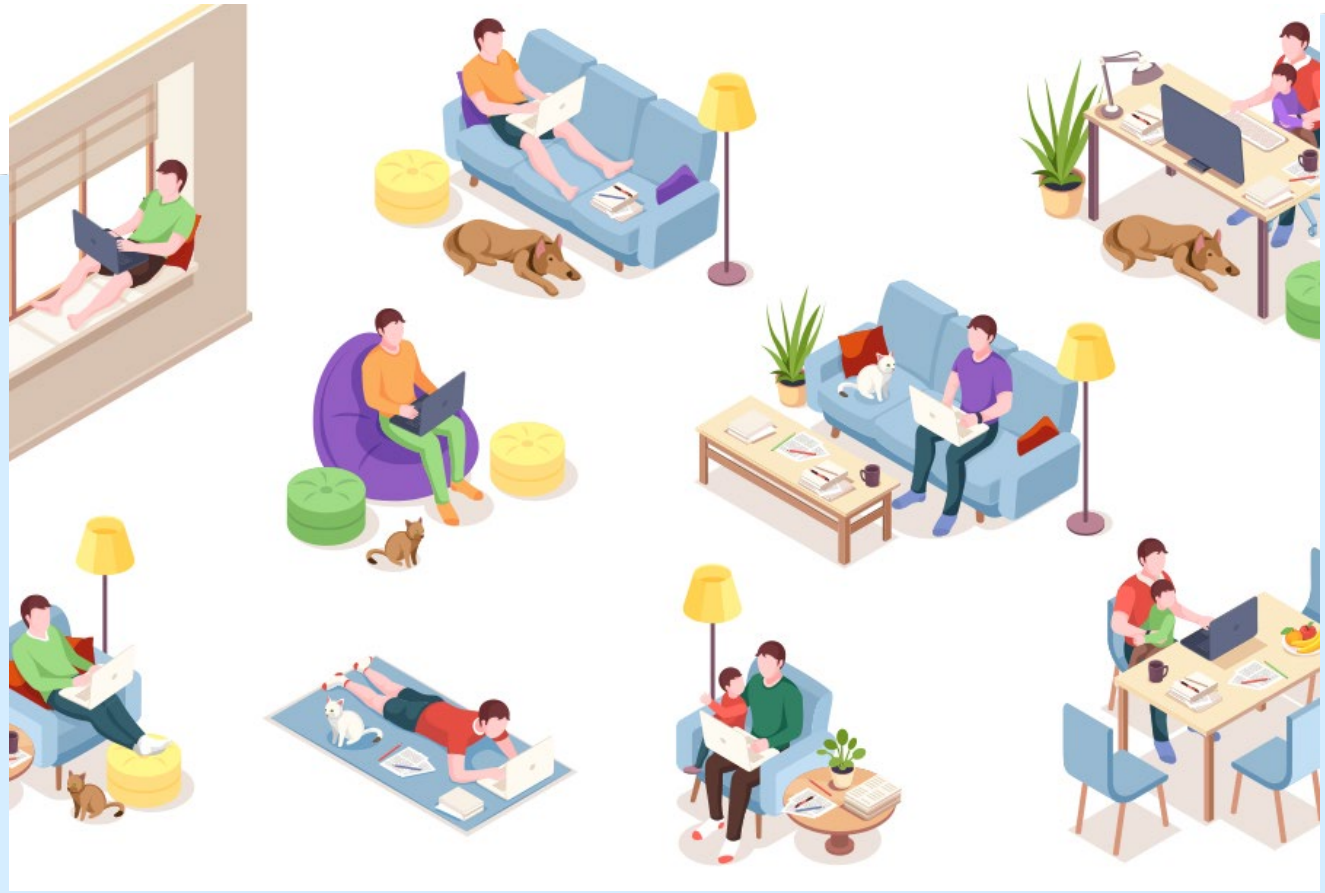
WSI Work Style Innovation

CLARA ONLINE

Work Style Innovation



セキュアで生産性の高い働き方の実現へ！

WSI Work Style Innovation

ニューノーマルな働き方の実現を目指すIT部門の方へ

Clara WSI Solutionとは

ゼロトラストベースのセキュアなテレワーク環境を
実現するクラウド活用ソリューションを、
ワンパッケージで提供するソリューションです。

特徴

- ゼロトラスト基盤に必要な各種サービスを
  ワンパッケージでご提供
- 月額サブスクリプションモデルのため、
  初期費用を抑え、柔軟に利用が可能
- クララオンラインが窓口となり提供するため、
  構成相談なども対応が可能
- IT部門のリソースが足りない企業でも、
  運用負担少なくセキュアに導入

COVID-19で半強制的に進んだ、在宅勤務へのシフト

コロナショックにより、様々な会社・業態に半強制的なリモートワーク＆テレワーク対応が迫られ、多くの企業が準備が整いきる前に「在宅勤務」にシフトしました。事業継続のため、ビジネスプロセスのオンライン化が迫られ、IT環境の見直しも余儀なくされています。これにより、2025年までの変革を一つの目標としていたデジタルトランスフォーメーション（DX）への取り組みが、一気に加速したといえるでしょう。

デジタルトランスフォーメーション(DX)※

課題１

ワーク環境(リモートワーク)の整備

- 働き方改革における社内制度整備
- 必要なツールの導入
- 優秀な人材の確保

課題２

ITを活用したビジネス促進

- 遠隔を前提とした業務やイベントの開催
- 必要なタイミングでのサービス提供
- 新たなチャネルの確保

- IT活用の必要性
- 意識の変化
- 連携が必要不可欠

課題３

レガシーシステムの刷新

- ビジネスITとの連携
- 情報の一元化/見える化
- 一枚岩でのITプロジェクト

※DX(Digital transformation) … 企業を取り巻く市場環境のデジタル化に対応するため、企業が行うあらゆる経済活動やそれを構成するビジネスモデル、ならびに組織・文化・制度といった企業そのものを変革していく一連の取り組み

