

クラウド導入時にチェックするべき点とは



アジェンダ

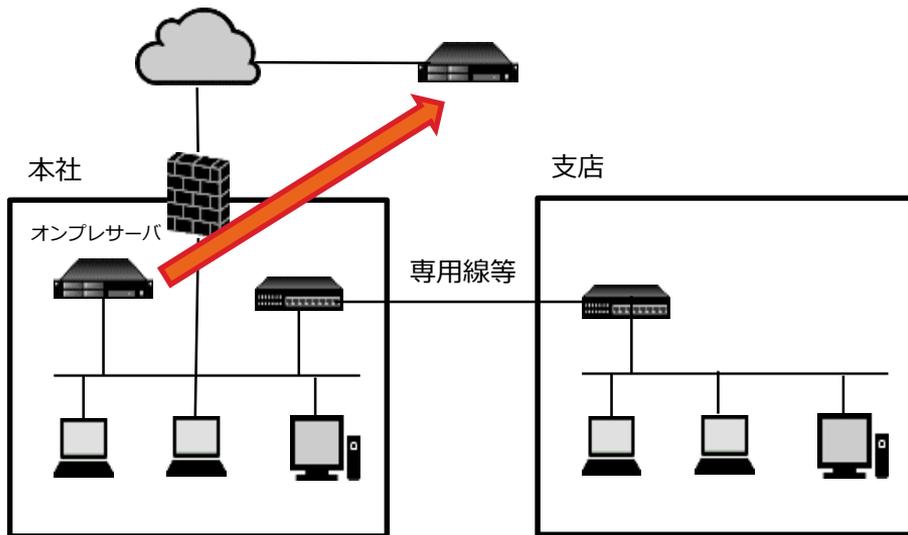
1. クラウドにおけるセキュリティ運用の変化
2. 運用の問題点
3. ID-Cross(アイディクロス)ご紹介
4. まとめ

オンプレサーバをクラウドに移行

クラウド運用は社内のサーバをクラウドに移行するところからスタートします。従来はホスティングやハウジングのようにデータセンターにサーバを預けていましたが、徐々にパブリッククラウドやプライベートクラウドにサーバを移行することが一般的になってきました。

このころセキュリティについては社内からしかアクセスすることが出来なかった為あまり考える必要はありませんでした。ポイントは費用や運用の工数の削減、拡張性の向上等がテーマでした。

