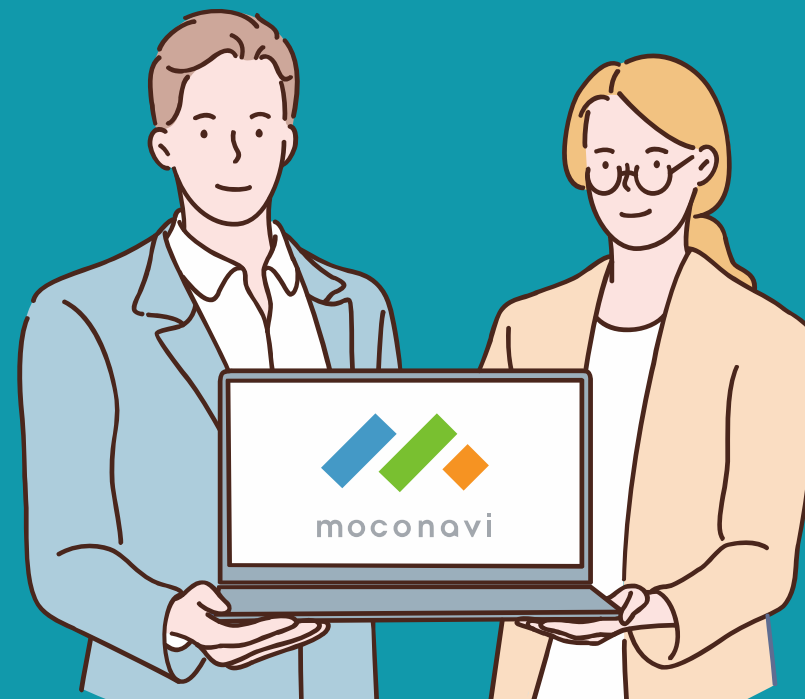


＼文教市場でのゼロトラストを実現する！／

ゼロトラストブラウザ 「mococho (モコクロ)」のご紹介

2024年8月版

株式会社レコモット



株式会社レコモットについて

Envision Your Style

誰もが「Your Style」を制約なく実現できる社会

会社名	株式会社レコモット
代表者	代表取締役CEO 東郷 剛
設立	2005年11月
資本金	100,000,000円
所在地	東京都千代田区麹町3-3-8 麹町センタープレイス8F
事業内容	携帯電話関連製品の開発・販売・運用 コミュニケーション関連システムの受託開発 電子通信事業 届出番号：A-30-16513

※レコモットコーポレートサイトより



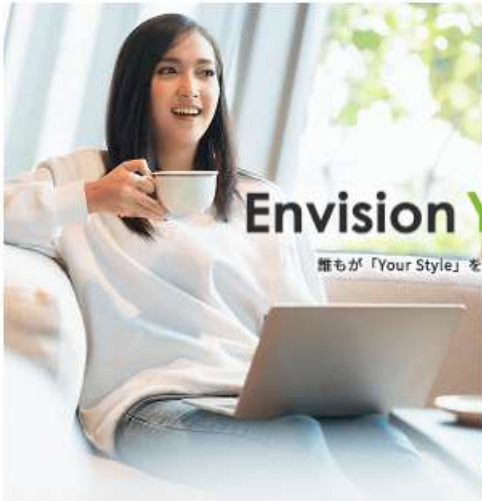
サービス

会社情報

採用情報

ニュース

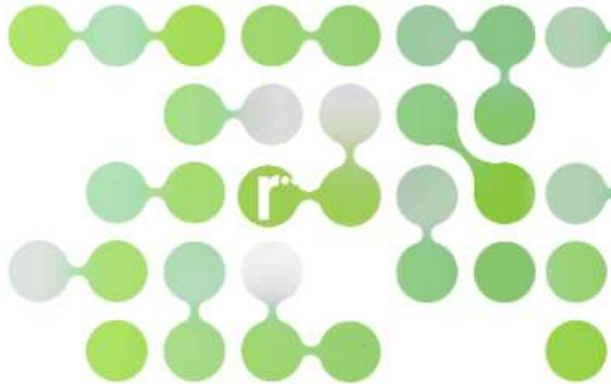
お問い合わせ



テクノロジーによって、
あらゆるコミュニケーションの
ハブとなる

世界中の人々のコミュニケーションを繋ぐための技術
「Relational Communication and Mobile Technology」をコンセプトに、
コミュニケーションに関わるあらゆるサービスを提供していく会社です。

会社情報



支給もBYODも、ハイブリッドワークを面でサポート

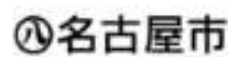
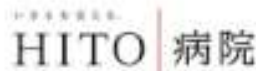
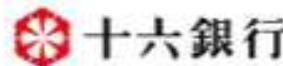
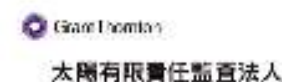
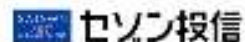
「moconavi」シリーズは、VPNレスのリモートアクセス、公私分計の電話サービスで、支給の端末でも個人端末の業務利用（BYOD）でもハイブリッドワークの課題を全て解決！



豊富な導入実績

5年連続MAM市場※ **No.1 !** 1,700社 33万IDの導入実績！

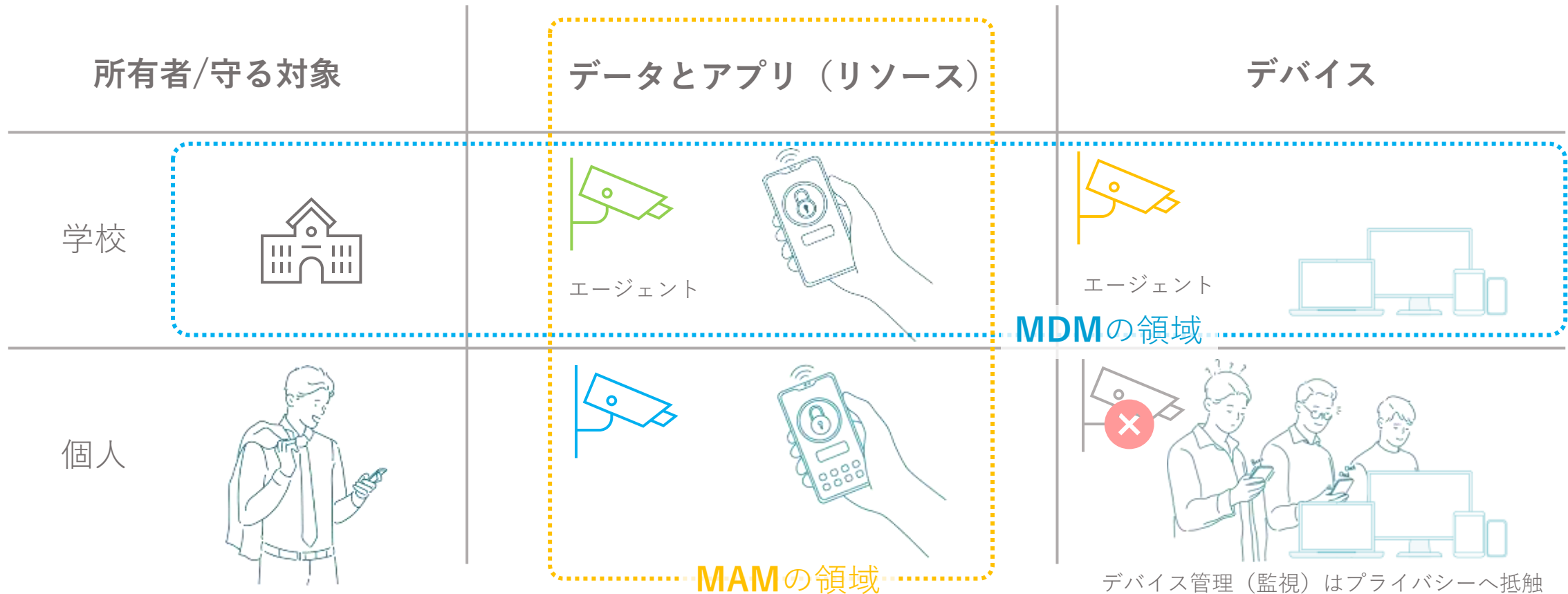
※出典株式会社テクノ・システム・リサーチ「2021-2022年版 エンドポイント管理市場のマーケティング分析モバイルアプリ管理市場-MAM市場-」市場調査より。



※岐阜県ロゴ使用許諾：清流の国®岐阜県 #0131

moconaviはデバイス管理ではなくアプリ管理※

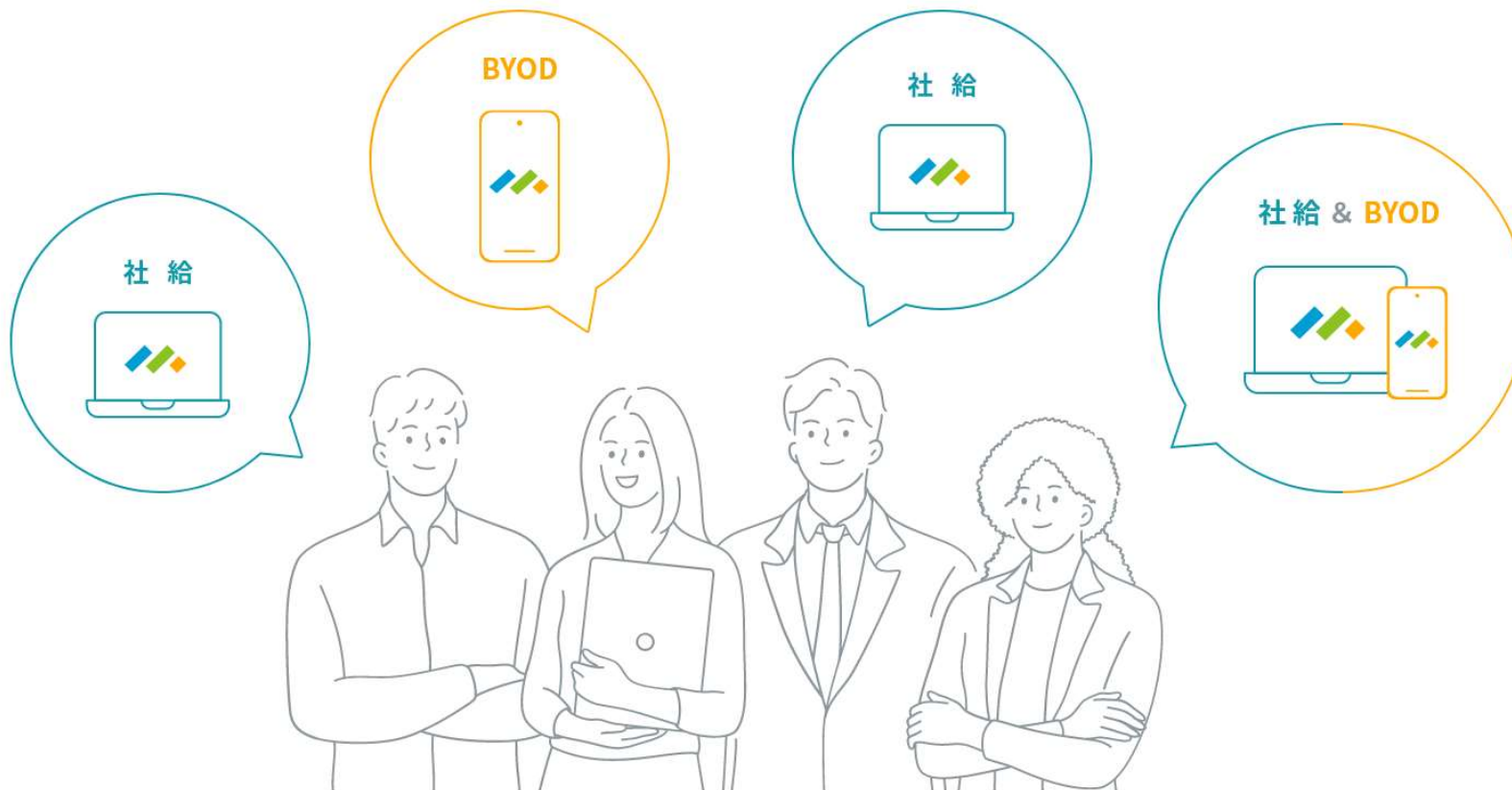
デバイスではなく、情報資産に限定して保護すれば、プライバシーも保護でき、社給でもBYODでも使える。



