KEEPER®

# ホワイトペーパー：

# 国内企業のDX化への現状と課題

企業や組織のDX化を素早く実施する方法とは？

# 目次：

# はじめに

経済産業省は、企業のデジタルトランスフォーメーション（DX）の進行が遅れることは、国全体にとって大きな損害をもたらす可能性があると指摘しています。大規模な経済損失が発生する時期が2025年以降と言われる理由として、21年以上稼働している基幹システムの割合が6割に達する時期が2025年となることや、それらのシステムのサポート期間が終了する時期もこの2025年が該当することが挙げられます。

このため、2025年のDX化を推進する目標達成には、企業側の取り組みだけでなく、国家レベルでの施策の導入も求められている状況です。では、DX化にはどのような課題があり、どのようなソリューションによってDX化を素早く実施することが可能となるのでしょうか。

ここでは、Keeper SecurityがTrendCandy Research社と協力 し、800名以上のITおよびセキュリティ担当者を対象とし て2024年に実施した世界規模の調査より、100名の日本企業担当者の回答を抽出してデータを提供しています。また、その他のデータでは、一般に公開されている各データに基づいてDX化や日本の現状を詳しく説明し、DX化を簡素化して実現する方法を解説しています。

# DX化とは？

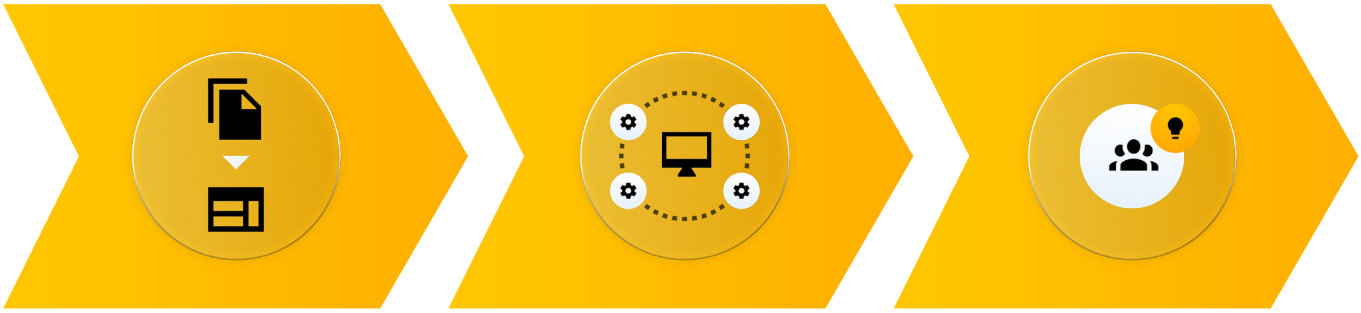
DX化、すなわちデジタルトランスフォーメーションとは、デジタル技術を駆使して企業や組織のビジネスモデル、業務プロセス、企業文化を根底から変革し、それによって新たな価値を創出し、競争力を高める活動を指します。企業のDXに関する自主的取組を促すため、経済産業省は2022年9月、既存の「デジタルガバナンス・コード」と「DX推進ガイドライン」を統合し、「デジタルガバナンス・コード2.0」として、経営者がDXを通じて企業価値向上の推進のために実践することが必要な事項を公表しました。

## IT化とDX化の違いとは？

IT化は、日々の業務や作業をデジタルに置換し、効率性や信頼性を向上させることを目的としています。具体的には、手作業などのアナログで対応していた業務を、IT技術を用いて自動化したり迅速化したりすることを意味します。

一方、DX化は、サービスをデジタル技術を使って根本的に製品・サービス・ビジネスモデルなどを変革し、新しい価値を生み出して競争上の優位性を確立することを指します。DX化は、単に技術を導入するだけでなく、組織のマインドセットやカルチャーの変革も伴う必要があり、全社員がデジタル技術の活用と変革に向けた意識を持つことが成功の鍵とされています。

DXの実施に先立って、アナログ・物理データのデジタル化という「デジタイゼーション」、次に業務プロセス全体をデジタル化する「デジタライゼーション」という段階があります。IT化とは、ここで言うところの最初のステップである「デジタイゼーション」にあたります。



**デジタイゼーション**
アナログデータ・業務の
デジタル化

**デジタライゼーション**
業務のプロセス・フローの
デジタル化

**DX**
デジタル化によってビジネスや社会に
変革を与える

出典元：Crossmedia Marketing「DX（デジタルトランスフォーメンション）とは？IT化と違いを徹底解説」IT?”

