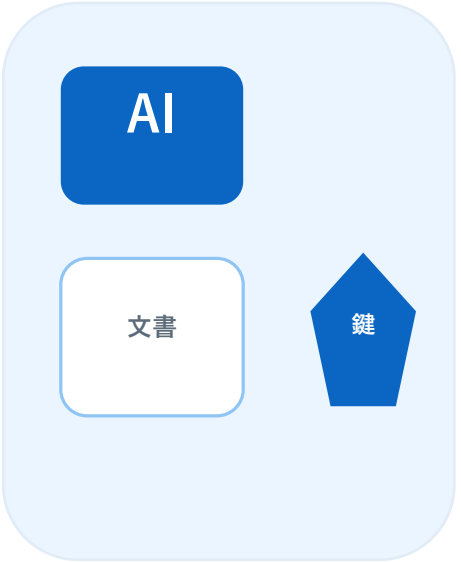
AIと人がつくる、
よりよい社会のために

生成AI時代の誤送信事故

RIZAP公表事例から学ぶ Shadow AI・個人情報保護・会社のガバナンス

公開事例から、自社のAI利用ルール・技術統制・委託先管理を考える

弁護士　渡邉雅之



事実を知る
公開された
事例から学ぶ

AIを正しく使う
利便性とリスクを
両立する

個人情報を守る
データの適切な
取扱いを徹底する

ガバナンスを強化
組織・委託先を含めた
統制を実現する

再発を防ぐ
実効性のある
ルールと運用へ

※公開情報に基づく整理

生成AI時代の誤送信事故

RIZAP公表事例から学ぶ　Shadow AI・個人情報保護・会社のガバナンス

AIと人がつくる、
よりよい社会のために

この資料で扱うこと

1. 事件の事実関係と時系列
2. Shadow AI の本質と発見方法
3. 許されるAIと自社限定APIの設計
4. 個人情報保護法・委託先管理の論点
5. 探知発見ツールとその限界
6. 会社のガバナンスチェックリストと初動

結論を先に

- ✓ これは「AIが暴走した事件」ではない
- ✓ 従来の持出し事故が、生成AIという出口から起きた
- ✓ 問題は「学習されたか」だけではない
- ✓ 禁止規程だけでは防げず、技術統制が必要
- ✓ 委託先も含めたAIガバナンスが問われる

💡 **要点：RIZAPの特殊事例ではなく、生成AIを使うすべての組織に共通する教材事例である**

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表、個人情報保護委員会資料を基に作成

事案の概要

まず何が起きたのか

公表された事実

● RIZAP株式会社の健康経営・保険者事業部の社員が対象
● データ集計作業中に、個人で利用していた外部生成AIへ顧客情報をアップロード
● 会社公認AIではなく、未承認の個人利用AIだった点が重要

期間・対象

● RIZAP公表日：2026年9月3日
● 対象データ：2026年1月1日～8月19日に登録された特定保健指導対象者データの一部
● IHI健保公表では、RIZAPの特定保健指導利用者210名に関係する事案と説明

ここが本質

● 健康情報を含む個人データが、会社の統制外にあるAIへ入力された
● 「便利だから使った」が、そのまま事故につながった
● Shadow AI と個人情報保護が交差した事案である

要点：この事件は、生成AI時代の“新しい誤送信事故”として理解するのが最も分かりやすい

出典：RIZAP株式会社 2026年9月3日公表、IHIグループ健康保険組合 2026年9月2日公表

時系列と初動対応

発覚から公表まで

時系列で見る主な対応

8月24日	IHI健保公表によれば、RIZAPから事案の報告を受領
発見直後	当該社員がチャット履歴削除、学習利用停止設定を実施
その後	生成AI事業者へデータ削除等を照会
9月1日	IHI健保公表では、OpenAI社から「当該データはモデル学習に利用されていない」と回答
9月3日	RIZAPが公表、個人情報保護委員会へ報告、対象者への連絡を開始

初動で見えること

✓ 比較的早い初動対応が取られている
✓ ただし、削除できたことと法的評価は別問題
✓ 発見から公表までの対応速度は、AI事故実務の重要論点

要点：AI誤投入では、最初の24時間の動きが、その後の評価を大きく左右する

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表

対象データと影響の重さ

なぜ“重い事故”なのか

AIと人がつくる、
よりよい社会のために

含まれていた情報と実務上の意味

区分	含まれていた情報	実務上の意味
基本属性	氏名・生年月日・性別・メールアドレス	本人特定性が高い
保険関連	保険証記号番号	センシティブな管理情報を含む
連絡先	一部の住所・電話番号	外部流出時の二次被害懸念
指導情報	特定保健指導の支援形態	健康管理情報として慎重な管理が必要
疾患情報	高血圧症・糖尿病・脂質異常症など	要配慮個人情報を含み、事故対応が重くなる

