資料３

2020年 7月31日

DXサービスに必要なサイバーセキュリティ対策

ＮＲＩセキュアテクノロジーズ株式会社
デジタルセキュリティコンサルティング部

【本日お話ししたいこと】
DXサービスに必要なサイバーセキュリティ対策

① 設計・開発前にリスク評価

⇒ サービスリスク分析

事前に知っていれば‥
の残念パターンをなくす

② サービス仕様の脆弱性の継続的な収集

⇒ 脆弱性情報の収集＋迅速改修

賢者は過去に学ぶ

③ 仕様上のリスクを統括する組織組成

⇒ Service SIRT

プロアクティブ推進組織
サービス企画者のサポーター

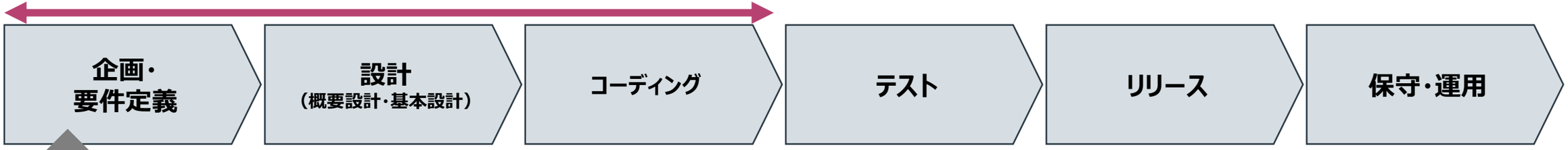
DXサービスのセキュリティでは、“企画・要件定義”段階でのサービス仕様・特性を考慮したリスク分析が重要

セキュリティ・バイ・デザインの定義（NISC）

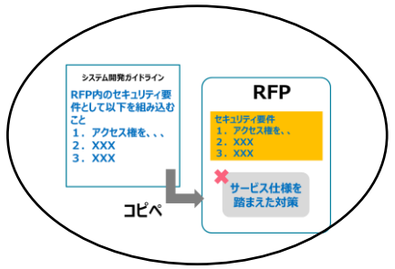
「情報セキュリティを企画・設計段階から確保するための方策」

企画・要件定義行程における脆弱性作りこみ防止策として、標準的なセキュリティ要件を作成することが主流であることから、
昨今セキュリティ・バイ・デザインが議論される際は、設計・開発工程における脆弱性を作りこみ防止策を指すことが多い。

セキュリティ・バイ・デザイン(広義)　＝　企画・設計・開発工程でセキュリティを確保する(≒シフトレフト)



