Logstorage

純国産 統合ログ管理システム
国内導入 / ログの収集実績多数！

適切なログ管理を抜きには実現できない監査対応や内部統制、法規制遵守

不祥事を防ぎ、株主やステークホルダーを守るために不可欠な種々の「監査」

粉飾決算に水増し請求、横領、あるいは法令に反する営業活動に認証試験に関する不正……残念ながら、企業ぐるみ、あるいは従業員による不祥事は後を絶たない。ひとたびこうした不祥事が発生すれば、企業は直接的な損害を被るのはもちろん、社会的な信用やブランド力の低下といった間接的な被害も受けることになる。株主や関係者も決して少なくない余波を被るだろう。

不祥事の発生を防ぐには経営層から従業員に至るまでが法令を遵守し、社会的な倫理に則って業務に取り組む意識を持つことが重要だが、個々人のモラルだけに頼るのは危険だ。「魔が差した」という言葉があるように、人間、ふとしたきっかけで不正を働いてしまう可能性はゼロではないし、うっかりミスがきっかけになることもある。また、そもそも組織ぐるみ、会社ぐるみで不正を働く場合、食い止めるのはなかなか難しい。

こうした事態を防ぎ、さまざまな不正を防止し、さらに業務の適正性を確保し、効率化を目的に実施されているのが、さまざまな「監査」だ。

監査にも、外部の監査法人によって財務諸表の内容が正しいかどうかを確認する「外部監査」（このうち財務諸表の内容が正しいかどうか確認を行うものを「会計監査」と呼ぶ）、企業の監査役や担当者が、不正防止や業務効率化などを目的に業務の遂行状況や組織体制を評価する「内部監査」に大別できる。

上場企業で働いている場合、何らかの形で外部監査や内部監査に必要な資料の提出やヒアリングを求められたことがあるかもしれない。取引の「証跡」やプロセスを定めた規定を確認することで、法令に準拠したプロセスが定められているか、効率的な業務フローが構築されているかといった事柄を確認していく。しかも一度チェックして終わりではなく、継続的にモニタリングを行うことで、内部統制が有効に機能しているかを評価していくことも求められる。

大規模会計不祥事をきっかけに、企業に求められるようになった内部統制

第三者による外部監査については、投資家を保護するといった目的から必要性は理解できるが、なぜそれに加えて内部監査が必要なのだろうか。自治は内部監査が求められるようになったきっかけは、2001 年に破綻したエネルギー大手の米エンロンの大規模会計不祥事に遡る。監査法人も巻き込んだ粉飾決算が発覚した結果、史上最大とも言われる 4 兆円を超える巨額の債務超過となり、市場はもちろん米国経済にも大きな影響を与えてしまった。

これを機に米国では、経営の透明性を高め、再び同様の不正を起こさないために内部統制の仕組みが求められるようになり、SOX 法が成立。これを受けて日本でも 2006 年 5 月に新会社法、6 月に金融商品取引法が成立し、内部統制が義務づけられることになった。

しばしば言及されていることだが、内部統制の目的は、

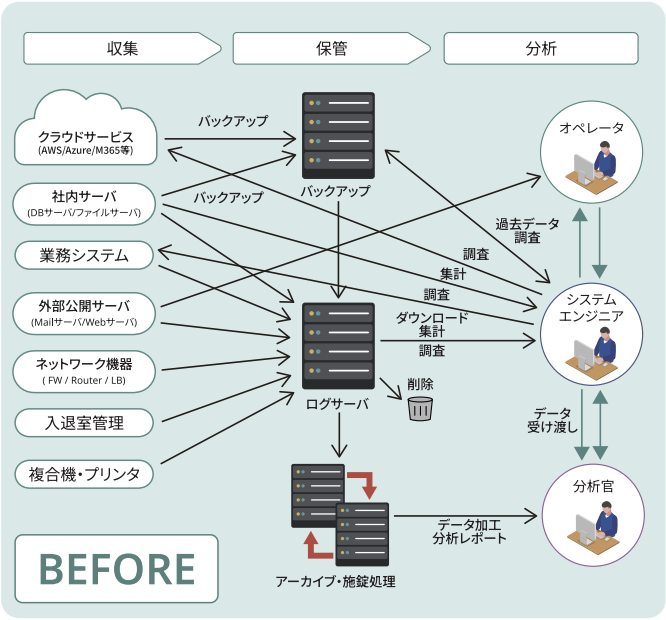
- 業務の有効性・効率性の確保
- 財務報告の信頼性の確保
- 法令順守
- 資産の保全

