テーマ２

ISMSの管理策の実装
「イベントログについての考察」

JNSA　標準化WG
日本ISMSユーザグループ
インプリメンテーション研究会

2019年12月4日

副主査　秋山、中村、松居、安田

アジェンダ

１章　はじめに

- テーマ２の活動経緯
- 2019年のテーマについて

2章　『ログ』の取得とレビュー

- いろいろなログとそのログの活用(例)
- ログをレビューして“生きたログ”へ

3章　イベントログのレビューとは

- イベントログのレビューの目的
- イベントログのレビューの対応ステップ

4章　ログにまつわる事例

- ファイルサーバのログ
- メールサーバのログ

５章　まとめ

- ログ取得・管理はやれるところから

6章　さいごに

- 2019年テーマ２の研究会活動の成果

Appendix

1章　はじめに

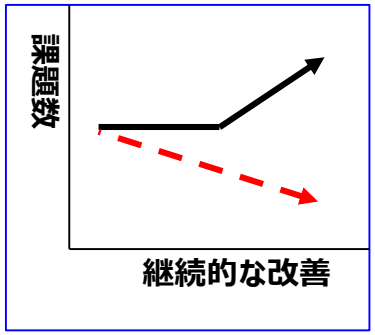
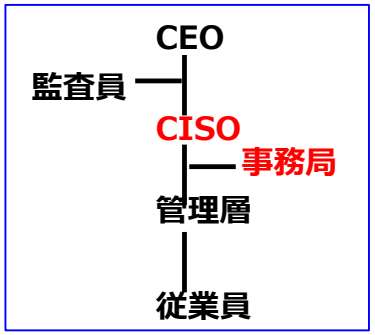
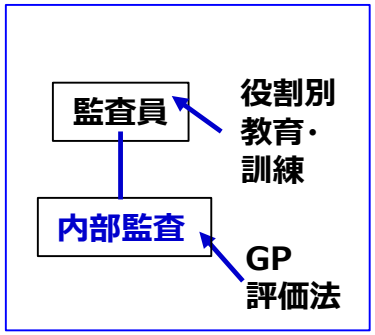
1-1. はじめに

テーマ2では、研究会参加メンバ各位におけるISMSの運用フェーズの課題が活発に議論されています。
毎年テーマを継続し、より良いISMSに向け課題整理を行っております。

可能な限り、当研究会の成果を本セミナーに参加頂いている組織の事務局や推進者などの皆様に持ち帰り頂き、自組織の運用フェーズにおける課題のヒントとして頂ければ幸いです。

2019年も研究会メンバ各位の間で多種多様な議論が行われました。しかしながら、すべての議論を本書に記載する事には至ってはおりません。
是非とも、本研究会へ参加いただき、実際の議論の場を体験し、自組織の課題解決に繋げて頂ければと思います。

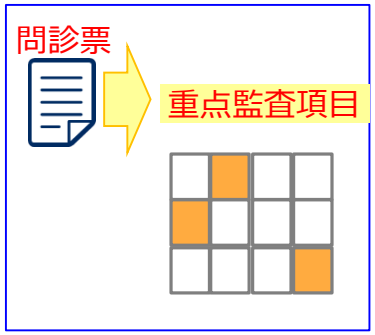
1-2. テーマ２の活動経緯（1）

2013年	2014年	2015年	2016年
ISMS推進各社が 抱える諸課題の対応策	ISMS推進事務局の 悩みと解決策	ISMSを成功させる ためのCISOの条件	運用フェーズにおける 有効性の評価
			
運用を継続しても 課題は減少しない	事務局自身が 機能不全是正不可に	規格の要求事項はCEO からCISOへ委嘱	時間経過によりISMSの 有効性が低下
⇩	⇩	⇩	⇩
「人」が原因	CISOと事務局の 「役割」が不明確	CISO機能の事務局への 過度な「委譲」	内部監査のマンネリ化

1-3. テーマ２の活動経緯（2）

2017年

内部監査を有効に
運用するための手法の
考察

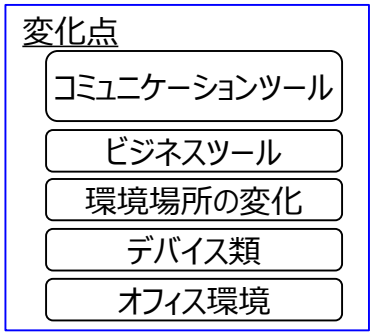


自覚症状が無い大きな
病気（不適合）を確実に
見つかる診察（監査）

監査前の事前準備

2018年

働き方改革における
情報セキュリティ



ITを活用して対応

セキュリティの側面の
変化点へのアセスメント

2019年

ISMSの管理策の実装
「イベントログについての
考察」

本日の資料

1-4. 2019年テーマ２の選定経緯

ISMSを組織へ実装する際の具体的な対応例を示す

2018年のテーマ2では「働き方改革における情報セキュリティ」とし、

- ✓ 働き方改革における、「新しい技術・インフラ、新しいツール、新しいルール」という変化に対するリスクアセスメント

について議論しました。

テーマ2は、昨年までは、具体的なISMSの対応(実装)の例示まで至ってはおりませんでした。ISMSの要求事項や管理策自体は、既に研究会でも議論してきており、年次発表会では度々報告をしてきました。
その為、2019年は「具体的な組織の対応(実装)」にフォーカスした議論とすべきテーマを選定するとし、年次発表会では、研究会で議論出来た範囲の中で、それらを例示するとしました。

1-5. 2019年テーマ２の内容

「ログのレビュー」について深堀し、組織への実装を例示！

研究会では、規格の中でも「A.12.4.1　イベントログ取得」にフォーカスして議論を行ないました。
多くの組織は『ログの取得』や『ログの保持』は出来ていると思われます。しかし、『ログのレビュー』については、戸惑っている組織が多いのではないでしょうか。

『ログのレビュー』について、専門的な解析手法や高価なツールに頼らず、一般的なログ管理のプロセスやシステム及び安価なツールを利用するために、参考になる事例を研究会メンバーが出し合うことで、ISMSを取得(又は取得しようと)している組織が運用しやすいように具体的で実用的な事例をまとめました。

