SAMAC
一般社団法人IT資産管理評価認定協会

仮想化・クラウドにおける
具体的なリスク検討項目例

IT資産管理評価認定協会
仮想化・クラウド検討WG
2018年6月8日

はじめに

SAMAC　仮想化･クラウド ワーキンググループの活動について

SAMACには、各種活動方針やガイドライン等を定めるために組織されるワーキンググループ（WG）が複数あります。

仮想化･クラウドWGでは、従来のソフトウェア資産管理（SAM）の手法では対応が困難な場合もある、仮想化およびクラウド環境においてのソフトウェア資産管理について研究し、情報提供ができるよう、日々活動しています。

他のWGの活動、SAMAC主催セミナーなどの詳細は、
http://www.samac.or.jp/activity/をご参照ください。

仮想化・クラウド環境での管理台帳

仮想化・クラウドで必要な管理台帳とリスクアセスメント

仮想化・クラウドでのリスクアセスメント管理表の目的

クラウドサービスおよび仮想化環境はこれまでの「単なるハードウェア、ソフトウェアの数や種類の管理」といった「従来のIT資産管理」の捉え方では管理しきれません。また、IT資産管理で実施してきたリスクアセスメントだけでは仮想化やクラウドサービスが保有するリスクを見つけることはできません。仮想化・クラウドでのリスクと、リスク対策のために管理したい項目についてご紹介します。

前半

仮想化・クラウド取り組みのためのリスクアセスメント

クラウドサービスや仮想化を利用することによるリスクの認識・利用を検討

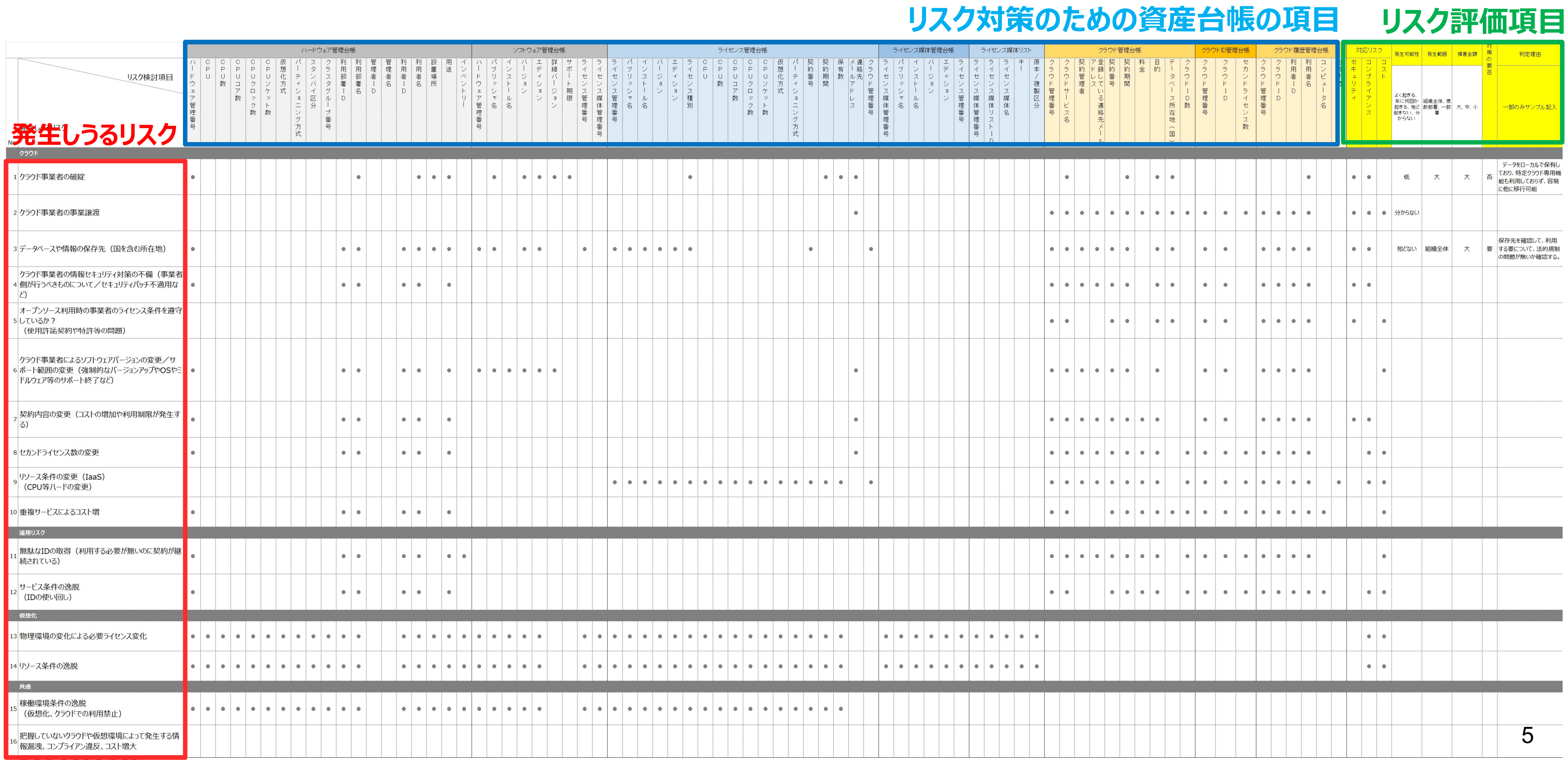
後半

仮想化・クラウドにおける具体的なリスク検討項目例

リスクを考えて管理しなければいけない項目の洗い出しと検討。

リスクアセスメントの項目について

クラウド・仮想化リスクアセスメント管理表は16の発生しうるリスク、リスク評価項目、リスク対策として管理したい資産管理台帳の項目を1つにまとめました。管理者はリスク評価を行って、クラウドサービスや仮想環境をどのように管理していくのか検討していただければと思います。



一般社団法人IT資産管理評価認定協会

発生しうるリスク

	クラウド
1	クラウド事業者の破綻
2	クラウド事業者の事業譲渡
3	データベースや情報の保存先（国を含む所在地）
4	クラウド事業者の情報セキュリティ対策の不備（事業者側が行うべきものについて／セキュリティパッチ不適用など）
5	オープンソース利用時の事業者のライセンス条件を遵守しているか？（使用許諾契約や特許等の問題）
6	クラウド事業者によるソフトウェアバージョンの変更／サポート範囲の変更（強制的なバージョンアップやOSやミドルウェア等のサポート終了など）
7	契約内容の変更（コストの増加や利用制限が発生する）
8	セカンドライセンス数の変更
9	リソース条件の変更（IaaS）（CPU等ハードの変更）
10	重複サービスによるコスト増

	運用リスク
11	無駄なIDの取得（利用する必要が無いのに契約が継続されている）
12	サービス条件の逸脱（IDの使い回し）
	仮想化
13	物理環境の変化による必要ライセンス変化
14	リソース条件の逸脱
	クラウド・仮想化共通
15	稼働環境条件の逸脱（仮想化、クラウドでの利用禁止）
16	把握していないクラウドや仮想環境によって発生する情報漏洩、コンプライアン違反、コスト増大

管理項目の一覧

ハードウェア管理台帳	ハードウェア管理番号
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	スタンバイ区分
	クラスタグループ番号
	利用部署ID
	利用部署名
	管理者ID
	管理者名
	利用者ID
	利用者名
	設置場所
	用途
	インベントリー
ソフトウェア管理台帳	ハードウェア管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	詳細バージョン
	サポート期限
	ライセンス管理番号
	ライセンス媒体管理番号

