Internet Week ショーケース

実践インシデント対応

～侵入された痕跡を発見せよ～

2017年6月2日

JPCERT コーディネーションセンター
分析センター マネージャー
竹田春樹

自己紹介

- 分析センターに所属（2006年より）
  - 分析センター マネージャー
- 主な業務
  - マルウエア分析（動的解析）などを中心に分析を実施
  - 講演活動なども行っています

アジェンダ

1 状況把握
標的型攻撃の動向
- 侵入経路について
- 侵入後のネットワーク内部での攻撃パターン
  - 攻撃者使用するコマンドおよびツール

2 資料紹介
コマンドおよび実行の痕跡
- 「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」の概要
- 報告書の活用例

3 調査手段
イベントログを用いた分析

はじめに

JPCERT/CCとは

一般社団法人　JPCERTコーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
ジェーピーサート コーディネーションセンター

- 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となるCSIRT（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、等)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

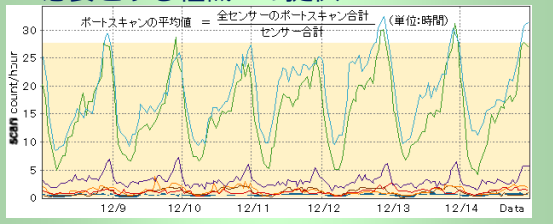
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

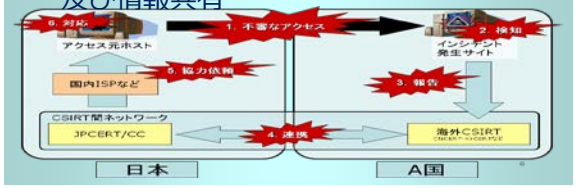
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有

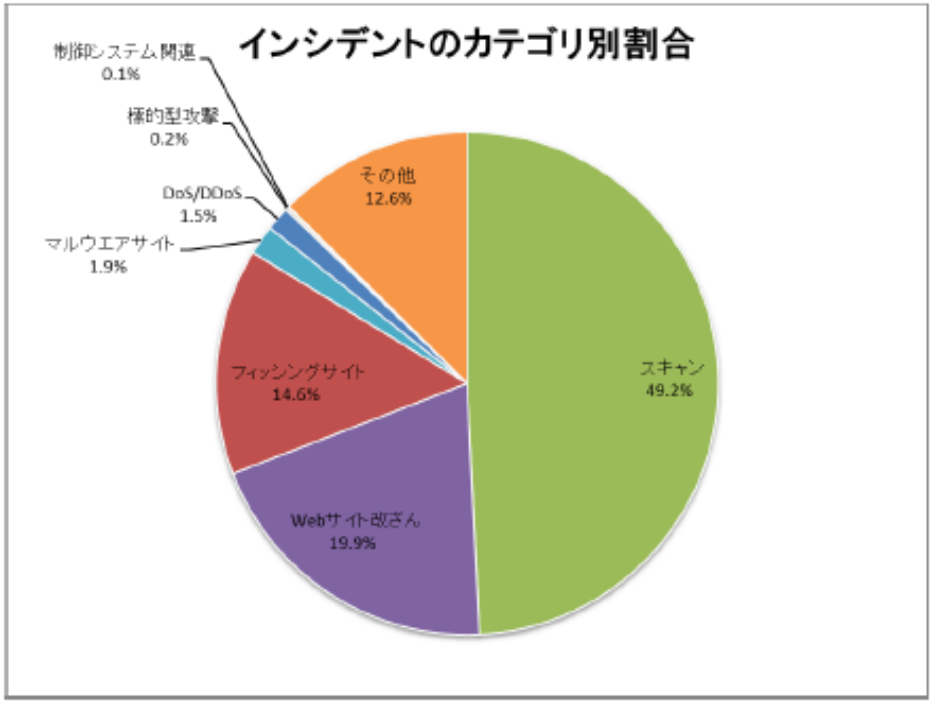


早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

標的型攻撃の動向

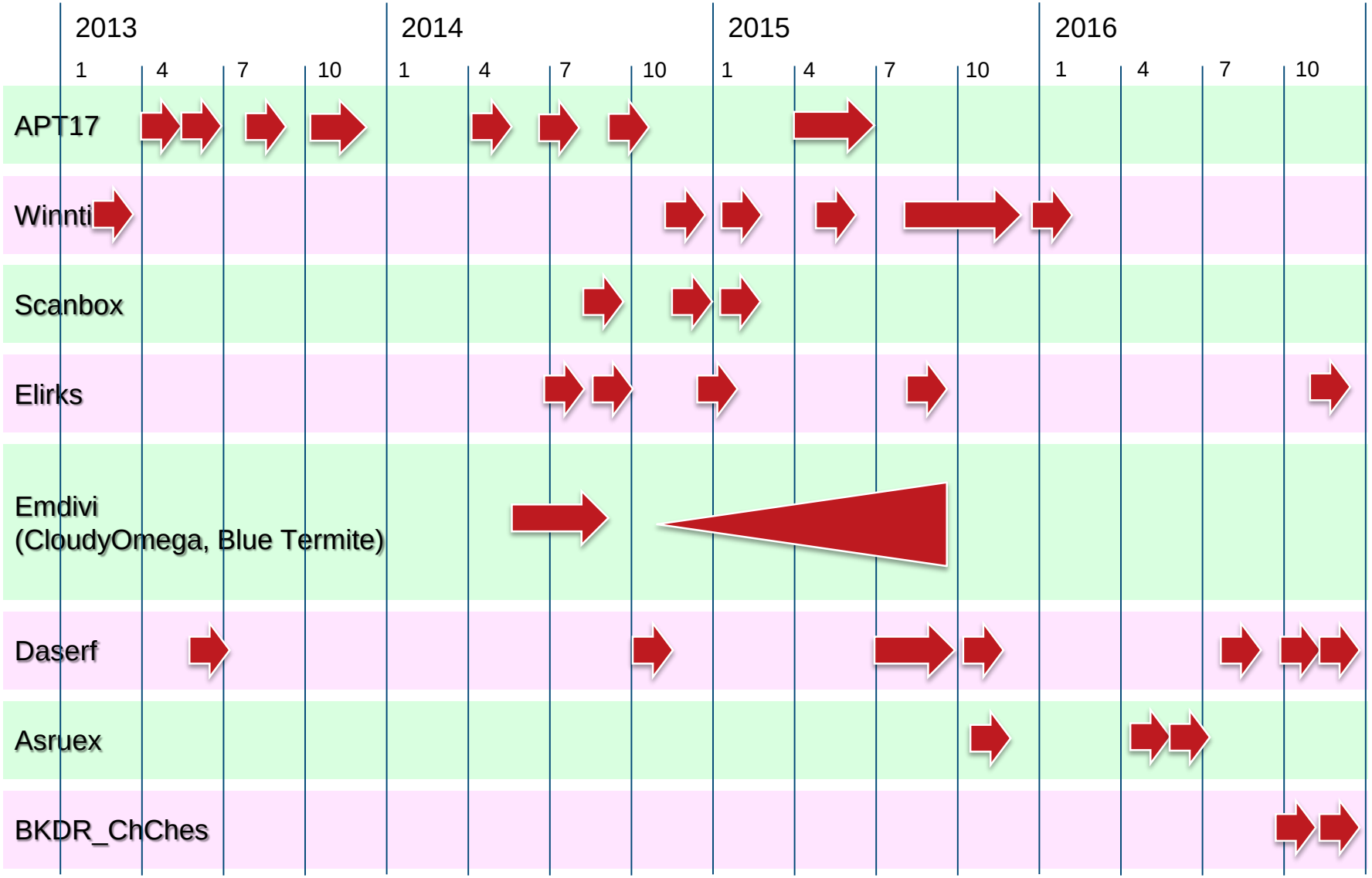
高度サイバー攻撃（標的型攻撃）とは何か？

- **特定の組織を狙った情報窃取や、システム破壊を主な目的とする執拗な攻撃**
  - 標的型攻撃、APTと呼ばれることも
  - 2015年以降、このタイプの攻撃について社会的にも注目されるようになりました



