令和５年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【はじめに】
今年度のシステム・セキュリティ管理者向け研修について

今年度の研修の構成

開催回	カテゴリ	概要	講師
第１回	オリエン	IT環境における組織の管理	萩原健太 インターバルリンク（株）、(一社)ソフトウェア協会
第２回	基礎	ID管理やアクセス制御 →ITガバナンスと組織管理	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第３回		脅威や脆弱性 →アクセス制御とセキュリティ対策	
第４回		効果的なセキュリティの実現	
第５回	実践	Windows標準機能の活用	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会
第６回		脆弱な機器の守り方	
第７回		インシデントに備える体制	

※内容は変更する場合がございます。

【第3回】システム・セキュリティ管理者向け研修

アクセス制御とセキュリティ対策

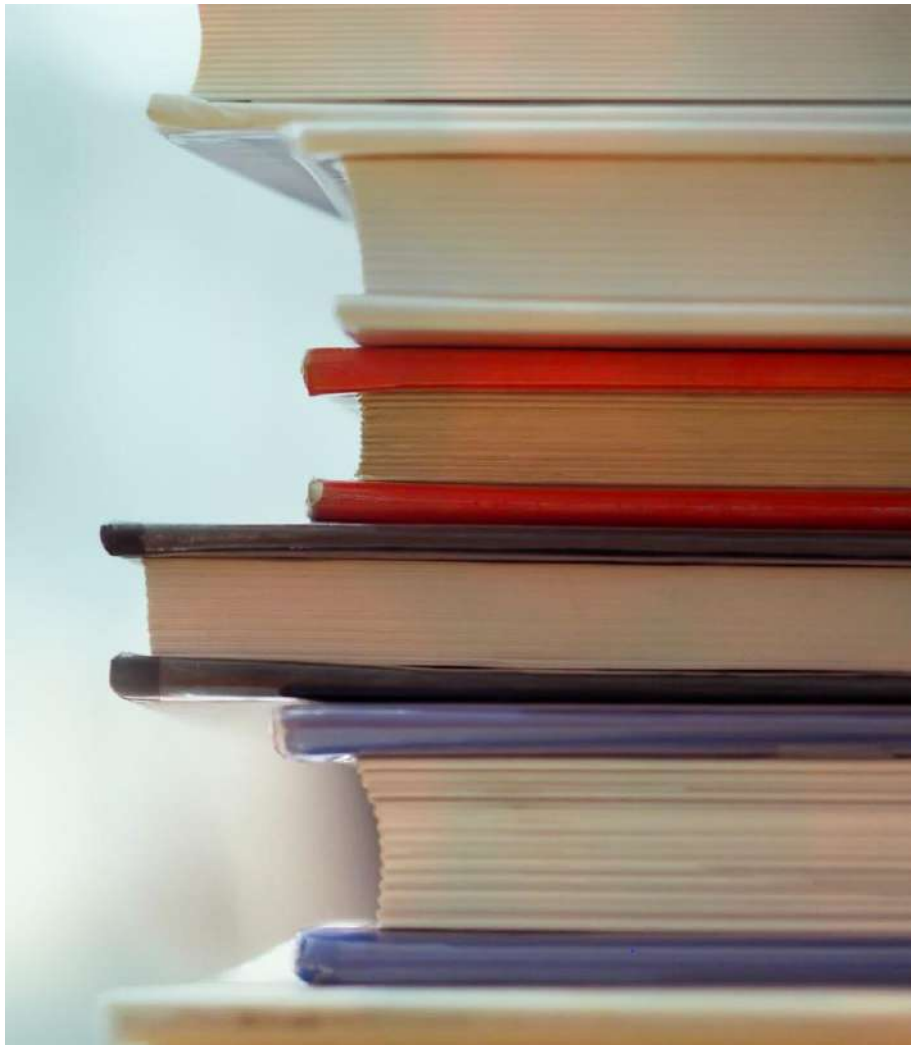
2023年11月2日

日本マイクロソフト株式会社
後藤 昌宏

本セッションのスピーカー

氏名	後藤 昌宏 （ごとう まさひろ）
所属	日本マイクロソフト株式会社 クラウド&AI ソリューション事業本部 モダンワーク統括本部 公共ソリューション営業本部
経歴	医療・公共など業界での経験を活かし、現在は Microsoft 365 の製品を中心とした医療機関・製薬企業のお客様のコミュニケーションを中心とした働き方改革、DXの推進、セキュリティ対策の強化を支援しております。
専門的な知識や知見（保有資格）	Microsoft 365を中心とするクラウドサービス、セキュリティ系サービス

本講座の目的



- 本講座では、組織管理のために一般的な管理の基本的な考え方について理解していただき、システム管理責任者もしくはセキュリティ責任者として、ITベンダーと十分なコミュニケーションができる知識とスキルを身につけていただきます。
- ITベンダーと協力しながら、現場でのさまざまな課題を解決することで、円滑なIT運用を行うことを目的としています。

参照すべき資料

- 厚生労働省
  - **医療情報システムの安全管理に関するガイドライン**
  - 医療機関におけるサイバーセキュリティ対策チェックリスト
  - 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～
- 経済産業省
  - 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
- つるぎ町立半田病院
  - コンピュータウイルス感染事案有識者会議調査報告書
- 大阪急性期・総合医療センター
  - 情報セキュリティインシデント調査委員会報告書

