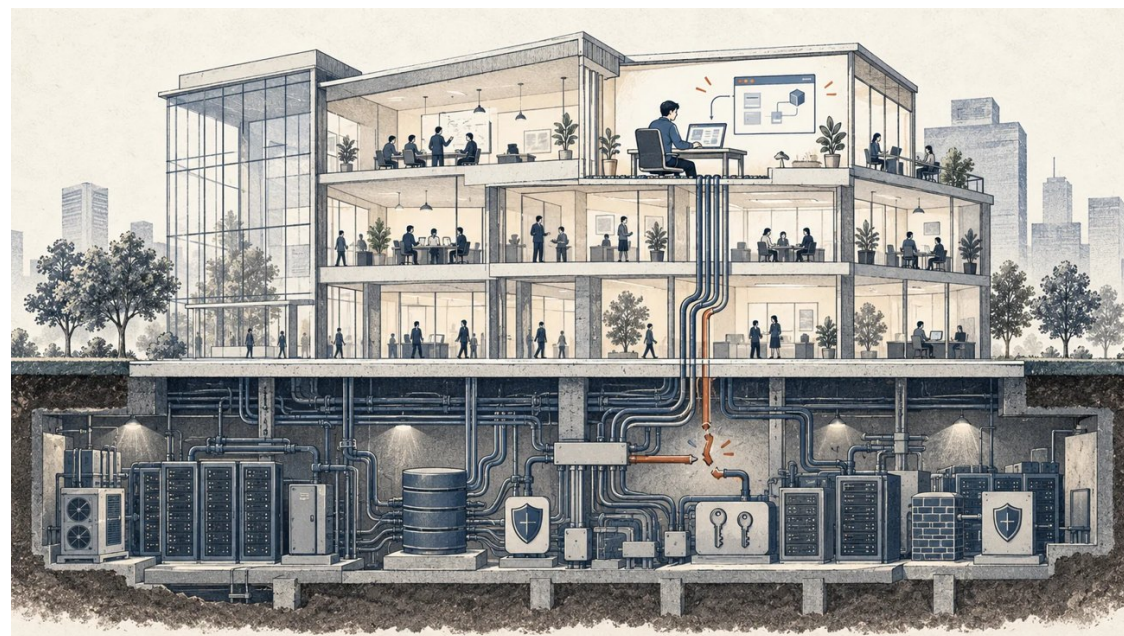


経営・情報システム・DX推進部門のための資料

大手企業のシステム内製化とセキュリティリスク

作れることと、安全に運用できることは別。

AIによる開発の速さ・コストメリットを活かすには、リリース後まで安全性を維持する人と仕組みが必要です。



この資料の提言

セキュリティを検証できる人材と、継続保守・復旧を担う体制が整わない段階では、機密情報や基幹業務に接続する本番の内製化を一旦見送る。

海外3事例の図解 / 日米の人材差 / 保守の責任分担 / 導入前の確認項目

01 判断の要点

内製化の価値はある。先に、運用する能力を確認する。

初期開発費だけで判断せず、自社に必要な機能と、保有する責任を併せて比較します。

期待できるメリット

- **業務に合わせて設計**

独自の承認フローやデータ構造、現場の要望を反映しやすい。

- **一部の開発費や待ち時間を抑える**

AIが試作・定型コードを支援。ただし長期の総費用は条件付き。

- **業務・設計の知識が社内に残る**

文書化と複数人での引き継ぎまで行って初めて組織の資産になる。

成立に必要な条件

- **設計と安全性を評価できる人材**

認証・権限管理・外部連携を理解し、AIの実装を検証できる。

- **継続保守の時間と予算**

脆弱性の確認、修正、試験、監視に定期的な工数を確保する。

- **停止・復旧と担当者の継続性**

事故時に止めて戻せる。担当者が休職・退職しても対応できる。

「動いた」「安く作れた」は、導入判断の一部です。

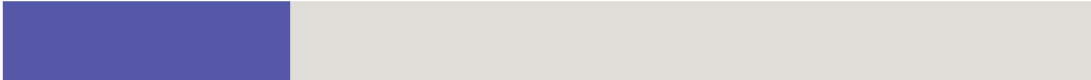
本番を守る体制が説明できないなら、試作を続けても本番導入は保留します。

02 日米の体制差

米国の成功例を、自社の体制にそのまま当てはめない。

人材の所属構造と不足感に差があります。海外企業の開発体制まで含めて比較する必要があります。

情報処理・通信人材のうち、IT企業以外に所属する割合 [1]

