査読論文

日本におけるサイバー攻撃の事例研究

A Survey of Cyber-Attacks in Japan

高原　尚志
TAKAHARA Hisashi[1]

近年，サイバー攻撃はますます激しさを増し，企業や官公庁のような組織に対してだけではなく，標的型攻撃に代表されるように個人に対する攻撃も増加しつつある．また，新たな展開として，すべてのものがインターネットに接続するIoT時代を迎え，コンピュータだけではなく，情報家電やネットワーク通信機器などのIoT機器への攻撃も増えつつある．更に，電気やガス，交通システムといった社会インフラを担うシステムへの攻撃も行われ，社会生活に大きな影響を及ぼそうとしている．しかし，どのような攻撃がどのように行われ，どのような影響が出たかといった攻撃に関する詳細な知識を得る機会は少なく，これにともなって対策もあまり講じられないことも少なくない．そこで本稿では，実際に行われた直近の事例について紹介し，事例が示されているサイトについても言及する．このようにすることによって，読者のサイバー攻撃に対する認識が高まることを目指す．

Recently, we are suffering very serious cyber-attacks. Targets are not only companies and public agencies, but also individuals. Now, we are seeing IoT(Internet Of Things) in which many kinds of devices access the Internet. So, as a new trend, IoT devices are suffering cyber-attacks. Moreover, attacks to our elements of our infrastructure such as electricity, gas and traffic systems are predicted, which could seriously affect our lives. However we do not know enough information about these attacks. Thus, we cannot deal with them adequately. In this paper we describe the latest incidents and we mention sites in which we can get information about cyber-attacks. Consequently, we hope readers will be better informed about this issue.

キーワード：　サイバー攻撃，事例，情報セキュリティ
Key words：　Cyber Attack, Incident, Information Security

1　はじめに

近年，サイバー攻撃の脅威が，特別な場所だけではなく，一般の職場や実生活の場にも浸透しつつある．直近では日本の社会インフラを担う企業のひとつである日立製作所がサイバー攻撃にさらされた[1]．また一般ユーザのスマートフォンを踏み台とした攻撃が行われたことも記憶に新しい[2]．一方で，サイバー攻撃は身近になっているが，どのような攻撃がなされ，どのような不具合が起こったのかを正確に理解していない人も少なくない．この原因のひとつとして，現在，多くのサイバー攻撃の情報が提供されているが，逆に情報が多過ぎてどの情報をどのように用いれば良いかがよく分からない状態となっていると考えられる．そこで本稿では，各情報を著者独自の視点で整理する．具体的には，各社から提供されているサイバー攻撃の種類についての解説を見やすく再構築したり，最近の事例を攻撃ごとに分類し見出しを挿

入したりするなどして分かり易く整理する．更に，考察として著者独自の分析も加える．これにより，読者のサイバー攻撃に対する理解が深まり，その対策の重要性が浸透することを目指す．

2　サイバー攻撃の種類

サイバー攻撃の種類については，さまざまな分類が行われているが，本稿では，情報セキュリティ会社が行っている機能による分類と侵入パターンによる分類の例を示す．

2.1　機能による分類

2.1.1　シマンテック社による分類

情報セキュリティ会社であるシマンテック社[3]では，自社のウイルス対策ソフトのブランド名であるノートンのサイトで，サイバー攻撃に用いられるユーザに迷惑をかける不正なソフトウェア（マルウェア）を次のように分類している[4]．

（以下，サイト[4]を基に，一部簡略化し，再構成したものである）

ウイルス…プログラムの一部を改ざんし増殖する

プログラムの一部を書き換えて，自己増殖するマルウェアである．単体では存在できず，既存のプログラムの一部を改ざんして入り込むことで存在し，自分の分身を作って増えていく様が病気の感染に似ているため，ウイルスという名称になったとされている．

本来はマルウェアのひとつに過ぎないが，ユーザに不利益を与えるプログラムやソフトウェアをひっくるめて，ウイルス，コンピュータウイルスと呼ぶ傾向にある．

ワーム…単独で生存可能，自己増殖する

自己増殖するマルウェアの一種．自身を複製して感染していく点はコンピュータウイルスと同じであるが，ウイルスのように他のプログラムに寄生せず，単独で存在可能である点から，ワーム（虫の意味）と呼ばれる．

ネットワークに接続しただけで感染するものも多数あり，2000年代前半にアウトブレイクした“Love Letter”，”CodeRed”，”Slammer”，“Mydoom”などは全てワームに該当する．

トロイの木馬…偽装して感染を試みる

一見して無害の画像ファイルや文書ファイル，スマートフォンのアプリなどに偽装し，コンピュータ内部へ侵入，外部からの命令でその端末を自在に操るマルウェアをトロイの木馬と呼ぶ．

語源はそのままトロイの木馬の故事．ギリシア神話のトロイア戦争において，敵兵が隠れた巨大な木馬を城内に運んだトロイアが，それをきっかけに滅亡したことから，内部に隠れている敵をトロイの木馬と表現する．

自己増殖機能はないため，この点でコンピュータウイルスと区別される．

スパイウェア…密かに活動する

情報収集を主な目的とし，ウイルスやワームのような自己増殖機能は持たない．

ユーザが気づかないうちにパソコンにインストールしているパターンが多く，表だって活動しないため，被害に遭っていることに気づきにくい特徴がある．

シマンテック社ではスパイウェアをマルウェアと定義していないが，ユーザに不利益を与えることにかわりはなく注意が必要である．

2.1.2　カスペルスキー社による分類

また，情報セキュリティ会社であるカスペルスキー社[5]では，マルウェアを，次のように分類している[6]．（以下，サイト[6]を基に，一部簡略化し，再構成したものである．）

ウイルス：

※サイト[4]と重複しているため説明部分を省略

ワーム：

※サイト[4]と重複しているため説明部分を省略

トロイの木馬：

※サイト[4]と重複しているため説明部分を省

略

ランサムウェア：

ランサムウェアとは，被害者からお金を巻き上げることを目的としたマルウェアである．ポップアップ広告や，フィッシングリンク，悪意あるWebサイトなどの形で人々の目の前に現れる．活動を始めると，感染したシステムにある脆弱性を引き金に，キーボードや画面，ひどいときはコンピュータ全体をロックしてしまう．さらに，「海賊版を使っている」「違法コンテンツを見た」と言いがかりをつける警告メッセージを出してユーザを慌てさせ，警告を消すにはお金を払うようにと要求してくる．

ルートキット：

ルートキットは，感染先での存在や活動がユーザやセキュリティソフトウェアに気付かれないように，特別に設計されたマルウェアである．ルートキットはOSの深い部分に入り込み，OSよりも前に起動することさえある（このタイプは「ブートキット」と呼ばれる）．高度なアンチウイルスソフトウェアであれば，ルートキットを検知して駆除できる．

