IIJ Technical Week 2016 – Day 3
(2016/11/11)

Windowsにおけるマルウェアの痕跡確認と防護手法のご紹介

wizSafe
安全をあたりまえに

株式会社インターネットイニシアティブ
セキュリティ本部 セキュリティビジネス推進部
セキュリティオペレーションセンター アナリスト
六田 佳祐

Ongoing Innovation

IIJ
Internet Initiative Japan

© 2016 Internet Initiative Japan Inc.

本日の内容

wizSafe

1. はじめに
   本セッションの概要をお話しします

2. 攻撃の例
   どのようにしてマルウェア感染が発生するか、お話しします

3. マルウェアの痕跡確認
   実行されたマルウェアが端末上に残す記録を確認する方法をお話しします

4. 防護手法の例
   感染が発生し辛くなるよう、護る方法をお話しします

5. まとめ

© 2016 Internet Initiative Japan Inc.

1. はじめに

© 2016 Internet Initiative Japan Inc.

自己紹介

wizSafe

- 名前
  - 六田 佳祐 （むだ けいすけ）
- 所属
  - セキュリティ本部 セキュリティビジネス推進部
    セキュリティオペレーションセンター
    - **IIJ C-SOCサービス**はじめます
- アナリスト
  - セキュリティデバイスが検知したイベントの真偽確認・通知
  - セキュリティ関係のトレンド調査

© 2016 Internet Initiative Japan Inc.

IIJ C-SOCサービス

wizSafe

- 10月31日発表、2017年3月提供開始
  - IIJ運用機器・お客様運用機器から送信されるログを収集・分析
  - 機器単体のセキュリティログでは検知出来ない、セキュリティインシデントを検知
  - アナリストがインシデントの重大度を判断し、適切な通知や対処を実施
  - レピュテーションデータや独自シグネチャを適用し、脅威からの迅速な防御を実施

- セキュリティオペレーションセンター
  - 2017年3月 見学ツアー開始予定

- 詳しくは担当営業へお問い合わせ頂くか、IIJ Webサイトをご覧ください
  - http://www.iij.ad.jp/wizsafe/

© 2016 Internet Initiative Japan Inc.

IIJとマルウェア調査

wizSafe

- IIJには、お客様から検体をお預かりして調査するサービスは、現時点ではご提供しておりません

- 一方で、観測情報やサービスに関連する情報から、マルウェアを調査することはあります
  - 調査の結果は、IIJサービスにフィードバックされることがあります
  - 調査で見つかった事象は、一般公開することがあります
    - Internet Infrastructure Review (IIR)
      http://www.iij.ad.jp/company/development/report/iir/
    - IIJ-SECT
      https://sect.iij.ad.jp/

- このセッションでは、感染時における調査に役立つ設定をいくつか紹介すると共に、感染する確率を下げる手法を紹介します

© 2016 Internet Initiative Japan Inc.

注意事項

- セキュリティに「絶対」はありません
  - 本セッションの内容を実施したからと言って、マルウェアに感染しなくなったり、確実に証拠を保全出来るものではありません

- 本セッションの内容は、2016年11月11日時点のものです
  - トレンドは常時変化します
  - 最新の情報を追いかけるように心掛けてください

- 本セッションは、Windows 10 Pro環境（x86/x86-64）を想定しています
  - バージョンやエディションが異なると、一部設定方法が異なる場合があります
    - Windows 10（無印）では、グループポリシーが使用出来ません
  - Linux、Unix、Mac OS、他スマートデバイス（Windows 10 Mobile・IoTを含む）
    などは、本セッションでは触れません
    - 同様の機能が存在する項目もありますので、探してみてください

© 2016 Internet Initiative Japan Inc.

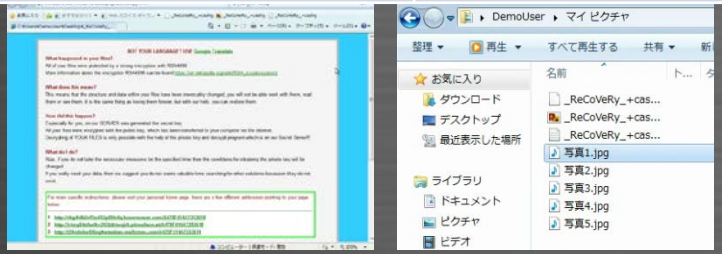
2. 攻撃の例

© 2016 Internet Initiative Japan Inc.

マルウェア

- コンピュータ上で動作する不正（malicious）なソフトウェア
- 最近の攻撃・マルウェア例

挙動	事例	ツール例
特定のタイミングに、特定のサイトに対して大量のトラフィックを送信	米セキュリティ情報サイトに対する、1TbpsのDDoS攻撃 (2016/9)	Mirai（bot）
特定のホストを踏み台とし、他のホストに通信させる	JTB社の情報流出 (2016/5)	PlugX（RAT: Remote Access Tool）
ファイルを開けないようにし、金銭を要求する	米ロサンゼルスの病院における、電子カルテなどの暗号化 (2016/2)	Locky（ランサムウェア）

