BalaBit

ISO 27001　運用管理と監査
Rev. 1.1



2016.01.26

ジュピターテクノロジー

目次

1 要旨 1
2 ミッションインポッシブル 3
3 ISO27001 のコンプライアンス要件 5
4 その他の基準や業界の規範との関連性 9
5 コツとヒント–プラクティスのワースト 7 とベスト 7 11
6 ビジネス上の利点 14
7 要約 17
8 著者について 18

1 要旨

競争の激化に加えて、ISO、PCI DSS、SOX、HIPAA、Basel Ⅱやその他の法的規制のコンプライアンスにより、企業の課題は増大しています。ITシステムに関するセキュリティ要件はとても厳格ですが、ISO/IEC 27001(ISO27001 と称される)基準の実施は、情報セキュリティマネジメントシステムを構成する明確な解決策となり得ます。このドキュメントでは、ISO27001 認証を取得するために管理者が実行することが推奨される要件と、ISO が保証するビジネス利益についての概要を説明します。ベストプラクティスとワーストプラクティスは、ISO27001 システムの実施とオペレーションについても分析されており、企業の中間管理層、または経営陣のための提案が作られています。

データの盗難や IT 悪用の件数は今までに例を見ないほどに増加しており、不適切な方法でのデータ保護は、全ての企業に重大な財務的ダメージと評判のがた落ちを招きます。それを防ぐための最良の方法は、完璧な IT 制御システムの実装です。Gartner 社や Forrester 社のような優れた調査会社は、予防にかかる費用は、サイバー攻撃やデータの盗難が成功した後の回復にかかる費用よりもずっと少なくてすむということに同意を表明しています。

ISO27001 を基にした情報セキュリティマネジメントシステムの実施には、企業からの出資が要求されます。しかし、適切に実施した場合、それは著しいビジネスの優位性をもたらします。“ISO27001 認証”の証明書は顧客や取引先の信頼を高め、電子データと情報のやり取りの安全性を高めます。しかし、このような厳格なシステムは経営陣の深い関与がなければ実施することができません。経営陣は金銭的、そして(法令を遵守するという)道徳的、両方の面からセキュリティの向上をサポートする必要があり、情報セキュリティポリシーの実施が IT 部門のみの責任ではないことを明確にしなければなりません。

ISO27001 規格の要件は特別な IT セキュリティデバイスでのみ完全に満たすことができますが、BalaBit 社が提供するセキュリティソリューションはこの点において役立ちます。

BalaBit 社の syslog-ng ロギングシステムは、一連の処理やデバイスの監視についての ISO 要件を満たす、IT システムの重要な処理に関する、信用できるデータの継続的な収集を可能にします。さらに、ほとんど全てのフォーラムや会議では、重大なセキュリティリスクは人の中に潜んでいて

特権ユーザー管理の実施が最も困難な仕事であることが提示されます。BalaBit Shell Control Box（SCB）は、管理者の操作や暗号化された（または暗号化されていない）チャンネルのトラフィックについての情報を記録し、この問題への信頼できるソリューションを提供します。

2 ミッションインポッシブル

この場合の“ミッションインポッシブル”は IT 技術チームのことではなく、有名なアクション映画のタイトルです。それとどのような関係があるのでしょうか。IT 経営者はいまやアクション映画のヒーローと同じような状況に置かれています。状況は刻々と変化し、予測も出来ないことが起こり、外部からの攻撃が発生し、スパイマスターや内部の敵からの攻撃も受けます。攻撃者はハイテク設備を備えています。いたるところに彼ら攻撃者はおり、あなたのデータを狙っています。
そして IT 責任者はいつも戦う準備をしておき、警戒し、すぐに対応することができるように全ての手順を知っておく必要があります。なおかつ規定も遵守しなければなりません。寝不足の夜だというのに・・・

