SAMAC
一般社団法人 IT資産管理評価認定協会

コンプライアンスとセキュリティのためのIT資産管理の必要性と推奨される管理

IT資産管理評価認定協会
公認SAMコンサルタントトレーナー
ライセンスセミナー WG　篠田 仁太郎

Agenda

IT資産管理とは？

- IT資産管理の範囲
- IT資産管理とは？
- IT資産のライフサイクル
- IT資産管理を取り巻く環境
- IT資産管理の「これまで」

IT資産管理の現状

- 情報セキュリティの対策
- 情報セキュリティの実際
- ライセンスコンプライアンスの対策
- ライセンスコンプライアンスの実際
- ITコストの実際
- 対策アプリケーションの罪

適切なIT資産管理の導入プロセス

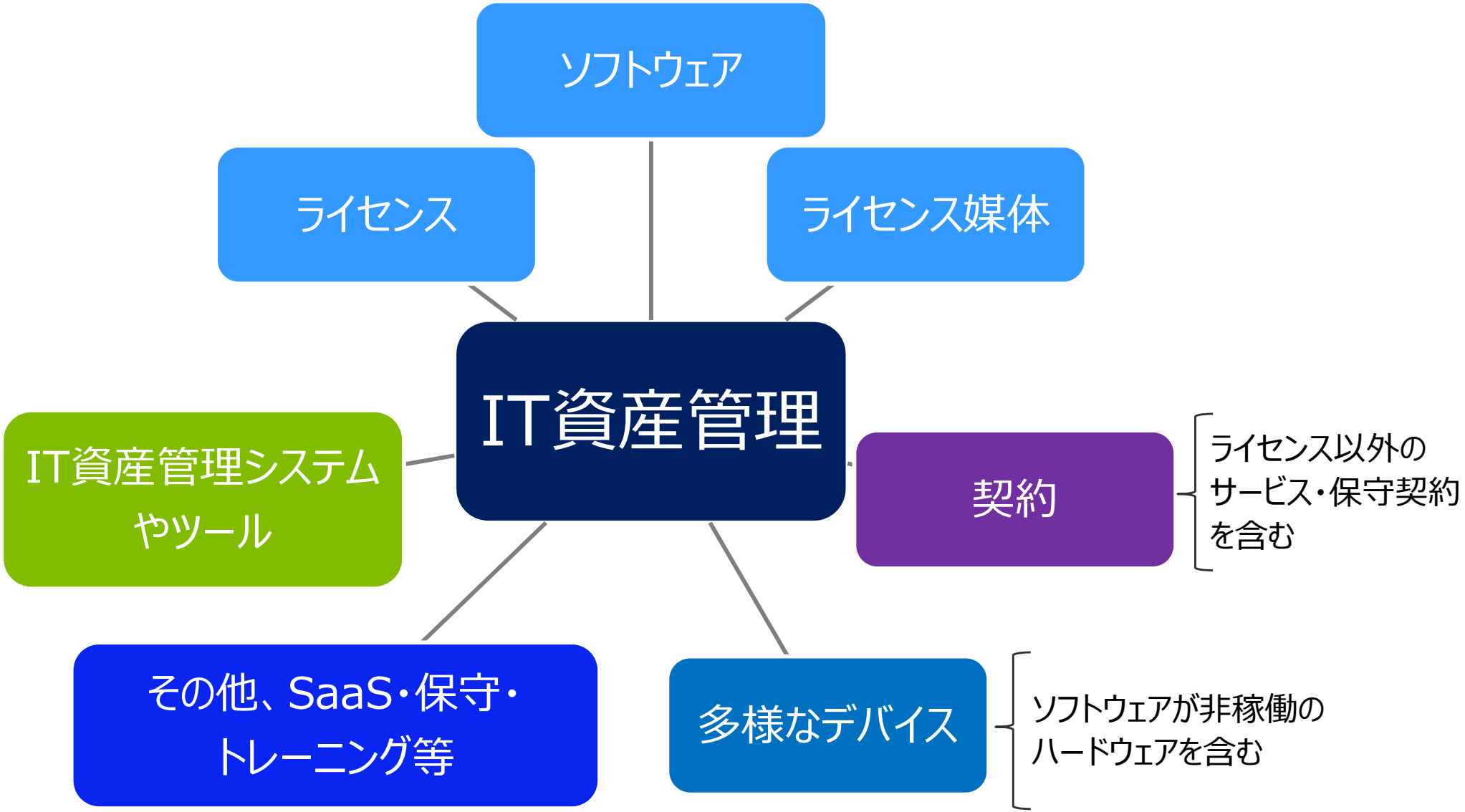
- IT資産管理導入～運用プロセス
- 現状把握の前に検討すべき事項
- IT資産管理を妨げている、「希望」と「思い込み」
- インベントリー分析
- インベントリー分析の結果
- サンプリング調査
- サンプリング調査の結果
- 現状把握のプロセス
- 台帳の策定
- 適切なIT資産管理導入プロセスのまとめ
- IT資産管理の「これから」

まとめ

- IT資産管理に望まれるモノ
- 適切なIT資産管理実現のために

IT資産管理とは？

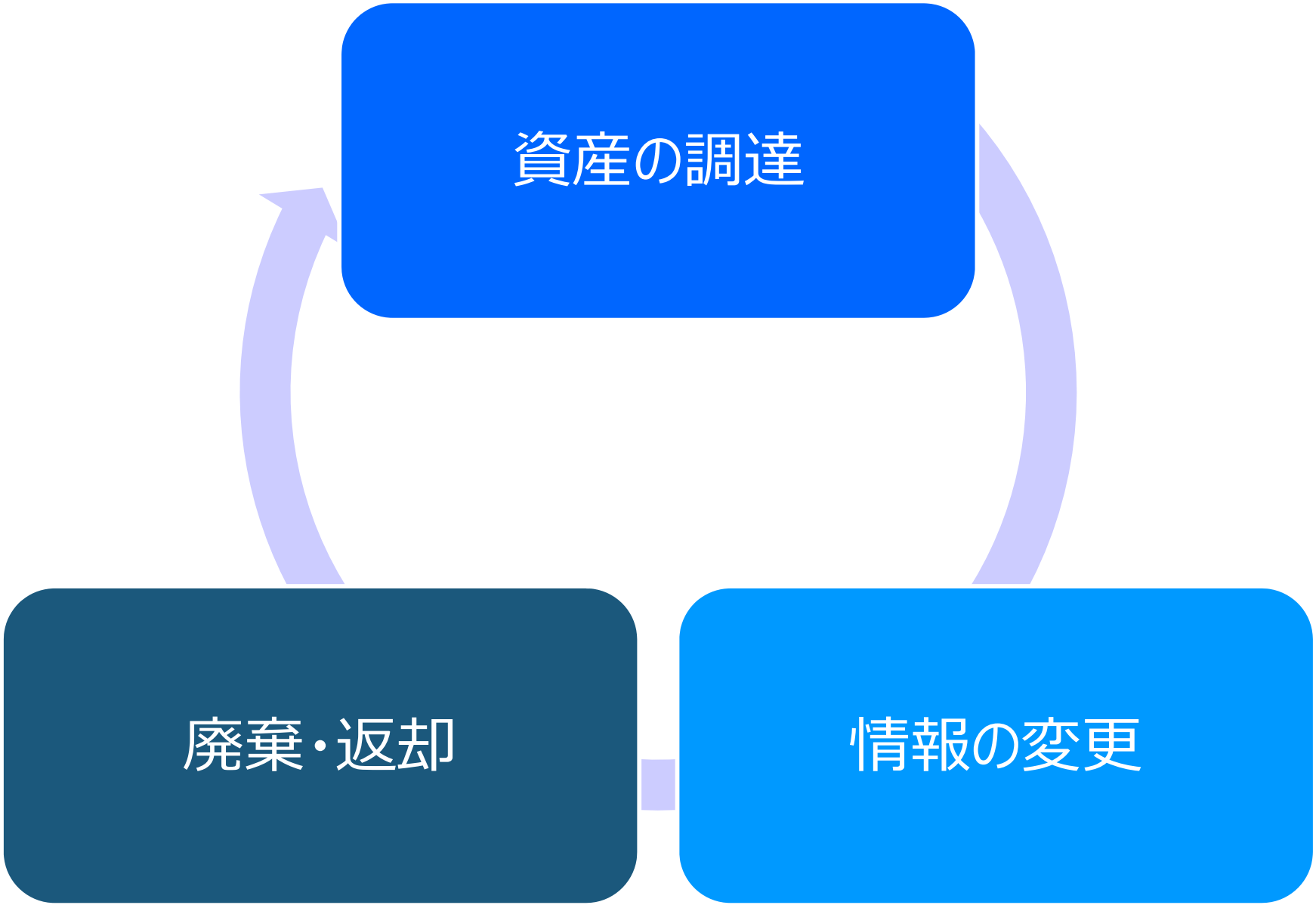
IT資産管理の範囲



IT資産管理とは？

IT資産に関するリスクをコントロールする仕組み

IT資産のライフサイクル（１）



IT資産のライフサイクル（２）

資産の調達

- 購入・リース・レンタル・ダウンロード・フリー・利用期間・利用条件・メーカー名・型番・シリアル・キー・etc.