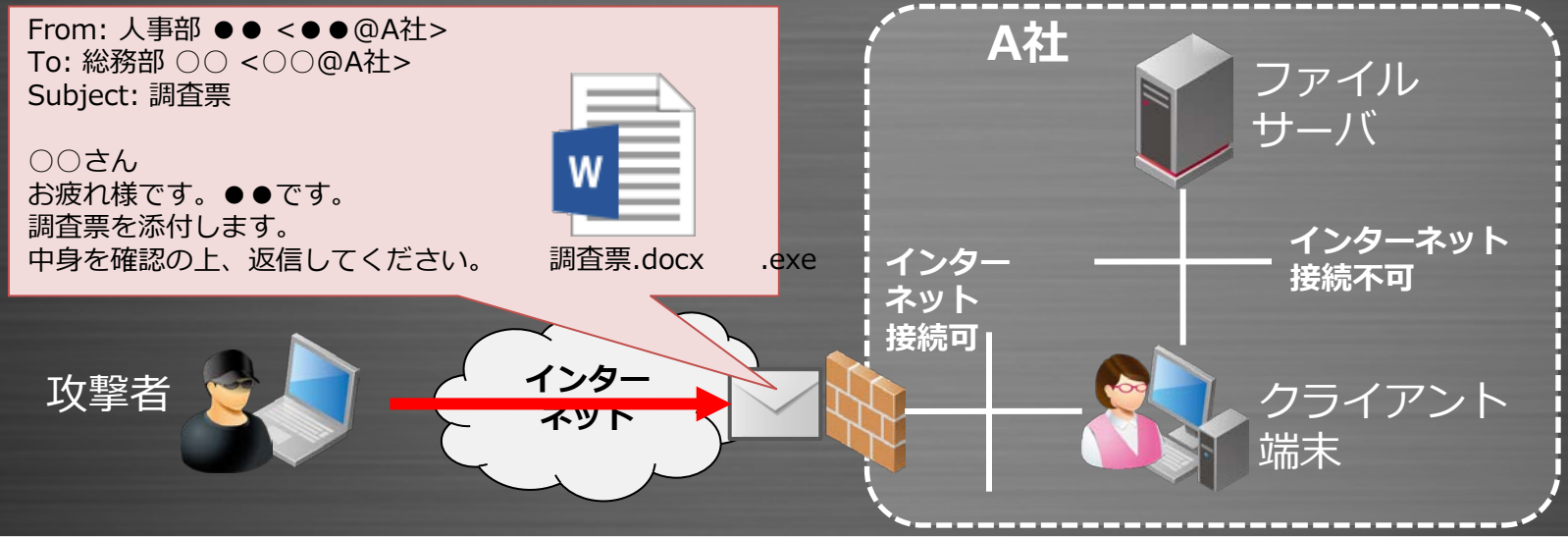


← TeslaCrypt（ランサムウェア）の感染例

© 2016 Internet Initiative Japan Inc.

標的型攻撃

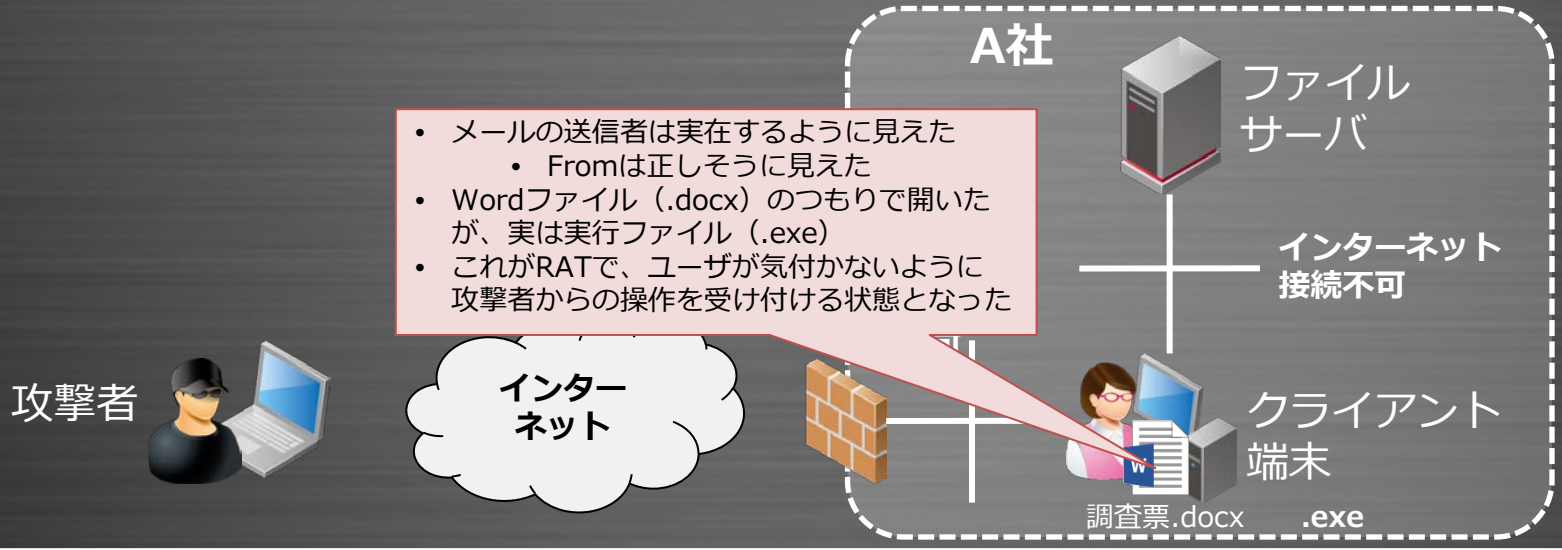
- 前項に記載の、RATを使用した例
  - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
  - それを開いたクライアント端末が感染し、RATが実行される
  - RAT経由で端末を操作し、他のホスト上にある情報を奪取する



© 2016 Internet Initiative Japan Inc.

標的型攻撃

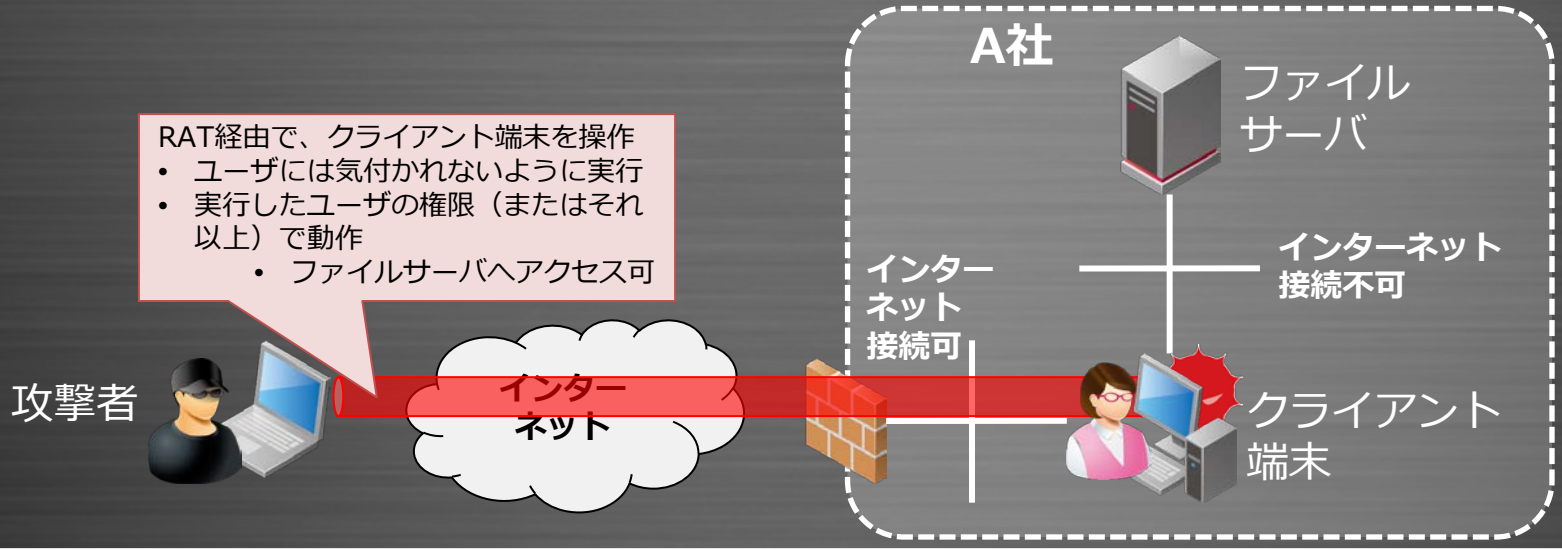
- 前項に記載の、RATを使用した例
  - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
  - それを開いたクライアント端末が感染し、RATが実行される
  - RAT経由で端末を操作し、他のホスト上にある情報を奪取する



