当社のサイバーセキュリティ対策について

株式会社 システムプランニング

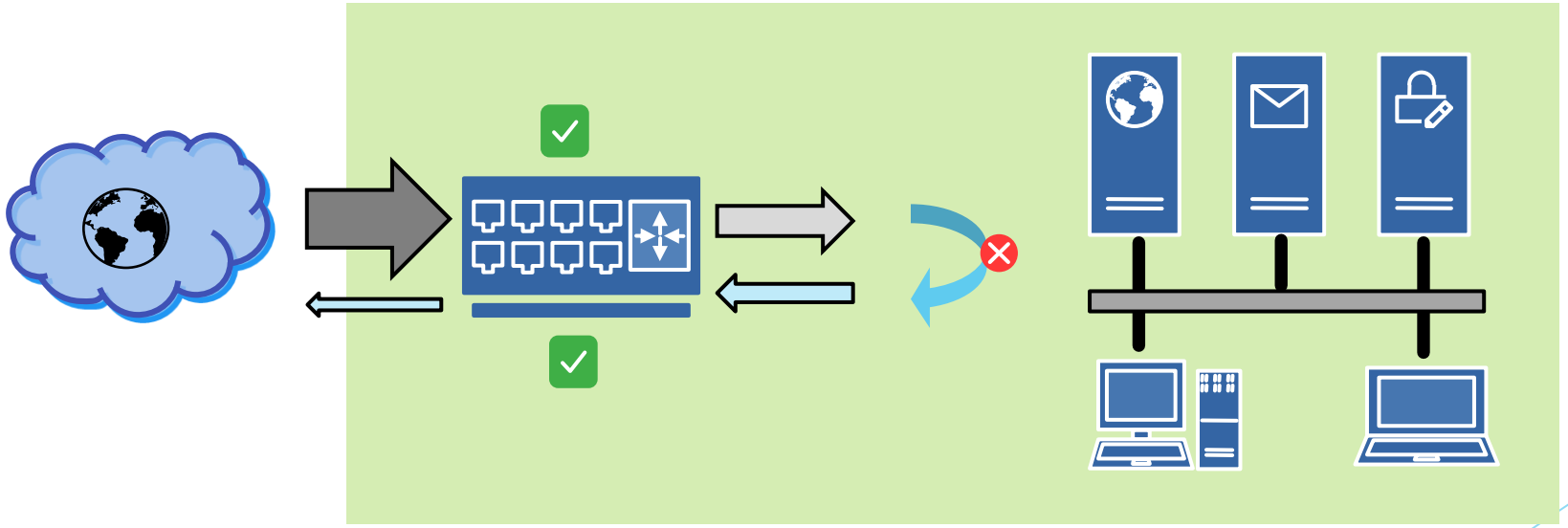
当社のサイバーセキュリティ対策概要

- 入口対策（不正侵入防止）
- 出口対策（不審送信防止）
- ネットワーク負荷を抑えつつ安全性を確保する取り組み

※能動的サイバー防御には影響を与えません。

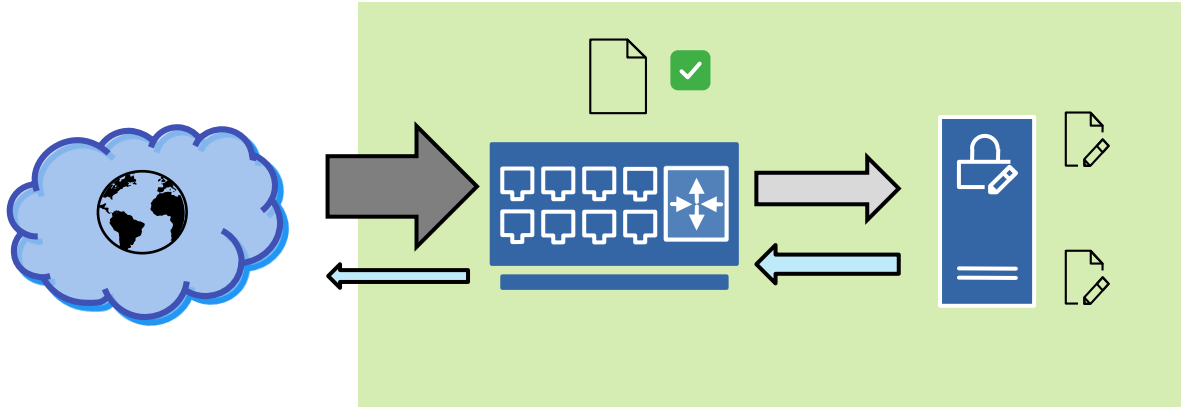
セキュリティ対策の基本思想

- 入口で侵入を防ぎ、出口で漏洩を防ぐ二重構造
  - LAN内に侵入させない（不要不審な接続をさせない）
  - 外部への不審な送信をさせない
  - 入口＝不正侵入対策
  - 出口＝不審送信対策