情報の変更

- 利用者の異動・利用部署の変更・スペックの変更・利用場所の変更・利用数の変更・保有数の変更・条件の変更・アップグレード・ダウングレード・etc.

廃棄・返却

- アンインストール・データ消去・マニフェスト・利用数の変更・同時廃棄（返却）資産の把握と処分・etc.

IT資産管理を取り巻く環境

SAMAC

- 日本最大のIT資産管理の推進団体

BSA

- 米国に本部を持つ、世界最大の権利者団体

JIS/ISO

- IT資産管理のISOである19770-1を中心に、JIS化推進中

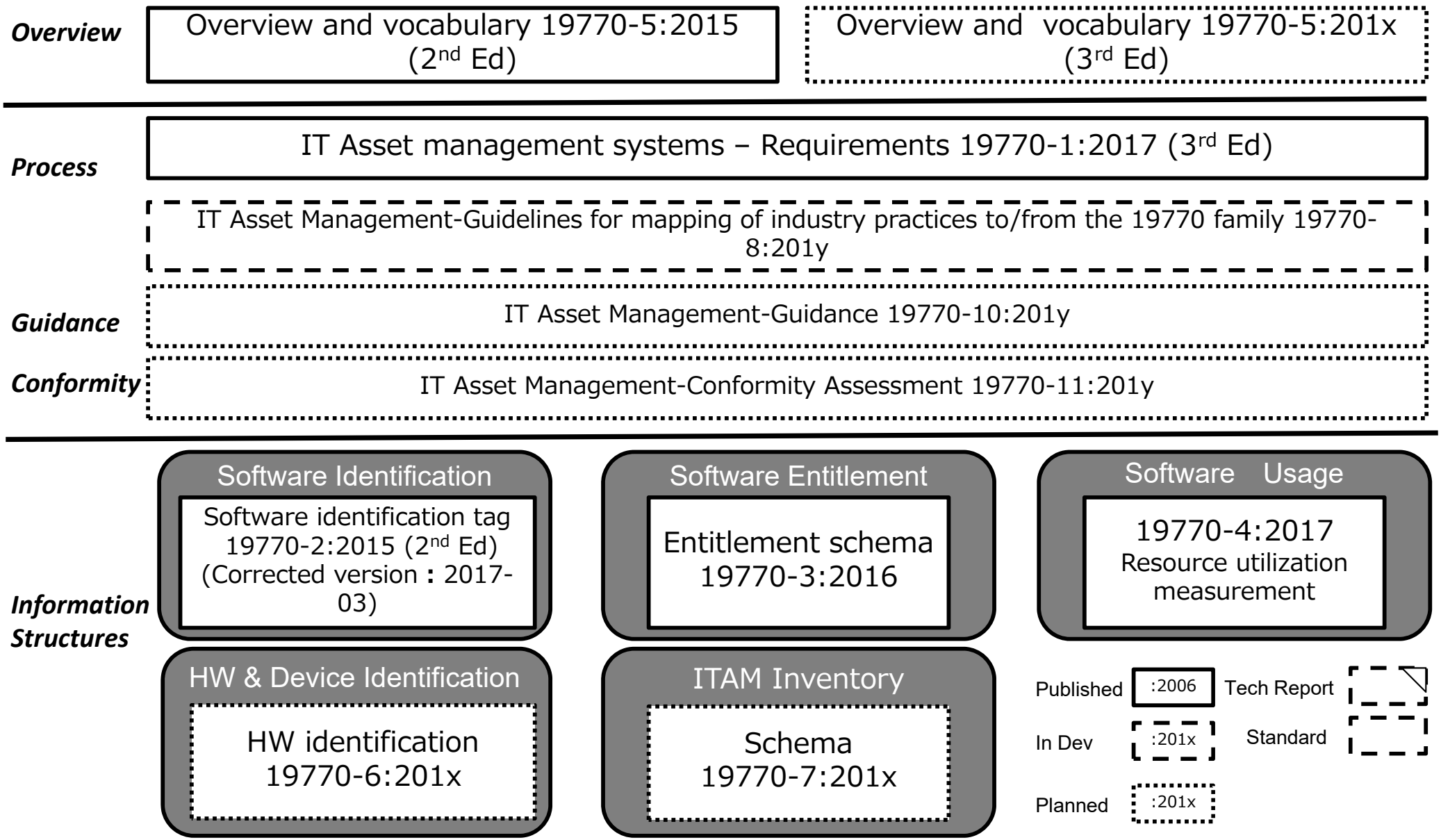
JIPDEC

- PマークやISMSを推進している団体で、IT資産管理の委員会を主催

itSMF

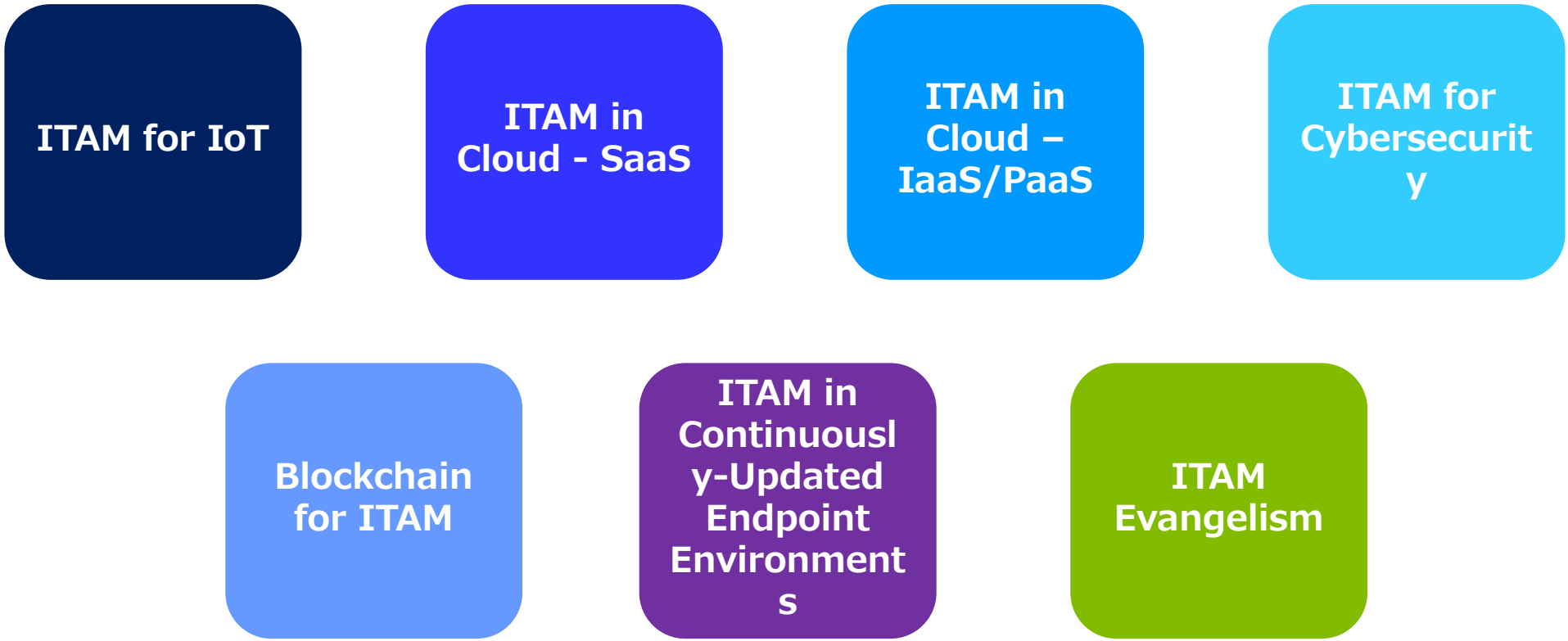
- 英国に本部を持つ、ITIL®を推進する団体
- IT資産管理にも関係

ISO/IEC:19770 Family

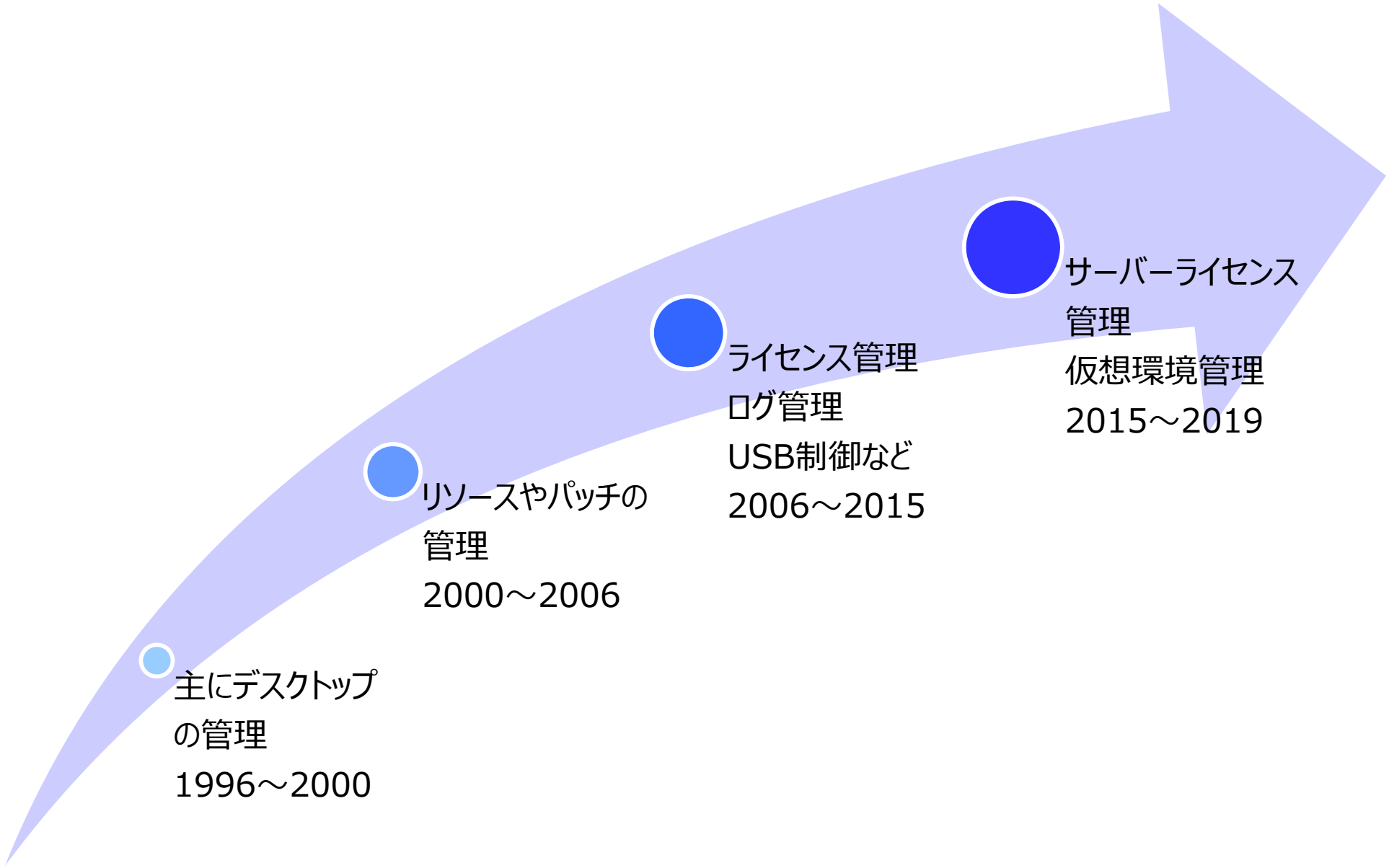


SAMAC
一般社団法人 IT資産管理評価認定協会

SC7/WG21で研究中のテーマ



IT資産管理の「これまで」



IT資産管理の現状

～情報セキュリティ・コンプライアンス・コストから～

SAMAC
一般社団法人IT資産管理評価認定協会

情報セキュリティの対策

情報漏えい抑止のための機密性の向上

- ディスクの暗号化
- 操作ログの収集
- ワンタイムパスワード
- 添付ファイルの自動暗号化
- USBの禁止
- ファイルの持ち出し制限
- ウィルス対策ソフトの導入
- サイトの接続制限
- 不正ソフトウェアの検知システムの導入
- 情報の取り扱いに対する規程類の作成

Etc.・・・

セキュリティアプリケーションによるコントロールと管理文書の策定・報知

情報セキュリティの実際

質問	一般的な回答	実際の状況
パソコンは何台ありますか？	ネットワークに接続されているのは○台 おそらく○台程度はある	ネットワークに接続しているかいないかに関わらず、予想数の2割増しのパソコンが存在
そのパソコンは誰が使っていますか？	台帳で管理しており、部門の申請に基づいて把握している	全体の３割程度は、人事異動や組織変更が反映されていない
