Tokio Marine Holdings

Internet Week 2022

C45：Cyber Hygiene Hunting

～セキュリティ実効性確認のすすめ～

2022年11月25日

東京海上ホールディングス株式会社

IT企画部 リスク管理G

石川 朝久, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP

自己紹介：石川　朝久（いしかわ　ともひさ）

- **所属　：東京海上ホールディングス株式会社　IT企画部　リスク管理グループ**
- **専門　：不正アクセス技術・インシデント対応・セキュリティ運用・グローバルセキュリティ戦略 etc.**
- **資格　：**博士（工学）, CISSP, CSSLP, CISA, CISM, CDPSE, CFE, PMP, 情報処理安全確保支援士, AWS Security, GIACs
- **経歴　：**
  - 2009.04 – 2019.03　　：某セキュリティ企業
    - 脆弱性診断・侵入テスト（Red Team）・インシデント対応・脆弱性管理・セキュア開発、セキュリティ教育 etc.
    - １年間、米国金融機関セキュリティチームに所属した経験あり
  - 2019.04 – 現在　　：東京海上ホールディングス株式会社
    - CSIRT運用・脅威インテリジェンス分析・グローバルセキュリティ戦略・国内外グループ企業のセキュリティ支援 etc.
- **対外活動（抜粋）：**
  - SANSFIRE 2011 Speaker（2011）
  - DEFCON 24 SE Village Speaker (2016)
  - Internet Week 2018 - 2020 (2018-2020)
  - IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）
  - IPA 「10大脅威執筆者会」メンバー（2010～2014, 2019~）
  - オライリー社『インテリジェンス駆動型インシデントレスポンス』翻訳（2018）
  - オライリー社『初めてのマルウェア解析』翻訳（2020）
  - オライリー社『詳解　インシデントレスポンス』翻訳（2022）
  - オライリー社『マスタリング Ghidra』監訳（2022）
  - 技術評論社　『脅威インテリジェンスの教科書』執筆（2022）

本日お伝えしたいこと

テーマ：Cyber Hygiene Hunting（Cyber Hygiene + Hunting を組み合わせた造語）

背景：

- 適切なセキュリティ態勢を実現するためには、**Cyber Hygiene**（サイバー衛生）が重要であることは良く知られています。 そのため、各社でさまざまなプロセスやポリシー、プログラムなどが準備しています。
- しかし、プロセスにおいて一つでも**ミス（Single Point of Failure）**があれば攻撃者に侵入されてしまいます。

→ セキュリティ態勢を能動的にチェックする手法が必要　→　**Cyber Hygiene Hunting**

アジェンダ：

- **Part I　　：理論編**
  - Cyber Hygiene Huntingの定義や必要となる背景、関連する概念についてご紹介します。
- **Part II　　：実務編**
  - Cyber Hygiene Huntingを実現するためのパラダイムシフトとスコープの考え方をご紹介します。
- **Part III　　：事例編**
  - 実例・具体的ツールなどを取り上げながら、Cyber Hygiene Huntingのやり方をご紹介します。

注意：

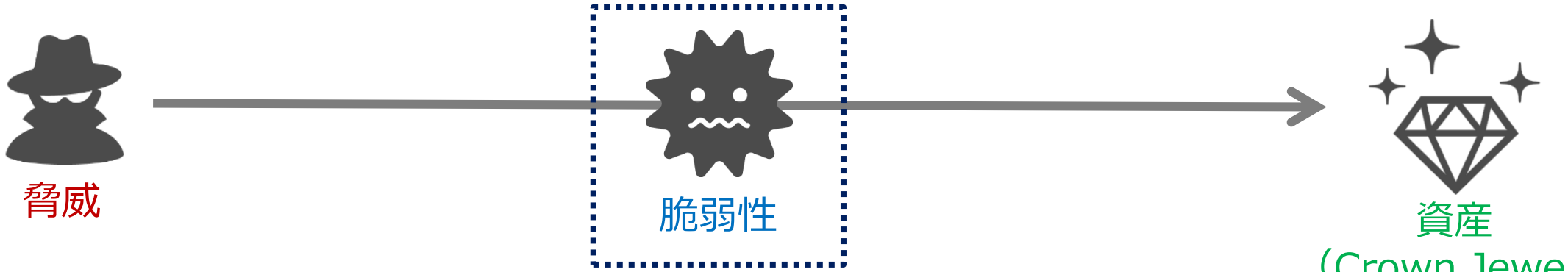
- 本内容は、全て講演者個人の見解を含んでおり、所属企業、部門、その他所属組織の見解を代表するものではありません。
- 製品名・ベンダー名・スクリプトなどが登場した場合、利用については各組織にて検証・判断をお願いします。

Part Ⅰ：理論編

セキュリティ管理のゴール

- セキュリティ管理のゴール：セキュリティリスクの低減

- **リスク = 脅威 × 脆弱性 × 資産**
  - リスクは３要素で定義されるが、（防御側が）コントロールできる要素は、「脆弱性」である。
  - 脆弱性を減らす試みは、Cyber Hygiene（サイバー衛生）として知られている。
    - CIS Critical Security Control（V8）が最も詳しく「何をすべきか？」を定義している。
    - https://www.cisecurity.org/controls/implementation-groups/ig1



