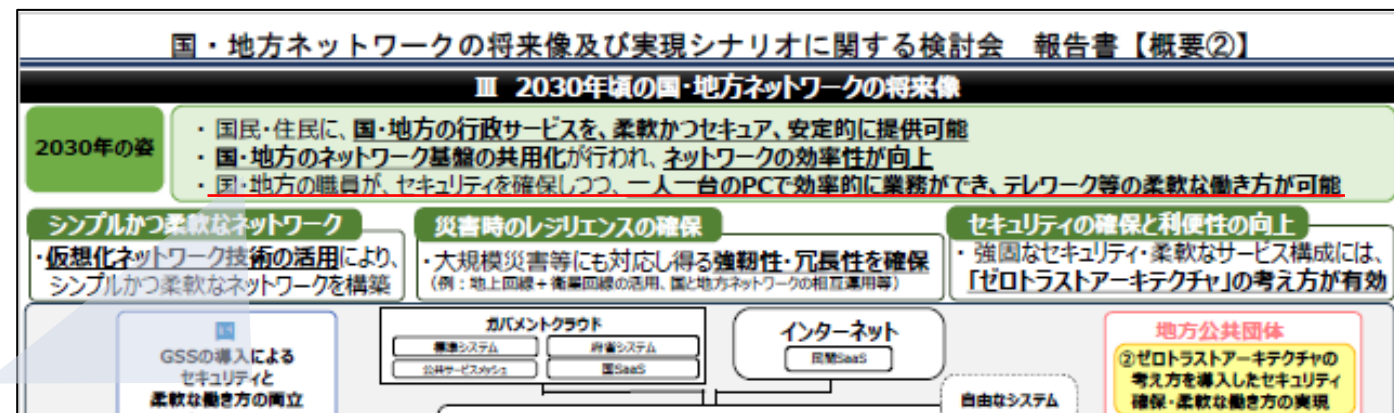


行政機関向け セキュリティソリューション



ガイドライン改定(R8.3)から端末集約の動き

□ 2030年頃に向けた国・地方ネットワークの将来像で定義された「一人一台端末」の実現



Ⅲ 2030年頃の国・地方ネットワークの将来像

2030年の姿

- ・国民・住民に、国・地方の行政サービスを、柔軟かつセキュア、安定的に提供可能
- ・国・地方のネットワーク基盤の共用化が行われ、ネットワークの効率性が向上
- ・国・地方の職員が、セキュリティを確保しつつ、一人一台のPCで効率的に業務ができ、テレワーク等の柔軟な働き方が可能

地方の負担軽減のため、仮想化技術を活用しつつ、国・地方の適切な役割分担の下、国が主体的に整備するネットワーク基盤の共用化を検討（※）

（※）GSSが国の地方機関向けに全国に整備しているネットワークや拠点について、国・地方のネットワーク基盤としての活用を検討。
その際、新技術（Beyond5G等）の活用や費用負担の在り方等も検討

国が主導で「ゼロトラストアーキテクチャ」の考え方に基づきセキュリティを強化

（※）ゼロトラストアーキテクチャの考え方の導入に当たって必要な要件等の整理、概念実証（PoC）による技術面、運用管理体制面、コスト面等に係る課題の洗い出しとその解決策の検討などを実施予定

環境としての「自由なシステム」（※）を整備

（※）行政人材によって自律的に発達するデジタル人材育成サイクルを支える仕組みや実験用ネットワーク等、他のデジタル人材に係る施策とも連携して官民人材を発掘・育成

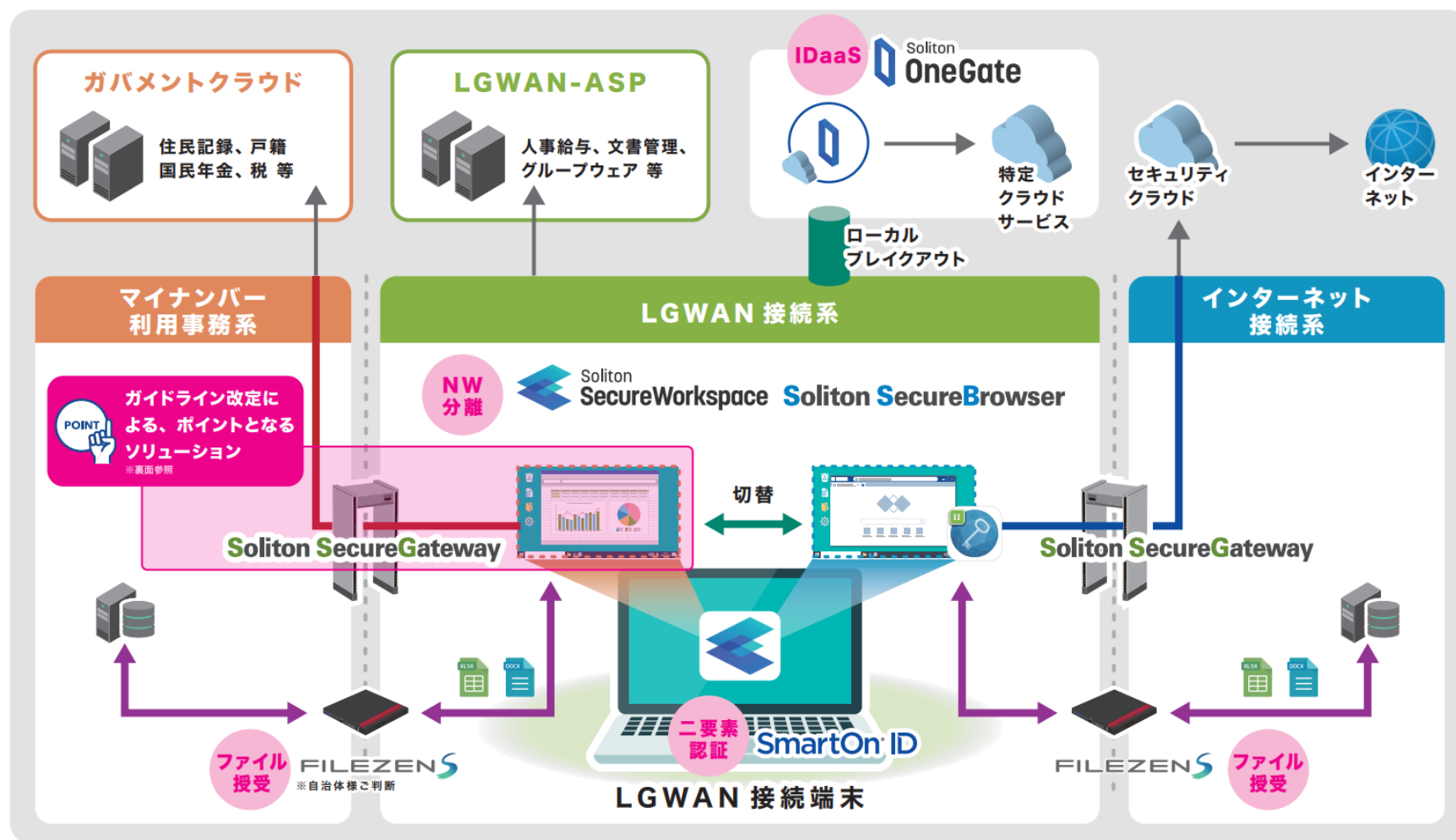
- ・LGWANが担っている重要情報のやり取りを行う機能（※）の在り方は引き続き検討（※）マイナンバー制度による情報連携、J-アラート等
- ・地方の強固なセキュリティ・さらなる利便性向上に向け、J-LIS・IPAによる共同研究・実証実験を推進
- ・ガバメントクラウド上のデータの保護のため、より一層低コストかつ安全な方法について、暗号技術を含む多角的な観点からの調査研究を実施

今後の
進め方

- ・本報告書について、地方の意見を丁寧に伺った上で、可能なものから速やかに上記実証等を実施
- ・標準化に取り組む地方の負担やネットワーク更改時期等を考慮した上で、新たなネットワークへの移行は、分散・段階的に実施

2

端末集約、クラウドサービスの本格的な利用も視野に 端末は分散から集約へ (αモデルの場合)



ソリトンが考える自治体情報セキュリティ考察

マイナンバー利用事務系へ
他セグメントからのアクセス

示された通信経路パターン

通信経路パターン

✓ 接続要件の検討にあたっては、利用形態としてDaaSも想定し、下記の通り10パターンの通信経路についてリスク分析を実施。

	接続元 (業務端末の設置場所)	画面転送の方式	ページ
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする	P16
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする	P25
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合	P34
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P42
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合	P52
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P61
通信経路(5)	LGWAN接続系	オンプレミス画面転送 (VDI/SBC) インターネット接続系に端末が残る場合を(5)'とする	P72
通信経路(6)	インターネット接続系	オンプレミス画面転送 (VDI/SBC)	P78
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする	P86
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ	P93

➡ DaaS利用は検討・調整事が多い

- 例: ①従量課金の場合、コスト積算が難しい
②固定料金プランは高い
③インターネット接続系を接続元にした場合は
自治体セキュリティアクラウドとの調整が必要

➡ VDI/SBCの価格高騰がネック

➡ 追加されたセキュアブラウザ方式

15

※マイナンバー利用事務系に係る画面転送方式の方式について P16

【参考】端末仮想化の定義

端末仮想化の各方式

方式	概要	
DaaS (Desktop as a Service)	仮想デスクトップ環境をクラウドサービスとして提供すること ガバメントクラウドのCSPにおいて、DaaSを提供している事業者も存在する	
オンプレミス仮想デスクトップ※	VDI (Virtual Desktop Infrastructure) サーバOS上でユーザ数分の仮想デスクトップを構築し、業務端末から利用する SBC (Server Based Computing) サーバOS上でマルチユーザーに対応した仮想環境を構築し、複数台の端末で共有する	
セキュアブラウザ	手元の端末に専用ブラウザをインストールすることで隔離された領域を確保し、専用ゲートウェイを介して、その領域内でWeb上のドキュメントやデータを表示することで、セキュアにWeb閲覧を行う ※サーバOS上のブラウザをセッション単位に仮想化する方法もある	

※VDIとSBCの違いは、主にOS上で仮想デスクトップを作成する単位（ユーザ数分作成かマルチユーザか）であるため、リスク評価上は同じ方式として扱う。

(注7) 仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。クライアントPCに設けられた隔離領域（コンテナ、仮想マシン等）で動作し、無害化されていないファイルのダウンロードや端末内のデータの漏洩が不可能なよう設計されたブラウザと、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイとの組み合わせで構成されたシステムであるセキュアブラウザも、アプリケーション仮想化の一種と考えることができる。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

※地方公共団体における情報セキュリティポリシーに関するガイドライン(令和7年3月版) P145

※マイナンバー利用事務系に係る画面転送方式の方式について P6

- 端末仮想化方式は、DaaS、オンプレミス仮想デスクトップ、セキュアブラウザの三方式
- 仮想方式の実現方法は問わない
- セキュアブラウザはアプリケーション仮想化の一種と考えられる

(隔離領域で動作、データの漏えいが不可能なよう設計されたブラウザ、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイとの組み合わせで構成されたシステムであることが前提)

【必須技術的対策項目とソリトンのソリューション】

NetAttest EPS

通信経路 (7) LGWAN接続系端末に1 台化 オンプレミス セキュアブラウザの対策イメージ

- ## 対策の実施場所



通信経路(8)

□ セキュアブラウザであればコストを抑えつつ導入が可能

【必須技術的対策項目とソリトンのソリューション】



Soliton SecureGateway

LGWAN接続系端末 セキュアブラウザでの対策	
画面転送機能	端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。
セキュアブラウザの選定	ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。
セキュアブラウザ基盤の脆弱性対応	セキュアブラウザ基盤の脆弱性にパッチを適用する。
セキュアブラウザでの不正プログラム対策	ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行う。
アクセスログ	不正アクセス等による被害の防止等のため、セキュアブラウザのアクセスログを取得し、確認する。

NetAttest EPS

VPN端末での対策

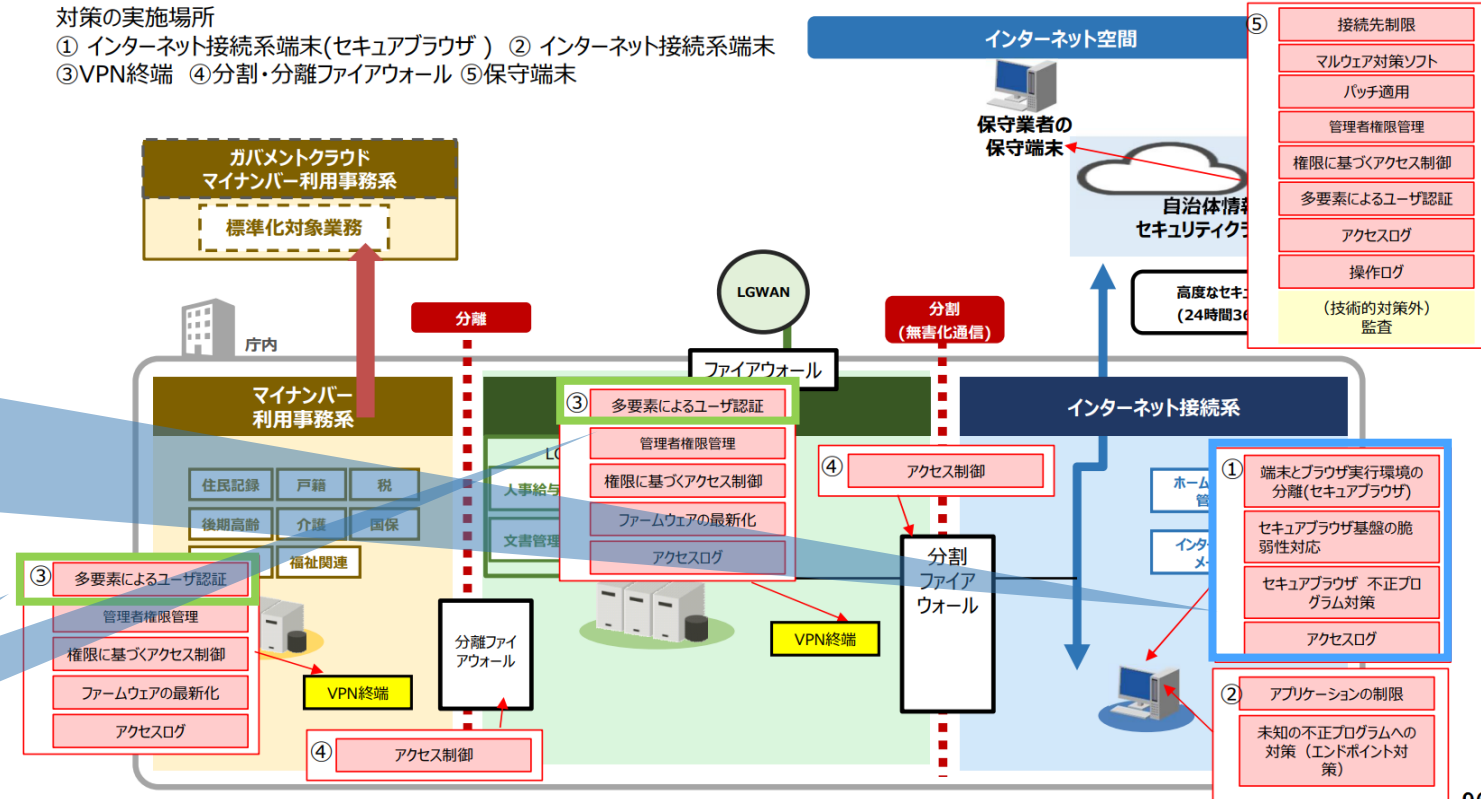
多要素によるユーザ認証	VPNのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。
-------------	--

