対策型監査の効果と重要性

木村　修二　深瀬 知寛　（情報システム監査株式会社）

Shuuji kimura　Tomohiro Fukase
(Information Systems Audit corp.)

キーワード: 新しいタイプの攻撃　出口対策　記憶による情報漏えい
対策型監査　認証の回避

概要

従来型の情報セキュリティ対策は「脅威を中に入れない（境界防護）」の入口対策が中心であった。しかし正当権限者の不正行為も新しいタイプの攻撃である「標的型攻撃」も入口対策をすり抜ける。

対応策として「出口対策の実施」「情報セキュリティ設計」が極めて重要となる。これを踏まえ監査も変わるべきと考える。「対策型監査」として某中央省庁で適用した事例をふまえ報告する。

１．はじめに

「最低限、情報漏えいの事故だけは防止したい」というのが監査依頼者の要望であった。監査依頼者にすれば事故を防止するために監査を依頼するのであり、監査が事故の防止に直接に役立たねば「無意味」と考えた。このため事故防止に直結する監査の在り方を考えることとした。（以下、特に断りのない限り「事故」は「情報漏えいの事故」に限定して使用する[1]。）

準拠性監査では主に規程類の遵守の状況を調査し評価するが、「規程類が完全に遵守されれば事故は起きないのか？ 」という基本的な疑義がある。たしかに情報セキュリティ対策は自己責任が原則で、規程類自体は監査対象組織側の問題であるが、監査人は規程類自体の改正も改善策として提案しなければならない。

監査依頼者の求める「最低限、情報漏えいの事故だけは防止したい。」に応えるためには、監査も変わらねばならない。今回の事例では「対策型監査」と呼称した監査を某中央省庁で実施した。これを踏まえ、以下、監査対象組織として地方自治体を想定しながら、事故防止のための助言型監査の在り方を考える。

２．情報セキュリティ事故と監査

２．１　情報セキュリティ事故

情報セキュリティ事故は、内部からであっても外部からであっても、①攻撃者（予備群）が存在し、②攻撃を企て、③攻撃が可能な環境であった、この３つの条件が整ったときに発生する[2]。「攻撃者予備群」は、国内を含む世界のどこかに存在し、組織内部では市長等を含む経営層、上級職員、一般のシステム利用者、システム管理者、常駐ＳＥ、委託事業者社員、警備員、清掃員等すべてである。組織への不満や上司への不満、金銭上の欲求や政治思想から等「攻撃者予備群」の中の一部が「攻撃を企て」る。組織内部の者へは研修や服務規律・罰則をもって攻撃をしようと考えないようにする努力がはらわれているが、確信犯や外部の者には効果はない。「攻撃が可能な環境であった」という要素だけがコントロール可能な要素であり、攻撃が不可能な状態さえ構築できれば事故は発生しないことになる。さらに攻撃による被害の発生という視点から「最低限、情報漏えいの事故」に限定するならば、情報漏えいを防止するための環境を構築することになる。コントロールのうちには脅威を受容することも含まれ、正当な理由により、具体的な脅威を受容するという意思決定を行うこともありうる。

したがって、監査依頼者の求めている「最低限、情報漏えいの事故だけは防止したい」に応える監査の課題は、①攻撃（情報漏えいの事故に直結する不正行為）が可能な環境か否かを調査し、②事故発生に直結する脅威を示し、攻撃の容易さを評価[3]し、③事故防止に直結する具体的な改善策の実施と脅威の受容の意志決定とを行うための資料、提言を提出すること、である。

２．２　事故の態様

電子情報漏えい事故に至る行為を①情報の入手段階と②情報持出し段階の２段階に分解すると非常に単純化することができる。

図表１　事故発生の可能性のある箇所（サーバ空間を除く）

		機器類	ネットワークを経由		外部媒体を経由	
		管理された機器類	管理されたネットワーク	私設のネットワーク	管理されたもの	私物の機器類・外部媒体
参考例		配布されたＰＣ等	庁内ＬＡＮ	スマホでネットワークを私設	貸与ＵＳＢ 許可されたＵＳＢ等	私物ＰＣ等 私物ＵＳＢ等
情報の入手経路	正当な権限行使による情報入手	業務の遂行（注１）	業務の遂行（注１）	該当なし	業務の遂行（注１）	該当なし
	不正な権限による情報入手	認証回避 なりすまし 削除ファイルの復元 侵入	盗聴	該当なし	認証回避 なりすまし 削除ファイルの復元	該当なし