バックドア（RAT）：

バックドア（またの名をRemote Administration Tool）とは，ユーザに気付かれずにコンピューターシステムへアクセスできるようにするアプリケーションである．システムのメンテナンスなどの目的でシステム管理者が利用することもあるが，サイバー犯罪者によって悪用されるケースもよく見られる．RATの機能によっては，他のソフトウェアのインストールや起動，キー入力情報の送信，ファイルのダウンロードや削除，マイクやカメラの有効化，コンピュータの動作の記録と攻撃者へのログの送信などが可能である．

ダウンローダー：

これはサイズの小さなコードで，実行可能ファイルや，攻撃者のサーバから被害者のコンピュータに命令を出して好きなタスクを実行させるファイルを，ひそかにダウンロードする．メールの添付ファイルや不正に細工のしてある画像を介してダウンロードされたコードは，命令を出すサーバと通信し，さらに別のマルウェアを被害者のシステムへダウンロードする．

更に，カスペルスキー社では，次のような分類も示している[7]．

（以下，サイト[7]を基に，一部簡略化し，再構成したものである）

ウイルス：

※サイト[4]と重複しているため説明部分を省略

ワーム：

※サイト[4]と重複しているため説明部分を省略

トロイの木馬：

※サイト[4]と重複しているため説明部分を省略

スパイウェア：

※サイト[4]と重複しているため説明部分を省略

アドウェア：

広告の表示を目的に，ユーザに気付かれずにソフトウェアに組み込んだプログラムコードである．通常アドウェアは無料配布のソフトウェアに組み込まれ，インタフェースを利用して広告を表示する．アドウェアはしばしばユーザの個人情報を収集し，それらをアドウェアの配布者に送信する目的にも使用される．

リスクウェア：

このタイプのソフトウェアはウイルスではないが，それ自体に潜在的な脅威を含んでいる．状況によっては，そのようなリスクウェアがPC上に存在することによってデータが危険にさらされる場合がある．このようなソフトウェアには，リモート管理ユーティリティやダイヤルアップ接続を使用するプログラム，また使用時間で課金されるインターネットサイトに接続するものなどがある．

ジョークウェア：

このタイプのソフトウェアは，実際にはコンピュータに危害を加えないが，被害が発生した，またはこれから発生するなどのメッセージ

を表示する．たとえば「ハードディスクを初期化しています」（実際には初期化は行われない），「ファイル内にウイルスを検知しました」（実際には感染の事実はない）など，実際には発生していない危険についての警告を発する．

ルートキット：

※サイト[6]と重複しているため説明部分を省略

スパム：

匿名で送信される大量の迷惑メールである．ある人物の支持を訴える政治的な宣伝活動を目的としたもの，多額のキャッシングを勧めるもの，ねずみ講への勧誘を行うもの，パスワードやクレジットカード番号を盗むもの，友達にメールを回すよう勧めるもの（チェーンメール）などがある．スパムのためにメールサーバの負荷が高まり，ユーザが必要な情報を見落とすリスクも高まる．

その他：

その他，マルウェアを作成するもの，リモートサーバに DoS 攻撃を仕掛けるもの，他のコンピュータに侵入するものなどがある．ハックツール，ウイルス自動生成ツールなどもその仲間である．

2.2　侵入パターンによる分類（シマンテック社による分類）

更にサイト[4]では，侵入パターンについても次のように分類している．

（以下，サイト[4]を基に，一部簡略化し，再構成したものである）

メールなどの通信時

古くからあるパターンで，メールに添付されているファイルを開くことで，ウイルスなどに感染してしまう．

ネットワーク経由

脆弱性が放置されている（セキュリティ対策を行っていない）パソコンがネットワークに接続するだけで，マルウェアに感染する可能性がある．

また社内などのネットワークにウイルスやワームが入り込むと，あっという間にパソコンからパソコンへと感染することがある．

不正なサイトへのアクセス時

もともと悪意を持って作られたサイトや，他者に改ざんされたサイトにアクセスすることで，マルウェアが自動的にダウンロードされることがある．

脆弱性を介して

本来は権限がなくてアクセスできないはずなのに，ソフトウェアの欠陥によりそれが可能になってしまうことがある．こういった脆弱性を介して，マルウェアが拡散することがある．

対策ファイルを入手し，ソフトウェアをアップデートすることで，こうした脆弱性は解消される．

3　最近の傾向

3.1　IPAによるレポート

サイバー攻撃の最近の傾向として，独立行政法人　情報処理推進機構（IPA）[8]は，情報セキュリティ10大脅威2017の中で，2016年において社会的影響が大きかったセキュリティ上の脅威について，「10大脅威選考会」の投票結果に基づき，「個人」「組織」における脅威を表 1 のように 1 位から10位に順位付けしている[9].

表１「情報セキュリティ10大脅威 2017」

（下表は，サイト[9]の表を基に，著者独自の視点（前年からの上昇（↑），下降（↓），現状維持（→），急上昇（☆）の標記）を加えて再構成したものである）

個人

2016年順位	脅威	2015年順位
1位（→）	インターネットバンキングやクレジットカード情報の不正利用	1 位
2位（→）	ランサムウェアによる被害	2位
3位（→）	スマートフォンやスマートフォンアプリを狙った攻撃	3位
4位（↑）	ウェブサービスへの不正ログイン	5位
5位（↓）	ワンクリック請求等の不当請求	4位
6位（↑）	ウェブサービスからの個人情報の窃取	7位
7位（↓）	ネット上の誹謗・中傷	6位
8位（→）	情報モラル欠如に伴う犯罪の低年齢化	8位
9位（↑）	インターネット上のサービスを悪用した攻撃	10位
☆10位（↑）	IoT機器の不適切な管理	ランク外

（注）表中の矢印は，前年度からの順位の上昇（↑），下降（↓），現状維持（→）を表す．また，☆印は，前年に比べて，急激に順位が上昇したものを表す．

組織

2016年順位	脅威	2015年順位
1位（→）	標的型攻撃による情報流出	1 位
☆2位（↑）	ランサムウェアによる被害	7位
3位（→）	ウェブサービスからの個人情報の窃取	3位
4位（→）	サービス妨害攻撃によるサービスの停止	4位
5位（↓）	内部不正による情報漏えいとそれに伴う業務停止	2位
6位（↓）	ウェブサイトの改ざん	5位
7位（↑）	ウェブサービスへの不正ログイン	9位
☆8位（↑）	IoT機器の脆弱性の顕在化	ランク外
☆9位（↑）	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
10位（↓）	インターネットバンキングやクレジットカード情報の不正利用	8位

（注）表中の矢印は，前年度からの順位の上昇（↑），下降（↓），現状維持（→）を表す．また，☆印は，前年に比べて，急激に順位が上昇したものを表す．

考察（著者の分析）

上記レポートで特に注目すべき点は，2015年はランク外であった「モノのインターネット（IoT=Internet Of Things）[10]」と称される，インターネットに接続された様々な機器への攻撃である（個人10位，組織８位）．

