『FFIEC Cybersecurity Assessment Tool に関する調査研究』

調査報告書

2016 年 3 月 31 日

株式会社 NTTデータ 経営研究所

目次

I. Cybersecurity Assessment Tool の概要 1
1. アセスメントツール提供の背景と目的 1
2. 概要 2
3. 第 1 部：固有リスクプロファイルの識別 6
(1) 固有リスクプロファイル識別のカテゴリ 6
(2) 固有リスクのレベル 8
(3) 固有リスクプロファイルの判断 9
4. 第 2 部：サイバーセキュリティの成熟度 30
(1) サイバーセキュリティの成熟度 32
(2) サイバーセキュリティ成熟度評価の実施 34
II. 国内金融機関へあてはめる際の課題 97
1. アセスメントツールの位置付け 97
2. アセスメントツールの活用の在り方 99
(1) 評価から対策検討へのスムースな移行メカニズムを実装すること 99
(2) 成熟度レベル判定ロジックの柔軟な設定 100
3. 評価項目や数値基準の在り方 100
(1) 理解しやすい評価項目の定義 100
(2) ベンダーとの関係やシステム等の環境の違いを反映した
評価基準等の妥当性の確保 101
(3) IT ベンダーを巻き込んだ検討 102
4. サイバーセキュリティの対応態勢 103
III. まとめ 105

I. Cybersecurity Assessment Tool の概要

1. アセスメントツール提供の背景と目的

情報技術（IT）の普及とともにサイバー攻撃の脅威も増加しており、サイバー攻撃に対する認識は国家レベルで高まっていることを受け、米国では 2013 年 2 月に「重要インフラのサイバーセキュリティ強化に関する大統領令（第 13636 号)」が発令された。これを受けて、2014 年 2 月に米国国立標準技術研究所（以下、NIST）が「重要インフラのサイバーセキュリティを強化するフレームワーク」[1]を発表している。サイバー攻撃の増加を受け、米国金融機関ではサイバーセキュリティ対策への投資額も年々増加しており、例えば、JP モルガンチェースでは 2016 年度予算として 2014 年度の倍にあたる 5 億ドルを予算計上している[2]。

Cybersecurity Assessment Tool（以下、「アセスメントツール」）は米国連邦金融機関検査協議会（以下、FFIEC）が、サイバー攻撃の脅威の拡大と高度化の一途を辿っている現状を受け、金融機関が自組織におけるリスクの識別とサイバーセキュリティの成熟度レベルを評価するために 2015 年 6 月に公表したものである。このアセスメントツールは 2014 年に FFIEC が各地域組織のサイバーリスクを低減するために試験的に実施したサイバーセキュリティ評価に基づいて設計されており、FFIEC の情報技術(IT)検査ハンドブック（以下、「IT ハンドブック」）の指針や上述の NIST のサイバーセキュリティフレームワークのほか、業界で受け入れられているサイバーセキュリティの実務に整合している。また、金融機関がアセスメントツールを用いた評価を実施しやすいよう、金融サービス情報共有分析センター(以下、FS-ISAC)と米国金融サービスセクター連携協議会（以下、FSSCC）は FSSCC Automated Cybersecurity Assessment Tool(以下、FSSCC ツール)を共同開発し、2015 年 12 月に公表[3]している。

最近大きな注目を集めたサイバー攻撃の例を見ると、サイバーインシデントによって、企業の資本や利益に大きな影響が及ぶことがわかる。そのコストには、電子機器に残る記録を収集・分析するデジタルフォレンジック調査や広報活動、訴訟費用、消費者の信用状況調査、およびテクノロジーの変更などが含まれるため、サイバーセキュリティは、その組織全体で全社的なガバナンスプロセス、情報セキュリティ、事業継続性および第三者のリスク管理の一部として統合される必要がある。このアセスメントツールは、その組織が保有するサイバーセキュリティの固有リスクプロファイルの識別と、その組織のサイバーセキュリティ対策の対応状況がどの段階にあるかを表すサイバーセキュリティ成熟度を測定し、商品やサービス提供の開始時等に繰り返しサイバーセキュリティ対

[1]http://www.nist.gov/cyberframework/
[2]http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#720334ad1112
[3]https://www.fsisac.com/article/fssc-automated-cybersecurity-assessment-tool

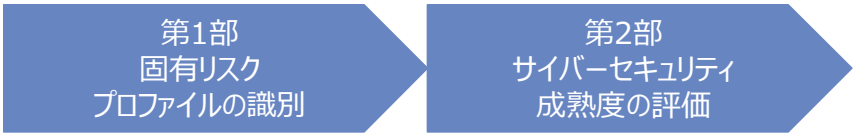
策の対応状況を評価できるように設計されている。これを受けて、米国の多くの金融機関はこのアセスメントツールを活用して、自己評価を始めている。

こうした中、2015 年 7 月に米国連邦準備制度理事会（以下、FRB）は、FFIEC からアセスメントツールが提供されたこと、2015 年後半から 2016 年初めにかけて実施を予定している金融機関のサイバーセキュリティへの備えを評価する際に、レビュープロセスの一環として金融機関が実施したアセスメントツールを用いた評価結果の利用を計画していると通達[4]を発出した。同様に、米国通貨監督庁（以下、OCC）も通達[5]を発出しており、金融機関のサイバーセキュリティへの取組みを評価するプロセスの一部として活用することを表明している。

2. 概要

前述のとおり、アセスメントツールは、固有リスクプロファイルの識別とサイバーセキュリティ成熟度の評価の 2 部構成になっている。このプロセスは、各組織のリスク管理プロセスおよびサイバーセキュリティプログラムを置き換えるのではなく、補完することを目的としている。

図表 I-1　アセスメントツールの構成



出典：アセスメントツールを基に NTT データ経営研究所にて作成

第 1 部の固有リスクプロファイルの識別では、自組織のサイバーリスク関連の固有リスクを 5 つのカテゴリ(**図表 I-2**)に基づいて識別する。具体的には、各金融機関が取り扱っている商品・サービスのラインナップ、販売チャネルや態勢などから、自組織がどの程度のリスクに晒されているかを 5 段階で評価する。大多数が同様のリスクレベルに評価される場合、そのリスクレベルが組織全体の固有リスクとなる。しかし、組織全体の固有リスクよりも上位の固有リスクレベルと評価されるカテゴリは、追加リスクとして考慮しておく必要がある。

第 2 部はサイバーセキュリティ成熟度の評価となっており、次の 5 つの領域(**図表 I-3**)における、その組織のサイバーセキュリティ対策の対応状況を評価する。サイバーリスクの管理と監督、脅威情報の収集と共有、サイバーセキュリティ統制等の 5 つの領域毎

[4]http://www.federalreserve.gov/bankinforeg/srletters/sr1509.htm
[5]http://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html

に、取組みの有無を確認することで、第 1 部の固有リスクプロファイルの識別と同様、5 段階で規定された成熟度として評価する。そのため、領域によって異なる成熟度レベルに評価される場合がある。

各カテゴリにおける自組織の固有リスクプロファイルと各領域における成熟度レベルの両方を確認することにより、経営陣は成熟度レベルがリスクとの関連で適切であるかどうかを判断する。評価単位は、**図表 I-2** に記載のカテゴリ毎及び**図表 I-3** の領域毎に実施される。金融機関が上述の評価作業を効率的に実施するため、アセスメントツールの内容が Excel 形式に整理された FSSCC ツールが FS-ISAC から公表[3]されている。

図表 I-2　固有リスクプロファイル識別のカテゴリと評価軸

カテゴリ	評価軸
テクノロジーと接続タイプ	• インターネットサービスプロバイダーの接続数 • セキュリティ対策が施されていない外部接続先数 • 無線ネットワークアクセス • 社内ネットワークへの接続が認められている個人所有機器 • 社内システムへのアクセス権限を持つ第三者の数 • 専用線接続の大口顧客 • 社内で構築、開発、変更を行う重要業務のアプリケーション数 • 社内で構築し、ベンダーが開発する重要業務のアプリケーション数 • 重要業務に係わるユーザー部門が開発した技術やツール数 • エンドオブライフ(EOL)システム • オープンソースソフトウェア(OSS) • ネットワーク機器 • 重要業務を支えている第三者の数 • 重要業務に係わる外部ホストのクラウドサービス
販売チャネル	• オンラインでの顧客向け事業展開 • モバイルでの事業展開 • ATM の運用状況
オンライン商品/モバイル商品とテクノロジーサービス	• デビットカード/クレジットカードの発行 • プリペイドカード

カテゴリ	評価軸
	• エマージング決済テクノロジー • 個人間決済(P2P) • ACH（Automated Clearing House）決済の仕向取引 • 大口決済 • 電信振込 • 加盟店リモートデポジットキャプチャー • 財務サービスとクライアント数 • 信託サービス • コルレス銀行としての機能 • 加盟店アクワイアラー • 他組織向けのホスティングサービス
組織的特徴	• 合併および買収 • 直接雇用の従業員 • IT および情報セキュリティ人材の配置における変更 • 特権的アクセス権限 • IT 環境の変更 • 支店/事業拠点の所在地 • 運用センター/データセンターの所在地
外部の脅威	• 試行されたサイバー攻撃数

出典：アセスメントツールを基に NTT データ経営研究所にて作成

図表 I-3　サイバーセキュリティ成熟度評価の領域と評価要素

領域	評価要素
領域 1：サイバーリスクの管理と監督	• ガバナンス • リスク管理 • リソース • 研修と企業文化
領域 2：脅威情報の収集と共有	• 脅威情報 • モニタリングと分析 • 情報共有
領域 3：サイバーセキュリティ統制	• 防御 • 検知

	• 改善
領域 4：外部依存関係の管理	• 外部との接続 • 関係管理
領域 5：サイバーインシデント管理とレジリエンス	• インシデントレジリエンスに関する計画策定と戦略 • 検知、対応および低減 • エスカレーションと報告

出典：アセスメントツールを基に NTT データ経営研究所にて作成

図表 I-4 は組織の固有リスクプロファイルとその領域の成熟度レベルの関係を示したものである。一般的に、固有リスクが増大すれば、その組織の成熟度レベルも引上げる必要がある。しかし、固有リスクレベル毎に求められる成熟度レベルは 1 つではなく、自組織の置かれている環境や事業目標などによって選択できる余地（例えば固有リスクレベルが最小であれば、ベースラインまたは進化途上の成熟度レベルを選択できる）が残されている。

図表 I-4　リスクと成熟度の関係

リスク/成熟度の関係		**固有リスクレベル** →				
		最小	軽微	中程度	重大	極めて重大
各領域のサイバーセキュリティ成熟度レベル ↑	革新 (Innovative)				■	■
	高度 (Advanced)			■	■	■
	中程度 (Intermediate)		■	■	■	
	進化途上 (Evolving)	■	■	■		
	ベースライン (Baseline)	■	■			

出典：アセスメントツール p.9

組織の固有リスクプロファイルと成熟度レベルは、サイバー攻撃の脅威、脆弱性および事業環境の変化に伴い、時間の経過とともに変化する。そのため、経営陣は定期的、もしくは、計画された変更が固有リスクプロファイルに影響を及ぼす可能性がある場合に、自組織の固有リスクプロファイルとサイバーセキュリティ成熟度を評価し直す必要がある。例えば、新商品またはサービスの新規取扱や外部接続先が増える場合には、固有リスクレベルが 1 段階上昇する可能性を認識しなければならない。

また、組織の成熟度が固有リスクプロファイルに適合していないと経営陣が判断した

場合、例えば、

① 商品またはサービスの提供の制限や提供チャネルの制限等により固有リスクレベルを低減させる

② 内部ルールの強化やツールの導入等により成熟度レベルを向上させる

のいずれかの施策を講じる必要がある。

さらに、経営陣は、その組織の事業目標およびリスクアペタイトに基づいて、各領域または全領域の目標とする成熟度レベルを設定した上で、現在の成熟度レベルと目標とする成熟度レベルのギャップ分析を行い、そのギャップに基づく改善を行うべきである。

このように、各領域の成熟度レベルを把握することにより、経営陣は自組織の全体的なサイバーセキュリティ対策を向上するために講ずべき施策を峻別できる。つまり、経営陣は、自組織が達成している上位の成熟度レベルに記載されている評価項目を確認することにより、次の成熟度レベルを達成するために必要なギャップを把握し、どのような施策を講ずるべきか認識することができる。さらに、自組織のアセスメントプロセスやサイバーセキュリティ対策の対応状況について、独立した社内の監査部門などに検証を要請することも可能となる。

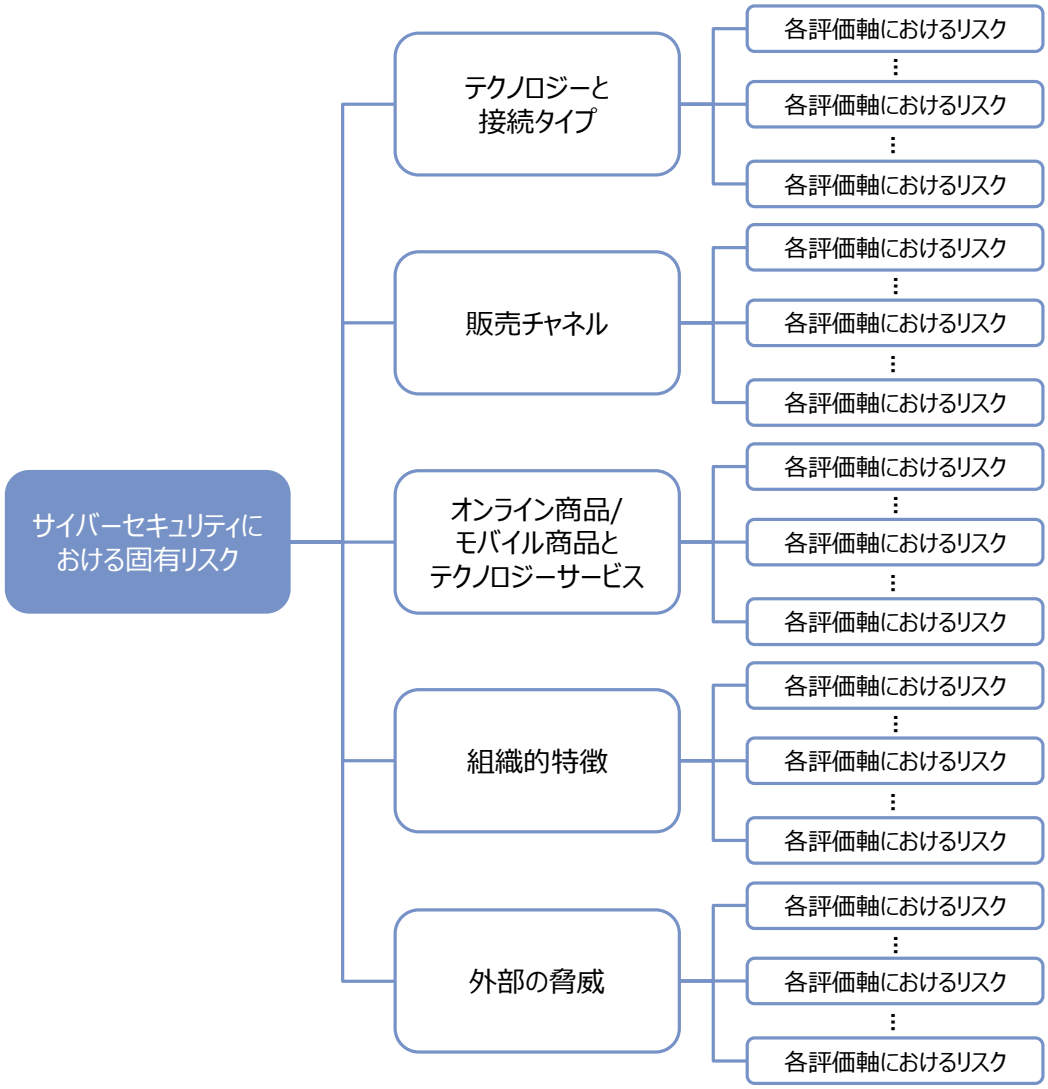
3. 第 1 部:固有リスクプロファイルの識別

アセスメントツールの第 1 部では、固有リスクを業務、サービス、商品のカテゴリに体系化した上で識別する。固有リスクには、各組織の業種や事業の規模、利用しているテクノロジー等の複雑性やその組織に対する脅威が評価に組み込まれる。

(1) 固有リスクプロファイル識別のカテゴリ

サイバーセキュリティの固有リスクとは、次の 5 つのカテゴリでそれぞれに生じるリスクのことを指し、カテゴリごとに固有リスクが異なる場合があり得る。

図表 I-5　各カテゴリでの固有リスクの識別



出典：アセスメントツールを基に NTT データ経営研究所にて作成

- **テクノロジーと接続タイプ:** ある種類の接続やテクノロジーを用いている場合、特定のテクノロジーを用いた商品およびサービスの複雑性、成熟度、外部接続のあり方や商品及びサービス自体の性質に応じて、高い固有リスクを生じさせる。このカテゴリには、インターネットサービスプロバイダー（ISP）の数、第三者との接続、システムが金融機関内でホストされているか（または外注されているか）、セキュリティ対策が施されていない接続、無線アクセスの利用、ネットワーク機器の数、エンドオブライフ（サポートが終了した）システム、クラウドサービスの利用範囲、個人所有機器の利用が含まれる。
- **販売チャネル:** 提供される特定の商品またはサービスの性質に応じて、それらを提供

するための多様な販売チャネルが高い固有リスクを生じさせる。固有リスクは、販売チャネルの多様性や数が増えるにつれて増大する。このカテゴリには、オンラインおよびモバイル販売チャネルを通じた販売の有無、および現金自動預入支払機（ATM）の運用の程度も評価の対象。

- **オンライン商品/モバイル商品とテクノロジーサービス:** 提供されている特定の商品またはサービスの性質に応じて、各組織が提供しているさまざまな商品およびテクノロジーサービスが高い固有リスクを生じさせる。このカテゴリには、デビットおよびクレジットカード、個人間決済（P2P）、ACH（Automated Clearing House）、小口電信送金、大口決済、加盟店リモートデポジットキャプチャー、財務サービスとクライアント数、信託サービス、各種決済サービス、国際送金、コルレス銀行業務、加盟店アクワイヤリング（契約）業務が含まれる。また、このカテゴリには、他金融機関へのテクノロジーサービスの提供の有無も含まれる。
- **組織的特徴:** このカテゴリでは、合併および買収、直接雇用の従業員とサイバーセキュリティ請負業者、セキュリティ人員の配置の変更、特権的アクセス権を持つユーザーの数、情報技術（IT）環境の変更、事業拠点の所在地、運用センター/データセンターの所在地など組織的特徴を考慮。
- **外部の脅威:** サイバー攻撃（試行または成功）の規模とタイプは、組織の固有リスクエクスポージャーに影響。このカテゴリでは、その組織を標的にしている攻撃の規模と巧妙さを考慮。

（2）固有リスクのレベル

リスクレベルは、「最小の固有リスク」から「極めて重大な固有リスク」までの 5 段階で定義されている。カテゴリごとに固有リスクを判定するためのパラメータが提供されており、業務、サービス、または商品に対して最も適切なリスクレベルを選択する。これらのパラメータは、厳格にあてはめるものではなく、各業務活動、サービス、または商品のリスクレベルの一助とするための示唆的なものである。ただし、リスクレベルが 2 つのレベルの中間に位置する場合には、経営陣は高い方のリスクレベルを選択しなければならない。

