cloudpack セキュリティ ホワイトペーパー

Security White Paper

リリース **1.5.6**

アイレット株式会社

第 2 章 はじめに

2.1 cloudpack とは

cloudpack は、アマゾンウェブサービス（AWS）の導入設計、環境構築、運用までをトータルでサポートするマネージドホスティングサービスです。

AWS を知り尽くし、その可能性を最大限に引き出せる cloudpack のスタッフが、 Amazon Elastic Compute Cloud（Amazon EC2）や Amazon Simple Storage Service（Amazon S3）をはじめとする AWS のプロダクトを、構築はもちろんのこと、 24 時間サポートや、サービス監視、バックアップなどの作業代行や技術サポートをスピーディかつ丁寧に行い、ユーザー様のさまざまな運用負荷を可能な限り軽減します。

ユーザー様が、これまで悩みの種だったサーバー周りに関するさまざまな課題から解放され、本来取り組むべきビジネスの課題に専念できるためのサービス、それが cloudpack です。

2.2 クラウド時代のシステム開発とシステム運用

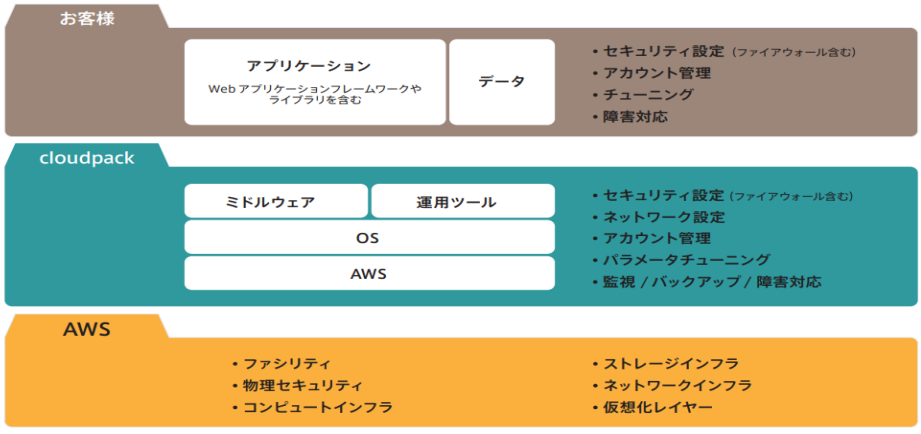
AWS の登場によって、システム開発や運用に対する考え方も大きく変わってきています。

2.2.1 セキュリティにおける「責任共有モデル」

AWS や cloudpack が提示する「責任共有モデル」（Shared Responsibility Model）は、クラウド運用の発展から生まれてきた考え方の一つです。

cloudpack は AWS クラウドインフラストラクチャを基盤にシステムを構築し、ユーザー様は cloudpack が構築したシステム上で業務アプリケーションを運用することになりますので、セキュリティ上の責任はユーザー様と cloudpack と AWS の三者による分担となります。

（責任共有モデル図）



ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティにおけるさまざまなコンポーネントの操作、管理、コントロールは、AWS によって行われ、AWS インフラストラクチャ上に cloudpack が構築したシステムにおけるセキュリティは cloudpack が保護いたします。cloudpack が構築したシステム上で運用される業務アプリケーションおよびデータのセキュリティについてはユーザー様ご自身で保護していただく必要があります。 従来のオンプレミス（構内設置）環境ではすべてについてセキュリティを確保する必要があったことと比較すると、cloudpack ご利用のユーザー様については、ご自分でセキュリティを確保していただく範囲が限定されることを意味いたします。

2.2.2 ベストプラクティスによるシステム開発とシステム運用

AWS と cloudpack はクラウドシステム運用の長い経験から、それぞれに数多くのベストプラクティスを蓄積しています。

cloudpack は AWS が提供するベストプラクティスに従ったシステムを構築し、 cloudpack の持つベストプラクティスに従ってユーザー様の環境を運用しています。従来はインフラストラクチャから業務アプリケーションまですべてにおいてユーザー様ご自身による運用ノウハウの蓄積が必要でしたが、cloudpack ご利用のユーザー様は、ユーザー様が利用される業務アプリケーションの範囲に集中してノウハウの蓄積をしていただければ良いことを意味いたします。

このように、システム構築、運用、セキュリティについて、ユーザー様、cloudpack、AWS がそれぞれに役割と責任を分担することで、より少ない労力で、より早く、求めるものが得られる時代になったといえます。

2.3 本ホワイトペーパーについて

本ホワイトペーパーは、前述の「責任共有モデル」の考え方に基づき、cloudpack が提供するサービス基盤におけるセキュリティの取り組み、およびユーザー様にご利用いただけるセキュリティサービスについてご理解を深めていただくために提供するものです。

対象読者 ：

・AWS、cloudpack 利用中の方

・AWS、cloudpack 導入をご検討中の方

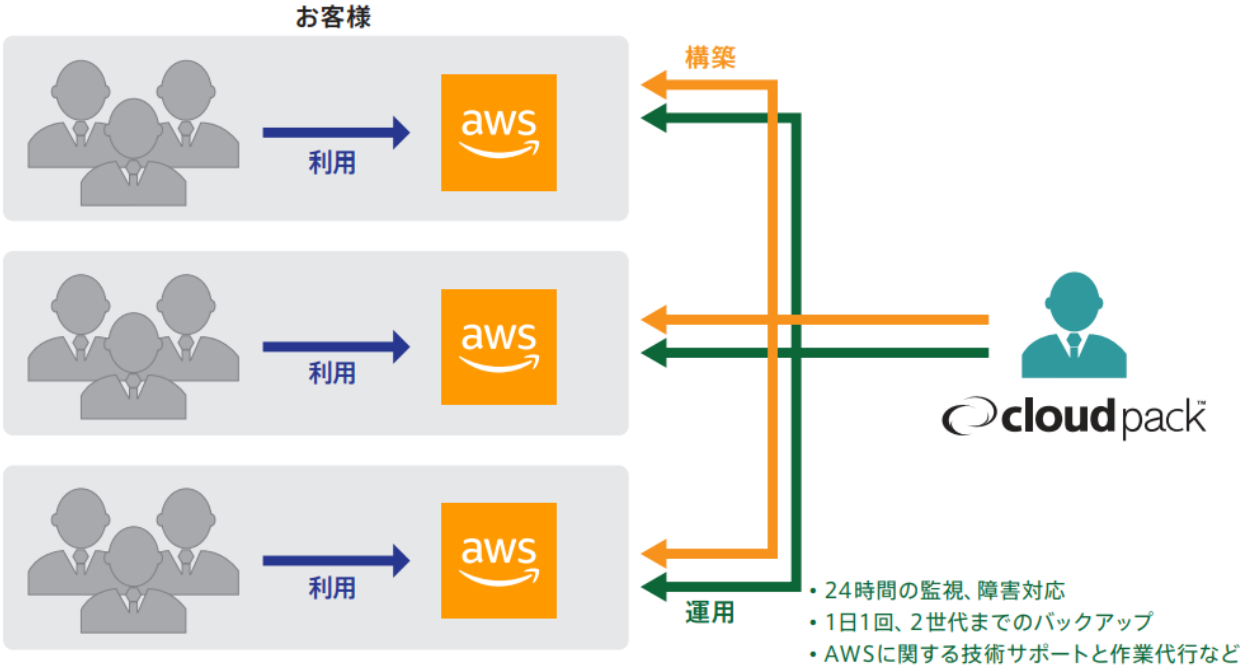
第 3 章　事業概要とセキュリティへの取り組み

3.1　事業概要

cloudpack　は、ユーザー様のシステム運用負荷を可能な限り軽減することを目的に、以下のマネージドホスティングサービスを提供する事業です。

・AWS　インフラストラクチャ上でのサーバー構築から運用（OS　からミドルウェアまで）
・24　時間の監視、障害対応
・1 日　1 回、2　世代までのバックアップ
・AWS　に関する技術サポートと作業代行
・　急激な負荷に対応する「バースト保障」
・AWS　公式サポート（エンタープライズレベル）による強力なバックアップ体制

cloudpack　の　24　時間の技術サポート、サービス　/　リソースモニタリング、バックアップ　/　リストアサービスを利用すれば、AWS　システムを管理する社内サーバーエンジニアを置く必要はありません。



cloudpack　が提供するマネージドホスティングサービスは、高度な AWS　テクノロジーの活用や多数のユーザー様の　AWS　利用に対する多大な貢献について高く評価をいただいております。最初は　2013　年度、その後は連続して　AWS　の世界的なパートナープログラムである AWS パートナーネットワーク（APN）の中でも、特にその販売実績、顧客事例数、顧客満足度の高さなどが優れている「APN プレミアコンサルティングパートナー」として cloudpack　は認定されています。

・AWS　プレミアコンサルティングパートナー　（現：　AWS　プレミアティアサービスパートナー）
　http://aws.amazon.com/jp/partners/premier/

