

# クラウド利用時のセキュリティと IDaaSについて

国内B2B営業本部 国内ソリューション営業部

2022年1月

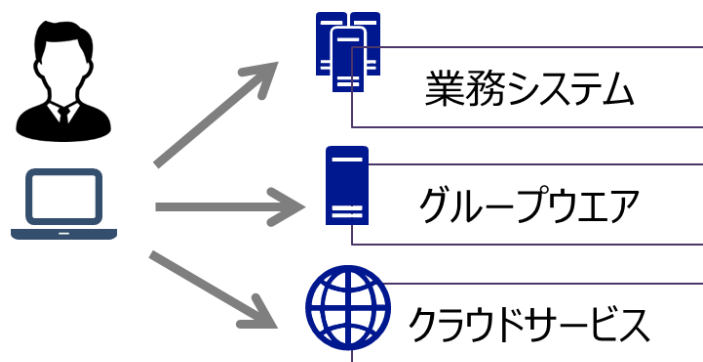


- **IDaaS** ..... **3**
- **HENNGE** ..... **12**
- **LINC Biz** ..... **19**

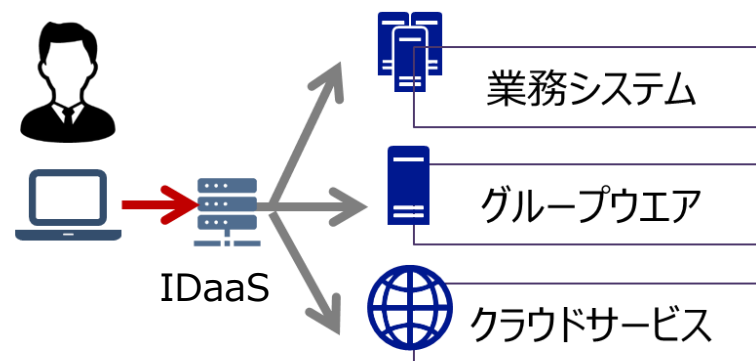
# IDaaSとは？

## IDaaS とはクラウド型ID管理・統合認証サービス

「ID管理」はこれまでオンプレミスの一部として機能しており、企業内と企業外の境界は「ファイアウォール」が保護してきました。しかし、現代はクラウドサービスやスマートデバイスの発展により、境界の概念が「アイデンティティ（身元情報）」に移り変わりつつあります。このクラウド時代に安全性と効率化を両立するためには、ID管理や認証・アクセス制御などをクラウド上でまとめて運用できる、IDentity as a Service : IDaaSが必要不可欠な仕組みとなります。



