二兎を追う「Box」の最新セキュリティ戦略

～CrowdStrike連携とBoxAIで実現する情報漏洩対策とコスト削減～

セッション１

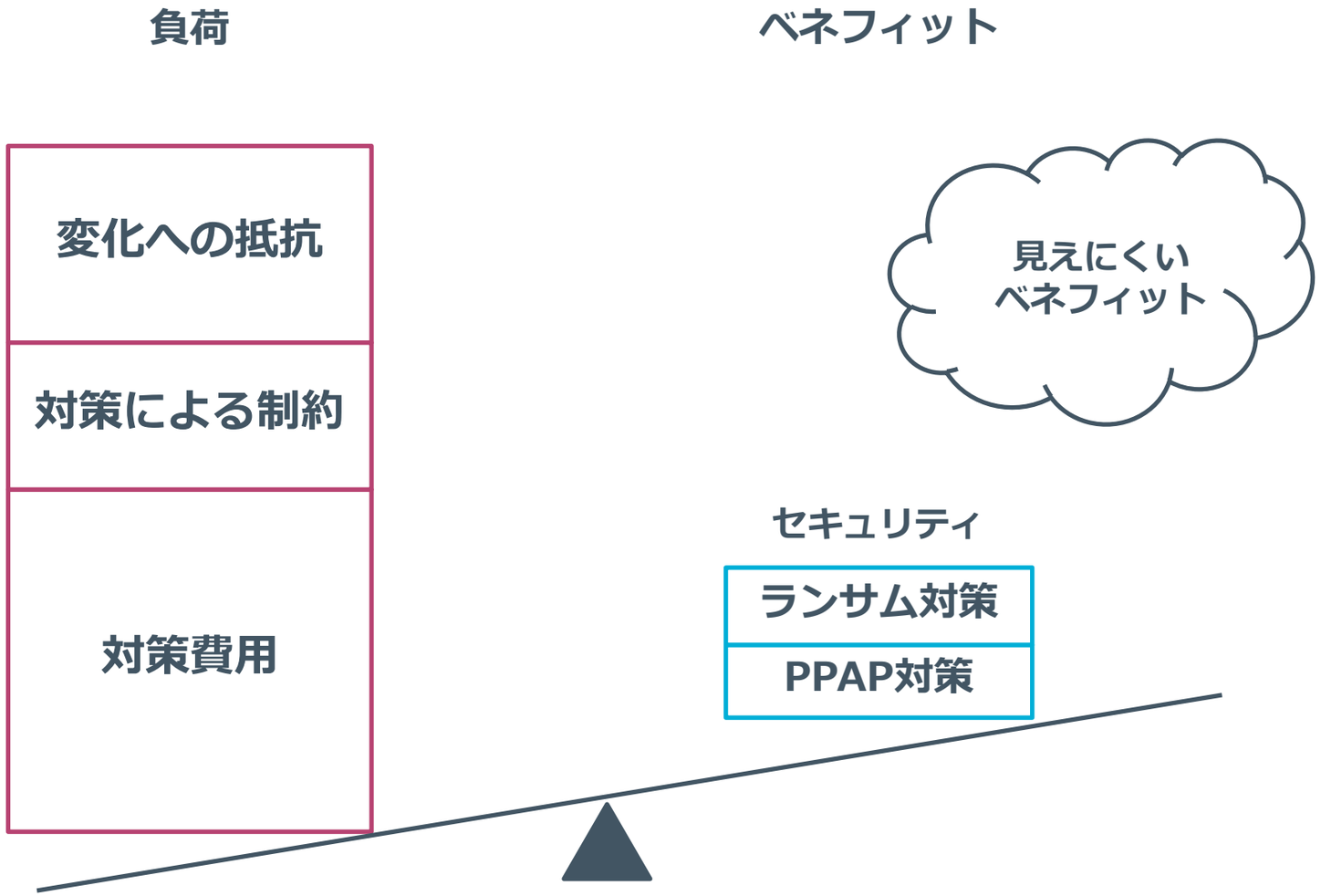
2024年1月25日

NRIセキュアテクノロジーズ株式会社

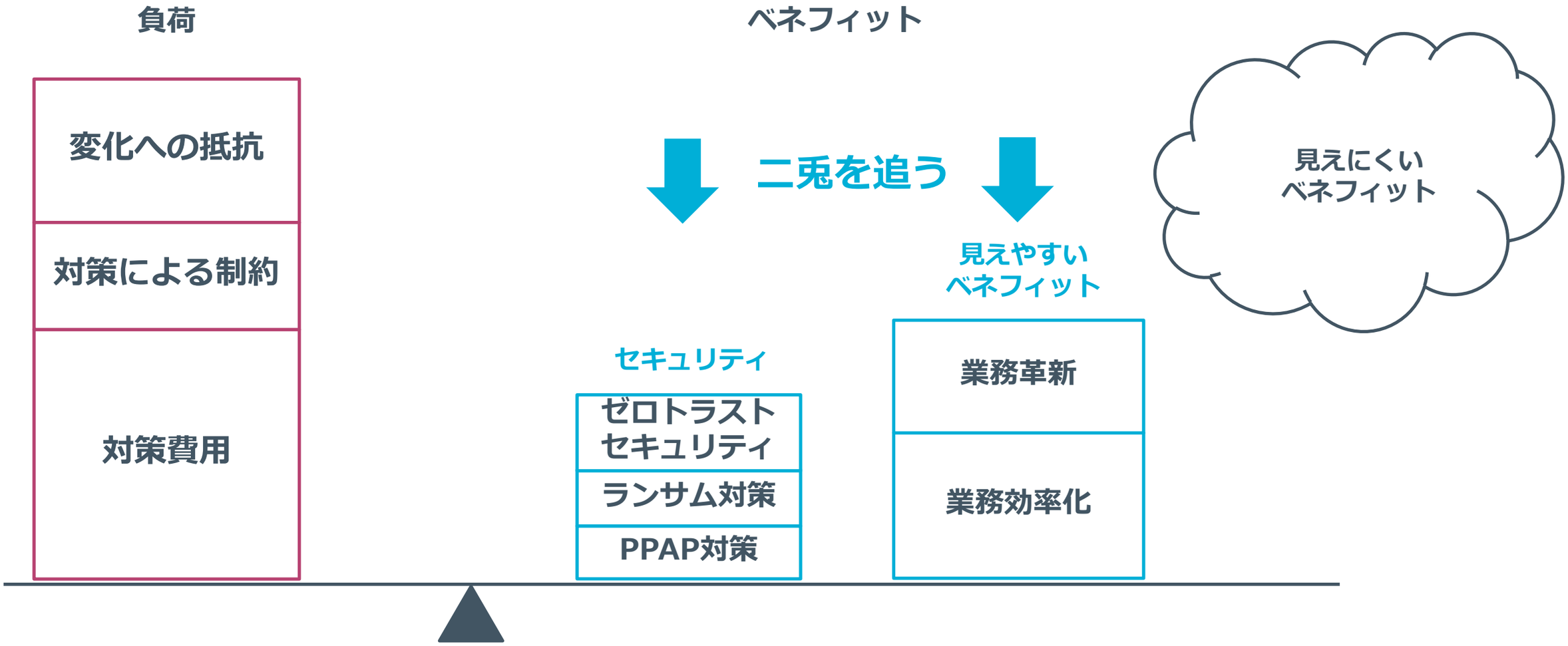
ファイルセキュリティ事業部

土屋　亨

セキュリティ投資はベネフィットが見えにくく、意思決定が難航する



「Box」導入でセキュリティと利便性（利益）の二兎を追うのは必然



自己紹介

土屋 亨

専門／
ファイル・ストレージセキュリティのクラウドソリューションの提案・設計・導入 など

■ 経歴

2009年4月｜株式会社野村総合研究所 入社

➢ **デジタルアイデンティティ、ID統合プロジェクト**
OpenIDをコアテクノロジーとしたUni-ID事業に従事し、コンシューマID統合管理基盤のグランドデザイン、要件定義・設計支援および番号制度を視野に入れた事業企画をおこなう

2014年5月｜担当製品移管に伴い
NRIセキュアテクノロジーズ株式会社出向

➢ **自社特権ID、コンテンツセキュリティ商材のプリセールス**
・AccessCheck｜特権ID管理
・クリプト便｜セキュアファイル転送・共有

2017年～現在｜
Boxを中心としたコンテンツセキュリティソリューションの提案、導入コンサルティングに従事

➢ **主なBox導入支援実績**
大手情報通信業　全社導入（1,500ライセンス規模）
大手学習塾　全社導入（1,500ライセンス規模）
大手化粧品会社　全社導入（1,200ライセンス規模）

■ 対外活動（これまでの主な活動）

講演

- テレワークでBoxを安全に使う方法とは ～無料アカウントに潜む情報漏えいリスクと対策～
- テレワーク時代に求められるBoxのファイルセキュリティ対策とは
- 待ったなしの脱PPAPセミナー ～セキュリティ専門会社が提案する代替手段とは～
- ユーザ企業が語るBox導入事例ウェビナー

執筆等

- ITソリューションフロンティア 2020年新春号（トピックス：ファイル共有のセキュリティ） 発行：野村総合研究所
- ITロードマップ2020年版（コラム：ファイル共有サービスにおけるセキュリティリスク）
  発行：東洋経済新報社
- ITロードマップ2021年版（4.2章 ファイルコラボレーションのセキュリティ）
  発行：東洋経済新報社

■ 保有資格

➢ Box Certified Professional(No.14493328)
➢ CISSP(No.626834)
➢ 情報処理安全確保支援士 第004671号

PPAPに関する記事では多くの反響をいただきました

脱PPAP対策はなぜ必要？「パスワード付きzipファイル」の文化から脱却する方法

更新日：2020.11.19
公開日：2020.11.19

土屋 亨

クリプト便　情報漏洩対策　テレワークセキュリティ

引用：https://www.nri-secure.co.jp/blog/break-away-from-the-password-protected-zip-file

NRI

NRI トップ > NRI JOURNAL > PPAPからの脱却はDXの試金石

NRI JOURNAL　未来へのヒントが見つかるイノベーションマガジン

PPAPからの脱却はDXの試金石

NRIセキュアテクノロジーズ　土屋 亨

#サイバーセキュリティ

2021/07/02

Share

引用：https://www.nri.com/jp/journal/2021/0702

待ったなしの脱PPAP

PAPP対策は必要か？

いまや自社を取り巻く外部環境の影響が無視できない

内部環境

■ PPAPでのファイル送付がデメリットになりにくい企業の例

- そもそも社外にファイルを送る機会が少ないか、ない
- 扱うファイルの機密度が低く、漏洩しても問題にならない
- PPAP送付の手間を織り込んでも業務が成り立っている
- 自動でパス付きZipにできる製品を導入したため送信側として手間がない

外部環境

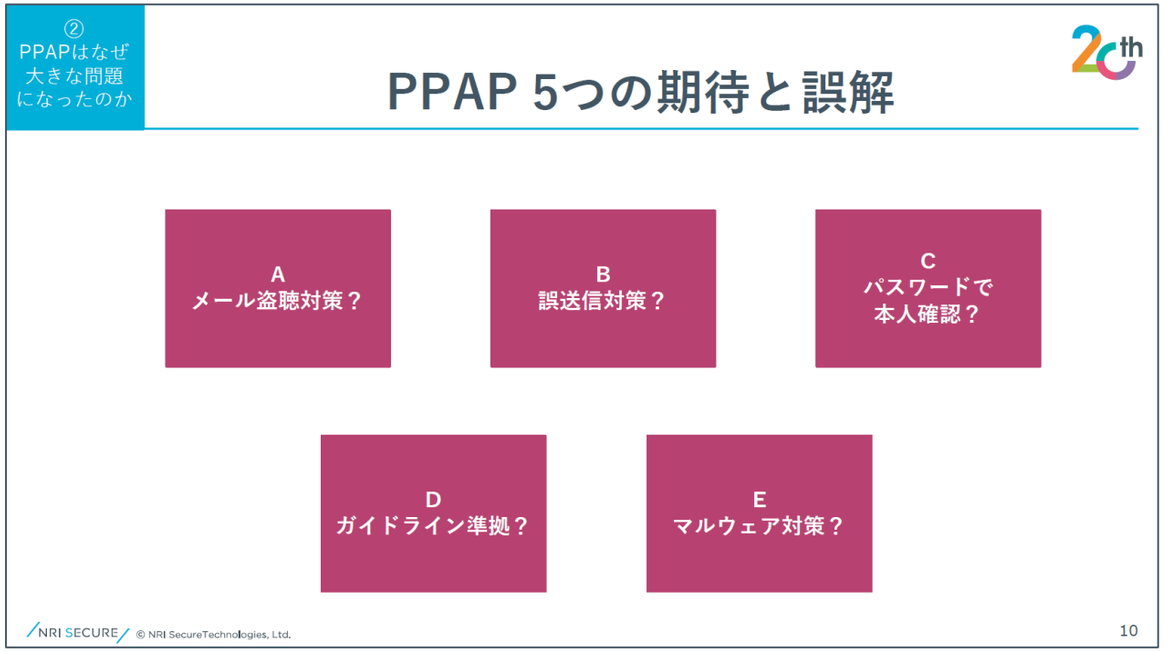
■ PPAPでのファイル送受信がデメリットになりやすい昨今の状況

- 取引先にPPAPを受け取ってもらえなくなった
  - 無償のファイル転送ツールを無断利用（シャドーITがもたらすリスク増）
- PPAPに偽装したマルウェアの手口が増加し、ランサムウェア被害も増えている
  - 社外からファイルを受け取る機会があるし、増えている
  - 受信した「パス付きZipを展開する」が基本動作になって手が勝手に動いている？

Zipファイルを辞めることがPPAP?

手段が目的になってしまう。PPAPの目的、期待していた効果とは

■ 弊社ホワイトペーパーから引用



② PPAPはなぜ大きな問題になったのか

A.メール盗聴対策への期待と誤解

盗聴対策になっていない

PPAPとは、仕組み上盗聴に弱いメールを使って

安全なファイル交換を目指す工夫だったが…

ファイルとパスワード双方をメールで送信する

現状では盗聴対策にならない

② PPAPはなぜ大きな問題になったのか

B. 誤送信対策への期待と誤解

誤送信そのものを防げない

メールを誤送信してもパスワードを送らなければ

取り返しがつくのではないか？

1通目の誤送信の時点で誤送信対策になっていない

ファイルそのものが相手に渡るうえ、

パスワードを解析されてしまう

③
PPAPはなぜ大きな問題になったのか

C. アクセス制御への期待と誤解

パスワードは容易に解析できる

パスワード付きzipファイルは暗号化されているから

パスワードがバレなければ安全ではないか？

十分複雑で長いパスワードでない限り

市販されているPCとツールを使って

パスワードを総当りで試す時間は数秒～数時間

② PPAPはなぜ大きな問題になったのか

D. ガイドライン準拠への期待と誤解

PPAPは推奨されない

プライバシーマークの付与審査に合格するためには

PPAPでの送付が必要ではないか？

プライバシーマークを運営するJIPDECは

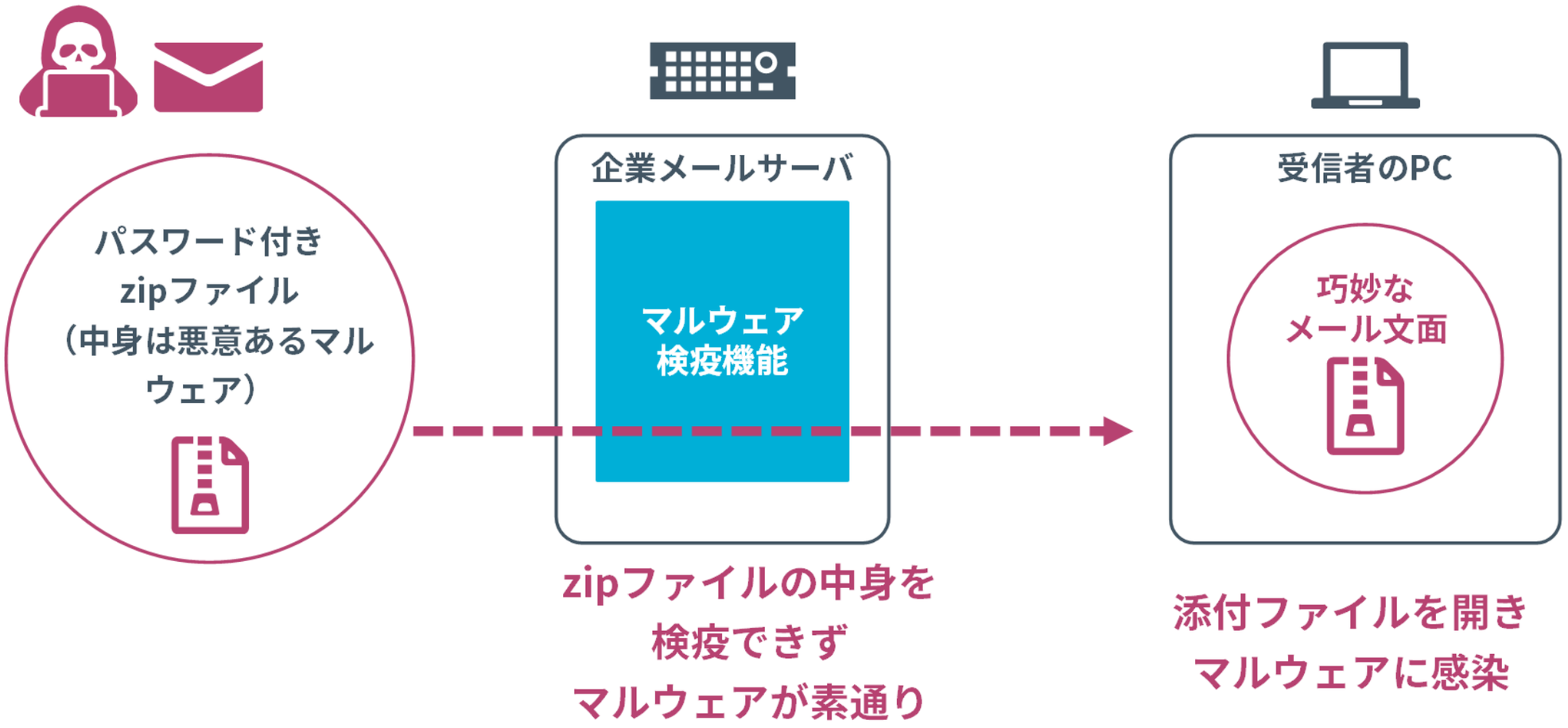
脱PPAPに関する政府会見のあと、従来からPPAPは

推奨していないことをお知らせに掲載※

※出典: JIPDEC（一般社団法人日本情報経済社会推進協会）, メール添付のファイル送信について（2020/11/18公開）,
https://privacymark.jp/news/system/2020/1118.html

② PPAPはなぜ大きな問題になったのか

E. マルウェア対策への弊害
検出回避にパスワード付きzipを利用した攻撃が登場



Zipファイルを辞めることがPPAP?

