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！

# 今や業務に不可欠なクラウド環境、セキュリティ対策の鍵は一元的なログ管理体制

## もはや特別なものではなく、当たり前になった「クラウド活用」と「ハイブリッド」

今、クラウドサービスを一切使わずに業務ができるだろうか？　おそらくほぼすべての企業において、クラウド抜きに仕事はできないと言っていいのではないだろうか。メールにはじまり、部署内の予定を調整するグループウェアや必要なファイル・資料類を共有するストレージサービス、さらには営業支援システムや名刺管理、ワークフローなど、当たり前のように SaaS を活用する場面が増えている。

そして、これまで社内環境、いわゆる「オンプレミス」に構築するのが当たり前だった、自社独自の業務アプリケーションもまた、徐々に Amazon Web Services（AWS）や Microsoft Azure といった IaaS への移行が進んでいる。

かつては、「クラウドで基幹システムを動かすなんて心配だ」と言われた時代もあった。だが今や、BCP も含めた可用性の確保や拡張性、何より固定資産を持たずに IT システムを運用できる経済性といった利点が評価され、クラウドファーストと言われるように、クラウドありきで構築されるケースがむしろ増えてきた。日本政府のセキュリティ評価制度「ISMAP」に複数のクラウドサービスが登録されたことも追い風になっている。

かといって、すべての業務、すべてのアプリケーションをクラウドベースで運用している企業ばかりかというと、決してそうではないだろう。新たに事業を開始したスタートアップ企業ならばともかく、大抵の企業には長年にわたって運用し続けてきた「長寿」のシステムがあり、なかなか移行が難しいといった事情がある。また、個人情報・機密情報を扱うという観点から、どうしてもクラウドに移行できないシステムも存在するだろう。結果として現実的には、クラウドとオンプレミスを適材適所で組み合わせる、ハイブリッドな環境が一般化している。

ハイブリッド化の流れは、システムだけでなく、「働き方」についても同様だ。

## 「事業者に全てお任せ」とはいかない、クラウドセキュリティの確保

こうした複数の意味での「ハイブリッド」環境は、コスト削減だけでなく、柔軟に、かつ効率的に業務を行えるなど、企業にも従業員にもさまざまなメリットをもたらした。

ただ、残念ながら明るい側面ばかりではない。中でも、最も企業が懸念するのはセキュリティリスクだろう。

確かにクラウド環境には、オンプレミス環境で運用する場合に比べて可用性が高く、クラウド事業者によるさまざまなセキュリティ対策が施されているといったメリットがある。ただ、クラウド環境全体のセキュリティは、クラウド事業者とユーザー企業がともに責任を果たすことで実現される「責任共有モデル」によって成り立っている。物理的なファシリティや基盤部分はクラウド事業者が確保するとしても、その上で動作するアプリケーションへのアクセス制御やアカウント管理、データの保護といった部分はユーザー企業側の責任だ。

