「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 version1.3第8版追補改訂対応

2016年11月10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）
株式会社ワークスアプリケーションズ
JBCC株式会社

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 、ワークスアプリケーションズ、JBCCの9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版追補改訂に対し、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」第1.3版として整理し、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 ウェブ サービス ジャパンの協力を得て、インタビューや第3者監査レポート等についても調査対象としています。さらに、9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』（以下　安対基準）（第8版及び第8版追補改訂で構成）

- 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、120の運用基準、53の技術基準、全311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版追補改訂）

- クラウドサービスの利用に関する従来の基準である（運108）は暫定対応であったのでこれを削除し、５つの新設基準【運108】～【運112】として全面改訂、再構成を行なった。
- 『金融機関におけるクラウド利用に関する有識者検討会報告書』の内容等を踏まえ、リスクベースアプローチの考え方を導入した
- 金融機関等におけるサイバー攻撃対応態勢の整備に関する内容について基準項目【運113】を新設した。
- 【運108】①事業者選定　②データ所在の把握
- 【運109】①契約締結・サービスレベル合意　②ベンダーロックイン防止
- 【運110】利用中のデータ漏洩防止策
- 【運111】契約終了時のデータ漏洩防止策
- 【運112】立入監査・モニタリング
- 【運113】サイバー攻撃対応態勢

3. セキュリティリファレンス第1.3版の内容（１）

金融機関向け『Amazon Web Services』対応セキュリティリファレンス第1.3版（以下、セキュリティリファレンスVer.1.3）は、安対基準（第8版追補改訂）に記載された各項目に対して、AWS の公開情報、非公開情報を含めて、SCSK、ISID、NRI、TIS、TrendMicro、MKI、CAC 、ワークスアプリケーションズ、JBCCの9社が調査、検討した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Ver.1.3の主要項目】

