GMO CYBER SECURITY IERAE

クラウド環境内の
データベースに対するDFIR

自己紹介

名前　寺岡 良真（traoka）

所属：GMOサイバーセキュリティ by イエラエ株式会社

ディフェンシブセキュリティ部

インシデント対応やフォレンジック調査を業務で行う関西人。元々セキュリティは攻守どちらも行います。また、過去にWeb系の開発や独自のWebサービス運用も行っていました。

過去に、 BlackHat USA Arsenal 採択や、Security-JAWS、Janog 等でお話させていただいたりしています。

アジェンダ

GMO CYBER SECURITY IERAE

・昨今のインシデント

・DFIRとは

・クラウド環境においての事例と調査

・まとめ

昨今のインシデント

昨今のセキュリティインシデント

2022/10/30 ― **JTB、クラウドサービスの「アクセス権限」の設定ミスで情報漏洩、～1万人超の個人情報・約1700件の申請書類が漏洩**

参照元：https://www.imagazine.co.jp/jtb-data/

2022/10/31 ― **大阪の病院で電子カルテシステムに障害、「ランサムウェア」によるサイバー攻撃か**

参照元：https://www.yomiuri.co.jp/national/20221031-OYT1T50162/

2022/11/2 ― **ワコムのネットショップで個人情報流出の可能性 - クレカ情報の窃取も**

参照元： https://www.security-next.com/141608

攻撃者の目的は…

一番多く目にするのはやはり金銭目的です。

他にも企業や団体組織などを狙った標的型攻撃など多岐にわたります。

攻撃者の目線では、目的を達成することが重要であるため、基本的にクラウドの有無などの環境についてはあまり関係ありません。

ただ、企業や団体の管理するシステムがクラウド環境に移行したことによって、クラウド環境での侵害が増加しています。

クラウド環境においての対応範囲

AWSの責任共有モデルに代表されるように、各クラウドサービスベンダには独自のコンプライアンスが明示されています。

多くの場合、国内のホスティング事業社などと同じように、セキュリティインシデントについては基本的にサービス利用者側の責任となるため、クラウドベンダがインシデント対応をサポートしてくれることはありません。

インシデントは自力で解決する必要があります。

DFIRとは

DFIR

DFIR （Digital Forensics and Incident Response ）はデジタルフォレンジックとインシデント対応を組み合わせた造語で、主にサイバー攻撃に関するセキュリティインシデントについての対応や調査にフォーカスしたものです。

フォレンジック調査とインシデント対応は混同されがちですが、ニュアンスが少し異なっており、違いはよく火事の現場で例えられます。

インシデント対応（Incident Response）：

いわゆる消火活動のように、火を消すことを目的としています。

フォレンジック調査（Digital Forensics）：

消火後の焼け跡から事故の原因や経緯などの調査を目的としています。

インシデント対応の場合

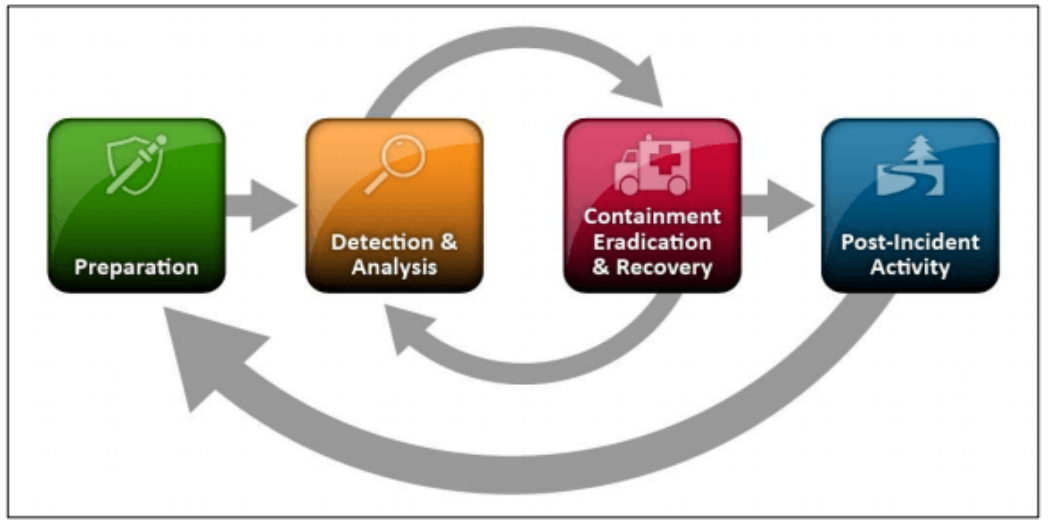
NIST（米国標準技術研究所） の「SP 800-61 」など、インシデント対応を体系的に理解できる資料が公開されています。

