はじめに

+ 本章では本システム基本設計のセキュリティに関する部分の基本設計を記述する。また、インターネットを利用することを前提としたセキュリティについての内容を記述する。

+ 利用が想定されるAS2（アプリケーションプロトコル）を踏まえ、電子証明書について記述した上でセキュティに関する基本設計を記述する。

セキュリティについて

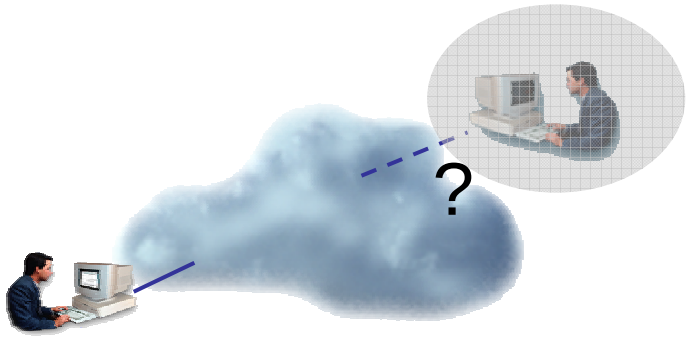
1. 認証の必要性
2. 電子証明書
3. マスターデータ同期化システム上の評価対象
4. セキュリティ基本設計
5. 詳細設計に向けた留意点

1. 認証の必要性

ビジネスインフラとしての課題：専用線からインターネットへ

+ **インターネットの根本的な課題**

  + **相手が誰なのか確認できない**



インターネットの特徴

メリット	問題点
• 公共性が高い • コストが安い • 双方向の伝達が可能 • 即時性 ・・・	• 通信相手が見えない • データの到達保証がない • 機密性が保たれない（盗聴、改ざん等）

+ **信頼できる相手かどうかを確認しなければ、安全な取引は成立しない**

インターネットでビジネスを行う際に認証は不可欠

+ **インターネット上でも重要なコミュニケーションや商取引で「認証」は不可欠**

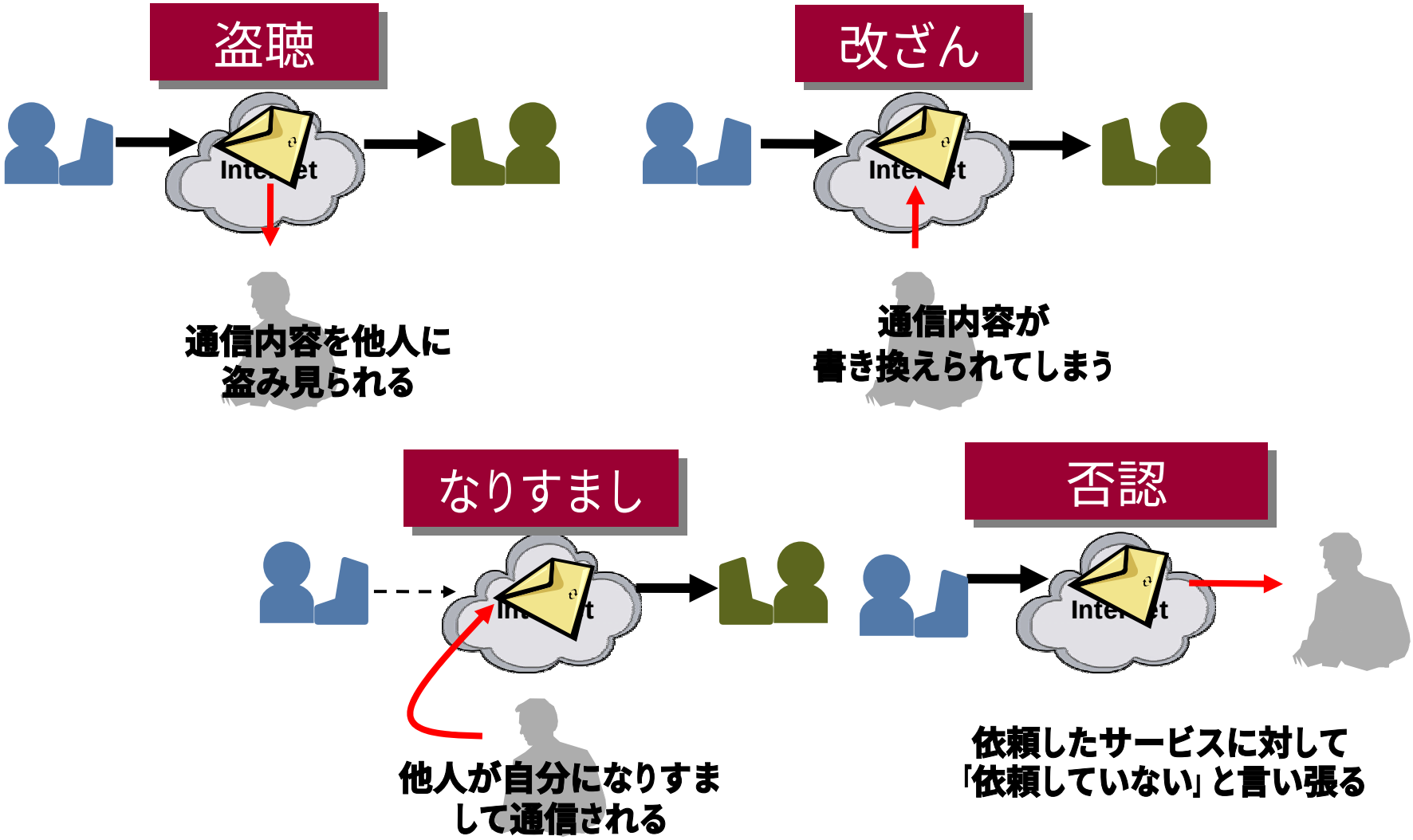
+ **現実世界では…**
  + **名刺・人の紹介による商談**
  + **建物と店名を確認して入店**