「脆弱性」を減らす試み = Cyber Hygiene（サイバー衛生）

Cyber Hygieneを実現するため、
様々なプロセスやポリシー、プログラムが用意されている。


CONTROL 01
Inventory and Control of Enterprise Assets
5 Safeguards
IG1 2/5
IG2 4/5
IG3 5/5
CONTROL 02
Inventory and Control of Software Assets
7 Safeguards
IG1 3/7
IG2 6/7
IG3 7/7
CONTROL 03
Data Protection
14 Safeguards
IG1 6/14
IG2 12/14
IG3 14/14
CONTROL 04
Secure Configuration of Enterprise Assets and Software
12 Safeguards
IG1 7/12
IG2 11/12
IG3 12/12
CONTROL 05
Account Management
6 Safeguards
IG1 4/6
IG2 6/6
IG3 6/6
CONTROL 06
Access Control Management
8 Safeguards
IG1 5/8
IG2 7/8
IG3 8/8
CONTROL 07
Continuous Vulnerability Management
7 Safeguards
IG1 4/7
IG2 7/7
IG3 7/7
CONTROL 08
Audit Log Management
12 Safeguards
IG1 3/12
IG2 11/12
IG3 12/12
CONTROL 09
Email and Web Browser Protections
7 Safeguards
IG1 2/7
IG2 6/7
IG3 7/7
CONTROL 10
Malware Defenses
7 Safeguards
IG1 3/7
IG2 7/7
IG3 7/7
CONTROL 11
Data Recovery
5 Safeguards
IG1 4/5
IG2 5/5
IG3 5/5
CONTROL 12
Network Infrastructure Management
8 Safeguards
IG1 1/8
IG2 7/8
IG3 8/8
CONTROL 13
Network Monitoring and Defense
11 Safeguards
IG1 0/11
IG2 6/11
IG3 11/11
CONTROL 14
Security Awareness and Skills Training
9 Safeguards
IG1 8/9
IG2 9/9
IG3 9/9
CONTROL 15
Service Provider Management
7 Safeguards
IG1 1/7
IG2 4/7
IG3 7/7
CONTROL 16
Applications Software Security
14 Safeguards
IG1 0/14
IG2 11/14
IG3 14/14
CONTROL 17
Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
CONTROL 18
Penetration Testing
5 Safeguards
IG1 0/5
IG2 3/5
IG3 5/5

CIS Critical Security Controls Implementation Group 1

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the **CIS Critical Security Controls** (CIS Controls). CIS Controls v8 defines Implementation Group 1 (IG1) as essential cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

In most cases, an IG1 enterprise is typically small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. A common concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime.

The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

Below is a list of the CIS Controls in v8, and how many Safeguards in each are applicable to each Implementation Group.

新しいセキュリティ戦略：Adaptive Security

Adaptive Security：柔軟かつ臨機応変なセキュリティ態勢

- 脅威動向が日々変化していること、また既存のセキュリティ対策の回避手法が進歩しているため、シグニチャに頼った防御モデルが成立しない。

- 脅威に柔軟かつ臨機応変に対応できる**プロアクティブなセキュリティ態勢**を構築し、**サイバーレジリエンス**を実現する必要がある。

- そのためには、リスクの各要素に注目し、継続的なアプローチで対応をする必要がある。
  - リスクの各要素に注目した２種類の手法　：**Threat Hunting ＋ Cyber Hygiene Hunting**
  - 継続的なアプローチ　：**CM/CI（継続的モニタリング/継続的改善）**

Adaptive Securityの実現に向けて： 2種類のHunting手法

Adaptive Security：柔軟かつ臨機応変なセキュリティ態勢

→ 変化する脅威へ適切に対応できるためには、リスクの要素に着目したアプローチが必要

→ **Adaptive Securityを実現する2種類のHunting アプローチ**

<Adaptive Securityを実現するアプローチ>

	アプローチ1：*Threat Hunting*		アプローチ2：*Cyber Hygiene Hunting*
日本語	脅威ハンティング		実効性確認
定義	**既存のセキュリティ対策を回避する現在/過去の脅威を能動的・再帰的に調査**し、その情報を利用して**サイバーレジリエンスを向上**させること		**将来の攻撃につながるCyber Hygieneの状態・脅威へのセキュリティ態勢が適切に確保されているか能動的・再帰的に検証**し、**サイバーレジリエンスを向上**させること。
対象	脅威		脆弱性
視点	過去・現在		未来
調査対象	IoC（＝Indicator of Compromise）		EoC（＝Enabler of Compromise）
補足	Appendixを参照してください。		**今日の講演ではこちらを中心に扱います！**

Adaptive Securityの実現に向けて：２種類のHunting手法

Cyber Hygiene Hunting（実効性確認）とは？

- 将来の攻撃につながるCyber Hygieneの状態・脅威への**セキュリティ態勢**（*1）が適切に確保されているか検証するため、**EoC（Enabler of Compromise）**を探しだす。

  - 具体的には、**予防・検知・対応プロセスが適切に機能していることを検証**する
    - 例）脆弱性管理、アカウント管理、攻撃検知
      - 脆弱性管理プロセス、アカウント管理プロセス自体は定義されても、オペレーションミス、不明確な責任範囲、認識相違などから、運用が適切に実現できていない可能性がある。
    - 検証した結果（＝EoC）をファクトベースで押させていく。

  - *Cyber Hygiene Hunting* ≠ 脆弱性スキャン・ペネトレーションテスト・*TLPT*（*2）
    - 脆弱性スキャン・ペネトレーションテスト・TLPTもCyber Hygiene Huntingの一部ではあるが、より広範囲の調査することを想定している。
    - 具体的な対象については、後ほどご紹介！

（※１） セキュリティ態勢 ≠ セキュリティ体制
「体制」は組織体制そのもの、「態勢」は実際に機能が発揮されている状態にあることを意味します。

（※２）TLPT = Threat Lead Penetration Test（脅威ベースのペネトレーションテスト）
2017年11月に金融庁が発表した『平成29年度 金融行政方針』と2018年に発表した『諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書』というホワイトペーパーで提唱された概念です。より詳細は、金融庁のホワイトペーパーを参照してください。
- 金融庁：https://www.fsa.go.jp/common/about/research/20180516.html

Adaptive Securityの実現に向けて：CM/CI

Adaptive Security：柔軟かつ臨機応変なセキュリティ態勢

→変化する脅威へ適切に対応できるためには、継続的なアプローチが必要

→ **CM/CI（継続的モニタリング/継続的改善）**

＜継続的モニタリング & 継続的改善とは？＞

CM

Continuous Monitoring

継続的モニタリング

継続的にCyber Hygieneの状態、
予防・検知能力を確認・検証・
モニタリングすること

×

CI

Continuous Improvement

継続的改善

継続的モニタリングの結果に基づき、
改善を繰り返し進めていくこと

Part II：実務編

理論編の総括 ＋ 実務編

＜理論編の総括＞

- Adaptive Security：柔軟かつ臨機応変なセキュリティ態勢
  - 脅威に柔軟かつ臨機応変に対応できる**プロアクティブなセキュリティ態勢**を構築