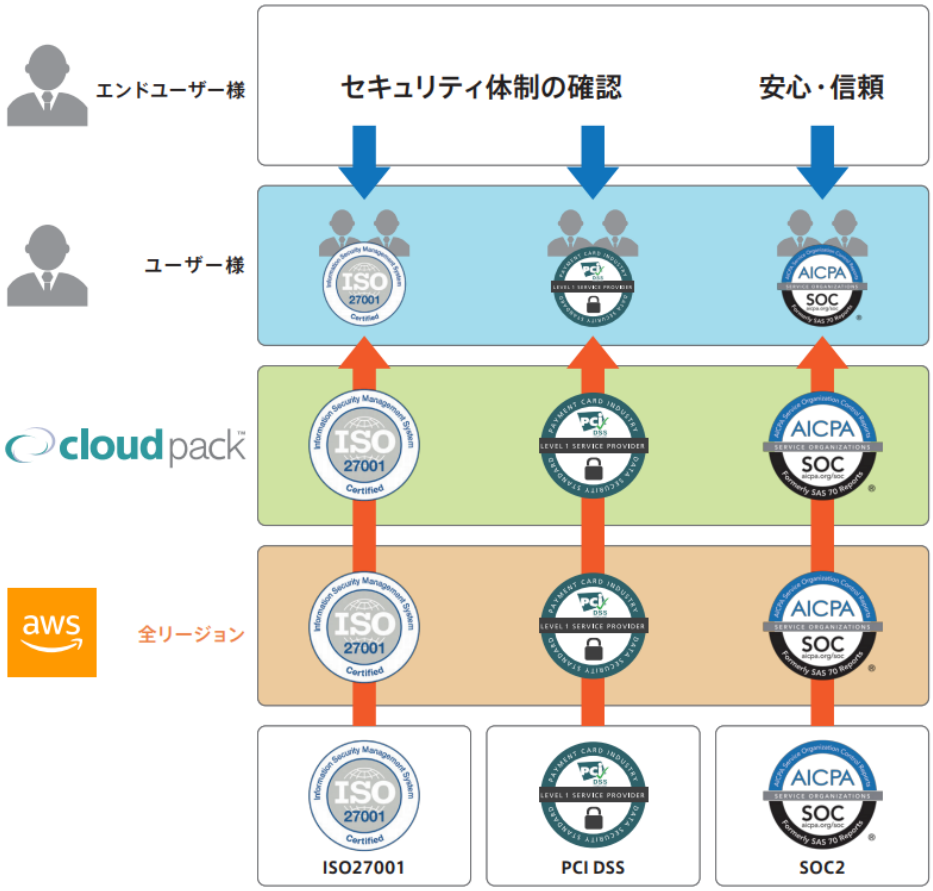
3.2 セキュリティへの取り組み

cloudpack においては、ユーザーの皆様に安心して AWS および cloudpack のサービスをご利用いただくために、第三者機関による認証を含む実効性の高いセキュリティ施策を実施し、情報セキュリティに対して万全の体制で取り組んでいます。

3.3 国際基準への取り組み

AWS が世界 36 箇所（2025 年 5 月時点）に設置するすべてのリージョンにおいて既に取得している国際的なセキュリティ認証については、cloudpack においてもその重要性を強く認識しており、各認証が要求する事項への準拠および各認証の取得に注力しています。

cloudpack をご利用ユーザー様の事業においても、必要に応じて同様の認証を取得いただく事により、cloudpack で稼動するユーザー様の IT システム全般について、セキュリティが高度に確保されていることを対外的に説明することが可能になります。



情報セキュリティマネジメントシステム（ISO/IEC27001）

cloudpack を運営するアイレット株式会社は、2013 年 3 月に情報セキュリティマネジメントシステム（ISMS: Information Security Management System）の国際規格である ISO/IEC27001 の認証を取得しました。

国際規格 ISO/IEC27001/日本工業規格 JISQ27001「情報セキュリティマネジメントシステム－要求事項」を基準として、cloudpack が保有する情報資産を機密性、完全性、可用性の観点から維持改善するために、事業内におけるセキュリティルールを確立し、継続的に運用、監視、見直しを行っています。

ISMS クラウドセキュリティ（ISO/IEC27017）

cloudpack を運営するアイレット株式会社は、2016 年 8 月にクラウドサービス向けの国際規格である ISO/IEC 27017 に基づく ISMS クラウドセキュリティの認証を取得しました。これにより、cloudpack を利用するお客様は、ISMS クラウドセキュリティ認証に準じたセキュリティレベルのサービスを受けることができます。

ISMS クラウドにおける個人識別情報保護（ISO/IEC27018）

cloudpack を運営するアイレット株式会社は、2020 年 3 月にクラウドにおける PII（個人識別情報）保護の国際規格である ISO/IEC 27018 の認証を取得しました。

ISO/IEC27018 認証は、ISMS（ISO/IEC27001）認証を取得していることを前提とし、その適用範囲においてクラウド上に保管する PII の保護に関して、PII プロセッサーとして ISO/IEC 27018：2019 の規格に沿った管理を行っている組織を認証するものです。

ISMS 個人情報保護管理マネジメントシステム（ISO/IEC27701）

cloudpack を運営するアイレット株式会社は、2020 年 3 月に個人情報保護管理マネジメントシステムの国際規格である ISO/IEC 27701 の認証を取得しました。「ISO/IEC27701」認証においては、ISO 認証機関「EY CertifyPoint」(※1)の審査を通じた取得は、アイレットが世界初となります。

ISO/IEC27701 認証は、2019 年 8 月に新しく規格が発行された PIMS（Privacy Information Management System：個人情報保護管理マネジメントシステム）の国際規格に関する認証です。ISMS（ISO/IEC27001）認証を取得していることを前提とし、その適用範囲において PII（Personally Identifiable Information：個人識別情報）コントローラーまたは PII プロセッサー（もしくは、その両者）として、ISO/IEC27701:2019 の規格に沿って個人情報を管理し、継続的に改善するためのシステムを整備、運用する組織を認証するものです。当社は PII コントローラー、PII プロセッサーの両者として認証を取得しました。

(※1)「EY CertifyPoint」は、グローバル市場をリードする先進企業に対しサービスを提供する ISO 認証機関です。
URL：https://www.ey.com/en_gl/services/assurance/certify-point

PCI データセキュリティスタンダード（PCI DSS v4.0） 完全準拠

cloudpack は、2013 年 8 月にクレジット業界におけるグローバルセキュリティ基準である PCI データセキュリティスタンダード（PCI DSS: Payment Card Industry Data Security Standard）レベル 1 v3.0（完全準拠）に認定されました。（2025 年 5 月現在、PCI DSS v4.0（完全準拠）に認定されています。）

PCI DSS は、カード会員様のクレジットカード情報および取引情報を保護するために American Express・Discover・JCB・MasterCard・VISA の国際ペイメントブランド 5 社が共同で策定した基準で、以下の 12 要件を満たすことが要求されています。

安全なネットワークの構築と維持
要件 1：カード会員データを保護するために、ファイアウォールをインストールして構成を維持する。
要件 2：システムパスワードおよび他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない。

カード会員データの保護
要件 3：保存されるカード会員データを保護する。
要件 4：オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する。

脆弱性管理プログラムの維持
要件 5：すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを
定期的に更新する。
要件 6：安全性の高いシステムとアプリケーションを開発し、保守する。

強力なアクセス制御手法の導入
要件 7：カード会員データへのアクセスを、業務上必要な範囲内に制限する。
要件 8：システムコンポーネントへのアクセスを確認・許可する。
要件 9：カード会員データへの物理アクセスを制限する。

ネットワークの定期的な監視およびテスト
要件 10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。
要件 11：セキュリティシステムおよびプロセスを定期的にテストする。

情報セキュリティポリシーの維持
要件 12：すべての担当者の情報セキュリティに対応するポリシーを維持する。

cloudpack においては、PCI DSS に完全準拠した専用セキュリティルームを設置し、カード会員情報を取り扱うシステムを持つユーザー様の高いセキュリティ要求にも対応できる運用体制を確立しています。

SOC2 への取り組み

cloudpack では、米国公認会計士協会(AICPA)が定める内部統制の有効性に関する第三者保証である SOC2(Service Organization Controls 2)の type1 報告書を 2015 年 8 月 31 日に、type2 報告書を 2017 年 3 月 31 日に受領し、以来年次にて type2 報告書を受領し続けています。

SOC2 に準拠することにより、cloudpack におけるセキュリティ、可用性、処理の整合性、機密保持、およびプライバシー保護への取り組みについて、より客観的な評価に基づく透明性の確保、極めて高度なセキュリティ体制の実現をもたらします。(この度の SOC2 の範囲は、セキュリティおよび可用性です)

日本国内における取り組み

cloudpack では、国内における拠点の多重化も進めています。

多拠点化への取り組み

cloudpack では、当社の定める事業継続計画に基づき、業務拠点の多拠点化を推進しています。

2025 年 5 月現在、東京・大阪・名古屋の 3 拠点体制となっています。天災などにより一部の拠点での業務運営が不可能となった場合においても、ユーザー様のシステムを持続的に運用することが可能となります。

