医療機関へのサイバー攻撃の実態と出来ることから始める対策　1

美代賢吾（みよけんご）
国立高度専門医療研究センター(JH)　医療研究連携推進本部
国立国際医療研究センター(NCGM)　医療情報基盤センター（CMii）

講師紹介

- 研究分野

  医療情報学（電子カルテ開発、情報セキュリティ、医療物流・メディカルロジスティクス）

- 医療情報に関わる主な経歴

  東京大学医学部附属病院中央医療情報部助手、神戸大学医学部附属病院医療情報部副部長・講師、東大病院企画情報運営部准教授・部長を経て、2017年にNCGMに異動、現在NCGM CMiiセンター長。

  2020年からは、JHデータ基盤課長も兼務

  2008年から2009年にドイツ連邦共和国 Peter L. Reicherz 医療情報学研究所にて、Prof. Dr. Reinhold Haux（国際医療情報学会会長（当時））に師事

この講義の概要

日本においても、医療機関へのサイバー攻撃とその被害が報告されています。サイバー攻撃への対策を立てるには、まず、最近のサイバー攻撃の特徴を知り、これまでの攻撃とは異なるという認識に立つことが必要です。

次に、実際のサイバー攻撃について、具体例を示しながら説明します。どのような方法で、どのような経路で侵入し攻撃されるのかを学びます。併せて、昨今話題となった事例も紹介します。

最終的には、サイバー攻撃に対応する体制を作り上げていくことが目標ですが、まずは出来るところから始める職員への教育について、説明します。

どのような強固なシステムを構築しても、すべての職員が、それを正しく認識し、正しく使わなければ、セキュリティは守られません。医療機関幹部、医療情報担当者、医療機関職員全体が当事者意識を持って取り組むという意識の醸成を目指すことが重要です。