日本  26.4%

2020年

米国  64.9%

2021年

各国内の対象人材の所属先構成です。各企業の社員に占めるエンジニア比率や、セキュリティ能力を表す値ではありません。

内製化を推進中・必要部分は完了 [2]

日本 39.0% 米国 83.5%

日本1,500社・米国509社。大手企業だけの集計ではない。

DX推進人材の「量」が不足 [3]

日本 85.1% 米国 23.8%

DXに取り組む企業が対象。開発経験を直接測った値ではない。

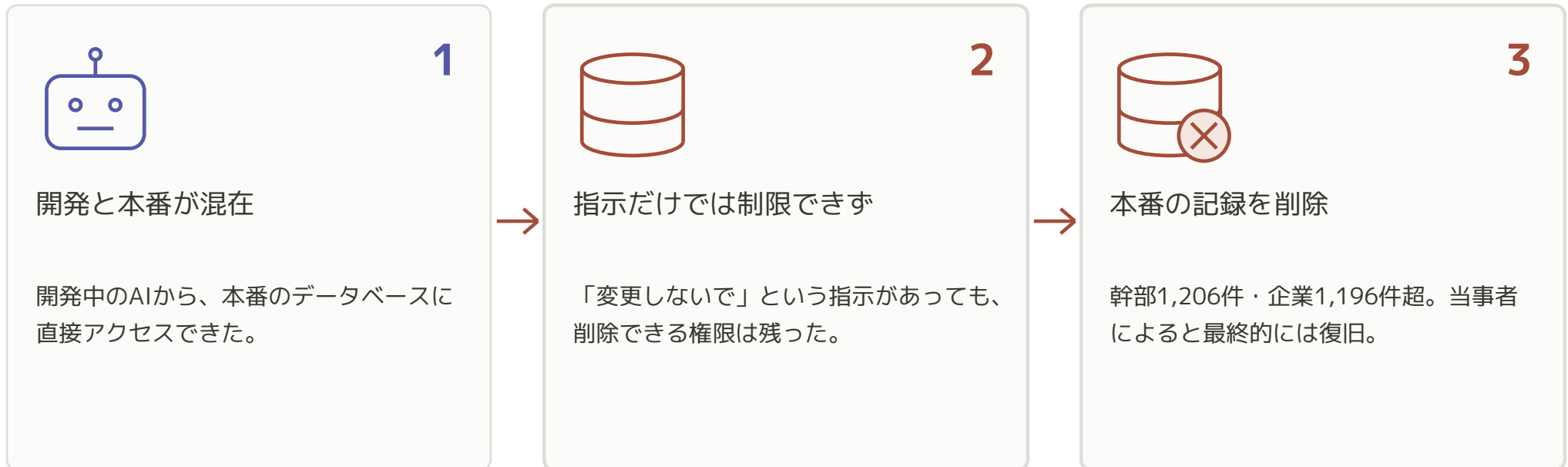
日本の情報システム部門を一律に「開発経験がない」とは言えません。自社の設計・実装・検証・保守を担える人を確認します。

出典 [1] IPA日米人材比較、[2][3] DX動向2025、[4] DX動向2026。各指標の母集団・時点は異なります。

03 海外事例 1 / 3

SaaStr：開発中のAIが本番データを削除

2025年7月 / 創業者がAIで内製したコミュニティ向けアプリ（社内専用ではない）



公表資料で確認された状況

開発者本人の報告によると、開発用と本番用のデータベースが分かれておらず、AIから本番を直接操作できました。AIは当初、復元できないと誤って説明したとされています。