+ **私が誰であって、本当に存在することをインターネット上で証明する必要がある**

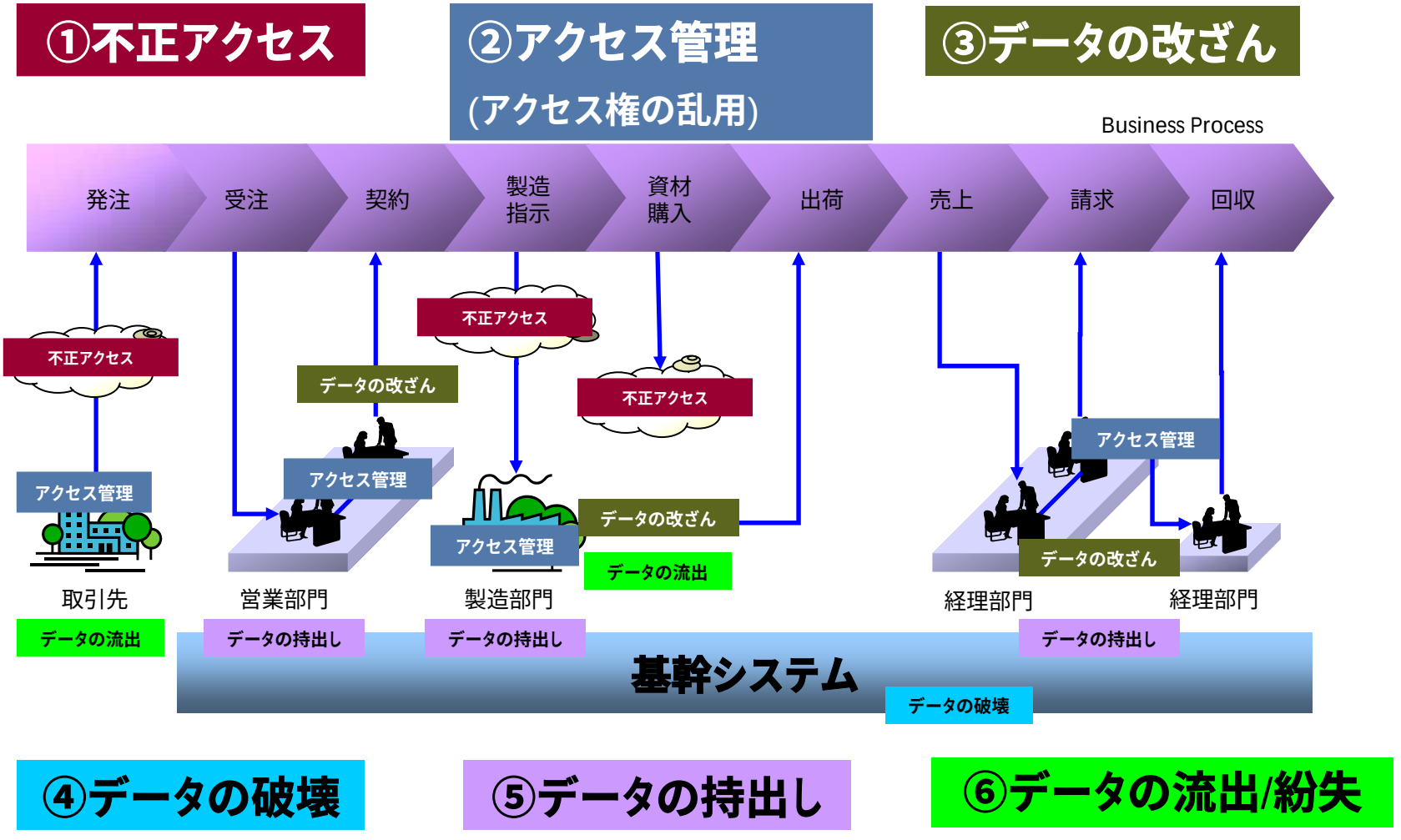
電子認証

- 私が誰であるか、第三者が証明し、電子的に認識できる仕組み
- 信頼のおけるネットワーク上の取引を行う為、個人または法人を確実に識別する

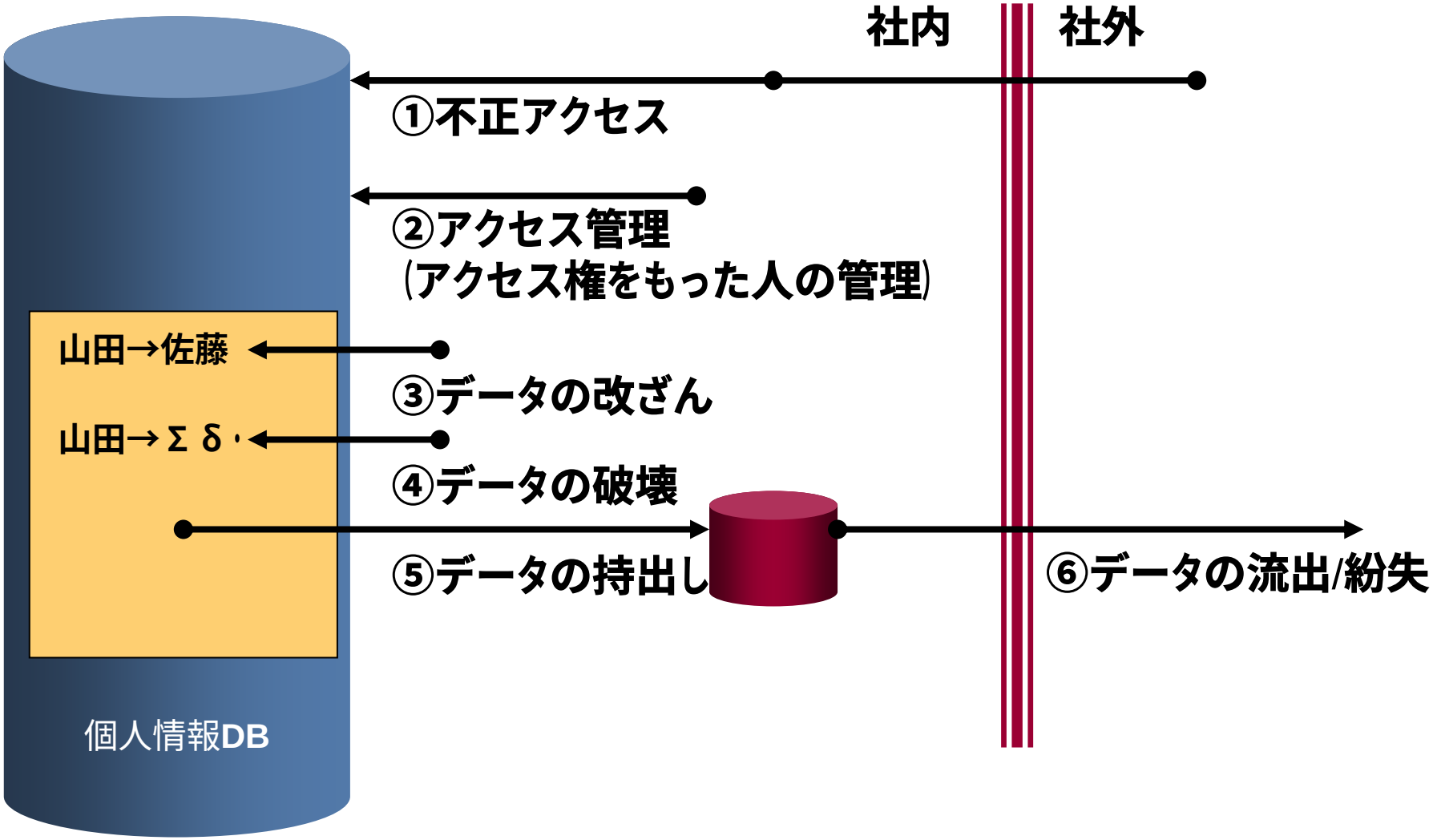
インターネット上で情報を交換する際の脅威



ビジネスプロセス上で見た脅威



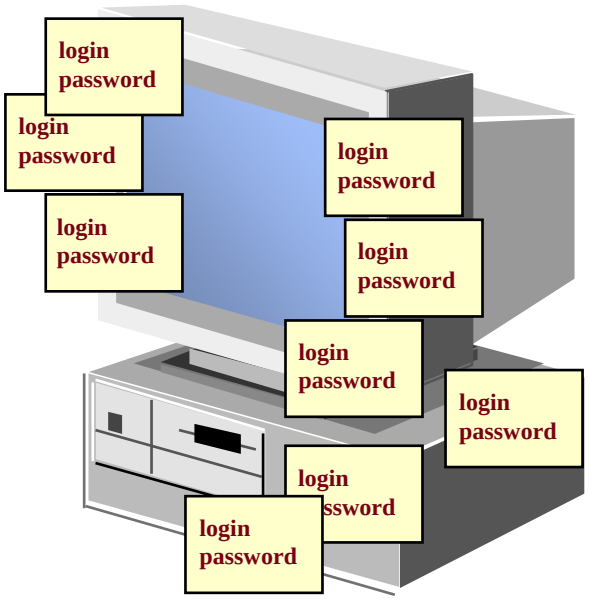
ファイル、データベースへの脅威



2. 電子証明書

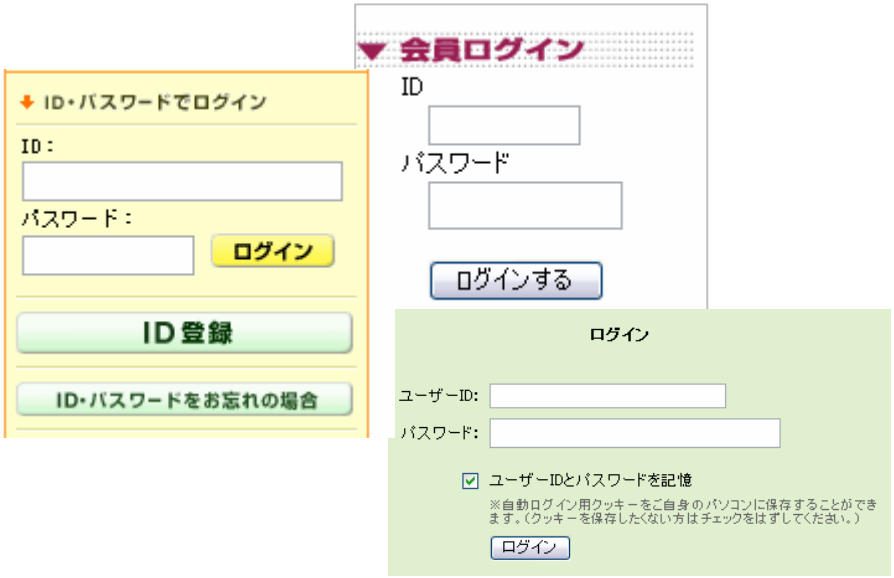
パスワードの問題点

- **唯一性を証明できない**
  - 推測されたり、盗まれやすい
  - 「知る」ことにより「他人になりすます」ことができる
  - 取引きの否認ができる
- **使い勝手が悪い**
  - 定期的な更新が必要
  - 忘れやすい
  - 個人の管理に依存
  - ポストイット症候群になる
- **管理費用が高い**
  - ヘルプデスク費用の約40%はパスワードの再設定
- **認証にしか使えない**
  - 署名や暗号化ができない



