

シリーズ 第3回目

マイクロソフトとシトリックスが語る

VDIの正しい選び方

セキュリティ編

シトリックス・システムズ・ジャパン株式会社



ゲスト紹介



日本マイクロソフト株式会社
牛上 貴司 氏



Microsoft Azure

検索 Q アカウント ポータル サインイン

概要 ソリューション 製品 ドキュメント 価格 トレーニング Marketplace パートナー サポート ブログ その他

無料アカウント

Microsoft はお客様の仲間です。COVID-19 の対応に役立つ、Azure のリソースとツールを詳しくご確認ください。

クラウドで開発することでコストを最適化しましょう。目的を持って創造する。

無料で始める

Azure の無料アカウントで構築を開始すると、次の内容を利用できます。

- 12 か月間の人気の無料サービス
- 25 を超える常に無料のサービス
- Azure を 30 日間探索するための ¥22,500 のクレジット

くろう道



The screenshot shows the 'くろう道' (Kouroudo) website, which is a Japanese blog focused on Microsoft Azure. The page layout includes a header with the site title and navigation links, a main content area with three featured articles, and a sidebar with a profile of the author, Ueno Takashi.

Featured Articles:

- Windows Virtual Desktop 最適化ツールを試す!**
Date: 2020/8/5 | Tags: Windows Virtual Desktop
Summary: WVD のSession Hostを軽量化する"PowerShellスクリプト"が登場したので、試してみたいと思います。通常のWin...
Link: [記事を読む](#)
- Azure モニターで WVDv2 をモニタリングしてみる!**
Date: 2020/7/20 | Tags: Azure Monitor, Windows Virtual Desktop
Summary: WVDv2にてログの出力が可能となりましたので、"Log Analytics"と"Azure Monitor"を利用してログ情報の可...
Link: [記事を読む](#)
- Citrix Managed Desktops with WVD に接続してみる!**
Date: 2020/7/15 | Tags: Citrix
Summary: 今回は、みなさんお待ちかねのデスクトップ配信を試してみたいと思います。Citrix Managed Desktops wit...
Link: [記事を読む](#)

Author Profile (Sidebar):

- 筆者: 牛上 貴司 (うしがみ たかし)**
- [@tushigamiさんをフォロー](#)
- 大阪出身 東京在住
- 日本マイクロソフト 所属
[受賞歴]
- Microsoft MVP, VMware vExpert
- 最近は、Windows Virtual Desktop 推し!
- ※発言は個人のもので誤解を恐れず
- 皆様のおかげで5万PVを達成する事ができました!
"v(^_^)=アリアガトウ=(v ^_^)v"
- ★次の目標は、1.0万PVだぁー
※前数のほど、よろしくお願ひしますm(_ _)m
- 皆様ませっせ!!
- [@03_マイクロソフトとシドリックスが語る子](#)

※くろう道の内容は牛上氏個人の見解です。

お知らせ : Citrix Future of Workにて登壇予定

CITRIX®

**Citrix Future
of Work**



 **Microsoft**

詳細は近日CitrixのWEBで公開予定

CITRIX

マイクロソフトとシトリックが語るVDIの正しい選び方

セキュリティ編

- 1 Windows Virtual Desktopに対するCitrixの価値

- 2 Citrixのみが提供するVDI環境のゼロトラストセキュリティ

- 3 Citrixが提供するセキュリティ機能の紹介及びデモ

- 4 Azure Windows Defender ATPで強化するVDIセキュリティ

- 5 まとめ

マイクロソフトとシトリックが語るVDIの正しい選び方

セキュリティ編

1 Windows Virtual Desktopに対するCitrixの価値

2 Citrixのみが提供するVDI環境のゼロトラストセキュリティ

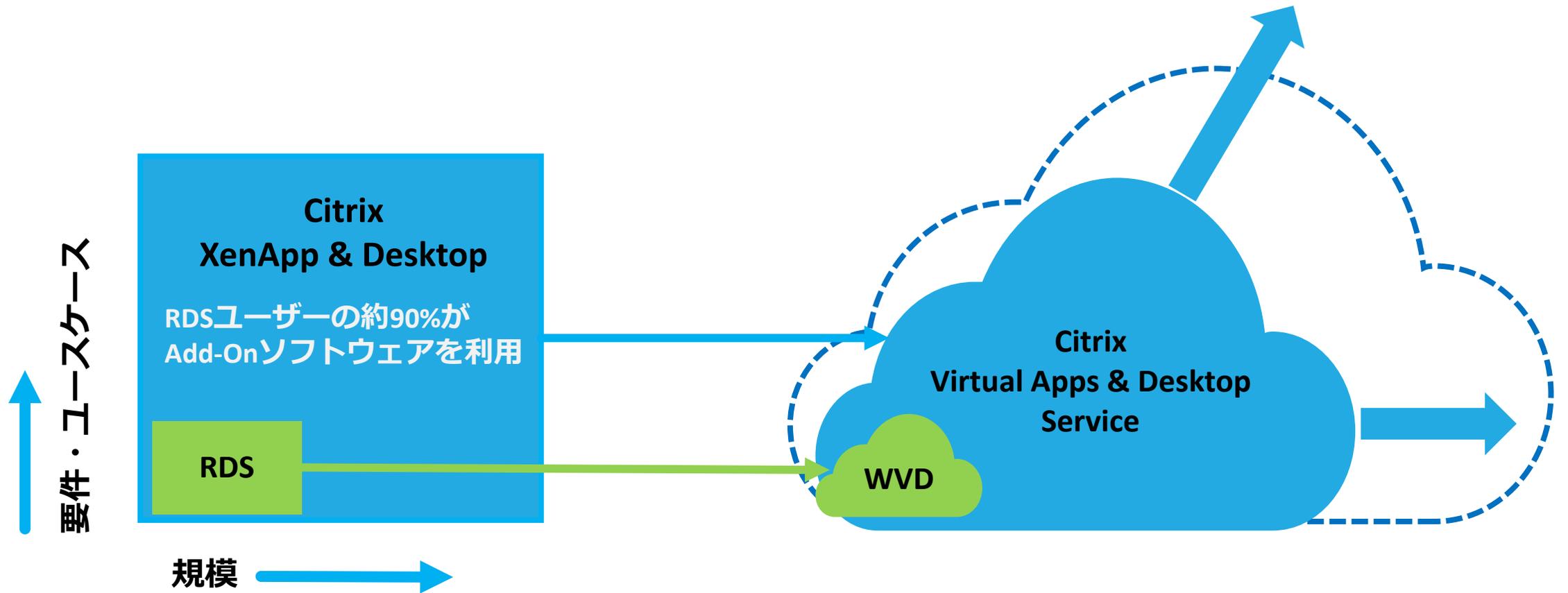
3 Citrixが提供するセキュリティ機能の紹介及びデモ

4 Azure Windows Defender ATPで強化するVDIセキュリティ

5 まとめ

Citrixが必要な理由

Citrixは常に最新・最強



進化なきVDIはVDIにあらず

セキュリティ
機能

コスト削減
機能

運用効率化
機能

生産性向上
機能

Citrix Cloud Virtual Apps and desktops



Windows Virtual Desktop

1,000を超える機能やパラメーターが追加されます

セキュリティ
機能

コスト削減
機能

運用効率化
機能

生産性向上
機能

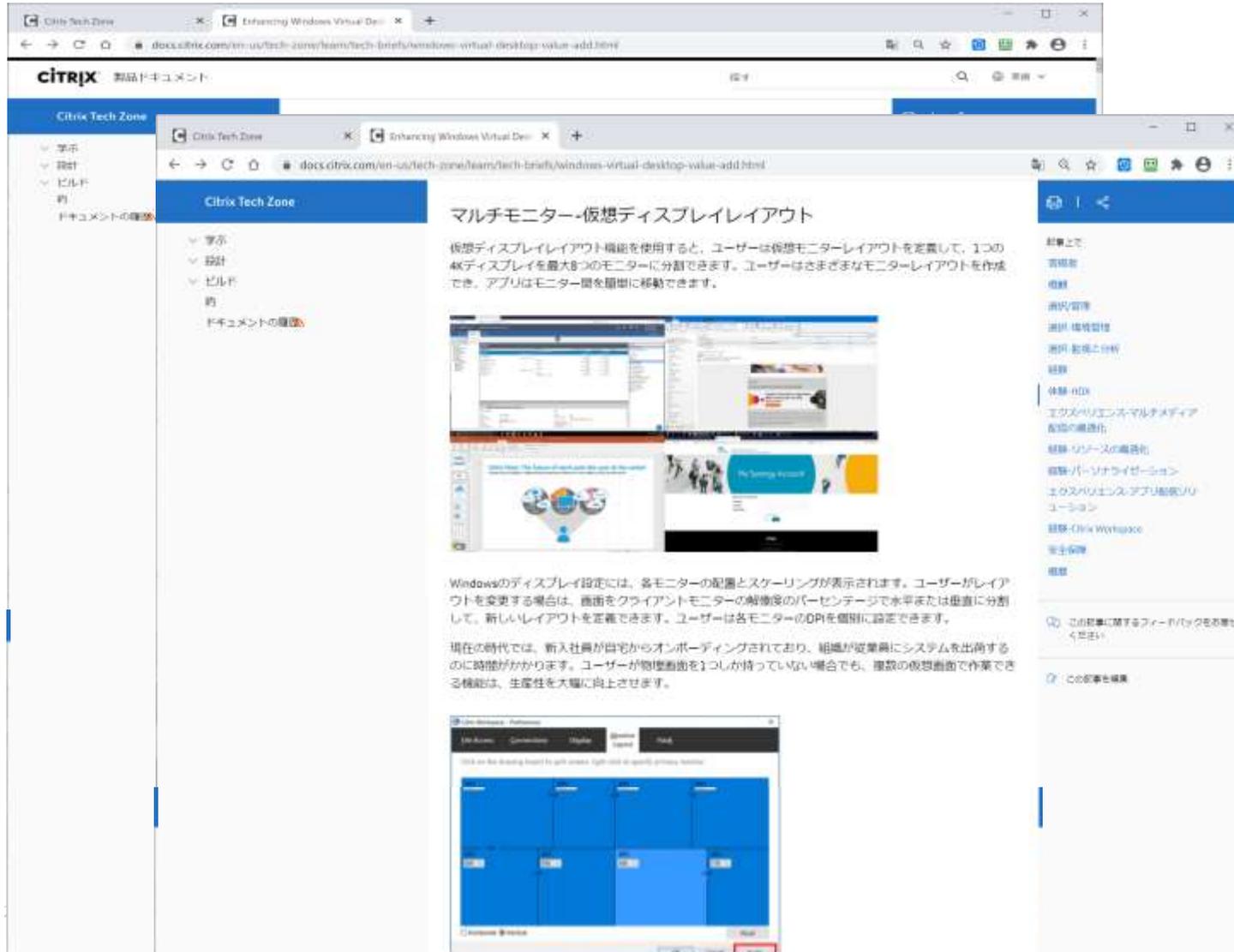
Citrixが提供する機能例

App Protection	消費帯域削減機能群	シングルマスターイメージ管理	多様なRTCサポート
セッションレコーディング& ウォーターマーク	ユーザー集約率向上機能群	ポリシー管理	HDXによるネットワークに左右 されないパフォーマンス
多様な認証のサポートとSSO	Auto Scaleによる高度な電源管理	管理委任と操作ログ	動的セキュリティポリシーによる 生産性とセキュリティの両立
Citrix ポリシー	高度な負荷分散機能	高度なモニタリング	マルチセッションにおける パーソナライズの維持
完全閉域網アクセス	Linuxのサポート	プルーブ機能による接続の事前 担保	ユーザーエクスペリエンス モニタリング



