**質問表別紙（第二種金融商品取引業用）**

**Questionnaire Sheet (for Type II Financial Instruments Business)**

※以下の事項について、該当する社内規則に基づいて、当社の対応の概要を記載すること。

なお、該当しない場合は、「該当なし」と記載すること。

\*Provide a summary of your response to the following matters in accordance with your relevant company rules. Put “Not applicable.” for any item that is not applicable to you.

７．システムリスク管理態勢（監督指針Ⅲ－２－８）

7. Control environment for managing information technology risk (Guidelines for Supervision III-2-8)

（１）主な着眼点

(1) Major Supervisory Viewpoints

①　システムリスクに対する認識等

イ．取締役会等において、システムリスクが十分認識され、全社的なリスク管理の基本方針が策定されているか。

ロ．取締役会等は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。

ハ．取締役会等は、システムリスクの重要性を十分に認識した上で、システムに関する十分な知識・経験を有し業務を適切に遂行できる者を、システムを統括管理する役員として定めているか。

ニ．取締役会等は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。
また、必要に応じて自らが指揮を執る訓練を行う等して、その実効性を確保しているか。

(i) Recognition of information technology risk

A. Whether the board of directors has formulated a basic policy for company-wide management of information technology risk based on a full recognition of information technology risk.

B. Whether the board of directors recognizes that prevention and efforts for speedy recovery from system troubles and cybersecurity incidents (hereinafter referred to as "system trouble, etc.") is an important issue and has developed an appropriate control environment.

C. Whether the board of directors fully recognizes the importance of information technology risk and has designated a person who has sufficient knowledge on and experience in computer systems and who is able to appropriately execute business as an officer that manages computer systems.

D. Whether the board of directors has specified in detail the responsibilities to be fulfilled and the measures to be taken at a time of crisis in which system trouble, etc. occurs.
In addition, whether it ensures the effectiveness of the responsibilities and measures by, for example, providing training under its leadership as needed.

②　適切なリスク管理態勢の確立

イ．システムリスク管理の基本方針が定められ、管理態勢が構築されているか。システムリスク管理の基本方針には、セキュリティポリシー（組織の情報資産を適切に保護するための基本方針）及び外部委託先に関する方針が含まれているか。

ロ．システムリスク管理態勢の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。

また、システムリスク管理態勢は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。

(ii) Establishment of Appropriate Control Environment for Risk Management

A. Whether the Financial Instruments Business Operator has specified a basic policy for the management of information technology risk and developed a relevant control environment. Whether the basic policy for the management of information technology risk includes a security policy (a basic policy for appropriately protecting the organization’s information assets) and a policy on outsourced contractors.

B. Whether the Financial Instruments Business Operator has developed its control environment for managing information technology risk based on guides that allow it to judge the objective levels of the details of the control environment.

In addition, whether the Financial Instruments Business Operator has constantly reviewed the control environment for managing information technology risk according to identification and analysis of system trouble, etc., risk management implementation results, and technological progress, etc.

③　システムリスク評価

システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。

また、洗い出したリスクに対し、十分な対応策を講じているか。

(iii) Assessment of information technology risk

Whether the division managing information technology risk recognizes and assesses risks periodically and in a timely manner by recognizing the fact that risks are becoming diversified due to changes in the external environment, such as seen in the examples of system troubles induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad based impact.

Also, whether it is taking sufficient measures to address the risks that have been identified.

④　情報セキュリティ管理

イ．情報資産を適切に管理するために方針の策定、組織体制の整備、社内規則の策定、内部管理態勢の整備を図っているか。また、他社における不正・不祥事件も参考に、情報セキュリティ管理態勢のＰＤＣＡサイクルによる継続的な改善を図っているか。

ロ．情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、管理者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。

