ARIS
Advanced Research & Information Service

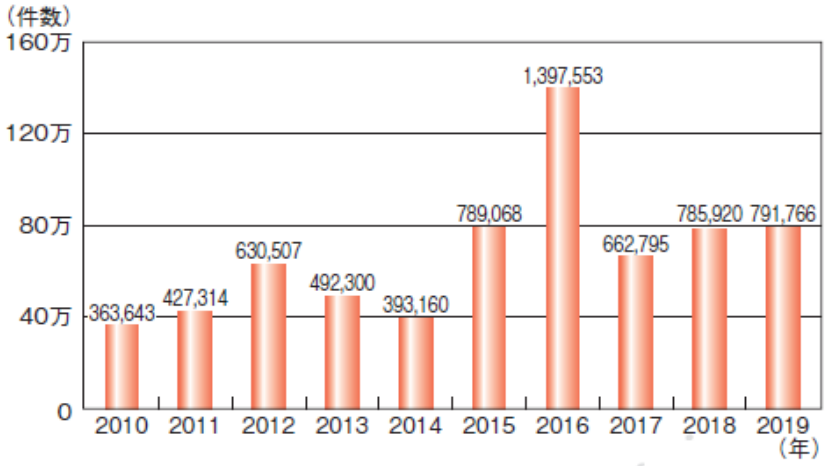
AIによる
セキュリティ対策

2020年12月
株式会社アリス AIセキュリティ事業部

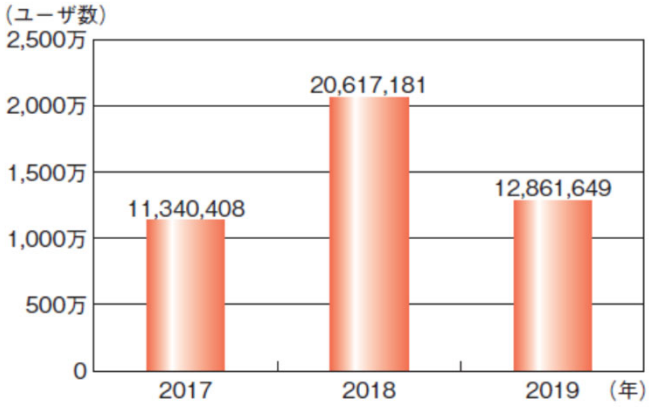
2020年度の情報セキュリテイの概況

- 2019 年7 月に米国の大手金融会社（Capital One Financial Corp）の1 億人を超える顧客情報が流出(WAF設定ミスを突いたSSRF攻撃）
- 2019年7 月に開始したスマホ決済サービスでのアカウント不正利用により800人を超える被害が発生
- 日本へのEmotet のばらまき型メールによる攻撃急増
- 2020 年1 月には複数の防衛関連企業から不正アクセスによる情報流出が流出
- 2020 年6 月にはホンダでランサムウェアにより工場の生産を停止 （医療分野でもIoT 機器への攻撃の脅威）
- コロナ禍により、リモートワークへのシフトやオンラインサービスへの依存度が高くなっ たことから、DDoS攻撃が2019年第4四半期から2020年第1四半期に542%に急増した。○ 出典：DDoS Threat Report 2020 Q1 (Nexuguard)
- 2020年9月10日、ドイツの大学病院のネットワークシステムがランサムウェア攻撃を受け、院内のサーバー30台以上が感染したことへの対応に追われていたため、緊急医療措置 を必要としていた女性を受け入れることができなかったため死亡した。

