中堅企業にSASE／ゼロトラストは必要なのか？
どこまでやるべきなのか？

～ 大企業とは異なり、要件を絞って必要な機能のみ導入する ～

2025.04.08

かもめエンジニアリング株式会社

KAMOME Engineering

日本でいちばん仕事が大好きなチームです！

スピーカー紹介

潮村 剛 （しおむら たけし）

1990年代半ば、食品メーカーからITベンチャーに。
国内の主要通信サービス事業者を中心に認証系システム案件を担当。

2008年、かもめエンジニアリング社を設立。
通信サービス事業向け統合認証基盤やビッグデータ処理のシステムの導入実績多数。

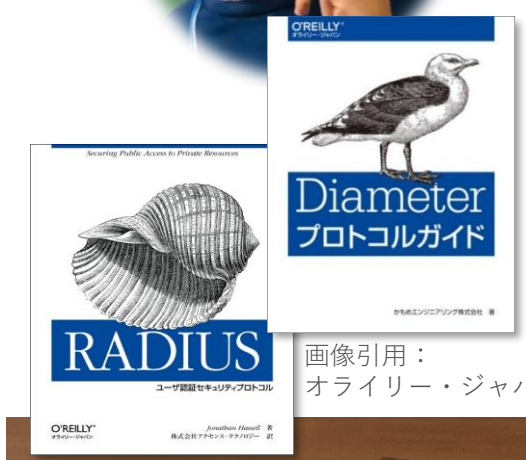
2017年、シングルサインオンシステム「KAMOME SSO」提供開始。

2019年、「クラウドID管理サービス　Keyspider」の提供開始。
日本企業のID管理の課題を解決するため、Keyspider社を設立。

2021年、「ゼロトラスト接続サービス　KeygatewayC1」提供開始。
日本企業のテレワーク環境のセキュリティ強化を推進。

2022年、「ゼロトラストアライアンス・ジャパン」、ITベンダーやSI事業者19社で設立。
日本企業へのゼロトラストセキュリティの普及を目的。理事。

SSOやID分野のセミナーで年間30回程度講師を担当。
オライリー・ジャパン社刊行IT技術書籍のプロデュース。
　『RADIUS – ユーザ認証セキュリティプロトコル』（2003年）
　『Diameter プロトコルガイド』（2015年）



画像引用：
オライリー・ジャパン

趣味 … 料理と読書。歴史小説とSF、時々マンガ。
最近のヒット　「ミッキー７　反物質ブルース」エドワード・アシュトン作

ID管理・ユーザー認証分野を中心に展開

統合認証基盤システム　KFEP（ケイフェップ）

特許取得

- 複数サービスの 「認証・認可」システムを統合、システム規模を最大93%削減の実績
- 運用コストを最大96%削減の実績
- 単一障害点が存在せず、運用SLA向上に貢献
- 通信事業者250ライセンス以上、エンタープライズ約4,000ライセンスの採用実績

認証システム　KAMOME SSO（かもめSSO） / Keygateway（キーゲートウェイ）

- OSSをベースに独自の機能をプラス、B2CからB2Bまでカバーする SSO認証サーバ「**KAMOME SSO**」
- SAMLやOIDC非対応の業務Webアプリを改変不要でSSO環境に対応、SAML/OIDCアダプター「**Keygateway T1**」
- VPNに代わるゼロトラスト接続サービス「**Keygateway C1**」

特許取得

- 官公庁、金融機関、医療機関、通信事業者、ECサイト、エネルギー大手、製造大手、各種団体、教育機関など、幅広い業種と規模での採用実績

RADIUS認証サーバ　fullflex KG（フルフレックスKG）

特許取得

- インターネット創成期からネットワーク認証を支える、導入実績国内No.1の信頼のブランド
- 単一障害点が存在せず、運用SLA向上に貢献
- WebGUIで運用状態の確認、ログの検索も実現
- 認証拠点の統合に最適なマルチテナント対応

ID管理クラウドサービス　Keyspider（キースパイダー）

- 企業内のユーザー情報、権限情報を統合的に管理できる、ID管理クラウドサービス（SaaS）
- Microsoft Entra ID（旧AzureAD）、Microsoft 365、Google Workspace、Salesforce、BOX、さらに国産のクラウドサービスやオンプレの社内システムとも簡単にID連携
- 独自のセキュア通信機能で、オンプレの社内システムとも安全に連携。日本特有の人事処理にも対応

主要実績

通信キャリア向け 大規模認証システム

- 携帯電話サービス 基幹認証システム
  - 国内通信事業者　4,500万ユーザ
- 企業顧客向けVPNサービス 認証基盤
  - 国内総合電機メーカー　100万ユーザ
- 社内LANアクセス　認証基盤
  - 国内大手移動体通信事業者　20万ユーザ
- Webフィルタリングサービス
  - 認証エンジンセキュリティベンダー OEM提供

etc.・・・

エンタープライズ市場向け シングルサインオン（SSO）& ID管理システム

- IDaaSサービス 認証基盤
  - 通信事業者　2,000社 ➡ 20,000社へ拡張
- 社内業務アプリ SSOシステム
  - 家電メーカー　7,000ユーザ
- 学内システム SSOシステム
  - 大学　15,000ユーザ
- ゼロトラスト ID管理サービス
  - 総合電機メーカー　OEM提供
- OEM提供先

NTT AT　FUJITSU　HCNET エイチ・シー・ネットワークス株式会社
Stylez 株式会社 スタイルズ　Marubeni Network Solutions　IP3

KAMOME Engineering

「ゼロトラスト化」の第一歩について、ひとつのアイデアの提示

- 最初から「完全なソリューション」の導入が必須なのか？
- 昨年から多くなっているご相談から考えてみました
- いくつか前提はありますが、ここから始めてもよいのではないかというアイデア、叩き台、をご提案します

ご意見・ご異論・ご反論もおありかと思いますが、
「まずはここまで」を満たすためのアイデアとして
一度お聴きいただければ幸いです。

KAMOME Engineering

あったほうが良い。しかし…

ゼロトラストには
パッケージングされたSASEソリューションが不可欠？

そうとも限りません。
「**今あるものプラスアルファ**」で、
できるところから段階的に導入することも可能です。

KAMOME Engineering

【結論】 これだけあれば、スタートを切れます

	まずは	あるいは
エンドポイント セキュリティ	**ウィルス対策ソフト**の機能強化、 **Microsoft Defenderなど**OSのセキュリティ機能、 などを活用	
業務用SaaSへの アクセス制限	SSO 中小規模なら **IDaaS**の活用を検討 Microsoft365の**Entra ID**活用も	SSO 中堅以上なら **自社専用IdP**の活用も要検討 Microsoft365の**Entra ID**も活用
業務外Webサイトへの アクセス制限	**Webブラウザのセキュリティ機能**を活用 Edge …「セキュリティ強化」 Chrome …「セーフ ブラウジング」	SWG
社内システムへの アクセス制限	SSOと連携したアクセス制御 **ZTNA**（アクセス可能リソースの制御）、 **ZTNA＋代理認証**（上記＋利用者のパスワード管理を廃止）	

次セクションから、順を追ってご説明していきます。

想定ケースや前提、ご提案について

KAMOME Engineering

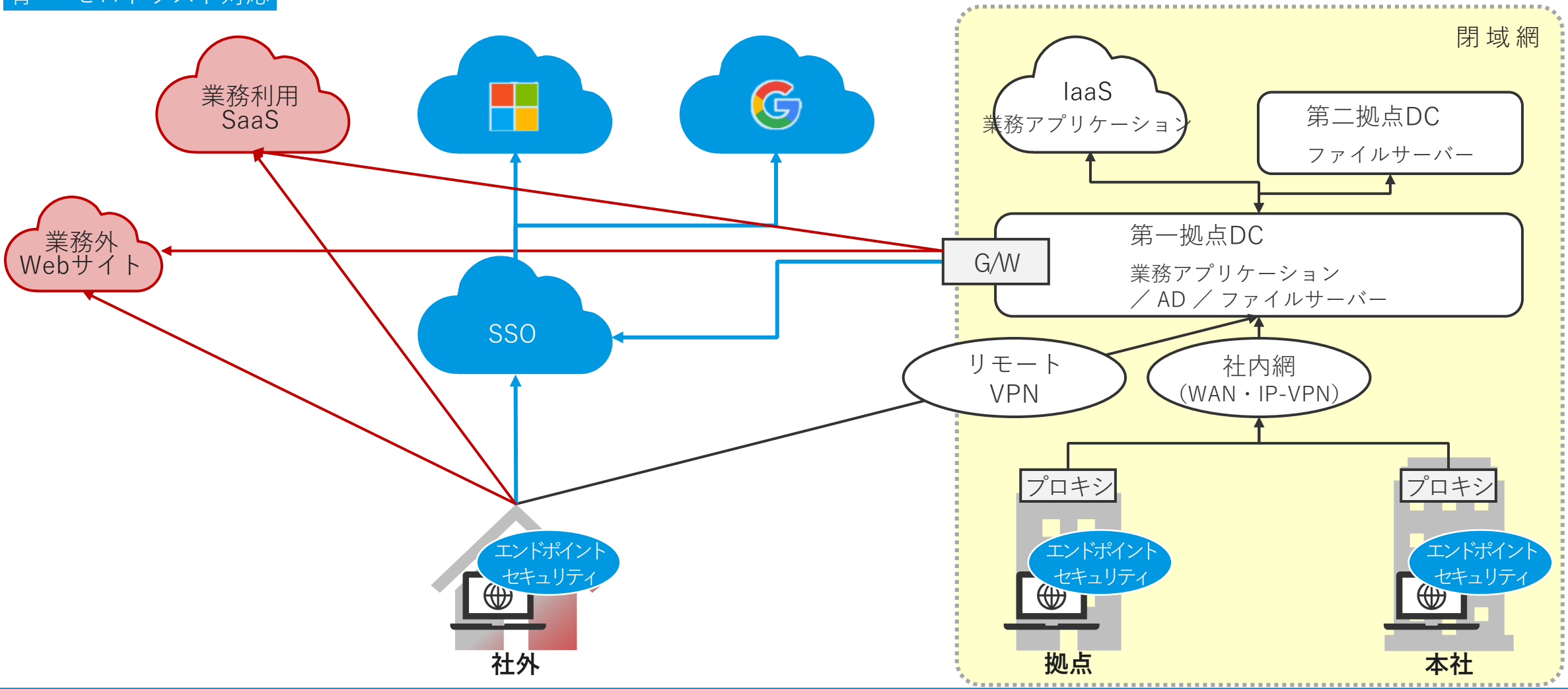
ご相談されることの多いパターンからケースを想定

■ 前提とした現状の構成

- 利用者数 … 1,000名前後
- クラウドサービス … 複数利用中、今後増加傾向
- 社内システム … データセンターにて複数運用
- 拠点 … 本社 ＋ 支店など複数あり
- 拠点間通信 … 各拠点⇔データセンター … VPN設置
  各拠点⇒インターネット … データセンター内GW経由に集約
- リモートアクセス … あり、VPNでデータセンターへ接続し業務システムを利用
- 利用者認証 … 一部SaaSだけで実施（IDaaSを利用）

