

# 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

---

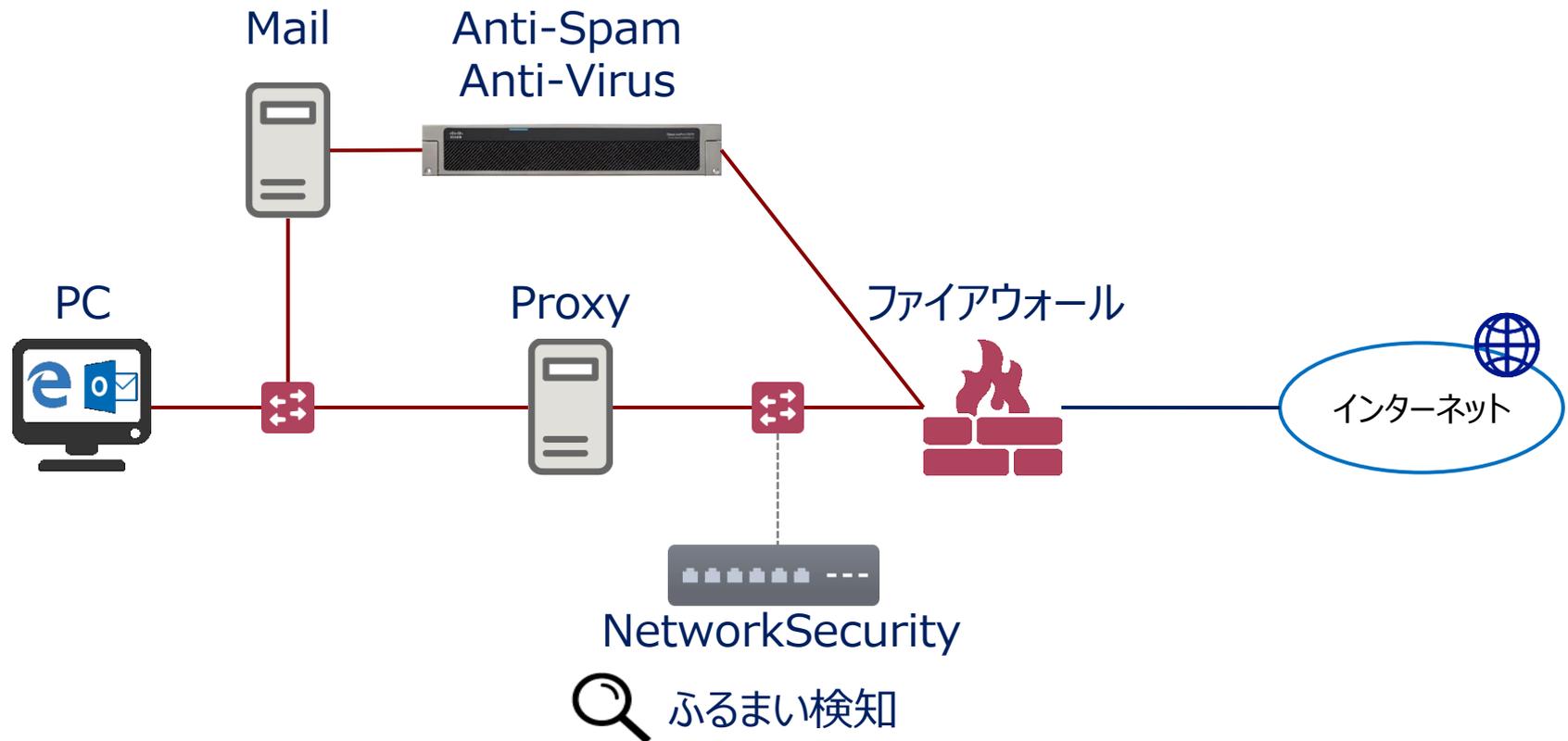
1. リスクを把握し、多層防御など  
リスクに応じた対策をたてていますか？
2. PDCAサイクルを実践するフレームワークを  
構築してありますか？

