サイバー時代の内部統制と三線防御モデル

石　島　　隆

要　旨

サイバー時代の環境に適合した組織体の内部統制を構築し運用するためには、「三線防御モデル」の下でITを利用して、組織体内部の情報のみでなく、サイバースペース上の情報を有効に活用することが必要となる。その際の情報インテグリティのリスクを軽減するためには、メタ情報を用いて共通のコンテキストの中で情報を目的に合致させることが必要である。今後、各組織体においては、自らの事業環境の下におけるサイバーリスクの意味を改めて問い直し、サイバー攻撃の防御とサイバースペース上の情報の有効活用の両面から取り組むことが求められる。

キーワード：内部統制（Internal Control）、サイバーリスク（Cyber Risk）、三線防御モデル（The Three Lines of Defense Model）、人工知能（Artificial Intelligence）、情報インテグリティ（Information Integrity）

I　はじめに

今日の企業をはじめとするさまざまな組織体は、事業の多様化とグローバル化、取引の複雑化や件数の増大により、様々なリスクに晒されている。リスクに対処し、サステイナブルな経営を行っていくためには、環境変化を認識したリスク評価を行い、有効な内部統制を構築し運用することが必要である。

ここに内部統制とは、「事業体の取締役会、経営者及びその他の構成員によって実行され、業務、報告及びコンプライアンスに関連する目的の達成に関して合理的な保証を提供するために整備された１つのプロセス」である（COSO 2013）。

内部統制における IT の利用は、従来、基幹業務システム上の機能として開発されるものや IT ツールを用いた基幹業務システム上のデータの分析が中心であったが、インターネットの飛躍的な発展、分析技術の革新により、基幹業務システムの枠を超えた機能の開発や企業内外の各種の非構造化データの活用も可能となっている。

一方、リスクマネジメントの体制として、三線防御モデルが提唱されている。第一線はビジネスのフロントを所管する部門における業務管理であり、第二線は経営者が設置したリスク管理、コンプライアンス及びコントローラの機能であり、さらに、第三線は執行部門から独立した内部監査機能である。そして、これらの各段階において IT の利用を進める必要がある。

さらに、サイバー時代の到来は、日常生活に大きな影響を与え始めており、組織体においてもセキュリティ面のリスクが増大する反面、サイバースペース上の情報の活用により大きな効用がもたらされることが期待されている。そこで本稿では、このような環境変化に対応する内部統制の方向性について検討する（石島 2016）。

Ⅱ　サイバー時代の内部統制

2.1　サイバー時代の持つ意味

サイバースペース（cyber space）とは、「サイバネティクス（cybernetics）」と「スペース（space）」を組み合わせた混成語であり、通信ネットワーク上やコンピュータの中につくられた仮想空間を意味し、電脳空間とも訳される（ASCII.jp 2016）。ここにサイバネティクスとは、「生物と機械における制御と通信を統一的に認識し、研究する理論の体系」である（デジタル大辞泉 2016 b）。

そして現在、サイバー（cyber）は、「他の語に付いて、インターネットが形成する情報空間（サイバースペース）に関連した、の意を表す」語素として使用されている（デジタル大辞泉 2016a）。

したがって、サイバー時代とは、サイバースペースが人間社会に大きな影響力を持つようになり、通信ネットワークやコンピュータに代表される機械が人間とともに社会を構成する時代を表している。

2.2 サイバー時代の情報処理プロセスにおけるリスク

サイバー時代の情報処理プロセスにおけるリスクについて、リスクの発生する箇所を模式的に示した第１図に基づいて検討したい。

まず、SaaS（Software as a Service）の利用を前提とすると、情報システムのユーザは、クラウドサービス（第１図の「クラウドサービス１」）上のアプリケーションプログラムにアクセスして情報処理を行い、必要な情報を取得する。そのクラウドサービス自身も他のクラウドサービス（第１図の「クラウドサービス２」）にアクセスして情報の交換を行っている。

その際には、まずユーザ自身の頭（人工知能や bot を含む）の中に目的やコンテキストがあり、これがクラウドサービスの目的やコンテキストと合致している必要がある。さらに、そのクラウドサービス自身が連携する他のクラウドサービスとの目的やコンテキストの合致も必要となる。

