Insights on IT risk
Business briefing

クラウドへの移行

アーンスト・アンド・ヤングによる
2011年グローバル情報セキュリティ調査

新日本有限責任監査法人
ERNST & YOUNG
Quality In Everything We Do

目次

はじめに

アーンスト・アンド・ヤングのグローバル情報セキュリティ調査はこの種の年次調査の中では最も長い間実施され認知度も高く評価されている調査のひとつです。14年間にわたり本調査はクライアントの皆様が最も重大なリスクに重点的に取り組み強みと弱点を把握し情報セキュリティを向上させるのに貢献してきました。

本調査は誰もが参加できるオンライン調査とは異なりCIO(最高情報責任者)CISO(最高情報セキュリティ責任者)CFO(最高財務責任者)CEO(最高経営責任者)その他の情報セキュリティ担当役員の方々に参加をお願いして実施しています。今年は世界52ヶ国のあらゆる業界の約1,700社にご回答いただきました。2011年度の調査参加者が増えたことは依然として情報セキュリティが組織が現在抱える最重要課題のひとつであることを示しています。

私たちを取り巻く環境はかつてなく変化しており新たな技術に支えられた新たなビジネスパラダイムが次々と現れています。従来型のビジネスであれ新たなビジネスであれますます多くの企業が「クラウド」に移行していくでしょう。その際にクラウドへと移行するのは単に情報だけではなくビジネスモデル全体になっていきます。モバイルコンピューティングソーシャルメディア共有ITインフラ及びサービスの利用が増えバーチャルビジネスが広まっていくのです。

しかしこのような新技術にはリスクも伴います。本調査報告書はそのようなリスクを認識せず対策を取っていない組織に警鐘を鳴らす役割を担っています。

多くの回答者が情報セキュリティ予算の増額を予定しています。その一方でビジネスニーズと組織における情報セキュリティの実態とのギャップが広がっていることも明らかになりました。情報を保護し情報リスクを管理するためにできることが依然として多いのは明らかです。基本に立ち戻り情報セキュリティの全体像を把握して対応できるように明確な情報セキュリティ戦略と改善課題を決めるべきときがきました。

今回の調査への参加をご快諾下さり情報セキュリティに対する見解を忌憚なく話し合い共有させて下さった回答者の皆様に心より御礼を申し上げます。

皆様が抱える具体的な情報セキュリティリスクや課題について直接話し合う機会を持たせていただければ幸いです。そのような話し合いにより皆様のニーズに応え皆様やご所属組織が情報セキュリティやこの分野への投資から得られる価値と信頼を高めるのに貢献できると確信しております。

ポール・バン・ケッセル
ITリスク・アンド・アシュアランス・サービス
グローバル・リーダー

クラウドへの移行

新たな技術に支えられまたコスト削減の必要性に迫られますます多くの企業がネット上の仮想世界へと参入してきています。そういった組織が乗り出したのは「クラウド」への素晴らしい旅であり多くの組織がそれに続くと思われます。

この新たな仮想世界では適切な情報セキュリティの実現が劇的に様変わりし多くの組織にとって「事業を行うためのライセンス」になってきました。私たちは情報セキュリティの役割と重要性に大きな影響を及ぼしてきたそして今後も及ぼし続ける3つの特徴的な傾向を確認しました。

第1にインターネット上でのデータ送受信が増えるにつれ企業の物理的境界が薄れてきています。従業員顧客サプライヤーその他のステークホルダーが自分の都合に合わせて「どこからでもいつでも」データにアクセスできるようになりモバイル機器の幅広い採用によってこの傾向に拍車がかかっています。私たちは昨年の調査ですでにこのような進展を「ボーダレス」な環境と呼んで注目していましたが今日も引き続き組織の主な懸念分野になっています。

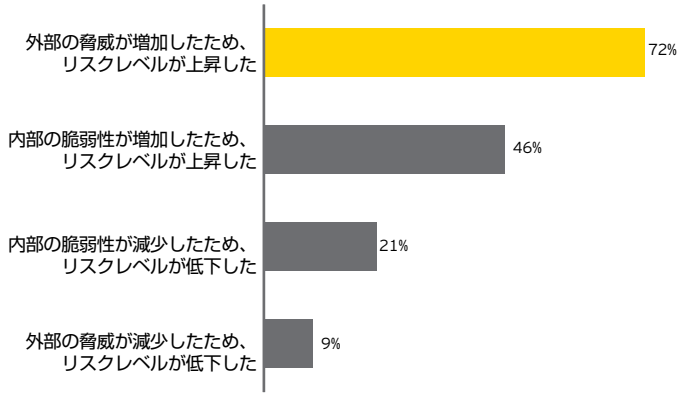
また変化のペースが加速し続けており技術が自動車業界から出版業界小売業界に至る全業界を変革していくのを目の当たりにしました。ここでのテーマは「物質」から「デジタル」への移行です。デジタル化はビジネスモデルに重大な影響を及ぼしつつあります。すなわち従来型の実店舗を持つ業界が本質的にはソフトウェアのみの上に築き上げられたモデルに多数派の座を奪われるあるいは完全に取って代わられてきているのです。本はeブックにCDはMP3に姿を変え自動車は今日では主としてソフトウェアによって制御されるようになりそれらによって消費者に商品を即時に届けまた価値を高めています。

最後になりましたが重要なことは企業が従来型のアウトソーシング契約からクラウド事業者の利用へと移行してきていることです。実際私たちの調査により回答者の61%が現在クラウドコンピューティングによるサービスを利用中評価中または今後12ヶ月以内に利用する予定だということが明らかになっています。これは2010年の45%から16ポイントアップの大幅な増加です。企業がビジネスをクラウドに移行させるメリットを認識しクラウドビジネスモデルへの信頼が高まり続けるなか各企業はより重要な機能を場合によってはITインフラやアプリケーション・プラットフォーム全体をクラウドに移行していくでしょう。その結果企業のビジネスモデルとIT部門は限りない変容を遂げて行くことになります。クラウドへの移行により企業は今やIT業務の大幅削減や廃止を行える可能性を手にしています。

組織が「デジタル化」しクラウドに移行し「ボーダレス化」するにつれリスクの種類が変

わってきています。調査参加者はこの傾向を認識しており、72%が外部からの脅威の増加によりリスクレベルが高くなったと回答しています。しかしながら過去12ヶ月間にこのように高まるリスクに対処するために情報セキュリティ戦略を更新したと答えたのは、回答者の3分の1にすぎません。さらに、回答者の46%が組織の内部からの脅威が高まってきたと指摘しています。

過去12ヶ月間に起こったリスク環境の変化について貴社に該当するものをすべて選択してください。



＊数値は回答者の割合（%）

回答者の72%が外部からの脅威の高まりによってリスクが増大したと回答

サイバー犯罪統計

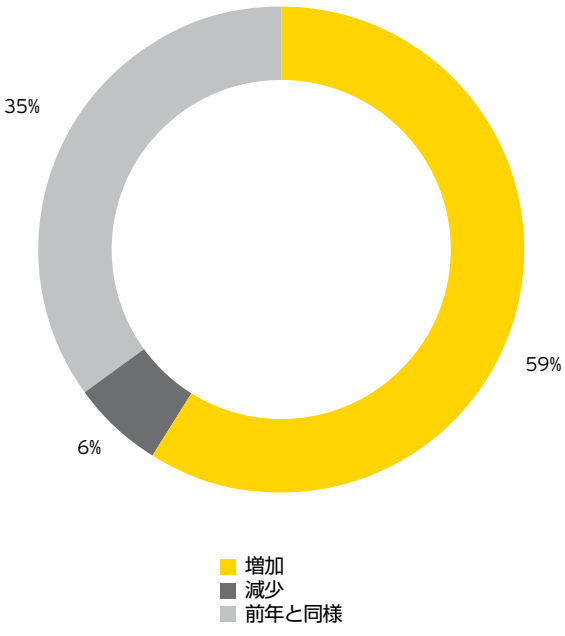
コンピュータ・セキュリティ・インスティテュート（CSI）とFBIが合同で行った『2001年度コンピュータ犯罪及びセキュリティ調査』はサイバー犯罪による経済的損失は調査に参加した約200社だけでも3,700万ドル以上だと報告している。2011年FBIは今年だけでも35万社以上がサイバー犯罪の被害に遭ったと報告している。この発表はサイバー犯罪の大半は報告されずにいることを示している。uscollegeresearch.orgの最新の報告によれば、米国のインターネット利用者の73%、世界のインターネット利用者の65%が、2011年6月までにサイバー犯罪の被害に遭っている。

情報セキュリティの明確化

情報セキュリティはクラウドへの移行を成功させるための重要な要素であり鍵となるものです。回答者の59%が今後12ヶ月間に情報セキュリティ予算増額を予定しているというのは心強いことです。しかしながらそういった資金が本来あるべき賢い使われ方をしていないことを示唆する兆候が見られました。情報セキュリティ戦略を文書化してあると答えたのは回答者の51%のみでした。前述の傾向ーボーダレス化クラウドでのITサービスビジネスのデジタル化ーには課題が伴い十分に考えた戦略と慎重に検討した対応が求められます。行き当たりばったりの解決方法はこれまでは役に立ったかもしれませんが今後はそれでは立ち行かなくなります。単に投資を増やすだけで重点的にやるべきことをやらなければ保護されないと認識することが大切です。

何かが起きてから対応するのではなく実務的かつ事前予防的な対応を取ることが求められます。クラウドなどでのビジネスを支援するために明確な情報セキュリティ戦略を定め情報セキュリティが取締役会でさらに目に見えるようにしていく必要があります。調査結果はその実現までの道のりが長い企業がほとんどであることを示しています。取締役会で毎回情報セキュリティを議題にしていると答えたのは回答者の12%にすぎず情報セキュリティ部門が組織のニーズを満たしていると答えたのは回答者の半数以下（49%）でした。情報セキュリティに対する姿勢についての外部の認識や評価も重要です。企業の情報セキュリティがしっかりしていなければ顧客は企業に自分の情報を預けることなどできずさらにはその企業のビジネス自体を信頼することもできないでしょう。