# 1. 多層防衛措置の実施

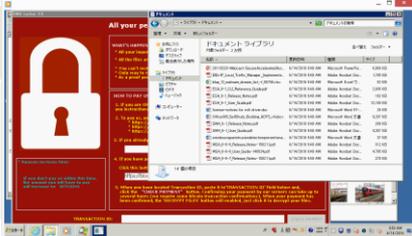
---

# デモ 1

# ふるまい検知機器の導入構成



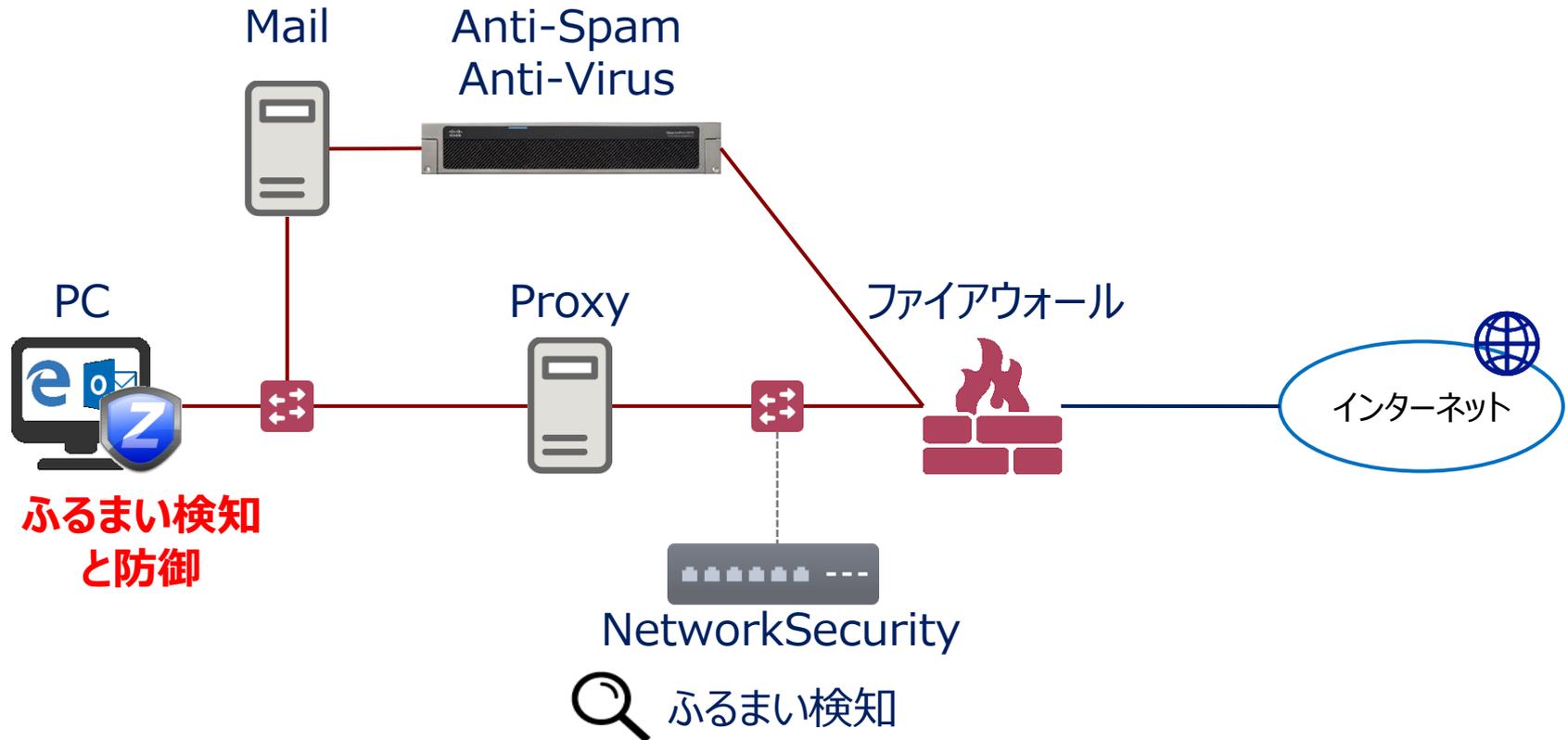
# 未知の脅威への対応

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

The image shows a screenshot of an email client interface. The main window displays an email from 'twharton@i.softbank.jp' with the subject '[info-rs:00836] doc'. The email body contains the text 'ご確認宜しくお願いします。' (Please confirm as appropriate). Below the text, there are two attachments: 'image\_n(1) 20160217\_png.PDF' and 'image\_n(1) 20160217\_png.PDF zip 161 KB'. A smaller window titled '受信トレイ' (Inbox) is overlaid on the main window, showing a list of emails. The selected email has a subject line containing a long string of numbers: '&#28023; &#22806; &#12398; &#37109; &#20415; &#23616; &#12522; &#12531; &#12463; - &#26085; &#26412; &#37109; &#20415;'. The email body of this window contains a message in Japanese: '配達員が注文番号[7281304099434]の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。従ってご注文の品はターミナルに返送されました。ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。このメールに添付されている委託運送状を印刷して、最寄りの郵便局 - 日本郵政取り扱い郵便局までお問い合わせください。' (The delivery person called to deliver the product with order number [7281304099434], but we couldn't get through. Therefore, your order items have been returned to the terminal. We found an error in the phone number you entered during registration. Please print the attached shipping order form and contact the nearest post office - Japan Post handling post office.) Below the message, it says '敬具' (Respectfully) and 'EMS(国際スピード郵便) - 郵便局 - 日本郵政' (EMS (International Speed Mail) - Post Office - Japan Post). At the bottom of the smaller window, there is another attachment: 'EMS&#36865;&#12426;&#29366;&#65288;&#12521;&#12505;&#12523;&#65289;-4159663966273.ZIP 219 KB'.