NIST：https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

日本語訳（IPA）：　https://www.ipa.go.jp/files/000025341.pdf

基本的には以下の４つのサイクルで考慮すると分かりやすいです。

準備　　**検知・分析**　　**封込・根絶・復旧**　　**事後処理**



参考：ありがちなトラブル

普段のセキュリティ対策に限らず**「管理」**に不備があると手間取りがちです。

・社内のIP 192.168.x.x から不審な通信が起きているが、動的割り当てなので誰のPCかわからない！

・多数のPCでウィルス検知がでているが、導入しているウイルス対策ソフトが環境ごとに異なっていてで駆除できない！

・WAF（Web Application Firewall）からアラートが起きているが操作や内容がわからない！

・ネットワーク図やシステム構成図が古くて実際の環境と異なっている！

フォレンジック調査とは

フォレンジック（Digital Forensics）は 、法科学の一種を指します。
パソコンやサーバなどのデジタルデバイスを解析し、そこに残された
情報からサイバー犯罪の証拠やインシデントの原因などを調査します。

イメージとしては刑事ドラマなどで登場する
鑑識さんのデジタル版みたいな形です。

調査結果は、実際に裁判の証拠として
取り扱われることもしばしばあります。

フォレンジック調査の主な流れ

フォレンジック調査にあたっては大きく分けて４つほどあり、基本的に一連の流れで進めます。

調査の内容や対象によっては長期化する場合があります

1. **調査の目的、方針、内容を決める**
2. **調査対象のデータの保全**
3. **保全したデータをもとに調査、解析**
4. **調査した結果のまとめ、報告**

フォレンジック調査の主な流れ

GMO CYBER SECURITY IERAE

1. 調査の目的、方針、内容を決める

調査対象の全てを調査することは俵の米粒を数えるように膨大な時間がかかるため、何を知りたいのか、目的や内容などを事前に決めます。

また、調査対象内に**必ず証拠があるわけではない**点も注意が必要です。

2.調査対象のデータの保全

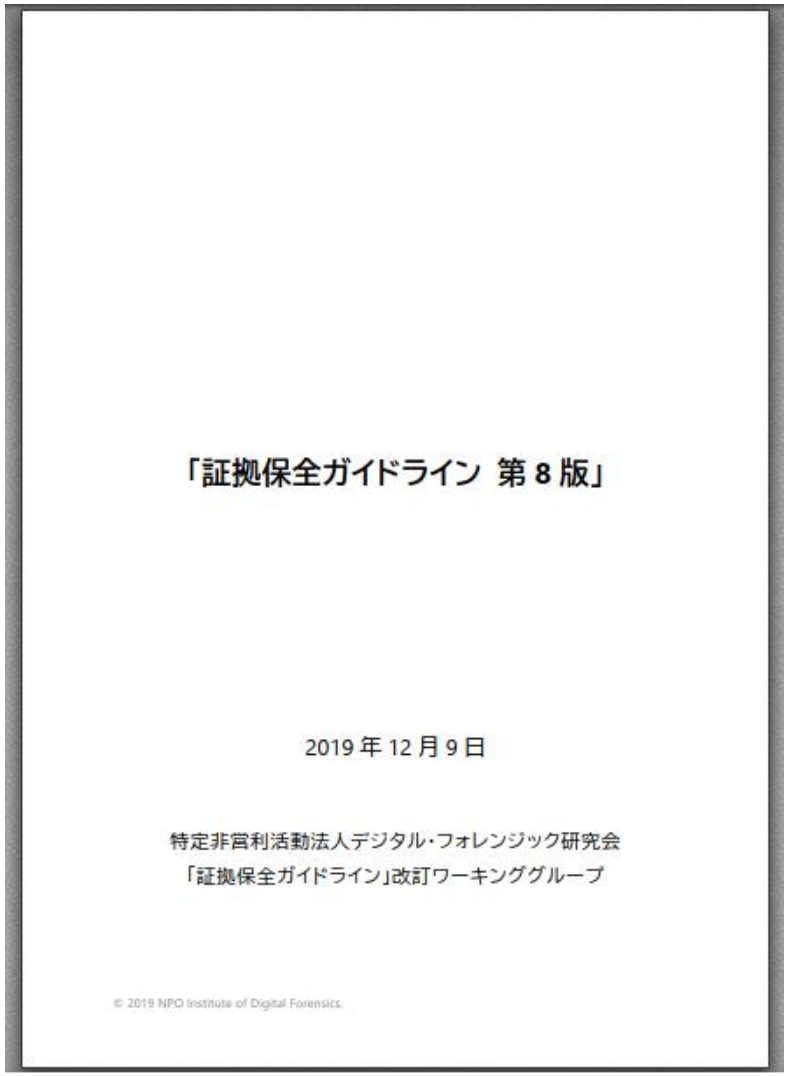
PC内のデータは時間とともに変化してしまうため、重要な手がかりが消えてしまう可能性があります。これを防ぐためにデータの保全という作業を行います。また、CoC（Chain of Custady）というデータの連続性を示すための手続きを行います。