手段が目的になってしまう。PPAPの目的、期待していた効果とは

A
メール盗聴対策？

B
誤送信対策？

C
アクセス制御？

D
ガイドライン準拠？

E
マルウェア対策？

コンテンツクラウド

コンテンツジャーニーを管理する
セキュアでインテリジェントな
プラットフォーム

引用：BoxJapan コーポレートピッチ

Boxは業界をリードするクラウド・コンテンツ・プラットフォーム

引用：BoxJapan コーポレートピッチ

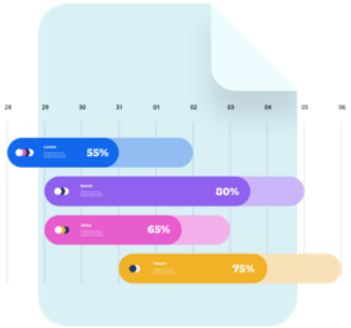
企業・組織全体を支えるプラットフォーム

セールス

デジタルなコミュニケーション、顧客契約管理、セールスイネーブルメント

マーケティング

デジタルアセットライブラリ、アセットの作成と配布、エージェンシーやパートナーとのコラボレーション



研究・開発

組織内コラボレーション、プロジェクト・製品の企画、
ドキュメントライブラリ

法務

仮想データルーム、契約書管理、顧客とのコラボレーション

人事

従業員のオンボーディング、人事書類管理、従業員研修ハブ

オペレーション

ベンダーのオンボーディング、ベンダー・サプライヤーのワークスペース、フィールドオペレーション管理

AstraZeneca

CISCO

KKR

Nationwide®

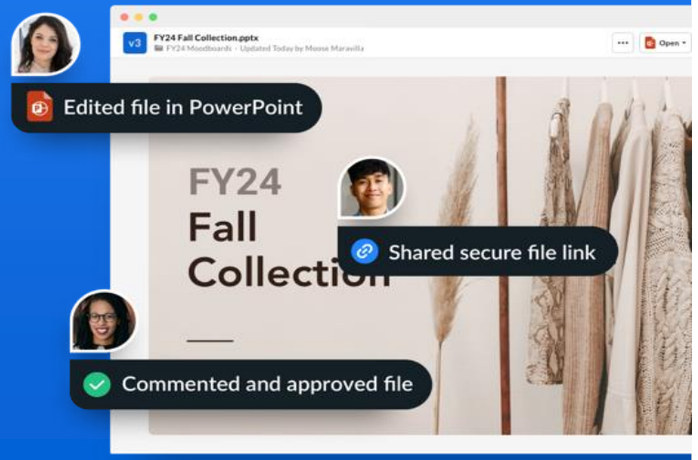
引用：BoxJapan コーポレートピッチ

コンテンツを保護する

フリクションレスな
セキュリティと
コンプライアンス

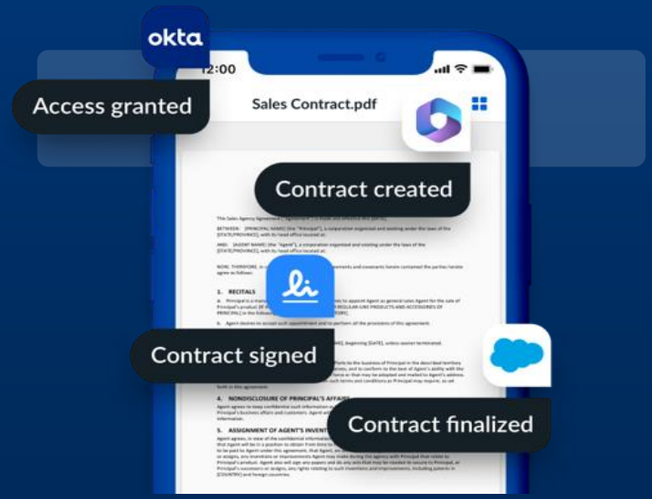
生産性を向上する

シームレスな
コラボレーションと
ワークフロー



ITをシンプルにする

すべてのアプリケーション
をつなぐ
コンテンツレイヤー



AIが拡張、強化

引用：BoxJapan コーポレートピッチ

Boxコアライセンス エディション一覧

		Business	Business Plus	Enterprise	Enterprise Plus
	メーカー希望小売価格　（年額/1ユーザ当りの費用）	21,600円	36,000円	50,400円	72,000円
ユーザ向け	Relay：簡易ワークフロー機能	✓標準	✓標準	✓高度	✓高度
	Box Sign：電子署名機能	✓標準	✓標準	✓高度	✓高度
	1ファイルの最大アップロードサイズ	5GB	15GB	50GB	150GB
	コラボレーション（ファイル共有）、共有リンク（ファイル転送）	✓	✓	✓	✓
	社外ドメインのファイル共有者	有償（費用を負担）	無償	無償	無償
	バージョン管理	50世代	50世代	100世代	無制限
管理者向け	管理コンソール（管理者向け画面）	✓	✓	✓	✓
	高度なパスワード設定/SSO連携　SAML2.0	標準/SSO	標準/SSO	カスタム/SSO	カスタム/SSO
	IPアドレス制限	×	✓	✓	✓
	コンテンツマネージャー（保存ファイルの一元検索）	×	✓	✓	✓
	3rd パーティ製品との連携 AD SAML/SSO, Salesforce, NetSuite, Jiveなど	1個のみ	10個	無制限	無制限
備考	契約人数 ※501名以上は最少20名～となります。	最少5名様～	最少5名様～	最少5名様～	35名～
	テナント当りのストレージの総容量	無制限	無制限	無制限	無制限
	Governance：ガバナンスオプション	×	有償追加可能	有償追加可能	標準搭載
	Shield：シールドオプション	×	×	有償追加可能	標準搭載
	Zones：ゾーンズオプション（データ保存先を指定 _ 例：日本にデータ保存）	×	有償追加可能 （Singleのみ）	有償追加可能	標準搭載

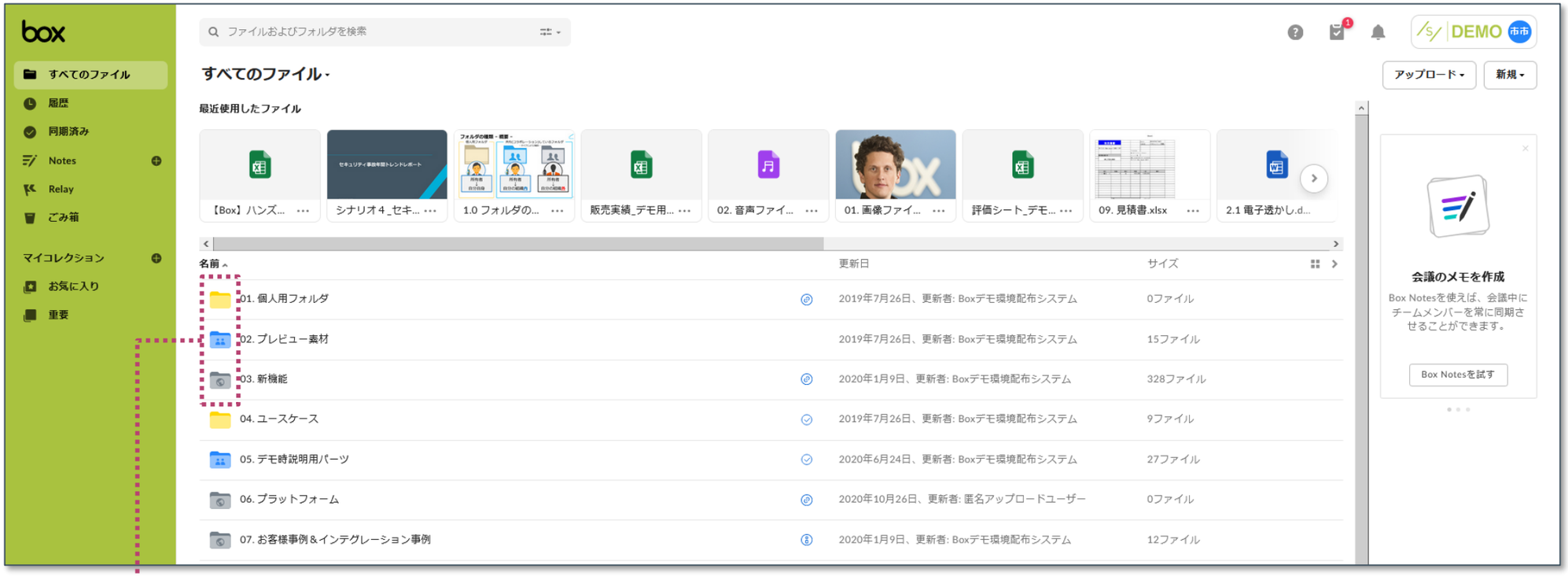
Boxを使ったPPAP対策

Boxを使ったPPAP対策

- セキュリティに絞った狭義の**PPAP対策**（メールでZipファイルとパスワードを送付）としては**Boxで充足可能**
- PPAP対策におけるBox導入の**真の課題はPPAP対策以外**である場合が多い（前例のない取り組みへの強い動機づくり）

Zipファイルのメール添付脱却	➢ Boxへのアップロード＆ダウンロード
アクセス制御（パスワード認証等）手段の用意	➢ ID指定で受信者をコラボレーションし、Boxにログイン ➢ ログイン不要の共有リンク（オープンリンク）をパスワード付きで発行する
パスワード配送の手間削減	➢ コラボレーションにより都度パスワードの生成・配送不要
メール経路のセキュリティリスク（SMTP)低減	➢ HTTPS通信（TLS1.2）による経路の暗号化
メール添付からの業務変化の摩擦低減	➢ MxHeroなどのメーラー連携ツールを利用し、送信側のオペレーション変化を低減可能
誤送信対策	➢ ７種類の権限ロール管理等で権限を最小化 ➢ Shieldオプション（有償）のスマートアクセス機能でファイル自体にセキュリティポリシーを適用・越権行為を水際阻止
ガイドラインへの準拠	➢ ISMAP（日本政府によるセキュリティ評価）、PCIDSS（クレジットカード業界ガイドライン）、FISC安全対策基準（金融庁ガイドライン）等をクリア

BoxのUI　フォルダ/ファイルの見え方



フォルダアイコンの種類

※管理者でも中身が見れないフォルダ

1

個人フォルダ
所有者：自分

2

コラボレーションフォルダ
所有者：社内ユーザー(自分含む)

3

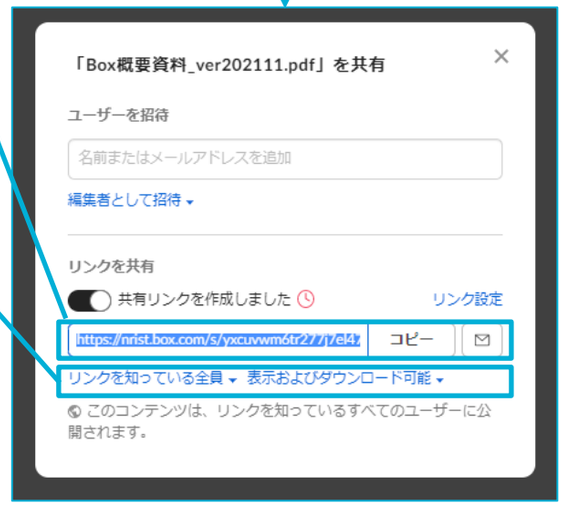
外部コラボレーションフォルダ
所有者：社外ユーザー

Boxを使ったアクセス制御・コラボレーション

① 顧客別授受資料置き場	② 共有リンク	③ コラボレータ	④顧客からのデータ収集先 （ファイルリクエスト機能）
• 各社と授受する/した資料はフォルダ別に格納してBox上で管理できます（サブフォルダも作成可能）	• 資料送付の場合は共有リンク（ファイル取得用URL）を発行し、具体的なファイルの代わりに当該URLをメール送付するなどしてファイルのやりとりが可能です • 共有リンクの設定によってはBoxアカウントを持たなくてもファイルを閲覧またはダウンロードさせることができます（オープンリンク）	• 本機能により、フォルダごとに、所属する社内ユーザ、社外ユーザが誰で、どんな権限を持たせるかを設定できます • ①の各フォルダに顧客をコラボレータとして招待してファイル授受もできますが、取引先にBoxアカウント（無料または有料）の作成が必要になります	• 本フォルダにファイルリクエスト機能を設定することによって、顧客からのデータ収集ができます（後述）。顧客はBoxアカウントが不要です • 各社ごとに収集先フォルダを個別に用意することも可能です（その場合ファイルリクエスト機能もそれぞれ有効化する）

②共有リンク

- 共有リンクとはBoxに格納したファイルに付与する閲覧・ダウンロード用URLです
- 設定によりBoxアカウントがなくてもファイルをプレビューだけさせたり、設定によりダウンロードもさせられます
- ファイルの実体をメール添付する代わりに共有リンクをメール本文記載すれば、メール添付の必要なくファイルを送ることができます



共有リンク（URL）

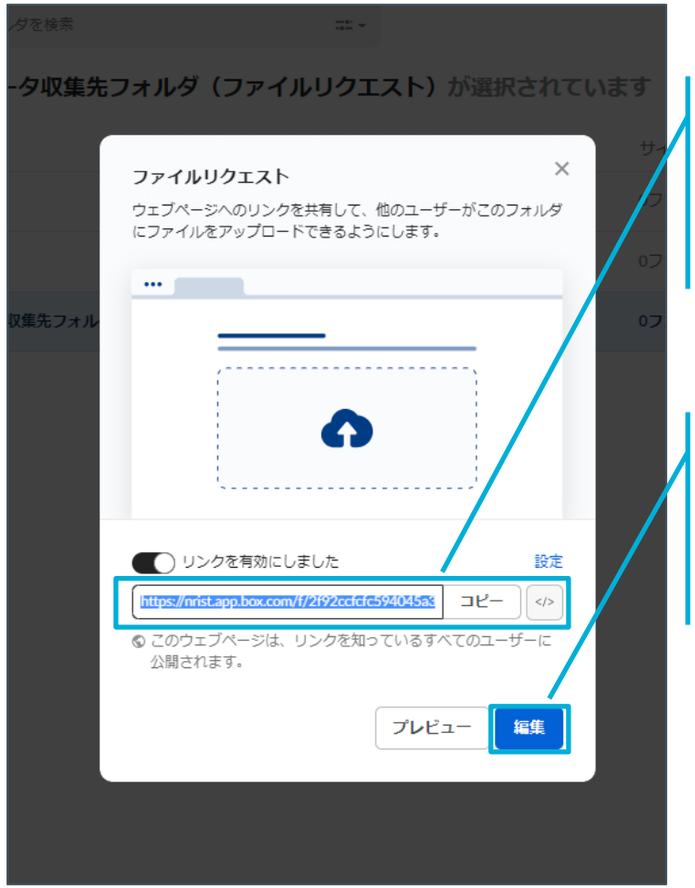
共有リンク（オープンリンク）の設定
→Boxアカウントがなくてもアクセスさせるには『リンクを知っている全員』を選択

共有リンクをメール送付

共有リンクにアクセスすると・・・
ブラウザ上でプレビューしたりダウンロード可能

④顧客からのデータ収集先　ファイルリクエスト機能

- 本機能は、あるフォルダを選択し、当該フォルダを保管場所として顧客からファイルを収集するだけのWebページを生成する機能です。
- Boxアカウントを持たないユーザからの一方的なファイル取得を目的に利用できます
- 収集用Webページはある程度のカスタマイズが可能です



収集ページへのリンク
→本リンクを顧客に連絡してアクセスしてもらいます

収集ページはこちらの編集ボタンからカスタマイズ可能です（次項）

④ファイルリクエスト機能　～収集ページのカスタマイズ～

- 左記の図のように、ページ内のタイトル、説明、ファイルアップロードエリア、メールアドレス、色、ロゴなどをカスタマイズ可能です
- 本ページを経由してアップロードされたファイルが、設定された収集用フォルダに格納されます

- サンプル収集ページのリンク
  - https://nrist.app.box.com/f/2f92ccfcfc594045a379d05ddee0b733

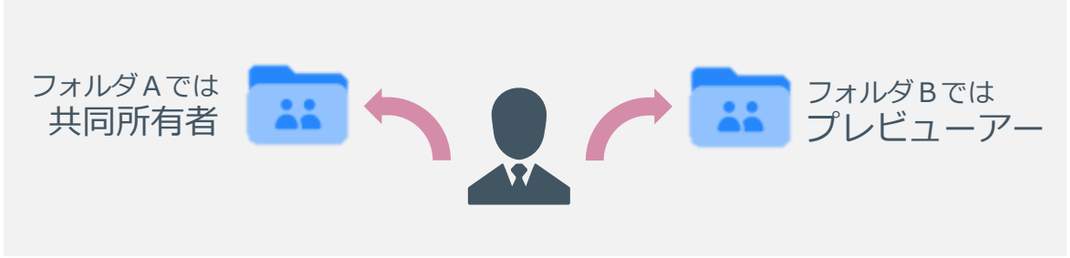
  - 上記URLまたはQRコードからにアクセスいただくと、顧客から見た収集ページのサンプルをご覧いただけます（リンク切れの際は弊社までお問い合わせください）

7種類の共有フォルダへのアクセス権限

ユーザーに対してフォルダ毎に柔軟な権限設定が可能

アクセス権限	アップロード	ダウンロード	プレビュー	リンクの取得	編集	削除	所有
共同所有者	●	●	●	●	●	●	●
編集者	●	●	●	●	●	●	
ビューアー /アップローダー	●	●	●	●	●		
プレビューアー /アップローダー	●		●				
ビューアー		●	●	●			
プレビューアー			●				
アップローダー	●						

※招待された方も、Boxのアカウントが必要（無償のPersonalアカウントでもOK）
※Businessプランの場合、外部コラボレータを招待すると従量課金が発生します



補足）7種類のアクセス権限

アクセスレベル	権限
共同所有者	所有者と同等の権限。ただし所有者の権限は変更不可。 通常は、社外の関係者には設定しない。
編集者	ビューアー/アップローダー権限に加え、新たに共有フォルダへの招待やアクセス権限の設定ができる権限。インタラクティブにファイルのやり取りをするときに利用。 主に、社内の関係者に設定。
ビューアー /アップローダー	コンテンツを編集したりアップロード／ダウンロードできる権限。 ただしファイルの削除は出来ない。インタラクティブにファイルのやり取りをするときに利用。
プレビューアー /アップローダー	プレビューに加えてアップロードもできる権限。ただし、ダウンロードは出来ない。 ファイルの中身を確認してもらい、必要に応じて適切なファイルをアップロードしてもらいたい時に利用。
ビューアー	コンテンツをプレビューしたりダウンロードできる権限。 厳密なアクセス履歴を残す、大容量ファイルの受け渡し。主に社外の関係者に設定。
プレビューアー	プレビューのみ可能な権限。 ファイル自体をダウンロードさせずに中身を確認させたい時に利用。主に社外の関係者に設定。
アップローダー	アップロードだけできる権限。 一方的なファイル提出(レポート、画像等）で利用。主に社外の情報提供者に設定。

ランサムウェア対策

Boxを使ったランサムウェア対策／ノーウェアランサム

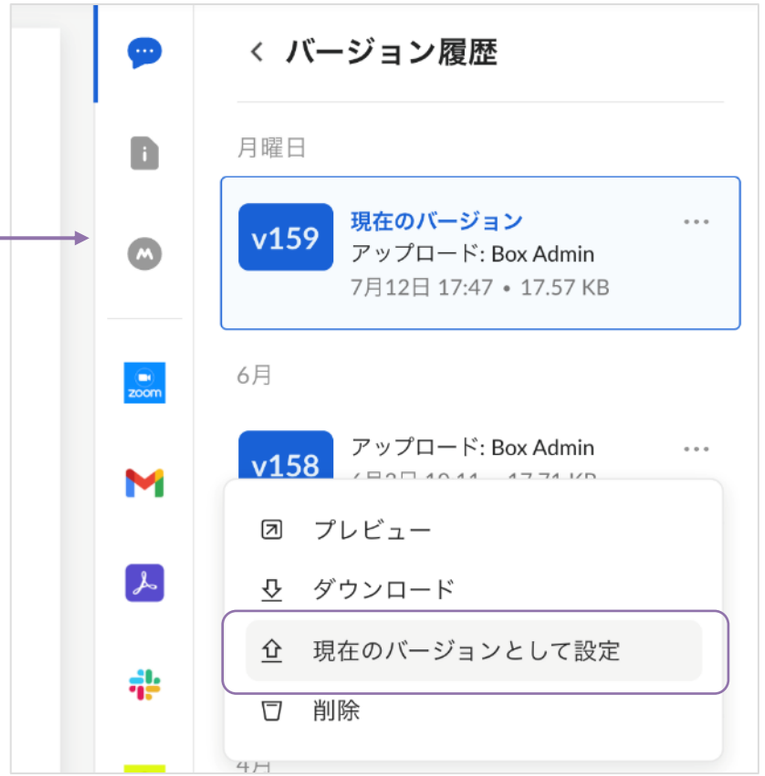
- **ランサムウェア**ではBoxのWebUI操作の実行難易度が高く、仮に**暗号化されても過去バージョンに復旧可能**
- そのためにも、**オンプレFSやPC端末に原本を残さずBox上にコンテンツを集約する＝純粋なBox活用**がそのままランサムウェア対策になる
- **ノーウェアランサム**（データの窃取のみを行いそのデータの公開と引き換えに対価の支払いを要求する）への脅威には**認証強度の向上（IPアドレス制御、端末認証、二段階認証等）で対抗。**さらに**Shieldオプション「脅威検出機能」**があれば**不審なアクセス**や**異常なダウンロードを検知し対抗**