Windows Virtual Desktop

Windows Virtual Desktopの拡張



Citrix Tech Zone



<https://v.gd/vYWY8z>

マイクロソフトとシトリックが語るVDIの正しい選び方

セキュリティ編

- 1 Windows Virtual Desktopに対するCitrixの価値

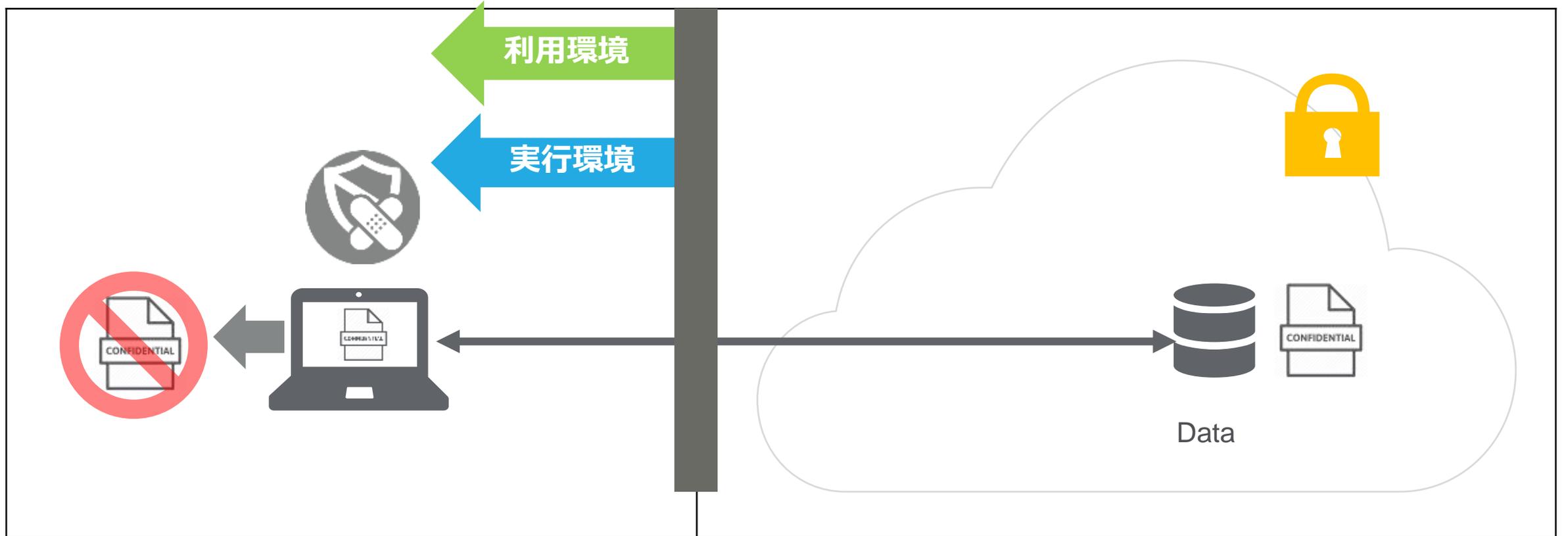
- 2 **Citrixのみが提供するVDI環境のゼロトラストセキュリティ**

- 3 Citrixが提供するセキュリティ機能の紹介及びデモ

- 4 Azure Windows Defender ATPで強化するVDIセキュリティ

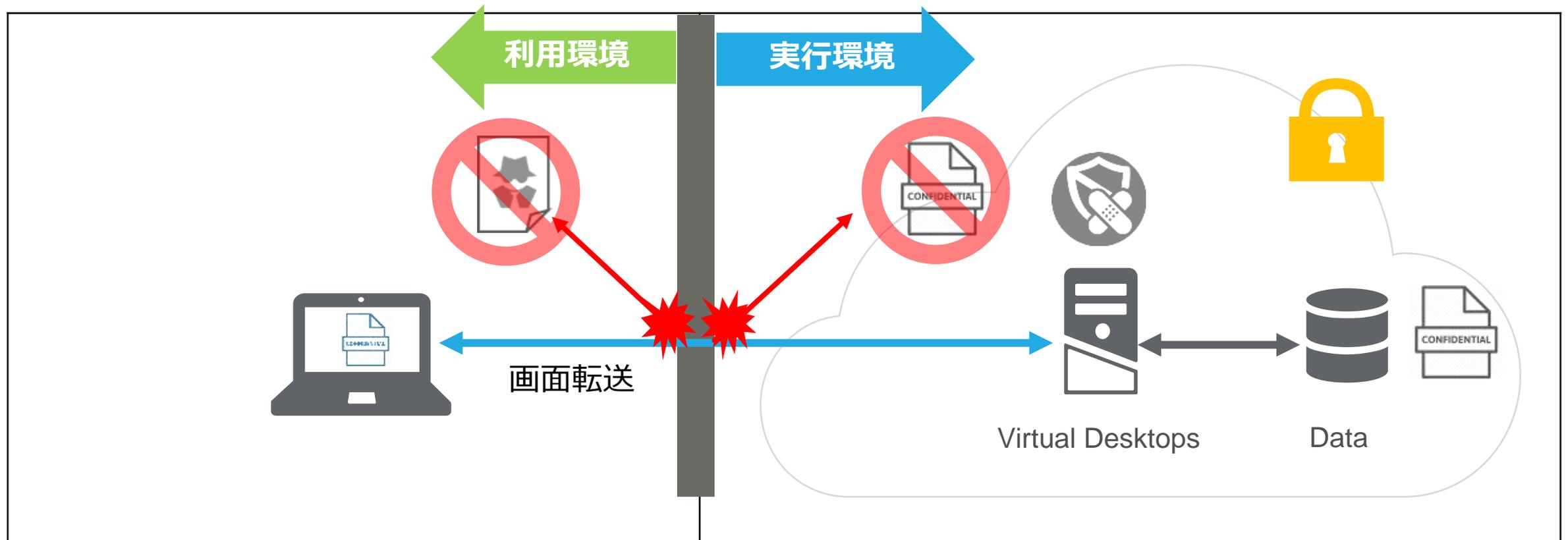
- 5 まとめ

FAT PCのセキュリティ



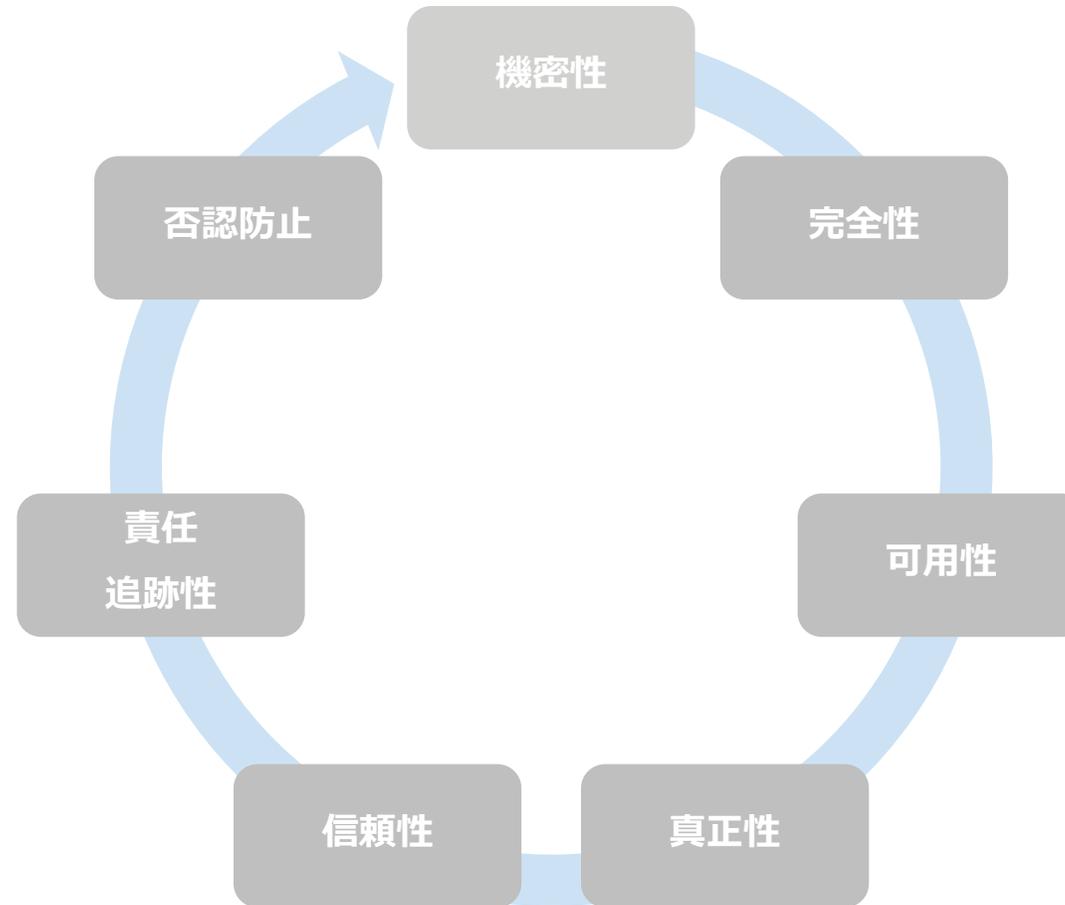
端末側でセキュリティを担保

一般的に言われているVDIのセキュリティ

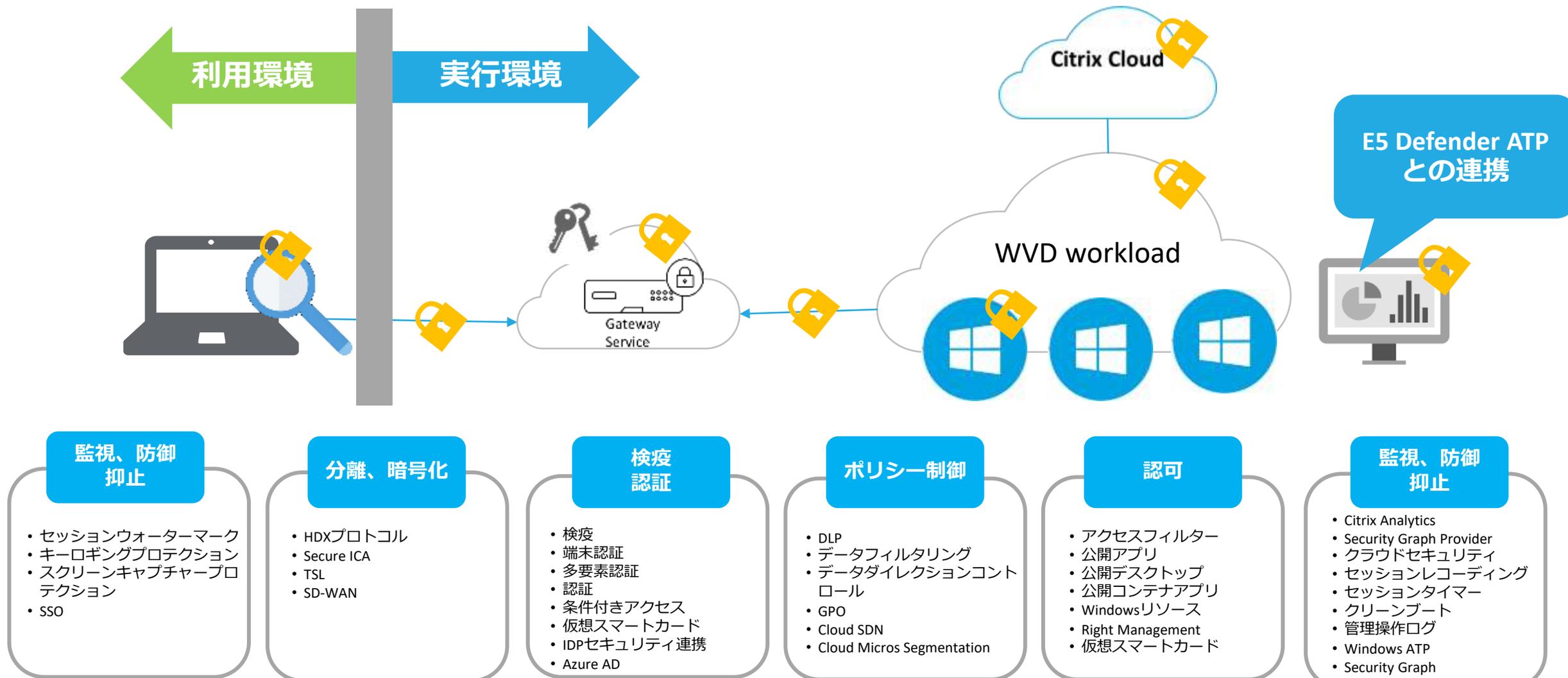


仮想化された企業端末が集中管理できることからセキュアだと言われている

ISO27001による情報セキュリティの要素



Citrixが提供するVDIゼロトラストセキュリティ



監視、防御 抑止

- セッションウォーターマーク
- キーロギングプロテクション
- スクリーンキャプチャプロテクション
- SSO

分離、暗号化

- HDXプロトコル
- Secure ICA
- TLS
- SD-WAN

検疫 認証

- 検疫
- 端末認証
- 多要素認証
- 認証
- 条件付きアクセス
- 仮想スマートカード
- IDPセキュリティ連携
- Azure AD

ポリシー制御

- DLP
- データフィルタリング
- データダイレクションコントロール
- GPO
- Cloud SDN
- Cloud Micros Segmentation

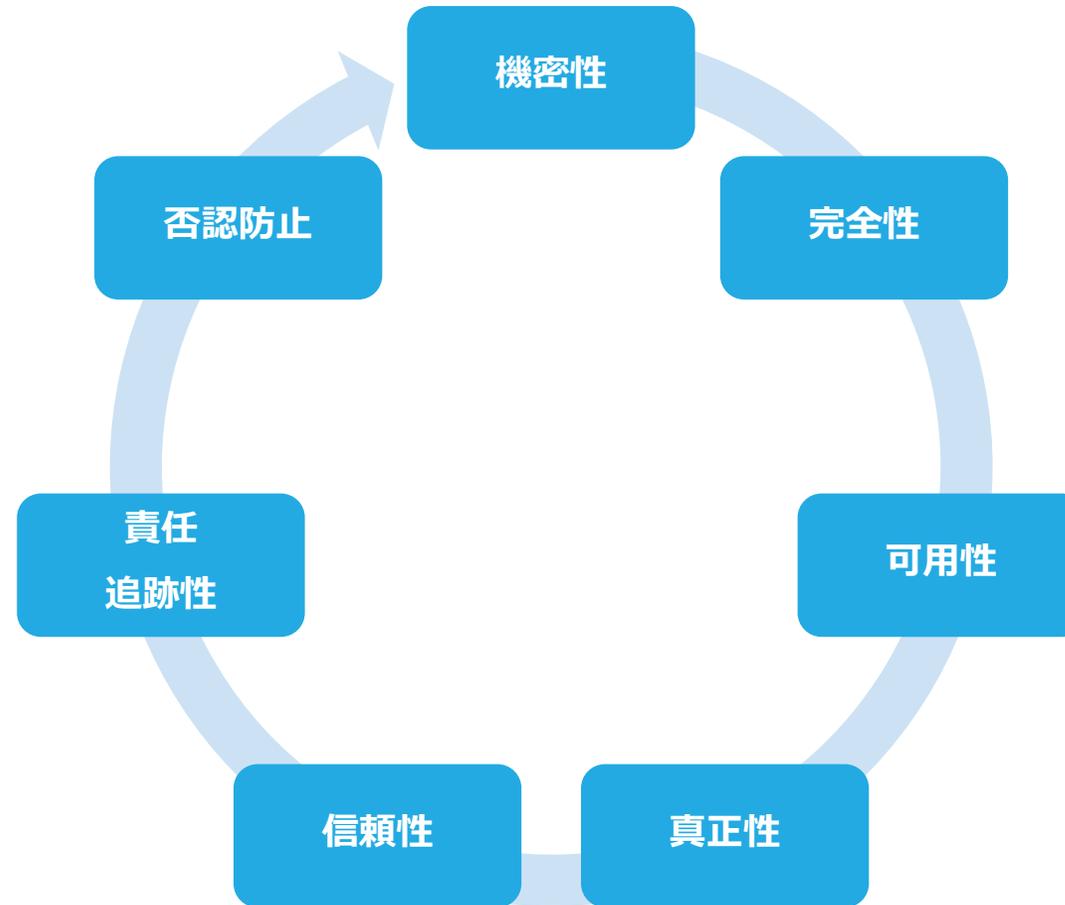
認可

- アクセスフィルター
- 公開アプリ
- 公開デスクトップ
- 公開コンテナアプリ
- Windowsリソース
- Right Management
- 仮想スマートカード

監視、防御 抑止

- Citrix Analytics
- Security Graph Provider
- クラウドセキュリティ
- セッションレコーディング
- セッションタイマー
- クリーンブート
- 管理操作ログ
- Windows ATP
- Security Graph