参考情報

証跡の取得や取り扱いについてはデジタル・フォレンジック研究会（IDF）が公開している「証跡保全ガイドライン」が参考になります。

URL:

https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/



フォレンジック調査の主な流れ

GMO CYBER SECURITY IERAE

3. 保全したデータをもとに調査、解析

データの保全後、それに対して解析を行い手がかりや証拠を調査します。削除したファイルを復元したり、マルウェアの活動痕跡などを探ったりと多岐に渡ります。

4. 調査した結果のまとめ、報告

調査、解析した結果を報告書にまとめます。原因や影響範囲、情報の漏洩、各種タイムライン等も記載します。

報告を受けた側については、調査結果をもとに再発防止など次のアクションの判断を行うことが大切です。

参考：調査に必要な事前情報

調査会社に依頼する場合、調査会社は侵害のあった環境やシステムを管理しているわけではないため、素早く情報共有ができるとスムーズです。

- インシデント発覚の経緯と実施した対応（日時も含む）
- 侵害のあった環境や対象についての情報
- 調査の位置づけ（何をするための調査なのか）
- 担当者の連絡先

これらの状況を整理して、調査の対象サーバ、各種ログ、ネットワークの通信やセキュリティ製品のイベントなどを選定します。

クラウド環境においての事例と調査

実際に発生したケースの例

GMO CYBER SECURITY IERAE

Webサイトの改ざんおよび情報漏洩、サーバの不正アクセスなど

クラウド環境で運営しているWebシステムに不正アクセスが発生し、改ざんや個人情報やクレジットカード情報が漏洩してしまうケース。

バックドア等でサーバを掌握され、様々な攻撃の踏み台などに悪用されることも。

フィッシングメールやマルウェア感染メールの大量発生

クラウド環境で利用しているメールサーバやメールサービスが不正アクセスされ、大量のメール送信に悪用されてしまうケース。

これによりフィッシングやマルウェア感染などの被害を助長してしまうことに。

実際に発生したケースの例２

GMO CYBER SECURITY IERAE

クラウドサーバ経由による社内ランサムウェア感染

新たにクラウド環境に導入したWebの社内グループウェアのサーバがランサムウェアに感染。

VPNで社内ネットワークに繋がっていたため社内ネットワークにも感染が広がってしまったケース。

大量サーバ起動による仮想通貨マイニング

利用しているクラウドのアカウントで不正アクセスが発生。

すべてのリージョンで大量のサーバが立ち上がり、仮想通貨のマイニングに悪用され、これにより莫大な利用請求が発生。（クラウドベンダからアラートが届きます。）

データベースの侵害パターン

GMO CYBER SECURITY IERAE

多種多様に存在しますが、大きく２つ考慮されます。

・データベース内に保存されている情報の侵害

・データベース自体の侵害

データベース内に保存されている情報の侵害

GMO CYBER SECURITY IERAE

サービス運営者に対して脅迫するケース

攻撃者がDB内のデータの改ざんや削除を行って、復旧のための身代金を要求する脅迫メッセージを残したり、窃取したDB内のデータを公開されたくなければと脅迫するなど。

データ自体の窃取を目的としているケース

クレジットカード情報や個人情報、機密情報の窃取を目的としているもの。ダークウェブでの取引や、フィッシングなどの2次被害、デジタルコンテンツや機密データの漏洩などの懸念があります。

