内部犯行から企業の秘密情報を守るには。ますます重要となってきた出口対策

ネットワンシステムズ株式会社
栗田 晴彦

1．初めに

本年 6 月に経済産業省から、「営業秘密の保護・活用について」という資料が公表されている。企業の情報資産を守るために「不正競争防止法」という法律があるが、その趣旨に沿って、保護すべき「営業秘密」の定義や、背景、体制、保護ガイドブックなどの説明がなされている。

最近は、サイバーセキュリティというと、標的型攻撃やランサムウェアといった言葉が話題になることが多いが、こと情報漏洩ということとなると、内部犯行の脅威は依然として非常に大きい。今までにも、ライバル会社への研究開発情報等の知的財産漏洩や個人情報漏洩・転売などの事件が、幾度となく発生してきてしまっており、度々ニュースにも取り上げられてきた。今後も、この脅威は増えることはあっても減ることはない。内部犯行対策に対してこれらの事件から学ぶべきことは今でも非常に多い。

内部不正に対する事例・調査やこのガイドブックに記載の対策内容を軸に、技術的な視点から企業における内部不正対策の考え方とポイント、特に出口対策の重要性について記述したい。

2．不正競争防止法が適用対象。「通常アクセス」による不正

本稿では、法律の詳しい説明・解釈をすることが趣旨ではないが、多くの内部犯行による情報漏洩事件で被告は「不正競争禁止法」で告発されている。この法律は、営業情報や設計情報などの企業の重要な知的財産を保護し、公正な競争と国際約束の的確な実施を確保するために 1993 年に作成されたものだ。

通常の、サイバー空間での不正アクセスや情報漏洩では、「不正アクセス禁止法」で訴えられるが、何故、それが適用されないのか？　その理由は、情報へのアクセス方法が「不正なアクセス」ではなく、業務上正当に与えられた「アクセス権限を濫用」して、情報漏洩を起こすということにある。

例えば、ハッキングなどで別な管理者の ID/PW を盗んで、それを悪用して顧客 DB にアクセスしたのであったら、不正アクセス禁止法で訴えられていたであろう。あるいは、不正なプログラムを作成してそれを動かし、情報を入手していたら同じく不正アクセス禁止法の対象となっていただろう。

内部犯行の典型的なパターンでは、システムの管理権限など正当に付与された権限を用いて情報を入手している。更に、日常の仕事の中で、それらを USB デバイスに書出す、メールに添付して送付するなど、持出をおこなっている。つまり、通常の業務遂行の一環で、「不正アクセス」せずとも情報の入手と持出しが可能であり、通常業務との見分けがつきにくいのが「内部犯行」の典型的であると言わざるを得ない。

様々な報告書を見てみると、以下の 3 つが共通する技術的な課題として挙げられている。

－過剰なアクセス権限の付与
－ログ取得やログ監視の漏れ
－ USB などの書出しの制御不足

以下では、これらの問題に対する対策を深堀したい。

3．秘密情報保護ハンドブック / 内部不正対策ガイドラインに見られるセキュリティ対策

内部不正に対抗し、企業の重要な情報を万全に守るためには、どうしたらよいのか?そのガイドとして以下の 2 つが挙げられる。

1.「秘密情報保護ハンドブック」（以下、保護ハンドブックと略称）：

2015 年 1 月の不正競争防止法の改正を受け、秘密情報を具体的にどのように守るかを示すために、2016 年 2 月に策定。

（経済産業省　秘密情報の保護ハンドブック）

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

2.「組織における内部不正対策ガイドライン」：

IPA（独立行政法人　情報処理推進機構）が、度重なる内部犯行を受け、2013 年に作成。最新版は第 4 版（2017 年 1 月）。前述の保護ハンドブックでも、技術的な対策面では本ガイドラインを参照している。

（IPA　組織における内部不正対策ガイドライン）

https://www.ipa.go.jp/files/000057060.pdf

本稿では、この2つを参考としながら、技術的対策を考察したい。内部不正への技術的な対応は、大きく分けると下記の 3 つの対策カテゴリーに分類するとわかりやすい。

1．ＩＤ管理：必要な人が必要な情報・リソースにのみアクセスできることを保証する。認証と権限管理を含む
2．ログ管理：不正やその予兆を事前に検知し、インシデント発生時にはその影響範囲や内容をすぐに特定できる
3．出口対策：USB デバイス、印刷物や電子メール、Web アクセスなどでの情報の持出を防止する

