IEICE ICT PIONEERS WEBINAR シリーズ 第 28 回

「デジタル時代のサイバーセキュリティ」 Source Note

2022.8.4 時点

三宅功

何が起こっているか？ 激しサイバー攻撃ハイブリッド戦争

(1-1) 2021~ Google TAG による情報操作、影響工作に関しては以下を参照

https://blog.google/threat-analysis-group/tag-bulletin-q2-2021/

https://blog.google/threat-analysis-group/tag-bulletin-q2-2022/

(1-2) 2021.11 ウクライナの司法機関等へのフィッシング攻撃による侵入の試み

https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/

(1-3) 2022.1.14 政府 Web サイトへの攻撃

2022.1.14 BLEEPINGCOMPUTER

https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/

2021.11.15 MANDEANT

https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

(1-4) 2022.2.15 DDoS 攻撃

2022.2.15 CYBERSCOOP

https://www.cyberscoop.com/ukraine-websites-ddos-joint-briefing/

https://www.cyberscoop.com/ukraine-ddos-russia-attribution-white-house-neuberger/

2022.2.18 英国政府による GRU 帰属の公表

https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine

(1-5) 2022.2.24 破壊活動

2022.2.26 CISA 公表、ウクライナの組織を標的とする破壊的なマルウェア

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

(1-6) 2022.2.24 衛星通信システム破壊

2022.5.31 SentinelLABS の公表

https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/#:~:text=SentinelLabs%20researchers%20discovered%20new%20malware,to%20wipe%20modems%20and%20routers.&text=AcidRain%20is%20the%207th%20wiper,the%20Russian%20invasion%20of%20Ukraine.

https://prtimes.jp/main/html/rd/p/000000021.000045349.html

(1-7) 本ページを含め、最近の動向全体に関しては以下も参考とした。

War in Ukraine インターネット時代の新しい戦争, MIT Technology Review e ムック, 2022.5.31 https://restricted.technologyreview.jp/wp-content/uploads/sites/2/2022/06/MITTR_eMook_Vol43_oo91jxqai.pdf

何が起こっているか？ 無差別なエスカレート

(2-1) 2022.6.21 ウクライナ CERT(CERT-UA)が政府機関、メディア、企業、NGO 等へ２つの攻撃を確認。
https://www.cyberscoop.com/ukraine-russia-hacking-apt28-trickbot-follina/
ウクライナ CERT の公表（ウクライナ語）
① https://cert.gov.ua/article/339662
② https://cert.gov.ua/article/341128
(2-2) 2022.7.19 Android アプリによるマルウェア配布 Google TAG が報告。
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/

何が起こっているか？ ハイブリッド戦争

(3-1) 2022.4.27 Special Report: Ukraine : An overview of Russia’s cyberattack activity in Ukraine, MicroSoft
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
(3-2) Cyberattacks in the first four monthe of the war
https://twitter.com/dsszzi/status/1542506653127364609
(3-3) 欧州議会の報告書
2022.6 Russia's war on Ukraine: Timeline of cyber-attacks
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

すでに始まっていたサイバー戦

(4-1) ロシアのウクライナ等に対するサイバー攻撃の経緯は以下を参考にまとめている。
Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Andy Greenberg, 2019.11.5, Anchor

Sand warm の攻撃プロセス APT*攻撃の Kill Chain

(5-1) 主に以下を中心にまとめている
Russian Cyber Espionage Campaign - Sandworm Team, iSIGHT Pertners 2014.10.14 https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf

重要インフラへの攻撃　　”サイバー攻撃の演習場”

(4-1)を中心に整理

電力網　ICS/SCADA への攻撃の様子

(6-1) 2017.6.28 ハッカーがパワーグリッドコンピューターのマウスを乗っ取るのを見る
https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/

電力網　ICS/SCADA への攻撃　第 1 波(2015.12)から第 2 波(2016.12)へ

(7-1) 第一波

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, Wired, 2016.3.3
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Analysis of the Cyber Attack on the Ukrainian Power Grid, E-ISAC, 2016.3.18
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

(7-2) 第 2 波

WIN32/INDUSTROYER A new threat for industrial control systems, ESET, 2017.6.12 https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations, Dragos, Ver.2 2017.6.13 https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

(7-3) ウクライナに大規模停電を発生させたマルウェア「Industroyer」の新バージョン（Industroyer2)を確認, ESET,　2022.5.25
https://eset-info.canon-its.jp/malware_info/special/detail/220525.html

NotPetya(ワイパーワーム）の拡散　2017.6.27~

(8-1) NotPetya の概要
https://en.wikipedia.org/wiki/Petya_and_NotPetya

(8-2) Petya 亜種による世界サイバー攻撃、65 カ国に拡大　会計ソフト更新の仕組みを悪用か, ITmedia, 2017.6.29
https://www.itmedia.co.jp/enterprise/articles/1706/29/news057.html