図表 I-6　5 段階で定義された固有リスクレベル

出典：アセスメントツールを基に NTT データ経営研究所にて作成

（3）固有リスクプロファイルの判断

経営陣は、すべての業務活動において各リスクレベルにあてはまる項目に基づき、自組織全体の固有リスクプロファイルを判定する。例えば、大部分の業務活動、商品またはサービスが中程度の固有リスクに該当する場合、経営陣は、自組織は中程度の固有リスクプロファイルを持っていると判定できる。ただし、各カテゴリで、異なるレベルの固有リスクが生じている場合、経営陣は全体の固有リスクとして判定したリスクレベルの評価に加え、特定のカテゴリにおける追加リスクの発生有無を評価しなければならない。

リスクレベルの定義は以下のとおりである。

- **最小の固有リスク:**全般的に非常に限られた範囲でのみテクノロジーを利用。コンピューター、アプリケーション、システムも少なく、外部との接続もない。商品やサービスの多様性も限られている。この組織は、拠点も小規模で従業員数も少数。
- **軽微な固有リスク:**全般的に利用しているテクノロジーの観点から、複雑性が限定されている。この組織は、多様性が限られた、リスクの低い商品やサービスを提供。ミッションクリティカル（業務の遂行に必要不可欠）なシステムは、外部に委託。この組織は、主に既に実証されて定評のあるテクノロジーを利用。顧客および第三者に対して、限られた複雑性を持つ少ない種類の外部との接続を維持。
- **中程度の固有リスク:**全般的に規模と複雑性の観点から、利用しているテクノロジーは幾分複雑。この組織は、ミッションクリティカルなシステムやアプリケーションを外部委託しており、設備の一部の構成要素のみを社内でサポート。また、比較的多様な商品やサービスを多様なチャネルで提供。
- **重大な固有リスク:**全般的に範囲と複雑性の観点から複雑なテクノロジーを利用。この組織は、リスクの高い商品やサービスを提供しており、その中には、エマージングテクノロジーが含まれている場合もある。また、社内で数多くのアプリケーションをホストしていることもある。この組織は、多数の個人所有の機器または多種多様な機器のいずれの使用を認めている。この組織は、顧客および第三者に対してかなりの数を接続。さまざまな決済サービスが第三者を通さずに直接提供されており、取引量は高水準。
- **極めて重大な固有リスク:**非常に複雑なテクノロジーを利用して、多種多様な商品やサービスを数多く販売。他の組織に提供されているものも含め、多くの商品およびサービスには高いレベルのリスク。多数の販売チャネルで新しいエマージングテクノロジーを利用。この組織は、一部のミッションクリティカルなシステムまたはアプリケーションを外部委託している場合があるが、多くのシステムやアプリケーションは社内でホスト。顧客や第三者とのデータ伝送のために多数の接続を維持。

図表 I-7　固有リスクレベルとレベルの評価軸

レベルの評価軸 / 固有リスクのレベル	テクノロジー	商品やサービス	接続
最小の固有リスク	• 限られた範囲で利用されている	• 多様性が限定的である	• 外部接続がない
軽微な固有リスク	• 利用しているが複雑性は限定的である	• 多様性が限定的であり、商品性のリスクも低い	• 業務上必要不可欠なシステムを外部委託している
中程度の固有リスク	• 利用しているものは複雑である場合がある	• 商品性は多様であり、多様なチャネルで提供している	• 業務上必要不可欠なシステムやアプリケーションを外部委託している
重大な固有リスク	• 利用しているものは複雑である	• リスクの高い商品やサービスを提供している	• 顧客および第三者に対してかなりの数の接続を維持している
極めて重大な固有リスク	• 非常に複雑なものを利用している	• 多種多様な商品サービスを数多く販売し、多くの商品サービスのリスクが高い	• 多くのシステムやアプリケーションは社内でホストし、顧客や第三者と多数の接続を維持している

出典：アセスメントツールを基に NTT データ経営研究所にて作成

固有リスクプロファイルは以下のとおり。

図表 I-8　固有リスクプロファイル

カテゴリ：テクノロジーと接続タイプ

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
インターネットサービスプロバイダー（ISP）の接続の総数（支店の接続も含む）	接続なし	複雑性が低い（1～20の接続数）	複雑性は中程度（21～100の接続数）	複雑性が高い（101～200の接続数）	複雑性が極めて高い（200を越える接続数）	△ IPS接続数の妥当性を検証する必要がある。
セキュリティ対策が施されていない外部接続先数（ユーザーの数ではない）（例: ファイル転送プロトコル（FTP）、Telnet（テルネット）、rlogin（リモートログイン））	なし	セキュリティ対策が施されていない外部接続はほとんどない（1～5件）	セキュリティ対策が施されていない外部接続がいくつかある（6～10件）	セキュリティ対策が施されていない外部接続が相当数ある（11～25件）	セキュリティ対策が施されていない外部接続がかなり多い（25件超）	△ 外部接続数の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
無線ネットワークアクセス	無線アクセスはない	ゲスト用無線と社内無線は、別個のアクセスポイントで用意されている	ゲストと社内の無線ネットワークアクセスは論理的に分離されており、ユーザーとアクセスポイントの数は限られている（ユーザー: 1～250、アクセスポイント: 1～25カ所）	無線による社内ネットワークへのアクセスがある。ユーザーとアクセスポイントの数が相当数ある（ユーザー: 251～1,000名超、アクセスポイント:26～100カ所）	無線による社内ネットワークへのアクセスがある。すべての従業員がアクセスでき、アクセスポイントの数がかなり多い（ユーザー: 1,000名超、アクセスポイント: 100カ所超）	○
社内ネットワークへの接続が認められている個人所有機器	なし	1種類の機器のみを利用可能。5%未満の従業員（社員、役員、管理者）および取締役が利用可能。Eメールにのみアクセス可能	複数の種類の機器が使用されている。10%未満の従業員（社員、役員、管理者）および取締役が利用可能。Eメールにのみアクセス可能	複数の種類の機器が使用されている。25%未満の許可された従業員（社員、役員、管理者）および取締役が利用可能。Eメールと一部のアプリケーションにアクセス可能	機器の種類を問わず使用されている。25%を越える従業員（社員、役員、管理者）および取締役が利用可能。すべてのアプリケーションにアクセス可能	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
社内システム（例：仮想プライベートネットワーク、モデム、イントラネット、直接接続）へのアクセス権を持つ第三者の数（外部企業の数およびベンダーや下請業者から派遣された個人の数を含む）	システムへのアクセス権を持つ第三者または第三者から派遣された個人はいない	限られた数の第三者（1～5社）と第三者から派遣された個人（50名未満）がアクセス権を持っている。社内システムへのアクセス方法の複雑性は低い	中程度の数の第三者（6～10社）と第三者から派遣された個人（50～500名）がアクセス権を持っている。社内システムへのアクセス方法にはある程度の複雑性がある	相当数の第三者（11～25社）と第三者から派遣された個人（501～1,500名）がアクセス権を持っている。社内システムへのアクセス方法にはある程度の高い複雑性がある	かなり多くの第三者（25社超）と第三者から派遣された個人（1,500名超）がアクセス権を持っている。社内システムへのアクセス方法の複雑性は高い	○
専用接続を持つ大口顧客	なし	専用接続は少ない（1～5）	いくつかの専用接続がある（6～10）	相当数の専用接続がある（11～25）	かなり多くの専用接続がある（25超）	△ 接続数の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
重要な業務活動をサポートしている、社内でホスト、開発または変更されるベンダーアプリケーションの数	なし	少しある（1～5）	いくつかある（6～10）	相当数ある（11～25）	かなりの数のアプリケーションがある（25超）。 複雑性も高い	△ アプリケーション数の数え方の定義が必要、かつ、アプリケーション数の妥当性を検証する必要がある。
重要な業務活動を支えている、社内でホストされているベンダーが開発したアプリケーションの数	数は限られている（0～5）	少しある（6～30）	いくつかある（31～75）	相当数ある（76～200）	かなりの数のアプリケーションがある（200超）。 複雑性も高い	△ アプリケーション数の数え方の定義が必要、かつ、アプリケーション数の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
重要な業務活動を支えている、ユーザーが開発したテクノロジーやユーザーコンピューティング（Microsoft Excelスプレッドシートやアクセスデータベース、またはその他のユーザーが開発したツールを含む）	ユーザーが開発したツールはない	1～100のツール	101～500のツール	501～2,500のツール	2,500超のツール	○
エンドオブライフ（EOL）システム	EOLを過ぎているシステムまたは2年以内にEOLになるおそれがあるシステムはない	2年以内にEOLになるおそれがあるシステムは少しあるが、重要な業務を支えてはいない	2年以内にEOLになる、重要な業務を支えているシステムがいくつかある	重要な業務を支えている多数のシステムがEOLであるか、2年以内にEOLになるおそれがある	大部分の重要な業務がEOLに到達しているか、今後2年以内にEOLになるシステムに依存している。あるいはEOLに到達しているシステムの数は不明	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
オープンソースソフトウェア（OSS）	OSSはない	重要な業務を支えているOSSはない、もしくは数が限られている	重要な業務を支えているOSSがいくつかある	重要な業務を支えているOSSが多数ある	大部分の業務がOSSに依存している	△ OSSの定義を検証する必要がある。
ネットワーク機器（例：物理および仮想を含むサービス、ルーター、ファイアウォール）	ネットワーク機器の数はないか、数が限られている	ネットワーク機器は少しある（250～1,500）	ネットワーク機器はいくつかある（1,501～25,000）	ネットワーク機器は相当数ある（25,001～50,000）	ネットワーク機器はかなり多い（50,000超）	○
重要業務を支えている第三者（社内システムへのアクセス権限はないが、組織は同社のサービスに依存している）	重要な業務活動を支えている第三者はない	重要な業務活動を支えている第三者は1～25社ある	重要な業務活動を支えている第三者は26～100社ある	重要な業務活動を支えている第三者は101～200社あり、1社以上は外資系である	重要な業務活動を支えている第三者は200社超あり、1社以上は外資系である	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
重要業務に係わる外部ホストのクラウドサービス	クラウドのプロバイダーは利用していない	利用しているクラウドのプロバイダーは少ない。プライベートクラウドのみ（1～3 社）	利用しているクラウドのプロバイダーは何社かある（4～7 社）	利用しているクラウドのプロバイダーは相当数ある（8～10社）。使用しているクラウドプロバイダーの所在地は、海外も含まれる。パブリッククラウドを使用している	利用しているクラウドのプロバイダーはかなり多い（10社超）。使用しているクラウドプロバイダーの所在地は海外を含む。パブリッククラウドを使用している	△ クラウドサービスの利用実態について検証が必要である。クラウドサービス利用数の妥当性を検証する必要がある。

カテゴリ：販売チャネル

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
オンラインでの顧客向け事業展開	Web 向けアプリケーションまたはソーシャルメディアはない	情報提供のための Web サイトまたはソーシャルメディアページとして機能している（例：支店および ATM の所在地および販促資料を提供）	小口のオンラインバンキングの販売チャネルとして機能している。ソーシャルメディアを通じて顧客に情報を伝えることがある	大口顧客向けの販売チャネルとして機能している。小口口座を基にした取引が含まれることもある	インターネットアプリケーションが高額の資産を管理するための大口顧客向けのチャネルとして機能している	○
モバイルでの事業展開	なし	SMS でのテキストアラートまたは通知のみ。ブラウザでのアクセスが基本	小口顧客向けモバイルバンキングアプリケーション（例：請求書支払、モバイルでの小切手キャプチャー、その金融機関内の口座間振込のみ）	外部金融機関への振込を含むモバイルバンキングアプリケーション（例：法人顧客向け、繰り返し行う外部との取引）	新しい取引の送信（例：ACH、電信）を含む全機能	△ 国内金融機関におけるモバイル事業に照らして、再定義する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
現金自動預入支払機（ATM）（運用）	ATM サービスは提供していない	ATM サービスは提供しているが、機械は所有していない	ATM サービスは、第三者によって管理されている。ATM は、地方または地域の支店にある。現金補填サービスは外部に委託されている	ATMサービスは、社内で管理している。ATMは、米国の各支店および小売店の所在地に設置されている。現金補填サービスは、外部に委託されている	ATMサービスは、社内で管理している。ATMサービスは、他の金融機関に提供されている。国内および海外の支店および小売店の所在地にATMがある。現金補填サービスは社内で管理している	◯

カテゴリ：オンライン商品/モバイル商品とテクノロジーサービス

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
デビットカード/クレジットカードの発行	デビットカードまたはクレジットカードは発行していない	デビットカードまたはクレジットカードあるいはその両方を第三者経由で発行している。カードの発行済み枚数は、10,000 枚未満	デビットカードまたはクレジットカードを第三者経由で発行している。カードの発行済み枚数は、10,000～50,000 枚	デビットカードまたはクレジットカードを直接発行している。カードの発行済み枚数は、50,000～ 100,000枚	デビットカードまたはクレジットカードを直接発行している。カードの発行済み枚数は、100,000枚超。 他の金融機関からカード発行を受託している	△ カード種別ごとに項目を分解し定義する必要がある。カード発行枚数の妥当性を検証する必要がある。
プリペイドカード	プリペイドカードは発行していない	プリペイドカードを第三者経由で発行している。カードの発行済み枚数は、5,000 枚未満	プリペイドカードを第三者経由で発行している。カードの発行済み枚数は、5,000～10,000 枚	プリペイドカードを第三者経由で発行している。カードの発行済み枚数は、10,001～20,000枚	プリペイドカードを社内で、または他の金融機関に代わって発行している。カードの発行済み枚数は、20,000 枚超	△ カード発行枚数の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
エマージング決済テクノロジー（例：デジタルウォレット、モバイルウォレット）	エマージング決済テクノロジーは、受け付けておらず、使用もしていない	エマージング決済テクノロジーを間接的に受け付けまたは使用している（顧客による使用が、普通預金口座またはクレジットアカウントに影響する場合がある）	エマージング決済テクノロジーを直接的に受け付けまたは使用している。ノンバンクプロバイダーとの提携または共同ブランドであり、取引量は限られている	エマージング決済テクノジーを直接的に受け付けまたは使用している。取引量は少ない。対外決済はない	エマージング決済テクノジーを直接的に受け付けている。中程度の取引量または対外決済およびその両方がある	○
個人間決済（P2P）	提供していない	顧客は、決済代金を送金できる。1,000人未満の顧客に使用されており、月次の取引量は、50,000 未満	顧客は、決済代金を送金できる。1,000～5,000 人の顧客に使用されており、月次の取引量は 50,000～100,000	顧客は、決済代金を送金できる。5,001～10,000人の顧客に使用されており、月次の取引量は、100,001～1,000,000	顧客は、決済を依頼または決済代金を送金できます。10,000人以上の顧客に使用されており、月次の取引量は、1.000,000超	△ 利用顧客数および取引量の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
ACH 決済の仕向取引	ACH による仕向取引は行っていない	ACH による仕向送金を行っている。日次の取引高は、総資産の 3%未満	ACH による仕向送金および引落としを行っている。日次の取引高は、総資産の 3%～5%	第三者決済処理機関に出資し、ACHによる仕向送金および引落としを行っている。日次の取引高は、総資産の 6%～25%	入れ子構造の第三者決済機関に出資し、ACHによる仕向送金および引落としを行っている。日次の取引高は、総資産の25%超	○
大口の決済（例: CHIPS）	大口の決済は行っていない	日次で行われる大口決済の取引高は、総資産の 3%未満	日次で行われる大口決済の取引高は、総資産の 3%～5%	日次で行われる大口決済の取引高は、総資産の6%～25%	日次で行われる大口決済の取引高は、総資産の25%超	△ 大口決済が総資産を占める割合の妥当性を検証する必要がある。

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
電信振込	提供されていない	来店による電信振込依頼のみ。国内電信振込に限る。日次の電信振込取引高は、総資産の 3%未満	来店、電話、および FAX による電信振込依頼。日次の国内電信振込取引高は、総資産の 3%～5%。日次の国際電信振込取引高は、総資産の 3%未満	複数の振込依頼手段を提供（例：オンライン、書面、電子メール、FAXおよび電話）。日次の国内電信振込取引高は、総資産の6%～25%。日次の国際電信振込取引高は、総資産の3%−10%	複数の振込依頼手段を提供（例：オンライン、書面、電子メール、FAXおよび電話）。日次の国内電信振込取引高は、総資産の25%超。日次の国際電信振込取引高は、総資産の10%超	△ 電信振込取引高が総資産に占める割合の妥当性を検証する必要がある。
加盟店リモートデポジットキャプチャー（RDC）	加盟店 RDC は提供していない	加盟店顧客は 100 店舗未満。日次の取引高は、総資産の 3%未満	加盟店顧客は、100～500 店舗。日次の取引高は、総資産の 3%～5%	加盟店顧客は、501～1,000店舗。日次の取引高は、総資産の 6%～25%	加盟店顧客は、1,000店舗超。日次の取引高は、総資産の25%超	× 日本ではRDCが提供されていない。
国際送金	国際送金は、提供していない	日次の総取引高は、総資産の 3%未満	日次の総取引高は、総資産の 3%～5%	日次の総取引高は、総資産の6%～25%	日次の総取引高は、総資産の25%超	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
財務サービスとクライアント数	財務管理サービスは、提供していない	限られたサービスを提供している。クライアント数は、1,000 社未満	提供されているサービスには、ロックボックス、ACH 決済、リモートデポジットキャプチャーなどが含まれる。クライアント数は、1,000～10,000 社	提供されているサービスには、売掛金ソリューションや流動性の管理などが含まれる。クライアント数は、10,001～20,000社	提供されている多数のサービスには、通貨サービス、オンライン投資、および投資スイープ口座が含まれる。クライアント数は、20,000超	△ クライアント数の妥当性を検証する必要がある。
信託サービス	信託サービスは、提供していない	信託サービスは、第三者プロバイダーを通して提供している。運用資産総額は、5 億ドル未満	信託サービスは、直接提供している。運用資産総額は、5 億ドル～9.99 億ドル	信託サービスは、直接提供している。運用資産総額は、10億ドル～100億ドル	信託サービスは、直接提供している。運用資産総額は、100億ドル超	△ 運用資産総額の妥当性を検証する必要がある。
コルレス銀行としての機能（銀行間送金）	コルレス銀行として機能しない	100 行未満の機関のコルレス銀行として機能する	100～250 行の機関のコルレス銀行として機能する	251～500行の機関のコルレス銀行として機能する	500行超の機関のコルレス銀行として機能する	○
加盟店アクワイアラー（加盟店支援または決済システムへのカー	加盟店アクワイアラーとして機能しない	加盟店アクワイアラーとして機能する。加盟	加盟店アクワイアラーとして機能する。カード	加盟店アクワイアラーおよびカード決済処理会	加盟店アクワイアラーおよびカード決済処理	△