現状

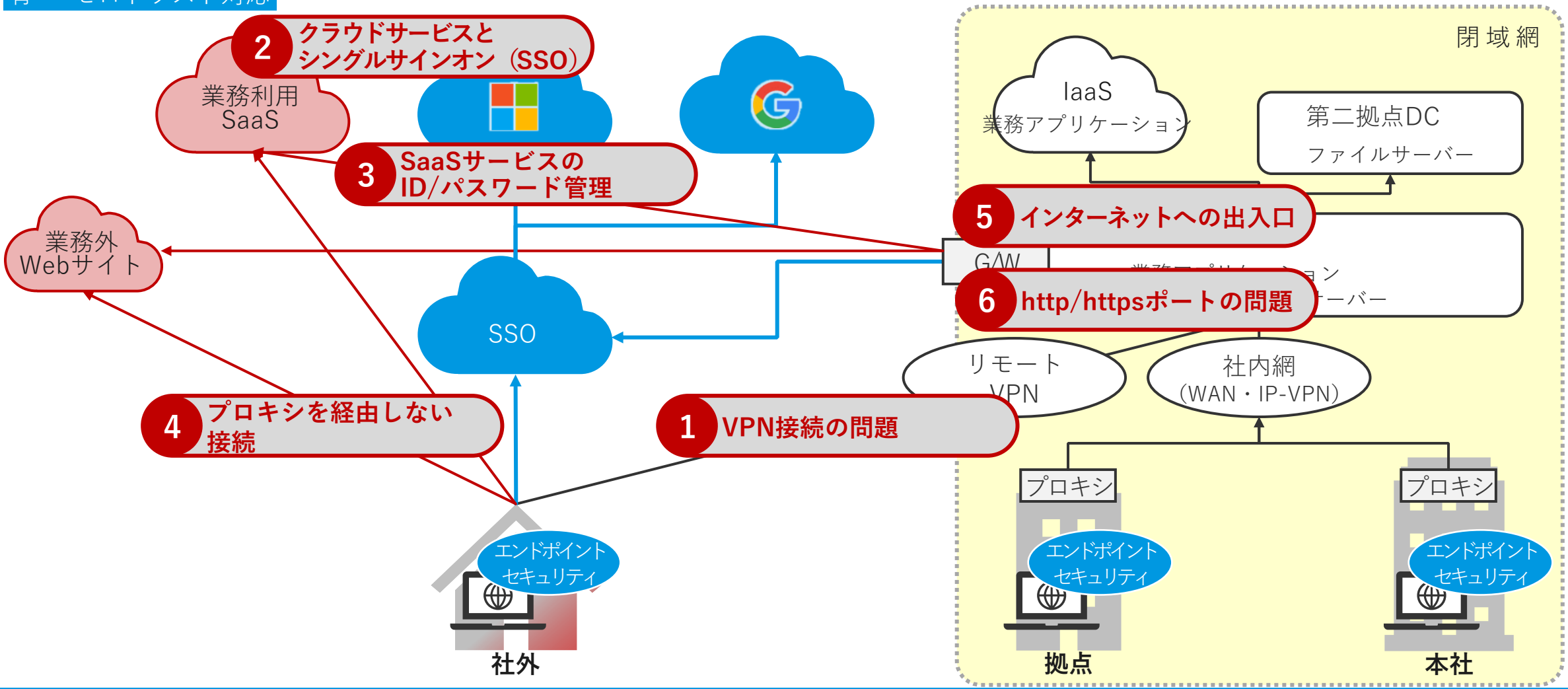
青 … ゼロトラスト対応



KAMOME Engineering

現状によく寄せられる課題

青 … ゼロトラスト対応



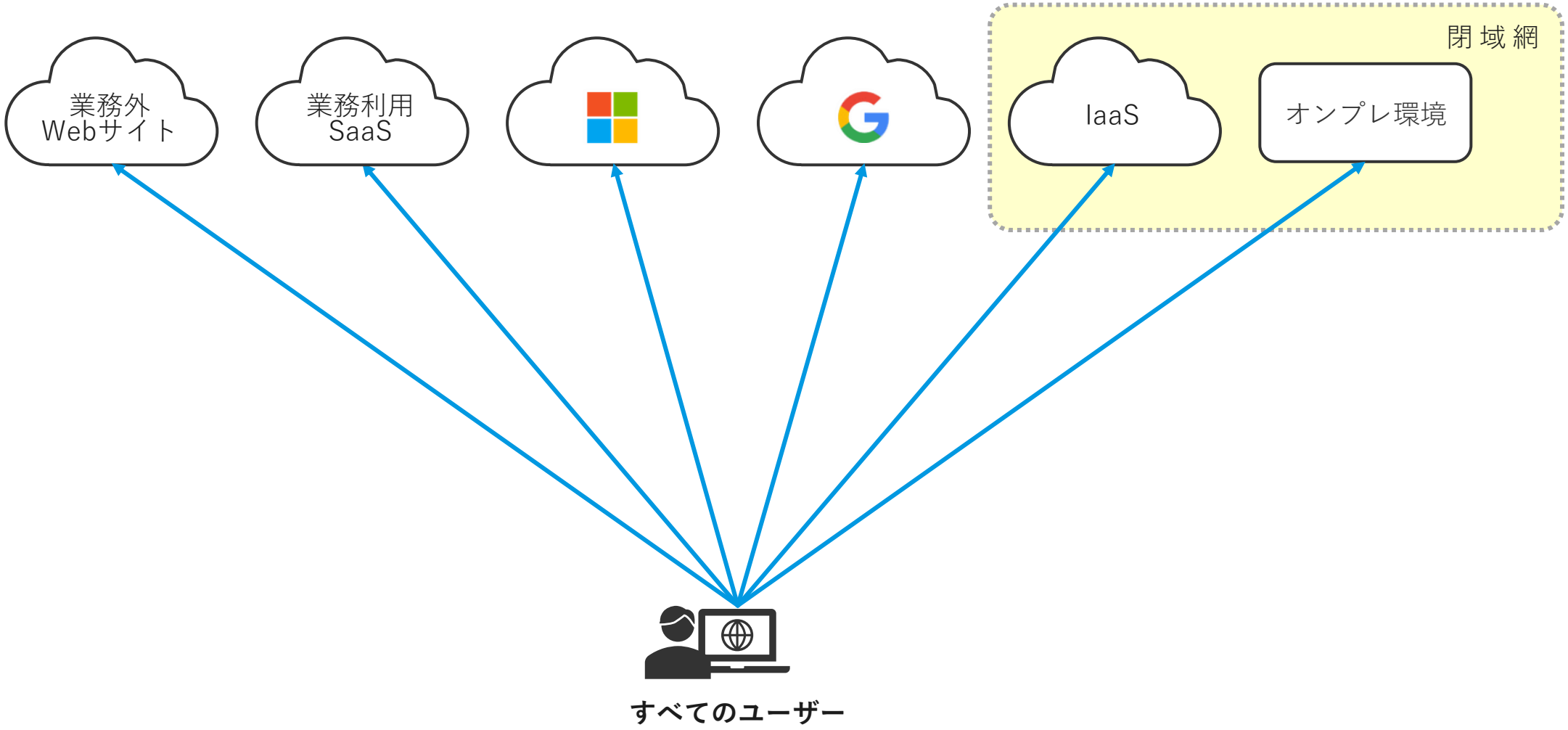
各課題と、それに対する要望

KAMOME Engineering

課題	要望
❶ VPN接続の問題	
社外から接続する際にVPN接続が不安定であり、使い勝手が悪い	・VPN接続の簡素化および安定化 ・利用者が簡単に安定して接続できるためのGUIやガイドの提供
❷ クラウドサービスとシングルサインオン（SSO）	
一部のクラウドサービスがSSOを経由せずにアクセスされている	全てのクラウドサービスに対して**SSOを強制**
❸ SaaSサービスの、ID/パスワード管理	
多数のSaaSサービスに異なるID/パスワードが必要で、 ユーザーは混乱し、管理者は管理が複雑になる	**セキュアなID/パスワード管理ソリューション**を導入し、 利用者と管理者双方の負担を軽減
❹ プロキシを経由しない接続	
社外からのインターネットアクセスがプロキシを経由しないため、 制御外の閲覧が可能	社外からのインターネットアクセスに**プロキシを必須**とし、 制限したい内容に対するフィルタリング機能を強化
❺ インターネットへの出入口	
インターネットの接続ポイントが1つしかなくアクセスが集中する	**複数のインターネット接続ポイント**を設定し、 負荷分散を図る
❻ http/httpsポートの問題	
http/httpsポートが開いており、その通信を使った不正アクセスが 制御できない	http/httpsポートを通じた不正アクセスを防ぐための、 **高度な通信監視とフィルタリング機能**の導入

実現させたい形（ゴール）

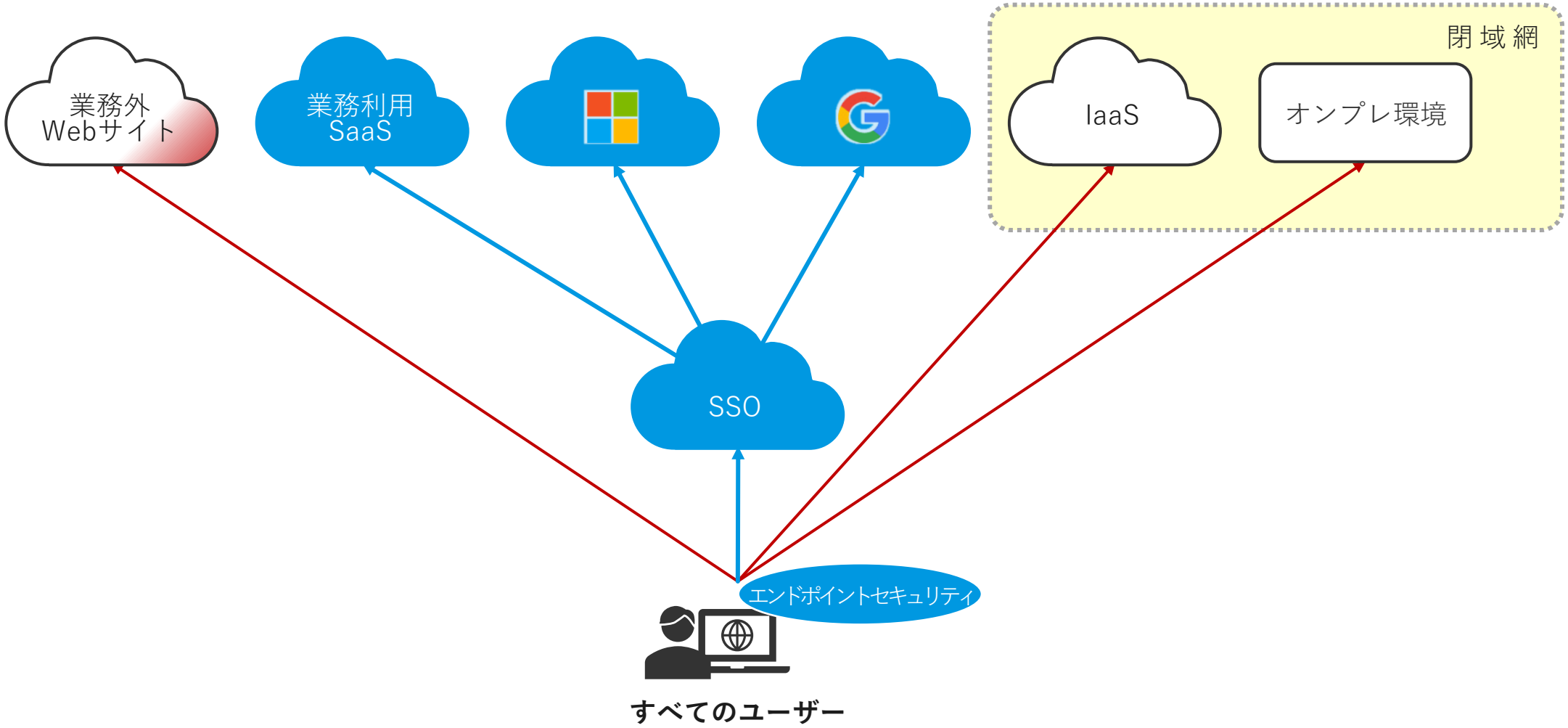
すべてのユーザーが、利用場所にかかわらず、
すべてのリソースへ安全にアクセスできること