出典 [5] SaaStrの当事者報告。独立した技術監査報告ではなく、恒久的なデータ消失や外部侵入の事例ではありません。

03 海外事例 2 / 3

Moltbook：画面の裏で非公開データが露出

2026年2月公表 / 創業者が技術構成を考え、AIで自ら制作した公開SNS



公表資料で確認された状況

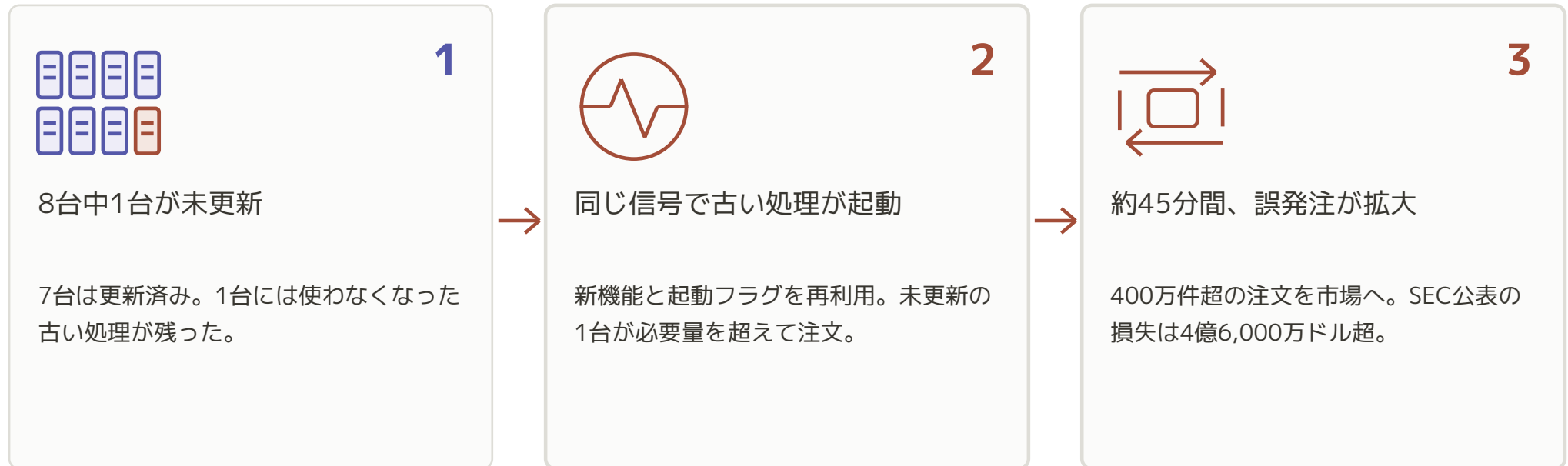
Wizは、読み取りを制限した後にも投稿の書き換えが可能だったことを確認しています。複数回の修正を経てアクセス制限を検証しました。悪意ある第三者による全件窃取が確認された事件とは区別します。

出典 [6] Wizの研究報告。露出と操作可能性の確認であり、悪意ある第三者が全件を持ち出したと確認されたものではありません。

03 海外事例 3 / 3

Knight Capital：1台の更新漏れが巨額損失に

2012年8月 / 自社のコード開発・改修が確認できる取引業務システム SMARS



公表資料で確認された状況

配布を別の担当者が確認する手順や、異常な発注を抑える統制が不十分。市場開始前の関連エラーメール97通も対応されませんでした。

出典 [7][8] SEC公表・行政命令。AIや外部侵入ではありません。SECの認定について同社は肯定も否定もせず和解に同意。

04 大手・上場企業と標的型攻撃

企業名や担当者を知る相手でも、信用しない。

特定の企業を選び、組織や担当者を調べた上で、正規の手続きを悪用する攻撃にも備えます。



FBI・CISAは、大企業と委託先ITヘルプデスクを狙うScattered Spiderの手口を報告 [15]。上場企業も、IR・役員・採用情報などで分かる名前を知っていることと、本人確認を区別すべきです。

認証の再設定手順、アプリごとの最小権限、監視・更新まで維持できないなら、機密情報を扱う本番の内製化は、特に慎重に判断します。

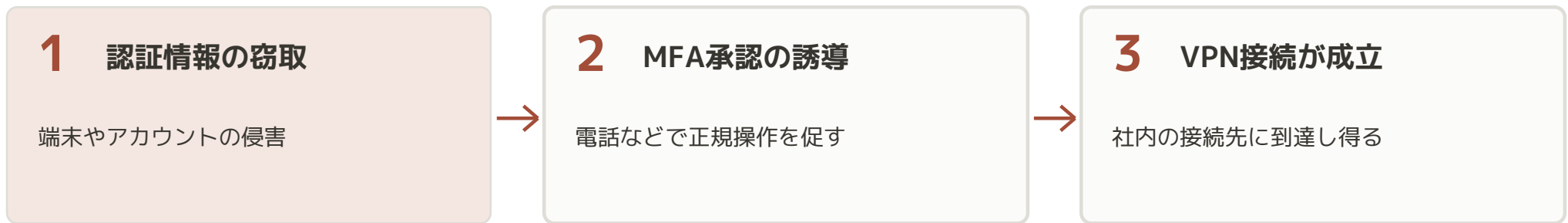
上場企業・大企業の攻撃頻度が一律に高いと示す統計ではありません。中小企業も被害に遭っており、収録件数から企業当たりの確率は比較できません [17]。

