METI

経済産業省
デジタルプラットフォーム構築

事業報告書

DX オフィス関連プロジェクト管理業務等の効率化に関する デジタルツールの導入実証・調査事業

経済産業省デジタル・トランスフォーメーション室
株式会社 クラウドネイティブ

経済産業省
Ministry of Economy, Trade and Industry

クラウドネイティブ
CLOUD NATIVE INC.

目次

1. 事業概要

令和 2 年度経済産業省デジタルプラットフォーム構築事業とは、DX オフィス関連プロジェクト管理業務等の効率化に関する、デジタルツールの導入実証・調査を目的として行ったものである。

1 - 1 . 背景

デジタル・ガバメントの実現に向けた取組を推進していくにあたり、行政サービスの利用者と行政機関間のフロント部分だけでなく行政機関内のバックオフィスを含めたプロセスについても、技術の進展に応じて、デジタル技術の活用を進めていくことが重要である。

令和元年 12 月に改定された『デジタル・ガバメント実行計画（令和元年 12 月 20 日閣議決定)』でも、政府の業務におけるデジタル技術の活用やデジタル・ワークスタイルの実現の重要性が示されている。

経済産業省では、平成 30 年度から、経済産業省デジタル・トランスフォーメーション室（以下、「DX オフィス」という。）を設置し、利用者の立場に立った行政手続きのデジタル化および省内業務の効率化の双方を実現するための方策の検討と実施を図っている。併せて、政府全体の動きも踏まえ、経済産業省におけるデジタル・ガバメント推進を戦略的に進めるため、令和 2 年 3 月に「経済産業省デジタル・ガバメント中長期計画」を改定し、当該計画の中で、タスク管理ツールやコミュニケーションツール、BI（ビジネスインテリジェンス）ツール等のデジタルツールについて、情報セキュリティ対策にも配慮しつつ活用し、いっそう効率的に業務を遂行できる環境の整備を目指すこととしている。

この取組を早期に具体化するためには、既存の経済産業省基盤情報システムとは連携しない範囲で、将来的な省内活用を視野においた形で実験的にクラウド関連ツールの徹底活用を試み、その知見を蓄積・共有していくことが必要である。

そこで本事業では、職員の業務効率化やシステム開発等のプロジェクトの標準化・最適化を進めるため、各種ツールの導入の実証を行うとともに、より効果的にこれらのデジタルツールを活用していくために必要となる管理のあり方について検討を行う。

1 - 2 . 目的

この取組を早期に具体化するためには、既存の経済産業省基盤情報システムとは連携しない範囲で、将来的な省内活用を視野においた形で実験的にクラウドサービスの徹底活用を試み、その知見の蓄積・共有が必要である。そこで本事業では、職員の業務効率化やシステム開発等のプロジェクトの標準化・最適化を進めるため、各種ツールの導入の実証を行うとともに、より効果的にこれらのデジタルツールを活用していくために必要となる管理のあり方について検討を行う。

また、本事業のアウトプットについて本実証事業では、経済産業省の DX を推進する部署における業務の現状とシステム環境の検討を前提としている。しかし、本事業は現行の基盤システムを前提とした技術仕様の検討ではないため、本事業の成果は他の行政機関においても参考となる知見であると考える。

1 - 3 . 適用するスコープ

本実証事業では仕様書の通り、既存の経済産業省基盤情報システムとは連携しない範囲で実証を行う。この趣旨は、既存の基盤情報システムを前提に業務環境の改善を検討するのではなく、理想のツール環境側からのアプローチを行うことで、短い事業期間の中でも柔軟かつ具体性のある検討を行うためである。

1 - 4 . 対象とする業務

本実証においてスコープとする業務は、経済産業省の DX を推進する業務、具体的には情報システムの構築、管理、運用等の業務である。これらの業務は、経済産業省職員に留まらず多くのステークホルダーとの円滑なコミュニケーションを必要とすることから、インターネットを経由してアクセス可能なクラウドサービスを前提としている。また、デジタルサービスを提供している観点からユーザビリティやパフォーマンス測定、セキュリティ設定管理など、デジタルサービスの品質を向上させるためのツールについても本実証の対象とする。

1 - 5 . BYOD 端末での業務

経済産業省では、基盤情報システムの一部となっている省内支給 PC の他に個人所有端末の利用が一部認められている。BYOD（Bring Your Own Device）はデバイスの調達や管理のコスト、およびユーザー自身の嗜好に合ったデバイスを利用することによるモチベーションの面で有用であるが、セキュリティやデータ管理に配慮して利用する必要がある。

1 - 6 . 事業計画

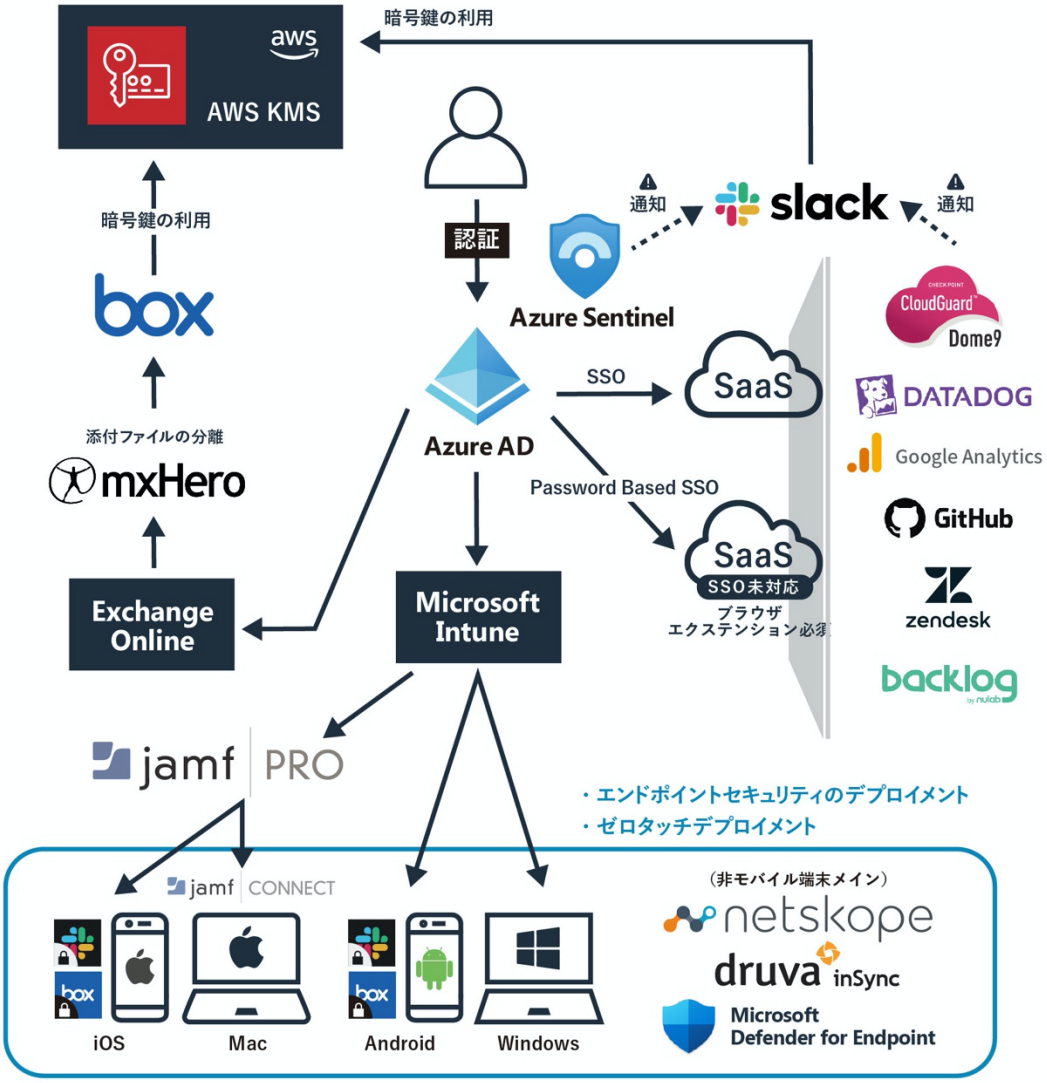
本事業は 2020 年（令和 2 年）7 月より開始され、事業は以下の計画に従って実施された。

❶ プロジェクト管理等に関するツールの調査･分析と効率化手法のための導入実証
❷ 適切にツールを管理し､安全に運用するための管理サービス導入実証
❸ 調査報告書の作成

	2020年 7月	8月	9月	10月	11月	12月	2021年 1月	2月	3月
	キックオフ					構築開始			
❶		✓		✓	✓	✓	✓	✓	✓
❷		✓		✓	✓	✓	✓	✓	✓
❸					✓	✓	✓	✓	✓

1 - 7 . 構成要素

本事業では、最終的に以下のようなシステムを構成した。



上記システム概要図記載の各システムコンポーネントについて、以下に示す。

- 認証認可機能を提供する基盤として、Microsoft Azure Active Directory を採用した
- 端末制御機能を提供する基盤として、Microsoft Intune と Jamf Pro を採用した
- エンドポイントセキュリティ機能を提供する基盤として、以下製品を採用した
  - EDR 機能として、Microsoft Defender for Endpoint を採用した
  - メールセキュリティ機能として、Microsoft Defender for Office 365 を採用した
- SaaS/Web 利用制御機能を提供する基盤として、Netskope を採用した
- データガバナンス機能を提供する基盤として、以下製品を採用した
  - 組織内のデータを集約・管理するストレージとして、Box を採用した
  - データの流通を管理する機構として、Netskope を採用した

    - 端末のローカルファイルシステム上のデータとメールのガバナンスを提供する機構として、Druva inSync を採用した
    - メール誤送信対策機構として、mxHero を採用した
- SIEM（Security Information and Event Management）機能を提供する基盤として、Microsoft Azure Sentinel を採用した
- サービスデスクツールの検証対象製品として、Zendesk 製品を中核としたサービス群を採用した
- クラウド設定管理ツールの検証対象製品として、CloudGuard Dome9 採用をした
- パフォーマンス計測ツールの検証対象製品として、Datadog を採用した
- ソース管理ツールの検証対象製品として、GitHub Enterprise を採用した
- コミュニケーション管理ツールの検証対象製品として、Slack Enterprise Grid を採用した
- 品質管理・タスク管理ツール、および結合プロジェクト管理ツールの検証対象製品として、ヌーラボ Backlog を採用した
- プロダクト改善のためのツールの検証対象製品として、Google Analytics を採用した

2. 適切にツールを管理し、安全に運用するための管理サービス導入実証

2 - 1 . 基本方針

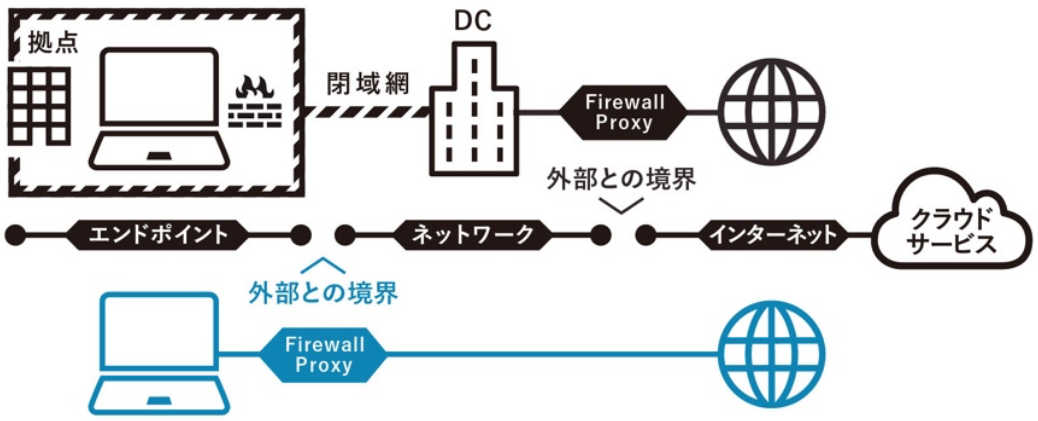
本章では、DX オフィスが業務遂行するインフラを設計する上での基本方針を示す。
基本方針は、DX オフィスが目指す実現構想を、多様な観点から目的、内容、方法をより具体化したものである。

【 DX オフィスが目指す構想 】

- インフラ管理の工数を最小化し、効率的かつ合理的に管理する
- 従来型の境界防御ではなく、クラウドファーストの観点でツール・セキュリティを検討する
- ツール利用者の適切な ID 管理を行う
- 適切なアクセス制限とセキュリティ機構を実装し、業務を安全に行うに足る環境を構築する
- ツールの利用状況を追跡可能とする
- ツール上のデータを安全に保護する

基本方針に沿ったアーキテクチャを考えるに先立ち、まずは現在のセキュリティ事情を考慮した業務インフラについて一般論を述べる。

2-1-1 . モダンかつセキュアな業務インフラの考え方



従来、組織における業務インフラは、ファイアウォールや IPS/IDS、プロキシーサーバー、VPN、閉域網に代表されるネットワーク境界により保護されており、境界内のセキュリティは保たれているものとされてきた。また、組織にて利用可能なアプリケーションをホワイトリストで制御し、当該ファイルを暗号化することで、データの保護がなされているものとしてきた。これらの従来型のセキュリティ施策は、限られた範囲内においては依然として有効だと考えられる。

一方で、近年の業務は境界内に留まらずに SaaS をはじめとするインターネット上のリソースの活用が進んでいる。また、COVID-19 への対応のために自宅やサテライトオフィスなど、組織ネットワーク外での業務を余儀なくされている現状は、業務を既存のネットワーク境界内で行うことをより困難にしている。そのため、現代の組織の業務インフラは、ネットワーク境界に依存しないセキュリティ施策が求められている状況にある。

組織のネットワークインフラは、セキュリティの境界をエンドポイント（端末）まで引き下げ、セキュリティを接続するネットワークに依存しない構成とする必要がある。また、ID と認証認可を制御し、エンドポイントを無条件に信頼することなく、エンドポイントの状態やコンテキスト（利用ブラウザやユーザーエージェントの変遷、地理的情報など）を動的に判断することが必要である。

これらは、ゼロトラストアーキテクチャの一部である。ゼロトラストアーキテクチャは概念であり、現在の技術ではその全ての要素を実装することはできない。これは、現行業務で利用している既存システムのほとんどまたは全てが、ゼロトラストアーキテクチャを前提に構成されておらず、境界型ネットワーク構成となっているためである。

そのため、組織のネットワークインフラは、現在利用可能な技術を用いて、ゼロトラストアーキテクチャの概念を取り込んだ構成とすることが現実解となる。

本節では、モダンかつセキュアな業務インフラの構成要素について解説する。

■ 認証認可

制御された ID の認証認可を行うために、さまざまなクラウドサービスに対して、識別可能な個人に紐づくユニークな ID を用いて行う必要がある。

これは、単一の IAM（Identity and Access Management）をソースとする IDaaS（Identity as a Service）から、SAML（Security Assertion Markup Language）、SCIM（System for Cross-domain Identity Management）、OIDC（OpenID Connect）、API（Application Programming Interface）を用いて各サービスにプロビジョニングすることで実現する。

IDaaS はクラウドサービスに対するユーザーの認証を行い、SaaS へのアクセスを認可する。このとき、ユーザーに与えられる認可レベルは、IDaaS のグループメンバーシップにもとづいて定義できる。

このように、SaaS への全てのユーザー認証を IAM へ集約することで、誰が・いつ認証し、どの SaaS に対して・どの権限で認可したのかを制御できる。

■ 端末認証

端末認証は、組織に登録された端末であることの確認と判断を行う認証である。端末認証は、端末に配布されている証明書（X.509 証明書など）を用いて行われる。組織が発行した証明書を端末が保持しているかどうかで、組織が保有する端末かどうか判定が可能となる。端末認証に用いる証明書は、窃取されることで、その正当性が危殆化される恐れがある。そのため、証明書の発行・配布・保管・更新・失効プロセスに人が介在しないよう、システムによってメンテナンスされる必要がある。端末に対して MDM を構成することで、それらのプロセスをシステムにより自動的に行うことが可能となる。

このように適切にメンテナンスされた証明書を用いて行う認証は、その組織で管理された端末を用いて認証している証明をできる。

■ 端末の健全性

セキュリティの境界をエンドポイントに引き下げるためには、SaaS をはじめとする業務サービスに接続する端末の健全性を評価する必要がある。端末の健全性は、以下のような要素で評価する。

- OS バージョン
- 所定のセキュリティツールのインストール状況
- OS やアプリケーションに対する所定の設定の実施状況
- OS やアプリケーションに対する脆弱性の保有状況
- 未対応のセキュリティインシデントの重要度

端末の健全性を可視化し、システムによる維持を強制することは、端末を制御する上で必要不可欠である。これにより、組織で利用される端末の健全性が保たれていることについて説明可能となる。

■ データ管理規則のコンプライアンス

組織は、どこにどのようなデータを保管しており、誰がどのようにアクセスするかを制御し、それらを記録しているか説明できる必要がある。通常、組織は情報セキュリティポリシーのデータ資産一覧にてこれを規定し、遵守するポリシーを策定する。システムによる制御がされておらず利用者の運用に依存した環境では、組織のデータは端末や各種 SaaS に散在しがちであり、ポリシーの遵守状況は客観的に説明可能な状況とは言い難いものとなっている。

組織は、その説明を可能とするために以下のアプローチを取ることができる。

- 組織のデータを集約するストレージとして、きめ細かなアクセス履歴やアクセス制御、および API による情報の取得やデータ操作の機能を有するものを用いる。
- データの所在を特定の場所に集約するサービスやインテグレーションを用い、それ以外の場所へのデータ転送を制御する機構と組み合わせることで、制御可能な範囲にデータの集約を促進する。
- 端末に保存しているデータを集約し、集約したデータの検索と保全を可能とするツールを導入する。

■ ネットワークによる制限

セキュリティ境界をエンドポイントに引き下げ、制御されたユーザー認証・端末認証を用いたとしても、攻撃面の削減の観点でネットワークによる制限は依然として必要である。前述のとおり、組織の業務システムにおいて、境界型ネットワークの制限によってセキュリティが保たれているとは言い難い状況ではあるが、多くの攻撃を遮断していることもまた事実である。ネットワーク制限によって攻撃面を削減することで、セキュリティ施策を効果的に配置することが可能となる。

ネットワーク制限には、ホスト型ファイアウォールの利用や、セキュリティ機構をホストするデータセンターの IP アドレスのみを許可する設定、および接続する Wi-Fi の暗号化規格にもとづく制御などが挙げられる。

2-1-2 . リスク対応を考慮した業務インフラの考え方

ID の認証認可と端末の認証を制御し、端末の健全性の可視化・維持を続けても、情報資産を取り巻く環境と利用状況、およびそれらの状態は刻々と変化する。組織における業務がネットワーク境界の外に広がりつつある現状では、端末が接続するネットワークによってもリスクは変動する。

そのため、認証認可の条件や端末の健全性は固定的なものでなく、さまざまなリスク要因にもとづいて変化していく必要がある。

本項では、リスクに応じた構成変更を行うための考え方について記載する。

■ 脅威情報と脆弱性情報の利用

リスクは、脅威の源泉と脆弱性、組織に与える影響の掛け合わせにて算出できる。脅威の源泉とは、組織に対する敵対者（アドバーサリ）や自然現象を指す。アドバーサリの戦術/技術/手順（TTP）や動機や意図、能力、およびリソース定義することで、リスクを評価するための材料とできる。脅威の源泉に係る情報は、JPCERT コーディネーションセンター（JPCERT/CC）や独立行政法人 情報処理推進機構（IPA）などの団体から公開されることがあるが、より詳細でタイムリーな情報は、脅威インテリジェンスサービスから入手できる。

また、脆弱性の情報も各ベンダーから公開されており、特に影響が大きいものについては、JPCERT/CC や IPA などの団体から公開されるものを入手できる。脆弱性の情報については、CVSS など重要度をスコア化するフレームワークがあるが、自組織における利用状況や環境要因によってスコアが変動するため、都度優先度付けを行う必要がある。何故ならば、全ての脆弱性が機関によって採番され公開されるわけではないためである。

■ 脅威情報のタイムリーな活用

従来、収集した脅威情報への対応を組織の業務インフラに適用するには、業務インフラの資産管理情報や構成管理情報との人手による突き合わせが必要であった。そして、その結果から導き出されたセキュリティ施策は、その適用までに多くの手間と時間を要していた。また、ID 利用状況の観察や、接続元ネットワークの変遷やログイン履歴の分析・評価が定期的に行われていたとしても、タイムリーなものではなかった。モダンな業務インフラでは、脅威情報の収集と突き合わせおよび分析をシステムで自動的に実施し、その結果のレポーティングやシステム制御の判断材料としてタイムリーに活用していくことが求められる。

■ シャドーIT への対応

組織が認知していないアプリケーションのインストールや、クラウドサービスの利用などをシャドーIT と呼ぶ。この状況を把握するためには、MDM の配備およびプロキシなど各種サーバーのログを定期的にチェックする以外に術はなく、ログから利用しているアプリケーションやクラウドサービスのドメイン、URL を調査するために多くの手間と時間が費やされていた。多岐に渡るアプリケーションや、各種サーバーログは、プロセス名や FQDN、URI での記録にとどまるため、組織で許可していないものであるか否かを識別することはできなかった。

SaaS など Web の通信を復号し、内容を評価する機構として古くから Data Loss/Leak Prevention（DLP）が存在するが、従来のアプライアンス機器を用いた実装方式では、インターネットへの接続点を集約する必要があり、拡大を続ける業務の現場に対応することは難しくなってきている。

モダンな業務インフラでは、ネットワークのトポロジに依存することなく、利用しているアプリケーションや SaaS とテナントを識別し、特に Web 通信は復号して内容を評価できることが求められる。

このように、組織における業務が、さまざまな場所やさまざまなアプリケーション、SaaS に広がっていく状況においては、証跡やログが分散することが予想される。そのため、アプリケーションの起動状況、SaaS や遠隔地の端末のログを集約・分析できる機構が求められる。

■ 脆弱性に迅速に対応できる環境構築とその維持

システムが日々脆弱性のない環境を作り上げ、対処し続けることをサイバーハイジーンと呼ぶ。脆弱性情報は日々更新されるため、脆弱性のない環境の構築と維持には、組織の業務インフラ環境において以下の要素が必要となる。

- 定常的な資産情報の収集（端末・OS／アプリケーション名・バージョンなど）
- 定常的な脆弱性情報の収集（OS／アプリケーション名・影響を受けるバージョン・脆弱性の内容・重要度・脆弱性の利用状況など）
- 定常的な資産情報と脆弱性情報との突き合わせによる、組織内における脆弱性の保有状況の可視化
- パッチやアップデートの配信および適用状況をモニタリングする機構

また、最新バージョンの OS は多くの脆弱性の対処がなされていることから、端末の OS バージョンはポリシーに従って制御可能であることが望ましい。一定のバージョンより古い OS の端末からのサービス利用を制限することで、脆弱性による影響を業務インフラから切り離すことができる。

■ 動的ポリシーを適用するための環境

これまで述べたとおり、端末や接続するネットワーク、利用 ID の状況は刻々と変化していくため、静的な認証認可ポリシーではその変化に対応することはできない。SaaS への認証認可を司る IAM は、接続する SaaS の重要度に応じて、端末や接続するネットワーク、利用 ID の状況に基づき、認証要素を追加する動的ポリシーの利用に対応している必要がある。

■ リスクに応じた構成変更が可能な業務インフラ

OS やアプリケーションが保有する脆弱性は、その全てに対応することで業務アプリケーションの稼働に影響を及ぼす可能性がある。また、脆弱性情報は日々更新されるため、脆弱性の内容から実際に影響を及ぼす可能性の多寡を推測することは容易でない。

リスクは顕在化することで組織への負の影響をもたらすため、実際に利用されている脆弱性がリスクの高い脆弱性であると言える。

そのため、組織の業務インフラでは、検出された脆弱性が実際に利用されているものであるかを自動的に識別する機構が必要である。

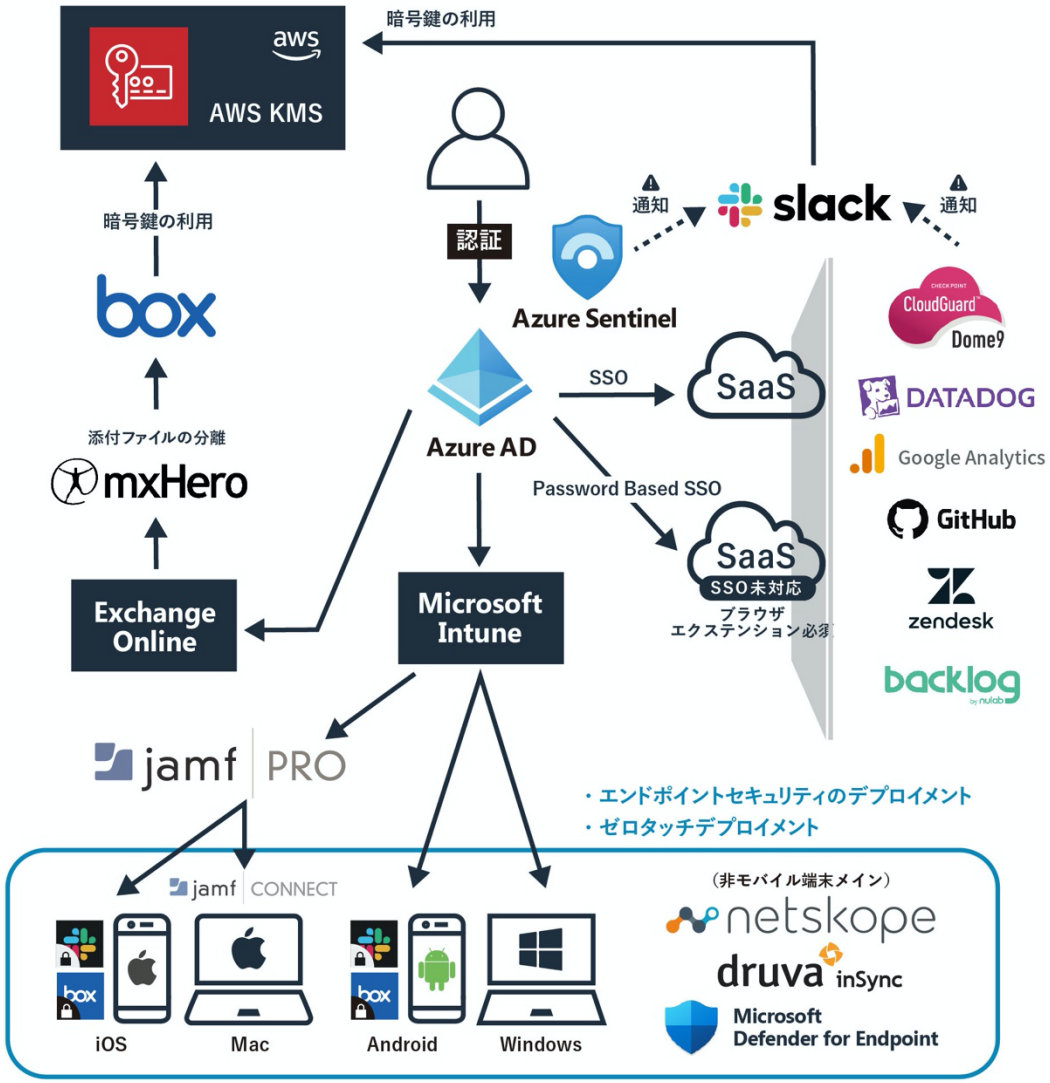
また、リスクが高いと識別された脆弱性に対して迅速に対応するためには、ネットワーク構成に依存しないパッチ配信機構が必要である。

2-1-3 . BYOD の考え方

BYOD の考え方については、別添の『BYOD ポリシー雛形』を参照すること。

2 - 2 . 基本方針を体現するアーキテクチャ

本節では、基本方針を実現するためのアーキテクチャと設計、設定ポリシー、および運用について記載する。まず、アーキテクチャの中心となる構成を以下に示す。



本アーキテクチャの軸となる要素は以下の通りである。

- 認証と認可
- 端末制御
- エンドポイントセキュリティ
- SaaS・Web 利用制御
- データガバナンス
- SIEM

2-2-1．構成要素

各要素の構成するために採用した製品とその概要について以下に示す。

■ 認証と認可

目的と概要

本アーキテクチャは、行政の事業データの取り扱いを前提とするため、従来の ID・パスワードによる認証のみではなく、より高度な認証認可の仕組みが必要となる。

一般的な要件

ID・パスワードを用いた知識認証に加え、スマートフォンや FIDO2（Fast IDentity Online 2）対応デバイスを用いた所有物認証、および指紋や顔などの生体認証への対応が必要である。

加えて、認証を通過した端末に対する認可について、刻々と変化する端末の状態や端末が接続するネットワーク、ログオンする端末 User Agent や OS バージョン、ブラウザなどの属性にもとづくログインパターンを基に動的に認可の可否や認証要素の追加要求を行うなど、高度な判断が行われる必要がある。

本アーキテクチャ特有の要件

事業で扱うさまざまなクラウドサービスに対して、事業に携わる職員による継続的かつ大規模なメンテナンスを行うことなく、ユーザーやグループのプロビジョニングが可能で、SAML や OIDC の認証プロトコルに非対応のクラウドサービスに対してもシングル・サインオン（以下、SSO）を構成して、先に述べた認証認可を適用できる必要がある。

また、職員が普段利用する ID に特権を付与し続けることや、特権をもつ ID を共有することで意図せぬインシデントが発生する可能性がある。そのため、事業に携わる職員が利用する ID には特権を付与せず業務上必要な作業時のみ一時的な特権を付与し、特権の利用を記録・管理するために単一の ID のみを利用できる環境が求められる。

選定

認証認可の基盤として、これらの要件を全て満たす環境を迅速に構成できる、Microsoft Azure Active Directory を採用する。

■ 端末管理

目的と概要

端末管理とは、端末の情報を収集し、設定やアプリケーション、証明書を配信することで、組織で管理する端末を一元的に管理・制御することである。端末を管理下におくことで、端末の健全性を保つだけでなく、アプリケーションの配布や変更が容易となる。

一般的な要件

事業に携わる職員はシステム上の理由で業務遂行する場所を制限されるべきではない。そのため、職員の所在や接続するネットワークに関わらず、インターネットを通じて端末に対する設定やアプリケーションを配信し、その端末の情報を収集、および端末の挙動を制御できることが求められる。

また、収集した情報は、認証認可に関わる制御を判定する材料として、認証認可の基盤に共有されなければならないことから、端末制御の基盤と認証認可の基盤は統合されている必要がある。

本アーキテクチャ特有の要件

本アーキテクチャは、事業に携わる人的リソースが限られていることと、証明書の安全な取り扱いに対する教育コストを低減する観点から、Windows や macOS、iOS、iPadOS、および Android に対して、デバイス認証に用いる証明書の発行・配布・更新・失効プロセスに、人が介在することなく自動的に行える必要がある。

また、事業の期間が数ヶ月～2 年と短期となる場合においても速やかに環境構築を行い、本来行うべき事業に注力するため、証明書発行管理のために専用システムの構築を別途行わなくてもよい構成であることが求められる。

選定

端末制御の基盤として、これらの要件を全て満たす環境を迅速に構成できる、Microsoft Intune と Jamf Pro を採用する。

Microsoft Intune と Jamf Pro の使い分けと関係性について、以下に示す。

- Microsoft Intune は、Windows 10 端末を制御するために用いる。
  Microsoft Intune は、Azure Active Directory と統合されているため、収集した端末の属性情報を Azure Active Directory に引き渡すことができる。

- Jamf Pro は、macOS と iOS、iPadOS を制御する上で秀でており、端末内のさまざまな情報にもとづいて動的にグルーピングするのに長けている。これは、制御が難しい構成を配信する上で適用順序を適切にコントロールすることに寄与する。また、Jamf Pro は、Microsoft Intune と連携することができ、収集した端末の属性情報を Microsoft Intune に引き渡せる。

■ エンドポイントセキュリティ

目的と概要

本アーキテクチャは、事業に関わる職員が接続するネットワークに関わらず安全に業務遂行する必要があるため、セキュリティ境界を端末に引き下げる観点から、端末への設定を徹底することが必要不可欠である。

一般的な要件

端末へ設定を徹底することには、以下の内容が含まれる。

- ホスト型ファイアウォールを用いたネットワーク接続の制御
- 攻撃者が利用する攻撃面を縮小する OS 設定
- タイムリーな OS アップデートやパッチ適用対応
- 未知・既知のマルウェアへのリアルタイム対応や不審な挙動の検出と制御
- フィッシングメールをはじめとする不審メールや添付ファイルに含まれる脅威の検出と防御

また、メールに係る脅威は、アンチマルウェアや振る舞い検知以外の部分でもメール特有の攻撃手法（スプーフィング、類似ドメインの利用、乗っ取ったエグゼクティブのメールアカウントの利用、Reply-to の置き換え、不審な URL）に対して検出・評価・抑止できる必要がある。特に、メール本文や添付ファイルに記載された URL への接続後にやり取りされる通信の内容に対して、HTTPS 通信を復号した上での評価や検査が必要である。メールに係る脅威は、端末上での挙動調査（送付された URL のクリック状況など）と密接な関係性があるため、統合した調査ができることも求められる。

別の観点として、端末は、侵害の可能性を避けられないものであるが、侵害の可能性のある端末を完全に利用停止状態（ネットワークの遮断を含む）とすることは、業務継続の観点から無理が生じる。そのため、侵害の疑いのある端末は、その程度に応じて、重要な情報を保有するシステムに対してのみアクセス制限をかけ、組織が保護したい資産へのアクセスを制限できる必要がある。

本アーキテクチャ特有の要件

端末への設定の徹底は、事業の期間が数ヶ月～2 年と短期となる場合においても速やかに環境構築を行い、本来行うべき事業に注力することが求められる。そのため、端末への設定を徹底するための基盤の構築や維持にかかる運用は、可能な限り低減する必要がある。特にエージェント更新や OS のアップデートに追従するためのメンテナンス作業を要する構成は、可能な限り避ける必要がある。

選定

端末への設定の徹底は、上記要件を満たす端末制御の基盤である Microsoft Intune と Jamf Pro を通じて実施する。

端末のマルウェア対策や未知の攻撃に対応するため、Endpoint Detection and Response （EDR）を導入する。

EDR は、上記要件を満たす Microsoft Defender for Endpoint を採用する。Microsoft Defender for Endpoint の特徴は以下の通りである。

- Windows 10 の OS 機能の一部であり、Windows 10 においては Microsoft アプリケーションへの干渉や OS バージョンアップに伴う影響が発生しないため、動作確認に係る運用業務を軽減できる。
- Windows 10 に対して Microsoft Intune を通じて有効化できる。
- macOS に対して Jamf Pro を用いて配信できる。
- 未解決のセキュリティインシデントのリスクレベルを Microsoft Intune を通じて、Azure Active Directory に属性情報として連携できる。

端末に導入しているアプリケーションの収集と脆弱性情報を管理するため、先述の要件を満たす Threat & Vulnerability Management（TVM）を導入する。

TVM の特徴は以下の通りである。

- Microsoft Defender for Endpoint が提供する機能を用いる。
- Windows 10 と macOS において、OS と導入しているアプリケーションのバージョンから脆弱性をリストアップする。リストアップされた脆弱性は、悪用されているものであるかを識別できる。

メールやファイルを通じたフィッシングやスパム、マルウェアを検出・対処する目的で、先述の要件を満たす Microsoft Defender for Office 365 採用する。

Microsoft Defender for Office 365 は、メールの添付ファイルに対するウイルスチェック・サンドボックス機能だけでなく、PDF や Office ファイルに含まれる URL を安全なものに置き換える機能を用いて、EDR と協調したエンドポイント保護を実現できる。

端末が接続する不審な URL の評価や、Web サービスと端末間でやり取りされる通信の内容に脆弱性を突く内容が含まれているかを検出・通信の抑止を行う目的として、上記条件を満たす Netskope と同製品の Threat Protection 機能を採用する。

■ SaaS・Web 利用制御

目的と概要

本アーキテクチャは、事業に関わる職員が利用するクラウドサービスを可視化し、認可された安全性の高いクラウドサービスのみ利用することを推進していく必要がある。職員が利用するクラウドサービスは、データの取扱状況やアクセスコントロール、監査性などが貧弱なものであってはならない。