  - そのためには、リスクの各要素に注目し、継続的なアプローチで対応をする必要がある。
    - **２種類のHunting手法　　：Threat Hunting ＋ Cyber Hygiene Hunting**
    - **継続的なアプローチ　　：CM/CI（継続的モニタリング/継続的改善）**

  → 今日は、Cyber Hygiene Huntingについてご紹介

＜実務編＞

継続的モニタリング/継続的改善を実現した*Cyber Hygiene Hunting*を行うためには？

- **ポイント１：３種類のパラダイムシフト**
  - 継続的かつ実効性をもったCyber Hygieneチェックを行うためには、３種類の新しい考え方が必要

- **ポイント２：Cyber Hygiene Huntingのスコープ**
  - Cyber Hygiene Huntingのスコープはどこに定めるべきか？

ポイント１：３種類のパラダイムシフト

CM/CIを実現するCyber Hygiene Huntingを行うためのパラダイムシフト

- **パラダイムシフト１：机上評価 → 実機評価へのシフト**
  - チェックリストによる確認など机上評価は、クイックに状況を確認できるメリットがあるが、プロセスの実運用面や実施上のミス（例：パッチ適用漏れ）などを検出することは難しい。
  - 実機評価へシフトし、現時点でのセキュリティ態勢を具体的に把握し、プロセス改善につなげていく。

- **パラダイムシフト２：ツール活用による データ化 + リアルタイム化**
  - ペネトレーションテストやTLPTなどは、年１回の定期実施が一般的（=スナップショットアプローチ）
    - 攻撃手法はより短いサイクルで登場し、脆弱性・アカウント管理は日々の運用でかなり変化してしまう。そのため、定期実施の結果ではセキュリティ態勢を適切に表現できているとは言えず、最新の脅威への対応が遅れてしまう。
  - そのため、継続的にモニタリング・チェックできる仕組み（=ツールの活用）を構築する。
    - ツールから取得したデータを根拠に改善活動を行うため、認識齟齬が生まれづらく、管理目標も設定しやすい。

- **パラダイムシフト３：標準的なフレームワークの活用**
  - 結果を標準的なフレームワーク（MITRE ATT&CK etc.）へ落とし込むことにより、共通言語化する。
    - MITRE ATT&CK = 攻撃手法を体系化したナレッジ集
  - これにより、様々な外部情報との比較・連携が実施しやすくなる。

ポイント２：Cyber Hygiene Huntingのスコープ

- **Cyber Hygiene Huntingのスコープはどこを対象とすべきか？**
  - **EOC（Enabler of Compromise）**を効果的に検出するために以下が候補に挙がる。

  - **Active Directoryのセキュリティ**
    - AD/AADの設定に何か不備がないか確認する。
  - **アカウントのセキュリティ**
    - 漏洩したパスワード文字列の利用・不適切な権限付与
  - **セキュリティコントロール（予防・検知）の失敗**
    - 既知の攻撃手法を適切に予防・検知できない。
  - **セキュリティ設定の不備**
    - 不要なポートの開放、S3バケットの公開、VPNの多要素認証
  - **脆弱性管理の不備**
    - 脆弱性の存在有無
  - **（標準から）逸脱した端末・ソフトウェア**
    - シャドーIT、標準外ソフトウェア、古いOSの存在

Part III：事例編

Cyber Hygiene Huntingの実際

- Part IIIでは、Cyber Hygiene Huntingの実例を示します。
  - 商用製品＋オープンソースツールを利用して行う方法もご紹介します。
  - 利用については各組織にて検証・判断をお願いします。

- **事例１：Active Directory**
  - Active Directoryを活用することで、ADのセキュリティやアカウントの管理状況、逸脱した情報を取得する。
- **事例２：コントロール不備の検証**
  - 実際に攻撃をテストすることにより、既に導入しているテレメトリー（センサー）が適切に反応するか検証する。
- **事例３：侵害調査**
  - ファストフォレンジック技術・脅威ハンティング技術を使って、侵害された痕跡＋Cyber Hygieneの情報を棚卸する。
- **事例４：SSPM**
  - クラウドセキュリティのセキュリティ態勢を確認する手法をご説明します。

事例 1 ：Active Directory + アカウント管理

実効性確認手法 事例１：Active Directory + アカウント管理

- Active Directoryは、標的型攻撃で非常によく狙われるシステムであり、適切な管理が重要！
  - 例）Golden Ticket、Silver Ticket、Kerberoasting、AS-REP Roasting、DCSync…
  - 例）Zerologon（CVE-2020-1472）、CVE-2021-42287/CVE-2021-42278

- ADを継続的モニタリングするツールを利用し、ADのヘルスチェックを行う！
  - ツールの具体例として以下の通り（評価は各自でお願いします）
  - 例）Attivo Network社 AD Assessor https://www.attivonetworks.com/product/adassessor/
  - 例）SpectorOps社 Bloodhound Enterprise https://bloodhoundenterprise.io/
  - 例）Tenable社 Tenable.ad https://www.tenable.com/products/tenable-ad
  - 例）PingCastle https://www.pingcastle.com/
  - 例）CrowdStrike社 Falcon ITP/ITD https://www.crowdstrike.jp/products/identity-protection/

- 参考）*ITDR：ID Threat Detection & Response*
  - Gartner社「2022年のセキュリティ／リスク・マネジメントのトップ・トレンド」として挙げている。
  - 侵害の多くは、IDの悪用が起点となるため、IDの利用を検知・対応するサービスが少しづつ登場している。