補足情報

**IHI健保公表では
210名が対象**

要点：単なる名簿ではなく、健康・保険・疾患情報が重なっている点が本件の深刻さである

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表

なぜこの事案は重大なのか

4つの危険が重なっている

要配慮個人情報

- 疾患情報を含む
- 本人通知・報告の判断が重い

DB 委託データ

- 委託元の期待とのズレ
- 委託先監督の論点が生じる

AI Shadow AI

- 未承認利用
- ログが乏しく発見しにくい

! 説明責任

- 顧客・委託元・監督当局への説明が必要
- 信頼毀損リスク

要点：本件は“AI利用ミス”ではなく、個人情報・委託・ガバナンスの複合事故である

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表

Shadow AI とは何か

本質はAIそのものではなく、統制の外で使うこと

定義

- 会社が承認・把握していないAI利用
- 私用アカウントや無料版も含む
- 問題は「AIを使ったこと」ではなく「統制外で使うこと」

なぜ増えるか

- 公認ツールが使いにくい、又は用意されていない
- 現場の要約・文案作成ニーズが強い
- ルールが抽象的で分かりにくい
- 便利さが先行し、リスク評価が後回しになる

主な例

- 個人契約のChat型AI
- ブラウザ拡張要約ツール
- 無承認の議事録AI
- 外部要約・翻訳サービス

要点：問題は“AIを使ったこと”ではなく、“会社が管理できない形で使ったこと”にある

なぜ判明したのか

IHI健保公表では“自己申告”が鍵

公開情報から読めること

1. IHIグループ健康保険組合の公表では「当該従業員の自己申告により判明」
2. 本人が気づき報告したことが発見の起点
3. 発見直後に削除・停止対応が行われた

そこからの教訓

✓ 本人申告に依存する事故は見逃されやすい
✓ 申告がなければ把握が遅れる可能性
✓ だからこそアクセス制御・アップロード制御・ログ監視が必要

要点：Shadow AIは“悪意”よりも“気軽さ”で起き、申告がなければ見つからないことがある

出典：IHIグループ健康保険組合 2026年9月2日公表

論点①「学習されなければセーフ」ではない

学習利用の有無は重要だが、それだけでは足りない

誤解しやすい整理

1. 学習に使われなければ問題ない
2. 削除できれば終わり
3. AI側の設定だけ見ればよい

実務上の整理

✓ そもそも社外AIに個人データを入力してよかったのかが論点
✓ 利用目的・委託・安全管理・契約条件も確認が必要
✓ 「学習オフ」は必要条件であって十分条件ではない

