# AWSクラウド利用における
# 政府機関向けセキュリティリファレンスの概要

PwCあらた有限責任監査法人
アクセンチュア株式会社
株式会社エヌ・ティ・ティ・データ
富士ソフト株式会社

# 政府機関向け、AWSクラウド利用のセキュリティリファレンス

- PwCあらた、アクセンチュア、NTTデータ、富士ソフトの4社にてAWSクラウド利用における政府機関向けセキュリティリファレンスを作成し、2018年12月25日より各社ホームページなどで提供を開始しました。
- 政府統一基準に対応した、AWSクラウド利用における情報システムの調達・構築～運用を行う際のご支援を致します。

平成30年度版政府統一基準で求められるもの

# クラウドファースト時代に求められる新たな行政サービス構築

- 政府機関においてはクラウド活用を前提とした行政サービスの構築が求められており、そこではクロスボーダー化したデジタルガバメントの推進が求められる一方、政府機関として高度なセキュリティ水準の維持が欠かせません。
- 政府情報システムの在り方が大きく変わる現在において、クラウドサービス「AWS」環境における政府統一基準準拠のノウハウを提供することにより、各政府機関が安全で信頼性の高いシステムを活用できるよう支援して参ります。


**政府による考え方の策定および公表の流れ**

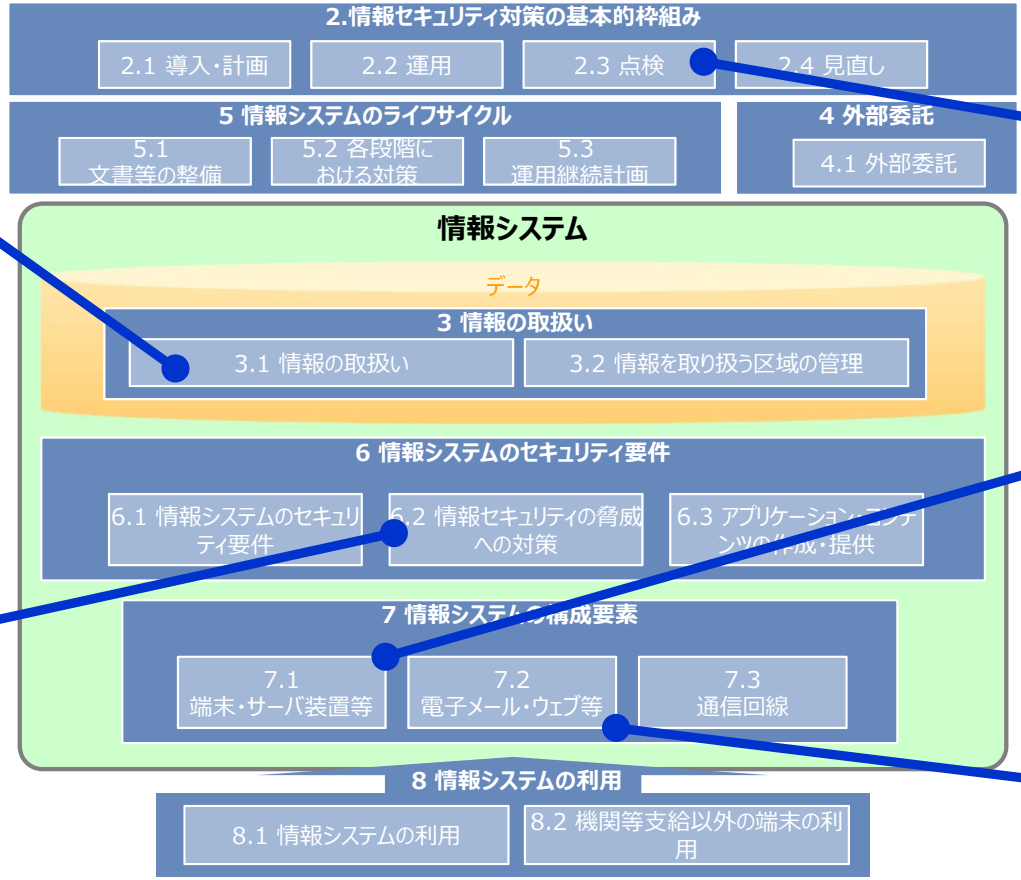
- デジタルガバメント実行計画の策定（2018年1月）
- 「デジタルファースト法案」概要の策定（2018年6月）
- クラウド・バイ・デフォルト原則の公表（2018年6月）