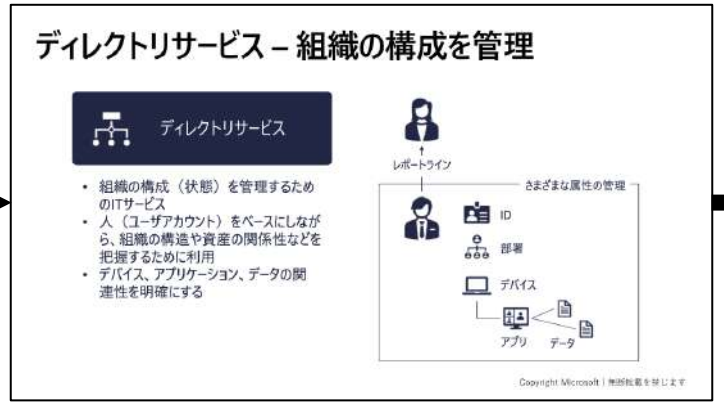
第3回のアジェンダ

1. アクセス制御
2. セキュリティ対策
3. まとめ

各章の構成と学習の進め方

日常的な課題

課題を解決するための知識



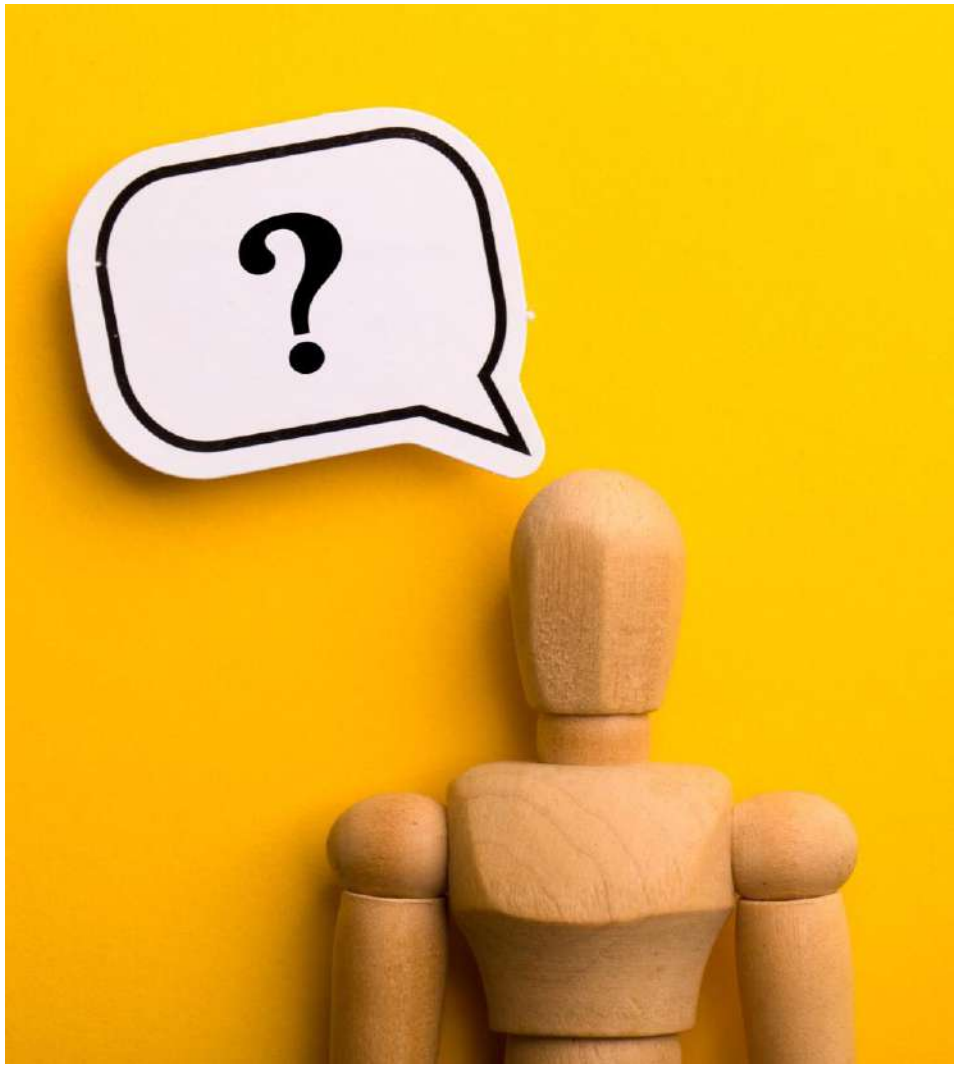
課題の解決例

インシデント報告書

日常的な課題をベースして、まずはみなさんの現在の知識について確認をします。その後、関連する基礎知識について理解していただきます。最後は医療機関で実際に発生した事例をもとに、対策が実践されているかどうかを確認します。

1. アクセス制御

課題〉 情報へのアクセスを許可する



病院内には様々な情報が存在します。

これらの情報は閲覧や編集をしても良い人としてはならない人がいます。

これらの情報を適切に扱うためのアクセス許可を行う場合、どういうことに気をつけたら良いでしょうか？

アクセス制御とは

知る必要性

- すべての情報にはそれを知ることができる人とそうでない人がいます
- 知ることができる人にはスムーズにアクセスできるようにし、知る必要がない人には絶対にアクセスできないようにすることをアクセス制御と言います

アクセス制御の対象

- すべての情報資産に対して適切なアクセス制御が必要になります
- ネットワーク、端末、アプリケーション、データなど

アクセス制御における説明責任

説明責任

- 説明責任（アカウンタビリティ）とは、説明の裏付けを明確にすること。もともとは金銭を支払うための根拠や明細のこと
- 説明する責任は説明義務と呼び、別の意味であることに注意

アクセス制御における説明責任

- いつ、どこで、誰が、どのように、なんの目的で、情報をどのように操作したか
- これらの説明根拠の連鎖によって、適切なアクセス制御であるかどうかを説明することができるようになる
- つまり、これらの情報をログとして取得する必要がある

アクセス制御の種類

物理的アクセス制御

入退室管理
（鍵や専用のカード、警備員による監視）
など

論理的アクセス制御

ネットワーク・
データアクセス管理
など

閉域網の
イメージ？

閉域網とは、直接的にインターネットに
アクセスできないよう制御しているだけ。

適切な
セキュリティ
が必須

機密性の確保の基本はアクセス制御

アクセス制御のプロセス

エンティティの確認を行い、識別子を発行する

識別子の有効性を確認し、認可のフェーズへ進む

適切な権限を付与する

識別 – 主体の確認

エンティティの確認を行い、識別子を発行する

- ユーザ登録の粒度
  - 識別時に確認した内容以上の確認を認証時に行うことはできない
  - パスワードしか登録していないのに、電話番号にコールバックはできないし、デバイスを登録していないのに、デバイスを限定することはできない
- ユーザアカウントの解除
  - ユーザアカウントの解除が行われた場合でも、ログを残しておく必要があるかなどを判断し、ユーザアカウントの設計を行う必要がある

認証 – 資格の確認

識別子の有効性を確認し、認可のフェーズへ進む

- 識別子の有効性の確認
  - 識別時に発行した識別子の有効性について確認する。本人性が必要かはサービスによって異なる
  - 認証によってアクセスが許可されるわけではなく、認可フェーズに進むに過ぎない
- 認証の強化という考え方
  - 認証を強化するという考え方は適切ではなく、認証をより詳細に行うかどうかという考え方が適切
  - なりすましをしにくくするためにはどのような確認方法があるかを検討することが望ましい

認証の三要素

パスワードなどの本人が知っていることをベースにした認証方式

本人所有しているものをベースにした認証方式。スマートフォンにインストールしたアプリなども対象

本人そのものベースにした認証方式。バイオメトリクスの他にも、筆跡なども対象

多要素認証 – Multi Factor Authentication (MFA)

認証の三要素のうち、二要素以上を利用した認証

- キャッシュカードと暗証番号 –
- 口座番号と暗証番号 –
- 暗証番号と3Dセキュアパスワード –
- スマートフォンとパスワード –
- 顔認証とパスワード –

二段階認証とは別の概念

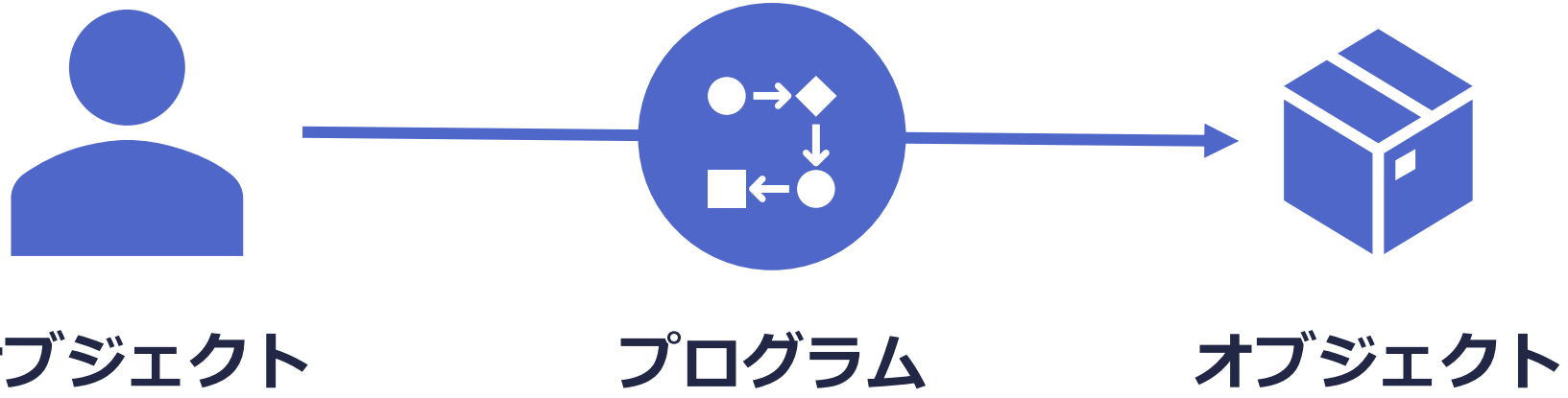
- ワンタイムパスワードパッドなど、毎回のように追加認証を必要とする考え方とMFAは別の概念。パスワードレス環境においてもMFAは有効になる

