2011.6.3

情報セキュリティニュース<2011 No.1>

いま見直すべきソフトウェア資産管理

ソフトウェア資産管理とは

今日では企業など多くの組織がITを幅広く活用しており、業務の効率化や付加価値の向上など様々なメリットを享受している。ITの活用にあたっては、必要なソフトウェアを、制作者の権利を侵さず、適法に、かつ効果的に利用することが求められる。ここで、様々なソフトウェア資産を、その入手から利用、廃棄にいたるまで、適切に管理するための活動を総称して、ソフトウェア資産管理（SAM：Software Asset Management、以下、SAMと略記する）と言う。一般に「ソフトウェア」には、画像や映像、音声、辞書など、コンピュータ等で実行されることを前提としないものも広く含まれる（後述の国際規格ISO/IEC 19770-1でもこれらを対象に含んでいる）が、本稿では話題の拡散を防ぐために、主にコンピュータ等で実行されるソフトウェアを中心に取り扱う。

ソフトウェア資産の管理にあたって、具体的には購入から廃棄までの各ステージにおいて、次のような管理プロセスが必要になるであろう。

(1) 購入

所定の手続きに沿ってソフトウェアを購入する。購入手続きの中で、そのソフトウェアを購入する妥当性ついての確認・承認や、購入済みで余剰のソフトウェアが無いかどうかの確認を行い、納品されたソフトウェアは所定の場所に保管する。なお、組織で使用するソフトウェアの種類が増えると、管理やユーザーサポートが煩雑になったり、ソフトウェア購入コストが非効率になる等の弊害があるので、組織で使用するソフトウェア標準を定め、これに適合しないソフトウェアの購入を制限するという方法も広く実施されている。

(2) 導入・インストール

使用するバージョンに動作上の問題やデータ互換性等の不都合がないかテストを行い、問題がなければインストールおよび環境設定を実施して使用可能な状態にする。

(3) 利用状況の管理

各ソフトウェアの購入状況や利用状況を把握するためのデータベース（以下、本稿では「管理台帳」と呼ぶ）を作成し、維持する。ソフトウェアの購入／廃棄、インストール／アンインストール（削除）、使用者や使用部署の変更等が発生した場合には、遅滞なく管理台帳を更新する。また、ソフトウェアが使用されている台数やユーザー数が、購入済みのライセンスの範囲に収まっているか確認し、もしライセンスの範囲を超えそうな（もしくは既に超えてしまった）場合にはライセンスの追加購入や使用数の削減等の対処を行う。

(4) 廃棄

使用しなくなったソフトウェアを廃棄する。ハードウェアの廃棄に伴ってソフトウェアも廃棄される場合もあれば、ハードウェアは継続利用するのものソフトウェアのみアンインストールされる場合もある。アンインストールされたソフトウェアが他のユーザーもしくはハードウェアで使用可能なものであれば、将来の再活用のために管理台帳で確実に記録する。また、廃棄したソフトウェアが組織外部に流出し、悪用されることがないよう、確実に廃棄する。

これらは当然ながら、企業でコンピュータを使用し始めた初期の頃から何らかの形で行われているはずであるから、SAMは企業にとって決して新しい話題ではない。しかしながら、SAMに関する活動はここ数年の間に活発になってきている（表1）。

表 1 ソフトウェア資産管理に関する主な活動

時期	活動内容	実施組織
2006.5.1	ISO/IEC 19770-1 発行	国際標準化機構（ISO）
2007.11.27	『ソフトウェア資産管理基準 Ver.2.0』および『ソフトウェア資産管理評価基準 Ver.2.0』発行	特定非営利活動法人ソフトウェア資産管理コンソーシアム
2009.8	『ソフトウェア資産管理対策基準』発行	ビジネスソフトウェアアライアンス（BSA）
2010.2	「ソフトウェア資産管理」を主テーマの一つとして「情報セキュリティ総合的普及啓発シンポジウム」を開催	（財）情報処理開発協会（JIPDEC）(注釈 1)
2010.6.16	『SAM ユーザーズガイド』発行	JIPDEC
2010.11.11	ISO/IEC 19770-2 発行	国際標準化機構（ISO）
2011.1	「クラウド時代におけるソフトウェア資産管理の側面」を主テーマの一つとして「情報セキュリティ総合的普及啓発シンポジウム」を開催	JIPDEC

