(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-148731
(P2007-148731A)
(43)公開日　平成19年6月14日(2007.6.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 40/00	(2006.01)	G06F	17/60	234E	5B017
G06F 21/24	(2006.01)	G06F	12/14	560C	

審査請求 未請求　請求項の数 2　OL　（全 12 頁）

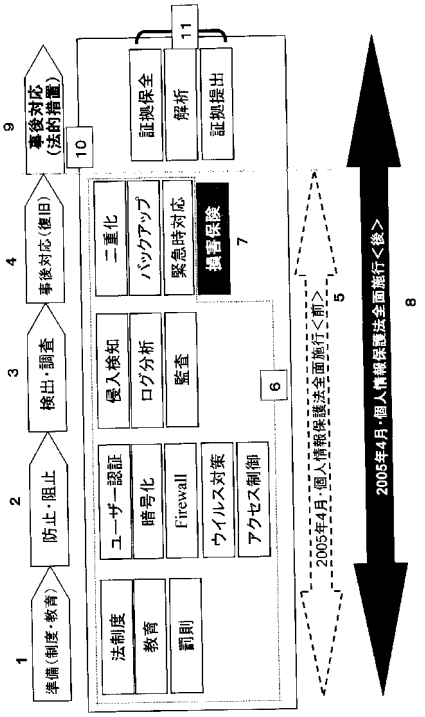
(21)出願番号　特願2005-341650 (P2005-341650)
(22)出願日　平成17年11月28日 (2005.11.28)

(71)出願人　304063864
株式会社ＵＢＩＣ
東京都港区港南２－１２－２３　明産高浜ビル７階
(74)代理人　100087790
弁理士　尾関　伸介
(72)発明者　守本　正宏
東京都港区港南２―１２―２３明産高浜ビル７Ｆ　株式会社ＵＢＩＣ内

Ｆターム(参考)　5B017 AA04　AA07　CA07

(54)【発明の名称】フォレンジック事後対応付き情報損害保険システム

(57)【要約】
【課題】個人情報の漏洩による損害に対して保険金を支払う情報損害保険システムであって、犯人の特定及び法的措置という事後対応を行うフォレンジックを損害補填の内容とする情報損害保険システムの提供。
【解決手段】個人情報の漏洩に対応した従来の損害保険では、個人情報の漏洩により発生した損害を金銭的に補填するものであったが、本発明の損害保険システムは、金銭的補填に加えて、証拠保全、解析および証拠提出という法的措置を補填の内容とする。証拠保全工程では、書き換えがなかったことを証明するために、情報漏洩の不正行為に関与している可能性のあるコンピュータのHDDのデータのコピーを行い、そのコピーは、HDDのデータを一切書き換えることなくコピーが行えることを証明された証拠保全用コピー機で行い、該コピーにより、100％コピーの証拠用マスターHDDを作成し、法的措置における犯人の立証を可能にする。
【選択図】図６



【特許請求の範囲】
【請求項１】
　コンピュータネットワークに記録された情報の漏洩、該情報の改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為による損害に対して保険金を支払い、その損害を補填するとともに、不正行為者である犯人の特定及び法的措置という事後対応を行うフォレンジックを損害補填の内容とするフォレンジック事後対応付き情報損害保険システムであって、
　前記フォレンジックは、証拠保全工程、解析工程および報告工程を含み、該証拠保全工程では、前記不正行為に関与している可能性のあるコンピュータのデータの100％の複製を実施し、該解析工程ではその複製データの解析し、該報告工程では該解析工程の解析に基づき証拠を見つけ出し、最終的に採るべき法的措置を報告することを特徴とするフォレンジック事後対応付き情報損害保険システム。
【請求項２】
　前記証拠保全工程では、前記不正行為に関与している可能性のあるコンピュータのハードディスクドライブ（HDD）のデータのコピーを行い、
　前記コピーは、HDDのデータを一切書き換えることなくコピーが行えることを証明された証拠保全用コピー機で行い、
　前記コピーにより、証拠用マスターHDDを作成する
　ことを特徴とする請求項１に記載のフォレンジック事後対応付き情報損害保険システム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、コンピュータネットワークに記録された情報の漏洩、該情報の改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為による損害に対して保険金を支払う情報損害保険システムであって、該不正行為に対する事後処置として、フォレンジック（forensic）によるインシデントレスポンスを行うための費用を該損害に含めるフォレンジック事後対応付き情報漏洩損害保険システムに関する。
【背景技術】
【０００２】
　東京電機大学工学部教授佐々木良一氏は、フォレンジックに関する用語として、コンピュータ・フォレンジックとデジタル・フォレンジックとが用いられているとし、次のように解説している。『フォレンジックスあるいはフォレンジックというのは「法の」とか「法廷の」という意味を持つ言葉であり、コンピュータ・フォレンジックは「計算機科学などを利用して、デジタルの世界の証拠性（evidence）を確保し、法的問題の解決を図る手段。ログの改ざん、破壊など、これまでの手法では証拠を検出することが困難な被害を受けたコンピュータに対しても、高度なツールによってコンピュータ内のデータを調査・分析することにより、不正アクセスの追跡を行なう手段を含む」と定義されることが多いようです。コンピュータ・フォレンジックスによって得られた証拠情報は、（１）刑事訴訟に用いる場合、（２）民事訴訟に用いる場合、（３）踏み台にされた場合に自分がきちんと対応していたことの証明に用いられます。これに対し、コンピュータ内のデータだけでなく、ネットワーク上や、携帯電話、情報家電内などのデータも積極的に扱おうというのが、デジタル・フォレンジックです。扱う対象以外に2つの言葉の間に、大きな定義の差はないようで、コンピュータ・フォレンジックの対象の部分を変更すれば、そのまま、デジタル・フォレンジックの定義といってよいでしょう。』
【０００３】
　本願では、上記佐々木良一教授の解説を基に、「フォレンジック（forensic）」は、不正アクセスや情報漏洩といった犯罪行為や、商取引上のトラブルといった訴訟沙汰になり得るリスクに備えて、法廷で用いることができるような証拠を残すための取り組みを指すものとし、前記コンピュータ・フォレンジックと同義の語として用いることとする。