© 2016 Internet Initiative Japan Inc.

標的型攻撃

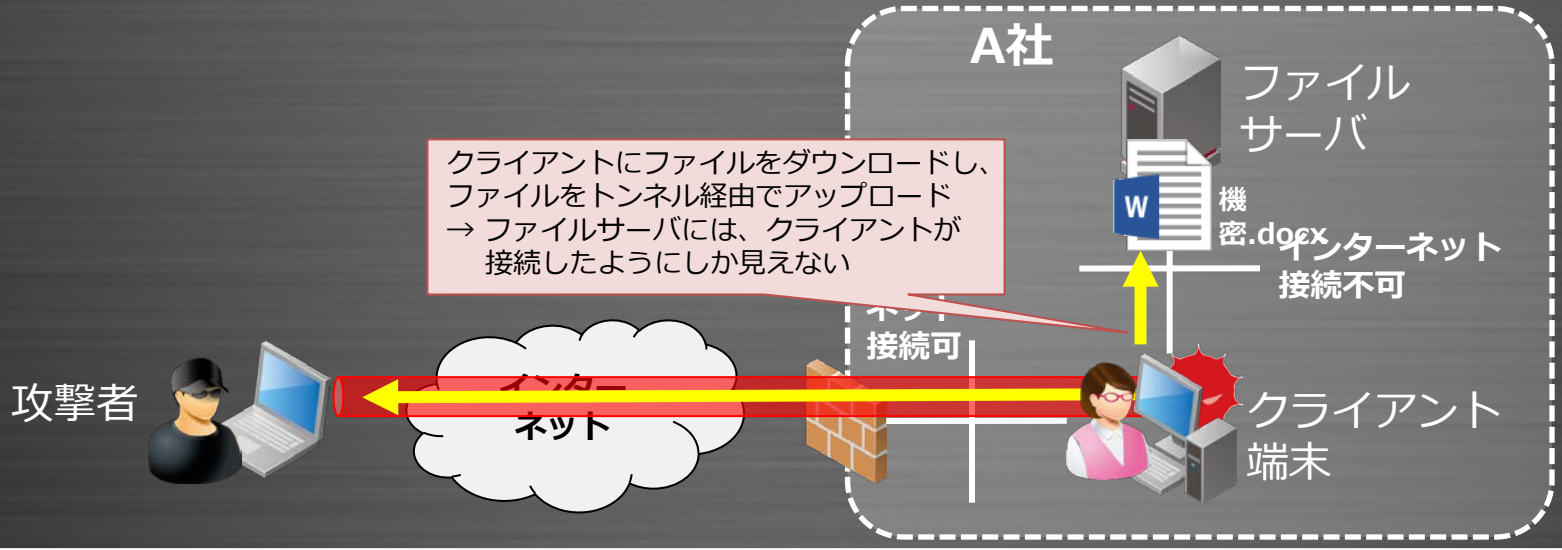
- 前項に記載の、RATを使用した例
  - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
  - それを開いたクライアント端末が感染し、RATが実行される
  - RAT経由で端末を操作し、他のホスト上にある情報を奪取する



© 2016 Internet Initiative Japan Inc.

標的型攻撃

- 前項に記載の、RATを使用した例
  - 組織内のユーザに、正しく見えるような添付ファイル付きメールを送信する
  - それを開いたクライアント端末が感染し、RATが実行される
  - RAT経由で端末を操作し、他のホスト上にある情報を奪取する

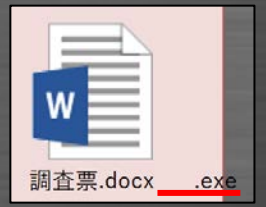


© 2016 Internet Initiative Japan Inc.

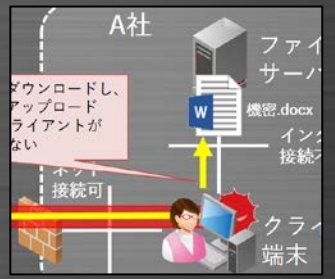
攻撃のポイント

- 送信者が**正しく見えた**
  - メールの送信元（From）アドレスは、簡単に**偽装が可能**
  - 本文も**本物のよう**に見えた
    - 片言の日本語ではなく、社内メールに見える

- 添付ファイルも一見すると、**正しいファイルに見える**
  - 実は見え辛い位置に本当の拡張子があった



- ファイルサーバにアクセスしたのは、社内の**正規アカウント**
  - 攻撃者の存在は、ファイルサーバ側には見えない
  - ファイルサーバのアクセスログがあっても、「日時」「ファイル」「端末」は割り出せるが、具体的な攻撃元は分からない



© 2016 Internet Initiative Japan Inc.

対策？

- ウイルス対策ソフト
- パーソナルファイアウォール
- ソフトウェアの更新

- いずれも、現在でも一定の効果がある

- しかし・・・

© 2016 Internet Initiative Japan Inc.

