「クラウドの重大セキュリティ脅威 パンデミック11」

一般社団法人　日本クラウドセキュリティアライアンス

業務執行理事　諸角昌宏

CCSP, CCSK, CSAリサーチフェロー

2022年11月17日

アジェンダ

1. CSA Top Threatの歴史、重大脅威の変化
2. 「クラウドの重大セキュリティ脅威　パンデミックイレブン」構成、解説
3. 「クラウドの重大セキュリティ脅威　パンデミックイレブン」トップ５概要

1. CSA Top Threatの歴史、重大脅威の変化

CSA Top Threatの歴史(1)

2010年（Top Threats）

1. Abuse and Nefarious Use of Cloud
   クラウドコンピューティングの不正および犯罪目的の利用
2. Insecure Interfaces and APIs
   安全ではないインターフェースおよびAPI
3. Malicious Insiders
   悪意ある内部者
4. Shared Technology Issues
   共有技術問題
5. Data Loss or Leakage
   データ喪失または漏えい
6. Account or Service Hijacking
   アカウントハイジャック、サービスハイジャック
7. Unknown Risk Profile
   未知のリスクのプロファイル

2013年（The Notorious Nine）

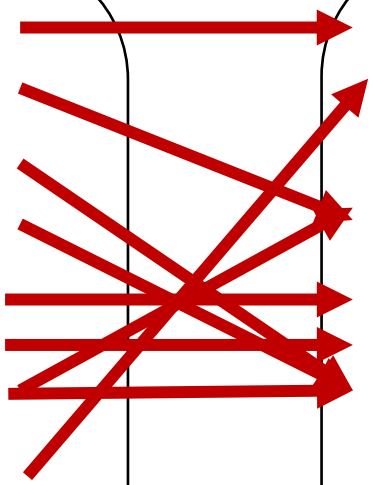
1. Data Breaches
   データ侵害
2. Data Loss
   データ喪失
3. Account Hijacking
   アカウントハイジャック
4. Insecure APIs
   安全ではないAPI
5. Denial of Service
   DoS攻撃
6. Malicious Insiders
   悪意ある内部者
7. Abuse of Cloud Services
   クラウドサービスの不正利用
8. Insufficient Due Diligence
   不十分なデューデリジェンス
9. Shared Technology Issues
   共有技術問題

注意：翻訳版の提供無し

CSA Top Threatの歴史(2)

2017年（Treacherous 12
危険な12 の落とし穴）

1. データ漏洩(Data Breaches)
2. 不十分なアイデンティティ・認証情報・アクセス管理
3. API のセキュリティ欠陥
4. システムとアプリケーションの脆弱性
5. アカウントの乗っ取り
6. 悪意ある内部者
7. 標的型攻撃の脅威（APT）
8. （CSP)データ喪失
9. 不適切なデューデリジェンス
10. クラウドサービスの誤用・悪用
11. DoS 攻撃
12. 共有技術の脆弱性



2019年（11の悪質な脅威）

1. データ侵害(Data Breaches)
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用

CSA Top Threatの歴史からわかること（2017~2019）

1. 「一般的な脅威」から「現実に即した脅威」への変化
   - 第3回（2017年）までのTop Threatは、クラウドに対する一般的な脅威、リスク、脆弱性に着目
   - 第4回（2019年）では、一般的な脅威等に関するものはあまりフォーカスされなくなってきている
2. クラウドに対する利用者の理解の成熟度の向上
   - プロバイダ責任に対する脅威の順位の低下（No worry to CSPの傾向）（第3回（2017年）の図の青色項目）
     - （CSP)データ喪失、DoS 攻撃、共有技術の脆弱性
     - 利用者がセキュリティ責任を持つ項目の増加