インターネット上における認証の実現

+ **ID/パスワードによる認証方法**
  + その人しか“知らない”もの
  + 複数のID/パスワード



すでに利用の限界

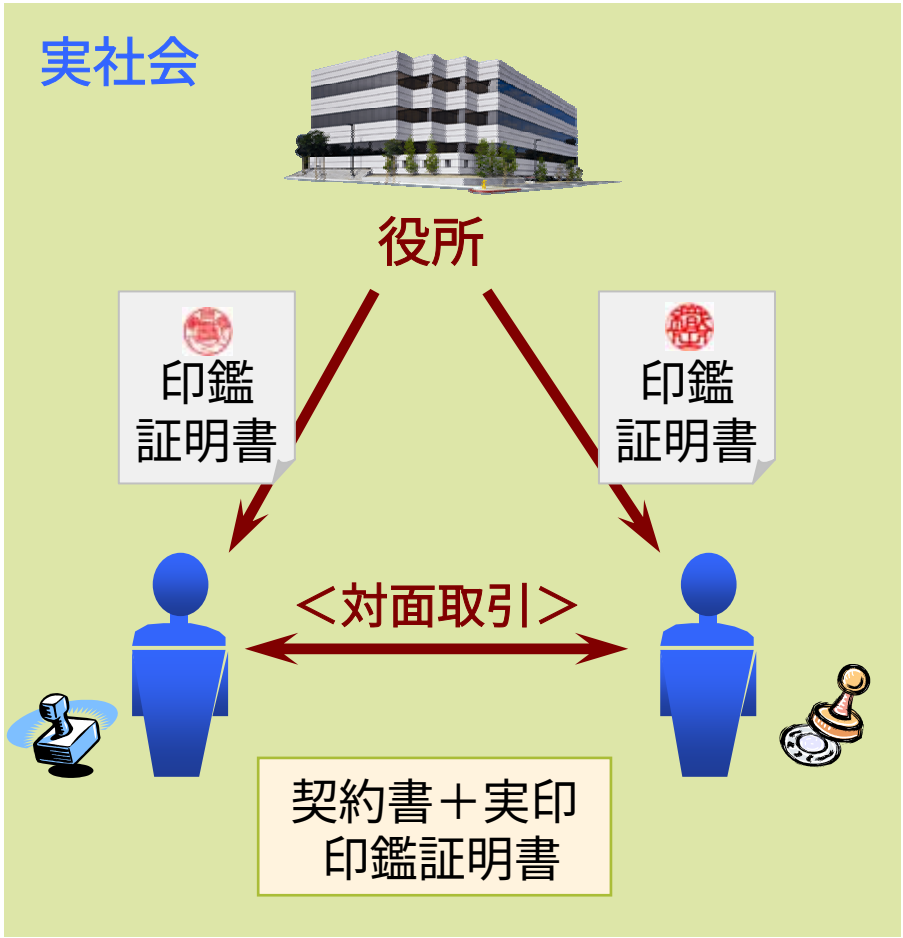
(例：フィッシング詐欺)

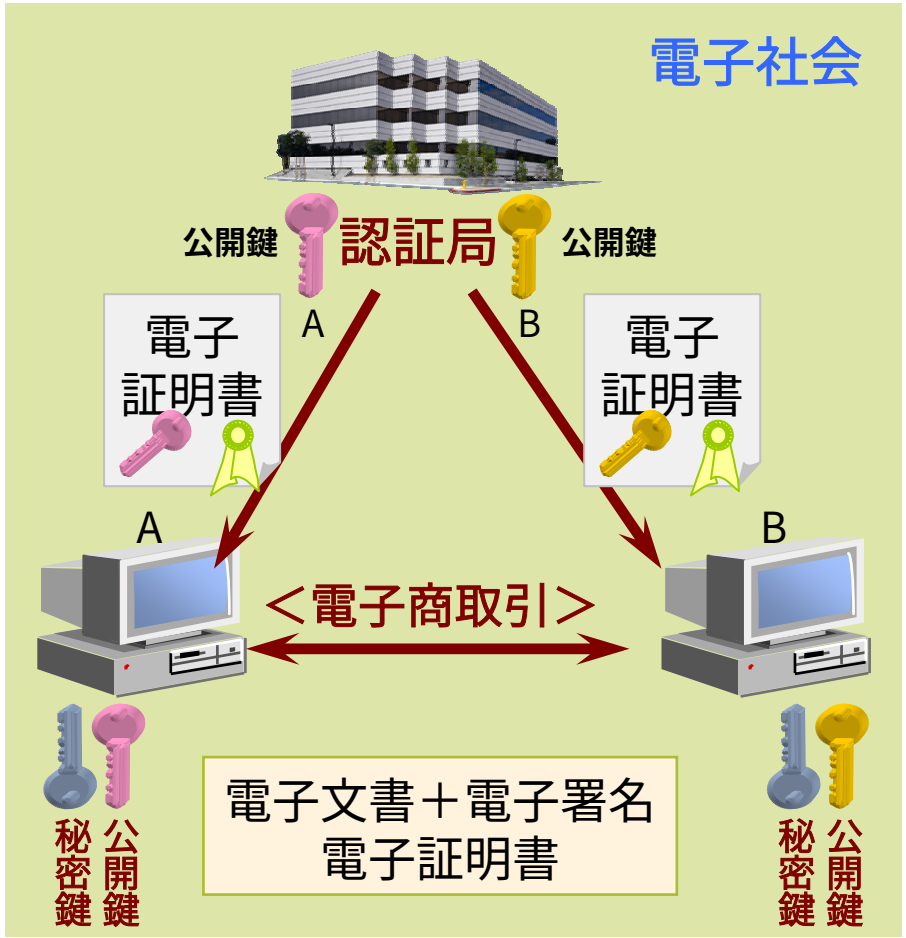
+ **PKI *による電子認証が必要**
  + **公開鍵暗号方式を用いて実現されるセキュリティの基盤**
  + **電子証明書による認証基盤**

*PKI : Public Key Infrastructure

実社会での証明書と電子証明書の比較

+ **実社会の証明書と基本的に同じ仕組み**
+ **信頼された機関から（身分）証明書を出してもらう**





電子証明書とは

+ **電子的な身分証明書**
  + パスポート、印鑑証明書、運転免許証に似た役割
+ **特別な暗号ファイルが基**
  + 偽造不可能なIDと署名
+ **認証局が発行**
  + 不特定多数、あるいは 特定のコミュニティを対象
+ **「信頼」の基礎を提供**
  + 所有者を認証
  + 暗号化によりプライバシーを保護
  + 取り引きの法的根拠(電子署名)

電子証明書を発行する際のクラス

- 電子証明書を発行する場合には通常いくつかのクラスを設定

- クラス設定例
  - クラス1

    電子メールアドレスの実在を到達確認によって電子証明書の発行を行う。
    (ex. Webでメールアドレスを登録、送付メールに再度確認のためのアクセス情報が記載。その後、発行)

  - クラス2

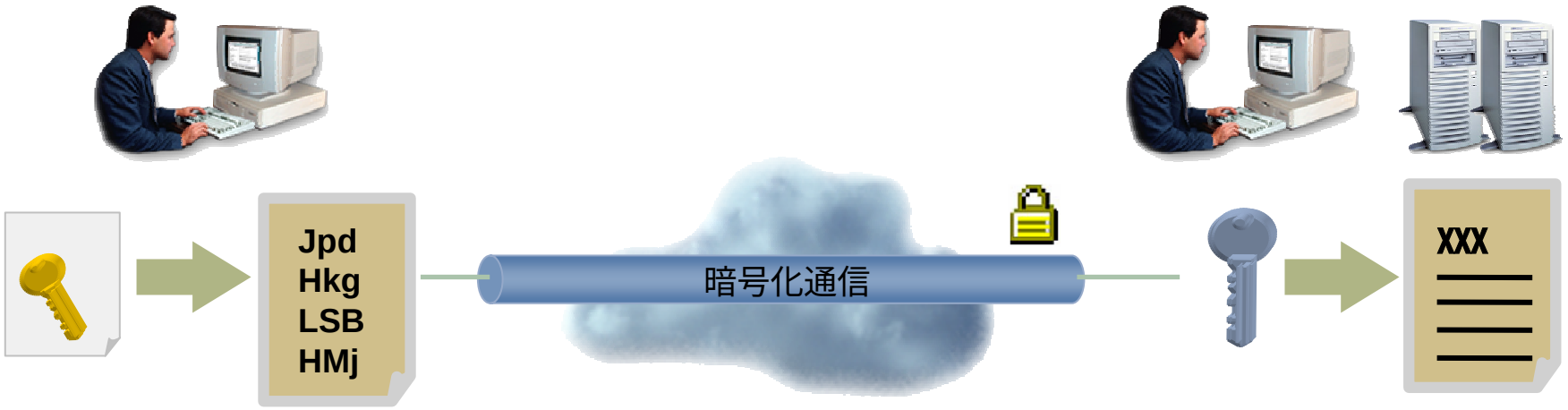
    本名、電子メールアドレス、組織名 その他、複数の要素を確認し、電子証明書をの発行を行う。(ex. 社員証を発行する場合)