各システム利用時に、毎回、  
個別 ID・PASSでログイン



一回のログインのみで、  
各システムの利用が可能になる

IDaaSはIDentity as a Serviceの略

# IDaaSは何故必要か？

## クラウドのメリット



IDとPWがあれば場所を選ばず  
誰でもどこからでもアクセス出来る

## クラウドのデメリット



辞書攻撃

フィッシング詐欺

リスト攻撃

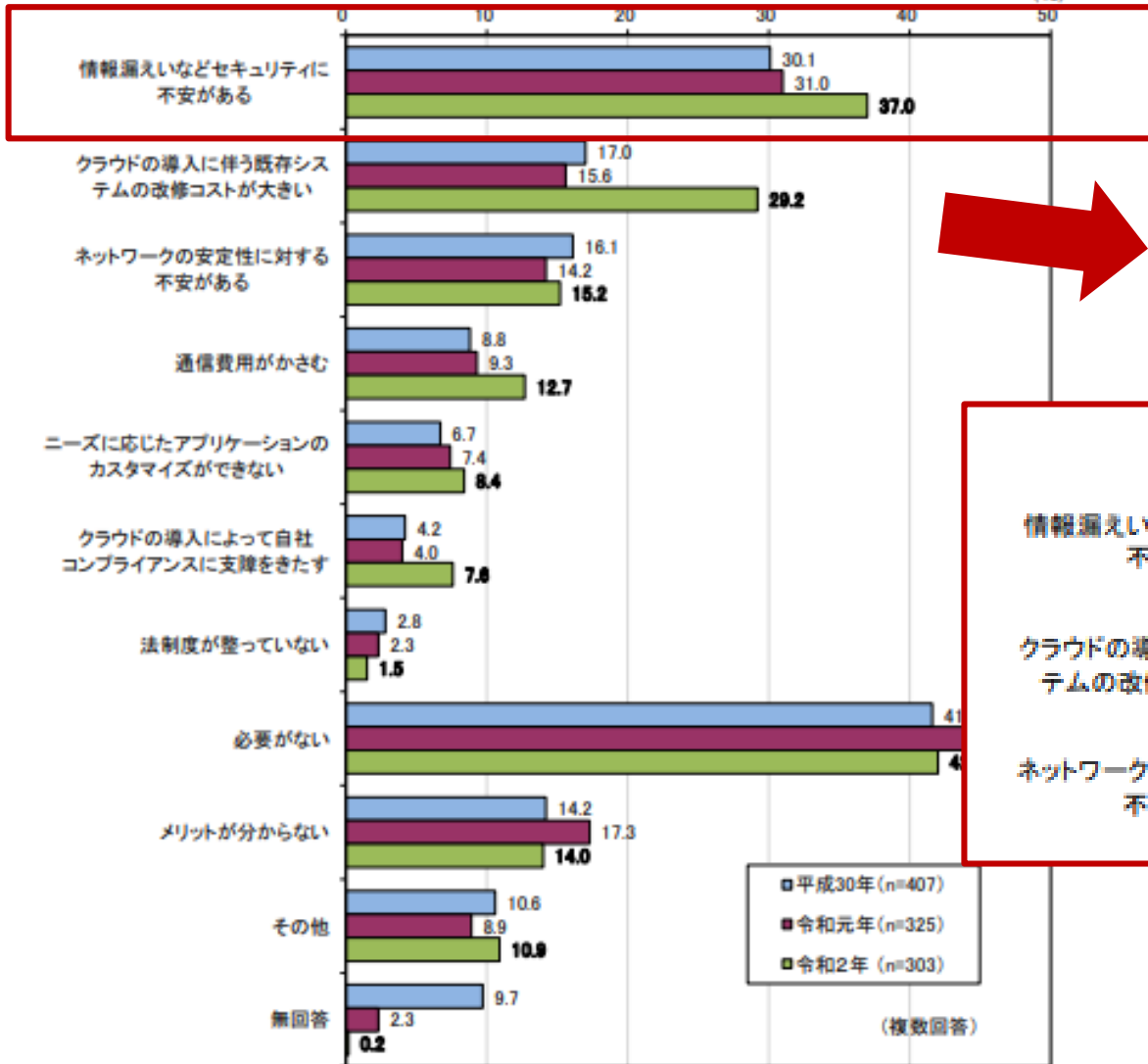
などなど

ID/PWが漏洩してしまうと  
不正アクセスによる情報漏洩が起こる

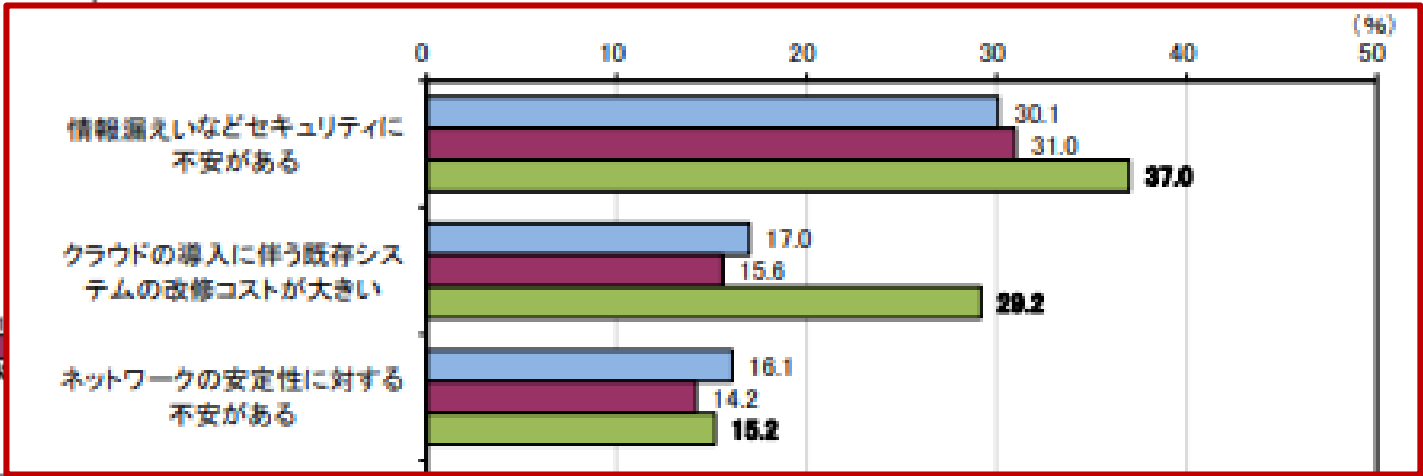


# 利用者が感じる不安

(出典)総務省 令和2年通信利用動向調査報告



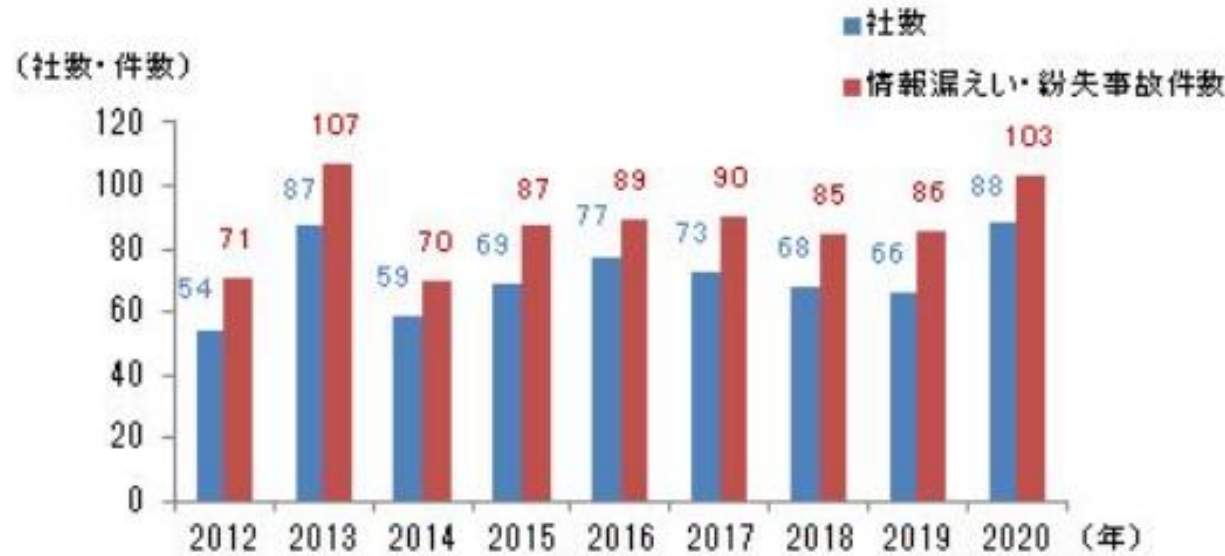
3社に1社が情報漏洩などのセキュリティに不安がある



# 個人情報漏洩

上場企業の個人情報漏洩事故件数は、前年比2割増で7年ぶりに100件超え、社数別では調査開始以来最多。原因別では「ウイルス感染・不正アクセス」が5割を占める。

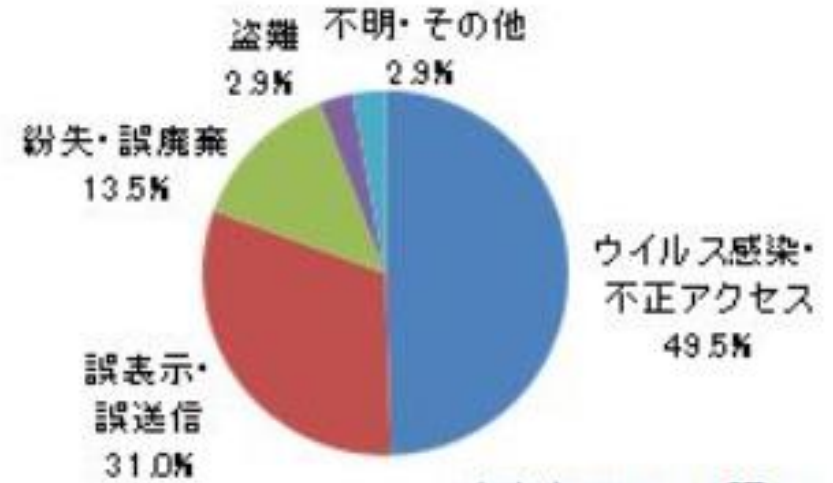
漏えい・紛失事故 年次推移



