株式会社 日立システムズ

SSRC-TR-Vol.40

S.S.R.C. 定期
トレンドレポート
Vol.40

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.40

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

5 月に公開された Windows の「リモートデスクトップサービスにおける脆弱性 CVE-2019-0708」は、認証されていない遠隔の攻撃者が任意のコードを実行する可能性があるものです。この脆弱性は「BlueKeep」と名付けられ、2017 年に流行したランサムウエア「WannaCry」のように、脆弱な端末に感染が広がる可能性があると JPCERT/CC が注意を促しており、今後特に注意が必要です。

Windows のゼロデイ脆弱性を狙った攻撃が引き続き確認される中、macOS のゼロデイ脆弱性を狙った攻撃も確認されています。

なお、Android や Adobe 製品については、毎月行う定期的な脆弱性情報及び修正プログラムの公開において多くの情報が公開されていますが、特段目立った傾向はありませんでした。

3. 2 脅威情報

脅威情報について、メールやショートメッセージ（SMS）を用いたフィッシングや、ランサムウェアを用いた攻撃、パスワードリスト攻撃が多く見られました。

フィッシングについては、国際 SMS（国際通信網を経由した SMS の配信）の仕組みを悪用して送信元を偽り、正規の企業から届いているメッセージと同じスレッド上に偽メッセージを表示する手口が出てきているように、より巧妙な手口になっています。

ランサムウェアについては、公的機関に対する攻撃が目立っており、米国において被害を受けた自治体が、データを復号するための身代金を支払った例が 2 件（50 万ドルと約 60 万ドル）ありました。

その他、オンラインショッピングサイトに対するパスワードリスト攻撃や Google Play から悪意のある Android アプリをインストールさせて情報を窃取するなどの攻撃が多く確認されています。

3. 3 その他のサイバー攻撃に関する傾向

「北朝鮮」「中国」「ロシア」が関与していると思われる攻撃が引き続き多く確認されています。また、5 月、6 月に報道されたようにサイバー犯罪グループ（APT10）による日本に対する攻撃が引き続き確認されています。

4. トレンドレポート(2019 年第 2、第 3 四半期)

2019 年 4 月 1 日から同年 9 月 30 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

4. 2 脅威情報

(1) フィッシング

(2) ランサムウェア

(3) パスワードリスト攻撃

(4) Android に対する攻撃

(5) 仮想通貨

4. 3 その他のサイバー攻撃に関する傾向

4. 1 脆弱性情報

(1) Microsoft

前回のレポートの内容と同様、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や、実際に悪用されているか否かは不明ですが概念実証コード（PoC）が公開されているものが含まれていました。

また、5 月の「リモートデスクトップの脆弱性」や、7 月の「Windows Defender に関する脆弱性」、9 月の「IE のゼロデイ脆弱性」等、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。

月	No.	概要	備考
4	1	Microsoft Edge 及び Internet Explorer に関するゼロデイ脆弱性、セッション情報が露出する恐れ	ゼロデイ
5	1	リモートデスクトップサービスにコード実行の脆弱性（Windows XP にも異例のパッチ提供）	RDP
	2	マイクロソフト製品のゼロデイ脆弱性情報、新たに 2 件が GitHub 上で公開	ゼロデイ
	3	Windows タスクスケジューラにゼロデイ脆弱性 － 悪用に警戒を	ゼロデイ
	4	「Microsoft SharePoint」の脆弱性「CVE-2019-0604」を解説、遠隔からのコード実行が可能に	その他
6	1	Microsoft Windows リモートデスクトップのネットワークレベル認証に Windows ロックスクリーンをバイパスされる問題	RDP
	2	CERT/CC、Windows の RDP に関する脆弱性を公開 Microsoft は反論	RDP
	3	グーグル研究者が「Windows」で使われる「SymCrypt」のバグについて情報公開	その他
7	1	月例パッチで脆弱性 77 件を修正 一部でゼロデイ攻撃も	ゼロデイ
	2	「Windows Defender アプリ制御」に脆弱性 － 定例外アップデートをリリース	定例外
8	1	各社の Windows 用デバイスドライバに権限昇格の脆弱性	その他
9	1	MS、月例パッチで脆弱性 79 件を修正 － 一部でゼロデイ攻撃が発生	ゼロデイ
	2	マイクロソフト、定例外のセキュリティ更新プログラムで IE のゼロデイ脆弱性など修正	ゼロデイ、定例外

（補足）「備考」欄は、ゼロデイ脆弱性に関するものを「ゼロデイ」、RDP を悪用したものを「RDP」、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」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、これ以降に記載している内容につきましても、すべての情報を網羅しているものではありません。

(2) Apple

iOS に関する脆弱性情報の公開及びセキュリティアップデートの配信は、ほぼ毎月行われています。また、macOS の脆弱性についても以前より頻繁に公開されているとともに、ゼロデイ脆弱性を狙ったマルウェアが見つかっており注意が必要です。

月	No.	概要	備考
4	1	iOS 用 WordPress アプリのバグによりアカウントトークンが第三者に漏洩	iOS
5	1	「令和」対応の「macOS Mojave 10.14.5」「iOS 12.3」では脆弱性の修正も	macOS、iOS
	2	macOS のシンボリックリンクと NFS 共有の不具合を利用し、最新の macOS 10.14.5 Mojave でも Gatekeeper をバイパスできる脆弱性が発見される。	macOS
6	1	Apple、「AirMac」向けファームウェアを公開 － 脆弱性 8 件に対処	その他
	2	macOS にゼロデイ攻撃しかけるマルウェア見つかる	macOS、ゼロデイ
7	1	盗聴の恐れありで Apple Watch のトランシーバー機能を一時停止へ	その他
	2	Apple、「iOS 12.4」をリリース － 脆弱性 36 件を修正	iOS
	3	macOS の Timemachine においてコマンドインジェクションにより管理者権限の奪取が可能となる脆弱性（Scan Tech Report）	macOS
	4	macOS 向けにセキュリティアップデート － 脆弱性 44 件を修正	macOS
	5	Apple、Google のエンジニアに指摘された iPhone の脆弱性をいまだ修正せず	iOS
8	1	今すぐ iOS 12.4 へのアップデートを	iOS
	2	iPhone の Bluetooth をオンにしているだけで付近の人に電話番号が漏れてしまうことが判明	iOS
	3	Wi-Fi モジュールを埋め込んだ充電ケーブルで iPhone をハッキングできることを証明	その他
	4	最新 iOS アップデートで脱獄手法と脆弱性が見つかってしまう…	iOS
9	1	iPhone 11 にセキュリティの脆弱性が発覚、購入は 9 月 30 日以降がベスト？	iOS