※MAM（Mobile Application Management）の略称でアプリケーションとデータにフォーカスして保護する仕組み

これからは端末もハイブリッドに

BYODでも支給端末でも高セキュリティ、プライバシーも万全、VPNもいらない…



ハイブリッドワーク対象が全職員に拡大
課題は端末の調達・安全性・運用のコスト



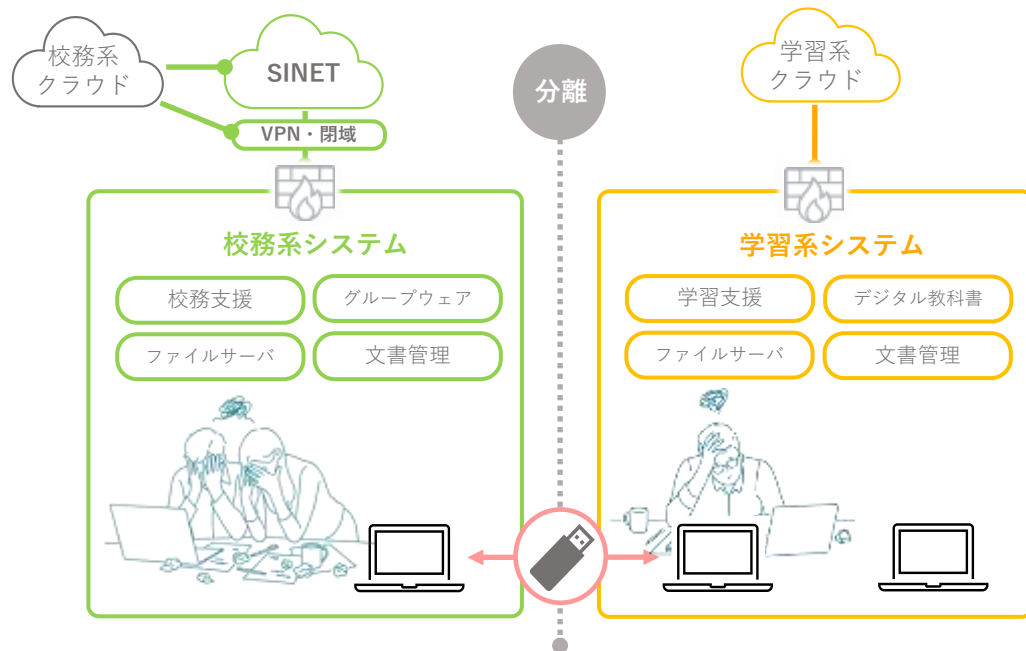
これからのハイブリッドワーク環境は支給と
個人端末（BYOD）も含めたハイブリッド型へ



文教市場の課題とゼロトラスト

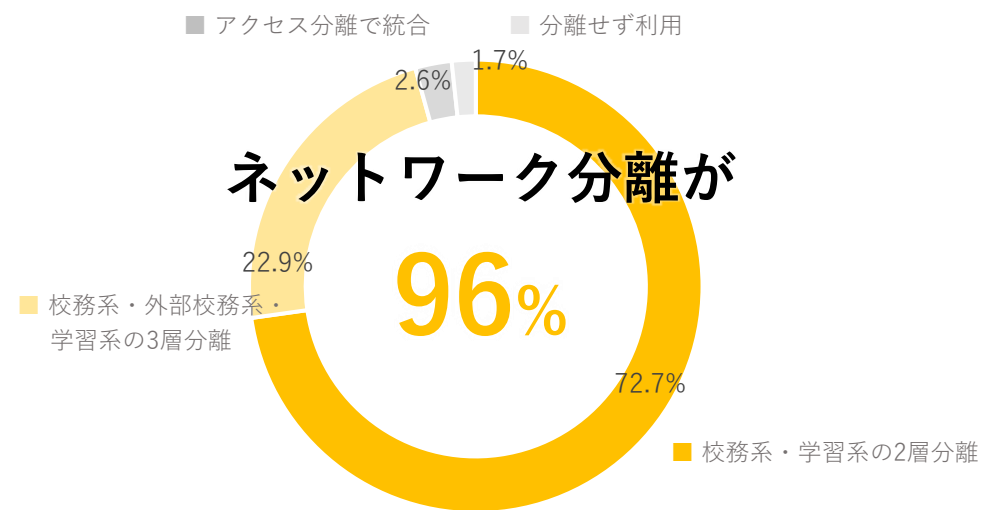
ネットワークは分離され、利便性が低い

よくある学校のネットワーク



過去のガイドラインに沿って、校務系と学習系を分離

全国の校内ネットワークの状況



出典：GIGAスクール構想の下での公務の情報化の在り方に関する専門家会議（第8回）配布資料

細かいことの積み重ねが時間を奪う

ネットワークが分離されていてUSBで移動

パソコンの切り替えや移動に時間がかかる

バラバラのクラウドサービスで煩雑

インターネット閲覧できない

校務系で教材を作れない

校務系で受け取った資料を学習系に移すのが手間

運用ルールやセキュリティポリシーが曖昧で不安

学校にこないと公務ができない



校務DXには**ゼロトラスト**が必要？**ゼロトラスト**ってなんだ？

学校向けゼロトラストクラウドサービス

大丈夫、moconaviなら**ゼロトラスト**が簡単に導入できます！

リモートデスクトップサービス

moconavi RDS



在宅勤務の導入に。
校外の端末から学校内の校務端末にアクセス
できる画面転送サービス。

クラウドゲートウェイサービス

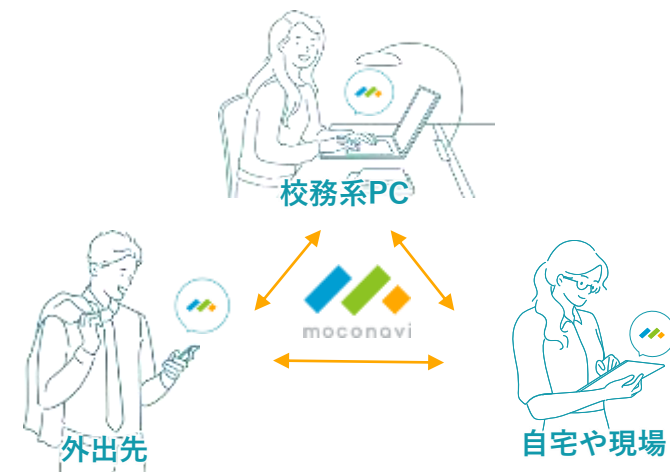
moconavi



校外からのクラウドサービスのご利用に。独
自の通信暗号化技術でインターネットファイ
ルを無害化。

クラウドコミュニケーションサービス

moconavi + moconavi 050



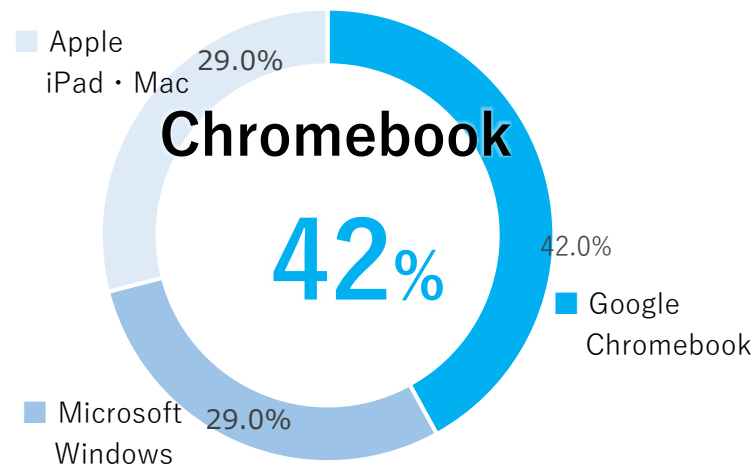
校内・校外のコミュニケーションをシームレ
スに。安全なコンタクトツール。

※クラウドコミュニケーションサービスの全ての機能は、クラウドゲートウェイサービスに含まれております。

moconavi（モコナビ）ならPCもタブレットも！

moconaviはWindowsだけでなく、MacやChromebookにも対応予定です！（25年2月）

GIGAスクール端末のOSシェア (2023年)



※出典：GIGAスクールにおけるベンダーシェアを分析（MM総研）

校務系PCはWindowsが多い
moconaviはWindows、iOS、Androidに対応！

moconaviの独自アプリはサンドボックス化され、業務システムを安全に利用可能。



サンドボックス化されたセキュアなオリジナルアプリ

※サンドボックス：外部に影響を与えない隔離された環境

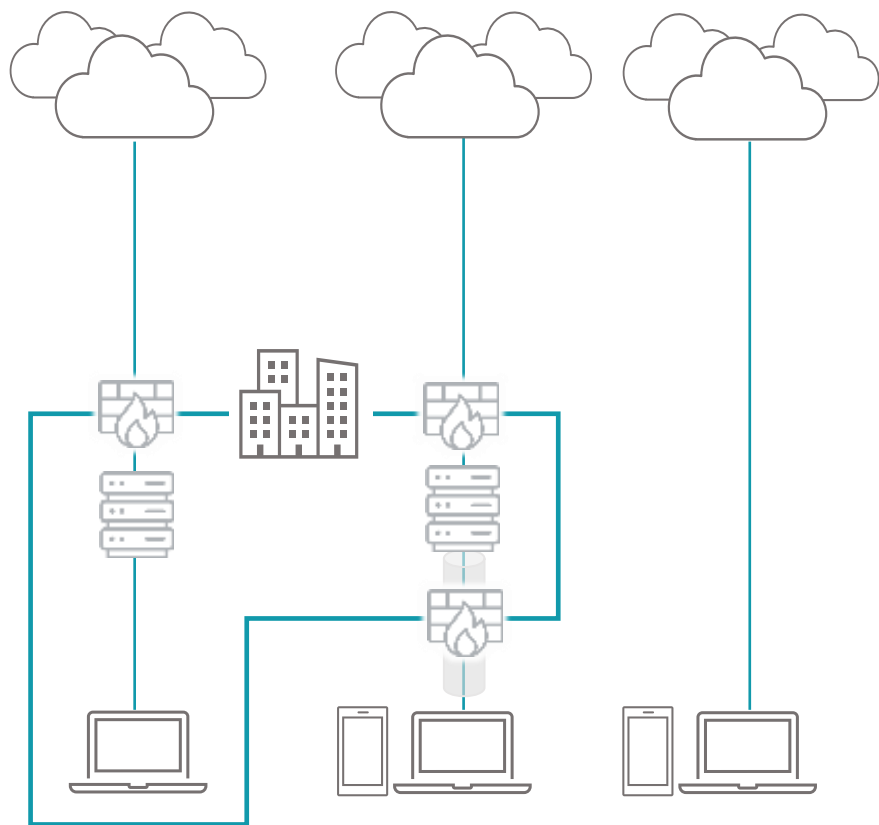
ウィルス感染リスク
端末がマルウェアに感染しても
アプリ内（=校内）に侵入しない

端末紛失リスク
端末にデータが残らないので
紛失時のリモートワイプも必要ない

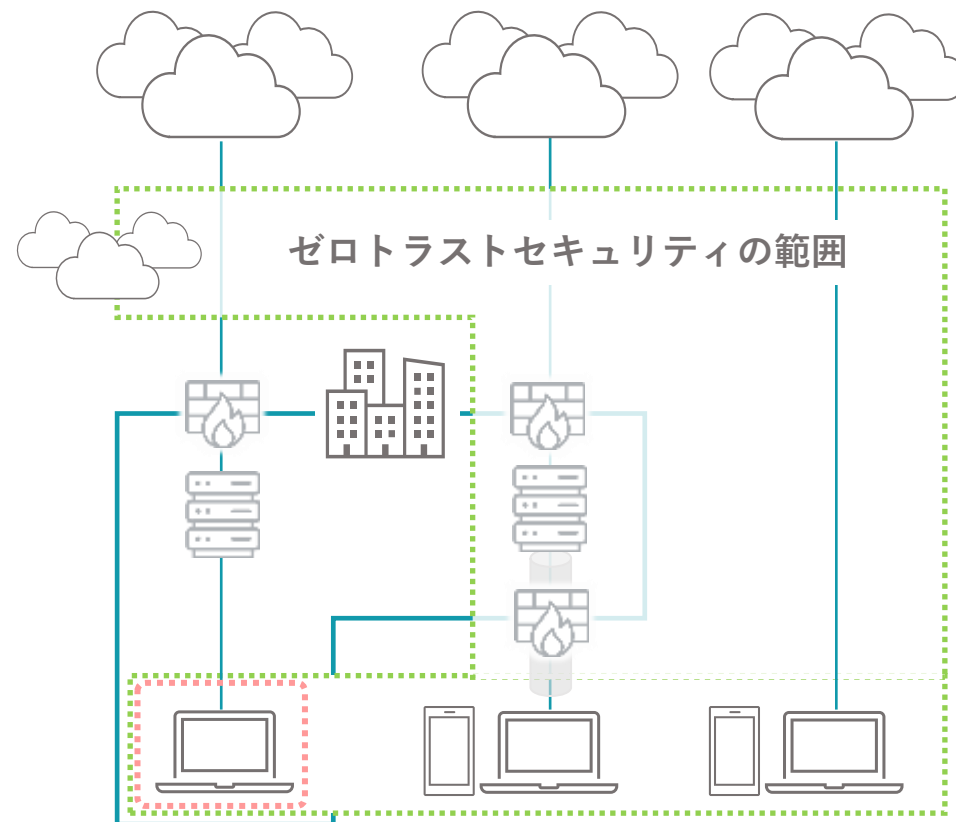
内部脅威リスク
画面キャプチャやコピペなど、ユー
ザ操作の制御設定で悪意ある情報持
ち出しを抑制