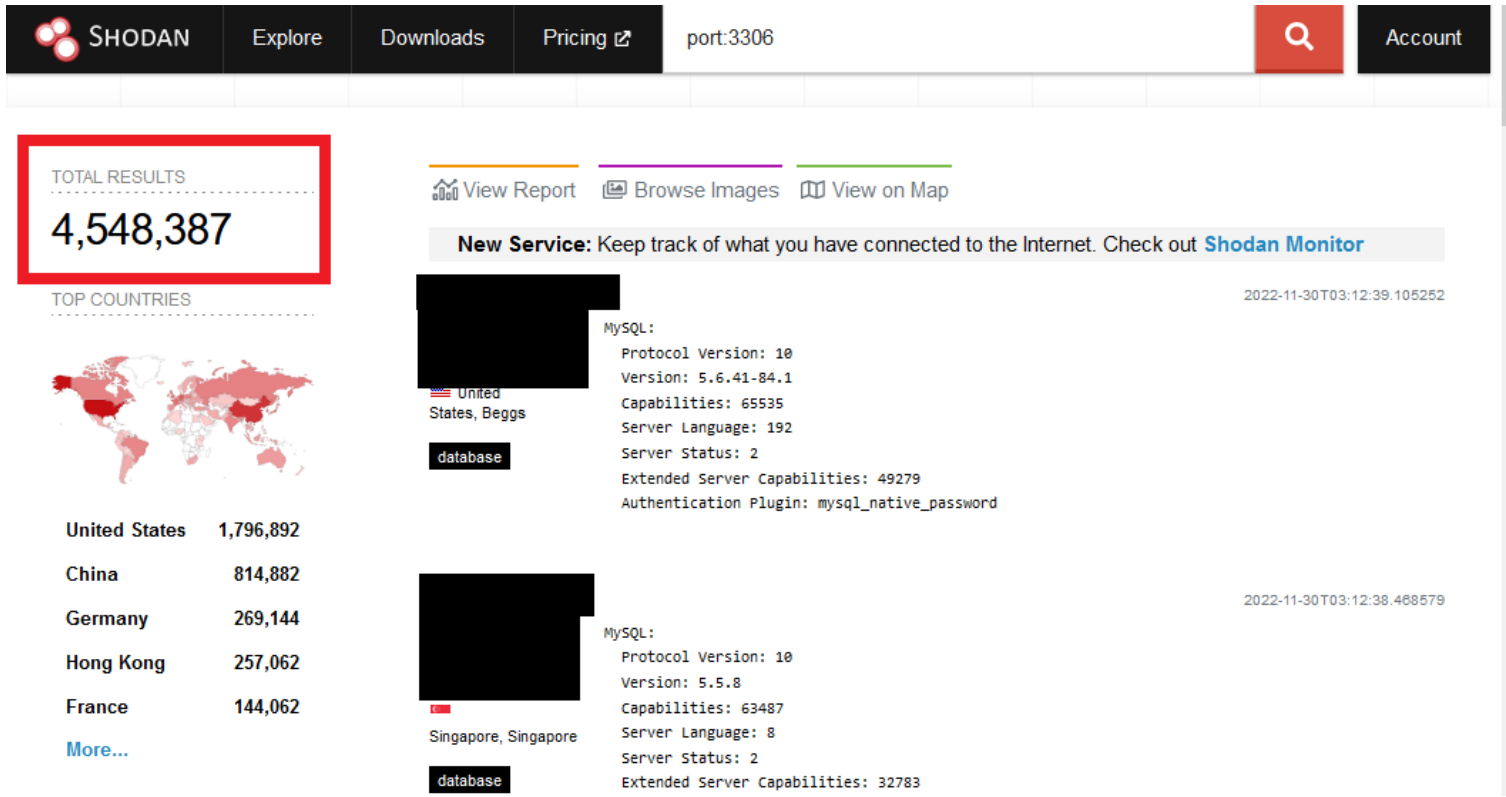
データベース自体の侵害

データベース自体の脆弱性が侵入口となってしまい、不正アクセスやマルウェアに感染などのインシデントの原因になることがあります。

ここでの脆弱性はCVE（共通脆弱性識別子）のみならず、設定のミスやパスワードが推測されやすいものなども含みます。

データベース自体の侵害

※軽くSHODAN （https://www.shodan.io）でMySQLのデフォルトポート番号を調べても450万ヒットしている状態です。



データベース調査のアプローチ

実際のところ、データベース（やサーバ）のみを対象としたフォレンジック調査を行うことはほぼありません。

データベース自体が業務システムの一部であったりと、基本的に何らかのシステムと連携して使われるため、データベースだけで状態を判断できるものではありません。

原因や影響範囲、攻撃者の目的や侵入経路等も痕跡をたどるために**トータルの環境を考慮して対処する必要がある**ことに留意してください。

調査対象の関連記録

GMO CYBER SECURITY IERAE

アクセスログ、エラーログ