実現させたい形

❶ シングルサインオンを用いてユーザー認証を行う

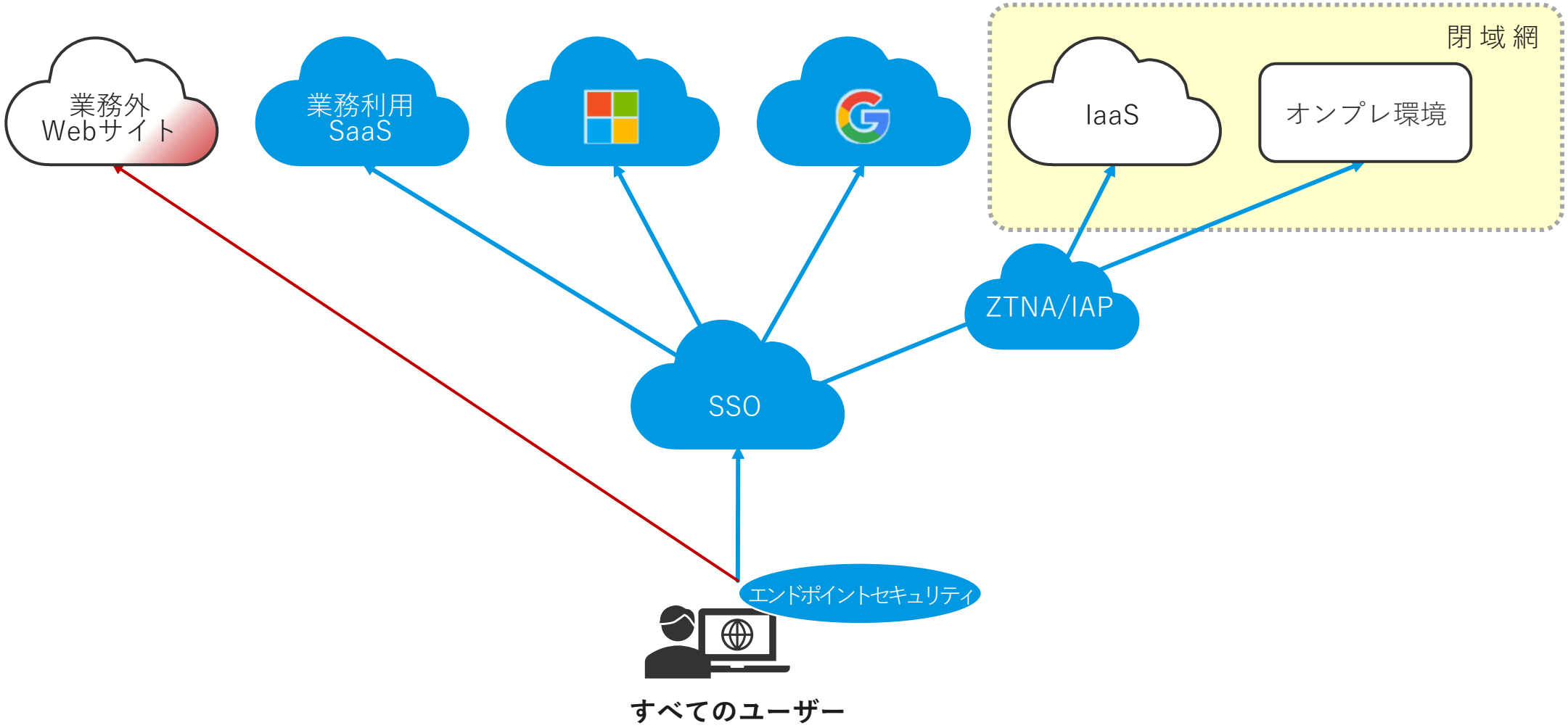
青 … ゼロトラスト対応



KAMOME Engineering

❷ 閉域網内のリソースにも、接続コントロールを行う

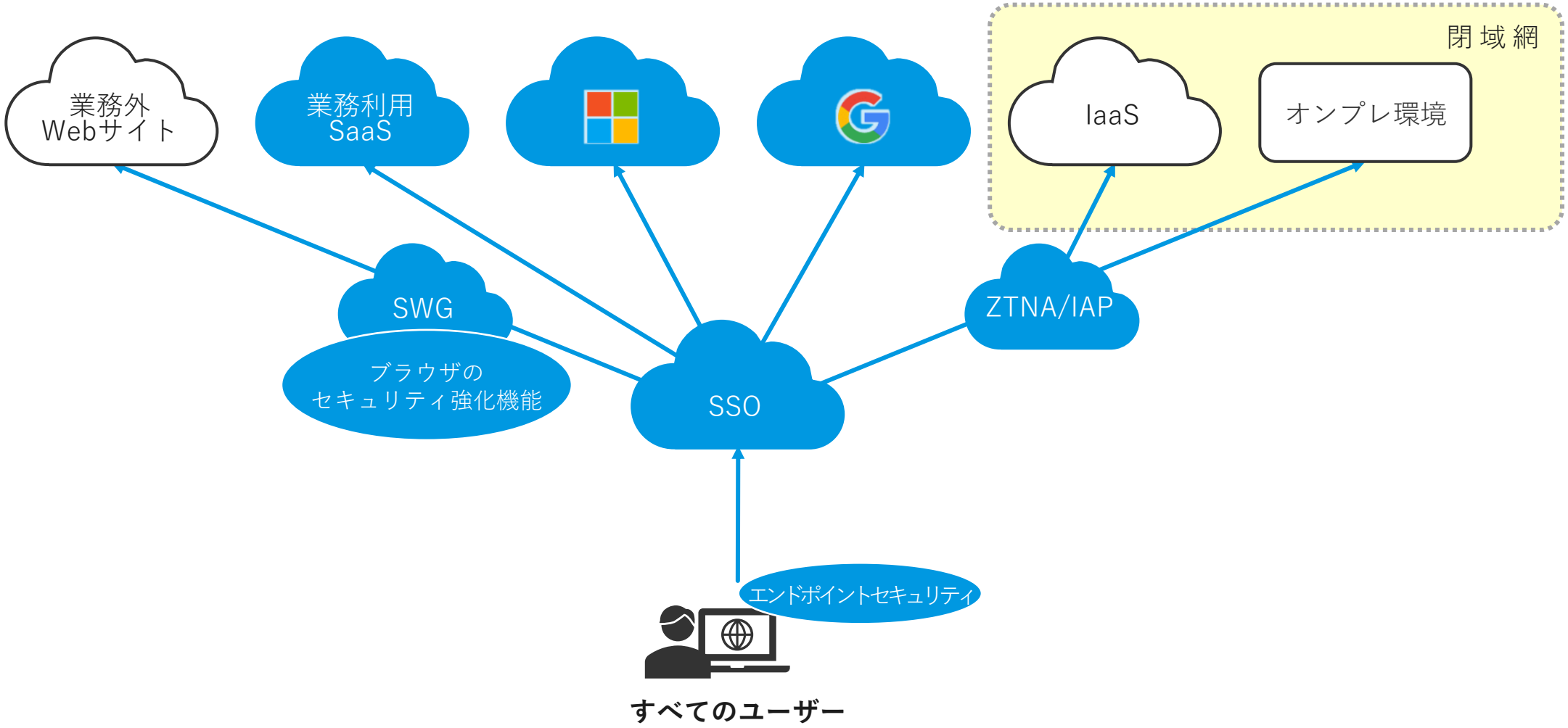
青 … ゼロトラスト対応



KAMOME Engineering

❸ SWG/Webブラウザの機能によるフィルタリングを行う

青 … ゼロトラスト対応



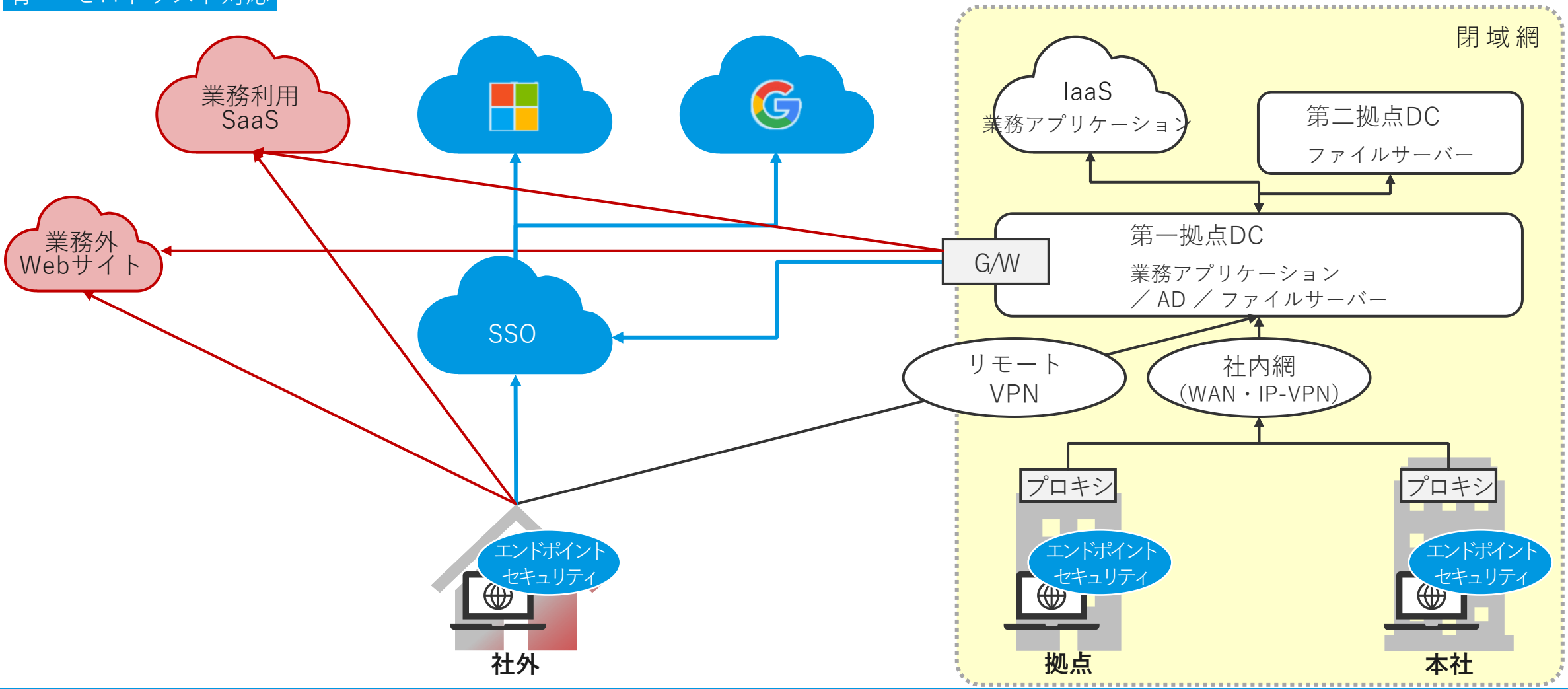
KAMOME Engineering

実現フェーズを
各課題に沿ってもう少しこまかく

KAMOME Engineering

現状

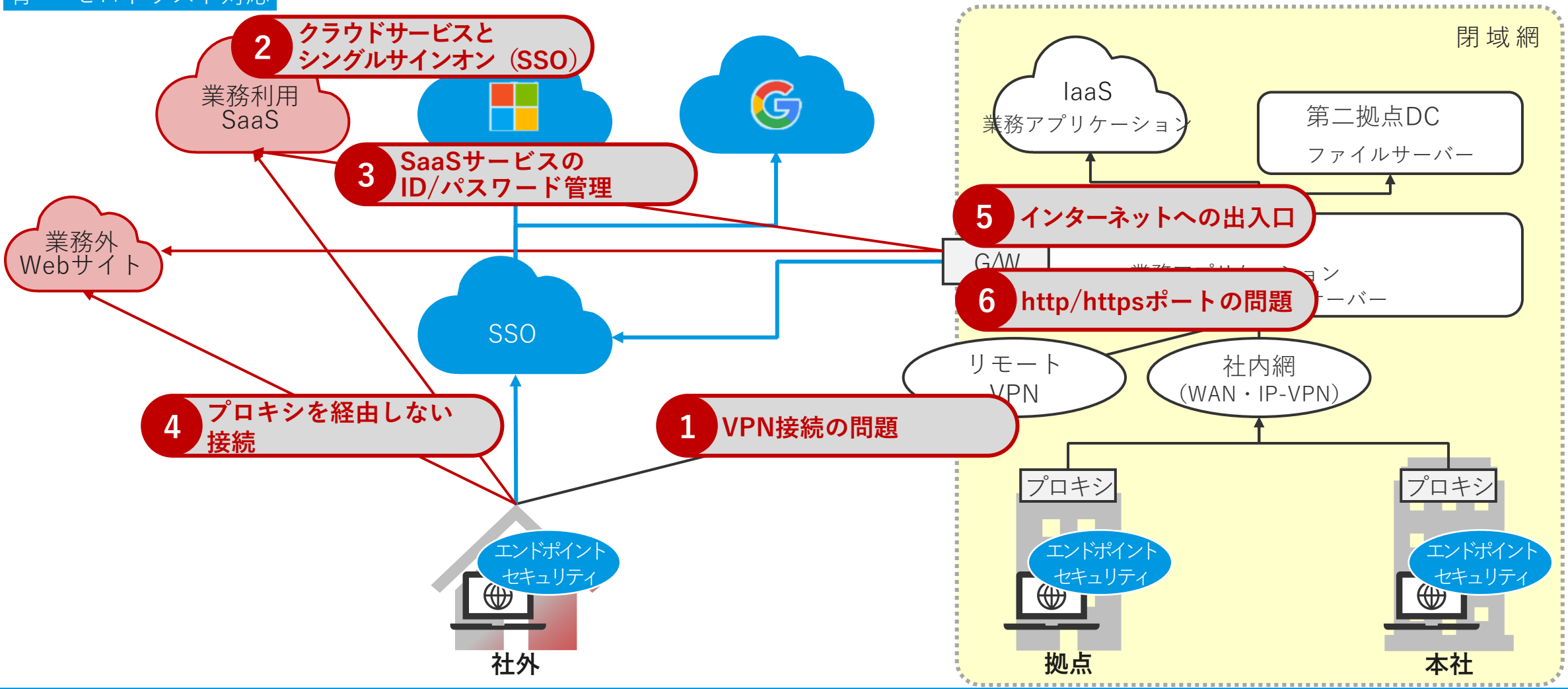
