NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ

今、求められるメールセキュリティ対策の在り方

～ メールセキュリティの脅威・動向と対策解 ～

NRIセキュアテクノロジーズ株式会社
ソリューション事業本部

〒100-0004
東京都千代田区大手町1-7-2　東京サンケイビル

Ver1.02 2016/11/01

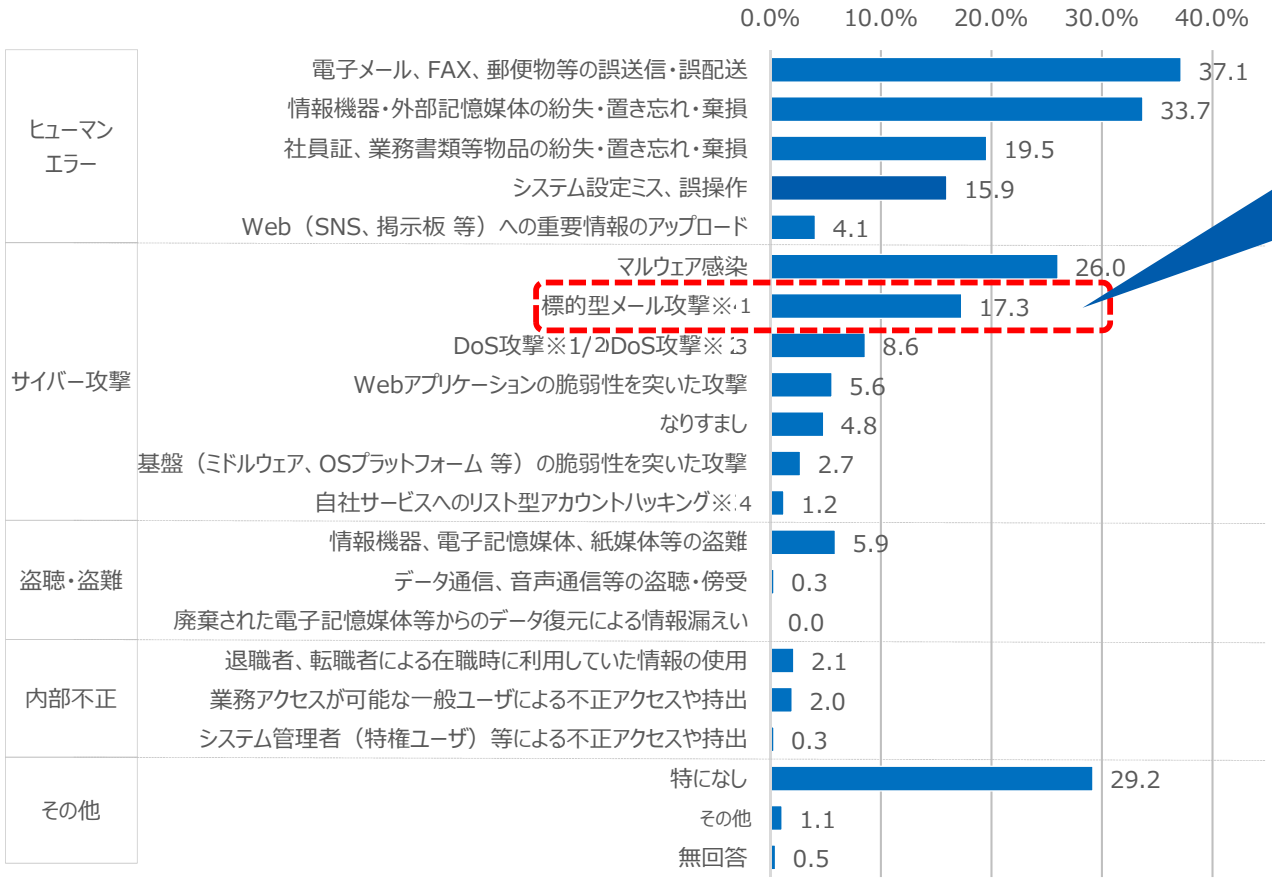
AGENDA

1. メールセキュリティの脅威・動向

2. 標的型メールへの対策解

標的型メール攻撃事件・事故の台頭

Q.過去1年間で発生した情報セキュリティに関する事件・事故はありますか。
以下の中からあてはまるものを全てお選びください。(n=665)