証跡の取得

wizSafe

- 残念ながら、マルウェアに**絶対に**感染しない、ということはあり得ない
  - ウイルスの亜種
    - 挙動やシグネチャが異なり、パターンファイルでは検出不可
    - ヒューリスティック機能で検知出来る場合もあるが、完全ではない
  - ファイアウォールとしては正常に見える通信： ポリシ上は通信を許可
    - 443/tcp（HTTPS）を用いたトンネル通信
    - 53/udp（DNS）を用いたリモート制御
  - 未発見の脆弱性

- 感染した場合に、「何が起こったのか」を把握出来るようにしたい
  - 影響範囲を知り、**復旧作業の内容を策定**
  - 関係者への説明時に、**経緯や影響を明確に説明**
  - **同様の事象が発生しないように対策**

© 2016 Internet Initiative Japan Inc.

3. マルウェアの痕跡確認

© 2016 Internet Initiative Japan Inc.

実行の痕跡

wizSafe

- マルウェアに限らず、アプリケーションを実行すると**痕跡**が残る
  - アクセスログ
    - ファイル
    - レジストリ
    - ネットワーク
  - 実行ログ
  - etc...

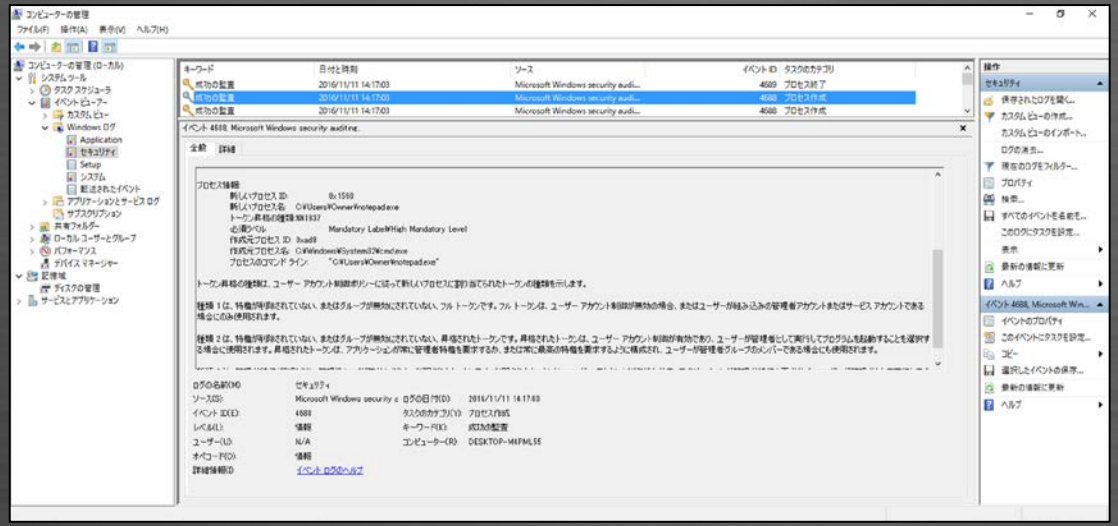
- Windowsの標準機能でも、ある程度は確認可能
  - しかし、初期設定のままでは確認出来ないことが多い
    - 予め、確認出来るように設定しておくことが必要
    - 設定には、Administrator権限が必要

© 2016 Internet Initiative Japan Inc.

痕跡の取得例

- マルウェアが参照したファイル・レジストリ
- ネットワークアクセスの痕跡
- マルウェアの実行

- これらを**Windowsのイベントログ**を用いて記録する方法をご紹介
  - 殆どは追加のソフトウェアを必要とせず、設定すれば利用可能



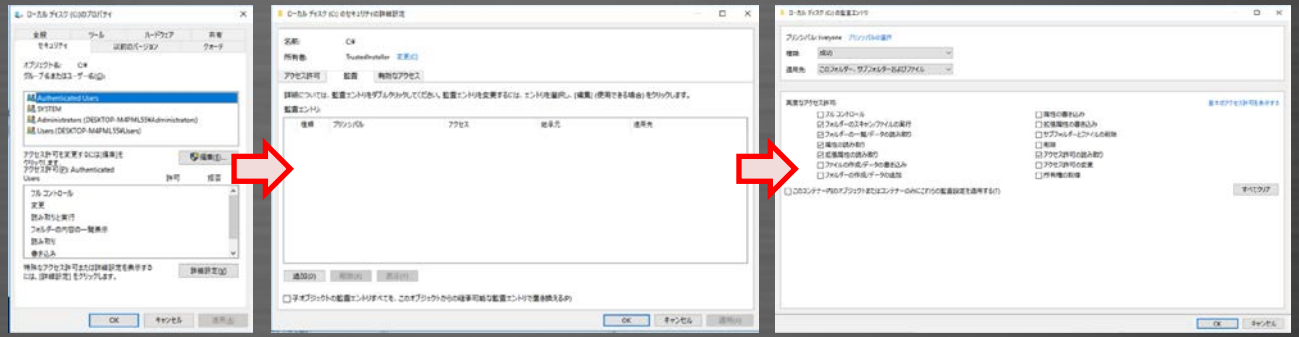
© 2016 Internet Initiative Japan Inc.