ハ．コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。

ニ．金融商品取引業者が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。

顧客の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。

・通常の業務では使用しないシステム領域に格納されたデータ

・障害解析のためにシステムから出力された障害解析用データ

・ＡＴＭ（店舗外含む）等に保存されている取引ログ 等

ホ．洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。

また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。

・情報の暗号化、マスキングのルール

・情報を利用する際の利用ルール

・記録媒体等の取扱いルール 等

ヘ．顧客の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。

・職員の権限に応じて必要な範囲に限定されたアクセス権限の付与

・アクセス記録の保存、検証

・開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 等

ト．機密情報について、暗号化やマスキング等の管理ルールを定めているか。

また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。

なお、「機密情報」とは、暗証番号、パスワード、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。

チ．機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。

リ．情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。

ヌ．セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む）を行っているか。

(iv) Management of information security

A. Whether the Financial Instruments Business Operator has developed a policy to appropriately manage information assets, prepared organizational readiness, introduced in-house rules, and developed an internal control environment. Also, whether it is making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of incidents or lapses at other companies.

B. Whether the company is managing information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity and availability of information. Also, whether the individuals responsible for information security are tasked to handle the security of system, data and network management.

C. Whether the company is taking measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses.

D. Whether the Financial Instruments Business Operator identifies important customer information it is responsible for protecting in a comprehensive manner, keeps its records and manages them. Whether the Financial Instruments Business Operator, in identifying important customer information, has set business operations, systems and external contractors as the scope of protection and includes data, such as listed below, in the scope where it tries to identify those calling for protection.

-Data stored in the areas within the system that are not used in ordinary operations

-Data output from the system for analyzing system troubles

-Transaction logs stored in ATMs (including those outside of branches), etc.

E. Whether the Financial Instruments Business Operator is assessing importance and risks regarding important customer information that has been identified.

Also, whether it has developed rules to manage information, such as those listed below, in accordance with the importance and risks of each piece.

-Rules to encrypt or mask information

-Rules for utilizing information

-Rules on handling data storage media, etc.

F. Whether the Financial Instruments Business Operator has introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as listed below, for important customer information.

-Provision of access authorizations that limits access to the scope necessary for the person's responsibility

-Storage and monitoring of access logs

-Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, administrators and those responsible for operations, etc.

G. Whether the Financial Instruments Business Operator has introduced rules for controlling confidential information, such as encryption and masking. Also, whether it has introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs.

Note that "confidential information" refers to information, such as PIN, passwords, credit card information, etc., whose misuse could lead to losses by customers.

H. Whether the Financial Instruments Business Operator give due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, of confidential information, and treats such information in a stricter manner.

I. Whether the Financial Instruments Business Operator periodically monitors its information assets to see whether they are managed properly according to management rules, etc. and reviews the control environment on an ongoing basis.

J. Whether the Financial Instruments Business Operator conducts security education (including by external contractors) to all officers and employees in order to raise awareness of information security.

⑤　サイバーセキュリティ管理

イ．サイバーセキュリティについて、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、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

ロ．サイバーセキュリティについて、組織体制の整備、社内規則の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。

・サイバー攻撃に対する監視体制

・サイバー攻撃を受けた際の報告及び広報体制

・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制

・情報共有機関等を通じた情報収集・共有体制 等

ハ．サイバー攻撃に備え、入口対策、内部対策、出口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ているか。

・入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入 等）

・内部対策（例えば、特権ＩＤ・パスワードの適切な管理、不要なＩＤの削除、特定コマンドの実行監視 等）

・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断 等）

ニ．サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。

・攻撃元のＩＰアドレスの特定と遮断

・DDoS 攻撃に対して自動的にアクセスを分散させる機能

・システムの全部又は一部の一時的停止 等

ホ．システムの脆弱性について、ＯＳの最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

ヘ．サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

ト．インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。

・可変式パスワードや電子証明書などの、固定式のＩＤ・パスワードのみに頼らない認証方式

・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証

・ハードウェアトークン等でトランザクション署名を行うトランザクション認証 等

チ．インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。

・取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供

・利用者のパソコンのウィルス感染状況を金融商品取引業者側で検知し、警告を発するソフトの導入

・電子証明書をＩＣカード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用

・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備 等

リ．サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

ヌ．サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

(v) Management of cybersecurity

A. Whether the board of directors, etc. recognizes the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment.

B. Whether the Financial Instruments Business Operator has introduced systems to maintain cybersecurity, such as listed below, in addition to making the organization more secure and introducing in-house rules.