それは本当に今日の IT 経営者の宿命なのでしょうか？

状況はこれよりも複雑ですが、多くの脅威を廃絶するよい解決策があります。IT システムの保護に加えて、産業によって満たさなければならない様々な要件や法律があります。特に金融機関や上場企業です。ISO、PCI DSS、SOX、HIPAA、Basel Ⅱやその他の法的規制のコンプライアンスは、多くの企業にとって重要な課題です。ビジネスの世界での信頼性、透明性、業務上の友好性を保つことは、競争に利益をもたらす明らかな価値です。そのため、多くの企業は用意された基準に基づいた分かりやすいオペレーションを公表し、様々な ISO 規格の証明書を得ることを目指しています。通常、企業はまず始めに ISO9001 品質（品質保証）管理の証明書を取りますが、主要企業の IT オペレーションの信頼性も同様に重要な課題です。継続的なオペレーションを保証し、ビジネス情報やビジネスデータを守らなければなりません。

2011 年春の最も大きな IT 関連の不祥事は、ソニーでデータが盗まれ、全部でおおよそ 1 億ものユーザーの機密データが間違った手に渡ってしまったことです。そのデータの中には名前、住所、

e-mail アドレス、生年月日、そしてクレジットカード情報も含まれていた可能性がありました。これを書いている時点では全ての詳細に関しては明らかにはなっていませんが、すでに打ちのめされていたソニーの株価は、即座に 4%低下し、これによるどの程度の長期的な損失が続くかは今の段階では見当をつけることもできません。しかし、ソニーはこのような醜聞は二度と起こしたくないと思っていることは確かです。

基準に基づき管理されており、全ての詳細が効果的に運用されている情報セキュリティマネジメントシステム（ISMS）の実施がこの解決策となり得ます。ISMS の最も重要な要件が、国際標準化機構（ISO）が発表した ISO/IEC 27001 基準の中の“情報技術、セキュリティ技術、情報セキュリティマネジメントシステム、要求事項”です。

ではどのようにして安全な運用状態を作り出すのか、そして 27001 認証を得るためにはどのような要件を満たさなければならないのでしょうか。ほとんどの要件に関する解決策は、物理的なセキュリティで作り出すことができ、バックアップシステムで提供することができます。しかし、今のところ、そのような問題は解決されていません。従って、多大な人的努力が必要となります。基準の実施での最も大きなリスクは、特権ユーザーとシステム管理者の仕事の管理にあります。

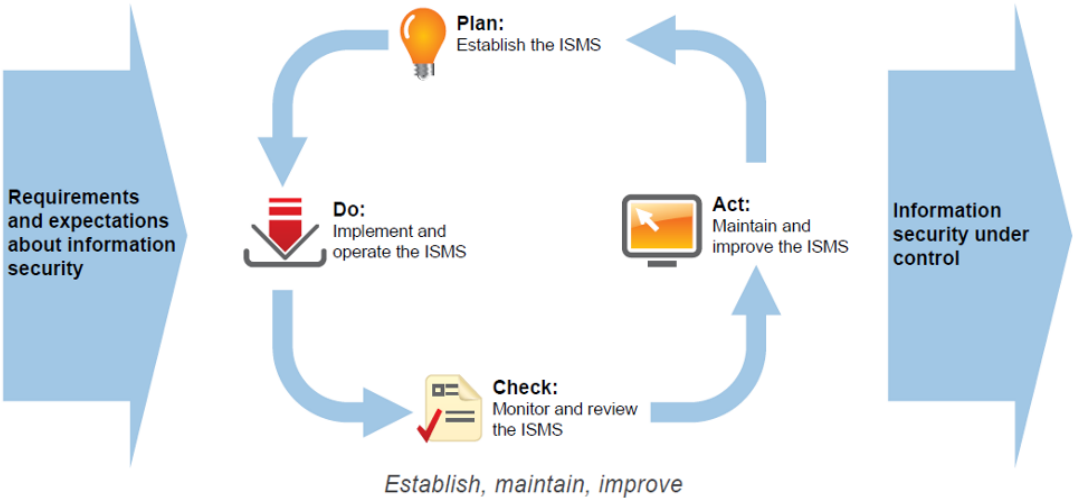
- 全ての権限を与えられたユーザーの操作をどのように管理するのか。
- 外部委託されたシステムの管理者の操作をどのように監視するのか。
- 強固な暗号化（SSH、VPN、SSL/TLS 等）の下で、実行されたファイル操作をどのように管理するのか。
- システムのイベントはどのようにして確実に文書化することができるか。
- 監査のためにどのように証拠を収集するのか。異常な操作をどのように発見し、防ぐのか。
- 不正や悪用をどのように証明するのか。信頼できる証拠をどのように収集し、安全に保管するのか。
- 過去を振り返って、出来事が起こった理由をできるだけ早くどのように調査するのか。正常な操作をどのようにしてできるだけ早く回復させるか。

