

クラウドストレージユーザ必見！ クラウド時代における情報漏洩ゼロへの道

丸紅ITソリューションズ株式会社
セキュリティソリューション事業部

秩父彩香

本セッションについて

こんな企業様にぜひ聞いていただきたい！

- クラウドストレージの**利用を検討中**の企業様
- クラウドストレージを**既に利用中で**
情報漏洩対策が出来ているか不安な企業様
- クラウドストレージを**既に利用中で**
セキュリティオプションなども付けて**情報漏洩対策に自信アリ**な企業様

本セッションについて

こんな企業様にぜひ聞いていただきたい！

- クラウドストレージの**利用を検討中**の企業様
- クラウドストレージを**既に利用中で情報漏洩対策が出来ているか不安**な企業様
- クラウドストレージを**既に利用中でセキュリティオプションなども付けて情報漏洩対策に自信アリ**な企業様

当社でも実際にBoxを使っており、情報漏洩対策は出来ているつもり！でした・・・

Boxはセキュアなクラウドストレージ

Boxでできる情報漏洩対策



恒常的なやり取りは **招待** で共同作業



一時的なやり取りには **共有リンク** 発行

極秘

社内限

公開

Shieldオプション追加で **機密情報にラベル** 付与

Boxはセキュアなクラウドストレージ

Boxでできる情報漏洩対策



恒常的なやり取りは **招待** で共同作業



一時的なやり取りには **共有リンク** 発行

極秘

社内限

公開

Shieldオプション追加で **機密情報にラベル** 付与

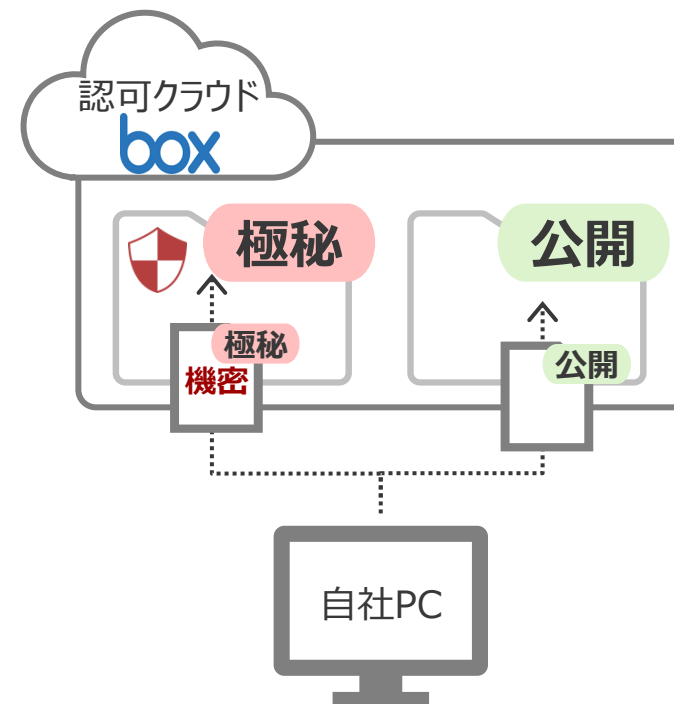
Boxのセキュリティを強化する
オプションライセンス

Boxはセキュアなクラウドストレージ