JPCERT/CC インシデント報告対応レポート（2017年1-3月）より
https://www.jpcert.or.jp/ir/report.html

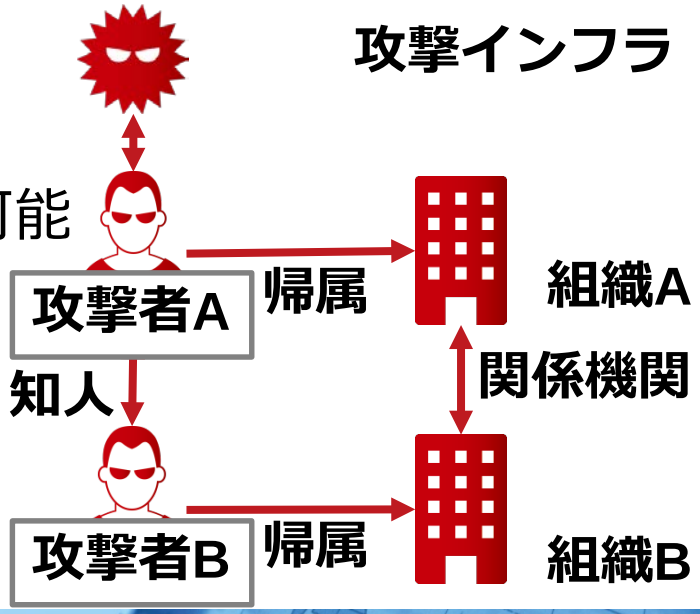
JPCERT/CC対応の主なAPT攻撃



攻撃者の背景

- **彼らの目的は複雑**
  - 機密情報の窃取や、システムの破壊
  - 海外では、様々な攻撃が発生している
    - **韓国 3.20 大乱 (2013/3)**
    - **フランス TV5monde 放送事故 (2015/4)**
    - **ウクライナにおける停電 (2015年12月、2016年12月)**

- **組織的に行動**
  - 長期にわたる (1年以上) 攻撃が可能



攻撃グループってどれくらいあるの？

- セキュリティベンダーにより命名されたもので攻撃の特徴毎に攻撃者グループの名称、オペレーション名がある
- 名称も命名した組織ごとに異なっており、把握するのは困難

［名称（例）］

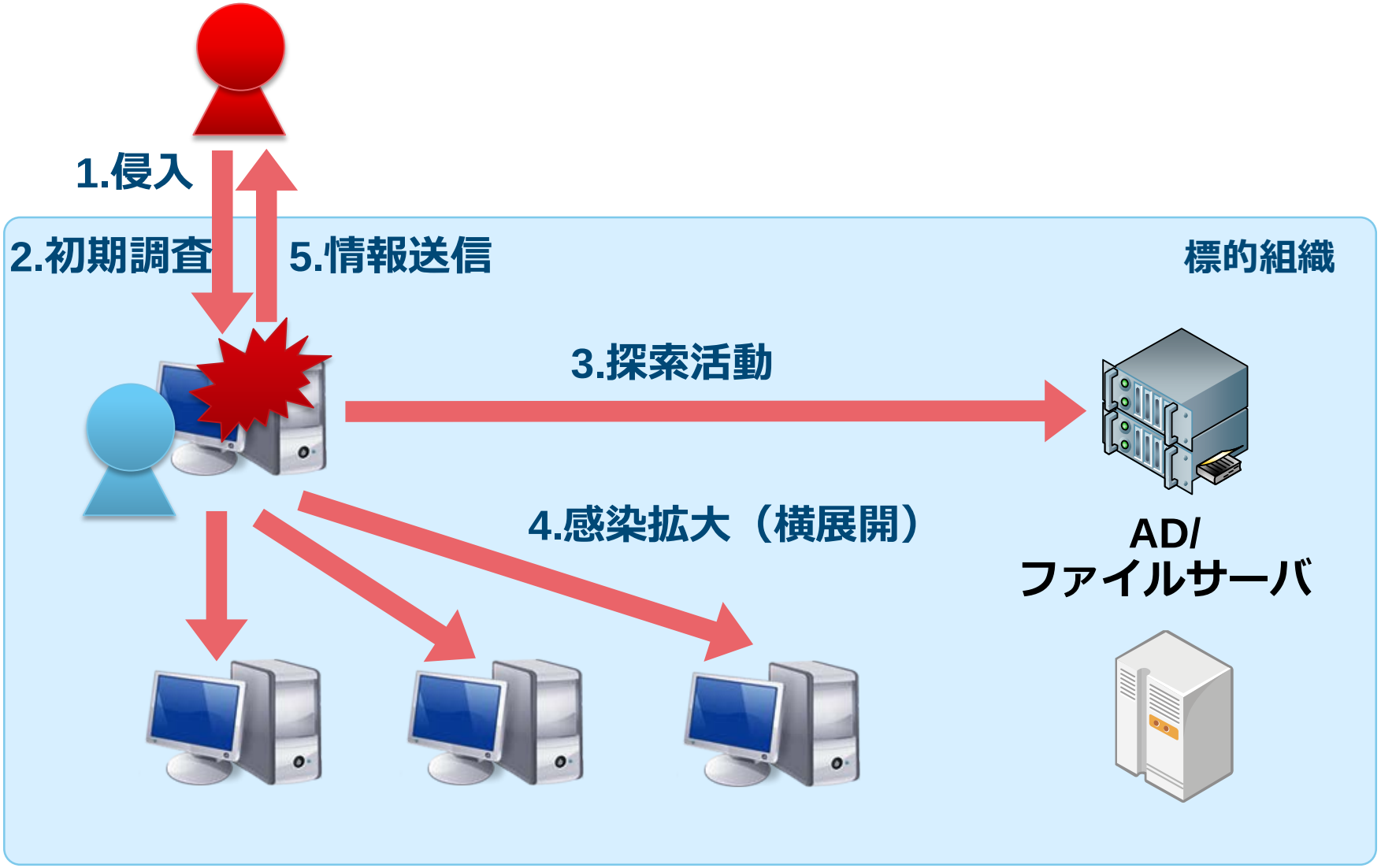
Mandiant	CrowdStrike	TrendMicro	Symantec
APT10	Stone Panda	N/A	N/A
APT17	Aurora Panda	N/A	Hydden LYNX
APT27	Emissary Panda	N/A	N/A
APT28	Fancy Bear	Pawn Storm	N/A

参考: APT Groups and Operations
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=361554658

標的型攻撃における侵入方法

攻撃手口	攻撃概要
標的型攻撃メール	攻撃対象とする組織の関係者などを装いメールを送付し、添付するマルウエアの実行や攻撃者が用意したWebサイトへの誘導を試みる攻撃
水飲み場型攻撃	攻撃対象とする組織が普段アクセスを行うWebサイトへ侵入を行い、マルウエアへの感染などを試みる攻撃
アップデートハイジャック	攻撃対象とする組織が普段使用するソフトウエアのアップデート配信元へ侵入を行い、ソフトウエアのアップデート機能を悪用しマルウエアなどを送り込む攻撃
ドメインハイジャック	攻撃対象とする組織が使用するWebサイトのドメインを乗っ取り、攻撃者が用意したWebサイトへ誘導する攻撃

