ARIS
Advanced Research & Information Service

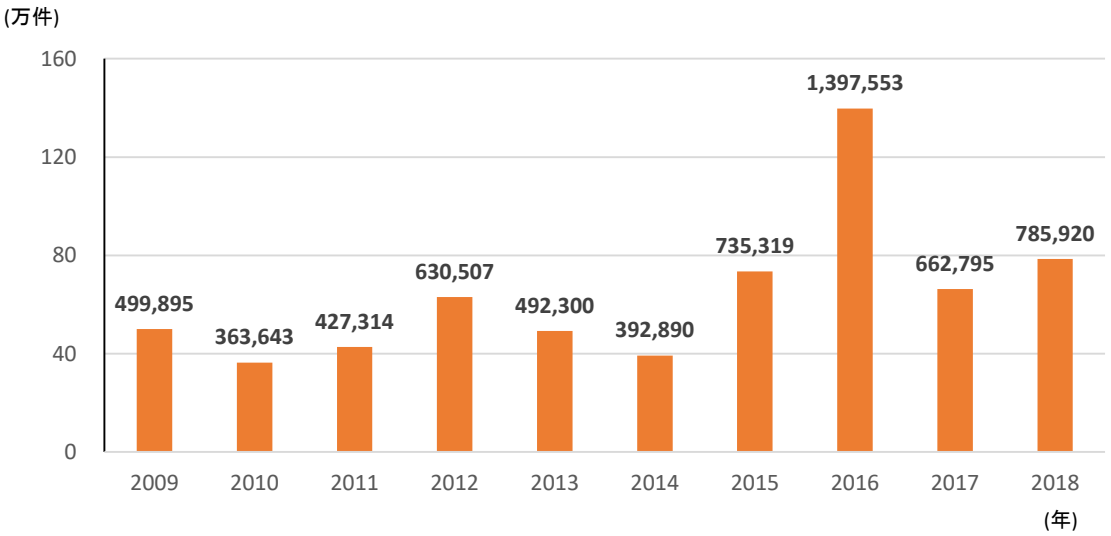
“AI 技術”で解決する医療機関システムの脆弱性対策

2019年12月

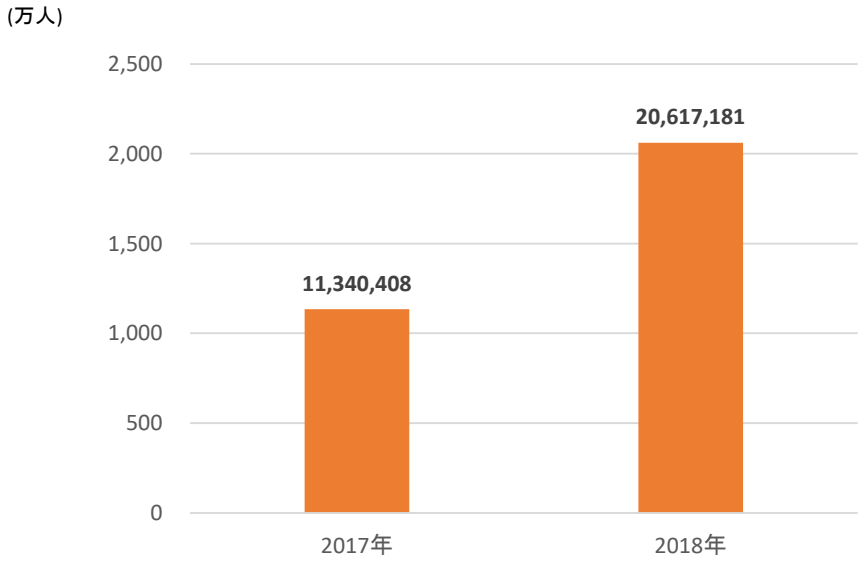
株式会社アリス AIセキュリティ事業部

2018年度の情報セキュリテイの概況

- Facebookが2900万人の個人情報流出
- マリオットホテルチェーンから3億8千300万件の顧客情報流出
- シンガポール最大の医療グループSingHealthから150万人の患者の個人情報が不正コピーされた
- 米国インディアナ州ハンコックリージョナル病院ではランサムウェアの感染により暗号化解除のために700万円を支払う
- 奈良県の病院で電子カルテシステムがランサムウェアに感染、1133人分の診療記録が暗号化される
- フィッシングサイトの総数は、2017年度比18.6%の増加