実効性確認手法 事例１：Active Directory

オープンソースで実施する方法：

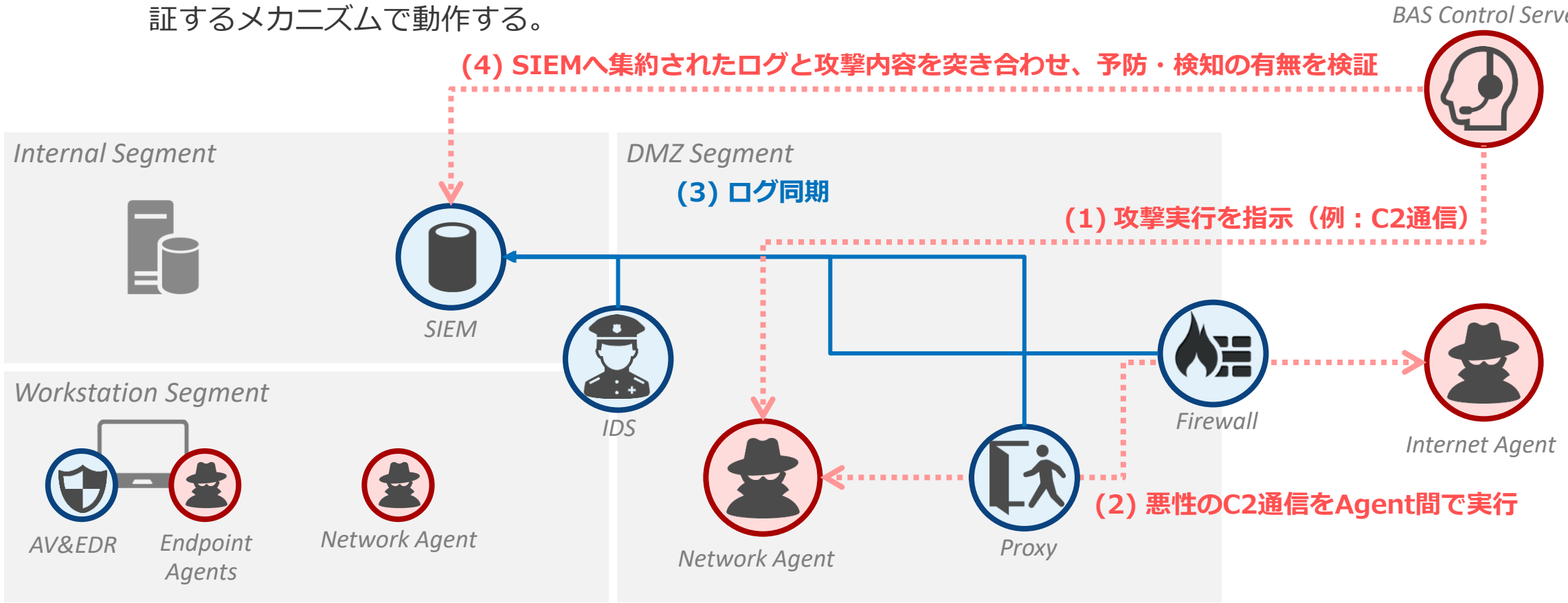
- PowerShellを利用すると、Active Directoryの様々な情報を取得できる。
  - 例）Get-ADUsers
  - 例）Get-ADComputer

- その他、様々なAudit Toolsも用意されている。
  - ADAudit
    - https://github.com/phillips321/adaudit
  - Active Directory Security Assessment
    - https://4sysops.com/archives/perform-active-directory-security-assessment-using-powershell/

事例２：コントロール不備の検証

実効性確認手法 事例２：コントロール不備の検証

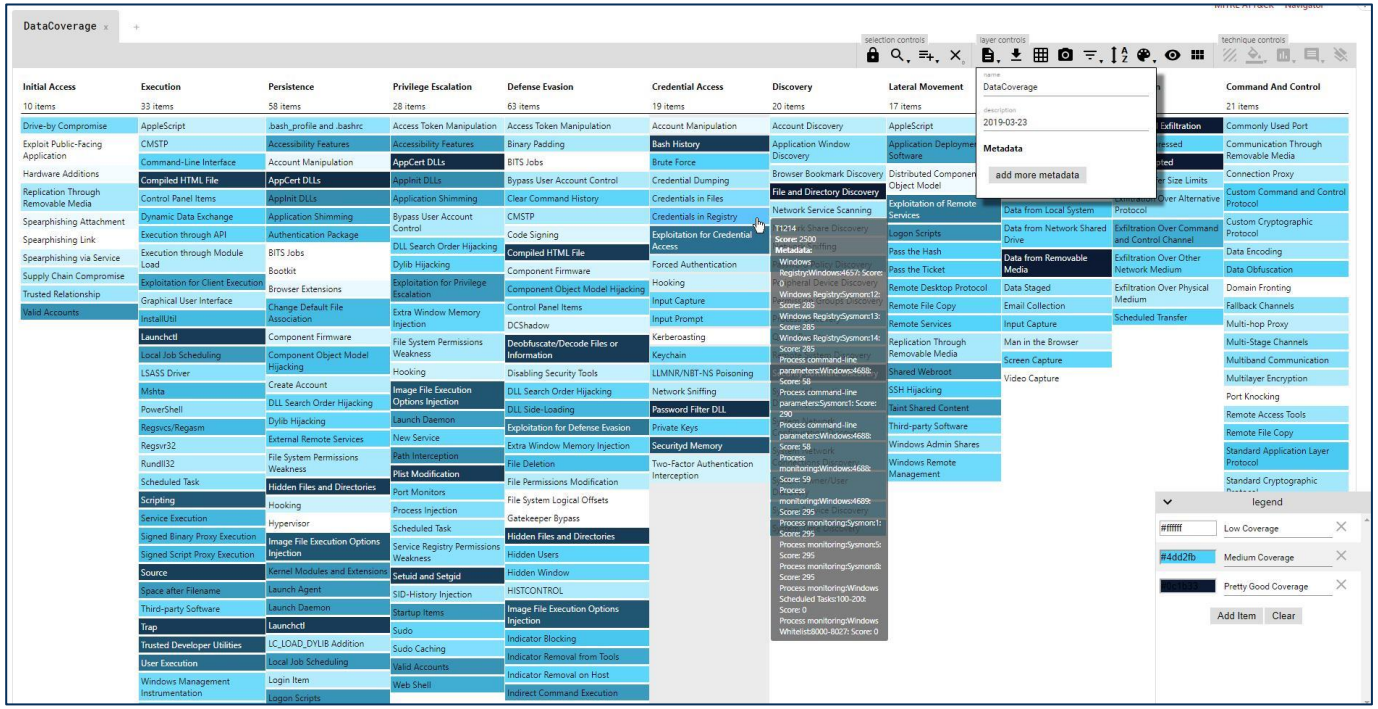
- **BAS（Breach & Attack Simulation）とは？**
  - 攻撃手法のエミュレーション（Adversary Emulation）をすることで、**セキュリティコントロールの有効性を検証**し、セキュリティ態勢を把握するツール。
  - 一般的な挙動：
    - BASは、Control ServerとAgent（Network・Endpoint）で構成されている。
    - 基本的には、Agent間で悪意のある挙動（Malicious Activity）を実行し、その予防・検知状況をSIEMと突合して検証するメカニズムで動作する。