セキュリティ・バイ・デザイン(狭義)　＝　設計・開発工程で脆弱性を作りこまない



会社として定義した標準的なセキュリティ要件を取り込むことで対処

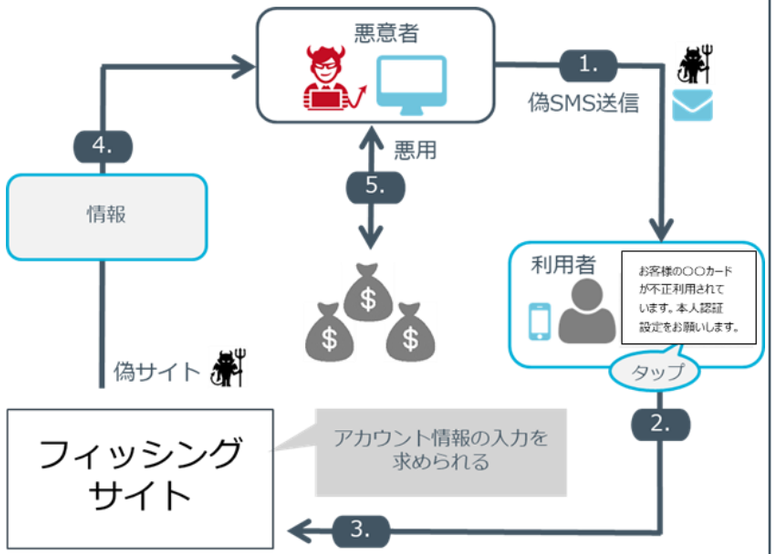
DXサービスの仕様・特性 の考慮が不足！

これら考慮不足(=サービスの脆弱性)を狙う脅威が発生！！

DXサービス上で問題となっている新たなリスクの具体例

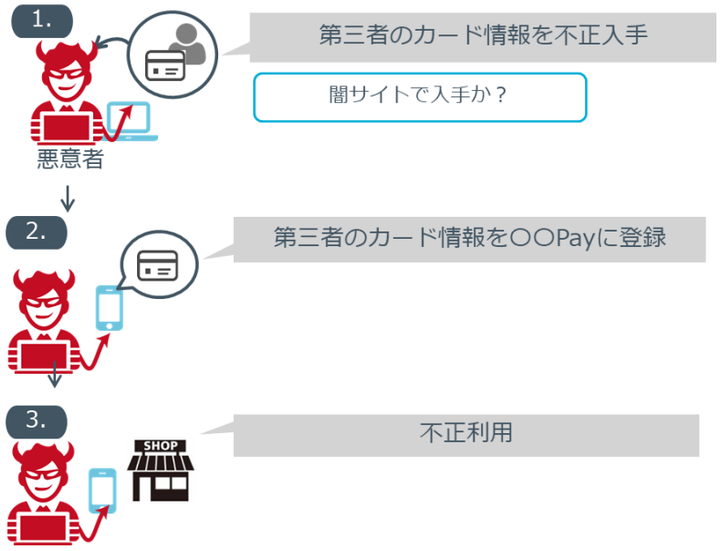
なりすまし

- なりすましログインしてキャッシュレス決済を行う
- なりすましログインして物品購入を行う
- なりすましログインしてSNSを利用する



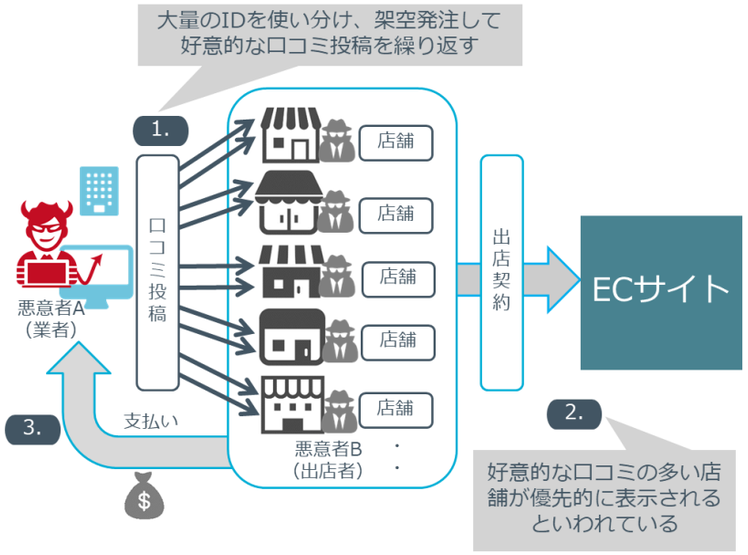
情報紐付

- 他人のクレジットカードを紐づける
- 他人の身分証を偽造してサービス申し込む
- 他人のポイントを自分のアカウントに紐づける



悪用アカウント利用

- 口コミ情報やランキング情報を操作する
- クーポンを大量獲得する
- サブスクサービスの初回特典を利用し続ける



そのほか、プライバシー情報の不適切な利用、コネクティッドデバイスの安全性考慮不足等

DX上のセキュリティリスク＝
デジタル技術の脆弱性＋サービス仕様の脆弱性

不正利用対策はサービス仕様の「隙」≠システムセキュリティ対策はシステムの脆弱性

DXで新たに考慮が必要なサービスリスク

①不正利用
犯罪集団等による
サービス仕様の悪用
(金銭獲得目的)

サービスの穴を悪用

✓なりすまし
✓盗難クレカ利用
✓クーポン大量獲得

②システムセキュリティ
高度技術を有する
ハッカーによる
システムに対する攻撃
(情報窃取・サービス妨害等)

攻撃

✓IoT機器の脆弱性
✓APIの設定不備

デジタルサービスの構成要素

サービスの隙

ビジネスモデル
- QR決済
- 民泊サービス
- 配車サービス
- AIチャット
- etc.

ユースケース
- 外部IDを用いて利用可能
- 独自ポイントを配布
- 活動状況を友人に共有
- etc.

