

# サイバーリスクを客観的に把握するための ベストプラクティスとは？

～ サイバーセキュリティ評価支援サービスのご紹介

株式会社パロンゴ 代表取締役社長 近藤学

# 通知簿

**通知簿**



**ASM: Attack Surface Management  
(アタックサーフェスマネージメント)**

いつものアイスブレイク

**部下がちゃんとやってる(はず)**

**業者がやってる(はず)**

**全ての設備は把握している(はず)**

**Excel シートに全部○ついてるからちゃんと  
やってる(はず)**

**このサーバがあることはうちの人間しか知らない(はず)**  
**Firewall があるから大丈夫(なはず)**  
**アンチウイルス製品いれたから大丈夫(なはず)**  
**外部とは通信しない環境だから大丈夫(なはず)**  
**新環境使ってて古い環境使ってないので大丈夫(なはず)**

**この春に脆弱性診断受けたから今も大丈夫(なはず)**  
**うちには取られるようなものないから大丈夫(なはず)**  
**うちよりももっと大きな企業さんが攻撃される(はず)**  
**パソコンが数台感染してもなんとかなる(はず)**  
**取引先とはシステム接続してないのでリスクはない(はず)**

**感想 · 希望 · 期待**



**攻撃者は皆さんの都合や気持ちに合わせて  
攻撃するわけじゃないですよ？**

**謙虛 · 客觀**

# 通知簿

# サイバーセキュリティリスクに関する 「通知簿」

# 企業のセキュリティリスク状況を OSINT<sup>(※)</sup>等をベースに可視化

※合法かつ一般的に入手可能な情報を用い、事象を深く分析する手法

**感染を示唆する情報はないか？  
放置されている脆弱性はないか？  
開いてるとまずいポートはないか？  
などなど…**

**(余談)「勝手にうちを調べたのか!!」**

# 企業のセキュリティリスク状況を OSINT<sup>(※)</sup>等をベースに可視化

※合法かつ一般的に入手可能な情報を用い、事象を深く分析する手法



**ちゃんとできているかを  
客観的・継続的・網羅的に  
確認しよう**

**他社の「通知簿」も!**

**サプライチェーンリスクへの備え**

**実例:Firewall の脆弱性が放置されているケース**

# - Findings

Vendor Access

Reports and Assessments

Actions

5 Rows

Vendor Access (0/10)

Search...

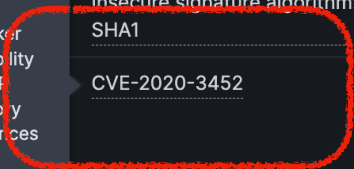
000



Search filter options...

Asset: xxx.xxx.214... Clear All

| Remaining Lifetime | Finding Severity | Asset Importance | Assets  | Details   | Comments | Country |
|--------------------|------------------|------------------|---|---|----------|---------|
| Major              | Moderate         | Medium           | xxx.xxx.214.250   | CVE-2020-3580   |          |         |
| Minor              | Minor            | Medium           | A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. | Detected service: HTTPS/CiscoASA  |          | Japan   |
| Severe             | Severe           | Medium           |   | Allows insecure protocol: TLSv1.0<br>Allows insecure protocol: TLSv1.1<br>Diffie-Hellman prime is less than 2048 bits<br>Short Diffie-Hellman prime is very commonly used |          | Japan   |
| Material           | Material         | Medium           |   | RSA public key is less than 2048 bits<br>Insecure signature algorithm: SHA1   |          | Japan   |
| Material           | Material         | Medium           |   | CVE-2020-3452   |          |         |



- Home
- Heart
- Grid
- Folder
- Network
- Mail
- Speaker
- Calendar

- Risk Vector +
- First Seen +
- Last Seen +
- Refresh +
- Grade +
- Impacts RV Grade +
- Remaining Lifetime +
- Finding Severity +
- Tag +
- Asset Importance +
- Vulnerability +
- Vulnerability Severity +
- Infection Family +
- File Sharing Category +
- Pass / Fail Test +

いくら高価で高性能な  
ソリューションを入れたって  
こんな有様じゃ…

~~年一とかで見ておけばいいんじゃないの？~~

### BitSight Security Rating

About Rating

**620** BASIC

[View Ratings Tree](#)