通信経路 (8) インターネット接続系端末に1台化 オンプレミス セキュアブラウザの対策イメージ

- ✓ インターネット接続系からオンプレミス セキュアブラウザに接続する方式。
- ✓ インターネット接続系へのLGWAN接続系からの画面転送はβモデルとしてガイドラインに規定済。
- ✓ マイナンバー利用事務系からの画面転送を行うにあたり、リスクアセスメント結果を踏まえると、βモデルの対策に、以下の図に示す対策を追加で実施する必要がある。

対策の実施場所

- ① インターネット接続系端末(セキュアブラウザ) ② インターネット接続系端末
③ VPN端末 ④ 分割・分離ファイアウォール ⑤ 保守端末



Solitonから提案する二つの製品

□ お客様の実施したい業務によって選択可能

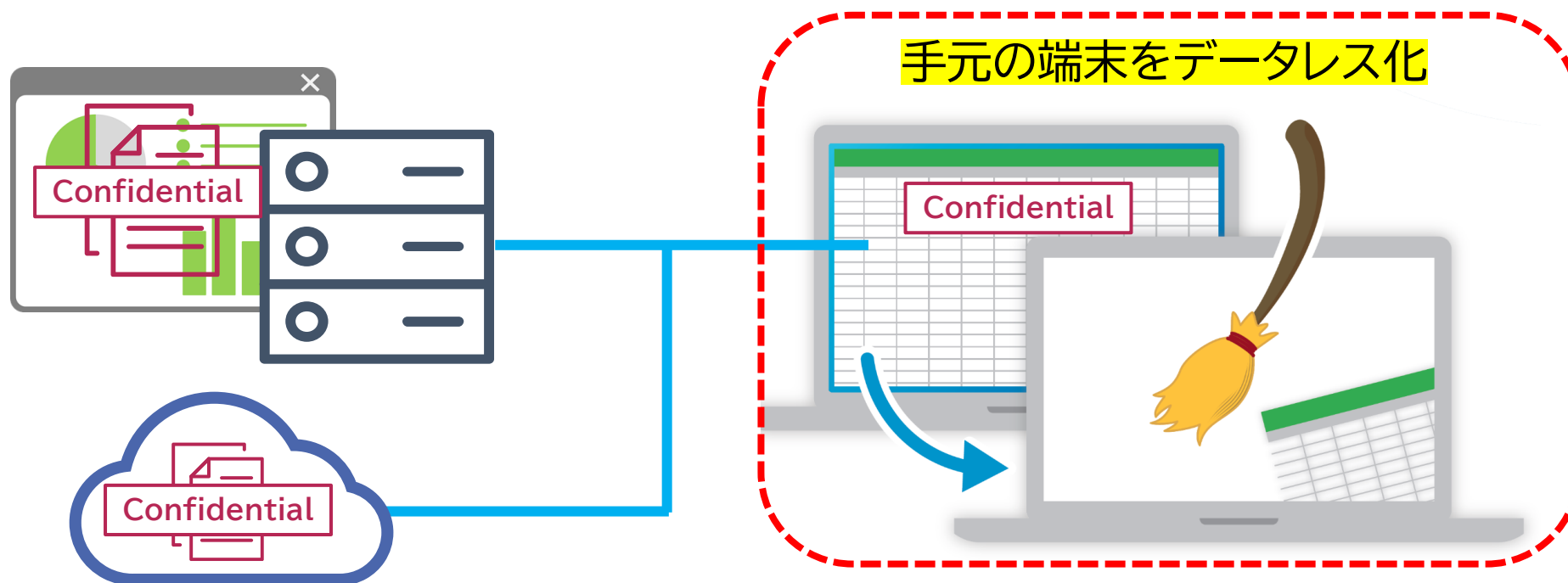
- ローカル端末にコンテナ領域を展開、アプリケーション(**セキュアブラウザ**や**RDP**)を稼働する
Soliton SecureWorkspace
- ローカル端末にコンテナ領域を展開、**セキュアブラウザ**を稼働するSoliton SecureBrowser

	ソリューション	説明	導入コスト
 画面転送	仮想デスクトップ(VDI)方式	仮想化基盤に集約された端末をリモートから操作	高
	アプリケーション仮想化(SBC)/RBI方式(Remote Browser Isolation)	サーバー側で実行されるアプリやブラウザをリモートから操作	高
	リモートデスクトップ方式	別ネットワークの端末をリモートから操作	中
 端末内仮想化	セキュアコンテナ方式 	ローカル端末に隔離環境を作り アプリケーション を稼働	中
	セキュアブラウザ方式 Soliton SecureBrowser	ローカル端末に隔離環境を作り ブラウザ を稼働	低

セキュアブラウザ・コンテナの特徴

動作の主体はあくまで手元の端末側

データの隔離や消去もクライアントソフトウェアで行う。**クライアント主体のアプローチ**



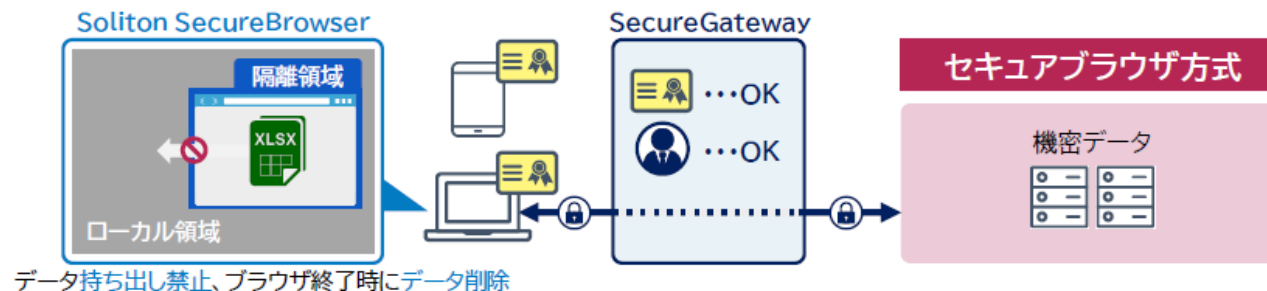
- 大規模なサーバーなどの物理リソースを抑制。導入・運用しやすい
- VDIやSBCと比べてライセンスに係るコストが安価
- 手元のFAT端末の処理性能をフル活用するため、生産性が高い

➡ 但し、上手く動かないアプリがあるため・・・**RDPも活用**

ソリトンセキュアアクセス(SSA)シリーズ

Soliton SecureBrowser

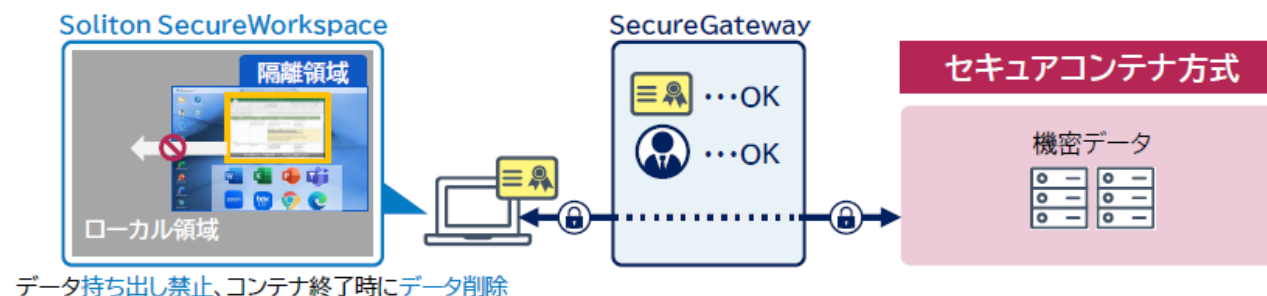
- セキュアブラウザはPCだけでなく
スマホ・タブレットにも対応
- 場所・デバイスを問わない柔軟な働き方で、
業務効率化を支援



接続先デスクトップ
不要

Soliton SecureWorkspace

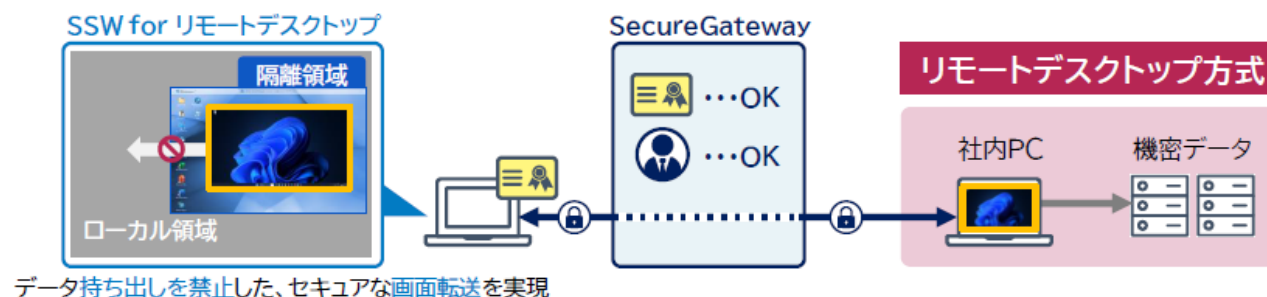
- いつものOfficeアプリでデータ編集し、
ファイルサーバーへのファイル保存が可能
- 端末内分離するセキュアコンテナ方式



接続先デスクトップ
不要

Soliton SecureWorkspace for Remote Desktop

- いつものPCを画面転送方式で操作
- 情報漏えいをブロックする隔離領域で動作、
強固な認証・暗号化通信で安全に利用可能



接続先デスクトップが
必要

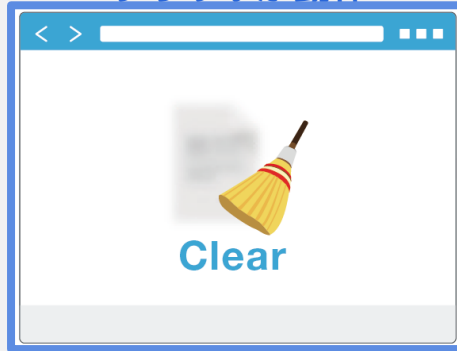
VDIレベルの
安全性を低コストで

ソフトウェアの技術で、端末にデータを残さないセキュアな業務環境を提供

ガイドラインへの対応

セキュアブラウザ方式

仮想分離領域内で
ブラウザが動作



ブラウジング
のみ

セキュアブラウザ

手元の端末に専用ブラウザをインストールすることで隔離された領域を確保し、専用ゲートウェイを介して、その領域内でWeb上のドキュメントやデータを表示することで、セキュアにWeb閲覧を行う
※サーバOS上のブラウザをセッション単位に仮想化する方式もある

※VDIとSBCの違いは、主にOS上で仮想デスクトップを作成する単位（ユーザ数分作成かマルチユーザか）であるため、リスク評価上は同じ方式として扱う。



※マイナンバー利用事務系に係る画面転送方式の方式について P6(抜粋)



専用
ゲートウェイ

Webサイト
SaaS
クラウドサービス

通信は限定
(汎用ブラウザなどの通信は制御)

デスクトップ
アプリも使える

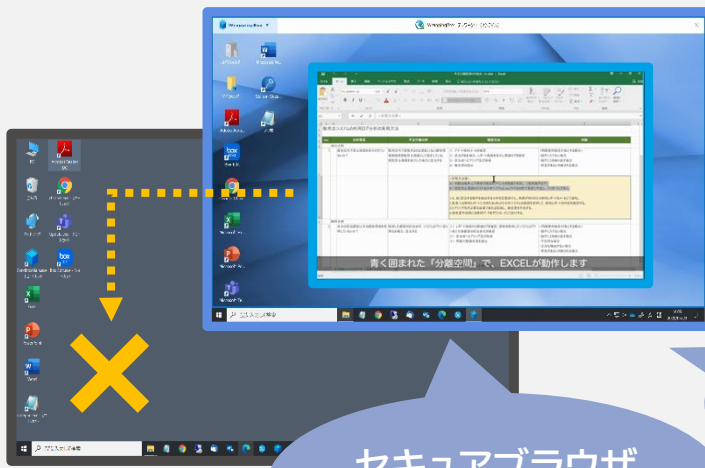
リモート
デスクトップも
使える

セキュアブラウザ
も使える

端末ローカルへのデータ保存を制御
マルウェアなどの脅威を仮想分離領域内に隔離
アプリを終了したらキャッシュはすべて消去

セキュアコンテナ方式

仮想分離領域で業務

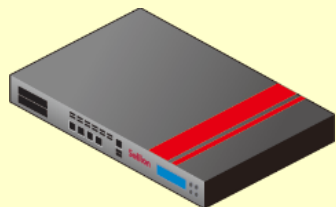


細かなところですが

ソリトンのサーバーアプライアンスは特定用途向けに専用機化

汎用サーバーとは異なる様々なセキュリティ対策や運用の利点をもたらします。

Soliton SecureGateway



ガイドラインが要求する技術的対策にも対応

- (1) クライアント証明書とIDパスワードによる2要素認証に対応
- (2) TLSベースの独自プロトコルでセキュアブラウザとゲートウェイサーバー間の通信を保護(VPN相当)

コスト削減

運用負荷低減

納期問題対応



通信経路 (7) LGWAN接続系端末に1台化 オンプレミス セキュアブラウザの技術的対策②

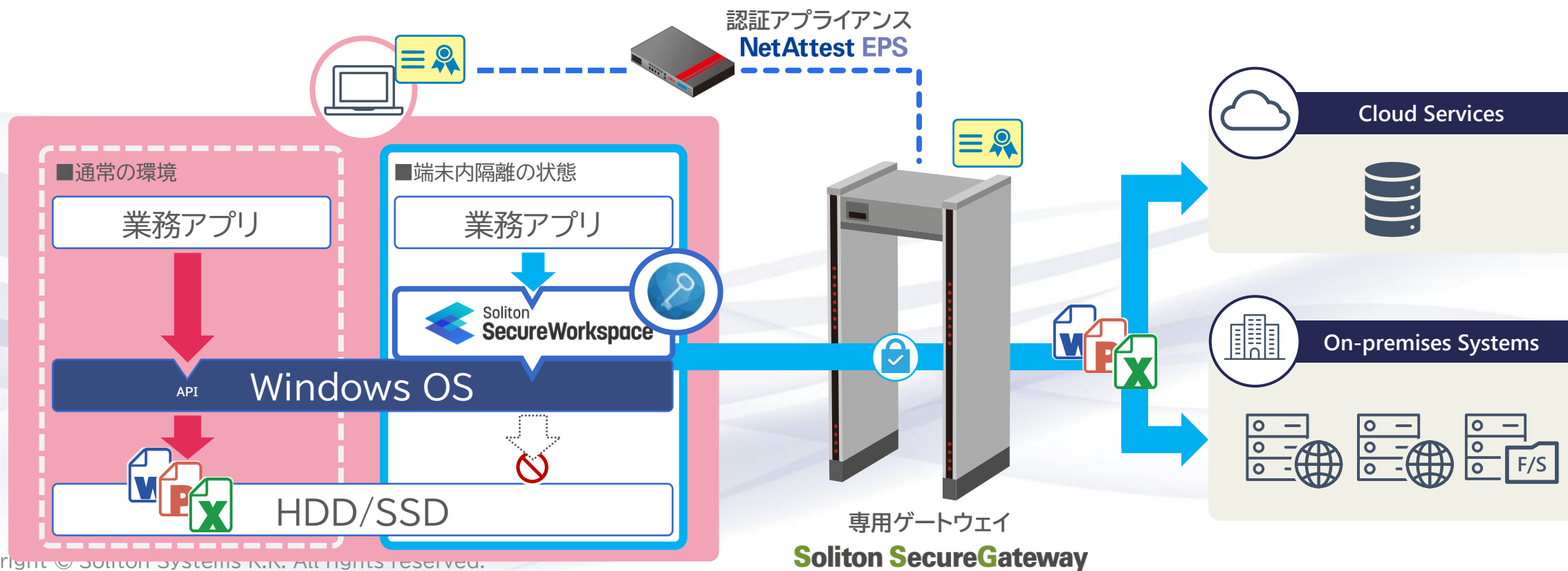
(1) 技術的対策 (前項からの続き)

技術的対策	対策の定義	「特定個人情報に関する安全管理措置 (行政機関等編)」との関連	必須	推奨
VPN終端での対策 (続き)				
ファームウェア最新化	VPN終端の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	

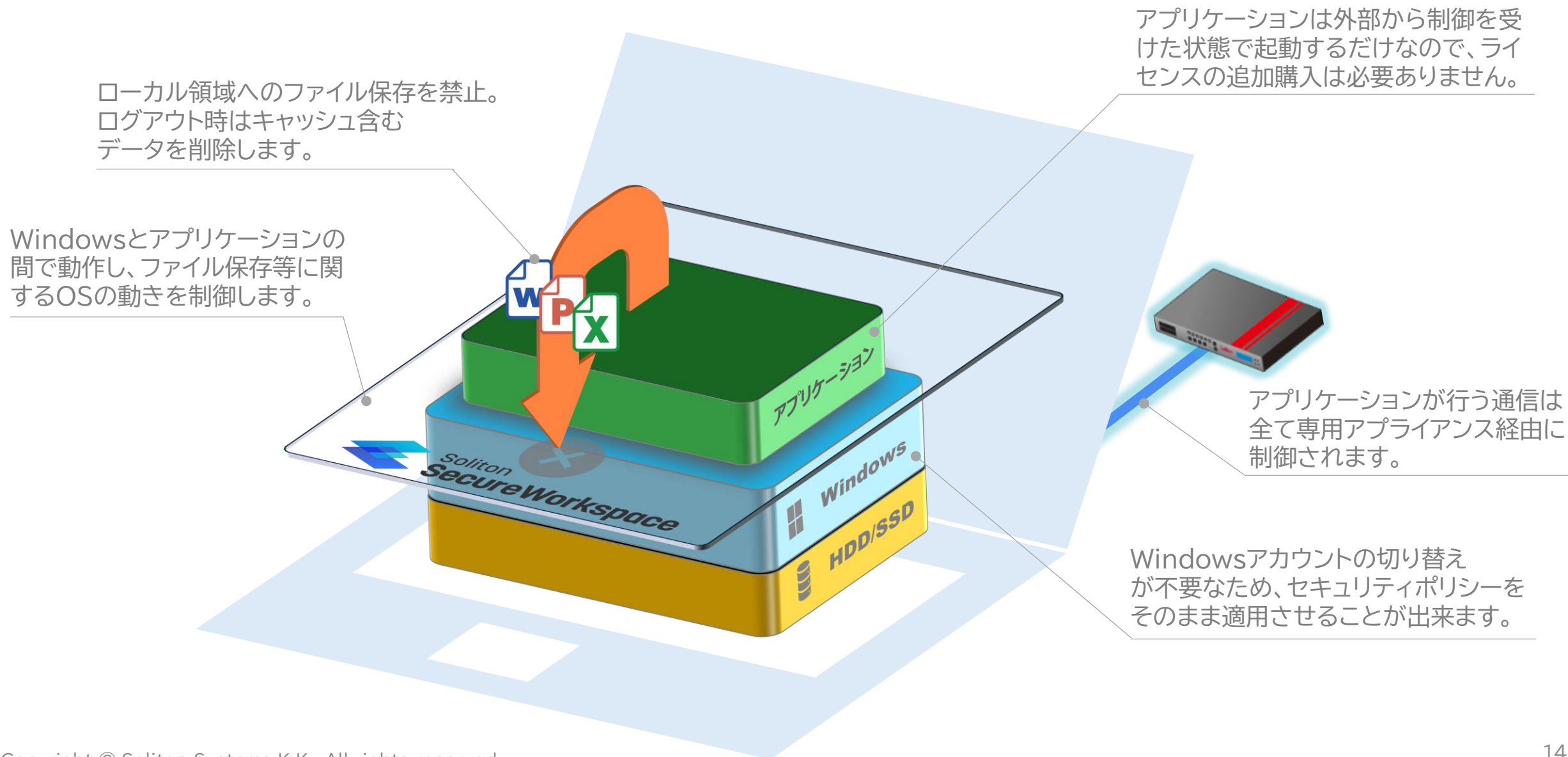
脆弱性対応は導入後の運用、監査対応でも必須

Soliton SecureWorkspace

- ブラウザ、Officeアプリ、Web会議などが**普段通りの操作感**で利用可能
- 制御下にあるアプリケーションは**ローカル領域へのファイル保存が出来ません**
- ファイルの引き渡しは不可能だが**テキストのみ許可する**、といった制御が専用ゲートウェイによって可能
- 専用ゲートウェイのアクセスには電子証明書を利用した**多要素認証**を行うことも可能
- セキュアコンテナ内の稼働アプリに**セキュアブラウザ**を内包

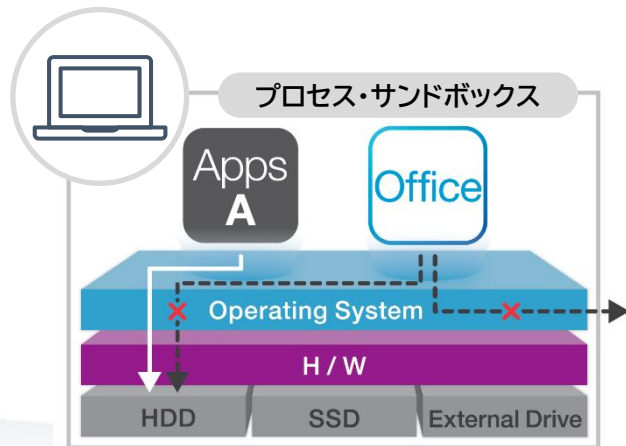


隔離領域の仕組みについて



Soliton SecureWorkspaceのセキュリティ技術

カーネルレベルのプロセス監視



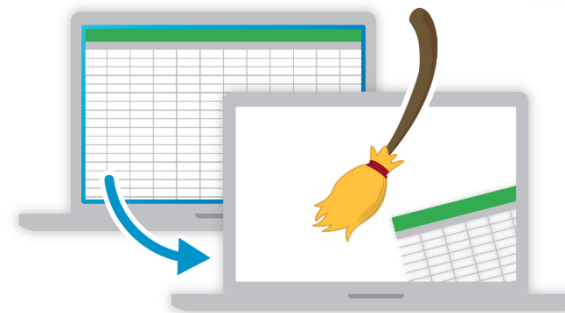
ガイドライン上の【技術的対策の定義】

ディスク領域(ファイル・レジストリ)の分離、メモリ領域の分離(プロセス分離)、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。

隔離環境内で動作しているアプリケーションの出入り口を『カーネルレベル』で監視し、情報漏えいにつながるプロセスの動作を制御します。

ファイル保存 / クリップボードコピー / レジストリ編集 / プリント / ネットワーク接続 / COMアプリ呼び出し

データの自動消去



ガイドライン上の【技術的な留意点】

画面転送システムの仮想機能(仮想端末、分離領域でのブラウザ等)は、利用後に仮想機能を第三者に悪用されることを防ぐため、手元の端末で仮想画面を閉じた際は、仮想機能もログオフする(手元端末から画面転送機能の利用終了時には仮想機能も終了する)。

作成・編集したファイルは隔離領域に。アプリケーションを閉じるとログオフ、読み書きしたデータは自動で消去します。



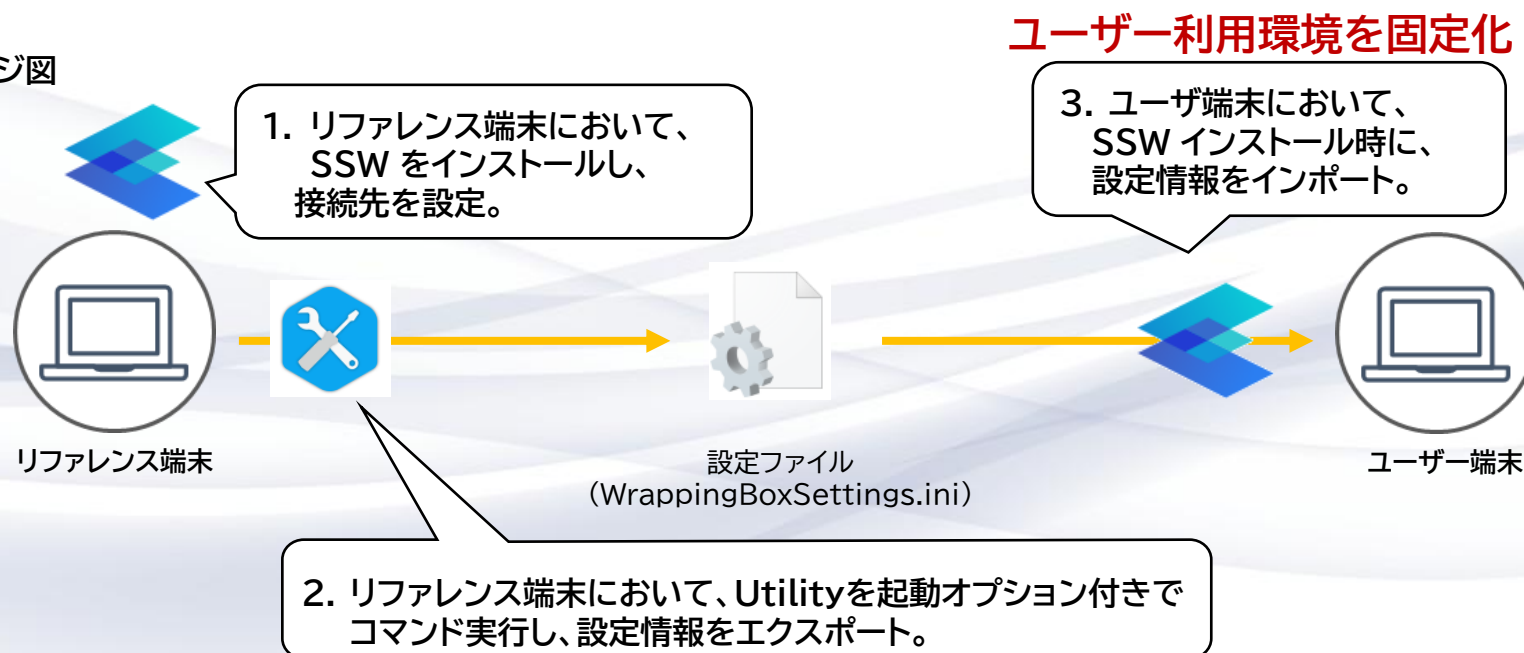
COM【(Component Object Model):ソフトウェアの機能を部品化し、他のソフトウェアから利用できるようにする仕組み。】経由のアプリケーション機能の呼び出しを制御。例えば、OfficeファイルからXPS文書やTIFF形式に変換して保存する際のデータのやり取りは、COMを利用して行われます。利便性を高める仕組みである一方、COM経由のデータ受け渡しが情報漏えいの糸口になることが課題となっていました。
特許第6104447号:<https://ipforce.jp/patent-jp-B9-6104447>

特許技術の高度なセキュリティ

(ご注意)Soliton SecureWorkspaceの利用にあたって

- Soliton SecureWorkspaceはUtility機能でネイティブアプリを任意に追加登録することが可能ですが、管理者もしくは運用ベンダー様で動作確認・検証作業をいただき、問題がない事を確認した上で追加登録の判断をお願いします。
- また利用者がUtility機能で個人の判断でアプリを登録することが出来ないよう、設定配布情報機能を利用してユーザー利用環境を固定化することをお奨めします。

手順イメージ図



Soliton SecureBrowser

- 端末にデータを残さない、**オリジナルセキュアブラウザ**
- 描画については**Edgeベース**のエンジンを利用しており、Web閲覧の再現性も考慮
- セキュアブラウザから**ローカル領域へのファイル保存はできません**
- 専用ゲートウェイのアクセスには電子証明書を利用した**多要素認証**を行うことも可能



【参考】VDIとの比較

	必要 コンポーネント	オフライン対応	アプリケーション の動作検証	操作性	ライセンス費用
	環境の構築に必要な ソフトウェア/ハードウェアの 構成要素	作業中の通信途絶、 瞬断の影響	導入前検証の 要否・検証のしやすさ	動画再生・オンライン会議	
	- クライアントソフトウェア - 専用ゲートウェイ プライアンスのみ	ログインやファイル保存 時のみ通信を行うため、 通信が途絶しても作業状 態を維持、通信帯域も抑 制できます。	必要 専用アプライアンスとク ライアントソフトのみで事 前の動作検証が可能	テレワークに必要なオン ライン会議もストレスな く利用可能 ※ブラウザ版推奨	ゲートウェイアプライアンス ¥1,200,000/台 +ユーザーサブスクリプ ション ~¥13,200/年 VDIと比べ 10分の1程度 ※当社比
VDI	- 中央管理サーバー - ハイパーバイザー - エージェントソフトウェア - クライアントソフトウェア - 追加PC - etc,etc,etc...	画面転送方式のため、 常にオンラインである必 要があります	必要 動作検証を行うには本番 と同じ環境を構築する必 要あり	画面転送方式のため、動 画再生やオンライン会議 に不向き	- 高額なライセンス 費用 - 為替影響 - 価格改定...

