docomo R&D Open House 2017 in TOKYO

G 05

docomo cloud package

パブリッククラウドの導入・運用をお助けします

NTTドコモがパブリッククラウドを利用することで培ったノウハウをご提供！

ドコモと同等レベルのセキュリティ基準を満たすことができます

特長

■ **高いセキュリティ**：セキュリティ基準(ISO/IEC27017:2015)に対する準拠性を高める

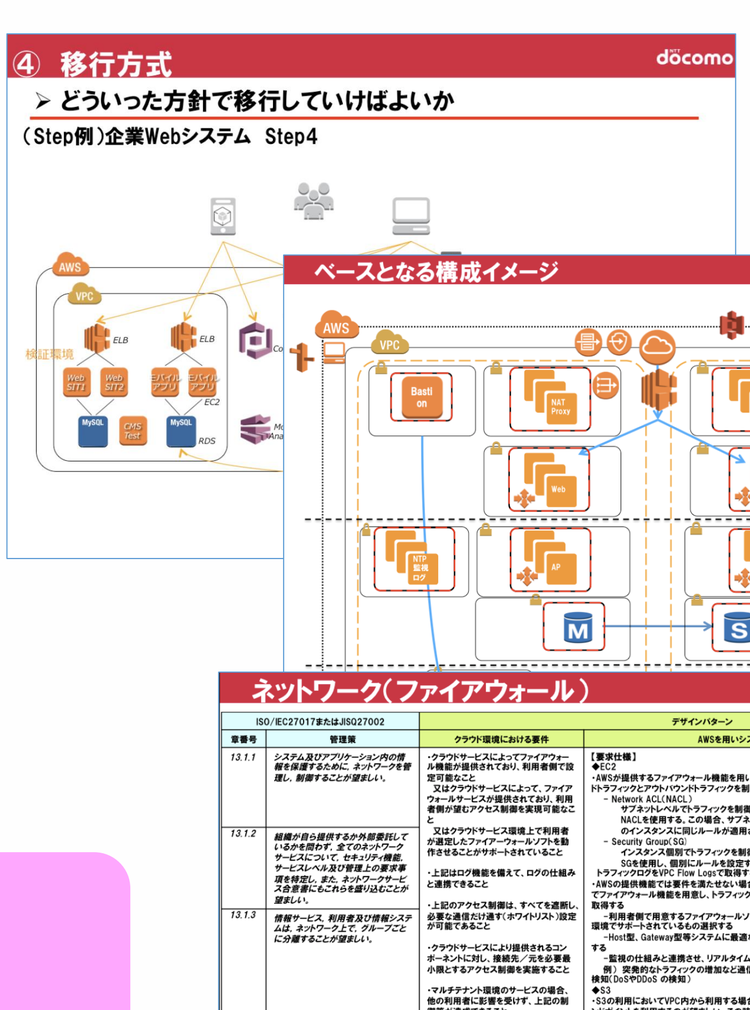
■ **わかりやすいガイドライン**：クラウド利用時のお作法や考慮・実地すべき指針が明確にわかる

■ **実績**：実際にドコモで実施している開発フローに沿ったノウハウがわかる

2015年2月に提供開始し、**100社以上**に導入済！！

<u>活用事例</u>

- システム要件（RFP）作成時に引用
- クラウド利用時の独自ガイドライン作成
- IAMデザインパターンをもとに権限見直し
- 社員教育に利用
- 移行案件をガイドラインを参考に実施
- サービス開発時に要求条件として参照