# 日本でDX化が必要な背景とその課題

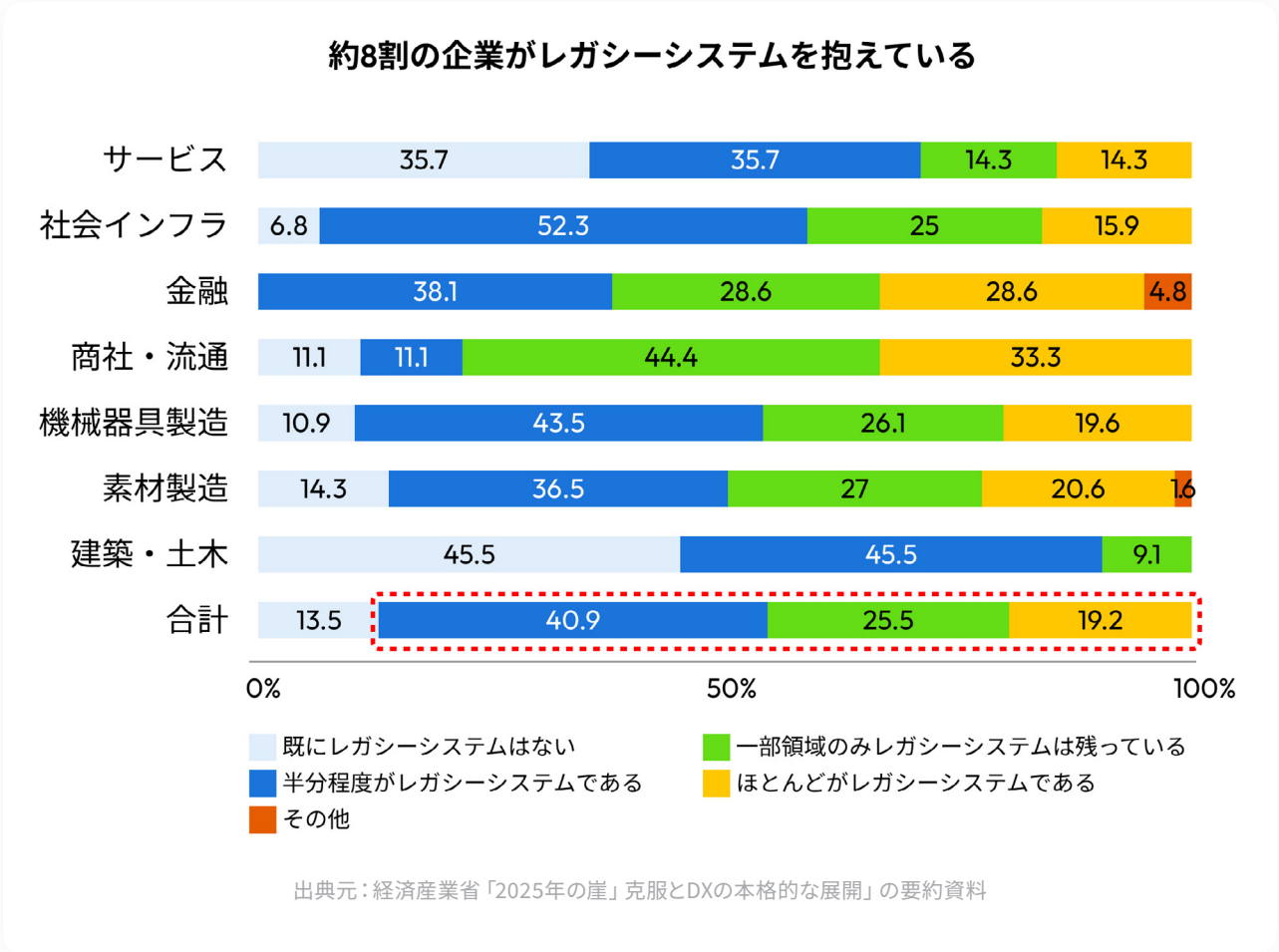
## 経済産業省が発表した「2025年の壁」問題

経済産業省の「DXレポート」では、「2025年の崖」という概念を提示しています。これは、2025年までに多くの企業が直面する基幹システムの老朽化とIT人材不足の問題を指しています。これらの問題を解決しなければ、2025年以降で毎年最大12兆円もの経済損失が生じる可能性を示唆し、大規模な経済的損失をもたらす可能性があると警告しています。

日本国内企業、特に中小企業はDX化が遅れていると言われており、「2025年の崖」による損失を回避するために、DX化を国全体で早期に進めていく必要があるとされています。

## レガシーシステムの継続的な使用

多くの日本企業では、未だに何十年も前から同じ老朽したシステムを使用し続けている会社も多く存在します。経済産業省が実際に発表した「2025年の崖」克服とDXの本格的な展開」の要約資料によると、日本企業の約80%は時代遅れのシステムを抱えているのが問題とされています。



