機械学習技術を使用し、脅威分析の結果に基づいて、より詳細な分析のためにファイルをスマートクラウドサンドボックスに送信するかどうかを決定します。疑わしいリスク指標がある場合、ファイルをサンドボックスに送り、そこで複数の仮想環境で実行して挙動を分析します。
スマートクラウドサンドボックスは、静的な識別子ではなく悪意のある挙動に注目して分析を行うことで、最も洗練されたマルウェアやゼロデイマルウェア、エクスプロイトであっても検知してブロックすることができます。

### 解析結果

アップロードされたファイルは、最終的な評価に基づいて有害か無害かのどちらかに分類されます。有害または不審な場合、設定に応じてファイルは削除され、ファイルをアップロードしたユーザーと管理者にインシデントが通知されます。セキュリティ上の脅威が発見されない場合、ファイルは元のアップロード場所でアクセス可能となり、ファイル脅威検知イベントは必要に応じてさらなる分析と監査のためにスキャンログに記録されます。

最終的な評価、ファイルのレピュテーション、およびその他の脅威分析の詳細は、将来の使用のために脅威検知キャッシュに保存されます。悪意のあるファイルの検知詳細は、ウィズセキュアの脅威インテリジェンスサービスに送信され、次の脅威検知クエリが脅威を即座に特定してブロックできるようにします。

## 4.2.2 Download Protection

Download Protection は、ユーザーが Chatter、Salesforce Files または Attachments から有害なコンテンツや許可されていないコンテンツをダウンロードできないようにします。WithSecure™ Cloud Protection が Upload Protection と同様のプロセスを実施し、ファイルの評価結果が脅威検知キャッシュですでに利用可能な場合、ファイルはそれに応じて許可/ブロックされ、そうでない場合も Upload Protection と同じプロセスが実行されます。

ファイルが安全な場合は、通常の Salesforce ユーザーエクスペリエンスと同様に、ユーザーはファイルをシームレスにダウンロードすることができます。ファイルが有害または未許可と判定された場合、アプリケーションはユーザーからファイルへのアクセスをブロックし、ソリューションの設定に応じて管理者にアラートを送信します。

アップロードとダウンロードの両方の段階でチェックを行うことは、常に最新のセキュリティインテリジェンスを確実に適用するために非常に重要です。一度検知プロセスを回避したマルウェアでも、新しい脅威インテリジェンスが利用可能になった後にに検知されることがあるからです。

## 4.2.3 手動スキャン

手動スキャンを使用すると、WithSecure™ Cloud Protection をインストールする前に Salesforce Cloud に追加されたファイルや、Upload および Download Protection によってスキャン対象外となった Salesforce ファイルと添付ファイルをスキャンすることができます。さらに、定期的にシステム全体をスキャンするようにスケジュールを設定することもできます。スキャンはバックグラウンドで実行され、ユーザーエクスペリエンスやパフォーマンスには影響を与えません

# 4.3 URL Protection

URL Protection は、Chatter の投稿・コメントやケースの説明・コメント、およびメール-to-ケースで受信したメッセージ本文の Web リンクを介して Salesforce ユーザーが悪意のあるコンテンツや右心なコンテンツにアクセスするのを未然に防ぐための、重要なセキュリティ機能です。

このセキュリティコンポーネントは、ユーザーの行動に早期に介入することで、悪意のあるコンテンツや攻撃に晒される部分を大幅に減らすことができるため、特に効果的です。例えば、一見正当なフィッシングサイトや悪意のあるサイトに騙されてアクセスしたり、アダルトサイトやギャンブルサイトなど、ビジネス上不適切と判断されるコンテンツにアクセスしたりすることを防ぐことができます。

URL Protection は、インターネット上の数十億のサイトと、常に変動するセキュリティ環境に効率的に対処するために開発されました。これは、ウィズセキュアの Security Cloud へのリアルタイムの検索クエリに基づいています。すべてのクエリは、ビジネスの機密性を最大限に確保するために、いくつかの匿名化の層を通過します。

クエリは、以下のような様々なデータポイントに基づいて、Web サイトとそのファイルの最新のレピュテーションを取得します：IP アドレス、URL キーワード、サイトパターン、iframe やファイルタイプなどの Web サイトのメタデータ、エクスプロイトの試みや悪意のあるリダイレクト、あるいはスクリプトなどの Web サイトの挙動など。