一般的な要件

クラウドサービスの利用を可視化・制御する機構は、多岐にわたる SaaS を識別し、さまざまな観点での分析結果に基づいた格付けをレポートし、その格付けに基づいた利用制御機能が必要である。

クラウドサービスのレポートとして必要な観点は、以下のものが挙げられる。

- 第三者認証の取得状況
- データの取り扱い
- アクセスコントロール
- 監査性
- ディザスタリカバリと事業継続
- 法律とプライバシー
- 脆弱性と侵害の実績

また、認可されたクラウドサービスであっても、組織や事業が契約したテナントと個人が契約したテナントを識別し利用を制御することで、データの持ち出しを抑止できる必要がある。そのため、SaaS を利用制御する機構は、HTTPS 通信を復号し、接続する SaaS のテナントを識別できる必要がある。

本アーキテクチャ特有の要件

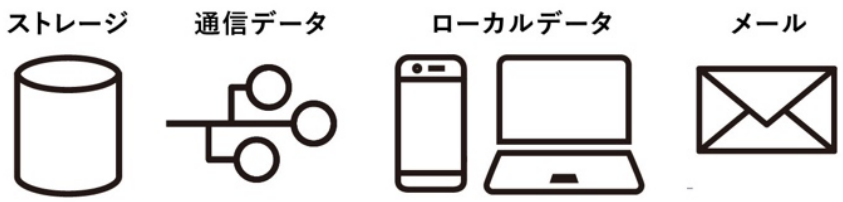
事業に携わる職員は、利用する端末からさまざまな Web サイトにアクセスすることが想定され、安全に業務を遂行するためには一般的なカテゴリフィルタリングや脅威情報にもとづくフィルタリングの他に、動的なカテゴリフィルタリングが必要となる。動的なカテゴリフィルタリングの対象には、作成されたばかりのドメインや管理者が変更されたばかりのドメインが分類される。

事業に携わる職員はさまざまな場所から業務遂行するため、ネットワークトポロジに依存せずにこれらを制御できることが求められる。

選定

SaaS・Web の利用制御機構として、上記要件を満たす Netskope を採用する。

■ データガバナンス



目的と概要

本アーキテクチャでは、事業で取り扱われるデータ管理の透明性（アクセス状況の可視化、アクセスと公開範囲の制御、データの所在の把握、流通状況の可視化と制御、データ暗号化に係る自組織で用意する鍵の利用と管理）が必要となる。

データガバナンスの対象をストレージ・通信データ・ローカルデータ・メールの 4 つに分け、それぞれ順に解説する。

一般的な要件

組織内のデータを集約・管理するストレージは、きめ細やかなアクセス権限と公開範囲の制御を、利用者に意識させないことが要求される。例えば、不特定多数の利用者からの情報収集は、内部に対する公開範囲を絞ったフォルダに格納する構成を容易に行える必要がある。そのため、当該ストレージは、設計・管理された権限を強力にフォルダツリーに伝播できる必要がある。

また、当該ストレージは、データの利用状況と管理に対する説明責任を果たす目的で、データのアクセス状況（閲覧、ダウンロード、更新、削除）と管理操作の記録が詳細に取得し、レポートできることが求められる。

本アーキテクチャ特有の要件

事業に携わる職員は、本来の事業で成すべき事柄に時間を費やすべきであり、特定の職員がストレージの維持や管理に時間を割かれることは望ましくない。そのため、ストレージ管理作業のうち、特に多くなることが予想される内部・外部とのコラボレータの管理を部門や、事業ごとの管理者に委任できることが望ましい。

また、当該ストレージは、行政文書を保管することから、インデックスを含む内容をストレージの運営事業者からも閲覧できないよう、事業側で用意した暗号鍵を用いてストレージ上のデータを暗号化する必要がある。一方で、事業側で用意した暗号鍵を用いた暗号化は、ストレージが提供する検索機能を阻害してしまう。そのため、ファイルやフォルダ、フォルダツリーに対して、検索性を補完するメタデータを付与できることが求められる。

別の観点として、事業に係る職員と外部事業者がデータ共有を行う上で、データをダウンロードして編集する運用は、事業で取り扱うデータが制御可能な領域外に分散していくことを意味する。そのため、当該ストレージは、さまざまな形式のデータのプレビューすることができ、特に編集する機会の多いオフィスファイル（Microsoft 形式や Google 形式）について、オンラインで編集できることが求められる。また、データ共有する相手にレビューを求める際に、編集やダウンロードを許可することなく、ストレージ上のデータに対してコメントを付与する形でのコラボレーションが求められる。

選定

組織内のデータを集約・管理するストレージとして、上記要件を満たす Box を採用する。

■ データガバナンス（通信データ）

目的と概要

データの機密性が 3 以上に類するものである場合、データの流通を管理し、制御できる必要がある。本アーキテクチャにおける通信データを対象としたデータガバナンスについて解説する。

一般的な要件

事業に係るデータが流通する場として、先に述べた SaaS・Web・ストレージの他にメールとチャットが挙げられる。

メールとチャットは外部事業者とデータやり取りする場となるため、データの流通を管理する機構は、メールとチャットシステムに対して API を用いたファイルの内容の検査が必要である。

本アーキテクチャ特有の要件

事業で取り扱うデータが機密性 3 以上に類するものである場合、データの流通を管理する機構は、その流通経路を問わず検出・抑止できる必要がある。

機密性ラベルは、日本語で文書上に表記されるため、データの流通を管理する機構は、分類ラベルを別途付与することなく SaaS や Web サービスを流通する HTTPS 通信を復号し、通信データからファイルの内容を日本語で識別できる必要がある。

選定

データの流通を管理する機構として、上記要件を満たす Netskope を採用する。

■ データガバナンス（ローカルデータ）

目的と概要

端末の利用はオフラインで利用されることも想定される。通信可否に関わらず、端末のデータは制御下である必要がある。本アーキテクチャにおけるローカルデータを対象としたデータガバナンスについて解説する。

一般的な要件

本アーキテクチャは、事業に係るデータが保存される場として、端末のローカルファイルシステムが含まれる。そのため、組織内の端末に保存されているデータを一元的に保全・追跡可能とすることで、内部犯による不正行為の記録や情報の持ち出しや改ざん、削除に対する否認を防止や漏えい情報の経路特定、および影響範囲を特定できる必要がある。

本アーキテクチャ特有の要件

不正行為の記録はメールにも含まれるため、職員が業務で利用する全ての端末内のデータとメールを保全し、職員毎に管理できる必要がある。端末ローカルのデータ漏えい防止を目的とした端末の所在追跡やインターネットと通信ができないオフライン状況でのリモートワイプを実現する必要がある。

選定

端末のローカルファイルシステム上のデータとメールのガバナンスを実現する機構として、上記要件を満たす Druva inSync を採用する。

■ データガバナンス（メール）

目的と概要

メールの誤送信時に添付ファイルが拡散した場合、管理や制御ができない点を解決する。本アーキテクチャにおけるメールを対象としたデータガバナンスについて解説する。

一般的な要件

本アーキテクチャでは、組織内外とやり取りするメールの添付ファイルについて、合理的かつ根本的な誤送信対策を行う目的で、ファイル自体を相手先に送付することなくやり取りすることを実現でき、誤送信が発生した際にはそのファイルへのアクセス権を取り消す必要がある。そのため、誤送信対策機構は、メールの添付ファイルをメールから分離・ストレージに格納した上で、メール本文にストレージに格納したファイルへの共有リンクに差し替えることが求められる。また、ストレージに格納したファイルには、受信者のみに認証を経てアクセス可能とする等の適切なアクセスコントロールを設定可能とする必要がある。

一方で、共有リンクを受け取った組織が、ストレージへの接続が許可されていない場合を考慮して、誤送信対策機構は特定のメールドメインに対して送受信する、メールの添付ファイル分離処理をバイパスできる必要がある。

本アーキテクチャ特有の要件

別の観点として、S/MIME をはじめとするメール暗号化技術と添付ファイル分離が干渉することのないようにすることも忘れてはならない。そのため、誤送信対策機構は、メール作成の時点でストレージ上のファイルをメールに共有リンクという形で直接添付することで、暗号化されたメールにはファイルが添付しない運用が行える必要がある。この操作は運用利便性を考慮して、容易であることが求められる。

選定

誤送信対策機構として、上記要件を満たす mxHero を採用する。

■ SIEM

目的と概要

本アーキテクチャは、Azure Active Directory や Office 365、Exchange Online、Microsoft Defender for Endpoint など Microsoft 製品を多く採用している。SIEM は、本来分析・調査したい事柄からログの出力や正規化、収集を設計し、分析ロジックと可視化の実装を要する。

一般的な要件

事業に係る職員や事業者は、事業で達成する目標に注力するべきであり、SIEM のパフォーマンスチューニングや冗長構成、およびシステムの維持管理に費やす労力は最小限に抑える必要がある。このことから SIEM 機構はクラウドで実装され、Microsoft 製品を中心としたクラウドサービスに対するコネクタを豊富に取り揃えており、分析や可視化のテンプレートが予めセキュリティ運用の観点で機能するよう取り揃えられている必要がある。

本アーキテクチャ特有の要件

数ヶ月～2 年程度の短い事業が多いことから、SIEM 機構の構築や実装にかかる期間は極力短くできることが求められる。

また、事業の規模は大小さまざまであり、予算が抑えられている小規模な事業であっても SIEM を導入できる必要がある。そのため、SIEM の課金体系は、データの流入量と保存期間をベースに従量課金に対応し、イニシャル・ランニングコストを抑えることが求められる。

選定

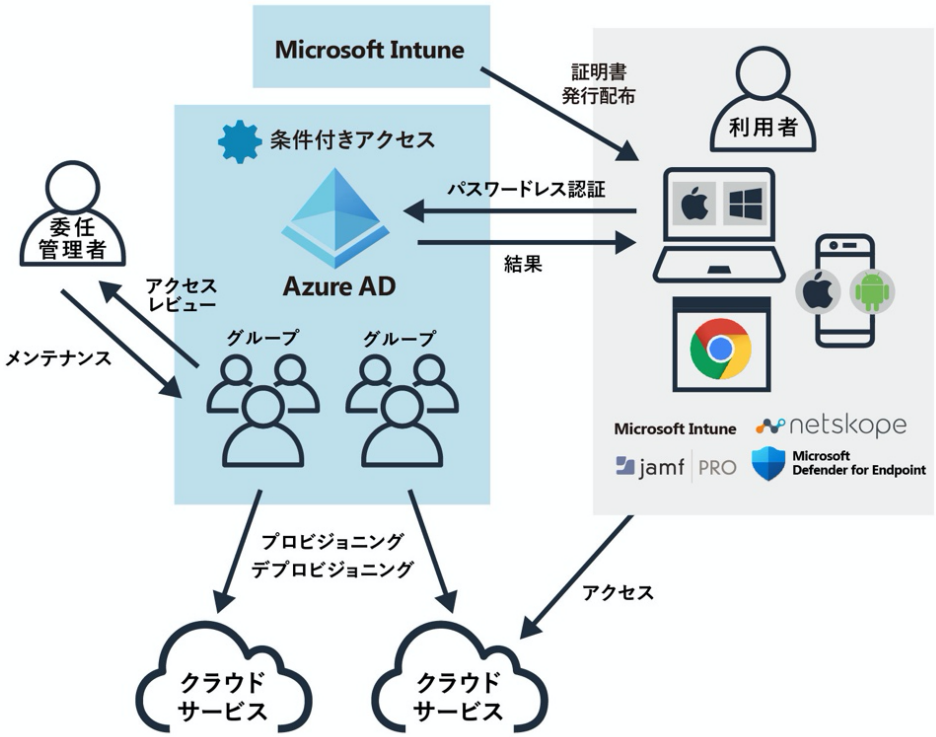
SIEM として、上記条件を満たす Microsoft Azure Sentinel を採用する。

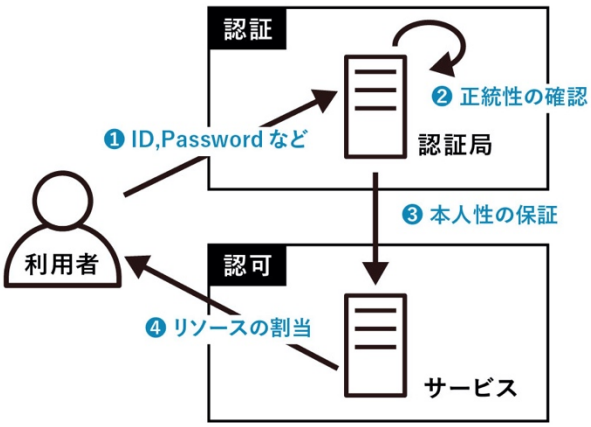
2-2-2 . 各アーキテクチャ要素における設計と運用

本項では、先に述べた一般的な課題や要件および経済産業省特有の課題に対して、各アーキテクチャ要素をどのような設計と運用で解決するかを記載する。

■ 認証と認可

本アーキテクチャの認証認可における設計と運用について以下に示す。





ID の管理

ID は、Azure Active Directory に登録したユーザーとグループをマスターとし、利用するクラウドサービスに対して、SAML、SCIM、OIDC、または API を用いてユーザーとグループをプロビジョニングする構成とする。グループは、クラウドサービス側で認可設定を行う際の設定単位として用いることができる。そのため、ID 管理者は、各クラウドサービスの認証と認可に係るグループメンバーシップの管理を Azure Active Directory 上でのメンテナンスをもって完結する構成とした。

認証の条件

認証は、各プラットフォームにおいて、多要素認証を構成した。

Windows 10 環境

Windows Hello for Business を構成し、PIN または生体認証を用いたパスワードレス認証を構成する。加えて、Azure Active Directory 条件付きアクセスを用いて、Microsoft Intune の登録状況と Microsoft Defender for Endpoint での未解決リスクの残留状況、および送信元 IP アドレス（Netskope のデータセンターであること）を条件とすることで、事業の情報資産を取り扱うクラウドサービスにアクセスするセキュリティ基準を満たしている端末からの認証であるということを検証する。

Azure Active Directory 条件付きアクセスは、Windows 10 環境においてはブラウザとして Microsoft Edge、Internet Explorer、Google Chrome にて動作する。そのため、Windows10 環境においては、これらのブラウザを標準ブラウザとして利用する。

macOS 環境

Jamf Connect を構成し、Web Auth 認証を通じて Microsoft Authenticator を用いた多要素認証を構成する。加えて、Azure Active Directory 条件付きアクセスを用いて、Jamf Pro の登録状況と Microsoft Defender for Endpoint での未解決リスクの残留状況、および送信元 IP アドレス（Netskope のデータセンターであること）を条件とすることで、事業の情報資産を取り扱うクラウドサービスにアクセスするセキュリティ基準を満たしている端末からの認証であるということを検証する。

Azure Active Directory 条件付きアクセスは、macOS 環境においてはブラウザとして Safari、Google Chrome にて動作する。そのため、macOS 環境においては、これらのブラウザを標準ブラウザとして利用する。iOS、iPadOS、Android 環境では、適切な強度の PIN を構成するよう MDM を通じて設定を配信する。PIN の強度設定は、『NIST SP800-63B』に準じて設定する。

認可の条件

認可は、Azure Active Directory Identity Protection Premium P2 を用いて、ログインする端末が接続するネットワークや UserAgent、ブラウザバージョンなどの端末情報（プロパティ）、およびログインパターンを鑑みて動的に認可を判定するサインインポリシーとユーザーリスクポリシーを構成する。

SSO の構成

IdP である Azure Active Directory を用いて組織が業務で利用する SaaS に対して、SSO を構成する。 SSO を構成する際に IdP から SaaS に対してユーザー名として引き渡す情報の方針について、以下にまとめる。

- SaaS がメールアドレスを要求する場合、原則として、IdP は UPN ではなくメールアドレスを渡すように構成する。

- ユーザー名（メールアドレス）がユニークであることを SaaS が要求する場合がある。管理する担当者のメールアドレスが、すでに別のテナントを管理しているケースにおいて、ユーザー登録できない可能性がある。このケースは、特に管理作業を行うユーザーで起こり得る。その場合は、別のメールアドレスを発行し、Azure Active Directory に外部ユーザーとして登録する方針とする。発行されたメールアドレスが、本人のものであるかを検証したいが、検証が難しい場合は、組織が払い出したメールアドレスを利用する方針とする。

外部ベンダーによる環境のメンテナンスを委託する場合

SaaS の運用を外部ベンダーが行う場合、SaaS に SSO するため IdP にユーザー登録を行う必要がある。SSO を構成する方針として、SaaS がメールアドレスを要求する場合、UPN ではなくメールアドレスを渡すように構成する。

SSO 非対応の SaaS への対応

SAML や OIDC といった SSO プロトコルに対応しない SaaS に対しては、Azure Active Directory の Password Based SSO を用いた管理を行う構成とする。 Password Based SSO は、ブラウザ拡張を用いて ID とパスワードを代理入力する機能である。利用者と管理者は、Password Based SSO において、ID とパスワードをブラウザ拡張に登録する必要がある。管理者自身が ID とパスワードを登録することで、利用者にパスワードを知られる事なくパスワードを登録できる。

本事業では、SSO 非対応の SaaS を利用しなかったことから、Password Based SSO を用いた検証は行わなかった。

SaaS 利用者の認証と認可のメンテナンス

SaaS 利用者への認証認可は、IdP におけるグループのメンバーシップにもとづいて制御する。グループメンバーシップのメンテナンスは、Azure Active Directory Identity Protection Premium P2 のアクセスレビュー機能を用いて、各グループの複数の代表者によって行う。アクセスレビュー機能は、直近 30 日の Azure Active Directory への認証履歴にもとづいて、グループメンバーシップの承諾・拒否の推奨を提示する。各グループの代表者は、指定された期間内にレビューを完了することで、SaaS に認証認可させる利用者のメンテナンスを行える。

この運用により、IdP 管理を行う担当者にグループメンバーシップのメンテナンス業務が集中することなく、各グループの責任者に委任できる。

共有アカウントの取り扱い

SaaS 利用者には個人を識別可能な一意の ID を発行し、共有アカウントを発行しない。

システムユーザーの管理

SaaS システムを管理・運用するために、人に紐付かないユーザーアカウント作成が必要な場合がある。また、Azure Active Directory 条件付きアクセスのような強い認証制御機構設定時の事故に対応する目的で、人に紐付かない緊急用ユーザーを作成する必要がある。このような場合、これらのユーザーアカウントには、ID/パスワードのみの認証を許可するよう構成し、その利用の際にアラート通知されるよう構成する。本実装については、「SIEM」の節を参照すること。

これらのユーザーアカウントを利用する際は、申請と承認を要する運用とする。組織の管理者はアラート通知の際に申請・承認記録を確認する運用とする。

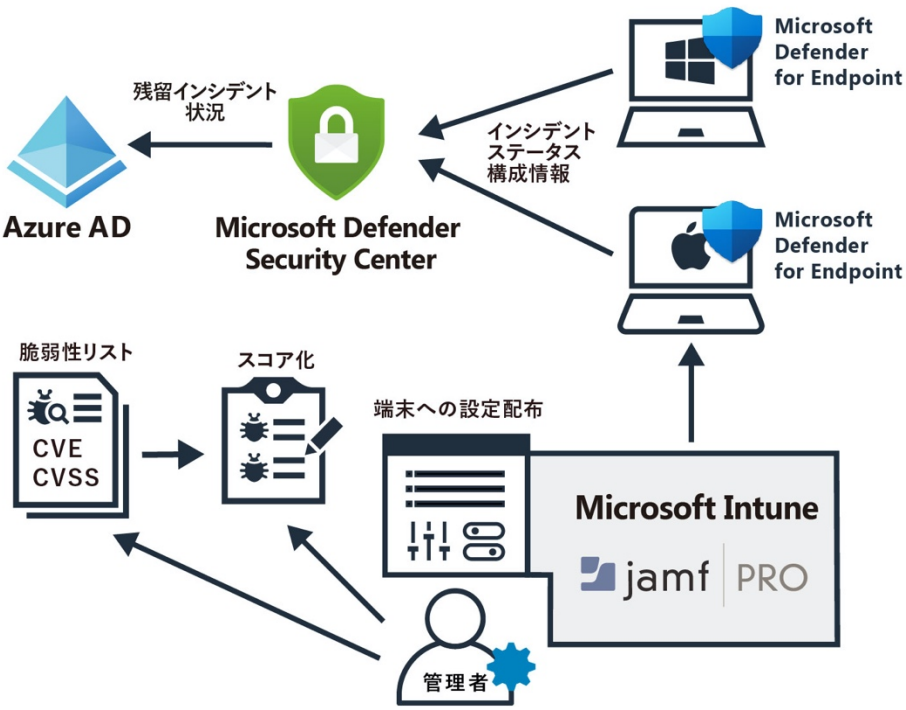
システムユーザーアカウントのパスワードは、SSO を構成可能なパスワードマネージャを用いて管理することが望ましいが、本事業では期間と予算の関係上、実装・検証するに至ってはいない。

認証認可に係る検証結果

SaaS 利用者に対して、正当性や本人性を適切に確認できる認証認可の基盤として動作することが確認できた。

■ 端末認証

本アーキテクチャの端末認証における設計と運用について以下に示す。



証明書の発行管理プロセス

端末認証に用いる証明書は、Microsoft Intune、Jamf Pro にて発行される証明書を用いる。この証明書は、Microsoft Intune、Jamf Pro にて自動的に発行され、24 時間の有効期限が設定されている。配布・更新プロセスも Microsoft Intune、Jamf Pro にて自動的に行われるため、証明書の発行・配布・保管・更新・失効プロセスに人が介在しない構成を実現した。そのため、証明書に係る運用は発生しない構成となった。

端末認証に係る検証結果

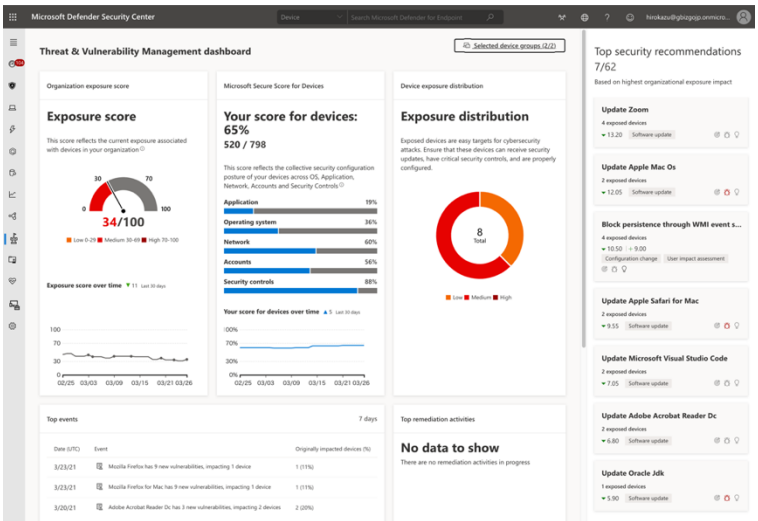
人的リソースの制約を鑑みた自動化の実装がなされており、管理者の作業負担を低減できると評価した。

■ 端末の健全性

本アーキテクチャの端末の健全性における設計と運用について以下に示す。

端末への設定の徹底と健全性の評価

組織のセキュリティ管理者は、Microsoft Defender for Endpoint の Threat & Vulnerability Management（TVM）機能を用いて、収集されたインベントリ情報にもとづいて可視化された、利用中の OS やアプリケーションに存在する脆弱性と、世の中で実際に利用されている脆弱性にもとづいてパッチ適用方針や優先度決定をする運用を行う。



Windows 10 環境への設定の徹底は、攻撃によく用いられる機能やアプローチを阻害する、攻撃面の縮小ルールをブロックモードで構成することを基本とする。

また、TVM 機能にてレポートされた OS の推奨設定にもとづいて、Microsoft Intune や Jamf Pro を用いて追加の設定を配布する。

TVM 機能は、対応状況のスコアリングを提供するが、スコアは日々変動するため完全な対応を目指すことはせず、世の中で実際に悪用されている脆弱性を優先的に対応していく方針で運用を行う。

セキュリティリスクにもとづくアクセス制御の強制

IdP は、Microsoft Defender for Endpoint で可視化された未対応のセキュリティリスクの残留状況にもとづいて、アクセス制御するよう構成する。セキュリティリスクは、マルウェアや不審なプロセスの検出状況に応じてレベル付けがなされる。検出されたセキュリティリスクは、Microsoft Defender for Endpoint にて自動的・半自動的に対応されるが、運用状況によっては軽微な検出について一定期間残留する可能性が考えられる。そのため、重要なデータを扱う SaaS 以外の認証については、軽微なセキュリティリスクが残留した状態での認証を許可するよう構成する。

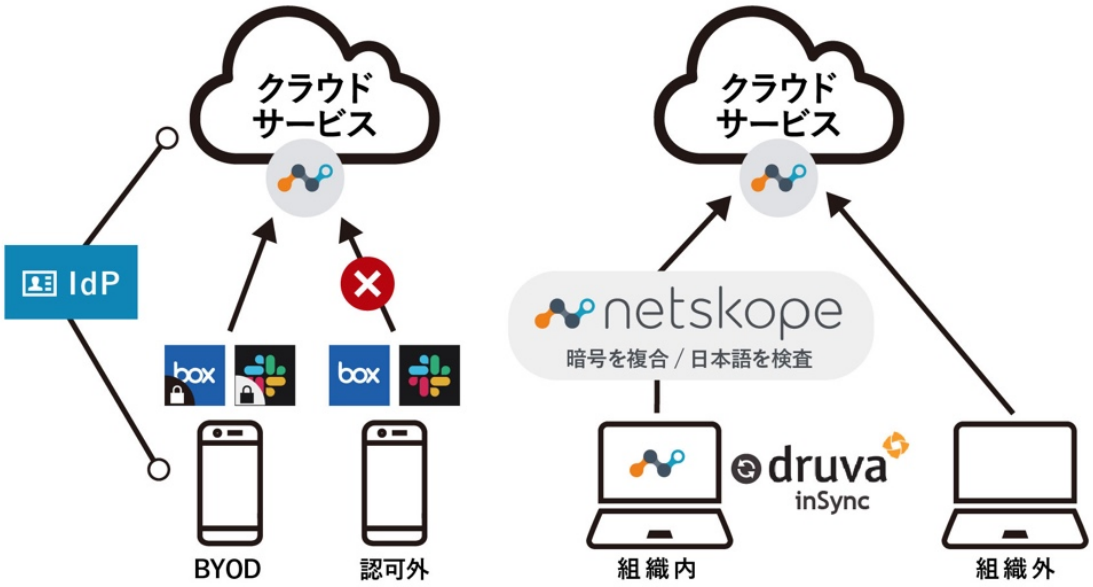
端末の健全性に係る検証結果

端末の健全性に関し、状況の可視化だけでなくセキュリティリスクの残留状況に基づいたアクセス制御が可能なことを確認できた。

■ データガバナンス

本アーキテクチャのデータガバナンスにおける設計と運用について以下に示す。

機密情報の流通の把握と制御



データが流通する経路や保存される箇所は以下のように定義される。

データが流通し得る経路

- インターネット（Wi-Fi、テザリング経由）
- メール（Exchange Online）
- 周辺機器接続ケーブル

データの流通先となり得る場所

- 組織で認可する SaaS、Web
  - Box
  - Slack
  - Backlog
  - GitHub
- 上記以外の SaaS、Web
- USB ストレージ・外部メディア
- PC・スマートフォン・タブレット

データは、PC・スマートフォン・タブレットを起点に Web やメール、周辺機器へ流通することから、これらのデバイスを起点とした流通先へのデータ保存を制御する方式として以下を実装する。

PC

データを加工編集する業務が中心となるため、データ保存自体の制限は行わず、USB デバイスに対する利用制限を Microsoft Intune と Jamf Pro で配信する。また、Netskope Agent を導入し、機密性 1〜3 を識別する日本語文字列を条件として、SaaS や Web へのファイルアップロードに対して制限や警告の記録を行うよう構成する。Netskope は、接続する SaaS や Web を可視化しつつ、テナント単位で認可 SaaS を登録し、認可外テナントや SaaS へのデータアップロードを制限するよう構成する。

スマートフォン・タブレット

スマートフォン・タブレットは、BYOD 利用が前提となっているため、端末初期化を伴う管理モードを用いたダウンロード制御はできない。また、スマートフォン・タブレットに対する Netskope の導入は、私的な Web や SaaS 利用を必要以上に監査してしまうおそれがある。そのため、スマートフォン・タブレットで行う業務は、アプリからのダウンロードが制限可能な MAM アプリケーションでのみ行うよう事業主体と調整を行った。スマートフォン・タブレットから MAM に対応していない SaaS の認証は、IdP で制限するように構成する。MAM アプリケーションは、Microsoft Intune と Jamf Pro を用いて配信するよう構成する。

上記実装から、Netskope が導入されている端末とスマートフォン・タブレットのみが制御範囲となっている。一方で最も多くの情報が流通・集約される Box や Slack、Exchange Online の利用者は必ずしも組織内の職員に限らない。そのため Netskope の API Introspection 機能を用いて、当該クラウドサービス上を流通するデータを利用者の区別なく監査するよう実装する。

また、PC にデータを保有する以上、端末の紛失やウイルス感染による影響範囲を特定できる必要がある。そのため、Druva inSync を用いて PC 上のユーザー領域をバックアップするよう構成する。これにより、PC 内に保存されているユーザーデータに対して利用者はデータ消失のおそれがなくなり、管理者による影響範囲特定が可能となる。

クラウドストレージに格納するデータのアクセスコントロール

データ格納先となる Box は、アクセス権限をウォーターフォール型で継承するため、データのアクセスコントロールを管理者側で制御する必要がある。そのため、トップレベルのフォルダ作成・管理を管理者でのみ行えるよう構成する。本事業向けに構成したトップレベルフォルダとその配下のフォルダについて、以下に示す。

省内共有

このフォルダでは、外部共有を禁止し、共有リンクの公開範囲はフォルダに設定されているユーザーに限るよう構成した。配下に部門フォルダとプロジェクトフォルダを用意し、これらのフォルダは、申請にもとづいて Box 管理者が作成する。部門フォルダには部門グループと部門管理者グループをアクセス許可グループとして登録している。部門管理者グループにはコラボレータの設定権限を付与することで、部門フォルダ配下の管理を部門管理者に委任する構成とした。プロジェクトフォルダも同様の設計方針で構成している。

省外共有

このフォルダでは、外部共有を許可し、共有リンクの公開範囲はフォルダに設定されているユーザーに限るよう構成した。配下に外部共有先会社ごとのフォルダとプロジェクトフォルダを用意し、これらのフォルダは、申請にもとづいて Box 管理者が作成する。各フォルダには省内関係者グループと省内関係者管理グループをアクセス許可グループとして登録している。省内関係者管理グループにコラボレーターの設定権限を付与することで、外部共有先のコラボレーター登録作業を省内関係者管理グループメンバーに委任する構成とした。なお外部共有先のコラボレーターの有効期限を予め設定しておくことで、棚卸しの手間を省く構成としている。

個人用

このフォルダでは、外部共有を禁止し、共有リンクの公開範囲はフォルダに設定されているユーザーに限るよう構成した。配下に個人を識別できる名称のフォルダを用意し、これらのフォルダは、申請にもとづいて Box 管理者が作成する。各フォルダには個人ユーザーをアクセス許可ユーザーとして登録している。

一般公開用

このフォルダでは外部共有を許可し、共有リンクの公開範囲は、利用者によって URL を知る者全員のアクセスが可能である設定をできるよう構成した。

配下にパンフレットや配布資料を配置するフォルダを用意し、これらのフォルダは、申請にもとづいて Box 管理者が作成する。各フォルダには、省内関係者グループをアクセス許可グループとして登録している。

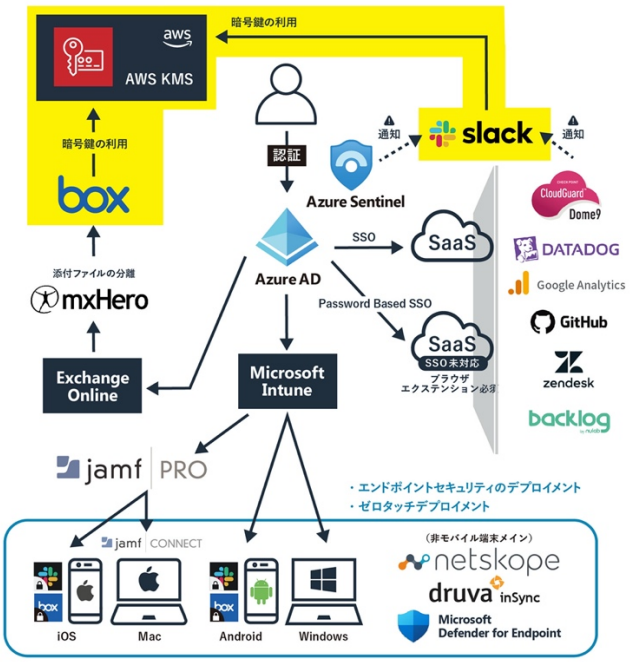
情報公開に慎重を期す場合は、Box Relay を用いたワークフローを経てレビューされたファイルが本フォルダに配置される方式は、検証期間の制約から本構成としている。

添付ファイル格納用

このフォルダでは、外部共有を禁止し、共有リンクの公開範囲はフォルダに設定されているユーザーに限るよう構成した。配下に、メール送信者や件名、送受信日時を識別可能なフォルダが、mxHero によって自動的に作成されるよう構成している。なお本フォルダを直接編集・管理できるユーザーは、管理者に限定している。

これらのアクセスコントロールは、グループメンバーシップにもとづいて制御している。グループメンバーシップは、IdP である Azure Active Directory 上のグループメンバーシップを反映するよう構成することで、メンテナンス箇所を一箇所に集約している。

クラウド事業者に対するデータのアクセスコントロール



クラウド事業者によるデータ読み取りを懸念する場合、利用者が生成した暗号鍵を用いたデータ暗号化（BYOK）を行うことで対応できる。本事業では、行政データをクラウド上で扱うことを前提とし、BYOK に対応している Box と Slack に対して、これを構成する。

また Box が提供する検索機能は、ファイルの内容をインデックスに登録する必要があることから、本目的を鑑みてインデックス機能を無効にするよう構成する。一方で Box における検索性を補完するため、検索に役立つ属性を登録したメタデータをフォルダ・ファイルに付与できるよう構成する。特にフォルダに対して配下のファイルやフォルダに指定したメタデータを再帰的に付与する構成としている。

なお Druva inSync は BYOK に対応しているが、侵害時の影響調査や内部犯の調査で利用する Enterprise Search 機能や e-Discovery 機能が利用できなくなることから、本事業では BYOK の適用を見送っている。

暗号鍵の管理

BYOK に用いる大元となる暗号鍵は、最終的にデータ復号に利用できることから厳重に管理する必要がある。また、当該の暗号鍵を利用者が参照する頻度は極めて低いものである。一方本事業において、当該の暗号鍵は組織の管理者がアクセス可能な場所に保管することが求められる。以上の条件を鑑みて、当該の暗号鍵は紙媒体として金庫で保管することが一定の合理性があるものと考えられる。

金庫の利用により、設置場所・コスト・省内に秘密情報が集中する状況が懸念される。そのためこれら懸念を鑑みて、当該の暗号鍵は銀行の貸金庫や組織内の金庫にすることが妥当であるという結論に達した。なお本運用は、期間的な問題から実施・検証には至っていない。

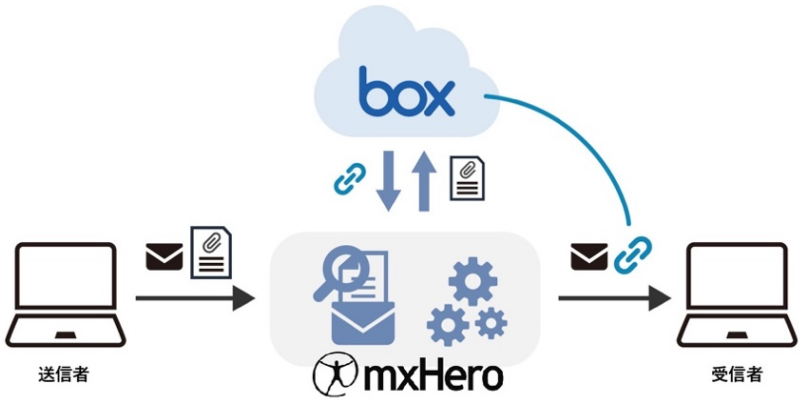
バックアップデータのアクセスコントロール

データ持ち出し経路の一つとして、バックアップデータへのアクセスがあることを忘れてはならない。本アーキテクチャでは、PC 上のユーザーデータは Druva inSync を用いてバックアップしている。そのためバックアップデータにアクセスできる環境は、組織のセキュリティ構成が配信されており、制御されている PC に限定する必要がある。