認可 – 権限の付与

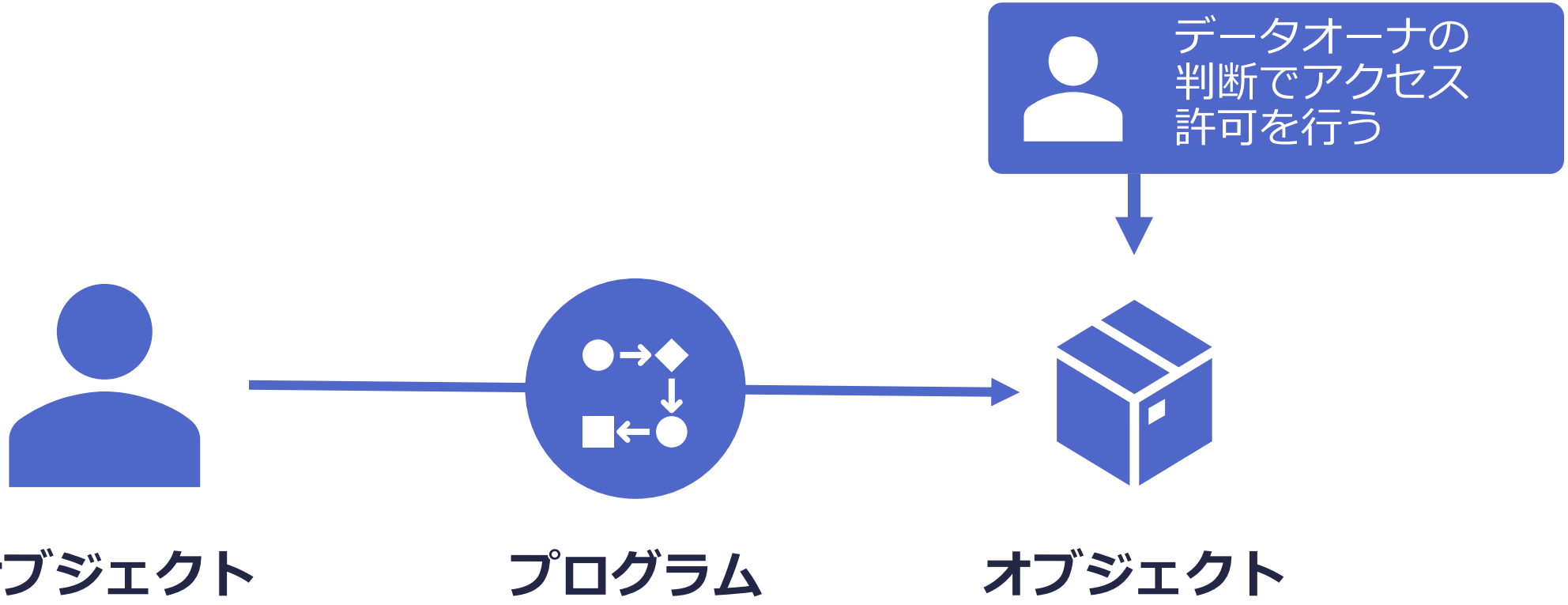
適切な権限を付与する

- 権限の付与
  - 認証によって得られた情報をもとに、オブジェクトに対する権限を付与
  - オブジェクトはデータだけではなく、サービスや通信のこともある
- 権限の付与の方法
  - システムなどへのアクセスには直接アクセスをする場合と、チケットなどを使ったアクセスの方法がある
  - チケットを利用したアクセスにおいては、一つのチケットを利用して、複数のシステムやサービスにアクセスすることも可能になる

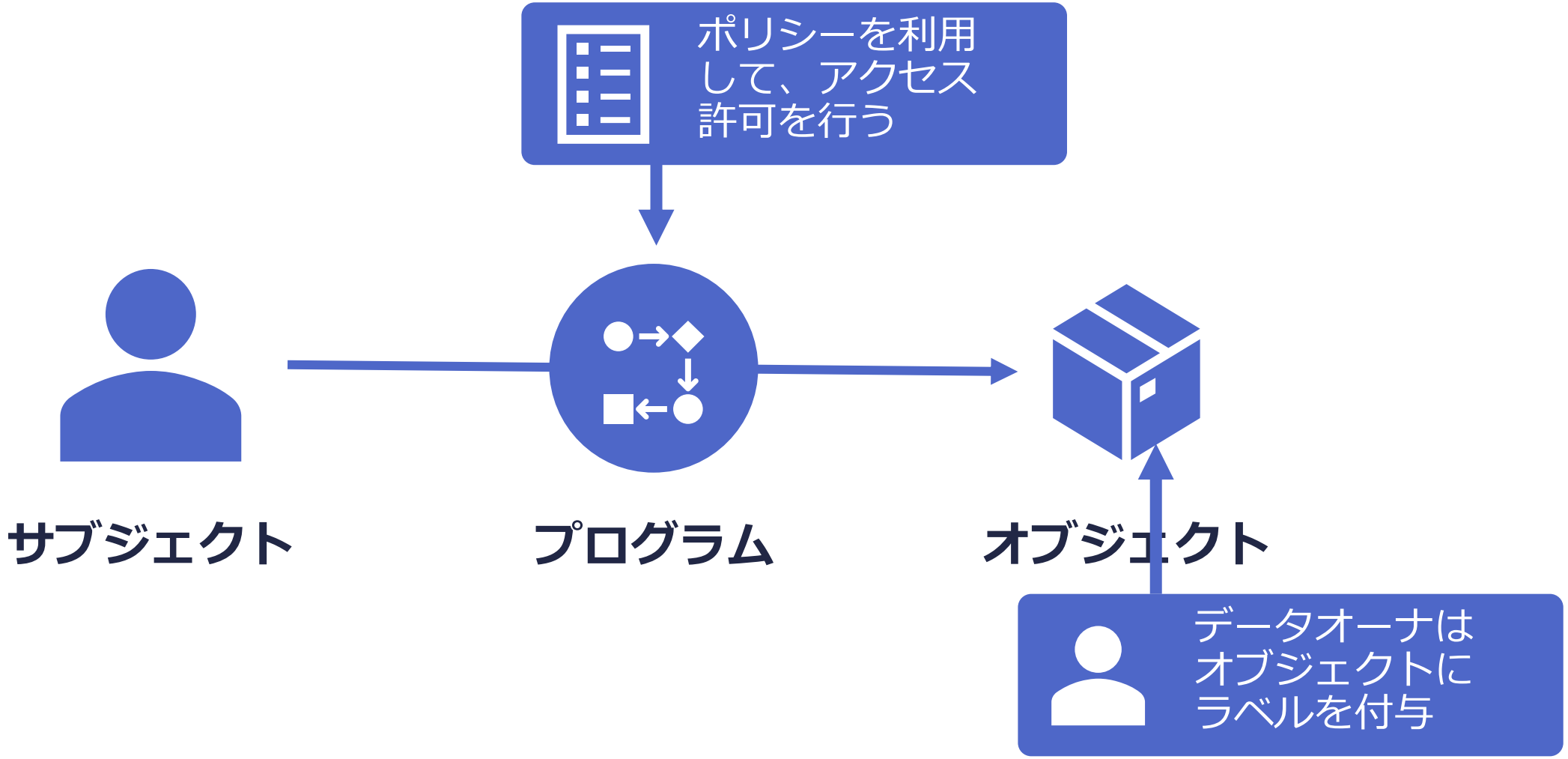
アクセス制御の実装



任意アクセス制御



強制アクセス制御


ポリシーを利用して、アクセス許可を行う
サブジェクト
プログラム
オブジェクト
データオーナはオブジェクトにラベルを付与

アクセスポリシーの種類

ルールを利用したアクセス制御

- ルールベースアクセス制御 – Rule Based Access Control
- 役割をベースにしたアクセス制御 – Role Based Access Control (RBAC)

特別なアクセス制御の考え方

- 非任意アクセス制御 – Non-Discretionary Access Control (NDAC)

粒度の高いアクセス制御

- 属性ベースのアクセス制御 – Attribute Based Access Control (ABAC)

