当資料は重要情報を含むためお取り扱いには
十分ご注意ください。

【サンプル版】

株式会社〇〇〇〇〇〇 御中

セキュリティ運用監視サービス
月次分析レポート

[2021-12-01～2021-12-31]

種別：UTM
製品名：PaloAltoNetworks PA-3220
作成日： 2022 年 1 月 10 日

サービス&セキュリティ株式会社

― 目　次 ―

ⅰ. サービスの概要

1. ネットワーク構成図
2. 監視期間
3. セキュリティ機器
4. サービス稼働率
5. アラート通知件数
6. 問合せ件数
7. 作業件数

ⅱ. 月次分析

1. 総括

1.1 全体分析

1.2 各監視機能別分析

1.2.1 ファイアウォールポリシー

1.2.2 URL フィルタリング

1.2.3 脆弱性防御

1.2.4 アンチスパイウェア

1.2.5 アンチウイルス

1.2.6 WildFire

2. 統計

2.1 ファイアウォールポリシー

2.1.1 日別アラート発生数

2.1.2 レベル別アラート件数

2.1.3 日別通信検知数

2.1.4 送信元 IP トップ 10

2.1.5 宛先 IP トップ 10

2.1.6 宛先 Port トップ 10

2.2 URL フィルタリング

2.2.1 日別アラート発生数

2.2.2 レベル別アラート件数

2.2.3 日別通信検知数

2.2.4 URL フィルタリングカテゴリトップ 10

2.3 脆弱性防御

2.3.1 日別アラート発生数

2.3.2 レベル別アラート件数

2.3.3 日別通信検知数

2.4 アンチスパイウェア

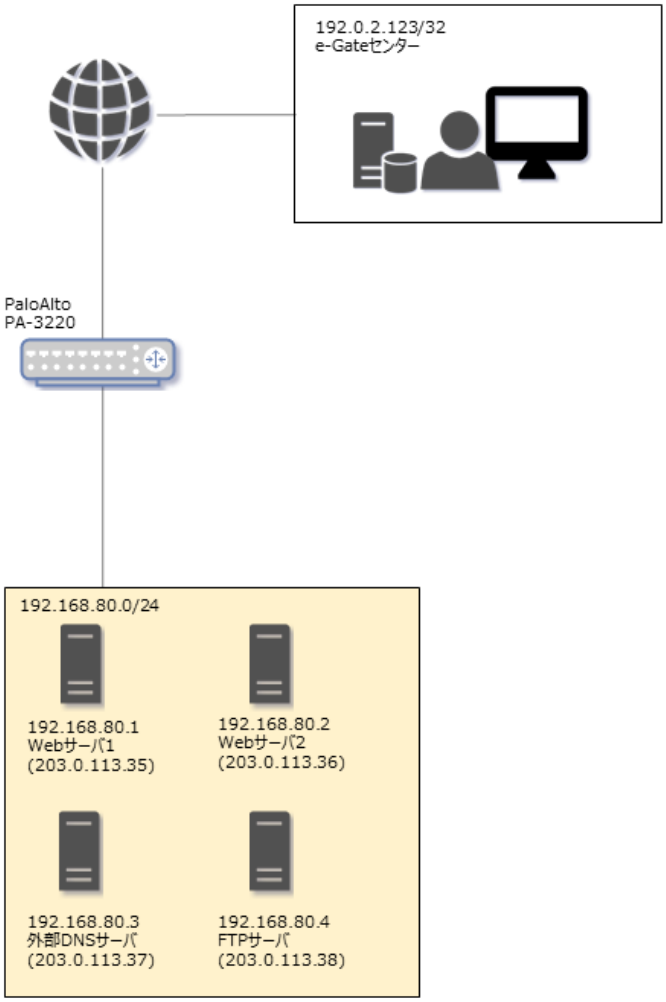
2.4.1 日別アラート発生数

2.4.2 レベル別アラート件数

2.4.3 日別通信検知数
2.5 アンチウイルス
2.5.1 日別アラート発生数
2.5.2 レベル別アラート件数
2.5.3 日別通信検知数
2.6 WildFire
2.6.1 日別アラート発生数
2.6.2 レベル別アラート件数
2.6.3 日別通信検知数
2.7 イベント トップ 10
2.7.1 イベント トップ 10 統計
2.7.2 イベント トップ 10 詳細分析
3. 問合せ履歴
4. 作業実施内訳
5. アラート通知履歴

i. サービスの概要

1. ネットワーク構成図



2. 監視期間

2021-12-01 00:00 ～ 2021-12-31 23:59

3. セキュリティ機器

お客様のネットワークおよびシステムを保護するため、下記セキュリティデバイスのセキュリティ監視を実施しました。

機器	機能	ホスト名	IP アドレス
PaloAltoNetworks PA-3220	UTM	sample-utm	192.0.2.13

4. サービス稼働率

対象期間内のセキュリティ運用監視サービスの稼働率です。

稼働率	停止時間	備考
100%	0.00 時間	障害は発生しておりません

5. アラート通知件数

対象期間内のアラート通知件数です。

対象機能	Fatal	Critical	Minor
ファイアウォールポリシー	0 件	0 件	1 件
URL フィルタリング	0 件	3 件	7 件
脆弱性防御	0 件	0 件	2 件
アンチスパイウェア	0 件	2 件	3 件
アンチウイルス	0 件	0 件	0 件
WildFire	0 件	3 件	6 件

6. 問合せ件数

対象期間内の問合せ件数です。

問合せ件数	対応済み	未対応・対応中
3 件	3 件	0 件

7. 作業件数

対象期間内の作業件数です。

作業件数	対応済み	未対応・対応中
2 件	2 件	0 件

ii. 月次分析

1. 総括

1.1 全体分析

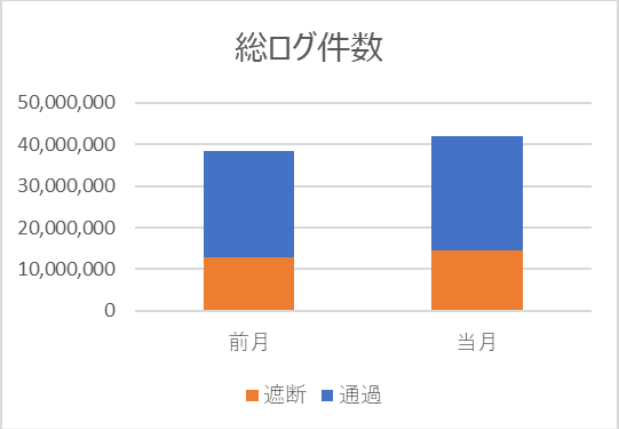
本月次分析レポートの期間内において、セキュリティ侵害によって実害が生じる事象は確認されておりません。

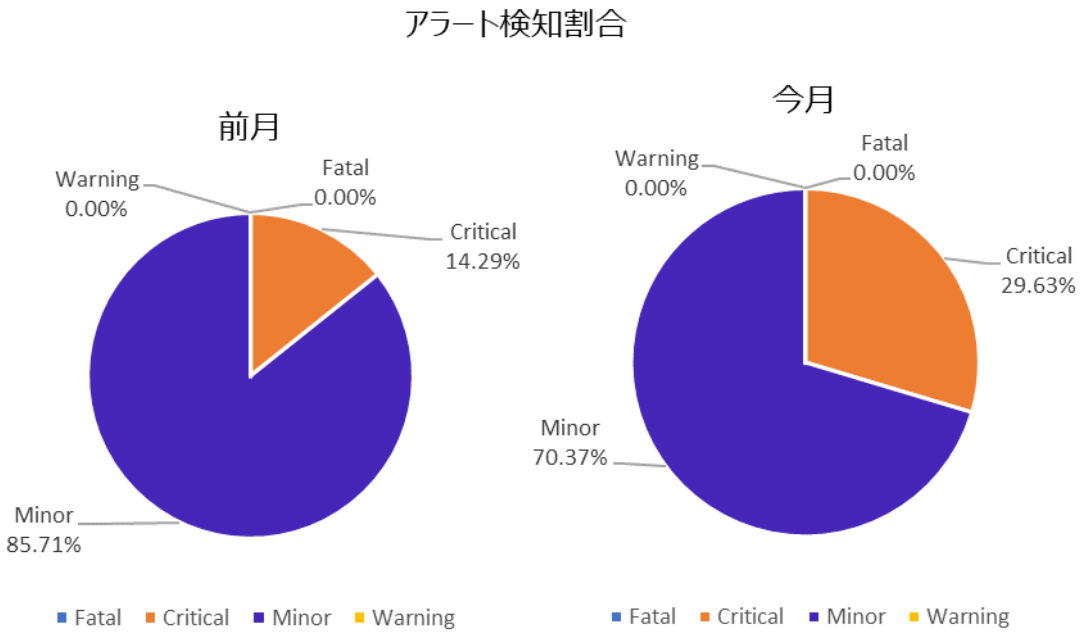
今月は URL フィルタリングにて Critical 以上のアラートが 3 件、アンチスパイウェアにて Critical 以上のアラートが 2 件、WildFire にて Critical 以上のアラートが 3 件発生し、追加でメール通知対応をしております。お客様に確認していただいた結果、問題なしとの回答を頂いております。詳細は「 iii . 統計分析」のイベント分析をご参照ください。

対象期間内の通信件数は次の図のとおりです。総ログ件数は前月と比較して増加傾向にあります。192.0.2.100 からの DNS 通信が約 187 万件発生し、全体の約 3.66%を占めております。通信は通過していますが、他に不審な傾向もみられませんでしたので特に問題はありません。

全体の通信の内 34.27%が遮断されておりますが、遮断比率も 1.16pt と微増であり大きな傾向の変化はみられません。また、遮断ログのうち 443/TCP 及び UDP の HTTPS 通信が約 1,300 万件と約 90%を占めております。通信の大半が内部から外部への通信となっております。詳細に関しましては「1.2.1 ファイアウォールポリシー」をご参照ください。

月度	総ログ件数	遮断ログ件数	遮断比率
前月	38,467,358	12,736,899	33.11%
当月	41,946,836	14,377,645	34.27%
先月比	109.04%	112.88%	1.16pt





危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	5	8	160.00%
Minor	30	19	63.33%
Warning	0	0	-
合計	35	27	77.14%

1.2 各監視機能別分析

1.2.1 ファイアウォールポリシー

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは下記のとおりです。

今月は Minor のアラートを 1 件通知しております。悪性情報のある国外の IP アドレスからの通信を検知したため、通知しております。当該 IP アドレスを調査した所、ポートスキャン等の悪性情報が報告されています。当該通信はこの 1 件のみで収束しておりますが、念のため宛先の機器にて使用していないサービスポートが開放されていないかご確認頂くとともに、当該通信が業務通信であったかどうかご確認頂き、業務通信でない場合は送信元 IP アドレスである「203.0.113.197」について遮断設定をして頂くことを推奨いたします。

No.	検知日時	送信元 IP アドレス	宛先 IP アドレス
1	12 月 4 日 9 時 43 分	203.0.113.197	192.0.2.214

■その他

全体の通信分析では、対象期間内の全体の通信の内 38.73%が遮断されています。遮断ログのうち 443/TCP 及び UDP の HTTPS 通信が約 1,300 万件と遮断ログの大半を占めております。アプリケーションが設定されていない通信(not-applicable)が約 690 万件発生しており、宛先は国内の悪性情報のない IP アドレスが上位の多数を占めています。内部から外部への通信で遮断されておりますが、意図した通信であるか、また遮断されていることにより業務に影響が出ていないか確認することを推奨いたします。

内部間の通信では主に、宛先ポート 162/UDP の SNMPTRAP 通信などシステム監視に関連した通信が多く発生しています。約 12 万件(前月比 74%)と前月と比較して減少しております。一般的な利用とみられる通信であり異常な通信傾向は確認できませんでした。