クラウドストレージでのランサムウェア対策

バージョン管理機能による復旧（50世代または100世代）

Governanceオプションなら無制限にバージョン管理可能

感染・不正暗号化される前のバージョンにファイルを戻すことで復旧



一つ前のバージョンを
現在のバージョンとして設定

一世代前のファイルが最新の
バージョンに昇格

Shieldオプション

クラウドストレージでのランサムウェア対策(1)

1. マルウェア・ランサムウェアの検知

- **悪意のあるコンテンツ**: 悪意あるコンテンツを検出して、ダウンロードや共有を制限することでファイルの拡散を防止する機能

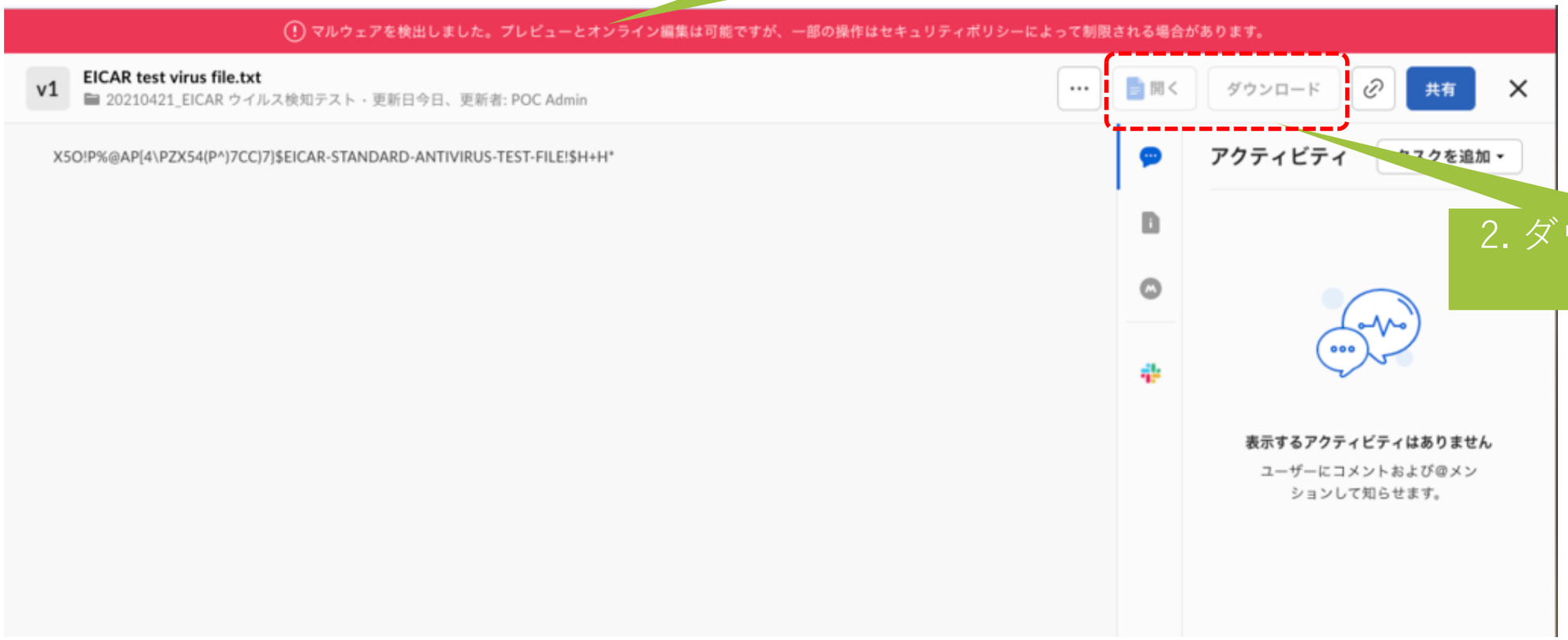
Shieldオプション

クラウドストレージでのランサムウェア対策(2)

2. 二次被害/拡散の防止

1. マルウエア検知表示

ユーザーに対して、このファイルがマルウェアであることを明示



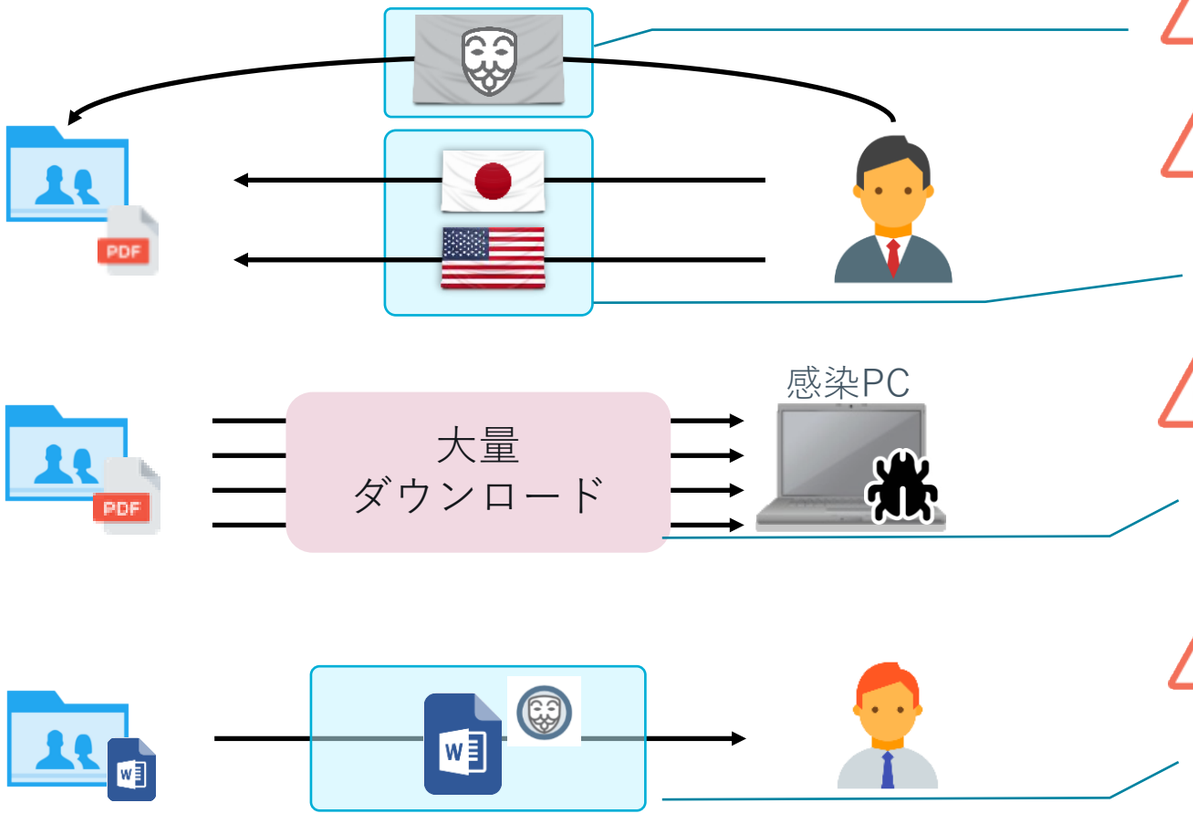
2. ダウンロードと共有抑止制御

ダウンロード、ローカル編集、ファイルコピーなどを自動的に制限することでファイルの拡散を防止

Shieldオプション

クラウドストレージでのランサムウェア対策(3)

3. ファイル窃取の自動検知



警戒地域からのアクセスを検知

同じタイミングに特定IDが複数の国からアクセスしているのを検知

通常では発生しない
大量ダウンロードを検知

マルウェアに感染したコンテンツを検知しダウンロードを制御

NRI SECURE

二兎を追う「Box」の最新セキュリティ戦略

～CrowdStrike連携とBoxAIで実現する情報漏洩対策とコスト削減～

セッション２

2024年1月25日

NRIセキュアテクノロジーズ株式会社

ファイルセキュリティ事業部

土屋　亨

はじめに

ビジネススピードの加速が
社会・企業に与える影響の感覚、を掴んでみる

極端に単純化した前提で

ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる

ちょっとした思考実験

インフレ社会における貨幣価値の考え方を拝借

50年前の1万円の価値は
今の1万円の価値と同一か？

50年前

金1g＝1,140円

現在

金1g＝約8,800円

インフレが起きるとお金が多く必要

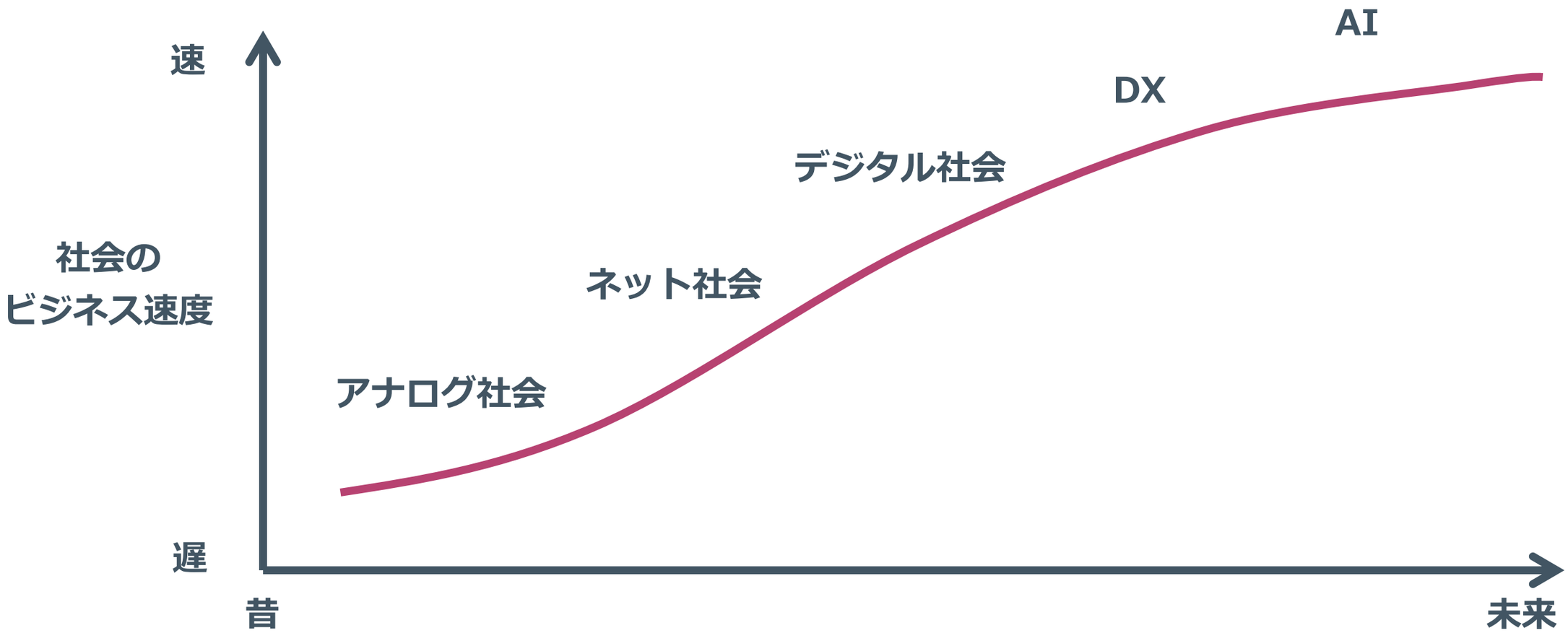
ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる
ちょっとした思考実験

５年前の社会が60分を消費してできたことと
今の社会が60分を消費してできることは同一か？

ビジネススピードがインフレすると
（期待される）成果が増える

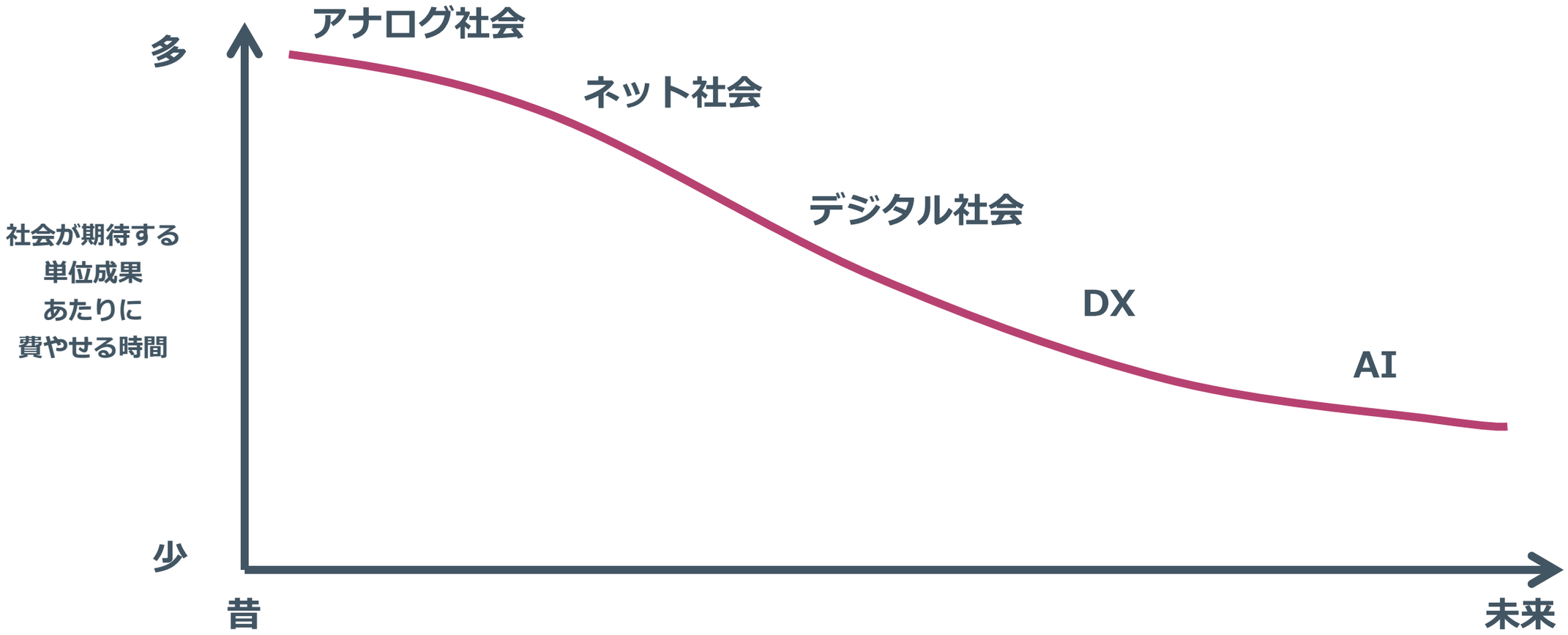
ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる
ちょっとした思考実験

毎年ビジネススピードがインフレしていると仮定



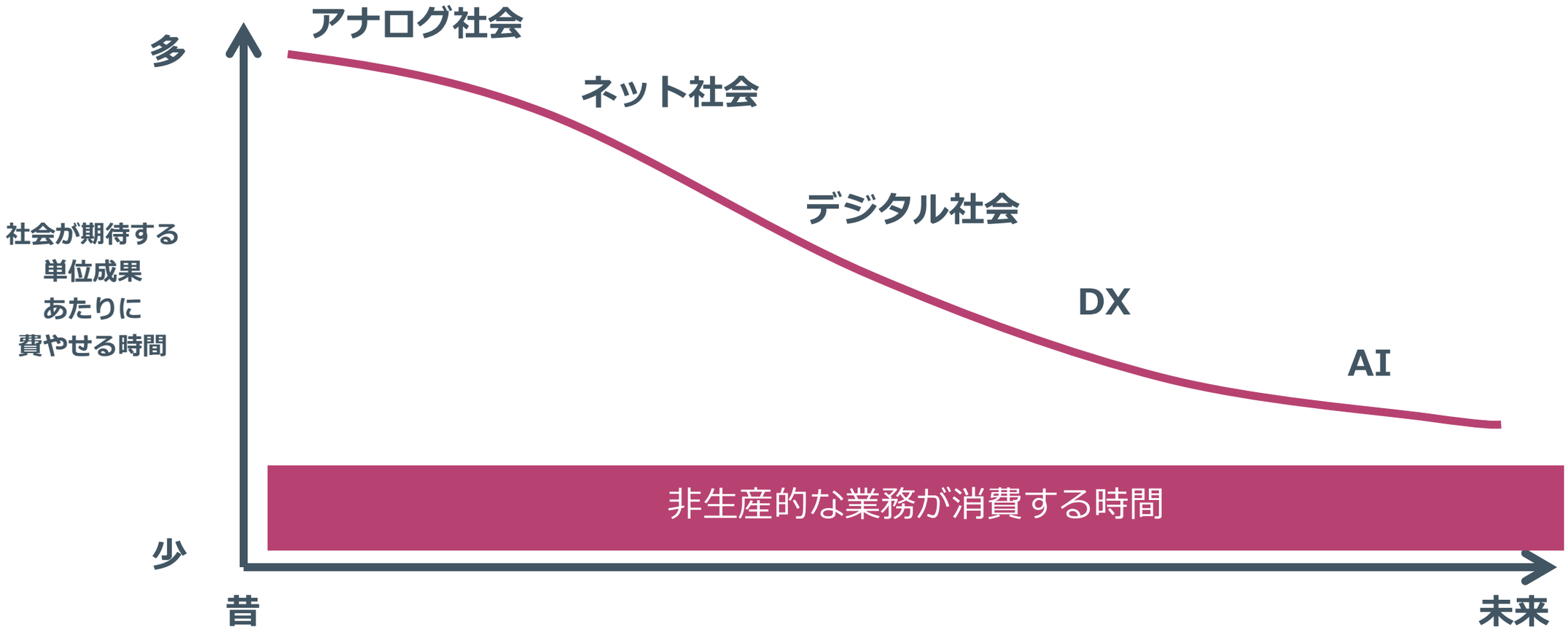
ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる
ちょっとした思考実験

