クラウド活用の変遷とセキュリティ脅威

株式会社アイティアイ
代表取締役
大和　敏彦

内容

- クラウド活用の現状
- クラウドの進化
- 生成AIによるクラウド変革
- クラウドセキュリティの変化
- まとめ

クラウド活用の現状

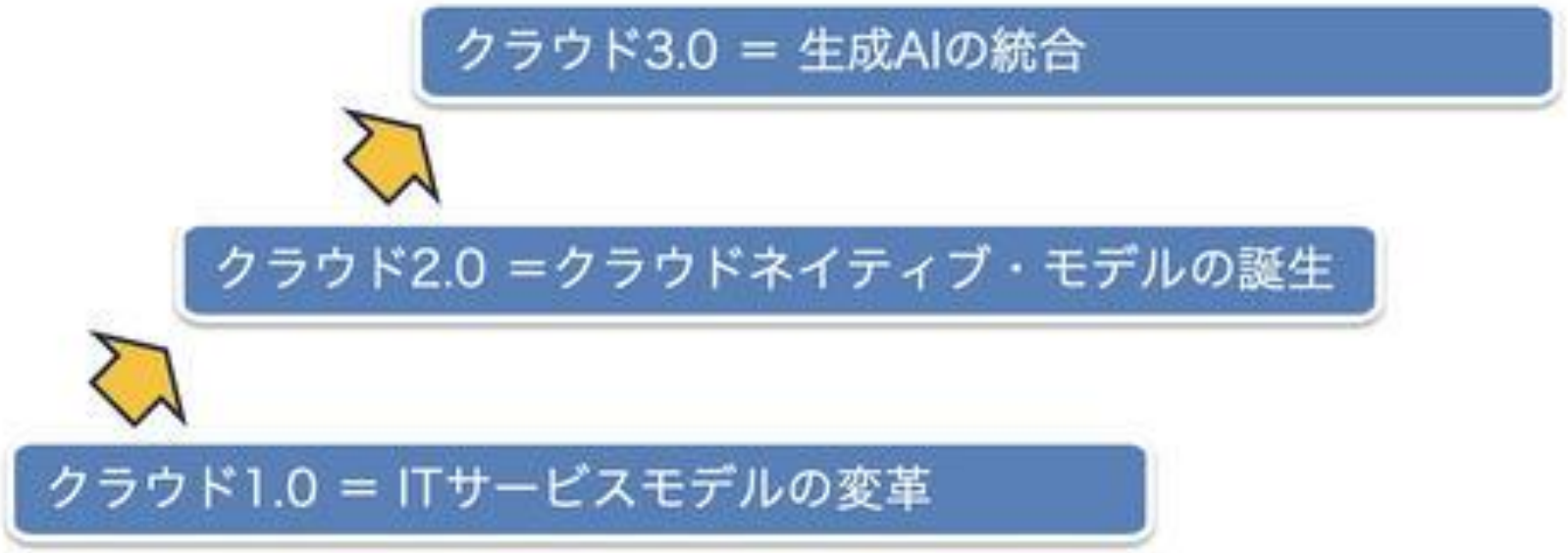
- クラウドインフラの伸び
  世界の2024年第3四半期のクラウドインフラサービス（IaaS、PaaS、Hosted Private Cloud）市場は前年度より24%増加し、838億ドルに。シェアのトップ3は、AWSがシェア31%、Microsoft　20%、Google 13%。（Synergy Research Group）

- SaaS
  世界のSaaS市場規模は、2024 年の 3175億5000万ドルが2032年には1兆2288億7000万ドルと年平均成長率18.4%で成長すると予測されている（米Fortune Business Insides調べ）。

クラウドの成長要因

- クラウドの成長要因は、DX（デジタルトランスフォーメーション）の広がりと、それを支えるサービスの多様化である。コンピューティング、ストレージ、ネットワークから、IoTや配信、ブロックチェーン、機械学習、それらに関するセキュリティ、サプライチェーンなどのビジネスアプリケーションまでがクラウドから提供されている。
- サービス例として、
  AWSは2024年7月時点で、324ものクラウドサービス製品を提供している。