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
ド処理業務）		店数は、1000 店舗未満	決済処理は、外部に委託している。加盟店数は、1,000～10,000 店舗	社として機能する。加盟店数は、10,001～100,000店舗	会社として機能する。加盟店数は、100,000店舗超	国内金融機関は単体でのアクワイアラ業務を行っていないことを考慮し、加盟店数の妥当性を検証する必要がある。
他の組織への IT サービスのホスティング（共同システムまたは管理サポートのいずれかによる）	他の会社に IT サービスは提供していない	傘下の組織に IT サービスのホスティング、または IT サービスを提供している	最大 25 社の外部組織に IT サービスのホスティングまたは IT サービスを提供している	26～50社の外部組織にITサービスのホスティングまたはITサービスを提供している	50社超の外部組織にITサービスのホスティングまたはITサービスを提供している	△ 外部組織数の妥当性を検証する必要がある。

カテゴリ：組織的特徴

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
合併および買収（会社分割および合弁事業を含む）	計画はない	合併および買収の協議を開始するまたは積極的に検討する用意がある	少なくとも、1 社と協議中である	過去1年以内に売却または買収を公表し、1社以上と交渉中である	複数の買収統合事案が進行中である	○
直接雇用している従業員（情報技術およびサイバーセキュリティの請負業者を含む）	総従業員数は、50 名未満	総従業員数は、50～2,000 名	総従業員数は、2,001～10,000 名	総従業員数は、10,001～50,000名	総従業員数は、50,000名超	○
IT および情報セキュリティ人材の配置や変更	重要な職位は埋まっており、人員の離職はないか、少ない	重要でない職務の人員に空きがある	重要な職位または上級職の一部に離職があった	重要な職位または上級職に頻繁に離職がある	長期間にわたり重要な職位または上級職に空きがある。ITまたは情報セキュリティの従業員の離職率が高い	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
特権的アクセス権限（管理者：ネットワーク、データベース、アプリケーション、システムなど）	管理者の数は限られている。外部の管理者はいない、もしくは数が限られている	管理者の離職率は、業務または活動に影響しない。何人かの外部の管理者がいる	管理者の離職率は、業務に影響する。個々のシステムまたはアプリケーションの管理数は、必要な管理者の数を超えている	外部の管理者への依存度が高い。変更の頻度に対して管理者の数が不足している	ネットワーク管理者の従業員の離職率が高い。管理者の多くまたはほとんどは、外部（請負業者またはベンダー）から派遣されている。ネットワーク管理において、限られた経験しか持っていない	○
IT 環境の変更（例：ネットワーク、インフラストラクチャ、重要なアプリケーション、新商品または新サービスに対応したテクノロジー）	IT 環境は安定している	IT 環境で、稀に、または軽微な変更がある	頻繁に新しいテクノロジーを採用している	大きな変更の頻度が高い	重要なITサービスの委託先のプロバイダーに大きな変更があった。環境への大きく、複雑な変更が頻繁に発生している	○

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
支店/事業拠点の所在地	1 州	1 地域	1 国	1～20カ国	20カ国超	△ 拠点の定義を日本の実態に合わせる必要がある。
運用センター/データセンターの所在地	1 州	1 地域	1 国	1～10カ国	10カ国超	△ センター所在地の定義を日本の実態に合わせる必要がある。

カテゴリ：外部の脅威

	リスクレベル					仮に日本にあてはめた場合の懸念点の有無 ○：懸念なし △：修正が必要 ×：あてはめない方がよい
	最小	軽微	中程度	重大	極めて重大	
試行されたサイバー攻撃	試行された攻撃や偵察はない	月次の攻撃数は少ない（100 件未満）。一般的なフィッシング詐欺を従業員および顧客が受けたことがある	月次の攻撃は何件か（100～500 件）ある。機関または重要な活動を支援している第三者の従業員または顧客を標的にしたフィッシング詐欺。過去１年以内に分散サービス妨害（分散 DDoS 攻撃）が試行されたことがある	月次に相当数の攻撃（501～100,000 件）がある。機関または重要な活動を支援している第三者の従業員および顧客を標的にしたスピアフィッシング詐欺。機関は、特に脅威レポートに名前が記載されている。過去1年以内に分散サービス妨害（分散DDoS攻撃）が試行されたことが複数回ある	月次にかなり多数の攻撃（100,000件超）がある。上級役員やネットワーク管理者を攻撃する執拗な試みがある。また、サービス妨害（分散DDoS攻撃）の標的になることが頻繁にある	○

出典：アセスメントツールを基に NTT データ経営研究所にて作成

4. 第 2 部:サイバーセキュリティの成熟度

第 2 部ではサイバーセキュリティ成熟度のレベルを、以下の 5 つの領域から判定する。

全社的なサイバーセキュリティプログラムの開発と実施の取り組みが評価対象となる領域 1「サイバーリスクの管理と監督」の中に、内部および外部、IT および非 IT の観点から区別できる領域 2「脅威情報の収集と共有」、領域 3「サイバーセキュリティ統制」、領域 4「外部依存関係の管理」および領域 5「サイバーインシデント管理とレジリエンス」が含まれている。

領域 1「サイバーリスクの管理と監督」は、取締役による監督、経営陣による適切な説明責任や監督するための全社的な方針および手続を備えた効果的なサイバーセキュリティプログラムの開発と実施の取組みである

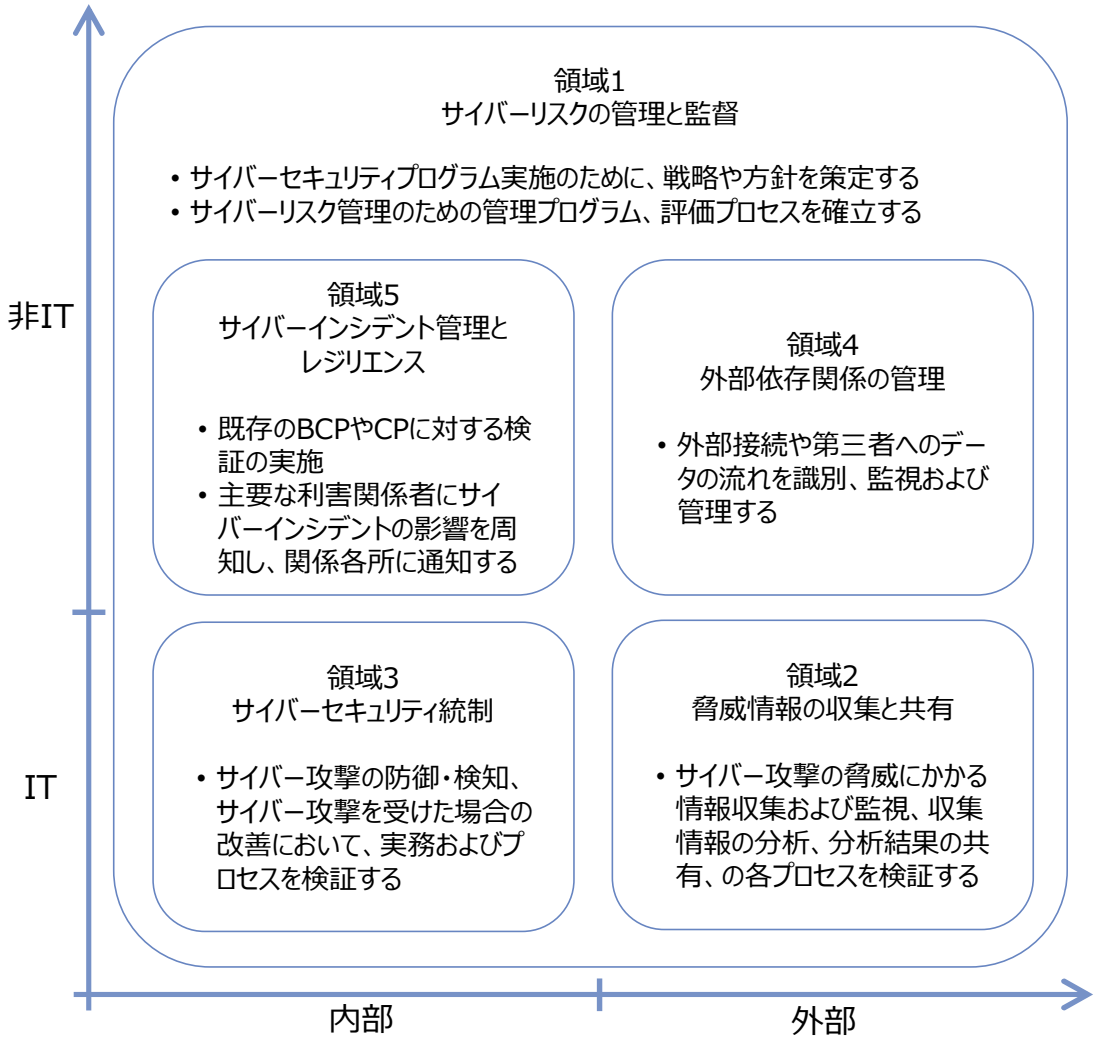
領域 2「脅威情報の収集と共有」は、外部からのサイバー攻撃の脅威にかかる情報収集、収集情報の分析および分析結果を社内や第三者へ共有する各プロセスが含まれる。

領域 3「サイバーセキュリティ統制」は、組織内部におけるサイバー攻撃への継続的な防御やサイバー攻撃を受けた場合の検知および改善におけるプロセスが含まれる。

領域 4「外部依存関係の管理」は、外部接続や情報へのアクセス権限を持つ第三者との委託関係を監視及び管理するプロセスが含まれる。

領域 5「サイバーインシデント管理とレジリエンス」は、既存の BCP や CP に対する検証の実施や、主要な利害関係者にサイバーインシデントの影響を周知し関係各所に通知するプロセスが含まれる。

図表 I-9　サイバーセキュリティ成熟度の領域



出典：アセスメントツールを基に NTT データ経営研究所にて作成

（1）サイバーセキュリティの成熟度

各領域に含まれる評価要素の定義は、**図表 I-10** のとおりである。

図表 I-10　各領域における評価要素の定義

領域	評価要素の定義	
領域1 **サイバーリスクの管理と監督**	**ガバナンス**	サイバーセキュリティプログラムの効果的なガバナンスを実施するための監督、戦略、方針、およびIT資産管理が含まれている。
	リスク管理	効果的にリスクを管理し、主要な統制の有効性を評価するためのリスク管理プログラム、リスク評価プロセス、および監査機能が含まれている。
	リソース	その組織の人員または外部のリソースが、確実にその組織のリスクプロファイルに見合った知識および経験を備えているようにするための人員配置、ツール、予算編成プロセスが含まれている。
	研修と企業文化	サイバーセキュリティ脅威の低減に重点を置く組織文化に寄与する従業員の研修および顧客意識向上プログラムが含まれている。
領域2 **脅威情報の収集と共有**	**脅威情報の収集**	サイバー対応力、意図および活動を識別、追跡および予測し、行動方針を提供して意思決定を改善するための情報の取得と分析。
	監視と分析	組織における脅威の原因の監視方法や、組織固有の脅威および従前とは異なる脅威情報にかかる対策を検討するための分析。
	情報の共有	同業者や情報共有評議会との関係の確立、およびこれらのグループや社内の利害関係者への脅威情報の伝達方法を包含。
領域3 **サイバーセキュリティ統制**	**防御**	サイバー攻撃を抑止および防止するもので、インフラストラクチャ管理、アクセス管理、デバイスおよびエンドポイントセキュリティおよびセキュアコーディングが含まれる。
	検知	脅威および脆弱性検知、変則的な活動の検知、イベント検知が含まれ、インシデントが発生または発生する可能性を示すアラートを送信してネットワークおよびシステムの不正行為を通知。
	改善	パッチ管理、脆弱性スキャンおよび侵入検査時に識別された問題の修復を通じて、システムやソフトウェアの脆弱性を解決するために利用。
領域4 **外部依存関係の管理**	**外部との接続**	外部接続や第三者へのデータの流れの識別、監視および管理が含まれる。
	関係管理	統制によって組織のサイバーセキュリティプログラムを確実に補完するために役立つデューディリジェンス、契約、および継続的な監視が含まれる。

領域	評価要素の定義	
領域5 **サイバーインシデント管理とレジリエンス**	**インシデントレジリエンスの計画策定と戦略**	既存の事業継続計画および災害復旧計画に、レジリエンス強化計画と検証を組み込み、サービスの中断とデータの破壊や破損を最小限に抑える。
	検知、対応と低減	内部および外部の脅威ならびに脆弱性の影響の識別、優先順位付け、対応、低減を行うために経営陣が取るべき措置。
	エスカレーションと報告	主要な利害関係者にサイバーインシデントの影響を周知し、規制当局、法執行機関および顧客に必要に応じて通知。

出典：アセスメントツール p.6～p.7

アセスメントツールにおける成熟度判定は、ベースライン成熟度レベルで開始され、最高位の成熟度レベルである革新レベルに進化していく。以下は各成熟度レベルの定義を示す。

図表 I-11　成熟度レベルの定義

成熟度レベルの定義	
ベースライン（Baseline）	ベースラインは、法規制で要求される、または監督上の指針で勧告されている最低限の期待値で特徴付けられる。このレベルには、コンプライアンス重視の目標が含まれている。経営陣は、指針を確認し、評価している。 ※FFIECの情報技術(IT)検査ハンドブックを満たす水準で記述されている。
進化途上（Evolving）	進化途上は、まだ要求されていない手続や方針の正式な文書へ追加として特徴付けられている。また、リスク重視の目標が整備されている。サイバーセキュリティの説明責任が正式に割り当てられ、顧客情報の保護を越えて拡大され、情報資産およびシステムが包含されている。
中程度（Intermediate）	中程度は、正式な詳細プロセスとして特徴付けられている。統制が検証され、一貫している。リスク管理の実務や分析は、事業戦略に統合されている。
高度（Advanced）	高度は、全事業分野にわたって統合されているサイバーセキュリティの実施方法で特徴付けられている。リスク管理プロセスの大部分は自動化され、継続的なプロセスの改善が含まれている。また、ビジネスの現場によるリスクの決定の説明責任が正式に割り当てられている。
革新（Innovative）	革新は、自組織や業界の人員、プロセス、およびテクノロジーにおけるサイバーリスクを管理するための革新の推進で特徴付けられている。これには、新しい統制、新規ツールまたは新しい情報共有グループの創設も伴う。また、リアルタイムの予測分析

	が自動対応に関連付けられている。

出典：アセスメントツール p.7

（2）サイバーセキュリティ成熟度評価の実施

各領域には、該当する成熟度レベルを判定しやすいよう評価軸が用意されており、評価軸毎に成熟度レベル別の評価項目が示されている。評価項目は組織の行動、実務およびプロセスを確認する内容となっている。

経営陣は、記載されたもののうち、どの項目が自組織の実務に最もあてはまるかを判定する。成熟度レベルの判定は、当該成熟度レベルと、それよりも下位の成熟度レベルの全項目を達成している必要がある。例えば、進化途上（Evolving）の項目が 1 つでも未達成の場合には、上位の成熟度レベルである中程度（Intermediate）以上には判定されないこととなる。

経営陣は、各評価項目が組織で達成されていることを検証しなければならない。一部の評価項目は、その商品やサービスが提供されていない場合や、テクノロジーが利用されていない場合はあてはまらないが、成熟度レベルの判定に影響はない。

以下に各領域における評価軸と、日本にあてはめた場合に、どのような懸念点があるかを示す。

図表 I-12　セキュリティ成熟度の各領域と評価軸

凡例：○　懸念点なし
　　△　懸念点あり

領域 1：サイバーリスクの管理と監督

評価要素：ガバナンス		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
監督	• 取締役会または適切な取締役委員会におけるサイバーセキュリティへの取組み • サイバーセキュリティに関わる経営陣の果たすべき責任 • 予算編成へのサイバーセキュリティに関わるツールの組込み	○
戦略/方針	• サイバーセキュリティ戦略と各種方針の整備 • サイバーセキュリティ情報の分析に伴う戦略や方針の見直し	○

	• 経営陣の改善意欲	
IT 資産の管理	• 自組織が保有する IT 資産の識別 • IT 資産管理に関わるプロセスの整備	○
評価要素：リスク管理		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
リスク管理プログラム	• リスク管理プログラムの整備 • リスク管理プログラムを用いたリスク分析と分析結果に基づいた改善	○
リスク評価	• リスク評価を用いたサイバーセキュリティリスクの識別 • リスク評価実務の更新	○
監査	• 独立した監査機能の存在 • サイバーリスクアペタイトステートメントの定期的なレビュー	○

評価要素：リソース		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
人員配置	• 必要とされる専門知識を識別するためのプロセスの整備 • 適切な知識を有する者への役割と責任、権限の付与 • サイバーセキュリティ担当人材の後継者育成計画策定プログラムの整備	△ 国内金融機関のシステム部門と IT ベンダーとの役割を考慮し、所掌に則した人員配置を定義する必要がある。
評価要素：研修と企業文化		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
研修	• サイバーセキュリティ研修プログラムの整備 • 職責に応じたサイバーセキュリティ研修の受講 • 研修有用性の検証	○
企業文化	• サイバーセキュリティ方針等を遵守する風土の整備 • 適切な会議体でのサイバーリスクに関する協議	○

領域 2：脅威情報の収集と共有

評価要素：脅威情報		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
脅威情報	• 情報提供される脅威情報の活用	○
評価要素：管理と分析		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
モニタリングと分析	• 脅威情報を監視し、新たな脅威を発見するプロセスの実装 • 脅威情報の分析や評価を実施する専門チームの整備 • 分析結果に基づく将来予想や準備態勢の整備	○

評価要素：情報の共有		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
情報共有	• サイバーセキュリティ情報の共有先の適切な管理と共有プロセスの整備 • サイバーセキュリティ情報を共有、評価する業界を横断した関係の確立	○

領域 3：サイバーセキュリティ統制

評価要素：防御		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
インフラストラクチャの管理	• ネットワーク境界防御ツールの利用 • 無線ネットワーク環境への適切な防御策の実装	○
アクセスとデータの管理	• 職務に応じたアクセス権限の付与 • アクセス権限変更に伴うプロセスとツールの実装 • 高リスクシステムへのアクセス認証のセキュリティ対策の実装	○
機器/エンドポイントのセキュリティ	• 各種ツールによるアクセス機器へのバッチの適用 • 権限外アクセスからの防御策の実装	○
セキュアコーディング	• ソフトウェアのセキュリティ制御の定期的な見直しの実施 • ソフトウェアコードのセキュリティ上の脆弱性を検査できるプロセスの実装 • 実稼働環境移行前のコード検査の実施	○
評価要素：検知		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
脅威と脆弱性の検知	• 独立した侵入試験や脆弱性スキャンの実施 • サイバー攻撃検知のためのツールの実装 • 制御ルールの定期的な見直しの実施	○

変則的な活動の検知	• 変則的な活動を自動的に検知するシステムの導入 • セキュリティログの定期的なモニタリングの実施 • ネットワークアラートやシステムアラートの実装	○
イベント検知	• イベント検知プロセスの整備 • ネットワークモニタリングと検知機能の実装 • リアルタイムでのアラート配信機能の実装	○
評価要素：改善		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
バッチ管理	• バッチ管理機能の実装と、適切なバッチの適用 • バッチの取得、テストおよび展開までのプロセスの整備	○
修復	• 緊急度に基づく対処の実施 • 侵入試験時における解決プロセスの整備	○

