株式会社 日立システムズ

SSRC-TR-Vol.41

S.S.R.C. 定期
トレンドレポート
Vol.41

株式会社　日立システムズ

セキュリティリサーチセンタ

株式会社 日立システムズ

S.S.R.C.トレンドレポート Vol.41

目次

1. はじめに

S.S.R.C.（Shield Security Research Center）は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信しております。

本文書は、株式会社日立システムズ、SHIELD　セキュリティセンタで日々収集を行っている世界中のサイバーセキュリティに関する情報にもとづき、セキュリティアナリストがセキュリティトレンドをまとめたレポートです。

次のご利用条件を十分にご確認の頂き、ご了承頂いた上でご利用いただきますよう、よろしくお願いいたします。

2. ご利用条件

本文書は株式会社日立システムズ（以下、「当社」といいます。）が作成しています。当社は、本ウェブサイト上の文書及びその内容に関し如何なる保証もするものではありません。万一、本文書の内容に誤りがあった場合でも当社は一切責任を負いかねます。また、本文書に記載されている事項は、予告なしに変更されることがありますので、予めご承知おきください。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3. 概要

3. 1 脆弱性情報

2020 年 3 月に公開された「Microsoft SMBv3 の脆弱性 (CVE-2020-0796)」は、認証されていない遠隔の攻撃者が細工したパケットを送信することで、任意のコードを実行されるおそれがあるものです。この脆弱性は 2017 年に流行した「WannaCry」のように脆弱な端末に感染が広がる可能性があり、今後も注意が必要です。

Windows 社製品の他、Adobe 社製品、トレンドマイクロ社製品、Citrix 社製品等、多くのソフトウェアにおいて深刻なゼロデイ脆弱性情報が公開されるとともに、概念実証コード(PoC)が公開されたものもありました。

3. 2 脅威情報

脅威情報について、マルウェア「Emotet」を用いた攻撃や、フィッシング、ランサムウェアを用いた攻撃が多く見られました。

Emotet の感染活動は 2019 年 6 月頃から減少傾向にありましたが、2019 年 10 月頃から再び活動が活発化しました。その後 11 月に活動が落ち着いたようにみえましたが、12 月に入り再び活動が活発化しました。攻撃メールの件名や内容には、「賞与支払い届」や「新型コロナウイルス感染症」等の社会的な関心事が含まれており、受信者をだましてメールを開かせようとする手口が多くみられました。

フィッシングについては、Amazon や Apple、金融機関等のブランドをかたる手口が引き続き確認されています。また、SMS を用いた二要素認証を突破する事例も多くみられました。

ランサムウェアを用いた攻撃については、「Maze」を用いた攻撃に代表されるように、身代金の支払い要求に応じない場合は盗み出した情報をインターネット上で公開するという事例が多くみられました。

3. 3 その他のサイバー攻撃に関する傾向

前回に引き続き「北朝鮮」「中国」「ロシア」が関与していると思われる攻撃が多く確認されています。

2020 年 1 月頃から、新型コロナウイルス感染症の拡大に便乗するサイバー攻撃が多く確認されました。この中には、国家の関与が疑われている「北朝鮮」「中国」「ロシア」等のサイバー攻撃グループによる攻撃が多く含まれていました。

また、新型コロナウイルス感染症の拡大に伴いテレワークを実施する企業が増えるなか、テレワークを実現するための VPN 製品やウェブ会議システム等に関する多くの脆弱性が確認され、実際に脆弱性を悪用した攻撃が確認されています。

4. トレンドレポート(2019 年第 4 四半期、2020 年第 1 四半期)

2019 年 10 月 1 日から 2020 年 3 月 31 日の間(以下、「当該期間」といいます。)に確認したサイバーセキュリティに関する傾向を次の分類に従って記載します。

4. 1 脆弱性情報

(1) Microsoft

(2) Apple

(3) Android

(4) Adobe

(5) その他

4. 2 脅威情報

(1) Emotet

(2) フィッシング

(3) ランサムウェア

(4) Android に対する攻撃

4. 3 その他のサイバー攻撃に関する傾向

(1) 国家の関与が疑われている攻撃の情報

(2) 新型コロナウイルス感染症関連のサイバー攻撃

(3) テレワーク環境関連

4. 1 脆弱性情報

(1) Microsoft

前回のレポートの対象期間(2019 年 4 月～2019 年 9 月)と同様、多くのゼロデイ脆弱性が見つかっています。これらのゼロデイ脆弱性の中には、セキュリティ更新プログラムが公開される前に攻撃が確認されているものが含まれていました。

また、3 月に公開された「Microsoft SMBv3 の脆弱性」等の緊急性の高い脆弱性が見つかり、月例のセキュリティ更新プログラムの公開とは別に、定例外のセキュリティ更新プログラムの公開が行われました。

Windows 7 のサポートは 2020 年 1 月 14 日で終了しましたが、1 月 17 日に公開された Internet Explorer の脆弱性(CVE-2020-0674)及び 3 月 23 日に公開された Adobe Type Manager ライブラリに起因する脆弱性は Windows 7 に影響を及ぼすものでした。今後も当該 OS に影響を及ぼす脆弱性情報の公開が予想されるため、注意が必要です。