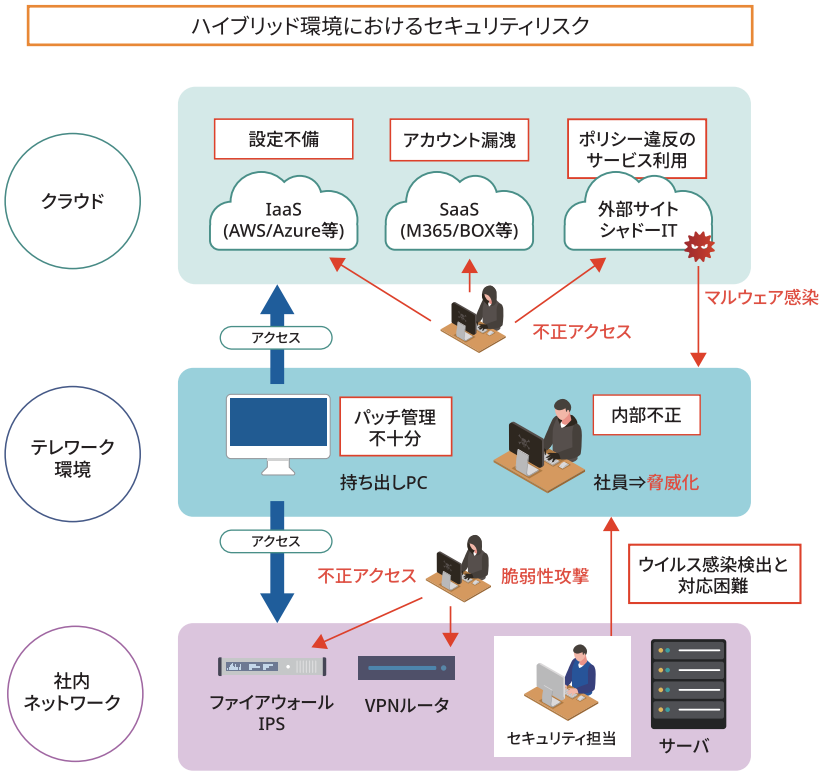
だが、残念ながらこの境界の曖昧な部分でセキュリティ事故も発生している。

たとえば、クラウド上のリソースに対するアクセス制御が不十分で、第三者に盗み見られる状態でデータを保管してしまっていた、といった事故は、古くからたびたび発生してきた。また、リモートワーク環境からクラウドサービスへのアクセス時に多要素認証（MFA）を設定していなかったためになりすましアクセスを許し、クラウド上のリソースを勝手に悪用され、仮想通貨のマイニングに使われてしまうといった問題も報告されている。最悪なのはこの結果、クラウドの管理者権限までが奪取され、悪用されてしまうケースで、設定が変更され、社内の重要なシステムでのさらなる被害につながる恐れがある。

## 対策のポイントは適切なアクセス制御とログの統合管理

では、具体的にどのような対策が必要だろうか。一例として、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）が参考になるだろう。

ここではセキュリティ基本方針の策定に始まり、組織の整備、資産やデータの特定・管理といった組織やプロセス面での対策に加え、技術的な対策について言及している。



特に多くの記述が費やされているのは、さまざまなリソースに対する「アクセス制御」だ。IT 管理者や利用者がそれぞれどのようなリソースに対してアクセスでき、適切な権限のみを与えるように設定するとともに、実際にそのポリシー通りに運用されているかを監視していく必要がある。万が一何らかのインシデントが発生した場合に備え、ログイン履歴などの証拠を保全できる仕組みとプロセスも必要だ。そのためには、「システム使用状況」や「実務管理者・運用担当者の作業ログ」「障害ログ」などの各種監査ログを取得し、一定期間保存しておく必要がある。

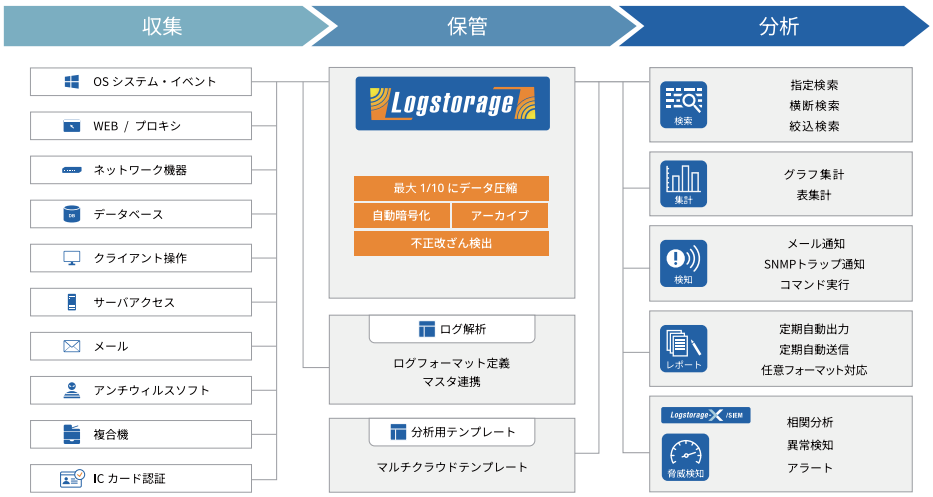
少しスコープはそれるが、ハイブリッドワークで働く従業員のセキュリティ対策においても、認証とアクセス制御と、動作の履歴をたどれるログの統合管理が重要になる。

## 各種クラウドサービスからログを収集し、統合的な管理を実現する「Logstorage」

こうした背景から、クラウド環境、ハイブリッド環境では、これまでにもましてログの収集・管理が重要になる。オンプレミス環境とクラウド、それも複数のクラウドサービスにまたがってさまざまなログを収集し、一元的に把握できる環境を整えることで、リスクに備えることができるだろう。