  - クラス3

    クラス2に加え、公的なデータによる本人確認し、電子証明書を発行する。
    (登記簿謄本を確認し、Webサーバ要の電子証明書を発行する場合)

電子証明書を利用した暗号化通信例

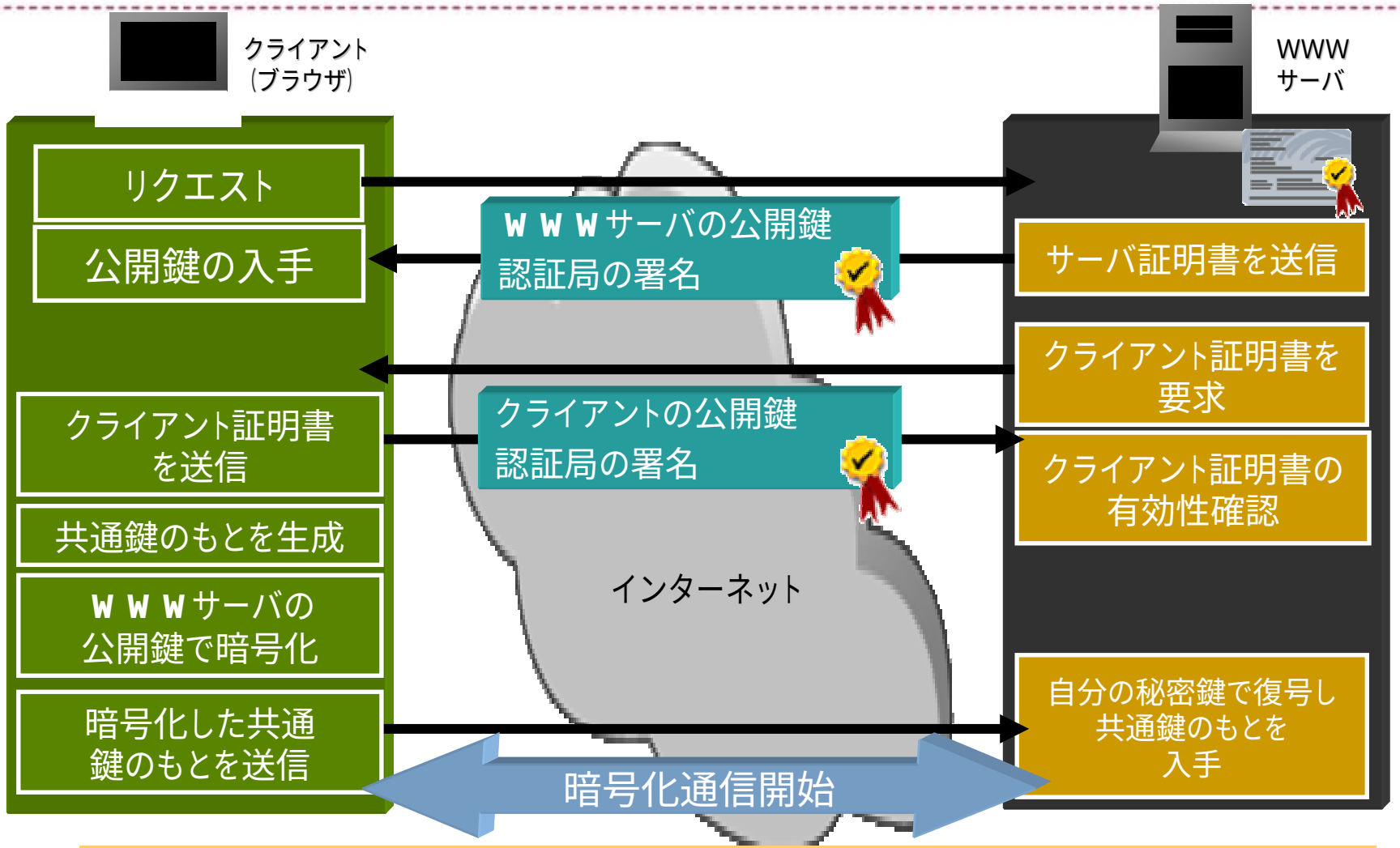
+ **相手の公開鍵を使って、データを暗号化して送信**
+ **インターネット上で暗号化通信が可能**



相手の公開鍵で暗号

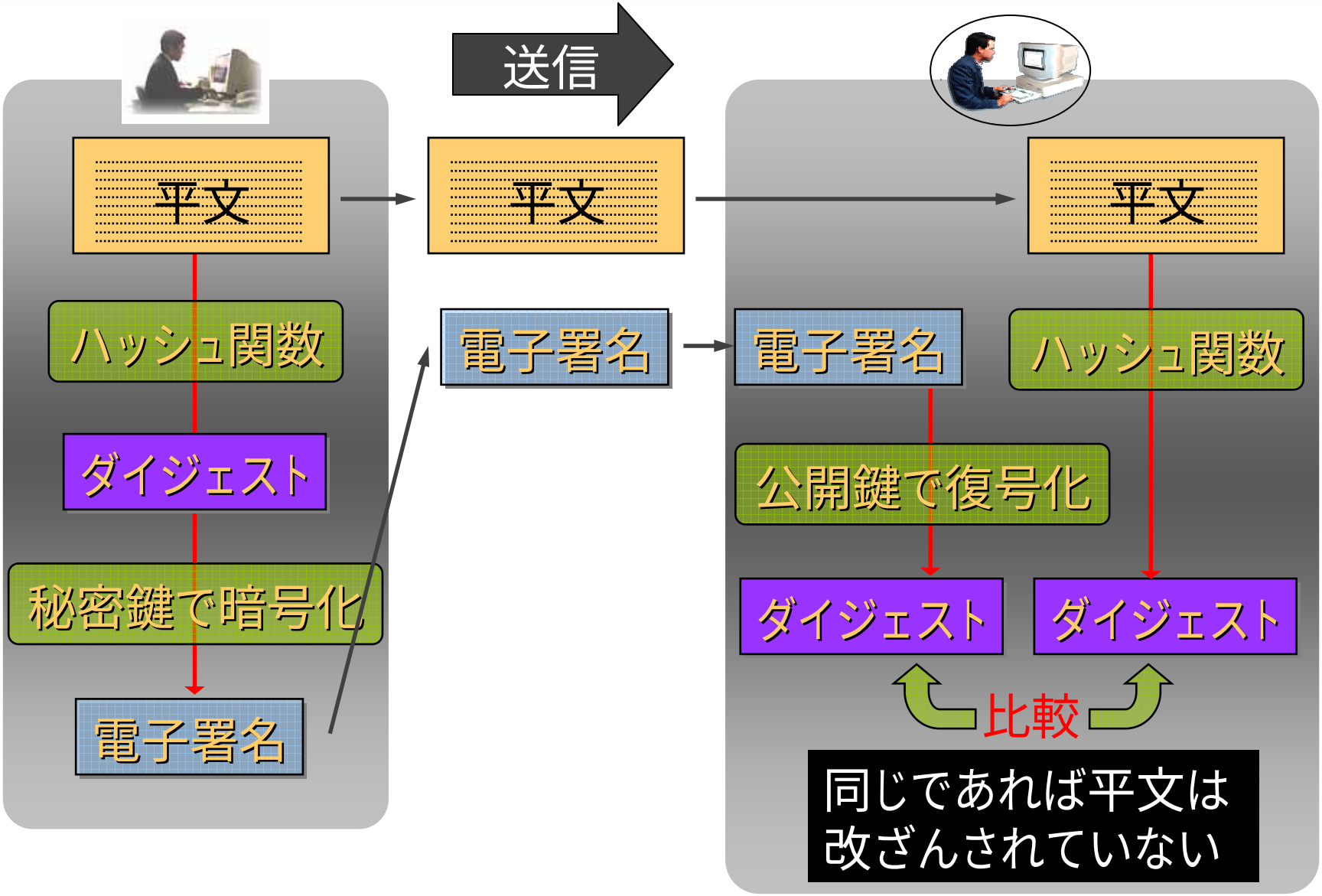
自分の秘密鍵で解読

認証（電子証明書を用いた相互認証の例：SSL）



一般にSSLはサーバとセッション開始時点に実行される

電子署名


送信
平文
ハッシュ関数
ダイジェスト
秘密鍵で暗号化
電子署名
平文
電子署名
平文
電子署名
ハッシュ関数
公開鍵で復号化
ダイジェスト
ダイジェスト
比較
同じであれば平文は
改ざんされていない