ネットワーク内部に侵入した攻撃者の活動



ネットワーク内部に侵入した攻撃者の活動

初期調査

- 侵入した端末の情報を収集

探索活動

- 感染した端末に保存された情報や、ネットワーク内のリモート端末を探索

感染拡大

- 感染した端末を別のマルウエアにも感染させる、または別の端末にアクセスを試みる

感染拡大パターン

- 管理用アカウント（共通パスワード）の悪用
- 脆弱性の悪用
- Domain Adminsグループのアカウントの掌握

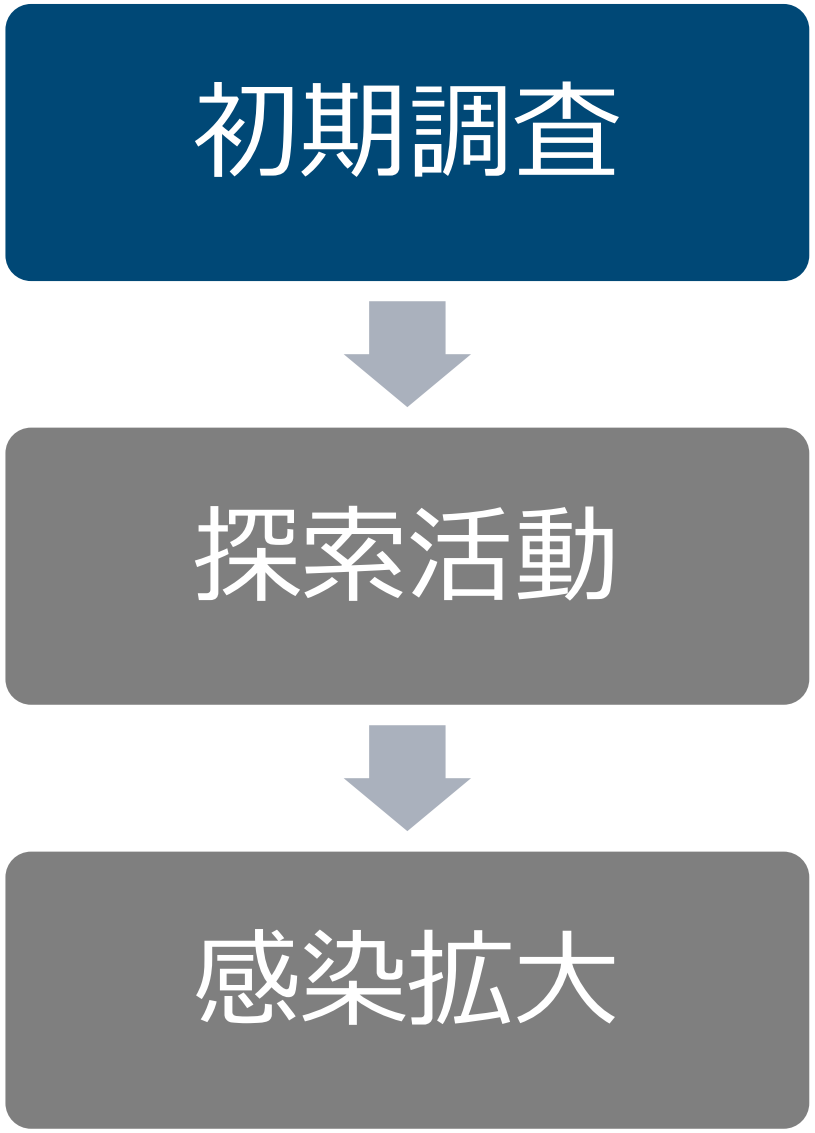
攻撃者が利用するコマンドおよびツール

攻撃者が使うのは、攻撃ツール（不正なツール）だけとは限らない

Windowsに標準で準備されている**コマンド**や、**正規のツール**も使用

コマンドや正規のツールはウイルス対策ソフトで検知されない

攻撃者の活動：初期調査



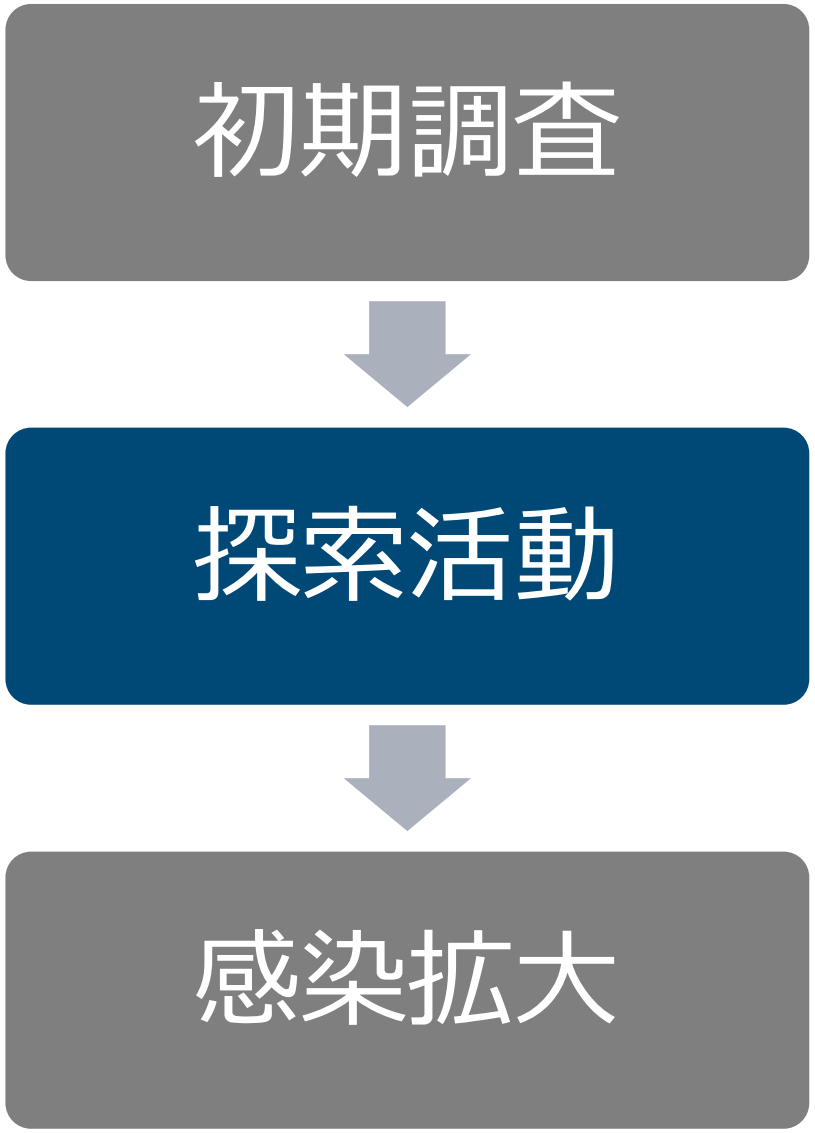
初期調査

初期調査

- 感染した端末の情報を収集する

- マルウエアの機能を利用して収集
- Windowsコマンドを利用して収集

攻撃者の活動：探索活動



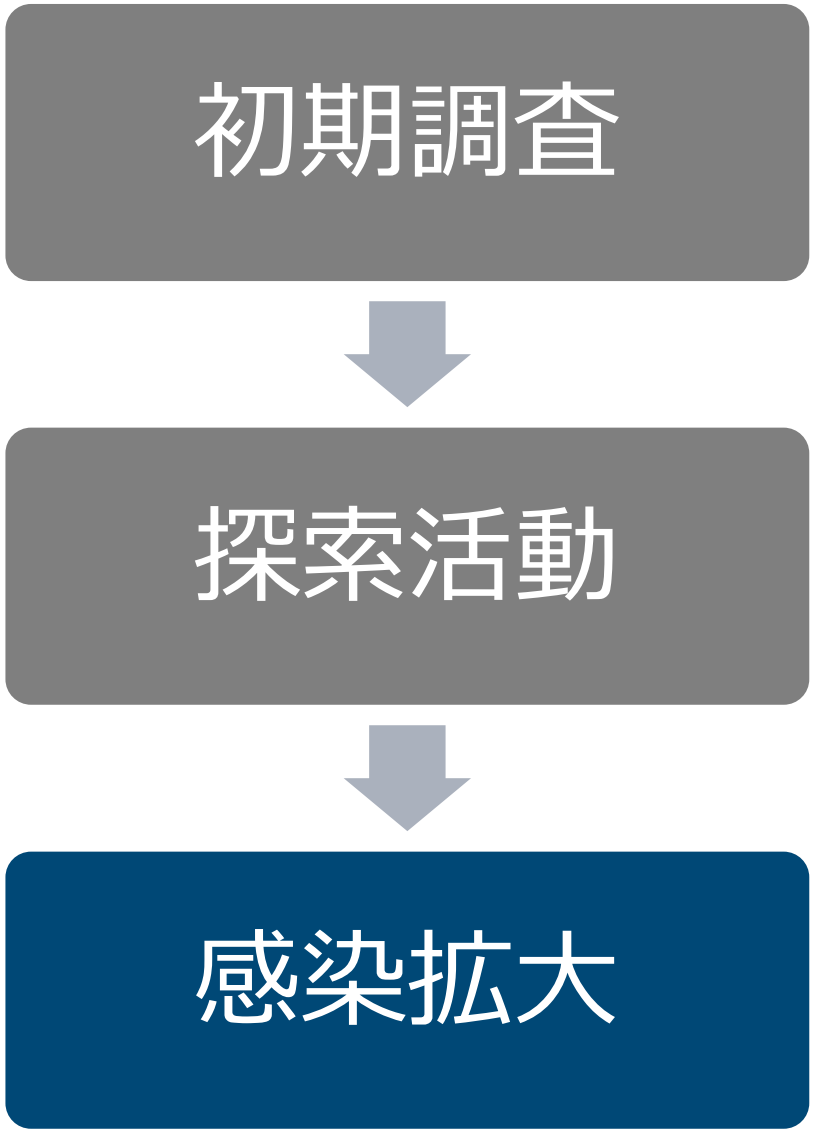
探索活動

探索活動

- 感染した端末に保存された情報を収集
- ネットワーク内のリモート端末を探索

- マルウエアの機能を利用して収集
- Windowsコマンドを利用して収集

攻撃者の活動：感染拡大



感染拡大

感染拡大

- 感染した端末を別のマルウエアに感染
- 別の端末に侵入し、マルウエアに感染させる

- パスワード、ハッシュダンプツールを使用
- Windowsコマンドを利用して感染拡大

情報の送信

機密情報の収集

- dirコマンド
- typeコマンド

ファイルの圧縮

- WinRARで圧縮

送信

- マルウエアの機能を利用
- クラウドサービスを利用

コマンドおよび
ツール実行の痕跡

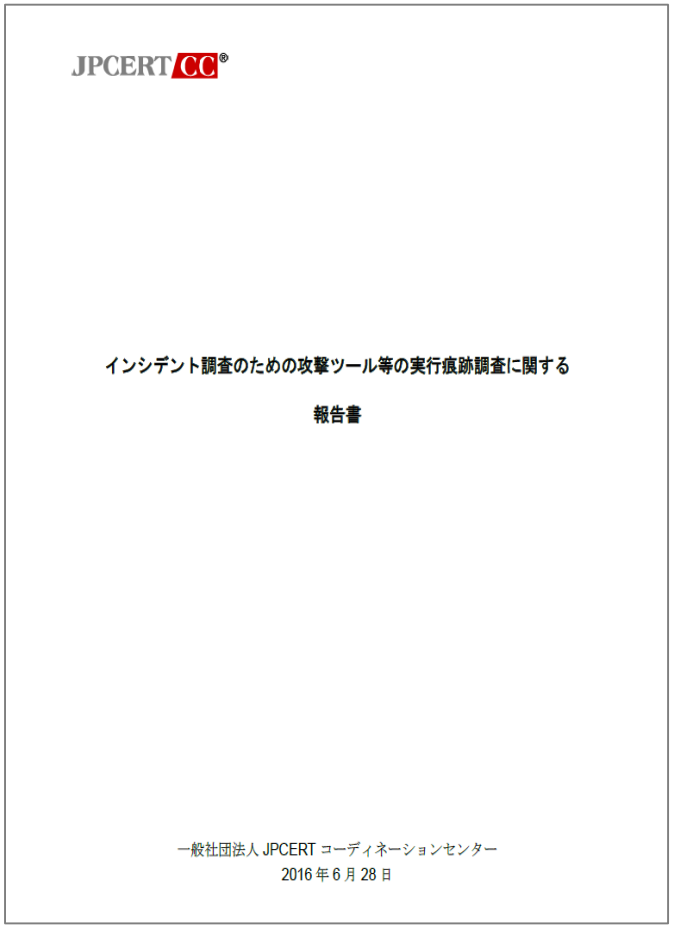
JPCERTCCの調査で確認している事実

ネットワーク内部での攻撃には
同じ攻撃ツール、Windowsコマンドが
利用されることが多い

攻撃ツール、Windowsコマンドが実行された痕跡を見つける方法を知っていれば、インシデント調査がスムーズになる

コマンドおよびツール実行の痕跡

コマンドおよびツール実行時に作成される痕跡を調査し報告書として公開



インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
https://www.jpcert.or.jp/research/ir_research.html

