フルパケットセキュリティ診断　サービス仕様書

第1版

2024年12月2日

株式会社クワッドマイナージャパン

1. はじめに

1.1. 本書の目的

フルパケットセキュリティ診断サービス（以下本サービス）とは何か、その目的と利用方法は何かを説明することです。

1.1.1. 本サービスとは?

ネットワーク内部の潜在的なリスクを把握し、お客様の環境に適したセキュリティ対策を提案するネットワーク診断サービスです。

1.1.2.本サービスの目的

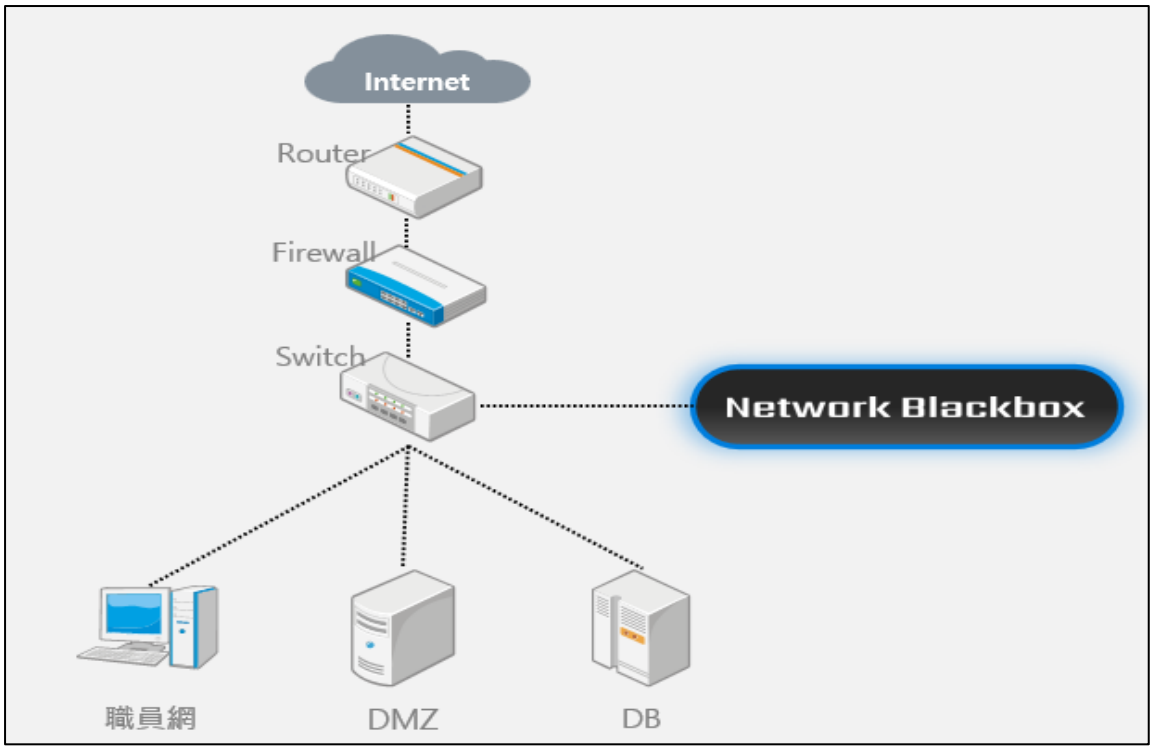
ネットワーク区間の通信内容をリアルタイムで収集、保存した後、分析を通じてセキュリティ問題などを事前に検出することを目的としています。