今後**12**ヶ月間の情報セキュリティ予算について貴社に該当するものを**1**つ選択してください。



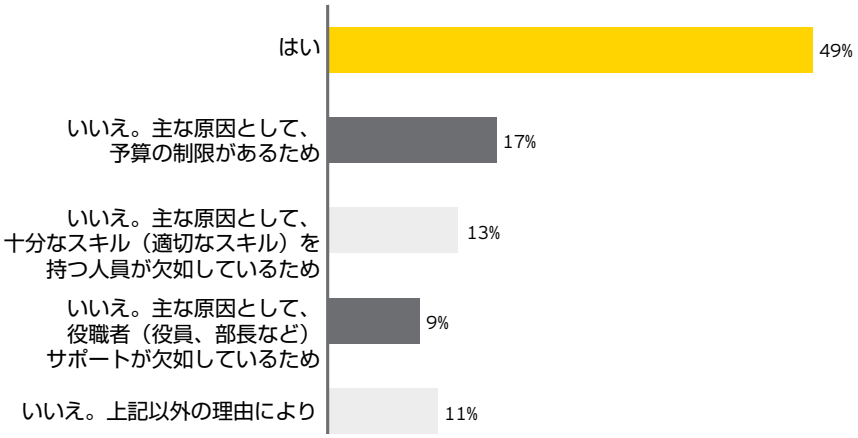
＊数値は回答者の割合（%）

情報セキュリティがサービス及び商品提供の一部となり経営幹部が日々考えることのひとつになるまで情報セキュリティは業績向上の戦略的手段とは見なされないでしょう。

本報告書の残りの部分では組織が現在の環境における情報セキュリティのニーズに具体的にどのように対応しているかを洞察します。また改善機会を分析し今後1年間の情報セキュリティ対策を検討する重要な短期的及び長期的傾向を特定します。

情報セキュリティ部門が組織のニーズを満たしていると回答したのは**49%**で残りの**51%**は満たしていないと回答

情報セキュリティ部門は貴社のニーズを満たしていますか**?**



＊数値は回答者の割合（%）

私たちの見解

- 情報セキュリティについて取締役会で討議すること。明確に情報セキュリティ戦略を定め、可視性を高めること。ビジネスニーズに合致した戦略は事業価値を高めかつ事業を守る。
- 情報セキュリティをサービス及び商品提供の一部とし各人が日常的に意識することのひとつにすること。
- 情報セキュリティは顧客情報や知的財産権など重要な情報資産に重点を置くこと。情報セキュリティが不十分であることでブランドの強化ができないならばビジネスにおける顧客の信頼を失う。

モバイルコンピューティングの進展

タブレットの台頭

過去20年間1990年代後半から2000年代初めの携帯情報端末（PDA）から今日のユビキタスで多機能のスマートフォンやタブレットに至るまで私たちはモバイル機器の著しい技術の進歩を目にしてきました。この進歩が自宅とオフィス従業員同士そして競合相手との境目を曖昧にし、企業の仮想境界を広げてきました。Eメールや会社のアプリケーションへの常時アクセスが新たなモバイル・ビジネス・アプリケーションを可能にし企業の機密データや私的な個人情報へのアクセスや保存を可能にします。言い換えればアクセスの向上は生産性の向上に等しいと同時にリスクの増大にも等しいのです。

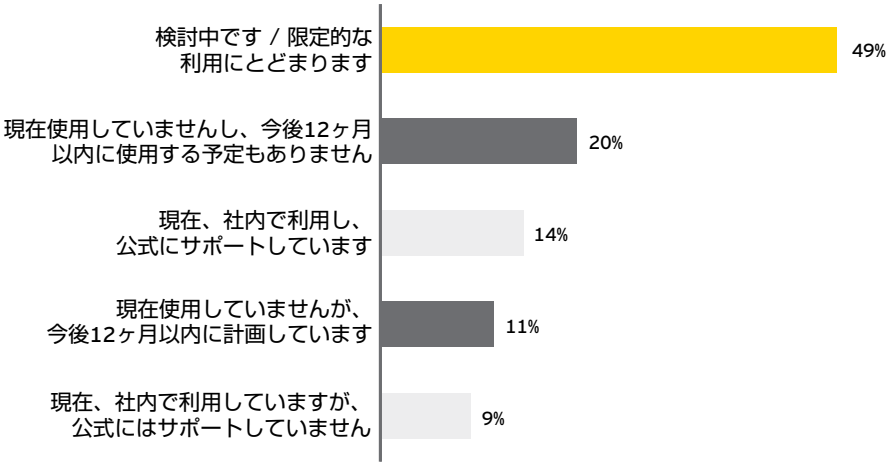
ノートパソコンスマートフォンタブレットの機能の重複が増すにつれてモバイル技術が収れんしてきています。さらに組織によるモバイル採用はかつてないペースで進んでいます。したがって組織は潜在リスクの特定有効な戦略の策定リスク対策の実施に要する時間を短縮して迅速なリスク統合を行う必要があります。

タブレットコンピューティングの採用が急速に広まっていることは調査結果で立証されています。タブレットの使用を許可する予定はないと答えたのは回答者の20%にすぎず回答者の大多数（80%）がタブレットコンピューティングの使用を計画中（11%）評価中（46%）または広く使用している（23%うち9%は使用をサポートせず14%はサポートしていると回答しています。その一方で調査ではタブレットやスマートフォンの採用は最も重要だと思う技術的課題の第2位にランクされ回答者の半数以上が「困難」または「非常に困難」な課題だと回答しています。

個人所有の機器の持ち込み

あらかじめ設定済みのシステムを備えた会社の機器を貸与するかわりに従業員の個人所有の機器にサポートを提供する企業が増えている。個人は会社で使っているソフトウェアとは違うものを使用しており会社の単一のソフトウェアビルドに対応していないが従業員に会社の ソフトウェアの採用を強いる法的権利はないためこれまでの統制方法が十分機能しなくなってきている。さらに従業員が故意または無意識にモバイル機器にセキュリティレベルが低くなるような変更を加える可能性も広がる。たとえば利用者がリモート管理サーバをインストールするかもしれずそのインタフェースが攻撃対象になったり「ジェイルブレーキング」（あらかじめ設けられた制限を非正規に解除すること）などのプロセスを通じて基本オペレーティング・システムの完全性を危うくしたりする可能性がある。

現在業務目的でタブレットコンピュータの使用を許可していますか**?**
該当するものを**1**つ選択してください。



＊数値は回答者の割合（%）

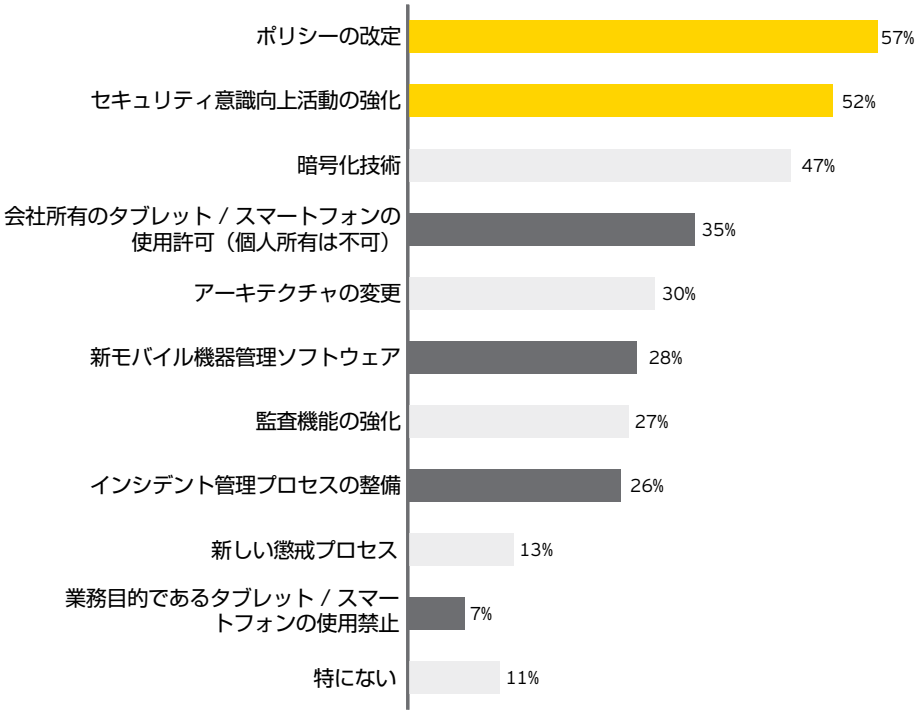
重要な管理対策としての情報セキュリティポリシー

調査結果では「ポリシーの見直し」と「セキュリティ意識向上プログラム」が組織がモバイルコンピューティングに係る新技術に伴うリスクに対処するために採用している施策の上位2位を占めました。セキュリティのガバナンス確立はあらゆる技術を保護するために広く認められた手法ですがモバイル機器とそれに使われているセキュリティ・ソフトウェア製品双方が進化を続けていくことを考えるとこれがますます効果を発揮すると思われます。モバイル機器のリスクについての利用者の意識向上も従業員による誤用が起きるのを抑え利用目的制限に関する方針を利用者に知らせるのに役立ちます。

ポリシーの見直しや利用者のセキュリティ意識向上といった取り組みと並行して企業がそれ以上のことを行う必要性を認識していることもわかりました。実際、上記の手法は万全のリスク緩和策には程遠いものです。そのため企業はモバイル機器用に市販されているセキュリティ・ソフトウェア製品の機能や設計について学び始めています。とは言え動きの速いモバイルコンピューティング市場においてはセキュリティ技術やソフトウェアの採用率はまだ低いのです。たとえば暗号化技術を利用している組織は全回答者の半数以下（47%）にすぎません。

回答者の**57%**がモバイルコンピューティングに関わるリスク低減のためにポリシーを見直している

モバイルコンピューティングを利用する際「新たな」または「増加する」リスクを低減するために実施しているコントロールについて該当するものをすべて選択してください。



＊数値は回答者の割合（%）

私たちの見解

- モバイル機器及びそれに関連するセキュリティ・ソフトウェア製品の双方の使用に関わるガバナンスとガイダンスを構築すること。
- 必須の管理対策として暗号化を使うこと。暗号化を利用しているのが回答者の半数以下だったため組織は暗号化の採用を検討すべきである。
- モバイルアプリの採用前に攻撃テスト及び侵入テストを実施することにより、組織のリスクレベルを制御すること。

