



**SAM
World
2015**

ソフトウェア資産管理のすべてがここにある

SAMACユーザーフォーラム1

不適切なSAMがもたらすリスク

～ユーザーがお伝えするリスクとその対策～

Sky株式会社
ソフトバンクモバイル株式会社
山梨県庁

公認SAMコンサルタント：片貝和人（兼松エレクトロニクス株式会社）・西原優子（株式会社日立システムズ）

はじめに

SAMの導入に当たっては、導入することによって生じるメリットが議論されることが多く、それが明確にできないが故に、組織の経営に承認されにくいことが多い。

しかしながら本来、SAM導入のメリットとは、適切に導入し運用していない状況がもたらすリスクを軽減するという「リスクコントロール」のための重要施策の一つである。したがって、軽減される前のリスクを正確に認知するところからSAMの導入をスタートする必要がある。

不適切なSAMがもたらすリスクとは、単にソフトウェアライセンスの不適切な利用（ライセンスコンプライアンス違反）だけではなく、情報セキュリティやIT運用管理コストにまで影響を及ぼす幅広いものである。

本セッションでは、実際にSAMを導入している組織が洗い出した不適切なSAMがもたらすリスクについて具体的に紹介する。

これからSAMに取り組もうとする組織、あるいはSAMのさらなる有効的な運用化を検討している組織の担当者の方々への一助になれば幸いである。

AGENDA

1. 不適切なSAMがもたらすリスク
2. ライセンスコンプライアンスリスク
3. 情報セキュリティリスク
4. ITコストリスク
5. リスク発生要因と防止策（まとめ）
6. SAMの未導入のリスクと導入後のメリット
7. 総括

1.不適切なSAMがもたらすリスク

不適切なSAMがもたらすリスク（抜粋）①

リスク	管理不備項目		
	ハードウェア	ソフトウェア	ライセンス
1.ライセンスコンプライアンス違反（損害賠償）	○	○	○
2.情報漏えいに関するリスク	○		
1) PCの紛失、盗難による情報漏えい	○		
2) 情報漏えいに関するリスク （不適切なソフトウェアの利用による情報漏えい）		○	
3) 必要なソフトウェアが導入されていない （暗号化がされていない（されていないことがわからない））	○	○	
3.余計なコスト	○		
1) 遊休のハード資産があるが、新規購入	○		
2) リース機の利用状況がわからないために発生する延長契約	○		
3) 過剰なライセンス契約 （過剰なエディション、過剰なライセンス数）		○	○
4) 過剰な利用数（使用していないがインストールされているなど）	○	○	
5) リース、レンタル機の紛失などの損金 （紛失したときに早く見つける、無いなら早期解約して紛失の損金処理をする）	○		
6) ハードが無くなった（盗難？紛失？）時の調査　【緊急調査費用】	○		

不適切なSAMがもたらすリスク（抜粋）②

リスク	管理不備項目		
	ハードウェア	ソフトウェア	ライセンス
4.コストの可視化ができていない	○	○	○
5.有事の際の取引先からの信用の低下	○	○	○
6. PCの可用性低下 1) ウィルス感染	○	○	
2) 故障時の対応（保守状況の確認、同条件のPCの準備など）	○	○	
7.ライセンスの可用性 1) 想定外のサポート費用	○	○	○
2) キーやメディアがない			○
8.会社の業態変化に追従できない	○	○	
9.脆弱性対策の徹底ができない （PC単体だけでなく接続されているNW全体への影響もある）	○	○	
10.システム更新時の確認作業コストがかかる（バージョンや台数の調査費用）	○	○	○
11.社員がゲームなどをしてしまう、業務外のWeb閲覧		○	

リスクが顕在化する具体例

2. ライセンスコンプライアンスリスク

ハードウェアの不適切な管理がもたらすライセンス違反

- ・ 部門で個別調達しているハードウェアで利用されているソフトウェアを把握していないことで発生する
- ・ 廃棄・返却予定で保管しているハードウェアをフォーマットしていないことで発生する



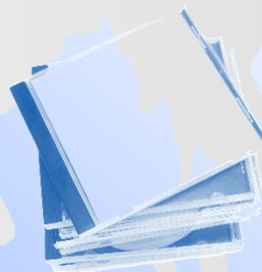
ソフトウェアの利用者の不適切な管理がもたらす ライセンス違反

- 部門のライセンスでインストールしたソフトウェアをアンインストールせずに異動することで発生する
- インストール媒体の貸出管理が適切になされないことで発生する
- ユーザーライセンスで割り当てられているソフトウェアを特定せずにインストールしていることで発生する