平成30年度版政府統一基準で求められるもの

# サイバーセキュリティ対策高度化を見据えたセキュリティ管理策の見直し

- 政府統一基準（平成30年度版）は、サイバーセキュリティ対策の高度化、政府機関等サービス利用者の保護、自律的な能力向上への誘導、業務形態に対応した規定の整備に関する見直しが行われました。

## 政府統一基準（平成30年度版）




### 3.1.1 情報の取扱い

- 独立行政法人及び指定法人における職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずること。
- (ア) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。

### 6.2.1 ソフトウェアに関する脆弱性対策

- 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。

### 2.3.2 情報セキュリティ監査

- 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。

### 7.1.3 IoT 機器を含む特定用途機器

情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

### 7.2.1電子メール

情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。

# AWSクラウド責任共有モデルの考え方

- AWSは責任共有モデルの考え方により、AWSクラウドが責任を持つ範囲とユーザーが責任を持ち対応する範囲を明確にしております。

責任分界点を理解したユーザーの
対応指針を提示

**アマゾン ウェブ サービス対応
セキュリティリファレンス**

- ✓ AWSクラウド利用におけるユーザーの対応指針
- ✓ AWSクラウドで実現可能なこと
- ✓ AWSクラウドの情報


- ユーザーが責任を持ち対応する範囲
- AWSクラウドが責任を持つ範囲

# AWSクラウドのインフラストラクチャセキュリティ

- AWSクラウドは、インフラストラクチャレイヤにおけるセキュリティ（物理セキュリティ、ネットワークセキュリティ、仮想化セキュリティ、管理者権限管理、認定＆認証評価）を管理します。

| | |
|---|---|
| 物理セキュリティ（データセンター、サーバ装置等） | ●AWSクラウドのデータセンターの場所は公開されておらず、物理的なアクセスが必要な管理者等に限り入館に関する情報が付与され、管理されている。<br>●データセンターでは専門のセキュリティスタッフが監視カメラ、侵入検出システム等を用い、物理的なアクセスを監視している。<br>●サーバ装置の運用にあたっては、 ISO27001等に準拠し、不正な持ち出し等からの保護するための対策を採用している。 |
| ネットワークセキュリティ | ●ネットワークセキュリティ対策として、DDoS攻撃対策、中間者（MITM）攻撃対策、IPスプーフィング対策、ポートスキャン対策、パケットスニッフィング対策等の実施している。<br>●インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御可能とする仕組みを有している。 |
| 仮想化セキュリティ | ●物理マシン上で実行中の各インスタンス同士は互いにアクセス権を有することは無く、ハイパーバイザーを経由して互いに分離している。（あたかも物理的に分離したホスト上に存在しているかのように扱うことができる。）<br>●AWSクラウドのファイアウォールはハイパーバイザー層の中に存在し、全パケットはこの層を通過しなければならない。 |
| 管理者権限管理 | ●AWS従業員のユーザアカウントは適時追加、変更、削除され、定期的に監査される。<br>●AWS従業員の特権の必要な作業は、完了後速やかにそのアカウントを削除する。 |
| 認定＆認証評価 | ●各種セキュリティのベストプラクティス、および各種 IT 統制の要件に合わせて運用されている。<br>（ISO 27001、SOC1(AT801)、PCI DSS、FISMA、HIPAA等） |

