清算・振替機関等向けの総合的な監督指針　新旧対照表（案）

改正案	現行
Ⅲ．監督上の評価項目と諸手続（清算機関）	Ⅲ．監督上の評価項目と諸手続（清算機関）
Ⅲ－３　業務の適切性	Ⅲ－３　業務の適切性
Ⅲ－３－４　システムリスク管理	Ⅲ－３－４　システムリスク管理
（２）主な着眼点 ①～④　（略） ⑤　サイバーセキュリティ管理 ア．取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。 （削除） （削除）	（２）主な着眼点 ①～④　（略） ⑤　サイバーセキュリティ管理 ア．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。 イ．サイバーセキュリティについて、組織体制の整備、社内規則等の策定のほか、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 ウ．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。

改正案	現行
	・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）
（削除）	エ. 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
（削除）	オ. 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。
（削除）	カ. 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。
イ.　（略）	キ. インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務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
	・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

改正案	現行
ウ.　（略）	ク．インターネット等の通信手段を利用して業務を行う場合には、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 ・参加者のパソコンのウィルス感染状況を清算機関側で検知し、警告を発するソフトの導入 ・電子証明書を IC カード等、当該業務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・異常な入力等を検知し、速やかに参加者に連絡する体制の整備　等
（削除）	ケ．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。
（削除）	コ．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。
Ⅳ．監督上の評価項目と諸手続（資金清算機関）	Ⅳ．監督上の評価項目と諸手続（資金清算機関）
Ⅳ－３　業務の適切性	Ⅳ－３　業務の適切性
Ⅳ－３－４　システムリスク管理	Ⅳ－３－４　システムリスク管理
（２）主な着眼点 ⑤　サイバーセキュリティ管理	（２）主な着眼点 ⑤　サイバーセキュリティ管理

改正案	現行
ア．取締役会又は理事会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。	ア．サイバーセキュリティについて、取締役会又は理事会等は、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。
（削除）	イ．サイバーセキュリティについて、組織体制の整備、規則等の策定のほか、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
（削除）	ウ．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）
（削除）	エ．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

改正案	現行
	・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
（削除）	オ．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。
（削除）	カ．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。
イ．　（略）	キ．インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務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 ・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
ウ．　（略）	ク．インターネット等の通信手段を利用して業務を行う場合には、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。 ・参加者のシステムのウィルス感染状況を資金清算機関側で検知し、警告を発するソフトの導入 ・電子証明書を IC カード等、当該業務に利用しているシステムとは別の媒体・機器へ格納する方式の採用 ・不正なログイン・異常な入力等を検知し、速やかに参加者に連絡する体制の整備　等

改正案	現行
（削除）	ケ．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。
（削除）	コ．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．監督上の評価項目と諸手続（振替機関）	Ⅴ．監督上の評価項目と諸手続（振替機関）
Ⅴ－３　業務の適切性	Ⅴ－３　業務の適切性
Ⅴ－３－４　システムリスク管理	Ⅴ－３－４　システムリスク管理
（２）主な着眼点	（２）主な着眼点
⑤サイバーセキュリティ管理	⑤　サイバーセキュリティ管理
ア．取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。	ア．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。
（削除）	イ．サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、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

改正案	現行
（削除）	ウ. 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）
（削除）	エ. 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
（削除）	オ. 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。
（削除）	カ. 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。
イ.　（略）	キ. インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務のリスクに見合った適切な認証方式を導入しているか。

改正案	現行
	・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 ・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
ウ.　（略）	ク. インターネット等の通信手段を利用して業務を行う場合には、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。 ・口座管理機関等のパソコンのウィルス感染状況を振替機関側で検知し、警告を発するソフトの導入 ・電子証明書を IC 電子証明書を IC カード等、当該業務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・異常な入力等を検知し、速やかに口座管理機関等に連絡する体制の整備　等
（削除）	ケ. 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。
（削除）	コ. 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。
Ⅵ. 監督上の評価項目と諸手続（取引情報蓄積機関）	Ⅵ. 監督上の評価項目と諸手続（取引情報蓄積機関）
Ⅵ－３　業務の適切性	Ⅵ－３　業務の適切性
Ⅵ－３－４　システムリスク管理	Ⅵ－３－４　システムリスク管理

改正案	現行
（２）主な着眼点 ⑤サイバーセキュリティ管理 ア．サイバーセキュリティについて、取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。 （削除） （削除）	（２）主な着眼点 ⑤サイバーセキュリティ管理 ア．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。 イ．サイバーセキュリティについて、組織体制の整備、社内規則等の策定のほか、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 ウ．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）

改正案	現行
（削除）	エ．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
（削除）	オ．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。
（削除）	カ．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。
イ．　（略）	キ．インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務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 ・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
ウ．　（略）	ク．インターネット等の通信手段を利用して業務を行う場合には、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。 ・利用者のパソコンのウィルス感染状況を取引情報蓄積機関側で検知し、警告を発するソフトの導入 ・電子証明書を IC 電子証明書を IC 電子証明書を IC カード等、当該業務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

改正案	現行
	・不正なログイン・異常な入力等を検知し、速やかに利用者に連絡する体制の整備　等
（削除）	ケ．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。
（削除）	コ．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。