(8-3) Ukraine cyber-attack: Software firm MeDoc's servers seized, BBC, 2017.7.4
https://www.bbc.com/news/technology-40497026

(8-4) NotPetya ランサムウェア攻撃の詳細分析, LastLine/NTT データ先端術, 2017.7

https://www.intellilink.co.jp/column/security/2017/070300.aspx
(8-5) M.E.Doc サーバへの攻撃, BLEEPINGCOMPUTER, 2017.7.6
https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/
(8-6) M.E.Doc に仕込まれたバックドアの概要, ESET, 2018.3.6
https://eset-info.canon-its.jp/malware_info/trend/detail/180306.html

NotPetya　拡散プロセスのイメージ
主に(4-1)に基づいて整理。また、EternalBlue 及び ShadowBroker については以下を参照。
(9-1) Schroedinger's Pet(ya), Kaspersky, 2017.6.27
https://securelist.com/schroedingers-petya/78870/
(9-2) The Shadow Brokers, Wikipedia
https://en.wikipedia.org/wiki/The_Shadow_Brokers

ロシアの国家によるサイバー攻撃組織
以下の資料の他に(4-1)を参考にしている。
(10-1) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, CISA, 2022.4.20
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
(10-2) Mapping the connections inside Russia's APT Ecosystem, CheckPoint, 2019.9.24 https://research.checkpoint.com/2019/russianaptecosyste/
参考
(10-3) FSB, SVR の前身である連邦政府通信情報局：FAPSI については以下を参照
FAPSI, Wikipedia
https://en.wikipedia.org/wiki/FAPSI
(10-4) GRU に関しては、以下を参考にした。
What is the GRU?, Economist, 2018.9.11
https://www.economist.com/the-economist-explains/2018/09/11/what-is-the-gru

欧米のロシアサイバー攻撃への対応状況　国家レベルの例
(11-1) 2020.10.19 DOJ　6 名の GRU ハッカーを起訴
https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
(11-2) 2021.6 DOJ GRU　関連の研究機関に帰属する 1 名を起訴、Power Grid 以外の石油精製施設へのサイバー攻撃のための技術を提供。

2021.8 DOJ FSB に帰属するハッカー3 名を起訴。石油・ガス会社、原子力発電所を含む国際エネルギー部門の企業や組織のコンピュータネットワークへの侵入、情報窃取。
2022.3.24　起訴状を公開
https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
(11-3) 2022.4.20　CISA、FBI、NSA、および国際的なパートナーが、ロシア国家が支援するサイバー犯罪アクターの実証された脅威と能力に関する勧告を発行
https://www.cisa.gov/news/2022/04/20/cisa-fbi-nsa-and-international-partners-issue-advisory-demonstrated-threfumeats-and
5eyes によるロシアの国家支援型サイバー攻撃に関連した組織の概要をレポート
(11-4) 2022.4.26 米国司法省　ロシア GRU に帰属する 6 名のハッカー（訴訟済）に関する情報提供プログラムの報奨金を最大 1 千万＄と発表。
https://twitter.com/RFJ_USA/status/1518983587697147906
(11-5) 2022.5.10 米国務省　ロシアのウクライナに対する悪意のあるサイバー活動の帰属
Attribution of Russia's Malicious Cyber Activity Against Ukraine
https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
(11-6) 2022.1.17　NATO がウクライナに対するサイバーセキュリティ対策支援の強化に関する覚書を締結。
https://www.nato.int/cps/en/natohq/news_190906.htm
(11-7) 2022.3.5 NATA CCDCOE の報告　Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis
https://ccdcoe.org/news/2022/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/
https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_vol2_15032022.pdf
　＜参考＞CCD-COE CyCon https://ccdcoe.org/cycon/
(11-8) 2022.7.6 NATO がウクライナのサイバー防衛に対する支援強化を発表。具体的には、サイバー防衛基金の設立など。
https://www.eurointegration.com.ua/articles/2022/07/6/7142651/

欧米のロシアサイバー攻撃への対応状況　民間レベルの例

(12-1) 2022.2.4 Microsoft Threat Intelligence Center (MSTIC)によりロシア由来の脅威グループがウクライナの組織を標的にしているとして、その詳細を公表。
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