使っていないパソコンはありますか？	廃棄予定のパソコンは場所を決めて、廃棄まで保管している	執務スペースの様々な個所に放置パソコンが存在
サーバはすべて把握していますか？	サーバはすべてに管理者を指定しており、把握できている	仮想環境が勝手に構築されており、把握しきれていない
すべてのサーバのバックアップ計画は把握され、検証されていますか？	サーバの管理規定は定められており、適切に運用するよう周知している	各自が各自の基準でサーバーを扱っている

ライセンスコンプライアンスの対策

コンプライアンス違反抑止のための利用状態の統制

インベントリーツールによるコントロールと管理文書の策定・報知

ライセンスコンプライアンスの実際

質問	一般的な回答	実際の状況
どんなソフトウェアが利用されているか把握していますか？	インベントリーツールで収集しているので、調べればわかる	積極的に確認していないため、Baiduなどのアドウェアが多数インストールされている
シェアウェアやフリーウェアは把握していますか？	有償ソフトウェアは調達部門が管理しており、フリーウェアは管理していない	有償かフリーウェアかの判別プロセスがなく、有償ソフトウェアが無管理で放置されている
ボリュームライセンス以外のライセンスも登録されていますか？	部門で調達しているパッケージソフトウェアは部門が管理している	個人が勝手に保管しており、異動に伴って紛失している
ボリュームライセンスはすべて把握していますか？	すべて把握しているし、わからなければベンダーに問い合わせれば良い	ベンダーの情報は必ずしも正確ではなく、情報自体も提示されない可能性もある
仮想環境のソフトウェアや開発用ソフトウェアは管理していますか？	管理者は詳しい知識を持っているので管理は問題ない	仮想環境の把握は不十分であり、ユーザーライセンスの管理は使用者任せ

ITコストの実際

- 他の部署で使えるハードウェアはないか？
- 遊休となっているハードウェアはないか？
- リースの延長ができるマシンはないか？
- インストールされているソフトウェアはどれくらい使われているのか？
- 同じような機能のソフトウェアが使われていないか？
- 入れ替え計画が適時に策定できるか？？
- 同じようなサービスが利用されていないか？？