使用許諾条件の軽視がもたらすライセンス違反

- ・ ライセンスされているエディションを確認せずにインストールすることで発生する
- ・ プリインストールソフトウェアで複製展開用マスターを作成したときに発生する
- ・ 同じソフトウェア・エディション・バージョンのメディアを使い回すことで発生する



ライセンスコンプライアンス違反がもたらすリスク

- 多額の損害賠償
 - 不足額の1.5倍の賠償額 + 対応コスト
- ライセンス監査への対応コスト
 - 全社的な調査対応コスト + 弁護士費用 + 専門家委託費用
- コンプライアンス違反に対するレピュテーションリスク



ライセンスコンプライアンスリスクが顕在化する具体例

【リスクの要因例】

管理外ハードウェアの存在

廃棄・返却手続の不備

人事異動時の手続の不備

インストールメディアの誤使用

使用許諾条件の確認ミス



【リスク発生の防止策例】

＜組織に整合したルールの制定＞

- ・ SAMの方針と体制の策定
- ・ 管理規程・手順の策定 など

＜仕組みの構築＞

- ・ ルールに反した状況の把握
- ・ 管理の証跡の記録 など

＜検証・改善＞

- ・ 点検、棚卸、監査
- ・ ルールや仕組みの評価、見直し など

リスクが顕在化する具体例

3. 情報セキュリティリスク

不適切なソフトウェアの利用による情報漏えい

- 組織内のPCに、どのようなソフトウェアがインストールされているか分からない場合に発生する
- 不適切なソフトウェアの利用により、インターネット接続時にWeb閲覧履歴やPCの情報などが外部に送信されてしまう場合に発生する
- 特定のソフトウェアの対策をしても、新たなソフトウェアへの対応が後手になる場合に発生する



PCの紛失や盗難による情報漏えい

- ハードディスクやファイルの暗号化を実施していない場合に発生する
- 適切なパスワードを設定していない場合に発生する
- パスワードを設定していても、PCに付箋等でパスワード文字列を貼付していた場合に発生する
- 悪意をもった自社もしくは業務委託スタッフによって持ち帰られた（盗難された）場合に発生する



外部媒体の不適切な利用による情報漏えい

- 社員がUSBメモリーなどの媒体を利用して、組織の情報を持ち歩く場合に発生する
- PDAなどの機器をPCにUSB接続した場合に発生する
- NASや外付けHDDなどを適切に管理していない場合に発生する
- USBメモリーなどの媒体の所有者・利用者や、格納されているデータの管理が適切に行われていない場合に発生する

組織のセキュリティレベルの低下

- メーカーサポートが終了しているソフトウェアを利用している場合に発生する
- 適切なパッチが適用されていない（適用されているか分からない）場合に発生する
- 脆弱性の高いソフトウェアを利用している場合に発生する



ウィルス対策の不備がもたらす脅威

- 保有しているすべてのPCが把握できていない場合に発生する
- ウィルス対策の実施状況を把握していても、運用体制や利用者をフォローする体制がない場合に発生する



対策やルールの検証不備がもたらすリスク

- 管理ルールを定めているものの、ルールの順守状況の検証や管理が不備・不十分な場合に発生する
- 単純に規程の雛形を適用するなど、実態にそぐわないルールを制定した場合には、実効性が伴わず、結果として管理不備が発生する



情報セキュリティリスクが顕在化する具体例

【リスクの要因例】

不適切なソフトウェアの利用

ハードウェアの紛失

外部媒体の不適切な利用

ウィルス感染

ルールに反する行為



【リスク発生の防止策例】

＜組織に整合したルールの制定＞

- ・ SAMの方針と体制の策定
- ・ 管理規程・手順の策定 など

＜仕組みの構築＞

- ・ ルールに反した状況の把握
- ・ 管理の証跡の記録 など

＜検証・改善＞

- ・ 点検、棚卸、監査
- ・ ルールや仕組みの評価、見直し など

リスクが顕在化する具体例

4.ITコストリスク

過剰なライセンス調達

- 正確な利用状況を把握していないために、不足が生じないように余分に調達することで発生する
- 利用していないソフトウェア（廃棄・予備機など）を管理できていない場合に発生する
- 利用実態（メータリング）を把握せず、調達することで発生する
- ソフトウェアの適切なエディションを理解していない場合に発生する