AWS ベストプラクティスへの取り組み

cloudpack は、世界でもトップクラスの APN コンサルティングパートナーとして、AWS におけるベストプラクティスの活用を積極的に推進しています。

AWS インフラストラクチャは数多くの規制、標準およびベストプラクティスに準拠するように設計管理されています。

参考 ：http://aws.amazon.com/jp/compliance/

さらに、AWS インフラストラクチャの利用場面におけるセキュリティとコントロールに関するベストプラクティスが蓄積されており、その多くが APN パートナーや AWS ユーザー向けにウェブサイトコンテンツやトレーニングの場を通して共有されています。

cloudpack では、ユーザー様のコンプライアンス要件、セキュリティ要件および運用要件に合致する範囲で、AWS における最新のベストプラクティスに準拠してサーバー環境を構築し、運用業務を実施しています。

ソフトウェア脆弱性情報に関する取り組み（CSIRT）

近年、インターネット基盤ソフトウェアで新たな脆弱性が多く発見されていることから、 cloudpack では、ソフトウェア脆弱性への対応を強化するために、cloudpack 内にコンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team: CSIRT、シーサート）、および脆弱性情報収集を行うセキュリティ運用グループを設置しています。

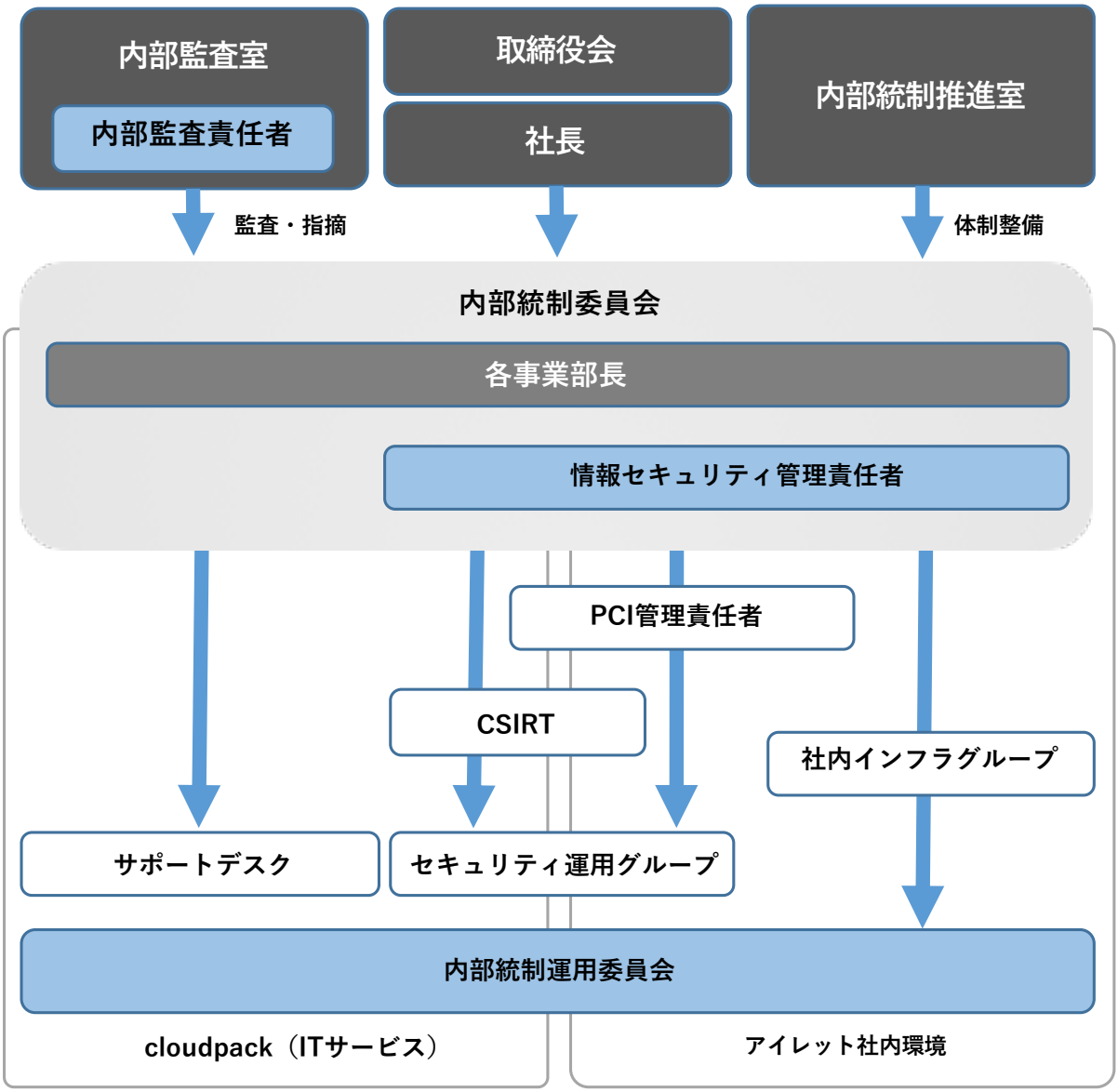
定常的に脆弱性情報の収集を行い、実際にソフトウェア脆弱性が発見された場合には、速やかにその影響の有無および緊急度について判断し、ユーザー様のシステムを防護するために適切な対応を行います。

第 4 章 cloudpack のセキュリティ体制とセキュリティポリシー

4.1 cloudpack における情報セキュリティマネジメント

4.1.1 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システムポリシー（以下「当社 ISMS ポリシー」）に基づき、以下の体制で行っています。



内部統制委員会

当社の IT サービス及び情報セキュリティに関する事案を審議し、組織内への周知活動を行っています。

社長が取締役、各事業部長および情報セキュリティ管理責任者らを招集して月次で開催しています。

情報セキュリティ管理責任者（以下「IS 管理責任者」という。）
当社情報セキュリティ推進に関する責任者です。

PCI 管理責任者
当社 PCIDSS 適用範囲における責任者です。社内システムのネットワーク機器等の設定及びハードニングの管理を行います。

内部統制運用委員会
IT サービス及び情報セキュリティの日常点検や運用上の課題を討議します。
内部統制の運用推進を担当する内部統制運用委員らにより定期開催しています。

コンピュータセキュリティインシデント対応チーム（以下、「CSIRT」という。）
ソフトウェア脆弱性情報に対する大局的な判断や指揮を行い、技術的な調査、情報共有、脆弱性対応を統括します。具体的には、脆弱性の影響の有無・緊急度の判断、対象となるユーザー様への告知全般、脆弱性収束の判断などを行います。

セキュリティ運用グループ
脆弱性情報の定期的な収集を行い、新規の脆弱性情報を検知したときは、CSIRT に対して速やかに情報共有を行います。

社内インフラグループ
運用保守端末および社内システムの各種サーバー等の設定、リリース、更新等の運用および社内システムの監視及びログのレビューを行います。

サポートデスク
サポートデスクは、監視センターとサポートセンターから構成され、24 時間 365 日の有人体制で
cloudpack のサーバー監視及び窓口業務を行います。

4.1.2 情報資産管理

当社は、当社 ISMS ポリシーに基づき、すべての情報資産に対して適切な管理方法を定めるための台帳を作成し、当社の定める機密レベルに応じたアクセス権設定および情報の取り扱い方法を行っています。

また、各情報資産に対するリスクを、推定される損害、脅威、脆弱性の観点から定量的に評価し、必要に応じて適切な管理策を適用することでリスク低減を図ることも定期的に行っています。

ユーザー様情報を含む社内情報の取り扱いについては、当社の定める手順に従って適切な保護および利用を行い、その文書・記録媒体については、保管期間を定め、必要な保護および定期的な検査の実施、保管期間を経過した記録の適切な廃棄を行っています。

当社は、当社プライバシーポリシーに基づき、個人情報保護を行っています。
https://www.iret.co.jp/privacy/

4.1.3 日常業務におけるセキュリティ運用の実践

当社では、全社員に対して当社の個人情報保護方針、情報セキュリティ基本方針、情報セキュリティに関する関連法令および契約事項について、その内容の理解および周知徹底を図っています。

社員が業務上知り得た社外秘以上の秘密情報および個人情報は、期限なくこれを秘密に保持し、関係者外への開示を禁止しています。また、社外に業務を委託する場合は、外部委託先評価を年 1 回以上行い、秘密保持契約ならびに個人情報取り扱いに関する覚書を締結しています。

当社では、日常業務におけるセキュリティ運用を、以下の PDCA(Plan-Do-Check-Action)サイクルに従い行っています。

P(Plan) : 情報の洗い出し、リスク分析、管理策の選定、マニュアルの整備
D(Do) : 社員の教育・研修、管理策の実行、記録および管理
C(Check) : 内部統制委員会の実施、内部監査の実施、マネジメントレビューの実施
A(Action) : 是正・予防処置の実施、リスク対応計画の策定、事業継続計画の策定

