NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ

Internet Week 2016

【T7】プロが厳選！低予算でもできる効果あるセキュリティ施策

1.マルウェア流入対策のもうひと工夫

2016年11月30日

NRIセキュアテクノロジーズ株式会社
サイバーセキュリティサービス事業本部

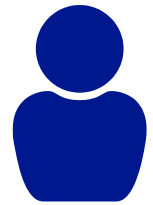
セキュリティコンサルタント　中島　智広

〒100-0004
東京都千代田区大手町一丁目7番2号 東京サンケイビル

目次

1.はじめに

マルウェア流入の多層防衛



ゲートウェイ

- パターンマッチング
- サンドボックス
- カテゴリ規制
- スパムフィルタ
- レピュテーション

端末

- パターンマッチング
- 実行時検出
- 設定堅牢化
- ユーザ警告

ヒト

- アウェアネス(気づき)

強度は**製品仕様と設定**に依存

強度はヒトに依存(**まばら**)

100%の対策はない、多層の取り組みでリスクを可能な限り低減する

マルウェアの2大流入経路

メール

- メールに添付された悪意あるファイルを実行あるいは開くことで感染
- あからさまな実行形式ファイルのほか、Officeマクロ、製品の脆弱性を悪用するものも多い
- 一般には利用者のアクションが前提

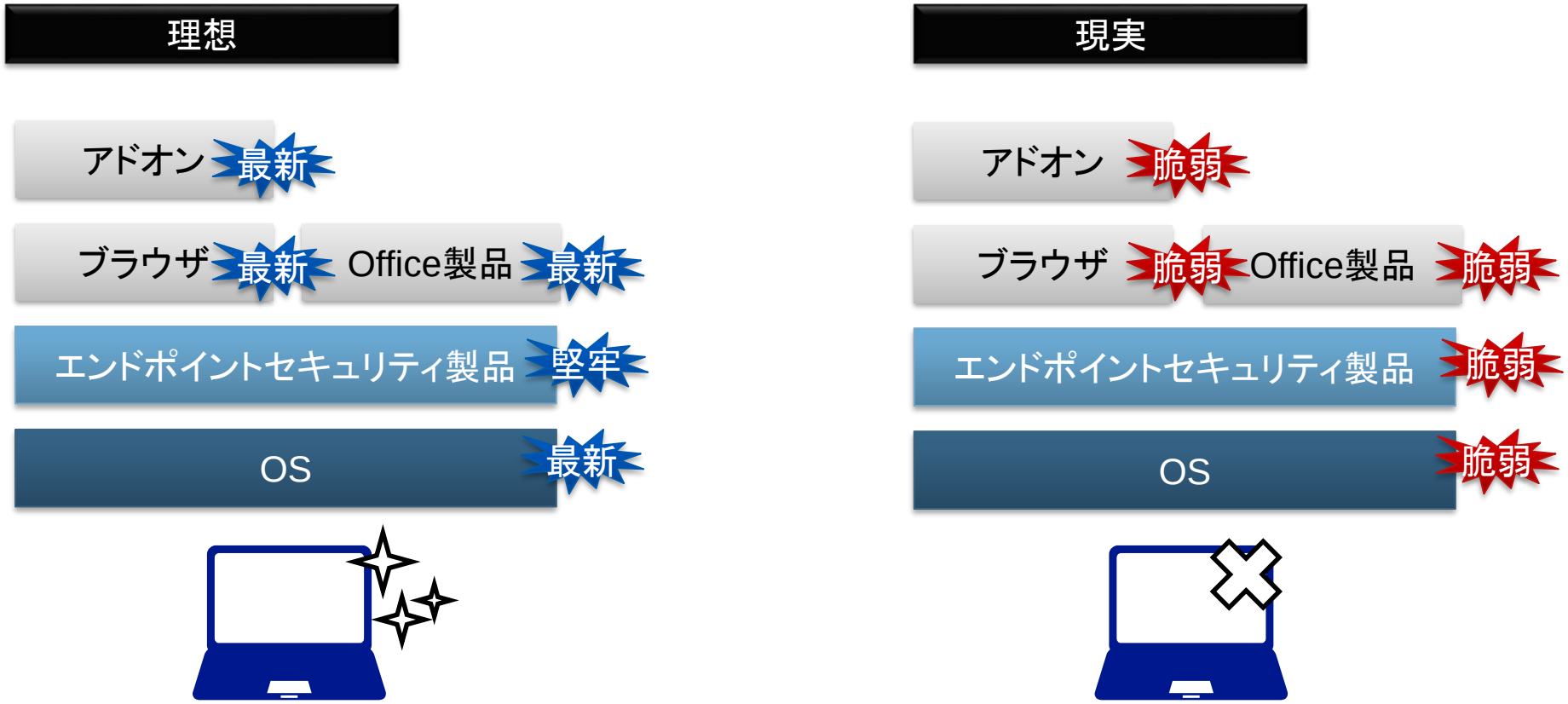
システム的な対策にくわえヒトの耐性強化への取り組みが課題

Web(ドライブバイダウンロード)

- 悪意のあるURLにブラウザでアクセスすることで感染
- 製品脆弱性の悪用が前提
  - ブラウザの脆弱性(Internet Explorer, Firefox, Chromeなど)
  - アドオンの脆弱性(Java, Flash Player, PDF Viewerなど)

どのように利便性を下げずに悪意あるURLへのアクセスを防ぐかが課題

端末セキュリティの理想と現実



脆弱な状態を取り繕いながら運用している組織は多い

システム担当者のジレンマ

現行保証	対策費用	対応工数
うちの業務システムはIE8+Java5しかサポートされていません。	パッチ適用作業は検証作業も含めて1回500万円かかります。	製品のセキュリティ強化の影響でサポート稼働が逼迫しています。
 事業部門	 保守運用委託先	 サポート窓口
		
サポート切れ製品の継続利用	パッチ適用断念	セキュリティ機能の無効化・設定脆弱化

わかっていながらも最善の対応は難しく、マイナスの対応をしてしまうこともある

代替ソリューション導入の陥りがちなポイント

代替ソリューション導入はなかなか順調に進まない

代替の限界

問題を本質的に解決するわけではなく、効果はベストエフォート。銀の弾丸は基本的にない。

評価を進めた結果としてこの結果に至ることや、導入後に効果が問題視されることもある。

タイミングとデリバリー

現場主導のボトムアップアプローチでは予算化のタイミングが限られがち。大きく次年度予算と下期修正予算の2回。

昨今のソリューションは一般に買い切りではないため余剰予算での一時費用計上といった対応も難しい。

コンセンサスと稟議

大きな組織ほど意思決定に時間と工数がかかる。スモールスタートを目指すも「全体最適」を求められ調整に時間を要することも。

既存ソリューションとの重複を指摘されることも多い。多層防衛と多重投資は切り離せない永遠の説明課題。

マルウェア流入対策のもうひと工夫

本命の取り組みと平行して、着手しやすく効果の出やすい取り組み(工夫)を

■アプローチ

- 当たり前のことをもう一度見直す
- 今あるものをより賢く使う
- トレンドを積極的に取り入れる

■**低予算でもできる**方法論や取り組み事例をご紹介

- 設定の見直し・堅牢化
- 送信ドメイン認証の活用
- メール添付ファイル拡張子規制
- セキュリティアウェアネス

2.設定の見直し・堅牢化

2.設定の見直し・堅牢化

セキュリティ対策製品の無効化防止

セキュリティ対策製品を無効化するマルウェアの報告

「セキュリティ対策製品を停止させるウイルスに注意」――IPA

勝村幸博　2004/11/04　ITpro

目次一覧

W32/Netskyは**1,243件**の届出が寄せられ8ヶ月連続でワースト1の届出となりました。続いて、W32/Bagle 485件、W32/Mydoom 385件となりました。