一方では、これらの情報処理システムを構成するユーザ、プログラム、データベース、ネットワークのそれぞれに様々なリスクが存在する。

まず、ユーザの目的やコンテキストとクラウドサービスが提供する機能や情報の内容が合致しないリスク、クラウドサービス間の連携において目的やコンテキストが合致しないことにより情報処理の目的が達成されないリスクなど、目的やコンテキストに関連するリスクがある。

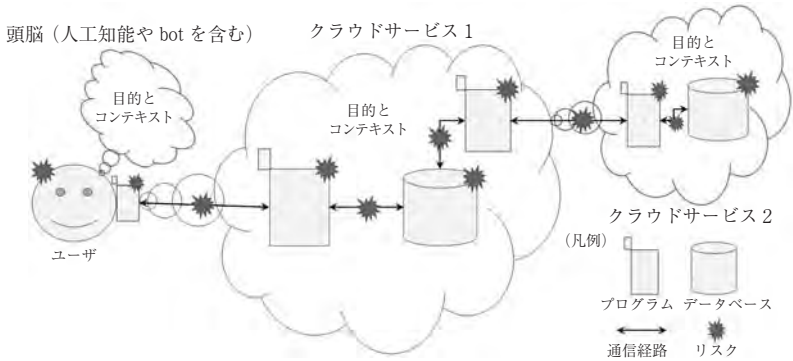
また、サイバー攻撃者がユーザになりすまして攻撃を仕掛けるリスク、不正なプログラムがインストールされ実行されるリスク、データベースの改ざんや情報漏洩のリスク、ネットワークの障害をもたらす攻撃のリスクなど、

サイバー攻撃に伴うリスクがある。

この他、アクセス権限の設定ミス等で正当なユーザがアクセスできないリスク、プログラムのバグに伴うリスク、データベース内のデータの誤謬に伴うリスク、ネットワークの障害に伴うリスクなど、従来からの情報システムの構築と運用に関連するリスクのほか、自然災害に伴うリスクも挙げられる。

サイバー時代の内部統制は、このようなサイバー時代の情報処理プロセスにおけるリスクを前提として、構築し運用する必要がある。

第１図　サイバー時代の情報処理プロセスとリスク



（出典）著者作成。

Ⅲ　サイバー時代の内部統制

3.1　内部統制を取り巻く環境変化

米国 COSO の『内部統制の統合的フレームワーク2013年改訂版』においては、次のようなビジネス環境の変化に伴ってフレームワークを強化したとしている（COSO 2013, p. 8）。

・市場や事業のグローバル化

・ビジネスプロセスの複雑性の増大

・法律・規則・規制・基準の要求と複雑性

・進化する技術の活用と依存

・不正の防止と検知への期待

上記の中で「進化する技術の活用と依存」が挙げられているが、ここにおける技術とはIT（Information Technology）を意味しており、さらにサイバー犯罪、サイバーテロが深刻化する現在の状況に対応するため、*COSO IN THE CYBER AGE* と称する報告書が作成・公表された（COSO 2015）。