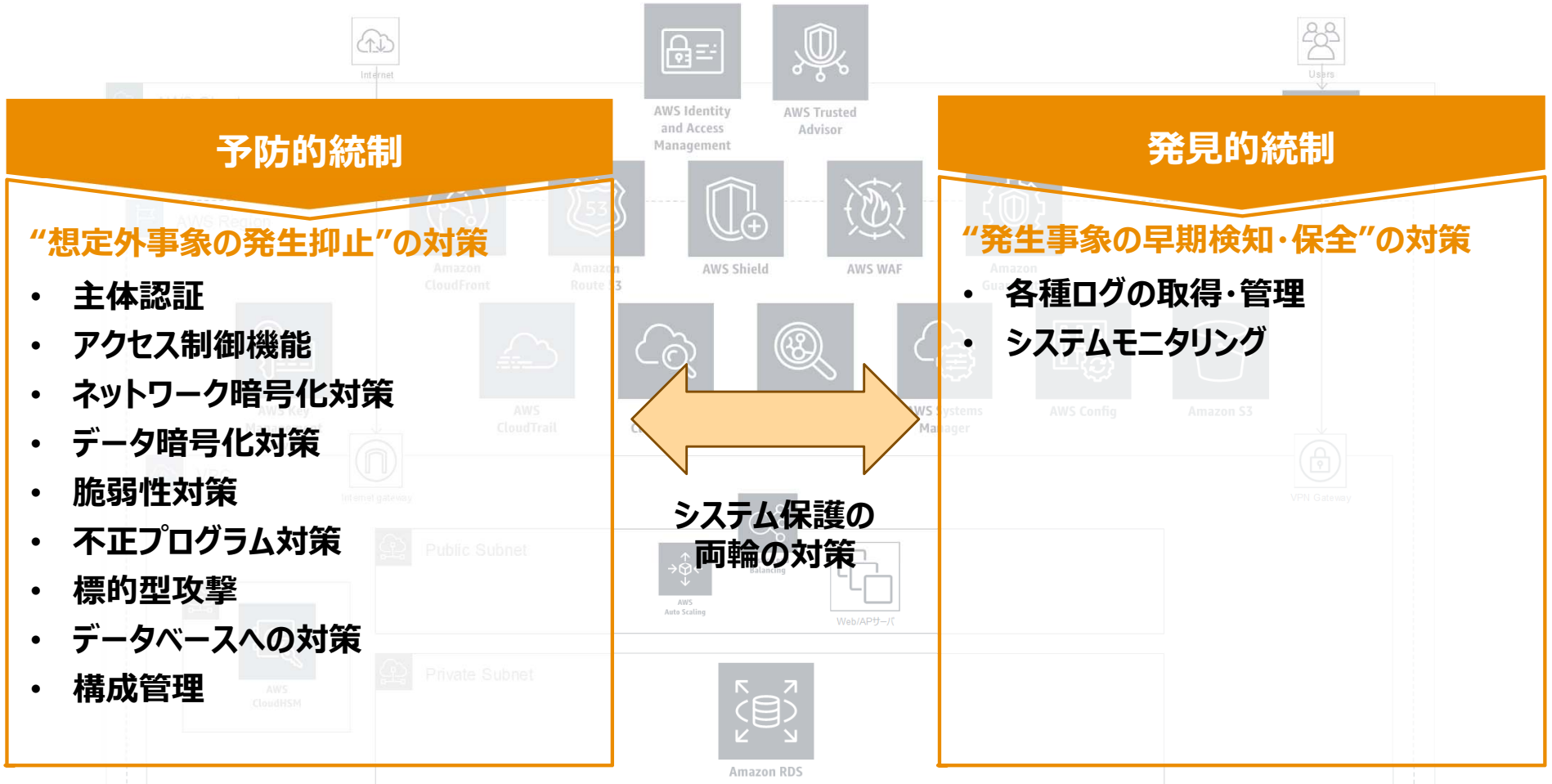
# クラウド選定時の考慮点への対応

- クラウドサービス選定時に懸念される適用法やデータセンタ設備やディスク廃棄におけるリスクに対し、AWSクラウドではリスク軽減のための対策を取ることが可能です。

| | AWSクラウドで実現可能なこと | リファレンス上の項番 |
|---|---|---|
| 国内法以外の法令が適用されるリスク | ●AWSクラウドでは、データとサーバーを配置する物理的なリージョンをAWSクラウドの利用者が指定することができるため、情報を日本に保存することができます。<br>●AWSクラウドでは、利用者がデータの統制と所有権を有しており、AWSクラウド上のリソースについてアクセス権、暗号化などのセキュリティ対策を施すことが可能です。 | 4.1.4 クラウドサービスの利用 |
| データセンタ関係者からの情報漏洩リスク | ●AWSクラウドは、ISO27001等に準拠し、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威からの保護を行っています。AWSクラウドの利用者は、これらの認証を取得していることを確認可能です。 | 3.1.1 情報の取扱い<br>3.2.1 情報を取り扱う区域の管理<br>7.1.2 サーバ装置<br>7.3.1 通信回線 |
| ディスク廃棄時の情報漏洩リスク | ●AWSクラウドは、ISO27001に準拠しており、ストレージデバイスが製品寿命に達した場合、廃棄プロセスの一環としてデータを破棄しています。 AWSクラウドの利用者は、これらの認証を取得していることを確認可能です。<br>●ハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁又は物理的に破壊します。<br>●また、削除したEBSボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。 | 3.1.1 情報の取扱い<br>3.2.1 情報を取り扱う区域の管理<br>7.1.2 サーバ装置<br>7.3.1 通信回線 |