情報持出し経路	正当な権限行使による情報の持ち出し	業務の遂行（注２）	業務の遂行（注２）	該当なし	業務の遂行（注２）	該当なし
	不正な権限による情報の持ち出し	盗難	偽装（画像に混入等） 暗号化等	制限なし	偽装（画像に混入等） 暗号化等	制限なし

注１）不正行為である可能性は存在する

注２）正当な持ち出しののち、不正行為に転換の可能性は存在する

図表１のように分類し、情報の入手経路を中心とした入口対策型・アクセス制御型対策と、情報の持ち出し経路を中心とした出口対策型を分離した。情報の入手経路対策では業務の遂行と不正行為を識別することができない。正当権限者の場合は、不正か否かは動作・行為の差ではなく、意図の差にすぎない。(「３．認証の課題」を参照)。情報の入手経路での対策（アクセス制御）の主要な手法は、暗号化という情報そのものへのアクセス制御、または「情報が記録された入れ物」（パケット、ファイル、フォルダ、サーバ、ＵＳＢメモリ等）へのアクセス制御であったが、内部からの正当権限者による情報漏えいの可能性という視点からは、正当権限者は業務として正当に入手しているのであるから遮断できない。また高度なウイルスには無力である。さらに正当権限者が正当に情報を入手し、正当に持出し、しかし持ち出した後に心変わりして、不正に利用するということもある。たとえ不正に情報を入手されたとしても、最低限、漏えいしなければいいという視点からは情報持ち出し経路の対策を重視することになる。にもかかわらず現状ではアクセス制御型がセキュリティ対策の主流である。インターネット等外部から侵入されることが主要な脅威であり、内部犯行は「ありえない」こと、との認識だったのであろうか。正規職員の比率が劇的に低下し（終身雇用ではない）非正規の従業員が増加しているので、もはや職員の忠誠心に依拠できなくなっていると考える。

２．３　記憶による情報漏えい

電子情報の情報漏えい対策であるならば出口での対策で対応が可能である。しかし人間の記憶（脳という外部記録媒体への保存）への対策は環境的（物理的）対策や技術的対策は不可能であり、次善の策として人的対策（強力な抑止策）を実施することになる。アクセスログを確実に保持し、さらには内部で検知するために、ログから各個人の作業日報[4]を作成し本人の確認の上、提出させる等の強力な抑止策である全件チェックで補完するしかない。これも含めて出口対策と位置付ける。

またローカルの管理権限を有するID/パスワードは、規模が大きくなるほどに更新を行いにくくなるが、これを職務上知りえた者の人事異動などで一斉更新を行うべき事象は多い。「３　認証の課題」で後述するが、防ぎえない認証の回避という課題もあることから、今

後はローカルアドミンの権限を解放しても支障のないセキュリティ対策に移行すべきと考える。

２．４　出口対策

今現在の技術では、意図を検知することは不可能なので、情報の入手経路での対策（アクセス制御）は不可能となり、情報の持ち出し経路での対策（出口対策）を実施することになる。出口対策という用語自体が、不正持出し対策の総称として使用されることが多く、確立した概念でもないし、未だ確立した手法はない。境界防御の限界から出口対策の重要性が主張されることとなってきたが、内部の正当権限者の不正行為（不正な情報の持ち出し）については出口でしか防衛できないことは従前から指摘されてきたことである。

出口対策は内部からの情報の持ち出し経路を完全に管理された少数の経路とプロトコルに限定し、この経路に防止策と強力な抑止策を講じることが中心となる対策の体系と考える。

２．５　従来の準拠性監査

以上のように、出口対策が強く求められるが、監査の在り方にも影響する。準拠性監査の場合には「既決の規程類」と「受容した脅威の一覧」[5]が監査基準であると考える。ここであえて「受容した脅威の一覧」も加えたが、「既決の規程類」と「受容した脅威の一覧（想定外の脅威[6]を除く）」の和は「すべての脅威を表す」はずだと考えたからである。そして現実の運用を調査し、「既決の規程類」が遵守されていれば、事故の起こる可能性は「受容した脅威の一覧」に存在することになる。ところが、この関係が成り立たないとき、事故の起こる可能性は「受容した脅威の一覧」に存在するだけでなく、「既決の規程類」に存在するかもしれないし、全く認知されていないかもしれない。ここから「規程類が完全に遵守されれば、事故は起きないのか？ 」という基本的な疑義が生じることになる。

また情報セキュリティ基本方針の策定では想定する脅威を定義しセキュリティ対策の全体像の設計図を描き、リスク分析を実施し、対策基準の策定を行い、と同時に受容した脅威の一覧を作成し、様々なセキュリティ設定を行ったり、セキュリティソフトを導入したりといったセキュリティ対策の全過程で、現実的には脆弱性を抱え込み、目標値と実現値が乖離してゆくことになる。ここでも受容した脅威が発生する[7]。