（1）新種ウイルスW32/Bagzの手口に騙されないように

10月に新たに出現した**W32/Bagz**及び**W32/Darby**はメールの添付ファイルを介して感染を拡大するウイルスです。添付ファイルを開くことで感染し、パソコン内から収集したアドレス宛に**ウイルスを添付したメールを送信**したり、ウイルス対策ソフトなどの**セキュリティ対策製品を停止**したりします。

10年以上前から観測されている常套手段

製品の無効化操作の例

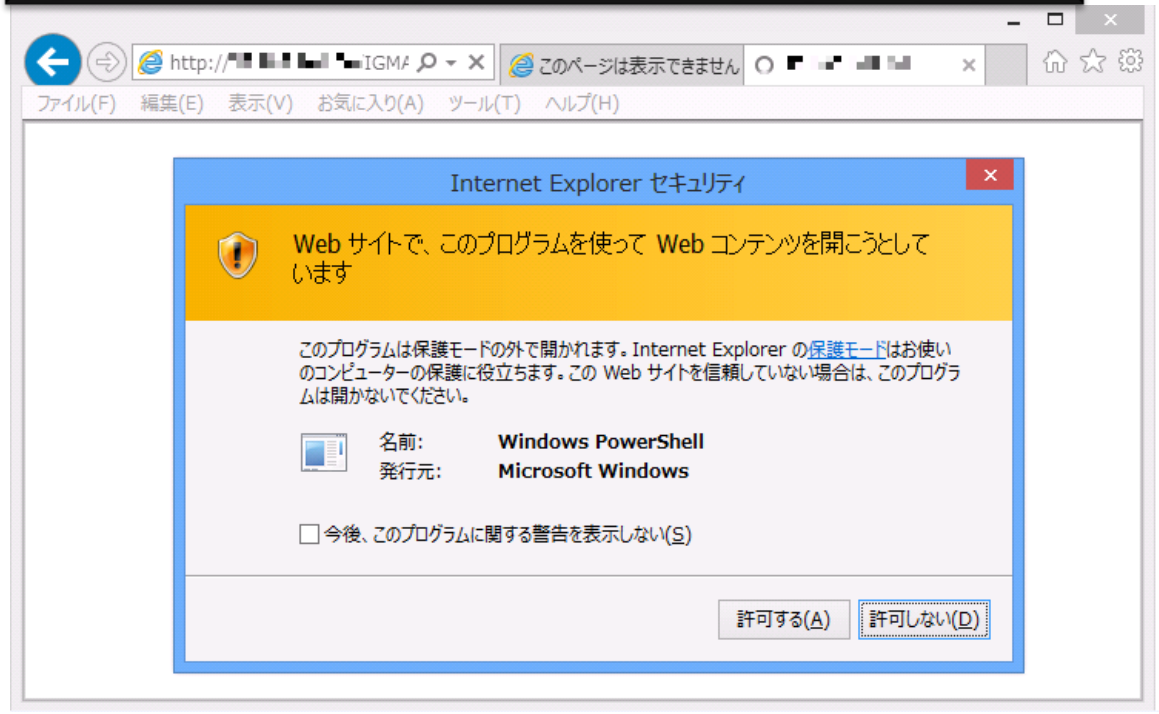
製品によっては、一律禁止とするほかにパスワードによる保護などの対策もある

[引用元]
http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20041104/152153/
http://www.ipa.go.jp/security/txt/2004/11outline.html
http://esupport.trendmicro.com/solution/ja-JP/1106684.aspx

攻撃者に導入済み対策を回避させず、守れるものを確実に守る

ブラウザの堅牢化（保護機能の利用）

保護機能により不正なプログラム実行を防御されている例



ドライブバイダウンロード攻撃を水際で防御可能だが、
現行保証や利用者の省力化のため無効化している組織も多い

保護機能の例(Internet Explorer)

保護モード

外部プログラム(アドオンを含む)の実行時に処理を停止させユーザへ警告を表示するほか、プロセスを隔離して権限を限定して実行させる

Smart Screen フィルター

悪意のあるプログラムを含むと判断したサイトを閲覧しようとした場合に処理を停止させ警告を表示する

UAC※Windows設定

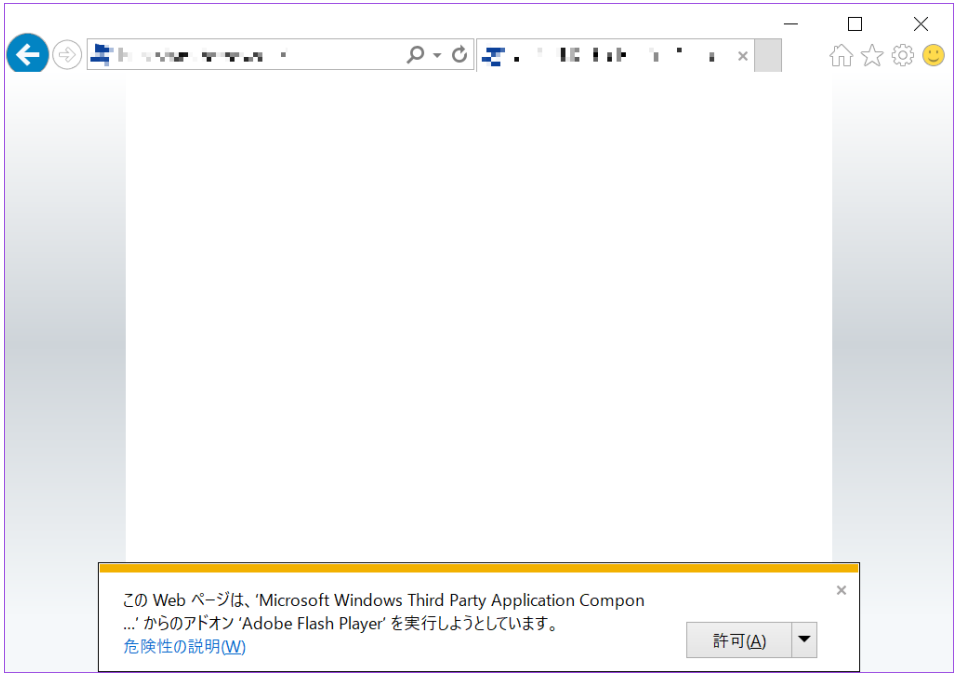
攻撃の一環で管理者権限を必要とする動作を試行した際に処理を停止させ警告を表示する