(12-2) MicroSoft　2022.2.28 ブラッドスミスによるウクライナ侵攻に対する声明　デジタル技術とウクライナ戦争　民間企業の立場で政府関係者と協議しつつウクライナに対する支援を表明
https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/
(12-3) MicroSoft　2022.6.22　ウクライナを守る：サイバー戦争からの初期の教訓
https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
上記と合わせて、6 月までの教訓をレポートとして公開。
Defending Ukraine:　Early Lessons from the Cyber War
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
(12-4) Google TAG の監視活動等に関しては以下を参照。
Google Project Shield
https://projectshield.withgoogle.com/landing

その他の例
(12-5) AWS の対応　主に政府機関を始めとするウクライナ各組織の重要データの保護と人道支援に注力
https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine
(12-6) Meta の対応　https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/
(12-7) Akamai の対応　https://www.akamai.com/ja/blog/news/ukraine-statement

MITER ATT&CK の整備　サイバー攻撃に対応した官民連携の基盤
(13-1) MITER ATT&CK ホームページ　https://attack.mitre.org/

ロシア国内の状況　インターネットの普及と監視、統制の強化
(14-1) インターネットの普及状況　ITU-T Statistics
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

ロシア国内の状況　インターネットの普及と監視、統制 2010 年頃まで
(15-1) OpenNet Initiative　https://opennet.net/

ロシア国内の状況　情報監視・統制の強化
(16-1) Internet censorship in Russia, Wikipedia
https://en.wikipedia.org/wiki/Internet_censorship_in_Russia
(16-2) 2016 年施行「ヤロヴァヤ法」（発案者のヤロヴァヤ下院公安委員長の名を取っている）

https://en.wikipedia.org/wiki/Yarovaya_law
(16-3) LINE が使えなくなった理由　2017.5.5
https://russiabuzz.hatenablog.com/entry/2017/05/05/lineprohibited
(16-4) A market of black boxes: The political economy of Internet surveillance and censorship in Russia, Ksenia Ermoshina, Benjamin Loveluck, Francesca Musiani
https://hal.archives-ouvertes.fr/hal-03190007
(16-5)「ネット主権法」 2019.11.1
https://www.jetro.go.jp/biznews/2019/11/a38ae40b5937dd7c.html
(16-6)ロシアが「国内のインターネットを国外から切り離す実験を行う予定
https://gigazine.net/news/20190212-russia-disconnect-internet-test/
ロシアが「国内ネットワークをインターネットから切り離すテスト」に成功、2019.12.25
https://gigazine.net/news/20191225-russia-internet-disconnect-test/
(16-6) ロシアの新しい「信頼されたルート CA」を信頼すべきではない、2022.3.15
https://www.eff.org/deeplinks/2022/03/you-should-not-trust-russias-new-trusted-root-ca

国家によるサイバー攻撃の多様化

以下の書籍を参考に集計。分類は講演者による。

(17-1) 世界サイバー戦争、リチャード・クラーク、ロバート・ネイク、2011
(17-2) サイバー完全兵器、デービッド・サンガー、2019

国家によるサイバー攻撃の動向　攻撃を受けた国

国家によるサイバー攻撃　どこが行っているか？

(18-1) Significant Cyber Incidents, CSIS, 2022.6
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
(18-2)　20 位までの集計は以下を参考にした
最も重大なサイバー攻撃を受けた国トップ 20, NordVPN, 2022.1.27
https://nordvpn.com/ja/blog/cyber-attack-incidents/

もう１つのグローバル化　Windows の寡占

(19-1) Disc Top OS のシェア　statcounter　2022.6
https://gs.statcounter.com/os-market-share/desktop/worldwide/
(19-2) サーバ OS のシェア　statista　2022.6
https://www.statista.com/statistics/915085/global-server-share-by-os/

Web サーバの状況

(20-1) 登録ホスト名とアクティブな Web サーバ Netcraft 2022.6
https://news.netcraft.com/archives/2022/06/30/june-2022-web-server-survey.html

(20-2) 全世界で使われる Web サーバーの開発元「NGINX」にロシア警察の強制捜査、従業員拘束＆機器押収へ、2019.12.13
https://gigazine.net/news/20191213-russian-police-raid-nginx/

モバイル通信の普及

(21-1) ITU-T Statistics （注）プリペイドを含む
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

移動体通信サービスのインパクト

(22-1) How Apple Has Changed The World In Just 7 Years
https://www.cultofmac.com/219813/how-apple-has-changed-the-world-in-just-7-years-picture-1000-words/

移動体通信サービスと GDP

(23-1) Our World in Data
https://ourworldindata.org/grapher/mobile-phone-subscriptions-vs-gdp-per-capita

固定電話サービスと GDP

(24-1) Our World in Data
https://ourworldindata.org/grapher/fixed-landline-telephone-subscriptions-vs-gdp-per-capita

メガプラットフォーマによるクラウドサービスの寡占

(25-1) Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total, synergy, 2022.4.28
https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues