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

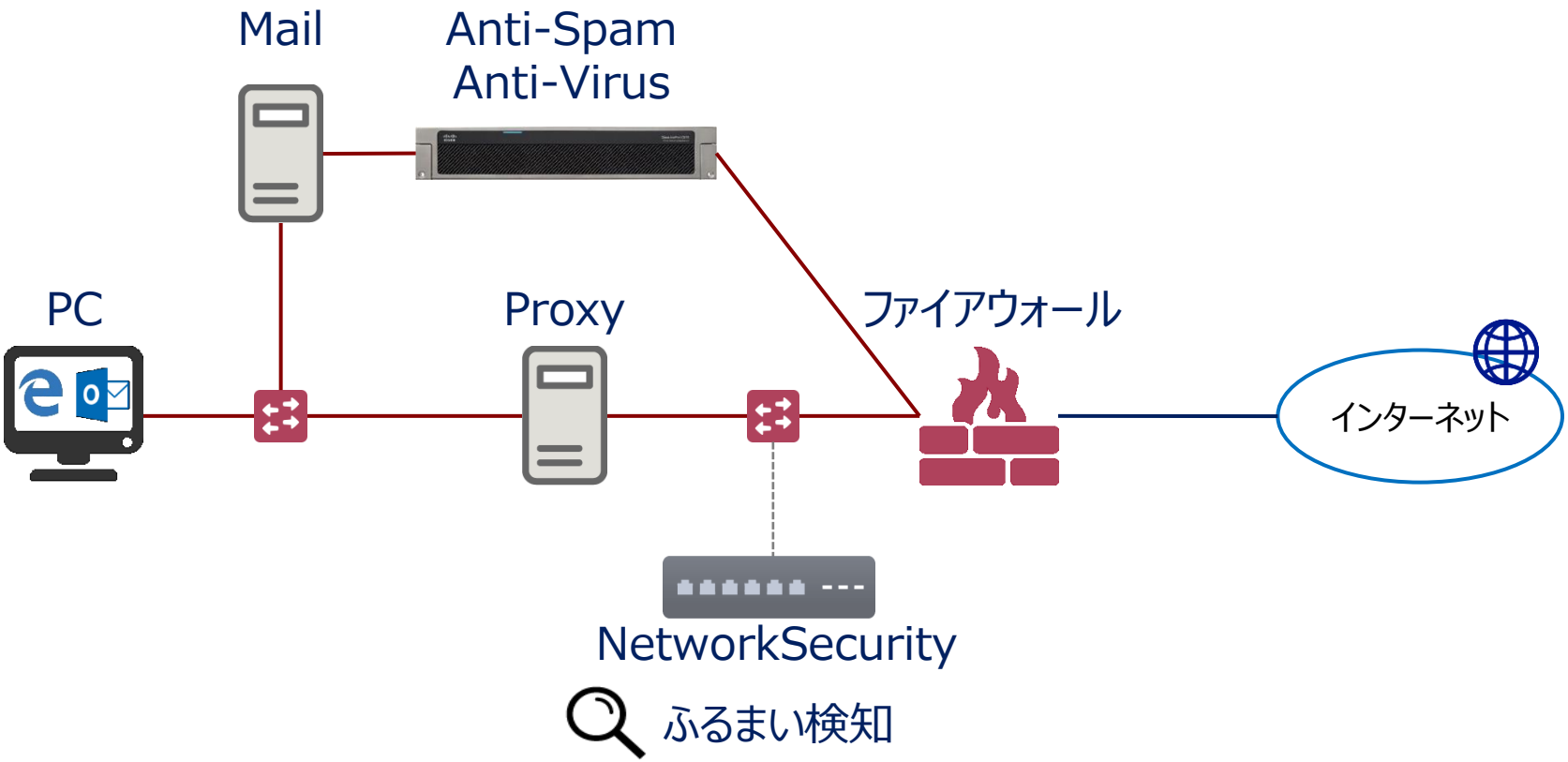
1. リスクを把握し、多層防御など
   リスクに応じた対策をたてていますか？

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？

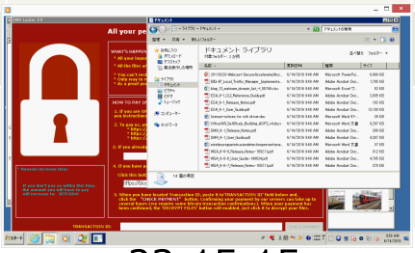
1.多層防御措置の実施

デモ１