境界型防御の限界とゼロトラストの範囲

クラウドの普及を背景に境界が曖昧に。
(VPN等の脆弱性などセキュリティ要件も背景)



ゼロトラストは全てのロケーションとリソースが対象
(局所的な対応はゼロトラストセキュリティではない！)



NEXT GIGAの背景と方向性

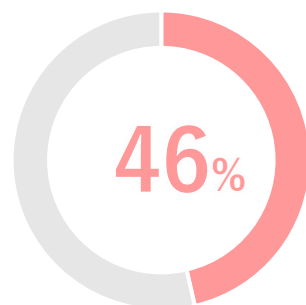
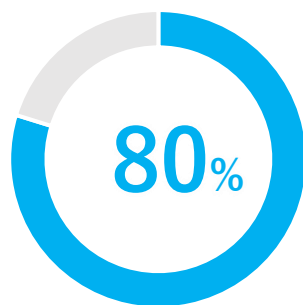
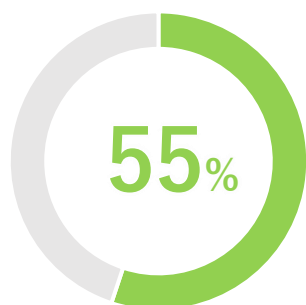
過労死基準といわれる 月100時間以上の時間外勤務をする教員の割合

※正し、持ち帰り残業を含む

小学校

中学校

高校



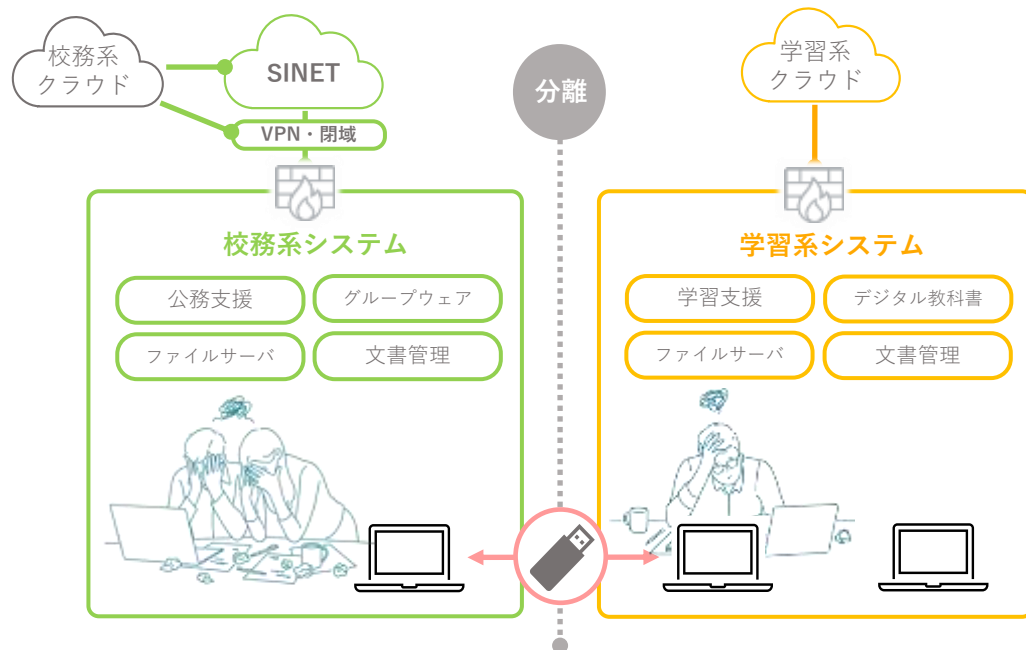
出典：「とりもどせ！教職員の「生活時間」-日本における教職員の働き方・労働時間の実態に関する調査研究報告書-」
(連動総研)

NEXT GIGAの方向性 (ChatGPTより)

- NEXT GIGA（ネクストギガ）では、**教員の働き方改革**や効率的な教育関連情報の管理のために、**クラウドベースの次世代校務支援システムの導入**が本格化しています。
- GIGAスクール構想の第2段階を指す「NEXT GIGA」では、教育DX（デジタル・トランスフォーメーション）を推進することで、学校教育のあり方を革新することが求められています。教育DXとは、デジタル技術を活用してカリキュラムや教育手法、**教職員の業務改革**などを行うことを指します。
- GIGAスクール構想では、児童・生徒に1人1台の端末（GIGA端末）が導入され、クラウドサービスを利用できるネットワーク環境が整備されています。しかし、端末の故障やバッテリーの劣化などのハード面の課題が生じており、早い自治体では**2024年度中に端末の更新**を要する状況です。

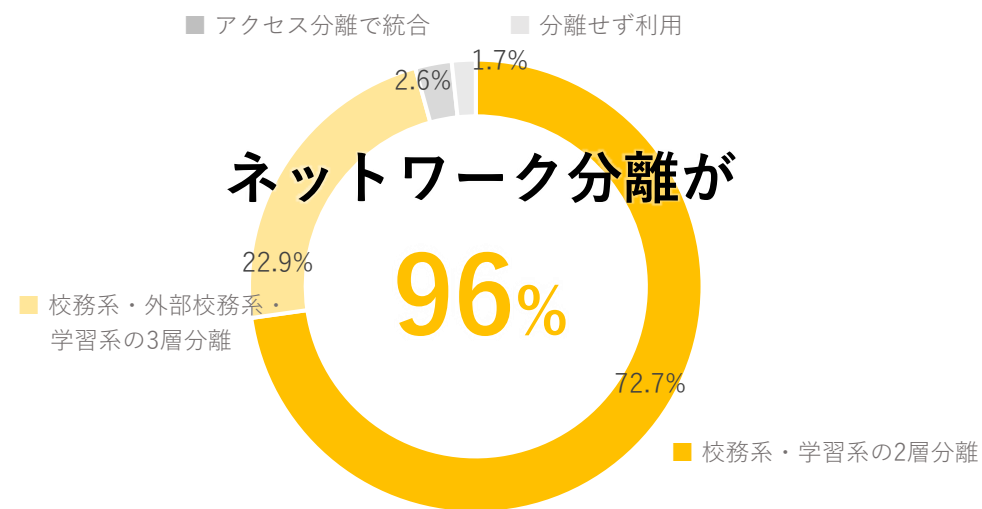
ネットワークは分離され、利便性が低い

よくある学校のネットワーク



過去のガイドラインに沿って、校務系と学習系を分離

全国の校内ネットワークの状況



出典：GIGAスクール構想の下での公務の情報化の在り方に関する専門家会議（第8回）配布資料

細かいことの積み重ねが時間を奪う

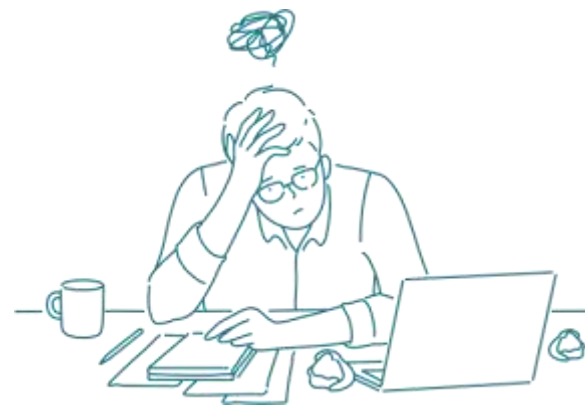
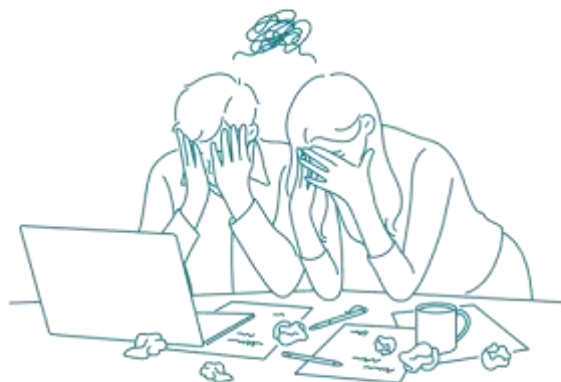
ネットワークが分離されていてUSBで移動

パソコンの切り替えや移動に時間がかかる

バラバラのクラウドサービスで煩雑

インターネット閲覧できない

校務系で教材を作れない



校務系で受け取った資料を学習系に移すのが手間

運用ルールやセキュリティポリシーが曖昧で不安

学校にこないと公務ができない

次世代校務DXにおけるゼロトラストセキュリティ

令和5年3月8日 GIGAスクール構想の下での校務の情報化の在り方に関する専門家会議
GIGAスクール構想の下での校務DXについて～教職員の働きやすさと教育活動の一層の高度化を目指して～

図3 アクセス制御を前提としたネットワークにおける情報セキュリティの確保（イメージ）

- 校務システムに蓄積される情報や、学習システムにおいて教員がアクセスし得る複数の児童生徒の学習履歴など、学校現場で取り扱う情報のうち機微度が高いものへのアクセスについては、前ページで示したセキュリティ技術を複数組み合わせることが適当。また、技術的対策だけでなく利用者のリテラシーも高める必要がある。
- 教職員が使用するネットワークや端末は、こうした情報・データを扱うことから、【①-1 多要素認証、①-3 SSO、②-1 通信経路の暗号化、②-2 Webフィルタリング、③-1 MDM、③-2 アンチウイルス、③-3 データ暗号化、③-5 IDS/IPS】の導入によるセキュリティの確保はどのような自治体においても必須である^{※1}。

（中1）他方、上記以外の要素技術もセキュリティの向上に資するものであり、取り扱うデータの重要度やリスク要因の発生頻度を踏まえたセキュリティリスクと導入・運用費用、以下のような特長等の諸要素を比較考慮する必要があるが、導入が望ましいものと考えられる。①-2 リスクベース認証は、リスクの判定基準によりセキュリティと利便性のバランスが変化するものであるが、適切な判定基準が用いられることで認証の強度を高めるものである。②-4 EDR、②-6 WAFは、その効果を最大化するためには専門的な知識を持つ人材による事前のチューニングとログ分析が必要であり、管理者がそれのためのスキルを習得する、外部の事業者による委託することが必要であるが、EDRは端末を攻撃するマルウェア対策として、WAFはWebサーバに対する不正アクセス対策として、いずれも有効である。

