C-Chorus

セキュリティホワイトペーパー

AWS リセール / マネージドサービス

1.00 版

NHN テコラス株式会社

目次

改訂履歴

版	改定日	改定内容
1.0	2019/12/24	初版のリリース

はじめに

本ホワイトペーパーについて

NHN テコラス株式会社（以降、当社と表記）の AWS を基盤としたマネージドサービス（以降、MSP サービスと表記）についてご理解をいただくために提供するものです。

対象読者　AWS、当社 MSP サービスをご利用中のお客様、または導入をご検討中の方

クラウドプラットフォームによる責任共有モデルに対応する責任分担の表記と理解について

国際的なクラウド事業者（AWS / GCP / Azure 等）はセキュリティに対して責任共有モデル（shared responsibility model）を採用しています。また、セキュリティに対する責任共有モデルは、各クラウド事業者、またはサービスモデルにより異なります。クラウドプラットフォームを正しく利用するためには、この責任共有モデルの考え方に対する理解が必要となります。

AWS の責任共有モデル

AWS の責任共有モデル（https://aws.amazon.com/jp/compliance/shared-responsibility-model/）は「AWS の責任はクラウド“の”セキュリティ」とし、「お客様の責任はクラウド“における”セキュリティ」と定義しています。

当社 MSP サービス提供時の責任共有モデル

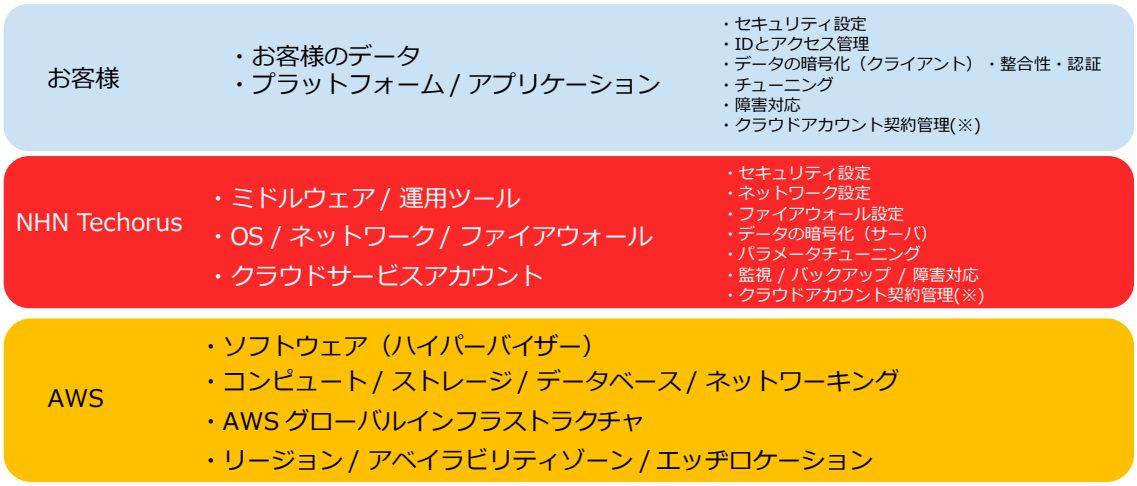
この AWS の責任共有モデルを踏まえたうえで、当社 MSP サービスの提供を受けているお客様に対しての責任共有モデルを示します。