実効性確認手法 事例２：コントロール不備の検証

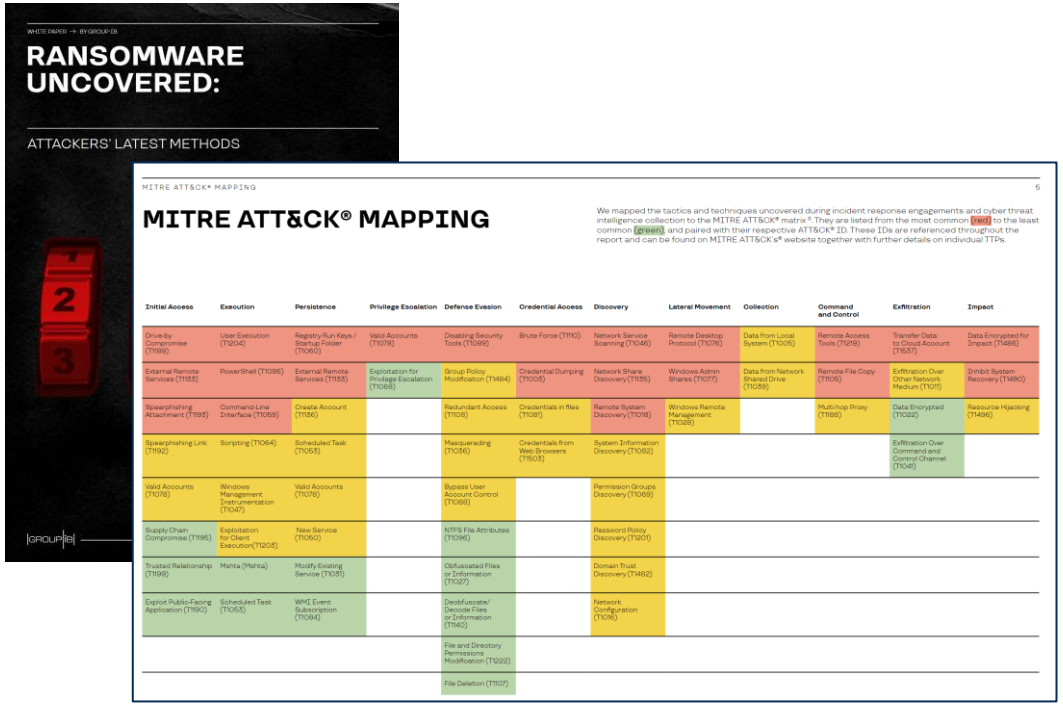
- **BASによる可視化：**
  - MITRE ATT&CKフレームワークにマッピングを行い、既存の攻撃手法に対する「予防・検知能力の可視化」を行う。
  - 標準フレームワークにマッピングすることで、他のデータと比較することも容易！

<MITRE ATT&CKによる予防・検知能力の可視化>



Source：https://twitter.com/olafhartong/status/1109569799863091201

<例：Group IB：ランサムウェアに関するホワイトペーパー>



Source：https://www.group-ib.com/whitepapers/ransomware-uncovered.html

実効性確認手法 事例２：コントロール不備の検証

オープンソースで実施する方法：

- **Red Canary社 Atomic Red Team :**
  - MITRE ATT&CKフレームワークに基づいて、どの攻撃テクニックを検知/防御可能であるか、可視化を行うためのスクリプト・ライブラリ
    - https://atomicredteam.io/
    - https://github.com/redcanaryco/atomic-red-team
  - 自動化するスクリプトも開発されている。
    - https://atomicredteam.io/invoke-atomic/
    - https://github.com/redcanaryco/atomictestharnesses
- **MITRE社 CALDERA :**
  - MITRE社謹製のBASで、無償で利用可能。
    - https://caldera.mitre.org/
- **Active Countermeasures社 Threat Simulator :**
  - ADHD（Active Defense Harbinger Distribution）の配布元が提供するC2通信のテストツール
  - https://www.activecountermeasures.com/free-tools/threat-simulator/

事例 3 ：侵害調査

実効性確認手法 事例３：侵害調査

- **侵害調査（Compromise Assessment）とは？**
  - センサー（例：EDR）を全端末・サーバ等に展開し、集中的な監視・調査・分析を行い、侵害された痕跡がないか確認するサービス
  - 技術的には、センサーを経由でディスクフォレンジック・ネットワークフォレンジックなどの技術を活用しながら**脅威ハンティング**を行う技術・サービス
  - サービスによっては、Cyber Hygiene（サイバー衛生）に関連する情報も取得できるため、管理状態を可視化することができる。
    - 例）脆弱性の有無
    - 例）アカウントの利用状況（長期間ログインされていないアカウント）
    - 例）インストールしているツール一覧・不要なプログラムの存在
    - 例）サポート切れのシステムの存在

実効性確認手法 事例３：侵害調査

- 侵害調査の実施結果イメージ（内容・指摘事項共にダミー）

指摘カテゴリー	件数	具体的指摘事項
分析対象端末	**2,500**	―
標的型攻撃の疑義	12	• C:¥tools ¥以下に、Mimikatz と PowerSploit.ps1が配置されていた。 • X件のシステムで、システムイベントログの消去が確認された。
一般的なマルウェア	158	• Adware, Spywareの存在。
望ましくないプログラム	549	• 標準化外のチャットツール、VPNツールがインストールされていた。 • ライセンス違反疑義が入っているソフトウェアが導入されていた。
管理用プログラム・ツール	1,490	• PSExecとNmapのインストールされている端末が全体のX%を占める。
脆弱性の存在	135,298	• のべ13.5万件以上の脆弱性を確認された。 →同じ脆弱性が複数端末にある場合はカウントしている。 • １台当たり、約54件の脆弱性が存在する計算となる。
アカウント管理上の課題	N/A	• 47システムにおいて、継続的なブルートフォース攻撃の痕跡あり • 全体の40%のユーザがDomain Admin権限を保持していた
パスワード運用上の課題	160	• X件のアカウントにおいて、パスワードが１回も変更されていない • 平文で保存されたパスワードの存在（例：password.txt）