リモートワークにおいての課題

リモートワーク導入における課題は様々ですが、主に3つに分類されます。
経営者視点からみた生産性やコスト課題、働く場所の確保やコミュニケーションコスト、
そして情報システム部に求められるセキュリティ担保や必要ツールの整備等があります。
今回ご紹介させていただくClara WSI Solutionは、情報システムのツール周りについてのご提案です。

経営者

- 生産性が下がらないか
- 就業規定の変更
- ツール整備のコスト

仕組み

従業員

- 働く場所の確保
- モチベーションの低下
- コミュニケーション

環境

WSI Work Style Innovation

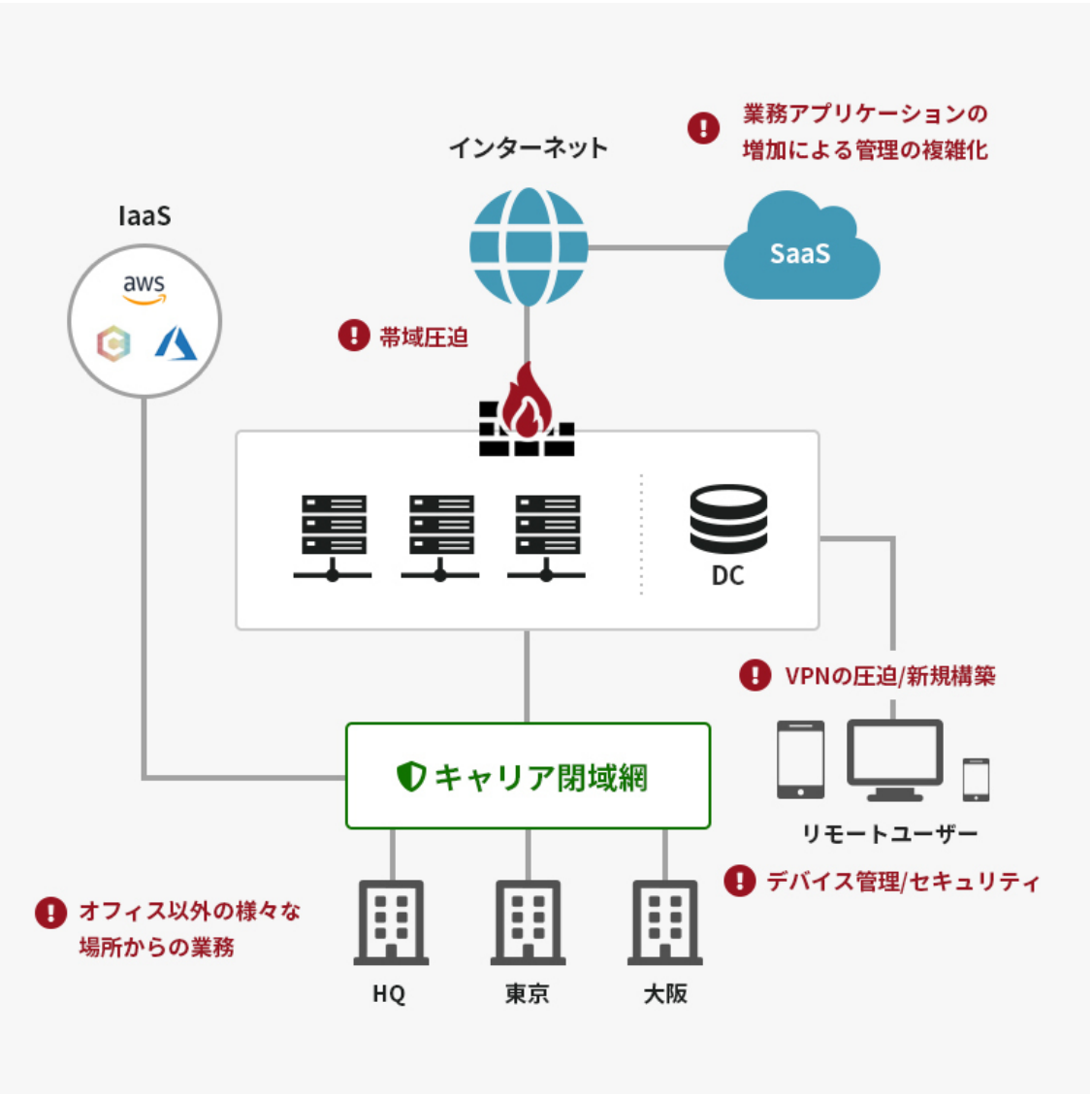
情報システム

- セキュリティの確保
- パフォーマンス
- 必要ツールの検討

ツール

リモートワークによる 従来型インフラの課題

以前はオフィス勤務が当たり前であり、オフィスから閉域網を利用してデータセンタへのアクセスをすることが一般的でした。
そんな従来型の情報システムの形のままリモートワークを実施すると様々な課題が発生します。
帯域の圧迫、情報システム部の運用工数・リソースの圧迫、セキュリティリスクなど、クリアしなければならない課題が山積しています。



クラウド活用自体にリモートワークに求められる ITインフラ/ツール

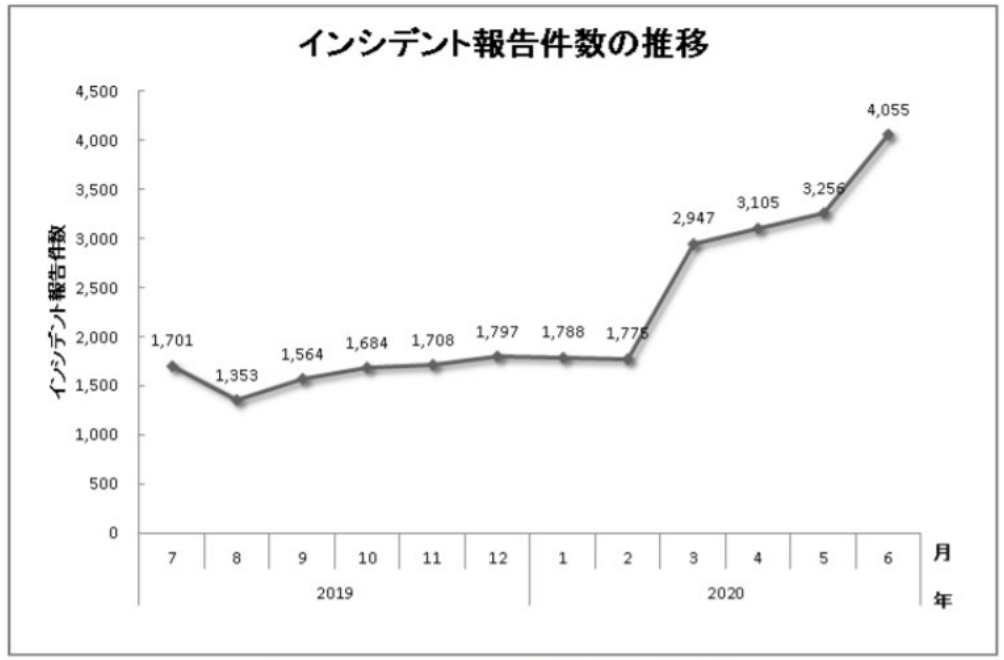
DX時代には、リモートワークを実現するためのVPNツールに限らず、様々なITインフラ/ツールが必要です。