要点：AI事故では、“どこに何を送ったか”を先に見るべきである

出典：個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」等

論点② 委託・再委託・監督

この事案を矢印で見る

保険者・企業等
（委託元）

→

RIZAP

RIZAP
（委託先）

→

AI

未承認の
外部生成AI

委託元は、委託先であるRIZAPの管理体制をどう見ていたか

委託データを外部AIへ入力することは、契約上どう位置づくか

再委託や外部サービス利用に関する事前ルールはあったか

事故時に委託元へどのように報告・説明するか

要点：「自社で入力していない」では足りず、委託先のAI利用まで見る必要がある

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表

論点③ クラウド例外・第三者提供との関係

“クラウドだから大丈夫”ではない

1 確認すること

● ベンダーが個人データを取り扱うのか
● 契約・仕様で学習や閲覧がどうなっているか

2 実務感覚

● 会社公認の管理された環境と、個人アカウント・無料版では前提が大きく異なる
● 生成AIではベンダー側の取扱いの有無が重要

3 本件への示唆

● 個人利用AIでは、クラウド例外で単純に片付けにくい
● 少なくとも慎重な検討と契約・設定確認が必要

💡 **要点：「クラウド」「AI」というラベルではなく、実際のデータ取扱い実態で判断する**

出典：個人情報保護委員会Q&A Q7-53等

論点④ 個人情報保護委員会報告・本人通知・初動

削除できた、で終わらない

AIと人がつくる、
よりよい社会のために

1 **事実確認**

入力した情報、時系列、経緯を正確に把握

2 **影響範囲の特定**

漏えい等のおそれがある個人データの種類・件数・本人を特定

3 **PPC報告要否**

要配慮個人情報を含む場合、報告対象事態となり得る

4 **本人通知要否**

報告対象事態では、本人通知も原則として検討

5 **委託元・経営陣共有**

委託元、法務、情シス、個人情報担当が連携

⚠ **要配慮個人情報を含むため、通常より重い判断が必要になりやすい**

期限感 速報：速やかに（概ね3〜5日以内）／確報：原則30日以内（不正目的等は60日以内）

💡 **要点：AI誤投入時は、削除対応と並行して、報告・本人通知・委託元説明を進める必要がある**

出典：RIZAP株式会社公表、個人情報保護委員会「漏えい等報告・本人への通知の義務化について」等

RIZAPの再発防止策をどう読むか

公表文から見える方向性

公表された主な再発防止策

- AIおよび個人情報保護に関する管理の徹底
- 従業員教育の強化
- アクセス権限・利用環境の点検見直し
- AI管理システム導入の検討

実務上の読み替え

- 規程整備だけでなく、未承認AIへのアクセス制御
- 顧客データのアップロード制御
- ログ監視と承認済みルート整備
- 現場が使える公認AIの用意

要点：再発防止の核心は、“禁止”ではなく、“安全に使える正規ルート”を整えることにある

出典：RIZAP株式会社 2026年9月3日公表

どういうAI利用ならよいのか

OK・要注意・NGで整理する

✓ OK（原則可）

- 会社公認AIを、会社アカウントで利用
- 公開情報・自作メモ・匿名化済みデータの要約、翻訳、構成整理
- 会議アジェンダ、社内文案、研修資料のたたき台作成
- 入力情報・用途・出力確認者が明確

! 要注意（条件付き）

- 契約書、社内文書、顧客資料の要約や分析
- コード補助、議事録整理、データ分類などの実務利用
- 承認済み環境、学習利用オフ、マスキング、DLP、出力レビューが前提
- 要配慮個人情報・委託データは原則、別途承認

× NG（原則禁止）

- 個人アカウントや無料版AIに個人情報・機密情報・委託データを入力
- 保存先や規約が不明なAIへファイルをアップロード
- ブラウザ拡張・外部要約ツールへ顧客資料を投入
- 出力を検証せず対外文書や意思決定に利用

判断の4つの視点

1. どのAIか
2. どのアカウントか
3. どのデータか
4. 出力を誰が確認するか

💡 **要点：良いAI利用とは、承認環境で、入力情報・用途・出力確認を管理して使うことである**

「許されるAI」の4類型

サービス名ではなく、契約・設定・統制で判断する

1 会社アカウント型AI

ChatGPT Enterprise/Business、Microsoft 365 Copilot等。管理者、SSO、ログ、アプリ制御が効く環境で使う。

2 自社限定API型

会社契約のAPIキー、利用者認証、プロンプトログ、DLP、保存期間、削除条件を自社で設計する。

3 社内RAG・検索型

社内文書を直接学習させるのではなく、権限に応じて検索・参照し、回答根拠を返す構成にする。

4 閉域・専用環境型

金融・医療・高度機密では、VPC/Private Endpoint、専用テナント、ZDR等を検討する。

注意 **「企業向け」「API」でも自動的に安全ではない。契約、設定、権限、ログ、DLP、出力確認が揃って初めて業務利用に耐える。**

💡 **要点：許されるAIは「会社が責任を持って管理できるAI」であり、個人の便利ツールではない**

出典：OpenAI、Microsoft、AWS、Google、Anthropic各社の法人向けデータ管理説明を基に作成

自社限定APIなら何がよいのか

会社が「入口・出口・ログ」を設計できる

API 自社限定APIの典型構成

- 契約・APIキーは会社名義
- 利用アプリは社内システム経由
- SSO・MFA・RBACで利用者を限定
- プロンプト・ファイル投入前にDLP/マスキング
- 出力は人が確認し、対外利用は承認制

契 法務・契約で見ること

- 入力・出力がモデル学習に使われないか
- 保存期間、削除、ログ開示、事故通知
- 再委託・国外移転・データ所在地
- ベンダー職員の閲覧可能性とアクセス制御
- 監査、証跡、利用目的外利用の禁止