本報告書について

報告書の内容

- ログに記録された情報から、どのツールが実行されたのかを割り出すためのログ調査ガイド
- 複数のツールを検証し、作成される痕跡を調査

報告書の想定ユーザ

- システム管理者
- インシデント調査の専門家ではない人でも比較的容易に調べることができるように構成（専門的なフォレンジックツールは不要）

本報告書の調査対象

検証環境

- クライアント
  - Windows 7 Professional SP1、8.1 Pro
- サーバ
  - Windows Server 2008 R2 SP1、2012 R2

検証を行ったツール

- JPCERT/CCが対応したインシデント調査で、複数の事案で攻撃者による使用が確認されたものの中から選定
- 44種類

検証ツールリスト 1

攻撃者がツールを使用する目的	ツール
コマンド実行	PsExec
	wmic
	PowerShell
	wmiexec.vbs
	BeginX
	winrm
	at
	winrs
	BITS
パスワード、ハッシュの入手	PWDump7
	PWDumpX
	Quarks PwDump
	Mimikatz(パスワードハッシュ入手)
	Mimikatz(チケット入手)
	WCE
	gsecdump
	lslsass
	Find-GPOPasswords.ps1
	Mail PassView
	WebBrowserPassView
	Remote Desktop PassView
通信の不正中継 （パケットトンネリング）	Htran
	Fake wpad
リモートログイン	RDP

検証ツールリスト 2

攻撃者がツールを使用する目的	ツール
Pass-the-hash Pass-the-ticket	WCE(リモートログイン)
	Mimikatz(リモートログイン)
SYSTEM権限に昇格	MS14-058 Exploit
	MS15-078 Exploit
権限昇格	SDB UAC Bypass
ドメイン管理者権限 アカウントの奪取	MS14-068 Exploit
	Golden Ticket (Mimikatz)
	Silver Ticket (Mimikatz)
Active Directoryデータベースの奪取 （ドメイン管理者ユーザの作成、もしくは 管理者グループに追加）	ntdsutil
	vssadmin
ローカルユーザー・グループの追加・削除	net user
ファイル共有	net use
	net share
	icacls
痕跡の削除	sdelete
	timestomp
イベントログの削除	wevtutil
アカウント情報の取得	csvde
	ldifde
	dsquery