社会インフラとして利用されるための電子証明書の要件

+ **電子認証は、技術だけでは可能にならない**

	証明書の要件	PKI による電子証明書
信用できる	+ 発行機関が信用できる + 発行プロセスが確立されていること	+ インターネット上の信頼できる第三者機関 ＝ 認証局 + 厳格な電子証明書の発行手順
誰でも認識できる	+ 統一規格であり、広く世の中に認められていること	+ 標準化された電子証明書の様式（仕様） + 標準仕様に基づいたハード・ソフトへの実装
偽造不可	+ すかし、ホログラム、マイクロプリントが施されていること	+ 暗号技術によって実現 + 理論的に解読不可能
法的根拠	+ 法的に裏づけがあること	+ 各国で進む法整備

認証局の運営に必要なもの

+ 堅牢な設備 (データセンター)
+ 人的セキュリティ
+ 安定した証明書発行システム
+ 認証局運用規程(CPS)
+ 内部監査・外部監査


認証局システム


PKI技術者


サーバ、ネットワーク


ファイアウォール、
侵入監視等


データベース

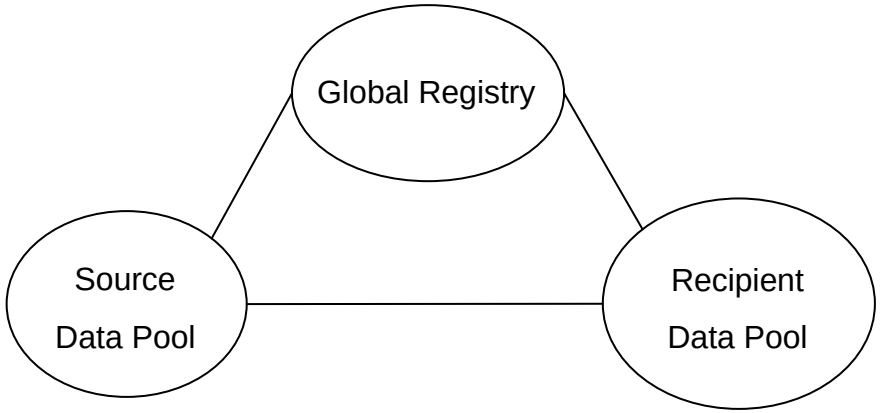

信頼できる運用人員
トレーニング


堅牢な設備
(データセンター)

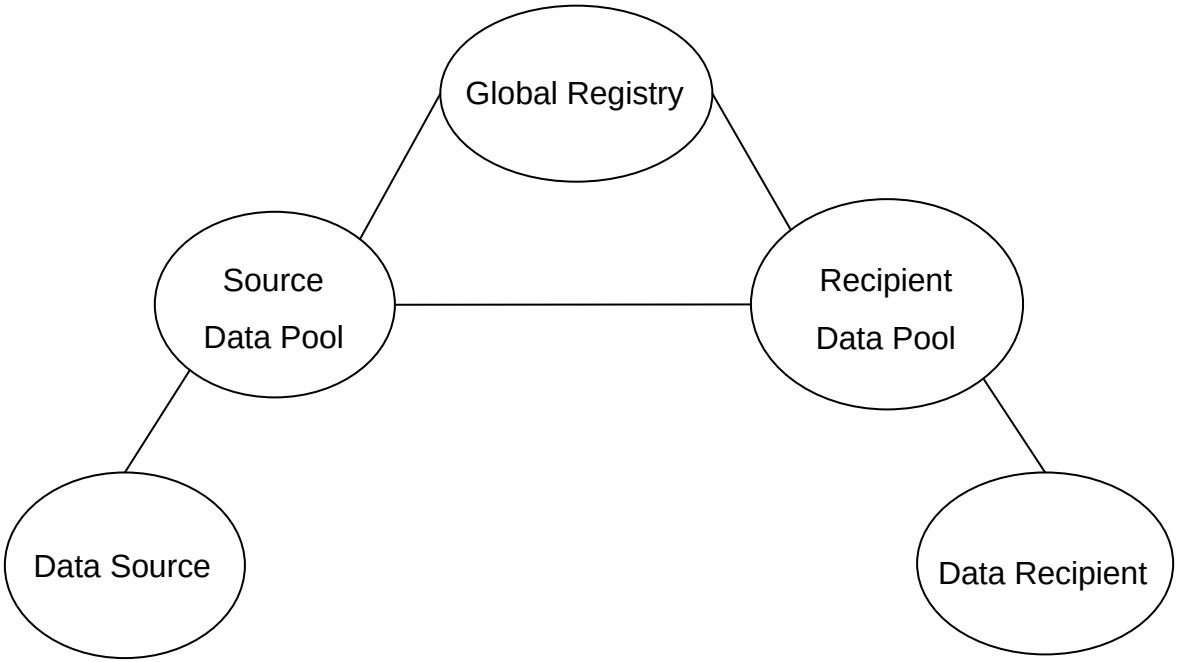
3. マスターデータ同期化システム上の評価対象

モデルについて

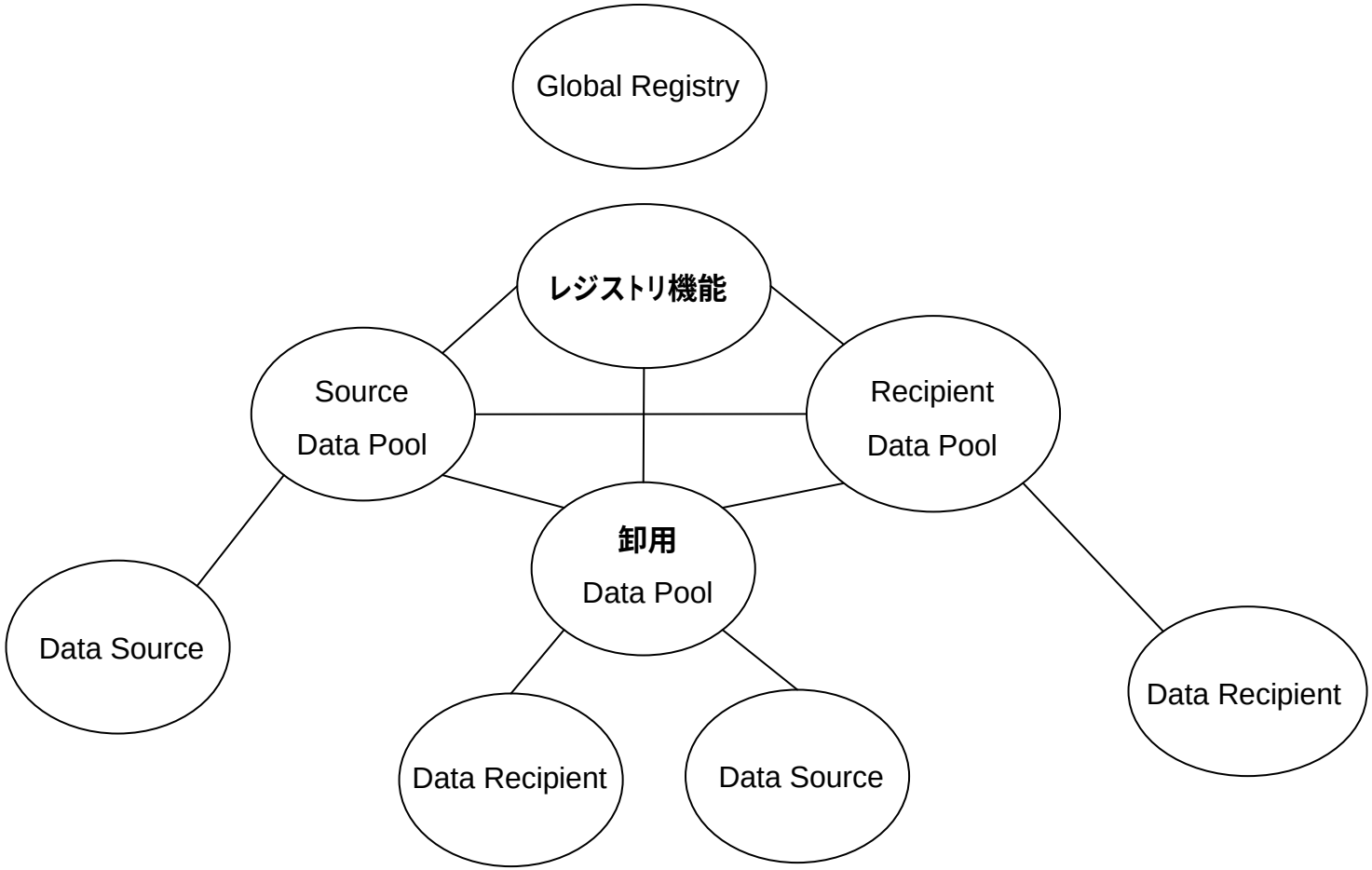
- **定義**
  - ドメイン
    - 本章においては円で示したものをドメインと定義する
  - ドメイン間通信
    - ドメインとドメイン間において発生する通信と定義し、ドメイン間通信が発生する相互の間は実線にて示す



