内部不正対策が難しい4つの理由、情報漏えいを防ぐツールの組み合わせ&使いこなし術

2014年は自社関係者による情報漏えい事故が多発した。中でも7月に発生した大手通信教育事業者の再委託先社員による大規模な顧客情報の持ち出し事件は記憶に新しいのではないだろうか。デロイトトーマツリスクサービス シニアマネジャーの高橋宏之氏は「内部不正関連のインシデントはさまざまな業界で起こっており、さらに発生元は社内だけに留まりません。複雑化してきているのが現状」とし、「こうした内部不正をいかに発生させないかを考えていくことは、今の企業にとって喫緊の課題です」と指摘する。

デロイト トーマツ リスクサービス
シニアマネジャー
高橋 宏之 氏

“不正のトライアングル”を成立させない取り組みが重要

内部不正に対する企業の認識が問われている。2014年は内部関係者からの情報漏えい事故が多発したにもかかわらず、自社に不正を行う職員はいない、自社の対策は万全だ、自社に漏えいして困る情報はない、という認識を持つ企業が依然として多いのだという。

デロイト トーマツ サイバーセキュリティ先端研究所主催の第3回サイバーセキュリティセミナー「内部不正対策とデジタル・フォレンジック～今求められる不正監視と証拠保全～」で登壇した高橋氏は、「まだまだ内部不正は多くの企業や組織にとって対岸の火事です。何かピンと来ていないという会社が多いのが現状ではないでしょうか」と内部不正に対する認識の甘さが実際の対策を阻害する要因なっていると指摘する。

「今後企業は、内部不正を発生させないためにどうするかを真剣に考えていかなければなりません。そこで重要なのが、『機会』『動機』『正当化』という“不正のトライアングル”を成立させないための取り組みです」

まず内部不正の「機会」となるのは、内部統制の不備や権限管理のずさんさ、あるいはモニタリングがされていないといった状態だ。また内部不正を働く「動機」としては、個人的な金銭目的や会社に対する不満、プレッシャーなどが挙げられる。そしてお金は返すつもりだ、会社が悪いからやってもいい、という理由で内部不正を「正当化」する。

「この3つのトライアングルの膨張が、実際の不正行為のトリガーになります。裏を返せば、この3つの要素をいかに小さくするかが、内部不正対策のポイントとして非常に重要だということです」

しかし3つのトライアングルをもとにした内部不正対策を採ったとしても、内部不正を完全に予防することはやはり難しい。そこで、もし内部不正が発生した時に、それをいかに早く見つけ、被害を最小化するかという“発見的統制”が求められる。その際に有用となるのが、ログを分析して、怪しい操作などがあった場合にはアラートを出してくれるSIEM（Security Information and Event Management）製品などのログ監視ツールだ。

ログ監視は、内部不正の検知という場面で非常に有効となるもので、たとえばクレジットカード情報の不正持ち出しや不正な給与操作、開発者による本番環境への不正アクセスなどを検知する場面で活用できる。

内部不正を定義し、複数ログの相関関係から不正をあぶり出す

ただし、ツールだけでも内部不正のログ監視は非常に難しいという。その背景にあるのが、内部不正の4つの特徴だ。

まず1つめが、そもそも内部不正の定義は非常に難しいということだ。定義に必要となる論点はさまざまだが、高橋氏の経験上、特にインパクトが大きいのは、完全な違法行為だけでなく、内部規定違反も内部不正に含めるのかどうかということだという。

2つめの特徴として、内部不正で利用されるデバイスは多種多様な点が挙げられる。内部不正の手順は、「内部情報の取得」から「加工・変更」、そして「外部への送信・持ち出し」という3つのステップを踏むが、その過程ではPCだけでなく、スマートフォンやタブレット端末も利用されることになる。

特徴の3つめが、一歩間違えると、企業と従業員との間で訴訟などのトラブルに発展する恐れがあること。内部不正を検知し、実行者を特定するまでには、まず不正を検知し、怪しい人物を絞り込み、その人たちに対して現場の部門長などが現場確認を行い、実際に不正があった場合には証拠保全を行うというステップを踏むが、ここで一番重要になるのが、現場確認のフェーズだという。

そして4つめの特徴が、内部不正は単一のログだけでは、あぶり出しが困難なことだ。そこで内部情報の取得、加工・変更、外部への送信・持ち出しという各フェーズで行われる行為に対してスコアを付け、それらを相関的に分析にして、累計スコアの高いユーザーを、内部不正の容疑が高い人物としてあぶり出していくことが重要となる。

こうした内部不正監視の仕組みを実際に構築するためには、SIEM製品などログ監視ツールを使って、まずリアルタイムの検知を行い、さらに取得した各種ログ間の相関関係を洗い出すことが先決だ。ただし内部不正の検知は1～2年をかけてじっくり見つけていくというケースもあり、その際には高度なデータ分析ツールを組み合わせることで、時系列をより深堀りした分析が可能となる。

一方、既にログ監視の仕組みを導入済みの企業から最近よく出る話として、検知量が多すぎて運用が回らない、逆に検知量が少なすぎる、あるいはまったく検知されないという相談だという。

「せっかくのログ監視の仕組みが形骸化してしまっている企業が多いというのが現状です。やはりチューニング、つまり効果的な改善が必要です」

PDCAサイクルは運用が始まってから考えるという企業も多いが、それではなかなか進展しないのが実情だろう。また、対策に抜け漏れがあっては元も子もない。複雑さを増す内部不正対策は、デロイトトーマツリスクサービスのように、ツール選定から、運用のノウハウも持っている企業と共同で取り組んでいくのが、企業にとって有力な選択肢となりそうだ。