社会が期待する、単位成果あたりに費やせる時間



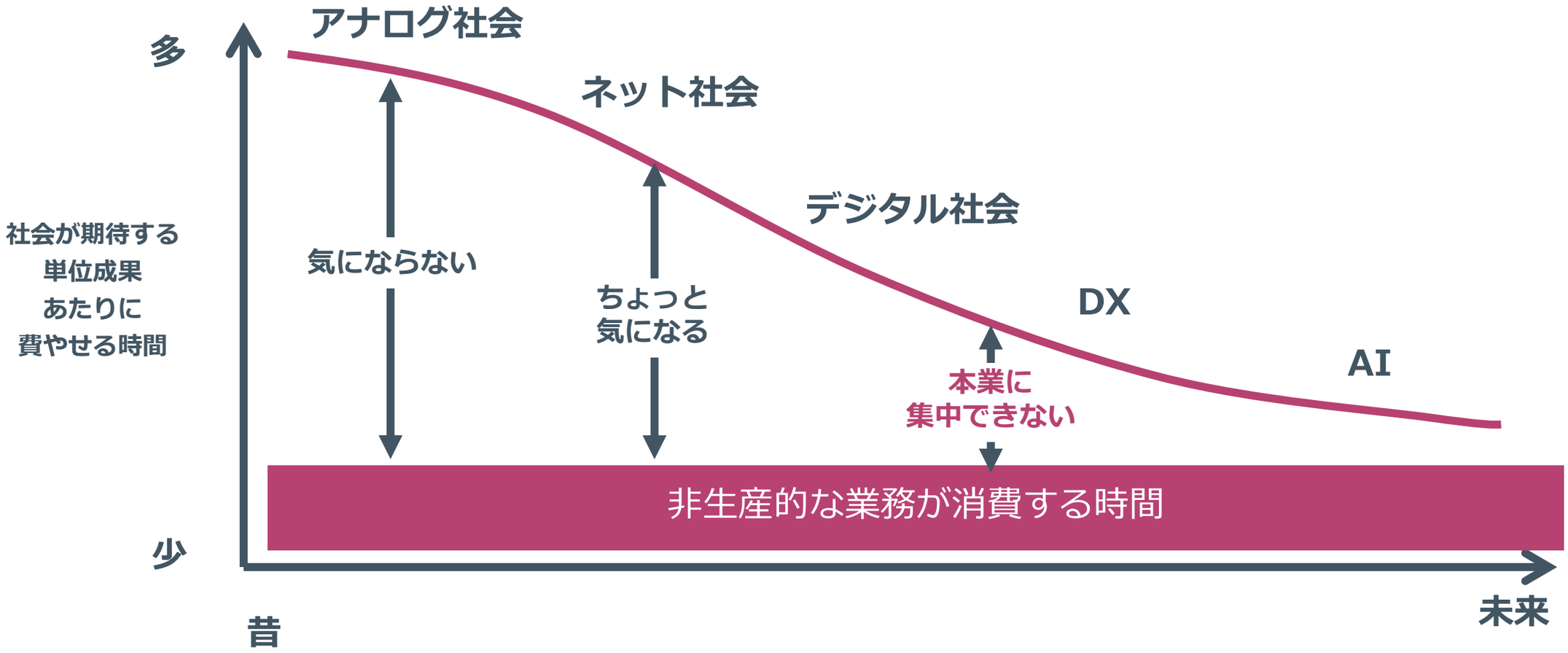
ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる
ちょっとした思考実験

昔から続く作業効率の悪い人力の業務が残っていたら？



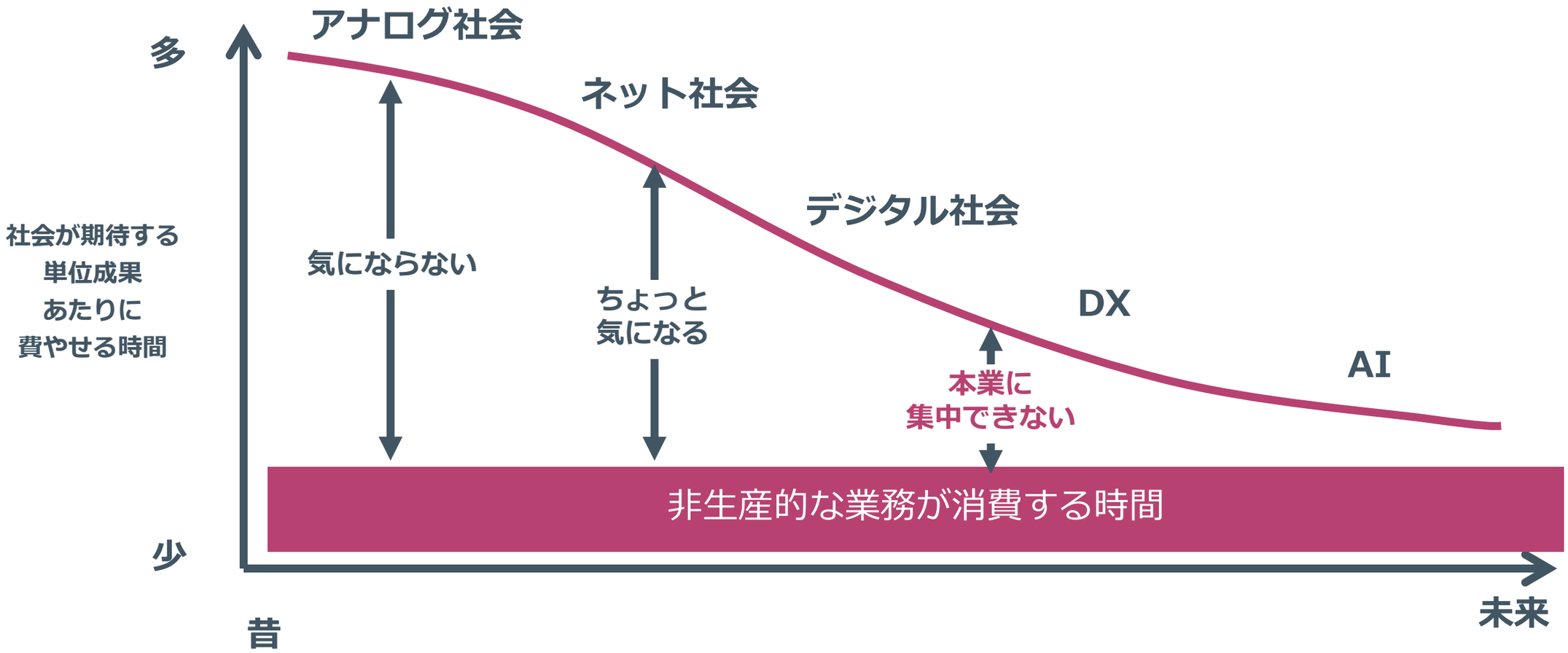
ビジネススピードの加速が社会・企業に与える影響の感覚を掴んでみる
ちょっとした思考実験

昔から続く作業効率の悪い人力の業務が残っていたら？



昔から続く作業効率の悪い業務

前例踏襲、はんこ、ペーパー、PPAP、が残っていたら？

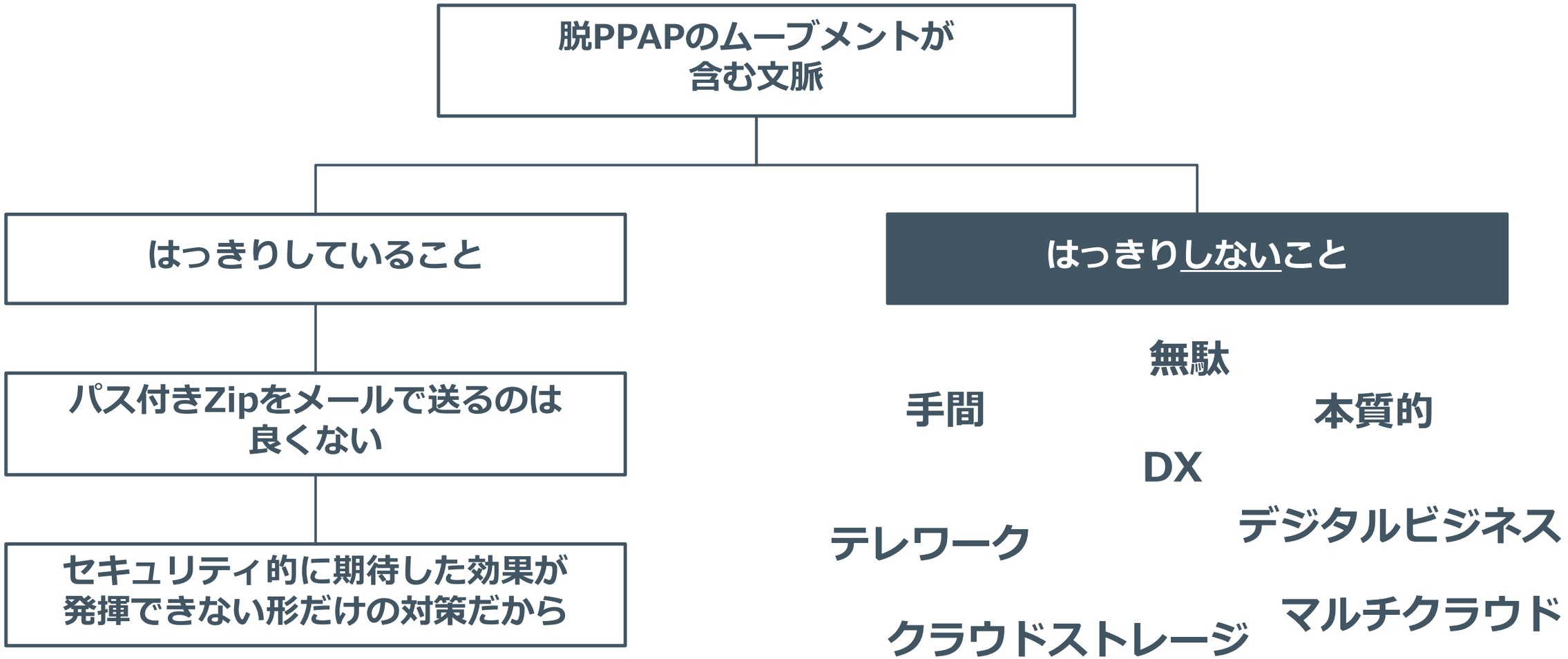


社会のビジネススピードは市場の競争原理によってつくられる

カーブが緩やかな企業であっても
社会情勢、技術革新、競合の台頭といった
外部要因の急峻な変化でトレンドは大きく動く時代

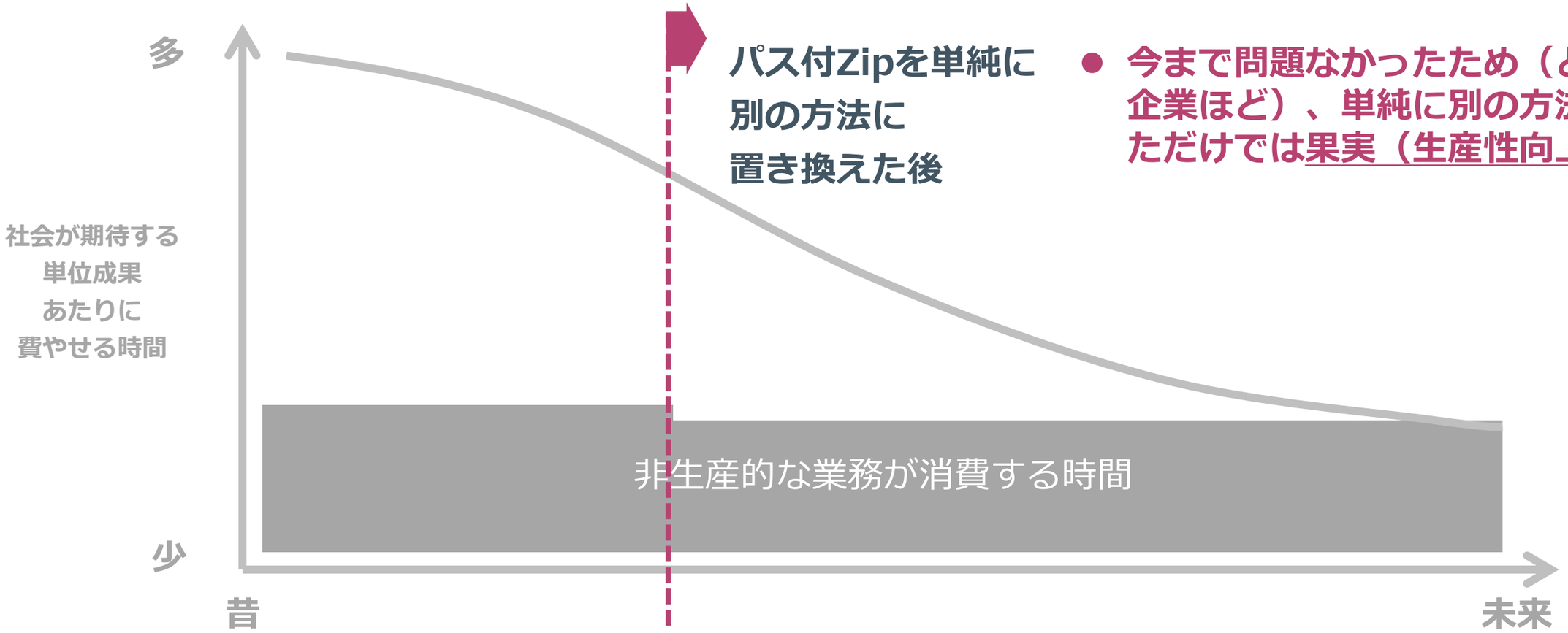
PPAP脱却の検討は、これをきっかけに
将来本業に集中する環境を手に入れる第一歩