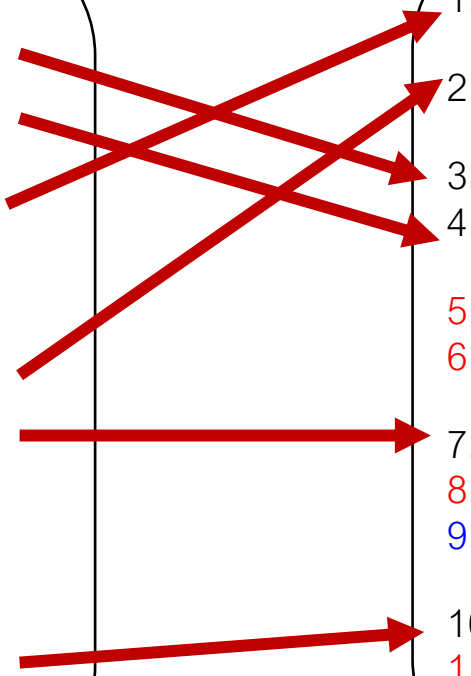
	第3回（2017年）	第4回（2019年）
利用者	2, 6, 9	2, 3, 4, 6, 8
プロバイダ	8, 11, 12	
両方	1, 3, 4, 5, 7, 10	1, 5, 7, 9, 10, 11

注意： 2017年は資料には明記されていない

CSA Top Threatの歴史(3)

2019年（11の悪質な脅威）

1. データ侵害(Data Breaches)
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用



2022年（パンデミック11）

1. 不十分なアイデンティティ、資格情報およびアクセスとキーの管理 (4)
2. セキュアでないインターフェースやAPI(7)
3. 設定ミスと不適切な変更管理(2)
4. クラウドセキュリティのアーキテクチャと戦略の欠如(3)
5. セキュアでないソフトウェア開発
6. セキュアでないサードパーティーリソース
7. システムの脆弱性 (8)
8. 予想外のクラウドデータ公開
9. サーバレスやコンテナワークロードの構成ミスや悪用
10. 組織的な犯罪、ハッカーとAPT(11)
11. クラウドストレージデータ流出

CSA Top Threatの歴史からわかること（2019~2022）

1. プロバイダ側のみに起因する脅威は引き続きゼロ
   - 利用者に起因する脅威はがセキュリティ責任を持つ項目は継続して増加

	第3回（2017年）	第4回（2019年）	第5回（2022年）
利用者	2, 6, 9	2, 3, 4, 6, 8	1, 4, 6
プロバイダ	8, 11, 12		
両方	1, 3, 4, 5, 7, 10	1, 5, 7, 9, 10, 11	2 3 5 7 8 9 10 11

2. 「より具体的な脅威」に移行
   - 2022年で新たに入ってきたもの
     - セキュアでないソフトウェア開発、セキュアでないサードパーティーリソース、予想外のクラウドデータ公開、クラウドストレージデータ流出
   - データ侵害が2022年で消えた
     - 予想外のクラウドデータ公開、クラウドストレージデータ流出など、具体的な脅威に着目

3. 「クラウドネイティブの脅威」に着目
   - 2022年で新たに入ったもの
     - サーバレスやコンテナワークロードの構成ミスや悪用

CSA Top Threatの歴史からわかること（まとめ）

1. CSPの管理下にあるクラウドセキュリティの課題は下がっている
   - 第3回（2017年）までのTop Threatは、クラウドに対する一般的な脅威、リスク、脆弱性に着目
   - 第4回（2019年）では、「一般的な脅威」から「現実に即した脅威」への変化
   - 第5回（2022年）では、「**より具体的な脅威**」に移行。新しいテクノロジーに絡む脅威に着目
2. 利用者がセキュリティ責任を持つ項目が継続して重大脅威としてリストアップ
   - クラウド利用者が弱点であることを指摘
   - 利用者が直接コントロールできる状況に焦点を当ててきている
3. 新しいテクノロジーに基づく脅威
   - サーバレスやコンテナワークロードの構成ミスや悪用
   - アジャイル、DevOpsなどセキュアなソフトウエア開発
   - プロバイダ管理責任が大部分となる

2. 「クラウドの重大セキュリティ脅威　パンデミックイレブン」

構成
解説

「クラウドの重大セキュリティ脅威　パンデミックイレブン」 構成(1)