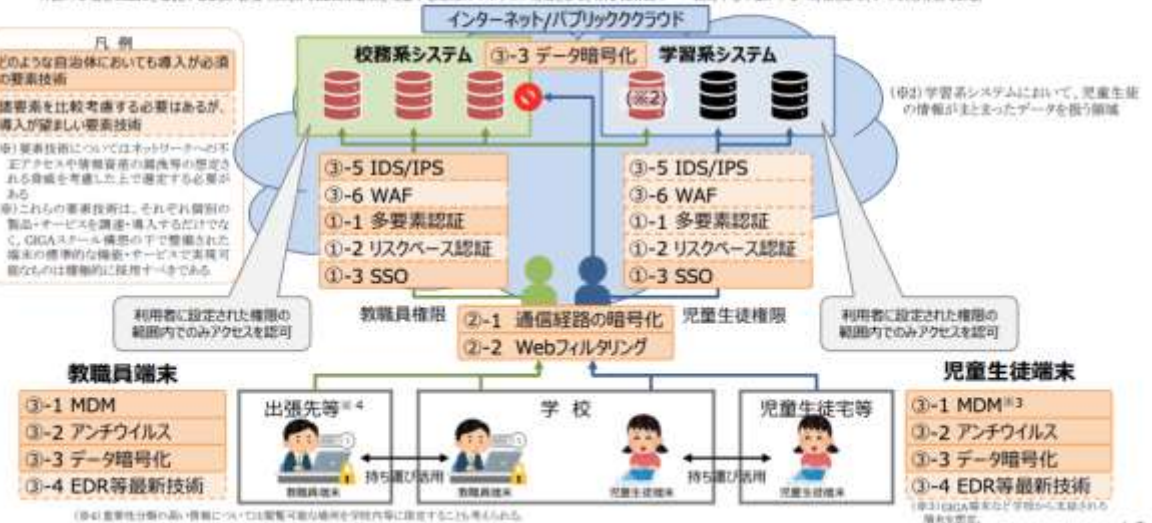


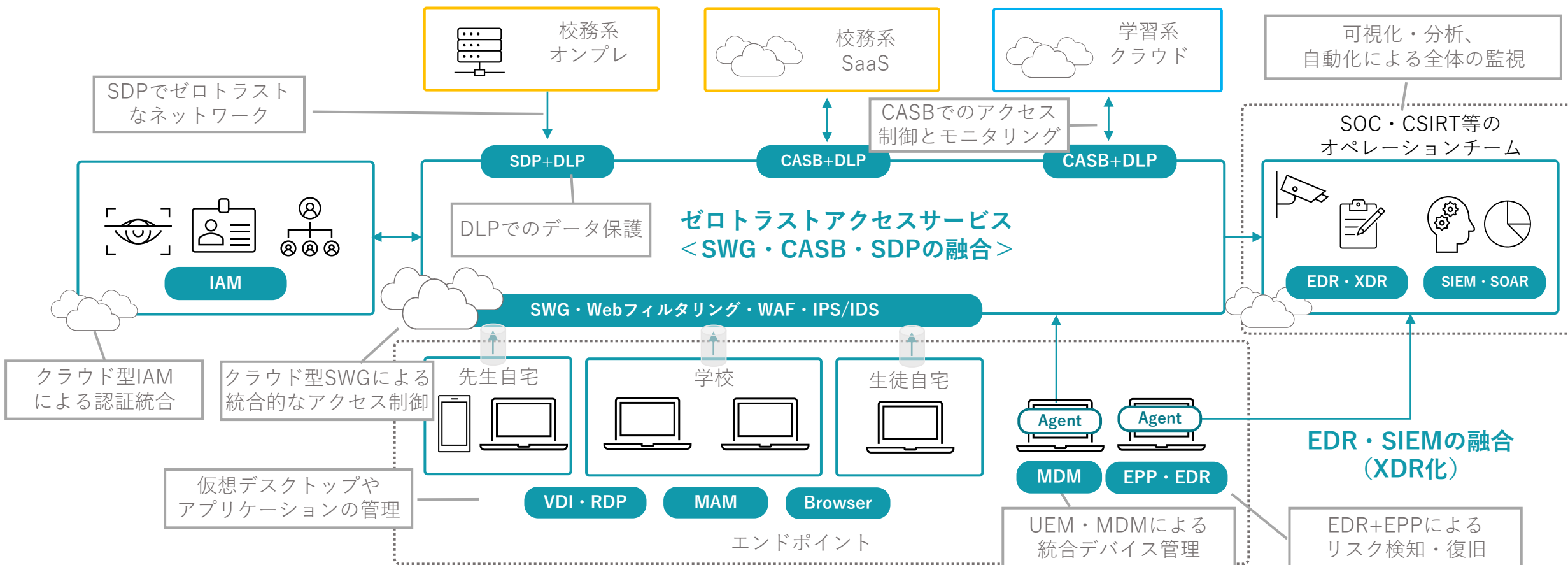
図2 いわゆるゼロトラストセキュリティに関する要素技術

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さは、複数のサービスで共通ID・パスワードを管理可能なパスワードを設定する端末となる
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高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と、画像・音声等の不適切なコンテンツに分類されたWebページへの接続を自動的に禁止するコンテンツ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権限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等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） ※のびに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

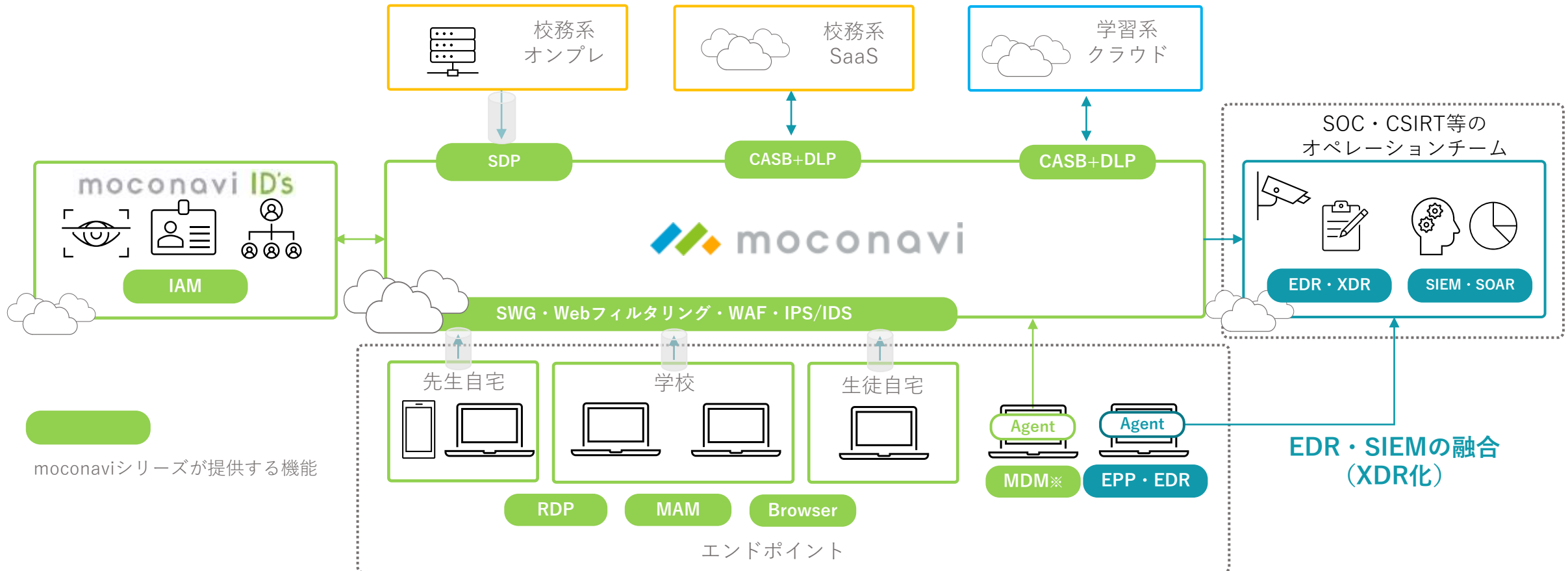
※これは、「教育情報セキュリティポリシーに関するガイドライン」（令和4年11月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するものを中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

次世代公務DXとゼロトラストの関係性

最近はCASB・SWG・SDPの融合したSSE化と、EDR・SIEMが融合したXDR化がトレンド。



moconaviシリーズ単独でゼロトラストセキュリティの主要部分のカバレッジを実現！



※moconavi RDS (Splashtop) 技術者ライセンスのデバイス管理機能・リモートサポート (Windows)

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

moconavi ID's

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

moconavi

カテゴリフィルターについてはi-Filterと連携可能

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が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。

他社のMDMでも可

moconavi RDS

※デバイス管理およびウィルススキャンは技術者ライセンスのオプション

任意（ローカルサンドボックスがあるため）

moconavi

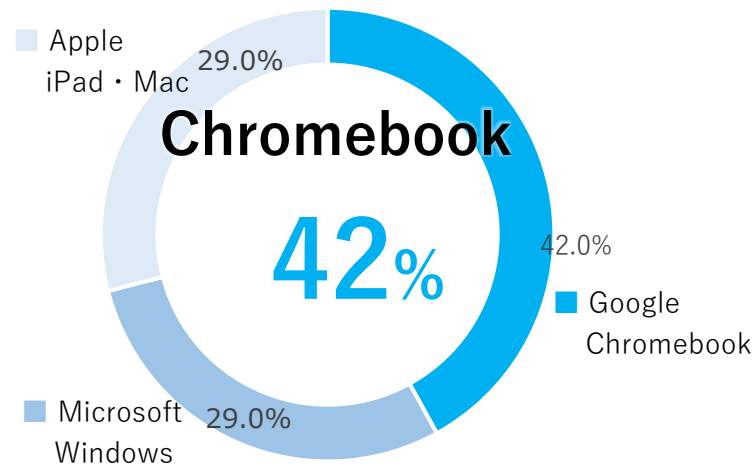
必要ない（ローカルサンドボックスがあるため）

moconavi

moconavi

学習系は三つ巴、校務系は Windowsが主流

GIGAスクール端末のOSシェア (2023年)



※出典：GIGAスクールにおけるベンダーシェアを分析（MM総研）

校務系のOSシェア想定 (2022年)

校務用PCのOSシェアは、主にWindowsです。
教員は校務用パソコンを1人1台持っていることが多く、そのOSの大多数はWindowsです。多くの教員はWindows搭載端末の使い方に慣れているためです。