## 4.3.1 URL Security Check

このソリューションは、ユーザーが Chatter に投稿した URL やメール本文（メール-to-ケース）に含まれるフォームを検知し、特別なリダイレクトリンクに置き換えます。元のリンクは認識のために括弧で囲まれていますが、ユーザーがクリックすることはできません。また、URL を難読化することでコピーを防止しています。

クエリから受け取った情報から、悪意のあるリンクと判断された場合は、コンテンツが読み込まれる前にサイトへのアクセスがブロックされ、エンドユーザーに警告が表示されます。

ユーザーがリダイレクトリンクをクリックした場合、WithSecure™ Cloud Protection は、元のURLを WithSecure™ Security Cloud に送信し、脅威インテリジェンスのチェックを行います。URL の脅威インテリジェンスに基づいて、元の URL へのアクセスが許可またはブロックされます。

## 4.3.2 URL カテゴリフィルタリング

URL カテゴリフィルタリングにより、管理者は Salesforce ユーザーがアクセスできる Web ページを制御し、適用することができます。

たとえば、ソーシャルメディアサイトなど業務に関係のないサイトへのアクセスを禁止して、作業時間のロスを防ぐことができます。アダルトやギャンブルなどのリスクの高いカテゴリのサイトをブロックすることで悪質なサイトの閲覧を防ぎ、ビジネス環境や顧客またはパートナーのポータルでの不適切なコンテンツの閲覧を防ぐことができます。

ユーザーがリダイレクトリンクをクリックすると、WithSecure™ Cloud Protection は元の URL を WithSecure™ Security Cloud に送信し、脅威インテリジェンスのチェックを行います。URL についての脅威インテリジェンス情報に基づいて、元の URL へのアクセスが許可またはブロックされます。

ソリューション管理者は、28 個の異なるカテゴリで利用ルールを適用することができます：

中絶、広告サービス、アダルト、アルコール・タバコ、アノニマイザー、オークション、バンキング、ブログ、チャット、デート、ドラッグ、エンターテイメント、ギャンブル、ゲーム、ハッキング、ヘイト、就職活動、決済サービス、詐欺、ショッピング、ソーシャルネットワーキング、ソフトウェアダウンロード、スパム、ストリーミングメディア、暴力、ウェアーズ、武器、Webメール

## 4.4 Email Protection

Salesforce のメール-to-ケースでは、ユーザーが指定したメールアドレスにメッセージを送信するとケースが自動で作成され、ケースフィールドが入力されます。WithSecure™ Cloud Protection が受信メールを検知すると、すべての添付ファイルと URL について脅威検知を行います。ファイルの評価がすでに判明しており、脅威検知の TTL（Time-To-Live）が有効な場合は、悪意のあるファイルが削除されるか、管理者にインシデントが通知されます。さらに、すべての URL が書き換えられます。

ファイルが新しい場合、または TTL が失効している場合には、WithSecure™ Cloud Protection は Upload Protection と同じ脅威検知プロセスを開始します。「4.2 File Protection」を参照してください。

ユーザーが URL をクリックすると、WithSecure™ Cloud Protection は URL Security Check と同じ脅威検知プロセスを開始します。詳しくは「4.3 URL Protection」を参照してください。

## 4.5 管理

豊富なレポート、高度なセキュリティ分析、完全な監査証跡により、システム管理者は脅威への対応が容易になり、Salesforce のコンテンツを 360 度全方向から可視化することで、Salesforce の利用パターンを確実に把握することができます。これは、Salesforce を介して発生した攻撃への対応、不明な攻撃源からの攻撃の調査、Salesforce がインシデントの一部であったかどうかの検証に役立ちます。

### 4.5.1 分析

WithSecure™ Cloud Protection は、Salesforce のコンテンツを360度全方向から可視化します。すべてのアップロードとダウンロードのファイル操作と URL クリックは、分析ログに保存されます。

分析にはファイルと URL のイベント履歴表示が含まれており、管理者が Salesforce コンテンツにアクセスしたすべてのユーザーを特定したい場合に役立ちます。

多くの IT 部門では、組織がどのようなコンテンツを Salesforce に保存しているかを把握できていません。しかし IT 管理者にそのような知見があれば、例えば Salesforce に保存すべきではない実行ファイルを見つけることができるなどのメリットがあります。

