

OGOD-20 2016.6.12

ランサムウイルスLocky

5月15日1時編集していたファイルが突然訳のわからぬ数字、アルファベット、¥などの記号の羅列にかわりました。そしてすべてのWordの拡張子がdocからlockyに変わっていました。そのファイルのトップにhelpメール記号があり、それをクリックすると送り先のあるメールが出てきました。そのメールを送るとこのファイルの回復用の暗号をおくるそうでしたが、いろいろな人に聞くと絶対にそのメールを開いてはならないと言われました。感染が広がり、さらに多くの金額を要求してくるそうです。エクスプローラーをLockyで検索するとたくさんの回復方法のメッセージが出てきましたソフトを買え、出張費を払えというメッセージばかりでした。いくつか無料のメッセージを3日徹夜でやってみましたが、回復はしませんでした。Norton、Macfeeでスキャンしたら、すべて安全ですというメッセージが返ってきました。Window10に変えたら残りのファイルの一部も消えました。最後にJCOMの「おまかせに」に連絡し、専門家を予約して見てもらいました。結論はパソコンを変えるしかない。もしがしたらOSを元のWindow7に変えるだけで少しは回復できるかもと言って、変更のプロセスを書いてくれ、JCOMに日程を予約するように頼めと言われ、それから3回のOS変更をしました。専門家は1項目30分3000円でした。幸いに3ヶ月程前に4GBのフラッシュメモリに一部バックアップを取っていたのが助かりました。メールも感染しているかも知れないのでメールは送れないとも言われました。現在は、メールは回復しましたが、ファイルはまだ回復作業が始まったばかりです。対策として怪しいメールは開けるなど言われますが、どれが怪しいか不明です。防御機能はWord、通信会社、メールソフト、ウェブサイト、アンチウイルスソフトとありますが、全部対策遅れで素通りします。ランサムウイルスは誰でも、いつか攻撃されます。唯一の対策は頻繁にバックアップをとることです。世界中の対策が、そのようになっています。FACEBOOKなどに似たメールやWebサイトに紛れこませています。しかも猛烈なスピードで変化しているので対策は常にまわりになっています。バックアップは頻繁に取って下さい。

自治体

1)OG

[1.オースチン市は Mozilla 財団が進めるギカビット市プロジェクトに参加\(ネットワーク、米国\)](#)

[4.ロスアンゼルス市は市のイノベーションに地域大学の起業家を求めている\(イノベーション、米国\)](#)

[5.スーパー公共イノ、ベション・ラボが地域の問題解決に挑戦\(イノベーション、米国\)](#)

2) OD

3.ソルトレイク市は警察データ運動に参加(データ、米国)

3) セキュリティ

2.市のデータベースは、不動産詐欺と戦っている(情報セキュリティ、米国)

州政府(県)政府

1) OG

1.退役軍人省は医療IoTの防護を考えている(IoT、米国)

2.予測分析、行動経済学、集合知が鍵(個人情報保護、米国)

4.NASCIOが州政府のIoTの価値と脆弱性を発表(IoT、米国)

5.政府透明性 Government Transparency 報告(オープンガバナメント、米国)

2) OD

3.コロラド州は子育てプログラムのデータ統合を行う(データ、米国)

3) セキュリティ

国政府

1) OG

5.クラウド分析を行うには柔軟な組織構築が不可欠(オープンガバナメント、米国)

7.オープン・ソース、COTS ベースの投票システム(オープンガバナメント、米国)

9.米国が遅れているデジタルIDベータ版を英国が先取り(個人認証、英国)

2) OD

3.Open データ市場は着実に成長している(オープンデータ、米国)

3) セキュリティ

1.報告: 18Fは Slack を使って情報漏れの原因を作る(セキュリティ、米国)

2.あなたのシミュレータは新しい FLEX 装置機器の 指針に対処できるか
(セキュリティ、米国)

4.政府機関が知るべき承認したベンダーの信頼度(セキュリティ、米国)

6.DHS 職員はフィッシング詐欺にだまされていない(セキュリティ、米国)。

8.政府データの安全を守る革新的な進入探知方法(セキュリティ、米国)

10.どのようにして 911 システムの安全を確保するか(セキュリティ、米国)

世界機関

1) OG

1.WHO は、医療サービスの回復を図る「リカバリツールキット」を公開(デジタル化、世界)

2.スホが世界のインターネットを占有(インターネット、世界)

3.コンピュータモデルは、乳がん手術前の乳房の維持を予測出来る(シミュレーション、EU)