（補足）「備考」欄は、iOS に関する脆弱性を「iOS」、macOS に関する脆弱性を「macOS」、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の多くは、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が、9 月に Google とは別の組織からゼロデイの脆弱性情報が公開されました。当該期間におけるゼロデイの脆弱性情報は 1 件のみでしたが、日頃からの情報収集及び脆弱性に対する対策が必要です。

月	No.	概要	備考
4	1	Android の 2019 年 4 月パッチが公開 –メディアフレームワークに任意コード実行の脆弱性	月例
5	1	Android の 2019 年 5 月パッチが公開 –最高深刻度は“Critical”	月例
6	1	Google、Android の月例セキュリティ情報を発表 – 2019 年 6 月版	月例
7	1	Google、Android 月例パッチ公開　深刻度「重大」9 件を含む修正　Pixel では機能強化も	月例
8	1	Google、Android の 2019 年 8 月セキュリティ情報を発表	月例
9	1	Google、Android の 2019 年 9 月セキュリティ情報を発表　～「Android 10」にも早速修正	月例
	2	Android　の未修正のゼロデイ脆弱性	ゼロデイ

（補足）「備考」欄は、月例の脆弱性情報の公開を「月例」、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

Adobe 社が公開している情報からは、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。しかしながら、月例のセキュリティ情報において多くの脆弱性が公開されており、その中には重要度の高い脆弱性が見つかっていることや、過去にはいくつかゼロデイの脆弱性が見つかっているため、日頃からの情報収集及び脆弱性に対する対策が必要です。

月	No.	概要	備考
4	1	Adobe、複数製品に対してアップデート – 「Flash Player」「Acrobat」以外のユーザーも注意を	月例
5	1	「Adobe Acrobat/Reader」に深刻な脆弱性 – 5 月 14 日にパッチを公開予定	月例
6	1	アドビ、「Flash Player」「ColdFusion」「Campaign Classic」の脆弱性を修正	月例
7	1	Adobe、月例セキュリティ情報を発表 –「Adobe Bridge CC」「AEM」などに脆弱性	月例
8	1	「Adobe Acrobat/Reader」に深刻な脆弱性 – パッチ公開は 8 月 14 日を予定	月例
9	1	Adobe、「Flash Player」で 2 件の“Critical”な脆弱性を修正	月例

4. 2 脅威情報

(1) 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(2019 年 10 月 2 日公開)によると、2019 年 4 月のフィッシング報告件数は 2,388 件であり、その後報告件数が増加し続け、2019 年 9 月は 6,218 件になっています。これらの攻撃において悪用されたブランドとしては、Amazon や LINE が特に多く、次いで Apple、楽天、マイクロソフトが多くなっています。

また、スマートフォン等のショートメッセージ(SMS)を使ったフィッシングが増加しており、特徴的なものとして、国際通信網を経由して配信する SMS の仕組みを悪用したものがあります。この仕組みを悪用することで送信元を偽ることができ、正規の企業から届いているメッセージと同じスレッド上に偽メッセージを表示し、フィッシングであることに気づきにくくなっています。

フィッシングに対する対策は、迷惑メールフィルタリング等の技術的な対策を実施することに加えて、スマートフォン等の利用者に対する周知等の対策も重要です。

月	No.	概要	備考
4	1	宅配業者の不在通知メールを装ったフィッシングメールで個人情報が流出(NHK 大阪放送局)	メール
	2	宅配偽装 SMS によるスマートフォンへの攻撃でまた新たな手口	SMS
	3	Instagram のログイン情報を盗むフィッシング詐欺 "Nasty List"	その他
5	1	正規ブラウザ拡張機能を利用するフィッシング攻撃を確認	メール
	2	日本通運を装う不審な SMS を確認、リンク先で偽警告を出したり Apple ID を窃取	SMS
6	1	「MUFG カード」利用者狙うフィッシング － 11 ドメインで展開	メール
	2	「本人認証サービス開始」などとだますフィッシング － ゆうちょ銀を偽装	メール
	3	正規サイトを改ざんして偽当選サイトへ誘導する攻撃、リダイレクト先はランダムに変化して偽警告なども表示	Web サイト
	4	元教員メルアカがフィッシングの踏み台に － 札幌医科大	メール
	5	検索サイト「Google」の広告を悪用したフィッシング詐欺にご注意ください(GMO コイン)	Web サイト
	6	「OneDrive」を悪用したフィッシング詐欺に注意、偽ログイン画面で認証情報を詐取	その他
	7	偽 NTT ドコモの SMS に注意 － 公式と同じスレッドに表示される可能性も	SMS

7	1	新種のフィッシングメール検出、今後さらに拡大の恐れ	メール
	2	ドコモを装うスミッシング －「高額料金発生」と不安煽る	SMS
	3	「カードが不正利用の可能性」と不安煽る SMS に注意 －「エポスカード」を偽装	SMS
	4	宅配業者による不在通知を装ったショートメッセージに関する相談が 459 件。前四半期の 335 件から 37%増。(IPA)	SMS
8	1	QR コードの飛び先はフィッシングサイト － MyEtherWallet 偽メール(フィッシング対策協議会)	メール
9	1	「地下鉄カードの現金返還キャンペーン」装うフィッシング － 情報詐取やマルウェア感染狙う	メール
	2	日本郵便の不在通知装うスミッシング再び －iPhone もターゲット	SMS
	3	「ビバリーホームページ」へ不正アクセス、フィッシングサイトへ誘導される事象を確認(ビバリー)	Web サイト

(補足)「備考」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。

(2) ランサムウェア

ランサムウェアを用いた攻撃は前回に引き続き、非常に多く発生しています。確認できている範囲において、個人に対する攻撃は少なく、公的機関等の組織に対する攻撃が多い傾向にあります。

ランサムウェアの被害にあった自治体(6 月に発生した米フロリダ州のリビエラ・ビーチ、及び 7 月に発生したの同州レイク・シティ)が、行政サービスを継続するために攻撃者に身代金を支払ったケースが報告されています。