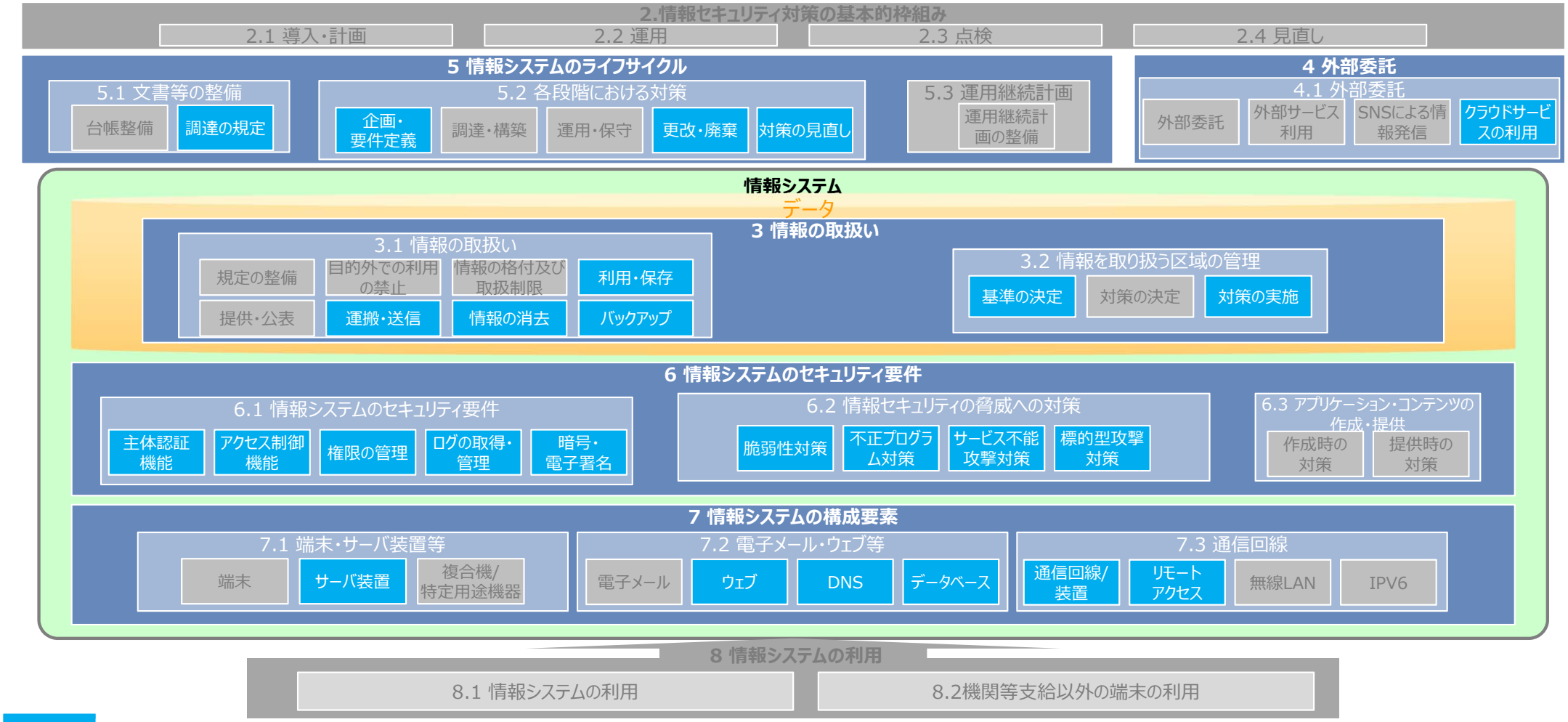
# クラウド利用時に考慮すべき代表的なセキュリティ施策

- システムを構築・利用する場合のセキュリティ施策として、誤用を防ぐための予防的統制と検知するための発見的統制が重要です。特にAWSクラウドにおいては、発見的統制のサービスを利用し、検知事象に対する対策を自動化することが可能です。



