「金融機関向け『Amazon Web Services』対応 セキュリティリファレンス」の概要 version1.2対応

2013年9月11日

SCSK株式会社（SCSK）
株式会社電通国際情報サービス（ISID）
株式会社野村総合研究所（NRI）
TIS株式会社（TIS）
三井情報株式会社（MKI）
トレンドマイクロ株式会社（TrendMicro）
株式会社シーエーシー（CAC）

Ver.1.20

本文書の構成

1. はじめに
2. FISC安全対策基準とは
3. セキュリティリファレンスの内容
4. セキュリティリファレンスの対象範囲と想定読者
5. セキュリティリファレンスを利用するメリット
6. セキュリティリファレンスの種類と開示
7. セキュリティリファレンスの項目例
8. セキュリティリファレンスの著作権と利用許諾
9. さいごに

1. はじめに

近年、AWSをはじめとするクラウド・サービスは、ビジネスを変革させる手段として、多数の企業で活用されはじめています。

しかし、企業の重要な情報システムにおいては、省庁や業界団体などのセキュリティガイドラインと、クラウド事業者が開示しているシステム仕様との対応、解釈が難しいという課題がありました。

AWSのソリューションプロバイダである SCSK、ISID、NRI、TIS、TrendMicro、MKI、CAC の7社は、セキュリティ基準の厳しい金融機関等においてクラウドの活用を促進することを目的に、AWSのセキュリティ対応内容が、FISC「金融機関等コンピュータシステムの安全対策基準・解説書」第8版および第8版追補の全項目に対し、どのように適合し得るか共同で調査／検討を行いました。その成果を「セキュリティリファレンス」として整理し、一部を無償で公開いたします。

リファレンスをまとめるにあたり、アマゾンデータサービスジャパンの協力を得て、これまで非公開であった情報についても調査対象としています。さらに、7社の豊富な金融機関へのシステム提供経験やノウハウに基づく解釈も加えました。

2. FISC安全対策基準とは（１）

◆『金融機関等コンピュータシステムの安全対策基準』（第8版）

- 公益財団法人金融情報システムセンター（FISC）が調査研究を通じて、専門委員会、検討部会により審議・作成する金融機関等の自主基準。
- 金融庁が金融機関を検査する際に使用される「金融検査マニュアル」において、検査官が具体的なシステム検査を行う際に、FISCの「金融機関等コンピュータシステムの安全対策基準」を参照するよう、記載されている。
- 138の設備基準、114の運用基準、53の技術基準、全305項目で構成。
- FISCから解説書として発刊。同サイトから購入可能。

金融情報システムに関する安全対策の共通のよりどころとなる具体的指針として、金融機関に広く活用されている。

FISC：The Center for Financial Industry Information Systems

出典：FISC ホームページ（http://www.fisc.or.jp）

2. FISC安全対策基準とは（２）

◆『金融機関等コンピュータシステムの安全対策基準』（第8版追補）

- クラウドサービスの利用に関わる現状の課題や留意点、スマートデバイスの業務利用における留意点などを検討。
- 「主な論点」へ論点と改訂方針を整理。
- 運用基準の1項目（運108）を新設。設備基準の変更4、運用基準の変更21、技術基準の変更14。全306項目で構成。
- FISCから平成25年3月に発刊。同サイトから購入可能。

運 108 クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。

出典：『金融機関等コンピュータシステムの安全対策基準』（第8版追補）

3. セキュリティリファレンスの内容（１）

「金融機関向け『Amazon Web Services』対応セキュリティリファレンス」（以下、セキュリティリファレンス）は、FISC安全対策基準で記載されている各項目に対して、AWS の公開情報、非公開情報を含めて、SCSK、ISID、NRI、TIS、TrendMicro、MKI、CAC の7社が調査、検討したセキュリティ対応の内容が記載されています。

【セキュリティリファレンスの主要項目】

- ◆ FISC安全対策基準の項目と説明（第8版および第8版追補からの引用）
- ◆ FISC安全対策基準（中項目レベル）へのAWSの見解
- ◆ FISC安全対策基準の各項目への適合性の可能性
- ◆ クラウド事業者(AWS)の対応状況とその根拠
  - ➢ 根拠は、①公開文書、②第3者認証からの類推、③AWS内部情報
  - ➢ 根拠となる公開文書については、その参照元箇所
- ◆ SI事業者・利用者で必要な対応