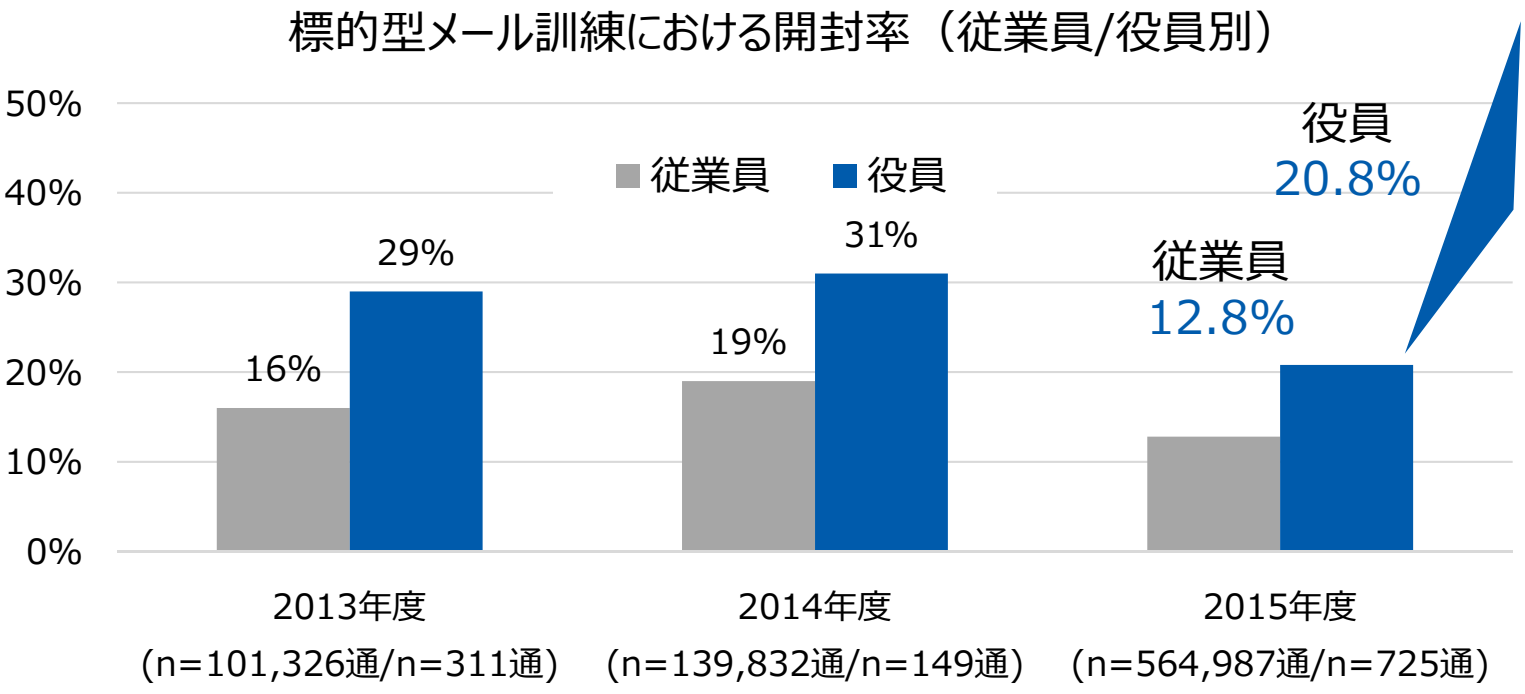
2014年度は5.8% 約3倍

※1 パターンマッチング型のマルウェア対策ソフトでは検知できない新種のマルウェアを添付したメールの送信。
※2 Denial of Service attackの略。ネットワーク経由で大量のパケットや不正な入力をし、サービスを停止に追い込む攻撃。
※3 Distributed Denial of Service attackの略。ネットワーク上に分散したコンピュータを踏み台として行うDoS攻撃。
※4 複数のオンラインサービスで同一IDとパスワードを設定していることを悪用し、そのリストから不正アクセスを行う攻撃。