ISO27001の情報セキュリティの定義

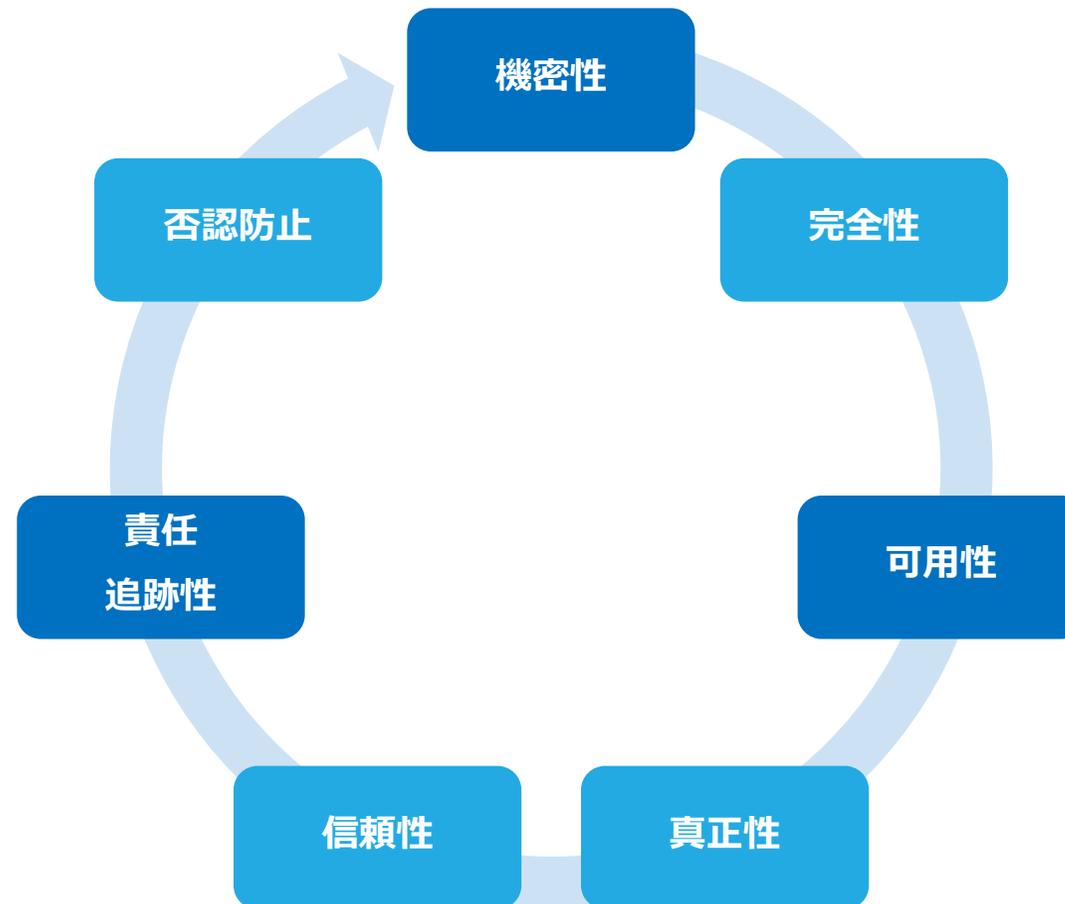


マイクロソフトとシトリックが語るVDIの正しい選び方

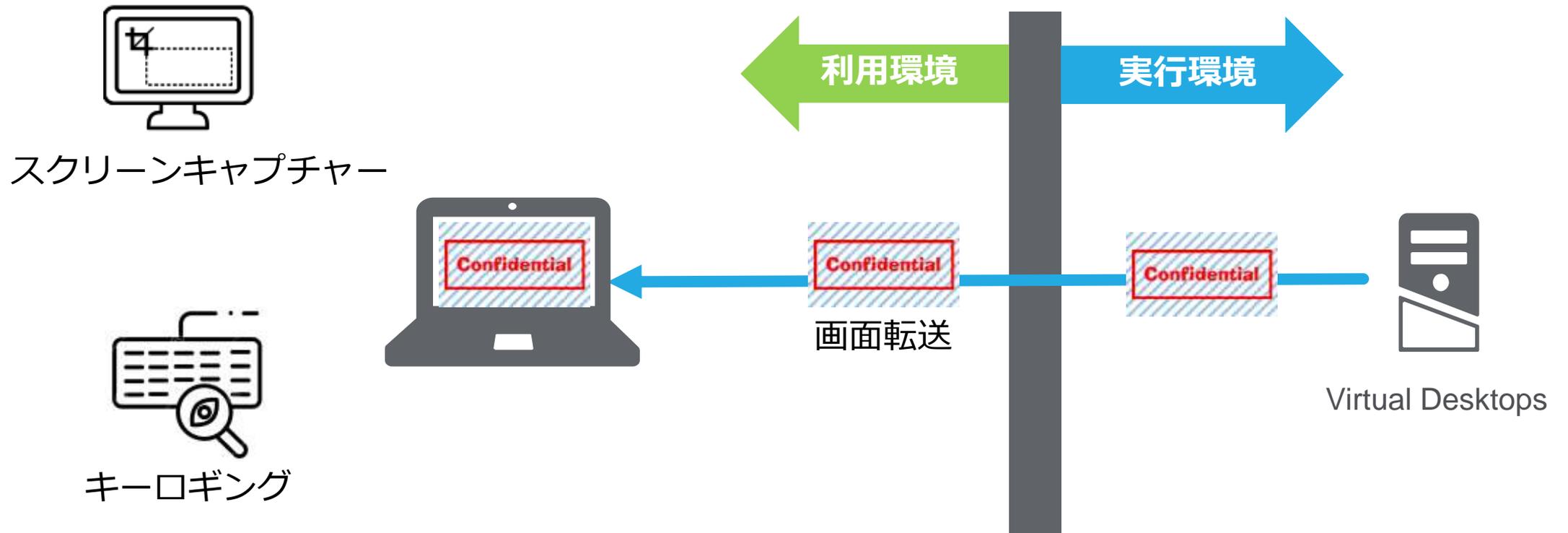
セキュリティ編

- 1 Windows Virtual Desktopに対するCitrixの価値
- 2 Citrixのみが提供するVDI環境のゼロトラストセキュリティ
- 3 Citrixが提供するセキュリティ機能の紹介及びデモ**
- 4 Azure Windows Defender ATPで強化するVDIセキュリティ
- 5 まとめ

Citrixによるデータ保護



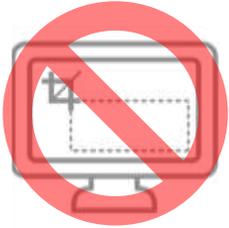
VDIでも懸念される端末からの情報漏洩





カメラ撮影による情報漏洩

スクリーンキャプチャー



携帯カメラ等による画面の撮影



キーロギング



画面転送

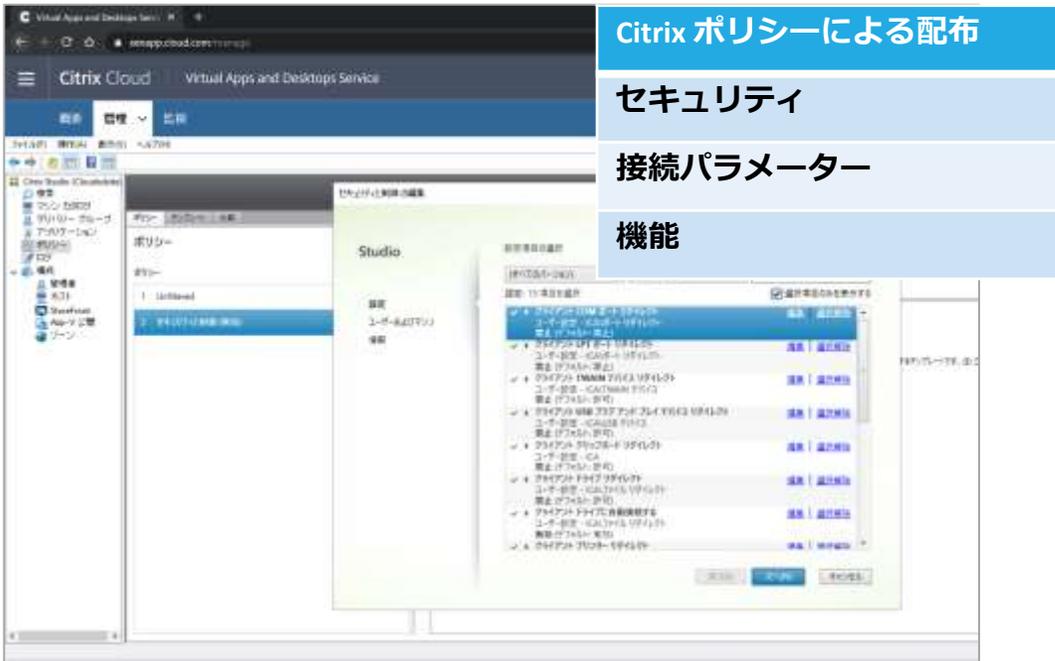


Virtual Desktops

セッションウォーターマーク



Citrix ポリシー



Citrix Cloud Virtual Apps and Desktops Service console. The 'Policies' section is active, showing a list of policies with columns for name, status, and actions. A 'Studio' window is overlaid on the right, showing the 'Policy Editor' for a selected policy, with tabs for 'General' and 'Users and Machines'.

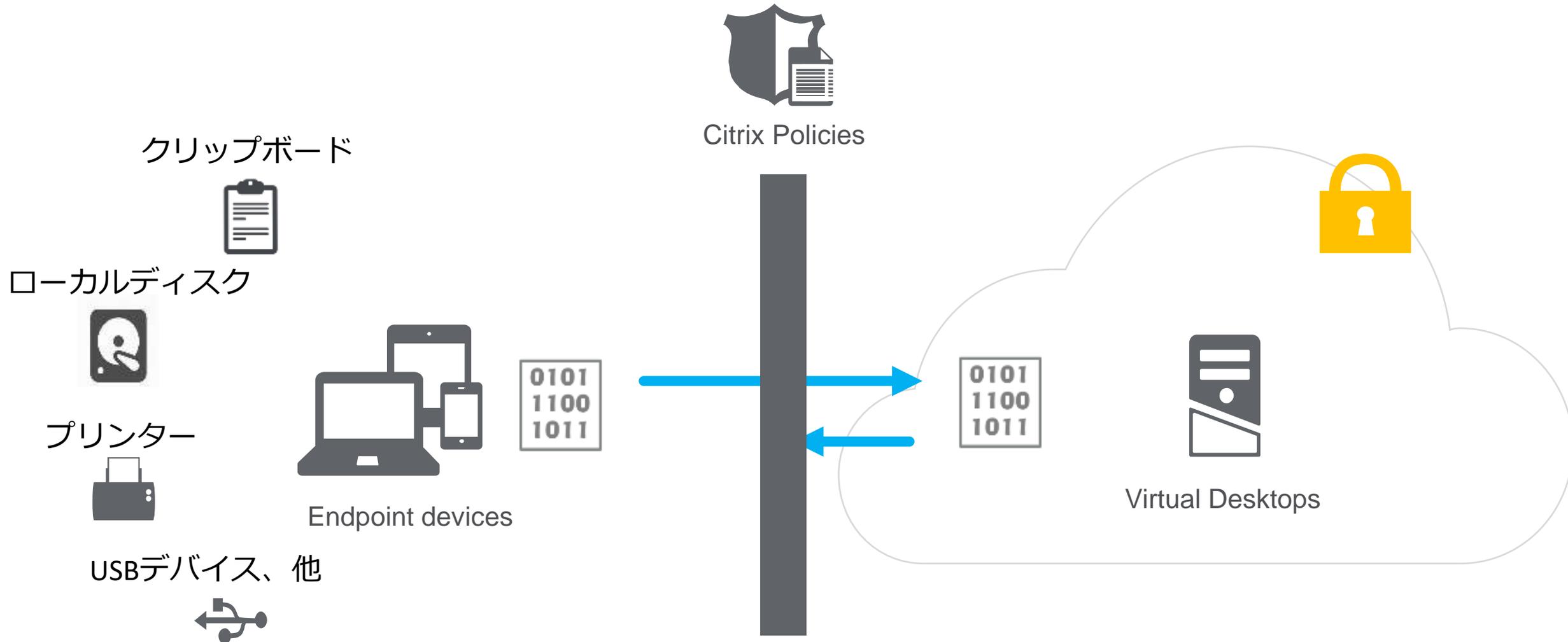
- Citrix ポリシーによる配布
- セキュリティ
- 接続パラメーター
- 機能



Citrix Studio 'Policy Editor' for 'Studio'. The 'Users and Machines' tab is selected, showing a list of conditions for user and machine objects. The 'NetScaler SD-WAN' condition is highlighted.

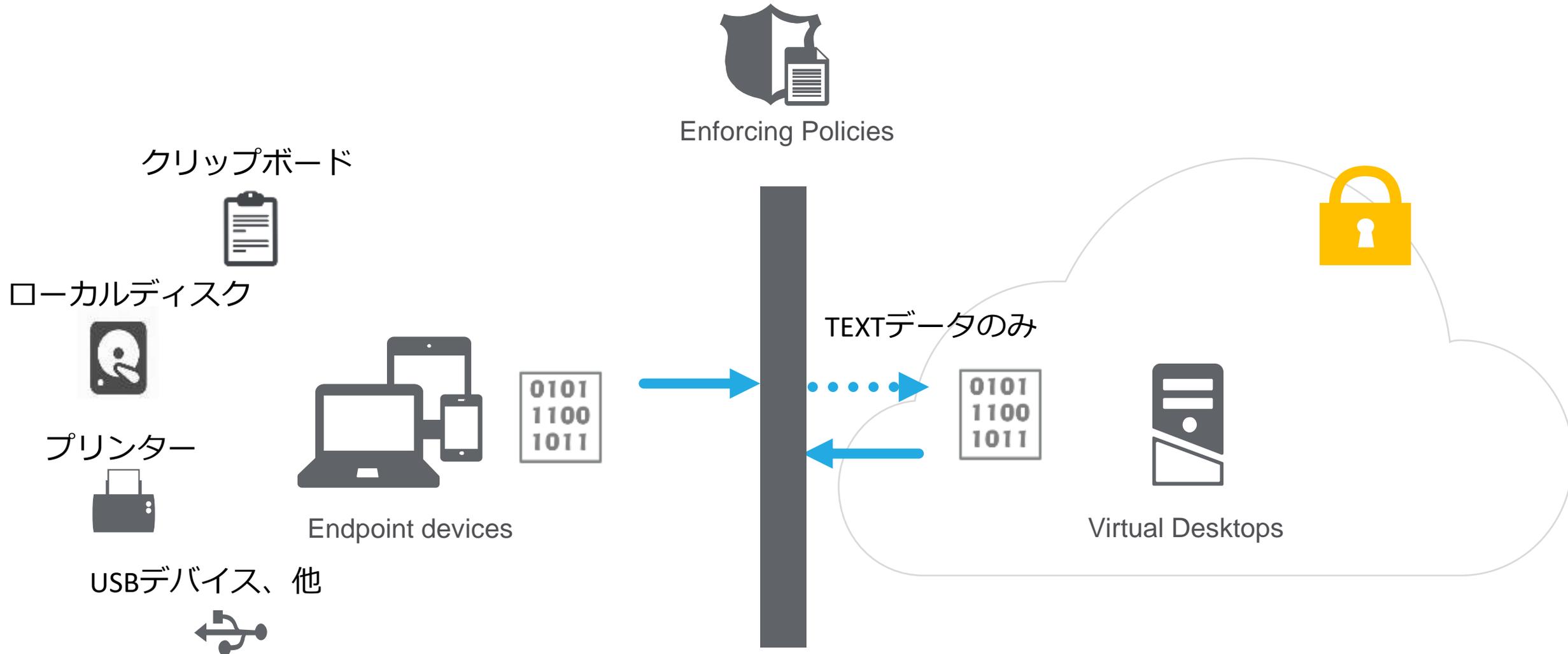
- Citrix ポリシーの適用条件
- ネットワークの種類
- ネットワーク経路
- 検疫結果による動的条件
- クライアントIPアドレス
- クライアント名
- デリバリーグループ
- デリバリーグループの種類
- ユーザーとユーザーグループ
- OU