Boxでできる情報漏洩対策

- 必要最小限権限を付与した **ユーザ招待**
- 適切な公開範囲に限定された **共有リンク**
- 利用ルールに沿った正しい **フォルダ運用**

Box上に保管された機密情報を保護！

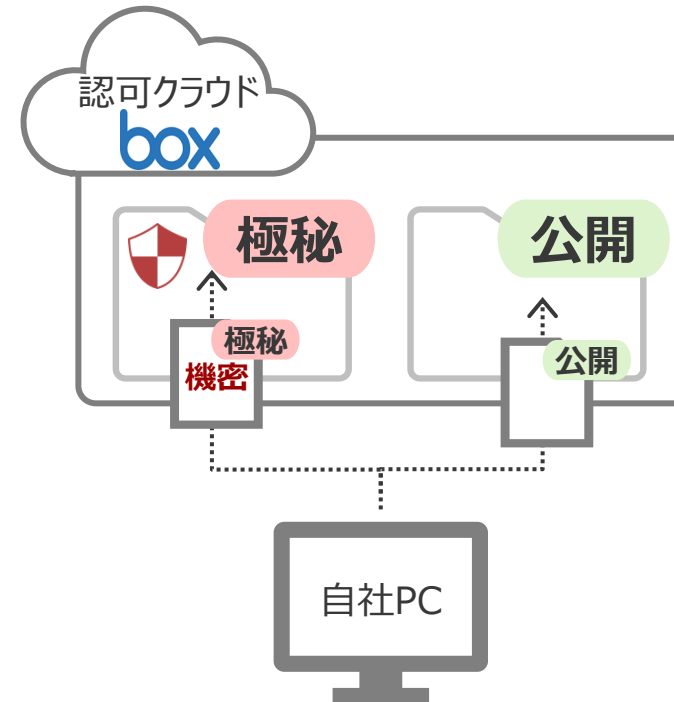


Boxはセキュアなクラウドストレージ？

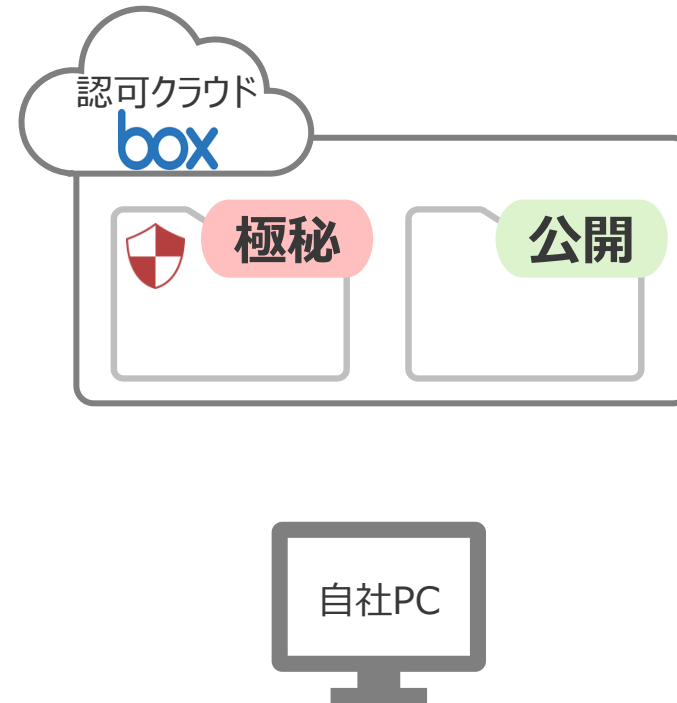
Boxでできる情報漏洩対策

- 必要最小限権限を付与した **ユーザ招待**
- 適切な公開範囲に限定された **共有リンク**
- 利用ルールに沿った正しい **フォルダ運用**

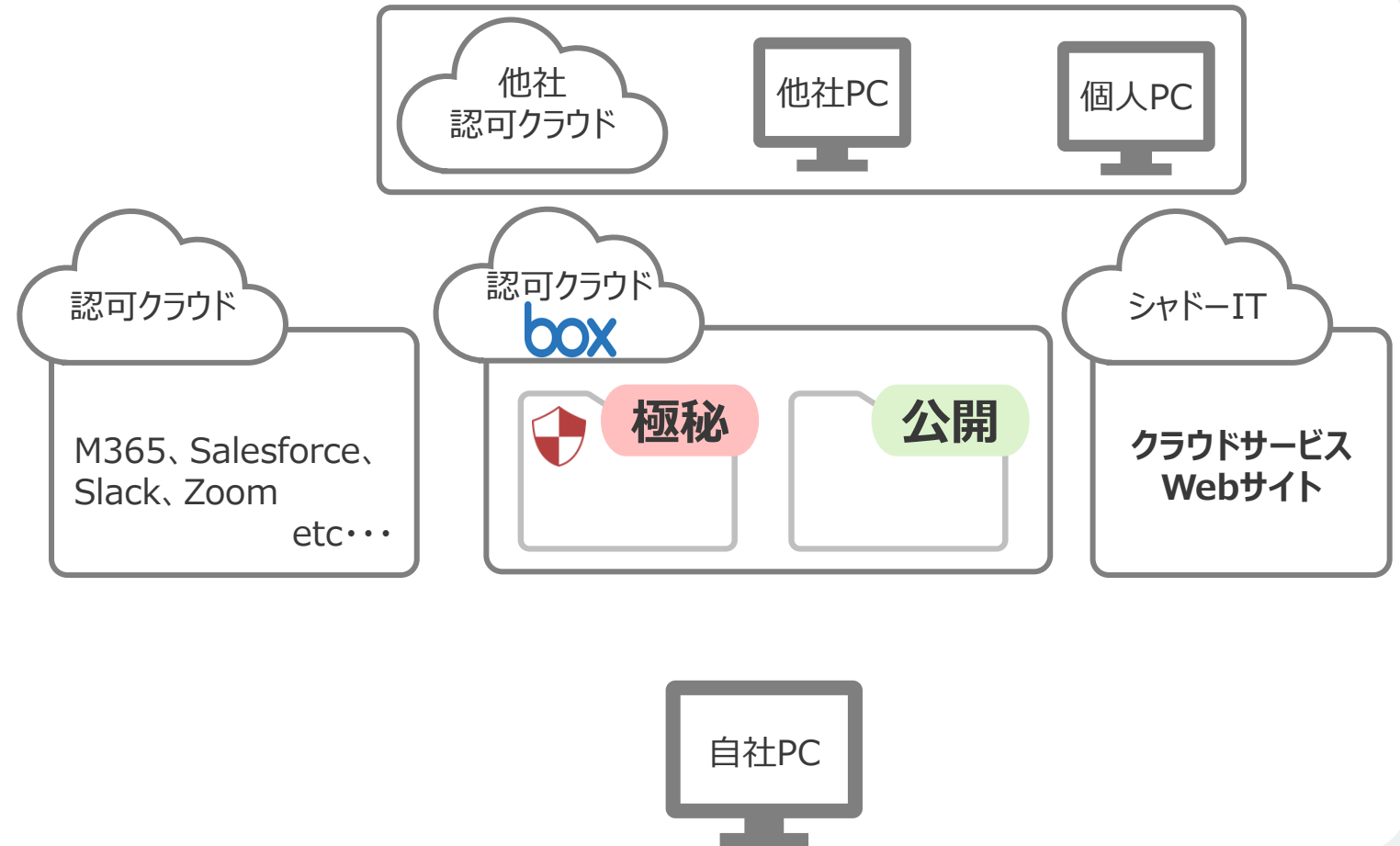
ほんとうに抜け穴ってないの・・・？



Boxを取り巻く周辺環境

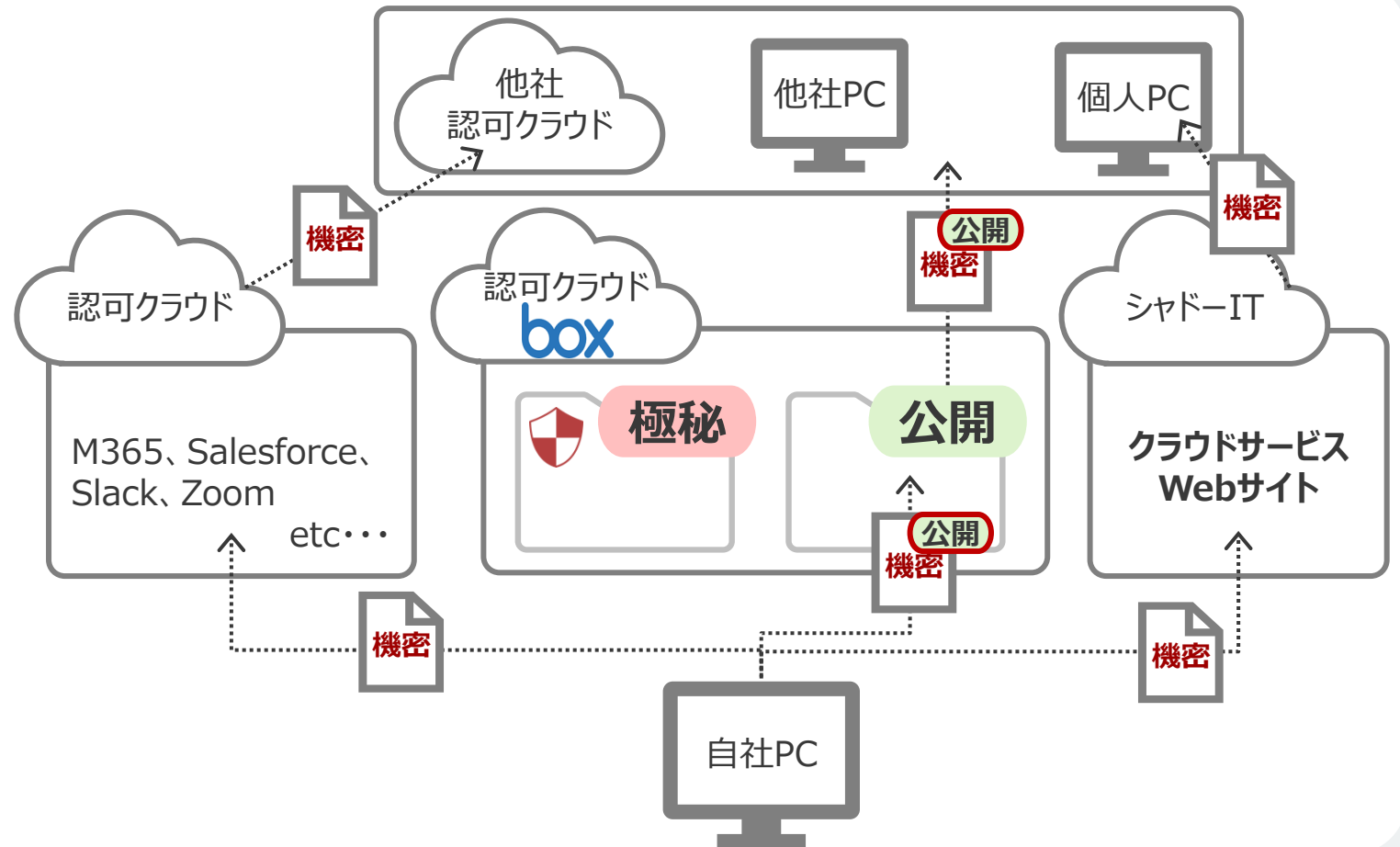


Boxを取り巻く周辺環境

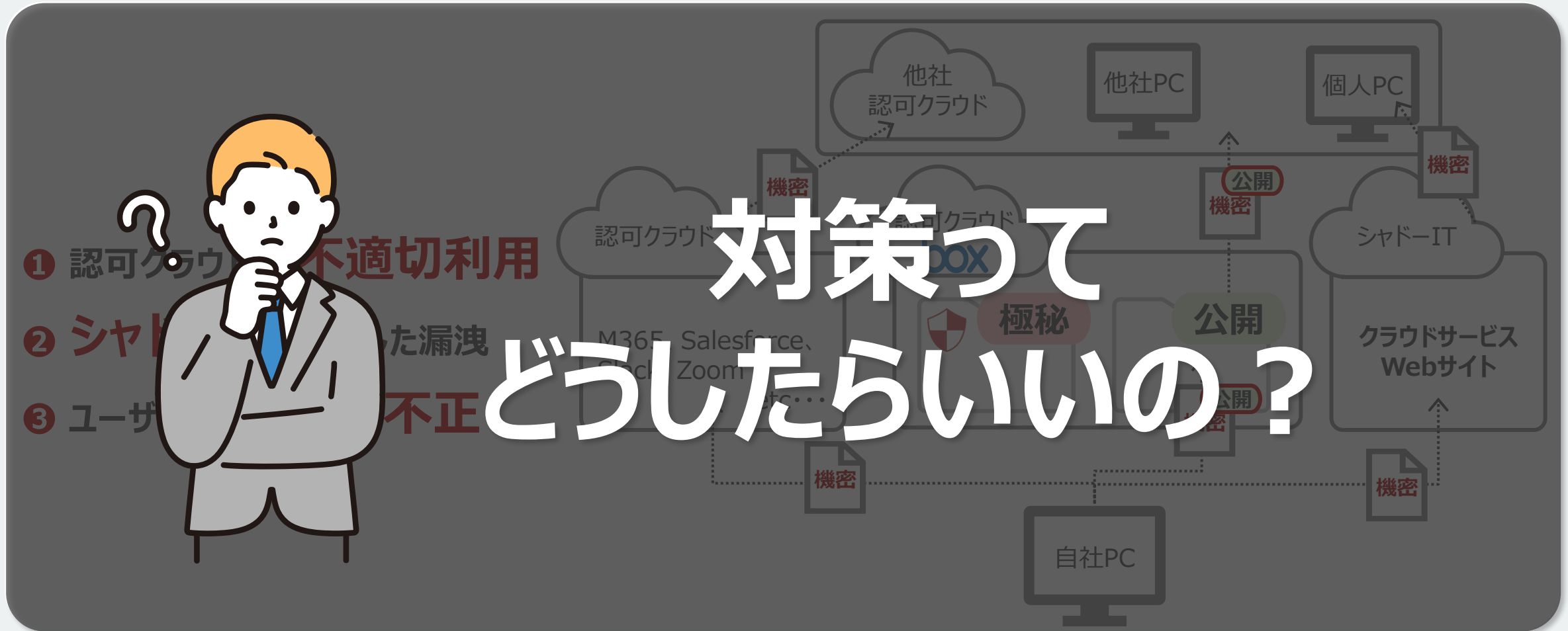


Boxだけでは防ぎきれない情報漏洩

- ① 認可クラウドの **不適切利用**
- ② **シャドーIT** を介した漏洩
- ③ ユーザの **オペミス・不正**



Boxだけでは防ぎきれない情報漏洩



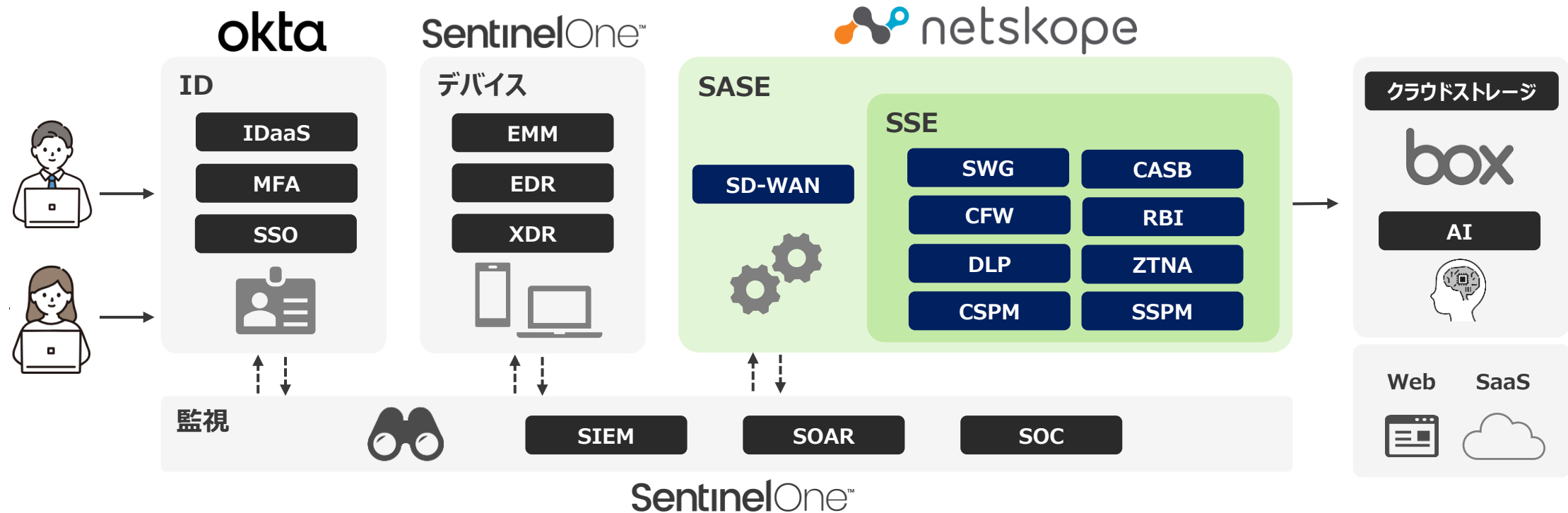
Boxを安全に利用するために

ユーザのあらゆる操作を
リアルタイムに可視化・制御



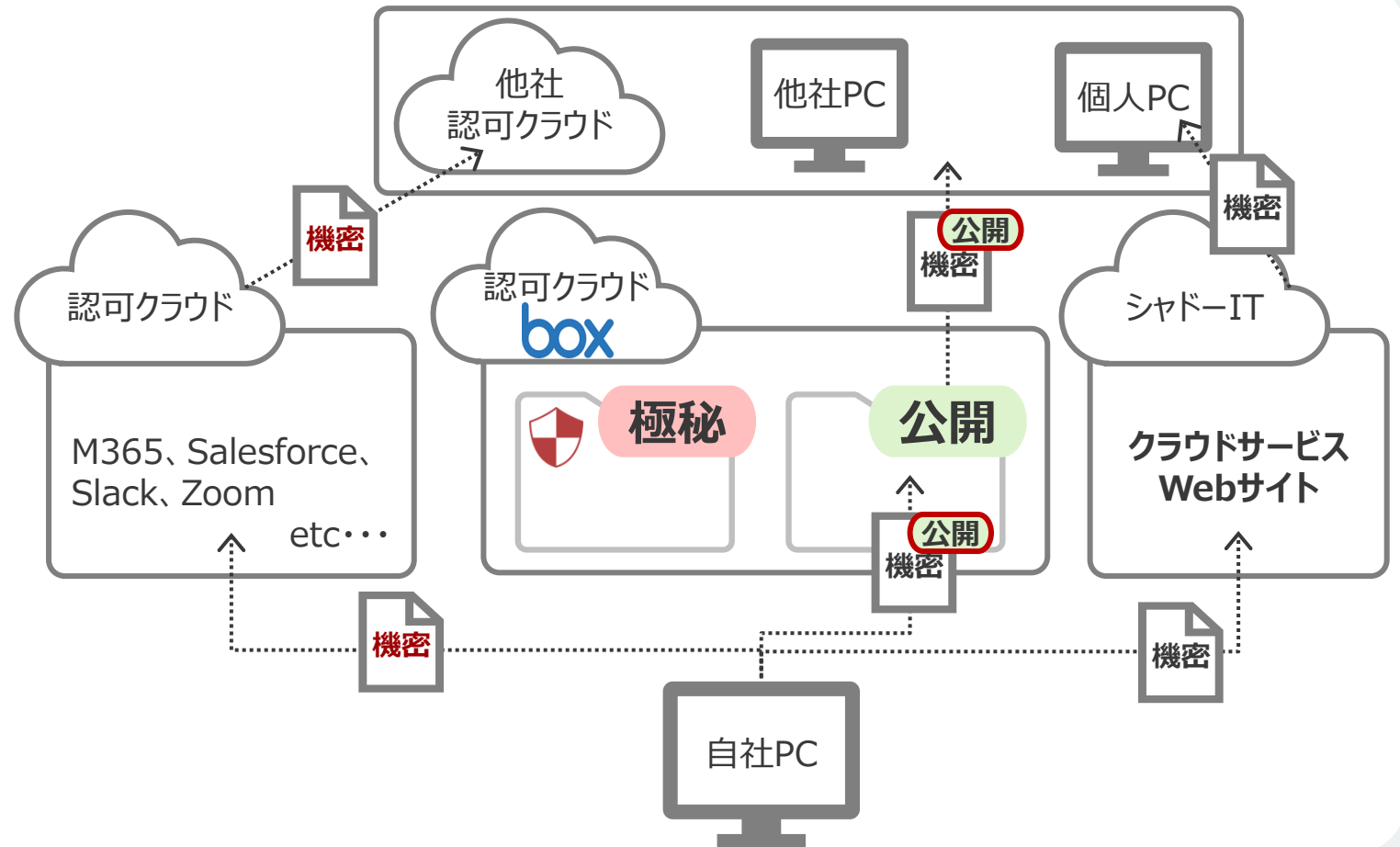
Boxを安全に利用するために

ゼロトラストセキュリティにおけるSASEを一手に担うNetskope