Center for Medical Informatics Intelligence

電医療機関へのサイバー攻撃とリスク

サイバー攻撃の実際

最近の出来事から

出来るところから始める対策

医療機関へのサイバー攻撃とリスク

これまでと、Stageが変わってきた。

一般的な病院職員の問題意識

電子カルテは、インターネットから切り離されているから大丈夫。

うちの病院には、狙われるような情報は無いよ。

医療機関を取り巻くサイバー攻撃の三つの変化

■攻撃の質的な変化

- 明確な目的をもって攻撃するようになってきた

■攻撃の量的な変化

- サイバー攻撃・資金回収ツールがパッケージ化され、誰でも攻撃できるようになった

■医療機関の情報環境の変化

- IoT医療機器の普及やクラウド活用機器の増加など、医療機関のICT依存度が高まってきている

サイバー攻撃の質的な変化

■2007年9月

- Ａ大学付属病院で、システムがウイルス感染し、院内のパソコンやサーバなど約1,300台に被害がおよび、処方箋の発行や会計ができなくなるなどの影響が出た。

■2021年10月

- B病院の電子カルテシステムがランサムウェアにより電子カルテが停止。救急、新患の受け入れを中止、手術も延期し、２か月後に復旧。

■2022年10月

- C病院の電子カルテシステムがランサムウェアにより電子カルテが停止。外来診療、手術の停止

サイバー攻撃の質的な変化

■従来の脅威

- ワーム活動による端末負荷の増大
- [illegible]域の占有によるサービス
- サービス不能攻撃

愉快犯

とりあえず、
ウィルス対策ソフト

