年月	攻撃名	分類	概要	攻撃が成立する条件	攻撃でできること	参考URL	コラム候補	備考
2014/9	POODLE	仕様に対する攻撃	SSL3.0で暗号利用モードとしてCBCモードを利用する際、パディングの設計の問題によってパディングオラクル攻撃により暗号文を復号できる TLS1.0でもパディングの正しさを確認しない実装では影響を受ける	攻撃対象者がSSL3.0を有効にしている 攻撃対象者がCBCモードを有効にしている 攻撃者が通信を改ざんできる（Man-In-The-Middle）	Cookieの復元	CVE-2014-3566 https://www.openssl.org/~bodo/ssl-poodle.pdf		
2014/4	Hertbleed	実装に対する攻撃	サーバのデータをランダムに盗み見る （あくまでランダムなので狙ったデータを盗み見るには運か試行回数が必要） サーバに脆弱性が存在するのみで攻撃可能 実際に攻撃された事例が多数存在	攻撃対象者がOpenSSL1.0.1f以前を使用している 攻撃対象者のSSL/TLSのheartbeat拡張機能を利用している	サーバ秘密鍵の復元 セッション鍵の復元 Cookieの復元	CVE-2014-0160 http://heartbleed.com/		
2014/11	FREAK	実装に対する攻撃	Export-grade RSAが有効になっている環境において、中間者としてハンドシェイク通信を改ざんして脆弱なRSA Export Suitesを使うよう強制させ、事実上暗号化されていないかのように通信させる	クライアント側がOpenSSL1.0.1j以前であること サーバーのRSA Export Suites(RSA_EXPORT)が有効であること 攻撃者が通信を改ざんできる（Man-In-The-Middle）	メッセージの復元	CVE-2015-0204 https://censys.io/blog/freak		
2011/8	DigiNotar	認証局に関する事件	DigiNotar社の認証局システムが攻撃者により侵入され、不正な証明書が発行された 同社のルートCA証明書は主要なブラウザから無効化された	認証局システムに侵入してCAの秘密鍵を入手できる	不正な証明書の発行	http://www.atmarkit.co.jp/news/201109/08/diginotar.html http://www.itmedia.co.jp/enterprise/articles/1109/05/news020.html		

年月	攻撃名	分類	概要	攻撃が成立する条件	攻撃でできること	参考URL	コラム候補	備考
2015/5/13	Logjam	仕様に対する攻撃	暗号スイート指定可能な仕様バグと輸出グレード暗号(Export-grade cryptography) を組み合わせ、攻撃対象者に脆弱な鍵を使わせることにより、事実上暗号化されていないかのように通信させる	攻撃対象者の暗号スイートのうち*_EXPORTのいずれかが有効である 攻撃者が通信を改ざんできる (Man-In-The-Middle)	メッセージの復元	CVE-2015-1716 https://weakdh.org/		FREAKと類似しているが、実装上の問題ではなく仕様の問題
2016/1/8	SLOTH	仕様に対する攻撃	クライアント認証をMD5ハッシュ衝突により鍵の漏洩なしでも突破する攻撃 ユーザー認証付きTLSにおける中間者攻撃などに利用可能	正規のサーバーおよびクライアント共にMD5が署名方式として有効である 正規ユーザーを攻撃者のサーバーに誘導する(ドメインを偽る必要はない) クライアントがDHパラメータに素数が使われているかの厳密チェックを行わない	通信データへの任意文字列の挿入（中間者攻撃）	CVE-2015-7575 http://d.hatena.ne.jp/jovi0608/20160113/1452649563		
2016/3/1	DROWN	仕様に対する攻撃	SSL2.0のRSA鍵交換プロトコルに対し、Bleichenbacher RSAパディングオラクル攻撃の亜種によってRSA暗号文を復号できる 任意のSSL/TLSプロトコルに対しても、SSL2.0と同じRSA鍵を使用していると攻撃可能（General DROWN） OpenSSLのバグおよびオンライン中間者攻撃と組み合わせることにより、より効率的な攻撃が可能（Special DROWN）	General DROWN 攻撃対象サーバがSSL2.0を有効にしている 攻撃対象サーバが任意のSSL/TLSプロトコルにおいてSSL2.0と同じRSA鍵を使用している Special DROWN 攻撃対象サーバにOpenSSLの脆弱性（CVE2015-3197, CVE-2016-0703）が存在する 攻撃者がオンライン中間者攻撃が可能	セッション鍵の復元	CVE-2016-0800 https://drownattack.com/		
2016/3/3	CacheBleed	実装に対する攻撃	同一マシン上で使用された鍵を復元できる	攻撃対象者がOpenSSL1.0.1r以前を使用している 攻撃対象者のマシンが特定のCPUを使用している 攻撃対象者のマシンでHyper Threadingが有効である 攻撃者が同一マシン上でアプリケーションを実行できる 攻撃者が最低16000回程度(RSA4096bit鍵の場合)復号/署名演算が実行されているのを観測できる	セッション鍵の復元	CVE-2016-0702 http://ts.data61.csiro.au/projects/TS/cachebleed/		
2016/9/1	SWEET32	仕様に対する攻撃	3DESを使用した暗号文を復号できる	攻撃対象者のSSL/TLS設定でAESなど他形式よりも3DESの方が高優先度になっている 攻撃者が最低32GB以上の同共通鍵による暗号文を入手できる 攻撃者がJavaScriptインジェクションなどによる平文のコントロールか、同じ内容が繰り返し通信され続けていると予想出来る環境にある (Man-In-The-Browser)	Cookieの復元	CVE-2016-2183 https://sweet32.info/ https://access.redhat.com/ja/node/2607321		
2017/2/23	SHAttered	暗号アルゴリズムに対する攻撃	SHA-1 のコリジョン(衝突)により、同一のハッシュ値を持つ異なるPDFファイルを作成できる	署名アルゴリズムにSHA-1を利用している 元のPDFファイルのファイルを入手でき、一部（PDFのヘッダ）を変更できる	同一のハッシュ値を持つ異なるPDFファイルの作成	https://shattered.io/ https://shattered.io/static/shattered.pdf https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html		SSL/TLSではない

