

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

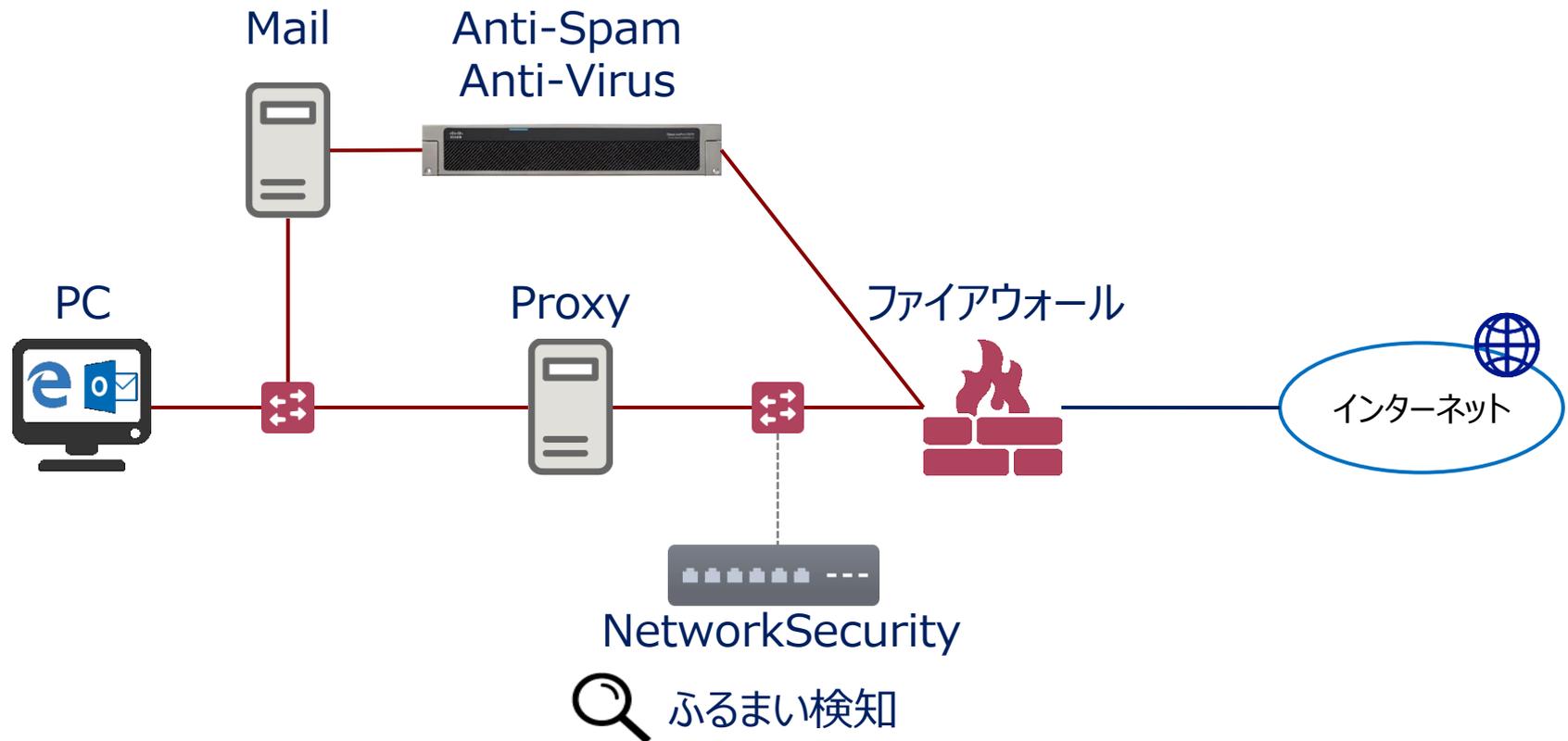
アジェンダ

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

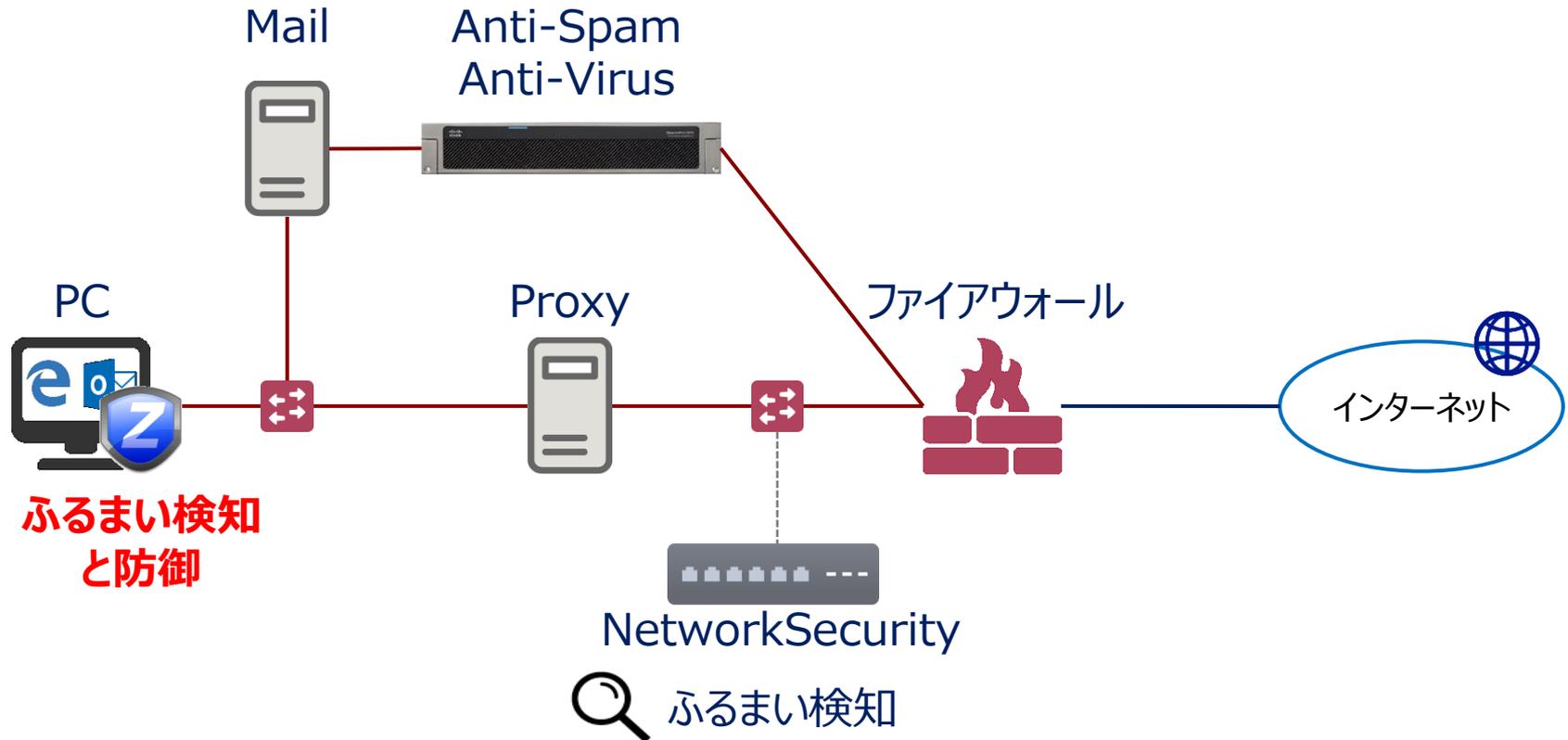
デモ 1

ふるまい検知機器の導入構成



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徴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 screenshot shows an email client window with a menu bar (File, Edit, View, Move, Message, Enigmail, Tools, Help) and a toolbar (Receive/Send, Create, Chat, Address Book, Tags). The main content area displays the following information:

差出人 twharton@i.softbank.jp ☆
件名 [info-rs:00836] doc
返信先 info-rs@list.soliton.co.jp ☆, twharton@i.softb
宛先 info-rs@list.soliton.co.jp ☆

ご確認宜しくお祈いします。

添付ファイル: image_n (1) 20160217_png.PDF z
image_n (1) 20160217_png.PDF zip 161 KB

The right-hand pane shows the '受信トレイ' (Inbox) window with a search bar and a list of emails. The selected email has the following details:

受信トレイ 海 外 &#... ×
ファイル(E) 編集(E) 表示(V) 移動(G) メッセージ(M) 予定とToDo(N) ツール(I) ヘルプ(H)
受信 | 作成 | チャット | アドレス帳 | タグ | クイックフィルタ 検索... <Ctrl+K>
返信 | リストに返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除 | その他