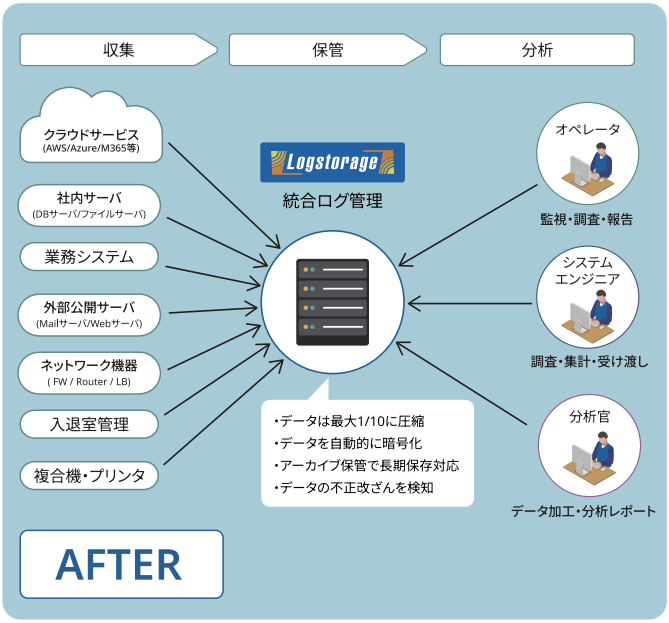
の 4 つだ。これらの目的を達成するために、

- 統制環境
- リスクの評価と対応
- 統制活動
- 情報の伝達
- モニタリング
- IT 対応

という 6 つの基本的要素が定義されている（https://www.fsa.go.jp/news/r1/sonota/20191213.html）。

情報セキュリティ管理のためのログ取得及び監視





要は、「企業の目的を効率的に達成するため、業務が効率的に遂行されているか」「財務報告書は信頼できる内容か」「企業活動が法令を遵守した形で進められているか」といった、文字にしてしまうと当たり前の事柄が当たり前に行われていることを確認するために、リスクに基づいて環境を整え、ルールを明文化し、適切にコントロールし、かつそのプロセスが有効に機能しているかを継続的に確認する仕組みを整えていくことを指している。

デジタル時代の内部監査・内部統制において無視できない「IT 対応」

ここでポイントになるのが「IT 対応」だ。今や、企業の業務は IT システムなしには成り立たない。営業活動にはじまり、生産管理や販売管理、経費や人事・労務に至るまで、あらゆる業務が IT システムに依存していると言ってもいいだろう。このため、企業の内部統制を実現していく上では、IT システムが戦略性や有効性、効率性を満たしているかを確認し、情報システムに想定されるリスクを適切にコントロールする手段として「システム監査」もまた、不可欠な要素となる。

しかも、システム監査がカバーする領域は、企業のデジタル化に伴って拡大している。当初は、会計システムにおけるデータに改ざんなどがないか、真性性を確保する「IT 監査」と呼ばれる領域が中心だったが、情報漏洩や内部不正の多発を受けて、セキュリティやコンプライアンス、ガバナンスといった領域もチェック対象となっている。おそらくこの先も、企業の社会的責任（CSR）といった分野へと広がっていくことだろう。

そして、システム監査のスコープは、目的や企業が置かれている状況によっても変わってくる。

たとえば、「新たなシステムを構築する場合に、そのプロジェクトが目的に沿った形で適切に進められているか」を問う場合もあれば、情報システムが適切な体制で運用されているか、また災害など不測の事態に備えた事業継続計画が定められているか、さらに外部に何らかの業務を委託している場合の体制が適切かなど、さまざまな項目が考えられる（参考：経済産業省「「システム監査基準」及び「システム管理基準」の改訂について」https://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html）

いずれにせよ、基準に沿って評価するには元となるデータがなければはじまらない。システムがいつ、どのように動作したか、設定変更などがどのように行われたかといった事柄を明らかにしてくれるのは、各システムやアプリケーションが出力する「ログ」であり、定期的な内部監査を実現するためには、ログを一定期間、第三者から見ても改ざんなどが加えられていないことが明らかな状態で保存し、必要に応じて確認できる環境を整えておくことが求められる。