ITコストの実際

余剰ハードウェアの存在	余剰ライセンスの存在	オーバースペックの存在
重複システムの利用	入れ替え計画のロス	無駄な対策コスト

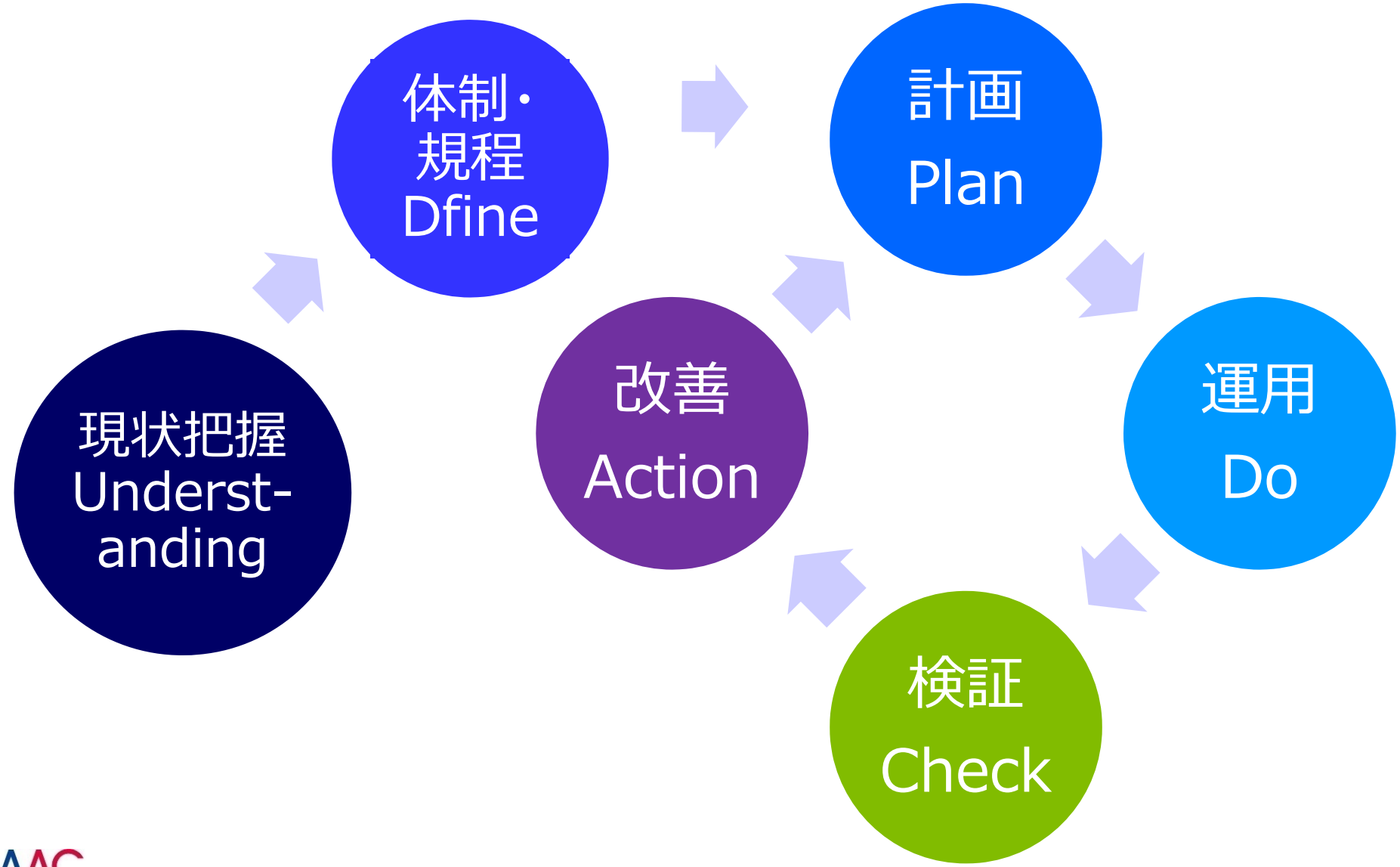
対策アプリケーションの罪

対策アプリケーションの導入で満足

- 全ての情報が収集できているか？
- スタンドアロンや社外ネットワークのハードウェアはどうするか？
- 仮想環境やクラウドの把握はどこまでできているか？
- 廃棄予定や廃棄済みで残っているハードウェアはないか？
- 利用しているソフトウェアが必要とするライセンスは適切に保有できているか？
- 不要・危険なソフトウェアは把握できているか？
- ライセンスやハードウェアが適切に割り当てられているか？

適切なIT資産管理の導入プロセス

IT資産管理導入～運用プロセス



SAMAC
一般社団法人 IT資産管理評価認定協会

21

現状把握の前に検討すべき事項

何（対象）をどこまで（情報）やるか？

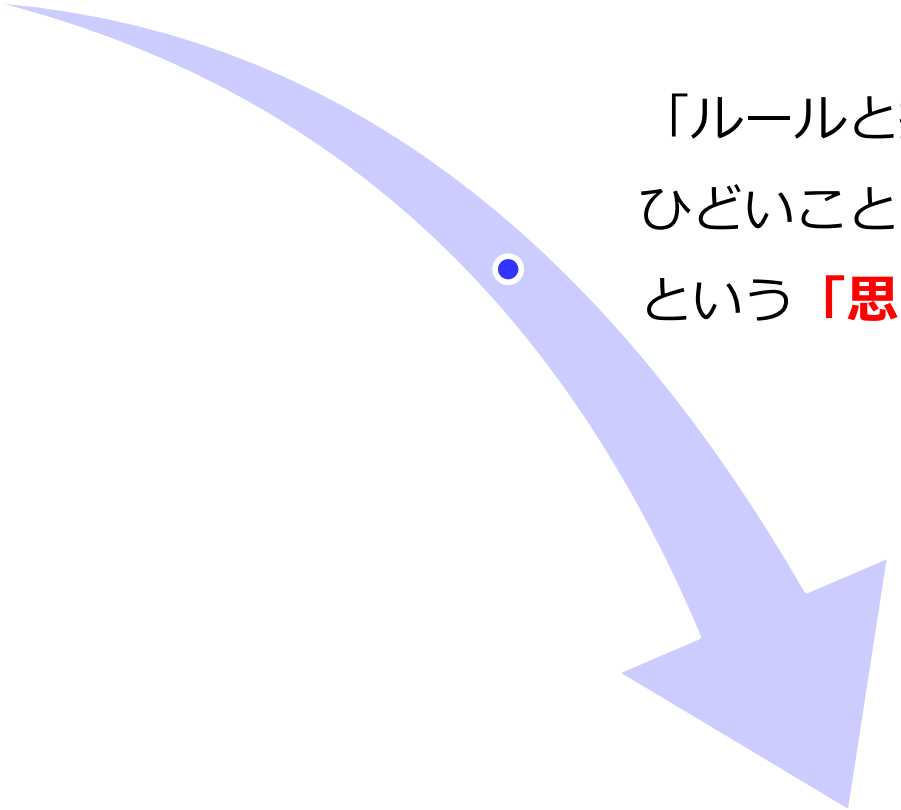
- 無駄にならない調査を行う
- リスクの多寡を判断した上で設計する

そのための事前準備が重要

- 例えば・・・
  - インベントリー分析
  - サンプリング調査

IT資産管理を妨げている、「希望」と「思い込み」

「ある程度何とかなっているだろう」
という**「希望」**



「ルールと抑止ソフトウェアの導入で、
ひどいことにはなっていないはずだ」
という**「思い込み」**

管理に意識を向けるために必要なこと
＝状態を「可視化」すること

インベントリー分析

可視化の第一歩はインベントリー分析

- 登録されているハードウェア・デバイスは何か？
- それはどこで誰が使っているか？
- そのデバイスのインベントリーは何日前に収集されているか？
- 同じ型番・シリアルのハードウェアが重複して登録されていないか？
- 同じログインユーザーで重複して登録されているデバイスはどれくらいあるか？
- 組織全体で利用されているソフトウェアはどれくらいの種類があるか？
- ５%未満のデバイスで利用されているソフトウェアはどれくらいあるか？
- 素性が把握できていないソフトウェアはどれくらいあるか？

インベントリー分析例（利用ソフトウェア）

1.ソフトウェア調査対象数概要

【調査対象数】

PC台数
4153機器

	種類	フト種類／機器	他社平均
ソフトウェア種類	3,510種類	0.85倍	3.45倍
除くMS等パッチ	3,394種類	0.82倍	2.62倍

2.ライセンス種別概要

【ライセンス種別概要】

種別	計	比率	他社平均
有償ソフトウェア	303種類	8.6%	10.2%
フリーウェア	822種類	23.4%	14.9%
ドライバー・ユーティリティー等	732種類	20.9%	22.3%
HOTFIX	116種類	3.3%	11.7%
アドウェア系	21種類	0.6%	0.2%
不明	81種類	2.3%	3.7%
文字化け	11種類	0.3%	1.1%
辞書未登録	1,424種類	40.6%	35.9%
合計	**3,510種類**	**100.0%**	**100.0%**