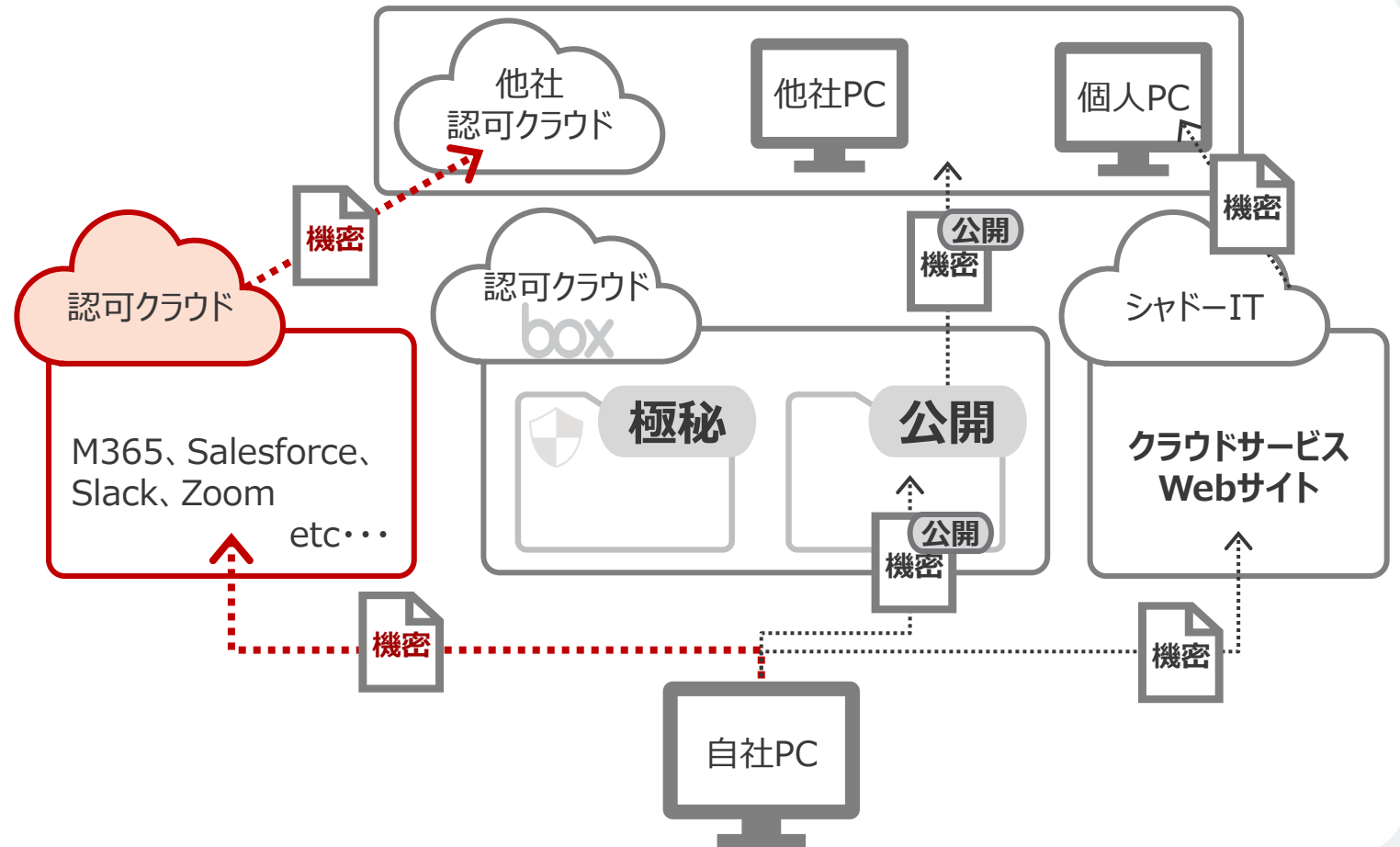
Netskopeでできる情報漏洩対策

- ① 認可クラウドの **不適切利用**
- ② **シャドーIT** を介した漏洩
- ③ ユーザの **オペミス・不正**



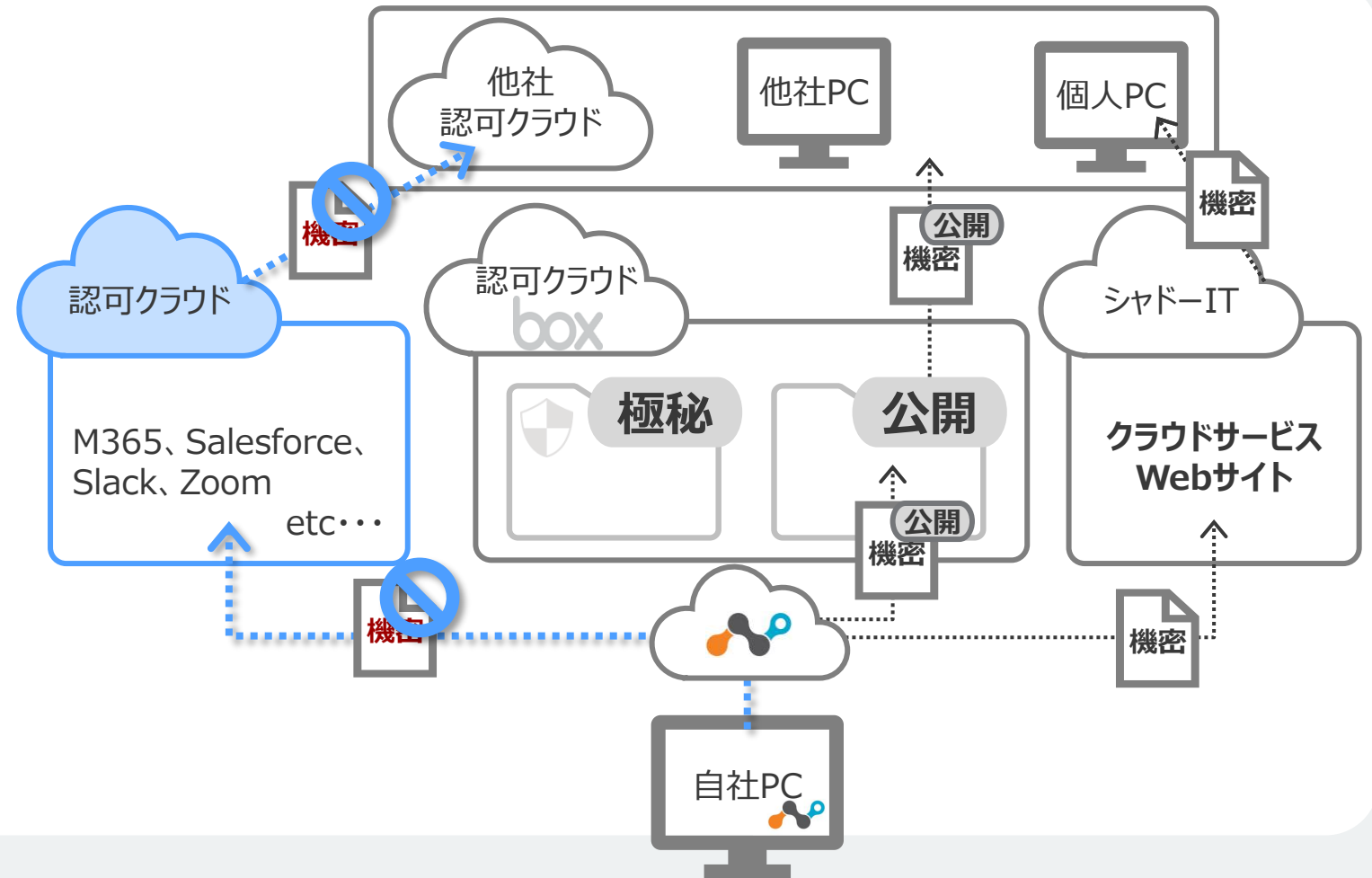
Netskopeでできる情報漏洩対策

① 認可クラウドの不適切利用

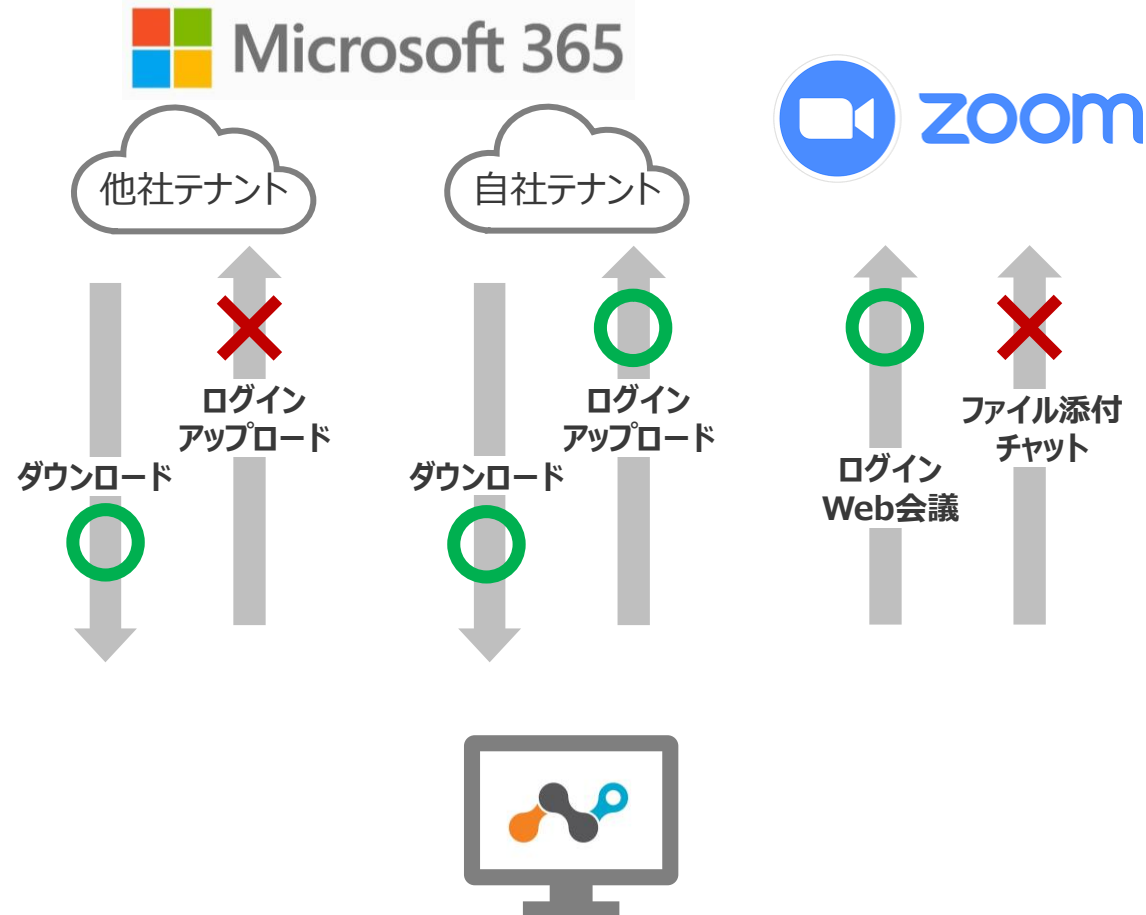


Netskopeでできる情報漏洩対策

- ① 認可クラウド であっても
ユーザがおこなった**操作の
内容ごとに細かく制御**



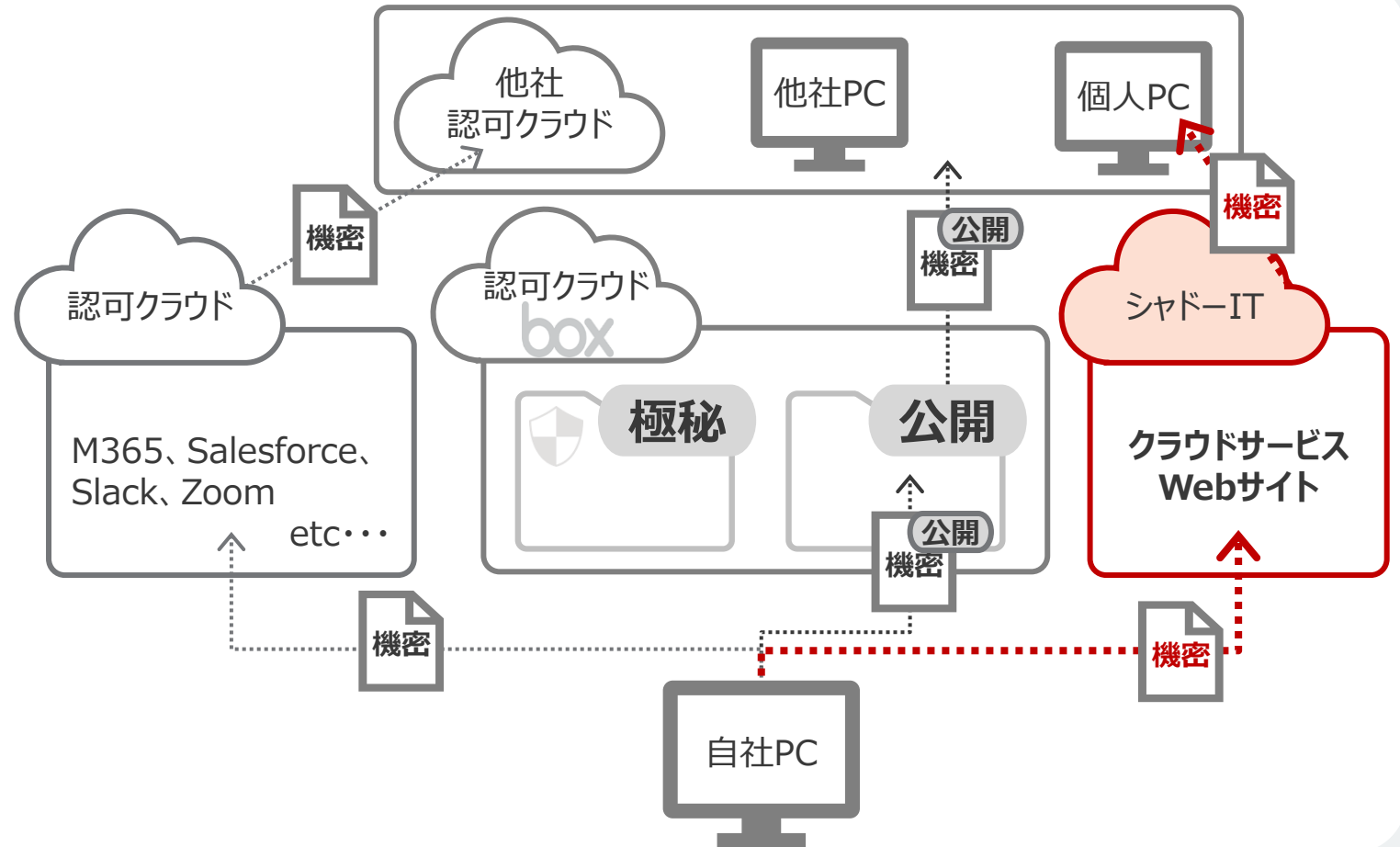
① 認可クラウドの不適切な利用をブロック



情報漏洩に繋がる操作は
たとえ認可クラウド内であっても、
ブロックが必要です。

Netskopeでできる情報漏洩対策

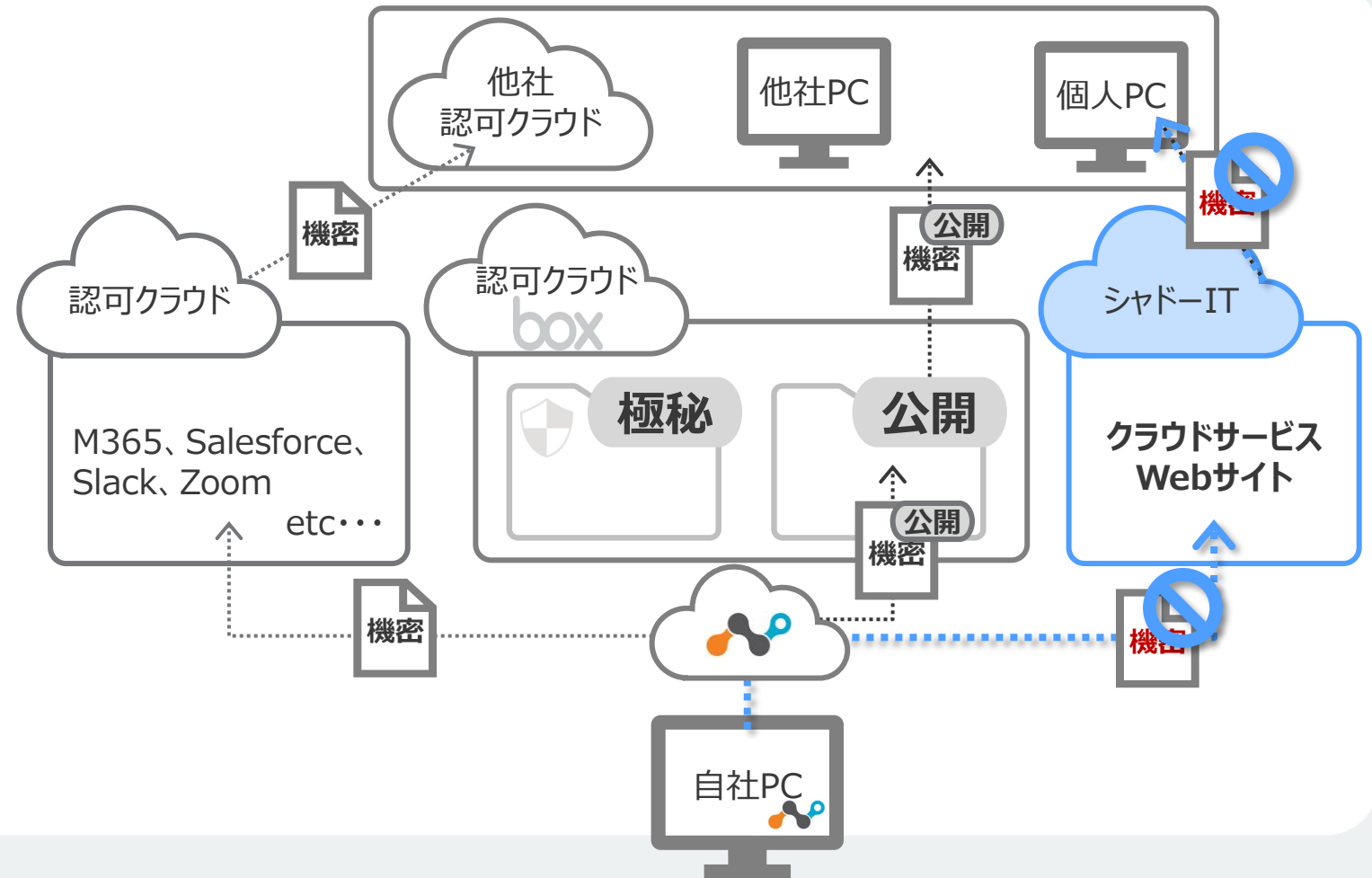
② シャドーIT を介した漏洩



Netskopeでできる情報漏洩対策

② シャドーIT へのアクセスは
もちろんブロック！
だけじゃなく、

利便性 も損なわない
柔軟な制御 を実現！



② 認可外のサービスでも柔軟な制御



サイトへのアクセス



危険なサイトは完全ブロック！

② 認可外のサービスでも柔軟な制御



サイトへのアクセス



ログイン
アップロード



閲覧
コメント書き込み
投稿



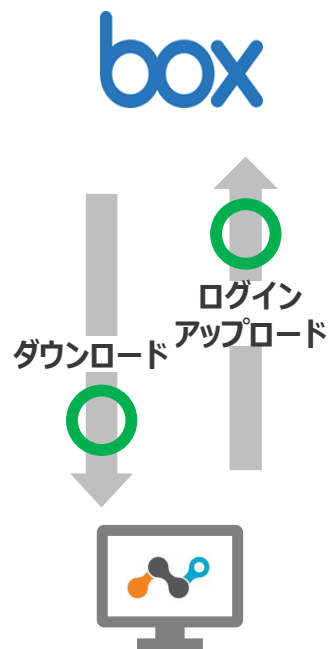
使い方次第で業務に有益なサイトは、
制限付きで利用させる方針とし、
利便性を損なわずに**生産性向上！**