アクセスポリシーを動的に生成する

ゼロトラスト・アーキテクチャの考え方の基本

動的にアクセスポリシーを作成するメリット

- アクセスポリシーが静的（Static,スタティック）に生成されている場合、アップデートが反映されるまで、新たな脅威に対応することができない
- 新しいOSやアプリでは、アクセスポリシーを動的に更新できる仕組みが備わっており、システムの再起動などをしなくてもセキュリティを確保できる

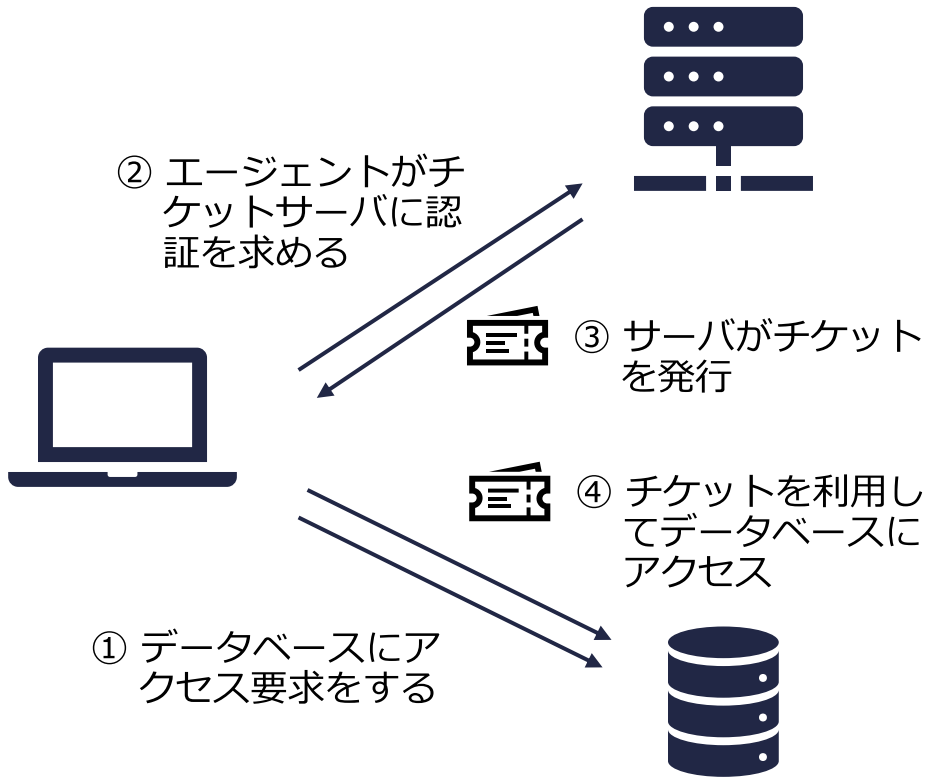
脅威インテリジェンスを活用したアクセスポリシーの生成

- 脅威インテリジェンスを活用することで、他の組織で発生したインシデントの要因となった脅威情報について入手し、対応に必要なポリシー（構成ファイル）を入手することが可能になる

閉域網ではなく、オープンネットワークとして考え（ゼロトラスト思考）で、新しい技術活用を検討

シングルサインオン（SSO）

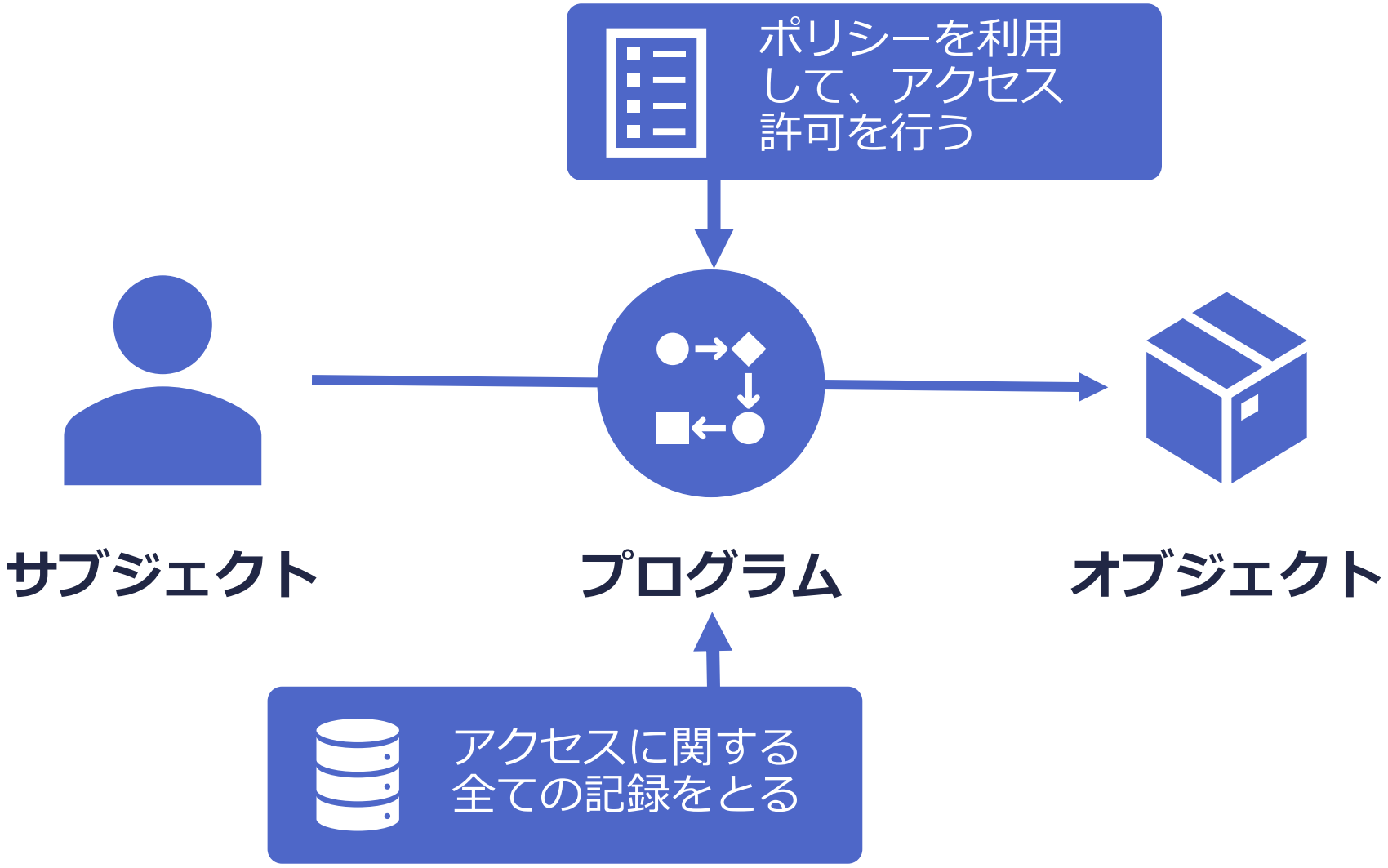
- 一度の認証で複数のシステムやサービスにアクセスする
  - シングルサインオンでは、シングルサインオンサーバを利用したシステム単位に毎回認証を行うものと、チケットを利用した方法がある
- ケルベロス認証
  - チケットを利用したシステムの代表的なものにケルベロスがある
  - ケルベロスは1つのドメイン（レルム）しか管理できないために、それを拡張したSESAMEが開発された



ケルベロスの簡単な仕組み

アクセス制御における説明責任

説明責任を果たすための仕組み



ユーザとエンティティの振る舞いによる検知

ゼロトラスト・アーキテクチャの実現に向けて

ユーザとエンティティのふるまい分析（UEBA）

- UEBA（User and Entity Behavior Analytics）を実現するためにはユーザとエンティティ（デバイスなど）の識別が重要なポイントとなる
- すべてのユーザとエンティティを把握し、それらをベースにログを取得する

