ランサムウェア感染 対応項目(案) ～ファイル暗号化～

Rev.20160906

※調査対象の機器にUSB機器などを接続した場合、接続したUSB機器内のファイルも暗号化される危険性があります。インシデント・レスポンスツールなどを配置したUSB機器を接続する場合は注意してください。

※ウイルス対策ソフトによっては、脅迫文のファイルを削除するケースがあります。感染元の端末をファイルの所有者情報から特定する事が困難になる場合がありますので注意してください。(支払い先の情報なども失われます)

	項目	対象	内容	補足
1		感染機器の特定(クライアント)	①ランサムウェアに感染した機器では、一般的にファイルが暗号化された後、ビットコイン等の支払いを要求する画像やファイルが生成され表示されます。その様な脅迫文が表示されている、または脅迫文のファイルが作成されているクライアント機器はネットワークから隔離します。 ②ランサムウェアが異常終了した場合などでは、一部ファイルが暗号化された後、脅迫文のファイルの作成や画像の表示が行われない場合があります。 ③ランサムウェアによっては、一定時間が経過する毎にファイルを削除するタイプも存在します。(感染機器を隔離した場合に、電源ONの状態ではファイルが削除される危険性があります) ④ランサムウェアによっては、遅延実行(ランダムな時間で実行を遅らせる)タイプも存在します。(実行を遅延させる事により、原因特定を困難にする目的が想定されます)	①マイドキュメントにある文書ファイルなどが正常に読める事を確認します。 ②正常にファイルを開いて読む事ができない場合には、感染の疑いがあります。 ③ランサムウェアにより作成された脅迫文(振り込み方法などを記した文書ファイル)がデスクトップ等に置かれていないかを確認します。(ランサムウェアの種類が特定でき、生成される脅迫文ファイルの名前が特定できている場合は、一致するファイル名を検索し有無を確認します) 参考URL: 暗号化型ランサムウェアの新種「JIGSAW」が仕掛ける悪質なゲーム http://blog.trendmicro.co.jp/archives/13258 CryptXXX: New Ransomware From the Actors Behind Reveton, Dropping Via Angler https://www.proofpoint.com/jp/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler
2		感染機器の特定(サーバ)	①ファイルサーバ等において、共有フォルダ内のファイルが暗号化、脅迫文のメッセージファイルが作成されている場合は、作成された脅迫文ファイルのプロパティにて所有者情報を確認し、どのユーザーによってファイルが作成されたか確認します。 **[重要]所有者** 共有フォルダ内に脅迫文ファイルを作成したアカウントが、(共有を提供しているサーバ側の)ローカルのAdministratorsグループに所属するユーザーの場合、ファイルの「現在の所有者」はAdministratorsとなり、感染したユーザーアカウントを特定できない場合があります。 Administratorsグループに含まれているアカウントが利用している機器を確認すると共に、セキュリティログなどでユーザーを追跡する必要があります。 ②共有フォルダ内のファイルを暗号化したユーザーが特定できた場合は、該当ユーザーが利用している機器がランサムウェアに感染している可能性が高い為、該当機器をネットワークから隔離します。 ③共有フォルダ内のファイルをどのユーザーが暗号化したか特定できない場合は、被害拡大を防ぐ為、一時的に共有を読み取り専用にすると共に、共有フォルダに対するアクセスログなどから感染機器の特定を行います。	①ファイルサーバ自体がランサムウェアに感染していないか、共有フォルダ“以外”に存在するファイルが暗号化されているか、脅迫文が置かれていないかを確認します。
3		感染機器の特定(Webサーバ)	①Webサーバのコンテンツが暗号化され、Webサイトへアクセスすると脅迫文が表示されるケースでは、影響を受けているコンテンツと範囲を特定します。(バックアップまたは正規のファイルとハッシュ値などを用いて比較を行います) ②データベースを利用している場合、データベース内に保存されているデータが暗号化されていないか影響が無い事を確認します。	参考URL: CTB-Locker for Websites: Reinventing an old Ransomware http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/

Copyright © LAC Co., Ltd. All Rights Reserved.

