

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つ工夫

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

2.設定の見直し・堅牢化

3.送信ドメイン認証の活用

4.添付ファイル拡張子規制

5.セキュリティアウェアネス

6.おわりに

1.はじめに

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пам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

1.はじめに

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

システムの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

1.はじめに

端末セキュリティの理想と現実

理想

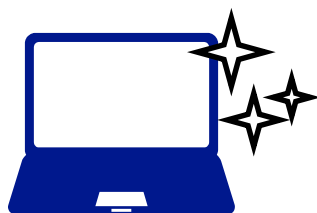
アドオン **最新**

ブラウザ **最新** Office製品 **最新**

エンドポイントセキュリティ製品 **堅牢**

OS

最新



現実

アドオン **脆弱**

ブラウザ **脆弱** Office製品 **脆弱**

エンドポイントセキュリティ製品 **脆弱**

OS

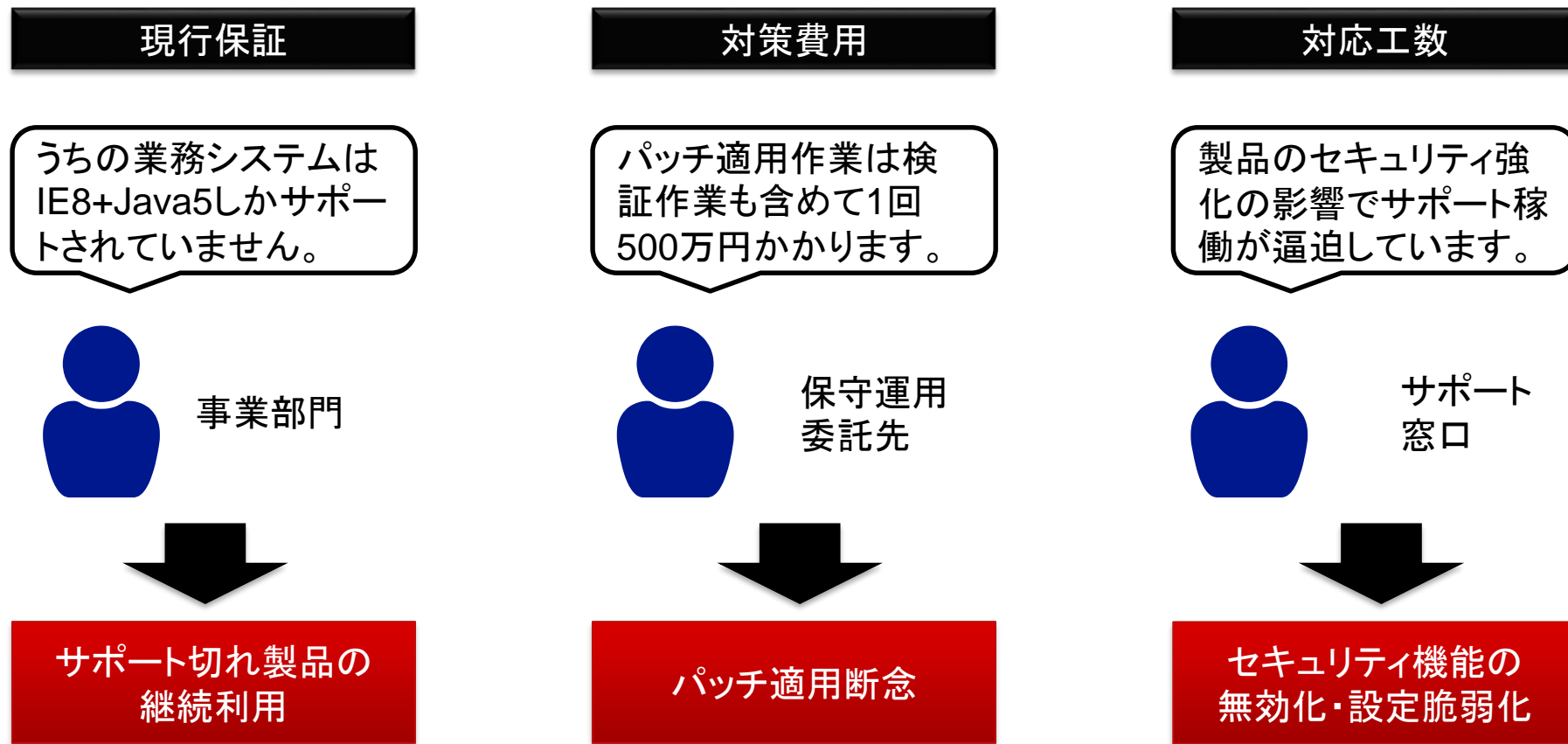
脆弱



脆弱な状態を取り繕いながら運用している組織は多い

1.はじめに

システム担当者のジレンマ



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つ工夫

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rend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します

- 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 Awareness

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



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

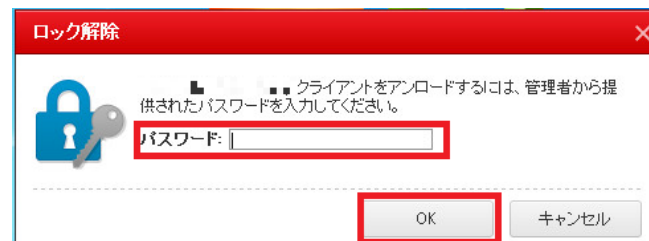
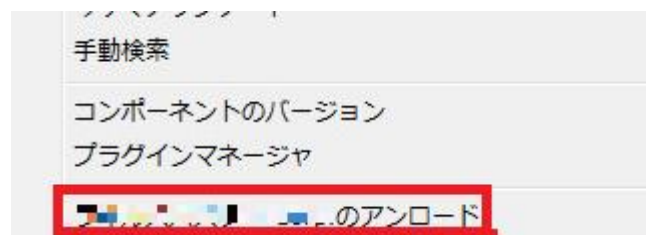
[引用元]