ライセンス管理台帳	ライセンス管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス種別
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	契約番号
	契約期間
	保有数
	連絡先:メールアドレス
	クラウド管理番号
ライセンス媒体管理台帳	ライセンス媒体管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス管理番号
ライセンス媒体リスト	ライセンス媒体管理番号
	ライセンス媒体リストID
	ライセンス媒体名
	キー
	原本/複製区分

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

ハードウェア管理台帳

ハードウェア管理台帳	ハードウェア管理番号
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	スタンバイ区分
	クラスタグループ番号
	利用部署ID
	利用部署名
	管理者ID
	管理者名
	利用者ID
	利用者名
	設置場所
	用途
	インベントリー
ソフトウェア管理台帳	ハードウェア管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	詳細バージョン
	サポート期限
	ライセンス管理番号
	ライセンス媒体管理番号

SAMAC
一般社団法人 IT資産管理評価認定協会

管理項目

ハードウェア管理番号

Q：クラウドサービスの管理にハードウェア情報は必要？
リスク①クラウド事業者の破綻にハードウェア情報は必要？

A：必要です。

該当するクラウドの利用者がわかるだけでは不十分です。クラウドサービスを利用する際にクライアントにインストールして利用するサービスなどは、どのPCでクラウドサービスを利用しているのか把握することが必要。PCが1人1台のみの環境であれば、利用者とPCはある程度紐付きますが、そうでなければ管理しておく必要があります。

クラウドサービス利用者が使っている端末を特定

利用者IDだけでもいいと考えがちだが、PCを複数台持っている場合でも、
どのPCで利用しているのか把握しておきたい

・アカウントを持っている人全員にどのPCで使っていますか？と聞くのは大変
・クラウドサービスを利用している端末がわかれば、リスクへ対策もしやすい考えやすい

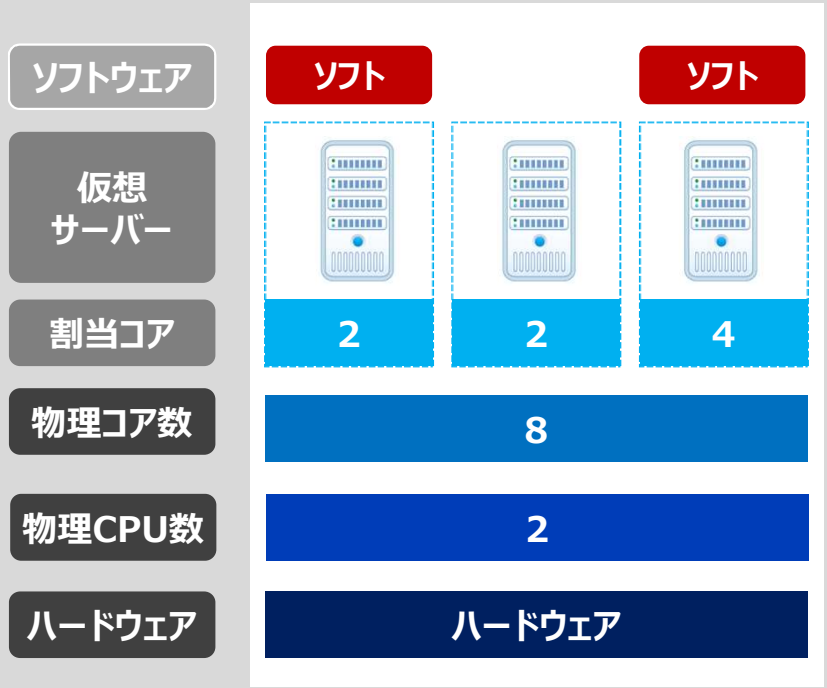
SAMAC
一般社団法人 IT資産管理評価認定協会

ハードウェア管理台帳：CPU,CPU数,コア数,クロック数,ソケット数

ハードウェア管理台帳	ハードウェア管理番号
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	スタンバイ区分
	クラスタグループ番号
	利用部署ID
	利用部署名
	管理者ID
	管理者名
	利用者ID
	利用者名
	設置場所
	用途
	インベントリー
ソフトウェア管理台帳	ハードウェア管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	詳細バージョン
	サポート期限
	ライセンス管理番号
	ライセンス媒体管理番号

CPU数やコア数、クロック数は
主に仮想環境の管理の際に必要な項目

仮想環境例



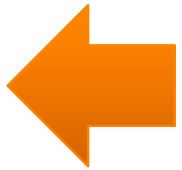
仮想環境で利用するライセンスの把握のためにも必要。

リスク⑬　物理環境の変化による必要ライセンスの変化(仮想化)

サーバーOSの多くは物理サーバーのコア数を元に必要ライセンス数が決まります。サーバーをリプレイスしてCPU数が増加したり、仮想環境でCPUのコア数割り当てが変更されている場合があります。

(仮想化) 物理環境が変化する例

- Windows Server 2016を12コアライセンスで購入して利用していたが、仮想サーバーのCPUが社内で勝手に割り当てを変えられていて、ライセンス違反になっていた。
- SAつきのWindows Server 2013は無償で2016にアップグレードできる。Windows Server 2013はCPUライセンスだが、Windows Server 2016はコアライセンスで算出。SAがあるから無償でライセンスが取得できる、と思っていてもバージョンアップをすると必要なライセンスが変わる場合もある。
- ハードウェアをリプレイスしたら、コア数も必ず増えるのでライセンス数の追加が必要。



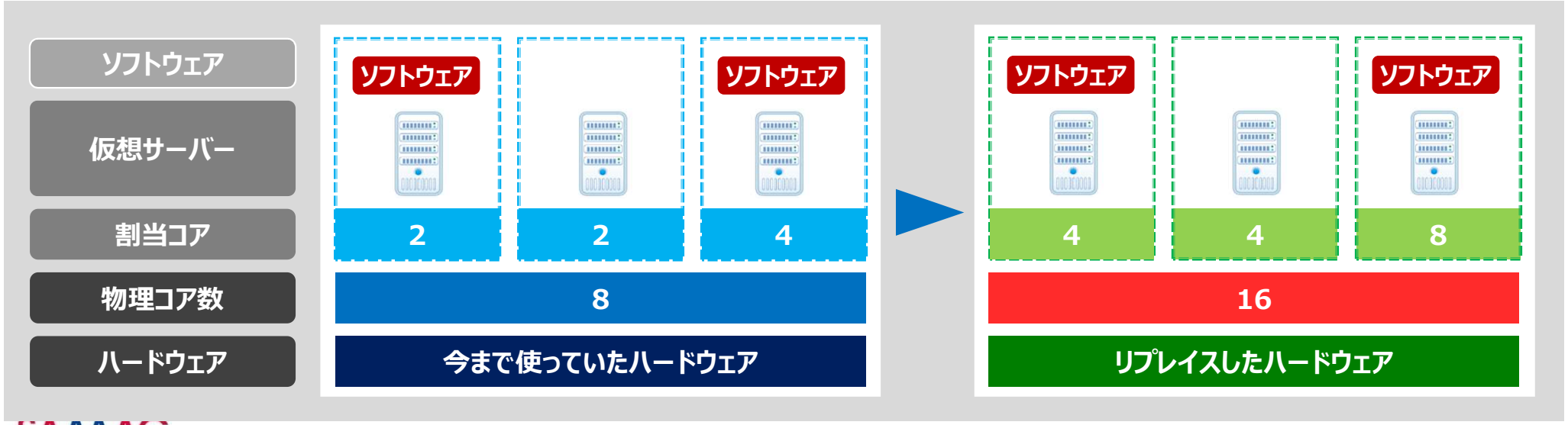
リスク：⑮ 物理環境の変化によるライセンスの変化

Q：ハードウェアをリプレイスしたら必要なライセンス数は変化する？

A： **仮想コア/プロセッサ数型でライセンスを算出していたら・・・**

仮想サーバーに割り当てたコア数が必要ライセンス数となる場合でライセンス数を計算していた場合・・・

以前のサーバー	2	＋	4	＝ 6コア分相当必要
リプレイスしたハードウェア	4	＋	8	＝ 12コア分相当必要



ライセンス管理台帳

ライセンス管理台帳	ライセンス管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス種別
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	契約番号
	契約期間
	保有数
	連絡先:メールアドレス
	クラウド管理番号
ライセンス媒体管理台帳	ライセンス媒体管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス管理番号
ライセンス媒体リスト	ライセンス媒体管理番号
	ライセンス媒体リストID
	ライセンス媒体名
	キー
	原本/複製区分