最初はこれでよかったのですが、徐々にセキュリティを含め、運用が変わってきました。



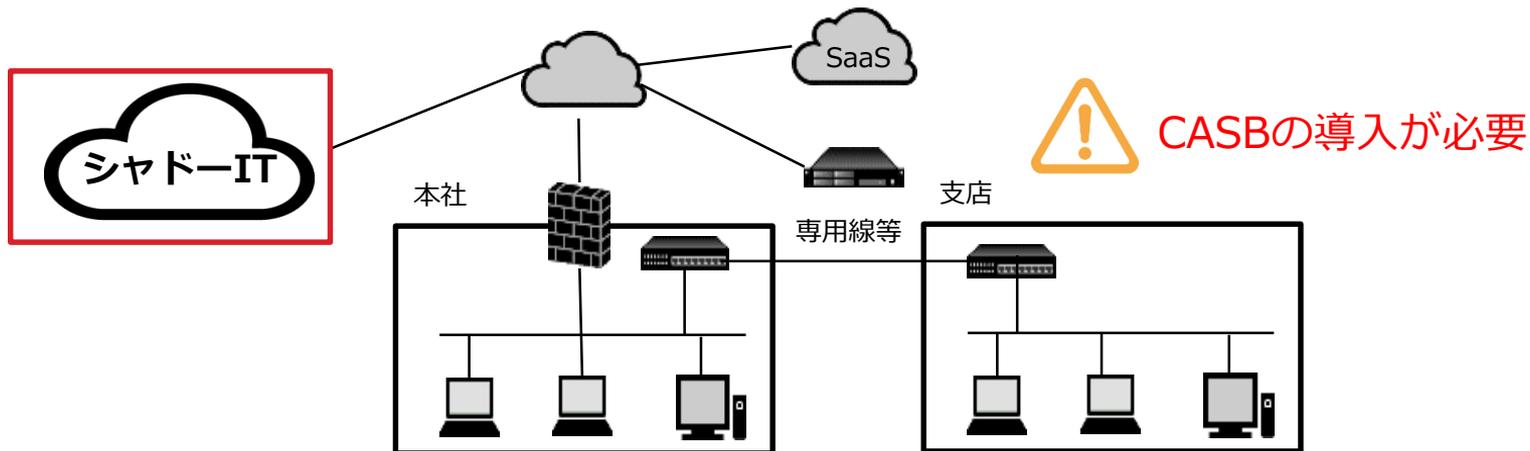
SaaS利用の増加

今ではグループウェア、会計ソフト、グループチャットなどSaaSを利用するのが一般的になっており、URLフィルタで一律にブロックするのが難しくなっています。更にHTTPS化が進み、ゲートウェイではどのような通信を行ったか判別することが難しくなっています。そして、このような環境に慣れてくると、シャドーITが問題になります。シャドーITと呼ばれるものはSNS、ストレージ、Webメール等でファイルも送付出来てしまいます。また、SaaSサービスは送信元IPでブロックできるものとできないものがあり、自宅からでもアクセスできてしまいます。

このような問題からCASB(Cloud Access Security Broker)の必要性が求められてきました。

CASBとはクラウドサービスの利用状況を可視化/制御するアプリです。

CASBに限らずですが、導入したら終わりというツールはほとんどありません。日々監視やレポート作成の運用が必要です。



リモート業務の増加

急に緊急事態宣言が出たため、VPNが足りなくて遅い、持ち出しPCが足りないと慌てて調達をされた会社もあると思います。また、クラウドサービスやWEBミーティングサービス等回線に負荷のかかる業務が増え、回線のひっ迫が顕著になり増強も視野に入れる必要が出てきました。

VPNは攻撃されたら危険なので使わないほうがいいと言われ始め、そうするとモバイルPCから直接インターネット越しにクラウドに接続するインターネットブレイクアウトが効率的ですが危険も伴います。

そこで出てきたのが**ゼロトラストセキュリティ**です。ゼロトラストセキュリティとは、社内外問わず全ての通信を信用しないという事であり、ユーザー管理とアクセス権の設定を厳格にし、更に監視を強化します。セキュリティ的には正しいのですが、運用が大変になります。**SASE**(サシー) (Secure Access Service Edge) はネットワークとセキュリティの機能を包括的にクラウドから提供するモデルとなり、現在サービスが少しずつ出始めてきています。**SASEではゼロトラストやEDRといったセキュリティを包括的に管理できるので効率よく監視が出来ますが、その分運用の高度化が必要になります。結果として、運用負荷がかかるという点が問題になっています。**



VPN増強、SASE、ゼロトラストセキュリティの導入などが必要

運用内容の増加

CASB、SD-WAN、SASE、EDR等様々な製品で、監視業務が増えています。
最初はベンダーが設定することが多いと思いますが、スコープをはっきりとしておかないと運用設計がきちんと行われな
いケースが多くなります。ただ、ユーザー側としては使ったことが無い製品の運用でリクエストを出すことは難しい
です。結果、アラートが飛んで来ても分からないので、まずはアラートの内容を調べて対応するという後手後手の
運用になりがちです。



運用内容例

マルチクラウド化により、管理不能 セキュリティポリシーの統一ができない

セキュリティツールが増えるほど設定は複雑になります。
また、セキュリティポリシーを統一することが望ましいのですが、
マルチクラウドになるとそもそも設定できないポリシーなども増えてきます。