	項目	対象	内容	補足
4	特定	ランサムウェアの種類特定	①ランサムウェアにより作成された脅迫文やお金の支払いに関連したファイルが存在する場合、該当ファイル名や文面を検索エンジン等で検索し、感染したランサムウェアの種類を推測します。 例）CryptWallに感染した場合には以下のようなファイルが作成され、お金の支払い方法などが記載されています。 HELP_DECRYPT.HTML HELP_DECRYPT.PNG HELP_DECRYPT.TXT ②ランサムウェアの種類によっては、ファイル名や拡張子を .vvv や .xxx など特徴のある文字列パターンに変更する場合があります。脅迫文やお金の支払いに関連したファイルと共に、拡張子が変更されている場合は、それらの文字列を元に検索エンジン等で検索し、感染したランサムウェアの種類を推測します。（ランサムウェアによってはファイル名もランダムに変更する場合があります） ③ランサムウェアによっては、別のランサムウェアの振りをするケースがあります。例えば拡張子 .locky を利用し、脅迫文も Locky と同じ文面を利用しつつも、ランサムウェア自体はPowerWareという種類のランサムウェアである場合があります。 ③ID Ransomwareサイトに脅迫文などのファイルをアップロードする事で、感染したランサムウェアの種類と、支払い以外の復号方法の有無を確認が可能。 ※アップロードするサンプルファイルにおける機密情報の取り扱いには十分注意してください。 https://id-ransomware.malwarehunterteam.com/ ④CRYPTO SHERIFFサイトに脅迫文などのファイルをアップロードする事で、感染したランサムウェアの種類と、支払い以外の復号方法の有無を確認が可能。 ※アップロードするサンプルファイルにおける機密情報の取り扱いには十分注意してください。 https://www.nomoreransom.org/crypto-sheriff.php	①Google等の検索エンジンで「ransomware <拡張子文字列>」などを検索すると、ランサムウェアの除去ツールの紹介記事などが多数ヒットします。ツールによってはAdwareなどを含むケースがある為、検索結果に表示されるツールをむやみにダウンロードやインストールせず、ウイルス対策ソフトベンダの記事など信頼のおけるソースの情報を確認します。 ②スパムメールなどでランサムウェアが拡散されている場合は、「Yahooリアルタイム検索」などで特徴的な文字列（拡張子など）を検索する事で参考情報を得られる場合があります。 参考URL： Version 4.0 of ransomware Cryptowall released, now encrypts file names http://www.scmagazine.com/version-40-of-ransomware-cryptowall-released-now-encrypts-file-names/article/452036/ PowerWare Ransomware Spoofing Locky Malware Family http://researchcenter.paloaltonetworks.com/2016/07/unit42-powerware-ransomware-spoofing-locky-malware-family/
5			①ランサムウェアの種類によっては、レジストリに特徴的なキーを作成する場合があります。感染が疑われるランサムウェアが、レジストリに特徴的なキーを作成しないかを確認し、該当するレジストリキーが作成されていないかを確認します。	参考URL The Locky Ransomware Encrypts Local Files and Unmapped Network Shares http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
6			①ランサムウェアの種類によっては、MBR を書き換える事で、ディスク全体へのアクセスをブロックする場合があります。	参考URL: 新暗号型ランサムウェア「PETYA」、MBRを上書きしてPCへのアクセス不能に http://blog.trendmicro.co.jp/archives/13106
7			①ランサムウェアの検体が特定できている場合は、該当ファイルのハッシュ値（MD5等）を確認します。 ②該当ファイルのハッシュ値を VirusTotal で検索し、各種ウイルス対策ソフトでの検出名を確認します。 ③ウイルス対策ソフトでの検知名を確認できた場合は、該当検知名を検索エンジン等で検索し、感染したランサムウェアの種類を推測します。 ④ランサムウェアによっては、ハッシュ値による検知を逃れる為に、数秒毎にダウンロードされるプログラムのハッシュ値を変更している場合があります。 VirusTotal ： https://www.virustotal.com/ja/	①検体を直接 VirusTotal にアップロードする場合は、検体内に機密情報が含まれていないか、アップロード操作にセキュリティポリシー上の問題が無いか確認後、アップロードを行います。 ②すでに解析結果が存在する場合は、そのまま情報を参照できますが、前回の解析から時間が経過している場合は再解析する事で最新の検知状況を確認する事が出来ます。 参考URL: CERBER: ANALYZING A RANSOMWARE ATTACK METHODOLOGY TO ENABLE PROTECTION https://www.fireeye.com/blog/threat-research/2016/07/cerber-ransomware-attack.html

Copyright © LAC Co., Ltd. All Rights Reserved.

