IBC セキュリティアセスメントサービス

IBC-SAS ログ解析サービス（年間）

パロアルトネットワークス社　次世代ファイアウォール PA シリーズで収集したログをもとに、解析をおこなうサービスです。PA シリーズのレポート機能をさらに深堀りし、お客様環境に即したレポートをご提示します。毎月分析をおこなうことにより、問題点・改善方法の早期把握を実現します。

よくあるお悩み

- ログの内容を解析するノウハウがない
- ログ情報を活用できていない
- ログ解析に工数がかかっている
- 脆弱性の具体的な対応方法を知りたい
- 脆弱性対策をタイムリーに実施できない
- 脆弱性の分析をおこないたいがノウハウがない

サービスの特徴

実績豊富なエンジニアが PA シリーズの詳細な分析をおこないます。毎月の分析により、セキュリティ強化を実現します。

リスク状況の可視化

- 情報漏洩の可能性を検出
- マルウェア感染の可能性を検出
- インシデント対象サーバーの洗い出し

具体的対策の提案

- 検出した脆弱性に関する分析
- PA 本体の脆弱性対応に関する情報提供

セキュリティ品質の保持

- 前月比較で傾向を把握
- 新規インシデントに対して迅速に対応

サービスの流れ

01 ログ情報のご提出（過去 1 か月分）

02 弊社で分析（約 2 週間）

03 報告会開催およびログ解析レポート提出

価格　月額 ￥ 400,000 ～

※ 1 年間のご利用を前提とした金額です。詳細はお問い合わせください。

ログ解析サービス結果 / レポート例

ログ情報をもとにした分析結果をレポートとしてご提供いたします。レポートでは、現状の設定状況とあわせて、お客様環境に則した推奨設定をご案内いたします。

インシデント件数サマリー

■ インシデント種類、重要度別件数

	Critical	High	Medium	Low	Informational
Vulnerability	8 件	30 件	3,879 件	23,230 件	4,232,454 件
Antivirus	0 件	0 件	172 件	0 件	0 件
Wildfire	0 件	0 件	1,649 件	0 件	0 件
Anti-Spyware	0 件	0 件	70 件	0 件	64,294,448 件

■ 総評

本件の解析対象期間 2019 / ×× / ××-2019 / ×× / ×× について、Vulnerability にて Critical 判定が 3 種類（8 件）、High の判定が 6 種類（30 件）ございました。

いずれも対象のソフトウェアを利用していない、もしくは、最新の状態であれば影響を受けません。念のため、ご確認いただくことを推奨いたします。

また、Vulnerability 以外の Antivirus 、Wildfire 、Anti-Spyware においても、全体的に Web サービスを対象とした脅威の検知・マルウェアに関連するトラフィックが多く見受けられました。

引き続き、万が一に備え推奨設定で運用いただくことをお勧めいたします。

インシデント詳細（Vulnerability）

No	重要度	件数	脅威 ID	名称	CVE 番号	詳細	送信元 IP	宛先 IP	コメント
1	critical	5	38598	Android Stagefright Library Overflow Vulnerability	2015-3864 2015-1538 2015-1539 2015-3824 2015-3826 2015-3827 2015-3828 2015-3829	Android の Stagefright（メディア再生サービス）ライブラリにて細工された MP4 ファイルを処理する際に、オーバーフローを引き起こす脆弱性	157.205.xxx.xxx (JP) 183.79.xxx.xxx (JP) 209.85.xxx.xxx (US) 40.107.xxx.xxx (US)	211.8.xxx.xxx (JP)	2015 年に発見された Android バージョン 6 以前の問題。また、ベンダーによってはパッチがリリースされている。 Android の OS バージョン別シェア (https://developer.android.com/about/dashboards/)では、対象端末は全体の 29.5 % (2019 年 1 月現在)。 そのため、現時点ではやや危険性は低い。 業務で Android 端末利用をしている場合、アップデートを推奨する。
2	critical	2	37057	Microsoft Schannel Remote Code Execution Vulnerability	2014-6321	Microsoft の S チャンネル（セキュリティパッケージ）において、細工されたパケットを処理する際に、ヒープオーバーフローが生じる脆弱性	10.10.xxx.xxx 10.10.xxx.xxx	117.18.xxx.xxx (AU) 192.229.xxx.xxx (US)	修正ファイルリリース済。 また、Windows 10 には影響しない。 必要に応じて、対応を推奨。
3	critical	1	38092	Microsoft OpenType Font Parsing Code Execution Vulnerability	2015-2459	Microsoft の OpenType（フォントフォーマット）において、細工された OTF ファイルを処理する際に遠隔でのコード実行を可能とする脆弱性	59.106.xxx.xxx (JP)	10.10.xxx.xxx	修正ファイルリリース済。 PoC が存在し、実際の攻撃も確認されているため、クライアント OS のアップデートがおこなわれていない場合、対策が必要。

IBC
アイビーシー株式会社
本社 〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780 fax.03-5117-2781
西日本事業所 〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014 fax. 06-7177-0542