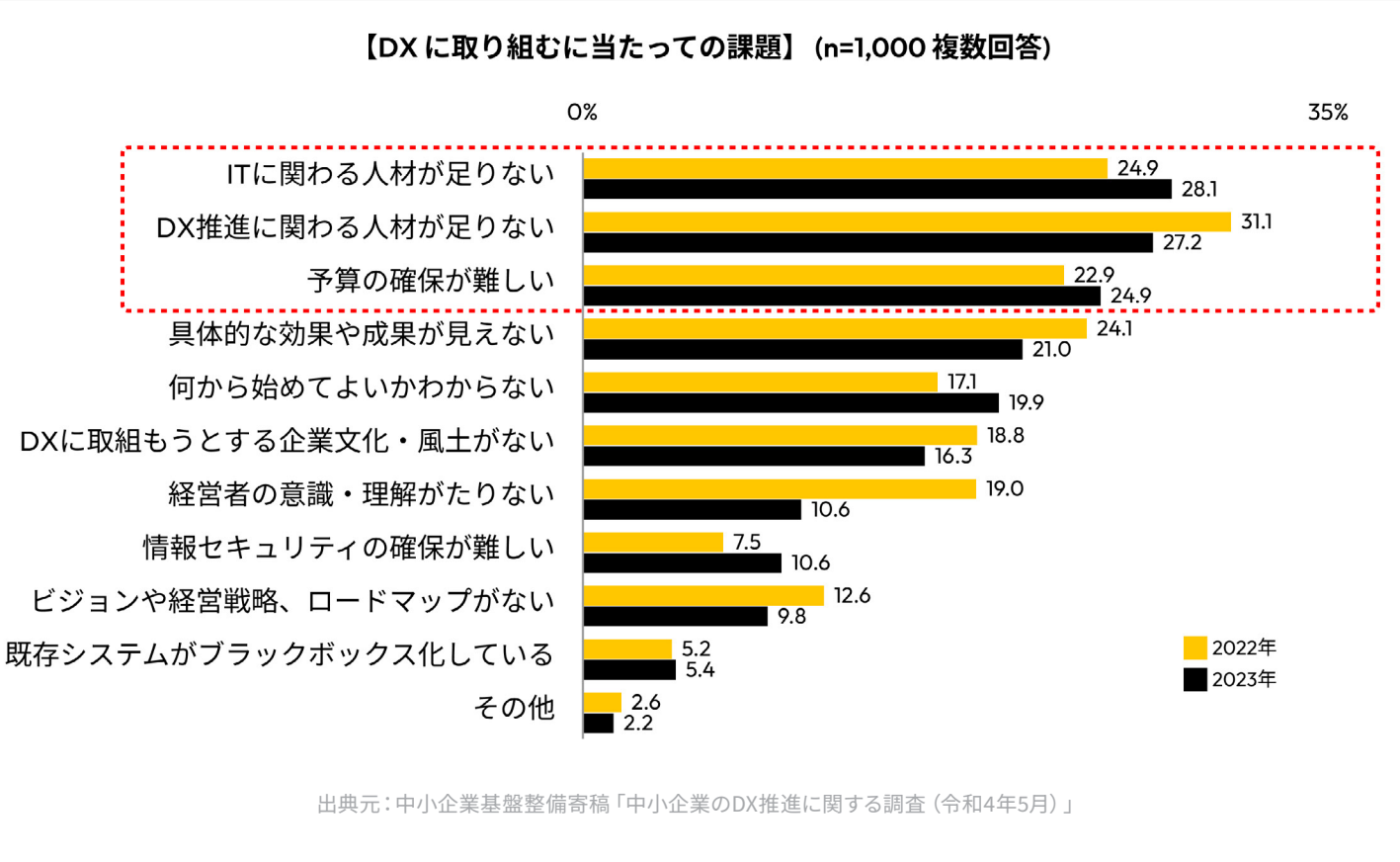

出典元：経済産業省「2025年の崖」克服とDXの本格的な展開」の要約資料

## IT人材の不足と負担

少子高齢化が進む中、労働力不足とその結果としての生産性の低下は重要な問題となっています。結果、日本では、各企業のIT人材の確保が大きな課題となっています。経済産業省のレポートによると、2025年には43万人のIT人材が不足すると推定されています。よって、DXを進めるには、IT人材の確保が必要になっています。

しかし、上記の通りレガシーシステムを利用する企業も多いことから、ITチームの作業負担が増えている傾向にあり、IT人材のより高い需要があることによって、人材獲得の困難さに拍車がかかっています。

そこで、業務自動化、AIの導入、ロボット技術の利活用を通じて作業効率を高め、人材不足を補いつつ生産性を向上させることにより、このIT人材不足のギャップを埋めることが可能になります。

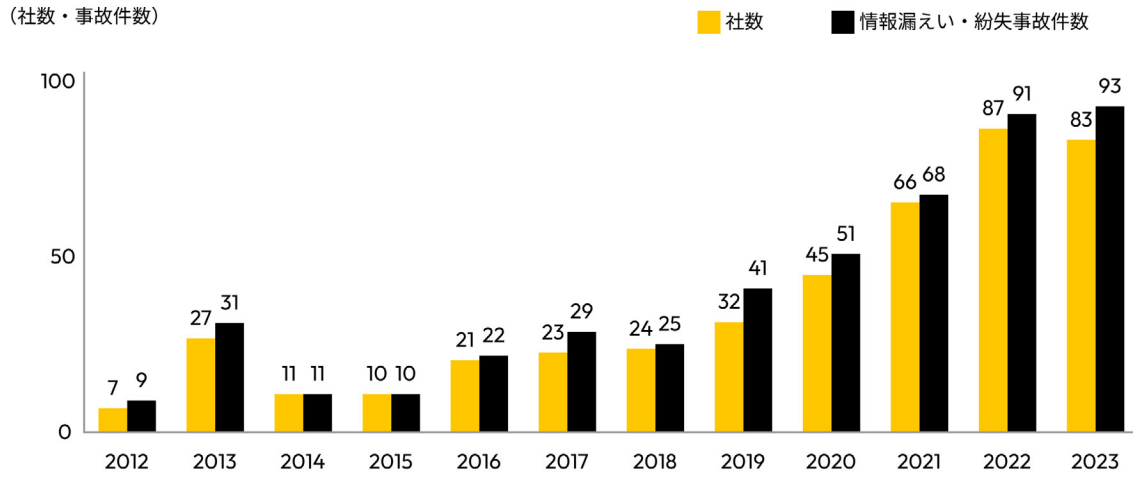



出典元：中小企業基盤整備寄稿「中小企業のDX推進に関する調査（令和4年5月）」

## データ管理の問題

企業内のデータの集約、管理、分析の向上は必須であり、また課題となっています。多くの企業ではデータが分散しており、一元的なデータ管理や分析が難しい状況にあります。それだけでなく、ログイン情報なども手動で管理されている企業もあり、個人に管理を任せている企業さえあります。これは、そのログイン情報を持つ人が退職してしまったり、内部脅威によってログイン情報が漏洩してしまったり、紛失してしまう可能性があることを意味します。