ふるまい検知機器の導入構成



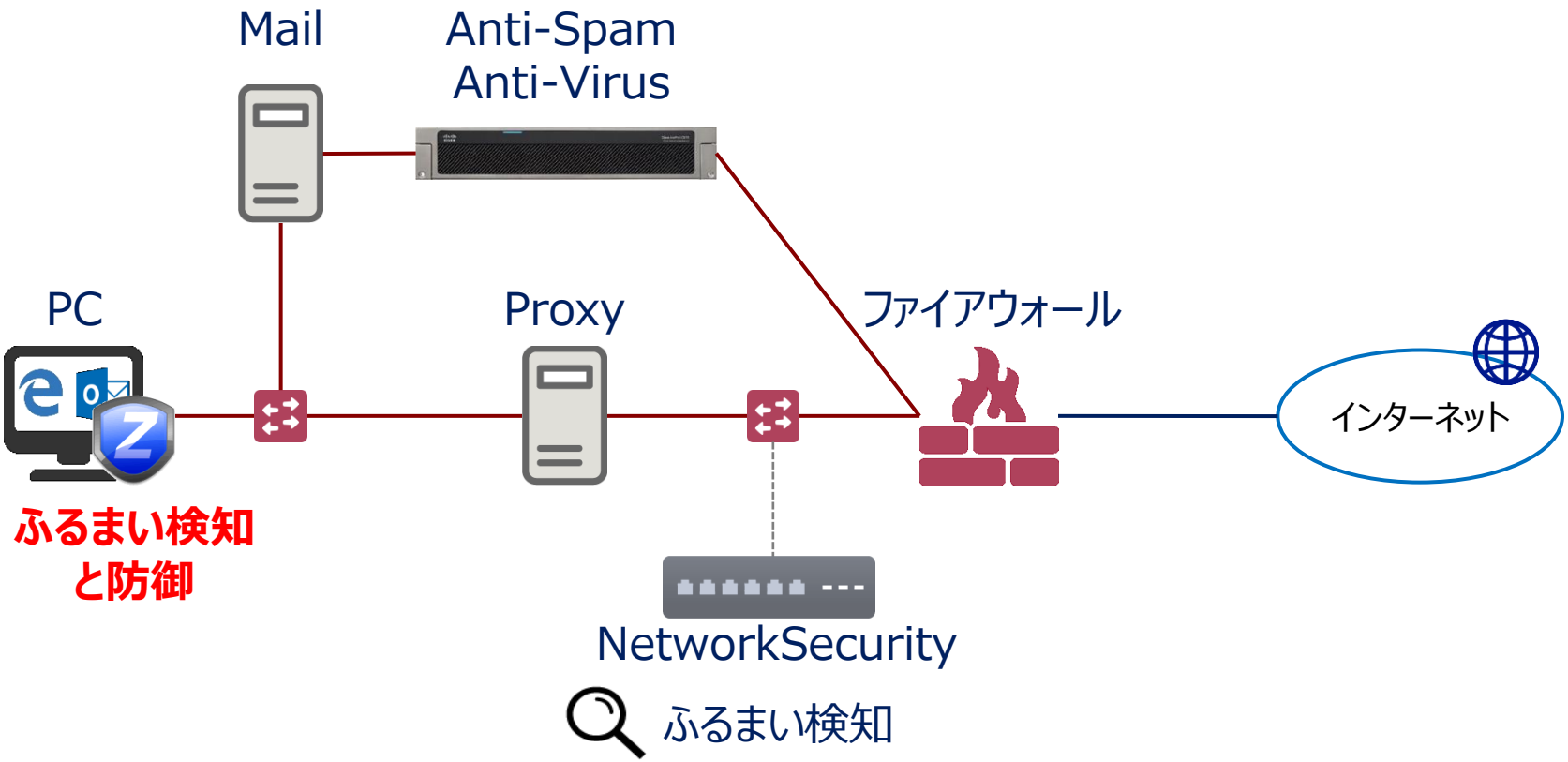
未知の脅威への対応

時刻	NetworkSecurity	PC	管理者
22:54:49	解析開始	ファイルダウンロード 実行 外部通信発生	
22:55:50	外部通信検知 アラート送信		アラート受信
22:58:56		ファイル暗号化開始	
23:00:16	解析終了 マルウェア検知 アラート通知	ファイル暗号化中 およそ1.5秒/ファイル	アラート受信
			調査開始
			端末対応

