情報漏洩リスク低減のための内部統制と情報資産管理

Internal Control and Information Assets Management for Reducing Information Leakage Risk

甲斐 賢 Satoshi Kai
手塚 悟 Satoru Tezuka
荒井 正人 Masato Arai

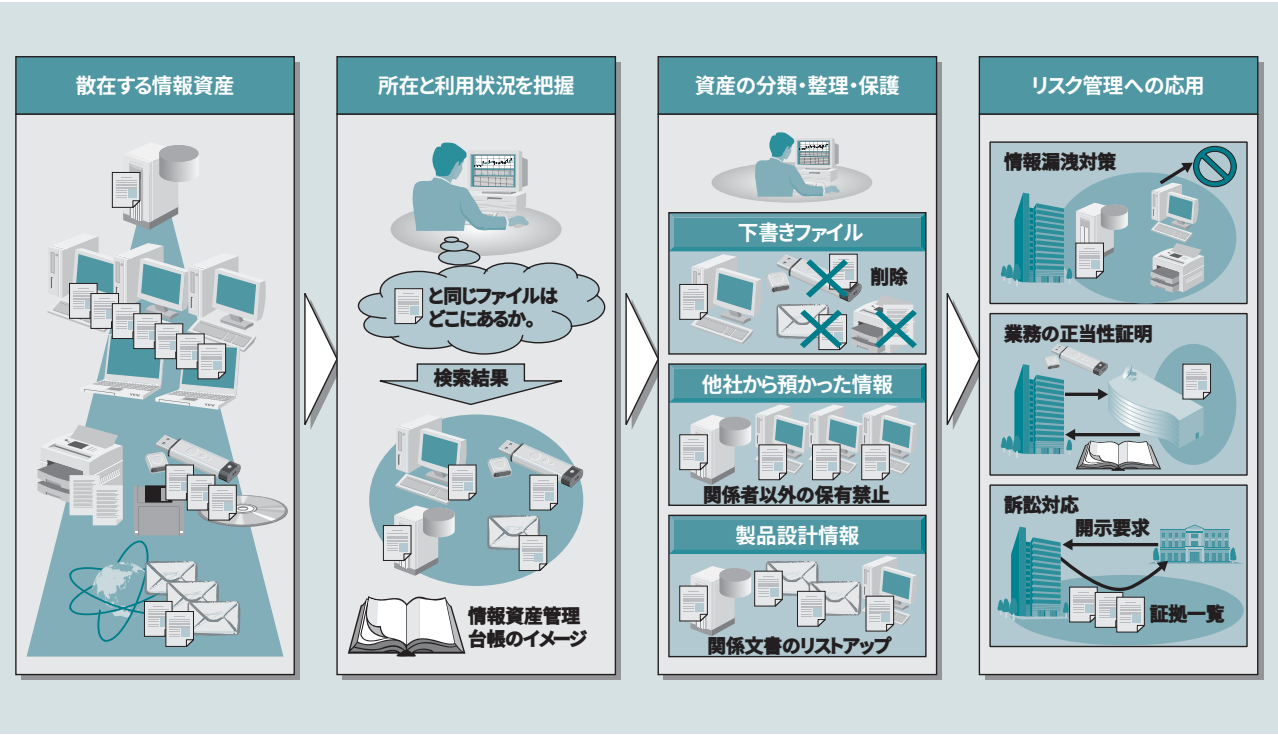


図1 情報資産管理の概念
ハードウェア資産，ソフトウェア資産を管理することと同様に，情報資産（データファイル）の所在や利用状況を把握し，適切なリスク管理につなげることで，情報漏洩（えい）対策，業務の正当性証明，訴訟対応などを迅速かつ効率的に行えるようになる。

情報漏洩事件・事故の多発や，金融商品取引法などを受け，企業はさまざまなリスクに対応するために内部統制を強化することが求められている。内部統制を強化するうえでの課題は，統制に手間がかかり，実施記録の抜けや漏れが生じやすい「手動による統制」にあると考えられる。例えば，情報漏洩リスク対応の内部統制において，自宅PCで業務をしないように社内ルールを定めていても，ルールが正しく守られているかどうかを厳密に確認するための実施記録がない。

日立製作所は，散在する情報資産を追跡するとともに，その利用履歴の記録と適切な保護を行うという「情報資産管理」のコンセプトを掲げ，セキュリティ技術の研究開発を推進している。これにより，事後対応が主であった情報漏洩問題についても，事前措置として対策可能となるような内部統制強化に貢献していく。