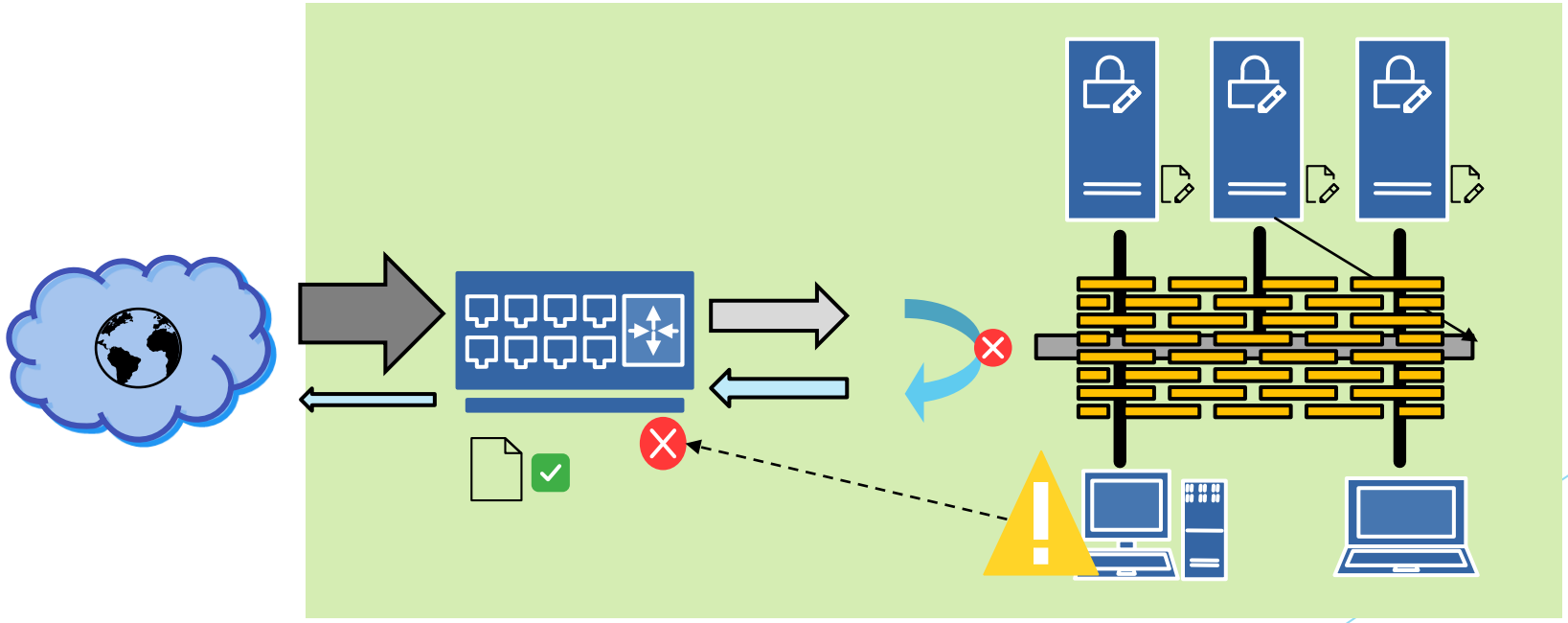
入口対策（不正侵入防止）

- ネットワーク入口での監視と自動記録
  - ルータでホワイトリスト方式で通信許可
  - 設定は手動だが自動化を検討中
  - 電文を1件ずつ監視し、侵入情報を自動でファイル保存
  - 以前は入力側のみ → 現在は送信側も監視
  - WindowsツールをLinuxでも動作可能に改良中