領域 4：外部依存関係の管理

評価要素：外部との接続		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
外部接続	• 外部接続に関わるプロセスマップの整備 • ネットワーク図の定期的な見直しの実施	○
評価要素：関係管理		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
デューディリジェンス	• 第三者のサイバーセキュリティ管理の評価分析プロセスの整備	○
契約	• 第三者とのサイバーセキュリティに関わる契約事項の取り交わしの実施 • セキュリティインシデントおよび脆弱性の通	△ IT ベンダーとサイバーセキュリティ対策も含めた契約の

	知等の責任に関する事項の取り交わしの実施	見直しが必要である。
継続的なモニタリング	• 第三者に対するリスク評価プロセスの整備 • リスクに応じた第三者に対するモニタリングの実施	○

領域 5：サイバーインシデント管理とレジリエンス

評価要素：インシデントレジリエンスに関する計画策定と戦略		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
計画策定	• サイバーインシデントへの対処・対応方法の整備 • 業務継続プロセスの整備	○
検査	• サイバー攻撃シナリオを用いたインシデント検知と対応策の整備 • サイバー演習への参加 • サイバー演習結果に基づく復旧シナリオ改善の実施	○
評価要素：検知、対応および低減		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
検知	• インシデント対応プログラムと稼働させるためのツールおよびプロセスの整備 • インシデントのリアルタイムでの検出可否 • 検知時の自動的なアラート機能の実装	○
対応と低減	• インシデント対応計画の策定 • サイバーインシデントの影響を最小限に抑えるためのプロセスの整備	○
評価要素：エスカレーションと報告		
評価軸	**評価項目**	**仮に日本にあてはめた場合の懸念点の有無**
エスカレーションと報告	• サイバーインシデントまたは脆弱性に関する情報の報告プロセス、および報告基準の確立	○

出典：アセスメントツールを基に NTT データ経営研究所にて作成

各領域で定義されているセキュリティ成熟度は以下のとおり。

図表 I-13　セキュリティ成熟度の定義

領域 1: サイバーリスクの管理と監督			
評価要素: ガバナンス			
		○、×	
監督	**ベースライン（Baseline）**		✓ 取締役会または適切な取締役委員会により指名された経営陣の一員が、情報セキュリティおよび事業継続性プログラムの実施と管理の説明責任を負っている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、3 ページ） ✓ 特に顕著なサイバーイベントや規制アラートによって要請があった場合には、情報セキュリティリスクについて経営会議で審議している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、6 ページ） ✓ 経営陣は、情報セキュリティおよび事業継続性プログラムの全体の状況に関する書面による報告書を取締役会または適切な取締役委員会に少なくとも年次で提出している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、5 ページ） ✓ 予算編成プロセスには、情報セキュリティ関連費用およびツールも含まれている。（FFIEC E-Banking Booklet（FFIEC E バンキングブックレット）、20 ページ） ✓ 経営陣は、他の重要なインフラストラクチャ（例：電気通信、エネルギー）によって組織にもたらされるリスクを考慮している。（FFIEC Business Continuity Planning Booklet（FFIEC 事業継続性計画策定ブックレット、J-12 ページ）

	進化途上 **（Evolving）**		✓ 取締役会または適切な取締役委員会は、少なくとも年次で組織のサイバーセキュリティプログラムを審査し、承認している。 ✓ 経営陣は、サイバーセキュリティ関連の法令遵守に責任を負っている。 ✓ サイバーセキュリティのツールおよび人員は、予算編成プロセスを通して要求されている。 ✓ 予算編成プロセスの一環として、サイバーセキュリティインシデント関連で発生し得る費用について、公式に協議や見積りを行うプロセスがある。
	中程度 **（Intermediate）**		✓ 取締役会または適切な取締役委員会は、サイバーセキュリティの専門知識を有し、あるいは専門家を採用して監督責任を果たすための支援を得ている。 ✓ 通常の取締役会の議案には、脅威情報の傾向に対処するためのイベントおよびインシデントならびに組織のセキュリティ体制を越える報告書や指標が含まれる。 ✓ 組織には、取締役会または適切な取締役委員会によって承認されたサイバーリスクアペタイトステートメントがある。 ✓ リスクアペタイトを越えるサイバーリスクは、経営陣にエスカレーションされている。 ✓ 取締役会または適切な取締役委員会は、経営陣による年次のサイバーセキュリティの自己評価において、自組織のサイバーリスク管理規定に準拠して組織の能力が評価されるようにしている。 ✓ 取締役会または適切な取締役委員会は、経営陣によるサイバー評価の結果に基づく優先順位の設定およびリソースの割当における意思決定を審査し、評価している。

			✓ 取締役会または適切な取締役委員会は、経営陣が変化するサイバーリスクや重大なサイバーセキュリティの問題に対処するため適切な施策を講じている。 ✓ サイバーセキュリティの人員やツールの追加を要求するための予算プロセスが各事業部門の予算プロセスに統合されている。
	高度 **（Advanced）**		✓ 取締役会または適切な取締役委員会が承認したサイバーリスクアペタイトステートメントは、企業全体のリスクアペタイトステートメントの一部である。 ✓ 経営陣は、継続的にサイバーセキュリティの監督を改善するための正式なプロセスを持っている。 ✓ サイバーセキュリティの人員やツールの追加を要求するための予算編成プロセスでは、現在のリソースやツールがサイバーセキュリティ戦略に対応付け（マッピング）されている。 ✓ 経営陣および取締役会または適切な取締役委員会は、各事業体に自己の活動に関連するすべてのサイバーリスクを効果的に管理する責任を課している。 ✓ 経営陣は、サイバー攻撃により物的損失を被った場合に根本原因を識別している。 ✓ 取締役会または適切な取締役委員会は、自組織と金融業界との関係におけるサイバーリスクを考慮した施策を経営陣が講じるものとしている。
	革新 **（Innovative）**		✓ 取締役会または適切な取締役委員会は、経営陣が業界全体で採用可能なサイバーセキュリティの改善策を策定する方法を協議している。 ✓ 取締役会または適切な取締役委員会は、経営陣の施策で自組織が他の重要なインフラストラクチャ（電気通信、

			エネルギー）にもたらすサイバーリスクが考慮されるよう確保している。
戦略／方針	**ベースライン（Baseline）**		✓ 組織には、リスクを低減するためのテクノロジー、方針、手続および研修を統合する情報セキュリティ戦略がある。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、3 ページ） ✓ 組織には、情報技術のリスク管理の概念に対応するため、組織のリスクと複雑性に相応した方針がある。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、16 ページ） ✓ 組織には、脅威情報共有の概念に対応するため、組織のリスクと複雑性に相応した方針がある。（FFIEC E-Banking Booklet（E バンキングブックレット）、28 ページ） ✓ 組織には、情報セキュリティに対応するため、組織のリスクと複雑性に相応の取締役会が承認した方針がある。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、16 ページ） ✓ 組織には、外部依存関係または第三者の管理の概念に対応するため、組織のリスクと複雑性に相応した方針がある。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット）、2 ページ） ✓ 組織には、インシデント対応およびレジリエンスの概念に対応するため、組織のリスクと複雑性に相応した方針がある。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ 情報セキュリティプログラムのすべての要素は、全社的に調整されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、7 ペー

			ジ）
	進化途上 **（Evolving）**		✓ 組織は、サイバーセキュリティとレジリエンスを組み込むためにその情報戦略を強化した。 ✓ 組織は、テクノロジーとセキュリティの業界標準または基準に基づいた正式な情報セキュリティプログラムを有している。 ✓ 組織の固有リスクプロファイルが変化したときに方針を変更するための正式なプロセスが整備されている。
	中程度 **（Intermediate）**		✓ 組織には、脅威情報の概念に対応するため、組織のリスクと複雑性に相応した包括的な一連の方針がある。 ✓ 経営陣は、定期的にサイバーセキュリティ戦略を見直し、進化するサイバー脅威および組織の固有リスクプロファイルの変化に対応している。 ✓ サイバーセキュリティ戦略は、組織の全社的なリスク管理戦略に組み込まれており、この戦略と概念的に一致している。 ✓ 経営陣は、戦略的なサイバーセキュリティの目標を戦術的な目標に関連付けている。 ✓ 全事業分野のサイバーリスクに関連するすべての方針を相互参照し、同時に変更するための正式なプロセスが整備されている。
	高度 **（Advanced）**		✓ サイバーセキュリティ戦略に、短期的な視点および長期的な視点の両方から見た、組織のサイバーセキュリティの将来の状態が概説されている。 ✓ サイバーセキュリティプログラムのギャップ分析時の情報源として業界で認められているサイバーセキュリティ標準が使用されている。

			✓ サイバーセキュリティ戦略に、金融サービス業界の重要なインフラストラクチャの構成要素としての組織の役割が明記され、周知されている。 ✓ リスクアペタイトが、重要なインフラストラクチャにおける組織の役割に基づいて周知されている。 ✓ 経営陣は、サイバーセキュリティの目標とする望ましい状態の変化に合わせて継続的に既存のサイバーセキュリティプログラムを改善している。
	革新 **（Innovative）**		✓ サイバーセキュリティの戦略は他の重要なインフラストラクチャと関連するため、戦略には組織の役割が明記され、周知されている。
IT 資産の管理	**ベースライン** **（Baseline）**		✓ 組織の資産（例：ハードウェア、ソフトウェア、データおよび外部でホストされているシステムなど）のインベントリ情報（一覧）が維持されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、9 ページ） ✓ 組織の資産（例：ハードウェア、システム、データおよびアプリケーション）には、データの分類および業務上の価値に基づいて保護の優先順位が設定されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、12 ページ） ✓ 経営陣は、組織の資産のインベントリの維持管理の説明責任を割り当てている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、9 ページ） ✓ システム構成、ハードウェア、ソフトウェア、アプリケーション、セキュリティツールに対する変更を要求および承認するための変更管理プロセスが整備されている。（FFIEC

			Information Security Booklet（FFIEC 情報セキュリティブックレット）、56 ページ）
	進化途上 **（Evolving）**		✓ 重要な資産の識別を含む、資産のインベントリは、新規資産、移転資産、再利用資産および末期資産に対応するために少なくとも年次で更新されている。 ✓ 組織には、取得資産が適切なセキュリティ安全策を備えているかどうかを考慮するための文書化された資産ライフサイクルプロセスがある。 ✓ 組織では、セキュリティリスクを制限するためにシステムのエンドオブライフ（EOL）（例：置換）を事前に管理している。 ✓ 変更は、職務分掌の下で適切な権限を持った個人または委員会によって、正式に承認されている。
	中程度 **（Intermediate）**		✓ ベースライン構成は、正式な変更要求、文書化された承認およびセキュリティ上の影響の評価なしでは、変更できない。 ✓ 正式な IT 変更管理プロセスによって、変更の分析、承認、検証および報告時にサイバーセキュリティリスクの評価が要求される。
	高度 **（Advanced）**		✓ システムコンポーネントも含め、ミッションクリティカルな情報システムの取得の前に、サプライチェーンのリスクを検討している。 ✓ 自動化ツールによって、資産のインベントリの追跡、更新、資産の優先順位の設定、カスタムレポート作成が可能である。 ✓ ソフトウェアおよびハードウェアに対する不正な変更を検知してブロックするため、自動化プロセスが整備されている。

			✓ 変更管理システムでは、変更の影響のリスク評価が必要な場合を識別するための閾値が使用されている。
	革新 **（Innovative）**		✓ 正式な変更管理機能によって、分権化された、または高度に分散された変更要求が管理され、サイバー攻撃に対するエクポージャーの増大を引き起こす恐れのあるセキュリティリスクが識別、評価されている。 ✓ ソフトウェアおよびハードウェアに対する不正な変更を検知し、ブロックするために包括的な自動化されたエンタープライズツールが実装されている。
評価要素：リスク管理			
リスク管理プログラム	**ベースライン** **（Baseline）**		✓ 組織には、情報セキュリティおよび事業継続性のリスク管理機能がある。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、68 ページ）
	進化途上 **（Evolving）**		✓ リスク管理プログラムには、サイバーリスクの識別、評価、低減、モニタリング（監視）および報告が組み込まれている。 ✓ 経営陣は、監査の結果を確認し、それを利用して既存のサイバーセキュリティの方針、手続および統制を改善している。 ✓ 経営陣は、サイバーリスク評価における中程度および高い残余リスクについて、問題のモニタリングをそれらが対処されるまで行っている。
	中程度 **（Intermediate）**		✓ サイバーセキュリティ機能には、利益相反がない明確な指揮命令系統がある。 ✓ サイバーセキュリティプログラムは、技術的影響（例：財政的影響、戦略的影響、規制上の影響、法令遵守上の影

			響）の境界をまたがったサイバーリスクに対応している。 ✓ 時間の経過に伴うセキュリティ体制の改善または後退を示すための基準または目標とするパフォーマンスの指標が確立されている。 ✓ 経営陣は、独立した監査の結果を利用して見直しを行い、サイバーセキュリティを改善している。 ✓ コストセンターには、サイバーセキュリティインシデント関連で発生し得る損失および関連する費用を分析し、割り当てるプロセスがある。
	高度 **（Advanced）**		✓ サイバーセキュリティ指標を使用して、必要な領域で戦略的な意思決定と資金拠出を促進している。 ✓ 独立したリスク管理機能では、各事業部門のサイバー関連リスクの制限値（限度額）を設定し、モニタリングしている。 ✓ 独立したリスク管理の人員は、サイバー関連リスクに関する各事業部門の評価における大きな差異や矛盾を、経営陣および取締役会または適切な取締役委員会にエスカレーションしている。 ✓ サイバーインシデントが組織の資本に及ぼす影響を分析するためのプロセスが整備されている。 ✓ サイバーリスクデータの集計とリアルタイムのレポート（報告書）作成機能によって、組織の継続的な報告のニーズ（特にサイバーインシデント時）に対応している。
	革新 **（Innovative）**		✓ リスク管理機能では、組織および他の全業界で発生したサイバーイベントの共通点を識別し、分析し、さらに予測可能なリスク管理を可能にする。

			✓ 組織のサイバーインシデントが金融業界全体に及ぼす財務的影響を分析するプロセスが整備されている。
リスク評価	**ベースライン（Baseline）**		✓ 顧客情報の保護に重点を置いたリスク評価では、論理的で予見可能な内部および外部の脅威、脅威の可能性および被り得る損害、方針、手続および顧客情報システムの十分性を識別する。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、8 ページ） ✓ リスク評価では、追加の認証を保証するインターネットベースのシステムや高リスク取引を識別している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、12 ページ） ✓ 新しいテクノロジー、商品、サービスおよび外部との接続を展開する前に、それらに対応するために、リスク評価を更新している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、13 ページ）
	進化途上（Evolving）		✓ リスク評価を利用して、新しい商品、サービスまたは関係に起因するサイバーセキュリティリスクを識別している。 ✓ リスク評価の焦点は、すべての情報資産に対応するために、顧客情報の保護を越えて拡大している。 ✓ リスク評価では、EOL ソフトウェアおよびハードウェアコンポーネントの使用のリスクを考慮している。
	中程度（Intermediate）		✓ リスク評価は、広く知られたリスクまたはリスク管理の実務を考慮して調整されている。
	高度（Advanced）		✓ 全社的なリスク管理機能には、企業のリスク評価の一環としてサイバー脅威の分析および特定のリスクエクスポージャーが組み込まれている。

	革新 **（Innovative）**		✓ リスク評価は、リスクプロファイルの変更発生時、新しい適用標準のリリースまたはアップデート時、および新しいエクスポージャーの予測時に、リアルタイムで更新される。 ✓ 組織では、リスク評価の情報を利用して脅威を予測し、リアルタイムの対応を推進している。 ✓ 先進的または自動化された分析によって、予測情報とリアルタイムのリスク指標が提供される。
監査	**ベースライン** **（Baseline）**		✓ 独立した監査またはレビューでは、組織全体の方針、手続および統制を評価して、新商品、エマージングテクノロジー、情報システムのリスクなど、重大なリスク、組織の業務に関連する統制の問題の有無を確認する。（FFIEC Audit Booklet、（FFIEC 監査ブックレット）、4 ページ） ✓ 独立した監査機能（部門）は、機密データの保存または送信に関連した統制を検証する。（FFIEC Audit Booklet、（FFIEC 監査ブックレット）、1 ページ） ✓ ログ記録の実務は、適切なログ管理を確保するために、別途定期的に検査される。（FFIEC Operations Booklet、（FFIEC運用ブックレット）、29ページ） ✓ 内部監査および独立した検査/評価で発見された問題および改善策は、有効性を失っている手続および統制が適時に解決されるように正式に追跡される。（FFIEC Information Security Booklet（FFIEC情報セキュリティブックレット）、6ページ）
	進化途上 **（Evolving）**		✓ 独立した監査機能は、リスク管理機能が組織のリスクと複雑性に相応のものであることを検証する。 ✓ 独立した監査機能は、脅威情報の共有が組織のリスクと

			複雑性に相応のものであることを検証する。 ✓ 独立した監査機能は、サイバーセキュリティの統制機能が組織のリスクと複雑性に相応のものであることを検証する。 ✓ 独立した監査機能は、第三者委託関係管理が組織のリスクと複雑性に相応のものであることを検証する。 ✓ 独立した監査機能は、インシデント対応プログラムおよびレジリエンスが、組織のリスクと複雑性に相応のものであることを検証する。
	中程度 **（Intermediate）**		✓ 独立した監査機能が、組織の固有リスクプロファイルに対する変更に基づいてその手続を更新するための正式なプロセスが整備されている。 ✓ 独立した監査機能は、脅威情報の収集と共有が、組織のリスクと複雑性に相応のものであることを検証する。 ✓ 独立した監査機能は、経営陣のサイバーリスクアペタイトステートメントを定期的に審査する。 ✓ 独立した監査または審査により、既存のセキュリティ機能および専門知識のギャップ（不足や欠落）を識別する。
	高度 **（Advanced）**		✓ 独立した監査機能が、業界全体で進化している脅威環境に対する変更に基づいて、その手続を変更するための正式なプロセスが整備されている。 ✓ 独立した監査機能は、組織のサイバーリスクアペタイトステートメントを評価結果と比較して定期的にレビューし、そのギャップを監査戦略に組み入れる。 ✓ 独立した監査またはレビューを利用して、サイバーセキュリティの弱点、根本原因および各事業部門に及ぼす可能性のある影響が識別される。

	革新 **（Innovative）**		✓ 独立した監査機能が、組織が依拠している他の業界で進行する脅威環境の変化に基づいて、その手続を更新するための正式なプロセスが整備されている。 ✓ 独立した監査機能では、高度なデータマイニングツールを利用して、サイバーセキュリティプロセスまたは統制の継続的なモニタリングを行う。
評価要素: リソース			
人員配置	**ベースライン** **（Baseline）**		✓ 情報セキュリティの役割と責任が明記されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、7 ページ） ✓ 情報セキュリティの防御を改善するために必要とされるその他の専門知識を識別するためのプロセスが整備されている。（FFIEC Information Security Work Program（FFIEC 情報セキュリティワークプログラム）、目標 I: 2.8）
	進化途上 **（Evolving）**		✓ サイバーセキュリティツールや必要とされる専門知識を識別するために、正式なプロセスが使用されている。 ✓ 適切な知識と経験を持つ経営陣が、組織のサイバーセキュリティの取り組みを統率している。 ✓ サイバーセキュリティの責任を負う人員は、その職位の職務を執行するために必要な資格がある。 ✓ 採用候補者、下請業者、第三者は、アクセスするデータの機密性、業務要件、許容リスクに応じて契約前調査の対象になる。
	中程度 **（Intermediate）**		✓ 組織には、サイバーセキュリティおよびレジリエンス担当人員向けの有能な人材の採用、定着、後継者育成計画策定プログラムがある。