2章　『ログ』の取得とレビュー

2-1. ログをみてみよう

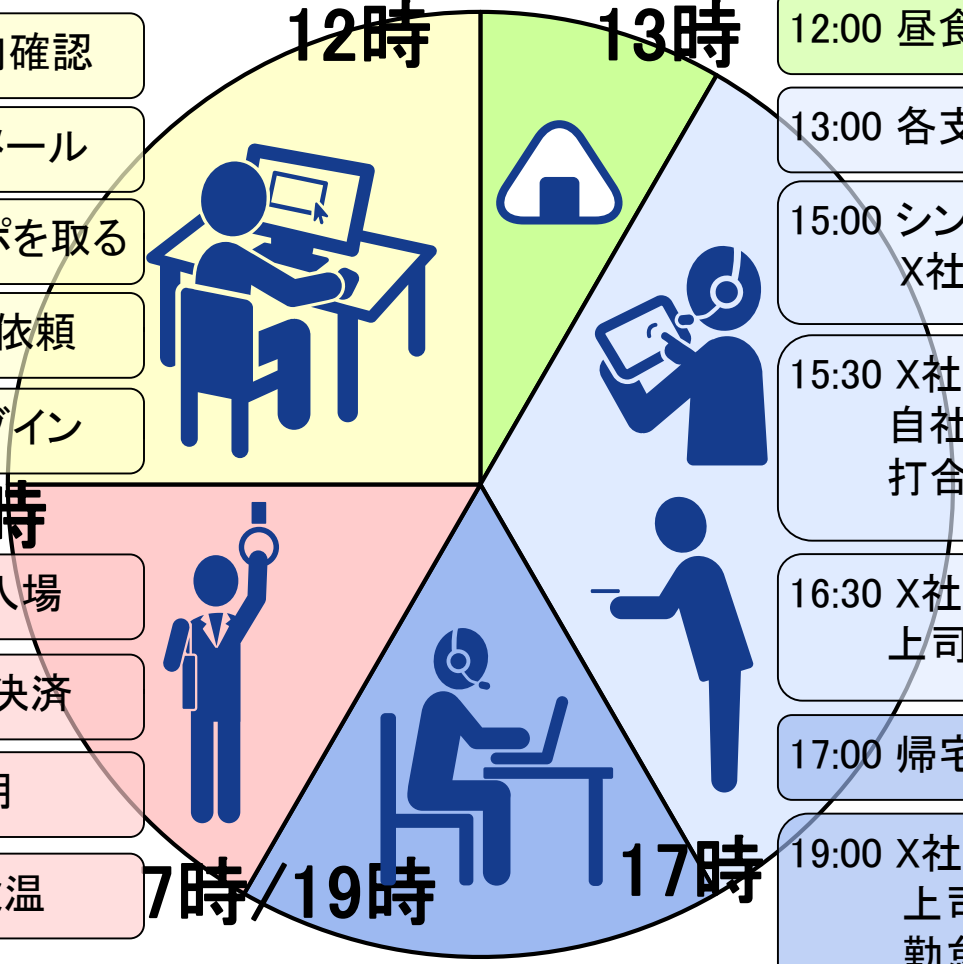
解説さん

ログとは、システムの中にだけ存在する特別なものではありません。
日常生活の中でも、多くのログが取得され、活用されています。

この章では、まずは、日常生活の中でログがどのように取得され、活用されているかから見てみましょう。

2-2. Aさんの１日のスケジュール

- 某社Aさん（営業マン）の１日を見てみましょう。



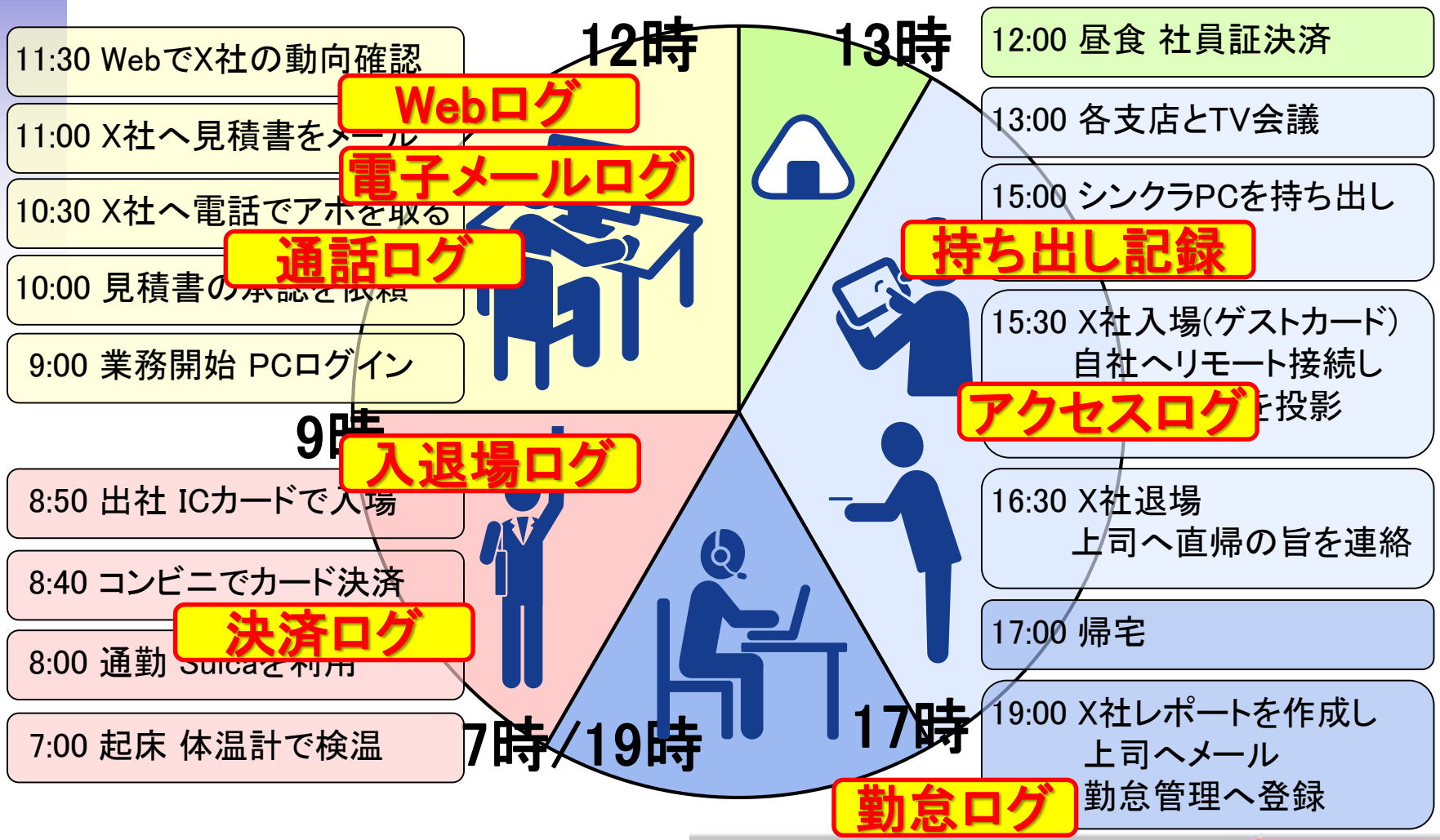
11:30 WebでX社の動向確認
11:00 X社へ見積書をメール
10:30 X社へ電話でアポを取る
10:00 見積書の承認を依頼
9:00 業務開始 PCログイン

8:50 出社 ICカードで入場
8:40 コンビニでカード決済
8:00 通勤 Suicaを利用
7:00 起床 体温計で検温

12:00 昼食 社員証決済
13:00 各支店とTV会議
15:00 シンクラPCを持ち出し
X社へ移動
15:30 X社入場(ゲストカード)
自社へリモート接続し
打合せ資料を投影
16:30 X社退場
上司へ直帰の旨を連絡
17:00 帰宅
19:00 X社レポートを作成し
上司へメール
勤怠管理へ登録

2-3. Aさんの１日の「ログ」

1日の中では、様々なAさんのログが取得されている！



2-4. いろいろなログとそのログの活用(例)

Aさんの１日を前頁で見てみました。それ以外にもさまざまなログが取得されており、
そのログから分かることがあります。

そうです。ログには取得する目的があるのです！

取得対象	取得されるログ	わかること（＝取得する目的）
入館申請	来訪者情報	不審な人物の来訪がないか
鍵管理簿	鍵貸出記録	不正な鍵の取り扱いはないか
監視カメラ	映像アーカイブ	不審な人物の行動履歴
携帯電話	通話履歴	どの番号に発信・着信をして、どれくらい通話したのか
ネットワーク機器	トラフィック	通信のキャパシティは十分か
ネットワーク機器	ログイン履歴	業務と関係のない、不審なログインはないか
ネットワーク機器	ポート状態	機器がいつNWに接続・切断されたか
サーバー機器	CPU・HDD	機器のキャパシティが十分か、正常に動作しているか
サーバー機器	Webアクセス	どこにアクセスしたか
サーバー機器	ログイン情報	業務と関係のない、不審なログインはないか
ファイルサーバー	アクセスログ	どのファイルに、いつアクセスしたのか
メール	メールヘッダー	メールがどのように転送されて配送されたのか

2-5. ログをレビューして“生きたログ”へ

ログは証拠や正常確認のために取得するだけではありません。
レビューして活用することで“生きたログ”になるのです。

ログは、多くの場面で取得され、活用されています。

ファイルサーバーや、メールサーバーなどでさまざまなログが取得されています。

それを確認(＝レビュー)することで、証拠や正常性の確認のための

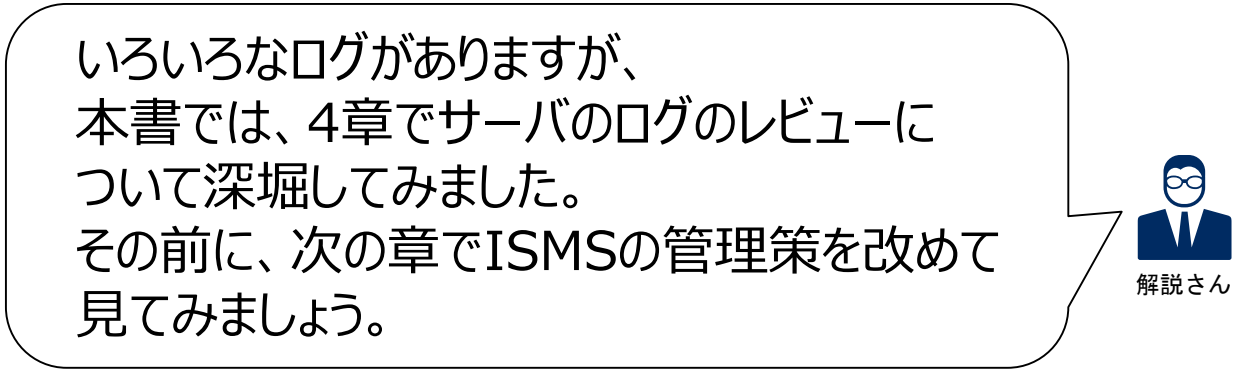
“生きたログ”になるのです。

（参考）
応用編です！ビッグデータなどでログを更に活用することで、
サービス向上、ビジネス視点で “生き生きしたログ” になりますね。
2019年は次のステップの応用編の議論は持ち越しとしました。
是非とも皆さんと本研究会で一緒にレビューしましょう！

2-6. いろいろなログ

ログは、組織における各種活動の記録です。ログには様々なログがあります。

- ✓ **組織の経理上の監査の記録など法規制対応に活用するログ**
- ✓ **情報システムにおける、不正アクセス、トラフィック増加、マルウェア感染のログ**
- ✓ **Webアクセス時のCookieもログ！**



