バンドエイドで情報漏洩は防げない
～情報漏洩防止を支えるITと運用～

基盤ソリューション本部
基盤イノベーション技術部
シニアプロジェクトスペシャリスト

野坂　照秋

Teruaki　nosaka
Teruaki-nosaka@exa-corp.co.jp

情報漏洩インシデントが後を絶たない。JNSAのレポートを分析すると、原因の大半は内部要員のうっかりミスである。情報利用者への指導・教育だけでは、このようなうっかりミスを防ぐ大きな効果は期待できない。強制的な統制手段として、機密情報持ち出し操作の「検出」、「警告」と機密情報の「保護」が有効であり、これらはITによって実現することが可能である。

本稿は、情報漏洩対策ツールである「Symantec Data Loss Prevention（DLP）」の機能を紹介しつつ、情報漏洩対策の考慮点と方向性を考察する。

1. はじめに

1.1. ネットワークの普及と情報漏洩

1980年代まで、多くの組織は外部との通信手段として電話かファックス、または郵便を利用していた。1990年代からは電子メール、Webをはじめ、ファイル共有ソフト、チャット、インスタントメッセンジャーなどが登場し、2000年代には、オンラインストレージサービス、ツイッター、フェイスブックなどのソーシャルネットワークサービスなどが普及してきた。

ビジネスの現場では電子メールやWebが不可欠のものとなり、巨大ファイルを無料で簡単にやり取りできるオンラインストレージサービスを利用している組織もある。

ICTの発展は、ビジネスの拡大や生産性の向上に貢献してきたが、その便利さと同居しているリスクにも目を向ける必要がある。

ファックスの登場によって手軽に文書を送付できるという利便性の一方で、あて先を間違えて企業秘密を漏洩させる事故が発生するようになった。

同様に、電子化された大量のデータが、インターネットによって複数の場所に、瞬時に、簡単に配布できるようになったことは、ビジネスに利便性を提供したが、意図しない相手に大量の企業秘密を送付する危険性をもたらした。

加えて外部記憶装置の小型化、高速化により、大量の機密情報を一気に持ち出せるという危険性が増大することにもなった。

このようなICTの発展、普及は利便性と引き替えに情報資産に対する脅威を増大させている。

1.2. 情報漏洩の一般的なパターン

情報漏洩は外部との接点で発生する。完全に外部と遮断され、入退室時に厳重な持ち物検査が実施されている環境であれば、情報漏洩の可能性は非常に低い。このような厳重機密ゾーンは一定の生産性を犠牲にしてでも機密情報を守ることができるが、このような仕組みを全社的に構築することは費用対効果の点からも、そしてビジネスのスピードの点からも非現実的である

今日のビジネススタイルは外部とのコミュニケーションを重視しており、コミュニケーションによる生産性向上はビジネス上の重要課題となった。このため、ICTを利用したコミュニケーションが招くリスクを許容して利便性を優先する場合がある。これはリスクと利便性のトレードオフの結果ともいえる。

日本ネットワークセキュリティ協会（以下、JNSAと表記する）は、個人情報漏洩インシデントに関する年次統計を「情報セキュリティインシデントに関する調査レポート～個人情報漏えい編～」として発表している。2010年度版[1)]によれば、情報漏洩の原因は内部要員によるミスが大半であることがわかる。これは過去数年にわたって同様の傾向にある。このレポートは個人情報に関するものであるが、さまざまな機密情報が漏洩する原因も同様の傾向があると推察される。

2010年度版の情報漏洩原因比率のグラフを図１に示す。

図１　漏洩原因比率（件数）

図１のグラフから管理ミス、誤操作、紛失・置き忘れの３項目だけで全体の８割を超えていることがわかる。

ソフトウェアのバンドエイドともいえるセキュリティパッチ、アンチウィルスの適用は、外部からの攻撃に対して有効であっても、内部要員のうっかりミスに対してはほとんど無力である。では、情報漏洩防止に有効な対応策とは何であろうか。

本稿では情報漏洩の原因のほとんどを占める「内部要員によるうっかりミス」に焦点を当て、電子データの情報漏洩対策方法について考察する。２章で機密情報管理に対する検討ポイントを列挙し、情報漏洩対策として検討すべきテーマを述べる。３章では情報漏洩対策ツールとして利用

可能なテクノロジーを紹介し、４章でツール利用を踏まえた運用のあり方を検討する。

2. 機密情報管理への取り組み

情報漏洩を防止するためには、自組織における情報漏洩リスクを分析し、リスクに応じた対策を講じる必要がある。対症療法的な対策は、バンドエイドのように部分的な効果しか期待できない。本章では原因療法的なアプローチで機密情報管理に必要なテーマを検討する。

2.1. 情報のライフサイクルと機密管理の課題

情報は、生成され、利用され、役割をおえて廃棄（削除）される。本稿ではこの一連の流れを情報のライフサイクルと呼ぶ。また生成、利用、廃棄などの操作を総称してライフサイクルイベントと呼ぶことにする。

情報のライフサイクルの概要を図２に示す。

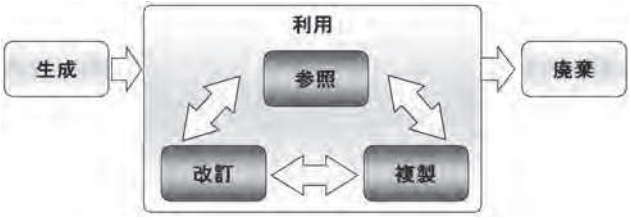

図２　情報のライフサイクル

情報漏洩は「利用」イベントによって発生する。そして、この図でわかるように情報を持ち続けている限り、「利用」イベントは発生する可能性があるので、情報が廃棄されるまで常に情報漏洩のリスクにさらされ続けることになる。