SAMAC
一般社団法人 IT資産管理評価認定協会

管理項目

CPU, CPU数, CPUコア数, クロック数など･･･

ライセンス管理台帳	ライセンス管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス種別
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	契約番号
	契約期間
	保有数
	連絡先:メールアドレス
	クラウド管理番号
ライセンス媒体管理台帳	ライセンス媒体管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	ライセンス管理番号
ライセンス媒体リスト	ライセンス媒体管理番号
	ライセンス媒体リストID
	ライセンス媒体名
	キー
	原本/複製区分

ハードウェアでCPU数などを管理したのと同様に保有ライセンスの管理にも必要

これまで

デバイス1台につき1本、というライセンス形態

これから

仮想化環境が進み、ライセンス管理台帳で管理が必要な項目が増加。ライセンス形態が複雑化し、保有しているライセンスは単に1本・2本と表すだけでは管理できなくなっています。

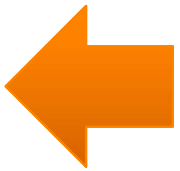
SAMAC
一般社団法人 IT資産管理評価認定協会

リスク⑬　物理環境の変化による必要ライセンスの変化(仮想化)

サーバーOSの多くは物理サーバーのコア数を元に必要ライセンス数が決まります。サーバーをリプレイスしてCPU数が増加したり、仮想環境でCPUのコア数割り当てが変更されている場合があります。

(仮想化) 物理環境が変化する例

- Windows Server 2016を12コアライセンスで購入して利用していたが、仮想サーバーのCPUが社内で勝手に割り当てを変えられていて、ライセンス違反になっていた。
- SAつきのWindows Server 2012は無償で2016にグレードできる。
  Windows Server 2012はCPUライセンスだが、Windows Server 2016はコアライセンスで算出。SAがあるから無償でライセンスが取得できる、と思っていてもバージョンアップをすると必要なライセンスが変わる場合もある。
- ハードウェアをリプレイスしたら、コア数も必ず増えるのでライセンス数の追加が必要。



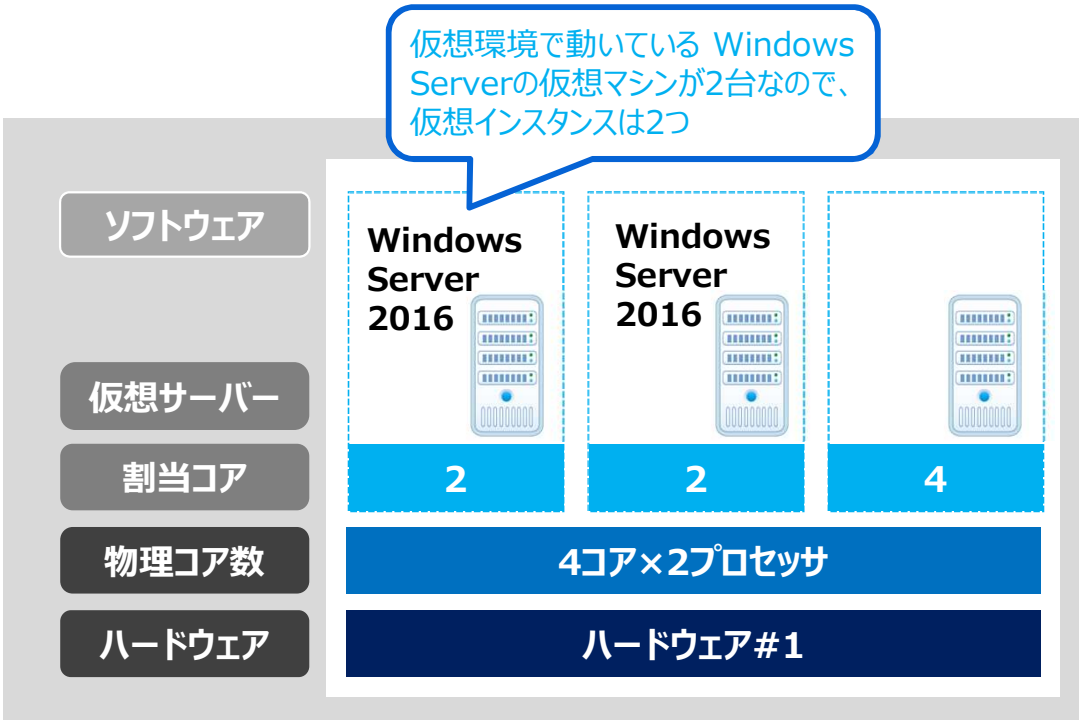
SAMAC
一般社団法人 IT資産管理評価認定協会

①Windows Server 2016のライセンス

Widows Server 2016 :

ライセンス利用条件

① ライセンスの単位は2コア単位
② 物理サーバー１台あたり最低16コアライセンス分必要
③ 物理CPU1つあたり最低8コア分ライセンスが必要（物理CPU数は最低2つとして算出）
④ 物理サーバーに割り当てるライセンスで仮想マシン(仮想インスタンス)2つまで利用可能



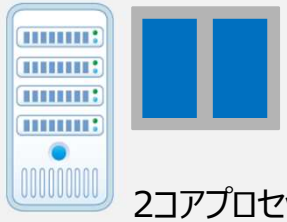
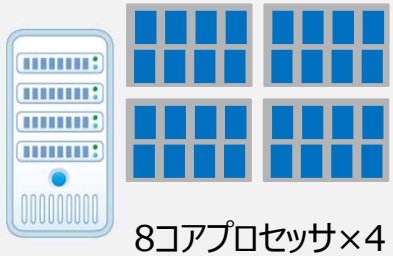
左の構成の場合：

・物理サーバーのコア数が8だが
最低16コア分のライセンスが必要　…②
・1つのCPUに4コアしかないが、
1CPUに最低8コアライセンス分×2必要　…③
・仮想インスタンスが2つ　…④

→16コア分のライセンス
(1ライセンス2コア＝8ライセンス)を購入

SAMAC
一般社団法人 IT資産管理評価認定協会

②Windows Server 2016のライセンス（コアライセンス）

物理サーバーの構成	Windows Server 2012/2012 R2			Windows Server 2016		
	必要なライセンス数 プロセッサライセンス数	仮想インスタンス数		必要なライセンス数 （コアライセンス）	仮想インスタンス数	
		Datacenter	Standard		Datacenter	Standard
 2コアプロセッサ× 1	1	無制限	2	16 (2コアパック ×8)	無制限	2
 4コアプロセッサ×2	1	無制限	2	16 (2コアパック ×8)	無制限	2
 8コアプロセッサ×4	2	無制限	4	32 (2コアパック ×16)	無制限	2
Standard でさらに2つの仮想インスタンスを実行したい	上記＋ 1	–	上記＋2	上記＋×2	–	上記＋2

