JAMF NATION LIVE

Macで校務DXを
もっと先へ

青野 寛之

セールスマネージャー

Jamf Japan 合同会社

Agenda

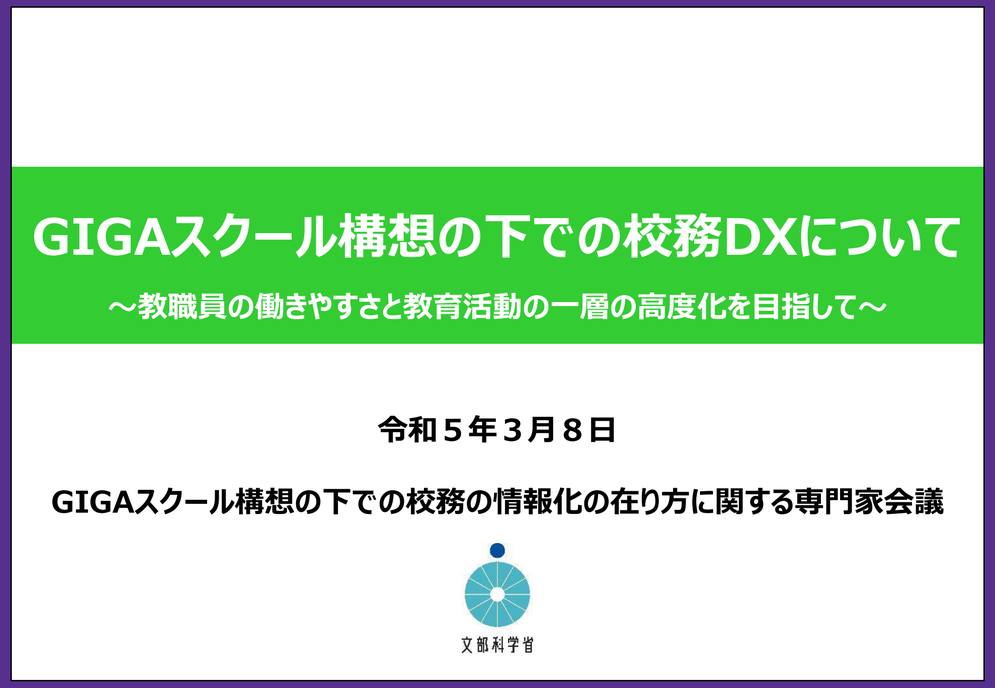
1 | 文科省校務DXにおけるMac
事例：岐阜市教育委員会

2 | 校務にMacが選ばれる理由
スペシャルゲスト登壇でご紹介

3 | 文科省校務DX方針をMac構成で読み解く
Mac構成におけるゼロトラストの実現

文科省：校務 DX についての方針

GIGAスクール構想と連動した校務環境の見直し



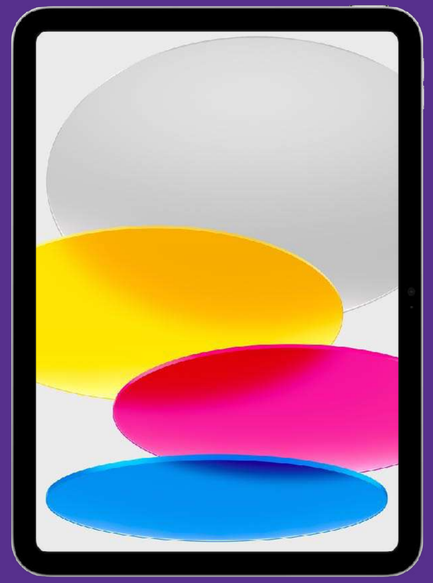
- 働き方改革：教職員1人1台PCかつロケーションフリーを進めることで職員室に縛られない柔軟な働き方を実現

- ゼロトラストセキュリティを土台とし、GIGAで選定したOSと親和性のある端末によってロケーションフリーを実現

“職員室の据え置きノートPC”から

”ロケーションフリーに対応した高性能モバイルノートPC”へ

授業用のiPadと校務用のWindows PC



連係できないOS親和性のない2台持ちが課題

岐阜市教育委員会様

校務デバイスとしてMacBook Airを1,849台導入

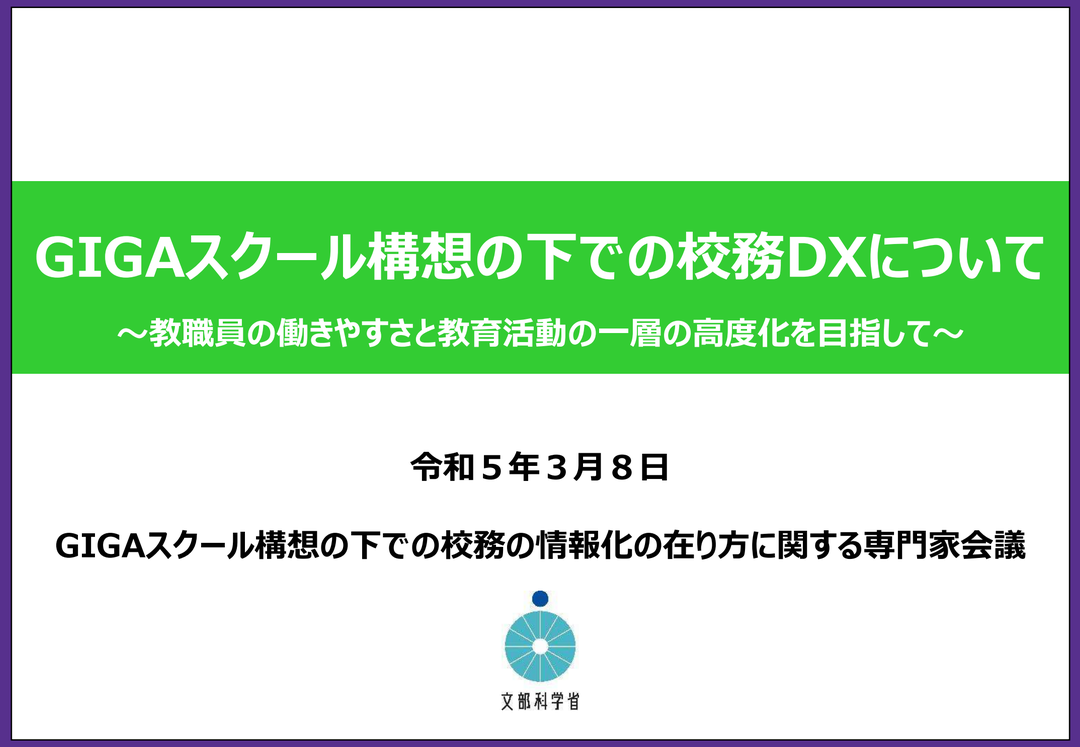
●JAMF NATION LIVE

文科省校務DX方針を Mac構成で読み解く

JAMF NATION LIVE

文科省：校務 DX についての方針

GIGAスクール構想と連動した校務環境の見直し



- 働き方改革：教職員1人1台PCかつロケーションフリーを進めることで職員室に縛られない柔軟な働き方を実現

- ゼロトラストセキュリティを土台とし、GIGAで選定したOSと親和性のある端末によってロケーションフリーを実現

文科省ガイドライン

図2　いわゆるゼロトラストセキュリティに関する要素技術

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術　※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知）　※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