侵入疑義として、調査！

タイムスタンプなどから、SOCや
センサーの改善活動にも利用可能。

Cyber Hygieneの実績として利用！

各種振り返りに利用可能！
- プロセスが適切に運用されていたか？
- 不足したプロセスはなかったか？
- パッチ適用除外の管理はできていたか？

当該センサーを利用し続ければ、
継続的モニタリング & 改善を実現可能！

実効性確認手法 事例３：侵害調査

オープンソースで実施する方法：

- **例）WMICを活用したパッチ情報の取得**

→ System.txt で指定したシステムに対し、qfe（Quick Fix Engineering)というエイリアスを呼び出し、パッチの適用状況に関する情報を出力することが可能。

```
wmic /node:@Systems.txt qfe get csname, description, ↵
      FixComments, HotFixID, InstalledBy,InstalledOn,ServicePackInEffect
```

- **例）脅威ハンティングツールの利用：**
  - **例）HAYABUSA**
    - **Windowsイベントログ**を利用したファストフォレンジックツール・脅威ハンティングツール
    - https://github.com/Yamato-Security/hayabusa

HAYABUSA

事例４：SSPM

実効性確認手法 事例４：SSPM

- **SSPM：SaaS Security Posture Management**
  - SaaS製品のセキュリティ態勢をチェックする製品
  - 関連用語）CSPM：Cloud Security Posture Management
    - CSPMは、IaaS・PaaSのセキュリティ態勢をチェックする製品
  - まだ新しい製品領域だが、複数の企業が登場している。
    - ツールの具体例として以下の通り（評価は各自でお願いします）
      - 例）Adaptive Shield　https://www.adaptive-shield.com/
      - 例）AppOmni　https://appomni.com/
      - 例）Obsidian Security　https://www.obsidiansecurity.com/

実効性確認手法 事例４：SSPM

無償で実施する方法：

- **例）Microsoft Scoreの利用**
  - Microsoft O365では、セキュリティスコアを提供してくれている。
  - こうした情報を使いながら、セキュリティを高めていく方法も一つの方法。

Wrap-Up

Wrap-Up

本日は、Cyber Hygiene Huntingについてお話させていただきました。

- **Part I　　：理論編**
  - Cyber Hygiene Huntingの定義や必要となる背景、関連する概念についてご紹介
    - 将来の攻撃につながるCyber Hygieneの状態・脅威へのセキュリティ態勢が適切に確保されているか検証するため、EoC（Enabler of Compromise）を探しだす。
    - Adaptive Securityと２種類のアプローチ（Threat Hunting vs. Cyber Hygiene Hunting）

- **Part II　　：実務編**
  - Cyber Hygiene Huntingを実現するためのパラダイムシフトとスコープの考え方をご紹介
    - CM & CI（継続的モニタリング & 継続的改善）を実現アプローチ

- **Part III　　：事例編**
  - 実例・具体的ツールなどを取り上げながら、Cyber Hygiene Huntingのやり方をご紹介
    - Active Directory・セキュリティ制御の検証 etc.
    - 無償・オープンソースの製品でも十分に始めることも可能

Thank You!

Appendix : Threat Hunting Overview

目次

- **目次：**
  1. 脅威ハンティングとは？
  2. 脅威ハンティングプロセス
  3. 脅威ハンティングの４種類のアプローチ
  4. 脅威ハンティングの前提条件・技術

- また、より詳しい解説は以下を参照してください。
  - 『脅威インテリジェンスの教科書』（拙著）
  - 『攻撃者をあぶり出す、プロアクティブなセキュリティアプローチ』（Internet Week 2019講演）
    - https://www.nic.ad.jp/ja/materials/iw/2019/proceedings/d2/

1. 脅威ハンティングとは？

脅威ハンティング（Threat Hunting）とは？

- **セキュアワークス社による定義：**
  - **既存のセキュリティ対策を回避する現在/過去の脅威を能動的・再帰的に調査**し、その情報を利用して**サイバーレジリエンスを向上**させること（=プロアクティブなアプローチ）

- **なぜ、脅威ハンティングが重要なのか？**
  - 攻撃手法、セキュリティ対策の回避手法が進歩しているため、シグニチャに頼った防御モデルが成立しなくなったため。
  - **LoLBaS攻撃**の割合が増え、正規のアクティビティなのか、攻撃なのか、判断が難しいケースが増えているため。