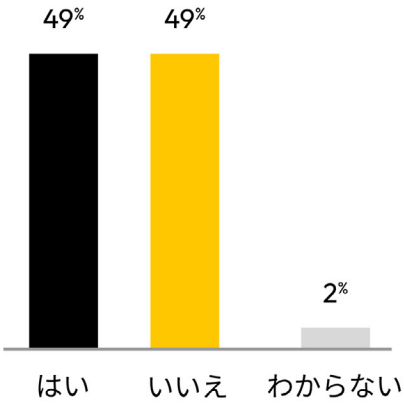
**ウィルス感染・不正アクセスによる事故　発生推移**



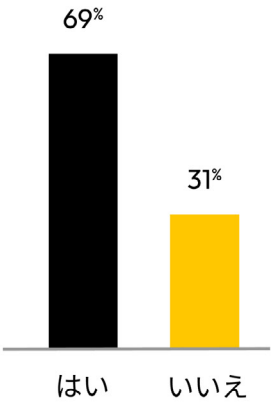

2023年に発覚した事故では、従業員が不正に個人情報を持ち出し、第三者に流出させる事例が多く、ガバナンスの徹底の重要性が顕著に表れる。

2023年の東京商工リサーチ「上場企業の個人情報漏えい・紛失事故」（日本経済新聞より）

**従業員から情報漏洩の被害を受けたことがありますか？**



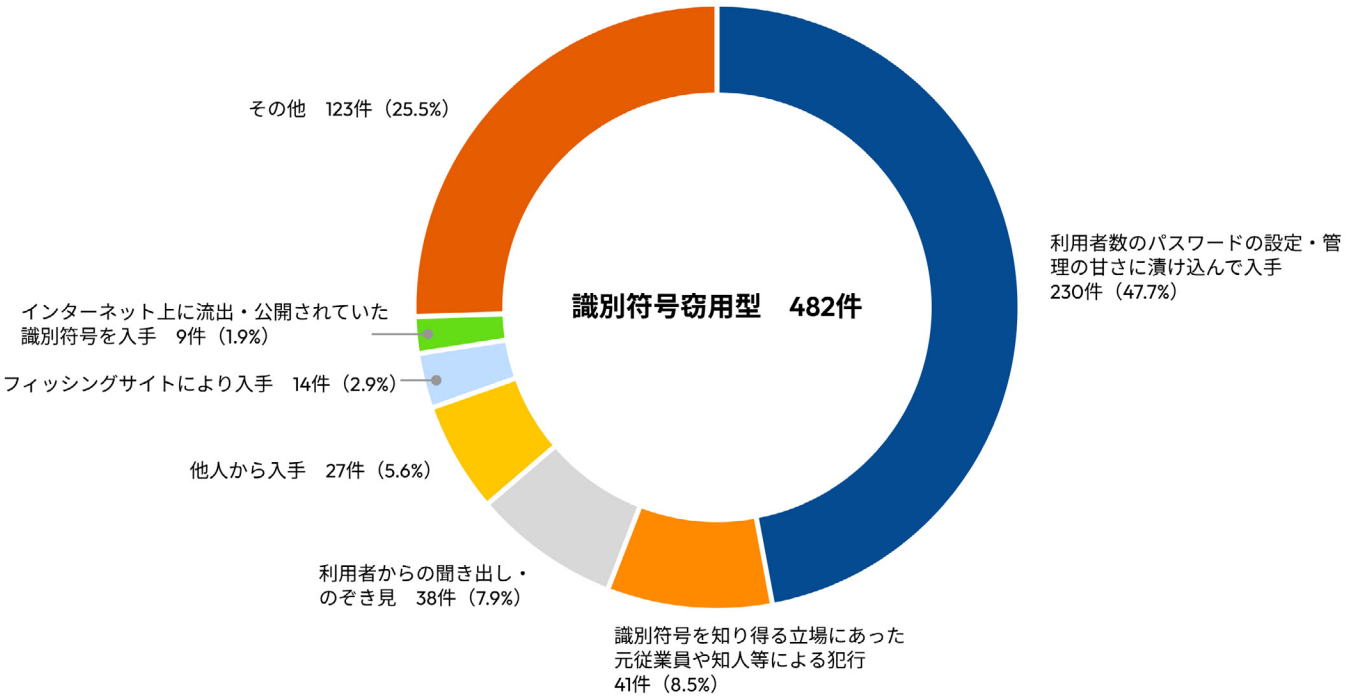

**社内ITチームは、頻繁に盗まれるパスワード管理方法に悩んでいますか？**




Keeper Security 独自の日本国内IT管理者を対象としたアンケート調査の結果より（2024年1月実施）

また、2022年での警視庁の調べによると、不正アクセス禁止法違反の国内検挙件数は522件と、前年同期と比べて93件増加しています。検挙件数のうち、482件が識別符号＊窃用型で全体の92.3%を占めました。また、「利用権者のパスワードの設定や管理の甘さに付け込んで入手」は一番多く、47.7%と結果が表れています。

