新型コロナウイルスとICTの光と影

国立研究開発法人 情報通信研究機構

サイバーセキュリティ研究所
サイバーセキュリティ研究室
井上 大介

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

ICTを活用した新型コロナウイルスへの対応

- **WFH（Work From Home）**
  - ✓ VPNによるリモートワーク（情シスの奮闘に感謝）
  - ✓ ビデオ会議ソフトによる遠隔多地点会議
  - ✓ チャットツールによる円滑なチーム運営

NICT 情報シスの業務量の推移（一部抜粋）

	1月	2月	3月	4月
問い合わせ件数	368	363	447	1248
各種申請対応	1828	1965	2569	4027

- **地方自治体等によるWeb経由のリアルタイム情報発信**
  - ✓ 効果的な情報可視化、インフォグラフィクス

- **プラットフォーマーによる対策提供**
  - ✓ Apple + Google：Contact Tracing（感染者との接触追跡・通知アプリ）
  - ✓ LINE：新型コロナ対策のための全国調査

- **オンライン教材による学習支援サービス**
  - ✓ 文科省：子供の学び応援サイト
    https://www.mext.go.jp/a_menu/ikusei/gakusyushien/index_00001.htm
  - ✓ **NICT：学び応援サイト**
    https://www.nict.go.jp/learning-site.html

etc. etc...

東京都 新型コロナウイルス対策サイト
https://stopcovid19.metro.tokyo.lg.jp

National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

ビデオ会議ソフト『Zoom』のセキュリティ問題

- **ユーザ数1000万 ➡ 3億に急増**（2019年12月 ➡ 2020年4月）

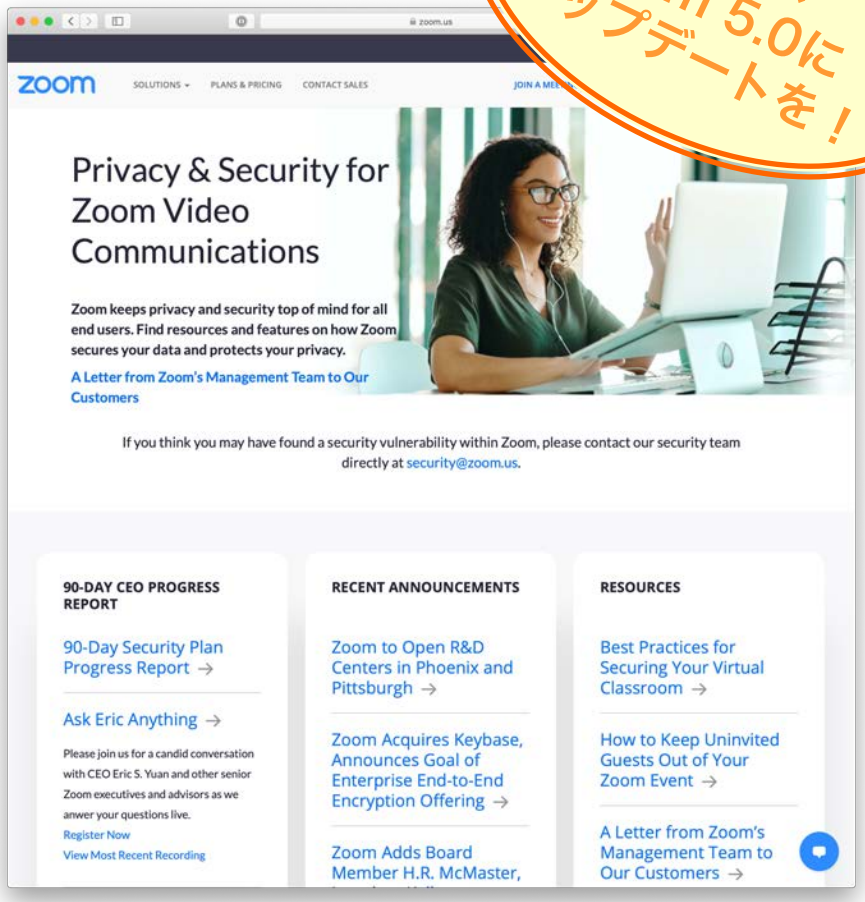
- **数々のセキュリティ問題が噴出**（大部分は対応済み）
  - ✓ Zoom-bombing（ミーティングへの第三者の乱入）
    - ミーティングIDとパスワードが画面上に表示される
    - ミーティングIDが容易に推測可能
  - ✓ End-to-end暗号化問題
    - 暗号利用モードが不適切（ECB ←ダメ。ゼッタイ。）
    - Zoomサーバが暗号化鍵を保持、北京の鍵サーバを経由
  - ✓ UNCパスインジェクション脆弱性
    - Windowsユーザの認証情報漏洩の可能性
  - ✓ Facebookにユーザの分析データを送信
    - iOSアプリがユーザ同意なしに分析データを送信