	高度 **（Advanced）**		✓ 組織では、サイバーセキュリティの人員をその同僚を基準に評価して、採用、定着、後継者育成計画策定プログラムが相応しいかどうかを識別している。 ✓ 専任のサイバーセキュリティスタッフが、統合されたエンタープライズレベルのセキュリティ戦略とサイバー防御戦略を開発しているか、またはその開発に寄与している。
	革新 **（Innovative）**		✓ 組織は、企業団体や学界と積極的に提携し、金融業界における将来的なサイバーセキュリティの人員配置のニーズに基づいた育成計画を整備している。
評価要素：研修と企業文化			
研修	**ベースライン** **（Baseline）**		✓ 年次で情報セキュリティ研修を実施している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、66 ページ） ✓ 年次の情報セキュリティ研修には、インシデント対応、現在のサイバー脅威（例：フィッシング、スピアフィッシング、ソーシャルエンジニアリングおよびモバイルセキュリティ）および新たな問題が含まれる。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、66 ページ） ✓ 特に顕著なサイバーイベントや規制アラートにより要請があった場合には、状況認識資料を従業員に配布している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、7 ページ） ✓ 顧客意識向上資料を簡単に入手できる（例：DHS のサイバーセキュリティ意識向上月間資料）。（FFIEC E-Banking Work Program（FFIEC E バンキングワークプログラム）、目標 6-3）

	進化途上 **（Evolving）**		✓ 組織には、サイバーセキュリティスタッフのサイバーセキュリティ研修および技能開発を継続的に行うためのプログラムがある。 ✓ 経営陣は、自身の職責に関連するサイバーセキュリティ研修を受講している。 ✓ 特権アカウントの権限を持つ従業員は、自身の責任レベルに合った追加のサイバーセキュリティ研修を受講している。 ✓ 各事業部門では、それぞれに特有の事業リスクに関連するサイバーセキュリティ研修を実施している。 ✓ 組織では、研修の有効性を検証している（例：ソーシャルエンジニアリングまたはフィッシングテスト）。
	中程度 **（Intermediate）**		✓ 経営陣は、ソーシャルエンジニアリング行為やフィッシング行為の事例から学んだ教訓を、従業員の意識向上プログラムを向上するために取り入れている。 ✓ サイバーセキュリティ意識向上のため、小口顧客や商業顧客に少なくとも年次で情報提供されている。 ✓ 各事業部門でそれぞれに特有の事業リスクに関連したサイバーセキュリティ研修を実施している。 ✓ 組織は、新しい脅威に適応するためにセキュリティスタッフに対する研修を日常的に更新している。
	高度 **（Advanced）**		✓ 独立取締役は、複雑な商品、サービスおよび各事業分野によって組織のサイバーリスクに及ぼされる影響に対処するためのサイバーセキュリティ研修を受講している。
	革新 **（Innovative）**		✓ 研修および意識向上プログラムが行動に良い影響を及ぼしているかどうかを判定するために主要業績評価指数（KPI）が使用されている。

企業文化	**ベースライン** **（Baseline）**		✓ 経営陣は、従業員に情報セキュリティプログラムを遵守する責任を課している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、7 ページ）
	進化途上 **（Evolving）**		✓ 組織には、すべての従業員にサイバーセキュリティの方針と手続を遵守する責任を課す正式な行動規範がある。 ✓ 事業部門の会議で、サイバーリスクに関する協議が積極的に行われている。 ✓ 従業員は、起こり得るサイバーセキュリティの問題の識別方法やエスカレーション方法について、明確に理解している。
	中程度 **（Intermediate）**		✓ 経営陣は、従業員に責任を負わせるために各自の業績計画とサイバーセキュリティ方針や規範の遵守を関連付けている。 ✓ 経営上の全ての意思決定においてサイバーリスクを考慮するリスク文化が根付いている。 ✓ サイバーリスクの報告書は、独立したリスク管理会議に提出され、協議される。
	高度 **（Advanced）**		✓ 経営陣は、文化的視点からサイバーリスクに関する意識の向上を継続的に行っている。
	革新 **（Innovative）**		✓ 組織は、業界全体および組織が依拠する他の業界においてサイバーセキュリティ文化を推進するための取り組みを主導している。

領域2：脅威情報の収集と共有			
評価要素：脅威情報			
		○、×	
脅威情報	**ベースライン（Baseline）**		✓ 組織は、脅威に関する情報を提供する脅威および脆弱性情報の共有元（例：FS-ISAC、米コンピューター緊急事態対策チーム（US-CERT））に帰属または登録している。（FFIEC E-Banking Work Program（FFIEC Eバンキングワークプログラム）、28 ページ） ✓ 脅威情報は、脅威および脆弱性のモニタリングに利用される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ 脅威情報は、社内のリスク管理および統制の強化に利用される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、4 ページ）
	進化途上（Evolving）		✓ 組織が受け取る脅威情報には、戦術、パターン、リスクを低減するための推奨策などが含まれる。
	中程度（Intermediate）		✓ 正式な脅威情報の収集プログラムが実装され、外部のプロバイダーや内部の情報源から脅威情報のフィードを受信するための登録機能も備えている。 ✓ 業界の同業者や政府から情報を収集するためのプロトコルが実装されている。 ✓ 読み取り専用のサイバー脅威情報の一元的なレポジトリが維持されている。
	高度（Advanced）		✓ 脅威情報を収集するために、サイバー情報モデルが使用されている。 ✓ 複数の情報源から脅威情報が自動的にリアルタイムで受

			信される。 ✓ 組織の脅威情報には、サイバーセキュリティ脅威レベルを増大させるおそれのある地政学的イベントに関連する情報が含まれる。
	革新 **（Innovative）**		✓ 脅威分析システムによって、脅威データは自動的に特定のリスクに関連付けられ、経営陣にアラートを通知すると同時にリスクベースの措置が自動的に講じられる。 ✓ 組織は、情報の収集および共有方法を変革する新しい脅威情報の収集と共有の仕組み（例：テクノロジー、ビジネスプロセス）の開発に投資している。
評価要素：モニタリングと分析			
モニタリングと分析	**ベースライン** **（Baseline）**		✓ 監査ログ記録およびその他のセキュリティイベントログが、安全な方法で確認され、保管されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、79 ページ） ✓ イベントが発生すると、コンピューターイベントログを利用して調査が行われる。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ）
	進化途上 **（Evolving）**		✓ 脅威情報をモニタリングして新たな脅威を発見するプロセスが実装されている。 ✓ 脅威情報および分析プロセスが、特定のグループまたは個人に割り当てられる。 ✓ セキュリティプロセスおよびテクノロジーは、一元的に管理され、セキュリティ運用センター（SOC）または同等の施設で調整される。 ✓ モニタリングシステムを、適切なサポートの下で継続的に動

			作させ、効率的なインシデント処理を行っている。
	中程度 **（Intermediate）**		✓ 複数の情報源からの脅威情報の信頼性、関連性およびエクスポージャーを評価する脅威情報チームが整備されている。 ✓ 脅威ごとに、脅威の想定される意図、機能および標的を識別するプロファイルが作成されている。 ✓ 脅威プロファイルのすべてのコンポーネントに対処する脅威情報の情報源の優先順位を設定し、モニタリングしている。 ✓ 脅威情報を分析し、組織のリスクや検討すべき特定の施策を含むサイバー脅威の概要を作成している。
	高度 **（Advanced）**		✓ 専用のサイバー脅威識別分析委員会またはチームが存在し、イニシアチブや通信を一元的に管理し、調整している。 ✓ 共有分析センターまたはその他の情報源から受信される情報で起こり得る不一致を解決するための正式なプロセスが定義されている。 ✓ 新たな内部および外部の脅威情報と相関付けられたログ分析を利用して、将来の攻撃を予測している。 ✓ 組織のリスクプロファイルおよびリスクアペタイトの観点から脅威情報を考慮し、脅威の予想における低減施策の優先順位を設定している。 ✓ 脅威情報を利用して、アーキテクチャおよび構成の標準を更新している。
	革新 **（Innovative）**		✓ 組織では、複数の情報源、相関ログ分析、アラート、内部トラフィックフロー、地政学的イベントを利用して、将来発生し得る攻撃や攻撃動向を予測している。 ✓ 最大リスクのシナリオを利用して、特定のビジネス目標に対

			する脅威を予測している。 ✓ IT システムでは、脅威情報とアラート管理に基づいて構成の脆弱性が自動的に検出されるため、施策の優先順位を設定できる。
評価要素: 情報共有			
情報共有	**ベースライン（Baseline）**		✓ 情報セキュリティの脅威が収集され、適切な社内の従業員と共有される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ 法執行機関および規制当局の連絡先情報を共有し、定期的に更新している。（FFIEC Business Continuity Planning Work Program（FFIEC 事業継続性計画策定ワークプログラム）、目標 I: 5-1） ✓ 必要に応じて、または要請があった場合に、脅威に関する情報を法執行機関および規制当局に提供している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ）
	進化途上（Evolving）		✓ 脅威および脆弱性情報を他の事業体と共有する正式で安全なプロセスが整備されている。 ✓ 組織の代表者が法執行機関または情報共有団体の会議に出席している。
	中程度（Intermediate）		✓ 脅威、脆弱性およびインシデント情報を各従業員の固有の職務権限に基づいて共有するための正式なプロトコルが整備されている。 ✓ 情報共有合意を必要または要求に応じて利用することにより、金融業界の他の企業または第三者との脅威情報の共有を促進している。

			✓ 業界、法執行機関、規制当局、情報共有評議会と情報を積極的に共有している。 ✓ サイバー脅威に関して、公共部門と連絡を取り合い、協力するプロセスが整備されている。
	高度 **（Advanced）**		✓ 経営陣は、脅威情報を事業リスク情報と特定のリスク管理の推奨事項とともに事業部門に連絡する。 ✓ 同業の他の組織の従業員との間にサイバー脅威情報の共有のための関係が確立されている。 ✓ サイバー脅威に関する情報を評価するための信頼関係のネットワーク（公式または非公式あるいはその両方）が確立されている。 、
	革新 **（Innovative）**		✓ サイバー脅威情報を、施策を講じない場合の財政的影響および業務上の影響も含め、各事業部門とリアルタイムで共有するための仕組みが整備されている。 ✓ システムによって自動的に経営陣に対し、自組織に固有の事業リスクのレベルとリスクを低減するために講じられた推奨策の進捗状況が通知される。 ✓ 組織は、外部向けの情報共有の仕組みの不足または欠如に対処するために新しい業界全体の情報共有チャネルを創設する取り組みを主導している。

領域3：サイバーセキュリティ統制			
評価要素：防御			
		○、×	
インフラストラクチャの管理	**ベースライン（Baseline）**		✓ ネットワーク境界防御ツール（例：境界ルーターおよびファイアウォール）を使用している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、33 ページ） ✓ インターネットから、または外部の利用者からアクセスされるシステムは、ファイアウォールまたはその他の類似の機器によって保護されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、46 ページ） ✓ すべてのポートはモニタリングされている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、50 ページ） ✓ 最新式のウィルス対策ツールおよびマルウェア対策ツールが使用されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、78 ページ） ✓ システム構成（サーバー、デスクトップ、ルーターなど）は、業界標準に従って実施されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、56 ページ） ✓ ポート、機能、プロトコルおよびサービスは、業務で必要なくなった場合は禁止される。（FFIEC Information Security Booklet（情報セキュリティブックレット）、50 ページ） ✓ システム構成を変更するためのアクセス（仮想マシンおよびハイパーバイザーを含む）は、制御され、モニタリングされる。（FFIEC Information Security Booklet（FFIEC 情

			報セキュリティブックレット）、56 ページ） ✓ システム、オブジェクト、ネットワーク、仮想マシン、アプリケーションの制御をオーバーライドできるプログラムは制限されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、41 ページ） ✓ 無操作状態であらかじめ設定した時間が経過すると、システムのセッションはロックされ、あらかじめ設定した条件が満たされると、終了する。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、23 ページ） ✓ 無線ネットワーク環境では、認証や送信には強力な暗号化を使用したセキュリティ設定が必要である（*この項目は、無線ネットワークがない場合は適用されない）。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、40 ページ）
	進化途上 **（Evolving）**		✓ インターネットの各接続部および非武装地帯と社内ネットワークとの間にファイアウォールがある。 ✓ ウィルス対策および侵入検知/防止システム（IDS/IPS）は、実際に試行された攻撃や侵入を検知しブロックする。 ✓ 技術的制御によって、不正な無線アクセス機器、リムーバブルメディアも含め、許可されていない機器の社内ネットワークへの接続が防止されている。 ✓ 組織またはインターネットホスティングプロバイダーに、破壊的なサイバー攻撃（例: DDoS 攻撃）を低減するためのリスクベースのソリューションが整備されている。 ✓ ゲストアカウントの無線ネットワークは、完全に内部ネットワークから隔離されている。（*この項目は、無線ネットワークがない場合には適用されない）

			✓ ドメイン名システムセキュリティ拡張（DNSSEC）が全社的に展開されている。 ✓ レガシーテクノロジーによってサポートされている重要なシステムは、潜在的な脆弱性、アップグレードの機会または新しい防御層の有無を識別するために定期的に検証される。 ✓ サポートされていないシステムの統制が実施され、検証されている。
	中程度 **（Intermediate）**		✓ 攻撃を低減するために、企業のネットワークが複数に分割され、多層防御戦略により信頼できるゾーン/セキュリティゾーンに分離されている（例：論理的ネットワーク分割、ハードバックアップ、エアギャップ）。 ✓ 制限された仮想システムを含め、すべての管理コンソールへのリモートアクセスに対して、セキュリティ制御が使用されている。 ✓ 無線ネットワーク環境には、不正なトラフィックを制限するように実装および構成された境界ファイアウォールが設置されている（*この項目は、無線ネットワークがない場合には適用されない）。 ✓ 無線ネットワークでは、頻繁に変更される暗号化キーを使用した強力な暗号化を利用している（*この項目は、無線ネットワークがない場合には適用されない）。 ✓ 無線ネットワークのブロードキャスト範囲は、組織によって制御される境界までの範囲内に限定されている。 ✓ 組織が所有または管理する機器での不正なコードの実行を防止するための技術的な方策が整備されている。
	高度 **（Advanced）**		✓ ネットワーク環境および仮想インスタンスは、信頼できるゾーンと信頼できないゾーン間のトラフィックを制限してモニタリングするように設計され、構成されている。

			✓ さまざまなセキュリティレベルを要求する各種機能が同じサーバーに共存しないようにするため、サーバーあたりに認められる主要機能は、1 つのみである。 ✓ 詐称した送信元 IP アドレスを検知し、ネットワークへの侵入をブロックするためのなりすまし対策が整備されている。
	革新 **（Innovative）**		✓ 組織のリスクスコアでは、すべてのインフラストラクチャ資産が採点され、脅威、脆弱性または業務上の変更に基づいてリアルタイムで更新される。 ✓ インフラストラクチャ資産のリスクスコアに基づいて、影響を受ける資産を自動的に切断するなどの自動化された統制が整備されている。 ✓ 組織は、ゼロデイ攻撃に利用される可能性のある統制のギャップ（不足または欠如）を識別するために積極的な取り組みを行っている。 ✓ 公衆インターネットからアクセスできるサーバーは、システムが潜在的な脅威に曝される時間枠を制限するために、定期的に交代させ、既知の初期化状態に戻している。
アクセスとデータの管理	**ベースライン** **（Baseline）**		✓ システムや機密データに対する従業員のアクセス権限は、職務と最小権限の原則に基づいて付与される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、19 ページ） ✓ システムや機密データに対する従業員のアクセス権限は、職務分掌に基づいて付与される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、19 ページ） ✓ 権限昇格（例：管理者権限）は制限され、厳しく管理されている（例：個人に割り当てる、共有しない、強いパスワードによる管理を要求するなど）。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、

			19 ページ） ✓ すべてのシステムおよびアプリケーションについて、アプリケーションまたはシステムのリスクに基づいてユーザーのアクセス権限の見直しを定期的に行う。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、18 ページ） ✓ 物理的および論理的なユーザーアクセス権限に対する変更は、自己都合退職および会社都合退職による変更も含め、適切な人員に送信され承認されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、18 ページ） ✓ システム、アプリケーションおよびハードウェアへのアクセスには、識別および認証が要求され、管理されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、21 ページ） ✓ アクセス制御にはパスワードの複雑性が含まれ、パスワードの試行と再利用は制限されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、66 ページ） ✓ デフォルトパスワードと不要なデフォルトアカウントはすべて、システム実装の前に変更されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、61 ページ） ✓ インターネットベースの商品またはサービスへの顧客のアクセスには、リスクに相当する認証制御（例：階層制御、多要素認証）が必要である。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、21 ページ） ✓ 不正なアクセスまたは情報資産の変更を防止するために実

			稼働環境と非実稼働環境は分離されている（*この項目は、自組織または自組織の第三者企業（外部委託会社）に実稼働環境がない場合は、適用されない）。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、64 ページ） ✓ 物理的なセキュリティ制御を使用して、情報システムや通信システムへの不正なアクセスを防止している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、47 ページ） ✓ 保存時および通信時のパスワードはすべて暗号化されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、21 ページ） ✓ 機密データを公衆ネットワークまたは信頼できないネットワーク（例:インターネット）を介して送信する場合には、暗号化している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、51 ページ） ✓ 機密データの保存に使用する場合には、モバイル機器（例:ラップトップ、タブレットおよびリムーバブルメディア）を暗号化している（*この項目は、モバイル機器が使用されていない場合は、適用されない）。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、51 ページ） ✓ 従業員、請負業者、および第三者による重要なシステムへのリモートアクセスでは、暗号化された接続と多要素認証が使用されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、45 ページ） ✓ 管理職務を持たないユーザーによる許可されていないソフトウェアのインストールを防止するために、管理、物理的制御、技術的制御が行われている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、

			25 ページ） ✓ カスタマーサービス（例: コールセンター）では、取引または要求のリスクに応じて、顧客を認証するための正式な手続が利用されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、19 ページ） ✓ データは、文書化された要件に従って、想定されている時間枠内に破棄または破壊される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、66 ページ）
	進化途上 **（Evolving）**		✓ ユーザーアクセス権限トリガーの変更により、自動的に適切な人物に通知が送信される。 ✓ 管理者は、管理者用と管理タスク以外の一般的な目的用の 2 つのアカウントを持っている。 ✓ 非実稼働環境での顧客データの使用は、機密データ要素の非表示または削除に関する法規制および社内の方針の要件に準拠している。 ✓ リスクの高いまたは機密性の高いシステムへの物理的なアクセスは制限され、ログに記録されており、不正なアクセスはブロックされる。 ✓ 暗号鍵への不正なアクセスを防止するための統制が整備されている。
	中程度 **（Intermediate）**		✓ 組織には、機密データへの不正なアクセスまたは外部からのデータの引き出しを防止するために実装されたツールがある。 ✓ ユーザー権限の不正な昇格を防止するための統制が整備されている。