4.EC(欧州委員会)が 2016 年度の欧州デジタル進捗報告書を発表した(デジタル改革、EU)

5.EUの殆どの加盟国がデジタル化で世界をリードしている(デジタル化、世界)

2) OD

3) セキュリティ

自治体

1.オースチン市は Mozilla 財団が進めるギガビット市プロジェクトに参加(ネットワーク、米国)

[Dave Nyczepir](#), routefifty, May 17, 2016

[Mozilla Gigabit Community Fund](#) が [Gigabit City Summit](#) でテキサス州、オーチンを 3 番目の hive city と命名した。この財団はカンサス市、チャタヌガ市などの [Gigabots](#) や [Wireless Earth Watchdogs](#) など 26 のプロジェクトを支援した [singing robots](#)。現在は非営利技術企業(nonprofit tech company)として知られる Firefox ブラウザの Mozilla が地方 Google Fiber ネットの構築し、博物館や図書館などの教育機関のウェブ開発するオーチン市の技術企業に 150,000ドル(約 1 億 5 千万円)の資金を提供した。

全文:

<http://www.routefifty.com/2016/05/austin-mozilla-gigabit-cities/128396/?oref=rf-today-nl>

2.市のデータベースは、不動産詐欺と戦っている(情報セキュリティ、米国)

Stephanie Kanowitz, GCN, May 17, 2016

ミシガン州オークランド市のシングルファーザーや元海兵隊が自宅の税の返済をしに行ったら、彼はもう所有していないので、その必要は無いと言われた。彼は不動産詐欺の被害者として家を取り戻すために、裁判所に提訴した。この事例はかなり広範囲に広がっている。これは市が Xerox の資産記録検索 (Property Records Notification、PRN)を使用しているからである。PRN では空白欄に誰かが書き込み料金を支払うと書き込んだ者が所有者として記録されるようになっている。

全文:

https://gcn.com/articles/2016/05/17/real-estate-fraud.aspx?s=gcntech_180516

3.ソルトレイク市は警察データ運動に参加(データ、米国)

Derek Major, GCN, May 17, 2016

ソルトレイクシティ警察署 (Salt Lake City Police Department、SLCPD)は、より透明の要求に応じて大統領府の警察データ運動 ([Police Data Initiative](#))に参加した。そして現在は毎月の暴力事件に関するデータを公開している。SLCPD はウェブサイト [web page](#) を立ち上げた。このサイトを使って、統計データ表の作成、容疑者の人種、どのような武器を見せたか、どのように武器を使ったか、容疑者に怪我を負わせたかなどのデータをデータのダウンロード出来る。

全文:

https://gcn.com/articles/2016/05/17/salt-lake-city-pdi.aspx?s=gcntech_180516

4.ロスアンゼルス市は市のイノベーションに地域大学の起業家を求めている(イノベーション、米国)

[Dave Nyczepir](#),、[routefifty](#), May 18, 2016

ロスアンゼルス市長は市の問題を解決する画期的な問題解決のアプリを市の大学の起業家からの募集し、優秀なアプリに知事賞 [Mayor's Cup](#) を授与する。最優秀アプリには25000ドル(約250万円)を授与する。そしてそのソフトを市のシステムに導入するのに8週間作業してもらう。予算・イノベーション課が主催するこのプロジェクトは住民の参加と地域経済の活性化になっている。詳細はここをクリック [here](#).

全文:

<http://www.routefifty.com/2016/05/la-university-entrepreneurs-innovations/128434/?oref=rf-today-nl>

5.スーパー公共イノ、ベション・ラボが地域の問題解決に挑戦(イノベーション、米国)

Amanda Ziadeh, GCN, May 11, 2016

市の行政サービスで開発し、提供するして地域の問題を解決する新しい部門横断ラ

ボが創設された。この新しいラボ [Superpublic](#) は市イノベーション室、商務部、総務部が5000平方フィート(450平方メートル)で民間企業のイノベーションチームと同じ場所で応答性の良い、効率の良い行政サービスとソフトを開発する。このスーパーラボは4つの活動に焦点を当てている。各活動はそれぞれのパートナーと協働する。州、連邦政府は政策とイノベーション、大学は研究開発、市のイノベーション財団はビジネス化、企業は製造を担う。

全文:

https://gcn.com/articles/2016/05/11/superpublic.aspx?s=STATELOCAL_190516&admgarea=TC_STATELOCAL