3章　イベントログのレビューとは

3-1. ISMSとイベントログ

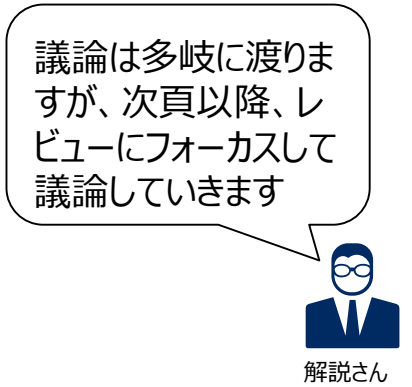
JIS Q 27001：2014（ISO/IEC 27001：2013）

A.12.4 ログ取得及び監視 目的 イベントを記録し，証拠を作成するため。		
A.12.4.1	イベントログ取得	管理策 利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューしなければならない。

皆さんは、この管理策をどのように実施していますか？

例えば、皆さんの組織でこんな事はありませんか？

- なんとなく、とれるログだけとっている
- そもそも何に使うのか、真剣に考えた事が無い
- 審査で指摘されないよう、「レビューした記録」は作成している



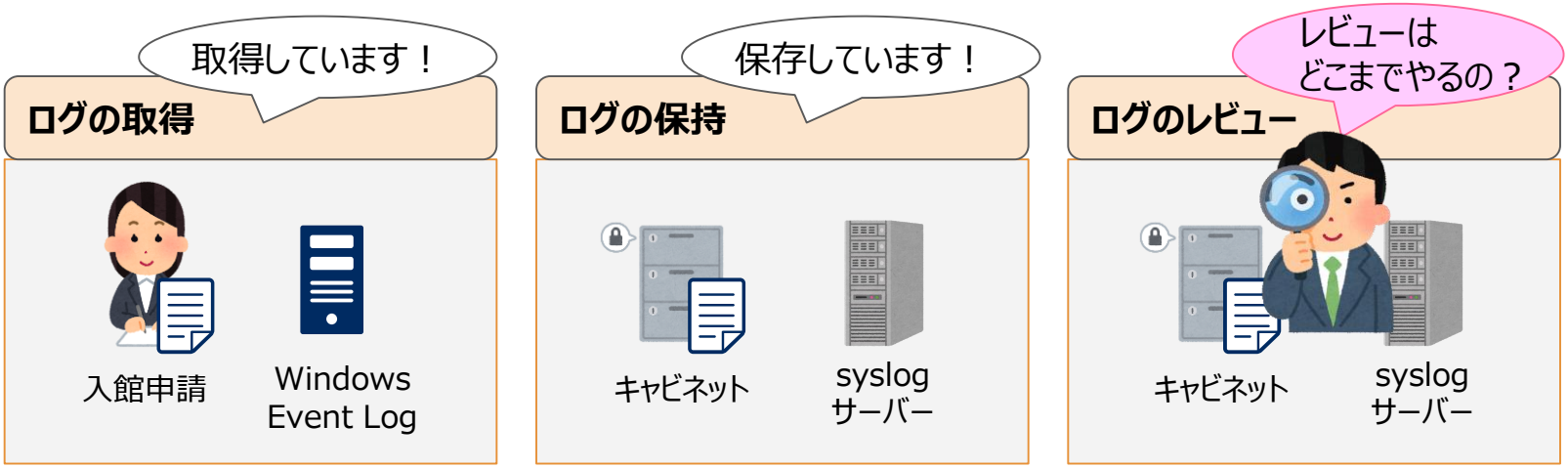
3-2. ログのレビューは？

そもそも「ログのレビュー」は、どうやればよいのだろうか？

ISMSの実装にあたって、組織では社内規程としてログのレビューを定めているかと思います。

また、多くの組織では『ログの取得』や『ログの保持』は出来ているでしょう。

しかし、『ログのレビュー』については、戸惑っている組織が多いのではないでしょうか。



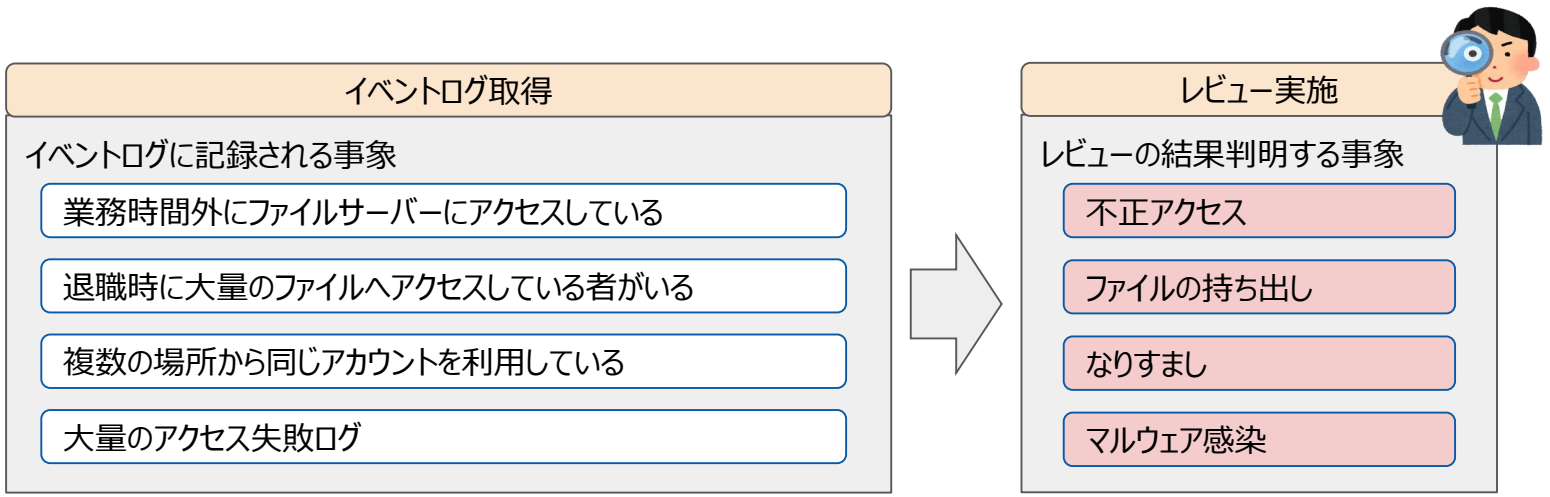
3-3. イベントログのレビューの目的

C･I･Aに影響を与える事象は、ログをレビューして認識する
ログレビューの目的は「原因調査」、「問題発見」、「予防」に分類

システムは、機密性(C)・完全性(I)・可用性(A)を維持するため、定期的にログをレビューすることが求められます。

ログのレビューの目的は、大きく分けて以下の3種類に分類できます。

- （事件・事故の）**原因調査**
- （いつの間にか発生してしまっているかもしれない）**問題発見**
- （起きるかもしれない事件事故の）**予防**



3-4. 目的によるログレビューの視点の違い

目的によりレビューの視点が違う！

ログのレビューの目的は3分類であり、まとめると以下の通り(詳細は次頁以降に明記)となります。

	原因調査	問題発見	予防
目的の解説	インシデントの解析に利用する	CIAの喪失が発生した事を事象が表面化する前に検知する	CIAの喪失につながるかもしれない事象の検知
レビューのタイミング	事件・事故発生時	定期レビュー	定期レビュー
調査の視点	・監視カメラのアーカイブ ・ハードウェアの動作ログ ・ネットワークトラフィックログ ・システム動作ログのアーカイブデータ ・バックアップ動作ログ	・監視カメラの映像 ・ハードウエアの動作ログ中の障害イベント ・ネットワーク異常検知 ・システムの異常終了イベント ・バックアップの失敗	・監視カメラの映像 ・ハードウエアの動作ログ中の機器内温度上昇イベント ・ネットワークの恒常的な過負荷 ・CPUやメモリの恒常的な高い使用率 ・バックアップ容量の低下

3-4-1. 「原因調査」のレビューの目的・視点

「原因調査」は、異常に対処するため

目的

システムに何か異常があることが分かった場合、「どのような異常なのか」、「どういう経緯で発生したのか」をたどる際、システムの動作記録(＝ログ)を確認(＝レビュー)し、異常の原因を調査することです(※)。

※多くの組織、運用者が認識しているログのレビューの目的はこれでしょう。

視点

問題発生前および発生時に何が起こったか(必要な場合、問題発生後どのような影響があったか)を確認することです。

例１：ハードウエアの故障時

・故障直前の操作、故障直前の機器温度、故障直前の負荷状況

例２：データベースシステム異常停止時

・異常停止直前の操作、異常停止直前の接続数、異常停止直前のシステム負荷

3-4-2. 「問題発見」のレビューの目的・視点

「問題発見」は、気付かない問題を発見するため

目的

システムのC・I・Aが損なわれていても、「操作中の画面に異常が出る」とか「機械が異音を発している」などの明確に目に見える現象がないと利用者や運用者がすぐに認識できるとは限りません。認識が遅れると、長期に渡って誤った処理が行われたり、大量の情報が漏洩してしまったりなど被害・損害が大きくなってしまうことがあります。しかし、多くの場合、問題が発生している時にはその状況がログとして記録されています。定期的にログを確認することで「気が付かない間に起こっていた問題を発見」できることがあります。