Macで実現する校務DX構成

JAMF NATION LIVE

Macで実現する校務DX構成

認証基盤

Microsoft Entra ID

Google

MacBook Air

文科省ガイドラインへの対応は？

図２ **いわゆるゼロトラストセキュリティに関する要素技術**

①アクセスの真正性に関する要素技術		
①-1	**多要素認証**	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	**リスクベース認証**	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	**シングルサインオン（SSO）**	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	**通信経路の暗号化**	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	**Webフィルタリング**	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	**モバイル端末管理（MDM）** (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	**アンチウイルス**	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	**データ暗号化**	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	**EDR** (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	**IDS/IPS** (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	**WAF** (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

文科省ガイドラインへの対応は？

①-1	多要素認証
①-2	リスクベース認証
①-3	シングルサインオン（SSO）
②-1	通信経路の暗号化
②-2	Webフィルタリング
③-1	モバイル端末管理（MDM） (Mobile Device Management)
③-2	アンチウイルス
③-3	データ暗号化
③-4	EDR (Endpoint Detection and Response)

Mac経由のアクセス・ログイン

Mac利用時の通信の安全性

Macの管理・セキュリティ

文科省ガイドラインへの対応は？

①-1	多要素認証	☑ idP + Jamf Connect
①-2	リスクベース認証	☑ idP + Jamf Pro/ZTNA
①-3	シングルサインオン（SSO）	☑ idP + Jamf Connect
②-1	通信経路の暗号化	☑ idP + Jamf ZTNA
②-2	Webフィルタリング	☑ Jamf Safe Internet
③-1	モバイル端末管理（MDM） (Mobile Device Management)	☑ Jamf Pro
③-2	アンチウイルス	☑ macOS + Jamf Protect
③-3	データ暗号化	☑ macOS + Jamf Pro
③-4	EDR (Endpoint Detection and Response)	☑ Jamf Pro + Jamf Protect
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	- ネットワークインフラ側のため範囲外
③-6	WAF (Web Application Firewall)	- ネットワークインフラ側のため範囲外

Jamfを活用すれば、

文科省のガイドラインの考え方に沿った構成が実現できます。

Mac上の管理・セキュリティ

		Jamf で対応できる範囲
③-1	モバイル端末管理（MDM） (Mobile Device Management)	☑ Jamf Pro
③-2	アンチウイルス	☑ macOS + Jamf Protect
③-3	データ暗号化	☑ macOS + Jamf Pro
③-4	EDR (Endpoint Detection and Response)	☑ Jamf Pro + Jamf Protect

Mac上の管理

		Jamf で対応できる範囲
③-1	モバイル端末管理（MDM） (Mobile Device Management)	☑ Jamf Pro
③-2	アンチウイルス	☑ macOS + Jamf Protect
③-3	データ暗号化	☑ macOS + Jamf Pro
③-4	EDR (Endpoint Detection and Response)	☑ Jamf Pro + Jamf Protect