**不正アクセス禁止法違反の国内検挙件数のうちの識別符号窃用型の内訳**



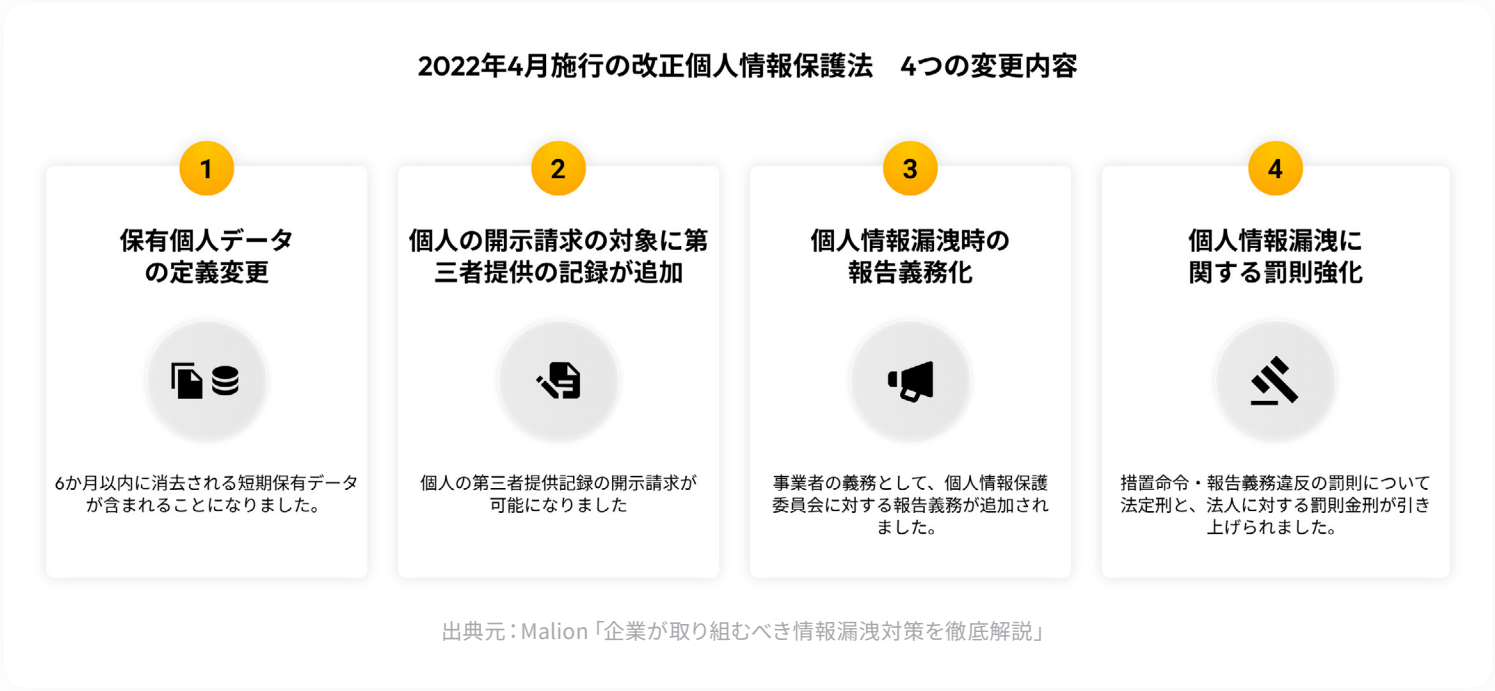

*識別符号とは、パスワード、指紋や虹彩などの影像または音声、署名等から作成される符号と警視庁によって定義されています。

出典元：警視庁「令和4年（2022年）におけるサイバー空間をめぐる脅威の情勢等について」

## セキュリティとプライバシー

デジタルトランスフォーメーション（DX）と同時に懸念されるのが、セキュリティとプライバシーのリスクです。DXが進むにつれ、大量のデータが収集・分析されるようになり、特に個人情報や機密情報を含むデータは、その保護のためのセキュリティ対策を複雑にします。

2022年4月施行の改正個人情報保護法では、以下のような保有個人データの定義見直しや個人情報利用・漏洩に関する変更などが行われ、情報漏洩した際の経済的損失が大きくなる可能性が高まりました。これにより、さらに情報漏洩対策を徹底する必要性が高まりました。

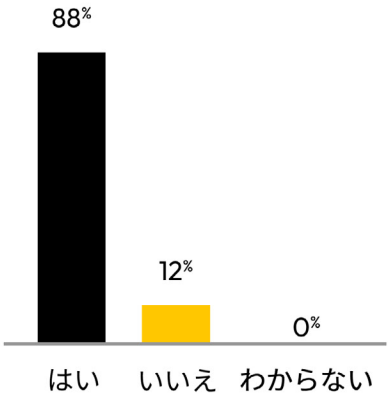



出典元：Malion「企業が取り組むべき情報漏洩対策を徹底解説」

サイバー攻撃は日々進化し、ランサムウェア、フィッシング、マルウェアなど、様々な手法が登場しています。また、企業がグローバルでの取引をする際に、日本国内の個人情報保護法だけではなく、GDPR（一般データ保護規則）やPCI DSSなどの各国・地域のコンプライアンス規制に準拠する必要が出てきます。そのため、より高度なセキュリティ向上と規制遵守が求められてきます。