SAMAC
一般社団法人 IT資産管理評価認定協会

③Windows Server 2016のライセンス(仮想インスタンス)

Windows Server 2008 R2, 2012と 2016 Standard Editionでは、
実行可能な仮想インスタンス数が異なります。

エディションとバージョン		ライセンス形態	仮想インスタンス数
Windows Server 2008	Standard	プロセッサライセンス	1ライセンスにつき１
	Enterprise		1ライセンスにつき４
	Datacenter		無制限
Windows Server 2012	Standard	プロセッサライセンス	1ライセンスにつき２
	Datacenter		無制限
Windows Server 2016	Standard	コアライセンス	物理サーバ上の全ての物理コアをカバーするごとに２。**仮想インスタンスを増やすには同じ数のコアライセンスを追加購入。（コアライセンスごとに最大2つの仮想マシンではない）**
	Datacenter	コアライセンス	無制限

Standard Editionの場合、2012まではプロセッサライセンスを1ライセンス追加購入するごとに、仮想インスタンスを2つずつ増やせましたが、Windows Server 2016からは単に最低購入数分のライセンスを追加するだけでは仮想インスタンスを増やせません。

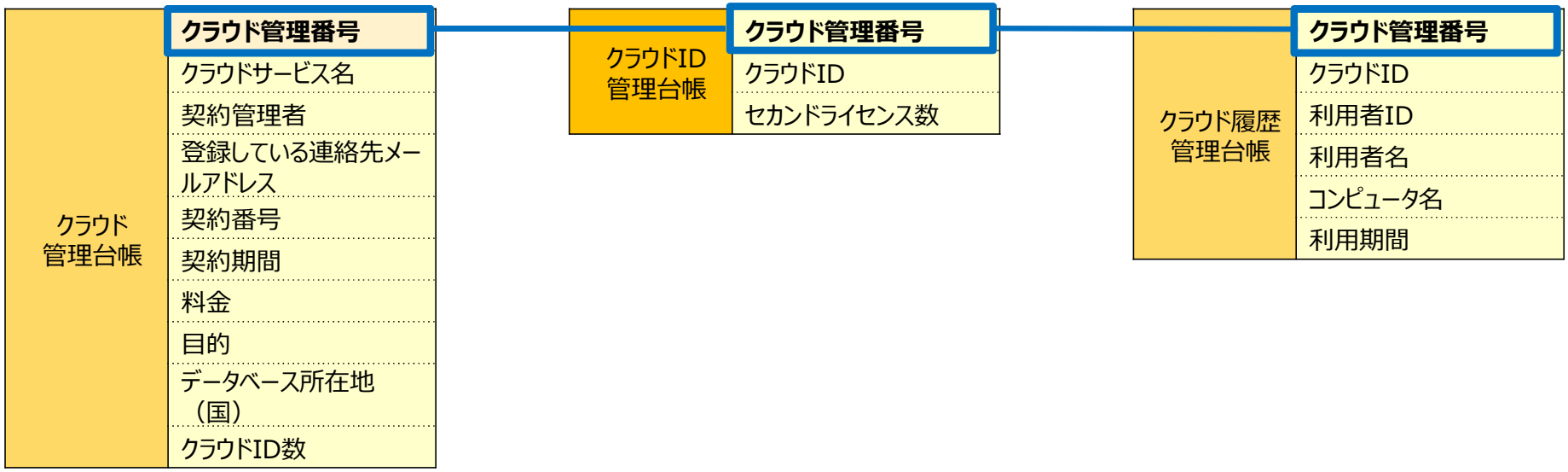
SAMAC
一般社団法人 IT資産管理評価認定協会

クラウド管理台帳

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

クラウド管理台帳の構成

どんなクラウドサービス　　誰が使っているか　　誰が何を使っているか



クラウド管理番号	利用しているクラウドサービスごとにふられる台帳上の番号
クラウドサービス名	「Azure」などのクラウドサービス名を入れたり、Azureでも各部署やプロジェクトごとに利用している場合はそれぞれが識別できるような名称を記載
クラウドID	クラウド上ユーザーを識別するID。Office365ならMicrosoftアカウントが該当。
利用者ID	社員番号など（同姓同名の識別など）
利用者名	利用している人の名前
セカンドライセンス数	Office 365などセカンドライセンスがあるサービスで必要

管理項目

利用者と契約管理者

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

利用者と契約管理者

クラウドサービスの管理は、管理者だけでなく、利用者、契約管理者など複数必要です。

サーバー

＝情報システム部

クライアントPC

＝ユーザー部門の利用者

クラウドサービス

＝ユーザー部門の管理職？利用者？
情報システム部の管理者？
毎月の支払い担当者

SAMAC
一般社団法人 IT資産管理評価認定協会

同じクラウドサービスでも管理者はまちまち

管理者は情報システム部門だけではないので・・・

情報システム部門以外に、ユーザー部門や個人が契約・運用していたり、利用者がクラウドサービスとして認識していないなど、全容の把握は容易ではありません。

IaaS, PaaSなら・・・

計画・設置・運用・バックアップなどは情報システム部が実施。

情報システム部

仮想サーバーなどは情報システム部管理がほとんど

SaaSなら・・・

情報システム部だけでなく、ユーザー部門や個人も契約・利用。

情報システム部

ユーザー部門

営業部の名刺管理システム

個人

メモ帳管理システム

管理項目

登録している連絡先メールアドレス

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

登録している連絡先メールアドレス

クラウドサービスの契約内容が変更になり、コスト増加や利用制限が発生。そのときに提供されるサービスや価格の変更はメールで連絡されることがほとんど。

会社で契約しているクラウドサービスに
登録しているそれぞれのメールアドレスは
わかっていますか？？

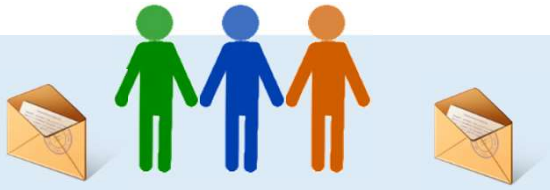
- 情報システム部の担当者の個人メール
- 情報システム部の複数人が受信できるメーリングリスト
- クラウドサービスを主に使っている部署の担当者の個人メール
- 購買部門の担当者の個人メール

ルールを決めてないと
意外とバラバラ・・・

SAMAC
一般社団法人 IT資産管理評価認定協会

管理項目：登録している連絡先メールアドレス

メールアドレスの登録は大事



クラウドサービスの管理者や契約者として登録するメールアドレス宛には、クラウドサービス事業者から様々な連絡がきます。事業譲渡や価格変更のお知らせ、価格変更のお知らせなど、クラウドサービスのリスクとして上がっているものに多く関わります。

- **情報システム部の担当者の個人メール** ▶見落とし・退職・異動
- **情報システム部の複数人が受信できるメーリングリスト** ▶○
- **クラウドサービスを主に使っているユーザー部門の担当者の個人メール**
  - ▶見落とし・退職・異動の問題。
  - ▶セキュリティの関連のお知らせなどは重要度がわからず放置される可能性もあり。
- **購買部門の担当者の個人メール** ▶担当者に転送してくれる？