1. Macの端末管理はどうやるの？

Jamf で対応可能です

デバイス管理：

Pro

1. Macの端末管理はどうやるの？

Jamf で設定の配信が一括で可能です

初期設定自動化
- 設定自動化
- 事前に設定した構成の配信
- アカウント設定の適用

管理コマンド
- コンピュータを初期化
- OSアップデート・アップデート延期
- リモートデスクトップ

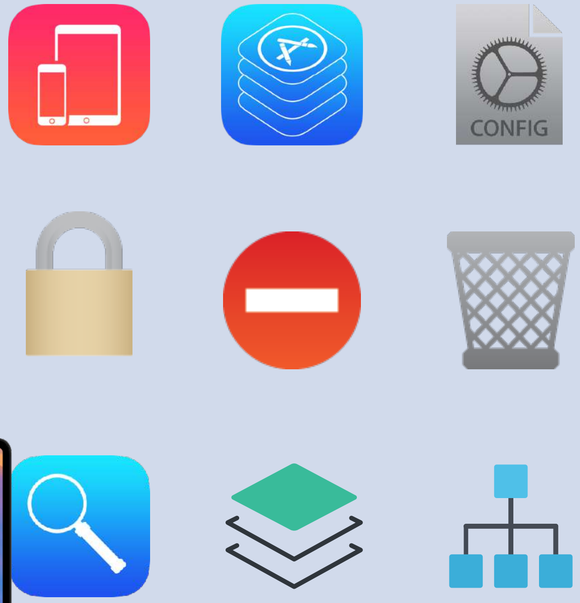
設定配信
- 構成プロファイル
- ポリシー設定

アプリ配信
- ASMを利用しライセンス一括購入
- AppSotre 以外のAppの配信、インストール
- アプリカタログ経由の配信

管理・制限・セキュリティポリシーなど
教育委員会様がやりたいことを実現

Jamf独自フレームワーク

MDMフレームワーク

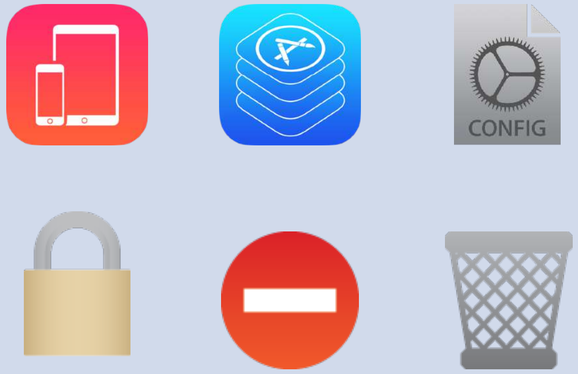


管理・制限・セキュリティポリシーなど
教育委員会様がやりたいことを実現

Jamf独自フレームワーク

Jamf Agent

MDMフレームワーク



1. Macの端末管理はどうやるの？

Jamfで300項目以上の情報の取得が可能です

ハードウェア詳細
コンピュータタイプ
コンピュータ名
シリアル番号
バッテリー状況

ソフトウェア詳細
macOSバージョン
インストール済みアプリ
ストレージ容量
空き容量

ネットワーク詳細
セキュリティ
IPアドレス
証明書情報

その他
マネージドステータス
インストール済み構成プロファイル
購入情報など

1. Macの端末管理はどうやるの？

Jamf で対応可能です

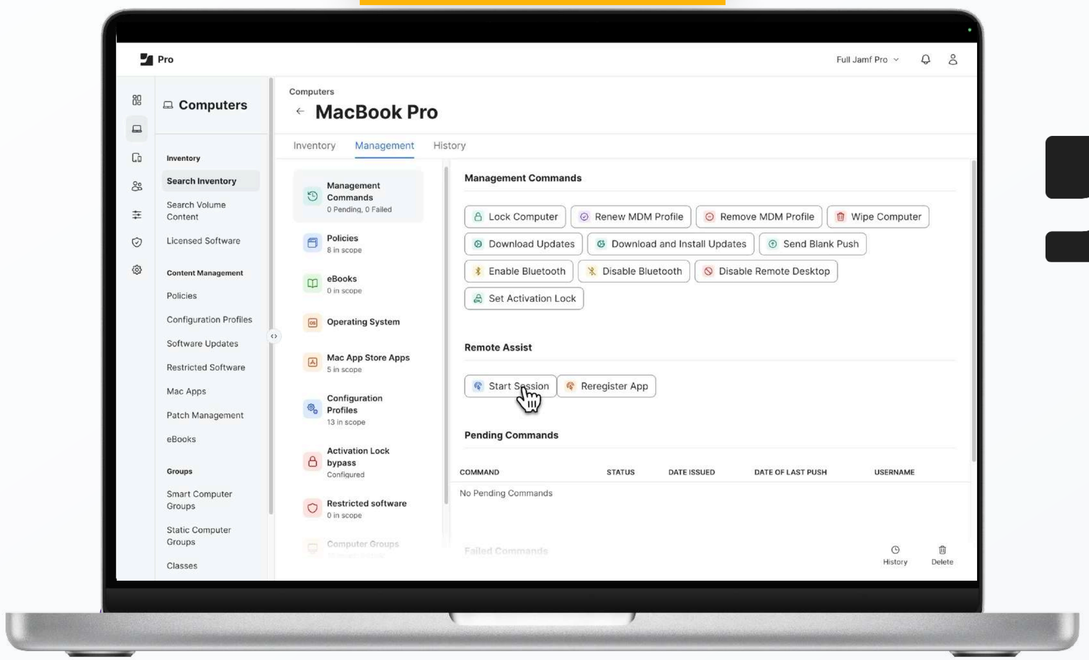
デバイス管理：

Pro

1. Macの端末管理はどうやるの？

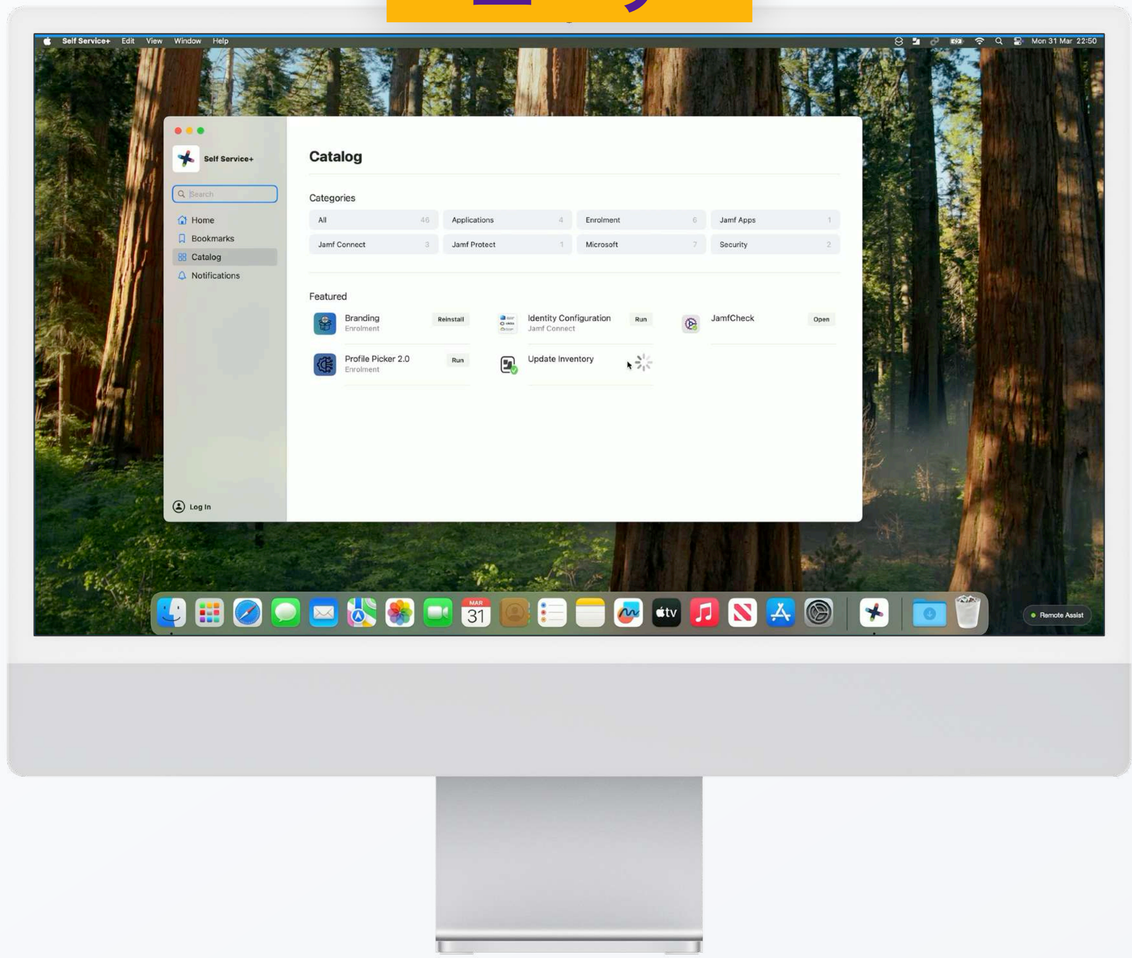
Jamf Remote Assistにより
有事の際は遠隔制御が可能

管理者



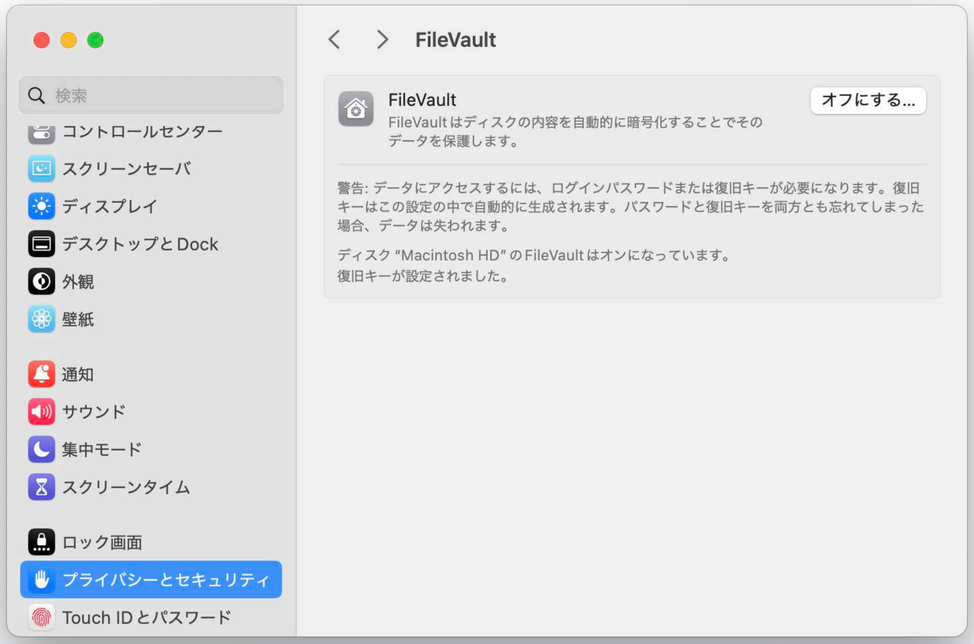
Pro

ユーザ



2. データ暗号化

MacはFileVaultによりデータ暗号化機能が内蔵



JamfでFileVaultの強制適用が可能です

Mac上の管理

		Jamf で対応できる範囲
✅③-1	モバイル端末管理（MDM） (Mobile Device Management)	☑ Jamf Pro
③-2	アンチウイルス	☑ macOS + Jamf Protect
✅③-3	データ暗号化	☑ macOS + Jamf Pro
③-4	EDR (Endpoint Detection and Response)	☑ Jamf Pro + Jamf Protect

Mac上のセキュリティ

		Jamf で対応できる範囲
③-1	モバイル端末管理（MDM） (Mobile Device Management)	☑ Jamf Pro
③-2	アンチウイルス	☑ macOS + Jamf Protect
③-3	データ暗号化	☑ macOS + Jamf Pro
③-4	EDR (Endpoint Detection and Response)	☑ Jamf Pro + Jamf Protect

