Confidential

文書番号 VSJ-SST-XXXXXXXX-XX-XX

株式会社 XXX 御中

シマンテッククラウド型 WAF 月次レポート (SAMPLE)

20XX 年 XX 月 XX 日

販売元

合同会社シマンテック・ウェブサイトセキュリティ

サービス提供元

株式会社 セキュアスカイ・テクノロジー

目次

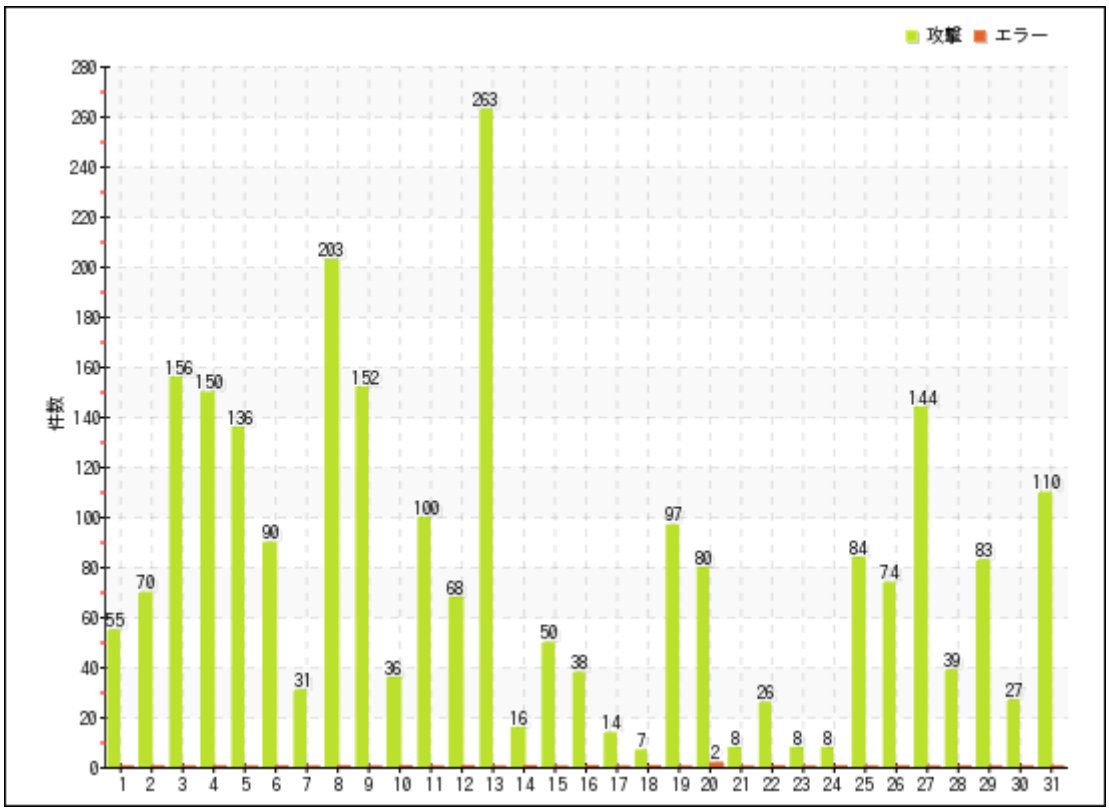
1. はじめに
1.1. 本レポートの目的

本レポートは、ご利用頂いておりますシマンテッククラウド型 WAF「Scutum」(以下、Scutum)の 20XX 年 X 月度の稼働状況をご報告するものです。

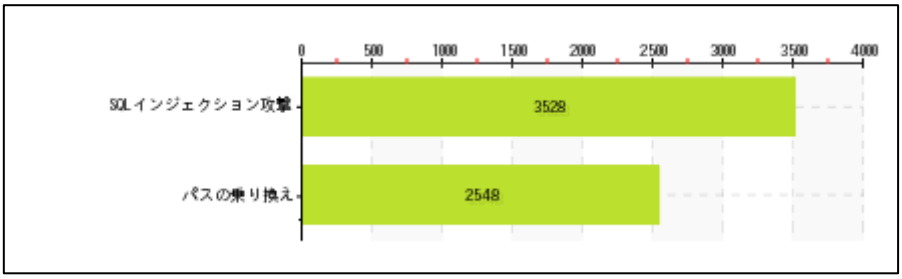
2. エグゼクティブサマリー

2.1. 20XX 年 X 月におけるお客様サイトにて検知された攻撃

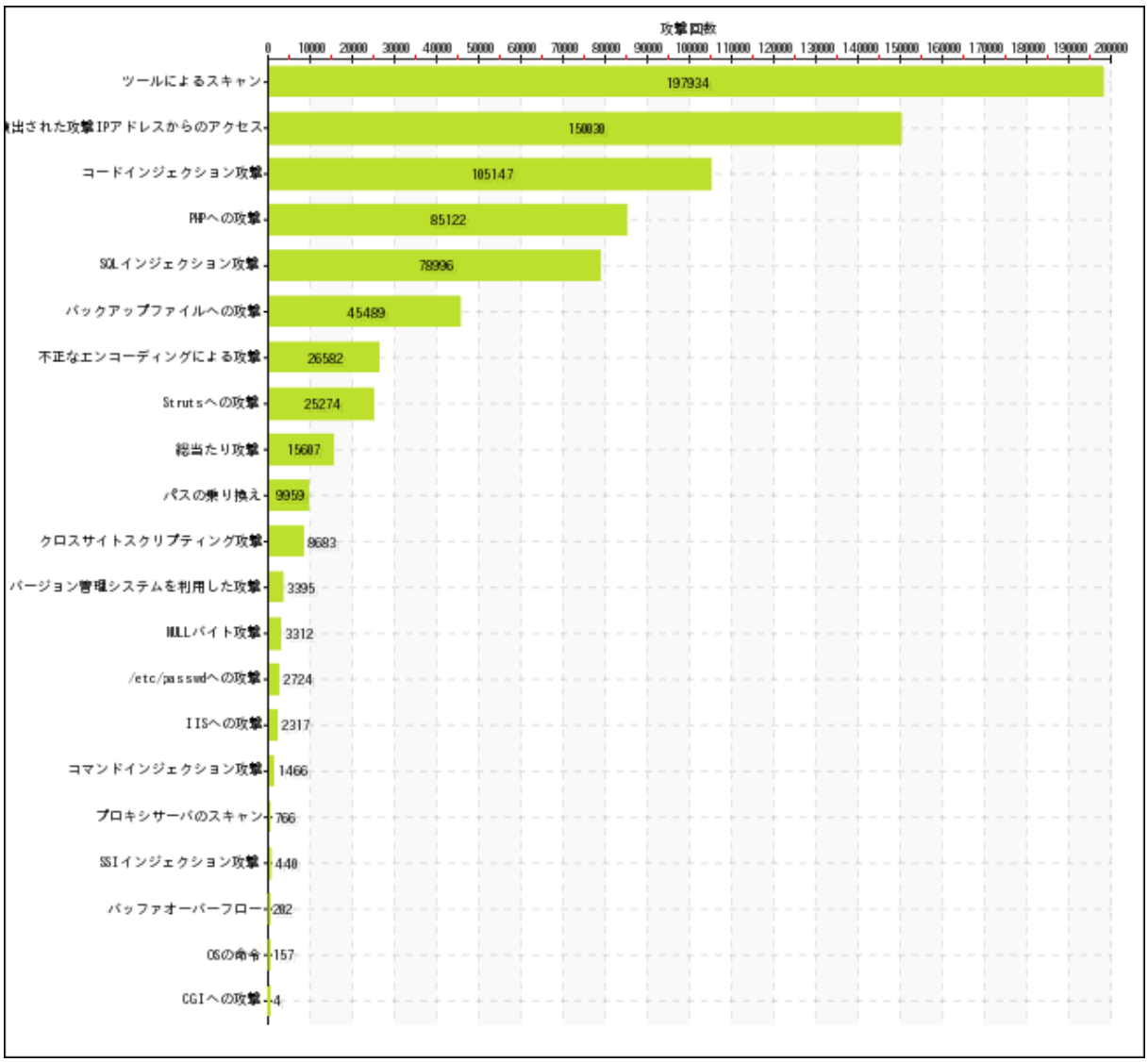
2.1.1. 20XX 年 X 月 アラート件数



2.1.2. 20XX 年 X 月 アラート種別（エラーは除く）



2.2. 20XX 年 X 月に Scutum 全体で検知された攻撃



総攻撃数：XXXXXXXXXX 件（エラーは除く）
対象サイト：約 XXXX サイト

2.3. 所見