脱PPAP論に含まれる期待と効果とは



脱PPAP論に含まれる期待と効果とは

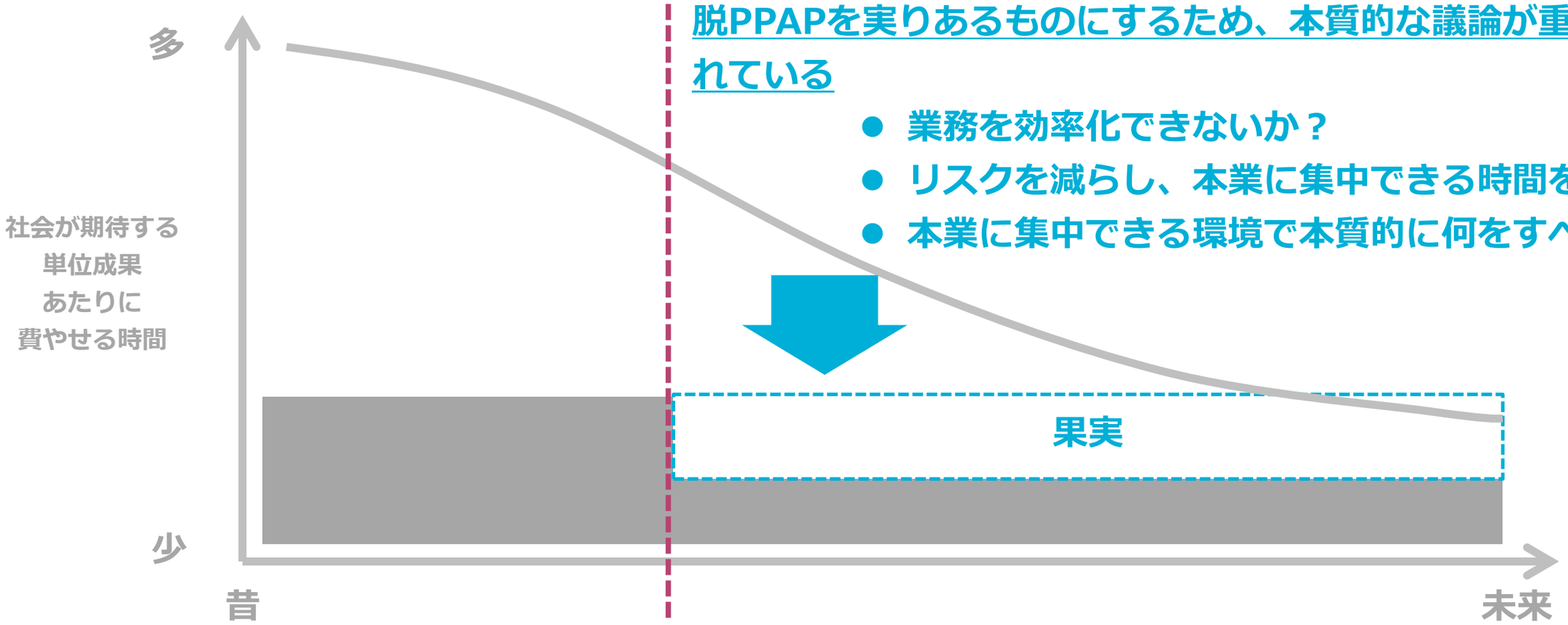
社会が期待する、単位成果あたりに費やせる時間



- 今まで問題なかったため（と思っていた企業ほど）、単純に別の方法に取り替えただけでは果実（生産性向上等）がない

脱PPAP論に含まれる期待と効果とは

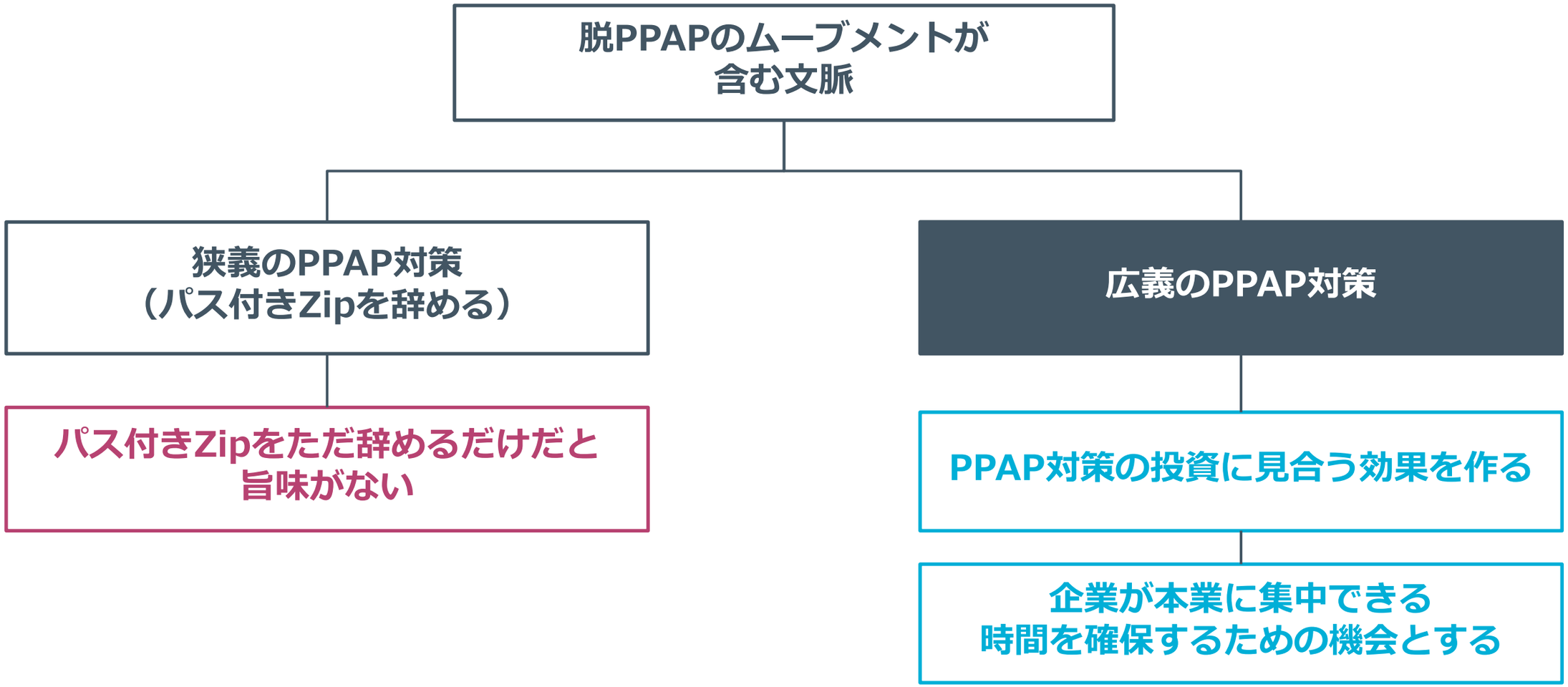
社会が期待する、単位成果あたりに費やせる時間



脱PPAPを実りあるものにするため、本質的な議論が重要視されている

- 業務を効率化できないか？
- リスクを減らし、本業に集中できる時間を増やせないか？
- 本業に集中できる環境で本質的に何をすべきか？

脱PPAPを企業が本業に集中できる時間を確保する機会と捉える



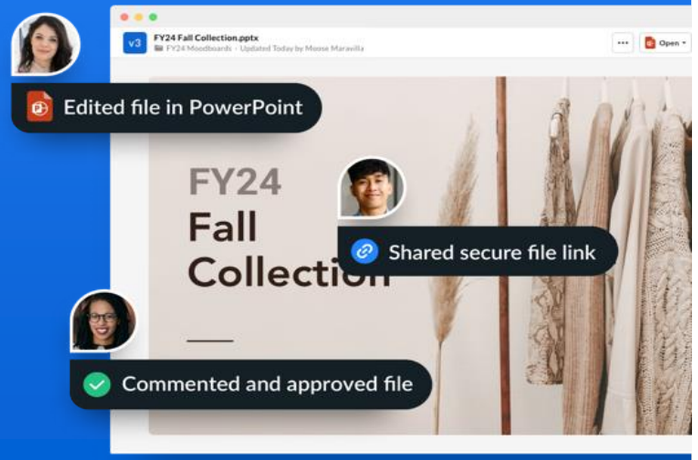
Boxの導入による
時間短縮・業務効率化

コンテンツを保護する

フリクションレスな
セキュリティと
コンプライアンス

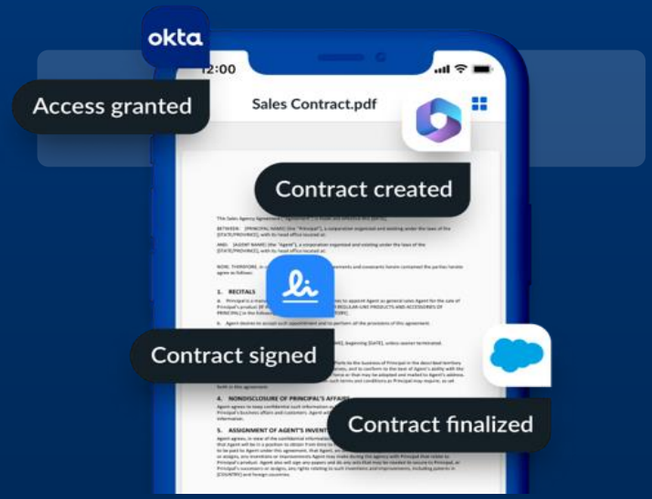
生産性を向上する

シームレスな
コラボレーションと
ワークフロー



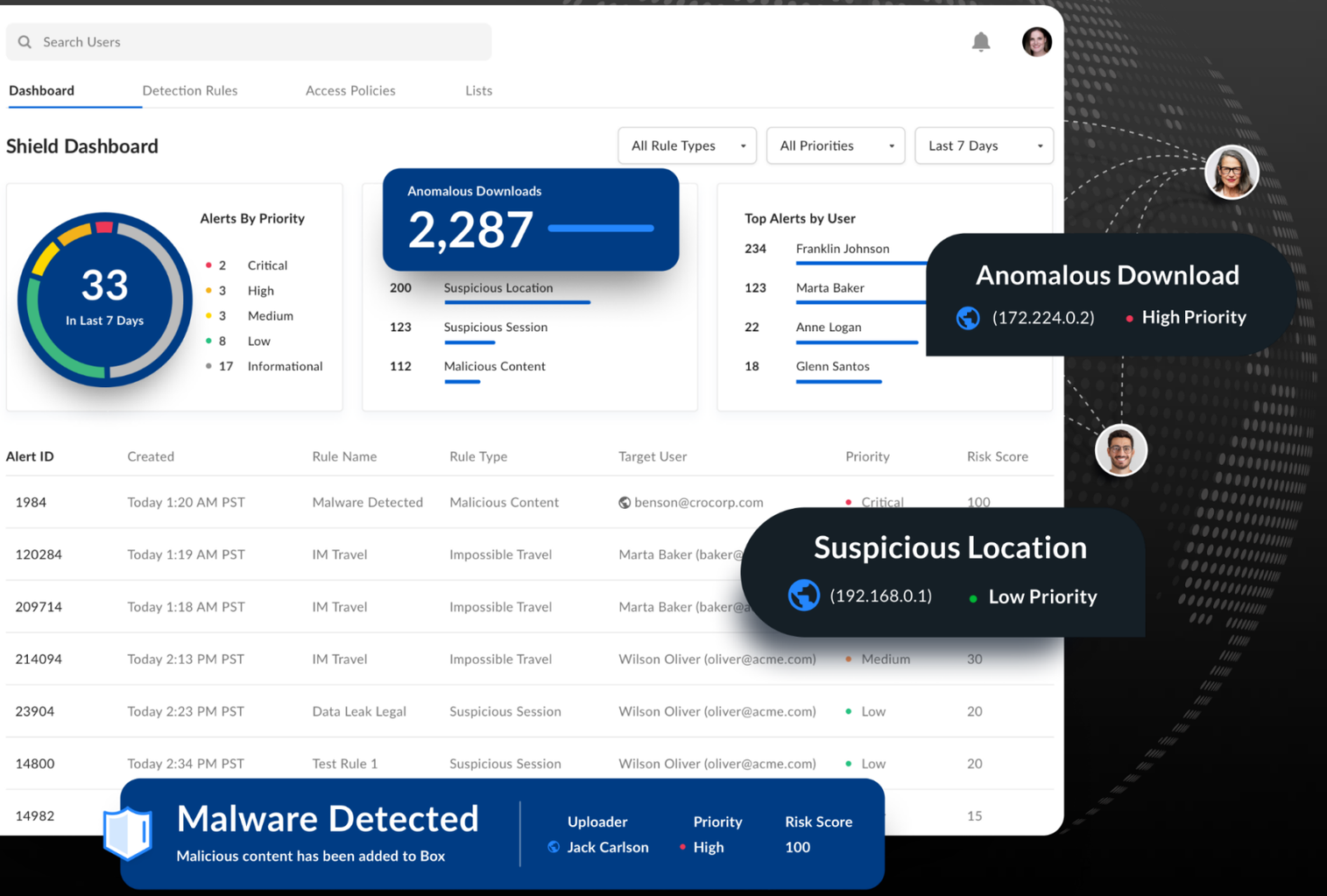
ITをシンプルにする

すべてのアプリケーション
をつなぐ
コンテンツレイヤー



AIが拡張、強化

引用：BoxJapan コーポレートピッチ



コンテンツを保護する

フリクションレスなセキュリティとコンプライアンス

脅威に対するセキュリティ

- 機微なコンテンツを識別 拡張
- データ漏えいを防御 拡張
- マルウェアやデータ盗難を検知 拡張
- 攻撃への対応と復旧

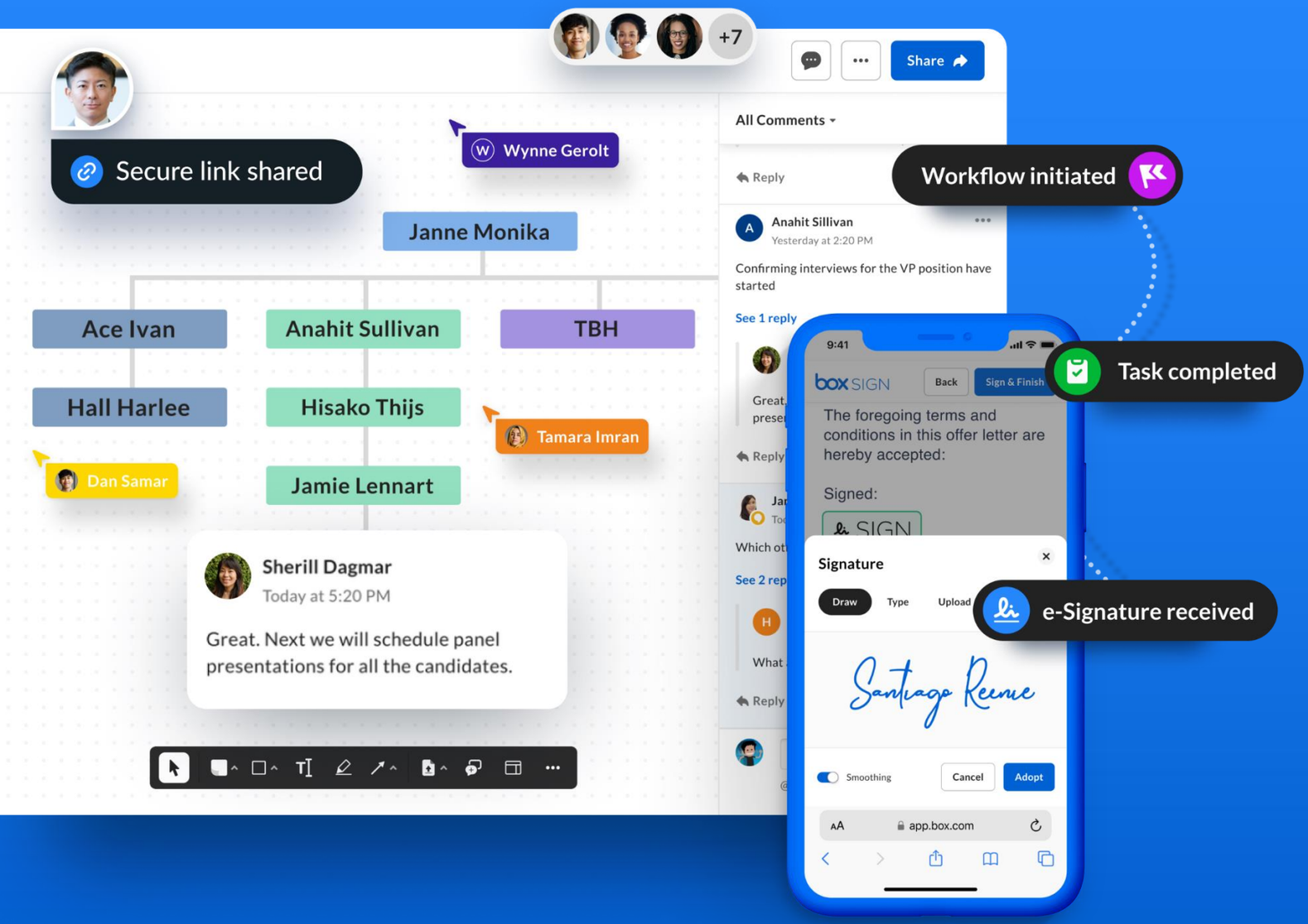
ゼロトラストアーキテクチャを維持

- コンテンツを暗号化 (転送時 / 保管時)
- ユーザーアクセスを識別、維持 拡張
- デバイスのセキュリティを確保 拡張
- 外部コラボレーションの許可
- 管理の可視性、制御、洞察 拡張

リスクの低減とコンプライアンスの確保

- 柔軟な保持スケジュール 新規
- リーガルホールドと共にコンテンツを保持 拡張
- ゴミ箱設定で廃棄を管理
- リージョン内コンテンツストレージ
- コンプライアンス認定 拡張

引用：BoxJapan コーポレートピッチ



生産性を向上する

シームレスなコラボレーションとワークフロー

どこからでもアクセス

- ファイル、フォルダ、メタデータ
- 検索 / プレビュー (140超のファイルタイプに対応) 拡張
- あらゆるデバイス(Web、デスクトップ、モバイル)

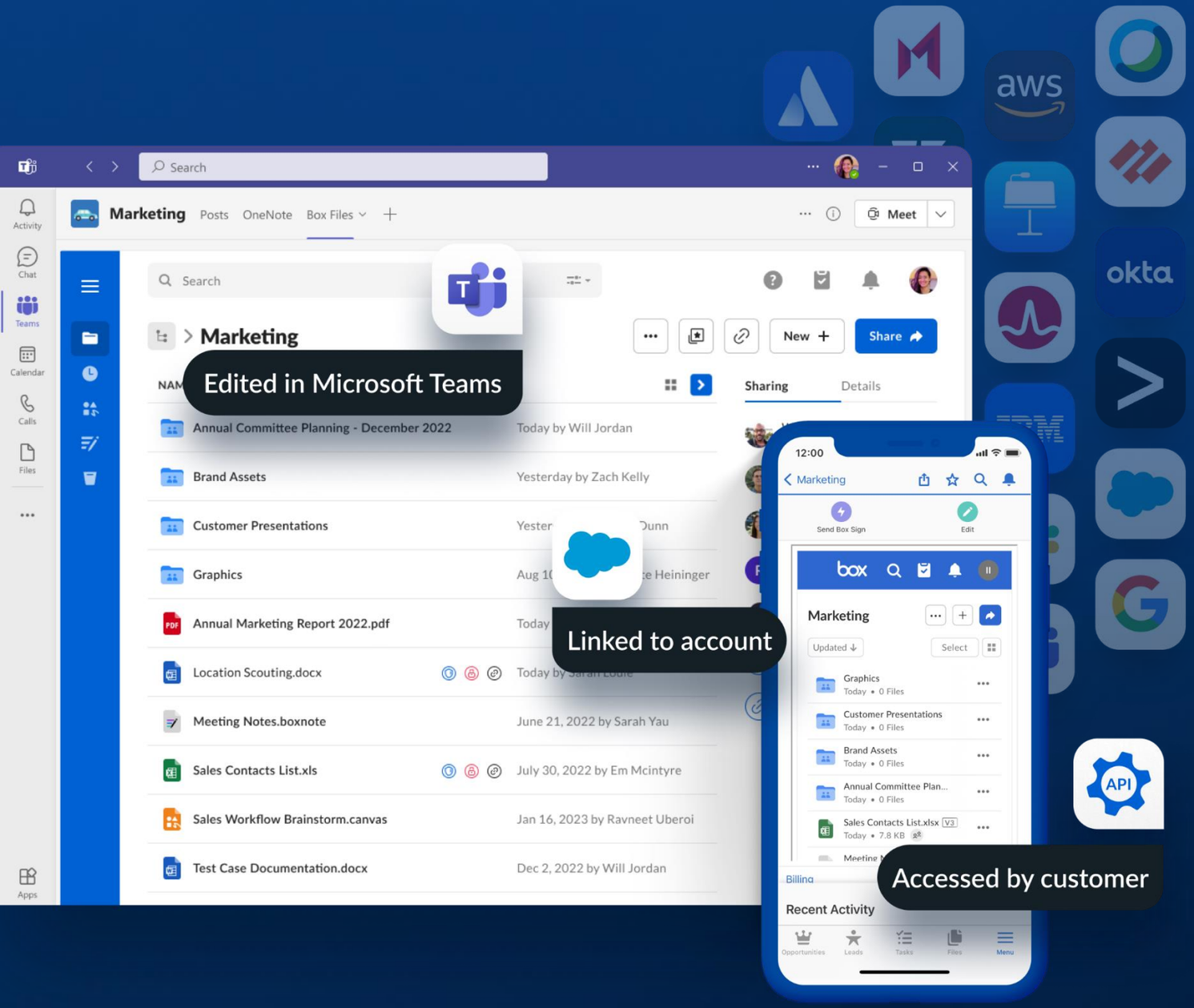
作成とコラボレーション

- 社内および社外とコラボレーション
- リアルタイムのノートとアノテーション 拡張
- デジタルなホワイトボード 新規
- 設定可能な共有リンク
- コンテンツインサイト / レポート 拡張

業務プロセスを強化

- ファイルリクエスト
- 無制限のネイティブ電子サイン 拡張
- セルフサービス、ノーコードのワークフロー
- タスクの割り当て

引用：BoxJapan コーポレートピッチ



ITをシンプルにする

すべてのアプリケーションをつなぐ
コンテンツレイヤー

セキュアなコラボレーションを促進

- あらゆる生産性スイート 拡張
  Microsoft, Google, Adobe、他
- セキュリティを統合 拡張
  Okta, Splunk, Palo Alto Networks、他

シームレスな体験を構築

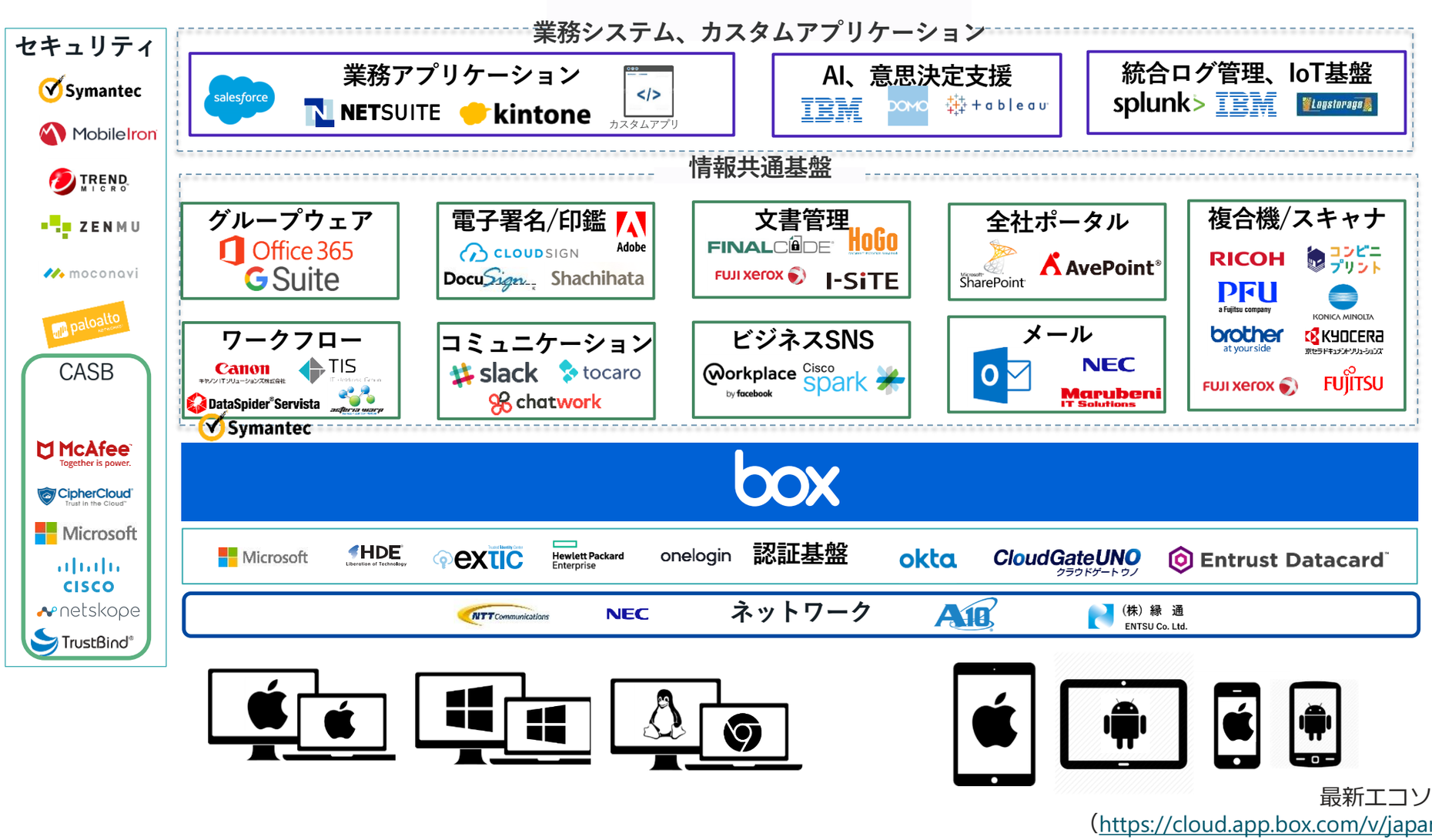
- 1,500超のアプリケーション連携
- ビジネスコンテンツを集約 拡張
  Salesforce, ServiceNow、他
- 一貫したコミュニケーション 拡張
  Zoom, Slack, Teams、他

コンテンツの価値を拡大

- コンテンツ管理ツール
  オンプレミスおよびクラウドソースから
- 堅牢な開発者ツール 拡張
  API, SDK, CLI, UIエレメント、他
- サードパーティおよびカスタムアプリケーション