内部から外部への通信では 443/TCP の HTTPS 通信などの通信が多く発生しております。約 2,800 万件(前月比 115%)と前月と比較して若干増加しております。業務利用とみられる通信であり、その他特定の偏りや不審な兆候など見られない為、問題ございません。

外部から内部への通信では 123/UDP の NTP 通信で 2,769 件発生しています。123/UDP はネットワークに接続されたコンピュータや各種機器の時刻同期に用いられるプロトコルで使用するポートです。2,769 件(前月比 104%)と前月と比較して大きな増減はございません。一般的な利用とみられる通信であり異常な通信傾向は確認できませんでした。

1.2.2 URL フィルタリング

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは下記のとおりです。

今月は Critical のアラートを 3 件通知しております。3 件とも PaloAlto を通過しており、検出された URL で悪性情報を確認しております。下表の宛先 URL に対して、12 月 10 日、12 月 24 日に遮断設定を実施しております。その他、本アラートに関しましてはクライアント端末のウイルスチェックやサイトへのアクセス有無をご確認頂くことを推奨いたします。

No.	送信元 IP アドレス	宛先 IP アドレス	カテゴリ	URL	説明/分析	件数
1	192.0.2.25	198.51.100.13	malware	EXAMPLE 1[.]JP	12 月 4 日に検知。DNS ポイズニングを行うサイトと情報があり、悪性情報が確認されました。12 月 10 日に遮断設定済み。	1
2	192.0.2.30	198.51.100.196	phishing	EXAMPLE 2[.]JP	12 月 9 日に検知。ユーザ認証偽装を利用したサイトと情報があり、悪性情報が確認されました。12 月 10 日に遮断設定済み。	1
3	192.0.2.30	203.0.113.210	malware	EXAMPLE 3[.]CO[.]JP	12 月 23 日に検知。マルウェア感染を引き起こすサイトと情報があり、悪性情報が確認されました。12 月 24 日に遮断設定済み。	1

■その他

今月の通過イベントは、先月に引き続き URL カテゴリ「computer-and-internet-info」や「web-based-email」の発生が多くみられました。

また、URL カテゴリで「proxy-avoidance-and-anonymizers」の通信を検知しております。「proxy-avoidance-and-anonymizers」はプロキシサーバやその他方式で URL フィルタリングや URL 監視をバイパスするサイトの URL カテゴリです。念のため、下記表を参照いただき業務にて使用している通信であるかご確認頂くことを推奨いたします。

No.	検知日時	宛先 URL	URL カテゴリ	件数
1	2021-12-06 06:06:06	EXAMPLE4[.]JP	proxy-avoidance-and-anonymizers	1

1.2.3 脆弱性防御

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは下記のとおりです。

今月は Minor のアラートを 1 件通知しております。国内の IP アドレスからの通信を 1 件検知しており、PaloAlto を通過しております。本アラートに関しましては、対象機器にて Apache Tomcat を使用していないか、また最新のバージョンに更新されているかをご確認頂くことを推奨いたします。詳細に関しましては「2.7.2 イベント トップ 10 詳細分析」をご参照ください。

■その他

今月は、「DCS-2530L Unauthenticated Information Disclosure Vulnerability(90255)」を検知しております。当該イベントは PaloAlto を通過しております。詳細は「2.7.2 イベント トップ 10 詳細分析」をご参照ください。宛先機器にて D-Link 製の IP カメラ「DCS-2530L」を使用していないかご確認をお願いいたします。

1.2.4 アンチスパイウェア

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは下記のとおりです。

今月は Critical のアラートを 2 件通知しております。2 件とも PaloAlto を通過しており、検出されたドメインで悪性情報を確認しております。通信は収束しており、その後不審な通信は確認されておりませんが、念のためクライアント端末のウイルスチェックやサイトへのアクセス有無を確認頂くことを推奨いたします。

以下に Critical のアラートの詳細情報を記載いたします。

No.	宛先 IP アドレス	イベント名	説明/分析	件数
1	192.0.2.253	Suspicious DNS Query(generic:omnatuor.com)(421897263)	検知されたドメインについて、マルウェアとの情報があり、悪性情報が確認されました。	2

■その他

今月は C2 トラフィックに関連付けられている可能性のあるドメインへの DNS 解決を検知しており、通信はすべて PaloAlto を通過しておりますが、ドメインに悪性情報は確認されておらず前後で不審な通信も検知されていないため、影響はないと判断しております。

1.2.5 アンチウイルス

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは発生しておりません。

■その他

今月の通過イベントは、悪性の疑いがあるファイルが添付されたメールを検知しています。添付されたファイルについて分析したところ、悪性情報は確認されず、またその後の通信において不審な通信も検知されておらず問題はございません。

1.2.6 WildFire

■アラート分析

本月次分析レポートの期間内において、即時報告対象となったイベントは下記のとおりです。

今月は Critical のアラートを 3 件通知しております。3 件とも PaloAlto を通過しており、検出されたリンクで悪性情報を確認しております。リンクにアクセスしたとの情報はございませんが、念のためクライアント端末のウイルスチェックやリンクへのアクセス有無を確認頂くことを推奨いたします。

No.	発生日時	送信元 IP アドレス	宛先 IP アドレス	イベント名	説明/分析
1	2021/12/13 15:32:20	203.0.113.167	192.0.2.38	Email Link(52143)	メールに含まれたリンクについて、フィッシングサイトとの情報があり、悪性情報が確認されました。
2	2021/12/18 11:12:47	203.0.113.167	192.0.2.18	Email Link(52143)	メールに含まれたリンクについて、フィッシングサイトとの情報があり、悪性情報が確認されました。
3	2021/12/18 17:22:10	203.0.113.167	192.0.2.18	Email Link(52143)	メールに含まれたリンクについて、フィッシングサイトとの情報があり、悪性情報が確認されました。

■その他

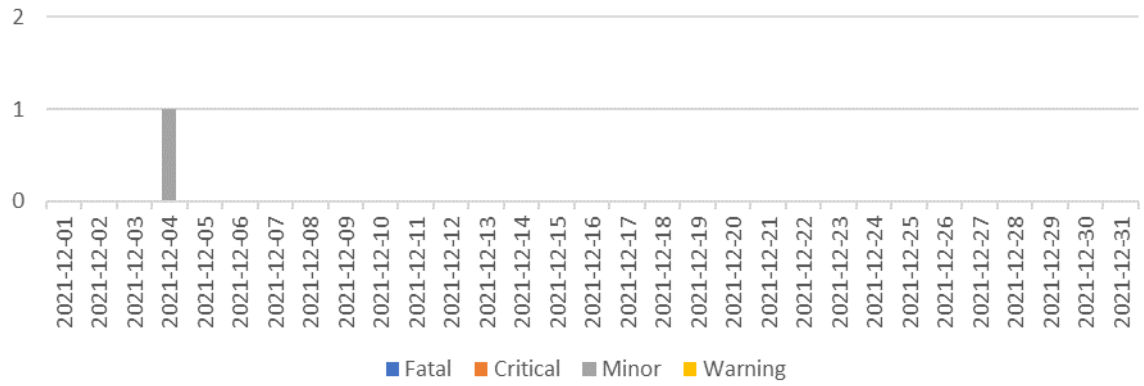
本月次分析レポートの期間内において、PaloAlto の重大度(Severity)「low」以上のイベントは発生しておりません。

2. 統計

2.1 ファイアウォールポリシー

2.1.1 日別アラート発生数

ファイアウォールポリシーの日別アラート発生数を報告いたします。



日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	0	1	0	1
2021-12-05	0	0	0	0	0
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	0	0	0	0
2021-12-10	0	0	0	0	0
2021-12-11	0	0	0	0	0
2021-12-12	0	0	0	0	0
2021-12-13	0	0	0	0	0
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0
2021-12-16	0	0	0	0	0

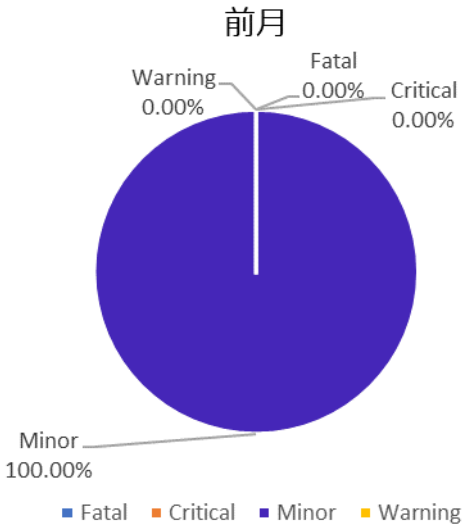
セキュリティ運用監視サービス 月次分析レポート

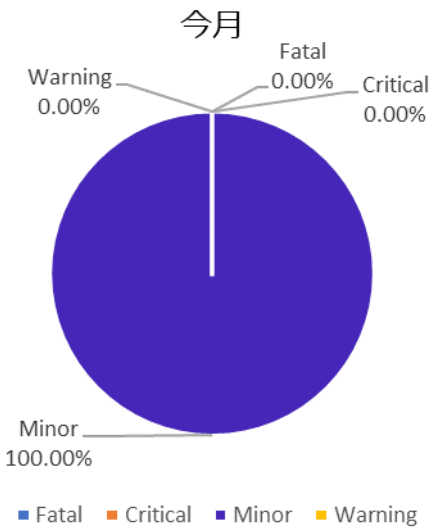
作成日 :2022-01-10

日付	Fatal	Critical	Minor	Warning	総計
2021-12-17	0	0	0	0	0
2021-12-18	0	0	0	0	0
2021-12-19	0	0	0	0	0
2021-12-20	0	0	0	0	0
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	0	0	0	0
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	0	0	0
2021-12-27	0	0	0	0	0
2021-12-28	0	0	0	0	0
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	0	1	0	1

2.1.2 レベル別アラート件数

ファイアウォールポリシーのアラート検知数を報告いたします。

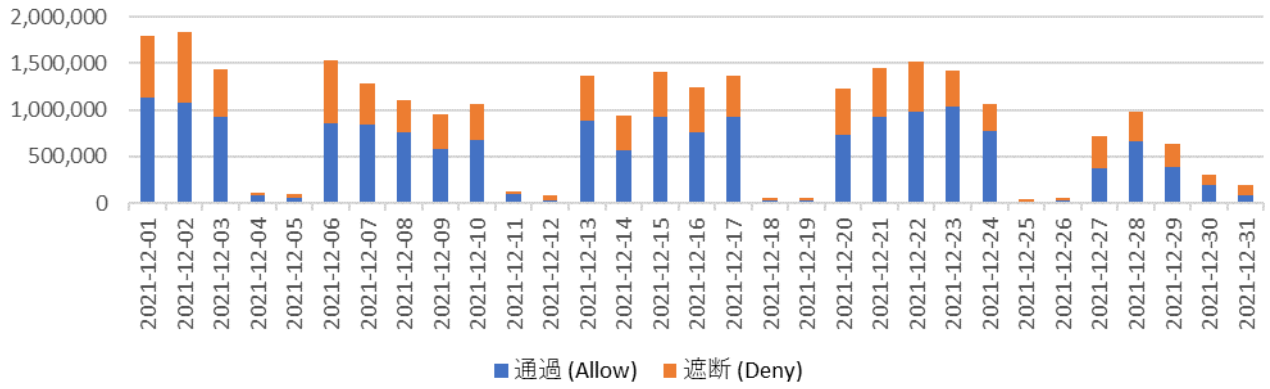




危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	0	0	-
Minor	3	1	33.33%
Warning	0	0	-
合計	3	1	33.33%