1. はじめに

近年，企業におけるセキュリティ対策の焦点は，外部者に起因するインシデントだけでなく，内部者に起因するインシデントにも向けられている。顕著な例は情報漏洩（えい）事件・事故[1]であり，例えば個人情報や営業情報へのアクセス権限を持つ者が，自宅PCで業務を行い，意図せずにウイルスに感染して情報流出事故を起こしてしまうなど，社会問題化している。また，今後は，2006年に制定された日本版SOX法を受け，財務諸表の信頼性，つまり財務データを取り扱う担当者が正しい手順を踏んで財務諸表を作成した経過を客観的に示すことが求められてくる。

このような背景から，企業は「内部統制」を再構築，あるいは強化することが緊急課題となっている。内部統制は手段・プロセスであり，その統制目的は，財務諸表の信頼性をはじめ，情報漏洩リスク対応，アウトソーシング企業が果たすべき業務

の正当性証明など多岐にわたる(図1参照)。

ここでは，情報漏洩リスク対応の内部統制に焦点を絞り，事後対応として近年注目を集めているデジタルフォレンジック※)技術，および事前対応として現在取り組んでいる情報資産管理の研究開発について述べる。

2．内部統制と統制上の課題 ―情報漏洩リスクを例に―

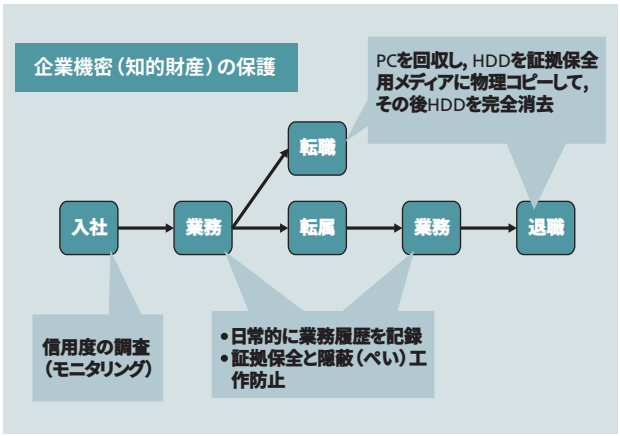
2.1 内部統制整備の一般的な流れ

企業が機密性を保持すべき情報資産は，個人情報をはじめ，営業情報，設計情報など，さまざまである。これらの情報資産を漏洩から保護するには，情報漏洩リスクを洗い出して対策を立案し(Plan)，立案した対策を実施し(Do)，立案したとおりに実施しているかどうかを確認し(Check)，新たなリスクへの対応などの改善を行う(Action)というPDCAサイクルを回す必要がある(図2参照)。PDCAサイクルを回す中で，統制活動の有効性を示す適切なエビデンス(証拠・証跡)を残すことが，その後のステークホルダーに対する報告や説明責任を果たすうえでの基礎となる。

2.2 デジタルフォレンジック技術の活用

PDCAサイクルを回すうえで，Checkは統制活動の有効性確認と改善を図るために重要である。このCheckで活用できる手段の一つとして，デジタルフォレンジック技術が注目を集めている[2)]。この技術は，従来，法執行機関で使われてきた鑑識技術であり，PCのHDD(Hard Disk Drive)に残るレジストリやタイムスタンプ情報などの痕跡を集め，証拠を抽出する。

情報漏洩リスク対応におけるこの技術の活用シーンを挙げると，Winny関連のウイルスに感染して情報流出させたクライアントPCを調査し，いつ，どのファイルが流出したのかを特定すること，また，退職者や転職者が会社を去る前に知的財産の盗用の有無をPC調査によって確認することなどがある(図3参照)。



注:略語説明　HDD(Hard Disk Drive)