内部不正の追跡方法、メモリ情報とハードディスク情報の連携がカギ

インターネットのセキュリティ組織である米CERT/CCの調査結果によれば、サイバー犯罪の犯行者の約70%が外部者なのに対し、内部者は約28%だが、実際の被害に占める割合は半々ぐらいで、内部不正は一旦発生すると組織に与えるインパクトがかなり大きなものになるという。デロイト トーマツ リスクサービス シニアコンサルタントの中田将之氏は「犯罪が実際に表面化するのは氷山の一角ですが、内部不正を対岸の火事として捉えることなく、取り組んでいく必要があります」と強調する。

デロイト トーマツ リスクサービス
シニアコンサルタント
中田 将之 氏

デジタル・フォレンジックでは、“証拠保全”が極めて重要

デロイト トーマツ サイバーセキュリティ先端研究所主催の第3回サイバーセキュリティセミナー「内部不正対策とデジタル・フォレンジック～今求められる不正監視と証拠保全～」で登壇した中田氏は一般的なデジタル・フォレンジックのプロセスは、保全、準備、解析、報告という4つのプロセスに分けて考えられると説明した。

まず保全フェーズでは、情報収集を行い、被害の対象となったPCやサーバを差し押さえる証拠保全を行う。次に準備のフェーズは解析に向けた準備段階で、調査を行う上での仮説を立て、取得したデータが暗号化されていれば複号化を行うといった作業を行う。そして解析フェーズが実際のフォレンジックを行う段階で、ファイルのタイムスタンプ解析（タイムライン）や各種ログの解析、データの復元などを行う。そして最終的に報告を行い、調べた事象から何が分かったのかをまとめていく。

一方で中田氏は、従来の証拠保全方法が、場合によっては落とし穴になってしまう可能性があるとも指摘する。

たとえば証拠保全の対象が、事象が発生したPCのハードディスクだけとなっている場合だ。それだけでは、メモリなどの揮発性情報までは保全されず、重要な情報を取り損ねてしまう恐れがある。

「発生した事案や対処する内容を考慮した上で、適切な対応を採る必要があります。これが証拠保全のフェーズにおける非常に重要なポイントです」

内部不正対策では、メモリ情報の解析が重要な鍵を握る

また最近では、組織内PC、個人のスマートフォン、クラウドの3つの環境が組み合わされた複雑な操作によって複数のシナリオが想定され、フォレンジック調査が大きく難航する可能性も高くなってきている。

こうした課題に対する有用なアプローチ方法が、メモリ情報を詳しく見ていくことだ。組織内PC、個人のスマートフォン、クラウドのいずれの環境においても、メモリ情報の解析が、事象を把握するための重要な鍵を握ることになる。

メモリの解析から得られる情報は大きく3つで、遠隔操作プログラムの実行プロセスといった“プロセス情報”、遠隔操作元のIPアドレスなどの“ネットワーク情報”、そしてパスワードや暗号鍵など“ユーザーの入力した値とその操作内容”だ。

次にメモリとハードディスクの情報をフォレンジックの観点から比較した場合、まずメモリからの情報は、先にも触れたプロセスやネットワーク、ファイル、パスワードや暗号鍵など“今現在の稼働状況が分かるもの”だといえる。一方ハードディスクからの情報は、ファイルやログ、レジストリ、ショートカットなどの各種アーティファクトなど“過去から現在までの状況が分かるもの”だ。

このメモリ・フォレンジックを進めていく上では、大きく3つのフェーズがある。1つめがメモリの証拠保全で、メモリ情報をダンプしてファイルに落とし込む作業、2つめがメモリ情報の解析で、メモリから必要な情報を抽出して解析する作業、そして3つめが、解析した情報から証拠となる情報を収集する作業だ。

証拠保全の手順整備、教育、演習を行い、全社を挙げて内部不正に対応する

内部不正に対する具体的な証拠保全方法を考える時、3つの手順が挙げられるという。順番に、証拠保全手続きの見直し、保全の教育、インシデント演習だ。

まず証拠保全をいきなり“本番”でやろうと思ってもなかなか難しい。そこでメモリやハードディスクの情報をどのタイミングで取得するかなど、事前に手続きや手順を整理、検討しておく必要がある。また1つの保全ツールだけに依存してしまうと、取得がスムーズに行えない可能性もあるので、複数の手段を準備しておくことが肝要だ。さらに対応していく中でのバグやエラー情報などを収集し、その解決方法や代替手段を対処するチームの中で共有することも大切な取り組みとなる。

証拠保全の手順を整備したら、次にその手順に基づいた証拠保全が実際にできるように従業員へ教育を施しておく必要がある。保全方法や手順を関係する部署へ展開しておくことも必要だ。また教育やトレーニングを定期的、継続的に実施して、知識のアップデートを図っていくことも重要となる。

そしてその教育の効果を、模擬演習で継続的に検証することが望ましい。これによってインシデント対応フローがきちんと回っているか、部門間の連携がきちんと取れているかなどを見極めることができる。そして演習後は必ず振り返りを行い、改善ポイントの検討と手順の更新を行う。

「内部不正の対象となった端末の解析を行う上で、メモリの情報は今後重要なウェイトを占めていきます。また証拠保全の手順の整備や教育、演習といった備えが必要不可欠です。そしてこうした一連の取り組みは情報システム部門だけが対応すればいい問題ではなく、部門横断的に全社を挙げて取り組んでいくべき重要なテーマだといえるでしょう」

※本記事は、2015年2月12日に掲載されたビジネス+ITからの転載です。

お問い合わせ先

Deloitte. トーマツ.

デロイトトーマツ リスクサービス株式会社
〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル
Tel:03-6213-1300　URL：www.deloitte.com/jp/dtrs