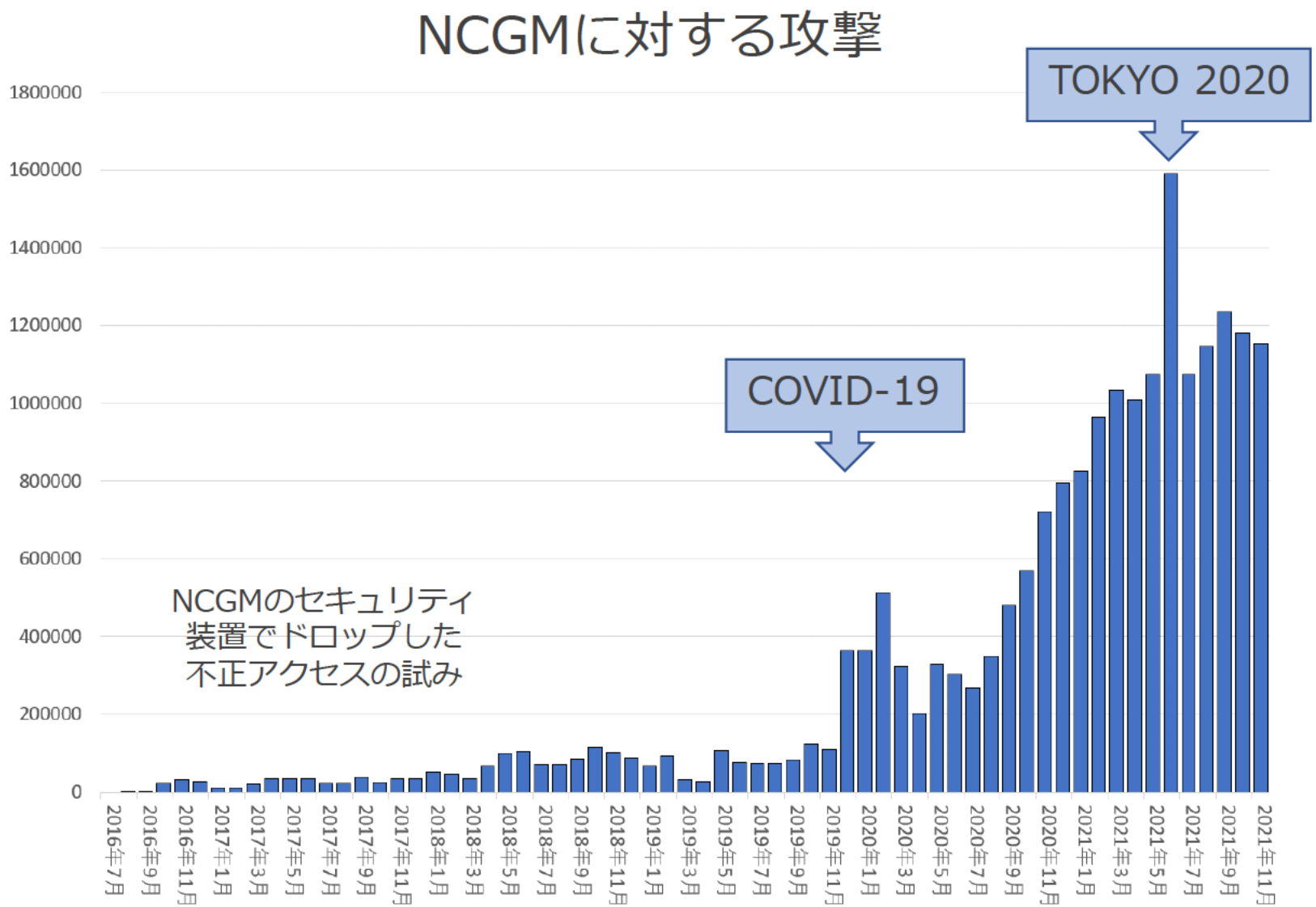
■情報・金銭[illegible]詐取を明確な目的とした攻撃ビジネス

- [illegible]
- ランサムウェア

ウィルス対策ソフトに引っかからないことを確認して送信

これまでと異なる対策が必要！

サイバー攻撃の量的な変化



医療機関の情報環境の変化

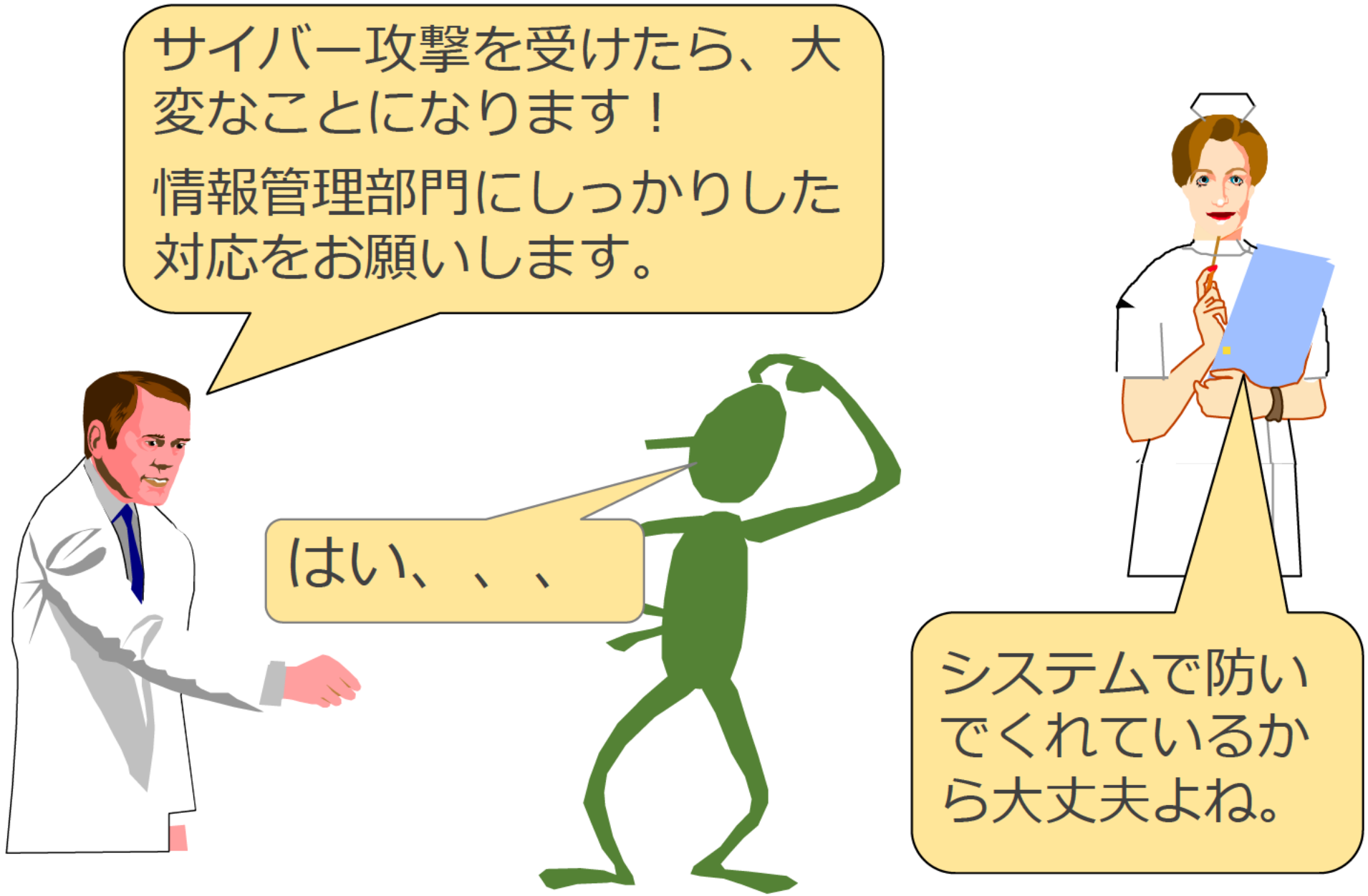
■外部ネットワークへの接続

- 電子レセプト普及率95%、健康保険証のオンライン資格確認の開始
- 医療機器のオンラインメインテナンス
- オンラインモニタリング（CGM、ペース
- PHR、地域医療ネットワークの広がり、

■IoT医療機器の増加

- バイタル測定機器のIoT化
- 医療機器のオンライン化

電子カルテからスマート輸液ポンプへのオーダ情報の送信
AMED　平成31年（令和元年）度「医工連携事業化推進事業」
（TERUMOとの共同研究）

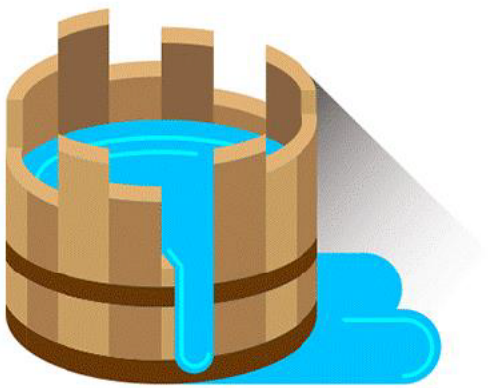


病院の情報部門／情報担当者やシステムだけで防ぐことができるのか

■これまでの事例では、**内部関係者**の**認識不足**や**過失**が引き金になったことも

■システム的な対応や体制の整備に加えて、

■管理者、スタッフを含め、医療関係者、職員全員が**当事者意識**を持つことが重要



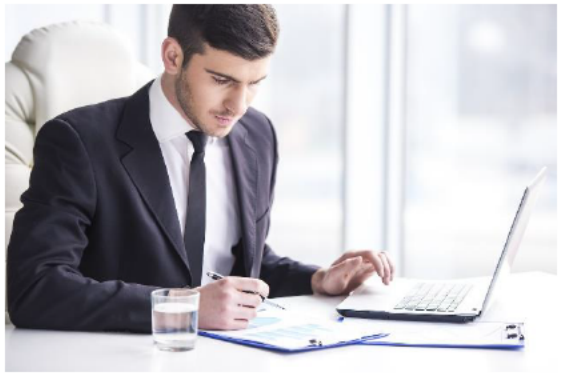
Center for Medical Informatics Intelligence