<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>

製品の無効化操作の例



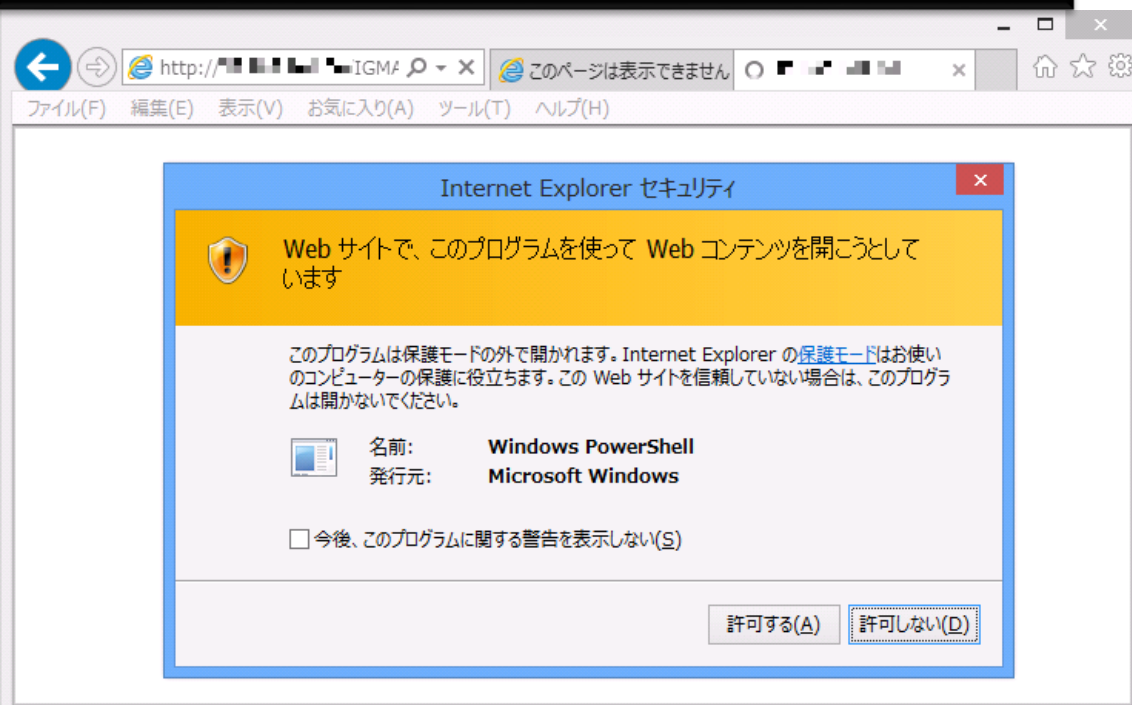
製品によっては、一律禁止とするほかにパスワードによる保護などの対策もある

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

2.設定の見直し・堅牢化

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

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

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

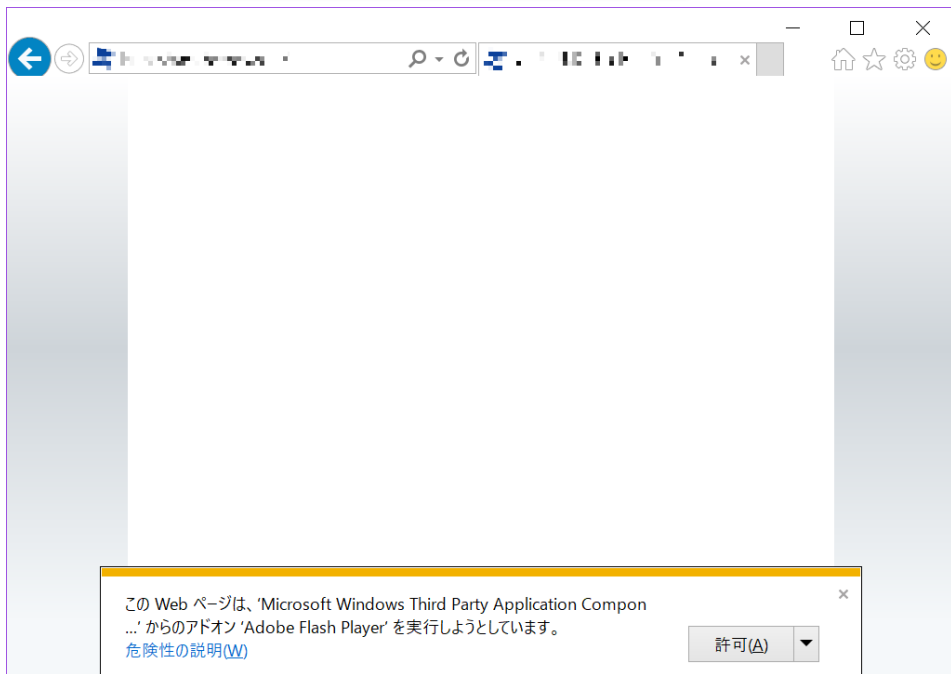
攻撃の一環で管理者権限を必要とする動作を試行した際に処理を停止させ警告を表示する