	項目	対象	内容	補足
8		ランサムウェアの検体特定	①ファイルの暗号化処理後、自動的に実行ファイルを削除（自己消滅）するタイプが存在します。この為、自己消滅したランサムウェアについては、削除ファイルのデータ領域が上書きされる前にファイルの復元処理を実施しない限り検体を取得する事が困難になります。 ②ランサムウェアが自動実行に登録された場合は、Autorunsツールなどを利用する事で検体を確認する事が可能です。 [重要]検体の扱い ランサムウェアの実行ファイルを発見した場合は、パスワード付与した圧縮ファイル(ZIP)に固め、ウイルス対策ソフトベンダへ提供してパターン作成を依頼してください。	例）CryptWallマルウェアの簡易特定方法（実行ファイルを探す例） C:¥<ランダム英数字文字列>¥<ランダム英数字文字列>.exe C:¥Users¥<ユーザ名>¥Appdata¥Roaming¥<ランダム英数字文字列>.exe C:¥Users¥<ユーザ名>¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup¥<ランダム英数字文字列>.exe ※マルウェアは複数個所に作成されます。 ■例: C:¥d2429bdf¥d2429bdf.exe C:¥Users¥<ユーザ名>¥Appdata¥Roaming¥d2429bdf.exe C:¥Users¥<ユーザ名>¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup¥d2429bdf.exe
9			①ウォッチドッグ（監視）機能が存在するランサムウェでは、ランサムウェアのプログラムが異常停止した場合などにおいて、ランサムウェアを再起動し暗号化を再開する場合があります。	参考URL: 暗号化型ランサムウェア「CryptXXX」、「CRYPTESLA」の後継となるか http://blog.trendmicro.co.jp/archives/13384
10			①通常利用しているウイルス対策ソフトではランサムウェアの検体を検知出来ない場合は、別のオフラインで利用可能なウイルス対策ソフト（例 KVRT等）を利用して検体を検知できるか確認します。 ②別のウイルス対策ソフトでランサムウェアの検体を検知できる場合は、感染が疑われる機器にてスキャンを行います。	オフラインで利用可能なツールの例: ①カスペルスキー社:Kaspersky Virus Removal Tool ②マカフィー社:McAfee Stinger
11	感染経路	電子メール	①電子メールに添付されていたファイルを実行しランサムウェアに感染	①電子メールの送信に、正規アカウントが乗っ取られマルウェア送信に利用されるケースがあります。この場合、正規のメール送信者から受信した電子メールにマルウェアのファイルが添付されている場合があります。
12		Web閲覧	①改ざんされた（正規の）Webサイトを閲覧し、Exploit Kitによりランサムウェアに感染する場合があります。	参考URL: http://www.itmedia.co.jp/enterprise/articles/1602/23/news061.html Angler exploit kit generated by "admedia" gates https://isc.sans.edu/forums/diary/Angler+exploit+kit+generated+by+admedia+gates/20741/
13			①スパムメールに記載されたWebページをクリック後、captcha 入力する事でランサムウェアを利用者にダウンロード・実行させる場合があります。	参考URL: TorrentLocker Ransomware targeting Swiss Internet Users https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users