情報システム部で持っているメーリングリストなどを登録して、複数人で受信できるのが理想

リスク⑦　契約内容の変更

多くのクラウドサービスの契約条項には、事業者の都合で契約内容が変更される場合があります。
契約内容の変更は事前にメール等で連絡されてきます。

・提供サービスの変更
・価格変更
・これまで無料で提供されていたものが有料化される　など・・・

クラウドサービス月額料金値上げの例

マイクロソフト社の「サービスプロバイダーライセンスアグリーメント(SPLA)」料金改定にともない、同社の提供しているマイクロソフト社のランセンスが含まれるサービスの月額料金を値上げ。

【対象サービス一覧】　　月額料金（税別）

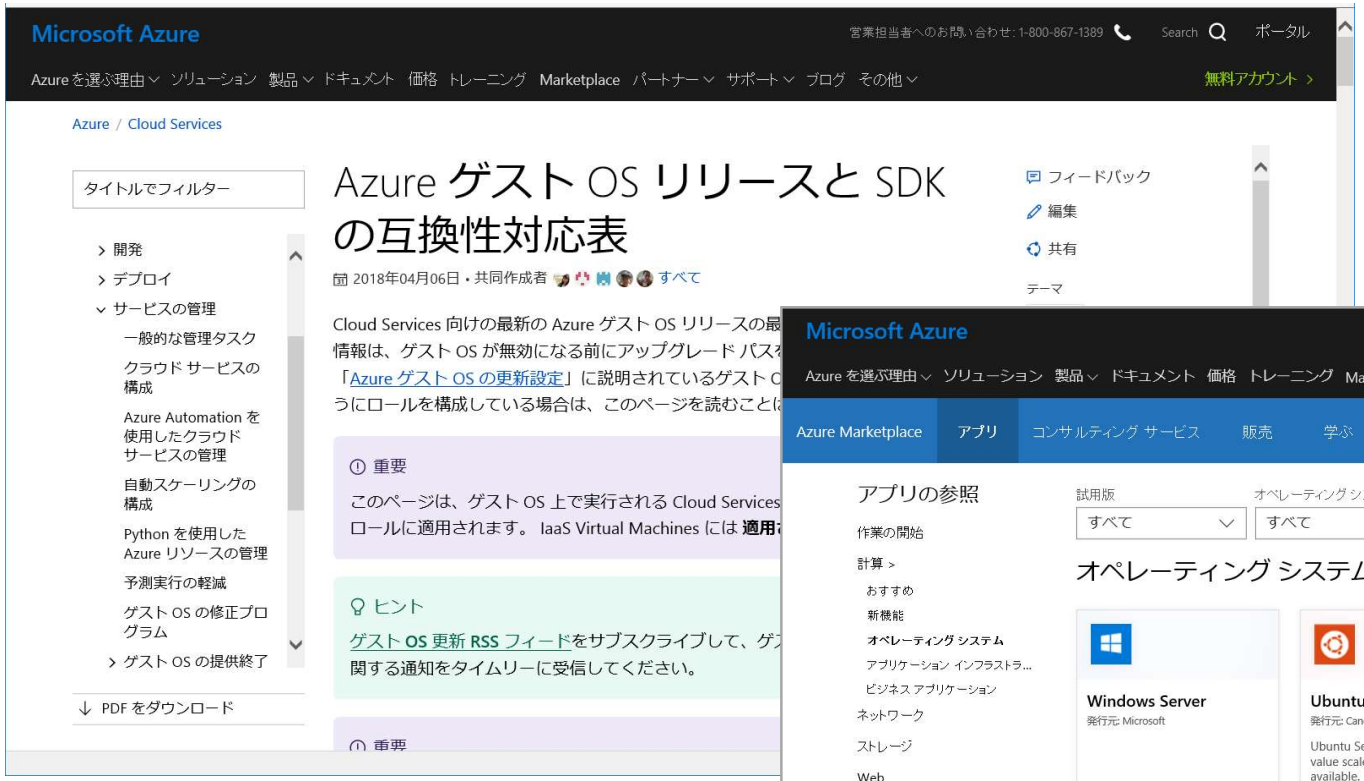
	サービス名	月額料金	
		新料金 2018 年 10 月以降	旧料金 2018 年 9 月まで
1	Windows Server RDS ライセンス	700 円	600 円
2	Microsoft Office Standard & RDS ライセンス	2,500 円	2,400 円
3	Microsoft SQL Server ライセンス(SAL)	2,400 円	2,200 円
4	Microsoft SQL Server2012（Windows Server 2012 R2）	54,400 円	52,400 円
5	Microsoft SQL Server2012（Windows Server 2008 R2）（100GB）	54,400 円	52,400 円
6	Microsoft SQL Server2012（Windows Server 2008 R2）	52,000 円	50,000 円

クラウドサービス事業者からの変更連絡を必ず受信して展開できるメールアドレスが必要。

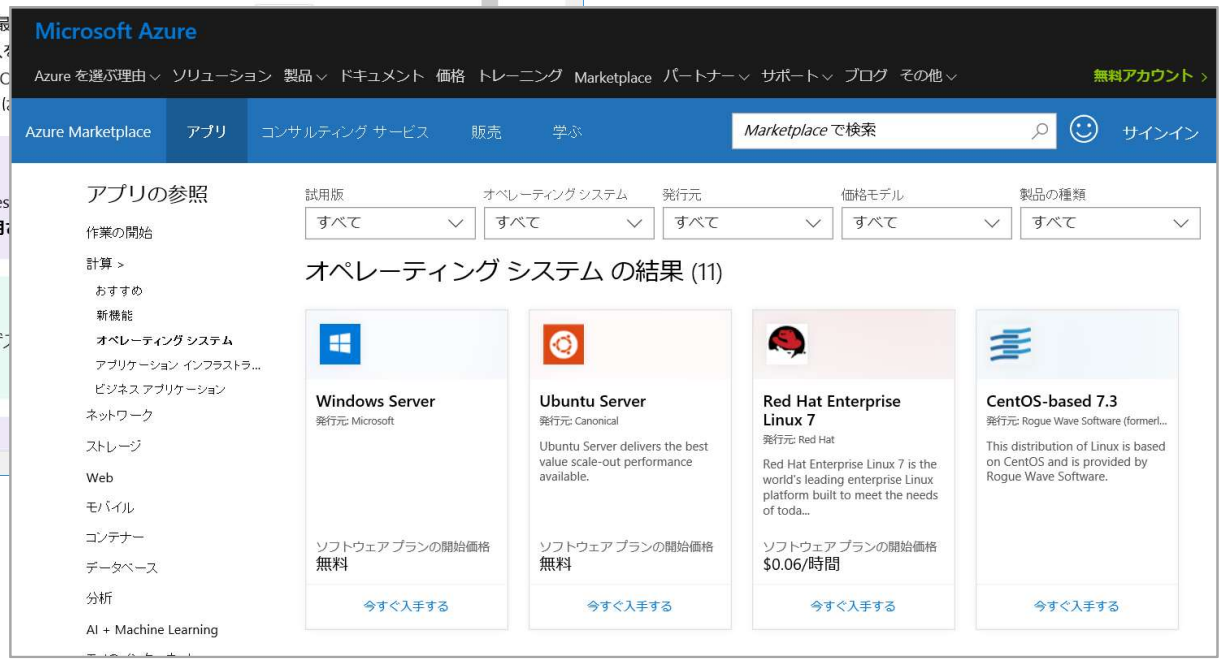
クラウドサービス事業者から変更連絡があれば、契約管理者(必要があれば利用者にも)に速やかに連絡するために利用者や契約管理者の管理が必要です。