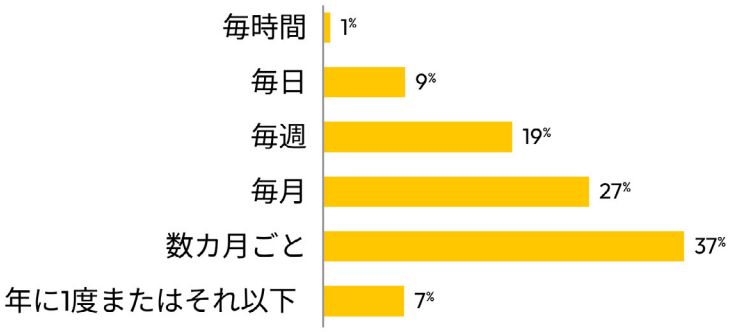
## サイバー攻撃の実情

**過去12ヶ月の間にサイバー攻撃による損害を受けましたか？**



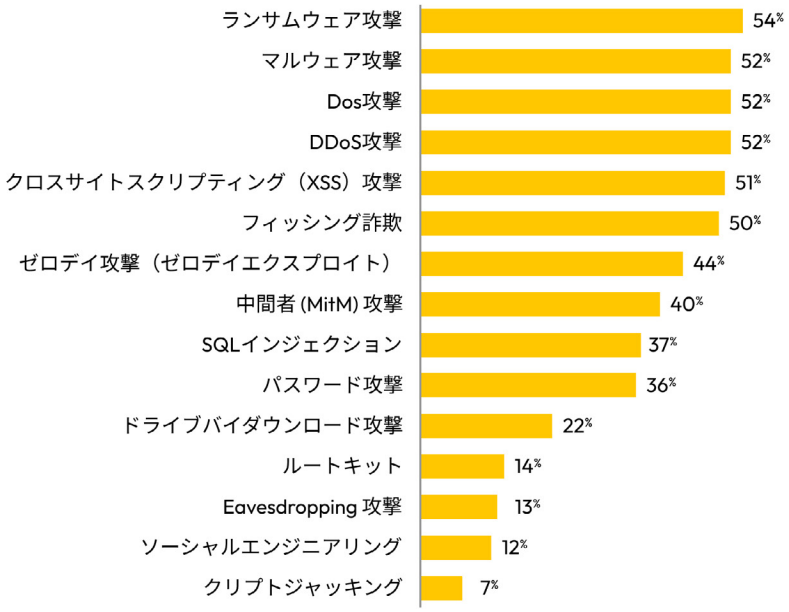

Keeper Security 独自の日本国内IT管理者を対象としたアンケート調査の結果より（2024年1月実施）

**貴社に対するサイバー攻撃の頻度について、最も適切なものはどれですか。**




Keeper Security 独自の日本国内IT管理者を対象としたアンケート調査の結果より（2024年1月実施）

## 貴社に対しての最も一般的なサイバー攻撃はどれですか？（複数回答可）




Keeper Security 独自の日本国内IT管理者を対象としたアンケート調査の結果より（2024年1月実施）

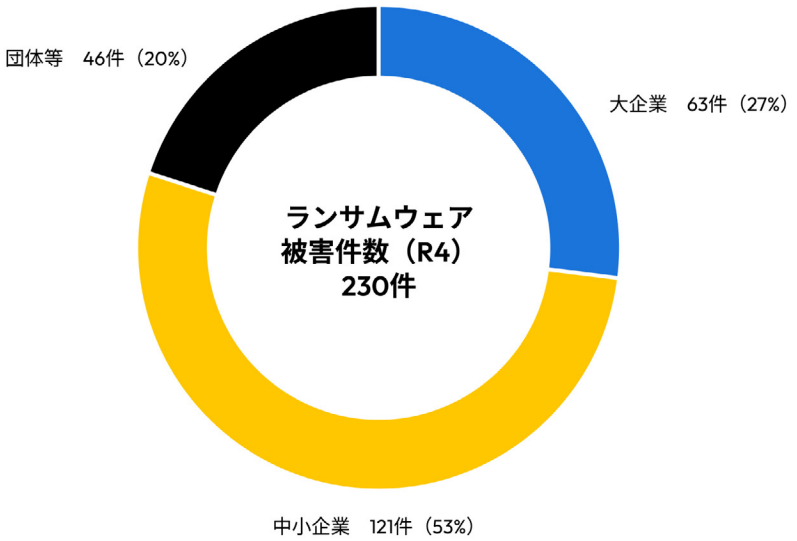
## 2023年の組織における情報セキュリティの脅威

| 2023年順位 | 組織における情報セキュリティ脅威 | 前年順位 |
|---|---|---|
| 1位 | ランサムウェアによる被害 | 1位 |
| 2位 | サプライチェーンの弱点を悪用した攻撃 | 3位 |
| 3位 | 標的型攻撃による機密情報の窃取 | 2位 |
| 4位 | 内部不正による情報漏えい | 5位 |
| 5位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 4位 |
| 6位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | 7位 |
| 7位 | ビジネスメール詐欺による金銭被害 | 8位 |
| 8位 | 脆弱性対策の公開に伴う悪用増加 | 6位 |
| 9位 | 不注意による情報漏えい等の被害 | 10位 |
| 10位 | 犯罪のビジネス化（アンダーグラウンドサービス） | 圏外 |