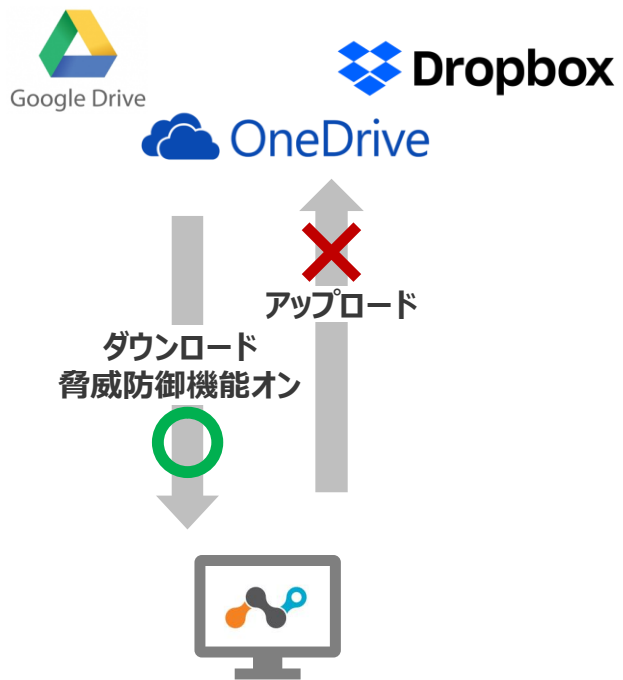
② 認可外のサービスでも柔軟な制御

多様なクラウドストレージをスコア毎に制御可能

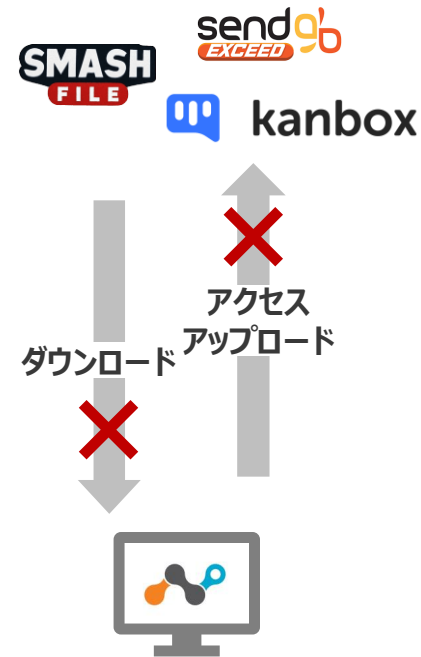
認可クラウドストレージ



高スコアの認可外クラウドストレージ

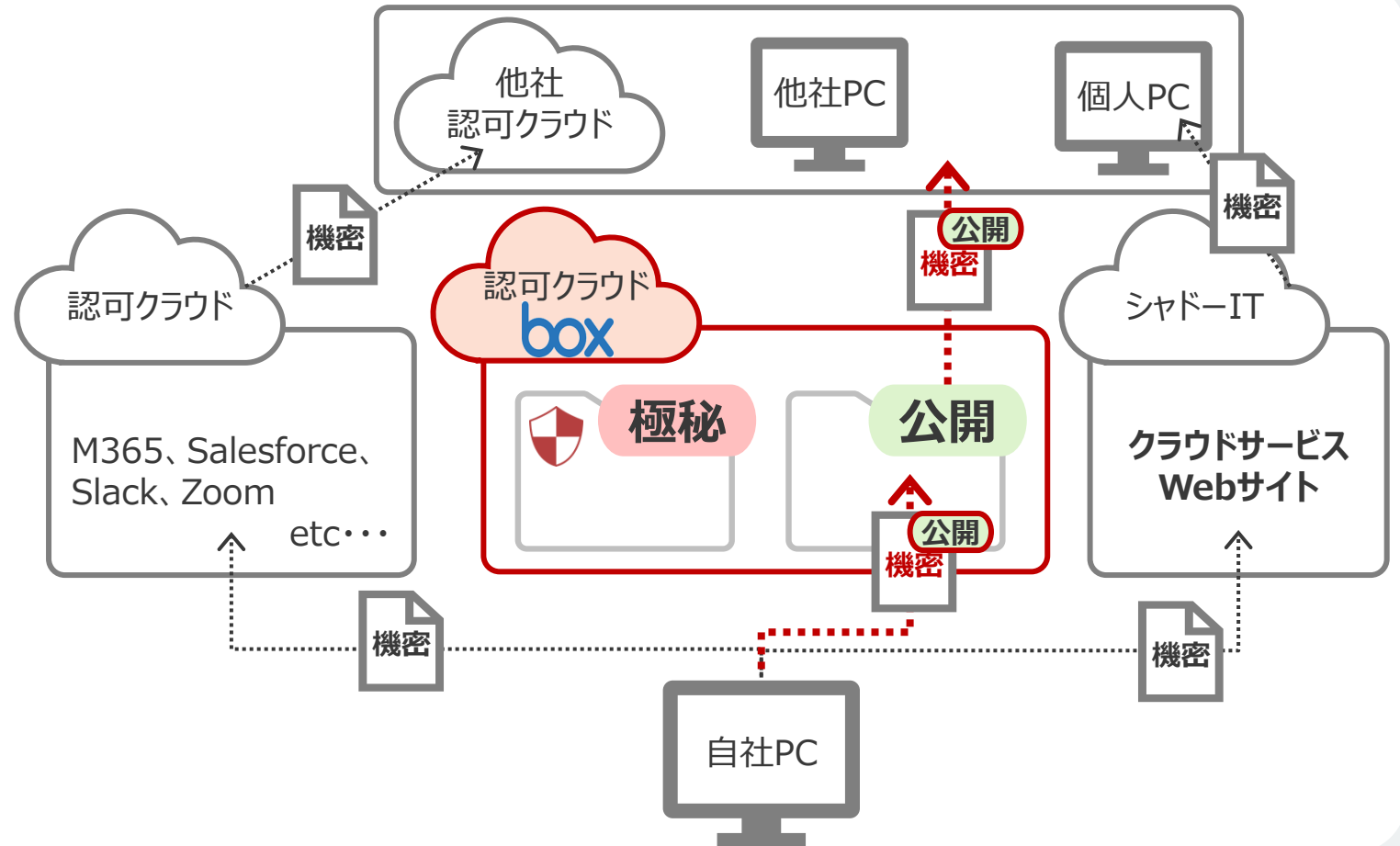


低スコアの認可外クラウドストレージ



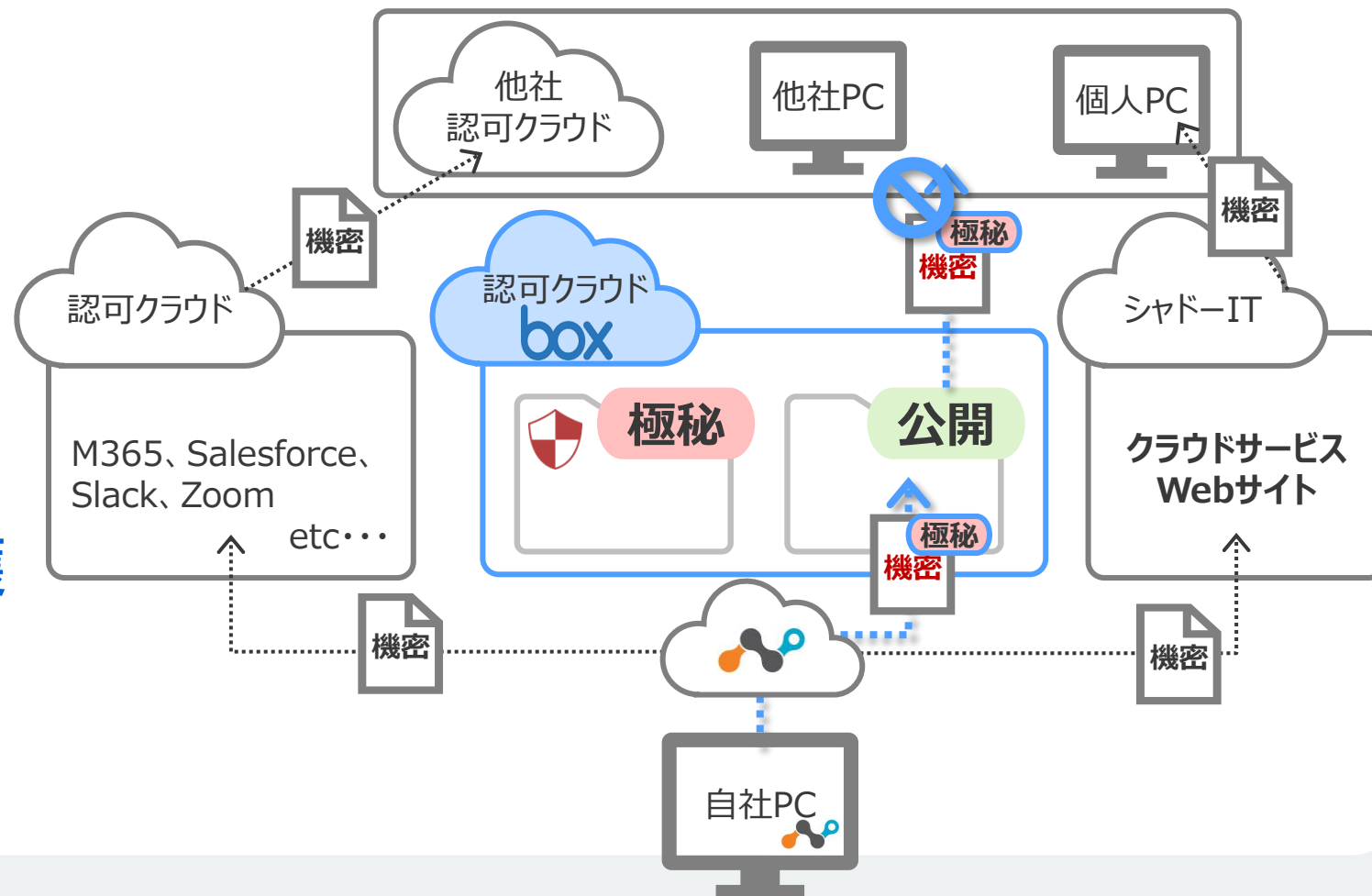
Netskopeでできる情報漏洩対策

③ ユーザの オペミス・不正

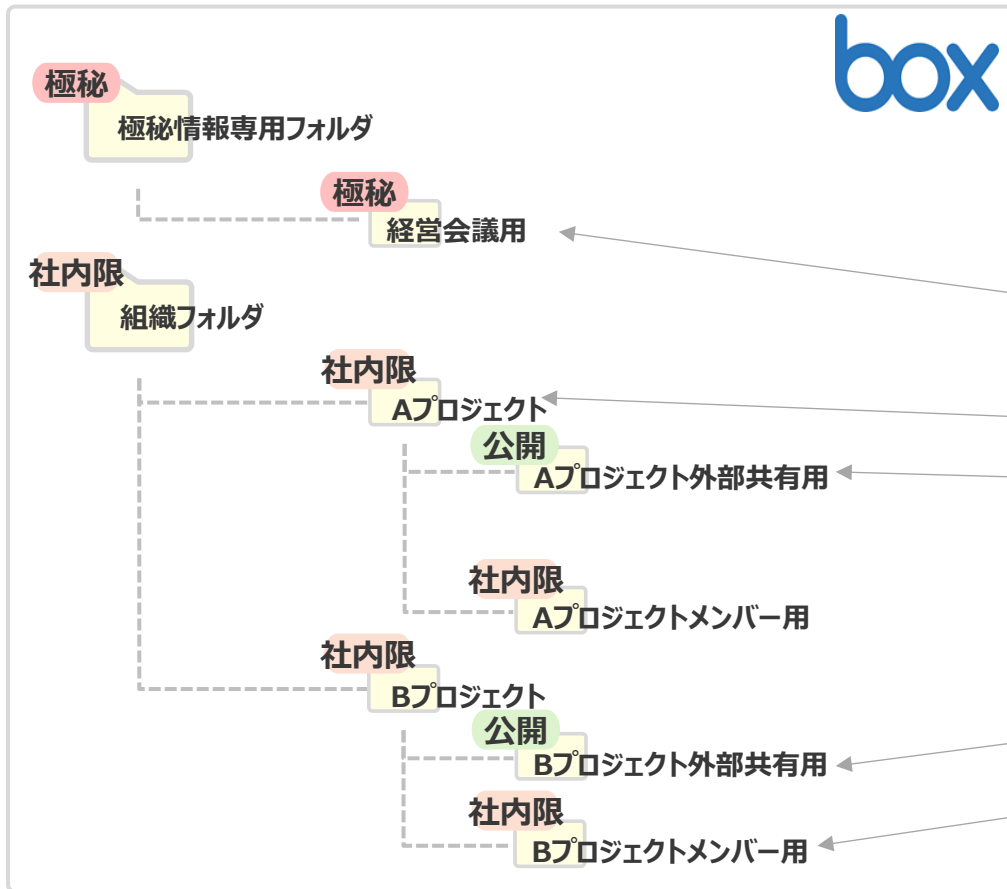


Netskopeでできる情報漏洩対策

③ ユーザの **オペミス・不正**
があっても、
データそのものを監視し
機密情報は適切に保護

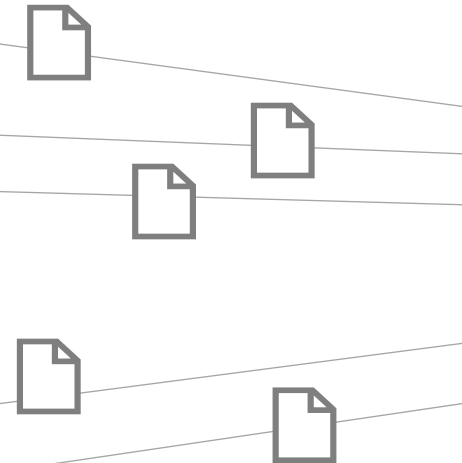


③ ユーザのオペミス・故意の不正を逃さない



Boxラベルによるデータ保護の流れ

(1) ユーザがBoxへファイルをアップロード

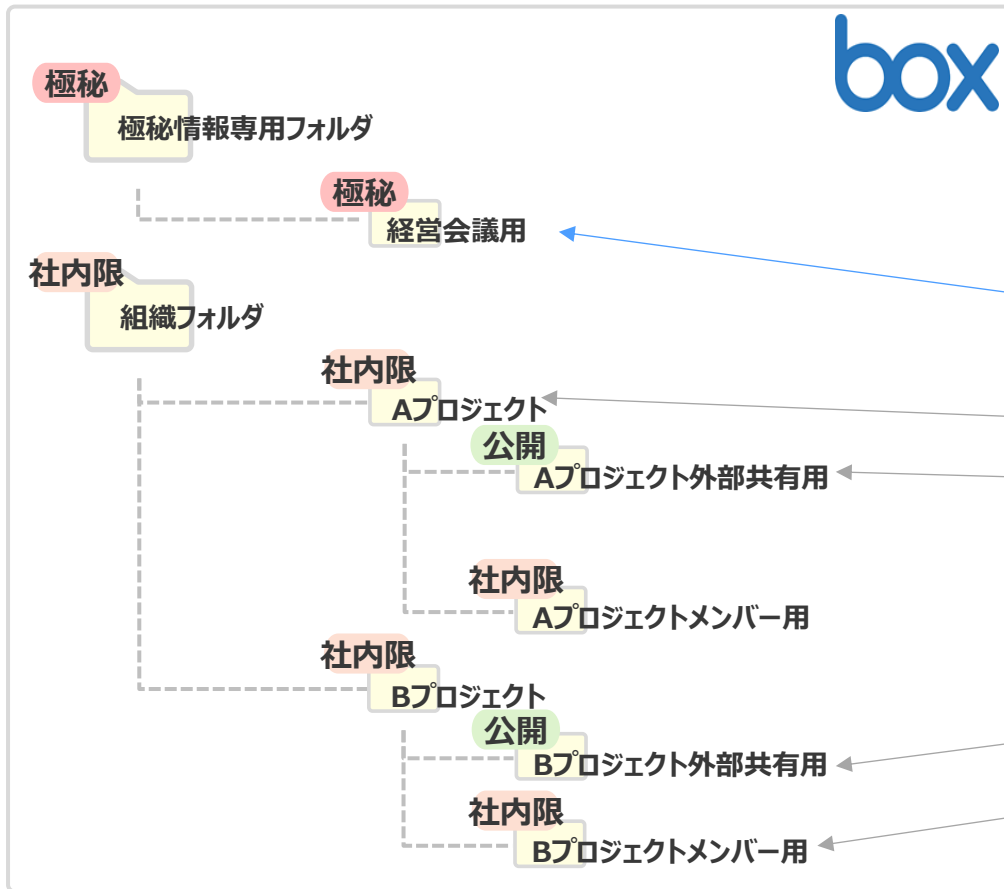


ユーザ



ユーザ

③ ユーザのオペミス・故意の不正を逃さない

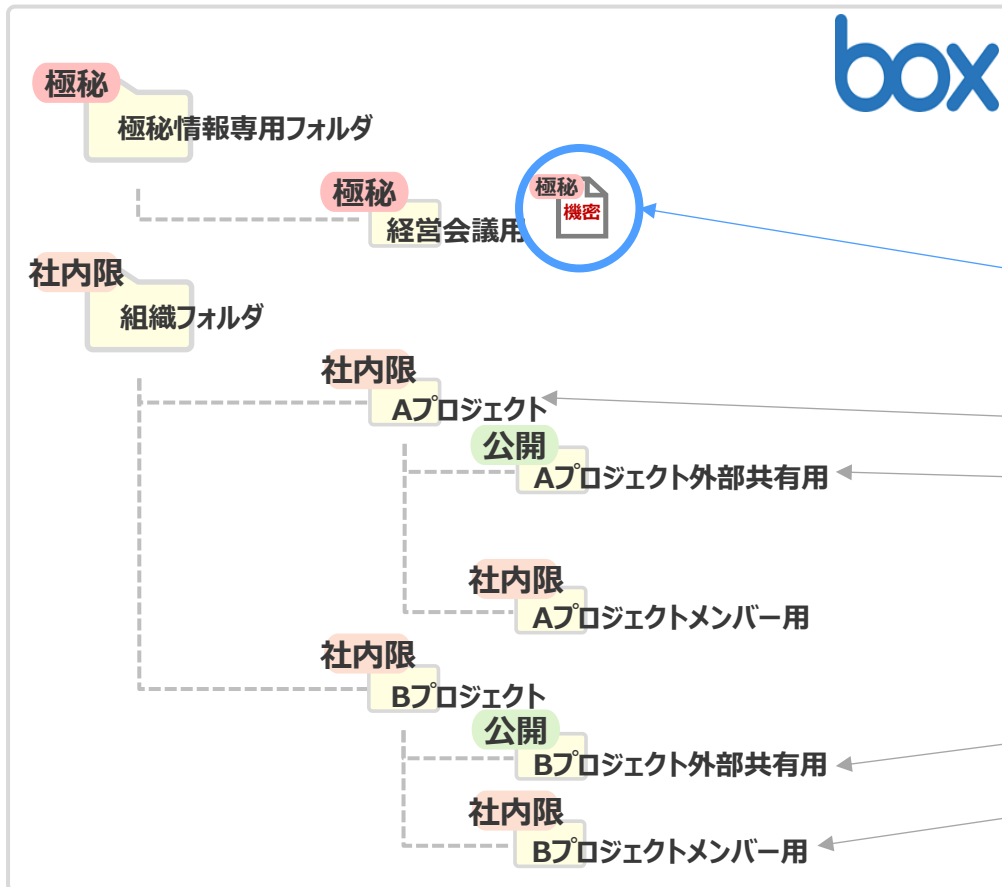


Boxラベルによるデータ保護の流れ

(1) ユーザがBoxへファイルをアップロード

※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている

③ ユーザのオペミス・故意の不正を逃さない



Boxラベルによるデータ保護の流れ

- (1) ユーザがBoxへファイルをアップロード
※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている
- (2) 格納先によって異なるラベルが付与され、機密情報は適切に保護される



ユーザ



ユーザ

③ ユーザのオペミス・故意の不正を逃さない

The diagram illustrates the data protection flow in Box. It shows a user uploading a file to a folder labeled '極秘情報専用フォルダ' (Top Secret Information Dedicated Folder). The file is then stored in a folder labeled '機密' (Confidential). The diagram also shows other folders with labels like '社内' (Internal), 'プロジェクト公開' (Project Public), and 'プロジェクト外部共有' (Project External Sharing). A large 'でも...' (But...) text is overlaid on the diagram, suggesting a potential issue or limitation in the current setup. A thinking man icon is also present, indicating a point of reflection or a question.