【０００４】
[個人情報保護法施行]
平成17年4月から施行された個人情報保護法により、個人情報取扱事業者の個人情報の取扱に対する責任はさらに明確になり、仮に情報漏洩した場合には、監督官庁から明確な指導を受けることになる。場合によっては業務停止命令が出される可能性も否定できない。個人情報を大量に取り扱っている多くの企業は、個人情報に関し適切に対策を講じておかなければならない。企業における個人情報の取り扱いの不備に起因して、個人情報の漏洩などの事故が起きれば、企業の存続そのものを危うくすると言っても過言ではない。
【０００５】
[情報漏洩事例と現在の情報セキュリティの問題点]
図１は、情報セキュリティトータルソリューションモデルとフォレンジックの位置づけを示す概念図である。現在の情報セキュリティは、その個人情報を漏洩させないようにするものであった（図1－10）。ここで、図1－10は、図における符号１０で示す処理・行為・プログラム等をいうものとし、以下同様とする。個人情報を漏洩させないようにするものは、たとえばファイアウォールであったり、侵入検知、漏洩検知システムであったり、あるいはアクセス制限を設けて、重要なデータには権限を持った人しか触れることができないようにすることであった。また、個人情報漏洩防止のために企業が行う別の方策は、社員に対し、セキュリティポリシーなるものを設定し、かつセキュリティ教育を徹底し、セキュリティの重要性をしっかり認識させ、社員一人一人の自覚を促すことであった。これらの情報漏洩防止対策で対処しようとする行為は、何らかの方法でシステムや企業の建物に侵入して情報を盗むという悪意の第三者の行為と、誤ってデータを放出してしまうという社員の行為である。
【０００６】
しかしながら、昨今発生している情報漏洩では、企業が個人情報にアクセスする権限を与えている人が情報を故意に漏洩したケースが非常に多い。アクセス権者による故意の漏洩の大きな理由としては、私利私欲や会社に対する遺恨がある。また、アクセス権者による故意の漏洩の別の原因として、私利私欲や遺恨が動機となり悪意の第三者を手引きするということもある。このようなアクセス権者による故意の漏洩に対しては、防御策はほとんどなく、仮に完全な防御策を設定するならば、社長から社員までのすべてが個人情報にアクセスできないようにするしかない。しかし、実際そのようなことは現時的に不可能である。しかも、昨今情報漏洩が発生した企業のなかに最先端のIT企業も含まれるという事実は、最先端のITセキュリティ技術を適用したコンピュータシステムであっても、情報漏洩が発生し得るということを示している。
【０００７】
以上に説明した事例から言えることは、コンピュータシステムからの情報漏洩を完全に防止することは不可能だということである。このことに気が付いたならば、視点を変えた処置が必要となる。その視点を変えた処置とは、インシデントレスポンスと呼ばれる事後対応対策である（図1－11）。
【０００８】
[情報セキュリティの現状]
コンピュータシステムに対する現在考え得る主な情報不正行為とは、プログラムやデータの破壊（図１－３）、プログラムやデータの不正改ざん（図１－４）、情報漏洩（図1－5）である。それらが行われる手段としては、インターネットからの不正アクセス（図1－6）、企業内部にある端末PCからの書き換え（図１－７）、インターネット経由によるデータの持ち出し（図１－８）、USBメモリやコンパクトフラッシュ（コンパクトフラッシュは登録商標）などの携帯記憶装置の人間による持ち出し（図１－９）が挙げられる。さらにそれに対するセキュリティ対策としては、図１－10に示すようにファイアウォール、アンチウィルスソフト、侵入・漏洩検知装置や暗号などの防止・阻止対策と、図1－11のような事後対応に主眼を置いた法的措置のための対策がある。現状では、わが国の情報セキュリティとして取られている対策はほとんどすべてが図1－10に示す防止・阻止の対

策であるといっていい。しかしながら、防止・阻止対策（図1－10）だけでは、基本的には、組織外部からの不正行為（図１－3）にしか対応していない。現在問題になっている、情報漏洩や情報改ざんなどの不正行為はほとんど組織内部の人間により行われている（図1－4，5）。結果的に、企業内の端末PCから行われる不正（図1－7，8）や持ち出し（図1－9）などの不正行為に対しては何の対策もできていないのが現状である。現在発生している情報漏洩事件のほとんどが内部の人間によるものであることを考えると、防止・阻止のための高度の対策を講じたとしても、ほとんど防ぐことができないということは、現実の不正行為報道が示している。このように、情報漏洩事件は必ず発生するといっても過言ではない。そこで、情報漏洩等の不正行為が発生した後に、早急に対応し法的措置を行う能力（図1－11）が不可欠になってきた。

【０００９】

[個人情報漏洩に対する従来の対策]

図２は、従来の情報セキュリティ体制を示す概念図である。従来の情報漏洩対策は、準備として法制度や企業規則、罰則規定などを設け、守るべきは何か、脅威は何かなどのセキュリティポリシーを決定する（図２－１）。その後セキュリティポリシーにしたがって防止・阻止の対策を講じる（図２－２）。そして、監査やログ分析等により異常を検知する（図２－３）。事後対応はシステムを復旧し、業務を速やかに再開させるようにする（図２－４）。これが情報漏洩に対する従来の対応の一連の流れである。このように、防止・阻止対策によって漏洩を起こさないようにすることに専念しているのが、従来の情報セキュリティ体制である。