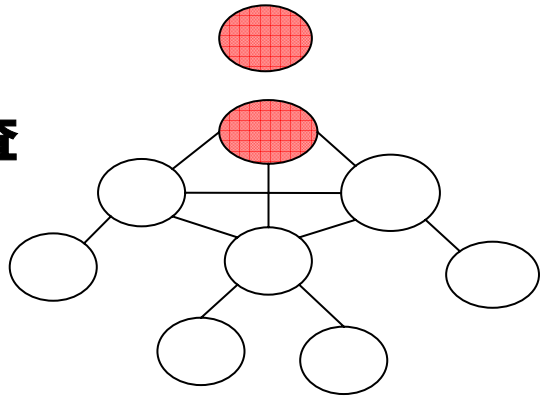
GDSNにおけるモデル定義



本基本設計におけるモデル定義



ドメイン定義：グローバルレジストリ/レジストリ機能



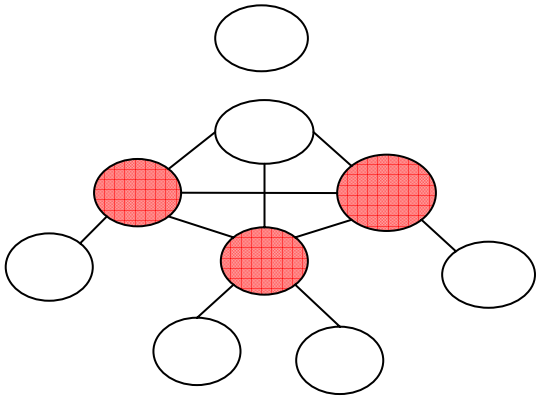
1. **定義(要全体との整合性)**

   マスターデータ同期化のためにデータプールの審査(Certification)およびデータ制御を行う機能

2. **種類：GDSNと本基本設計の対比**
   1. GDSN
      1. グローバルレジストリ
   2. 本基本設計
      1. レジストリ機能
3. **評価対象**

   本基本設計におけるレジストリ機能のみ評価対象とする。

ドメイン定義：データプール



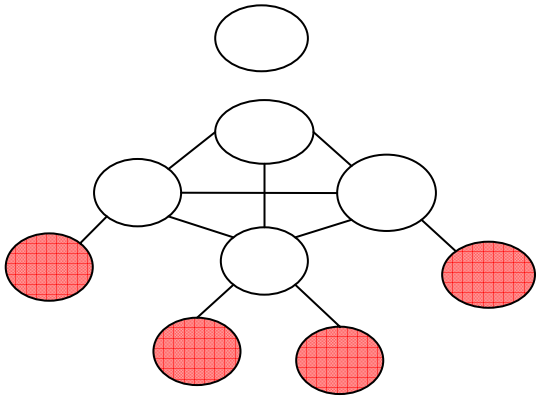
1. **定義(要全体との整合性)**
   マスターデータ同期化のためのデータ集約機能
   およびサービス
2. **種類：GDSNと本基本設計の対比**
   1. GDSN
      1. ソース データプール(Source Data Pool)
      2. レシピエント データプール(Recipient Data Pool)
   2. 本基本設計
      1. ソース データプール(Source Data Pool)
      2. 卸用 データプール(Source Data PoolおよびRecipient Data Pool)
      3. レシピエント データプール(Recipient Data Pool)
3. **評価対象**
   本基本設計ソースデータプールおよびレシピエントデータプールを評価対象とする。

※卸用データプールはセキュリティ評価対象としてはソースデータプールおよびレシピエントデータプールと
同等であるため、本基本設計においては評価を行わない。

ドメイン定義：データソース/データレシピエント

1. **定義(要全体との整合性)**

   マスターデータ同期化のためにデータプール対して
   データを送付もしくは授受する機能



2. **種類：GDSNと本基本設計の対比**
   1. GDSN
      1. データソース (Data Source)
         1. 基本項目
      2. データレシピエント (Data Recipient)
         1. 基本項目
   2. 本基本設計
      1. データソース (Data Source)
         1. 基本項目
         2. 関係依存項目
         3. 個別項目
      2. データレシピエント (Data Recipient)
         1. 基本項目
         2. 関係依存項目
         3. 個別項目

3. **評価対象**

   本基本設計におけるデータソースおよびデータレシピエントを評価対象とする。

   ※評価対象としてはデータソースとデータレシピエントは同等であるため、同一ドメインとして評価を行う。

定義：データ

1. **定義**

   ドメイン内部にて生成され、ドメイン間通信で授受される情報

2. **種類：GDSNと本基本設計の対比**

   1. GDSN
      1. グローバルレジストリドメイン内部のデータ
      2. ソースデータプール/レシピエントデータプール ドメイン内部のデータ
      3. ソースデータ/レシピエントデータ ドメイン内部のデータ
   2. 本基本設計
      1. レジストリ機能 ドメイン内部のデータ
      2. ソースデータプール/卸データプール/レシピエントデータプール ドメイン内部のデータ
      3. データソース/データレシピエント ドメイン内部のデータ

3. **評価対象**

   セキュリティ評価の観点から全ての情報をデータとして評価する。
   データの細分化、細分化データごとの定義および評価は基本設計においては
   対象外とする。

定義：アプリケーション

1. **定義**

   ドメイン内部においてデータを処理するソフトウェアもしくはプログラム

2. **種類：GDSNと本基本設計の対比**

   1. GDSN
      1. グローバルレジストリドメイン内部のデータアプリケーション
      2. ソースデータプール/レシピエントデータプール ドメイン内部のデータアプリケーション
      3. ソースデータ/レシピエントデータ ドメイン内部のデータアプリケーション
   2. 本基本設計
      1. レジストリ機能 ドメイン内部のデータアプリケーション
      2. ソースデータプール/卸データプール/レシピエントデータプール ドメイン内部のデータアプリケーション
      3. データソース/データレシピエント ドメイン内部のデータアプリケーション

3. **評価対象**

   セキュリティ評価の観点から全てのソフトウェアおよびプログラムをアプリケーションとして評価する。アプリケーションの細分化、細分化アプリケーションごとの定義および評価は基本設計においては対象外とする。

定義：利用者

1. **定義**

   ドメイン内部にてアプリケーションを介してデータに関与する全ての者

2. **種類：GDSNと本基本設計の対比**

   1. GDSN
      1. グローバルレジストリドメイン内部の利用者
      2. ソースデータプール/レシピエントデータプール ドメイン内部の利用者
      3. ソースデータ/レシピエントデータ ドメイン内部の利用者
   2. 本基本設計
      1. レジストリ機能 ドメイン内部の利用者
      2. ソースデータプール/卸データプール/レシピエントデータプール ドメイン内部の利用者
      3. データソース/データレシピエント ドメイン内部の利用者

3. **評価対象**

   詳細設計にて行うものとし、基本設計においては対象としない

4. セキュリティ 基本設計

+ **本項では、前述の定義、且つ評価対象としたものに対して必要となる要件と機能を記述する。**

セキュリティ要件の種別

+ IETF (The Internet Engineering Task Force)によるRFC2196[4]、及び、ISO (InternationalStandard Organization) TC68における種別

  + 認証
  + 機密性
  + 完全性
  + 認可
  + 証拠性 (否認防止)
  + 可用性
  + 耐複製性

※ 証拠性 (否認防止) 、耐複製性はRFC2196では定義されていないが、重要なセキュリティ要件であると考えるため追加。

本基本設計におけるセキュリティ要件は上記の7種別から適切な要件を抽出することとする。

セキュリティ要件の種別詳細(1/4)

認証

論理的リソース（物理的アクセスについては対象外とする）に対し「利用者を識別する手段」。

閉塞されたネットワークにおいて長い間ID、パスワードが利用されてきたが、インターネットの普及に伴い、また、メールの盗聴やトロイの木馬型ウィルスによるID、パスワードの盗聴といった損害が多発したため、チャレンジレスポンス型認証やワンタイムパスワード、バイオメトリクス、PKIといった高度な認証技術が適用され始めている。また、厳格な認証を行うためには、複製可能な秘密トークンを耐タンパ性ICカードへ格納するなど十分な保護が望ましい。「なりすまし」「不正アクセス」などは適切な認証技術によって防止することができる。

機密性

機密性は「承認されていない主体に（情報が）開示されることを防ごうとする」ために求められる要件。

機密性の保護には物理的、論理的アクセスコントロールによる制御と、暗号化によるものがある。暗号化とはデータをある定数をもとにスクランブルすることにより、定数を知らない主体が平文を得るために非常に大きなコストと時間がかかる、という特性に基づく。「盗聴」などは、適切な機密性保証技術によって防止することができる。

セキュリティ要件の種別詳細(2/4)