			✓ データベース管理者が機密データの不正なダウンロードまたは送信を防止するためのアクセス制御が整備されている。 ✓ すべての物理的および論理的なアクセス権限は、会社都合退職の通知後直ちに、自己都合退職の従業員の退職後24 時間以内に削除される。 ✓ 組織のネットワーク、システムおよびアプリケーションに対するすべての第三者によるアクセスのセキュリティを確保するために、多要素認証または階層制御あるいはその両方が実装されている。 ✓ リスク評価で識別されたリスクの高いシステムへの従業員のアクセスには、多要素認証（例：トークン、電子証明書）技術を使用している。（*この項目は、リスクの高いシステムがない場合は、適用されない） ✓ プライベート接続（フレームリレーおよびT1）を介した送信時や自組織の信頼できるゾーン内でも、機密データは暗号化される。 ✓ 協同作業用コンピューター機器およびアプリケーション（例：ネットワーク接続のホワイトボード、カメラ、マイク、インスタントメッセージングや文書共有などのオンラインアプリケーション）への不正なアクセスを防止するための統制が整備されている。（*この項目は、協同作業用機器が使用されていない場合には適用されない）
	高度（Advanced）		✓ 特定の保存（蓄積）データの暗号化は、組織のデータ分類とリスク評価に基づいて決定されている。 ✓ リスクの高い取引における顧客認証には、マルウェア攻撃や中間者攻撃を防止するための方策（例：ビジュアル式トランザクション署名機能の使用など）も含まれる。
	革新		✓ 適応型アクセス制御によって、悪意のある行為が疑われる場合には、従業員、第三者または顧客の認証情報のプロビジョ

	（Innovative）		ン解除または隔離を行う。 ✓ 構造化されていない機密データは、社内の脅威から保護し、ユーザーアクセスを監視し、変更を追跡する、個人識別型でクロスプラットフォームのストレージシステムによって、追跡され、セキュリティが確保されている。 ✓ トークン化を使用して、機密情報を一意の値に置き換えている（例：バーチャルクレジットカード）。 ✓ 組織は、顧客、従業員および第三者の認証やアクセスを管理するための新しい技術やプロセスを創設する取り組みを主導している。 ✓ ユーザーの認証情報の自動化されたリスク採点に基づいて、リスク低減策がリアルタイムで実行されている。
機器/エンドポイントのセキュリティ	**ベースライン（Baseline）**		✓ リムーバブルメディアの使用を許可された人員に制限する統制が整備されている。（FFIEC Information Security Work Program（FFIEC 情報セキュリティワークプログラム）、目標 I: 4-1）
	進化途上（Evolving）		✓ 各種ツールによって、従業員および第三者のパッチが適用されていない機器からのアクセスの試行は自動的にブロックされる。 ✓ 各種ツールによって、登録されていない機器による社内ネットワークへのアクセスの試行は自動的にブロックされる。 ✓ 組織には、許可のない新規接続の追加を防止するための統制がある。 ✓ 権限のない個人によるリムーバブルメディアへの機密データのコピーを防止するための統制が整備されている。 ✓ エンドポイント機器（例：ワークステーション、ラップトップおよ

			びモバイル機器など）には、ウィルス対策ツールおよびマルウェア対策ツールが展開されている。 ✓ 組織のデータにアクセスできるモバイル機器は、一元的に管理してウィルス対策やパッチの適用を行っている。（*この項目は、モバイル機器が使用されていない場合は、適用されない） ✓ 組織は、モバイル機器が紛失または盗難にあった場合には、その機器上にあるデータをリモートから削除している。（*この項目は、モバイル機器が使用されていない場合は、適用されない）
	中程度 **（Intermediate）**		✓ インバウンド通信およびアウトバウンド通信で、データの損失を防止するための制御または機器を実装している。（例：電子メール、FTP、Telnet、大容量のファイル転送の防止など） ✓ モバイル機器の管理には、整合性スキャン（例：ジェイルブレーク/ルート化された端末の検知）が含まれる。（*この項目は、モバイルデバイスが使用されていない場合は、適用されない） ✓ 会社の情報の保存や情報にアクセスするために企業ネットワークに接続しているモバイル機器では、リモートからのソフトウェアバージョン/パッチの検証が可能である。（*この項目は、モバイル機器が使用されていない場合は、適用されない）
	高度 **（Advanced）**		✓ 最新のセキュリティパッチが適用されていない従業員および第三者の機器（モバイル機器を含む）は、その機器にネットワークへのアクセスを許可する前に隔離され、パッチが適用される。 ✓ モバイル機器上の機密データおよびアプリケーションは、セキュアな、分離されたサンドボックスまたはセキュアコンテナを介してのみアクセスされる。

	革新 **（Innovative）**		✓ 一元的に管理されたエンドポイント管理ツールは、完全に統合されたパッチ、構成および脆弱性管理を提供する一方で、マルウェアを侵入時に検知し、悪用を防止する。
セキュアコーディング	**ベースライン** **（Baseline）**		✓ 組織に勤務している開発者は、業界標準を満たす、システム開発ライフサイクル（SDLC）の一環としてプログラムのセキュアなコーディングの実務に従っている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、56 ページ） ✓ 社内で開発されたソフトウェアのセキュリティ制御は、定期的に見直され、検査されている（*この項目は、ソフトウェアの開発を行っていない場合は、適用されない）。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、59 ページ） ✓ 社内で開発されたソフトウェアのコードのセキュリティ制御は、そのコードを実稼働環境に移行する前に別個に検査される（*この項目は、ソフトウェアの開発を行っていない場合は、適用されない）。（FFIEC Development and Acquisition Booklet（FFIEC 開発と取得ブックレット）、2 ページ） ✓ 知的財産および実稼働コードは、エスクロウに預託されている（*この項目は、エスクロウに預託されている実稼働コードがない場合は、適用されない）。（FFIEC Development and Acquisition Booklet（FFIEC 開発と取得ブックレット）、39 ページ）
	進化途上 **（Evolving）**		✓ セキュリティの検査は、モバイルアプリケーションを含むすべてのアプリケーションにおいて、SDLC のすべての設計後段階で行われる。（*この項目は、ソフトウェアの開発を行っていない場合は、適用されない）
	中程度 **（Intermediate）**		✓ システムおよびアプリケーションのセキュアな開発の一環として識別された脆弱性を低減するためのプロセスが整備されている。

			✓ インターネットに接続されている Web ベースアプリケーションを含む、アプリケーションのセキュリティは、既知のタイプのサイバー攻撃（例: SQL インジェクション、クロスサイトスクリプティング、バッファオーバーフロー）に対する試験が実施されている。 ✓ ソフトウェアコードの実行ファイルやスクリプトには電子署名を行うことで、ソフトウェアの作成者を確認し、コードが変更または破損されていないことを保証している。 ✓ リスクベースの独立した情報保証機能によって、社内アプリケーションのセキュリティが評価されている。
	高度 **（Advanced）**		✓ 静的コード解析によって識別された脆弱性は、新しく開発されたまたは変更されたアプリケーションを実稼働環境に実装する前に低減される。 ✓ アプリケーションおよびサービス間の相互依存性はすべて識別されている。 ✓ 社内で開発された、またはベンダーによって提供されたカスタムアプリケーションに対してセキュリティギャップがないように、独立したコードレビューが実施されている。
	革新 **（Innovative）**		✓ ソフトウェアコードは、セキュリティ上の脆弱性を設計段階で直ちに解決できるように、開発環境で自動化ツールによって動的にスキャンされる。
評価要素: 検知			
脅威と脆弱性の検知	**ベースライン** **（Baseline）**		✓ 外部向けシステムおよび内部ネットワークのリスク評価に従い、独立した検査（侵入試験や脆弱性スキャンを含む）を実施している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、61 ページ） ✓ 攻撃を検知するために、ウィルス対策ツールおよびマルウェア対策ツールを使用している。（FFIEC Information Security

			Booklet（FFIEC 情報セキュリティブックレット）、55 ページ） ✓ ファイアウォールルールは、少なくとも四半期ごとに監査または検証されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、82 ページ） ✓ 電子メール保護機構を利用して、一般的なサイバー脅威（例：添付されたマルウェアまたは悪意のあるリンク）のフィルタリングを行っている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、39 ページ）
	進化途上（Evolving）		✓ ネットワーク境界と重要な Web 向けアプリケーションの独立した侵入試験を定期的に実施し、セキュリティ制御のギャップを識別している。 ✓ インターネット向けアプリケーションまたはシステムを立ち上げる前または大きな変更を実施する前に、独立した侵入試験を実施している。 ✓ ウィルス対策ツールおよびマルウェア対策ツールは、自動的に更新される。 ✓ ファイアウォールルールは、日常的に更新している。 ✓ 新しい機器または既存の機器を展開または再展開する前に、脆弱性スキャンの実施と分析を行っている。 ✓ データの窃取または破壊につながる可能性がある潜在的なインサイダー活動をモニタリングするプロセスが整備されている。
	中程度（Intermediate）		✓ 監査の人員またはリスク管理の人員が、侵入試験の範囲および結果を検討し、仕事の品質に基づいて試験委託会社のローテーションのニーズを決定する。

			✓ マルウェアを検知し、マルウェアが存在する場合にはブロックするために電子メールおよび添付は自動的にスキャンされている。
	高度 **（Advanced）**		✓ 週次の脆弱性スキャンは、環境間で交代に実施され、1 年を通してすべての環境のスキャンが実施されている。 ✓ 侵入試験には、サイバー攻撃シミュレーションまたはレッドチーム演習など実際の戦術やテクニックあるいはその両方が含まれ、従業員の行動、セキュリティ防御、方針およびリソースにおける統制の不足/欠如が検知される。 ✓ 自動化ツールによって、リスクの高い行為を事前に識別し、インサイダー脅威をもたらす可能性のある任意の従業員が通知される。
	革新 **（Innovative）**		✓ ユーザーのタスクとコンテンツ（例：電子メールの添付ファイルの開封）は、セキュアコンテナまたは仮想環境で自動的に分離されているため、マルウェアを分析することはできるが、マルウェアは組織のネットワークの重要なデータ、エンドポイントのオペレーティングシステム、アプリケーションにアクセスすることはできない。 ✓ 脆弱性スキャンをすべての環境で週次で実施している。
変則的な活動の検知	**ベースライン** **（Baseline）**		✓ 組織は、全環境でのモニタリングによって変則的な活動を検知できる。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、32 ページ） ✓ 変則的な活動アラートが発生する顧客の取引は、モニタリングされ、検証される。（FFIEC Wholesale Payments Booklet（大口決済ブックレット）、12 ページ） ✓ イベント後に物理的アクセスまたは論理的アクセスあるいはその両方のログが検証される。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、73 ページ）

			✓ 第三者による重要なシステムへのアクセスについては、不正または異常な活動の有無がモニタリングされている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット）、26 ページ） ✓ 権限昇格はモニタリングされている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、19 ページ）
	進化途上（Evolving）		✓ 顧客、従業員および第三者の認証時に変則的な振る舞いを自動的に検知するシステムを設置している。 ✓ セキュリティログは、定期的に確認されている。 ✓ ログによって、個々のユーザーによるすべてのシステムへのアクセスの追跡可能性が確保される。 ✓ ログ内で経営陣の対応を必要とする可能性のある活動を特定するために閾値を設定している。
	中程度（Intermediate）		✓ オンラインの顧客取引については、変則的な振る舞いの有無を積極的にモニタリングしている。 ✓ 不正なデータマイニングを検知するためのツールを使用している。 ✓ ツールを利用して、セキュリティログのモニタリングを積極的に行い、設定したパラメータの範囲内の変則的な振る舞いやアラートの有無を確認している。 ✓ 監査ログは、改ざんが困難な、一元的に管理されたログサーバーまたはメディアにバックアップされている。 ✓ セキュリティログ記録の閾値は、定期的に評価されている。

			✓ 多面的な攻撃（例：同時に行われるアカウント乗っ取りとDDoS 攻撃）を検知し、防止するために、変則的な活動と他のネットワークアラートやシステムアラートが、事業部門を横断して相関付けられている。
	高度 **（Advanced）**		✓ 顧客の複数回のログインが物理的に遠い複数のIP 所在地から短い時間内に行われた場合、自動化ツールによって、システムアラートや不正アラートが発動される。 ✓ 顧客のアカウントからの外部転送によって、アラートが生成され、変則的な振る舞いが検知された場合には、検査と承認が要求される。 ✓ 従業員の行動（ネットワークの使用パターン、勤務時間、および既知の機器）をモニタリングし、分析して変則的な活動を通知するシステムが整備されている。 ✓ インサイダー脅威によるデータマイニングを検知して防止する自動化ツールが整備されている。 ✓ データへのアクセス時に起こり得る悪意のある活動について事前にアラートを通知するために、偽の機密データまたはファイルにタグを付けて使用している。
	革新 **（Innovative）**		✓ 組織には、リアルタイムで自動的に脅威のリスクスコアを採点する仕組みがある。 ✓ 組織は、潜在的なインサイダー脅威を検知し、その活動をリアルタイムでブロックする新しいテクノロジーを開発している。
イベント検知	**ベースライン** **（Baseline）**		✓ 通常のネットワーク活動のベースラインが確立されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、77 ページ） ✓ 起こり得る攻撃について経営陣に警告する仕組み（例：ウィルス対策アラート、ログイベントアラートなど）が整備されてい

			る。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、78 ページ） ✓ 不正なユーザー、機器、接続、ソフトウェアの存在の有無をモニタリングするプロセスが整備されている。（FFIEC Information Security Work Program（FFIEC 情報セキュリティワークプログラム）、目標 II: M-9） ✓ 疑わしいシステム活動をモニタリングし、通知する責任が割り当てられている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ 起こり得る不正アクセスを検知するために物理的環境がモニタリングされている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、47 ページ）
	進化途上（Evolving）		✓ 複数の情報源（例: ネットワーク、アプリケーションまたはファイアウォール）からのイベント情報を相関付けるプロセスが整備されている。
	中程度（Intermediate）		✓ 機密データの不正なまたは意図的ではない送信を検知するための統制またはツール（例: データ損失防止など）が整備されている。 ✓ イベント検知プロセスの信頼性は実証済みである。 ✓ インフラストラクチャ全体で重要な資産には、専用のセキュリティモニタリングが使用されている。
	高度（Advanced）		✓ 自動化ツールによって、重要なシステムファイル、ファイアウォール、IPS、IDS またはその他のセキュリティ機器に対する不正な変更が検知される。 ✓ リアルタイムのネットワークモニタリングと検知機能が実装され、

			業界全体のイベント情報が組み込まれている。 ✓ 不正なソフトウェア、ハードウェア、または変更が発生すると、アラートがリアルタイムで自動的に送信される。 ✓ 複数の情報源からのイベント情報を動的に相関付け、設定されたパラメータに基づいてアラートを送信するツールが整備されている。
	革新 **（Innovative）**		✓ 組織は、複数のイベントがまさに発生しようとしている時にリアルタイムで相関付けるイベント検知システムを開発する取り組みを主導している。 ✓ 組織は、潜在的なインサイダー脅威を検知し、活動をリアルタイムでブロックする新しいテクノロジーを設計するための開発の取り組みを主導している。
評価要素：改善			
パッチ管理	**ベースライン** **（Baseline）**		✓ パッチ管理プログラムが実装され、ソフトウェアやファームウェアのパッチは確実に適時に適用されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、62 ページ） ✓ パッチは、システムやソフトウェアに適用される前にテストされている。（FFIEC Operations Booklet（FFIEC 運用ブックレット）、22 ページ） ✓ パッチ管理レポートが検証され、適用漏れのセキュリティパッチが反映される。（FFIEC Development and Acquisition Booklet（FFIEC 開発と取得ブックレット）、50 ページ）
	進化途上 **（Evolving）**		✓ 緊急度に基づいてソフトウェアパッチを取得、テストおよび展開するための正式なプロセスが整備されている。 ✓ システムは、パッチを自動的に取得するように設定されている。

			✓ セキュリティパッチを展開する前に業務上の影響が評価されている。 ✓ 自動化ツールを使用して、適用が漏れているセキュリティパッチと各パッチが提供されてからの経過日数を識別している。 ✓ すべての環境で適用が漏れているパッチを優先して追跡している。
	中程度 **（Intermediate）**		✓ リスクが高い脆弱性用のパッチは、リリース時にテストされ、適用される。適用されない場合は、リスクは受け入れられ、説明責任が割り当てられる。
	高度 **（Advanced）**		✓ オペレーティングシステムソフトウェア、ミドルウェア、データベースおよびその他の主要ソフトウェアの適用が漏れているパッチを識別するために、パッチ監視ソフトウェアが、すべてのサーバーにインストールされている。 ✓ 組織は、パッチ管理レポートをモニタリングし、セキュリティパッチが、アグレッシブな時間枠設定内（例: 0～30 日間）にテストされ、実装されているかを確認している。
	革新 **（Innovative）**		✓ 組織は、セキュリティパッチまたはバグ修正プログラムを開発しているか、使用しているシステムのオープンソースコードの開発に貢献している。 ✓ 実稼働システムをミラーした隔離または分離されたシステムが用意され、迅速なパッチのテストと実装が可能であり、必要に応じた迅速なフォールバックに備えている。
修復	**ベースライン** **（Baseline）**		✓ 評価で識別された問題は、緊急度に基づいて評価レポートに対する回答で設定された時間枠内に優先順位が設定され、解決される（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、87 ページ）

	進化途上 **（Evolving）**		✓ 機器が紛失または盗難にあった場合、あるいはもはや必要なくなった場合には、ハードウェア上およびポータブルメディア/モバイルメディア上のデータは破壊または削除される。 ✓ 侵入試験時に識別された脆弱性を解決するための正式なプロセスが整備されている。
	中程度 **（Intermediate）**		✓ 修復のための取り組みの効果は、フォローアップ脆弱性スキャンの実施により確認される。 ✓ 侵入試験は、繰り返し実施され、中程度、高リスク、悪用可能な脆弱性が解決されたことが検証される。 ✓ 資格のあるスタッフまたは第三者によりセキュリティ調査、デジタルフォレンジック分析、修復が行われる。 ✓ 一般的に受け入れられている、証拠の連鎖を含む適切なデジタルフォレンジック分析プロセスを利用して、今後起こり得る訴訟を裏付けるための証拠を収集して提示する。 ✓ 権限のある個人が承認され、制御されたツールを利用して組織の資産のメンテナンスおよび修理を実施する。 ✓ 組織の資産のメンテナンスおよび修理は、適時、ログに記録される。
	高度 **（Advanced）**		✓ 侵入試験、脆弱性スキャン、およびその他の独立した検査で識別された中程度および高リスクの問題はすべて、適時に解決されない場合には、取締役会または適切な取締役委員会にエスカレーションされ、リスクの容認の可否が審議される。
	革新 **（Innovative）**		✓ 組織は、現在の復旧時間の目標を維持するために、ゼロデイ攻撃によって損傷したシステムを修復するテクノロジーを開発している。