2.設定の見直し・堅牢化

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

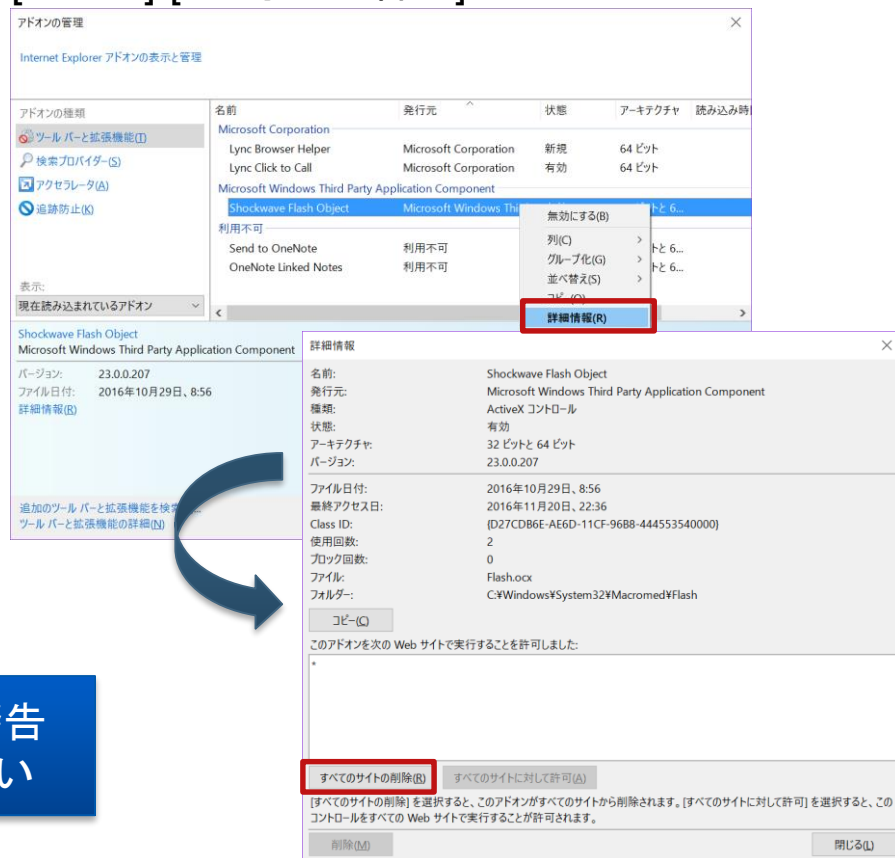
アドオンの自動実行を抑止された例



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

設定方法

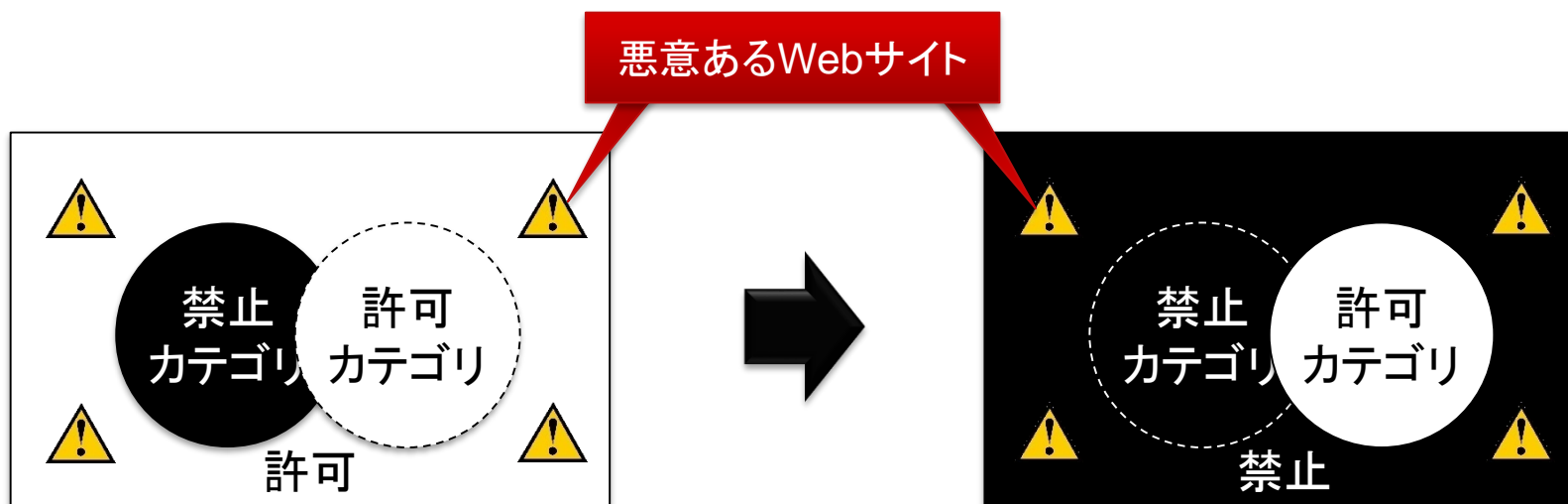
[ツール]-[アドオンの管理]