14			①家庭用ルータ等において、DNS 設定が不正な DNS サーバへ変更された事により、不正な広告サイトが表示されランサムウェアに感染する可能性があります。	参考URL: DNS Changer Malware Sets Sights on Home Routers http://blog.trendmicro.com/trendlabs-security-intelligence/dns-changer-malware-sets-sights-on-home-routers/ 家庭用ルータを狙う不正スクリプト「JITON」、国内でも攻撃継続中 http://blog.trendmicro.co.jp/archives/13114
15		リムーバブル機器	①ランサムウェアに感染した機器に外部記憶媒体が接続されていた場合、外部記憶媒体にランサムウェアがコピーされ、autorun.inf が変更される場合があります。	参考URL: RANSOM_ZCRYPT.A http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_zcrypt.a Link (.lnk) to Ransom https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/
16		Skype	①ランサムウェアに感染した機器に Skype がインストールされている場合、Skype が表示する広告（Exploit Kit）経由でランサムウェアに感染する場合があります。	参考URL: Malvertising via skype delivers angler https://labsblog.f-secure.com/2016/02/10/malvertising-via-skype-delivers-angler/
17		ブラウザアドオン経由の広告	①ブラウザのアドオンとしてインストールされているアプリケーションが表示する広告（Exploit Kit）経由でランサムウェアに感染する場合があります。	参考URL: Wajam Browser Add-on Serves Malvertising https://blog.malwarebytes.org/malvertising-2/2016/02/wajam-browser-add-on-serves-malvertising/
18		Adware（アドウェア）	①ランサムウェアに感染した機器にAdwareがインストールされている場合、Adwareが表示する広告（Exploit Kit）経由でランサムウェアに感染する場合があります。 ②感染機器にAdwareがインストールされていないかを確認すると共に、Adwareが存在する場合には削除します。	
19		リモートデスクトップ（RDP）	①インターネットに接続されているサーバの場合は、リモートデスクトップを経由でランサムウェアが侵入する事例も報告されています。	参考URL: Ransomware using Remote Desktop to spread itself http://www.scmagazine.com/ransomware-using-remote-desktop-to-spread-itself/article/448398/ Help recover files.txt Ransomware installed by targeted Remote Desktop or Terminal Services Attacks http://www.bleepingcomputer.com/news/security/help-recover-files-txt-ransomware-installed-by-targeted-terminal-services-attacks/