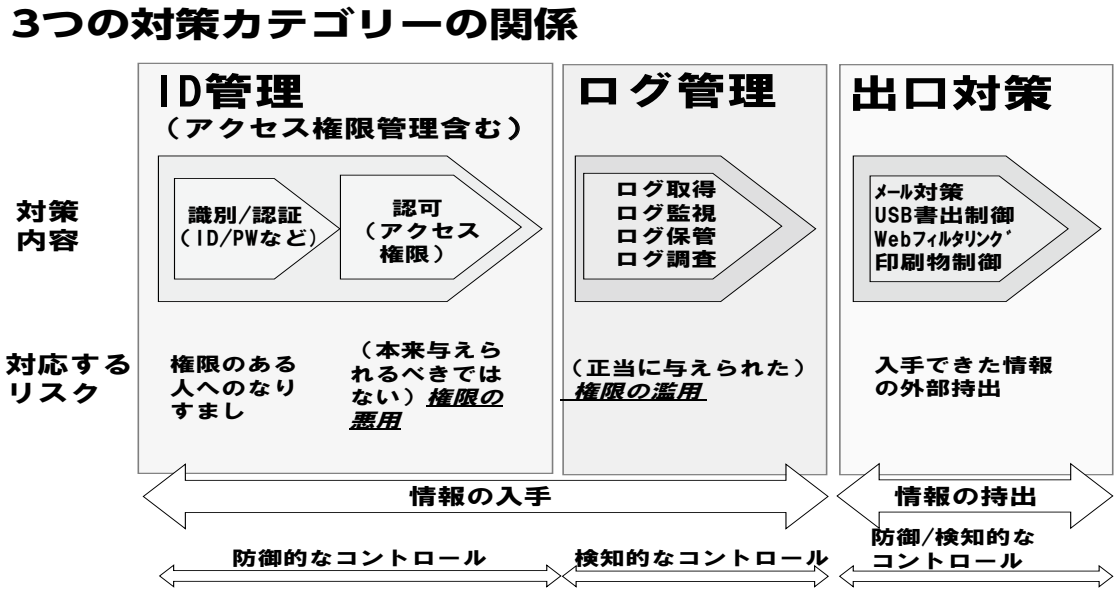

図 1：3 つの対策カテゴリーの関係

これらが、多層防御の考えでみられる「各層」を構成し、企業の秘密情報の外部への「不正な」漏洩リスクを低減する働きをしている。なお、これらの３対策カテゴリーは、図２で示す、保護ガイドブックでの５つの対策目的の最初の３つの技術的対策にほぼ対応している。

接近の制御⇒　　ＩＤ管理
持出し困難化⇒　出口対策
視認性の確保⇒　ログ管理

この３つを主軸で考えることで、大まかには対策はカバーできると考えてよいであろう。

図２：　秘密情報保護ハンドブック　の５つの「対策の目的」と３対策カテゴリーの関係

注：保護ハンドブックでの「対策の具体例」には、物理的対策も含まれているので、３対策カテゴリーとは必ずしも一致しない。また、接近の制御の例には、ネットワーク分離が含まれるが本稿では省いている。6. まとめの項を参照のこと。

4．ＩＤ管理やログ管理の限界

内部不正対策、あるいは内部統制を考えた場合、あるいはセキュリティ管理の基本を考えた場合、対策のベースは、ＩＤ管理とログ管理と言っても異論はないであろう。金融業界でのデータ保護のデファクトスタンダードである、PCI DSS や、個人情報保護法のガイドラインでも、ID 管理とログ管理は大項目で取り扱われているし、最近 IoT(あるいは、IIoT）で話題となっている制御系システムに対する基準の IEC62443-1-1 でも、7 つの基本要求のうちの 3 つが、この分野である。

ただし、内部不正対策として現実の業務への適用を検討してみると、以下の限界が見えてくる。

＜ID管理の限界＞

認証強化：そもそも、正当な本人がアクセスするので、どれだけ認証を強化しても意味がない。

権限管理強化：必要最小限の権限に出来たとしても、そもそも情報へのアクセスを許すわけであるから、権限の濫用は防ぎようがない。それを、防止するには、複数名に権限を細分化するなどがあるが、業務プロセスの変更を伴い、業務効率が落ちる。