このため情報漏洩対策としては、情報のライフサイクル全体を視野に入れ、ライフサイクルイベントごとに必要な管理施策を適用する必要性が生じる。

2.1.1. 情報の生成

文書の新規作成や既存文書の複製、または外部からの入手などによって、組織内に情報が生成される。これらの情報を適切に管理するためには、情報の生成過程でその情報が機密情報に該当するかどうかを判断し、機密情報であれば適切な機密管理の方法を決定する必要がある。

しかし、多数の従業員やビジネスパートナーの業務遂行によって生成される情報は大量であるため、そのひとつひとつを対象とした機密管理の運用を徹底できていないのが現状である。

「生成」イベントに対する主な検討課題を以下に示す。

- 日々大量に生成される情報から、機密情報に該当するものをどうやって識別するか。
- 機密情報と識別された情報の機密管理をどのようにおこなうか。

2.1.2. 情報の利用

情報は利用するために生成される。情報漏洩は主に「利用」イベントの中で発生するため、情報利用時の機密管理に注意を払うことが重要となる。

情報は、パソコンで文書を開くことで参照され、メール添付やファイルサーバからのダウンロードなどで複製される。また、情報の維持管理の過程で内容が改訂される。

機密でなかった情報が、改訂によって機密情報に変化することもあるので、改訂のたびに機密情報かどうかの判断が必要になる。したがって、改訂操作であっても「2.1.1 情報の生成」で挙げた検討課題と同様の考慮が必要となる。

情報の利用イベントである参照・複製・改訂は、機密レベルに応じた適切な権限を有した情報利用者のみがおこなうように制御されるべきである。

「利用」イベントに対する主な検討課題を以下に示す。

- 機密情報に対する不適切なアクセスを、どうやって排除するか。
- 権限外のアクセスに対して、情報利用者に不正操作であることを通知するとともに、その事象をログとして記録できるか

2.1.3. 情報の廃棄

利用しなくなった情報や保管期間が経過した情報は廃棄しなければならない。しかし実際には、ディスクの容量不足によるハードウェアのアップグレードや、パソコンの廃棄などのイベントが発生するまで放置されるケースが多い。機密情報が保管されていること自体が忘れ去られたパソコンも存在する。

機密情報の廃棄作業としてデータの削除操作をおこなっ

てもゴミ箱フォルダにはまだ保管されていたということもあるし、ハードディスクをフォーマットしても、ディスク上には通常は読めないが物理的には一部データが残っている。このような技術的には情報が取り出し可能な状態であることを知らずに廃棄作業を完了したつもりになると、情報漏洩のリスクが残る。

機密情報を廃棄する際に重要なことは、データの再利用ができない状態にすることである。このためには、ディスク装置そのものを物理的に破壊するか、ディスク全体または削除対象データ格納エリアに無意味なデータを上書きするツールを使用する必要がある。

「廃棄」イベントに対する主な検討課題を以下に示す。

- 情報の廃棄作業をタイムリーに実施できるか
- 廃棄によって再利用できない状態にできるか

2.2. 機密情報管理の検討ポイント

情報のライフサイクルを分析することで見出した検討課題を整理すると、機密情報管理の検討ポイントは次の４点に集約される。

- 機密情報の条件と機密区分の定義
- 機密情報の棚卸し
- 機密情報のアクセス制御
- 機密情報アクセスのログ管理

検討課題と検討ポイントの関連を図３に示す。

2.2.1. 機密情報の条件と機密区分の定義

機密情報の漏洩を防止するために最初に実施すべきことは、どの情報をどの機密区分に位置づけるのかを定義することである。

ここで最も重要なのは、ひとつひとつのデータに対してどの機密区分に該当するかを識別するために、機密区分の条件を具体化することである。

ところが、一般的な組織が機密情報の定義を社内規定などに記載する場合、定義文は以下の例のような抽象的表現となるケースが多い。

表１　一般的な機密情報定義の例

機密情報の条件		機密性の低下により事業運営上の損害をもたらすもの
機密区分	極秘	事業運営上の損害が著しいもの
	秘密	事業運営上の損害が発生するもの
	社外秘	特定部門にのみ影響するもの