セキュリティで重要なことはツールの導入ではありません。
いかに監視を行うか、インシデントの際に対応を行えるかという事が重要です。

皆さん消火器を設置してると思いますが、火事が起きたら買いに行くから消火器はいらないって方はいらっしゃいませんよね。
よって、セキュリティの導入は重要なのですが、問題はその先です。消火器を置いても火災報知器が無いと火事に気付かない可能性がある。さらに、火事が起きてても消火器を使ったことが無いと使い方が分からず火が消せないということはあってはなりません。

つまり、**監視とインシデント対応**というのは**非常に重要**なのです。



クラウドの設計において 運用やセキュリティの設計は後回しにされがち

設計はクラウドの設計時にベンダーに任せることも多いと思いますが、既存の運用やセキュリティ設計を十分理解したうえで構築を行わないと大変でことになります。

まず既存の運用に乗らないケースがあります。セキュリティもポリシーに沿った設計が必要ですが、運用にもポリシーがあります。ポリシーは、制定した背景を大事にして設計しなければ無駄が発生します。

別途ツールが必要になったり、余計な工数が発生したりと、コストが発生する場合があります。

設計時こそ専門家が必要です。

クラウドの運用は重要度も難易度も以前とは比べ物にならないほど重要になっています。

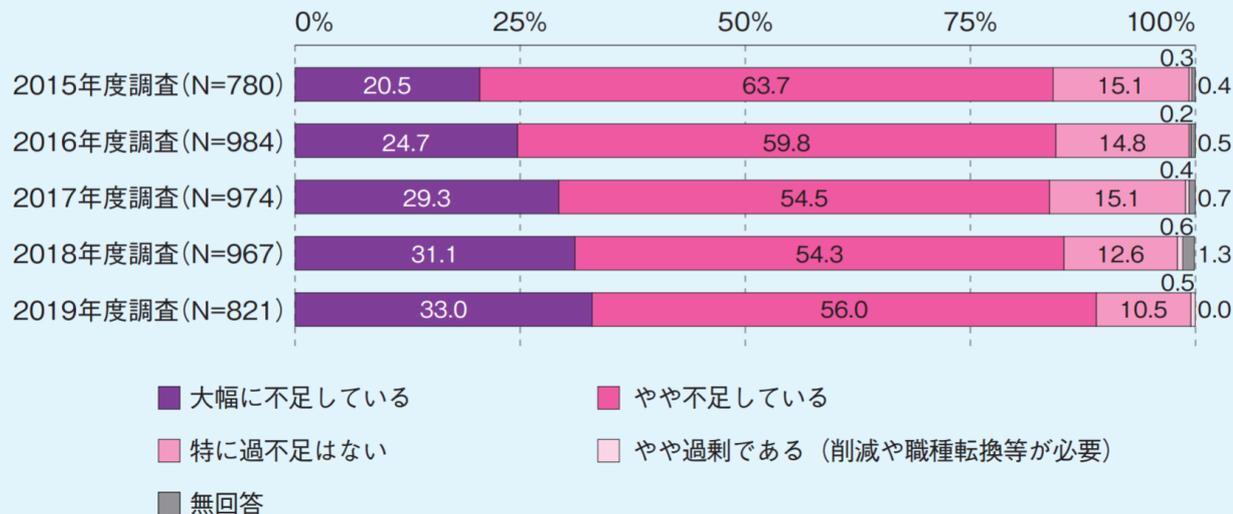


要員の不足

IT人材の不足は89%の企業が『不足』と回答しています。