# 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
  - ※ $-10.0 \leq \text{スコア} \leq 10.0$ ,  $-5.0$ 以下は受信拒否
    - $-5.0 < \text{スコア} \leq -4.0$  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

---

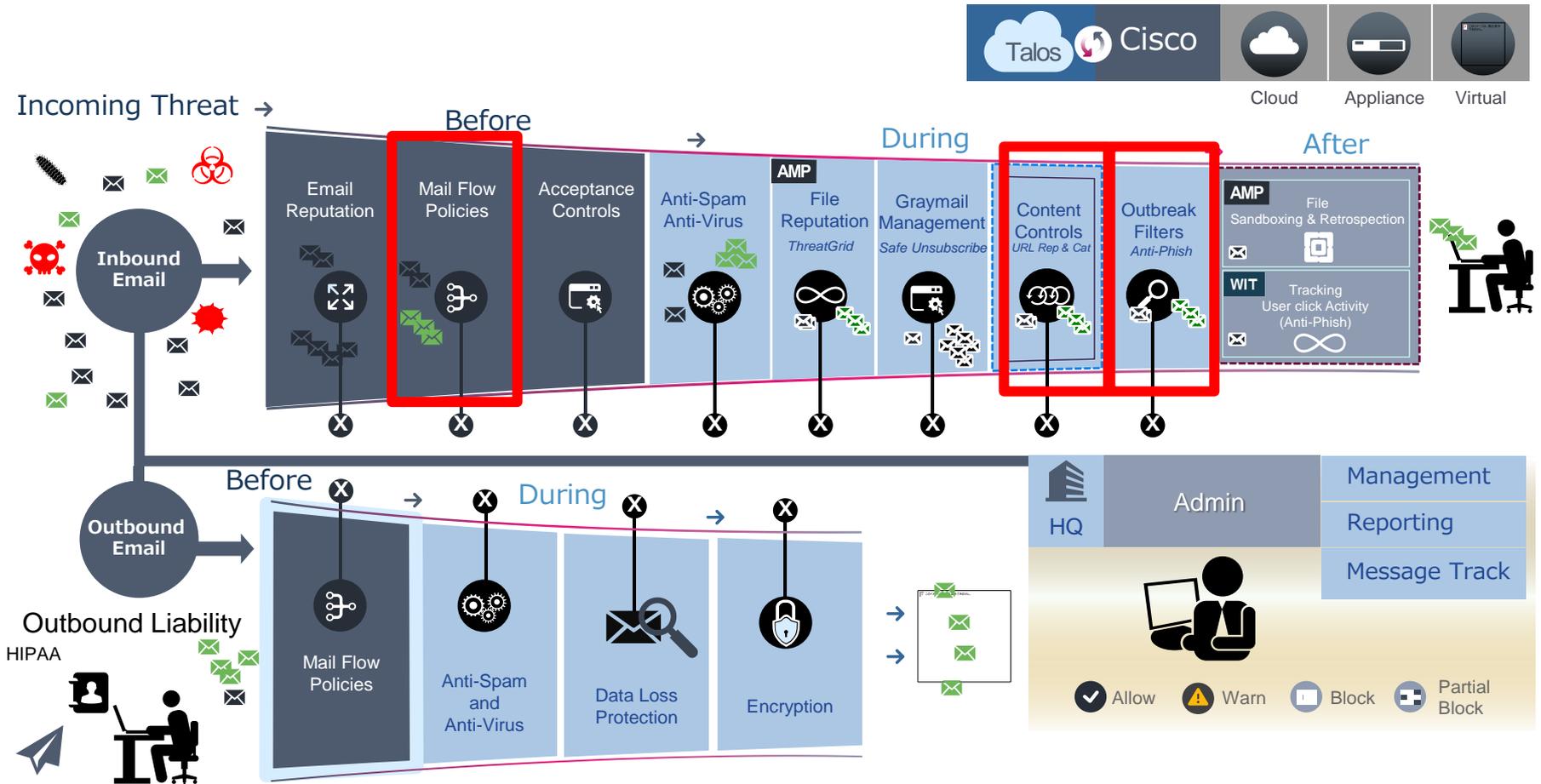
## ■設定 1 : フィルタのチューニング

- $-5.0 < \text{評価スコア} \leq -4.0$  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