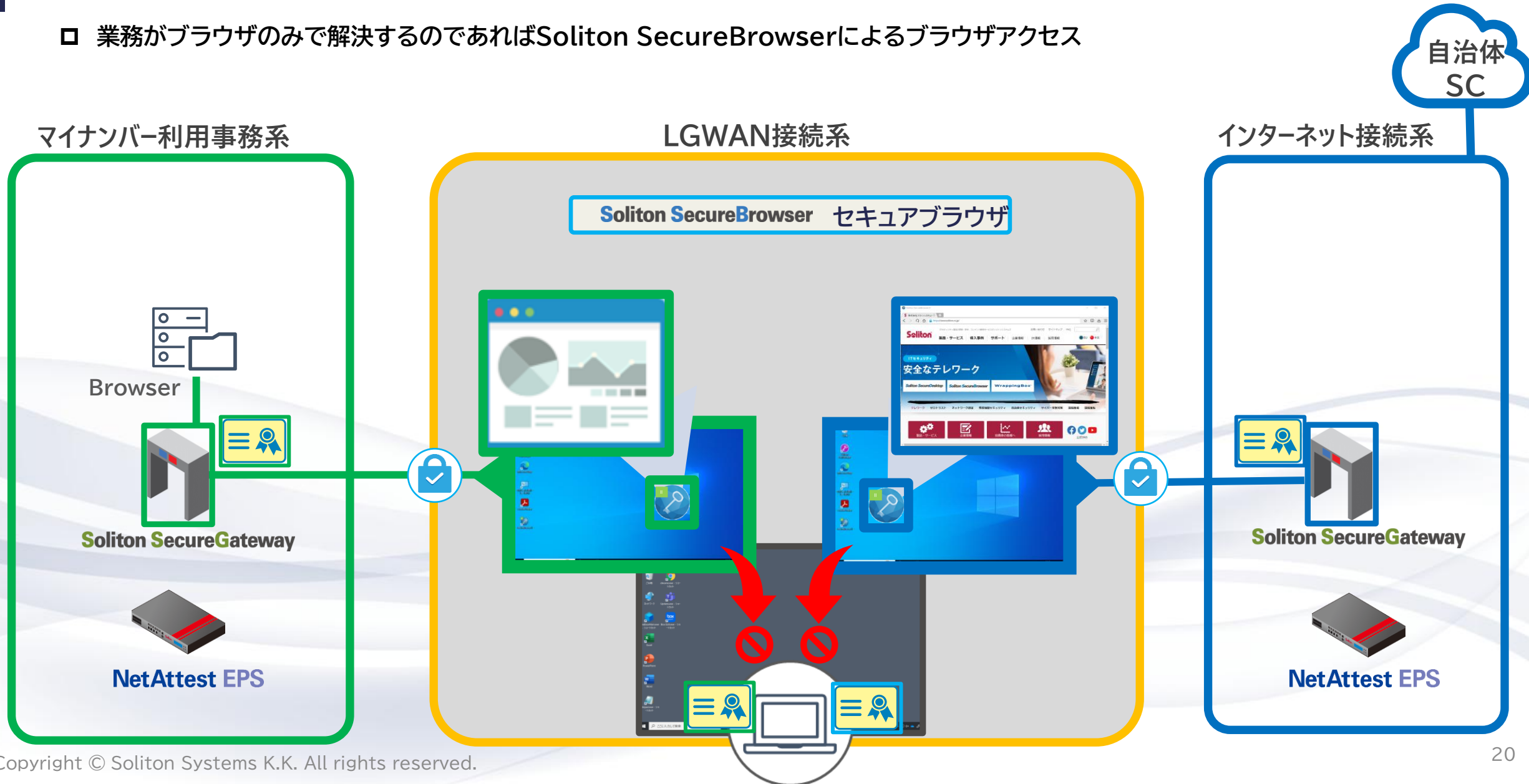
各方式に対する提案イメージ

■端末仮想化の各方式

方 式	概 要	対応ソリューションと特徴	
オンプレミス 仮想デスクトップ	マイナンバー利用事務系で構築されたデスクトップ 環境を手元の端末に画面転送	 + RDP	・ 転送元のリソース、同時接続数等の考慮不要 ・ 既存の業務アプリケーションをそのまま利用可能
セキュアブラウザ	手元の端末に専用ブラウザを導入し隔離環境を構築 専用ゲートウェイ経由でWebを安全に閲覧可能な 仕組みを実現	 	・ 最小コストで実現が可能 ・ 業務アプリケーションの仕様によっては 利用不可の場合も

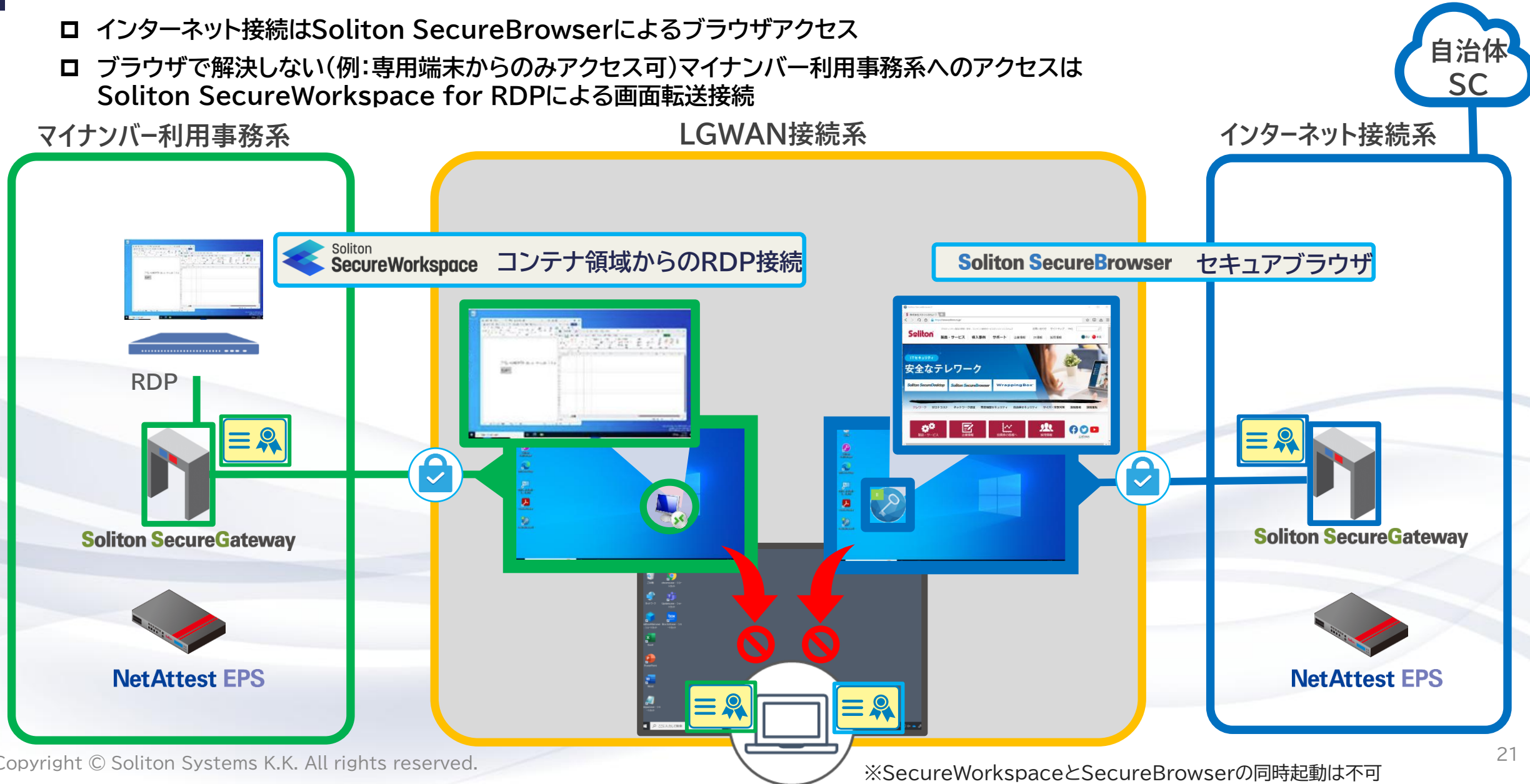
端末集約化構成例① (※二方向の同時接続は不可)

- 業務がブラウザのみで解決するのであればSoliton SecureBrowserによるブラウザアクセス



端末集約化構成例② (※二方向の同時接続は不可)

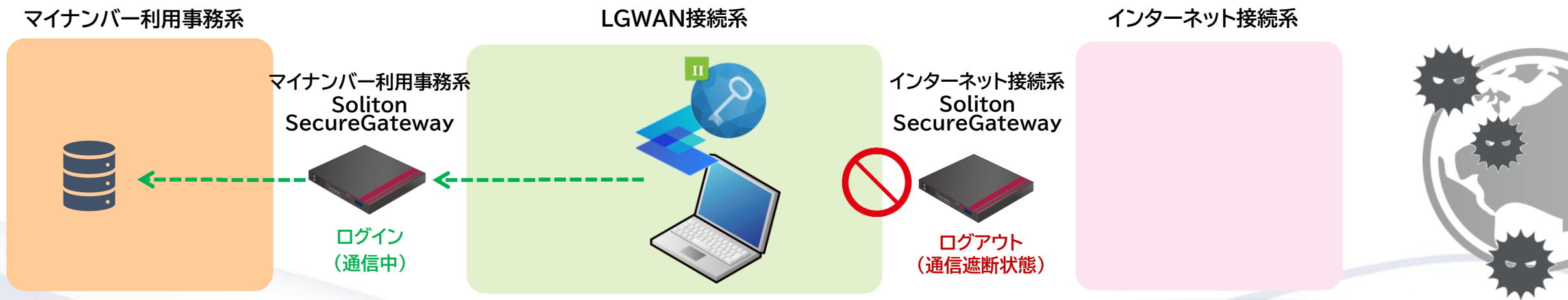
- インターネット接続はSoliton SecureBrowserによるブラウザアクセス
- ブラウザで解決しない(例:専用端末からのみアクセス可)マイナンバー利用事務系へのアクセスはSoliton SecureWorkspace for RDPによる画面転送接続



(参考)なぜ二方向の同時接続は出来ないのか？

- LGWAN接続系から片方の系統を利用している時に、もう片方の系統への通信は物理的に遮断されるため
マイナンバー利用事務系とインターネット接続系はネットワークとして繋がることはなく、マイナンバー利用事務系へのアクセスを隔離した安全な状況で利用する事を可能としています。

■マイナンバー利用事務系を参照中はインターネット接続系との通信を物理的に遮断



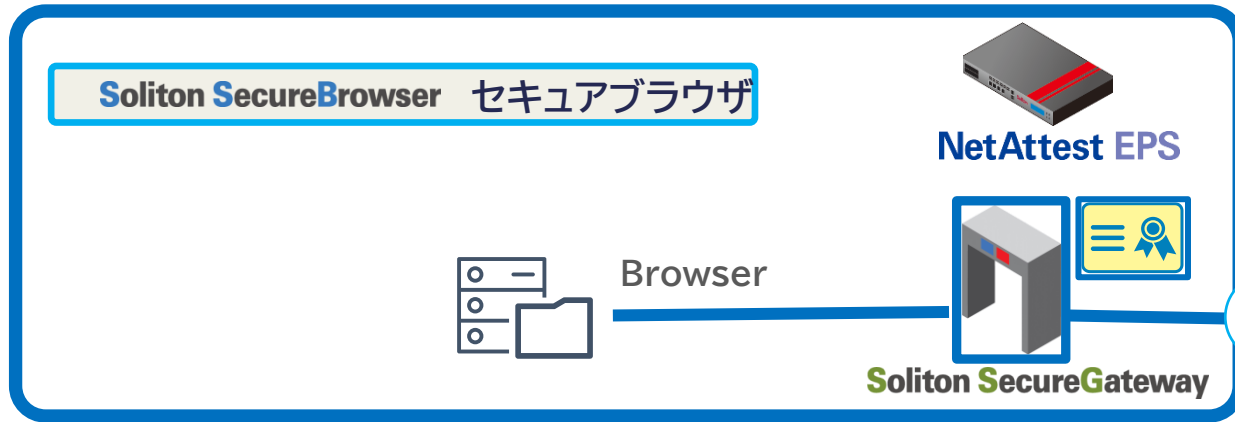
■インターネット接続系を参照中はマイナンバー利用事務系との通信を物理的に遮断



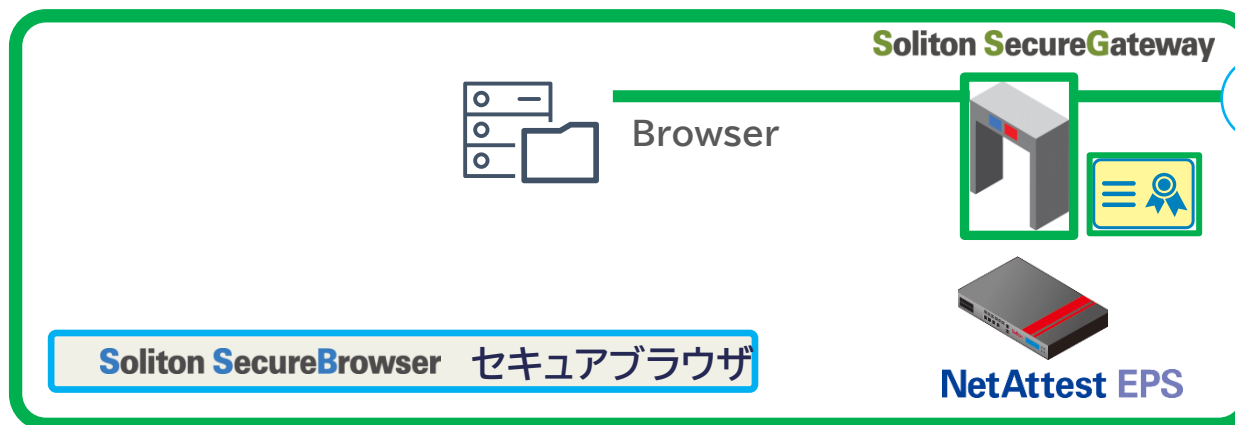
端末集約化構成例① (※二方向の同時接続は不可)