出典 日経 **XTECH**

学校向けクラウドサービス

リモートアクセスサービス

moconavi RDS



在宅勤務の導入に。
校外の端末から学校内の校務端末にアクセス
できる画面転送サービス。

クラウドゲートウェイサービス

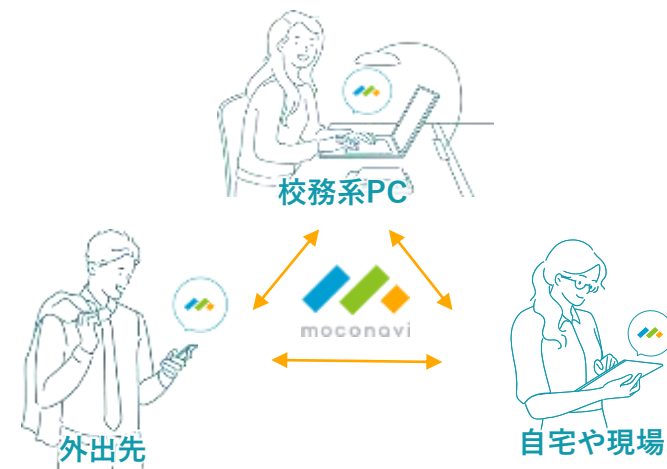
moconavi



校外からのクラウドサービスのご利用に。独
自の通信暗号化技術でインターネットファイ
ルを無害化。

クラウドコミュニケーションサービス

moconavi + moconavi 050

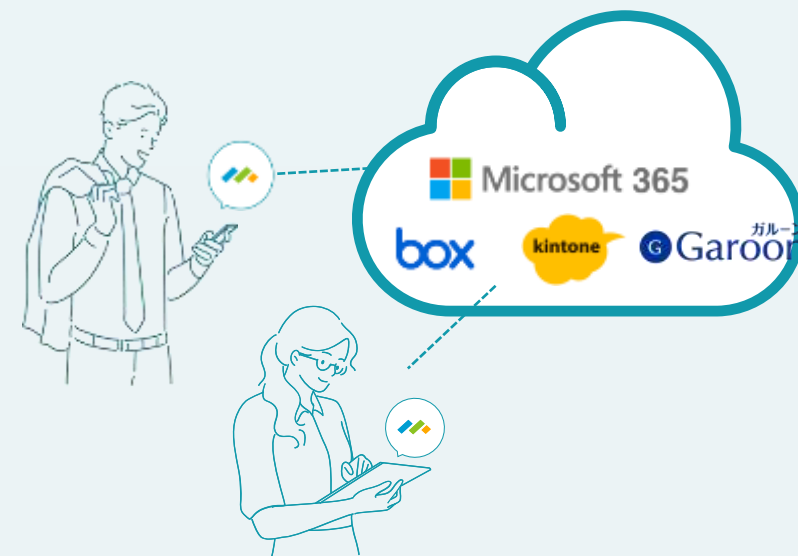


校内・校外のコミュニケーションをシームレ
スに。安全なコンタクトツール。

※クラウドコミュニケーションサービスの全ての機能は、クラウドゲートウェイサービスに含まれております。



クラウドゲートウェイ機能



今いる場所がオフィスになる！

スマホやPCにはmoconaviアプリを入れるだけ。場所を問わない安全で快適なテレワークを実現します。

クラウドサービスも

Google
Workspace

Microsoft 365

sansan

kintone

ガルーン
Garoon

salesforce

オンプレミスも

外出先からスマホで

端末にはアプリを入れるだけ！

自宅やオフィスからPCで

端末や通信経路にデータが残らない

moconaviの独自アプリはサンドボックス化され、業務システムを安全に利用可能。



サンドボックス化されたセキュアなオリジナルアプリ

※サンドボックス：外部に影響を与えない隔離された環境



ウィルス感染リスク

端末がマルウェアに感染しても
アプリ内（＝校内）に侵入しない



Empty

端末紛失リスク

端末にデータが残らないので
紛失時のリモートワイプも必要ない

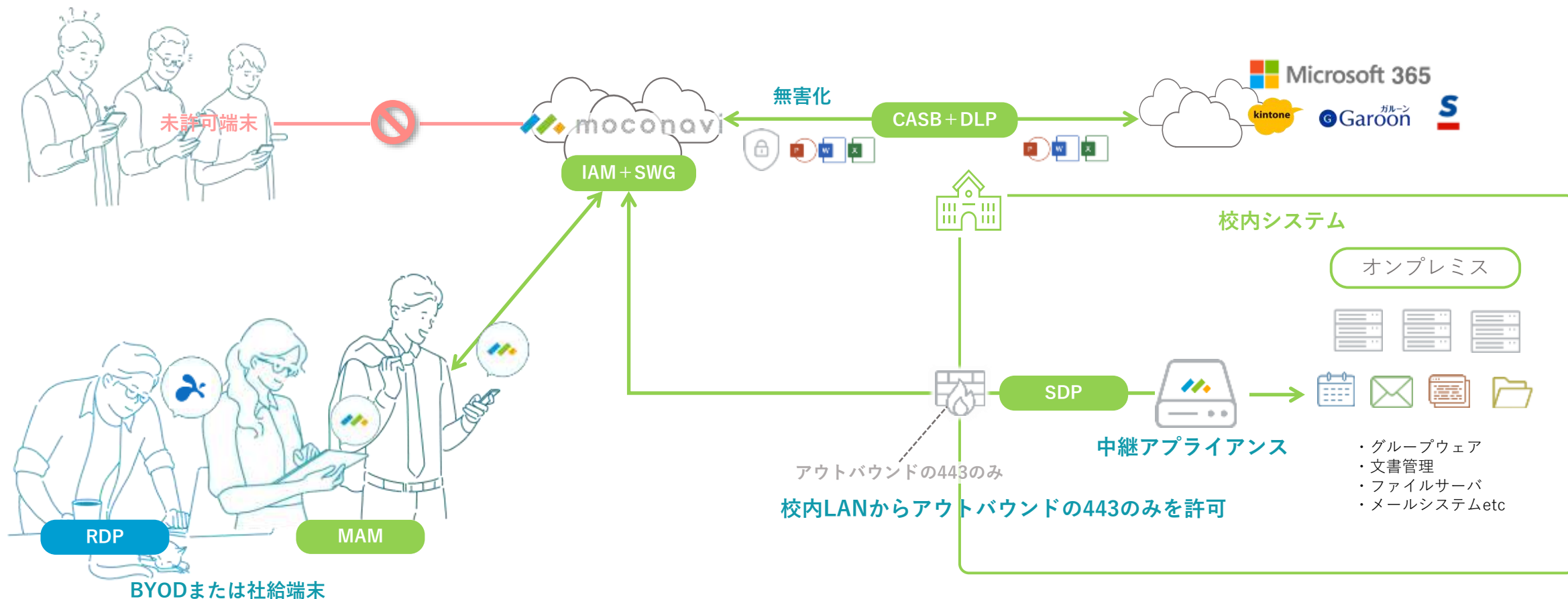


内部脅威リスク

画面キャプチャやコピペなど、ユーザ操作の
制御設定で悪意ある情報持ち出しを抑止

VPN不要、証明書不要、IP制限可能

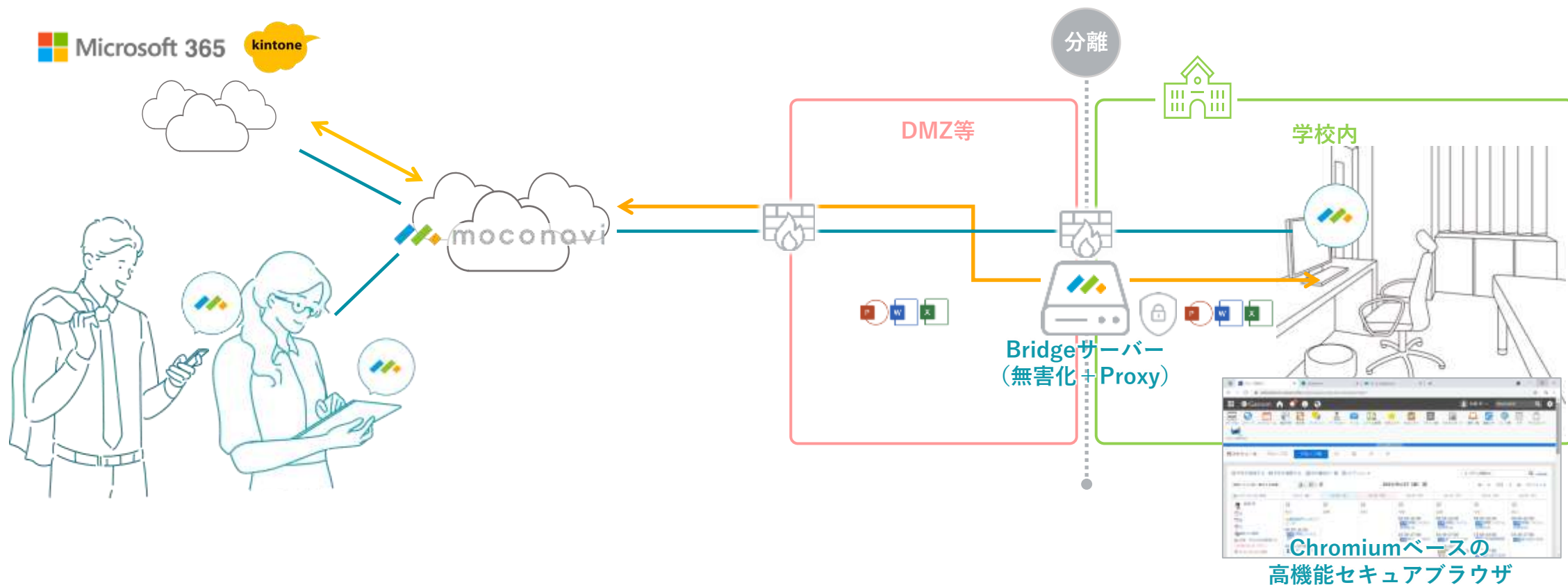
VPN不要、証明書不要で、デバイス認証とIP制限が可能！クラウドもオンプレもゼロトラストで安全に接続。



※中継アプライアンスを利用したトライアルについては個別にお問い合わせください。

校内PCからセキュアにクラウドアクセスを実現

校内からのクラウドアクセスに、moconavi Bridgeサーバーによる無害化処理と特定URLのみのアクセス制御を可能にするローカルブレイクアウト（LBO）環境の構築が可能。さまざまなクラウドサービスを利用できます。



※Bridgeサーバーを利用したトライアルについては個別にお問い合わせください。

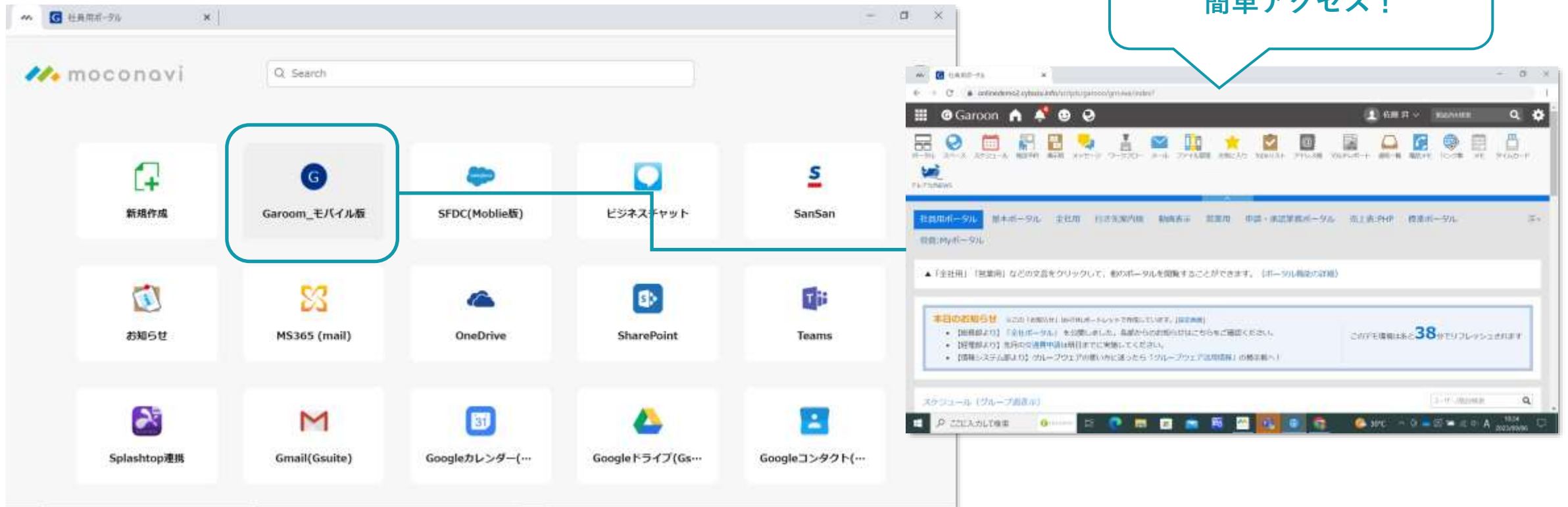
moconaviの新セキュアブラウザ「mococho (モコクロ)」



Google ChromeやMicrosoft Edgeでも採用されている**Chromium**をベースに開発。
Google ChromeやEdgeにより近い見た目や操作性を実現したセキュアブラウザです。

※Chromium・・・フリーかつオープンソースのウェブブラウザ向けのコードベース

利用アプリを集約できるmocochoホーム画面



万全のセキュリティ機能

moconaviのポリシー設定による高機能なセキュリティは
そのままだ、mococho (モコクロ) 独自のセキュリティ機能を豊富に搭載。

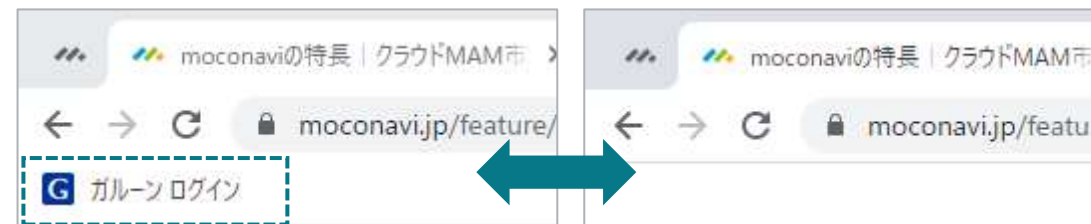
■ ウォーターマークの表示



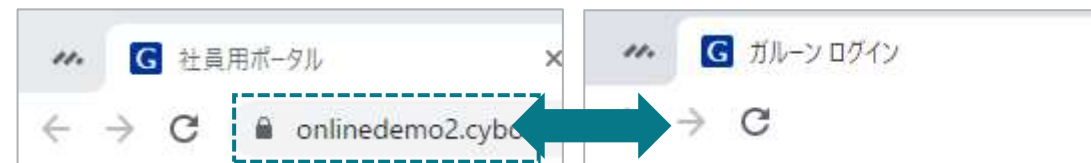
2024年4月時点の無害化対応

- Microsoft Officeファイル (doc, docx, xls, xlsx, ppt, pptx) は、拡張子そのまま無害化処理をしてダウンロード可能
- 以下の拡張子は、PDF変換することで無害化しダウンロード可能
odp, ods, odt, gdoc, gxls, gppt, xdw, xbd, pdf, jpg, jpeg, png, bmp, gif, tif, tiff, txt, csv

■ ブックマークの利用可否制御



■ URL入力欄の利用可否制御



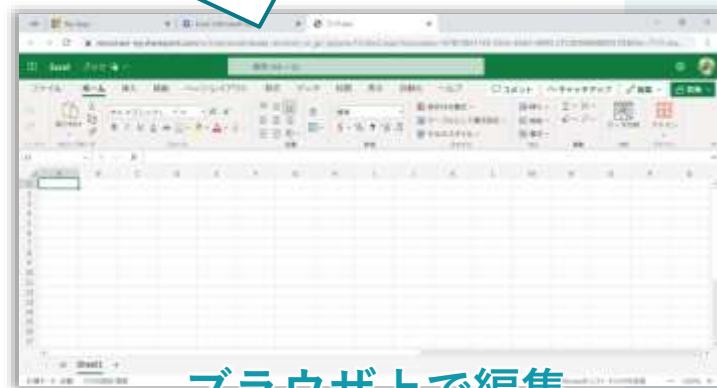
■ ダウンロードファイルの無害化



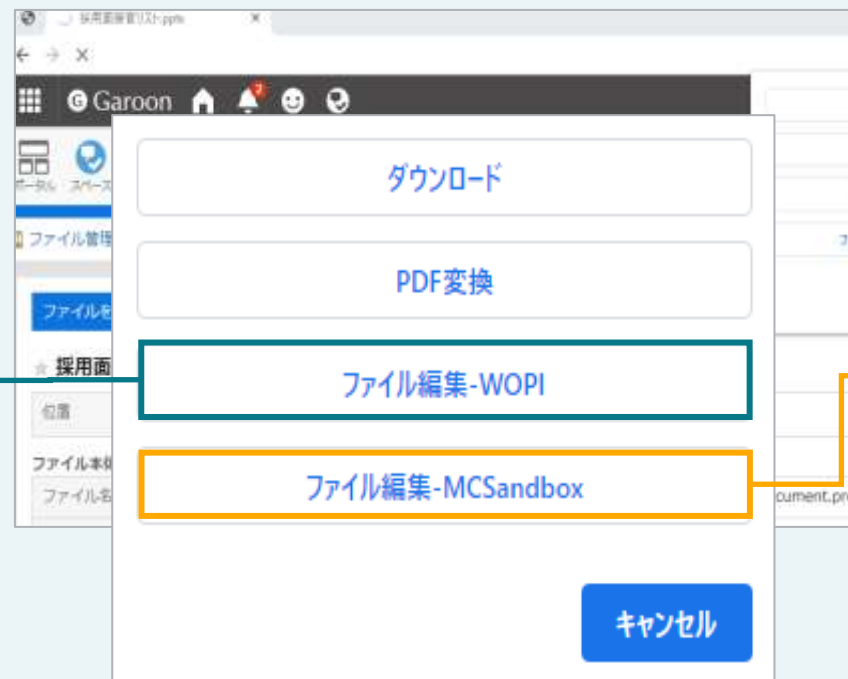
2通りのOfficeファイル編集機能を搭載

mocochro（モコクロ）にはデータを残さない、2つのOfficeファイルの編集機能を提供！
ブラウザアプリあるいは、独自のサンドボックス内でMS Officeアプリをそのまま利用する方法。