### Rating Related Risk

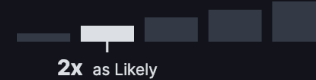
Ransomware Incidents vs a **750+** company

Source

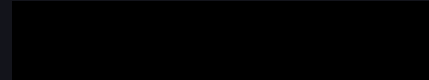


Data Breach Incidents vs a **700+** company

Source

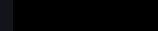


### Company Info



+ more

Homepage



Industry

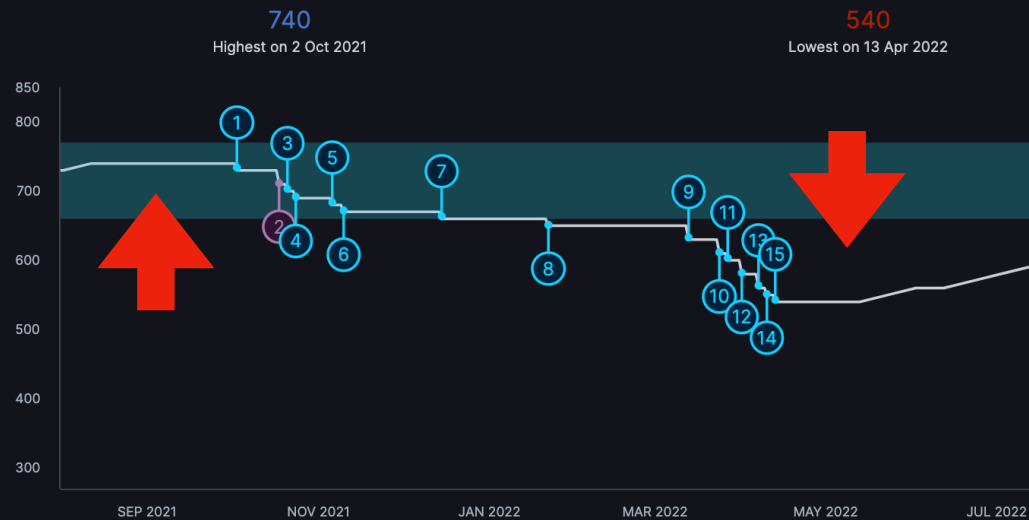
**Technology**

Monitored by

**3 companies**

[Show Details](#)

### Security Ratings



### Highlights

- 15 Effective Date: **13 Apr 2022**  
**10 point drop** (550 ↘ 540)  
Botnet Infection: [Beapy \(1\)](#)
- 14 Effective Date: **10 Apr 2022**  
**10 point drop** (560 ↘ 550)  
Botnet Infection: [Beapy \(1\)](#)  
SSL Certificates: grade change from D to C.
- 13 Effective Date: **7 Apr 2022**  
**20 point drop** (580 ↘ 560)  
Botnet Infection: [Beapy \(1\)](#)
- 12 Effective Date: **1 Apr 2022**  
**20 point drop** (600 ↘ 580)



**皆様の会社は大丈夫ですか？**

**お取引先は大丈夫ですか？**

# サイバーセキュリティリスク評価支援サービス powered by BitSight

～ 企業のサイバーセキュリティリスクを可視化 ～

## セキュリティ対応度合いを評価し、可視化

セキュリティ対策が適切に設定・運用できているかを外部から得られる情報にて監視・観察し、客観的にセキュリティ対策の抜け、漏れ、陳腐化を「通信簿」的に評価、ドリルダウンすることが可能。

