Boxのテナント制限と ファイルリクエストのアクセス制限 構成ガイド

2019年6月

A10ネットワークス株式会社

第1.0版

Reliable Security Always™

改訂履歴

版	日付	担当者	改訂内容
1.0	2019/6/25	石塚 健太郎	初版（Box用のクラウドプロキシと情報漏洩対策）

本ガイドの対象読者と概要

- A10 Thunderを用いてBox用のプロキシを構成したい方向けの構成ガイド
- Thunderを利用してフォワードプロキシの設定とSSLインサイトを用いたBoxのテナント制限とファイルリクエストへのアクセス制限の実現方法について紹介
- 利用したACOSバージョン：4.1.4-GR1-P1

目次

- Box連携ソリューション概要
- クラウドプロキシの設定例

Box連携ソリューション概要

Boxとの連携ソリューションの概要

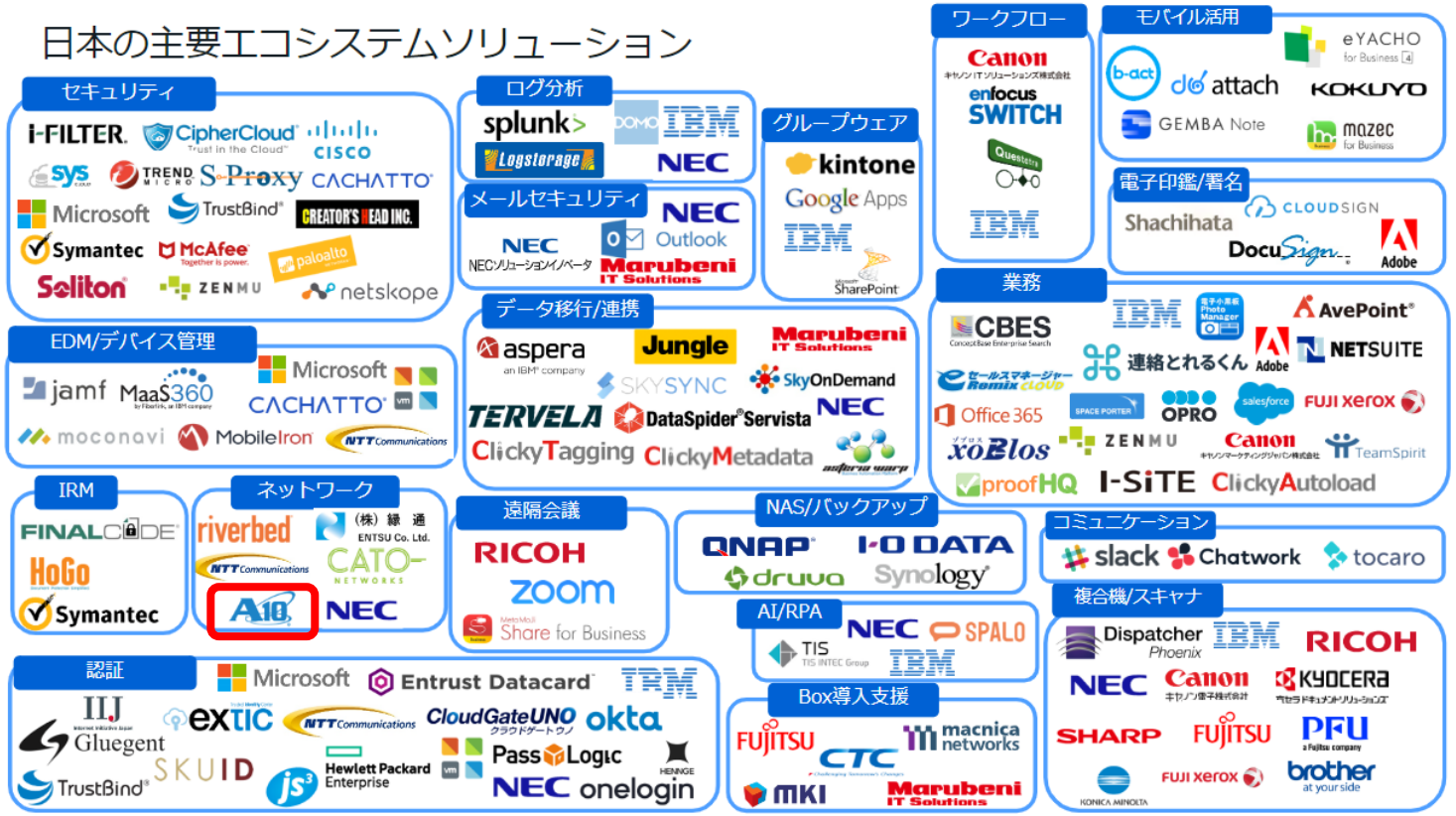
- **Box利用により生じるインターネット向けトラフィックのハンドリング**
  - プロキシサーバーの負荷軽減
  - Box向けトラフィックを特定の回線へ振り分けることによる回線の負荷軽減
- **コンテンツ共有を妨げない形での利用アカウント制御**
  - 企業内で許可されたアカウントのみへのログインを許可
  - URLフィルタを利用せず、他のBoxユーザーとのコンテンツ共有を阻害しない
- **ファイルリクエストへのアクセス制限**
  - 他社アカウントへの情報漏洩の阻止