◆FISC安全対策基準の項目と説明（第8版追補改訂からの引用）

◆対応の主体

◆対応可否判断のための情報参照元

- 根拠となる公開文書及びその該当箇所

◆AWSの該当情報

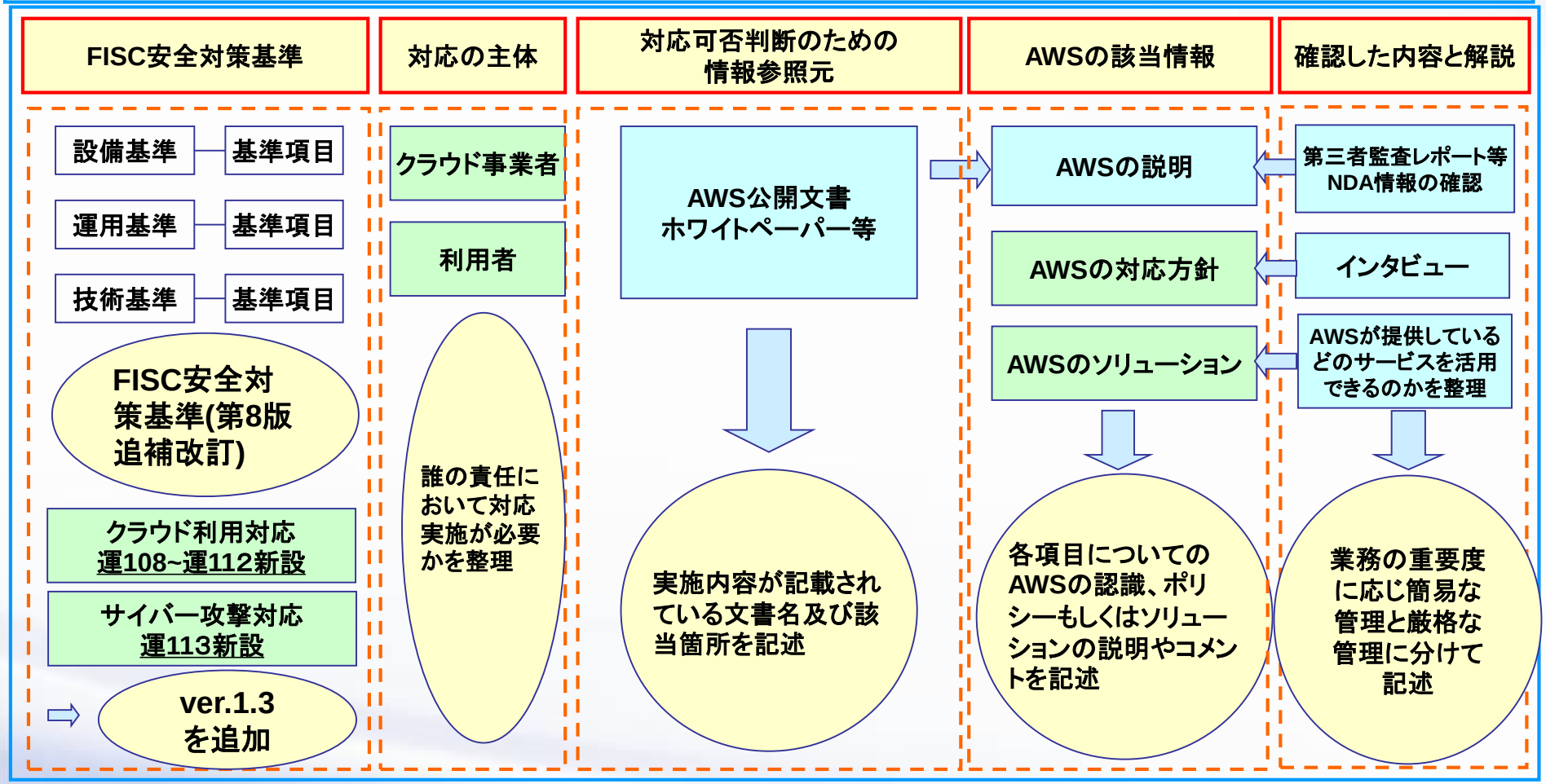
- 公開文書についてのAWSの説明。対応方針や提供ソリューション等

◆9社が確認した内容と解説

- パートナー各社がAWS提供情報について、NDA情報やインタビューを含めて確認、整理した結果を記載。なお、「NDA情報」とはAWSとの秘密保持契約の締結にもとづき提供される各種報告書等を指す。（例：SOC1監査報告書、SOC2監査報告書等）

3. セキュリティリファレンスVer.1.3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」第1.3版



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（第8版追補改訂）における新設6項目、変更20項目より主眼となる「クラウドサービスの利用」及び「サイバー攻撃対応態勢整備」の新設6項目を抽出し、調査、検討をしました。
解説にあたり、今回導入されたリスクベースアプローチの考え方に対応し、利用者である委託元金融機関が委託する業務の重要度に応じ『簡易な管理が求められる場合』と『厳格な管理が求められる場合』に分けて判り易く記述しております。
尚、FISCでは安対基準における語尾により、適用区分を下記のとおりとしております。「可能である」⇒「必要最低限の安対基準」の適用が必要。
「すること」「必要である」⇒「高い安対基準」の適用が求められる

【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、対応する安対策基準の違いにより、第1.2版と第1.3版の2つの種類があります。その違いは以下の通りです。

	第1.2版	第1.3版
対応内容	安対基準第8版追補	安対基準第8版追補改訂
公開時期	2013年10月	2016年11月
入手方法	7社のWebサイトで公開（サマリー版）。詳細版は個別案件にて開示。AWSとのNDAも必要。	9社のWebサイトで公開 誰でもダウンロード可

各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）

FISC 安全対策基準第8版追補改訂からの引用

安対基準をダウンロード

Ver1.3

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	基準項目の目的　内容説明　具体例等の解説
運109	V. 運用基準	クラウドサービスの利用	運109　クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること。	安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。	2. SLAの締結やSLOの確認により、サービスレベル(注)について合意することが望ましい。 SLA及びSLOに記載すべき指標には以下のような例がある。 (注) クラウド事業者との契約の中にはSLAが含まれるのが通例であるが、多くの標準的なSLAでは、基準となる月間稼働率などを定めたうえで、実際の稼働率が基準を下回った場合にサービスの利用料を減額するといった内容にとどまっている。そのため、例えば、勘定系システムのオンライン処理など高い稼働率が求められる場合では、こうした標準的なSLAによる契約締結では不十分な可能性がある。クラウド事業者の顧客は金融機関をはじめ、さまざまな業種にわたる。その中で各顧客企業との間で個別の内容の契約を準備するのは効率的ではないとの考えから、クラウド事業者はSLAを個別に締結することに対し消極的な場合もある。一方で、金融機関が特に重要な業務を委託する場合においては、その社会的な重要性に鑑み、相応の高いサービスレベルが求められる。