青 … ゼロトラスト対応



KAMOME Engineering

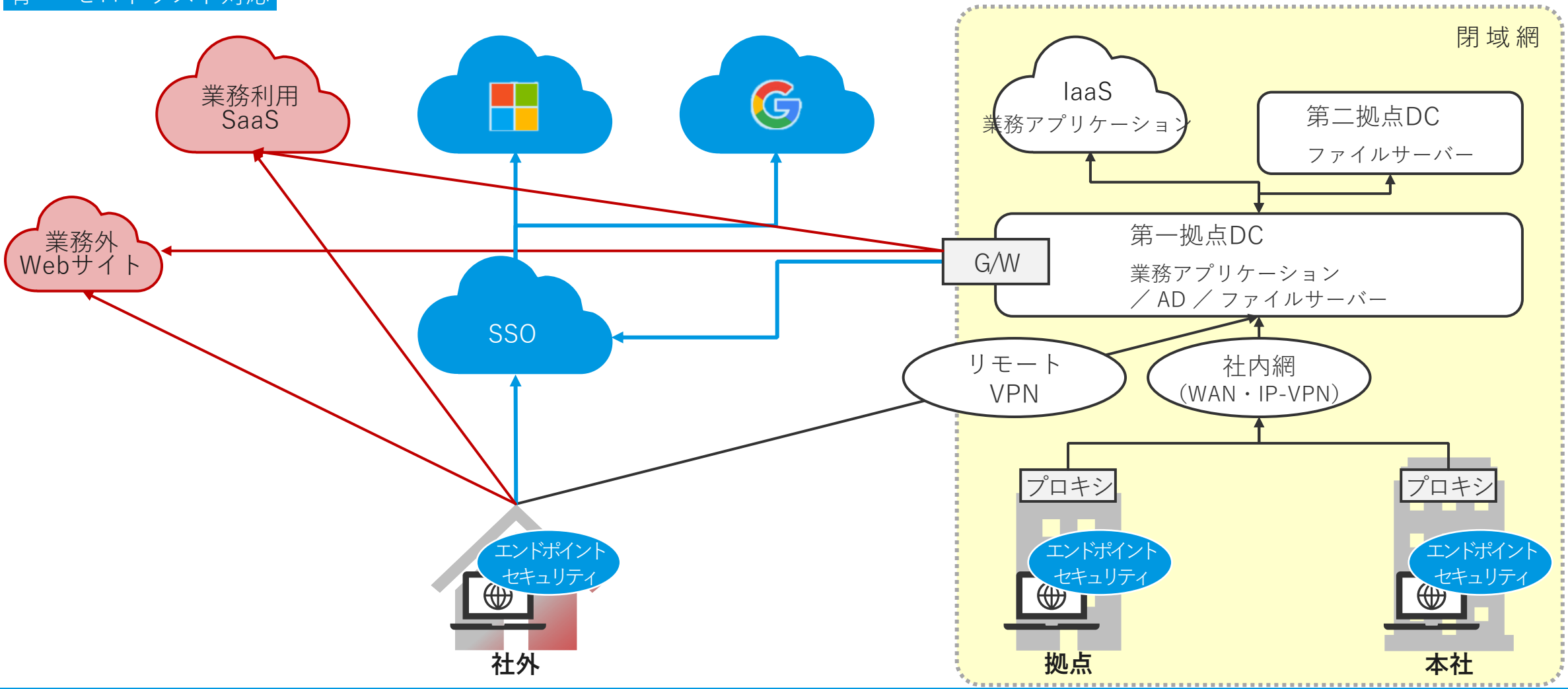
よく寄せられる課題

青 … ゼロトラスト対応



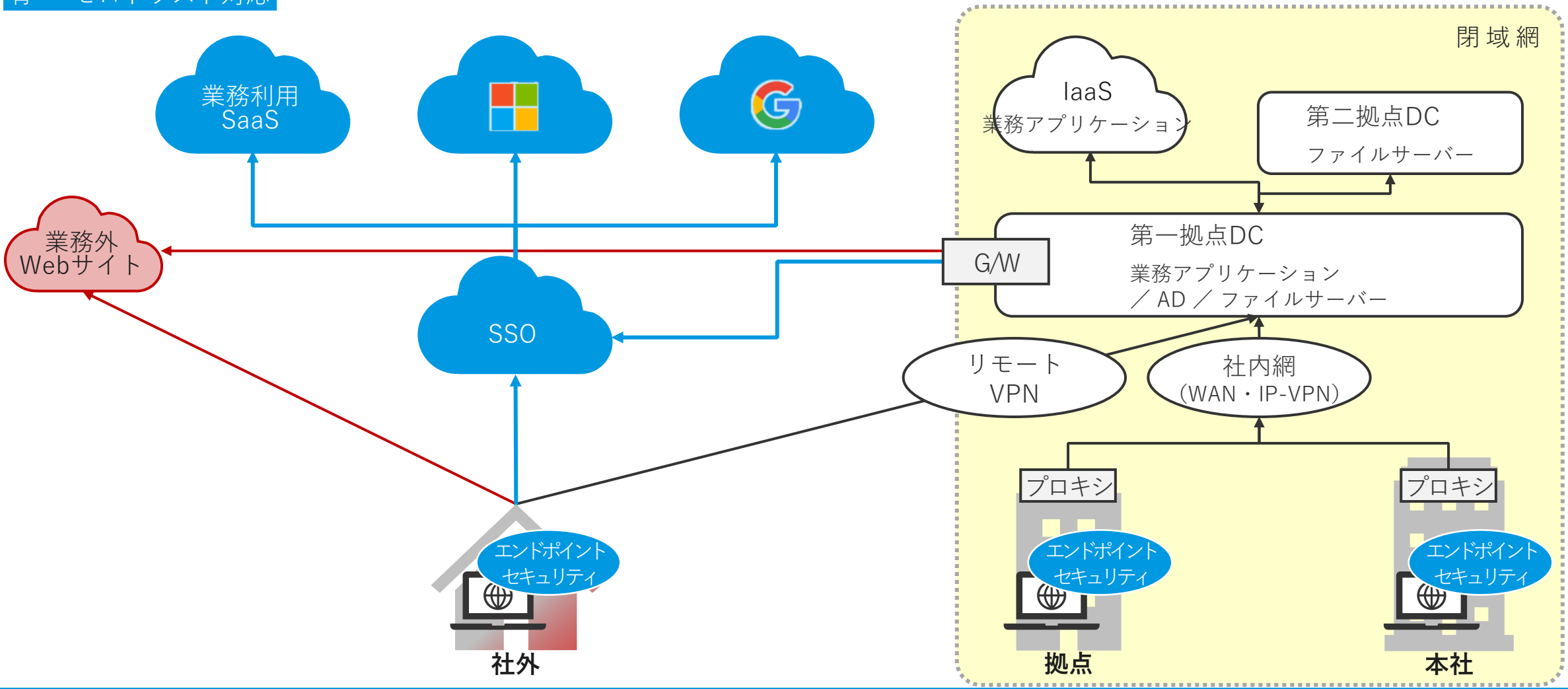
Phase ❶　業務利用SaaSをSSO利用に

青 … ゼロトラスト対応



Phase ❶　業務利用SaaSをSSO利用に

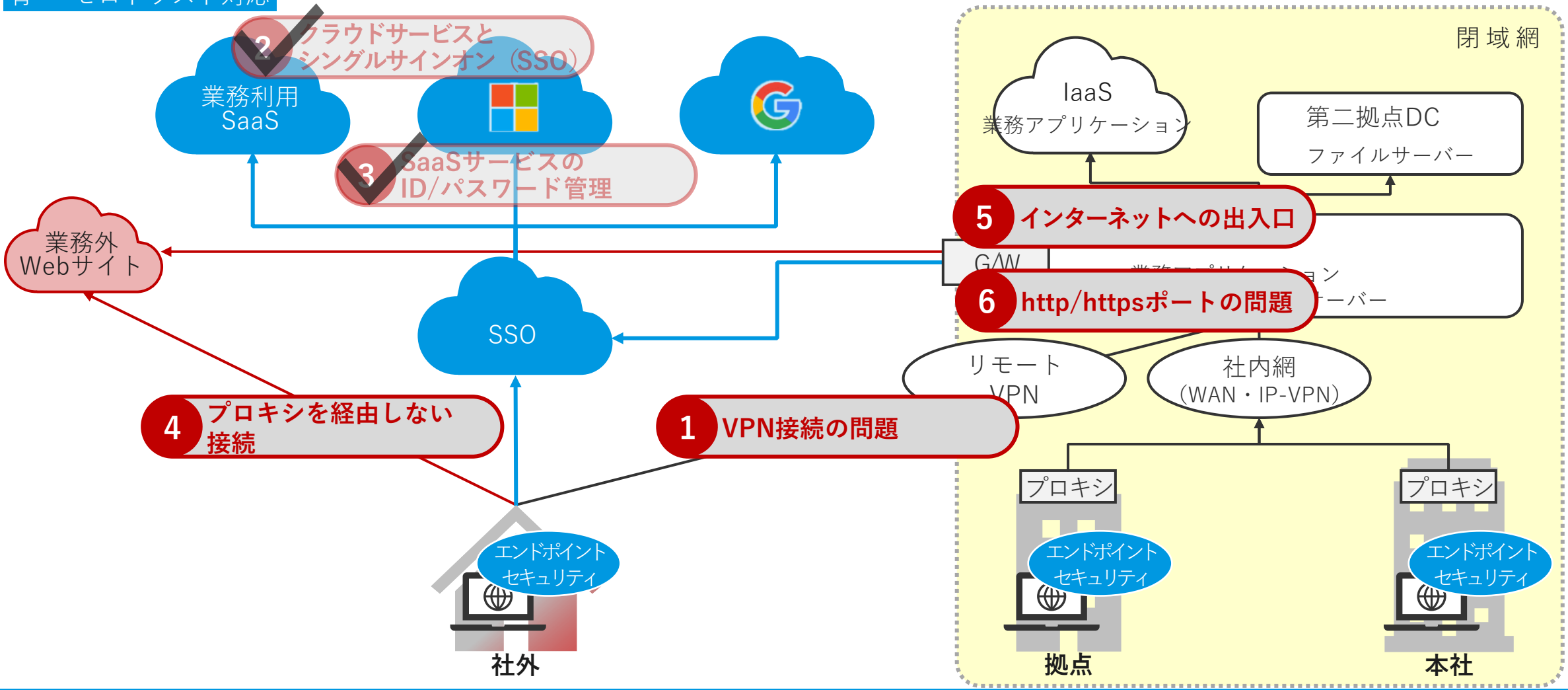
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❶　業務利用SaaSをSSO利用に

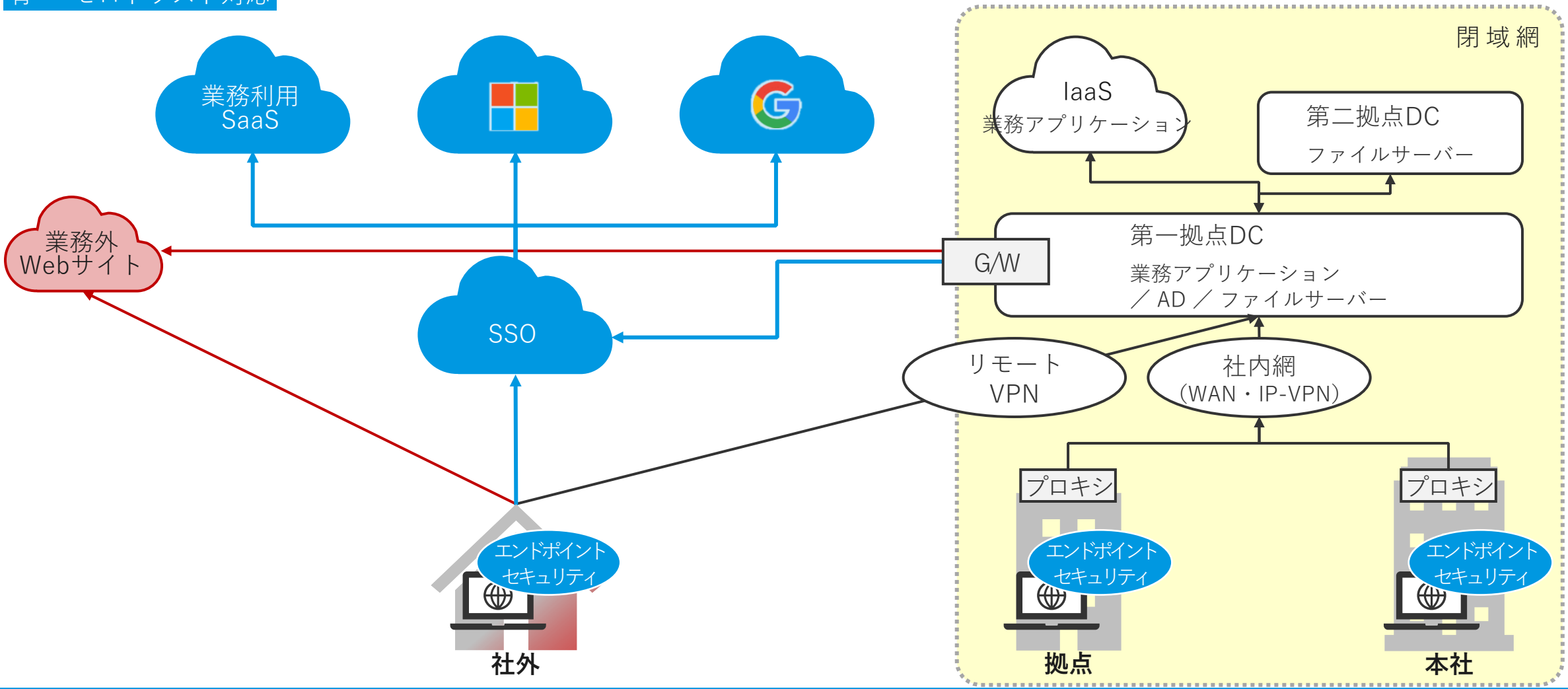
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❷　社外VPN廃止