etc. etc...

- **Zoom 90-Day Security Plan**
  - ✓ 4月1日から新機能開発を凍結し全リソースをセキュリティに投入

➡ **上記の問題が順次解消されていっている**

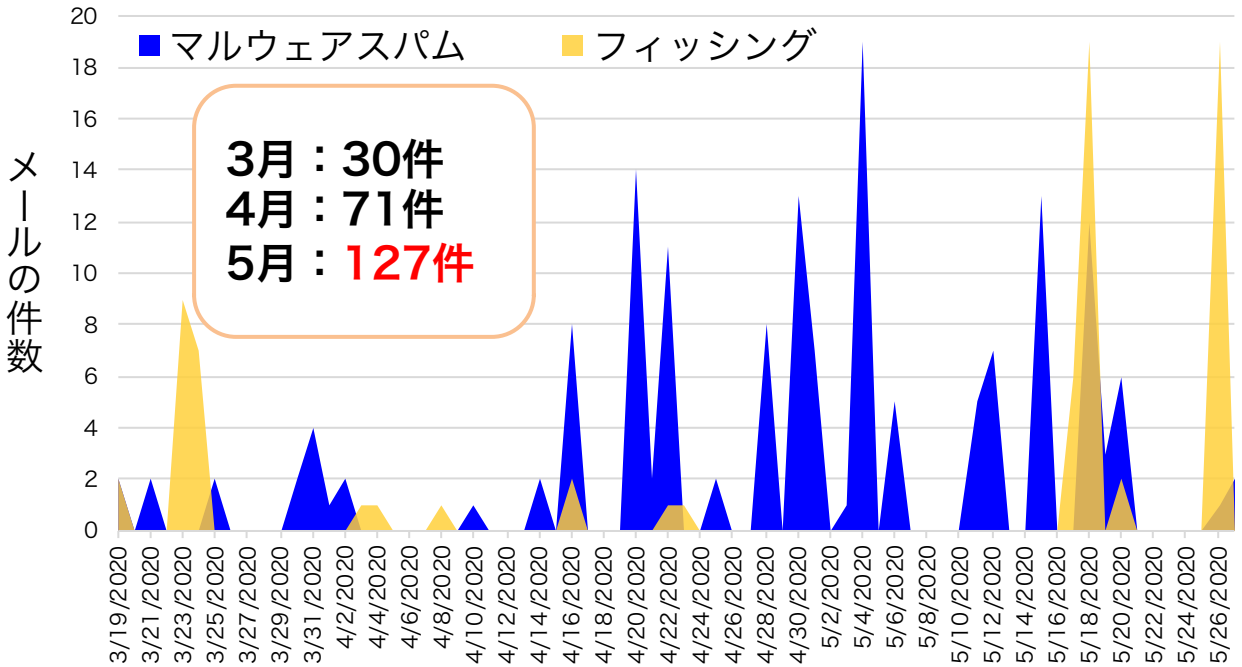
いますぐ Zoom 5.0に アップデートを！



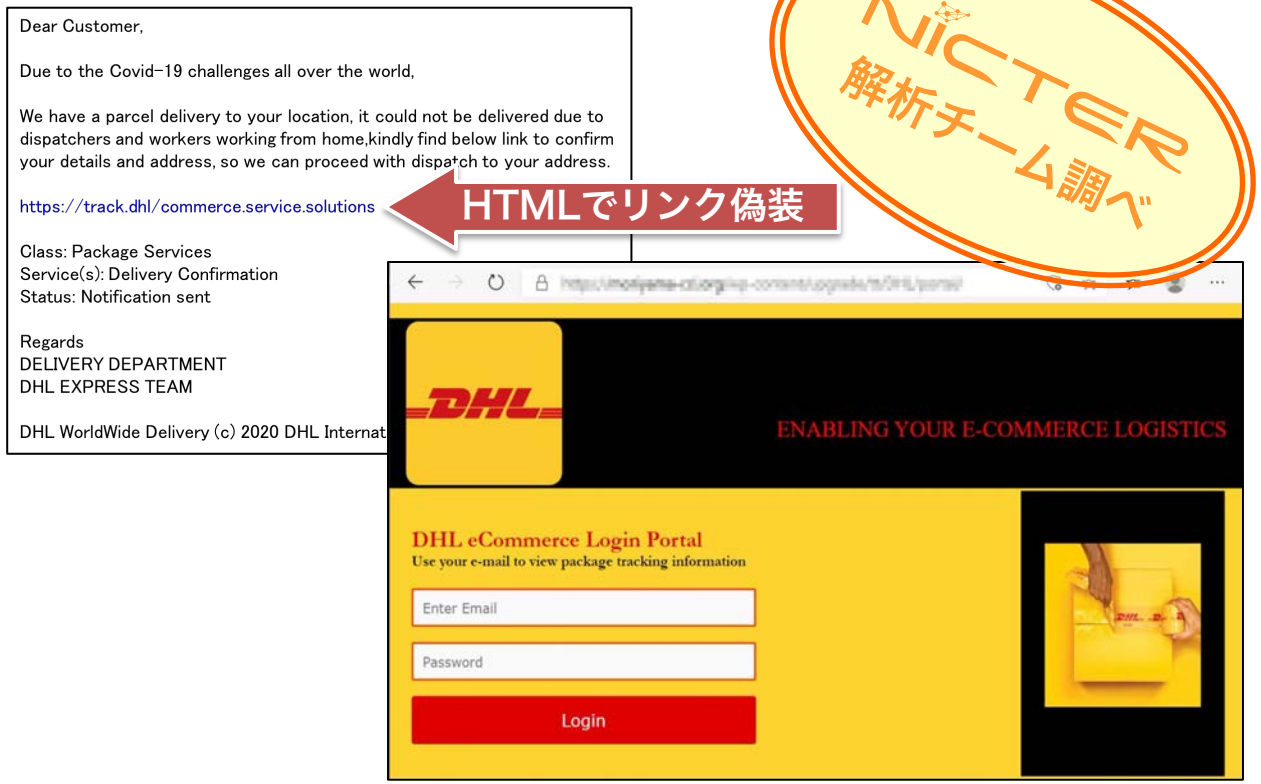
https://zoom.us

新型コロナウイルスに関連した攻撃メールの増加

- **新型コロナウイルス（Covid-19）を騙った攻撃メールが世界各地で増加中**
  - ✓ マルウェアスパム：マルウェアが添付されたスパム（Ransomware, Infostealer, Downloader, RAT, etc.）
  - ✓ フィッシングメール：Covid-19に関連したフィッシングサイトに誘導するメール