引用：BoxJapan コーポレートピッチ

Boxをコンテンツのハブとし、周辺デジタル業務を連携しワンストップに効率化



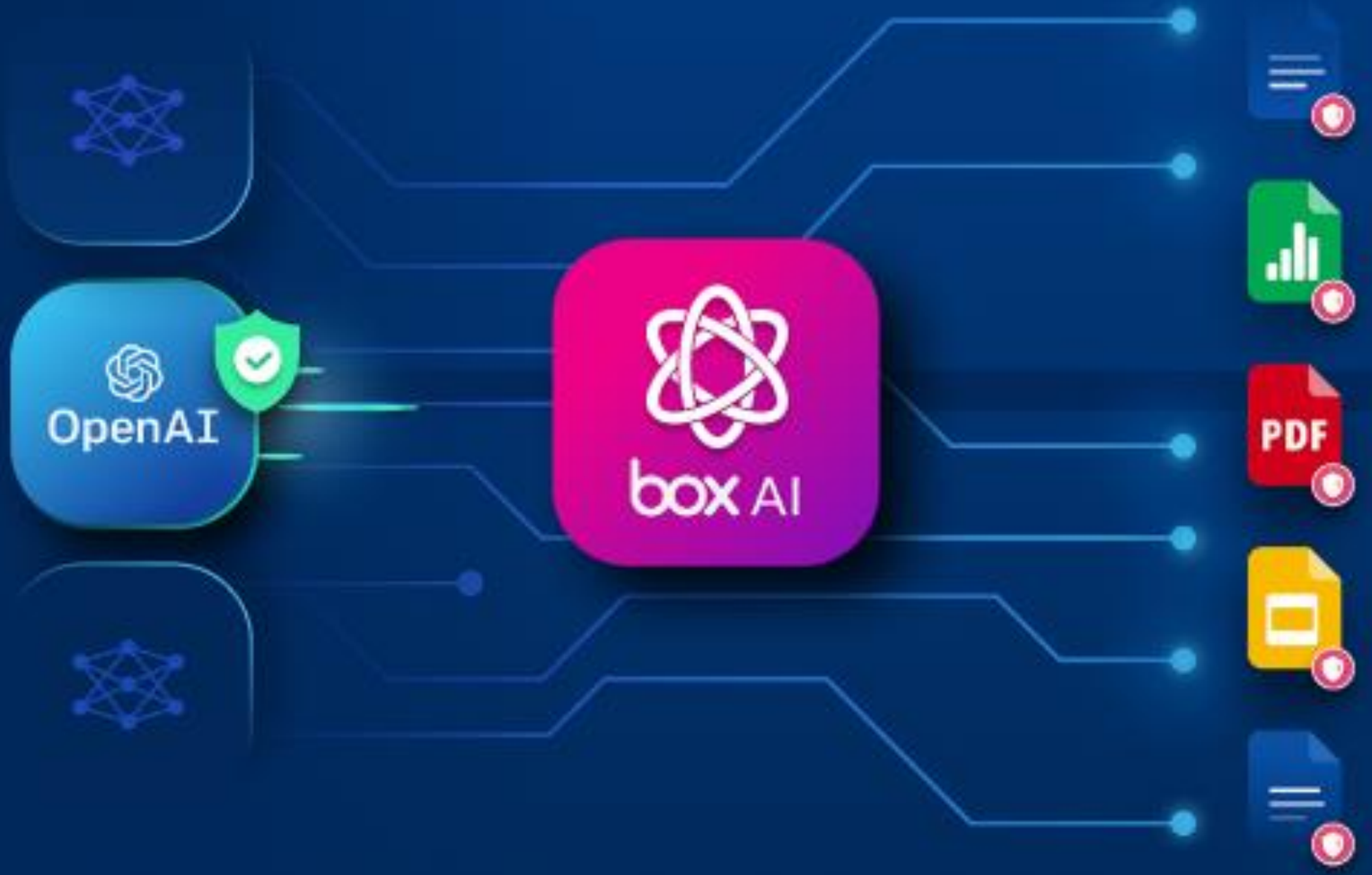
最新エコソリューション
（https://cloud.app.box.com/v/japanecosystem）

box

ご紹介

Box AI

企業コンテンツに
インテリジェンスを提供



引用：BoxJapan　Pitch Deck Box AI

box

ベータ版

Box AI

Box AI for Notes と Box AI for Documents
ベータ版は、すべてのEnterprise Plusのお客様で
2023 年11月に利用可能になりました

引用：BoxJapan　Pitch Deck Box AI

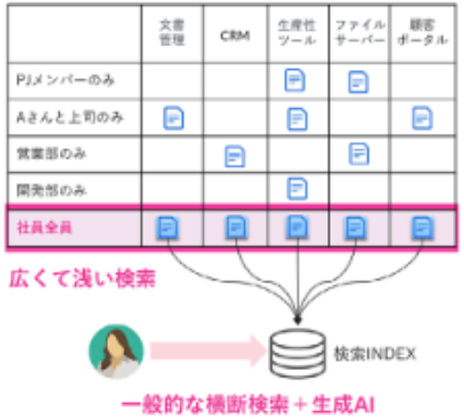
Box AIのご紹介

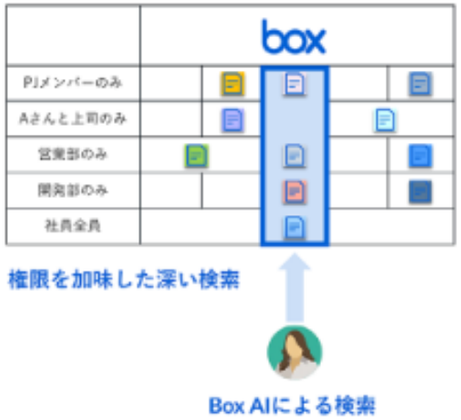
https://www.boxsquare.jp/resource/box-ai

Box AIによるコンテンツ活用

Box AIは、高度なAIモデルをコンテンツクラウドに統合した革新的な新機能です。コラボレーションやドキュメントの分類、プロセスの自動化などコンテンツ管理のあらゆる側面でBox AIを活用できます。

Box AIは、コンテンツの作成と管理、検索と探索、要約と理解といったコンテンツを活用する場面で、コンテンツを瞬時に価値ある情報に変えナレッジやインサイトを提供することで、情報を探す時間と理解する時間を劇的に短縮します。





Box AIは、Boxが提供するエンタープライズグレードのセキュリティ、コンプライアンス、プライバシーも維持します。フォルダレベルでのアクセス制御、共有リンクの設定オプション、アカウントレベルでのロール割り当て、強固なセキュリティポリシーにより、ユーザーは適切な権限で適切なコンテンツにアクセスできます。

Boxなら、通常の検索機能だけでも「権限を加味した深い検索」が可能ですが、Box AI in Hubs により、セキュアなインテリジェント検索も利用可能となります。

Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

Box AIのセキュリティとコンプライアンス

Box AIのアーキテクチャ

Box AIは、大規模言語モデル(LLM)にデータを送信する前に、アクセス権限をチェックし、質問に関連する部分だけを抽出するため、統一されたセキュリティポリシーにしたがって、適切なコンテンツのデータだけを情報源にすることができます。

Box AIの原則

Boxはお客様の利益を優先し、コンテンツを保護することを第一にしています。Box AIもこのコミットメントにしたがって、セキュリティ、コンプライアンス、プライバシーに対するガイドラインを遵守しています。

フルコントロール

企業は自社のデータおよびプロセスに対するフルコントロールを維持できます。

管理コンソールでシンプルにオン/オフを切り替えられます。

セキュリティとプライバシー

明示的な承諾を得ることなく、お客様のコンテンツを使用したAIモデルのトレーニングは行いません。

プライバシー、セキュリティに適用される規制に遵守します。

透明性

AIの動作とデータの使用に関する透明性を確保します。

合理的な範囲でAIの出力を説明し、コンテキストを提供します。

Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

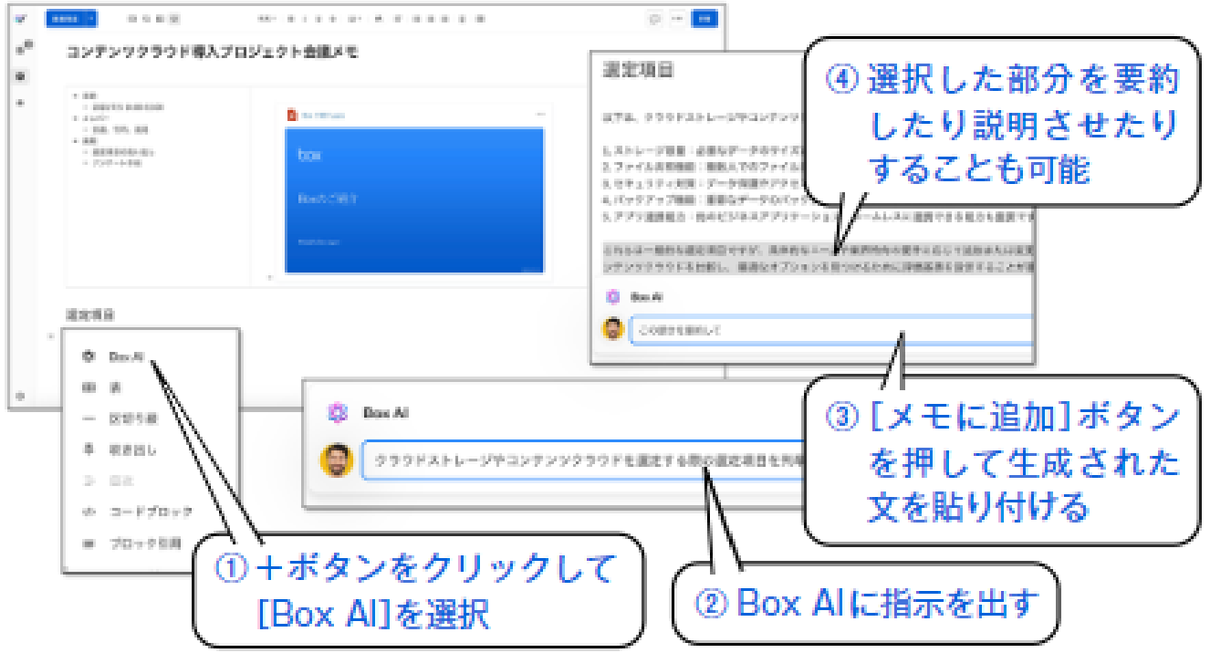
Box AI for Notes　アイディア出しや文面作成を支援する

＊ベータ版提供中。製品版は2024年提供開始予定

Box Notesで作業中に、概要の下書きや議題のテンプレート、メールの文面など、さまざまなコンテンツのアイディアの作成をBox AIに依頼することができます。営業、マーケティング、チームが新しいプロジェクトに着手する時間を短縮できます。

ユースケース

- 情報システム部が、エンドユーザーへの通知メールの文面を作成する。
- 人事部が、新入社員向けのオンボーディング資料の草案を作成する。



Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

Box AI for Documents Box上のドキュメントの要約、要点整理を行う

＊ベータ版提供中。製品版は2024年提供開始予定

Boxでプレビュー表示したドキュメントに対して、内容の要約、要点の検索、概要の下書きをBox AIに依頼することができます。会議メモやレポート、マーケティングアセットの分析にかかる時間を短縮し、より適切なインサイトを得ることができます。

ユースケース

- 営業チームが、商談の議事録を要約して、お客様の課題をより的確に理解する。
- 法務部が、複雑な契約条件を効率的に調査する。

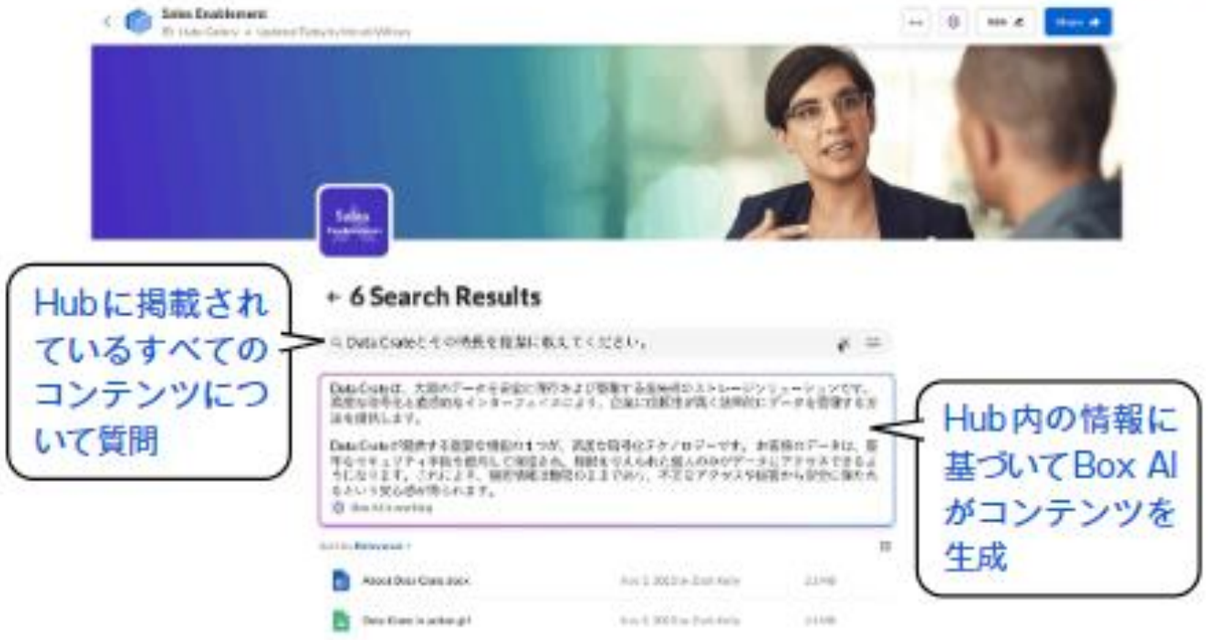
Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

Box AI in Hubs　複数のドキュメントに対して質問し、回答やインサイトを得る

＊2024年ベータ版提供開始予定

Box Hubsは、企業内のコンテンツを組織全体で安全かつシンプルに管理、整理、公開するポータル(Hub)を提供する新機能です。管理者の手を借りることなく、数分でBox内のコンテンツを見やすいプレイリストに整理して公開できます。ユーザーにはアクセス権限のあるコンテンツのみが提供されます。



ユースケース

- 営業ポータル(Hub)で、自社製品のセールスポイントを簡潔にまとめる。
- 人事ポータル(Hub)で、出張手続きの手順を確認する。

Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

Box AI API　Box AIの力をカスタムアプリにも拡張する

*2024年ベータ版提供開始予定

Box AIをAPI経由で利用できます。これを使えば、テキスト生成、コンテンツに関するQ&A、コンテンツの要約などの機能をカスタムアプリに統合できます。メタデータの自動付与にBox AI APIを活用すれば、大量のデータを処理する時間を大幅に節約できます。

ユースケース

- 営業ポータルで、顧客の関するファイルを横断検索して情報を得て、ミーティングに備える。
- 契約書にメタデータを自動的に付与する。

Box AIのご紹介

https://www.boxsquare.jp/resource/box-ai

Box for Microsoft 365 Copilot

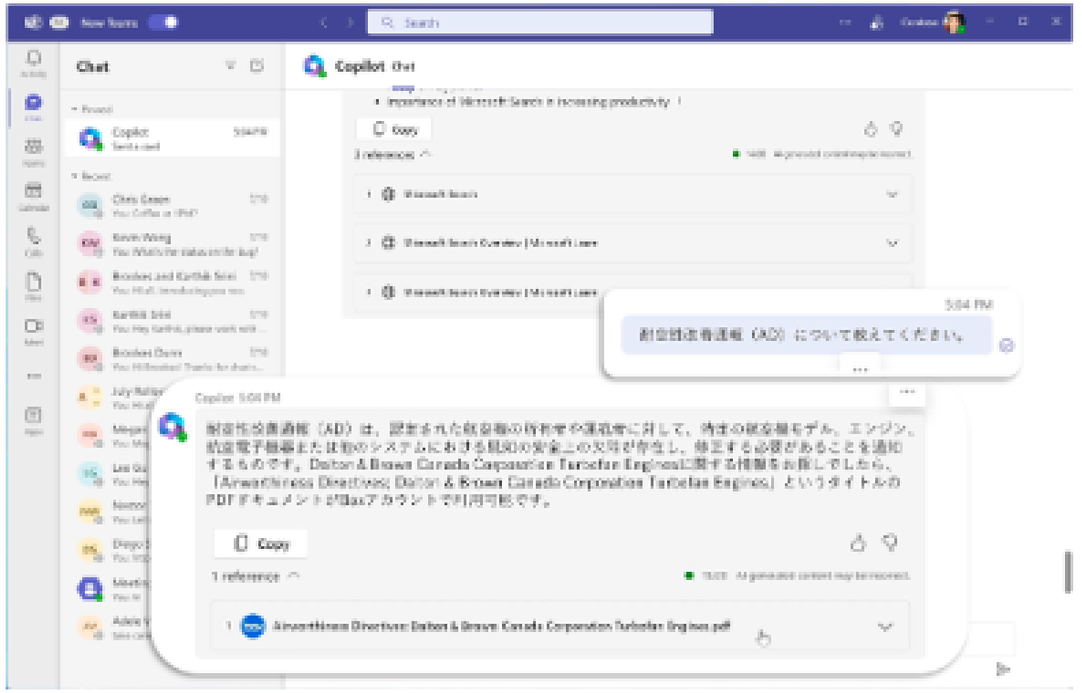
Copilot for Microsoft 365で
Box内のコンテンツを活用する

＊2024年提供開始予定

Box for Microsoft Graphコネクタを利用してMicrosoft 365とBoxとを接続することで、Copilot for Microsoft 365でBox内のコンテンツを活用できます。

ユースケース

- Microsoft Teamsで、Boxで共有されているドキュメントを要約して、インサイトを引き出す。
- Microsoft Searchで、Boxで共有されているコンテンツから質問に対する有益な情報を得る。



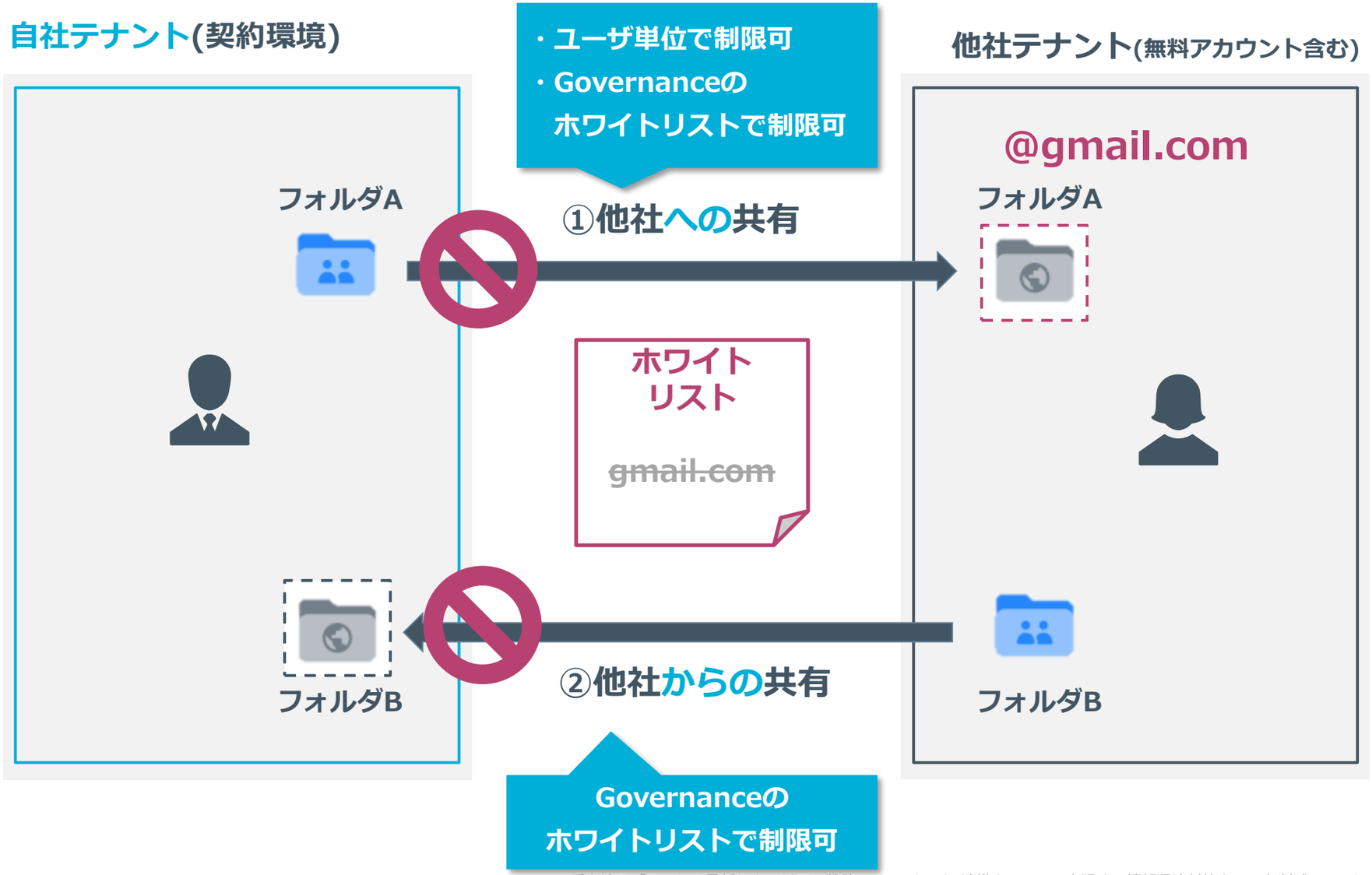
蓄えたコンテンツを守る
高度なセキュリティ

Box Governance
によるセキュリティ統制の強化

Boxの情報漏洩リスクと対策例
Box Governance

- セキュリティ統制の強化を図る有償オプション
  - 細かなコラボレーション制限
    - コラボレーションのホワイトリスト制御
  - 不正操作の証拠隠滅防止
    - 無制限のバージョン管理
    - ゴミ箱からの抹消権限管理