3.導入比率別分布

【導入比率別分布】

種別	合計	インストール台数									
		1～3台	4～5台	6～10台	11～15台	16～20台	21～30台	31～50台	51～100台	101～200台	201台～
有償ソフトウェア	303	189	14	33	22	9	4	13	5	1	13
フリーウェア	822	526	71	97	35	11	7	14	17	8	36
ドライバー・ユーティリティー等	732	417	54	64	41	19	18	33	30	16	40
HOTFIX	116	61	9	19	2	3	3	1	3	4	11
アドウェア系	21	11	5	5	0	0	0	0	0	0	0
不明	81	44	13	11	2	1	1	4	3	0	2
文字化け	11	7	0	2	1	0	0	1	0	0	0
辞書未登録	1424	1211	71	72	13	9	10	14	6	2	16
合計	**3,510**	**2,466**	**237**	**303**	**116**	**52**	**43**	**80**	**64**	**31**	**118**
比率	**100.0%**	**70.3%**	**6.8%**	**8.6%**	**3.3%**	**1.5%**	**1.2%**	**2.3%**	**1.8%**	**0.9%**	**3.4%**

インベントリー分析例（利用ソフトウェア）

4.標準ソフトウェア候補

ソフトウェアの利用シェア(%)	100.0%	29.7%	23.0%	14.4%	11.1%	9.6%	8.3%	6.1%	4.2%	3.4%
ソフトウェアの利用シェア(種類)	3,510	1,044	807	504	388	336	293	213	149	118

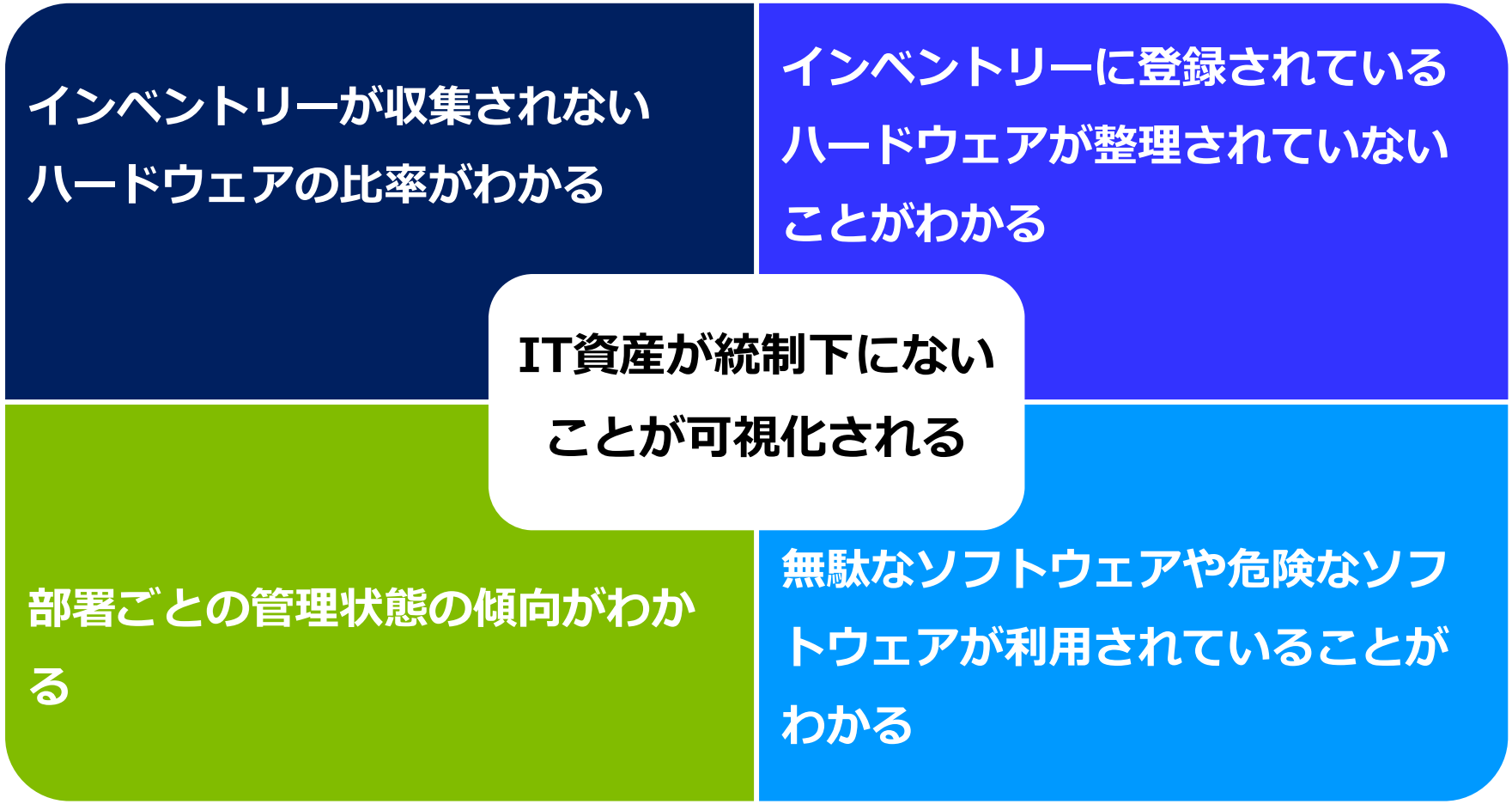
有償・フリーウェアの利用シェア(%)	32.1%	11.7%	9.3%	5.6%	3.9%	3.4%	3.0%	2.3%	1.7%	1.4%
ドライバ・ユーティリティ等の利用シェア（%）	20.9%	9.0%	7.4%	5.6%	4.4%	3.9%	3.4%	2.5%	1.6%	1.1%
HOTFIXの利用シェア（%）	3.3%	1.6%	1.3%	0.8%	0.7%	0.6%	0.5%	0.5%	0.4%	0.3%
有償・フリーウェアの利用シェア(種類)	1125	410	325	195	138	118	107	80	58	49
ドライバ・ユーティリティ等の利用シェア（種類）	732	315	261	197	156	137	119	86	56	40
HOTFIXの利用シェア（種類）	116	55	46	27	25	22	19	18	15	11
標準ソフトウェア候補計（%）	**29.7%**	16.1%	14.3%	11.9%	9.1%	7.9%	7.0%	5.2%	3.7%	2.8%
標準ソフトウェア候補計（種類）	**1043**	565	502	419	319	277	245	184	129	100

その他利用シェアの高いソフトウェア（%）	43.2%	7.2%	4.8%	2.4%	2.0%	1.7%	1.4%	0.8%	0.6%	0.5%
その他利用シェアの高いソフトウェア（種類）	1516	254	170	85	69	59	48	29	20	18
追加標準ソフトウェア候補計（%）	**2.4%**									
追加標準ソフトウェア候補計（種類）	**85**									

見込標準ソフトウェア候補合計（%）	**32.1%**
見込標準ソフトウェア候補合計（種類）	**1128**
内 有償（%）	1.9%
内 有償（種類）	67
内 フリーウェア（%）	3.6%
内 フリーウェア（種類）	128
内 ドライバ・ユーティリティ等（%）	20.9%
内 ドライバ・ユーティリティ等（種類）	732
内 HOTFIX（%）	3.3%
内 HOTFIX（種類）	116
内 不明等（%）	2.4%
内 不明等（種類）	85

※分析結果は、SAMACの辞書の利用を前提

インベントリー分析の結果



サンプリング調査

組織の一部の状況から、全体の状況を推定し、可視化する

- どのようなハードウェアが利用されているか？
- （仮想環境も含め）想定外のハードウェアが存在していないか？
- 組織全体でどのようなソフトウェアライセンスがどれだけ不足しているか？
- 機密性に影響を与える可能性のあるソフトウェアがどれくらい利用されているか？
- 部門におけるソフトウェアライセンスの保管状況はどうなっているか？