お客様は、

１．当社が AWS を基盤として初期構築したシステム上で各種アプリケーションを運用する

２．お客様が構築したシステムの部分の運用を当社に委託する

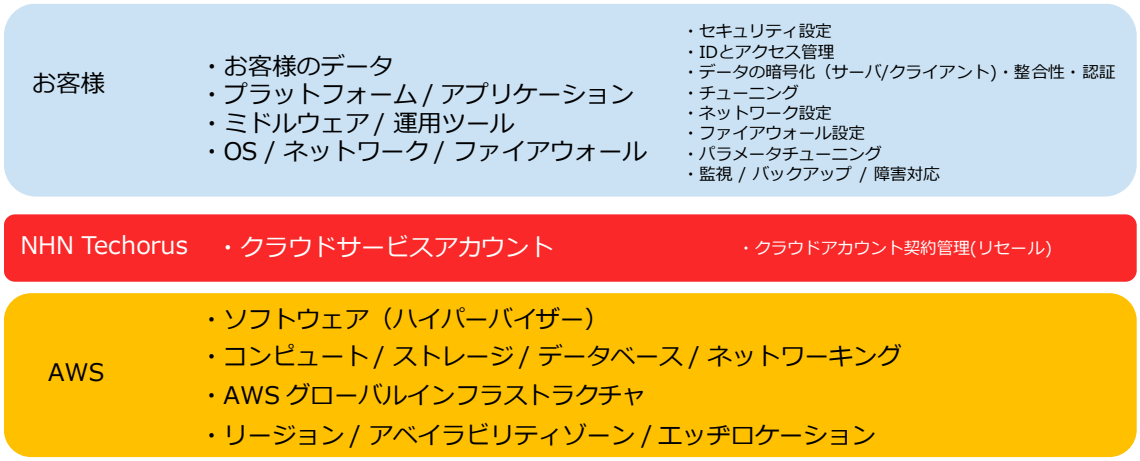
のいずれかに該当しますので、セキュリティ上の責任は、お客様と当社と AWS の三者による分担となります。



※AWS アカウント契約の主体がお客様（直接契約)の場合と、当社リセールサービスからの提供を受けている場合でセキュリティにおける責任が異なります。

当社リセールサービスの責任共有モデル

当社リセールサービスのみをご利用時の責任共有モデルを示します。



セキュリティへの取り組み

当社では、情報セキュリティリスクに対して、組織的・物理的および技術的セキュリティ管理策を講じております。
お客様の重要な情報資産を預かり運用する立場から、情報セキュリティの継続的改善をおこない、安心・信頼していただけるサービスの提供に、日々努めてまいります。

情報セキュリティマネジメントシステム（ISO/IEC 27001）

当社は 2005 年 3 月に「BS7799-2:2002」および「ISMS 認証基準(Ver.2.0)」による認証を取得
2007 年 4 月に認証基準の国際規格化に伴い、従来規格から国際規格 ISO27001 に準拠したマネジメントシステムへ移行し、認証を取得（兼、維持審査）しております。

ISMS クラウドセキュリティ（ISO/IEC 27017）

当社は 2018 年 4 月に ISO27017 認証を取得しております。

当社のセキュリティ体制とセキュリティポリシー

情報セキュリティマネジメントシステム（ISMS）

当社の情報セキュリティマネジメントは、当社の情報セキュリティマネジメント管理規定に基づき、以下の体制で行っています。

情報セキュリティ委員会

情報セキュリティマネジメント管理規定に基づき情報セキュリティ委員会を設置しています。当社の情報セキュリティに関する事案を審議するもので、月次で開催しています。

情報セキュリティ管理責任者

当社の ISMS の運営、維持、推進に関する責任者です。

監査

ISMS 監査

当社の ISMS が ISO27001 規格および関連する法令・規制に適合し、有効に実施・維持されていることを確認するため、内部監査を年 1 回実施しています。
なお、情報セキュリティ委員長が必要と判断した場合は、臨時に監査を実施します。

