

平成13年9月12日  
金 融 庁

柳澤金融担当大臣談話

1. 日本時間の昨夜、米国において発生した同時多発テロに関連し、金融庁としては9月11日午後11時30分をもって、金融庁長官を本部長とする対策本部を設置したところである。
2. 当庁としては、金融システムの維持に万全を期すため、日本銀行及び海外金融市場当局等とも緊密に連携を図りつつ、事態に適切に対処していくこととしている。
3. 本日の我が国の株式市場及び金融先物市場については、我が国市場の信頼性を維持する必要があること、また、欧州市場でも基本的に通常どおりの取引が行われたことから、通常どおり、開場することとした。
4. なお、株式市場に不測の混乱が生じないよう、東京証券取引所等においては、制限値幅を通常の2分の1とする措置を講じるものと聞いている。
5. 市場参加者におかれては、冷静な対応をお願いしたい。

以上

平成13年9月25日  
金 融 庁

### 米国における同時多発テロを踏まえた対応について

9月11日の米国における同時多発テロの発生を受けて、当庁としては、同日、金融庁長官を本部長とする対策本部を設置し、状況の把握及び対応等に努めてきたところであるが、政府対処方針（9月12日安全保障会議）、「米国における同時多発テロへの対応に関する我が国の措置について」（9月19日テロ対策関係閣僚会議決定）及びG8首脳声明（9月19日）等を踏まえ、こうしたテロ事件等が金融システムに与える影響を最小化するとともに、テロ防止の観点から、当面以下の措置を講ずることとする。

#### 1. 金融システムの維持

- (1) 金融システムの維持に万全を期すため、日本銀行及び海外金融市場当局等と緊密に連携を図りつつ、引き続き適切に対処する。
- (2) 特に、バーゼル銀行監督委員会（BCBS）、証券監督者国際機構（IOSCO）、保険監督者国際機構（IAIS）を通じ、有事の際における金融監督者間の連絡体制について一層の強化を図る。

#### 2. タリバーン関係者等に対する資産凍結等

今般、外務省、財務省、経済産業省は、国連安全保障理事会決議（1267号及び1333号）に基づき、タリバーン関係者等に対し、外国為替及び外国貿易に関する法律による資産凍結等の措置を講じたところであるが、当庁としても所管金融機関に対しその遵守について周知徹底を図る。

#### 3. マネー・ローンダリング対策等

マネー・ローンダリング対策については、平成12年に組織的犯罪処罰法が施行され、犯罪収益に係る疑わしい取引の届出制度が整備されたところであるが、テロ資金が犯罪収益から来ている場合マネー・ローンダリングの問題として対応可能であることから、特に以下の点について重点的に対応する。

- (1) 現行のマネー・ローンダリングをチェックする体制を活用し、上記2.の措置の対象となるタリバーン関係者等と関連する疑いのある取引については、

犯罪収益の疑いのある取引として届出を行うよう金融機関に対し要請する。  
また、金融機関から届出のあった犯罪収益に係る疑わしい取引に関する情報について整理・分析を行い、捜査に役立つ情報を捜査機関等へ提供する。

(2) 犯罪収益に係る疑わしい取引に関する情報について、外国当局との間で国際的な情報交換の二国間取極めの締結を推進する。

(3) テロ資金供与対策については、テロ資金供与防止条約の年内署名を前提に、同条約の早期実施に向けて、金融機関等に対する「テロ資金に係る疑わしい取引の届出」等の義務づけ等につき、関係省庁におけるテロ資金供与等の犯罪化に係る検討と連携して検討を進める。

#### 4. 不公正取引の監視

(1) 米国の同時多発テロに関連して、不公正な証券取引が行われていなかったかどうかについて、証券取引等監視委員会において東京証券取引所・大阪証券取引所とも連携して調査を行っており、仮に取引の公正性を害すると疑われる事例が認められれば、事実関係を解明する等、適切に対応する。

(2) 不正取引監視についての国際的な協力体制の整備を図る。このため、市場監督当局者間の情報交換取極めを速やかに締結する。

#### 5. 金融機関における危機管理体制等

防犯・防災対策等の整備については、従来から金融検査マニュアル等に基づき厳正にチェックを行ってきたが、今般の事件を踏まえ危機管理に万全を期するため、特に以下の点について改めて要請及び周知徹底を図る。

- ① 不穏な情報を入手した際や有事発生時における治安当局との連携確保、
  - ② テロ事件を未然に防止するための体制の整備、特に、コンピュータシステムの安全性を脅かす行為を防止するため、入退室管理・重要鍵管理等、適切かつ十分な管理を行うほか、サイバーテロ等ネットワークを通じたコンピュータ犯罪に対して十分に留意した体制を整備し、点検等の事後チェック体制を整備、
  - ③ 有事における、被災軽減及び業務継続のための体制整備、特に、イ) 重要データ等の避難場所をあらかじめ確保するほか、バックアップの取得、分散保管、隔地保管等保管場所に留意した管理方法の整備、ロ) コンピュータシステムのコンティンジェンシー・プラン（緊急時対応計画）の整備、
- 等。

(以上)