このような抽象的な条件表記は、個別データの機密性評価を困難にしてしまうことから、不用意な持ち出し操作の原因になりやすい。

情報漏洩は主に「利用」イベントの中で生じることから、情報利用者が実際に操作している情報の機密性を自身で評価できるよう、機密区分の条件が明確でなければならない。

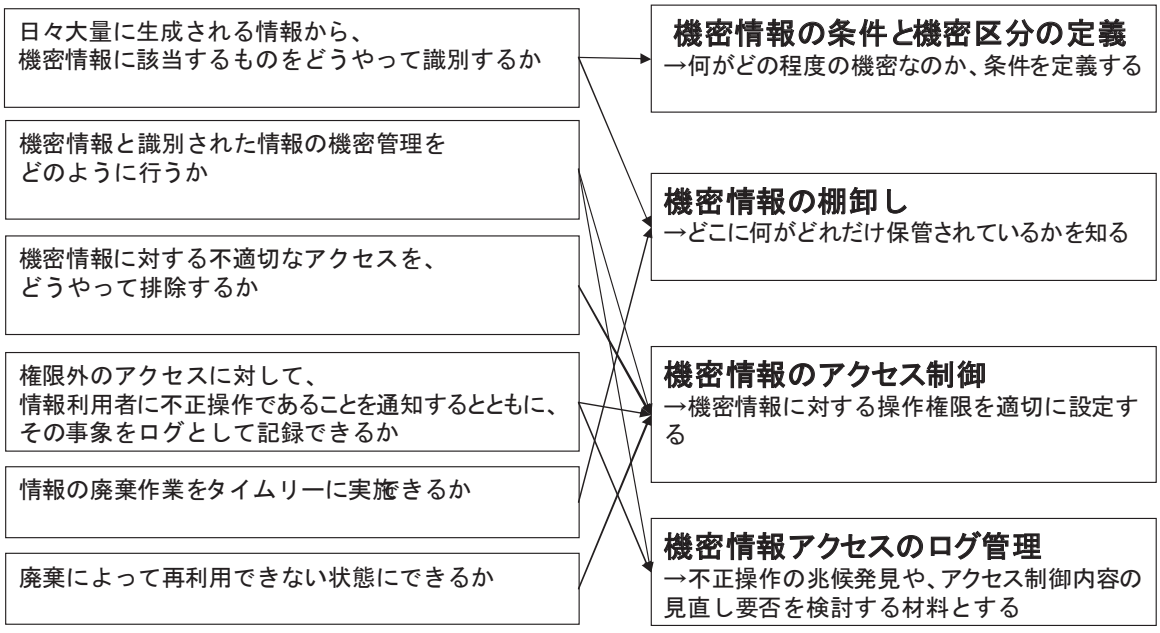

図３　機密情報管理の検討ポイント

2.2.2. 機密情報の棚卸し

機密情報の棚卸しとは、組織内に保管されているすべてのデータを対象として、機密区分の定義内容に沿ってこれを評価し、該当物の一覧を作成し、情報の管理状態を把握することである。

データは日々、生成・改訂されるため、棚卸し情報の鮮度・精度を維持するには、データの保管場所を定期的に点検し続けることが重要となる。機密情報を正確に棚卸しできれば、次のようなメリットを享受できる。

- 共有エリアでの機密情報保管など、不適切な管理状況が把握できる。
- 業務用パソコン内の機密情報を列挙することで、機密区分の定義を情報利用者に想起させるとともにセキュリティ意識の向上が期待される。
- 機密情報の管理実態を把握することで、規程・方針の見直し、通達、指導など実態に応じた施策を講じることができるようになる。

このようなメリットがあるが、データは組織内のあちこちで毎日生成されるため、すべてのデータを対象に人手で機密区分を管理し続けることはきわめて困難である。

このような棚卸しにかかる煩雑な手作業を避けるためにIT利用の検討が必要となる。

2.2.3. 機密情報のアクセス制御

アクセス制御は、特定のデータに対する操作要求を許可、または拒否するメカニズムである。

データのパスワード保護はよく知られたアクセス制御の一種である。データの所有者があらかじめデータにパスワードを設定し、アクセスを許可する情報利用者のみにパスワードを開示することでデータ操作の権限を付与する。

この他にアクセス制御リストを利用する方式がある。データに対して、何の操作を、誰に、許可または拒否するかをあらかじめアクセス制御リストとして定義しておき、操作要求が発生した際にアクセス制御リストにしたがって操作の許可または拒否を決定する。

このような一般的なアクセス制御メカニズムは、生成、保管されたデータの重要性があらかじめ決められていることを前提にして実装されている。言い換えれば、生成されたデータの所有者が機密区分を適切に判断できない場合、アクセス制御の対象にならない危険性がある。

機密情報の棚卸しが完了し、機密区分が明確になれば、一般的なアクセス制御メカニズムによって正確なアクセス制御を実装することは可能であるが、次々に大量に生成されるデータに対して、機密情報の棚卸しとアクセス制御設定をタイムリーかつ網羅的に実施することは困難が予想され、結果的に機密区分が曖昧でアクセス制御設定もされていないデータが大量に発生する。

このような状況では、データに対する操作要求が発生するタイミングで、そのデータが機密情報であるかどうかを判定することが情報漏洩を防ぐためにきわめて有効であると考えられる。

2.2.4. 機密情報アクセスのログ管理

機密情報アクセスのログ管理とは、機密情報の取り扱いに関する監査や万一の場合の調査に備えて、実際のアクセス内容を記録・保管することである。

不正競争防止法や個人情報保護法、PCI-DSSなど、機密情報管理に影響を与える法規制や業界標準でもアクセスログの取得が求められている。これらの法や標準が取り扱う機密情報の種類はそれぞれ各様であるが、いずれも共通して機密情報へのアクセスを記録し保管することを要件としている。

3. ITによる情報漏洩対策

これまで、情報漏洩にかかわる機密情報管理のあるべき姿と要件を説明してきたが、これら情報漏洩対策を支援するさまざまなITツールが登場している。手作業では膨大な時間とエネルギーを要するデータの機密管理のために、どのようなITツールを応用すると効果的なのか、その特徴を以下に説明する。

3.1. 情報漏洩対策製品の分類

市場に数多くリリースされている情報漏洩対策ツールは、提供している機能の特徴によって以下のように分類できる。

① デバイス制御型

USBポートや印刷機能など、パソコンのデータ持ち出しインターフェースを無効化する。持ち出し機能自体を停止するため、すべてのデータの持ち出し操作を排除する。

② ネットワーク制御型
メールやWebなどのネットワークトラフィックを制御する。文字列でブラックリストやホワイトリストを指定することにより通信をフィルタリングする。