7. セキュリティリファレンスの項目例（2）

Ver1.3

FISC 安全対策基準第8版追補改訂からの引用（続き）		対応の主体	
基準項目の目的　内容説明　具体例等の解説	基準項目の目的　内容説明　具体例等の解説	クラウド事業者	利用者
2.　SLAの締結やSLOの確認により、サービスレベル(注)について合意することが望ましい。 SLA及びSLOに記載すべき指標には以下のような例がある。 (注) クラウド事業者との契約の中にはSLAが含まれるのが通例であるが、多くの標準的なSLAでは、基準となる月間稼働率などを定めたうえで、実際の稼働率が基準を下回った場合にサービスの利用料を減額するといった内容にとどまっている。そのため、例えば、勘定系システムのオンライン処理など高い稼働率が求められる場合では、こうした標準的なSLAによる契約締結では不十分な可能性がある。 クラウド事業者の顧客は金融機関をはじめ、さまざまな業種にわたる。その中で各顧客企業との間で個別の内容の契約を準備するのは効率的ではないとの考えから、クラウド事業者はSLAを個別に締結することに対し消極的な場合もある。一方で、金融機関が特に重要な業務を委託する場合においては、その社会的な重要性に鑑み、相応の高いサービスレベルが求められる。	(1) システム運用(可用性(注)、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制)の保証 (注) システム運用の可用性に関する指標の評価にあたっては、以下のような事項を考慮する必要がある。 1) 障害等に伴うシステムの停止時間 2) システムの更新・保守(緊急的なセキュリティパッチ対応を含む)や新サービスの追加などシステムの品質・セキュリティ向上のための計画停止期間 なお、上記2)に関して、グローバルベースでサービスが提供されるパブリッククラウドでは、緊急的なセキュリティ対策等に係る計画停止作業について、ユーザー全体の安定性を優先するため、必ずしも個々のユーザーの要望(作業のタイミングや時間等)に沿わない形で実施される可能性があることにも留意する必要がある。	クラウド事業者・利用金融機関の責任分担を明確化 ○ SLA締結はクラウド事業者と利用金融機関の共同作業につき双方に○	○

7. セキュリティリファレンスの項目例（3）

対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
基準項目に対するクラウド事業者の一般公開情報の所在	各項目についてのAWSの説明。AWSの対応方針やソリューション等	パートナー各社がＡＷＳからの提供情報をNDA情報やインタビューを含めて確認整理し、FISC安対基準に則った利用者側の対応を説明
5、21、24 情報参照元一覧シートの該当記号を表記（1～24)一覧には公開文書名と所在（URL）を記載 5:AWSリスクおよびコンプライアンス（ホワイトペーパー）https://s3.amazonaws.com/awsmedia/jp/wp/AWS_Risk_and_Compliance_Whitepaper.pdf 21：ホワイトペーパー DDoSに対するAWSのベストプラクティス http://media.amazonwebservices.com/jp/DDoS%20White%20Paper_Revised.pdf	AWSは、サービスレベルアグリーメント（SLA）で高レベルの可用性を提供しています。例えば、Amazon EC2 は、1 年のサービス期間で 99.95% 以上の稼働時間となっています。Amazon S3 は毎月 99.9% 以上の稼働時間です。こうした可用性の評価指標が基準に満たない場合は、サービスクレジットが提供されます。 24：サービスレベルアグリーメント一部（EC2のSLA) https://aws.amazon.com/jp/ec2/sla/	簡易な管理が求められる場合には、標準的約款のカスタマイズは必須でなく、AWS標準のカスタマーアグリーメント、各種SLAですぐにでもAWSが利用可であることを確認した。 FISC安対基準のリスクベースに則った対応説明 厳格な管理が求められる場合には、各金融機関のセキュリティポリシーに合わせクラウド事業者が提供する標準的約款をカスタマイズしリスク管理に必要な事項を業務委託契約、SLA/SLOに盛り込む必要がある。

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、ワークスアプリケーションズ、JBCC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。

- 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9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 ウェブ サービス ジャパンにも、多大な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の入手方法（ver1.3）

・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。