クラウドの実態

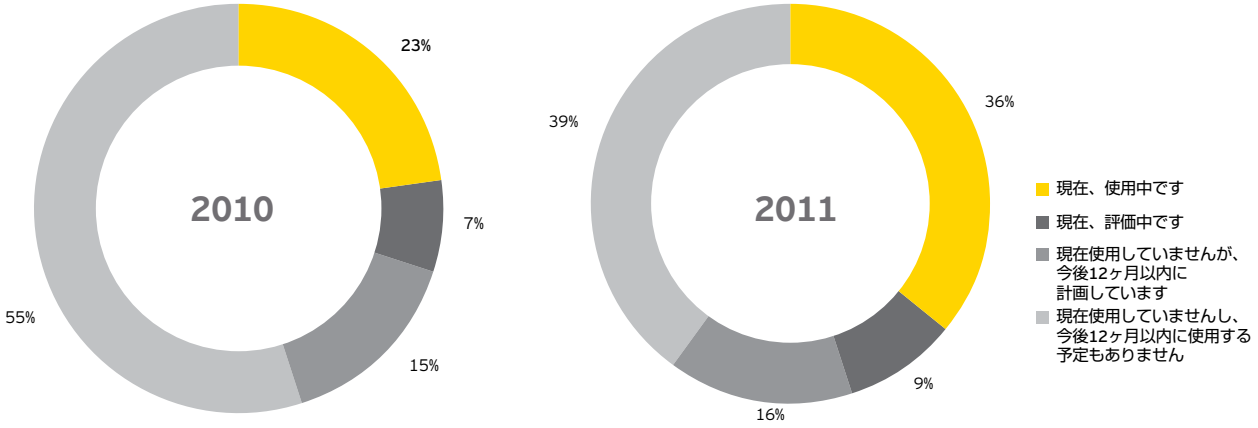
回答者の**61%**が
クラウドサービスを
現在利用中、評価中
または**1**年以内に利用
する計画だと回答

クラウドコンピューティングのメリットの先を見る

クラウドコンピューティングが進化するにつれクラウドサービス利用者も進化してきています。見識あるビジネス専門家はクラウド技術を取り入れることによってもたらされるスピードと効率を認識しています。IT事業を行うことに関心のない組織はコア・コンピタンス（中核事業）に集中しITサービス利用者の立場にとどまることに大きな価値を認めています。従来型のITモデルの場合は基本的なビジネスプロセスを実行するだけでもそのために巨大なインフラと複雑なアプリケーション・アーキテクチャの構築が求められました。クラウドコンピューティングは新しいビジネスユーザーを生み出しました。メニューから注文を決めるのと同じように簡単にどのサービスを消費するか選び組み合わせられる洗練された消費者が生まれたのです。

クラウドを採用したくなるような説得力のある話を聞いても多くの組織はまだクラウドがもたらす影響がよくわからずその影響とリスクを理解する取り組みに力を入れています。情報セキュリティの16分野のうち回答者はクラウドコンピューティングを今後12ヶ月間の投資の最優先分野として挙げており前年よりも投資額を増やす可能性が高い分野の第2位にランクされました。組織が意識しているか否かに関わらず高度に設定可能で迅速に採用できる外部管理アプリケーション（すなわちクラウド）の恩恵を受けるためには代償を払わなければなりませんすなわちトレードオフせざるを得なくなるのです。監査・コンプライアンスなどの管理機関はそのようなリスクの高い決定を下す人材に専門性や経験が不十分な場合があることからこのようなトレードオフを危険だと見なしています。認識の有無を問わず外部のクラウドサービス利用を求めることにより第三者への依存が強まりコア・ビジネス・アプリケーションの内部構造の把握が困難になってきているのです。またクラウド事業者についてベンダー・ロックインが生じ、企業はコンプライアンスリスク契約及び法的リスク統合リスクにも直面するようになってきています。クラウドへの移行は単なる変革プログラムのひとつではなくそれに伴うリスクも含めたビジネスプロセスの全面的な変革にほかなりません。

現在クラウドコンピューティングベースのサービスを使用していますか**?**
該当するものを**1**つ選択してください。



＊数値は回答者の割合（%）（2010年及び2011年の調査結果）

カテゴリー	主なリスクと課題
コンプライアンス及び プライバシー	クラウドコンピューティングは「ボーダレス」な場合が多くてもコンプライアンスはそうではありません。クラウド利用者にはデータがどこに存在するかわからないことが多くそれがコンプライアンスやプライバシー面での課題を生じさせています。たとえばクラウド事業者がサーベンス・オクスリー法（SOX）米国の医療保険の相互運用性と説明責任に関する法律（HIPAA）カード業界データセキュリティ基準（PCI / DSS）米国愛国者法EUのデータ保護法などプライバシーに関する法律の適用対象となる可能性があります。
情報セキュリティ及び データの完全性	社内ネットワークで完結する場合とは対照的にクラウド事業者を利用したデータ処理とその後のインターネット上でのコミュニケーションはデータや情報の脆弱性を高めます。主なリスクに、システムやデータの不正変更、データの不正消去などがあります。そのためにクラウド利用によりアプリケーションのセキュリティ（ID・アクセス管理認証暗号化データ分類に関して新たな課題が生じます。
契約及び法	契約リスクは主に企業がクラウド事業者と締結する契約の種類に起因するものです。このような契約には業務遂行の合意と評価に用いるサービス品質保証契約（SLA: service level agreements）と重要業績評価指標（KPI）を盛り込むべきです。複雑な業者との関係の管理には経験と高度に専門化したスキルが求められます。多くの場合この複雑さのせいでどこで誰がリスクを負うのか把握するのが困難になります。
ガバナンス及び リスク管理・保証	クラウドコンピューティングの利用を開始するならばメリット面とリスク面の両方から見て全体的な事業目標に合致するようにしたいものです。そのためにはクラウドリスク管理手法を含めたガバナンスモデルとクラウド戦略が必要になります。クラウド利用者とクラウド事業者双方を対象とした標準先進的な取り組み（リーディング・プラクティス）ガイダンスについてはいくつかの独立機関が整備中ですが利用可能な合意された基準はありません。
信頼性及び 事業の継続	事業の継続は最優先課題です。クラウド事業者の地理的な事業範囲とそれがクラウド利用者にどのように影響を与えるかを理解することが重要です。加えてクラウド利用者はクラウド事業者の事業継続プログラムとディザスタリカバリ機能に依存しています。またクラウド利用者は事故管理やサービスデスクといったサービス及びサポートプロセス面でもクラウド事業者に依存しています。
統合及び 相互運用性	クラウド上でのシステム統合は重要なものです。システムがクラウド利用者とクラウド事業者の間でやりとりできる必要があります。場合によってはクラウド利用者はこれを実現するために全面的なテストを含めた移行サービスを交渉します。継続的な相互運用性を備えるためには技術変更及びシステムのアップグレード（テストを含む）にも取り組みこれを管理しなければなりません。

なぜ外部のクラウド事業者を理解する必要があるのか

クラウドコンピューティングを利用していると回答した大多数（80%）はSaaS（ソフトウェアをサービスとして提供を 利用している。しかし、状況をより複雑にしているのはSaaSを購入しているつもりでいてもSaaSを提供するクラウド事業者が他のクラウド事業者の提供するPaaS（ソフトウェアを稼働させるプラットフォームをサービスとして提供を利用しておりそのPaaS事業者は共用データセンターのスペースを貸しているIaaS（インフラをサービスとして提供事業者からインフラを購入しているという場合があるという点だ。

簡単に言えばこれは自動車メーカーが提供する車のようなもので、メーカーがエンジンの生産を別の会社に外注しその会社がさらに別の業者に製鋼を外注しているのと同じだと思えばよい。業者間の境界が曖昧になりデータが業者から業者へと自由に流れる世界の中で信頼は貴重な商品となる。だから事業管理に使われるプロセスやデータが信頼でき当てになるという確信を得るためにクラウド事業者との信頼関係の構築が重要になる。

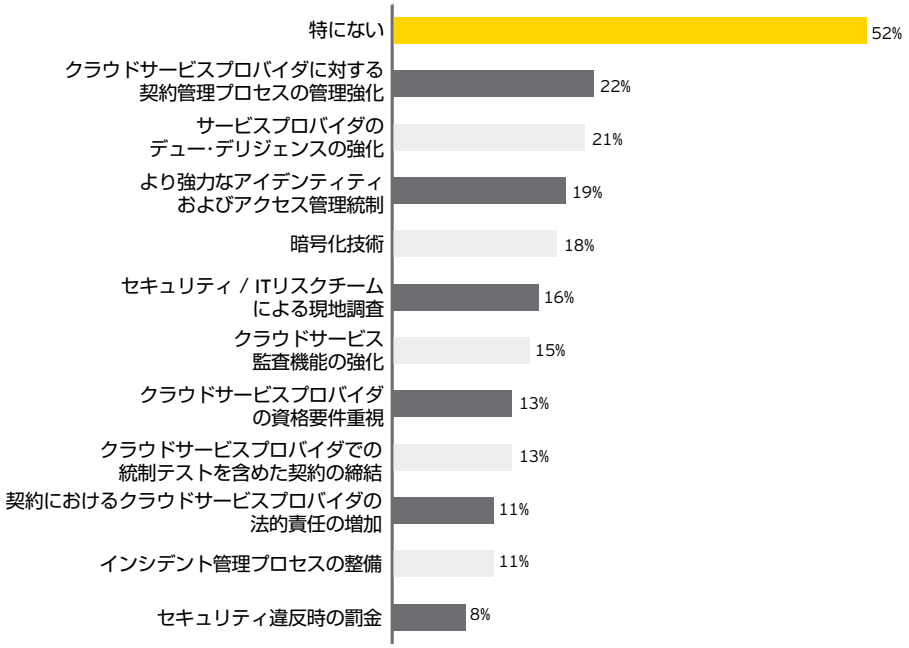
クラウドの実態（つづき）

ガイダンスはどこに

クラウドコンピューティングが進化しクラウド事業者は価値が高くて使いやすいソリューションを提供できるにもかかわらず組織は外部のクラウドコンピューティングをビジネスに統合するのに苦心しています。2011年は回答者の48%がクラウドコンピューティングの実施を「困難」または「非常に困難」だと答えています。半数強の回答者がクラウドに伴うリスクを緩和する管理対策を全く実施していないと回答しています。組織は管理対策にどんなオプションがあるかよくわからないまま利用可能なオプションの一部だけを選んで実施しており何も手を打たないという選択をすることもあります。最も多く取られている対策はクラウド事業者との契約管理プロセスの監督強化ですがこれさえも実施しているのは回答者の20%にすぎず信頼度の高さー誤った信頼である可能性もあるーを示唆しています。

明確なガイダンスがない中で多くの組織が十分な情報を得られないままクラウドに伴うリスクを十分に検討することなく時期尚早にクラウドに移行するまたはクラウドを全面的に敬遠するという決断を下そうとしているようです。調査結果ではクラウドに移行した組織は多いものの、クラウドコンピューティングや仮想化などの新技術の情報セキュリティ対策を実現するのが困難だと答えた回答者が80%に上ることから多くの組織は仕方なく移行したのかもしれません。