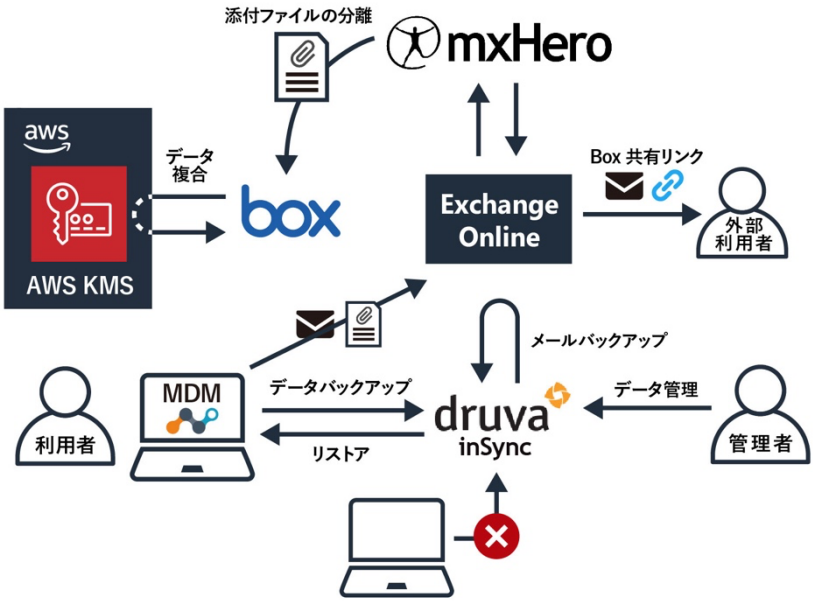
ユーザーは、ユーザー向け Web コンソールと inSync Agent 画面からバックアップデータにアクセスできる。そのためまず、Druva inSync のユーザー向け Web コンソールからのバックアップデータリストアやダウンロードを禁止し、inSync Agent からのアクセスに限定するよう構成する。また、inSync Agent の認証を IdP である Azure Active Directory を用いて SSO するよう構成し、その認証の条件として Microsoft Intune の登録と Netskope が稼働していること、および未対応のセキュリティリスクが残留していないことを Azure Active Directory 条件付きアクセスを用いて構成する。

一方で、Druva inSync で取得したバックアップデータのリストアやダウンロード操作は、定期レポートとして管理者に配信するよう構成することで、管理者によるバックアップデータへのアクセスについても制御できるようにした。

メールによる情報漏えいへの対応



外部とのファイルを用いたコラボレーションの基盤として、Box の外部共有フォルダを用意しているが、依然としてコミュニケーションの中心は当面の間メールとなることが予想される。また、メールにファイルを添付する操作に慣れている職員は、Box に格納したファイルへの URL や共有リンクの利用を即座に受け入れ対応するとは考えにくい。そのため、mxHero を用いて Exchange Online を経由する送受信メールに対して、添付ファイルを Box へ格納し、Box に格納したファイルへの URL に置き換えるよう構成した。 また、Box に格納したファイルへのアクセス権は、メール受信者のみ閲覧可能となるよう構成している。メール受信者は、Box アカウントやライセンスを保有している必要はなく、自身のメールアドレスをユーザーID とする、無料の独立アカウントを登録することで利用可能となるよう構成した。なお独立アカウントのパスワードは、強固な条件のものを強制するよう構成している。本構成により、添付ファイル付きメールを誤送信した場合であっても、管理者が Box に格納したファイルの共有設定を解除することで、情報漏えいの封じ込めを行える。また、管理者が Box に格納したファイルの共有設定を解除する以前のアクセス状況は、Box のアクセス記録にて、いつ・どのユーザーが閲覧・ダウンロードしたかを確認できる。



添付ファイル分離と S/MIME への対応

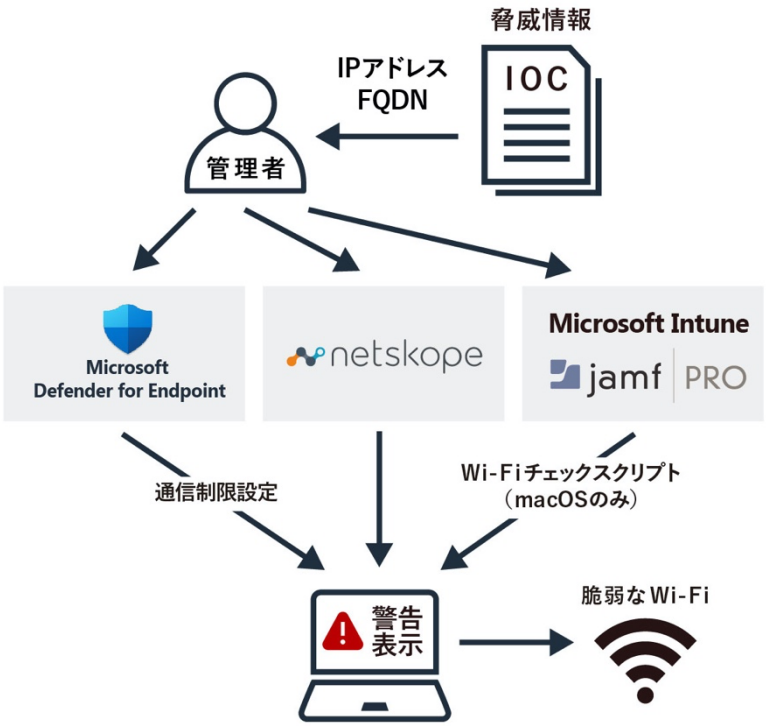
本事業では、メール送信時における S/MIME の利用は要件としては挙がらなかったが、mxHero を利用した環境での S/MIME 利用について言及する。mxHero は、S/MIME で署名・暗号化されたメールの添付ファイルについて、添付ファイルを分離する操作は行わない。そのため、メール送信前に添付ファイルを外部共有フォルダに格納し、ファイルの Box URL や共有リンクをメールに記載する必要がある。この操作を簡略化するために、mxHero for Outlook などのプラグインを利用できる。なお本事業では、検証期間の問題から mxHero for Outlook の利用検証は行わないこととした。

データガバナンスに係る検証結果

複数のクラウドサービスの組み合わせにより、データがどこにどのように保管されており、誰がどのようにアクセスしているかを記録し、客観的に説明可能な状態が維持できることを確認した。

■ ネットワークによる制限

本アーキテクチャのネットワークによる制限における設計と運用について以下に示す。



地理的に分散している業務環境におけるネットワーク制御

ネットワーク制御は、Microsoft Intune、Jamf Pro を用いて、OS のファイアウォール機能にて全ての受信を拒否する設定を構成する。IoC（Indicator of Compromise）情報にもとづく送信を制御する必要が生じた場合は、Microsoft Intune、Jamf Pro を用いて、OS のファイアウォール機能に送信先を指定しての拒否設定を行えるよう構成する。IoC が FQDN で提供された場合を考慮して、Netskope を用いて送信先を制御する構成としている。

脆弱な暗号化規格への対応

Wi-Fi の暗号化規格が古いなど、接続するネットワークが脆弱である場合、通信内容を傍受される可能性がある。Windows 10（1903）以降では、OS の機能として暗号化規格が WEP である Wi-Fi への接続に警告を表示できるため、これを用いて利用者に注意を促す方針とした。macOS については、Jamf Pro で取得した情報にもとづいて、警告を表示するスクリプトを配信することで、同様の挙動を実現する実装を行った。

ネットワーク制限に係る検証結果

脆弱なネットワークへの接続リスク対策として、ネットワーク制御や制限が可能であることを確認できた。

■ BYOD

本アーキテクチャの BYOD における設計と運用について以下に示す。

BYOD 端末におけるプライベート領域の侵食に対する配慮

BYOD 端末のプライベート領域への侵食を可能な限り配慮する目的で、各プラットフォームにおいて、以下の構成を実装する。

Windows10 環境

端末は、Azure Active Directory Join を用いて組織の MDM で管理し、ユーザープロファイルを別途作成するよう構成する。組織で制御する端末の設定は、ユーザープロファイル上に構成されるため、個人利用のプロファイルに対しての監査は可能な限り行わないよう配慮している。また Netskope をマルチユーザーモードで配信することで、個人利用のプロファイルにおいて、Web トラフィックを監査しないよう構成している。

macOS 環境

端末は、Jamf Connect を用いて組織の MDM に接続し、ユーザープロファイルを別途作成するよう構成した。組織で制御する端末の設定は、ユーザープロファイル上に構成されるため、個人利用のプロファイルに対しての監査は可能な限り行わないよう配慮している。また Netskope をマルチユーザーモードで配信することで、個人利用のプロファイルにおいて、Web トラフィックを監査しないよう構成できる。

本事業では、期間的な問題から Netskope をシングルユーザーモードで配信している。実際に BYOD 端末を用いて業務する際は、Netskope をマルチユーザーモードで配信するよう構成されたい。

iOS、iPadOS

端末は、Jamf Pro を用いて組織の MDM で管理し、端末ローカルや個人所有のアプリケーションに組織のデータのコピーやダウンロードを制御する MAM アプリケーションや、同様の制御機能を有するアプリケーションを配布する。本事業において、組織で利用する iOS、iPadOS アプリケーションを以下に示す。

MAM アプリケーション

- Box for EMM
- Skype for Business
- Microsoft Excel
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Word
- Microsoft Office
- Microsoft OneNote
- Microsoft SharePoint
- Microsoft OneDrive
- Microsoft Teams
- Microsoft To-Do

MAM アプリケーションと同等の制御を可能とするアプリケーション

- Slack for EMM

本事業では、検証期間の問題から、Jamf Pro を用いたユーザープロファイルの分離に係る検証は行っていない。事業で取り扱うデータが MAM アプリケーション内で完結しない場合を考慮して、Jamf Pro を用いたユーザープロファイルの分離を検証する余地は十分にある。

Android 環境

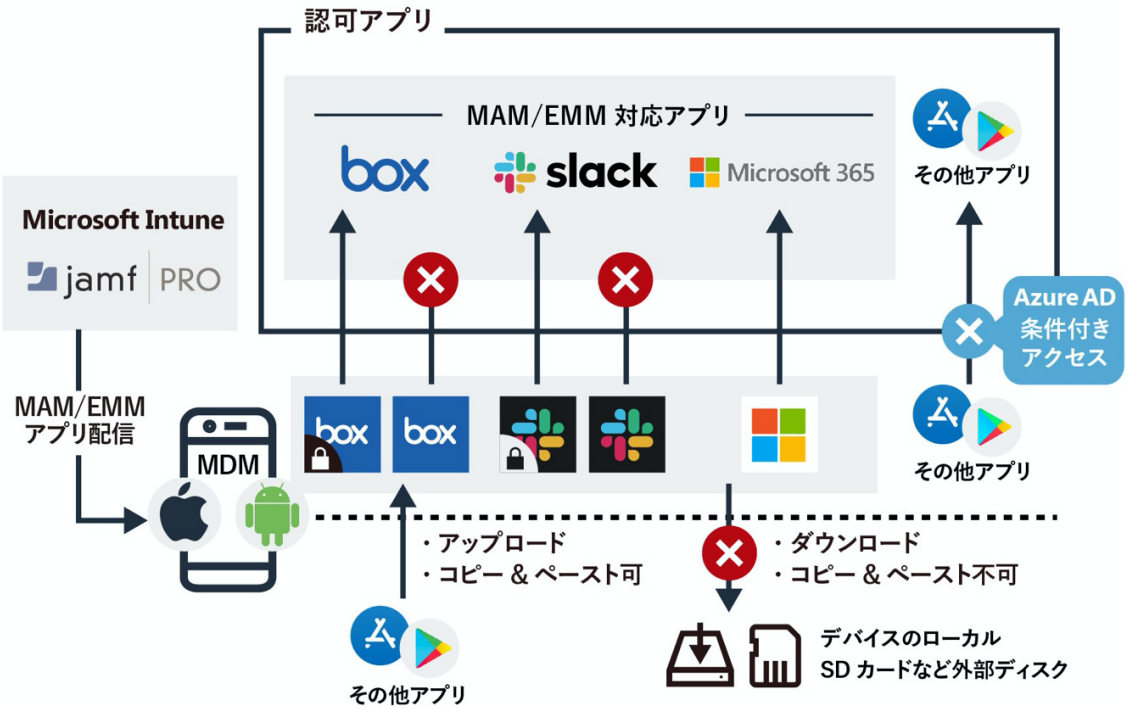
端末は、Microsoft Intune を用いて組織の MDM で管理し、端末ローカルや個人所有のアプリケーションに組織のデータのコピーやダウンロードを制御する MAM アプリケーションや、同様の制御機能を有するアプリケーションを配布する。本事業において、組織で利用する Android アプリケーションを以下に示す。

MAM アプリケーション

- Box
- Microsoft Excel
- Skype for Business
- Microsoft Office
- Microsoft Office [HL]
- Microsoft Office [ROW]
- Microsoft OneNote
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Word
- Microsoft SharePoint
- Microsoft OneDrive
- Microsoft Teams
- Microsoft To-Do

MAM アプリケーションと同等の制御を可能とするアプリケーション

- Slack for EMM



本事業では、iOS、iPadOS と同じ制御レベルとする目的で、仕事用プロファイルを用いた検証は行っていない。iOS、iPadOS の Jamf Pro を用いたユーザープロファイル分離の検証結果次第では、仕事用プロファイルを用いた構成を採用する余地は十分にある。

BYOD で利用する端末

BYOD で利用する端末は、『BYOD ポリシー雛形』を参照すること

BYOD 端末で行える業務の規定

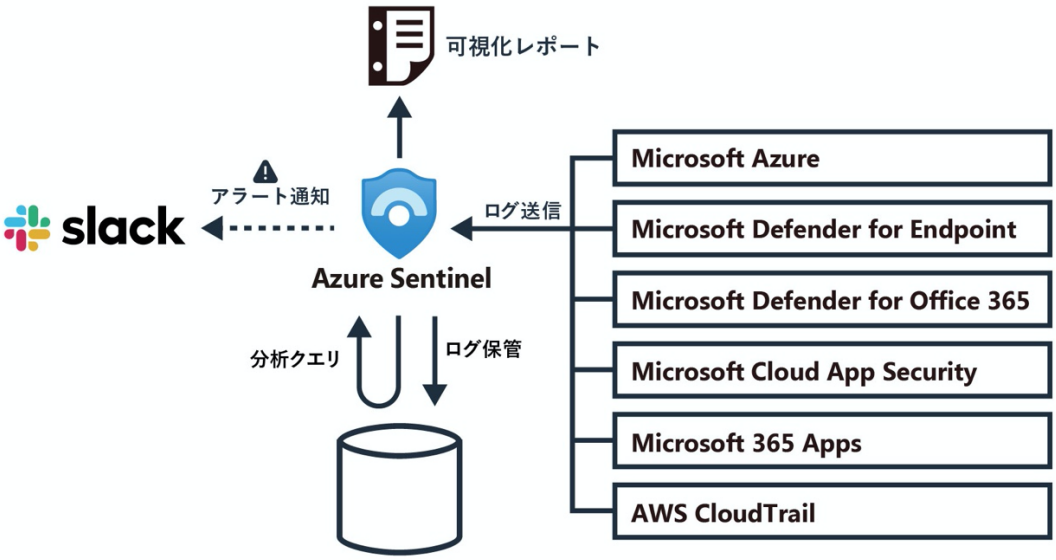
本事業では、BYOD 端末で行える業務は、機密性 3 に該当しないデータを取り扱う業務としている。Netskope の DLP 機能を用いて、SaaS や Web に流通するデータを監査し、機密性 3 に該当するデータを識別し、その流通をブロックするよう構成する。また機密性 2 に該当するデータについては、Netskope 側でその流通を検出し、記録するよう構成する。

BYOD に係る検証結果

BYOD 端末のプライベート領域への侵食を可能な限り配慮しながら、機密データへのアクセスを検知・制限する方法について確認ができた。

■ SIEM

本アーキテクチャにおける、SIEM の設計と運用について以下に示す。



データソースの繋ぎこみ

インシデント間の関連性の可視化を実現するために、以下のサービスから Azure Sentinel にログやセキュリティイベントを集約し、相関分析をできるよう構成した。これらのデータソースから Azure Sentinel への繋ぎ込みは、Azure Sentinel が標準で備えているコネクタを用いて実装している。

Azure

- Azure Active Directory 認証ログ
- アクティビティログ（サブスクリプションレベル）
- Azure Identity Protection ログ

Microsoft Defender for Endpoint

- インシデント情報
- EDR センサーログ

Microsoft Defender for Office 365

- インシデント情報

Microsoft Cloud App Security

- インシデント情報

Office 365

- Exchange アクティビティログ
- SharePoint アクティビティログ
- Teams アクティビティログ

Amazon Web Services（以下、AWS）

- CloudTrail ログ

なお Box と Netskope のログは、API を用いて Azure Sentinel に集約可能であったが、実装する基盤（AWS Lambda）の AWS 環境調達と費用確定に要する調整期間が本事業の期間と折り合わなかったことから、実装を見送っている。

分析クエリーの設定

集約したログを相関分析するために、Azure Sentinel がデフォルトで備えているクエリーのうち、本アーキテクチャで使用する各製品に対応したものを有効化する。特に、Microsoft 製品内での相関分析に留まらず、Microsoft 製品と他製品との相関分析を実証するために、AWS 環境のログ(CloudTrail)との相関分析を行うクエリーテンプレートが利用可能なように構成している。

各クエリーの実行間隔は、クエリーの性質とクラウドの特性を鑑みて 1 時間～24 時間間隔で実行するよう構成している。

クエリーの性質は、アラートなどの単発での応答を要するものと、複数のデータソースをある程度のスパンで集計した結果を相関分析するものに区別される。

クラウドの特性とは、クラウドサービスのログは必ずしもリアルタイムで発行・収集されるものではないというものである。一概に断定はできないが、実際に行われた操作から 10～15 分程度、クラウドサービスの稼働状況によっては更に遅れたタイミングでコンソールでの確認やクエリーの実行が可能な状態となるサービスもある。セキュリティイベント管理システムへの転送は、一定間隔で行われることを鑑みると、ログの発行から集約までの時間は、最低でも 30 分～1 時間を見込んでおく必要がある。単一のデータソースで 1 時間程度の遅れがあることを鑑みると、複数のデータソースのログを相関分析する上では更に多くのリードタイムを見込んでおく必要がある。

以上を踏まえてクエリーの実行間隔を決定した。

自動対応の設定

分析クエリーの検知結果にもとづいて、Azure Logic App で自動応答機能を構成する。自動応答機能は、検出したクエリーの内容を Slack に通知するものをはじめに構成し、通知された内容やアラートの発生状況の傾向を鑑みて、個別の自動応答機能を構成する方針とする。本事業では、個別の自動応答機能として、人に紐付かない緊急用ユーザーの利用を Slack に通知するよう構成した。

なお Slack に通知する内容は、複数の検知でも流れにくくするよう、以下 3 項目に絞るよう構成している。

- 分析クエリー名
- 重要度
- アラート一覧へのリンク

検証に参加した利用者が少なかったこと、検証期間が限られていたことから、運用を簡易化する必要が生じるほどの検知は見受けられず、個別の自動応答機能を構成するには至っていない。

可視化テンプレートの設定

収集したログからアクティビティを可視化するテンプレートを構成した。

可視化した内容は以下のとおりである。

Azure Active Directory 監査ログ

- ユーザー操作にもとづく API の発行状況と API のカテゴリランキング
- アクティビティが多いユーザー
- API の成功、失敗のトレンド

Azure Active Directory 監査、アクティビティ、サインインログ

- ログイン失敗理由の比率
- ログインタイプの変動推移
- ログインが成功したロケーションのランキング
- ログインが成功したアプリケーションのランキング
- API の種類毎の成功レートとトレンド
- API の種類毎の失敗レートとトレンド
- 直近の監査ログ
- Azure 上でのオペレーション内容のレートとトレンド

Azure Active Directory サインインログ

- サインインの国別ランキングとトレンド
- サインインのデバイス種別ランキングとトレンド
- 直近のサインインの動向
- 条件付きアクセスの成功・失敗の動向
- 条件付きアクセス失敗に係るエラー内容の動向

Exchange Online

- ユーザーアクティビティの時系列データ
- ユーザーアクティビティの一覧
- 管理者操作の比率
- 外部からの不審な操作の発生状況
- ユーザーによる手動削除の発生状況
- メールボックスに係る操作の発生状況

セキュリティイベントログ

- ユーザーログイン動向
- デバイスログイン動向
- セキュリティイベントログの一覧
- ログインタイプランキング

セキュリティ通知

- 重要度別発生件数
- セキュリティアラート発行元ランキングとトレンド
- セキュリティアラート発行の時系列データ
- セキュリティアラート発行元 IP アドレスのランキング
- セキュリティアラート発生元タイプの比率

データ収集の正常性監視

- データソースからのログ流入量ランキング
- ログ流入量の時系列データ
- 秒間データ件数ランキング
- 最後のデータ受信から期間が経っているデータソースランキング

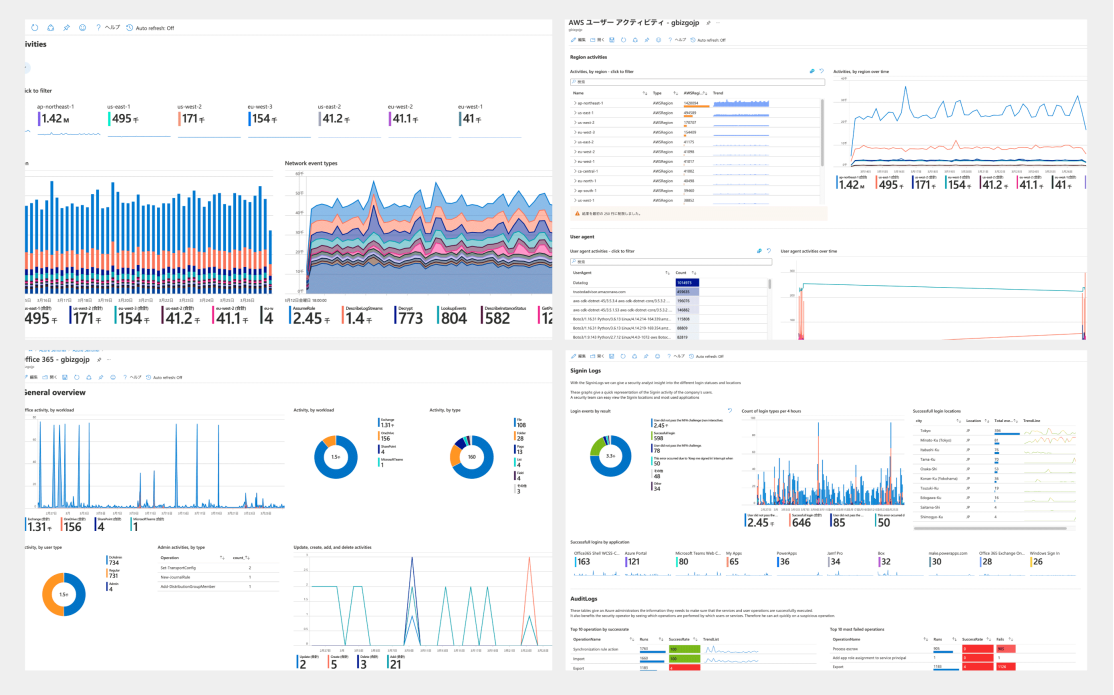
AWS ユーザーアクティビティ

- サインインイベントの発生推移
- サインインの成功・失敗のトレンド
- コンソールや API による操作の比率
- AWS アカウント毎のユーザーアクティビティの動向
- リージョンごとの API 発行状況
- コンソール操作や API 発行元の User Agent のランキングと発行トレンド

AWS ネットワークアクティビティ

- リージョンごとのネットワーク流量
- API の発行ランキング
- ネットワークリソースの作成・削除イベントの一覧
- セキュリティグループとネットワーク ACL の変更イベントの一覧

本来であれば、ログ収集の目的やログ収集を通じて成したいこと、説明責任にもとづいて可視化を設計するが、事業の期間を鑑みて Azure Sentinel がデフォルトで備えるテンプレートを用いてログの可視化を構成している。



SIEM に係る検証結果

各種クラウドサービスから出力されるログとその相関分析ができ、個別に連携すべきアラートについては、Slack 等を経由して通知を受け取ることが可能であることを確認できた。

2 - 3 . 本アーキテクチャ構築に係る提言

本事業では、DX オフィスが目指す構想を具現化する取り組みを行ってきた。本事業の遂行を通じて、行政組織がクラウドファーストの原則に則って、モダンかつセキュアな業務インフラを構成する上で見出した現状のギャップと、これから議論されるべき観点を提言としてまとめる。

2-3-1 . 行政組織におけるクラウドサービスの契約の課題

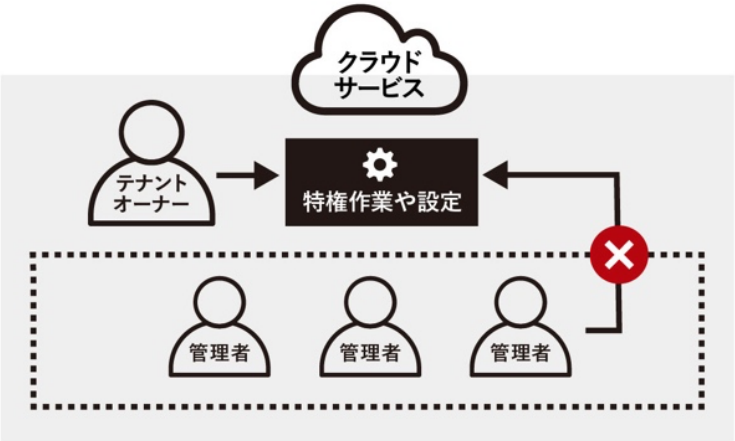
本事業を遂行するにあたり、さまざまなクラウドサービスを契約している。その際に直面した課題を以下に示す。

（1）クラウドサービス契約におけるテナントオーナーと管理者の分離の課題

（2）クラウドサービス利用料の支払方法と賦課の課題

（3）従量課金の予算化の課題

（1）クラウドサービス契約におけるテナントオーナーと管理者の分離の課題



課題

クラウドサービス契約の際に、テナントオーナーとして管理者を登録する必要がある。
しかし、管理者とテナントオーナーに求められる要件・操作については、必ずしも一致するものではない。

管理者は、クラウドサービスの利用規約の確認を求められることから、システムの責任者として行政側の担当者を登録することが望ましい。

一方でテナントオーナーは、クラウドサービスのテナントを開設する際にメール送付される初期認証情報を受信し、クラウドサービスの環境設定を行う関係者を登録する必要がある。

またクラウドサービスの種類によっては、テナントオーナーのみが管理者権限でも操作できない設定が許可されているものも存在する。

そのためテナントオーナーと管理者が同一である場合、クラウドサービス操作に係る知識や慣れが要求される操作についても、非技術者である行政の担当者がそれを担う場面が予想され、困難なケースがあると想定される。

また別の観点で、行政の担当者は一定期間で異動するため、クラウドサービスに対する重要な権限をもつユーザーの移管業務が定常的に発生することも忘れてはならない。

提言

本課題に対して、クラウドサービス事業者は、利用許諾を承認する担当者（管理者）とテナント上の特権作業を担う担当者（テナントオーナー）を分けて登録可能とする方式をオプションとして用意する余地がある。

上記方式であれば、利用許諾の承認をもって、テナント上の特権作業をおこなう担当者に接続情報を送信する構成が考えられる。非技術者である行政の担当者は、システムの責任を負うという本来の責任範囲で利用許諾の承認行為を行うことができ、特権作業は受託ベンダーの担当者で速やかに実施できるものと考える。

（2）クラウドサービス利用料の支払方法と賦課の課題

課題

クラウドサービス契約の際に、支払方法としてクレジットカード情報の登録を要するものが多く存在する。

事業単位でクラウドサービスを提供する場合、応札事業者のクレジットカードを登録し、クラウドサービスで発生する課金をクレジットカードにて、応札した予算の範囲内において決済する。

しかし、事業を横断するプラットフォームの場合、行政組織はクレジットカードを所有しないため、事業単位同様に応札事業者のクレジットカードを登録せざるを得ないが、どの事業者のカードを登録するかが判然としない問題が生じる。

また、各事業で発生する費用の按分と賦課を行うための方式が確立されていないため、クレジットカードを登録した事業者が費用を回収しきれない可能性が考えられる。

現時点では、事業毎にクラウドサービスのテナントを個別で用意する方式以外に選択肢がなく、結果としてクラウドサービスのテナントを個別調達する形となるため、構築作業などにおいても、既存テナントについて実施済みの作業をテナントごとに都度再実施する必要がある。

提言

本課題に対して、クラウドサービス事業者は、テナント内のリソースから生じる課金を任意のサブスクリプションに割り当てる方式を、オプションで用意する余地がある。

サブスクリプションに対して各事業のクレジットカードをそれぞれ登録することで、各事業の応札事業者は、サブスクリプションに紐づくリソースに対しての課金額のみを支払うことが可能になると考えられる。

このような方式は、Microsoft Azure のリソース管理と課金方式が参考となる。

一方で、クラウドサービスのテナントを管理する担当者に負担が集中しないよう、事業および応札事業者間での利害を調整する枠組みについて議論する必要がある。

なお本提言に関連する報告が、内閣官房と総務省より「第二期政府共通プラットフォームにおけるクラウドサービス調達とその契約に係る報告書」として報告されている。

詳細は以下 URL を参照すること。

https://cio.go.jp/node/2704

（3）従量課金の予算化の課題

課題

クラウドサービスの多くは従量課金モデルであるため、まだ実装されていないシステムの利用金額を予想することは難しい。

クラウドサービスは、迅速に小さく利用を開始し、事業のスケールに伴って利用を拡大していくことに最大の利点がある。

そのためシステムや予算のサイジングに時間や労力を要する状況は、本来期待できる効果が得られない状況と言える。

クラウドファーストの原則に則って、行政における事業にクラウドサービスの利用を促進する上で、本課題は重大な問題である。

提言

本課題に対して、行政は、調達の際に一括で予算の確定を求めるのではなく、一定期間のテストドライブの結果に基づいた補正予算の申請を許容する方式を検討する余地がある。

入札は、テストドライブ期間中の予算と技術点・提案点・課題実現点で評価し、テストドライブ中の予算に対して一定の係数を掛けた値を上限に補正予算の申請を許容することで、入札者のリスクやサイジングに伴う工数をある程度コントロール可能できるものと考える。

2-3-2 . エンタイトルメント管理

本事業においては、ユーザーアカウントの管理は Azure Active Directory のみで実施している。Azure Active Directory は大規模な組織の利用を前提とした機能をもっている。しかし組織の人事情報との連携、組織上の役割と各種システムに対するアカウントの権限の割り当てなど、エンタイトルメント管理に課題がある。

課題

本アーキテクチャにおいて、人事システムとクラウドの認証基盤は、連携する仕組みが整備されていないのが現状である。人事による職員の所属や職掌の情報から、認証基盤やクラウド・オンプレミスの各種サービスのアカウントに対して連携する、いわゆるライフサイクル管理は標準化が不十分である。

認証基盤から各種サービスに連携するためのプロトコルとして SCIM が存在する。SCIM によるアカウントの作成、更新、削除は可能でも、適切な権限のライフサイクル管理まで可能なクラウドサービスは少ない。SCIM には未対応でも、独自の API を使うことで管理できるケースがあるが、クラウドサービスごとに機能の実装が個別で必要になる。

API を使った管理ができないクラウドサービスもいまだ多く、そのようなクラウドサービスは管理者による手作業での対応が必要になるため、管理コストが増大する傾向にある。

提言

クラウドサービスを中心に利用する本アーキテクチャでは、システム間連系が重要であるため、連携が容易でないクラウドサービスを選定しないことが重要である。また、利用が避けられないクラウドサービスに対しては、連携が容易になるように、API を整備することなど改善するように要求することが望ましい。

なおエンタイトルメント管理の分野は未成熟であり、認証基盤のエンタイトルメント管理機能の充実だけでなく、アイデンティティ制御を専門に行うシステムやサービス自体の拡充を期待したい。

2-3-3 . シークレットの管理

本事業において、BYOK で利用する暗号鍵（秘密鍵）の管理方法について検討した際に、いまだ最適解がなく、多くの課題が明らかとなった。以下は暗号鍵のみならず、職員が利用するパスワードも含め、秘密にするべきデジタルデータのことを、ここではシークレットと表現し記述する。

組織または個人が管理するべきシークレットには、用途に応じて以下の 3 つに分類できる。

（1）システム管理者を除く行政側業務従事者が日常業務で利用するシークレット

（2）システム管理者が管理業務で利用するシークレット

（3）システム管理者が緊急時に利用するシークレット

（1）システム管理者を除く行政側業務従事者が日常業務で利用するシークレット

日常業務に利用する、管理権限を持たないユーザーのアカウントの認証情報など、重要性が高くなく、利用頻度が多いものが対象となる。

課題

現状は、各個人がもつシークレットを管理する方法が確立されていない。主なシークレットであるパスワードの管理は、暗号化されていないテキストファイルに記録して端末内への保存や、手書きのメモに記録などといった、安全性の低い手法によって管理されている。

提言

個々人がもつシークレットを管理するには、いわゆるパスワードマネージャを使うのが望ましい。パスワードマネージャは、パスワードなどのシークレットを暗号化して保管・共有する機能を有する。

また、システム全体として可能な限りパスワードを減らす方向に向かうべきであり、例えばパスワードを使わない認証方式である、パスワードレス認証の使用を推奨する。

パスワードレス認証のために、職員に FIDO 2.0 に対応したセキュリティキーを配布するのが望ましい。少なくとも、管理職以上の役職者はセキュリティキーを必須にすることを推奨する。

（2）システム管理者が管理業務で利用するシークレット

システムの管理業務上必要になる大きな権限をもつアカウントの認証情報など、日常業務では利用しないが、重要性が高く、複数人での共有が必要かつ利用頻度が大きいものが対象となる。

課題

システム管理者は重要な役割であるため、管理者が存在しない状態はリスクである。そのため必ず複数人をもってその任に当たるべきであるが、システムによっては、最上位権限をもつアカウントを複数作成できない場合がある。その場合は、最上位権限をもつアカウントを個人に関連付けるのではなく、システム管理者間で共有するアカウントとして設定し、共有アカウントの認証情報をシステム管理者間で共有する必要がある。

提言

認証情報のようなシークレットを共有するには、シークレットを安全に共有する機能を有するパスワードマネージャを利用する。ただしシークレットを共有すると、そのシークレットが漏えいするリスクが人数に比例して高まる。そのため対策として、個々のシークレットに対するアクセスのログの記録、シークレットの不正利用の検出、シークレットを利用する際の承認を必須にするためのワークフローなどの機能が利用できる必要がある。

またシステム管理者の増減により、シークレットの共有範囲が変わる際には、共有しているシークレットを変更する運用を定義する必要がある。

加えて、シークレットを共有しなければならない状況そのものを回避するため、利用するクラウドサービスについては、最上位権限を複数のアカウントに付与できるものを選定することが望ましい。

その他、認証システムは、このようなユースケースのための共有アカウントを利用する際に、シークレットを共有することなくアカウントを利用できる代理認証のような仕組みをもっていることが望ましい。

（3）システム管理者が緊急時に利用するシークレット

BYOK で使う秘密鍵（暗号鍵）や、緊急アクセス用管理アカウントの認証情報など、通常業務では利用せず、緊急時にのみ必要となるものが対象となる。

課題

通常業務で利用せず、かつ重要性や緊急性が高いシークレットは、広義の行政文書に当たると考えられる。しかし現在はこのような情報を管理する適切な仕組みが存在しない。

提言

本アーキテクチャでは、紙媒体に記録して銀行の貸金庫や組織内の金庫に暗号鍵を保管する手法を検討した。このような情報を保管する仕組み、管理プロセスについては、法整備が必要である。