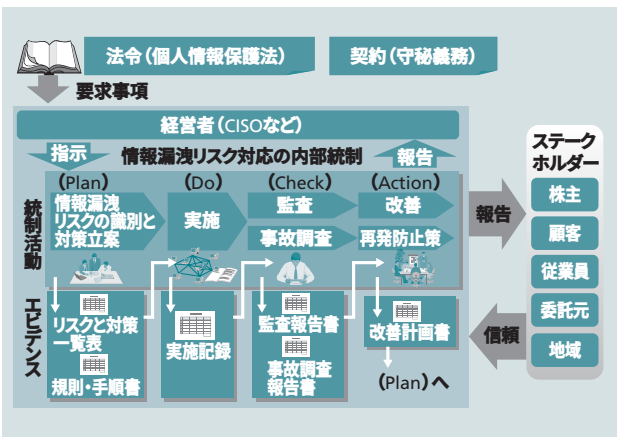
図3　デジタルフォレンジック技術の活用シーン
従業員が入社してから退職するまでの間に，PCを使う業務の多様なシーンでデジタルフォレンジック技術が活用できる。

これらの調査において，例えばPCのHDDを探しても証拠が見つからない場合は，当該PCで過去に接続していた外部記憶媒体をレジストリから調べ，そこから証拠を抽出することもある。

2.3 統制上の課題

前述したデジタルフォレンジック技術は情報漏洩の調査に有用な一方で，鑑識技術ゆえに事後対応の側面が強い。そのため，「時間がかかる」，「確実に解明できるとはかぎらない」といった事後対応固有の問題が残る。そこで，事前の取り組みとして，PlanやDoの改善も必要となる。最近の情報漏洩事例を考慮すると，内部統制を強化するうえで大きな課題が2点

※) デジタルフォレンジックとは，デジタルデータに対する鑑識技術のことであり，不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に，原因究明や捜査に必要なデジタルデータの証拠保全および調査・分析を行うとともに，デジタルデータの法的な証拠性を明らかにする一連の科学的手法・技術を言う。



注:略語説明　CISO(Chief Information Security Officer)

図2　情報漏洩リスク対応の内部統制
統制活動により，リスク対策を行うとともに，活動記録であるエビデンス(証拠・証跡)をベースに，ステークホルダーへの説明責任を果たす。

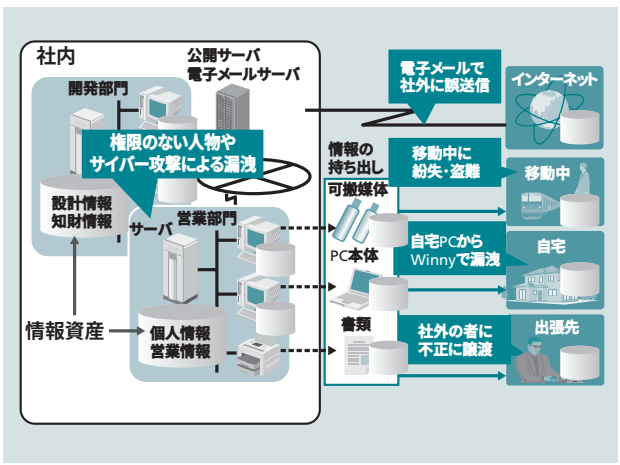


図4　情報漏洩リスクの識別
Planフェーズにおいて，社内に散在する情報資産すべてについて漏洩リスクを識別する。

あると考える。

まず，情報漏洩リスクを洗い出すには，情報資産の識別が前提となる(**図4**参照)。しかし，社内の情報システムを見渡すと，文書管理システムや構成管理システムで一元管理される情報資産もあれば，同等の価値(重要性)を持つ情報資産がクライアントPCや外部記憶媒体などに放置される場合もある。さらに情報資産の洗い出しは，通常，定期的に実施するために，いったんは棚卸ししても業務で活用するうちにクライアントPCに散在することもある。そのため，情報資産の洗い出しに抜けや漏れの多いことが一つ目の問題である。

また，立案した対策を行うDoフェーズでは，通常，ユーザー認証やアクセス制御などの自動化された統制と，管理台帳記録や誓約書へのサインなど手動による統制とがある。二つ目の問題は，後者の手動による統制には不確実性が残る点である。例えば，自宅PCで業務を行うことが社内ルールで禁じられていたとしても，ほんとうに自宅PCで業務を行っていない事実を管理者が確認することは困難である。また，外部記憶媒体を持ち出す際に，管理台帳に持ち出し目的を記入していたとしても，その目的以外に利用していない事実を確認することは難しい。さらに自動化された統制としてパスワード保護された暗号ファイルを外部記憶媒体に格納したとしても，パスワードを知っている本人であればルールを違反するのはたやすいことから，管理者は決して安心できない。つまり，個人のモラルに依存した統制や，実施記録に抜けや漏れのあることが，手動による対策の不確実性を招いていると言える。