例 データの取り込みは許可、持ち出しは禁止



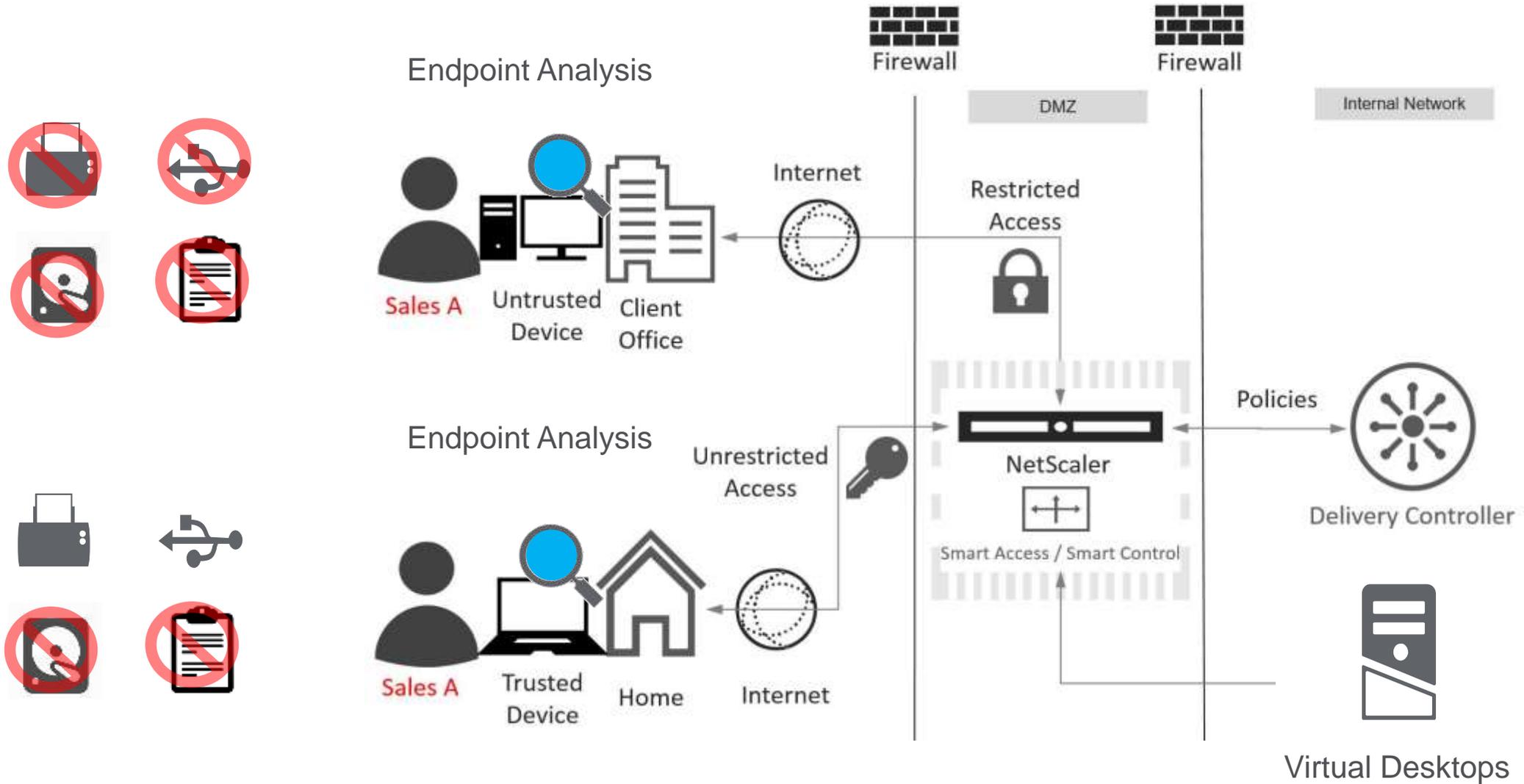


例 一部データの取り込みは許可、持ち出しは禁止





End Point Analysisとポリシーの連動によるデータ制御



Endpoint Analysisによる検疫の様子



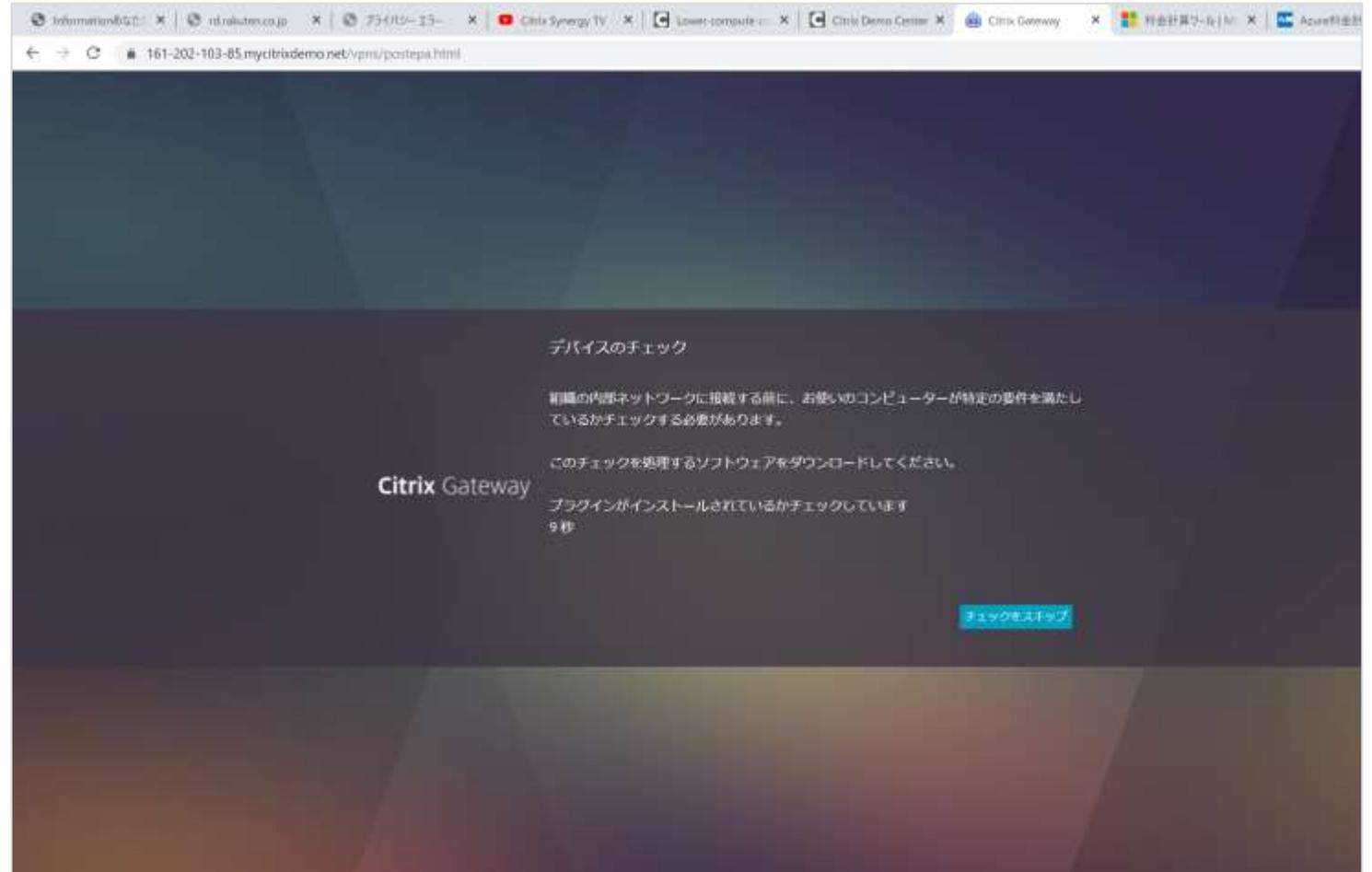
検疫内容

自宅？海外拠点？ネットカフェ

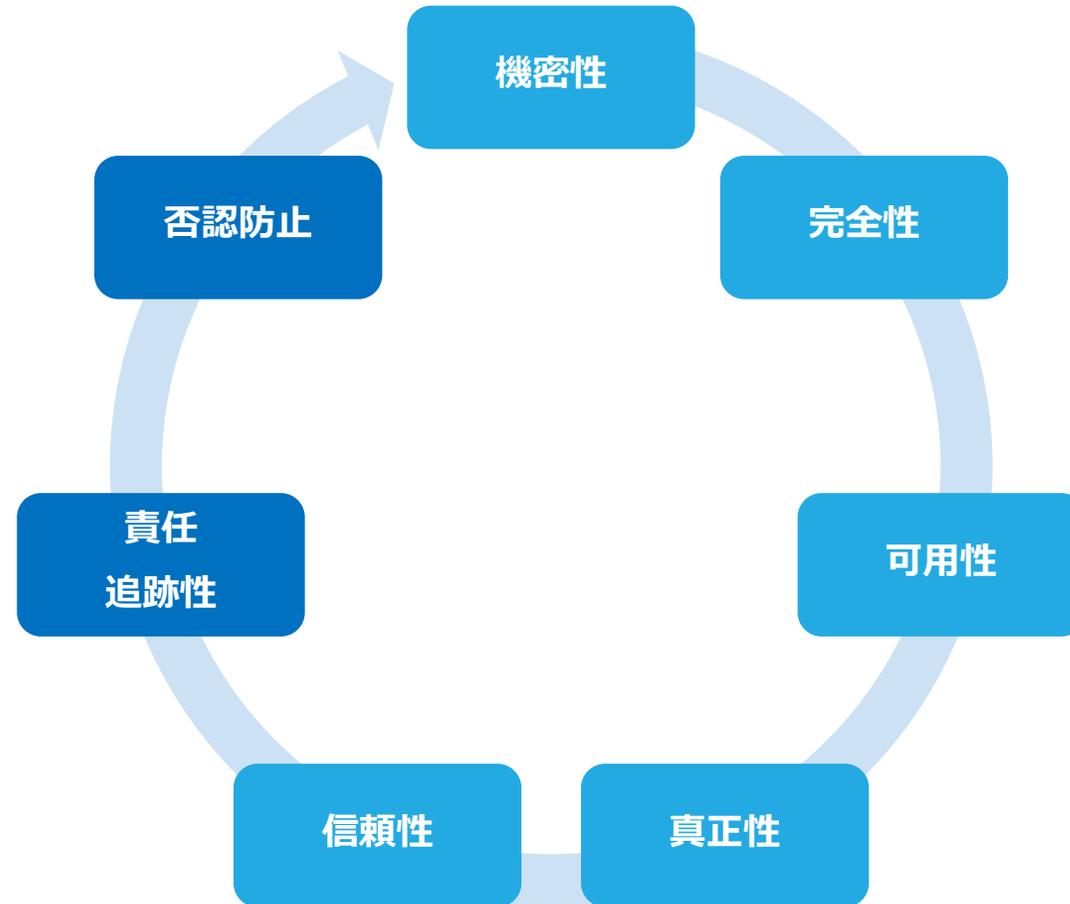
BYODデバイス？会社支給？カフェ端末？

OSのセキュリティパッチ？

暗号化ソフトの有無、動作中？



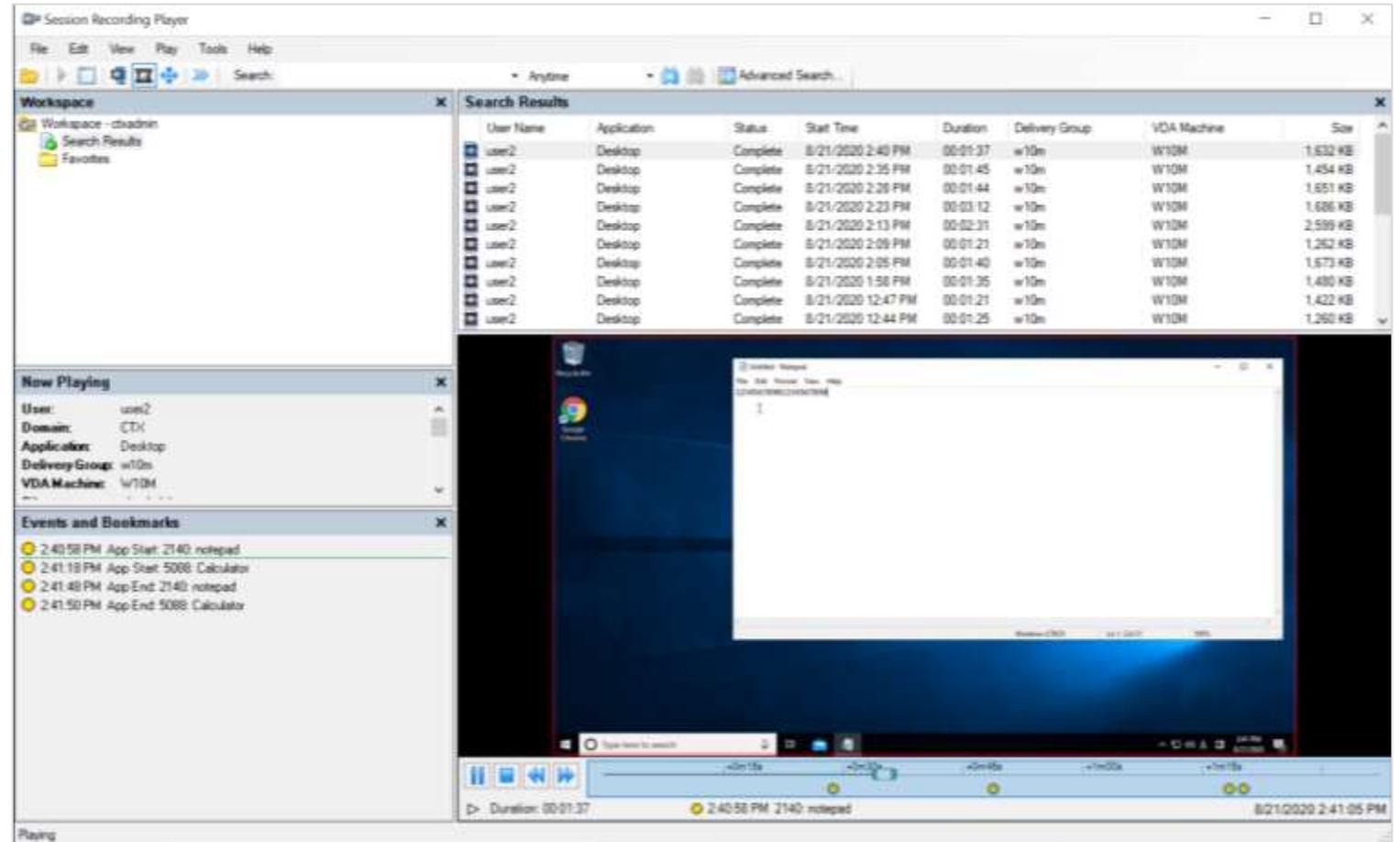
VDIテレワークを行う上で考慮すべきセキュリティ



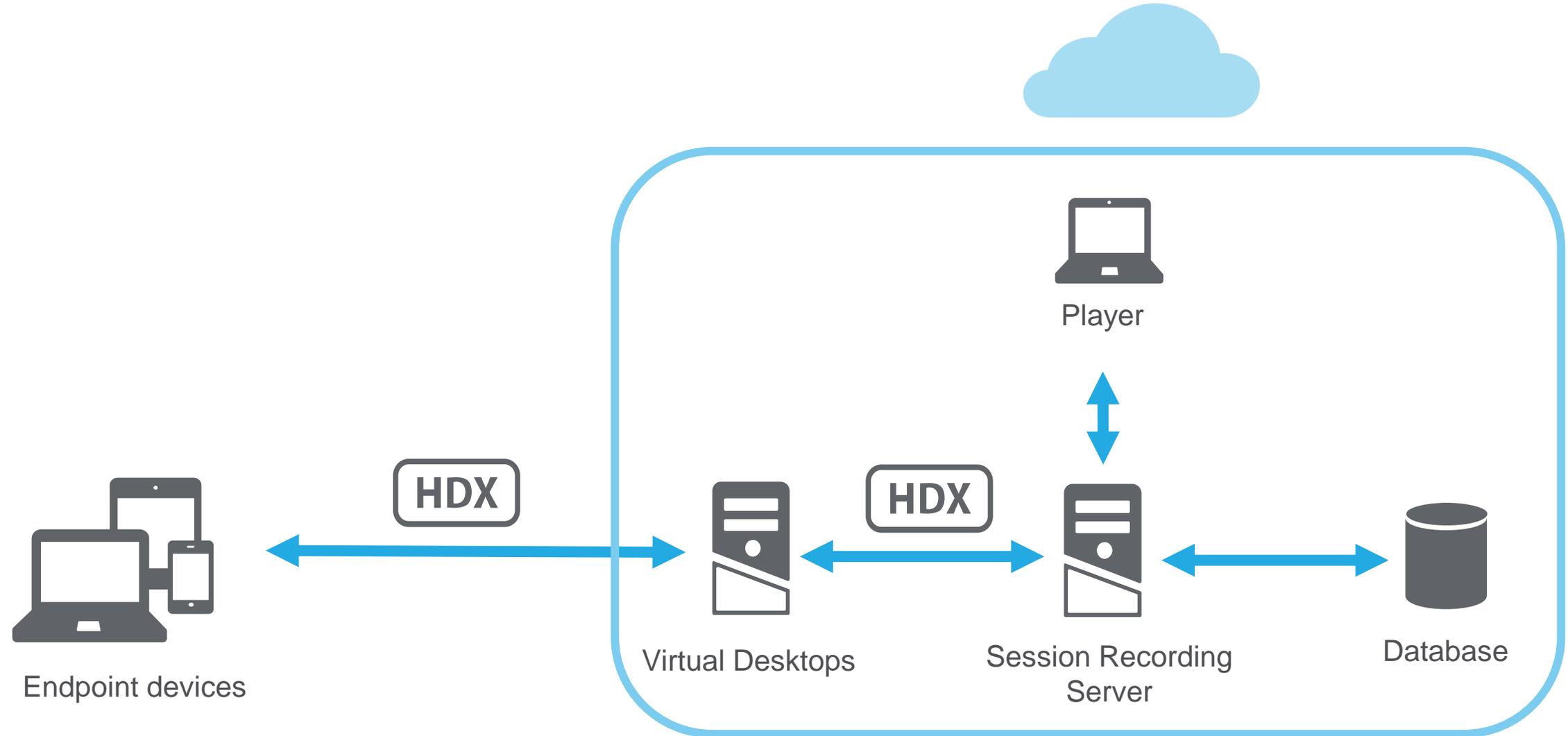
セッションレコーディング機能

抑止力の強化

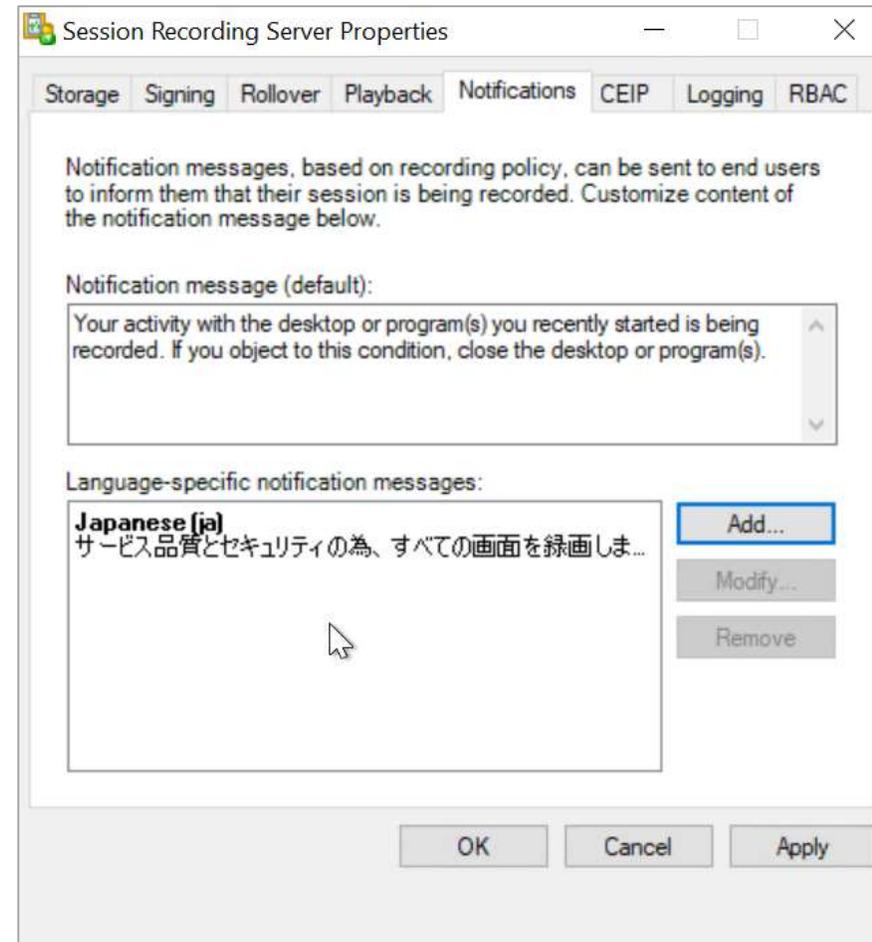
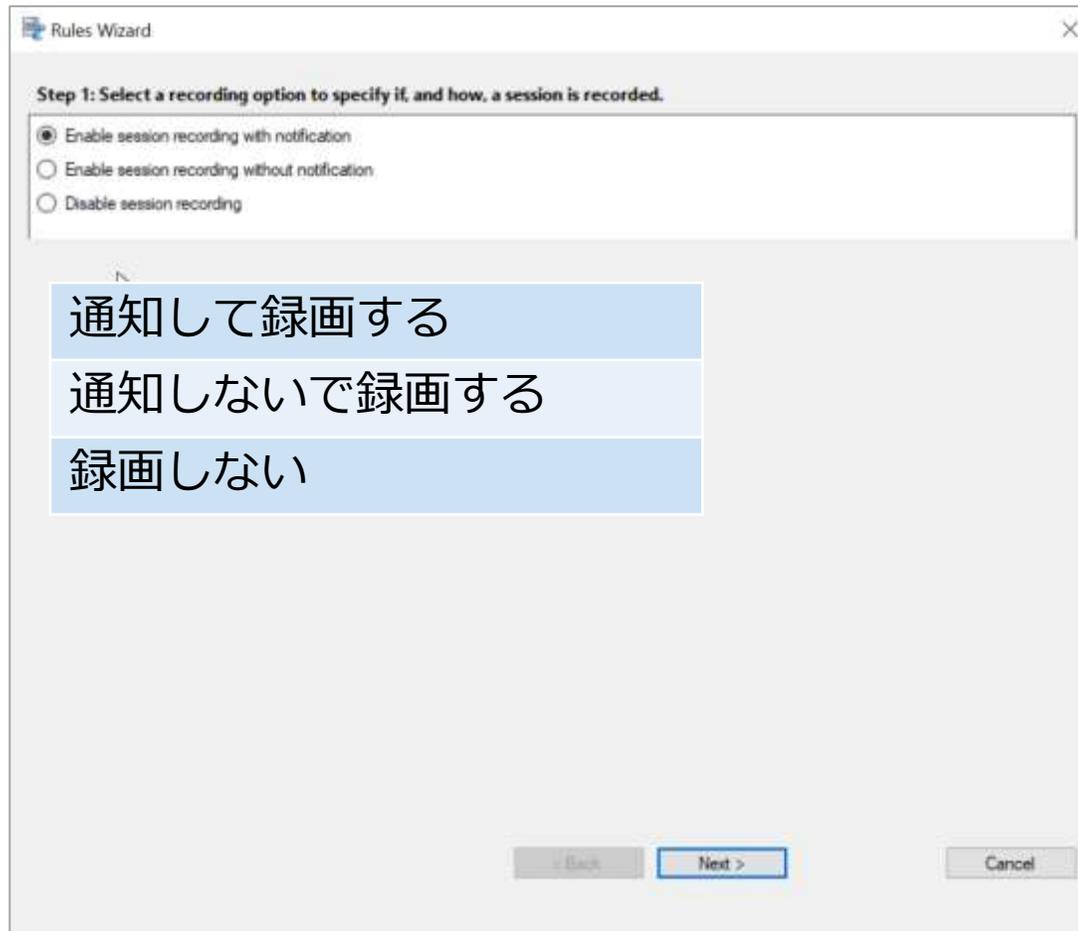
サポータビリティの向上



セッションレコーディング



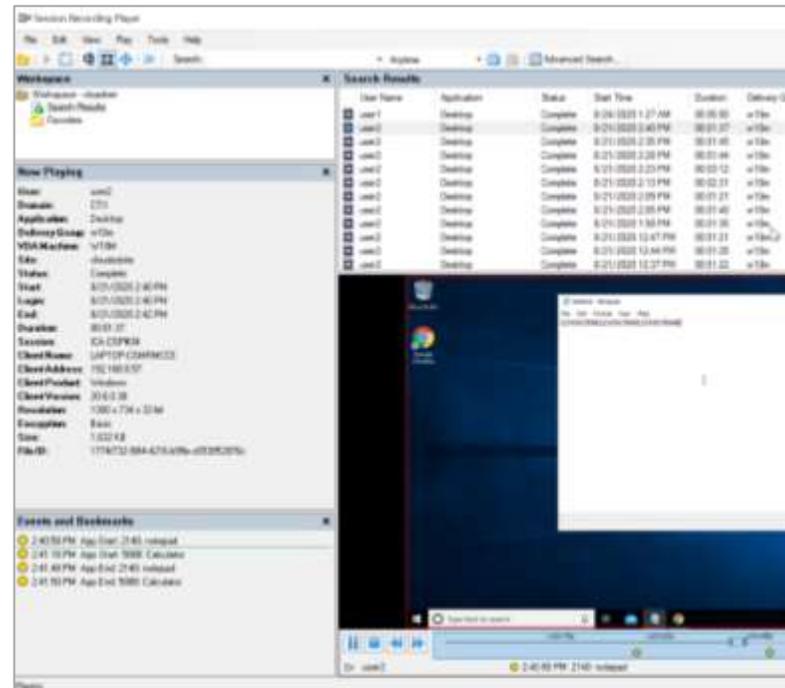
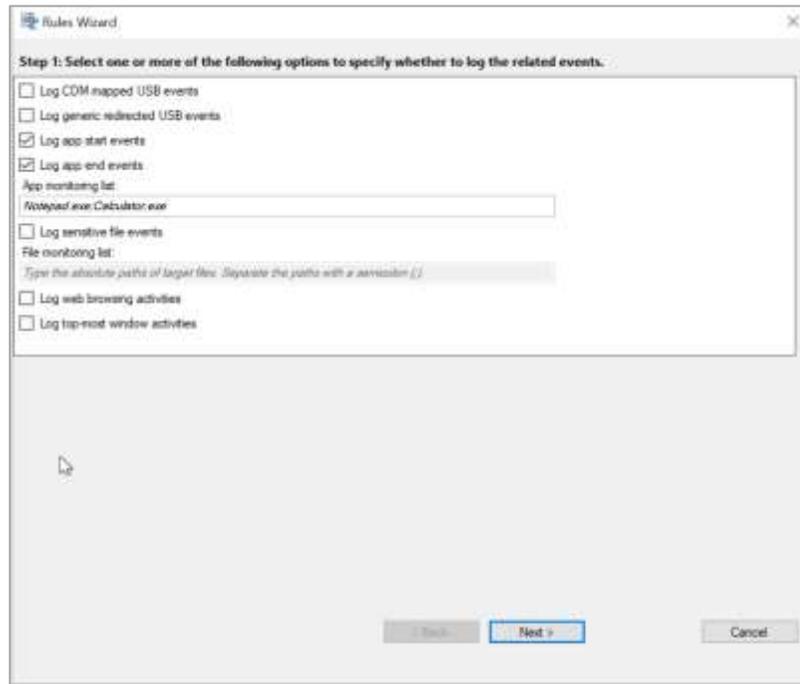
録画と事前録画通知の設定



通知メッセージのカスタマイズも可能

イベントログ

動画ファイルの中にイベントとブックマークを記録



USBドライブの認識

USBデバイスの認識

特定アプリの開始

特定アプリの終了

特定ファイルへのアクセス

Webブラウジングの開始

Webブラウジングの終了



セッションレコーディング構成変更ログ

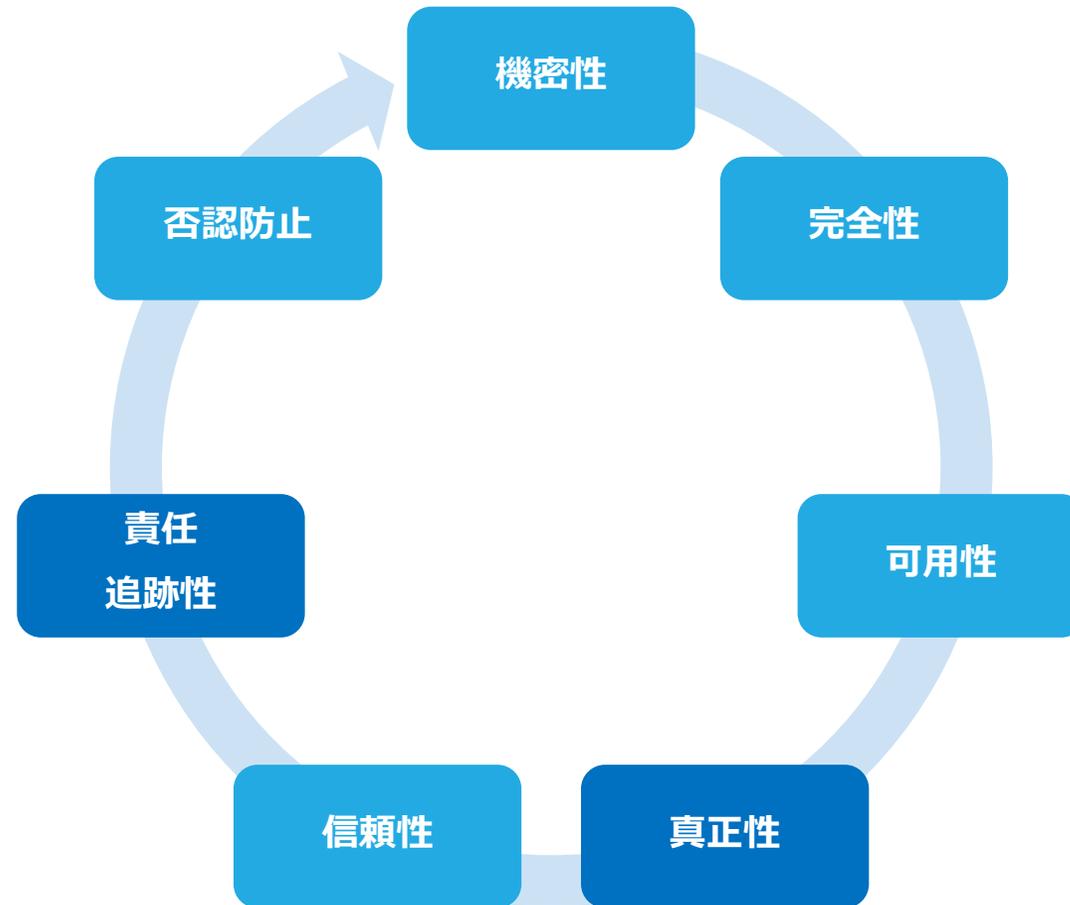
セッションレコーディング構成変更ログ

ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
177	8/24/2020 11:55 PM	Policy Document Change	Session Recording Policy Console	Action = SetPolicyConsoleConfigur... DiffFile	CTXAdmin	Yes
178	8/24/2020 3:02 AM	Policy Document Change	Session Recording Policy Console	Action = SetPolicyConsoleConfigur... DiffFile	CTXAdmin	Yes
179	8/24/2020 3:01 AM	Policy Document Change	Session Recording Policy Console	Action = SetPolicyConsoleConfigur... DiffFile	CTXAdmin	Yes
174	8/24/2020 3:08 AM	Recording File Play Back	Session Recording Player	Action = Session File Download...	CTXAdmin	Yes
173	8/24/2020 3:01 AM	Recording File Play Back	Session Recording Player	Action = Session File Download...	CTXAdmin	Yes
172	8/24/2020 2:57 AM	Recording File Play Back	Session Recording Player	Action = Session File Download...	CTXAdmin	Yes
171	8/24/2020 2:52 AM	Recording File Play Back	Session Recording Player	Action = Session File Download...	CTXAdmin	Yes
170	8/24/2020 2:42 PM	Recording File Play Back	Session Recording Player	Action = Session File Download...	CTXAdmin	Yes
168	8/24/2020 2:48 PM	Policy Document Change	Session Recording Policy Console	Action = SetActivePolicyDocument...	CTXAdmin	Yes