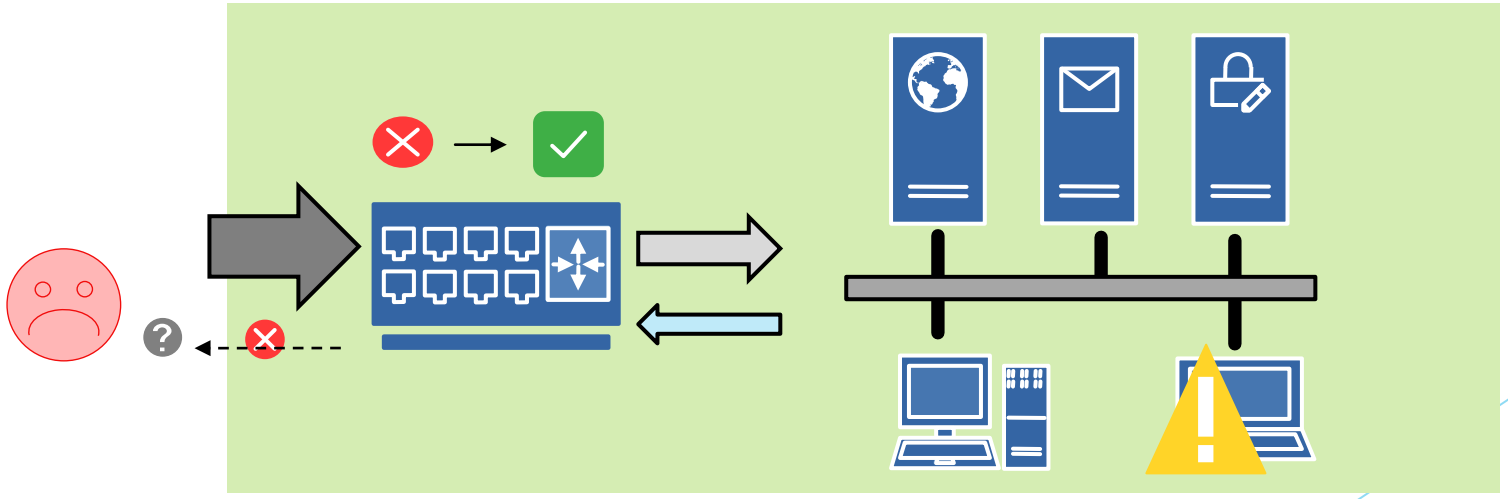
出口対策（不審送信防止）

- 不要な外部接続を遮断し、情報漏洩を防止
  - ルータ・サーバ・PC端末に設定
  - ネットワーク負荷を増やさない設計
  - サーバで入出力監視、必要に応じて分散監視
  - ウイルス感染時でも外部送信ができず被害を最小化



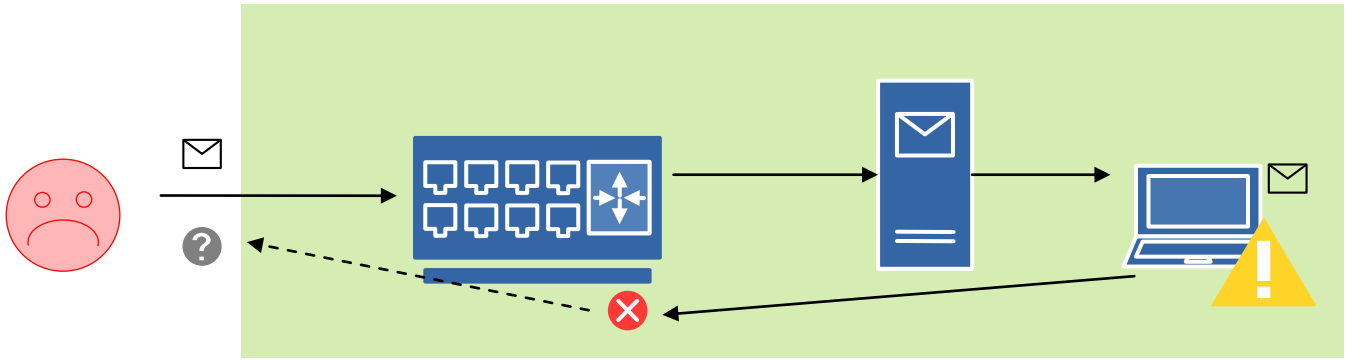
過去の事例（2011年 計画停電）

- リモート開発開始時の侵入事例と対策強化
  - セキュリティ不足により不明アカウント作成
  - PC乗っ取りと判断
  - 一旦全入力禁止 → 必要通信のみ許可する方式で対策
  - ネットワーク負荷が減り快適性向上
  - 世界中のハッカーから攻撃 → 対策により防御成功