3.2　サイバーリスクに対応するための内部統制の構成要素

(1)　COSO 内部統制の統合的フレームワークにおける17の原則

前掲の COSO のフレームワークでは、有効な内部統制を構築し運用する

第１表　COSO 内部統制の統合的フレームワークにおける17の原則

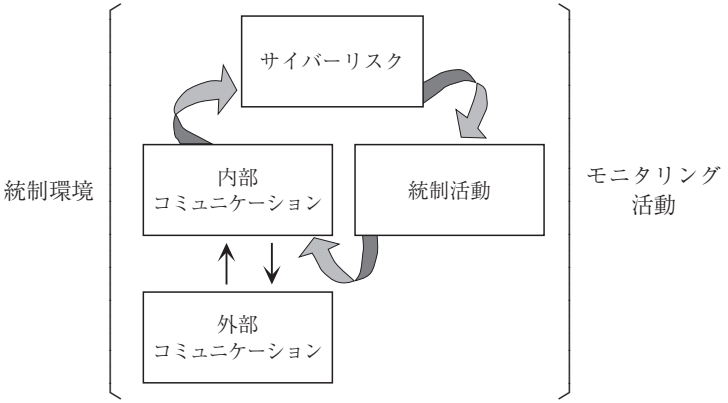
区分	原則の要約
統制環境	1. 誠実性と倫理的価値へのコミットメント 2. 取締役会の経営者からの独立性と、内部統制の構築と実施の監視 3. 経営者による組織構造、報告ライン、適切な権限と責任の確立 4. 有能な人材を惹き付け、育成することへのコミットメント 5. 各個人の内部統制への説明責任の保持
リスク評価	6. 十分な明瞭性をもった目標の特定 7. 企業全体のリスクの識別と、リスク管理の方法決定の基礎としての分析 8. リスク評価に当たっての不正の可能性の検討 9. 内部統制システムに影響を与える変化の識別・評価
統制活動	10. リスクを軽減するための統制活動の選択と構築 11. 目標達成を支援する技術に関する全般統制活動の選択と構築 12. 期待されていることを定めた方針と、方針を実行するための手続による統制活動の展開
情報と伝達	13. 内部統制機能を支援する関連性と品質の高い情報の入手又は作成 14. 内部統制の目標と責任を含む内部統制の機能に必要な情報の内部的なコミュニケーション 15. 内部統制の機能に影響を与える事項に関する外部関係者とのコミュニケーション
モニタリング活動	16. 内部統制の構成要素の存在と機能状況に関する継続的・独立的評価の選択・開発・実施 17. 内部統制の不備の適時な評価と、上級経営者や取締役を含む是正措置責任を有する関係者に対するコミュニケーション

（出典）COSO（2013）

ための17の原則を挙げている（COSO 2013）。その要約を第１表に示した。

また、*COSO IN THE CYBER AGE* においては、サイバーリスクに対応するための内部統制の構成要素を第２図のように示し、COSO の17の原則に沿って、サイバー時代におけるリスク評価、統制活動、情報と伝達のプロセスへの影響が解説され、その後、全体に関係する統制環境とモニタリング活動の鍵について述べられている。なお、ここにいうサイバーリスクは、サイバー攻撃のリスクを意味している。以下、その内容を紹介する。

第２図　サイバーリスクに対応するための内部統制の構成要素



（出典）COSO（2015）p. 4

(2)　サイバーリスクの評価

サイバーリスクの評価においては、まず、サイバー攻撃の加害者（国家とスパイ、組織化された犯罪者、テロリスト、ハクティビスト、インサイダーなど）を特定する必要がある。

その上で、まず、事業の目標、外部財務報告の目標、外部非財務報告の目標、内部報告の目標、コンプライアンスの目標を特定する（原則６）。次に、サイバーリスクプロファイルの理解、攻撃者にとっての価値・目標（攻撃の発生可能性の理解を含む）、攻撃者の動機、攻撃のメソッド、技術・ツール・

プロセスの注意深い評価を行う（原則７、８）。さらに、Web、モバイル、クラウド、ソーシャルメディア技術の継続的な導入、外部委託、オフショアリング、サードパーティとの契約などの変化を識別・評価する（原則９）（COSO 2015, pp. 5-7）。

(3)　サイバーリスクに対応した統制活動

サイバーリスクに対応した統制活動においては、予防的統制（脅威が弱点に接触することを防ぐ統制）と発見的統制（脅威がシステムに到達したことを識別する統制）を構築し運用する（原則10、11、12）。

これらは、IT 全般統制（General Information Technology Controls）と共通する事項が多いが、サイバー環境に適合した基準やフレームワークとして、COBIT フレームワーク（ISACA）、ISO27000 シリーズ、NIST（National Institute of Standards and Technology of the U.S.）のフレームワーク等を活用する（COSO 2015, pp. 8-9）。

(4)　サイバーリスクに対応した情報と伝達

サイバーリスクに対応した情報と伝達においては、まず、情報の要件の識別、関連するデータの情報への加工、データの内部・外部ソースの捕捉、プロセスを通じた品質の維持を行う（原則13）。

また、すべての担当者、サイバーリスクと統制の管理とモニタリングの明示的責任者及び取締役会との双方向のコミュニケーションを行う（原則14）とともに、そのときの状況に対応して、インバウンドのコミュニケーションとアウトバウンドのコミュニケーションを行う（原則15）（COSO 2015, pp. 10-15）。

(5)　サイバーリスクに対応した統制環境とモニタリング活動

サイバーリスクのマネジメントは、ガバナンスなくしては不可能であり、統制環境とモニタリング活動における以下のような取り組みが鍵となる（COSO 2015, p. 17）。