⚙ 技術で見ること

- Private Link/VPC/閉域接続
- IP制限、API Gateway、レート制限
- 暗号化、鍵管理、ログ保全
- Zero Data Retention 等の保持制御
- SIEM連携とアラート

💡 **要点：自社限定APIは「安全」なのではなく、「安全に設計しやすい」点に価値がある**

出典：OpenAI API Data Controls、Azure OpenAI/AWS Bedrock/Google Gemini/Anthropic API各種公開資料を基に作成

「APIなら安全」とは限らない

自作AIアプリで起きる落とし穴

! 安全そうに見えて危ない例

- 個人のAPIキーや私用アカウントで業務利用している
- 社内アプリ側がプロンプトや添付ファイルを平文保存している
- ログに個人情報・要配慮情報が残り、閲覧権限が広すぎる
- 外部プラグイン、Web検索、コネクタ連携で意図せず情報が出る
- 出力の誤り・幻覚・著作権侵害を確認せず使う

✓ 安全構成にするための必須要件

- ✓ 会社名義契約・会社管理のアカウント/APIキーに限定
- ✓ DLP、マスキング、サンプルデータ利用を標準化
- ✓ プロンプト・出力・添付ファイルのログ保全とアクセス制限
- ✓ モデル学習、保存期間、削除、職員閲覧可能性を確認
- ✓ 外部連携・エージェント権限は最小権限で管理

💡 **要点：API利用の肝は、モデルよりも「周辺アプリ・ログ・権限・外部連携」を管理することである**

Shadow AI 探知・発見ツールの全体像

単一製品ではなく、複数ログを組み合わせる

1	入口を見る	SWG / SASE / DNS / Proxy	生成AIサイトへのアクセス先、時間、ユーザー、端末を把握する
2	出口を見る	DLP / CASB / アップロード監視	CSV・Excel・PDF・個人情報パターンの送信を検知・遮断する
3	端末を見る	EDR / MDM / ブラウザ管理	ブラウザ拡張、外部送信アプリ、私用端末の抜け道を可視化する
4	統合して見る	SIEM / SOAR / UEBA	ログを相関分析し、異常利用をアラート化・調査可能にする

運用上の注意：ログ取得は、従業員への周知、目的限定、権限管理、保存期間の設計とセットで行う。

💡 **要点：Shadow AIの探知は、アクセスログ・DLP・端末管理・SIEMをつなげて初めて実効性が出る**

探知・発見ツールの実務例

「何が見えるか」で製品カテゴリを分ける

具体製品名は“推奨”ではなく、機能イメージを掴むための例

カテゴリ	代表例	見えること・止められること
Microsoft系	Purview DSPM for AI / Defender for Cloud Apps	AI利用の可視化、生成AIアプリ発見、データ保護・コンプライアンス統制
SASE / SWG	Zscaler / Netskope / Palo Alto / Cloudflare等	未承認AIへのアクセス制御、プロンプト・ファイルのDLP、ユーザーコーチング
DLP / データ分類	Microsoft Purview DLP / Google Sensitive Data Protection等	個人情報・機密情報パターンの検知、匿名化、マスキング、遮断
端末・ブラウザ	MDM / EDR / Enterprise Browser	ブラウザ拡張、ローカルアプリ、外部送信、私用端末利用の可視化
ログ統合	SIEM / SOAR / UEBA	アクセス・DLP・端末ログを相関し、異常なAI利用を調査・対応する