暗号鍵は非常に重要な情報であるため、適切なアクセスコントロールと継続した保管を前提とした機構が必要である。また緊急時の利用が想定されるため、適切な権限をもつ利用者が、利用の申請と承認、情報の取得が迅速に行える仕組みであるべきである。同時に、災害時などに情報が失われないように、分散保存をする必要がある。

2-3-4 . Box KeySafe の実装に係る手続き

課題

Box KeySafe は、Box のデータを利用者が用意した鍵を用いて暗号化するものである。

Box KeySafe の設定は、Box テナント内の緻密な設定変更や調整が伴うため、Box 社のエンジニアによるコンサルティング支援を受ける必要がある。

また Box テナントの所有者は、暗号鍵をホストする環境を AWS 上に作成する必要があり、用意した環境の情報を Box 社に引き渡すなどの調整を行う必要がある。

本事業では、これらの調整や課題解決に多くの時間を要する状況が見て取れた。

まず Box KeySafe の契約関連の調整完了後、Box 社のエンジニアのアサインまで 1 ヶ月を要した。

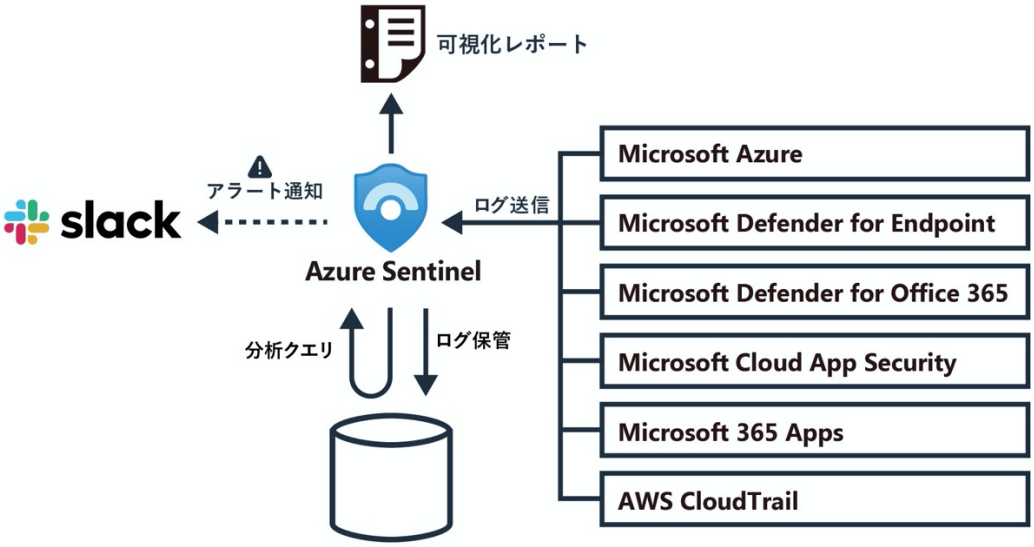
アサイン後のやり取り一つひとつの応対に 5 営業日以上の待ち時間が発生するなど、コミュニケーション面での時間的なオーバーヘッドが多く見受けられた。

これらにより最終的に、Box KeySafe の契約から実装完了までに約 3 ヶ月を費やした。

提言

Box KeySafe を採用する応札事業者は、十分な時間的余裕をもって実装スケジュールを組むことが求められる。

2-3-5 . アラート対応自動化の実装最適化



課題

本事業では、Microsoft Azure Sentinel を用いて、SIEM 機能で本来行うべきログ集約と相関分析機能の実装に加えて、各種セキュリティ機構のアラートの集約と通知機構の実装を行っている。

また Microsoft Azure Sentinel は自動化機能を有しており、定型的な初期調査や暫定処置など、アラートの内容に応じた作り込みを行うことが可能である。

一方でアラートの検出傾向は、システムを利用する組織の運用方式やデータの取り扱い方式などの運用状況に左右されるため、運用開始前に行える一般的な自動化機能の実装の最適化は極めて限定的である。

例えば構築期間と運用開始期間に比較的開きがある場合では、先んじて作り込みを行うケースが考えられるが、アラートの調査の仕方は扱うシステムによって異なるため、利便性の向上に繋がらない、いわゆる“的外れな実装”になることが予想される。

そのため従来のウォーターフォール型の開発モデルでは、システムの特性や利用状況に則した効果的な自動化機能の実装最適化を行うことが非常に難しい。

提言

構築期間中に行う SIEM 機能の自動対応についての実装最適化は最低限に留め、運用開始後にアラートの検出傾向と調査方式を鑑みた上で順次行っていくことが、有効かつ効率的な実装の最適化を行う上で必要となる。

加えて、実装の最適化を実施する事業者とアラート対応や調査を行う事業者が異なる場合、実装の最適化を実施する事業者の担当者は、アラート対応を実施する事業者の担当者の調査対応プロセスを観察し、調査対応を行うオペレーションや利用者とのコミュニケーションを簡略化するアプローチで実装の最適化を行うことが望ましい。また、アラート対応を実施する事業者の担当者は、実装の最適化を実施する担当者に対して、実装されたシステムの最適化を、利用した結果としてフィードバックし、運用利便性を継続的に向上させていくことが求められる。

上記のように、継続的な開発・改善プロセスを行う必要があることから、開発モデルはアジャイル方式を用いることが望ましい。

そのため調達仕様を作成する行政の担当者は、運用期間中に継続的な開発と改善を無理なく実施できるよう、調達仕様の記載に留意することが求められる。

3. プロジェクト管理等に関するツールの調査・分析と効率化手法のための導入実証

3 - 1 . 概要

本事業では、職員の業務効率化やシステム開発等のプロジェクトの標準化・最適化を進めるため、各種ツールの導入の実証を行うとともに、より効果的にこれらのデジタルツールを活用していくために必要となる管理のあり方について検討を行った。

その上で上記目的を達成するため以下のとおり、DX オフィス関連プロジェクト管理業務等の効率化に資するツールおよびツール管理のためのサービスについて、機能・性能、セキュリティ、移行性、規格等について、調査・分析し、効率化に資するツールの導入実証を行った。

本章に記載する各ツールの選定と評価は、特定のツールの利用を強制するものではない。ツールの選定は、事業に携わる事業者が事業の特性を鑑みた上で行われるべきである。本章の内容は、事業者がツールの選定を行う上での参考とされたい。

3 - 2 . 各ツールの調達意図

3-2-1 . 品質管理・タスク管理ツール

本事業で使用する品質管理・タスク管理ツールは、以下の要件を満たす必要がある。

- Web ブラウザおよびモバイルクライアントで利用可能
- カンバン形式でタスクを管理できる
- 認証・認可の連携が可能
- 他サービスとの連携が可能（最低限 Webhook が利用可能）
- コミュニケーションツールとの親和性が高い

当室では現在、扱う情報の機密性について十分に考慮した上で Trello を試用しているが、同様にカンバン形式でタスクを管理できる、スクラムのフレームワークを標準的に採用したツールの採用が好ましい。

またプロジェクトマネジメントを進めていく中では、プロジェクトで取り扱う各種データの統計分析を行う必要がある。

そのためプロジェクトマネジメントを行う担当者およびプロジェクト参加者自身が、簡易に統計分析を行える環境が望ましい。

3-2-2 . サービスデスクツール

各種補助金についての FAQ サイトなど、問い合わせ対応を主とした委託事業の運用時、チケット管理ができ、かつ他サービスと連携が容易であるサービスデスクツールが必要である。

その他個別の委託事業内において、Redmine などのチケット管理システムを利用している例があるが、更に汎用的に運用全般に活用でき、多くのプロジェクトで利用できることが必要である。

3-2-3 . パフォーマンス計測ツール

運用時におけるプロダクトのパフォーマンス計測等で、リアルタイムにサービス稼働状況を可視化でき、委託事業者と円滑なコミュニケーションを容易にするシステムが必要である。

個別の委託事業内において、ログ等を収集し毎月定期的な報告を受けている例があるが、迅速なサービス改善につなげるため、リアルタイムでの状態把握や分析、KPI の達成状況をダッシュボード化し、多くのプロジェクトで利用できることが求められる。

3-2-4 . クラウド設定管理ツール（Cloud Security Posture Management）

クラウドサービス（特に IaaS、PaaS）を利用する場合、設定不備に起因する事故の発生リスクを低減するため、脆弱な設定を自動検出しセキュリティ上の懸念に対処することが望ましい。

継続的なリアルタイム監視と自動修復によるクラウドガバナンス、セキュリティ、コンプライアンス強化のツールを多くのプロジェクトで利用できる必要がある。

3-2-5 . ソース管理ツール

成果物を Web サイトやリポジトリで公開するだけでなく、フィードバックやイシューなどの改善要望の受付機能も必要である。

3-2-6 . ドキュメント管理ツール

各種コミュニケーションツール（メール、ショートメッセージ、その他）に情報が分散する中、重要なドキュメントは最新の状態のものを 1 か所に集約して適切に管理する必要があり、そのためにはクラウド対応ドキュメント管理ツールが必要である。

適切に暗号化およびアクセス権を管理でき、かつ編集権限のある複数人で同時に編集できる機能が必要となる。

3-2-7 . コミュニケーション管理ツール

通知先を一箇所に集約することで運用コストを低減するべく、本事業で利用が想定される全てのツールの通知先として、連携が可能なコミュニケーション管理ツールが必要である。

3-2-8 . 統合プロジェクト管理ツール

プロジェクトを円滑に進めるためにはプロジェクト全体を見通し、管理を容易にするためのシステムが必要である。プロジェクト登録やタスクの登録・管理、ファイル共有、スケジュール・ガントチャートなどの表示などの機能を有するツールが求められる。

3-2-9 . アクセス解析

WEB サイトとして提供しているプロダクトについて、アクセス状況や処理状況を可視化・分析でき、レポーティングのために適宜必要な項目について抽出したダッシュボードを作成できるシステムが必要である。

円滑なコミュニケーションを容易にするために、関係者の閲覧に供する可能性があるため、単体で一定のアクセス制御を備えている必要がある。同時に機能において汎用的であり、かつ安価である必要がある。

3 - 3 . 各ツールグループ名と対応する検証実施サービス群

前節で挙げた要件を満たすツールとして選定した検証対象の製品は、以下の表の通り。

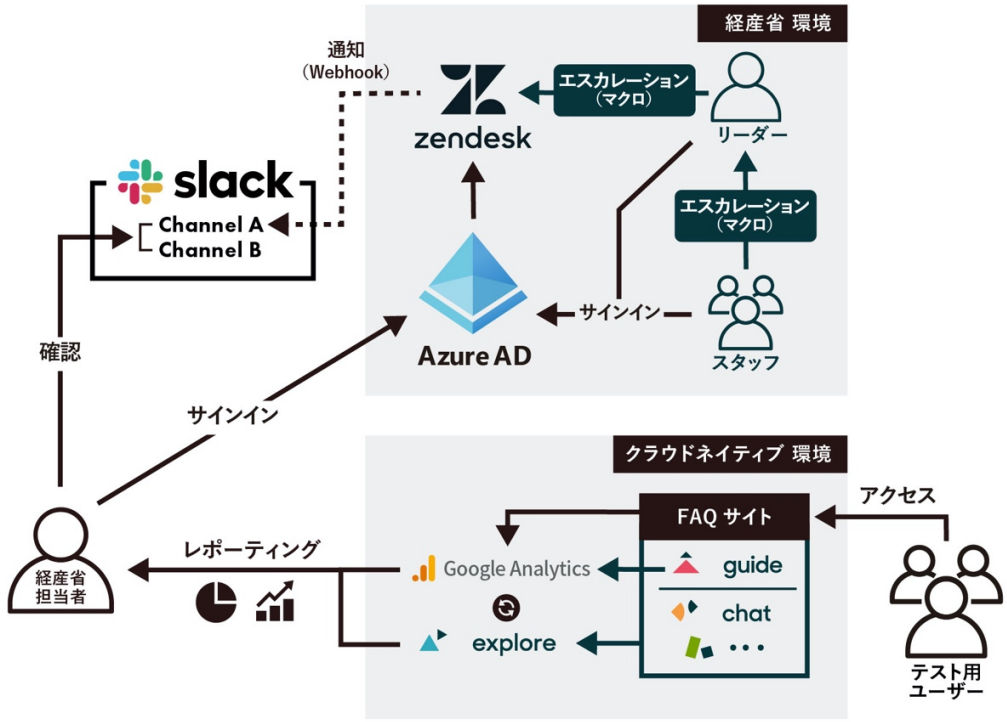
ツール	製品	社名
品質管理・タスク管理ツール	Backlog	ヌーラボ
サービスデスクツール	Zendesk を中核としたサービス群	Zendesk
クラウド設定管理ツール（CSPM）	CloudGuard Dome9	Dome9 Security
パフォーマンス計測ツール	Datadog	Datadog
ソースコード管理ツール	GitHub Enterprise Cloud	GitHub
コミュニケーション管理ツール	Slack Enterprise Grid	Slack

3 - 4 . 検証実施サービス群各論

本節では、各サービス群の構成、選定理由、構成上の注力点、検証実施内容および検証結果について述べる。

3-4-1 . Zendesk を中核としたサービス群

■ 1.製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である以下の 4 点を必須要件とした。

- チケット管理機能を有する
- 他サービスと連携が容易である
- 汎用的に運用全般に用いることができる
- 多くのプロジェクトで利用できる

加えて、事業の性質上要求されると考えられるセキュリティやガバナンスのほか、サービスベンダー自体の事業継続性にも着目した。また、現在各種 FAQ サイトの問い合わせ対応については委託事業として実施していることを踏まえ、以下の 4 点についても勘案した。

- 受託事業者と委託側担当者のリレーション
- 受託事業者システムが将来的に移行した場合の負荷の程度
- 委託側での効果測定が容易であること
- 知見の再利用という点でも汎用的であること

さらに、問い合わせ対応に付随して考慮点となる、ナレッジの集積・問い合わせ対応の効率化についても勘案した。効率化の視点としては、定型業務のワンクリック化、AI の利活用による無人対応やチャット機能での夜間対応の少人数化、ナレッジ導線の簡略化など、自動化・省力化を志向したほか、電話での問い合わせ対応などの問い合わせ者と対応者が 1 対 1 で同じ時間拘束されてしまう業務についても現状の踏襲ではなくいかにして効率的な他の方法で代替していくかという観点に注意を払った。

またこれらの効率化は、問い合わせ対応に要する人員数の削減にも必然的に寄与するため、広義のコスト削減策としても機能すると思われる。

具体的には以下の機能を有するかを考慮点とした。

- 委託事業の内容が問い合わせ対応であることから、チケット管理、関連製品利用基盤としての管理機能、および問い合わせ対応フローの省力化機能
- 問い合わせについて、国民の自己解決を促進するためのナレッジ集積・管理機能
- 通話対応と遜色のない品質の対応が可能なチャット対応機能
- 上記ナレッジおよびチャット機能の効率化を支援する AI を利活用したサジェスト機能
- サービス群内部の対応時間平均や、AI サジェストによる問い合わせ件数削減効果などの集計・レポート機能

加えて、製品自体のヘルプが充実していること、知見が比較的巷間に豊富であることから、受託事業者が現在のシステムから今回の検証製品に将来的に移行した場合の負荷についても比較的低いであろうことも想像された。

ほか、利用対象プロジェクトの汎用性の観点および、委託事業ごとのシステム構成についても可能な限り標準化を図り、知見の汎用性を高める意図から、以下のような製品は選定対象から除外した。

- IT サービスマネジメントに特化した製品
- チケット管理のみを提供する製品など、他社製品との連携が可能というレベルを超え、他社製品に依存することを前提とした製品
- 他製品と比較して国内シェアが著しく低い製品

また事業継続性を推し量る指標として、採用事業者数を確認した。結果、機能の充足に加え、世界約 14 万 5,000 社、国内 2,500 社にて採用実績のある、Zendesk 製品を中核としたサービス群をサービスデスクツールの検証対象として選定した。

サービス群内の具体的な製品は以下である。

製品	機能
Support	チケット管理およびグループ製品の利用基盤
Guide	ナレッジサイトの設置
Chat	チャットによる問い合わせ受付
Answer bot	AI サジェスチョン
Explore	チケット処理状況などのダッシュボード化

（2）注記

Zendesk サービス群には、調達意図に対して有用と思われる関連製品である「Talk（コールセンター機能）」と「ソーシャルメッセージングアドオン（SNS を問い合わせ窓口とする機能）」が存在するが、以下の理由により今回の検証では対象外とした。

Talk（コールセンター機能）

コールセンターについては、製品機能以前に、コールセンター自体の体制や業務フローなどについての把握と検討が必要となり、また、検証においてもそれらを踏まえたものでなければ有効性を持ち得ないことから、今回の検証期間および費用の観点から検証を見送った。

また上記にかかわらず、通話については本質的に 1：1 の対応が前提となり、業務効率化に限界があることから、他の機能で通話と遜色のない対応の実現を模索することが本検証の意義に叶うと判断した。

ソーシャルメッセージングアドオン（SNS を問い合わせ窓口とする機能）

現在 SNS を窓口とした対応は各委託事業で行われておらず、今回の検証では見送り、Zendesk サービス群のみでの検証に注力した。

なお本機能で対応可能な SNS として、LINE・Facebook・Twitter などの主要な SNS が含まれていることから、Zendesk 本体での運用が確立された上で導入するならば、将来的に非常に有用な機能となると思われる。ただし、その際は各 SNS アカウントそのものの運用方針についても一定の取り決めが必要となると思われる。

ほか、Answer bot アドオンについては従量課金制である。また Explore については案件ごとに必要な分析の粒度が変わってくるため、今回は無料版の Lite で構成した。

■ 3.構成上の注力点

選定理由中の考慮事項である、「国民の自己解決を促進する」という点をテーマとして設定し、その上で省庁所管事業であることも踏まえ、以下に注力した。

セキュリティ

全般的に、業務インフラにおいて構成したアーキテクチャとの整合性をとるように注力した。具体的には、認証・認可については業務インフラにおける IAM 製品との SAML・SSO を実現する構成とした。

ガバナンス

中核となる Support・Guide・Chat の 3 製品について、内部不正の抑止とトレーサビリティーの確保のため、いずれも監査ログを取得可能な Enterprise プランを選定した。

ユーザー間トラブルとハラスメント抑制

Guide によるナレッジサイトの構成について、ユーザー間でのコミュニケーション機能はユーザー間トラブルの発生要因となりえるため、「国民の自己解決を促進する」というテーマを阻害しない範囲内で、機能を無効化した。

また、ユーザーからのナレッジサイトへのコメント機能もテーマ編集により無効化し、問い合わせ対応スタッフの氏名や性別などの属性情報も非公開とし、カスタマーハラスメントが発生する懸念について考慮した構成とした。

効果測定・レポーティング

通常の効果測定に加え、先述のユーザー間トラブルとハラスメント抑制のための構成によるユーザーフィードバックの減少を補完する意図で、Explore による製品内部の網羅的なレポーティングを行う構成とした。また、後述 Google Analytics サービス群と一体として構成している。

効率向上と管理側コスト/工数/オペレーションミスの削減

「国民の自己解決を促進する」というテーマに沿わせながら、Answer bot による夜間対応、AI によるメール応答文のナレッジサジェストなど、効率向上のためのさまざまな可能性を模索できる構成とした。

加えて、「マクロ機能により、ワンクリックで定型ワークフローを半自動で実施可能とする」「エスカレーション通知についても Slack への通知を発信する」など、管理側コスト・工数・オペレーションミスの削減を意識した構成とした。また、権限外のマクロが表示されない設定とした。 Slack 通知についても、Slack 内部に機微情報類が残置しないように件名・チケット URL など、最低限の通知項目記載にとどめた。

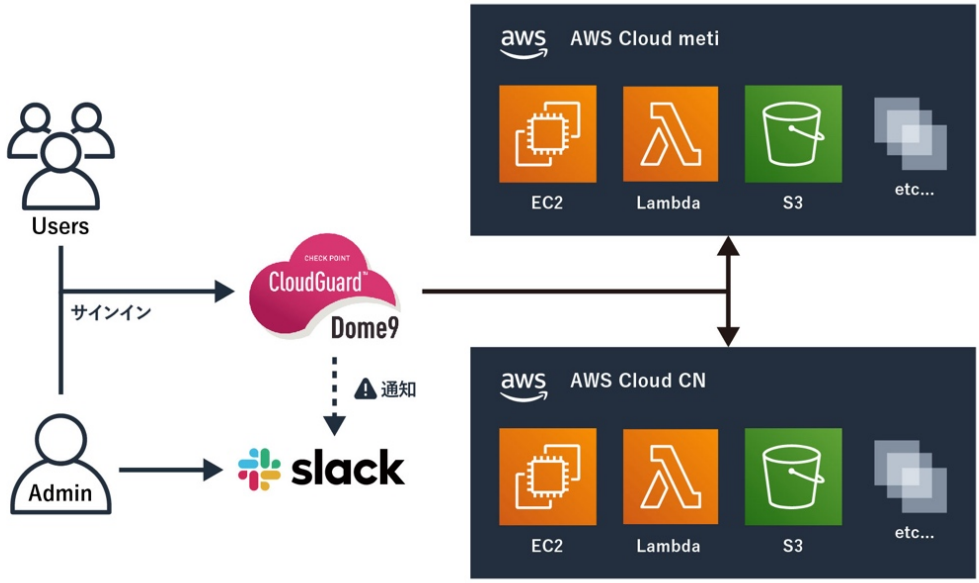
■ 4.検証結果概要

委託事業を行う際の問い合わせ管理については、委託事業者の提案を前提としているため、事業ごとに管理システムが異なっている現状がある。問い合わせに対して、夜間対応など利便性を高めながら効率的に対応していく為に、FAQ の充実や Chatbot による自動応答などのサービスを追加したいというニーズがある。

本事業にて検証したサービスについては事前に想定していた機能が充足していることを確認したが、ライセンス体系が複雑であり多少の機能差もあるため精査が必要、もしくは運用後のアップデート検討等も視野に入れて導入することを推奨する。

3-4-2 . CloudGuard Dome9 を中核としたサービス群

■ 1.製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である以下の 3 点を必須要件とした。

- 設定不備に起因する事故の発生リスクを低減できる
- 不備のある設定の自動修復ができる
- 多くのプロジェクトで利用できる

上記に加え、クラウドサービスのプラットフォームを使う上での責任共有モデルにて利用者が責任を負う部分の設定が管理できることにも着目した。

事業が準拠すべきコンプライアンス基準は、事業が関わる領域によって決まるが、柔軟にコンプライアンス基準を設定できることを勘案した。

クラウドサービスの設定を監査する機能は、AWS、Azure、GCP などのプラットフォームでも用意されているが、プラットフォーム毎に管理性や操作内容、および結果の出力が異なるため、管理が複雑となる。

そのためそれぞれのプラットフォームの監査基準を揃え、同一 UI にて管理することで監査運用のための学習コストを削減できる。

クラウドサービス（特に IaaS、PaaS）を利用する場合、設定不備に起因する事故の発生リスクを低減するため、脆弱な設定を自動検出・自動修復しセキュリティ上の懸念に対処する必要がある。

脆弱と判定された設定においても、事業の特性や取り扱う情報の性質上、コンプライアンス基準に準拠している必要がないと判断したリソースについては、個別に例外設定できることが望ましい。またシステム管理者が、大量の監査アラートに忙殺されることがないよう、本番環境や本番環境に設定を準じさせているステージング環境など、環境の重要度に応じて通知の有無を設定できる必要がある。

稼働中のシステムのファイアウォール設定を正規のレビューを経ずに変更してしまった場合、攻撃面の暴露によるセキュリティの低下や業務への影響が生じる可能性がある。そのため、正規の手続きを経ないファイアウォール設定の変更があった際に、自動で元の設定に修復する機構を検討する必要がある。

クラウドサービス （特に IaaS、PaaS） 上にシステムを構築する際、運用利便性を重視して、ユーザーに対して必要以上に大きな権限を付与してしまう場合がある。平常時は最小権限で運用し、必要に応じて特権が利用できるよう管理し、その利用状況を監査できる状態が望ましい。

上記要件を鑑みて、監査や特権管理の柔軟性が高い CloudGuard Dome9 をクラウド設定管理ツール（CSPM）として選定した。

（2）注記

CloudGuard Dome9 は AWS のみならず、Azure、GCP などのプラットフォームにも対応しているが、期間内に検証可能な環境が AWS のみであったため、今回の検証では AWS のみを対象としている。

また本番環境に対する自動修復機能の検証は、期間的な問題で調整することができなかった。そのため、本検証の事業者が用意した環境で検証を行っている。

■ 3.構成上の注力点

選定理由中の考慮事項である、「設定不備に起因する事故の発生リスクを低減できる」の実現のため、以下に注力して構成した。

アクセスコントロール

Dome9 には複数の AWS 環境を接続しているため、各 AWS 環境のシステム管理者自身が管理しない環境に対して、誤って閲覧や編集などを実施してしまう恐れがある。そのため、担当者の職務範囲に応じてアクセス権限

の異なる Role を割り当て、必要な操作のみを行える構成とした。本構成に置いて用いた Role を以下の表に示す。

Role	説明
Owner Role	Dome9 で管理している全ての AWS 環境に対して、Dome9 上で行える全ての操作を実行する権限を有する。 本事業の責任者である行政の職員に割り当てている。
Super User Role	Dome9 で管理している AWS 環境に対して、Dome9 上で行える操作のうち、閲覧・編集の権限を有する。 接続可能な AWS 環境のうち必要な範囲を定義し、当該 AWS 環境を担当するシステム管理者に割り当てている。
Auditor Role	Dome9 で管理している AWS 環境に対して、Dome9 上で行える操作のうち、閲覧権限のみを有する。 Dome9 を利用したコンプライアンス基準への準拠状態の確認や、Alert の確認のみを行う担当者に割り当てている。

AWS セキュリティグループを正規の手続きを経ずに更新することで、担当者が意図しない影響が生じる場合がある。検証環境の AWS セキュリティグループを Dome9 管理画面以外の場所から更新した際に、元の設定に自動修復されるよう Network Security 機能を構成する。

サーバーへのログインを伴うメンテナンスのために、グローバル IP アドレスを指定してメンテナンスポートを開放する方法が一般的に採られるが、メンテナンスのために登庁する必要があるなど、運用負荷が懸念される場合がある。また固定された IP アドレスそのものを信頼し続けるのは、ネットワーク境界防御の思想にもとづくものであり、本事業の方向性と異なるものである。Dome9 の管理画面から、特定の送信元 IP アドレスに対し、時限的なセキュリティグループ開放を設定できるよう、Dynamic Access Leases を構成する。

Dynamic Access Leases の利用履歴の監査では、Dome9 の Auditlogs から AWS セキュリティグループのトラフィック制限を解除したユーザー情報、該当のセキュリティグループ、制限を解除していた時間などを確認する。

IAM User や IAM Role に普段利用しない大きな権限を設定することで、IAM User や IAM Role を付与したインスタンス侵害時に広範囲に影響を及ぼしてしまうおそれがある。そのため IAM User や IAM Role に設定されている権限のうち、通常利用よりも高位の権限を制限し、必要な時に Dome9 管理画面上からの申請にもとづいて高位の権限を利用できるよう、IAM Safety 機能を構成する。 IAM Safety 機能を用いた申請によって許可された権限は、指定した時間を経過すると剥奪される。

IAM Safety 利用履歴の監査では、Dome9 の Auditlogs から、利用した IAM User、IAM Role の情報、特権利用した時間を確認する。

コンプライアンス準拠状況の監査

AWS 環境の構成不備や準拠すべきコンプライアンス基準の違反を継続的に監査するため、Dome9 がデフォルトで備えている Rule Sets を用いて、AWS 環境の設定内容を指定したコンプライアンス基準にもとづいて定期的（おおよそ 1 時間間隔）に監査するよう構成している。コンプライアンス基準を満たしていないリソースに対して、Dome9 の管理コンソールと、Slack へ通知するように設定している。

一方でコンプライアンス基準を満たしていないリソースのうち、特別な理由によって監査対象から除外したいリソースに関しては、個別に例外設定を実施している。また、Rule Sets にて定義されている Severity（重要度）が Medium 以上の項目について Slack に通知するように構成した。Severity が Low 以下の通知を行わない項目に関しては、定期的にコンソールを確認して都度対応する運用方式としている。

本構成で利用した Rule Sets の一覧を以下の表に示す。

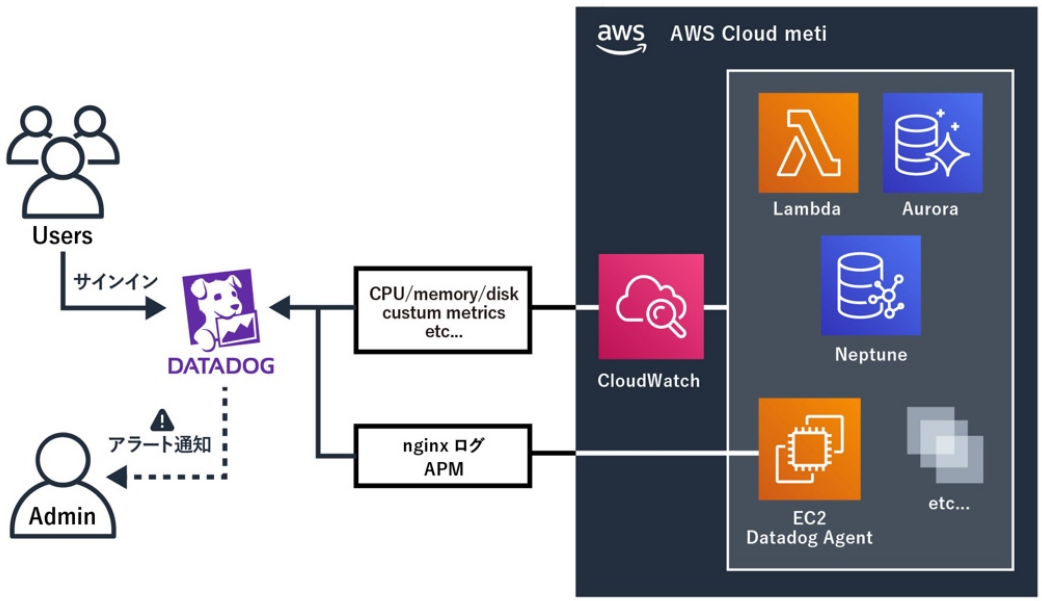
コンプライアンス基準	概要
AWS CIS Foundations v. 1.1.0	CIS V 1.1.0 による AWS の自動評価
AWS CSA CCM v.3.0.1	Cloud Controls Matrix（CCM） v3.0.1 による AWS の自動評価
AWS Dome9 Best Practices	AWS アカウントをセキュアにする Dome9 ベストプラクティス
AWS Dome9 Network Alerts	AWS のための Dome9 ネットワークアラート
AWS Dome9 S3 Bucket Security	S3 のベストプラクティスおよび潜在的な誤設定の検出の自動評価
AWS GDPR Readiness	AWS のための自動 GDPR アセスメント
AWS HIPAA	U.S. Health Insurance Portability and Accountability Act （HIPAA）の自動評価
AWS ISO 27001:2013	ISO 27001:2013 における AWS の必要要件の自動評価
AWS NIST 800-53 Rev 4（FedRAMP）	NIST Special Publication 800-53 （Rev. 4） の自動評価 NIST 800-53 は FedRAMP をコントロールしている
AWS PCI-DSS 3.2	Payment Card Industry （PCI） Data Security Standard Version 3.2 の自動評価
AWS PCI-DSS	PCI-DSS 準拠のために必要なセキュリティ設定の自動評価

■ 4.検証結果概要

クラウドサービスは利用者とクラウド事業者の責任共有モデルで成立しており、ネットワーク設定や ID・アクセス権限設定の構成不備など、準拠すべきコンプライアンス基準の違反を継続的に監査することが求められる。本事業で検証したサービスについて、それらの機能が充足していることを確認し、また、複数のクラウド事業者のサービスに対し一定の基準で評価できる点が優れていることを確認できた。

3-4-3 . Datadog を中核としたサービス群

■ 1.製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である以下の 4 点を必須要件とした。

- リアルタイムにサービス稼働状況が可視化できる
- インフラ・アプリケーション・NW 機器のメトリクス情報を収集できる
- リアルタイムでの状態把握や分析ができる
- KPI の達成状況をダッシュボード化できる

本来の業務遂行に影響を及ぼさないために、パフォーマンス計測ツールの実装・展開が容易である必要がある。

またシステムになんらかの異常が発生した際に、原因を特定するための情報が複数箇所に管理されていると、原因究明までに時間がかかる。そのためインフラストラクチャの情報だけでなく、アプリケーション・ネットワークを含めた情報を一元的に収集・管理することで原因究明を迅速に行うことが可能となる。

さらに、インフラストラクチャ、アプリケーション、ネットワークなどさまざまな情報が集約されることでリソースが増加し、管理が複雑になる恐れがある。そのような問題を回避するために、「自動生成したタグにもとづいてリソースを分類することができる」「各リソースの依存関係を可視化できる」など、複雑な環境の中からボトルネックを特定する機能を有することが求められる。

上記要件を鑑みて、インフラストラクチャ、アプリケーション、ネットワークなどさまざまな情報を集約でき、実装が容易な Datadog をパフォーマンス計測ツールに選定した。

（2）注記

Datadog には、セキュリティ監視、外形監視などさまざまな側面から監視を行えるソリューションが用意されているが、経済産業省の利用環境に合わせて実装する監視項目を下記に絞った。

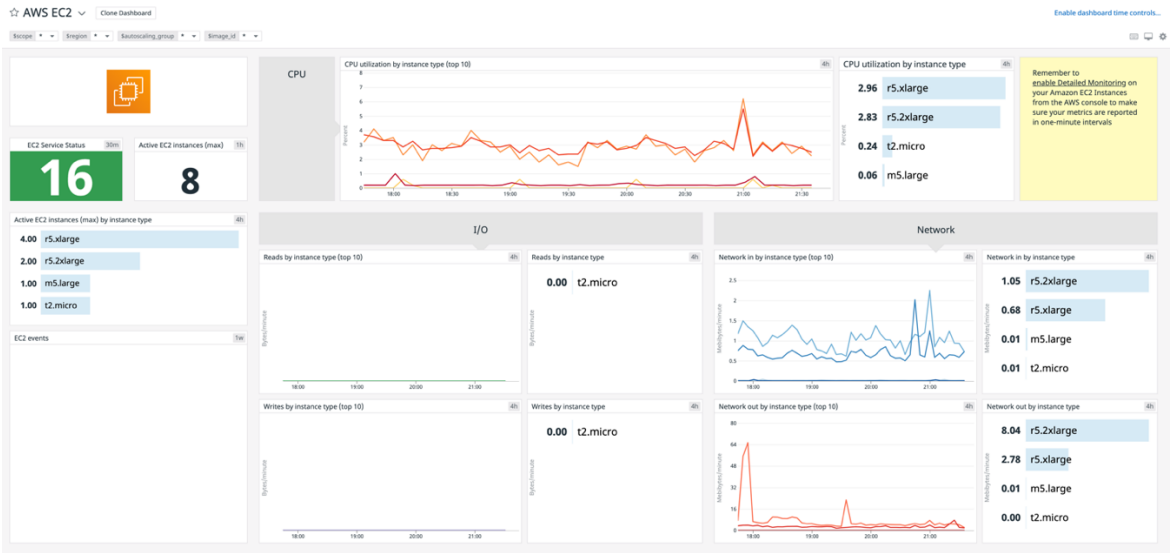
- AWS インフラ監視
- CloudWatch ログ監視
- Nginx ログ監視
- JAVA（spring boot）/APM 監視

■ 3.構成上の注力点

（1）AWS のパフォーマンス異常を検出する

AWS で稼働する EC2 インスタンスの CPU 使用率、メモリ使用率、Disk 使用率などを計測し、Datadog の Integration 用いて AWS のリソース情報を可視化・監視できるよう構成した。また、監視対象のメトリクスが異常値に達した場合は管理者ユーザーにメール通知が行われるよう、Monitor を構成した。

また AWS のログを Datadog に取り込み、ログを検索できるよう、CloudWatch ロググループ統合を構成した。異常が発生した場合は、Datadog の管理コンソールのログ分析画面にてログの検索を行い、異常発生箇所の特定に役立つ。



（2）JAVA/Spring boot アプリケーションの異常を検出する

EC2 インスタンスに Datadog の APM（Web-Application Performance Monitoring）モジュールを導入し、リクエストを処理するために必要な外部サービス処理呼び出しを、Datadog ダッシュボードの APM コンソールにて可視化できるよう構成した。