2. 本サービス　仕様

2.1. 概要

診断が必要なネットワーク区間にミラリングの形でパケットを収集します。

例2.1：トラフィック収集イメージ



2.2. ご利用条件

内部ネットワークから内部ネットワークへの通信、内部ネットワークから外部ネットワークへの通信をしている環境が対象になります。

2.3. 利用ツール、環境

自社のNDR製品である「Network Blackbox」をアプライアンスで利用します。

本アプライアンスはオンプレミスの形でネットワークに設置され、ミラリングポートを通じて**フルパケット**を収集します。

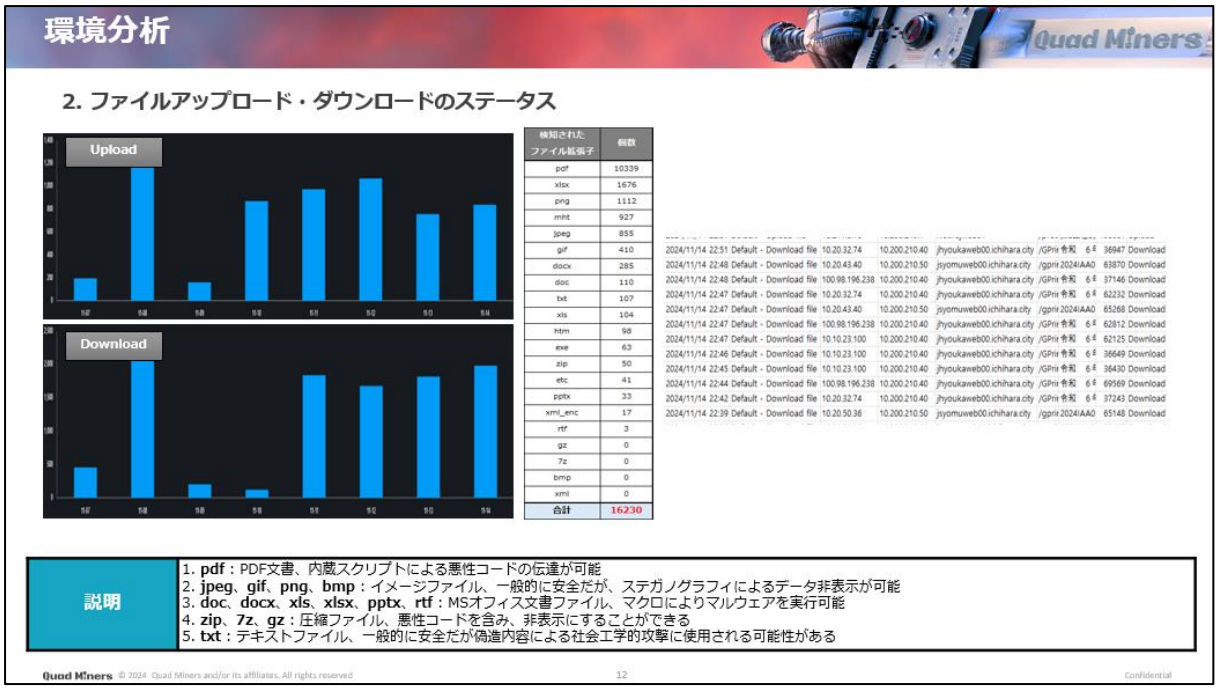
2.4. 診断内容

2.4.1. 環境分析

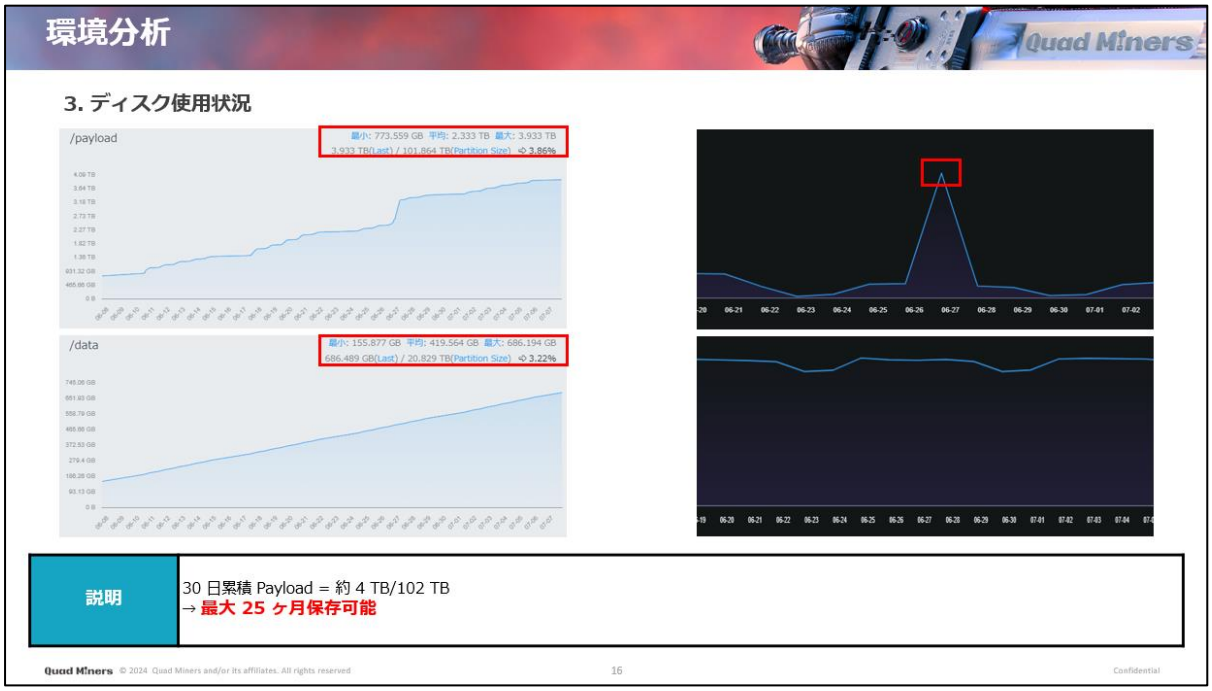
お客様の環境を把握する作業でより効率的な分析が可能です。

レポート例2.4-1：環境分析　トラフィックの検知ステータス