2.1.3 日別通信検知数

ファイアウォールポリシーの日別検知数を報告いたします。

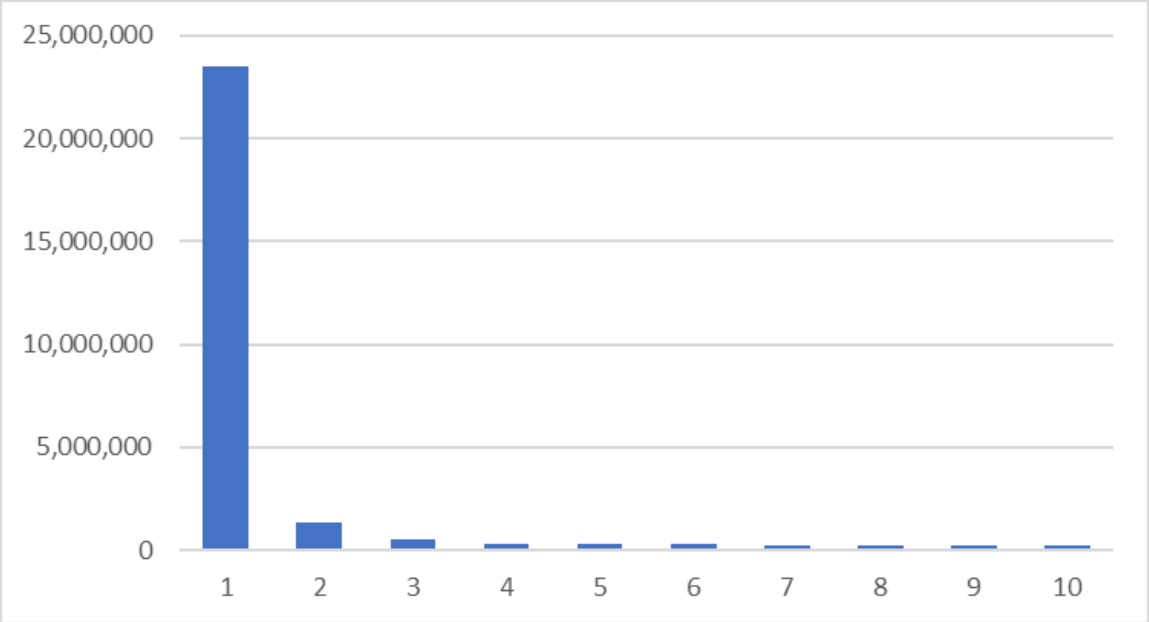


日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	1,135,189	655,218	1,790,407
2021-12-02	1,083,679	752,572	1,836,251
2021-12-03	926,253	515,942	1,442,195
2021-12-04	83,527	26,737	110,264
2021-12-05	62,537	29,375	91,912
2021-12-06	853,437	673,778	1,527,215
2021-12-07	846,523	437,472	1,283,995
2021-12-08	763,694	342,839	1,106,533
2021-12-09	574,846	374,772	949,618
2021-12-10	674,943	392,725	1,067,668
2021-12-11	92,639	37,649	130,288
2021-12-12	29,936	49,846	79,782
2021-12-13	882,692	483,628	1,366,320
2021-12-14	572,002	373,723	945,725
2021-12-15	926,273	487,269	1,413,542
2021-12-16	765,252	472,814	1,238,066
2021-12-17	924,293	441,240	1,365,533
2021-12-18	27,722	33,728	61,450
2021-12-19	26,666	28,763	55,429
2021-12-20	728,372	505,194	1,233,566

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-21	927,363	529,767	1,457,130
2021-12-22	975,383	539,203	1,514,586
2021-12-23	1,039,596	383,393	1,422,989
2021-12-24	772,362	293,667	1,066,029
2021-12-25	10,179	32,628	42,807
2021-12-26	27,462	24,866	52,328
2021-12-27	373,937	343,765	717,702
2021-12-28	659,197	327,538	986,735
2021-12-29	384,289	252,508	636,797
2021-12-30	187,477	116,257	303,734
2021-12-31	86,307	111,219	197,526
合計	17,424,027	10,070,095	27,494,122

2.1.4 送信元 IP トップ 10

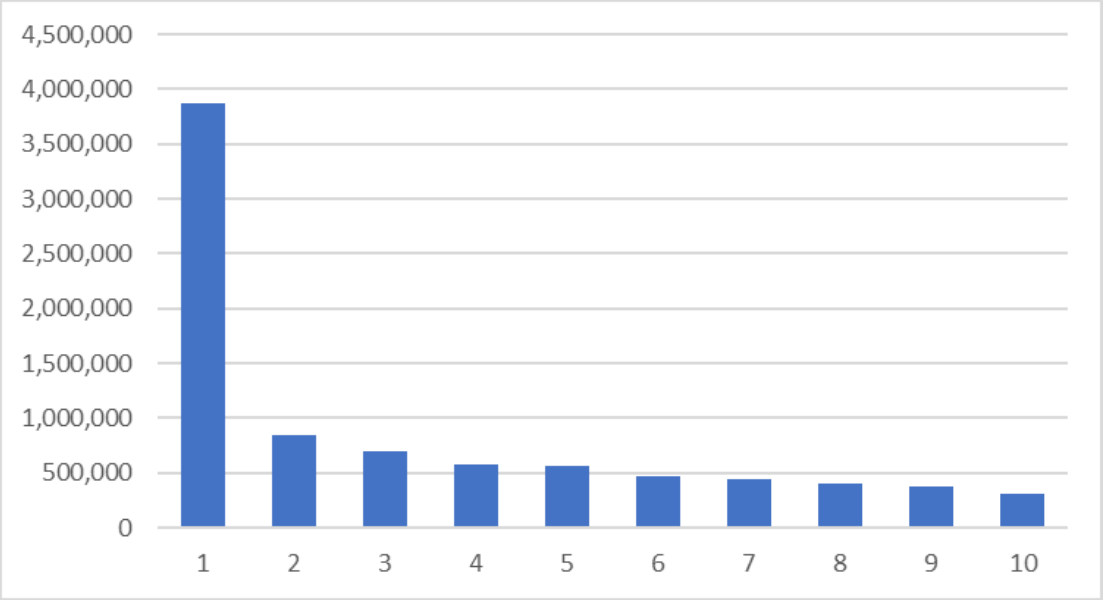
ファイアウォールポリシーの発生件数が多い送信元 IP アドレス トップ 10 を報告いたします。



No	送信元 IP アドレス	国名	機関名	前月度	今月度	前月比
1	192.0.2.214	-	-	25,753,563	23,473,522	104.41%
2	192.0.2.95	-	-	2,936,822	1,381,678	128.77%
3	192.0.2.135	-	-	835,292	524,317	62.77%
4	192.0.2.129	-	-	836,272	287,637	34.40%
5	192.0.2.23	-	-	362,772	283,750	78.22%
6	192.0.2.222	-	-	263,426	269,328	102.24%
7	192.0.2.180	-	-	362,618	247,546	68.27%
8	192.0.2.75	-	-	287,362	226,772	78.92%
9	192.0.2.76	-	-	328,672	218,756	66.56%
10	192.0.2.114	-	-	123,800	207,253	167.41%

2.1.5 宛先 IP トップ 10

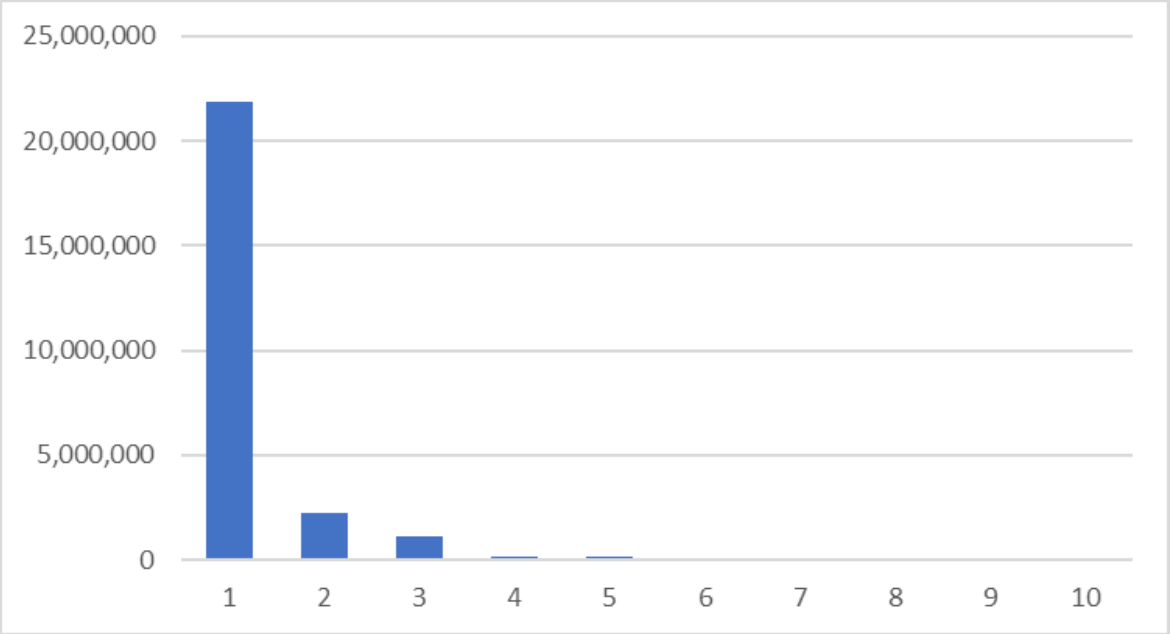
ファイアウォールポリシーの発生件数が多い宛先 IP アドレス トップ 10 を報告いたします。



No	宛先 IP アドレス	国名	機関名	前月度	今月度	前月比
1	203.0.113.146	AU	Test Net	2,893,671	3,866,289	133.61%
2	203.0.113.242	AU	Test Net	278,572	852,346	305.97%
3	203.0.113.123	AU	Test Net	278,321	698,132	250.84%
4	203.0.113.22	AU	Test Net	786,322	577,826	73.48%
5	203.0.113.15	AU	Test Net	987,256	567,625	57.50%
6	203.0.113.207	AU	Test Net	682,612	469,062	68.72%
7	203.0.113.138	AU	Test Net	1,872,772	438,709	23.43%
8	203.0.113.160	AU	Test Net	636,236	397,986	62.55%
9	203.0.113.91	AU	Test Net	273,272	379,822	138.99%
10	203.0.113.196	AU	Test Net	673,813	308,457	45.78%

2.1.6 宛先 Port トップ 10

ファイアウォールポリシーの発生件数が多い宛先 ポート トップ 10 を報告いたします。

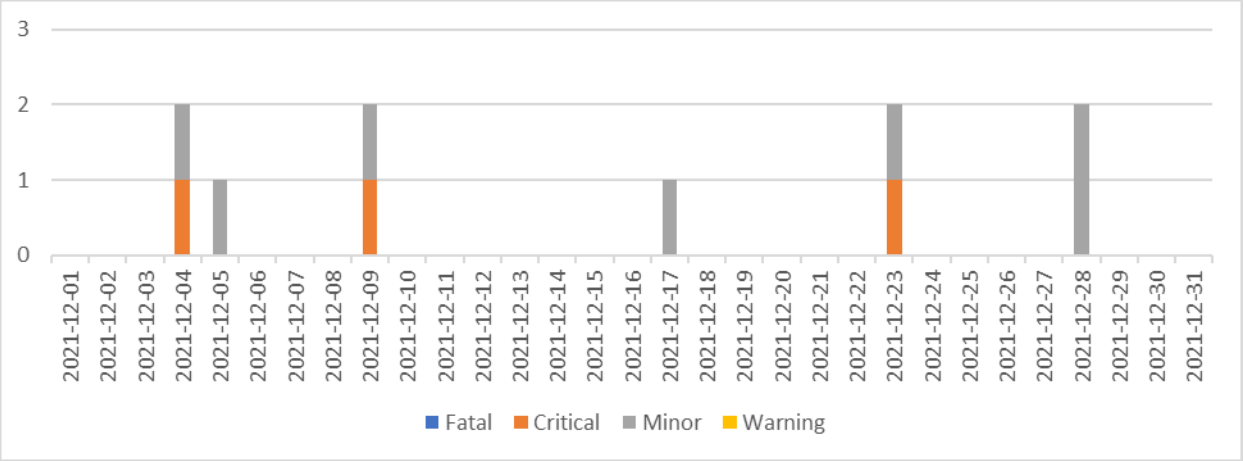


No	宛先ポート	プロトコル	件数
1	443	TCP	21,900,362
2	53	UDP	2,211,866
3	80	TCP	1,127,375
4	162	UDP	162,859
5	5228	TCP	124,468
6	123	UDP	70,418
7	3544	UDP	51,178
8	514	UDP	36,511
9	161	UDP	21,836
10	445	TCP	17,854