ファイルアクセスのログ

- マルウェアが参照したり、作業フォルダに書き込んだりしたファイルを記録すれば、使用されたツールや狙われた情報が分かるかもしれない

- NTFSには、ファイルアクセスに対する**監査**機能がある
  - NTFS： Windows標準で使用されているファイルシステム

- 2か所を設定する
  - ファイルのSACL
    - Everyoneに対して設定
  - 監査ポリシー

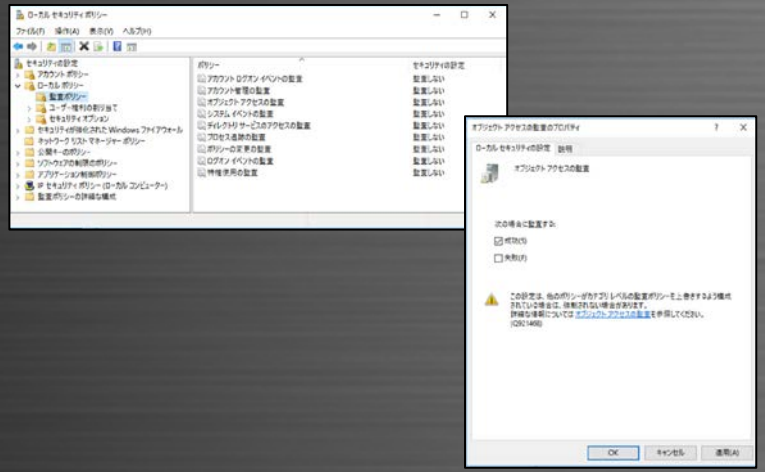


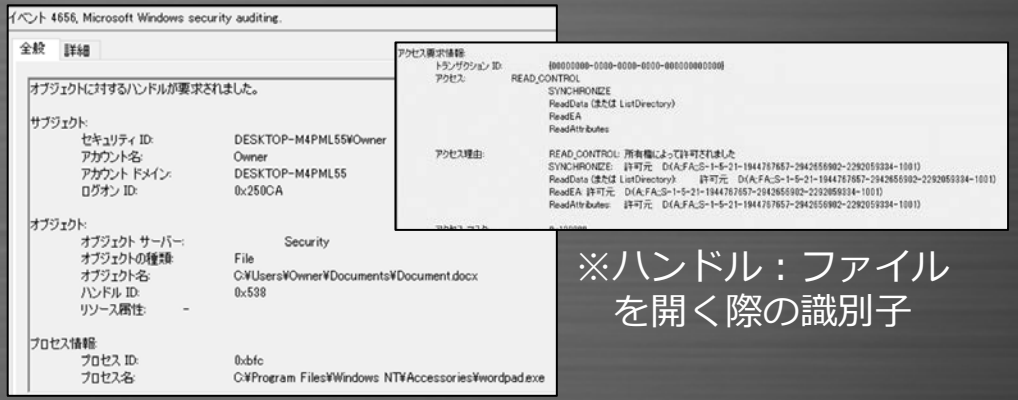
↑SACLの設定例

© 2016 Internet Initiative Japan Inc.

監査ポリシーの有効化

- SACLを有効化した状態で「オブジェクトアクセスの監査」を設定すると、イベントログの「**セキュリティ**」ログにアクセスログが記録





※ハンドル：ファイルを開く際の識別子

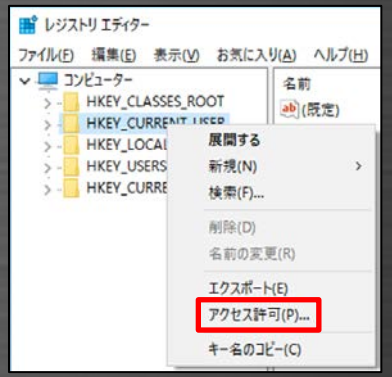
- 設定すると、他にWindowsフィルタリングプラットフォーム（Windowsファイアウォール）やファイル共有なども監査されるようになる
  - ファイルアクセスのみに絞りたい場合は、「詳細な構成」から

© 2016 Internet Initiative Japan Inc.

レジストリ

- レジストリエディタでSACLを設定し、「オブジェクトアクセスの監査」を設定することで、監査が可能
  - 詳細構成で「レジストリの監査」を設定しても良い

- レジストリのキーを右クリックし、「アクセス許可」から設定
  - **予めレジストリの構造や、作業時のリスクを理解すること**
  - ファイルアクセスと同様に、読み取りに対して設定すると、膨大な量のログが記録されるため、注意が必要



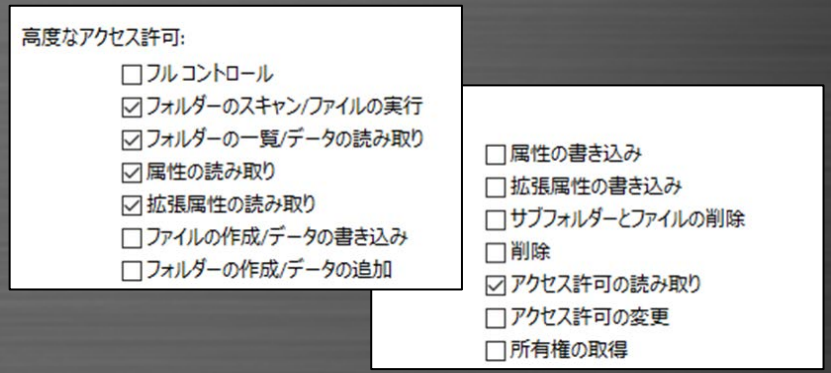
© 2016 Internet Initiative Japan Inc.

監査対象の選定

- 「**読み取り**」を監査すると、**ログ量が膨大**になる
  - アプリケーションのDLL呼び出しが監査される場合も
  - 一方で、欲しい監査ログは「読み取り」である場合も多い

- 「読み取られた」ことを知りたければ、「**成功**」を監査すれば良い
  - 一方で、全てのアクティビティを記録したい場合は、「成功および失敗」

- 「何でも取る」は**必ずしも良いとは限らない**

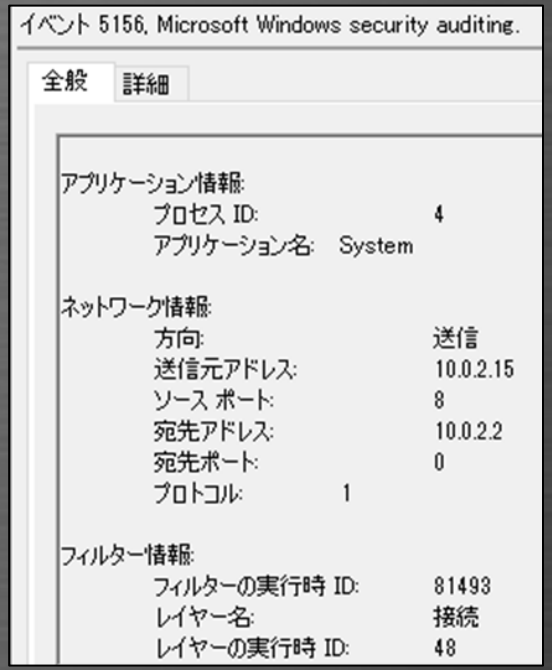


© 2016 Internet Initiative Japan Inc.

ネットワークアクセスのログ

wizSafe

- 「オブジェクトアクセスの監査」（一括設定時）又は「Windowsフィルタリングプラットフォームの監査」（詳細な構成時）を設定
  - Windowsフィルタリングプラットフォーム：Windowsファイアウォールなどで使用されている、パケットフィルタのAPI
  - Windowsフィルタリングプラットフォームを使用しない場合は効果無し
    - パーソナルファイアウォールソフトウェアのログで代替
    - 追加ユーティリティの使用（後述）



© 2016 Internet Initiative Japan Inc.