- 業務がブラウザで解決する場合はSoliton SecureBrowserによるブラウザアクセス

LGWAN接続系

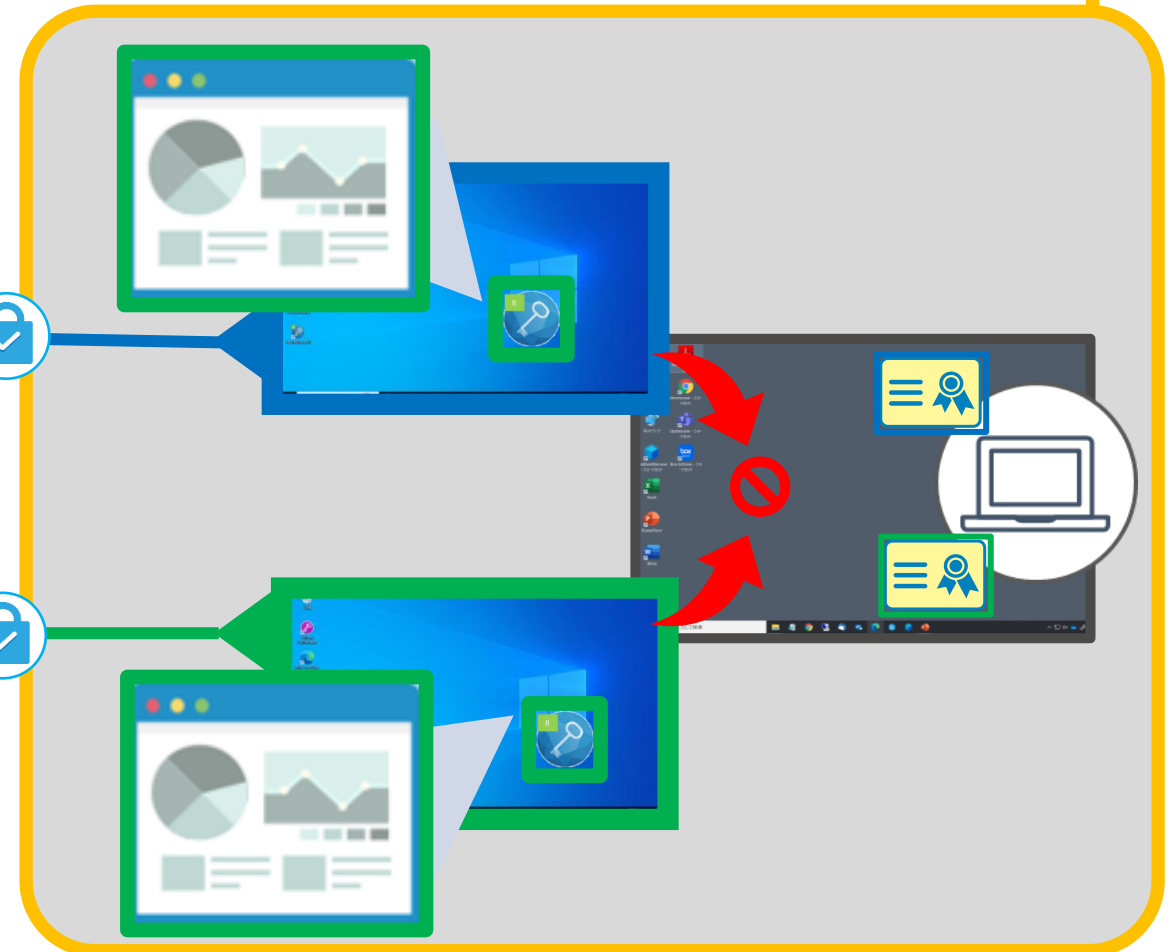


マイナンバー利用事務系



インターネット接続系

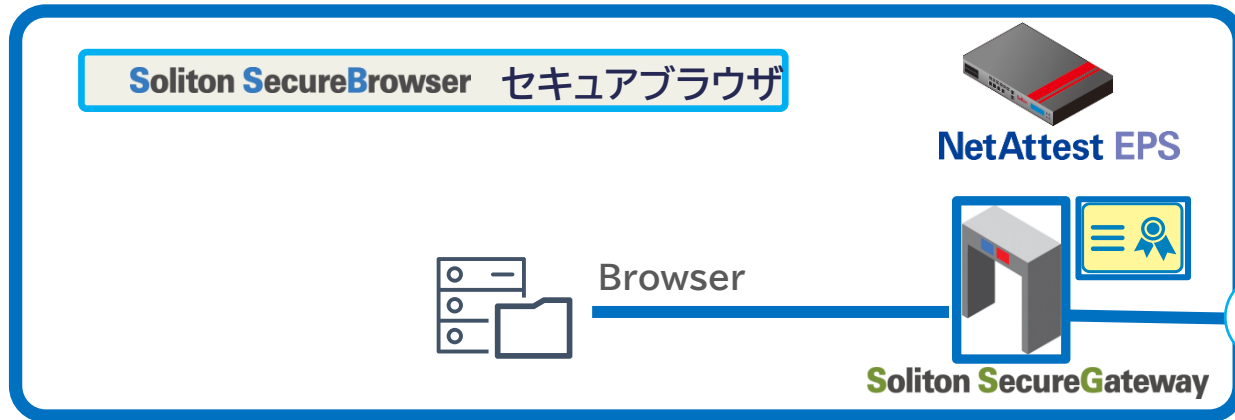
自治体
SC



端末集約化構成例② (※二方向の同時接続は不可)

- LGWAN接続系へのアクセスはSoliton SecureBrowserによるブラウザアクセス
- ブラウザで解決しない(例:専用端末からのみアクセス可)マイナンバー利用事務系へのアクセスはSoliton SecureWorkspace for RDPによる画面転送接続

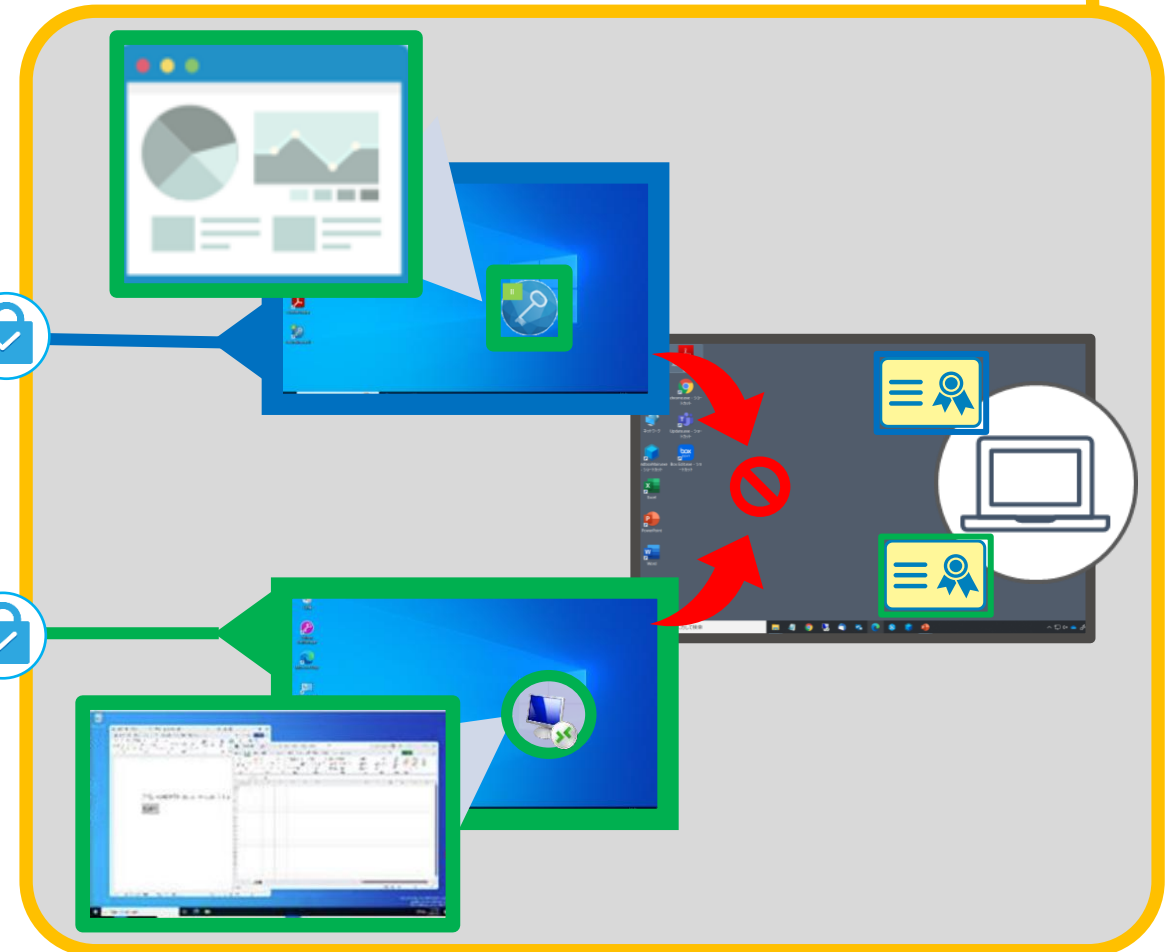
LGWAN接続系



マイナンバー利用事務系



インターネット接続系



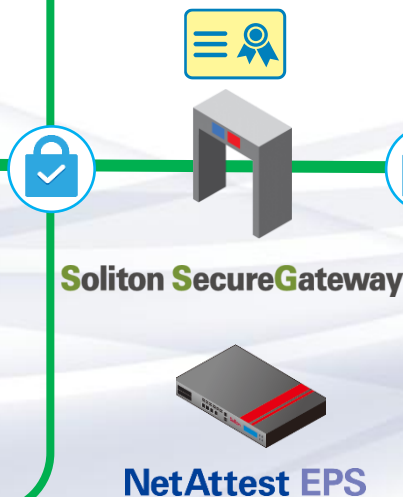
画面転送(RDP)の利用を行う場合

- コンテナ領域からリモートデスクトップ接続、ローカルにファイルのダウンロードを禁止
- 接続先端末へのログイン時に多要素認証を適用させることが可能（マイナンバー利用事務端末の多要素認証は**必須**）
- 同一セグメント、セグメント跨ぎのリモートデスクトップで適用ポリシーを変えることも可能

マイナンバー利用事務系

【接続先】

端末ログインについて
VDI・SBCであればSmartOn ID for RA
HDI・FAT端末であれば SmartOn ID

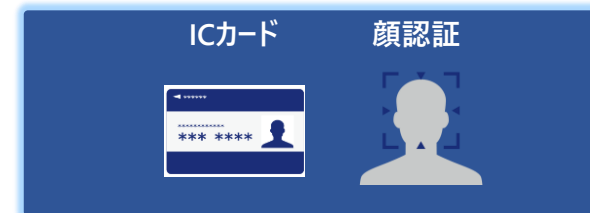


LGWAN接続系

【接続元】



SmartOn ID



RDP接続時、多要素認証ログインも可



多要素認証システム SmartOn ID

- マイナンバー利用事務端末、LGWAN接続端末の多要素認証システムとして多くの実績
- FAT端末、仮想デスクトップ環境どちらにも対応
- デバイス認証ツール分野で22年連続シェアNo.1の実績（富士キメラ総研調べ）