・情報システム保護の重要性に関するトップの明確な姿勢

・潜在的なサイバーエクスポージャー軽減のための統制の設計と運用の有

効性評価のための継続的で独立した評価プログラム
・資格のあるサイバーリスク専門家の援助と関与
・外部サービスプロバイダに関連する適切な統制とモニタリング
・サイバーリスク対策の不備に関する適切で適時なコミュニケーション[1)]
・統制オーナーによる情報システム保護を支援する責任の保持

すなわち、サイバーリスクへの対応においては、まずトップがその重要性を認識して、経営資源を配分するとともに、関連する内部統制を有効に構築し運用する必要がある。そのためには、最先端のテクノロジーとマネジメントを理解した専門家の援助と関与を受けるとともに、組織体内部におけるコミュニケーションと組織体外部とのコミュニケーションが欠かせないことを示している。

3.3 サイバー時代の内部統制における課題

これまでに述べたように、*COSO IN THE CYBER AGE* は、サイバーリスクへの対応をテーマとしているが、サイバー時代において組織体をとりまく外部・内部の環境変化は、サイバーリスクに代表されるダウンサイドのリスクのみでなく、組織体における内部統制の目標達成に好影響を与える機会も与えるものである。

サイバー攻撃は、情報漏洩や情報システム障害をもたらし、これが組織体のレピュテーションリスクやビジネスを正常に継続できなくなるリスクに繋がる。その対策は際限のないコストの上昇を招き、経営が成り立たなくなる危険性もある。しかしながら、今日の組織体の活動は、サイバー空間との繋がりを絶っては成立し得ない状況にあり、サイバー時代の経営上のメリットを享受することが必須である。

すなわち、サイバー時代においては、その組織体のコアとなるビジネスにおいて IT を中心とするテクノロジーの利用を高度化しなければならないこ

1) 原文では、「サイバーの不備（cyber dificiencies）」という表現であるが、「サイバーリスク対策の不備」を意味していると考えられる（COSO 2015, p. 17）。

とはいうに及ばないが、サイバー時代の環境に適合した内部統制を構築し運用することも重要であり、そのための観点としては、次の三点を挙げることができる。

その第一は、経営意思決定のために多様な観点を考慮できる組織体制を構築することであり、第二は、活用可能な組織体内外からの様々な情報を内部統制に生かすことである。そして、第三は、これらに資する IT を積極的に活用し、組織体内部の情報のみでなく、サイバースペース上の情報を有効に活用することである。

これらの観点を踏まえた組織体制のモデルとしては、次節で述べる「三線防御モデル」がある。そのような組織体制の下で IT を利用した内部統制を構築することがサイバー時代の内部統制として求められる。

Ⅳ　三線防御モデルと IT を利用した内部統制

4.1　三線防御モデルが持つ意味

三線防御モデルでは、リスクマネジメントにおける防御機能を三段階に分けている。まず、防御の第一線は、リスクオーナーやマネージャーが行う業務管理である。次に、防御の第二線は、経営者が設置したリスク管理、コンプライアンス及びコントローラの機能であり、財務管理、セキュリティ、リスク管理、品質、検査、コンプライアンスを統括する部門がその機能を担う。さらに、防御の第三線は、執行部門から独立した内部監査機能であり、その報告先は、監督機能を担う取締役会（Governing body）となる（IIA 2013, pp. 2-6）。

一方、内部統制は、業務、報告及びコンプライアンスに関わるマネジメントシステムの中から、意思決定及び執行に直接関わる部分を除いた概念であり、その構成要素は、統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動からなる（鳥羽 2007, p. 117）。このうちモニタリング活動は、他の構成要素の運用状況のフィードバックを提供するものである（Rittenberg 2014）。

以下においては、三線防御モデルの各段階における防御機能のうち、意思決定及び執行に直接関わらない機能（内部統制機能）を対象に検討する。

4.2 三線防御モデルと IT を利用したモニタリング活動

IT を利用したモニタリング活動は、三線防御の各段階で利用可能である。

まず、第一線では、業務を担当するマネージャーがリスクの保有と管理を行う。彼らは、日常のリスクとコントロールの手続の実行のための有効な内部統制の維持に責任を負っている（IIA 2013, p. 3）。したがって、IT を利用したモニタリング活動においても、日常の個々の取引や会計処理に関するモニタリングの実施が中心となる。