3と4. Macのアンチウイルス、EDR

macOSの標準機能として
セキュリティ対策の機能が搭載されています

XProtect / MRT

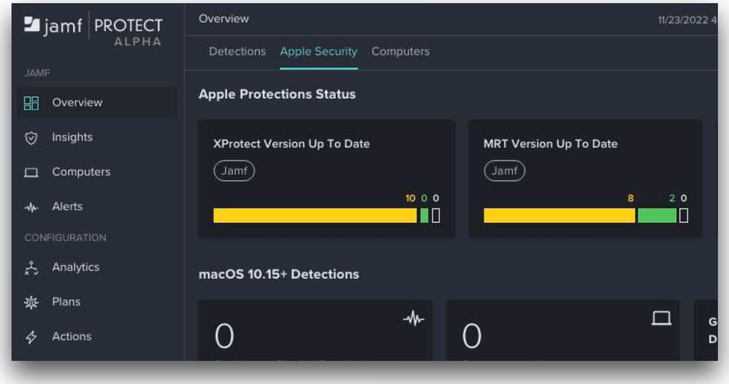
- 既知の脅威からの対策
- マルウェアのブロック
- マルウェアに感染した場合の自動修復

Gatekeeper

- App実行の前の検疫
- 認定開発者の署名の確認
- 開発者の確認

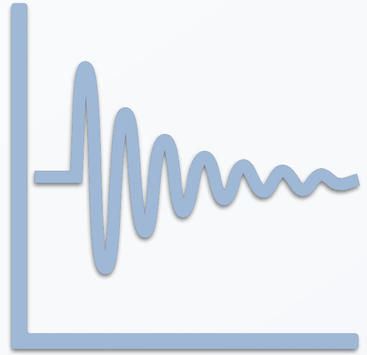
3と4. Macのアンチウイルス、EDR

組織で必要となるセキュリティ対策が可能です



- セキュリティログ可視化
  (AirDropの転送ログ等)
- 未知の脅威対策

- 外部ドライブの制御



- 軽快な動作

Protect

3と4. Macのアンチウイルス、EDR

macOS標準機能とJamfでMacの安全性の確保が可能です

XProtect / MRT

Gatekeeper

+

Protect

文科省ガイドライン

図２ **いわゆるゼロトラストセキュリティに関する要素技術**

①アクセスの真正性に関する要素技術		
①-1	**多要素認証**	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	**リスクベース認証**	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	**シングルサインオン（SSO）**	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	**通信経路の暗号化**	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	**Webフィルタリング**	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
✅ ③-1	**モバイル端末管理（MDM）** (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
✅ ③-2	**アンチウイルス**	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
✅ ③-3	**データ暗号化**	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
✅ ③-4	**EDR** (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	**IDS/IPS** (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	**WAF** (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

Mac経由のアクセス・ログイン

		Jamfで対応できる範囲
①-1	多要素認証	☑ IdP + Jamf Connect
①-2	リスクベース認証	☑ IdP + Jamf Pro/ZTNA
①-3	シングルサインオン（SSO）	☑ IdP + Jamf Connect