月	概要	分類
10	**MS 月例パッチが公開、脆弱性 59 件を修正 － 悪用は未確認** *http://www.security-next.com/108833*	定例
	「Windows 10 更新アシスタント」にローカル特権昇格の脆弱性 － 修正版がリリース *https://forest.watch.impress.co.jp/docs/news/1212598.html*	定例外
11	**MS 月例更新がリリース、脆弱性 74 件を修正 － 一部でゼロデイ攻撃も** *http://www.security-next.com/109780*	定例、 ゼロデイ
12	**MS 月例パッチが公開、脆弱性 35 件を修正 － 一部ですでに悪用も** *http://www.security-next.com/110601*	定例、 ゼロデイ
	Windows Hello for Business に脆弱性、アップデートを *https://news.mynavi.jp/article/20191206-933931/*	定例外
1	**MS、2020 年最初の月例パッチを公開 － 脆弱性 49 件を修正** *http://www.security-next.com/111440*	定例
	「IE」に未修正の RCE 脆弱性、ゼロデイ攻撃も －「Windows 7」にも影響 *http://www.security-next.com/111579*	定例外、 ゼロデイ、 Windows 7
2	**MS、月例パッチで脆弱性 99 件を解消−ゼロデイ脆弱性も修正** *http://www.security-next.com/112260*	月例、 ゼロデイ
	マイクロソフト、「Zombieload」に対処するマイクロコード更新プログラムを提供 *https://japan.zdnet.com/article/35148898/*	その他

月	概要	分類
3	**MS、月例パッチを公開、脆弱性 115 件に対処 － 悪用未確認** *http://www.security-next.com/113036*	定例
	MS が定例外アップデート、「SMBv3」処理の脆弱性を解消 *http://www.security-next.com/113117*	定例外
	ゼロデイ脆弱性、攻撃対象は「Windows 7」 － 「Windows 10」への影響は限定的 *http://www.security-next.com/113411*	定例外、ゼロデイ、Windows 7

（補足）「分類」欄は、定例外のセキュリティ更新プログラムが公開されたものを「定例外」、ゼロデイ脆弱性に関するものを「ゼロデイ」、Windows 7 に関する脆弱性情報を「Windows 7」と記載しています。

（注）上記内容は、当該期間に公開されたすべての情報を網羅しているものではありません。また、「分類」につきましては、独自に分類した内容を記載しています。
これ以降に記載している内容についても同様です。

(2) Apple

Apple 社製品に関する脆弱性は Windows 等の他のソフトウェアと比較すると少ないものの、ほぼ毎月脆弱性情報が公開され、セキュリティアップデートの配信が行われています。

前回のレポートの対象期間（2019 年 4 月～2019 年 9 月）においては macOS に関するゼロデイ脆弱性情報が公開されましたが、当該期間において Apple 社製品に関するゼロデイ脆弱性情報は確認されませんでした。

月	概要	分類
10	**Apple 製品に複数の脆弱性 –「macOS Catalina」、Windows 版「iTunes」「iCloud」など** *https://forest.watch.impress.co.jp/docs/news/1211689.html*	macOS
	「iOS 13.2」「同 12.4.3」など最新 OS 公開 – 修正内容は今後公開予定 *http://www.security-next.com/109331*	iOS、iPadOS
11	**iOS や macOS に複数の脆弱性、アップデートを** *https://news.mynavi.jp/article/20191031-917189/*	iOS、macOS、watchOS
	iPhone やスマートスピーカーが「光」でハッキング可能？研究者が脆弱性を報告 *https://japanese.engadget.com/2019/11/04/iphone/*	その他
	macOS 暗号化メールの一部が平文保存されるバグ発見。アップルは修正を約束 *https://japanese.engadget.com/2019/11/08/macos/*	macOS
12	**iPhone の修正困難な脆弱性 – 公開実証コードをフォレンジック企業が採用** *http://www.security-next.com/110926*	その他
1	**Apple、「iOS 13.3.1」をリリース – 脆弱性 23 件を修正** *http://www.security-next.com/111870*	iOS、iPadOS
3	**Apple、「iOS 13.4」「iPadOS 13.4」を正式公開** *https://forest.watch.impress.co.jp/docs/news/1242795.html*	iOS、iPadOS
	iOS で VPN 利用時、一部の通信が VPN をバイパスする脆弱性 *https://www.zaikei.co.jp/article/20200330/559700.html*	iOS

（補足）「分類」欄は、iOS に関する脆弱性を「iOS」、macOS に関する脆弱性を「macOS」、iPadOS に関する脆弱性を「iPadOS」、watchOS に関する脆弱性を「watchOS」、それ以外の Apple 製品に関する脆弱性を「その他」と記載しています。

(3) Android

Android に関する脆弱性情報は、主に Google が月例で行うセキュリティパッチの提供とともに公開されました。当該期間において公開されたゼロデイの脆弱性情報は、10 月に公開された 1 件のみでしたが、公開された時点で悪用が確認されていたものです。