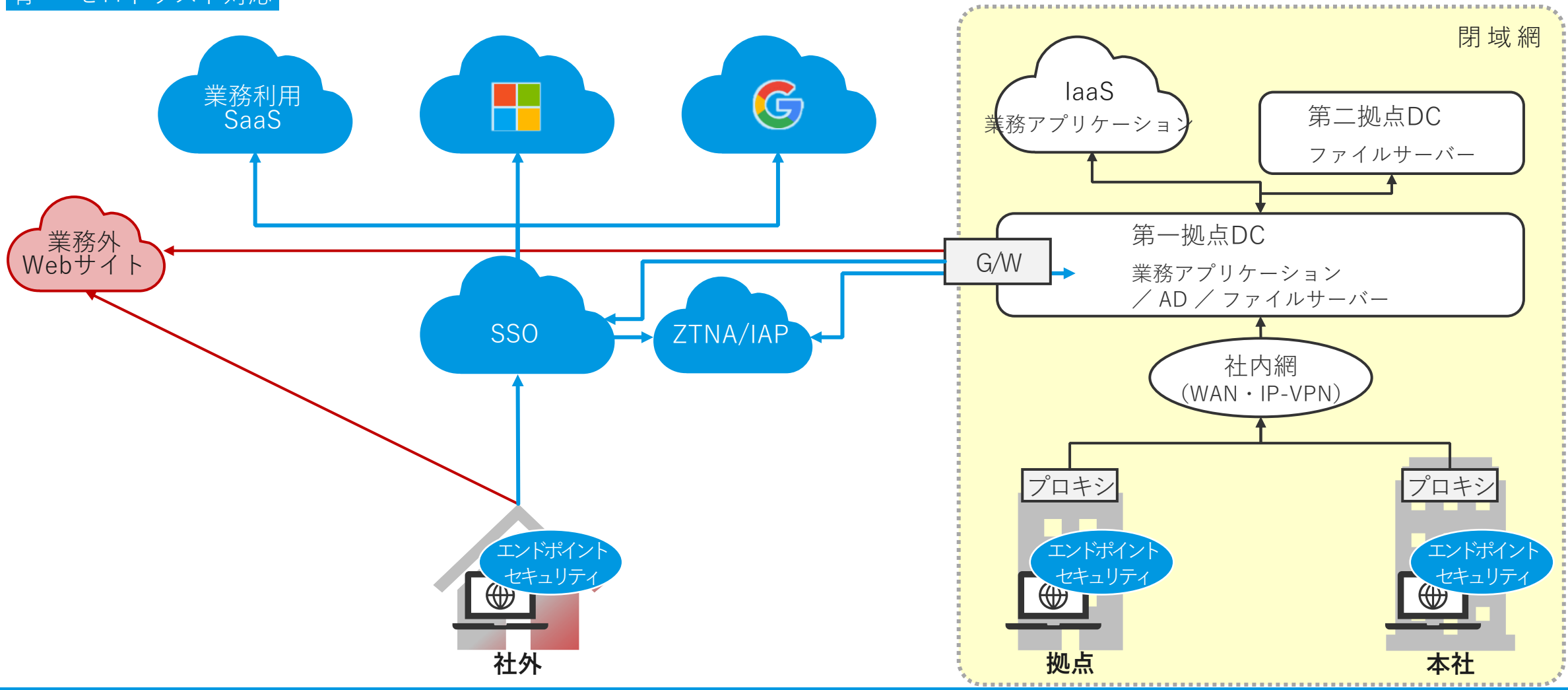
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❷　社外VPN廃止

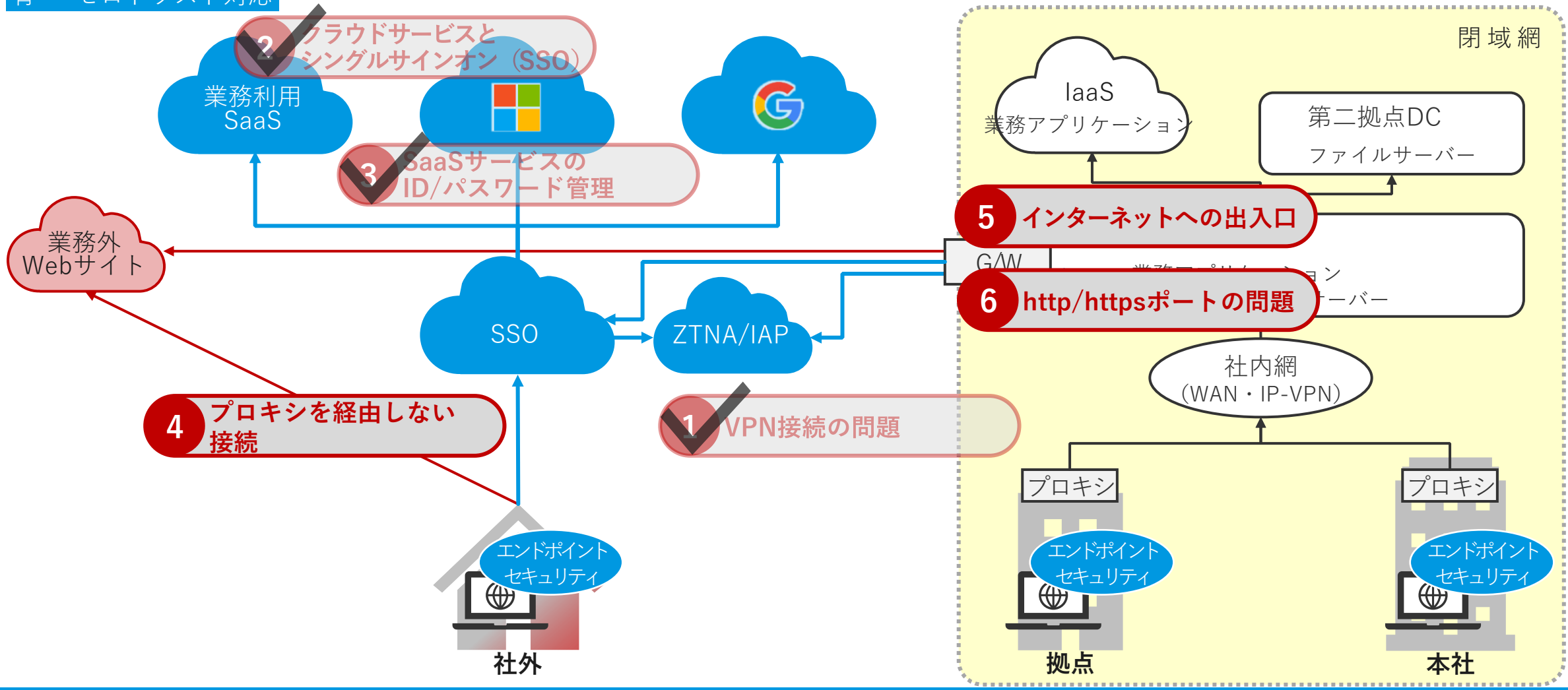
青 … ゼロトラスト対応



KAMOME Engineering

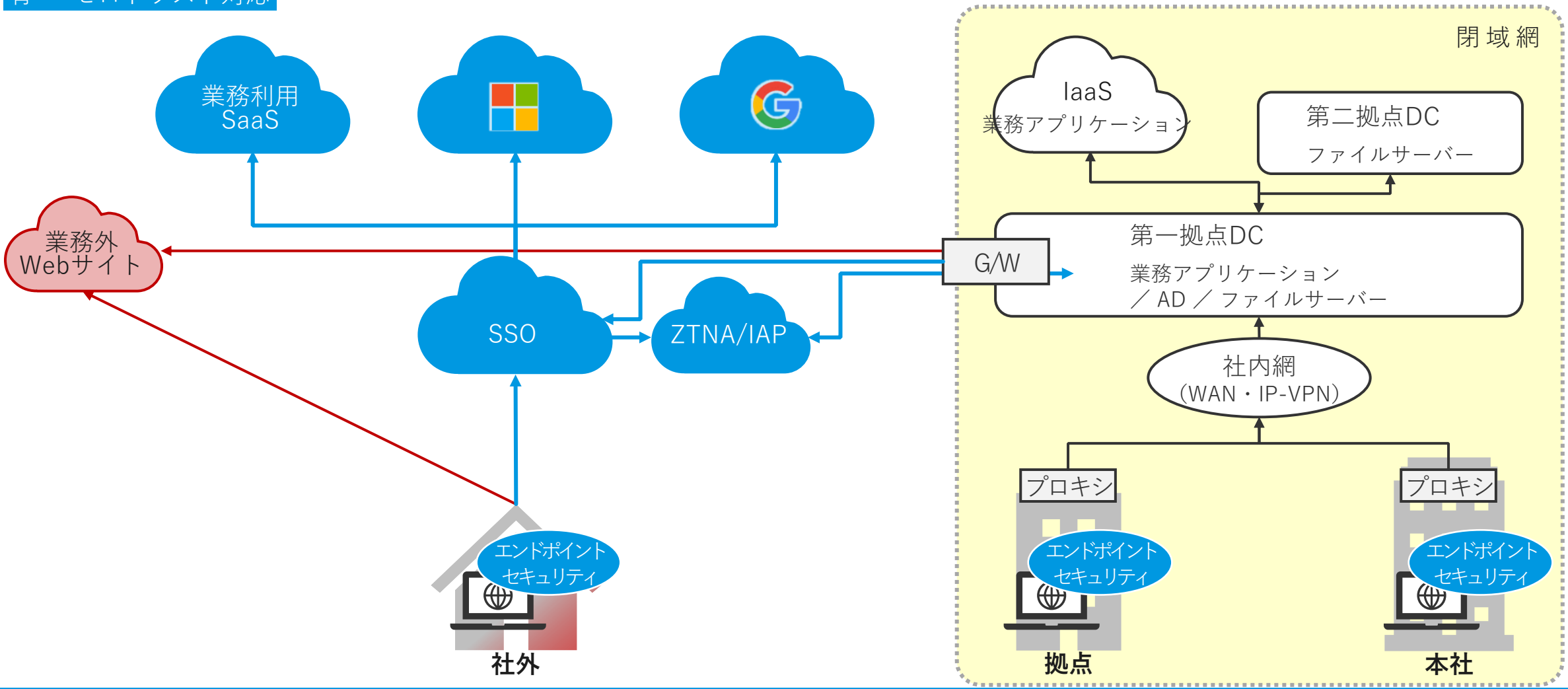
Phase ❷　社外VPN廃止

青 … ゼロトラスト対応



Phase ❸　社外アクセスの制御

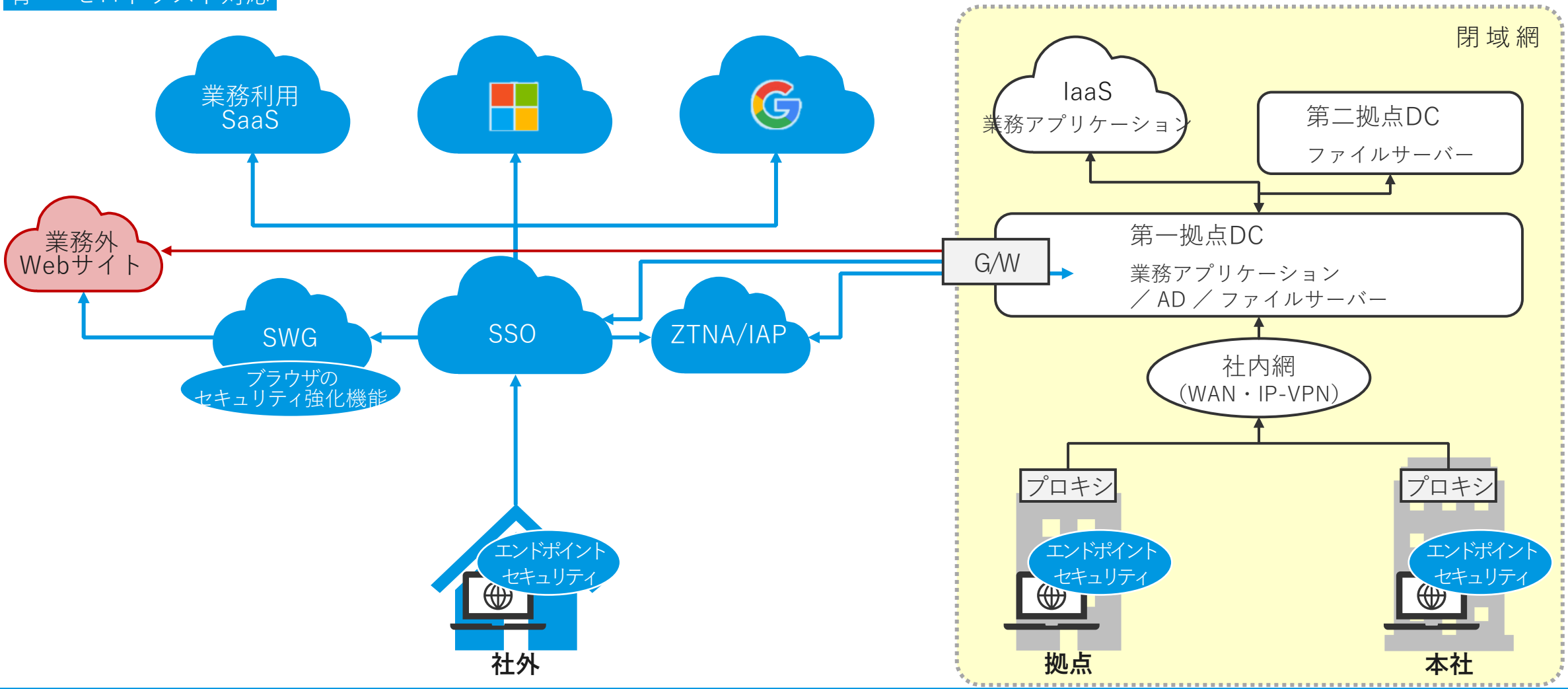
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❸　社外アクセスの制御