	課　題	ITインフラ/ツール
1	社内環境へアクセスが必要なインフラ	リモートアクセス
2	セキュリティ確保	エンドポイント保護、標的型攻撃対策、ID管理
3	従業員の業務管理	業務の見える化/SDx化*
4	業務遂行に必要なアプリケーション	SaaS（捺印処理/請求書処理/経費処理/書類の電子化）
5	社内/外とのコミュニケーションツール	SaaS（テレビ会議/コミュニケーションツール）
6	高度なコラボレーションツール	SaaS、グローバルNW（共同ファイル編集/海外拠点）

*SDx（Software-Defined anything）…物理的なITインフラをソフトウェアでコントロール。SDN、SDI等

高まるセキュリティリスク

一般社団法人JPCERTコーディネーションセンターが公表したインシデント報告対応レポートによると、
2020年4月から6月の報告件数は10,416件で、前四半期の6,510件から約60%増加したと報じられています。



［図 1：インシデント報告件数の推移］

左の図は、過去 1 年間の月別のインシデント報告件数推移を表したものです。

増加理由のすべてが新型コロナウイルスに関連するとは言えませんが、様々な企業がテレワークを導入した3月～6月に被る期間で増加傾向が見られており、実際に新型コロナウイルスの混乱を狙った事案も発生しています。

参考　https://www.jpcert.or.jp/pr/2020/IR_Report20200714.pdf

COVID-19、働き方改革により急増するサイバー攻撃
テレワークは格好の的

COVID-19で外出自粛が求められるなか、オフィスに出社せず自宅から業務を進めるテレワークが急速に広がりました。しかし、セキュリティが十分でないままテレワーク導入に踏み切る企業も目立ち、サイバー攻撃の標的となる危険にさらされています。

警視庁は、テレワークの防犯対策をホームページに掲載し、警戒を呼び掛けています。

警視庁ホームページ　https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

政府も注目するゼロトラストの考え方

従来のVPNなどに代表される境界型防御では、クラウド時代のセキュリティとしては不十分！

2020年3月、政府CIOポータルは、境界型セキュリティの限界、ゼロトラストと呼ばれるこれからのセキュリティの考え方を紹介し、政府情報システムにおけるゼロトラスト適用の取り組みについて「政府情報システムにおけるゼロトラスト適用に向けた考え方」と題したディスカッションペーパーを公表しました。

パブリック・クラウドの利用、働き方改革、APIによる官民連携等が政策上の大きなテーマとなっていますが、これまでの境界型セキュリティの考え方だけではその実現が困難として、これらを推進するために、このディスカッションペーパーを公表し意見を募集しています。

政府 CIO 補佐官等ディスカッションペーパー
https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf

政府CIOポータル　https://cio.go.jp/dp2020_03

ゼロトラストとは

ゼロトラストネットワークとは、ファイアウォールやVPNに代表される従来型のセキュリティ(境界防御モデル)が通用しなくなった現状を踏まえ、すべてのトラフィックを信頼しないことを前提とし、検証することで脅威を防ぐというアプローチです。
近年、クラウドサービスやモバイルの普及により、セキュリティで守るべき内外の境界があいまいになってきたことにより、強く注目を集めています。

出典：ゼロトラストネットワーク ―境界防御の限界を超えるためのセキュアなシステム設計
著者：Evan Gilman, Doug Barth／翻訳：鈴木研吾

ゼロトラストの五大原則

1. ネットワークは常に敵意にさらされているとみなす
2. 外部と内部の脅威が常に存在する
3. ローカルネットワークであることは、ネットワークを信頼するための条件として十分ではない
4. すべてのデバイス、ユーザー、ネットフローが認証および承認されていること
5. ポリシーは動的で、多くのデータソースから決定されていること

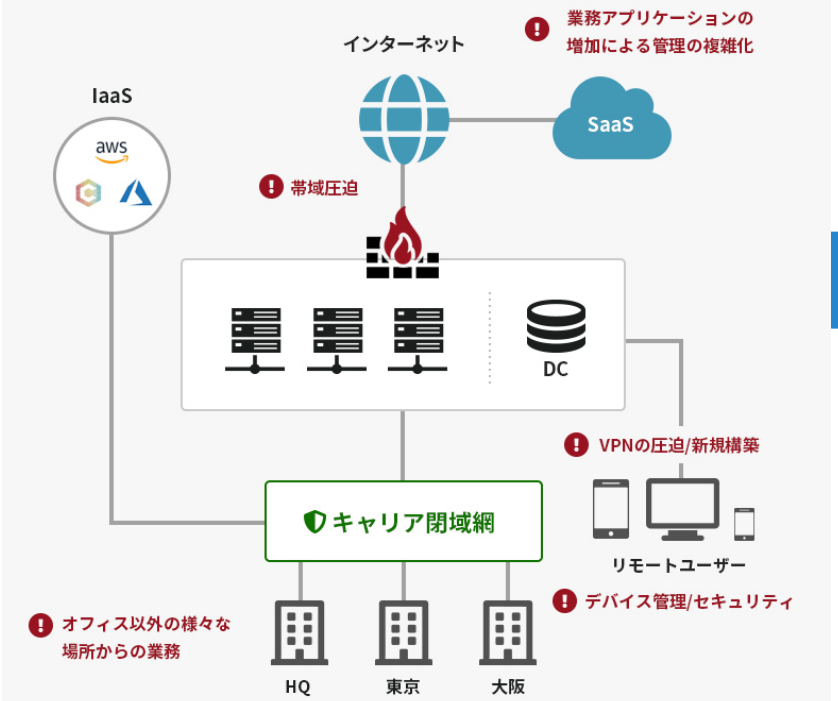
従来のVPNなどに代表される境界型防御では、クラウド時代のセキュリティとしては不十分です

**WSIソリューションで、
ゼロトラストベースのセキュアなネットワークを実現しましょう。**

Clara WSI Solutionとは

クララオンラインが提唱する、ゼロトラストベースの新しい情報システムの形

オフィス to データセンタ時代の 従来型のインフラの形



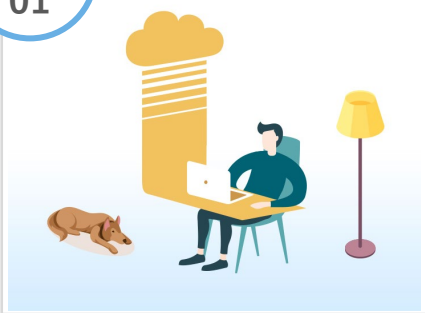
デバイス to クラウド時代の ゼロトラストベースのソリューション

Clara WSI Solution

導入までの3Step

【STEP 01】のリモートアクセス環境の整備から【STEP 02】のID認証の充実、クラウド活用・可視化、そして【STEP 03】のクラウドベースのGatewayとエンドポイントのセキュリティ強化までを、ゼロトラストネットワーク導入プランとしてご提案します。

STEP 01

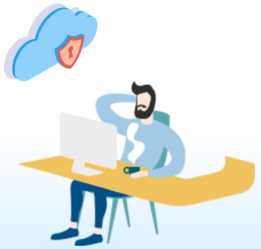


リモートワーク環境整備

Zero-Trust Access

どこからでも社内NWへ接続

STEP 02



クラウドの活用

Cloud Secure Gateway - CASB
IDentity Management

クラウドの利便性と
セキュリティ確保を両立

STEP 03

内部脅威と外部脅威

Cloud Secure Gateway
Endpoint Protection Platform

クラウド時代の
ゼロトラストセキュリティへ

お客様に合わせてカスタマイズ

上記プランは導入ステップイメージです。
お客様の既存環境に合わせて一部のみ導入など、プランはカスタマイズが可能です。

Clara WSI Solution

提供機能一覧

Clara WSI Solutionは4つのベンダーの5つのコンポーネントで構成されたワンパッケージソリューションです。

01

Zero-Trust Access

– ゼロ-トラストアクセス –

VPNアプライアンスに依存しない、次世代型クラウドベースのリモートアクセスです。

netskope　CLOUDFLARE

02

IDentity Management

– アイデンティティマネジメント –

シングルサインオン、多要素認証、IDライフサイクル管理機能を有し、企業のID管理などの認証基盤です。

okta

03

Cloud Secure Gateway - CASB

– クラウドセキュアゲートウェイ-キャスビー –

SaaS利用が当たり前になってきた今、クラウドサービスを安全に利用するため、利用状況の可視化を可能にします。

netskope

04

Cloud Secure Gateway

– クラウドセキュアゲートウェイ –

プロキシ・DNS/URLフィルタリングといったベーシックな機能に加え、CASBやDLPといった最新のセキュリティ機能をクラウドベースで提供します。

netskope

05

Endpoint Protection Platform

– エンドポイント プロテクション プラットフォーム –

EPP+EDDにより、検知・対応・修復までの一連の流れがほぼ自動化された、エンドポイント保護のセキュリティです。

SentinelOne

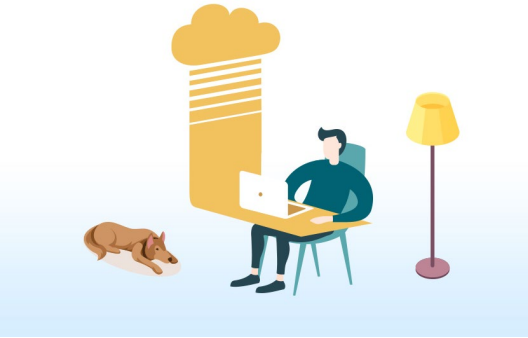
Clara WSI Solution 全体像

クラウド活用とどこからでも働ける環境を目的とした、クララオンラインが提唱する次世代の情報システムの形です。

STEP 01 | リモートワーク環境整備

CASE 1

クラウドベースでリモートワーク環境整備



まずは、リモートアクセス環境を整えたい！

- 社外からセキュアに社内ネットワークへアクセスさせたい
- 社員の増減に柔軟に対応したい
- 一日も早くリモートワーク環境の構築がしたい

Zero-Trust Access

netskope　CLOUDFLARE

・従来のVPN接続のボトルネック課題を解消します。
・データセンタと接続場所の距離による遅延を解消します。
・クラウドベースのため、ハードウェアの設備投資・管理コストを削減します。

サービス名	ソリューション	Step01	Step02	Step03
Zero-Trust Access Netskope / Cloudflare	リモートアクセス	○	○	○
IDentity Management Okta	Identitiy 認証・管理	-	○	○
Cloud Secure Gateway - CASB Netskope	クラウドサービスの可視化：CASB	-	○	○
Cloud Secure Gateway Netskope	クラウドベースのGateway	-	-	○
Endpoint Protection Platform SentinelOne	エンドポイント端末の保護	-	-	○

STEP 01 | リモートワーク環境整備

Zero-Trust Access

－ゼロ-トラストアクセス－

Zero-Trust Accessは、VPNアプライアンスに依存しない、次世代型クラウドベースのリモートアクセスです。
従来型のハードウェアベースのリモートアクセスで課題となっていた、納期・サイジング・設計・構築から解放され、
また、DCとの距離による遅延やハードウェアのボトルネック課題を解決し、パフォーマンスを向上します。