州政府(県)政府

1. 退役軍人省は医療IoTの防護を考えている(IoT、米国)

[Mohana Ravindranath](#)、nextgov、May 12, 2016

ハックされたペースメーカー [hacked pacemakers](#) が本当の脅威であるかどうかは不明であるが、退役軍人省(Veterans Affairs Department、VA)は患者が決して発見されないことを確認しようとしている。VAはこのペースメーカーがIoTにつながるのを防止する方法に関する情報を集めている [gathering](#)。IoTにつながれば、この医療機器を使って外部の侵入者が患者の医療記録を使うことが出来る。

全文:

http://www.nextgov.com/cio-briefing/2016/05/va-wants-protect-medical-internet-things/128260/?oref=nextgov_today_nl

2. 予測分析、行動経済学、集合知が鍵(個人情報保護、米国)

[Dave Nyczepir](#)、routefifty May 16, 2016

デロイト大学の新しい報告書 [Deloitte University Press report](#) によると、州政府はデジタル技術を導入して従来のフードスタンプと医療詐欺ネットによる大規模な個人情報の盗難を防護しなければならない。予測分析による「包括的な取り組み [holistic approach](#)」ではなく、行動経済学と集合知が対応が求められている。

全文:

http://www.routefifty.com/2016/05/state-fraud-prevention/128352/?oref=rf-today_nl

3. コロラド州は子育てプログラムのデータ統合を行う(データ、米国)

[Paul McCloskey](#)、routefifty、May 09, 2016

コロラド州の子育てや教育プログラムの評価システムを改善するために子育て支援

課 (Office of Early Childhood) はクラウドを使うようになった。これに 4 年間 4480 万ドル (約 4 億 4800 円) の教育予算獲得競争資金 (Race-to-the-Top grant) が投入され、州全体の幼児教育業者と両親の評価データ・システムが作成される。

全文:

https://gcn.com/articles/2016/05/09/colorado-child-care-rating-cloud.aspx?s=STATELOCAL_190516&admgarea=TC_STATELOCAL

4. NASCIO が州政府のIoTの価値と脆弱性を発表 (IoT、米国)

NASCIO、June 1 2016

NASCIO が州政府のIoTに関する政策 www.NASCIO.org/ValueAndVulnerability を発表した。この政策は現在利用しているIoTとは異なる方法に焦点を当てている。そして将来の見通しも行っている。

全文:

<http://173.188.123.141/Newsroom/ArtMID/484/ArticleID/386/NASCIO-Releases-Value-and-Vulnerability-The-Internet-of-Things-in-a-Connected-State-Government>

5. 政府透明性 [Government Transparency](http://www.uspirgedfund.org) 報告

[uspirgedfund.org](http://www.uspirgedfund.org)

毎年全国の州政府は、経済発展、助成金、および支出や他の形態で商品やサービス、補助金のための民間団体との契約を通じて数百億ドルを費やしている。その説明責任と公的機関の監査が必要である。2013年に、初めて、50州すべてがインターネットを介して州支出に関する詳細な情報を公開した。そのカルフォルニア州とバーモント州を除く48州が、その情報が詮索可能である。4年前には32州しかオンラインで情報を提供していなかった。その内29州しかオンラインで検索できなかった。

Ohio State checkbook:

<http://ohiotreasurer.gov/Transparency/Ohios-Online-Checkbook>

全文: <http://www.uspirgedfund.org/reports/usp/following-money-2013>

国政府

1. 報告: 18Fは Slack を使って情報漏れの原因を作る (セキュリティ、米国)

[Mohana Ravindranath](https://www.nextgov.com/nextgov/2016/05/13/mohana-ravindranath-slack-18f/)、nextgov、May 13, 2016

技術コンサルティングチーム 18F の Slack アカウント

(https://selectk.cc/note/selectk_howto/article/8) が外部に政府の機密情報を漏らし、データもれが起こる可能性があるという監視報告 (watchdog report)

(<https://www.treasury.gov/tigta/auditreports/2016reports/201640037fr.pdf>)は述べている。調達局(GSA)の18Fはデジタル化を進めようとしている企業や技術プロジェクトをもつ省庁に、スプレッドシートやPDFなどのドキュメントを共有するために Slack の使用を勧告している。Slack は今や、GitHub (https://seleck.cc/note/seleck_howto/article/30) チームで作業をするのような起業や技術企業に破竹の勢いで拡大を続けている。