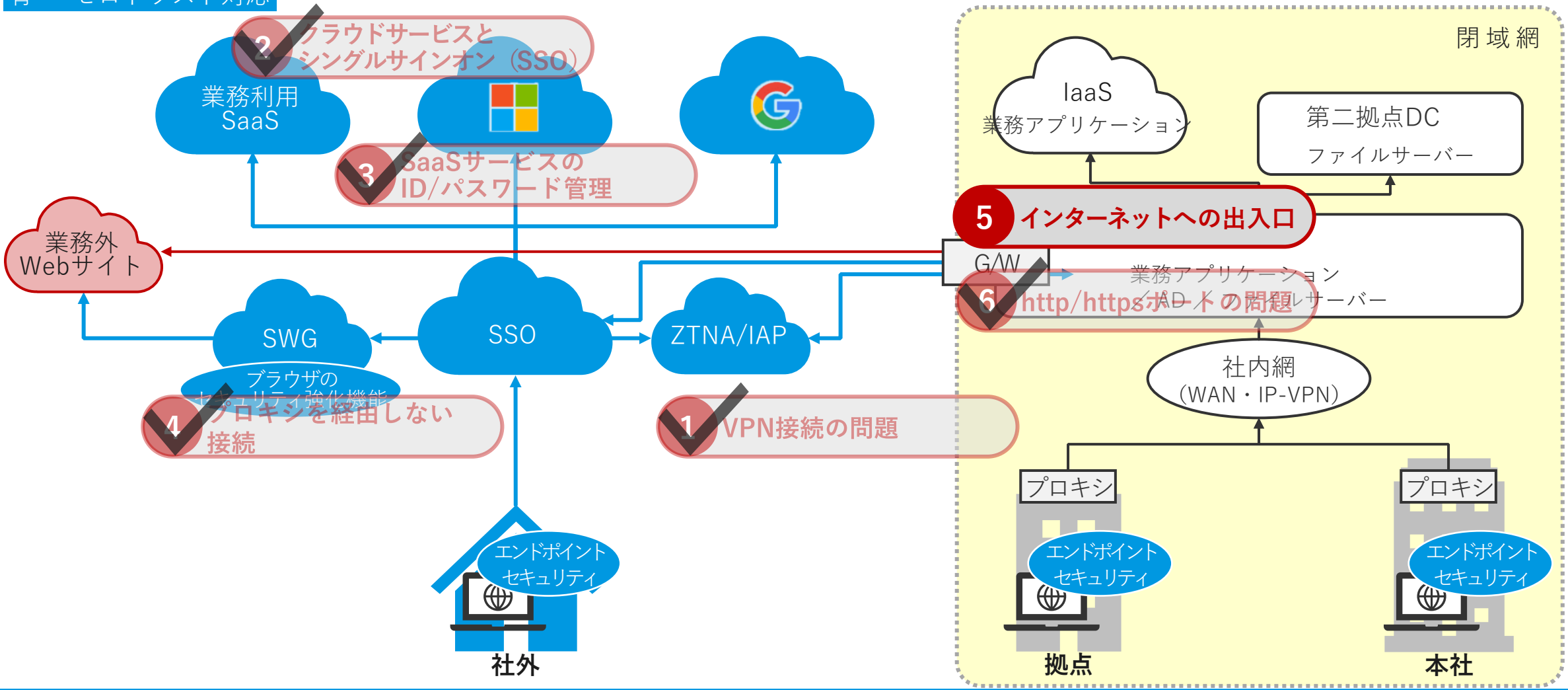
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❸　社外アクセスの制御

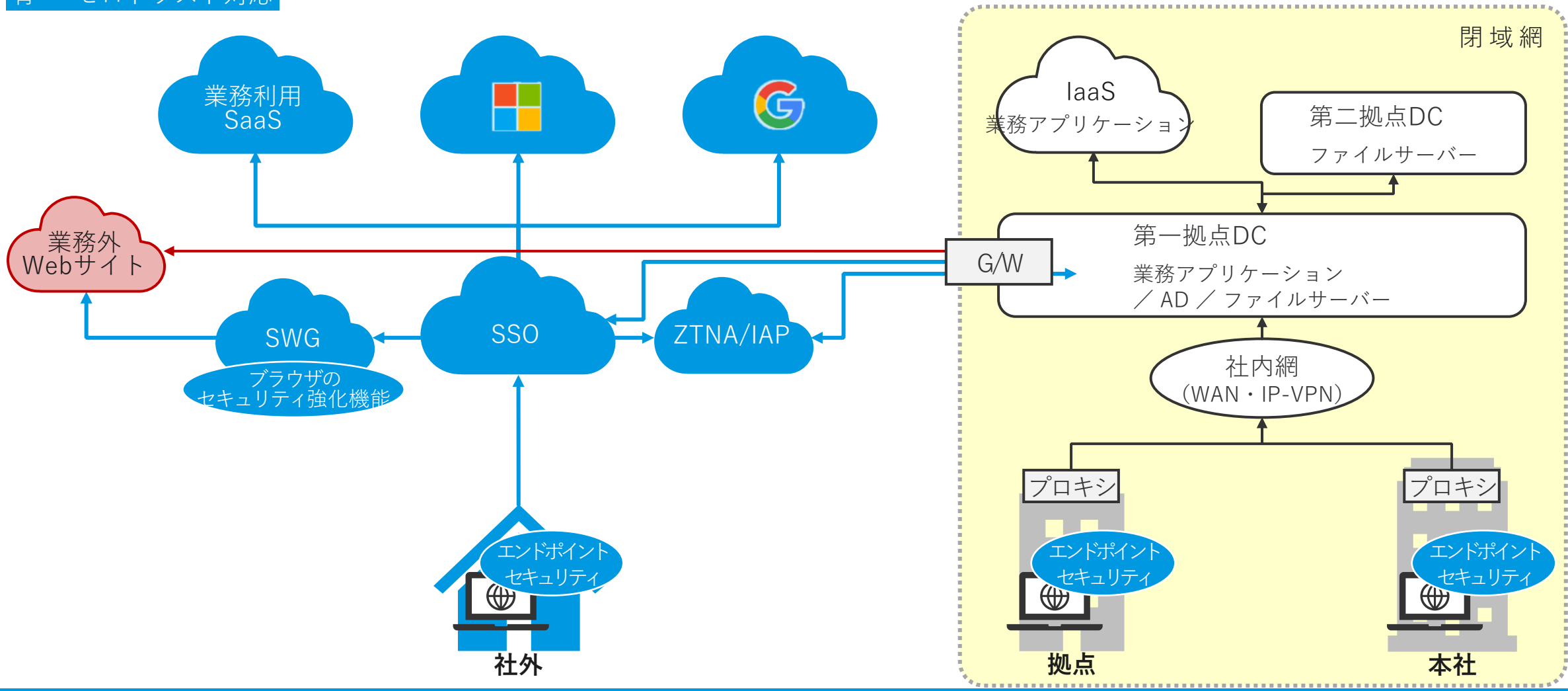
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❹　一部拠点VPN離脱

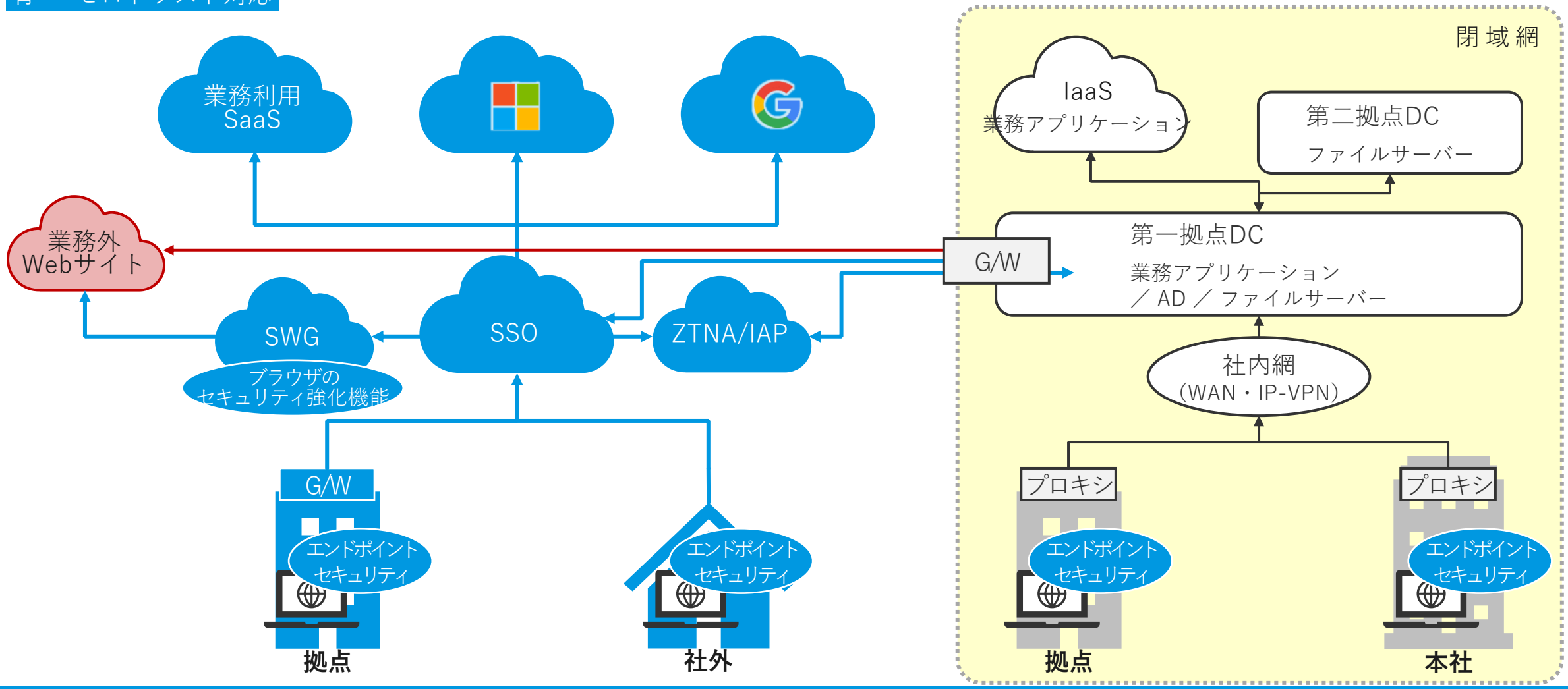
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❹　一部拠点VPN離脱

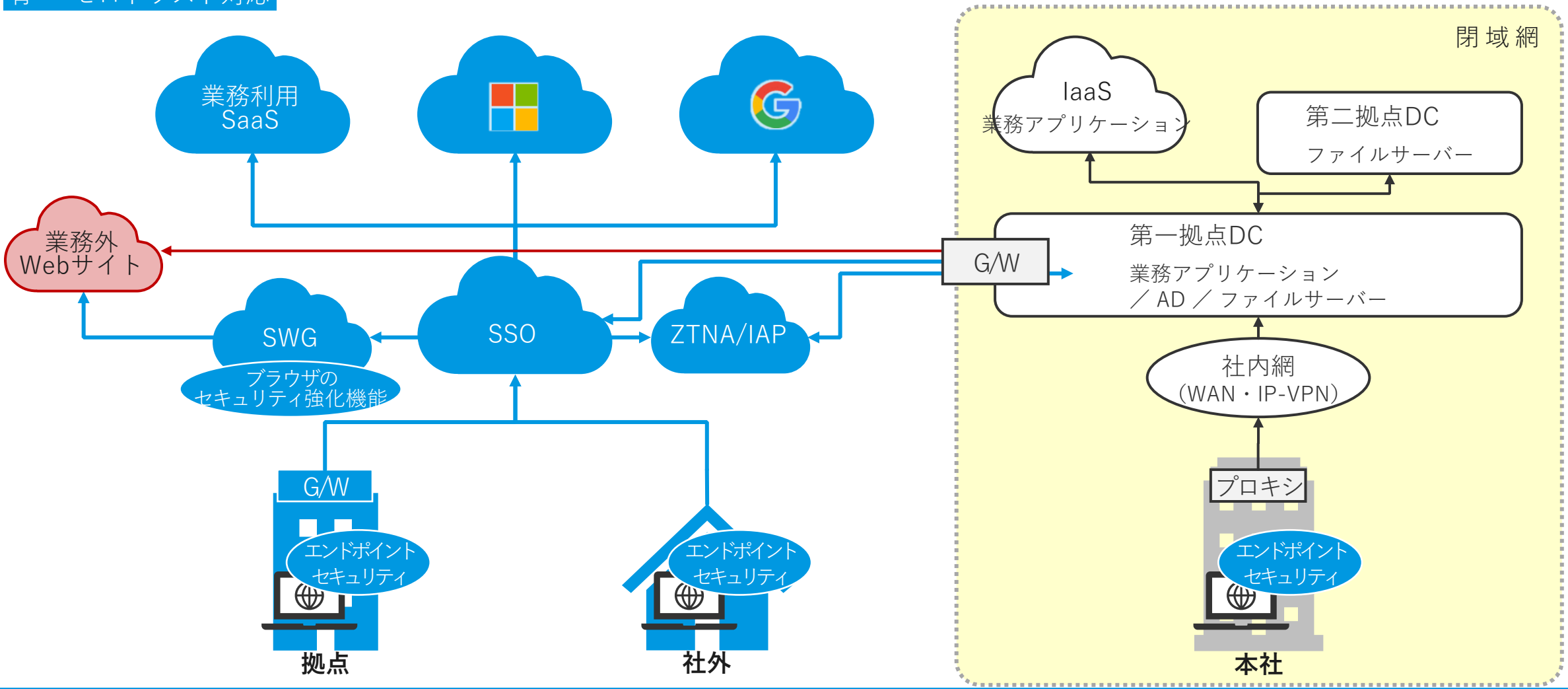
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❺　全拠点VPN離脱