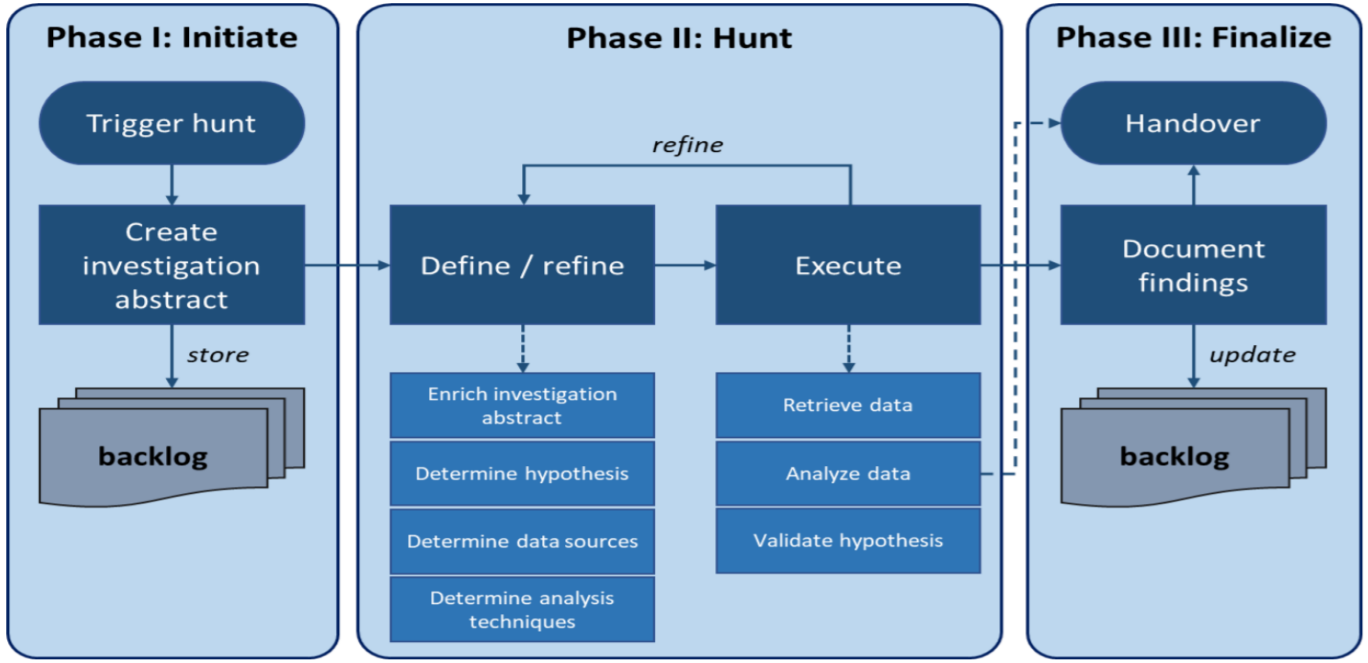
  - 参考： LoLBaS攻撃（Living Off the Land Binaries and Script攻撃）
    - 侵入環境にインストールされているソフトウェア、OSデフォルト機能、ネイティブツール・スクリプトを悪用して攻撃する手法

- **プロセスモデル：どのように脅威ハンティングを実施するか？**
  - 色々なモデルは存在しますが、今日はエッセンスを抽出した簡易版でご紹介します。

参考：脅威ハンティングプロセスモデル

- **プロセスモデル：どのように脅威ハンティングを実施するか？**
  - Sqrrl社　：Hunting Loop
  - Carbon Black社　：The Carbon Black Hunt Chain
  - CyberReason社　：Threat Hunting 8 Steps
  - SANS Institute　：SANS Threat Hunting Model
  - SANS Institute　：Intelligence Driven Threat Hunting
  - FI-ISAC NL　：TaHiTI（**Ta**rgeted **H**unting **i**ntegrating **T**hreat **I**ntelligence）

- **TaHiTI：　Targeted Hunting integrating Threat Intelligence**



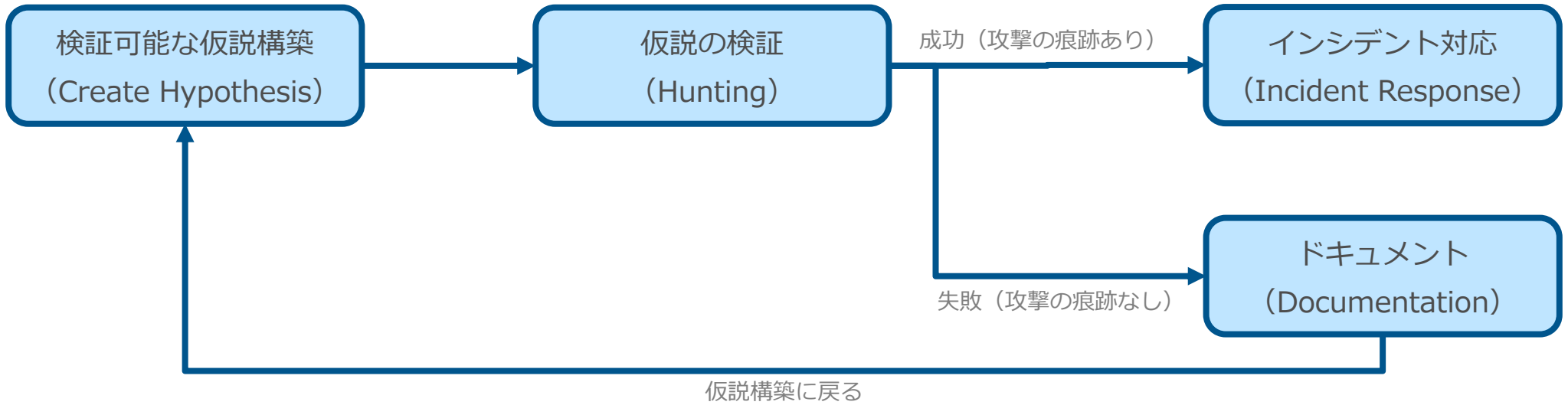
2. 脅威ハンティングプロセス

脅威ハンティングプロセスは、本質的に３つのフェーズで構成される。

- その中でも、「仮説構築」フェーズが最も重要。
  - 仮説により、脅威ハンティングの品質や、実際にHuntingを行う「仮説の検証」フェーズの作業が決まるため。

- 「仮説構築」の具体例：４点を整理する
  - **仮説構築**：（攻撃により）不審なドメインアカウントが作成されている。
  - **調査対象**：ドメインコントローラサーバ上のWindows Event Log
  - **調査方法**：イベントID（ID : 4720）で絞り込み、サービスデスクが稼働していない時刻にアカウント作成されたログエントリを探す。
  - **判断基準**：当該エントリがでた場合、悪性（＝攻撃の痕跡あり）と判断する。

<脅威ハンティングプロセス>



2. 脅威ハンティングプロセス

- **仮説構築の重要性：**
  - 脅威ハンティングは、**「既存のセキュリティ対策を回避する現在/過去の脅威」を見つける手法**である。
  - そのため、**「仮説 → 検証」の科学的アプローチ**を採用しないと以下の危険性がある。
    1. 終わりなき作業になってしまう。
    2. 再現性がない作業になってしまう。
    3. 悪性か否かの判断がアナリストの主観的判断になってしまう。