年月	攻撃名	分類	概要	攻撃が成立する条件	攻撃でできること	参考URL	コラム候補	備考
2017/10/16	KRAcks	仕様に対する攻撃	4ウェイハンドシェイクのメッセージ3の再送信を収集し再生することによってNonceのリセットを強制し、暗号文を復号できる	WPA2が正しく実装されている	セッション鍵の復元	CVE-2017-13080 https://www.krackattacks.com/		SSL/TLSではない
2017/9/11	NIAPが2018年1月1日からRSA鍵交換のciphersuiteを排除	ニュースリリース	CCの米認証機関であるNIAP（National Information Assurance Partnership）は、NIST Special Publication 800-131A Revision 1, dated November 2015により、NIST Special Publication 800-56B Revision 1, dated September 2014で定義されていないRSA PKCS#1.5は2018年以降（after 2017）は使用不可（Disallowed）であることを受けて、以下を発表しました ・RSAが鍵交換で使用されるciphersuiteを使用する製品をPCL（Product Compliant List ）に掲載しない ・NIAPは、有効期限前にPCLリストを維持するために保証保守が必要であることをPCL上の製品とともにベンダーに通知する ・PCLに掲載されたこれらの暗号スイートのみを使用する製品はすべてアーカイブする	–	–	https://www.niap-ccevs.org/Documents_and_Guidance/labgrams/labgram.cfm?id=106		
2017/10/31	NISTがCMVPのSP800-56の準拠を延長	ニュースリリース	SP 800-131A rev1で現在規定されている移行スケジュールは、CMVPはSP 800-56シリーズへの準拠を要求しないことを反映するように改訂される予定 関連する基準およびガイドラインが確定してから、改訂されたスケジュールに関する追加の詳細はCMVPによってリリースされる予定	–	–	https://csrc.nist.gov/News/2017/Transition-Plans-for-Key-Establishment-Schemes		
2017/8/16	Measuring HTTPS Adoption on the Web	論文発表	WebでのHTTPS普及率について調査した結果が発表 インターネット利用率の高い13ヵ国のうち、韓国と日本が最下位2ヵ国であった	–	–	https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf		
2017/12/4	中央省庁の8割が非対応、常時SSL化の実態を独自調査	ニュースリリース	日経コンピュータと日本経済新聞が2017年9月下旬から10月下旬まで調べたところ、中央省庁37機関のうち常時SSL化を終えているのは内閣官房や国家公安委員会、国税庁など9機関。残る28機関は問い合わせや電子申請の画面など対応は一部にとどまる。独立行政法人など政府系106機関のうちでも常時SSL化が完了しているのは2割強だった	–	–	http://itpro.nikkeibp.co.jp/atcl/column/14/346926/112801222/?rt=nocnt		
2017/5～7	TLS1.0無効化	ニュースリリース	Salesforce： 2017 年 7 月 22 日までに TLS 1.1 以上へのアップグレード https://help.salesforce.com/articleView?id=000221207&language=ja&type=1 サイボウズ： TLS 1.0の無効化 2018年6月10日（日） 3DESを含む暗号化スイートも併せて廃止 https://cs.cybozu.co.jp/2017/006411.html PyPal： The Foundation for PayPal's June 2017 TLS 1.2 Upgrade https://www.paypal-engineering.com/wp-content/uploads/2016/03/Foundation-for-June-2017-TLS-1.2-Upgrade-5.4.16.pdf 国税庁： 平成29年5月13日（土）以降「TLS1.0」及び「TLS1.1」のサポートを終了 https://www.nta.go.jp/news/tls/tls.htm	–	–	背景として考えられるPCIの記事2015年4月発行のPCI DSS v3.1で2016年6月までにTLS1.0、1.1を無効化する規定を2015年12月付けのプレス記事で2018年6月に延期 https://www.pcisecuritystandards.org/pdfs/15_12_18_SSL_Webinar_Press_Release_FINAL.pdf		

年月	攻撃名	分類	概要	攻撃が成立する条件	攻撃でできること	参考URL	コラム候補	備考
2014/4/1	NIST SP800-52	NIST文書	Executive Summary ～ It also recommends that agencies develop migration plans to TLS 1.2, configured using Approved schemes and algorithms, by January 1, 2015. ～	－	－	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf	「政府期間は2015年1月1日までにTLS1.2への移行計画を立てることを推奨する」 TLS1.2への移行を指示していないが推奨している	
2017/9/11	Chrome’s Plan to Distrust Symantec Certificates	Google security blog mozilla wiki	●Google ・2016年5月以前に発行された証明書： Chrome Ver.66から信頼されなくなる ・2016年6月以降に発行された証明書： Chrome Ver.70から信頼されなくなる ●Firefox December 1st, 2017: Symantec to implement "Managed CA" proposal January 2018 (Firefox 58): Notices in the Developer Console will warn about Symantec certificates issued before 2016-06-01, to encourage site owners to migrate their TLS certs. May 2018 (Firefox 60): Websites will show an untrusted connection error if they have a TLS cert issued before 2016-06-01 that chains up to a Symantec root. October 2018 (Firefox 63): Removal/distrust of Symantec roots, with caveats described below.	－	－	https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html https://wiki.mozilla.org/CA:Symantec_Issues http://www.atmarkit.co.jp/ait/articles/1712/01/news033.html		