2.2 URL フィルタリング

2.2.1 日別アラート発生数

URL フィルタリングの日別アラート発生数を報告いたします。

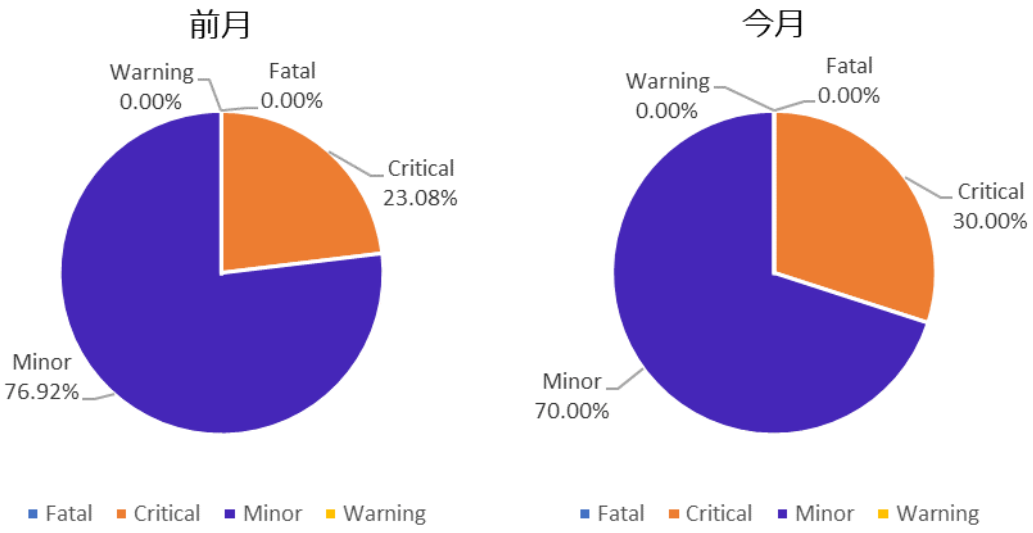


日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	1	1	0	2
2021-12-05	0	0	1	0	1
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	1	1	0	2
2021-12-10	0	0	0	0	0
2021-12-11	0	0	0	0	0
2021-12-12	0	0	0	0	0
2021-12-13	0	0	0	0	0
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0
2021-12-16	0	0	0	0	0
2021-12-17	0	0	1	0	1
2021-12-18	0	0	0	0	0

日付	Fatal	Critical	Minor	Warning	総計
2021-12-19	0	0	0	0	0
2021-12-20	0	0	0	0	0
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	1	1	0	2
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	0	0	0
2021-12-27	0	0	0	0	0
2021-12-28	0	0	2	0	2
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	3	7	0	10

2.2.2 レベル別アラート件数

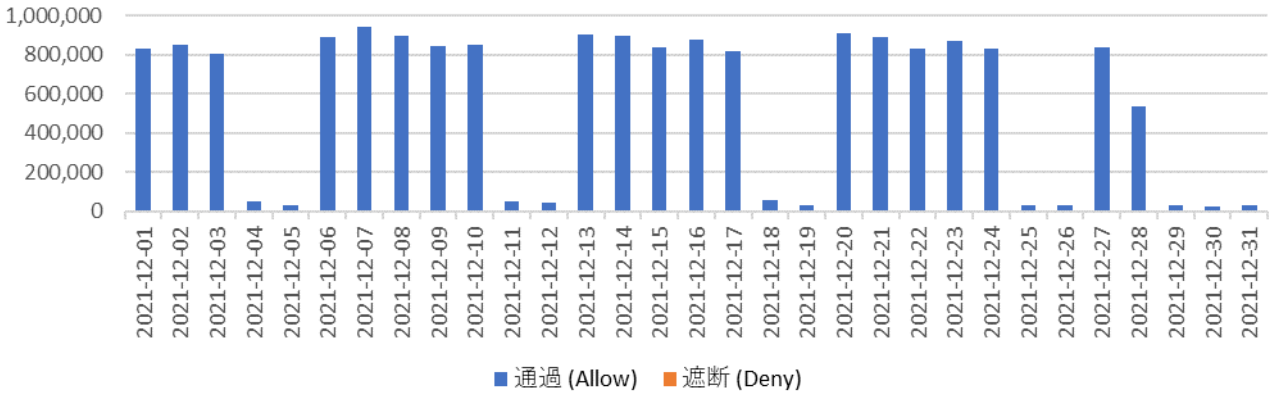
URL フィルタリングのアラート検知数を報告いたします。



危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	3	3	100.00%
Minor	10	7	70.00%
Warning	0	0	-
合計	13	10	76.92%

2.2.3 日別通信検知数

URL フィルタリングの日別検知数を報告いたします。



日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	835,096	0	835,096
2021-12-02	853,650	0	853,650
2021-12-03	808,282	0	808,282
2021-12-04	51,641	0	51,641
2021-12-05	31,287	0	31,287
2021-12-06	888,579	0	888,579
2021-12-07	944,800	0	944,800
2021-12-08	894,763	0	894,763
2021-12-09	846,841	0	846,841
2021-12-10	849,671	0	849,671
2021-12-11	52,692	0	52,692
2021-12-12	44,661	0	44,661
2021-12-13	901,234	0	901,234
2021-12-14	899,521	0	899,521
2021-12-15	836,583	0	836,583
2021-12-16	876,296	0	876,296
2021-12-17	821,292	0	821,292
2021-12-18	58,137	0	58,137
2021-12-19	33,488	0	33,488
2021-12-20	910,483	0	910,483

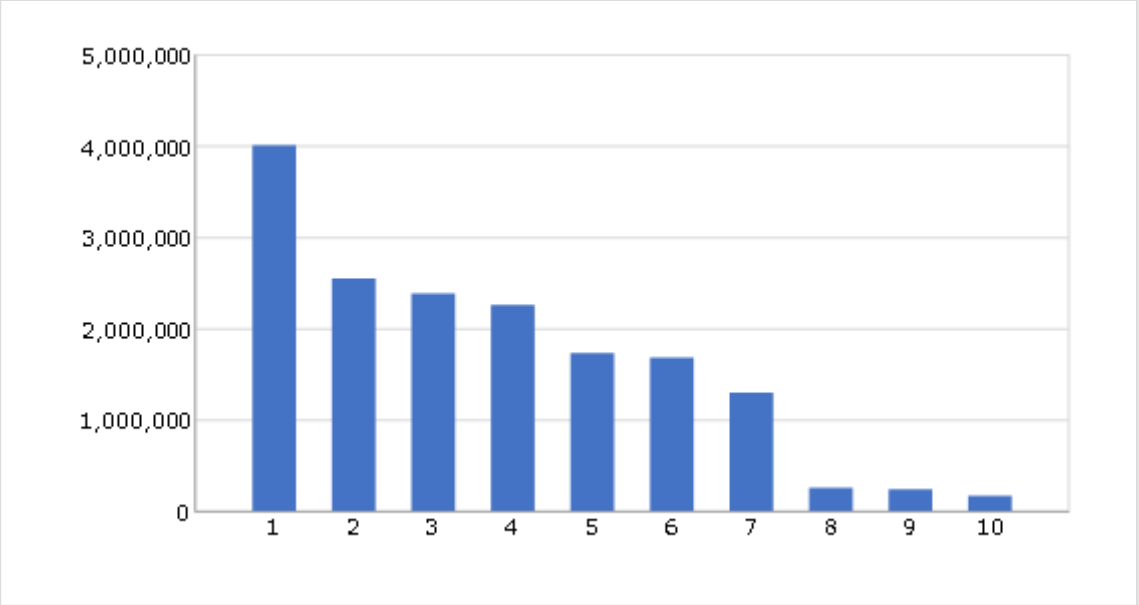
セキュリティ運用監視サービス 月次分析レポート

作成日 :2022-01-10

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-21	893,757	0	893,757
2021-12-22	829,893	0	829,893
2021-12-23	869,109	0	869,109
2021-12-24	832,359	0	832,359
2021-12-25	32,173	0	32,173
2021-12-26	35,275	0	35,275
2021-12-27	836,859	0	836,859
2021-12-28	539,374	0	539,374
2021-12-29	32,478	0	32,478
2021-12-30	24,012	0	24,012
2021-12-31	30,552	0	30,552
合計	17,394,838	0	17,394,838

2.2.4 URL フィルタリングカテゴリ トップ 10

URL フィルタリングの発生件数が多いアクセスカテゴリトップ 10 を報告いたします。

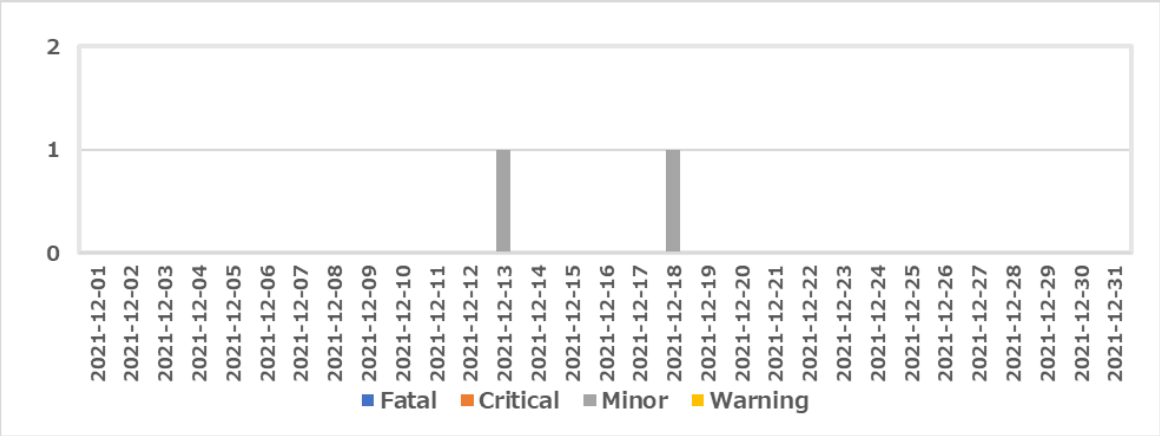


No	URL カテゴリ	件数
1	computer-and-internet-info	3,914,275
2	web-based-email	2,538,375
3	search-engines	2,398,835
4	business-and-economy	2,222,634
5	content-delivery-networks	1,792,356
6	internet-portals	1,683,385
7	web-advertisements	1,318,754
8	social-networking	252,019
9	government	242,345
10	news	174,936