既知の対策で防げたはずの被害が多いが、対策が難しいゼロデイ攻撃による情報流出も見られた。



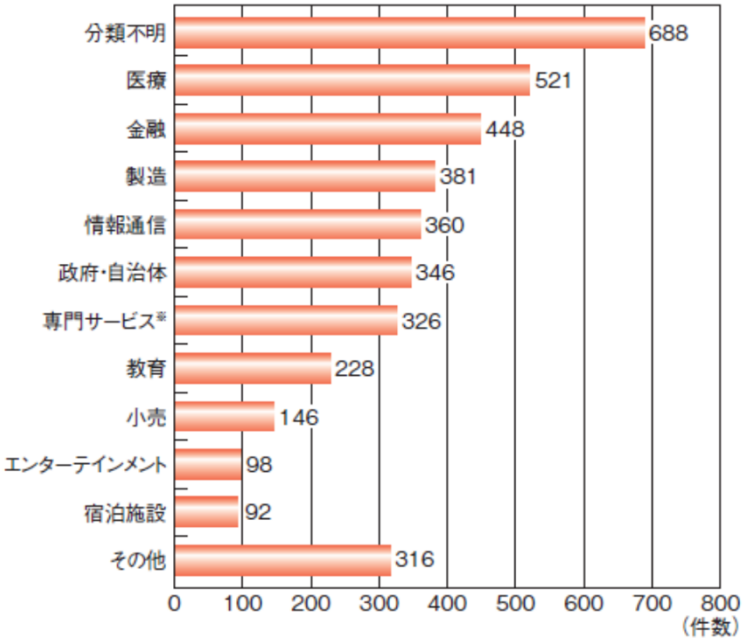
■図 1-1-1　世界における届け出されたフィッシングサイト件数
（出典）APWG「Phishing Activity Trends Report」（2010～2019年）
を基に IPA が作成



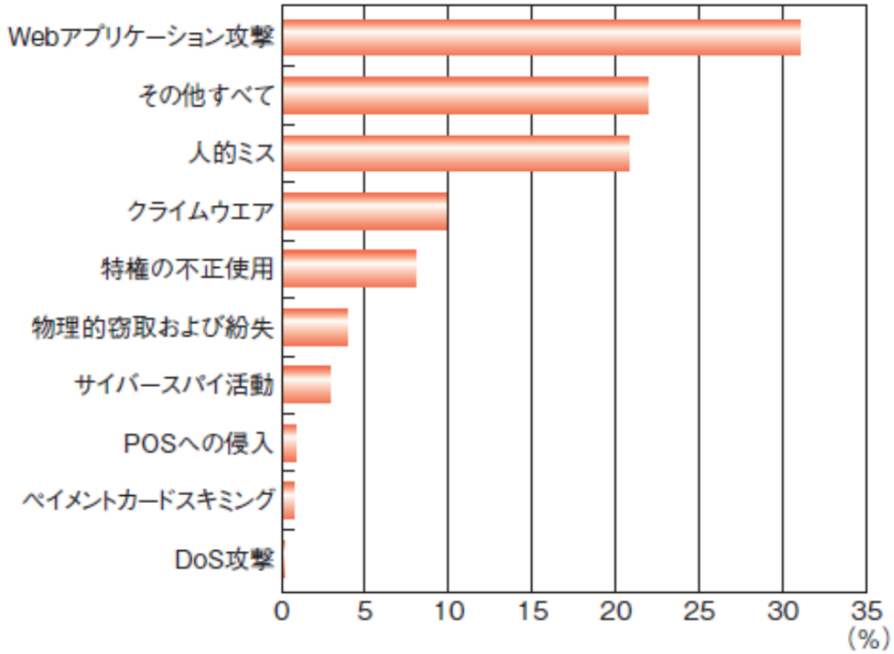
■図 1-1-2　フィッシング関連 URL へのアクセスがブロックされた
ユーザ数推移（全世界）
（出典）トレンドマイクロ社「2019 年年間セキュリティラウンドアップ」及び
「2018 年年間セキュリティラウンドアップ※6」を基に IPA が編集

医療機関におけるセキュリティの現状

- 2019年中に発生した情報漏洩インシデントのうち、医療分野はついに１位
  金融が2位、製造が3位、情報通信が4位
- 情報漏洩インシデントはWebアプリケーション攻撃が31%（前年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、弁護士、会計士、アーキテクト、研究所、コンサルティング会社等を指す



AIは必ずしも正義の味方ではない

- AI技術を応用した様々なセキュリティ製品、サービスが登場
- ハッカーも高度なAI技術を使っている
  - 脆弱点の探索
  - 侵入手口の巧妙化、複雑化
  - うっかりミスの削減（侵入経路の消去など）
  - 防御システムをすりぬける
  - シグネチャーを微妙に変える
  - 膨大な亜種の生成
- ツールはDark Webや闇市場で売買され、だれでも手に入れられる