【００１０】

利用者のネットワーク上におけるデータの窃盗、改ざんおよび破壊を含む不正行為を保険の目的とする損害保険に関する従来の技術には次のようのものがあった。特許文献１（特開２００３－３４５９８９）には、不特定多数の者が利用する通信ネットワークに接続された、利用者のネットワークへの不正侵入により当該ネットワーク上におけるデータの窃盗、改ざんおよび破壊を含む不正行為があった場合に、当該不正行為に起因する損害を保証するネットワーク損害保険システムであって、前記利用者の識別情報および当該利用者のネットワーク上におけるデータの保険料が登録されたデータベースと、前記不正行為されたデータを示す情報とともに前記不正行為された利用者の識別情報を受付ける不正行為受付手段と、前記データベースを参照して前記不正行為されたデータの保険料を特定し、当該保険料に基づいて前記利用者に支払うべき保険額を決定する保険額決定手段と、を備えるように構成したネットワーク損害保険システムが開示されている。

【００１１】

特許文献２（特開２００３－２８１３６７）には、情報機器使用に伴う関連情報の漏洩等に基づく保険契約システムが開示されている。この保険契約システムは、セキュリティソフトウェア購入に併せて機密情報若しくは情報機器の使用に伴う関連情報の漏洩等に基づく保険契約を迅速に成約させて、保険契約の成約率の向上及びセキュリティソフトウェアの販売促進を図ることを目的とする。この保険契約システムでは、インターネット接続業者であるプロバイダーのＷｅｂサーバ（１）には、このプロバイダーに加入する一般の保険契約企業の端末（２）が接続されている。また、インターネット回線（３）には、プロバイダーのＷｅｂサーバ（１）の他、保険会社のＷｅｂサーバ（４）や、セキュリティソフトウェアやＦＤ、ＣＤ－ＲＯＭ等電子媒体の販売企業や代理店のＷｅｂサーバ（５）が接続されている。

【００１２】

特許文献３（特開２０００－２０７４５３）には、各種の商品・サービスの提供者と利用者との間の商取引を、電子的ネットワークを利用して行う電子商取引システムにおいて、商品・サービスの提供者（１０）または利用者（２０）と保険会社（３０）との間、もしくはこれらの三者間、あるいは必要に応じてその他の関係者（４０）を交えた形でプライバシー保護のための保険契約を締結し、商取引に伴って商品・サービスの提供者（１０）または利用者（２０）、更には関係者（４０）のプライバシーが犯された時に、その損

害を賠償することを内容とする保険契約に関する技術が開示されている。この保険契約に関する技術により、インターネット等の電子的ネットワークを利用した電子商取引において、取引の当事者の個人情報の漏洩、盗用、改ざん、不正な売買等によるプライバシーの侵害が防止され、取引の安全性が高められるとしている。

【００１３】

図２のような対策を徹底して実施してきたにもかかわらず、情報漏洩事件の報道は後を絶たない。多大の顧客に対して多額の損害賠償金を企業側は支払った事例がいくつかある。図３は、情報漏洩を完全に防ぐことは不可能という観点から、情報漏洩の被害を受けたときには、情報漏洩による損害賠償金を保険金で補填しようとするときに採用するセキュリティ体制を示す概念図である。

【００１４】

個人情報保護法では、情報漏洩を起こした企業に対する罰則規定は設けられていないが、個人情報取扱事業者には個人情報保護の義務が課せられているので、監督官庁は情報漏洩企業に対して何らかの指導を行わなければならない立場にある。情報漏洩の態様によっては、改善策の策定までは該情報漏洩企業に対し業務停止が要求されるケースも考えられる。個人情報保護法の施行により個人情報取扱事業者の負う責務が格段に増大したにも拘らず、同法施行後も従来のセキュリティ体制（図３－６）に損害保険（図３－７）を加えただけの体制で個人情報保護法施行を迎えなければならないという結果になった。

【００１５】

【特許文献１】特開２００３－３４５９８９

【特許文献２】特開２００３－２８１３６７

【特許文献３】特開２０００－２０７４５３

【発明の開示】

【発明が解決しようとする課題】

【００１６】

従来の情報セキュリティ体制における情報漏洩対策は、図２に概念図で示したように、法制度や企業規則、罰則規定などを設け、守るべきは何か、脅威は何かなどのセキュリティポリシーを準備段階で決定し（図２－１）、次にセキュリティポリシーにしたがって防止・阻止の対策を講じ（図２－２）、そして、監査やログ分析等により異常を検知し（図２－３）、システムを復旧し、業務を速やかに再開させるようにする事後対応の措置（図２－４）を行うことであった。このように、防止・阻止対策によって漏洩を起こさないようにすることに専念しているのが、従来の情報セキュリティ体制であったことは既に述べた。

【００１７】

特許文献１乃至３に挙げた従来の損害保険では、情報の漏洩、該情報の改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為の発生という情報事故が起きたときに、その損害を保険金でもって単に補填するだけであった。このような損害の補填だけでは、被保険者である個人情報取扱事業者の満足は得られない。従来のセキュリティ体制では、基本的には情報漏洩をすべて防止できるわけではないことは分かってきたので、情報漏洩はするものであるという前提に基づいた事後対応策が必要になってきた。また、情報漏洩後の企業側の対応では、損害賠償金的な対応だけでは、十分な顧客満足が得られない。顧客（被保険者である個人情報取扱事業者）は、早急な犯人特定と法的措置ができる体制を求めることが経験上明らかになった。早急な犯人特定および法的措置は、悪意の情報漏洩などの不利益行為の再発を抑制し、セキュリティに対する信頼性を向上する。個人情報保護法施行により、個人情報の保護に関し同法の施行前より一層重大な責務を負った各組織は、情報漏洩等の事故の発生後の犯人特定と法的措置、即ち事後対応、が早急にとれる体制を構築しなければならない。情報漏洩等の事故の発生後の犯人特定と法的措置、即ち事後対応、が早急にとれる体制とは、フォレンジックの体制である。

【００１８】

そこで、本願の目的は、コンピュータネットワークに記録された情報の漏洩、該情報の

改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為による損害に対して保険金を支払う情報損害保険システムであって、その損害を補填するだけではなく、情報事故を起こした犯人の特定及び法的措置という事後対応を行うフォレンジックを損害補填の内容とするフォレンジック事後対応付き情報損害保険システムの提供にある。