多様な認証方式に対応（顔認証はマスク認証も強化）

※ Panasonic CONNECT社提供の顔認証エンジン採用時

離席時に自動画面ロック

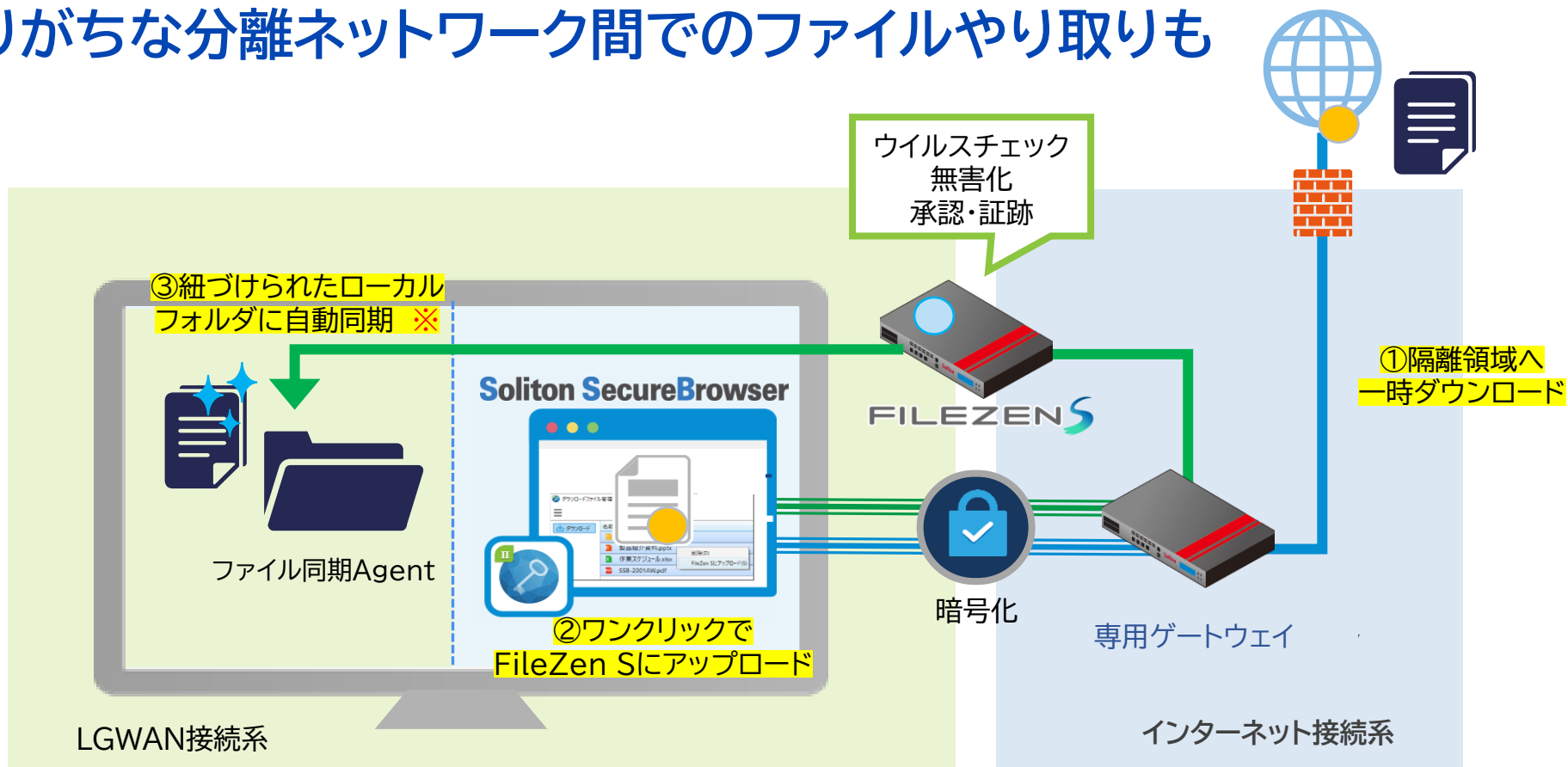
パスワード代行入力（SSO）

USBメモリ制御

利用者・利用履歴の確認（ログ）

ファイル受け渡しソリューションとも連携

手間が掛かりがちな分離ネットワーク間でのファイルやり取りも



ネットワークの独立性を担保しながら、ユーザビリティを追求

事例紹介: 山口県庁様

業務効率・生産性向上を目指したネットワーク分離

α モデルでLGWAN接続系から安全なインターネット利用



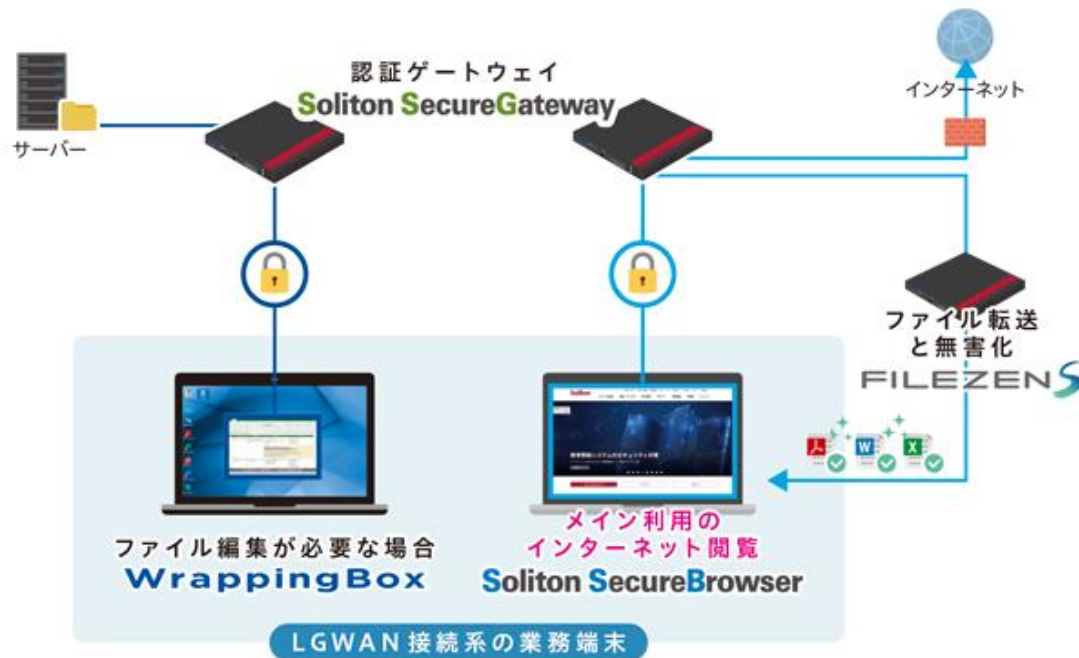
導入前の課題

- オンライン会議の利用が急増し、**LGWAN接続系端末からのインターネット利用環境の整備が必要**に
- インターネットからLGWAN接続系をファイルに取り込む際は、**適切な無害化処理**を行いたい
- 自治体ネットワークの三層モデルは α モデルのまま、**構成を大きく変えずに利便性を上げたい**

導入後の効果

- 安全かつ利便性の高いセキュアブラウザに変更し、**オンライン会議も快適**に行える環境を実現
- 専用のファイル転送ツールと無害化製品の自動連係により、**ファイル取り込み時の安全性も確保**
- 大掛かりな**変更が不要なソリューション**で、 α モデルの運用を継続しながら業務の効率化と生産性の向上を達成

山口県庁 導入イメージ



既存のWebブラウザと遜色なく使えて、山口県庁ではオンライン会議にTeamsを利用していましたが、セキュアブラウザ上でも支障なく参加出来ています。Youtubeの動画配信や視聴も問題ありません。



- ◎セキュアブラウザ以外の製品もPoCを進めたうえで、導入のしやすさ・使いやすさ・コストなど様々な面でセキュアブラウザを最善の選択とした(ソリトンの対応も親身で、実証に伴走いただけたこともポイント)
- ◎FileZenSによるファイル転送と無害化についてはファイルの取り込みが直感的に分かり、職員のセキュリティ意識向上にも繋がっている

事例紹介:奈良県庁様

VDIの課題をセキュアコンテナ方式で解消

操作性と運用性の両立(β' モデル)を低コストで実現



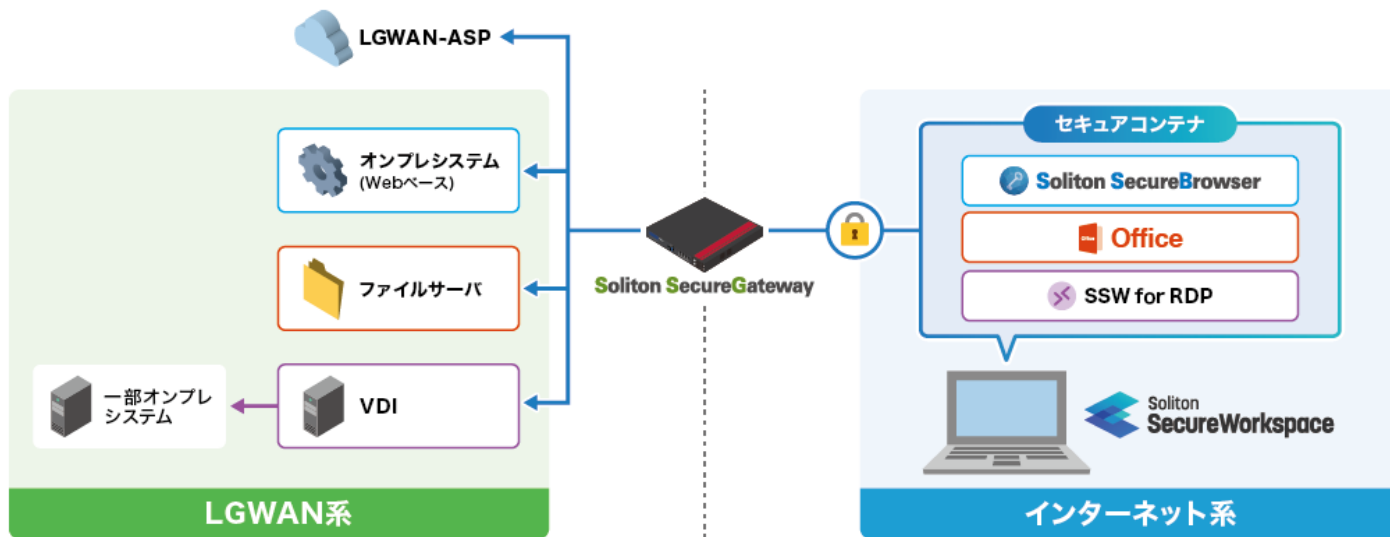
導入前の課題

- β' モデル移行にあたり、**セキュリティの担保とコスト抑制**が必要
- セキュリティパッチの適用、夜間・休日対応など、**保守運用の負担が膨大**
- 操作性が大きく変わると、職員の**業務効率が低下するリスク**

導入後の効果

- **セキュアコンテナ方式**で、高い安全性と低コストを両立した β' モデルを構築
- 休日・夜間の保守対応がほぼゼロとなり、**少人数での運用が可能**に
- **直感的に使える操作性**により、 β' モデルでもスムーズな業務施行を実現

奈良県庁 導入イメージ



セキュアコンテナ方式のSSWなら、LGWAN系の業務は今までと同じ操作性を保ちつつ、機密性の高い情報をLGWANに保管したまま、インターネット系端末でセキュアに行えます。



奈良県
総務部
デジタル管理室
共通基盤運用係
主査

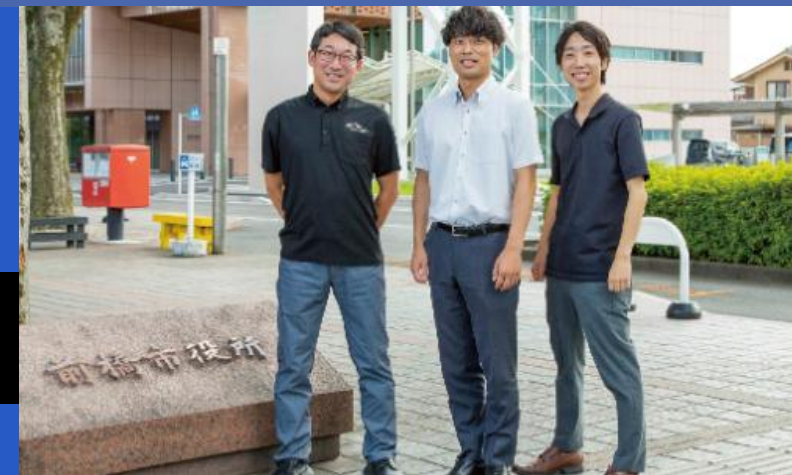
安浪 皓星 氏

- ◎VDIを利用した β' モデルへの移行には数億規模の投資が必要だったが、そのコストを半減できた
- ◎対象のLGWAN系システム約100種類のうち、PoCで約9割をSSB/SSWで使用可能なことを確認、支援いただけた
- ◎移行前の α' モデルからSSBを利用していたことによる安心感、使いやすさが職員に浸透していた

事例紹介:群馬県前橋市様

全職員のChromebook™活用をさらに拡大

自席・外出先で安全な利用 効率化とコスト削減を両立



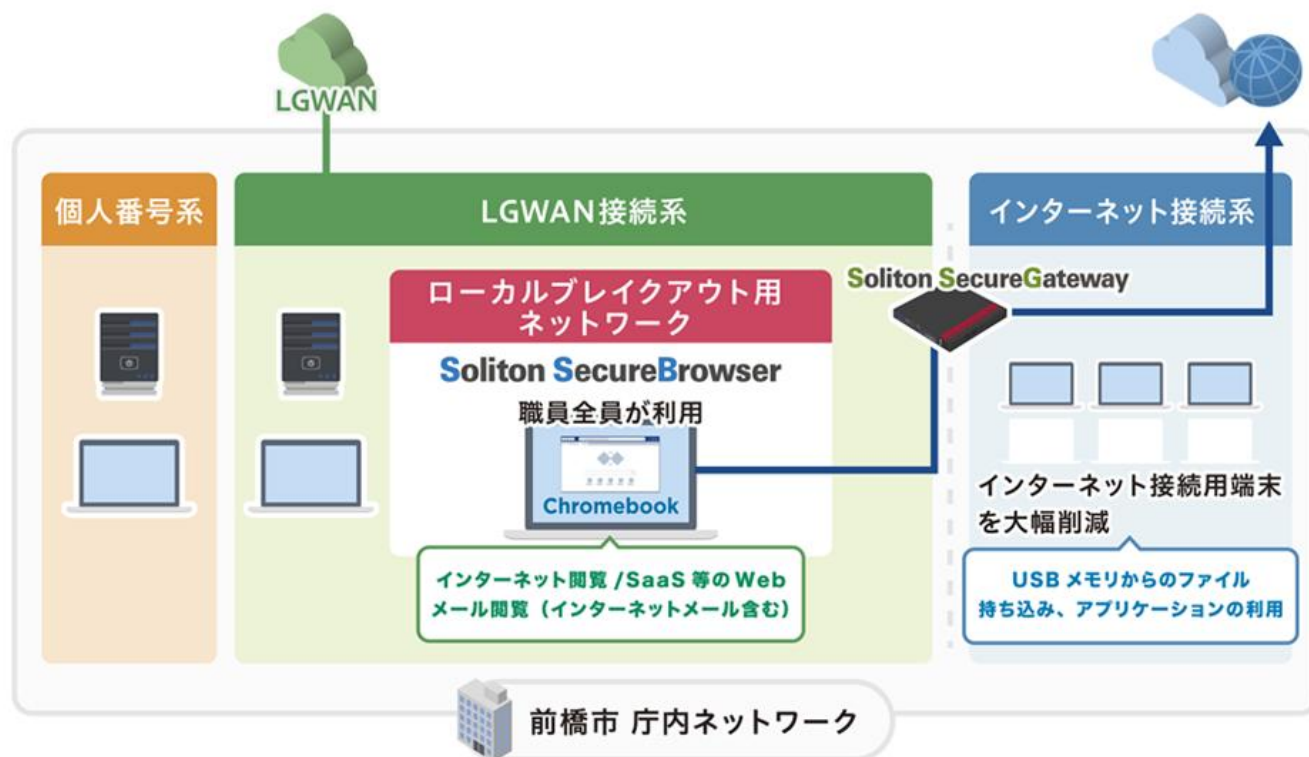
導入前の課題

- 全職員へ業務用端末として支給している
Chromebookの利用拡大
- インターネット接続用の共用端末利用の際、席を移動する・順番待ちによる**非効率性**
- Windows10のサポート終了に伴い、端末台数を見直して**コスト削減**