※ 年毎に集計しているため社数の合計は424社を上回る

東京商工リサーチ調べ

情報漏えい・紛失件数 原因別

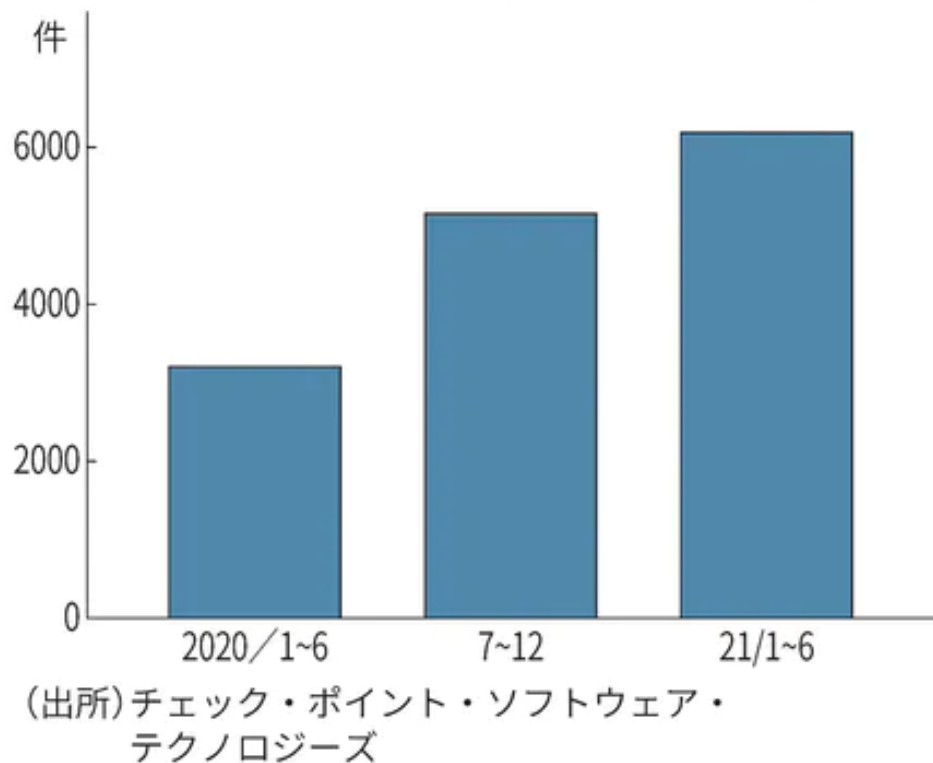


東京商工リサーチ調べ

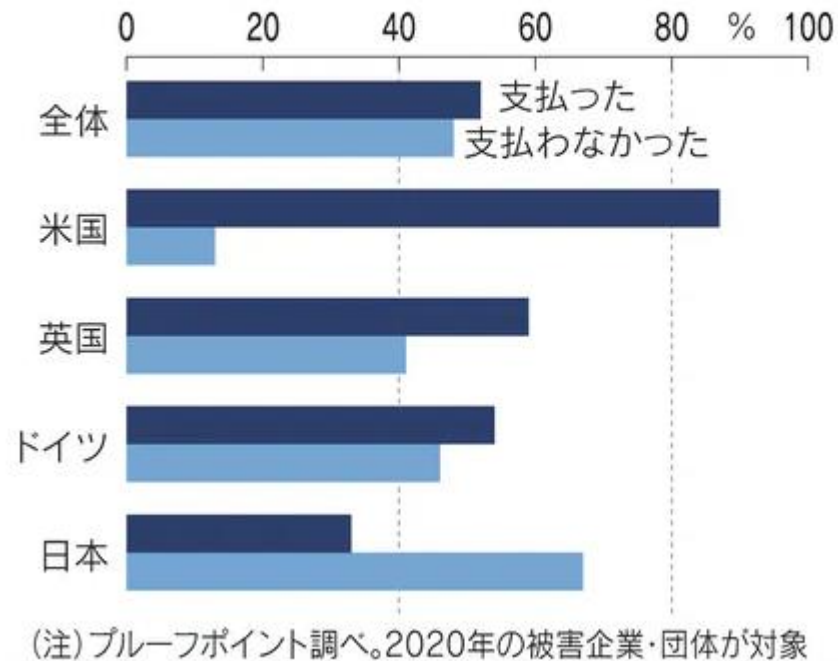
# ランサムウェア

ランサムウェアの被害は世界で拡大。一件あたりの身代金要求額も増加しており、かつ身代金支払いに応じる企業が増えています。

ランサムウェアの被害件数は世界で拡大



ランサムウェアの身代金支払いに応じる企業は多い



# IDaaSが利用されるようになった背景

ITの利用環境の多様化とID利用の増加がもたらすリスクを抑止するソリューションとして、クラウド上のさまざまなサービスのID管理を一元的に行うIDaaSが注目されています。

## IDaaSが注目される背景

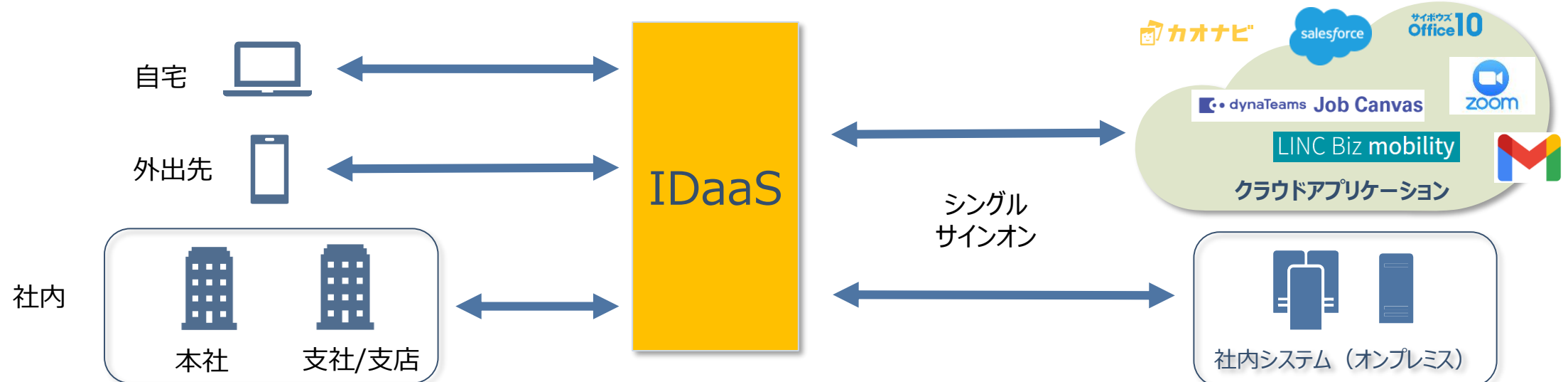
- 働き方の変化
- テレワーク環境の普及
- SaaSサービスの拡大

## ID管理の課題

- SaaSシステム毎のID/パスワード管理が煩雑
- いつでもどこからでもアクセスできてしまう
- 不正アクセスによる情報漏えいリスクの増加
- 管理者の工数増大