月	概要	分類
10	**Google、Android の 2019 年 10 月セキュリティ情報を発表** *https://forest.watch.impress.co.jp/docs/news/1211457.html*	定例
	Android に新たなゼロデイ脆弱性、アップデートに注目 *https://news.mynavi.jp/article/20191008-905974/*	定例外、 ゼロデイ
11	**Google、Android の 2019 年 11 月セキュリティ情報を発表** *https://forest.watch.impress.co.jp/docs/news/1216759.html*	定例
	「WhatsApp」だけではない、Android 向け GIF 処理ライブラリの脆弱性に注意 *http://www.security-next.com/110181*	定例外
12	**Google、Android の 2019 年 12 月セキュリティ情報を発表** *https://forest.watch.impress.co.jp/docs/news/1222298.html*	定例
	Android にマルウェアがスマホを乗っ取る脆弱性「StrandHogg」が発見される、既に一部銀行口座からは盗難被害も *https://gigazine.net/news/20191203-android-strandhogg/*	定例外
1	**Google、Android の 2020 年 1 月セキュリティ情報を発表** *https://forest.watch.impress.co.jp/docs/news/1227675.html*	定例
2	**Google、Android の 2020 年 2 月セキュリティ情報を発表** *https://forest.watch.impress.co.jp/docs/news/1233093.html*	定例
	Android に任意コード実行の深刻な脆弱性、すぐにアップデートを *https://news.mynavi.jp/article/20200211-970974/*	定例外
3	**Google、Android の月例セキュリティ情報を発表 ～Amazon Fire など MediaTek 端末でルートを奪取される問題にも対処** *https://forest.watch.impress.co.jp/docs/news/1238758.html*	定例

（補足）「分類」欄は、月例の脆弱性情報の公開を「定例」、月例以外の脆弱性情報の公開を「定例外」、ゼロデイの脆弱性が公表されたものを「ゼロデイ」と記載しています。（次の(4)も同様です。）

(4) Adobe

前回のレポートの対象期間(2019 年 4 月～2019 年 9 月)においては、月例の脆弱性情報以外に目立った情報は確認できませんでしたが、当該期間においては月例以外で脆弱性情報が公開されるとともに、セキュリティアップデートがリリースされました。

月例及び月例以外で公開された脆弱性は、いずれも重要度が「Critical」、「Important」と危険度の高いものでした。

月	概要	分類
10	「Adobe Acrobat/Reader」にセキュリティアップデート、68 件の脆弱性を修正 *https://internet.watch.impress.co.jp/docs/news/1212974.html*	定例
	「Adobe Acrobat」「Adobe Reader」の定例外更新 － まもなく公開予定 *http://www.security-next.com/108977*	定例外
11	「Adobe Acrobat/Reader」に深刻な脆弱性 Adobe、複数製品向けにアップデートをリリース － 深刻な脆弱性を修正 5 月 14 日にパッチを公開予定 *http://www.security-next.com/104734*	定例
12	「Adobe Acrobat/Reader」に複数の深刻な脆弱性 － 更新リリース *http://www.security-next.com/110597*	定例
1	Windows 版「Illustrator CC 2019」に致命的な脆弱性 -Adobe、月例セキュリティ情報を発表 *https://forest.watch.impress.co.jp/docs/news/1229174.html*	定例
2	「AdobeAcrobat/Reader」にアップデート-脆弱性 17 件を解消 *http://www.security-next.com/112258*	定例
	「AdobeFlashPlayer」に深刻な脆弱性-アップデートが公開 *http://www.security-next.com/105638*	定例
	「Adobe Framemaker」に深刻な脆弱性 － 適用優先度は低設定 *http://www.security-next.com/112446*	定例
3	「Adobe Acrobat/Reader」に深刻な脆弱性 －3 月 17 日に定例外パッチ *http://www.security-next.com/113124*	定例外

(5) その他

「4.1 脆弱性情報 (1) Microsoft」で示したように Windows に関するゼロデイ脆弱性情報は以前から頻繁に公開されています。加えて、当該期間において「Chrome」や「ウイルスバスター」、「Citrix ADC」、「Citrix Gateway」等、Windows 以外の多くのソフトウェアについても深刻なゼロデイ脆弱性情報や PoC(概念実証コード)が公開されました。

月	概要	分類
10	**ウイルスバスター コーポレートエディションの脆弱性(CVE-2019-18187)を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い** *https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=3592*	ゼロデイ
11	**「Chrome」ゼロデイ脆弱性、水飲み場攻撃「WizardOpium 作戦」に悪用** *http://www.security-next.com/109528*	ゼロデイ
	全文検索システム「Apache Solr」に脆弱性 - ゼロデイ攻撃のおそれも *http://www.security-next.com/110115*	ゼロデイ PoC
1	**「Firefox」に深刻な脆弱性、ゼロデイ攻撃も - 今年 2 度目の更新** *http://www.security-next.com/111312*	ゼロデイ
	「Citrix ADC」などに深刻な脆弱性、パッチ未提供 - 早急に緩和策実施を *http://www.security-next.com/111115*	ゼロデイ
	Apache Tomcat における脆弱性(CVE-2020-1938)について *https://www.ipa.go.jp/security/ciadr/vul/alert20200225.html*	PoC
3	**ウイルスバスター ビジネスセキュリティの脆弱性(CVE-2020-8468)を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い** *https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=3729*	ゼロデイ

(補足)「分類」欄は、ゼロデイ脆弱性に関するものを「ゼロデイ」、PoC が公開されたものを「PoC」と記載しています。

4. 2 脅威情報

(1) Emotet

Emotet の感染活動は 2019 年 6 月頃から減少傾向にありましたが、2019 年 10 月頃から再び活動が活発化し、公的機関から注意喚起が行われました。その後、11 月に入りいったん落ち着いたかのようにみえましたが、12 月に入り再び活動が活発になりました。