そのためにはIDの統合が必要

- システムやサービスごとにID管理を行っていると、UEBAのためのアクセスデータ収集が難しいだけではなく、IDを起点としたログの分析などが困難になる
- UEBAを行うためには、単なるSSOではなく、IDaaSを利用したID管理が必要になる

システムへのアクセス

システムへのアクセスにおける留意点

- システムへのアクセスは共有IDを使わない（共有IDを利用するときには、その利用記録を別途取得する必要がある）
- 認証情報（パスワードなど）を定期的に変更する
- 定期的にログを確認する

システムへのアクセス制御ができていないと

- システム管理者の権限を奪われてしまうと、システム内の全てのデータを閲覧されたり、削除されたりしてしまう
- システム管理者の権限を分割し、全ての権限を持つ管理者アカウントを作成しないことが重要

ファイルへのアクセス

ファイルにパスワードをつける（暗号化）

- ファイルにパスワードをつけることで、パスワードを知っているものしかアクセスできないようにする
- パスワードの受け渡しに十分な注意をしないと、パスワードが漏れてしまうだけでなく、ファイルにつけたパスワードが変更できないためにアクセス制御が破綻する

ファイルに証明書をつける

- Windows 10からはファイルの管理が大きく変わり、Windows Serverのファイルサーバを利用することなく、ファイル単位でのアクセス制御ができるようになった
- ID管理サーバから付与される証明書などを利用してアクセス制御を行う

報告書の読み方

3.2.1 認証認可システムの管理（プロセスの実行/システム管理者/L1）

- 最低半期に一度、すべてのユーザーアカウント、管理者アカウントの使用目的、権限、変更の有無を評価 する。これには、ディレクトリ、Radius、802.1X、WPA、VPN、クラウドサービス、SOAP、Auth、 SMTP-AUTH などが含まれる。

3.2.8 多要素認証の導入（プロセスの実行/システム管理者/L2）

- 組織のすべてのアカウントに可能な限り多要素認証（MFA）を使用する。MFA が使用可能なら PIN は 6 桁以上とする。MFA が使用できない場合は 16 桁以上のパスフレーズを設定する。パスワードはすべてユニ ークでなければならない。

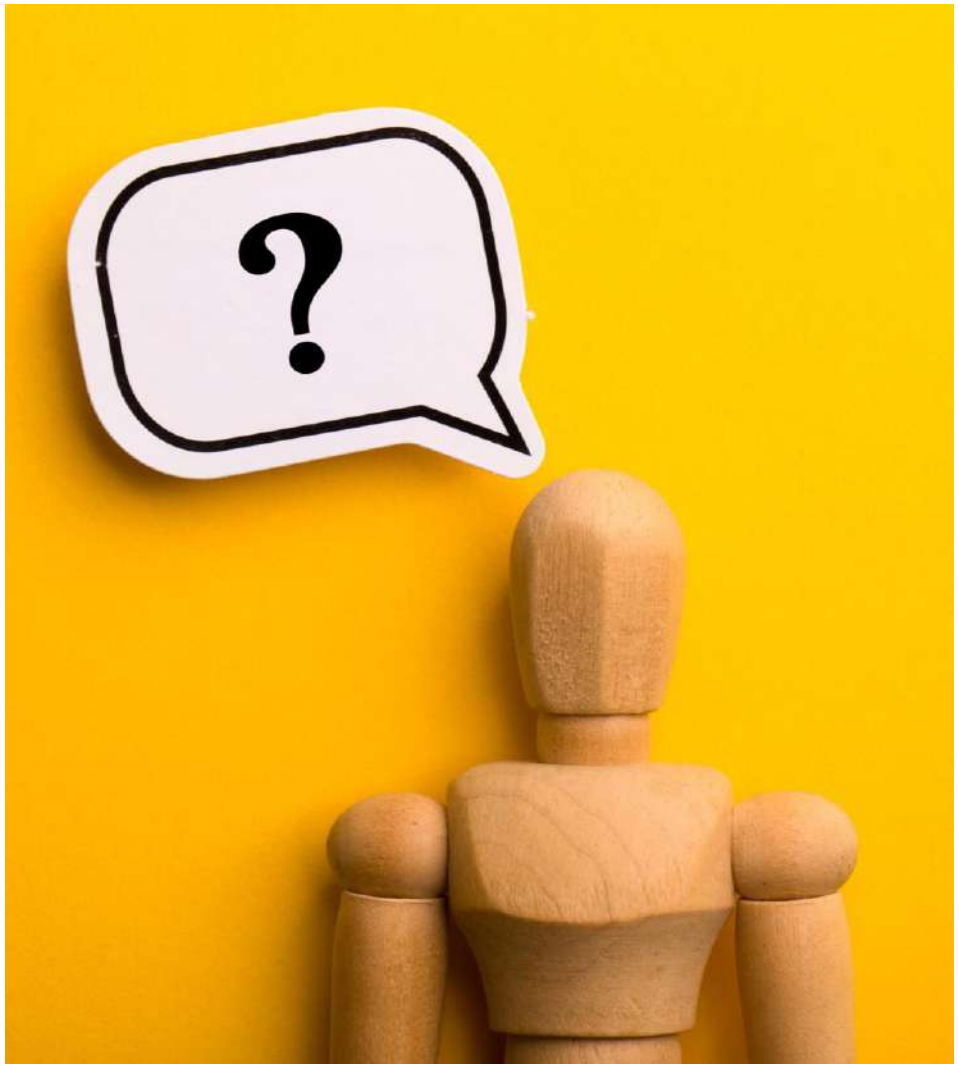
3.3.2 知る必要に基づくアクセス制御（プロセスの実行/システム管理者/L1）

- 組織のデータの特性に基づいた知る必要に基づくアクセス制御を設定する。これにはファイル、データベ ース、アプリケーション、クラウド、サービス等での認証と読取、書込、変更、削除などの操作権限、ログ の取得、バックアップ及び復旧の権限設定が含まれる。

徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書
情報システムにおけるセキュリティコントロールガイドライン
https://www.handa-hospital.jp/topics/2022/0616/report_03.pdf