2.設定の見直し・堅牢化

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

□□□□



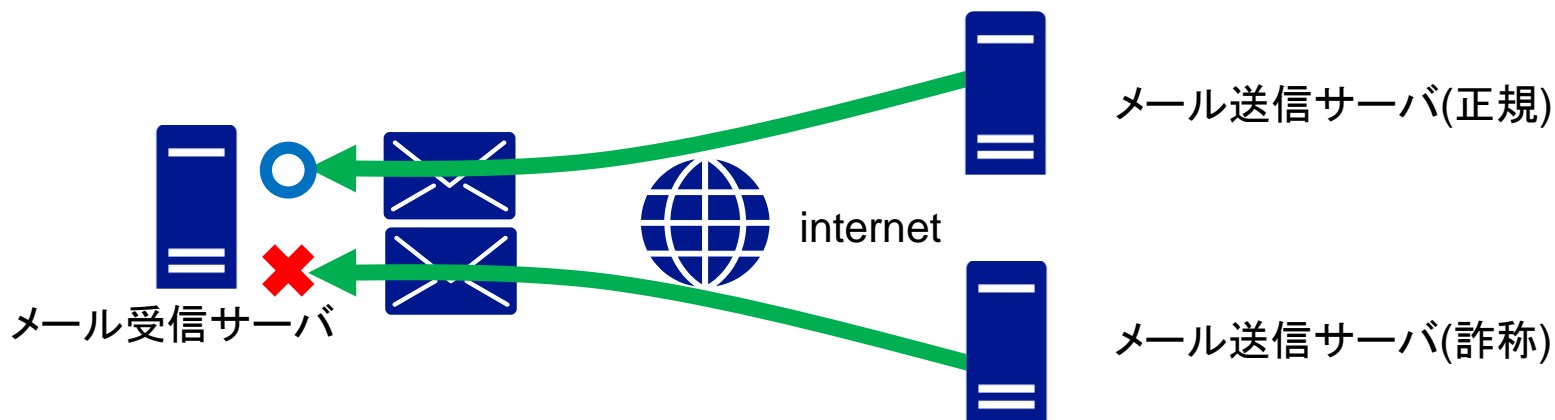
旅程表.zip

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

3.送信ドメイン認証の活用

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%**と高い普及率を保持しており、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

3.送信ドメイン認証の活用

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

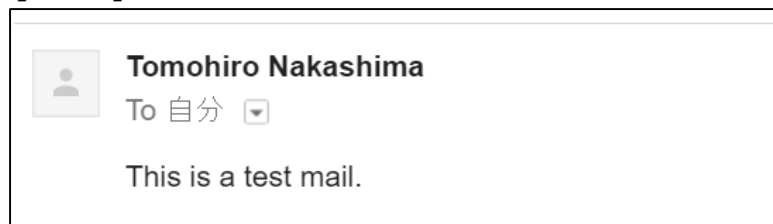
警告文言の付与

Web UIでの注意喚起(Gmailの事例)