Emotet への感染を目的とするメールの件名や内容は、公的機関の職員になりすましたものや、メールの件名に「Re:」を入れてあたかも返信のメールと思わせるもの、「請求書」等の業務に関連しそうなキーワードを使用しているものが多く見受けられました。また、ハロウィンやバレンタイン等のイベントに便乗したものや、新型コロナウイルス感染症の拡大に便乗したものもありました。

機能面について、従来の機能に加えて Wi-Fi 経由で感染する機能の追加が確認されています。

月	概要	分類
10	**10 月は「Emotet」が急増 － 3 カ月間の休止経て** *http://www.security-next.com/110007*	その他 （活動傾向）
	大阪大学を騙る不審メールについてのお知らせとお詫び *https://www.osaka-u.ac.jp/ja/news/topics/2019/10/03_01*	大学
	神戸大学構成員を騙る不審メールについてのお知らせとお詫び *https://www.kobe-u.ac.jp/NEWS/info/2019_10_24_01.html*	大学
	パソコンのウイルス感染による情報流出の可能性に関するお知らせとお詫び *http://fukudashin.jp/news/552*	会社
11	**EMOTET(エモテット)感染により 1 万 8 千件超のメール情報が流出か ｜ 首都大学東京** *https://cybersecurity-jp.com/news/34022*	大学
	イオングループの従業員を騙る不審なメールについてのお知らせ *https://www.aeon.info/important/release_18835/*	会社
12	**「Emotet」に感染、なりすましメールが送信 － サンウェル** *http://www.security-next.com/110402*	会社
	「賞与支払い届」装うスパムメールに注意　中身はマルウェア「Emotet」 パスワードなど流出の恐れ *https://www.itmedia.co.jp/news/articles/1912/12/news109.html*	会社
	「Emotet」感染、なりすましメールに注意喚起 － 群馬中央病院 *http://www.security-next.com/110707*	病院

月	概要	分類
12	ばらまき型攻撃メール(Emotet)に関する注意喚起 *https://www.cc.uec.ac.jp/blogs/news/2020/01/20200130malwareemotet.html*	大学
	「Emotet」に感染、なりすましメールに注意喚起 － 加藤製作所 *http://www.security-next.com/110885*	会社
	グループ会社で「Emotet」感染、なりすましメールが送信 － シナネン *http://www.security-next.com/111041*	会社
1	引き続き国内で拡大する「EMOTET」の脅威 *https://blog.trendmicro.co.jp/archives/23648*	その他 (活動傾向)
	Emotet 感染、なりすましメールが送信 － 軽金属製品協会 *http://www.security-next.com/111205*	会社
	「Emotet」感染でなりすましメール送信 － 岐阜新聞社 *http://www.security-next.com/111681*	会社
	千葉県のなりすましメール出回る －Emotet 感染は確認されず *http://www.security-next.com/111719*	自治体
	Emotet 感染メールに「新型コロナウイルス」、流行便乗攻撃に警戒を *https://japan.zdnet.com/article/35148659/*	不特定
2	「Emotet」など複数マルウェア、新型コロナ拡大に便乗 － フィッシングも *http://www.security-next.com/112111*	不特定
	「Emotet」に近接「Wi-Fi」経由で感染を拡大する機能 *http://www.security-next.com/112341*	その他 (機能)
3	NICT に届いた Emotet への感染を狙ったメール(2019 年 9 月 －2020 年 2 月) *https://blog.nicter.jp/2020/03/emotet-mail-201909-202002/*	その他 (活動傾向)
	「Emotet」に感染、メアド流出の可能性 － 関電グループ会社 *http://www.security-next.com/112956*	会社

(補足)「分類」欄は、攻撃対象となった組織を独自に分類して記載しています。また、Emotet の感染活動に関する内容については「その他(活動傾向)」、Emotet の機能に関する内容については「その他(機能)」と記載しています。

(2) フィッシング

フィッシング対策協議会が公開している情報(2020 年 4 月 2 日公開)によると、月別のフィッシング報告件数は、2020 年 1 月は 6,653 件、2 月は 7,630 件であり 2019 年 12 月の 8,208 件と比べて減少しましたが、2020 年 3 月は 9,671 件となり過去最多となりました。

当該期間において、二要素認証を突破する事例が多く見られました。ユーザに偽 SMS を送信して偽サイトに誘導し認証情報を窃取するとともに、正規サイトから発行されるワンタイムパスワードを入力させるなどの手口が確認され、10 月には警察庁と日本サイバー犯罪対策センター(JC3)、国内大手銀行から同手口に関する注意喚起が行われました。

2019 年 11 月、フィッシング詐欺キャンペーンに Android アプリが使用された事例が確認されました。米セキュリティ会社 Sucuri 社によると、フィッシング詐欺キャンペーンにモバイルアプリが使われるのは初めてである可能性が高いとのことです。

月	概要	分類
11	**Office365 ユーザを狙う新たなフィッシング攻撃が登場。ボイスメールを利用して緊急性の高さ装う** *https://news.yahoo.co.jp/byline/ohmototakashi/20191104-00149479/*	メール
	WebEx への招待を装い、被害者パソコンの遠隔操作を狙うフィッシングキャンペーンが発生 *https://news.yahoo.co.jp/byline/ohmototakashi/20191110-00150235/*	メール
	MyJCB をかたるフィッシング (2019/11/12) *https://www.antiphishing.jp/news/alert/myjcb_20191112.html*	メール
	フィッシング詐欺に使われる Android アプリを確認、要注意 *https://news.mynavi.jp/article/20191115-923594/*	Android アプリ
	「Office 365」の管理者狙うフィッシング攻撃 - さらなる攻撃の起点に *http://www.security-next.com/109996*	メール
	「PayPay」装うフィッシング - 加盟店やフリマ利用者がターゲット *http://www.security-next.com/110087*	メール
12	**スマートスピーカー「Google Home」や「Alexa」を悪用して盗聴やフィッシング攻撃を行う手法が実証される** *https://blog.trendmicro.co.jp/archives/22976*	その他
	トレンドマイクロを騙るフィッシング詐欺サイトについて調べてみた *https://piyolog.hatenadiary.jp/entry/2019/12/10/064915*	Web サイト
	金融機関を装ったフィッシングについて *https://tike.hatenablog.com/entry/2019/12/28/234925*	メール、SMS