クラウドは新しいモデルや考え方を生み出してきた



クラウド1.0＝ITビジネスモデルの変革

- クラウドの利用で物理的なインフラを管理する負担なしに、オンデマンドでコンピューティングリソースを使える、柔軟かつ経済的で効率的なインフラモデル

  - 新たなインフラを構築するための時間の遅延や投資が必要なく、企業はコアビジネスに集中できる。
  - 需要に応じてリソースを増減できるため、ビジネスニーズに合わせたサイズのインフラを使える。

クラウド1.0＝ITビジネスモデルの変革

- クラウドインフラを使い、アプリケーションをサービスとして提供するSaaSも急速に増えた。
- ネットワークの高速化によって実現したが、さらに並行してモバイルネットワークが進化したことで、どこからでも高速アクセスが可能になりスマホ主体のサービスが生まれ、モバイルありきの“モバイルファースト”化が進んでいる。クラウドとモバイルのメリットを生かした新しいビジネスモデルも生まれた。

クラウド活用のメリット

- 拡張性、柔軟性
- 活用、変化対応の迅速性
- 必要以外の技術力が不要
- 安定性、セキュリティ対策
- 固定資産不要
- コスト低減

クラウド2.0＝クラウドネイティブ・モデルの誕生

- クラウドの特性をより生かしたモデルが「クラウドネイティブ・モデル」である。
「クラウドネイティブ・スタック」と呼ばれるコンテナ、マイクロサービス、サービスメッシュなどを使って、アプリケーションは迅速な開発ができ、最新の機能や使い勝手を提供できる。

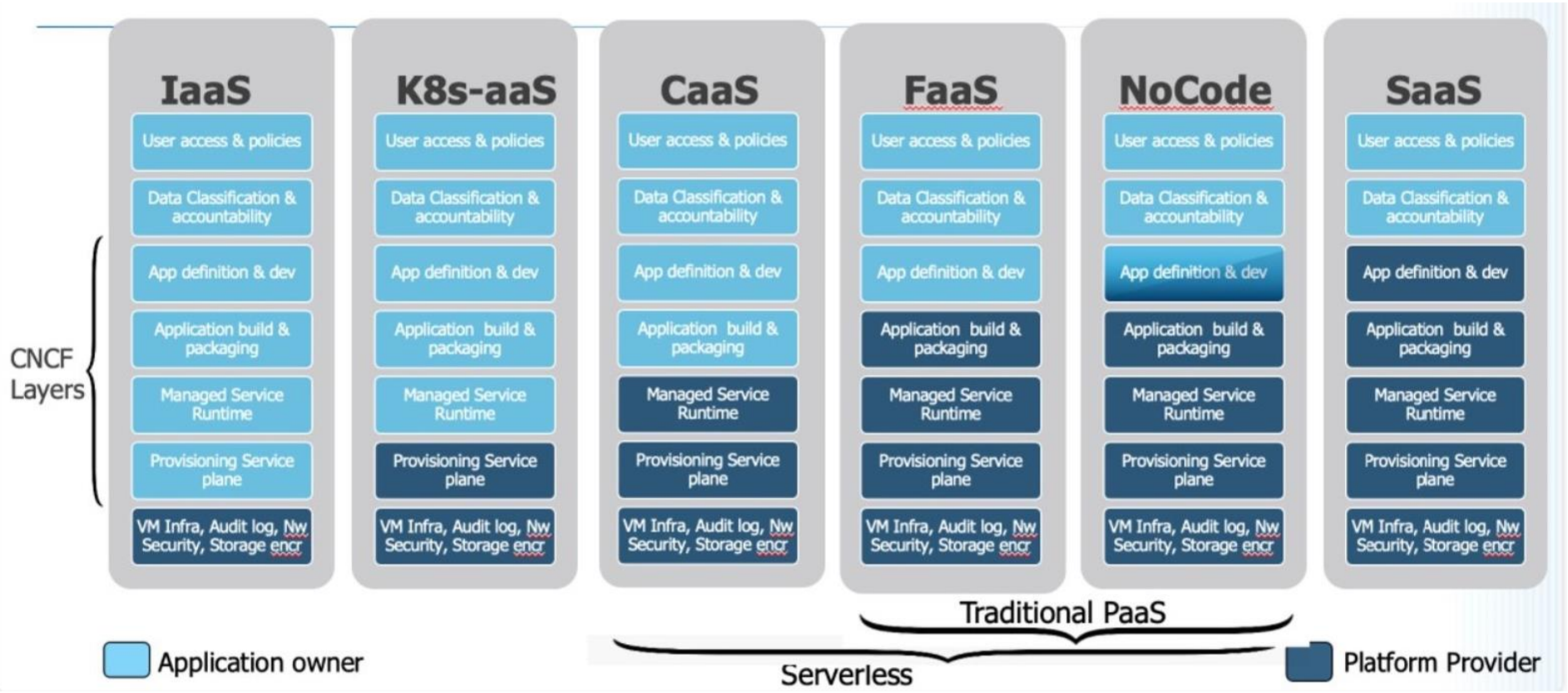
- コンテナ技術では、その推進と進化を取り巻くテクノロジー業界の足並みを揃えることを目的に「Cloud Native Computing Foundation（CNCF）」と呼ぶ財団も、Linux Foundationのプロジェクトとして設立されている。