製品標準のセキュリティ強化には意味がある、安易に無効化せず守れる攻撃を守る

ブラウザの堅牢化（アドオンの自動実行抑止）

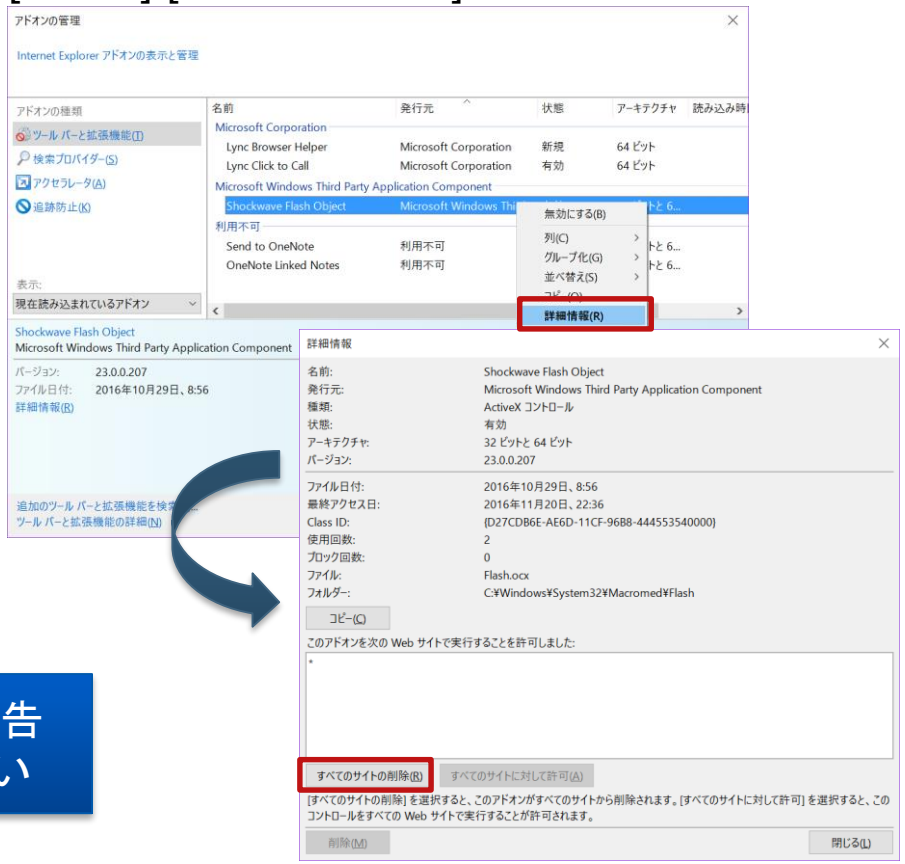
日常的なWebアクセスによって生じる意図しないアドオンの自動実行を抑止

アドオンの自動実行を抑止された例



設定方法

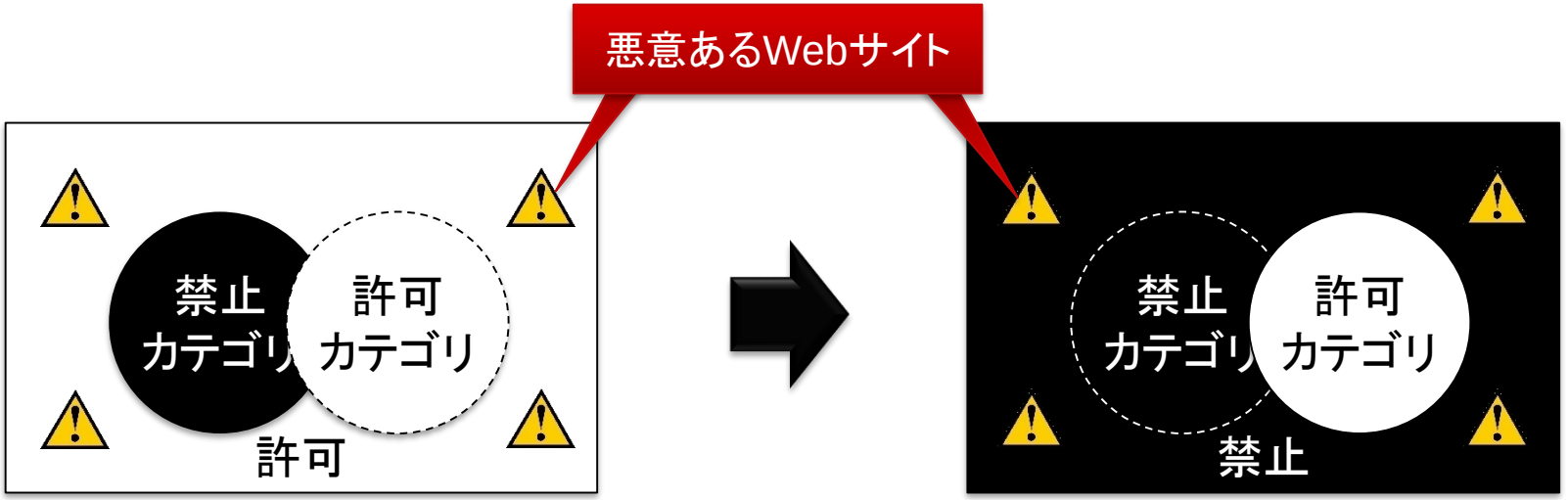
[ツール]-[アドオンの管理]



初めてアドオン実行を要求するURLに対して実行前に警告
一度実行したURLには登録され次回以降は警告されない

コンテンツフィルタのルール見直し

対策の不十分な端末は、悪意あるWebサイトにアクセスさせないことが鉄則



原則として許可URLをホワイトリストで管理することが望ましい
管理が煩雑な場合は**オーバーライド機能**の活用も検討するとよい

オーバーライド機能とは

アクセスが許可されていないURLに対し、規制画面上の操作により一時的に数分間だけアクセス許可する機能。ホワイトリスト運用の負荷を低減する。実行ログの監査を組み合わせることにより、機能が悪用され定常的にオーバーライドが実行されている場合には疑わしい振る舞いとしての検出を期待できる。

