公表されている内容そのものとなります。

一般的に検討したほうがよい見解（※クラウドに限定しない）と、AWS上でどう実現できるかについて記載しております。

項番	小番号	分類	タイトル・内容	一般的に考えられる対応内容 （当社コンサルタント見解）	AWS環境上で当社の設計含めて 実現すること／実現できること
2			サイバーセキュリティ管理態勢		
2.1			サイバーセキュリティ管理態勢の構築		
2.1.1			基本方針、規程類の策定等		
	①	基本的な対応事項	取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部としてとらえ、サイバーセキュリティ管理の基本方針を策定すること。サイバーセキュリティ管理の基本方針には、例えば、以下の事項を記載すること。 ・セキュリティ対策の目的や方向性 ・関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び法規制等法規制等への対応 ・経営経営陣陣によるコミットメント	一般的な組織であれば「情報セキュリティポリシー」などの名称で、代表取締役名でWebサイトなどで公表されており、左記項目も一般的に入っていることから特に改めての対応は不要となります。（※法規制などが変わった際は更新が必要な点は注意となります）	対象外となります。 ※組織全体のポリシーであり、個別サービスに言及することはないため
	②	基本的な対応事項	取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、組織の経営目標にとってのサイバーセキュリティの確保の重要性を認識し、関係主体等からの要求事項や、法規制等の内外環境を踏まえ、必要なサイバーセキュリティ管理態勢を整備すること。また、サイバーセキュリティ管理態勢について少なくとも１年に１回レビューを行うなどにより、十分な検証、議論を行うこと（必要に応じ、外部専門家によるレビューを含む）。	何をもって十分な検証、議論が行われたかを判断することは難しいですが、一般的には ①経営目標にサイバーセキュリティの要素が入っている ②要求事項、法規制等を考慮した組織のセキュリティガイドラインが年次で見直しが行われている ③それらを独立した部署でチェックがしている 点がポイントとなります。 ②についてはFISC、日銀、金融庁から出されているガイドラインなどをベースに検討する必要があります。（※他NISTなど海外のドキュメントもありますが、先に挙げた３つの組織のガイドラインはNISTの各種ドキュメントをベースにして作成されている部分が多く、時間の余裕があるか、海外拠点を多く持つ組織でなければ優先度は相対的に低くなります）	対象外となります。 ※組織全体のポリシーであり、個別サービスに言及することはないため
2.1.2			規程等及び業務プロセスの整備		
	①	基本的な対応事項	経営陣は、サイバーセキュリティに係る規程及び業務プロセスを整備し、少なくとも１年に１回見直しを行うこと。サイバーセキュリティに係る規程等には、例えば以下の事項を含めること。 ・情報資産管理 ・リスク評価 ・脆弱性管理 ・脆弱性診断及びペネトレーションテスト（侵入テスト） ・演習・訓練 ・認証・アクセス管理 ・教育・研修 ・データ管理 ・ログ管理 ・セキュリティ・バイ・デザイン ・技術的対策（物理的セキュリティ、ネットワークセキュリティ等） ・インシデント対応及び復旧 ・サードパーティリスク管理	一般的な組織では「情報セキュリティスタンダード」などといったFISC安対基準や金融庁から出ているドキュメントなどを参考にした組織としての上位文書が存在しており、当該文書の承認者を経営陣とすることで左記事項は対応できます。各金融機関で利用している当該上位文書は金融系に強いコンサルタント会社で作っていることが多く、左記項目は入っている可能性が高いものの、「セキュリティ・バイ・デザイン」と「サードパーティリスク管理」の２点はここ最近重要視されてきたものであるため、もし入っていない場合はNISCの政府統一基準令和５年度版がインターネットで一般公開されており、当該項目があるので自組織のみでも反映することが可能となります。 また定期的な見直しが求められますがセキュリティの業務は年[illegible]低限１[illegible]更新が必[illegible]プロセス[illegible]	対象外となります。 ※組織全体のポリシーであり、個別サービスに言及することはないため
2.3.			サイバー攻撃の防御		
	①	基本的な対応事項	サイバー攻撃に備え、不正侵入を防止するための境界ネットワーク対策、内部ネットワークでのシステム不正利用を防止するための対策、外部への情報漏洩対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じること。	入口対策・内部対策・出口対策の３つの対策による組み合わせの要件が求められています。 境界ネットワーク対策で主に侵入を防ぐ入口対策が主になっていることが多いものの、内部対策であればEDRの導入やコアスイッチに近いところでパケットの異常値を検出するツール類の導入、出口策であればProxyを使っている組織であれば分類noneのものをブロックする、IPでの通信を許可しないなどの対策が[illegible]	当社設計においてはAWS WAF、SecurityGroup、NACLなどノード単位で必要となるIP/Port番号による最小のアクセスとなるように設計を行います。 またマルウェア感染や改ざんに備え、CloudOneというホスト型IPSの導入を推奨しており、お客様と相談の上導入させていただ[illegible]
2.3.1			認証・アクセス管理		