月	概要	分類
1	サーバ公開後に不正アクセス、フィッシングの踏み台に － お茶大 *http://www.security-next.com/111895*	メール
2	「Emotet」など複数マルウェア、新型コロナ拡大に便乗 － フィッシングも *http://www.security-next.com/112111*	その他
	個人情報の漏洩及びフィッシングメールの送信について *https://www.tuat.ac.jp/NEWS/info/20200205_01.html*	メール
	映画賞の話題に便乗するマルウェアとフィッシング詐欺 *https://blog.kaspersky.co.jp/2020_and-the-malware-goes-to/26845/*	その他
	新型コロナウイルスに乗じて WHO かたるフィッシング詐欺の恐れも *https://japan.zdnet.com/article/35149169/*	メール
	バレンタインデーに乗じたマルウェア感染やフィッシング詐欺に注意 *https://news.mynavi.jp/article/20200214-973464/*	Web サイト
	プエルトリコ政府機関がフィッシング被害。260 万ドルを詐欺グループに送金 *https://japanese.engadget.com/jp-2020-02-14-260.html*	メール
	佐川急便など宅配業者をかたる偽 SMS に引き続き注意、累計相談数が 2000 件超に *https://internet.watch.impress.co.jp/docs/news/1236449.html*	SMS
3	新型コロナウイルスに便乗したスピアフィッシング″、中国やロシアなどの攻撃グループが仕掛ける″ *https://internet.watch.impress.co.jp/docs/news/1241721.html*	メール
	「PayPay」装うフィッシング － 電子署名説明 URL でも偽サイト誘導 *http://www.security-next.com/113394*	メール
	「Pokemon GO」利用者狙うフィッシング － 偽領収書で不安煽る *http://www.security-next.com/113531*	メール
	巧妙な手口で「二要素認証」を突破、ネットバンキングの「ワンタイムパスワード」を狙う偽サイトに注意 *https://internet.watch.impress.co.jp/docs/column/security_basic/1240360.html*	メール SMS

（補足）「分類」欄は、メールを用いた手口を「メール」、SMS を用いた手口を「SMS」、正規 Web サイトを改ざんするなど Web サイトを用いた手口を「Web サイト」と記載しています。

(3) ランサムウェア

ランサムウェアを用いた攻撃が引き続き多く発生しており、会社や公的機関等の組織を標的としたものが多い傾向にあります。

当該期間において、「Maze」というランサムウェアを用いた攻撃キャンペーンが確認されました。Maze を用いた攻撃の特徴は、ファイルを盗み出すとともに暗号化を行い、復号するための身代金の支払いに応じない場合に、盗み出した情報をインターネット上で公開をするというものです。このように、当該期間において身代金の支払いに応じない場合に盗み出した情報を公開するという事例が多く確認されました。

保険に加入している企業がランサムウェアの被害に遭った場合、保険金を使って身代金を払うことができるため、攻撃者が身代金を高く設定する傾向にあります。サイバーセキュリティ企業のエムシソフトの報告によると、2019 年の米国での被害額は 75 億ドル以上に達した可能性があるとのことです。

月	概要	分類
10	**ランサムウェア「BitPaymer」、Windows 版「iTunes」の脆弱性を悪用** *https://japan.cnet.com/article/35143857/*	会社
	多数の医療機関で被害、ヘルスケア業界を狙うランサムウェア *https://blog.trendmicro.co.jp/archives/22711*	医療機関
11	**Windows 10 更新促す偽メールでランサムウェア被害の恐れ-セキュリティ企業が注意喚起** *https://japan.zdnet.com/article/35145650/*	Microsoft ユーザ
	政府機関になりすましてドイツ、イタリアおよび米国の組織を狙う TA2101 *https://www.proofpoint.com/jp/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us*	会社
12	**米データセンター大手にランサムウェア攻撃、仮想通貨で身代金を要求される** *https://jp.cointelegraph.com/news/texas-based-data-center-cyrusone-hit-by-ransomware-attack*	会社
	ニューオーリンズ市にランサムウェア攻撃、システムを遮断して緊急対応 *https://japan.cnet.com/article/35146890/*	自治体
	ランサムウェア「Maze」による Allied Universal の侵害と盗まれたデータの漏洩 *https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/*	会社 データ公開
	Maze ランサムウェアによりペンサコーラ市から盗まれたファイルが公開 *https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/*	自治体 データ公開