クラウドコンピューティングを利用する際「新たな」または「増加する」リスクを低減するために実施しているコントロールについて該当するものをすべて選択してください。



＊数値は回答者の割合（%）

クラウドにおける信頼構築

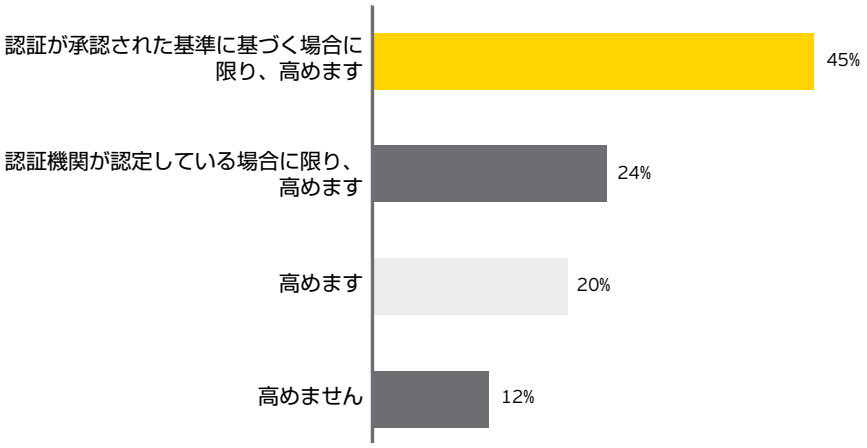
実際に必要なのは信頼に加え妥当性確認と検証認証なのですが回答者の大多数が信頼に大きく依存していると答えています。ほぼ90%が外部認証を支持しており、ほぼ半数（45%）が合意された基準に従った認証のみを支持しています。独立機関による検証や認証に対する市場のニーズを認識している独立機関もいくつかあります。実際クラウド認証に関わる洞察力に富むガイダンスに関しては最近大きな前進が見られました。

多くの組織は認識された課題の多くに対処しサービス認証登録や金融サービス業界が用いているような共通の監査フレームワークを通じたガバナンスプロセスに着手しています。共通の信頼モデルの確立に向けて大きな進展が見られています（クラウド・セキュリティ・アライアンス等）。信頼のコミュニティに参加しているクラウド事業者については多くの回答者が安心できると思うようになると見込まれます。

クラウド業界は進化する必要があります。現在は拡張性カスタマイゼーション低コストといったアピールがクラウドサービスを利用する際の決め手となっています。しかし実際にリスクが存在するからにはクラウドサービスの利用はクラウドがもたらすメリットとの比較という点から検討されなければなりません。クラウド業界が進化するにつれ信頼する力も進化しなければなりません。これは規定された信頼水準が設けられることにより達成されるでしょう。現在この目標に向けて作業をしているグループが民間と連邦政府にあります。組織はクラウド事業者の間で標準化が進むのを促すために業界慣行と足並みをそろえてこれらグループのガイダンスを利用していかなければなりません。クラウドコンピューティングに伴うリスクのすべてに対処するのに外部組織に頼るだけでは不十分です。こういったリスクは組織が事業活動を行う方法に大きな変更を迫りかねないことから正式な企業の手続き及びITリスク管理手続きによって低減を図らなければなりません。

回答者のほぼ**90%**が外部認証はクラウドコンピューティングへの信頼を高めると回答

クラウドのサービスプロバイダが取得した外部認証や証明書はクラウドコンピューティングに対する信頼を高めますか**?**　該当するものを**1**つ選択してください。



＊数値は回答者の割合（%）

私たちの見解

- 検証を信頼よりも上位のものとして位置付けること。
- クラウド契約を結ぶ前に誰がリスクを取るのか把握すること。
- 継続性を考慮して回復能力に関して透明性の高いクラウド事業者を選び、バックアップを構築し復元可能性をテストすること。
- 過去に他の技術に対して用いて効果的だった標準的セキュリティプロセス及び手法を活用すること。
- ビジネスと情報セキュリティ戦略の整合性を取り法規制や業界基準を遵守するために継続的にリスクを評価すること。

ソーシャルメディアでつながる

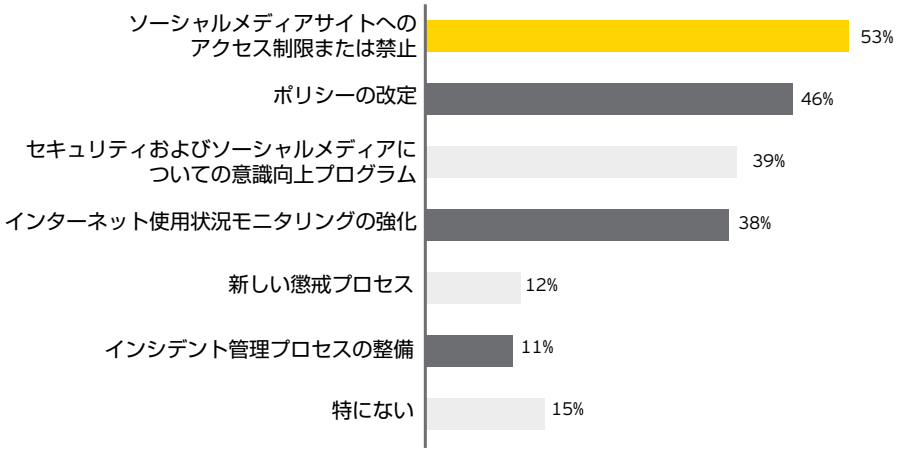
ソーシャルメディアに関わるリスクを緩和するための管理対策として、回答者の**53%**がソーシャルメディアサイトへのアクセスを制限または禁止している

ソーシャルメディアのリスクを直視する

世界人口の約15%にあたる10億人以上が世界で最も人気の高いソーシャル・ネットワーキング（SNS）やビジネス・ネットワーキング（BNS）のサイトに登録しています。もしも世界最大のSNS登録ユーザーがひとつの国を形成するならばその国は中国、インドに次ぐ世界第3位の大国になります。ソーシャルメディアの人気と巨大な成長はそれがもたらす恩恵が大きいからです。ソーシャルメディアによってかつてないほど人が人とつながっていられるようになりそれにより組織は顧客とのつながり方を変革しブランド・ロイヤルティを育てより効果的に販売できるようになります。ソーシャルメディアによって組織はリアルタイムで顧客に向き合い、直接フィードバックを求めることができるようになりそれが市場への提供商品・サービスや市場におけるポジショニングを恒常的に改善していくのに役立ちます。

ソーシャルメディアの採用が増えてきていることがITリスクの様相に影響を及ぼしています。現実には「バーチャルの友人」はソーシャルメディアの世界で与えている印象どおりの人物だとは限りません。ソーシャルメディアのリスクとしてソーシャルネットワークに潜む悪意のあるソフトウェアの取り込み、情報入手に使うアカウントに対するハッキング、機密性を帯びたあるいは当事者にとって望ましくない企業情報や個人情報の公開などが挙げられます。 調査の結果、高い

ソーシャルメディアを利用する際「新たな」または「増加する」リスクを低減するために実施しているコントロールについて該当するものをすべて選択してください。



＊数値は回答者の割合（%）

割合の回答者がリスクを認識していることが明らかになりました。回答者の40%近くがソーシャルメディア関連の問題を「困難」または「非常に困難」だと捉えているのです。回答者のほとんど（72%）が外部からの悪意のある攻撃が一番のリスクだと答えています。こういった攻撃にはソーシャルメディアを利用して個人を標的としたフィッシングメッセージを送って詐取した情報が悪用される可能性があります。

ソーシャルメディアがもたらす潜在リスクに対処すべく組織は強硬路線を取るようになってきたようです。変化を受け入れたり全社的施策を採用したりするのではなく、サイトへのアクセスをブロックまたは制限すると答えた回答者が半数をやや上まわっています（53%）。このような対応は効果的な場合もあるかもしれませんが、（個人所有の）モバイル機器を通じたアクセスが容易になったことで個人が就業時間中にソーシャルメディアに直接アクセスできるようになっているのです。したがってソーシャルメディアサイトへのアクセスをブロックまたは制限しても完全に有効な対応にはなりません。

回答者の40%近くがソーシャルメディア関連リスクの問題を困難だと回答

私たちの見解

- ソーシャルメディアサイトへの厳重な「アクセス禁止 / 利用禁止」というポリシーの適用を再考すること（妥当な場合には）。この対策は社内のハードウェアやソフトウェアに対する外部からの脅威には対応できるかもしれないが個人によるソーシャルメディアの利用が世界的に広まってモバイル機器など別のチャネルを介してソーシャルメディアが間接的に業務利用に組み込まれる状況には十分に対応できない。組織は従業員のこういったサイトの利用をアクセスを制限することなくモニタリングを行うことを検討してもよいかもしれない。
- ソーシャルメディアの強みを最大限に受け入れること。ソーシャルメディアへのアクセスと利用の双方についての総合的な情報セキュリティポリシーを持たなければ企業は競合相手に遅れを取り従業員の間に不信感を生む可能性がある。
- 自社のソーシャルメディアポリシーに打ち出されたセキュリティ対策のベースとなる技術的ソリューションのテストと利用を検討すること。
- 攻撃者がソーシャルメディア上で何を発見するのか理解するために自社で検証を行うこと。