DBへの不正アクセスなどの検出が期待できる。

クエリログ

攻撃者の実行したクエリの検出、情報窃取や改ざんやデータ破壊などの検出が期待できる。

データベースのダンプ

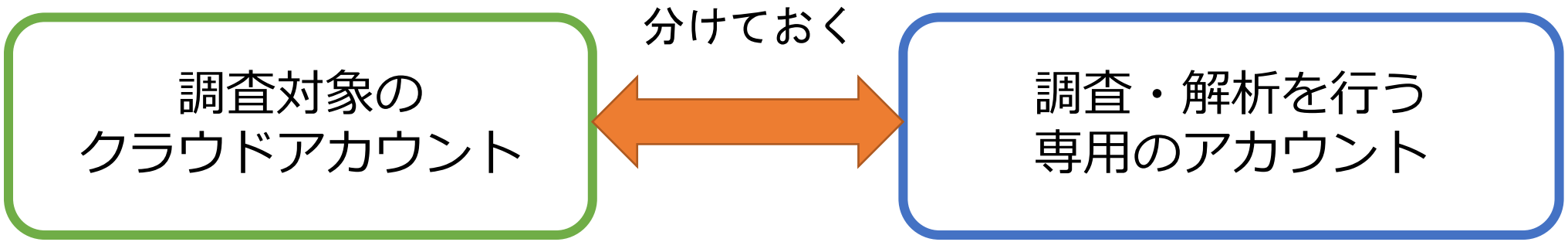
差分より改ざん箇所の特定や追跡が期待できる。

調査環境の分離（クラウド）

クラウド環境にあるデータを取り扱うために、調査専用のクラウドアカウント環境を分離しておくと有用です。

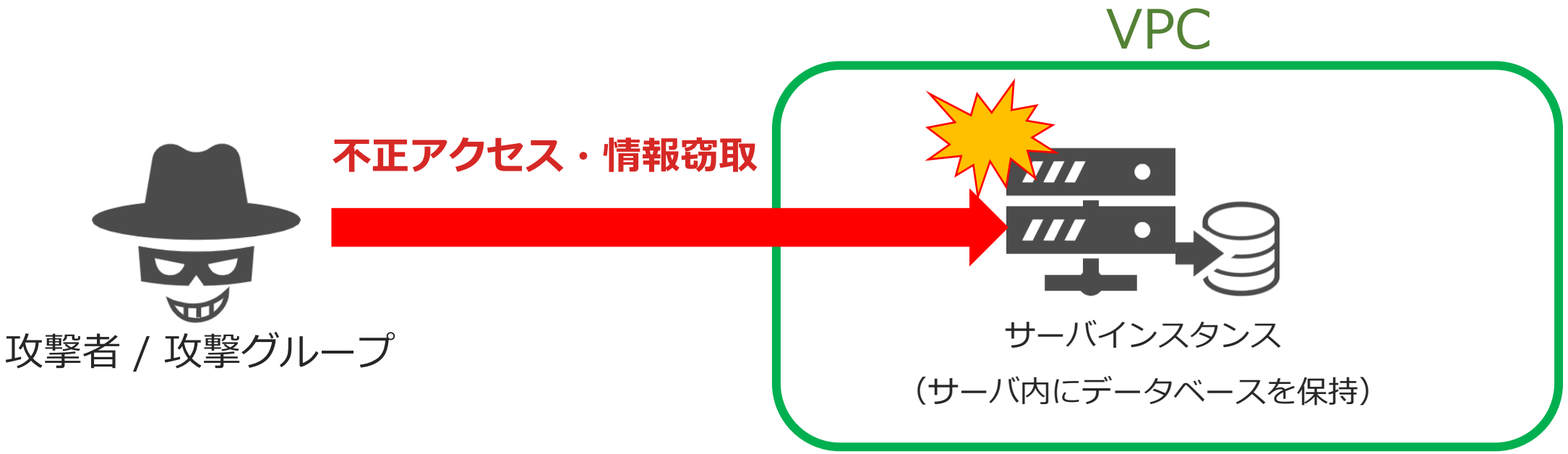
１つのアカウント内で住み分けもできますが、運用管理が複雑となりコストが高くついたり、調査によって痕跡を汚したり、調査内容や結果の改ざんの懸念が拭えないためです。

また、複数クラウドアカウントがある場合も柔軟に対応ができます。



IaaS系の侵害調査例

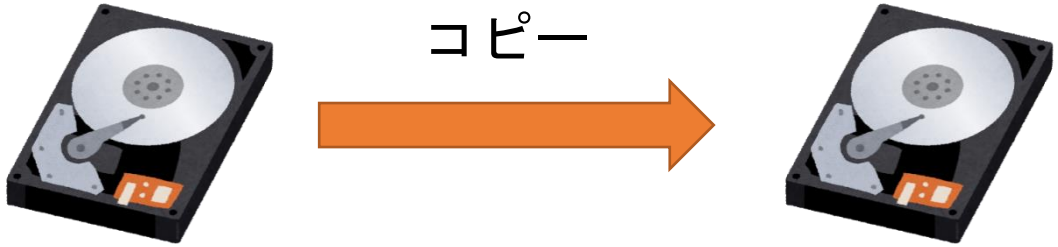
一番多いケースでは、AWS EC2 やGCE、Azure Virtual Machine のような、仮想サーバ上で稼働しているシステム（IaaS系）に対する侵害の調査です。