これらの管理については基準によって規制されており、簡単に実施することができます。BalaBit 社が開発した syslog-ng ロギング製品群は、各、そして全ての重要なログファイルを収集し、これらのログが作られた場所に関わらず、信頼できるタイムスタンプ付きのログの保存を可能にします。特権ユーザーの操作は、BalaBit のほかのソリューションである Shell Control Box(SCB)によって、管理・監査されます。SCB は、暗号化されたリモートアクセスプロトコルを“調べる”ことができ、システム管理者の各操作、全操作、そしてデータ転送を管理・追跡・監査可能にします。

3 ISO27001 のコンプライアンス要件

情報セキュリティマネジメントシステムの国際基準では、以下のような運用モデルが定義されています。

情報セキュリティマネジメントシステムの中核は要件を定義している 27001 規格です。システムの実施中に、最新の IT システムにとって不可欠となる、継続的なメンテナンス及び監視を必要とする処理過程に焦点を置いたセキュリティモデルを確立しなければなりません。一般的に用いられている PDCA（Plan, Do, Check, Act）モデルを実施する必要があります。



このような厳格なシステムは、経営陣の深い関与なしでは実施することはできません。経営陣は、セキュリティを金銭的、または道徳的に(必要条件を強化して)支援しなければならず、セキュリティ対策が IT 部門のみの役割および責任ではないことを明確にしなければなりません。そして情報セキュリティ規制は企業のシステム規制と統合しなければなりません。

ISO27001 の要件は企業の内部ポリシーに組み込む必要があり、また、展開の過程も文書で記録しなければなりません。この文書化の目的は、規制とリスク評価を関係付け、リスク処理手順を検知できるようにすることです。

一般的なセキュリティポリシー要件とは別に、IT オペレーションおよびそれらの管理に関する、特定の要件と記述を確立しなければなりません。そしてさらにポリシーを最新に保ち、全社員が各々

で自分に関連がある要件を学び、納得したことの確認を定着させなければなりません。

組織の確立や変革の間、全社員が自分の仕事に重要な最低限の特権セットのみは受け取れるように保証しなければなりません。また、情報セキュリティ手順の確立中に、役員と管理の職務を分けなければなりません（職務分掌）。保護すべきデータやデータのリスクレベルの決定は、ビジネスを担当するデータ所有者の職務です。

管理者の職務を管理するにはよくできた内部監査システムのサポートが必要です。適切なセキュリティマネジメントシステムの鍵となる要素は、修正手段や予防的統制の確立です。適切に確立していく過程では、狂いが生じたときにそれらの原因が判明し、必要な手段や実行の管理が確実に行われます。

ISO 27001 に基づいて情報セキュリティマネジメントシステムが制定される際には、リスクベースのアプローチが採用される必要がありました。継続的にリスク評価を行う間、企業の目的と要件に一致し、また、起こった結果を確実に比較して再現できるようなリスク評価の手法を選択する必要があります。企業の情報資産を脅かしたり、機密性(Confidentiality)、完全性（Integrity）、可用性(Availability)（この 3 つは情報セキュリティの基本理念で、CIA と呼ばれます）に違反したりするような影響を与える事柄を把握する必要があります。

制度が実施される間に管理が確立されて、情報セキュリティマネジメントシステムの成立、情報の分類、社内の従業員及び社外のパートナーの管理、アプライアンスのセキュリティ及び物理的な保護に対する対策が講じられました。これらの対策は具体的なため、より容易にセキュリティマネジメントシステムを確立する要素となっています。すなわち、要件が定められる必要があり、企業はこれらの要件に沿って運用を行う必要があり、物理的なセキュリティは期待される構造に従う必要があり、ウイルスやハッカーに対する保護システムがインストールされている必要があります。

これらとは対照的に、通信及び運用管理について定めた ISO 27001 の A10 項または A10 項の中の特定の項目は、より漠然としています。”運用の実践と職責が分離されている”間は、違反の危険性は低減されなくてはいけません。A10.2 項では“第三者が提供するサービス、レポート、レコードは常に監視及びレビューされなくてはいけない。また、監査も定期的に実施しなければならない”と定められています。委託され遠方で運用されているシステムの管理において、これを実行することは容易ではありません。多くの場合、管理とは年に一度の監査だけを意味していて、監査の時でさえ、監査人は、ある種の操作が定期的に行われていることを認識するどころか、実際の操作を管理することもできないのです。ふさわしいアプライアンスの手助けなしに、共通のシステム