2. セキュリティ対策

課題〉 セキュリティ対策の必要性

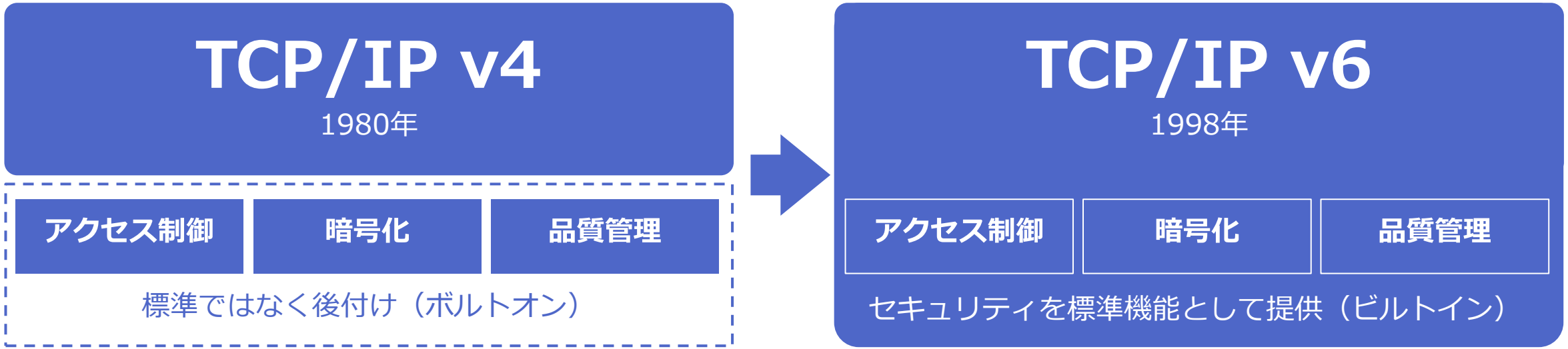


セキュリティ対策は重要であると言われていましたが、これまで「閉域網だから安全」と、閉域網神話でセキュリティ対策を検討してきませんでした。

システムを使う以上セキュリティ対策は必要です。

そもそもセキュリティはどのように考えればよいでしょうか。

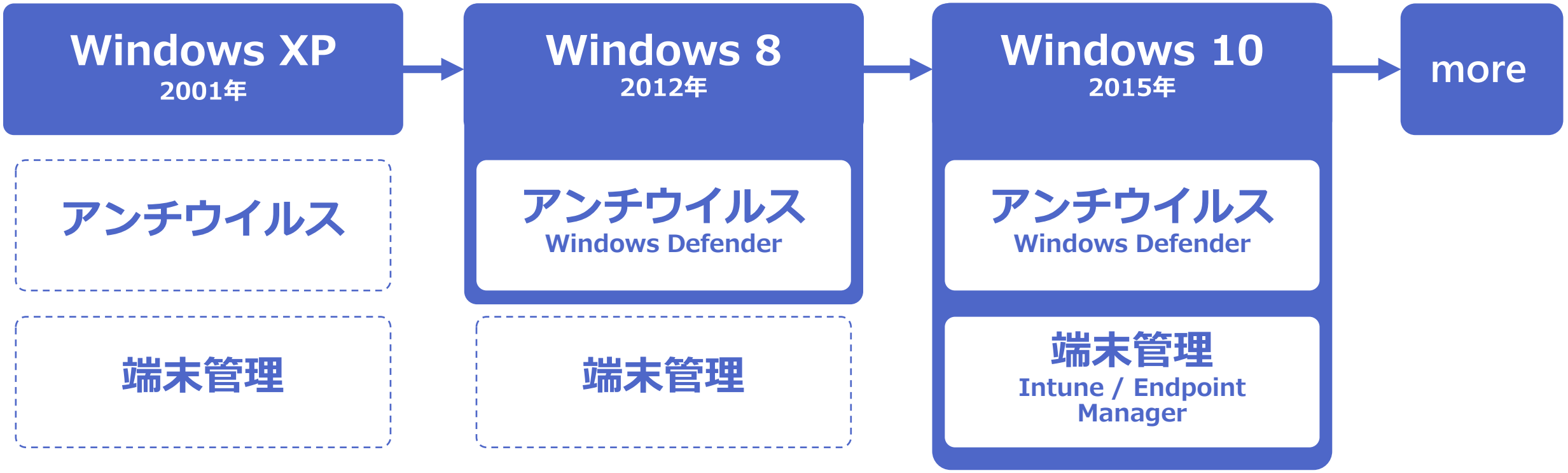
セキュリティ機能のないITシステム



TCP/IP v4は利用者が見える環境での利用を想定していたために、通信の可否だけで、現在求められるセキュリティ機能は搭載されていない。これを後付けにすることで、環境によって実装が異なり、管理が複雑になり、ガバナンスが構築しにくくなっている。

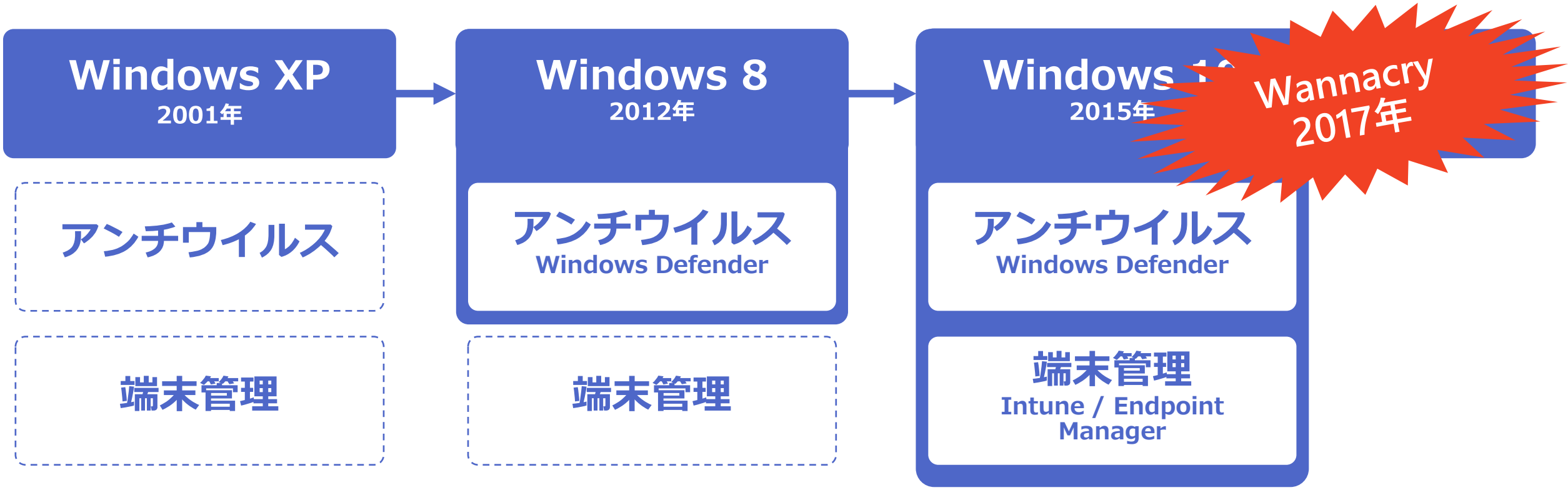
SMTPも1982年から大きな変化なく使われており、もちろんセキュリティ機能は十分ではない。

Windowsのセキュリティ機能の変化



OSにセキュリティ機能が組み込まれることで「独立性がなくなる」というエンジニアもいますが、
独立が必要なのはモニタリング（検査）機能であり、セキュリティは機能として必要なものなので
組み込まれている方が望ましいといえます。

Windowsのセキュリティ機能の変化



OSにセキュリティ機能が組み込まれることで「独立性がなくなる」というエンジニアもいますが、
独立が必要なのはモニタリング（検査）機能であり、セキュリティは機能として必要なものなので
組み込まれている方が望ましいといえます。