③ 統合型
ハードディスクやネットワーク通信の内容から機密情報を識別し、デバイス制御、ネットワーク制御などによって機密情報の持ち出しを制御する。

④ 著作権保護型
データの持ち出し先でも閲覧期限、閲覧可能者、複製可否などを制御する。いわゆるDRM（Digital Rights Management）製品として提供されている。

これらの中で、保管されたデータの中から機密情報を検出する棚卸し機能を提供するのは、統合型のみである。以下では統合型のひとつであるSymantec Data Loss Prevention（以下、Data Loss Prevention は DLPと表記する）を取り上げ、Symantec DLPを使った情報漏洩対策管理の実現方法を考察する。

なお、情報漏洩対策管理をはじめるための前提条件である「機密情報の条件および機密区分の定義」については、組織の方針としてあらかじめ規定されているものと想定する。

3.2. Symantec DLPによる棚卸し

膨大な数の電子データを対象として機密情報の棚卸しをおこなうためには、ITツールの活用が有効である。ただし、ITツールを活用するには、機密区分を識別するための判断基準の整備と、対象データの内容を検索できるアクセス権限をITツールに付与することが必要となる。

3.2.1. 検索対象

機密情報が電子的に保管、伝送される場所は、パソコン、サーバ、ネットワークの３ヶ所になる。

① パソコン
ハードディスクを検索して機密情報の保管状況を確認する。パソコンに導入するDLPエージェントに検索処理を実行させるため、全データを対象とした参照権限をDLPエージェントに付与する必要がある。

② サーバ
Symantec DLPが情報利用者としてサーバ内のデータを検索し、機密情報の保管状況を確認する。

機密情報を格納するサーバとしては、ファイルサーバ、グループウェアサーバ、DBサーバなどがあり、それぞれ認証、認可プロセスが異なるため、それらサーバのクライアントとなるSymantec DLPに対して、それぞれに必要な参照権限を付与する必要がある。

一般権限によるアクセスが可能な場所で機密情報を検出した場合、セキュリティインシデントとして捉えることになる。

③ ネットワーク
通信内容に機密情報が含まれているかどうかを検査し、機密情報の送信有無を確認する。

すべての通信内容を検査するために、ネットワークスイッチのポートミラーリングの設定が必要になる。Symantec DLPサーバをポートミラーリング先に接続し、外部とのすべての通信内容を検査する。

3.2.2. 文書検索技術

Symantec DLPの文書検索機能に機密区分の定義を指定することで、機密情報の棚卸しを機械的におこなうことが可能である。

文書検索機能を大別すると次の３種類になる。

- キーワード検索
- 登録表要素一致検索
- 登録文書類似性検索

① キーワード検索

Symantec DLPのキーワード検索機能は、指定文字列検索や正規表現検索、固定フォーマット文字列形式の検索ができる。

指定文字列検索の例としては、「厳秘」、「機密」「社外秘」といった文字列を検索キーワードとして対象データを検索し、当該文字列を含むデータを機密情報として棚卸しすることができる。前方一致や後方一致など特定の文字パターンなどを検知したい場合には、正規表現による検索キーワード指定も可能である。

固定フォーマット文字列形式の例としてはクレジットカード番号や、クレジットカード背面の磁気ストライプ情報などが挙げられる。Symantec DLPは、14桁から16桁の

数字がクレジットカードに該当するかどうかを識別することができる。

また、クレジットカード背面の磁気ストライプに記載されているセンシティブ認証データも同様に識別可能である。

PCI-DSSの定義[2)]では、クレジットカード番号を保存、処理、または送信する事業者にPCI-DSSが適用されることになっている。また、磁気ストライプ情報を含むセンシティブ認証データを保管することは禁止されている。

Symantec DLPの検索機能によってクレジットカード情報の不適切な保管状況を確認できるため、クレジットカードを取り扱う事業者にとって本機能は非常に有効である。

クレジットカード関連以外にも、IPアドレスやSWIFTコード（金融機関識別コード）などを検出することができる。

②　登録表要素一致検索

事前にSymantec DLPに登録した表形式のデータをマスターとして、パソコンなどに保管されている検索対象データの中に含まれる文字列が、どの程度マスターに一致しているかを評価する検索機能である。

この機能の典型的な利用シーンのひとつは、個人情報の棚卸しである。一人分を１行で記述した表形式の個人情報マスターをSymantec DLPに登録し、検索条件として個人情報マスターと合致するレコード数、項目数、項目値などの組み合わせを指定する。具体的な例としては、「一人につき３項目以上で２人分以上を含むデータ」といった内容を検知することが可能である。検索対象の文書は表形式である必要はなく、検索対象データ内に含まれる文字列が、指定した条件に合致するかどうかを評価する。

個人情報漏洩関連の報道では、漏洩件数が注目されやすいが、個人情報取扱事業者としては、たとえ一人分であっても外部に漏洩しないよう、個人情報を適切に保護しなければならない。このため、不適切な場所に個人情報を保持していないかどうかを検知することが重要となる。

③　登録文書類似性検索

事前にSymantec DLPに登録した文書ファイルをマスターとして、検索対象文書がどの程度マスターと一致しているかを評価する検索方式である。

事前登録する文書データは、契約書、履歴書、設計書、プログラムソースなどであり、MS-Officeをはじめ、PDF、XML、HTMLなど多種多様なファイル形式をサポートしている。

利用シーンとして契約書ファイルの棚卸しを考えてみる。契約書作成時の組織運用ルールとして、内部公開された契約書テンプレートをベースに個別の契約書が作成されている場合を想定する。