レポート例2.4-1：環境分析　ファイルアップロード・ダウンロードステータス



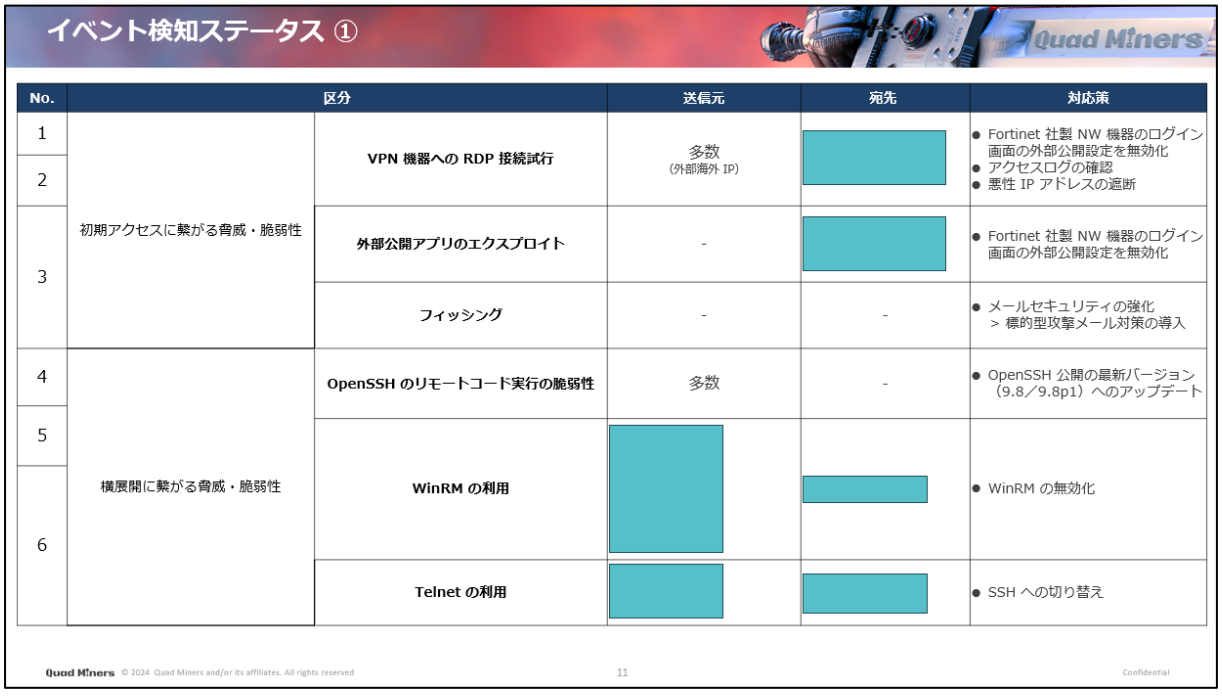
レポート例2.4-1：環境分析　ディスク使用状況



2.4.2. 脅威分析

見つかった脅威をより詳細に分析して、対応策までご提案します。

レポート例2.4-2：脅威分析　イベント検知ステータス



レポート例2.4-2：脅威分析 イベント検知ステータス2

イベント検知ステータス ②

No.	区分		送信元	宛先	対応策
7	情報流出に繋がる脅威・脆弱性	デフォルトポートを使用した FTP 通信 （内部 -> 内部）			● FTP の使用を禁止 ● SFTP を使用 ● デフォルトポートからの変更
8		デフォルトポートを使用した FTP 通信 （内部 -> 外部）	多数 （内部 IP）	多数 （SPF レコード内の国内 IP）	● FTP の使用を禁止 ● SFTP を使用 ● デフォルトポートからの変更
9	内部不正に繋がる脅威・脆弱性	業務利用外の外部サーバへの SSH アクセス	多数 （内部 IP）		● 該当サーバの用途の確認 ● 通信の悪性の有無の確認 ● 該当ユーザーの特定・確認 ● 該当サーバへの通信の遮断
10		業務時間内での Netflix・アダルトサイトへのアクセス	多数 （内部 IP）	多数	● 就労規則をもとにユーザーへ確認 ● 継続的な通信の監視
11	その他の脆弱性	Oracle の通信	多数 （内部 IP）		● 該当サーバのアクセスログの確認 ● デフォルトポートからの変更
12		VPN 経由での 100MB 以上の ファイルアップロード		多数	● 該当サーバのアクセスログの確認
13		Untrust IP（Poor Reputation Ip） からの接続試行	多数 （外部海外 IP）		● NW 機器のアクセスログの確認 ● 悪性 IP アドレスの遮断