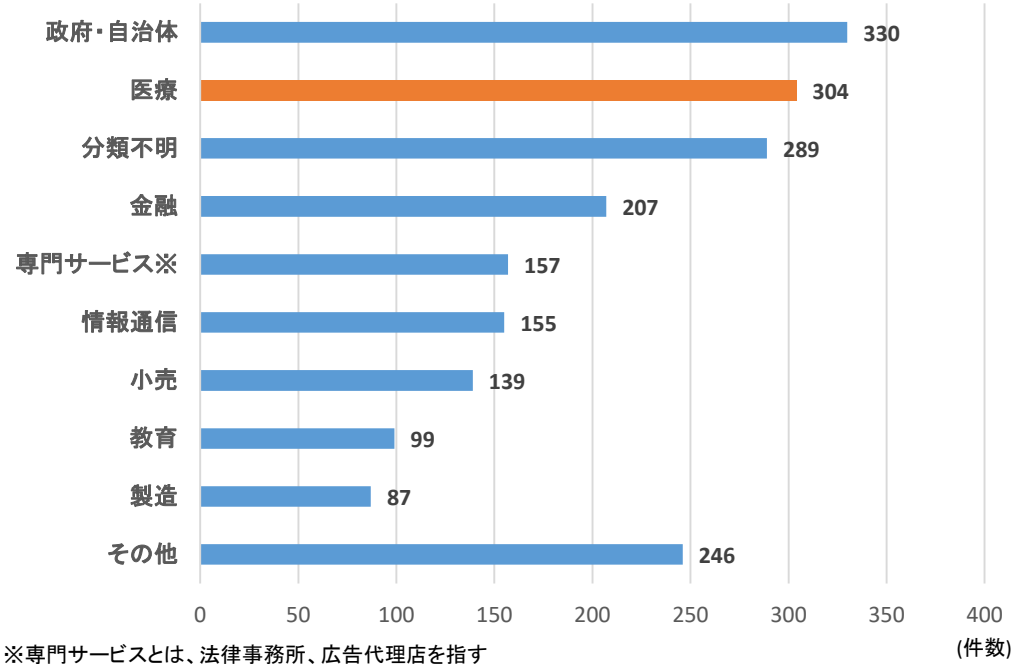
■世界における届け出されたフィッシングサイト件数
(出典)APWG「Phising Activity Trends Report」(2009～2018年)を基にIPAが作成



■フィッシングサイトに誘導された利用者数推移
(出典)トレンドマイクロ社「2018年 年間セキュリティラウンドアップ」を基にIPAが編集

医療機関におけるセキュリティの現状

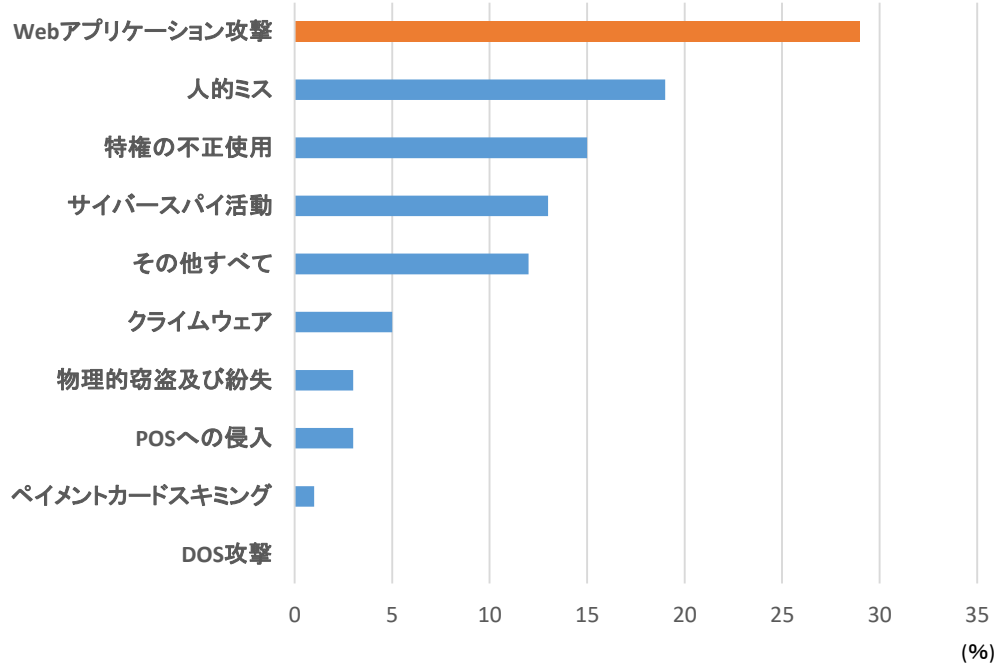
- 2018年度に発生した情報漏洩インシデントのうち、医療分野は2位
- 情報漏洩インシデントはWebアプリケーション攻撃が29%
- 個人情報が狙われている－医療機関は個人情報、機微情報の宝庫