一般的なセキュリティの2つの側面

維持
Security

安全な状態を維持する

保護
Protection / Defense

情報資産を攻撃から守る

セキュリティ対策の3つの視点

維持
Security

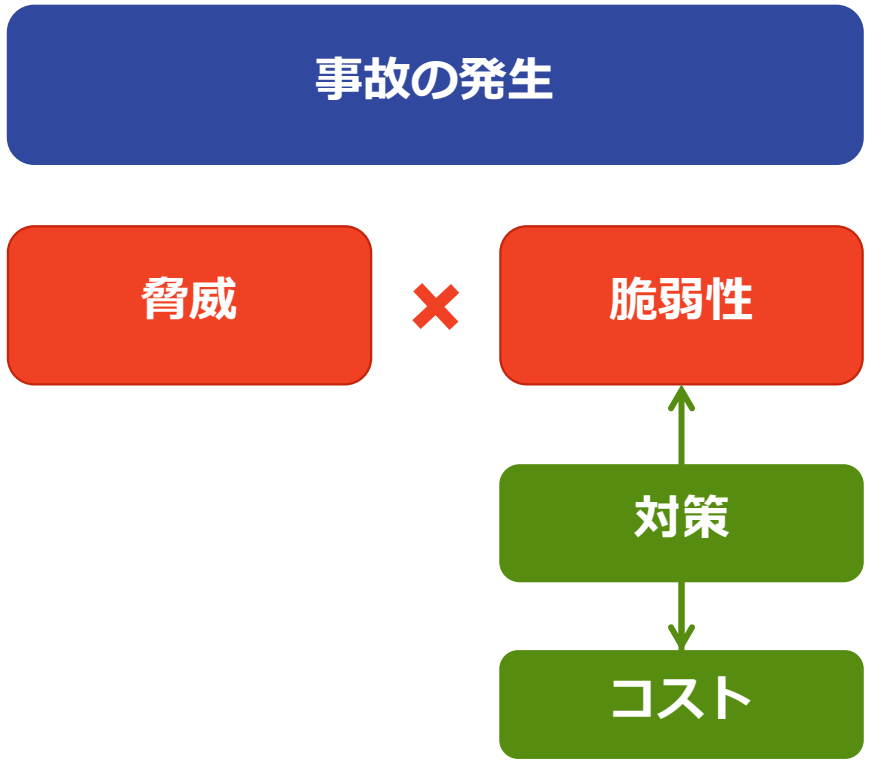
安全な状態を維持する

機密性：Confidentiality
許可されたものだけが情報にアクセスできるような状態にしておくこと

完全性：Integrity
最後に確認された状態から許可なく変更されたり、削除されないようにしておくこと

可用性：Availability
資産やサービスなどを必要な時にいつでも利用できる状態にしておくこと

事故はなぜ起きるのか



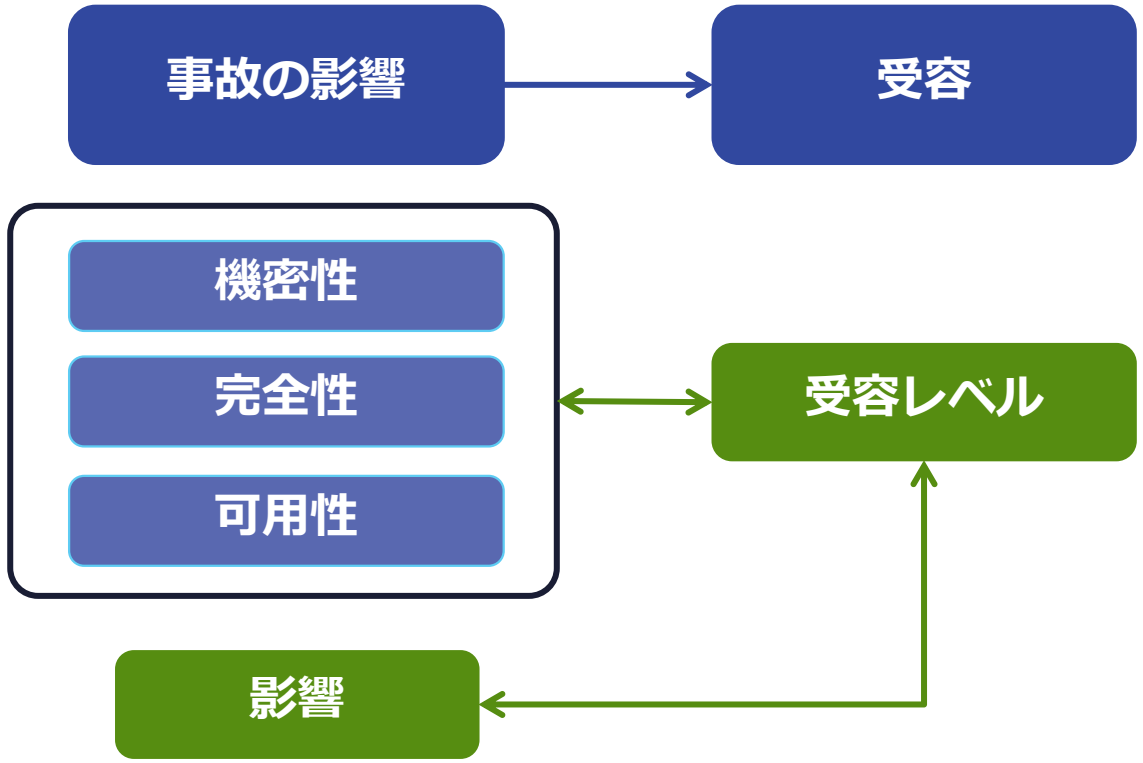
事故が発生するのは脅威と脆弱性が合致するから

- 脅威は外部にあるためにコントロールすることが難しい（抑止）
- 脆弱性は内部にあるためにコントロールが可能。脆弱性を低減することをセキュリティ対策という（防止）
- セキュリティ対策にはコストが発生するため、費用対効果を考慮する必要がある

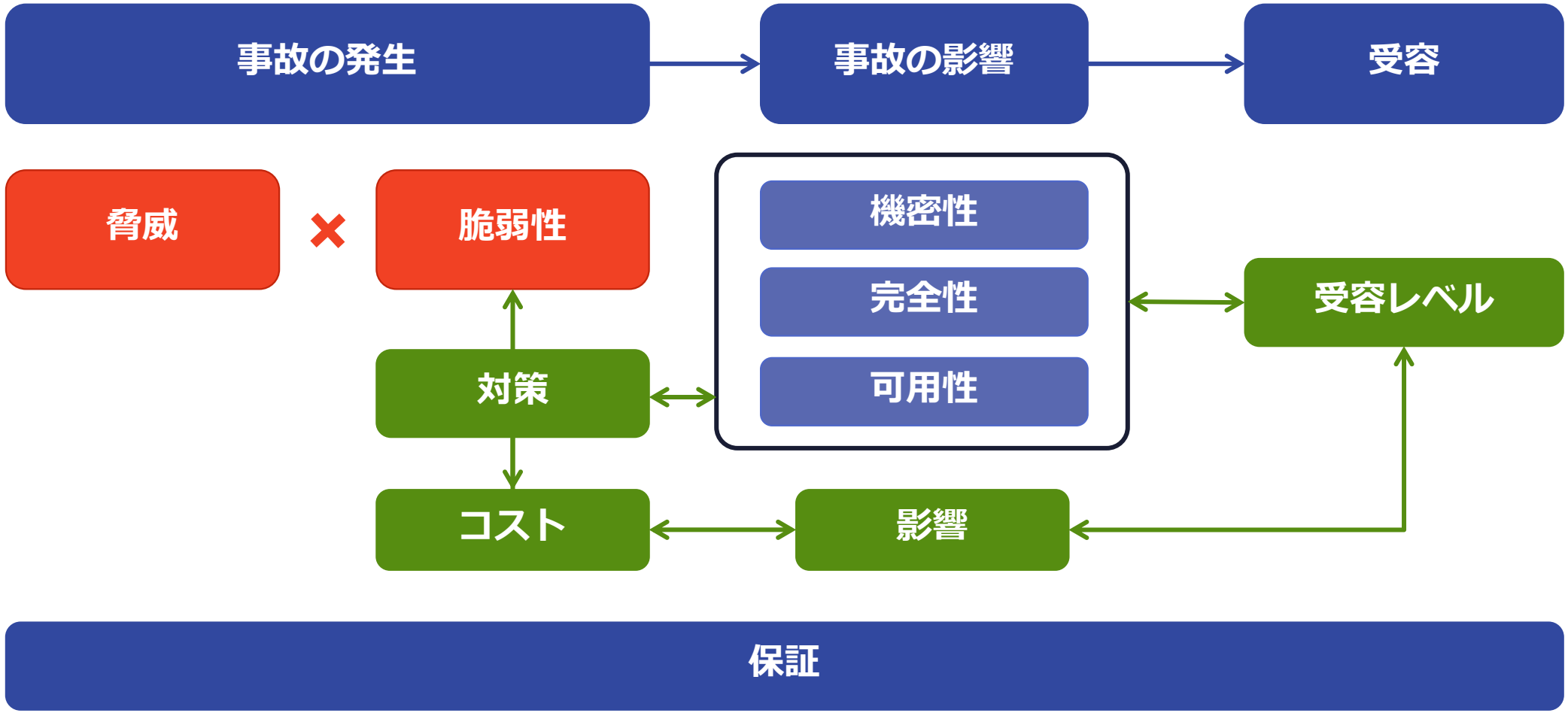
事故の影響を判断する

影響を受容できるまで、セキュリティ対策を行う

- 事故の影響は、機密性、完全性、可用性が維持されなくなることによって算出される（損失）
- 影響は3つの視点のそれぞれの合計となるため、情報漏洩だけを考えていると、費用対効果を適切に判断できない