「？」アイコンで警告

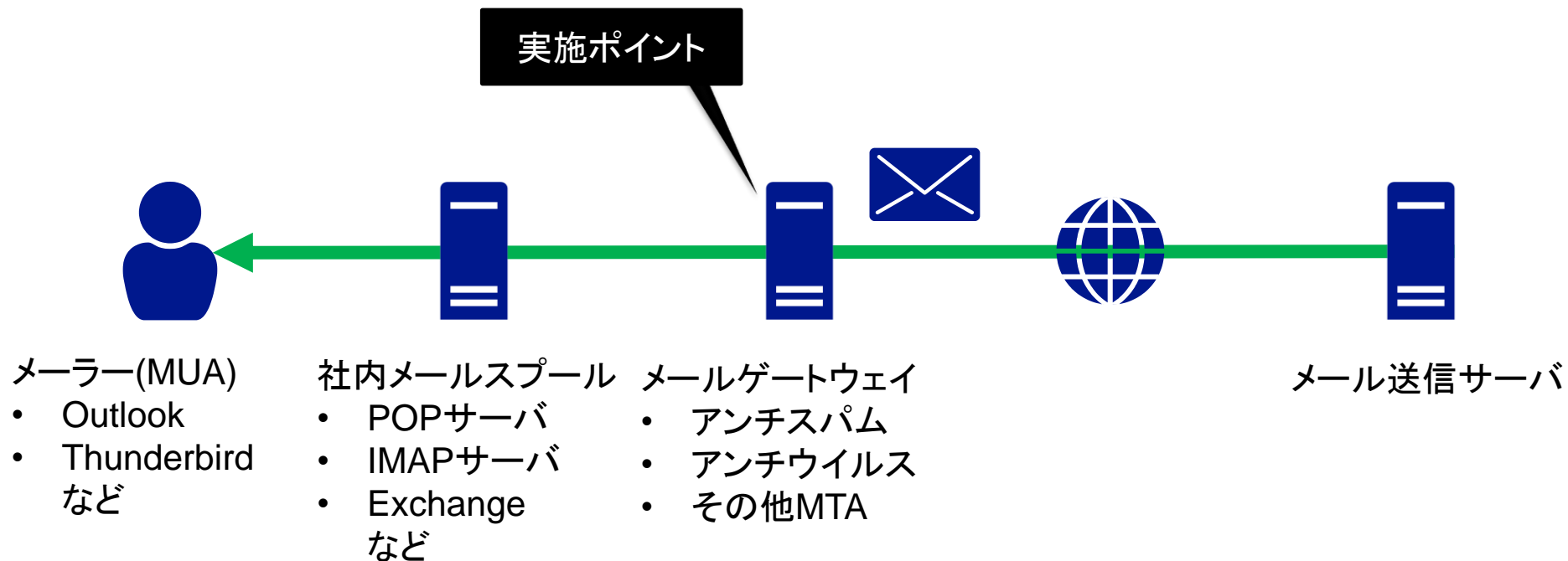
[参考]通常の表示



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

3.送信ドメイン認証の活用

送信ドメイン認証の実装箇所



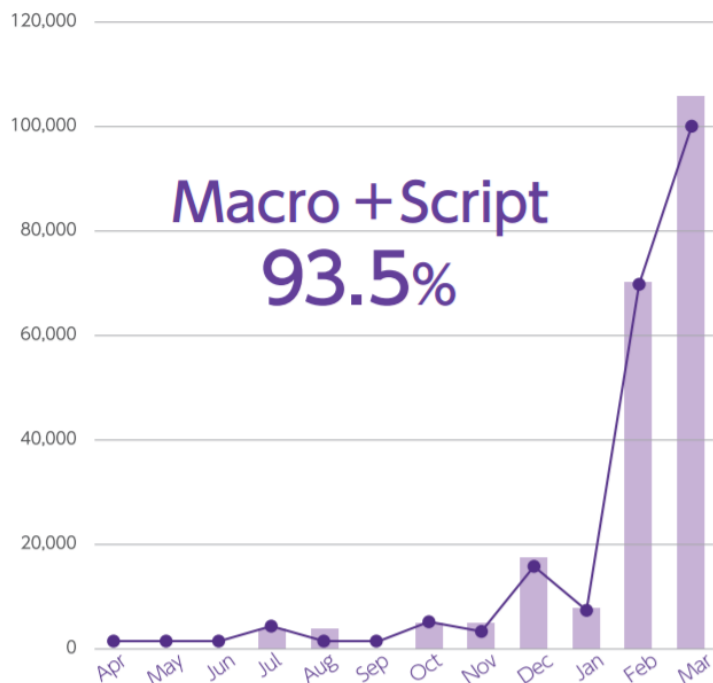
普及率の高いSPFでは送信元IPアドレスの識別が可能な箇所で実施する必要がある

4.添付ファイル拡張子規制

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)

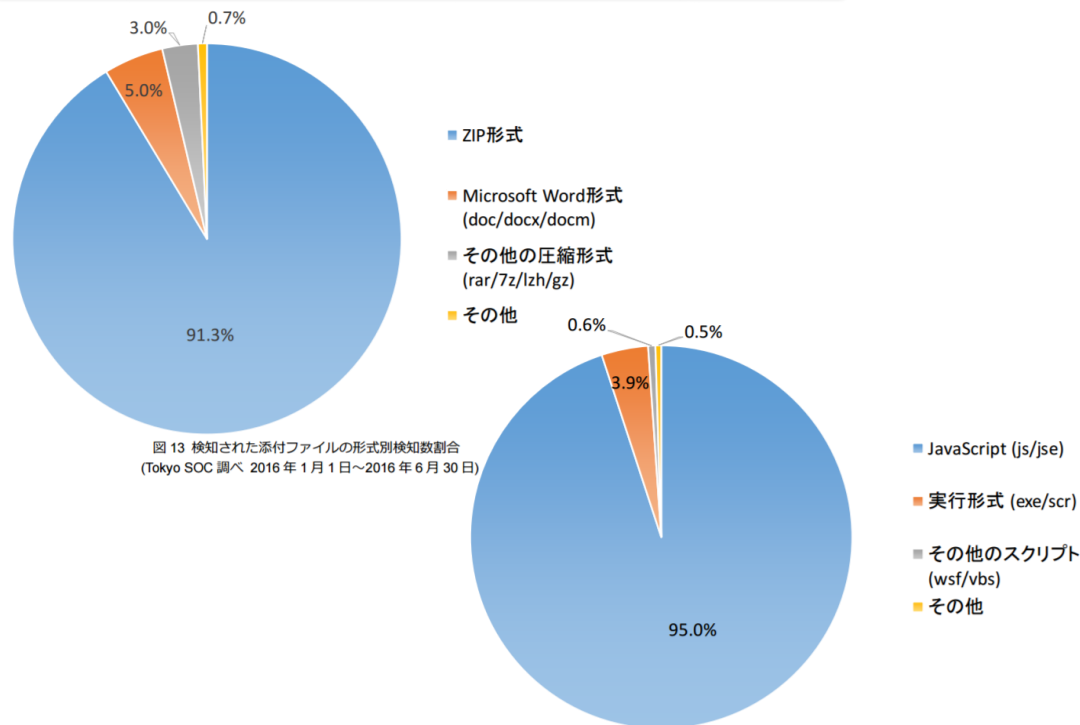


[引用元]

<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

IBM Tokyo SOC殿統計(2016年上半期)



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

4.添付ファイル拡張子規制

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>

File name extension	File type
.ade	Access Project Extension (Microsoft)
.adp	Access Project (Microsoft)
.app	Executable Application
.asp	Active Server Page