追加ログ取得の重要性

デフォルト設定で痕跡が残るツール

- Windowsで標準的に搭載されているツール
- RDP、at、net、PsExec など

追加設定が必要なツール

- Windowsで標準的に搭載されていないツール
- 攻撃ツール

今回の検証で行った追加設定

追加設定

- 監査ポリシーの有効化
- Sysmonのインストール

監査ポリシー

Windowsに標準で搭載されているログオン・ログオフやファイルアクセスなどの詳細なログを取得するための設定

Sysmon

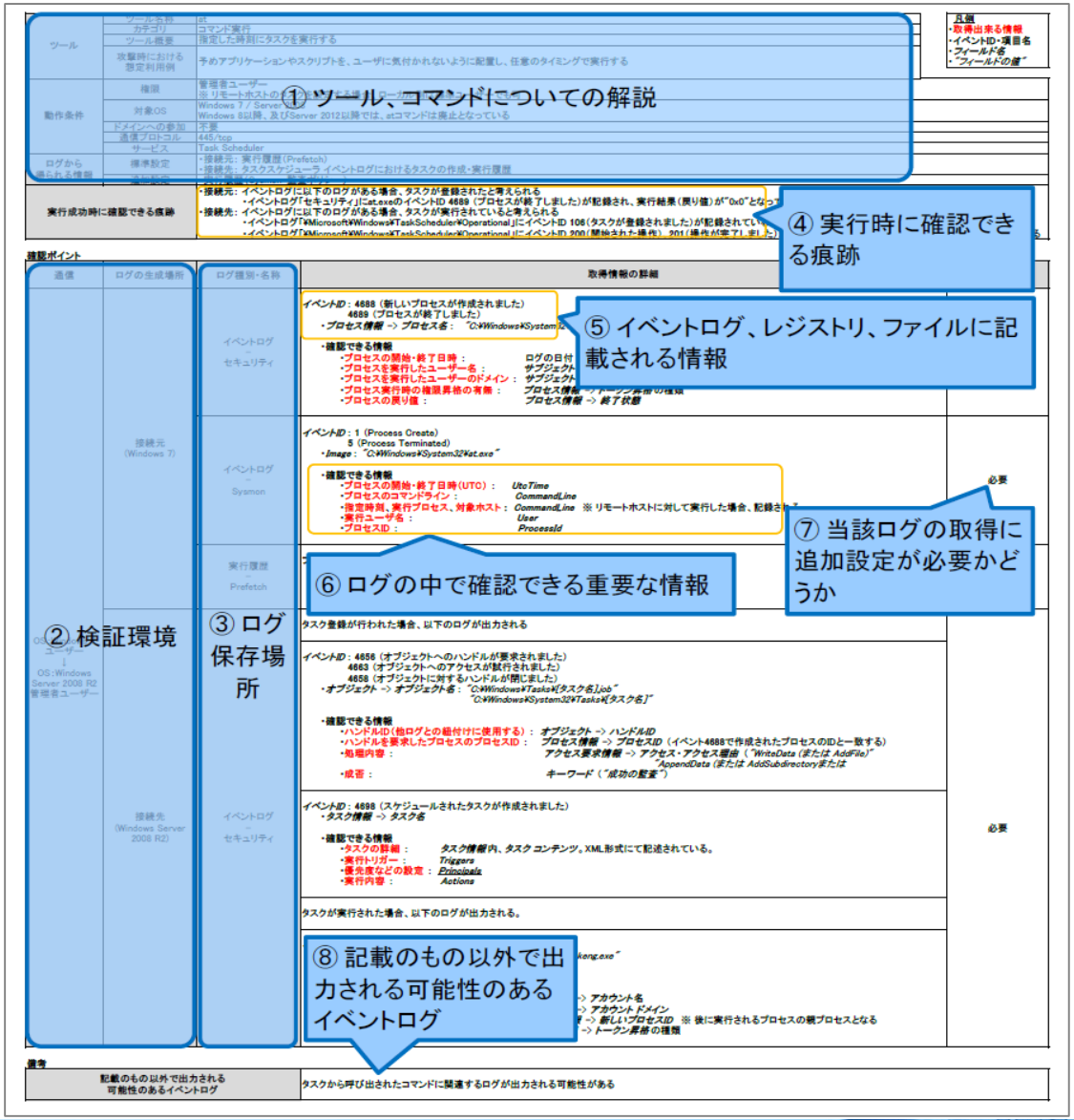
マイクロソフトが提供するツールで、プロセスの起動、ネットワーク通信、ファイルの変更などをイベントログに記録する

追加ログ取得設定の影響

- 監査ポリシーを有効にすることで、ログが増加する
  - ログのローテーションが早くなり古いログが残りにくくなる

- 監査ポリシーを有効化する場合は、イベントログの最大サイズの変更もあわせて検討する
  - イベントビューアー
  - wevtutilコマンド

報告書の例



報告書の活用例

報告書を用いたインシデント調査

192.168.31.42-PWHashes.txtが作成された痕跡を確認した場合

報告書を用いたインシデント調査

「PWHashes.txt」を報告書で検索すると、
以下の情報がヒットする（P.26）

3.3.2 PWDumpX

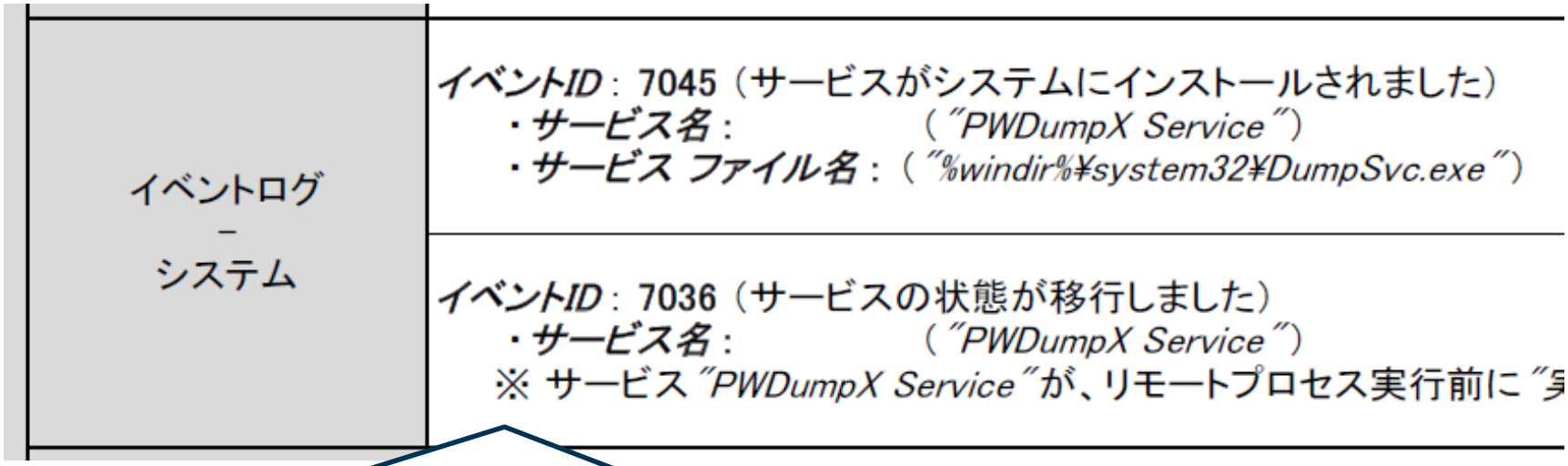
〈基本情報〉

ツール	ツール名称	PWDumpX
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	リモートホストからパスワードハッシュを取得する
	攻撃時における想定利用例	取得したハッシュを用いて、pass-the-hashなどの攻撃をおこなう ・接続元：PWDumpX実行元 ・接続先：PWDumpXによってログインされた先
動作条件	権限	・接続元：標準ユーザー ・接続先：管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp, 445/tcp
	サービス	-
ログから得られる情報	標準設定	・両ホスト：実行履歴（Prefetch）
	追加設定	・接続先：PWDumpXサービスがインストールされ、実行されたことが記録される ・接続元から接続先へ、PWDumpXサービスが送信され、実行されたことが記録される ・ハッシュ情報の作成・受領に、テキストファイルが利用されていることが記録される
実行成功時に確認できる痕跡		・接続元："[検体のパス]¥[宛先アドレス]-PWHashes.txt"が作成されている場合、実行が成功したものと考えられる

"[検体のパス]¥[宛先アドレス]-PWHashes.txt"
が作成されている場合、実行が成功したものと
考えられる

報告書を用いたインシデント調査

PWDumpXはパスワードハッシュを入手するツールで、[宛先アドレス]はターゲット



イベントログ － システム	イベントID：7045（サービスがシステムにインストールされました） ・サービス名：（"PWDumpX Service"） ・サービス ファイル名：（"%windir%¥system32¥DumpSvc.exe"）
	イベントID：7036（サービスの状態が移行しました） ・サービス名：（"PWDumpX Service"） ※ サービス"PWDumpX Service"が、リモートプロセス実行前に"実