ソフトウェア資産管理に期待されるもの

SAM が適切に実施されることによって、どのようなメリットがあるのだろうか？また、適切に行われないことによって、どのようなリスクがあるのだろうか？後述の国際規格 ISO/IEC 19770-1 の序文では、SAM の主な便益（benefit）として次のようなものを挙げている。

a) リスクマネジメント：
   1) IT サービス中断リスクの低減
   2) IT サービスの品質低下リスクの低減
   3) 法律や規制に違反するリスクの低減
   4) 上のいずれかに起因して組織の対外的イメージが失墜するリスクの低減

b) コスト管理：
   1) ソフトウェアをまとめて大量購入することによる購入価格交渉、既存のライセンスの有効活用による新規購入の回避等による、コスト削減
   2) ソフトウェア管理にかかる事務処理の効率化によるコスト削減
   3) ユーザーサポートの効率化によるコスト削減

c) 競争上の優位性：
   1) IT 調達やシステム開発、導入等に関する意思決定の質の向上
   2) 事業のニーズにより合致した IT を提供することによる、エンドユーザーの業務の質の向上
   3) 企業の買収、合併、または分割時に IT 面の処理を迅速に行う
   4) IT に関する問題を減少させることによって、要員のモチベーションを高め、顧客満足度を向上させる

これらのうち特に a) の 3) については、組織による故意の違反は言うに及ばず、組織が把握していなかったために発生した、意図しないライセンス違反についても訴訟の対象となりうる。違反の規模によっては多額の損害賠償が発生するだけでなく、違反の事実が公知となることによって、組織のレピュテーションに重大な影響を与える可能性があり、既にそのような実例も発生している。

なお、あずさ監査法人が、日本国内の大手企業 (注釈 2) を対象として SAM の実態に関するアンケート調査を実施している (参考文献 2)。これによると、調査対象の 7 割の企業でソフトウェア資産管理体制が整備されており、またソフトウェア資産管理台帳の整備も実施されている。しかしながら SAM の効果については、「ソフトウェアライセンス違反の不安が払拭された」という項目に対して「強く感じる」

または「まあまあ感じる」と回答した企業の合計は63%に上るものの、「ソフトウェア購入費用を削減することができた」について同様に肯定的な回答をしたのは23%、「現場の管理負担が軽減され生産性が向上した」については16%にとどまっている。これは前述したSAMの便益のうち、リスクマネジメントという観点では導入効果が現れているのに対して、コスト管理面での効果がまだ現れていない、ということであり、リスクマネジメントのために追加コストがかかっている状態であると言える。

もちろんリスクマネジメントの面で効果があるだけでも、SAMに取り組む意義はあるが、運用にかかるコストが大きければ継続的な取り組みが困難になるし、やはり取り組むからにはコスト管理面のメリットも享受したいものである。

ソフトウェア資産管理に関するコスト削減のポイント

SAMの運用にかかるコストを削減するためには、標準化と定着化が鍵となる。標準化によって管理対象の種類を減らすことによって管理業務の削減を狙う。また、ユーザーの理解を得てSAMの運用を定着させることによって、例外対応やルール違反への対応を減らすことが期待できる。

過度な標準化は別の弊害を生むことが多いため、標準化の程度をどのくらいにするかは慎重に検討すべきだが、次のような観点で標準化を進めることで管理業務量を減らせる可能性がある。

(a) 使用するソフトウェアの標準化

ソフトウェアの種類（オペレーティングシステム、アプリケーション、等）や用途（文書作成、画像編集、データベース、等）ごとに、組織で統一的に使用するソフトウェアの製品およびバージョンを定め、それ以外のソフトウェアの使用を原則として認めないようにする。これによってソフトウェア資産の棚卸しがシンプルになるだけでなく、ソフトウェア購入の際にまとめ買いすることによって有利な価格で購入できる可能性がある。また、社内のデスクトップ環境が統一化されることで、システム開発における要件の単純化やユーザーサポートの円滑化といった副次的な効果も期待できる。