Copyright © LAC Co., Ltd. All Rights Reserved.

	項目	対象	内容	補足
20		脆弱性の利用 （Web サーバ）	①Web サーバが利用しているコンポーネント（CMS等）の脆弱性が利用され、Webページがランサムウェアの脅迫文に書き換えられる場合があります。	参考URL： Crooks Used SQL Injections to Hack Drupal Sites and Install Fake Ransomware http://news.softpedia.com/news/crooks-used-sql-injections-to-hack-drupal-sites-and-install-web-ransomware-504300.shtml
21		NAS機器	①Synology製 NAS の OS「Synology DSM」の古いバージョンにある脆弱性を利用	参考URL： ランサムウェア・レース（パート2）：パーソナルメディアが次のフロンティア？ http://blog.f-secure.jp/archives/50732483.html
22	横展開 （samsam）	アカウント情報の不正利用	①RAT（Win32/Derusbi と MSIL/Bladabindi ）を利用したパスワード情報の取得（Webブラウザ、Outlook等に保存しているアカウント・パスワード情報） ②Mimikatz を利用した認証情報の取得	参考URL： Ransomware Deployed by Adversary with Established Foothold https://www.secureworks.com/blog/ransomware-deployed-by-adversary
23		RAT	①Win32/Derusbi（過去に国内APTケースで利用？、文書ファイルの収集機能があります） ②MSIL/Bladabindi	参考URL： Win32/Derusbi https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/derusbi Catching the silent whisper: Understanding the Derusbi family tree https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Pun-etal-VB2015.pdf MSIL/Bladabindi https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=MSIL/Bladabindi
24		psexecによる展開	①psexecを利用し、リモートからのプログラム実行によりランサムウェアをネットワーク内で展開 ②psexec を利用し、ボリュームシャドウコピー（VSS)のデータ、バックアップファイルの削除を実施	参考URL： No mas, Samas: What’s in this ransomware’s modus operandi? https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/
25		SDeleteを利用した削除	①自己消滅に SDelete を利用	参考URL： Targeted Ransomware No Longer a Future Threat http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
26	被害拡大防止	ネットワークドライブの割り当て解除 （クライアント機器）	①感染機器の特定などが完全ではない場合、一時的なサーバへの被害拡大の対応策として、クライアント機器からファイルサーバに対するネットワークドライブの割り当てを解除します。 ②ファイルサーバ上の共有フォルダへのアクセスが必要な場合は、ネットワークドライブを割り当てずに、ネットワークコンピュータなどからアクセスします。 ③クライアント機器がランサムウェアに感染していない事を確認後、ネットワークドライブの割り当てを再設定します。	①ランサムウェアによっては、ネットワークドライブをマッピングしていない共有に対しても接続を行い、ファイルの暗号化を行う場合があります。 参考URL： DMA Locker Ransomware targets Unmapped Network Shares http://www.bleepingcomputer.com/news/security/dma-locker-ransomware-targets-unmapped-network-shares/ Price Hikes and Deadlines: Updates in the World of Ransomware http://blog.trendmicro.com/trendlabs-security-intelligence/price-hikes-and-deadlines-updates-in-the-world-of-ransomware/
27		USB機器による感染拡大	①ランサムウェアの動作により、USB機器などリムーバブル機器にランサムウェアのファイルが配置される場合があります。 ②感染した機器でUSB機器などを利用していた場合は、それらの機器にランサムウェアの感染が拡大していないかを確認します。	参考URL： New CryptoLocker Spreads via Removable Drives http://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/
28		ファイル感染型	①ランサムウェアの動作により、ファイルへの感染が行われる場合があります。 ②ランサムウェアの動作としてファイル感染が疑われる場合は、ウイルス対策ソフトを利用し感染が疑われるファイルのスキャンを実施します。	参考URL： VIRLOCK Combines File Infection and Ransomware http://blog.trendmicro.com/trendlabs-security-intelligence/virlock-combines-file-infection-and-ransomware/
29		Spam	①ランサムウェアへの感染と平行し、スパムメールの送信に悪用される場合があります。 ②ランサムウェアの被害を受けた端末から、スパムメールが送信されていないかを確認します。	参考URL： CERBER RANSOMWARE PARTNERS WITH THE DRIDEX SPAM DISTRIBUTOR https://www.fireeye.com/blog/threat-research/2016/05/cerber_ransomware_partners_with_Dridex.html
30		DDoS	①ランサムウェアへの感染と平行し、DDoSを行うマルウェアが被害機器に設定されている場合があります。 ②ランサムウェアの被害を受けた端末から、不審なパケットが送信されていないかを確認します。	参考URL： Ransomware developers seem to have found another way to monetize their operations by adding a DDoS component to their malicious payloads. http://news.softpedia.com/news/ransomware-adds-ddos-capabilities-for-annoying-other-people-not-just-you-504323.shtml

Copyright © LAC Co., Ltd. All Rights Reserved.