視点

問題になるようなイベントが発生していたかを確認することです。

例１：ハードウエアに異常がないかの確認

・想定外の時間での停止・再起動イベント、機器温度警告イベント、
動作指示に対する異常終了イベント、障害発生の警告イベント

例２:データベースシステムに異常がないか

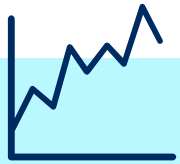
・想定外の時間での停止・再起動イベント、システムの異常終了イベント、容量超過のイベント

3-4-3. 「予防」のレビューの目的・視点

「予防」は、これから起きるかもしれない問題を発見するため

目的

定期的なレビューは、「起きているけれど気づいていない問題」の発見だけではなく、「まだ起きていない問題」の兆候の発見にも役立つ場合があります。システム上の問題の中には実際に被害・損害が発生する前に、なにかしらの兆候を伴うものがあります。こうした兆候を発見して問題(被害・損害)が発生する前に対処する(＝予防する)ことです。



視点

問題発生の予兆はあるかを確認することです。

例１ ：ハードウエアの故障予兆

・処理時間の推移、システム負荷の推移、機器温度の推移、代替セクタの急増(HDDの場合)

例２ ：データベースシステム異常の予兆

・システム負荷の推移、容量(メモリ・HDD)残量の推移

3-5. イベントログのレビューの対応ステップ

ログのレビューは取得成否から内容分析などのステップがある

イベントログへの対応は、最初から他のログと突合するような解析を行うことは難しいでしょう。複数のステップに分けて対応することとなります。

STEP1	**【ログが取れている事を確認】** ・意図したタイミングでの取得、文字化けやファイル長の不足などがないことを確認
STEP2	**【明らかな異常を確認】** ・普段見かけないエラー、大量のログなどの異常値を定期的に確認
STEP3	**【統計的な手法結果、傾向分析結果を確認】** ・外れ値などの統計的な情報、時間等の傾向を確認
STEP4	**【他のログと突合】** ・アクセス権限、勤務情報、作業申請などの情報と突き合わせて確認

※STEP毎のレビュー内容は次頁以降に示す

3-5-1. STEP 1

必要なログが取得できているかをレビュー

原因調査　問題発見　予防

イベントログが、組織の定める方針に従い**取得出来ているか**確認する必要があります。

必要な項目の取得漏れが発生していないかなど、以下の視点での確認が望まれます。

- ✓ **意図したタイミングで、意図したデータの取得ができているか**
- ✓ **文字化けやファイル長の不足がないか**

＜その他：特定の環境下で注意が必要な事例＞

- ✓ **SaaS サービス**では、ログの取得が**組織の目的にあった内容か**
- ✓ **冗長構成**により、IPアドレスが**内部IPに変換されていないか**
- ✓ **仮想サーバー**では、停止時に**ログが揮発していないか**

3-5-2. STEP 2

イベントログに明らかな異常が記録されていないかレビュー

原因調査　問題発見　予防

明らかな異常としては、下記のようなログがあります。

- ✓ 明らかな異常状態を示す、 **FATAL** や **ERROR** などのキーワード。
- ✓ **普段見かけないイベント**、イベント中に記載される数値に**極端に大きな値**があるなど。
- ✓ **時間外**、**休日**など、一般的に負荷が少ない時間帯の大量ログ。
- ✓ 日中帯など、明らかにアクセスが有る時間帯の**空白期間**。

3-5-3. STEP 3

統計的な手法などを用いてレビュー

原因調査　問題発見　予防

異常なログのレビュー手法には、下記のような方法があります。

- ✓ **頻度が多い項目**(※1)、**外れ値**(※2)などの統計的な情報を確認。
- ✓ 日毎や、週毎のログの**時間による傾向（トレンド）分析**。
- ✓ ユーザーごとのログの**人による傾向（トレンド）分析**。
- ✓ キーワードによる**抽出分析**。

※1 頻度が多い項目：ここではイベントログとして数多く出力されるログを示す。
※2 外れ値：ここでは通常では記録されない数値等を示す。例えば、定時間外に入退場記録があるなど。

3-5-4. STEP 4

他のログと突合し、多面的にレビュー

原因調査　問題発見　予防

突合の方法としては、下記のような方法があります。

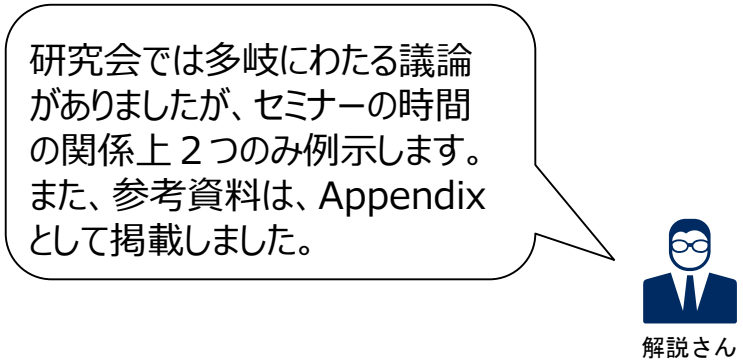
- ✓ **アクセス権限**、**勤務情報**、**作業申請**などの情報と突き合わせて確認。
- ✓ 入館申請書などの**紙の情報**と突き合わせて確認。
- ✓ 作業申請やアクセス申請と、**実際のアクセス先**を突き合わせて確認。
- ✓ **AIにより分析**。

4章　ログにまつわる事例

4-1. ログ活用の事例

本章では、ログのレビューについて、事例を見ていきます。

- ファイルサーバのログ
- メールサーバのログ



4-2. ファイルサーバのログ

4-2-1. ファイルサーバのイベントログ

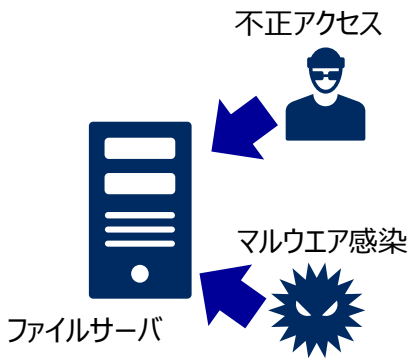
イベントログを確認し、ファイルサーバのC・I・Aを維持する

ファイルサーバには以下のようなログがあります。

また、イベントには、誰が、いつ、何をしたかが記録されます。

これをレビューすることで、組織の方針にマッチしない異常な動作を確認し、ファイルサーバの機密性・完全性・可用性を維持します。

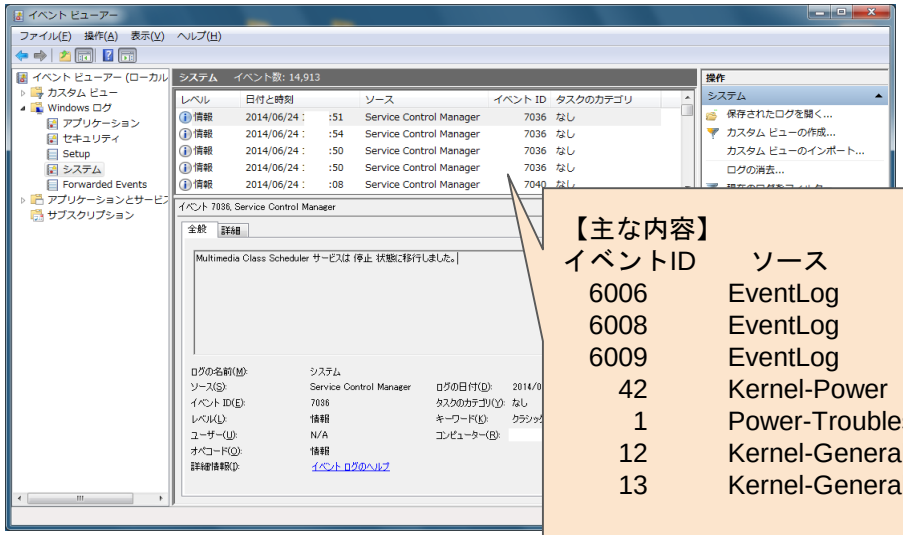
- ✓ **キャパシティ**：HDD、メモリ、CPU ⇒ 4-2-3項
- ✓ **バックアップ**：テープやストレージへのバックアップの成功/失敗 ⇒ 4-2-4項
- ✓ **ファイル操作**：ファイルアクセス(削除、コピー) ⇒ 4-2-5項
- ✓ 認証結果：ログイン成功/失敗(それは、誰が、いつ)
- ✓ トラフィック：大量のアクセスの有無
- ✓ マルウエア感染：ウイルス対策ツールの結果　　etc.