のリソースを使ってもこの業務は実現できません。業務を実現するには、監査と監視のデバイスが必要です。ここで BalaBit 社の SCB が役に立ちます。SCB は、必要な場合は個々の認証についてもリモートシステム管理に必要なネットワーク接続の制御と監査を可能にします。システム管理者の操作は、フィルムのようにレビューまたは監視され、リアルタイムで制御されます。

監視について定めた A10.10 項も、IT の責任者にとって深刻な悩みの種です。ユーザーとシステム管理者のアクティビティもログに記録する必要があり、ログに記録された情報が不正に使用されたり（読まれたり修正されたり削除されたり）、不正にアクセスされたりすることがないように管理する必要があります。システム管理者のアクティビティはシステムログに記録されていますが、管理者はそのファイルにアクセスしたり、痕跡を残さずに修正したり削除したりすることもできます。この問題を解決するには、syslog-ng ロギングシステムのような専用のツールを使って、独立したプラットフォームに認証してログの収集と保存を行うことです。syslog-ng のソリューションは幅広い種類のプラットフォームと OS に対応していて、ログメッセージを確実かつ安全に転送することができ、暗号化された信頼できる方法でログメッセージを保存できます。

アクセス制御について定めた A11 項には、従来のシステムユーティリティでは部分的にしか対応できません。特権ユーザーや管理者は監視目的でアプライアンスにアクセスできるので、これらのユーザーのアクティビティはきちんと監視されていないのです（A11.2.2 項）。慎重な扱いが求められるデータに暗号化されたチャンネルを通して多くの委託された業者がリモートでアクセスしたり企業の従業員が自分でアクセスしたりしているにも関わらず、ネットワークレベルのアクセス制御、とりわけ企業の境界を越えた接続は問題になります。通常のシステムツールでこの制御を確立することは難しいのですが、SCB は理想的なソリューションです。SCB は透過型で制御されたシステムから独立しているので制御されたユーザーは SCB にアクセスできない一方で、暗号化されたチャンネルを制御して監査できます。

ISO 27001 は、情報セキュリティインシデントの管理についても定めています。違反時に民事的または刑事的に法的責任を問うためには、その事象について妥当かつ信頼できる証拠を収集してその証拠を確実に保守及び保護する必要があります。ログが確実に収集される、すなわち、ログメッセージが暗号化及び認証された上で転送されて、更にタイムスタンプ付で保管されて、そしてその後そのデータが変更されないように保護されていれば、このメッセージからの情報は証拠として使用できます。SCB は管理者のアクティビティと暗号化されたチャンネルのトラフィックについて

信頼できる情報を収集し、管理者のアクティビティをビデオ再生及び検索を可能にして説明責任を果たせるようにします。

法令に沿った要件と制御について、企業が情報セキュリティマネジメントに基づいた ISO 27001 より優れたシステムを確立してそれを正しく運用する場合、そのシステムを定期的にチェックする必要があります。企業のアクションとプロセスが法令の要件、関連する規定、社内の管理に準拠しているかを確認するために、社内の監査が定期的に計画されて実行されます。“ISO 27001 認定”のクラスに分類されるためには、公認の認証機関によって監査が行われていてその監査が毎年繰り返されていることを証明する必要があります。

4 その他の基準や業界の規範との関連性

ISO 27001 は、情報セキュリティに関する国際基準であり情報セキュリティマネジメントシステムの最も重要な根幹を定めていますが、独占的なものではありません。ISO 27001 以外にも情報セキュリティをサポートする枠組み、ベストプラクティス、その他の基準は数多く存在します。ISO 27001 の大きな長所は、コンプライアンスを公式に証明できるという点です。

セキュリティに関しては、業界によってより正確な詳細を定める異なった要件が規定されていますが、それらは基本的に ISO 27001 のアプローチと大きくは変わりません。