完全性

情報が、通信の途中、または、保存期間中において不当に改変（改竄）されていないことを確認するための技術である。単純な方法としてチェックサムの計算が挙げられるが、RFCも推奨するように、現在ではMD5、SHA-1といった暗号アルゴリズムが使用されている場合が多い。

「改竄」などは適切な完全性保証技術によって防止することができる。

認可

認可とは「利用者（プログラムなどの情報を含む）に権限（特権）を与えること」であり、本人性確認手段である「認証」とは区別される。認可によって提供されるセキュリティサービスは権限、権利 、プロパティ、許可された行為等である。例えば、認証されてアクセスしたサーバ上においてアクセスできるフォルダの範囲の設定（アクセス権限）は、認証情報と認可データベースを参照することで決定される。

セキュリティ要件の種別詳細(3/4)

証拠性

証拠性とは時間的に継続する認証情報と完全性の複合によって実現される。複数のセキュリティ要件の複合として実現されるため、独立したセキュリティ要件としてみなされない場合もある。一般的に否認防止は電子署名と呼ばれる技術によって提供される。代表的な電子署名は完全性を保証するメッセージダイジェストに対し、DSAなどのデジタル署名を行うことで実現される。

デジタル署名技術による証拠性は、現時点で有効とみなされても、将来の技術的発展によってその信頼性が下がる可能性があり、現在IETFでは長期に渡るデジタル署名の証拠性確保のために時間保証（タイムススタンピング）などを署名とともに記録すること、適切な公証機関を用意するなどの必要性について標準化を進めている。

可用性

可用性とは「アプリケーションが継続的に提供されること」であり、停止による機会損失を避けるための要件である。本要件は情報の保護ではなく情報を取り扱う装置に対する保護を行うことにより実現される。例えばシステムや電源設備の二重化や、データのバックアップなどといった運用上の仕組みにより提供される。

セキュリティ要件の種別詳細(4/4)

耐複製性

耐複製性は情報の不正な複製が行われないことを目的とする技術であり、著作権管理の一環として近年注目されている。耐複製といった場合、主に複製後に複製前の情報が改竄なく複製されることが求められる場合と、複製自体を防止することを要求する場合がある。

耐複製技術は単一の要件を要求するものではなく、機密性維持による複製防止というように複数の要件の言い換えである場合が多い。

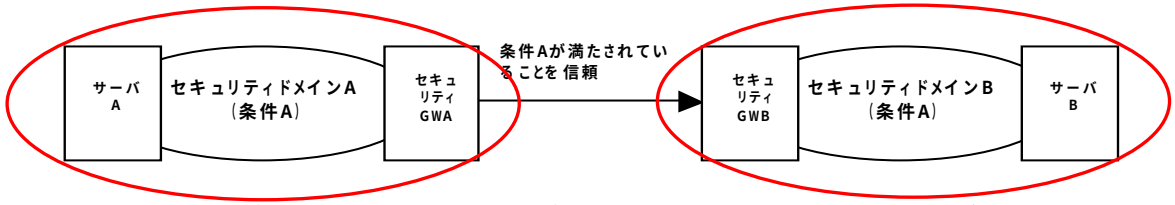
具体的には耐タンパ装置内に情報を保護するなどの物理的な対策と、電子透かしなどによる付帯情報によって情報の取り扱い（コピー防止）などを規定し、運用によって耐複製性を保護するものがある。

評価対象抽出モデル作成の前提（トラストモデルとセキュリティドメイン）

トラストモデルとは信頼の関係に関する前提事項。トラストモデルは「誰が誰を（信頼関係）どのような点について信頼（信頼事項、トラスト条件）しているのか」というマトリクスであり、誰に対し、どのようなセキュリティ環境を提供すべきかを決定するための前提条件。

また、セキュリティドメインとは一定のトラスト条件を満たしている閉塞空間を意味し、セキュリティドメイン内部では、トラスト条件が満たされていると考えられるため、当該条件が満たしているセキュリティ要件に対する対策は必要ない。セキュリティドメインはトラストモデルの一部を構成する。セキュリティドメインには条件を満たさない外部との境界にセキュリティゲートウエイが存在する。このゲートウエイが内部のセキュリティ要件を維持するための機能を提供する。

例えば、あるサーバ運営者はFW等で守られた内部ネットワークが「外部からの不正進入がなく、情報の漏洩、改竄が不可能（トラスト条件A）」なセキュリティドメインであると考えるのが一般的である。仮に「外部からの不正進入がなく、情報の漏洩、改竄が不可能（条件A）」を満たすセキュリティドメインA,Bが存在している場合のセキュリティドメインとトラストモデルの関係は下のようになる。

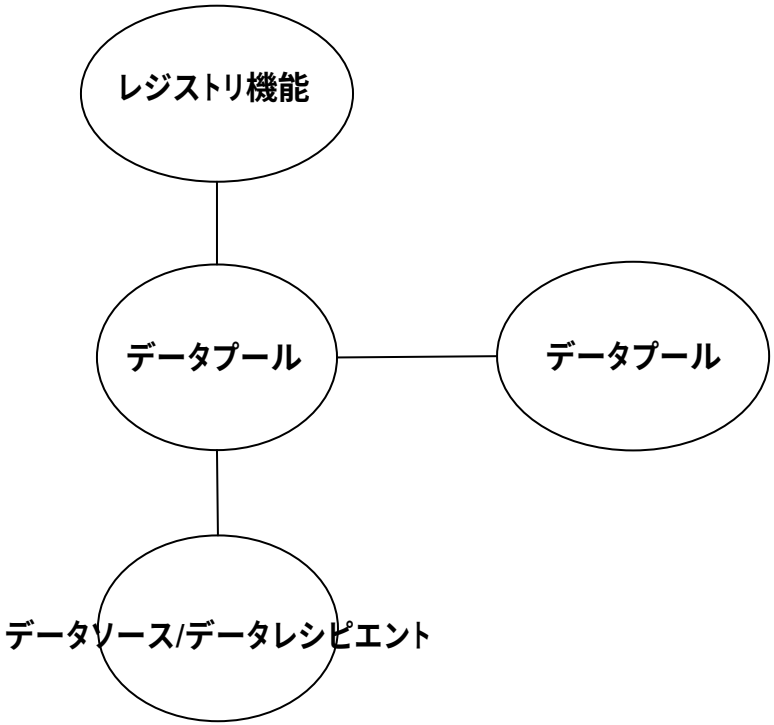


（注）ドメインAがドメインBにおいて条件Aが満たされることを信頼するトラストモデル
赤の実線で括られる部分が今回のモデルにて定義されるドメイン

この図においてセキュリティゲートウエイの内部は、条件Aが満たされていると考えられる。この場合のトラストモデルは、外部の通信者は、セキュリティゲートウエイまでの通信が保護されていれば、その内部が条件Aに関して安全であると信じる。となる。具体的には、サーバAとサーバBが安全に通信するためにサーバAが考慮すべき条件Aに関するセキュリティ対策はセキュリティGW間の通信のみでよい、ということになる。

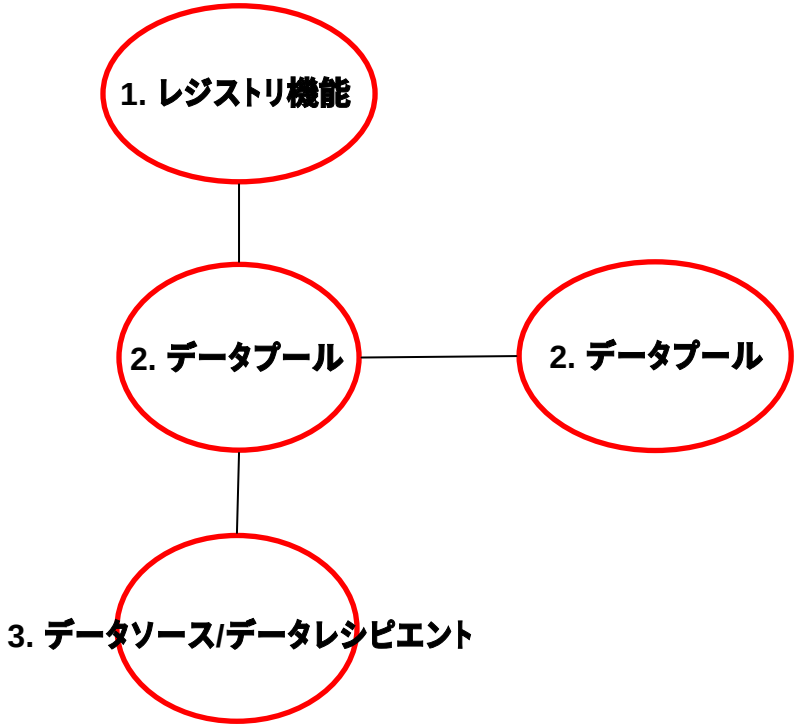
評価対象抽出モデル

トラストモデルとセキュリティドメインを踏まえ、本基本設計での
評価抽出モデルは下の図ようにまとめられる



ドメインの評価対象

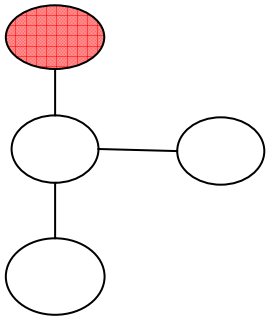
+ **評価対象モデルにおいてドメインの評価対象としては以下の3つ**
  1. **レジストリ機能**
  2. **データプール**
  3. **データソース/データレシピエント**