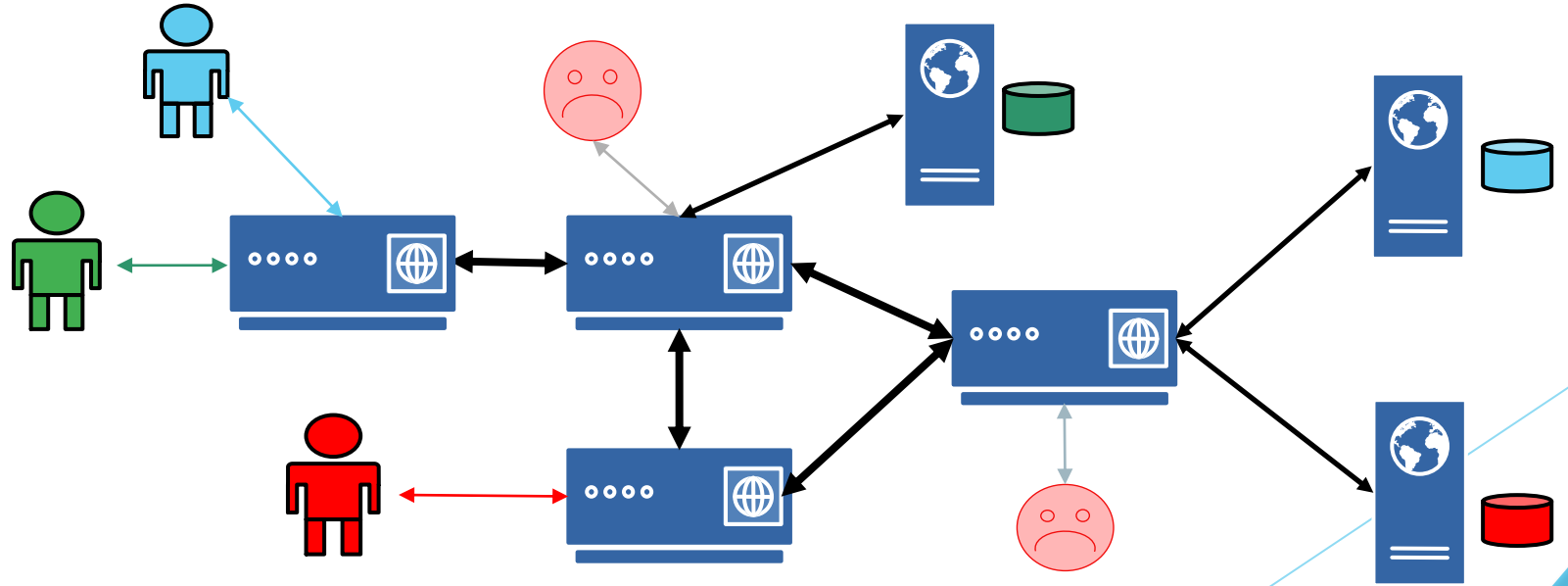
ウイルス・ランサムウェアへの対策

- 外部接続遮断により遠隔操作型ウイルスを無効化
  - 外部接続を遮断しているため遠隔操作型ウイルスは機能しない
  - ランサムウェアは添付ファイル開封で感染（開かないことが重要）
  - 復元資金要求メールが来る場合は別ウイルスの可能性
  - 当社対策ではランサムウェア実行が外部に伝わらない



ネットワーク構造と情報漏洩の考察

- 回線上での情報漏洩は構造上ほぼ不可能
  - ISP回線には接続者の情報しか流れない
  - 他社情報を読み取ることは構造上不可能
  - 回線を物理的に摘んでもどの回線か特定できない
  - 情報漏洩は接続元か接続先ネットワークで発生
  - メール改竄はメールサーバ側で起こり得る
  - VPNや暗号化はネットワーク構造上あまり意味がないという立場



まとめ

- 当社セキュリティ対策の強み
  - 入口・出口の二重対策で侵入と漏洩を防止
  - 不要な外部接続を遮断し攻撃負荷を軽減
  - ウイルス感染時でも外部送信ができず被害を最小化
  - 過去の攻撃経験を踏まえた強固な対策
  - ネットワークを快適に保ちながら安全性を確保