X 月 Scutum 全体で確認された攻撃は先月に比べ減少しておりますが、件数としては多い状況が続いております。本サイトに対しても多数の攻撃が確認され、検知された攻撃は、Scutum が導入されていなかった場合、今後の攻撃に発展する恐れのあるものでした。
また、本月も影響度の高い脆弱性が公表されました。 Apache Struts 2 の脆弱性(CVE- XXXX- XXXX) (S2-XXX)で IPA や JPCERT からも注意喚起がされております。

JPCERT の注意喚起：https://www.jpcert.or.jp/example.html
IPA の注意喚起：https://www.ipa.go.jp/example.html

本脆弱性は、遠隔の攻撃者が、細工した HTTP リクエストを送信することで、任意のコードが実行できる可能性がございます。 攻撃の難易度も低く、悪用する攻撃コードも確認されており、実際に情報漏えい等の影響が出たサイトが多数存在しました。Scutum では、X 月 XX 日 に防御機能を追加し影響を受けない状態となっております。

もし Scutum 経由ではない Web サイトへの通信（IP アドレスで Web サイトに接続できるなど）ができる状態の場合、Scutum を導入していても攻撃の影響を受ける可能性がございます。そのような場合、Scutum の IP アドレスからのみに接続を許可するような形として頂くことを推奨します。