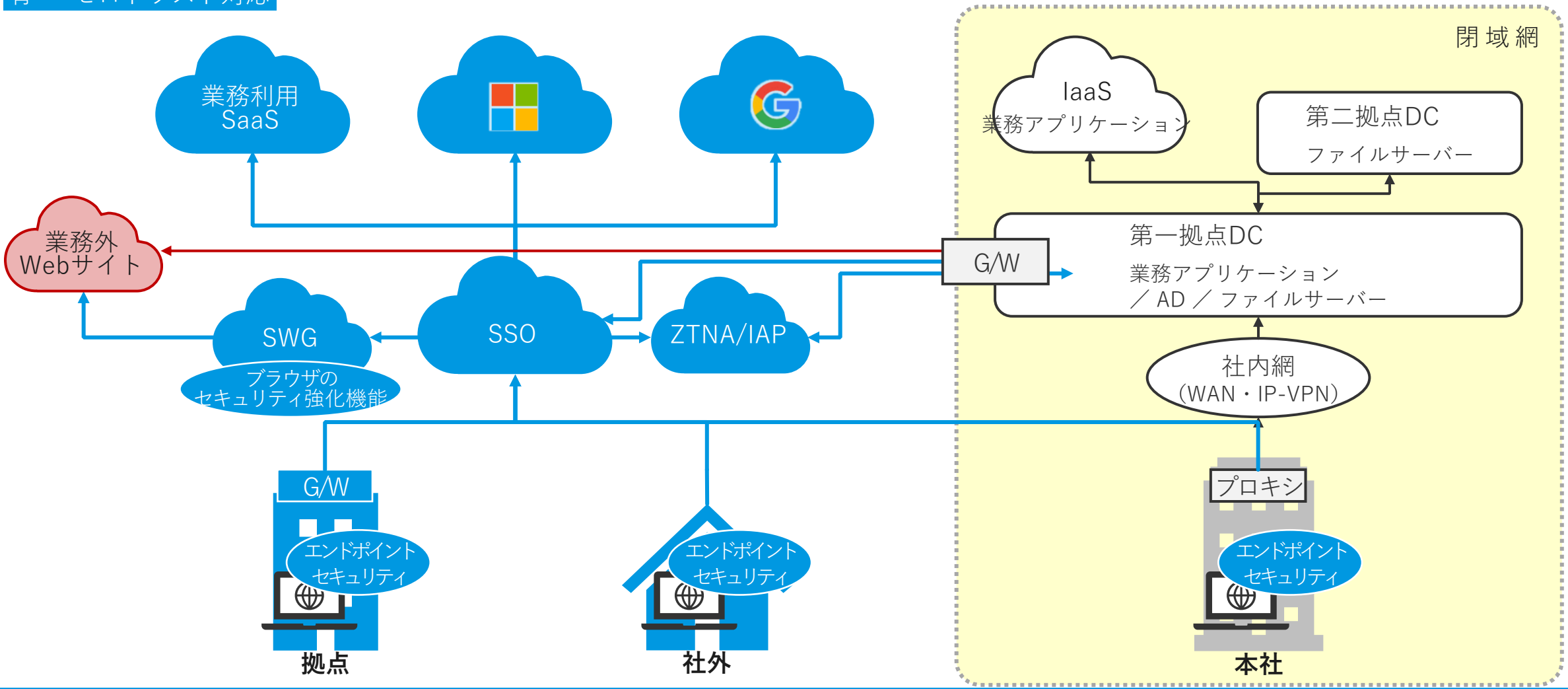
青 … ゼロトラスト対応



KAMOME Engineering

Phase ⑥　本社VPN離脱

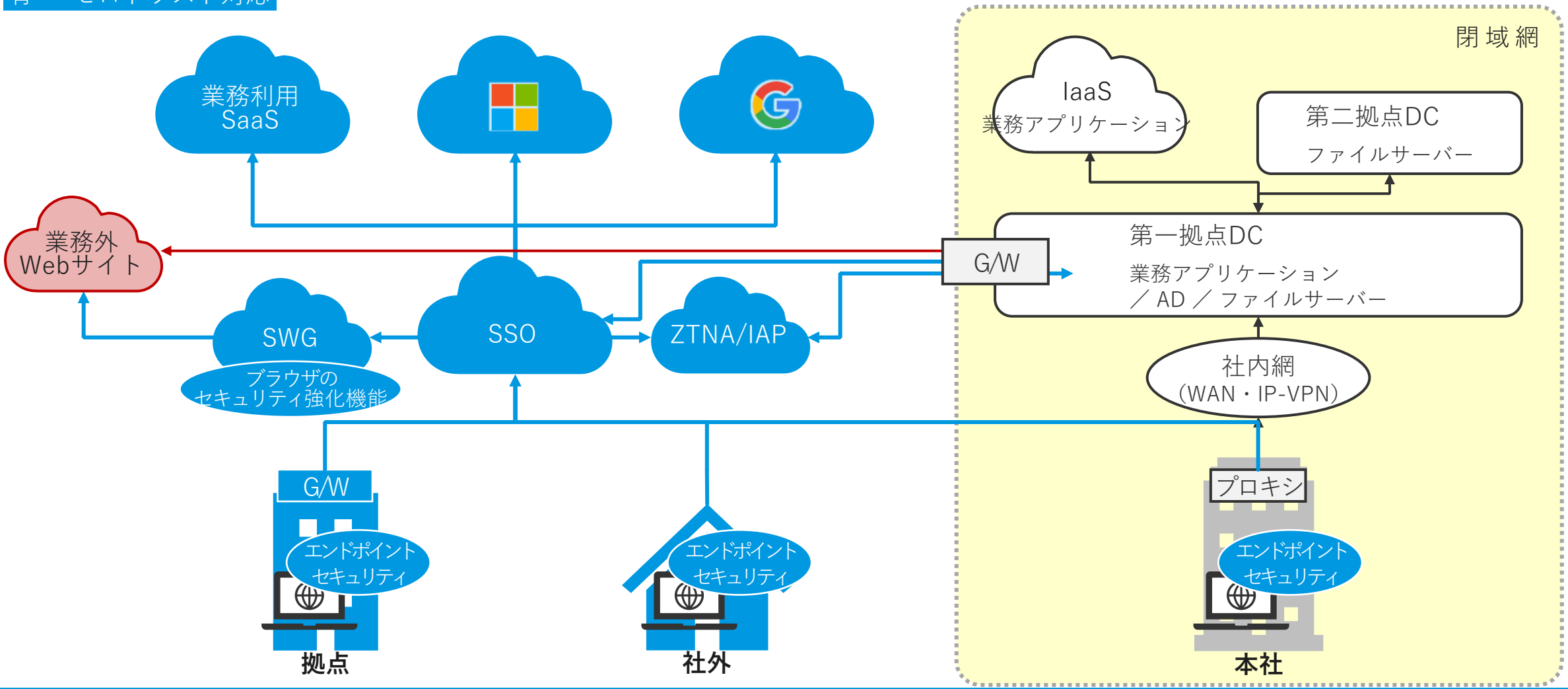
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❼　DC・本社間VPN網撤去

