

ReadNotify を使ったフォレンジック対応のご提案

フォレンジックとは

フォレンジック (Forensic) とは、「法廷の」「法医学の」といった意味ですが、元々は犯罪現場に遺留された毛髪や血痕、破片などを分析して犯罪との関わりを立証したり、事故の発生原因をシミュレーション解析することを指していました。「デジタルフォレンジック」と言う場合には、コンピュータやネットワークの不正使用や情報漏洩などの違法行為に対して行われる一連の科学捜査という意味になります。

法令による体制整備の必要性

近年、米国のエンロン事件や日本でのインサイダー取引等による被害を未然に防がなければならないという動きや、IT の発達による個人情報流出による被害を未然に防ぐシステムが求められて来ました。この基になっているのは、即ちエンロン等のスキャンダルに対応して資本主義を守るためには経営者に対して性悪説に立った体制が必要だという認識です。また、たとえ内部のごく一部の内部の不心得者の犯行でもその被害が甚大であることから、業務全般にわたって従業員に対して性悪説に立ったシステムが必要だという認識です。日本企業は従来性善説に立って運営されて来ましたが、その認識は変わりつつあります。

その結果、日本では、個人情報保護法、新会社法、金融商品取引法 (日本版 SOX 法) の施行に伴い、企業や団体は内部統制が強く求められ、その活動が適正なものであることを証明できる体制整備が求められる様になりました。企業や団体はその要求に応えること、即ちフォレンジック対応が義務となりました。

例えば、会社法 362 条 4 項 6 号では、以下の様に規定しています。

取締役の職務の執行が法令及び定款に適合することを確保するための体制整備

株式会社の業務の適正さを確保するために必要なものとして法務省令で定める体制の整備

これに従い、法務省令 (規則 100 条 1 項) では以下の体制整備を求めています。

- 一 取締役の職務の執行に係る情報の保存及び管理に関する体制
- 二 損失の危機の管理に関する規定その他の体制
- 三 取締役の職務の執行が効率的に行われることを確保するための体制
- 四 使用人の職務の執行が法令及び定款に適合することを確保するための体制
- 五 当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

内部統制の導入・実施

これらの法令や省令により義務化され、金融庁など監督官庁に毎年提出する内部統制報告書ではその内容の正しさを“担保”しなければならず、業務全体にわたって報告内容の正しさを証明する情報の整備が必要です。

その為の体制は以下の3段階を経て整備することになります；

- 1．現状分析と業務ワークフローの最適化
- 2．業務ワークフローの各段階での報告書作成とその内容の基となる源データを容易に参照できるシステムの構築
- 3．上記システムのレビューと試行

ここで言う報告書の基になる源データは、その正当性が客観的に証明できなければなりません。更に、その客観性は、問題が発生し、法廷での論争になった時に証拠として提出できる精度が求められます。

従って、企業や団体が日常業務で使用する社内文書、社外文書、メールなどの有効性、信憑性を確保しそれを適正に保存（証拠保全）し、解析し、証拠提出できる体制の整備が求められます。且つ、これらの情報が証拠として提出できる為には、その情報が適正なものであること、つまり事後の改竄がないこと、そしてそれらを、何時、何処の誰が作成したか（送ったか）、受取ったか（閲覧したか）が客観的に保障されるものでなくてはなりません。これらの情報が社内（イントラネット内）のみならず、社外（インターネット上）でどの様に流通したかも客観的に証明できる必要があります。

ソリューションのご提案

企業、団体の業務に ReadNotify を組み込むことにより、日常業務で使う社内文書を適正に管理し、会社・団体の健全な経営発展に資することができます。具体的には、社内文書に追跡因子を組み込み、それらがイントラネット内（社内）のみならず、インターネット（社外）でどの様に流通したか、閲覧履歴をログとして記録します。閲覧履歴は記録媒体にコピーし、オフラインで持運び、別の PC で閲覧した場合でも取ることができます。これにより、組織内での文書の取扱いに対する牽制効果も期待できます。

同様に、日常業務で使用するメールのイントラネット、インターネットでの開封履歴もログとして取ることができます。ReadNotify の「認証+送信証書」機能を使えば、メールの送信、開封という事実を第三者の立場から証明し、法廷での検証可能な証拠としてお使い頂ける体制の構築が可能です。

これらのログから社内の情報が社内及び社外でどう流通しているかの報告書を自動的に作成できます。この報告書を内部統制の報告資料の正確さを担保する源データとして必要に応じて参照する様にでき、これにより、より優れた内部統制報告書の自動作成システムを構築して頂けます。

ReadNotify の「認証+送信証書」メール機能の用途は以下の通りです；

1. 当該メールがインターネット網を通して送信された日付と時間の証拠として
2. 当該メールのヘッダーと本体が送信以降書き換えられていないことの証拠として

3. 当該メールがコンピュータ画面上に表示されたことの証拠として、ここでは当該メールを(コンピュータプログラムではなく)人間である受信者が読んだ証拠、及びその行為を行ったおおよその場所、日時、使用したメールまたはブラウザに関する情報も提供します

ReadNotify の「認証+送信証書」機能を使ってメールを送ると、ReadNotify はメールの終りに、そのメールがインターネット上に送信された日時、メールに与えたユニークな連続番号(連番)、メール自体のユニークな暗号識別番号を付加情報としてメールの末端に付加します。更に、このメール全体(通常ヘッダーも含む)とメールの末端に付けた付加情報全体をデジタル署名します。ReadNotifyはこのデジタル署名付きの認証メールを受信者のメールサーバに送り、そのコピーを“送達証明”の添付資料として送信者に戻します。

ReadNotify の第三者としてのメールの送受信の証明は、デジタル認証内に示してある連番を ReadNotify の署名用 Web サイト www.readnotify.com/showsig.asp にアクセスし、指定することにより参照できます。

ReadNotify が作成するデジタル署名に関する詳細は www.readnotify.com/postcert.asp をご参照ください。

機能の提供形態

ReadNotify のこれらの機能は、現在 ASP サービス(<http://www.readnotify.com>)としてご利用頂けます。また、既存の内部統制システムの一部として、インハウスシステムとして企業、団体内のイントラネットシステム内に設置してもご利用頂けます。内部統制システムを ASP サービスとして提供されている企業への提供も可能です。

詳細は販売代理店にお問合せください。

ReadNotify 社について

ReadNotify 社はメール、文書追跡に関するリーディング企業です。ReadNotify の機能は現在 A S P としても提供されています。詳しくは <http://www.readnotify.com> をご参照ください。

参考；

デジタルフォレンジックとは？ <http://www.digitalforensic.jp/C-F.html>

デジタルフォレンジック？ <http://www.cyberpolice.go.jp/column/explanation08.html>

ReadNotify デジタル証明書の署名表示と照合について <http://www.readnotify.com/readnotify/postcert.asp>

ReadNotify 法廷利用のガイド <http://readnotify.com/court.asp>

以上