3.送信ドメイン認証の活用

標的型メール攻撃とドメイン詐称

インシデント報告書から類推される標的型攻撃メール

From	[苗字]@[取引先のドメイン]
To	[実在メールアドレス]
Subject	旅程ご確認のお願い

お世話になっております。

<内容の確認を促す文章>

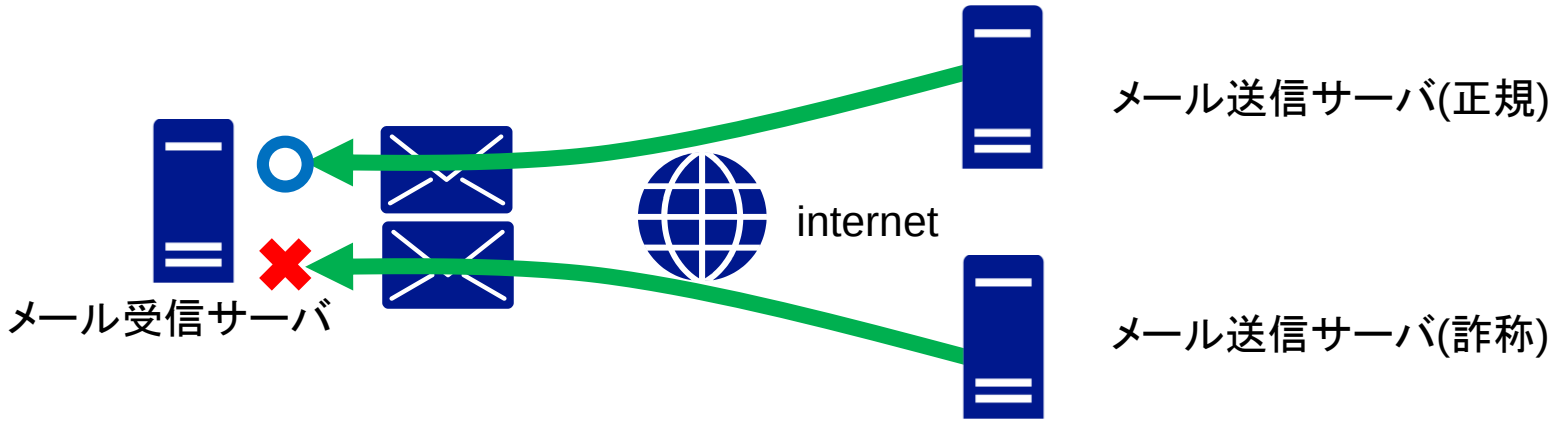
〇〇株式会社
△△△△部
□□□□

旅程表.zip

標的型攻撃メールでは、実在のドメインを詐称して送られてくる

送信ドメイン認証とは

受信したメールが正規のメールサーバから送信されたものかを判別可能とする仕組み



プロトコル	概要
SPF	正規のメール送信サーバのIPアドレス情報を公開することで受信側で詐称メールを判別可能とする仕組み
DKIM	メールヘッダに電子署名を付与することで受信側で詐称メールを判別可能とする仕組み
DMARC	SPFとDKIMといった送信ドメイン認証をより活用しやすくするための仕組み

送信ドメイン認証の普及状況

正規メールのスパム誤認を防ぐ意味も有り、送信者側の設定は一般化している

↓

受信者への警告に活用すれば誤遮断などの大きな弊害なく対策効果を期待できる

また、総務省が行っている電気通信事業者における全電子メール数の送信ドメ イン認証結果調査によると、2014 年（平成 26 年）6 月時点での SPF の普及率は 94.31%と高い普及率を保っており、DKIM の普及率は 39.84%と徐々に普及率が増加 している。

[引用元]
特定電子メール等による電子メールの送受 信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気 通信事業者によるその導入の状況
http://www.soumu.go.jp/main_content/000354170.pdf
[参考]
送信ドメイン認証結果の集計（2015年6月時点）
http://www.dekyo.or.jp/soudan/image/anti_spam/archive/2015/201510_r2.pdf

送信ドメイン認証の活用事例

Subject(件名)での注意喚起

From	alice@example.jp
To	[自分]
Date	YYYY/MM/DD hh:mm:ss
Subject	[ドメイン詐称の可能性]Test mail

警告文言の付与

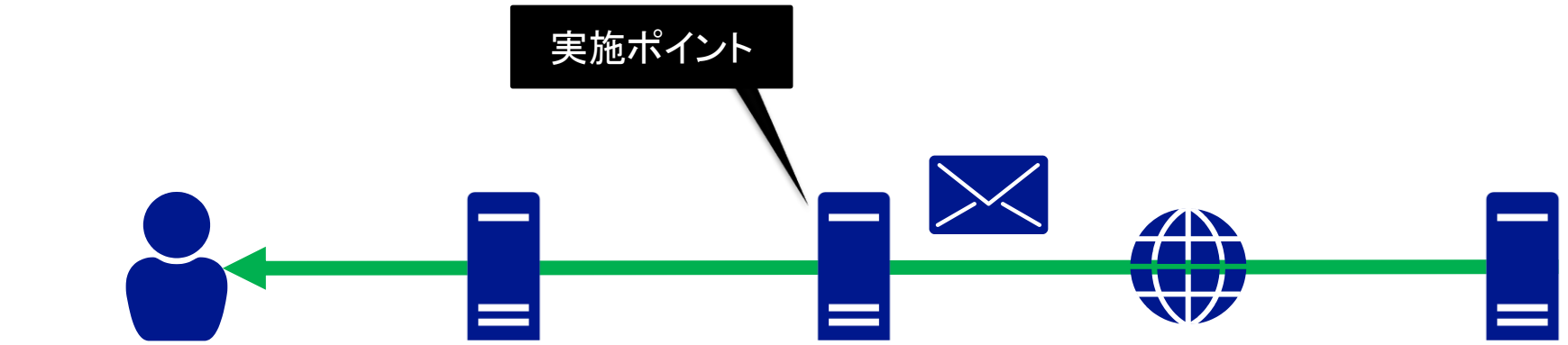
Web UIでの注意喚起(Gmailの事例)

「？」アイコンで警告

[参考]通常の表示

視覚効果により、ユーザにドメイン詐称を警告、周知啓発もセットで必要

送信ドメイン認証の実装箇所



メーラー(MUA)
- Outlook
- Thunderbird
  など

社内メールスプール
- POPサーバ
- IMAPサーバ
- Exchange
  など

メールゲートウェイ
- アンチスパム
- アンチウイルス
- その他MTA

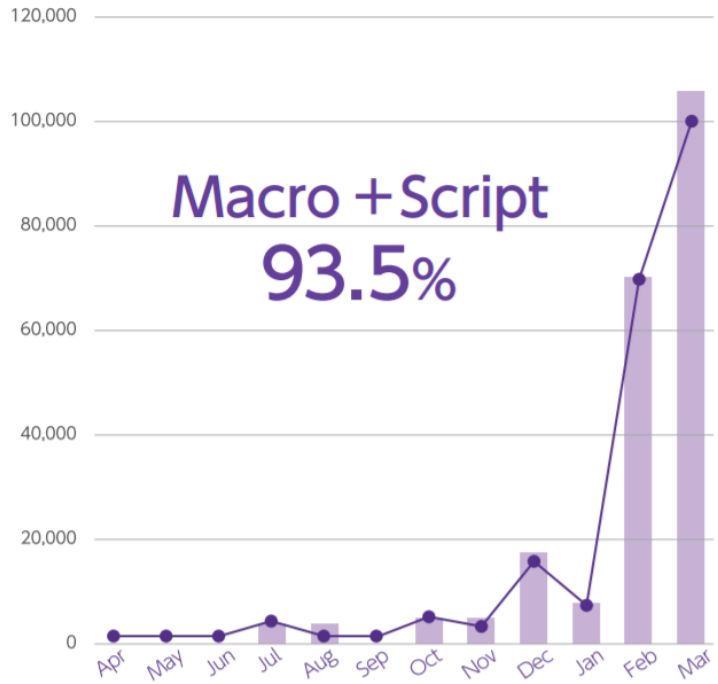
メール送信サーバ

普及率の高いSPFでは送信元IPアドレスの識別が可能な箇所で実施する必要がある

4.添付ファイル拡張子規制

メール添付マルウェアの拡張子傾向

当社統計(2015年度)