レポート例2.4-2：脅威分析 フィッシングの例

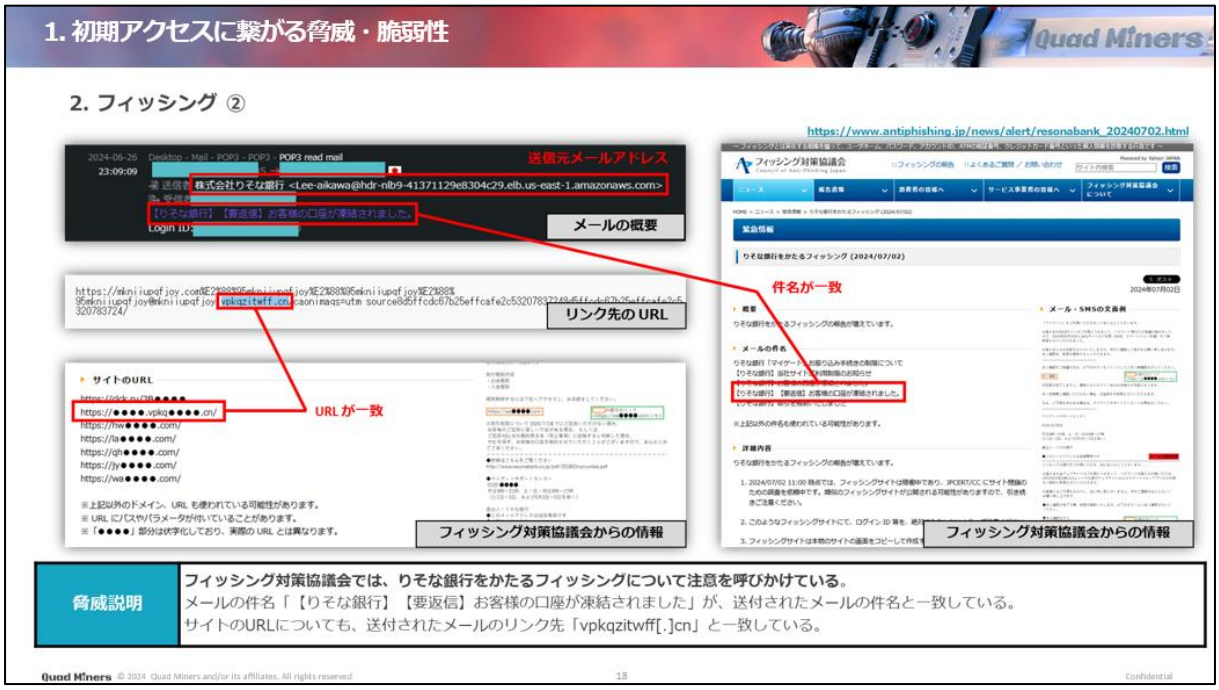
1. 初期アクセスに繋がる脅威・脆弱性

2. フィッシング ①

「ファイル検索」機能から再構築されたメール本文を確認したところ

脅威説明	メールアドレス「　　@　　」に対し、**フィッシングメールが送付されていた**ことを確認した。 りそな銀行をかたっており、内容としては、パスワード入力相違が繰り返されたことにより口座が凍結されたので本人確認をしてください、というもの。