2.3 脆弱性防御

2.3.1 日別アラート発生数

脆弱性防御の日別アラート発生数を報告いたします。

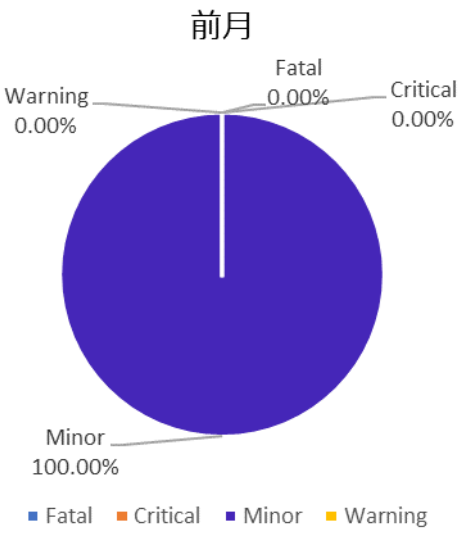


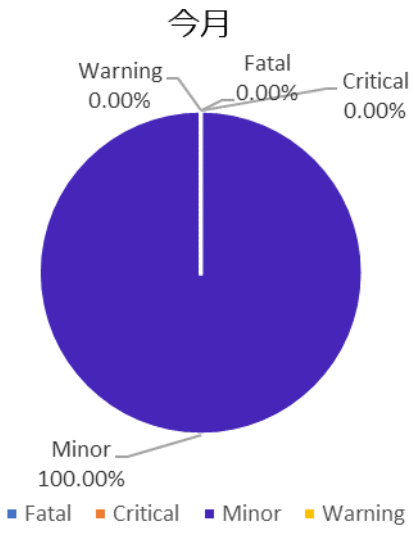
日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	0	0	0	0
2021-12-05	0	0	0	0	0
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	0	0	0	0
2021-12-10	0	0	0	0	0
2021-12-11	0	0	0	0	0
2021-12-12	0	0	1	0	1
2021-12-13	0	0	0	0	0
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0
2021-12-16	0	0	0	0	0
2021-12-17	0	0	1	0	1
2021-12-18	0	0	0	0	0
2021-12-19	0	0	0	0	0

日付	Fatal	Critical	Minor	Warning	総計
2021-12-20	0	0	0	0	0
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	0	0	0	0
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	0	0	0
2021-12-27	0	0	0	0	0
2021-12-28	0	0	0	0	0
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	0	2	0	2

2.3.2 レベル別アラート件数

脆弱性防御のアラート検知数を報告いたします。

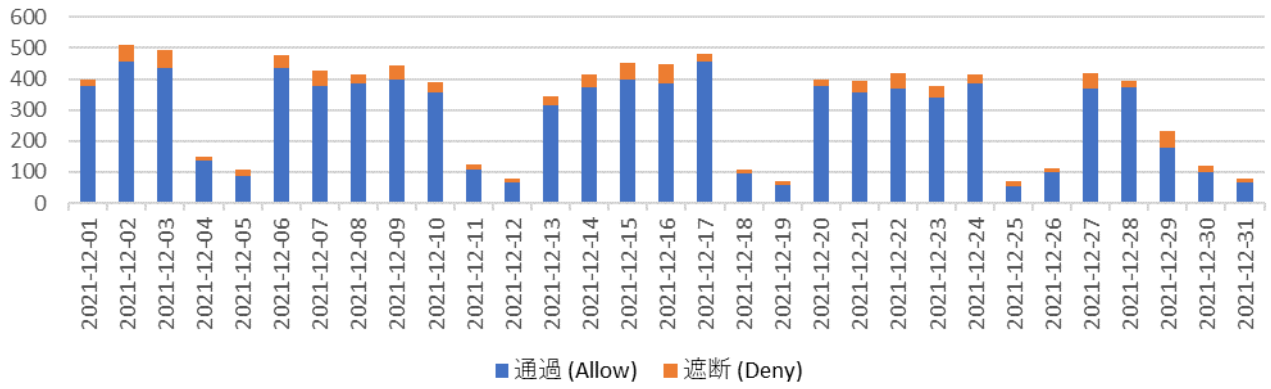




危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	0	0	-
Minor	1	2	200.00%
Warning	0	0	-
合計	1	2	200.00%

2.3.3 日別通信検知数

脆弱性防御の日別検知数を報告いたします。



日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	377	23	400
2021-12-02	456	53	509
2021-12-03	435	58	493
2021-12-04	135	15	150
2021-12-05	86	21	107
2021-12-06	437	39	476
2021-12-07	376	49	425
2021-12-08	386	28	414
2021-12-09	399	44	443
2021-12-10	357	31	388
2021-12-11	107	17	124
2021-12-12	67	12	79
2021-12-13	317	27	344
2021-12-14	375	41	416
2021-12-15	399	51	450
2021-12-16	385	63	448
2021-12-17	456	26	482
2021-12-18	97	11	108
2021-12-19	57	12	69

セキュリティ運用監視サービス 月次分析レポート

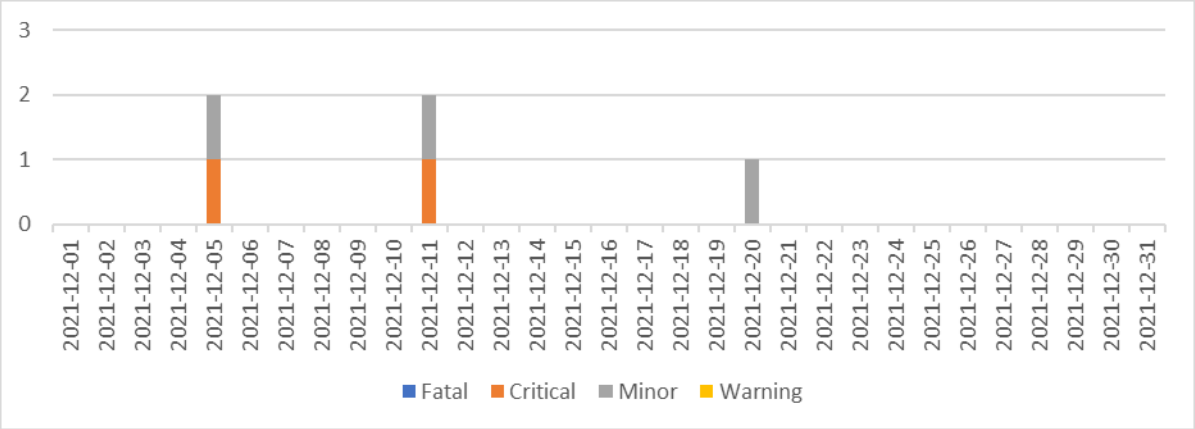
作成日 :2022-01-10

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-20	376	23	399
2021-12-21	358	34	392
2021-12-22	367	53	420
2021-12-23	338	39	377
2021-12-24	386	29	415
2021-12-25	56	16	72
2021-12-26	99	12	111
2021-12-27	368	51	419
2021-12-28	375	18	393
2021-12-29	178	53	231
2021-12-30	98	23	121
2021-12-31	68	13	81
合計	8,771	985	9,756

2.4 アンチスパイウェア

2.4.1 日別アラート発生数

アンチスパイウェアの日別アラート発生数を報告いたします。

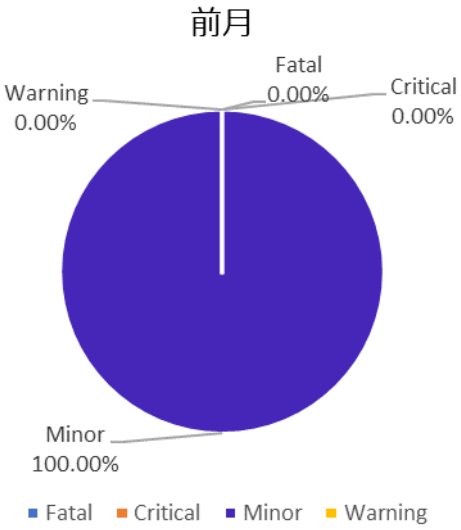


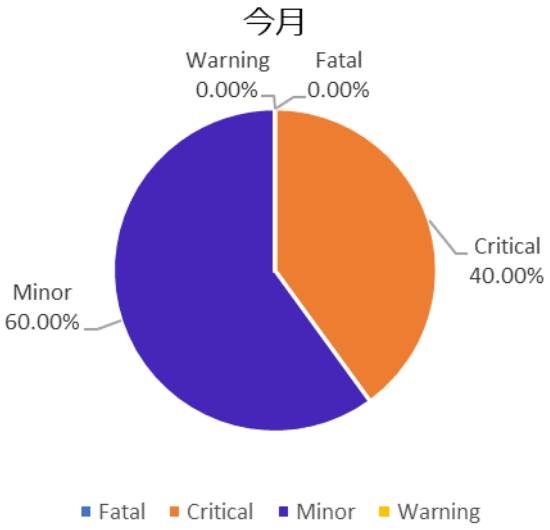
日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	0	0	0	0
2021-12-05	0	1	1	0	2
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	0	0	0	0
2021-12-10	0	0	0	0	0
2021-12-11	0	1	1	0	2
2021-12-12	0	0	0	0	0
2021-12-13	0	0	0	0	0
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0
2021-12-16	0	0	0	0	0
2021-12-17	0	0	0	0	0
2021-12-18	0	0	0	0	0
2021-12-19	0	0	0	0	0

日付	Fatal	Critical	Minor	Warning	総計
2021-12-20	0	0	1	0	1
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	0	0	0	0
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	0	0	0
2021-12-27	0	0	0	0	0
2021-12-28	0	0	0	0	0
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	2	3	0	5

2.4.2 レベル別アラート件数

アンチスパイウェアのアラート検知数を報告いたします。

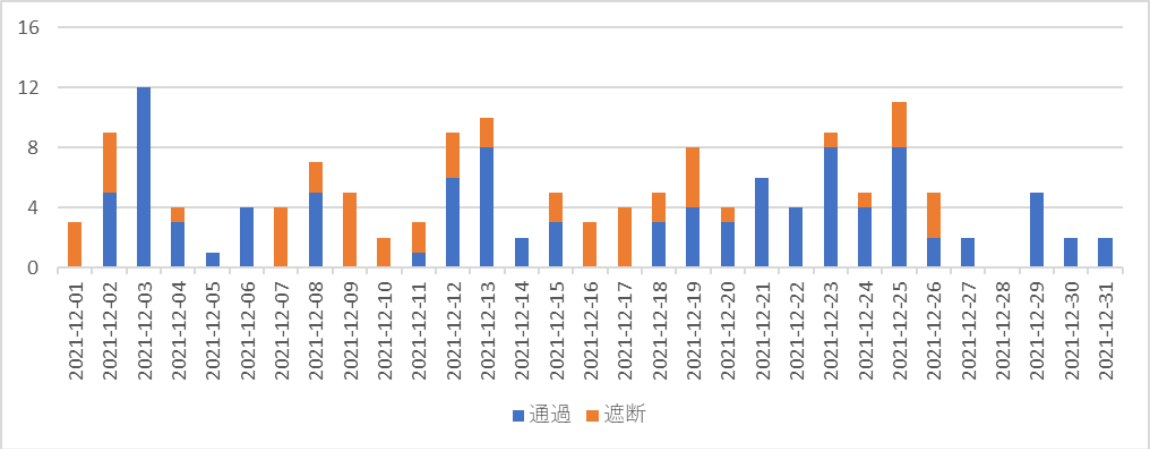




危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	0	2	-
Minor	5	3	60.00%
Warning	0	0	-
合計	5	5	100.00%