-Monitoring systems against cyberattacks

-Systems to report cyberattacks and public-relation systems when attacks occur

-Emergency measures by Computer Security Incident Response Teams and systems for early detection

-Systems of information collection and sharing through information-sharing organizations, etc.

C. Whether the Financial Instruments Business Operator has introduced a multi-layered defence system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control and outbound perimeter control.

-Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, Instruction Detection System, Instruction Protection System etc.)

-Security measures for internal network security control (e.g. proper management of privileged IDs/passwords, deletion of unnecessary IDs, monitoring of execution of certain commands, etc.)

-Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

D. Whether measures such as listed below are implemented to prevent damage from expanding when cyberattacks occur

-Identification of IP addresses from which the cyberattacks originate and blocking off of attacks

-Functions to automatically spread out accesses when under DDoS attacks

-Suspension of the entire system or its part, etc.

E. Whether necessary measures for vulnerabilities in the system, such as updating of the operating system and application of security patches, are introduced in a timely manner.

F. Whether the Financial Instruments Business Operator is, as part of cybersecurity measures, assessing its security levels by taking advantage of tests on network intrusion, vulnerability scanning or penetration tests, etc. and making efforts to improve security.

G. Whether the Financial Instruments Business Operator, when executing transactions using communication methods such as the Internet without any face-to-face contact, has introduced appropriate authentication methods in line with the risks associated with such transactions, such as listed below.

-Authentication methods that do not rely on fixed IDs/passwords, such as variable passwords and digital certificates

-Transaction authentication through multiple channels by using, for example, devices other than the PC web browser used in transactions, such as a mobile phone

-Transaction authentication using transaction signatures by means of a hardware token, etc.

H. Whether the Financial Instruments Business Operator, when executing transactions using communication methods without any face-to-face contact, such as the Internet, has introduced preventative measures in line with operations, such as listed below.

-Provision of security software that allows the user to detect and remove viruses, etc. when executing transactions

-Introduction of software that allows the Financial Instruments Business Operator to detect virus infection of the user's PC and issue a warning

-Adoption of methods to store digital certificates in mediums or devices separate from PCs used in transactions, such as IC cards

-Introduction of a system that allows the Financial Instruments Business Operator to detect unauthorized log-ins, abnormal transactions, etc. and immediately notify such anomalies to users

I. Whether the Financial Instruments Business Operator has developed contingency plans against potential cyberattacks, conducts exercises and reviews such plans. Also, whether it participates in industry-wide exercises as necessary.

J. Whether the Financial Instruments Business Operator has formulated plans to train and expand the personnel responsible for cybersecurity and implements them.

⑥　システム企画・開発・運用管理

イ．経営戦略の一環としてシステム戦略方針を明確にした上で、中長期の開発計画を策定しているか。また、中長期の開発計画は、取締役会の承認を受けているか。

ロ．現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行っているか。

ハ．開発案件の企画・開発・移行の承認ルールが明確になっているか。

ニ．開発プロジェクトごとに責任者を定め、開発計画に基づき進捗管理されているか。

ホ．システム開発に当たっては、テスト計画を作成し、ユーザー部門も参加するなど、適切かつ十分にテストを行っているか。

ヘ．人材育成については、現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施しているか。

(vi) System planning/development/management

A. Whether the Financial Instruments Business Operator has clearly established a policy for system strategy as part of its business strategy and developed medium- to long-term development plans. Also, whether such medium- to long-term development plans are approved by the board of directors.

B. Whether the Financial Instruments Business Operator is making continuous efforts to identify the risks inherent in the current system and making scheduled investment to maintain and improve it.

C. Whether rules to authorize plans, development and transitions of development projects are clearly established.

D. Whether individuals responsible for development projects are designated and progress of the development plans are managed accordingly.

E. Whether the Financial Instruments Business Operator works out plans to test the system and its system development efforts and conducts tests in an appropriate and sufficient manner, such as by involving user divisions in them.