IBM Tokyo SOC殿統計(2016年上半期)

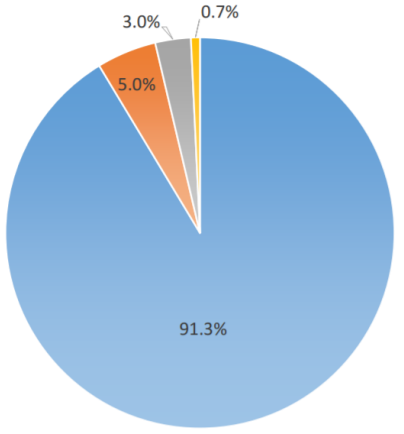


図 13 検知された添付ファイルの形式別検知数割合
(Tokyo SOC 調べ 2016 年 1 月 1 日～2016 年 6 月 30 日)

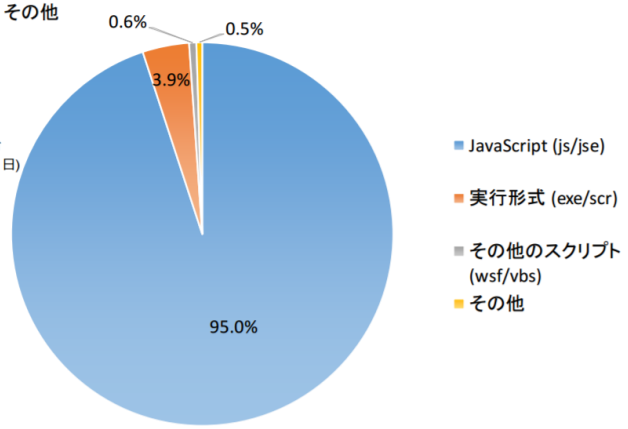


図 14 検知された圧縮形式ファイル展開後の形式別検知数割合
(Tokyo SOC 調べ 2016 年 1 月 1 日～2016 年 6 月 30 日)

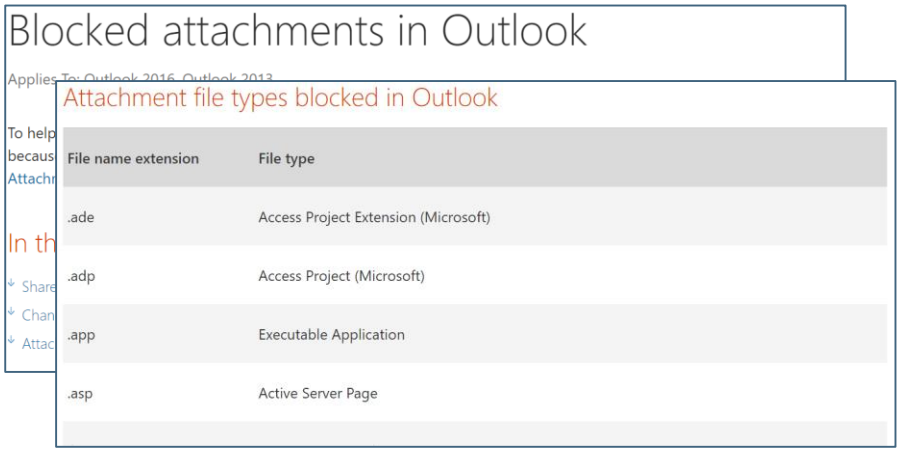
[引用元]
http://www.nri-secure.co.jp/security/report/2016/cstar.html
https://www.ibm.com/blogs/tokyo-soc/wp-content/uploads/2016/02/tokyo_soc_report2016_h1.pdf

悪用される拡張子には傾向があり、不要なものは規制することで防御を期待できる

対象となる拡張子と定義方法

ブラックリスト

既知のリストを取り入れて定義
<リストの例>



[参考]
https://support.office.com/en-us/article/Blocked-attachments-in-Outlook-434752e1-02d3-4e90-9124-8b81e49a8519

抜けや漏れ、トレンドの変化に追従が必要
(例:docm/xlsm)

おすすめ！

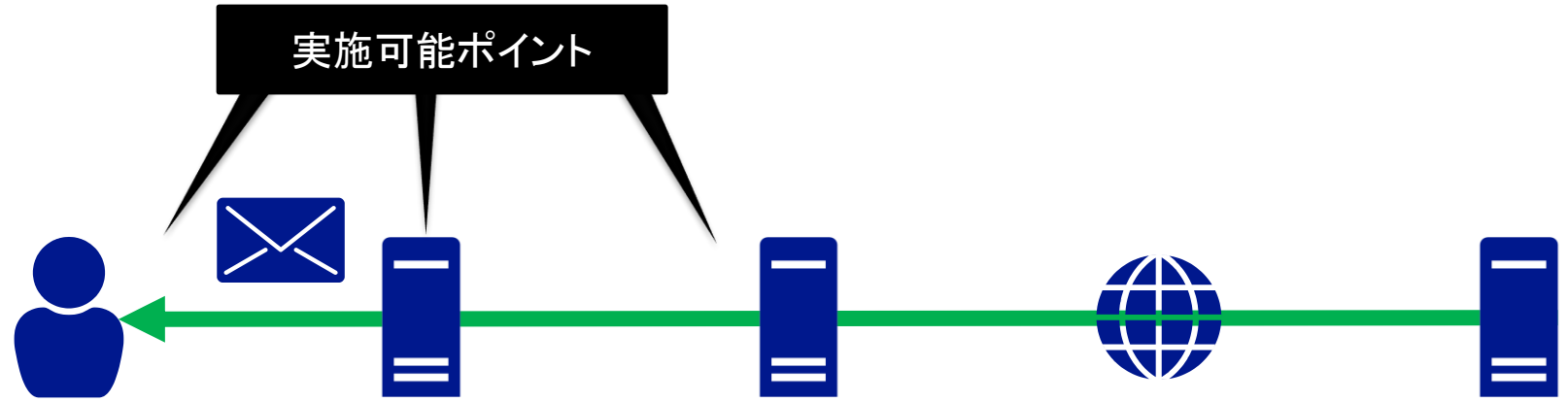
ホワイトリスト

自社の業務を踏まえて必要なもののみを定義
<リストの例>

.zip/.gz/.7z	.xlsx/.xls
.pdf	.docx/.doc
.jpg	.pptx/ppt
.png	.vsd/.vsdx
.bmp	.jtd
.ai	など