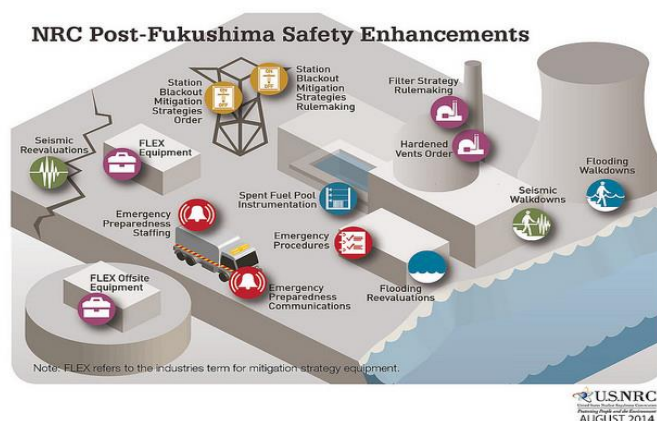
詳しくはここ [rest of the story here](#).

全文:

http://www.nextgov.com/cio-briefing/2016/05/watchdog-18f-caused-data-breach-using-slack/128288/?oref=nextgov_breaking_alert

2.あなたのシミュレータは新しい FLEX 装置機器の 指針に対処できるか (セキュリティ、米国)

[GSE Systems](#) | Apr 26, 2016



原子力規制委員会(Nuclear Regulatory Commission's、NRC)の福島第一原子炉事故の短期評価作業グループの評価報告書は、原子炉発電所は自然災害やテロ攻撃に対処する時間を現在の標準である 8 時間を 72 時間にすべきであると述べている。原子力産業界は冷却能力や電力の損失を防ぐために携帯機器の追加を要求している FLEX 戦略

(<http://safetyfirst.nei.org/industry-actions/flex-the-industry-strategy-to-enhance-safety/>)に対応している。電力界は殆どの原子力発電所にスタッフの訓練と新しい機器を図る FLEX 戦略を 2016 年末までに導入する。[Nuclear Energy Institute](#).

<http://safetyfirst.nei.org/industry-actions/flex-the-industry-strategy-to-enhance-safety/>

全文:

<http://www.gses.com/blog/can-your-simulator-cope-with-the-new-flex-equipment-guidelines>

3.Open データ市場は着実に成長している(オープンデータ、米国)

[Colin Wood](#)、govtech、May 13, 2016 0

オープンデータ会社 Socrata (www.socrata.com) の調査によると、オープンデータへの投資は堅調に推移している。報告書 [a new study](#) は連邦政府のレベ(9かし、地方自治体レベルは積極的でない。

全文:

<http://www.govtech.com/data/Open-Data-Market-is-Growing-Study-Says.html>

4.政府機関が知るべき承認したベンダーの信頼度(セキュリティ、米国)

Bob Ainsbury、nextgov、May 16, 2016

FedRAMP ([Federal Risk and Authorization Management Program \(FedRAMP\)](#)) (<http://techtarjet.itmedia.co.jp/tt/news/1202/09/news03.html>) は最近、メディアの関心を集めている。FedRAMP はクラウドの機密性、完全性、可用性のバーを上げている。その結果、市民と政府機関のデータが大幅に安全で信頼の高いシステムになった。

全文:

https://gcn.com/articles/2016/05/16/agency-fedramp-responsibilities.aspx?s=gcn_tech_170516

5.クラウド分析を行うには柔軟な組織構築が不可欠(オープンガバナメント、米国)

David Wang、FCW、May 16, 2016

オバマ政権になって、連邦政府のデータ量、データ形式、作成スピードが驚異的に殖えている。その結果、発生データとデータ分析との間に分析ギャップが生じている。これに対して民間企業はパブリッククラウドとオープンソースの Apache Spark (https://ja.wikipedia.org/wiki/Apache_Spark) を使って運用コストと導入期間を大幅に減らしている。政府機関が導入するには柔軟な政府組織 (agile government) 欠である。

全文:

https://fcw.com/articles/2016/05/16/comment-agile-cloud.aspx?s=fcwdaily_170516

6.DHS 職員はフィッシング詐欺にだまされていない(セキュリティ、米国)。

[Jack Moore](#)、nextgov、May 17, 2016

良いニュース: 独立監査人によって行われた「ソーシャルエンジニアリング」のテストは、国土安全保障省 (Homeland Security Department、HSD) の職員は基本的なサイバーセキュリティを知っていることである。しかし、悪いニュースは、一部の職員が機密の紙文書をまだ自室に残していることである。これらの調査結果は、HSD 監察官による DHS セキュリティ対策調査 [May 6 report](#) で公表された。