リスクマネジメントとは

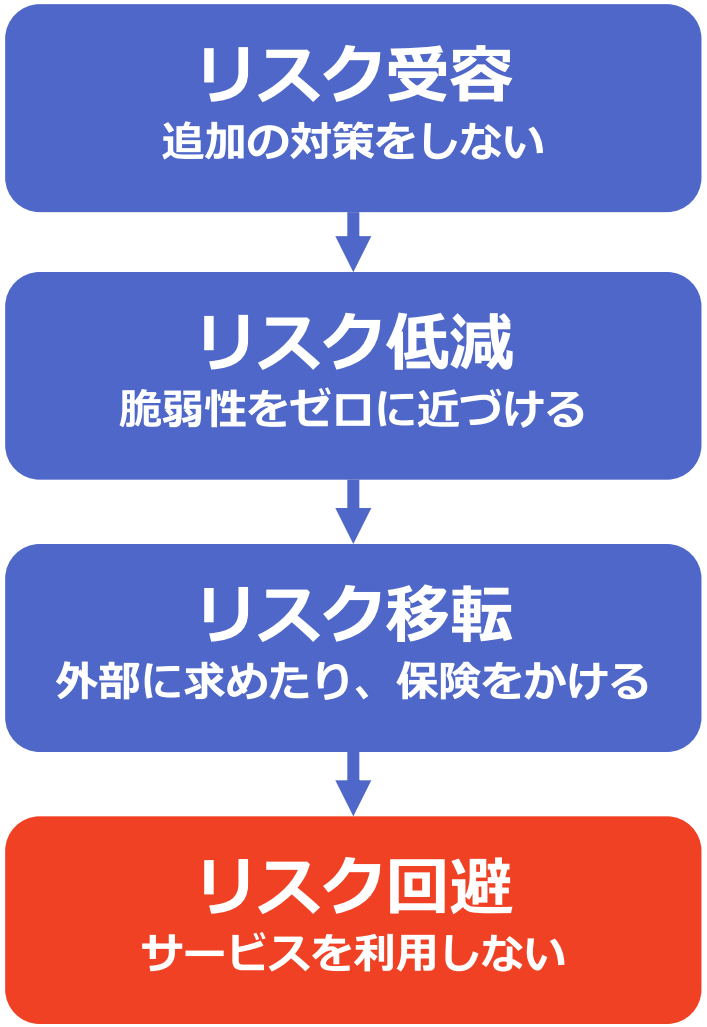


セキュリティに求められているもの

セキュリティの目的

手段の一つ

セキュリティ対策の選択



- **対策の3つの視点**
  - 管理的、技術的、物理的
- **対策の7つのフェーズ**
  - 事故の検知（インシデントの検出）の前後で対応が異なる
  - 検知前：指示、抑止、防止、補正
  - 検知後：検知、修正、回復
- **対策のモニタリング**
  - 対策を実施したら、必ず効果を測定

対策の3つの視点

管理的対策

- セキュリティ対策の推進を経営者が推進し、体制を整備する
- ポリシーや手順書を策定して、セキュリティを意識した活動を推奨する
- システム調達の標準仕様などを作成、活用する

技術的対策

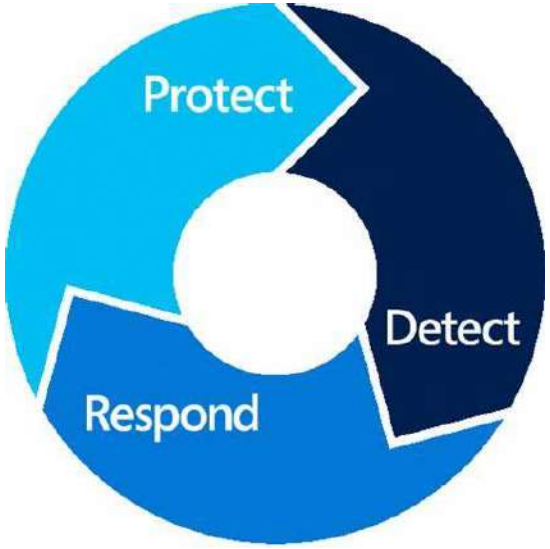
- アクセス制御などを論理的に行うことで情報を適切に管理する

物理的対策

- 入退室管理や建物そのもののセキュリティ対策を行う

セキュリティ管理のフェーズ

Cyber Security Frameworkによるセキュリティフェーズの追加とビジネスモデルの変化



「攻撃への迅速な対応」ではなく、
どんな攻撃にも耐えながら、ビジネスを継続していくための
基盤づくりとして、IDENTIFYとRECOVERが含まれた。
個別のベンダーでは対応できないために、大手による買収が進んでいる。→ **予防とサイバーレジリエンスへのシフト**

NIST「**Cyber Security Framework**」https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf

脆弱性のない環境を維持するために

- 脅威がある程度わかっているのだとすれば、それに対応する脆弱性も特定できる
  - すべての資産における脆弱性を管理し、対応状況を可視化しておけば、脅威に応じた損失予測などを実施しやすくなる
- 最新の脅威情報を入手する
  - 最新の脅威情報を入手し、脆弱性への対策を適宜行っていくことで、安全な状態を維持するだけではなく、サービスの継続性なども維持できる
  - 脆弱性のないIT環境をを維持することをサイバーハイジーン（衛生）という

報告書の読み方

表 3　IT ガバナンスの問題と予防提案の整理

No	IT ガバナンスにおける問題点	予防に向けた提案
1	各契約単位で、保守や脆弱性管理といったセキュリティに関する責任分界点と役割が明確になっていない領域が存在した。	契約毎に、受注者と 2 省ガイドラインに基づいたサービス仕様適合開示書及びサービス・レベル合意書（SLA）により双方の責任分界点や役割を明確にし、文書化すること。
2	複数のベンダーが関与する契約において、そのプロジェクトマネジメント体制が明確になっていない状況があり、重要なセキュリティに関する事項について、関係者による十分なリスク評価が行われていないケースがあった。	合同企業体（JV）によるプロジェクトの場合（構築だけでなく保守も含む）は、受注側のプロジェクト体制を明確にさせるなど、責任の所在を明確にすること。
3	医療機器やその保守に係るセキュリティ仕様が、総合情報システムにおけるセキュリティ仕様に適合していないケースがあり、運用が共通化されていなかった。	調達が行われる場合には、病院共通のセキュリティポリシーに基づく共通仕様を作成し、共通運用となるような調達を行うこと。
4	医療情報部で調達している情報資産以外の医療機器（リモート保守用機器を含む）や建築関係の情報システムについて、一元管理されていなかった。	診療情報系のネットワークに接続されている機器やシステムはすべて情報資産としてリストアップしたうえで、安全管理上の重要度に応じて分類し、リスク分析を実施すること。
5	総合情報システムの仕様における厚労省ガイドラインは第 4.3 版であるが、現時点では第 5.2 版まで更新されている。第 5.2 版についてベンダーを交えて組織的に検証されている状況が確認されなかった。	ガイドライン改定時には組織的に適合状況を確認し、不足している項目があれば改善に向けた PDCA サイクルを回す活動を行うこと。

情報セキュリティインシデント調査委員会報告書（15ページ）
https://www.gh.opho.jp/pdf/report_v01.pdf

医療機関にあるすべての
システムや機器で
セキュリティ対策を考える

↓

組織の健全なセキュリティ対策

||

ITガバナンス確立へ

第3回のまとめ

セキュリティ対策の基本であるアクセス制御の実践

セキュリティ対策考え方の整理

オープンなネットワーク思考とゼロトラストの推進

標準機能の活用がセキュリティ強化につながる

ありがとうございました。

次回は11月16日(木)
効果的なセキュリティの実現についてお話します。

※本日の講義でご紹介したリンク先は、アンケートに記載しております。
本研修ではリアルタイムでの質問はお受けしておりません。
ご質問のある方は、アンケートにご記入ください。

https://forms.gle/qsMybXt6srPjVqqd6