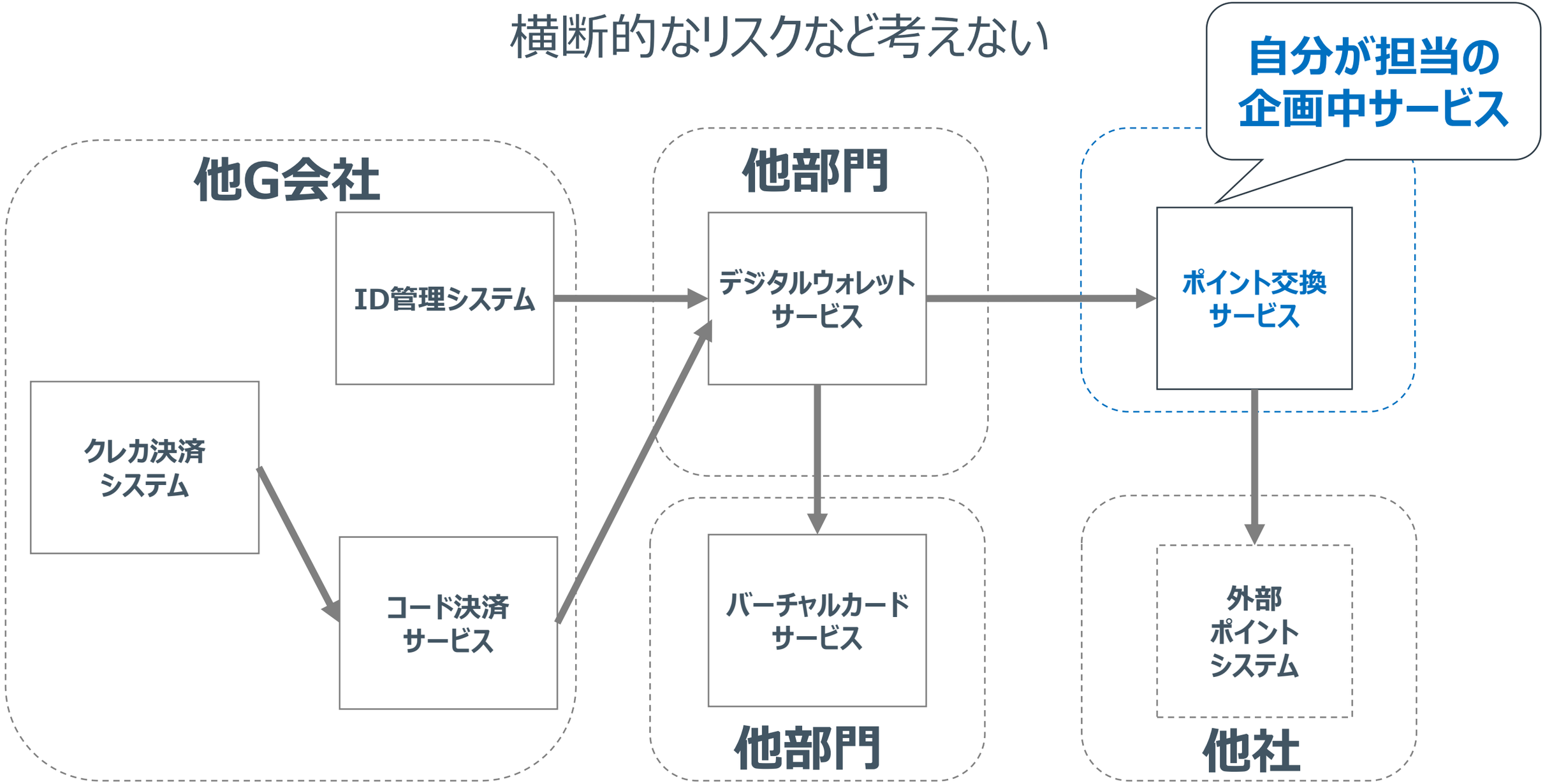
システムの脆弱性
- インフラ
- サーバ
- Webアプリ
- etc.

サービスリスク分析のために
サービス仕様への脅威情報の収集が必要

ITシステムへの脅威情報 (システムの脆弱性を突いた攻撃)		サービス仕様への脅威情報 (サービス仕様の穴を突いた攻撃)
サイバー攻撃の攻撃傾向 Threat Landscape 例：マルウェアの統計情報	戦略 Strategic	サービス仕様への攻撃傾向 Scammer Motivation 例：サイバー犯罪の傾向
所謂サイバー攻撃の手法 Cyber Attack Method 例：攻撃方法の解説ブログ	作戦 Operaional	サービス仕様の悪用手法 Scam Method 例：決済不正や詐欺の事例
攻撃者の痕跡/脆弱性 IoC/TTPs 例：IPブラックリスト	戦術 tactical	サービス仕様の悪用の兆候 Sign of Scam 例：不正行為成功のつぶやき