個人においては，情報家電と呼ばれるインターネットへ接続される電化製品などへの攻撃の増加が予測される．例えば，お風呂のスイッチを，出先からON/OFFできたり，温度調節ができたりすることはもはや珍しくない．また，外出中に子どもやペットの様子を見るためなどに部屋の中に監視カメラ（見守りカメラ）が設置されていることも少なくないだろう．これらの機器がサイバー攻撃を受ければ，お風呂が空焚きにされたり，部屋の中が丸見えになったりして，利便性や安全性を得るためのものが，返って危険性を高める道具となってしまう可能性もある．

組織においては，外部からルータなどの設定を変更したり，ログなどの情報を見ることができたりするものが多くなりつつあるが，これらのIoT機器に対するセキュリティの意識は薄く，パスワードなどが初期設定のままになっている場合や容易に推測されやすいパスワードとなっている場合が多く存在する[10]．このような機器がサイバー攻撃を受ければ，ネットワークの混乱によりシステムを利用することができなくなったり，機密情報が漏洩したりといった事態になりかねない．

更に，近年は，空港や原子力施設などの社会インフラへのサイバー攻撃も行われ，社会生活に影響を及ぼす事例も多くなりつつある．

将来に目を向ければ，近年自家用車の自動運転技術が注目されているが，自動運転の車が本格的に導入されれば，それらへのサイバー攻撃は，社会をパニックに陥らせかねない．

上記のことから分かるように，インターネットは，私たちの社会生活に計り知れない利便性を提供する可能性があるが，一方で，利便性が大きくなればなる程，サイバー攻撃がもたらす

社会生活への影響も大きくなることをしっかりと認識しておく必要がある．

また，組織の9位にあるように，近年，サイバー攻撃のビジネス化が進んでおり，報酬を得て指定された組織などにサイバー攻撃を行うビジネスも横行しつつある．このことは，サイバー攻撃が，コンピュータに精通した一部の人間が行うものから，お金を出せば誰でも行うことができるものへと変容しつつあることを意味している．

今後，サイバー攻撃の影響は，私たちの実生活にも及ぶなど，ますます大きくなることが予測される一方で，サイバー攻撃のビジネス化により専門知識がない人も攻撃を行うことができるようになるなど，サイバー攻撃のハードルは，ますます低くなることが予測される．上記レポートは，昨年（2016年）が，その傾向が顕著に表れた初めての年ということを示している．

今後，私たちは，インターネットの利便性だけではなく，利便性と引き換えに上記のような危険性もはらんでいるということを常に認識しつつ，その利便性を享受する必要があると考えられる．

3.2　トレンドマイクロ社によるレポート

その他，情報セキュリティ会社のトレンドマイクロ社[11]からも，2017年セキュリティ脅威予測として次のようなレポートが示されている[12]．

（以下，サイト[12]を基に，一部簡略化し，再構成したものである）

■2017年 セキュリティ脅威予測

2016年はランサムウェアの被害が国内外に拡大し，業種規模問わず様々な組織にインパクトを与え，トレンドマイクロが予測したとおり「ネット恐喝」の年となった．トレンドマイクロでは，最新の脅威動向やIT技術を取り巻く市場動向を基に，2017年のセキュリティ脅威予測をまとめた．

1．ランサムウェアの増加が高止まりとなり，攻撃の手口や標的が多様化
2．DDoS攻撃[2]でIoT デバイスが悪用され，IIoT システムは標的型攻撃に狙われる
3．手口のシンプルさによって，2017年もBEC事例は増加を続ける
4．「ビジネスプロセス詐欺」が勢いを増し，サイバー犯罪者の標的は金融機関以外へ拡大
5．Adobe 製品やApple 製品で見つかる脆弱性の数はマイクロソフト製品の数を上回る
6．定着化するサイバープロパガンダ
7．GDPR 施行と順守に伴い，企業の負担が増加
8．最新セキュリティ技術を回避する攻撃手法の出現

3.3　シマンテック社によるレポート

更に，シマンテック社からも最近のサイバー攻撃の脅威の傾向が2017年インターネットセキュリティ脅威レポートとして提供されている[14]．以下にその一例を示す．

（以下，サイト[14]を基に，一部簡略化し，題名と内容に分けて再構成したものの一部抜粋である）

■革新的かつ高度な組織的攻撃による深刻な被害…世界規模の銀行強盗，選挙の妨害工作，そして国家支援を受けた攻撃が目立った2016 年

内容

2016 年は，被害総額数百万ドル規模の仮想銀行強盗，政府支援グループによる米国大統領選の妨害を狙う表立った試みなど，サイバー犯罪者の野望が新たな段階に入ったことが明らかになった 1 年であった．

新しい高度な革新的手法が用いられ，攻撃対象も大きく変化した．ゼロデイ脆弱性や高度なマルウェアの利用は減ったものの，国家がスパイ活動や直接的な妨害工作に関与するようになっている．

3.4　その他のレポート

情報セキュリティ会社のチェックポイント[15]では，「上半期レポート　サイバー攻撃トレンド2017」[16]の中で，2017年上半期のトレンドとして，ランサムウェア，バンキングマルウェア，モバイル脅威が多く観測されているとしている．

また，カスペルスキー社では，リアルタイムにサイバー攻撃の様子を可視化して攻撃の状況を直感的に把握することができるサイト[17]を公開して，ユーザの注意を喚起している．サイバー攻撃の様子を可視化して直感的に把握することができるサイトとしては，他にも国立研究開発法人　情報通信研究機構[18]からNICTER[19][20][21]が提供されている．

4　事例

4.1　IPAから提供されている事例

IPAの被害事例集[22]によると，2016年前半の被害事例は次の通りである．

（以下，サイト[22]を基に，「閲覧障害」，「情報漏洩」などの被害の種類別に分け，更にその中をDDoS，ランサムウェア，インジェクション攻撃[3]など攻撃の種類別に分けることにより，著者独自の視点で再構成したものである．なお，更に分かり易くするために，各項目の中に「日にち」，「対象」，「内容」，「原因」，「対応」，「被害の範囲」，「その後の状況」などの小見出しも挿入した．）

（※以下の日にちは，報道発表またはメディア掲載日）

4.1.1　閲覧障害

（1）　DDoS攻撃

① DDoS攻撃によりWebサーバに閲覧障害が発生

日にち　2016年1月12日

対　象　企業

内容

当該企業の発表によると，2016年1月12日に，同社のWebサーバに異常な負荷が発生し，同日中に改善見込みがないため，同社はWebサーバを公開停止した．

原因

負荷の原因は不特定な第三者によるサイバー攻撃と考えられている．

対応

その後，セキュリティ強化等の対策を実施し，Webサーバを再開した．

被害の範囲

なお今回の攻撃による個人情報の漏えいや，サイト改ざん，マルウェア感染は確認されていない．

② DDoS攻撃により，官庁Webサーバに閲覧障害が発生

日にち　2016年1月18日

対　象　官公庁

内容

当該機関のWebサーバにおいて，2016年1月18日に閲覧障害が発生した．

対応

内閣サイバーセキュリティセンターより，Anonymousと見られるアカウントから犯行声明が出ているとして，1月18日に同機関に対して連絡が行われた．後の取材に対して同機関はDDoS攻撃を受けたことで断続的に接続障害が発生していると回答している．