特に、cloudpack においては、適切なリスクマネジメントを実現するために、PCI DSS に準拠した事業部内標準のリスクアセスメント手法と評価基準を定めています。

4.1.4 教育

当社では、教育研修規程の定めに従い、中期教育計画を作成し、下記のセキュリティ教育を実施しています。

全社における情報セキュリティ教育
当社では、全従業員を対象に情報セキュリティに関する教育および理解度チェックを年 1 回以上実施し、当社の業務に関わる全スタッフのセキュリティへの理解を継続的に強化しています。

cloudpack におけるセキュリティスキルの向上
cloudpack では、その業務に従事する全スタッフに対して、AWS サービスおよびセキュリティに関連したトレーニングの受講および認定資格の取得を奨励し、セキュリティ知識およびスキルの向上に努めています。

cloudpack スタッフは、配属後速やかに以下のトレーニングの受講および認定資格の取得をすることとしています。

トレーニング

・AWS トレーニング（アマゾン ウェブ サービス ジャパン株式会社）
http://aws.amazon.com/jp/training/

・ 実践的セキュアプログラミングトレーニング（株式会社セキュアスカイテクノロジー）
https://www.securesky-tech.com/wp-content/uploads/2022/01/press-20110419-1.pdf

認定資格

・AWS 認定プログラム（アマゾン ウェブ サービス ジャパン株式会社）
http://aws.amazon.com/jp/certification/

最新セキュリティ情報の共有

cloudpack では、セキュリティに関する最新情報を社内に共有する体制を確立しています。

4.1.5 監査

当社では、当社 ISMS ポリシーに従い、下記の通りセキュリティ監査を実施しています。

ISMS 監査

ISO27001、ISMS 規定文書および当社で定めた手順書類、関連法令または規制条項を監査基準とした定期内部監査を年 1 回実施しています。

臨時監査

内部統制委員会が必要と認めた場合には臨時監査を実施することを社内規定で定めています。

PCI DSS 監査

cloudpack において、PCI DSS 規定に基づく監査を年 1 回実施しています。

4.1.6 クレーム・苦情窓口

cloudpack においては、ユーザー様が cloudpack スタッフに直接伝え難い内容のクレーム（苦情）をお受けする窓口として、「クレーム・苦情窓口」を設置しています。

万が一、cloudpack スタッフの素行、態度、ご回答の遅延、スキルレベル、理解力、ミスの繰り返し、等の問題が発生し、担当者に伝えても改善が見られない、または担当者に直接は言い難い場合、クレーム・苦情窓口にお寄せいただければ、適切に対応いたします。

4.2 cloudpack スタッフによる運用業務の遂行

cloudpack においては、その運用業務に携わるスタッフ（以下「cloudpack スタッフ」）について正社員雇用契約（もしくは正社員雇用契約に相応する個別の契約）を締結し、内部からの攻撃リスクを最小限に抑えています。また、cloudpack スタッフの雇用に際しては、当社 ISMS ポリシーおよび cloudpack において定める PCI DSS 基準（以下、総称して「cloudpack セキュリティポリシー」）に従い、過去の職歴や経歴などを可能な範囲（地域法の制約内）で調査し、cloudpack における職務を理解しその役割に適材な人物により運用業務を遂行しています。

4.3 建物・部屋のセキュリティ

4.3.1 安全な建物・部屋の選定

cloudpack では、事業に関連する情報資産の物理的な保護を図るために、当社の定める手順に基づき、その事業の用に供する建物や部屋について、堅牢性、遮蔽性、防犯性など当社の定めるセキュリティ条件による審査および選定を実施しています。

4.3.2 利用中の建物・部屋のセキュリティレベル

cloudpack では、業務上アクセスする必要のある情報資産の重要度に応じて、現用中の建物や部屋に対して、cloudpack セキュリティポリシーに従い、建物や部屋に下記のセキュリティ区画を設定し、入退室管理および監視を行っています。

セキュリティエリア 1（会議室エリア）
当社の従業員が訪問者の対応を行うエリアです。エリアの入口は、セキュリティキーにより常に施錠しています。IS 管理責任者に認可され、セキュリティキーの交付を受けた当社従業員が入室時に開錠しています。

セキュリティエリア 2（オフィスエリア / 事務室）
当社従業員が通常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。

セキュリティキー（IC カード）により当社従業員の物理的なアクセスを制限しています。業務上の必要により部外者が入室する際は、管理台帳に記録の上、部外者が入室許可書を着用することにより当社従業員と部外者を常に識別できるようにしています。

セキュリティエリア 3（セキュリティルーム / 特別セキュリティ領域）
cloudpack におけるセキュリティ要求がより高い業務を行う高セキュリティエリアです。 IS 管理責任者に入室許可され、尚且つ教育を受けた専任の cloudpack スタッフのみ入室可能としています。

セキュリティキー（IC カード）による入室管理を実施し、入室ログはデータセンター上のサーバーに 1 年間保管しています。

外部訪問者の入室は禁止としています。ルーム内での補修工事など特別な理由により内部統制運用委員が許可した場合は、訪問者には常に cloudpack スタッフが同行し、作業内容の記録および内部統制運用委員への報告を行います。

4.3.3 建物・部屋の防犯および入退室管理

cloudpack においては、事業に関連して保有する情報資産を保護するために、特にセキュリティ保護が必要な領域において、防犯カメラまたは入室ログ収集システムを導入し、その領域へのアクセスについて監視およびログ収集を行っています。防犯カメラの録画映像および入室ログについては、cloudpack セキュリティポリシーにより 1 年間保管しています。

退職・休職により cloudpack スタッフの異動があった場合は、速やかに交付されたセキュリティカードや専用 IC カードを回収し、万が一紛失があった場合には当該セキュリティキーおよび専用 IC カードを無効化することにより、部外者の物理的な侵入を防止できる体制を実現しています。

4.3.4 建物・部屋の物理的なネットワークの保護

cloudpack においては、社内ネットワーク上の情報資産を保護するために、当社で管理する建物・部屋に敷設された物理的なネットワークに対して、下記の保護策を行っています。

・ 最低限必要な権限者のみがネットワークに接続できるように、物理的な保護を行っています。

・ サーバーラックは常時施錠し、鍵は社内インフラグループが厳重に管理しています。

・通信回線への物理アクセスを可能とする機器（ワイヤレスアクセスポイント、ゲートウェイ、ハンドヘルドデバイス、ネットワーク/通信ハードウェア）については、事前に IS 管理責任者が認めたものを除き、セキュリティエリア 2 および 3 への持ち込みを禁止しています。

・外部からの訪問者に関しては、特別に IS 管理責任者の明示的な承認がある場合を除いて、セキュリティエリア 2 および 3 における物理ネットワークへの接続を禁止および遮断しています。

また、物理ネットワークの保護策について実効性を確保するため、当社で管理する物理ネットワークの変更作業についても、cloudpack セキュリティポリシーにより下記のように変更ルールを定めています。