導入後の効果

- **Chromebookでできること**に、インターネットやメールの利用を追加
- 自席・外出先からいつでも調べ物やメール確認ができ、**業務効率が向上**
- Windows11端末の購入台数が**1/3ほどに縮小**できる見込み

群馬県前橋市 導入イメージ



“Chromebookで使えるセキュアブラウザは他に例がありませんでした”
“Chromebookで使えるセキュアブラウザを一緒に作らせてもらった感じです”



前橋市
未来創造部
情報政策課

主任
小林 悟 氏

- ◎数か月におよぶPoCで実運用に向けた改善ポイントの洗い出し・機能拡張・修正を実施して、製品に実装
- ◎試用期間も含めて1年近い稼働期間の中でシステム上のトラブルやセキュリティ事故はなし
- ◎職員も使い方をすぐに習得し、使い方に対する問い合わせも、ほとんどなし

事例紹介: 愛媛県庁様

災害時にも止まらない行政へ

BYODで実現した庁外からの安全な業務環境



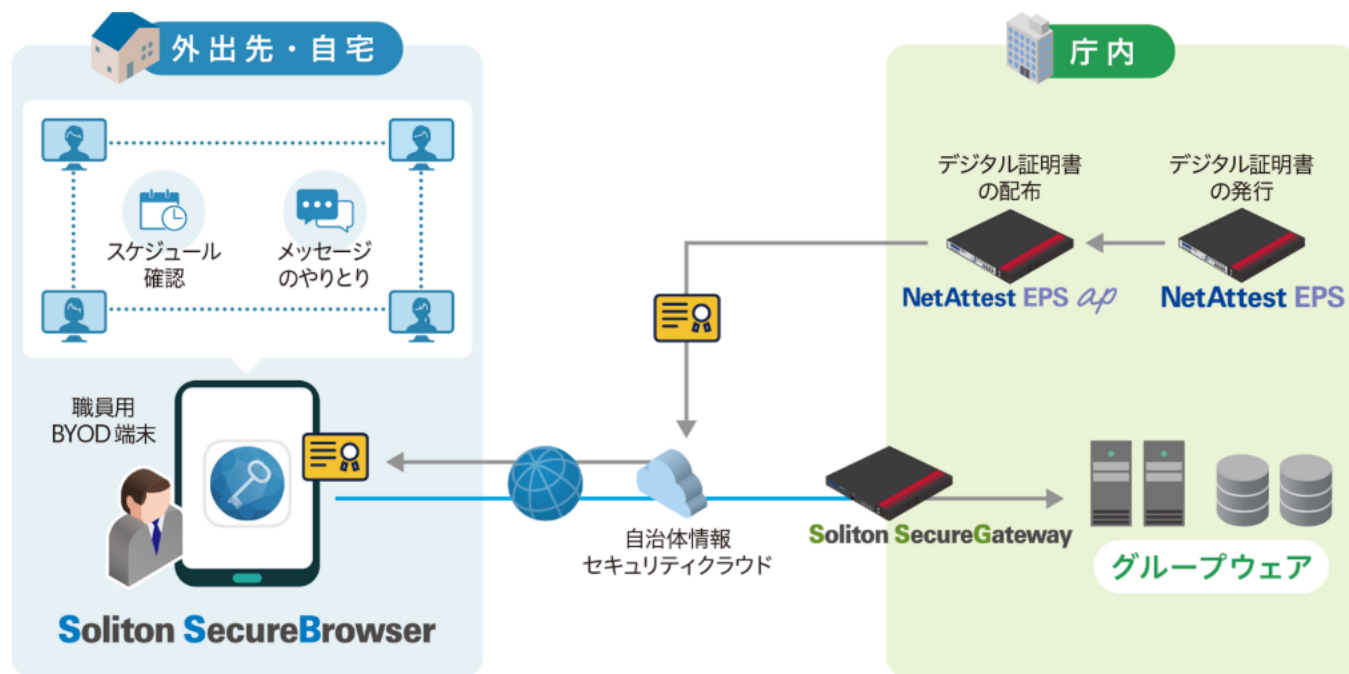
導入前の課題

- 働き方改革や緊急対応のため、**庁外からシステムを活用したい**
- 支給端末がなくても済むよう、**BYODを安全に使用したい**
- 若手**職員の定着**に向け、快適に働けるICT環境を整えたい

導入後の効果

- **デジタル証明書認証**により、庁外から安全にシステムを利用可能に
- **データを端末に残さないブラウザ**により、情報漏えいリスクを低減
- BYOD活用により、**自由度が高く効率的な働き方**を実現

愛媛県庁 導入イメージ



愛媛県は南海トラフ地震での被害が予想されており、豪雨被害の経験もあります。災害時にも業務に必要な情報へ支給端末が手元になくても、庁外から庁内 LAN に安全にアクセスできる仕組みが必要でした。



愛媛県
企画振興部
デジタル戦略局
スマート行政推進課
スマート行政情報グループ

担当係長
峯松 啓太 氏

- ◎適正な価格に加え、ローカル領域へのファイル保存禁止、デジタル証明書による端末認証の要件に合致
- ◎現在、全職員の20%にあたる約1,000名が自分のスマートフォンにデジタル証明書を問題なくインストール
- ◎日常業務、出張時の負担が軽減、隙間時間の活用による業務改善にもつながっている

なぜクラウド利用に 多要素認証が必要なのか

考慮事項① 日常的なアカウント漏えい

調査を行った 99% 以上の企業・団体で
社員のパスワード漏えいが発覚

ソリトンシステムズがこれまでにご依頼いただいて実施した「漏えいアカウント被害調査」のうち、全体の 99.9%(ドメインベース)の企業・団体で、現職職員のパスワードを含むアカウント情報の漏えいが確認されました。

しかし、ほとんどの企業・団体は、自社職員のアカウント情報がインターネット上に漏えいしている事実気付いておらず、調査によって初めて漏えいの被害が明らかになりました。

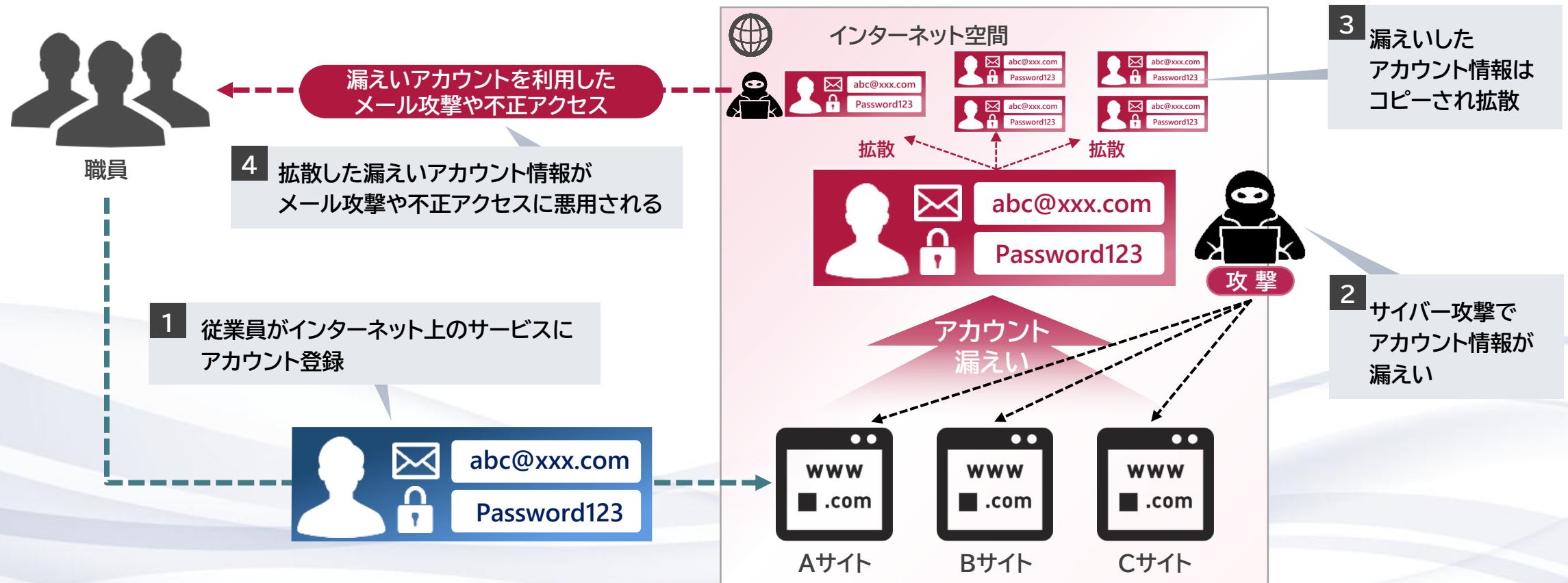


調査数 2500ドメイン以上

民間企業・政府機関学術機関など
ソリトン「漏洩アカウント被害調査サービス」調べ

アカウント漏えいのメカニズム

なぜ職員のアカウント情報が漏えいしているのか？

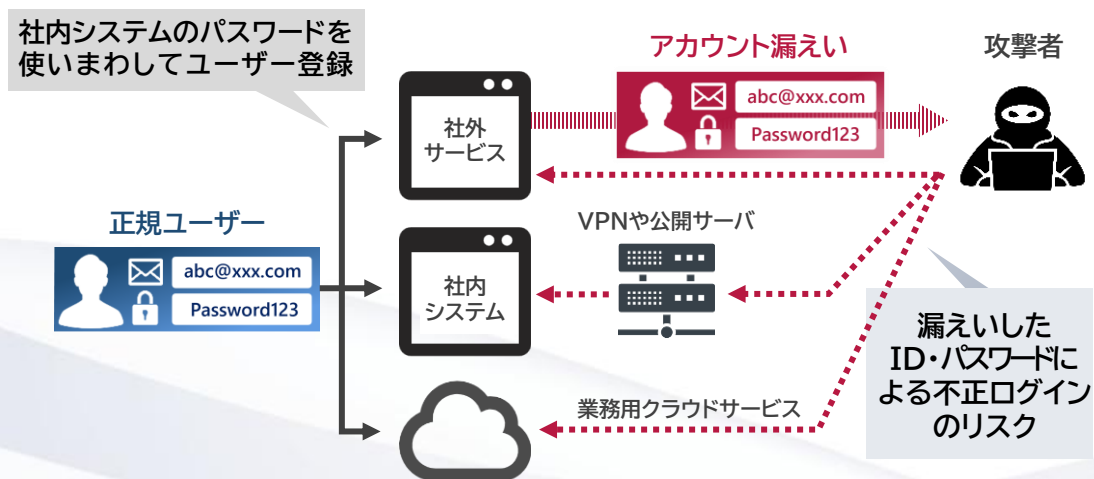


- インターネット上のサービスがサイバー攻撃され、登録していたアカウント情報が漏えい
- 漏えいしたアカウント情報は際限なく拡散し、メール攻撃や不正アクセスに悪用される

漏えいアカウントを利用した攻撃

(1) 不正ログイン

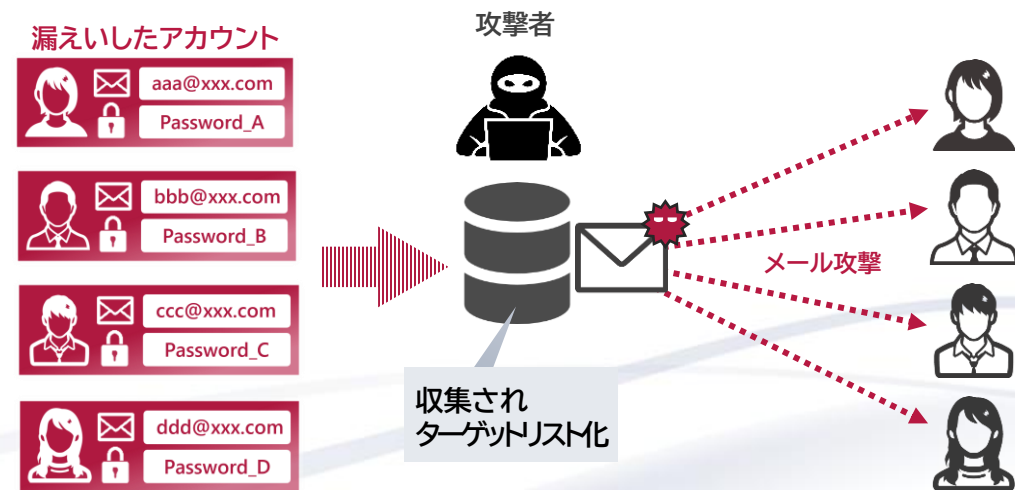
- ・ 漏えいしたアカウントを第三者が入手することにより漏えい元サイトに不正ログインされるリスク
- ・ 社内システムに不正ログインされるリスク



過去に漏えいしたパスワードは攻撃者によってリスト化されており、不正ログインのための”総当たり攻撃”などに使われる危険があります

(2) メール攻撃

- ・ 漏えいしたメールアドレスはメール攻撃のターゲットになる
- ・ メール攻撃によるマルウェア感染／フィッシング詐欺のリスク



漏えいしたアカウントのメールアドレスは攻撃者のターゲットリストとしてばらまき型メール攻撃に利用されます

考慮事項：クラウドサービス利用時の多要素認証 再警鐘

- Salesforce社「Salesforce環境のセキュリティ強化(MFAの必須化)」を発表

<https://help.salesforce.com/s/articleView?id=005321561&type=1>

Salesforce社より2026年5月5日、Salesforce環境のセキュリティ強化に関する重要なアップデートが発表されました。

これまでもSalesforceでは、ID・パスワードに加えて、SMS・ワンタイムコード・Authenticatorアプリを併用する多要素認証(MFA:Multi-Factor Authentication)が導入されていました。

