サイバー攻撃の実態

株式会社ソリトンシステムズ
サイバーセキュリティラボ
小伊藤　成毅

※第1回より内容を追記・改訂しています。

セキュリティ製品は

IT管理者が製品をちゃんと
選定し、使いこなさないと
いけない世の中に
なりつつあるようです。

重要10項目

分類	10項目
■基本方針	（1）リスク認識とグランドデザイン
	（2）リスク管理体制
■管理の枠組み	（3）目標と計画策定
	（4）PDCAの構築
	（5）系列とパートナー
■防ぐ対策	（6）経営資源の確保
	（7）外部委託対策
	（8）社外コミュニケーション
■有事の対処	（9）対応体制
	（10）開示と広報

多層防御措置の実施

PDCAサイクルの実施と改善

アジェンダ

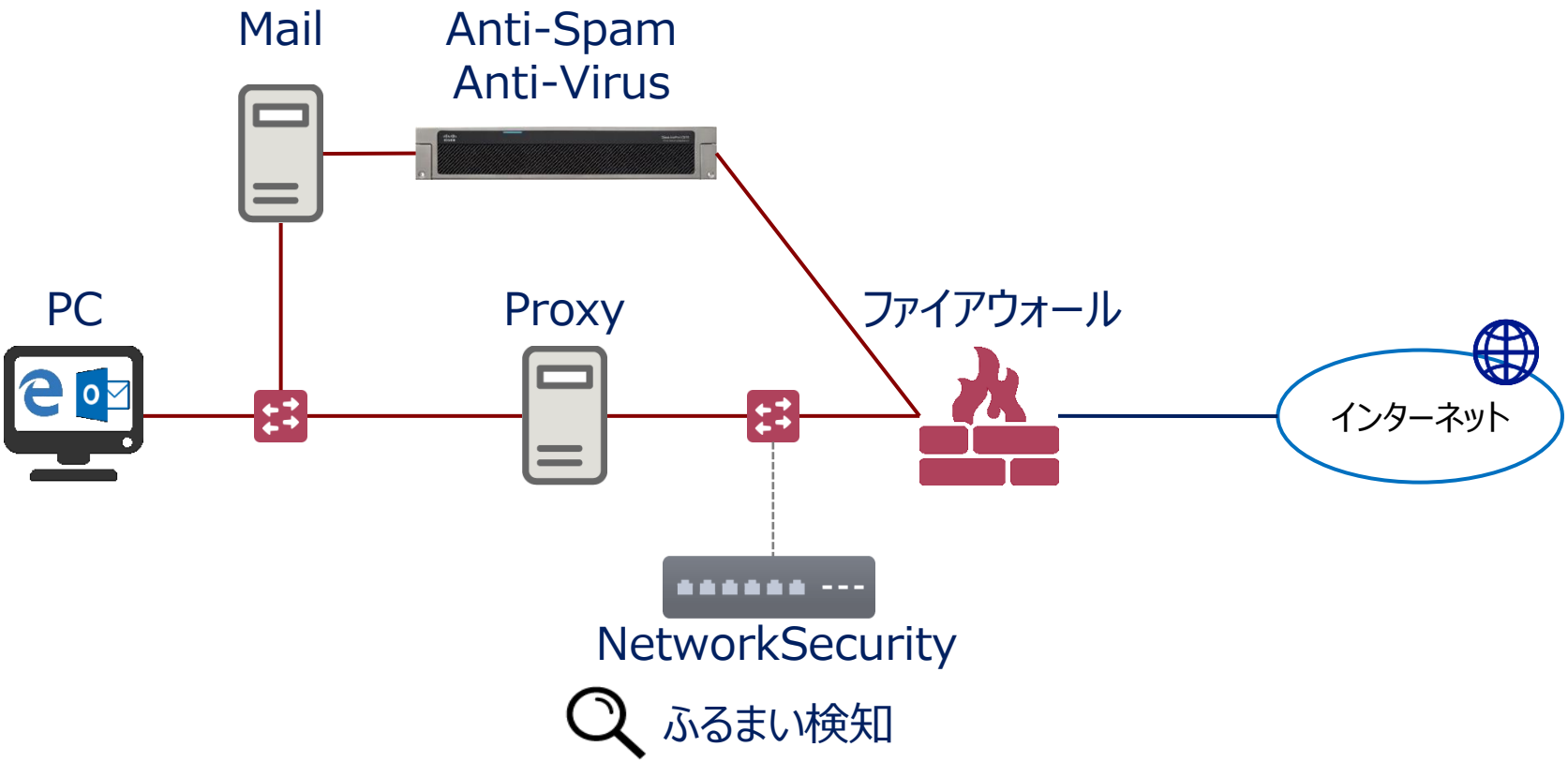
1. リスクを把握し、多層防御など
   リスクに応じた対策をたてていますか？

2. PDCAサイクルを実践するフレームワークを