次に、第二線は、リスク管理、コンプライアンス及びコントローラに関する次のような機能を担う（IIA 2013, pp. 4-5）。

- 経営方針を支持する役割と責任を定義し、実装するための目標を設定する。
- リスク管理の枠組みを提供する。
- 既知及び新たな問題を識別する。
- 組織体の暗黙のリスク選好の変化を識別する。
- リスクと問題を管理するためのプロセス及びコントロールの開発について経営者を支援する。
- リスク管理プロセスに関するガイダンスとトレーニングを提供する。
- 業務管理による効果的なリスク管理実務の実装の促進とモニタリングを行う。
- 新たな問題、規制及びリスクシナリオの変更に関する業務管理について警鐘を鳴らす。
- 内部統制の妥当性と有効性、報告の正確性と網羅性、法令と規制の遵守性、欠陥のタイムリーな改善をモニタリングする。

以上のように、第二線の役割は、組織体にリスク管理の枠組みを実装し、リスクを識別するとともにその変化の状況をモニタリングし、経営者に報告

することにある。したがって、IT を利用したモニタリング活動においても、組織体全体のレベルでリスクの状況を把握し、異常値や変化の兆しを検出することが必要となる。

さらに、第三線では、独立した内部監査部門が、次のような機能を担う（IIA 2013, p. 6）。

・内部監査の実施のために認められた国際基準に準拠して行動する。
・組織体の中で独立してその職務を果たすことができるように十分に高いレベルの責任者へ報告する。
・取締役会への積極的かつ効果的な報告ラインを持つ。

第三線は、組織体の中で独立した立場でモニタリングを行うことが役割であるため、IT を利用したモニタリング活動においては、第一線や第二線が利用している情報の活用と当該情報の信頼性の検証を行うとともに、第三線として独自の観点からの情報の追加や部門横断的な情報の関連付けを行い、これらを活用する。

4.3　サイバー時代の内部統制における IT の利用の具体策

(1)　サイバー時代の内部統制における IT の利用の特徴

既に述べたように、従来、企業における情報システムは、基幹業務システムと称される IT を利用した業務処理のための情報処理システムが中心であり、内部統制との関係でも基幹業務システムの機能及びデータの利用が中心となっていた。

しかしながら、企業内の情報のやりとりにおいても、また、企業外部との情報のやりとりにおいても、インターネットの活用が著しく進歩し、従来、人間が時間と労力をかけて自ら収集・処理・報告していた情報を、インターネット上に散在する情報の中から瞬時に収集し、処理・報告することが可能となった。また、センシング技術の進歩により、従来記録し得なかった人間の行動や地球環境の変化に関する情報の記録・収集も可能となった。

以下においては、これらの状況を踏まえた内部統制における IT の利用の

第２表　金融機関のコンプライアンスと規制における課題とソリューション

課題	ソリューション
リスクデータの集約と管理	・暗号、セルレベルセキュリティ、データ取り込み及び情報共有の技術 ・ブロックチェーンによる機関の間及びレギュレーターとのデータ管理、セキュリティ及び集約の改善 ・大容量の構造化データと非構造化データを整理するための機械学習と高度な分析 ・業界全体で堅牢な標準データ・ディクショナリの構築を支援するためのオープンプラットフォームとネットワーク ・コンプライアンスの API（Application Program Interface）上で実行される規制当局からのより良く自動化されたセキュアなオンラインデータレポーティングポータル
モデリング、シナリオ分析と予測	・機械学習、高度な分析及び新しいタイプのモデル ・データの保存、アクセス、共有及び収集技術 ・最新のデータ可視化技術及び高度なデータ分析
（リアルタイムの）支払監視、報告、ブロッキング	・ブロックチェーンによる既存の階層型決済システムの代替 ・支払の受益者の識別など、決済システムの非構造化（メタ）データ出力を解釈する機械学習
本人確認	・ブロックチェーンによる安全な情報共有システムの開発 ・非構造化データの処理及び分析のためのデータマイニング、自然言語処理及び視覚的な分析 ・特に新興市場における生体認証、社会的認証又は身元確認に関する他の新しい手段の促進
行動と組織文化のモニタリング	・音声からテキストへの変換機能を組み合わせた非構造化データ分析による、コミュニケーションの監視、データからの行動パターン認識、迅速な消費者への適合性の見極め
リアルタイム取引タスク（金融市場取引）	・市場取引の監視のための機械学習や予測分析 ・リアルタイムマージン算出、CCP（Central Counter Party：中央清算機関）の選択とリスクマネジメントエンジン、コンプライアンス監視、業務終了時の全取引の照合調整及びデリバティブ取引のための報告 ・ブロックチェーンによる取引プラットフォーム
規制の動向をより意識した金融	・規制の理解のための「規制レーダー」ソフトウェアを可能にする認知コンピューティングや深層学習技術
補足事項 ファイル転送方式	・イントラネットのモデルである JWICS（Joint Worldwide Intelligence Communications System）を利用した主要な国際金融規制機関のファイル転送のための安全なメカニズム