遊休資産の存在に気づかぬままの新規調達

- 部門単位で調達しているハードウェア（スタンドアロン等）を把握していない場合に発生する
- 予備機・余剰機が適切に管理されていない場合に発生する

本来は必要としない契約等の費用

- リース契約している機器について、所在不明なために返却できない場合に発生する（リースの延長契約、リース会社への紛失損害金）
- IT機器やライセンスに関する年間保守契約について、使用状況（程度、有無）を確認しない場合に発生する

障害対応

- 想定していないハードウェアの利用により発生する
- 想定していないソフトウェアの利用により発生する
- 保守契約要項（期間、条件、範囲など）を把握していない事で発生する
- 保証書を適切に保管していない事で発生する



権利の喪失（サポート、アップグレード等）

- ライセンス契約内容（保守サポート、契約期間など）を把握していない場合に発生する
- ライセンス保有証明情報（契約者番号など）を適正に管理していない場合に発生する
- ソフトウェア使用許諾条件（アップグレード、ダウングレード権など）を把握していない場合に発生する
- サポートなどに必要となる情報（ID、キー、証書など）を適正に管理していない場合に発生する

会社の業態変化への追従が困難

- 会社の方針転換（変更）等により、ドキュメントソフトウェア、表計算ソフトウェア、プレゼンテーションソフトウェアやメールソフトウェアを入れ替えねばならない場合に発生する
- それまで利用していたPCをリプレイスする場合に発生する



ITコストリスクが顕在化する具体例

【リスクの要因例】

過剰な調達・リース契約（ハード、ソフト）

過剰な保守契約（ハード、ソフト）

遊休資産の存在（不認知）

保証書の紛失

システム更新毎の全体調査



【リスク発生の防止策例】

＜組織に整合したルールの制定＞

- ・ SAMの方針と体制の策定
- ・ 管理規程・手順の策定 など

＜仕組みの構築＞

- ・ ルールに反した状況の把握
- ・ 管理の証跡の記録 など

＜検証・改善＞

- ・ 点検、棚卸、監査
- ・ ルールや仕組みの評価、見直し など

5.リスク発生要因と防止策（まとめ）

リスク発生要因と防止策（まとめ）

【リスクの要因】

ライセンスコンプライアンスリスク

情報セキュリティリスク

ITコストリスク

【リスク発生の防止策】

＜ルールの制定＞

＜仕組みの構築＞

＜運用管理＞

【防止策の実現】

- ・ 対象資産の網羅的把握
- ・ 体制の整備
- ・ 継続管理

II

SAMの導入

6. SAMの未導入のリスクと導入後のメリット

SAMの未導入のリスクと導入後のメリット

不適切なSAMがもたらすリスク(例)