Boxラベルによるデータ保護の流れ

- (1) ユーザがBoxへファイルをアップロード
※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている
- (2) 格納先によって異なるラベルが付与され、**機密情報は適切に保護される**

でも・・・

ユーザー

ユーザー

③ ユーザのオペミス・故意の不正を逃さない

Boxラベルによるデータ保護の流れ

(1) ユーザがBoxへファイルをアップロード
※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている

(2) 格納先によって異なるラベルが付与され、機密情報は適切に保護される

どんなデータが機密情報に該当するか、ユーザ自身で正しく判断できるのか？

極秘
極秘情報専用フォルダ

社内限
社内限
社内限

公開
公開
公開

プロジェクト外部共有用
プロジェクト外部共有用
プロジェクト外部共有用

プロジェクトメンバー用
プロジェクトメンバー用
プロジェクトメンバー用

ユーザー
ユーザー

③ ユーザのオペミス・故意の不正を逃さない

Boxラベルによるデータ保護の流れ

(1) ユーザがBoxへファイルをアップロード
※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている

(2) 格納先によって異なるラベルが付与され、機密情報は適切に保護される

✓ **どんなデータが機密情報に該当するか、**
ユーザ自身で正しく判断できるのか？

✓ **機密情報を故意にまたは誤って**
公開フォルダへ格納 されてしまう可能性は？

③ ユーザのオペミス・故意の不正を逃さない

ここで、頼りになるのが

Boxラベルによるデータ保護の流れ

(1) ユーザがBoxへファイルをアップロード
※機密情報を含む文書は、極秘情報専用フォルダの配下へ格納するルールとなっている

(2) 格納先によって異なるラベルが付与され、機密情報は適切に保護される

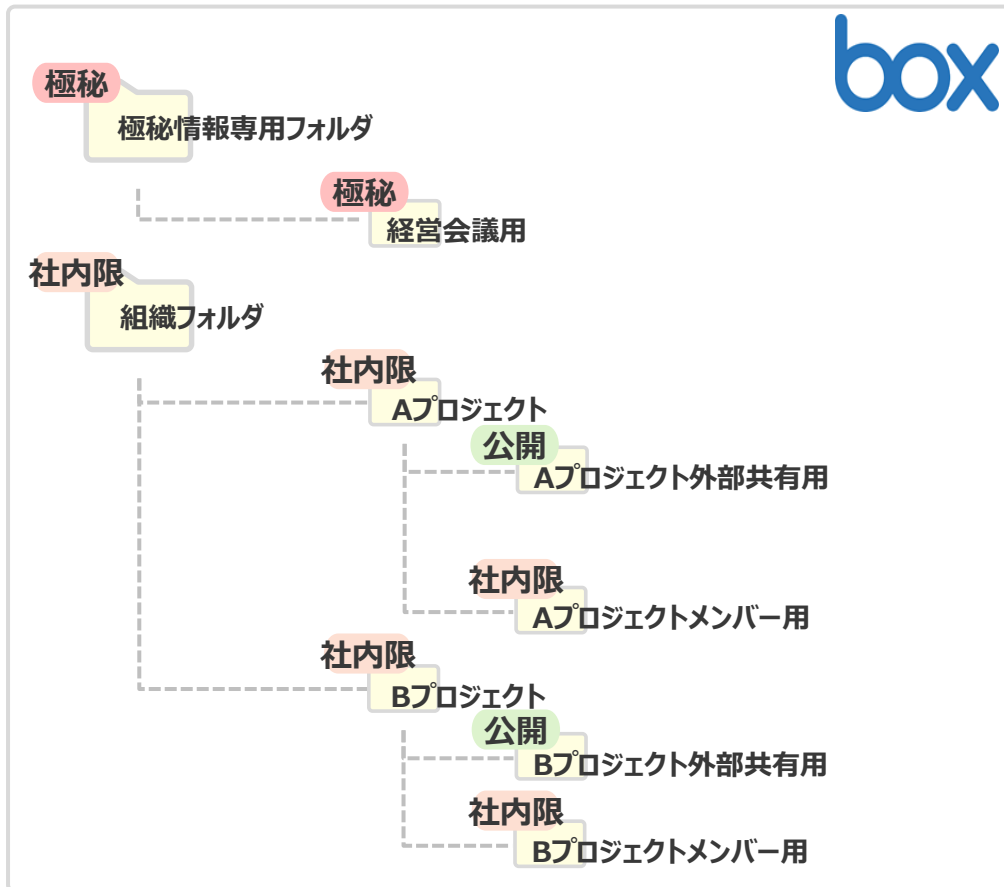
極秘
極秘情報専用フォルダ
社内
会議用
機密
社内
プロジェクト公開
Aプロジェクトメンバー用
社内限
Aプロジェクトメンバー用
プロジェクト公開
Bプロジェクト外部共有用
社内限
Bプロジェクトメンバー用

機密

ユーザー

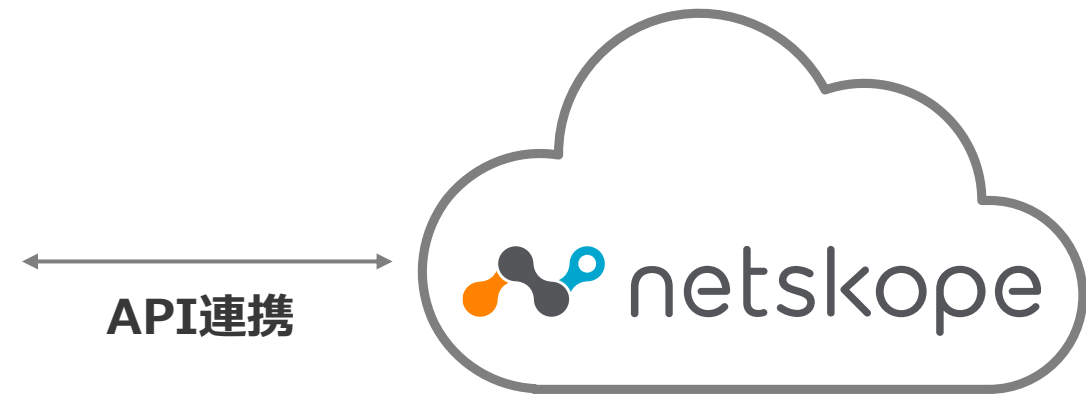
netskope

③ ユーザのオペミス・故意の不正を逃さない

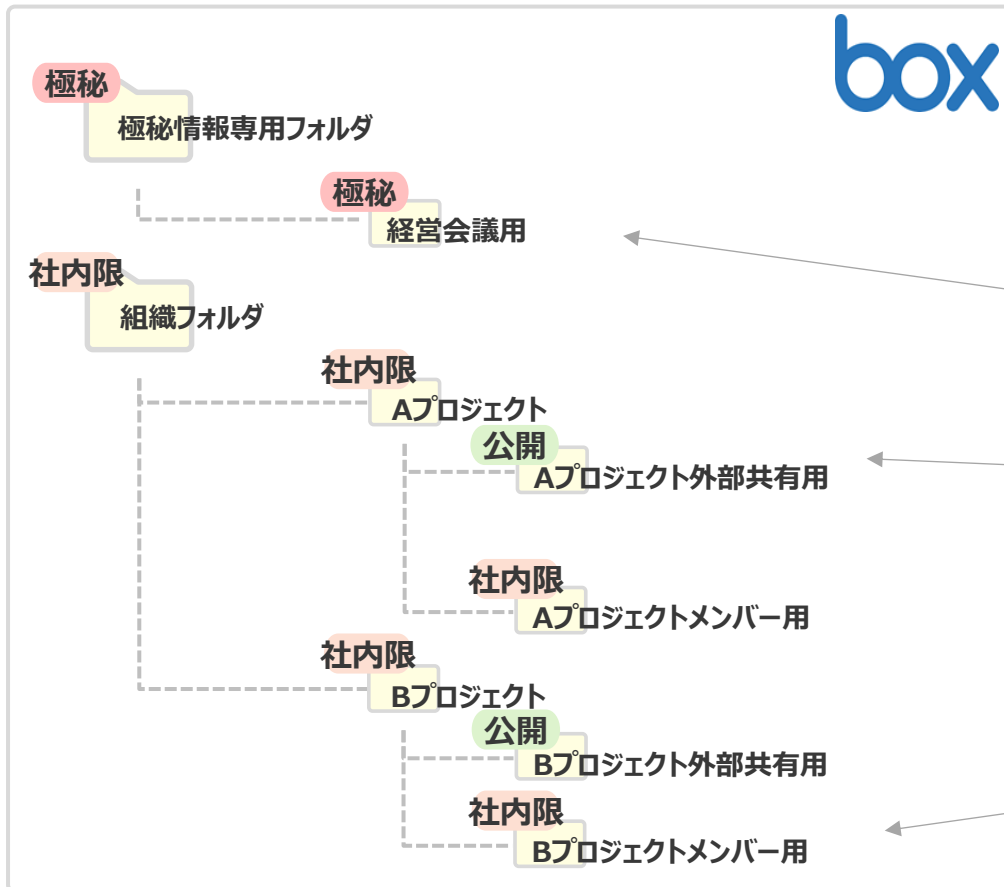


BoxラベルとNetskopeによるデータ保護

(1) BoxとNetskopeをAPI連携



③ ユーザのオペミス・故意の不正を逃さない



BoxラベルとNetskopeによるデータ保護

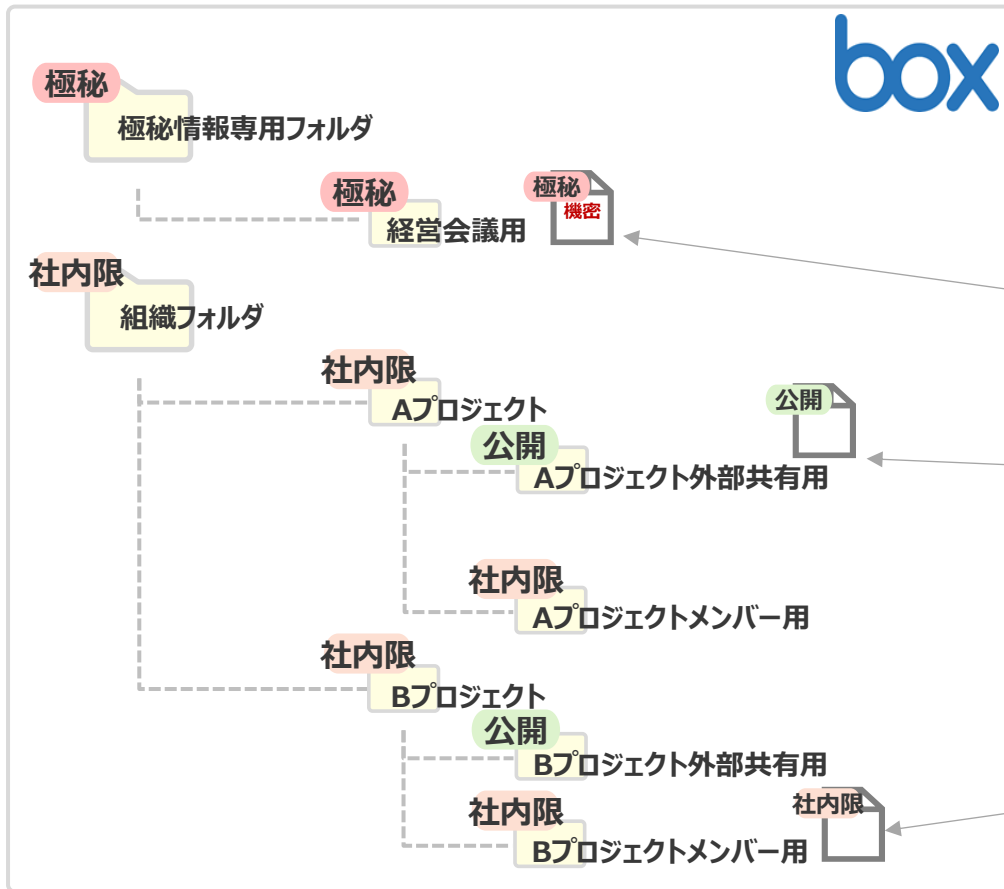
- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード



ユーザ

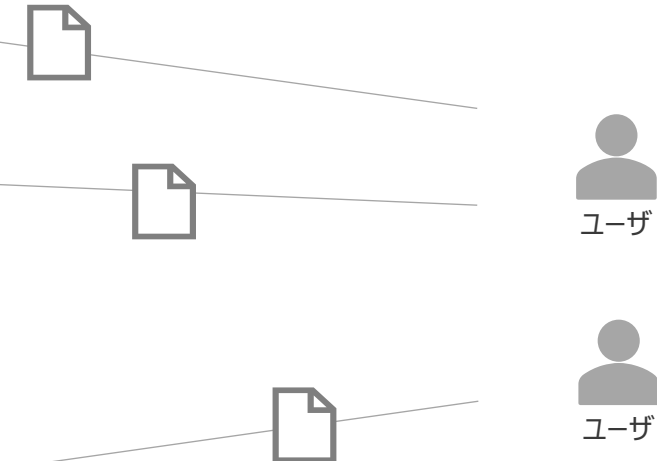
ユーザ

③ ユーザのオペミス・故意の不正を逃さない

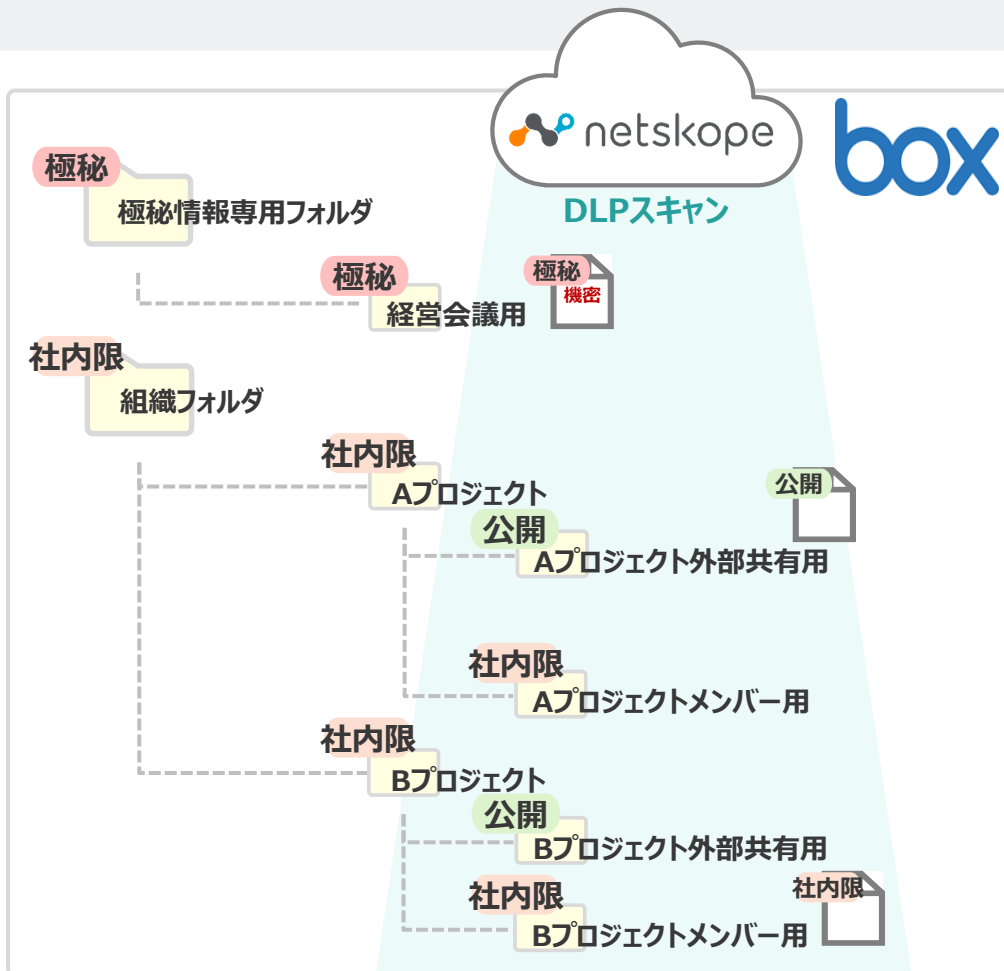


BoxラベルとNetskopeによるデータ保護

- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード
- (3) 格納先に応じてBoxラベルが付与される --- ここまではBoxだけの保護