※専門サービスとは、法律事務所、広告代理店を指す

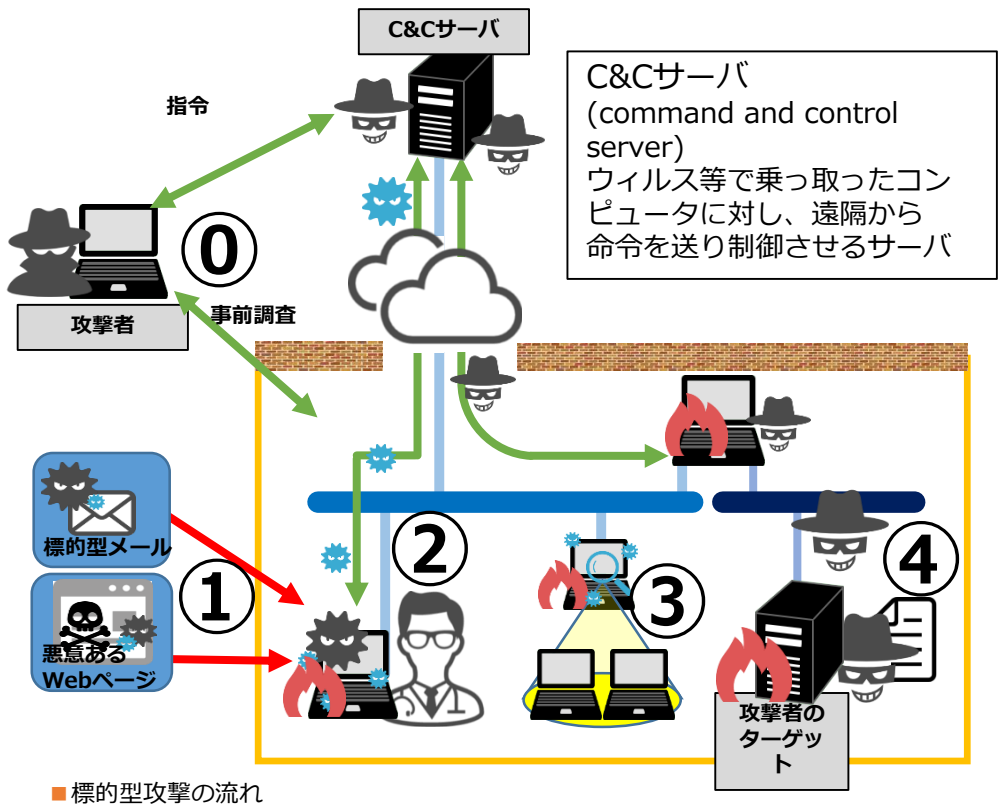
■業種別の情報漏洩の件数
(出典)Verizon 社「2019 Data Breach Investigations Report」を基にIPAが作成

出典



■情報漏えい事件の分類
(出典)Verizon 社「2019 Data Breach Investigations Report」を基にIPAが編集

標的型攻撃の手口



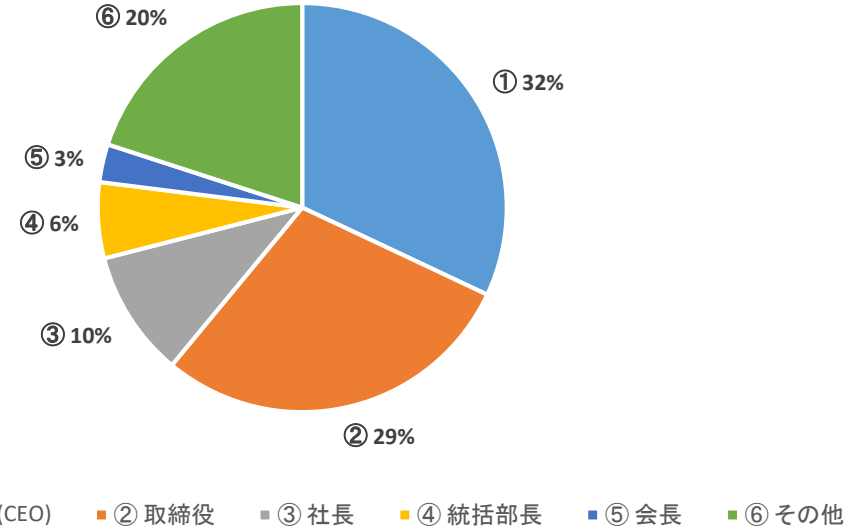
C&Cサーバ
(command and control server)
ウィルス等で乗っ取ったコンピュータに対し、遠隔から命令を送り制御させるサーバ