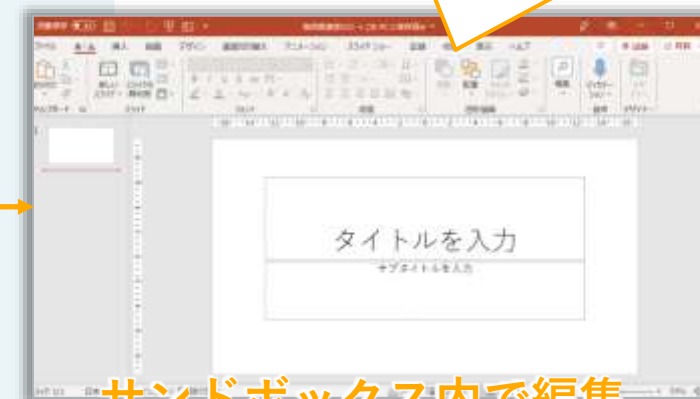
Webアプリ
を用いたファイル編集



ブラウザ上で編集



ローカルSandbox
を用いたファイル編集



サンドボックス内で編集

他社セキュアブラウザとの比較

	mococho	他社製品C	他社製品S
端末にデータを残さない仕組み	◎	△	△
データ持ち出し制御	◎	○	○
ダウンロードファイル無害化 ウォーターマーク ブックマーク・URL制御	◎	×	×
Chromiumのフル機能	◎	× (Web Viewベースの簡易版)	× (Web Viewベースの簡易版)
操作性	◎	△	△
ファイル編集機能	◎ (ブラウザ・Officeアプリの二種類)	△ 1種類 (別売専用アプリ)	△ 1種類 (別売専用アプリ)
利用可能 クラウドサービス	100種類以上	約40種類	約40種類

スマホのセキュアブラウザでこんなことも

ブラウザで閲覧可能なWebサービスであれば、多くのものがmoconaviのセキュアブラウザからご利用いただけます。

CRM



訪問先の
情報をチェック

ワークフロー



移動時間で
ワークフローの承認

勤怠管理



直行・直帰の時は
moconaviから打刻

グループウェア



校内の掲示板や
スケジュールを確認

moconavi × APIでMS365を使う

Microsoftの公開されたAPIを使って、moconaviアプリのメールやチャットクライアントがTeamsやOutlookのクライアントとして接続可能です。



API連携

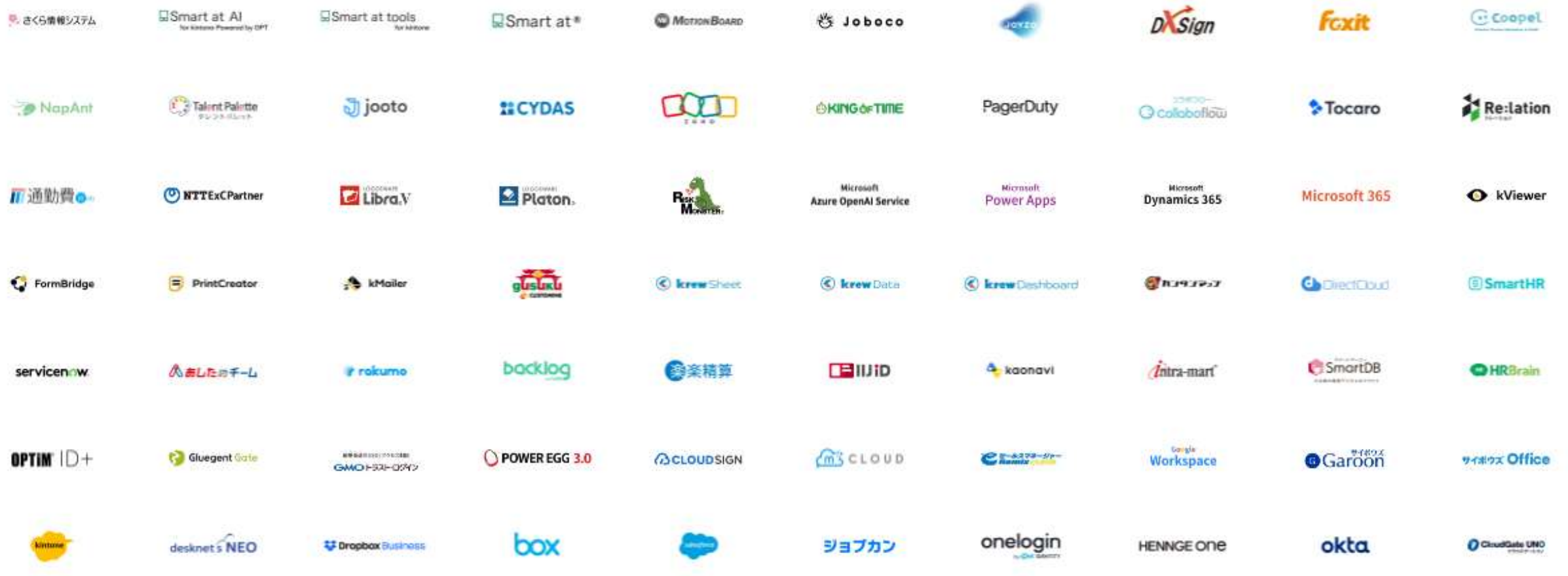


Microsoft Teams (Graph API)



Exchange online (EWS、Graph API)

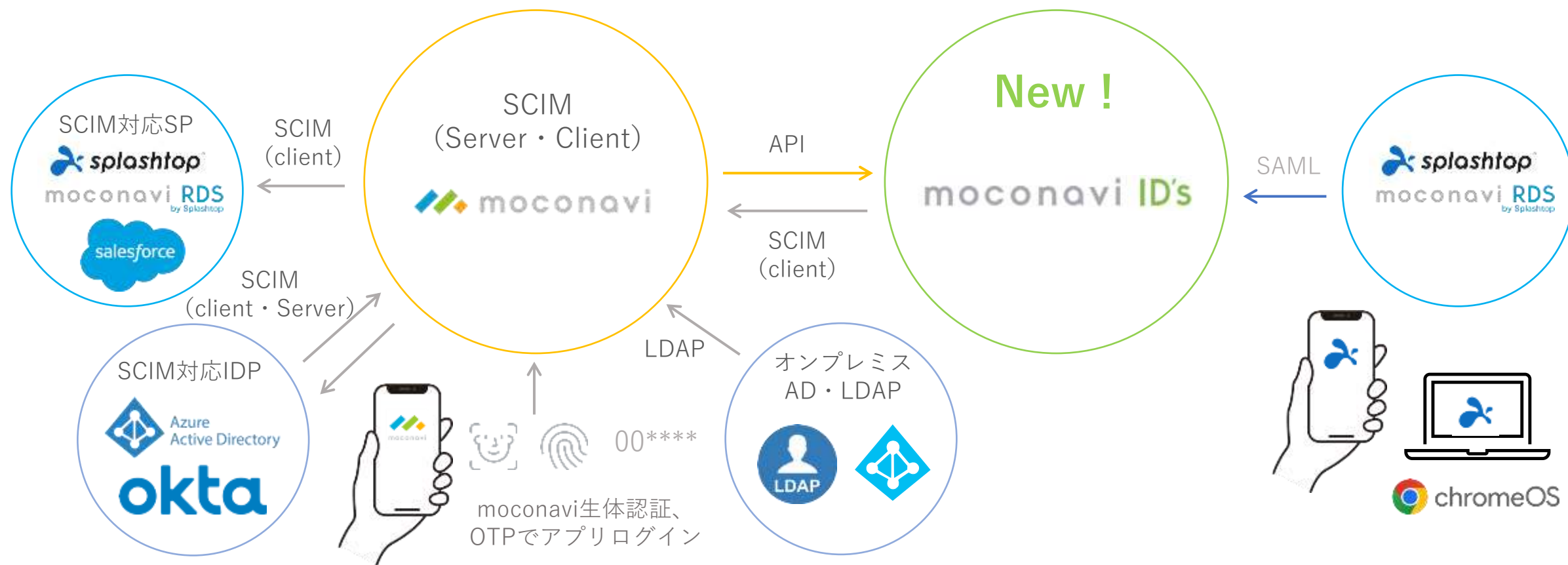
さまざまなクラウドサービスと連携



※「Chromium版ブラウザ」、「無害化」の仕様上、接続先クラウドサービスの機能に一部制限が生じるケースがございます。J-LIS申請時に簡易な検証を行っておりますが、ご利用に際してはお客様環境で事前に動作検証の上、ご利用ください。
※上記に含まれないサービスについてはお問い合わせください。

moconavi ID'sとSCIMプロトコル対応（24年8月）

SCIMプロトコルに対応したIDP機能や自社IAMサービスとのID連携も可能！
moconavi ID'sにIVRやSMS、OTPでの認証機能を実装。moconavi RDSとのSSOも検証済み。

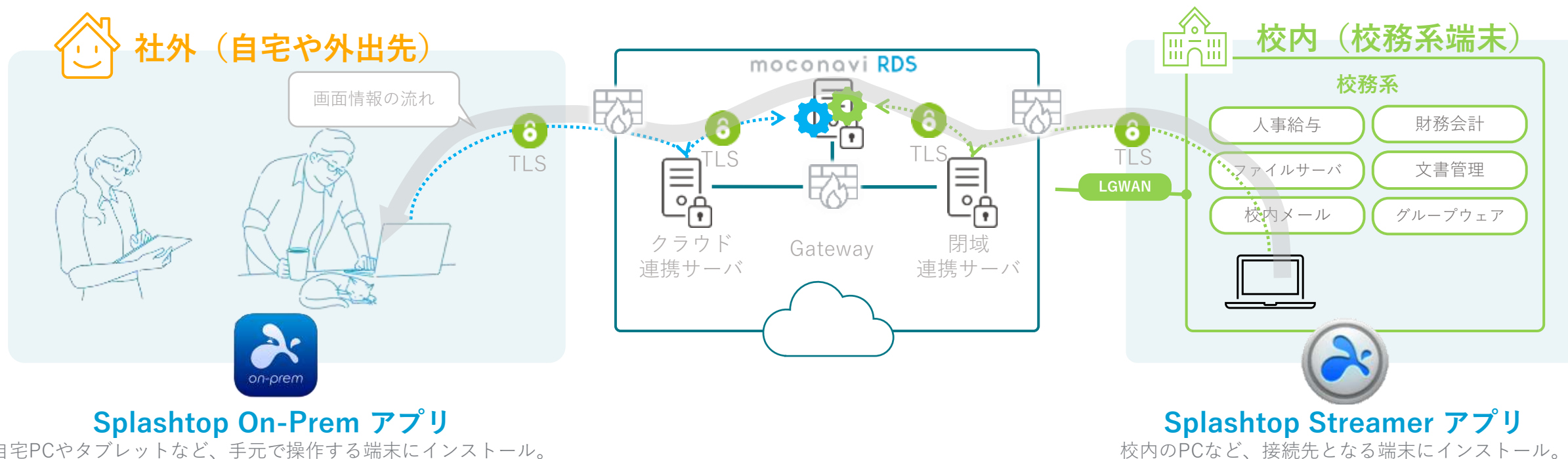


moconavi RDS

リモートアクセスサービスとは？



画面転送方式でLGWAN ASP登録済のリモートアクセスサービス。
高品質で高機能なサービスと万全のサポート体制と高い品質。もう不安はありません。



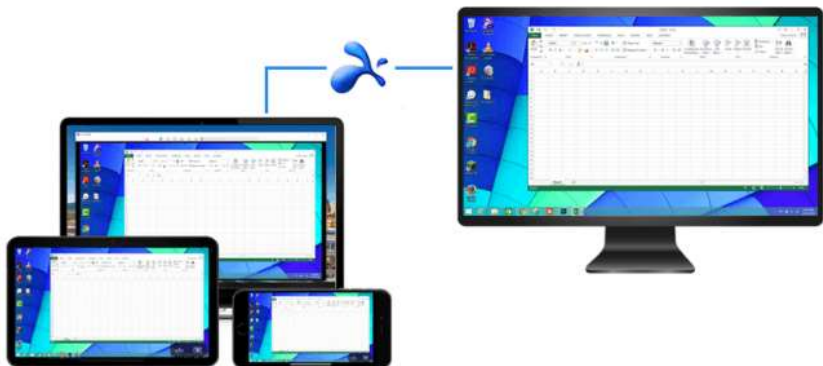
 **chromebook** にも対応！

遅延なく直感的な操作性とセキュリティ

クリエイターも認めるハイパフォーマンス

1秒あたり最大60フレームでリアルタイムに高速描写する

最新技術を採用し、画面遅延のないストレスフリーな操作性を実現します。会社で作業するのと変わらない操作性で業務効率低下の心配ありません。より繊細な画面操作が求められる映像制作の現場でも導入されています。