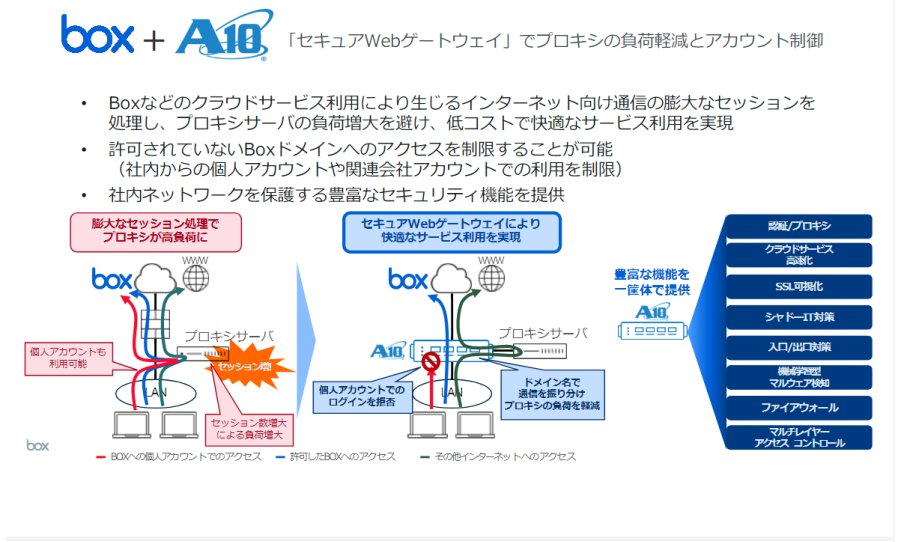
box

Boxエコシステムに参加

通信トラフィックの制御と利用アカウントを制限するソリューションを提供

https://cloud.app.box.com/v/japanecosystem



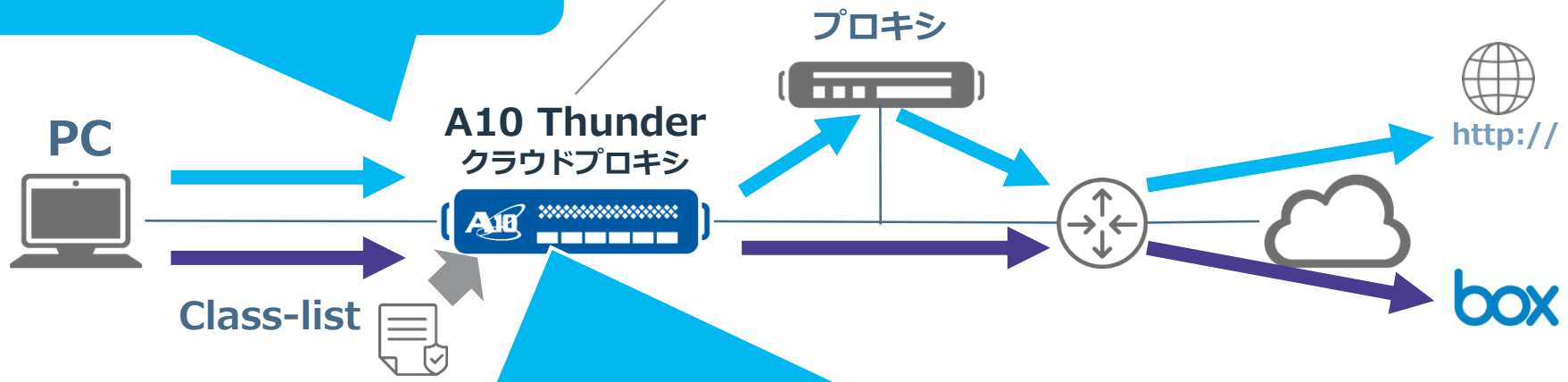


クラウドプロキシソリューションによるオフロード

PCのプロキシ接続先をA10 Thunderに変更するだけで、宛先ドメイン名に応じて通信を振り分け、プロキシをオフロード