さらに、内部の顧客のニーズやユースケースをよりよく理解することで、管理者はより効果的にサービスを提供することができます。

強力な検索機能により、ソリューション管理者と IT セキュリティ部門は、コンテンツベースの攻撃を数秒で調査することができます：

- Salesforce が攻撃経路かどうかの確認、またはルールからの除外
- IP アドレスなどの攻撃者の詳細を調査
- 悪意のあるコンテンツにアクセスしたユーザーを特定

**分析ログには以下の情報が含まれます：**

- タイムスタンプ
- アクション
- 評価＋ファイルの拡散度
- 理由
- ディレクション（アップロード/ダウンロード/投稿/クリック）
- ユーザー名
- ファイル名
- ファイルタイプ
- ファイルのバージョン
- ファイルサイズ
- URL
- URL カテゴリ
- ロケーション（どこにファイル/URL が保存されているか）
- ファイル SHA-1 チェックサム
- IP アドレス

### 4.5.1 アラート

すべてのセキュリティアラートと監査イベントは、セキュリティアラートログに書き込まれます。Salesforce 管理者は、ソリューション管理者と IT セキュリティ担当者が次のような状況でアラートを受信できるように設定することができます：

- 有害なコンテンツを発見した場合
- アップロード時に有害なコンテンツがブロックされた場合（内部ユーザーの場合はアップローダへの警告）
- 有害な URL を発見した場合
- アップロード時に有害な URL を発見した場合（内部ユーザーの場合はアップローダへの警告）
- 許可されていない URL を発見した場合（内部ユーザーの場合はアップローダへの警告）
- ファイルまたは URL のスキャン結果が安全から有害に変更された場合
- 許可されていないファイルタイプを発見した場合
- アップロード時に許可されていないファイルタイプを発見した場合（内部ユーザーの場合はアップローダへの警告）

### 4.5.3 レポート

WithSecure™ Cloud Protection では、Salesforce のコンテンツを詳細に見ることができます：

**サマリー保護ダッシュボード：**

- 保護されたファイルのアップロード+トレンド
- 保護されたファイルのダウンロード+トレンド
- 保護された URL 投稿＋トレンド
- 保護された URL クリック＋トレンド
- 脅威インテリジェンスイベント+トレンド
- 保護されたユーザー＋トレンド

**保護されたコンテンツの分析 - ダッシュボード：**

- 保護されたユーザー
- アクティブなファイル保護ユーザー
- アクティブな URL 保護ユーザー
- ファイルアップロード
- ファイルダウンロード
- ユーザーごとのファイルイベント
- ロケーションごとのファイルコンテンツ
- ファイルタイプごとのファイルコンテンツ
- 脅威インテリジェンスイベント
- URL の投稿
- URL のクリック
- ユーザーごとの URL イベント
- ロケーションごとの URL
- カテゴリごとの URL

**ファイル保護の詳細 - ダッシュボード：**

- 重要度別ファイル保護アラート
- 処理されたファイル脅威
- ロケーションごとの処理されたファイル脅威
- ファイルタイプごとの処理されたファイル脅威
- ユーザーごとの処理されたファイル脅威
- トップのファイル脅威（感染）

**URL 保護の詳細 - ダッシュボード：**

- 重要度別 URL 保護アラート
- 処理された URL 脅威
- ロケーションごとの処理された URL 脅威
- ユーザーごとの処理された URL 脅威
- トップの URL カテゴリ

**WithSecure™ Cloud Protection は、Salesforce Reports を介したカスタムレポートにも対応します。**

**ファイル保護レポートでは、以下の属性を使用できます:**

- **作成者:** フルネーム、作成日、日時、ファイル拡張子、ファイル名、ファイルスキャン ID、ファイルサイズ、ファイルタイプ、IP アドレス
- **最終更新:** フルネーム、最終更新日、名前、所有者:フルネーム、レコードID、スキャンタイプ、SHA1、ロケーション
- **ユーザー:** フルネーム、評価、所有者(姓、名、フルネーム、所有者ID、電話番号)
- **プロフィール:** 名前ルール:名前、肩書、ユーザー名、電子メール、エイリアス、アクティブ、理由、ファイルの拡散度、ファイルのレピュテーション評価