リスク⑥
クラウド事業によるソフトウェアバージョンの変更/サポート範囲の変更

クラウド事業者によるソフトウェアバージョンの変更や強制的なバージョンアップが行われる場合もあります。また、PaaSではミドルウェアのサポート終了による影響も検討が必要です。



▼Azure上で利用できるソフトウェアの一覧



管理項目

クラウド管理台帳：目的

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

何のために利用しているクラウドサービスなのかを記載

メールサーバー用、ファイルサーバー用、ファイル転送サービス用、バックアップ用、名刺管理システム、など利用目的を記載します。

1つのクラウドサービスでも、何のために利用するのかは部署によって異なる場合があります。

SAMAC
一般社団法人 IT資産管理評価認定協会

リスク⑩：重複サービスによるコスト増

似たようなクラウドサービスを自社ですでに契約していることに気づかず複数契約していてコストが増加

調査をしてみたら・・・

似たようなサービスがある

1 OneDrive があるのにDropboxを契約している部署がある・・・

Office 365 を利用するとOneDrive（オンラインストレージ）を利用できる（社内利用も許可している）。なのにDropboxを別途契約している。

目的を確認すると、Dropboxを社外の人とのファイル転送サービスとして利用している

→ 似たような機能をもつクラウドサービスを契約する場合もあります。
棚卸や見直しの際に「これって重複じゃない？」とならないよう、目的に記載。

SAMAC
一般社団法人 IT資産管理評価認定協会

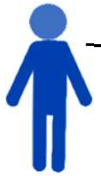
リスク⑩　重複サービスによるコスト増

似たようなサービスがある

2 Office 365 E3　と　オンプレのOffice Professional 2016

一見重複して無駄なサービスの契約に見えるが・・・

オンプレのOfficeからOffice 365への移行を行い、ほとんどの社員がOffice 365へ移行完了。



→**常に最新版にアップデートされるOffice 365**を使って問題ない社員は、オンプレのOfficeをアンインストール（ライセンスの権利を手放す）

→**旧バージョンのOffice でないと利用できないシステムがある。**

旧バージョンのAccessでないと動かない社内の業務システム（受注管理システムなど）があっても、Office 365はダウングレードができません。オンプレのOffice Professionalはダウングレード権があるため、旧バージョンを利用したい社員のみオンプレのOfficeを利用する

SAMAC
一般社団法人 IT資産管理評価認定協会

管理項目

クラウド管理台帳：契約期間

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

クラウドサービスの切り替えや変更などの時に必要な項目

クラウドサービスの契約期間

- 月額でいつでもやめられるクラウドサービス
- 年間契約のクラウドサービス
  ・・・途中でやめると残りの期間分の料金が戻ってこない
- 月額払いでも契約期間があり、解約金が発生する

→リスク対策として新しいサービスを検討したり、
いままでの契約内容の変更を考える際に必要となる項目。

SAMAC
一般社団法人 IT資産管理評価認定協会

管理項目

データベース所在地

クラウド管理台帳	クラウド管理番号
	クラウドサービス名
	契約管理者
	登録している連絡先メールアドレス
	契約番号
	契約期間
	料金
	目的
	データベース所在地（国）
	クラウドID数
クラウドID管理台帳	クラウド管理番号
	クラウドID
	セカンドライセンス数
クラウド履歴管理台帳	クラウド管理番号
	クラウドID
	利用者ID
	利用者名
	コンピュータ名
	利用期間

クラウドサービスに保存しているデータは日本にある？

国内クラウドサービス事業者と契約していても、実際のデータは海外のサーバーに保存されていたり、自分のデータがどの国に設置されたサーバに保存されているかを特定できない場合があります。

契約したクラウドサービス事業者は国内企業でも、
クラウドサービスのためのサーバーは海外に設置

災害対策としてクラウドサービスのデータ保存場所を国内のリージョンだけでなく海外にも保存したい

SAMAC
一般社団法人 IT資産管理評価認定協会

リスク：データベースや情報の保存先（国外）

米国愛国者法（USA Patriot Act）

2001年9月11日に発生した同時多発テロ事件を受け、捜査機関の権限の拡大や国際マネーロンダリングの防止、国境警備、出入国管理、テロ被害者への救済などについて規定。捜査機関は金融機関やプロバイダの同意を得れば、裁判所の関与を求めることなく操作を行うことができることを規定

→ アメリカのサーバにデータを保存する場合は、政府機関の捜査権限が大きい

→ クラウドサービスを利用する場合、仮想的に分離された環境であっても、他ユーザと物理的に同一のサーバ機器などを共有している場合があり、他ユーザが捜査を受けると、自社もシステム停止などの影響

一般データ保護規則（General Data Protection Regulation）

EU内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁止。

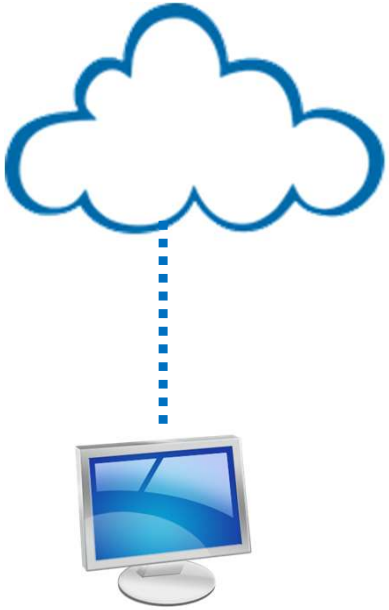
→ EUの住民情報が1件でもデータベースに入っているとGDPRに従った対応が必要。
データの保存先がEU外でも適用されます。

データが海外に保存される場合は、アメリカの愛国者法やGDPRの問題がある。クラウド事業者の選定時には、データの保存先も確認しておく。

ハードウェア管理台帳：インベントリ

ハードウェア管理台帳	ハードウェア管理番号
	CPU
	CPU数
	CPUコア数
	CPUクロック数
	CPUソケット数
	仮想化方式
	パーティショニング方式
	スタンバイ区分
	クラスタグループ番号
	利用部署ID
	利用部署名
	管理者ID
	管理者名
	利用者ID
	利用者名
	設置場所
	用途
	インベントリー
ソフトウェア管理台帳	ハードウェア管理番号
	パブリッシャ名
	インストール名
	バージョン
	エディション
	詳細バージョン
	サポート期限
	ライセンス管理番号
	ライセンス媒体管理番号