領域4：外部依存関係の管理			
評価要素：外部との接続			
		○、×	
外部接続	**ベースライン（Baseline）**		✓ 外部接続に依存している重要なビジネスプロセスが識別されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、9 ページ） ✓ 組織は、第三者の接続が許可されたものであることを確認している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、17 ページ） ✓ ネットワーク図が用意され、すべての外部接続が識別されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、9 ページ） ✓ データフロー図が用意され、外部企業への情報の流れが文書化されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、10 ページ）
	進化途上（Evolving）		✓ 重要なビジネスプロセスをサポートしている外部接続がマッピングされている。 ✓ ネットワーク図は、第三者との接続が変更された場合、または少なくとも年次で更新されている。 ✓ ネットワーク図およびシステム図は、安全な方法で保存されており、アクセスは適切に制限されている。 ✓ 第三者のプライマリ接続とバックアップ接続は、モニタリングされ、定期的に検査されている。
	中程度（Intermediate）		✓ 検証済み資産のインベントリを基に、データリポジトリ、データの流れ、インフラストラクチャおよび接続を示す包括的な構成

			図を作成する。 ✓ セキュリティ管理は、第三者の接続からの侵入を検知し、防止するように設計され、検証されている。 ✓ モニタリングによる統制は、対象をすべての外部接続（例：第三者サービスプロバイダー、提携先企業、顧客）として網羅している。 ✓ モニタリングによる統制は、対象をすべての内部のネットワーク間接続として網羅している。
	高度 **（Advanced）**		✓ セキュリティアーキテクチャは、ネットワーク接続インフラストラクチャを変更する前に検証され、文書化されている。 ✓ 組織は、第三者サービスプロバイダーと緊密に連携して、外部接続のセキュリティを維持し、改善している。
	革新 **（Innovative）**		✓ 外部接続の図は、対話型であり、ネットワーク接続インフラストラクチャに対するリアルタイムの変更、新規接続、数の増減、リスク発生時のアラートが示される。 ✓ 組織内の接続は、サイバー攻撃による感染を防止するために、瞬時に分割または切断可能である。
評価要素：関係管理			
デューディリジェンス	**ベースライン** **（Baseline）**		✓ 第三者（外部委託会社）の候補企業に対し、契約を締結する前に、バックグラウンド調査、評判、財政状態、安定性、セキュリティ管理を含む、リスクベースのデューディリジェンスを実施している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、69 ページ） ✓ 第三者サービスプロバイダーのリストが保持されている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブッ

			クレット）、19 ページ） ✓ リスク評価が実施され、サービスプロバイダーの重要度が識別されている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット）、6 ページ）
	進化途上 **（Evolving）**		✓ 第三者のサイバーセキュリティ管理の評価を分析するための正式なプロセスがある。 ✓ 取締役会または適切な取締役委員会は、デューディリジェンスの結果の概要を、組織の固有リスクプロファイルに影響を及ぼす第三者の採用に関する経営陣の提案を含めて検証する。
	中程度 **（Intermediate）**		✓ 組織の第三者サービスプロバイダーが、その第三者（例：下請け業者）のデューディリジェンスを実施していることを検証するためのプロセスが整備されている。 ✓ リスクが高いベンダーに対しては、組織または資格のある第三者によって契約前に実地の現地訪問が実施されている。
	高度 **（Advanced）**		✓ 第三者のデューディリジェンス活動においては、継続的なプロセス改善プログラムが整備されている。 ✓ リスクの高いベンダーの監査が年次で実施されている。
	革新 **（Innovative）**		✓ 組織は、効率的で徹底したセキュリティレジリエンス調査につながるデューディリジェンスの仕組みを構築するための業界全体の取り組みを推進している。 ✓ 組織は、監査可能な新しいプロセスを開発し、デューディリジェンスを実施し、第三者によってもたらされるサイバーセキュリティリスクの継続的なモニタリングを実施するための取り組みを主導している。

契約	**ベースライン（Baseline）**		✓ 機密データを処理、保管、または送信するか、重要なサービスを提供するすべての第三者について、関連するセキュリティおよびプライバシーの要件に対応する正式な契約書が取り交わされている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、7 ページ） ✓ 契約書では、第三者が、自身が所有、保管、処理または送信する組織の機密データのセキュリティの責任を負うことを認めている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、12 ページ） ✓ 契約書には、第三者のセキュリティ管理は定期的に見直され、独立した者により検証される旨が定められている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、12 ページ） ✓ 契約書には、万一第三者が定められているセキュリティ要件を満たすことができなかった場合に、組織として遡及して確認できるよう明記されている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット、12 ページ） ✓ 契約書には、セキュリティインシデントに対応する責任が定められている。（FFIEC E-Banking Booklet（E バンキングブックレット）、22 ページ） ✓ 契約書には、契約の終了時のデータの返却または破壊のセキュリティ要件が規定されている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット、15 ページ）
	進化途上（Evolving）		✓ 第三者との接続のセキュリティを確保するための機器（例: ファイアウォール、ルーターなど）管理責任が、契約書に正式に記載されている。 ✓ 直接的および間接的なセキュリティインシデントおよび脆弱性の通知の責任が契約書またはサービスレベル合意書（SLA）に記載されている。

			✓ 契約書には、データを保管または送信できる場所に関する地理的制約事項も定められている。
	中程度 **（Intermediate）**		✓ セキュリティイベントの適時の通知を要求する第三者とのSLA または類似の手段が整備されている。
	高度 **（Advanced）**		✓ 契約書では、第三者サービスプロバイダーのセキュリティ方針が、組織の方針を満たすか、それを上回ることが要求されている。 ✓ 第三者の契約終了/出口戦略が策定され、経営陣と検証されている。
	革新 **（Innovative）**		✓ 組織は、業界にとって重要な第三者の契約要件に影響を及ぼす業界全体の取り組みを推進している。
継続的なモニタリング	**ベースライン** **（Baseline）**		✓ 第三者のリスク評価は、定期的に更新されている。（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット）、3 ページ） ✓ 監査、評価および業績の報告書が取得され、重要な第三者のセキュリティ管理が定期的に検証されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、86 ページ） ✓ 継続的なモニタリングの実務には、重要な第三者のレジリエンス計画の検証も含まれる（FFIEC Outsourcing Booklet（FFIEC 外部委託ブックレット）、19 ページ）
	進化途上 **（Evolving）**		✓ 正式な承認を経ずに確立された新しい関係の識別も含め、新しい第三者との関係を識別するプロセスが整備されている。 ✓ 正式なプログラムによって、第三者のアクセスの継続的な監督責任が割り当てられている。

			✓ 第三者のモニタリングは、そのリスクに応じて深度および頻度の観点から拡大・縮小される。 ✓ 必要な第三者の情報を取得または分析する必要がある時期を識別するための、自動化された注意喚起のための通知や備忘録などが整備されている。
	中程度 **（Intermediate）**		✓ 組織の機密データへの第三者従業員のアクセスは、最小権限の原則に基づいて動的に追跡される。 ✓ リスクの高いベンダーには、定期的な現地評価が実施され、適切なセキュリティ管理が整備されている。
	高度 **（Advanced）**		✓ 第三者がホストするシステムにある機密データへの第三者従業員のアクセスは、自動化されたレポートおよびアラートによって動的に追跡される。
	革新 **（Innovative）**		✓ 組織は、第三者によってもたらされるサイバーリスクを継続的にモニタリングするための新しい監査可能なプロセスを開発するための取り組みを主導している。

領域5：サイバーインシデント管理とレジリエンス			
評価要素：インシデントレジリエンスに関する計画策定と戦略			
		○、×	
計画策定	**ベースライン（Baseline）**		✓ 組織は、サイバーインシデントに対する対処・対応方法を文書化している。（FFIEC Business Continuity Planning Booklet（事業継続性計画策定ブックレット、 4 ページ） ✓ 従業員が情報セキュリティイベントについて適時に報告するための手段を提供するために通信チャネルが設けられている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ インシデント対応チームの各人員の役割と責任が定義されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ） ✓ 対応チームには、広範な経歴と専門知識/技術を持つ、組織の異なる分野（例：経営陣、法務、広報、情報技術）の複数の個人が含まれている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ） ✓ 重要なすべての事業分野について、正式なバックアップおよび復旧計画が用意されている。（FIEC Business Continuity Planning Booklet（FIEC 事業継続性計画策定ブックレット、 4 ページ） ✓ 組織は、事業継続性プログラム、災害復旧プログラムおよびデータバックアッププログラムを利用してインシデント後に業務を復旧することを計画している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、71 ページ）

	進化途上 **（Evolving）**		✓ 修復計画およびプロセスには、低減施策、リソース、および時間パラメータの概要が記載されている。 ✓ 企業の災害復旧計画、事業継続性計画、危機管理計画には、サイバーインシデントについての考慮事項が組み込まれている。 ✓ 妥当な期間内で重要な活動を継続するために代替プロセスが確立されている。 ✓ 事業影響度分析も、サイバーセキュリティを含むように変更されている。 ✓ インシデント時またはインシデント後に組織の支援を要請する可能性のある技術提供会社、コンサルタント、フォレンジックサービス会社に対し、デューディリジェンスを実施している。
	中程度 **（Intermediate）**		✓ サイバー攻撃時または攻撃後に社内外の利害関係者と協力し、コミュニケーションを取るための戦略が整備されている。 ✓ インターネット向けシステムに対する攻撃によって影響を受ける可能性がある重要な機能やサービスを、ルート変更または置き換える計画が整備されている。 ✓ 低減の取り組みを迅速に支援するインシデント対応企業またはプロバイダーとの直接的な提携契約、または契約上の取り決めが用意されている。 ✓ 組織または他の企業に対する実際のサイバーインシデントや攻撃から学んだ教訓を基に、リスク低減機能や対応計画を向上している。
	高度 **（Advanced）**		✓ サイバーインシデントに対応し、そこから復旧するための方策は、各事業部門の災害復旧計画、事業継続計画、危機管理計画全体に緊密に組み込まれている。

			✓ 破壊的でさまざまな悪影響を及ぼす可能性のあるサイバーインシデント後に業務を維持し、影響を最小限に抑え、復旧するために、包括的なサイバーレジリエンスプログラムには複数のシステム、プログラムまたはプロセスが実装されている。 ✓ レジリエンス計画を継続的に改善するためのプロセスが整備されている。
	革新 **（Innovative）**		✓ インシデント対応計画は、サービスの中断からの復旧、データの完全性の保証、サイバーインシデント後に損失、破壊されたデータの復旧を確保するように設計されている。 ✓ インシデント対応プロセスには、自動化された対応のための詳細なアクションおよびルールベースのトリガーが含まれている。
検査	**ベースライン** **（Baseline）**		✓ シナリオを利用して、インシデントの検知と対応を改善している。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、71 ページ） ✓ 事業継続性検査には、重要な第三者との協力が必要となる。（FFIEC Business Continuity Planning Booklet（FFIEC 事業継続性計画策定ブックレット）、J-6 ページ） ✓ システム、アプリケーションおよびデータ復旧は、少なくとも年次で検査されている。（FFIEC Business Continuity Planning Booklet（FFIEC 事業継続性計画策定ブックレット）、J-7 ページ）
	進化途上 **（Evolving）**		✓ 復旧シナリオには、データ破壊やデータの完全性、データの損失およびシステムやデータの可用性への影響から復旧するための計画が含まれる。 ✓ 一般に広く報道されたサイバー攻撃を基に、組織の対応を評価し、向上させている。 ✓ 情報のバックアップは、定期的に検査され、それらのバックアップ

			がアクセス可能であり、読み取り可能であることが確認されている。
	中程度 **（Intermediate）**		✓ サイバー攻撃シナリオは分析され、重要なビジネスプロセスに対する影響が想定される。 ✓ 組織は、業界別のサイバー演習またはシナリオ（例: FS-ISAC の決済処理会社に対するサイバー攻撃（CAPP）演習）に参加している。 ✓ レジリエンス検査は、現実的に発生する可能性が高い脅威のほか、組織が直面している新しい脅威および顕在化しつつある脅威の分析や識別に基づいて実施されている。 ✓ 重要なオンラインシステムやプロセスは、長期間にわたる運用に対するレジリエンスが検査される(例:DDoS)。 ✓ サイバーイベント演習の結果は、インシデント対応計画や自動トリガーの改善に利用される。
	高度 **（Advanced）**		✓ レジリエンス検査は、包括的なものであり、重要なすべての事業部門間で調整される。 ✓ 組織は、他企業へ実行された既知で高度な攻撃に類似したサイバーイベントが発生した場合に、自組織が復旧できることを確認する。 ✓ インシデント対応検査では、攻撃者の視点から組織を評価し、組織または重要な第三者組織の資産が標的にされる方法を特定する。 ✓ 組織は、サイバーセキュリティレジリエンス検査時に発見された問題の根本原因を是正する。 ✓ 重大な財政的損失を伴うサイバーセキュリティインシデントのシナリオを基に、組織のリスク管理のストレステスト（健全性検

			査）を実施している。
	革新 **（Innovative）**		✓ 組織は、サイバーインシデントに備えて異なる処理センターまたはテクノロジーシステム間で、業務の中断、生産性やデータの損失を伴うことなく、ビジネスプロセスまたは機能を移転する能力を検査している。 ✓ 組織は、ゼロデイ攻撃によって損傷したシステムを修復して、現在の復旧時間の目標を維持することが可能であることを確認している。 ✓ 組織は、より現実的な検査環境を開発している。 ✓ サイバーインシデントシナリオを利用して、業界全体の財政的損失を想定したストレステストを実施している。
評価要素：検知、対応および低減			
検知	**ベースライン** **（Baseline）**		✓ サイバーセキュリティインシデントを検知するために、低減措置を促すアラートパラメータが設定されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、43 ページ） ✓ システムパフォーマンスレポートには、情報セキュリティインシデントを検知するためのリスク指標として利用できる情報が含まれている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、86 ページ） ✓ インシデントを検知し、アラートを送信し、インシデント対応プログラムを発動するためのツールおよびプロセスが整備されている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ）
	進化途上 **（Evolving）**		✓ 組織は、インサイダーの可能性がある活動を検知して、その活動がデータの窃取または破壊につながる兆候が見られる場合に、インシデント対応チームに警告するプロセスを有している。

	中程度 **（Intermediate）**		✓ 変則的な振る舞いや攻撃パターンまたはシグネチャが検出された場合には、インシデント対応プログラムが発動される。 ✓ 組織は、攻撃者がシステムを横断し、足掛かりをつくって情報の窃取などを行って、データやシステムに損傷を与える前に、侵入を検知する能力を有している。 ✓ インシデントは、対応できる適切な人員へのインスタントアラートを含む自動化されたプロセスを通してリアルタイムで検出される。 ✓ 多面的攻撃（例：同時に行われる DDoS 攻撃とアカウント乗っ取り）の検知と防止を向上するために、ネットワークアラートとシステムアラートが事業部門を横断して相関付けられている。 ✓ インシデント検知プロセスでは、企業全体のイベントを相関付けることができる。
	高度 **（Advanced）**		✓ 企業全体の脅威指標によって外部的および内部的脅威の可能性が示されている場合に、インシデントを検知し、インシデント対応チームに特定のタスクを通知するアラートを送信する高度な適応型テクノロジーが展開されている。 ✓ 資産のリスクに基づいて専門的なセキュリティモニタリングを行い、インシデントを検知し、インシデント対応チームにリアルタイムでアラートを送信するために、自動化されたツールが実装されている。
	革新 **（Innovative）**		✓ 組織は、ゼロデイ攻撃を検知しブロックして、経営陣およびインシデント対応チームにリアルタイムで通知することができる。
対応と低減	**ベースライン** **（Baseline）**		✓ インシデントを封じ込め、制御し、顧客情報へのさらなる不正アクセスや不正利用を防止するために適切な措置が講じられている。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ）

	進化途上 **（Evolving）**		✓ インシデント対応計画は、インシデントを優先順位付けすることで、重大なサイバーセキュリティインシデントまたは脆弱性に対して迅速な対応を可能にするように設計されている。 ✓ インシデントを封じ込め、最小限のサービス中断で業務を復旧するために役立つプロセスが整備されている。 ✓ 複数のインシデントタイプ（例: DDoS、マルウェア）に対して封じ込め戦略および低減戦略が策定されている。 ✓ プロセスには、封じ込め戦略が含まれており、影響を受けた可能性のある第三者に通知する。 ✓ 第三者にインシデントが発生した場合に、インシデント対応プログラムを発動するプロセスが整備されている。 ✓ インシデント調査および低減を裏付ける記録が生成される。 ✓ 組織は、必要に応じて第三者に低減サービスの提供を要請する。 ✓ イベントの分析を基に、組織のセキュリティ対策および方針を改善する。
	中程度 **（Intermediate）**		✓ セキュリティインシデントの分析は、侵入の早期の段階で行い、インシデントの影響を最小限に抑える。 ✓ システム/アプリケーションや、インシデント管理に必要なアクセス権限の変更は、実装される前に経営陣によって審査され、正式に承認される。 ✓ セキュリティインシデントによって影響を受け、使用可能な状態に戻すことができない資産を、隔離し、取り外して、廃棄または交換、その両方を確実に行うためのプロセスが整備されている。

			✓ 復旧した資産を適切に再構成し、稼働状態に戻す前に徹底した検査を実施するためのプロセスが整備されている。
	高度 **（Advanced）**		✓ インシデント時には、インシデント管理部門は、サイバー脅威情報部門と効果的に協働する。 ✓ 脅威情報、ネットワーク運用、インシデント対応間の連携によって、起こり得るインシデントに対する事前の対応を可能にしている。 ✓ 技術的な対策では、ディープパケットインスペクションやブラックホール技術などの多層防御技術を適用して検知し、変則的な進入トラフィックまたは退出トラフィックパターン、DDoS 攻撃あるいはその両方に関連したネットワークベースの攻撃に適時に対応する。
	革新 **（Innovative）**		✓ 組織の重大なサイバーインシデントに対するリスク管理によって、重要なサービスの中断はゼロに抑えている。 ✓ リスク低減からバックアップ環境（例：エアギャップ環境およびプロセス）まで、テクノロジーインフラストラクチャは、実稼働環境に対するサイバー攻撃の影響を制限するように設計されている。
評価要素：エスカレーションと報告			
エスカレーションと報告	**ベースライン** **（Baseline）**		✓ インシデントを分析して対応する責任を負う人員に連絡するプロセスが存在する。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、83 ページ） ✓ 組織が顧客の機密情報への不正アクセスまたは不正利用に関わるインシデントの発生に気付いた場合に、必要に応じて、顧客、規制当局、法執行機関に報告するプロセスが存在する（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、84 ページ）

			✓ 組織は、セキュリティインシデントまたは違反に関する年次報告書を作成し、取締役会または適切な取締役委員会にエスカレーションする。（FFIEC Information Security Booklet（FFIEC 情報セキュリティブックレット）、5 ページ） ✓ インシデントは、分類され、ログに記録され、追跡される（FFIEC Operations Booklet（FFIEC 運用ブックレット）、28 ページ）
	進化途上 **（Evolving）**		✓ サイバーインシデントまたは脆弱性を取締役会および上級役員にエスカレーションするための基準が、そのリスクの想定される影響および緊急度に基づいて確立されている。 ✓ 規制当局、法執行機関およびサービスプロバイダーは、組織がシステムへの不正アクセスに気付いた場合、またはサービスの品質の低下につながるサイバーインシデントが発生した場合には、必要に応じて通知する。 ✓ 追跡したサイバーインシデントは相関付けし、傾向分析や報告を行う。
	中程度 **（Intermediate）**		✓ リスク（例：不正、ビジネスレジリエンス）の低減に必要不可欠な従業員は、インシデント発生時のエスカレーションにおける自身の職務を認識している。 ✓ 連絡計画は、第三者を含む他の組織にインシデントについて通知する際に利用する。 ✓ 外部連絡計画は、該当する場合に報道組織にインシデントについて通知する際に利用する。
	高度 **（Advanced）**		✓ 組織は、サイバーセキュリティインシデント対応プロセスに対して定量的な指標と定質的な指標を確立している。 ✓ サイバーインシデントとイベントの概要に関する詳細な指標、ダッシュボードまたはスコアカードが、経営陣に提供され、取締役

			会の議案の一部になっている。
	革新 **（Innovative）**		✓ 経営陣および重要な従業員に複数の通信チャンネルを介してインシデントに関する即時の通知を送信し、追跡や受取の確認もできる仕組みが整備されている。

出典：アセスメントツール p.19～p.57

II. 国内金融機関へあてはめる際の課題

Ⅰ章では、アセスメントツールの概要をみてきた。Ⅱ章では、アセスメントツールに内在する問題点を整理し、仮に将来的に同様のアセスメントツールを我が国金融機関へあてはめる場合の課題を導出する。なお、アセスメントツールをあてはめる際の問題点などについては、国内外の金融機関へのインタビューを通じ、意見を聴取した。

図表 II-1　インタビュー先一覧

業態	インタビュー先
預金取扱金融機関	金融機関 A
	金融機関 B
	金融機関 C
	金融機関 D
	金融機関 E
	金融機関 F
米国商業銀行	金融機関 G

出典：NTT データ経営研究所にて作成

1. アセスメントツールの位置付け

我が国金融機関では、金融 ISAC や金融情報システムセンター（FISC）などの外部機関が公表する情報などを踏まえ、独自のリスクプロファイルを行ったうえで、機能や商品・サービス単位で自組織のサイバーセキュリティ対策を施している。また、場合によっては、IT ベンダーなどに当該作業の一部を委任している場合もある。ただし、業界に共通するリスクであっても、講ずべき対策が個々の金融機関のリスクプロファイルに依存するため、同じ業界内であっても必ずしも同一レベルで対策が施されるとは限らない。また、我が国の金融当局がモニタリングを通じて個々の金融機関の対策の有用性や実効性を評価しようとしても、金融機関ごとのリスクプロファイルが異なれば、業界共通要素の認識や行政としてのコントローラビリティ確保が困難となりかねない。

アセスメントツールの利点は、金融機関自身が、新商品・新サービスの提供に際して、固有リスクプロファイルの変化を容易に検証できるところにある。これにより、金融機関は自組織のサイバーセキュリティ対策について、対策の強化の必要性や対策のレベルを「業界共通の尺度」により判断できる。あわせて、業界共通の尺度であるアセスメントルールが浸透すれば、我が国金融当局としても金融機関に対するモニタリングを通じた評価が容易となり、金融機関のコントローラビリティを確保しやすくなると考えられる。

このように、アセスメントツールは我が国金融機関のみならず、金融当局も活用しやすく、かつ客観的な評価に耐えうる業界標準として位置付ける必要がある。

ただし、自組織での運用に任せられているはずのアセスメントツールが金融当局から提供された場合、金融機関は「参考資料ではなく、活用しなければならないツール」として受け止める可能性が高い。つまり、金融当局がアセスメントツールを公表すると、アセスメントツールを活用した評価が金融機関に事実上義務付けられることとなり、金融機関の自主的な判断に委ねられているはずのアセスメントツール本来の利点が薄れることとなる。また、義務化された場合、金融機関のリスク管理の高度化が目的にもかかわらず、アセスメントツールを使っての評価自体が目的化することになりかねず、本来の目的の趣旨から外れるおそれがある。

このような懸念から、アセスメントツールを我が国金融機関にあてはめる場合には、金融当局からの公表という形式ではなく他の外部組織、たとえば、金融情報システムセンター（FISC）や一般社団法人金融 ISAC といった第三者組織からの提供が一案として考えられる。これにより、金融機関ごとにリスクレベルの調整や対策の決定を個々の事情に即して行うことが可能となると考えられる。

なお、既に NIST からも同様のフレームワークがアセスメントツールとして公表されている。アセスメントツールは金融機関向けのフレームワークであり、NIST のフレームワークと必ずしも一致している訳ではない。そのため、公表手法によっては、金融機関は両方のアセスメントを実施しなければならず負担が増大するおそれがある。したがって、第三者組織からの提供であってとしても、その活用のあり方についての丁寧な説明がなされることが望ましい。

インタビューにて頂戴したご意見１

- 金融庁からこのような評価ツールが出ると、評価すること自体が目的化してしまう可能性がある。（金融機関 A）
- 監督当局がアセスメントツールを提供することで強制力が生じてしまうと、組織でリスクレベルを調整できる利点が薄れてしまうのではないか。（金融機関 G）
- アセスメントツールをサイバーセキュリティ意識の高い金融機関向けに、公表することは良いことに感じる。しかしながら、金融庁から公表すると義務化されてしまうため、例えば当局以外の機関から参考資料として公表するのが良いのではないか。（金融機関 A）
- NIST のフレームワークと必ずしも一致している訳でもないため、両方のアセスメントを実施しなければならず負担である。（金融機関 G）

サイバー攻撃の技術が日々進化・高度化するなか、金融機関におけるサイバーセキュリティの導入技術の陳腐化スピードも速く、投資対効果を期待する金融機関にとっては悩ましい環境が続いている。したがって、アセスメントツールにより現状とあるべき姿とのギャップを把握できたとしても、外部環境変化の著しさから、将来的なセキュリティ対策の万全性を保証するツールにはなりえないと考えられる。そのため、アセスメントツールに

より課題認識が容易となったとしても、自組織が講ずべき具体的かつ効果の高い対策に悩むという状況は変わらないと考えられる。

アセスメントツールはサイバーセキュリティに対する現状レベルの把握と対策を施すべき対象を特定するうえでは有用であるが、評価結果や現状の対応状況とのギャップへの対策は、金融機関の判断に委ねられる。実際、インタビューを通じて、アセスメントツールを活用して自組織のサイバーセキュリティ成熟度が可視化できたとしても、それがサイバーセキュリティ対策の万全性を示すものではないとの意見が聞かれた。

これらを踏まえると、同様のアセスメントツールを仮に国内に導入する場合は、金融機関における利用目的及び制約要因、カバーしていない検討領域、といった点を明確に示すことが肝要となる。

インタビューにて頂戴したご意見 2

- アセスメントツールを用いてセキュリティ対策の対応実施の可視化を行っても、セキュリティ対策の万全性を表すものとは別の話である。ある一定の基準を突破したとしても、それでセキュリティが万全とは言い切れないのではないか。（金融機関 B)
- サイバー攻撃は日々高度化しているため、サイバーセキュリティ対策のゴールが描けない。（金融機関 D)

2. アセスメントツールの活用の在り方

（1）評価から対策検討へのスムースな移行メカニズムを実装すること

アセスメントツールは、金融機関ごとの固有リスクを明らかにした上で、サイバーセキュリティの成熟度を図っていくものである。しかし、金融機関におけるサイバーセキュリティ対策を示唆する機能は有していない。

したがって、評価結果が金融機関のリスクマネージメントプログラムの評価プロセスに乗らず、その結果が活用されないおそれがある。そのため、アセスメントツールにおいて、サイバーリスク（攻撃者、攻撃の目的、事象、想定されるリスクや被害など）に対する、チャネルごとの有意な事例を示すことにより、金融機関を対策検討プロセスへと容易に進めさせるための配慮が求められる。

なお、あまりにも具体的な対策をアセスメントツールに記載してしまうと、そのセキュリティ対策を実施すること（ソリューション導入等）自体が目的化しかねないため、記載粒度への留意も必要である。

インタビューにて頂戴したご意見 3

- 評価結果に対し、どのような対策を行えばよいか分からないと実質的には評価に留まってしまうのではないか。（金融機関 E)
- どのようなサイバーセキュリティ対策を、いつまでに講ずるべきかゴールがないため動きづらい。対策水準のようなものを定義してもらった方が動き易い。（金融機関 F)
- 具体的な事例があると、評価した後の対応を検討しやすい。（金融機関 C)
- 対応を基準化してしまうと、特定のソリューションを入れることが目的化してしまうのは問題である。（金融機関 A)

（2）成熟度レベル判定ロジックの柔軟な設定

アセスメントツールは、成熟度レベルを機械的に判定している点が特徴である。ところが、セキュリティ成熟度の評価において各項目の各成熟度レベルに到達するためには、その成熟度レベルと、それ以前の成熟度レベルで定義されている内容を全て達成しなければならない。そのため、成熟度レベル達成に注力しなければならない状況が発生してしまい、他の投資案件よりも優先される結果、金融機関の本来業務を含め本来投資すべき事案への投資余力が乏しくなるおそれや、本来業務における投資の優先順位が下がってしまうおそれも否定出来ず、ひいては金融機関の競争力を損ないかねない。

そのため、我が国において成熟度レベルの判定ロジックを検討する際には、この点を考慮する必要がある。具体的には、このような歪みが発生しないよう、各固有リスクに対応する成熟度レベルは参照程度にとどめ、各金融機関の置かれている状況に応じて柔軟に紐付けできる余地を残すべきである。

インタビューにて頂戴したご意見 4

- ベースラインの項目を 100%達成しないと次のレベルに行けないと整理されている等の評価の仕方に疑問を感じる。最優先で対応しなければいけなくなることで、本来投資すべき項目に投資できなくなる可能性がある。（金融機関 A)
- 監督当局がアセスメントツールを提供することで強制力が生じてしまうと、組織でリスクレベルを調整できる利点が薄れてしまうのではないか。（金融機関 G)

3. 評価項目や数値基準の在り方

（1）理解しやすい評価項目の定義

評価項目自体に抽象的な表現が多く、自組織がどのレベルにあてはまるか判断しづらいという意見も聞かれた。実際米国では、自組織では判断しづらい部分も含め、外部専門家やコンサルタントの知見を導入しつつ、評価作業を実施する例も存在している。

アセスメントツールの導入にあたっては、金融機関における評価作業自体の負担軽減を実現する必要がある。したがって、評価項目や基準そのものから抽象的な表現や誤謬を排除したツールの構築が肝要である。また、アセスメントツールは、機能や商品といった評価項目について、必ずしも金融機関のサービスが網羅的に捕捉されたうえで合理的に整理されているとは言えない。

我が国金融機関が活用しやすいツールとするうえでは、我が国の実情に照らし合わせたうえで金融機関の機能や外部依存関係、商品ラインナップなどを網羅的に取り上げ、わかりやすく整理された評価項目を設定し、個々の評価項目における具体的な事例の例示等により、金融機関が活用しやすい体系を構築する必要がある。

インタビューにて頂戴したご意見 5

- 評価すること自体難しいのではないか。評価項目については、判断が難しい設問もあるため、あまり知識のない人は難しいかもしれない。（金融機関 A)
- アセスメントツールの評価項目が抽象的であるため、具体的な例示があると、評価した後の対応を検討しやすい。（金融機関 C)
- 自分たちがどのくらいできるかは把握できるが、それがどのレベルなのか判断材料のために例示がほしい。その例示がないと、外部への説明ができないため、第三者評価に頼らざるを得ない可能性がある。（金融機関 C)

（2）ベンダーとの関係やシステム等の環境の違いを反映した評価基準等の妥当性の確保

我が国金融機関のうち、とりわけ中小規模の金融機関は情報システムの開発・保守・運用を IT ベンダーに依存しており、サイバーセキュリティ対策の一部を IT ベンダーに依存せざるを得ない状況にある。米国においては、サイバーセキュリティ対策は金融機関側の責任と認識されているが、我が国金融機関向けにアセスメントツールをあてはめるうえでは、金融機関と IT ベンダーとの責任分界点が曖昧になっている点を考慮する必要がある。

また、米国と日本ではシステム等の環境(システム構成や運用体制等)も異なるため、評価項目で定義されている数値は日本に合う数値や水準・基準に定義し直す必要がある。仮に我が国金融機関にあてはめるうえでは、アセスメントツールのフィージビリティの確保に向け、FFIEC と同様、公表前に試験的に特定の金融機関におけるプレ評価作業を実施し、想定している評価項目などに潜在化する問題点を炙り出し、数値基準などの精緻化を図るべきである。

インタビューにて頂戴したご意見 6

- IT ベンダーがリスク評価を引き受けられる制度があっても良い。8 割程度はベンダーが担当し、金融機関はリスクマネジメントやガバナンスに注力できるようなものができれば面白い。金融機関と

IT ベンダーの役割分担を整理できれば良い。（金融機関 A）

- システム開発は外部委託せざるを得ない部分があるが、銀行としての責任意思は存在している。外部委託しているから、銀行側が免責されるという考えはない。（金融機関 G）
- ベンダーにガバナンスやインテリジェンスを任せることは難しく、運用（コントロール）を任せることが妥当ではないか。（金融機関 A）
- 米国と日本では環境も異なるため、評価項目で定義されている数値（アプリ数など）を見直す必要がある。セキュリティ評価をプレ的に実施してみても良いかもしれない。（金融機関 C）

（3）IT ベンダーを巻き込んだ検討

アセスメントツールに基づく評価結果の活用は、各金融機関が独自に定義するリスクマネージメントプログラムによって決定される。自らを取り巻く環境や事業戦略によってリスク許容度は異なることから、仮に同じ評価結果であったとしても、金融機関ごとに講ずべき対策も異なる。そのため、アセスメントツールの設計に際しては、評価後の対策を一律に強制するようなものではなく、リスクベースアプローチに基づき個々の金融機関の判断に委ねるべきである。評価結果に応じて講ずべき対策を具体的に定義して公表した場合、本来であれば各金融機関の方針に基づく個々の対応が促されるべきところが、公表された基準への適合自体が目的化されてしまうおそれもある。

したがって、アセスメントツールによる評価後の具体的な対策の検討は、個々の金融機関が定義するリスクマネージメントプログラムに含まれるべきものと解釈したうえで、評価結果をリスクマネージメントプログラムの評価プロセス上で検討していく仕組み自体が重要視されるべきである。

なお、我が国金融機関とりわけ中小規模金融機関の多くは、IT ベンダーが提供する共同システムを利用している。したがって、情報システムの対応を伴うサイバーセキュリティ対策には、IT ベンダーの関与が必須となっている。そのため、アセスメントツールを導入する際には、情報システムへの技術的対応や情報システムの監視については IT ベンダーが担い、リスクマネジメントや IT ガバナンスあるいは意思決定を金融機関側が担うという実態に合わせた役割分担が可能となるよう考慮すべきである。

インタビューにて頂戴したご意見 7

- 結果を受けて、どこまで対応するかは、「リスク管理」として別の枠組みで実施すべきものと考えている。どこまでリスクを許容するかが重要であるため、ツールだけでは終わらない。（金融機関 A）
- 経営環境や戦略によって各金融機関が取るべきスタンスは異なるはずであり、FISC の安全対策基準のように、各金融機関が取るべきスタンスは異なるはずである。（金融機関 A）
- リスク評価し、優先順位をつけて、どのようなタイムスケジュールで対応していくかを内部で検討していくことが重要なはずである。評価プロセス自体が金融機関に存在することが、評価されるべきである。

（金融機関 A）

- アセスメントツールはあくまでサイバーセキュリティ対策の対応状況を評価するものであり、結果やギャップへの対策は各金融機関の判断に委ねられている。（金融機関 G）
- 評価結果を基に対策を策定することに苦戦していることは確かである。（金融機関 G）
- 評価結果に対し、どのような対策を行えばよいか分からないと実質的には評価に留まってしまうのではないか。（金融機関 E）
- 中小金融機関ではベースラインレベルの対策を講ずることも難しいのではないか。（金融機関 A）
- 攻撃の定義ひとつみても、自分たちだけでは判断できない場合もあるが、専門部隊と外部コンサルにノウハウがあるためカバーできている。（金融機関 G)

4. サイバーセキュリティの対応態勢

CISO や CIO といった役員レベルもさることながら、サイバーセキュリティの対応要員の確保は、サイバーセキュリティ態勢を整備する上での課題となっている。

中小規模の金融機関の多くでは、人員の制約から組織内 CSIRT の設置まで至っておらず、他の組織の人員が当該業務として求められる機能を兼務により担っている。大規模金融機関を除く中小金融機関において、人的リソースの不足により情報システムを所掌する部署がサイバーセキュリティへの対応を兼務する例が多いのが実態だ。他方、フィナンシャルグループとして複数のグループ企業を抱える大手金融機関では、グループ内組織として CSIRT を設置する例もあり、この場合、グループ内金融機関に共通する課題に対し、共通リソースで一元的に対応することを可能としている。

これらから、アセスメントツールが提供された場合であっても、その評価作業自体に人的リソースを割くことができない金融機関が出てくることが想像できる。したがって、業界団体などがアセスメントツールの評価作業をサービスプログラムとして各金融機関に提供し、その結果を踏まえ各金融機関が具体的な対策の検討に着手する、といった業界を挙げた取組態勢も一考の余地があるだろう。

インタビューにて頂戴したご意見 8

＜サイバーセキュリティ体制の人数＞

- 今年度からシステム統括部下にサイバーセキュリティ管理グループという専任グループを設けた。13 名＋グループの IT 会社で体制構築している。（金融機関 B）
- 事務統括部システム企画グループが CSIRT として活動しており、3 名＋責任者の計 4 名体制である。（金融機関 D）
- 事務管理課の 2 名で対応している。（金融機関 E）
- 組織内 CSIRT の体制構築まで至っておらず、業務部事務課 2 名で担当している。

（金融機関 F）

＜体制構築の状況＞

- フィナンシャルグループにて CSIRT を組織し、日本 CSIRT 協議会へ加盟している。（金融機関 B）
- IT 部門の業務と兼務しているため、他業務があると CSIRT 業務が回らなくなることから、専任での組織が望ましいと感じている。（金融機関 C）
- 専門のセキュリティ部隊を組成し、セキュリティ監視等を行っている。役割に応じてチームを複数組成し、経験のある専門家を採用している。中小のセキュリティベンダー程度の人員数を確保しており、人員は増加傾向にある。（金融機関 G）

III. まとめ

以上のとおり、FFIEC の公表したアセスメントツールの有用性については一定程度確認出来た。体系や評価メカニズムの多くが合理的な視点で定義されており、業態にかかわらず金融機関が利用しやすいツールとなっている。

ただし、アセスメントツールをそのまま我が国に導入し、金融機関向けにあてはめることは困難であると考えられる。まずは我が国の金融メカニズムや商品ラインアップ、金融機関の IT ベンダーへの依存関係を踏まえた改変が必要である。また、回線数やアプリケーション数などの数値条件を評価尺度として導入しているが、我が国の実態に合わせてその根拠を改めて定義する必要がある。加えて、義務的位置付けによる金融機関側の負担増大に配意すべく、金融当局ではなく FISC などの第三者機関が公表すべきとの声も聞かれた。

我が国においても金融機関を取り巻く現下のサイバー攻撃の脅威を念頭に、我が国金融機関にあてはめるにあたってのメリット、デメリットを十分に考慮した上で、金融機関の負荷軽減を実現しつつ、金融機関におけるサイバーセキュリティ対策に資する有意なアセスメントツールの構築を検討すべきである。

以　上