Box Governance
Externalを許容できる信頼先をホワイトリストに登録しコラボレーションを制限



ご参考：Box Governance

※導入時にBox Consultingの契約が必要

コラボレーションホワイトリスト

コラボレーションを許可するドメインを指定

無制限のバージョン履歴

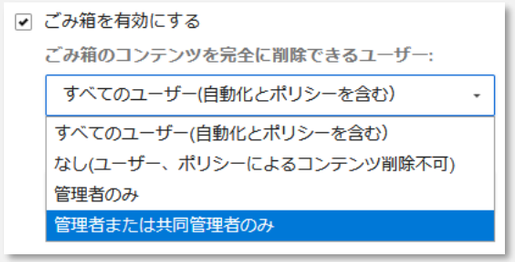
バージョン履歴をすべて保存可能

■デフォルトのバージョン履歴数
Business Plus版：**50**
Enterprise版：**100**

➡ **無制限**

ごみ箱の設定

ごみ箱のコンテンツを
完全に削除できる権限を、
適切なユーザーだけに付与



リテンション管理

コンテンツ保持期間の指定や
ファイルの削除を自動化する
ためのポリシーを設定

設定例

ファイル/フォルダ/テナント単位でポリシー適用

リーガルホールド

訴訟や調査に関連した
ユーザーやコンテンツを保持

選択した期間に対象ユーザーが
アクセス権限を保有/操作した
すべてを保持

Box Shieldによる不正操作防止強化

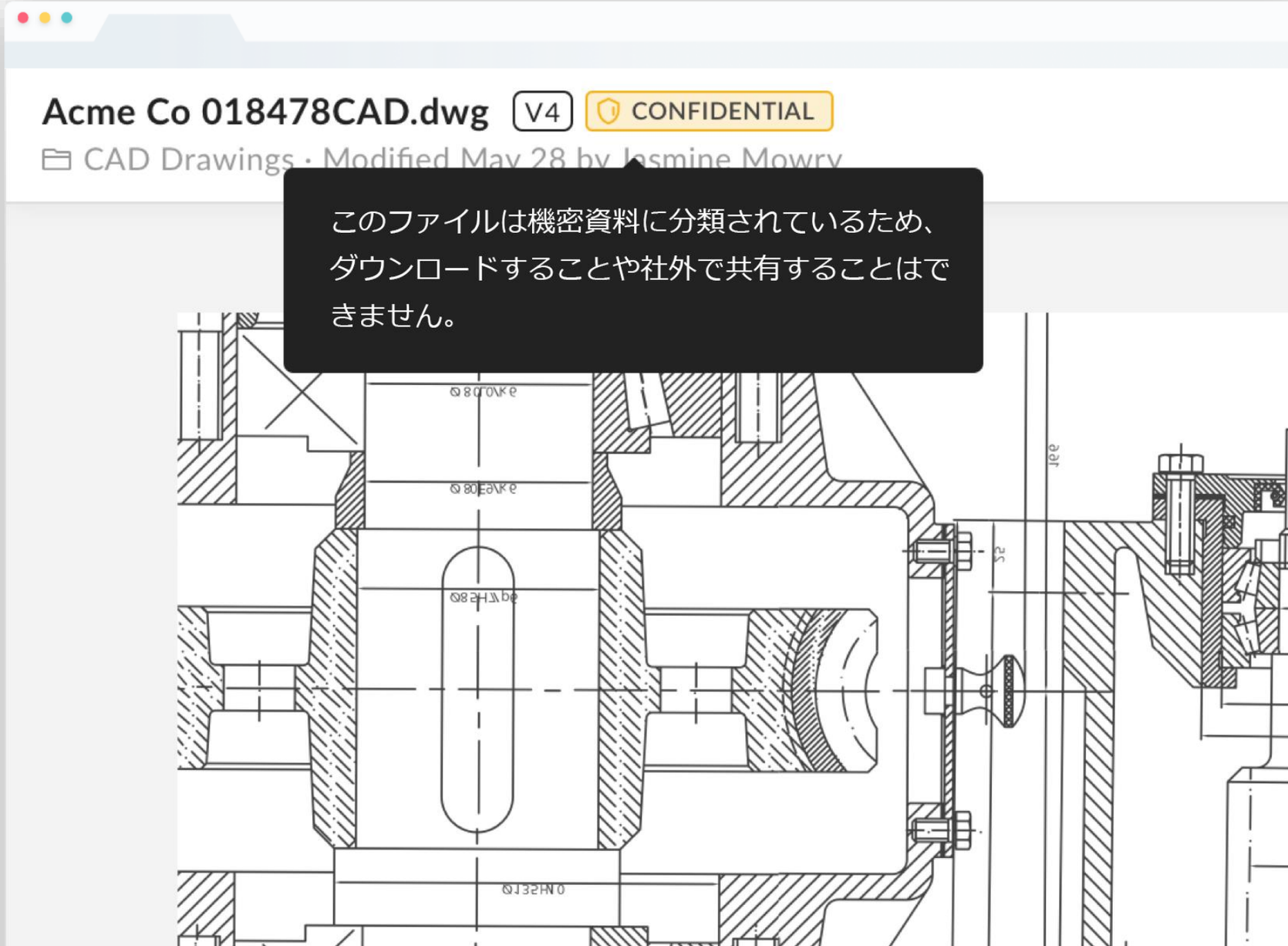
Box Shield
不正操作防止の強化を図る有償オプション

スマートアクセス

- あらかじめポリシー設計したラベルをファイルに付与
- たとえユーザに権限があってもファイルにとって許可されない操作は禁止される（→）

脅威検出

- 機械学習を用いた不審な振る舞いの検知



ご参考：Box Shield

※Box Consulting/Box Premier サポートの契約が必要

誤操作(不正操作)が心配…
誤った人の招待や、
非公開データを外部に共有しないかな..

不正なアクセスや
悪意のあるコンテンツを検知したい

スマートアクセス

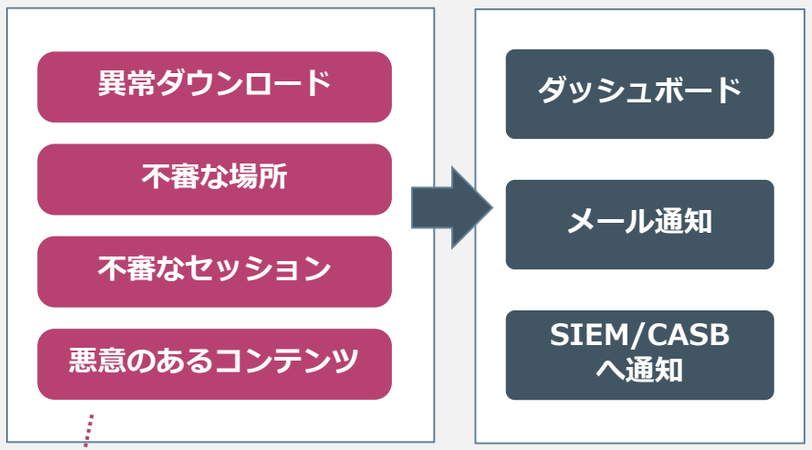
分類ラベルが付与してコンテンツを制限

■アクセスポリシー設定例
外部コラボレータ：主要パートナーリストを除くすべてを制限
ダウンロード　　：外部コラボレータは不可
印刷　　：外部コラボレータは不可

※分類ラベルはCASB製品によって自動付与可能

脅威検出

脅威シナリオを想定し検知ルールを作成



機械学習に基づくルールと
手動設定するルールで構成

ゼロトラストセキュリティとEDR

企業活動背景の変化

レガシーなセキュリティ施策を**見直すべきタイミング**が来ている

カテゴリ	従来	現在
脅威動向	**愉快犯・金銭窃取を目的とした攻撃** ➢ 公開システムがターゲット ➢ シンプルな動機（愉快犯、金銭）をベースとした攻撃	**脅威動向はより複雑に** ➢ 攻撃目的の多様化（情報窃取や金銭目的の脅迫、破壊） ➢ 手法の高度化（ファイルレスマルウェア）、経路の複雑化（サプライチェーン攻撃）
IT環境	**入口・出口対策** ➢ インターネットと社内ネットワークを分離 ➢ NW境界での一元管理・多層防御	**ゼロトラスト・セキュリティ** ➢ クラウド、組織NW外でのデバイス利用が前提 ➢ 個々のデバイスにおける防御・対処
法律・ガイドライン	**業界・組織主導での対策** ➢ セキュリティのスタンダードは少ない ➢ 特定の業界や個々の組織が主体的に実施	**ガイドライン、法律の要求増加** ➢ 所管省庁からのサイバー攻撃対策や体制構築の指示（サイバー経営ガイドライン等） ➢ 海外の法令対応（GDPR、サイバーセキュリティ法等）
組織・人	**セキュリティ部門の立ち上がり** ➢ CSIRTの立ち上げ ➢ セキュリティ対応態勢を構築	**セキュリティオペレーションの負荷増加** ➢ インシデント対応の増加 ➢ IT人材の不足、働き方改革に伴う残業規制

引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

1. 背景と課題

エンドポイントが狙われる理由とは？

考えられる３つの観点

機密・重要情報が多い

- ✓ 多くのドキュメントファイルはエンドポイントで作成される
- ✓ メール、チャット等のコミュニケーションツールを通じて、機密情報がやり取りされる

攻撃の起点にしやすい

- ✓ エンドポイントを起点にファイルサーバや認証サーバへ到達可能
- ✓ メール等の情報を通じて、他組織への攻撃の足掛かりにしやすい

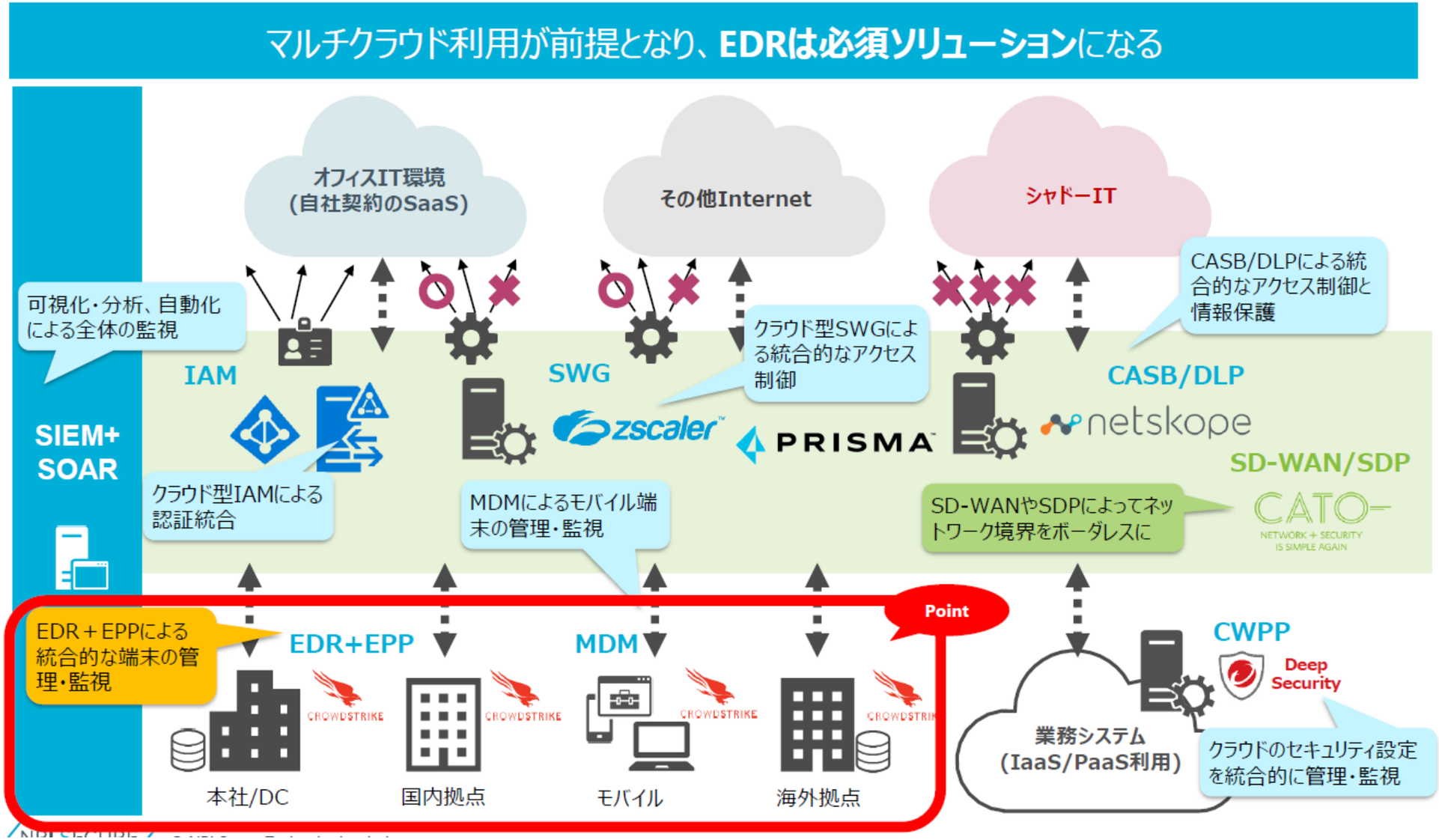
攻撃が成功しやすい

- ✓ 端末利用者によって、ITリテラシの差が大きく、ソーシャルエンジニアリング的な手法が効果的
- ✓ 端末の台数が多いと管理が行き届きにくい

引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

1. 背景と課題

ゼロトラスト化で求められるソリューション例



引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

2. EDRとは
EDRの概要

下記の４つの機能が相互に、効果的に働くことで、
脅威を可視化でき、素早く・正確にインシデントに対応できるソリューション

記録	**良質な情報を収集** 検知・調査の高精度化・高速化の礎となるデータを収集
検知	**あらゆる攻撃を識別** 高度な検知技術によって高精度に攻撃を識別
調査	**攻撃の全容を把握** ユーザビリティの高い分析機能によって迅速に攻撃を把握
対処	**迅速・適切な対処** 適切な範囲・内容の対処を迅速に実施

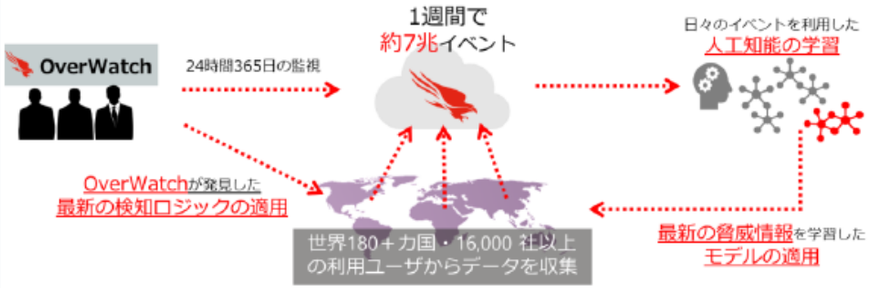
引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

3. 製品紹介

CrowdStrike Falconの強み

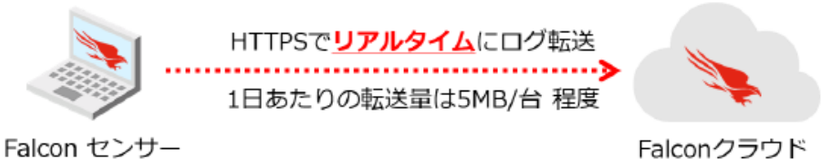
テクノロジー

- **AI/機械学習**によって、収集された全端末データと脅威インテリジェンス（IoA）でリアルタイムに**相関分析**
- 導入した組織毎ではなく、**世界規模で収集**したデータを分析し、高度で新たな攻撃手法もより 素早く発見
- 直感的操作・調査可能なグラフィカルな**分析ウィンドウ**



アーキテクチャ

- クラウドとエンドポイントセンサーによるシンプルな構成（**オンプレ管理サーバ不要**）で、保守運用負荷が軽い。
- **単一の軽量エージェント**で、アンチウィルス含む様々な機能を提供し、**追加機能も容易に導入可能。**導入後の**再起動が不要。**
- WindowsやMac、Linuxなど**複数OSに対応**



インテリジェンス

- 1週間で約7兆の蓄積されるビックデータを活用・分析することで構築する**脅威インテリジェンス**
- 各国のサイバー攻撃グループのTTPs*に関する情報を調査・保持しており、米国政府などへの協力実績も豊富