**URL Protection レポートでは、以下の属性を利用できます:**

URLスキャン:ID、URLスキャン:名前、アクション、カテゴリ、日時、ディレクション、IPアドレス、ロケーション、理由、レピュテーション、レピュテーションの詳細、URL、ユーザー、評価、所有者名、所有者のエイリアス、所有者のロール、作成者、作成者のエイリアス、作成日、最終更新者、最終更新者のエイリアス、最終更新日

## 4.5.4 管理

ソリューション管理者は、企業のセキュリティポリシーに基づいて保護機能やアクションを有効または無効にすることができます。例えば、厳格なコンプライアンスや秘密保持の要件により、分析のためにクラウドにファイルをアップロードすることを禁止するような場合には、設定の変更によって対応できます。

## 4.5.5 導入

WithSecure™ Cloud Protection はネイティブの Salesforce アプリケーションと WithSecure™ Security Cloud の組み合わせで、他のウィズセキュア製品やサードパーティ製品でも使用されているレピュテーションとセキュリティサービスを提供します。
このソリューションは Salesforce プラットフォームにインストールされ、Sales、Service、Community Cloud のような企業が使用するすべての Salesforce Cloud を保護します。他のソフトウェアやネットワーク構成の変更は必要ありません。

## 4.5.6 カスタマイズ

WithSecure™ Cloud Protection では、Salesforceの管理者がすべてのエンドユーザーメッセージをカスタムバナー上にカスタマイズすることができます:

- 有害なコンテンツが見つかりました(管理者へのアラート)
- アップロード時に有害なコンテンツが見つかりました(内部ユーザーへのアラート)
- 悪意のあるファイルをテキストファイルに置き換えました(ファイルコンテンツ)
- 有害な URL が見つかりました(管理者へのアラート)
- アップロード時に有害な URL が見つかりました(内部ユーザーへのアラート)
- 許可されていない URL が見つかりました(管理者へのアラート)
- アップロード時に許可されていない URL が見つかりました(内部ユーザーへのアラート)
- ファイルや URL のスキャン結果が安全から危険に変更されました(管理者へのアラート)
- 許可されていないコンテンツが見つかりました(管理者へのアラート)
- アップロード時に許可されていないコンテンツが見つかりました(内部ユーザーへのアラート)

# 5. WithSecure™ Security Cloud

WithSecure™ Security Cloud は、ウィズセキュアが運営するクラウド型のデジタル脅威分析システムです。クライアントシステムのデータと自動化された脅威分析サービスによって提供されるデジタル脅威のナレッジベースは、常に成長し進化を続けています。Security Cloud のインフラは、世界中の Amazon Web Services データセンターにある複数のサーバー上でホストされており、毎日 80 億件以上のクエリを処理する大容量のシステムです。

ウィズセキュアでは、サービスを提供するために必要な最低限のクライアントデータのみを収集しています。転送されるすべてのデータは脅威防止の観点から適切でなければならず、将来の必要性を想定してデータが収集されることはありません。
Security Cloud は、デフォルト設定では IP アドレス、ファイル、その他の個人情報を収集しません。お客様は、疑わしい実行ファイルや実行ファイル以外の疑わしいファイルを保存する許可をウィズセキュアに与えることができます。

ウィズセキュア社内のデータベースやその他の様々な情報源から取得した情報と組み合わせたメタデータを評価することで、自動分析システムが脅威に対する十分な情報に基づいた最新のリスク評価を提供し、Security Cloud に接続されている他のサービスやデバイスが事前に検知した脅威を即座にブロックします。

また Security Cloud では、自動化されたシステムやホスト上のスキャン技術を補完するために WithSecure™ Response Labs のアナリストが人によるインテリジェンスと判断を提供します。アナリストはデータベースや自動分析システムを支えるルールの作成と維持に加えて、最新の脅威を積極的に監視しており、マルウェアの特性や行動パターンを研究して悪意のあるプログラムを最も効果的に特定する方法を見つけ出します。