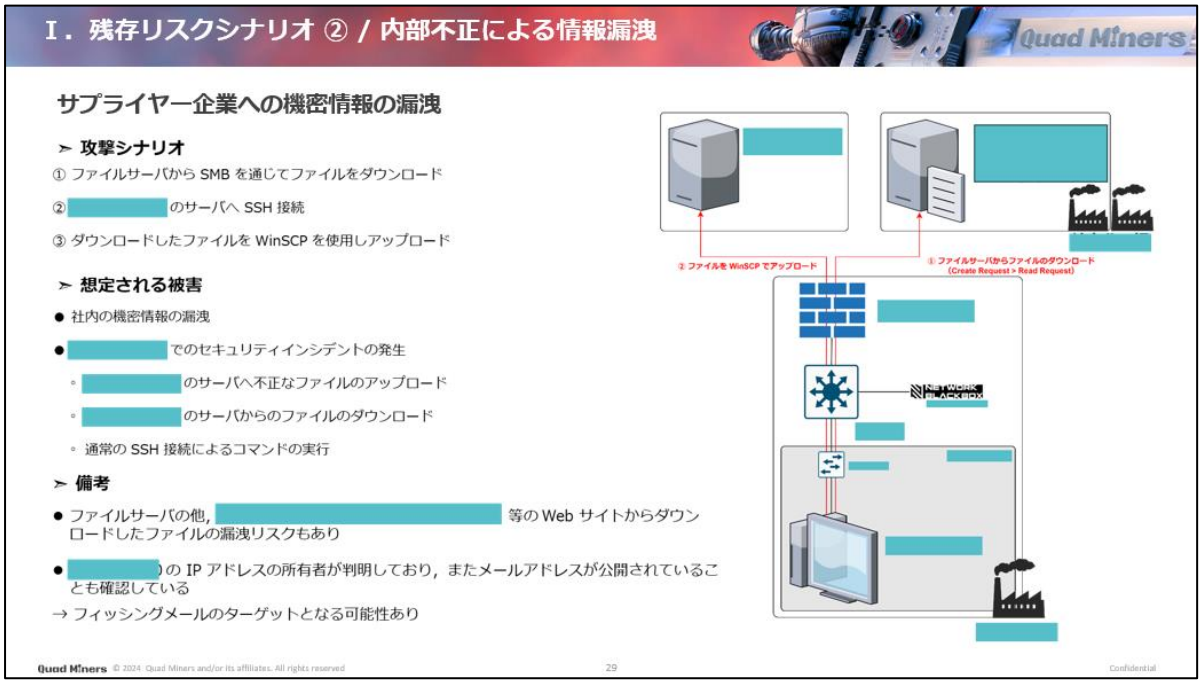
レポート例2.4-2：脅威分析 フィッシングの例2



2.4.3. 残存リスクシナリオ

見つけた脆弱性を基づいた攻撃シナリオを組んで攻撃の流れやその攻撃による被害を想定して、対策ご提案する事ができます。

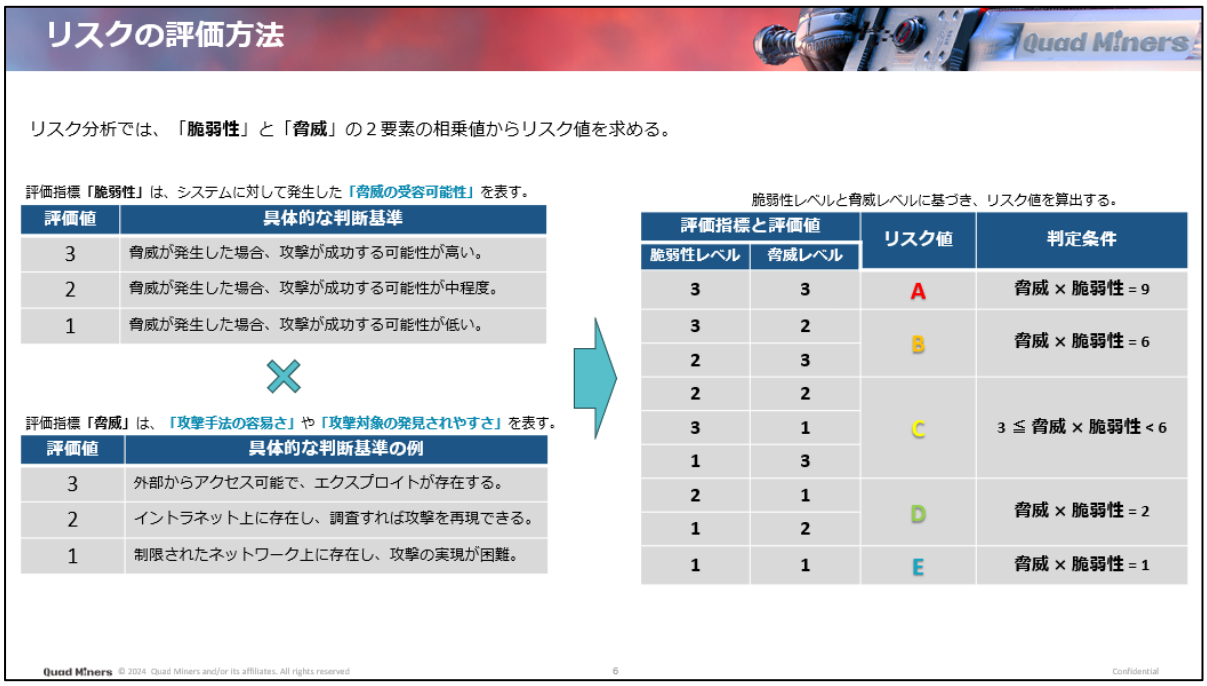
レポート例2.4-3：残存リスクシナリオ サプライヤー企業への秘密情報の漏洩



2.4.4. リスクスコアリング

基準に点数をつけてリスクレベルを決めてレベルごとに対応方法をご提示します。

レポート例2.4-4：リスクスコアリング リスクスコアリングの基準



リスクの評価方法

リスク分析では、「**脆弱性**」と「**脅威**」の２要素の相乗値からリスク値を求める。

評価指標「**脆弱性**」は、システムに対して発生した「**脅威の受容可能性**」を表す。

評価値	具体的な判断基準
3	脅威が発生した場合、攻撃が成功する可能性が高い。
2	脅威が発生した場合、攻撃が成功する可能性が中程度。
1	脅威が発生した場合、攻撃が成功する可能性が低い。