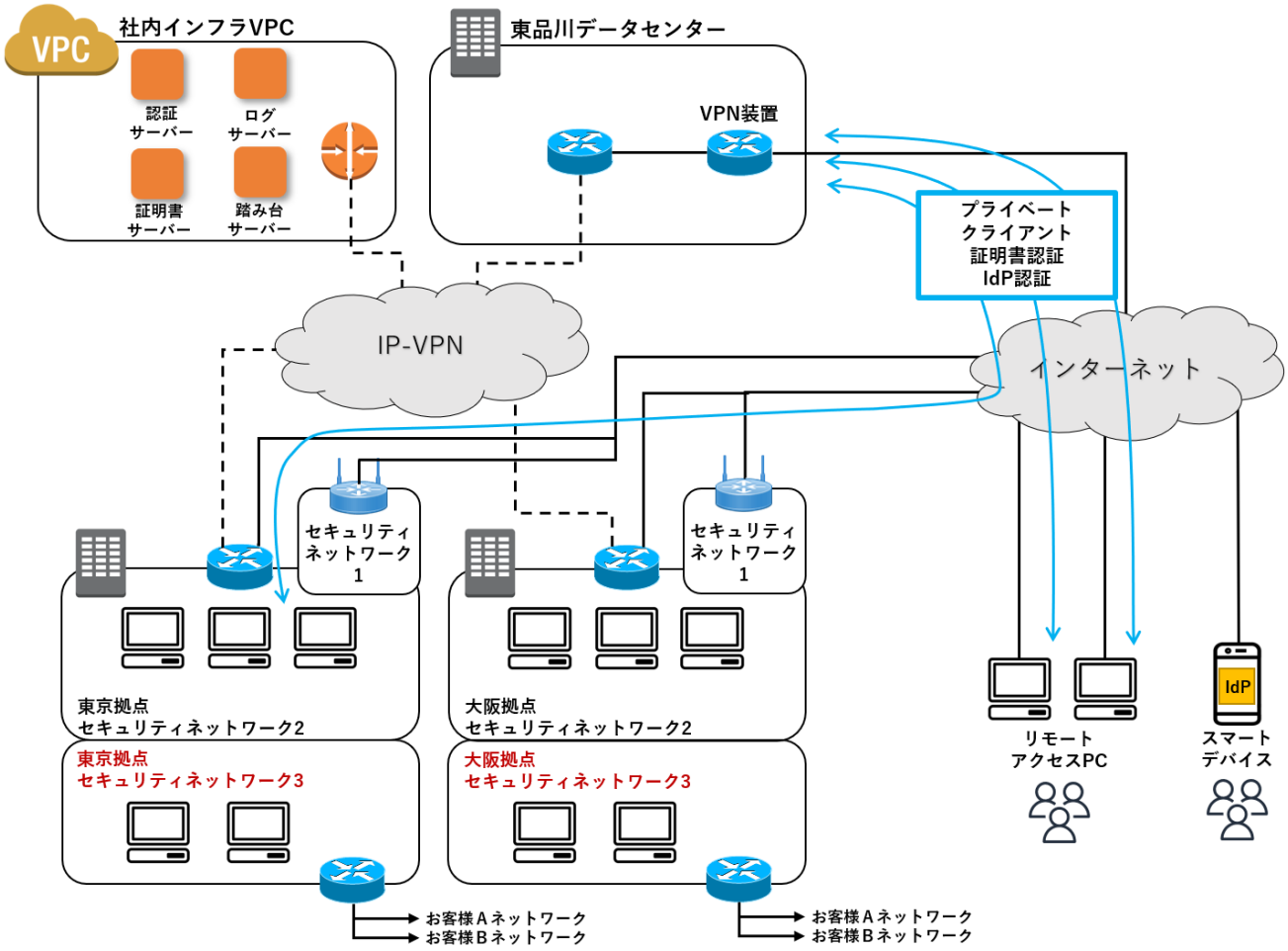
・サーバーやネットワークの変更などネットワーク機器に関して設定変更の必要がある場合は、承認フローに従い、IS 管理責任者に承認を得た上で実施し、作業終了後、作業内容および変更した設定の内容について、IS 管理責任者に報告し記録しています。

・機器の保守などで業務上、やむを得ずネットワーク機器を持ち込む場合には事前に IS 管理責任者の承認を必要としています。

4.4 業務ネットワークのセキュリティ

cloudpack においては、事業に関連する情報資産を保護するため、当社の他事業と独立した社内ネットワークを構築しています。さらに、各種閉域ネットワークサービスを活用し、認証情報を外部から隔離された場所で一元管理することにより、極めてセキュリティ強度の高い業務ネットワークおよび認証システムを導入し、運用業務の基盤として利用しています。

（ネットワーク構成図）



4.4.1 ネットワークのセキュリティレベル

cloudpack において利用する業務ネットワークについては、セキュリティレベルに応じて 3 つのネットワークに分割することにより、利用者の区分に従った適切なアクセス制御を行っています。

セキュリティネットワーク 1（cloudpack ゲストネットワーク）

訪問者など部外者向けのネットワークです。

無線（暗号化通信）による接続のみ提供しています。cloudpack の他のネットワークと接続されておらず、cloudpack の持つ情報資産へのアクセス経路はありません。

セキュリティネットワーク 2（cloudpack オフィスネットワーク）
cloudpack において通常の運用業務に利用するネットワークです。
予め許可された業務端末のみが接続可能です。
インターネットのみに接続可能です。cloudpack の持つ情報資産へアクセス際は認証が必要となります。
無線（暗号化通信）および有線による接続を行っています。

セキュリティネットワーク 3（cloudpack セキュアネットワーク）
cloudpack において特別にセキュリティ強度が求められる運用業務に利用するネットワークです。

許可された運用業務端末についてのみ、有線による接続を行っています。このネットワークには無線で接続することはできません。

cloudpack スタッフは、高度なセキュリティシステムに防御された cloudpack セキュアネットワークおよび cloudpack オフィスネットワーク（以下「cloudpack 業務ネットワーク」）上で cloudpack の運用業務を遂行します。

4.4.2 複数の認証システム

cloudpack 業務ネットワークでは、以下の 3 つの認証システムを併用することで、外部からの侵入が極めて困難なネットワーク環境を実現しています。

ハードウェア認証
接続する端末が cloudpack に属するパソコン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 cloudpack スタッフであることを認証します。

多要素認証
ログインするユーザーしか持ち得ない情報、もしくは知り得ない一時的な情報を利用した認証を行います。

さらに、認証経路の暗号化、パスワードの複数回失敗に対するアカウントロックアウト、一定期間非アクティブであったアカウントの無効化など、認証情報の保護に有用な措置を実施しています。

4.4.3 パスワードポリシー、多要素認証

cloudpack においては、cloudpack スタッフアカウントの本人以外による不正利用を防止するために、cloudpack セキュリティポリシーに従い、認証システム上でのパスワード管理について PCI DSS や ISMS などの国際認証の基準の要求よりも大幅に強度の高いポリシーで運用しています。また、多要素認証や生体認証などを利用して多重に本人確認を行うことで、万が一 cloudpack スタッフのパスワード情報が漏えいした場合であっても、cloudpack 業務ネットワークへの侵入を防御するための高度なセキュリティ運用を行っています。

4.4.4 認証情報の一元管理

cloudpack 業務ネットワークでは、cloudpack スタッフの認証情報を統合認証システムで一元管理しており、cloudpack 業務ネットワークへの接続に統合認証システムによる 認証を必要としています。これにより、退職・休職によるスタッフの異動があった場合や、万が一認証情報が漏えいした場合にも速やかに当該アカウントを無効化することにより、 cloudpack 業務ネットワーク上の情報資産へのアクセスを完全に遮断できる体制を実現しています。

4.4.5 業務ネットワークの監視

cloudpack 業務ネットワークでは、cloudpack セキュリティポリシーに従い、ネットワークリソースへのアクセスを追跡および監視し、その記録を事後に変更できないように保護した上でアクセスログとして保存しています。さらに、不正侵入検知システム（IDS）、不正侵入予防システム（IPS）およびファイル整合性監視システムによる常時監視を行っています。万が一 cloudpack のセキュリティに対して影響のある事象が発生した場合には、24 時間即応可能な cloudpack スタッフが、当社の定めるインシデント対応手順書に従い、迅速かつ効果的に対応する体制を確立しています。

4.4.6 運用業務端末のセキュリティ

cloudpack 業務ネットワークへの接続は、当社で管理する建物・部屋に設置されている運用専用端末および高度なセキュリティ防御を施したリモート運用端末のみ可能としています。これら運用業務を行う端末（以下、「運用業務端末」）については、事前に承認を受けた cloudpack スタッフ以外の利用は禁止しています。

運用業務端末については、以下のセキュリティポリシーを適用し、その操作について常に監視および操作ログの保存を行っています。

・ ウィルス対策ソフト、プログラムについては常に最新を維持する。

・ ベンダーが提供する OS や業務用ソフトウェアの修正プログラムは、自動更新に設定する。

・事前に認められたプログラム以外はインストールしない。

・USB メモリーなどの外部デバイス利用を禁止する。

・インターネットへの接続については、業務上必要な場合のみ利用することとし、適切な URL フィルタリングの導入により意図しない不正サイトへの接続をブロックする。

・クライアント操作ログを取得する。

リモート運用端末については、セキュリティについて技能および経験に裏打ちされたスキルを持つと認定された cloudpack スタッフのうち、特に必要があると認められた者だけが所持できるものとし、通常の運用業務端末のセキュリティポリシーに加えて下記の特別なポリシーを適用しています。

・接続時に証明書による端末認証を行い、接続を要求してきたデバイスを特定し許可されたリモート運用端末のみ接続を認める。

・リモートアクセスの利用に関して、利用者、利用日時、作業内容、アクセス時間など詳細なログを取得し保存する。

・社外のユーザーによるリモートアクセスは全面的に許可しない。

・万が一リモート運用端末を紛失した時にも情報が漏えいすることを防止するためハードディスクや SSD などの記憶装置に暗号化を施す。
・第三者による覗き見を防止するためリモート運用端末にスクリーンシート等の防護器具を装着する。

4.4.7 業務ネットワークの定期的な検査

cloudpack 業務ネットワークにおいては、cloudpack セキュリティポリシーに従い、定期的に以下のネットワーク検査およびテストを実施することで、セキュリティの強度を適切なレベルに維持しています。

・不正なネットワーク機器の検出
・ネットワークの脆弱性検査
・インフラストラクチャの内部および外部ペネトレーションテスト

4.5 cloudpack から AWS へのアクセスに関するセキュリティ

cloudpack においては、ユーザー様のサービス基盤としてのセキュリティを確保するため、 cloudpack スタッフがユーザー様のサーバー環境および AWS インフラストラクチャにアクセスする経路について、厳しく制限をしています。