違反を防ぐために最も多くの情報セキュリティ要件が適用されているのは、おそらく金融業界です。その中で最も重要なのが、PCI DSS(Payment Card Industry Data Security Standard)、SOX(Sarbanes-Oxley Act)、SAS 70(Statement on Auditing Standards No. 70)、GLBA(Gramm-Leach-Bliley Act)です。上記の基準の中には、クレジットカードのデータと取引のセキュリティに対して適用される PCI DSS のように技術的な要件を詳細に定めたものもあれば、SOX のように IT の要件は厳密には定めずにアメリカの上場企業に対して詳細なコンプライアンス要件を定めたものもあります。一般的に、多くの要件において可制御性、透明性、証拠書類の作成、ログの記録、重要なアクティビティの制御が厳しく要求されています。

技術が進歩してシステムが複雑になったことで、企業を取り巻く IT の環境のレベルは急速に高まりました。もはや専門知識なしに簡単なツールを使えば事足りるようなわかりやすいものではありません。セキュリティに対する内なる脅威は常に大きくなっていて、社外秘のデータが社内の従業員の不当なアクティビティが原因で流出することが増えているため、極めて重要な情報を処理する従業員を管理する必要性が高まっています。簡単に社内のシステムに組み入れられて継続して監視を行い信頼できるデータを提供する、独立した監査ソリューションが急速に必要になっています。大規模な IT システムは日々数十億のシステムメッセージを生成するので、その中から関連する情報を見つけ出すことはますます難しくなっています。

この要件のレベルでのソリューションとは、自動化されて簡単に組み込めるシステムだけを意味し

ます。

BalaBit 社の syslog-ng ロギングシステムは、既存の複雑なインフラにも適応でき、簡単に組み込むことができます。暗号化された署名とタイムスタンプ付のログデータを集めることで、運用の手助けとなる重要なデータを入手できるだけでなく、社内の監査、監視監査、公的な検査にも対応でき、基準となるログ記録の要件を満たすことができます。

ログ記録以外にも、SCB は極めて重要な管理アクティビティの制御を直接手助けします。リモートアクセスヲ使用するサポートアクティビティの制御を可能にし、また、不正アクセスを制御して、重要なアクティビティの監査を常に確実に行います。

5 コツとヒント-プラクティスのワースト 7 とベスト 7

複雑な要件に沿って ISO 27001 を実践して監査を行うと、多くの問題が発生します。この問題は、最もありがちな罠を避けて別の方法を選んでいれば容易に避けることができるものです。例えば、要件やプロセスの確立、物理的なセキュリティの確立など、簡単に解決できるものもあります。本当に困難なのは、システム制御、ログ記録、アクセスと制御、第三者の IT サービス管理、信頼できる監査の証拠の収集です。

BalaBit 社は、システムに元々備わっている機会を利用しなくてもターゲットアプリケーションを導入することで制御の要件を満たすことができると考えている IT セキュリティの責任者の監査を何度か経験しました。制御システムが基準や要件に準拠するのは、要件に従って設定されている場合だけです。例えば、ロギングシステムに関しては、週に一度標準的なリストを確認するだけでは十分ではなく、不正行為は毎日分析される必要があり、問題（操作の失敗や違反行為）は素早く検出され、適切なアラームが規定される必要があります。

企業でセキュリティをサポートするシステムやアプリケーションが導入されたら技術者が休憩できるというのはよくある誤解です。ハイレベルなセキュリティは、手段とプロセスを継続的に管理して保守することではじめて保証されます。

ISO 27001 のシステムやその他の監視デバイスを導入した後、財務の責任者が IT の責任者に経費の節約と即時のコストの軽減を要求することがあります。このような場合、通常、以前は提供されていなかった機能がセキュリティシステムによって補完されるので、プロジェクトと期待される結果は上手く折り合いません。しかし、例えば要件を遵守するために（およそ）3 人の技術者を雇う必要はもうありません。

セキュリティ管理と制御システムの導入に関して、これまでの経験のいくつかの側面を、以下にハイライトします。

データセキュリティの観点からのプラクティスベスト 7

1. セキュリティリスクを特定して評価する
2. 情報セキュリティマネジメントシステム(ISMS)の範囲を決定する： 特に関連する人材と設備を明確に特定する
3. ビジネスの継続性を念入りに計画する： そして計画を改善して定期的に試験する
4. 集中監視（ログ管理）システムを導入する
5. 定期的に監査を行い、自動的にログ分析を行う： 重要な出来事が起こった際にはアラームをあげる
6. 機能分野を詳細に詰める： 両立できない部分を検出する（SOD/職務分掌）
7. データ漏洩（データ損失、データ窃盗）やリスクを分析する、システム管理者の操作を厳しく管理する