プロキシ接続時、
宛先ドメイン名で振り分け（宛先IPも可）

エントリー機器でもハイエンドプロキシの20倍以上のセッションを処理できるため、ボトルネックにならない



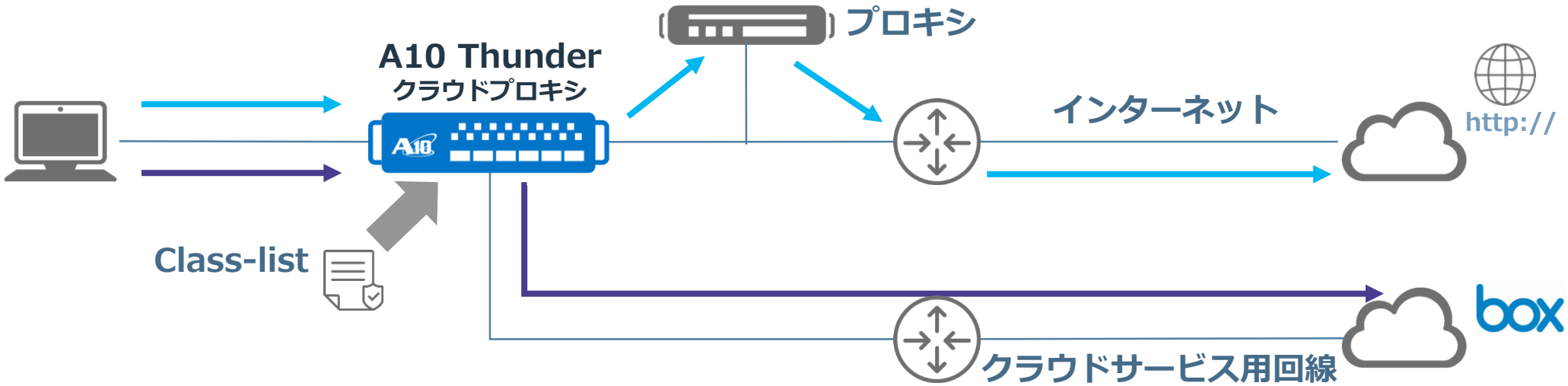
- Class-listとURL・ホストヘッダー・IPアドレスをマッチング
  - サービスのドメイン以外　→ プロキシサーバへ振り分け
  - サービスのドメイン　→ インターネット回線へ振り分け