接続先（ [宛先アドレス] ）ではサービス名“PWDumpX Service”がインストールされると報告書に記載されている（P.27）

報告書を用いたインシデント調査

[宛先アドレス]のイベントログを確認すると“PWDumpX Service”が確認できる

以上の調査結果から[宛先IPアドレス]のパスワードハッシュが攻撃者に入手されていると断定することができる

追加設定していない場合はどうするの？

詳細なログを取得する他の方法

- 監査ソフトウエア（資産管理ソフトなど）でも同様のログを取得可能な場合がある
  - プロセスの実行
  - ファイルの書込み

- 詳細なログがなくても、デフォルト設定で痕跡が残るツールもある

どこから見たらいいの？

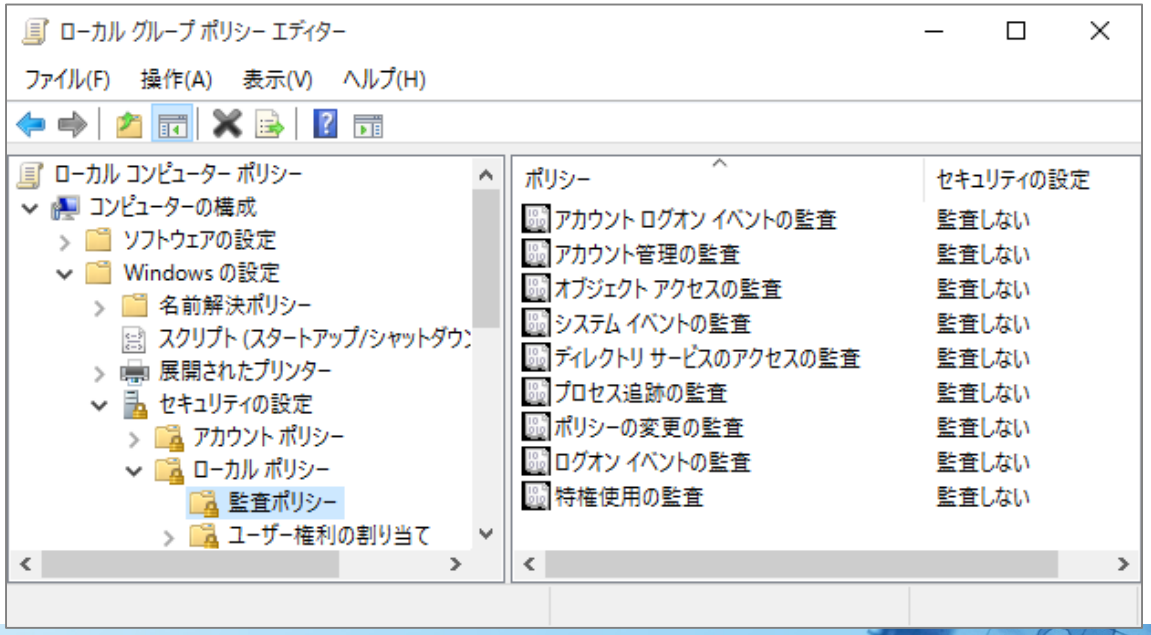
- インシデント調査の際に辞書として使うことを想定しているので、すべてを把握する必要はない

- 「3.16. ツールの実行成功時に見られる痕跡」にすべてのツールの確認ポイントをまとめているので、まずはそのページから見ることをお勧めする

参考情報: 監査ポリシーの有効化方法

設定方法 ①

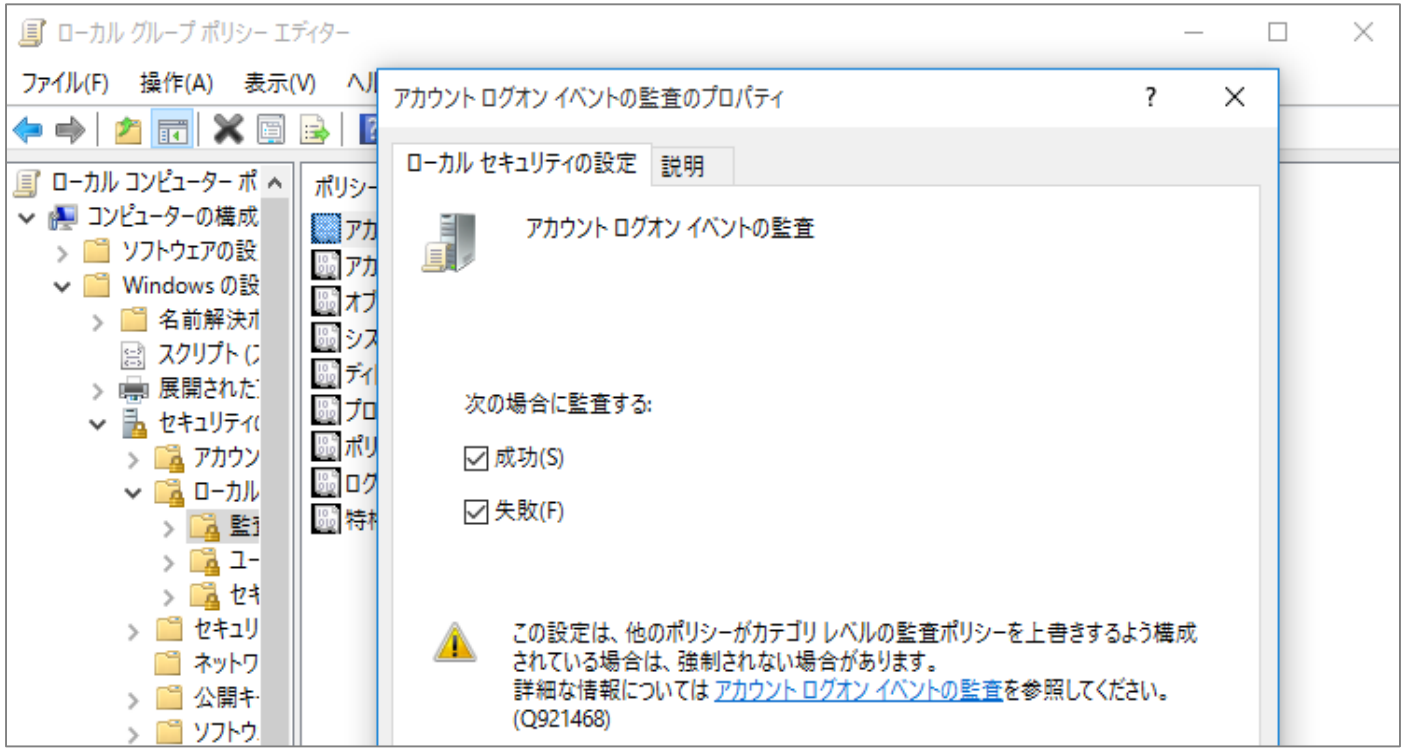
- ローカル グループ ポリシーの編集
  - [コンピューターの構成]→[Windowsの設定]→[セキュリティの設定] →[ローカル ポリシー]→[監査ポリシー]