権限管理強化の限界の良い例は、運用管理者の特権がある。特権は与えない方がよいが、どうしても必要な業務がある。特権を与えた場合の濫用を防ぐために、権限を分けての 2 名体制での作業などがよく取られるが、夜間や緊急時などどうしても 1 名での作業を認めざるを得ないのが現状である。

ID 管理の限界、つまり権限の濫用を防ぐことに限界があるので、通常はその部分をログ管理（特にログ監視）でカバーするという考えとなるが、残念ながらそれにも大きな障壁が存在する。

＜ログ管理の限界＞

ログ監視：不正と思われるアクセスパターンを考え、そのクライテリアでアラートを出すのが通例であるが、誤報がほとんどで有効な監視となりにくい。

内部不正対策で、よくログ監視の閾値に挙げられるのが、「大量のダウンロードや印刷」、「休日や夜間などのアクセス」、「退職予定者の秘密情報へのアクセス」などである。ただし、それを行ったから必ずしも不正行為という訳ではなく、正当な目的でアクセスする場合がほとんどである。そもそも、最小権限の考え方に沿えば、アクセス出来るということは、その行為（「例えば休日や夜間のアクセス」）が認められていることなので、それが不正かどうかの判断は困難を極める。休日や夜間のアクセスが問題なら、そもそも権限をなくしアクセスを禁止する方が最小権限の考えに沿っているのだ。

また、誤報か不正かどうかの最後の判断は、セキュリティ部門では困難でありその利用者部門でせざるを得ず、大量の誤報が出てしまうので、そのチェックが形式的にならざるを得ない。

この点で、標的型攻撃やマルウェアなどの外的脅威を、IDS 等のセキュリティ監視システムで監視するモデル（ＳＯＣ等）とは、同じログ監視とはいっても本質が異なることを留意すべきである。外的脅威は、攻撃のパターン化がしやすく、明らかに通常アクセスとは異なる振る舞いがある。そのため、（最近は高度な攻撃も多いが）まだ監視がしやすく、実際に多くの標的型攻撃では監視システムにひっかかっている。

＜内部不正では、検知より抑止を＞

図 1 では、ログ管理を技術的対策である「検知策」としているが、面白いことに、図 2 の保護ハンドブックでは、ＩＤ管理（接近の制御）や出口対策（持出困難化）を「物理的･技術的な防御」とまとめているのに対し、ログ管理は、

「心理的な抑止」の一項目としている。内部犯行対策に関しては、ログ管理へはこのぐらいの思い切りが重要と考える。権限の濫用に伴う内部不正に対するログ監視は、非常に困難であるうえ、それで発見されたケースは非常に少ない。よって、無理に発見することだけを目指すのではなく、「ログを取得し監視されているのだ」という抑止効果を狙うのである。こう考えれば、「いくら頑張って監視しても結局内部不正は見つからない。監視は意味がない、やめてしまえ」という圧力に対抗できる。

コンサルティングで関わったあるお客様では、「不正の発見」ということをあきらめ、抑止効果を中心に考えているところがあった。例えば、大量のファイルアクセス上位 30 名を社内に Web 公表する、不定期に部門を選び出し、その部門員のアクセスを徹底的にチェックするなど、監視していることを「情宣」することで不正のやる気をそぐ方法だ。

5．出口対策の重要性

ID 管理やログ管理でも十分コントロールできない情報漏洩リスクを、最後に「水際で」制御するのが、出口対策であり、近年、重要性がさらに強調されている。

IPA の「内部不正による情報セキュリティインシデント実態調査　－調査報告書－（2016 年 3 月）」の中に、出口対策の考察に重要な 2 つのデータがあるので紹介したい。

表 1　効果的だと思う対策の比較

内部不正経験者		対　策	経営者・システム管理者	
順位	割合		順位	割合
1位	50.0%	ネットワークの利用制限がある（メールの送受信先の制限、Web メールのアクセス制御、Web サイトの閲覧制限）	2位	30.0%
2位	46.5%	技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）	4位	27.0%
3位	43.0%	技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる	1位	43.9%
4位	25.0%	職務上の成果物を公開した場合の罰則規定を強化する	12位	12.8%
5位	23.5%	管理者を増員する等、社内の監視体制を強化する	11位	13.1%