当社役職員による MSP サービス運用業務の遂行について

オフィス・データセンターのセキュリティ

当社役職員が利用するオフィス、およびデータセンターは、火災、落雷、津波、地震などを含む自然災害、および障害を避けた立地の建物を選定しています。
データセンターでは 24 時間 365 日体制で設備管理訓練を受けた警備員が常駐し、建物への入館者をチェックすると共に、館内各フロア入退室口に設置された監視カメラにて常時監視しています。
電源は東京電力からリング状経路にて 3 系統で受電。各階には容量 500KVA の UPS を設置しており、お客様には無停電の電源環境を用意しています。また万一商用電源の供給が停止した際には自動的に 3,500KVA のガスタービン発電機 2 台に切り替え運転、地下タンクに貯蔵する 70,000ℓ の燃料により、24 時間以上の電源を安定供給いたします。
サーバルーム空調は空冷式のパッケージ空調機を各階に設置し、機器類に適した温度管理を行います。床吹き上げ式の空調で常時温度を 23℃±2℃に保ちます。当社役職員の入館は個人ごとの IC セキュリティカードにより、ビルエントランス/サーバルームにセキュリティレベルに応じ各区画に入室権限を設定し施錠管理されております。お客様を含む当社役職員以外の人員の入館につきましては事前申請の上、身分証明書による本人確認後、当社役職員が立会いの下での入館としています。
管理室中央監視装置にて、電源空調等、各ファシリティの運転状況を常時監視しています。

物理的セキュリティ境界の設定

オフィス・データセンターでは下記のセキュリティ区画を設定し、入退室管理を行っています。

セキュリティエリア 0（当社の管理外エリア）

当社がオフィス・データセンターで契約する建物・部屋以外のビルのエントランス・エレベーターホールなどの共用部に相当する部分です。

セキュリティエリア 1（会議室・カフェエリア・喫煙室）

当社役職員が部外者の対応を行うエリアです。エリアの入り口は IC セキュリティカードで常時施錠しています。IC セキュリティカード保有の当社役職員が入室時に開錠しています。

セキュリティエリア 2（データセンター・オフィス執務室・倉庫エリア）

当社役職員が業務を行うエリアおよび機密性の高い資産を保管するエリアです。IC セキュリティカードによって当社役職員の物理的なアクセスを制限しています。当社役職員は、ネックストラップに IC セキ

ュリティカードを入れて着用し、役職員が識別できるようにしています。当社役職員以外の入館につきましては事前申請の上、身分証明書による本人確認後、当社役職員が同行します。

セキュリティエリア３（データセンター / オフィスサーバルーム）

セキュリティの要求が高い業務を行うエリアです。情報セキュリティ管理責任者により許可された当社役職員の入退室が可能なエリアです。当社役職員以外の入館につきましては事前申請の上、身分証明書による本人確認後、当社役職員が同行します。

建物・部屋の物理的なネットワークの保護

当社で管理する物理的なネットワーク、及び外部通信回線はネットワーク機器の専用ラックをセキュリティエリア３に設けて入退室を制限し、ラックへは施錠を行っています。
ネットワーク機器及び外部通信回線機器への物理的な接続を可能とする機器の設置は情報セキュリティ管理責任者が許可したものを除き、持ち込みを禁止しています。
部外者には、障害対応や保守の理由により情報セキュリティ管理責任者から明確な承認がある場合を除き、セキュリティエリア２およびセキュリティエリア３の物理的なネットワークへの接続を禁止及び遮断しています。

ネットワークのセキュリティレベル

情報セキュリティマネジメント管理規定のアクセス管理規則に基づき、セキュリティレベルに応じて業務ネットワークと安全領域外のネットワークを分離しています。

不特定の第三者が接続するネットワーク（ゲストネットワーク）

セキュリティエリア１で訪問者などへのインターネットアクセスを提供するネットワークです。
無線（暗号化通信）による接続のみ提供し、一般的な Web アクセスに絞った接続を許可しています。業務ネットワークとは分離されています。

当社役職員が接続するインターネットアクセス

セキュリティエリア２およびセキュリティエリア３で当社役職員が使用する端末でインターネットアクセスのみを提供するネットワークです。
無線（暗号化通信）による接続のみ提供しています。このネットワークから業務ネットワークへのアクセスはできません。

業務ネットワーク

セキュリティエリア２およびセキュリティエリア３で当社役職員が使用する端末で業務を行うためのネットワークです。
無線（暗号化通信）及び有線ネットワークで接続が可能で、登録された端末のみが利用可能で、業務ネットワークへの接続には認証が必要です。