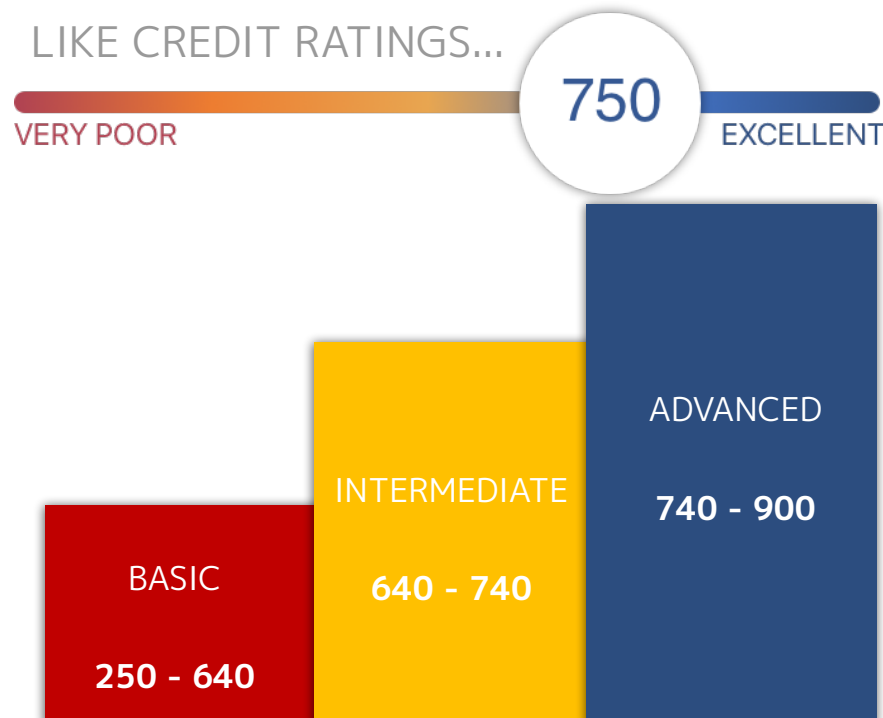
## サプライチェーンリスクも可視化

自社のみならず、取引先や M&A 先にまでセキュリティ対応度合い評価の対象を広げることができるため、取引先等に対するサイバーセキュリティ的サプライチェーンリスクも明確化。