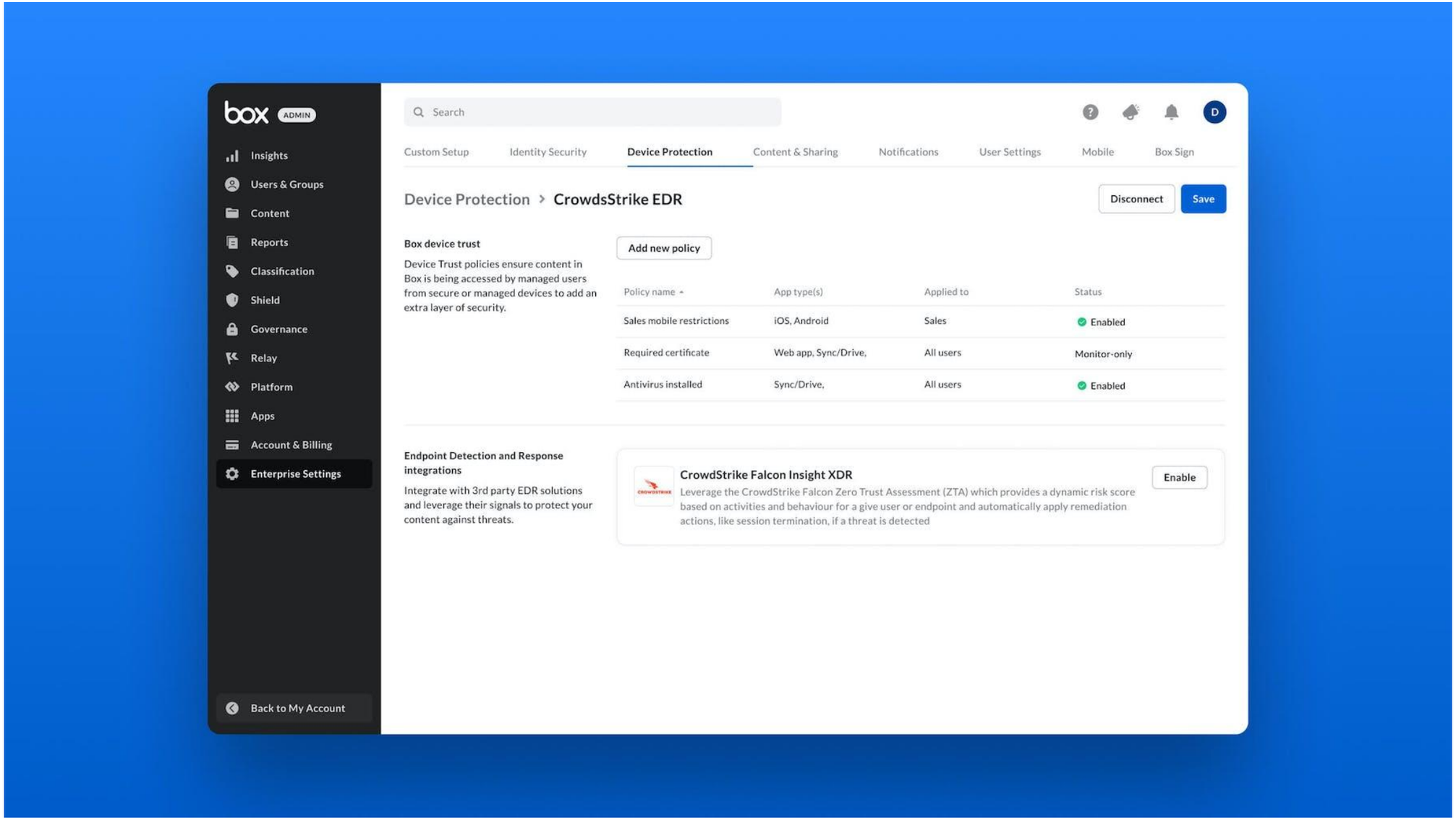
*Tactics, techniques and procedures

引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

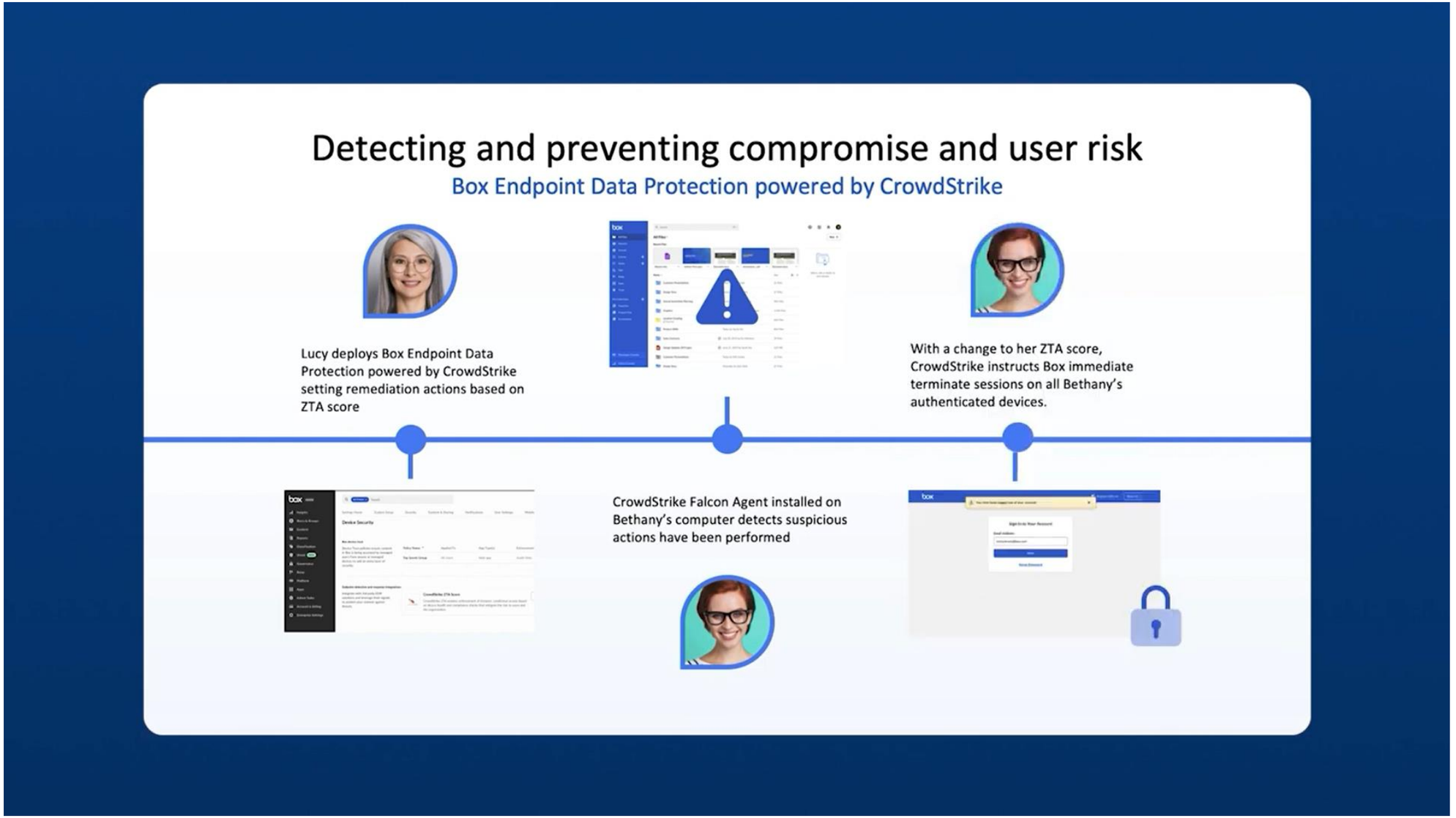
引用：CrowdStrike Blog, CrowdStrike Partners with Box to Add Automated Protections Against Security Breaches and Data Loss
https://www.crowdstrike.com/blog/crowdstrike-box-partnership-adds-automated-protections/

大手EDR製品 CrowdStrikeとの連携機能が登場（クローズドβ中）

https://www.boxsquare.jp/blog/boxworks-2023-unlock-value-your-content



Falcon Zero Trust Assessmentのリスクスコアを使って Boxへのアクセスを動的に制御



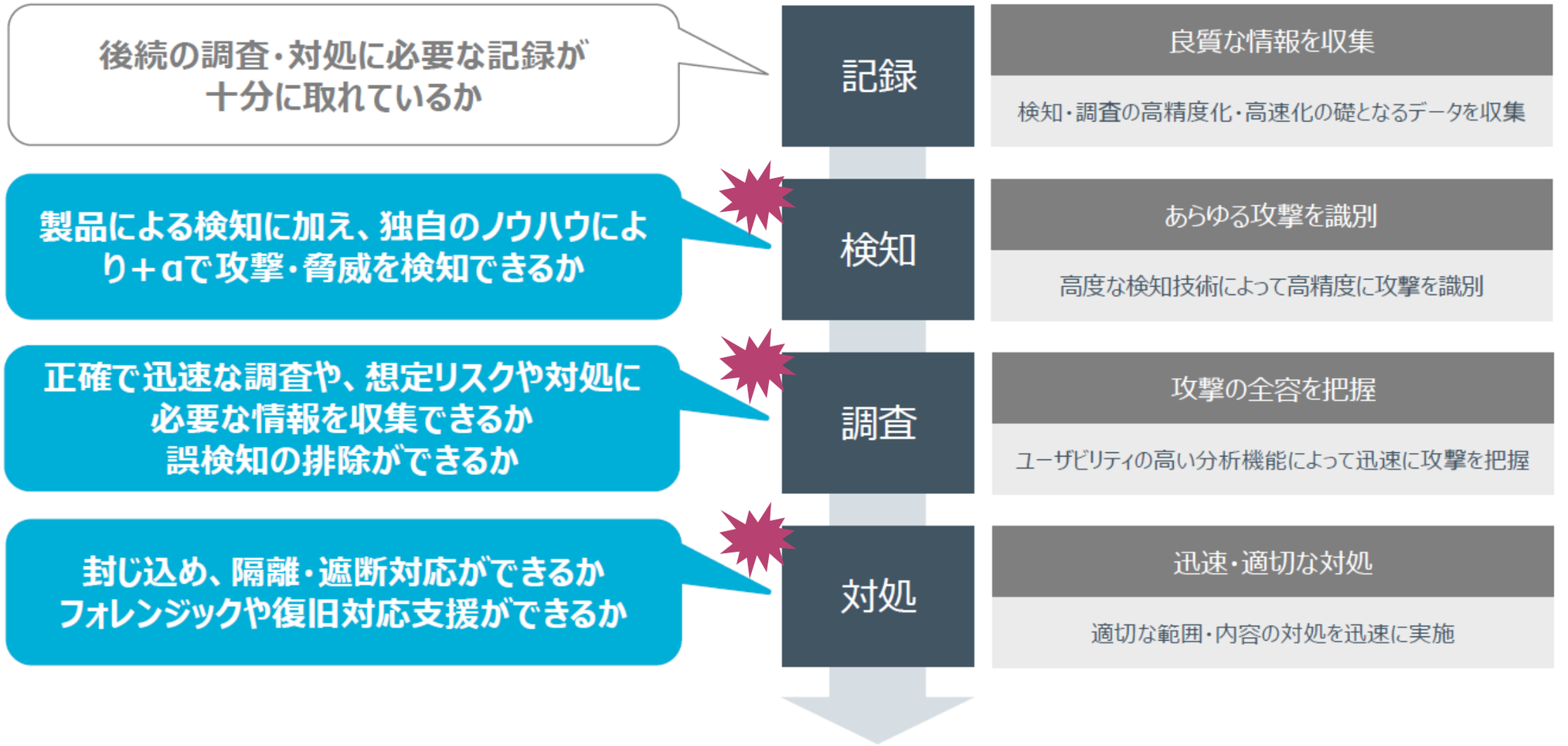
引用：Box公式Youtube, Combating cyberthreats with powerful security tools, https://www.youtube.com/watch?v=HXFIknf7fDU

NRIセキュアの
マネージドEDRサービス

4.運用における課題

EDR運用のポイント

EDRの特徴的な４つの機能（記録・検知・調査・対処）を相互に効果的に働かせ、適切なセキュリティ運用を行うには、高度なノウハウやスキルが必要です。

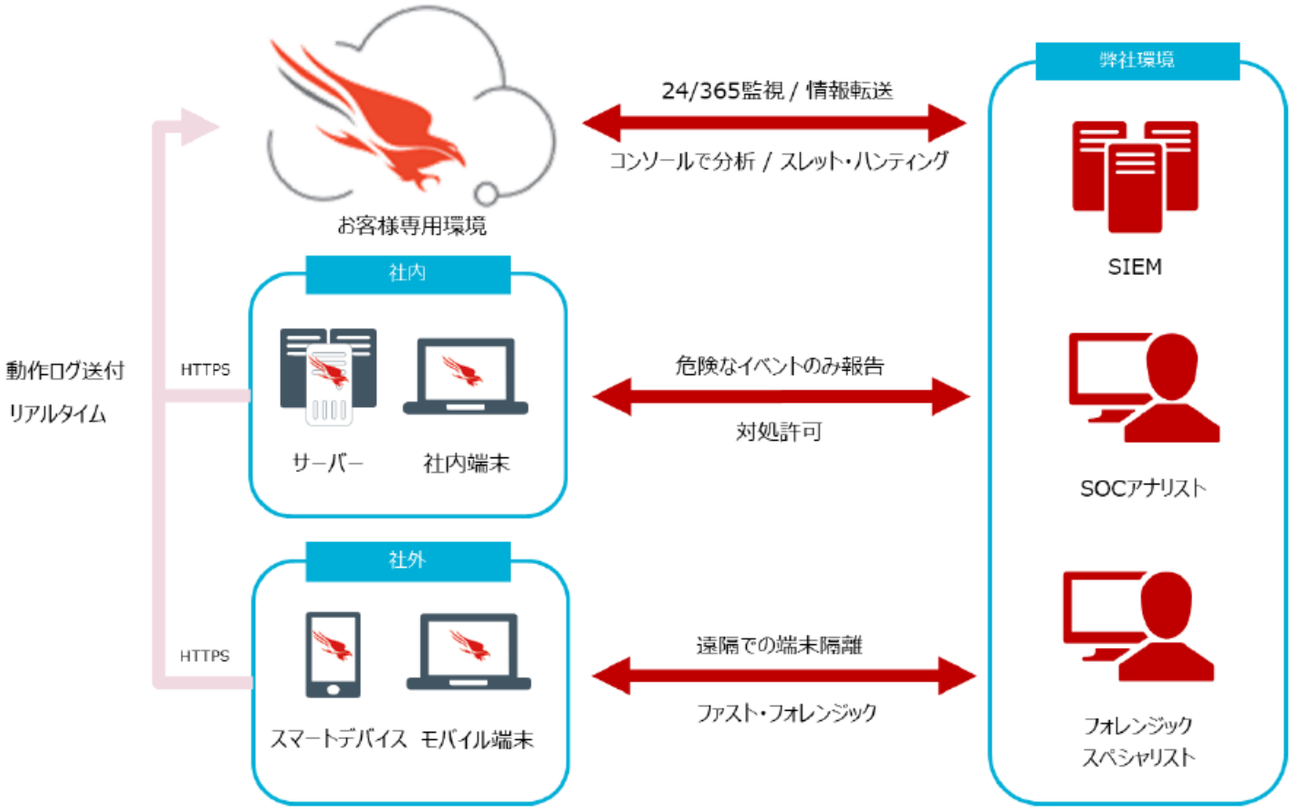


引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

5. 運用サービスの紹介

サービス導入イメージ

- 社内端末やモバイル端末で発生するリスクを**24時間365日監視**します
- 潜伏していた**未知の脅威も洗い出し**、危険な端末は**遠隔でNW隔離**することができます
- 万一インシデントが発生した場合も、**リモートで迅速にフォレンジック調査**を実施します



※NRIセキュアテクノロジーズ株式会社は、CrowdStrike社製品の取扱を認められた日本初のMSSPベンダです
※スマートデバイス(iOS/Android)については、本サービスの提供範囲外です。（2021年4月現在）

引用：NRIセキュアテクノロジーズ, マネージドEDRサービスご紹介資料

NRIセキュアが実現できること

会社概要

NRIセキュアテクノロジーズは野村総合研究所を母体とする
企業情報セキュリティのリーディングカンパニーです

社名	NRIセキュアテクノロジーズ株式会社（略称：NRIセキュア）
事業内容	企業の情報セキュリティに関するソリューションの開発・提供
設立年月日	2000年8月1日　※サービス提供開始：1995年
資本金	4.5億円
株主	株式会社野村総合研究所
代表取締役社長	建脇 俊一
社員数	連結：750名、単体：638名　（2024年1月1日現在）
拠点	東京（本社）、横浜、アメリカ合衆国（北米支社）
グループ会社	株式会社ユービーセキュア、株式会社NDIAS
認証取得	ISO/IEC 27001認証取得　IS 75215 / ISO 27001

セキュリティコンサルティング

国内サイバーセキュリティ
コンサルティングサービス市場

ベンダー別
売上
No.1

3年連続
シェアNo.1
ITR Market View2019

セキュリティ監視・SOC

ジャパン
マネージドセキュリティサービス

プロバイダー
オブザイヤー

4年連続受賞
2020フロスト&サリバン
ベストプラクティスアワード

セキュリティ診断

国内Webアプリケーション
脆弱性検査ツール市場

市場シェア
No.1

5年連続
シェアNo.1
富士キメラ総研2019年度調査

セキュリティソリューション

統合IAMソリューション
「Uni-ID Libra」
IDM／IAM市場

市場シェア
No.1

3年連続
シェアNo.1
ITR Market View2021

セキュリティと利便性は利益相反の関係になりやすい。
NRIセキュアはその構造上、セキュリティを正義とした事業継続が行える

NRIセキュアという会社

- NRIの完全子会社であり、株式市場の原理から離れて**経営の自由度が高く**、敵対的買収のリスクもない
- NRIグループから**セキュリティの専門家集団**としての職能を期待されており、**自らの職能に集中**できる
- **セキュリティ**は目に見えず、**利益追求を前に一定の線引きがされがち**な部分
  NRIセキュアはその構造上、**セキュリティに軸足をおいた意思決定**や投資開発を付加価値とし事業継続できる企業
- **社員は全員野村総合研究所(NRI)の採用**を経て出向し、待遇は共通※
  NRI社員としてのマインド・スキルセットを備えマネジメントや品質の基準も同等

※ 参考：NRIセキュア採用ページ募集要項： https://www.nri-secure.co.jp/recruit/recruit/recruitment-info

NRIセキュアテクノロジーズの付加価値

セキュリティをごまかさない。
便利・便益を前にしても揺るがない。

NRIセキュアテクノロジーズの付加価値

このスタンスを取れる会社だからこそ
セキュリティにフェアな立場から
お客様にメリット・デメリットを
正直にご提案できる

テナント設定のハードル

unsplash.com

Boxのセキュリティ課題と対策ノウハウ提供が可能です
弊社までお問い合わせください

- NRIセキュアはセキュリティ専門家としての立場から、**Boxの高い自由度ゆえの情報漏えいリスクを検証**しノウハウとして整理し、有償オプションや他のセキュリティ製品との併用を含め**取りうる対策例をご用意しております**
- フォルダ設計やテナント設定に関する工程では**弊社セキュリティ設計のノウハウをご提供し**、貴社セキュリティベースラインに合わせた**セキュリティ要件・設計のチューニングをご支援します**

Boxセキュリティ課題と対策一覧
操作ミスや内部不正を含め、Boxを使うことで生じる情報漏えいリスクについて課題と対策をまとめております

Boxの情報持ち出しリスクと対策一覧

お問い合わせを多く頂くポイント　○：根本対策　△：部分対策

観点	項番	持ち出しリスク／監査リスク	Box機能による対策例				その他対策	
			Bus	Bus+	Ent/Ent+	有料オプション	運用対策	3rdParty
認可外アカウントの利用	1-1	会社ドメインを使った無料アカウントの作成・私的利用	○AutoRoll-in					○CASB製品
	1-2	私的に作成した無料アカウントの社内環境からの利用	△BoxVerifiedEnterprise				○URLフィルタリング	○CASB製品
	1-3	プロジェクト終了、退職など役目を終えた残存アカウントの利用	△レポート出力				○ログから棚卸	
認可外環境への持ち出し	2-1	許可されたネットワーク外からの契約テナントの利用	–	○IPアドレス制限				
	2-2	ポリシー違反デバイスからの契約テナントの利用	○SSO認証連携(IdPにてポリシー判定) ※Entはデバイストラストあり					
	2-3	会社アカウントとコラボレーションした私的／不正な外部ドメインアカウント	–			○Governance（ホワイトリスト）		
	2-4	Box上の特定コンテンツを本来許可されていない相手に誤共有（コラボ／共有リンク）	–			○Shield		
	2-5	認証強度不足を要因とした不正ログイン	○SSO認証連携(IdPにて認証強度を保証) ※Entはパスワードポリシー設定可					
危険・不正なBox操作	3-1	ユーザのモラル・リテラシーの無い無秩序なフォルダ作成・共有	○クローズドフォルダ構成					
	3-2	ウィルス／マルウェアのアップロード・共有	△VirusScan			○Shield		○CASB製品
	3-3	不正操作の証拠隠滅（ゴミ箱からの抹消、バージョン履歴からの追い出し）	–			○Governance（版数、ゴミ箱制御）		
危険なBox操作の監視	4-1	Boxへのアップロードミス（ファイルの取り違え、機密情報の誤った社外共有）	△通知機能（アップロード）			△Relay（承認タスク）		
	4-2	不正な操作（振る舞い）（マルウェアアップロード/大量ダウンロード/セッションハイジャック等）	–			○Shield	△ログ監査	
社外フォルダの匿名化	5	社外から招待されたフォルダや操作の履歴が管理者向けには匿名化される	–			△Governance（ホワイトリスト）		△CASB製品
データレジデンシー	6	データが海外DCに保管される	–			○BoxZones†		
ファイルの独り歩き	7	Boxからダウンロードされたあとのファイルはトレースできない	–					○IRM製品

† インデックス情報など、一部データはBox北米DCに保管

NRI SECURE © NRI SecureTechnologies, Ltd.　8

NRI SECURE