23:15:15

デモ2

多層防御の導入構成



未知の脅威への多層防御対応

時刻	NetworkSecurity	PC(ふるまい検知)	管理者
22:54:49	解析開始	ファイルダウンロード 実行 **ふるまい検知防御** 	
22:54:50		アラート通知	アラート受信
23:00:16	解析終了 アラート通知		アラート受信
			調査開始
			改善案の検討
			報告

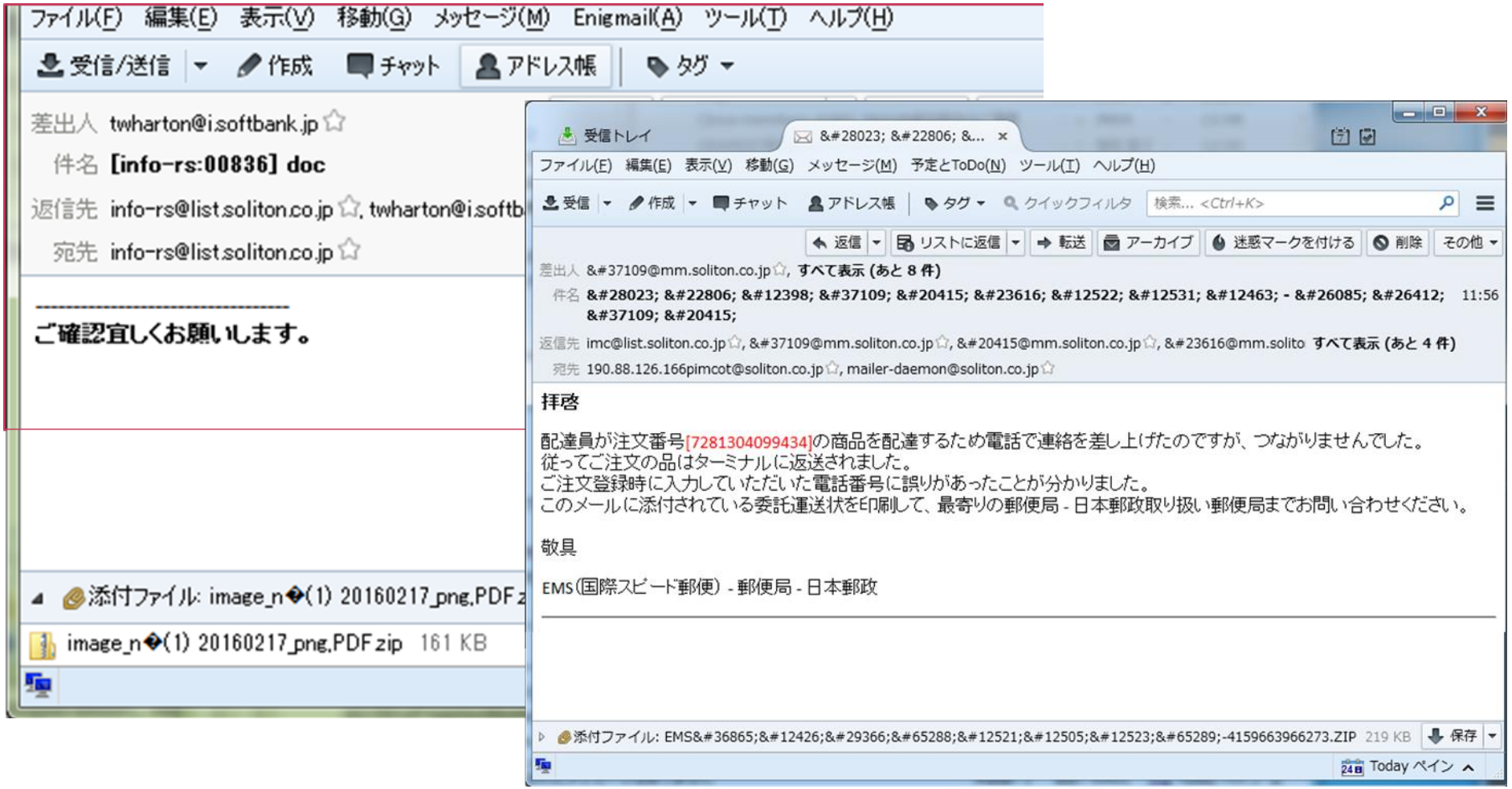
結果

■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



マルウェア添付メールの大量受信

- 2016/1～ EMS/DHLなどを装ったマルウェア添付メールを大量受信
  - ピーク時 200-300通/600ユーザ
  - 送信元は携帯キャリアやフリーメールなど
  - zipファイル添付
  - 毎日ではないが月に数回発生
- 受信時はウイルスではないが後日ウイルスとして検知
- ログ詳細分析の実施