NRIセキュアテクノロジーズ実施「企業における情報セキュリティ実態調査2015」

標的型メールは、【役員】の方が開封する

- 2015年度に実施した標的型メール訓練の対象者の開封率(*1)は12.8%
- 役員(*2)と従業員を比べると(*3)、役員の開封率は従業員の約1.6倍。2014年度の結果1.5倍とほぼ同程度
  - 役員は比較的機密度の高い情報へのアクセス権を有し、標的となる可能性が高い



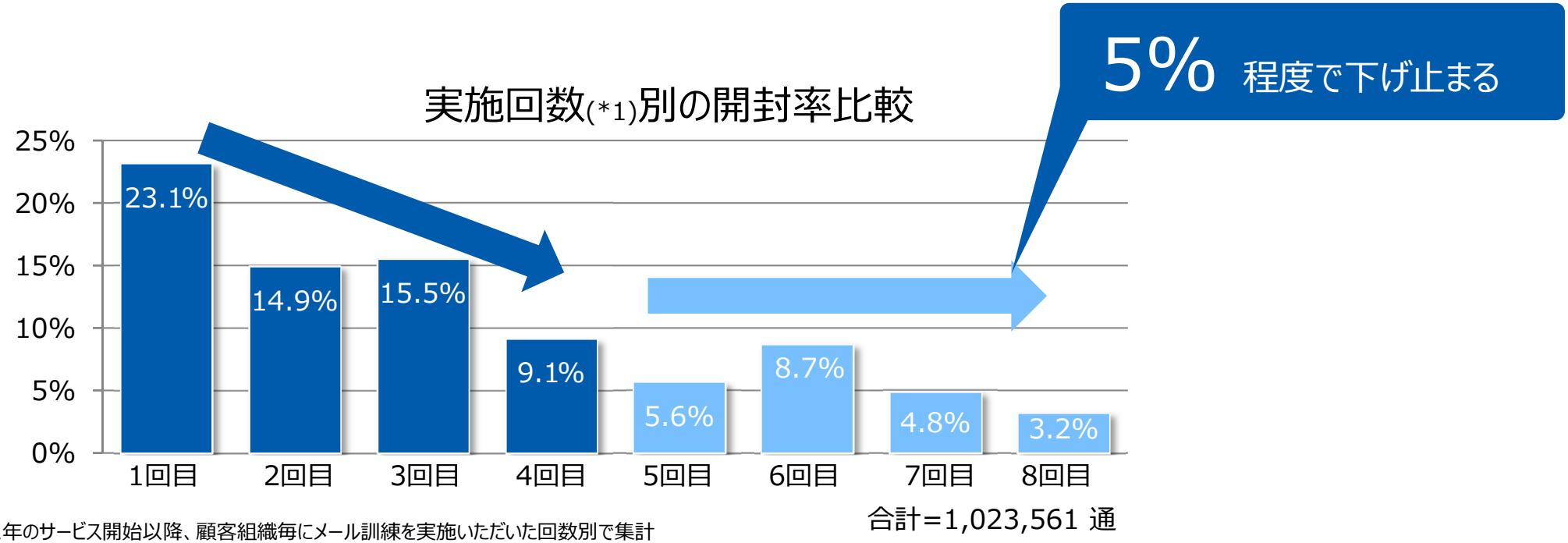
役員の開封率は、従業員の開封率の約1.6倍

*1: 訓練メールに添付した疑似攻撃ファイルを実行、あるいは訓練メールに記載した疑似攻撃サイトへのリンクをクリックした割合
*2: 会社法における役員などを「役員」と表現
*3: 通常は1人1メールアカウントなので、メール配信数をメール訓練対象者数ののべ人数として集計・分析