（注）　JWICS は、機密・機微情報を送信するためにインテリジェンスコミュニティ全体で使用される米国国防総省によるイントラネットであり、暗号化されたファイル転送プロトコルの基盤は、現在、様々な米国規制当局によって利用されている。

（出典）IIF（2016）pp. 16-18 より著者作成。

具体策を検討する。

(2)　金融機関における内部統制への IT の利用

世界の大手民間金融機関が参加する国際組織 Institute of International Finance（国際金融協会）は、2016年 3 月に *REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING* と題する報告書を公表した。この報告書は、金融機関のコンプライアンスと規制における課題とソリューションについて取りまとめたものである。

その中で、課題として①リスクデータの集約と管理、②モデリング、シナリオ分析と予測、③（リアルタイムの）支払監視、報告、ブロッキング、④本人確認、⑤行動と組織文化のモニタリング、⑥リアルタイム取引タスク（金融市場取引）、⑦規制の動向をより意識した金融を挙げている。これらの課題に対するソリューションとして示されている内容は、第 2 表のとおりである。

(3)　内部統制における人工知能の活用可能性

内部統制におけるデータ分析の高度化には、人工知能の活用が欠かせない。矢野（2014）は、人工知能を、「運転判断型」「質問応答型」「パターン識別型」の 3 つに分類しているが、以下に述べるように、いずれのタイプの人工知能も内部統制の有効性向上に資すると考えられる。

まず、「運転判断型」は、これまで仮説を人間が設定してデータによる検証を繰り返してきたプロセスそのものを自動化するものであり、内部統制の目的に従ったオペレーションの改善要因と阻害要因を帰納的に見出すことにより、より効率的・効果的な業務プロセスの構築・運用が可能となる。人工知能の効果が最も期待できる分野である。

帰納的な推論の技術には、種々のものがあるが、代表的なものとして、インバリアント分析[2)]、異種混合学習技術[3)] を挙げることができる。これらの

2)　インバリアント分析は、多数のセンサから大量の時系列データを収集・分析し、平常時に成り立つセンサ間 の不変関係（インバリアント：invariant）を関係式として自

技術を内部統制において活用するためには、基幹業務システム上のデータのみでなく、人間の動きや人的ネットワークに関するセンシングデータなどの収集と活用が必要となる。

次に、「質問応答型」は、質問文を分析し、事前に収集した情報の中から、正解の確率の高いものを選び出して回答するシステムである。投資判断、与信判断、取引可否判断などにおいて、関係する情報を網羅的に収集・分析することにより、人間による意思決定の誤りの防止を支援する機能を果たすものであり、自動化により内部統制を強化するという役割がある。

質問応答型には、様々な技術が利用されるが、事前の情報収集にはインターネットサイトのクローリング技術が、事前に収集した情報から質問に関連するものを選び出すには概念検索[4] の技術が、そして正答率を高めるためには機械学習の技術が用いられる。

さらに、「パターン識別型」は、画像や音声のパターンを識別することで、同一性の識別や画像・音声データのテキスト化を行う技術である。例えば、コールセンターや営業部門における顧客との対話の音声データをテキスト化することにより、質問応答型で処理可能な情報として活用することが可能となる。

パターンの自動識別により、誤謬の防止、業務の精度の向上に資する。また、音声認識ソフトでテキスト化した情報を質問応答型と組み合わせることにより、さらなる効果を発揮する。

動でモデル化し、このモデルの予測値とリアルタイムデータを比較することで、「いつもと違う」 動きを検出する技術である（日本電気 2016）。

3） 異種混合学習技術は、多種多様なデータに混在するデータ同士の関連性から、特定の規則性を自動で発見するとともに、分析するデータに応じて参照する規則を切り替えることにより、「規則性が変化するデータ」に対する高精度な予測や異常検出を可能とする技術である（日本電気 2016））。