[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



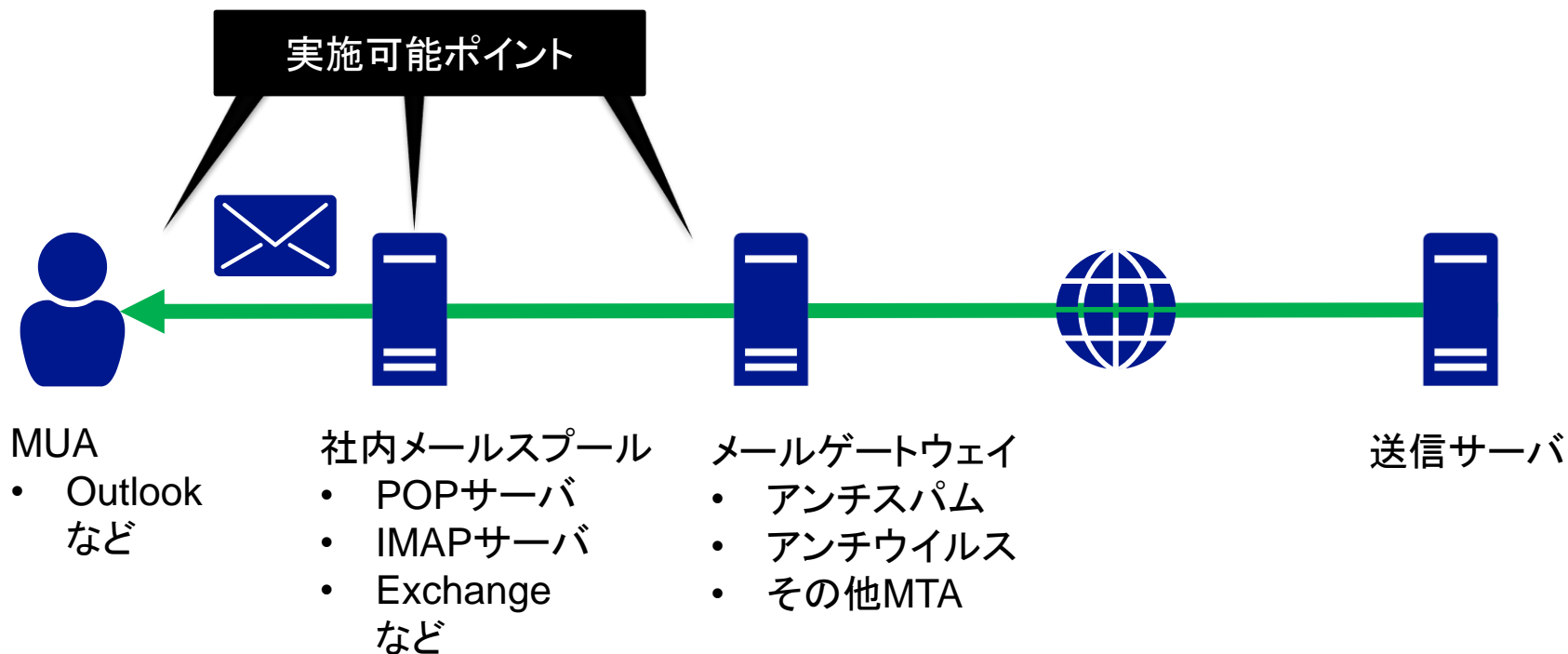
自社の業務を踏まえて必要なもののみを定義
<リストの例>

.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

4.添付ファイル拡張子規制

拡張子規制の実装箇所



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

4.添付ファイル拡張子規制

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

受信者通知の例(メール本文冒頭に通知付与)

差出人: ご不在連絡eメール <mail@... > 宛先: ...
件名: 宅急便お届けのお知らせ 日時: Tue, 13 Sep 2016 05:38:56 +0900

セキュリティ上の理由により添付ファイルを削除しました。
必要に応じてクリプト便を利用しての再送を送信者にご依頼ください。
削除されたファイル名 : 20160913049254027.zip
#####

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

4.添付ファイル拡張子規制

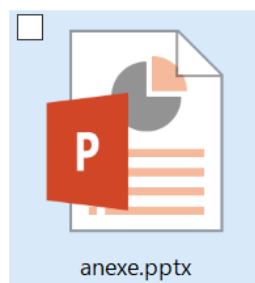
拡張子規制の考慮点②

■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

> PC > Windows (C:) > workdir



```
c:¥workdir>dir /b  
anexe.pptx  
an xtpx.exe
```

RLO(Right-to-Left Override)を悪用し見た目を偽装したものの
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пам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

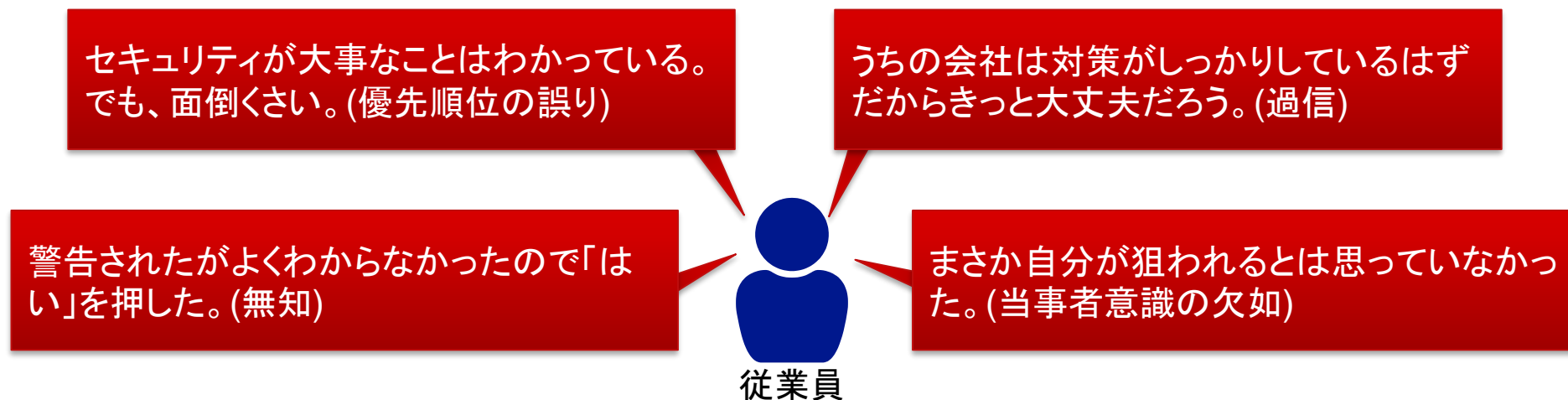
- アウェアネス(気づき)