4-2-2. Windows Event Viewer

一例を示します。これは、Windows Event Viewerです。
Windowsに標準搭載されているログツールです。
アプリケーション、セキュリティ、セットアップ、システム等のログが取得されており、各種ログのレビューに活用できます。
ログを定期的にレビューすることにより、キャパシティ不足などを予防的に検知することが可能です。
次ページ以降でこのようなツールを使ったログ取得事例を紹介します。
※記載するツールについてはAppendix A2項を参照ください。

画面イメージ（例）



【起動方法】
「コントロールパネル」→「システムとセキュリティ」→「管理ツール」→「イベントビューアー」
※Event IDでフィルターして、検索することが出来ます。

【主な内容】

イベントID	ソース	概要
6006	EventLog	正常にシャットダウン
6008	EventLog	正常にシャットダウンせずに終了
6009	EventLog	起動時にブート情報を記録
42	Kernel-Power	スリープ状態になったとき
1	Power-Troubleshooter	スリープ状態から復帰したとき
12	Kernel-General	OS起動時
13	Kernel-General	OSシャットダウン時

4-2-3. ファイルサーバのキャパシティ状況

事例

【可用性の損失の予防】
キャパシティが不足し、**サーバが停止**することを予防する。

システムとイベントログ

ログ管理対象	キャパシティ（サーバの容量、パフォーマンス(能力)など）
使用ツール	Zabbix
取得ログの種類	「HDD使用量」、「メモリ使用率」、「CPU使用率」 など
分析の観点	【HDD容量】 ディスク容量の枯渇により、データの保存ができなくなる、あるいは異常動作する。 【Swap / 仮想メモリ】 物理メモリが不足すると、Swap / 仮想メモリを使用し、パフォーマンスが著しく低下する。 【CPU Load Avg.】 CPUが飽和し場合、パフォーマンスの低下が発生する。

4-2-4. ファイルサーバのバックアップ結果

事例

【完全性の問題発見】
バックアップが失敗し、**完全性が損なわれる事象**を検知する。

システムとイベントログ

ログ管理対象	バックアップ結果
使用ツール	Windows Event Viewer
取得ログの種類	「バックアップ取得状況(成功、失敗)」に関するログ
分析の観点	【Event ID 25 (VolSnap)】 バックアップ保存先が差分データに対して不足しており、 バックアップが失敗したことを通知する。 容量のチューニングが必要となる。 【Event ID 33 (VolSnap)】 バックアップの上限値に対して差分データが大きく、 正常に取得されなかったことを通知する。 設定の見直しが必要となる。

4-2-5. ファイルサーバへのアクセス状況

事例

【機密性の問題発見】
夜間などの**業務時間外にファイルサーバにログイン**し、給与や人事情報などの**機密性が高いファイル**を不正操作する事を検知する。

システムとイベントログ

ログ管理対象	ファイル操作
使用ツール	Windows Event Viewer、Excel
取得ログの種類	「ログイン時刻」、「アクセス先ファイル」 など
分析の観点	【Event ID 560 (Security)】 ファイルのアクセスに関するログで、時刻、ユーザID、対象ファイルなどの情報が含まれる。 Excelなどで、時刻とアクセス数、時刻とアクセス先などで分析し、時間外にアクセスが多い、時間外に機密情報へアクセスしているなどの分析を行う。 夜間のアクセスや、退職者などは、注意して確認する必要があります。

4-3. メールサーバのログ

4-3-1. メールサーバのイベントログ

メールは外部との接点。情報のC・I・Aを維持しよう！

メールサーバは、組織の内部と外部を繋いでいるシステムです。

組織の情報を維持するために、以下のログをレビューすることが望まれます。

ログを分析することで、インシデント事象を事前に検知が可能です。

- ✓ **情報漏えい**：大量のデータ送信が無いか ⇒ 4-3-2項
- ✓ **不審メール**：なりすましなど怪しいメールではないか ⇒ 4-3-3項
- ✓ 不正な通信：機密性の高いファイルが社外へ送信されていないか
- ✓ 不適切な利用：私用など不適切な利用がないか　　etc.

4-3-2. メールサーバでの”情報漏えい”

事例

【機密性の問題発見】
電子メールでの**「誤送信」や「ファイル誤添付」による機密性が損なわれる事象**を発見する。

システムとイベントログ

ログ管理対象	不必要な送信先
使用ツール	PowerShell、Excelなど
取得ログの種類	メール送信準備中や送信済の「送信先メールアドレス」、「メール添付ファイル」など
分析の観点	【例：Postfixの場合】 postfix/qmgr　postfix/smtp メール転送に関するログが記録されています。 from、to、size などの項目で重要な情報が記録されてます。 送信先として不必要な、もしくは不適切なもの、そしてメーリングリスト アドレスによる送信者の意図しない送信先が含まれている場合もあり得る ため、特に組織の外部への送信についてレビューすることが重要となります。 メール転送ソフトは、複数の行にまたがりログが記録されるため、 統合し、レビューすることが重要となります。

4-3-3. メールサーバでの“不審メール“

事例

【完全性の問題発見】
メールが、**第三者に“なりすまし”され完全性が損なわれていないか**を発見する。

システムとイベントログ

ログ管理対象	不審メール
使用ツール	Outlook、PowerShell
取得ログの種類	送信元や送信先、経路を特定する為の「メールのヘッダー情報」など
分析の観点	Received: ヘッダーには、メールの転送履歴が記録されています。 メールは、相手方メールサーバーから直接到達する事が多いため、 不審な経由をしている場合、なりすましの可能性があります。 Authentication-Results: ヘッダーには、相手方メールサーバーの なりすましに関する確認の結果が保存されています。 不審なメールの場合、拒否理由や、注意を必要とする理由が 記載されます。

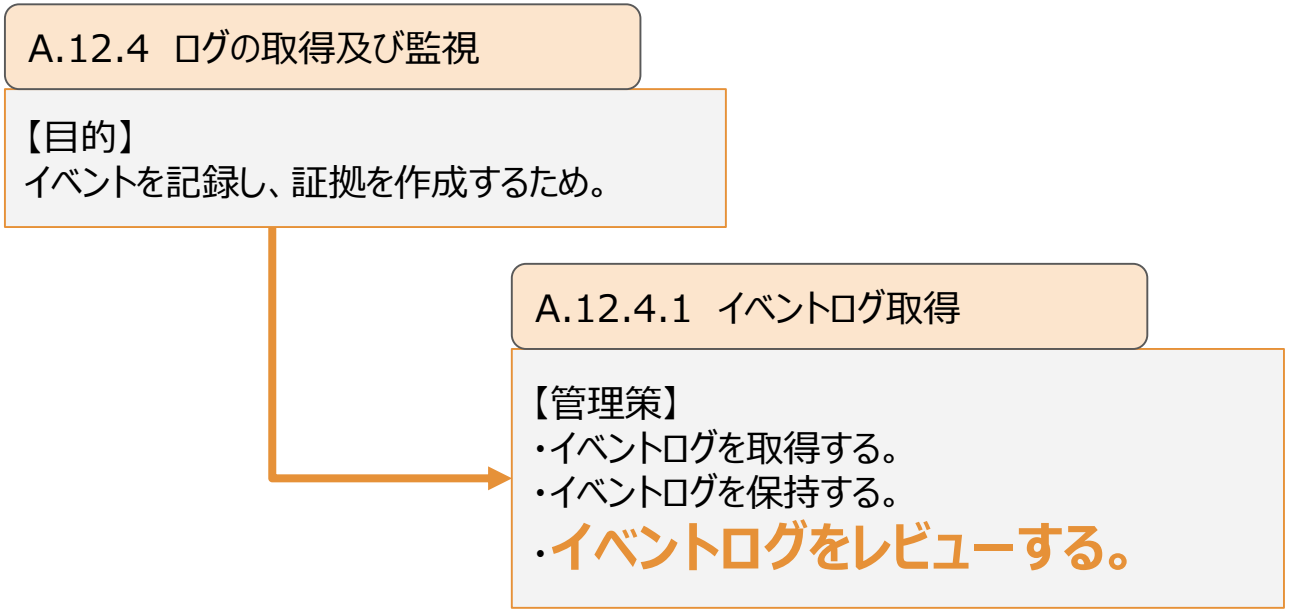
5章　まとめ

5-1. イベントログのレビューについて

イベントログのレビューは、自ら実施できる！

イベントログのレビューについて具体的な実例を紹介致しました。
ログのレビューは、高価な解析ソフトや、専門家に依頼しなくても、自組織で十分に実施(実装)出来ることが確認できました。

『ログが取得されているか』、『明らかな異常は無いか』を確認することから、ログのレビューを始めてみるとよいでしょう。



5-2. ログ取得・管理はやれるところから

組織におけるログ取得の実装はやれるところからスタート！

本研究会では以下を確認しておくことが必要であると確認しました。

◆ ログ管理の目的の明確化

組織としてログ管理の目的を明確化する。
目的が曖昧では何の為のログ管理か分からず、何となく取得しているだけとなる。
目的を明確化することで、その達成のために必要な環境を整備しやすくなる。
（例）情報漏えい防止のため