■標的型攻撃の流れ
(出典)IPA「標的型サイバー攻撃の脅威と対象」を基に編集

⓪［事前調査段階］
ターゲットとなる組織を攻撃するための情報を収集する。
①[初期潜入段階]
標的型メールや、Webサイト閲覧を通してウィルスに感染させる。
②[攻撃基盤構築段階]
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い新たなウィルスをダウンロードする。
③[システム調査段階]
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を元に新たな攻撃を仕掛ける。
④[攻撃最終目的の遂行段階]
攻撃専用のウィルスをダウンロードして、攻撃を遂行する。

このような動きを検知して事前に防ぐことが大事

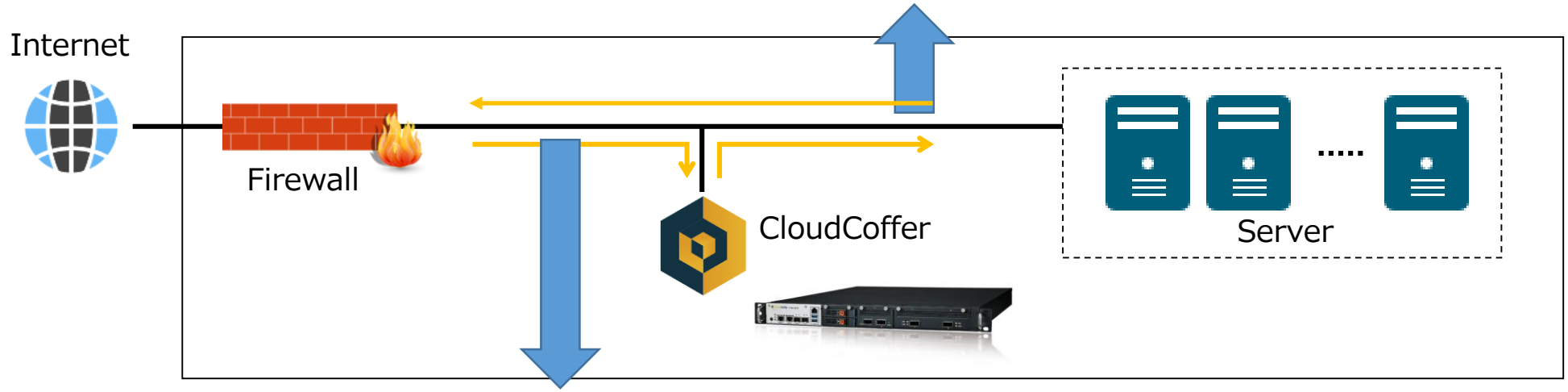
重役（権限、信用を持っている）人がなりすましに利用される



■ビジネスメール詐欺関連のなりすましに利用された職位の割合
(出典)トレンドマイクロ社「2018年 年間セキュリティラウンドアップ」を基にIPAが作成

攻撃からどのようにシステムを守るか

・怪しいアドレスへの応答やサーバからの不正な応答を検知し遮断する。
・バックドア（攻撃に利用される裏口）を作ろうとするような動きを検知し遮断する。
・システム情報や機密データを外部に漏洩しようとする通信を検知し遮断する。
・外部の特定IPのアドレスとの継続的な通信や、攻撃の疑いがある通信を制限する。



・様々なシステムの脆弱性を突いてシステムに侵入を試みる攻撃を検知し遮断する。
・システムに負荷をかけ利用不能にする攻撃を検知し遮断する。
・フィッシングサイト（情報を奪う詐欺サイト）に誘導される攻撃を検知し遮断する。
・重要な情報が格納されているデータベースへの攻撃を検知し遮断する。
・Webサイトを改竄したり、データを窃盗するような攻撃を検知し遮断する。
・CMS（Webサイト管理ソフト）の脆弱性を突きWebサイトを乗っ取るような攻撃を検知し遮断する。

CloudCofferは何が優れているのか

担当者の悩みや課題

1. 次々の現れる新たな脅威（ゼロデイ攻撃）、脆弱期間の問題の情報収集に追われる
2. 知らないうちにセキュリティシステムを突破する事象が発生していないか不安
3. 続々と作り出される新たなマルウェアやステルス型攻撃への不安
4. 頻繁に発生するシグネチャファイル更新などのメンテナンス、本番環境に適応するための導入試験など煩わしい作業
5. 手間のかかる過検知・誤検知を防ぐための設定作業
6. 脅威情報の入手、セキュリティイベント発生時の確認作業など人手のかかる作業
7. 攻撃の種類ごとに様々な種類のセキュリティ製品が必要
8. 人材不足と増大する既存システムの維持費用