サイバー攻撃の実際

だますほうが悪いのか、

だまされるほうが悪いのか

どのように 病院から情報を盗むか



金庫をこじ開ける ＜ 銀行員をだます

セキュリティシステムを こじ開ける ＜ 病院職員をだます

フィッシング（Phishing）
（Phreaking + fishing 又は、Password Harvesting fishing）

【お詫び】フィッシングメールによる個人情報の漏えいについて

2018.06.27 更新

このたび，フィッシングメールの被害により，本学教職員の電子メールが不正転送され，メールアドレス情報を含む個人情報の漏えいが判明しました。

本学の情報管理において，このような問題が発生し，関係者の皆様に多大なるご迷惑をおかけしたこと，信頼を損ねることとなりましたことを深くお詫び申し上げます。

本学といたしましては，今回の事態を重く受け止め，真摯に対応していくとともに，再発防止に関して全学で取り組んでまいる所存です。

平成30年
国立大学法人
学　長

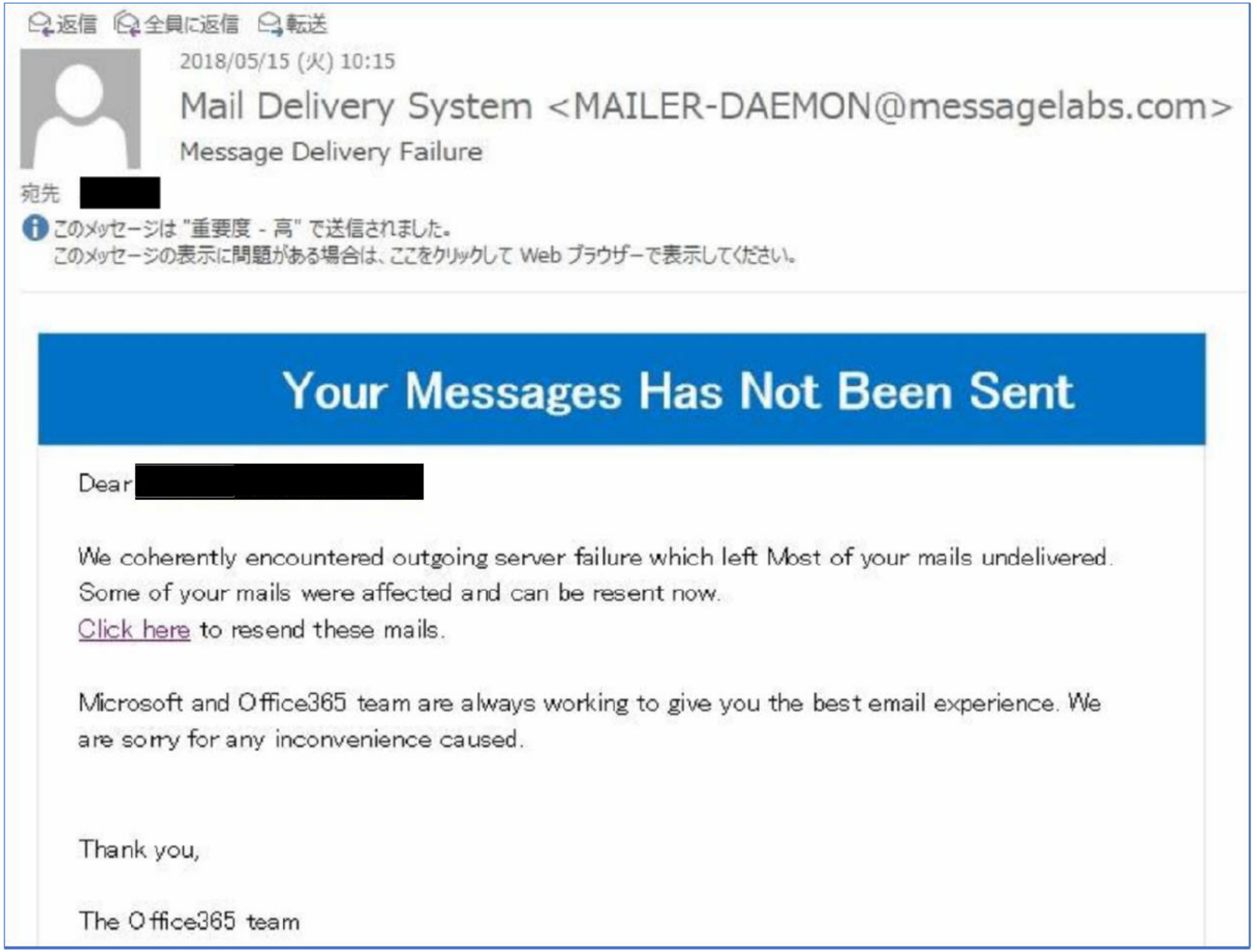
T県立大
O県立看護大
Y市立大
S大学
R大学　も！

■漏えいが確認された個人情報

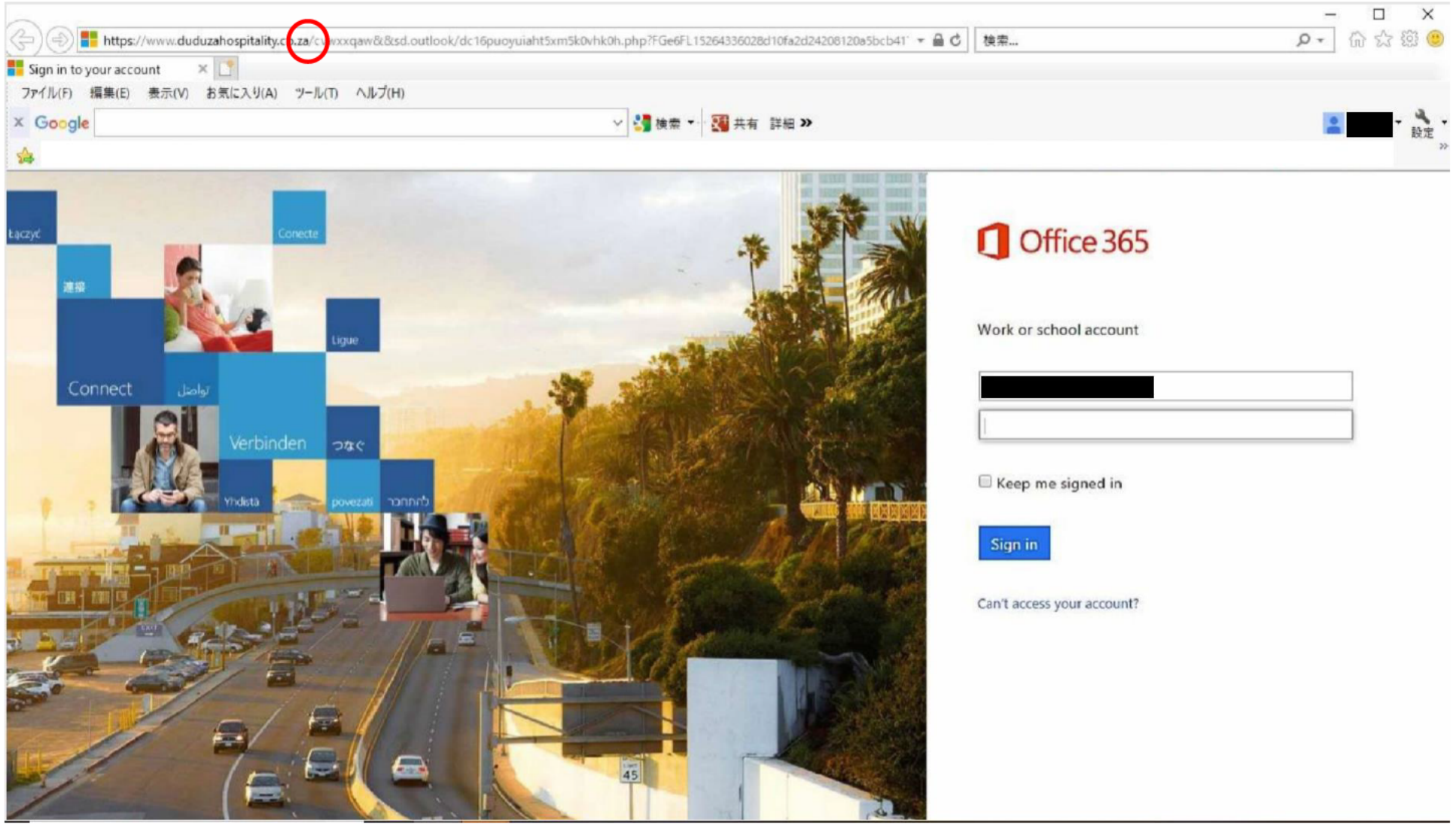
- 送受信者氏名，メールアドレス 約2,000件
- 氏名，性別，住所，電話番号等 約2,000件
- フィッシングメールが届いたアドレス数：約200件
- 不正転送設定をされたメールアドレス数：12件
- 不正転送メール数：約3,000通