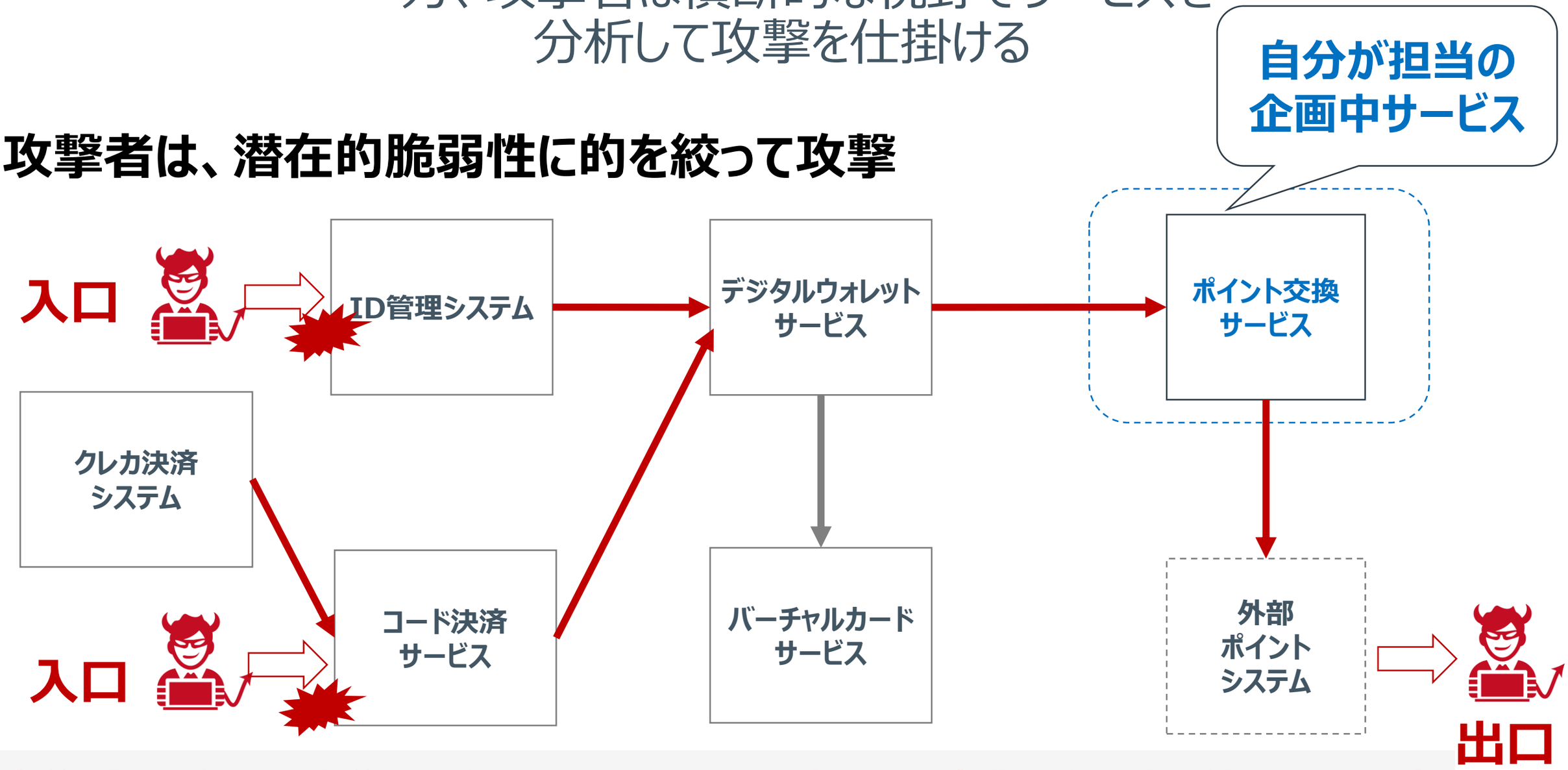
ニュースサイト、ブログ、ソーシャルメディア等の公開情報に有益な情報が多く存在する。