## IDaaSの特徴

- シングルサインオンによるID入力の手間削減
- アクセス環境に応じた認証方法の強化
- 多要素認証を用いた不正アクセスの防止
- IDの一元管理による管理者の工数低減





# IDaaSを利用しない場合の問題

## (1) パスワードマネージャでは不十分

パスワードマネージャは、個人による管理が前提のため、企業で利用する場合に適用される、多要素認証、アクセス元IPアドレスの制限、Active Directoryや人事システムなどとの連携、パスワードなどクレデンシャルの一元化といった管理を行うことができません。

## (2) Active Directoryでは不十分

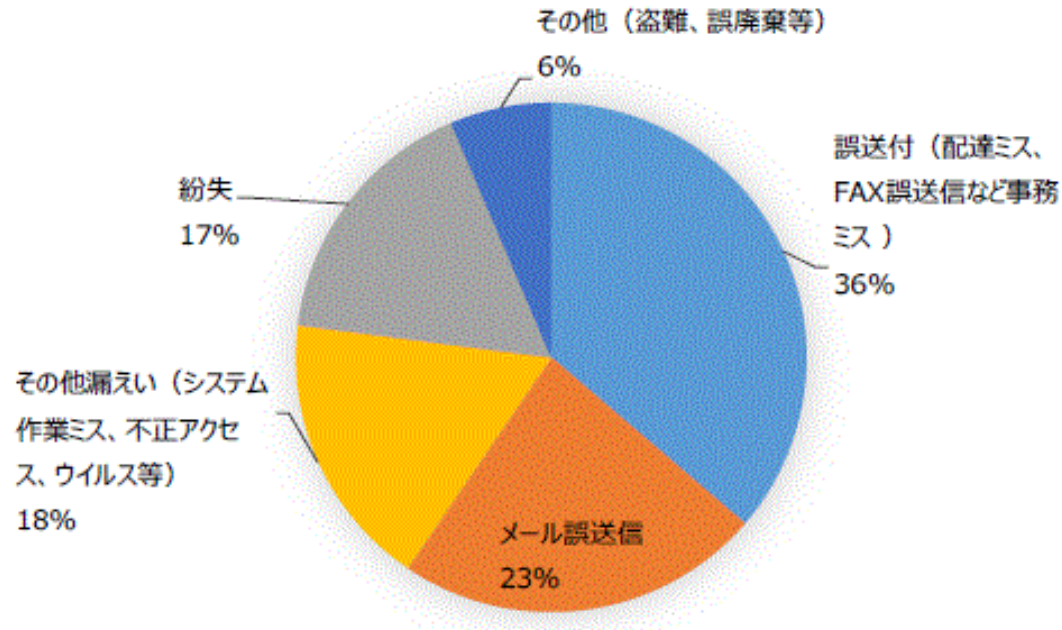
「Active Directory Federation Services (ADFS)」を利用することでファイアウォール外（社外）のクラウドサービスへシングルサインオンすることが可能になりました。この「ADFS」を採用するとID管理のベースとなるシステムを、AD環境がある「社内ネットワーク」に置くこととなります。ただし、ADFSにはデメリットがあります。

- ・社外から社内へのネットワークの穴あけなどによるセキュリティリスク
- ・中継するリバースプロキシなどの導入による運用管理の負担増
- ・クレームルール（ADFSに記述する制御ルール）の複雑化による運用管理の負担増

# 脱PPAP

PPAP（パスワード付きzipファイルをメールで送り、別のメールでパスワードを送信する暗号化の手順）は2020年11月に内閣府と内閣官房で利用廃止に踏み切りました。今後、同様の動きは民間にも拡大すると予想されます。

## 【個人情報漏洩事故の多くはメール誤送信】



（出所）日本情報経済社会推進協会（JIPDEC、2019年度）の資料を基に三井住友DSアセットマネジメント作成

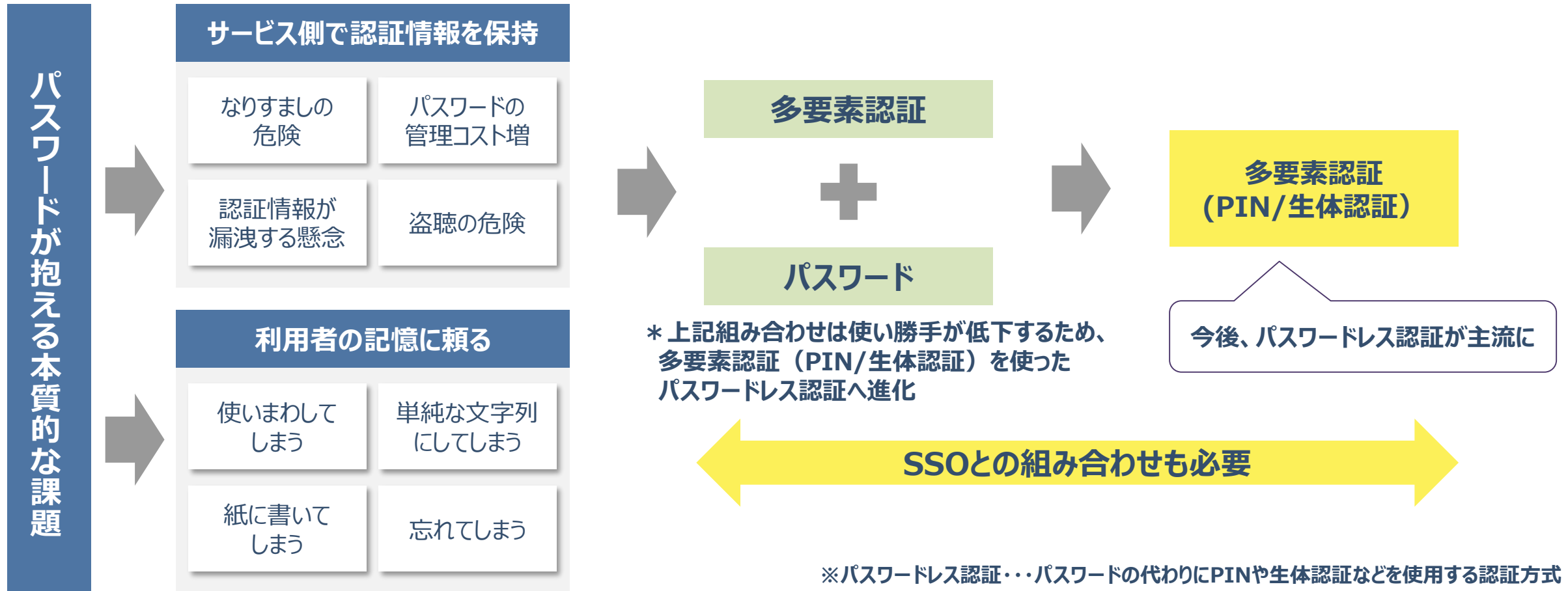
## 【PPAPの問題点】

- (1)パスワード付きzipファイルになりすましたマルウェア攻撃が報告されている。
- (2) zipファイルは暗号強度が弱く、パスワードが短時間で解読される
- (3)パスワード付きzipファイルが、攻撃者に奪取された場合、同じ通信経路で送信しているパスワードも同様に奪取される事が予想される