AI技術を使ったハッキング技術の数々

- Black Hat USA、DEF Conなどでもデモンストレーションされている
  - OpenAIのフレームワークを使用し、セキュリティソフトのスキャンを回避するマルウェアを機械学習によって自動生成
  - DeepHack　ニューラルネットワークによる試行錯誤を経てウェブサービスに侵入し、そこにある脆弱性を発見して悪用
- 100万件のユーザパスワードを1分足らずで見つけるAIツール
- 脆弱点を探し出すツール
- マルウェアをウィルスチェックに見つからないように変身させるツール
- 既知の攻撃を組み合わせて新手の攻撃を作り出すツール

AI技術を使った攻撃は従来手法では防げない

- 簡単なAIツールでシグネチャーを変更
- 既知の攻撃の難読化 （多重暗号、コマンドの分断、既知の攻撃の組み合わせによりシグネチャーマッチングや人の目をすりぬける）
- 新しい脆弱点を探し出す
- 特定の攻撃に対する応答から攻撃文を進化させる

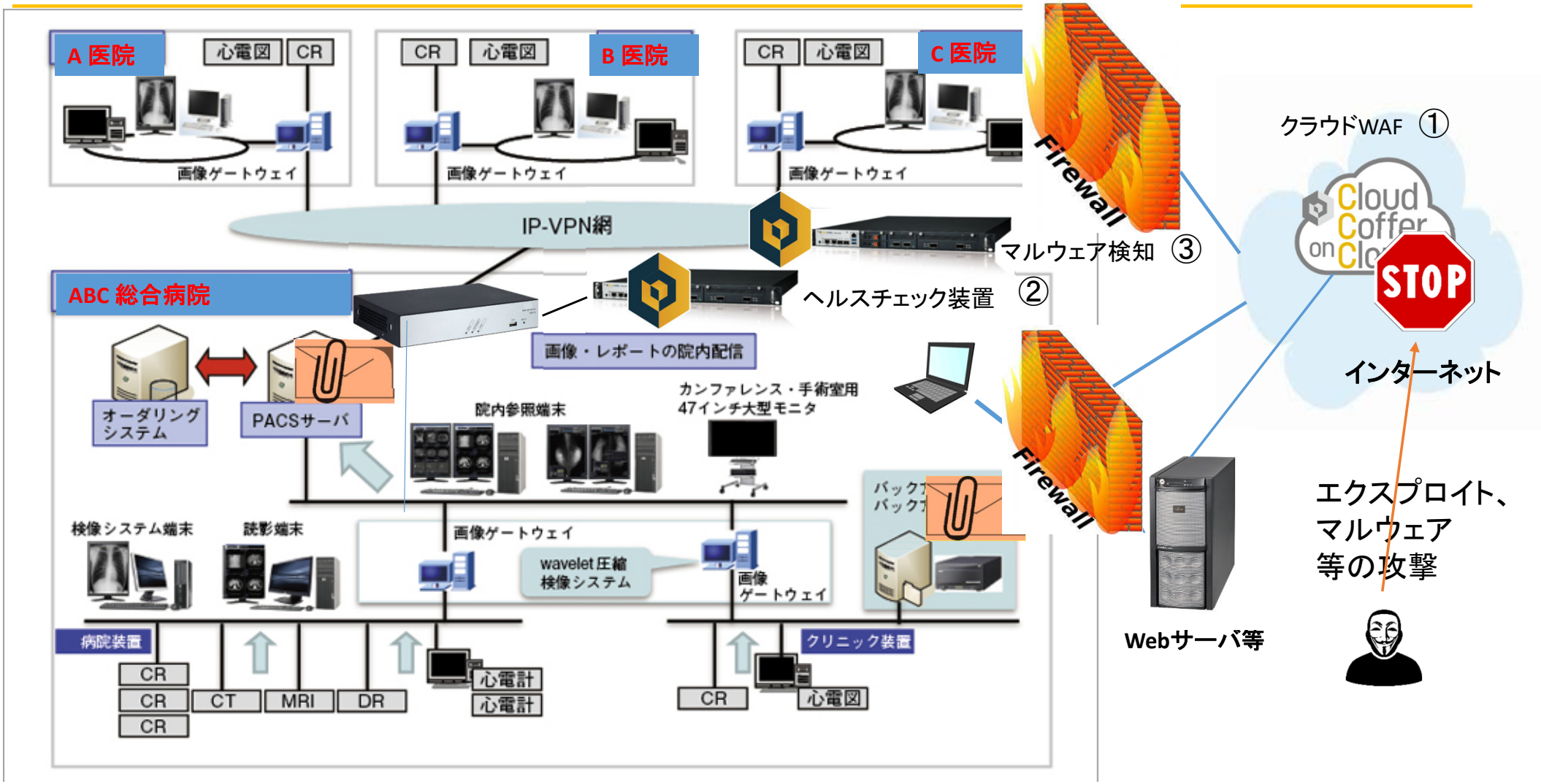