ただし、6 月 28 日～7 月 1 日にハワイ州のホノルルで開催された全米市長会議において、ランサムウェアによる攻撃を受けても身代金を支払わないという決議案に 220 人を超える市長が署名したことにより、今後は攻撃を受けても身代金を支払わない傾向[1]になると思われます。

[1] 米国連邦捜査局(FBI)は、2019 年 10 月 2 日に公表した「ランサムウェアの身代金要求への対処法に関する指針」において、組織の判断によってはデータ復旧のために身代金を支払う選択肢もある、ということについて触れています。

月	No.	概要	備考
4	1	ランサムウェア「LockerGoga」、産業・製造業界で被害続出	その他（製造業）
	2	攻撃者グループ PINCHY SPIDER のパートナー、「Big Game Hunting」の手法で GandCrab ランサムウェアを拡散	その他
5	1	メール管理システムがランサムウェア感染 – 神大	大学
	2	ランサムウェア「Dharma」、不正活動を隠ぺいするために正規ソフトウェアを利用	医療等
	3	ランサムウェア攻撃を受けたボルチモア	自治体
6	1	新型ランサムウェアに感染しシステム停止　ユーロフィンジェノミクス株式会社	会社
	2	米フロリダ州リビエラ・ビーチ、ランサムウェアに屈する　身代金約 6440 万円を支払いへ	自治体
7	1	米フロリダ州レイク・シティ、ランサムウェアに屈した地方自治体が IT 担当職員を解雇−約 5400 万円支払	自治体
	2	ランサムウェア「Sodin」が日独韓台に感染集中 – カスペルスキー	その他（MSP）
	3	法医学など手がける Eurofins Scientific、ランサムウェア攻撃で身代金を支払ったとの報道	会社
	4	全米市長会議、ランサムウェア攻撃で身代金支払い拒否へ−年次総会で決議採択	自治体
	5	クラウドベースの仮想デスクトッププロバイダーiNSYNQ がランサムウェア被害	プロバイダ
8	1	Android に新しいランサムウェア、日本も標的の可能性	その他
	2	テキサス州内の 23 の政府機関がランサムウェアの被害に	自治体
	3	＜Kaspersky サイバー脅威レポート: 2019 年 4 月−6 月統計＞ランサムウェアの新たな亜種が増加、前年同期の 2 倍に	その他
	4	何百もの歯科医院がランサムウェア被害に−MSP のインフラを悪用	医療
9	1	5 億 6000 万円ものランサムウェア身代金を突っぱねて自力で問題を解決した自治体が現る	自治体
	2	数千の Linux サーバ、ランサムウェア「Lilu」に感染 – 経路は不明	その他
	3	ランサムに感染、データ損害は確認されず – シミックグループ	医療

（補足）「備考」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。

(3) パスワードリスト攻撃

フィッシング及びランサムウェアによる攻撃の他、パスワードリスト攻撃が多く確認され、攻撃対象としてオンラインショッピングサイトが多い傾向がみられました。

オンラインショッピングサイトには個人情報の他にクレジットカード情報やショッピングサイトのポイント情報が含まれていることがあり、これらの情報を窃取することを目的としたものと思われます。

月	No.	概要	備考
4	1	通販サイトへ PW リスト攻撃、遮断直後に発信国変更して継続	オンラインショップ
5	1	ユニクロ・GU の通販サイトにリスト型攻撃、不正ログイン 46 万件　氏名や住所、身体のサイズなど流出	オンラインショップ
	2	アカマイ、ストリーミングサービスが リスト型攻撃の最大の標的の一つと報告	その他
	3	パスワードリスト攻撃で一部会員情報が閲覧の可能性（コジマ）	オンラインショップ
6	1	RDP に総当たり攻撃するボット「GoldBrute」 – 試行ごとに異なる IP アドレス	その他
	2	パスワードリスト攻撃による不正ログイン、カード不正利用確認（イオン銀行、イオンクレジットサービス）	金融機関
	3	パスワードリスト攻撃で顧客アカウントに不正ログイン被害（ベビータウン）	オンラインショップ
7	1	ブックオフ会員に心当たりない PW 再設定メール – リストを用いて試行か	オンラインショップ
	2	Chatwork にパスワードリスト型攻撃確認、2 段階認証呼びかけ（Chatwork）	その他
	3	「クロネコメンバーズ」に PW リスト攻撃 – 不正ログイン 3400 件	その他
	4	和菓子店通販サイトに不正アクセス – 偽決済画面でクレカ情報詐取	オンラインショップ
8	1	決済サービス「7pay」廃止へ – 原因「PW リスト攻撃」と説明	決済サービス
	2	セシール通販サイトに PW リスト攻撃 – 試行 22 回を検知	オンラインショップ
	3	アルペンに PW リスト攻撃　攻撃者は複数店舗でポイント使用	オンラインショップ

（補足）「備考」欄は、いわゆるオンラインショッピングサイトや通販サイトと言われるサイトを「オンラインショップ」と記載しています。

(4) Android に対する攻撃

Android を搭載した機器に対する攻撃として、ユーザに悪意のあるアプリをインストールさせる方法があり、ここ数か月の間においても、Google Play 上で不正なアプリがいくつか発見されています。

アプリをインストールする際には、Google が推奨している Google Play プロテクトを使用すること、また、最新バージョンの Android を使用する、アプリをインストールする前に開発元を確認するなどの対策が必要です。

また、SMS のメッセージにリンクを記載し、リンク先から不正なアプリをダウンロードさせる手口が確認されているため注意が必要です。

月	No.	概要	備考
6	1	トレンドマイクロは 6 月中旬、111 個の不正な無料ゲームアプリおよびカメラアプリが Google Play で配布されていたことを確認した。	Google Play
7	1	2500 万台の Android 端末が感染しているマルウェア「Agent Smith」見つかる	Google Play
	2	Android 端末向けバンキングトロジャン「Anubis」が再登場、17,000 個以上の検体を確認	Google Play
	3	1000 万人以上が Samsung を装う詐欺アプリ「Updates For Samsung(サムスン用アップデート)」に引っかかっていることが判明	Google Play
8	1	Android に新しいランサムウェア、日本も標的の可能性	Google Play
	2	日本と韓国を狙った新たな Android スパイウェアを Google Play で発見	Google Play
	3	悪意あるアプリに変貌したスキャナーアプリ（CamScanner）	Google Play
9	1	フォトアプリやゲームアプリを装うアドウェアを Google Play で確認、800 万回以上ダウンロード	Google Play
	2	日本郵便の不在通知装うスミッシング再び － iPhone もターゲット	SMS