# セキュリティリファレンスの対象範囲

- 本セキュリティリファレンスでは、システム全体のセキュリティ設計について、AWSクラウドの機能を利用して対応可能なものの対応指針を提供しています。




適合可能 …AWSクラウドの機能を利用して対応可能。

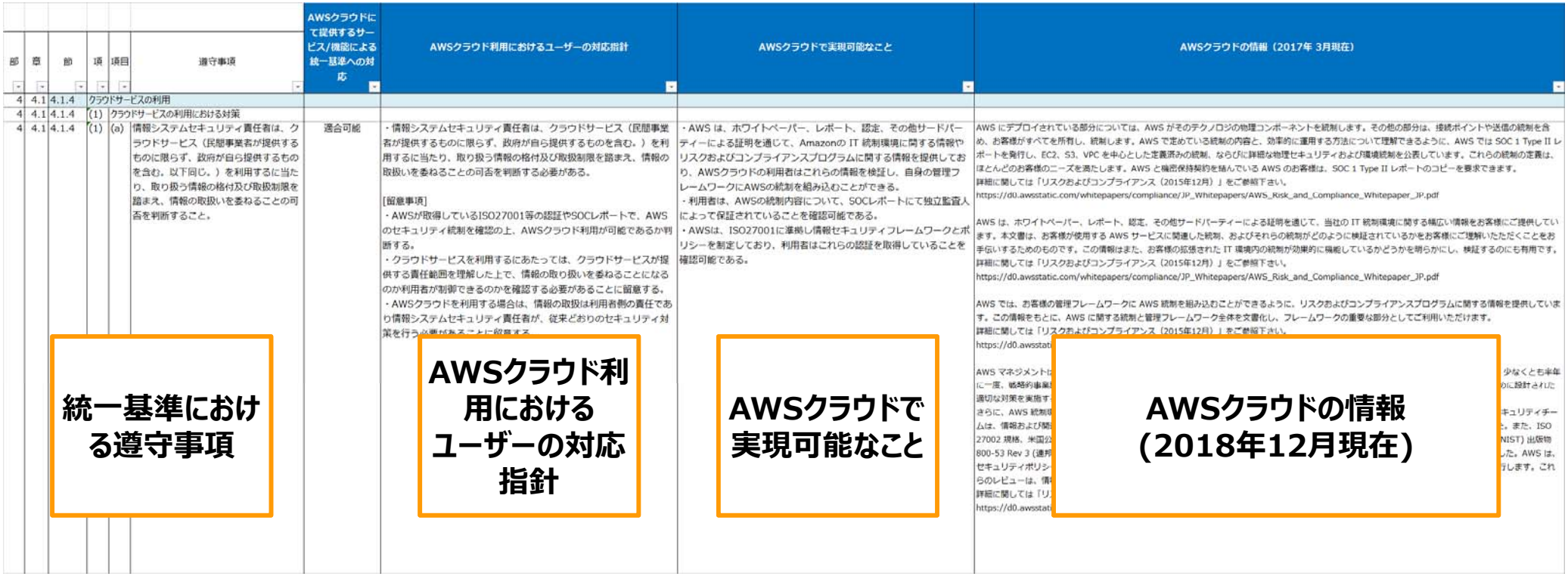
対象外 …本リファレンスでは対象外。クラウド利用有無にかかわらず検討が必要。

詳細は、「AWSクラウド利用における政府機関向けセキュリティリファレンス」参照。

# セキュリティリファレンスの構成

- 本セキュリティリファレンスは、「政府統一基準における遵守事項」「AWSクラウド利用におけるユーザーの対応指針」「AWSクラウドで実現可能なこと」「AWSクラウドの情報」 を解説しています。

## セキュリティリファレンスの記載内容(イメージ)



| 部 | 章 | 節 | 項 | 項目 | 遵守事項 | AWSクラウドにて提供するサービス/機能による統一基準への対応 | AWSクラウド利用におけるユーザーの対応指針 | AWSクラウドで実現可能なこと | AWSクラウドの情報（2017年 3月現在） |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 4.1 | 4.1.4 | クラウドサービスの利用 | | | | | | |
| 4 | 4.1 | 4.1.4 | (1) | クラウドサービスの利用における対策 | | | | | |
| 4 | 4.1 | 4.1.4 | (1) | (a) | 情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。 | 適合可能 | ・情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する必要がある。<br><br>[留意事項]<br>・AWSが取得しているISO27001等の認証やSOCレポートで、AWSのセキュリティ統制を確認の上、AWSクラウド利用が可能であるか判断する。<br>・クラウドサービスを利用するにあたっては、クラウドサービスが提供する責任範囲を理解した上で、情報の取り扱いを委ねることになるのか利用者が制御できるのかを確認する必要があることに留意する。<br>・AWSクラウドを利用する場合は、情報の取扱は利用者側の責任であり情報システムセキュリティ責任者が、従来どおりのセキュリティ対策を行う必要があることに留意する。 | ・AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、Amazonの IT 統制環境に関する情報やリスクおよびコンプライアンスプログラムに関する情報を提供しており、AWSクラウドの利用者はこれらの情報を検証し、自身の管理フレームワークにAWSの統制を組み込むことができる。