不認知ハードウェアによる情報漏えい

不適切なソフトウェアによる情報漏えい

不適切なソフトウェアによるシステム障害

不認知ハードウェアによるシステム障害

不適切なライセンス管理による損害賠償

想定外の障害による過剰な運用コスト

過剰なIT資産投資

SAM導入後のメリット

ライセンスコンプライアンスの強化

- ハードウェア・利用ソフトウェア・保有ライセンスの適切な把握によるライセンス不足状況の発生を抑止と損害賠償請求の回避

情報セキュリティの強化

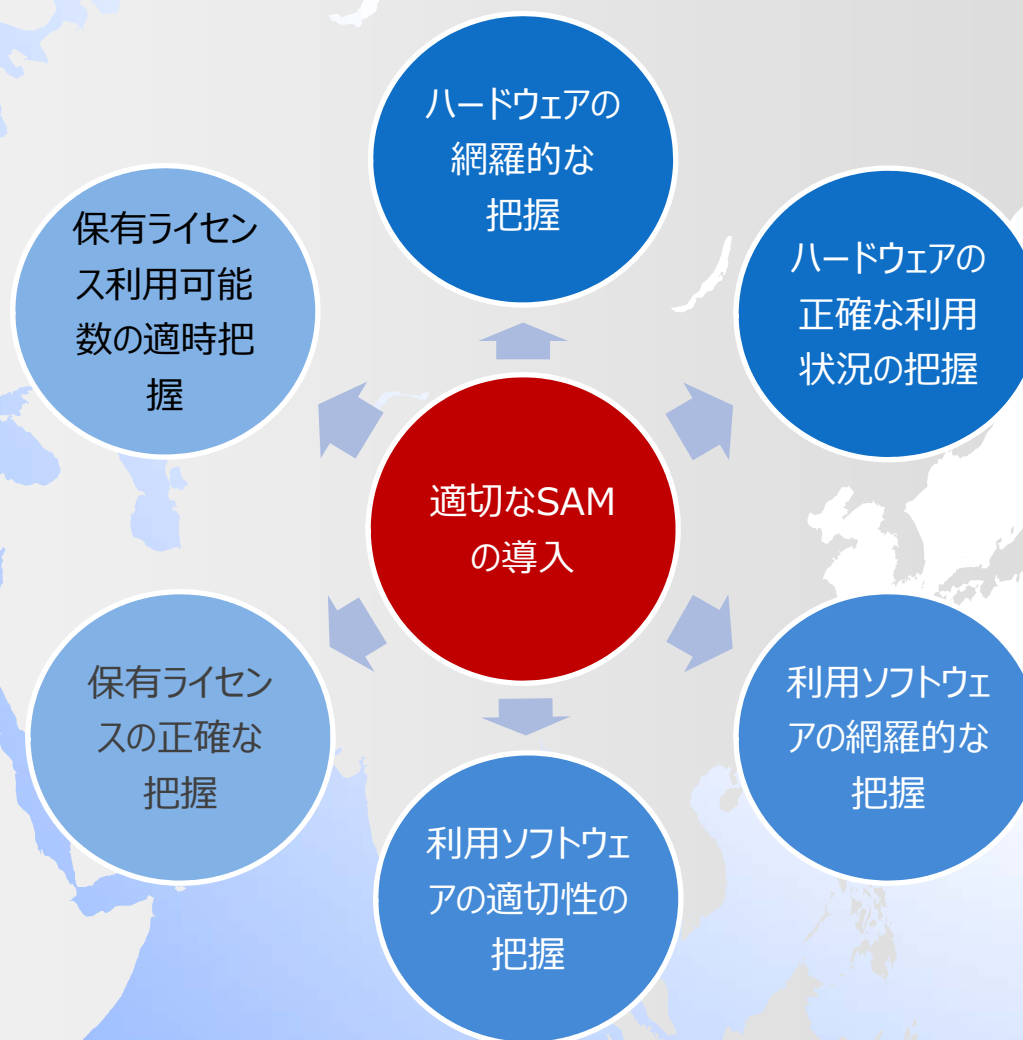
- ハードウェアの適切な把握による漏えい抑止策の徹底
- 利用ソフトウェアの適切なコントロールによる危険なソフトウェアの排除

IT投資コストの最適化

- ハードウェアやライセンスの正確な利用状況の把握による調達コストの最適化
- ハードウェアや利用ソフトウェアの正確な把握による障害対応コストの削減
- 監査・調査請求時の迅速な対応による対策コストの削減

7.総括

適切なSAMの導入により可視化される状況



まとめ

- SAMは、単にライセンスコンプライアンス対策ではなく、情報セキュリティやITコストの最適化にも大きな影響を及ぼすものであることを認識すること
- 「禁止をしているから大丈夫」、「インストール制限をしているから大丈夫」「部門に管理責任を負わせているから大丈夫」ではなく、管理状況を検証し、「適切な運用が守られているか」を把握すること
- そのために、対象資産を網羅的に把握し、可視化すること
- その上で、SAMの実効性を高めるために、組織全体で適切な教育を実施すること

潜在リスク簡易診断シート

ワーキンググループの検討過程で出された項目等を整理して20項目の「潜在リスク簡易診断シート」を作成しました。

（本資料とは別に配布します。）

本シートを参考に、ご自身の組織の状態をチェックしてみてください
はいかがでしょうか。

ユーザーフォーラムSAMAC WGメンバー

篠田 仁太郎 (WGリーダー) 株式会社クロスビート(公認SAMコンサルタント)

神 明彦 エムオーテックス株式会社(公認SAMコンサルタント)

刀根 伸行 リコージャパン株式会社(公認SAMコンサルタント)

