Kiteworks | servicenow

ソリューション概要

ServiceNow AI Platformの管理責任者、ITサービスマネジメント部門、セキュリティ部門の皆様へ

ServiceNow AI Platform内で実現する、ガバナンスの効いたデータ交換

レコード上でやり取りされるファイルは企業のデータポリシーに従い、その証跡もレコード上に残ります

課題

チームはServiceNow AI Platform上でITサービス、運用、変更管理を行っており、すべてのチケットが小さなファイル転送になります。ログ、スクリーンショット、契約書などの機密文書は、添付ファイルやメールとして、企業のデータポリシーの外でやり取りされています。社外の関係者にServiceNow AI Platformへのアクセスを付与するにはコストがかかり、リスクの範囲も広がります。Verizonの「2026年データ漏えい・侵害調査報告書」では、**侵害の48%**がサードパーティに起因すると報告されています。

ソリューション

Kiteworks for ServiceNow AI Platformは、Incident、Problem、Change Request、Service Catalog Request、Knowledgeの各レコードに、ガバナンスの効いたKiteworksフォルダを追加します。チームはレコードを離れることなく、セキュアメールの送信、ガバナンスの効いたフォルダでのファイル保管、ベンダー、監査人、お客様へのファイル依頼を行えます。Kiteworks Data Policy Engineが各ファイルを評価し、最大16 TBの転送に対応します。

対象：ServiceNow AI Platformの管理責任者、および規制対象組織のセキュリティ責任者の皆様

チームによるServiceNowの活用場面と、Kiteworksが加える価値

ITサービスマネジメント（ITSM）は、約8,700社とされるServiceNowのお客様の大半にとって中核となる製品であり、ITSM市場での推定シェアは44.4%です。また、IT運用管理（ITOM）は、2026年第2四半期のServiceNowの大型案件上位20件のうち18件に含まれていました。

ユースケースとレコード	レコード上でのチームの作業	Kiteworksが加える価値	重要な理由
ITサービス管理 Incident Service Catalog Request	サービスデスクの担当者が、スクリーンショット、ログ、文書が添付された、従業員やベンダーからのインシデントとカタログリクエストを処理します。	担当者は、ログやスクリーンショットを添付せず、インシデントのガバナンスフォルダに集めます。フルフィルメント担当者は、カタログリクエストの機密文書をレコードからセキュアメールで送信します。	アプリを通じてやり取りされるすべてのファイルにデータポリシーが適用され、ファイルが大きくてもレコードを離れる必要はありません。
変更管理 Change Request	変更管理者は、変更を進める前に、ベンダーからの証跡と承認を収集します。	変更管理者がベンダーにファイルを依頼すると、ベンダーはセキュアなリンクからアップロードでき、ServiceNow AI Platformにアクセスする必要はありません。ポリシーは受信時に適用されます。	ベンダー用のライセンスがなくても、ベンダーの証跡をレコードに集約できます。依頼とアップロードは、それぞれ記録されます。
問題管理 Problem	問題管理者は、ベンダーのエンジニアとともに根本原因を調査し、調査結果を共有します。	ベンダーのエンジニアは、DownloaderまたはCollaboratorとしてフォルダに参加します。問題管理者は、問題のクローズ時に社外関係者のアクセス権を取り消します。	ベンダーはServiceNow AI Platformのアカウントなしで問題に対応でき、作業の完了とともにアクセスも終了します。
IT運用管理とAIOps Incident Problem	運用チームは、イベントをインシデントに変換し、診断ファイルや構成ファイルをベンダーに送ります。	最大16 TBの診断バンドルやキャプチャは、ガバナンスフォルダを経由して移動し、ダウンロード前にスキャン結果が確認されます。	構成ファイルは環境の詳細を示すものです。大容量のキャプチャを送る方法を探す時間は、障害を長引かせます。
ナレッジ管理 Knowledge	作成者は、一部に閲覧制限のある元資料から記事を作成します。	作成者は、管理対象の元資料を、ボタン1つで作成される記事用フォルダに保管します。誰が開けるかはポリシーが決定します。	元資料はガバナンス下に保たれ、記事は引き続き共有しやすい状態です。

ServiceNow AI Platformはワークフローを実行します。Kiteworksは、そこを流れるデータをガバナンスします。

認証・認定：Kiteworks Secure Gov CloudはFedRAMP Class D（機関認可手続き中）、Kiteworks Federal CloudはFedRAMP Class C認定を取得しています。また、SOC 2 Type II、ISO 27001、FIPS 140-3の検証済みです。PCI DSS、HIPAA、GDPR、CMMC 2.0、NIST SP 800-171の要件への対応を支援します。

Kiteworks for ServiceNow AI Platformのしくみ

メールとファイル共有をガバナンスするKiteworks Data Policy Engineが、レコード上のファイルもガバナンスします。



Kiteworks for ServiceNow AI Platform：すべてのレコードでガバナンスの効いたデータ交換を実現

01
封じ込め
ファイルはどこに保存され、誰が所有するのか。

ファイルは、Kiteworksのハードニング済み仮想アプライアンス内のガバナンスフォルダに保管され、シングルテナントアーキテクチャ、お客様所有の鍵、ジオフェンシングを備えています。

02
制御
すべてのファイルがポリシーに従っているか。

Data Policy Engineは、操作する人とデータの内容に基づいて、ブロック、閲覧のみへの制限、承認の要求、ファイルへのタグ付けを判断します。ダウンロード前にスキャン結果が確認されます。

03
証明
審査担当者に何が起きたかを示せるか。

Governance Eventsは、アプリを通じた人の操作をレコード上に記録します。Kiteworks監査ログはすべてのファイル操作を記録し、お客様のSIEMにストリーミングします。

04
移動
人の仕事を止めないか。

セキュアメール、ガバナンスフォルダ、ファイル依頼のすべてを、レコードから実行できます。転送は最大16 TBに対応するため、実質的なサイズ制限はありません。社外の関係者にServiceNow AI Platformへのアクセスは不要です。

ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries.

ServiceNow AI Platform内のファイル交換にガバナンスを効かせませんか。

www.kiteworks.com

Kiteworks

in f X ig yt

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

© 2026 Kiteworks LLC. All rights reserved.