	項目	対象	内容	補足
31	情報漏えい	ファイルの送信	①ランサムウェアによる外部へのファイル送信・公開については、Chimera 型の事例がありますが、具体的なファイル送信機能は持っていなかったとされています。 参考URL； Chimera Ransomware Promises to Publish Encrypted Data Onlin https://threatpost.com/chimera-ransomware-promises-to-publish-encrypted-data-online/ Diving into Chimera Ransomware https://reaqta.com/2015/11/diving-into-chimera-ransomware/	①ファイルの操作ログを取得している場合は、ランサムウェアへ感染した時間帯に、正規の利用者による操作ではないファイル操作が無いことをログで確認してください。
32		ファイルリストの送信	①ランサムウェアが暗号化したファイルリストをC2サーバへ送信する事例が報告されています。 （偽の画像ファイルとして送信）	参考URL： The Central Security Treatment Organization Ransomware uses the Cry Extension and Communicates via UDP http://www.bleepingcomputer.com/news/security/the-central-security-treatment-organization-ransomware-uses-the-cry-extension-and-communicates-via-udp/
33		電子メール コンタクト情報	①ランサムウェアによるファイル暗号化処理とは別に、電子メールのコンタクト情報をC2サーバへ送信する事例が報告されています。（Thunderbird, Outlook, Windows Live Mail）	参考URL： The current state of ransomware: TorrentLocker https://blogs.sophos.com/2015/12/23/the-current-state-of-ransomware-torrentlocker/
34		パスワード情報	①ランサムウェアによるファイル暗号化処理とは別に、パスワード情報を取得するマルウェア Pony (Fareit) が実行される事例が報告されています。 参考URL: Pony, Angler and CryptoWall mixed into dangerous cyberthreat cocktail http://www.computerworld.com/article/3012101/security/pony-angler-and-cryptowall-mixed-into-dangerous-cyberthreat-cocktail.html ②ランサムウェアへ感染した端末において保存していたパスワード情報は全て変更します。	参考URL： Reveton ransomware has dangerously evolved https://blog.avast.com/tag/password-stealer/ Win32/Fareit https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Fareit
35		プライベートデータ（認証情報）	①CryptXXX ランサムウェアによるファイル暗号化処理とは別に、パスワード情報を取得する“private stealer”が実行される事例が報告されています。 ・Bitcoin ウォレット ・インスタントメッセンジャークライアントが保持しているデータ ・FTPクライアントソフトウェアが保持している認証情報 ・電子メールクライアントソフトに関連する情報 ・ブラウザに関連する情報、クッキー情報 ・CISCO VPN クライアント関連情報	参考URL： CryptXXX: New Ransomware From the Actors Behind Reveton, Dropping Via Angler https://www.proofpoint.com/jp/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler CryptXXX Ransomware Learns the Samba, Other New Tricks With Version 3.100 https://www.proofpoint.com/jp/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100
36		コンピュータ名 （Google Docs利用）	①ランサムウェアが利用する RSA 鍵、ランサムウェアを実行した機器のコンピュータ名の収集に Google Docs を利用するケースがあります。	参考URL： cuteRansomware Uses Google Docs to Fly Under Radar https://www.netskope.com/blog/cuteransomware-uses-google-docs-fly-radar/
37	復旧	暗号化ファイルの復号	①ランサムウェアの種類・バージョンによっては暗号化されたファイルを復号できる場合もあります。 ②ウイルス対策ソフトベンダがツールやサービスを提供している場合もある為、利用中のウイルス対策ソフトベンダの提供サービス等を確認します。 ②ボリュームシャドウコピーが削除されていない場合は、「以前のバージョン」からファイルを復元する事が出来る場合があります。	①削除ファイルから復元できる場合もありますが、ランサムウェアによっては空き領域を完全消去するタイプも報告されています 参考URL: XRTN Ransomware uses Batch Files to Encrypt your Data http://www.bleepingcomputer.com/news/security/xrtn-ransomware-uses-batch-files-to-encrypt-your-data/
38		復号ツールの確認	①ラインサムウェアに対応した無償の復号ツールが存在するか、ID Ransomware サイトなどを使い確認します。（ランサムウェアのバージョンによって復号可能かどうかが変わります） ※アップロードするサンプルファイルにおける機密情報の取り扱いには十分注意してください。 ID Ransomware https://id-ransomware.malwarehunterteam.com/	参考URL； Emsisoft Decrypter： https://decrypter.emsisoft.com/ Kaspersky Utilitie： https://support.kaspersky.com/viruses/utility
39		暗号化されたファイルの特定 （Cryptwall へ感染した場合）	①感染したランサムウェアが Cryptwall である場合、暗号化されたファイルのリストがレジストリ内に保存されている場合があります。 ②感染ユーザーのレジストリにて、暗号化されたファイルや範囲を確認し、バックアップからのリストアを行います。 HKEY_CURRENT_USER¥Software¥{UID}	例）感染ユーザーのレジストリファイル内の下記キー配下を確認（数字文字列はケース毎に異なります） HKCU¥Software¥5D04390F68AF645F72B33104F74D1918¥0111233447789BDF

Copyright © LAC Co., Ltd. All Rights Reserved.