CloudCoffer が提供するもの

1. 脆弱期間なし、不安を解消
2. 人間が見るようにトラフィックをチェックし、不審なトラフィックを見逃さない
3. SandBox (Option) による新たなマルウェアの検出、ステルス型攻撃もキャッチ
4. シグネチャ更新、パッチ不要
5. 過検知・誤検知がない（過検知を防ぐ前に、1か月くらい試行してホワイトリストの調整をすることが望ましい）
6. 確認作業はミニマム
7. IPS/WAF/Sandbox機能をひとまとめ
8. 人間の代わりに判断、少コスト

CloudCofferが脅威・攻撃強い理由

カーネギーメロン大学由来のAIエンジン
世界中に配置した15万か所のハニーポットを使って脅威を収集し、ラベル付けをしながら学習
姉妹企業のRayAegisの200名に及ぶホワイトハッカーとAI技術を使った攻撃による攻撃から学習
ヘッダーだけではくペイロードまでチェックし、脅威の有無を確認

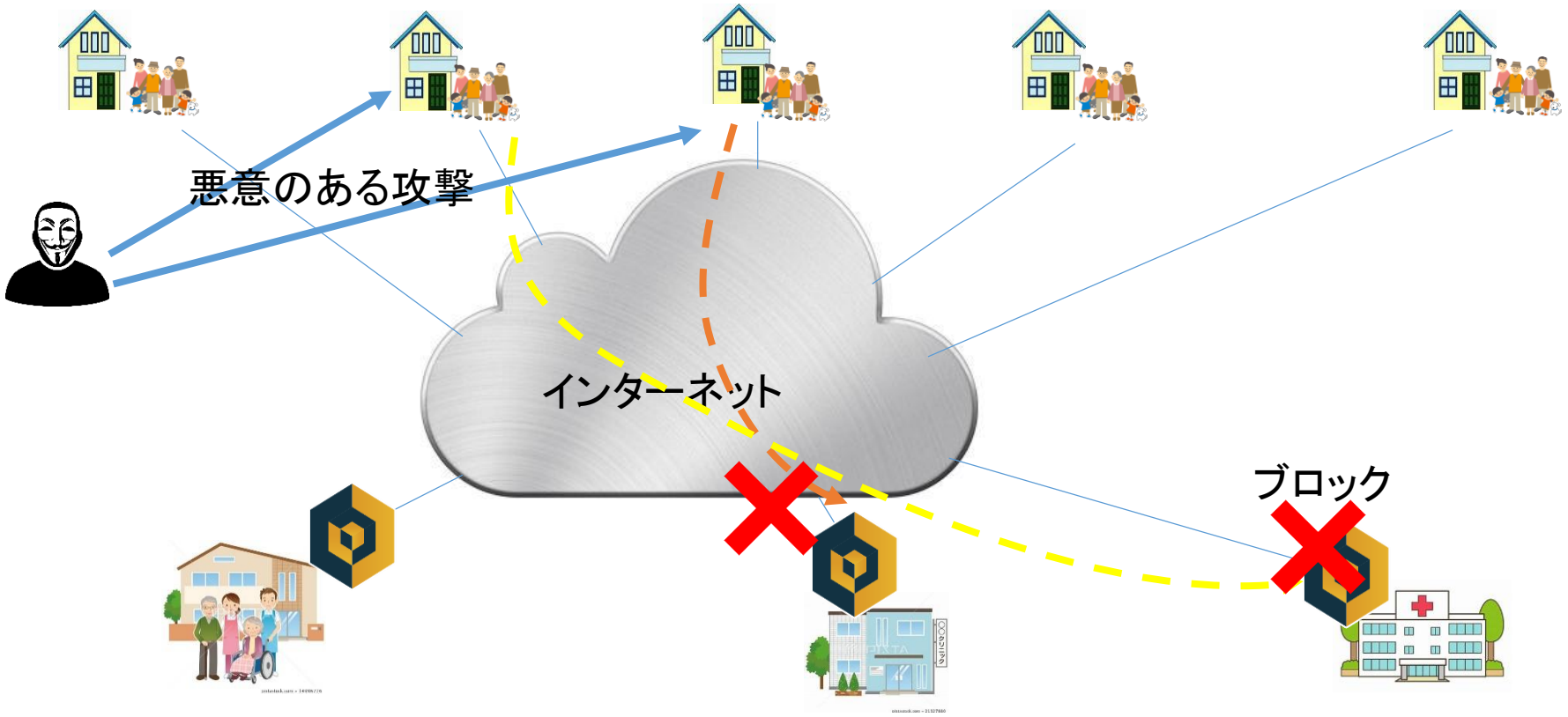
脅威・攻撃

検知・防御