全文:

http://www.nextgov.com/cybersecurity/2016/05/audit-dhs-employees-not-falling-phishing-scams/128372/?oref=nextgov_today_nl

7. オープン・ソース、COTS ベースの投票システム (オープンガバナメント、米国)

Derek Major、GCN、May 19, 2016

オンライン投票には障害物 [obstacles](#) が多数あるが、より良い投票方法を開発しよとする起業家の活動はとめられない。新しい企業 Free & Fair 社は選挙を検証可能で、透明で、安全なプログラムを提案している。この企業は連邦政府の個人認証、個人情報 [privacy services](#)、サイバーセキュリティ (cybersecurity defense [solutions](#))、モバイル暗号化認証 (mobile cryptographic [authentication](#))、安全なドローンソフトウェア (secure drone [software](#)) の開発を手がけている研究企業 Galois 社からスピノフした。

注: COTS: コツツ (Commercial Off-The-Shelf)

http://www.zuken.co.jp/club_Z/z/word1/word060.html

全文:

https://gcn.com/articles/2016/05/19/open-source-election-tech.aspx?s=gcntech_230516

8. 政府データの安全を守る革新的な進入探知方法 (セキュリティ、米国)

Paul Kraus、GCN、May 19, 2016

近代的なオンラインセキュリティの悲しい真実は、ハッカーが防衛する人よりも早く行動することである。ハッカーは、モバイル利用者からサーバーまで、すべての vector ([https://ja.wikipedia.org/wiki/%E3%83%99%E3%82%AF%E3%82%BF%E3%83%BC_\(%E4%B0%81%E6%A5%AD\)](https://ja.wikipedia.org/wiki/%E3%83%99%E3%82%AF%E3%82%BF%E3%83%BC_(%E4%B0%81%E6%A5%AD))) によって画期的な方法で政府機関を攻撃してくる。連邦人事管理局 (Office of Personnel Management) は 2015 年には 2 度進入された。同局はこのような進入を防止するために防衛体制の改善のスピードアップを呼びかけている。ファイアウォールやウイルス対策ソフトウェアなどの境界防衛線 (Perimeter defenses) は進入のフィルターにはある程度役立っているが、確実ではない [but certainly not all](#)。既存

の資源を活用して敏速な方法でアクティブな漏洩探知システム (active breach detection) を改良して行くことを提案している。そのシステムは 24 時間の監視をする夜警オンラインシステムである。これらのシステムの可視化は非常に効果がある。

全文:

https://gcn.com/articles/2016/05/19/active-breach-detection.aspx?s=gcntech_230516

9. 米国が遅れているデジタルIDベータ版を英国が先取り(個人認証、英国)

Adam Mazmanian, Bianca Spinosa, FCW, May 20, 2016

英国の国民は一つの安全なサイト GOV.UK Verify

(<https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>) から税金、年金、運転免許などの情報にアクセスできる。このシステム(マイナンバー)は公開ベータ版

(<https://claim.redundancy-payments.service.gov.uk/claims/choose-how-to-verify>) が 5 月 23 日から運用される。

GOV.UK Verify で、英国郵便局と民間企業のクレジット会社 Experian、モバイル会社 Verizon、銀行 Barclays も参加して政府取引で使われる既存の安全認証のブローカーとして行動する。米国が遅れているデジタルIDベータ版を英国が先取りする。

全文:

https://fcw.com/articles/2016/05/20/nstic-connectgov-ukverify.aspx?s=fcwdaily_230516

10. どのようにして 911 システムの安全を確保するか(セキュリティ、米国)

Mark Pomerleau, GCN, May 23, 2016

コンピュータシステム、データベース、および個人のデバイスに対するサイバー攻撃は近年上昇している。同様に国民と第一応答者をつなぐ 911 緊急応答システムもサイバー攻撃を受けている。緊急応答機関(public safety answering points、PSAPs)に対する、これらのサイバー攻撃は、ますます拡大している。これに対応して、連邦政府、州政府の規制当局や担当局は、これらのシステムの強化を求めている。緊急応答機関を受けている、これらの脅威は、受け持っている管轄区によって異なる。古くなったコンピュータシステムへの攻撃、電話サービスの妨害(Telephony Denial of Service、TDoS)などで、無線周波数妨害で出来るように緊急応答機関センターを電話コールで溢れさせて、真の危機を演出するのが目的である。新しい個人認証システム(IP-based systems)はサービス拒否攻撃やウイルス、ワーム、トロイの木馬攻撃で攻撃される。