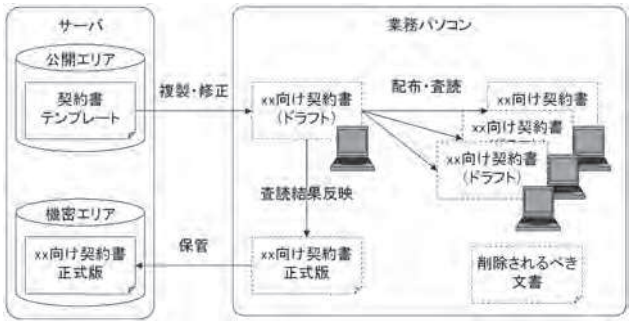

図４　テンプレート利用と査読で複製される例

契約書テンプレートを個別契約のために修正した後の文書は関係者外秘となり、文書へのアクセスが契約関係者のみに制限される。

個別契約に向けたテンプレートの修正過程で複数人による査読が繰り返されると、ドラフト版の個別契約書が複数のパソコンに保管される。個別契約書の完成時点で、これらのドラフト版をすべて消去し、完成版原本のみが適切なアクセス制御定義とともに機密管理対象サーバに保管されるべきである。

しかし、ドラフト版の消去は個人用業務パソコンに対する属人的作業となるため、タイムリーな消去実施と他者による消去作業の完了確認をおこなうことは困難である。このようなケースで登録文書類似性検索が活躍する。

仮に契約書テンプレートの２割程度を修正することで完成版となる場合、Symantec DLPはテンプレートをマスターとして一致率８割の文書は個別契約書であると判定することができる。

個人用業務パソコンに対して一致率８割以上の文書を検索することで、ドラフト版の消去漏れや完成版原本の不正な複製を検出することが可能になる。

3.2.3.　機密情報の検索条件展開

前節までに説明したSymantec DLPの文書検索技術を組み合わせることで、組織の機密情報をもれなく検出できればよいが、検出結果は検索条件の設定内容に依存している。機密区分の定義内容は組織によって異なるため、機密情報の検索条件も組織ごとに異なる。また、事業構造の変化や

法規制の改定など、状況の変化によって機密情報の条件が変わる場合も考えられる。したがって組織にとって適切な検索条件を維持するためには、継続的な維持管理が必須となる。

特に機密情報棚卸しの初期段階は、検索条件の設定と検出結果の評価を頻繁に繰り返しながら、検出精度の向上を図るフェーズである。検出精度が高いということは、検出件数に占める過検出（False-Positive）と検出漏れ（False-Negative）の割合が低いということである。

検索対象データ数が少ない環境では検出精度の高い検索条件を見つけやすいが、検索範囲を広げると検索条件に合わないデータが増えるため検出漏れが発生しやすく、検出精度は低下する傾向がある。検出漏れ対策のために検索条件を緩くすると過検出の原因になる。

過検出や検出漏れがまったく発生しない検索条件を見つけ出すことは困難なので、許容できる検出率を想定し、これを達成できる検索条件を見つけるアプローチが現実的となる。例としては、あらかじめ内容を把握したデータ/データ群を用意し、これに対する検出条件の設定と検出結果の評価を繰り返すことで、想定する検出率を実現する検出条件を見出す方法がある。

検索対象とする機密情報に優先順をつけると、重要な情報を早期に検出しやすくなるため効率的である。漏洩時の影響度が高く、広範囲に分散配置されている可能性のある情報から優先的に対応することが望ましい。

3.3. Symantec DLPによるアクセス制御

棚卸しによって機密情報の所在が判明したら、不適切な状況に対するアクションを決定する。そのための検討テーマとして次のような項目が考えられる。

- なぜそこにあるのか
- そこにあって漏洩することはないのか
- 安全な管理のために何をするのか

これらを検討することで、どのようなアクセス制御が必要か判明する。例えば、

① なぜそこにあるのか
　情報利用者が名刺から作成した顧客情報リストが業務用パソコンに保管されていた。

② そこにあって漏洩することはないのか
　業務用パソコンからのメール送信、Web送信、USBメモリへのコピー、印刷などによる情報漏洩の可能性がある。また、業務用パソコンが盗まれた場合も同様に情報漏洩の可能性がある。

③ 安全な管理のために何をするのか
　対象データをパスワード設定や暗号化で保護するか、しかるべきアクセス制御設定が可能な機密保持サーバへ移動する。メール添付などのネットワーク送信や外部記憶装置への複製、印刷などの操作を禁止する。パソコン内の保管が不要なら業務用パソコンから安全に削除する。

③で検討した対策の多くは、Symantec DLPが提供するアクセス制御機能によって実現可能である。

Symantec DLPは、機密情報に対して次のようなアクセス制御機能を提供している。

- 対サーバ
  - a　機密情報の検疫（別エリアへの隔離）やコピー
  - b　隔離したことを示す痕跡としてテキストファイルを作成
- 対ネットワーク
  - c　機密情報を含む電子メール送信の遮断/SMTPメッセージの修正（機密情報の除去）
  - d　機密情報を含むhttp(s)送信の遮断/コンテンツの削除（機密情報の除去）
  - e　ftp要求の遮断
- 対パソコン
  - f　機密情報の検疫
  - g　隔離したことを示す痕跡としてテキストファイルを作成
  - h　リムーバブルメディア/CD/DVD//印刷/クリップボード/ネットワーク共有への持ち出しの遮断