抑止力としてのプラクティスのワースト 7

1. 我々は管理者を信頼します、また管理者は誠実です。
   ⇒ これはおそらく本当のことですが管理するということが極めて重要です。リモートアクセスで外部パートナーを管理することが基準で求められています。
2. ログ解析システムの実装サポートは必要ありません、インターフェースはシンプルです。
   ⇒ 我々は監視の微調整としてこれを推奨しません。監査システムは専門技術と経験が必要です。
3. システムのサプライヤーは知識がたくさんあるのでどんな情報が必要か教えてくれます。
   ⇒ これは必ずしも本当のことではありません。内部の専門家が助言して法律分野でも関与することが重要です。
4. 一度必要になったら全員が全てに対して特権持つことがあります。
   ⇒ これは大変危険です。システムは間違いやヒューマンエラーに対して保護されなければならないので違反が起こっていないとしても機能管理は必要です。
5. 我々は同じパスワードを持っていて、皆同じようにしています。
   ⇒ 管理パスワードや共同のユーザーID を共有すると事件の違反者を特定できなくなります。
6. ISO27001 プロジェクトには IT 専門家のみが担当します、それが彼らの仕事です。
   ⇒ 強調したいのは IT セキュリティというのは IT プロジェクトだけではないということです。営業と経営が関与しなければ上手くいきません。

7. ISO27001 認証を獲得しました、そのため情報セキュリティに関して 1 年間は何もする必要がありません。

   ⇒ これは真実ではありません。コンプライアンスと保護を維持するには継続して行動することが必要です。

6 ビジネス上の利点

株式市場に上場している会社に対するデータ窃盗事件が連日ニュースになっています。

以下にここ数年間のデータ不正行為、データ喪失、データ窃盗事件の一例を挙げます。

年	企業	影響を受けたデータ	結果
2011 年 5 月	Sony	1 億人の顧客データ	交換レートの下落、およそ 20 億ドルの収益損失、その他コスト
2011 年 1 月	ホワイトハウス(アメリカ)	25 万人の個人データ	信頼の失墜、物的損害
2009 年	Heartland 請求システム	1 億のクレジットカードデータ	交換レートの下落、その後会社の閉鎖
2008-2009 年	RBS Worldpay	150 万のカードデータ	交換レートの下落、莫大な物的喪失
2007 年	Deutsche Telekom	1700 万人の顧客データ	社会的評価の失墜
2005 年	Cardsystem Solutions	4000 万人の顧客データ	会社の閉鎖

ここにデータに対する不正行為に関する興味深い統計があります。

17%

データ窃盗と攻撃のうち約 17%が正社員による犯行です。(Data Breach Investigations Report 2011, Verizon)

86%

セキュリティ違反のうち 86%が、第 3 者が喚起するまで当事者の企業が発見できませんでした。

96%

事例のうち 96%が適切な管理を行うことによってデータに対する不正行為を簡単に防げたでしょう。(Data Breach Investigation Report 2011, Verizon)

こうした数字は示唆に富むものです。「巨大な」不正事件の犯行の 5 分の 1 が正社員であり、しかもデータの安全性を保護する立場の IT 担当として信頼されていたシステム管理者によるものによるものでした。そのためインターネットに対する従業員の意識がきちんと共有されていなければなりません。影響を受けた企業は必要な規則に従い徹底的に従業員を管理することができていませんでした。必要とされる規則と徹底とはどんなものでしょうか。それは簡単です。常に、継続して全ての重要なプロセスをチェックすることです。

影響を受けた企業が不正を見つけるために適切な手段を講じていなかったため、データ盗難をほとんどの場合において認識していなかったことは驚くべきことです。

機密データの漏洩は大きな損害をもたらします。例えば調査には資金を都合しなければならず、通常のビジネスの業務は崩壊し、損失補償や罰金が必要になります。直接的な損害より間接的な損害の方が深刻となる場合がほとんどです。不正行為が長期的な観点からビジネスの過程に影響を与えます。企業は営業上の信用を失い、株価は下がります。また企業がデータの扱いに軽率だったために倒産に追い込まれたケースさえあります。