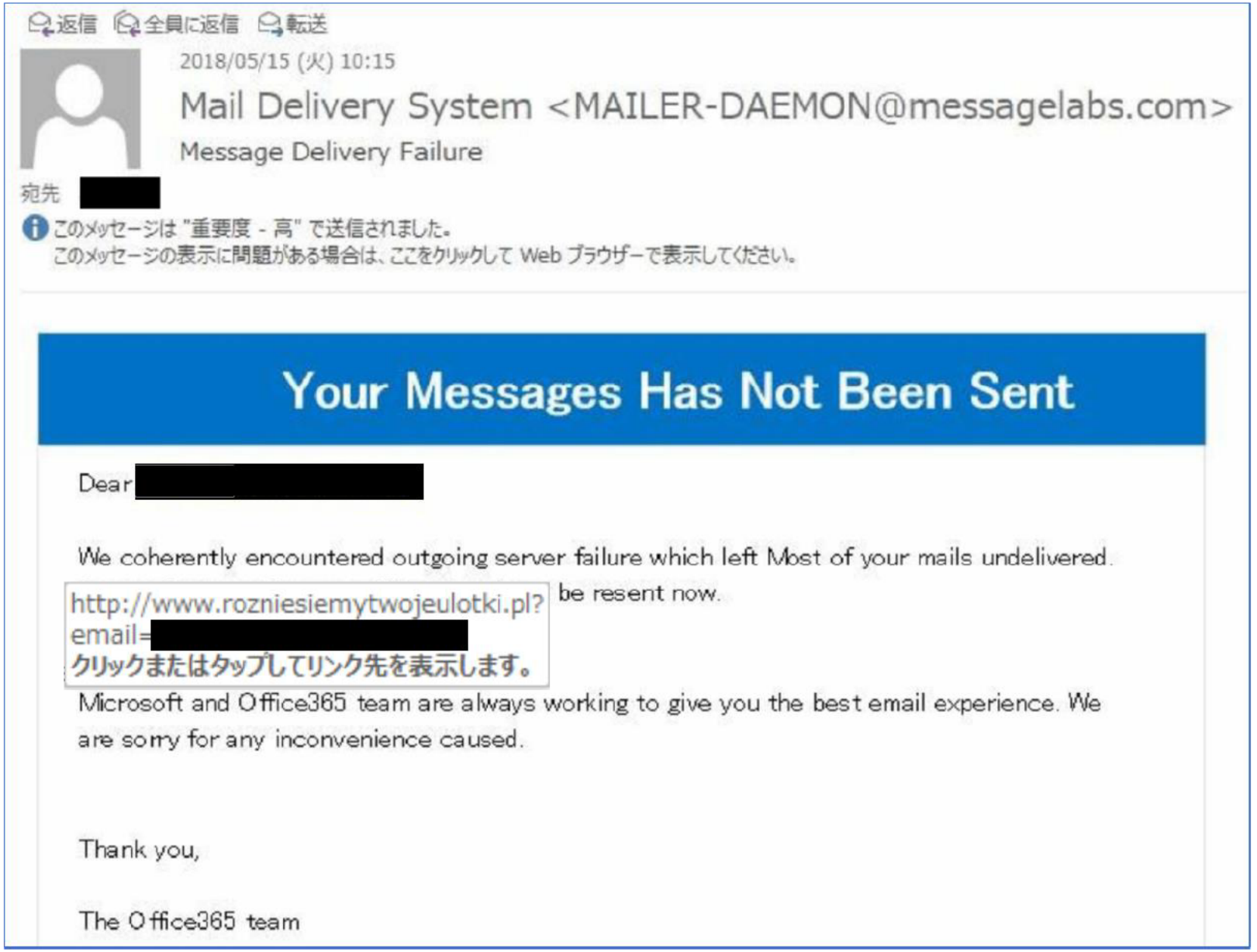
■経緯（大学報道発表より）

- ○月23日　学内利用者からの通知により，情報部門がフィッシングメールの存在を把握
- ○月24日　偽サイトへのブロック設定
- 翌月 7日　不正な転送先設定による，受信メールの流出が判明。全員の不正な転送設定を削除
- 翌月18日　学外への自動転送設定を禁止


返信 全員に返信 転送
2018/05/15 (火) 10:15
Mail Delivery System <MAILER-DAEMON@messagelabs.com>
Message Delivery Failure
宛先 [redacted]
このメッセージは "重要度 - 高" で送信されました。
このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。
Your Messages Has Not Been Sent
Dear [redacted]
We coherently encountered outgoing server failure which left Most of your mails undelivered.
Some of your mails were affected and can be resent now.
Click here to resend these mails.
Microsoft and Office365 team are always working to give you the best email experience. We are sorry for any inconvenience caused.
Thank you,
The Office365 team

.za


https://www.duduzahospitality.co.za/
Sign in to your account
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
Google
検索 共有 詳細
設定
Łączyć
Conecte
連接
Ligue
Connect
تواصل
Verbinden
つなぐ
Yhdistä
povezati
להתחבר
45
Office 365
Work or school account
Keep me signed in
Sign in
Can't access your account?


返信
全員に返信
転送
2018/05/15 (火) 10:15
Mail Delivery System <MAILER-DAEMON@messagelabs.com>
Message Delivery Failure
宛先 [redacted]
このメッセージは "重要度 - 高" で送信されました。
このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。
Your Messages Has Not Been Sent
Dear [redacted]
We coherently encountered outgoing server failure which left Most of your mails undelivered.
be resent now.
http://www.rozniesiemytwojeulotki.pl?email=[redacted]
クリックまたはタップしてリンク先を表示します。
Microsoft and Office365 team are always working to give you the best email experience. We are sorry for any inconvenience caused.
Thank you,
The Office365 team