特徴

1. ハードウェアアプライアンスによる設計/構築/運用の手間から解放
2. データセンタのバックホール問題による遅延やセッション数問題の解消
3. 短納期での構築、利用人数増減に迅速な対応が可能
4. クラウド活用時代のリモートアクセス

Cloud Secure Gatewayへの拡張をお考えの方向け

Zero-Trust Access type-N

netskope

- 多様なセキュリティGateway機能との連携
- 今後のゼロトラスト環境への移行を見据えた1st Step

中国でのリモートアクセスをご利用される方向け

Zero-Trust Access type-C

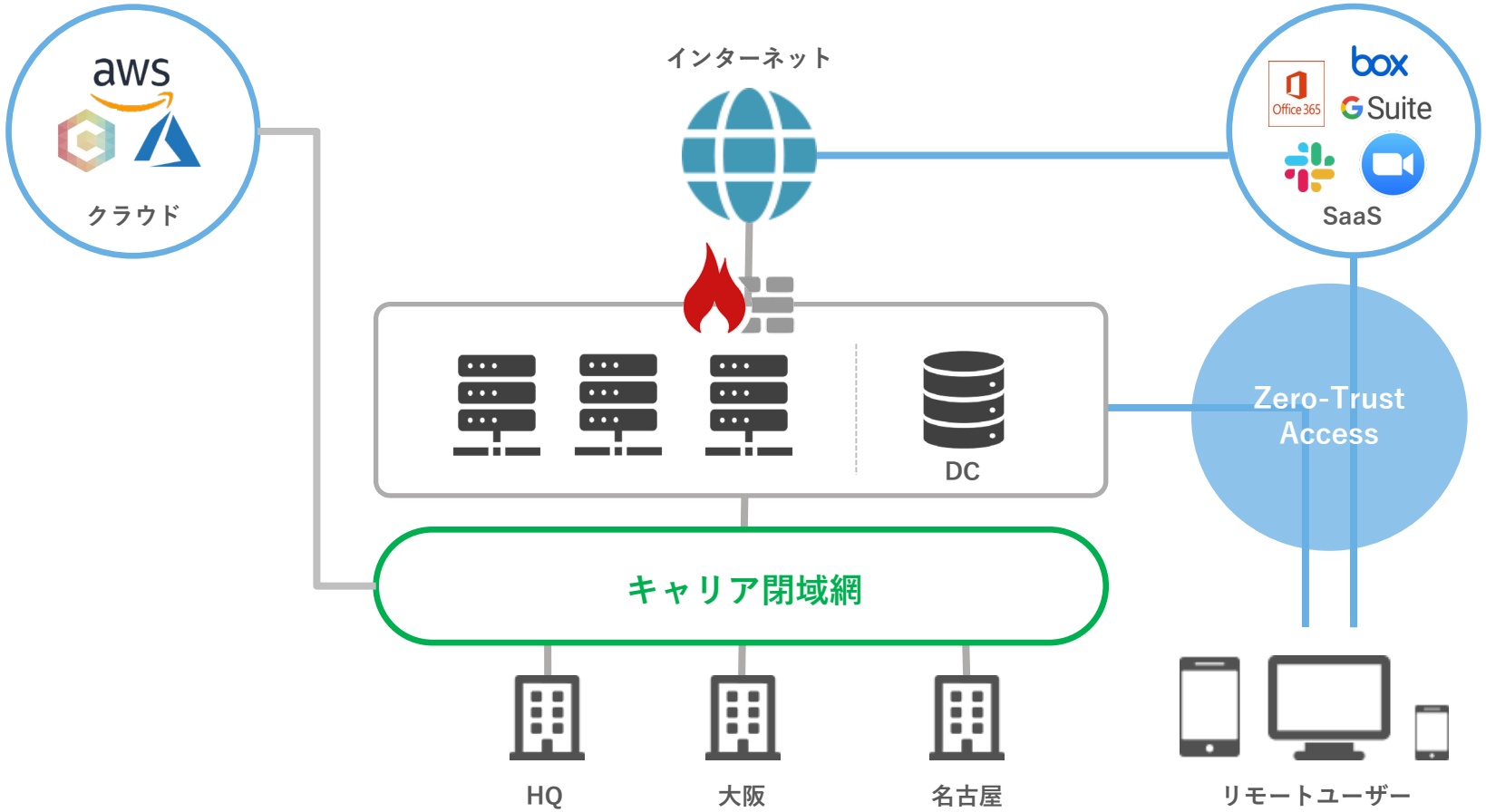
CLOUDFLARE

- CDN/DDoS/WAFも同一プラットフォームで提供し、一元的に管理が可能
- 世界トップクラスのバックボーンに加え、エニキャスト方式による高速アクセス

STEP 01 | リモートワーク環境整備

CASE 1

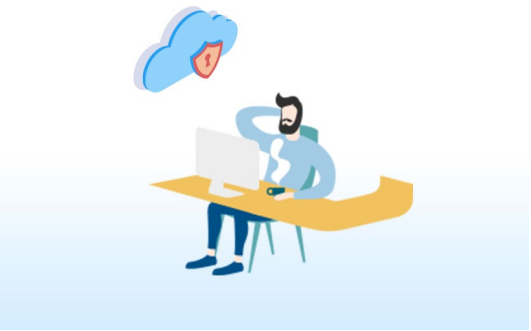
構成イメージ図



STEP 02 | クラウドの活用

CASE 2

クラウド活用とセキュリティ確保の両立



クラウドサービスを積極的に活用したいのですが、セキュリティが心配…

- アプリケーションごとのパスワード管理が煩雑で運用負担が大きい
- ID/Passのみのクラウドサービスへの認証によりセキュリティが万全ではない
- 従業員が個人で利用するクラウドサービスからの情報漏洩が不安

IDentity Management okta

Cloud Secure Gateway - CASB netskope

・SSOによりアプリケーションの利便性確保とID/PWの一元管理をします。
・SaaS/IaaS/Webアプリの利用状況を可視化し、ガバナンスを強化します。
・多要素および動的な認証により、クラウドサービスへの認証をよりセキュアにします。