サンプリング調査結果報告書サンプル（１）

５．サンプリング調査対象先の概要

(1) 今回のサンプリング対象先

今回のサンプリング対象先並びにヒヤリングの実施日は以下の通りである。

実施日	実施部門	保有ハードウェア （）はスタンドアロン	部門保有 ライセンス[1]
201X 年 M 月 D 日	XXXX 課	26 台（0 台）	66 本
	AAAA 課	41 台（16 台）	172 本
201X 年 M 月 D 日	BBBB 課	26 台（0 台）	4 本
	YYYY 課	33 台（0 台）	5 本
201X 年 M 月 D 日	ZZZZ 課	66 台（46 台）	39 本
201X 年 M 月 D 日	CCCC 課	37 台（11 台）	10 本
	合計	229 台（73 台）	296 本

(2) IT 資産管理の取組み概要（詳細については、添付「ヒヤリング結果シート」参照）

社内ネットワーク（以下「社内ネット PC」という。）に接続されているハードウェアと、それ以外のハードウェア（以下「スタンドアロン」という。）に大別される。

社内ネット PC については、利用者に管理者権限は与えられておらず、ソフトウェアのインストール・アンインストールの手順についても定められ、周知されている。

運用状況の検証プロセスは特に定められておらず、検証行為自体も行われてはいないが、管理の今回のサンプリングの範囲では、大きな齟齬はないように見受けられた。ただし、社内ネット PC にインストールされるソフトウェアの内、情報システム部が指定しているソフトウェア以外のライセンスについては、各部門が保管しているものの、その具体的な保管手続や保管方法等については文書化されておらず、組織的な管理が行われている状況にはない。

スタンドアロンについては、組織全体として承認された管理手続は確認できなかった。現状では、各部門の自主的な管理に基づいて利用されているが、技術系の部門においては、一部のソフトウェアについて、AAAA 課が中心となり、組織横断的に管理を行う仕組みが確認された。対象としているライセンスについても、管理効率を意識した調達を行っており、望ましいものと言える。

Ⅱ．利用資産状況

１．ハードウェア並びに利用ソフトウェアの状況

確認したハードウェアは全部で２２９台あり、内、社内ネット PC は１５６台で全体の約６８．１%、スタンドアロンが２１．９%となっている（表１ご参照）。

一部、業務上特殊な部門（ZZZZ 課）も入ってはいるが、それを除いてもスタンドアロンの比率は１６．６%あり、単純に計算すれば、４，３７７台の社内ネット PC に対して、約８７０台のスタンドアロンが存在している計算になる。

利用されているソフトウェアの種類を確認してみると、１５６台ある社内ネット PC が利用しているソフトウェアの種類は合計で１９９種類と、社内ネット PC 全体の利用ソフトウェア種類の１０．６%程度なのに対し、スタンドアロンでは、７３台で１，０６７種類と、同じく社内ネット PC 全体の利用ソフトウェア種類の６０%程度が利用されていることになる。（表１ご参照）。

表 1

実施日	部門名	対象資産数			
		ハードウェア台数		インストール数	
		社内ネット PC	スタンドアロン	社内ネット PC	スタンドアロン
yyyy.m.d	XXXX 課	26 台	0 台	52 種類	0 種類
yyyy.m.d	AAAA 課	25 台	16 台	105 種類	308 種類
yyyy.m.d	BBBB 課	26 台	0 台	100 種類	0 種類
yyyy.m.d	YYYY 課	33 台	0 台	75 種類	0 種類
yyyy.m.d	ZZZZ 課	20 台	46 台	69 種類	759 種類
yyyy.m.d	CCCC 課	26 台	11 台	80 種類	196 種類

サンプリング対象先個別合計[1]	156 台	73 台	340 種類	1,263 種類
サンプリング対象先統合合計[2]	**156 台**	**73 台**	**199 種類**	**1,067 種類**
社内ネット PC 組織全体合計	4,377 台	–	1,883 種類	–

もちろん、スタンドアロンとして利用する以上、そこでは特殊なソフトウェアが利用される可能性は高くなり、これがソフトウェアの利用種類が増えていく一因になっていることは間違いないが、これだけたくさんの、且つ特殊なソフトウェアが利用されるのであれば、それを利用する側には、そのソフトウェアの利用方法だけでなく、利用条件や必要な管理要件等についても相応の知識が求められることになる。

サンプリング調査結果報告書サンプル（２）

2．利用ソフトウェア種類の考察（社内ネット PC とスタンドアロンの比較）

社内ネット PC とスタンドアロンで、利用されているソフトウェア種類の比率を見ると、社内ネット PC の方がスタンドアロンよりも有償ソフトウェアの構成比が高いが、これは、スタンドアロンにインストールされているソフトウェアの特殊性に拠り、有償ソフトウェアに付随するユーティリティソフトウェアや特殊な機器と接続するためのドライバ等が多くインストールされていることによるものと推察されることから、ここではその構成比ではなく、利用種類自体の比較から見ていく（表２ご参照）。

ここで注意すべき点はまず、社内ネット PC に比べスタンドアロンの方が、有償ソフトウェアとフリーウェアが、それぞれ 3.6 倍、3.1 倍と高いことである。現時点の運用状況においては、ライセンスの調達やソフトウェアのインストールに際し、使用許諾条件や管理方法、納品物の適切な確認を行う手続が定められておらず、導入されているソフトウェアの適切性が担保されない状況にある。

フリーウェアに加え、SAMAC の辞書で種別が判別できていないソフトウェアや SAMAC の辞書に登録されていないソフトウェアについても、それぞれ 6.9 倍、4.4 倍と非常に高く、これらについては特に、セキュリティ上大きな問題が発生する可能性のあるソフトウェアが利用されていないとは言えないため、早急な確認が望まれる状況にある。アドウェア系についても、スタンドアロンの方だけで２種類（５件）発見されており、早期の適切な管理の確立が望まれる。

表 1

種別	社内ネットワーク PC		スタンドアロン		比較※1
有償ソフトウェア	32種類	16.1%	115種類	10.8%	3.6
フリーウェア	38種類	19.1%	117種類	11.0%	3.1
ドライバー・ユーティリティー等	78種類	39.2%	566種類	53.0%	7.3
HOTFIX※2	8種類	4.0%	68種類	6.4%	8.5
アドウェア系	0種類	0.0%	2種類	0.2%	-
不明	7種類	3.5%	48種類	4.5%	6.9
文字化け	2種類	1.0%	2種類	0.2%	1.0
辞書未登録	34種類	17.1%	149種類	14.0%	4.4
合計	**199種類**	**100.0%**	**1,067種類**	**100.0%**	

※１：社内 PCとスタンドアロンで、利用されているソフトウェアの種類の違いを明確にするために、スタンドアロンの利用ソフトウェア種類数を市政PCのそれで除した結果を表示したもの

※２：ソフトウェアベンダーから提供されるセキュリティパッチやサービスパックをいう

3．保有ライセンスと見込み過不足数

本調査で確認できた部門ごとに保有している有償ソフトウェアのライセンス媒体は、ソフトウェアベンダー別に、表３の通り。

表 1

ソフトウェアベンダー名	ライセンス媒体保有数	ライセンス保有数
Adobe	6	6
Agilent Technologies	5	5
Applied Biosystems	2	6
Applied Biosystems/MDS Analytical Technologies	2	2
CASIO計算機株式会社	1	1
COREL	2	2
e frontier	1	1
Fujixerox	16	143
JASC Software （現：コーレル株式会社）	1	1
Lifetechnologies	2	2
McAfee	1	1
Microsoft	40	40
NEC	1	1
Nishikawa	1	1
Oracle		
総計	**102**	**296**