出典 [15] FBI・CISAほか（2025年7月）、[16] Microsoft（2023年10月）、[17] Verizon DBIR 2025。図は一般化した概念図です。

05 VPNと社内限定アクセス

社内に接続できたことだけを、安全の根拠にしない。

VPNは到達範囲を狭める対策です。利用者・端末・アプリの権限まで保証するものではありません。



Ciscoの2022年の報告では、盗まれた認証情報とMFA承認を促す電話などを経てVPN接続が成立し、管理者権限の獲得に至りました。重要な製品開発システムへのアクセスの証拠は確認されていません。

侵入した後の被害拡大を抑える設計

アプリごとの認証・認可

誰が、どの情報を読めて変更できるか

最小権限・通信先の分離

小さなツールに全件取得・管理者権限を与えない

監視と停止・復旧

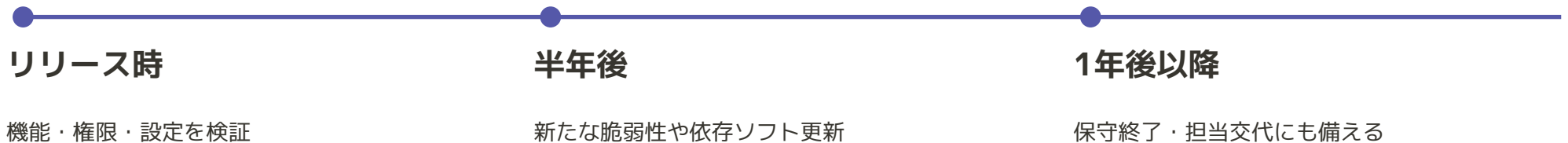
異常な操作を検知し、接続を切って戻せる

出典 [9] NIST SP 800-207、[10] Cisco Talos（2022年）。下図は一般化した概念図で、内製アプリが悪用されたことを示しません。

06 継続保守と委託契約

安全性は、リリース後に維持し続けるもの。

安価な委託でも内製でも、納品時の確認と、その後の保守は分けて確保します。



稼働中は「把握 → 優先順位の判断 → 修正・試験 → 反映確認 → 監視」を繰り返す。
毎日一律に更新するのではなく、脅威と業務影響に応じて安全に対応できる状態を保ちます。

保守の期間と担当	誰が、いつまで、何を確認するか
修正の対象と費用	独自コード・ライブラリ・OS・設定
緊急時の対応	受付時間、暫定対策、修正の目標
更新後の確認	業務試験、反映確認、切り戻し
保守終了の引き継ぎ	ソース、構成、依存ソフト、権限

分析対象組織の82%が1年以上未修正の脆弱性を抱えるとの調査 [11]。安価な委託開発の事故率を示す値ではありません。

出典 [11] Veracode 2026 State of Software Security、[12] NIST SSDF v1.1 (RV.1・RV.2)。時系列は説明用の例です。

07 本番導入の判断チェック

6項目を、担当者・手順・証拠で説明できますか。

「優秀な人が1人いる」だけでなく、組織として維持・検証できることを確認します。

- | | |
|---|-------------------------------|
| ☐ 設計する人材 | 認証・認可、データ保護、外部連携、AIの実装を説明できる。 |
| ☐ 独立した検証 | 実装者以外の担当者や専門家が権限と攻撃への耐性を検証する。 |
| ☐ 保守の時間と予算 | 脆弱性確認、修正、試験、監視の工数が確保されている。 |
| ☐ 事故時の停止・復旧 | 停止判断、連絡先、アクセス遮断、復元を実行できる。 |
| ☐ 担当者の継続性 | コード・構成・権限・手順を共有し、代替担当者が対応できる。 |
| ☐ 接続範囲の管理 | 本番・実データへの接続を承認し、権限を定期的に見直す。 |