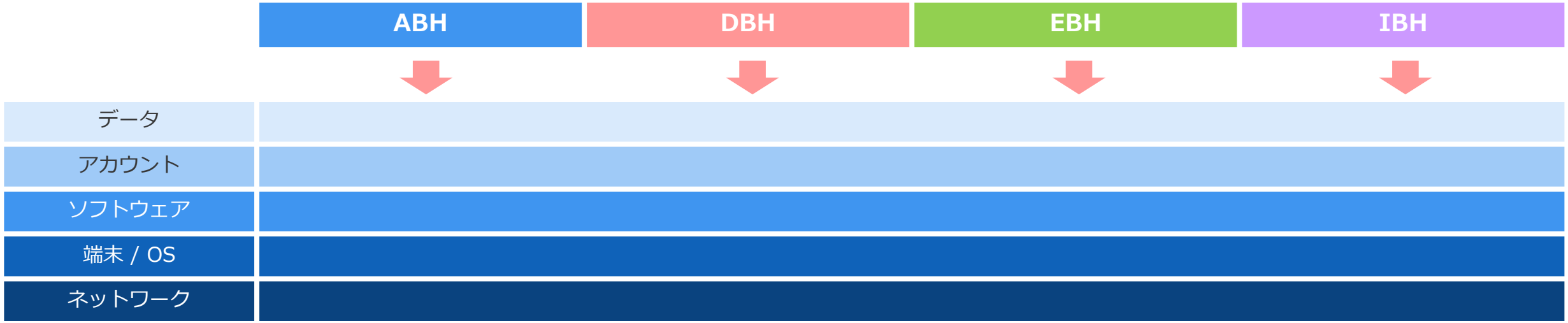
- **適切な「検証可能な仮説構築」を行うためにはどうすればよいか？**
  - **脅威ハンティングのアプローチ手法：**
    - 「検証可能な仮説」をどのように構築するか、考え方・思考法を整理します。
  - **脅威ハンティングの前提条件・技術：**
    - 「検証可能な仮説」を支える前提条件・技術についてご説明します。

3. 脅威ハンティングの４種類のアプローチ

- 脅威ハンティングアプローチは、大きく４種類存在する。

	ABH （Attack based Hunting）	DBH （Data based Hunting）	EBH （Entity based Hunting）	IBH （Intel based Hunting）
概要	MITRE ATT&CKなど、攻撃手法を軸に仮説構築を行う手法。	データに現れるアノマリー（異常値）に注目して仮説構築を行う手法。	特定のデータ・端末・ユーザなど、高リスク・高価値のエンティティに注目して仮説構築を行う手法。	外部から入手した脅威インテリジェンスを軸に仮説構築を行う手法。
事例	• 「不審なドメインアカウント作成」（T1136.002）の調査を行う。	• 接続先IPアドレスをGeolocation情報とマッチングして頻度分析を行い、頻度が低いかつ普段やり取りしない国のIPアドレスを調査する。	• 脆弱性パッチの当たっていない端末に対する不信な挙動有無を確認する。 • ドメイン管理者権限を持つアカウントに対し、不審なログイン挙動がないか検証する。	• IOCに基づく調査。 • ISACから得た他社攻撃情報をもとに、調査を行う。 • Deceptionを活用する。

- この４種類の観点から、各レイヤーの調査を行っていく。



4. 脅威ハンティングの前提条件・技術

- 脅威ハンティングを実現するための前提条件は以下の通り。
  - **Full-Spectrum Visibility（徹底的な可視化）**
    - 脅威ハンティングを行う上では、仮説をちゃんと検証できるためのデータが必要となる。
    - そのため、「技術的」には検証可能な仮説も、データ収集基盤・データ分析基盤がないと分析ができず効率的な脅威ハンティングができない可能性がある。
  - **Know-Normalの原則：**
    - 脅威ハンティングの重要なキーワードの一つにアノマリー（異常値）がある。
    - 異常値を把握するためには、普段の状態（Normalな状態）を知っておく必要がある。そのため、徹底的な可視化を行った後、「普段の状態」を正しく理解する必要がある。
      - 例）端末の命名則
      - 例）普段利用されているアカウント
      - 例）ドメイン管理者アカウントの割合・利用状況
      - 例）普段組織内で利用されているバイナリ・EXEファイル

4. 脅威ハンティングの前提条件・技術

- **脅威ハンティングを支える技術：**
  - Windows Event Logからすると始めやすい！
    - Hayabusa : https://github.com/Yamato-Security/hayabusa
    - Sysmon Search : https://github.com/JPCERTCC/SysmonSearch


4. 脅威ハンティングの前提条件・技術

登場してきているキーワード・トレンド：

- ***XDR : Extended Detection and Response***
  - XDRの定義はまだ厳密に定まっていない（講演者の観測範囲において）
  - 参考：Gartnerによる定義
    - XDRとは、（予防・検知・対応を支援する）複数のセキュリティ製品からのデータとアラートを統合・相関・コンテクスト化するプラットフォーム
  - （講演者の）現時点での理解：製品領域・自由度を減らす代わりに、サービス提供領域を拡大
    - 対象製品　：（サービス提供会社の）自社製品 OR 厳選されたパートナー製品に限定
    - 分析の自由度　：カスタマイズ性などを減らす代わりに、対象製品の相関分析に特化
    - サービスのカバー領域　：Detection & Responseの領域を拡大（例：Endpoint → Endpoint + α）

  → 脅威ハンティングの新しいプラットフォームとなっていく（と思う）。

- ***ITDR : ID Threat Detection & Response***
  - Gartner社「2022年のセキュリティ／リスク・マネジメントのトップ・トレンド」として挙げている。
  - 侵害の多くは、IDの悪用が起点となるため、IDの利用を検知・対応するサービスが少しづつ登場している。
  - 脅威ハンティングの観点でも、IDに注目する重要性はより高くなる（と思う）。

まとめ

- 脅威ハンティングとは？
  - **既存のセキュリティ対策を回避する現在/過去の脅威を能動的・再帰的に調査**し、その情報を利用して**サイバーレジリエンスを向上**させること

- 脅威ハンティングプロセス
  - 「仮説構築　→　検証」のプロセス

- 脅威ハンティングの４種類のアプローチ
  - ABH（Attack based Hunting）
  - DBH（Data based Hunting）
  - EBH（Entity based Hunting）
  - IBH（Intelligence based Hunting）

- 脅威ハンティングの前提条件・技術
  - Full-Spectrum Visibility（徹底的な可視化）
  - Know Normalの原則
  - XDR, ITDR…

Thank You!