◆ 取得するログを決定

組織において取得するログを決めておく。（優先順位を決めて決定する）
目的が決まれば、取得するログも自ずと決まる。
（例）外部通信のログ（プロキシサーバログなど）

◆ ログの保存期間を決定

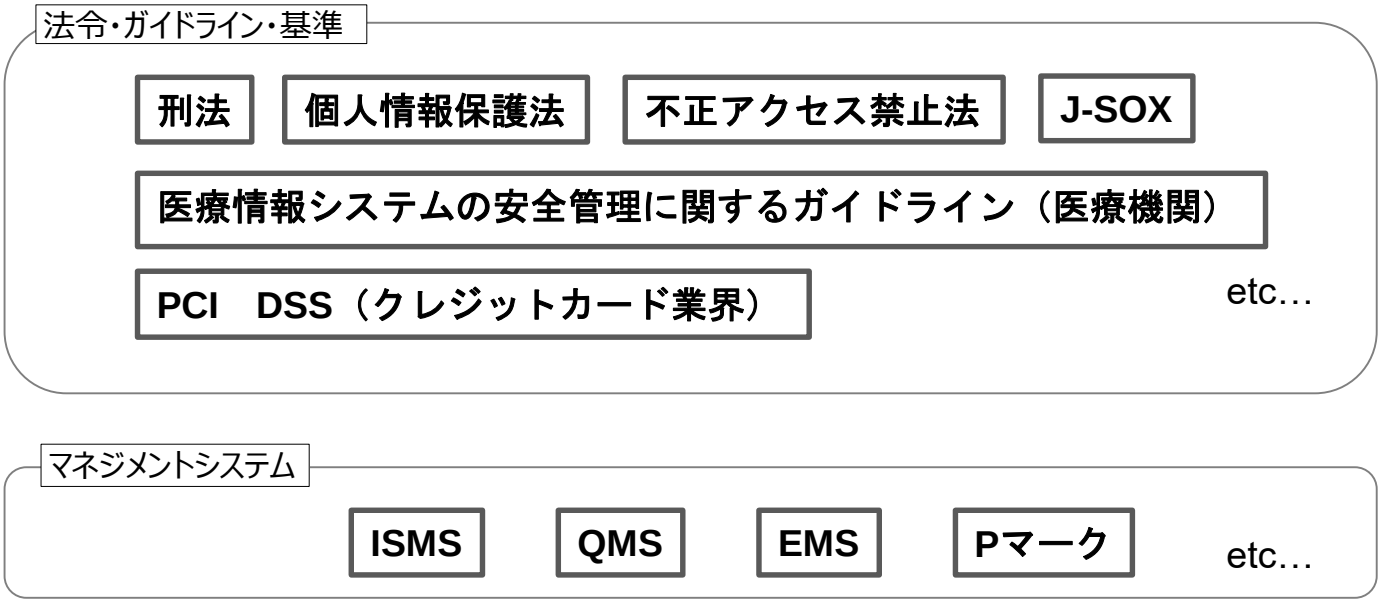
組織の目的、法規制で求められる要件を参考に保存期間を決定する。
（例）プロキシサーバ：1 年

5-3. イベントログをレビューすることで..

イベントログのレビューで、法令等にも対応

イベントログの取得や管理は、ISMSのみならず各種法令やマネジメントシステムで、組織に求められております。

ログのレビューをすることで、これらの要求を満たすことも可能となります。



参考：PCI DSS におけるログの要件

クレジットカード業界のセキュリティ基準である PCI DSS では、

ログ取得について以下が明記されています。

> 10.3 イベントごとに、すべてのシステムコンポーネントについて
> 少なくとも以下の監査証跡エントリを記録する。
>
> 引用元：PCI DSS 要件とセキュリティ評価手順、バージョン 3.2.1

10.3.1 ユーザ識別

10.3.2 イベントの種類

10.3.3 日付と時刻

10.3.4 成功または失敗を示す情報

10.3.5 イベントの発生元

10.3.6 影響を受けるデータ、システムコンポーネント、またはリソースのIDまたは名前

参考：ログ保存期間

保存期間	法令・ガイドライン等
1か月間	刑事訴訟法 第百九十七条 3「‥業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、**三十日**を超えない期間を定めて、これを消去しないよう、書面で求めることができる。‥」
3か月間	サイバー犯罪に関する条約 第十六条 2 「‥必要な期間（**九十日**を限度とする。）、当該コンピュータ・データの完全性を保全し及び維持することを当該者に義務付けるため、必要な立法その他の措置をとる。‥」
1年間	PCI DSS 10.7「監査証跡の履歴を少なくとも **1 年間保持**する。少なくとも 3 カ月はすぐに分析できる状態にしておく‥」
3年間	不正アクセス禁止法違反の時効
5年間	電子計算機損壊等業務妨害罪の時効
7年間	電子計算機使用詐欺罪の時効
10年間	不当利得返還請求権の時効

参考：「企業における情報システムのログ管理に関する実態調査」報告書について（IPA　2016年6月9日）
https://www.ipa.go.jp/security/fy28/reports/log_kanri/index.html

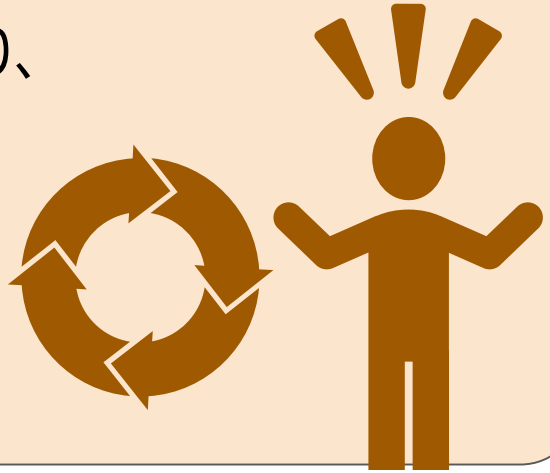
6章　さいごに

6-1. さいごに

各組織の継続的改善に向け、本研究会の報告がお役に立ちますと幸いです。

Before：ログをどうレビューすれば
いいのかわからない。

After：各組織のログレビュー手法により、
具体的なツールも把握した！
継続的改善に向け運用を行う！



6-2. 2019年テーマ２の研究会活動の成果

インプリメンテーション研究会では約1年にわたり、**「ログレビュー」**に関する議論を重ねてきました。
本テーマについて、全てを議論するには至ってはおりません。継続的に議論をしていく予定ですので、是非とも、皆様と同じテーブルで一緒に情報を共有しましょう！

STEP1. 研究テーマの選定

管理策を組織に実装する際の具体的な事例を示すとした。
「イベントログ取得」の管理策を選定。
イベントログは「取得」、「保持」している。「レビュー」はどこまでやれば良いのだろう？とし議論開始。

STEP2. ログのレビューの目的を整理

ログのレビューの目的を3つに分類した。

- （事件・事故の）**原因調査**
- （いつの間にか発生してしまっているかもしれない）**問題発見**
- （起きるかもしれない事件事故の）**予防**

STEP3. 研究会メンバで成果を取りまとめ

✓ 今すぐにでも実施可能なログレビューの手法を共有

⇒ **ログレビューは自組織で十分に実施できる！**

6-3. 継続検討事項

2019年のテーマ2では「ログレビュー」について議論しました。

本日の報告会では、時間の関係からも以下については、大きく触れませんでした。しかし、本研究会ではメンバ各位から多数多様の意見・議論があり、以下はその一例です。引き続き、継続検討を予定していきます。

- **大量のログの中でどこに注目すればよいか**
  - ITベンダに頼らずに自らどこまで実施するか、すべきか
- **不正なログの閾値はどう決めるのか**
  - 特異点を特定して不正なログを把握すれば良いが、不正と正常の閾値はどのように決めるべきか（誤検知もある…）
- **多要素認証におけるログ管理**
  - ID/PWから2要素（2段階）認証へ。ログ管理が忙しい…
- **アラート通知（メール、パトライト）**
  - 不正な通信を検知した際には自動遮断。生産工場では無理…

研究会活動について

是非とも、本研究会へ参加いただき、実際の議論の場を体験し、自組織の課題解決に繋げて頂ければと思います。

〔連絡先〕
日本ネットワークセキュリティ協会（JNSA）
標準化部会　日本ISMSユーザグループ
URL　：　https://www.jnsa.org/

Appendix

※以降の資料は参考資料です。セミナーでのご説明は割愛させて頂きます。

A1.応用編
インシデントにおけるログの活用

A1-1. インシデントにおけるログの活用①

インシデント例:業務用スマホの紛失

ログは、適切にレビューをすることにより、

インシデントの調査に活用することが出来ます。

社員から組織支給の**業務用スマホの紛失インシデント**の

報告があったようです。

ログを活用する事により実施可能な管理策を例示いたします。

A1-1-1. スマホ位置情報の確認

事例

【可用性の原因調査】
スマートフォンが、現時点でどこに有るかの原因を調査する。

システムとイベントログ

ログ管理対象	スマホの位置情報
使用ツール	ブラウザ、位置情報サービス
取得ログの種類	携帯キャリアのスマホの位置情報や追跡ログ
分析の観点	通常、ログの調査というと自組織で取得したログを対象と考えがちですが、 事件・事故の状況によっては外部の事業者が取得しているログを 活用する方法もあります。 スマートフォンは、設定により位置情報をアカウントに 記録することが可能です。 このログはブラウザから閲覧可能であり、過去の位置や、現在の位置を ブラウザからリアルタイムに確認することが出来ます。 盗難の場合は犯人の行動情報を確認することが可能です。