参考情報: 監査ポリシーの有効化方法

設定方法 ②

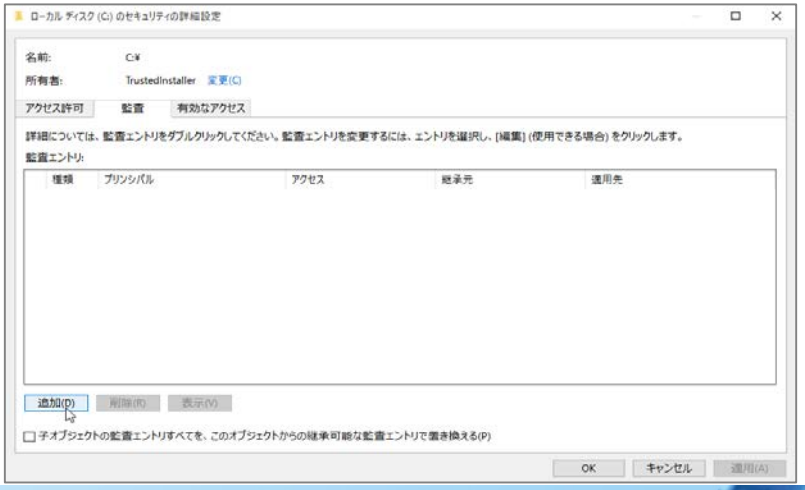
- 各ポリシーの「成功」「失敗」を有効



参考情報: 監査ポリシーの有効化方法

設定方法 ③

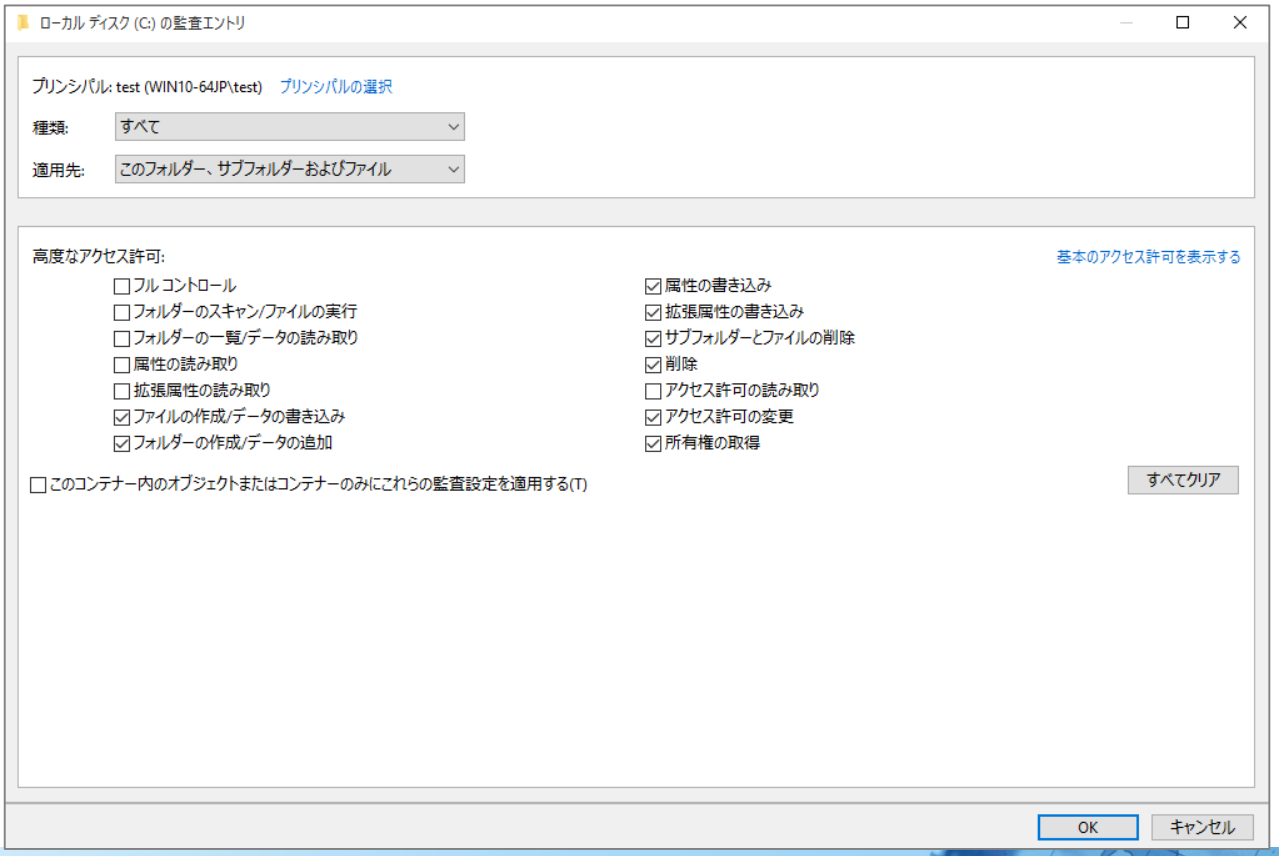
- 監査対象オブジェクトの追加
  - [ローカル ディスク(C:)]→[プロパティ]→[セキュリティ]タブ→[詳細設定]
  - [監査]タブから監査対象のオブジェクトを追加



参考情報: 監査ポリシーの有効化方法

設定方法 ④

- 監査対象のユーザおよび、監査するアクセス方法を選択



参考情報: 監査ポリシーの有効化方法

以下の「アクセス許可」を設定

- ファイルの作成/データ書き込み
- フォルダーの作成/データの追加
- 属性の書き込み
- 拡張属性の書き込み
- サブフォルダーとファイルの削除
- 削除
- アクセス許可の変更
- 所有権の取得

参考情報: Sysmonのインストール方法

ダウンロードURL

- https://technet.microsoft.com/ja-jp/sysinternals/dn798348

インストール方法

- **Sysmon.exe –i**
  - -n オプションを追加することでネットワーク通信のログも取得可能

対応バージョン

- クライアント： Windows 7以降
- サーバ： Windows Server 2012以降

イベントログを用いた分析

イベントログの変換方法

イベントログを変換

イベントビューアから
ログ調査を行うのは困難

テキスト形式にエクスポート・変換する

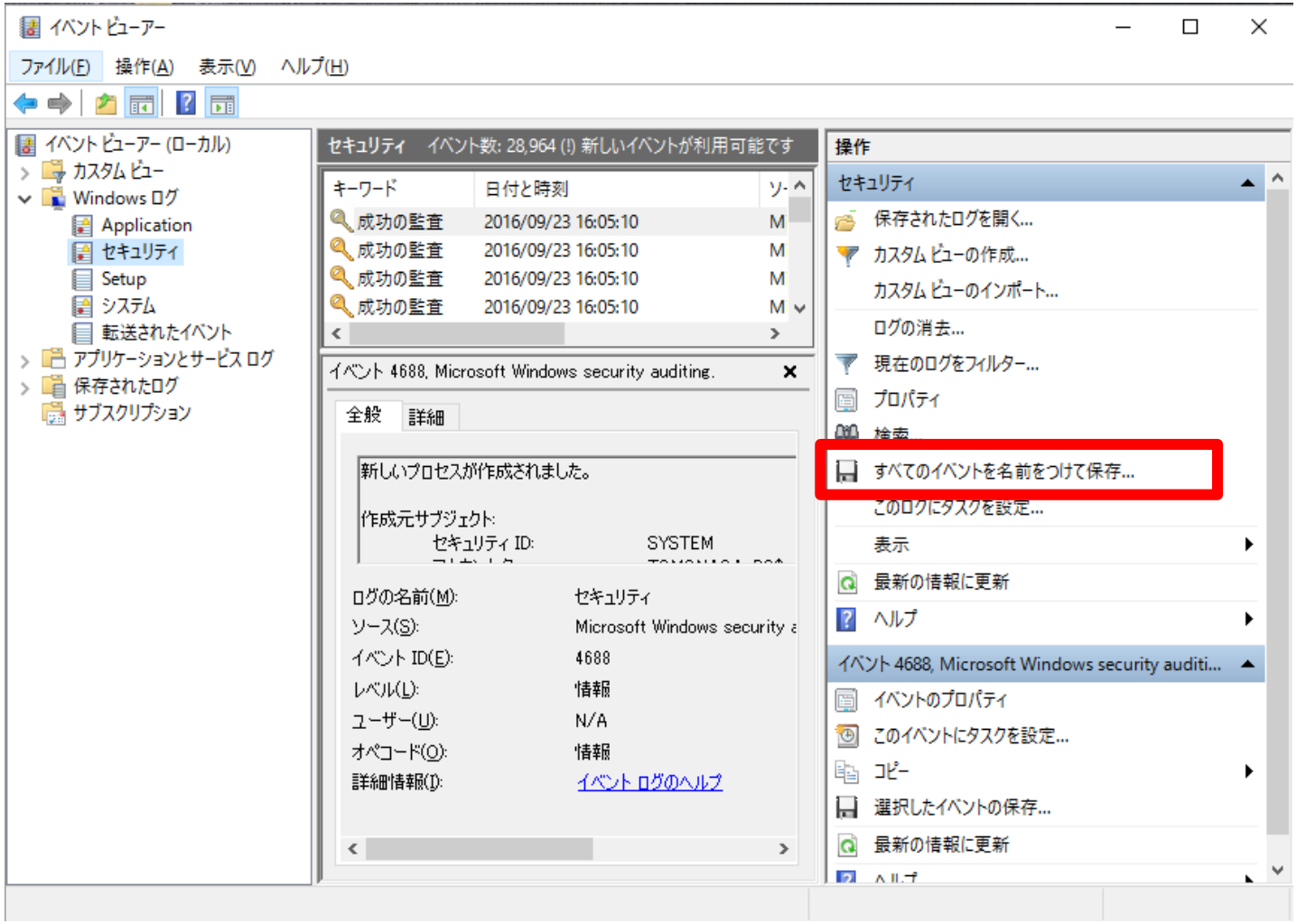
方法

① イベントビューアからExport

② Log Parserを使用して変換

イベントログの変換方法

イベントビューアからExport



イベントログの変換方法

Log Parserを使用して変換

Log Parserは、マイクロソフトが提供するログ取得ツール

SQL命令を使い、テキストやCSVなど様々な形式に変換可能

以下からダウンロードし、インストールする

https://www.microsoft.com/ja-jp/download/details.aspx?id=24659

イベントログの変換方法

Log Parserを使用して変換

例1 イベントログをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF
"select * from [input]" > [output]
```

LogParser.exe