PPAP: Password Password Angouka Protocol の略

# 脱パスワード

サービス側が保持する認証情報が、サイバー攻撃により情報漏洩することで、パスワードが悪用されます。パスワードを複雑にしたとしても、フィッシング詐欺等には効果がありません。

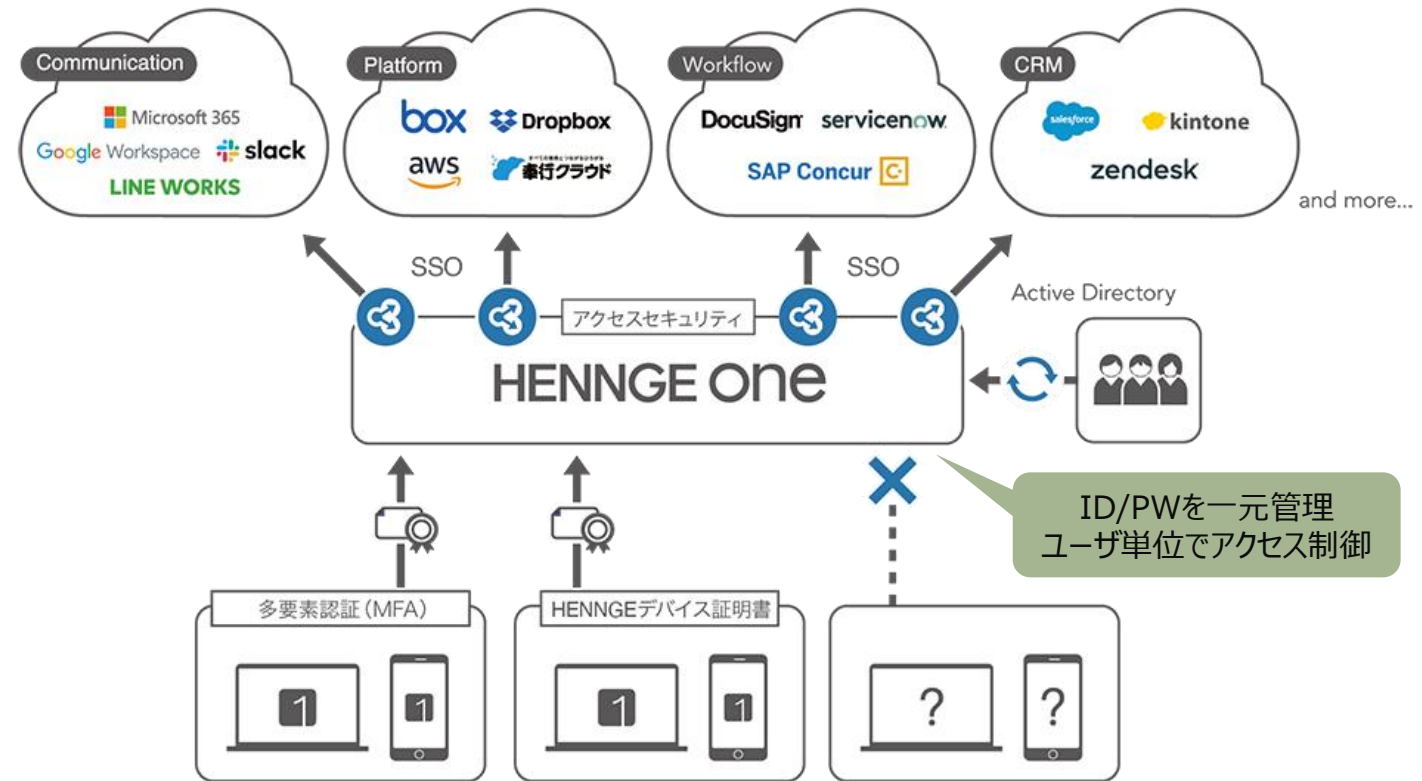


# HENNGE One概要

## HENNGE Oneとは

- HENNGE One はMicrosoft 365、Google Workspace、Box、LINE WORKSなど複数のクラウドサービスへのセキュアなアクセスとシングルサインオンを実現するSaaS認証基盤 (IDaaS)
- IP制限、デバイス証明書、セキュアブラウザ、パスワードレス認証、多要素認証 (MFA) など豊富な認証機能で利便性と安全性のバランスのとれたセキュリティサービスを提供
- メール誤送信対策、メールバックアップ、等のメッセージングセキュリティ機能もご提供

連携先サービス：170以上  
導入実績：1,800社以上



<https://hennge.com/jp/service/one/>

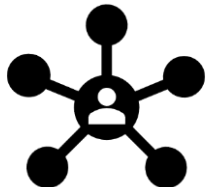
# DynabookがHENNGE Oneをご提案する理由

## HENNGE Oneのお勧めポイント



### 1. 短期間で導入可能

Azure ADと比較して設定が容易であり、短期間（1.5ヶ月～2ヶ月）で導入可能。  
その分、初期構築にかかるコストも安価。



### 2. 運用時の負担が少ない

HENNGE Oneの管理画面については、M365に関する知識がなくても操作可能。  
また、アクセスポリシーの変更、アカウント追加、等のHENNGE Oneに関わる設定作業であれば、HENNGEに設定作業を代行してもらうことが可能。トラブル発生時のサポート体制も充実。



### 3. 低コスト

AzureAD Premium (M365 E3/E5) と比較して安価に導入可能。  
SSOだけでなく、メールセキュリティも含めて1パッケージで導入できるため、複数製品を導入する場合と比較してコストパフォーマンスが高い。



# DynabookがHENNGE Oneをご提案する理由

## アクセスセキュリティ機能 (IdP Edition)

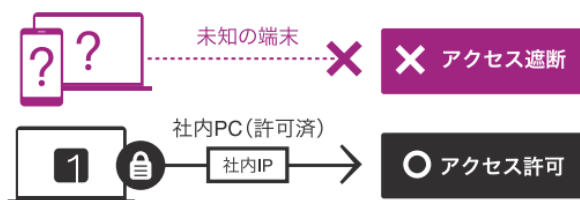
各種クラウドサービスに対して、IP制御や二要素認証機能などのアクセス制限機能を付加することで、不正アクセスによる情報漏洩のリスクからクラウドサービスを守ります。