中でも留意したいのが、情報セキュリティ体制だ。一例として経済産業省の「情報セキュリティ管理基準（平成 28 年改正版）」（https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf）が参考になるが、マネジメントや人・組織的な対策に加え、技術的な側面、運用面からどのような対策が行われているかを問う内容となっており、ここでもやはり「ログ取得及び監視」が管理項目の 1 つとして定められている。

情報漏洩事件の多発を背景に、法規制やガイドラインへの遵守も不可避に

企業には内部統制と同時に、さまざまな法規制やガイドラインへの遵守、いわゆるコンプライアンスも求められている。特に、情報漏洩事件の多発を背景に、「プライバシーマーク」や、オンラインでのクレジットカード情報保護に必要な対策をまとめた「PCI DSS」に加え、防衛省の新たな調達基準の参照元でもある米国政府機関の調達基準「NIST SP-800」など、抑えておくべきセキュリティ関連の法規制やガイドラインは増えるばかりだ。

最近の動きの中でも注目すべきは、改正個人情報保護法の施行だろう。2020 年の改正では、個人情報に関する個人の権利の拡大と、それを収集・保有する事業者側の責務の強化が図られた。これはヨーロッパの「GDPR」、米国の個人情報保護規制など、プライバシーを重視する全世界的な流れに沿ったものと言えるだろう。

改正によって、これまでは「努力義務」とされていた、個人情報の漏洩が発生した場合の本人への通知と個人情報保護委員会への報告が、「財産的被害が生じるおそれがあるもの」など、個人の権利利益を害する恐れが大きい漏洩の場合、本人への通知および報告が「義務」となった。しかも、個人情報保護委員会への報告は、速報は「速やか」に、つまり 3〜5 日以内に行うことが求められ、確報についても 30 日以内の報告が目安とされている。

従って、過去の個人情報漏洩事件でいくつかの企業が陥ってしまった、「詳細は調査中」として数ヶ月も待たせる姿勢では法令の求めに間に合わない。いざと言うときには、明白な証拠を元に「いつ、何が起きたか」「何が漏れたのか」を速やかに示せる体制作りが求められる。

ログの一元管理・長期保存を通して内部統制やコンプライアンスを支援する「Logstorage」

このように、内部統制やコンプライアンスといった観点からも情報システムに対する要求は高まるばかりだ。

これらの要請に応えるにはさまざまな取り組みが必要だが、中でも重要なのは「証拠」「証跡」をいかに残すかだ。監査の際のヒアリングに答えるにも、万一セキュリティインシデントが起こった時に、法の定めに従って速やかに報告・対応するにも、何が起きたかを示せなければ意味がない。

それには、企業を構成するさまざまな情報システムが出力している「ログ」を日頃から収集し、法規制が定める期間、適切に保管しておく必要がある。それも、オンプレミス環境だけでなくクラウド環境にもまたがってログを収集・管理しておかなければならない。

こうした部分をサポートするのが「Logstorage」だ。さまざまなログの収集・保管を行い、検索・集計・検知や横断的なレポート、分析を可能にするシステムで、400 種類以上のソフトウェアやネットワーク機器に対応し、さまざまな種類のログを取り込めること、ログのデータを圧縮し、効率よく長期間保管できることが特徴だ。

内部統制やコンプライアンスの観点で重要なポイントとして、不正を働く人間や攻撃者が証拠隠滅や改ざんを図ろうとしてもそれを防ぎ、安全に元のデータを保管しておく仕組みも備えている。まさに「動かぬ証拠」を元に、監査要求に応え、企業としての説明責任を果たしていく上で不可欠の仕組みと言えるだろう。

クラウドサービス
AWS
Azure
Google Cloud Platform
Microsoft 365
Google Workspace
box
Cybereason

ファイアウォール
Palo Alto Networks NGFW

PC資産管理
CWAT
LANSCOPE
MaLion
SKYSEA Client View
秘文

クライアントログ
DEFESA Logger
MylogStar

特権管理
SecureCube Access Check
iDoperation

データベース監査
PISO
SSDB 監査

Webフィルタリング
i-FILTER

Logstorage 連携製品

問い合わせ先

インフォサイエンス株式会社
プロダクト事業部
〒108-0023 東京都港区芝浦 2-4-1
インフォサイエンスビル
TEL: 03-5427-3503
URL: https://logstorage.com/
E-Mail: info@logstorage.com