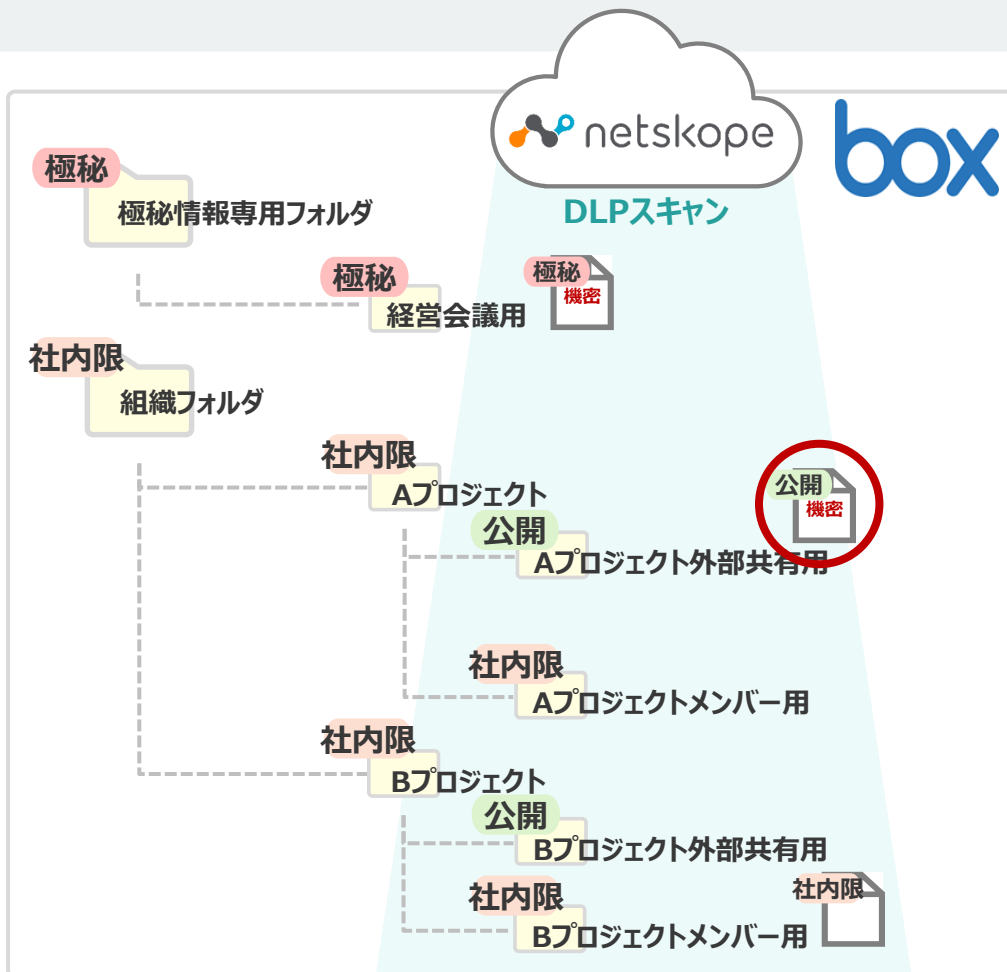
③ ユーザのオペミス・故意の不正を逃さない



BoxラベルとNetskopeによるデータ保護

- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード
- (3) 格納先に応じてBoxラベルが付与される
- (4) アップロードされたファイル内に機密情報が含まれていないかNetskopeのDLP機能で漏れなくスキャン

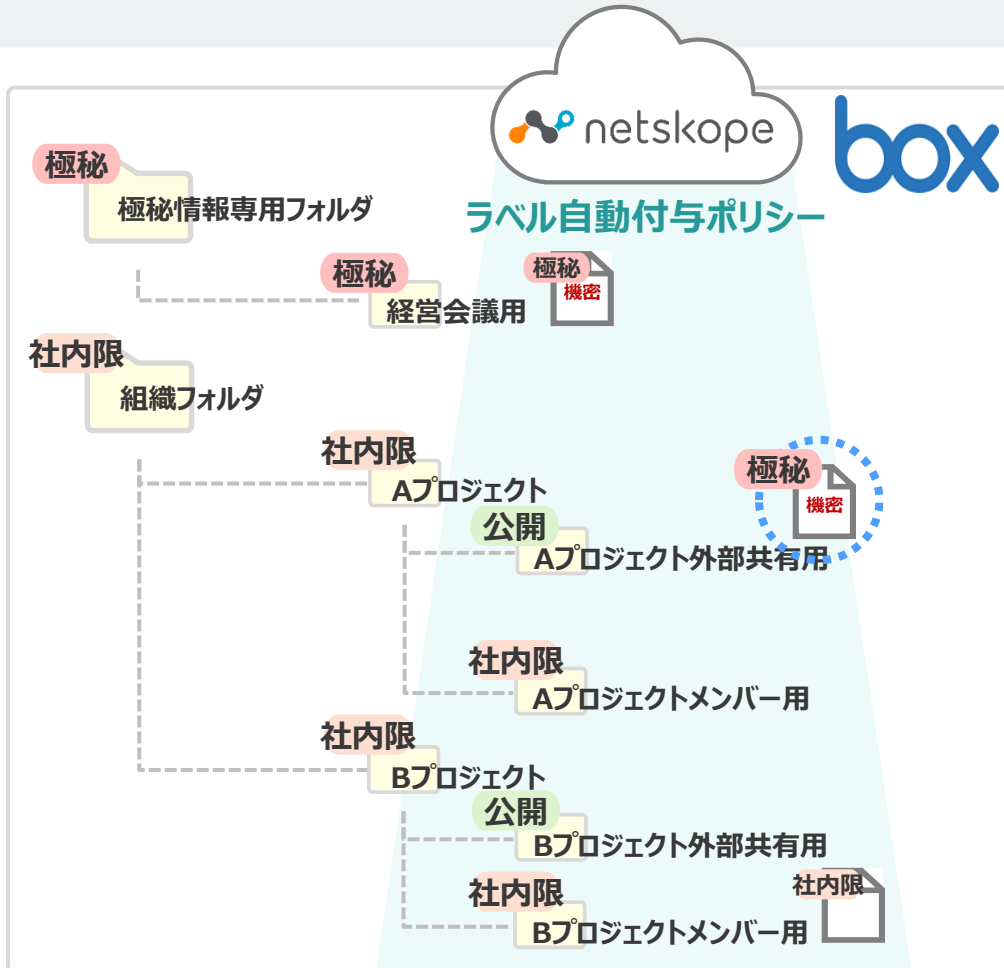
③ ユーザのオペミス・故意の不正を逃さない



BoxラベルとNetskopeによるデータ保護

- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード
- (3) 格納先に応じてBoxラベルが付与される
- (4) アップロードされたファイル内に機密情報が含まれていないかNetskopeのDLP機能で漏れなくスキャン
⇒公開フォルダ内に機密情報を含むファイルを発見！

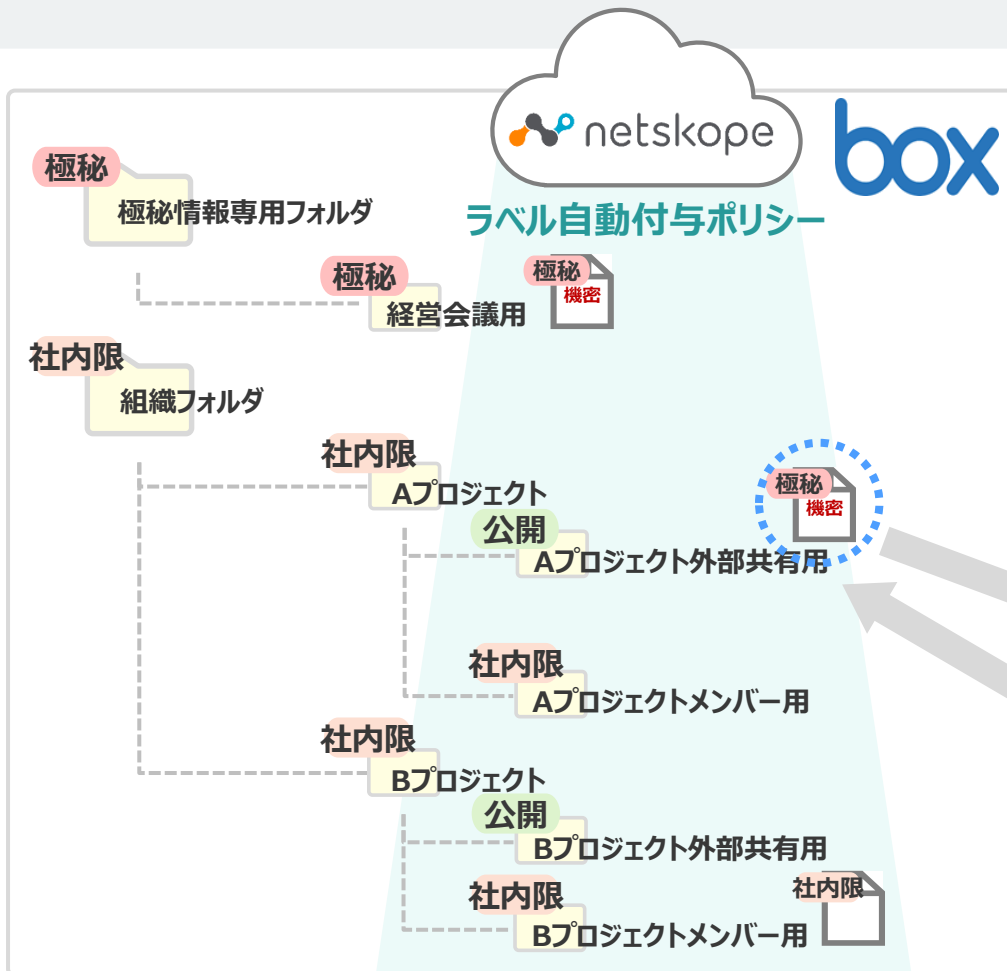
③ ユーザのオペミス・故意の不正を逃さない



BoxラベルとNetskopeによるデータ保護

- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード
- (3) 格納先に応じてBoxラベルが付与される
- (4) アップロードされたファイル内に機密情報が含まれていないかNetskopeのDLP機能で漏れなくスキャン
⇒公開フォルダ内に機密情報を含むファイルを発見！
- (5) 機密情報を含むデータに「極秘」ラベルを付与するポリシーが強制発動！
公開フォルダに置かれたデータであっても機密情報はしっかり「極秘」に

③ ユーザのオペミス・故意の不正を逃さない



BoxラベルとNetskopeによるデータ保護

- (1) BoxとNetskopeをAPI連携
- (2) ユーザがBoxへファイルをアップロード
- (3) 格納先に応じてBoxラベルが付与される
- (4) アップロードされたファイル内に機密情報が含まれていないか
NetskopeのDLP機能で漏れなくスキャン
⇒公開フォルダ内に機密情報を含むファイルを発見！
- (5) 機密情報を含むデータに「極秘」ラベルを付与するポリシーが強制発動！
公開フォルダに置かれたデータであっても機密情報はしっかり「極秘」に
- (6) 「極秘」ラベルによってデータが適切に保護される

極秘

更新/ダウンロード：所有者以上
閲覧：プレビューアー以上

『Aプロジェクト共有用』に招待されていないユーザ

クラウドストレージからの情報漏洩対策

NetskopeとBoxの組み合わせが
凄いのは分かったけど、

Shieldオプション**買ってない。**



クラウドストレージからの情報漏洩対策

そもそも

Box使っていない んだよね。



クラウドストレージからの情報漏洩対策



もちろん、Shieldなしでも、
Box以外のクラウドストレージでも、

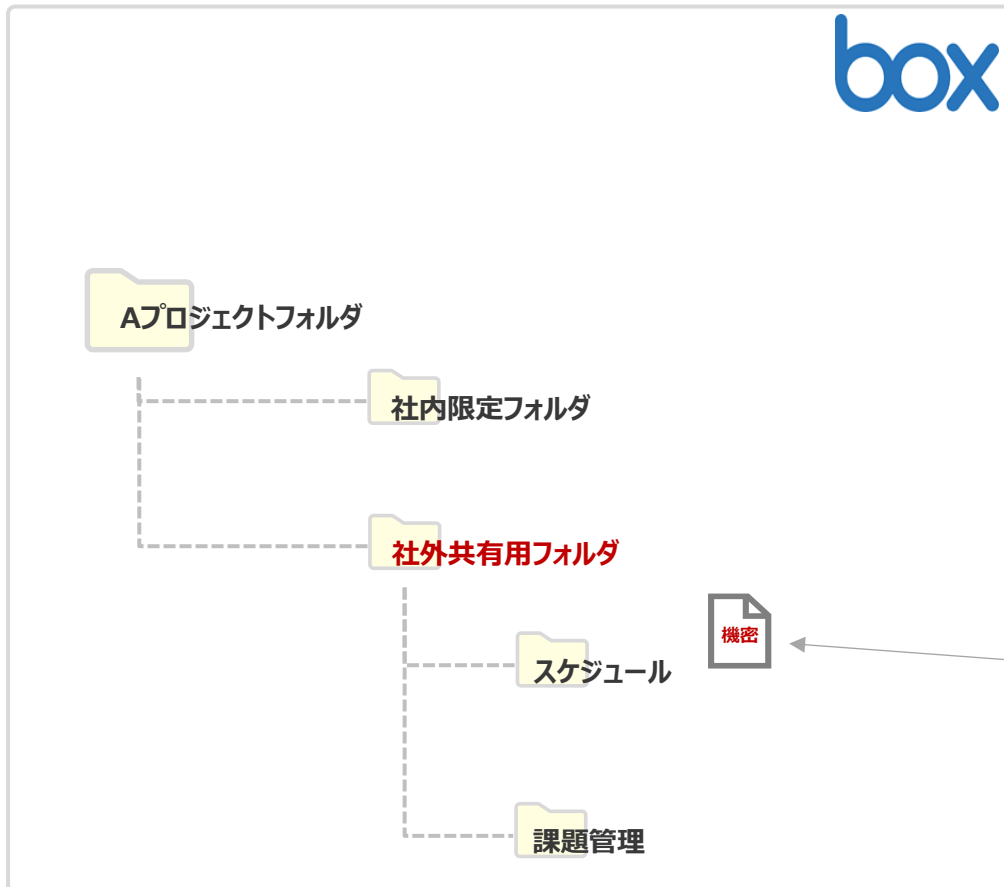


netskope

で

ちゃんと 情報漏洩対策できます。

Box Shieldなしでもできる、オペミス・不正対策



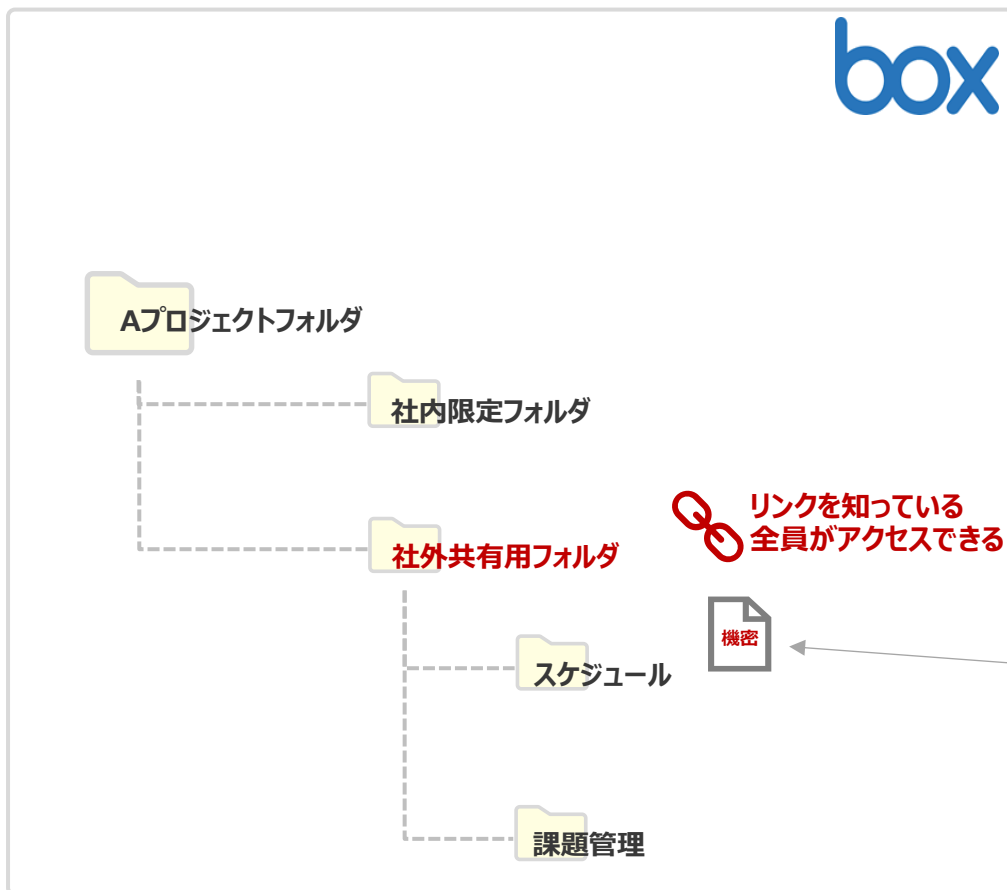
社外共有用フォルダへのアクセス権を持つユーザ

社内ユーザのCさん	所有者
社内ユーザのDさん	編集者として招待
取引先A社のXさん	編集者として招待
取引先A社のYさん	編集者として招待
取引先A社のZさん	編集者として招待