NICTへのCovid-19関連メールの推移



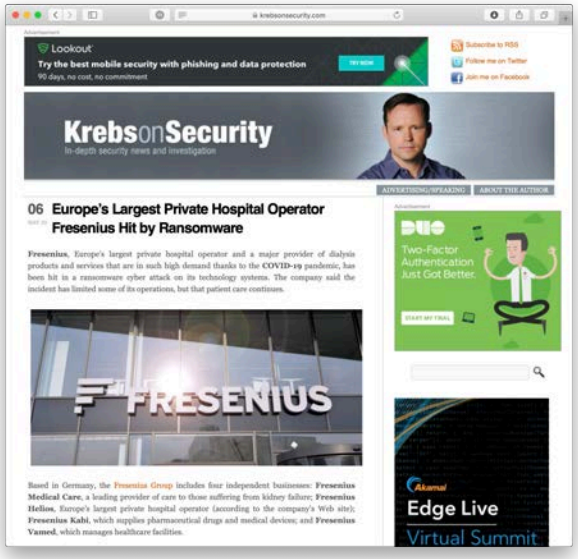
国際宅配サービスのフィッシングメールとフィッシングサイト

National Institute of Information and Communications Technology

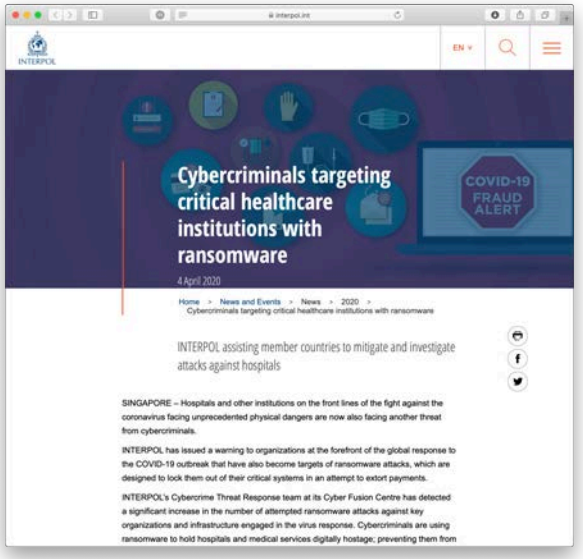
NICTER
Network Incident analysis Center for Tactical Emergency Response

医療機関を狙った標的型ランサムウェア

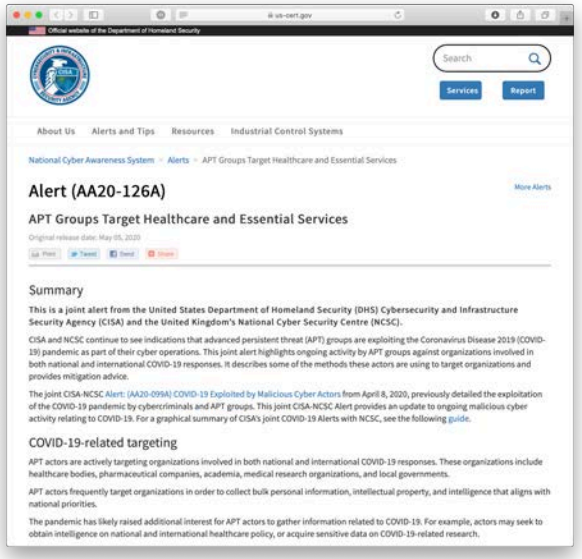
- **ランサムウェア**：感染端末のデータを暗号化し**復号の見返りに金銭を要求するマルウェア**
- 医療機関をターゲットにした**標的型ランサムウェア**の出現
  - ✓ 2016年：米国Hollywood Presbyterian Medical Center ➡ 1万7000ドルの身代金を支払いデータ復旧
  - ✓ 2018年：奈良県宇陀市立病院 ➡ 電子カルテシステムの利用が不可能に
- 欧州最大の**民間病院運営会社『Fresenius』**がランサムウェアに感染（2020年5月）
  - ✓ Freseniusは過去にもマルウェア感染し150万ドルを支払ったことがあるらしい[#1]
  - ✓ INTERPOL[#2]とDHS[#3]から医療機関を狙った標的型ランサムウェアに注意喚起



[#1] Krebs on Security
https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/