【課題を解決するための手段】

【００１９】

前述の課題を解決するために、本発明は次の手段を提供する。

【００２０】

（１）コンピュータネットワークに記録された情報の漏洩、該情報の改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為による損害に対して保険金を支払い、その損害を補填するとともに、不正行為者である犯人の特定及び法的措置という事後対応を行うフォレンジックを損害補填の内容とするフォレンジック事後対応付き情報損害保険システムであって、

前記フォレンジックは、証拠保全工程、解析工程および報告工程を含み、該証拠保全工程では、前記不正行為に関与している可能性のあるコンピュータのデータの100％の複製を実施し、該解析工程ではその複製データの解析し、該報告工程では該解析工程の解析に基づき証拠を見つけ出し、最終的に採るべき法的措置を報告することを特徴とするフォレンジック事後対応付き情報損害保険システム。

【００２１】

（２）前記証拠保全工程では、前記不正行為に関与している可能性のあるコンピュータのハードディスクドライブ（HDD）のデータのコピーを行い、

前記コピーは、HDDのデータを一切書き換えることなくコピーが行えることを証明された証拠保全用コピー機で行い、

前記コピーにより、証拠用マスターHDDを作成する

ことを特徴とする請求項１に記載のフォレンジック事後対応付き情報損害保険システム。

【発明の効果】

【００２２】

前記の本発明の構成によれば、コンピュータネットワークに記録された情報の漏洩、該情報の改ざん、該情報への不正なアクセス、その他の該情報に関する不正行為による損害に対して保険金を支払う情報損害保険システムであって、その損害を補填するだけではなく、情報事故を起こした犯人の特定及び法的措置という事後対応を行うフォレンジックを損害補填の内容とするフォレンジック事後対応付き情報損害保険システムを提供できる。

【発明を実施するための最良の形態】

【００２３】

以下、図４乃至図１０を参照して、本発明のフォレンジック事後対応付き情報損害保険システムの実施の形態を説明する。

【００２４】

[フォレンジックと事後対応]

フォレンジックは、前述のとおり、不正アクセスや情報漏洩といった犯罪行為や、商取引上のトラブルといった訴訟沙汰になり得るリスクに備えて、法廷で用いることができるような証拠を残すための取り組みを指す。例えば、情報漏洩事件に関するフォレンジックは、情報漏洩に関係する端末PCのデータを調査して、情報漏洩に関する事実と犯人を特定する法的証拠を見つけ出す一連の取り組み、即ち行為である。図４は、フォレンジックの流れを示す概念図である。まず証拠保全工程で、情報漏洩に関与している可能性のあるコンピュータのデータを100％の複製を実施して証拠保全し、次の解析工程でそのデータの解析を行う。最後の報告工程では、解析工程の解析に基づき証拠を見つけ出し、最終的に採るべき法的措置を報告する（図4）。フォレンジックにおいて最も留意すべき点は、調査対象コンピュータのデータを一切（1ビットも）書き換えることなく、保全、解析、報告を行うとともに、どの工程においても書き換えがなかったことを証明することである。

フォレンジックでは、そのことに主眼をおいた技術やツールを使用する。書き換えがなかったことを証明するために、証拠保全工程では、情報漏洩の不正行為に関与している可能性のあるコンピュータのハードディスクドライブ（HDD）のデータのコピーを行い、そのコピーは、HDDのデータを一切書き換えることなくコピーが行えることを証明された証拠保全用コピー機で行い（図４－１）、該コピーにより、100％コピーの証拠用マスターHDDを作成する。

【００２５】

図５は、図４における解析工程および報告工程で行う行為の具体例を示す図である。個人情報漏洩事故が発生した場合、情報漏洩したファイルを保全したデータの中から探し出す（図5－１）。そして、情報漏洩手段がEメールであったか？（図5－２－１）又は外部接続機器であったか？（図5－2－2）を調査する。次に、その調査に基づき、誰が行ったかを特定する（図5－３）。図5－３の場合は、ログイン情報を解析して、情報漏洩者を特定している。その調査により得たデータおよび特定した情報漏洩者を報告書で報告し（図5－4）、法的措置も執る。

【００２６】

[フォレンジックの導入]

現状のセキュリティ体制では、基本的には情報漏洩をすべて防止できるわけではないことは分かってきたので、情報漏洩はするものであるという前提に基づいた事後対応策が必要になってきた。また、情報漏洩後の企業側の対応では、損害賠償金的な対応だけでは、十分な顧客満足が得られない。顧客は、早急な犯人の特定と法的措置ができる体制を求めることが経験上明らかになった。早急な犯人の特定および法的措置は、悪意の情報漏洩などの不利益行為の再発を抑制し、セキュリティに対する信頼性を向上する。個人情報保護法の施行により、個人情報の保護に関し同法の施行前より一層重大な責務を負った各組織は、情報漏洩等の情報事故の発生後の犯人特定と法的措置、即ち事後対応、が早急にとれる体制を構築しなければならない。図６は、図３の従来の情報セキュリティ体制に、新たな事後対応措置を加えた情報セキュリティ体制を示す概念図である。図３に示した従来の情報セキュリティ体制における事後対応は復旧や損害保険金の取得だけであった（図３－４、図6－４）。これに対し、図６の新たな情報セキュリティ体制では、フォレンジックによる法的措置（図6－11）が加えられている。法的措置は、証拠保全、解析および証拠提出を内容とするものである。

【００２７】

[保険ビジネスとフォレンジックのコラボレーション]

情報漏洩に対する損害保険は既に存在している（図４－７）が、従来の損害保険による保障は、保険金と情報漏洩予防のコンサルテーションにとどまっている。コンサルテーションでは、少しでも情報漏洩が起こらないようにする予防措置等についての指導を行う。従来の損害保険では、実際に情報漏洩が発生した場合には、記者会見や顧客の対応などの渉外活動以外の実質上のインシデントレスポンスは対応できていない。損害保険に関しても、従来の体制では、情報漏洩発生後の調査体制が確立しておらず、犯人特定や被害状況などが予測できないため、支払うべき保険金の上限は低く、実質気休め程度の保険にしかならない。