サービス名	ソリューション	Step01	Step02	Step03
Zero-Trust Access Netskope / Cloudflare	リモートアクセス	○	○	○
IDentity Management Okta	Identitiy 認証・管理	-	○	○
Cloud Secure Gateway - CASB Netskope	クラウドサービスの可視化：CASB	-	○	○
Cloud Secure Gateway Netskope	クラウドベースのGateway	-	-	○
Endpoint Protection Platform SentinelOne	エンドポイント端末の保護	-	-	○

STEP 02 | クラウドの活用

IDentity Management

－アイデンティティ マネジメント－

シングルサインオン、多要素認証、IDライフサイクル管理機能を有し、企業のID管理などの認証基盤をクラウド上から提供するサービスです。ニューノーマルな働き方に注目が集まり、各種クラウドサービスの活用が求められる中、最適なID管理と便利でセキュアなアクセス制御を可能にするプラットフォームを提供します。

okta

機能

01. シングルサインオン(SSO)

シングルサインオン（SSO）は、認証に使うデジタルIDを一組だけ管理し、一度の認証で複数のシステムに安全にログインすることができる機能です。

02. 多要素認証(MFA)

MFA(多要素認証)とは、ユーザーの ID を複数の信用情報を要求することにより検証するセキュリティシステム です。

03. ライフサイクル管理(LCM)

従業員の入退社や人事異動に応じて、ユーザー情報を多数のクラウドサービスやアプリケーションに自動で反映させます。

04. Provisioning 機能

プロビジョニング機能は、登録されたユーザー情報を参照し、指定のSaaSやアプリケーションへのユーザー追加・変更・削除の自動対応を可能にします。

05. ふるまい検知とブロック

ユーザーにスムーズなアクセス機能を提供するだけでなく、不審なIPからの認証リクエストを、認証プロセスが走る前に検出することが可能です。

06. ユニバーサルディレクトリ

無制限のユーザーディレクトリとして利用することができます。Active Directoryや人事システムのユーザー情報と同期をするだけでなく、パスワードポリシー管理も認証基盤で一元管理することが可能になります。

STEP 02 | クラウドの活用

Cloud Secure Gateway-CASB

― クラウド セキュア ゲートウェイ - キャスビー ―

CASB(Cloud Access Secure Broker)は、Office365やGsuiteをはじめとしたSaaSサービスの活用が広がり、ビジネスにおいてSaaS利用が当たり前 になってきた今、クラウドサービスを安全に利用するため、利用状況の可視化を可能にします。

netskope

機 能

01. 可視化・分析

自社で利用されているすべてのクラウドサービス（SaaS）とIaaSを検出・可視化し、リスク評価を数値で提示。SaaS/IaaS/Webサービスでのアップロードやダウンロードといったユーザーのアクティビティを詳細に可視化します。

02. コントロール

詳細に解析された通信のコンテキスト情報（ロケーションやアクティビティ）に基づき、通信のブロック、アラート通知などの制御を実行します。1つのセキュリティポリシーで、SaaS/IaaS/Webサービスのコントロールが可能。