利用者

攻撃者

フィッシングメール

IDとパスワード
入力

IDとパスワード
詐取成功

９時５０分２７秒

１０分かからずに
アタック開始

詐取したIDとパスワードでログイン試行

９時５９分

NCGMでは、多要素認証を採用しているため、不正アクセスは無し

Center for Medical Informatics Intelligence

最近の出来事から

ランサムウェア被害により

２か月間電子カルテが停止

被害総額は３億円

リモートメンテナンスからの侵入

どのように **病院から情報を盗むか**

金庫をこじ開ける ＜ 裏口から入る

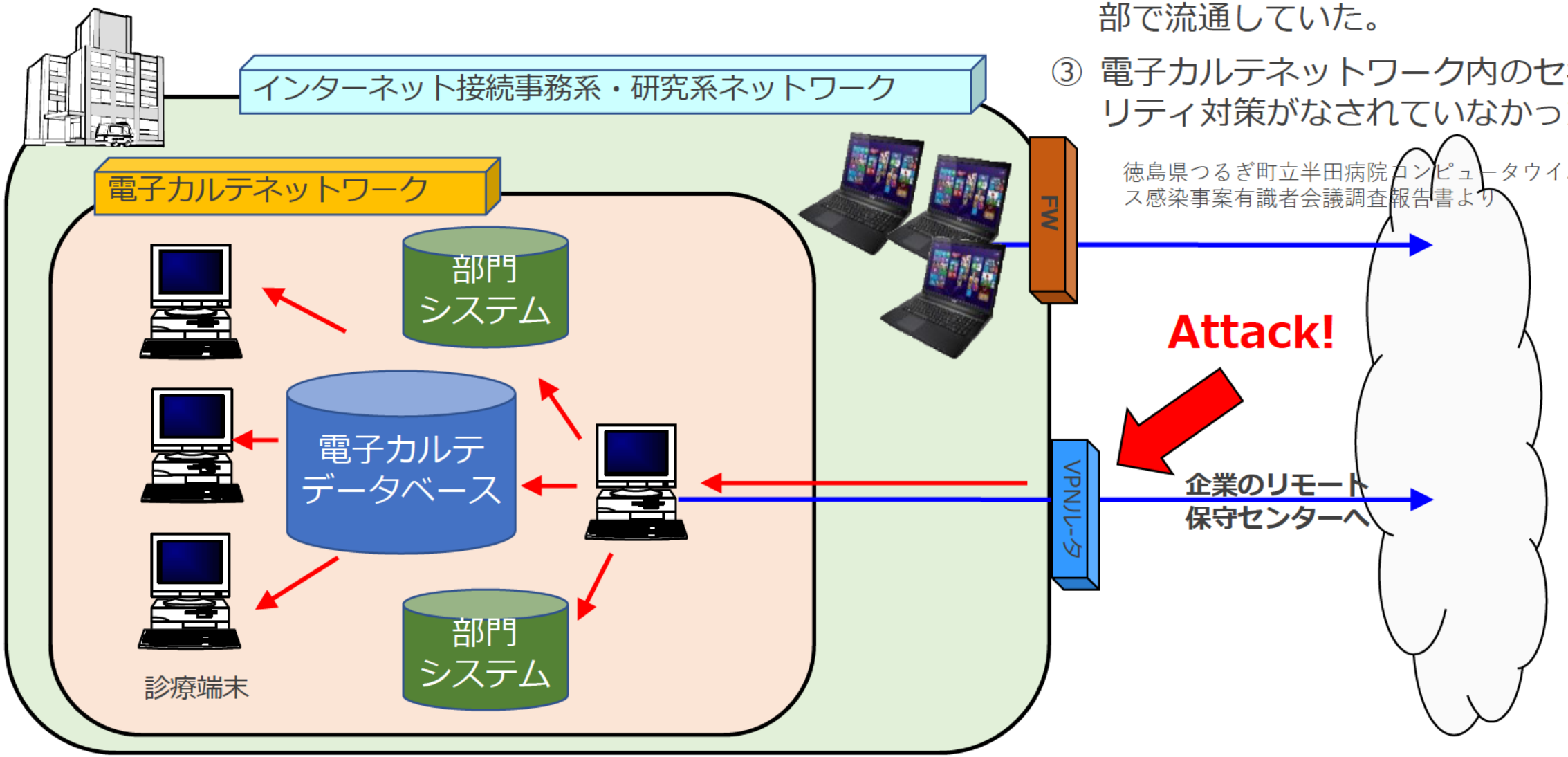
セキュリティシステムを こじ開ける ＜ リモートアクセス の入り口から入る

徳島県の公立病院でのランサムウェア事例

① VPNルータのソフト（firmware）がアップデートされていなかった。

② VPNルータのID、パスワードが外部で流通していた。

③ 電子カルテネットワーク内のセキュリティ対策がなされていなかった

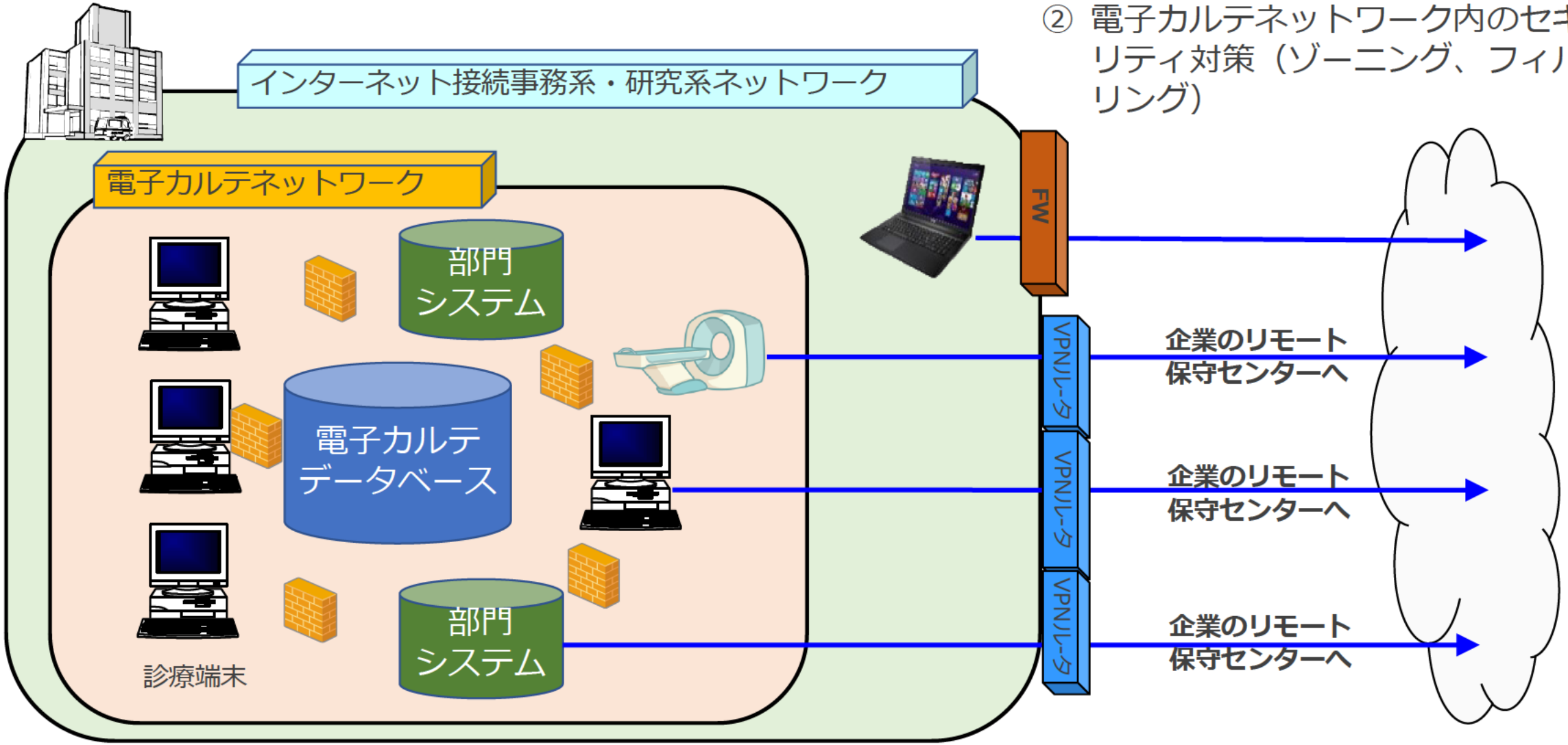


徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書より

増加するリモート保守への対策

① VPNルータの把握と管理状況の確認

② 電子カルテネットワーク内のセキュリティ対策（ゾーニング、フィルタリング）