（3）NGINX ログの異常を検出する

EC2 インスタンスに Datadog の Agent を導入し、Integration にて NGINX と統合することで、NGINX 内で発生した異常なログを Datadog のコンソール上で監視できる構成にした。

また、異常なログが発生した場合にメール通知が行われるよう、Monitor を構成した。異常が発生した場合は、Datadog の管理コンソールのログ分析画面にてログの検索を行い、異常発生箇所の特定に役立つ。

（4）Dashboard のカスタム

Datadog は、Integration にて統合したサービスごとにデフォルトで Dashboard を作成される。本事業では、注視したいインスタンスやサービスに合わせて Dashboard をカスタムし、必要な情報を瞬時に確認できるよう構成した。

（5）ユーザーごとに Datadog 内で実施できる操作を制限する

個々のユーザーそれぞれに指定した操作のみを実施できるよう、Team 機能を用いて Role の割り当てを実施している。

■ 4.検証結果概要

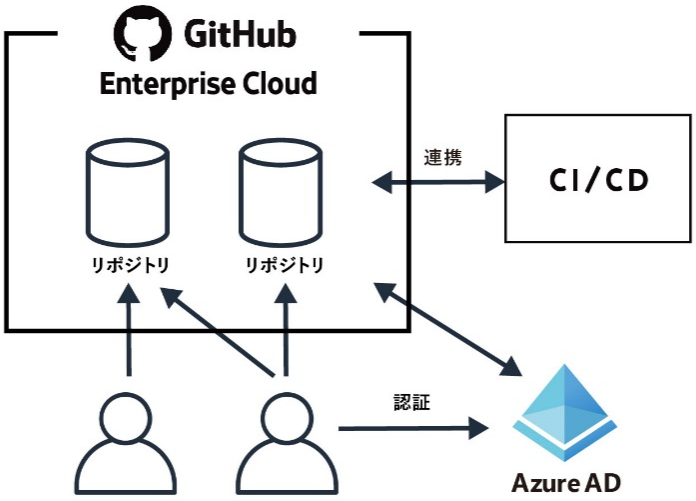
各委託先事業者にてシステムの稼働監視、異常アラート通知等を実装しているが、障害発生時の原因特定のために各種ログを検索して調査・対処を実施するには時間がかかる。予め各種ログを一元的に収集し、ダッシュボードなどで可視化しておくことで、過去の傾向から見た異常の原因究明が容易になる。

運用業務として KPI を手作業で集計して月次業務報告を行っているケースもあるため、運用コストの低減にも寄与することが期待できる。

本事業にて検証したサービスは、インフラストラクチャ、アプリケーション、ネットワークなどさまざまな情報を集約でき、実装が容易であるというメリットがあり、事前に想定していた機能が充足していることを確認したが、ライセンス体系が豊富かつ複雑であるため、測定したい対象リソースを明確にして導入した後に、対象範囲を拡大する方法を推奨する。

3-4-4 . GitHub を中核としたサービス群

■ 1.製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である以下の 4 点を必須要件とした。

- 省内で開発しているソフトウェアのソースコードを管理できる
- チーム内でソースコードを共有できる
- 外部委託業者の SE との開発・保守が可能である
- CI/CD ツールとの連携が容易である

（2）注記

GitHub には複数のサービスプランがある。組織の認証基盤との連携が必須のため、GitHub Enterprise が必要になる。今回は GitHub Enterprise Cloud を利用して検証を行う方針とした。本事業の実施期間中に GitHub を用いた事業とのコラボレーションが調整できなかったため、実際に構成するに至っていない。

そのため以下に記載する構成上の注力点は、構成する上で留意する事柄について記載する。

■ 3.構成上の注力点

組織（Organization）の取り扱い

IdP と連携する

github.com の組織のリソースにアクセスするために、SAML 認証が利用できる。省の認証基盤と連携することで、ユーザーが GitHub にアクセスする権限を IdP で管理できる。省に所属していないアカウントに関しても、可能な限り、IdP 経由でのアクセスを要求することが望ましい。

MFA を要求する

GitHub と連携している IdP を経由しないでアクセスするコントリビューターがいる場合は、MFA の設定を要求できる。MFA を設定していないセキュリティレベルの低いアカウントのアクセスは許可しないことが望ましい。

Verified バッヂをつける

github.com の組織は、ドメインを登録することで、Verified バッヂをつけることができる。GitHub 上の組織とインターネットドメインの関係性を明示することで、なりすましを防げる。

アカウントの取り扱い

GitHub のアカウントの特徴

github.com のアカウントは、組織から独立して存在しており、アカウントの管理を組織で行うことができない。個人の所有しているアカウントは、個人で管理する必要がある。例えば、アカウントの作成や SSH の鍵管理は、アカウントを所有している個人で行わなければならない。

github.com のアカウントは、組織に対してメンバーまたはコラボレーターとして参加できる。

メンバー

メンバーは、組織に所属するアカウントで、組織にある GitHub のリソースに対するアクセス権をまとめて設定ができる。IdP と連携している場合は、メンバーは IdP での認証を要求される。

コラボレーター

コラボレーターは、組織外のアカウントを特定のリポジトリにアクセス許可する場合の形式で、組織に所属していないアカウントに対するアクセス権を表す。IdP と連携している場合は、コラボレーターは IdP での認証を要求されない。

アカウントの所有者を確認する

GitHub の組織にアカウントを追加する際に、そのアカウントの所有者が本当に組織のリソースにアクセスする権限をもっている個人であるのかを確認することが望ましい。

組織に属するメンバーの場合は、IdP による認証が要求され、組織のアカウントを利用し認証することで所有者本人であることを確認できる。

GitHub では、個人アカウントを組織に招待する形になるため、コラボレーターを招待する際に、GitHub のアカウントが対象者のアカウントであることを確認する方法や、アカウントの取り違えについて対策の検討が必要である。

リポジトリ公開手続き

プライベートで開発した成果を公開する目的で、プライベートリポジトリをパブリックリポジトリに変更できる。

公開する際の手続き

プライベートリポジトリをパブリックリポジトリに変更するための権限は、安易に付与してはならない。リポジトリを公開するためには確認の手続きを必要とすることが望ましい。対象となるリポジトリを公開するためには、以下のような手順を踏むようにすること。

1. リポジトリを公開するための申請をする
2. その内容が公開に値するのかを精査する
3. 精査した結果、公開しても問題がない場合は公開を許可する

公開内容の精査

リポジトリ公開の際の精査は、以下のような観点で実施する。

- リポジトリ内にシークレットが含まれていないか確認する
  ※シークレットとは、パスワードやアクセストークンのような認証情報、
  その他公開してはいけない情報を指す
- コメントなどに、公開に相応しくない文言が入っていないか確認する

外部システムとの連携

Webhook、Third-party Access、Actions などの機能により、外部のシステムと連携できる。経済産業省では現在、Microsoft Power Platform 用 GitHub Actions を使用してソリューションのデプロイ自動化を検証しているところである。

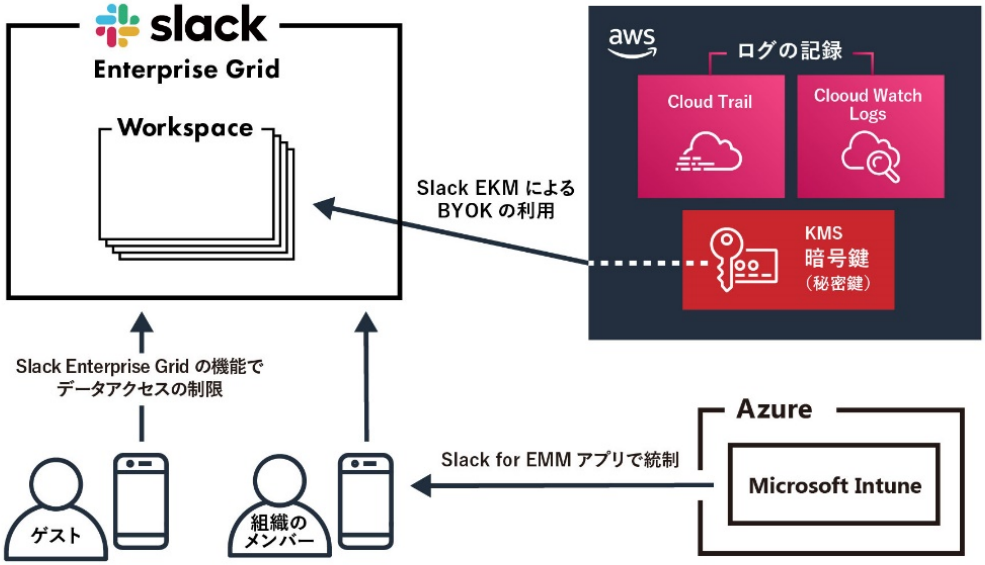
下記のような観点で連携対象のシステムを精査し、問題ないことを確認してから連携すること。

- 連携対象となるシステムに渡す権限やアクセス許可
- 連携先のシステムのデータ保護についての安全性の評価
- データ流通経路の把握

また、連携先の棚卸しを定期的に実施することが望ましい。

3-4-5 . Slack を中核としたサービス群

■ 1.製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である以下の 3 点を必須要件とした。

- チャットを使った円滑なコミュニケーションができる
- 独立した暗号キー管理（BYOK）ができる
- 本事業で利用が想定される全てのツール類の通知先として連携できる

また、リアルタイムでのコミュニケーションのしやすさや、組織に所属しないメンバーとのコミュニケーションのやりやすさに加え、情報制御のやりやすさなど、利便性とセキュリティのいずれも実現する必要がある。

これらの要件を鑑みて、コミュニケーション管理ツールとして Slack を選定した。

（2）注記

Slack には複数のサービスプランがある。BYOK や、モバイルデバイスにおける情報制御の機能を利用するためには Enterprise Grid プランが必要になる。今回は Enterprise Grid を用いて検証を行った。

■ 3.構成上の注力点

（1）BYOK（Bring Your Own Key）を使う

情報漏えいのリスク軽減のため、Slack Enterprise Key Management（Slack EKM）を採用する。Slack EKM は、Slack で取り扱うメッセージやファイル、検索履歴などのデータを暗号化するための鍵を利用者が管理できる機能である。

鍵の管理には、AWS の Amazon Key Management Service（Amazon KMS）を利用する。データの暗号化や復号をする鍵の使用状況が CloudWatch や CloudTrail に記録される。

暗号鍵に対するアクセスポリシーの設定によって、Slack のテナント全体ではなく一部のチャンネルに絞った形で復号を制限できる。情報に対するアクセスを一時的に制限したい場合に利用できる。

Slack EKM は、Slack Enterprise Grid でのみ利用可能である。

（2）個人と組織のデータを分離する

モバイルデバイス（スマートフォン）を利用する場合、情報漏えいリスク軽減のため、個人と組織の情報を分離する必要がある。

組織が管理するモバイルデバイス（スマートフォン）で利用する Slack アプリは、Slack for EMM を採用する。Slack for EMM は、その他のアプリに対してデータの移動を制限できるため、Slack のデータのアプリ外持ち出し制御が実現できる。

個人が所有する BYOD 端末からの利用を許可するかの課題については、下記の制御されていない端末に対しての制限を有効にすることで対応する。

ファイルのダウンロードとメッセージのコピーをブロックする

アプリ外にデータをコピーできないようにする。

モバイル用パスコードを必須にする

管理下にないデバイスからのアクセスを許可する場合の設定。一定時間操作がない場合にアプリをロックする。アンロックには PIN コード、生体認証を使用する。

脱獄またはルート化されたデバイスをブロックする

脱獄またはルート化されたデバイスは制御の実現が困難であるため、Slack の利用を禁止する。

モバイルアプリの最小バージョンを設定する

脆弱性のある古いバージョンのアプリの利用を禁止する。

（3）情報公開範囲の設定

Slack の構造

情報公開範囲について述べる前に、Slack の構造について解説する。Slack Enterprise Grid を構成する要素は以下の表の通りである。

構成要素	説明
組織 （オーガナイゼーション）	Slack Enterprise Grid におけるもっとも大きな管理単位。 組織には複数のワークスペースを作成できる。ワークスペースやユーザーは組織に属している。ユーザーは複数のワークスペースに参加できる。ワークスペースの設定では、「ユーザーが自由に参加できる」「参加に承認が必要」のいずれかが選択できる。
ワークスペース	複数のチャンネルが属するコミュニケーションの単位。 ワークスペースに所属するユーザーは、プライベートチャンネルを除き、任意のチャンネルに参加できる。
チャンネル	Slack でコミュニケーションを行う際の最小単位（ダイレクトメッセージを除く）。 トピックや部門ごとにチャンネルを作成し、チャンネルに参加しているユーザー間でメッセージのやり取りをする。 チャンネルはワークスペースに所属しており、ワークスペースに所属しているユーザーが参加できる。 また、Slack Connect を使って他のワークスペースとチャンネルを共有できる。 Slack Enterprise Grid は、組織内・組織外いずれのワークスペースとも共有可能である。

ワークスペース

組織内で取り扱う情報へのアクセスを明確に分離する必要がある場合はワークスペースを分けることで、アクセス可能なユーザーを明確に分けられる。組織全体で共有するべきではない機密性の高い情報を取り扱うために

は、プライベートチャンネルの利用を常態化するよりも部署ごとにワークスペースを分離し、パブリックチャンネルを利用すべきである。

また組織の規模が大きく、ワークスペースの管理を部署ごとに委任したい場合も、ワークスペースの分割を検討する。

チャンネル

チャンネルには、情報の公開範囲が異なる複数の種類がある。

- パブリックチャンネル
- プライベートチャンネル
- 組織内共有チャンネル
- 組織外共有チャンネル
- ダイレクトメッセージ

通常の業務において取り扱う情報は、透明性を確保するため秘匿するべきではない。そのため、組織のメンバーが自由に参加できるパブリックチャンネルの利用を原則とする。

一方で、機微情報など共有先を限定しなければならない情報の取り扱いは、プライベートチャンネルを使って限られたメンバーのみで行うべきである。取り扱う情報の判断が必要になるため、プライベートチャンネルの利用を制限する。

プライベートチャンネル

プライベートチャンネルの作成を管理者のみに制限し、一般ユーザーが作成できないようにする。

プライベートチャンネルの作成は申請制とし、申請者は利用目的を明らかにする。取り扱う情報がプライベートチャンネルで扱うのに相応しいかどうかは、申請者の所属する組織の長が判断する。

プライベートチャンネルで取り扱うべき情報の例として、以下が挙げられる。

- 個人情報
- 事故、内部不正、刑事事件などの情報

プライベートチャンネルは管理者が作成するが、管理者がそのチャンネルのメンバーとして不要な場合は、チャンネルから退出すべきである。

プライベートチャンネルは、管理者であってもチャンネルに参加していない場合はチャンネル内の情報を閲覧することができない。Discovery API などを用いて機械的にアクセスすることや、JSON 形式で取り出すことが可能ではあるものの、監査が容易とは言い難い。そのため無期限でのプライベートチャンネルの利用は許可せず、利用目的に合わせて期間を設定することが望ましい。無期限での利用が必要な場合は、異なるワークスペースの利用を検討すべきである。

組織内共有チャンネル

Slack Enterprise Grid の同じ組織に所属するワークスペース間で、組織内共有チャンネルを作成して情報を共有できる。ワークスペースを分離して情報の共有範囲を限定している場合は、組織内での共有チャンネルは一般ユーザーが自由に作成できないように制限することが望ましい。

組織内共有チャンネルの作成権限を制限し、作成が必要な場合は申請制とすることで、必要性を検討できる状態にすべきである。

組織外共有チャンネル

経済産業省以外の省庁や企業と協業する場合は、組織外共有チャンネルを使って情報を共有できる。組織外共有チャンネルの情報は、連携しているワークスペースそれぞれにコピーが存在する状態になるため、組織外に共有された情報は制御できない。

組織外共有チャンネルの作成権限を制限し、作成が必要な場合は申請制とすることで、必要性を検討できる状態にすべきである。

ダイレクトメッセージ

他のユーザー間のダイレクトメッセージのやり取りはプライベートチャンネルと同じ性質をもつため、原則利用しないことが望ましい。しかし Slack の機能としてダイレクトメッセージの使用を制限することができないため、ダイレクトメッセージを利用しないように利用者への指導が必要である。

ただし例外として、幹部同志が直接コミュニケーションを行うような場合は、取り扱う情報の性質上、ダイレクトメッセージの利用を制限するものではない。

また Slack Connect を使って、組織外のユーザーとダイレクトメッセージのやり取りが可能だが、Slack Connect による組織外とのダイレクトメッセージは、利用できないように設定すること。

Slack App による外部システムとの連携

ワークスペースごとに、利用可能な Slack App コントロールの設定が可能である。取り扱う情報や法規制などにもとづいて、利用可能な Slack App コントロールを検討する必要がある。連携先のシステムが要求する Slack App コントロールを確認した上で決定し、定期的に棚卸しを実施することが望ましい。

アップロードファイル

Slack にアップロードされたファイルの共有範囲はワークスペース全体となり、アップロードされたファイルに対するアクセス履歴の追跡は困難である。そのため、アクセスコントロールが必要なファイルについては Box に別途格納し、その URL を Slack で共有することが望ましい。

Slack へのファイルアップロードを、Slack の設定で制限することはできない。Box の利用を徹底するためには、Slack にアップロードされたファイルを自動的に Box に格納するような連携ツールの導入検討が必要である。

機密性 2 と機密性 3 に該当するデータは Slack では取り扱わないことが前提であるため、それらに該当するファイルは、Netskope の API Introspection を用いて Slack へのアップロードを検出または削除する。

（4）ゲストアカウント

Slack を利用していない外部組織とのコミュニケーションが必要な場合や、契約形態などの都合により一部のチャンネルのみ利用を許可したい場合は、ゲストアカウントを作成して一部のチャンネルに招待できる。

ゲストアカウントの発行には申請を必要とする。ゲストアカウントは原則利用期限を設け、無期限の利用を認めない。一定期間ごとにゲストアカウントの棚卸しを実施し、不要なものは削除すべきである。

ゲストアカウントには、シングルチャンネルゲストとマルチチャンネルゲストの 2 種類が存在する。シングルチャンネルゲストは、1 つのチャンネルのみ参加可能で、ライセンス費用は発生しない。マルチチャンネルゲストは、任意の複数のチャンネルに参加できるが、通常のアカウントと同様にライセンス費用が発生する。そのため、シングルチャンネルゲストの利用を原則とし、マルチチャンネルゲストが必要な場合は追加コストが発生することを踏まえた上で検討する。

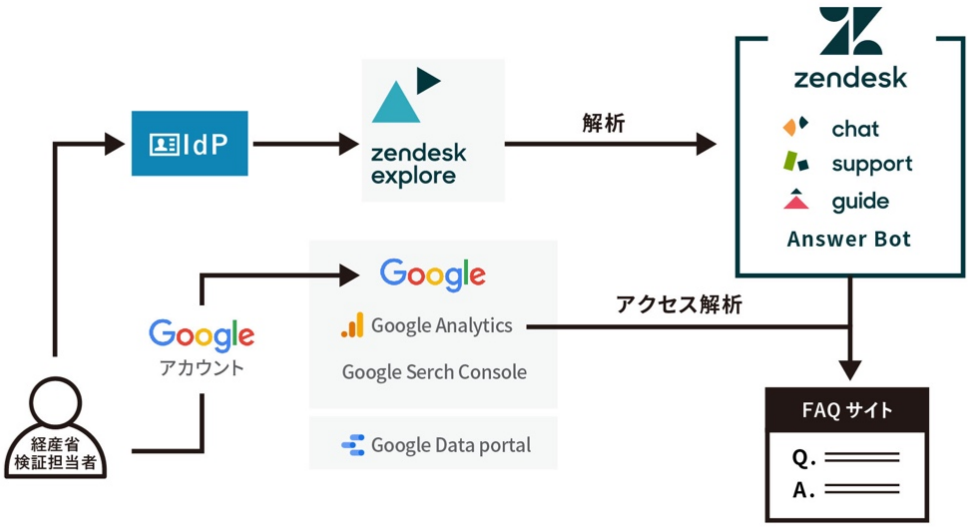
ゲストアカウントによるログインは、Azure Active Directory による SSO を使用する。Azure Active Directory の External Identities 機能により、外部アカウントを招待して Slack を利用する権限を付与する。セキュリティを担保するため、条件付きアクセスを利用して多要素認証の利用を強制することが望ましい。

4.検証結果概要

Slack には、チャットを使ったリアルタイムでのコミュニケーションや組織に所属しないメンバーとのコミュニケーションのやりやすさなど、円滑なコミュニケーションを促進するメリットがある。今回、情報漏えいのリスク軽減のため、独立した暗号鍵管理（BYOK）が実現できることを検証し、Slack で取り扱うメッセージやファイル、検索履歴などのデータを暗号化するための鍵を利用者が管理でき、利便性とセキュリティのいずれも実現できることを確認できた。

3-4-6 . Google Analytics を中核としたサービス群

1. 製品グループ関連範囲の構成図



■ 2.選定理由

（1）理由

選定にあたり、調達意図である、以下の 4 点を必須要件とした。

- アクセス状況や処理状況を可視化・分析できる
- 適宜必要な項目について抽出したダッシュボードを作成できる
- 単体で一定のアクセス制御を備えている
- 機能において汎用的であり、かつ安価である

加えて、解析対象となることが多いと想定される Zendesk Guide によるナレッジサイトとの連携を考慮した。

また現在中小企業庁にて、中小企業向け補助金・総合支援サイトである「ミラサポ plus」などで Tableau と KARTE を使用している例があり、それらとの差異についても考慮した。

まず Google Analytics サービス群の各サービスが、現在の KARTE と Tableau との組み合わせに対して、基本的な機能をカバー可能であるか検討した結果、Google Analytics サービス群内では Google Analytics がアクセス解析・分析・ダッシュボード機能を提供し、Google Data Portal がダッシュボード・レポーティング機能を提供していた。検索キーワード解析については Google Search Console によって提供されるため、サービス群内でアクセス解析ツールとして求められる機能の全てを提供しており、無料で利用できるという利点が見受けられた。

ほか、Google Analytics 単体で見た場合、アクセス解析ツールにおけるデファクトスタンダードであり、習熟度の観点から人的リソースの確保についても、Tableau と KARTE の組み合わせと比べて容易であることが予想された。

加えて Google Analytics は Tableau との接続も可能であり、予算と用途により、ダッシュボード・レポーティングについては、Google Data Portal ではなく Tableau を用いるという柔軟な対応が可能であることから、アクセス解析基盤として適切であると思われる。

また KARTE の特性として、俯瞰的なアクセス解析よりも、個々のユーザーの行動解析に機能が特化している。例として、ユーザーの操作をリアルタイムで追跡・表示する機能を備えている。

要件によっては非常に有用であるが、俯瞰的なアクセス解析が求められるケースも想定されるため、KARTE が有償である点も考慮すると、第一の選択肢とするよりは、ユーザーの行動の把握が必要である場合に採用するなど、Google Analytics との使い分けが適切であると思われる。

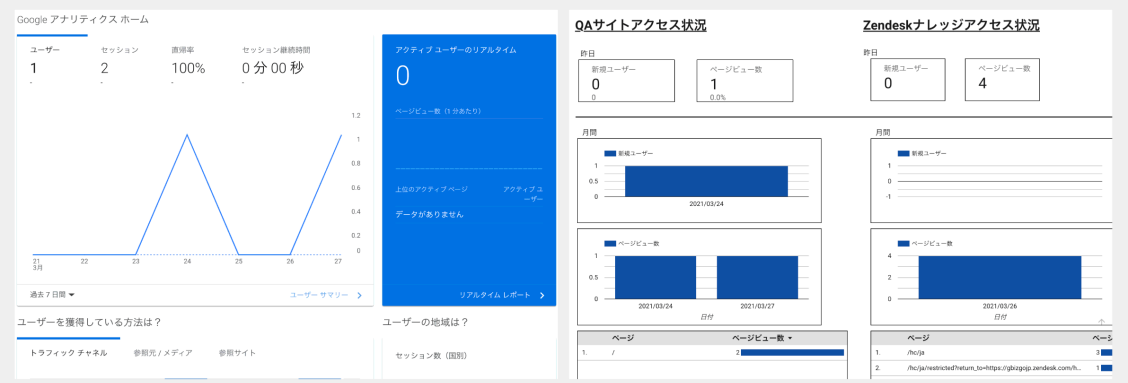
なお Tableau と KARTE については、比較的機能習得が容易という長所があり、特に製品のヘルプの充実度については Google Analytics に勝っている。しかし、Google Analytics はアクセス解析ツールにおけるデファクトスタンダードであることから知見について巷間に豊富であり、利用経験者も多数存在することから、汎用性の観点で採用優先度を高めても差し支えないと判断した。

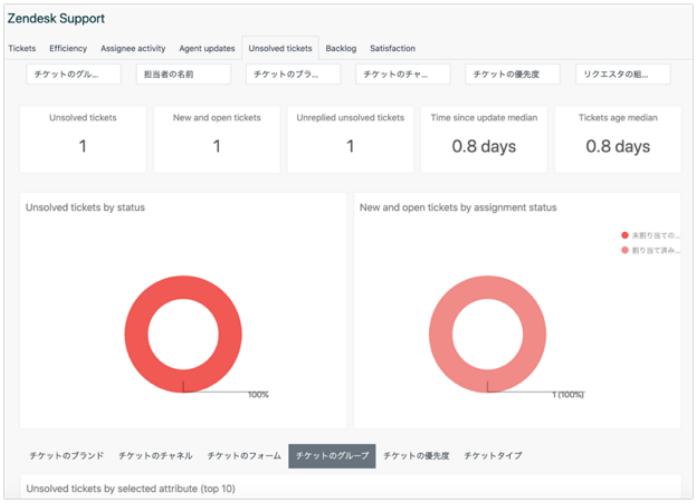
上記の理由から、アクセス解析ツールとして選定した。

（2）注記

FAQ サイト本体および Zendesk Guide を利用したナレッジサイトのアクセス解析については Google Analytics を利用するが、チケットの対応状況やナレッジ記事の効果測定などについては、Zendesk サービス群に含まれる Explore の機能を利用する構成とした。

なお、データソースとして Zendesk の処理内容を Google Data Portal で表示する機能は用意されていないこともあり、FAQ サイト本体・ナレッジサイトの個別の詳細なアクセス解析ダッシュボードとしては Google Analytics を使用し、レポーティングについては Google Data Portal と Zendesk Explore のダッシュボードのふたつを併用する形式とした。





ほか、Google Analytics サービス群については有償版が存在するが、大規模 Web サイト向けかつ応分の比較的高額な費用が必要となるため、調達意図との相違以外の観点でも、今回のような一時的な検証には適さないと判断した。各アカウントについても、検証規模を勘案し、有償の Google Workspace テナントは調達せず、無償の Google アカウントでの検証に留めた。

加えて Google Analytics については、GA4 と Universal Analytics のふたつのバージョンが存在するが、取得可能な項目を考慮し、Universal Analytics を採択した。

また検証環境については外部公開を行わないことから、Search Console については基本的な機能の確認に留めた。Google Optimize についても、検証環境では根幹部分である A/B テストの有効な検証が行えないことから、今後の課題事項とし、検証は見送った。

■ 3.構成上の注力点

プライバシー保護、汎用性、および事業の性質を勘案し、極力 Web サイト全体のアクセス数やランディングページごとのアクセス数などの取得にとどめ、属性情報などについては可能な限り取得しないように構成した。

具体的には、「広告向け機能に必要なデータ収集」「ユーザー属性とインタレストカテゴリに関するレポート」「User-ID に関する機能」など、属性情報の取得につながる機能を全てオフにしており、表示についても同様の設定を行った。

また、データの保持期間についても最短の 14 ヶ月と設定することで、明確な保持期間を設定できた。

加えて権限設定についても、Google Analytics では、データソースごとの権限管理が可能である。レポーティング機能を提供し、多くの関係者が閲覧するであろう Google Data Portal についても、閲覧者によるダウンロード、印刷、コピーが制限できた。

さらに、ユーザー追加の権限を制御可能であり、新たに追加されたユーザーについては、ダッシュボードの管理画面上で視認できることを確認した。

なお、Google Data Portal については共有リンクの発行も可能であるが、リンクを知っていれば誰でもアクセスできてしまうため、やむを得ない事情がない限りは使用せず、原則ユーザーを追加して対応する必要がある。

ほか、Google Analytics では設定値の変更履歴が取得され、管理画面で確認可能である。

■ 4.検証結果概要

ユーザーの Web サイトへのアクセス・行動分析を行い、サービスをよりよいものに近づけていく活動は、行政の Web サイト、Web サービスに特に求められている。アクセス状況や処理状況を可視化・分析でき、適宜必要な項目について抽出したダッシュボードを作成できるなど機能において汎用的でありかつ安価であるため、本事業で検証したサービスについては事前に想定していた機能が充足していることを確認したが、データの取得においてはプライバシーに十分に配慮が必要となる。

3-4-7 . Backlog を中核としたサービス群

■ 1.製品グループ関連範囲の構成図

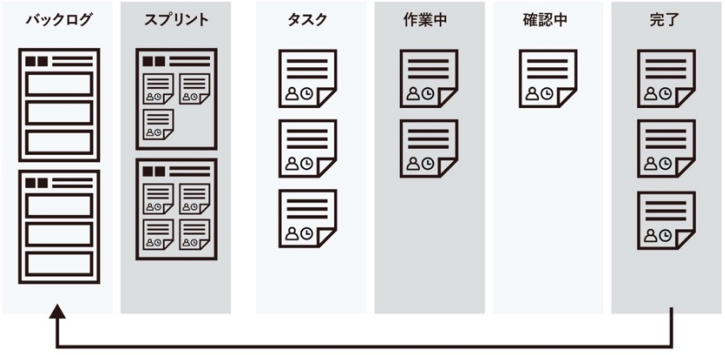
■ 2.選定理由

（1）理由

選定にあたり、調達意図である、以下の 3 点を必須要件とした。

- Web ブラウザで利用できる
- ユーザーアカウントの追加に対し定額プランが提供されている
- 他サービス（主にコミュニケーションツール）との連携ができる

上記に加えカンバン形式でタスク管理ができる点にも着目した。



情報プロジェクト室では、経済産業省のデジタルプラットフォーム構築プロジェクトにおいて外部ベンダーとの問合せ管理や課題管理をメールや Excel ではなく Web ベースのタスク管理ツールで実現するため、2018 年からヌーラボの Backlog を利用している。

タスク管理ツールおよびプロジェクト管理ツールは、Atlassian の JIRA や Trello、Microsoft の Azure DevOps など、他アプリケーションとの連携や CI/CD の機能、スクラムボードやレポート機能などアジャイル開発に必要な豊富な機能が用意されているものもあるが、ライセンスがユーザー単位になるため、利用する範囲を明確にしたうえで導入する必要がある。

Backlog は、提供されている複数のプランでユーザー数無制限（定額）のプランを用意しており、プロジェクト拡大や外部ベンダー増加、経済産業省内のメンバー増加などに追加コストなしで対応できる。ただし SAML による SSO を構成する場合は有償のオプションが必要となる。

また Backlog は Slack やメールなどとの連携機能を有し、チケットの登録や更新の際の通知や、逆にメール等からチケット自動起票が可能など、チケット管理システムを利用していないユーザーに対しての利便性が考慮された体験を提供している。

その他の機能として、ファイル共有や Wiki の機能などプロジェクト管理に必要な一通りの機能が提供されている。セキュリティ面では、経済産業省による『クラウドサービスレベルのチェックリスト』、および IPA（独立行政法人情報処理推進機構）による『安全なウェブサイトの作り方 改訂第 7 版』への準拠について Web サイトで公開している。

上記を鑑みて、プロジェクト管理に必要な機能が一通り揃っており、利便性やコスト管理面で柔軟性が高い Backlog をタスク管理およびプロジェクト管理ツールとして選定した。

（2）注記

Backlog を利用するにあたり、経済産業省が定める「セキュリティ対策基準」にもとづいた情報の管理を行うため、個人情報や非公開情報など機密性の高い情報は Backlog 上で扱わないという運用ルールを定めている。

■ 3.構成上の注力点

すでに運用中のサービスであるため、省略する。

■ 4.検証結果概要

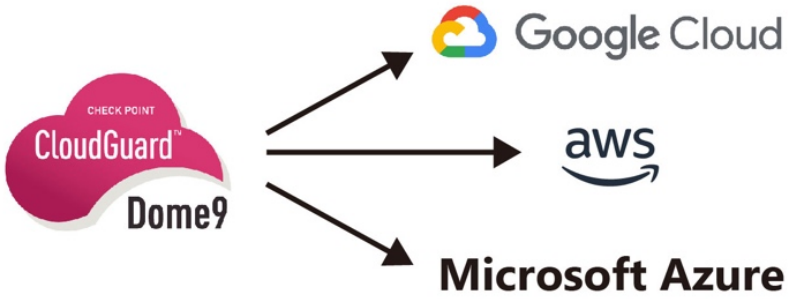
すでに運用中のサービスであるため、省略する。

3 - 5 . ツールの導入実証に係る提言

本事業では、DX オフィスが目指す構想を具現化する取り組みを行ってきた。本事業の遂行を通じて、プロジェクトマネジメントおよびプロジェクトの成果物であるプロダクト改善を行うためのツールの導入実証を行う上で見出した現状のギャップとこれから議論されるべき観点を提言としてまとめる。

3-5-1．ツールを用いたクラウドサービス環境の監査

本事業では、Dome9 を用いて AWS 環境の設定を監査し、各種準拠ポリシーにもとづく監査を行っている。



本取り組みを実施する中で、見受けられた課題とそれに対する提言を以下に示す。

■ 課題

Dome9 は非常に簡便に利用でき、粒度の細かな制御ができる一方で、小規模な構成で利用するには費用が高額となるため、本事業に係る関係者間で各クラウドサービス（AWS、Azure、GCP）で用意されている監査サービスの利用を検討した方がよいのではないかという議論がなされた。

また監査の実施間隔を短くすることで、運用者の負担が増えるのではないかという意見も交わされた。

■ 提言

各クラウドサービスが用意している監査サービスは、監査対象となるオブジェクトごとの除外やカスタマイズについて行き届いておらず、監査項目自体を無効化するなど、大きな粒度の制御が必要となる場合が多い。細かな粒度の制御を行う場合、監査を実施するためのプログラムを別途実装する必要がある。このような実装は、事業によってユースケースが異なるため、別のユースケースで同じ実装が有効に機能するかは未知である。

また、別の事業にて作成されたプログラムで不具合が発覚した場合、のメンテナンスコストを誰が負担するかなどの議論や整理が必要となる。そのため、安易に各クラウドサービスで用意されている監査サービスを採用することで、別の運用コストや実装コストが発生する可能性があることに強い認識と留意が必要である。

なお、小規模な環境ごとに Dome9 を契約することは、指摘された懸念の通り高コストであるため、複数の環境を管理する枠組みを整理し、1 環境あたりのコストとして捉えて利用することが解決策の一つであると考える。本取り組みで、管理する環境ごとのアクセスコントロールがすでに実証されているため、上掲のようなコスト分担の整理が主な課題となると考えられる。

次いで、監査間隔は、その長さに応じて、構成ミスが発見されずに存置・暴露されている時間が長くなる。通常、監査は人手を介して設定項目の棚卸しやチェックが行うため、以前は監査間隔が長くなることはやむを得ない側面があった。しかしながら、本アーキテクチャでは、ツールを用いて監査を行うため、必要な監査設定を構成・調整しておくことで、監査業務の一部を自動化できることが実証されている。

このような監査は、構築が完了し安定稼働している環境に対して行うものであるため、調整済みの監査設定が通知を繰り返すことは考え難く、必ずしも運用者の負担になるとは言えない。

そのため、監査する環境を絞った上で、短い間隔で監査を実施することが望ましい。

一方で本事業では、IaaS を対象とした監査を目的としているが、SaaS や PaaS に類するクラウドサービスや OS、ミドルウェア、コンテナ環境などの各領域においても、利用者の責任範囲に対しての同様のアプローチでの監査が必要となる。

このような監査機能を提供するアプリケーションやサービスは領域毎に複数存在するが、各領域を網羅し一元管理できるツールはいまだ現れていない。

この論点は分野として、Compliance as a Code に類しており、日々発展しているため、動向を注視したい。

なお、Compliance as a Code については、以下 URL を参照されたい。

https://github.com/ComplianceAsCode/content

3-5-2 . オンラインサービスを利用するアカウントの本人確認

■ 課題

GitHub のアカウントは個人が所有していて、組織が管理できない。したがって、組織のメンバーまたはコラボレーターとして登録するアカウント自体を組織で管理できない。組織は、そのアカウントの利用者が、実際にその組織の構成員または契約している本人が所有しているアカウントであることを確認しなければならない。