プロセスの監査

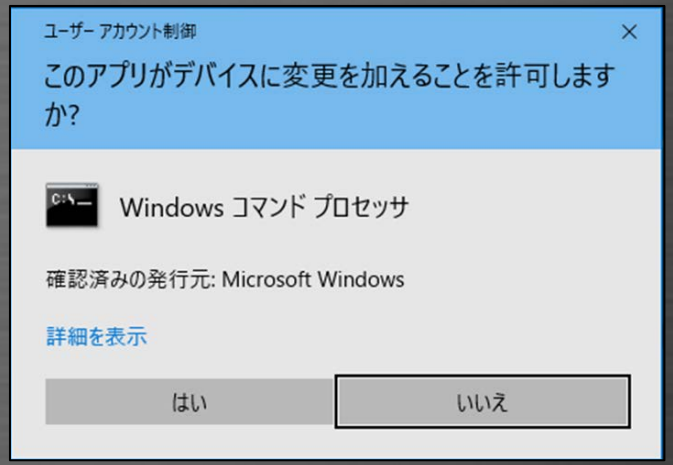
- 実行ファイル（exe）が起動・終了したことを記録
  - 通常はインストールしていない実行ファイルが起動されると、端末上で不正な処理がされた可能性がある
- 「プロセス追跡の監査」を有効化することで、イベントログに記録されるようになる

© 2016 Internet Initiative Japan Inc.

プロセス監査から分かること

- 日時
- 実行ユーザ
- プロセスID
- プロセス名
- 権限
  - UAC有効環境では、「管理者権限が必要」な場合に「昇格」する
    - トークン昇格
    - 必須ラベル
- 呼び出し元プロセス

```
新しいプロセス ID:              0xaf8
新しいプロセス名:    C:¥Windows¥System32¥notepad.exe
トークン昇格の種類:%%1938
必須ラベル:                     Mandatory Label¥Medium Mandatory Level
作成元プロセス ID:  0xa60
作成元プロセス名:    C:¥Windows¥System32¥cmd.exe
プロセスのコマンド ライン:
```



© 2016 Internet Initiative Japan Inc.

コマンドライン

wizSafe

- 単に「プロセス追跡の監査」を設定するだけでは、実行されたexeファイルと、付随情報が分かるのみ

```
C:¥Windows¥PSEXEC.EXE
```

© 2016 Internet Initiative Japan Inc.

コマンドライン

wizSafe

- 単に「プロセス追跡の監査」を設定するだけでは、実行されたexeファイルと、付随情報が分かるのみ

```
C:¥Windows¥PSEXEC.EXE
```

- 実行内容を知りたい

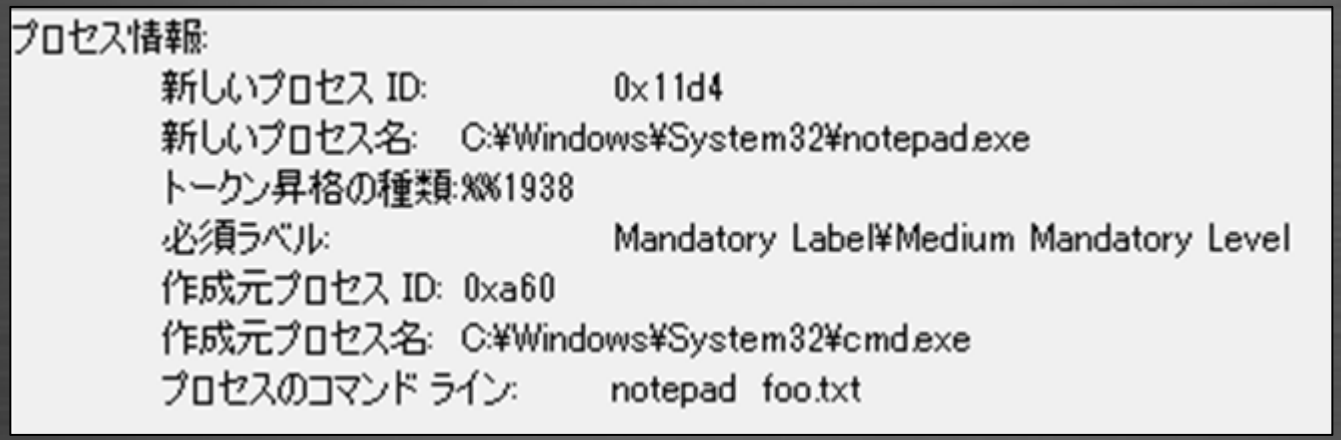
```
C:¥Windows¥PSEXEC.EXE ¥¥target_host net use ¥¥fileserver¥share
```

© 2016 Internet Initiative Japan Inc.

コマンドラインを記録

wizSafe

- グループポリシ
  - 「コンピューターの構成」→「管理用テンプレート」
    →「システム」→「プロセス作成の監査」
    →「プロセス作成イベントにコマンドラインを含める」
    - Windows 8.1・Windows Server 2012 R2以降で有効
    - KB3004375 をインストールすると、Windows 7・8、Windows Server 2008R2・2012でも設定可能



© 2016 Internet Initiative Japan Inc.

追加ツールを使う

wizSafe

- Sysmon（SYStem MONitor）
  - Windows Sysinternals
    - https://technet.microsoft.com/en-us/sysinternals/sysmon
  - Windows 7・Windows Server 2012以降で利用可能
- 記録可能な情報
  - レジストリは、Sysmonでは記録不可

イベントID	項目
1	プロセス作成
2	ファイル作成日時の変更
3	ネットワーク接続
4	Sysmonサービスの状態変更
5	プロセス終了
6	ドライバ読み込み

イベントID	項目
7	イメージ呼び出し
8	リモートスレッドの実行
9	ディスクのRAW読み出し
10	プロセスアクセス
255	Sysmonのエラー

© 2016 Internet Initiative Japan Inc.