調査の方法について

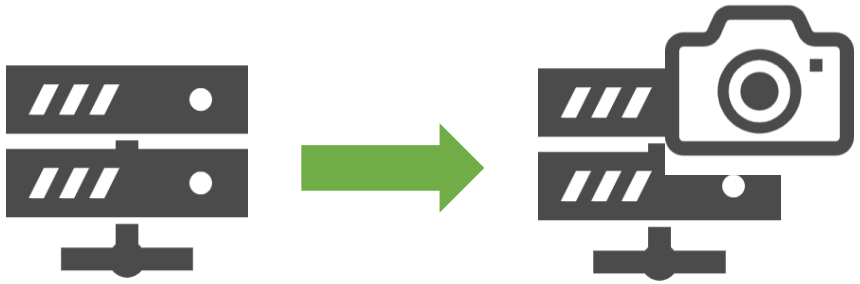
この場合はHDDの保全が実施可能であるため、一般的なHDDイメージの解析手法をとります。

保全データから侵害端末のデータベースを復元して内容の調査を行ったり、データベースのログ（アクセスログやバイナリログ、各種クエリログ等）と相関して調査を行います。

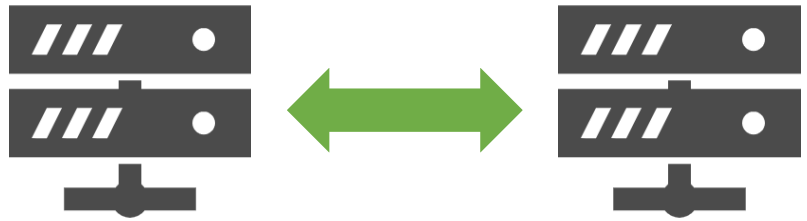


仮想サーバのHDD保全

オンプレミスと違い、仮想サーバの場合はスナップショット機能を使用できるため、これを用いることで簡易的に侵害を受けた状態を保存することができます。スナップショットをとれない場合でも、インスタンスのコピーを残しておくことで、後からある程度調査を行うことができます。



スナップショットで簡易保全

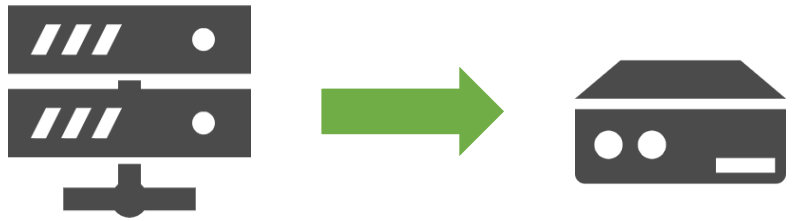


イメージのコピー

仮想サーバのHDD保全

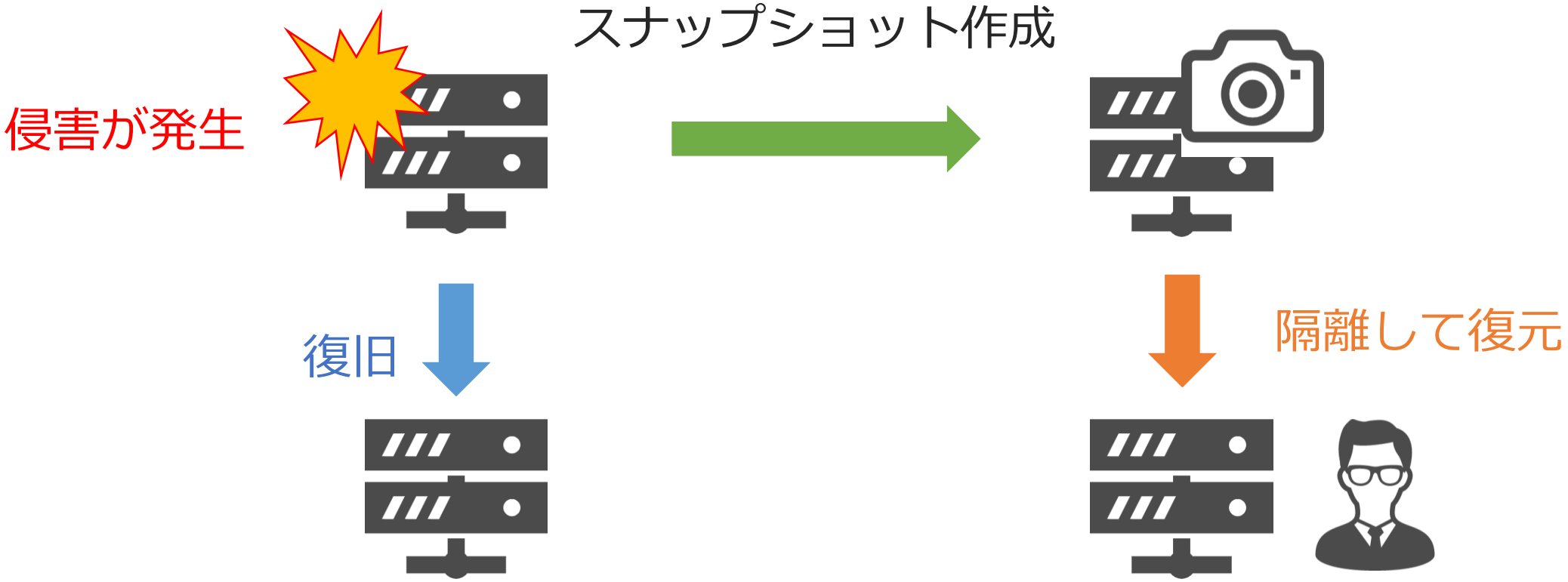
自動バックアップ機能を使用している環境ではサーバイメージがバックアップされるため、これらを対象しての調査も可能です。