■ 提言

組織に所属しているメンバー

GitHub と連携している、組織が所有する認証基盤を使った認証を必須とすることで、本人確認が可能になる。

GitHub の組織にメンバーとして参加する場合は、個人のアカウントで GitHub にサインインするだけでなく、組織の認証基盤での認証が必要になる。組織の認証基盤で管理されているアカウントでサインインできることを以ってして、連携している GitHub のアカウントの利用者を確認できる。

組織に所属していないメンバー

組織外の協力者をコラボレーターとして招待する場合は、そのアカウントを協力者本人が所有していることを証明する必要がある。GitHub アカウントをコラボレーターとして招待する場合は、GitHub 以外のチャンネルを使って、GitHub アカウントが本人のものであることを確認できる情報の提供をさせる必要がある。少なくとも、契約している組織に所属していることを証明できる情報が必要となる。

このとき、個々の事情によって、トラストアンカーとして何が利用できるのかを検討する必要がある。例えば、連携済みである組織の Slack ワークスペースのアカウント経由であったり、オンラインではなく対面で情報を交換したり、対面で交換した PGP 公開鍵を使って署名したメールを使うなどの方法が挙げられる。

3-5-3 . チャットツールによる情報の公開範囲の変化

■ 課題

Slack は、グループやトピック毎にチャンネルを作成し、コミュニケーションを活発に行うために、同一ワークスペース内に所属するユーザーが自由に出入りできるパブリックチャンネルの利用を基本としている。

メンバーを限定しないオープンなコミュニケーションが行われるパブリックチャンネルは、ハラスメントや不公正なやり取りを抑止し、健全で活発なコミュニケーションの推進が期待できる。

そのため、限られたメンバーのみが参加できるプライベートチャンネルの利用は、限られたユースケースでのみ行うことが望ましい。

一方で Slack 上の情報の公開範囲は、各チャンネルに所属しているメンバーである。

パブリックチャンネルは、その性質上、情報の公開範囲の最大値が Slack 利用者全員となる。

パブリックチャンネルにファイルをアップロードする行為は、コミュニケーションを効率化する一方で、情報の公開範囲を不必要に広げてしまうおそれがある。

■ 提言

本事業では、ファイルは Box に格納し、適切なアクセスコントロールを設定している。

そのため Slack にファイルそのものをアップロードせずに、Box 上のファイル URL を記載する必要がある。

Slack 自体には、ファイルのアップロードを抑止する機能がないため、上記運用の徹底には別の手段を用いての実現を検討する余地がある。

上記運用が実現するアプローチを以下に示す

1. Netskope を用いて、Slack へのファイルアップロードをブロックするポリシーを実装する
2. Slack チャンネルへのファイルアップロードを検出して、Slack へアップロードされたファイルを削除する機能を実装する
3. Slack Enterprise Grid の設定にて、共有チャンネルへのファイルアップロードを抑止する設定を有効にする

1. Netskope を用いて、Slack へのファイルアップロードをブロックするポリシーを実装する

本アプローチは、Netskope の Realtime Protection 機能または API Enabled Protection 機能を用いてポリシーを実装する。

本アプローチを採用する場合は、以下を留意すること。

1-1. Realtime Protection 機能で実装した場合の適用範囲

Netskope Agent が導入されているデバイスのみを制御の対象とし、Netskope Agent を導入していないデバイスから接続するゲストユーザーを制御の対象とすることができない。

1-2. API Enabled Protection 機能で実装した場合の適用範囲

Netskope Agent を導入していないデバイスやゲストユーザーも含めて制御の対象とすることが可能だが、外部組織のワークスペースと共有チャンネルに対して制御することができない。

2. Slack チャンネルへのファイルアップロードを検出して、Slack へアップロードされたファイルを削除する機能を実装する

本アプローチは、先述の挙動を行うプログラムを作成し、AWS Lambda や Azure Functions のような FaaS（Function as a Service）で関数を実行する方式である。

本アプローチを採用する場合は、以下に留意すること。

- 作成したプログラムを実行する関数が意図通りに稼働しているか、エラーレートなどの実行状況を監視する必要があること
- 関数がサポートする言語バージョンのライフサイクルに応じたメンテナンスが可能な体制や契約を準備しておくこと

3. Slack Enterprise Grid の設定にて、共有チャンネルへのファイルアップロードを抑止する設定を有効にする

本アプローチは、Slack にて提供される機能としては共有チャンネルのみを対象とするものであるという点にて留意が必要である

以上を鑑みて、本節内 1-2 と 3 のアプローチを組み合わせることが、最もカバー範囲が広いものと言える。

実際に適用する際は、ユースケースを精査した上で実施されたい。

3-5-4 . クラウドサービスの SSO

■ 課題

クラウドサービスの SSO 機能については、SSO に対応している場合と SSO に対応していない場合それぞれに課題がある。

SSO を利用する場合のコスト

SSO に対応しているサービスの課題は、SSO を利用するための障壁が高いことである。多くのサービスは、ライセンスに複数の種類がある。SSO に対応しているライセンスが上位のライセンスであり、上位ライセンスの他の機能が不要であったとしても、SSO のために上位ライセンスの選択を強制される場合が多いことである。

SSO 非対応サービス

SSO に対応していないサービスの課題は、セキュリティの確保が難しいことである。SSO 非対応サービスについては利用者の利便性向上のため、Password Based SSO を採用する設計としている。しかし、Password Based SSO は以下のような理由で問題がある。

1. クラウドサービスのセキュリティレベルが向上するわけではない。
2. クラウドサービスが多要素認証に対応している場合は、認証基盤による認証とは別にクラウドサービス側の多要素認証が要求されてしまうため、利用者の利便性が向上するわけではない。
3. Web ブラウザに拡張機能が必要になるため、スマートフォンでは利用できない。

Password Based SSO は、あくまで SSO が利用できない場合の次善の策であり、利用を推奨するものではない。

■ 提言

SSO は、法人がクラウドサービスを安全に利用するために最低限必要な機能である。SSO に非対応であるサービスは採用を見送ることが望ましい。サービス事業者は SSO に対応するべきである。

また先に述べたように、SSO を利用したいがために高価なライセンス費用が必要になることが多く、予算に限りがある場合は SSO が利用できないライセンスを選択することになる。クラウドサービス事業者は、下位のライセンスにおいても SSO を提供するように努めていただきたい。

4. 事業まとめ

本事業では、職員の業務効率化やシステム開発等のプロジェクトの標準化・最適化を進めるため、各種デジタルツールの導入実証を行うとともに、より効果的にこれらのデ ジタルツールを活用していくために必要となる管理のあり方について検討を行った。

既存の経済産業省基盤情報システムとは連携しない範囲で、将来的な省内活用を視野においた形で実験的にクラウド関連ツールの徹底活用を試み、その知見を今回報告書という形で取りまとめたものである。

本実証を進めるにあたり、特にデジタルツールを活用していくために必要となる管理のあり方については、モダンかつセキュアな業務インフラの考え方（ゼロトラストアーキテクチャの概念を取り込んだ構成）を念頭に検討を行っており、今後の省内活用だけでなく広く一般企業でも参考となる部分があるのではないかと考える。

5. Appendix

5 - 1 . 用語集

本書で使用する用語を以下に示す。

API

Application Programming Interface の略。

SaaS が提供するソフトウェアコンポーネント同士がプログラムを介して互いに情報をやりとりするのに使用するためのインターフェイスのこと。

APM

Application Performance Management の略。

アプリケーションの性能管理や監視を行うこと。

BYOK

Bring Your Own Key の略。

独自の暗号鍵をクラウド環境へ持ち込み、クラウド上のデータを暗号化して保護すること。

CASB

Cloud Access Security Broker の略。

組織が利用するクラウド・アプリケーションについて可視化、データ・プロテクション、ガバナンスを実現するサービス・製品のこと。

CVSS

Common Vulnerability Scoring System の略。

詳細は以下 URL を参照のこと。https://www.ipa.go.jp/security/vuln/CVSS.html

DLP

Data Loss Prevention、または Data Leak Prevention の略。

DLP は情報漏えいを検出・防ぐことを目的とするセキュリティツール、またはシステムのこと。

EDR

Endpoint Detection and Response の略。

ファイルベースのマルウェア攻撃を防御し、悪意あるアクティビティを検知して、動的なセキュリティインシデントとアラートに対応する際に必要な調査・修正機能を提供する目的でエンドポイント・端末上に展開されるセキュリティツール、またはシステムのこと。

FIDO2

Fast IDentity Online 2 の略で FIDO が推進する認証技術の名称の一つ。 指紋認証や顔認証、虹彩認証といった「パスワードを使わない認証情報」を専用のハードウェアやソフトウェアを利用せずにオンライン上でやりとりするための認証技術のこと。 詳細は以下 URL を参照のこと。

https://fidoalliance.org/%E4%BB%95%E6%A7%98%E6%A6%82%E8%A6%81/

IaaS

Infrastructure as a Service の略。

利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースであり、利用者はオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し、実行できる。

利用者は基盤にあるインフラストラクチャをコントロールできないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント（例えばホストファイアウォール）についての限定的なコントロール権をもつサービスのこと。

IDaaS

Identity as a Service の略。

IdP のクラウドサービスのこと。

IAM

Identity & Access Management の略。

デジタルアイデンティティとその権限を管理すること、または、その機構（ID 基盤）と、アクセスする際の一連のプロセス（制御）を管理する機構（IdP）を有するツール、またはシステムのこと。

IDS

Intrusion Detection System の略。

ネットワーク通信を監視し、悪意のある第三者からのアクセスや侵入を検知・通知するシステムのこと。

IdP

Identity Provider の略。

デジタルアイデンティティ情報を管理し、分散システムに対する認証・認可を提供するシステムのこと。認証基盤とも呼ばれる。従来型の代表的な認証基盤である LDAP と異なり、主に SAML や OpenID Connect、OAuth などのシングルサインオンに対応したプロトコルを扱う。

IoC

Indicator of Compromise の略。

サイバー攻撃を受けた際の痕跡となるさまざまな指標のこと。

IPS

Intrusion Prevention System の略。

ネットワーク通信を監視し、悪意のある第三者からのアクセスや侵入を検知・遮断・通知するシステムのこと。

MDM

Mobile Device Management の略。

PC やスマートフォン、タブレットなどを一元的に管理するための仕組みのこと。

OAuth

権限の認可（authorization）を行うためのオープンスタンダード。詳細は以下 URL を参照のこと。

https://www.openid.or.jp/document/

OIDC

OpenID Connect の略。

OAuth 2.0 プロトコルの上にシンプルなアイデンティティレイヤーを付与したもの。シングルサインオンに利用される。詳細は以下 URL を参照のこと。

https://www.openid.or.jp/document/

PaaS

Platform as a Service の略。

利用者に提供される機能は、クラウドのインフラストラクチャ上に利用者が開発または購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたもの。

利用者は、基盤にあるインフラストラクチャをコントロールすることはできない。一方、利用者は自身が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権をもつ。

PIN

Personal Identification Number の略。

記憶シークレットの一種で、数字で表現されるもの。

SaaS

Software as a Service の略。

利用者に提供される機能は、クラウドのインフラストラクチャ上で稼動しているプロバイダ由来のアプリケーションのこと。アプリケーションには、利用者のさまざまなデバイスから、Web ブラウザあるいはプログラムインターフェイスを通じてアクセスする。

利用者は基盤にあるインフラストラクチャをコントロールすることはできない。

SAML

Security Assertion Markup Language の略。

OASIS（Organization for the Advancement of Structured Information Standards）によって策定された、異なるインターネットドメイン間でユーザー認証を行うための XML をベースにした標準規格のこと。シングルサインオンに利用される。

SCIM

System for Cross-domain Identity Management の略。

ユーザープロビジョニングの自動化を可能にするオープン標準規格のこと。

SIEM

Security Information Event Management の略。

ターゲットを絞った攻撃やデータ侵害を早期に検出するためにイベント・データをリアルタイムで分析し、インシデント対応、科学捜査、規制へのコンプライアンスのためにログ・データを収集、保存、調査、レポートするシステムのこと。

SSO

Single Sign-On の略。

端末の OS やグループウェア、Web アプリケーション、クライアント・サーバー型アプリケーション等に一括してログインすること。利用者は、SSO システムに 1 度だけログインすれば、利用可能なアプリケーション個別にログインすることなく利用きる。

VPN

Virtual Private Network の略。

通信事業者のネットワークやインターネットなどの公衆ネットワーク上で、暗号化機能を利用して構築する仮想的な専用ネットワークの総称。

エンドポイント

端末のこと。詳細は「端末」を参照のこと。

コンテキスト

文脈を意味する。ゼロトラストにおけるコンテキストは、ユーザー、端末、場所、アプリにもとづく文脈を意味する。

スプーフィング

送信元を偽装して行う攻撃手法のこと。

トラストアンカー

デジタルアイデンティティのおける信頼の基点のこと。

デジタルアイデンティティでは、アカウントに対して権限を付与して、さまざまなシステムを利用したり情報にアクセスすることを許している。アカウントを利用する際には認証を行って、本人であることを確認する。この時、アカウントを発行した相手が確実に意図したその人であることを信頼できることが必要となる。このように、デジタルアイデンティティの信頼性は連鎖している。その信頼の基点のことをいう。日本語では「信頼の基点」と呼ぶ。認証の手続きを行う際に、何をトラストアンカーにするのかは、予め定められたポリシーに従う。

プロビジョニング

設備やサービスに新たな利用申請や需要が生じた際に、資源の割り当てや設定などを行い、利用可能な状態にすること。

リモートワイプ

PC や携帯電話、スマートフォンなどのモバイル端末を遠隔で操作し、端末に保存されているデータを削除する機能およびサービスのこと。

端末

ネットワークの末端に接続され、他の機器と通信を行う主体となる機器のこと。特に利用者が直接操作する機器を指す。文脈上、PC を端末、スマートフォンやタブレットをモバイル端末と表現することが多い。

5 - 2 . 採用するクラウド事業者の評価

採用するクラウド事業者の客観的評価については、以下に示す別添資料を参照のこと。

クラウドサービス名	ファイル名
AWS Key Management Service	AWSKMS_CCI.pdf
Microsoft Azure Active Directory	AzureAD_CCI.pdf
Backlog	Backlog_CCI.pdf
Box	Box_CCI.pdf
Datadog	Datadog_CCI.pdf
CloudGuard Dome9	Dome9_CCI.pdf
Druva inSync	Druva_CCI.pdf
Microsoft Exchange Online	ExchangeOnline_CCI.pdf
GitHub	GitHub_CCI.pdf
Google Marketing Platform	GoogleMarketingPlatform_CCI.pdf
Microsoft Intune	Intune_CCI.pdf
Jamf Pro	Jamf_CCI.pdf
mxHero	MxHero_CCI.pdf
Slack Enterprise Grid	SlackEG_CCI.pdf
Zendesk	Zendesk_CCI.pdf

5 - 3 . 各サービスおよび採用するサブスクリプションモデルの SLA と SLO

別添資料『各サービスおよび採用するサブスクリプションモデルの SLA と SLO』参照のこと。

5 - 4 . ベンダーロックインの可能性とポータビリティ

別添資料『ベンダーロックインの可能性とポータビリティ 』参照のこと。

5 - 5 . 政府専用サービスの有無

本事業で採用するクラウドサービスについて、日本国政府が専用で利用できるサービスは存在しなかった。

5 - 6 . 検証実施サービスの各機能と留意事項

別添資料『検証実施サービスの各機能と留意事項』参照のこと。

（様式２）

二次利用未承諾リスト

報告書の題名：令和２年度経済産業省デジタルプラットフォーム構築事業報告書　ＤＸオフィス関連プロジェクト管理業務等の効率化に関するデジタルツールの導入実証・調査事業

委託事業名：令和２年度経済産業省デジタルプラットフォーム構築事業（ＤＸオフィス関連プロジェクト管理業務等の効率化に関するデジタルツールの導入実証・調査事業）

受注事業者名：
株式会社クラウドネイティブ

頁	章番号	タイトル
89	5-2	採用するクラウド事業者の評価

METI

経済産業省様向け

BYOD ポリシー雛形

2021 年 3 月

経済産業省
Ministry of Economy, Trade and Industry

目次

1. はじめに

1 - 1 . 文書の目的

本文書は、日本国政府の政策文書や BYOD（Bring Your Own Device）の要件文書ではない。

本文書は、音声およびデータ通信のための安全な環境を維持する必要性と相まって、個人所有のデバイスの使用を含む政府調達基準の要件を満たしながら、効果的なソリューションを選定するための最低限のガイドライン、考慮事項、および推奨事項の考慮したポリシーを提供することを目的としている。

なお本文書では、経済産業省職員ならびに企業とその従業員、および関係者を包括して、「職員」と呼称する。

BYOD ポリシーは、職員のサインアッププロセス、トレーニング、利用者契約、承認されたデバイス、モバイルセキュリティ、利用者サポート、アクセス可能なデータソース、コストと使用方法の問題、職員のプライバシー、および継続的なコンプライアンスと手順に対応している。本文書は職員が利用するためのポリシーを提供しているが、採用する各局課は、職員の参加、サインアップ、トレーニング、セキュリティ要件、参加資格のあるグループまたは個人、コスト削減の機会、標準化、簡素化のニーズを満たすために採用される最終的なソリューションについて、それぞれのプロセスに合わせて調整する必要がある。

1 - 2 . BYOD の定義

本文書は、経済産業省関連業務における職員の個人的なデバイスの自主的な使用を取り上げるものである。本文書は、組織が所有するデバイスの個人的な使用に対処することを意図したものではない。BYOD プログラムでは、職員が、業務関連の通信、データアクセス、および組織が所有するアプリケーションの使用のために個人のデバイスを使用できる。これらのデバイスには、PC およびスマートフォンやタブレットが含まれる。

ほとんどの組織では、電子メール・プラットフォームやその他のシステムにアクセスする多くのデバイスがあるが、それらは事前に承認されていない可能性があり、組織が利用実態を掌握できているとは言えない。BYOD プログラムを適切に定義して実施することで、承認プロセスの下でこれらのデバイスを管理し、リスクを排除できる。BYOD プログラムが適切に実施されていれば、便利さ、スタッフの生産性の向上、セキュリティの向上、および組織のコスト削減の可能性を提供できる。また BYOD プログラムは、職員が自分のデバイスを介して接続するための公式のガイドラインと要件を作成し、IT チームが適切な管理、制御、およびコンプライアンスを確保できるようにする。

2. BYOD のポリシーとパラメータ

本章では、個人所有のデバイスを用いて、職員が業務を行うための基本的なポリシーを定めている。BYOD 要件の程度は各局課によってさまざまである。従って本ポリシーは、さまざまな技術を使用して多様な組織リソースへのアクセスを可能にすると同時に、各局課がニーズに応じて BYOD プログラムを構成できるようにするための十分な柔軟性を意図している。各局課は、特有の法的および技術的な問題に直面している可能性があり、

プログラム・ポリシーおよび利用者同意書を適切に調整する必要がある。そのプログラムを積極的に分析し、適切に修正することは、承認されたプログラムの所有者の責任である。

本章では、「プログラム」とは、ハードウェア、ソフトウェア、およびポリシーを含む、個人所有の デバイスにエンタープライズアクセスを提供するシステムを指す。

「プライベート」とは、デバイス所有者が個人的な機能に使用するデバイスの部分を意味する （アプリケーション、電話、メッセージング、データ保存など)。「組織的」とは、組織データの処理または保存に使用されるデバイスのコンポーネントを指す。政府調達基準を満たし、個人所有のデバイスが組織にアクセスするために使用される可能性のある、多くの異なる技術（例：コンテナ、仮想デスクトップ、Web ブラウザ）があるが、これはデバイスの「組織的な」コンポーネントがプログラムによって異なることを意味する。

2 - 1 . TCO の見直し

BYOD を採用する各局課がコスト構造を評価する際は、総所有コスト（TCO：Total Cost of Ownership）モデルを見直す必要がある。TCO の観点から計算しない場合、デバイス・コストまたはサービス・プラン・コストを排除または削減することで達成された金銭的節約が、BYOD プログラムの管理やソフトウェアなどの他の分野でのコスト増加から相殺される可能性がある。

コストを評価する最良の方法の 1 つは、BYOD にかかる総コスト分析を行うことである。

各局課は、BYOD の実施に伴う各コスト要因への影響を判断する必要がある。各局課が BYOD で考慮すべき関連コスト・カテゴリーのいくつかを以下に示す。

- 音声・データプランと利用方法
- アクセサリー - IC カードリーダーなど
- EMM / MDM ソフトウェア
- エンドポイントセキュリティ
- その他のエンド利用者向けクライアントライセンス
- 生産性の向上
- ヘルプデスク/サービスデスク
- 省庁支給デバイス vs. BYOD プログラム管理
- IT その他の開発費
- エンジニアリングまたは技術サービス

2 - 2 . 自主的な参加

職員の BYOD プログラムへの参加は、自発的なものであるものとする。経済産業省、および各局課は、いかなる状況においても、職員に対して公務のために個人所有のデバイスを使用するように指示・要求してはならない。公務遂行のためにデバイスの使用を必要とする役割を割り当てられた職員は、経済産業省、または各局課の支給するデバイスを使用する選択肢を持たなければならないが、利便性や個人的な好みを考慮して、個人所有のモバイル・デバイスを自主的に使用することを選択できる。デバイス所有者に発生した費用を職員に払い戻しても、プログラムの自主的な性質は変更できない。

2 - 3 . デバイスの所有権の承認

BYOD プログラムは、職員が所有するデバイスを対象とする。各局課は、政府調達基準を満たすデバイス、オペレーティング・システム（OS）、および OS への必要なアップデートの承認済みリストを使用することが望ましい。承認済みリストには以下のものを含むが、これらに限定しない。

デバイス

- Windows の場合は、TPM 1.2 以上互換のセキュリティチップの搭載

オペレーティング・システム

- Windows 10 Professional
- macOS
- iOS
- Android

OS への必要なアップデート

- Windows 10 バージョン 1709（OS ビルド 16299.1085 KB4493441）以降
- 10.13（High Sierra）以降 ※M1 チップ搭載の macOS 除く
- iOS 11.0 以降
- Android 6.0 以降

2 - 4 . デバイスの没収

個人所有のデバイスが物理的破壊、電子的検索、工場出荷時の再設定およびデバイスのワイプのために没収される可能性がある。没収は一時的または恒久的なものである場合がある。個人所有のデバイスを没収するためには、BYOD プログラムは正当な要件（機密情報漏洩など）を定義し、プログラムポリシーに文書化すること。また、プログラムポリシーについて利用者である職員の同意を事前に得ること。プログラムポリシーに対する事前の利用者の同意が、利用者同意書によって対処され、取得されること。没収につながるさまざまな状況の定義には以下のものを含むが、これらに限定しない。

- マルウェアの感染や機密情報漏洩、および犯罪捜査に係る調査（フォレンジック）のための保全活動
- BYOD プログラムからのオプトアウトや職員資格の停止、および退職・異動に伴う、デバイス上からの機密性 1、2 に該当する情報の消去
- 法的執行によるデバイスの差し押さえ

2 - 5 . 接続状態と非接続状態でのリモートワイプ

DRM などを利用したファイル単位でのアクセス制御を実施することができない場合は、リモートワイプによるファイルの削除を行う必要がある。この時、デバイスの没収がなんらかの理由で遂行できない場合、インターネット接続状態および非接続状態でのリモートワイプが行われる可能性がある。個人所有のデバイスをリモートワイプするには、BYOD プログラムは正当な要件（機密情報漏洩など）を定義し、プログラムポリシーに文書化すること。また、プログラムは利用者である職員の同意を事前に得ること。プログラムポリシーに対する事前の

利用者の同意が、利用者同意書によって対処され、取得されること。リモートワイプにつながるさまざまな状況の定義には以下のものを含むが、これらに限定しない。

なお、インターネット接続状態の場合は OS を含む全領域が対象となる。非接続状態の場合は、事前に定義された領域が対象となる。

デバイス没収が行えない状況

なんらかの理由でデバイスの没収が行えない場合、インターネット接続状態、または非接続状態でのリモートワイプを行う。

デバイスの紛失

職員からの申請に基づき、紛失したデバイスからの情報漏えいを防止する目的でリモートワイプを行う。

一定期間のインターネットアクセスの途絶

なんらかの事情により、職員からの申請が行えない状況を考慮して、一定期間のインターネットアクセスが途絶したデバイスの保護領域に対して、リモートワイプを行う。

2 - 6 . プライベートエリアと組織的なエリアの分離

職員は、個人所有のデバイスが組織のデータにアクセスするために使用されている場合でも、個人所有のデバイスのプライバシーについては、合理的な期待をもっている。これを容易にするために、BYOD プログラムおよび技術は、デバイスのプライベート部分と組織的な部分の分離を確実にすることを意図して設計する。しかし、実装が不完全である可能性があり、その結果プログラムがデバイスのプライベート部分へのアクセスを必要とする状況が発生する可能性がある場合、プログラムはデバイスのプライベート部分を検索する権利を留保する。

各局課は、デバイスのプライベート部分と組織的な部分の分離を行うために、設計に以下を盛り込むが、これらに限定しない。

PC（Windows、macOS）

- MDM を用いて組織のデータにアクセスするための設定を配布する際、利用者プロファイルをプライベートで利用するプロファイルとは別に作成する設計とすること。
- プライベートで利用するプロファイルとは分離されたプロファイルにおいて、操作情報や保有するデータを検索すること。

モバイルデバイス（iOS、Android）

- MDM や MAM を用いてモバイルデバイス内に組織のデータを保存しない設計とすること。
- 操作情報や保有するデータの検索は行わないこと。

2 - 7 . アプリケーションとデータの分離

BYOD プログラムポリシーと利用者同意書は、組織的な目的のためにどのアプリケーションが使用される可能性があるかを特定する。これは、モバイルデバイスの所有者である職員が、デバイスのプライベート部分をエンタープライズデータで 不用意に汚染しないことを確実にするためである。各局課のプログラム設計者は、利

用者がどのようなエンタープライズ機能を必要とするかを検討し、それらの 機能をプライベート側から切り離すことを可能にするツールやアプリケーションが、デバイスの組織的な部分内で利用可能であることを確認すること。

各局課が選定する組織的な目的のための機能を、プライベート側から切り離すことを可能にするツールやアプリケーションとしては以下が挙げられるが、これらに限定しない。

- Box for EMM
- Slack for EMM
- Microsoft Teams
- Microsoft Edge
- Microsoft Office
- Tableau Mobile
- Zoom.us

2 - 8 . デバイス設定

BYOD プログラムは、組織情報のセキュリティを確保するために、個人所有のデバイス設定（最小長のデバイスアクセス PIN など）を適用、制御する必要がある。デバイス設定は、アクセスのレベル、情報の機密性、アクセスを可能にする技術、およびその他の要因にもとづいて、プログラムによって異なる。利用者同意書を通じて、プログラムに参加する職員は、プログラムに参加する前に、個人所有のモバイルデバイス上でのエンタープライズセキュリティコントロールの適用または変更に同意すること。

2 - 9 . 第三者アクセス

デバイスに適用される BYOD プログラムのセキュリティ管理とポリシー、およびエンタープライズおよびデバイスの組織的な部分へのアクセスを確保する技術がある場合に応じて、プログラムはデバイスの所有者にデバイスの使用を制限する場合がある。またデバイスの紛失、盗難、または家族を含む不正な第三者によるアクセスがあった場合、プログラムを管理する局課は直ちに通知を行う場合がある。

2 - 10 . 時間外労働

組織のシステムへのアクセスに個人所有のデバイスを使用しても、時間外承認ポリシーは変更されない。経済産業省、および各局課から支給されるデバイスの使用に適用される時間外承認のためのローカル ポリシーおよび手順は、職員がエンタープライズ アクセスのために個人所有のデバイスを使用する方法と時期を管理するために使用する。

2 - 11 . 受け入れ可能な使用

個人的なデバイスの使用についての承認は、職場での許容される行動の基準を変更するものではなく、経済産業省、および各局課から支給されるデバイスの使用に関する制限は、承認を受けた職員の個人的なデバイスにも

適用される。利用者同意書は、デバイスの使用が全ての適用される使用ガイダンス（各局課の受け入れ可能な使用方針など）に従うことを明確に示すこと。

2 - 12 . 知的財産

BYOD プログラムにもとづいて承認を受けた個人デバイス使用時に作成された知的財産については知的財産が個人的な時間に作成されたか否かにかかわらず、職員が職務上の必要により知的財産を作成した場合には、経済産業省、および各局課から職員個人に知的財産の所有権の移転・付与はなされないことを明確に示すこと。

2 - 13 . 賠償責任と安全性

経済産業省、および各局課の公式な目的のために個人所有のデバイスを使用する際においても、利用者が適用される全ての安全関連の法律、規制、およびポリシー（運転中のモバイルデバイスの使用禁止など）を遵守するという要件は免除しない。このことは、利用者契約書に明記すること。責任の観点からは、個人所有のデバイス、経済産業省および各局課から支給されるデバイスのいずれであっても、業務目的で使用することに大きな差異はなく、職員が個人のデバイスを職務に利用する目的で使用する場合においても、経済産業省や各局課から支給されるデバイスの安全な使用を規定しているのと同様の規則と方針を適用すること。

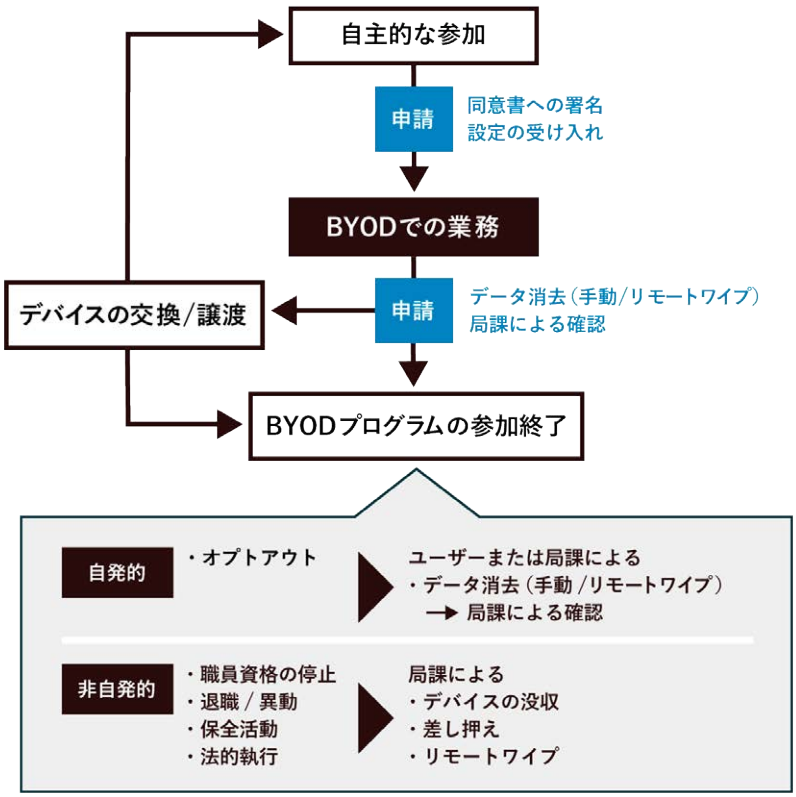
2 - 14 . デバイスのアップグレード、または所有権の譲渡

組織データを確実に削除するために、BYOD プログラムに参加している職員は、個人所有のデバイスを新しいモデルにアップグレード（現有デバイスの廃棄）するか、または所有権を他の個人（第三者または家族）に譲渡する前に、各局課へ通知を行い、書面による承認を受けるか、または経済産業省のデバイス管理者に通知し、デバイスからアプリケーションやデータなどの政府コンテンツが消去されていることを確認すること。正確なプロセスは経済産業省で策定し、利用契約書に記載されること。その目的は、デバイスのアップグレードを妨げることではなく、デバイスがアップグレードされるなどの端末変更が行われた際にも、他の個人の使用のために提供される前に、全ての適切なセキュリティ対策が取られていることを確実にすることである。利用者同意書は、デバイスのアップグレードまたは譲渡が、プログラムへの参加を自動的に終了させることを記載すること。

2 - 15 . BYOD プログラムの参加終了

承認された個人所有のデバイスを自主的に使用する職員は、参加終了時にエンタープライズデータとサポートするデータ分離技術を、デバイスから削除することに同意すること。BYOD プログラムへの参加は、利用者が自発的に終了させることも、組織が指示することも、個人が自発的または非自発的に組織から離脱した結果として終了させることもできることとする。デバイスのプライベートな部分からのデータ損失を制限するためにあらゆる試みがなされるべきであるが、不注意によるデータ損失を排除することはできない。利用者同意書は、潜在的なデータ損失、デバイスの検索、およびあらゆる償還の考慮事項を記載すること。

BYOD プログラムの参加から終了までのライフサイクルを以下に示す。



3. 行動規範とガイドライン

3 - 1 . 行動規範

BYOD プログラムを実施する全ての各局課は、本書の Appendix に記載されている利用者契約書の例と同様に、以下の利用者・ガイドライン・サマリーおよび管理ガイドライン・サマリーを参照する必要がある。これらのガイドラインは、利用者の行動に責任を持ち、情報セキュリティに責任をもつことを目的としている。行動規範は、知識のあるユーザーがセキュリティ・プログラムを成功させる基盤であるという事実を認識し、行動基準を確立する。プログラムの利用者は、自分のデバイスとそれに含まれるデータのセキュリティに個人的な責任を負うことが、仕事の重要な部分であることを理解する必要がある。これらのガイドラインは、BYOD プログラムに自発的に参加する全ての職員に適用される。参加する全ての職員は、セキュリティ・ポリシーを十分に認識し、これを遵守する必要がある。

3-1-1 . 利用者行動規範の概要

- BYOD プログラムへの参加は任意であり、職員はいつでも解消できる。

- 参加者は、確立された全ての省庁の行動規則および関連する省庁の IT セキュリティガイダンスを遵守し、倫理に基づき、信頼できる方法で行動するものとする。
- 参加者は、BYOD プログラムの一部としてインストールされた技術的または管理上の制御または構成を上書きしようとしてはならない。ただし、利用者や省庁が管理するソリューションの構成プロファイルを自己削除して参加を自主的に終了し、利用者のデバイスから全ての業務に係るコンテンツが自動的に失われる場合を除く。
- 参加者は、経済産業省、および各局課の方針に従った BYOD プログラムによって許可された場合を除き、行政情報システム上で取り扱われる情報を個人のデバイスにダウンロードまたは転送しない。
- 参加者は、BYOD ソリューションで必要とされる場合、電子メールの添付ファイルを閲覧するプロセスを通じて不注意でダウンロードされたものなど、デバイスに保存される可能性のある業務関連の機密ファイルを削除することに同意するものとする。
- 参加者は、通信事業者のサービスプラン費用および通信事業者が払い戻しの対象とならないその他の費用を負担するものとする。
- 参加者は、携帯電話やスマートフォンの使用に関する法律を遵守するものとする。例えば、運転中の利用制限などを指す。
- BYOD プログラムを介した機関の IT リソースへのアクセスは、経済産業省の情報技術セキュリティポリシーに準拠する。
- 参加者は、政府の情報や情報資源の確保に万全を期すものとする。
- 参加者は、BYOD デバイスの譲渡、廃棄、アップグレードを行う前に、ヘルプデスクまたはその他の指定された連絡先に通知する必要がある。
- 参加者は、BYOD デバイスの盗難防止対策、不正使用対策など物理的に保護する必要がある。参加者は特に、旅行中の紛失に注意する必要がある。機関の BYOD プログラム・パスワードに加えて、デバイス・パスワードの使用を推奨する。
- 参加者は、BYOD デバイスの紛失または盗難を直ちにヘルプデスクまたはその他の指定された連絡先に報告し、デバイス管理ソリューションのリモートワイプを行うこと。
- 参加者は、経済産業省のパスワードポリシーに従うものとし、ログインスクリプト、バッチファイル、またはデバイスの他の場所にパスワードを保存しないなど、他の個人によるアクセスからパスワードを保護すること。
- 参加者は、セキュリティ上の事故、または不正行為、浪費、またはシステムの不正使用の疑いがある場合は、直ちに適切な連絡窓口に報告すること。
- 参加者は、オリジナルのデバイスのオペレーティングシステムを維持し、メーカーがリリースしたセキュリティパッチやアップデートでデバイスを最新の状態に保つことに同意するものとする。
- 参加者は、デバイスを「脱獄」または「ルート化」など標準的な内蔵セキュリティ機能や制御を迂回できるようにするソフトウェアのインストールをする行為をしてはならない。
- 参加者は、業務上の利用のために、デバイスを他の個人や家族と共有しないことに同意するものとする。