	項目	対象	内容	補足
40	クライアント機器 （監視・復旧対応）	セキュリティログのサイズ変更	一時的な対応として、監査設定などを増やす事を想定し、セキュリティログのプロパティで、最大ログサイズを十分なログが記録可能なサイズまで値を増やします。	一時的な対応措置が完了後、サイズは適切な値に戻してください。
41		「プロセス作成の監査」の有効化	クライアント機器で不審なプロセス実行が疑われる場合は、システム監査ポリシーの“詳細追跡”において、プロセス作成の監査を有効にします。 プログラム実行の履歴がセキュリティログに記録されるようになります。	一時的な対応措置が完了後、監査設定は適切な状態に変更してください。
42		Windows Updateの実施	①Windows機器についてはWindows Updateを実施し、OSを最新の状態にします。（IEを含む）	
43		Adobe Flash Player を最新版へ更新	①必要が無い場合は、アンインストールします。 ②必要な場合は最新版へアップデートを行います。 ※通信先を制限している場合、アップデートに必要となる通信をホワイトリストへ追加し許可する必要があります。	
44		Adobe Acrobat Reader を最新版へ更新		
45		Java を最新版へ更新		
46		Microsoft Silverlightを最新版へ更新		
47		利用ブラウザを最新版へ更新		
48		Office製品のマクロ自動実行を無効化	WordやExcel等でマクロが自動実行される事を防ぐため、セキュリティセンターにてマクロの自動実行を無効化します。	
49	サーバ機器（Windows） 監視・復旧対応	バックアップの取得	必要に応じ、現在のデータについてバックアップを取得します。	ファイルが暗号化された際にリストア可能な状態としてください。
50		VSSのサイズを増加	ボリュームシャドウコピー（VSS）は一定サイズ以上の変更が発生した場合、既存のスナップショットが破棄される仕様となっています。大量のファイルがランサムウェアにより変更された場合、スナップショットが破棄され復元できなくなる危険性があります。この為、システムの保護機能において、スナップショット用として確保するディスク領域の使用量を十分確保する事を検討します。	VSSが破棄または削除されたケースに備え、オフラインでのバックアップは別途取得する必要があります。
51		セキュリティログのサイズ変更	一時的な対応として、監査設定などを増やす事を想定し、セキュリティログのプロパティで、最大ログサイズを十分なログが記録可能なサイズまで値を増やします。	一時的な対応措置が完了後、サイズは適切な値に戻してください。
52		「ファイル共有の監査」の有効化	一時的な対応として、システム監査ポリシーの“オブジェクト アクセス”において、これらの監査設定を有効にします。監査設定を有効にすることで、ファイル共有を通じたファイルへのアクセスがセキュリティログに記録されるようになります。 大量のログが記録されるようになる為、セキュリティログのサイズなどに十分注意します。 ※ランサムウェアによりファイルが再び暗号化された際には、該当ファイルにアクセスしたユーザー・機器をセキュリティログから特定します。	一時的な対応措置が完了後、監査設定は適切な状態に変更してください。
53		「詳細なファイル共有の監査」の有効化		
54		「プロセス作成の監査」の有効化	サーバ上での不審なプロセス実行が疑われる場合は、システム監査ポリシーの“詳細追跡”において、プロセス作成の監査を有効にします。 プログラム実行の履歴がセキュリティログに記録されるようになります。	一時的な対応措置が完了後、監査設定は適切な状態に変更してください。
55	被害防止	ブラックリストを利用した遮断	①ランサムウェアが利用しているC2サーバ、支払いサイトへのアクセスをPROXYサーバなどで遮断します ②ブラックリストは随時更新されている為、一定期間毎に最新版のブラックリストを適用する必要があります。 ③C2サーバとの通信を行わず、ファイルの暗号化を行うランサムウェアも存在します。	参考URL； Blocklist： https://ransomwaretracker.abuse.ch/blocklist/ Malware Corpus Tracker - Malware C&C Sites - locky： http://tracker.h3x.eu/c2/400 RockLoader Delivers New Bart Encryption Ransomware http://phishme.com/rockloader-downloading-new-ransomware-bart/

参考URL
Ransomware Overview https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml
Autoruns for Windows https://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx
“Offline” Ransomware Encrypts Your Data without C&C Communication http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/

Copyright © LAC Co., Ltd. All Rights Reserved.