サイバーセキュリティ傾向分析レポート 2016

開封率はゼロにはならない

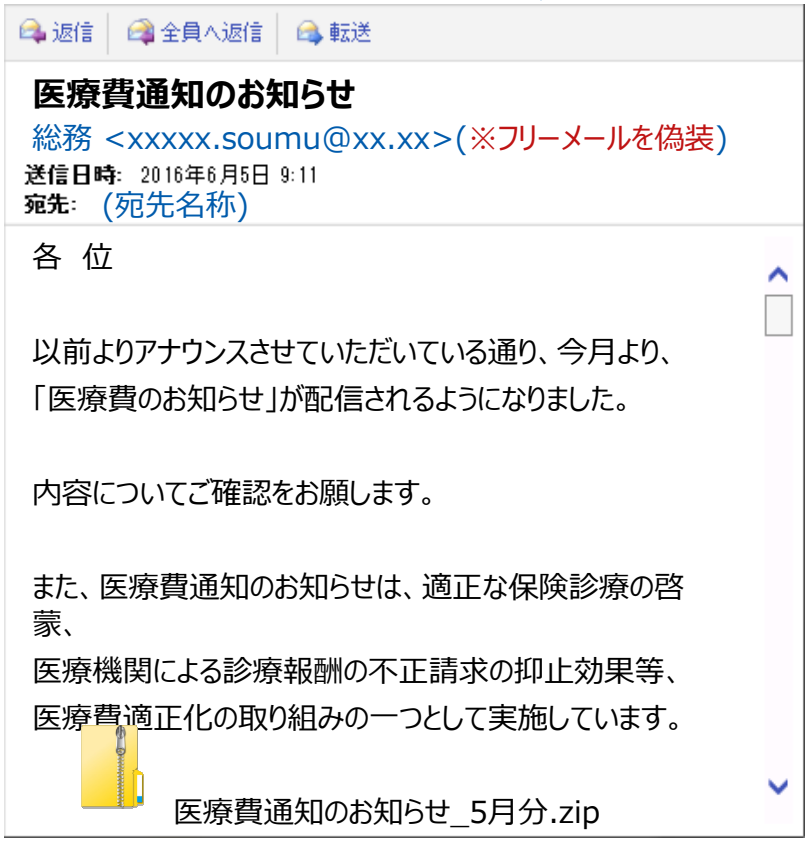
- 標的型メール訓練を繰り返すと開封率は下がる
  - 初めて訓練を実施した組織では開封率が23.1%であるのに対し、訓練を重ねると徐々に開封率は小さくなっていく
  - 理由：メール攻撃の疑似体験による効果 ⇒ 標的型メールに対して意識が向くようになる
- しかし、開封率をゼロにすることは非常に難しい
  - 回数を重ねるごとに開封率の下げ幅は小さくなり、5%程度に収束する
  - 理由：個人的関心・業務上の役割 (次スライド参照)、攻撃メール内容の巧妙さの向上など



*1: 2011年のサービス開始以降、顧客組織毎にメール訓練を実施いただいた回数別で集計

違和感 ＜ 個人的関心

落ち着いて見れば、明らかに怪しいと分かる


返信　全員へ返信　転送

医療費通知のお知らせ

総務 <xxxxx.soumu@xx.xx>(※フリーメールを偽装)

送信日時: 2016年6月5日 9:11

宛先: (宛先名称)

各　位

以前よりアナウンスさせていただいている通り、今月より、
「医療費のお知らせ」が配信されるようになりました。

内容についてご確認をお願します。

また、医療費通知のお知らせは、適正な保険診療の啓蒙、
医療機関による診療報酬の不正請求の抑止効果等、
医療費適正化の取り組みの一つとして実施しています。

医療費通知のお知らせ_5月分.zip

- 個人的関心の高いテーマ・・・金銭　健康　趣味
  - 2015年度、開封率が最も高かった訓練メールは左図
    - 2014年頃から「医療費通知」を名乗る攻撃メールが、国内で散布され続けた事象を踏まえて作成(*)
  - 個人的関心が高いテーマであるため、違和感を感じる前に添付ファイルを開封・クリックしてしまった可能性

訓練メール文面別の開封率比較(上位10パターン)

件名	開封率
医療費通知のお知らせ	38.8%
先ほどの写真の件	24.9%
メールボックスの設定が変更されました	23.4%
取材のお願い	17.6%
Re: グループ全体会議	16.9%
調査事項	15.8%
お知らせ【eチケットお客様控え】	14.7%
Re: 経営戦略セミナー事務局につきまして	14.0%
【緊急】ウィルス感染の検出（自動配信）	13.8%
【重要】Windows の脆弱性暫定回避策	13.7%

上位10パターンの配信数合計＝151,778 通

セキュリティリスク ＜ 業務遂行

■ 業務上の役割

- 業務上の役割から、添付ファイルの開封や本文内のURLリンクをクリックすることに対して、一定の強制力が働く場合がある
- 例：対外の不特定多数の相手とやり取りする必要のある、メールでの問い合わせ窓口担当者が下図のメールを受け取った場合は？

差出人	[苗字]@xxxxxxxx.co.jp
宛先	[問い合わせ窓口のアドレス]
件名	商品の破損について
添付	商品の画像.zip

お世話になっております。

先日注文して届いた商品が添付の通り破損していました。
至急交換をお願いします。

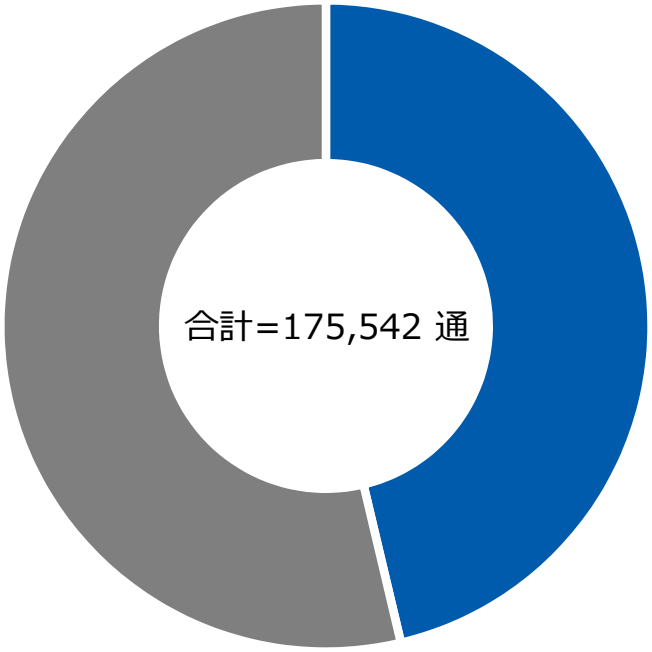
XXXXXXXX株式会社
○○部
氏　名
E-mail: ....

お客様からのメールだ
確認しなきゃ！！

社内メールに見せかける＝「なりすましメール攻撃」

- 2016年2～3月に検出したマルウェア付きメールのうち、46.3%のメールで送信元/送信先メールアドレスのドメイン(@よりも後ろの部分)が一致
  - 社内メールを装って、外部から送信している（＝なりすまし）
  - メールアカウント名(@よりも前の部分)は、customer、service、adminといった汎用的に使われ得る単語を組み合わせたもののほか、copier、scanner、などが多い