月	概要	分類
1	**ジョージア州の製造業者のサウスワイヤーの「Maze」による被害** *https://diriga.com/2019/12/16/maze-ransomware-demands-6-million-ransom-from-southwire/*	会社
	Maze ランサムウェアにより Medical Diagnostic Laboratories から盗まれたファイルが公開 *https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/*	医療機関 データ公開
2	**Maze がランサムウェア攻撃で PEI から盗まれたとされるデータを投稿する** *https://www.itworldcanada.com/article/maze-posts-data-allegedly-stolen-from-pei-in-ransomware-attack/427931*	政府機関
	法律事務所のランサムウェア「Maze」による被害 *https://blog.knowbe4.com/law-firms-are-the-latest-victims-of-mazes-ransomware-and-extortion-attacks*	会社
	Maze の蔓延は、フランス、FBI 当局からの勧告の中でも継続 *https://www.cyberscoop.com/maze-ransomware-law-firms-fbi/*	政府機関 等
	米信用組合の CUNA がランサムウェア感染の疑いでシステムダウン *https://jp.techcrunch.com/2020/02/07/2020-02-07-cuna-ransomware-offline/*	その他
	知人からのメール装い感染狙うランサムウェア「Mailto」に注意 *http://www.security-next.com/112199*	個人他
	天然ガス圧縮施設、ランサムウェアによるサイバー攻撃受け 2 日間操業停止 *https://news.mynavi.jp/article/20200221-978348/*	会社
	ランサムウェアを操る脅迫犯、盗んだデータを公開 *https://blog.kaspersky.co.jp/ransomware-data-disclosure/26862/*	会社 データ公開
	「SODINOKIBI」被害事例に見るランサムウェアの攻撃手法 *https://blog.trendmicro.co.jp/archives/23716*	会社 データ公開
	ランサムウェアの開発者が「身代金を支払わなかった企業のデータを公開するブログ」を作成すると脅迫 *https://gigazine.net/news/20200116-nemty-ransomware-data-leak-strategy/*	会社 データ公開
3	**米セキュリティー保険大手の Chubb がランサムウェア「Maze」の攻撃を受けデータを盗まれる** *https://jp.techcrunch.com/2020/03/27/2020-03-26-chubb-insurance-breach-ransomware/*	会社
	フィンテック企業の Finastra にランサムウェアによる攻撃 *https://www.cpomagazine.com/cyber-security/ransomware-attack-hits-fintech-company-finastra*	会社

（補足）「分類」欄は、攻撃対象となった組織を独自に分類して記載しています。また、攻撃対象となった組織から盗まれたデータが公開されたもの又は公開すると脅迫されたものは「データ公開」と記載しています。

(4) Android に対する攻撃

ユーザに悪意のあるアプリケーションをインストールさせるため、Google Play 上で不正なアプリケーションを配信する事例が多く確認されています。

以前から Google Play 上に不正なアプリが存在することが確認されていましたが、2019 年 12 月に 3,4,33 個、2020 年 2 月に約 600 個の不正アプリに関する情報が公開されているとおり、その数が非常に多くなってきています。

これらの不正なアプリは、Android 端末を遠隔で操作可能とするような機能を持つものや、不正決済機能を持つものがあります。「StrandHogg」という脆弱性が悪用され事例では、銀行口座の情報が抜き取られる被害が確認されています。

月	概要	分類
10	**Android で工場出荷時の状態に戻しても撃退不可なマルウェア「xHelper」** *https://gigazine.net/news/20191030-unremovable-malware-xhelper/*	Google Play
11	**フィッシング詐欺に使われる Android アプリを確認、要注意** *https://news.mynavi.jp/article/20191115-923594/*	その他
	新しい検出回避機能を備えた Android 向けアドウェアが Google Play から拡散 *https://blog.trendmicro.co.jp/archives/22910*	Google Play
	不正決済機能を備えた「カメラアプリ」が Google Play に *http://www.security-next.com/109744*	Google Play
12	**情報窃取などにつながる脆弱性を抱えたアプリを Google Play 上で 3,433 個確認** *https://is702.jp/news/3602/partner/101_g/*	Google Play
	Android にマルウェアがスマホを乗っ取る脆弱性「StrandHogg」が発見される、既に一部銀行口座からは盗難被害も *https://gigazine.net/news/20191203-android-strandhogg/*	その他
1	**Android の UAF 脆弱性を利用する不正アプリを初確認、サイバー犯罪集団「SideWinder」が関与か** *https://blog.trendmicro.co.jp/archives/23528*	Google Play
2	**削除を困難にするトロイの木馬、Android ユーザの約 1/4 が影響(Dr.WEB)** *https://scan.netsecurity.ne.jp/article/2020/02/03/43621.html*	その他
	グーグル、悪質なアドウェア約 600 本を「Google Play」から削除 *https://japan.cnet.com/article/35149725/*	Google Play
3	**新型コロナの情報提供をうたいユーザーを追跡する Android アプリが見つかる** *https://japan.cnet.com/article/35151083/*	その他
	偽クリーナーアプリ、日本で過去 3 ヶ月間に約 5 万件の感染被害 *https://securitynews.so-net.ne.jp/news/sec_30147.html*	Google Play

（補足）「分類」欄は、Google Play にて不正なアプリが配信されていたものを「Google Play」、その他の Android アプリ関連の情報を「その他」と記載しています。

4. 3 その他のサイバー攻撃に関する傾向

(1) 国家の関与が疑われている攻撃

以前から「北朝鮮」「中国」「ロシア」の関与が疑われている攻撃が多く確認されており、当該期間においても同じ傾向が見られました。

2020 年 1 月以降、新型コロナウイルス感染症の拡大に便乗したサイバー攻撃が多く確認されており、その中で国家の関与が疑われているサイバー攻撃グループの活動も多く見られました。