ただ、経済産業省のガイドラインにも示されているとおり、「ログから得られる情報をクラウド事業者から提供するために、想定以上の時間を要する場合がある」のが実情だ。自社のコントロール下にあるオンプレミス環境とは異なり、クラウド環境の場合、自社が必要とする範囲や深さのログ情報が得られるとは限らない。まずその部分をクラウド事業者と確認し、収集方法を検討する必要がある。

次の課題はログの保存期間だ。これも、オンプレミス環境ならば、予算やストレージ容量といった制約はあるが、自社のポリシーに沿って中長期にわたる保存が可能だ。だがたいていのクラウドサービスでは一定期間後にログは消去されてしまう。このため、後から監査やインシデント調査を行おうと思っても肝心な時期のログが残っておらず、それ以上の解明が困難になる恐れがある。



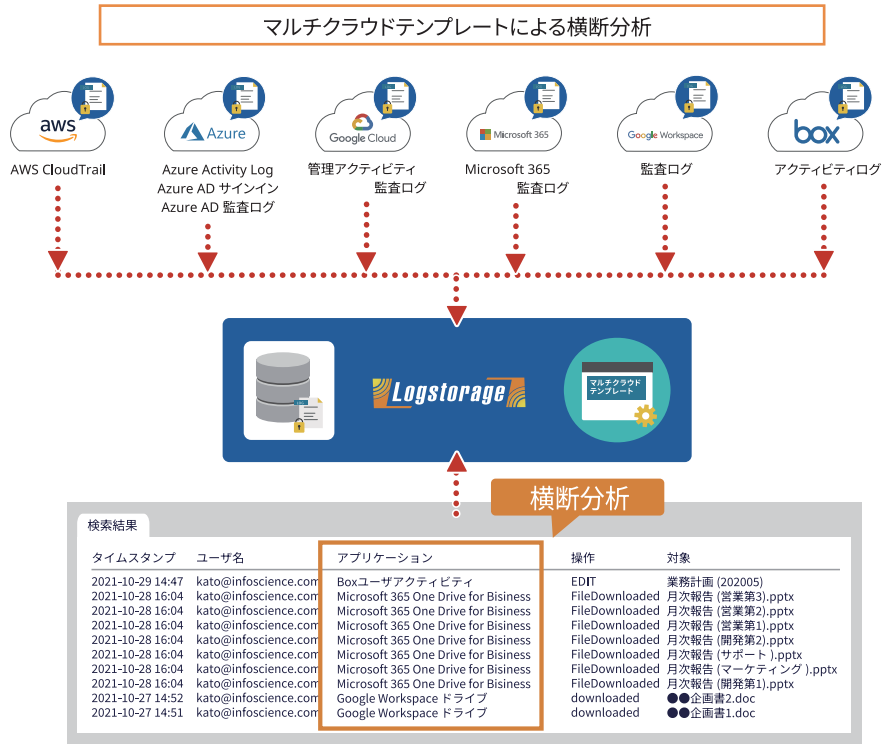

Logstorage システム概要

| クラウドサービス | ファイアウォール | クライアントログ | データベース監査 |
|---|---|---|---|
| AWS<br>Azure<br>Google Cloud Platform<br>Microsoft 365<br>Google Workspace<br>box<br>Cybereason | Palo Alto Networks NGFW | DEFESA Logger<br>MylogStar | PISO<br>SSDB 監査 |
| **PC資産管理** | | **特権管理** | **Webフィルタリング** |
| CWAT<br>LANSCOPE<br>MaLion<br>SKYSEA Client View<br>秘文 | | SecureCube Access Check<br>iDoperation | i-FILTER |

Logstorage 連携製品

こうした部分をサポートするのが「Logstorage」だ。ログの収集・保管を行い、検索・集計・検知、レポートや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、そして幅広いクラウドサービスに対応し、さまざまな種類のログを取り込めることが特徴だ。またログのデータを圧縮し、効率よく長期間に渡って保管することもできる。もしポリシーに反する動きがあればアラートを送るようにキーワードを定義することも可能だ。

ポイントの 1 つは、「マルチクラウドテンプレート」で、マルチクラウド環境においても、複数のクラウドサービスから一元的にログを収集・管理できる。オンプレミス環境でもそうだが、ログの形式はまちまちだが、そこをツール側で自動的に整形し、把握しやすい形で提示することで、ハイブリッドかつマルチクラウドな環境においても、適切な監視体制を構築できるだろう。





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