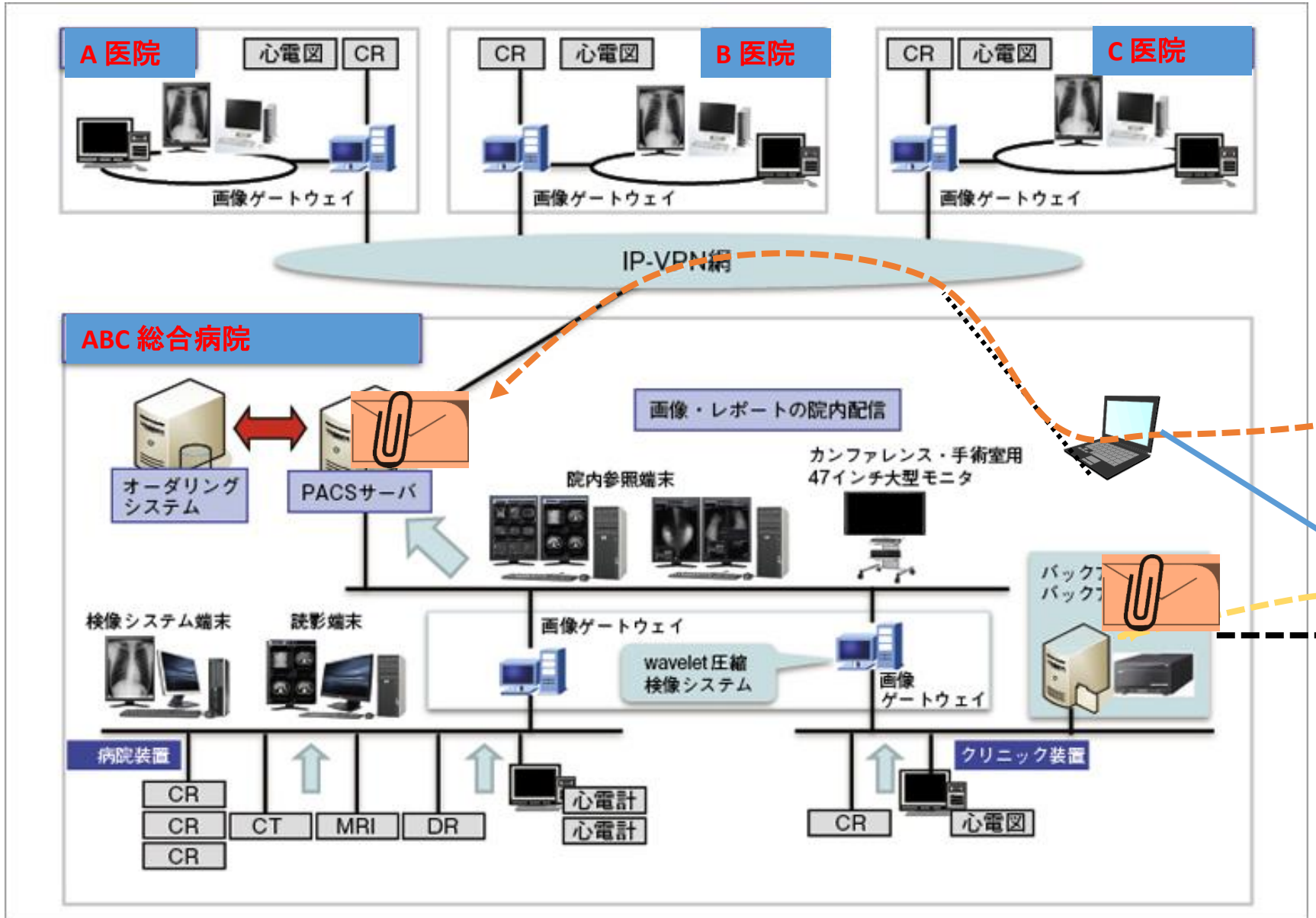
CloudCoffer

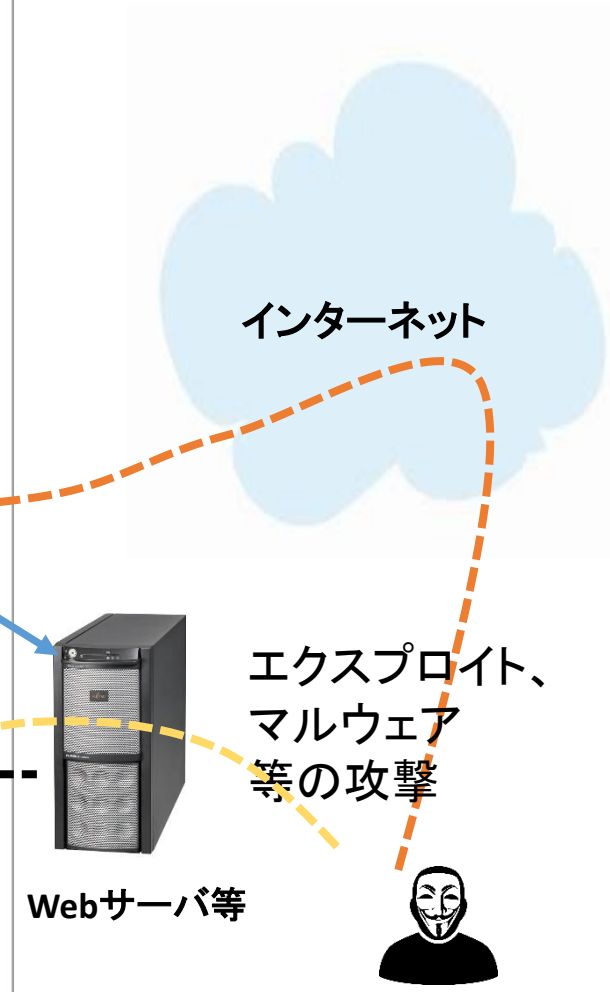
病院ネットワークにおけるCloudCofferの適用

- 患者宅から病院へのデータ送受信で使われるインターネット経路を病院側の出入り口で安全性確保

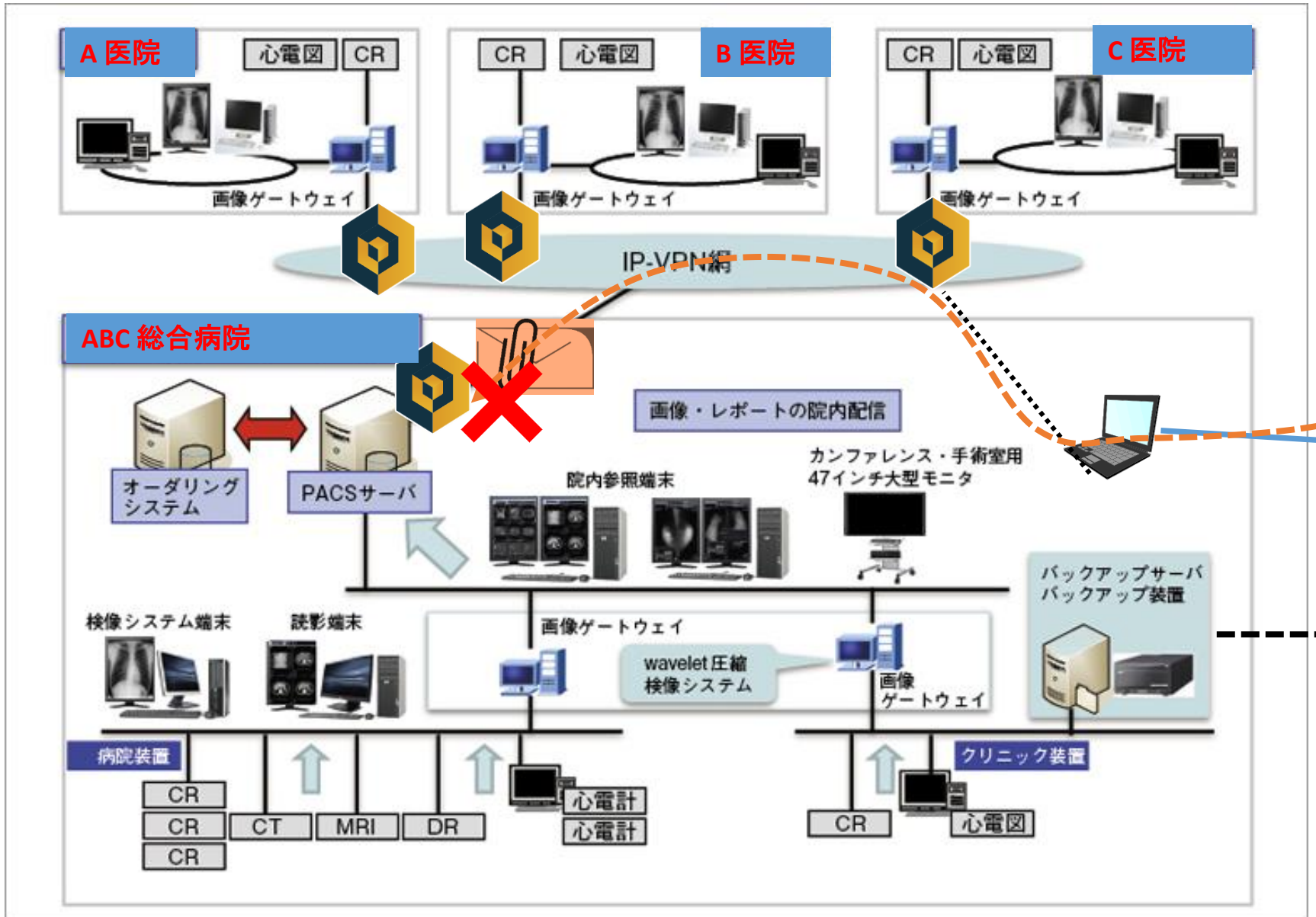


病院内ネットワークにおけるCloudCofferの適用