3. レポート結果

3.1. レポート期間

20XX 年 X 月 X 日 ～ 20XX 年 X 月 X 日

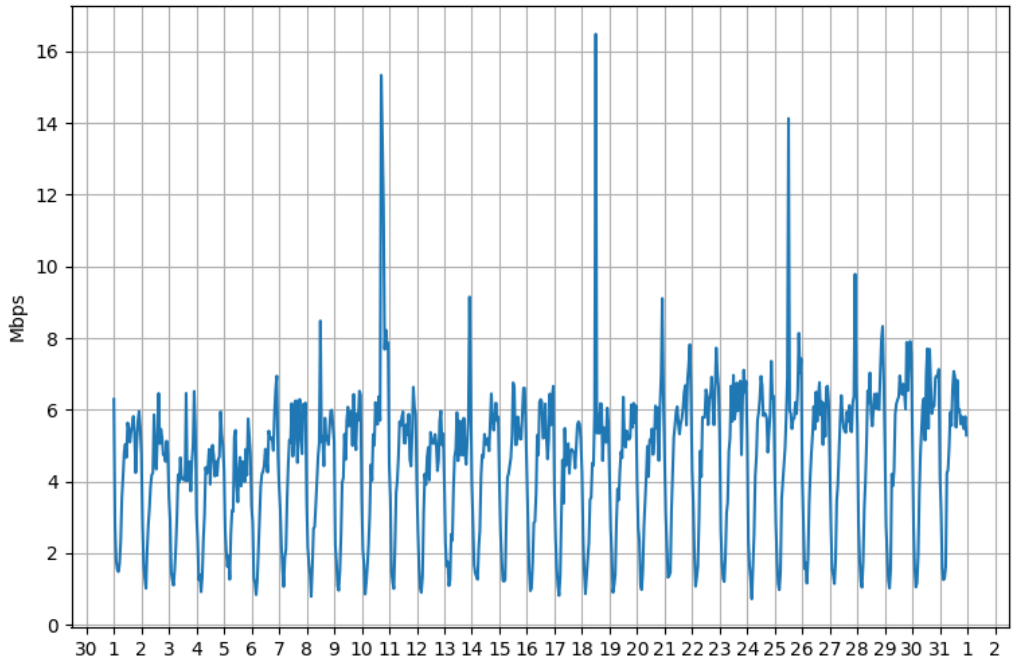
3.2. レポート対象

ドメイン名	www.example.com
IP アドレス	XXX.XXX.XXX.XXX
HTTPS の有無	有り

3.3. トラフィックの状況

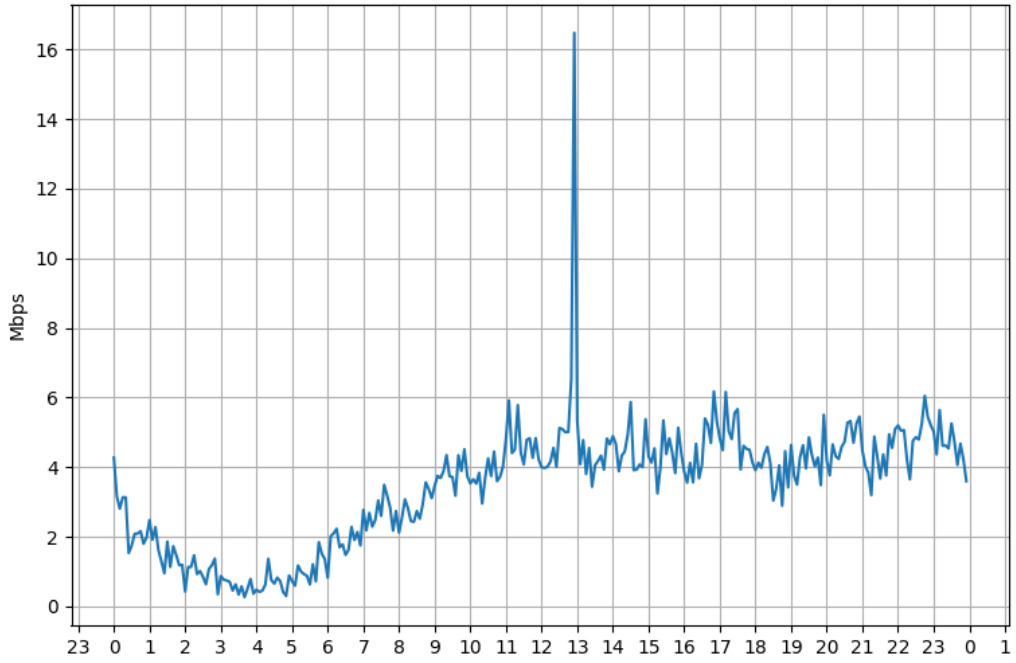
3.3.1. トラフィック状況（月別）

20XX 年 X 月日 ～ XX 日にかけてのトラフィックレポートとなります。



3.3.2. トラフィック状況（日別）

www.example.com において、もっともトラフィックが発生した日のトラフィックレポートとなります。



3.4. 誤検知の有無

誤検知はありませんでした。

3.5. 検知した攻撃およびエラー

検知した攻撃およびエラーの種類、名称、件数は以下の通りです。

タイプ	名称	件数
攻撃	SQL インジェクション攻撃	3528
攻撃	パスの乗り換え	2548
エラー	エラー	2

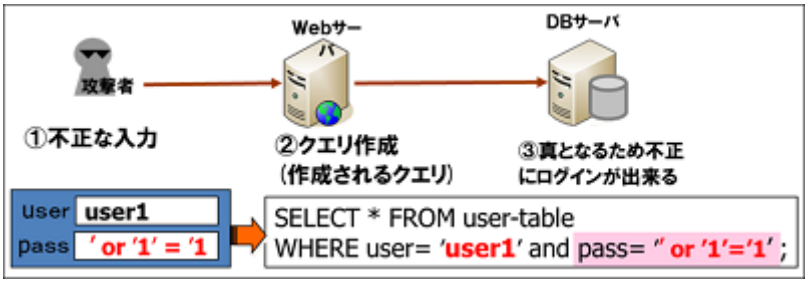
3.6. 検知した攻撃およびエラーの詳細

3.6.1. SQL インジェクション攻撃

検知した HTTP リクエストは次のようになっていました。

```
GET /data/data.asp?id=123456'%20And%20char(124)%2b(Select%20Cast(Count