## エキスパートによる対応方針アドバイス

業界経験 25 年以上のエキスパートによる、評価結果のレビューから改善方針に対するアドバイスまでもパッケージ化。

重要度、優先度の選定を効率的かつ確実に行うことで、より効果的なセキュリティ施策実現をサポート。

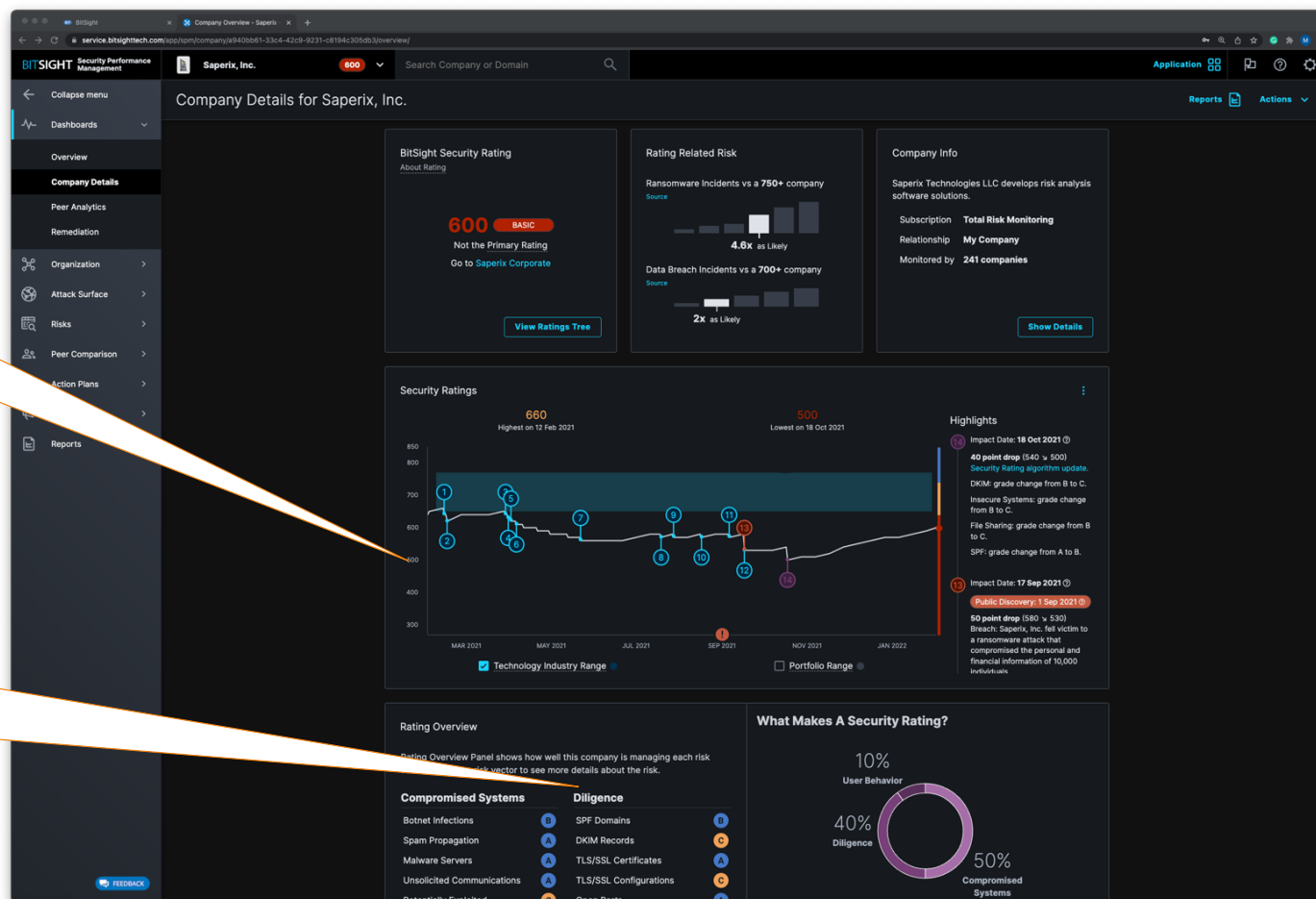


# BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

スコアの変動を時系列で  
確認。  
過去1年間の動きを  
チェックできる。

評価項目毎のグレードを表示。  
どこができていてどこに問題が  
あるのかが一目瞭然。



# BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

評価項目毎に A (良) ~ F (悪) でグレード付け。

マルウェアへの感染状況や、放置されている脆弱性の一覧なども確認可能。

The screenshot displays the BitSight dashboard for Saperix, Inc. The main section is titled "Company Details for Saperix, Inc." and features a "Rating Overview" panel. This panel shows a "What Makes A Security Rating?" donut chart with segments for "User Behavior" (10%), "Diligence" (40%), and "Compromised Systems" (50%). Below the chart, a list of risk vectors is displayed with corresponding grades (A-F) and "N/A" status. The dashboard also includes two tables: "Infections" and "Confirmed Vulnerabilities", both showing data for the last 90 days. The "Infections" table lists "CrossRider" and "AMCleaner" with severity levels and impacted hosts. The "Confirmed Vulnerabilities" table lists various CVEs with severity levels and impacted hosts.

| Name       | Severity | First Seen | Change | Impacted Hosts |
|------------|----------|------------|--------|----------------|
| CrossRider | Material | 2021/11/08 | 0%     | 1              |
| AMCleaner  | Material | 2021/11/10 | 0%     | 1              |

| Name           | Severity | Change | Impacted Hosts |
|----------------|----------|--------|----------------|
| POODLE         | Minor    | 0%     | 20             |
| CVE-2019-10909 | Moderate | 0%     | 2              |
| CVE-2019-11359 | Moderate | 0%     | 2              |
| CVE-2019-11831 | Severe   | 0%     | 2              |
| CVE-2019-6338  | Material | 0%     | 2              |
| CVE-2019-6339  | Severe   | 0%     | 2              |
| CVE-2019-6340  | Material | 0%     | 2              |
| CVE-2019-6341  | Moderate | 0%     | 2              |
| CVE-2020-13863 | Material | 0%     | 2              |
| CVE-2020-13864 | Material | 0%     | 2              |

# BitSight ダッシュボード

セキュリティ対応状況やリスクの詳細を一元管理し詳細まで可視化

良くない結果の詳細をドリルダウンして表示。  
どこの何が悪いのかを深く  
チェックすることが可能。

| Risk Vector        | Finding Identifier | First Seen | Last Seen  | Refresh | Grade | Impacts Risk Vector Grade | Remaining Lifetime | Attributed To   | Finding Severity | Asset    |
|--------------------|--------------------|------------|------------|---------|-------|---------------------------|--------------------|---|------------------|----------|
| SPF                | kramerandross.com  | 2021/12/03 | 2022/01/28 |         | BAD   | Yes                       | 54 days            | Saperix, Inc.   | Material         | Critical |
| SSL Configurations | 23.4.128.47:443    | 2021/08/15 | 2022/01/20 |         | BAD   | Yes                       | 46 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.128.95:443    | 2020/11/15 | 2022/01/31 |         | BAD   | Yes                       | 57 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.128.175:443   | 2020/11/10 | 2022/01/29 |         | BAD   | Yes                       | 55 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.129.15:443    | 2020/11/22 | 2022/01/31 |         | BAD   | Yes                       | 57 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.129.63:443    | 2021/05/28 | 2022/01/31 |         | BAD   | Yes                       | 57 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.129.143:443   | 2020/11/15 | 2022/01/30 |         | BAD   | Yes                       | 57 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.129.239:443   | 2020/11/11 | 2022/02/01 |         | BAD   | Yes                       | 58 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |
| SSL Configurations | 23.4.130.31:443    | 2020/11/20 | 2022/01/26 |         | BAD   | Yes                       | 52 days            | Saperix Corporate<br>Saperix Corporate - US West<br>Saperix, Inc - Wifi testing | Severe           | Low      |

**ちゃんとできているかを  
客観的・継続的・網羅的に  
確認しよう**

# **ASM: Attack Surface Management**



「ASM (Attack Surface Management)」の導入ガイドラインに関するウェブページ。経済産業省のウェブサイトからアクセスされたページで、2023年5月29日に更新された。記事のタイトルは「ASM (Attack Surface Management) 導入ガイドライン～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめた。記事の要約として、経済産業省は、サイバー攻撃から自社のIT資産を守るための手法として注目されている「ASM (Attack Surface Management)」について、自社のセキュリティ戦略に組み込んで適切に活用してもらえよう、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「ASM (Attack Surface Management) 導入ガイドライン～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を作成しました。

### 1. 背景、趣旨

デジタルトランスフォーメーション (DX : Digital Transformation) が進展する中、クラウド利用の拡大に加え、民間事業者が所有するIT資産が増加、点在するとともに、コロナ禍によるテレワークの拡大等を通じて、社会全体でリモート化が進められました。これらにより、サイバー攻撃の起点が増加しています。

こうしたサイバー脅威に対して、自社が保有するIT資産を適切に管理しリスクを洗い出すことが求められますが、人手を介した管理の下では、システム管理部門の把握しきれないシステムが生じやすく、機器の実際の設定も見えづらいことから、自社の全てのIT資産を管理するのは必ずしも容易ではありません。一方で、IT資産について、外部 (インターネット) から把握できる情報を用いた管理サービスを利用することで、既存の管理方法を補完することが可能となっていることから、このような管理サービスの提供が広がっています。

そこで、外部 (インターネット) から把握できる情報を用いてIT資産の適切な管理を可能とするツールやサービスを活用して、外部 (インターネット) に公開されているサーバやネットワーク機器、IoT機器の情報を収集・分析することにより、不正侵入経路となりうるポイントを把握するASM (Attack Surface Management) について、民間事業者における利用の実態を明らかにし、ASMに関連する各種ツールやサービスの特徴や活用方法について整理し、ガイドラインとして取りまとめました。

#### 一般的なASMの特徴とイメージ

- インターネットにつながっている世界中の機器の公開情報を継続的に収集・蓄積
- 特定の条件に合致する機器などを検索可能 (無料でも可能)

The diagram illustrates the process of ASM. On the left, a box labeled '自組織' (Self-Organization) contains icons for various IT assets. Text boxes point to these assets, stating: 'IT資産すべての状況を人手で管理し続けるのは現実的ではない、' (It is not realistic to continue managing all IT assets manually), '設定ミスが発見' (Misconfiguration detected), '意図しない公開設定の発見' (Discovery of unintended public settings), '放置された脆弱性の発見' (Discovery of neglected vulnerabilities), and '未把握の機器の発見' (Discovery of unmonitored devices). On the right, a box labeled 'ASMツール' (ASM Tool) contains icons for a magnifying glass, a database, and a person. Text below it states: '組織の外から、組織に関連する機器の情報を収集しデータベース化する。' (Collect information on devices related to the organization from outside the organization and database it). Arrows indicate the flow of information from the external sources to the organization's IT assets.

**自分たちが実際はどう見えているのか  
どういう状態にあるのかを  
常に分析し、確認しておくことが  
「想定外」を極力少なくする  
第一歩ではないでしょうか？**

**お問い合わせ:  
info@parongo.com**