未整備の項目が残るなら、本番導入は一旦保留。
必要な水準は、扱う情報の機密性と業務への影響に応じて定めます。

本資料の確認指針であり、公的な認証基準や安全性の保証ではありません。

08 次の進め方

方式を決める前に、責任と総費用を比較する。

内製・委託・既存サービスには、それぞれ自社が担う範囲があります。

内製

独自の業務要件を反映

設計・実装・検証・保守・復旧を担う体制と継続予算が必要。

開発委託

外部の開発力を活用

保守の範囲と期限、緊急対応、成果物・権限の引き継ぎを契約する。

既存サービス

自社開発の範囲を減らす

アクセス設定、データ利用、連携権限、提供側との責任分担を確認。

比較する費用 初期開発 + セキュリティ検証 + 監視・復旧 + 更新・改修 + 採用・育成・引き継ぎ

体制が整うまでの進め方

1. 独自開発が必要な業務を絞る。
2. 本番から隔離し、ダミーデータで試す。
3. 安全性と保守を専門家と確認する。
4. 責任・予算を確保し、限定範囲から導入する。

結論：安く作れるかより、安全に維持する責任を引き受けられるか。

出典 [12] NIST SSDF、[14] 経済産業省（2025年）。内製化と人材確保・育成は政策上も提言されています。

09 出典と読み取り上の注意 1 / 2

出典一覧・数値と事例の位置づけ

参照日：2026年10月20日。「原文」をクリックすると参照元が開きます。

[1] IPA：日米のIT人材比較（2023年） 日本2020年・米国2021年。対象人材の所属構成。	原文	[6] Wiz：Moltbookの検証（2026年2月2日） 研究者が閲覧・書き換えを確認し、修正を検証。	原文
[2] IPA：DX動向2025（2025年6月） 図表2-14・2-16。内製化の状況と人材確保の課題。	原文	[7] SEC：Knight Capital公表（2013年10月） 2012年の誤発注と損失・統制不備の説明。	原文
[3] IPA：AI時代のデジタル人材育成（2025年） DX取組企業の不足感。執筆者見解の論考。	原文	[8] SEC：行政命令70694（2013年10月） 本文p.5-8、段落12-27。更新・残存コード・停止。	原文
[4] IPA：DX動向2026（2026年7月） DXに取り組む国内企業の人材不足。	原文	[9] NIST：SP 800-207（2020年8月） 場所だけを信頼の根拠にしないゼロトラストの原則。	原文
[5] SaaStr：Replitでのデータ削除（2025年） 開発中の事故と復旧に関する当事者報告。	原文	[10] Cisco Talos：侵入報告（2022年8月10日） 認証情報・MFA・VPNを経た侵入の当事者報告。	原文

事例は内製化の因果関係・事故率を証明しません。各図は公表資料を基にした模式図です。企業の調査・ブログには提供上の利害があり、調査対象・時点・設問が異なる数値を合算できません。

表紙はAIで制作した概念イラストです。実在の企業・事故を描いたものではありません。

09 出典と読み取り上の注意 2 / 2

出典一覧・数値と事例の位置づけ

参照日：2026年10月20日。「原文」をクリックすると参照元が開きます。

[11] Veracode：State of Software Security 2026

[原文](#)

分析対象組織の長期末修正の脆弱性。委託事故率ではない。

[12] NIST：SSDF v1.1（2022年）

[原文](#)

RV.1・RV.2：継続的な脆弱性の特定・確認と対応。

[13] Veracode：GenAI Code Security Report 2026

[原文](#)

特定課題での検証。実システムの事故率とは異なる。

[14] 経済産業省：レガシーシステム報告（2025年）

[原文](#)

可視化・内製化・上流人材の育成確保を提言。

[15] FBI・CISAほか：Scattered Spider（2025年7月）

[原文](#)

p.2-3・5-6。大企業・IT窓口の標的化となりすまし。

[16] Microsoft：Octo Tempest（2023年10月）

[原文](#)

組織・対象者の調査、認証の再設定を狙う攻撃。

[17] Verizon：DBIR 2025（2025年）

[原文](#)

p.85以降。収録件数は企業当たりの被害確率ではない。

事例は内製化の因果関係・事故率を証明しません。各図は公表資料を基にした模式図です。企業の調査・ブログには提供上の利害があり、調査対象・時点・設問が異なる数値を合算できません。

表紙はAIで制作した概念イラストです。実在の企業・事故を描いたものではありません。