ここではハードウェア管理台帳のインベントリを指していますが、クラウドサービスの利用状況や把握を含めたインベントリの収集についてご紹介します。



SAMAC
一般社団法人 IT資産管理評価認定協会

クラウドサービスのインベントリ情報の把握

「CASB（Cloud Access Security Broker：キャスビー）の利用」

企業におけるクラウドサービス利用が進む中で、従業員のクラウドサービス利用をコントロールするための企業向けサービスの総称。

CASBの4つの役割

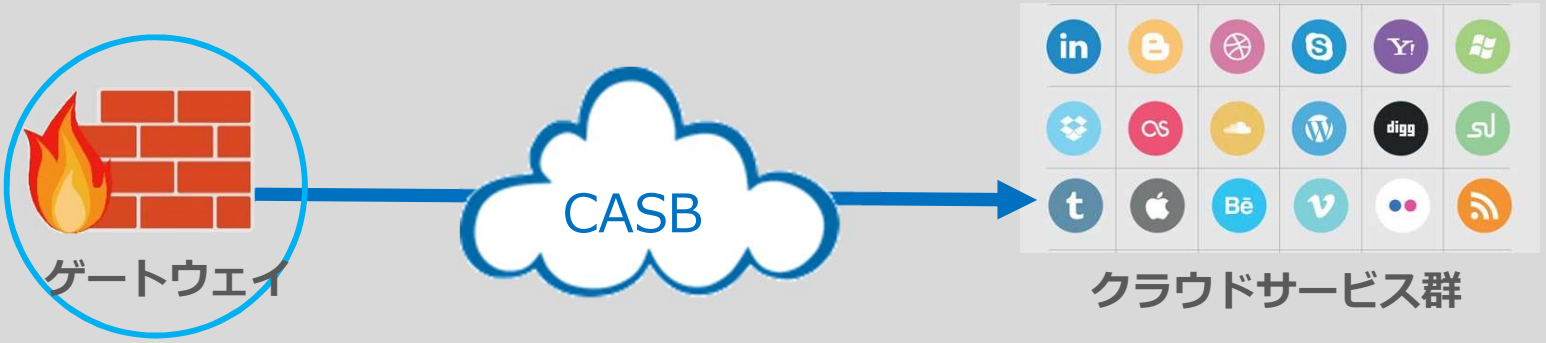
①可視化：社内ユーザーがどのようなSaaSを使っているのかをIT管理者が監視できるようにする
②データセキュリティ：アクセス権限の逸脱や機密情報の持ち出しをチェック/ブロックする
③コンプライアンス：セキュリティに関する基準やポリシーを満たしていることを監査する
④脅威防御：セキュリティ脅威の検出/分析や防御を行う

シャドーITの実態や「怪しいサービス」などのリスクを可視化し、クラウドサービスを管理された状態にすることで、コンプライアンス要件が満たされる状態にする。重複するサービスや無駄なIDを発見するのにも活用できます。

CASBでインベントリ情報を集める方法

ゲートウェイで確認

クラウドサービス用にゲートウェイを用意し、そこを通過するトラフィックから情報を収集する方法(ゲートウェイで許可しているクラウドサービス以外を遮断するシステムもあり)



クライアントPCで確認

ユーザーが使用するデバイスにエージェントをインストールして、情報収集や制御を行う方法。（モバイルデバイスでは特定のゲートウェイにトラフィックを送れなくても、エージェント型なら可能）

運用リスク⑫：サービス条件の逸脱（IDの使い回し）

Office 365 などのクラウドサービスでは、アカウントがユーザーごとに発行され、そのユーザー以外は利用できません。クラウドサービスとして提供される名刺管理システムなど、社員全員が利用しないサービスなどでは、「このアカウントで入れるから」と社内でIDの使い回しなどが行われている場合があります。

Q：複数人が同時に使わないなら、Office 365は1ライセンスでいい？

A：人数分必要です。Office 365はどのライセンスもユーザー単位なので、
同時に1人しか使わなくてもライセンスが必要です

運用リスク⑫：サービス条件の逸脱（IDの使い回し）

「使える＝ライセンス違反していない」は誤り。

クラウド環境でおこりやすいライセンス違反

IDやパスワード等でログインして使うクラウドサービスは、**「ログインできたからライセンス違反していない」と考えることは誤り**です。サービス提供者はそこまで把握できていません。

✖ 社内のみで使えるサービスを出先から社内の人に見てもらう

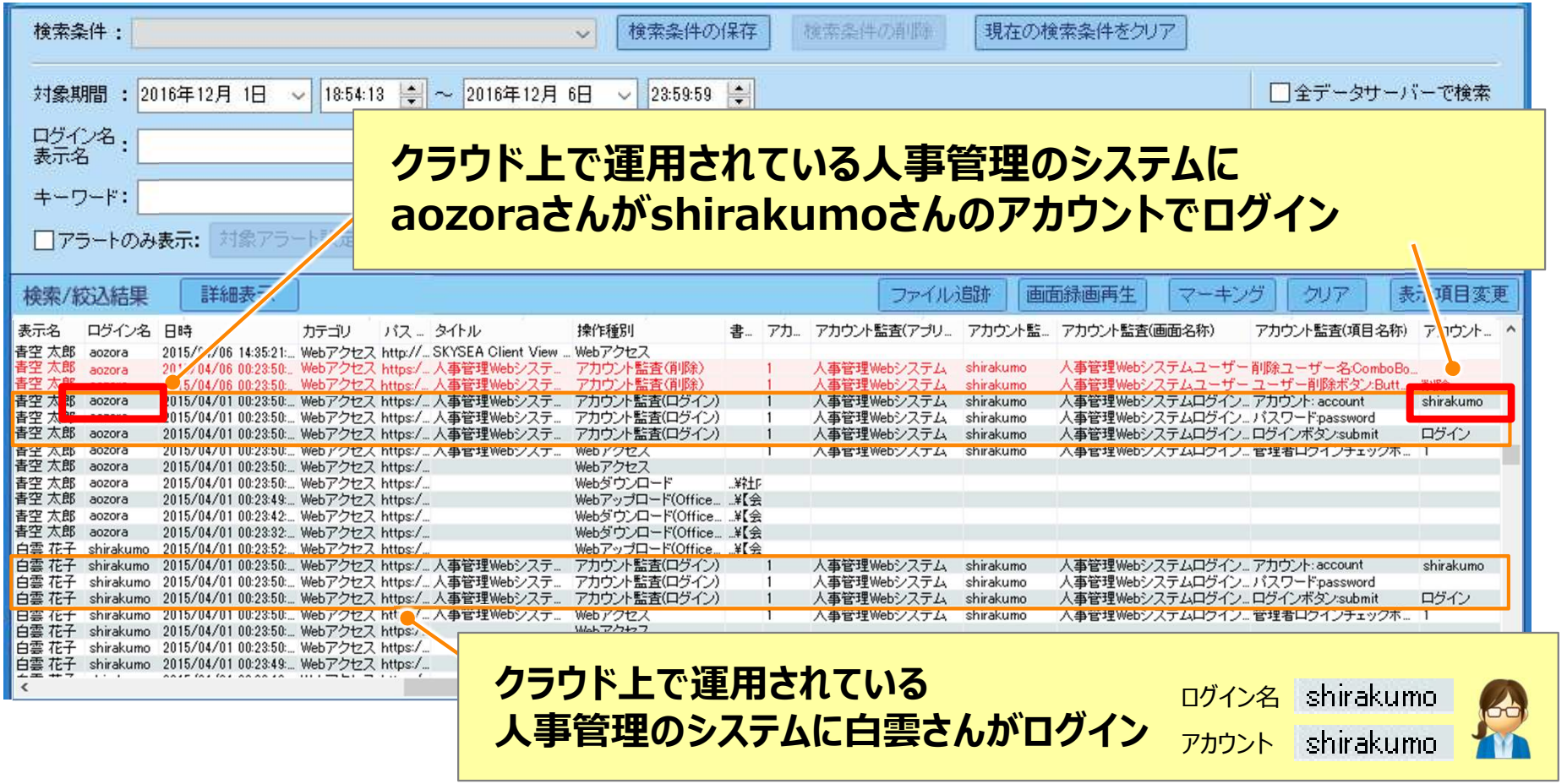
営業部の社員だけが名刺管理サービス(SaaS)を契約。営業マンが外出中に、社内にいるアシスタントにIDとパスワードを教えてデータを見てもらう。