オペミス

社内ユーザのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、

Box Shieldなしでもできる、オペミス・不正対策



社外共有用フォルダへのアクセス権を持つユーザ

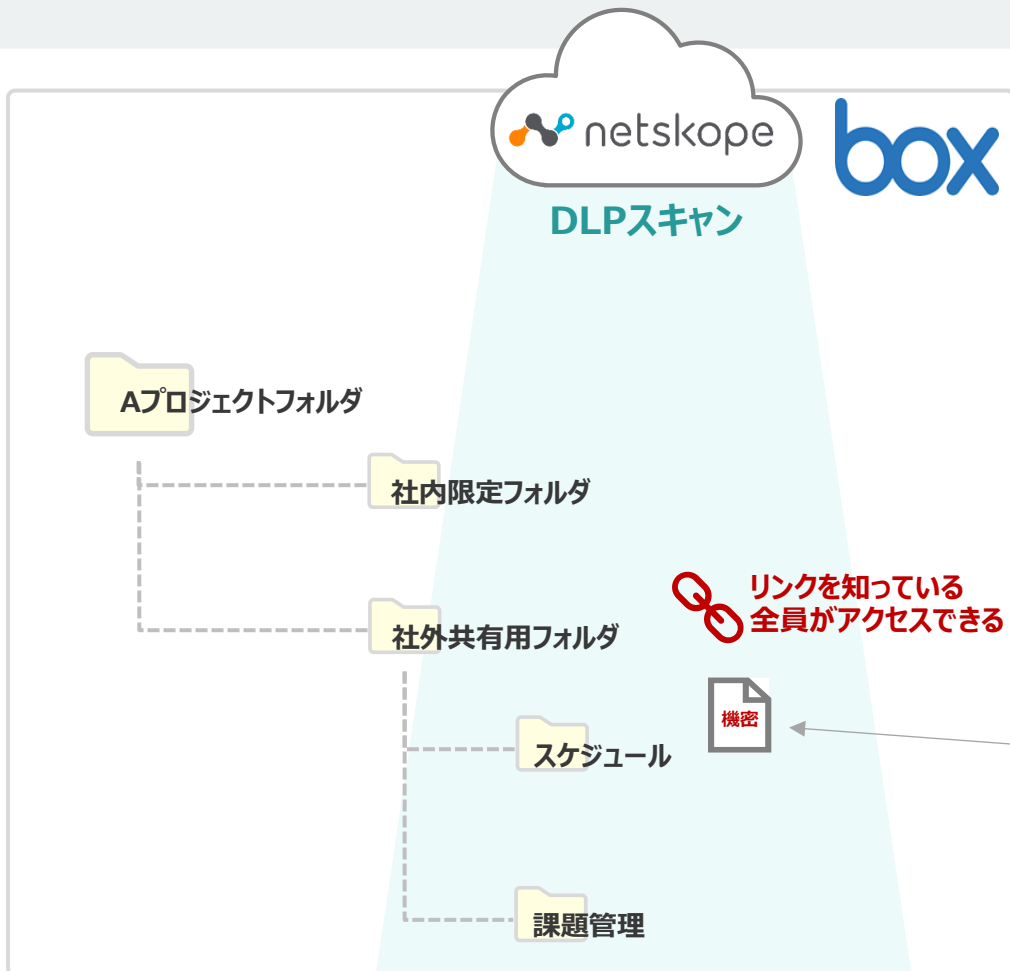
社内ユーザのCさん	所有者
社内ユーザのDさん	編集者として招待
取引先A社のXさん	編集者として招待
取引先A社のYさん	編集者として招待
取引先A社のZさん	編集者として招待

オペミス

社内ユーザ
Dさん

社内ユーザのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、共有リンクの公開範囲を「リンクを知っている全員」に誤って設定してしまうケースが発生

Box Shieldなしでもできる、オペミス・不正対策



社外共有用フォルダへのアクセス権を持つユーザ

社内ユーザのCさん	所有者
社内ユーザのDさん	編集者として招待
取引先A社のXさん	編集者として招待
取引先A社のYさん	編集者として招待
取引先A社のZさん	編集者として招待

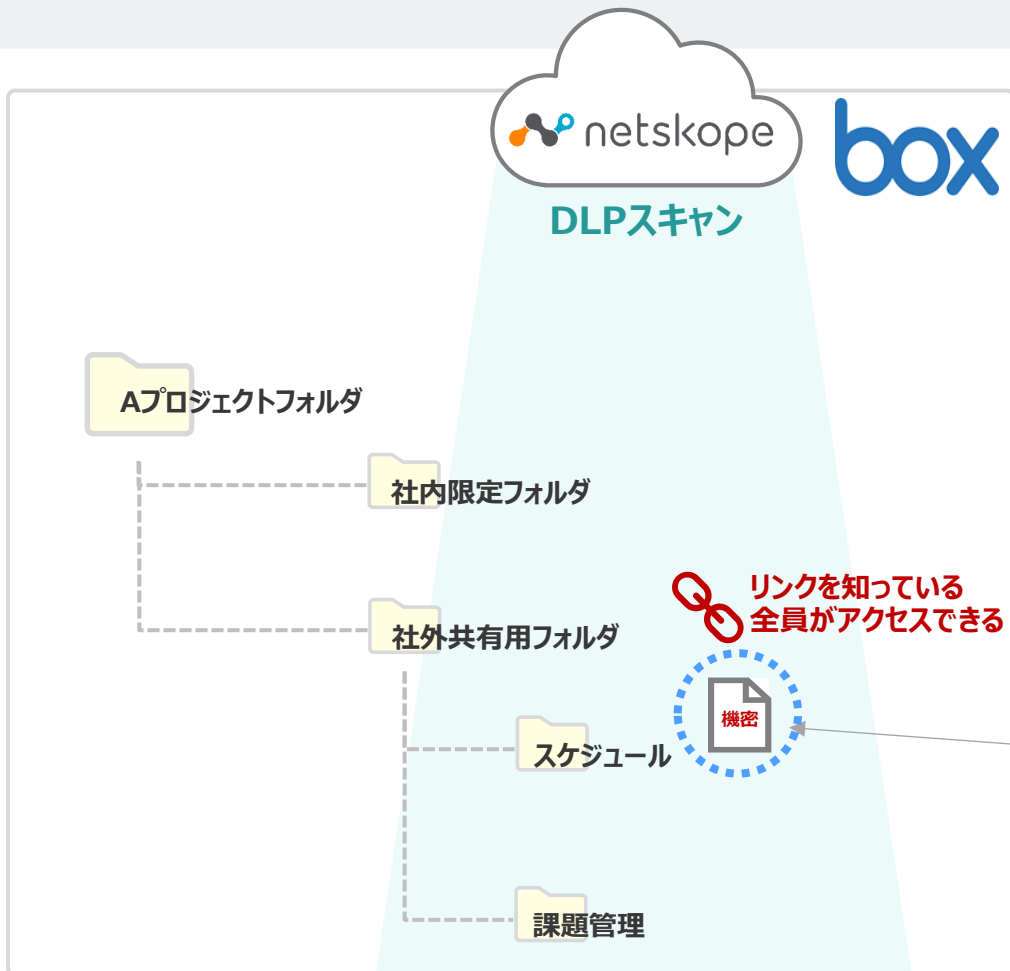
オペミス

社内ユーザのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、共有リンクの公開範囲を「リンクを知っている全員」に誤って設定してしまうケースが発生



(1) NetskopeのDLPスキャンで機密情報ファイルを検知

Box Shieldなしでもできる、オペミス・不正対策



社外共有用フォルダへのアクセス権を持つユーザー

社内ユーザーのCさん	所有者
社内ユーザーのDさん	編集者として招待
取引先A社のXさん	編集者として招待
取引先A社のYさん	編集者として招待
取引先A社のZさん	編集者として招待

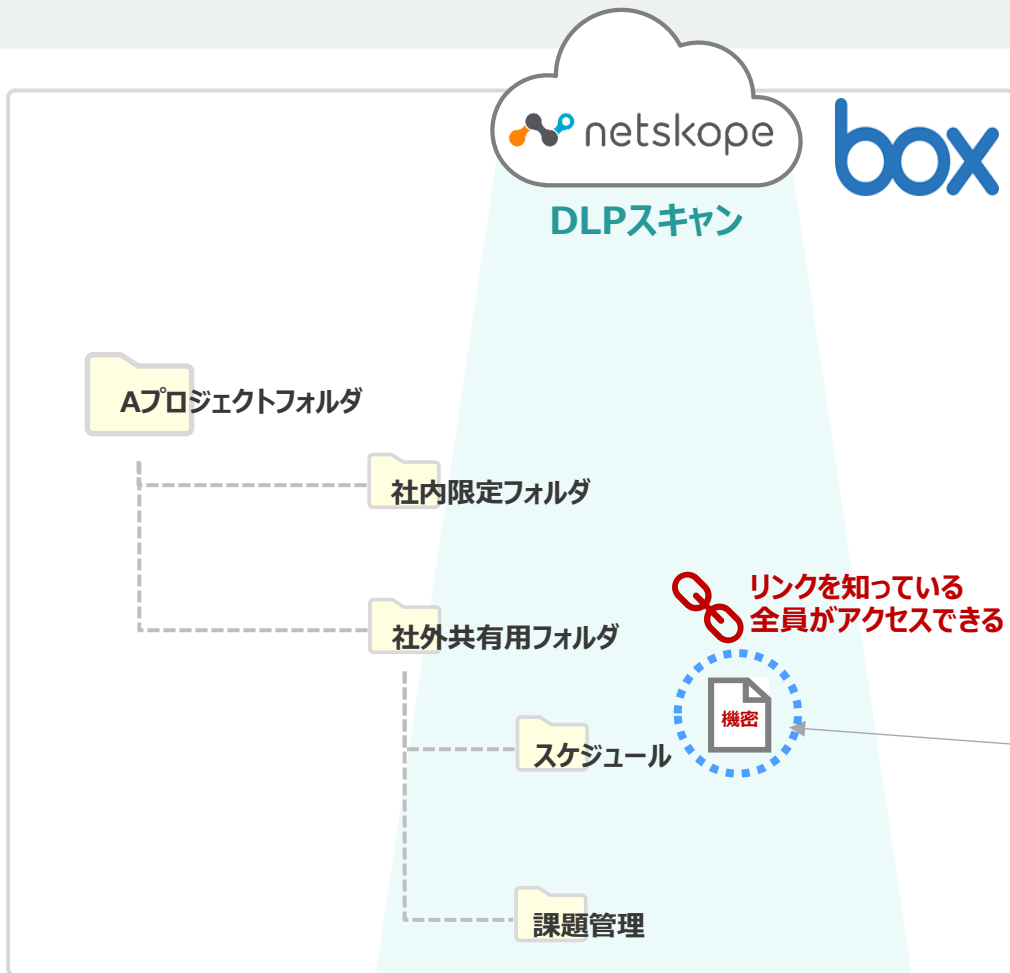
オペミス

社内ユーザーのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、共有リンクの公開範囲を「リンクを知っている全員」に誤って設定してしまうケースが発生



- (1) NetskopeのDLPスキャンで機密情報ファイルを検知
- (2) Netskopeのポリシーで、以下2つを強制適用
 - ①所有者以外を閲覧・アップロード権限のみに降格
 - ②当該ファイルの共有リンクを削除

Box Shieldなしでもできる、オペミス・不正対策



社外共有用フォルダへのアクセス権を持つユーザ

社内ユーザのCさん	所有者	
社内ユーザのDさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のXさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のYさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のZさん	編集者として招待	閲覧・アップロード権限に降格

オペミス

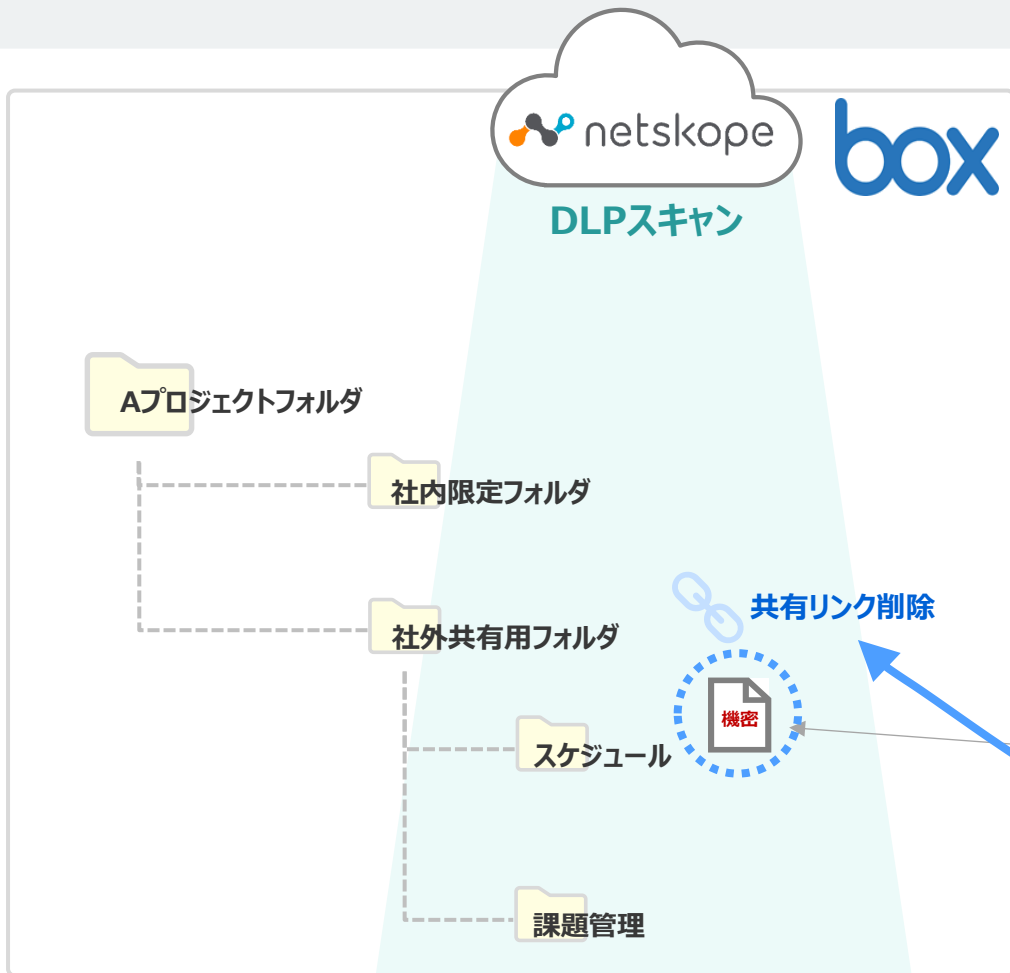
社内ユーザのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、共有リンクの公開範囲を「リンクを知っている全員」に誤って設定してしまうケースが発生