	①	基本的な対応事項	認証及びアクセス権の付与に係る方針及び規程等を策定し、定期的に見直すこと。 当該規程等には、以下の観点を含めること。 ・ユーザ（システムを含む）のアクセス権限を必要最小限に制限し、職務の分離を考慮すること。 ・アカウントのライフサイクル（作成、使用、終了）を管理し、アカウントの定期的な棚卸しや操作履歴のレビューを実施し、無権限者によるアカウントの不正使用を防止すること。 ・特権アカウントの利用を厳格に制限し、管理すること（多要素認証、操作のダブルチェック、アカウントの時間制限の設定等）。 ・外部委託先によるアクセス権の利用を適切に管理すること。	一般的な組織であればすでに定まっている規程であり特に目新しさはないものとなります。 項目の中で多要素認証の箇所は昨今はクラウドサービス関連であればほぼ実装されていることから、インターネット経由でアクセス可能なクラウドサービスは多要素認証必須など、条件を定義した規定類になっているか確認する必要があります。	当社設計では多要素認証必須、特権アカウントの厳密な管理を実施しており、AWSのPartnerとして受検するAWSの監査においても厳密に実施しております。 基本的にはアカウント管理はお客様のポリシーで規定されている以上に厳密な設計となっておりますが、ポリシーと齟齬がある場合は別途設計の中で対応いたします。
	②	基本的な対応事項	システムへのアクセス権限は、正当な業務上の要請があり、承認され、適切に教育・研修を受け、管理されている個人に対してのみ付与すること。また、ユーザによる機器及びシステムへのアクセス権限は、システムや情報の重要度を考慮して付与すること。	多くの組織で委託業者含めてセキュリティ教育など基本的な教育を実施し、その結果を残した上で作業する規程になっていることが多くなっているものと思われます。 一方、特にオンプレ環境ではアカウントが共通的なものになっている場合があり、個人単位で作れない場合もありますが、そのアカウントが特定の時間誰が使ったかをきちんと記録を残していること、アクセス権限においても厳密になっていない場合はどういった代替手段で実現しているか確認する必要があります。	当社においてもお客様の環境を触る前には必ず当社内の教育を受検後にアカウントを個人単位で割り振りを行っております。 また、アクセス権限も作業承認後都度付与しており、作業終了時にアクセス権限の解除含めてルール化されております。
	③	基本的な対応事項	機器（APIに認証情報を組み込むことを含む）及びユーザのID及び認証情報を適切に管理すること（初期設定されたパスワードの変更、パスワード強度の要件、IDの自動失効、システム責任者による定期的なアクセスレビュー等）。	多くの組織で初期アカウントの利用禁止、初期パスワードの強制リセットのルールがあり、定期的なアクセスレビューもルール化されているものとなります。 一方、クラウド環境の増加に伴い対話型ログオンではない、APIで使う認証情報の管理がルール化されていないケースがあります。 本認証情報漏洩時にはクラウドのリソースを無断で利用されてしまい仮想通貨の発掘などで大量の課金となる場合があるため、規定しておくことをおすすめします。	当社においてもAWS環境で発行いただいたものを組み込むケースがありますがAWS環境上で完結するようにしており、PC上での管理はしないように徹底しております。
	④	基本的な対応事項	IDを認証し、システムへのアクセスを許可する前にユーザのアクセス権限の適切性を検証すること。また、アクセスしたユーザを特定できる措置を講じ、処理内容をログに記録し、ユーザの操作内容と対応させること。	本項目では基本的には個人単位で振られたアカウントが存在し、人が特定できることが望ましいものの、仕組み上個人単位で付与されないアカウントの場合であっても記録を残す手段を求めています（※例えば本番アカウントの利用申請などで利用者が特定できる状態になっているなど）。 またクラウドサービスなどではすべてのログがテキスト化され残ることが一般的にはなってきたものの、オンプレではイベントログだけでは操作が追えないこともあるため、作業の重要性などに応じて操作を録画する製品などでログを記録する必要があります。	AWS上の機能で必ずアクセス許可前に適切性の検証が行われた上で、AWS上での操作は全てログに記録され改ざん不可能な形で保存されます。
	⑤	基本的な対応事項	システムや情報の重要度に応じて、認証要件（多要素認証、リスクベース認証等、認証時におけるリスク低減策等）を決定すること。特に、重要なシステムへのリモートアクセスには、多要素認証を使用すること。	クラウドサービスにおいては多要素認証が一般的となってきたものの、オンプレシステムでは必ずしも多要素認証が実装できないケースがあります。 専用線接続や送信元IPなど厳密には多要素認証にはならないものもありますが、ID/Passwordのみで重要システムのリモートアクセスができないような制御を検討する必要があります。	当社設計においては重要なアカウントは必ず多要素認証を設定し、お客様との合意次第ではありますが基本的にはすべてのアカウントに多要素認証を強制させる設定をしております。
	⑥	基本的な対応事項	第三者による不正行為を阻止するための仕組みや取組みを活用すること（メールの送信ドメイン認証（SPF/DKIM/DMARC）、安全なファイル交換機能、顧客へのサポートと啓発活動（注意喚起やセミナー）等）。	当局からの要請事項にもなっているDMARCの実装は勿論のこと、DMARCのアクションをquarantine以上にあげること、ZIP暗号化ではなくメールサーバー間の暗号化やファイルストレージ、ならびに公式アカウントにはS/MIMEを使うなどを検討する必要があります。	AWSのSESというメールサービスを使う場合はSPF/DKIMの設定を行わせていただいております。 DMARCはドメイン単位でかかることから当社単独での設定にはならないことから、お客様と相談の上決定させていただいております。

AWSに関係のない項目であっても、お客様に理解いただけるように、解説をしております。

当社に関係のある個所はどのように実現できるか実装などを記載させていただいております。