サービス企画者は自分の担当範囲しか見ない
横断的なリスクなど考えない



一方、攻撃者は横断的な視野でサービスを分析して攻撃を仕掛ける

攻撃者は、潜在的脆弱性に的を絞って攻撃



事前に横断的なリスク分析を旗振りするのは難しい（そもそも事業投資起案の範囲ではない）

Service SIRT（SSIRT）とは

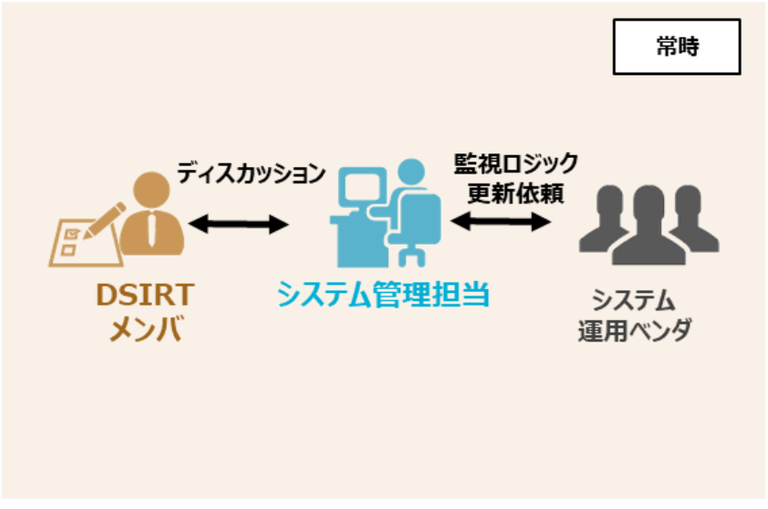
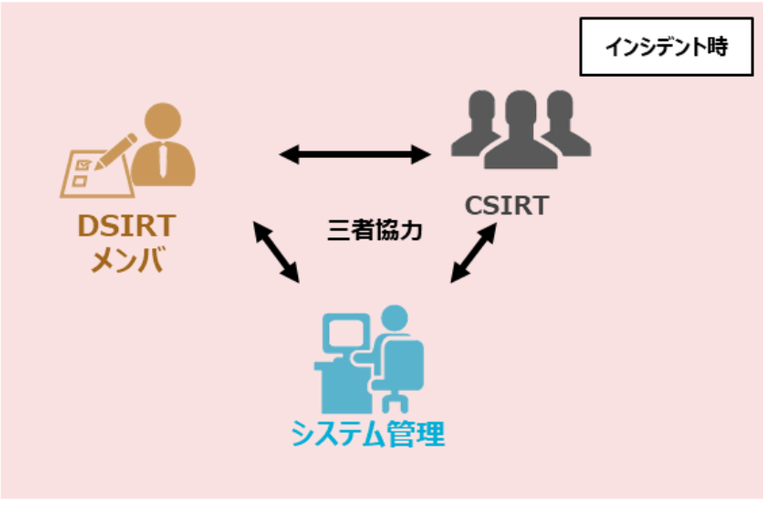
デジタルサービスのサービス要件上に存在するリスクに対応するには、**各事業部が企画するサービスを横断的・俯瞰的に確認できる体制が必要**である。一方で、これらリスクはサービス内容に依存し、その対策はサービス仕様に盛り込む必要があることから、**統制的な立場(第２線)ではなく、より事業部門に近い立場で、実務的な提言・サポーターとしての機能が求められる**。

上記機能を有する組織として、**一部の先進企業では専門組織(Service SIRT)を構築**しはじめている。
SSIRTは、**事業部と横並びの独立部署**、もしくは、**各事業部のセキュリティ担当を集めたバーチャル組織として構築される**ことが多い。

SSIRT: 事業部門と同等の立場(第１線)で、事業部門におけるセキュリティ対応を支援
CSIRT: 本社機構の立場(第２線)で、セキュリティガバナンスの実行を支援

SSIRTの主要な業務

SSIRTの主要な業務として、下記３つが挙げられる

サービス企画時のサービスリスク分析	デジタルサービスの不正利用の検知	大規模サービス悪用発生時の対応
		
デジタルサービス企画時に、ビジネスモデルやユースケース等のサービス仕様に脆弱な点が無いかリスク分析を実施。 (RFP/RFIの提示前に実施)	デジタルサービスの不正を検知するための監視ロジックの設計を支援。 なお、監視ロジックは類似サービスの脅威事例を踏まえ随時アップデートを実施。	大規模サービス悪用発生時に、CSIRTやシステム管理担当と協力し、インシデント対応を実施する。

NRI SECURE

NRI SecureTechnologies, Ltd.

www.nri-secure.co.jp