その後の状況

1月18日，Twitterに同庁のWebサーバを落としたという内容がOpKillingbayのハッシュタグとともに投稿される．一方，同機関はTwitterへ行われた投稿と実際の攻撃についての因果関係は確認できていないとコメントしている．

③ 空港のWebサーバへのDDoS攻撃により，閲覧障害が発生

日にち　2016年1月24日

対　象　空港（社会インフラ）

内容

2016年1月22日に当該企業の公式Webサーバで閲覧障害が発生した．同公式Webサーバに対して，短時間に外部から大量のアクセスが行わ

れたことにより，1月22日から1月26日まで繰り返し閲覧障害が発生した．

対応

1月22日に閲覧障害を報じる記事を取り上げ，米国人活動家の解放を要求する内容，1月26日に同社のWebサーバを落としたとする攻撃を示唆する内容がそれぞれOpKillingbayのハッシュタグとともに投稿されたことから，同社はサイバー攻撃を受けた可能性があるとみて監視を強化し，警察と情報共有を行った．

④ DDoSとみられる攻撃により，厚生労働省のWebサーバにおいて閲覧などに障害が発生

日にち 2016年1月25日

対　象 官公庁（厚生労働省）

内容

2016年1月25日に当該機関のWebサーバで閲覧障害が発生した．さらに同日には電子メールも送受信ができなくなる事象が発生している．1月26日に電子メールシステム及びWebサーバの障害の復旧を発表したものの，1月26日に再度，Webサーバで閲覧障害が発生した．

対応

最終的に1月27日にWebサーバの閲覧障害の復旧が発表されている．

⑤ DDoSとみられる攻撃により，警察庁のWebサーバにおいて閲覧障害が発生

日にち 2016年1月27日

対　象 官公庁（警察庁）

内容

2016年1月27日に当該機関のWebサーバが閲覧できない障害が発生した．また，同機関のWebサーバ以外にも複数のサイトで障害が発生した．

被害の範囲

Webサーバが閲覧できなくなったことに伴い，利用者からの問い合わせの受け付けも一時不可となった．なお同機関職員が利用する電子メールシステムは別系統のシステムであったため，影響は生じなかった．また同機関からの情報漏えいなどは確認されていない．

原因

障害の原因は，外部から大量のアクセスが集中したためとされている．

その後の状況

1月28日にOpKillingBayのハッシュタグとともに同機関のWebサーバを落としたとする投稿があった．

⑥ ２つの空港を対象とする海外からのDDoS攻撃により，Webサーバの閲覧障害が発生

日にち 2016年1月27日

対　象 空港（社会インフラ）

内容

2016年1月27日に国内２つの空港のWebサーバがインターネットから閲覧できなくなる障害が発生した．

被害の範囲

両空港とも1月27日の時点で，それぞれのWebサーバへのアクセスが一時的に繋がりづらい状況となっていることを公表している．

原因

いずれも「外部からの大量のアクセスを受けたこと」が原因としており，サイバー攻撃を受けた可能性があることを取材に対してコメントしている．

その後の状況

なお，2016年1月27日に「２つの空港を落とした」旨の書き込みがOpKillingbayのハッシュタグとともに投稿されていた．

対応

１つの空港では，サーバの負荷を低減する対策を講じ，警察へ被害相談を行なった．他方の空港は，海外からのアクセスを遮断する措置を講じた．

⑦ DDoSとみられる攻撃により，複数の省庁のWebサーバにおいて閲覧障害が発生

日にち 2016年1月31日

対　象 官公庁（中央省庁）

内容

2016年1月31日夜に複数の機関（中央省庁5件以上）で閲覧障害が発生した．

原因

障害発生の原因は，外部から大量のデータ送信を受けたことによるものと考えられている．

（2） ランサムウェアによる攻撃

⑧ ランサムウェア感染により電子カルテ等のデータが閲覧不可能となり，攻撃者にビットコインを支払ってデータの復号を依頼

日にち 2016年2月5日

対 象 病院（社会インフラ）

内容

2016年2月5日に当該病院の電子カルテを含むデータの多くがランサムウェアと呼ばれるマルウェアによって暗号化され，院内での電子的な情報共有が困難となった．

対応

攻撃者は暗号解除のための鍵と引き換えに身代金を要求してきたことから，同病院では要求額の40ビットコイン（約180万円）を支払うことで2月15日システムを復旧させた．

被害の範囲

攻撃を通じた患者の診療への影響はなく，患者や職員の個人情報に対して不正アクセスが発生した形跡はないとされている．

4.1.2 情報漏洩

（1） 電子メールを利用した攻撃

⑨ マルウェア感染による情報漏えい

日にち 2016年1月3日

対 象 官公庁

内容

標的型攻撃のための電子メールを受信した当該機関の職員用PC合計31台がマルウェアに感染し，当該PCからアクセス可能なファイル共有サーバに保存されていた国民の個人情報125万件が漏えいした．

対応及び状況

2015年5月8日に内閣サイバーセキュリティセンター（NISC）が異常なデータの流れに気付き，関係省庁に連絡したことによって発覚し，調査を依頼された警察が国内の無関係な企業が有するサーバ上で当該機関の情報を発見したことにより，漏えいの事実が明らかとなった．

原因

標的型攻撃はマルウェアの添付とマルウェアをダウンロードするURLの記載の2種類の方法で行われ，感染したPCにはいずれもウイルス対策ソフトウェアが導入されていたが，マルウェアとしての検出はいずれもなされなかったとしている．

被害の範囲

漏えいした情報には，氏名・生年月日・住所及び社会保障用の番号が含まれる．漏えい元となったファイル共有サーバには個人情報の格納は原則禁止とされていたが，個人への連絡を目的とした文書作成のため，基幹システムに保存されていた個人情報から抽出した情報が格納されていた．

（2） インジェクション攻撃

⑩ テレビ局のWebサーバへのコマンドインジェクション攻撃により，視聴者からの投稿43万件に含まれる個人情報が漏えいした恐れ

日にち 2016年4月21日

対 象 テレビ局（社会インフラ）

内容

当該企業は同社のWebサーバが不正アクセスを受け，顧客情報が漏えいした可能性があると発表した．

対応

2016年4月21日にサーバの異常を発見した外部専門会社からの連絡により，同社の関連会社が不正アクセスを確認した．

原因

同局のブログプログラムで使用しているソフトウェア「ケータイキット for Movable Type」にコマンドインジェクションの脆弱性が存在し，これを悪用した不正アクセスを受けたものとみられる．