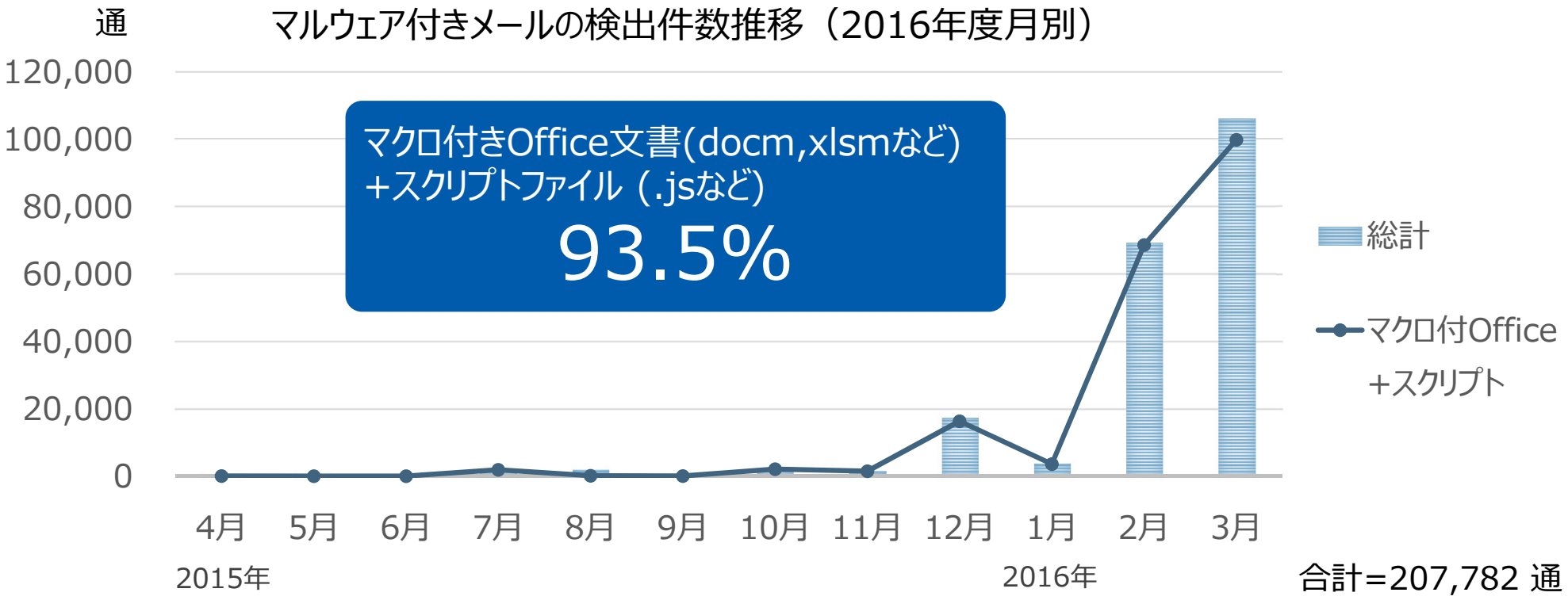
2016年2～3月に検出したマルウェア付きメール



From:△△@●●
To: XX@●●
のように、送信元/送信先ドメインが同じメールが
46.3%

悪用される添付ファイルにはトレンドがある

- 2016年2月以降、マルウェア(*2)付きメールが急増
  - 通年(2015/4-2016/3)拡張子(*1)を分析(*3)すると、Word/Excelなどのマクロ付きOfficeドキュメント(55.3%)と、スクリプト(*4)ファイル(38.2%)が、マルウェア付きメール全体の93.5%を占める



*1: ファイルの種類を識別するためにファイル名の末尾に付与される文字列。docxやxlsxなどがそれにあたる
*2: コンピュータウイルスなど、不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアなどの総称
*3: 当社のマネージドセキュリティサービス(MSS)において、スパムフィルタを通過したメールのうち、アンチウィルス製品にてマルウェア付きと判定されたメールが対象。
圧縮ファイルが添付されていたケースでは、展開後の拡張子を基に集計
*4: 機械語への変換や実行可能ファイルの作成などの過程を省略、あるいは自動化した簡易なプログラム