3-1-2 . 運営ガイドラインの概要

以下にまとめる運営ガイドラインでは、各局課にそれぞれに責任をもつ具体的な管理資源を特定することを要求する。

- 経済産業省は、職員が適切な承認なしにプログラムに参加していないことを保証すること。

- 各局課は、職員がプログラムに参加するためのビジネス上の必要性が存在することを確認するために、毎年認可を見直すこと。管理職は、終了すべきアカウントを特定すること。
- 各局課は、BYOD プログラムへの参加を認められた職員が、準拠すべき IT セキュリティポリシー、ガイドライン、および手順に従うことを保証するものとする。
- 各局課は、BYOD プログラムに参加している職員の離職、異動、または部門からの解雇を担当部門に通知し、担当部門が適切な措置を講じるようにするものとする。

3 - 2 . 違反した場合の罰則

全ての参加者は、BYOD プログラムによって提供される利用契約書に記載されている、行動規則およびエンド利用者・ガイドラインを遵守する必要がある。行動規則並びに利用者契約書に署名することで、参加者は、特定された全ての条件を理解し、受け入れ、遵守することに同意したことを示す。これらの規則に従わない場合、口頭または書面による警告、システム・アクセスの削除、解雇、または罰金で罰せられる軽犯罪の有罪判決を受ける可能性がある。

4. BYOD の適用範囲

各局課が BYOD を採用するためには、全体的な BYOD 適用範囲の戦略が必要である。既存の BYOD およびテレワークの展開から学んだ教訓を活用した BYOD の適用範囲を以下に示す。

- BYOD は、BYOD ポリシーを適用したデバイスであっても、経済産業省や各局課が支給するデバイスの実装と同等に安全であると考えるべきではなく、経済産業省や各局課の業務を補完するために使用され、経済産業省や各局課が支給するデバイスを代替するものではない。
- BYOD デバイスは、位置情報追跡データプログラムの適用範囲内で利用されるべきであることが望ましい。
- 各局課が個人のデバイスを活用すべきではない条件を以下に示す。
    - 高度な戦術環境 - 個人デバイスは、敵対者から利用者を保護するための適切なセキュリティ対策（ジオロケーション、トランスミッションセキュリティなど）が施されていないため、戦術的なオペレーションに使用すべきではない。
    - 機密性の高いミッション - 個人のデバイスは、機微情報取り扱いの要件を満たしていないため、機密情報を処理したり、機密環境で操作したりするために使用すべきではない。
    - VIP 通信 - 上級レベルのデータを処理する個人的なデバイスは、上級リーダーに対しての攻撃や追跡の可能性を高める。
    - 経済産業省や各局課が支給するデバイスが提供する追加のデータ保護を必要とするその他の高度に機密性の高いミッションに使用すべきではない。
- 各局課は、BYOD デバイスがアクセスする情報システムに見合った適切な Identity およびアクセス管理ソリューション（NIST SP 800-63-3 参照）を明確に特定すること

5. APPENDIX：利用者同意書例

以下は、各局課が使用し、カスタマイズできる利用規約の例である。

上記の参照されたポリシーと行動規則に従わなかったことを理由に、アクセス権限を制限したり取り消したり、その他の管理上または法的措置を取ることは、[局課名]の権利です。これらの規則に違反した場合、懲戒処分の根拠となり、解雇を含む懲戒処分を受けることがあります。

認定された個人用デバイスには、Windows、macOS、および iPhone、iPad、Android ベースの携帯電話およびタブレットで、「脱獄」または「ルート化」されていないものが含まれます。個人用デバイスは、TPM1.2 互換のセキュリティチップが搭載されている必要があります。Windows デバイスの場合は、Windows 10 Pro バージョン 1709 以降、macOS デバイスの場合は、10.13 （High Sierra）以降、Apple デバイスの場合は iOS バージョン 11 以降、Android デバイスの場合はバージョン 6.0 以降である必要があります。利用者は、デバイスが電子政府推奨暗号リスト、および携帯用暗号化デバイスの業界標準に準拠していることを確認する必要があります。この規格に準拠していないデバイスを購入した場合、この BYOD ポリシーとは互換性がありません。

この契約書に署名することで、BYOD 利用者はこれらの条件に同意したことになります。

- BYOD 利用者である私は、使用しているデバイスのサービスおよびメンテナンスに関連する全ての費用に責任を負う。これには、全ての国際料金およびローミング料金、BYOD アプリケーションの使用に関連するデータ使用、モバイル・デバイス・アクセスのための追加料金等が含まれるが、これらに限定しない。
- 機密情報が流出した場合、アプリケーションや関連するアプリケーションの削除が必要となり、私の個人的なデバイスが完全に破壊される可能性がある。
- 個人デバイスのセキュリティ設定が、組織が定める基準に適合するよう変更される可能性がある。
- BYOD アプリケーション内で許可されたデータ使用以外に、私の個人デバイスに組織からのデータを保存、転送、またはその他の方法で意図的に保持しない。
- 政府の BYOD アプリケーションの利用者として、私は、自宅や旅行先であるかどうかに関わらず、私のアプリケーションおよびデータは [局課名]に対してのプライバシーの保護を期待せずに、無制限に監視されることに同意する。
- 法執行や情報セキュリティを含む公的な目的のために検査やフォレンジック評価が必要な場合、私は個人のデバイスを適切な当局に引き渡す事に同意する。私の個人的なデバイスは、調査および証拠保全の目的で無期限に保管され、永久押収または破壊の対象となる可能性があることに同意する。
- BYOD/アプリケーションへのアクセスは、管理された環境で、安全な接続（すなわち、安全な Wi-Fi）の下で使用する。公共 Wi-Fi または他者の携帯電話のデータ接続と同様に、デバイスからエンタープライズ・アプリケーションにアクセスすると、第三者が企業のリソースとの通信を盗聴あるいは傍受することで、国民の個人データが危険にさらされる可能性があることを理解している。既知の環境下で信頼できるネットワークを介してエンタープライズ リソースにアクセスする際には、利用者として細心の注意を払うことが、データの損失を防ぎ、利用者、利用者のデータ、および組織のリスクを軽減するための最善な方法であることを理解している。

私は、[局課名] サービスの BYOD 利用に適用される上記のセキュリティポリシーと行動規則を認め、理解し、遵守します。私は、[局課名]が提供するサードパーティ製ソフトウェアを追加すると、私の個人デバイスの利用可能なメモリやストレージが減少する可能性があること、およびサードパーティ製ソフトウェアの使用および本プログラムでのデバイスの使用に起因するデバイスの損失や盗難、損傷、故障について、[局課名]は一切の

責任を負わないことを理解しています。私は、サードパーティ製ソフトウェアのトラブルシューティングやサポートのためにベンダーに連絡することは私の責任であり、[局課名]が提供する限定的な設定サポートやアドバイスは私の責任であることを理解しています。私は、組織ミッションでの使用により、個人の月々の通信費や通話料などにおけるサービスプラン費用が増加する可能性があることを理解しており、経済産業省、および[局課名]からの払い戻しが提供されないことを理解しています。

後日、BYOD プログラムへの参加を中止することを決定した場合、私は[局課名]が提供するサードパーティ製のソフトウェアおよびサービスを個人のデバイスから削除し、無効にすることを許可します。

職員名：_____

BYOD デバイス：_____

接続する業務システム：_____

デバイスにインストールされているアンチウイルスまたはその他のセキュリティソフトウェア

_____

職員の署名：_____日付：_____

6. 出典

（MSCT） Bring Your Own Device （BYOD） Guidance 2018/5/3

https://hallways.cap.gsa.gov/system/files/MSCT%20BYOD%20Guidance%20Report%20FINAL%20-%203May2018-1530555996.docx

クラウドサービス名	ベンダーロックインの可能性	データのポータビリティ	参考サイト
AWS Key Management Service	現時点でBoxとSlackがBYOKとして用いる基盤は、AWS Key Management Serviceのみであるため、事実上のベンダーロックイン状態である。	Customer Managed Key（CMK）として登録した秘密鍵をエクスポートする手段はない。 関連するURLを参考サイトに記載する。	https://d1.awsstatic.com/whitepapers/International/jp/KMS_Cryptographic_Details_JP.pdf
Backlog	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低い	件数の上限はあるが、課題とコメントをエクスポートすることは可能である。 関連するURLを参考サイトに記載する。	https://backlog.com/ja/enterprise-help/userguide/userguide1908/
Box	現時点において、BYOKに対応しているクラウドストレージは、Boxのみであるため、事実上のベンダーロックイン状態である。	クラウドストレージ各社で移行手順を用意している。例として、Onedriveへの移行について、参考サイトに記載する。	https://docs.microsoft.com/ja-jp/sharepointmigration/box-to-onedrive-and-sharepoint-migration-guide
CloudGuard Dome9	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	利用者のデータを保持しないサービスであるため、対象外とする。	
Datadog	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	取り込んだログをエクスポートすることが可能である。また、アーカイブしたログをAWS S3に保存することが可能である。 関連するURLを参考サイトに記載する。	https://docs.datadoghq.com/logs/explorer/ https://docs.datadoghq.com/ja/logs/archives/?tab=awss3
Druva inSync	同水準の機能を提供するサービスが見受けられないため、事実上のベンダーロックイン状態であると考える。	バックアップデータは管理者によりダウンロードできるが、データサイズが大きいことから、その実施は容易ではない。 関連するURLを参考サイトに記載する。	https://docs-jp.druva.com/inSync/020_Backup_and_Restore/020_Backup_and_Restore/070_Back_up_and_restore_data/060_Download_user_data
Exchange Online	メールシステムの移行自体は可能であるため、ベンダーロックインの可能性は低い。メールセキュリティシステムとの連携を鑑みると、同等の機能を提供できる製品は限られてくるものと考える。	クラウド型メールサービス各社で移行手順を用意している。例として、Google Workspaceへの移行について、参考サイトに記載する。	https://support.google.com/a/answer/180898?hl=ja
Github Enterprise	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	ソースコード管理ツール各社で移行手順を用意している。例として、GitLabへの移行について、参考サイトに記載する。	https://www.tecmint.com/migrate-from-github-to-gitlab/
Google Analytics	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	レポートをエクスポートすることが可能である。関連するURLを参考サイトに記載する。	https://support.google.com/analytics/answer/1038573?hl=ja
Jamf Connect	類似の機能を持った製品は存在するものの、MDMの種類を問わず利用できる製品は見受けられないため、事実上のベンダーロックイン状態であると考える。	利用者のデータを保持しないサービスであるため、対象外とする。	
Jamf Pro	MDM機能の移行自体は可能であるため、ベンダーロックインの可能性は低い。本事業で実装している機能連携を鑑みると、同等の機能を提供できる製品は、限られてくるものと考える。	利用者のデータを保持しないサービスであるため、対象外とする。	
Microsoft Azure Active Directory	別のIdPを採用することは可能であるが、本事業で実装している制御を行える製品はほとんど見受けられないため、事実上のベンダーロックイン状態である。	IDや認証情報、SSO設定の可搬性はなく、再設定する必要がある	
Microsoft Azure Sentinel	先行のSIEM製品は多数存在するため、ベンダーロックイン状態ではない	データをBlobに順次エクスポートする機能が提供されているが、プレビュー段階である。 APIを用いたログの書き出しは可能であるが、1回のAPIで実行するクエリーが返すレコード数は、500,000行が上限であるため、注意が必要である。 関連するURLを参考サイトに記載する。	https://docs.microsoft.com/ja-jp/azure/azure-monitor/logs/logs-data-export?tabs=portal https://docs.microsoft.com/ja-jp/azure/azure-monitor/service-limits
Microsoft Defender for Endpoint	エンドポイントプロテクション機能として、同水準の機能を提供する製品は存在するが、認証機能と連携する製品は見受けられないため、事実上のベンダーロックイン状態である	Advanced Hunting機能やAPIを用いて、ログをエクスポートすることは可能であるが、エクスポート可能なレコード数が10,000レコード程度と限られているため、データ移行用途には適さない。そのため、ログをSIEMに順次転送するよう構成する必要がある。 関連するURLを参考サイトに記載する。	https://docs.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/raw-data-export-storage?view=o365-worldwide https://docs.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/enable-siem-integration?view=o365-worldwide
Microsoft Intune	MDM機能の移行自体は可能であるため、ベンダーロックインの可能性は低い。本事業で実装している機能連携を鑑みると、同等の機能を提供できる製品は、限られてくるものと考える。	利用者のデータを保持しないサービスであるため、対象外とする。	
mxHero	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	利用者のデータを保持しないサービスであるため、対象外とする。	
Netskope	日本語を用いたDLPに対応している製品が見受けられないため、事実上のベンダーロックイン状態である。	APIを用いたログのエクスポートが可能である。また、ログ収集コネクタを有するSIEMへのエクスポートが手段として挙げられる。 例として、Exabeamへの連携について、参考サイトに記載する。	https://www.exabeam.com/wp-content/uploads/2019/07/EXA_Solution-Brief_Netskope.pdf
Slack Enterprise Grid	現時点において、BYOKに対応しているチャットツールは、Slackのみであるため、事実上のベンダーロックイン状態である。	ワークスペースのデータをエクスポートすることが可能である。 関連するURLを参考サイトに記載する。	https://slack.com/intl/ja-jp/help/articles/201658943-%E3%83%AF%E3%83%BC%E3%82%AF%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%82%92%E3%82%A8%E3%82%AF%E3%82%B9%E3%83%9D%E3%83%BC%E3%83%88%E3%81%99%E3%82%8B
Zendesk	移行を阻害する要素は見受けられないため、ベンダーロックインの可能性は低いものと考える。	JSON、CSV、またはXMLファイルにデータをエクスポートすることが可能である。 関連するURLを参考サイトに記載する。	https://support.zendesk.com/hc/ja/articles/203662346-JSON-CSV-XML%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB%E3%81%B8%E3%81%AE%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E3%82%A8%E3%82%AF%E3%82%B9%E3%83%9D%E3%83%BC%E3%83%88

サービス名/サプスクリプションモデル名	SLA	SLO	参考サイト
AWS Key Management Service	99.90%	なし	https://aws.amazon.com/jp/kms/sla/
AWS S3	99.90%	なし	https://aws.amazon.com/jp/s3/sla/
Azure Active Directory	99.90%	なし	https://azure.microsoft.com/ja-jp/support/legal/sla/active-directory/v1_0/
Azure Sentinel	99.90%	なし	https://azure.microsoft.com/en-us/support/legal/sla/log-analytics/v1_3/
Backlogスタンダードプラン	なし	なし	https://support-ja.backlog.com/hc/ja/articles/360036151633
Box Enterprise	99.90%	なし	https://www.box.com/static/html/BSA_080113_jp.html
Datadog	99.80%	なし	https://www.datadoghq.com/legal/terms/2014-12-31/
Dome9	99.90%	なし	https://www.checkpoint.com/about-us/cloud-terms/
Druva inSync	99.50%	なし	https://www.druva.com/documents/druva-cloud-services-master-customer-agreement-20201209.pdf
Exchange Online	99.90%	なし	https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37
Github Enterprise	99.90%	なし	https://github.com/enterprise-legal/github-online-services-sla
Google Analytics（無償版）	なし	なし	https://marketingplatform.google.com/intl/ja/about/analytics-360/compare/
Jamf Connect	99.90%	なし	https://www.jamf.com/resources/product-documentation/hosted-services-availability-commitment/
Jamf Pro	99.90%	なし	https://www.jamf.com/resources/product-documentation/hosted-services-availability-commitment/
Microsoft Defender for Endpoint	99.90%	なし	https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37
Microsoft Intune	99.90%	なし	https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37
mxHero Platform	99.50%	なし	https://www.digitalmarketplace.service.gov.uk/g-cloud/services/862147093428668
Netskope	99.90%	なし	https://www.netskope.com/jp/support-terms
Slack Enterprise GRID	99.99%	なし	https://slack.com/intl/ja-jp/terms/service-level-agreement
Zendesk support suite Enterprise	Talkの使用状況：99.95%	なし	https://support.zendesk.com/hc/ja/articles/360057234534

METI

経済産業省
デジタルプラットフォーム構築

事業報告書:付録

検証実施サービスの各機能と留意事項

DX オフィス関連プロジェクト管理業務等の効率化に関する
デジタルツールの導入実証・調査事業

経済産業省デジタル・トランスフォーメーション室
株式会社 クラウドネイティブ

経済産業省
Ministry of Economy, Trade and Industry

クラウドネイティブ
CLOUD NATIVE INC.

目次

はじめに

本書では、検証を実施したサービスについての各機能の概要と留意事項を記述する。

記述項目は以下の通り。

- サービス名
- 選定したライセンス・プランとその選定理由、取得時の留意事項
- 機能概要
- 注記

なお、複数サービスで構成される場合、構成各サービスを併記している。また注記については、検証中に検証担当者が体験に基づき、注意を要すると判断した項目について記述している。

本文書で記述するサービスまたは製品群は以下の通り。

- Amazon Web Services
- Backlog
- Box
- CloudGuard Dome9
- Datadog
- Druva inSync
- GitHub Enterprise
- Google Analytics
- Jamf Pro
- Jamf Connect
- Microsoft Azure Active Directory
- Microsoft Azure Sentinel
- Microsoft Defender for Endpoint
- Microsoft Defender for Office365
- Microsoft Intune
- mxHero
- Netskope
- Slack Enterprise Grid
- Zendesk

> 注記
> 上記サービス内に含まれる機能のうち、本件検証にて利用しなかった機能については、記述していない。

1. Amazon Web Services

1 - 1 . ライセンス・プラン

機能を利用するための特別なライセンスプランは存在しないが、サポートサービスとしてビジネスサポートを契約している。

1 - 2 . 取得時の留意事項

AWS は、1 つの組織で複数の AWS アカウントを利用するための仕組みがあり、組織全体にルールを適用したり、支払い方法を管理できる。そのため、組織内の複数の部門で AWS を利用する際には、ばらばらに契約するのではなく、1 つの契約に統一するべきである。すでに組織内の他の案件で AWS を契約している場合は、個別に契約しないことを推奨する。

また、AWS の契約方法は大きく分けて 2 つある。クレジットカードを登録して直接契約する方法と、代理店を経由して契約する方法があり、後者の場合は請求書による支払いが可能になる。

1 - 3 . 機能概要

1-3-1 . AWS Key Management Service

AWS Key Management Service（AWS KMS）は、データの暗号化やデジタル署名に利用できる鍵管理機能を提供する。Box KeySafe や Slack EKM の BYOK 機能を使う際に、鍵を AWS KMS に登録して、API を通じて鍵を利用する。

1-3-2 . AWS CloudTrail

AWS CloudTrail は、利用している AWS サービスの利用状況をログに記録する機能を提供する。AWS の機能は全般的に API を通じて利用するように設計されており、その API の個々の呼び出し履歴をログとして記録することで、AWS を統制できる。

1-3-3 . Amazon S3

Amazon S3 は、汎用的なクラウドストレージである。利用者が直接利用する以外にも、AWS の各種サービスのデータを配置するために利用する。CloudTrail のログを S3 に保管するためにも利用する。

1 - 4 . 注記

AWS KMS は、利用するサービス側の指定により、対象となるリージョンが固定されている。Box KeySafe は米国西部（北カリフォルニア）、Slack EKM は米国東部（バージニア北部）を要求する。

2. Backlog

2 - 1 . ライセンス・プラン

利用するプロジェクト数や機能によってプランが異なる。スタンダードプラン以上のプランではユーザー数が無制限であり、現時点でプロジェクトが 100 以下であったため、スタンダードプランを調達した。

2 - 2 . 取得時の留意事項

契約パターンには年契約と月契約の 2 種類があり、年契約のほうが価格を抑えられるが、月契約のように柔軟なライセンス変更ができないため注意が必要である。

年契約の場合、月契約よりも 2 ヶ月分の価格を抑えられる。

30 日間の無料トライアルが利用でき、申込後にすぐ利用開始できる。

2 - 3 . 機能概要

2-3-1 . プロジェクト管理

プロジェクトのスケジュールや課題の進捗管理機能を提供する。

チケットに担当者や期限を記入し、プロジェクトの進捗情報を管理できる。

その他、課題が書かれているチケットのステータスをドラッグ＆ドロップで直感的に変更できるカンバンボード、作業スケジュールをグラフィカルに表示するガントチャートといった、プロジェクト管理に役立つさまざまな機能が用意されている。

2-3-2 . Wiki

プロジェクトに関わる情報や文書管理のための Wiki 機能を提供する。

会議の文書や作業マニュアル、仕様書などのチームメンバーに向けた情報や文書を管理でき、リンク共有や PDF 出力機能が用意されている。

2-3-3．ファイル共有

プロジェクトに関するファイル共有機能を提供する。

プロジェクトに関わる PDF や画像ファイルといったさまざまなファイルを共有できる。

2-3-4．外部サービス連携

外部のサービスやアプリケーションと連携する機能を提供する。

チケットの作成やコメント返信などをメール経由で行ったり、更新状況を Slack でリアルタイムに受け取るなど、さまざまなサービスと連携できる。

2 - 4．注記

特になし。

3. Box

3 - 1．ライセンス・プラン

Box Keysafe 機能の利用条件となる Box Enterprise プランを選定した上で、Zones オプションと Keysafe オプションを調達した。

3 - 2．取得時の留意事項

Box Keysafe を契約する上で、Box コンサルティングを契約する必要がある。

また、Box Keysafe を設定する上で必要な AWS KMS と Amazon S3 をホストする AWS 環境と AWS ビジネスサポート契約を別途調達する必要があり、AWS KMS と Amazon S3、および AWS CloudTrail の設定を利用者側で実施する必要がある。

3 - 3．機能概要

3-3-1．ファイルプレビュー機能

ブラウザ上でファイル閲覧する機能を提供する。

100 種類以上の拡張子に対応しており、閲覧に必要なソフトが端末にインストールされていない場合でも、ファイルプレビュー機能でファイルの内容を確認できる。

3-3-2．ファイル共有機能

フォルダ単位で、社内外のユーザーとファイル共有機能を提供する。

また、共有にあたって付与する権限のレベルが 7 種類あり、ユーザに適切な権限を割り振る事が可能である。

権限のレベルについては、以下 URL を参照すること。
https://support.box.com/hc/ja/articles/360044196413

3-3-3．ファイル検索機能

ファイル名やファイルの中の文字列からファイル検索のための機能を提供する。

また、各ファイル・フォルダに設定したタグやメタデータにもとづいて検索する事も可能である。

フォルダ名・コンテンツの種類・日付・ファイルサイズ・所有者でフィルタリングできる。

3-3-4．ファイルロック機能

Box に保存されているファイルが変更されないよう保護する機能を提供する。

ロックされたファイルは他のユーザによる更新ができないため、コンフリクトを防ぐ意味で、複数ユーザで同じファイルを編集する可能性がある場合に役立つ。

3-3-5．ファイルの世代管理機能

ファイルが更新された際に、自動的に履歴を保存して世代管理する機能を提供する。過去のファイルの参照や復元が可能となる。Enterprise プランでは、100 世代まで管理できる。

3-3-6．ログ検索機能

ユーザーや管理者が Box 上で行ったオペレーションログを検索し、レポートとしてダウンロードできる機能を提供する。

処理を行った日時・ユーザー名・処理内容・対象ファイル名などをログから確認できる。

3-3-7．フォルダでのメタデータのカスケード機能

フォルダに適用したメタデータを、フォルダ配下のファイルやフォルダに再帰的に適用する機能を提供する。

3-3-8．Box Keysafe

Box 上のデータを利用者が用意した暗号化鍵を用いて暗号化する機能を提供する。

Box は、AWS KMS にホストした暗号化鍵を用いて暗号化を行う。

検索機能を維持するために、ファイルの先頭 1 万文字をインデックス化できるが、本事業では利用していない。

3-3-9．Box Zones

米国を拠点とする Box の既存データセンターではなく、任意の国（日本、ドイツ、イギリスなど 8 ヶ国）を指定してデータ保管が行える機能を提供する。

3 - 4．注記

インデックスを有効化しない場合、検索性の保持のためにメタデータの設計が重要となる。また運用利便性の観点から、メタデータの作成はユーザーが実施可能とすべきであるが、あわせてメタデータ作成ポリシーを定義することが望ましい。

Box Sync は、ローカルにファイルを全て同期するため、利用すべきではない。

また Box Drive は、ローカルにファイル同期をするという性質上、ランサムウェアの影響を受ける可能性が高い。機能面の制約も多く、トラブルシュートの運用負荷が運用利便性を上回ることが懸念される。そのため Box Drive は、マクロの外部ファイル参照など限られたユースケースにおいてのみ利用することが望ましい。

4. CloudGuard Dome9

4 - 1．ライセンス・プラン

本事業では、無償のトライアルライセンスのみを利用した。トライアル期間中は全ての機能を利用できる。

4 - 2 . 取得時の留意事項

Dome9 は、単一の事業の環境のみに利用するには高額である。したがって、Dome9 を利用する場合は、複数事業にまたがっての利用を検討する必要がある。

また、脅威の可視化とポリシー違反のリアルタイム確認ができる Log.ic は、別途料金が発生するため注意が必要である。

4 - 3 . 機能概要

4-3-1 . NETWORK SECURITY

パブリッククラウドの管理コンソールでの把握が困難な、ネットワークファイアウォール設定の論理構成や依存関係を可視化する機能を提供する。また、AWS セキュリティグループを完全保護モードに設定することで、AWS コンソールでのセキュリティグループの意図しない変更を自動修復できる。

4-3-2 . COMPLIANCE ENGINE

自動化によるコンプライアンス/セキュリティポリシーへの準拠支援機能を提供する。また、準拠支援にて修正が必要と判断された項目について Remediation を構成することで自動修正ができる。さらに、コンプライアンス基準を満たしていないリソースに対して Dome9 管理コンソールへの表示、Slack、メール通知を行える。

Dome9 で予め用意されている Rule Sets には、AWS CIS Foundations v. 1.1.0 や AWS PCI-DSS などが存在する。

4-3-3 . PRIVILEGED IDENTITY

一時的なネットワークアクセス制限解除などの不正な設定変更を防止する機能を提供する。

4-3-4 . IAM Safety

高位の権限が必要な場合は、Dome9 管理コンソールでの申請・承認を必要とする設定が可能である。また、IAM Safety の申請によって許可された権限は、指定した時間を経過すると剥奪される。

IAM Safety 利用履歴の監査では、Dome9 の Auditlogs から、利用した IAM User、IAM Role の情報、特権の利用時刻を確認できる。

4-3-5．Dynamic Access Leases

Dome9 の管理コンソールから、特定の送信元 IP アドレスに対し、時限的なセキュリティグループ開放の設定ができる。また、Dynamic Access Leases の申請によって解放されたセキュリティグループは、指定した時間を経過すると閉塞される。

Dynamic Access Leases の利用履歴の監査では、Dome9 の Auditlogs から AWS セキュリティグループのトラフィック制限を解除したユーザー情報、該当のセキュリティグループ、制限を解除していた時間などを確認できる。

4-3-6．CloudGuard Log.ic

脅威の可視化と、ポリシー違反をリアルタイムで通知する機能を提供する。

VPC Flow Logs や Cloudtrail から収集したログやイベントを、クラウドインベントリおよび設定情報と組み合わせ、可視化・分析できる。

4 - 4．注記

NETWORK SECURITY の機能を利用して、AWS セキュリティグループを完全保護モードに設定すると、AWS コンソールからの変更は自動修復される。AWS セキュリティグループの設定変更が必要な検証環境などでは、Read-Only モードの利用を検討する必要がある。

Dynamic Access Leases を構成する際は、AWS セキュリティグループごとに設定する必要がある。Dome9 で管理する必要がある重要ホストなどを選定し、利用することが望ましい。

5. Datadog

5 - 1．ライセンス・プラン

Datadog は無償トライアル期間が 15 日間あり、トライアル期間中は全ての機能が利用できる。ライセンスは年払いか月払いを選択できる。年払いの方が利用料金を抑えられる。本事業では、下記監視項目、機能を利用するためのライセンスを 4 ヶ月分調達した。

- インフラストラクチャーpro
- Serverless
- APM （Application Performance Management）
- ログ監視 取り込み

5 - 2 . 取得時の留意事項

Datadog の AWS Integrations を利用した場合、インフラストラクチャーpro の課金対象は EC2 のみである。AWS Managed Service（RDS、DynamoDB、Neptune など）は課金対象外である。

また、ログ監視は従量課金となるため、おおよそのログの流入量をトライアル中に確認しておく必要がある。

5 - 3 . 機能概要

5-3-1 . Integrations

システム、アプリケーション、サービスの横断的な監視機能を提供する。スタック全体のメトリクスとイベントをシームレスに集約できる。

本事業で利用した Integration を下記について記載した。

AWS Integrations

CloudWatch メトリクスと連携してホストの CPU 使用率、メモリ使用率、Disk 使用率などを定期的に計測できる。さらに Serverless のメトリクス、トレース、ログを 1 つのビューにまとめて表示できる。

Nginx Integrations

Nginx インスタンスから合計リクエスト数や接続数（許可された接続数、処理された接続数、アクティブな接続数）を収集できる。

5-3-2 . Log Management

ログ・データ分析および調査機能を提供する。 ログをすばやく検索、フィルタリング、分析して、トラブルシューティングやデータ調査のために使用する。

本事業で利用したログを以下に記載する。

- AWS CloudWatch ログ
- Nginx ログ

5-3-3 . Datadog APM（Application Performance Management）

Web サービス、キュー、データベースリクエスト、エラー、レイテンシを監視するためのパフォーマンスダッシュボードを表示して、アプリケーションの状態を詳細に可視化する機能を提供する。

本事業で利用したアプリケーションを以下に記載する。

- Java/Spring boot アプリケーション

5-3-4 . Dashboards

重要なパフォーマンスメトリクスを視覚的に表示する機能を提供する。また、必要に応じてダッシュボードをカスタマイズできる。

5-3-5 . Monitors

メトリクス、インテグレーションのアベイラビリティ、ネットワークエンドポイントなどをチェックするためのモニターを提供する。 注視したいメトリクスに閾値を設定することで、閾値を超過した場合にメール通知などを行える。

5 - 4 . 注記

AWS Integrations は CloudWatch メトリクスの API を利用するため、AWS の制約によりデータのリアルタイム性が低下する場合がある。リアルタイム性を求められる環境には各ホストに Datadog Agent を導入する必要がある。

6. Druva inSync

6 - 1 . ライセンス・プラン

横断検索、e-Discovery 機能が提供される Druva inSync Cloud Elite プランを選定した上で、各サービス単体としてではなく、Exchange Online をバックアップ対象とするバンドルライセンスとして調達した。

6 - 2 . 取得時の留意事項

代理店から、一年単位の契約期間で購入できる。

Web より 2 週間の無償トライアルを申請できる。

6 - 3 . 機能概要

6-3-1 . Backup & Restore

デバイス上の指定フォルダに格納されているデータを Druva inSync のクラウド環境へバックアップする機能を提供する。

バックアップは、永久増分バックアップモデルであり、ソースベースのグローバル重複排除を行う。

バックアップデータの復元は、ユーザー自身で行えるセルフサービス機能があり、ファイル単位・端末単位の復元が可能である。

6-3-2 . Persona Backup

システムやアプリケーションの設定をバックアップする機能を提供する。

Persona Backup は、Windows 7 以降、macOS 10.10 以降に対応しており、設定情報をバックアップする。以下に代表的なものを掲載する。

Windows

- オペレーティング・システムの設定
- 地域と言語の設定
- フォルダオプション
- 暗号化（ネイティブ EFS キー）
- グループメンバーシップ
- ブラウザ設定（Google Chrome 他）
- ブックマーク
- ホームページ
- 規定の検索エンジン
- ダウンロードの場所
- フォント
- 一般的な設定、セキュリティ、プライバシー、プロキシを含む全ての設定
- プリンタの設定
- ネットワークプリンタ（プリンタ設定のみ）

macOS

- キーチェーン
- キーチェーンに保存されたパスワード

6-3-3 . DLP

端末内のデータを遠隔で消去するリモートワイプ機能を提供する。

端末内データの消去を指示した場合、端末側がオンラインの状態であればバックアップ対象フォルダを全て消去できる。

また、一定期間 Druva inSync との通信が途絶えた端末に対して、Druva inSync Agent が自動的にバックアップ対象フォルダを全て消去できる。

6-3-4．Federated Search

バックアップデータ中のファイルや、メールの検索と検索結果にもとづくデータの削除をサポートする機能を提供する。

ファイル名やメールの件名だけでなく、以下のようにメタデータを用いて検索できる。

メタデータ属性を用いたファイルの検索

- ファイル名
- 拡張子
- チェックサム
- 変更された時間
- 作成時間
- サイズ

メタデータ属性を用いたメールの検索

- 件名
- 送信者（差出人、宛先、Cc、Bcc）
- 受信時間
- 添付ファイル名
- 添付ファイルの拡張子
- 添付ファイルチェックサム
- 添付ファイルのサイズ

6-3-5．Legal Hold

ユーザーのバックアップデータを保持し、削除から保護する機能を提供する。

保持はユーザー単位で行い、そのユーザーのバックアップデータは、圧縮と削除の対象から除外される。

事案ごとにケースを作成し、保持対象ユーザーを指定することで、法務管理者に対して、特定の事案に係るユーザーのバックアップデータのみを開示できる。

6 - 4．注記

ユーザーごとのバックアップデータは 50GB が上限であるため、バックアップ対象のフォルダや除外設定を適切に設定する必要がある。また大規模展開を行う際は、初期バックアップ通信が拠点のネットワーク帯域を逼迫するおそれがあるため、設定にて通信量を制限したり、ローリング方式を採用した展開方式を検討するなどの考慮が必要である。

7. GitHub

7 - 1 . ライセンス・プラン

シングルサインオンが利用できる、GitHub Enterprise Cloud を調達した。

7 - 2 . 取得時の留意事項

特になし。

7 - 3 . 機能概要

7-3-1 . ソースコード管理

分散型ソースコード管理システムである git のリポジトリをホスティングする。git は分散型であるが、組織で利用する場合は中央集権を実現するための機能を提供する。

7-3-2 . 開発コラボレーション

ソフトウェアを開発するにあたって、Issue を登録して議論し、ブランチを作成して機能追加や不具合を修正した結果を取り込む Pull Request といった作業を、内部の開発チームで閉じることなく、外部からの参加を可能にするコラボレーション機能を提供する。

7-3-3 . 外部アプリケーションとの連携

開発したソフトウェアのテストを自動的に行う機能や、修正した結果を動作環境に自動的に配置する機能などとの連携ができる GitHub Actions を提供する。GitHub Actions は、GitHub 上のイベントを引き金にワークフローを実行できる。

7-3-4 . 組織管理

GitHub は、基本的に個人がリポジトリを管理する。そこで、個人ではなく組織がリポジトリを管理できるようにする機能がある。組織にはメンバーやコラボレーターを参加させ、リポジトリ単位で権限を付与できる。

また、インターネットドメインの DNS を使うことで、本当にその組織が登録していることを Verified バッヂで示せる。

7 - 4 . 注記

GitHub Enterprise Cloud は個人アカウントの組織による管理ができない。そのため、アカウントの管理は利用者自身が実施しなければならないことに加え、外部アカウントとコラボレーションをする際は、アカウント利用者の本人確認を徹底しなければならない。

8. Google Analytics

Google Analytics は以下のサービス群で構成した。

- Google Analytics
- Google Data Portal
- Google Search Console

8 - 1 . ライセンス・プラン

有償版である Google Analytics360 については、検証規模と調達意図に反するため、無償の Google アカウントを作成して、各サービスを利用した。

8 - 2 . 取得時の留意事項

有償版のみにて提供される機能があるため、差異について事前の確認が必要である。特に無償版ではサポートが提供されておらず、ヘルプセンター、コミュニティフォーラムなどによる自己解決が求められるため、注意が必要である。