×

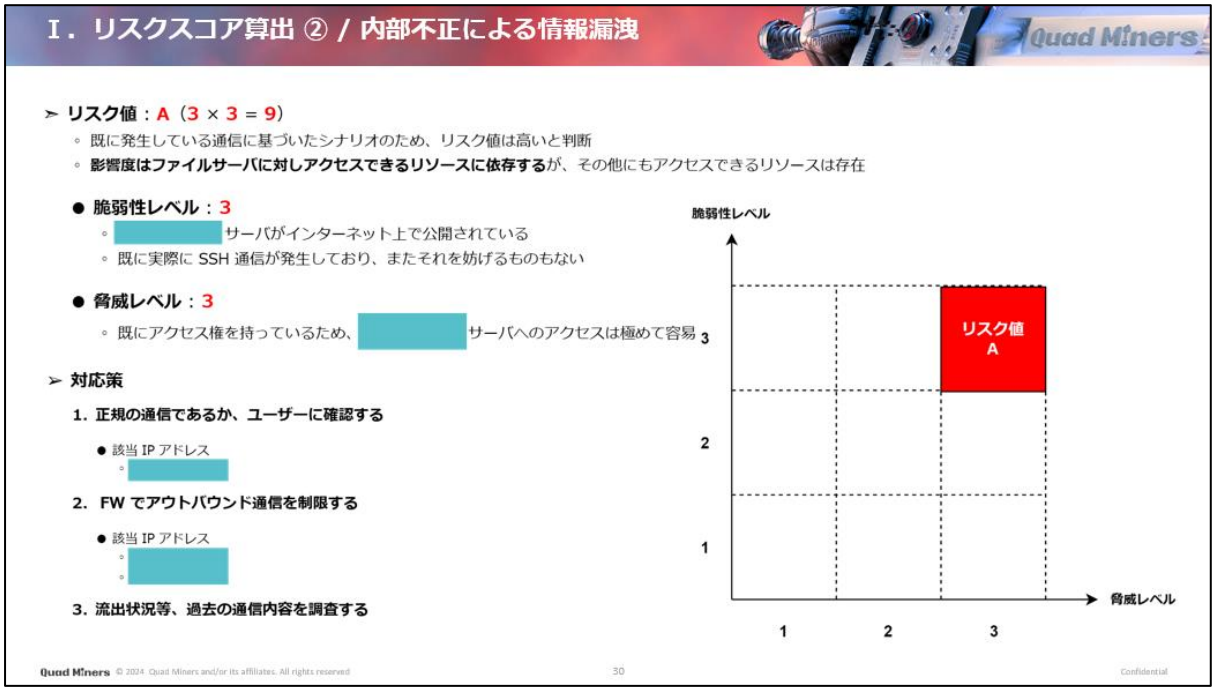
評価指標「**脅威**」は、「**攻撃手法の容易さ**」や「**攻撃対象の発見されやすさ**」を表す。

評価値	具体的な判断基準の例
3	外部からアクセス可能で、エクスプロイトが存在する。
2	イントラネット上に存在し、調査すれば攻撃を再現できる。
1	制限されたネットワーク上に存在し、攻撃の実現が困難。

脆弱性レベルと脅威レベルに基づき、リスク値を算出する。

評価指標と評価値		リスク値	判定条件
脆弱性レベル	脅威レベル		
3	3	A	脅威 × 脆弱性 = 9
3	2	B	脅威 × 脆弱性 = 6
2	3		
2	2	C	3 ≦ 脅威 × 脆弱性 < 6
3	1		
1	3		
2	1	D	脅威 × 脆弱性 = 2
1	2		
1	1	E	脅威 × 脆弱性 = 1

レポート例2.4-4：リスクスコアリング リスクスコアリングの例



Ⅰ．リスクスコア算出 ② / 内部不正による情報漏洩

➢ **リスク値：A（3 × 3 = 9）**
- 既に発生している通信に基づいたシナリオのため、リスク値は高いと判断
- **影響度はファイルサーバに対しアクセスできるリソースに依存する**が、その他にもアクセスできるリソースは存在

● **脆弱性レベル：3**
- [redacted]サーバがインターネット上で公開されている
- 既に実際に SSH 通信が発生しており、またそれを妨げるものもない

● **脅威レベル：3**
- 既にアクセス権を持っているため、[redacted]サーバへのアクセスは極めて容易

➢ **対応策**

1. 正規の通信であるか、ユーザーに確認する
- 該当 IP アドレス
  - [redacted]