セッションレコーディングログ

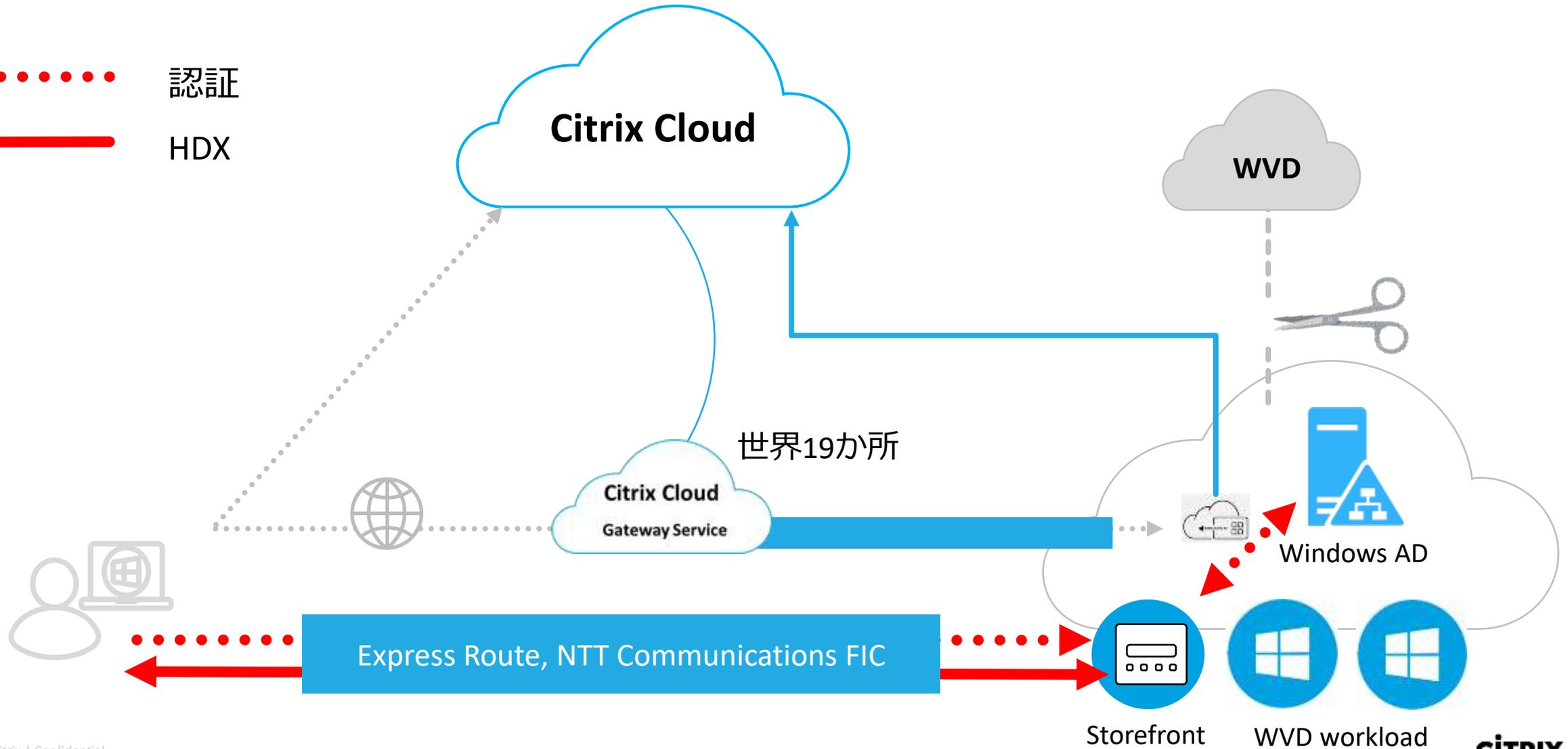
ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
47	8/24/2020 2:02 AM	Record Reason	Session Recording Agent	Application = CitrixOnlineDesktop... URL = https://www.citrix.com/... Reason = (27)(1441)	CTXUser1	Yes
46	8/24/2020 2:00 AM	Record Reason	Session Recording Agent	Application = CitrixOnlineDesktop... URL = https://www.citrix.com/... Reason = (27)(1441)	CTXUser1	Yes
45	8/24/2020 2:00 AM	Record Reason	Session Recording Agent	Application = CitrixOnlineDesktop... URL = https://www.citrix.com/... Reason = (27)(1441)	CTXUser1	Yes
44	8/24/2020 2:45 AM	Record Reason	Session Recording Agent	Application = CitrixOnlineDesktop... URL = https://www.citrix.com/... Reason = (27)(1441)	CTXUser1	Yes

VDIテレワークを行う上で考慮すべきセキュリティ



完全閉域網

- 認証
- HDX



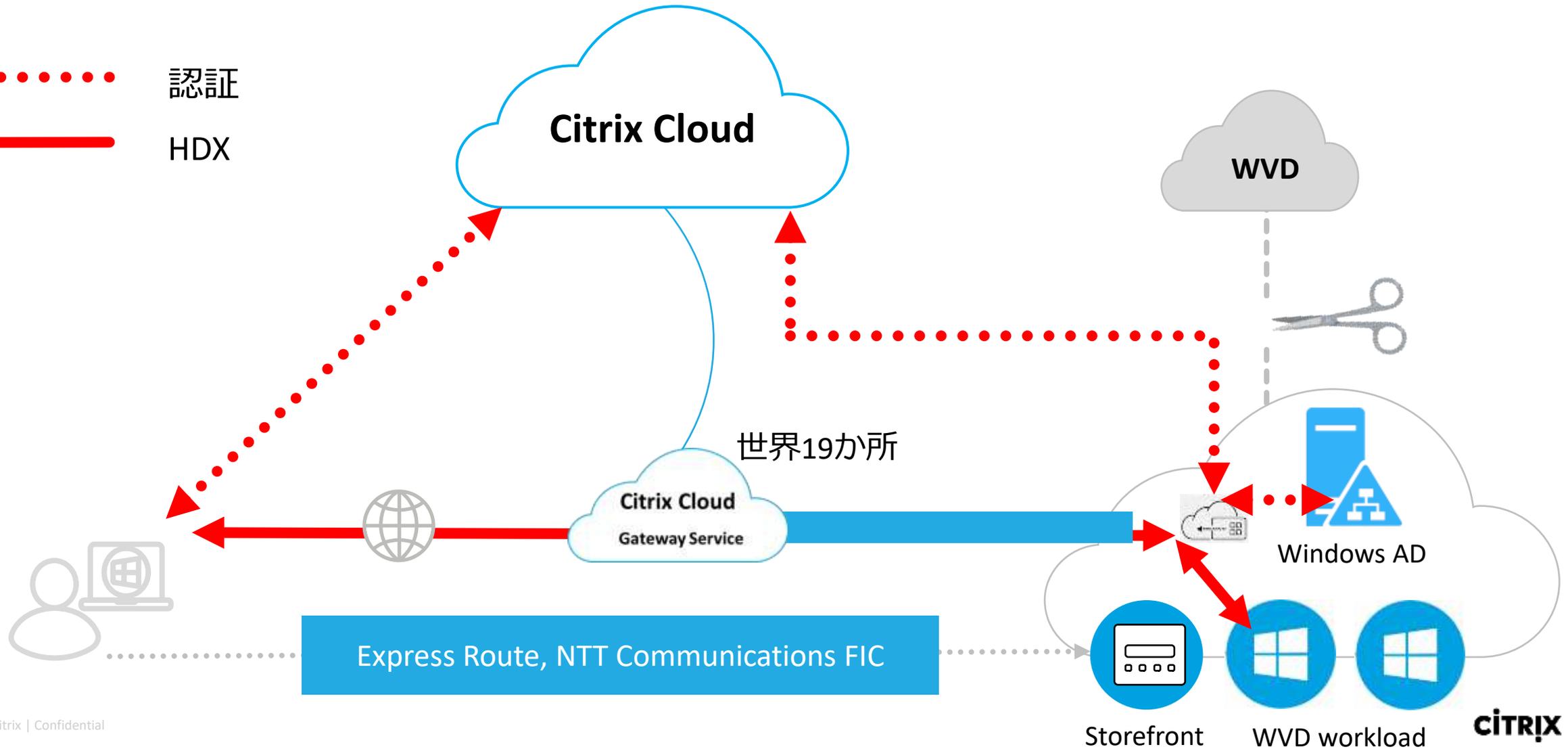
インターネット直接アクセス



認証



HDX



Citrix Cloudが対応する多様な認証

対象	認証プロバイダー
 <p>Users</p>	<ul style="list-style-type: none">• Active Directory• Azure Active Directory• Okta• Google• On-Premises Gateway as an IdP,• Federated Authentication Service (FAS)• Active Directory + 無償ワンタイムパスワード• BYO SAML• RADIUS
 <p>Admin</p>	<ul style="list-style-type: none">• Citrix Identity + OTP• Azure Active Directory Support

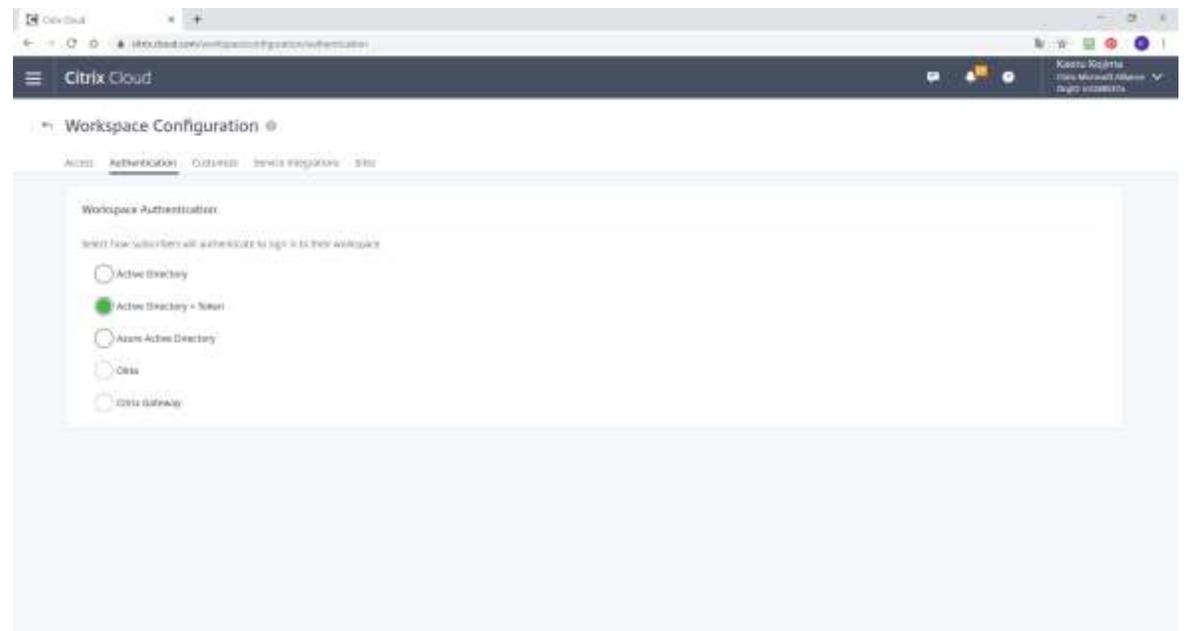
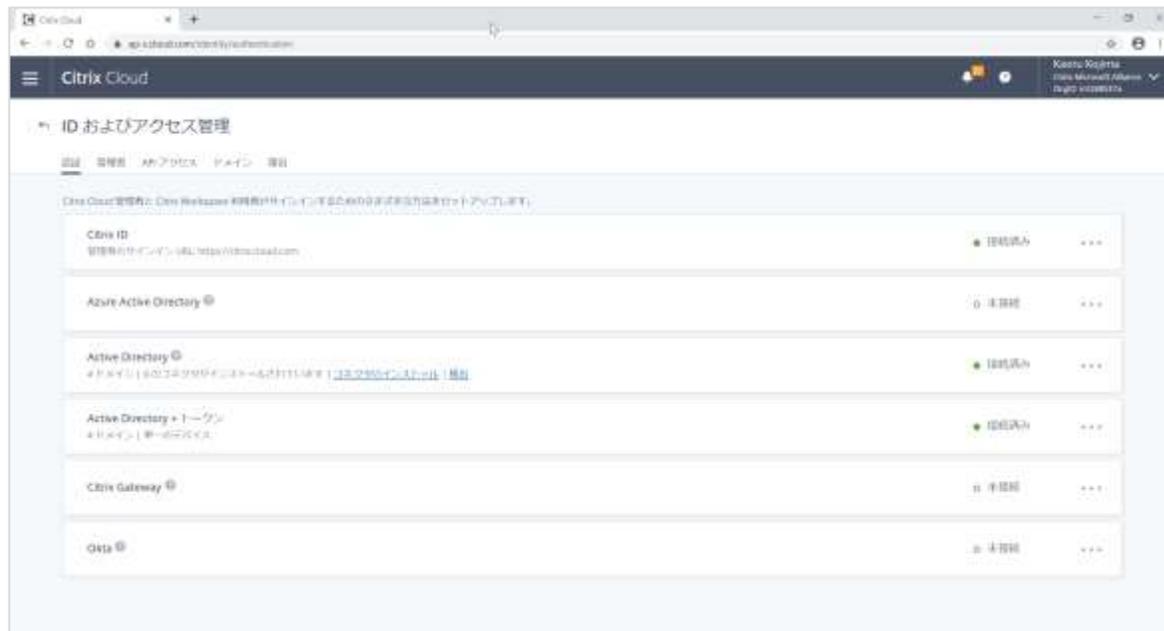


Azure Active Directory

okta



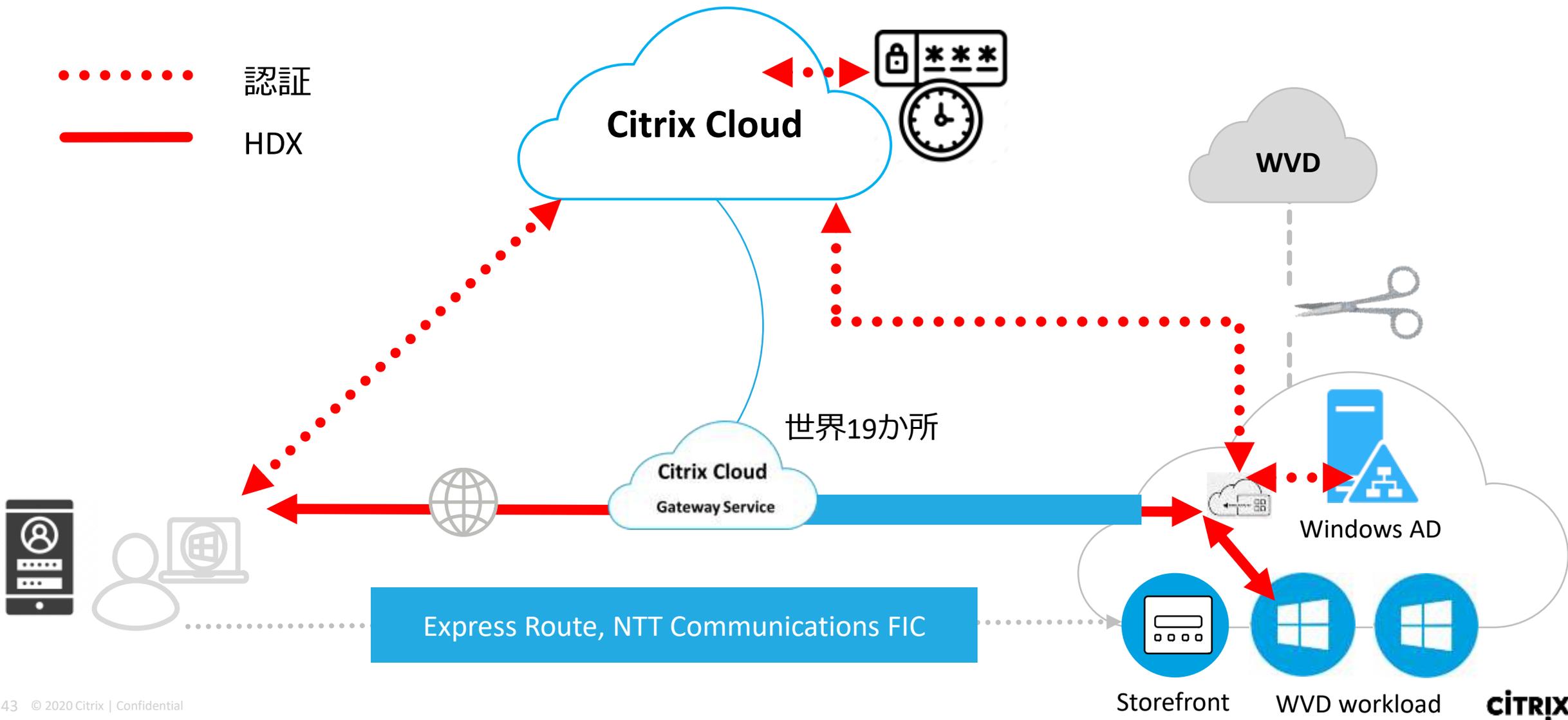
設定



Citrixの無償のワンタームパスワード

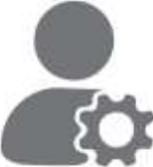
..... 認証

———— HDX





Citrix Cloudが対応する多様な認証

対象	認証プロバイダー
 <p>Users</p>	<ul style="list-style-type: none">• Active Directory• Azure Active Directory• Okta• Google• On-Premises Gateway as an IdP,• Federated Authentication Service (FAS)• Active Directory + 無償ワンタイムパスワード• BYO SAML• RADIUS
 <p>Admin</p>	<ul style="list-style-type: none">• Citrix Identity + OTP• Azure Active Directory Support