注意：製品導入だけで解決しない。公認AIの整備、ログ運用、例外承認、教育・自己申告制度と組み合わせる。

💡 **要点：ツール選定は「生成AIサイトを見たいのか、投入データを止めたいのか、ログを調査したいのか」から逆算する**

出典：Microsoft、Zscaler、Netskope、Palo Alto Networks、Cloudflare、Google各社公開資料を基に作成

会社のAIガバナンス全体像

5つの柱で考える

AIと人がつくる、
よりよい社会のために

1 体制・責任者

誰が承認し、誰が例外判断するか

2 ルール・データ分類

何を入れてよいかを明確化

3 技術統制

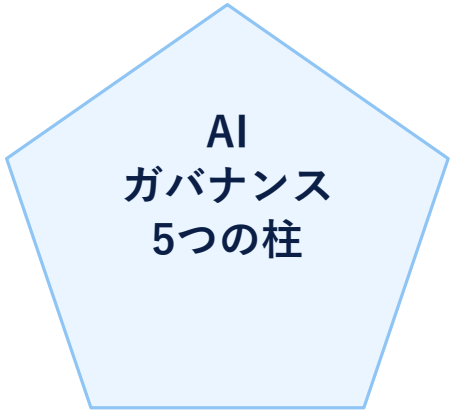
アクセス制御、DLP、ログ監視

4 委託先・ベンダー管理

契約、通知、再委託、削除、監査

5 教育・監査・改善

現場浸透、訓練、モニタリング



要点：AIガバナンスは“規程一枚”ではなく、体制・技術・委託先管理を束ねる仕組みである

ガバナンスチェックリスト① 体制・ルール

まず整えるべき基本項目

項目	確認ポイント	状況
責任者	AI利用の所管部署と決裁者が明確か	☐
公認AI	利用可能なAIサービス一覧があるか	☐
アカウント	会社アカウントと個人アカウントの境界が明確か	☐
入力ルール	個人情報・機密情報・委託データの取扱ルールがあるか	☐
承認手続	例外利用や新規ツールの承認フローがあるか	☐
記録	利用記録や判断記録を残す仕組みがあるか	☐

💡 **要点：「何を使ってよいか」「何を入れてよいか」が曖昧な会社ほどShadow AIが増えやすい**

ガバナンスチェックリスト② 技術統制

人の注意だけに頼らない

項目	確認ポイント	状況
アクセス制御	未承認AIへのアクセス制限、ホワイトリスト化	☐
認証	SSO、MFA、会社アカウント利用の徹底	☐
アップロード制御	DLPでCSV・Excel・PDF・個人情報パターンを検知・遮断	☐
ログ監視	誰がいつどのAIに何を送ったかを把握	☐
端末統制	ブラウザ拡張、外部送信アプリ、私用端末の利用制御	☐
データ加工	匿名化、マスキング、サンプルデータ利用の標準化	☐

💡 **要点：技術統制は「入れない・出さない・見逃さない」の三層で設計すると整理しやすい**

ガバナンスチェックリスト③ 委託先管理・教育

自社だけ見ていては足りない

委託先・ベンダー管理

✓ AI利用の有無と利用範囲を確認しているか
✓ 契約上、利用目的、学習利用、削除、保存先、再委託、事故通知を定めているか
✓ 監査や報告の仕組みがあるか

教育・浸透

✓ 現場向けにOK・NG事例が示されているか
✓ Shadow AIのリスクと通報方法が周知されているか
✓ 管理職・法務・情報システムの連携訓練があるか
✓ 定期見直しの指標があるか

💡 **要点：AIガバナンスの弱点は、委託先と現場教育の二か所に出やすい**

インシデント初動フロー

AI誤投入が起きたら何をするか

初動フロー（7つのステップ）

1. 検知
2. 送信停止・アクセス遮断
3. ベンダー削除依頼・学習停止確認
4. ログ保全・影響範囲確認
5. 法務・情シス・個人情報担当へ報告
6. 委託元・本人・当局対応の判断
7. 再発防止策の実装

最初の24時間

- ✓ 事実確認
- ✓ 証跡保全
- ✓ 管理者連携
- ✓ 外部照会
- ✓ 一次報告

要点：初動フローが決まっていない会社では、AI事故は“二次被害”でさらに大きくなる

出典：個人情報保護委員会資料を基に作成

「許されるAI」の序列

自社限定APIを頂点に、管理可能性で整理する

上ほど管理しやすく、下ほど原則NG

1	**自社アプリ＋法人API**	会社契約APIを社内アプリ経由で利用。SSO、RBAC、DLP、プロンプト・出力ログ、保存期間、削除条件、監査を自社で設計できる。	最も管理しやすい
2	**法人契約 Enterprise/Business版AI**	管理者コンソール、会社アカウント、学習利用オフ、ログ、DPA等を確認し、利用範囲を定めて使う。	管理しやすい
3	**会社承認済みSaaS内蔵AI**	議事録、CRM、検索、文書管理などのAI機能。SaaS側の保存・学習・外部連携・権限継承を確認する。	条件付き
4	**個人契約・無料版・ブラウザ拡張**	会社が契約・設定・ログ・削除・権限を管理できない。個人情報・機密情報・委託データの入力は原則禁止。	原則NG