(1)%20as%20varchar(8000))%2Bchar(124)%20From%20[sysobjects]%20Where%
201=1)>0%20and%20''=' HTTP/1.1
User-Agent: czxt2s
Host: www.example.com
Cookie: SESSIONID=82bjXGVDtBi8N2C
X-Forwarded-For: xxx.xxx.xxx.xxx
X-Forwarded-For2: xxx.xxx.xxx.xxx
X-Client-Port: xxxxx
```

本攻撃は、データベースの SQL クエリのパラメータとなる入力に、不正な文字列を挿入（インジェクション）して、不正な SQL クエリを実行させる攻撃です。下図は不正な文字列により認証を回避する際の SQL インジェクション攻撃の例です。

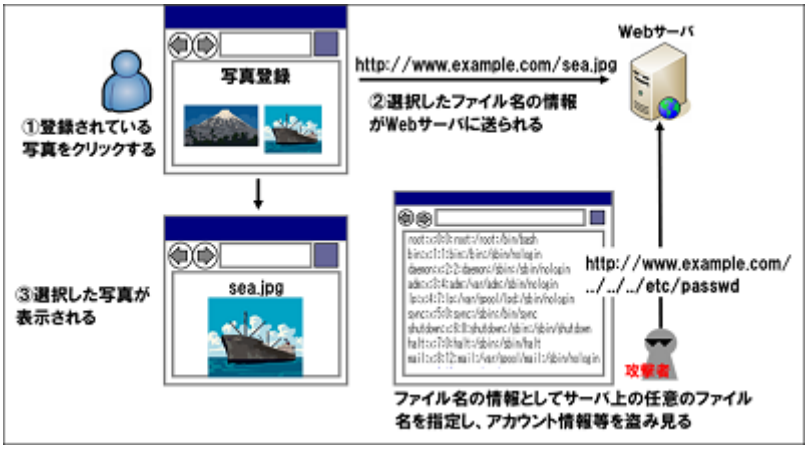


3.6.2. パスの乗り換え

検知した HTTP リクエストは次のようになっていました。

```
GET /index.php?option=../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Accept: text/html
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en-US
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; nl; rv:1.8.1) Gecko/
Cookie: SESSIONID=82bjXGVDtBi8N2C