シングルサインオンの接続実績▶170以上



### シングルサインオン アクセス制御

#### HENNGE Access Control



∞ SaaS (SAML) 接続数は無制限

ID/Passwordの一元化

ユーザー単位でのアクセス制御

アクセスログの取得

Active Directory連携

### デバイス制御

#### HENNGE Device Certificate



証明書での厳密なデバイス制御

未許可デバイスへのインストール制限

パスワードレス認証の実現

### BYOD対策

#### HENNGE Secure Browser



セキュアな環境でのメール閲覧

添付ファイルのダウンロード制御

アクセス可能なURLの制限

# DynabookがHENNGE Oneをご提案する理由

## メッセージングセキュリティ機能 (E-Mail Security Edition)

各種クラウド型のメールサービスと連携し、メール誤送信対策、情報漏えい対策、メール監査、暗号化などの高度なメールセキュリティをクラウド上で実現します。

接続対象クラウド



### メールの誤送信対策

#### HENNGE Email DLP



- 送信メールの一時・永久保留
- 添付ファイルへの自動パスワード設定
- 送信メールのフィルタリング
  - 上長承認
  - 宛先ドメイン数チェック
  - 個人情報チェック
  - BCC自動転送
  - 送信取り消し 等々

### メールのアーカイブ

#### HENNGE Email Archive



- 永年保管・容量無制限  
※年数を制限しての保管も可能
- 添付ファイル内のテキスト検索
- 検索権限の設定
- 退職者のメール保持
- アクセス・操作ログの検索

### URLでのファイルの受け渡し

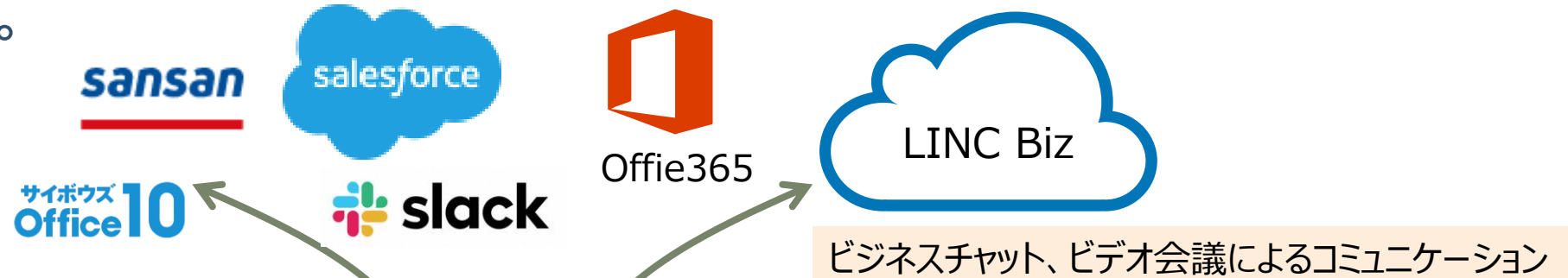
#### HENNGE Secure Transfer



- 最大2GBまでアップロード可能
- アップロード/ダウンロード通知
- ファイル受け取り人の確認
- URLの公開停止
- 受け渡しログの検索

# IDaaSを利用したDynabookによる提案事例

SaaS認証基盤「HENNGE One」と、コミュニケーションツール「LINC Biz」を組み合わせることにより、セキュアで効率的なセキュアなモバイルワーク環境をスピーディかつ安価に構築します。



## ✦ HENNGE

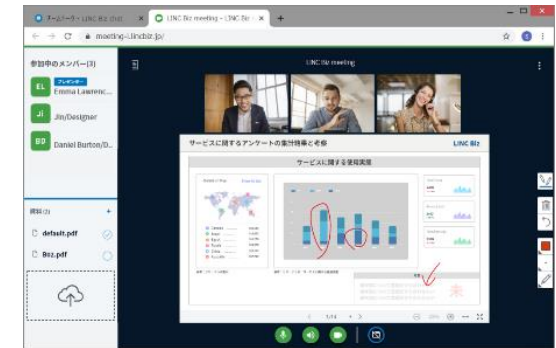
多要素認証やデバイス証明書等を用いた不正アクセス対策

シングルサインオンの実現

ユーザあたり月額料金設定

社内・社外の各種サービスへ

**HENNGE One**



# 主なIDaaSの機能比較

## HENNGE One と Azure AD

		Office 365	M365 E3
	HENNGE One	Azure AD	Azure AD Premium P1
AD同期	○	○	○
シングルサインオン	○	○	○
多要素認証	○	○	○
デバイス証明書	○		○
条件付きアクセス制御 *1	○		○
プロビジョニング *2			○
アプリケーションプロキシ *3 (オンプレ用)			○

主要な機能に特化  
シンプルにパッケージング

多機能かつ詳細な設定項目を用意  
設定にはM365に関する知識が必要

### 補足説明

#### \*1 : 条件付きアクセス制御

条件に応じて追加の認証を要求したり、アクセスをブロックしたりする機能  
例) 社外からのアクセスの場合は多要素認証を必須とする

#### \*2 : プロビジョニング

ディレクトリ情報と連携して、自動的に連携先のクラウドアプリケーション (SaaS) のアカウントの生成/更新/削除を行う機能

#### \*3 : アプリケーションプロキシ

オンプレ上のアプリケーションに対してもクラウド上のアプリケーションと同様にアクセスできるように中継する機能

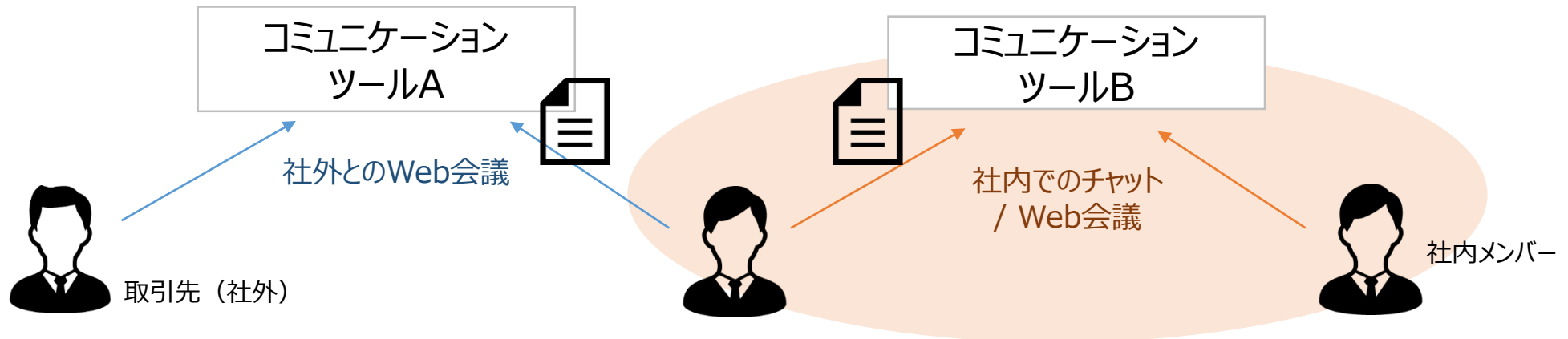
# コミュニケーションツール

コミュニケーションツールは利便性が高い一方で、以下のような問題を抱えています。

- 既存のグループ（チーム）に社外のゲストユーザが含まれているかを一覧画面で把握するのは難しいことから、本来は想定していない相手に対して、社外秘のファイルを共有してしまう危険性がある。