必要なものだけで構成されていれば、
メンテナンスは基本的に不要

拡張子規制の実装箇所



MUA
- Outlook
  など

社内メールスプール
- POPサーバ
- IMAPサーバ
- Exchange
  など

メールゲートウェイ
- アンチスパム
- アンチウイルス
- その他MTA

送信サーバ

実施可能なポイントは多く検討しやすい、実施しやすいところを選んで実施

拡張子規制の考慮点①

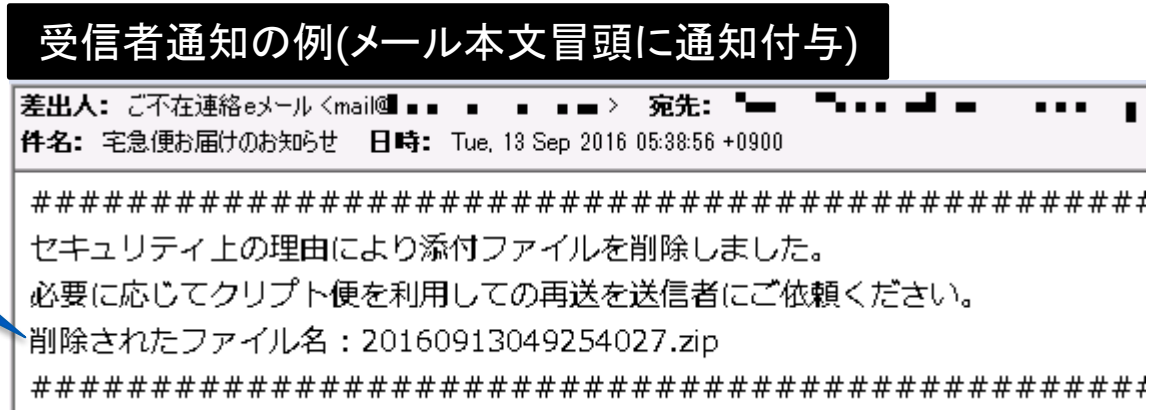
- 圧縮アーカイブ形式/winmail.dat
  - ゲートウェイ製品によっては展開後のファイル名やMIMEタイプで判定してくれるものもあるが、対応できない場合は抜け穴となり得るため、対応可能な製品での実装が望ましい
  - winmail.datはOutlook環境にてHTMLメールにファイル添付する際にカプセル化されるもの、テキスト形式で送信することでカプセル化を回避可能なため周知徹底により規制は可能

    [参考]Outlook を使用する送信者から受信された電子メールに Winmail.dat 添付ファイルが含まれる
    https://support.microsoft.com/ja-jp/kb/278061

- 受信者への通知
  - 規制により削除されたことを受信者が認知するための工夫が望ましい
  - 送信者に対しての通知は規制の存在を知られ、回避試行が可能なためしない方がよい

メールセキュリティ製品の機能によりアーカイブ展開後に拡張子規制された通知の例

受信者通知の例(メール本文冒頭に通知付与)

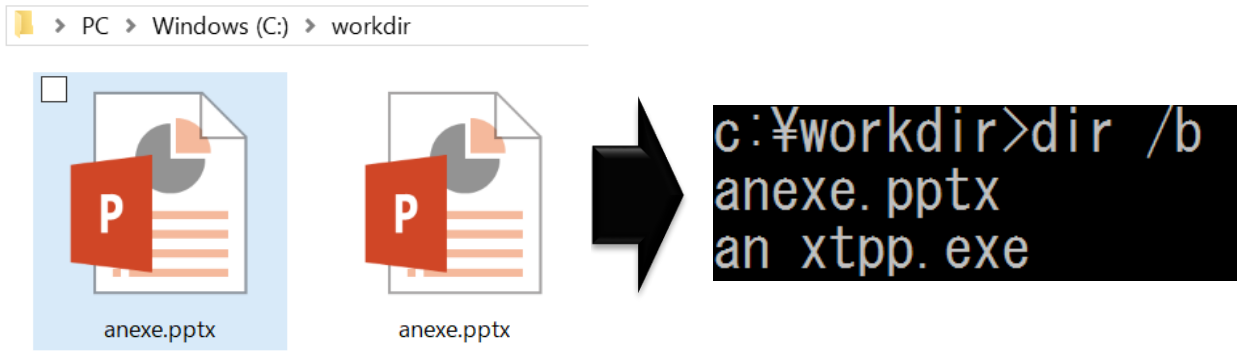


拡張子規制の考慮点②

■実行ファイル形式(.exe)の取り扱い

- 主に自己解凍形式のアーカイブファイル送付をする場合に課題
- 自己解凍形式を標準とする製品の利用が義務づけられている会社もあり悩ましい問題
- とはいえ遮断が望ましいことは自明であるため、取引先との調整も含めて検討したい

Unicode制御文字の悪用した拡張子偽装の例



RLO(Right-to-Left Override)を悪用し見た目を偽装したもの
ヒトは見抜けないが機械は見抜ける(=拡張子規制の効果有)

5.セキュリティアウェアネス

［再掲］マルウェア流入の多層防衛

ゲートウェイ

- パターンマッチング
- サンドボックス
- カテゴリ規制
- スパムフィルタ
- レピュテーション

端末

- パターンマッチング
- 実行時検出
- 設定堅牢化
- ユーザ警告

ヒト

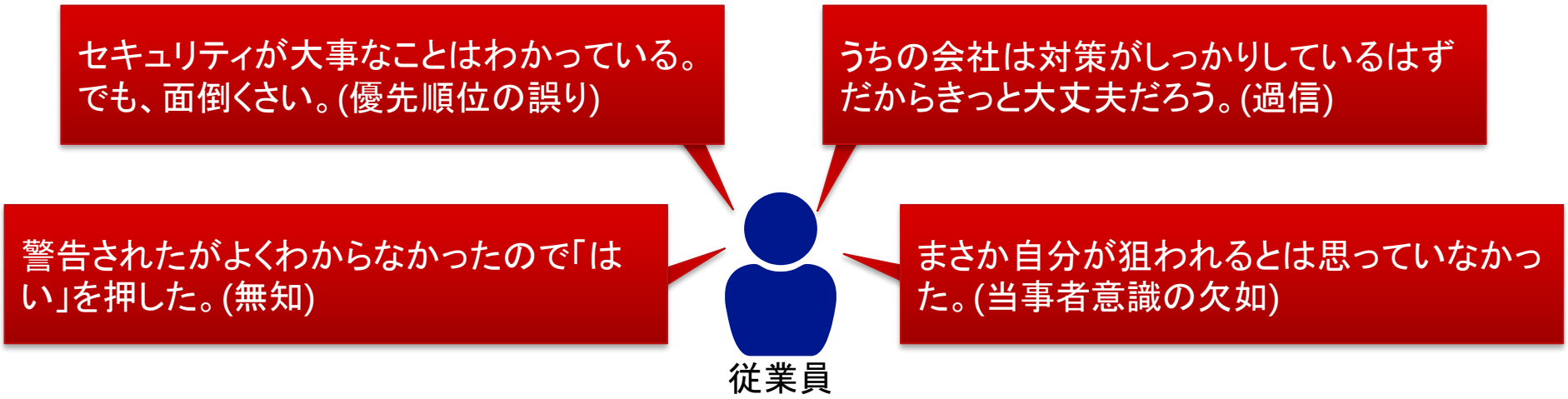
- アウェアネス(気づき)