（補足）「備考」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」、SMS に記載されたサイトにて不正なアプリが配信されていたものを「SMS」と記載しています。

(5) 仮想通貨

当該期間において、仮想通貨の発掘や、仮想通貨を窃取することを目的とした攻撃が多く見られました。

仮想通貨の発掘については、攻撃対象となる機器にマルウェアを感染させ、当該機器のリソースを悪用したもの、仮想通貨の窃取については、仮想通貨の取引所に対するサイバー攻撃や仮想通貨を利用するユーザに対して攻撃を行うものでした。

月	No.	概要	備考
4	1	クリップボードを書き換えて仮想通貨を盗み出すマルウェア「Clipper（クリッパー）」	窃取
	2	人気仮想通貨ウォレット「Electrum」サイバー攻撃の標的に	窃取
	3	IoT マルウェア「Bashlite」の更新を確認、仮想通貨発掘などのバックドアコマンドを追加	発掘
5	1	Muhstik ボットネットが最新の WebLogic 脆弱性を暗号通貨マイニング、DDoS 攻撃に悪用	発掘
	2	仮想通貨取引所バイナンスでハッキング被害 約 44 億円分のビットコインが引き出される	窃取
	3	「EternalBlue」を含む複数の手法で拡散する仮想通貨発掘マルウェアを日本でも確認	発掘
	4	仮想通貨の無断マイニングを行うマルウェアが、セキュリティ脅威リスト上位を独占	発掘
	5	「CVE-2019-3396」の利用を再び確認、ルートキットと仮想通貨発掘マルウェアを拡散	発掘
	6	1-3 位をマイニングマルウェア占める-月例レポート（チェック・ポイント）	発掘
	7	北朝鮮、経済制裁に対抗するため仮想通貨取引所にサイバー攻撃を行う FBI 担当者が指摘	窃取
6	1	北朝鮮ハッカーが暗躍 韓国の仮想通貨取引所ユーザーを狙ったフィッシング詐欺を警告	窃取
	2	トレンドマイクロ、ウェブサーバーに感染し仮想通貨モネロの無断マイニングを行うマルウェアを報告	発掘
	3	8 つの脆弱性を利用し仮想通貨発掘ツールを送り込むワーム「BlackSquid」を確認	発掘
	4	仮想通貨を発掘する不正な Docker コンテナを確認、Shodan を利用して露出した API を検索	発掘
	5	仮想通貨取引所になりすまし二段階認証を突破するマルウェアが見つかる	窃取
	6	仮想通貨 Monero を発掘するマルウェア「PCASTLE」が再び中国を標的に、多層的なファイルレス活動により拡散	発掘
	7	欧州刑事警察機構（ユーロポール）、30 億円相当のビットコイン盗難事件で容疑者逮捕	窃取

7	1	仮想通貨取引所ビットゥルー(Bitrue)で 4 億円以上のハッキング、バイナンスも対策へ	窃取
	2	当社子会社における仮想通貨の不正流出に関するお知らせとお詫び（第一報）	窃取
9	1	ビットコインのライトニングネットワークで脆弱性を確認、実際に被害も	窃取

（補足）「備考」欄は、仮想通貨を発掘することを目的としたものを「発掘」、仮想通貨を窃取することを目的としたものを「窃取」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。また、日本に対する攻撃が引き続き確認されています。

月	No.	概要	備考
4	1	金融機関サイバー攻撃の犯人、断トツは北朝鮮	北朝鮮
	2	TRITON を利用する攻撃者の TTP、カスタム攻撃ツール、 検出結果、ATT&CK マッピング	ロシア
5	1	日本も狙う「APT10」にあらたな動き － 一見問題ない実行ファイルから攻撃展開	中国
	2	北朝鮮、経済制裁に対抗するため仮想通貨取引所にサイバー攻撃を行う FBI 担当者が指摘	北朝鮮
	3	北朝鮮ハッカーが暗躍 韓国の仮想通貨取引所ユーザーを狙ったフィッシング詐欺を警告	北朝鮮
6	1	台湾人兄弟、日米最新ミサイルや F35 戦闘機などの情報盗む 中国スパイ＝FBI	中国
	2	在ロシア EU 大使館、サイバー攻撃受け情報漏洩との報道 ロシアが関与か	ロシア
	3	豪州国立大、19年間ハッキング被害 中国を疑う声も	中国
	4	中国ハッカー、世界の通信大手にサイバー攻撃か	中国
	5	中国、富士通やNTTデータにも不正侵入 大規模サイバー攻撃	中国
7	1	ロシア企業が関与のモバイル監視マルウェア「Monokle」、セキュリティ企業が報告	ロシア
8	1	＜Kaspersky APT レポート: 2019 年第 2 四半期＞乗っ取りや虚偽情報の拡散などの APT 攻撃が中東で発生	その他
	2	APT41：スパイ活動とサイバー犯罪の両方を遂行する双頭龍の攻撃者	中国
	3	北朝鮮のサイバー攻撃による被害 韓国が最多＝国連報告書	北朝鮮
	4	中国のハッカー、がん研究機関を標的に--FireEye 報告書	中国
9	1	北朝鮮関与「HIDDEN COBRA」のツールに新亜種 － 米政府が情報公開	北朝鮮
	2	iOS・Android の脆弱性を突いてスパイウェアを送り込むハッキングが発覚、犯行グループの背景には中国政府の可能性	中国
	3	北朝鮮に所属するハッカーグループ、インドの ATM をターゲットにしたマルウェア開発	北朝鮮