セキュリティの課題1:
不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント

アイデンティティ、クレデンシャル、アクセス管理システムには、組織が貴重なリソースへのアクセスを管理、監視、セキュアにするためのツールやポリシーが含まれています。例えば、電子ファイル、コンピュータシステム、サーバールームやアイデンティティ、クレデンシャル、アクセス管理システムには、組織が貴重なリソースへのアクセスを管理、監視、セキュアにするためのツールやポリシーが含まれています。例えば、電子ファイル、コンピュータシステム、サーバールームや建物などの物理的なリソースが含まれる場合があります。

適切なメンテナンスと継続的な警戒が重要です。IAM（アイデンティティ・アンド・アクセス・マネジメント）においてリスクスコアリングを使用することで、セキュリティ体制を強化することができます。明確なリスク割り当てモデルを使用し、入念に監視し、その動作を適切に分離することで、IAM システムのクロスチェックが可能

Security Responsibility	
✓ Customer	
✗ Cloud Service Provider	
✗ Shared	

Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra

Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

管理責任の対象者
- 利用者
- プロバイダ
- 両方

アーキテクチャ
- インフラストラクチャ
- メタストラクチャ
- インフォストラクチャ
- アプリストラクチャ

サービスモデル
- SaaS
- PaaS
- IaaS

「クラウドの重大セキュリティ脅威　パンデミックイレブン」 構成(2)

ビジネスインパクト

不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵管理、ならびに特権アカウントによる悪影響は、以下を含む場合があります。

- 後手後手の過剰なロックダウンによる業績悪化と生産性の低下
- 従業員のテスト疲れによるコンプライアンス不足とセキュリティへの無関心
- データの置き換えや破損と、不正または悪意のあるユーザによるデータの流出の比較
- 市場からの信頼と収益の損失
- インシデント対応およびフォレンジックにかかる金銭的費用

要点

適切なIAM、クレデンシャル、鍵管理の結果には、以下のようなものがあります。

1. エンタープライズアーキテクチャの中核をなす強固な防御は、ハッキングの標的を攻撃がより容易なエンドポイントユーザのアイデンティティへ移します。
2. 堅牢なゼロ・トラストレイヤには、個別のユーザに対する単純な認証や、アプリケーションベースの隔離以上のものが必要です。
3. また、運用ポリシーや構造化リスクは、CIEMのような先進的なツールに不可欠なモデルです。[1]
4. ユーザオブジェクトには、ビジネスの要求に応じて動的に調整されるリスクスコアを与えなければなりません。信頼は獲得されるべきもので、単に鍵やコードを提供することではありません。

想定事例と実例

このセキュリティ課題のクラウドインシデントの最近の事例を紹介します。

- (2021)国家による攻撃は増加傾向にあり、より巧妙になっている。2021年は、Twitch、Cosmology Kozmetik、PeopleGIS、Premier Diagnostics、SeniorAdvisor、Reindeer、Twilloを巻き込んだ侵入があり、これらの攻撃の大半は内部脅威からの特権乱用でした。リスクとレジリエンスを監視していない企業は、ダイナミックな脅威の状況に足元から直面しています。[2]
- (10/2021) SEGA Europeのクラウドを詳しく見ると、2つの重要な構成管理クラウドの設定ミスが浮き彫りになりました – AWS S3バケットがパブリックアクセス権限に設定されていました。ハードコードされたクレデンシャルは、クラウドに保存されていました。AWSとCDNネットワークにおける

「クラウドの重大セキュリティ脅威　パンデミックイレブン」 構成(3)