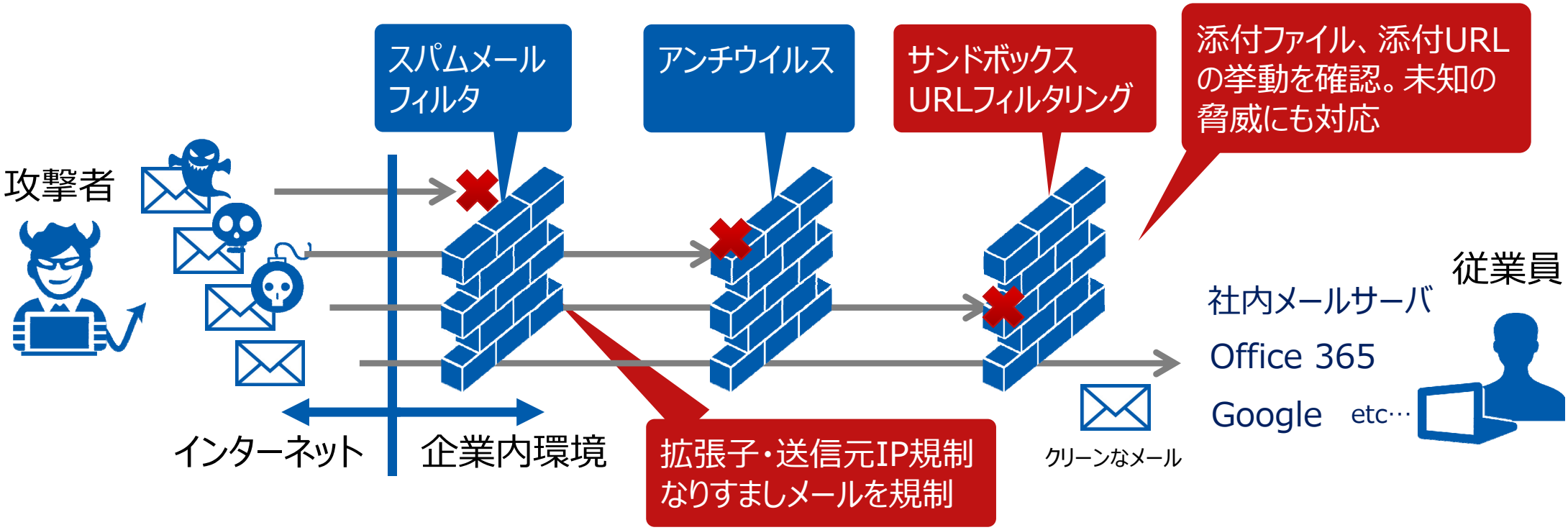
標的型メール攻撃への対策は多層で行う

- ヒトの対策例：開封率を目安に、メール訓練の実施・継続を検討する
  - 開封率が5%水準に低下するまで：標的型メールに対して意識を向けさせる
    - 攻撃の手口となる基本的なパターンを、従業員や役員が一通り疑似体験する
  - 開封率が5%水準に下がった後：標的型メールへの意識を維持しつつ、被害を最小限に抑えるための訓練を行う
    - 新たな気づきを与える
      - 興味を強くかき立てるメール文面/「業務内容」に応じたメール文面を用いる
    - 被害の最小化に向けた訓練
      - 不審メール受信後の対応の整備・訓練
      - 不審メールの添付ファイル開封やURLリンクへアクセスした後の対応の整備・訓練
- システム対策例：添付ファイル・URLの取扱い方法と・侵入経路を見直す
  - 添付ファイルを取り扱わずに済む業務設計
  - 添付ファイルをメールフィルタリングシステム側で制御
    - 業務で不要な添付ファイルはシステムで規制する
  - 添付ファイルを「安全」に開くことができる環境を整備
    - サンドボックス解析　仮想化　無害化ソリューションなど
  - フィッシング(URL誘導型)へ対応するソリューションの検討

システム対策：未知の脅威への対策も

- 多くの企業では既にスパムメールフィルタリング製品やアンチウィルス製品が導入されている
  - 加えて振る舞い検知型製品など高度な入口対策が重要

- 基本的には多層での防御、さらに拡張子規制で効率よく攻撃メールの流入を防ぐ
  - 後続機器に負荷をかけないよう、最もインターネットに近い位置でフィルタをかけることが重要
  - 流行に沿って規制対象を定期的に見直す




NRI
未来創発
Dream up the future.