（補足）「備考」欄は、関与が疑われている国家を記載しています。

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/

6. 出典元

6.1 脆弱性情報

(1) 4.1(1) Microsoft の脆弱性情報

月	No.	概要及び出典元 URL
4	1	*Microsoft Edge 及び Internet Explorer に関するゼロデイ脆弱性、セッション情報が露出する恐れ* *https://blog.trendmicro.co.jp/archives/20774*
5	1	*リモートデスクトップサービスにコード実行の脆弱性（Windows XP にも異例のパッチ提供）* *https://forest.watch.impress.co.jp/docs/news/1184520.html*
	2	*マイクロソフト製品のゼロデイ脆弱性情報、新たに 2 件が GitHub 上で公開* *https://japan.zdnet.com/article/35137367/*
	3	*Windows タスクスケジューラにゼロデイ脆弱性 － 悪用に警戒を* *http://www.security-next.com/105104*
	4	*「Microsoft SharePoint」の脆弱性「CVE-2019-0604」を解説、遠隔からのコード実行が可能に* *https://blog.trendmicro.co.jp/archives/21297*
6	1	*Microsoft Windows リモートデスクトップのネットワークレベル認証に Windows ロックスクリーンをバイパスされる問題* *https://jvn.jp/vu/JVNVU94741708/*
	2	*CERT/CC、Windows の RDP に関する脆弱性を公開 Microsoft は反論* *https://www.itmedia.co.jp/enterprise/articles/1906/07/news076.html*
	3	*グーグル研究者が「Windows」で使われる「SymCrypt」のバグについて情報公開* *https://japan.zdnet.com/article/35138431/*
7	1	*月例パッチで脆弱性 77 件を修正 一部でゼロデイ攻撃も* *http://www.security-next.com/106392*
	2	*「Windows Defender アプリ制御」に脆弱性 － 定例外アップデートをリリース* *http://www.security-next.com/106590*
8	1	*各社の Windows 用デバイスドライバに権限昇格の脆弱性* *https://pc.watch.impress.co.jp/docs/news/1201475.html*
9	1	*MS、月例パッチで脆弱性 79 件を修正 － 一部でゼロデイ攻撃が発生* *http://www.security-next.com/108078/2*
	2	*マイクロソフト、定例外のセキュリティ更新プログラムで IE のゼロデイ脆弱性など修正* *https://japan.zdnet.com/article/35142978/*

(2) 4.1(2) Apple の脆弱性情報

月	No.	概要及び出典元 URL
4	1	*iOS 用 WordPress アプリのバグによりアカウントトークンが第三者に漏洩* *https://jp.techcrunch.com/2019/04/03/2019-04-02-wordpress-bug-account-tokens/*
5	1	*「令和」対応の「macOS Mojave 10.14.5」「iOS 12.3」では脆弱性の修正も* *https://forest.watch.impress.co.jp/docs/news/1184513.html*
	2	*macOS のシンボリックリンクと NFS 共有の不具合を利用し、最新の macOS 10.14.5 Mojave でも Gatekeeper をバイパスできる脆弱性が発見される。* *https://applech2.com/archives/20190526-symbolic-links-and-nfs-share-bypass-macos-10-14-5-mojave-gatekeeper.html*
6	1	*Apple、「AirMac」向けファームウェアを公開 － 脆弱性 8 件に対処* *http://www.security-next.com/105912*
	2	*macOS にゼロデイ攻撃しかけるマルウェア見つかる* *http://www.security-next.com/106055*
7	1	*盗聴の恐れありで Apple Watch のトランシーバー機能を一時停止へ* *https://jp.techcrunch.com/2019/07/11/2019-07-10-apple-disables-walkie-talkie-app-due-to-vulnerability-that-could-allow-iphone-eavesdropping/*
	2	*Apple、「iOS 12.4」をリリース － 脆弱性 36 件を修正* *http://www.security-next.com/106711*
	3	*macOS の Timemachine においてコマンドインジェクションにより管理者権限の奪取が可能となる脆弱性（Scan Tech Report）* *https://scan.netsecurity.ne.jp/article/2019/07/23/42679.html*
	4	*macOS 向けにセキュリティアップデート － 脆弱性 44 件を修正* *http://www.security-next.com/106788*
	5	*Apple、Google のエンジニアに指摘された iPhone の脆弱性をいまだ修正せず* *https://jp.ubergizmo.com/2019/07/31/10706/*
8	1	*今すぐ iOS 12.4 へのアップデートを* *https://blog.kaspersky.co.jp/ios-critical-vulnerabilities-124/23807/*
	2	*iPhone の Bluetooth をオンにしているだけで付近の人に電話番号が漏れてしまうことが判明* *https://gigazine.net/news/20190801-iphone-bluetooth-leaks-phone-numbers/*
	3	*Wi-Fi モジュールを埋め込んだ充電ケーブルで iPhone をハッキングできることを証明* *https://jp.techcrunch.com/2019/08/13/2019-08-12-iphone-charging-cable-hack-computer-def-con/*
	4	*最新 iOS アップデートで脱獄手法と脆弱性が見つかってしまう…* *https://www.gizmodo.jp/2019/08/ios-update-jailbreak.html*
9	1	*iPhone 11 にセキュリティの脆弱性が発覚、購入は 9 月 30 日以降がベスト？* *https://realsound.jp/tech/2019/09/post-416747.html*

(3) 4.1(3) Android の脆弱性情報

月	No.	概要及び出典元 URL
4	1	*Android の 2019 年 4 月パッチが公開 -メディアフレームワークに任意コード実行の脆弱性* *https://forest.watch.impress.co.jp/docs/news/1177723.html*
5	1	*Android の 2019 年 5 月パッチが公開 -最高深刻度は"Critical"* *https://forest.watch.impress.co.jp/docs/news/1183501.html*
6	1	*Google、Android の月例セキュリティ情報を発表 -2019 年 6 月版* *https://forest.watch.impress.co.jp/docs/news/1188176.html*
7	1	*Google、Android 月例パッチ公開 深刻度「重大」9 件を含む修正 Pixel では機能強化も* *https://www.itmedia.co.jp/mobile/articles/1907/02/news065.html*
8	1	*Google、Android の 2019 年 8 月セキュリティ情報を発表* *https://forest.watch.impress.co.jp/docs/news/1200261.html*
9	1	*Google、Android の 2019 年 9 月セキュリティ情報を発表 ～「Android 10」にも早速修正* *https://www.itmedia.co.jp/mobile/articles/1907/02/news065.html*
	2	*Android の未修正のゼロデイ脆弱性* *https://www.watchguard.co.jp/security-news/unpatched-0-day-android-vulnerability.html*