<br>・利用者は、AWSの統制内容について、SOCレポートにて独立監査人によって保証されていることを確認可能である。<br>・AWSは、ISO27001に準拠し情報セキュリティフレームワークとポリシーを制定しており、利用者はこれらの認証を取得していることを確認可能である。 | AWS にデプロイされている部分については、AWS がそのテクノロジの物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制します。AWS で定めている統制の内容と、効率的に運用する方法について理解できるように、AWS では SOC 1 Type II レポートを発行し、EC2、S3、VPC を中心とした定義済みの統制、ならびに詳細な物理セキュリティおよび環境統制を公表しています。これらの統制の定義は、ほとんどのお客様のニーズを満たします。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。<br>詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。<br>https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf<br><br>AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、当社の IT 統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張された IT 環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。<br>詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。<br>https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf<br><br>AWS では、お客様の管理フレームワークに AWS 統制を組み込むことができるように、リスクおよびコンプライアンスプログラムに関する情報を提供しています。この情報をもとに、AWS に関する統制と管理フレームワーク全体を文書化し、フレームワークの重要な部分としてご利用いただけます。<br>詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。<br>https://d0.awsstati<br><br>AWS マネジメント…に一度、戦略的事業…適切な対策を実施す…さらに、AWS 統制…ムは、情報および関…27002 規格、米国公…800-53 Rev 3（連邦…セキュリティポリシ…らのレビューは、情…詳細に関しては「リ…https://d0.awsstati…少なくとも半年…のに設計された…キュリティチー…。また、ISO…NIST）出版物…した。AWS は、…行します。これ… |