X-Forwarded-For: xxx.xxx.xxx.xxx
X-Forwarded-For2: xxx.xxx.xxx.xxx
X-Client-Port: xxxxx
```

本攻撃は、攻撃者が任意のファイルを閲覧しようとする攻撃となります。外部からのパラメータでウェブサーバ内のファイル名を指定している場合、ファイル名を指定している機能の実装に問題があると、この攻撃が成功します。
以下は、パスワードファイルの情報を閲覧しようとする攻撃例となります。



3.6.2. エラー

攻撃により、発生したものでは無く、サーバ内部のエラー情報などが表示されたものとなります。
原因としては、サーバが高負荷状態にあったり、入力フォームに対して入力文字数が多いなど想定外の入力に対してプログラムが処理しきれずに不正に終了していることから、これらのエラーが発生しているものと推測されます。このようなエラーから、攻撃者はプログラムに何らかの欠陥があるものと考え、さらにさまざまな値を入力することで攻撃者にとってより有意な結果が得られるように攻撃を仕掛けてくる可能性がありますので、不必要な情報を攻撃者に与えないことが重要です。そのためには詳しいエラー内容が特定できるようなエラーメッセージの表示を抑制し、代わりのエラーページを作成して表示するか、何も表示しないようにすることをご推奨いたします。

4. お問合せ

4.1. お問合せ先

本レポートの内容に関するお問合せは、下記メールアドレスまでご連絡ください。 なお、電話やＦＡＸでのお問合せは受付けておりませんので、ご了承ください。

support@scutum.jp