✖ 産休に入る人のアカウントを、代替で来る担当者に使わせる

Aさんが産休に入るので、その間代わりに来る人にアカウントを使ってもらう。

アプリケーションのアカウント取り扱い状況をログから確認

ログ管理のツールなどを利用してアプリケーションへのログオンやユーザーアカウントの作成/削除状況を確認します。



リスク⑯　把握していないクラウドや仮想環境によって発生する情報漏洩、コンプライアンス、コスト増大

把握できていないクラウド・仮想化のため、管理項目に○はつきません。

		ハードウェア管理台帳								ソフトウェア管理台帳								
No	リスク検討項目 発生しうるリスク	ハードウェア管理番号	利用部署ID	利用部署名	利用者ID	利用者名	設置場所	用途	インベントリー	ハードウェア管理番号	パブリッシャ名	インストール名	バージョン	エディション	詳細バージョン	サポート期限	ライセンス管理番号	ライセンス媒体管理番号
16	把握していないクラウドや仮想環境によって発生する情報漏洩、コンプライアン違反、コスト増大																	

管理者が把握していないクラウドサービス

高額なソフトウェアを購入することなく、サービスとして利用した分だけ支払えばいいので、従業員のクレジットカードで決済ができてしまいます。交通費などと同様に経費として申告されてしまえば、組織の中でIT管理者が把握しないままクラウドサービスが使われてしまうことになります。

SAMAC
一般社団法人 IT資産管理評価認定協会

クラウドサービス利用状況/実態の把握の難しさ

社内の誰がクラウドサービスがあることを知っている？

情報システム部で管理なら・・・

情報システム部

仮想環境の管理者と同じ人に調査を依頼

-システム導入時の検討メンバー、業務システム開発・保守部門、ハードウェア管理部門
セキュリティ対応部門、システム運用部門、災害対策検討メンバー、インフラ管理部門、契約担当部門など

ユーザー部門で管理なら・・・

基本的には**管理者権限を持った利用部門・個人に確認**

ユーザー部門

より細かく見るなら・・・

クラウドの利用者(全員)・契約者・管理者も全て把握。

SAMAC
一般社団法人 IT資産管理評価認定協会

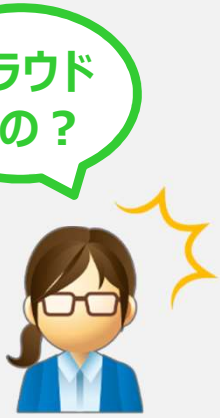
申告漏れのリスクと対処法

申告漏れの一番の原因

利用者がクラウドサービスと認識していない

クラウドサービスと知らずに使っていたが、実はクラウド。

最初にIDとパスワードを入れたけど、その後は使ってないはず･･･



申告のない環境の構築・サービス契約は認めないなどのルール化

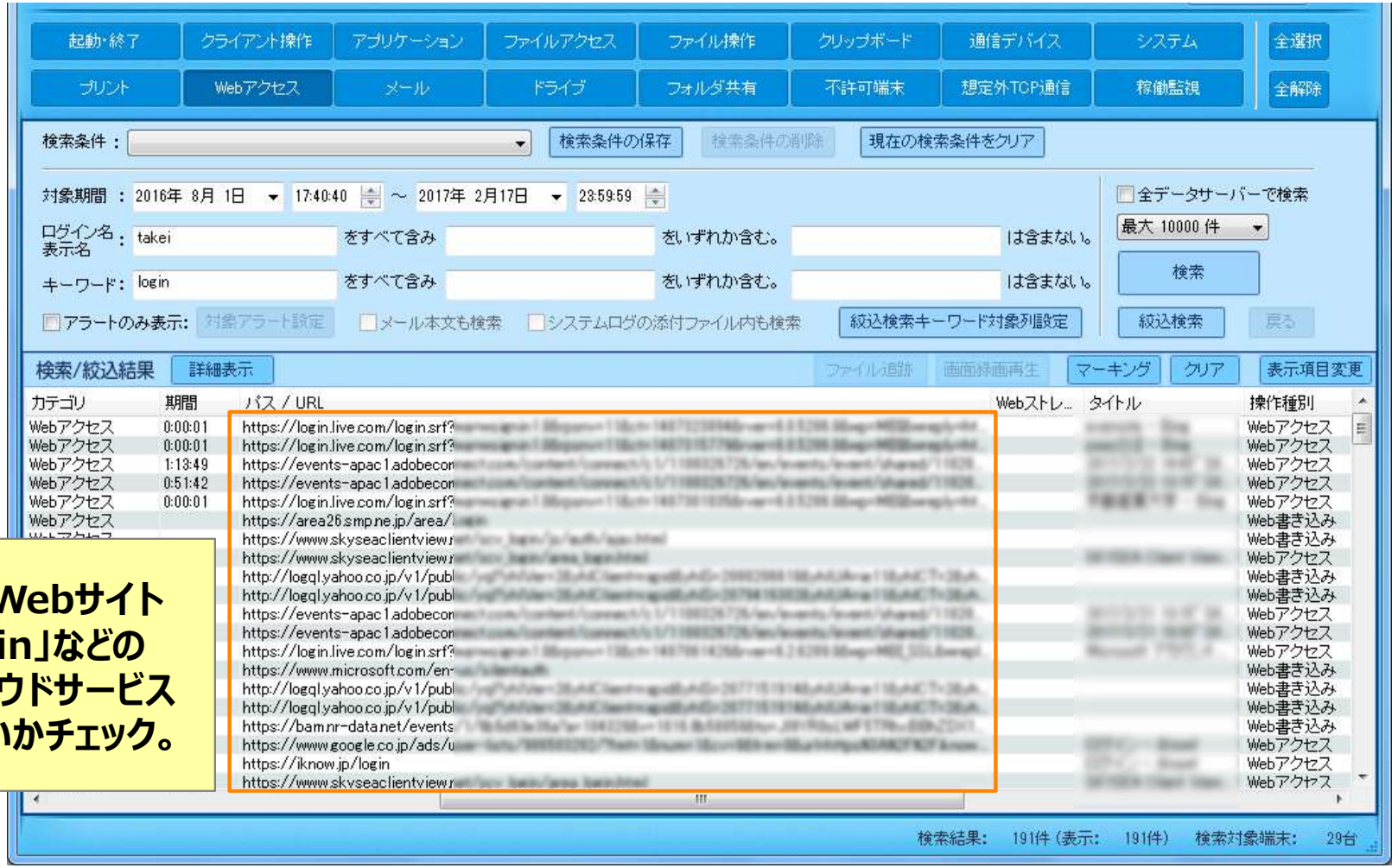
経理部門の支払いデータの活用

物品申請や稟議書のデータを経理からもらう。
クレジットカード払いも多いので、それらしきものを含むように調査。

SAMAC
一般社団法人 IT資産管理評価認定協会

Webアクセスログを確認

Webアクセスログからもクラウドサービスと思えるログを探して詳細を確認できます。



アクセスしているWebサイトの一覧から「login」などのキーワードでクラウドサービスらしきURLがないかチェック。

まとめ

仮想化・クラウドへの流れは今後も加速

今後も仮想化・クラウドへの流れにより、これまで以上に複雑な管理が求められます。

仮想化・クラウド利用時に台帳として管理する項目

当セミナーでは、台帳として管理すべき項目の具体例を、想定されるリスクと共にご紹介しました。

皆様の組織において、「何を管理すればいいのかわからない」「何のために管理すべきか」といった疑問の解消に、今回のセミナーがお役に立てば幸いです。

リスクアセスメントのExcelデータ

仮想化・クラウド検討WG活動報告に掲載しています(予定)
http://www.samac.or.jp/cloud/

SAMAC
一般社団法人 IT資産管理評価認定協会

一般社団法人IT資産管理評価認定協会