複数のコミュニケーションツールを併用し、用途に応じて使い分けすることでデータ漏洩の防止効果が見込めます。



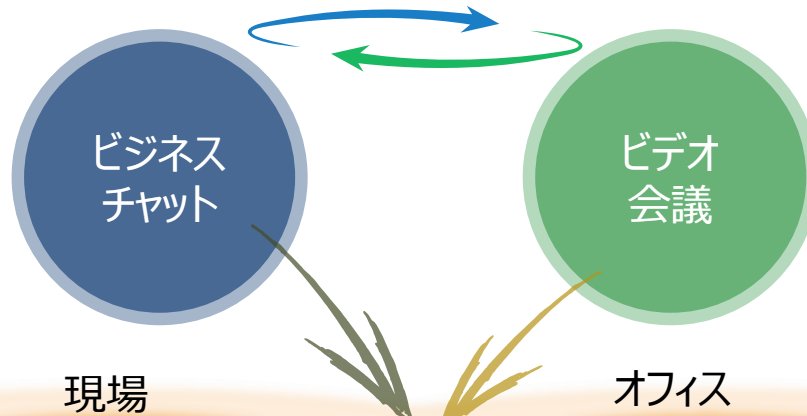


# コミュニケーションツールを1ストップで提供

LINC Bizでは、ビジネスコミュニケーションを改革するために必要な、チャット機能とミーティング機能(ビデオ会議)をオールインワンで提供。

## フラットな議論

ビジネスチャットによる  
部門横断の活発な議論



## スピーディな意思決定

チャットからワンアクションで  
切替可能なビデオ会議の活用

## 業務効率化

現場からの情報は  
業務報告ボットで入力、自動集計  
FAQチャットボットによる  
業務問合せの効率化

# DynabookがLINC Bizをお勧めする理由

シャープ\*向けに開発。自社導入でも様々な効果を実感

- 部門横断コミュニケーションの活性化
- 資料共有の効率化
- ビデオ会議活用の促進
- メールの削減



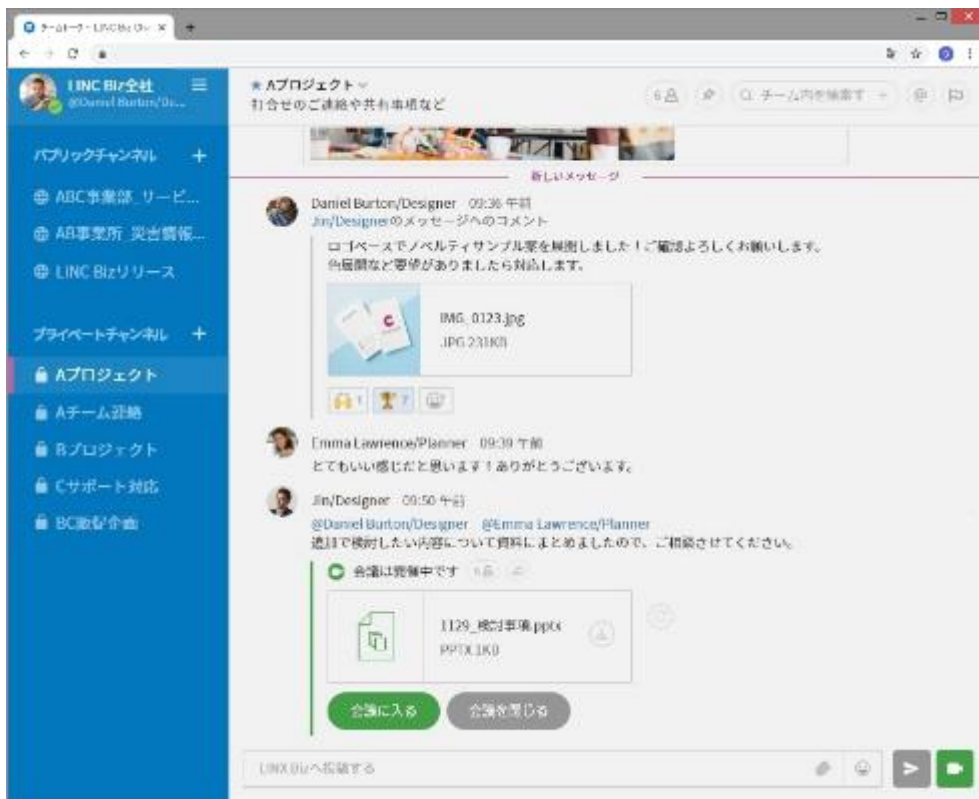
低コスト  
で実現

\*総ユーザー数：26,000以上（派遣社員、海外拠点含む）  
約8割のユーザーがアクティブに利用中

# LINC Biz chat機能紹介

## LINC Bizchat

いつでもサクッとチャット開始ファイル共有も手軽で安全に



- **チャンネルによる複数人のチャット**
  - パブリック/プライベートチャンネル
- **ダイレクトメッセージによる特定メンバーとのチャット**
  - 同時最大8名まで
- **メッセージ送信**
  - テキスト、添付ファイル、絵文字
- **メッセージ検索**
  - 条件指定（投稿者、チャンネル、日付など）
- **新着メッセージの通知**
  - チャンネルや宛先ごとに通知/非通知設定可
- **モバイルアプリ**
  - iOS/Android