2.4.3 日別通信検知数

アンチスパイウェアの日別検知数を報告いたします。



日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	0	3	3
2021-12-02	5	4	9
2021-12-03	12	0	12
2021-12-04	3	1	4
2021-12-05	1	0	1
2021-12-06	4	0	4
2021-12-07	0	4	4
2021-12-08	5	2	7
2021-12-09	0	5	5
2021-12-10	0	2	2
2021-12-11	1	2	3
2021-12-12	6	3	9
2021-12-13	8	2	10
2021-12-14	2	0	2
2021-12-15	3	2	5
2021-12-16	0	3	3
2021-12-17	0	4	4
2021-12-18	3	2	5
2021-12-19	4	4	8

セキュリティ運用監視サービス 月次分析レポート

作成日 :2022-01-10

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-20	3	1	4
2021-12-21	6	0	6
2021-12-22	4	0	4
2021-12-23	8	1	9
2021-12-24	4	1	5
2021-12-25	8	3	11
2021-12-26	2	3	5
2021-12-27	2	0	2
2021-12-28	0	0	0
2021-12-29	5	0	5
2021-12-30	2	0	2
2021-12-31	2	0	2
合計	103	52	155

2.5 アンチウイルス

2.5.1 日別アラート発生数

アンチウイルスの日別アラート発生数を報告いたします。

当月はアラートが発生しておりません。

日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	0	0	0	0
2021-12-05	0	0	0	0	0
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	0	0	0	0
2021-12-10	0	0	0	0	0
2021-12-11	0	0	0	0	0
2021-12-12	0	0	0	0	0
2021-12-13	0	0	0	0	0
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0

日付	Fatal	Critical	Minor	Warning	総計
2021-12-16	0	0	0	0	0
2021-12-17	0	0	0	0	0
2021-12-18	0	0	0	0	0
2021-12-19	0	0	0	0	0
2021-12-20	0	0	0	0	0
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	0	0	0	0
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	0	0	0
2021-12-27	0	0	0	0	0
2021-12-28	0	0	0	0	0
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	0	0	0	0

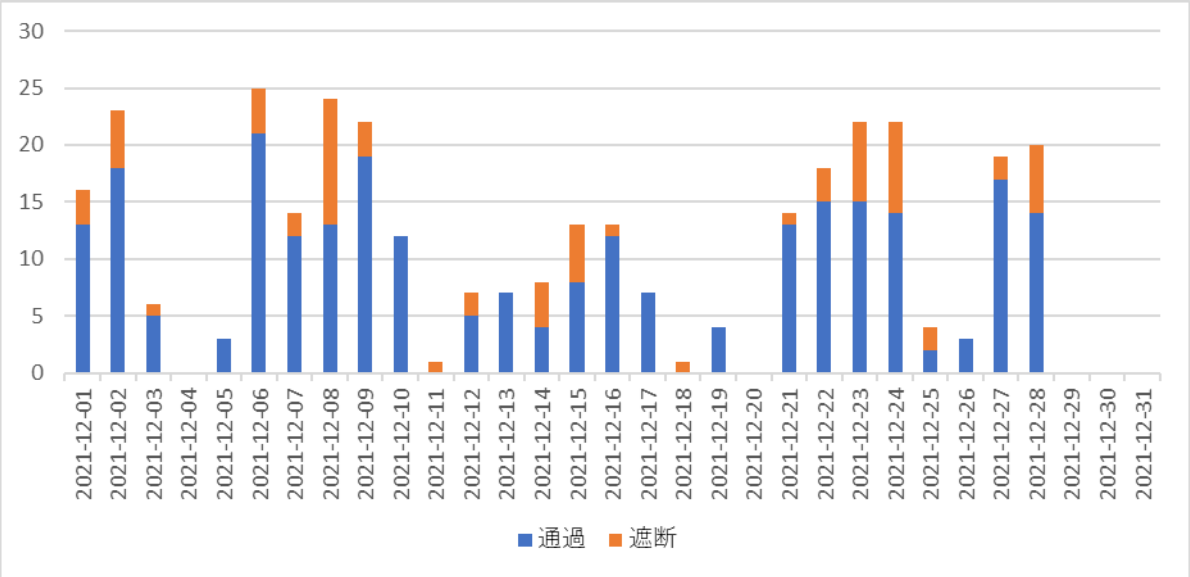
2.5.2 レベル別アラート件数

アンチウイルスのアラート検知数を報告いたします。

危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	0	0	-
Minor	0	0	-
Warning	0	0	-
合計	0	0	-

2.5.3 日別通信検知数

アンチウイルスの日別検知数を報告いたします。



日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	13	3	16
2021-12-02	18	5	23
2021-12-03	5	1	6
2021-12-04	0	0	0
2021-12-05	3	0	3
2021-12-06	21	4	25
2021-12-07	12	2	14
2021-12-08	13	11	24
2021-12-09	19	3	22
2021-12-10	12	0	12
2021-12-11	0	1	1
2021-12-12	5	2	7
2021-12-13	7	0	7
2021-12-14	4	4	8
2021-12-15	8	5	13
2021-12-16	12	1	13

セキュリティ運用監視サービス 月次分析レポート

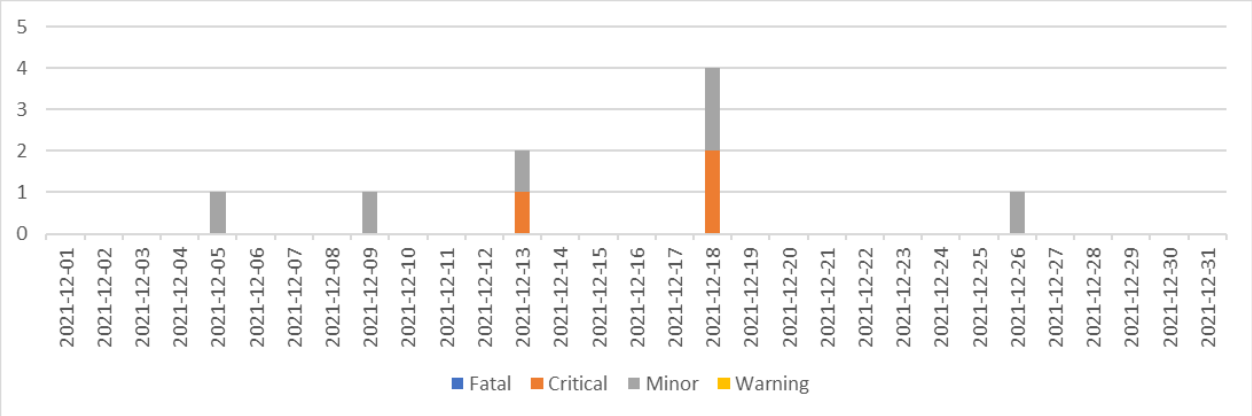
作成日 :2022-01-10

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-17	7	0	7
2021-12-18	0	1	1
2021-12-19	4	0	4
2021-12-20	0	0	0
2021-12-21	13	1	14
2021-12-22	15	3	18
2021-12-23	15	7	22
2021-12-24	14	8	22
2021-12-25	2	2	4
2021-12-26	3	0	3
2021-12-27	17	2	19
2021-12-28	14	6	20
2021-12-29	0	0	0
2021-12-30	0	0	0
2021-12-31	0	0	0
合計	256	72	328

2.6 WildFire

2.6.1 日別アラート発生数

WildFire の日別アラート発生数を報告いたします。

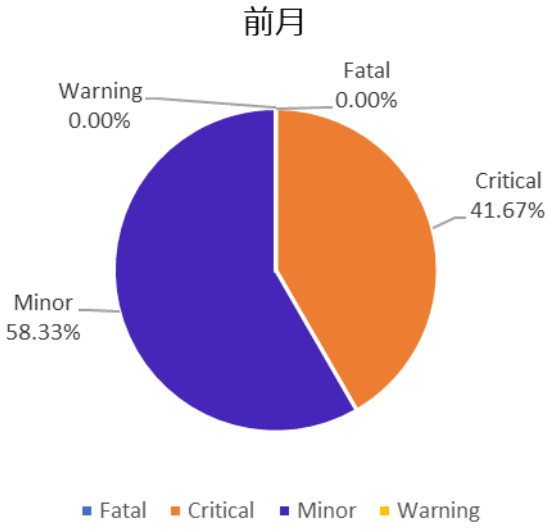


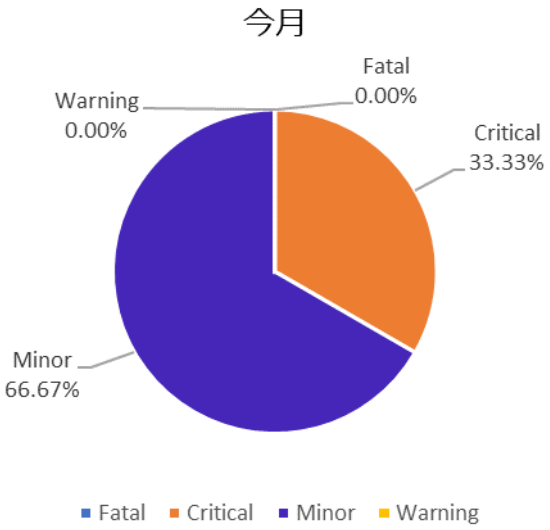
日付	Fatal	Critical	Minor	Warning	総計
2021-12-01	0	0	0	0	0
2021-12-02	0	0	0	0	0
2021-12-03	0	0	0	0	0
2021-12-04	0	0	0	0	0
2021-12-05	0	0	1	0	1
2021-12-06	0	0	0	0	0
2021-12-07	0	0	0	0	0
2021-12-08	0	0	0	0	0
2021-12-09	0	0	1	0	1
2021-12-10	0	0	0	0	0
2021-12-11	0	0	0	0	0
2021-12-12	0	0	0	0	0
2021-12-13	0	1	1	0	2
2021-12-14	0	0	0	0	0
2021-12-15	0	0	0	0	0
2021-12-16	0	0	0	0	0
2021-12-17	0	0	0	0	0
2021-12-18	0	2	2	0	4
2021-12-19	0	0	0	0	0

日付	Fatal	Critical	Minor	Warning	総計
2021-12-20	0	0	0	0	0
2021-12-21	0	0	0	0	0
2021-12-22	0	0	0	0	0
2021-12-23	0	0	0	0	0
2021-12-24	0	0	0	0	0
2021-12-25	0	0	0	0	0
2021-12-26	0	0	1	0	1
2021-12-27	0	0	0	0	0
2021-12-28	0	0	0	0	0
2021-12-29	0	0	0	0	0
2021-12-30	0	0	0	0	0
2021-12-31	0	0	0	0	0
合計	0	3	6	0	9