F. Whether the Financial Instruments Business Operator works out specific plans for the current system structure and development technology to be inherited and to train specialized personnel, and implements them

⑦　システム監査

イ．システム部門から独立した内部監査部門において、定期的なシステム監査が行われているか。

ロ．システム関係に精通した要員による内部監査や、システム監査人等による外部監査の活用を行っているか。

ハ．監査の対象はシステムリスクに関する業務全体をカバーしているか。

ニ．システム監査の結果は、適切に取締役会等に報告されているか。

(vii) Computer system audits

A. Whether an internal audit section that is independent from the computer system division conducts periodic audits of the computer system.

B. Whether the Financial Instruments Business Operator conducts internal audits by subject matter about computer systems and is taking of external audits by information system auditors.

C. Whether the audited division accounts for all business operations involving information technology risk.

D. Are the results of computer system audits properly reported to the board of directors?

⑧　外部委託管理

イ．外部委託先（システム子会社を含む。）の選定に当たり、選定基準に基づき評価、検討の上、選定しているか。

ロ．外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続、提供されるサービス水準等を定めているか。また、外部委託先の役職員が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。

ハ．システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。

システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。

ニ．外部委託した業務（二段階以上の委託を含む）について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。

また、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。

(viii) Management of outsourcing of business operations

A. Whether the Financial Instruments Business Operator is assessing outsourced contractors (including system-related subsidiaries) against selection standards, giving careful consideration and selecting them.

B. Whether the Financial Instruments Business Operator sets out division of roles and responsibilities with outsourced contractors, supervising authority of auditors, procedures to renew contracts, level of services provided, etc. in outsourcing contracts. Also whether the Financial Instruments Business Operator presents to outsourced contractors rules their officers and employees are required to adhere to and security requirements, as well as defines them in contract forms, etc.

C. Whether risk management is carried out properly in outsourced system-related work (including work further subcontracted). In particular, whether the Financial Instruments Business Operator has risk management arrangements and procedures that have been developed with full awareness that a higher level of risk management is required when there are multiple outsourced contractors as the management work becomes more complicated.
And whether risk management is carried out properly in system-related office functions contracted out, as in system-related work.

D. Whether the Financial Instruments Business Operator, as a consigner, periodically checks to confirm that outsourced work (including work further subcontracted) is carried out appropriately.
Also, whether there is a system that allows the consigner to monitor and track the status of customer data being processed at outsourced contractors.

⑨　コンティンジェンシープラン

イ．コンティンジェンシープランが策定され、緊急時体制が構築されているか。

ロ．コンティンジェンシープランの策定に当たっては、その内容について客観的な水準が判断できるもの（例えば「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編））を根拠としているか。

ハ．コンティンジェンシープランの策定に当たっては、災害による緊急事態を想定するだけではなく、金融商品取引業者の内部又は外部に起因するシステム障害等も想定しているか。
また、バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定しているか。

ニ．コンティンジェンシープランは、他の金融機関におけるシステム障害等の事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。

ホ．コンティンジェンシープランに基づく訓練は、全社レベルで行い、外部委託先等と合同で、定期的に実施しているか。

ヘ．業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害等が発生した場合に、速やかに業務を継続できる態勢を整備しているか。

(ix) Contingency Plan

A. Whether the Financial Instruments Business Operator has formulated a contingency plan and has established arrangements and procedures for dealing with emergencies.

B. Whether the Financial Instruments Business Operator is basing the details of its contingency plan on guides that allows it to judge objective levels of its details (such as "Guide to Formulate Contingency Plans at Financial Institutions" compiled by the Center for Financial Industry Information Systems).

C. Whether the Financial Instruments Business Operator, in developing a contingency plan, assumes not only contingencies due to natural disasters but also system troubles, etc. due to internal or external factors.

Also, whether it assumes risk scenarios of sufficient extent for cases such as a major delay in batch processing.

D. Whether the Financial Instruments Business Operator reviews assumed scenarios in its contingency plan by, for example, taking into consideration case studies of system troubles at other financial institutions and results of deliberations at the Central Disaster Management Council, etc.

E. Whether exercises in accordance with the contingency plan involve the entire company and are periodically conducted jointly with outsourced contractors, etc.