Azure Active Directory

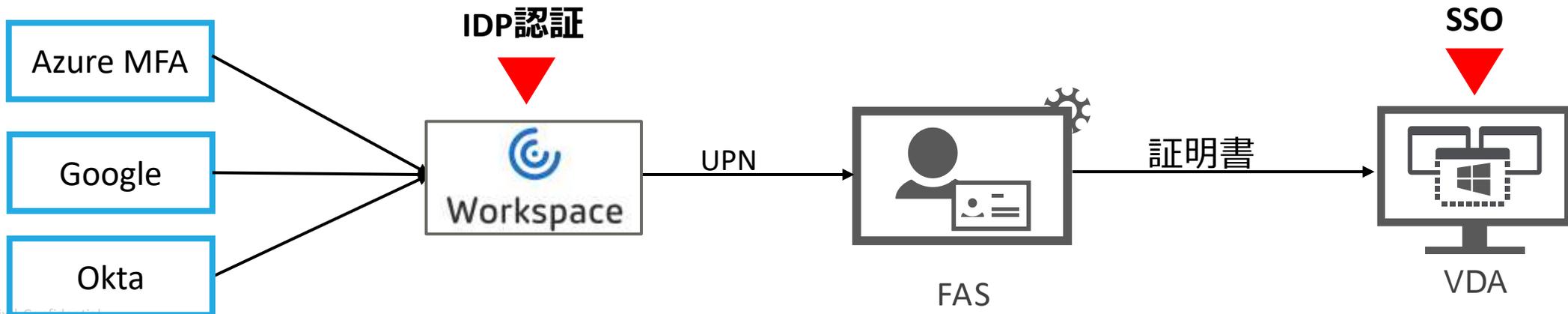
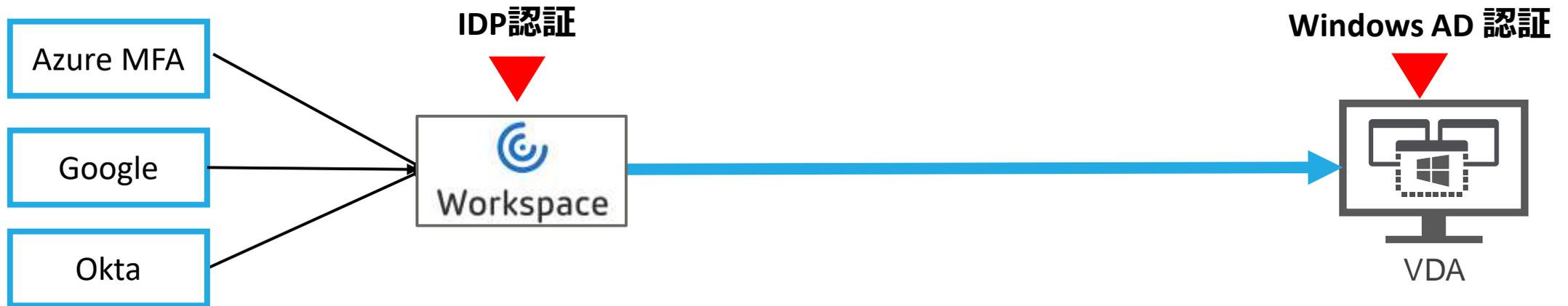
okta



WindowsマシンへのSSO

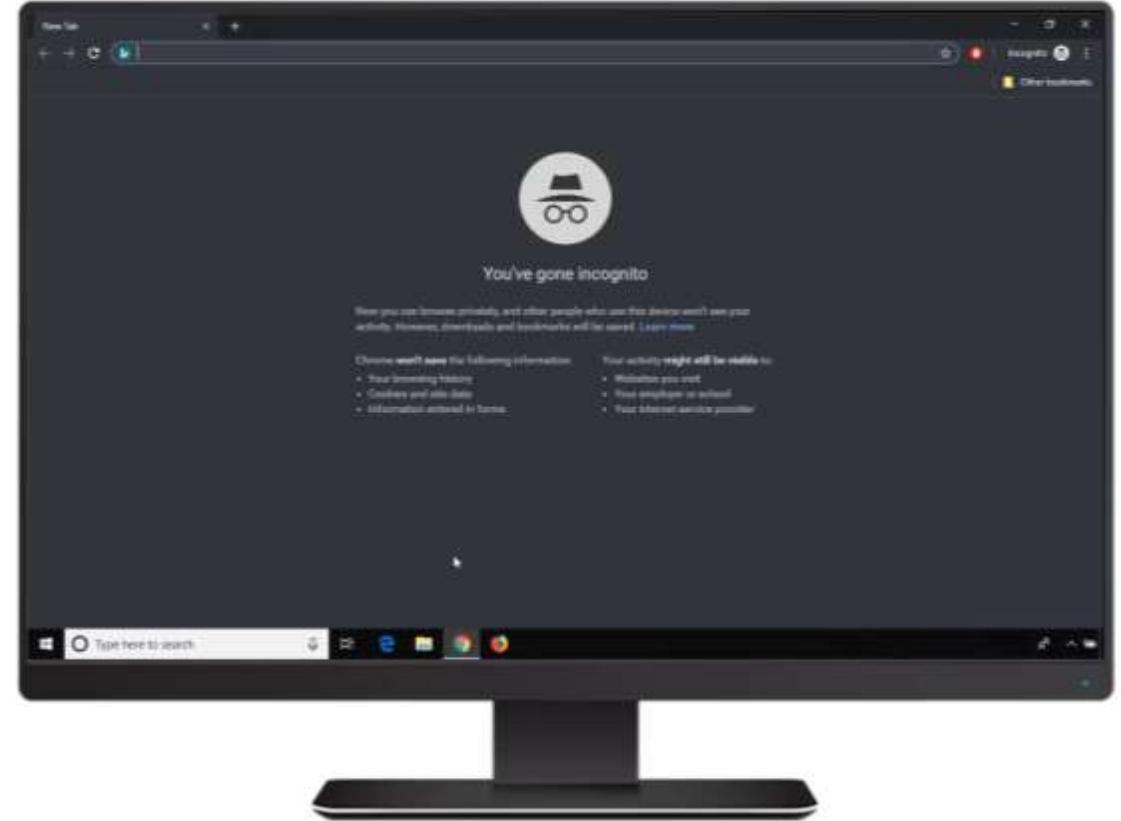
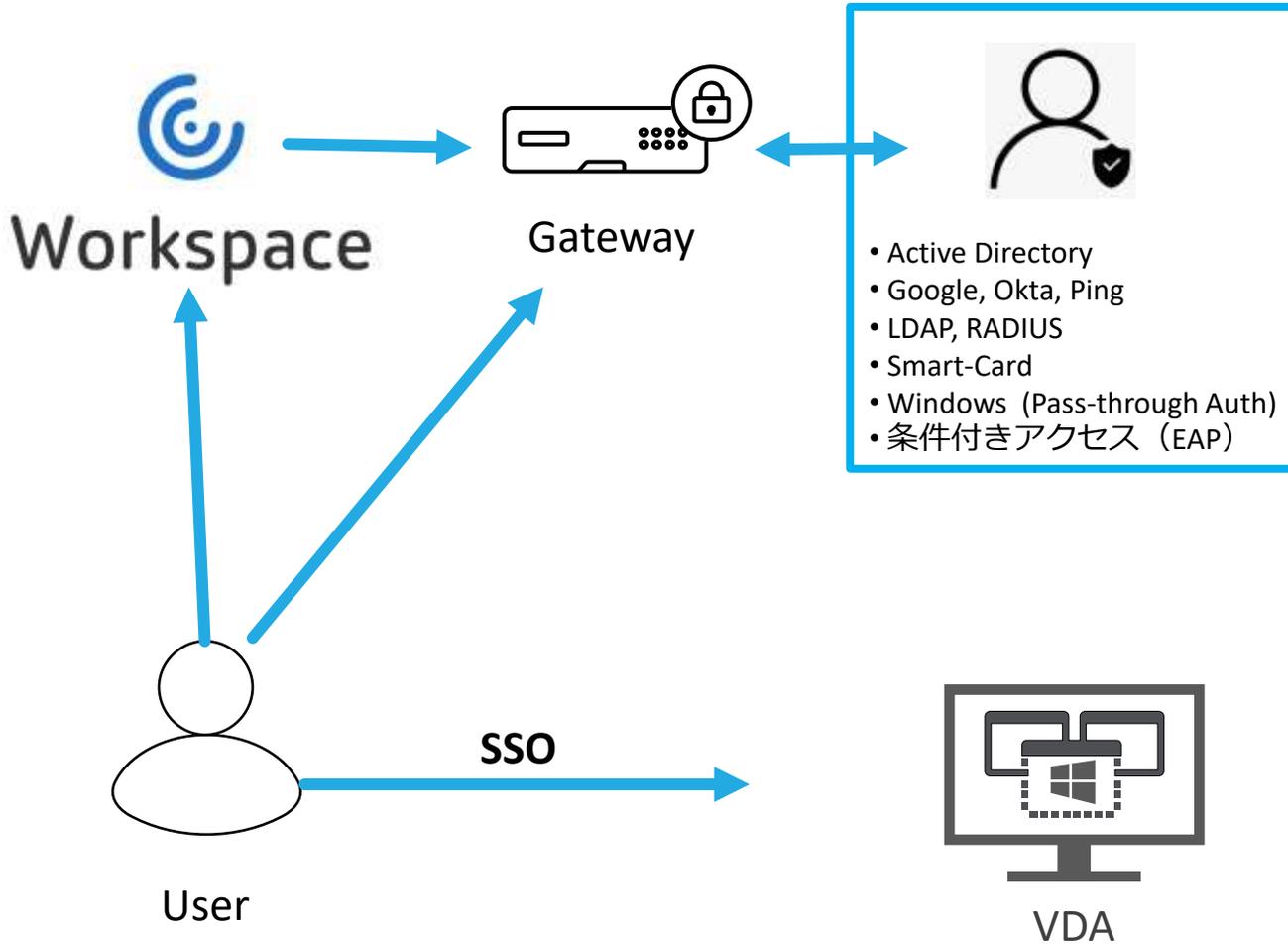
1回目

2回目





AAAとしてのGatewayの活用



マイクロソフトとシトリックが語るVDIの正しい選び方

セキュリティ編

- | | | |
|---|--|-----|
| 1 | Windows Virtual Desktopに対するCitrixの価値 | 5分 |
| 2 | Citrixのみが提供するVDI環境のゼロトラストセキュリティ | 5分 |
| 3 | Citrixが提供するセキュリティ機能の紹介及びデモ | 20分 |
| 4 | Azure Windows Defender ATPで強化するVDIセキュリティ | 7分 |
| 5 | まとめ | 3分 |



Microsoft Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams. Invisible to users.

Microsoft Defender ATP とは？

EDR* と呼ばれるジャンルのセキュリティ

現在 Defender ATP はセキュリティ統合プラットフォームとして発展。EDR は多くの機能のうちの一つに。

*EDR : Endpoint Detection and Response
以下の 4 機能を備えたソリューション

- ① セキュリティ インシデントの検出
- ② セキュリティ インシデントの調査
- ③ インシデントを封じ込め
- ④ エンドポイントを修復

ウイルス対策ソフトが侵入防御が前提であるのに対し、EDR は侵入されたときの対処を前提に考えられています。EDR はウイルス対策ソフトと組み合わせて使用します。

Defender ってウイルス対策じゃないの？

以前は Defender はウイルス対策を目的とした製品でしたが、現在ではセキュリティ製品のシリーズ名になっています。

Defender シリーズ例：

- Windows Defender ウイルス対策 (従来のウイルス対策)
- Windows Defender ファイアウォール (パーソナルファイアウォール)
- Windows Defender SmartScreen (危険な Web サイトからの保護)
- Windows Defender Device Guard (標的型攻撃からのデバイス保護)
- Windows Defender Credential Guard (標的型攻撃からの資格情報保護)
- Windows Defender Application Guard (仮想ブラウザ)
- Microsoft Defender ATP (EDR をはじめとしたセキュリティ統合監視・管理)

Defender シリーズを組み合わせてセキュリティを統合管理が可能

ウイルス対策



Windows Defender
ウイルス対策

EDR + セキュリティ管理

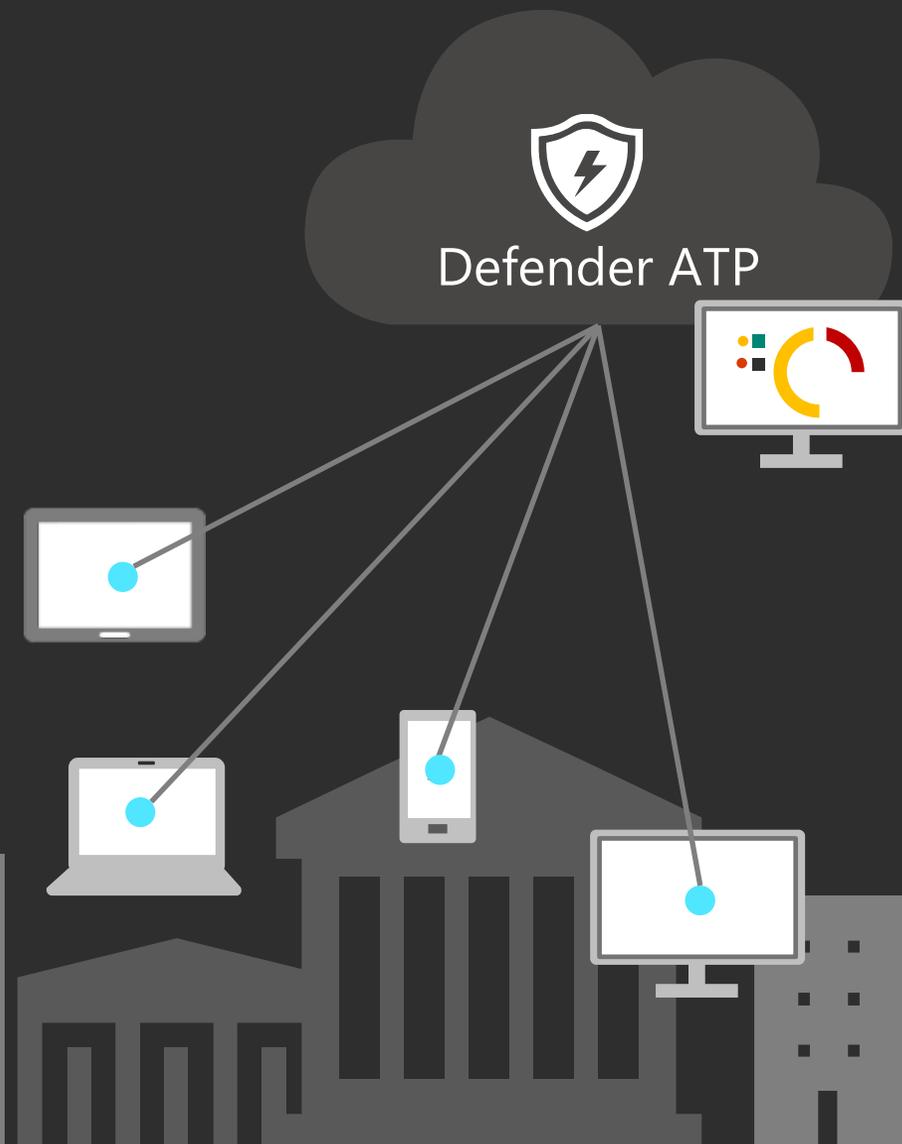


Microsoft Defender
ATP

Microsoft Defender ATP とは？

予防的な保護、ふるまい検知、自動化された調査と対応を含む
クラウドベースのエンドポイントセキュリティ統合プラットフォーム サービス

- 追加ライセンスで有効化。インフラ構築不要で即使用可能
- 場所を選ばず 24 時間 365 日 PC を監視・保護
- 脅威の可視化と自動調査・対応によるオペレーション補助