データ流出防止

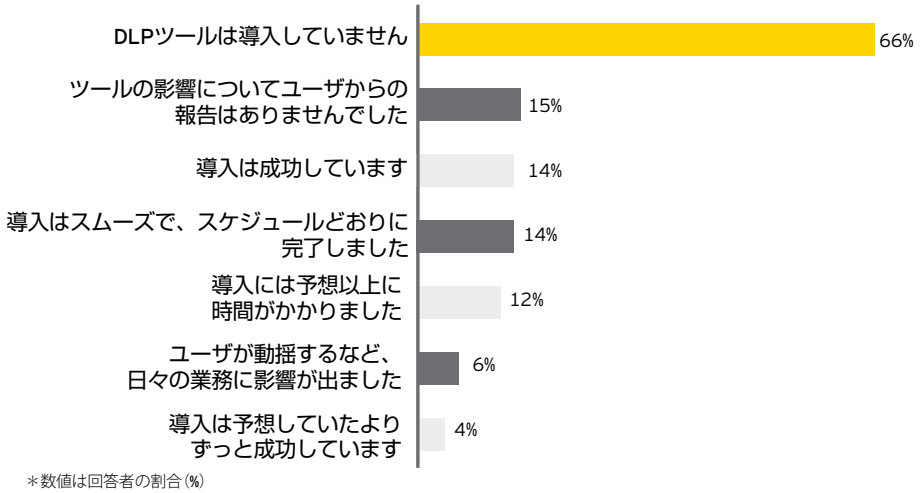
回答者の**66%**がデータ流出防止（**DLP**）ツールを導入していない

データ流出防止の重要性

知識は力でありデータから得られる情報はどのような組織にとっても最も貴重な資産です。最近話題となったデータ流出事件の数々がこの問題への世間の注目を集めました。今までにないボーダレスな事業環境とクラウド採用の増加によりデータ流出リスクが急速に高まっています。モバイル機器により携行されるデータの量が増加したことにより権限のない者が機密データにアクセスする危険性が高まっています。しかし、データ流出は単にタブレット携帯電話ノートパソコンなどの機器の物理的紛失リスクに限られるものではありません。事件の多くは電子送信による予期せぬ開示によっても起きています。多くの場合従業員は暗号化されていないEメールインスタントメッセージ、ウェブメールファイル転送ツールによる機密データの送信に伴うリスクに気づいてさえいません。技術的な利便性とデータへのアクセスは密接に結びついているので意図せぬ機密データの拡散が比較的行われやすくなったのです。

データが流出するセキュリティホールは（技術やプラットフォームの拡大によりすでに大きいのですが）分散型システムや業務コラボレーションツールの利用によりさらに大きくなり企業が社内の情報を追跡し管理するのが一層困難になっています。データ管理の取り組みを複雑にするもうひとつの要因は記憶装置がますます安価で入手できるようになってきていることです。何ギガバイトものデータが従業員のキーホルダーに取り付けられたりスマートフォンに詰め込まれたりして文字どおりドアから「出て行く」ことや低コストまたは無料のクラウド事業者やストレージ事業者を利用して送信するときに傍受されることがあり得ます。

社内のシステムやデータに対するアクセス権のリスクに対応するためアイデンティティ**/**アクセス管理プログラムを使用していますか**?** 該当するものをすべて選択してください。



＊数値は回答者の割合（%）

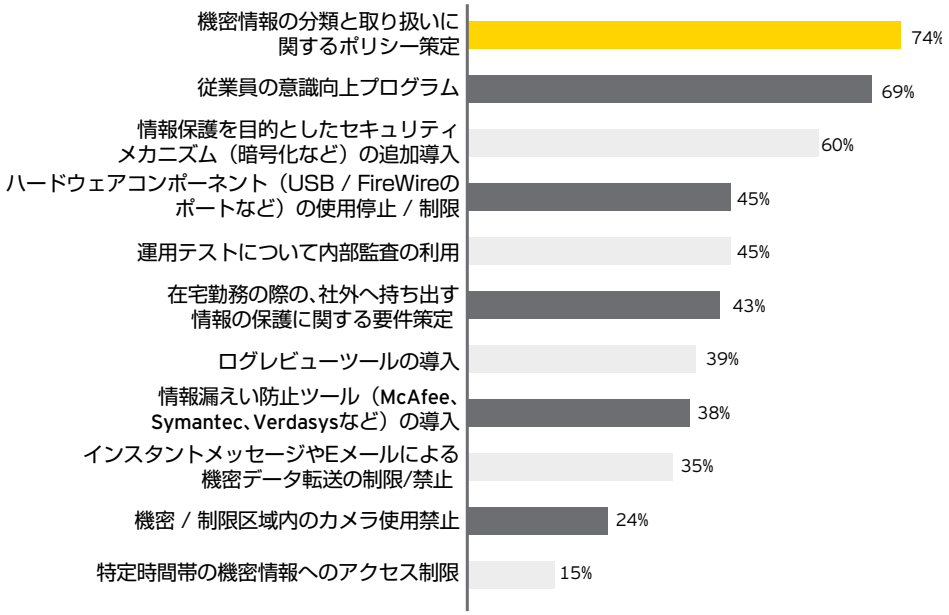
しかしながらDLP技術やプロセスは管理上の最優先事項のひとつとして広く認知されており予算配分を増やす可能性の高い分野の第2位にランクされています。半数以上の企業がDLP関連の取り組みに昨年以上にお金をかける予定です。

機密情報が含まれるデータの漏洩を防ぐために行っている対策として回答者の74%がそのようなデータの分類と取り扱いに関する具体的なポリシーを策定しています。70%近くが従業員の意識向上プログラムを実施しほぼ3分の2が情報保護のための暗号化などの追加のセキュリティメカニズムを実施しています。

ログ管理・モニタリング手法としてネットワーク侵入検知とネットワークの分割などが挙げられます。この2つは外部からの脅威の予防検知対処を行うために導入される対策の上位2位を占めています。さらに来年外部ネットワーク攻撃・侵入評価を実施予定の回答者は75%外部ネットワーク脆弱性スキャンを実施予定の回答者は73%に上りました。

回答者の**74%**がデータ漏洩リスク管理対策として、機密データの分類と取り扱いに関するポリシーを策定

貴社の機密情報漏えい防止対策について該当するものをすべて選択してください。

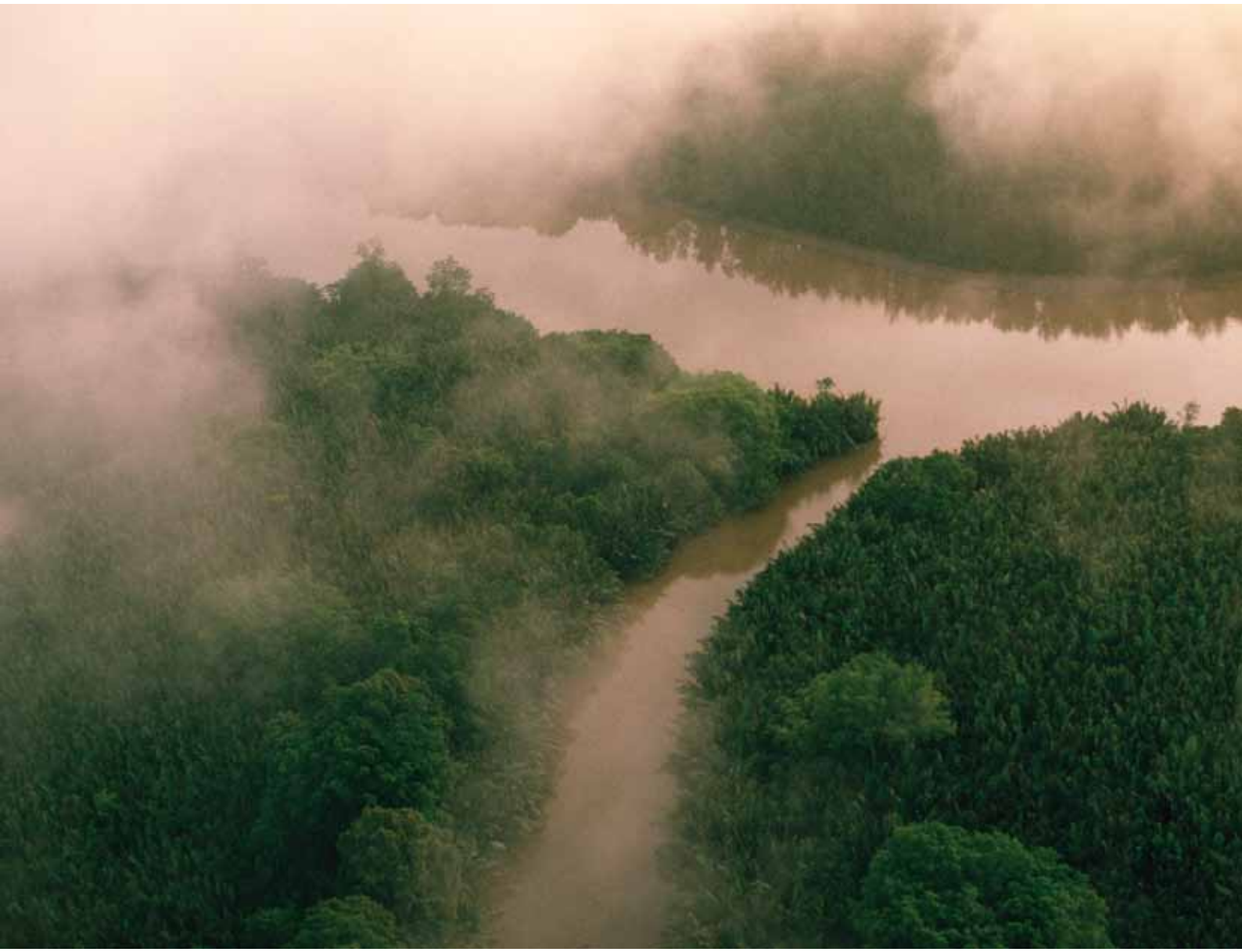


＊数値は回答者の割合（%）

データ流出防止（つづき）

私たちの見解

- 多くの潜在リスク及びデータ流出エリアを評価・理解し正しく認識すること。具体的には組織内に存在するデータ流出経路に関わるリスクを文書化しランク付けをすること。
- 組織が有する最も機密性が高いデータの保護に重点を置いたDLP管理対策が取れるように全社にわたって機密データを識別評価分類すること。
- 主要なDLP管理対策を特定しその有効性を測定することによりデータ流出防止を総合的に見ること。資産管理物理的なセキュリティ管理をはじめデータ流出防止プログラムをサポートする主要な管理対策をすべて理解しデータ流出のリスクと管理対策の正確な報告を提供しなければならない。
- DLP管理対策では移動中のデータ（data in motion）保存中のデータ（data at rest）使用中のデータ（data in use）を網羅すること。
- 事故調査を実施しプログラム実行にあたる強力なチームに協力を求め成功するDLPプログラムを組むために全社の主要なステークホルダーの支援を求めること。
- 企業の機密情報にアクセスする第三者に特別な注意を払うこと。
- どのようなデータがどのようにして第三者に送信されるか送受信のメカニズムは安全か把握すること。組織はデューデリジェンスを行って第三者データスチュワードが企業の機密データ保護のために妥当な保護手段を整備しているか検証する責任を負う。