3. 情報資産管理の研究開発

3.1「資産」としての情報管理

ソースコードや知財情報などの資産価値の高い情報は，従来から構成管理システムや文書管理システムなどで管理されてきた。これらは情報資産を集約して管理することで，共有に適した分類・整理や，管理者によるアクセス権の設定などが可能となっていた。

しかし，クライアントPC側にも多くの情報資産が散在しているのが現状である。そこには，本来ならアクセスを制限すべき情報資産が多くあるにもかかわらず，適切なアクセス権が設定されていない，多くの者にメールで転送し，今やどこにあるかわからないなど，管理が行き届かないのが実態である。

前述した，情報資産の洗い出しの抜けや漏れ，手動による統制の不確実性は，情報資産を管理することの不備に起因していると考えられる。そのため，社内にある情報資産が，「どこに」あって，「どのように」利用されているかを管理することは，情報漏洩リスク対応の内部統制で重要となる。つまり情報資産管理とは，(1)「どこに」情報資産があり，「どのように」利用されているかを明確化する追跡と，(2)現状では手動で実施している対策をIT対策に置き換えることで自動化/効率化を図り，保護するという，二つの要件を満たすべきと考える。

3.2 情報セキュリティ技術開発のトレンド

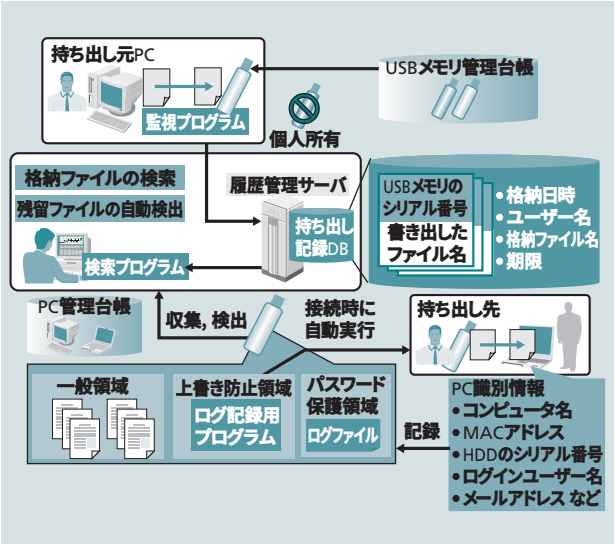
社内に散在する情報資産を「管理する」という観点から分類・整理を試みると，そこでは一切持ち出しを禁止する資産と，業務上，持ち出しを許可せざるを得ない資産に大きく分類することができる。

持ち出しを禁止する情報資産に対しては，セキュアクライアントソリューション[3]の適用が効果的である。このソリューションは，クライアントPC側にHDDを持たせず，情報資産を蓄積しないことで，PC紛失・盗難による情報漏洩を極力抑え込む技術をベースとする。また，クライアントPCでの外部記憶媒体などの周辺デバイスの使用も制限することにより，情報の不正流出を抑止する。さらに，情報流出の経路をネットワークに限定できるため，管理者は電子メールや印刷の監視ソフトウェアを活用し，持ち出し状況を集中管理することができる。

一方，持ち出しを許可せざるを得ない資産に対しては，前述した追跡と保護の要件を満たすようなセキュリティ技術が見当たらないのが現状である。そのため，情報資産を安全に持ち出すことも想定したセキュリティ技術の研究開発も必要となる。

3.3 特徴的な技術

情報資産管理の研究開発は，デジタルフォレンジックの研究から得た知見などを取り入れながら推進している。情報資



注:略語説明 USB(Universal Serial Bus)，DB(Database)
MAC(Media Access Control)

図5 持ち出し記録管理方式
外部記憶媒体ごとに格納ファイルを記録し，履歴管理サーバで管理する。外部記憶媒体の紛失・盗難時にも，被害範囲の影響を迅速に把握することができる。一定期間以上，残留するファイルを検出し，消し忘れを通知する。