結論：APIだから安全なのではない。会社が入口・出口・権限・ログを管理できるから、安全性を高めやすい。

💡 **要点：許されるAIは「便利なAI」ではなく、「会社が責任を持って管理できるAI」である**

出典：OpenAI API Data Controls、Microsoft Purview 等の公開資料を基に作成

個人情報保護委員会報告・本人通知の判断フロー

報告対象4類型から事後対応を整理する

4 まず見るべき4類型

1	**要配慮個人情報**	健康・疾患情報などを含む漏えい等のおそれ
2	**財産的被害のおそれ**	不正利用により財産的被害が生じる可能性
3	**不正目的**	不正の目的をもって行われた漏えい等
4	**1,000人超**	本人の数が1,000人を超える漏えい等

✓ 該当した場合の対応

速報	速やかにPPCへ報告（概ね3〜5日以内）
確報	原則30日以内。不正目的等は60日以内
本人通知	事態の状況に応じて速やかに通知。通知困難時は代替措置を検討
委託先事故	委託元への報告、役割分担、本人・当局対応の調整が必要

本件では疾患情報等の健康情報が問題となるため、「要配慮個人情報」類型を中心に重い事故対応が必要になりやすい。

💡 **要点：AIへの誤投入でも、報告・本人通知の判断は通常の漏えい等対応と同じく、4類型から始まる**

出典：個人情報保護委員会「漏えい等報告・本人への通知の義務化について」

委託先事故での事後対応

委託元・本人・PPC・ベンダーを同時に見る

受

委託先（RIZAP側）

事実確認、削除依頼、ログ保全、委託元報告、PPC報告・本人通知要否判断

↔

委

委託元（保険者・企業等）

委託先から報告を受け、対象者・範囲・説明内容・契約上の対応を確認

↔

AI

AIベンダー

データ保持、学習利用、削除、職員閲覧可能性、ログ保全について回答

↔

本

本人・PPC

本人通知、相談窓口、PPC報告、再発防止策の説明

実務の勘所：AI誤投入では、技術的削除・法的報告・委託元説明・本人対応が並行して走る。窓口と判断者を事前に決めておく。

💡 **要点：委託先のAI事故は、単なる社内インシデントではなく、委託元を巻き込む説明責任の問題である**

出典：RIZAP株式会社公表、IHIグループ健康保険組合公表、個人情報保護委員会資料を基に作成

Shadow AI 探知ツールの限界

ツールを入れても“見えない領域”は残る

✓ かなり見える領域

- ✓ 会社PC・会社ネットワーク経由のAIサイトアクセス
- ✓ 社内プロキシ、SASE、CASBを通るファイルアップロード
- ✓ 会社アカウントで利用する公認AIの操作ログ
- ✓ EDR/MDMで管理された端末上のアプリ・ブラウザ拡張

! 見えにくい・限界がある領域

- ● 個人スマホ、私物PC、テザリング、私用ネットワーク経由の利用
- ● TLS復号をしない場合、プロンプト本文・添付内容まで見えないことがある
- ● SaaS内蔵AI、ブラウザ拡張、外部要約ツールは単純なURLブロックで捕まりにくい
- ● DLPも画像化、暗号化、手入力、コピペ分割には限界がある
- ● 監視強化には、従業員周知・目的限定・保存期間・アクセス権限管理が必要

実務上の結論：探知ツールだけでなく、使いやすい公認AI、現場ヒアリング、自己申告しやすい文化を組み合わせる。

💡 **要点：Shadow AI対策は「監視」だけでは不十分で、正規ルート・教育・申告制度と組み合わせて初めて機能する**

出典：Microsoft、Zscaler、Netskope、Palo Alto Networks、Cloudflare等の公開資料を基に作成

まとめと役員向けの問い

“RIZAPだから起きた”で終わらせない

役員が問うべき5つ

1. **公認AIは本当に用意されているか**
2. **高リスクデータの入力を止められるか**
3. **ログで実態を見えているか**
4. **委託先まで管理できているか**
5. **事故時の初動は決まっているか**

本資料の結論

- ✓ 生成AI事故は従来の持出し事故の延長線上にある
- ✓ 問題は学習利用の有無だけではない
- ✓ 禁止規程だけでなく技術統制と正規ルート整備が必要
- ✓ Shadow AI対策はガバナンスそのものの課題である

結論：生成AIについて100%安全な組織はほとんどない。重要なのは、事故が起こり得る前提で、ルール・技術・委託先管理を一段ずつ整えることである。

主要出典：RIZAP株式会社 2026年9月3日公表、IHIグループ健康保険組合 2026年9月2日公表、個人情報保護委員会資料