4.5.1 サーバー環境へのアクセス経路の限定

cloudpack では、cloudpack スタッフがユーザー様のサーバー環境（Amazon EC2 インスタンス）にアクセスする経路について、以下の制限を行っています。

・cloudpack では、AWS ネットワーク上に cloudpack スタッフ専用の踏み台サーバー（以下「cloudpack 踏み台インスタンス」）を設置しています。cloudpack スタッフがユーザー様のサーバー環境において実施する OS 操作などの運用作業については、この cloudpack 踏み台インスタンスからのみ実施が可能となっています。この制限により、外部の第三者がユーザー様のサーバー環境を不正に変更することを防止します。

・cloudpack 踏み台インスタンスに対しては、cloudpack 業務ネットワークから暗号化された安全なプロトコルによる直接アクセスのみが可能となっています。この制限により、外部の第三者が cloudpack 踏み台インスタンスにアクセスすることを防止するとともに、 cloudpack 業務ネットワーク内の各種監視システムによる一元的な防護が可能になります。

・cloudpack スタッフが、cloudpack 踏み台インスタンスにログインするためには、 cloudpack 業務ネットワーク上の統合認証システムによる認証を受ける必要があります。この制限により、退職もしくは異動した cloudpack スタッフがユーザー様のサーバー環境にアクセスできないことを保証することが可能になります。

・cloudpack 踏み台インスタンスでは、すべての操作がテキスト形式、もしくは動画として記録されます。これらの制限により、万が一現任の cloudpack スタッフの認証情報が漏えいした場合にもユーザー様のサーバー環境に直接危険を及ぼすことはありません。

4.5.2 AWS インフラストラクチャへのアクセス経路の限定

cloudpack では、cloudpack スタッフがユーザー様の AWS インフラストラクチャにアクセスする経路について、以下の制限を行っています。

1. ユーザー様の AWS インフラストラクチャを操作するための「AWS マネジメントコンソール」（Web インターフェイス）、「API（アプリケーション・プログラマブル・インターフェイス）」、「AWS アカウント」、「IAM（AWS Identity and Access Management）」、「アクセスキー・シークレットキー」に対し、cloudpack 業務ネットワークからのアクセスのみ、かつ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

した社内専用ツールを用いて厳しくアクセスを制限し、管理しています。この制限により、cloudpack スタッフ以外がユーザー様の AWS インフラストラクチャにアクセスすることを防止するとともに、cloudpack 業務ネットワーク内の各種監視システムによる一元的な防護が可能になります。

2. cloudpack スタッフがユーザー様専用 AWS インフラストラクチャを操作する場合は、 AWS が提供する権限管理機能の一つである「IAM ロール」と cloudpack 業務ネットワーク上の統合認証システムの連携による個別認証を行っています。個別認証により、退職もしくは異動した cloudpack スタッフがユーザー様専用 AWS インフラストラクチャにアクセスできないことを保証することが可能となります。

これらの制限により、万が一現任の cloudpack スタッフの認証情報が漏えいした場合にもユーザー様専用 AWS インフラストラクチャに直接危険を及ぼすことはありません。

4.5.3 ユーザー様環境における各種作業の監視

cloudpack では、ユーザー様のサーバー環境および AWS インフラストラクチャにおける各種作業の監査証跡を確保するために、原則下記の通り監視および操作ログの保存を行っています。

1. AWS CloudWatch および当社監視基盤による監視

2. cloudpack 踏み台インスタンスにおける作業ログの保存
   syslog およびイベントログにより取得可能なログ（保存期間 1 年間）

3. ユーザー様専用 AWS インフラストラクチャに対する作業ログの保存
   （Amazon EC2/Amazon VPC、Amazon RDS など） AWS CloudTrail により取得可能なログ（保存期間 1 年間）

4. 上記以外（ユーザー様のサーバー環境における各種通信ログや操作ログ等）につきましては、ログの取得設定を含めて、ユーザー様にて管理いただきます。

4.6 cloudpack が利用する社外リソースのセキュリティ

cloudpack においては、AWS 環境の構築および運用の進捗管理、課題管理およびユーザー様と各種情報を共有するために、ヌーラボ社が提供する Web サービス「Backlog」を利用しています。 cloudpack では、当社 ISMS ポリシーに従いヌーラボ社に対して外部委託先評価を定期的に行い、秘密保持契約ならびに個人情報取り扱いに関する覚書を締結しています。

4.6.1 Backlog

Backlog はブラウザ上で課題管理や進捗管理ができる Web ベースの総合的なプロジェクト管理ツールです。

cloudpack では、ご契約後の課題管理に Backlog を利用し、ユーザー様と cloudpack スタッフの間で課題および情報の相互共有を行っています。これにより、障害発生時など緊急時にユーザー様と情報共有することを可能としています。

Backlog を利用する 3 つのメリット

POINT1 相互共有することで、電話やメールのやりとりでの抜け漏れや見落としを防止します。

POINT2 課題が増えてもカテゴリ分けや検索が容易です。

POINT3 担当者不在の場合でも課題のステータスをすぐに把握可能です。

Backlog のセキュリティ

cloudpack は、ヌーラボ社と共同で Amazon EC2 上に Backlog を構築・運用する「専用 Backlog プラン」を提供しています。

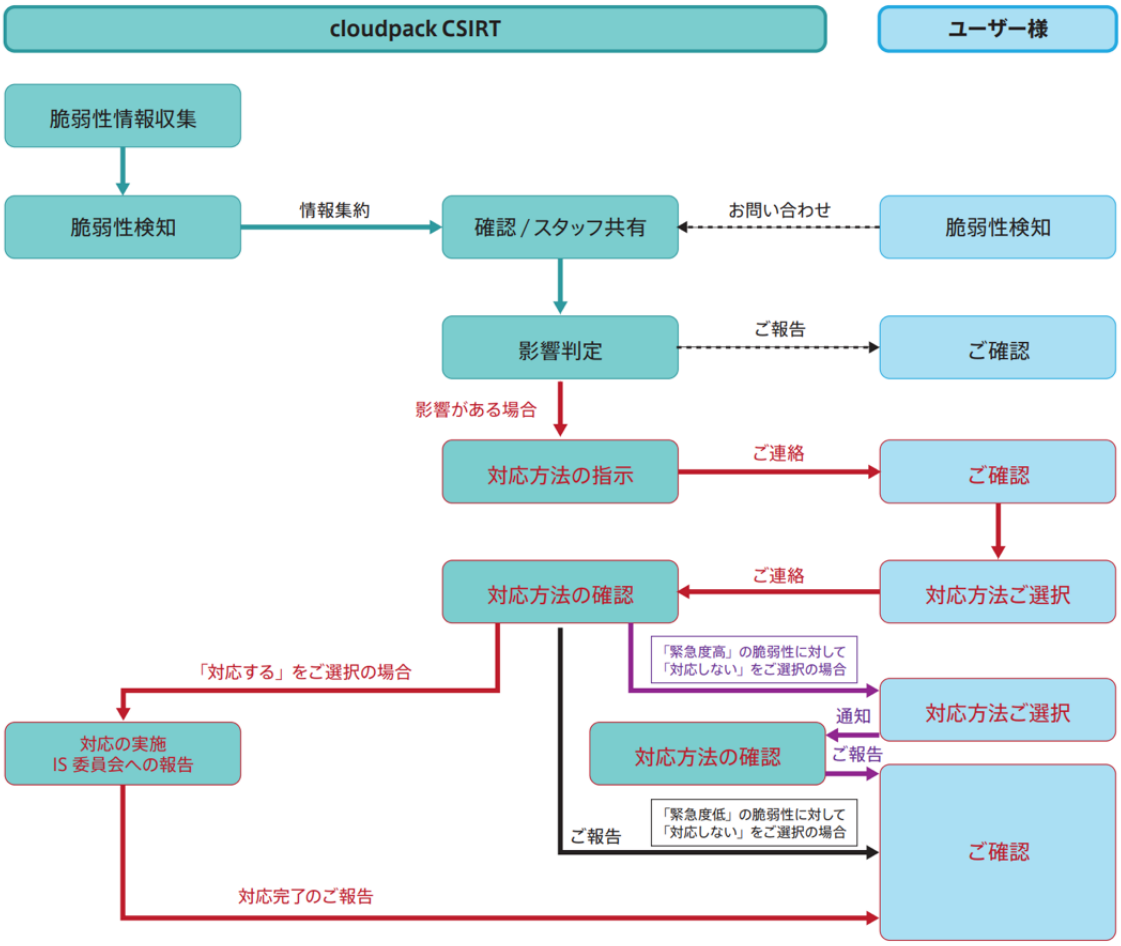
https://cloudpack.jp/service/backlog.html

このプランでは、Amazon VPC などの活用によりセキュアに Backlog を利用することが可能な上、その運用を cloudpack スタッフが担当しています。

ユーザー様と cloudpack スタッフの情報共有に利用する Backlog についても、この「専用 Backlog プラン」運営において蓄積したベストプラクティスを基に、独自のセキュリティ保護策を導入しています。