F. Whether off-site backup systems, etc. are introduced for important systems whose failure could seriously affect business operations, and that a control environment is in place to address disasters, system troubles, etc. so that normal business operations can be speedily brought back.

⑩　システム統合リスク・プロジェクトマネジメント

イ．金融商品取引業者の役職員は、システム統合リスクについて十分認識し、そのリスク管理態勢を整備しているか。

ロ．テスト体制を整備しているか。また、テスト計画はシステム統合に伴う開発内容に適合したものとなっているか。

ハ．業務を外部委託する場合であっても、金融商品取引業者自らが主体的に関与する態勢を構築しているか。

ニ．システム統合に係る重要事項の判断に際して、システム監査人による監査等の第三者機関による評価を活用しているか。

ホ．不測の事態に対応するため、コンティンジェンシープラン等を整備しているか。

x) System Integration Risk / Project Management

A. Whether the Financial Instruments Business Operator has developed a control environment for managing system integration risk by ensuring that its officers and employees fully recognize the risk.

B. Whether the Financial Instruments Business Operator has established arrangements and procedures for conducting tests. Whether its test plan is suited to the nature of the system development necessitated by the system integration.

C. Whether the Financial Instruments Business Operator has established a control environment that enables itself to be proactively involved in the system integration when this task is outsourced.

D. Whether the Financial Instruments Business Operator makes use of third-party evaluation, such as evaluation by a system auditor, when making judgment regarding important matters related to the system integration.

E. Whether the Financial Instruments Business Operator has developed a contingency plan for dealing with an unexpected incident.

⑪　障害発生時の対応

イ．システム障害等が発生した場合に、顧客に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。

また、システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢となっているか。

ロ．システム障害等の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。

ハ．経営に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに代表取締役をはじめとする取締役に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。

また、必要に応じて、対策本部を立ち上げ、代表取締役等自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。

ニ． システム障害等が発生した場合、障害の内容・発生原因、復旧見込等について必要に応じて公表するとともに、顧客からの問合せに的確に対応するため、コールセンターの開設等を迅速に行っているか。

また、システム障害等の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。

ホ．システム障害等の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。

また、システム障害等の原因等の定期的な傾向分析を行い、それに応じた対応策をとっているか。

へ．システム障害等の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。

ト．システム障害等が発生した場合、速やかに当局に報告する体制が整備されているか。

(xi) Actions to System Troubles

A. Whether the Financial Instruments Business Operator is prepared to implement appropriate measures to avoid causing unnecessary confusion among customers when system troubles, etc. occur and take actions to speedily recover the system or activate alternative measures.
Also, whether it has developed a worst-case scenario in preparation for system troubles and is prepared to take necessary measures accordingly.

B. Whether the Financial Instruments Business Operator has prepared procedures that also subjects outsourced contractors to reporting system troubles, and has a clearly defined system of command and supervision.

C. Whether the Financial Instruments Business Operator is prepared to immediately notify the representative director and other directors when a system trouble that may significantly affect business operations occurs, and report the largest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect customers, the reporting persons should not underestimate the risk but immediately report the biggest risk scenario).
In addition, whether it is prepared to launch a task force, have the representative director issue appropriate instructions and orders, and seek resolution of the issue in a swift manner.

D. When system trouble, etc. occurs, whether the Financial Instruments Business Operator publicizes the details of the trouble, the cause of occurrence, expectation of restoration, etc. as needed, and promptly establishes a call center to precisely respond to inquiries from customers.
In addition, whether the method and contents of information provision to related business divisions have been made clear to prepare for the occurrence of system trouble, etc.

E. Whether the Financial Instruments Business Operator precisely carries out investigation of the cause of the system trouble, etc., investigation of the impact the system trouble, etc. has until the restoration, improvement measures, measures to prevent recurrence, etc.
Also, whether it periodically analyzes tendencies of factors that have led to system trouble, etc. and introduces measures to address them.

F. Whether the Financial Instruments Business Operator has developed a systemic mechanism, such as circumventing the troubled part, in order to minimize the impact of system trouble, etc.

G. Whether the Financial Instruments Business Operator has established arrangements and procedures for immediately reporting system trouble, etc. to the authorities.