監査ログから見つけられる事象の例（注：いずれも可能性）

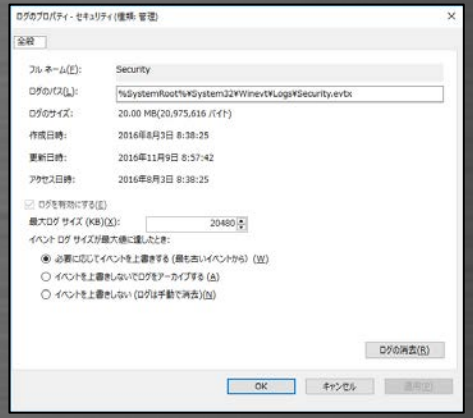
wizSafe

- ファイルサーバ上のファイルが、ローカルディスクにコピーされていた
  - 攻撃者が当該端末でファイルをまとめ、一括してアップロードする可能性
- 他端末や、インターネット上のホストへの通信が記録されていた
  - クライアント同士の通信の場合、攻撃者が他ホストにも侵入した可能性
  - インターネット上のホストである場合、それが攻撃者のホストである可能性
- インストールしていない実行ファイルが起動した
  - 攻撃に使用された実行ファイルである可能性
- 自動起動の設定
  - 何度でも侵入可能とするよう、RATを常時起動するよう設定した可能性

© 2016 Internet Initiative Japan Inc.

ログの消去

- ログ容量には上限がある
  - クライアントOSの初期設定は20MB
  - 超過すると、古い方から上書きされる



- 攻撃者はログを消去する
  - 取得する設定をしても、消去されると意味が無い

キーワード	日付と時刻	ソース	イベント...	タスクのカテゴリ
成功の監査	2016/11/07 13:11:12	Eventlog	1102	ログの消去

- ログを外部転送するなど、消去されないように対策することを推奨
  - 転送しておくと、ホスト上で消去されてもログが残る
    - 当然、ログ収集ホストの権限を奪取されないことが前提
    - 例： https://technet.microsoft.com/ja-jp/library/cc748890(v=ws.11).aspx

© 2016 Internet Initiative Japan Inc.

調査とアンチウイルスソフトウェア

wizSafe

- とりあえずウイルススキャン？
  - 感染が発見された際によく聞くフレーズ
  - 「**とにかく消去したい**」場合は有効

© 2016 Internet Initiative Japan Inc.

調査とアンチウイルスソフトウェア

wizSafe

- とりあえずウイルススキャン？
  - 感染が発見された際によく聞くフレーズ
  - 「**とにかく消去したい**」場合は有効

- 調査を目的としている場合、適切でない場合もある
  - ウイルススキャナがファイルシステムにアクセスし、「読み取り」のログで**監査ログが埋まってしまった**
  - 調査したいファイルが、**検疫により削除**されてしまった

- 調査をしたい場合、**電源は起動したままネットワークケーブルを抜く**
  - 調査する場合も、他端末に対する感染のリスクは避けるべき

- 状況に合わせて**適切に判断**すること
  - 「調査するより止めることが先決」という状況もあるかもしれない

© 2016 Internet Initiative Japan Inc.

4. 防護手法の例

© 2016 Internet Initiative Japan Inc.

よくある感染例

wizSafe

- スクリプトを実行した
- 正規アプリケーションから不正な呼び出しが発生した

- こういったものを実行しないようにすると、リスクを低減出来る

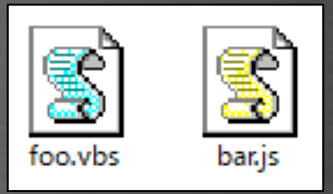
- 注意
  - 下記に示すような一般的な対策は、既に実施していることを前提とする
    - アンチウイルスの使用
    - パーソナルファイアウォールの使用
    - ソフトウェアの更新を実施
    - バックアップの取得
    - 不要アカウント・不要アプリケーションの削除

© 2016 Internet Initiative Japan Inc.

Windows Script Host

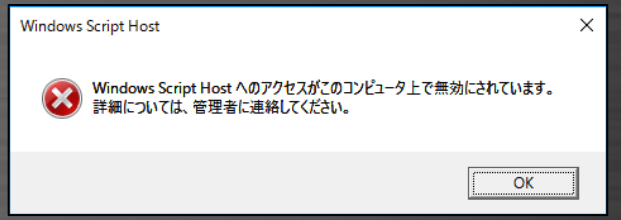
wizSafe

- Windowsで古くから使用されているスクリプティング手法
  - VBScript： Visual Basic記法
  - Jscript： JavaScript記法



- 使用しない場合は、レジストリで無効化出来る
  - コンピュータ上の全ユーザ
    - HKLM¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled
  - 現在のユーザのみ
    - HKCU¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled
  - それぞれ上記のDWORD値を作成し、”0”を設定

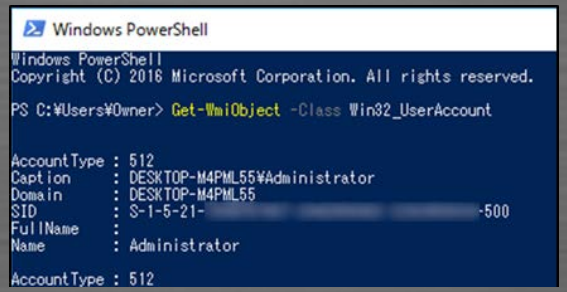
- ログオン・ログオフスクリプトで使用している場合、動かなくなるため注意



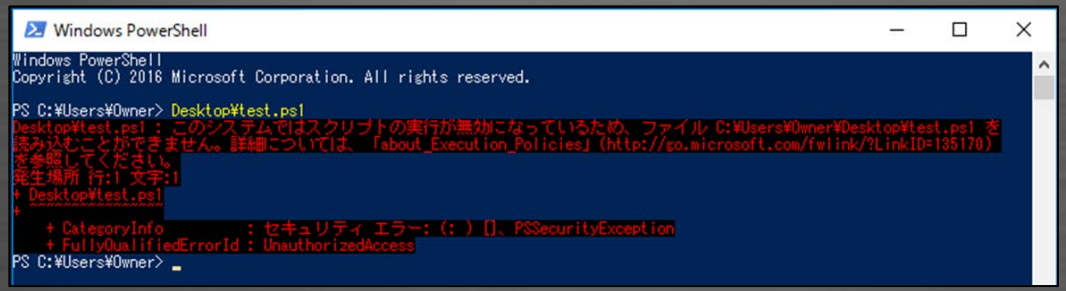
© 2016 Internet Initiative Japan Inc.

PowerShell

- 比較的新しいWindowsのコマンド操作機構
  - Windowsの様々な情報を取得・設定可能



- 初期設定では、スクリプト実行が許可されていない
  - しかし、レジストリ値を1つ変更すると実行可能



© 2016 Internet Initiative Japan Inc.