A1-1-2. スマホの発信ログの確認

事例

【機密性の問題発見】
スマートフォンから、不審な発信がないかの問題を確認する。

システムとイベントログ

ログ管理対象	スマホの通信
使用ツール	ブラウザ、発信ログサービス
取得ログの種類	携帯キャリアの通話相手先や通話時間のログ
分析の観点	通常、ログの調査というと自組織で取得したログを対象と考えがちですが、 事件・事故の状況によっては外部の事業者が取得しているログを 活用する方法もあります。 携帯キャリアは、追加の契約により発信ログを取得することが可能です。 このログを確認することにより、電話が発信されてない事や、 発信された場合は、相手先番号や通話時間などを確認することが 可能となります。

A1-1-3. 公共交通機関の入場記録や決済記録

インシデントにおけるログの活用①

事例

【機密性の問題発見】
不正な電子決済や、公共交通機関などの利用がないかの問題を確認する。

システムとイベントログ

ログ管理対象	公共交通機関への入場、決済
使用ツール	ブラウザ、決済サービス
取得ログの種類	公共交通機関への入場記録、決済機関が保持する決済記録
分析の観点	通常、ログの調査というと自組織で取得したログを対象と考えがちですが、 事件・事故の状況によっては外部の事業者が取得しているログを 活用する方法もあります。 スマートフォンで電子決済や、公共交通機関のICカード情報を 紐付けている場合、決済や入場の記録を確認することが可能です。

A1-1-4. リモート接続サーバへのアクセスログ

事例

【機密性の問題発見】
リモート接続サーバに不正に接続がされていないかの問題を確認する。

システムとイベントログ

ログ管理対象	サーバへのリモートアクセス
使用ツール	Windows Event Viewer、PowerShell など
取得ログの種類	リモートアクセスサーバへのアクセス記録
分析の観点	リモートアクセスサーバの接続ログを保存している場合は、 紛失した時間以降に接続があったか追跡することが可能です。 紛失したユーザのアクセスだけでなく、 同一IPからの多数のアカウントへのログイン試行などにも 注目して確認する必要があります。 イベントID 200 (TerminalService-Gateway) ・接続した時刻 ・利用したアカウント ・接続元IPアドレス

A1-2. インシデントにおけるログの活用②

インシデント例:端末のウイルス感染

社員から業務用パソコンのウイルス感染インシデントがあったようです。

ログを活用する事により実施可能な管理策を例示いたします。

A1-2-1. HTTPやHTTPS経由での情報漏えい

事例

【機密性の問題発見】
プロキシサーバから組織外への情報流出。

システムとイベントログ

ログ管理対象	プロキシサーバ
使用ツール	Powershell、Excel
取得ログの種類	アクセスログ
分析の観点	Apache や Squid などの プロキシサーバのログには、 通信元のIPや、通信先のHost名、通信サイズが記録されています。 これらの情報を活用することで、どこから不正侵入(ウイルス感染)したかなどの、 情報を取得することが可能となります。 通信サイズが大きい通信などでは、外部へのデータ送信を行っている 可能性があります。 近年ではEnd to End暗号化がされることが多いため、クライアント型の 監査ソフトを入れることで、詳細を確認することが可能となります。

A2.ログ分析に利用するツール（例）

A2-1. Windows Event Viewer

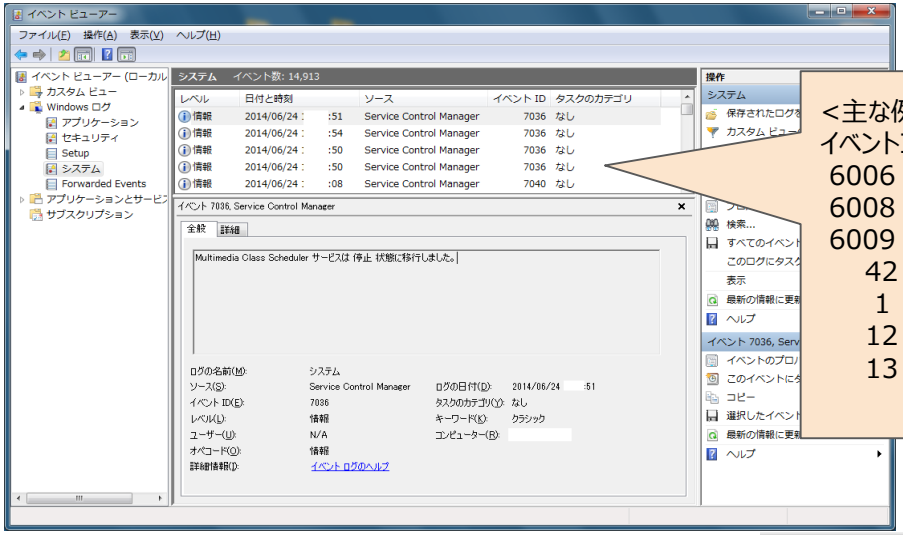
ツールの概要

Windows Event Viewerは Windowsに標準搭載されたログツールです。
アプリケーション、セキュリティ、Setup、システム等のログが取得されています。

操作方法

【起動方法】
「コントロールパネル」→「システムとセキュリティ」→「管理ツール」→
「イベントビューアー」

Event IDでフィルターして、検索することが出来ます。



<主な例>

イベントID	ソース	概要
6006	EventLog	正常にシャットダウン
6008	EventLog	正常にシャットダウンせずに終了
6009	EventLog	起動時にブート情報を記録
42	Kernel-Power	スリープ状態になったとき
1	Power-Troubleshooter	スリープ状態から復帰したとき
12	Kernel-General	OS起動時
13	Kernel-General	OSシャットダウン時

A2-2. evntwin

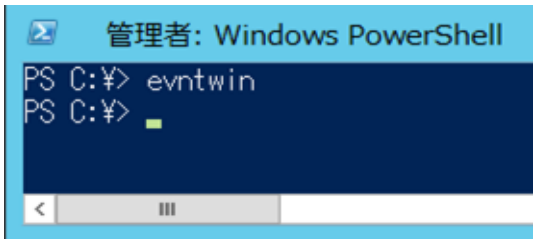
ツールの概要

イベントトラップトランスレーター （evntwin.exe）は、WindowsのSNMP Service に
付属しているコンポーネントでイベントトラップができます。

操作方法

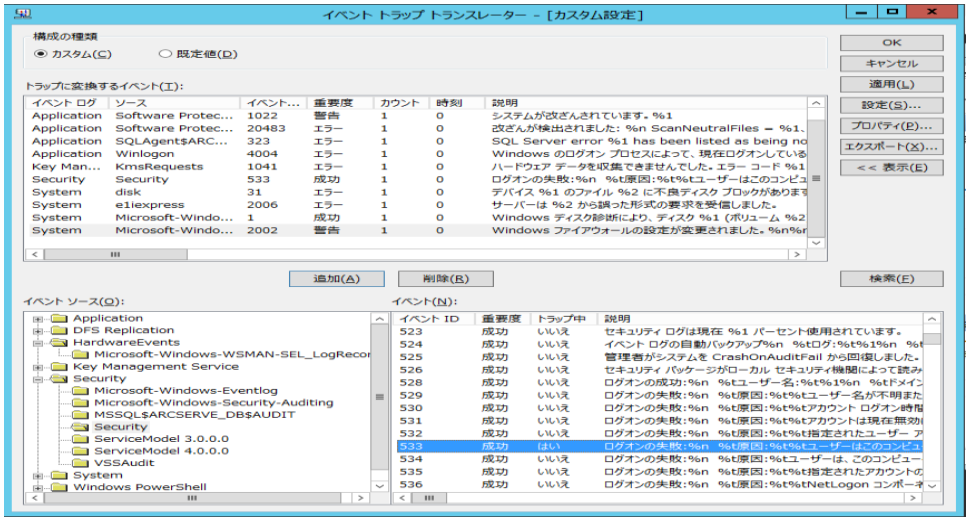
特定のソースやイベントIDがイベントログに記録された場合に、SNMPトラップを
発生させ管理者へ通知できます。膨大なログから指定のイベントをチェックできるので、
これにより日々のチェックの手間軽減や、チェック洩れを防ぐ等が期待できます。