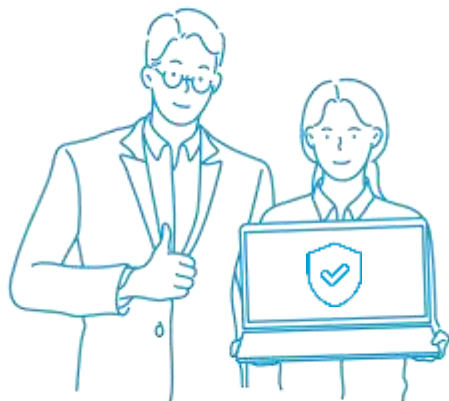
直感的なジェスチャー

iOS、Androidなどのタッチデバイスで活躍

ジェスチャーメニューでは、セッションで使用できるさまざまなスクリーンコントロールアクションが表示されます。



不正なアクセスや操作から情報を守る



堅牢な通信暗号化・認証方式

- TLS、AES256で暗号化
- ワンタイムパスワードやデバイス認証による2段階認証に対応

不正な操作への対策

- 接続先端末の画面非表示やキーボード・マウスロック
- コピー＆ペーストの禁止設定
- ウォーターマーク(電子透かし)機能
- USB等の差し込み不要
- データ持ち出し不可(クリップボード共有、プリンターリダイレクト、アップロード・ダウンロードすべて禁止！)

主な機能の紹介

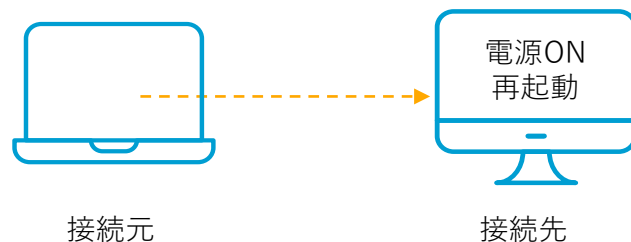
リモートウェイク

接続先PCの電源がOFFの場合、リモートで電源をONにすることができる機能。

※利用環境に条件あり

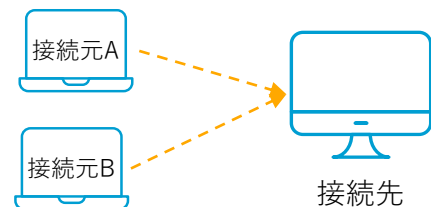
リモート再起動

StreamerやPCを再起動することができる機能。



共有機能

管理者が権限を付与することで、接続先PCに複数のユーザーが接続可能。
共有PCもこれまで通り使えます。



リモートマイク

手元のデバイス (Windows、iOS) からリモート先PC (Windows) へリモートでマイク入力が可能。これにより、リモート先のZoom、Teamsなどのリモート会議システムやチャットアプリで音声会話ができます。



ビジネス向けならではの管理者機能



履歴の確認

接続/操作/管理設定の履歴やアクティブな接続を確認する事ができます。不正アクセスやユーザーの利用状況等をリアルタイムでモニタリングする事が可能です。

端末管理

テレワーク端末やオフィスPC等の登録端末の管理ができます。企業利用端末を可視化する事により、不透明な端末での利用を防ぎます。

ユーザー管理

校内環境内へユーザーを招待し登録する事ができます。招待ユーザーに対しオフィスPCへの接続権限の有効/無効の切り替えを行うことにより、統制の取れたテレワーク環境を最小限のコストで柔軟に構築・管理する事ができます。

ポリシー設定

セキュリティポリシーを設定する事が可能です。ファイル転送機能、コピー＆ペースト機能などの各種オプションをOFF ⇄ ONするなど、各企業のポリシーに合わせた運用ルールを簡単に構築する事ができ、安全な運用を担保します。

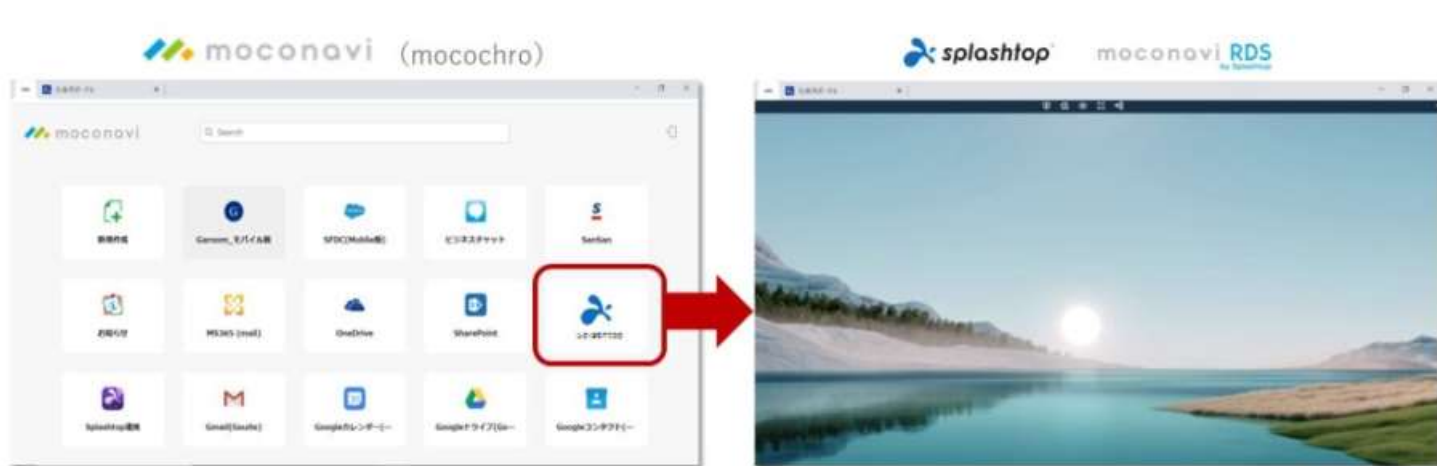
mocochro（ブラウザ）からリモートデスクトップ



moconavi RDSはブラウザから利用できる**Webアプリケーションに対応**。端末に専用アプリをインストールすることなくPCブラウザを介して接続先PCへ簡単アクセスできます。（導入時の設定にかかる手間と時間を軽減）

Chromebookからも利用可能で、mocochroと組み合わせれば、**コピー＆ペースト制御**、**画面キャプチャ制御**、**ウォーターマーク追加**のほか、Webアプリの**SSO（シングルサインオン）**が適用でき、一層高いセキュリティと利便性を実現。

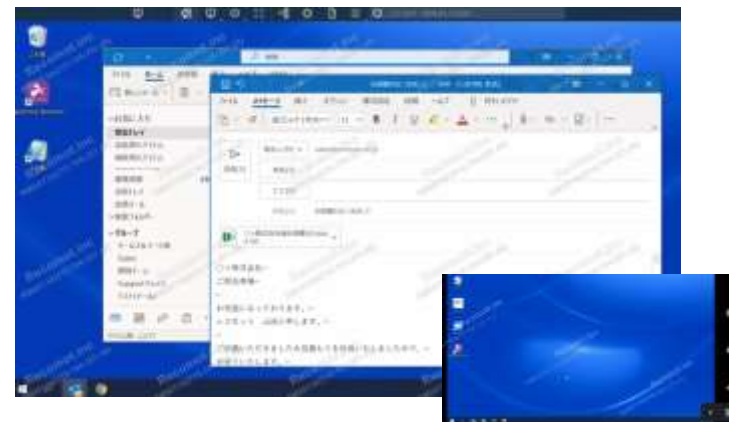
mocochroからの利用イメージ



moconaviRDSオンプレミス版の導入をご希望の場合は、レコモットまでご相談ください。

ウォーターマーク（電子透かし）の表示機能

Windows、Android・iOSに対応

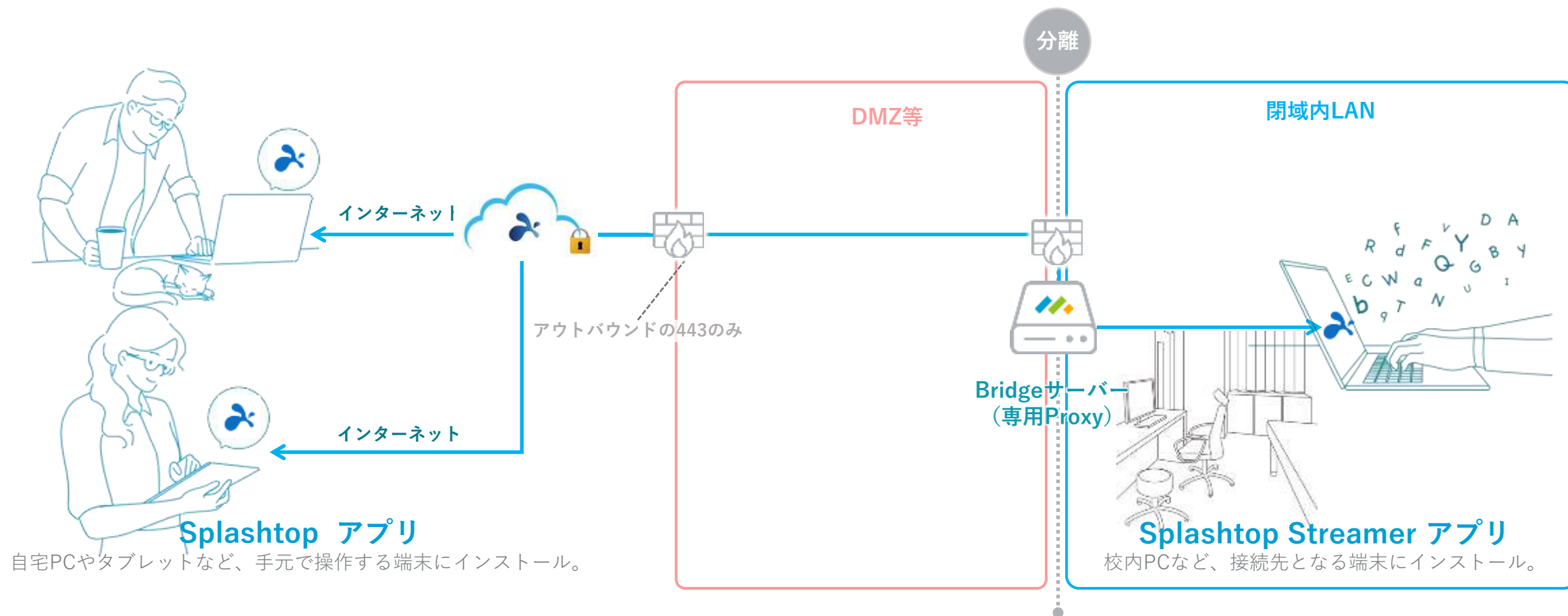


**画面キャプチャや印刷による情報漏洩を抑止
追跡に役立つ表示テキストのカスタマイズ**

（コンピュータ名/IPアドレス/ユーザアカウント名の表示が可能）

moconavi RDS BridgeサーバーによるLBO

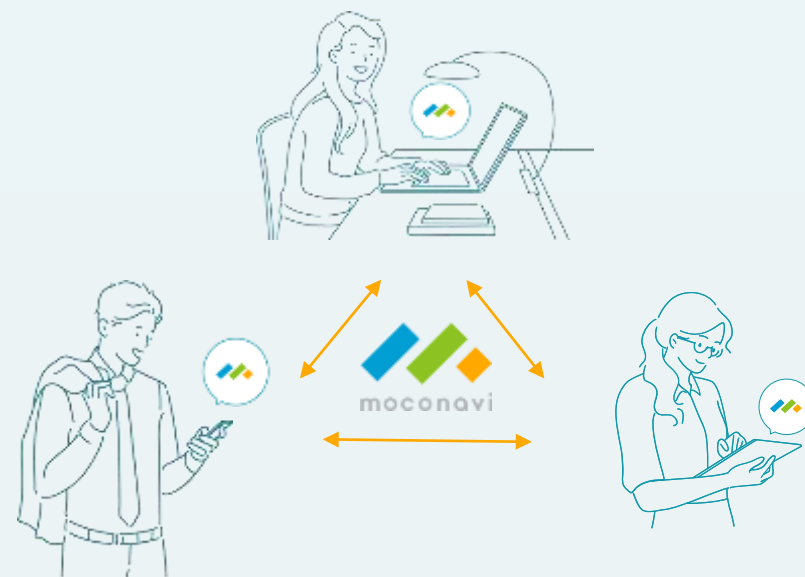
校内で物理的にネットワークが分離された環境においても、特定のURLへのアクセスのみ通す専用Proxyでリモートデスクトップのローカルブレイクアウトが可能です。VPN不要で、セキュリティリスクも低いゼロトラストなサービスです。