5と6. 多要素認証とSSO

MacのIdP連携方法は？

Microsoft Entra ID

Google

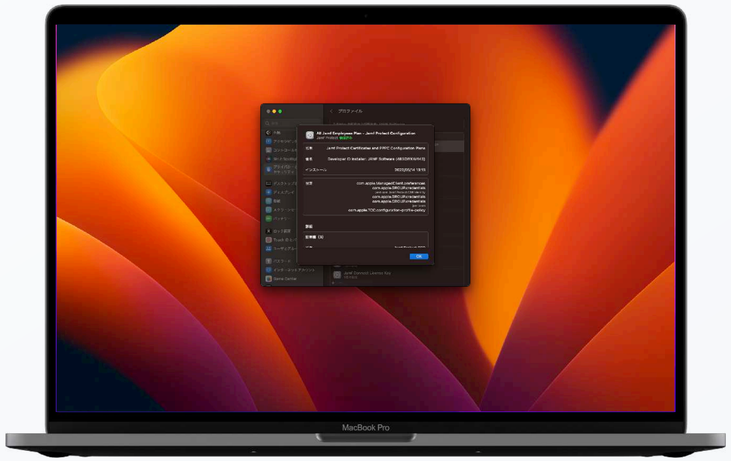
5と6. 多要素認証とSSO

Jamfにより、IdPとの連携が容易に可能です

Microsoft
Entra ID

Google

Connect



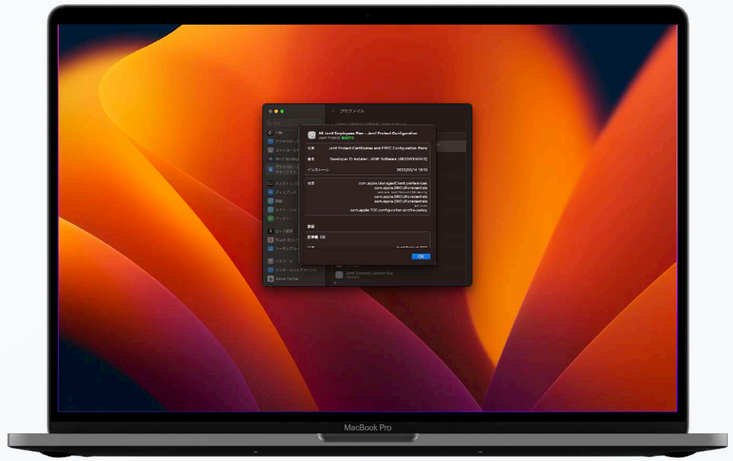
5と6. 多要素認証とSSO

Macのサインイン画面を差し替え

Microsoft
Entra ID

Google

Connect



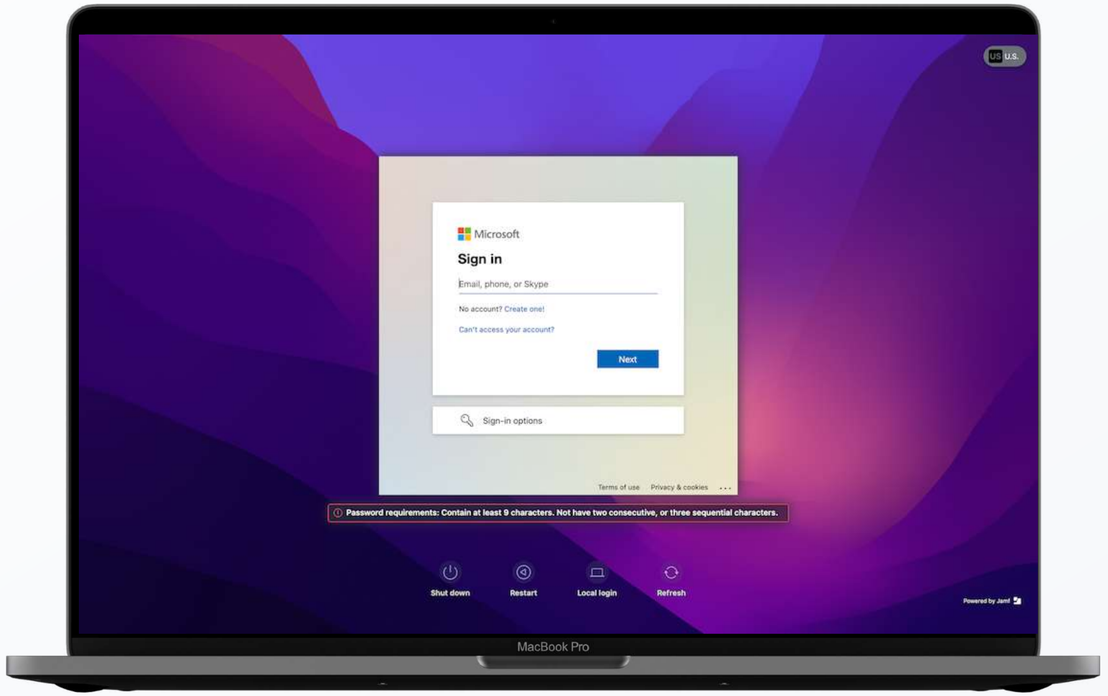
5と6. 多要素認証とSSO

Macのサインイン画面を差し替え

先生は今まで通りのIDとPWでMacを使えます

Microsoft
Entra ID

Google



Connect

Mac経由のアクセス・ログイン

		Jamfで対応できる範囲
✅	①-1 多要素認証	☑ IdP + Jamf Connect
	①-2 リスクベース認証	☑ IdP + Jamf Pro/ZTNA
✅	①-3 シングルサインオン（SSO）	☑ IdP + Jamf Connect

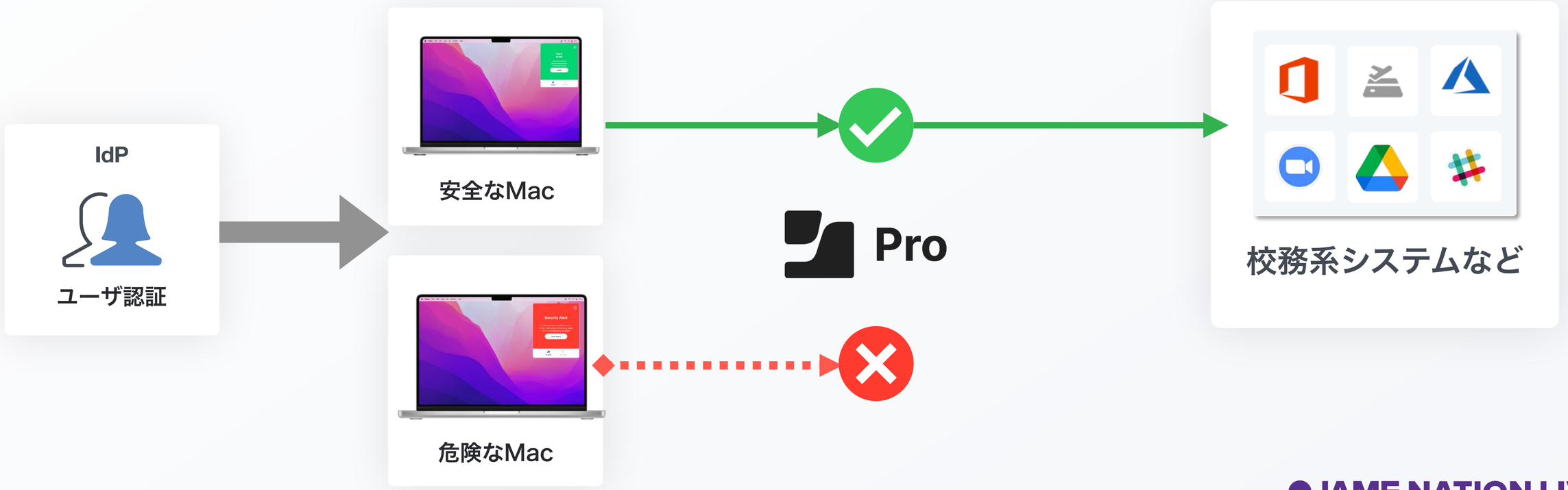
Mac経由のアクセス・ログイン

		Jamfで対応できる範囲
①-1	多要素認証	☑ IdP + Jamf Connect
①-2	**リスクベース認証**	**☑ IdP + Jamf Pro/ZTNA**
①-3	シングルサインオン（SSO）	☑ IdP + Jamf Connect