被害の範囲

同局が保有する個人情報のうち，約64万件が漏えいした恐れがある．情報漏えいした恐れの

ある情報は，2007年以降に同社のWebサーバのメッセージフォームから番組へメッセージを送付した人，またはプレゼント応募をした人が対象であり，情報漏えいした恐れのある情報項目は，氏名，住所，電話番号，メールアドレス，職業である．

対応

同局では，原因となったソフトウェアの削除，および安全性の確認作業を実施し，Webサーバからの個人情報関連データの削除を行うとともに，個人情報を安全な場所に退避した．さらに，警察，監督官庁への相談・届け出を行い，問い合わせ窓口を設置し，情報漏えいした可能性のあるユーザへ電子メールで連絡を行った．

⑪ FM放送局のWebサーバへのコマンドインジェクション攻撃により，メッセージ送信者及びプレゼント応募者の個人情報64万件が漏えいした恐れ

日にち 2016年4月22日

対　象 FM放送局（社会インフラ）

内容

サーバの異常を発見した外部専門会社からの連絡により，同社の関連会社が不正アクセスを確認した．

原因

同局のブログプログラムで使用しているソフトウェア「ケータイキット for Movable Type」にコマンドインジェクションの脆弱性が存在し，これを悪用した不正アクセスを受けたものとみられる．

被害の範囲

同局が保有する個人情報のうち，約64万件が漏えいした恐れがある．情報漏えいした恐れのある情報は，2007年以降に同社のWebサーバのメッセージフォームから番組へメッセージを送付した人，またはプレゼント応募をした人が対象であり，情報漏えいした恐れのある情報項目は，氏名，住所，電話番号，メールアドレス，職業である．

対応

同局では，原因となったソフトウェアの削除，および安全性の確認作業を実施し，Webサーバからの個人情報関連データの削除を行うとともに，個人情報を安全な場所に退避した．さらに，警察，監督官庁への相談・届け出を行い，問い合わせ窓口を設置し，情報漏えいした可能性のあるユーザへ電子メールで連絡を行った．

⑫ 所属アーティスト公式サイトへのコマンドインジェクション攻撃により，キャンペーン応募者の個人情報が漏えいした恐れ

日にち 2016年4月28日

対　象 企業（芸能事務所）

内容

当該企業は2016年4月28日に所属のアーティスト公式サイトが不正アクセスを受け，個人情報が漏えいした恐れがあることを発表した．外部からの不正アクセスをシステムが検知したため，同社がアクセスログを解析し判明した．

被害の範囲

同社が保有するキャンペーン応募者等の氏名，住所，メールアドレス，電話番号などの個人情報が約35万件漏えいした恐れがある．

原因

同社の調査では，公式サイトで使用されていたソフトウェアのコマンドインジェクション脆弱性を利用されたと発表している．なお，脆弱性が確認されたソフトウェアは「ケータイキット for Movable Type」と報じられている．

対応

同社では，ソフトウェアの脆弱性へ対応するとともに，対策本部を設置し，詳細解析や専門家の意見聴取により対策を強化した．また，問い合わせ窓口を設置した．

（3） 不正アクセスによる攻撃

⑬ グループ企業への標的型攻撃により，顧客の個人情報が社外に漏えいした可能性

日にち 2016年6月14日

対　象 企業

内容

当該企業は2016年６月14日，不正アクセスによる個人情報流出の可能性について報道発表を行った．３月15日に同社のインターネット販売を受け持つ子会社の従業員が標的型攻撃電子メールを開封したことにより，子会社の端末がマルウェアに感染した．マルウェア感染後，社内で不審な通信が観測されているほか，社内サーバ内に攻撃者が作成したとみられるCSV形式のファイルが作成され，その後削除された形跡が発見されており，セキュリティ会社を交えた検討の結果，個人情報漏えいの可能性があるとの判断に至っている．

被害の範囲

漏えいした可能性のある個人情報は自社分が678万名，このほかに提携先企業が扱う個人情報が34万件以上ある．個人情報の内容には，氏名・性別・生年月日・電子メールアドレス・住所・郵便番号・パスポート番号・パスポート取得日が含まれている．

対応

情報漏えいの可能性に関する公表が遅れた理由として，対象者の特定が不十分な状態では利用者に不安と混乱を招くことを懸念し，特定できた段階で公表することとしたと同社は説明している．同社では事故を受けてCSIRT（コンピュータセキュリティインシデントレスポンスチーム）を社内に設置したほか，再発防止策をまとめた報告書を所管官庁に提出した．

⑭　少年による教育情報システム及び校内LANへの不正アクセスにより，教員及び生徒の個人情報が漏えい

日にち　2016年６月26日

対　象　官公庁（教育庁など）

内容

当該自治体の教育情報システム及び校内LANが当自治体在住の17歳の少年を中心とする犯行グループによる不正アクセスを受け，個人情報が漏えいする被害が生じていることが2016年６月26日に報じられた．

対応１（攻撃への対応）

同自治体では，２月15日に警察より同自治体教育庁が不正アクセスを受けた疑いがあるとの連絡により把握したとしている．同自治体の教育情報システムは，同自治体内が運営する中学校，高校，及び一部の公立小中学校約210校が利用している．少年の不正アクセス発覚後に警察から同自治体教育委員会に対して，管理者アカウントが生徒，教職員から閲覧可能な状態であることに対して対応すべきとの助言が行われた．また，同自治体教育委員会は警察からの助言を受け６月20日に改善を実施した．

原因

少年による不正アクセスは，教育情報システムの学習管理のメッセージ機能に脆弱性が存在し，その欠陥を突かれたことによる．メッセージ送信の指定時に自身が在籍する学校の全教職員，生徒の名簿が参照可能な仕様であった．犯行グループの少年は正規のID，パスワードを用いて，メッセージ機能を通じ名簿から個人情報を入手した．

被害の範囲

把握されている不正アクセスの内容には，４校の校務用サーバ（校内LAN）にアクセスしたことによって取得した教員・生徒の個人情報，６校の学習用サーバ（校内LAN）にアクセスして取得した，教材コンテンツ・一部生徒の氏名・部活動・趣味，さらに７件の教育情報システムにアクセスして取得した教員のID・氏名・電子メールアドレス，生徒のID・氏名などが含まれている．

対応２（事後の対応）

同自治体では，問い合わせ窓口の設置，教育情報システムのシステム改修，教育情報システムに係るパスワードの変更などを実施．さらに，生徒，保護者宛に経緯を説明した文書を送付し，警察への情報提供依頼，関係者への聞き取りを実施した．