8 - 3 . 機能概要

8-3-1 . Google Analytics

設置した Web サイトのアクセス解析を行い、アクセス数などの情報を取得し、各種解析結果をダッシュボードで表示でき、リアルタイムレポート機能も備えている。

8-3-2 . Google Data Portal

複数の Google Analytics 設置サイトのアクセス解析結果を一元的にダッシュボード化し、レポーティングに活用できる。ダッシュボードの表示項目や配置などは自由にカスタマイズが可能である。

8-3-3 . Google Search Console

ページごとの流入元となった検索エンジンの検索キーワードについて詳細な情報を提供する。これらの情報は、データソースとして Google Data Portal で活用できる。

8 - 4 . 注記

今回の検証では、Google Analytics サービス群については、検証内容を考慮して意図的に機能を大きく制限して構成している。今回は非公開環境での機能検証であり、実際に公開されている Web サイトにおいての運用検証ではない。

そのため本章の記述は、Google Analytics サービス群が備える機能に対して著しく限定された記述となっている点に留意されたい。

9. Jamf Pro

9 - 1 . ライセンス・プラン

単一プランであるため省略する。

9 - 2 . 取得時の留意事項

「macOS、iOS/iPadOS、tvOS の合算で 50 ライセンス以上」という最低契約数の制限がある。

販売代理店との契約となり、年契約のみである。

また、無償トライアルの利用期間は 2 週間である。注意事項として、トライアル環境から本番環境への引き継ぎはできない。

契約時にあたり、以下の情報が必要となる。

- 組織名
- 担当者個人名（英文）
- 担当者メールアドレス
- 組織所在住所
- 電話番号
- 希望サブドメイン

導入時には Jamf JumpStart という有償オンボーディングサービスの受講が必須となる。 Jamf JumpStart の受講所要時間は購入したライセンスの対象 OS によって異なり、以下の通りである。

- macOS と iOS/iPadOS 両方：8 時間×3 日間

- macOS のみ：8 時間×2 日間
- iOS/iPadOS のみ：4 時間または 8 時間

9 - 3 . 機能概要

Jamf Pro は Apple デバイス（macOS/iOS/iPadOS/tvOS）専用のデバイス管理ツールであり、主に以下の機能を有する。

9-3-1 . デバイスインベントリ情報の取得

デバイスのハードウェア情報、OS バージョン、セキュリティツールをはじめとした各種アプリケーションのインストール状況、バージョン情報などの収集を行う。

9-3-2 . MDM コマンドによるリモートワイプ/ロック

MDM コマンドを利用して遠隔からデバイスを消去/ロックが可能である。ただし、MDM コマンドの実行には対象デバイスがネットワークに接続されている必要がある。

また、MDM コマンドの実行状況や実行ログを確認できる。

9-3-3 . 構成プロファイルによるデバイス設定の配布

ディスクの暗号化およびリカバリーキーの収集、AirDrop の利用制限、iCloud の利用制限、USB デバイスの利用制限、ファイアウォールの有効化などの設定の強制が可能である。ただし、iOS/iPadOS の一部の機能制限については対象デバイスを監理モードにする必要があり、監理モードにするためにはデバイスの初期化を行う必要がある。

9-3-4 . アプリケーション制限機能

macOS において制限付きソフトウェア機能を利用し、macOS アップグレーダーや特定のアプリケーションの起動制限を行うことが可能である。

iOS/iPadOS において特定のアプリケーションの制限を行う場合は、構成プロファイルで設定可能である。

9-3-5 . アプリケーションとアップデートの配布

アプリケーションとアップデートの配布が可能である。

macOS の場合、Microsoft Defender for Endpoint や Netskope といったセキュリティツールを含む各種アプリケーションのインストールとアップデートの配布が可能である。

iOS/iPadOS の場合、App Store 経由で Box for EMM や Slack for EMM などのアプリケーションの配布が可能である。通常、App Store 経由のアプリケーションインストールには Apple ID が必要となるが、Apple Business Manager（Apple 社提供のエンタープライズ向けサービス）と連携させることで、Apple ID を利用せずに配布が可能となる。

9-3-6．スクリプトの配布および実行（macOS のみ）

任意の macOS や特定の条件に該当する macOS に対して、スクリプトの配布と実行が可能である。例として、所定のバージョン以下の macOS に対して通知を表示するスクリプトの実行や、暗号化規格が古い Wi-Fi に接続した場合に警告を表示するスクリプトの配布などを行える。

9-3-7．Microsoft Intune 連携による条件付きアクセスの利用

Microsoft Intune と連携させることで、Jamf Pro からデバイスのコンプライアンス情報を Microsoft Intune へ送付し、送付したコンプライアンス情報に基づいた Azure Active Directory 条件付きアクセスによるアクセス制御が可能である。

9-3-8．Smart Computer/Device Group による動的グルーピング

デバイス内のさまざまな情報にもとづいて動的にグルーピングすることが可能である。

OS バージョンやアプリケーションバージョンが一定以下のデバイスをグルーピングし、適切なアップデートの配布対象とすることや、1 週間以上オフラインのデバイスを抽出することが可能である。

9-3-9．ダッシュボードによる各種情報の可視化

構成プロファイルやアプリケーションの配布状況、Smart Computer/Device Group の条件に合致する対象デバイス数などをダッシュボードに表示して可視化が可能である。

9 - 4．注記

特になし。

10. Jamf Connect

10 - 1 . ライセンス・プラン

単一プランであるため省略する。

10 - 2 . 取得時の留意事項

「25 ライセンス以上」という最低契約数の制限がある。

販売代理店との契約となり、年契約のみである。

無償トライアルの利用期間は 2 週間である。

導入時には Jamf Connect Onboarding という有償オンボーディングサービスの受講が必須となる。受講所要時間は 4 時間で、原則オンラインで開催される。

10 - 3 . 機能概要

Jamf Connect は主に 2 つのアプリケーションから構成されるバンドル製品である。

10-3-1 . Jamf Connect Login アプリ

macOS のログイン画面をクラウド IdP の認証画面に置き換えるアプリケーション。クラウド IdP の認証情報にもとづいてローカルアカウントの作成やデバイスへのログインを行うことで、認可されていないユーザーのログインを禁止できる。さらに macOS のログイン時に、クラウド IdP で指定した MFA の要求が可能となる。

10-3-2 . Jamf Connect メニューバーアプリ

クラウド IdP アカウントと macOS ローカルアカウントのパスワード同期を行う常駐型アプリケーション。パスワードの同期機能の他、メニューバーからクラウド IdP アカウントのパスワードを変更・リセットする機能や、利用者に確認させるヘルプサイトなど特定の Web サイトへのショートカットの配備などの機能が提供される。

10 - 4 . 注記

Jamf Connect Login アプリによるクラウド IdP 認証（MFA 要求含む）は、macOS のログイン時にのみ行われるため、スリープからの復帰時やスクリーンセーバーのロック解除時には適用されない。

Jamf Connect Login アプリによるクラウド IdP 認証はネットワークに接続されていることが必須条件となるが、ネットワークに接続されていない時にローカルログインを許可するか否かは設定可能である。

クラウド IdP アカウントのパスワードを変更した場合、Jamf Connect メニューバーアプリによって macOS アカウントとのパスワード同期が行われるが、このパスワード同期の際に古いパスワードの入力を求められるため注意が必要である。

11. Microsoft Azure Active Directory

11 - 1 . ライセンス・プラン

特権 ID 利用の申請・承認や特権 ID 利用ユーザの定期的な棚卸し機能の利用条件である Azure Active Directory Premium P2 ライセンスを単体で購入できるが、他のサービスと連携して利用するため複数のライセンスが含まれる Microsoft 365 E5 を調達した。

各サービスのライセンスを個別調達するより、Microsoft 365 E5 ライセンスを調達したほうが価格を抑えられるためである。

11 - 2 . 取得時の留意事項

契約パターンは年契約と月契約の 2 種類があり、年契約のほうが価格を抑えられるが、月契約のように柔軟なライセンス変更に対応できないため注意が必要である。

Microsoft との直接契約も可能だが、代理店契約も可能である。

Azure Active Directory Premium P2 のライセンスが含まれる Enterprise Mobility + Security E5 というバンドルライセンスの無料トライアルができる。トライアル期間は 90 日間である。

11 - 3 . 機能概要

11-3-1 . クラウドサービスへの SSO

Azure Active Directory に登録したユーザー情報でクラウドサービスにログインする機能を提供する。

ユーザーが Azure Active Directory に一度ログインすると、その資格情報を用いて SSO 設定を行ったクラウドサービスにログインができる。ユーザーは ID やパスワードをクラウドサービスごとに作成し、記憶しておく必要がなくなる。

11-3-2．クラウドサービスへのプロビジョニング

Azure Active Directory に登録したユーザーやグループ情報を、連携先のクラウドサービスに自動で登録する機能を提供する。

管理者はプロビジョニング設定を行ったクラウドサービスに対して、手作業でユーザーやグループ情報を登録する必要がなくなる。ただし、グループ情報はグループの入れ子に対応していない点に注意が必要である。

11-3-3．条件付きアクセス

ユーザーに割り当てられている役割や、ユーザーやデバイスの状態を評価し、適切にアクセス制御するための機能を提供する。条件付きアクセスポリシーを活用し、管理者はユーザに多要素認証の利用を要求できる。

また Microsoft Intune と連携することで、端末の OS バージョンやセキュリティリスクなどのデバイス状態をもとにアクセスの制御ができる。

11-3-4．Privileged Identity Management

特権 ID 利用の申請・承認機能と期限付きで特権 ID を付与するための機能を提供する。

申請者はいつどのような理由で特権 ID を利用するかを申請に記載し、承認者は申請者の要求を承認または拒否できる。申請と承認の履歴は記録されるため、監査に利用できる。

11-3-5．アクセスレビュー

特権 ID を利用するユーザの定期的な棚卸し機能を提供する。

過剰なアクセス権の付与や、異動や退職に伴うアクセス権の削除漏れ等のチェックに利用できる。

11 - 4．注記

Azure Active Directory に参加もしくは登録できるデバイスの最大数は既定値で 50 台である。最大数を無制限に設定もできる。Microsoft Intune で登録可能なデバイス数とは別の設定である点、注意が必要となる。

意図せず Azure Active Directory に管理者がログインできなくなった状態から復旧するために、緊急アクセス用管理者アカウントを作成しておくべきある。

緊急アクセス用管理者アカウントの要件として以下がある。

- 個人ユーザーと関連付けしない
- 認証方法は通常利用とは異なるものにする
- 認証情報は安全に管理する
- パスワードは最低でも 16 文字以上にする

- グローバル管理者ロールを永続的に割り当てる
- 少なくとも 1 つのアカウントは MFA を使わないように構成する
- 少なくとも 1 つのアカウントは条件付きアクセスを使わないように構成する
- フェデレーションしないクラウドベースのアカウントにする
- サインインログと監査ログを監視する

12. Microsoft Azure Sentinel

12 - 1 . ライセンス・プラン

サブスクリプションを作成することで、31 日間は追加費用なしで Azure Monitor Log Analytics ワークスペース上で有効化できる。そして Azure Sentinel には、容量予約と従量課金制のふたつの支払い方法が用意されている。本事業では、データの流入量と保存期間をベースにした従量課金制を利用した。

12 - 2 . 取得時の留意事項

データの流入量と保存期間をベースにした従量課金制であるため、利用 31 日間のログ流入量から月ごとのコストを予測する必要がある。 Log Analytics の 「使用量と推定コスト」を利用することで、おおよそのコストを予測できる。Azure Active Directory の監査データについては、Azure Sentinel と Azure Monitor Log Analytics の両方に対する取り込みが課金される。

なお、容量予約を行うことで、選択した容量予約にもとづいて割引 （最大 60%）が適用される。契約から 31 日間経過後は、容量予約をいつでも柔軟に変更できる。

追加費用なしで Azure Sentinel と Azure Monitor Log Analytics の両方に取り込める製品は以下の通り。

- Azure のアクティビティログ
- Office 365 の監査ログ （全ての SharePoint アクティビティおよび Exchange 管理者アクティビティ）
- Microsoft Defender 製品（Azure Defender、Microsoft 365 Defender、Microsoft Defender for Office 365、Microsoft Defender for Identity、Microsoft Defender for Endpoint）、Azure Security Center、Microsoft Cloud App Security、Azure Information Protection からのアラート

12 - 3 . 機能概要

12-3-1 . データコネクタ

Microsoft 365 Defender ソリューションや、Office 365、Azure Active Directory 、Microsoft Defender for Identity、Microsoft Cloud App Security を含む Microsoft 365 ソースだけでなく、Amazon Web Service などのサードパーティ製品のデータをソースとしてログを収集し、容易にリアルタイム統合を可能とする機能を提供する。

一般的なイベント形式（CEF）、Syslog または REST-API を使用して、使用中のデータ ソースを Azure Sentinel に接続することも可能である。

12-3-2．ログ分析

収集したログから必要な情報検索のための機能を提供する。

検索を行う際は、クエリ言語である Kusto を利用する。また、作成したクエリをお気に入りに登録することで、再利用や他の管理者との共有が可能である。

12-3-3．Workbooks

予め用意されている組み込みのブックテンプレートを使用してデータソースに接続することで、分析情報の可視化機能を提供する。

また任意のデータに対して、分析した結果を可視化するカスタムブックが作成できる。

12-3-4．脅威検出

脅威検出規則の作成に役立つテンプレートを提供する。

このテンプレートは、セキュリティ専門家とアナリストから構成される Microsoft のチームが、既知の脅威、一般的な攻撃ベクトル、疑わしい行動の段階的拡大チェーンにもとづいて設計したものである。

検出規則を有効化すると、疑わしい行動がないか環境全体が自動的に検査される。

テンプレートの多くは、ニーズに合わせて特定の行動を検索したり、除外するようにカスタマイズできる。検出規則で生成されるアラートによって、環境内で割り当てて調査できるインシデントが作成される。

12-3-5．セキュリティプレイブック

アラートに対する応答として、Azure Sentinel から実行できる手順のコレクションであり、応答の自動化機能を提供する。

セキュリティプレイブックは手動で実行することも、特定のアラートがトリガーされたときに自動実行するように設定できる。

12-3-6．インシデント管理

分析ロジックにて作成されたインシデント管理のための機能を提供する。現在プレビュー段階にある Azure Sentinel の詳細調査ツールを使用して、潜在的なセキュリティの脅威の範囲を把握し、根本的な原因を見つけるために役立つ。

12 - 4 . 注記

脅威検出規則によって検出されるインシデントの傾向が環境によって異なるため、実際に検出されたインシデントを確認し、傾向を確認していく必要がある。そのため、中長期的に運用を考え、対応方針を修正していく必要がある。

13. Microsoft Defender for Endpoint

13 - 1 . ライセンス・プラン

Windows10 Enterprise E5 単体でのライセンス購入にて含まれているが、他のサービスと連携して利用するため、複数のライセンスが含まれる Microsoft 365 E5 を選定した。この時、各サービスのライセンスを個別調達するよりも、 Microsoft 365 E5 ライセンスを調達したほうが価格を抑えられる。

13 - 2 . 取得時の留意事項

契約パターンは年契約と月契約の 2 種類があり、年契約のほうが価格を抑えられるが、月契約のように柔軟なライセンス変更に対応できないため注意が必要である。

Microsoft との直接契約も可能だが、代理店契約も可能である。

Microsoft 365 管理センターから、Microsoft 365 E5 の 30 日間無料トライアルを申し込める。

13 - 3 . 機能概要

通常のパターンマッチによるマルウェア検知に加え、ネットワーク、デバイス、カーネルの動作全体でセキュリティ信号を受信し、加えて ID、電子メール、データおよびアプリにわたる幅広い情報を加味してその振る舞いを、端末とクラウドに備わる AI や機械学習を用いて評価し、脅威検出する機能を提供する。

クラウドに備わる AI や機械学習は、Microsoft が世界的に収集したセンサー情報にもとづいてアップデートされており、その結果が日々配信される。

Windows 環境においては、エンジン自体が OS 機能の一部であるため、OS アップデート対応や Agent 配布運用を行う必要がないことも特徴の一つである。

13-3-1 . 応答

検出された脅威に応じ、当該端末に対して以下のようなアクションが実施できる機能を提供する。

- 自動調査の開始
- Live Response セッションの開始
- 調査パッケージの収集
- ウィルススキャン実行
- アプリ実行の制限
- デバイスの分離
- 脅威の専門家への相談

現在、応答機能に対応している OS バージョンは以下の通りである。

Windows 10

- バージョン 1909 以降
- バージョン 1903 （KB4515384）
- KB4537818 のバージョン 1809 （RS 5）
- バージョン 1803 （RS 4） KB4537795
- バージョン 1709 （RS 3） KB4537816

13-3-2 . Block Mode

EDR 機能を通じて検出された、悪意のあるファイルやプロセス、サービスなどの動作をブロックする機能を提供する。

本機能によって、次のような攻撃手法をブロックできる。

- LSASS からの資格情報のダンプ
- プロセス間の挿入
- プロセスの空洞化
- ユーザーアカウント制御のバイパス
- ウイルス対策の改ざん （機能を無効化する、マルウェアを除外対象に追加するなど）
- ペイロードをダウンロードするコマンドとコントロール （C&C）への連絡
- コインマイニング
- ブートレコードの変更
- ハッシュパス攻撃
- ルート証明書のインストール
- さまざまな脆弱性に対する悪用の試み

なお本機能は、Windows 10 の全てのバージョンにおいて、利用可能である。

13-3-3 . Live Response

リモートシェル接続を使用して、デバイスに瞬時にアクセスできる機能を提供する。

Live Response 機能を用いて以下のオペレーションを行える。

- リモートシェル用コマンドを用いたオペレーション
- ファイルダウンロード
- 端末に導入されている全てのドライバの表示
- 端末 上のファイル検索
- 端末 上のファイルに対する詳細情報の取得
- 端末上の既知の永続化メソッドの表示
- 端末 上で実行している全てのプロセスの表示
- 端末 上の全てのスケジュールされたタスク
- 端末 上の全てのサービスの表示
- 犯罪エンジンを用いたエンティティの詳細調査
- 端末 に配布したライブラリから PowerShell スクリプトを実行
- 端末 上のエンティティの修復（ファイル削除、プロセスやサービスのイメージファイルの停止・削除、レジストリエントリの削除、スケジュールされたタスクの削除、スタートアップフォルダ内のファイル削除）
- 修復されたエンティティの復元

なお Live Response 機能の利用履歴は、Microsoft Defender Security Center に記録され、監査できる。

13-3-4．Threat Analytics

Microsoft のセキュリティ研究者から提供される、以下に係る脅威分析レポートを表示する機能を提供する。

- アクティブな脅威アクターとそのキャンペーン
- 人気のある新しい攻撃手法
- 重大な脆弱性
- 一般的な攻撃面
- 一般的なマルウェア

脅威分析レポートには、概要・アナリストレポート・軽減策が掲載されている。

概要

詳細なアナリストレポートのプレビューが表示される。そして組織に対する脅威の影響と、構成が正しく設定されていないデバイスや、パッチ未適応のデバイスを可視化する。

アナリストレポート

エキスパートによって報告された詳細のレポートが表示される。

ほとんどのレポートには MITER ATT&CK フレームワークにマップされた戦術や手法、推奨事項の網羅的なリスト、強力な脅威検出ガイダンスなど、攻撃チェーンの詳細な説明が記載されている。

軽減策

脅威に対する組織の回復力を高めるのに役立つ、具体的でアクション可能な推奨事項の一覧を表示する。軽減策の一覧には次の事項が含まれる。

- 脆弱性に対するセキュリティ更新プログラムやパッチの展開
- Microsoft Defender ウイルス対策の設定（セキュリティインテリジェンスのバージョンやクラウド保護の設定、望ましくない可能性のあるアプリケーション保護の設定、リアルタイム保護の設定）

13-3-5．Threat and vulnerability management

Defender for Endpoint にオンボードされた端末からプッシュされた脆弱性とセキュリティ構成データをスコア化し、ダッシュボードに表示する機能を提供する。

ダッシュボードに表示される脆弱性やセキュリティの推奨構成は、以下のような特徴を持っている。

- 新たに発見された脆弱性は、アプリケーションに対する対処可能な軽減策の推奨事項が報告される
- 悪用されている脆弱性は、リスクが高い脆弱性として表記される
- 端末のセキュリティに関する推奨事項は、優先順位が表記され、アクション可能な修復手段が含まれる
- 脆弱性やセキュリティの推奨構成に対して、修復チケットを作成し、Microsoft Intune へタスクとして登録できる

13 - 4．注記

Threat and vulnerability management で表示される脆弱性は、端末から収集したインベントリ情報にもとづいて評価される。端末から収集されるインベントリ情報には、インストールされている全てのアプリケーションが必ずしも含まれている訳ではない。

Live Response 機能は、対象となる端末のネットワーク接続環境によって、応答速度が変化する。

14. Microsoft Defender for Office 365

14 - 1． ライセンス・プラン

Defender for Office 365 （プラン 2）単体でのライセンス購入にて含まれているが、他のサービスと連携して利用するため複数のライセンスが含まれる Microsoft 365 E5 を調達した。各サービスのライセンスを個別調達するより、 Microsoft 365 E5 ライセンスを調達したほうが価格を抑えられる。

14 - 2． 取得時の留意事項

契約パターンは年契約と月契約の 2 種類があり、年契約のほうが価格を抑えられるが、月契約のように柔軟なライセンス変更に対応できないため注意が必要である。

Microsoft と直接契約することもできるが、代理店契約も可能である。

Microsoft に申請することで 30 日間の無料トライアルが利用でき、その場合は Defender for Office 365 のライセンスが含まれる Enterprise Mobility + Security E5 というバンドルライセンスの契約となる。

14 - 3． 機能概要

Exchange Online と統合し、以下のセキュリティ機能を提供する。

14-3-1． マルウェア対策

複数のマルウェア対策エンジンを使用して、既知のマルウェア全てを捕捉するよう設計された多層的な保護を提供する。

サービスを使用して送信されるメッセージは、マルウェアが含まれていないかスキャンされる。マルウェアが検出された場合にメッセージは削除されるが、マルウェア検出によりメッセージが削除され配信されない場合は、送信者または管理者に通知が送信される場合がある。添付ファイルからマルウェアが検出されたことを受信者に通知するメッセージはカスタマイズすることもできる。

14-3-2． 迷惑メール対策

Microsoft 独自のスパム対策技術を使用して、全ての受信メッセージに対して送信者の評価を確認する、強力な接続フィルターとスパムフィルターを用いて、高い精度でのフィルタリングを実現する。

送信スパムフィルターも常に有効となり、本機能を使用している組織とその目的の受信者を保護できる。

スプーフィング対策として、メッセージ本文の From ヘッダーの偽造を調べ、From ヘッダーが偽造されていると判断した場合、メッセージはスプーフィングされたものとして識別される。

14-3-3．安全な添付ファイル

メッセージングシステムを未知のマルウェアからゼロデイ保護する機能を提供する。

既知のマルウェアや署名がない全てのメッセージと添付ファイルは、Defender for Office 365 がさまざまな機械学習および分析テクノロジを使用して悪意を検出する特別な環境にルーティングされる。

不審な動作が検出されない場合、メッセージは解放されてメールボックスに配信される。

14-3-4．安全なリンク

メッセージまたは Office ドキュメント内の悪質な URL から、予防的にユーザーを保護する。リンクをクリックした後も保護は毎回継続し、悪意のあるリンクは動的にブロックされ、適切なリンクにはアクセスできる。

安全なリンクは、次のアプリに対して機能する。

- Windows または Mac 上のエンタープライズ向け Microsoft 365 アプリ
- Web 用 Office（Web 用 Word、Web 用 Excel、Web 用 PowerPoint、Web 用 OneNote）
- Windows の Word、Excel、および PowerPoint
- Microsoft Teams チャンネルおよびチャット

14-3-5．安全なドキュメント

Microsoft Defender for Endpoint を使用して、保護ビューで開かれたドキュメントやファイルをスキャンする。本機能は、Office バージョン 2004（12730.x）以降を使用するユーザーに一般公開されている。この機能は既定ではオフになっており、セキュリティ管理者が有効にする必要がある。

この機能は、Microsoft 365 E5 または Microsoft 365 E5 セキュリティライセンス（Defender for Office 365 プランには含まれない）をもつユーザーのみが利用でき、以下アプリケーションが対応している。

- Windows の Word、Excel、および PowerPoint
- Microsoft Teams チャンネルおよびチャット

14-3-6．フィッシング対策ポリシー

受信メールのメッセージをチェックして、メッセージがフィッシング詐欺に該当する可能性がないか確認する。 メールを受信したユーザーが Defender for Office 365 ポリシー（安全な添付ファイル、安全なリンク、またはフィッシング詐欺対策）に含まれる場合、受信メッセージは構成されたポリシーにもとづいてメッセージを分析し、適切なアクションを実行する複数の機械学習モデルによって評価される。

14 - 4． 注記

構成アナライザを用いて、Microsoft 推奨の構成を設定できるが、安全なリンク機能において Microsoft Teams の中での悪意のある URL へのアクション設定は、プレビュー機能であるため設定できなかった。

15. Microsoft Intune

15 - 1． ライセンス・プラン

Microsoft Intune 単体でライセンス購入できるが、他のサービスと連携して利用するため複数のライセンスが含まれる Microsoft 365 E5 を調達した。各サービスのライセンスを個別調達するより、 Microsoft 365 E5 ライセンスを調達したほうが価格を抑えられる。

15 - 2． 取得時の留意事項

契約パターンは年契約と月契約の 2 種類があり、年契約のほうが価格を抑えられるが、月契約のように柔軟なライセンス変更に対応できないため注意が必要である。

Microsoft との直接契約もできるが、代理店契約も可能である。

Microsoft Intune のライセンスが含まれる Enterprise Mobility + Security E5 というバンドルライセンスの無料トライアルができる。トライアル期間は 90 日間である。

15 - 3． 機能概要

15-3-1． リモートワイプ

端末内のデータを遠隔で消去する機能を提供する。

不要になった端末や紛失した端末を工場出荷時の既定の設定に復元できる。

端末内データの消去指示を送信した場合、端末がオンラインの状態であればデータを消去できる。

15-3-2． デバイスコンプライアンスポリシー

端末の OS バージョンやセキュリティリスクなどの判定をもとに、端末の状態評価機能を提供する。

端末の正常性を評価し、評価結果をもとに Azure Active Directory の条件付きアクセス機能にてアクセス許可の判定を行う。

15-3-3．デバイス構成プロファイル

端末に対して設定の配信機能を提供する。

ファイアウォールの設定や Microsoft Defender for Endpoint のオンボード設定の配信など、端末への設定を徹底できる。

15-3-4．Windows 10 更新リング

端末の OS バージョン管理のための機能を提供する。

更新プログラムの配信の遅延や受信時の挙動を制御できる。

更新プログラムには品質更新プログラムと機能更新プログラムが存在し、品質更新プログラムは最大 30 日、機能更新プログラムは最大 365 日の遅延を設定できる。

15-3-5．アプリケーションの配信

端末に対してアプリケーション配信する機能を提供する。

msi 形式と intunewin 形式のファイルで、インストールを行うアプリケーション配布ができる。exe やスクリプトなどのその他のファイル形式は、intunewin ファイルとしてパッケージ化することで配信できる。

15-3-6．アプリ保護ポリシー

モバイル端末のアプリケーションにおいて、組織のデータのローカルへの保存や切り取り、コピー、貼り付けといった動作制限機能を提供する。

組織のデータを取り扱うアプリケーションのみが対象であり、取り扱いのないアプリケーションに対しては制御を行わない。

15 - 4．注記

Microsoft Intune ライセンスを割り当てられたユーザーが登録可能なデバイスは最大 15 台までである。複数のユーザーがアクセスするデバイスを管理するには、各ユーザーにライセンスを付与する必要がある。

16. mxHero

16 - 1 . ライセンス・プラン

単一プランであるため省略する。

16 - 2 . 取得時の留意事項

「最低契約数は 20 ライセンス以上」という制限がある。

販売代理店との契約となり、年間契約である。

また、無償トライアルの利用期間は 14 日間である。

ほか、メールリレー機能を有せず、本検証で使用した Exchange Online の場合は、「メールフロー」の「ルール」と「コネクタ」を利用して、Exchange Online と直接接続する必要がある。このため、メールに関連する既存の他システムとの整合性を事前に確認する必要がある。

16 - 3 . 機能概要

送受信したメールの添付ファイルを、オンラインストレージへの共有リンクへ置き換え、格納する機能を提供する。

上記に付帯して、添付ファイルのみならず、メール本文もオンラインストレージに格納し、オンラインストレージへのアクセス無しではメール本文を読めないようにする、Secure Email 機能がある。

16 - 4 . 注記

mxHero がファイルを格納するオンラインストレージによって、利用可能な機能に差異が生じる。今回の検証は、Exchange Online と Box Enterprise の組み合わせとなったが、本構成が最も高機能かつ安定した構成となる。

17. Netskope

17 - 1 . ライセンス・プラン

アクセス制限、フィッシングサイトへのアクセス対策、SaaS との API 連携、DLP 機能を利用するためのライセンスが包含されている Netskope SaaS and Web Enterprise プランを選定した。

Netskope ライセンスは機能別に単体購入を行えるが、各サービスのライセンスを個別調達するより、Netskope SaaS and Web Enterprise プランを調達したほうが価格を抑えられる。

17 - 2． 取得時の留意事項

Netskope SaaS and Web Enterprise は、本事業における調達を行った時点でのライセンス体系である。ライセンス体系は今後変更となる可能性があるため、適宜代理店へ確認すること。

Netskope SaaS and Web Enterprise プラン内で API 連携できる SaaS は 3 種類のみである。それを超える SaaS と API 連携を実施する場合は、別途ライセンスの購入が必要である。

ライセンスの購入を前提に、代理店に検証テナントの利用を申請できる。検証テナントの利用可能期間は 30 日間である。ライセンスは代理店から年単位で購入する。

ライセンスの最小購入数は 100 ユーザーであるが、最小購入数を下回る場合は代理店に相談できる。

17 - 3． 機能概要

17-3-1． Netskope Active Platform

利用しているクラウドサービスの可視化・分析や、定義したポリシーに応じてリアルタイムにアクセス制御する機能を提供する。

Netskope は独自にクラウドサービスの安全性の格付け評価をしており、評価が低いクラウドサービスへのアクセスを制御できる。

また、認可したクラウドサービスと非認可のクラウドサービスを識別でき、非認可のクラウドサービスへのアクセスを制御できる。

17-3-2． Netskope for Web

Web サイトのカテゴリに基づいたフィルタリング機能を提供する。

ギャンブルやアダルトなど、業務上不要なサイトへのアクセスを制限できるほか、30 日以内に登録や所有者が変更されたドメインや、攻撃性のあるアクティビティが行われているドメインに対するアクセスをフィルタリングできる。

17-3-3． Netskope API Introspection

SaaS との API 連携により、クラウドサービス内のデータやユーザーアカウント等の可視化やユーザ操作の制御機能を提供する。

本機能は、ユーザーが利用する端末に Netskope エージェントが未導入であっても利用できる。

API 連携できる SaaS は数十種類と限定されている点、SaaS ごとに可視化や制御できる内容に差異がある点に注意が必要である。

17-3-4 . Standard DLP

Netskope が保有する辞書情報や正規表現を利用して通信データやファイルを評価し、データ漏えい防止につながる機能を提供する。

機密に該当するデータのアップロードの検出や遮断ができる。ここでは英数字だけではなく、日本語も評価の条件として使用できる。

17-3-5 . Advance Threat Protection

クラウドサービス内のマルウェア検知機能を提供する。

パターンマッチングによる検知に加え、Advance ライセンスでは振る舞い検知、ランサムウェアの検知、クラウド環境にあるサンドボックス環境での分析機能が提供される。

マルウェアを検知すると、重大度に応じてアラートの通知やマルウェアを含むファイルの隔離ができる。

さらにネットワークトラフィックをスキャンして、 CVSS の評価に基づいた検知や侵入防止を行うレベルの設定に従い、ネットワークに影響を与える可能性がある悪意のあるプログラムを検知し、侵入を防止できる。

17 - 4 . 注記

業務上必要なクラウドサービスへのアクセスが意図せず遮断される場合を考慮して、都度ポリシーをチューニングする必要がある。

本契約時に検証テナントを本番テナントとして昇格でき、検証テナントで行った設定やポリシーチューニングを引き継げるが、昇格にあたり Netskope のテナント名は変更できない。

18. Slack

18 - 1 . ライセンス・プラン

BYOK が利用できる Slack EKM 及び、Slack for EMM を利用するために、Slack Enterpise Grid を調達した。

18 - 2． 取得時の留意事項

Slack EKM を利用するためには、米国東部（バージニア北部; us-east-1）リージョンに構成された AWS KMS が必要である。

また、Slack for EMM を利用するには EMM プロバイダを使って構成した Slack for EMM アプリを配布する必要がある。

すでに Slack を利用している状態で Slack Enterprise Grid に更新する場合は、必要に応じて Enterprise Gird のサンドボックス環境が提供される。

18 - 3． 機能概要

18-3-1． 組織内チャット

リアルタイムでのコミュニケーションに特化したチャット機能を提供する。チャンネルを作成して、話題ごとに特化したコミュニケーションがとれる。

18-3-2． ファイル共有

文字だけでなく、任意のファイルをアップロードして共有する機能を提供する。

18-3-3． 外部アプリケーションとの連携

各種アプリケーションからの通知を受け取ったり、API を使ってアプリケーションを直接操作したりする機能を提供する。

18 - 4． 注記

最初に Enterprise Grid を構成する担当者のアカウントが、Primary Owner となる。その担当者と Primary Owner であるべき者は異なる可能性があるため、構成完了後に Primary Owner を別のアカウントに変更する必要が生じる。その場合は、Slack 社に連絡して変更してもらう必要がある。

19. Zendesk

Zendesk は以下のサービス群で構成した。

- Support Enterprise

- Guide Enterprise
- Chat Enterprise
- Answer bot アドオン
- Explorer Lite および Professional

19 - 1 . ライセンス・プラン

監査機能が提供される Enterprise プランを選定した上で、各サービス単体ではなく、Suite ライセンスとして一体で調達した。3 製品以上を利用する場合は Suite ライセンスを調達した方が安価なためである。

19 - 2 . 取得時の留意事項

支払い方法は、クレジットカードのほか、国際送金も使用可能であり、年額払いと月額払いが選択できる。年額払いの場合、月額払いと比べ、月当たりの金額が安価となる。国際送金の場合は、ライセンス契約時に利用の有無にかかわらず、Zendesk Talk の従量利用料について一定額の前払いが必要になるなど、契約条件が変化するため注意を要する。

無償トライアル期間は 14 日間である。

豊富なアドオン機能を有するため、主要サービス単体で提供される機能なのか、アドオンで別途追加する必要がある機能なのかを契約前に入念に確認する必要がある。

上述の Talk 以外でも Answer bot アドオンなど従量課金のサービスがある。

19 - 3 . 機能概要

19-3-1 . Support Enterprise

チケット管理機能に加え、主に以下の機能を提供する。

- マクロ（定型操作を登録し、ワンクリック実行）
- トリガ（特定の操作・条件を起点として処理を実行）
- コンテキストワークスペース（条件による機能制限）
- モバイルアプリケーション

そしてサービス群に対しては、Zendesk 管理センターとして主に以下の機能を提供する。

- SAML・SSO・MFA・OIDC など、サービスプロバイダとしての認証管理
- パスワードポリシーの設定
- パスワード変更のメール通知

19-3-2．Guide Enterprise

ナレッジサイト機能に加え、主に以下の機能を提供する。

- Google Analytics 連携
- 記事公開のモデレート
- テーマカスタマイズ（ナレッジ記事へのコメント投稿部分不可視化に利用）

19-3-3．Chat Enterprise

チャット機能に加え、主に以下の機能を提供する。

- Web サイト設置用のウィジェットスクリプトの発行
- 営業時間設定
- Guide によるナレッジサイトへの Chat ウィジェットの自動設置

19-3-4．Answer bot アドオン

Support のサポートチケットに対する自動応答メールや、Chat ウィジェットからの問い合わせがあった際にナレッジ記事のサジェスト機能を提供する。

19-3-5．Explorer Lite および Professional

Zendesk Support・Chat・Guide・Answer bot アドオンの処理状況をダッシュボード化する。

19 - 4．注記

モバイルアプリケーションは複数のテナントに対して切り替えができず、都度サインアウト・サインインが必要となる。そのため、複数のテナントを跨って対応する必要がある要員の簡易確認に用いるには不適である。