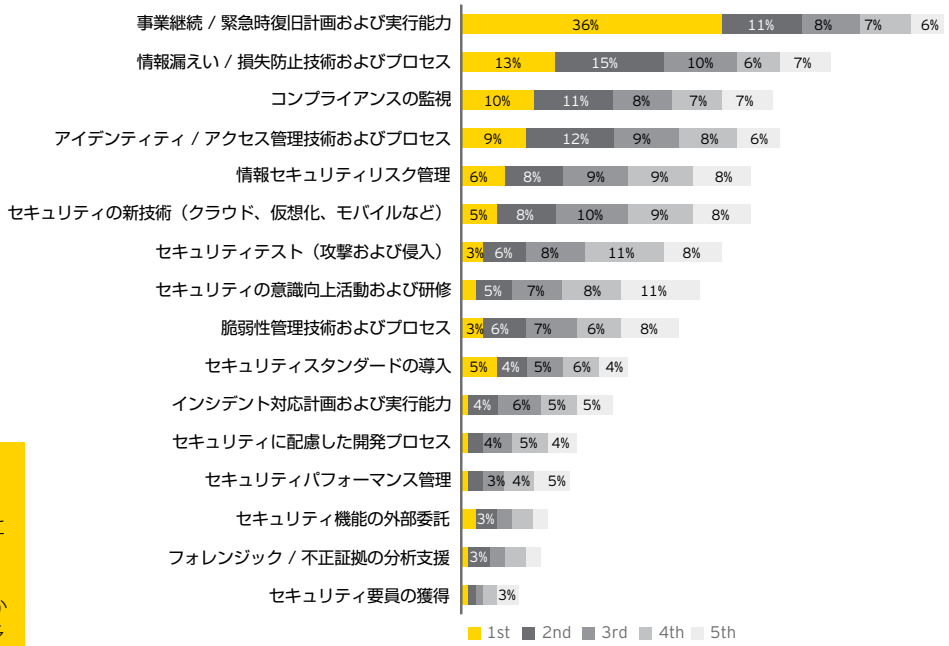


最悪の事態に備える

事業継続計画の必要性

自然災害やテロ攻撃をはじめとする予期せぬ大惨事の発生は個人レベルでもビジネスレベルでも悲惨な損失をもたらしかねません。ボーダレスな世界で組織の規模が大きくなり複雑さが増した分重要リソースが利用できなくなった場合の影響は増大しています。大災害やそれよりも規模の小さな事業の中断は企業幹部に単に幸運を祈るだけではなく効果的な事業継続マネジメント（BCM: business continuity management）に投資して最悪の事態に備えるよう促してきました。ここで情報セキュリティ対策が中心的な役割を果たします。調査結果には次のような傾向が現れています。回答者のほとんどが「事業継続及びディザスタリカバリ」を今後1年間の投資の最優先課題に挙げています。回答者の36%がこれを最優先課題としており第2位となった「データ漏洩及びデータ流出防止対策」を最優先とした回答者の3倍に上っています。

今後**12**ヶ月間で支出予定のあるセキュリティ項目を下記より**5**つ選択し金額が高いものから順に**1,2,3,4,5**と番号を記入ください（**1:**高⇔**5:**低）



＊数値は回答者の割合（%）

「ブラック・スワン（黒い白鳥）」事象

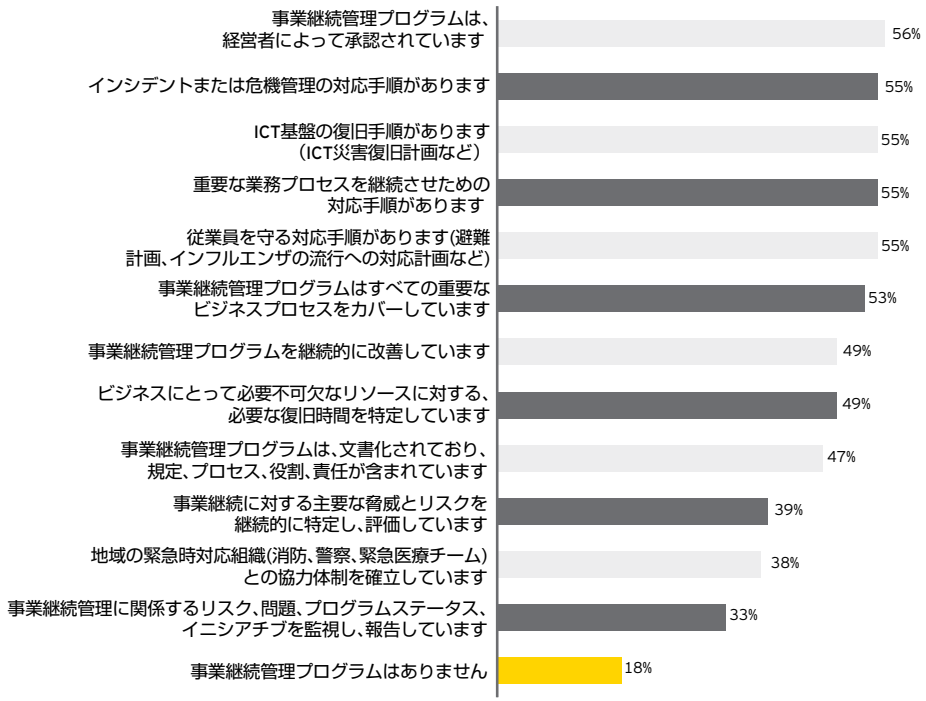
ブラック・スワン事象（黒い白鳥の発見のように実際に起こるまではありえないと考えられ誰も予想しなかった事象）は意図的ではないヒューマンエラー過失悪意のある行為天災といった要因のひとつまたはいくつかの組み合わせにより生じる。原因は何であれ発生が予測・予期できない急展開する壊滅的規模直接的な財務リスク以上の災害を及ぼす命を危険にさらす資産の損害が大きい解決にかなりのリソースが必要といった共通項がある。
（N.N.Taleb, The Black Swan, Second Edition, Penguin, 2010.）（邦訳タレブ『ブラック・スワン』）

とはいえ準備をしていない組織もあります。BCMプログラムを整備していないと回答した組織が18%に上った一方で経営陣がBCM活動を承認していると回答した組織は56%にすぎません。実施している場合でも多くの組織においてBCM計画の成熟度が不十分で肝心のときに機能しない危険性があります。事業の継続が予算配分の最優先項目であるにもかかわらず多くの回答者はBCMを部分的にしか行っていないと報告しており45%もの組織が危機発生時の対応手順、スタッフを守る手順重要な事業プロセスすべてを網羅した計画はないと回答しています。さらに情報通信技術（ICT）インフラが組織にとって決定的に重要であることを考えるとそういったインフラが災害発生時に確実に稼働し続けるようにする手順がないと回答した組織が45%に上ることは注目に値します。多くの組織にとって本当に最悪の事態のシナリオに備えて計画の策定が完了していると自信を持って言えるまでまだ遠い道のりがあることは明らかです。

戦略ガバナンス管理の見地から回答者の67%が事業継続計画を定期的にテストしていますがBCM能力を「維持するための適切なリソース」を持っていると回答したのは52%にすぎません。また災害時の連絡手段としての技術を採用している組織（36%）やBCMデータを管理するツールを利用している組織（28%）は3分の1程度にすぎません。

2年連続で回答者は事業の継続が予算配分の最優先項目だと回答

貴社の事業継続管理（BCM）戦略およびプログラムにあてはまる項目について該当するものをすべて選択してください。



＊数値は回答者の割合（%）

私たちの見解

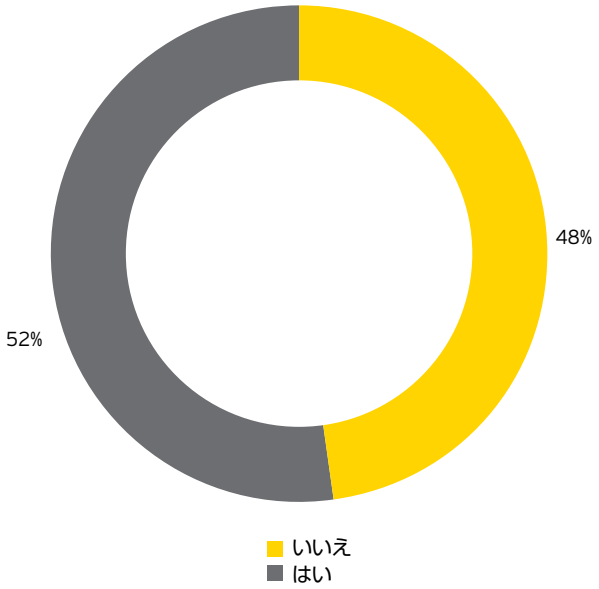
- 発生頻度は低くても影響が大きい事象を予期し組織を壊滅的損失から守ることに重点を置いた広範なリスク管理フレームワークにどれを含めるか決めた上で事業継続計画を策定し実効性を確保すること。
- 最新動向や新技術に照らして事業継続計画の成熟度が適正か評価すること。
- 実際に事業の回復力が妥当か確認できるように組織の事業継続計画を高い頻度でテストすること。テストの際のリスクシナリオが複雑であればあるほどテストで確認できる範囲が広がる。
- 取締役会及び監査委員会に事業継続プログラムへの協力を仰ぐこと。

今後の展望

基本に集中する

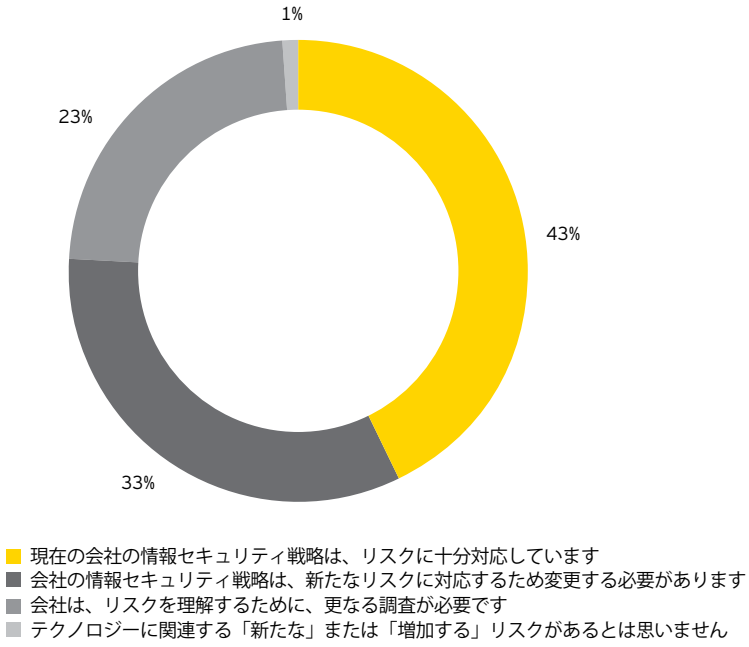
今年の調査結果はリスクの様相が加速度的に変化していることを表しています。境界の希薄化クラウドサービスクラウド上でのビジネスモデルといったものに直面し企業は新たに出現したリスクにどのように対処するか自社戦略の見直しの必要があるか自問しています驚くべきことにセキュリティ戦略を文書化していると回答したのは53%現行の戦略が適切にリスクに対応していると回答したのは47%にすぎません。さらに回答者の過半数（56%が情報セキュリティ戦略を変更する必要がある（33%または新たなリスクを理解するためにさらに調査が必要である（23%と答えています。明確に定めた最新の戦略計画を持つということは企業のリーダーやステークホルダーに対して組織がセキュリティを実現し改善していくためのビジョンと明確な課題を持っていることを示すということです。これにより不透明な霧の中にあった情報セキュリティが目に見えるようになります。それが今日の仮想世界では絶対必要条件である然るべきレベルの信頼を築いていきます。