03. データ保護

企業の機密情報を定義することで、キーワードや多数の識別方法で、精度の高いDLP（情報漏えい対策）を実施。
※一部プランでは対象外です。

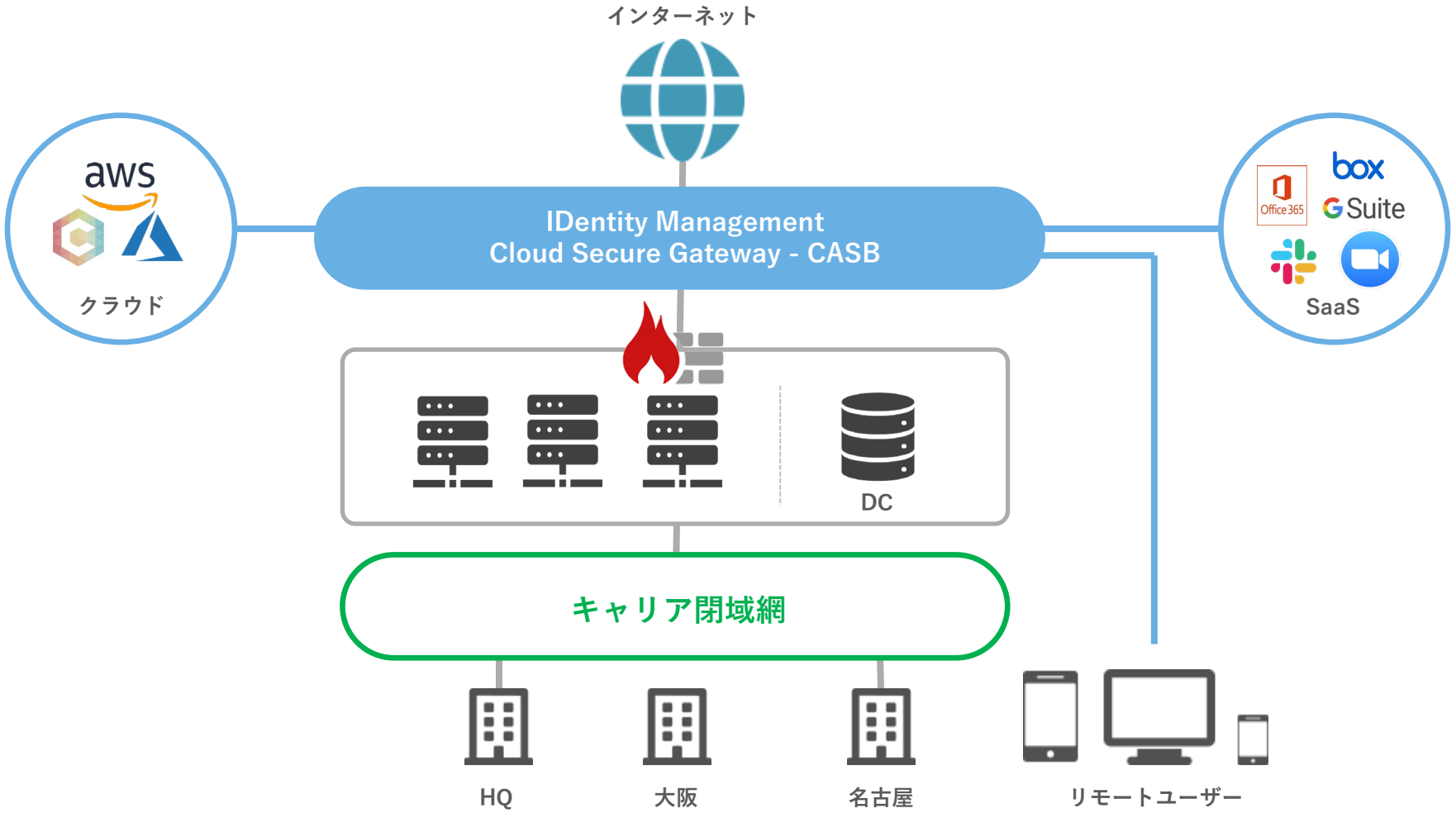
04. 脅威防御

クラウドサービスに潜んでいるマルウェアやランサムウェアを検知し、隔離。また、共有アカウントの利用、データのコピー、大量データのダウンロードといった異常値を検出します。

STEP 02 | クラウドの活用

CASE 2

構成イメージ図



STEP 03 | 内部脅威と外部脅威

CASE 3

クラウド時代のゼロトラストセキュリティ

セキュリティはいまや経営リスク！
しかし、どこまでやればいいのかわからない。

- 外部からの攻撃に対する防御が必要になってきた
- 内部不正による情報流出への対応が出来ていない
- 新しい攻撃・未知の脅威に対する対策が不十分

Cloud Secure Gateway — netskope

Endpoint Protection Platform — SentinelOne

・セキュリティの欠かせないエンドポイント端末の保護を強化します。
・社内から持ち出されるデータ保護のために、DLP(情報漏えい対策)を適用します。
・クラウドベースのGatewayにより、全てのアクセスへ統一のポリシーを
適用可能です。

サービス名	ソリューション	Step01	Step02	Step03
Zero-Trust Access Netskope / Cloudflare	リモートアクセス	○	○	○
IDentity Management Okta	Identitiy 認証・管理	-	○	○
Cloud Secure Gateway - CASB Netskope	クラウドサービスの可視化：CASB	-	○	○
Cloud Secure Gateway Netskope	クラウドベースのGateway	-	-	○
Endpoint Protection Platform SentinelOne	エンドポイント端末の保護	-	-	○

STEP 03 | 内部脅威と外部脅威

Cloud Secure Gateway

－クラウド セキュア ゲートウェイ－

プロキシ・DNS/URLフィルタリングといったベーシックな機能に加え、CASBやDLPといった最新のセキュリティ機能をクラウドベースで提供します。クラウドベースのセキュリティのため、ハードウェアの管理や運用から解放され、世界中に統一のセキュリティポリシーの提供を可能します。

netskope

特徴

01. クラウドベースのため世界中どこからでも、全てに統一のポリシーを適用
02. ハードウェアを保有しないため、拡張性に優れ、ボトルネックに悩まない
03. データセンタを経由することにより発生していたレイテンシー課題を解決
04. 他セキュリティ製品と連携することにより、総合的なセキュリティを実現
05. SSLの完全な可視性を実現し、よりセキュアな環境を提供
06. Webセキュリティにとどまらない機能を備えた次世代セキュリティ

STEP 03 | 内部脅威と外部脅威

Endpoint Protection Platform

－エンドポイント プロテクション プラットフォーム－

EPP + EDRを含んだエンドポイントセキュリティ製品です。高セキュリティではあるが、通常運用が手間であるEDR機能を含んでいるにも関わらず、 検知・対応・修復までの一連の流れがほぼ自動化されており、運用の工数を大幅削減できることが特徴です。