また、日本の自動車メーカーや総合電機メーカーに対するサイバー攻撃に関する報道があったように、日本に対する攻撃が引き続き確認されています。

月	概要	分類
10	**中国関与の「APT10」、マレーシアやベトナムの医療関連に攻撃展開** *http://www.security-next.com/108894*	中国
	PKPLUG: 東南アジアを狙い続ける中国の攻撃グループの追跡 *https://unit42.paloaltonetworks.jp/pkplug_chinese_cyber_espionage_group_attacking_asia/*	中国
	北朝鮮のハッカー集団が MacOS を標的にしたマルウェアを作成 *https://markets.bitbank.cc/article/j1z5xrib30516*	北朝鮮
	中国ハッカー、SQL サーバー改変するマルウエア開発 *http://www.alertchina.com/archives/20467978.html*	中国
	北朝鮮のハッカー集団が作成したマルウェアが原子力発電所のネットワークに侵入 *https://gigazine.net/news/20191031-indian-nuclear-power-plant-hacked/*	北朝鮮
11	**通信事業者のサーバーから SMS メッセージを盗むマルウェア-中国が関与か** *https://japan.zdnet.com/article/35144781/*	中国
	全米製造業協会にサイバー攻撃、中国ハッカー集団関与か＝関係筋 *https://jp.reuters.com/article/usa-trade-china-cyber-idJPKBN1XN2L5*	中国
	10 年以上活動するロシアのハッカー集団、2 年ぶりに表舞台に *https://www.technologyreview.jp/s/168417/kremlin-hackers-are-back-in-the-spotlight-after-2016-election-breach/*	ロシア
12	**北朝鮮「ラザルス」、東欧サイバー犯罪集団と共謀＝報告書** *https://jp.reuters.com/article/usa-cyber-north-korea-idJPKBN1YF2OC*	北朝鮮
	中国のハッカー集団、2 要素認証をかいくぐり政府機関などを攻撃 － 研究者が発表 *https://japan.cnet.com/article/35147287/*	中国
	トヨタも標的か、ハッカー集団にベトナム政府の影ー知財権窃盗関与も *https://www.bloomberg.co.jp/news/articles/2019-12-24/Q2ZMEHT1UM0Y01*	ベトナム

月	概要	分類
1	**ロシア軍関連のハッカー、ウクライナ企業にサイバー攻撃　米民主党バイデンの息子が勤務** *https://www.newsweekjapan.jp/stories/world/2020/01/post-92138.php*	ロシア
	危ないのは三菱電機だけじゃない！ベトナム・韓国などからも日本企業を狙ったサイバー攻撃・不正アクセスが激化 *https://finders.me/articles.php?id=1598*	韓国、ベトナム他
2	**北朝鮮が文大統領側近らにサイバー攻撃** *https://www.worldtimes.co.jp/world/korea/102499.html*	北朝鮮
	ロシア情報機関の関与非難＝ジョージアへのサイバー攻撃―英米 *https://www.jiji.com/jc/article?k=2020022100231*	ロシア
3	**「Exchange Server」への APT 攻撃が進行中、修正済みの脆弱性を悪用** *https://japan.zdnet.com/article/35150555/*	複数国
	新型コロナウイルスに便乗したスピアフィッシング"中国やロシアなどの攻撃グループが仕掛ける" *https://internet.watch.impress.co.jp/docs/news/1241721.html*	中国、ロシア
	ロシアの攻撃グループが戦術を変更-脆弱性を持つメールサーバーをスキャン *https://japan.zdnet.com/article/35151187/*	ロシア
	中国ハッカー集団のスパイ行為、1 月下旬以降に急増＝米調査会社 *https://jp.reuters.com/article/usa-china-cyber-idJPKBN21D0K2*	中国
	国家の支援を受けたハッカーも新型コロナ騒動に乗じた攻撃キャンペーン *https://japan.zdnet.com/article/35150872/*	中国、ロシア、北朝鮮
	新型コロナ「便乗」、中国・ロシア系ハッカーが活発化 *https://www.technologyreview.jp/s/192450/chinese-hackers-and-others-are-exploiting-coronavirus-fears-for-cyberespionage/*	中国、ロシア
	国家関与のサイバー攻撃、新型コロナ問題に便乗 － 中国のグループも *http://www.security-next.com/113281*	中国、ロシア、北朝鮮

（補足）「分類」欄は、関与が疑われている国家を記載しています。

(2) 新型コロナウイルス感染拡大に便乗したサイバー攻撃

「4.2 脅威情報 (1) Emotet」で示したとおり、2020 年 1 月以降、新型コロナウイルス感染症の拡大に便乗した「Emotet」等のマルウェアへの感染を目的とした攻撃が多く観測されています。