(4) 4.1(4) Adobe の脆弱性情報

月	No.	概要及び出典元 URL
4	1	*Adobe、複数製品に対してアップデート - 「Flash Player」「Acrobat」以外のユーザーも注意を* *http://www.security-next.com/104108*
5	1	*「Adobe Acrobat/Reader」に深刻な脆弱性 - 5 月 14 日にパッチを公開予定* *http://www.security-next.com/104734*
6	1	*アドビ、「Flash Player」「ColdFusion」「Campaign Classic」の脆弱性を修正* *https://japan.zdnet.com/article/35138401/*
7	1	*Adobe、月例セキュリティ情報を発表 -「Adobe Bridge CC」「AEM」などに脆弱性* *https://forest.watch.impress.co.jp/docs/news/1195189.html*
8	1	*「Adobe Acrobat/Reader」に深刻な脆弱性 - パッチ公開は 8 月 14 日を予定* *http://www.security-next.com/096697*
9	1	*Adobe、「Flash Player」で 2 件の"Critical"な脆弱性を修正* *https://forest.watch.impress.co.jp/docs/news/1206557.html*

6. 2 脅威情報

(1) 4.2(1) フィッシングの情報

月	No.	概要及び出典元 URL
4	1	*宅配業者の不在通知メールを装ったフィッシングメールで個人情報が流出（NHK 大阪放送局）* *https://scan.netsecurity.ne.jp/article/2019/04/16/42223.html*
	2	*宅配偽装 SMS によるスマートフォンへの攻撃でまた新たな手口* *https://blog.trendmicro.co.jp/archives/20953*
	3	*Instagram のログイン情報を盗むフィッシング詐欺 "Nasty List"* *https://blogs.mcafee.jp/instagram-nasty-list*
5	1	*正規ブラウザ拡張機能を利用するフィッシング攻撃を確認* *https://blog.trendmicro.co.jp/archives/21077*
	2	*日本通運を装う不審な SMS を確認、リンク先で偽警告を出したり Apple ID を窃取* *https://internet.watch.impress.co.jp/docs/news/1185876.html*
6	1	*「MUFG カード」利用者狙うフィッシング － 11 ドメインで展開* *http://www.security-next.com/105455*
	2	*「本人認証サービス開始」などとだますフィッシング － ゆうちょ銀を偽装* *http://www.security-next.com/105502*
	3	*正規サイトを改ざんして偽当選サイトへ誘導する攻撃、リダイレクト先はランダムに変化して偽警告なども表示* *https://internet.watch.impress.co.jp/docs/news/1190567.html*
	4	*元教員メルアカがフィッシングの踏み台に － 札幌医科大* *http://web.sapmed.ac.jp/jp/news/press/jmjbbn000000fmdy.html*
	5	*検索サイト「Google」の広告を悪用したフィッシング詐欺にご注意ください（GMO コイン）* *https://coin.z.com/jp/news/2019/06/1777/*
	6	*「OneDrive」を悪用したフィッシング詐欺に注意、偽ログイン画面で認証情報を詐取* *https://internet.watch.impress.co.jp/docs/news/1193011.html*
	7	*偽 NTT ドコモの SMS に注意 － 公式と同じスレッドに表示される可能性も* *http://www.security-next.com/105839*
7	1	*新種のフィッシングメール検出、今後さらに拡大の恐れ* *https://news.mynavi.jp/article/20190722-863409/*
	2	*ドコモを装うスミッシング －「高額料金発生」と不安煽る* *http://www.security-next.com/106850*
	3	*「カードが不正利用の可能性」と不安煽る SMS に注意 －「エポスカード」を偽装* *http://www.security-next.com/106359*
	4	*宅配業者による不在通知を装ったショートメッセージに関する相談が 459 件。前四半期の 335 件から 37%増。（IPA）* *http://www.security-next.com/106753*
8	1	*QR コードの飛び先はフィッシングサイト －MyEtherWallet 偽メール（フィッシング対策協議会）* *https://scan.netsecurity.ne.jp/article/2019/08/14/42780.html*
9	1	*「地下鉄カードの現金返還キャンペーン」装うフィッシング － 情報詐取やマルウェア感染狙う* *http://www.security-next.com/107797*
	2	*日本郵便の不在通知装うスミッシング再び －iPhone もターゲット* *http://www.security-next.com/107856*
	3	*「ビバリーホームページ」へ不正アクセス、フィッシングサイトへ誘導される事象を確認（ビバリー）* *https://scan.netsecurity.ne.jp/article/2019/09/11/42915.html*

(2) 4.2(2) ランサムウェアの情報

月	No.	概要及び出典元 URL
4	1	ランサムウェア「LockerGoga」、産業・製造業界で被害続出 https://www.itmedia.co.jp/enterprise/articles/1904/02/news076.html
	2	攻撃者グループ PINCHY SPIDER のパートナー、「Big Game Hunting」の手法で GandCrab ランサムウェアを拡散 https://scan.netsecurity.ne.jp/article/2019/04/04/42180.html
5	1	メール管理システムがランサムウェア感染 - 神大 http://www.security-next.com/104620
	2	ランサムウェア「Dharma」、不正活動を隠ぺいするために正規ソフトウェアを利用 https://blog.trendmicro.co.jp/archives/21215
	3	ランサムウェア攻撃を受けたボルチモア https://blog.kaspersky.co.jp/baltimore-encrypted/23343/
6	1	新型ランサムウェアに感染しシステム停止　ユーロフィンジェノミクス株式会社 https://cybersecurity-jp.com/news/31910
	2	米フロリダ州リビエラ・ビーチ、ランサムウェアに屈する　身代金約 6440 万円を支払いへ https://japan.zdnet.com/article/35138825/
7	1	米フロリダ州レイク・シティ、ランサムウェアに屈した地方自治体が IT 担当職員を解雇-約 5400 万円支払 https://japan.zdnet.com/article/35139315/
	2	ランサムウェア「Sodin」が日独韓台に感染集中 - カスペルスキー https://japan.zdnet.com/article/35139470/
	3	法医学など手がける Eurofins Scientific、ランサムウェア攻撃で身代金を支払ったとの報道 https://japan.zdnet.com/article/35139584/
	4	全米市長会議、ランサムウェア攻撃で身代金支払い拒否へ-年次総会で決議採択 https://japan.zdnet.com/article/35139937/
	5	クラウドベースの仮想デスクトッププロバイダーiNSYNQ がランサムウェア被害 https://japan.zdnet.com/article/35140244/
8	1	Android に新しいランサムウェア、日本も標的の可能性 https://news.mynavi.jp/article/20190801-869221/
	2	テキサス州内の 23 の政府機関がランサムウェアの被害に https://japan.zdnet.com/article/35141403/
	3	<Kaspersky サイバー脅威レポート: 2019 年 4 月-6 月統計>ランサムウェアの新たな亜種が増加、前年同期の 2 倍に https://www.kaspersky.co.jp/about/press-releases/2019_vir29082019
	4	何百もの歯科医院がランサムウェア被害に-MSP のインフラを悪用 https://japan.zdnet.com/article/35141974/
9	1	5 億 6000 万円ものランサムウェア身代金を突っぱねて自力で問題を解決した自治体が現る https://gigazine.net/news/20190906-us-city-reject-ransom-demand/
	2	数千の Linux サーバ、ランサムウェア「Lilu」に感染 - 経路は不明 https://news.mynavi.jp/article/20190910-891436/
	3	ランサムに感染、データ損害は確認されず - シミックグループ http://www.security-next.com/108204