クラウド2.0＝クラウドネイティブ・モデルの誕生

- クラウドネイティブ化によって開発も変化し、DevOps、DevSecOpsと呼ばれる開発担当と運用担当を連携し、確実なリリースを迅速に行える体制も生まれた。

- クラウドを開発・運用の観点で使い分け、パブリック、プライベート、ハイブリッドなど、それぞれの利点を活かす方法が広がっている。

クラウドの進化



クラウドによる進化

- クラウドは、「持つ」モデルから「使う」モデルへの変革
- システム活用の迅速化や効率化
- 開発や運用の変革
- クラウドサービスを使った新しいビジネスモデルの創出、ビジネス自体の変革

クラウド分散化

ソブリンクラウド

エッジコンピューティング

- データ量急増への対応
- 低遅延処理の要求への対応
- 帯域の制限やオフラインへの対応

分散化： Web3.0

分散化された環境でのマネジメント
分散化されたデータ、アプリケーションをどう守るか

クラウド3.0＝生成AIの統合

- 浸透する生成AI
  『生成AIに関する実態調査2024春（PwC Japan）』によれば、日本の大手企業の生成AI技術の活用において、「活用中」から「推進中」「検討中」までの合計が前回（2023年秋）の22%から91%にまで増加した。このうち「活用中」は43%と9ポイント増えた。
  進捗が進んでいる業界は上位から、通信、テクノロジー、サービス／接客業、公益事業／エネルギー、銀行／証券／保険／その他金融サービスである。
  活用対象は、事務作業の効率化や、チャット業務の自動化、新事業への展開などだ。活用効果も48%が「期待通り」とし、9%は「期待を上回っている」と回答している。

生成AIによるクラウドの進化と加速化

- あらゆる分野において生成AIによる改革は大幅に広がる。
- その内容は、ドキュメンテーションの処理、リーガルなどで文書の起草、要約、最適化した調査等ホワイトカラーの仕事を劇的に変え、自動化や新しい仕事、また、新しい仕事の仕方が生まれる。
- AI機能が組み込まれたSaaSも多くの分野で生まれている。

生成AIによるクラウドの進化と加速化

- アプリケーションだけでなく、クラウドのインフラの管理・自動化、セキュリティにも生成AIが使われる。
- 生成AIの学習のためには、データが必要とされる。データ蓄積と活用のためにもクラウドが使われる。データを統合して、使い易くするデータクラウドも生まれている。

クラウド活用への生成AI活用

- インフラ構築の自動化
  リソースの割り当てや設定、スケジューリング、バックアップ、セキュリティ設定、ネットワークなどの自動化によって、運用負荷を軽減し新しいサービスを迅速かつ正確に稼働できるようにする。

クラウド運用への生成AI活用

- ワークロード最適化
- リソース管理の自動化
- コストの最適化と予算管理：クラウドコストは、変動する需要や変動する価格設定モデル
- 予知保全と障害解決
- エンドユーザーとの対話
- セキュリティ対策の強化
- データの自動分類やインテリジェントな移行

生成AIによるコード生成

- 人が書いた指示や要件に従ってプログラミングコードを自動生成
- 例
  GitHub Copilot：GitHubのコードベースから学習、多様なコーディングスタイルや言語に対応したコード生成