Box以外にも
多くのクラウドサービスに
柔軟な振り分け設定が可能

Boxトラフィックを別回線に振り分け

同じ仕組み（ドメイン名）で回線を振り分けることが可能（3回線以上も可）
別回線にBoxトラフィックを流すことで主回線への影響を軽減

- クラウドサービス → クラウドサービス専用回線へ振り分け
- クラウドサービス以外 → プロキシサーバ経由で既存の回線で通信



Boxのアカウント利用制御

✓ 企業内からの個人アカウントや関連会社アカウントでのログインをブロック
✓ 他のBoxユーザーとのコンテンツ共有を妨げないアカウント制御を実現

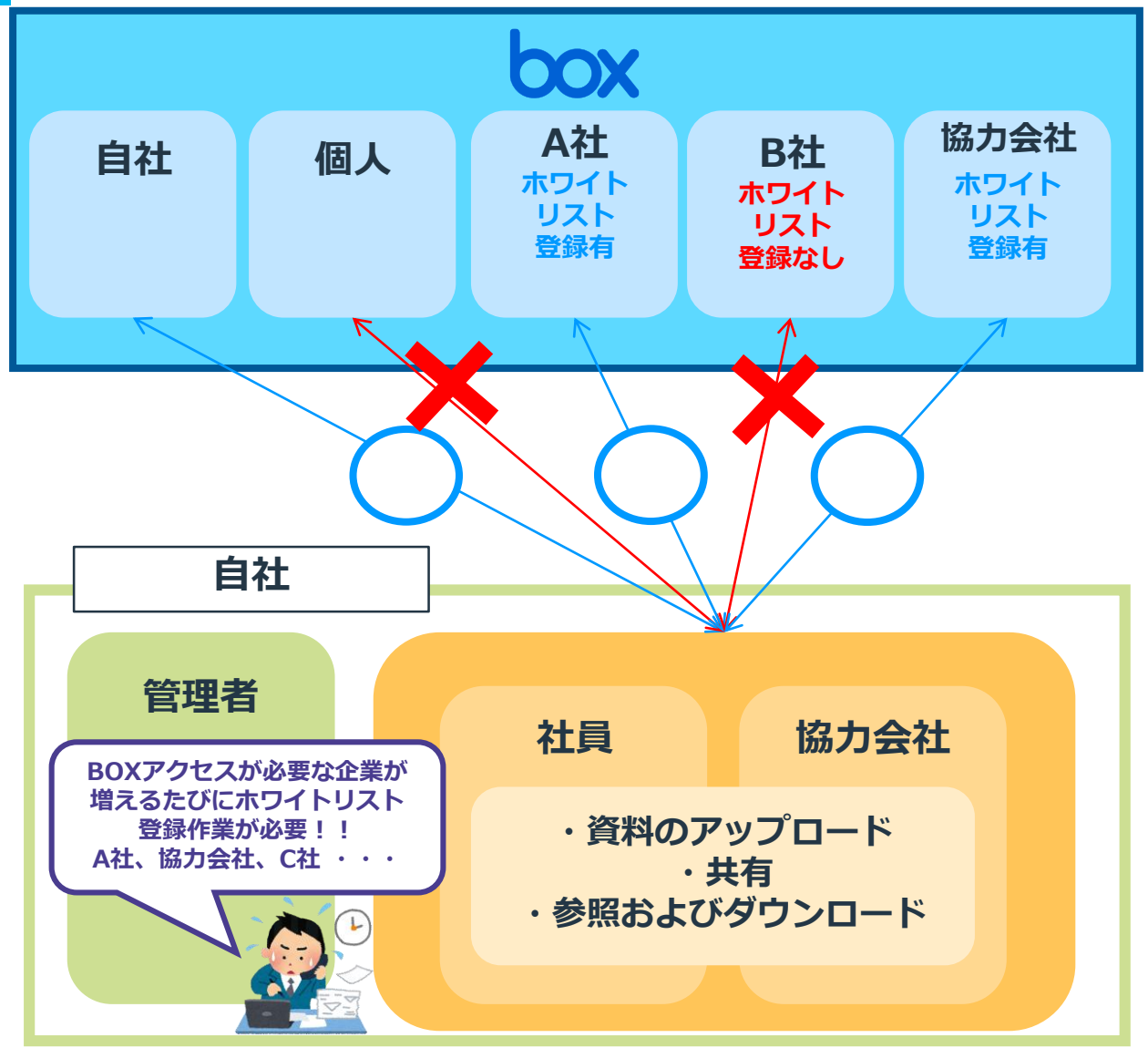
Verified Enterpriseを利用すると
xxx.{ent|app}.box.comをフィルタ対象として設定する必要がある。
そのためBoxの本来の利点であるコンテンツ共有の利点が損なわれる