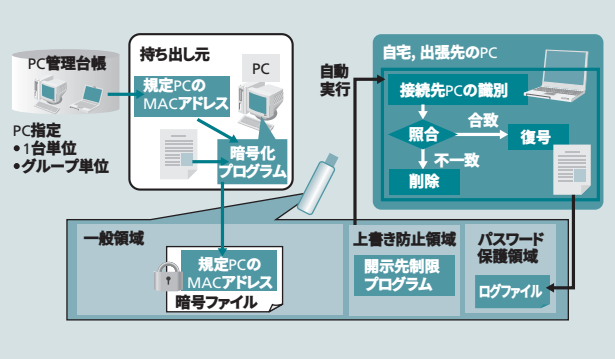


図6　開示先制限暗号方式
持ち出すファイルを自己復号型で暗号化し，規定PCの識別情報（MACアドレスなど）を暗号ファイルに格納することにより，自宅PCや不審なPCでの閲覧・編集を防止する。

産が存在する場所は，サーバ，クライアントPC，紙，外部記憶媒体など多様であり，それらすべてに対して情報資産を追跡し，適切な保護を行うことを研究テーマとする。

特に管理者から見たときに目が行き届きにくい個所として，低価格かつ大容量化している外部記憶媒体〔特にUSB（Universal Serial Bus）メモリ〕による情報持ち出しを中心に研究開発を推進している。

外部記憶媒体による情報資産の持ち出し時には，通常パスワードで保護された暗号ファイルを格納することや，指紋認証によって本人認証を強化する対策，および時限消去によって放置を防止する対策などもある。しかし，そうした既存の対策では，持ち出した本人が持ち出し先でどのように利用したかを，管理者が把握することは困難である。

そこで，まず外部記憶媒体への書き出し時には，どの媒体に何を格納したかをクライアントPCで記録する（図5参照）。外部記憶媒体をシリアル番号などで個体識別し，識別できない外部記憶媒体や，規定外の外部記憶媒体の利用は一切禁止する。これにより，クライアントPCから「どの」外部記憶媒体に，「何の」ファイルが持ち出されているかを管理者が把握できる。

次に持ち出し先では，どのクライアントPCに接続したかを，外部記憶媒体内から自動実行されるプログラムが監視し，媒体内に記録する。このプログラムは，持ち出し先の機器や利用者を特定するための情報を取得することで，「どのように」媒体が利用されたかを自動的に記録する。社内に持ち帰ったときにその記録をPC管理台帳と突き合わせることで，規定外のPC接続の有無を確認できる。以上により，追跡の要件を満たす。

また，持ち出し先で不正に情報流出しないように，外部記憶媒体への書き出し時には自動暗号化を行う。そのファイルの復号化時には，外部記憶媒体から自動実行されるプログラムに問い合わせ，規定PCで処理されているかどうかを判定する（図6参照）。もし規定外PCで復号した場合には，ファイルを削除する。復号可能なPCの指定は，持ち出し元で，例えばワークフローによってPC管理台帳から選択することを想定している。これにより，前述した保護の要件を満たす。

4．おわりに

ここでは，デジタルフォレンジック技術と情報資産管理の研究開発について述べた。

情報資産管理の重要性は，ITが普及したころから叫ばれているが，特に近年の情報漏洩の事件・事故の多発や内部統制ニーズの高まりを受け，今後ますます重要性を増すものと考えられる。情報資産管理を実現することで，情報漏洩対策にかぎらず，情報資産を預かって業務を行うITアウトソーシング企業の正当性証明や，法執行機関から電子証拠を開示要求された場合に迅速に提出することにも応用可能である。また，紙の情報資産については，電子透かしプリントソリューション[4]と連携しつつ研究開発を推進するとともに，情報の持ち出しに関するこの研究開発の成果を活用して早期に製品開発を図っていく考えである。

参考文献など

1）NPO日本ネットワークセキュリティ協会，http://www.jnsa.org/
2）デジタル・フォレンジック研究会：デジタル・フォレンジック事典，日科技連出版社（2006.12）
3）日立セキュアクライアントソリューション，
http://www.hitachi.co.jp/products/secure_client_solution/
4）日立電子透かしプリントソリューション，
http://www.hitachi.co.jp/Prod/comp/Secureplaza/sec_prod/densisukasi/index.html

執筆者紹介

甲斐 賢
1998年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，デジタルフォレンジックの研究開発に従事
情報処理学会会員

荒井 正人
1992年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，セキュリティソリューションの研究開発に従事
情報処理学会会員

手塚 悟
1984年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，セキュリティシステムの研究開発に従事