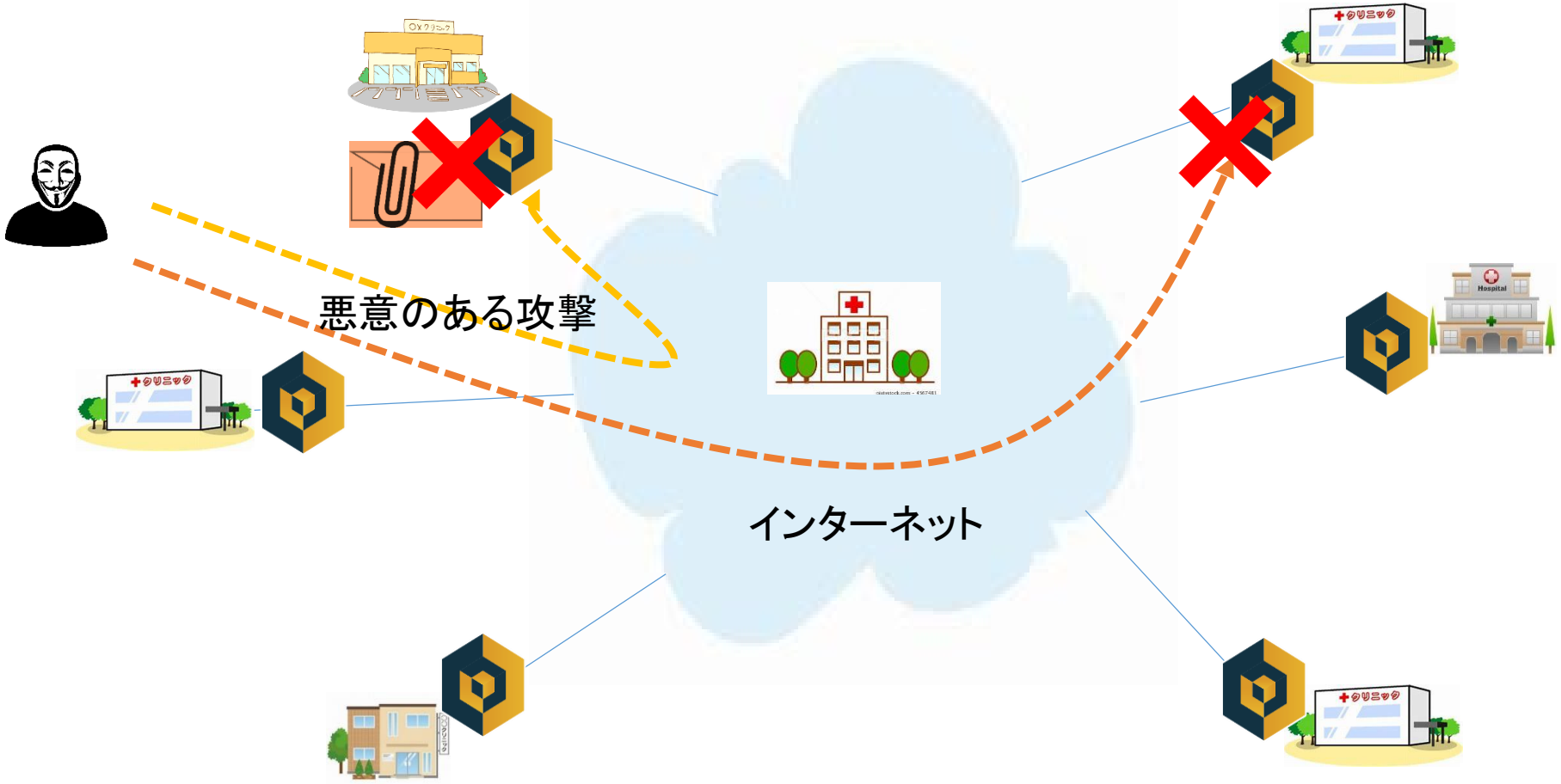


病院内ネットワークにおけるCloudCofferの適用



バーチャル総合病院構想におけるCloudCofferの適用

- 病院間のデータ連携で使われるインターネット経路を出入り口で安全性確保
- 1つの病院におけるセキュリティ侵害が他の病院に影響を与えない



ARIS
Advanced Research & Information Service

ご清聴ありがとうございました