A10のクラウドプロキシを利用したソリューションでは、
コンテンツ共有の利点を残したまま、
特定ドメインへのログインのみを許可することが可能

Verified EnterpriseでのURLフィルタ設定

- Boxのドメインとして、xxx.{app|ent}.box.comが各企業に払い出されている（例えばa10-demo.app.box.com）が、
社内からこのドメインへのアクセスのみをURLフィルタで許可する形では不十分
- Boxの大きな利点の一つである他者との安全なファイル共有を実施する際に、
他社のドメインや個人アカウントで利用される **app.box.com** が使われるため

Verified Enterpriseによるアクセス制御



管理者
Boxへのアクセスが必要な企業に対して
その都度ホワイトリスト登録が必要
（URLフィルタ設定が必要）

自社ユーザ（協力会社含む）
ホワイトリスト登録された企業のみに対して
Boxサービスの利用が可能

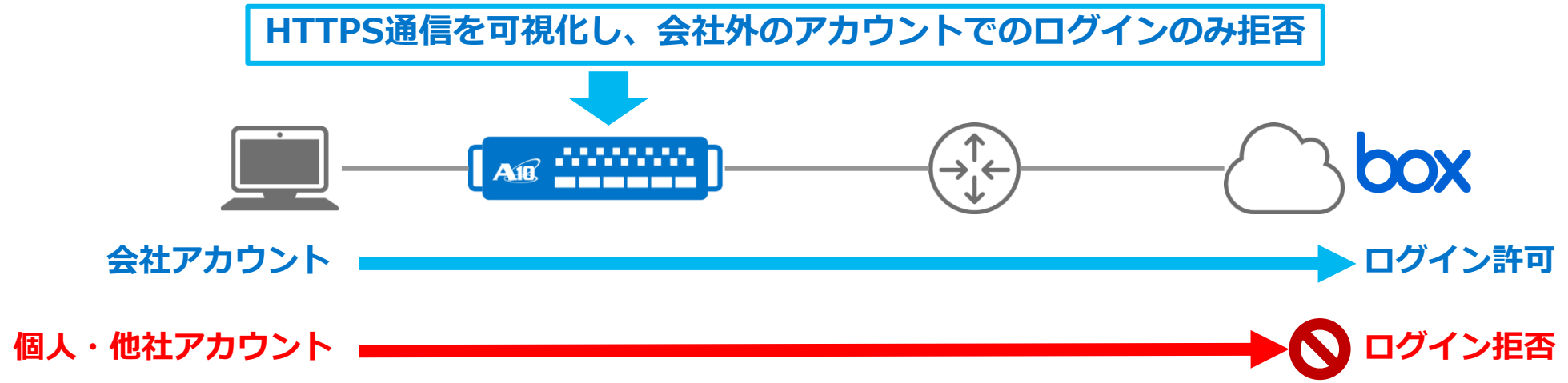
取引先企業
ホワイトリスト登録されていれば
Box利用可能
（ログインとアップロードも可能）
登録されていない企業は利用不可能