強度は製品仕様と設定に依存

強度はヒトに依存(まばら)

100%の対策はない、多層の取り組みでリスクを可能な限り低減する

ヒトに対する啓発、意識付けの必要性



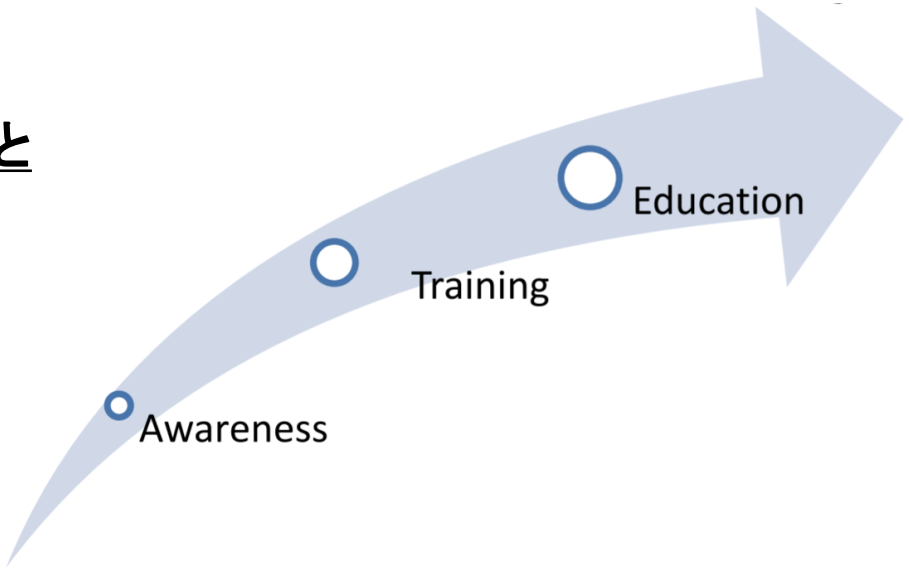
システム的な対策を推し進めても、ヒトの意識が脆弱なままでは多層防衛たりえない

身近な問題として認識させ、優先度を上げさせることが肝要

アウェアネスとは

「アウェアネスがセキュリティの最初の防衛線となる。」

- 組織の教育戦略の一要素
- **シンプルにセキュリティに注意を向けさせること**
- 幅広い対象に浸透させられる取り組み
- 職務成果を促進するための知識と技能を築くことを目標としたトレーニングとは異なる
- 標的型メール攻撃訓練はその代表



[引用元]
https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport
[参考]
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