**統一基準における遵守事項**

**AWSクラウド利用におけるユーザーの対応指針**

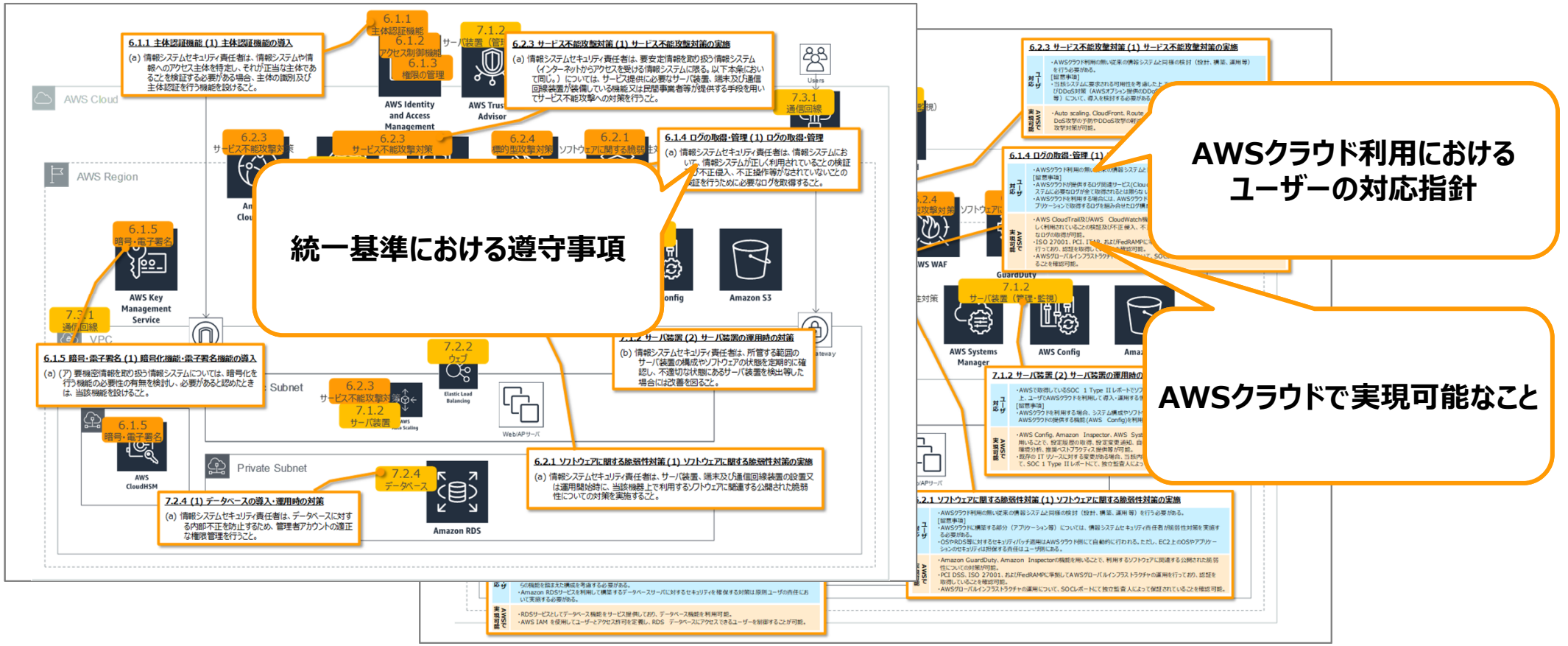
**AWSクラウドで実現可能なこと**

**AWSクラウドの情報（2018年12月現在）**

# セキュリティリファレンスの構成

- 【AWSクラウド利用における政府機関向けセキュリティリファレンス別紙】では、システム構成例に対して、「政府統一基準における遵守事項」「AWSクラウド利用におけるユーザーの対応指針」「AWSクラウドで実現可能なこと」を記載しています。

## 【AWSクラウド利用における政府機関向けセキュリティリファレンス別紙】の記載内容(イメージ)



# 対象とするAWSクラウドのサービス名と参照文書

- 本セキュリティリファレンスにおいて対象とするAWSクラウドのサービス名と参照文書は以下の通りです。

## AWSクラウドのサービス名

**コンピューティング**
Amazon Elastic Compute Cloud (Amazon EC2)
Elastic Load Balancing
Auto Scaling

**ストレージ**
Amazon Simple Storage Service (Amazon S3)
Amazon Elastic Block Store (Amazon EBS)
Amazon Glacier

**データベース**
Amazon Relational Database Service (Amazon RDS)
Amazon Redshift
Amazon ElastiCache

**ネットワーク**
Amazon Virtual Private Cloud (Amazon VPC)
AWS Direct Connect
Amazon Route 53

**管理ツール**
Amazon CloudWatch
AWS CloudTrail
AWS Config
AWS Trusted Advisor
AWS Systems Manager

**セキュリティとアイデンティティ**
AWS Identity and Access Management (IAM)
AWS Key Management Service (KMS)