A10を用いたBoxの利用アカウント制御

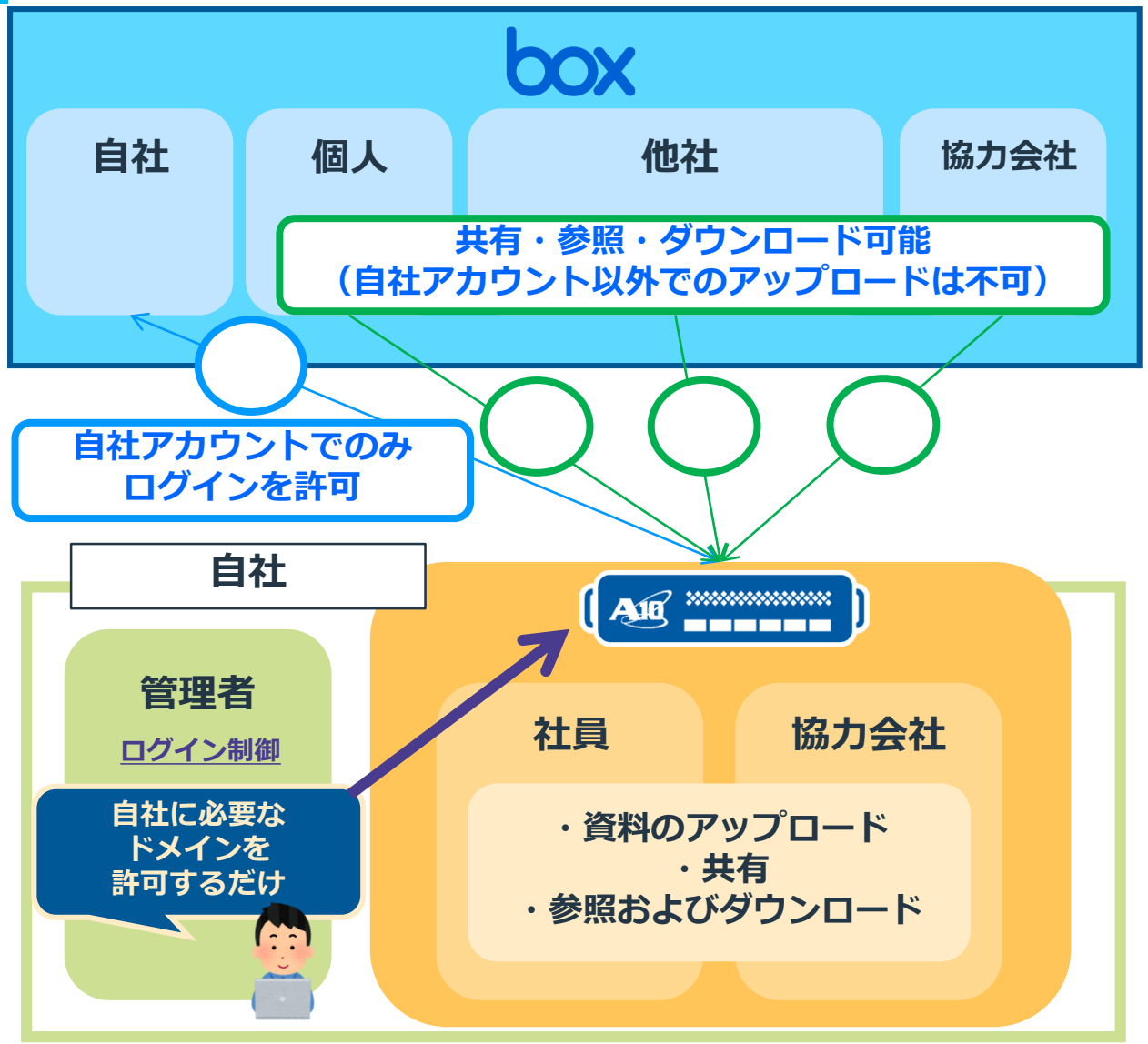
社内からのログインは法人アカウントのみ許可し、
個人や他社アカウントはログインさせたくない

A10のソリューション

①A10をプロキシとして利用、SSL通信可視化（SSLインサイト）機能でHTTPS通信を復号
②会社ドメインへのログインかどうかを検査し、個人アカウント利用であればログインをブロック
利点：コンテンツ共有の利点を残したまま、個人や他社アカウント利用を制限



クラウドプロキシによるアクセス制御



管理者
自社からのログインが必要な
ドメインを許可するだけ
（URLフィルタ設定が不要）

自社ユーザ（協力会社含む）
全ドメインからのコンテンツ共有を利用可能
個人アカウントや他社アカウントでの
ログインを制御し、
資料のアップロードを防ぐことが可能

取引先企業
コンテンツ共有を利用可能
ログインが許可されていなければ
アップロードは不可