考察（著者の分析）

上記事例を時系列で見ると，はじめは，DDoSやランサムウェアによるWebなどの閲覧

障害の事象が多く発生しているが，後半はコマンドインジェクションなどによる情報漏洩が多く発生している（図１）．

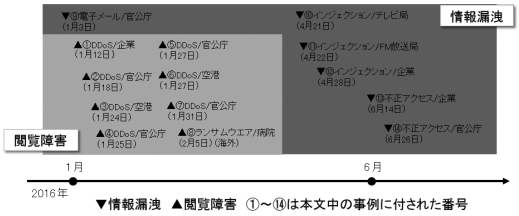

図１　2016年前半サイバー攻撃被害一覧

（注）上図は，文献[22]を基に，著者が独自に作成したものである．

また対象としては，企業や官公庁だけでなく，空港や放送局などの社会インフラにまで攻撃の範囲が及んでいる．更に，攻撃別にみるとDDoS攻撃によるシステムダウンを狙ったものやコマンドインジェクションなど公開されているシステムの脆弱性を狙ったものが多く見受けられる．更に最近では，システムを閲覧不能にして，解除ための身代金を要求するランサムウェアの事例も目立っている．

4.2　カスペルスキー社から提供されている事例

また，カスペルスキー社からも，ウイルスやスパムの情報が，月別にウイルスニュースとして，具体的なマルウェア名を示すなどやや専門的な観点から提供されている[23]．最新（2017年）の情報は以下の通りである．

（以下，サイト[23]を基に，題名と日にち，内容に分けて再構成したものの一部抜粋である）

■Kaspersky Lab，メモリに潜み痕跡を消す「見えない」攻撃を発見

日にち　2017年２月14日

内容

米国，南米，ヨーロッパ，アフリカなど40か国，140以上の組織に侵入し，主に銀行，電気通信，政府機関を標的にしていたこの攻撃は，広く利用されている侵入テストツールや管理ツール，WindowsのPowerShellフレームワークなど，正規のソフトウェアのみを用いる．ハードディスクではなくメモリに潜み，ホワイトリストによる検知を回避し，フォレンジック調査時に手がかりとなる痕跡やマルウェアの検体をほとんど残さない．コンピュータ再起動時には，その痕跡は消去される．

■Kaspersky Lab，Windows環境下でマルウェア「Mirai」を拡散する新たなマルウェアを解析，約500システムへの攻撃を確認

日にち　2017年２月24日

内容

WindowsプラットフォームからLinuxプラットフォームへと感染するMiraiの出現は極めて憂慮すべき事態であり，その開発者のスキルが高いことも懸念点である．コネクテッドテクノロジーに莫大な投資を行っている新興市場への影響が懸念される．

■Kaspersky Lab，データを破壊する新しいマルウェア「StoneDrill」を発見

日にち　2017年３月10日

内容

Kaspersky Labのグローバル調査分析チームは，悪名高いワイパー型マルウェアShamoonと同じく，感染したコンピュータ内のデータを破壊する新たなマルウェアをShamoon2.0の調査中に発見した．StoneDrillは高度な検知回避技術やスパイツールも備えており，中東や欧州の組織を標的にしている．

■20年前のサイバースパイ攻撃「Moonlight Maze」が，近年のAPT攻撃に関連

日にち　2017年４月05日

内容

1990年代後半に米国防総省やNASAなどを標的とした「Moonlight Maze」が使用したバックドアと，2011年に世界有数の高度なサイバースパイグループ「Turla」が使用したバックドアとの関連性を発見した．2017年の別の攻撃に使われたバックドアとも関連している可能性があり，このつながりが証明されれば，Moonlight Mazeは約20年にわたる活動期間の長い攻撃グ

ループとなる．

■Kaspersky Lab，ATMから現金を窃取する「ATMitch」の手口を解明

日にち　2017年４月06日

内容

サイバー犯罪者がファイルレスのマルウェアを使用し，標的の行内ネットワークに侵入した後，ATMのリモート管理機能を悪用してATMを感染させ現金を不正に入手していたことがわかった．

■Kaspersky Lab，世界数百の大企業が使用する正規ソフトウェアのアップデートにバックドアを仕込んだ「ShadowPad」を発見

日にち　2017年８月18日

内容

NetSarangが配信したソフトウェアパッケージに，バックドアが仕込まれていることを発見した．ShadowPadの攻撃者はこのバックドアを使って侵入先のデータを窃取し，外部に送信することができる．Kaspersky Labからの連絡により，NetSarangは直ちに悪意あるコードを削除したソフトウェアのアップデートをリリースし，顧客をデータ窃取の被害から守ることができた．

４.３　その他

上記の他，セキュリティブログとして最新の情報が，トレンドマイクロ社やシマンテック社（ノートン），マカフィー社[24]，カスペルスキー社などから提供されている[25][26][27][28]．

５　対策（トレンドマイクロ社の例）

トレンドマイクロ社では，マルウェアの分類ごとに，その対策を提供している[29]．ここでは，「…とは？」の項で攻撃についての解説を行った後，「脅威内容」でその手法などについて解説し，「影響と被害」でどのような被害が予測されるかについて述べられている．最後に，「対策と予防」として，ユーザ及び管理者が予め行っておくべき予防策と事象が発生した際にとるべき対策などについて述べられている．以下に，一例（ランサムウェア[30]と標的型サイバー攻撃[31]の例）を示す．

（以下，[30][31]を基に，著者が独自に小見出しを入れるなど，分かり易く再構成したものである）

５.１　ランサムウェア

５.１.１　「ランサムウェア（Ransomware）」とは？

ランサムウェアとは，感染したPCをロックしたり，ファイルを暗号化したりすることによって使用不能にした後，元に戻すことと引き換えに「身代金」を要求する不正プログラムである．身代金要求型不正プログラムとも呼ばれる．

５.１.２　脅威内容

手法

スパムメールや，改ざんした正規サイトから，脆弱性を攻撃する不正サイトへ誘導され，ランサムウェアに感染させる．

活動

ランサムウェアが活動開始すると，感染PCの特定機能を無効化し操作不能にする，もしくは，データファイルを暗号化し利用不能にする，などの活動が行われる．

目的

PCを感染前の状態に戻すことと引き換えに金銭の支払いを要求する画面が表示される．

５.１.３　影響と被害

・感染PCの有効な操作ができなくなる．
・感染PC内のファイルやネットワーク共有上のファイルが暗号化され，利用できなくなる（ランサムウェアの駆除を行っても暗号化されたまま残る）．

5.1.4　対策と予防

ユーザ側

・基本的なセキュリティ対策の導入.
・ウイルス対策機能：ランサムウェア本体を検出する．また不正プログラムの行う不審な活動を警告，ブロックする.
・不正サイトへのアクセスブロック：外部不正サイトへのアクセスをブロックすることにより，ランサムウェアや他の不正プログラムの侵入，認証情報の送信などを防ぐことが可能.
・電子メール対策：添付ファイルへのウイルス検出とスパム対策機能により，電子メール経由での不正プログラム侵入を防ぐことが可能.
・脆弱性のアップデート：不正プログラム侵入時に脆弱性への攻撃が利用される事例が多いため，OSや使用しているソフトの脆弱性をアップデートしておくことが重要.