(3) 4.2(3) パスワードリスト攻撃の情報

月	No.	概要
4	1	*通販サイトへ PW リスト攻撃、遮断直後に発信国変更して継続* *http://www.security-next.com/103948*
5	1	*ユニクロ・GU の通販サイトにリスト型攻撃、不正ログイン 46 万件　氏名や住所、身体のサイズなど流出* *https://www.itmedia.co.jp/news/articles/1905/14/news059.html*
	2	*アカマイ、ストリーミングサービスが リスト型攻撃の最大の標的の一つと報告* *https://webtan.impress.co.jp/n/2019/05/23/32755*
	3	*パスワードリスト攻撃で一部会員情報が閲覧の可能性（コジマ）* *https://scan.netsecurity.ne.jp/article/2019/05/27/42379.html*
6	1	*RDP に総当たり攻撃するボット「GoldBrute」 - 試行ごとに異なる IP アドレス* *http://www.security-next.com/105545*
	2	*パスワードリスト攻撃による不正ログイン、カード不正利用確認（イオン銀行、イオンクレジットサービス）* *https://scan.netsecurity.ne.jp/article/2019/06/17/42485.html*
	3	*パスワードリスト攻撃で顧客アカウントに不正ログイン被害（ベビータウン）* *https://cybersecurity-jp.com/news/31784*
7	1	*ブックオフ会員に心当たりない PW 再設定メール - リストを用いて試行か* *http://www.security-next.com/106759*
	2	*Chatwork にパスワードリスト型攻撃確認、2 段階認証呼びかけ（Chatwork）* *https://scan.netsecurity.ne.jp/article/2019/07/23/42677.html*
	3	*「クロネコメンバーズ」に PW リスト攻撃 - 不正ログイン 3400 件* *http://www.security-next.com/106808*
	4	*和菓子店通販サイトに不正アクセス - 偽決済画面でクレカ情報詐取* *http://www.security-next.com/106716*
8	1	*決済サービス「7pay」廃止へ - 原因「PW リスト攻撃」と説明* *http://www.security-next.com/107030*
	2	*セシール通販サイトに PW リスト攻撃 - 試行 22 回を検知* *http://www.security-next.com/107062*
	3	*アルペンに PW リスト攻撃 攻撃者は複数店舗でポイント使用* *http://www.security-next.com/107219*

(4) 4.2(4) Android に対する攻撃の情報

月	No.	概要
6	1	トレンドマイクロは 6 月中旬、111 個の不正な無料ゲームアプリおよびカメラアプリが Google Play で配布されていたことを確認した。 https://blog.trendmicro.co.jp/archives/21844
7	1	2500 万台の Android 端末が感染しているマルウェア「Agent Smith」見つかる https://gigazine.net/news/20190712-mobile-malware-agent-smith/
	2	Android 端末向けバンキングトロジャン「Anubis」が再登場、17,000 個以上の検体を確認 https://security.srad.jp/story/19/09/27/1411246/
	3	1000 万人以上が Samsung を装う詐欺アプリ「Updates For Samsung(サムスン用アップデート)」に引っかかっていることが判明 https://blog.trendmicro.co.jp/archives/21900
8	1	Android に新しいランサムウェア、日本も標的の可能性 https://news.mynavi.jp/article/20190801-869221/
	2	日本と韓国を狙った新たな Android スパイウェアを Google Play で発見 https://blogs.mcafee.jp/new-android-malware-google-play
	3	悪意あるアプリに変貌したスキャナーアプリ(CamScanner) https://blog.kaspersky.co.jp/camscanner-malicious-android-app/23979/
9	1	フォトアプリやゲームアプリを装うアドウェアを Google Play で確認、800 万回以上ダウンロード https://blog.trendmicro.co.jp/archives/22313
	2	日本郵便の不在通知装うスミッシング再び - iPhone もターゲット http://www.security-next.com/107856

(5) 4.2(5) 仮想通貨の情報

月	No.	概要
4	1	クリップボードを書き換えて仮想通貨を盗み出すマルウェア「Clipper(クリッパー)」 https://eset-info.canon-its.jp/malware_info/special/detail/190402.html
	2	人気仮想通貨ウォレット「Electrum」サイバー攻撃の標的に https://coinotaku.com/news/articles/34224
	3	IoT マルウェア「Bashlite」の更新を確認、仮想通貨発掘などのバックドアコマンドを追加 https://blog.trendmicro.co.jp/archives/20879
5	1	Muhstik ボットネットが最新の WebLogic 脆弱性を暗号通貨マイニング、DDoS 攻撃に悪用 https://www.paloaltonetworks.jp/company/in-the-news/2019/muhstik-botnet-exploits-the-latest-weblogic-vulnerability-for-cryptomining-and-ddos-attacks
	2	仮想通貨取引所バイナンスでハッキング被害 約 44 億円分のビットコインが引き出される https://jp.cointelegraph.com/news/binance-discovered-a-large-scale-security-breach
	3	「EternalBlue」を含む複数の手法で拡散する仮想通貨発掘マルウェアを日本でも確認 https://blog.trendmicro.co.jp/archives/21051
	4	仮想通貨の無断マイニングを行うマルウェアが、セキュリティ脅威リスト上位を独占 https://jp.cointelegraph.com/news/crypto-miners-dominate-top-10-list-of-most-prolific-malware-threats
	5	「CVE-2019-3396」の利用を再び確認、ルートキットと仮想通貨発掘マルウェアを拡散 https://blog.trendmicro.co.jp/archives/21314
	6	1-3 位をマイニングマルウェア占める-月例レポート(チェック・ポイント) https://www.excite.co.jp/news/article/Scannetsecurity_42374/
	7	北朝鮮、経済制裁に対抗するため仮想通貨取引所にサイバー攻撃を行う FBI 担当者が指摘 https://jp.cointelegraph.com/news/north-korea-launched-cryptocurrency-attacks-in-response-to-sanctions-says-fbi

6	1	*北朝鮮ハッカーが暗躍 韓国の仮想通貨取引所ユーザーを狙ったフィッシング詐欺を警告* *https://jp.cointelegraph.com/news/upbit-exchange-phishing-email-scam-came-from-north-korea-source-claims*
	2	*トレンドマイクロ、ウェブサーバーに感染し仮想通貨モネロの無断マイニングを行うマルウェアを報告* *https://jp.cointelegraph.com/news/trend-micro-blacksquid-malware-infects-servers-to-install-monero-cryptojacking-software*
	3	*8 つの脆弱性を利用し仮想通貨発掘ツールを送り込むワーム「BlackSquid」を確認* *https://blog.trendmicro.co.jp/archives/21521*
	4	*仮想通貨を発掘する不正な Docker コンテナを確認、Shodan を利用して露出した API を検索* *https://blog.trendmicro.co.jp/archives/21525*
	5	*仮想通貨取引所になりすまし二段階認証を突破するマルウェアが見つかる* *https://apptimes.net/archives/25626*
	6	*仮想通貨 Monero を発掘するマルウェア「PCASTLE」が再び中国を標的に、多層的なファイルレス活動により拡散* *https://blog.trendmicro.co.jp/archives/21642*
	7	*欧州刑事警察機構（ユーロポール）、30 億円相当のビットコイン盗難事件で容疑者逮捕* *https://coinpost.jp/?p=91973*
7	1	*仮想通貨取引所ビットゥルー(Bitrue)で 4 億円以上のハッキング、バイナンスも対策へ* *https://coinchoice.net/bitrue-attacked-lost-over-400million-binance-took-action_201907*
	2	*当社子会社における仮想通貨の不正流出に関するお知らせとお詫び（第一報）* *https://www.release.tdnet.info/inbs/140120190712471249.pdf*
9	1	*ビットコインのライトニングネットワークで脆弱性を確認、実際に被害も* *https://jp.cointelegraph.com/news/lightning-labs-cto-confirms-ln-vulnerabilities-exploited-in-the-wild*

6．3 その他のサイバー攻撃に関する動向

（1） 4.3(1) 国家の関与が疑われている攻撃の情報

月	No.	概要
4	1	*金融機関サイバー攻撃の犯人、断トツは北朝鮮* *http://jbpress.ismedia.jp/articles/-/55943*
	2	*TRITON を利用する攻撃者の TTP、カスタム攻撃ツール、 検出結果、ATT&CK マッピング* *https://www.fireeye.com/blog/jp-threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html*
5	1	*日本も狙う「APT10」にあらたな動き － 一見問題ない実行ファイルから攻撃展開* *http://www.security-next.com/105283*
	2	*北朝鮮、経済制裁に対抗するため仮想通貨取引所にサイバー攻撃を行う FBI 担当者が指摘* *https://jp.cointelegraph.com/news/north-korea-launched-cryptocurrency-attacks-in-response-to-sanctions-says-fbi*
	3	*北朝鮮ハッカーが暗躍 韓国の仮想通貨取引所ユーザーを狙ったフィッシング詐欺を警告* *https://jp.cointelegraph.com/news/upbit-exchange-phishing-email-scam-came-from-north-korea-source-claims*
6	1	*台湾人兄弟、日米最新ミサイルや F35 戦闘機などの情報盗む 中国スパイ＝FBI* *https://www.excite.co.jp/news/article/EpochTimes_43641/*
	2	*在ロシア EU 大使館、サイバー攻撃受け情報漏洩との報道 ロシアが関与か* *https://www.zaikei.co.jp/article/20190612/515432.html*
	3	*豪州国立大、19年間ハッキング被害 中国を疑う声も* *https://www.asahi.com/articles/ASM645X1WM64UHBI03D.html*

	4	中国ハッカー、世界の通信大手にサイバー攻撃か https://jp.wsj.com/articles/SB12120469692213223839204585386420879216614
	5	中国、富士通やNTTデータにも不正侵入 大規模サイバー攻撃 https://jp.reuters.com/article/china-cyber-cloudhopper-companies-idJPKCN1TR2I2
7	1	ロシア企業が関与のモバイル監視マルウェア「Monokle」、セキュリティ企業が報告 https://japan.zdnet.com/article/35140374/
8	1	<Kaspersky APT レポート: 2019 年第 2 四半期>乗っ取りや虚偽情報の拡散などの APT 攻撃が中東で発生 https://www.kaspersky.co.jp/about/press-releases/2019_vir08082019
	2	APT41：スパイ活動とサイバー犯罪の両方を遂行する双頭龍の攻撃者 https://www.fireeye.com/blog/jp-threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
	3	北朝鮮のサイバー攻撃による被害 韓国が最多＝国連報告書 https://news.goo.ne.jp/article/yonhap/world/yonhap-20190813wow005.html
	4	中国のハッカー、がん研究機関を標的に--FireEye 報告書 https://japan.zdnet.com/article/35141754/
9	1	北朝鮮関与「HIDDEN COBRA」のツールに新亜種 - 米政府が情報公開 http://www.security-next.com/108040
	2	iOS・Android の脆弱性を突いてスパイウェアを送り込むハッキングが発覚、犯行グループの背景には中国政府の可能性 https://gigazine.net/news/20190925-poison-carp-hacked-tibet/
	3	北朝鮮に所属するハッカーグループ、インドの ATM をターゲットにしたマルウェア開発 https://security.srad.jp/story/19/09/27/1411246/

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