SentinelOne

特徴

01 ブラックリストだけでは止められない未知の攻撃をふるまいで判別

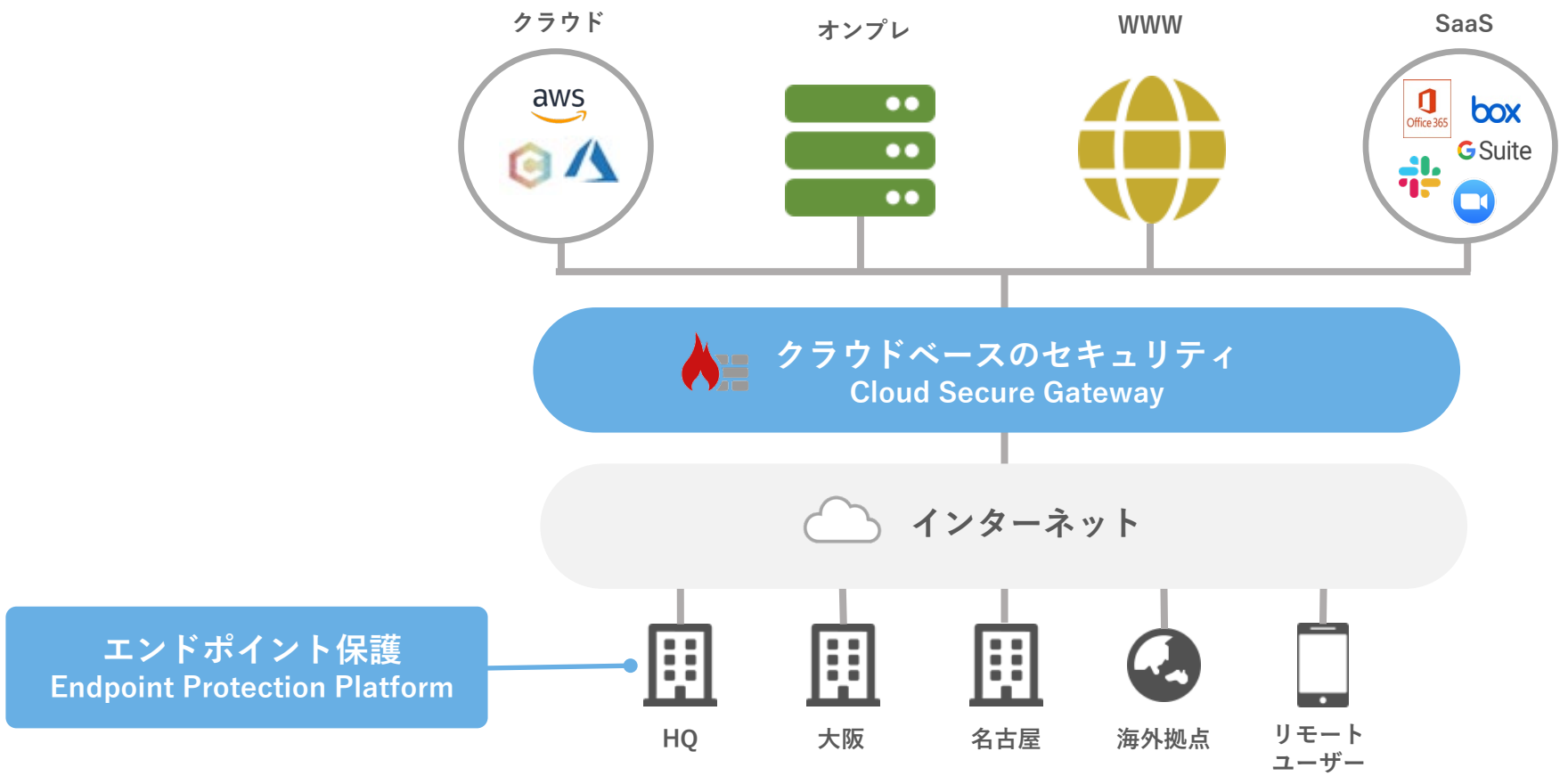
02 自律型エンドポイントセキュリティで感染後もワンクリックで修復可能

03 運用に必要な機能が標準装備
- VSSを利用したロールバック(感染前の状態に修復)
- ロケーション制御を含むファイアウォール補完機能
- USBやBluetoothの制御
- インストールされているソフトウェアの把握と脆弱性診断

04 機械学習に運用工数・コスト削減を実現

STEP 03 | 内部脅威と外部脅威

CASE 3 構成イメージ図



ニューノーマル時代のインフラへのロードマップ

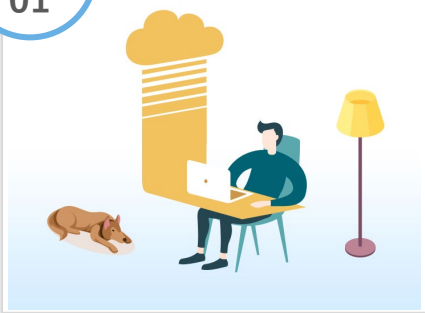
改革原資の捻出 1

クラウドコストの最適化

CloudHealth by vmware

https://www.clara.jp/solution/cloud-opt/

STEP 01



リモートワーク環境整備

Zero-Trust Access

どこからでも社内NWへ接続

STEP 02

クラウドの活用

Cloud Secure Gateway - CASB
IDentity Management

クラウド活用と
セキュリティ強化

STEP 03

内部脅威と外部脅威

Cloud Secure Gateway
Endpoint Protection Platform

ゼロトラスト化によるクラウド
時代のITプラットフォームへ

改革原資の捻出 2

既存システム・ライセンスの見直し

Clara WSI Solution

Clara WSI Solutionの設計・導入・運用支援

クララがワークスタイル変革をお手伝いします！

ゼロトラストネットワークの実現に向け、導入のお手伝いをいたします。
お客様の現状のヒアリング、システム構成のご提案、導入支援、運用までトータルサポートさせていただきます。

ヒアリング	設計・提案	導入支援	運用支援
・現状のヒアリング ・要件確認	・システム構成のご提案 ・サービス選定 ・ロードマップ策定	・PoC ・操作方法のレクチャ ・ライセンス提供	・定例会（定期的な見直し支援） ・問い合わせサポート

30日間の無料トライアルアカウント発行も可能！

働き方改革無料コンサルティングも随時受付中です。
お気軽にご相談・お問い合わせください。

お問い合わせはこちらから▶ https://www.clara.jp/wsi/#wsi__contact

社会のボーダーを解決する

CLARA ONLINE

インターネット黎明期である1997年に創業。
ホスティング事業を皮切りに、クラウドインテグレーション、スポーツ領域でのITソリューションサービス提供のほか、
アジア・日本双方でのIT・コンサルティングサービス提供を行っています。
近年ではIoTを活用したモビリティ事業への進出などその領域を広げています。

専門性

ITインフラのプロフェッショナル

20年以上に渡る
ITインフラサービスの提供実績

先進性

次の時代を道づくる

Clara CloudやWSIソリューションを
はじめとした革新的なサービス

提案力

期待値を超える

単なるモノ売りではなく、お客様の
目的から最善の手段をご提案

会社概要

企業理念

- Clara Philosophy -

次の時代を道づくる

社　名	株式会社クララオンライン CLARA ONLINE, Inc.
設　立	1998年5月22日
資本金	1億円
代表者	代表取締役社長　家本 賢太郎
所在地	東京(神谷町・三田)・名古屋

事業分野	• インターネットサービス基盤事業 • ビジネスコンサルティング事業 • 有料職業紹介事業（許可番号：13-ユ-306859）
従業員数	単体:51名、連結:167名（2020年4月30日現在）
関連会社	客乐来技术咨询(北京)有限公司（クララオンライン中国） 株式会社スポーツITソリューション セイノーアジアトレーディング株式会社 自転車投資合同会社 株式会社ちゃりカンパニー neuet株式会社 wimo株式会社

ご相談・お問合せ・お申込み

株式会社クララオンライン
クロスボーダービジネス部

メール sales@clara.ad.jp

お電話 0120-380-966
受付平日 10:00 - 18:00

CLARA ONLINE
https://www.clara.jp/wsi/