2. FW でアウトバウンド通信を制限する
- 該当 IP アドレス
  - [redacted]

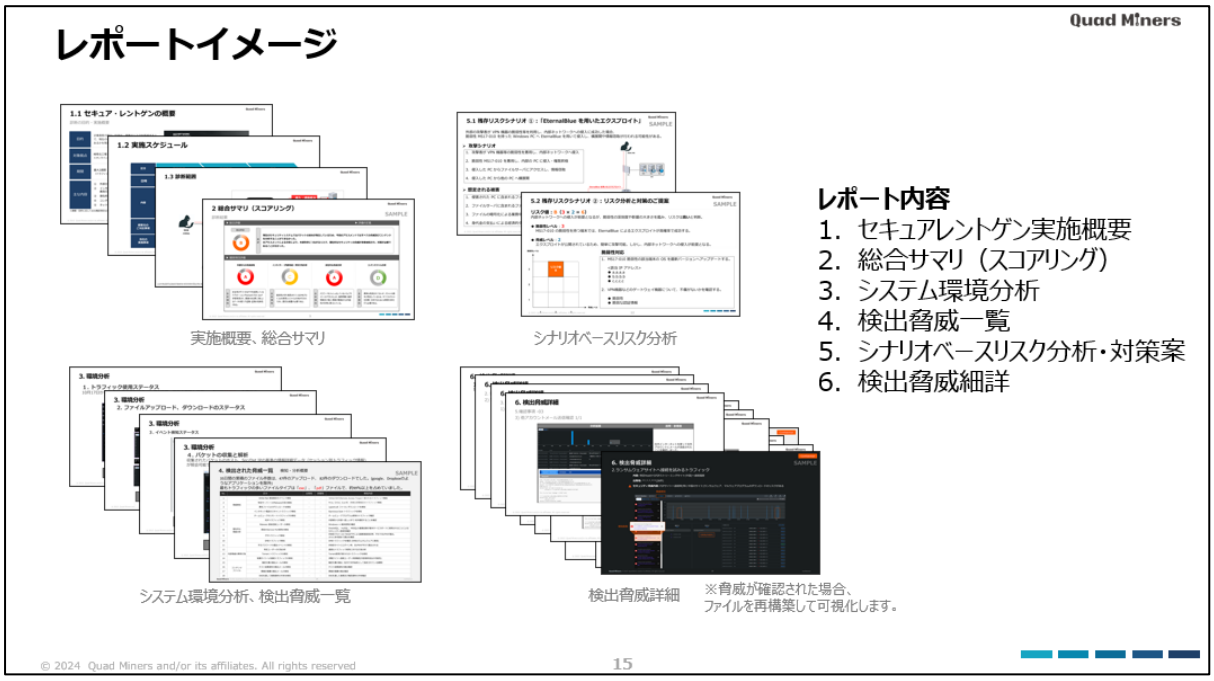
3. 流出状況等、過去の通信内容を調査する

2.5. レポート

2.5.1. レポートについて

レポートは診断終了後5営業日を目途に提出します。

レポート例2.5-1：レポートについて　レポートイメージ



2.5.2. 報告会について

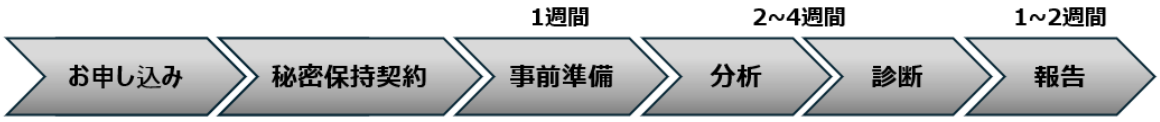
報告会はお客様の状況に合わせてオンライン又は現地で行います。

3. 利用料金

別途営業担当よりお見積りを提示いたします。

4. 契約の流れ

サービス全体の流れを記載しています。



4.1. お申し込み

お客様のニーズと目的の確認を行います。

4.2. 秘密保持契約

診断することにあたって、機密情報を扱うための秘密保持契約を行います。

4.3. 事前準備

診断目的の整理とお客様のネットワーク環境のヒアリング、設置機器のご説明を行います。

4.4. 分析

機器の設置と環境分析を行います。

4.5. 診断

お客様の環境におけるネットワークセキュリティ上のリスクについて診断します。

4.6. 報告

分析、診断結果のレポートを作成して、リスクに対するご提案などを行います。

5. その他

設置後少なくとも1週以上はトラフィックを収集する必要がある為、設置直後1週間は分析を開始しません。

この期間はトラフィックの発生状況により前後する可能性があります。

6. 本書に対するお問い合わせ先

株式会社クワッドマイナージャパン（英文名:Quad Miners Japan Co.,Ltd）

住所：東京都千代田区霞が関3-2-5　霞が関ビル5階

TEL：03-3500-3221

Mail：sales_jp@quadminers.com