今後3年間の情報セキュリティ戦略を策定していますか？　該当するものを1つ選択してください。



＊数値は回答者の割合（%）

今日のセキュリティ脅威の背景という観点から貴社の情報セキュリティ戦略に最も該当するものを、下記の項目から**1**つ選択してください。



＊数値は回答者の割合（%）

回答者の**56%**が現行の情報セキュリティ戦略に変更が必要またはさらに調査が必要だと答えている

問題毎に対応するポイントソリューションはもう通用しない

今年の調査結果によると回答者の約3分の1（31%が自分の所属組織が最近情報セキュリティ・ソリューションを購入したものの失敗だったまたは期待はずれだったと考えています。必ずしも最新のツールを入手することが組織に役立つわけではなく基本に集中した方が目的を果たせる場合があります。脆弱性の修正パッチシステム構成の強化適切なソフトウェアの設定などは依然として防御の最前線にあるものです。「Back to Basic（基本に立ち戻る）」プログラムは何百万ドルもするソフトウェアの購入や多目的の新型セキュリティアプライアンスのような派手さはありませんが実効性があることは実証済みです。

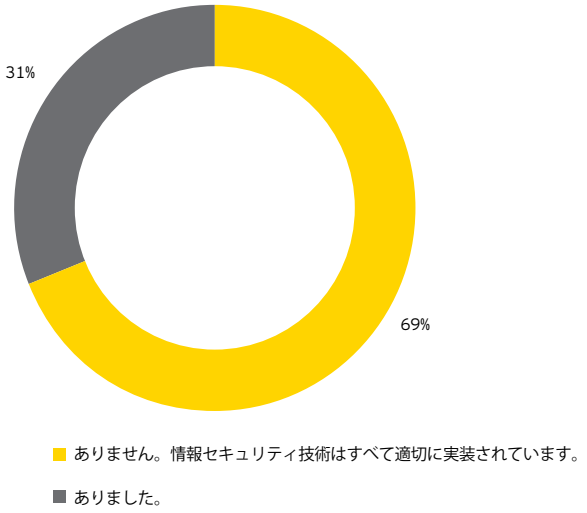
新たに出現したリスク：ウェブサイトに対する脅迫（Web Blackmail）

ある人気インターネットサイトが、DoS（Denial of Service）攻撃を経験し、1時間にわたってダウンした。取引が先に進まなくなり、サイトの所有者は損害を被った。心配した顧客はメールで何が起きているのかと問い合わせてきた。そのほかに、「心配した」セキュリティ会社からのメールも届いた。その会社は、彼のサイトが1時間にわたりダウンしたことを検知し、脆弱性に対するソリューションを提案してきた。その会社は、決して安くはない1回限りの手数料を支払えば、サイトがもうDoS攻撃を受けないことを保証した。また、支払わなければ、明日は2時間、あさっては4時間サイトがダウンし、問題を「解決」するための対価も支払が1日延びるごとに高くなると伝えてきた。

今後の展望（つづき）

過去18ヶ月以内に情報セキュリティ対策のためにソフトウェアやハードウェアを購入して失敗または期待はずれに終わったことがありましたか?

回答者の**31%**が自社が最近購入した情報セキュリティ・ソリューションは失敗または期待はずれだったと思っている



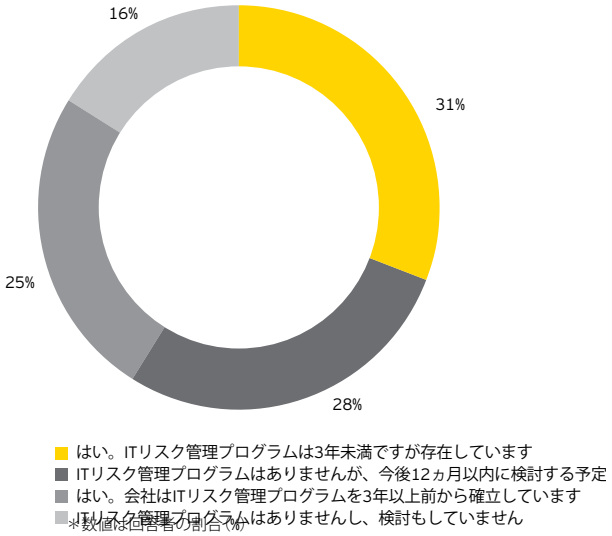
＊数値は回答者の割合（%）

体系的手法としてのITリスク管理の登場

組織はITリスク一般を効果的に管理するために幅広い包括的な視点からITリスク全体を把握する必要があります。このような包括的な視点は組織が現在のITリスクと課題そして今後生じる可能性のあるリスクと課題を特定し管理するのに役立つ出発点になります。これにより組織は、ポイントソリューションに力を入れるのではなく最も影響の大きいリスクに重点的に取り組むことができるようになるでしょう。調査結果を見ると回答者の84%がITリスク管理プログラムを整備しているまたは今後12ヶ月以内に整備することを検討中です。

回答者の**84%**が**IT**リスク管理プログラムを整備している、または**1**年以内に整備することを検討中である

貴社では正式な**IT**リスク管理プログラムはありますか**?**（正式な**IT**リスク管理プログラムには指定されたリーダーリスクアセスメントの実施リスクレベルの測定が含まれます） 該当するものを**1**つ選択してください。



私たちの見解

- 情報セキュリティ戦略を現在のリスクの種類に合致するように見直すこと。
- 最新のツールを入手するかわりに基本的なことに集中的に取り組むこと。
- ITリスクを管理する場合には大きな影響のあるリスクに重点的に対処できるように体系的実用的な手法を実施すること。私たちはITリスク管理またはガバナンス・リスク・コンプライアンス（GRC）手法は多くの組織にとって今後の重点投資分野になると考えている。
- ITリスク管理またはGRCプログラムにおいては情報セキュリティのみならず幅広いITリスク領域全体に対処すること。

調査結果のまとめ

データは仕事の場生活の場遊びの場のいたるところにあります。コンピュータテレビ電話車電化製品上に存在します。一部の世界最大手企業は何十年も事業活動を行う上でデータに依存してきました。しかし最近では世界最大手企業は単にデータを利用するだけではなく事業そのものになっています。

モバイルコンピューティング、クラウドベースのサービスの利用、ソーシャルメディア利用の爆発的な増加ーそしてそういったものがいつも身近にあることによりデータはますますリスクにさらされるようになってきています。2011年グローバル情報セキュリティ調査の結果経済的圧力にもかかわらず多くの回答者がデータを保護し安全管理する必要性を認識していることがわかりました。事実調査参加者は情報セキュリティ関連予算の増額を示唆しています。

その一方で、調査結果は、新たな技術がもたらす課題に対する認識が必ずしもリスクに対処する適切な行動につながっていないことも示しています。調査結果は、ビジネスニーズとそれに対応する情報セキュリティへの取り組み能力とのギャップが広がっていることも明らかにしています。今こそ短期的な解決策ではなく長期的な企業の戦略目標と一体化した包括的手法に重点を置いた有効な戦略的情報セキュリティ計画を策定してこのギャップを埋めるべきときです。

全体

- 回答者の72%が外部からの脅威の高まりによりリスクが増大したと感じている。
- 情報セキュリティ部門が組織のニーズを満たしていると回答したのは回答者の49%である。

モバイルコンピューティング

- 回答者の80%がタブレットPCの使用を計画中評価中または実際に使用中である。
- 回答者の57%がモバイルコンピューティングに関わるリスクを緩和するためにポリシーの見直しを行っている。

クラウドコンピューティング

- 回答者の61%がクラウドベースのサービスを現在利用中評価中または今後1年以内の利用を予定している。
- 回答者のほぼ90%が外部認証はクラウドコンピューティングへの信頼を高めると考えている。

ソーシャルメディア

- 回答者のほぼ40%が、ソーシャルメディア関連のリスクは大きな問題だと答えている。
- 回答者の53%がソーシャルメディア関連リスクを低減するための管理対策としてソーシャルメディアサイトへのアクセスを制限または禁止している。

データ流出防止

- 回答者の66%はデータ流出防止（DLP）ツールを導入していない。
- 回答者の74%がデータ漏洩リスクの管理対策として機密データの分類と取り扱いに関するポリシーを定めている。

事業継続マネジメント

- 2年連続で回答者は事業の継続が予算配分の最優先項目だと回答している。

ITリスク管理

- 回答者の56%が現行の情報セキュリティ戦略を変更する必要があるまたはさらに調査が必要だと回答している。
- 回答者の31%が 自社が最近購入した情報セキュリティ・ソリューションは失敗または期待はずれだったと思っている。
- 回答者の84%がITリスク管理プログラムを整備しているまたは今後12ヶ月以内に整備することを検討していると回答している。

調査手法

アーンスト・アンド・ヤングの2011年グローバル情報セキュリティ調査は私たちのアシュアランス業務とアドバイザリー業務のクライアントの皆様のご協力を得て進めたものです。