【００２８】

そこで、本発明のフォレンジック事後対応付き情報損害保険システムでは、具体的にインシデントレスポンスにより早急に犯人特定と法的措置を行う手段であるフォレンジックを保険の対象（損害保険商品）としている。損害保険の対象としてフォレンジックを導入する価値は非常に高い。その理由を以下にあげる。

（１）フォレンジック対応は高額な費用がかかる。保険金としてプールしておけば、フォレンジック対応時は、その保険金でまかなうことが可能となる。

（２）情報漏洩発生時に対応体制が確立されていることによって、損害額が予測可能となり、必要な保険金の算定が可能となる。また、フォレンジック体制を確立している企業はより安価な保険料の支払いで高額な保障が得られる保険に加入できる。

（３）保険会社が被保険者（顧客）に情報漏洩後のソリューションを与えることができる。
（４）被保険者は損害額の補償（保険金）や防止のコンサルテーションに加え、事後対応に特化したソリューションがまとめて保険会社から得ることができる。
（５）情報事故発生後の事を対応している業界は損害保険のみであり、事後対応を主目的としているフォレンジック事業との対象の領域が類似しているため、コラボレーションが組みやすい。
（６）従来の情報漏洩保険では、お金による補填しかできなかったが、フォレンジックを保険の対象として導入することにより、具体的な技術手法による補填が可能となる。すなわち情報漏洩保険の目的に、金銭的損害だけでなく、フォレンジックという具体的なサービスを加えた新たな損害保険が誕生することになる。
（７）情報漏洩後に早急な犯人特定・法的措置を執ることができる体制は、被保険者の顧客に満足を与えることができ、顧客に対する情報漏洩後の損害賠償金の低減を可能にする。
（８）被保険者（企業）側で、情報漏洩後に早急に犯人特定・法的措置がとれると、顧客の批判の目が企業側から犯人へと移行し、企業のイメージダウンを回避できる。損害保険の本来の目的であるリスクヘッジ機能を一層向上できる（図7）

【００２９】

上述のように、フォレンジックを保険の対象に含める本発明のフォレンジック事後対応付き情報損害保険システムは被保険者の企業（個人情報取扱事業者）および損害保険会社の双方に有利なシステムであり、かつ新規性があるビジネスモデルである。特に、本損害保険への加入により、情報漏洩発生後に直ちに技術的な事後対応が可能となるので、被保険者にとっては、リスクのコントロールが可能となるというところが本損害保険システムの重要なポイントである。

【００３０】

[フォレンジックを含めた情報漏洩損害保険のモデル]

（１）情報漏洩損害保険の対象

本実施の形態のフォレンジック事後対応付き情報損害保険システムにおいける保険対象は、コンサルティングとインシデントレスポンスとに分けられる。図８は、そのコンサルティングの概要を示す図である。コンサルティングで行う主な項目は、事後対応に適した体制を構築するための環境設定とインシデントレスポンスチームの編成である（図８）。事後対応環境の設定では、セキュリティポリシーの設定、コンピュータの設定、コンピュータネットワークの設定などを行う。これらの設定により、事後対応がスムーズにできる体制を構築する。インシデントレスポンスチームの編成は、インシデントレスポンスチームのトレーニング及びツールの導入が主な内容である。インシデントレスポンスは、損害賠償金に対する保険金による補填と専門弁護士等による記者会見等の従来の損害保険おいて既に行われている対応に加えて、実際にコンピュータを調査して早期解決にあたるフォレンジックのサービスを加える。図９は、そのインシデントレスポンスを例示する概念図である。

【００３１】

（２）本発明の実施の形態における契約から対応までの流れ

損害保険契約をしようとする顧客は、図８に示したコンサルティングとインシデントレスポンスとのうちの双方又は一方を選択し、損害保険会社と契約する。図１０は、本実施の形態のフォレンジック事後対応付き情報損害保険システムにおいて顧客が選択できる保険対象の３つの例Case1乃至Case3を示す概念図である。

【００３２】

Case1（図10－5）では、フォレンジックの導入・運用において、フォレンジック調査環境の設定（図10－8）及びフォレンジックチームの設立（図10－9）を選択している。そして、実際のセキュリティインシデント発生の際には、自社（損害保険の被保険者）のフォレンジックチームが対応する。このCase1の特徴は、初期導入費用は非常に高くなるが、

いざインシデントレスポンスをする際には、自社で対応可能であり、しかもフォレンジックするのに適した環境設定をあらかじめ行っているので、非常に早期に解決することができる。結果的に、顧客に支払う損害賠償等を含めてインシデントレスポンス費用を低く抑えることができる。何よりも、インシデント（情報漏洩等の事件）発生から犯人特定までの処理が長期化して、企業イメージを低下させるというリスクを回避できる（図10－14）。

【００３３】

Case2（図10－6）では、フォレンジックチームは設立しないで、フォレンジックに適した環境のみを予め設定しておく（図10－10）。そして、インシデント発生時は、フォレンジック対応を他社（損害保険の被保険者以外の会社、フォレンジック専門企業など）に依頼する。この場合は、初期導入費用はCase1に比較して低くなるが、インシデントレスポンスを他社に依頼する（図10－11）ので、その分だけインシデント発生後の費用は高くなる。ただし、予め、フォレンジックがするのに適した環境に設定してあるので、インシデントレスポンスがインシデント発生後直ちに適切に開始され、下記Case3に比べ、インシデントレスポンスが早期に終了し、犯人の特定にまで至る可能性が高くなる（図10－15）。

【００３４】

Case3（図10－7）では、準備段階ではなにもしない。さらにインシデント発生後も他社に依頼することになる。この場合、初期導入費用はほとんど発生ないので、初期コストは低くなるが、インシデント発生後は膨大な時間と経費がかかるので、調査費用や損害賠償金は多額となり、その上に企業イメージ低下の可能性が高い。