Microsoft Defender ATP の特徴

Windows に標準組み込み

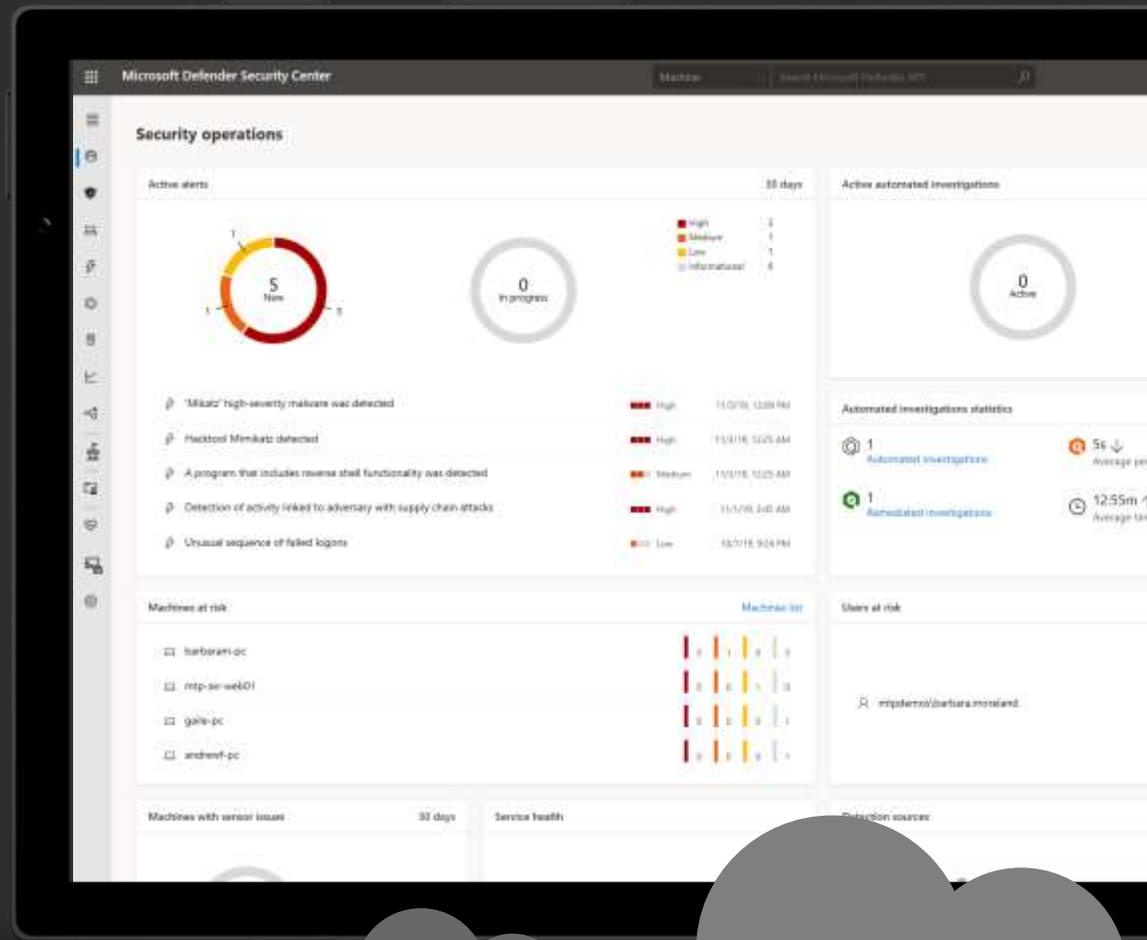
OS に組み込まれた挙動センサーによって、セキュリティ イベントやエンドポイントの挙動をログに詳しく記録。エージェントの展開・管理も不要で、非常に高度なパフォーマンス基準に対応。

クラウド ベースのセキュリティ分析サービス

Microsoft の広範なデータをエンドポイントから収集したデータと組み合わせることで、異常な挙動や攻撃者の手法を検出し既知の攻撃との類似点を特定。攻撃の痕跡 (IOA)、挙動分析、機械学習のルールを組み合わせ利用。

Microsoft とコミュニティの脅威インテリジェンス

脅威の検出をする Microsoft の専門部隊がデータを継続的に調査し、新しい挙動パターンを特定して、収集したデータを過去の攻撃やセキュリティ コミュニティから収集した既存の侵入の痕跡 (IOC) と関連付け。





Microsoft Defender ATP の最小要件

ライセンス

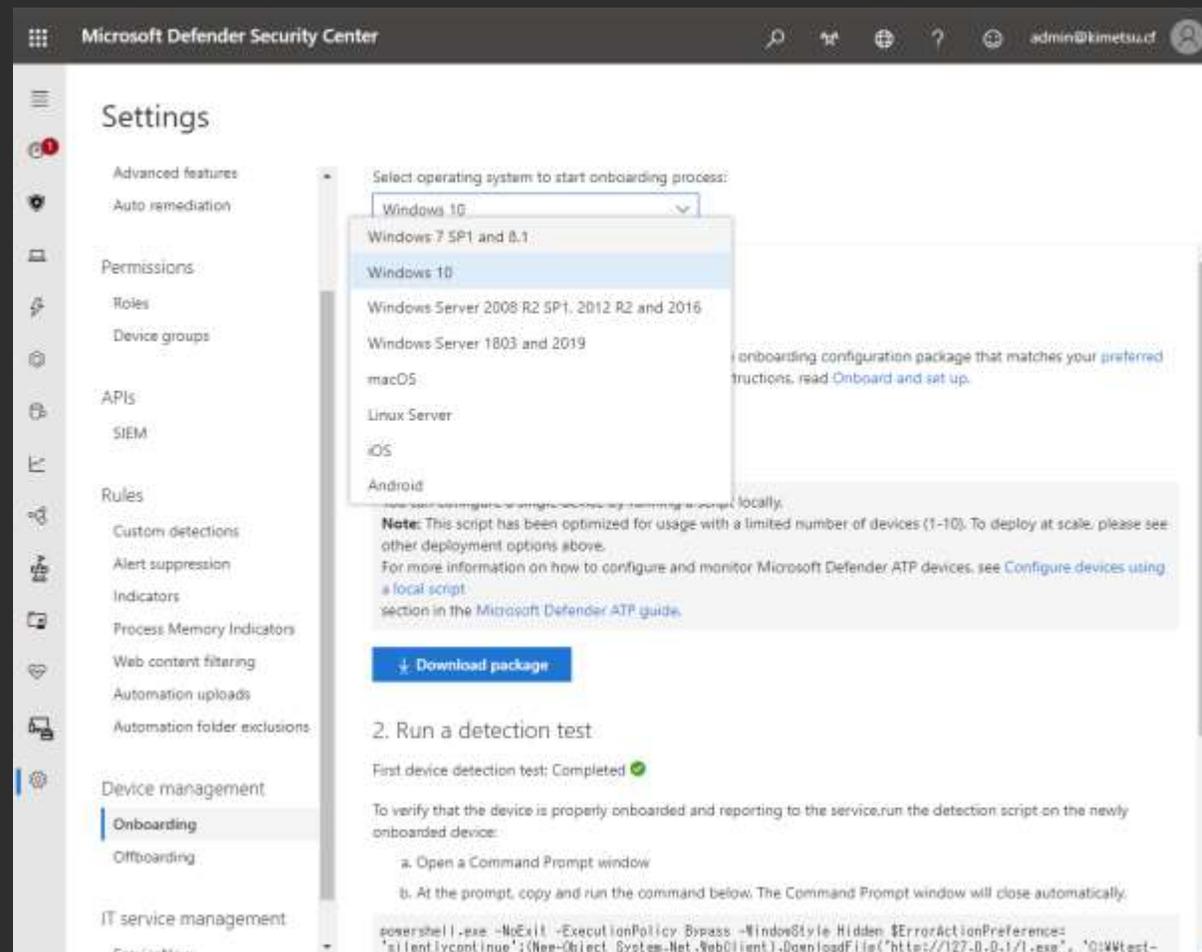
- Defender ATP のライセンス

サポート OS

- Windows 7, 8.1, 10
- Windows Server 2008 R2, 2012 R2, 2016, 2019
- macOS
- プレビュー : Linux, Android, iOS

ネットワーク接続

- 各 PC から [サービス URL](#) にアクセスできること



他社 EDR 製品に対する Defender ATP の優位性

Windows にビルトインされてるから可能なこと

攻撃への耐性

Windows OS に組み込み込まれた挙動センサーを使用するため、プロセスやサービス停止などによる攻撃を受けない。

メンテナンスフリー

エージェントの展開不要、アップデートの管理不要。
Windows OS の毎月の更新プログラムを適用するのみ。
アップデートに伴う検証も不要

高パフォーマンス

OS 標準のセンサーを利用するため負荷が非常に低い。
また通信データも最適化され、1 台あたり 1 日 5MB 程度。

Microsoft 365 セキュリティ製品連携

Windows セキュリティ製品はもちろん、Azure AD や Intune, MCAS や Office 365 といった様々な製品と連携



Microsoft Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams. Invisible to users.

Microsoft Defender ATP ライセンス

- ▶ Windows 10 Enterprise E5
- ▶ Windows 10 エデュケーション A5
- ▶ Windows 10 Enterprise E5 を含む Microsoft 365 E5
- ▶ Microsoft 365 E5 セキュリティ
- ▶ Microsoft 365 A5

Scene 11

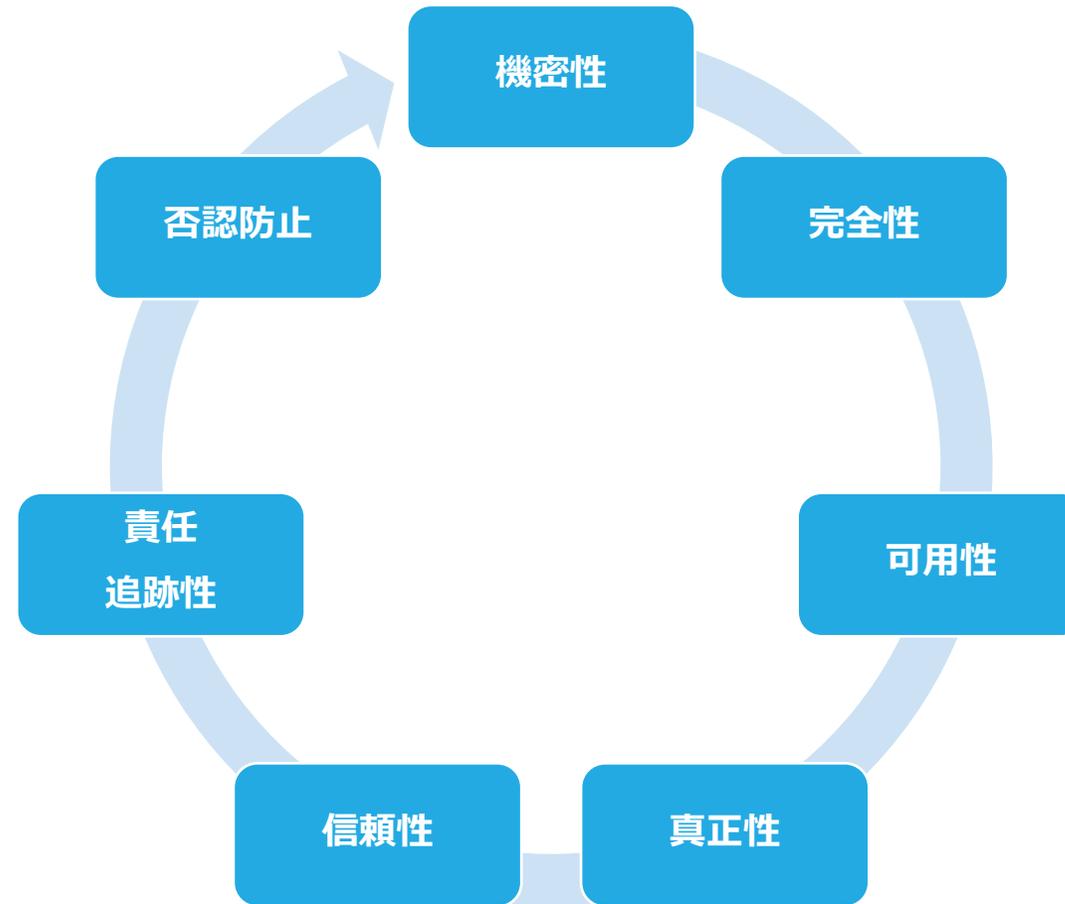
min

マイクロソフトとシトリックが語るVDIの正しい選び方

セキュリティ編

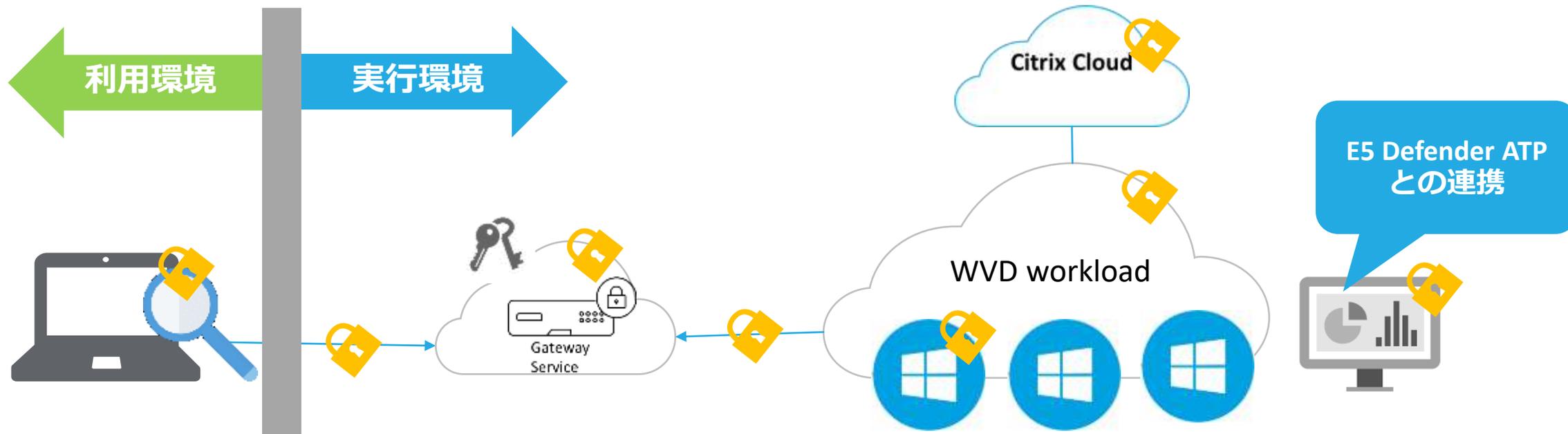
- | | | |
|---|--|-----|
| 1 | Windows Virtual Desktopに対するCitrixの価値 | 5分 |
| 2 | Citrixのみが提供するVDI環境のゼロトラストセキュリティ | 5分 |
| 3 | Citrixが提供するセキュリティ機能の紹介及びデモ | 20分 |
| 4 | Azure Windows Defender ATPで強化するVDIセキュリティ | 7分 |
| 5 | まとめ | 3分 |

VDIテレワークを行う上で考慮すべきセキュリティ



VDIは画面転送だから安全ということではない

Citrixが提供するVDIゼロトラストセキュリティ



監視、防御 抑止

- セッションウォーターマーク
- キーロギングプロテクション
- スクリーンキャプチャプロテクション
- SSO

分離、暗号化

- HDXプロトコル
- Secure ICA
- TLS
- SD-WAN

検疫 認証

- 検疫
- 端末認証
- 多要素認証
- 認証
- 条件付きアクセス
- 仮想スマートカード
- IDPセキュリティ連携
- Azure AD

ポリシー制御

- DLP
- データフィルタリング
- データダイレクションコントロール
- GPO
- Cloud SDN
- Cloud Micros Segmentation

認可

- アクセスフィルター
- 公開アプリ
- 公開デスクトップ
- 公開コンテナアプリ
- Windowsリソース
- Right Management
- 仮想スマートカード

監視、防御 抑止

- Citrix Analytics
- Security Graph Provider
- クラウドセキュリティ
- セッションレコーディング
- セッションタイマー
- クリーンブート
- 管理操作ログ
- Windows ATP
- Security Graph

CITRIX®