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



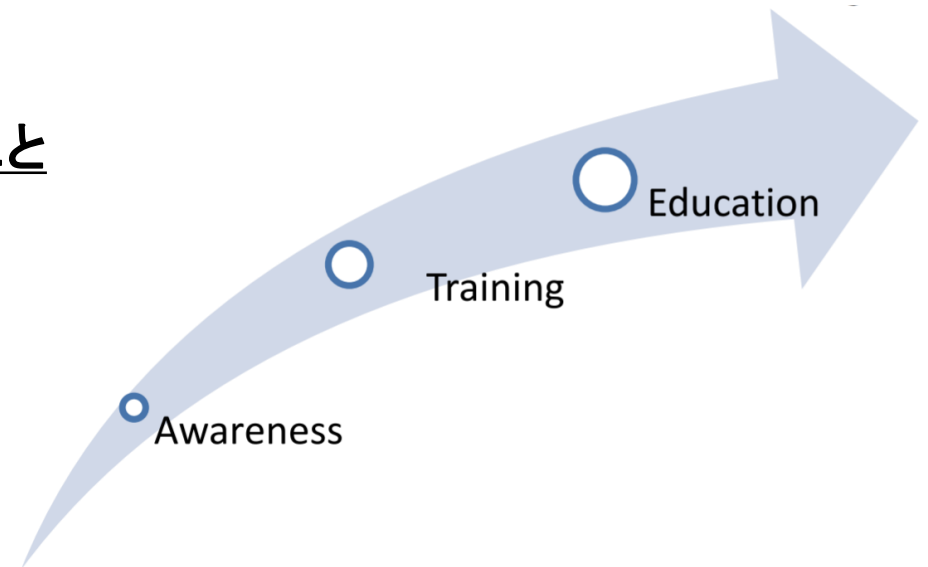
システムの対策を推し進めても、ヒトの意識が脆弱なままでは多層防衛たりえない

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

5.セキュリティウェアネス ウェアネスとは

「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>

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

システムの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

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

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

実施回数に応じた課金
が一般的



ASP/SaaS活用

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

自社向けのカスタマイズは自前で必要

一般に契約期間内は
何度でも実施可能



オープンソース活用

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

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

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

5.セキュリティウェアネス

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

New Template

Name: TEST

Subject: ウェブメールのパスワード再設定のお願い

Text HTML

[[LastName]]様
XXX株式会社です。お世話になっております。
記録によりますと、ご利用いただいているウェブメール関係で漏洩した可能性があります。つきましては、
ご確認のほどよろしくお願い致します。
[[From]]

Add Tracking Image

New Campaign

Name: TEST3

Email Template: TEST

Landing Page: TEST

URL: http://192.168.1.3/

Sending Profile: TEST

Groups: TEST

Show 10 entries

Group Name

TEST

Showing 1 to 1 of 1 entries

Results for TEST3

Overview

Campaign Timeline

Email Status

Targets Map

Details

Show 10 entries

First Name	Last Name	Email	Position	Status
太郎	テスト			Success
花子	テスト			Email Sent

[参考] セキュリティウェアネスのロードマップ

SANS SECURING THE HUMAN

Security Awareness Roadmap

Just like computers, people store, process, and transfer information. However, very little has been done to secure this "human" operating system, or HumanOS. As a result, people rather than technology are now the primary attack vector. Security awareness training is one of the most effective ways to address this problem. This roadmap is designed to help your organization build, maintain and measure a high-impact security awareness program that reduces risk by changing people's behavior and also meets your legal, compliance, and audit requirements. To use this roadmap, first identify the maturity level of your security awareness program and where you want to take it. Then follow the detailed steps to get there.

1 No Awareness Program

Program does not exist. Employees have no idea that they are a target, do not know or understand organizational security policies, and easily fall victim to cyber or human-based attacks.

How To Get There:

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards, which will likely require coordination with compliance or audit officer.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training, and when.

Deliverables:

- Annual training materials such as videos, newsletters and on-site presentations.
- Reports of who has and who has not completed required training.

2 Compliance Focused

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis. Employees are unsure of organizational policies, their role in protecting their organization's information assets, and how to prevent, identify, or report a security incident.

How To Get There:

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards, which will likely require coordination with compliance or audit officer.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training, and when.

Deliverables:

- Annual training materials such as videos, newsletters and on-site presentations.
- Reports of who has and who has not completed required training.