【００３５】

本実施の形態のフォレンジック事後対応付き情報損害保険システムでは、各ケースにおいて、発生する事後対応の費用に関しては、初期導入時の費用に比例して割引率を設定しておく。たとえば、Case1（図10－5）の場合は、事後対応が容易な環境を実現し、他社が対応する必要はほとんどないので、仮に他社が行うフォレンジック費用に関しての割引率は非常に高いものとなる。逆にCase3（図10－７）のように、事前に準備を怠っていると、事後対応も非常に困難になるため、実際の作業時の割引率は低くなる。早期解決ができる場合は、個人情報取扱事業者である被保険者がその顧客に対し支払う謝罪金の額も、低廉に抑えることができるか、又は謝罪金そのものの支払いを要しないように、顧客の悪感情を緩和できる場合もあり得る。そのことは、損害保険会社にとっても、被保険者の企業にとってもおおきなメリットとなり得る。

【００３６】

[結論]

以上に詳しく述べたようにところから明らかなように、インシデント発生後の対応を視野に入れているフォレンジック企業と損害保険会社の協業は、個人情報保護法が施行された今、社会の必要に対応するものである。いくらかのコストをかけて、インシデント発生後の対応に備え、実際に発生した際には、既定の手法で対応し、リスクヘッジを行うフォレンジックを対象とする損害保険は、まさにお金ではない、技術による保険であるといえる。これまで、情報漏洩発生後は対処するための明確な手段がなかったが、フォレンジックの導入によって、早期解決、被害極小ができるので、リスクマネージメントができることになるということが、本実施の形態の非常に重要なポイントであるといえる。また、本発明の損害保険システムは、個人情報漏洩だけでなく、あらゆる情報漏洩や、その他の企業内情報に関する不正行為にも対応可能である。

【図面の簡単な説明】

【００３７】

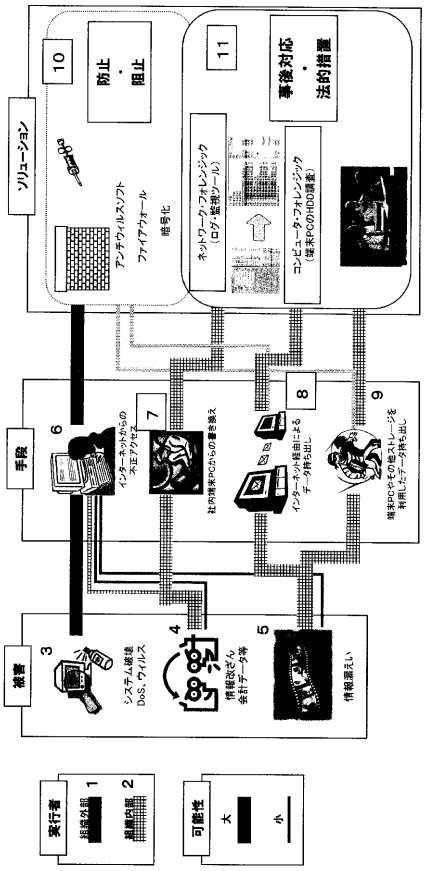
【図１】情報セキュリティトータルソリューションモデルとフォレンジックの位置づけを示す概念図である。

【図２】従来の情報セキュリティ体制を示す概念図である。

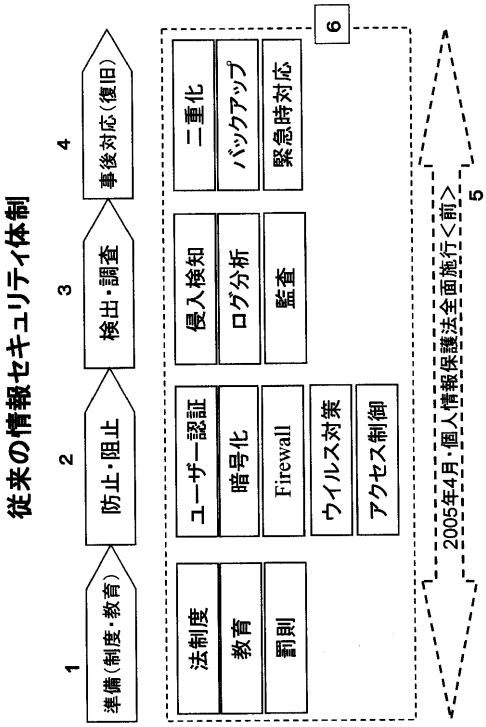
【図３】情報漏洩を完全に防ぐことは不可能という観点から、情報漏洩の被害を受けたと

きには、情報漏洩による損害賠償金を保険金で補填しようとするときに採用するセキュリティ体制を示す概念図である。
【図４】フォレンジックの流れを示す概念図である。
【図５】図４における解析工程および報告工程で行う行為の具体例を示す図である。
【図６】図３の従来の情報セキュリティ体制に、新たな事後対応措置を加えた情報セキュリティ体制を示す概念図である。
【図７】被保険者（企業）側で、情報漏洩後に早急に犯人特定・法的措置がとれると、顧客の批判の目が企業側から犯人へと移行し、企業のイメージダウンを回避でき、損害保険の本来の目的であるリスクヘッジ機能を一層向上できることを示す概念図である。
【図８】本発明の実施の形態においけるコンサルティングの概要を示す図である。
【図９】本発明の実施の形態においけインシデントレスポンスを例示する概念図である。
【図１０】本発明の実施の形態のフォレンジック事後対応付き情報損害保険システムにおいて顧客が選択できる保険対象の３つの例Case1乃至Case3を示す概念図である。