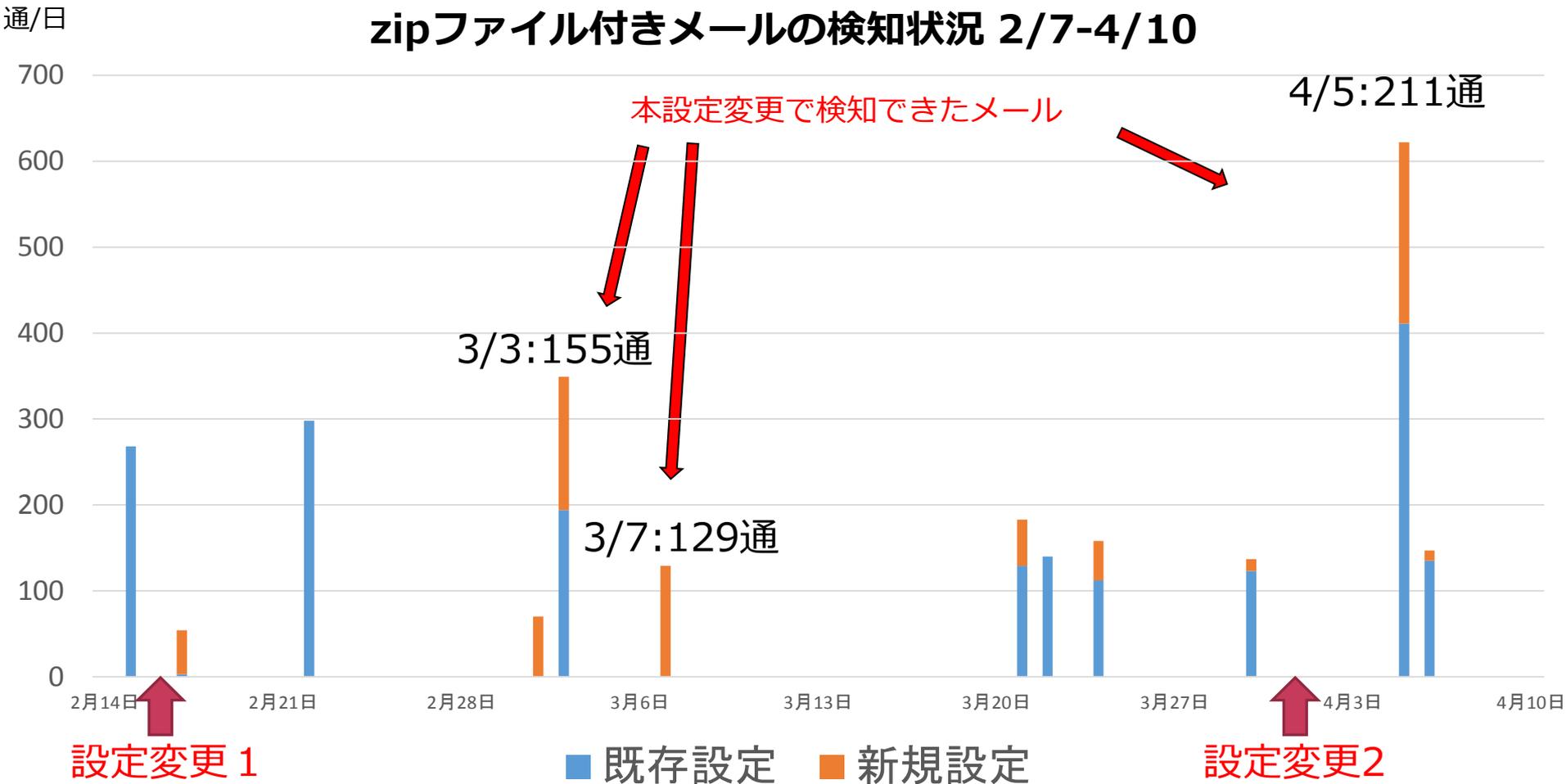
- 大量発生する添付ファイル付き不審メールを自動的に一時隔離
- 一定時間経過後にリリースし再度ウイルスチェック実施

# 設定変更実施



# 適用結果

## zipファイル付きメールの検知状況 2/7-4/10



# 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
- メーカー、導入担当、運用担当、外部の知見を取り入れ積極運用

**Soliton<sup>®</sup>**