3 Promotes Awareness & Change

Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

How To Get There:

- Begin by identifying stakeholders in your organization. These are the individuals who are key to making your program a success. Once identified, build and execute a plan to gain their support. Methods to gain support include a human risk survey, awareness assessments, root cause analysis of recent incidents, industry reports or cost-benefit analysis.
- Create a baseline of your organization's security awareness level, such as with a human risk survey or phishing assessment. For additional examples refer to the Metrics section.
- Create a Project Charter that gives you authorization to begin the planning process. The Project Charter should set key expectations including identifying the project manager, cost estimates, program scope, goals, milestones, and assumptions.
- Have management review the Project Charter. Once it is approved, planning can officially begin.
- Establish a Steering Committee to assist in planning, executing, and maintaining the awareness program. Steering Committee should include 5-10 volunteer advisors from different departments or business units within your organization.
- Identify WHO you will be targeting in your program. Different roles may require different or additional training, including employees, help desk, IT staff, developers, and senior leadership.
- Identify WHAT you will communicate to the different groups targeted by your program. The goal is to create the shortest training possible that has the greatest impact. Begin with a risk analysis to identify the different human-based risks to your organization, document those risks in a matrix, and then prioritize the risks from high to low. Then select which risks you will address in your program based on priority level, time restrictions and other organizational requirements. Create a separate Learning Objectives document for each topic that identifies the different behaviors you need to change.
- Once you have determined WHO is the target of your awareness program and WHAT you will teach them, determine HOW you will communicate that content. To create an engaging program focus on how people will benefit from the training, how most of the lessons apply to their personal lives. There are two categories of training: Primary and Reinforcement. Primary training teaches new content and is usually taught annually or semi-annually and either onsite or online. Reinforcement training is employed throughout the rest of the year to reinforce key topics. Common examples of reinforcement training include newsletters, posters, podcasts, assessments and blogs. When teaching a specific topic, refer to that topic's Learning Objectives document to determine what content to communicate. This way regardless of the different ways you communicate a topic, the message will always be consistent.
- Create an execution plan in coordination with your Steering Committee. The plan should begin with WHY you are launching a security awareness program and its goals and overall scope. Then document WHO you will target in your awareness program. WHAT you will teach them and HOW. Include a timeline that identifies key milestones and the launch date of the program, critical resources involved and any other relevant information your organization may require for planning purposes.
- Have management review the plan. Once the plan is approved, you can execute your awareness program. Have the most senior stakeholder (such as your CEO) announce the program to the organization, such as by email, blog posting, or taped video.

Deliverables:

- Stakeholder matrix
- Gaining stakeholder support presentation
- Human risk survey
- Project Charter
- Steering Committee matrix
- Topics matrix
- Learning objectives document for each topic
- Execution plan

4 Long-Term Sustainment

Program has processes and resources in place for a long-term life cycle, including at a minimum an annual review and update of both training content and communication methods. As a result, the program is an established part of the organization's culture and is current and engaging.

How To Get There:

- Identify when you will review your awareness program each year.
- Identify new or changing technologies, threats, business requirements, or compliance standards that should be included in your annual update.
- Conduct an assessment of your organization's security awareness level and compare that to the baseline taken in stage 3.
- Survey staff for feedback, including what elements they liked best about the program, what needs to be changed, which topic they found most interesting, and which behaviors they changed.
- Review all the topics you are communicating and identify if new topics need to be added, and which existing topics should be removed or updated.
- Once topic changes have been identified, review and update the learning objectives for each topic.
- Review how the topics are communicated, which methods have had the greatest impact, and which need to be updated or dropped.
- Conduct an annual review and update of the budget to address changing business objectives.

Deliverables:

- Content tracking matrix used to document which topics and learning objectives were updated, by whom, and when.

5 Metrics Framework

Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. In addition, some set of metrics will be used in previous stages.

How To Get There:

- Identify key metrics that relate to business outcomes.
- Document how and when you intend to measure the metrics.
- Identify who is responsible to collect, when, and how.
- Execute metrics measurement.

Deliverables:

- Metrics matrix

Examples of Metrics:

- No. of people who fall victim to monthly phishing assessments.
- No. of monthly infected systems.
- No. of monthly incidents reported.
- No. of people who completed the awareness training.
- No. of weak or shared passwords.
- Employee scores from before/after testing.
- % of users sampled with positive attitude towards information security.
- % of users sampled who believe their actions can have an impact on security.

Additional Materials:

- NIST SP800-50
- Building an Information Technology Security Awareness and Training Program
- ENISA Awareness Guide (2010)
- How to Raise Information Security Awareness
- 20 Critical Controls
- Twenty Critical Security Controls for Effective Cyber Defense

Standards Requiring Awareness Training

- ISO/IEC 27002 §8.2.2
- PCI DSS §12.6
- SOX §404(a), (a), (1)
- GLBA §6601 (b), (1), (3)
- FISMA §3544 (b) (4) (A), (B)
- HIPAA §164.308 (a), (5) (i)
- NERC §CIP-004-3(B)(R1)
- EU Data Protection Directive

About the Poster

This roadmap was developed as a consensus project by security professionals actively involved in security awareness programs. If you have any suggestions or would like to get involved please contact community@securingthehuman.org

Contributors Include: Randy Marchany (Virginia Tech), Courtney Stephens (Union Gas), Julie Sobel (Alliance Data), Tonia Dudley (Honeywell), John Andrew (Honeywell), Pieter Danheux (BAE Systems Dallas), Vivian Gernand (Corning), Christopher Ipsen (State of Nevada), Jenn Lesser (Facebook), Mark Merkow (PayPal), Sam Segran (Texas Tech University), Tracy Grung (Arizona State University), Geordie Stewart (Risk Intelligence), Greg Aurigemma (Flight Safety), Janet Roberts (Progressive Insurance), Chris Sorenson (GE Capital), Mary Napheon (Lincoln Financial Group), David Vaughn (HP Enterprise Services), Tim Harwood (BP), Tanja Craig (BP), Dave Piscitello (CANN), Eric Phifer (Seacoast National Bank), Antonio Merola.

Documents followed by this icon may be downloaded at: www.securingthehuman.org/resources/planning

[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.