ログ分析で分かったこと

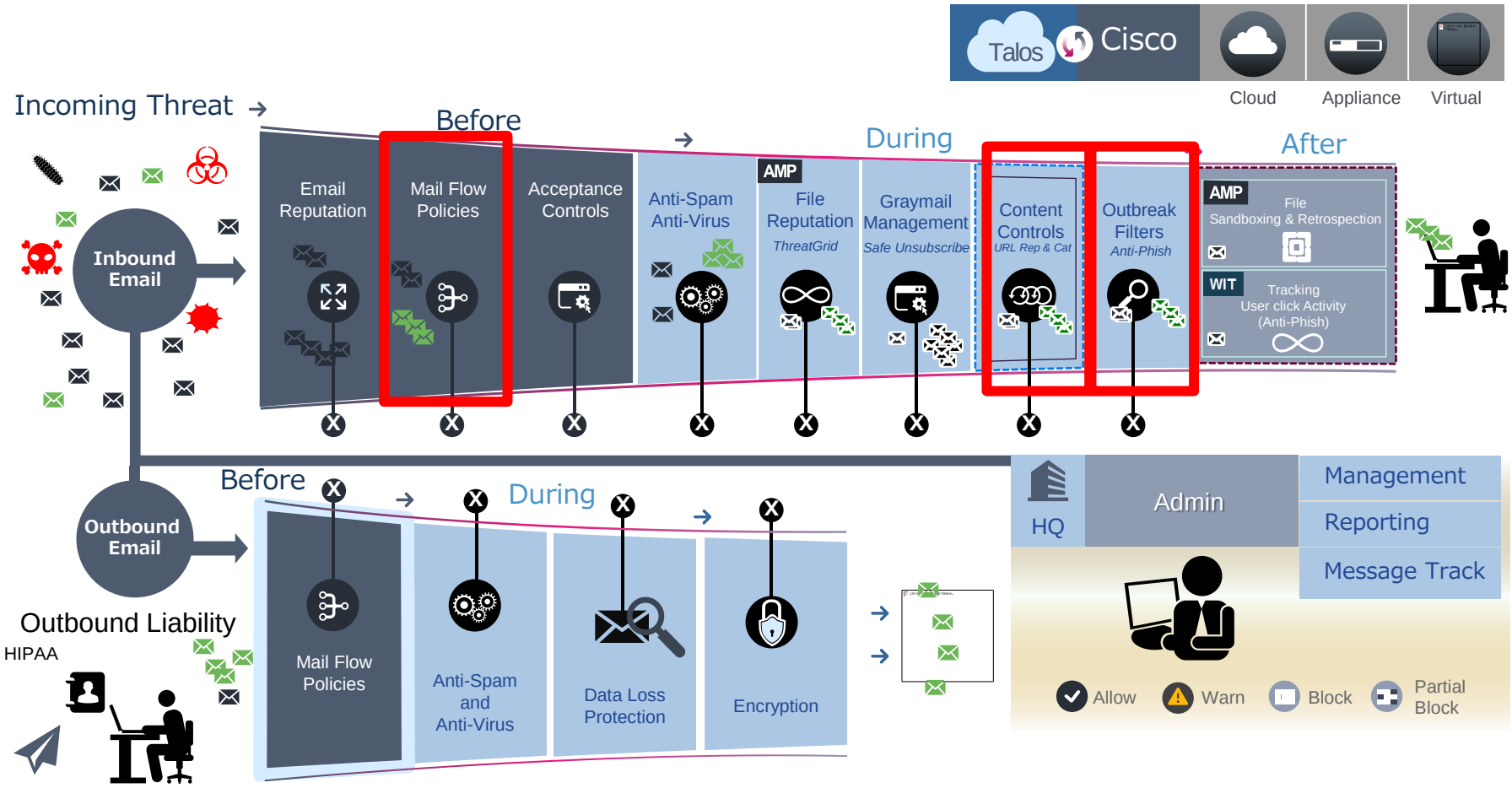
- 送信元の評価スコアが比較的悪い
  ※-10.0≦スコア≦10.0, -5.0以下は受信拒否
  - -5.0<スコア≦-4.0 のメールへの対処
- zipファイル添付のばら撒き型
  - ばら撒き型メールへの対処
- 数時間～1日後にウイルスシグネチャ提供
  - バンキングマルウェア