クラウド環境については年率15%以上の伸びを示している一方、『クラウド要員』『セキュリティ要員』の不足は更に深刻になっています。

図表2-1-1 ユーザー企業のIT人材の“量”に対する過不足感【過去5年間の変化】



今後クラウドの要員、特にマルチクラウドに対応できるようなプロフェッショナルは流動性がますます高くなりますので、欠員の補充は難しくなります。

では、どうすればよいのでしょうか？

ID-Cross(アイディクロス)ご紹介

「ID-Cross」は
2つのサービスで構成されています

About

クラウドシステムの導入・移行

システムのリモート運用

マルチクラウド導入サービス

マルチクラウドマネージドサービス

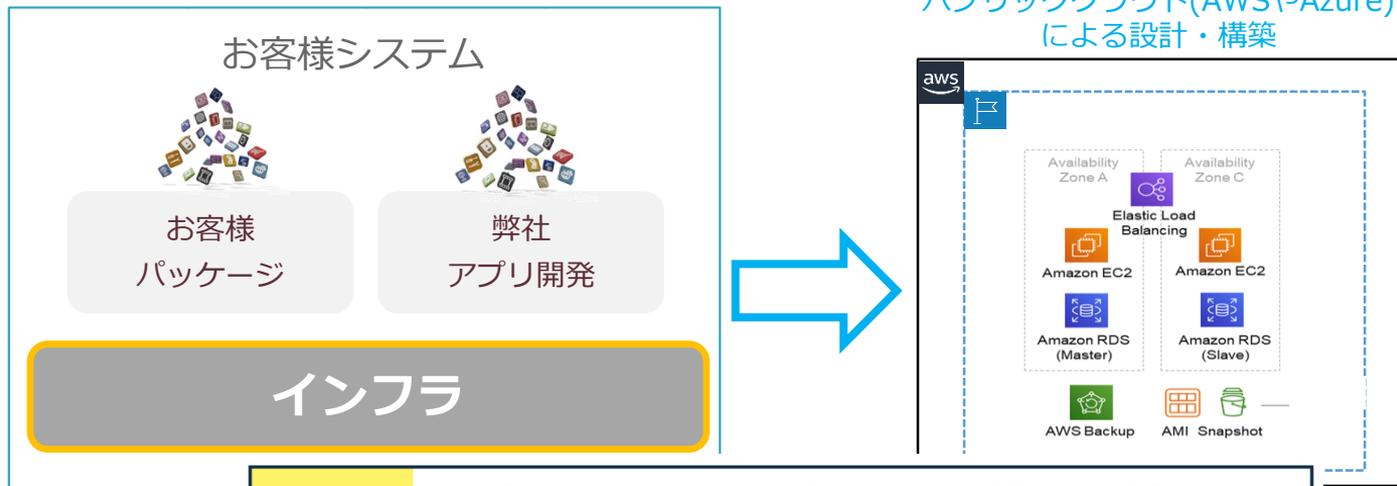


ご提案から設計・構築・移行、運用まで一貫した体制で課題解決を支援

ID-Cross(アイディクロス)ご紹介

スピーディーな設計・構築・移行サービス

お客様の要件に沿ったシステムをパブリッククラウド上に設計・構築します。



POINT

- ◎50年のシステム運用で積重ねてきた、要件定義の知見を活用
- ◎多業種におけるクラウド化の課題・ノウハウをお客様と共有

ID-Cross(アイディクロス)ご紹介

弊社は20年以上にわたって培ってきたセキュリティの知見があります。
こちらはサービスのごく一部ですが、セキュリティスペシャリストによるコンサルと、独立系であるが故のメーカーやベンダーにとらわれることのない最適なソリューションの提案が行えます。