＜evntwinの起動＞



powershellプロンプトより
evntwinを実行

＜evntwin画面イメージ＞



A2-3. Message Analyzer

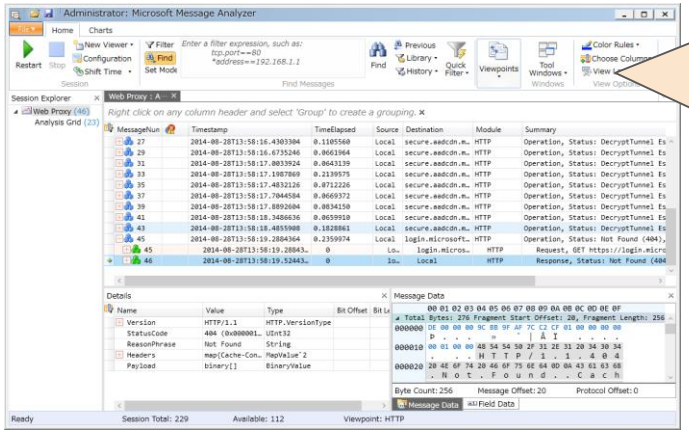
ツールの概要

Message Analyzerは、Microsoftが公開しているネットワーク解析ツールで、
パケットキャプチャとログ解析ができます。

操作方法

複数の「トレースシナリオ（Trace Scenarios）」が組み込まれており目的に沿った
シナリオを選択してプロトコル／メッセージをキャプチャし、キャプチャデータを
オンラインまたはオフラインで分析することができます。
また、Windows標準コマンド（netsh）で取得したパケットキャプチャログも取り込んで
解析ができます。

＜ Message Analyzer画面イメージ１＞



この「Microsoft Message Analyzer」は、
「Microsoft Network Monitor」の後継ツール。
主な機能として

- Windowsのイベントトレース機能『Event Tracing for Windows（ETW）』を活用して
- トレースログを採取し、フィルター機能で絞り込んだり、
- 『ビューポイント（Viewpoints）』機能で視点を切り替えて分析したり、
- チャート機能で可視化したりすることが可能。
- ネットワークのみならず、USB/Bluetooth デバイスや『SMB』などのファイル共有のトレースにも対応している。

A2-4. Zabbix

ツールの概要

Zabbix は、オープンソース(※)の統合監視ツールです。
サーバ / ネットワーク / アプリケーションなどを集中監視し、
アラート通知 / パフォーマンス可視化などが行えます。

※オープンソースの注意事項はｐ.67を参照

操作方法

統合監視ツールとして必要な機能を網羅的に搭載しており、監視 / 障害検知 / 通知機能などが行えます。Web管理画面でグラフやアイコン等での可視化も可能。
また、様々なプラットフォーム（Linux / Windows / SNMP対応ネットワーク機器など）に
対応可能なので、システム全体を1つの Zabbix で監視が可能です。

＜ Zabbix 画面イメージ１＞

＜ Zabbix 画面イメージ２＞

A2-5. Wireshark

ツールの概要

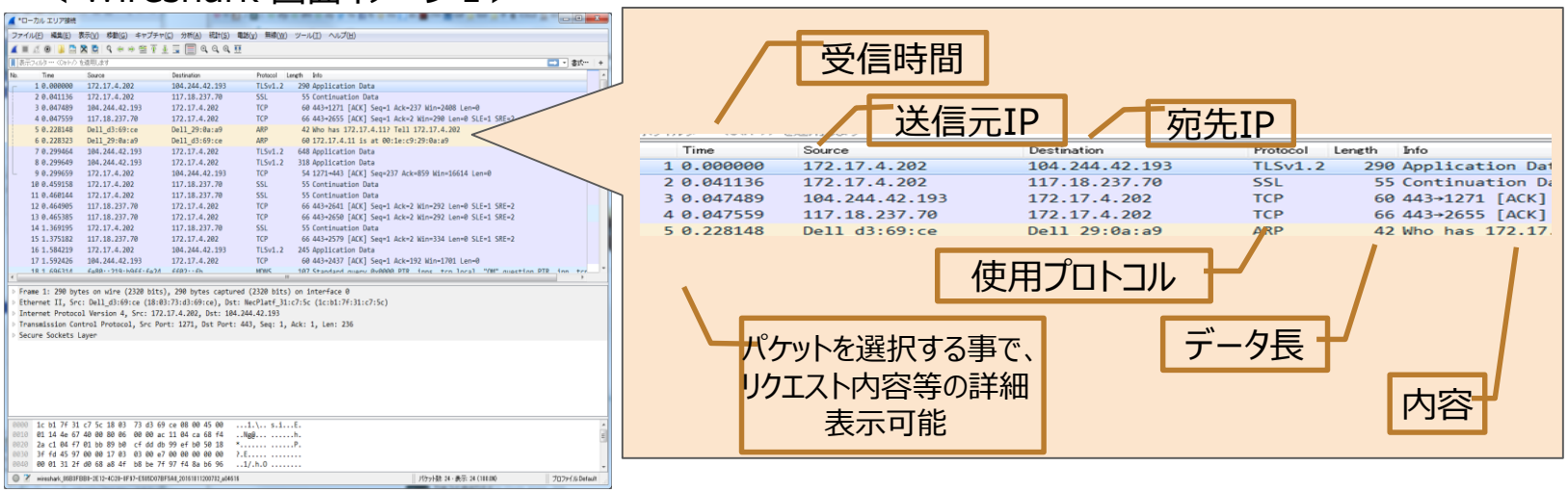
Wireshark は、ネットワーク解析ツール(オープンソース(※))でネットワークプロトコルアナライザ（パケット取得/プロトコル解析ツール）です。

※オープンソースの注意事項はｐ.67を参照

操作方法

このツールはネットワーク解析に十分な機能を備えており、ネットワーク解析を
行うための定番ツールとなっています。
ネットワークインターフェイス上を通過するパケットをキャプチャして解析します。
また、様々なプラットフォーム（Windows / Mac OS X / Linux）で利用が可能です。

＜ Wireshark 画面イメージ１＞



（補足）オープンソースの注意事項

A2-4,A2-5ではオープンソースの“Zabbix”や“Wireshark”を紹介しました。
オープンソースは、開発費用を抑えられる、開発期間を短縮できるなど多くのメリットがありますが、以下のデメリットもあります。

・マニュアルが不十分
・開発元にバグ(脆弱性など)の法的責任はない
・開発元のサポートが受けられない場合が多い

その為、オープンソース利用時には、社内関係者(特に経営層)とデメリットも共有し、理解頂いた上での利用が望まれます。
また、IT部門としては、脆弱性が露見した際などにどのように対応するかを事前にマニュアル化しておき、万が一の為の事前準備を十分に行うことが望まれます。

A2-6. SysmonSearch

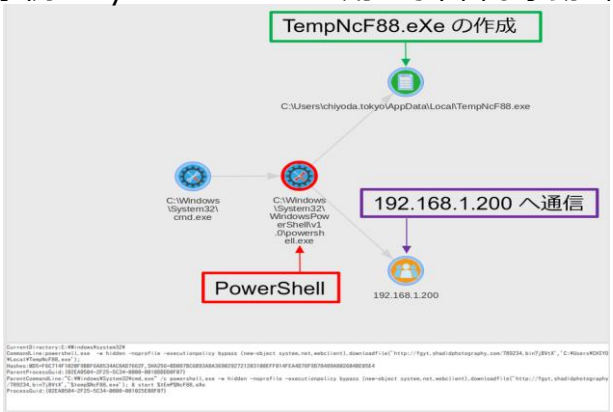
ツールの概要

SysmonSearchは、JPCERTコーディネーションセンター(JPCERT/CC）が公開している
ログ管理・解析ツールです。

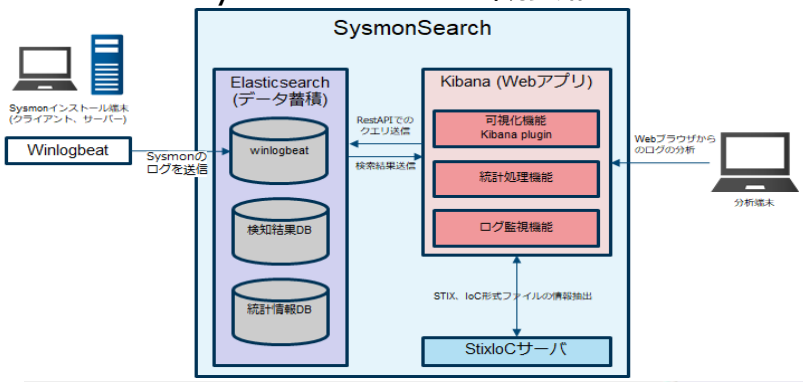
操作方法

Microsoftが提供するWindowsのログ収集ツール「Sysmon」から出力されるログを
管理・解析できるツール「SysmonSearch」です。
このツールではサイバー攻撃を受けたとき等、複数の端末のログを一元的に管理し
解析ができます。

＜SysmonSearch画面イメージ１＞
事例：SysmonSearchを用いて不審な挙動を調査



＜SysmonSearchの概要構成＞



A2-7. Excel

ツールの概要

Excelの関数やグラフを活用することで可視化が可能となります。

操作方法

COUNTIFS 関数を使うと特定の条件（9時から10時など）のログ件数を調べることが可能です。
『散布図』と組み合わせることで、24時間の間の変化を可視化することが可能です。

A2-8. PowerShell

ツールの概要

Windowsに搭載されたコマンド、PowerShellを活用することで、大量のログに対して
条件での検知や、ログのCSV化が可能です。

操作方法

Get-Content
　大量のログファイルを統合して検索することができます。
Select-String
　ファイルから特定の文字を含む行を抽出できます。
Set-Content
　抽出結果を別のファイルに保存出来ます。

以上