AIでしかAIを使った攻撃は防げない

- シグネチャーに依存しない
- 暗号を自動的に復号化（復号化キーを探す）
- 人の目では見逃がしそうな分断化されたコマンドを見分ける
- レスポンスが正常通信かどうかを確認する
- 使われているコマンド、ポートなどが組み合わせを含めて不自然でないかどうかを確認する
- 一連のコマンドの応答に不自然さがないかを確認する
- 人では見逃がすことを見逃さない（コンピュータは疲れない）

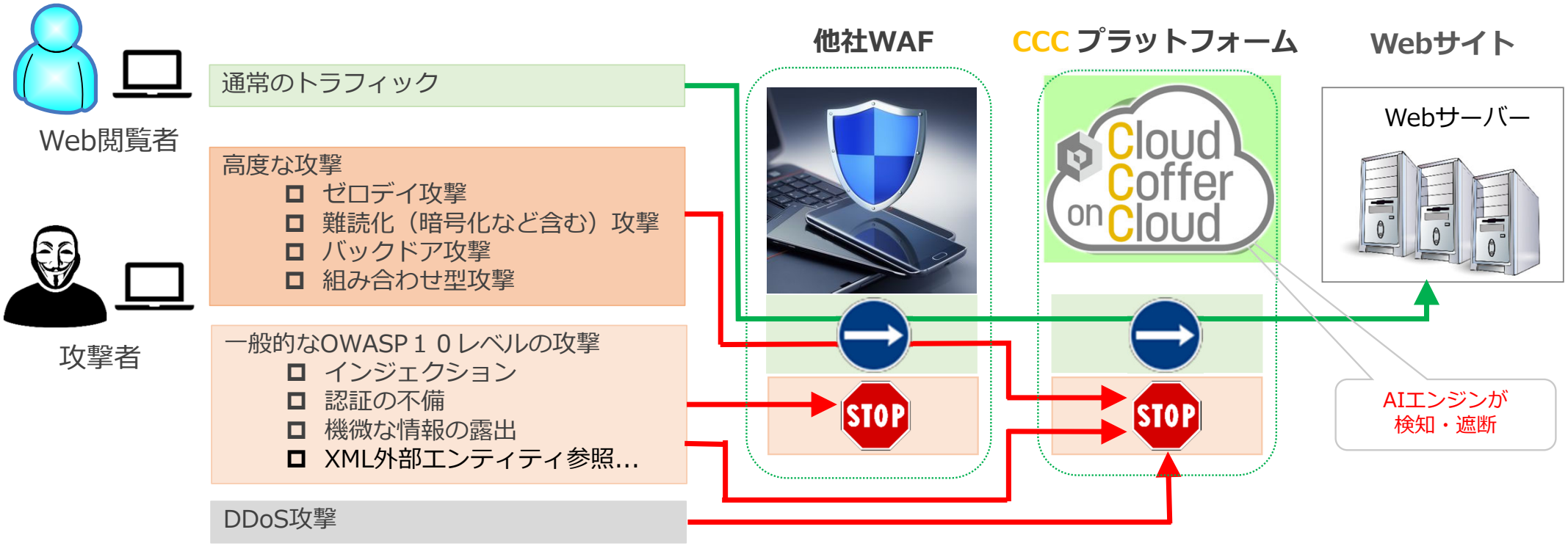
CloudCofferの検知能力が抜群な訳

- AIの本場カーネギーメロン大学で生まれた検知エンジンに、世界中に配置されたハニーポットや銀行、政府機関で検出した本物のきわどい攻撃を学習
- 兄弟会社に優秀なホワイトハッカーを多数抱えたセキュリティ診断会社を持っており、その豊富な経験と知見から侵入手口を検知
- 脆弱性検出や侵入用に開発されたAIツールによって日々検知能力を鍛え上げてきた