調査報告書　P42 表 13 を転記

お分かりのように、内部不正経験者の答えた有効な対策上位 1 位～ 3 位が、それぞれ出口対策、ログ管理、ID 管理に該当している。内部不正を経験した本人の意見なので説得力があるが、やはり ID 管理やログ管理の対策の限界と、それに比べた出口対策の重要性を示す証拠と考えてよいだろう。

また、この調査報告書の P19 に、持出手段のランキングがあり、上位から USB メモリー(53.0%)、電子メール(28.9%)、

紙媒体（18.8%）となっており、それにHDD、Webアップロードなどが続いている。
今後のクラウドなどの外部ストレージやコラボレーションインフラの普及を考えると、外部記憶媒体、電子メール、Webアップロードの3種類が主な出口対策の対象と考えるが妥当であろう。

PCI DSS、個人情報保護法のガイドラインなどの今までの基準では、出口対策はほとんどカバーされることはないが、保護ハンドブックや、内部不正防止ガイドラインには、かなり具体的な記載が見られる。

＜「秘密情報の保護ハンドブック」に記載のある出口対策　（従業員等に向けた対策部分）＞

－社外へのメール送信・Webアクセスの制限
－電子データの暗号化による閲覧制限等
－遠隔操作によるデータの消去機能を有するPC・電子データの利用
－私物のUSBメモリーや情報機器、カメラ等の記憶媒体・撮影機器の業務利用・持込の制限

＜「内部不正対策ガイドライン」に記載のある出口対策＞

－私物の記憶媒体の持込制限、外部記憶媒体の利用制限ソフトウェアの導入
－ Webアクセスでのコンテンツフィルタリング
－電子メールでのメール送信再確認や上司の承認機能、添付ファイルの強制暗号
－リモートで情報機器内の重要情報を消去できるツールやサービス

これからは、内部不正に対する対策として、出口対策は必須の検討対象となったということであろう。

＜今後、主流となる、IRM、CASB＞

保護ハンドブックでは、出口対策「電子データの暗号化による閲覧制限等」の中で、「アクセス権を有するIDでログオンしたPCでのみ閲覧できる」 として、対策を具体例で記載している。これを実現できるソリューション、IRM (Information Right Management) が、最近注目を浴びており、幾つかのソリューションが出ている。
これを導入すれば、ログオンした人への閲覧制限のみならず、コピーや複製、転送の制限、更には漏洩後のデータの消去（暗号化鍵の権限制限）など遠隔操作でのデータ消去へも対応できる。
データ自身を暗号化するので、外部記憶媒体、メール、Webなどの流出経路に関係なく制御がかかるので、今後は、出口対策の決め手として、導入する企業が増えてくるであろう。10年前にあるお客様のコンサルティングでこのIRMの選定に関わったが、当時に較べてツールの完成度も高まっており、導入の敷居は確実に下がっている。
この場合は、残存するリスクとして、暗号化をし忘れる、あるいは暗号化するが権限設定を間違えるという事象を考える必要があり、フォルダーに入れると自動的に適切な権限で暗号化する、DLP（Data Loss Prevention）などと組み合わせて未暗号のものを探すなど、そのリスクを低減するためのソリューションも検討すべきであろう。
また、Webアクセスの多様化と高度化の動きを受け、出口対策の中にCASB（Cloud Access Security Broker）などが、含まれてくる時代も遠からず来ると考えており、すでにCASB、DLP、IRMなどの統合も生まれてきている。

6．まとめ

以上、内部犯行の事例・調査やガイドブック等をベースに、内部犯行に対する出口対策の重要性を述べてきた。この出口対策はお分かりのように、当然標的型攻撃を代表とする外部脅威への対策としても極めて有効である。乗っ取りなどを受けた端末からの情報持出を防ぐ最後の防波堤として機能するのである。

なお、本稿では、最近話題のネットワーク分離については触れなかったが、Web分離や、基幹ネットワークとOA ネットワークの分離などとしてよく検討されるこの対策も、「入口対策」と同時に「出口対策」としても有効である。これに関しては、紙面の都合で、割愛せざるを得なかったことをご了承いただきたい。

最近、セキュリティ対策として多層防御が当たり前に言われ始めたが、各々の層での防御の内容と目的が明確にされているとは言い難い。やみくもに防御を重ねても、実は大きなリスクへの検討が抜けている場合があり、効率的で効果的な対策とはならない。それぞれの対策で何が出来るかと同程度に、何が出来ないかを理解することも重要である。

本稿が皆様のセキュリティアーキテクチャ検討の一助となれば幸いである。