連邦通信委員会 (Federal Communications Commission、FCC) は次世代 Next Generation 9-1-1 (NG9-1-1) に Public Safety Answering Points (PSAPs) を移行する。

[report](#)

全文:

https://gcn.com/articles/2016/05/23/secure-911.aspx?s=gcntech_240516

世界機関

1. WHO は、医療サービスの回復を図る「リカバリツールキット」を公開(デジタル化、世界)

WHO、12 May 2016

世界保健機関が医療サービスの活性化と感染症や、その他緊急医療の回復を図る国を支援する Recovery

Toolkit http://apps.who.int/iris/bitstream/10665/205944/1/WHO_HIS_SDS_2016.2_eng.pdf?ua=1 を開発した。この Recovery Toolkit はすばやく、容易にアクセスできる行動

指針を一ヶ所で提供できる図書館である。このキットは国の医療システムを機能させるのに重要な情報を提供する。このキットの主目的は緊急医療と同じ結果の対応に苦しむ医療活動の再活性化である。

詳細はここ [More details](#)

全文:

<http://www.continuitycentral.com/index.php/news/resilience-news/1105-who-launches-recovery-toolkit-for-health-service-resilience>

2. スマホが世界のインターネットを占有(インターネット、世界)

drienne LaFrance、nextgov、May 16, 2016

ラップトップは、まだ正確には古くなってはいない。しかし、パソコンでのインターネットアクセスが少なくなるとモバイル革命が近づく。デスクトップからスマートフォンへの傾向は 10 年以内の起こるであろう。最近モバイルへの移行は特に顕著である。2014 年のいくつかの調査 [several measures](#) で、モバイルのインターネット利用は、デスクトップのインターネットアクセスを上回った。アフリカとアジアでは、すべての年齢層の人々が最も重要な通信機器としてパソコンではなく、スマホを求めている

GlobalWebIndex 社の昨年の調査によっても 34 歳以下の人はほとんどの人がスマホを使っている。

全文:

<http://www.nextgov.com/mobile/2016/05/smartphones-rule-internet/128334/?oref>

[=nextgov_today_nl](#)

3.コンピュータモデルは、乳がん手術前の乳房の維持を予測出来る(シミュレーション、EU)

Europa、12/05/2016

乳がん手術の結果、女性の30%以上が乳がんの再発か醜い乳房になっている。EUが資金を提供する [PICTURE project](#) はこの問題を述べている。個々の患者に合わせて、醜くならない乳房の手術を予測し、評価するツールを提供して、この問題に対処すると発表した。

全文:

<https://ec.europa.eu/digital-single-market/en/news/computer-models-can-predict-aesthetic-result-breast-cancer-surgery>

4.EC(欧州委員会)が2016年度の欧州デジタル進捗報告書を発表した(デジタル改革、EU)

Europa、23/05/2016

欧州デジタル進捗報告(Europe's Digital Progress Report、EDPR)

(<https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2016>)は示している。この報告書はデジタル公共サービスの接続、デジタル技術、インターネットの使用、ビジネスによるデジタル技術の統合、デジタル行政サービスの5異なる観点から各参加国を開発状況と各国の報告書を分析している。このモニタリング報告書の目的は、単一市場の市民、企業が加盟国のデジタル革命の進行状況を把握できるようにすることである。

全文:

<https://ec.europa.eu/digital-single-market/en/news/commission-releases-2016-european-digital-progress-report-unequal-progress-towards-digital>

5.EUの殆どの加盟国がデジタル化で世界をリードしている(デジタル化、世界)

Europa、23/05/2016

EC(欧州委員会)は、EU参加国と15の非EU参加国(オーストラリア、ブラジル、カナダ、中国、アイスランド、イスラエル、日本、韓国、メキシコ、ニュージーランド、ノルウェー、ロシア、スイス、トルコ、米国)とのデジタル化の比較を発表した

<http://www.project-consult.de/files/GermanyEDPRcountryprofile.pdf>。

International DESI (I-DESI)社も同様の比較を発表した。

[I-DESI Final Report - Executive Summary - Background data and calculations](#) は

<https://ec.europa.eu/digital-single-market/en/news/most-digital-eu-countries-lead-globally>

全文:

<https://ec.europa.eu/digital-single-market/en/news/commission-releases-2016-european-digital-progress-report-unequal-progress-towards-digital>