  Amazon Codewhisperer：AWSサービスに最適化したコード提案。セキュリティ脆弱性検出と修正提案。

  OpenAI codex：人の指示に基づいてPython、JavaScript、Ruby、Goなど、複数のプログラミング言語を生成

クラウド化によるセキュリティ脅威

- サイバー攻撃
  不正アクセス
- Ransomware
- 情報窃取　Emotet
- 情報漏洩
- データ消去
- シャドウIT

IPA「情報セキュリティ十大脅威2024」組織向け

順位	脅威内容
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正のよる情報漏えい等の被害
4	標的型攻撃による機密情報の窃盗
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

サイバー攻撃の激化

- 子会社のドワンゴが運営する動画配信サービス「ニコニコ動画」「ニコニコ生放送」をはじめとする一連の「ニコニコ」サービスのほか、チケット販売の「ドワンゴチケット」などが提供不能になった。業務サーバーも影響をうけた
- 他にもランサムウェア被害を公表している企業は、
  株式会社日立製作所、ホンダ自動車、株式会社カプコン、株式会社エーザイなど
- 中小企業の7割が何かしらのサイバー攻撃の被害にあった（総務省）
- 身代金の支払いが急増
- クラウドへの攻撃がますます増加。2023年にはクラウドへの侵入が75%増加し、クラウドを意識した事例は110%の急増が見らた。

境界型セキュリティの崩壊

- 「社内は安全」「社外は脅威」ということが前提となり、社内と社外の境界を防衛する「境界型セキュリティモデル」を採用。
- クラウド、マルチクラウド、ハイブリッドクラウド、SaaSの活用によって、ますます境界はなくなる。

CSA本部が提供しているZero Trust Resource Hubの日本語ウエブページ

ゼロトラストの指針となる原則

- 包括的なセキュリティ戦略とアプローチで「信頼せず、常に検証する」、
- 最小特権の概念、セグメンテーションの実践
- 防衛力を高め、インシデントによる損害を削減し、復旧時間の 短縮を促進する。
- 範囲を制限し、侵害の影響を軽減すると同時に、迅速な回復を促進する 手段を提供する
- IT資産やデータだけでなく、アプリケーション、資産、サービスも含む。

ゼロトラスト

- ゼロトラストは、ネットワーク内のすべての通信を検証するセキュリティモデル。
- アクセス制御と監視を組み合わせて、セキュリティの透明性と可視性を向上させる。リソースにアクセスを正確に把握することにより、セキュリティインシデントの検出と対応を容易にする。
- 下記の徹底
  - アイデンティティとアクセス管理 (IAM):
  - マイクロセグメンテーション
  - 通信やアクセスの検証
  - セキュリティ インシデントの監視と対応

生成AI技術の悪用

- サイバー攻撃における、セキュリティシステムの脆弱性や潜在的な攻撃点を迅速に特定
- AIによる自動的な攻撃
- フィッシングで様々な目的で正当に見えるメールの作成
- マルウェア生成

Splunk CISOレポート

- 35%のCISOがすでに生成AIをセキュリティ業務に活用し、61%が今後1年以内に活用することを検討中と回答している。
- 86%のCISOが、生成AIはセキュリティチームのスキル不足や人材不足を補うために役立つと期待している。
- CISOが考えるAIの悪用で上位に入ったのは、攻撃のスピードと効率の向上(36%)、フェイク音声/画像を使ったソーシャルエンジニアリング(36%)、サプライチェーン攻撃での対象領域の 拡大(31%)

AIによる対策

- 攻撃手法、インシデントの点検におけるAIによる攻撃検知支援
- ログデータのリアルタイム分析による潜在的な脆弱性の発見
- AIによるインシデント分析支援
- リアルタイムでの脅威検出やインシデント対応
- インシデントの優先順位付け
- インシデントの通知の自動化

- セキュリティオペレーションの自動化

AIの進化

- 会話能力の強化
  自然な会話、同時通訳
- 推論機能の搭載
- マルチモーダル機能
- 信頼性の向上、ハルシネーションの削減
- 役割の実現
  小規模生成AIの連例による処理
- 分散化
  PCやスマホ

まとめ

- クラウドは進化し、更に活用は増える
- マルチクラウド、ハイブリッドクラウド化が進む
- 処理形態やデータストアは多様化し、分散化する
  それへの対処が必要
- サイバー攻撃は増加し、攻撃スピードは上がっている
  AIによる対処が必要
- ゼロトラストの考え方はますます重要になる