2.6.2 レベル別アラート件数

WildFire のアラート検知数を報告いたします。

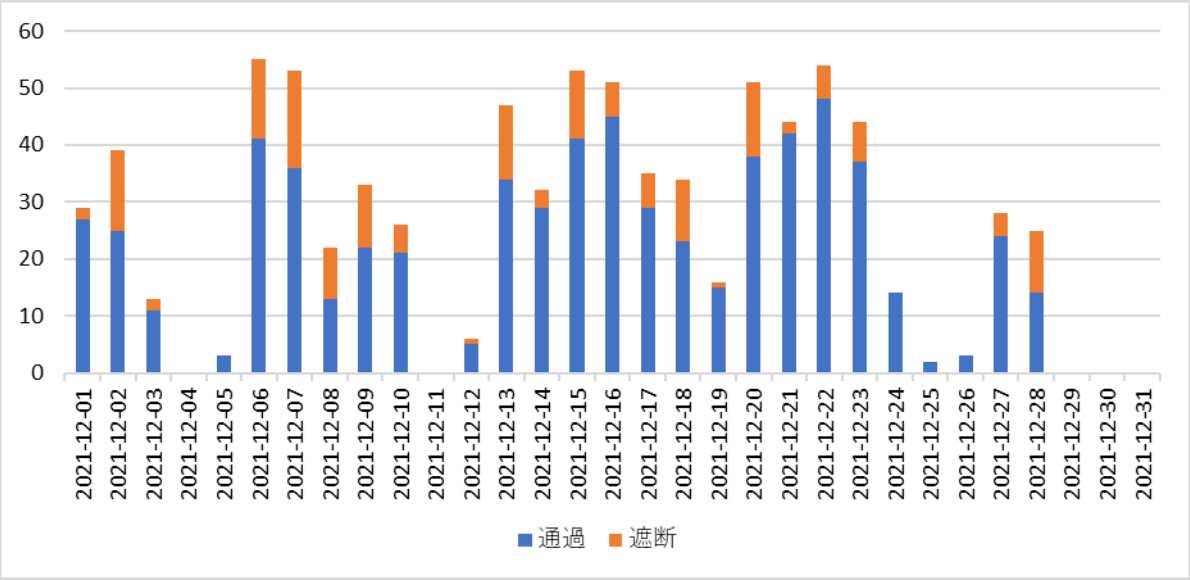




危険度	前月度	今月度	前月比
Fatal	0	0	-
Critical	5	3	60.00%
Minor	7	6	85.71%
Warning	0	0	-
合計	12	9	75.00%

2.6.3 日別通信検知数

WildFire の日別検知数を報告いたします。



日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-01	27	2	29
2021-12-02	25	14	39
2021-12-03	11	2	13
2021-12-04	0	0	0
2021-12-05	3	0	3
2021-12-06	41	14	55
2021-12-07	36	17	53
2021-12-08	13	9	22
2021-12-09	22	11	33
2021-12-10	21	5	26
2021-12-11	0	0	0
2021-12-12	5	1	6
2021-12-13	34	13	47
2021-12-14	29	3	32
2021-12-15	41	12	53
2021-12-16	45	6	51

セキュリティ運用監視サービス 月次分析レポート

作成日 :2022-01-10

日付	通過 (Allow)	遮断 (Deny)	合計
2021-12-17	29	6	35
2021-12-18	23	11	34
2021-12-19	15	1	16
2021-12-20	38	13	51
2021-12-21	42	2	44
2021-12-22	48	6	54
2021-12-23	37	7	44
2021-12-24	14	0	14
2021-12-25	2	0	2
2021-12-26	3	0	3
2021-12-27	24	4	28
2021-12-28	14	11	25
2021-12-29	0	0	0
2021-12-30	0	0	0
2021-12-31	0	0	0
合計	642	170	812

2.7 イベント トップ 10

2.7.1 イベント トップ 10 統計

脆弱性防御・アンチスパイウェア・アンチウイルス・WildFire のイベント トップ 10 を報告いたします。
※Severity は監視機器から送出されるログに準じております。
※Severity の Low 以下は省いております。

No.	イベント名	対象機能	Severity	件数
1	Email Link(52143)	WildFire	high	3
2	generic:crt.sectigo.com(435686358)	アンチスパイウェア	Medium	2
3	Suspicious DNS Query (generic:omnatuor.com)(421897263)	アンチスパイウェア	Medium	2
4	Apache Tomcat Remote Code Execution Via JSP Upload Vulnerability(38761)	脆弱性防御	Medium	1
5	Gh0st.Gen Command and Control Traffic(13264)	アンチスパイウェア	Medium	1
6	DCS-2530L Unauthenticated Information Disclosure Vulnerability(90255)	脆弱性防御	Medium	1

2.7.2 イベント トップ 10 詳細分析

脆弱性防御・アンチスパイウェア・アンチウイルス・WildFire のイベント トップ 10 の詳細分析を報告いたします。

No.	イベント名	対象機能	Severity	件数
1	Email Link(52143)	WildFire	high	3

■ イベント説明

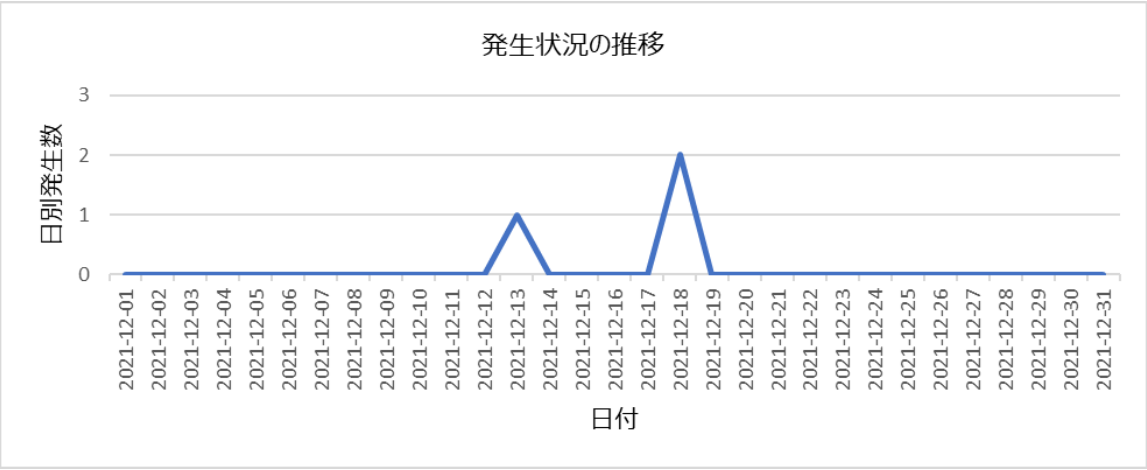
悪性情報があるフィッシングサイトへのリンクを含むメール通信を検知しています。これはマシンの侵害を示している可能性があります。

■ イベント分析

内部から外部への通信にて検知しております。宛先は国外の IP アドレスで、検出されたリンクはフィッシングサイトと情報がありました。該当ページは確認できず詳細情報は不明です。悪性情報が確認されており、通信は全て PaloAlto を通過しているため、クライアント端末のウイルスチェックやサイトへのアクセス有無を確認頂くことを推奨いたします。

■ 送信元 IP アドレスの状況（トップ 5）

宛先 IP アドレス	国名	機関名	件数
192.0.2.18	-	-	2
192.0.2.38	-	-	1



No.	イベント名	対象機能	Severity	件数
2	generic:crt.sectigo.com(435686358)	アンチスパイウェア	Medium	2

■ イベント説明

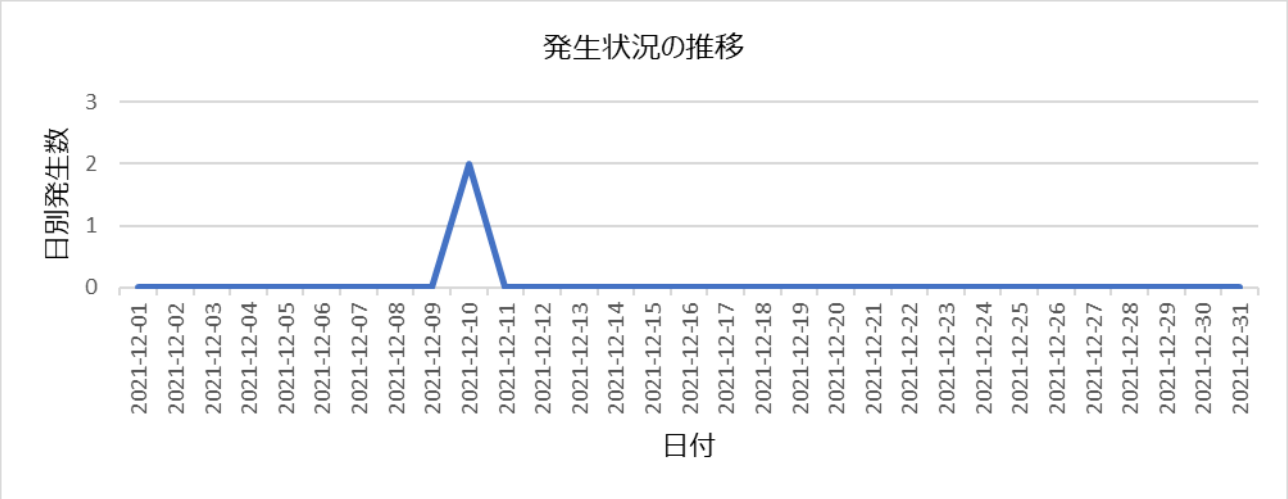
C2 トラフィックに関連付けられている可能性のあるドメインへの DNS 解決を検知しています。これはマシンの侵害を示している可能性があります。

■ イベント分析

内部から外部への通信にて検知しております。宛先は国内の IP アドレスで、検出されたドメイン名は「crt[.]sectigo[.]com」になります。ドメイン名「crt[.]sectigo[.]com」は WEB 会議システム「V-CUBE」のサービスでサーバ証明書更新時にアクセスする URL と考えられます。悪性情報が確認されましたが、通信は全て PaloAlto にて遮断されているため、影響はございません。

■ 送信元 IP アドレスの状況（トップ 5）

送信元 IP アドレス	国名	機関名	件数
192.0.2.185	-	-	2



No.	イベント名	対象機能	Severity	件数
3	Suspicious DNS Query (generic:omnatuor.com)(421897263)	アンチスパイウェア	Medium	2

■ イベント説明

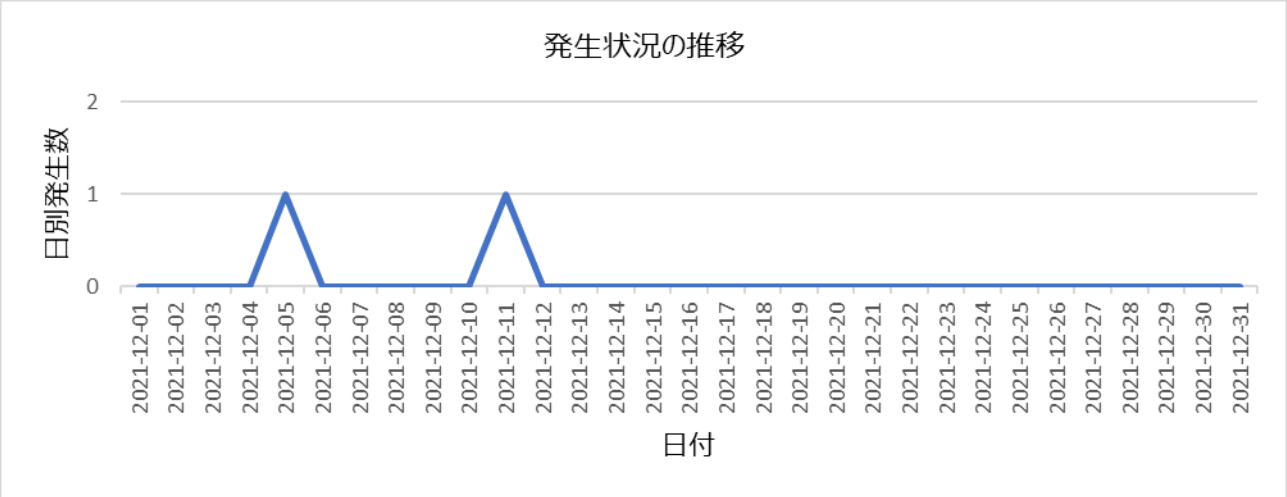
C2 トラフィックに関連付けられている可能性のあるドメインへの DNS 解決を検知しています。これはマシンの侵害を示している可能性があります。

■ イベント分析

内部から外部への通信にて検知しております。宛先は国内の IP アドレスで、検出されたドメイン名は「omnatuor[.]com」になります。ドメイン名「omnatuor[.]com」はマルウェアサイトと情報がありました。該当ページは確認できず詳細情報は不明です。悪性情報が確認されており、通信は全て PaloAlto にて通過しているため、クライアント端末のウイルスチェックやサイトへのアクセス有無を確認頂くことを推奨いたします。