3. セキュリティリファレンスの内容（２）

「金融機関向け『Amazon Web Services』対応 セキュリティリファレンス」

FISC安全対策基準

- 設備基準 ― 基準項目
- 運用基準 ― 基準項目
- 技術基準 ― 基準項目

FISC安全対策基準(第8版、第8版追補)から引用

第8版追補関連

⇨ 関連項目を明確化
運108関連を補足

ver.1.2 追加

クラウド事業者（AWS）の対応

対応状況 ／ 実施内容 ／ 実施内容の参照先

公開文書への参照	実施内容が記載されている公開文書の該当箇所
第三者認証からの類推	実施内容が妥当と判断される取得済み第三者認証の名称と該当項目
AWS/ADSJの非公開情報	AWS/AWSJへのインタビュー、内部資料など

根拠となる事由を整理

SI事業者・利用者で必要な対応

対応要否 ／ 対策例

SI事業者・利用者の責任において実施すべきか否か、また、その対策例を記載。

クラウド特有の対応方法

一般的方法

クラウド利用時に一般的に検討される対応方法を記載。

AWS特有の方法

クラウド事業者（AWS）が提供しているどのサービスを活用できるのかを整理。

ver.1.1 追加

3. セキュリティリファレンスの内容（3）

FISC安全対策基準（第8版追補）で追加、変更されている各項目に対して、次の改訂を行っています。

【主要改訂項目】

- ◆ セキュリティリファレンスへ、第8版追補にて追加、変更された項目および新設の運108から参照される各項目を明記
- ◆ FISC安全対策基準（第8版追補）の主な論点に対し、クラウド事業者やSI事業者/利用者の対応の要否とその説明を第8版追補変更点として新設
- ◆ 新設の運108に関連する項目をセキュリティリファレンス(運108関連)として新設

4. セキュリティリファレンスの対象範囲と想定読者

【セキュリティリファレンスの対象範囲】

FISC安全対策基準（設備基準/運用基準/技術基準）に記載されている306項目について、調査、検討をしました。
各項目は、適用にあたり以下の分類がされています。
「◎」 当該基準を取り入れることが必要な項目
『～すること』と記述されてる。
「○」 金融機関等の業務の実態に照らし、必要に応じて取り入れる項目
『～が望ましい』と記述されている。
※ 設備基準の84～137は、営業店などへの機器設置に関する項目のため、セキュリティリファレンスでは省略しています。

【セキュリティリファレンスの想定読者】

AWSの利用を検討する金融機関とSIerを基本的に想定していますが、FISC安全対策基準のほとんどの項目は、金融業務システム以外でも普遍性があるため、金融機関以外の利用者においてもご活用いただけます。

5. セキュリティリファレンスを利用するメリット

【AWSを利用する金融機関、SIerの利用者のメリット】

- ◆FISC安全対策基準の項目毎に、クラウド事業者(AWS)と利用者との間の責任境界を把握できます。
- ◆FISC安全対策基準の項目毎に、AWSのセキュリティ対応について、その内容と根拠となる文書の記載箇所が把握できます。
- ◆これらの把握と理解を通じて、FISC安全対策基準の各項目に適合させるための検討が効率よく行えます。
- ◆FISC安全対策基準のほとんどは普遍性のある管理項目であるため、非金融の企業、団体においても、重要な業務システムをAWS上で安全に稼働させるための検討が効率よく行えます。

6. セキュリティリファレンスの種類と開示

セキュリティリファレンスは、記載内容のレベルから、サマリー版と詳細版の2つの種類があります。その違いは以下の通りです。

	サマリー版	詳細版
目的	AWSの対応状況の概要を把握	AWSの対応状況の詳細を把握
記述レベル	利用者視点での対応状況・方法を記載	AWSへのインタビュー等の詳細を記載
入手方法	7社のWebサイトで公開誰でもダウンロード可	各社個別のAWS案件にて開示。AWSとのNDAも必要。

7社がご提供する内容はいずれも同一のものです。

7. セキュリティリファレンスの項目例（1）

Ver1.0

FISC 安全対策基準第8版からの引用							FISC安全対策基準に対するAWSの見解	FISC安対基準への適合性	クラウド事業者の対応（Amazon Web Services）						SI事業者・利用者で必要な対応	
SEQ	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	必須項目			対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から類推（詳細版で開示）	AWS/ADSJへのインタビュー結果（詳細版で開示）	NDAベース資料への参照（詳細版で開示）	対応要否	対策例（詳細版で開示）
A2400001	運17	V.運用基準	運用管理（アクセス権限の管理）	運17 パスワードが他人に知られないための措置を講じておくこと。	パスワード等の漏洩防止のため、他人に知られないための注意喚起等の措置を講じておくこと。	◎	ISO 27001に則り、AWSリソースへの論理的なアクセスのために必要な手順やポリシーを定めています。SOC1タイプ2レポートには、AWSリソースへのアクセスを管理するためのコン	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、PCI DSS Level 1の認証を取得している	・Amazon Web Services: セキュリティプロセスの概要/従業員のライフサイクル、Amazon アカウントセキュリティ機能 ・Amazon Web Services: リスクとコンプライア ス/AWS				●	