4.7 脆弱性情報に対する対応

cloudpack においては、cloudpack 責任共有モデルに基づいて、AWS インフラストラクチャ上に cloudpack が構築したシステムで利用しているソフトウェアに関する脆弱性情報を常に収集しています。もしこれらソフトウェアに関する脆弱性情報を検知したときには、速やかにその影響調査を行い、ユーザー様に対してご連絡し、ご回答を基に迅速に対応する体制を確立しています。



4.7.1 脆弱性情報の検知から影響調査

JPCERT コーディネーションセンター（JPCERT/CC）による脆弱性情報の公開、 cloudpack スタッフによる脆弱性情報の検知もしくはユーザー様からの脆弱性情報のお問合せがあった場合は、速やかに Backlog 上で情報共有を開始し、CSIRT による影響調査およびその緊急度の判定を行います。

4.7.2 対応

脆弱性対応が必要と判定した場合は、影響するユーザー様に対して Backlog もしくはメールにてご連絡し、そのご回答内容に従って脆弱性対応を行います。もし、緊急度高の脆弱性に対して対応しない旨のご判断をいただいた場合には、そのご判断をいただいた旨の証跡（エビデンス）として Backlog 上での承認作業をお願いしています。対応の進捗や過程および承認証跡については Backlog 上にて随時ご確認いただけます。

4.8 順守状況および是正対策の報告

cloudpack では、本ホワイトペーパー等の内容が順守されているかどうかの確認を年次にて行います。確認にて、順守されていない事項を検出した場合は、その解決策を検討し、是正対策を実施いたします。

これら順守状況および是正対策の内容につきましては、毎年 1 回の本ホワイトペーパーの更新にて、報告いたします。

4.9 セキュリティインシデントの報告

cloudpack が情報セキュリティインシデントを検出した場合においては、そのインシデントがユーザー様に影響するものと判断した段階にて速やかに、影響するユーザー様に対して Backlog もしくはメールにてご連絡し、そのご回答内容に従って対応を行います。

第 5 章　cloudpack が提供するマネージドプランにおけるセキュリティマネジメント

5.1 cloudpack が提供する主な AWS サービスとセキュリティ

5.1.1 AWS のプライベートクラウド環境（Amazon VPC）を活用したサービス

Amazon Virtual Private Cloud（Amazon VPC）

Amazon VPC は、AWS 内でユーザー様独自に隔離されたプライベートクラウドを構築する仕組みです。

cloudpack では、ユーザー様の利用する Amazon Elastic Compute Cloud（Amazon EC2）インスタンス、Amazon Relational Database Service（Amazon RDS）インスタンス、Amazon ElastiCache キャッシュノードを Amazon VPC 上で構築しているため、プライベートネット環境での共有リソースに対する不安が解消されます。

また、cloudpack では、Amazon VPC の内部をユーザー様のサービス要件に従ってセグメント化し、各セグメント間のアクセス経路（ルーティング）を制限しています。この経路制限に加えてセキュリティグループ、ネットワークアクセスコントロールリスト（ネットワーク ACL）など Amazon VPC に備えられたセキュリティ機能を活用することで、Amazon VPC の内部ネットワークのセキュリティを保護しています。

Amazon Elastic Compute Cloud（Amazon EC2）

Amazon EC2 は、規模の変更が可能なコンピュータ処理能力をクラウド内で提供する AWS のサービスです。

cloudpack「サーバープラン」では、Amazon EC2 上にサーバーを構築してユーザー様の専用サーバーとしてご提供しています。

サーバープラン ：https://cloudpack.jp/service/plan/server.html

ユーザー様社内におけるセキュリティポリシーなどによりハードウェアの専有が求められる場合にも、Amazon EC2 の Dedicated インスタンスを利用することで Amazon EC2 インスタンスが稼動するハードウェアを専有することが可能ですので、速やかにポリシーに準拠することが可能です。

Amazon Relational Database Service（Amazon RDS）

Amazon RDS は、MySQL、PostgreSQL、Oracle などのリレーショナルデータベースのセットアップ、運用、およびスケーリングを容易に行えるようにする AWS のサービスです。 cloudpack「データベースプラン」では、Amazon RDS 上にデータベースサーバーを構築し、ユーザー様の専用データベースとしてご提供しています。

データベースプラン ：https://cloudpack.jp/service/plan/database.html

Amazon RDS は、データベースソフトウェアに自動的にパッチを当て、データベースをバックアップし、ユーザーが定義した保持期間バックアップを格納して、特定時点へのデータベースの復旧を可能にします。

Amazon ElastiCache

Amazon ElastiCache は、メモリー内キャッシュのデプロイ、運用、スケーリングをクラウド内で簡単に実行できる AWS のサービスです。

cloudpack「キャッシュプラン」では、Amazon ElastiCache 上に Memcached（メモリーオブジェクトキャッシュシステム）や Redis（メモリーキーバリューストアシステム）などのキャッシュシステムを構築し、ユーザー様専用のキャッシュサーバーとしてご提供しています。

キャッシュプラン ：https://cloudpack.jp/service/plan/cache.html

Amazon ElasticCache は、データアクセスを高速化し、ユーザー様のウェブアプリケーションなどのパフォーマンスを向上させます。サーバープラン（Amazon EC2）やデータベースプラン（Amazon RDS）と組み合わせて利用することで、アクセス負荷の高いサイトを構築し、安定かつ高速にコンテンツ配信することが可能となります。

5.1.2 静的コンテンツのホスティングサービス

Amazon Simple Storage Service（Amazon S3）

Amazon S3 は、AWS が提供する容量無制限の高信頼性インターネット用ストレージサービスです。

cloudpack「S3 ホスティングプラン」では、サーバー（Amazon EC2）を使わずに HTML / CSS / JS / 画像 / 動画 / Flash などの静的なコンテンツのみをホスティングするサービスを提供しています。

S3 ホスティングプラン ：https://cloudpack.jp/service/plan/s3-hosting.html

Amazon S3 は 99.999999999% の耐久性と、99.99% の可用性を提供するよう設計されています。「S3 ホスティングプラン」では、この Amazon S3 を利用することで非常に障害に強く、急なアクセス増にも対応可能な Web ホスティング環境をご提供しています。

参考 URL : http://aws.amazon.com/jp/s3/

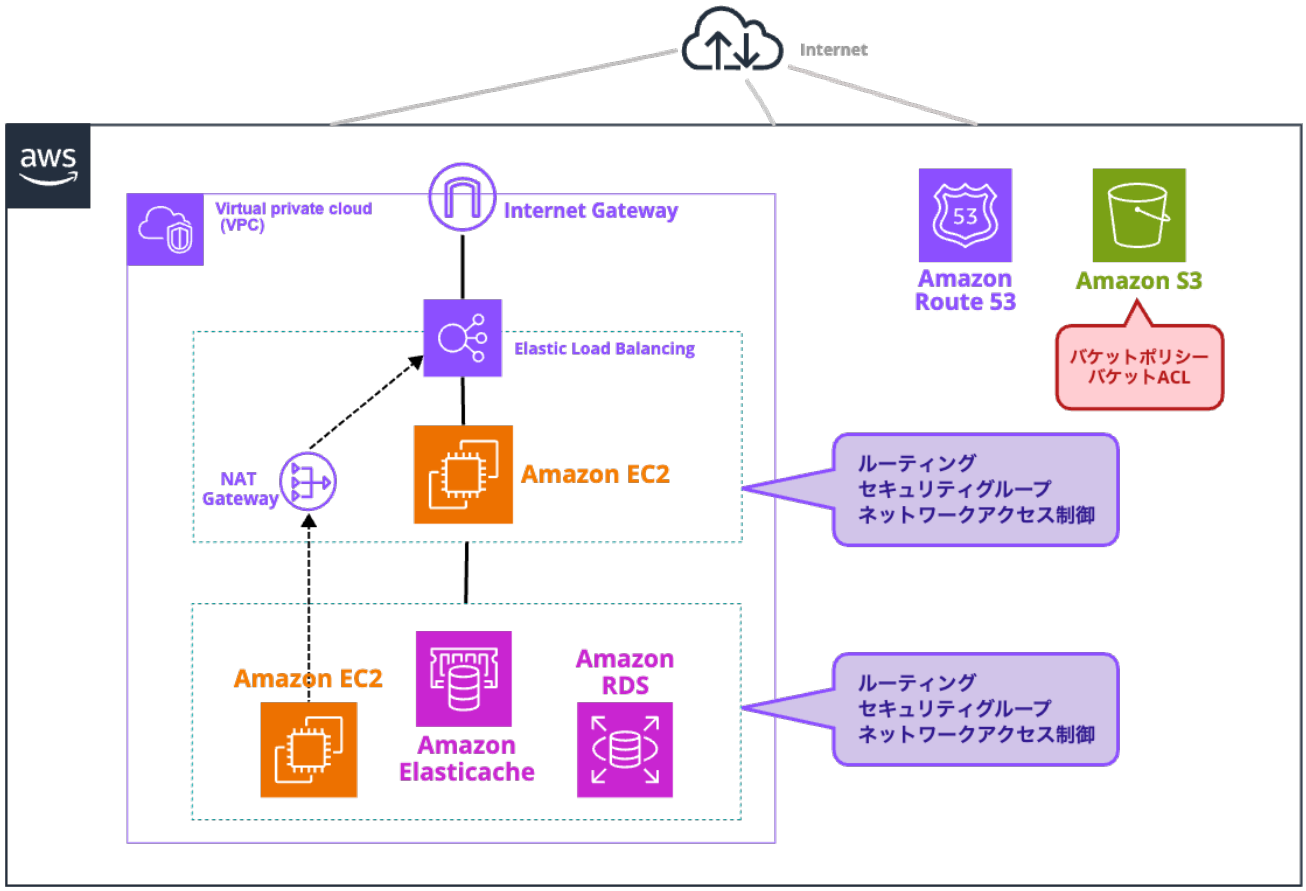
Amazon S3 へのアクセス制御には、Amazon S3 の「バケット ACL」および「バケットポリシー」の機能を利用します。「バケット ACL」および「バケットポリシー」では、標準で外部からのアクセスを禁止しており、必要のあるコンテンツや通信先のみ許可することになります。例えば公開用コンテンツについてはインターネット全体に公開し、社内向けコンテンツについてはユーザー様ご使用の固定 IP アドレスからのアクセスのみ許可する設定をします。