**以下の表は、ウィズセキュアのプライバシー原則の詳細を文書化したものです。**

| | |
|---|---|
| **技術データの送信を最小限に抑える** | WithSecure™ Security Cloud は、多段階のコンテンツ分析を採用しています。ファイルデータは保護を提供するために必要不可欠であり、お客様が許可した場合を除き Security Cloud には送信されません。 |
| **個人データを送信しない** | 分析されたファイル/URL を誰が投稿したりアクセスしたりしたか、またはどこからアクセスしたかに関する情報は、WithSecure™ Security Cloud には送信されません。 |
| **ネットワークを信頼しない** | すべてのメタデータ、ファイルおよびその他のコンテンツは、HTTPS 経由で、または暗号化され署名された上で HTTP 経由で、安全に Security Cloud に送信されます。 |

**Security Cloud 原則：**

| | |
|---|---|
| **セキュアバイデザイン** | システムは、安全であるように設計されていない限り、決して安全にはなりません。セキュリティを後付けとして追加することはできないのです。Security Cloud とその関連システムを開発する際には、この原則が実践されました。 |
| **ネットワークトラフィックの暗号化** | インターネット上を、データが平文で転送されることはありません。また、さまざまなオブジェクトの整合性を確保するためにも暗号化が使用されます。ウィズセキュアでは、一般的に利用されている暗号化ライブラリやプロトコルと、カスタマイズされた暗号化プログラムを組み合わせて使用しています。 |
| **マルウェア環境の分離** | ウィズセキュアは、悪意のあるソフトウェアの保存とテストにおける課題への対応において、20 年以上の経験を持っています。すべてのマルウェア処理は、インターネットや他のウィズセキュアネットワークから隔離されたネットワークで行われます。ストレージネットワークとテストネットワークは互いに隔離されており、ファイルの転送は厳密に制御された方法で行われます。 |
| **専門家による監視** | すべての重要な Security Cloud システムは、ウィズセキュアの担当者によって監視されています。<br>また、マルウェアを保存またはテストするすべてのシステムは、ウィズセキュア本社によってホストされています。 |
| **制御されたアクセス** | Security Cloud の重要なシステムにアクセスすることができるのは、限られた数のウィズセキュアの従業員のみです。このようなアクセスは、文書化され厳密に管理されたプロセスに従って許可、無効化、文書化されます。 |
| **オープンな姿勢** | すべてのセキュリティ業務において最も基本的なことは、オープンで謙虚な姿勢を持つことです。私たちは Security Cloud のセキュリティ向上に力を入れてきましたが、その作業に決して終わりはありません。システムの問題が報告され、分析され、迅速に修正されるようなオープンな姿勢を持ち続けることによってのみ、安全なシステムを維持することができます。この姿勢には、お客様のセキュリティを危険にさらすような事件に遭遇した場合の公開性も含まれています。 |

## 5.1 脅威インテリジェンスサービス

数千万ものセンサーから収集したリアルタイムの脅威インテリジェンスを活用することで、新たに出現し急速に拡散する脅威を数分以内に特定し、常に進化する脅威ランドスケープに対して卓越したセキュリティを提供します。脅威インテリジェンスサービスは、WithSecure™ Cloud Protection がファイルや URL などのオブジェクトのレピュテーションを照会することを可能にします。ファイルは、オブジェクトの暗号化ハッシュ SHA-1 を計算し、レピュテーションサービスに送信することで検証されます。

## 5.2 マルチエンジンアンチウイルス

マルチエンジンアンチウイルスは、複数のセキュリティ層を使用して、標的型攻撃に使用されるエクスプロイトや未知のマルウェアを検知します。このシステムは、行動分析とヒューリスティックおよび機械学習による検知機能を組み合わせており、特定のマルウェア、類似の特徴を持つマルウェアファミリー、幅広い物理的な特徴やパターンを特定することができます。この分析結果によりファイルに不審フラグが立てられると、スマートクラウドサンドボックスに送られてさらなる処理が行われます。

## 5.3 スマートクラウドサンドボックス

スマートクラウドサンドボックスは、複数の仮想環境で疑わしいファイルを実行し、ファイルの挙動を分析します。ファイルの挙動が疑わしいと判断された場合、情報はマルチエンジンアンチウイルスおよび脅威インテリジェンスサービスに送られ、次段の脅威検知クエリが脅威をブロックします。

WithSecure™ Security Cloud の詳細については、Security Cloud ホワイトペーパーおよび Security Cloud プライバシーポリシーを参照してください。

# ウィズセキュアについて

ウィズセキュアは、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

**ウィズセキュア株式会社**
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2022/05

WITH secure™