■ 送信元 IP アドレスの状況（トップ 5）

送信元 IP アドレス	国名	機関名	件数
192.0.2.33	-	-	2



No.	イベント名	対象機能	Severity	件数
4	Apache Tomcat Remote Code Execution Via JSP Upload Vulnerability(38761)	脆弱性防御	Medium	1

■ イベント説明

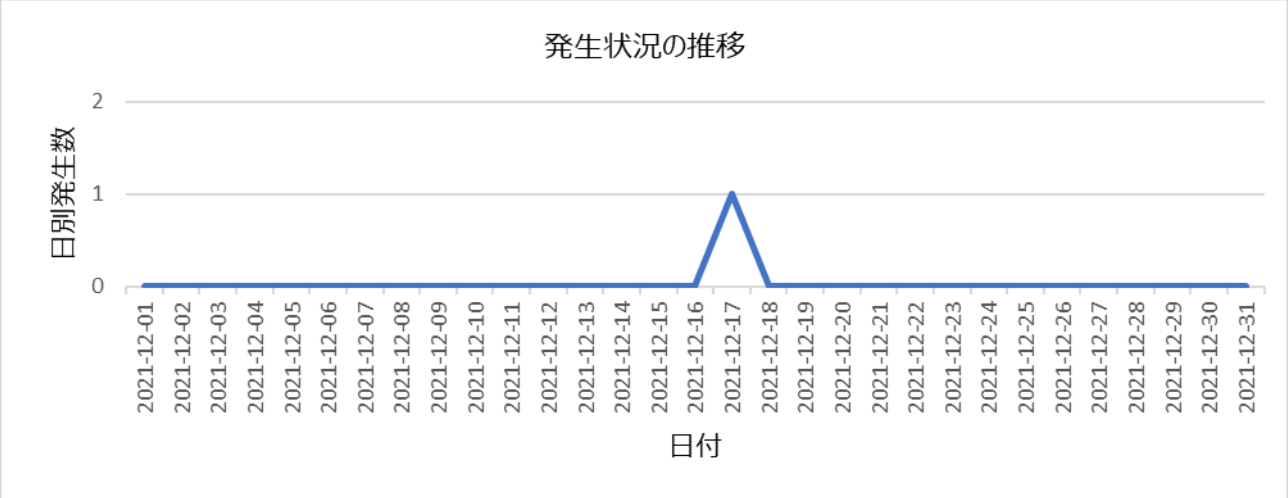
Apache Tomcat には、特定の細工された HTTP リクエストを解析しているときに、リモートでコードが実行される脆弱性が存在します。これはマシンの侵害を示している可能性があります。

■ イベント分析

外部から内部への通信にて検知しております。送信元は国内の IP アドレスで、通信は PaloAlto を通過しております。前後で不審な通信等は確認されませんでしたが、念のため対象機器にて Apache Tomcat を使用していないか、また最新のバージョンに更新されているかをご確認頂くことを推奨いたします。

■ 宛先 IP アドレスの状況（トップ 5）

宛先 IP アドレス	国名	機関名	件数
192.0.2.109	-	-	1



No.	イベント名	対象機能	Severity	件数
5	Gh0st.Gen Command and Control Traffic(13264)	アンチスパイウェア	Medium	1

■ イベント説明

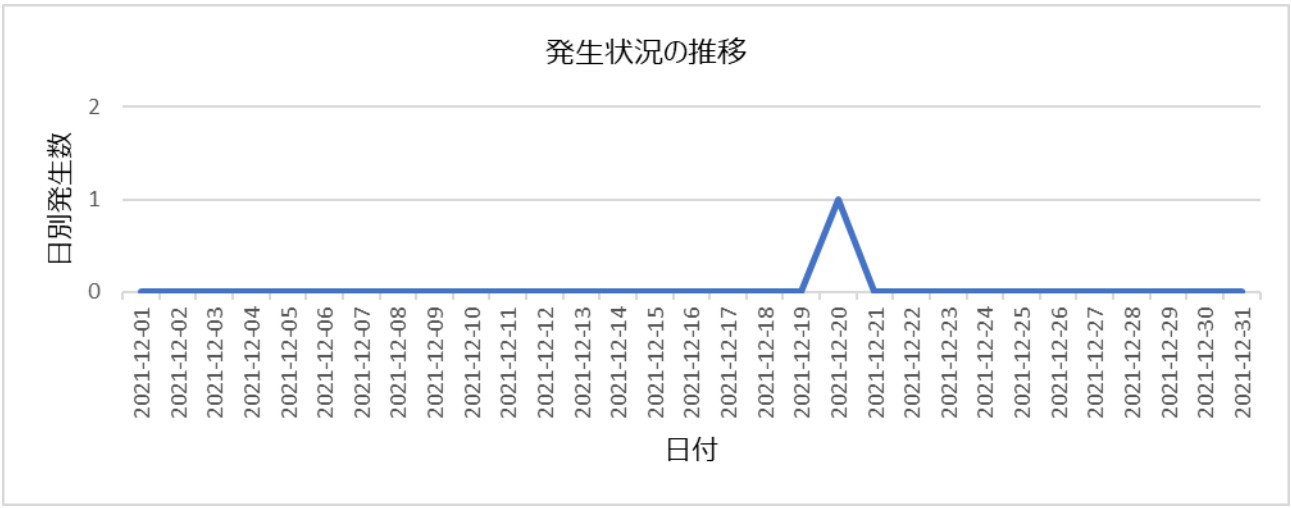
C2 サーバとの通信を検知しています。これはマシンの侵害を示している可能性があります。

■ イベント分析

外部から内部への通信にて検知しております。通信は PaloAlto により遮断されており、前後で不審な通信等は確認されていないため問題はありません。

■ 宛先 IP アドレスの状況（トップ 5）

宛先 IP アドレス	国名	機関名	件数
192.0.2.201	-	-	1



No.	イベント名	対象機能	Severity	件数
6	DCS-2530L Unauthenticated Information Disclosure Vulnerability(90255)	脆弱性防御	Medium	1

■ イベント説明

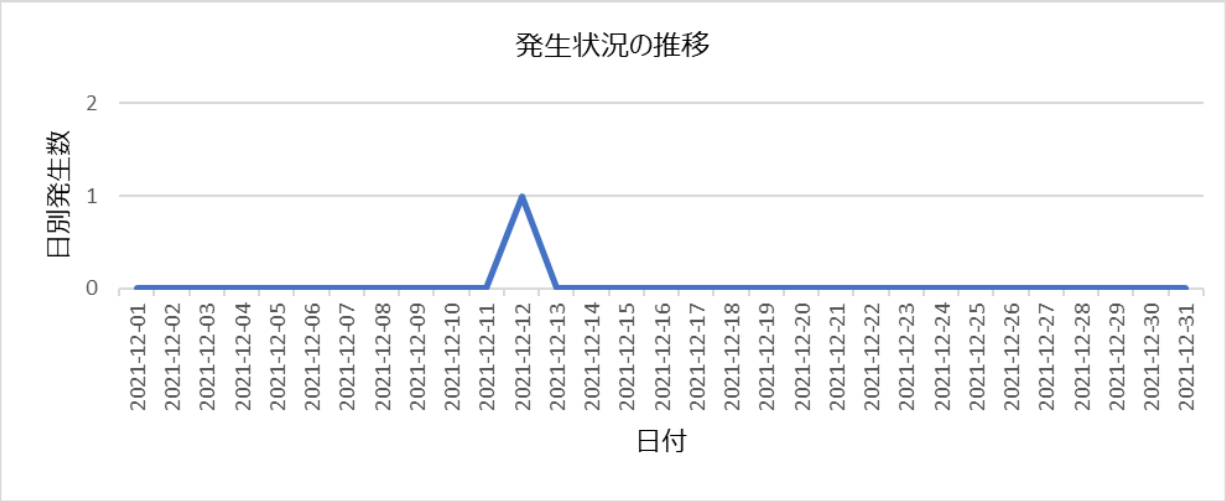
D-Link 製の IP カメラ「DCS-2530L」には、認証されていない情報開示の脆弱性が存在します。これはマシンの侵害を示している可能性があります。

■ イベント分析

外部から内部への通信にて検知しております。通信は PaloAlto により遮断されており、前後で不審な通信等は確認されていないため問題はありません。

■ 宛先 IP アドレスの状況（トップ 5）

宛先 IP アドレス	国名	機関名	件数
192.0.2.104	-	-	1



3. 問合せ履歴

対象期間内の問合せの履歴です。

問合せ番号	問合せ日時	問合せ内容	回答内容	ステータス
CN2112001	2021-12-06 09:49	12 月 4 日アラートについて下記の通り問合せ。 ・サイトの悪性情報	下記の通り回答。 ・DNS ポイズニング等の悪性情報が報告されているサイト。	対応済み
CN2112002	2021-12-9 17:11	12 月 9 日アラートについて下記の通り問合せ。 ・サイトの情報 ・リスク想定	下記の通り回答。 ・CAPTCHA 認証の偽装を利用したサイト。 ・ユーザが通知を許可した場合、スパムを送信されるリスク有り。	対応済み
CN2112003	2021-12-23 11:47	12 月 23 日アラートについて下記の通り問合せ。 ・サイトの情報 ・リスク想定	下記の通り回答。 ・悪意のあるコンテンツ、実行可能ファイル、スクリプト、ウイルス、トロイの木馬、およびコードを含むサイト。 ・マルウェアに感染するリスク有り。	対応済み

4. 作業実施内訳

対象期間内の作業実施内訳です。

作業日付	作業内容	ステータス
2021-12-10	監視機器に特定のサイト(2 件)への通信を遮断する設定を追加	対応済み
2021-12-24	監視機器に特定のサイト(1 件)への通信を遮断する設定を追加	対応済み

5. アラート通知履歴

対象期間内のアラート通知の履歴です。

送信日時	報告書番号	対象機能	検知イベント	件数
2021-12-4	-	ファイアウォールポリシー	Access from Malicious IP High	1
2021-12-4	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-4	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-5	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-5	TR2112-12345-00001	アンチスパイウェア	Suspicious DNS Query (generic:omnatuor.com)(421897263)	1
2021-12-9	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-9	-	URL フィルタリング	URL-Paloalto-Malicious Category	1

送信日時	報告書番号	対象機能	検知イベント	件数
2021-12-10	TR2112-12345-00002	アンチスパイウェア	generic:crt.sectigo.com(435686358)	1
2021-12-10	TR2112-12345-00003	アンチスパイウェア	generic:crt.sectigo.com(435686358)	1
2021-12-11	TR2112-12345-00004	アンチスパイウェア	Suspicious DNS Query (generic:omnatuor.com)(421897263)	1
2021-12-13	TR2112-12345-00005	WildFire	Email Link(52143)	1
2021-12-13	TR2112-12345-00006	脆弱性防御	DCS-2530L Unauthenticated Information Disclosure Vulnerability(90255)	1
2021-12-17	TR2112-12345-00007	脆弱性防御	Apache Tomcat Remote Code Execution Via JSP Upload Vulnerability(38761)	1
2021-12-18	TR2112-12345-00008	WildFire	Email Link(52143)	1
2021-12-18	TR2112-12345-00009	WildFire	Email Link(52143)	1
2021-12-20	TR2112-12345-00010	アンチスパイウェア	Gh0st.Gen Command and Control Traffic(13264)	1
2021-12-23	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-23	-	URL フィルタリング	URL-Paloalto-Malicious Category	1
2021-12-28	-	URL フィルタリング	URL-Paloalto-Malicious Category	2