アウェアネスに意味はないか？ ～標的型メール訓練を題材に～

よくある反対意見

ALL or Nothing論

マルウェア感染をゼロにはできない。ゼロにできない以上やっても意味がない。

そもそも100%防ぐ対策はない。多層防衛が基本。

持続性問題視論

意識が高まるのは実施直後だけ。徐々に低下していくので意味がなくなる。

正しい。ただし繰り返し実施することで効果の持続を期待できると考えられている。

システム対策優先論

システム的な対策を強化したほうがよい。

正しい。コストの優先順位が要因であれば低コストでの実施方法を模索することが望ましい。

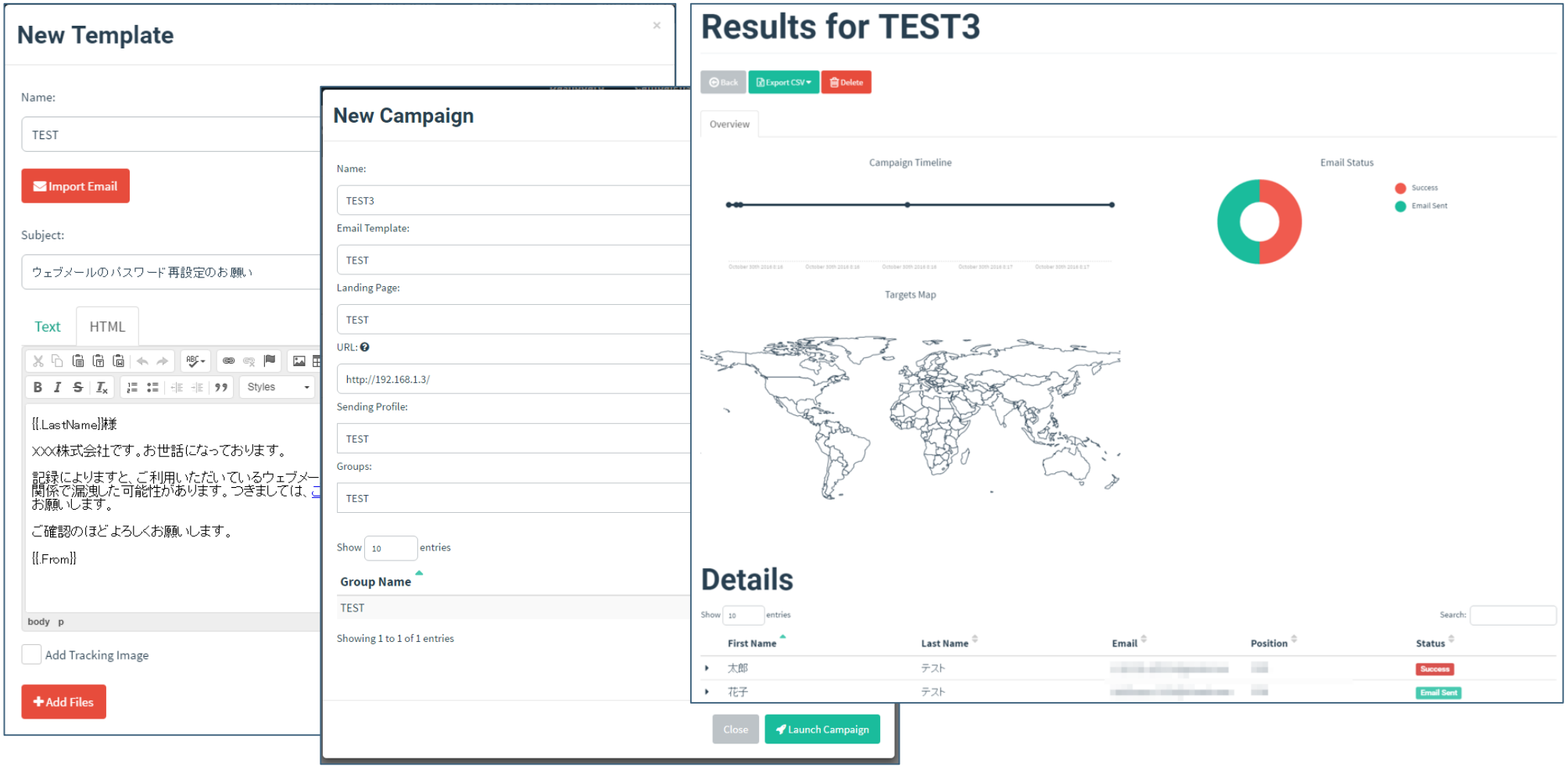
「意味はない」ではなく、「依存した対策はいけない」が適した解釈

いろいろある取り組み方

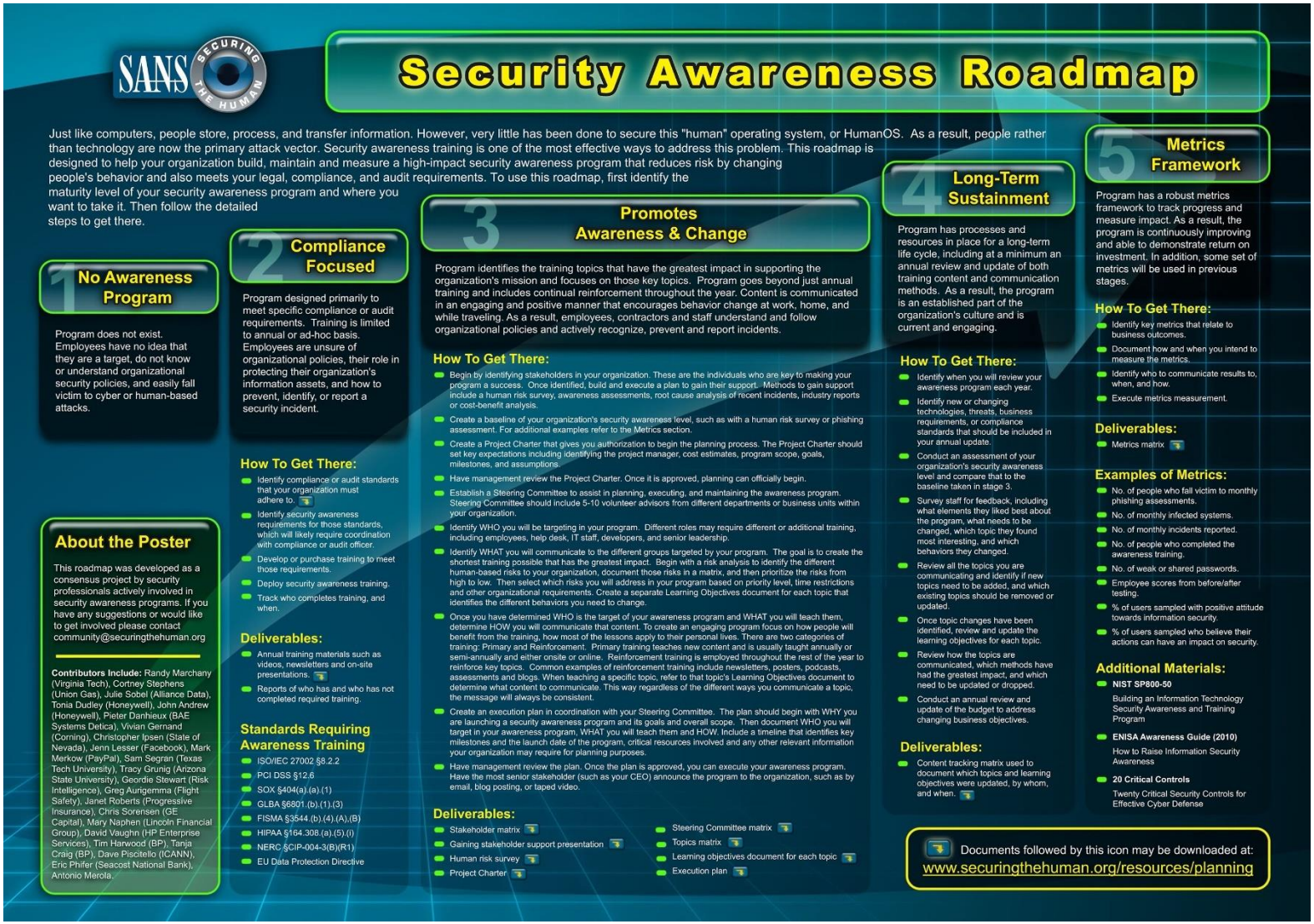
フルマネージドサービス	ASP/SaaS活用	オープンソース活用
豊富なノウハウに基づく魅力的な提案とコンサルティングが強み	費用を抑えつつ定型化による手間を抑えた取り組みが可能	とにかく費用をかけずに現場の稼働のみで取り組みが可能
実施だけでなく経営報告まで含めた効果的な取り組みを期待できる	自社向けのカスタマイズは自前で必要	すべて自前で内製化、知恵を絞りながら進める必要がある
実施回数に応じた課金が一般的	一般に契約期間内は何度でも実施可能	現場の稼働があれば何度でも実施可能

組織の状況に応じて最も最適な実施方法を選択

［参考］GoPhish Open-Source Phishing Framework (https://getgophish.com)



[参考] セキュリティアウェアネスのロードマップ



[引用元]https://securingthehuman.sans.org/blog/2012/12/11/security-awareness-roadmap-officially-released

6.おわりに

施策まとめ

- 防げる攻撃を防げないのはもったいない、防ぐために設定の見直しを
  - セキュリティ対策製品の無効化防止
  - OSやブラウザのセキュリティ機能を無効化しない
  - コンテンツフィルタのルール見直し

- 傾向を踏まえるとレガシーな対策も効果を期待できる、使えるものは最大限活用を
  - 送信ドメイン認証の活用
  - メール添付ファイルの拡張子規制

- ヒトの意識が脆弱なままでは多層防衛たりえない、幅広く意識向上の取り組みを
  - セキュリティアウェアネス

このあとのお話

1. マルウェア流入対策のもうひと工夫
   中島 智広(NRIセキュアテクノロジーズ株式会社)

2. マルウェア流入後の社内ネットワーク侵害対策
   蔵本 雄一(日本マイクロソフト株式会社)

3. 手軽にできる外部公開サーバ観測の効用と活用法
   藤崎 正範(株式会社ハートビーツ/株式会社ウォルティ/日本MSP協会)

4. できるところから始める運用の備え
   山賀 正人(CSIRT研究家)


NRI
未来創発
Dream up the future.