ISO/IEC27017またはJISQ27002		デザインパターン	
章番号	管理策	クラウド環境における要件	AWSを用いシステム構築を行う場合の要求仕様
13.1.1	*システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御することが望ましい。*	・クラウドサービスによってファイアウォール機能が提供されており、利用者側で設定可能なこと 又はクラウドサービスによって、ファイアウォールサービスが提供されており、利用者側が望むアクセス制御を実現可能なこと 又はクラウドサービス環境上で利用者が選定したファイアーウォールソフトを動作させることがサポートされていること ・上記はログ機能を備えて、ログの仕組みと連携できること ・上記のアクセス制御は、すべてを遮断し、必要な通信だけ通す（ホワイトリスト）設定が可能であること ・クラウドサービスにより提供されるコンポーネントに対し、接続先／元を必要最小限とするアクセス制御を実施すること ・マルチテナント環境のサービスの場合、他の利用者に影響を受けず、上記の制御等が達成できること	【要求仕様】 ◆EC2 ・AWSが提供するファイアウォール機能を用い、インバウンドトラフィックとアウトバウンドトラフィックを制御する －Network ACL(NACL) サブネットレベルでトラフィックを制御する場合は、NACLを使用する。この場合、サブネット内の全てのインスタンスに同じルールが適用される －Security Group(SG) インスタンス個別でトラフィックを制御する場合は、SGを使用し、個別にルールを設定する トラフィックログをVPC Flow Logsで取得する ・AWSの提供機能では要件を満たせない場合、利用者側でファイアウォール機能を用意し、トラフィックログは必ず取得する －利用者側で用意するファイアウォールソフトは、AWS環境でサポートされているもの選択する －Host型、Gateway型等システムに最適な構成を採用する －監視の仕組みと連携させ、リアルタイム通知を行う 例）突発的なトラフィックの増加など通信傾向の異常検知(DoSやDDoS の検知） ◆S3 ・S3の利用においてVPC内から利用する場合は、VPCエンドポイントを利用するのが望ましい。この時、適切なポリシーをVPCエンドポイントに設定して、必要に応じて利用を制御すること。 ・VPCエンドポイントを利用する場合、VPC内の通信制御をNetworkACLで行うのは難しくなるため、各インスタンスはSecurityGroupでインスタンス間やVPCエンドポイント、その他に対して適切な通信制御を行うこと。 ・インターネットからのアクセスが不要な場合は、利用するS3バケットのバウケットポリシーによってVPCエンドポイントからのアクセスのみ利用できるようにするのが望ましい。 ・S3は外部セグメントからのアクセス可否を設定できるので、必要のない場合はPrivateに設定する。 ◆AWS提供マネージドサービス全般 ・必要に応じIAM機能のRole設定やPolicy設定を用いた接続制限を行う	【AWSの仕様（提供機能・サービス）】 ・ファイアウォール相当機能が2つ提供されている －Network ACL(NACL) ・サブネットレベル ・ステートレスのフィルタリング機能 ・許可と拒否のルールがサポートされる －Security Group(SG) ・インスタンスレベル ・ステートフルのフィルタリング機能 ・許可ルールのみがサポートされる ・VPCでFlowLogsを有効にすることで、サブネットやENIのトラフィック情報がCloudWatchLogsへ保存される ・SGは、IPアドレス／ネットワーク／他のSGのGroup IDを接続元に指定することができる ・ELBにて通信元のPortが取得でき、許可ログの代替となる ・IAM機能のRoleの設定を用いると、AWSの提供コンポーネントに対し、通信元IPアドレスによる接続制限が可能 ・VPCエンドポイントを利用することで、VPC内のインスタンスはパブリックIPを利用せずに他AWS提供コンポーネントにアクセス可能 ※2015/6/8時点でS3利用可 ・ポリシーをVPCエンドポイントに設定することで通信を制限することが可能 【備考】 ・一部WAFに関して、AutoScalingへの対応がうたわれているが、Gateway型を用いた場合、Auto Scalingと連携したアタッチ・デタッチが出来なくなる可能性がある。利用する場合は注意する必要がある。 ・Host型を用いた場合、保護するインスタンス分ライセンスが必要となるため、Auto Scalingによるインスタンス数増加に対応したライセンスとする ・VPCエンドポイントを利用する場合、利用するインスタンスが含まれるサブネットのNetworkACLは「すべて許可(0.0.0.0/0)」を設定するか、VPCエンドポイント用のCIDRを設定する必要がある。このCIDRは変更となる可能性があるため、定期的に確認・設定する必要性がある。
13.1.2	*組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込むことが望ましい。*		
13.1.3	*情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離することが望ましい。*		

価格

初年度　　19万円（税別）
2年目以降　10万円（税別）更新する場合

コンサルティングは必要に応じてご提供　2万円/H

今後の展開

- AWSセキュリティ自動チェックツールのご提供

© 2017 NTT DOCOMO, Inc. All Rights Reserved.