ドメインの評価対象：レジストリ機能

1. セキュリティ要件

+ 接続するデータプールの認証
+ 一定のシステム監査に対応したデータの証拠性（否認防止）
+ データプールとのデータ通信における可用性



2. セキュリティ機能

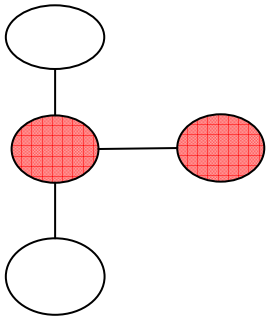
GDSNにて規定されるセキュリティ機能に準ずる

3. 関連対象組織・企業・団体等

GS1 Japanもしくは第三者機関

ドメインの評価対象：データプール

1. セキュリティ要件



- 接続するレジストリ機能、データプール、データソース/データレシピエントの認証
- GDS準拠のデータに対する完全性
- データの証拠性（否認防止）
- 可用性
- 耐複製性

2. セキュリティ機能

レジストリ機能およびデータプールに接続を行う場合はGDSNにて規定されるセキュリティ機能に準ずる。

データソース/データレシピエントへの接続については原則GDSNにて規定されるセキュリティに準ずるが、データプールとデータソース/レシピエントが同一ドメインである場合は当該ドメインの規定するセキュリティポリシに基づく。

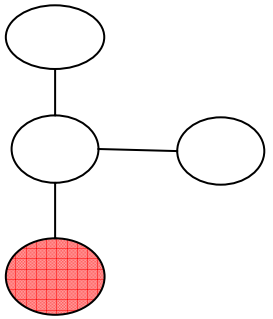
3. 関連対象組織・企業・団体等

データプール事業者、サービスプロバイダー

ドメインの評価対象：データソース / データレシピエント

1. セキュリティ要件

+ データプールの認証
+ データプールから送付されるデータの証拠性（否認防止）
+ 認可
+ 耐複製性



2. セキュリティ機能

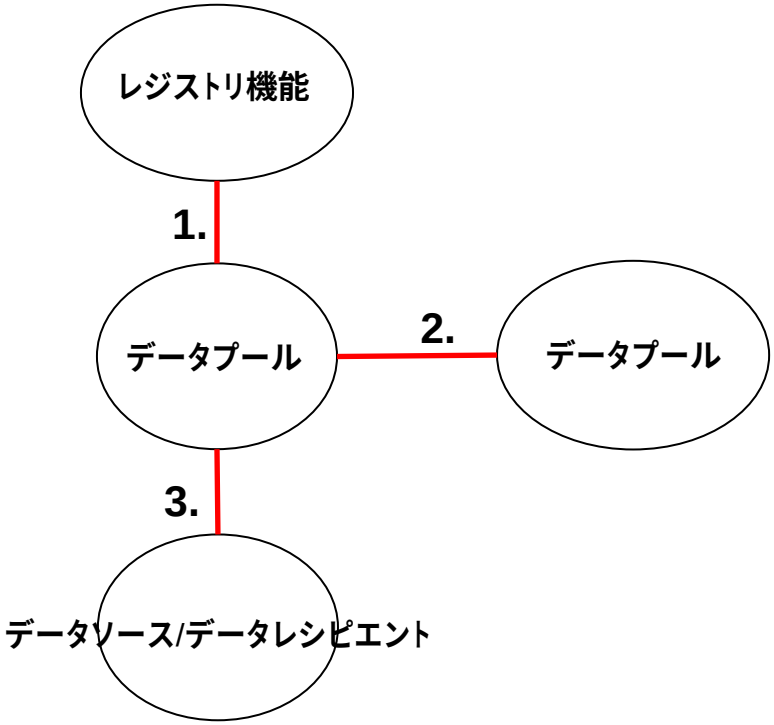
データプールに接続を行う場合はGDSNにて規定されるセキュリティ機能に準ずる。

3. 関連対象組織・企業・団体等

メーカー、卸売業、小売業

ドメイン間通信の評価対象

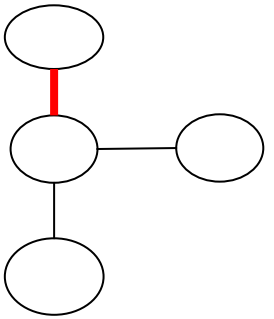
+ **評価対象モデルにおいてドメイン間通信の評価対象は以下の3つ**
  1. **レジストリ機能とデータプール**
  2. **データプールとデータプール**
  3. **データプールとデータソース/データレシピエント**



ドメイン間通信（レジストリ機能とデータプール）

1. セキュリティ要件

+ 情報に対する機密性
+ GDS準拠のデータに対する完全性



2. セキュリティ機能

原則としてセキュリティ要件を満たすデータの暗号化および署名を行う。

※AS2を利用する場合は、AS2のセキュリティポリシに基づく。AS2を利用しない他の通信方式(他の通信レイヤ)を利用するはレジストリ機能とデータプール相互で定義される一定のセキュリティポリシに基づく。(例：IPSec, SSL-VPN等)

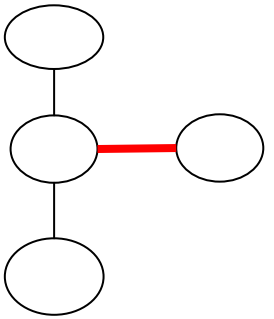
3. 関連対象組織・企業・団体等

GS1 Japan、第三者機関、データプール事業者、サービスプロバイダ

ドメイン間通信（データプールとデータプール）

1. セキュリティ要件

+ 情報に対する機密性
+ GDS準拠のデータに対する完全性



2. セキュリティ機能

原則としてセキュリティ要件を満たすデータの暗号化および署名を行う。

但しソースデータプールとレシピエントデータプールが同一ドメイン内に存在する場合は、当該ドメイン内部のセキュリティポリシに基づく。
(例：WWRE)

※AS2を利用する場合は、AS2のセキュリティポリシに基づく。AS2を利用しない他の通信方式(他の通信レイヤ)を利用するはレジストリ機能とデータプール相互で定義される一定のセキュリティポリシに基づく。
(例：IPSec, SSL-VPN等)

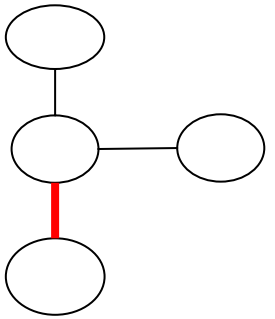
3. 関連対象組織・企業・団体等

データプール事業者、サービスプロバイダ

ドメイン間通信 (データプールとデータソース/データレシピエント)

1. セキュリティ要件

+ 情報に対する機密性
+ GDS準拠のデータに対する完全性



2. セキュリティ機能

原則としてセキュリティ要件を満たすデータの暗号化および署名を行う。

但しデータプールドメインとデータソース/データレシピエントドメインが
同一ドメインである場合は含める場合は当該ドメインのセキュリティポリシに基づく。
に存在する場合は、当該ドメイン内部のセキュリティポリシに基づく。
(例：データプール事業者がサービスとしてデータソース/データレシピントドメインを
管理し、データソースドメインに対してWebベース等のASPサービスを提供する場合)

※AS2を利用する場合は、AS2のセキュリティポリシに基づく。AS2を利用しない他の通信方式(他の通信レイヤ)を利用するはレジストリ機能とデータプール相互で定義される一定のセキュリティポリシに基づく。
(例：IPSec, SSL-VPN等)

3. 関連対象組織・企業・団体等

データプール事業者、サービスプロバイダ、メーカー、卸売業、小売業

5. 詳細設計に向けた留意点

- **セキュリティについて**
  - 責任分解点の定義
  - セキュティポリシの策定
  - PKIの適応
    - WEBサーバ、XMLデータ、アプリケーション、利用者
  - 評価対象の細分化
    - 暗号通信、相互認証、改竄防止、事後否認
    - 電子証明書の有効期間
    - ドメイン内における細分化
      - データへアクセスするプログラム
      - 利用者等
  - システム上のログに対して
    - データの監査
- **認証局について**
  - 海外との連携
  - 登録管理主体の決定
  - 発行者の決定
  - 運用規程の策定