7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

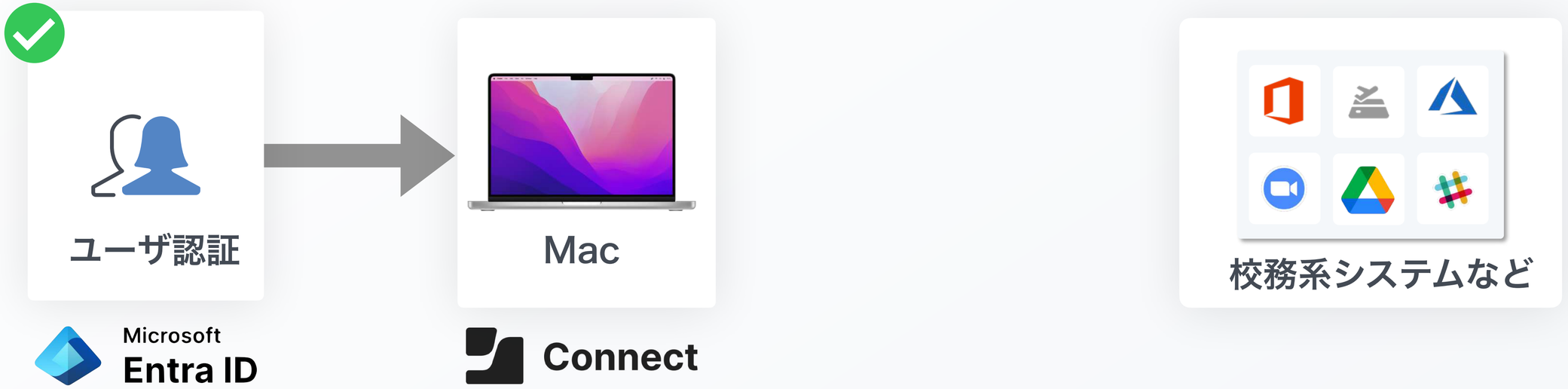
- 許可したMac かつ 安全なMac のみ校務系システムに接続
- 利用者は何も意識せず、安全な環境で業務を開始



7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携



7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携

7. リスクベース認証

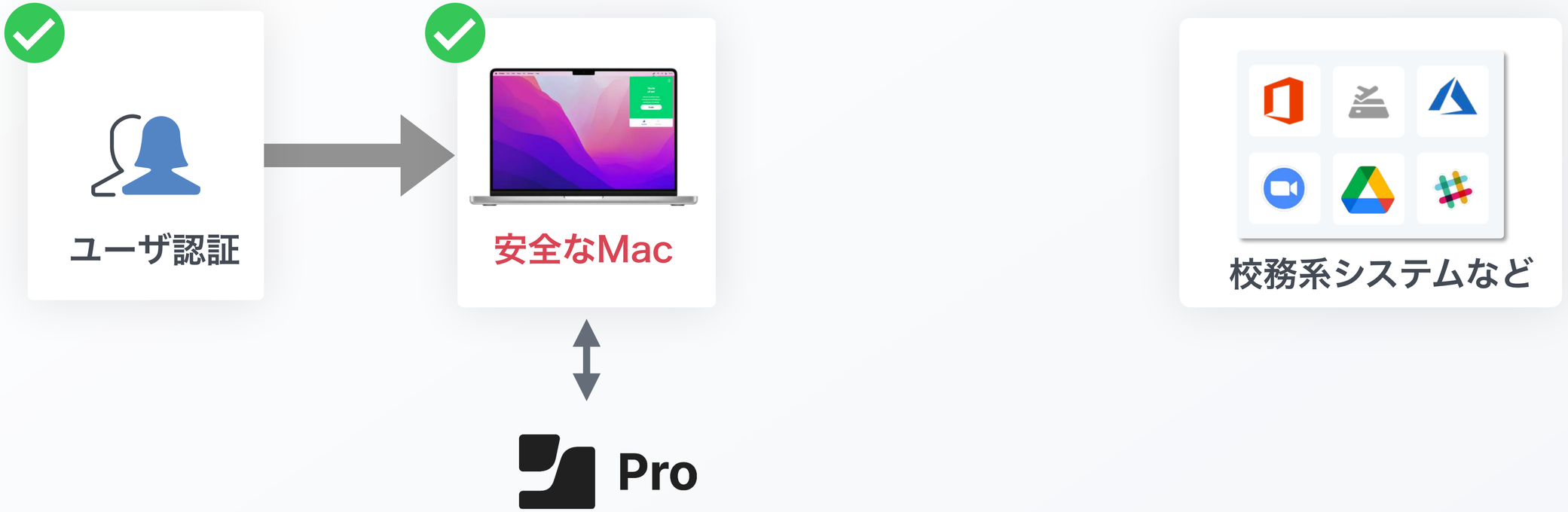
“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携

7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携



7. リスクベース認証

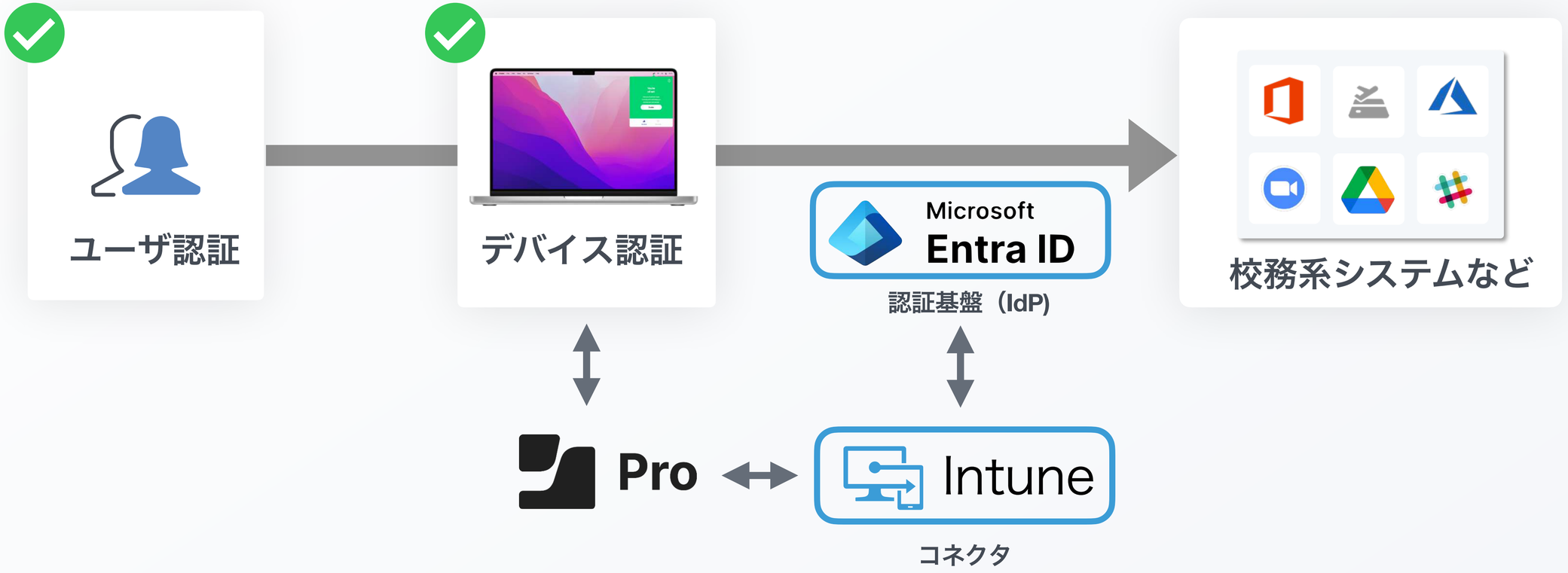
“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携