ランサムウェアの脅威は3年連続1位であり、サプライチェーンの弱点を悪用した攻撃は業務停止を招く事例もある。

出典元：独立行政法人情報処理推進機構 (IPA)「情報セキュリティ10大脅威 2023　組織における情報セキュリティ脅威」

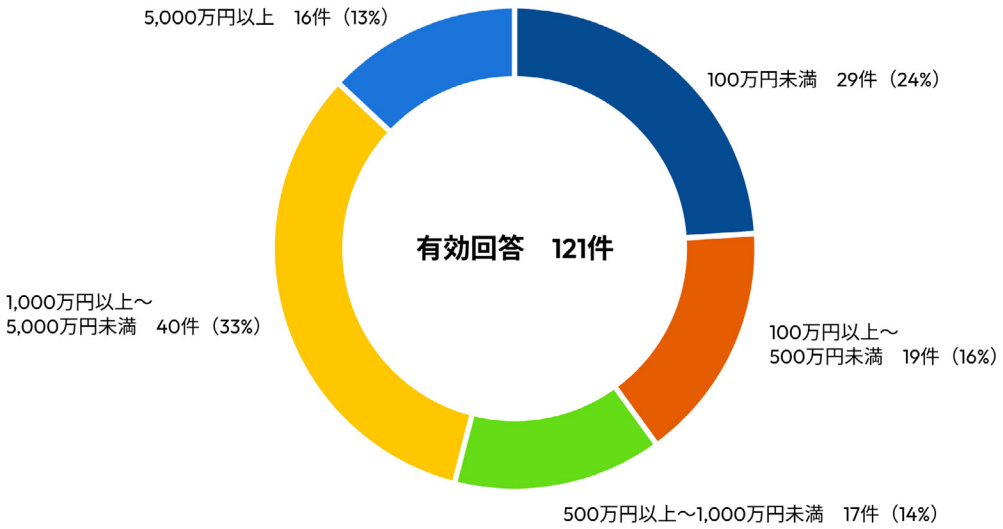
### ランサムウェア被害の企業・団体等の規模別被害件数




中小企業や非営利団体が、ランサムウェア被害全体の73%を占める。

出典元：2022年警視庁報告「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

### ランサムウェア被害の調査・復旧費用の総額




ランサムウェア攻撃からの被害金額は、60%以上が各社・団体500万円を超える結果に。

出典元：2022年警視庁報告「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

# 企業のDX化に役立つパスワードマネージャー

独立行政法人情報処理推進機構の「情報セキュリティ10大脅威 2023」によると、多数の脅威がある中で、攻撃の糸口はすべて似通っており、基本的な対策の重要性は長年変わらず、情報セキュリティ対策は常に意識するべきという説明がされています。

また、その中でも攻撃の糸口として「パスワード窃取」があげられており、「パスワード窃取によるリスクを低減する」ための対策として、「パスワードの管理・認証の強化」を挙げています。

| 攻撃の糸口 | 情報セキュリティ対策の基本 | 目的 |
|---|---|---|
| ソフトウェアの脆弱性 | ソフトウェアの更新 | 脆弱性を解消し攻撃によるリスクを低減する |
| ウィルス感染 | セキュリティソフトの利用 | 攻撃をブロックする |
| パスワード窃取 | パスワードの管理・認証の強化 | パスワード窃取によるリスクを低減する |
| 設備不備 | 設定の見直し | 誤った設定を攻撃に利用されないようにする |
| 誘導（罠にはめる） | 脅威・手口を知る | 手口から重要視するべき対策を理解する |

出典元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2023」

これまでの説明からもわかるように、日本国内の特に中小企業の多くは、企業や組織のDX化に多くの課題を抱えています。その解決策の一つが、パスワードマネージャーを使い、社内のセキュリティを確保し、DXの迅速な導入を支援することです。しかし、すべてのパスワード管理ツールが同じようにできているわけではありません。

## ブラウザのパスワードマネージャーは安全？

ブラウザのパスワードマネージャーとは、例えばGoogle Chrome などのウェブブラウザに組み込まれているパスワード管理機能のことです。最近のブラウザでは、登録したウェブサイトでアプリのログイン情報またパスワードを次回ログインする手間を省くために、ブラウザ上に保存することが可能です。これらは無料で提供され、一見実用的な機能と言えるかもしれません。また、ブラウザのパスワードマネージャーとパスワード管理に特化したパスワードマネージャーとの違いが分からないという方も多く存在するのではないでしょうか。

ブラウザに内蔵されているパスワード管理機能は、サイバーセキュリティ的に安全とは言えません。その理由は、Webブラウザのパスワードマネージャーは、Webサイトにアクセスする目的で設計されており、プライバシーを保護する目的ではつくられていないからです。その便利さがアカウントを脆弱にし、悪意のあるものが侵入した場合、セキュリティに重大なリスクをもたらす場合もあります。

### ブラウザでのパスワード管理の注意点

- ブラウザにログインしたままになり、サイバー犯罪者がアクセスするとパスワードを見ることができる
- 使用は特定のブラウザに依存している
- パスワードの使い回しを管理者が検知することができない
- 脆弱なパスワードの利用を管理者が検知することができない
- パスワードの漏洩を管理者が検知することができない
- パスワードを他人に安全に共有することができない
- フィッシングやキーロガー、マルウェア等の攻撃にさらされる可能性が高い

### Google Chrome（クローム）などのブラウザのパスワードマネージャーとの違いは？

| 機能 | KEEPER | ブラウザ |
|---|---|---|
| パスワード保管・保護 | ○ | △ |
| パスワードの暗号化 | ○ | ○ |
| パスワード自動生成・入力 | ○ | ○ |
| パスワードの共有 | ○ | × |
| マルチ環境対応 | ○ | × |
| パスワードの使い回し検知 | ○ | △ |
| 弱いパスワードの利用検知 | ○ | △ |
| パスワード漏洩検知 | ○ | △ |
| シークレット管理 | ○ | × |

○ ＝最良　△ ＝可　× ＝不可

そこで、Keeperのパスワードマネージャーが、どのようにDX化に役に立ち貢献できるのかを詳しくご紹介します。

# DX化に役立つKeeper パスワードマネージャーのご紹介

## セキュリティの向上

Keeperのパスワードマネージャーを活用してセキュリティが向上する理由には、以下のようなポイントが挙げられます

- ゼロ知識暗号化の採用
- ゼロトラストセキュリティモデル
- 多要素認証(MFA)や2要素認証(2FA)のサポート
- 容易な最小特権アクセス管理
- 自動でパスワードの定期的な変更が設定可能

DX化の中でも懸念されているのが、サイバーセキュリティの脅威の増加です。Keeperのパスワードマネージャーは、最先端のセキュリティ技術を駆使して、企業のデジタル資産を守ります。