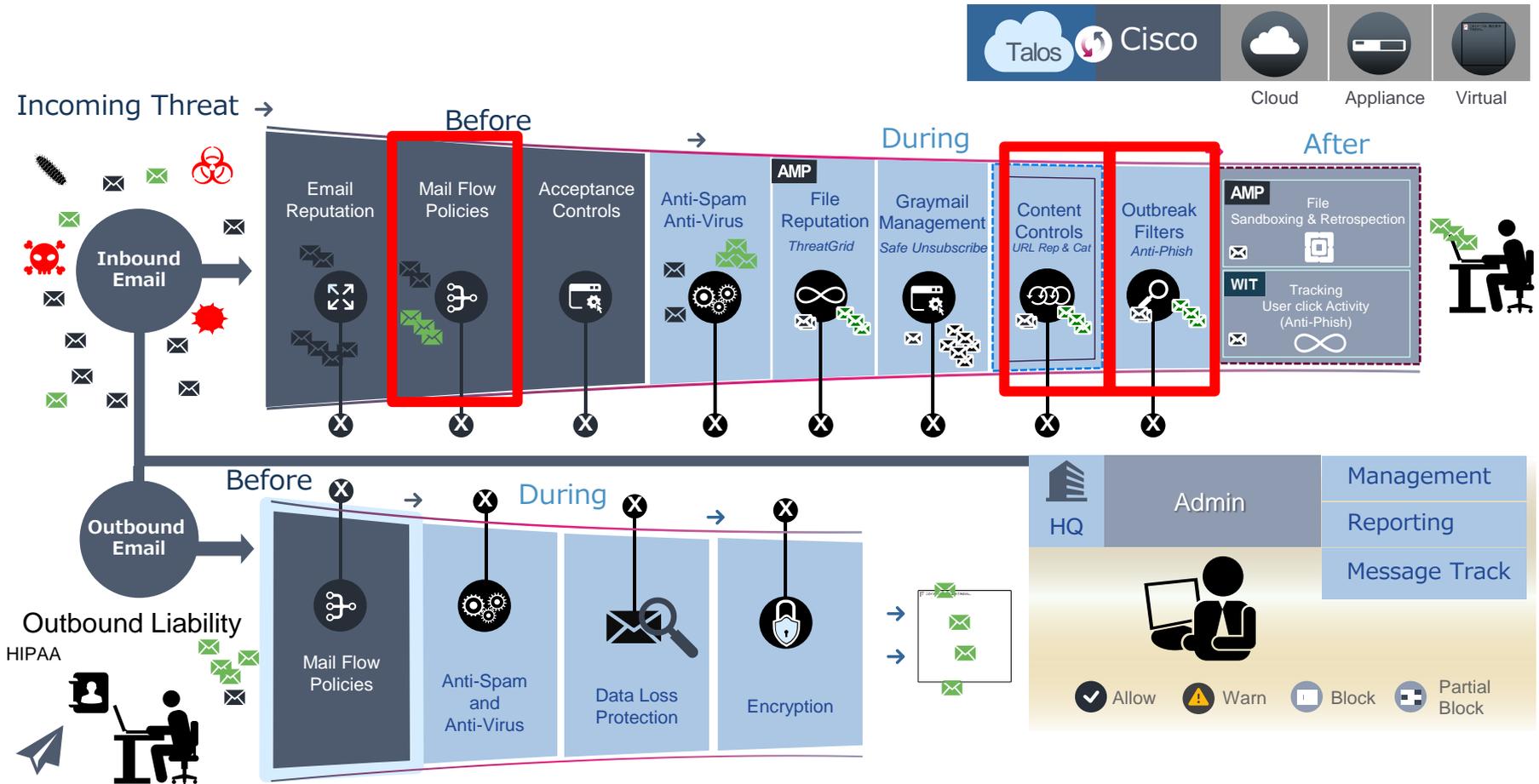
差出人 郵@mm.soliton.co.jp ☆, すべて表示 (あと 8 件)
件名 海 外 の 郵 便 局 リ ン ク - 日 本 11:56
郵 便
返信先 imc@list.soliton.co.jp ☆, 郵@mm.soliton.co.jp ☆, 便@mm.soliton.co.jp ☆, 局@mm.solito すべて表示 (あと 4 件)
宛先 190.88.126.166pimcot@soliton.co.jp ☆, mailer-daemon@soliton.co.jp ☆

拝啓
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。

敬具
EMS(国際スピード郵便) - 郵便局 - 日本郵政

添付ファイル: EMS送り状（ラベル）-4159663966273.ZIP 219 KB 保存

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
- メーカー、導入担当、運用担当、外部の知見を取り入れ積極運用

Soliton[®]