7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携



7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Googleの「Context Awareness Access」とJamf Proの連携

7. リスクベース認証

“安全なMacだけ”が校務系へアクセスできる仕組み

- Entra IDの「条件付きアクセス」とJamf Proの連携
- Googleの「Context Awareness Access」とJamf Proの連携

デバイスの状態からリスク判定

・MDM管理下の確認

・組織のセキュリティ準拠済

文科省ガイドライン

図２ **いわゆるゼロトラストセキュリティに関する要素技術**

①アクセスの真正性に関する要素技術		
✅ ①-1	**多要素認証**	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
✅ ①-2	**リスクベース認証**	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
✅ ①-3	**シングルサインオン（SSO）**	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	**通信経路の暗号化**	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	**Webフィルタリング**	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
✅ ③-1	**モバイル端末管理（MDM）** (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
✅ ③-2	**アンチウイルス**	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
✅ ③-3	**データ暗号化**	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
✅ ③-4	**EDR** (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	**IDS/IPS** (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	**WAF** (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

Mac利用時の通信の安全性

		Jamfで対応できる範囲
②-1	通信経路の暗号化	☑ IdP + Jamf ZTNA
②-2	Webフィルタリング	☑ Jamf Safe Internet

8. 通信経路の暗号化 (ZTNA)

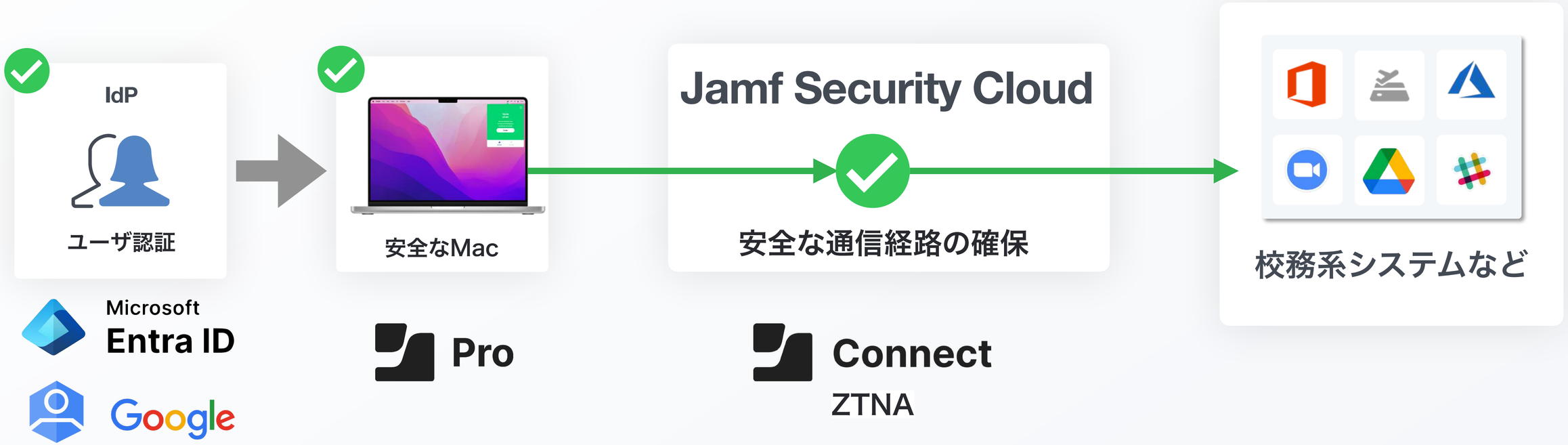
Macから校務系へセキュアにアクセスする仕組み

- WireGuardとPer App VPNの採用により軽快な動作を実現

8. 通信経路の暗号化 (ZTNA)