Symantec DLPのアクセス制御機能は、棚卸しによる機密情報の検出や情報利用者の操作要求発生時に機能する。

3.4. Symantec DLPによるログ管理

ユーザからの操作要求内容を記録したアクセスログは、一般的に監査証跡として活用される。

アクセスログに記録される典型的な情報は、アクセス日時、ユーザID、操作要求内容、操作結果、システムメッセージなどである。アクセスログに操作したファイル名を記録することはあっても、データの中身まで記録するケースはほとんどない。しかし、「ついうっかり」で組織に巨

大な損害をもたらしかねない機密情報については、データの中身を含んだログを保管するべきである。情報漏洩インシデントが発生した際に、漏洩した具体的な内容がわかれば影響や原因を分析しやすくなるため、迅速に説明責任を果たすことができる。また、具体的な記録は、再発防止策の検討時に非常に有用となる。

Symantec DLPは機密情報の不適切な保管や不正操作を検知すると、その内容を「インシデントログ」として記録する。インシデントログを構成する主な項目は以下のとおりである。

- 日時
- 操作対象の所在と名前
- 操作対象データ内容
- 操作者
- インシデントステータス（発生～完了）履歴
- メモ（インシデント管理者の手入力）

「操作対象データ内容」に機密情報のデータ内容が記録される。

「メモ」にはテキストを自由記入できるため、どの機密情報に対する、どのようなインシデントを、どのように終息させたかを記録するとよい。これはアクセス制御の自動化方針検討や、DLPポリシーの改善検討などで実績情報として活用される。新任セキュリティ担当者への引継ぎ、育成資料としても利用できる。

Symantec DLPはインシデント情報をデータベースに保管するため、さまざまな切り口でのインシデントレポートが作成可能である。

インシデントログのデータ量は、DLPポリシーの精度やインシデント発生頻度、機密情報データ容量などに左右される。資源上の制約でデータベースから削除する場合でも、エクスポートデータを所定の期間、保管しておくべきである。

3.5. DLPポリシー展開のベストプラクティス

DLPポリシーは、機密情報の検索条件と、機密情報検出時の応答ルール（実施するアクセス制御機能）を組み合わせたものである。応答ルールはアクセス制御機能を使用して操作拒否を発動することができるため、業務上必要な作業を停止させるようなことがないよう、慎重に設定する必要がある。このためにも検索条件の精度向上が必須となる。これらを踏まえ、DLPポリシーの展開プロセスは以下のステップで進めるとよい。

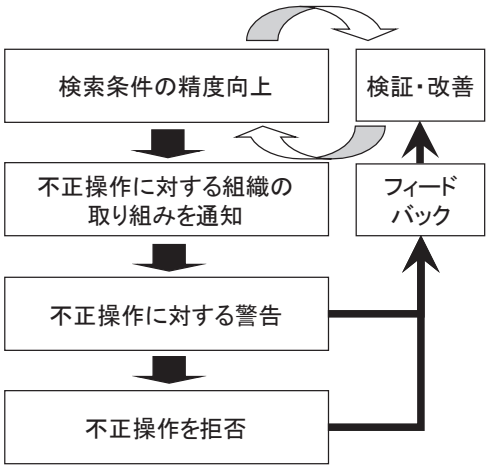

図５　DLPポリシーの展開プロセス

①　検索条件の精度向上

精度が高い検索条件を獲得するためには、検証を繰り返す必要がある。最初は検索場所を絞り、検出結果に応じて検索条件を改善する。検索条件の精度がある程度向上したら検索場所を徐々に拡大し、さらなる検索条件の改善を図る。検索条件を改善するプロセスの中で、機密情報が不適切な場所に保管されていることを検出できるため、アクセス制御方針の検討材料として利用する。

検索条件の精度が一定の水準に達し、過検出や検出漏れが許容範囲になったら、アクセス制御の実装計画を検討する。

②　不正操作に対する組織の取り組み通知

Symantec DLPのアクセス制御機能を実装すると、情報利用者のデータ操作を拒否するなど作業効率に影響を与えるため、業務上の混乱や個人的な不満の原因となる。このため、組織の上位層から情報利用者に向けてあらかじめ機密情報の取り扱いに関する目的やルールなどを通知し、認識を共有しておくことが望ましい。

③　不正操作に対する警告

アクセス制御実装の初期段階における応答ルールは、業務の混乱を避けるためにも、警告画面の表示程度にとどめておくとよい。機密情報操作に対する警告画面が表示されるだけでも、情報利用者は情報漏洩に対する意識を高めるとともに、操作内容が監視されていることを認識するため、悪意による不正操作の抑止力にもなる。

警告内容はすべてインシデントログに記録されるため、対象データの種類や発生件数、頻度、場所、情報利用者などの情報を収集できる。そこから傾向や特徴を分析し、必

要な応答ルールを設計する。

④　機密情報の不正操作を拒否

機密情報に対するアクセス制御の最終局面では、不正操作の自動拒否を実装する。拒否の内容は機密区分や情報の種類により異なるため、応答ルールのタイプは多岐にわたる。例えば、ネットワーク送信は不可だが印刷は許可する、あるいは、あて先を限定したメール送信を許可する、などのバリエーションが考えられる。

これらのステップを経てSymantec DLPのアクセス制御機能で自動拒否を実装すると、不正な情報持ち出し操作のほとんどを防止できるようになる。

4. 運用による情報漏洩対策

３章では機密情報管理の検討ポイントに対応するSymantec DLPの機能を説明した。本章では、この機能を効率的に活用するための運用方法を検討する。

4.1. 情報利用者教育

機密情報の条件や機密区分を定義して公開し、研修で教えても情報漏洩インシデントは発生する。教わったことを全員がすべて修得し、機密情報を常に適切に取り扱い続けることは困難だからである。