```
C:¥Program Files (x86)¥Log Parser
2.2¥LogParser.exe
```

ログフォルダ

```
C:¥Windows¥System32¥winevt¥Logs
```

イベントログの変換方法

Log Parserを使用して変換

例2 特定のカラムをCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF
"select EventLog, RecordNumber,
TimeGenerated, TimeWritten, EventID,
EventType, EventTypeName, SourceName,
Strings, ComputerName from [input]"  >
[output]
```

イベントログの変換方法

Log Parserを使用して変換

例3 日時を指定してCSVで出力

```
LogParser.exe -i evt -o csv -stats:OFF -
resolveSIDs:ON "select EventLog,
RecordNumber, TimeGenerated, TimeWritten,
EventID, EventType, EventTypeName,
SourceName, Strings, ComputerName from
[input] WHERE TimeGenerated > '2016-11-01
00:00:00' AND TimeGenerated < '2016-11-02
00:00:00'" > [output]
```

イベントログの変換方法

Log Parserを使用して変換

Log Parserの注意ポイント
特定のエントリが複数行にわたるケースがある

対策例（Linuxコマンドで改行を削除する）

```
nkf –w [input] | sed ‘s/¥t¥t¥t/ /g’ | sed
‘s/¥t¥t/,/g’ | tr -d “¥n” | tr -d “¥n¥r” |
sed ‘s/[file path]/¥n[file path]> [output]
```

※ [file path]は処理を行ったイベントログのパス

今回用意したログ

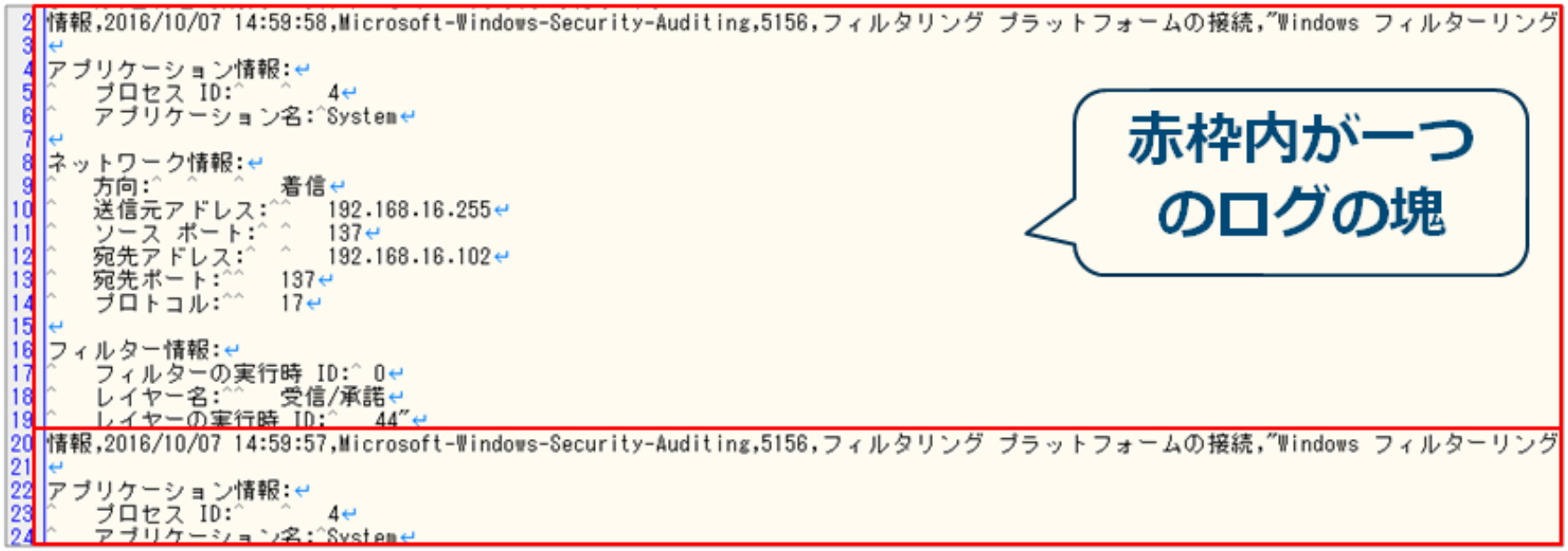
イベントログ

- Security.csv
  （セキュリティログ）
- Sysmon.csv
  （Sysmonログ）

ログの形式（Security.csv）

- 「Windowsログ-セキュリティ」を「すべてのイベントを名前を付けて保存」で取得したファイル
  - 形式: CSV（ログが複数行に出力される）

レベル	日時	ソース	イベントID	タスクのカテゴリ



ログの形式（Sysmon.csv）

- 「アプリケーションとサービス-Microsoft-Windows-Sysmon-Operational」を「すべてのイベントを名前を付けて保存」で取得したファイル
  - 形式: CSV（ログが複数行に出力される）

レベル	日時	ソース	イベントID	タスクのカテゴリ

```
情報,2016/10/07 14:59:00,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),"Process Create:
UtcTime: 2016-10-07 05:59:00.065
ProcessGuid: {02EA0504-39A4-57F7-0000-0010532F2400}
ProcessId: 1052
Image: C:¥Program Files (x86)¥Google¥Update¥GoogleUpdate.exe
CommandLine: ""C:¥Program Files (x86)¥Google¥Update¥GoogleUpdate.exe"" /ua /installsource scheduler
CurrentDirectory: C:¥Windows¥system32¥
User: NT AUTHORITY¥SYSTEM
LogonGuid: {02EA0504-AA74-57F5-0000-0020E7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=ADB860FF9C00B308BF4ABBCB77E2C5233FEB61C5
ParentProcessGuid: {02EA0504-AA95-57F5-0000-00107EB10100}
ParentProcessId: 1860
ParentImage: C:¥Windows¥System32¥taskeng.exe
ParentCommandLine: taskeng.exe {BE0F3FE8-EA3F-4EC2-9BC1-FE64B80A6228} S-1-5-18:NT AUTHORITY¥System:Service:"
情報,2016/10/07 14:51:12,Microsoft-Windows-Sysmon,5,Process terminated (rule: ProcessTerminate),"Process terminated:
UtcTime: 2016-10-07 05:51:12.407
ProcessGuid: {02EA0504-376B-57F7-0000-0010A6FF2300}
ProcessId: 1660
```

赤枠内が一つのログの塊

イベントログを用いた分析

① 不審な通信先の確認

［投影データのみ］
スクリーンにてデモを予定しています

イベントログを用いた分析

② マルウエアの動作時刻と動作要因を特定せよ

［投影データのみ］
スクリーンにてデモを予定しています

イベントログを用いた分析

③　横展開の痕跡の調査

［投影データのみ］
スクリーンにてデモを予定しています

さいごに

- ネットワーク内部への侵入をすべて防御するのは難しい

- 攻撃者のネットワーク内部での行動を把握するためには、追加で詳細なログを取得する必要がある

インシデント発生後の被害状況調査のため、ログの取得方法、期間等について再検討することをお勧めします

参考情報（1）

- 報告書
  - インシデント調査のための攻撃ツール等の実行痕跡調査報告書
    https://www.jpcert.or.jp/research/ir_research.html

- 分析センターだより
  - 攻撃者の行動によって残る痕跡を調査
    https://www.jpcert.or.jp/magazine/acreport-ir_research.html
  - 攻撃者が悪用するWindowsコマンド
    https://www.jpcert.or.jp/magazine/acreport-wincommand.html

参考情報（2）

- 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて

  http://www.jpcert.or.jp/research/apt-guide.html

- 高度サイバー攻撃への対処におけるログの活用と分析方法

  http://www.jpcert.or.jp/research/apt-loganalysis.html

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form