社内ユーザ
Dさん

- (1) NetskopeのDLPスキャンで機密情報ファイルを検知
- (2) Netskopeのポリシーで、以下2つを強制適用
 - ①所有者以外を閲覧・アップロード権限のみに降格
 - ②当該ファイルの共有リンクを削除

Box Shieldなしでもできる、オペミス・不正対策



社外共有用フォルダへのアクセス権を持つユーザ

社内ユーザのCさん	所有者	
社内ユーザのDさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のXさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のYさん	編集者として招待	閲覧・アップロード権限に降格
取引先A社のZさん	編集者として招待	閲覧・アップロード権限に降格

オペミス

社内ユーザのDさんが、機密情報が含まれるファイルを公開フォルダにアップロードし、共有リンクの公開範囲を「リンクを知っている全員」に誤って設定してしまうケースが発生

- (1) NetskopeのDLPスキャンで機密情報ファイルを検知
- (2) Netskopeのポリシーで、以下2つを強制適用
 - ①所有者以外を閲覧・アップロード権限のみに降格
 - ②当該ファイルの共有リンクを削除

Box Shieldの有無でできることの違い



Box Shield あり

- フォルダやファイル単位での制御が可能
- DLP違反したファイルにだけラベルを貼りかえるポリシーを適用できるため、復旧が容易

Box Shield なし

- 共有リンクの削除はファイル単位で可能
- 権限の降格は対象のフォルダ配下すべてに継承され、違反していないフォルダ・ファイル・招待ユーザ全員に適用される
- 降格した権限の復旧作業が大変



権限降格はかなり強力で影響範囲が広範囲に及ぶため、適用する場合には慎重な検討が必要

Box以外のクラウドストレージも情報漏洩対策OK

認可クラウドでも機密情報の取り扱いには注意が必要



認可クラウドだから、
通常ファイルのアップロードOK！



Box以外のクラウドストレージも情報漏洩対策OK

認可クラウドでも機密情報の取り扱いには注意が必要



認可クラウドだから、
通常ファイルのアップロードOK！

機密情報のアップロードは、
認可クラウドであっても慎重になっ
てほしい



Box以外のクラウドストレージも情報漏洩対策OK

認可クラウドでも機密情報の取り扱いには注意が必要
とはいえ、機密情報のアップロードを
その都度許可制にするなんて運用は
到底無理・・・

機密情報のアップロードは、
認可クラウドであっても慎重になっ
てほしい



認可クラウドが
通常ファイルのアップロードOK！



Box以外のクラウドストレージも情報漏洩対策OK

認可クラウドでも機密情報の取り扱いには注意が必要
とはいえ、機密情報のアップロードを
その都度許可制にするなんて運用は
到底無理・・・

認可クラウドが
通常ファイルのアップロードOK！



機密情報のアップロードは、
認可クラウドであっても慎重になっ
てほしい

いっそ、認可クラウドなら
一律アップロードを許可するべき？

Box以外のクラウドストレージも情報漏洩対策OK

認可クラウドでも機密情報の取り扱いには注意が必要



諦めるのはまだ早い！
許可でもブロックでもない、

第三の選択肢、あります。

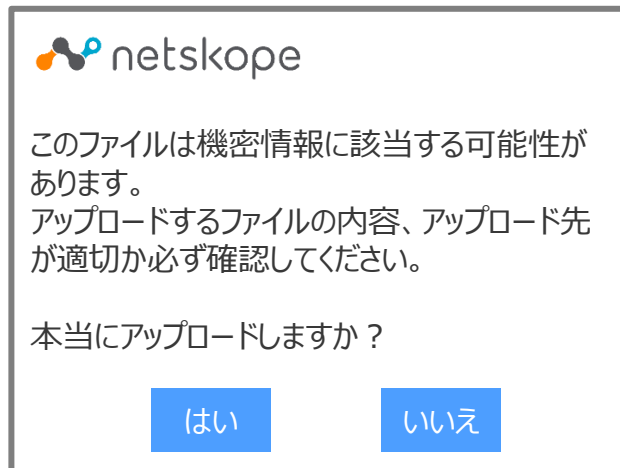
機密情報
認可クラウドでも慎重になっ
てほしい


認可クラウドだから、
機密ファイルのアップロードOK！



Box以外のクラウドストレージも情報漏洩対策OK

ユーザアラートで柔軟な制御



 netskope

このファイルは機密情報に該当する可能性があります。
アップロードするファイルの内容、アップロード先が適切か必ず確認してください。

本当にアップロードしますか？

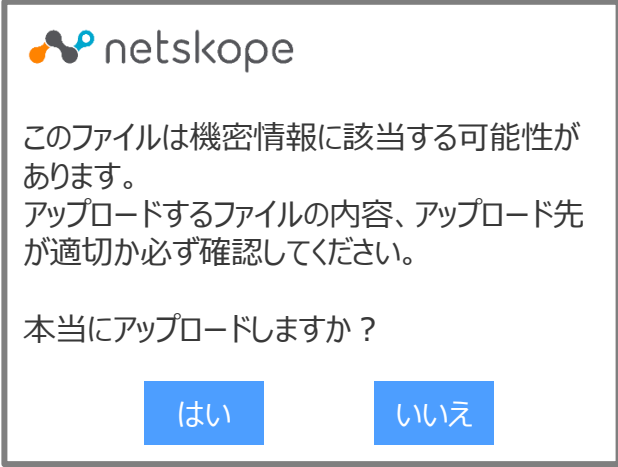



機密情報が含まれているファイルの場合には、ブラウザ上に警告を表示することが可能



Box以外のクラウドストレージも情報漏洩対策OK

ユーザアラートで柔軟な制御



 netskope

このファイルは機密情報に該当する可能性があります。
アップロードするファイルの内容、アップロード先が適切か必ず確認してください。

本当にアップロードしますか？



機密情報が含まれているファイルの場合には、ブラウザ上に警告を表示することが可能

⇒ユーザの誤操作による
情報漏洩を軽減！



本セッションのまとめ

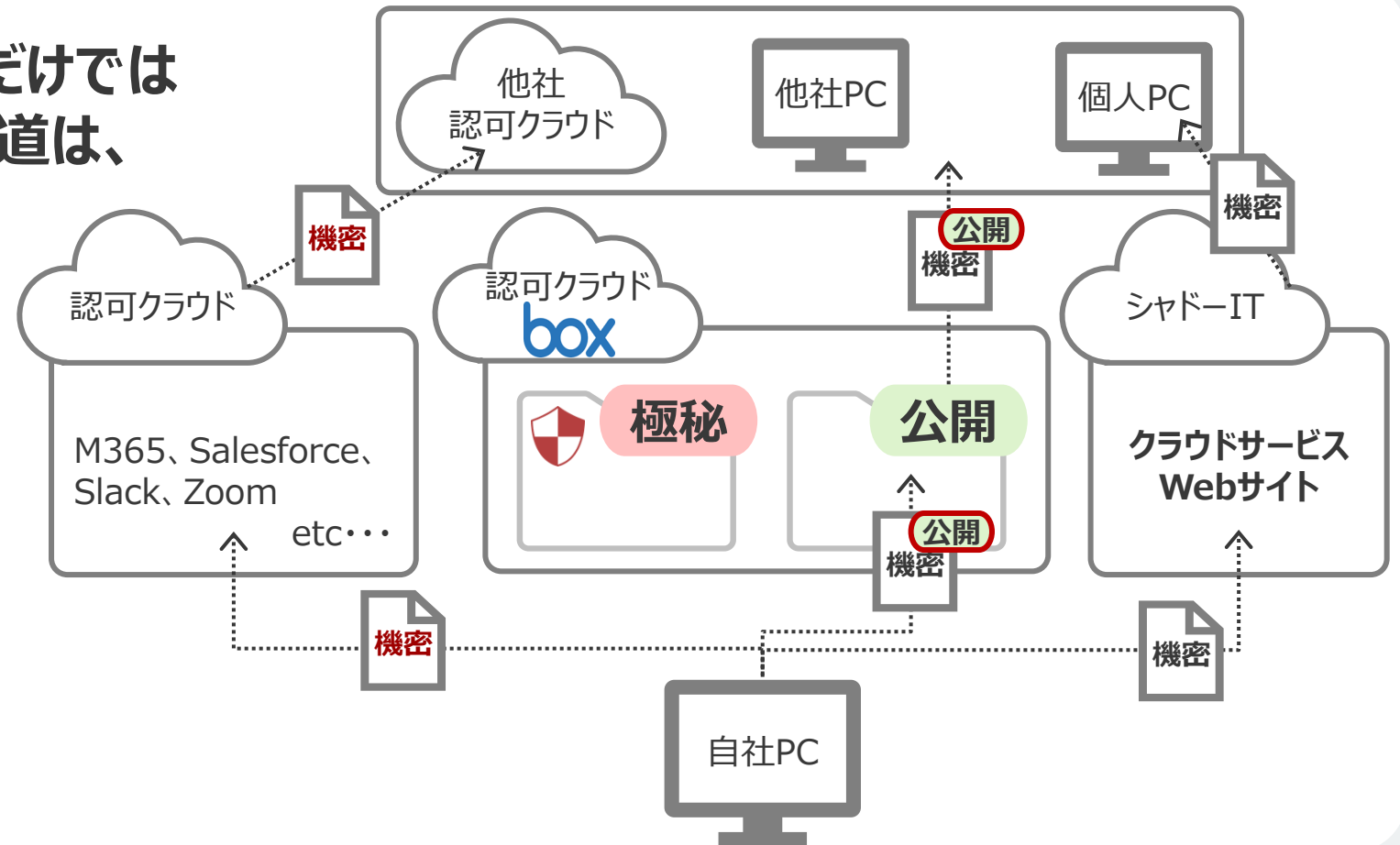
クラウドからの情報漏洩ゼロを目指す、当社のベストプラクティス

データ種別	データの内容	Netskopeポリシー
取り扱い禁止	<ul style="list-style-type: none">会社ルールとしてBox内での取り扱い禁止データ(マイナンバー等)	<ul style="list-style-type: none">DLPで検知してリアルタイムブロック
極秘	<ul style="list-style-type: none">社外への持ち出しを一切許可しない極秘資料社内でも限られたユーザがアクセス可能なデータ	<ul style="list-style-type: none">DLPで検知してユーザーアラートDLPで検知してラベル変更(Shieldあり)DLPで所有者以外の権限降格(Shieldなし)
社内限	<ul style="list-style-type: none">極秘以外の各組織で必要な資料	<ul style="list-style-type: none">DLPで検知してユーザーアラートDLPで検知してラベル変更(Shieldあり)
公開	<ul style="list-style-type: none">社外の方と共同で作業するプロジェクト資料不特定多数のユーザーに公開するカタログやマニュアルなど	<ul style="list-style-type: none">制限なし
全てのデータ	<ul style="list-style-type: none">全てのデータ	<ul style="list-style-type: none">Box以外のクラウドストレージへのアップロードは一律ブロックダウンロードは脅威防御機能を有効にしたうえで、高スコアのサービスからのみ許可

本セッションのまとめ

クラウドストレージを利用するだけでは防ぎきれない情報漏洩の抜け道は、

- ① 認可クラウドの **不適切利用**
- ② **シャドーIT** を介した漏洩
- ③ ユーザの **オペミス・不正**

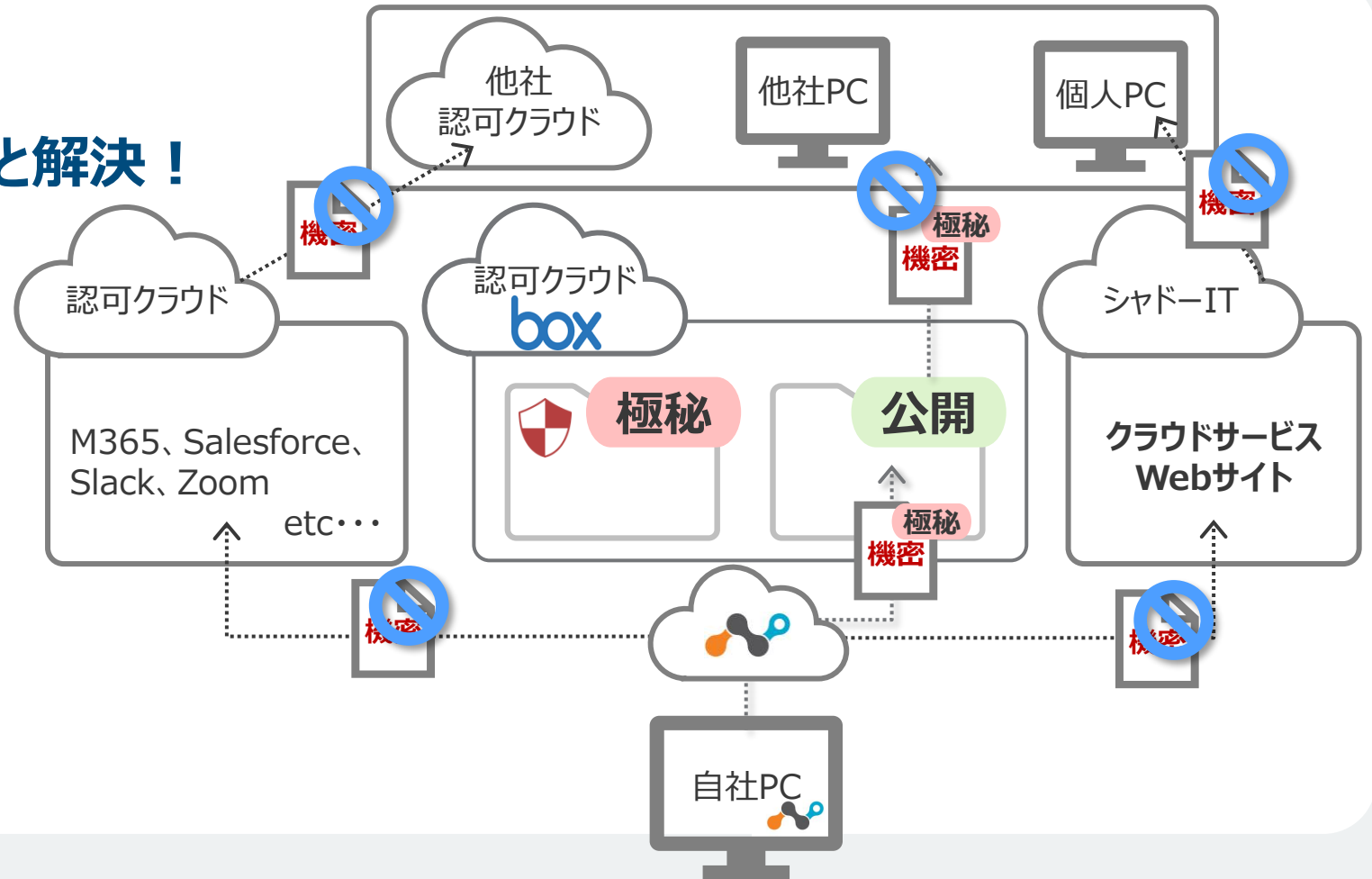


本セッションのまとめ



でまるっと解決！

- ① 認可クラウドの **不適切利用**
- ② シャドーIT を介した漏洩
- ③ ユーザの **オペミット不正**



本セッションのまとめ

 netskope

でまるっと解決！

- ① 認可クラウドの **不適切利用**
- ② シャドーIT を介した漏洩
- ③ ユーザの **オペミット不正**