※Bridgeサーバーを活用したmoconavi RDSのトライアルについては個別にお問い合わせください。

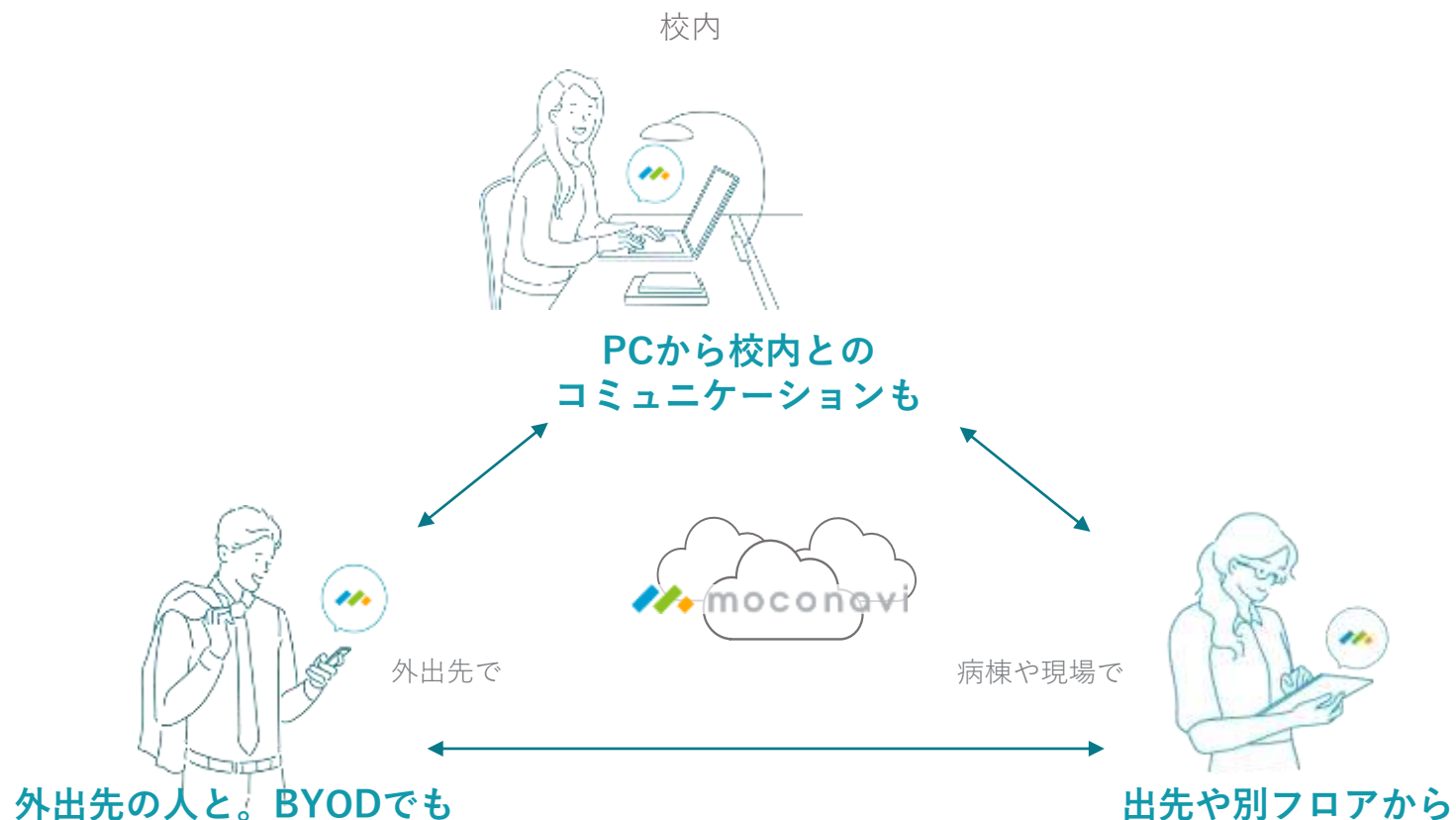


モバイルコミュニケーション機能



校内外のコミュニケーションに特化した機能をパッケージ化。

連絡先の一元管理、電話やチャット、お知らせ機能による組織内外との情報伝達をより手軽に、セキュアに行えます。IP-PBXや位置情報システム（オプション）と連携させることも可能です。



様々なコミュニケーション機能を搭載



NFC認証



クラウド電話帳



電話連携(UC)



ビジネスチャット



お知らせ機能

職員証（NFC）認証で端末所有者の問題を解決！

共有iPhoneに**職員証のFeliCa**で簡単にログイン！誰がどの端末を持っているか可視化でき、**電話番号ではなく人を探して**連絡が可能です。端末の電話帳もリセットされるので、いつでも最新の状態を維持できます。



内線番号、端末情報と利用者を自動紐付け！

今日、誰がどの端末を持っているかが分かる！

前任者の情報をクリアし、自分の電話帳を同期！

NFCと端末IDを利用した強固な多要素認証！

※NFC認証はiPhoneでご利用いただけます

クラウド電話帳とUC（電話）連携

スマホでもPCでも、セキュアなビジネスチャット

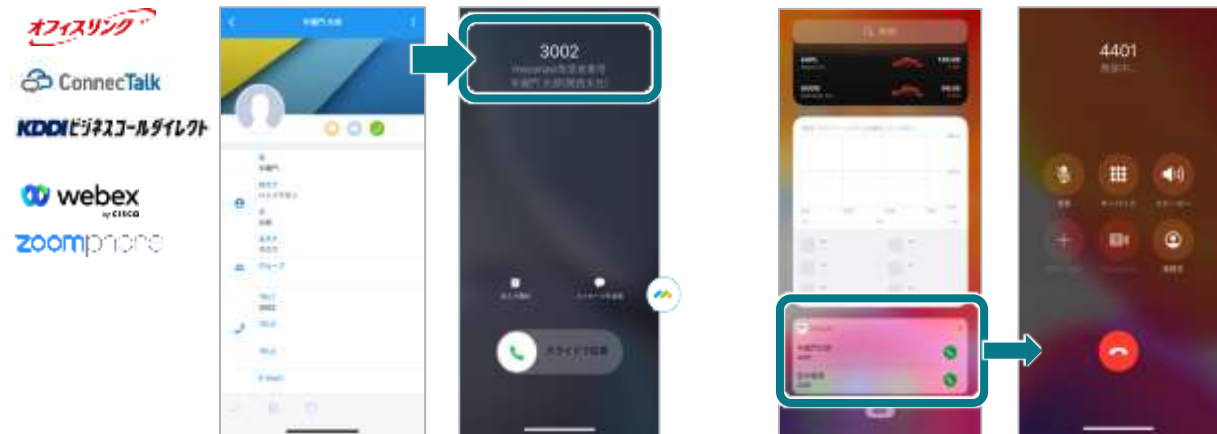
moconaviのクラウド電話帳はクラウド上で一元管理され、**個人情報**を端末に残しません。他社のグループウェアや名刺管理、**ナースコールシステム**とAPI連携し、一元管理することも可能です。



お知らせ機能、プッシュ通知とコンテンツ連携

IP PBXやモバイルキャリアなどの主要なFMC（**内線サービス**）とも連携し、電話発信や着信時の名前解決機能を実装。さらに固定内線や緊急時の連絡先をウィジェット登録し、ワンタップで発信。

moconavi電話帳登録があれば、発信者の名前を解決。さらに処置室の固定内線などの連絡先も登録できます。よく使う連絡先をウィジェットで表示し、発信も。



ビジネスチャットとお知らせ機能

スマホでもPCでも、セキュアなビジネスチャット

端末にデータを残さない**セキュアなビジネスチャット**です。**1対1の音声やビデオの通話**をサポートし、災害時の通話機能として利用可能です。PCでも利用でき、ログ管理による内部監査も可能です。



お知らせ機能、プッシュ通知とコンテンツ連携

お知らせ機能として、2パターンの情報発信が可能です。通常の情報発信だけではなく、BCPのインフラとしても活用いただけます。

掲示板のように利用し、情報に簡単アクセス



オプション) 050のBYOD通話でBCP対策

LGWANクラウドゲートウェイサービスに加えて、公私分計の050電話サービスを付与。
BYOD（個人端末の業務利用）活用でコストと利便性、セキュリティとプライバシーの保護を両立します。

着信情報表示機能



名刺スキャン機能

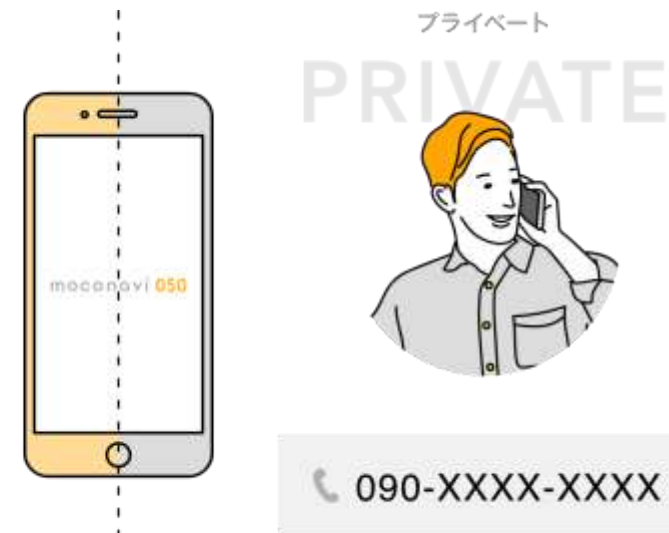


高品質な音声通話



ビジネス利用は050で発信

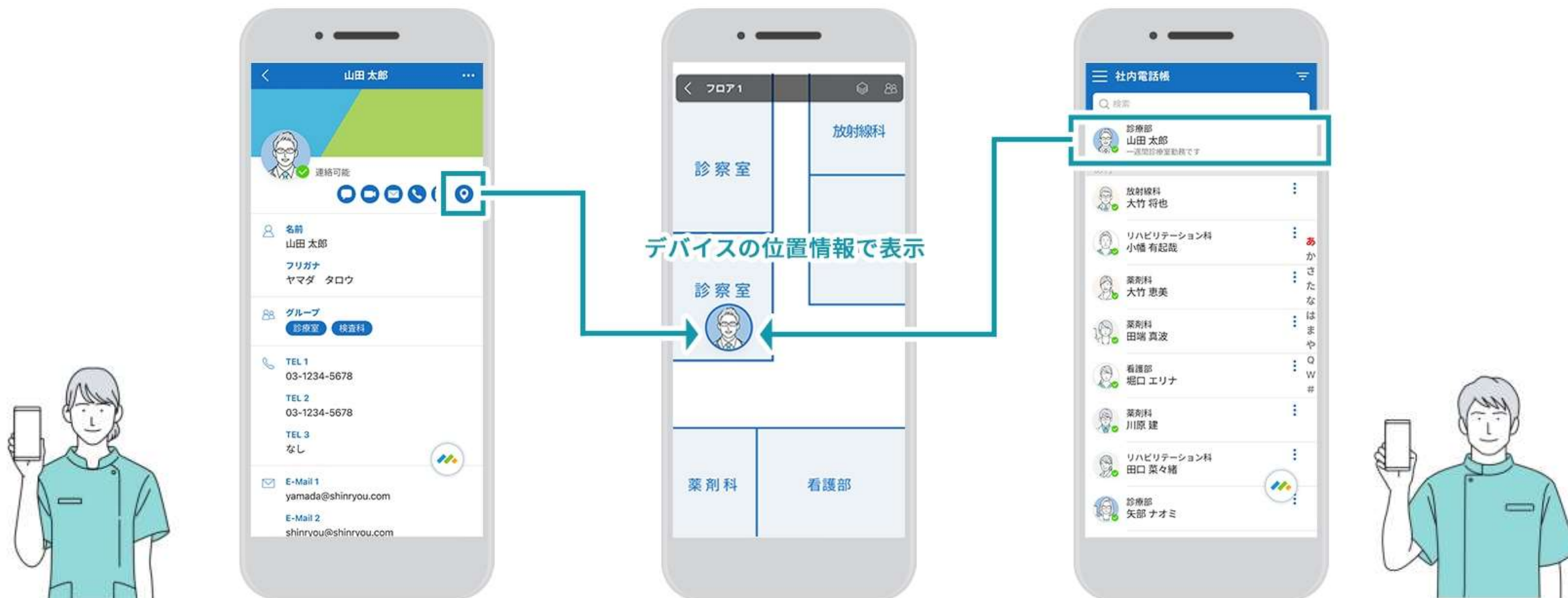
公私分計



プライベートはいつも通りに発信

位置情報連携機能（オプション）

CiscoのCMXやSpaces (※) と連携し、Wi-Fiのアクセスポイントからの三点測位で**職員の居場所**がPCやスマホから参照できます。本機能を利用するには、ライセンスの（フル機能版への）アップグレードが必要です。



※Spaces連携は今後対応予定です。最新の対応状況はレコモットまでお問い合わせください。

万全のトライアル支援体制！

製品導入の決定に向けて、トライアルから充実した支援

お客様が安心して導入を決定できるよう、トライアルフェーズでは**お客様環境との接続確認や操作確認**が実施できます。

導入フェーズとご支援の概要イメージ

製品提案

トライアル

本契約



セールス

moconaviの製品提案やご導入までの**課題整理**、**ご契約関連**についてのご案内を行います。



サポート

moconaviをご利用いただく中で発生する**個別具体のお悩みやご要望**に対して、課題解決を支援します。
製品についてのお問い合わせや、連携サービスの追加、設定変更などのご依頼もお任せください。

今いる場所がオフィスになる



※記載の各商品名・各製品名は各社の登録商標または商標です。