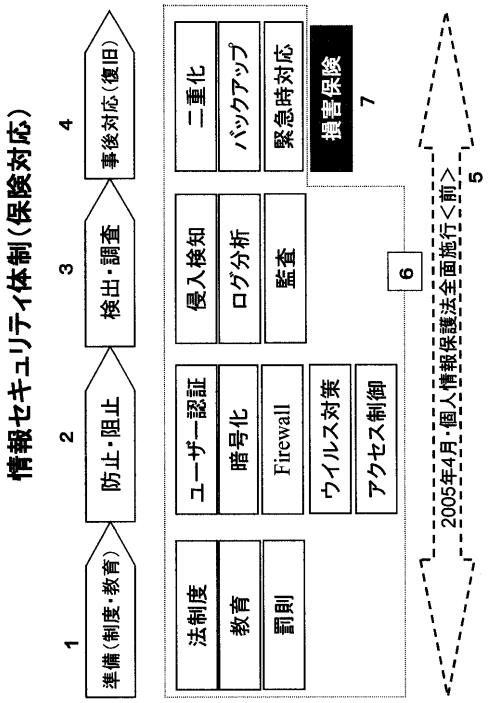
【図１】



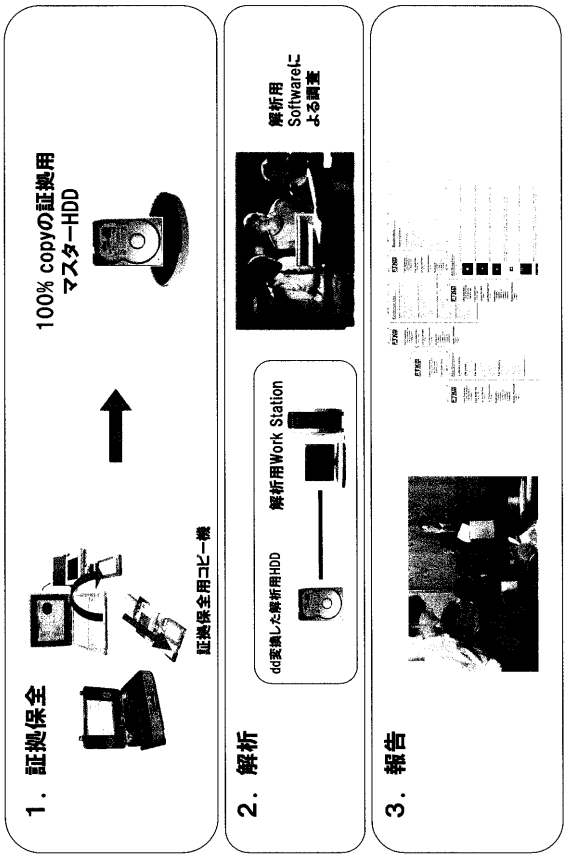
【図２】



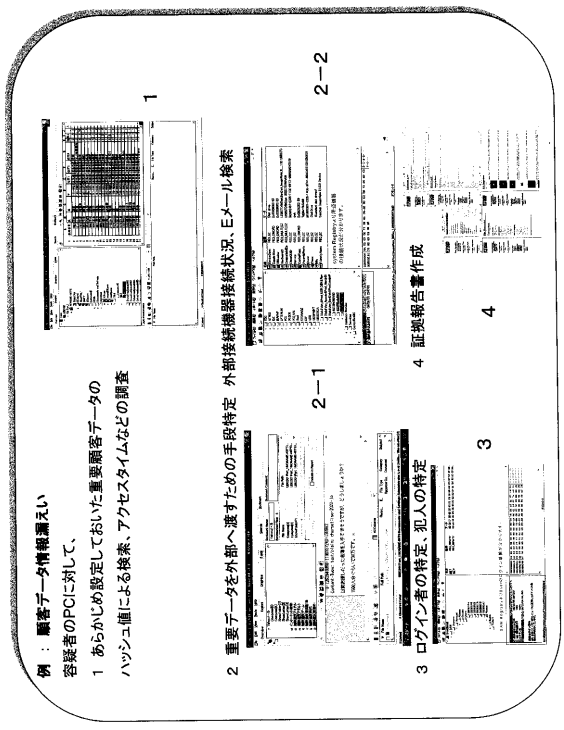
【図３】


情報セキュリティ体制（保険対応）
1
準備（制度・教育）
2
防止・阻止
3
検出・調査
4
事後対応（復旧）
法制度
教育
罰則
ユーザー認証
暗号化
Firewall
ウイルス対策
アクセス制御
侵入検知
ログ分析
監査
二重化
バックアップ
緊急時対応
損害保険
7
6
2005年4月・個人情報保護法全面施行＜前＞
5

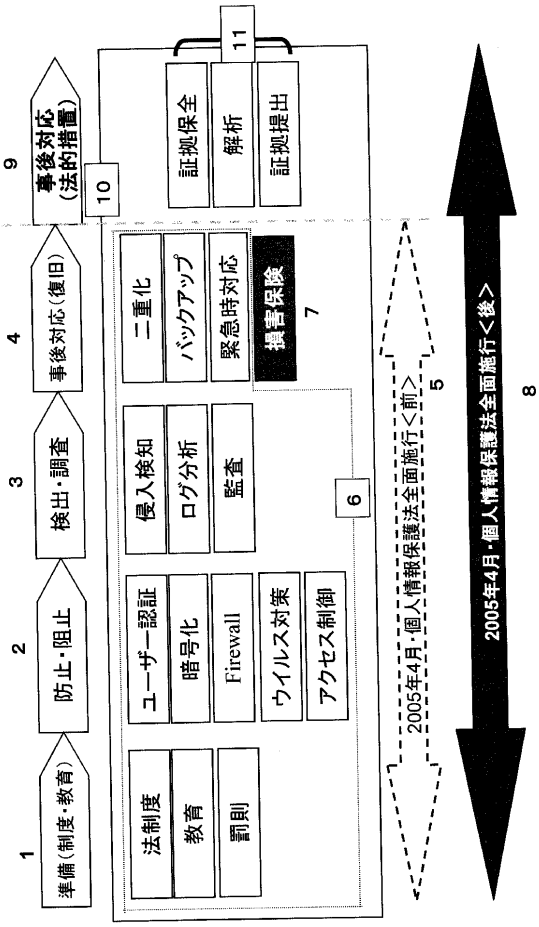
【図４】


1．証拠保全
100% copyの証拠用
マスターHDD
証拠保全用コピー機
2．解析
dd変換した解析用HDD
解析用Work Station
解析用
Softwareによる調査
3．報告