4） 概念検索は、自然言語で書かれた任意の文章や文献を入力とし、その文章の内容に類似する文献を、検索対象となる文献集合の中から検索し、類似度の高い順に 出力する検索方式である（八木 敬宏ほか 2009）。

(4)　三線防御の各段階の内部統制における IT の利用

三線防御の各段階の内部統制において利用可能な IT ツールの例を第 3 表に示した。

三段階の内部統制機能を連携させるためには、IT を利用して運用状況のフィードバック情報を共有して活用することが求められるが、目的に応じて、機密保持対策を講じた上での情報共有が必要である。

第 3 表　三線防御の各段階の内部統制で利用可能な IT ツールの例

区分	IT ツールの例
第一線	・基幹業務システムに組み込まれた内部統制機能（「IT 業務処理統制」のための ERP パッケージの機能など） ・投資判断、与信判断、取引可否判断等の誤り防止支援機能（レイティングシステム、シミュレーションシステムなど） ・センシングデータの活用によるコミュニケーション改善支援機能（ソーシャルグラフの作成、動線の可視化など）
第二線	・リスク分析・評価ツール（信用リスク、市場リスク、流動性リスク、オペレーショナルリスクの分析・評価を行う） ・統制自己評価（Control Self Assessment）ツール（各部門における自己評価を行い、リスク管理部門でリスク評価を行う） ・業績管理ツール（ERP パッケージにおける部門業績管理・予算管理機能など） ・取引・行動モニタリングツール（インサイダー取引、顧客対応、情報漏洩の監視システム、センシングデータを用いた監視システムなど） ・非構造化データ連携・絞込みツール（関連する各種のデータを連携させ、絞込みを行う） ・アクセスログ分析ツール ・教育ツール（e ラーニングシステムなど）
第三線	・CAATs（Computer Assisted Audit Techniques）ツール（自社開発ツールを含む） ・ERP パッケージの監査モジュール ・リスク分析・評価ツール ・監査業務管理用ツール ・EUC（End User Computing）ツール（集計、階層化、散布図、絞込み、監査証跡トレースなど）

（出典）著者作成。

4.4 統制機能の見直しと情報インテグリティ

(1) 環境変化に対応した統制機能の見直し

経済のグローバル化と取引の複雑化に対応して、基幹業務システムに組み込まれた統制機能についても見直しが必要となっている。

例えば、国際会計基準（International Financial Reporting Standards）第15号「顧客との契約から生じる収益」において、複合した取引の収益の履行義務への割り当て方法が、今後の基準適用において課題となっており、経営成績の内部・外部報告との関連で考慮が必要である。

一方では、海外での取引に関連して、贈収賄、マネーロンダリング等にからんで、国境を越えて高額の制裁金が課されるリスクも高まっており、これまで取引に関連して取得してきた範囲にとどまらない広範囲の情報の収集とモニタリングの実施が必要となっている。贈収賄、マネーロンダリング等の防止に関連して、金融機関では、より深く顧客の実態を知ること（Know Your Customers）が求められているが、一般事業会社においても、取引先の実態を把握することがより求められるようになるであろう。

また、これらの統制機能の見直しに関しては、組織体内部でのソリューションの導入だけでは目的を達成することが難しいケースが多いと考えられ、自らの組織体と外部のステークホルダーとの情報共有が必要である。さらに、そのためには概念の共有とデータ定義の標準化が必要となる。

(2) 情報共有の前提としての情報インテグリティ

前述した概念の共有とデータ定義の標準化に関連して、情報インテグリティの確保が重要となる。

従来、情報インテグリティは、正確性、網羅性、正当性、維持継続性などの情報処理のプロセスにおいて情報の内容に直接関わる品質特性として説明されてきた。しかし、これは、組織体内部でコンテキスト（context）を共有していることを前提としたものであり、サイバースペース上の情報の利用を想定したものではない。

米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）が作成

したホワイトペーパー *Information Integrity* では、情報インテグリティを「その情報の対象物への表現の忠実性及びその意図する利用への情報の一致性」と定義した（AICPA ほか 2013, p. 4）。

また、その情報が有用であるためには、その情報の目的及び利用に必要なコンテキスト情報（情報に関する情報）を示す必要があり、これをメタ情報と呼んでいる。なお、ここにいうコンテキストとは、「事業体、エンティティ、プロセス、個人の活動に影響する、又はそれらの活動を決定するような内外の要因の全体的な集合」をいう（ISACA 2012, p. 102）。