Gartner 社の分析によれば、データ関連のセキュリティ事件の後に講じる補償手段の費用は保護のために必要不可欠な IT デバイスの費用より、少なくとも 5 倍になります。例えば IT デバイスとはロギングシステム、IDS/IPS システムや監査を常にサポートするデバイスなどです。分析では、1 万クライアントのアカウントを持つ企業は適切なセキュリティの構築に 1 アカウントあたり約 16 ドルをかけています。試算ではデータの軽率な扱いによる事件の後にかかる費用は 1 アカウントあたり少なくとも 90 ドルです。

この数字は Forrester 分析調査会社の計算と一致しています。同事務所は 28 のセキュリティ事件の回復のコストを分析し、損害は 1 クライアントアカウントにつき 90 から 305 ドルと結論づけています。

上記の事実からみても、最も効率的に費用がかからないように**予防**するためには、適切な情報セキュリティシステムを構築し維持していくということが最善であることは明らかです。データ盗難に巻き込まれた企業の 87%が適切な管理を行っていませんでした。

ISO27001 にもとづく情報セキュリティマネジメントシステムは実行する段階で企業のリソースをかなり必要としますが、うまく実行できれば重要なビジネス上の利点となります。“ISO27001 認証”という分類自体は顧客とパートナーの信頼を高めます。電子データと情報の交換を促進し、より安全なものとします。

例えば IT ツール、デバイス、ケーブリング、データ転送、警報、防火、エアコンなどを含む IT インフラストラクチャー全部を査定し、評価できるといった利点ももたらします。

7 要約

BalaBit の技術を導入し、ISO27001 を取得すると、以下の企業利益を勝ち取ることができます。

- リスクが審査され最少となります
  （例、アクセスコントロール、職務分掌）

- 既存のプロセスと管理が再調査され、向上します。
  足りないものを作成します。

- 予備のデバイスやソリューションが導入され、ビジネスの重要なプロセスのセキュリティと信頼性が向上します。予備のラインやフェールセーフのサーバーといった追加のリソースがリスク分析で認識された重要なプロセスをサポートします。

- IT コストが自動ロギングシステム（syslog-ng）の実装で減少し、ログファイルをレビューする時間が、より早くなり時間が短縮されます。管理機能は自動にすることも可能です（Shell Control Box 4eyes の原理）。

- 管理デバイスを実装することで悪意あるアクセスに対して技術的・心理的な制御となるため、データ喪失、データ盗難のリスク確実に減ります。

- 監査に必要なコストと時間が減ります。システムの情報の関連記録をロギングシステムから容易に検索できるからです。これとは別に Shell Control Box アプライアンスはシステムの全てのドキュメンテーションとデータベース管理アクティビティを再現し、完全な監査情報を提供します。

- 事件の原因を探るのが早くなればなるほど、無計画な分析に要する時間が短くなります。Shell Control Box でサービス水準の管理がより簡単になり、事件が起こってしまったときにより多くの情報を受け取ることができます。

8 著者について

Mr. László Dellei は認定 CISA、CGEIT、CRISC、ITIL-F のでISO 27001 LA のエキスパートです。現在ハンガリーの一流システム企業で IT シニアセキュリティコンサルタントをしています。過去数年間 Mr.Dellei は情報セキュリティに主に取り組んできました。IT Governance と IT Audit のシニアプロフェッショナルです。この間公的・民間機関で多くの課題を実行してきました。多くのプロジェクトでリーダー的存在としてまたプロとしてリーダーシップを発揮してきました。

IT セキュリティ分野で多くの著作があり、セキュリティの様々なトピックで多くのプレゼンテーションを行っています。特に情報セキュリティインテリジェンス分野で新手法やテクニックと、独特のソリューションを模索しています。非常に高い効率性と有効性を達成するためにカスタマーの期待に沿って課題を遂行することが彼の主な仕事です。

日本語マニュアル発行日　2012 年 2 月 20 日

更新日　2016 年 1 月 26 日

本マニュアル原文は『BalaBit Whitepaper ISO　27001』です

ジュピターテクノロジー株式会社 翻訳グループ