認証

業務ネットワークでは以下の認証を併用しています。

端末認証

接続する端末が当社組織に属する端末であることを認証します。

ユーザー認証

ログインするユーザーが当社役職員であることを認証します。

パスワードの管理

当社役職員の本人以外の不正利用を防止するため、情報セキュリティマネジメント管理規定のアクセス管理規則に基づき、強度の高いパスワードの管理をしています。

認証情報の管理

当社役職員の認証情報は統合認証基盤で一元管理されております。業務ネットワークへのアクセスには、この統合認証基盤による認証を必要とし、これにより退職者および休職者の役職員のアカウントを即日無効化または削除を行い業務ネットワークへのアクセスを遮断しています。

MSP サービス利用時の AWS アカウントの管理

AWS アカウントとルートユーザーの取扱いについて

当社リセールサービスを利用して AWS アカウントを新規に取得、または当社リセールサービスへアカウントを移管した場合、AWS アカウントのルートユーザーの所有・管理は、お客様が直接 AWS とご契約をした場合と異なります。

	お客様で作成されたAWSアカウント (リセラーを使用しない一般的なご契約)	当社リセールサービスをご利用のAWSアカウント (リセラーを使用したAWSのご契約)※
AWSアカウントの所有・管理	お客様	リセラー（当社）
ルートユーザーの所有・管理	お客様	リセラー（当社）

※既にお持ちの AWS アカウントを当社リセールサービスへ契約移管した場合の移管後の所有・管理も当社となります。

当社リセールサービスをご利用の AWS アカウントの管理

AWS アカウントの作成

当社リセールご契約後、お客様が利用する AWS アカウントを新規に作成します。

AWS アカウントの管理

AWS アカウントのルートユーザーは当社が所有・管理をし、AWS の契約内容の確認や変更等、当社が規定する作業等を除き、通常は使用しません。
ルートユーザーには多要素認証（MFA）を設定し当社が厳重に管理をします。

AWS アカウントの廃止

当社リセールサービスの AWS をご解約の場合、解約の申請からサービスの規約に定めている期間で AWS アカウントの廃止手続きが完了します。

お客様が直接ご契約されている AWS アカウントの管理について

AWS アカウントのルートユーザーはお客様の所有・管理となります。
MSP サービスをご利用される場合、当社からはルートユーザーの取扱いについて、AWS のベストプラクティスに則り、当社と同等のレベルでの利用を推奨させていただいております。

お客様ご利用の AWS アカウントへのアクセスの制限

当社では当社役職員が MSP サービスご利用のお客様の AWS アカウントへアクセスを実施するにあたり、以下の制限を行っています。

当社リセールサービスをご利用の AWS アカウントの場合

MSP サービスを提供する際には、お客様ご利用の AWS アカウントに対して、当社役職員が利用する必要最低限のアクセス権限を付与した IAM ロールを作成します。当社役職員は、統合認証基盤によるログイン認証、多要素認証によるアクセスのみを可能とした環境へログインを実施し、お客様がご利用の AWS アカウントへアクセスを実施します。

お客様が直接ご契約されている AWS アカウントの場合

MSP サービスを提供する際には、当社の踏み台用 AWS アカウントからのアクセスを許可していただき、必要最低限のアクセス権限を持った IAM ユーザーまたは、IAM ロールを作成していただきます。
当社役職員は、統合認証基盤によるログイン認証、多要素認証によるアクセスのみを可能とした環境へログインを実施し、当社の踏み台 AWS アカウントを経由してお客様がご利用の AWS アカウントへアクセスを実施します。

当社が提供する MSP サービスのセキュリティマネジメント

当社リセールサービスをご利用の AWS を基盤とした MSP サービスでは、AWS セキュリティのベストプラクティス、および AWS Well-Architected Framework セキュリティの柱を参照し、AWS ホワイトペーパーのセキュリティチェックリストを元にした当社独自のチェックシートを作成しチェックを実施しています。
お客様が直接ご契約されている AWS アカウントでの MSP サービスの場合は、当社リセールサービスをご利用の AWS アカウントと比較してギャップがあった場合は、同等のセキュリティに配慮した設計・構築・運用への変更をご提案させていただいております。