◎：当該基準を取り入れることが必要
○：金融機関等の業務の実態に照らし、必要に応じて取り入れる基準

適合可能
(適合不可)
対象外: クラウド環境では対象外

○: 対応実施
—: 対応不要
対象外: クラウド環境では対象外

公開情報
(実施内容はサマリー版に記載)
詳細版に記載
(実施内容は非公開情報のため詳細版に記載)

●: 対応必要
—: 対応不要
対象外: クラウド環境では対象外

7. セキュリティリファレンスの項目例（2）

Ver1.1

クラウド事業者の対応（Amazon Web Services）							SI事クラウド事業者の対応（Amazon Web Services）業者・利用者で必要な対応		
対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から類推	AWS/ADSJへのインタビュー結果（詳細版で開示）	NDAベース資料への参照（詳細版で開示）	対応要否	対応パターン	対策例
○	公開情報	・ISO 27001を始め、SOC1 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理／システム文書のセキュリティ」に従った対策の実施。			●	1	通常のシステム運用と同様に、システム運用における手順書等のドキュメントを保管管理する。

ISO等第三者認証の認証状況から対応状況が類推できる対応

SI事業者・利用者側でのFISC安全対策基準への対応となる対策例。
大きく次の２つに分類
・クラウド特有の対応
・従来通りの対応

7. セキュリティリファレンスの項目例（3）

Ver1.1

クラウド特有の対応方法　○・・・対応必須、△・・・対応推奨

クラウドの一般的対応方法				AWS特有の対応方法		
実装		プロセス		実装		プロセス
暗号化	・・・	FW/IDS/IPS	・・・	API	・・・	AWSサポート
―				―	・・・	
パター						
○		△		―	・・・	―
パターン２						
○	・・・	△	・・・	○	・・・	△
パターン３						

実装と、プロセスを明記

実装：「機能（製品、ツール含む）」を使用すれば実現可能

プロセス：単に機能を使うのではなく、いくつかの手続きをへて実現可能

各機能、手続きを明記

7. セキュリティリファレンスの項目例（4）

Ver1.2

「セキュリティリファレンス」の変更箇所

FISC 安全対策基準第8版および第8版追補からの引用		
必須とされている項目	第8版追補での改訂	運108関連
◎	■	□

■：第８版での改訂項目

□：運108および運108から参照されている項目

○、●：対応の要否

改訂有、改訂無：リファレンスにおける対策例の改訂有無

「第8版追補変更点」を新設

No	第8版追補からの引用			セキュリティリファレンス改訂箇所			
	項目	論点	改訂方針	クラウド事業者の対応	SI事業者/利用者の対応	説明	備考
2	【運1】【運3】セキュリティ管理の責任の明確化	セキュリティ管理のための環境整備について、経営層の関与を明確にすべきではないか。	セキュリティ管理のための文書や体制の整備にあたっては、経営層の主体的な関与が重要と考え、その旨を追記することとした。	○ 改訂無	● 改訂有	SI事業者/利用者は、システム運用におけるセキュリティの管理方針や体制の整備を進める上で、全社的な方針や体制に重大な影響を与えるものがある場合については、経営層の指示、承認を得た上で実施することを追記した。	本項目は、運108における管理事項として、参照されている。

8. セキュリティリファレンスの著作権と利用許諾

- セキュリティリファレンス（以下、本件ドキュメント）の著作権、知的財産権は、SCSK、ISID、NRI、TIS、TrendMicro、MKI、CAC が保有します。
- 本件ドキュメントを現状有姿にて提供し、複製、配布、改変、改変後の再配布について利用許諾します。
- 本件ドキュメントに瑕疵がないこと等は一切保証しません。評価、業務への適用などは、ユーザがすべての責任を負うものとします。
- 本件ドキュメント詳細版については、ユーザは、事前にアマゾンデータサービスジャパンとの間で別途秘密保持契約(NDA)を締結し、その条件を遵守するものとします。
- 詳細は、本件ドキュメントと共に配布される利用許諾契約書をご参照ください。

9. さいごに

本書は、金融機関等におけるクラウド活用を促進することを目的に作成しています。

作成にあたっては、ビジネス上、競合となりうることもある7社が、金融業界におけるクラウドの利活用促進を行うため、協力を行い、リスク評価や対応策について、検討を繰り返し、作成した成果となります。作成においては、アマゾン・データ・サービスジャパンにも、多大に、調査の協力をいただきました。

ご活用いただき、安心・安全なIT環境の実現の一助になれれば、幸いです。

◆セキュリティリファレンス　サマリー版の入手方法（ver1.2）

・下記のSI事業者のご担当にお問い合わせください。

・各社のホームページから入手が可能です。