Macから校務系へセキュアにアクセスする仕組み

- WireGuardとPer App VPNの採用により軽快な動作を実現



9. Webフィルタリング

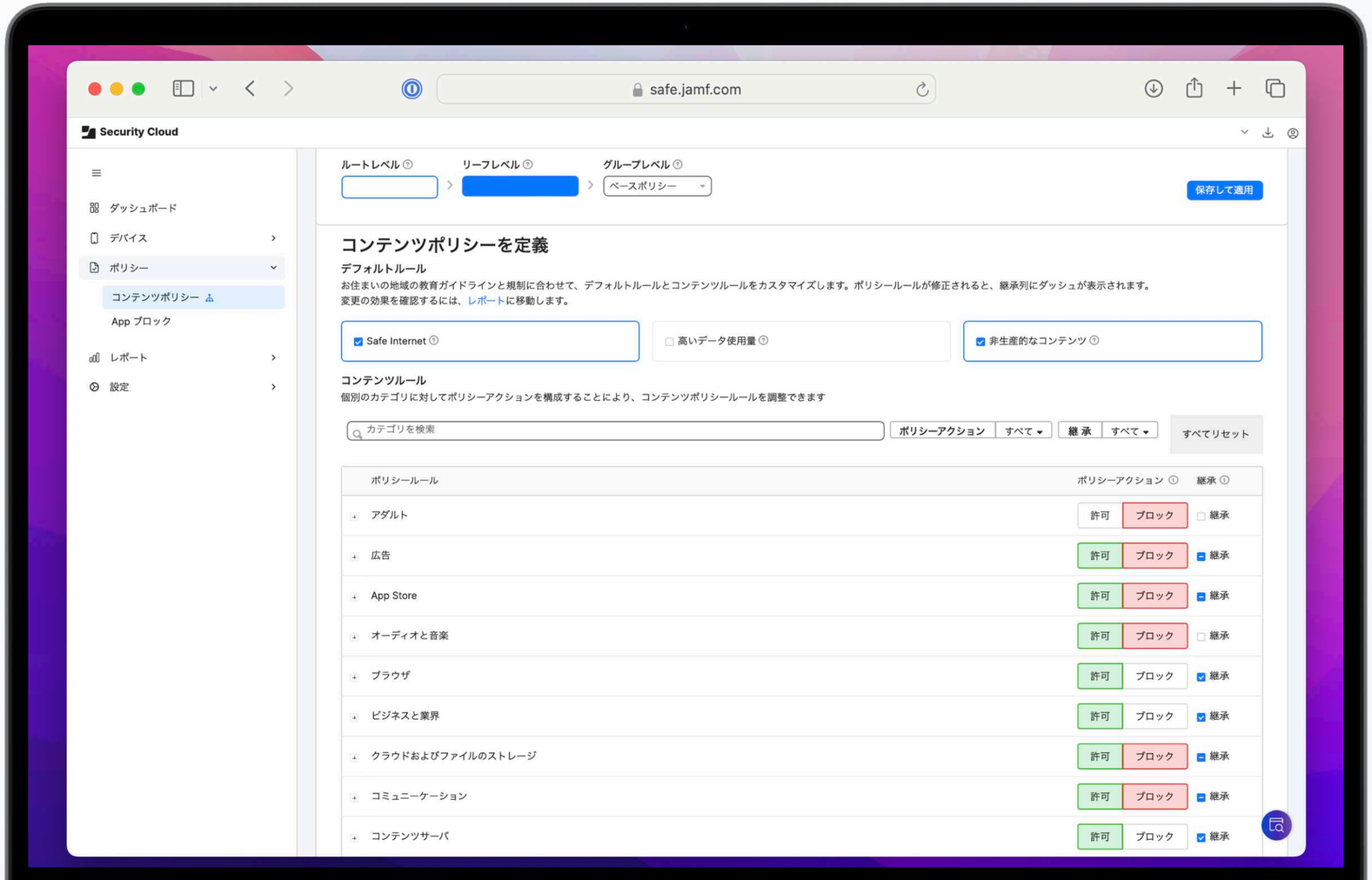
危険なサイト、過激コンテンツへのアクセスをブロック

Jamf Safe Internet

カテゴリごとに
許可/ブロックを設定

カテゴリの例

- 広告
- アダルト
- ギャンブル
- クラウドストレージ等



●JAMF NATION LIVE

文科省ガイドライン

図 2	いわゆるゼロトラストセキュリティに関する要素技術		校務系 macOS
①アクセスの真正性に関する要素技術			
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術	☑ IdP + Jamf Connect
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術	☑ IdP + Jamf Pro/ZTNA
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる	☑ IdP + Jamf Connect
②通信の安全性に関する要素技術			
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術	☑ IdP + Jamf /ZTNA
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される	☑ Jamf Safe Internet
③端末・サーバの安全性に関する要素技術			
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術	☑ Jamf Pro
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある	☑ macOS + Jamf Protect
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術	☑ macOS
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術	☑ Jamf Pro + Jamf Protect
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術	× ネットワークインフラにて対策
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。	× ネットワークインフラにて対策

MacはJamfと組合せることで文科省ガイドラインに沿った構成が実現できます

ご紹介した4製品

MDM	セキュア認証	エンドポイントセキュリティ	Webフィルタリング
端末をリモートで一括管理	安全な認証と通信の確保	端末を脅威から保護する	危険なサイトへのアクセスをブロック
DEVICE MANAGEMENT	MAC ACCOUNT & SECURE AUTHENTICATION	macOS THREAT DETECT & PREVENTION	Content Filter & AntiSpam, Malware, Fishing
Pro	Connect	Protect	Jamf Safe Internet

ご紹介した 4 製品

MDM	セキュア認証	エンドポイントセキュリティ	Webフィルタリング
端末をリモートで一括管理	安全な認証と通信の確保	端末を脅威から保護する	危険なサイトへのアクセスをブロック
DEVICE MANAGEMENT	MAC ACCOUNT & SECURE AUTHENTICATION	macOS THREAT DETECT & PREVENTION	Content Filter & AntiSpam, Malware, Fishing
Pro	Connect	Protect	Jamf Safe Internet

Jamf for K-12 (Pro mac)

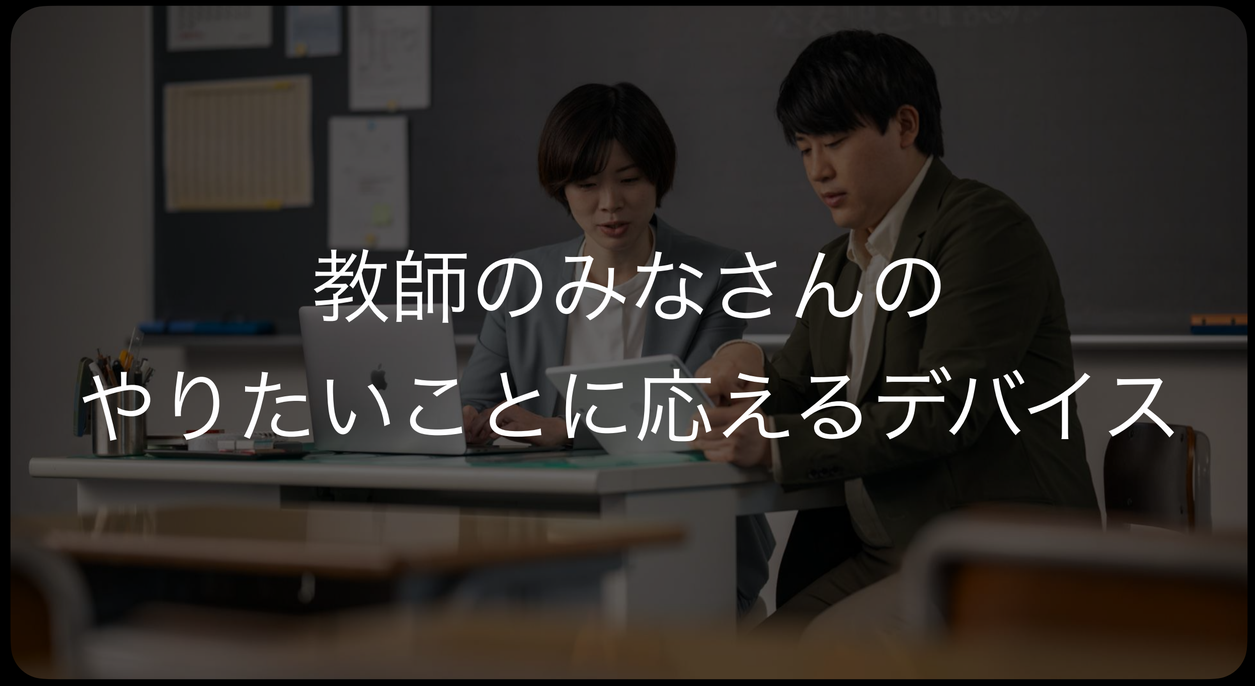
まとめ

ワークライフバランスに
合った使い方ができる

持ち歩いて
どこでも使える

学習用iPadと
合わせても使える

大切な情報
を守れる



直感的に
使える

やりたいことに
チャレンジできる

子どもたちの学びを
受け止められる

バッテリーが
長持ちする

Jamf for K-12 (Pro mac)

jamf

ペアレンタル
コントロール

特権昇格

& セキュアな
プライバシー

クラスルーム
管理

Macの
エンドポイント保護

オンデバイス
ネットワーク
脅威対策

オンデバイス
コンテンツ
フィルタリング

マルチデバイス
対応

Appインストーラ

Blueprintによる
宣言型デバイス
管理

ロールベース
管理

時間ベースの
ポリシー

学生に
フォーカス

JAMF NATION LIVE

THANK YOU