CSAガイダンスの対象ドメイン

対象となるCCMの管理策

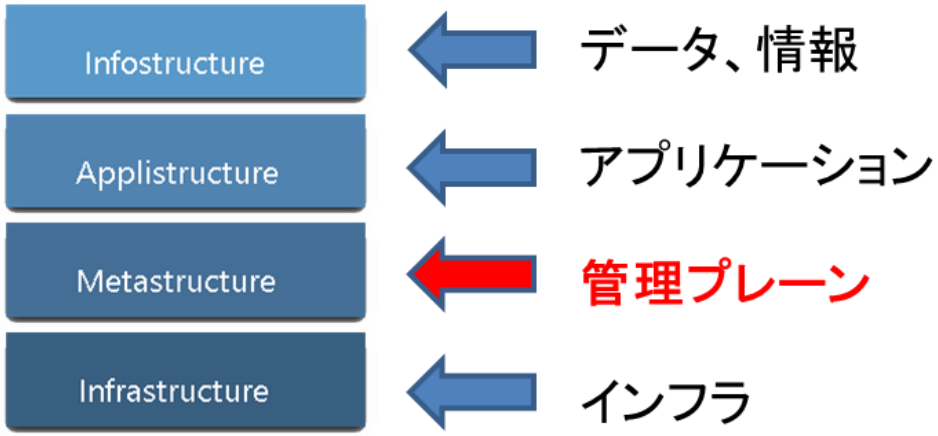
対象となるSTRIDE脅威モデル

参照情報とリンク

アーキテクチャ　ー　論理モデル

- インフラストラクチャ
  - コンピューティングシステムの基本構成要素： CPU 、ネットワーク、ストレージ。その他の全てがその上に形成される基盤。（物理的に）動作する部分である。
- メタストラクチャ
  - インフラストラクチャレイヤーと他の レイヤ の間の インターフェイス を提供するプロトコルおよびメカニズム。各技術の間を結び付ける「のり」で、管理と設定を実現する。
- インフォストラクチャ
  - データと情報。データベース、ファイルストレージその他の中身。
- アプリストラクチャ
  - クラウド上に展開されたアプリケーションと、その構築のために使われる下層のアプリケーションサービス。例としてはメッセージキューのような PaaS の機能、人工知能分析、通知サービスなど。

（CSAガイダンス4.0より引用）



CCM

責任共有モデルにおける推奨事項（CSAガイダンスより引用）

- クラウド事業者 は、内部のセキュリティ対策と利用者向けのセキュリティ機能をはっきりと文書で示し、クラウド利用者が情報に基づく意思決定をできるようにすること。事業者はまた、それらセキュリティ対策を適切に設計し実装しなければならない。
- クラウド利用者 は、クラウドプロジェクトに際し、責任分担表を作成して誰がどの対策をどのように実装する必要があるのかを文書で示さなければならない。これは同時に、必要な準拠すべき基準に対応していなければならない。

CCM, CAIQはそのためのツール

A&A	Audit and Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization Security
CCC	Change Control and Configuration Management	LOG	Logging and Monitoring
CEK	Cryptography, Encryption and Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency & Accountability
DSP	Data Security and Privacy	TVM	Threat & Vulnerability Management
GRC	Governance, Risk Management and Compliance	UEM	Universal EndPoint Management
HRS	Human Resources Security		

STRIDE脅威モデル

STRIDE	日本語	セキュリティ対策
Spoofing Identity	なりすまし	認証
Tampering with data	データの改ざん	デジタル署名
Repudiation	否認	監査、ログ
Information Disclosure	情報漏洩	暗号化
Denial of Service	サービス拒否	可用性（クラスタ、フェールオーバーなど）
Elevation of privilege	特権の昇格	認可