今年の調査は2011年6月から2011年8月にかけて実施されました。世界52ヶ国のあらゆる主要業界から約1,700社が調査に参加しました。

調査方法

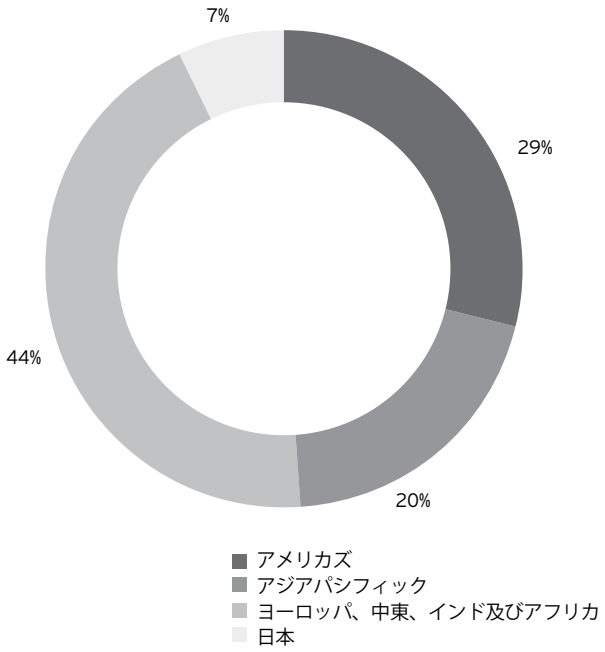
私たちの調査は誰もが参加できる単なるオンライン調査ではなくCIO（最高情報責任者）CISO（最高情報セキュリティ責任者）その他の情報セキュリティ専門家及び役員に参加をお願いして実施しています。

質問票は調査プロセスの一貫性を確保するための指示書とともに各国を担当するアーンスト・アンド・ヤングの専門家に配布されました。

回答の過半数は直接会って聞き取り調査を行って得たものです。それができなかった場合にはオンラインでのアンケート調査を実施しました。

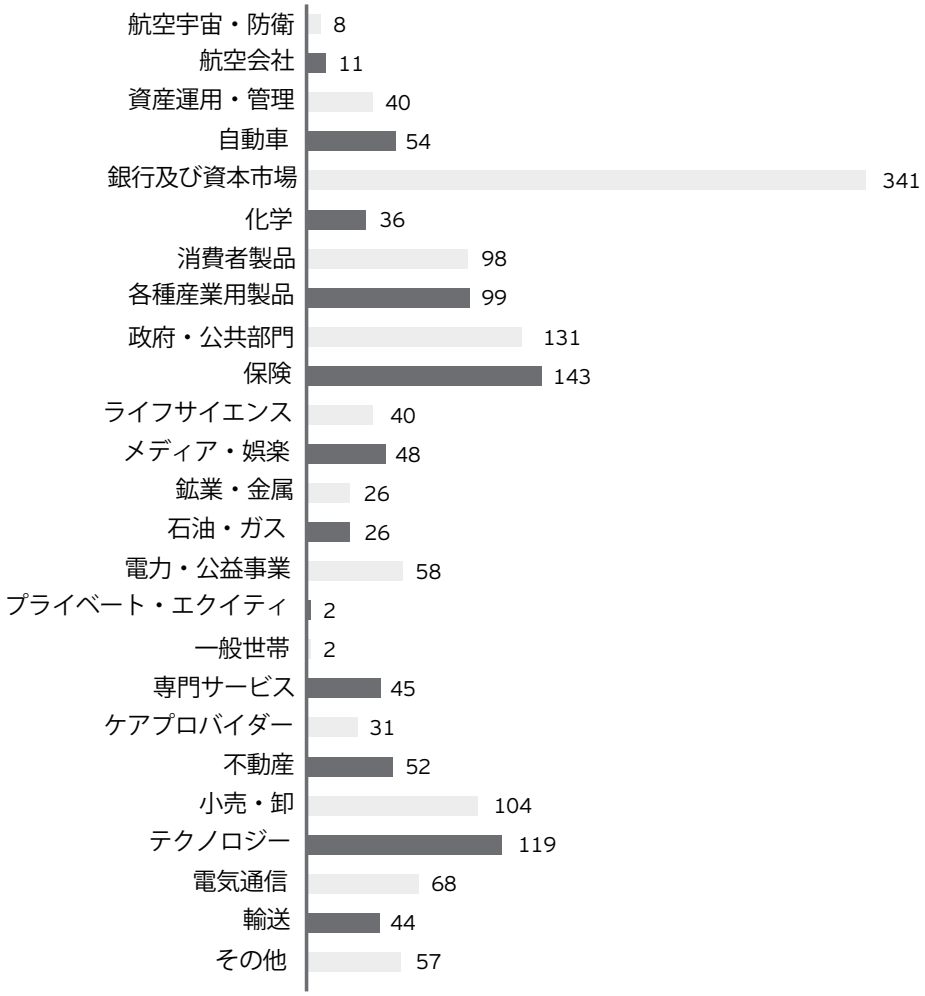
アーンスト・アンド・ヤングの2012年グローバル情報セキュリティ調査への参加をご希望の場合は新日本有限責任監査法人にご連絡下さい。

調査回答者の地域別内訳



＊数値は回答者の割合（%）

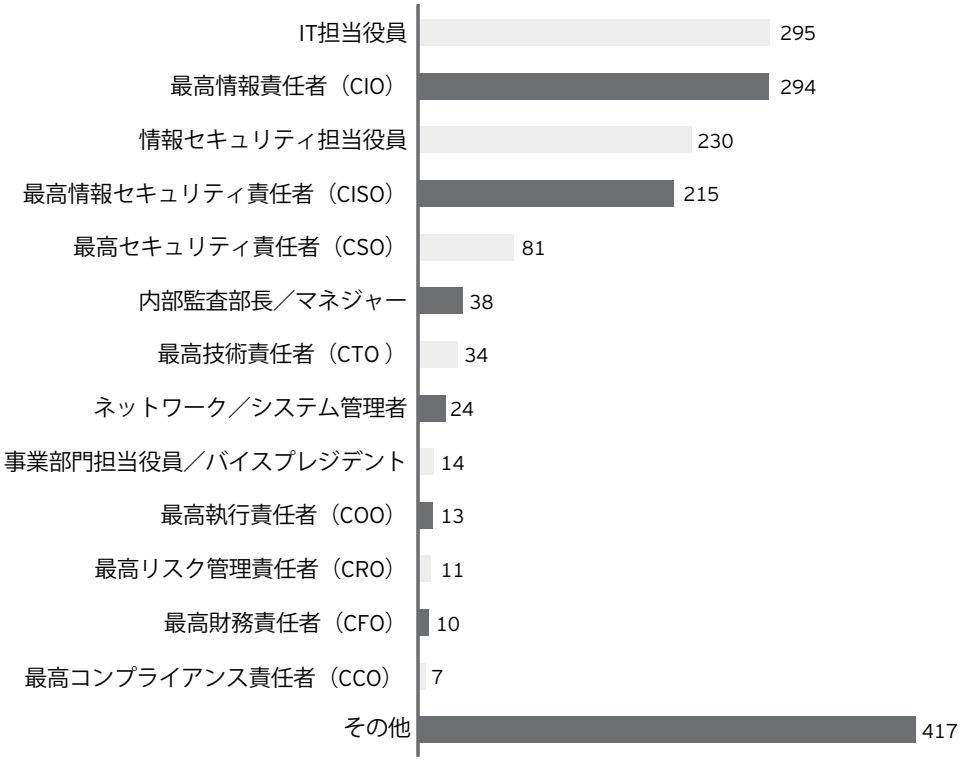
調査回答者の業界別内訳



＊数値は回答者数

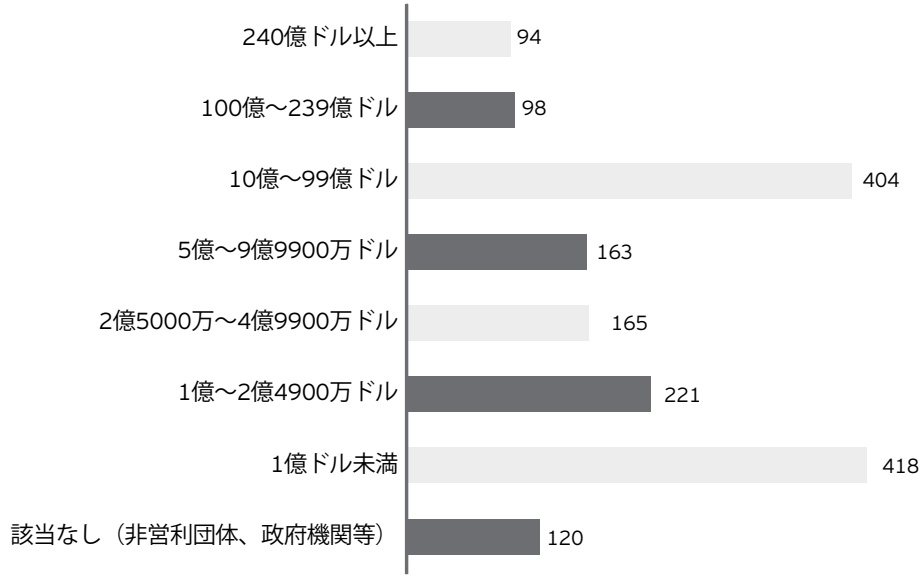
調査手法（つづき）

調査回答者の役職別内訳



＊数値は回答者数

調査回答者の年間売上高別内訳（単位：米ドル）



＊数値は回答者数

Ernst & Young ShinNihon LLC

アーンスト・アンド・ヤングについて

アーンスト・アンド・ヤングは、アシュアランス、税務、トランザクションおよびアドバイザリーサービスの分野における世界的なリーダーです。全世界の15万2千人の構成員は、共通のバリュー（価値観）に基づいて、品質において徹底した責任を果します。私どもは、クライアント、構成員、そして社会の可能性の実現に向けて、プラスの変化をもたらすよう支援します。

「アーンスト・アンド・ヤング」とは、アーンスト・アンド・ヤング・グローバル・リミテッドのメンバーファームで構成されるグローバル・ネットワークを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、ey.comにて紹介しています。

新日本有限責任監査法人について

新日本有限責任監査法人は、アーンスト・アンド・ヤングのメンバーファームです。全国に拠点を持ち、日本最大規模の人員を擁する監査法人業界のリーダーです。品質を最優先に、監査および保証業務をはじめ、各種財務関連アドバイザリーサービスなどを提供しています。アーンスト・アンド・ヤングのグローバル・ネットワークを通じて、日本を取り巻く世界経済、社会における資本市場への信任を確保し、その機能を向上するため、可能性の実現を追求します。詳しくは、www.shinnihon.or.jpにて紹介しています。

本資料はSCORE no. AU0981 の翻訳版です。

連絡先

ITリスクアドバイザリー部

〒100 - 6028
東京都千代田区霞が関三丁目2番5号
霞ヶ関ビルディング28F

Tel : 03 3503 1704
E-mail: AS-Markets@shinnihon.or.jp