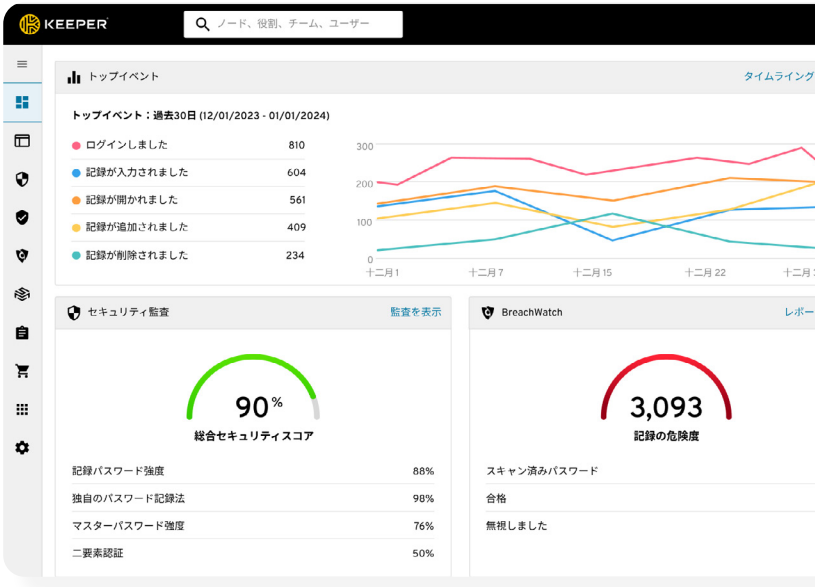
ゼロ知識暗号化の原則に基づき、ゼロトラストセキュリティモデルを採用という高度な暗号化技術を活用してパスワードや機密情報を保護しています。また、Keeperの従業員でさえ、ユーザーのパスワードやデータの内容を知ることができない仕組みのため、完全に安全な管理が可能です。さらに、不正アクセスやデータ漏洩のリスクを最小限に抑えるために、多要素認証(MFA)の導入が可能で認証プロセスを一層強化できます。

加えて、簡単に詳細な権限を設定できる機能も備えています。よって、最小特権アクセスの原則を企業内で実施することにより、従業員は必要最小限のアクセス権限のみを与えられるため、セキュリティの向上とリスク管理が図れます。

## アカウント情報の可視性が向上

どのように可視性が上がるのかを簡単にご紹介すると、以下のようなものがあります。

- 一元管理できる管理者ダッシュボード
- アカウント漏洩時のリアルタイムのアラート
- BreachWatchによるダークウェブモニタリング機能
- セキュリティポリシーの遵守状況
- ロールベースのアクセス制御（RBAC）




強力なパスワード管理機能により、企業が多数のアカウントとパスワードを一元的に管理するのを助けます。従業員が各自使用する複数のサービスやアプリケーションへのアクセス情報をKeeperに保存することにより、ログイン情報の検索や入力の手間が省け、作業効率が大幅に向上します。また、アクセス権限の管理も容易になり、必要な時に迅速にアクセス権を変更・削除できるため、セキュリティを保ちながらも柔軟なアクセス管理が可能になります。

## 利便性の良さにより社内全体の生産性が向上

Keeperのソリューションでどのように利便性が上がるのかを簡単に挙げると、以下のようなポイントがあります。

- 1つのマスターパスワードのみでボルトにアクセス可能
- 自動入力ログイン機能
- 多様なデバイスに対応・アクセス可能
- アクセス権の簡単な変更や割り当て
- 安全なログイン情報の共有

Keeperのパスワードマネージャーで企業内のアカウント情報を管理することで、従業員は個々のサービスやアプリケーションのパスワードを一つ一つ覚える負担から解放されます。必要なのは、マスターパスワードのみを記憶しておくことだけです。

それだけでなく、SNSマーケティング用のアカウントなど、複数人でアカウント情報の共有が必要な場合でも、パスワードを安全に共有できたり、アカウントログイン時に自動入力を補助してくれたりするため、効率性が上がります。また、パスワード忘れの問題がほぼ皆無となるので、IT ヘルプデスクにパスワードのリセットを依頼する案件が減り、IT チームと従業員の両方の時間が節約されます。このように、パスワードマネージャーの利便性により、社内全体の生産性が向上されます。

## 監査とコンプライアンスのサポート

DX化だけではなく、日本企業がグローバル化を果たすとともに求められるのが、コンプライアンスの遵守です。Keeperは、アクセスログの詳細な記録、セキュリティポリシーの適用、ユーザー行動の監視機能を提供し、企業が規制要件に準拠しやすくなるサポートをします。これにより、監査時に必要な情報を迅速に提供できるため、コンプライアンスと監査のプロセスが大幅に効率化されます。

Keeperは、SOC2やISO 27001認証も取得しており、以下の規制をはじめとする日本の個人情報保護法（APPI）やサイバーセキュリティ基本法に準拠した、数多くの法規制に対するコンプライアンスの確保を支援しています。

- 個人情報保護法（APPI）
- ISO/IEC 27001などの国際規格への準拠
- マイナンバー法および関連する個人情報保護法
- 経済産業省 サイバーセキュリティ経営ガイドライン
- サイバーセキュリティ基本法
- 重要インフラ保護（CIP）
- 金融分野におけるコンプライアンス
- 電気通信事業法
- SOX準拠
- SOC 2
- GDPR準拠

# 最後に

DX化を推進するのは、大企業だけの話でなく、また国に任せきりという訳にはいかないのが現状です。企業や組織のデジタルトランスフォーメーション（DX）を加速させつつ、セキュリティリスクを最小限に抑えるためには、大規模なソリューションを導入しなくてもパスワード管理ソリューションから簡単に始められることをご理解いただけたでしょうか。その中でもKeeperのような強力なパスワードマネージャーなら、安全性の確保のみでなく、利便性による生産性や効率性の向上が約束されます。

柔軟な統合性、コスト削減の効果、一元化された管理プラットフォーム、そして最小限のスタッフ要件という点で、企業が直面する現代のセキュリティ課題に対応する理想的なパスワードマネージャーを活用することで、非営利団体や中小企業を中心とした企業のDX化への移行に拍車がかかると言えるでしょう。