   構築してますか？

1.多層防御措置の実施

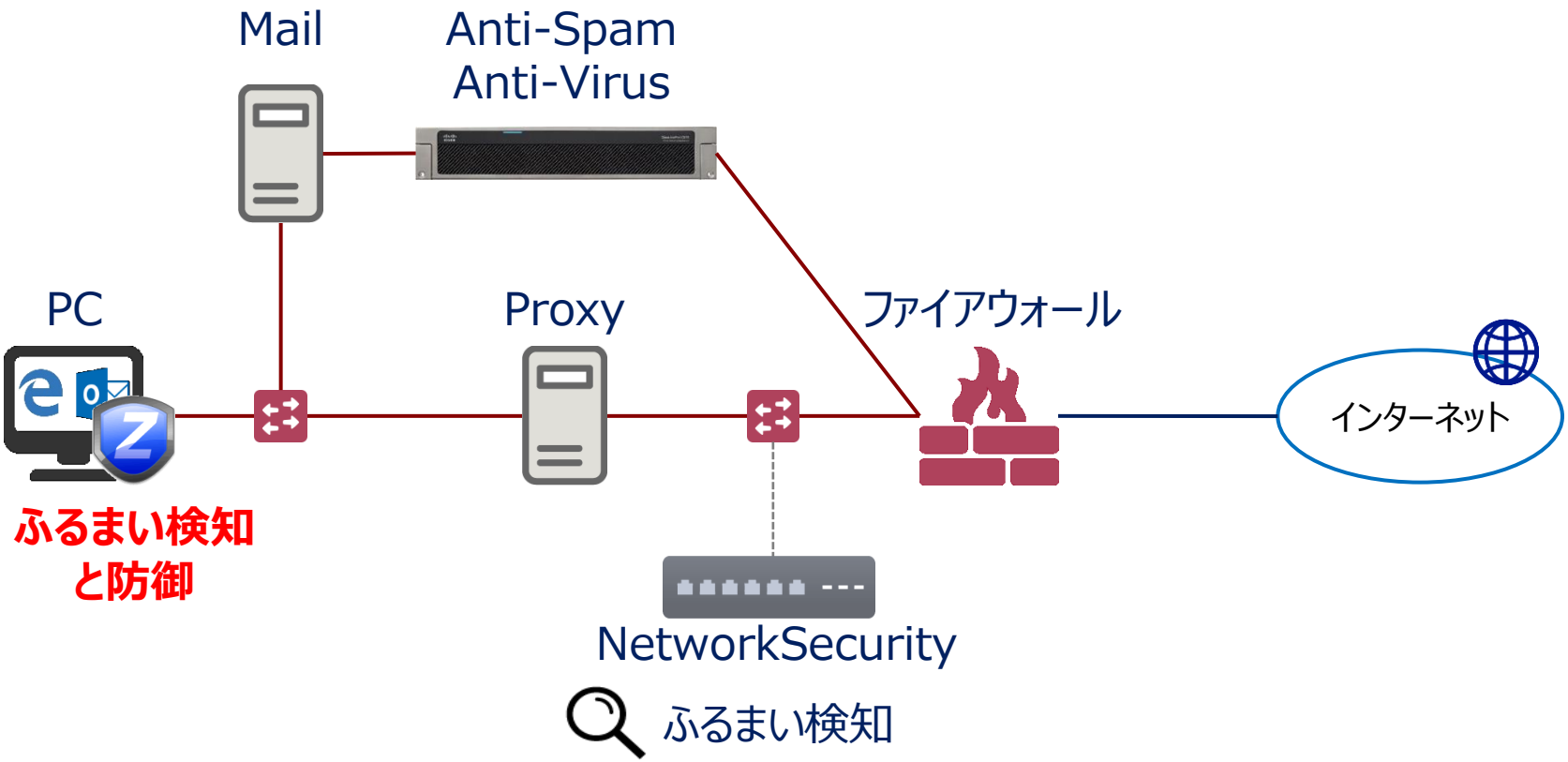
デモ１

ふるまい検知機器の導入構成



デモ2

多層防御の導入構成



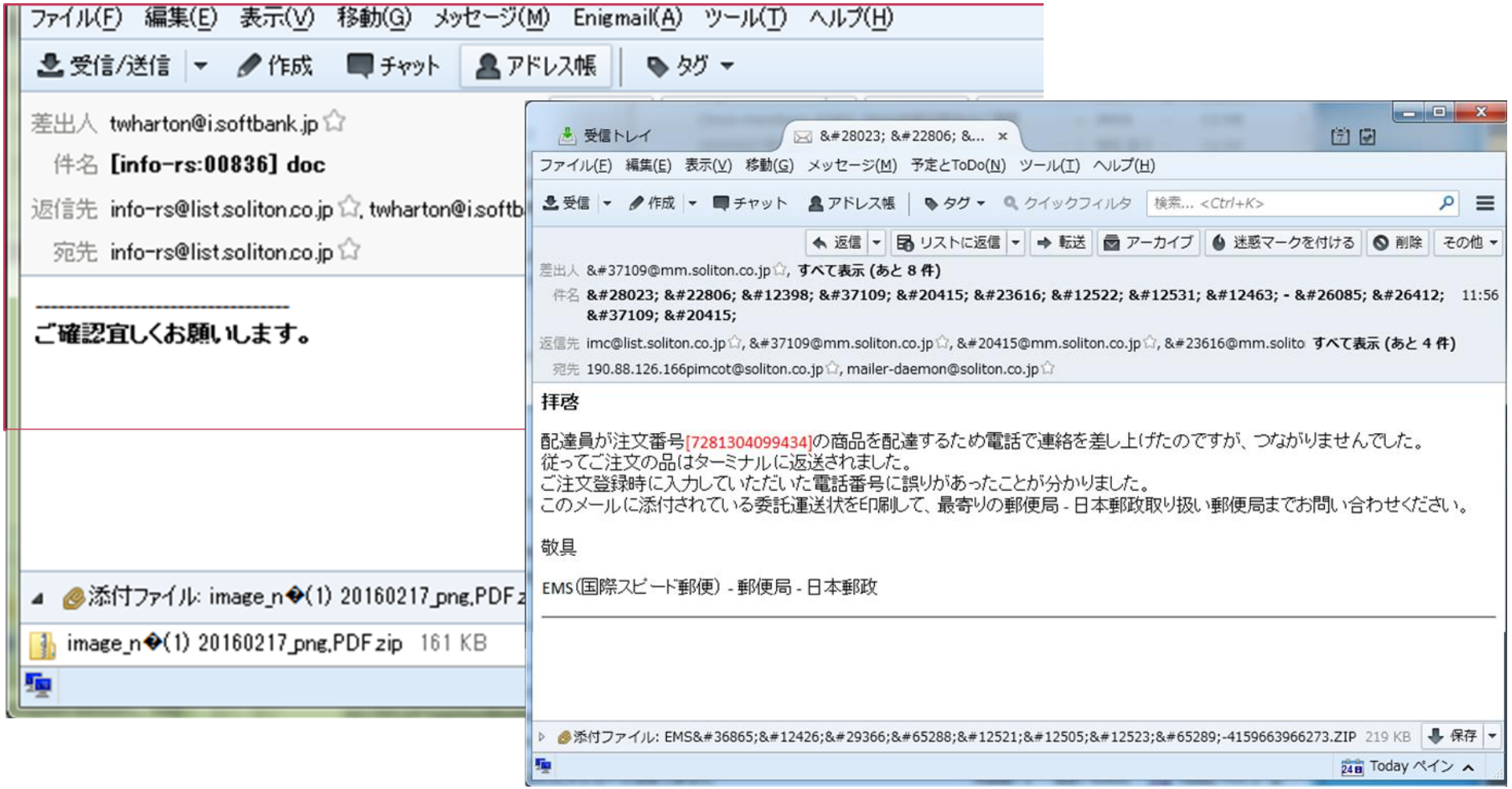
結果

■未知の脅威の検知には多層防御が効果的

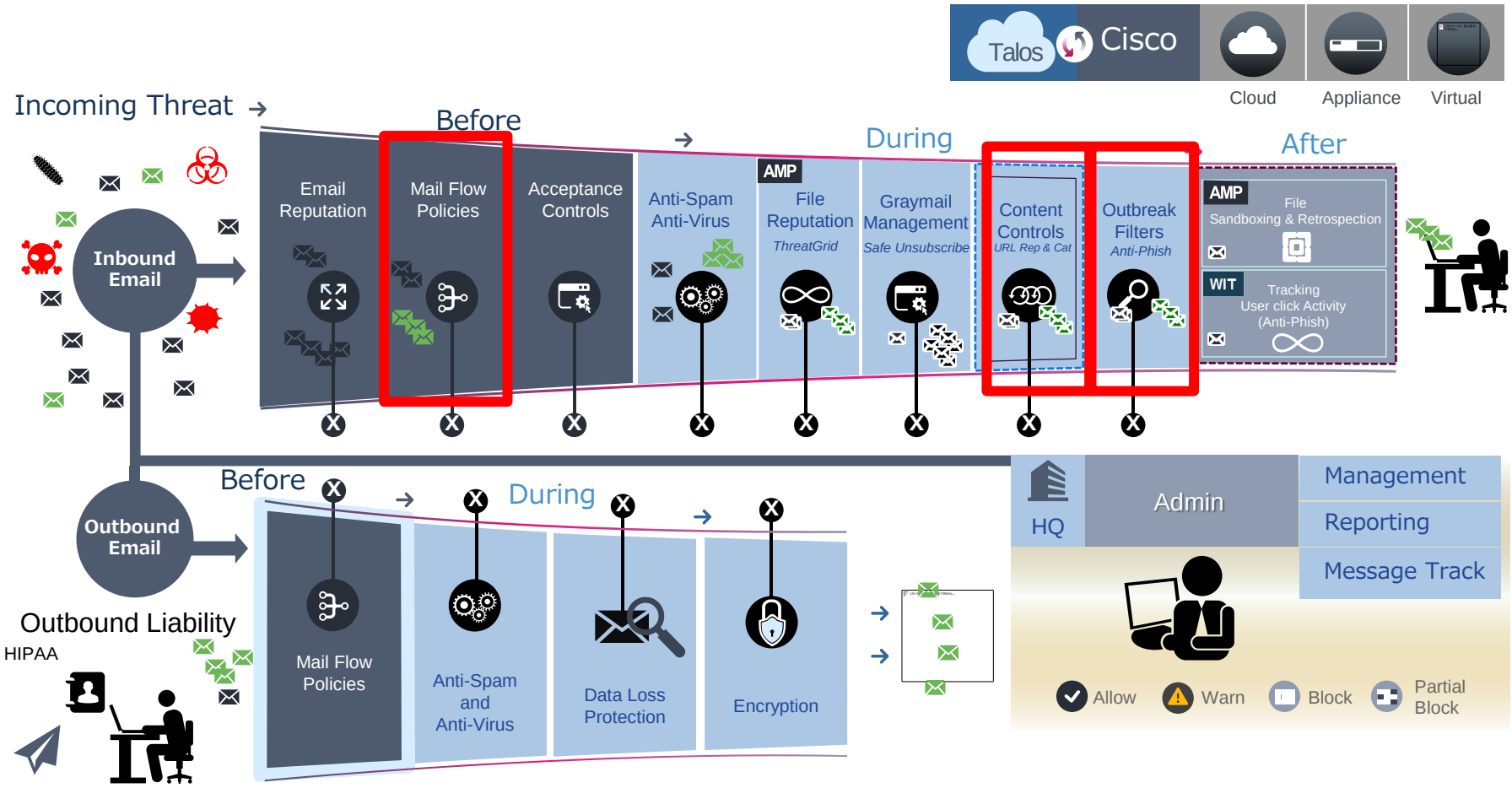
■検知と防御製品の特性を把握することが重要

2.PDCAサイクルの実施と改善

怪しいメールの受信



設定変更実施



フィルタの適用結果(2016/6/15現在)

■キャンペーンの被害者ゼロ

■バンキングマルウェアの被害ゼロ

■ランサムウェアの被害ゼロ

まとめ

■リスクに応じた多層防御を実施

■環境に即した運用と設定変更の適用

■メーカ、導入担当、運用担当、外部の知見を取り入れ積極運用