ただし、業務内容によっては標準ソフトウェアだけでは対応できないケースもあるため、標準外のソフトウェアを導入する際の手続きや承認権限などを決めておき、ユーザー側に過度の不都合が発生しないような配慮は必要である。

現実には、様々なソフトウェアが混在している状況から標準化に取り組み始めることになることが多いと思われるので、ハードウェアを設置（新規または入れ替え）する時やバージョンアップが必要な時期を狙って、少しずつ標準ソフトウェアに揃えていく。

(b) ソフトウェア導入プロセスの標準化

ある程度大きな組織になると、ソフトウェアの購入に関する事務手続きや、管理台帳のアップデートにかかる作業量が多くなる。また、各部署で個別にソフトウェアを購入すると、これが管理台帳に正しく反映されない場合があり、組織全体として所有しているライセンス数等が把握しにくくなる。まずソフトウェア購入は全て特定部署（例えば情報システム部門）を通して購入するようにし、購入のための申請・承認・発注手続きを決めることによって、ソフトウェアの入り口を一本化する。これにより事務手続きの種類が減少し作業量が軽減されると同時に、管理台帳のアップデート漏れも減る。組織全体としてソフトウェア購入にかかっている費用が分かりやすくなり、予算管理がしやすくなるというメリットもある。

またソフトウェアのインストール作業も手順を決め、インストール作業者が管理台帳のアップデートを行う（もしくは管理台帳の担当者に報告する）ところまで手順に含めてルーティンにしてしまう。クライアントPCを含めてシステムの運用をアウトソーシングしている場合は、受託業者との間でソフトウェア導入作業の仕様や手順を決めるときに、上のような観点を含めて確実に実施するよう依頼すればよい（このような標準化がしやすいのもアウトソーシングの利点であろう）。

また、上のような標準化を進めるのと並行して、SAMを組織内に定着させるための取り組みが必要

である。標準化によってルールを決めるだけでなく、そのルールを守ってもらうために、組織における SAM の必要性と、そのために標準化を進める必要性を説明し、理解を得なければならない。上のような標準化が進められたとしても、ルール違反（意図したものか否かにかかわらず）が多いと標準化がなかなか進まないし、ルールの個別説明や説得、事後処理（事務手続きやソフトウェアの削除等）に現場の労力が割かれることになる。

したがって、SAM は特定部門だけで取り組むものではなく、ユーザー部門の理解と協力が不可欠であり、組織全体で取り組むというスタンスで、組織内での説明や普及啓発に取り組むべきである。SAM の必要性という観点では、著作権の侵害やライセンス違反に関するコンプライアンス教育に重点を置くべきであろう。またルールを守ってもらうための説明については、エンドユーザーはもとより、物品購入の権限を持つ管理職に十分な理解を得て協力を依頼する必要がある。

関連するガイドライン

SAM に関する国際規格としては 2006 年に発行された ISO/IEC 19770-1 がある（参考文献 3）。ただし前述のあずさ監査法人の調査結果によると、この規格に対する認知度は低いようである。また財団法人 日本情報処理開発協会（注釈 1）（JIPDEC）からは『SAM ユーザーズガイド』（参考文献 4）が発行されており、同協会の Web サイトから無償でダウンロードできる。

上に上げたものは SAM を中心的に取り扱っているガイドラインであるが、SAM はもともと情報セキュリティへの取り組みの一環として進められてきたため、情報セキュリティに関する規格である ISO/IEC 27002（注釈 3）や、IT サービスマネジメントの規格である ISO/IEC 20000、さらには ITIL®（注釈 4）の中にも SAM に関連する記述が含まれている。ISO/IEC 27002 では「資産の管理」という項目が該当する。ここでは具体的な指針はあまり書かれていないが、情報セキュリティの一環として最低限取り組むべき SAM の要求・推奨事項が示されている。ISO/IEC 20000 では「構成管理」、ITIL® V3 では「サービストランジション」（参考文献 5）の中で「サービス資産管理および構成管理」というセクションが SAM に関連する。ここではソフトウェアに限らず、IT 関連のハードウェアなども含めて IT サービスの提供に必要な資産を包括的に管理することが推奨され、そのための指針が示されている。