5.1.3 DNS マネージドサービス

Amazon Route 53 は、AWS が提供する可用性（SLA100%）と拡張性に優れたドメインネームシステム（DNS）サービスです。

cloudpack では、ユーザー様のご要件に応じて Amazon Route 53 による DNS サービスを構築し、ユーザー様のドメインを安定的に運用する環境をご提供します。

5.1.4 cloudpack が提供する主な AWS サービスとセキュリティ（図）



5.2 cloudpack マネージドプランにおけるセキュリティ運用

5.2.1 セキュリティ設定の変更

cloudpack では、ユーザー様のサービス要件に最適なアクセス制御などのセキュリティ設定を行っておりますが、もし変更が必要となった場合は、Backlog 経由でご連絡いただければ速やかに対応いたします。お急ぎの場合は、メールや電話にてご依頼いただくことも可能です。

5.2.2 脆弱性情報への対応

cloudpack では、前述の通り、cloudpack 内にコンピュータセキュリティインシデント対応チーム（CSIRT）および脆弱性情報収集チーム（cloudpack セキュリティ運用グループ）を設置し、脆弱性情報に対する対応フローを定めています。ユーザー様のサービス環境に影響のある脆弱性情報を検知したときには、速やかにご連絡をし、対応についてユーザー様の判断いただき、適切な対応を行っています。大切なユーザー様のサービス環境を適切に保護するためにも、迅速なご回答をいただけますようお願いいたします。

5.3 cloudpack マネージドプランにおける AWS アカウントの管理

5.3.1 AWS アカウントの作成

cloudpack ご契約後、ユーザー様専用の AWS インフラストラクチャおよびサーバー環境を構築運用するために、cloudpack にてユーザー様専用 AWS アカウントを新規に作成し、運用管理します。

5.3.2 AWS Root アカウントの管理

ユーザー様専用 AWS Root アカウントについては、AWS インフラストラクチャに関連する契約内容の変更など特段の事情がある場合を除き、通常時は使用いたしません。

その保護のために、初期構築作業完了後、多要素認証（MFA）を設定します。MFA デバイスは、セキュリティエリア 2 において厳重に保管します。

5.3.3 AWS アカウントの廃止

cloudpack ご解約の場合は、解約日から起算して次項に定める期日経過後に、AWS に対してユーザー様専用 AWS アカウントの廃止手続きを行います。
cloudpack では原則として AWS アカウントの移転を認めておらず、廃止手続き開始後は解約をキャンセルすることができませんのでご注意ください。

5.4 解約時のユーザー様データの取り扱い

cloudpack では、ユーザー様環境のデータについてサービスご解約日から 1 週間以内に AWS アカウント内の全リソースを削除いたします。その後、60 日以内に専用 AWS アカウントを廃止することで完全に破棄いたします。

ご解約により、その AWS アカウントに紐付いたインスタンス、ストレージ、データベース、ログ、バックアップおよびユーザー様が保存したデータなどのリソースが破棄されます。 cloudpack では、ユーザー様環境のデータを AWS 環境外に持ち出すことを禁止し、厳重に監視しているため、ご解約と共にユーザー様環境におけるデータは cloudpack の管理範囲からは安全に消去されることになります。

5.5 ユーザー様環境におけるセキュリティを確保するために

cloudpack では、ユーザー様側でアプリケーション管理業務を行うための経路について、原則としてユーザー様拠点からのアクセスのみに限定しています。また、アクセス方法についても、セキュリティ強度の高い方法を中心にご提案しています。

本ホワイトペーパーに記載の無いさらに高度なセキュリティ設定については、ユーザー様のご要件に合わせて AWS サービスの運用に精通したスタッフが丁寧に設計いたしますので、お気軽に cloudpack スタッフにご相談ください。

5.6 AWS のリージョンについて

cloudpack は、AWS が世界 36 箇所（2025 年 5 月時点）に設置するすべてのリージョンを利用することができます。
AWS のリージョンは、契約時にユーザー様側にて選択することができます。標準では日本リージョンが選択されます。（cloudpack は、原則としてサービス利用規約および日本国内法に順守しています。）
ユーザー様環境のデータが物理的に存在するリージョンでの地域的なコンプライアンス要件およびデータレジデンシー要件については、ユーザー様側にて対応いただきます。

第 6 章　参考

6.1 各種ガイドライン

6.1.1 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

6.1.2 総務省

クラウドサービス提供における情報セキュリティ対策ガイドライン

https://www.soumu.go.jp/main_content/000771515.pdf

6.1.3 PCI Security Standards Council

PCI DSS（v4.0）基準

https://listings.pcisecuritystandards.org/documents/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1-JA.pdf

6.1.4 ISO（International Organization for Standardization）

ISO/IEC27001

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

6.2 AWS 技術情報

AWS セキュリティー手順および技術については、下記 URL をご確認ください

https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Best_Practices.pdf

保管時及び転送時のデータ暗号化については、下記 URL をご確認ください

https://docs.aws.amazon.com/whitepapers/latest/logical-separation/encrypting-data-at-rest-and--in-transit.html

グローバルインフラストラクチャについては、下記 URL をご確認ください

https://aws.amazon.com/jp/about-aws/global-infrastructure/

第 7 章　セキュリティおよび可用性対策の順守状況

2024 年実施の内部監査にてセキュリティおよび可用性対策の順守状況を監査し、順守状況は良好であることを確認しました。（監査対象期間：2024 年 1 月 1 日～2024 年 12 月 31 日）

監査項目	順守状況
4.1　cloudpack における情報セキュリティマネジメント	○
4.1.1 情報セキュリティマネジメントシステム（ISMS）	○
4.1.2 情報資産管理	○
4.1.3 日常業務におけるセキュリティ運用の実践	○
4.1.4 教育	○
4.1.5 監査	○
4.1.6 クレーム・苦情窓口	○
4.2　cloudpack スタッフによる運用業務の遂行	○
4.3　建物・部屋のセキュリティ	○
4.3.1 安全な建物・部屋の選定	○
4.3.2 利用中の建物・部屋のセキュリティレベル	○
4.3.3 建物・部屋の防犯および入退室管理	○
4.3.4 建物・部屋の物理的なネットワークの保護	○
4.4　業務ネットワークのセキュリティ	○
4.4.1 ネットワークのセキュリティレベル	○
4.4.2 複数の認証システム	○
4.4.3 パスワードポリシー、多要素認証	○
4.4.4 認証情報の一元管理	○
4.4.5 業務ネットワークの監視	○
4.4.6 運用業務端末のセキュリティ	○
4.4.7 業務ネットワークの定期的な検査	○
4.5　cloudpack から AWS へのアクセスに関するセキュリティ	○
4.5.1 サーバー環境へのアクセス経路の限定	○
4.5.2 AWS インフラストラクチャへのアクセス経路の限定	○
4.5.3 ユーザー様環境における各種作業の監視	○
4.6　cloudpack が利用する社外リソースのセキュリティ	○
4.6.1 Backlog	○
4.7　脆弱性情報に対する対応	○
4.7.1 脆弱性情報の検知から影響調査	○
4.7.2 対応	○
4.8　順守状況および是正対策の報告	○
4.9　セキュリティインシデントの報告	○

https://cloudpack.jp/

お問い合わせ

sales@cloudpack.jp
0120-677-989

運営 アイレット株式会社

東京都港区虎ノ門 1-23-1
虎ノ門ヒルズ森タワー7F
https://www.iret.co.jp/