管理者側

「ランサムウェア」は一般ユーザを狙った攻撃であるが，組織内のユーザの活動により組織のネットワークに侵入する可能性もある．基本的な不正プログラム対策にて対応可能である.

・基本対策：エンドポイントへのウイルス対策製品を導入して，内部ネットワークから外部不正サイトへのアクセスをブロックする.
・脆弱性のアップデート：不正プログラム侵入時に脆弱性への攻撃が利用される事例が多いため，クライアントPCの脆弱性対策が重要.
・ファイルサーバのバックアップ強化：ランサムウェアに感染したPCからアクセス可能な共有ファイルが暗号化される被害が増加中.サーバのバックアップをこまめにとることにより，被害を最小限に留められる.

5.2　標的型サイバー攻撃

5.2.1　「標的型サイバー攻撃」とは？

標的型サイバー攻撃とは，重要情報の入手を最終目標として，時間，手段，手法を問わず，目的達成に向け，特定の組織を攻撃対象として，その標的に特化して継続的に行われる一連の攻撃を指す．一般に「APT攻撃」,「持続的標的型攻撃」と呼ばれる場合もある.

5.2.2　攻撃の手法・特徴

標的型サイバー攻撃は，組織的な攻撃者によって長期間にわたり段階的な攻撃を継続して行われる.

目的

攻撃目的：攻撃対象の持つ重要情報の入手を最終的な目標として攻撃が実施される.

対象

攻撃対象：政府，官公庁，企業など，攻撃者の目的となる重要情報を持つ組織が標的となる.

手法

攻撃の「事前準備」段階では標的組織へ侵入するための足掛かりとして，関連する他の組織や個人が一時的な攻撃対象となる場合がある.

攻撃開始から目的達成まで，標的型サイバー攻撃の攻撃手順は，以下の段階に分類できる.

1．事前準備：攻撃標的の決定，標的とその周辺への偵察による情報入手，初期潜入用不正プログラムやC&Cサーバの準備.
2．初期潜入：標的型メールの送信，受信者による添付不正プログラム実行，公開サーバへの脆弱性攻撃による侵入.
3．端末制御：感染環境と所属するネットワーク情報の確認，バックドア型不正プログラムによる標的内端末への感染.
4．情報探索：内部活動ツールのダウンロード，ネットワーク内の情報探索.
5．情報集約：重要情報の収集.
6．情報送出:収集した重要情報の外部入手.

活動

・標的型メールにおいては，関係者や関連業務を偽ったソーシャルエンジニアリングを利用して標的ユーザを信用させ，添付された不正プログラムを開かせる.
・侵入後は，C&Cサーバと呼ばれる攻撃基盤を使って，標的ネットワーク内部のバックド

ア型不正プログラムを遠隔操作し，内部活動ツールを使って標的ネットワーク内部の情報を探索し，情報の収集を行う．

5.2.3　影響と被害

・組織的な攻撃のため，攻撃の目的が達成されるまで攻撃は執拗に継続される．また，事前準備段階での偵察により，標的の弱点を調べ上げた上で攻撃が実施されるため，侵入段階で防ぐことは非常に難しい．
・侵入に成功されると，標的組織内のネットワークや業務，従業員などに関する情報が外部に持ち出される．
・最終的には，攻撃者が目的としている重要情報が外部に持ち出される．

5.2.4　対策と予防

ユーザ側

・標的型サイバー攻撃は，手段，手法を問わず継続して行われる攻撃のため，組織内部のユーザ一人一人が高いセキュリティ意識を持つ必要がある．
・標的型メールなど，侵入時に使用される攻撃手法を理解し，騙されないようにする．
・不審なメールやリンクを安易にクリックしない．
・個人用端末にも総合的なセキュリティソフトを導入し，常に最新の状態に保つ．
・会社や業務，取引先などに関する情報をインターネット上に個人的に投稿しない．

管理者側

・標的型サイバー攻撃は，事前に標的に関する情報収集を行い，弱点を調べた上で執拗に攻撃を継続するため，総合的，多面的な対策を導入するとともに，侵入を前提とした対策を行うことが重要となる．
・エンドポイントやサーバには総合的なセキュリティソフトを導入する．
・メールサーバにおける標的型メールの検出．
・外部への不正なネットワーク通信・接続の検出．
・ネットワーク内部での不審な挙動を可視化する．
・セキュリティポリシーの策定．
・従業員に対するセキュリティ教育，注意喚起の実施．

また，トレンドマイクロ社は，ユーザサポートとして，コンピュータウイルスの一般的な対処方法を記したサイト[32]も提供している．

その他，シマンテック社においても，種別ごとに対処方法を記したサイト[33]が提供されている．

6　まとめ

本稿では，まず各社が示すサイバー攻撃の種類について述べた．サイバー攻撃の種類については，各社異なる場合が多いが，共通する部分もあるので，参考にして頂ければと考える．

次に，最新のサイバー攻撃の傾向を示した後，著者独自の視点から分析し，次の3点を指摘した．①個人，組織ともに情報家電やルータなどのネットワーク機器をはじめとしたIoT機器への攻撃が増加しているが，ユーザのサイバーセキュリティに関する認識はあまり高くなく，パスワードが初期設定のまま使われていたり，容易に推測されやすかったりと課題が残るケースも少なくない．②サイバー攻撃を請け負うサイトなども登場し，専門知識がなくとも攻撃を行える環境が構築されつつある．③既に空港などへのサイバー攻撃がなされているが，今後交通システムなどの社会インフラへの攻撃も増すものと考えられ，実生活に直接的に影響を及ぼす可能性がある．

また，攻撃事例についても，攻撃別に分類し，時系列に沿って図示するなど，著者独自の観点で整理した後，2016年前半のサイバー攻撃の傾向について，著者独自の分析を行った．その結果，IPAの事例では，はじめはWebなどの閲覧障害を狙った攻撃が多く，後半は個人情報などを取得する攻撃が多く報告されていることを指摘した．

サイバー攻撃の手法は巧妙であり，完全に防ぐことは難しいとされているが，少なくとも次の3点により攻撃されにくくすることは可能であると考える．①推測されにくいパスワードを用いる．②デバイスやサイトごとに異なるパスワードを設定する．③システムやアプリケーションのアップデートを行い常にシステムを最新の状態に保つ．

攻撃を防ぐためには，手間を惜しむことなく，上記のような対策を地道に行うことが大切であると考える．

今後，サイバー攻撃について様々な機関から出されている情報を整理して，どの場合にどの情報を使うべきかを論文などを通じて示し，ユーザの認識の向上を図って行く予定である．

謝　辞

本研究はJSPS科研費 JP17K00187の助成を受けたものです．この場を借りて，感謝の意を表します．

参考文献

[1] 日経新聞：Web刊（online）, available from <https：//www.nikkei.com/article/DGXLASDZ15H76_V10C17A5 MM0000/>（accessed 2017-09-26）．