２．６　対策型の準拠性監査

事故防止の視点からの評価では、評価基準は「キュリティ全体像（図）からの期待される機能」や「期待値」となる。「既決の規程類」に表現されている事柄もあるだろうし、欠落している事柄もある。事故防止に直結する監査を実施するためには、監査基準に次の事項を含めることとした。

① キュリティ全体像からの期待される機能や実装されているセキュリティシステムから期待されている機能を洗い出し、「期待値」を監査基準に含めること。（基準の拡大）

② 「期待値」含めて、受容した脅威を明確化、具体化すること。
脅威を受容するときの手続きを明文規定すること。

③ 「期待値」を実現するための手法を提案すること。（改善策の提案）

④ 新たな脅威を把握する手続きを明文規定すること。

そして事故防止に直結する具体的な改善策の実施と脅威の受容の意志決定を行うための資料を提案する、このような準拠性監査の拡大を考えた。これを「対策型監査」と呼称することとした。

簡易な対策型監査では「実施されているセキュリティ対策の有効性」（有効性の判断基準は、設計意図・期待値を推定することにより作成）を調査・評価し、事故防止に直結する具体的な改善策の実施と脅威の受容の意志決定を行うための資料を提案する。

実施されている技術的・環境的（物理的）セキュリティに含まれる脆弱性、実施されている人的セキュリティの脆弱性も人的セキュリティというもの自体の脆弱性、また組織的セキュリティに含まれる脆弱性についても、事故に直結する場合には指摘し改善策を提示することになる。

３．認証の課題

３．１　認証の種類

情報の入手経路対策の根幹をなす認証について検討する。認証には次の４つの種類があると考える。

図表２　認証の種類

認　証	説　　明	例　　示
個体認証	登録されている情報と物体（生の個体）との認証	情物一致 情報と物体とのひも付け
主体認証	操作者がDBに登録されているかの認証	ID/パスワード　2要素認証 DB上の「本人」であることの認証
意図認証	操作者の行為の意図の認証	正当な意図か不正な意図か 頭の中で考えていることの認証
利用目的認証	操作者の情報の利用範囲の認証	個人情報の収集目的内の利用か 当該情報を何に使おうとしているのか、その利用目的の認証

このうち、「個体認証」は情報セキュリティの課題ではないので除外する。本来は「主体認証」「意図認証」「利用目的認証」がすべて満足して情報へのアクセスが許可されるべき

であるが、一般に主体認証のみを認証として取り扱っている。前述のとおり正当権限者の不正行為は意図認証の課題であることから、これでは不十分であることは自明であろう。さらには利用目的認証がおろそかになるとプライバシー権を侵害することにもなりかねない。

たとえば機密性は、JIS Q 13335-1:2006 では「認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性」、政府統一基準では「情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。」と定義されている。いずれも主体認証のみであり、意図認証、利用目的認証については触れられていない。たとえばサーバ室の入退室管理では、マニュアル管理のときには、「入室目的」（意図認証）という欄が必ずあったが、カードシステムが導入され、カード保持者は入室許可という取り扱いに「退化」した。人の意思を様々なセンサーで取り出す研究が進められているが、これらの研究成果がでてくれば意図認証を機密性の定義に追加するのであろうか。意図認証ができていないことは受容する脅威として整理すべきと考える。

個人情報については、収集目的外の利用は法律・条例で禁止されている。操作者が個人情報にアクセスするときに、「利用目的」を確認しなければならない。少なくとも情報資産の分類には追加すべき事項である。

３．２　認証の回避

正当権限者の不正行為の防止には認証は無力であるが、さらに認証を回避することも可能である。主体認証も意図認証も利用目的認証も、OS を含めたソフトウエアで実現しようとするのであるが、「成り済まし」は大きな脅威として語られるが、認証の回避については語られない。どのようなシステムも物理的にアクセスされてしまえば、セキュリティはないようなものである。チップや HDD から直接に情報を取り出す方法は様々研究されているが、もっとも簡単な認証の回避の手法は別の OS で起動することである。主体認証やアクセス制御などが OS や OS 上のアプリケーションソフトによって行われることから、別の OS で起動することはこれらのすべてを無効にすることができる。Linux と Windows のファイルシステムとの互換を確保したことにより表面化した（２００７年３月以降）脅威で、大きな脅威であるにも関わらず見過ごされてきた。端末機は物理的にアクセスが可能な状態で休日夜間はワイヤーでつながれて放置されている。サーバ類も同様で未だにサーバ室内でのサーバオペレーションが行われている。内部 LAN の盗聴も同様で、認証なしに情報を入手することができる。認証の回避への対策はない。物理的にアクセスされない空間に情報を保存すべきである。