アクセスポリシー設定

ネットワーク上のファイアウォール設定やリソースへのアクセスポリシーを要件に応じて適切に設定

PaaSセキュリティ設定

AWS、Azure付属のセキュリティサービス構築・設定

エンドポイント セキュリティ構築

アンチウィルス、EDR等のクラウドインスタンス導入

ネットワーク振る舞い検知 ソリューション構築

ネットワークトラフィックAI分析ソリューションツール導入

統合ログ監視環境構築

統合的なログ監視環境構築

CASB構築

クラウドサービスごとの利用状況の可視化、アクセス制御などを行うCASB(Cloud Access Security Broker)構築

POINT

- ◎セキュリティスペシャリストによる丁寧なコンサル
- ◎独立系企業の特徴を活かした柔軟な提案

ID-Cross(アイディクロス)ご紹介

ID-Crossが選ばれる4つのポイント！

01



スピーディーな設計・
構築・移行サービス

要件定義シートと設計テンプレートを活用した、クラウド環境の構築。導入期間を短縮し、コストダウン、品質向上を実現します。

02



専門部門による
高度なセキュリティ

課題・要望に合わせた包括的なセキュリティ環境の構築を行います。

03



月利用料の
固定化を実現

クラウド運用・保守費用にクラウド利用料を含め月額固定化を実現しました。

04



充実の
運用サポート

クラウドサービスの管理者アカウント含め管理。フルマネージドサービスとしてご提供いたします。

ID-Cross(アイディクロス)ご紹介

	サービス	内容	条件	価格 (月額/1ノード)
基本 パ ッ ク	監視運用 ・ 9:00~17:00 ・ 24h365	死活監視、リソース監視（CPU・メモリ・ディスク）、プロセス監視、アラート監視を実施。メール、電話にてご連絡。監視項目、監視対象はカスタムが可能。	基本パックは1ノードで監視対象は10個までを上限。10個以上の監視は別途費用が発生。	<9:00~17:00> (土日祝日を除く) ¥13,000~
	障害対応	予めお客様から引き継いだ障害対応手順書をもとに障害対応を実施。	監視アラート発報を契機とし障害対応を実施。 1手順は30分以内として3手順まで。	<24h365> ¥45,000~

ID-Cross(アイディクロス)ご紹介

	サービス	内容	条件	価格 (月額/1ノード)
オ プ シ ヨ ン	リソース 分析	リソース状況確認と運用レポートを作成し提供。 必要に応じてリソース拡張等をご提案。 ＜レポート内容＞ ・システム運用状況 ・障害、アラート発生状況 ・定期、保守作業結果 ・翌月作業スケジュール ・メモリ、HDD容量、ストレージ容量等のパフォーマンス	メモリ、HDD容量、ストレージ容量等のパフォーマンス分析。 システムの運用状況や障害発生状況が把握できる運用レポートを作成し、月1回報告。	¥6,000～
	個別対応	定例作業、非定例作業対応。	作業手順書に従って実施。 1作業は30分以内とし、1手順まで。	¥4,000～ (30分毎)

手順書作成サポートや定例・非定例作業の代行など、
弊社50年の運用実績を活かした質の高い運用サービスをご提供いたします。

お客様の声

ラジオ局のお客様

- ✓ 他社と比較して圧倒的に「手軽に」「早く」を実現
- ✓ 導入から監視運用までプラットフォームを問わない**ワンストップ**提供
- ✓ 既存ベンダーとの協業による、**オンサイト+リモート運用の複合提案**

Point こちらのお客様はサービスインまで1か月かからず、圧倒的にスピードに対する評価を頂きました。また、導入から運用までワンストップである点、オンサイト、リモート運用の複合提案を評価いただきました。

最近のリクエストの傾向

- ✓ クラウドを導入したいが、**要員がない**
- ✓ **地方**で運用を相談できる会社が無い

Point 今までは、新規にクラウド移行したいがノウハウのある社員がないというお声が多かったのですが、最近は運用の幅が広がり既存の要員では対応できないという声も多くなっています。

まとめ

- ✓ セキュリティの導入には運用設計が重要
- ✓ クラウド運用はID-Crossへのアウトソーシングによる、
人員リスクの回避をお勧めします
- ✓ 運用のリソースを新企画に割り当て攻めの経営を

お気軽にお問い合わせ下さい

ID-Crossの詳細
資料DLはこちら→



マルチクラウド導入サービス × マルチクラウドマネージドサービス

ID-Cross

高度なセキュリティでクラウド化を実現
保守運用も低コスト・月額固定制

- スピーディーな設計・構築・移行サービス
- 専門部隊による高度なセキュリティ
- 月額料金の固定化を実現
- 充実の運用サポート

株式会社インフォメーション・ディベロップメント
担当：三好（みよし） 宝示戸（ほうしど） 涌井（わくい） 小椋（おぐら） 出利葉（いでりは）

✉ id-cross@idnet.co.jp

☎ 03-3262-8708