ただ、バックアップタイミングによっては時間経過によってインシデントの痕跡が残っていなかったり、バックアップ自体が一定期間で消去されてしまうことがあるため注意が必要です。



自動バックアップイメージから侵害直後のHDDの保全

保全と復旧を平行することが可能

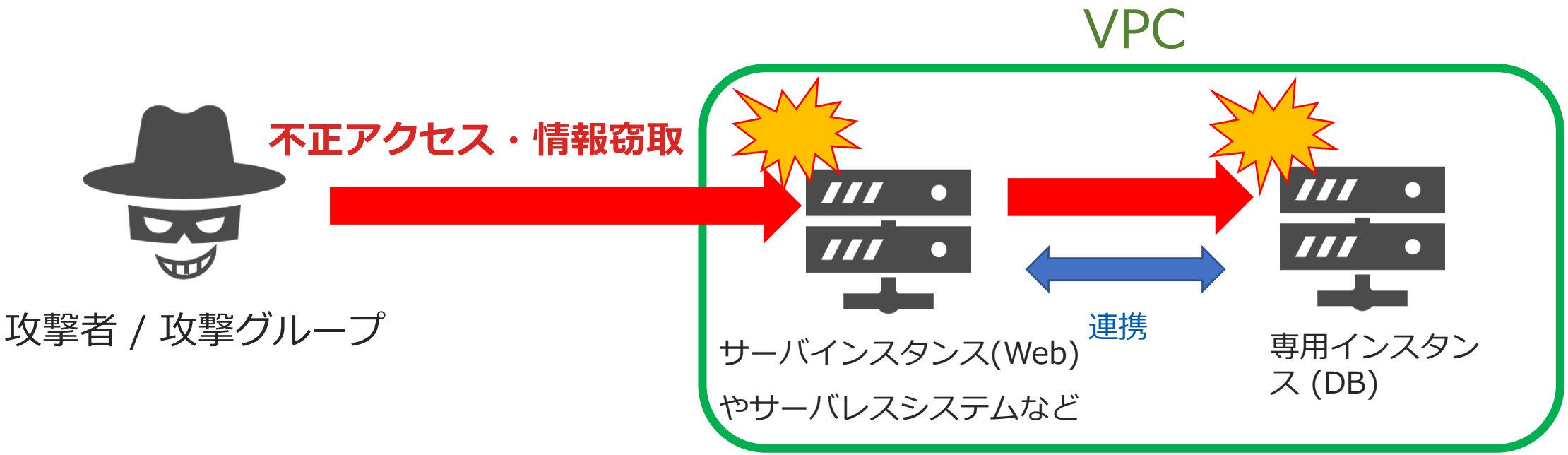


バックアップや過去の正常なスナップショットから復旧や、新規インスタンスへの移行など

別環境で侵害の調査

PaaS系の侵害調査例

AWS RDSやGCP Cloud SQL、Azure SQL Databaseなどの専用インスタンスを含む環境（PaaS）のインシデント場合です。

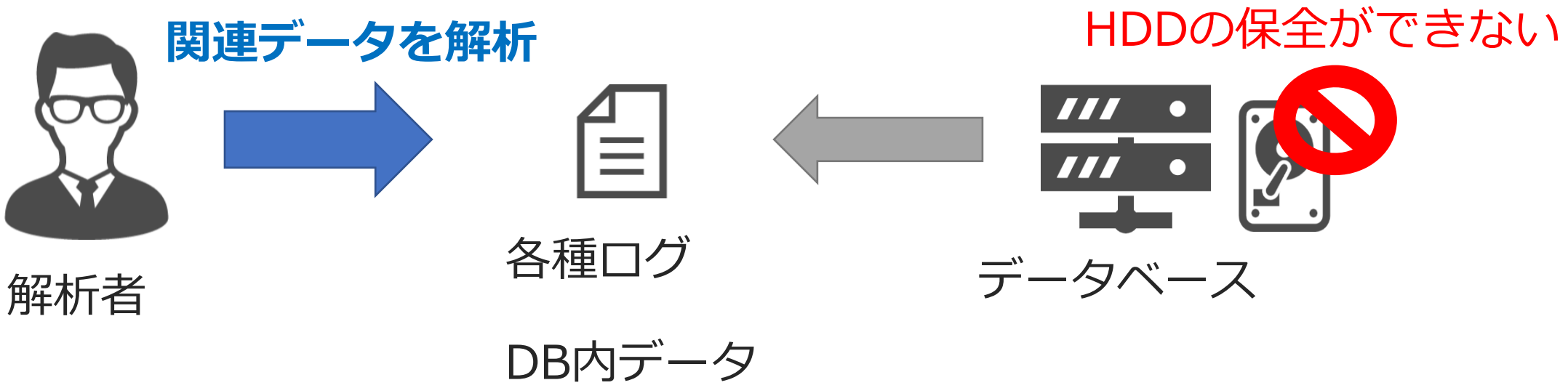


専用インスタンスの場合

GMO CYBER SECURITY IERAE

データベース専用インスタンスの場合、**HDDの保全ができません。**

代わりとして、各種ログ（アクセスログ、エラーログ、イベント、アラート、クエリログ）などの関連データが調査の対象となります。



あると有用なデータの例（AWS）

- AWS CloudTrail のアクティビティ全般
- CloudWatchのイベントおよびログ
- Config
- S3アクセスログ
- AmazonVPCフローログ
- WAFのログ
- Cloud Front ログ
- ELB アクセスログ
- その他使用サービスなど

調査不能な項目

専用インスタンス内の不正なファイル生成や他の侵害については基本的に調査できません。専用インスタンスであるため、データベース以外の影響はクラウドベンダ側の実装に依存します。

復旧においては既存のインスタンスを継続するより、別途立て直した方が不要なリスクを負わなくて済みます。

コンテナ環境の場合

GMO CYBER SECURITY IERAE

Docker やKubernetesなどのコンテナを使用した仮想環境の場合について、IaaS系などで独自で作成した仮想サーバ上でコンテナ環境を構築している場合はHDDの保全から復元が可能です。

コンテナサービスの場合、HDDでの保全ができないため、専用インスタンスと同じようにログやスナップショットなどを対象としたアプローチをとることになります。