3.　「クラウドの重大セキュリティ脅威　パンデミックイレブン」

トップ５概要

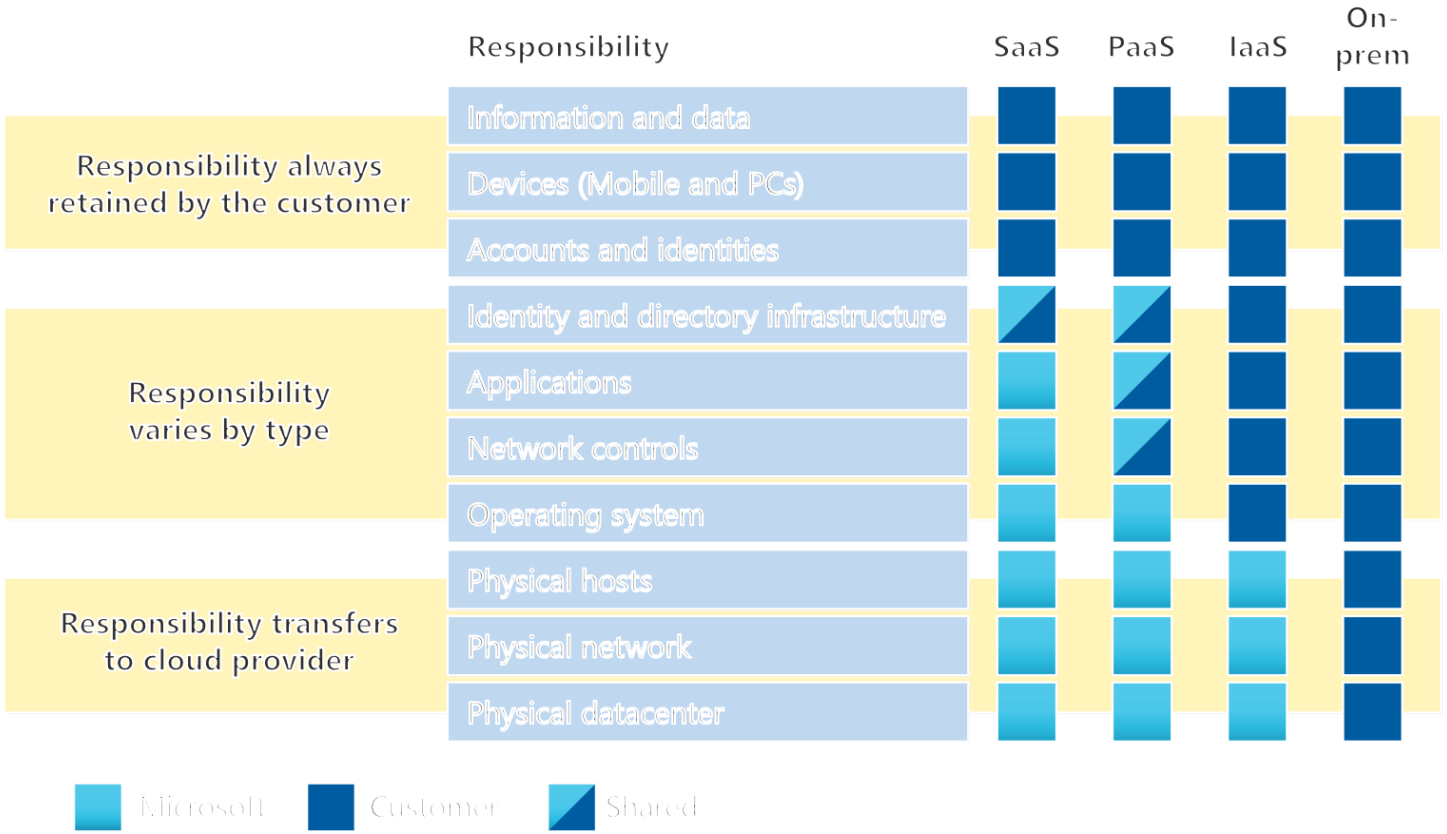
1. 不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント (1)

責任共有モデルの3つのカテゴリ

① すべてのサービスモデルにおいてクラウド利用者が責任を持つ

② クラウド利用者とクラウド事業者がサービスモデルによって責任範囲が決まる

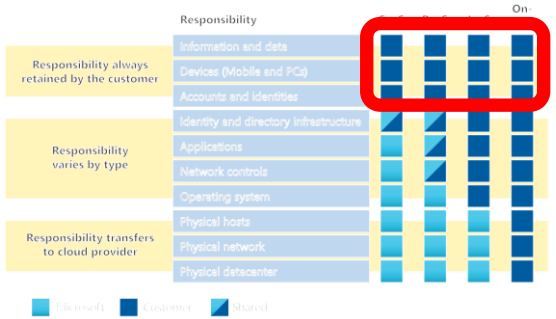
③ すべてのサービスモデルにおいてクラウド事業者が責任を持つ



引用：https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

1. 不十分なアイデンティティ、クレデンシャルおよびアクセスと鍵の管理、ならびに特権アカウント (2)