情報利用者に対して機密情報を操作していることをタイムリーに指摘し続ければ、機密情報に対する知識が深まると同時に意識が高まる。Symantec DLPは情報利用者が機密情報を操作していることをポップアップ画面で指摘するとともに、その操作内容を上司またはセキュリティ管理者にDLPインシデントの発生としてメールで通知することもできる。

パソコンからの警告、上司または管理者からのインタビューや叱責を経験すると、同じ目に遭わないために情報利用者自身が工夫するようになる。

4.2. インシデント対応チームの設置

Symantec DLPはインシデントの発生をメールで通知するだけでなく、インシデントログとしてデータベースに保管する。インシデントログは組織別、重要度別、インシデントタイプ別など、さまざまな切り口でDLP管理コンソールに表示され、CSV形式によるパソコンへのダウンロードも可能である。したがって、いつどこで何が起きたのかをいつでも知ることができる。

インシデントが発生した場合、対症療法的な対策でなく、再発防止策として有効な対策を講じるべきである。

この役割を担う組織として、インシデント対応チームを設置することが望ましい。インシデント対応チームの構成と登場人物の役割の例を以下に示す。

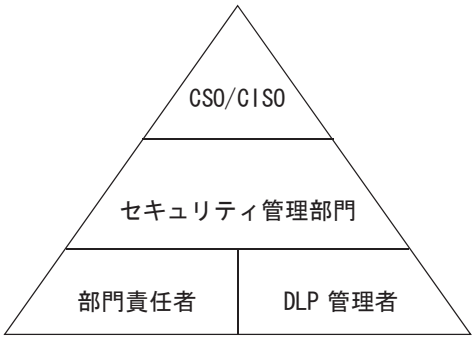

図６　インシデント対応チーム構成の例

① CSO/CISO：セキュリティポリシー策定、機密情報の条件、機密区分の定義、組織内通達
② セキュリティ管理部門：DLPポリシーの策定とインシデント管理
③ 各部門管理者：個別インシデントに対する原因調査、再発防止策の検討と実施、部門情報利用者の育成と啓蒙
④ DLP管理者：DLPポリシーの実装、発生したインシデントの傾向分析とレポート作成

4.3. インシデント対応フローの例

Symantec DLPが発行するインシデント通知メールにはインシデントログの参照URLが含まれており、そのURLをクリックするだけでDLP管理コンソールから、いつ、誰が、どんな機密情報を、どのように操作しようとしたかをすぐに調査することができる。

インシデント内容を把握した後は、インシデント発生の根本原因をつきとめる必要がある。

根本原因は大きく２種類に分類できる。ひとつは情報利用者のうっかりまたは悪意、もうひとつはDLPポリシーの不備である。

前者の場合、アクセス制御機能によって不正操作が拒否されていれば情報漏洩を防止できているので、システム的な対応ではなく、利用者に対する機密情報管理の指導・啓蒙などが必要となる。作業が監視され、不正操作が摘発される可能性を情報利用者に認識させることは、セキュリティ意識向上の一助となる。

アクセス制御を設定せず、警告モードの場合は機密情報が不正に持ち出された可能性があるので、原因調査の上、必要に応じてアクセス制御を設定する。

後者の場合はDLPポリシーの精度に原因があるので、DLPポリシーの改善が必要である。例えば、一部の情報利用者が一時的な権限委譲や特命任務を受ける場合、業務上必要なデータ操作であるにもかかわらず、不正操作と判定されてしまうケースなどが該当する。このような場合はDLPポリシーに例外条件を設定する。すなわち、権限委譲または特命を受けた情報利用者を個別に指定して持ち出し操作を許可する。この例外条件設定によりDLPポリシーが改善される。

DLPポリシーの改善要否にかかわらず、各インシデントに対して実施した対策を記録することは非常に重要である。Symantec DLPは個別のインシデントログにメモを作成できるので、そこに実施された対策を記録しておき、類似インシデントに対する対策の迅速化や、傾向分析によるDLPポリシーの改善などに役立てることができる。

インシデント発生から対策完了までのフローには、複数の関係者が関与することが一般的である。基本的には以下のようなモデルになる。

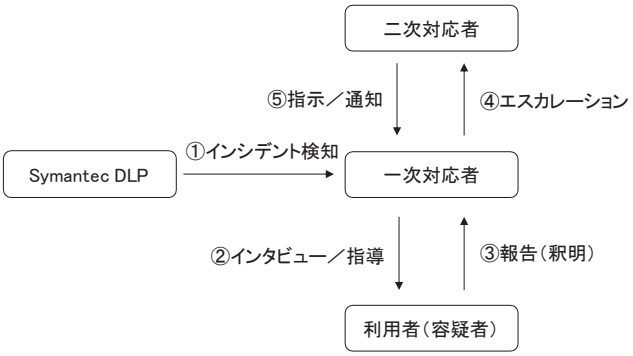

図７　インシデント対応概略フロー

a　一次対応者

インシデントを検知して必要な対策を講じる。インシデントの内容や影響が深刻なケース、対応に専門知識が必要なケースなど、一次対応者のみでインシデント対応を完結しきれない場合は、二次対応者にエスカレーションをおこなう。

b　二次対応者

一次対応者からのエスカレーションを受けて、必要な対策を講じる。主な役割はインシデント対応に関する判断や意思決定である。

エスカレーションモデルは一極集中対応型と部門別分散対応型に分類できる。

●　一極集中対応型

発生したすべてのインシデントについて、一次対応をセキュリティ管理部門が少人数で担うモデルである。インシデント全体の情報が一ヶ所に集約されるため、傾向分析や対策検討に一貫した方針を適用しやすい。このため、DLPシステム導入初期に適したモデルといえる。