４．今後の課題

どうすれば監査は事故防止に有効な手段となりえるのか、という問題意識があり、当面、実施されている技術的セキュリティに対する有効性の監査の手法についての検討を進めたいと考えていた。

本稿では、対策型監査として事故防止に直結する監査の在り方を示し、特に認証システムの回避策を例として技術的セキュリティに対する有効性の監査の手法を検討した。

今後、出口対策の手法等が確立されていくことで、さらに同様な検討を深めることができると考えている。

新しいタイプの攻撃による出口対策の重視、セキュリティ報告書による関係者への説明、スマホ等の普及による持ち込み規制の無力化などが契機となって情報セキュリティの大きな転換点を迎えている。本稿は監査がこれらの転換をどう受け止めるべきかについての検討の第一歩でもある。

[1]事故

情報漏えいの事故に限定して検討する。情報漏えいの事故は機密性確保のごく一部でしかないが、出口対策の体系、情報入手経路対策の体系、完全性確保の体系、可用性確保の体系はそれぞれ別の体系であると考えるので、独立して検討することも意味があると考えた。

[2]事故発生の要素

事故発生確率に最も強く影響するのは攻撃を企てる人の発生率と考える。ただしこの発生率はわからない。「攻撃可能な環境」というのは、攻撃を企てる人の意思力、技術力等の総合力と環境の防衛力との差であり、環境の有する脆弱性そのものではない。

攻撃の対象は要素としなかった。情報資産の価値等の要素は情報保有者にとっての価値は判断できるが、すべての者にとって同じ価値とは限らない。漏えい情報の内容よりも漏えいしたという事実が重いこともある。被害想定の要素ではあるが攻撃者の意図はわからないので、事故発生の要素にはできない。

[3]攻撃の容易性を評価する

「攻撃の容易性」（パソコン利用者の何%の人が攻撃可能な脆弱性か評価する）という評価基準を位置付け、事故発生率の代用とすることが可能と考える。

[4]作業日報

持ち出し許可の偽装等によるすり抜け対策の意義も持つ。（単なる DB のアクセスログだけではなく、端末の操作ログをも含む。）作業密度の測定等の経営情報としての活用も考えられる。

[5] 受容した脅威の一覧

「情報セキュリティ監査人は、監査計画の立案に役立たせるため、リスクアセスメントを実施することが望ましい。」「被監査側においてリスクアセスメントが行われている場合、情報セキュリティ監査人は、リスクアセスメントの適切性を確かめた上で、被監査側によって実施されたリスクアセスメントの結果を監査計画の立案に活用することができる。」（情報セキュリティ監査基準実施基準ガイドラインVer1.0　経産省）とのガイドラインから、監査計画を策定するまでにはリスクアセスメントは実施されており、その成果である受容した脅威の一覧は保有していることを前提とした。

[6]想定外の脅威

基本方針で「想定する脅威」を定義するので、「想定しない脅威」が存在する。これは枠組みとなり、想定しない脅威が議論されることはないので、ここではあえて記載しておくが、以下では「想定しない脅威」は議論しない。

[7]追加される脅威

採用したセキュリティシステムが抱える「仕様としての脆弱性」の例は多い。製品ごとに調査することになる。ＩＰアドレス、ＭＡＣアドレスは偽装が可能である。ＶＬＡＮはＡＲＰ攻撃により突破された事故が発生している。また情報の持ち出しにあたりステガノグラフィー（画像にデータを隠す）で加工されていれば目視では確認できない。通信による持ち出しについても同様である。平文で確認することになる。

実装したセキュリティ対策に脆弱性が混入して期待された機能を果たしていないとき、また新たなクラッキング技法が発見されれば新たな脆弱性として、脅威の一覧に追加しなければならない。暗号化は最良の手法ではあるが、暗号アルゴリズムは検証されていたとしても実装段階で失敗している例もあり、また解読ツールが多く提供されている。これらも脅威の一覧に追加しなければならない。

【参考文献】

経済産業省　「システム監査基準」2004年10月8日改訂
http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kansa.pdf（2013.5.30 参照）
情報セキュリティ政策会議　「政府機関の情報セキュリティ対策のための統一基準(第 4 版) 」2009 年 2 月 3 日
http://www.nisc.go.jp/active/general/pdf/K303-081.pdf（2013.5.30 参照）