# LINC Biz meeting機能紹介



## LINC Biz meeting

チャットとビデオ会議がシームレスだから議論が途切れない



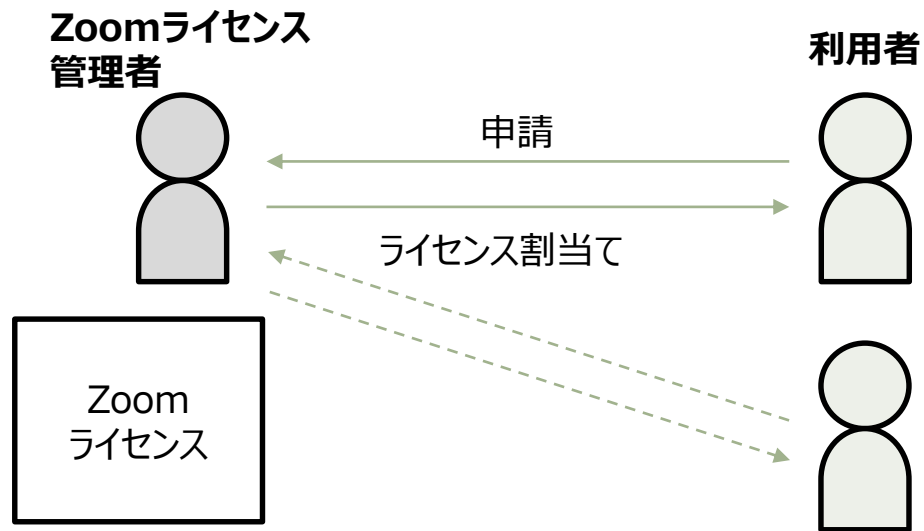
- **音声・ビデオによるリモート会議**
  - 大人数会議(100~1000人)に対応
  - 研修等のグループワークに使える  
ブレイクアウトセッション対応
  - ウェビナー(Webセミナー)に対応
- **資料の共有**
  - 動画共有(YouTube)
  - PDFファイル、PCアプリ/デスクトップ画面
  - 複数人同時書き込み、チャットに自動投稿
- **一時的なゲスト招待**
  - 参加用URLにWEBブラウザで簡単アクセス
- **セキュリティ**
  - 会議資料のダウンロード制限
  - 参加者の強制退出、ミュート制御
  - 録画・録音

# お勧めポイント「Zoom連携」

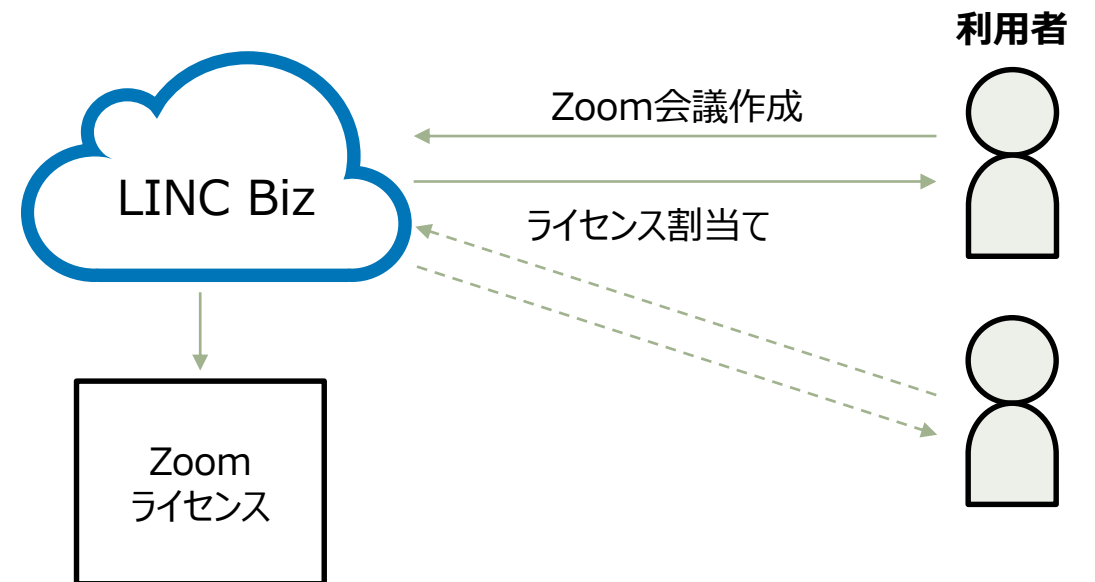
## Zoomライセンス管理機能

- Zoomの有料ライセンスは組織内の任意の利用者に割り当て可能
- Zoomライセンスの管理をLINC Bizに任せることで、管理者の負担軽減を実現

ライセンス管理者が、利用者に空きライセンスを都度割り当てる必要がある



LINC Bizが空きライセンスを自動的に割り当てるため、管理者の負担なし





# お勧めポイント「Zoom連携」

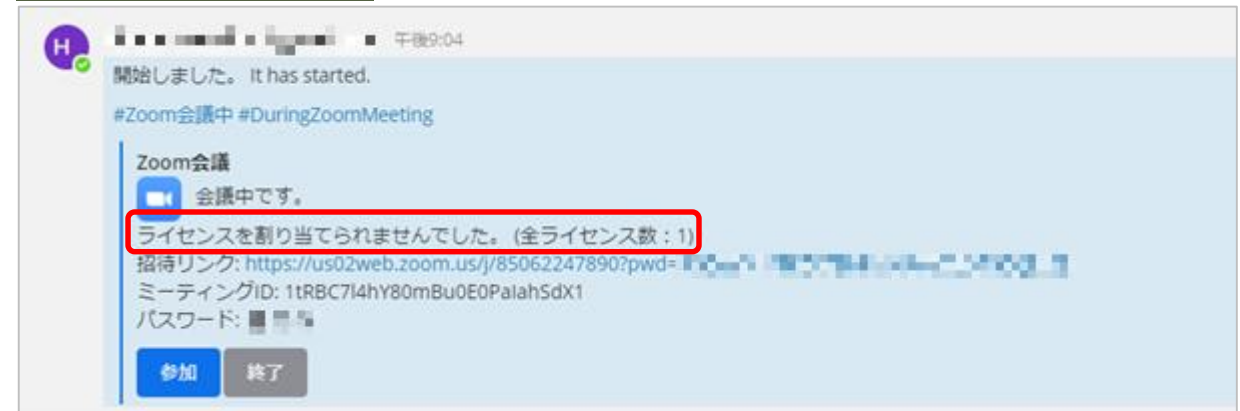
## Zoom会議開始

- チャット上でZoom会議の開始/予約可能
- Zoom会議開始時、空いているライセンスを自動割り当て
- 空きライセンスがない場合、「ライセンスを割り当てられませんでした」と表示し、ライセンス割り当てなしで会議作成する

### 空きライセンスあり



### 空きライセンスなし





Active Directory、Azure、Microsoft、Microsoft 365、Office 365、Officeロゴは、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。

Android、Chromebook、Gmailアイコン、Google、Google Workspaceは、Google LLCの登録商標または商標です。

HENNGEは、株式会社HENNGEの登録商標です。

その他の記載されている社名・商品名・サービス名などは、それぞれ各社が商標として使用している場合があります。