情報インテグリティリスクは、端的には、コンテキストの共有を阻害するリスクであり、このリスクを軽減するためには、メタ情報を用いて共通のコンテキストの中で情報を目的に合致させる必要がある。さらに、メタ情報を用いて情報ポータビリティを実現するためには、ビジネスプロトコルの標準化を前提とした情報モデルの標準化が必要である。

一方、情報処理システムの側での対応も必要である。その例としては、クラウドストレージのデータアクセスと管理インターファイスの規格（CDMI: Cloud Data Management Interface）が ISO/IEC 17826:2012 として国際規格化されている。

V　おわりに

サイバー時代においては、セキュリティ面のリスクが増大する反面、サイバースペース上の情報の活用により大きな効用がもたらされることが期待されている。本稿では、このような環境変化に対応する内部統制の方向性について検討した。

サイバー時代の環境に適合した内部統制を構築し運用するための組織体制のモデルとしては「三線防御モデル」があり、その下で IT を利用して、組織体内部の情報のみでなく、サイバースペース上の情報を有効に活用することが必要となる。そして、その際の情報インテグリティのリスクを軽減するためには、メタ情報を用いて共通のコンテキストの中で情報を目的に合致さ

せることが必要である。

今後、各組織体においては、自らの事業環境の下におけるサイバーリスクの意味を改めて問い直し、サイバー攻撃の防御とサイバースペース上の情報の有効活用の両面から取り組むことが求められる。

（筆者は法政大学大学院イノベーション・マネジメント研究科教授）

引用文献

American Institute of Certified Public Accountants（AICPA）and Canadian Institute of Chartered Accountants（CICA）(2013), *Information Integrity.*

Committee of Sponsoring Organizations of the Treadway Commission（COSO）(2013), *Internal Control – Integrated Framework.*（八田進二・箱田順哉監訳／日本内部統制研究学会新 COSO 研究会訳、2014、『COSO 内部統制の統合的フレームワーク（フレームワーク篇）』、日本公認会計士協会出版局、9 頁）.

――――（2015）, *COSO IN THE CYBER AGE.* https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

Institute of International Finance（2016）, *REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING*

Rittenberg, L. E.（2013）, *COSO Internal Control – Integrated Framework: Turning Principles into Positive Action*,（ラリー・E・リッテンバーグ、八田進二監訳、堺咲子訳、2014、『COSO 内部統制の統合的フレームワーク－内部監査に活かす原則主義的実践ガイド』、一般社団法人日本内部監査協会、27頁）

The Institute of Internal Auditors（IIA）(2013), *IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL*

ASCII.jp デジタル用語辞典（2016）「サイバースペース」http://yougo.ascii.jp/caltar/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%B9%E3%83%9A%E3%83%BC%E3%82%B9（2016/8/14）.

ISACA（2012）『COBIT5 Framework 日本語版』.

石島隆（2016）「三線防御と IT を利用した内部統制」、『研究部会報告　IT を利用した内部統制のモニタリングの有効性向上策の研究－最終報告－』、日本内部統制研究学会.

デジタル大辞泉（2016 a）「サイバー」https://kotobank.jp/word/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC-508285#E3.83.87.E3.82.B8.E3.82.BF.E3.83.AB.E5.A4.A7.E8.BE.9E.E6.B3.89（2016/11/25）.

デジタル大辞泉（2016 b）「サイバネティクス」https://kotobank.jp/word/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%8D%E3%83%86%E3%82%A3%E3%83%83%E3%82%AF%E3%82%B9-508324#E3.83.87.E3.82.B8.E3.82.BF.E3.83.AB.E5.A4.A7.E8.BE.9E.E6.B3.89（2016/11/25）.

鳥羽至英（2007）『内部統制の理論と制度』、国元書房.
日本電気（2016）「ビッグデータを支える先進技術」http://jpn.nec.com/bigdata/analyze/index.html（2016/1/6）.
八木敬宏・間瀬久雄・岩山真（2009）「概念検索技術および特許検索への適用可能性について」『特技懇 2009.1.30.no.252』43頁.
矢野和男（2014）『データの見えざる手－ウェアラブルセンサが明かす人間・組織・社会の法則』、草思社.