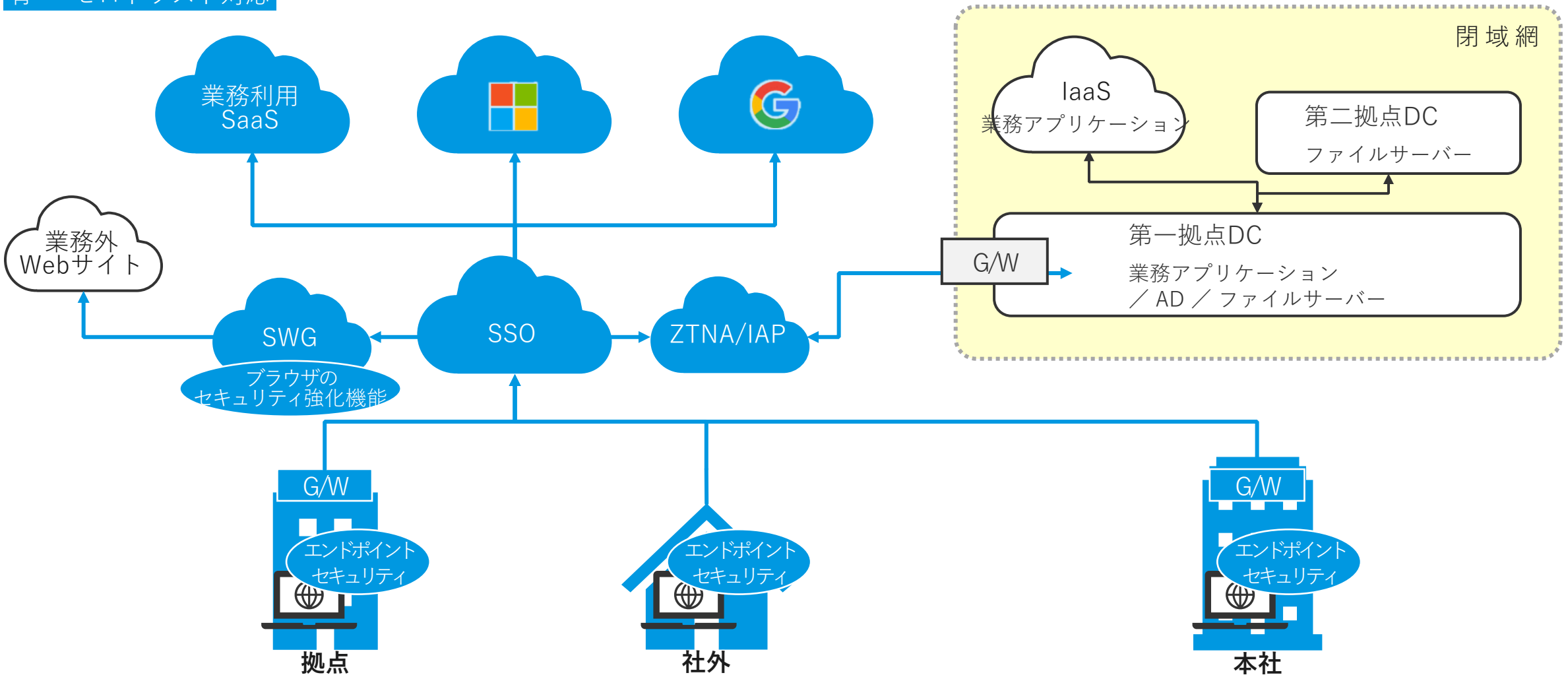
青 … ゼロトラスト対応



KAMOME Engineering

Phase ❼　DC・本社間VPN網撤去

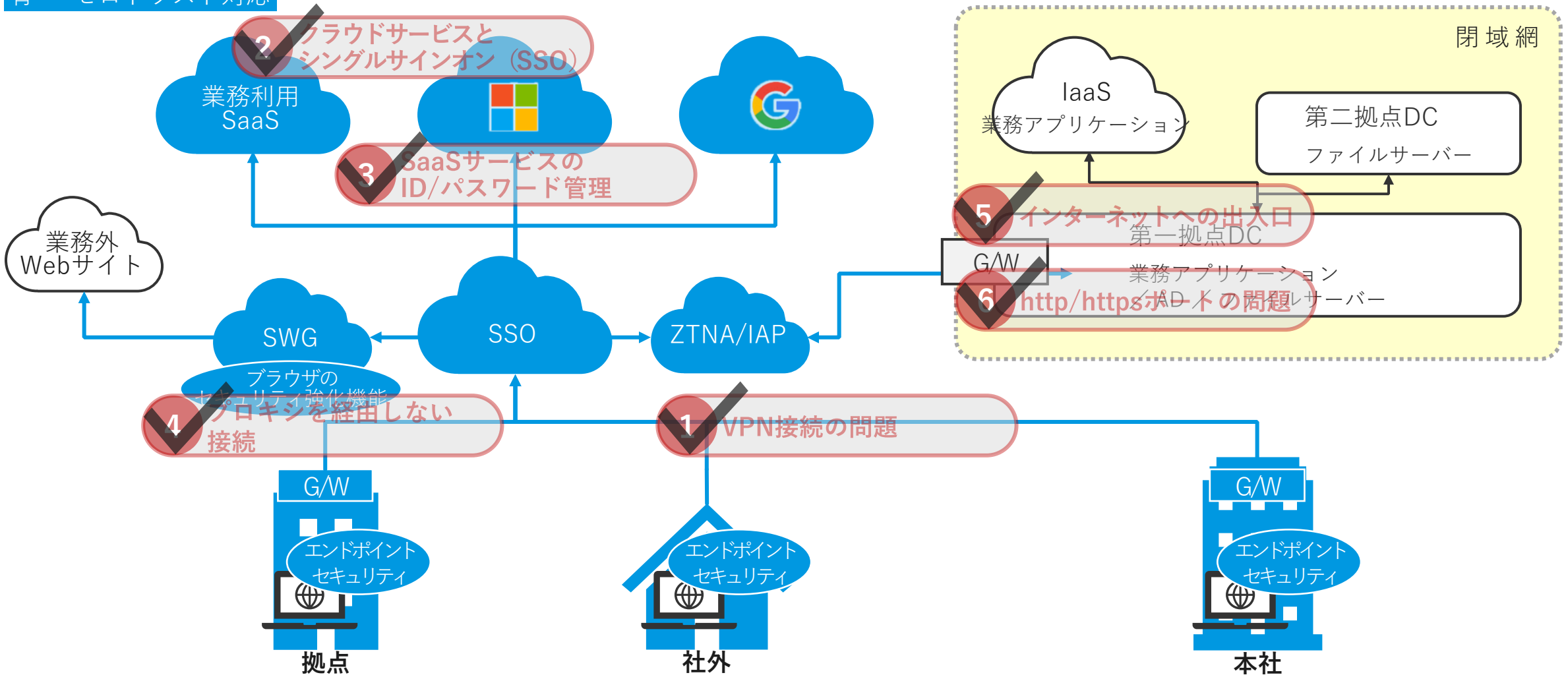
青 … ゼロトラスト対応



KAMOME Engineering

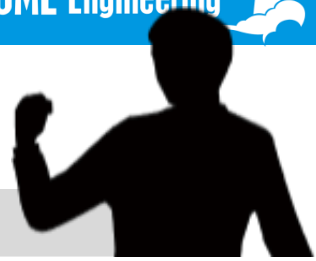
Phase ❼　DC・本社間VPN網撤去

青 … ゼロトラスト対応



各課題を解決

KAMOME Engineering



課題	解決
❶ VPN接続の問題	
社外から接続する際にVPN接続が不安定であり、使い勝手が悪い	ZTNAを採用。リモートアクセス手段をZTNAに切り替えて、回線数や容量不足、パスワード管理の不便さなどから解放
❷ クラウドサービスとシングルサインオン（SSO）	
一部のクラウドサービスがSSOを経由せずにアクセスされている	SSOを適用。業務で利用するクラウドサービスをすべてSSOの対象とすることで、セキュリティと利便性を向上
❸ SaaSサービスの、ID/パスワード管理	
多数のSaaSサービスに異なるID/パスワードが必要で、ユーザーは混乱し、管理者は管理が複雑になる	SSOを適用。業務で利用するクラウドサービスをすべてSSOの対象とすることで、セキュリティと利便性を向上
❹ プロキシを経由しない接続	
社外からのインターネットアクセスがプロキシを経由しないため、制御外の閲覧が可能	Webブラウザのセキュリティ強化機能の活用、あるいはSWGの採用。危険なサイトの閲覧を制御
❺ インターネットへの出入口	
インターネットの接続ポイントが1つしかなくアクセスが集中する	拠点間VPNの廃止。VPNでのデータセンターアクセスをやめてインターネットへ直接アクセスへ切り替えてアクセスを分散
❻ http/httpsポートの問題	
http/httpsポートが開いており、その通信を使った不正アクセスが制御できない	データセンター内の社内システムへの接続にZTNAを採用することで、認証と認可を受けたアクセスだけに限定

KAMOME Engineering

構成要素のまとめ

	まずは	あるいは	余裕ができれば
エンドポイント セキュリティ	**ウィルス対策ソフト**の機能強化、 **Microsoft Defenderなど**OSのセキュリティ機能、 などを活用		EDR、XDR
業務用SaaSへの アクセス制限	SSO 中小規模なら **IDaaS**の活用を検討 Microsoft365の**Entra ID**活用も	SSO 中堅以上なら **自社専用IdP**の活用も要検討 Microsoft365の**Entra ID**も活用	SASE、SSE
業務外Webサイトへの アクセス制限	**Webブラウザのセキュリティ機能**を活用 Edge …「セキュリティ強化」 Chrome …「セーフ ブラウジング」	SWG	SASE、SSE
社内システムへの アクセス制限	SSOと連携したアクセス制御 **ZTNA**（アクセス可能リソースの制御）、 **ZTNA＋代理認証**（上記＋利用者のパスワード管理を廃止）		SASE

次セクションでご紹介します

かもめからご提案するZTNAソリューション

KAMOME Engineering

2つの課題を解決できます。

❶

SAML等のフェデレーション方式に非対応のシステムはSSO対象から外されがち

❷

社内ネットワークへのアクセス経路は、VPNを使うことが多く心配

認証統合できるだけでなく、
より厳密なアクセスコントロールが
可能になります。

暗号化されたトンネリング通信により
VPN以上のセキュリティが実現します。

ZTNAを簡単に利用するには、どうすれば…？

海外グローバルベンダーが提供している
大規模向けサービスがあります

でも、あんなに多機能じゃなくていいし、
何よりあんなに高額では手が出ないんですよね

ゼロトラスト接続サービス
Keygateway C1

がお役に立ちます。

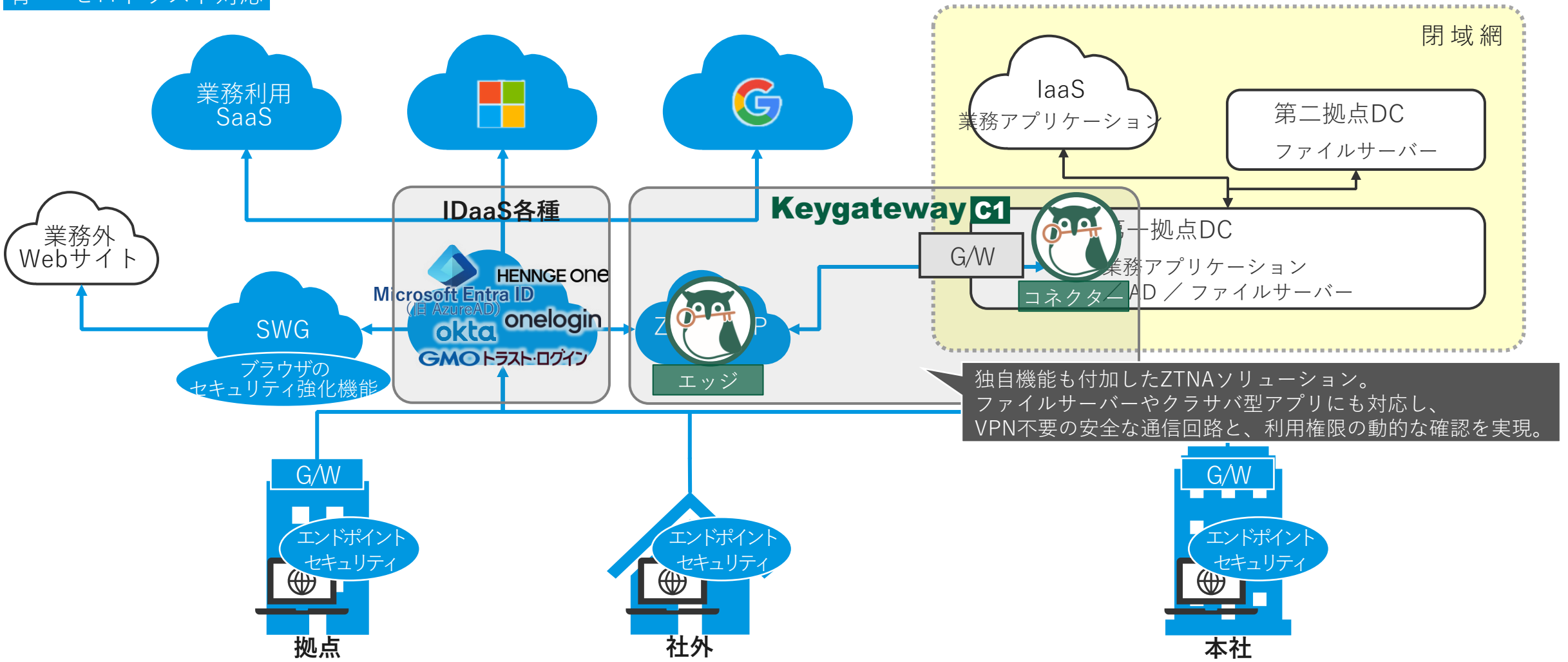
選ばれる理由

ゼロトラスト接続サービス
Keygateway C1

- IDaaSと組み合わせ、パスワード不要で
  Webアプリに簡単アクセス
- 社内のファイルサーバや
  クラサバ型アプリにも利用可能
- クラウドサービスで運用負荷を低減
  設置・サポートは国内提供
- 企業が今必要とするシンプルなZTNA、
  他製品との組合せも可能
- そして、高いコストパフォーマンス

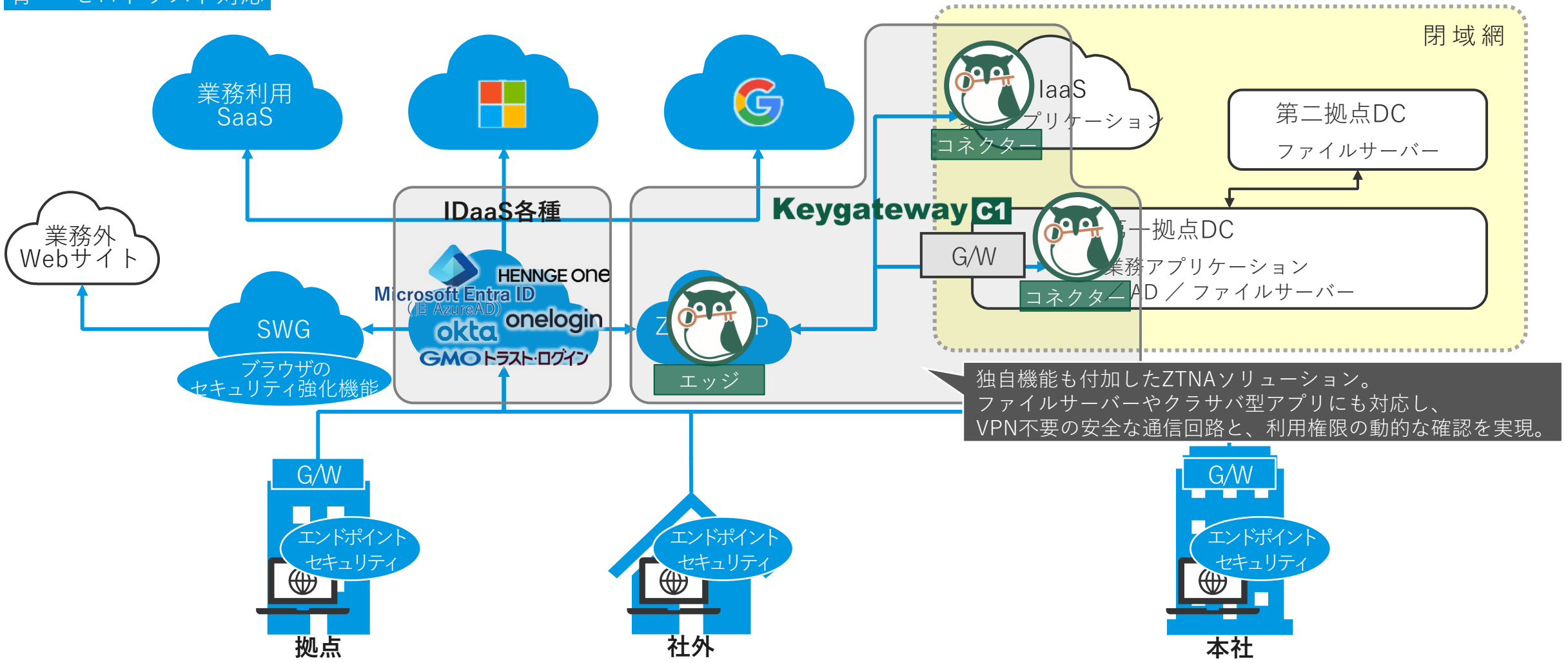
Webアプリ以外のシステムにも、ZTNAを適用

青 … ゼロトラスト対応



※ 拠点～IaaS間のシステム連携がない場合

青 … ゼロトラスト対応

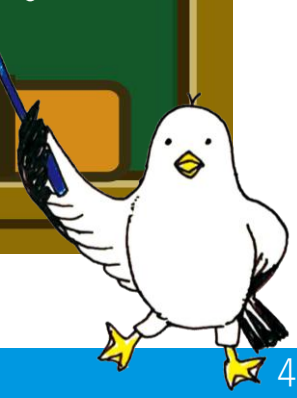


部分導入 ➡ 対象の拡大　も容易です

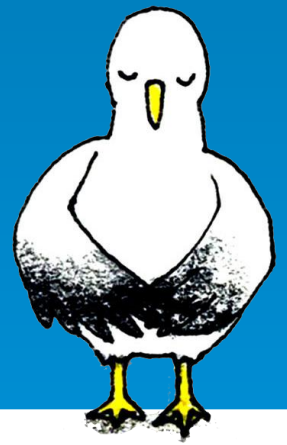
部署・事業所ごとに	属性・雇用形態ごとに	役職ごとに	勤務形態ごとに
例 「機密性の高い情報を 扱う部門から先に」	例 「関係会社など 外部スタッフの アクセス管理強化を」	例 「権限の大きな 役職者を優先したい」	例 「まずは リモートワーカーを 対象に」

まとめ

- お受けすることが増えたご相談をもとに、代表的なケースを想定しました。
- 高機能なSASEサービスでは、すべてを一括管理できるものもあります。
  それに比べると、今回ご紹介したような複数サービスの組合せは、
  管理のポイントが複数になる点は課題となります。
- 皆さまそれぞれの課題に合致する部分・しない部分があると思いますが、
  一歩でもゼロトラスト化を進めるための参考になっていますと幸いです。
- 一般的なZTNAの機能にはない、代理認証機能やWebアプリ以外へのアクセス方式
  を追加したゼロトラスト接続サービス「KeygatewayC1」もお役に立ちます。
- SSOやID管理などの関連課題も、かもめの得意分野です。一度ご相談ください。
  課題を伺い、御社にとっての最適の解決方法を一緒に考え、ご提案します。



ありがとうございました



■ **お問い合わせ先**

- かもめインサイドセールスチーム　i-sales@kamome-e.com
- お問い合わせフォーム　https://solution.kamome-e.com/contact/

かもめエンジニアリング株式会社 KAMOME Engineering

日本でいちばん仕事が大好きなチームです！