設定の検討

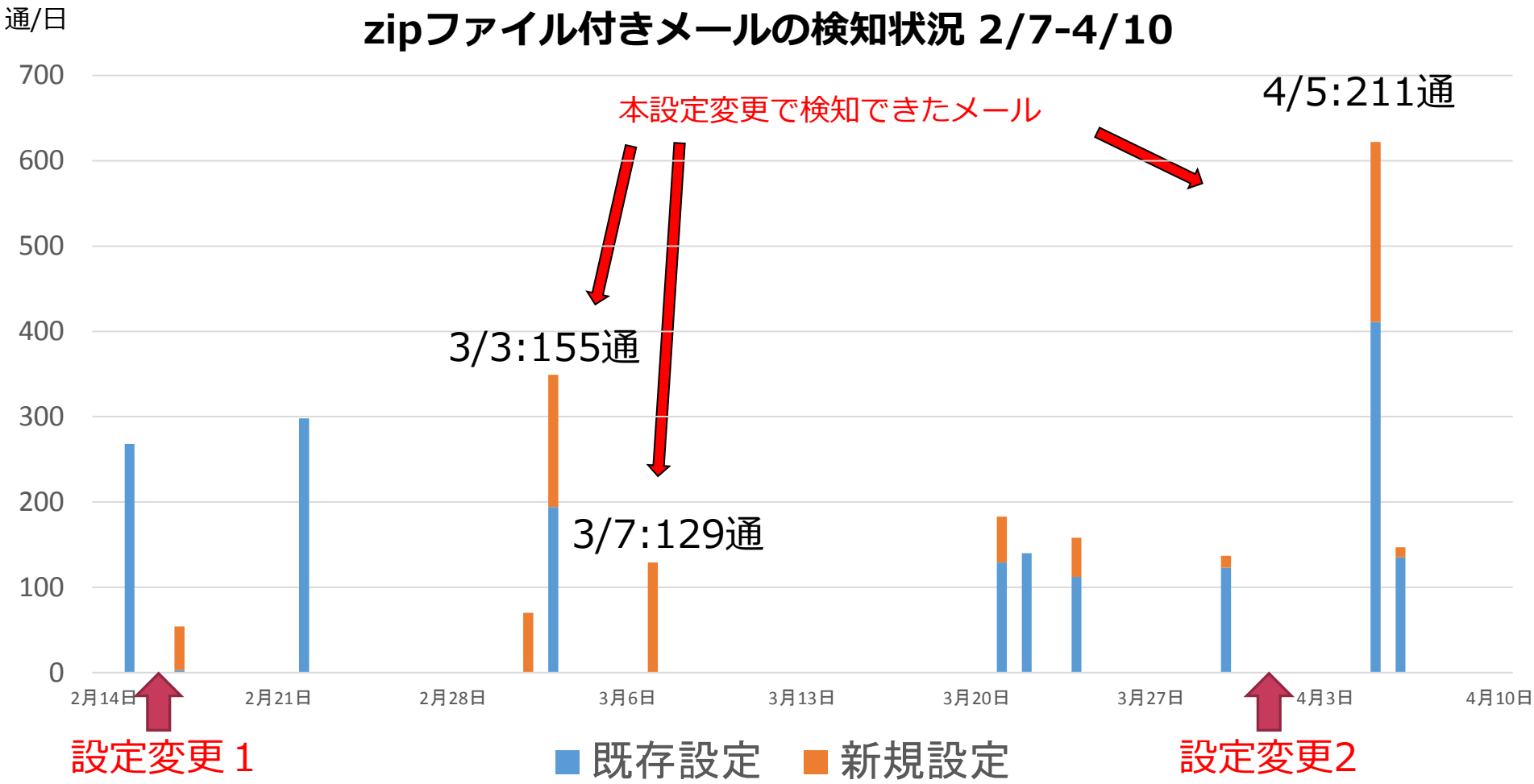
- 設定１：フィルタのチューニング
  - -5.0<評価スコア≦-4.0のメール隔離
  - 一部のメールはFalse-Positiveのため問合せ対応

- 設定２：新機能の追加
  - 大量発生する添付ファイル付き不審メールを自動的に一時隔離
  - 一定時間経過後にリリースし再度ウイルスチェック実施

設定変更実施



適用結果



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