PowerShellの監査

wizSafe

- PowerShell v5では、実行したコマンドと出力の記録が可能
  - Windows Management Framework 5.0 に含まれる
    - Windows 10では標準搭載
    - Windows 8.1・7やServer 2012/R2・2008R2では個別にインストールが必要
      https://www.microsoft.com/en-us/download/details.aspx?id=50395

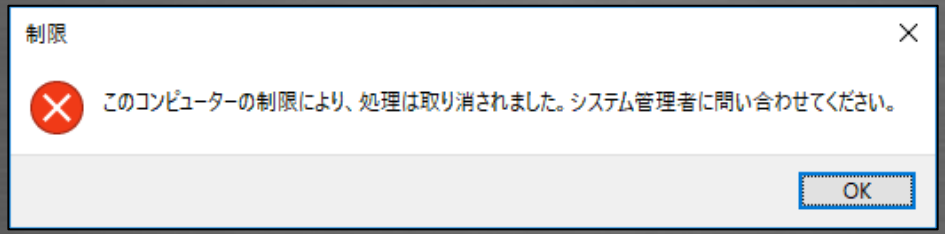
- グループポリシー
  - (コンピューター|ユーザー)の構成¥管理用テンプレート¥Windowsコンポーネント¥Windows PowerShell¥PowerShellトランスクリプションを有効にする
  - 既定では「ドキュメント」フォルダに作成される
    - 攻撃者により削除される可能性はあるが・・・

© 2016 Internet Initiative Japan Inc.

特定のexeファイルを実行しない

wizSafe

- グループポリシ
  - 「ユーザーの構成」→「管理用テンプレート」→「システム」→「指定されたWindowsアプリケーションを実行しない」
    - 実行すると、下記ダイアログが表示される



  - 「指定されたWindowsアプリケーションだけを実行する」というポリシもあるが、以下のような場合は回避が可能
    - コマンドプロンプトから実行
    - 正規のファイル名と同じ名前に変更（パスを含めた場合はこの限りではない）

© 2016 Internet Initiative Japan Inc.

攻撃を知る（管理者向け）

wizSafe

- 全ての攻撃手法を把握することは不可能だが、一定数を知っておくことは可能

- よく使用されるツールの例
  - PSEXEC（Sysinternals）
  - Windowsリモートシェル（WinRS）
  - リモートデスクトップ
    - **特徴的なログが記録される**
      - PSEXEC：**システムサービス**（PSEXESVC）**のインストール・削除**
      - WinRS： Windows Management Instrument**（WMI）の実行**
      - リモートデスクトップ： **専用のログ**が存在
    - PSEXEC・WinRSはコマンドラインオプションに実行プログラムを指定するため、コマンドラインを含めたログを取得していれば記録可能

- 上記は全て、**ツール自体は正規**のもの
  - 「**システム上で使用しているかどうか**」が判断基準の1つ

- システムの**「定常」を知っておく**ことが必要

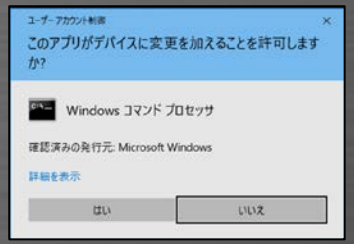
© 2016 Internet Initiative Japan Inc.

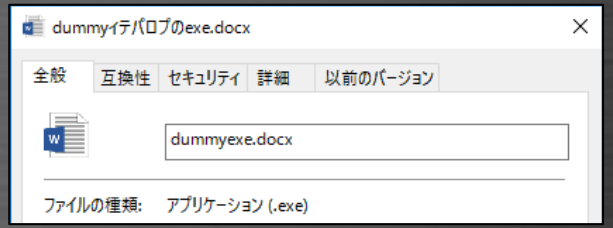
攻撃を知る（一般利用者向け）

- 機械的に制御することと併せて、ユーザにも一定の知識が必要

- 例えば・・・
  - メールのFromは**詐称可能**
    - 詐称されたことを確認する技術として、SPF・DKIM・DMARCなどの認証技術
  - UACで、**意図しない権限昇格**を許可しない
    - 手動で実行したなら意図したもののはず
    - ユーザが何も実行していないのに表示された場合、不正な処理を目的したものである可能性がある
    - 何も考えずに「はい」とは言わない
  - **アイコン・ファイル名と中身が一致するとは限らない**
    - Wordファイルのアイコンを用いた実行ファイル
    - ファイル名の偽装（RLOなど）
      - グループポリシで制限可

```
Authentication-Results: mx.example.jp; spf=fail
smtp.mailfrom=notreal@example.jp; dkim=none;
dkim-adsp=unknown header.from=notreal@example.jp;
dmarc=fail header.from=notreal@example.jp;
x-country-code=JP
```





© 2016 Internet Initiative Japan Inc.

他にも

- Internet Infrastructure Review（IIR）では、他の対策も紹介しています
  - http://www.iij.ad.jp/company/development/report/iir/

Vol.31 第1.4.2節

- アプリケーションホワイトリスティング
  - AppLocker（Enterprise向け）
  - ソフトウェアの制限ポリシー（SRP）
- 制限回避の脆弱性
- WinSxSフォルダ
- 管理者権限の制限

Vol.32 第1.4.2節

- EMET
- UACの厳格化
- WSHの無効化
- rundll32.exe、regsvr32.exeの通信の禁止
- PowerShellの禁止
- HTAの禁止
- Webブラウザのプラグインを自動実行させない
- マッシュアップコンテンツを制限
- ストアアプリの禁止

- 他にも、技術トレンドなどを掲載しております

© 2016 Internet Initiative Japan Inc.

5. まとめ

© 2016 Internet Initiative Japan Inc.

まとめ

wizSafe

- 最近の攻撃は身近な場所で、**気付かない形**で発生する
  - 「一見正しく見える」ことが特徴
- マルウェアの実行を追跡出来るようにしておくことで、万一感染があっても**経緯を追いかける**ことが可能
  - 感染しないことが一番だが、感染した場合の情報源となる
- 標準設定のWindowsには、**強化出来る点が沢山**ある
  - 対策可能な項目を知り、業務影響の無い範囲で強化することが必要
- セキュリティに**絶対は無い**
  - トレンドを追いかけることが必要

© 2016 Internet Initiative Japan Inc.

Ongoing Innovation

IIJ Internet Initiative Japan

ご清聴ありがとうございました

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示しておりません。©2016 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。