[2] Android端末を踏み台にしたDDoS攻撃発生 Google Playに300本の不正アプリ - ITmedia エンタープライズ（online）, available from <http：//www.itmedia.co.jp/enterprise/articles/1708/29/news052.html>（accessed from 2017-09-26）．

[3] Japan　Symantec JP（online）, available from <https：//www.symantec.com/ja/jp>（accessed 2017-09-28）．

[4] マルウェアとウイルスの違い｜端末保護の基本をシンプルに知る（online）, available from <https：//japan.norton.com/malware-virus-difference-2041>（accessed 2017-09-28）．

[5] カスペルスキー｜ウイルス対策ソフト｜インターネットセキュリティ（online）, available from < http：//www.kaspersky.co.jp/>（accessed 2017-09-26）．

[6] マルウェアにはどんな種類がある？ – カスペルスキー公式ブログ（online）, available from <https：//blog.kaspersky.co.jp/a-malware-classification/1895/>（accessed 2017-09-28）．

[7] Kaspersky：脅威の種類（online）, available from < https：//support.kaspersky.co.jp/614>（accessed 2017-09-26）．

[8] IPA 独立行政法人 情報処理推進機構（online）, available from < https：//www.ipa.go.jp/>（accessed 2017-09-26）．

[9] 情報セキュリティ10大脅威 2017：IPA 独立行政法人 情報処理推進機構（online）, available from < https：//www.ipa.go.jp/security/vuln/10threats2017.html>（accessed 2017-09-26）．

[10] 中山颯，鉄穎，楊笛，田宮和樹，吉岡克成，松本勉：IoT機器へのTelnetを用いたサイバー攻撃の分析, 情報処理学会論文誌, Vol.58, No.9, pp.1399-1409（2017）．

[11] トレンドマイクロ - サイバーセキュリティソリューション（online）, available from <https：//www.trendmicro.com/ja_jp/business.html>（accessed 2017-09-28）．

[12] 資料ダウンロード　2017年 セキュリティ脅威予測　トレンドマイクロ（online）, available from < https：//appweb.trendmicro.com/doc_dl/select.asp?type= 1 &cid=218&cm_re=mainbnr-_-pre-_-2017>（accessed 2017-09-28）．

[13] IT用語辞典 e-Words, available from <http：//e-words.jp/>（accessed 2017-12-08）．

[14] 2017 年インターネットセキュリティ脅威レポート　Symantec JP（online）, available from < https：//www.symantec.com/ja/jp/security-center/threat-report>（accessed 2017-09-28）．

[15] ネットワーク，データ・センター，エンドポイント，モバイル・デバイス対応サイバーセキュリティ・ソリューションのリーディング カンパニーチェック・ポイント・ソフトウェア・テクノロジーズ　Check Point Software Technologies（online）, available from < http：//www.checkpoint.co.jp/>（accessed 2017-09-26）．

[16] Check Point Software Technologies：上半期レポート　サイバー攻撃トレンド 2017（online）, available from < http：//www.checkpoint.co.jp/report/cyber_attack_trend_2017h1.pdf>（accessed 2017-09-26）．

[17] Kaspersky Cyberthreat real-time map（online）, available from <https：//cybermap.kaspersky.com/ja/>（accessed 2017-09-27）．

[18] NICT - トップページ　NICT-情報通信研究機構（online）, available from <https：//www.nict.go.jp/>（accessed 2017-09-28）．

[19] NICTERWEB 2.0（online）, available from <http：//www.nicter.jp/#>（accessed 2017-09-28）．

[20] 中尾浩二，松本文子，井上大輔，馬場俊介，鈴木和也，衛藤将史，吉岡克成，力武健次，堀良彰：インシデント分析センタnicterの可視

化技術, 情報処理学会技術研究報告, Vol.2006, No.81（2006-CSEC-034）, pp.313-319（2006）.
[21] Inoue, D., Yoshioka, K., Eto, M., Hoshizawa, Y. and Nakao, K.：Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities, IEICE Trans. Information and Systems, Vol. E92-D, No.5（2009）.
[22] 別添：被害事例集 - IPA 独立行政法人 情報処理推進機構（online）, available from < https：//www.ipa.go.jp/files/000056149.xlsx>（accessed 2017-09-26）
[23] ウイルスニュース　ニュース　カスペルスキー（online）, available from <https：//www.kaspersky.co.jp/about/news/virus?page= 0 >（accessed 2017-09-27）.
[24] サイバー セキュリティ対策　マカフィー（online）, available from <https：//www.mcafee.com/jp/index.html>（accessed 2017-09-28）.
[25] トレンドマイクロ セキュリティブログ　セキュリティ（ウイルスや脆弱性による攻撃）の最新動向を追うなら，Regional TrendLabs ウイルス解析担当者が執筆するトレンドマイクロ セキュリティ ブログ.（online）, available from < http：//blog.trendmicro.co.jp/>（accessed 2017-09-26）.
[26] ノートン ブログ（online）, available from < https：//japan.norton.com/>（accessed 2017-09-26）.
[27] マカフィー株式会社　公式ブログ（online）, available from < http：//blogs.mcafee.jp/>（accessed 2017-09-26）.
[28] カスペルスキー公式ブログ（online）, available from < https：//blog.kaspersky.co.jp/>（accessed 2017-09-28）.
[29] 脅威と対策　Trend Micro（online）, available from <https：//www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution.html?cm_re=side-_-threatsol-_-top>（accessed 2017-09-28）.
[30] ランサムウェア　トレンドマイクロ（online）, available from <https：//www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.html>（accessed 2017-09-28）.
[31] 標的型サイバー攻撃　トレンドマイクロ（online）, available from < https：//www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/apt.html >（accessed 2017-12-05）.
[32] Virus Support Web（ウイルスサポートウェブ）サポート トレンドマイクロ（online）, available from <http：//esupport.trendmicro.com/ja-jp/enterprise/virus_support/top.aspx?cm_sp=Sup-_-virus-_-sercurity_info_virus_suptop>（accessed 2017-09-28）.
[33] 最新のウイルス　電子メールを介した攻撃からの保護　Security Response（online）, available from <https：//jp.norton.com/security_response/secureemail.jsp>（accessed 2017-09-28）.

注

1 新潟県立大学国際地域学部
2 DDoS攻撃
Distributed Denial of Service attack
DDoS攻撃とは，複数のネットワークに分散する大量のコンピュータが一斉に特定のネットワークやコンピュータへ接続要求を送出し，通信容量をあふれさせて機能を停止させてしまう攻撃.
（「IT用語辞典 e-Words [13]」より完全引用）
3 インジェクション攻撃
injection attack
インジェクション攻撃とは，ソフトウェアへの攻撃手法の一つで，文字列の入力を受け付けるようなプログラムに対し，セキュリティを無効化するような不正な文字列を混入し，システムを乗っ取ったり秘密のデータを詐取したりする手法.
（「IT用語辞典 e-Words[13]」より完全引用）