AWS インフラストラクチャの保護

Amazon Virtual Private Cloud (VPC)の使用

Amazon VPC は、AWS 内で隔離されたプライベートクラウドを作成できます。
当社では Amazon Elastic Compute Cloud（Amazon EC2）や Amazon Relational Database Service（Amazon RDS）などを VPC 上に構築します。

VPC のネットワーク設計

Amazon VPC の内部では、お客様のサービス要件に合わせてサブネット化し、サブネット間は経路制御（ルーティング）をすることでセグメンテーションを行っています。
セキュリティグループ、およびネットワークアクセスコントロールリスト（NACL）を利用してトラフィックの許可または拒否を制御します。
オンプレミス環境からのアクセスなどセキュリティ要件に応じて、IPsec（VGW の設定）、AWS Direct Connect を採用します。

Amazon Elastic Compute Cloud （Amazon EC2）

Amazon EC2 インスタンスで実行されるアプリケーションから AWS 各リソースへアクセスするユースケースに対応する場合、EC2 インスタンス上に認証情報を保持することはせず、Amazon EC2 に IAM ロールを設定し、ロールの一時的な認証情報を使用するようにします。
メンテナンスのために EC2 インスタンスへの SSH や Windows リモートデスクトップ（RDP）接続は、セキュリティグループを使用して送信元の IP アドレスを制限し、インターネットから直接アクセスできないプライベートセグメントに配置した踏み台サーバーなどを経由したうえで接続をします。

Amazon Relational Database Service（Amazon RDS）

Amazon RDS はインターネットから直接アクセスできないプライベートセグメントへ配置します。

データの保護

保管時のデータの保護

お客様のデータの重要度に基づいてカテゴリー分けを行い、適切なアクセス制限、暗号化などを実施します。

Amazon Simple Storage Service（Amazon S3）

Amazon S3 では標準で外部からのアクセスが禁止されています。さらにバケット ACL、バケットポリシーを利用してバケットレベルまたはオブジェクトレベルのアクセス権限をしようすることによって不正なアクセスからリソースを保護します。
Amazon S3 は、サーバー側での暗号化(SSE)をサポートしています。サーバー側の暗号化はエンドユーザーに対して透過的です。AWS によって、各オブジェクトについて一意の暗号化キーが生成され、AES-256 を使用してオブジェクトが暗号化されます。Amazon S3 上に作成したバケットにはデフォルト暗号化の設定を有効にします。

Amazon EC2 / Amazon Elastic Block Store（Amazon EBS）

Amazon EBS は､業界標準の AES-256 アルゴリズムを使用してデータキーでボリュームを暗号化します。Amazon EC2 インスタンスを作成する際のルートボリュームと、アタッチする EBS データボリューム共に暗号化を有効にします。

Amazon RDS

Amazon RDS の暗号化された DB インスタンスでは、業界標準の AES-256 暗号化アルゴリズムを使用して、Amazon RDS DB インスタンスをホストしているデータをサーバーで暗号化します。お客様側での暗号化の指定がない場合、RDS の暗号化を有効化してデータを保護します。

参考資料

経済産業省

クラウドサービス利用のための情報セキュリティマネジメントガイドライン
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

クラウドセキュリティガイドライン活用ガイドブック
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

ISO（International Organization for Standardization）

ISO/IEC27001
https://www.iso.org/isoiec-27001-information-security.html

AWS 技術情報

責任共有モデル
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWS セキュリティのベストプラクティス
https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Best_Practices.pdf

AWS Well-Architected フレームワーク
https://d1.awsstatic.com/whitepapers/ja_JP/architecture/AWS_Well-Architected_Framework.pdf

NHN テコラス株式会社