[#2] INTERPOL
https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware



[#3] DHS
https://www.us-cert.gov/ncas/alerts/AA20126A

在宅勤務

今すぐできる！WFH環境のセキュリティ対策 6選

1. IoT機器※の再起動（揮発型のマルウェアを消滅させる）
2. ファームウェアのアップデート（脆弱性を塞ぐ）
3. ID/パスワードを変更（初期パスワードでの侵入を防ぐ）

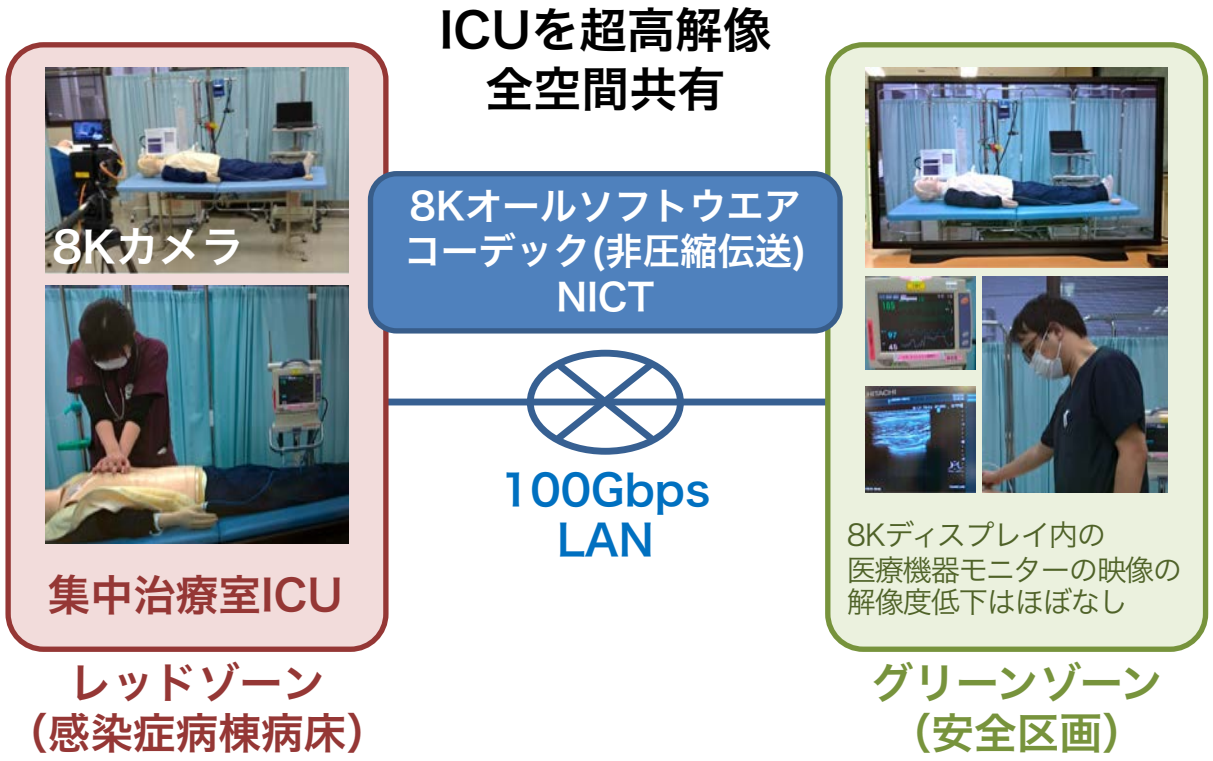
4. インターネット側からのアクセス拒否設定（外から繋がせない）
5. ゲートウェイ機器の内側に設置（直接インターネットに繋がない）
6. 古い機器は買い換える（自動アップデート機能がない機器はNG）

※IoT機器：ホームルータ、モバイルルータ、Webカメラ、プリンタ、NAS等のネットワーク接続された機器。
更新方法や設定方法などは機器の取扱説明書や製造元のWebページをご参照下さい。

第二波・第三波に備えるNICTのSEEDs

● 超高解像全空間共有を活用した新型コロナ感染症遠隔医療（集中治療）

- ✓ 医師/看護師の感染リスクの低減、負担/ストレスの低減を目指す
- ✓ 8Kディスプレイ内のバイタルモニター、超音波エコーモニターの映像で遠隔医療（解像度の低下ほぼなし）



● IoT無線技術を使った自律走行ロボットの構内誘導技術とモノ・データの自動収集・配信技術

- ✓ NFC/GPS・Wi-SUN・ミリ波を融合利活用

※JR東日本商事・アンドロボティクス社と連携して実証実験を予定

まとめ

●新型コロナウイルスとICTの光と闇

- ✓ICTによる**働き方大改革**
- ✓コロナに便乗したサイバー攻撃（定常運転）

●第二波・第三波に備えた研究開発

- ✓NICTのSEEDs vs 現場のNEEDs
- ✓基礎研究から実戦配備への迅速な展開
- ✓**普段使いが重要**