日本において、保健所や障害者福祉施設からの感染予防に関するメールを装ったものが確認されており、Emotet への感染を目的としたものでした。

海外においては、世界保健機構(WHO)や米国疾病管理予防センター(CDC)等からのメールを装ったフィッシング詐欺が確認されています。

月	概要	分類
1	**Emotet 感染メールに「新型コロナウイルス」、流行便乗攻撃に警戒を** *https://japan.zdnet.com/article/35148659/*	メール
2	**「Emotet」など複数マルウェア、新型コロナ拡大に便乗 － フィッシングも** *http://www.security-next.com/112111*	メール、SMS
	新型コロナウイルスに乗じて WHO かたるフィッシング詐欺の恐れも *https://japan.zdnet.com/article/35149169/*	メール
	新型コロナウイルス関連情報を装うマルウェアや詐欺メール *https://blog.kaspersky.co.jp/coronavirus-reached-the-web/26781/*	メール
3	**スマホ狙う「Roaming Mantis」、新型コロナ便乗も** *http://www.security-next.com/112732*	SMS
	「新型コロナウイルス感染症の拡散状況マップがマルウェアの拡散に使われている」とセキュリティ専門家が指摘 *https://gigazine.net/news/20200316-live-coronavirus-map-spread-malware/*	Web サイト
	米保健福祉省にサイバー攻撃-新型コロナ対応を遅らせる狙いか *https://japan.cnet.com/article/35150909/*	DDoS
	国家の支援を受けたハッカーも新型コロナ騒動に乗じた攻撃キャンペーン *https://japan.zdnet.com/article/35150872/*	メール
	新型コロナウイルスに便乗したスピアフィッシング"中国やロシアなどの攻撃グループが仕掛ける" *https://sawzow.com/18/08/43/45/8196/post-0/*	メール
	新型コロナの追跡アプリを装ったマルウェア、パスワード解除に仮想通貨を要求 *https://coinpost.jp/?p=138968*	Android アプリ
	新型コロナの情報提供をうたいユーザーを追跡する Android アプリが見つかる *https://japan.cnet.com/article/35151083/*	Android アプリ
	ファイア・アイ、新型コロナに便乗したサイバー攻撃を複数観測、おとり文書でマルウェアの展開を狙う *https://enterprisezine.jp/news/detail/12799*	メール

月	概要	分類
3	**新型コロナウイルスに便乗するサイバー攻撃、日本も標的に** *https://crypto.watch.impress.co.jp/docs/news/1242918.html*	メール
	ルーターの DNS を乗っ取り、COVID-19 感染情報と称してダウンロードさせ、パスワードを盗む悪質なマルウェアが横行中 *https://pc.watch.impress.co.jp/docs/news/1243173.html*	DNS 乗っ取り

（補足）「分類」欄は、メールを用いた攻撃の手口を「メール」記載しているように、それぞれの攻撃の手口を記載しています。

(3) テレワーク環境関連

新型コロナウイルスの感染拡大に伴いテレワークを実施する企業が増えているなか、VPN 製品（リモートアクセス製品）やウェブ会議システム等のテレワークを実現するための製品やサービスに多くの脆弱性が見つかりました。また、これらの脆弱性を悪用した攻撃や、ウェブ会議システムへの招待を装ったフィッシング詐欺キャンペーン等が確認され、公的機関から注意喚起が行われました。

米ファイア・アイ社によると、中国のサイバー攻撃グループ「APT41」が、2020 年 1 月～3 月にかけて Citrix NetScaler/ADC や Cisco ルーター等の脆弱性を悪用して攻撃活動を行っていたとのことです。

月	概要	分類
10	**Cisco Webex Meetings Suite と Cisco Webex Meetings Online における未認証会議参加の脆弱性** *https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-20200124-webex-unauthjoin.html*	ウェブ会議
	複数の Citrix 製品の脆弱性（CVE-2019-19781）に関する注意喚起 *https://www.jpcert.or.jp/at/2020/at200003.html*	リモート アクセス
1	**Webex への招待を装い、被害者パソコンの遠隔操作を狙うフィッシングキャンペーンが発生** *https://news.yahoo.co.jp/byline/ohmototakashi/20191110-00150235/*	ウェブ会議
3	**セキュリティ製品の「VPN」機能に相次いで脆弱性** *http://www.security-next.com/106918*	VPN
	急増した怪しい「Zoom」関連ドメイン--人気ビデオ会議サービスを狙うサイバー犯罪者 *https://japan.cnet.com/article/35151651/*	ウェブ会議
	複数のシスコ製品に脆弱性、一部は深刻度重大 - アップデートを *https://news.mynavi.jp/article/20200306-989697/*	ウェブ会議
	Pulse Connect Secure の脆弱性を狙った攻撃事案 *https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html*	VPN
	テレワークでの VPN 利用にセキュリティリスク--米当局が注意喚起 *https://japan.zdnet.com/article/35150877/*	VPN

月	概要	分類
3	**APT41 が複数のエクスプロイトを使用して世界中で侵入攻撃を開始** *https://www.fireeye.com/blog/jp-threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html*	VPN、 リモート アクセス

（補足）「分類」欄は、各製品やサービスの分類を記載しています。

5. 参考情報

5. 1 脆弱性情報

当該期間に公開された主な脆弱性情報は、次のサイトから確認することができます。

「Hitachi Incident Response Team（HIRT）CSIRT メモ【チェックしておきたい脆弱性情報】」

https://www.hitachi.co.jp/hirt/publications/csirt/index.html

5. 2 危険な可能性があるウェブサイト

危険な可能性があるウェブサイトの確認は、次のサイトからチェックすることができます。

自組織や、アクセス先のウェブサイトのセキュリティ対策状況を確認することができます。

株式会社セキュアブレイン「gred でチェック」

http://check.gred.jp/

株式会社　日立システムズ

〒141-8672 東京都品川区大崎 1-2-1

https://www.hitachi-systems.com/index.html

https://www.shield.ne.jp/ssrc/index.html