AWS WAF
AWS Certificate Manager
Amazon GuardDuty
AWS Shield
Amazon Inspector

## 参照文書

セキュリティプロセスの概要（2014 年 11 月）
リスクとコンプライアンス（2015 年 12 月）

等

# お問い合わせ先

**【本リファレンスに関するお客様からのお問い合わせ】**
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
Email: jp_aarata_aws_nisc@pwc.com

**【報道関係の皆様からのお問い合わせ】**
PwCあらた有限責任監査法人　マーケット部　ブランド＆コミュニケーションズ　広報担当
電話： 03-3546-8476（広報代表）
Email：pwcjppr@jp.pwc.com

**【本リファレンスに関するお客様からのお問い合わせ】**
アクセンチュア株式会社　公共サービス・医療健康本部
AWSセキュリティリファレンス担当
Email: info.tokyo@accenture.com

**【報道関係の皆様からのお問い合わせ】**
アクセンチュア株式会社　マーケティング・コミュニケーション本部
広報担当
Email: accenture.jp.media@accenture.com

**【本リファレンスに関するお客様からのお問い合わせ】**
株式会社ＮＴＴデータ　データセンタ＆クラウドサービス事業部
電話： 050-5546-8622
Email：datacenter@kits.nttdata.co.jp

**【報道関係の皆様からのお問い合わせ】**
株式会社ＮＴＴデータ　広報部
電話： 03-5546-8051

**【本リファレンスに関するお客様からのお問い合わせ】**
富士ソフト株式会社　営業本部　クラウド&ソリューション事業部
プラットフォームソリューション営業部
電話： 050-3000-2100
Email: cs-sales@fsi.co.jp

**【報道関係の皆様からのお問い合わせ】**
富士ソフト株式会社　コーポレートコミュニケーション部
電話： 050-3000-2735
Email: mkoho@fsi.co.jp