ソフトウェア並びに関連資産に係る潜在リスク簡易診断シート

ご自身の組織内の状態について下記の設問に「はい」「いいえ」でお答えください。

2015年 6月 日

SAM運用状況チェック表		関連管理項目			回答		評点
設問		ハードウェア	ソフトウェア	ライセンス			
1	ハードウェア・ソフトウェア・ライセンスの異動等は、適時に記録されていますか？	☐	☐	☐	はい ☐	いいえ ☐	7
2	保有している全てのハードウェア・ソフトウェア・ライセンスは、一意に識別されていますか？	☐	☐	☐	はい ☐	いいえ ☐	7
3	ハードウェア管理台帳を作成し、スタンドアロンも含めて組織で利用している全てのハードウェアを把握できていますか？	☐			はい ☐	いいえ ☐	7
4	全てのソフトウェアが、使用許諾条件を満たして利用されていることを確認していますか？			☐	はい ☐	いいえ ☐	7
5	ソフトウェア管理台帳を作成し、組織で利用している全てのソフトウェアを把握できていますか？		☐		はい ☐	いいえ ☐	7
6	保有ライセンス管理台帳を作成し、組織で保有している全てのライセンスを把握できていますか？			☐	はい ☐	いいえ ☐	7
7	ライセンスを保有していることを証明するために必要な部材（メディア、キー、IDなど）を適切に管理していますか？			☐	はい ☐	いいえ ☐	7
8	組織内のIT資産を利用する全従業員に対して、モラル向上やルール遵守の教育を定期的実施していますか？	☐	☐	☐	はい ☐	いいえ ☐	5
9	組織で利用しているハードウェアに不適切なソフトウェアが導入されたことを検知できる状態になっていますか？	☐	☐		はい ☐	いいえ ☐	5
10	ハードウェアの紛失、盗難発生時の情報漏えいや、ライセンス違反が発生した場合、発生する損失（損害の規模）を試算できますか？	☐	☐	☐	はい ☐	いいえ ☐	5
11	利用しているソフトウェア（ライセンス）のサポート契約状況が適切に記録され、把握できていますか？		☐	☐	はい ☐	いいえ ☐	5
12	悪意のあるソフトウェアの定義や制御はできていますか？		☐		はい ☐	いいえ ☐	5
13	万一、情報漏えいやライセンス違反が発生した場合には、その発生元を特定できますか？	☐	☐	☐	はい ☐	いいえ ☐	5
14	現在利用中のIT資産に関わる費用（TCO）は把握できていますか？	☐	☐	☐	はい ☐	いいえ ☐	3
15	新システム構築やシステム更改時に対象となるシステム毎の利用ハードウェアとソフトウェアの特定はできていますか？	☐	☐	☐	はい ☐	いいえ ☐	3
16	廃棄・リース返却したハードウェア、ソフトウェアで利用していた保守契約の解約処理は、プロセスに沿って適切に処理できていますか？	☐	☐	☐	はい ☐	いいえ ☐	3
17	ソフトウェアメーカーや権利保護団体などから、調査・監査請求があった場合、対応できる体制になっていますか？	☐	☐	☐	はい ☐	いいえ ☐	3
18	ハードウェア、ソフトウェアに関する保守費用とその内容が適正であることを定期的に確認していますか？	☐		☐	はい ☐	いいえ ☐	3
19	組織で利用している全てのソフトウェアが最新の状態に保たれている（パッチ、アップデート、定義ファイルの適用）、あるいは、任意のタイミングで最新の状態にできることを確認できていますか？	☐	☐		はい ☐	いいえ ☐	3
20	組織全体として利用できるソフトウェアを定めていますか？		☐		はい ☐	いいえ ☐	3
評点合計							100

【潜在リスク度と対策】

評点合計	潜在リスクと対策
45点以下	高いリスクが見込まれます。早急なSAMへの取り組みを検討することをおすすめします。
46点～60点	一部リスク対策は認められますが、SAMの管理レベルを上げる取り組みを検討することをおすすめします。
61点～74点	SAMに関して、ある程度の対策が認められます。未対策の項目への対応を検討することをおすすめします。
75点以上	SAMに関する対策が認められます。必要に応じ、現行の運用の見直し、対策の強化を検討することをおすすめします。

※本診断シートは、本ワーキング活動にてSAMに関する組織のリスク値を簡易的に可視化するために作成したものであり、結果については一切の保証をするものではありません。予めご了承ください。