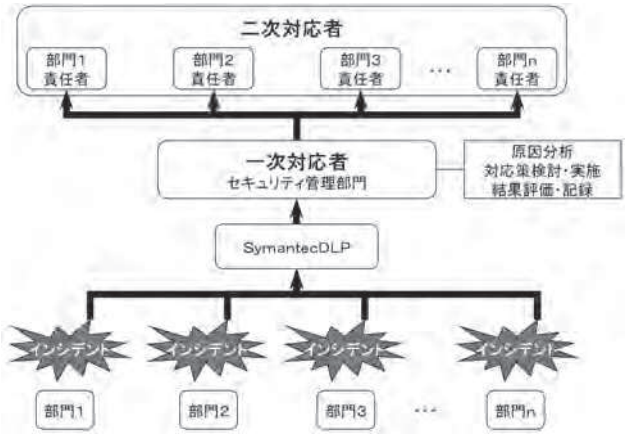

図８　一極集中対応型

●　部門別分散対応型

情報利用者が所属する各部門が、自部門で発生したインシデントの一次対応を担うモデルである。

DLP適用対象を拡大すると、インシデント数の増大や発生場所が地理的に分散されることになる。少人数での集中対応ではインシデント対応チームの負荷が増大するとともに、迅速性が失われる。このため、情報利用者の所属部門にインシデント対応を移管し、セキュリティ管理部門では統計分析や個別事案のアドバイスなどの役割を担う。

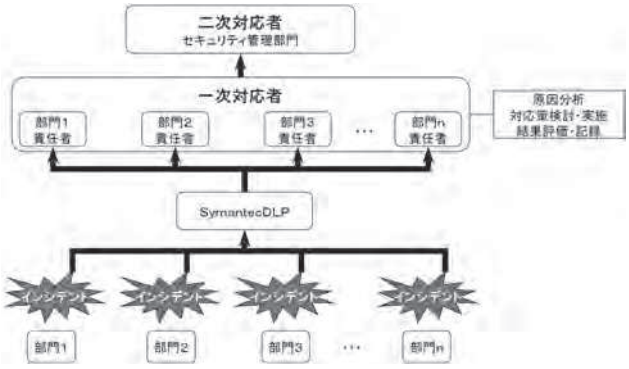

図９　部門別分散対応型

4.4. DLPポリシーのPDCA

DLPポリシーは一度設定したらおわりではなく、繰り返して見直すことで、組織の現状にさらに適合するよう維持・管理しなければならない。このため、定期的な見直し計画の策定や、必要に応じた臨時見直しが欠かせない。

アクセス制御機能の実装によって、データの取り扱いを自動的に制御することが可能となるが、人事異動や組織改正によるアクセス権限付与対象の見直しや、市場の多様化、法規制の制定・改正などの環境変化によって、アクセス制御内容の見直しが必要となる。また、インシデントの原因分析から、DLPポリシーと日常業務との乖離が発覚し、DLPポリシーを見直すことも考えられる。

5. おわりに

人はミスを犯すし勘違いもする。つまり、注意していてもうっかりミスを完全に排除することはできない。そして、コンピュータやネットワーク技術の発展により、「うっかり」が組織に巨大な損失を与えるケースが生じている。

「うっかり」を完全に排除するためには、定められた操作以外をまったく不可能にできればよいだろう。だが、強い制限や制約は、効率化のアイデアや臨機応変な対応力など、ビジネスの現場で不可欠な人の創意工夫をつぶしてしまいかねない。

とはいえ業務効率に影響を与えないで情報漏洩を完璧に防止できる対策は、残念ながら現状では存在しない。したがって、情報漏洩リスクを低減するためには、リスクと利便性のトレードオフを図りながら継続的な工夫と努力が欠かせない。

セキュリティポリシーのPDCAサイクル実現と情報利用者の意識・知識向上を図りつつ、うっかり抑止策の道具としてITを利用することが有効である。本稿で示したSymantec DLPの機能は意識・知識向上とうっかり抑止の両方に効果をもたらすことができる。

「3.1. 情報漏洩対策製品の分類」で述べたとおり、情報漏洩対策を標榜するITツールが数多くリリースされ、自組織の要件に応じて各種ツールを選択することができる。ただし、バンドエイドのように対症療法的な製品導入を繰り返すと根本原因を解消しないまま部分最適のシステムが乱立し、運用が複雑化するなど全体最適にならない。

全体最適を考えるためにも、情報漏洩対策の専門家を抱えるパートナー選びが重要になる。プランニングから導入・展開のサポートを含めてPDCA全体をカバーできるパートナーを選び、原因療法的アプローチを取ることが、最適な投資対効果を得るために必要となる。

当社はSymantecDLPの取扱いを開始した2011年に、シマンテック社のDLPスペシャリゼーション資格を取得し、現在はプラチナパートナーの認定を受けている。優れた技術を実装した製品を道具としながら、当社の知識と経験をフル稼働して、お客様のセキュリティレベル向上のお役に立てるよう活動を継続していく所存である。

参考文献

1)　日本ネットワークセキュリティ協会,”2010年情報セキュリティインシデントに関する調査報告書　～個人情報漏洩編～” p.12

2)　“Payment Card Industry(PCI)データセキュリティ基準 要件とセキュリティ評価手順 バージョン2.0”　p.7