【図５】


例：顧客データ情報漏えい
容疑者のPCに対して、
1 あらかじめ設定しておいた重要顧客データの
ハッシュ値による検索、アクセスタイムなどの調査
1
2 重要データを外部へ渡すための手段特定 外部接続機器接続状況、Eメール検索
2−1
2−2
3 ログイン者の特定、犯人の特定
3
4 証拠報告書作成
4

【図６】

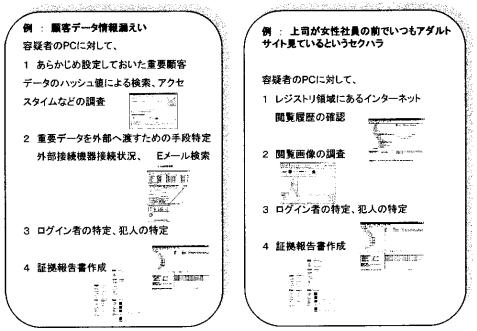

1
準備（制度・教育）
2
防止・阻止
3
検出・調査
4
事後対応（復旧）
9
事後対応
（法的措置）
10
法制度
教育
罰則
ユーザー認証
暗号化
Firewall
ウイルス対策
アクセス制御
侵入検知
ログ分析
監査
二重化
バックアップ
緊急時対応
損害保険
7
6
証拠保全
解析
証拠提出
11
2005年4月・個人情報保護法全面施行＜前＞
5
2005年4月・個人情報保護法全面施行＜後＞
8

【図９】

インシデントレスポンス

コンピュータインシデントが発生した際の様々な対応を技術的・人的・金銭的な面からサポート。コンピュータ・インシデントが発生した際の取るべきいくつかの対応を適切に行い、問題を迅速に解決し被害を極小する。

➢ ***フォレンジックによるインシデントレスポンス***



対象HDDからの物理複製（クローニング）

解析PCで容疑HDDデータを調査

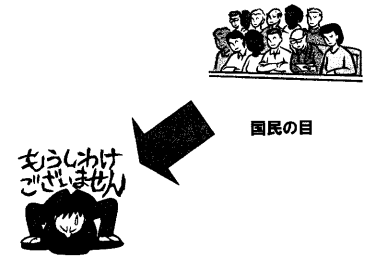
➢ ***損害賠償に対する保険金による補填***

➢ ***専門弁護士による会見・訴訟対応***

【図７】

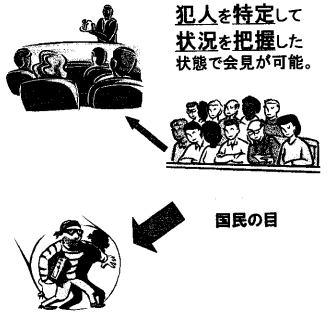
■ 企業で情報漏えい等の不祥事が発生した場合、早期に犯人を特定した場合と特定できなかった場合とでは、企業におけるダメージは大きく異なる。

早期に特定できなかった場合



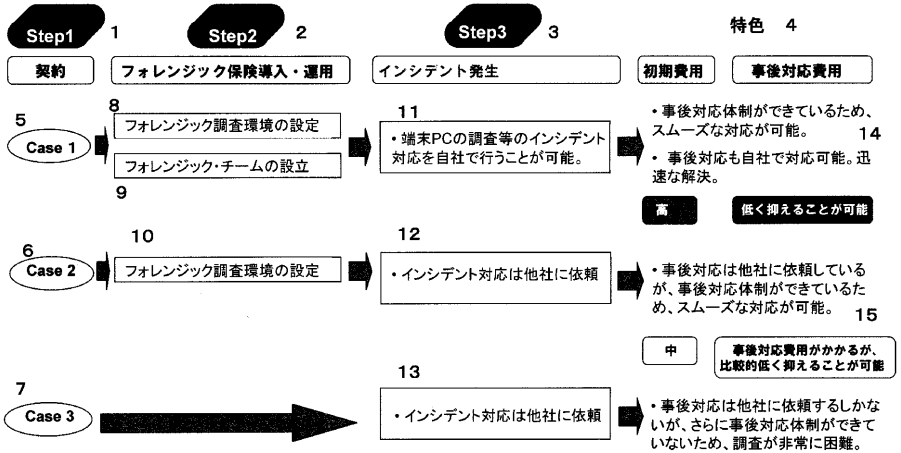
企業のセキュリティ担当者

早期に特定できた場合



不正行為者

【図１０】



【図８】

フォレンジックセキュリティ体制確立支援

フォレンジックが可能な環境・人員等の整備により、事前監査ならびにコンピュータ・インシデントが発生した際に、迅速に解決し被害を極小する。または事象の発生そのものを抑止する効果をもつ。

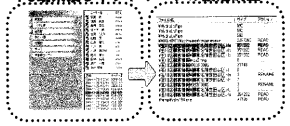
➢ ***コンサルティング***

・セキュリティポリシーの設定

・アクセスコントロールポリシー
・PC取扱い規定
消去ソフト使用禁止
HDDパスワード禁止
・私物のPCを持ち込まない。
・PC調査規定
退職時、異動、
アクセス権限保持者
不正行為発生、兆候
・重要データの指定

・調査時にフォレンジックを容易にするためのルール作成がポイント
・セキュリティポリシー違反に対する罰則規定

・PC端末及びネットワークの設定照準

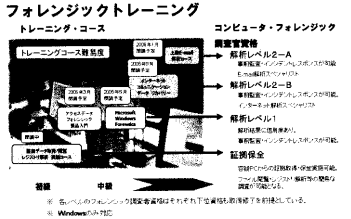


検知・ログ保存ツールの導入等

➢ ***フォレンジックチームの編成***

・ツールの導入

・フォレンジックトレーニング



※ 各レベルのフォレンジック調査官資格はそれぞれ下位資格も取得終了を前提としている。
※ Windows向け対応

JP 2007-148731 A 2007.6.14