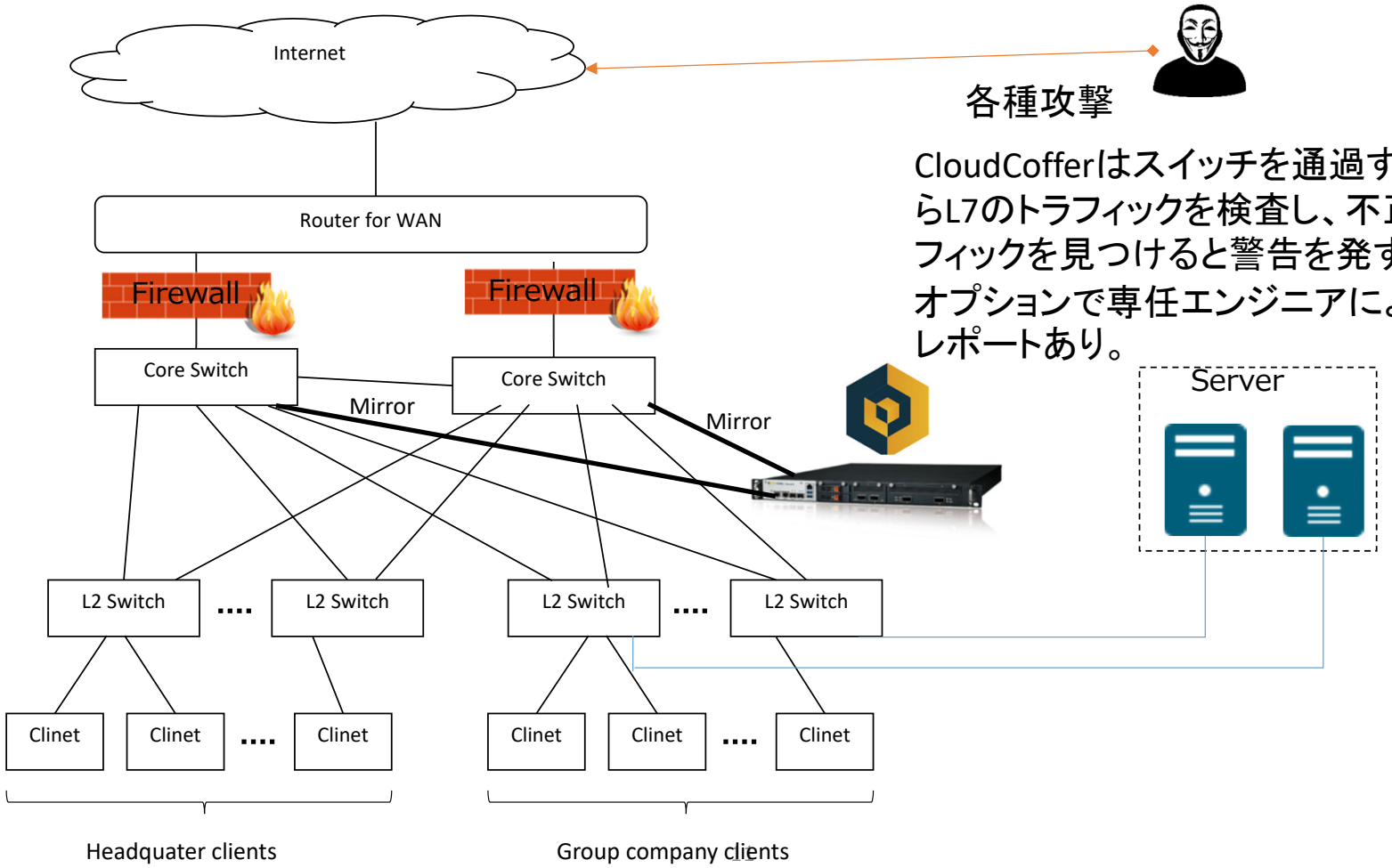
病院内ネットワークにおけるCloudCofferの適用



①クラウドWAFによってWebサーバ経由での侵入・侵害を防御



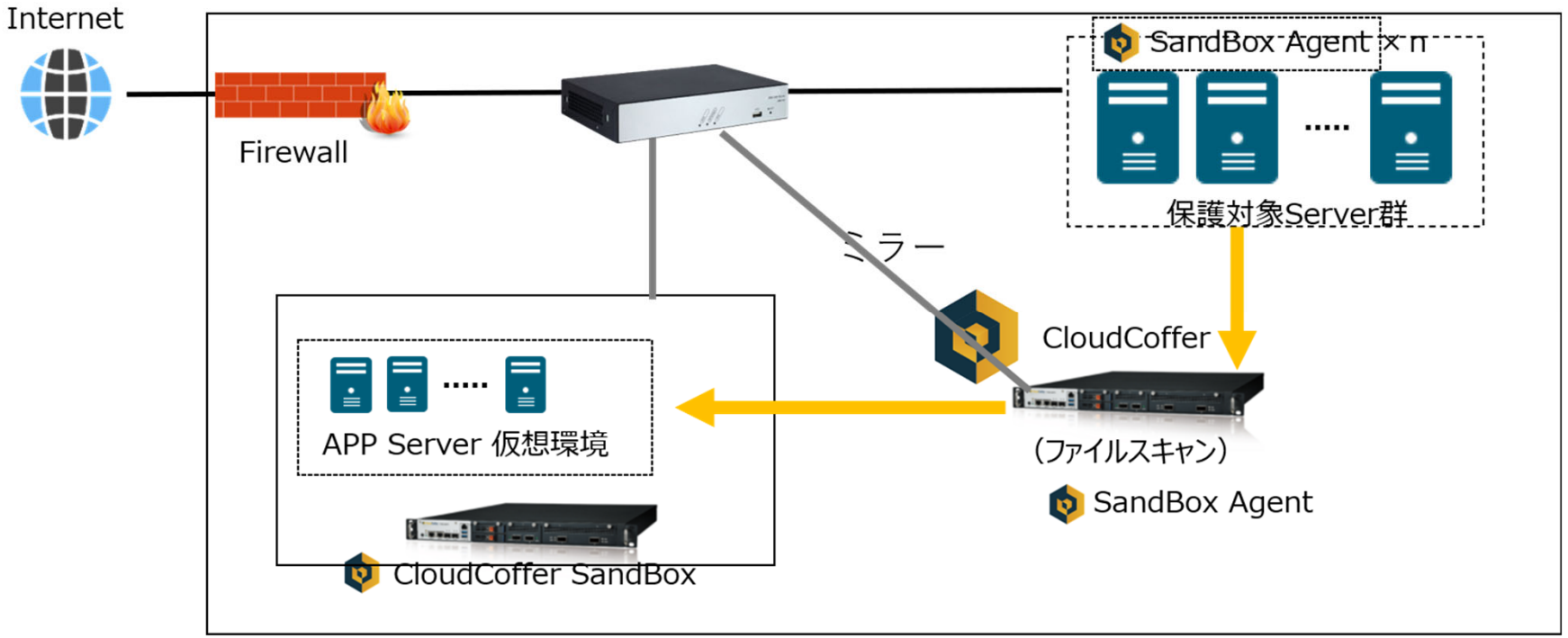
②CloudCofferのAIエンジンで社内ネットワーク上の不正なトラフィックやその痕跡を検知



CloudCofferはスイッチを通過するL4からL7のトラフィックを検査し、不正なトラフィックを見つけると警告を発する。
オプションで専任エンジニアによる月次レポートあり。

③社内システムに埋め込まれたマルウェアを AIエンジンを使ったSandbox機能により検知

保護対象サーバにAgentを導入することで、サーバ内のファイルをAgentがCloudCofferに送り、検査結果から必要なものはさらにSanBoxに送り込んで検疫を行う。（以下の図参照）
CloudCofferはここでは②の不正トラフィック検査用のものを使用。



ゼロトラストとはいうものの

- 多層防御、侵入・汚染からのリカバリは必要
  - FireWall、WAF、IPS、IDS
  - アンチウィルスソフトウェア
  - EDR
  - SandBox
  - NDR (Network Detection and Response)
- システムの脆弱性は定期的にチェック
  - 診断ツール
  - プラットフォーム診断
  - Webアプリケーション脆弱性診断
  - ペネトレーションテスト
  - ヘルスチェック

お問い合わせ　連絡先

株式会社 アリス　A.I.セキュリティ事業部

住所　：〒163-0510　東京都新宿区西1-26-2新宿野村ビル10F
TEL　：03-3340-1053
Mail　：aisec@aris-kk.co.jp
URL　：aris-kk.co.jp, ccc.cloudcoffer.jp, rayaegis.co.jp