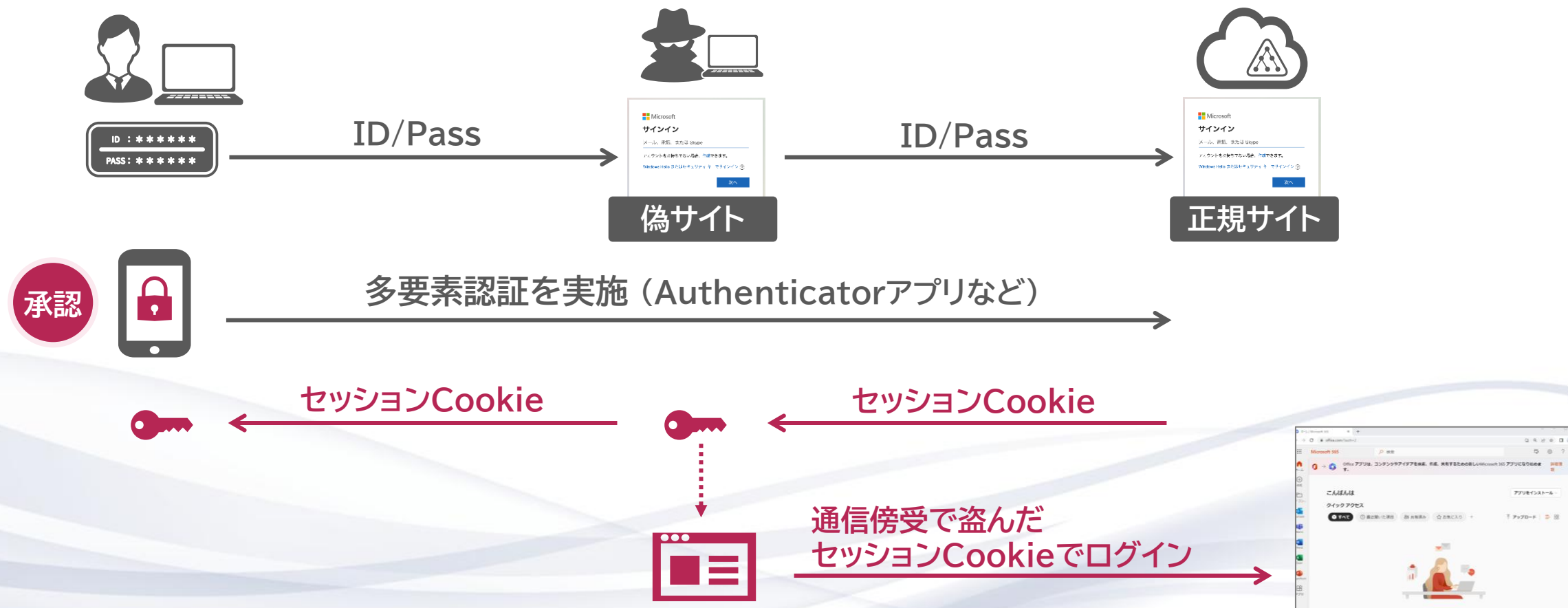
しかし近年、本物そっくりの偽ログイン画面にユーザーを誘導して、ID・パスワードと一緒にMFAのワンタイムコードまで盗み取ってしまう高度なサイバー攻撃(フィッシング詐欺)が急増しています。

これに対抗するためにフィッシング耐性のあるMFAの利用を特権ユーザー向けに必須化することを発表しました。

【SandBox(検証)環境では2026年6月22日、Production(本番)環境では2026年7月1日より段階適用】

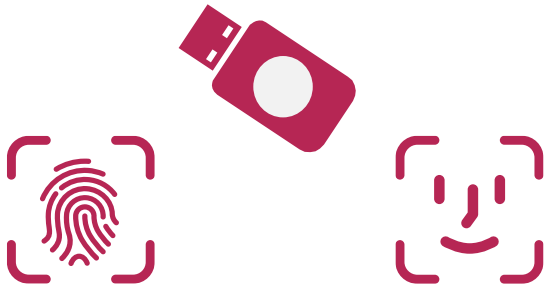
特権ユーザーが乗っ取られると、重要データの漏洩、改ざんがされ、致命的な被害に直面することを防ぐために今回は特権ユーザーのみ厳格なルールが適用されましたが、対象範囲は今後拡大する可能性も考えられます。

攻撃耐性のあるMFAが必要な理由(AiTM攻撃)



攻撃耐性のある多要素認証が必要（弱い多要素認証は突破される）

多要素認証(MFA)の選択肢

	スマートフォン用アプリ SMS、音声案内	FIDO2 セキュリティキー	デジタル証明書
			
フィッシング耐性※	×	○	○
導入	スマートフォンが必要	FIDO2に対応した デバイスが必要	専用デバイス不要 マルチOS対応
注意・特徴	- 私物スマホ利用は課題多い - スマホ忘れ時の対応を考慮する必要がある	- FIDO2デバイスの管理が煩雑 - 外付けデバイスの場合、故障・紛失・交換の考慮が必要	- 遠隔で配布・失効可能 - 利用デバイスを限定できる - VPN/無線LANにも利用できる
パスワードレス	×	○	○
コスト	¥ ¥	¥ ¥ ¥	¥

フィッシング耐性のあるMFA(証明書認証の場合)

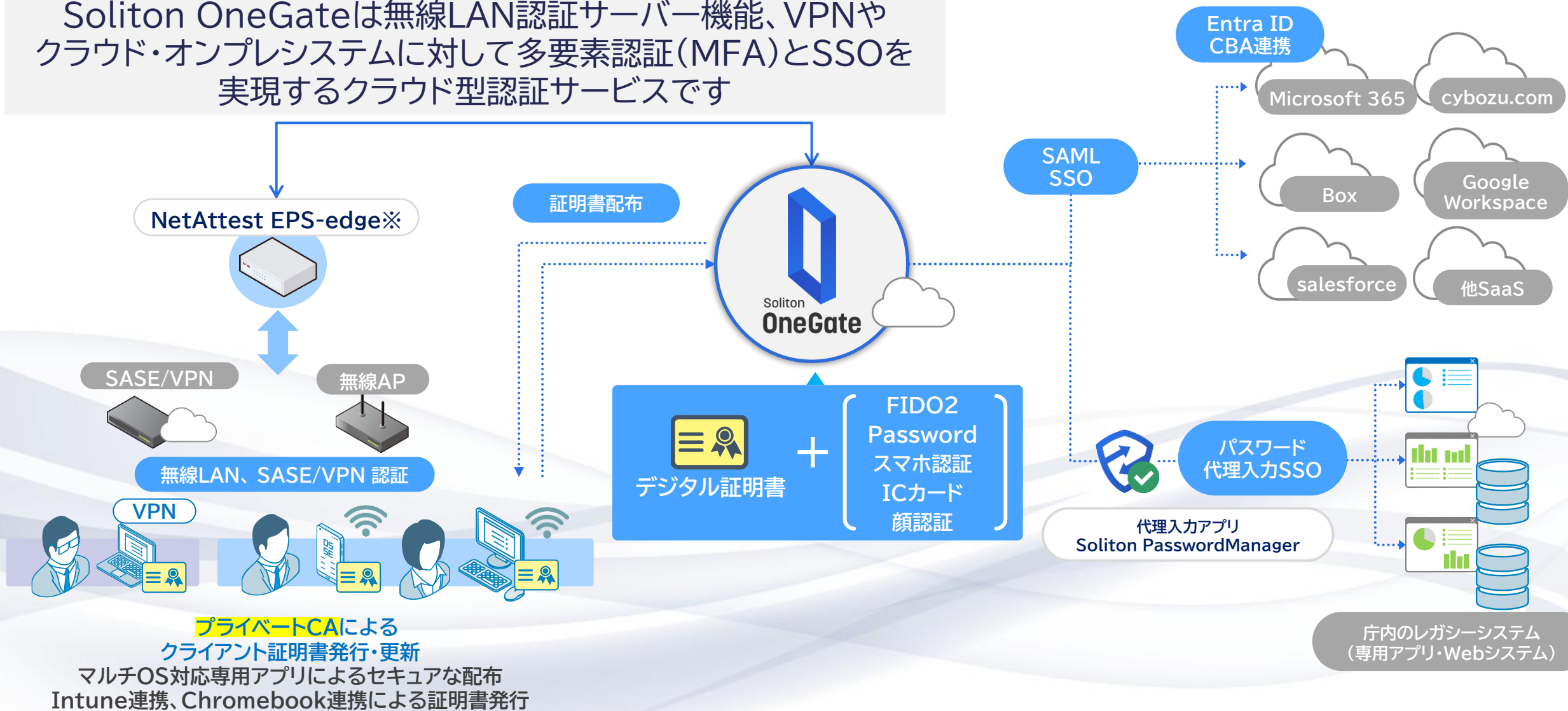


デジタル証明書認証 vs 他の多要素認証

	デジタル証明書	他の多要素認証(所有、生体)
攻撃耐性 (フィッシング耐性)	 <u>攻撃者に、ログイン画面まで到達させない</u> <u>ログイン画面の脆弱性攻撃にも効果あり</u> <u>MFA突破攻撃(AiTM)にも耐性あり</u>	 攻撃者は、ログイン画面まで到達できる場合が多い※
紛失時の対応	 当該証明書をセンター側で失効し、新しい 端末へ証明書を再発行する	 緊急時の代替認証の手順を整備しておく 物理デバイスの場合は代替機へ交換する
様々な用途に 活用できる	 VPN/SASE、無線LAN、クラウドサービス など様々な認証に利用できる	 無線 Wi-Fi 認証に利用できないなど、用途 が限られる
マルチOS	 PKI技術は実績豊富で信頼性が高く、マルチ OSで動作	 OS毎に利用可能な認証要素が異なる場合 がある

多要素認証サービス Soliton OneGate 全体像

Soliton OneGateは無線LAN認証サーバー機能、VPNやクラウド・オンプレシステムに対して多要素認証(MFA)とSSOを実現するクラウド型認証サービスです



政府のセキュリティ基準を満たしています



は ISMAP 認証取得済の国産IDaaS 第一号！

政府情報システムのためのセキュリティ評価制度

政府が求めるセキュリティ基準を満たすクラウドサービスを評価・登録する制度。

政府や地方公共団体などのクラウドサービス調達を支援する。

指定された監査法人による安全評価を受けたクラウドサービスは、ISMAP運営委員会の厳格な審査を通過した後、ISMAPのクラウドサービスリストに登録される。



ISMS、ISO27017等の基準を遥かに超える膨大なチェック項目をクリア



多額の費用、社内の広範な部署の人的リソースを注いだ継続的な監査対応



中央省庁での利用にも対応可能な企業経営・サービス運用におけるセキュリティ対策

Soliton OneGateは、高度な「セキュリティ」に誇りをもってサービス提供しています！

パスワードレスと多要素認証に対応

Microsoft 365を快適に利用する環境を低コストで実現



®わんこきょうだい



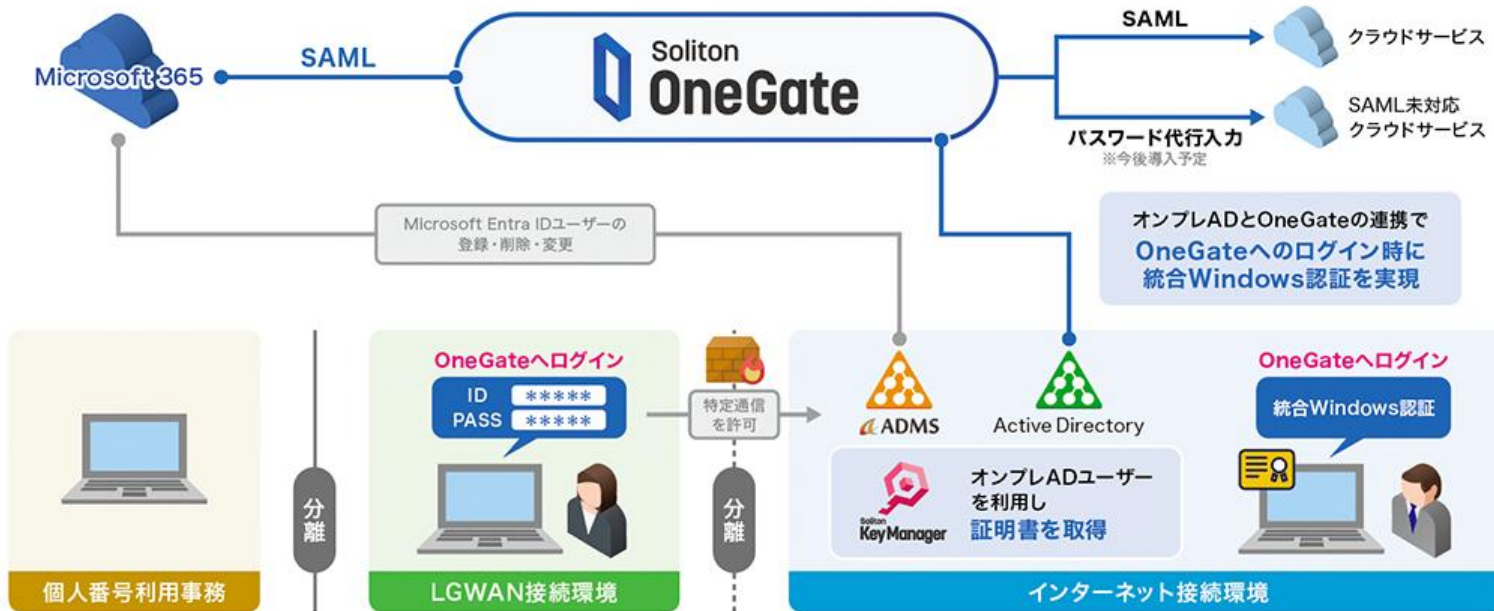
導入前の課題

- 業務のクラウドシフトに向け、IDaaSで**多要素認証・SSOを実現**したい
- Microsoft 365のライセンスを見直して**コストを削減**したい
- 多要素認証要素を負荷なく運用できるようにして、**将来的なBYOD利用**も見据えたい

導入後の効果

- **デジタル証明書**による多要素認証・SSOを実現
- コストを大幅に抑えながら、**Microsoft365上位ライセンス相当のセキュリティ**を確保
- 付帯する「Soliton Key Manager」を活用して、**証明書配布・管理業務の効率化**を実現

岩手県庁 導入イメージ



統合Windows認証と証明書発行が可能なIDaaSで、ISMAPに対応した認証基盤はOneGateだけでした



岩手県
科学・情報政策室 担当

- ◎採用要件とした日本政府のクラウドサービスのセキュリティ評価制度「ISMAP」を取得
- ◎統合Windows認証と連携できることで職員は新たなID・パスワードを覚える必要がなし
- ◎証明書の運用もKeyManagerのおかげで、管理者負担はほとんどなし

ソリトン製品・サービスの
全国自治体への導入率

約55%(市町村)

約97%(都道府県)

セキュアブラウザ・セキュアコンテナ導入数

200超





<https://www.soliton.co.jp/>

株式会社 ソリトンシステムズ

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811

netsales@soliton.co.jp

大阪営業所 06-7167-8881

東北営業所 022-716-0766

福岡営業所 092-263-0400

札幌営業所 011-242-6111

名古屋営業所 052-217-9091