今後の取り組み

このように SAM の実践には様々な課題があるものの、IT の活用によるメリットを最大限に享受しつつ、これに関わるリスクを最小限におさえるためには、SAM への取り組みを避けて通るわけにはいかない。適切な SAM の運用が、組織全体としてのコスト削減やライセンス違反に関するリスクの低減等に繋がることを考えれば、単に IT 部門や調達部門の業務としてでなく、組織全体の合理化・リスクマネジメントのテーマとしてとらえるべきであろう。

この紙面では紹介しきれないが、SAM に関しては様々な団体がそれぞれの立場で普及啓発活動を展開しており、参考資料やセミナー等も数多く提供されている。SAM に関するコンサルティングサービスやツールを提供している企業も多い。また、ソフトウェアベンダーにもユーザー組織の SAM への取り組みを積極的にサポートしようという姿勢が見られる。違法コピー行為の監査活動が活発に行われてきたこともあって、ソフトウェアベンダーが違法コピーを行ったユーザー企業を訴えるという関係が多いと思われるかも知れないが、一部の大手ソフトウェアベンダーは、ユーザーとの良好な関係を維持しつつ、様々な情報提供やツールの提供などを通して SAM への取り組みを後押しすることによって、ライセンス違反を減らしていくという施策を進めている（注釈 5）。このようなサービスも上手に利用しながら、全体最適を目指した SAM に取り組まれることを強くお勧めしたい。

以上

株式会社インターリスク総研
コンサルティング第二部 主任研究員 田代 邦幸
kuniyuki.tashiro@ms-ad-hd.com

［参考文献］
(1) 『ソフトウェア資産管理の基礎と実践』SAM の基礎と実践編集委員会 編著、財団法人 日本規格協会、2009 年 6 月
(2) 『ソフトウェア資産管理（SAM）サーベイ 2010』（http://www.kpmg.or.jp/resources/research/r_ba201007/01.html）あずさ監査法人、2010 年 7 月
(3) 『ISO/IEC 19770-1 Information technology --- Software asset management --- Part 1: Processes 英和対訳版』財団法人 日本規格協会、2007 年 1 月
(4) 『SAM ユーザーズガイド - 導入のための基礎 -』財団法人 日本情報処理開発協会 (注釈 1)、2010 年 6 月
(5) 『ITIL®サービストランジション』特定非営利活動法人 itSMF Japan、2008 年 6 月
(6) 『ソフトウェア資産管理及び IT サービス継続管理に関する国際動向調査研究報告書』財団法人日本情報処理開発協会 (注釈 1)、2011 年 3 月
(7) 『詳解 ISO/IEC 17799 情報セキュリティマネジメントの実践のための規範』中尾康二、中野初美、平野芳行、吉田健一郎 共著、財団法人 日本規格協会、2007 年 3 月
(8) 『対訳 ISO/IEC 2000-1 2000-2 情報技術 - サービスマネジメントの国際規格』財団法人 日本規格協会、2007 年 12 月

［注釈］
(1) 財団法人 情報処理開発協会は 2011 年 4 月に「一般財団法人 日本情報経済社会推進協会」に改称している。
(2) この調査では、上場企業および売上高 500 億円以上の未上場企業を調査対象としている。
(3) ISO/IEC 17799:2005 が 2007 年に改称されて ISO/IEC 27002:2005 となった。
(4) IT Infrastructure Library の略で、IT サービスマネジメントに関するガイドラインである。ITIL®は英国商務局が所有しており、商標登録されている。ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.
(5) 例えば日本マイクロソフト（株）（http://www.microsoft.com/japan/resources/sam/）、アドビシステムズ（株）（http://www.adobe.com/jp/elicensing/licensemanagement/sam/）などがある。

株式会社インターリスク総研は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
弊社では情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研　コンサルティング第二部　BCM第一グループ
TEL.03-5296-8918　http://www.irric.co.jp/