また、サービスで用意されているAPIなどを用いることで情報取得やライブフォレンジックを行う場合があります。

調査のポイント

GMO CYBER SECURITY IERAE

・コンテナ内のファイル差分　（標準コマンドなどを使用）

・プロセス

・共有フォルダ内のログ

・コマンド履歴

・ネットワーク

・ログ(監査、認証、API、マネージャ、スケジューラ)関連

※CroudWatch 等と連携してあると比較的調査難易度が減ります

・セキュリティ製品やSIEMなど

参考情報

GMO CYBER SECURITY IERAE

- Container Explorer

  https://github.com/google/container-explorer

- cloud-forensics-utils

  https://github.com/google/cloud-forensics-utils

- kube-forensics

  https://github.com/keikoproj/kube-forensics

- Kubernetes のロギングアーキテクチャ

  https://kubernetes.io/ja/docs/concepts/cluster-administration/logging/

まとめ

まとめ

本セッションでは、DFIRの大まかな内容や実際のケースを交えた対応や調査について解説しました。

クラウド環境では各種サービス連携や、仮想ならではのメリットがある反面、普段の運用時からの準備や検証が行われていないと対応不能になることがあります。

「構築や定義して終わり」ではなく、日々の運用の一部としてセキュリティ品質を向上する一助となりましたら幸いです。

まとめ

自社ブログで大変恐縮ですが、

「AWS EC2 のHDD解析（フォレンジック）」という記事を以前書かせていただきました。

https://bit.ly/3bY56G5

AWS EC2 の内容となりますが、インスタンスの解析手順をスクリーンショットつきで掲載しています。調査の雰囲気や手順を記載しているので、ぜひ試していただけたらと思います。

ご清聴ありがとうございました