- カテゴリ①に含まれるもの
  - データ、情報ガバナンス
  - **アイデンティティ、アクセス管理（IAM)**
  - クライアントセキュリティ



- クラウドを利用するにあたって、クラウド利用者が設定、管理、監視等の責任を持つ。クラウド事業者は、環境を用意
- 従来のインフラセキュリティでは対応しきれない
  - インフラセキュリティ　ー＞　データセキュリティが必要
- 複雑なID、アクセス管理が必要
  - クラウドサービスごとのID、アクセス管理
  - 場所、デバイス等の属性に基づくアクセス管理
- 暗号化における利用者鍵管理の必要性

2.　セキュリティの課題2: セキュアでないインターフェースやAPI

- クラウド観点での脅威
  - API:　クラウドサービスにアクセスするためのインターフェース
    - クラウドサービスにはAPIを通してアクセス
    - クラウドサービス同士のAPIを通した相互運用
    - APIを通した監視、管理
  - 脅威の例
    - 未認証のエンドポイント、弱い認証、過剰な権限、標準的なセキュリティコントロールの無効化、パッチ未適用のシステム、など。

- セキュリティ対策
  - API、アプリケーションの安全な設計
    - セキュリティ・バイ・デザイン
    - 構成管理、テスト、監査など
  - プロバイダが公開する仕様の確認
  - 提供されるSDKやコマンドの脆弱性情報、パッチ情報の把握、運用

3.　設定ミスと不適切な変更管理

- クラウド観点での脅威
  - なぜ、クラウド設定ミスによる問題が多発するのか？
    - オンプレのアプローチでは、クラウドでは効果的ではない
      - インフラセキュリティ　->　データセキュリティ
    - クラウドサービス固有の設定、クラウドに依存した変更管理
  - 脅威の例
    - 過剰な権限、パッチが適用されていないシステム、ロギングの無効化またはモニタリングの無効化、ポートおよびサービスへの無制限のアクセス、など。

- セキュリティ対策
  - 変更管理の徹底
  - 自動化の採用
  - 継続的に検査、監視
  - アプリケーション設計におけるセキュリティ

4.　クラウドセキュリティアーキテクチャと戦略の欠如

- クラウド観点での脅威
  - 「フォークリフト」、「リフト＆シフト」思考
    - クラウドベースのサービスを念頭に置いて開発されていない
    - すべてのアプリケーションがクラウドに移行できるわけではない
    - クラウド固有のリスクへの対応
  - 管理責任の明確化の欠如。責任共有の理解の欠如
  - 不十分なデューデリジェンス

- セキュリティ対策
  - ガバナンスの見直し
  - 十分なデューデリジェンス、デューケアの実施
  - アプリの理解と追加のセキュリティ対策
  - クラウド・インフラのセキュリティ
  - サプライチェーン管理

5： セキュアでないソフトウェア開発

- クラウド観点での脅威
  - クラウド対応のアプリ開発の問題。クラウドセキュリティ基準への対応
  - クラウド環境での開発のトレーニング、認識の不足
  - クラウドへのデータの保存、移動に対する暗号化依存の考慮
  - プロバイダのAPIとの統合の複雑さ
  - マルチテナンシー環境としてのセキュリティ要件の課題

- セキュリティ対策
  - セキュリティに配慮したアプリケーション開発（セキュリティバイデザイン）
    - ISO/IEC 27034, NIST SP800-218, Microsoft Security development Lifecycle など
  - アプリケーションセキュリティテストの自動化
  - アイデンティティとアクセス管理

ありがとうございました！

https://cloudsecurityalliance.jp
info@cloudsecurityalliance.jp