サンプリング調査の結果

想定していないデバイスが存在していることがわかる

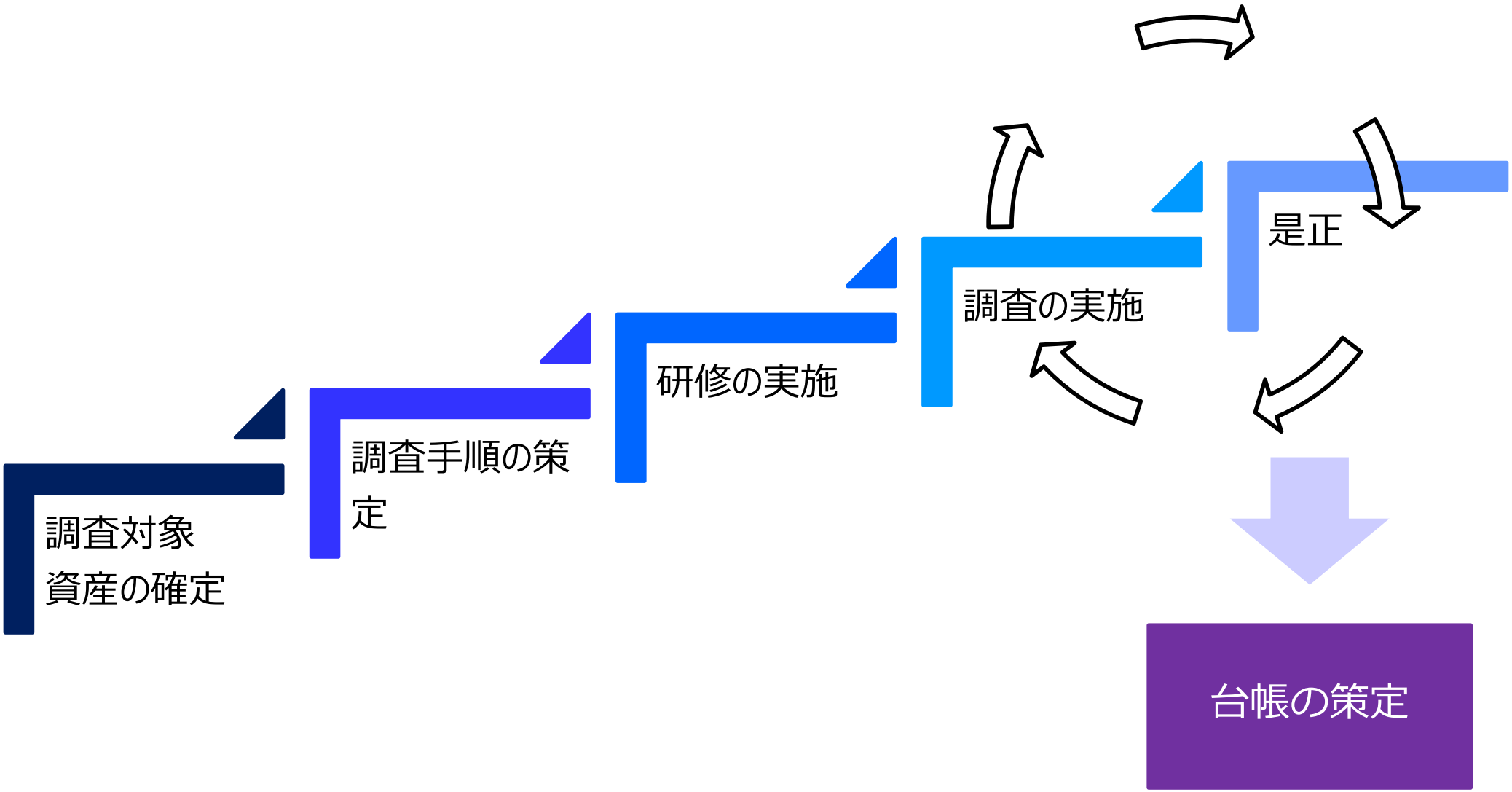
想定していないソフトウェアが利用されていることがわかる

IT資産が統制下にないことが「より」可視化される

部署ごとの管理状態の傾向がわかる

保有すべきライセンスが確認できないことがわかる

現状把握のプロセス



台帳の策定

管理項目は対象資産とその属性から決定される

対象のハードウェアは何か？

- PC・サーバー・ネットワーク接続分・ネットワーク非接続分・常駐業者持ち込み分・お客様への持ち込み分・ハウジングサーバー・ホスティングサーバー・仮想環境・検査機等

対象のソフトウェアは何か？

- Windows・Windows以外・実行形式のソフトウェア・非実行形式のソフトウェア

対象のライセンスは何か？

- ボリューム・パッケージ・プリインストール・クラウド・CPU・デバイス・ユーザー・セカンド・サイト・CAL・サブスクリプション

適切なIT資産管理導入プロセスのまとめ

可視化できるものから可視化してみること

欲張らないこと

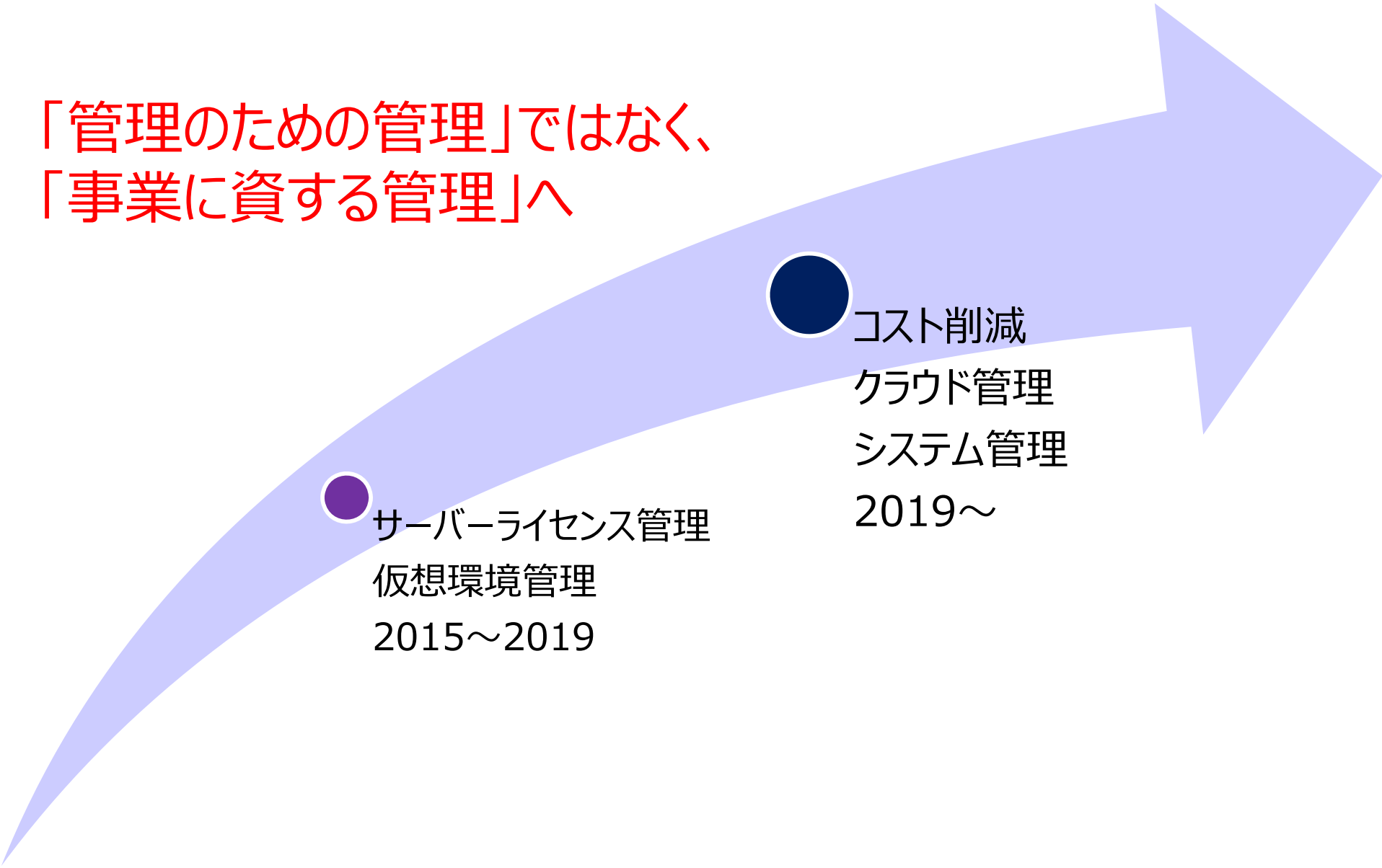
できること、できるものから始めること

決めたことは徹底して実行すること

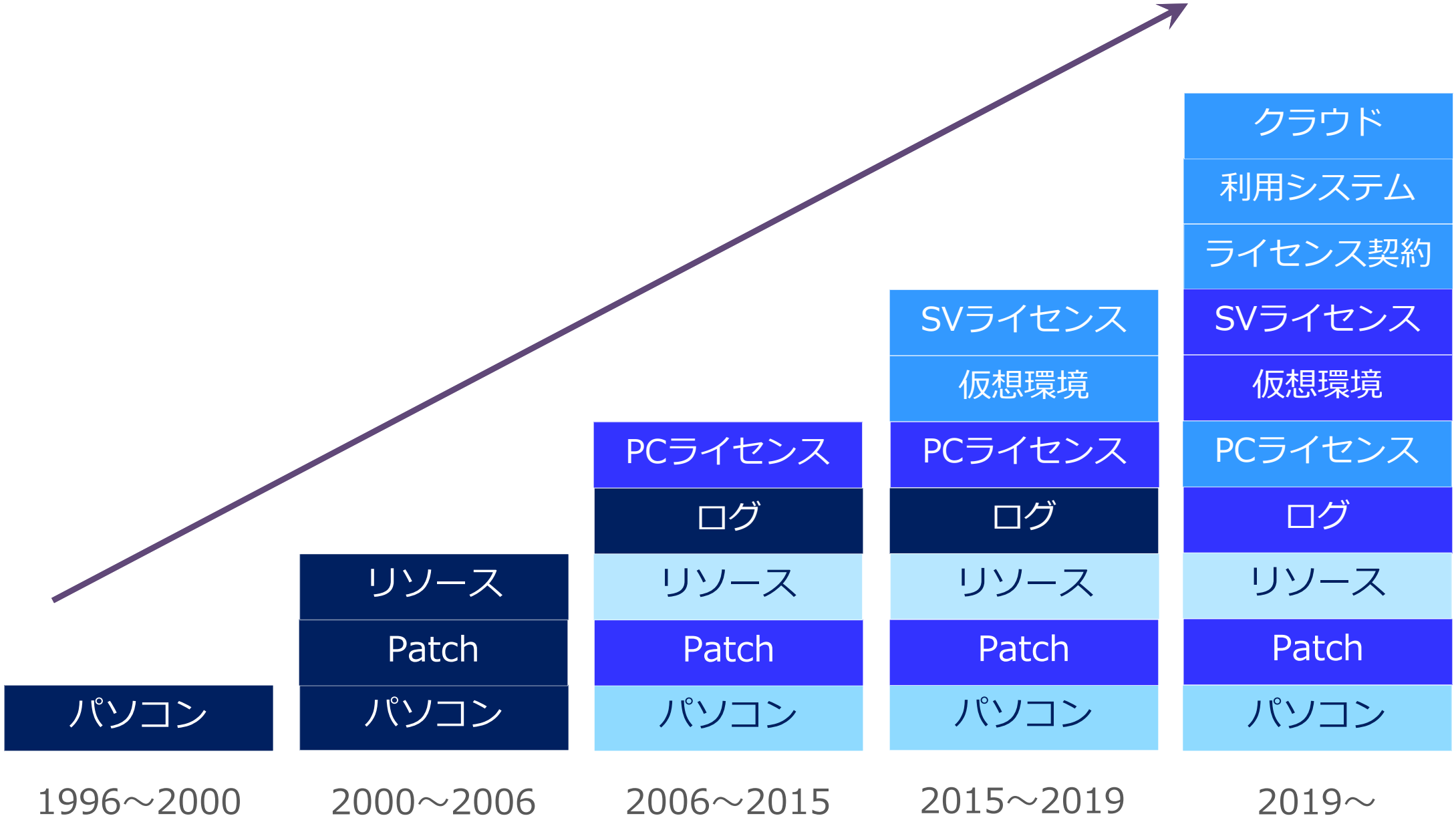
34

IT資産管理の「これから」

「管理のための管理」ではなく、
「事業に資する管理」へ



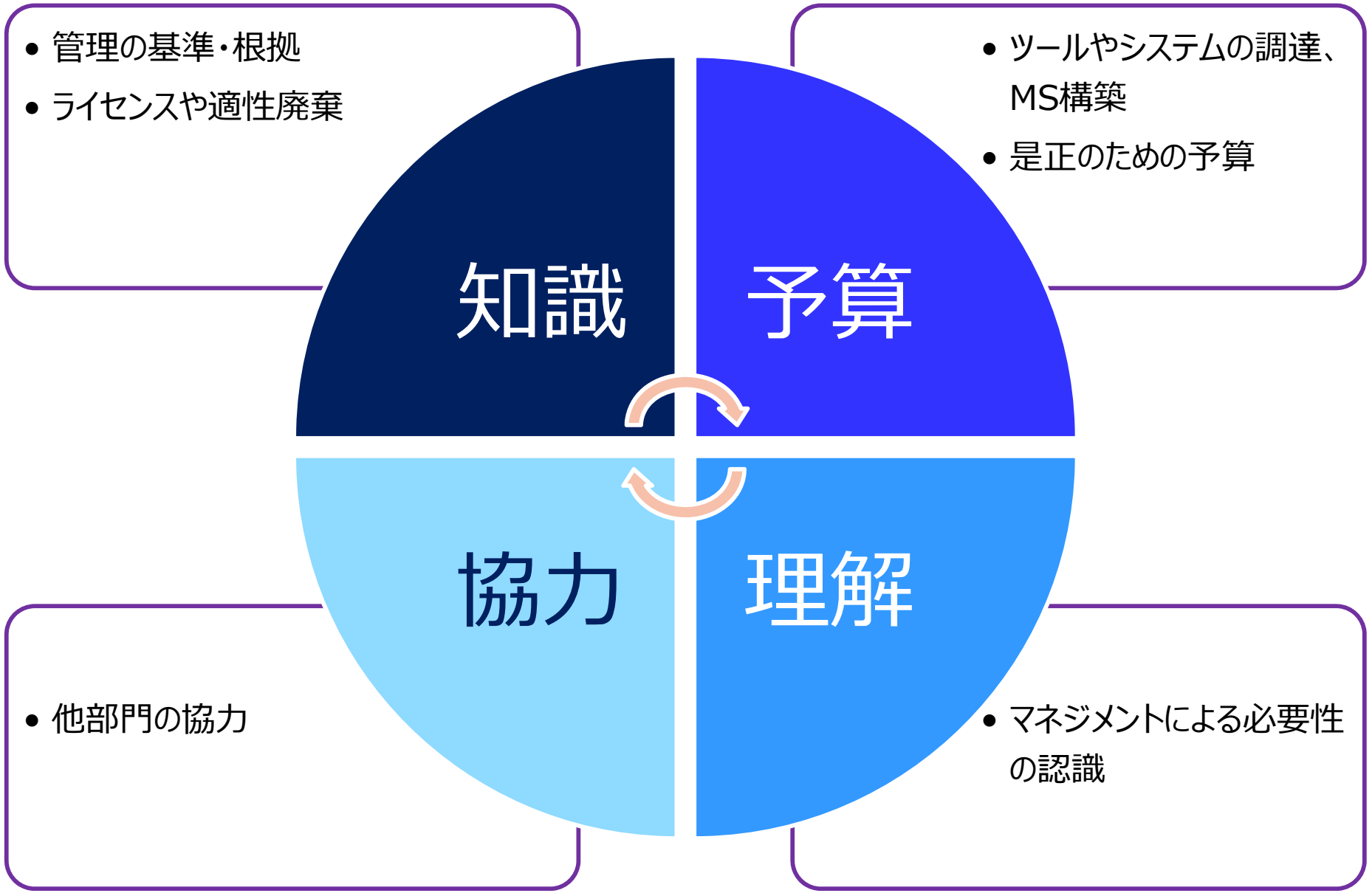
IT資産管理の「これから」



SAMAC
一般社団法人 IT資産管理評価認定協会

まとめ

IT資産管理に望まれるモノ



適切なIT資産管理の実現のために

適切なIT資産管理の知識

必要なIT資産管理のシステム

- インベントリーツール
- 台帳システム
- マネジメントシステム

適切な専門サポート

- 特に導入後３年間がポイント

そのために「リスク」と、（できれば）「メリット」を可視化すること

一般社団法人IT資産管理評価認定協会