出来るところから始める対策

情報セキュリティポリシーの策定
情報セキュリティ監査
ペネトレーションテスト

情報セキュリティ機器の導入
情報セキュリティソフトウェアの導入
SOCサービスの契約

入り口対策
出口対策
エンドポイント対策
被害拡大防止対策
データバックアップ

そして、教育・研修

ある組織のある事例より

メールシステム

SPAMとして隔離

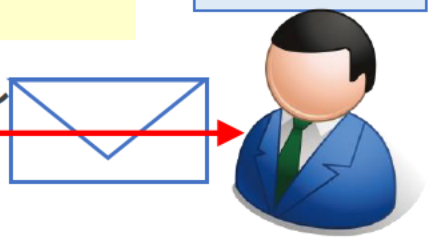
攻撃者

フィッシングメール

実在する会社を騙った
注文確定メール

利用者

隔離フォルダから取り出し



PDFに偽装

メール開封

添付文書を開く
お問い合わせをクリック

管理者

不正通信検知・警報

LAN抜線

2時間後に
自分でウィルススキャン

何もなかったので、
自己判断で接続

不正通信検知・警報

LAN抜線

攻撃対策と医療情報システム安全管理者の役割

- システム的な対応をおこなう
- インシデントがあれば、駆けつけて対処する
- 病院幹部に説明しセキュリティ予算を確保する

どんな対策をとっても、この人みたいに自分でチーズの穴を開ける職員がいる

- 職員に対する、事例を用いた具体的な情報セキュリティ教育
- 対策の具体的で簡潔な指示

個人情報保護のために職員が守るべき情報セキュリティ対策　第2.2版

2020.7.20

情報委員会　個人情報保護委員会
医療情報基盤センター

侵入を防ぐ

- ウィルス対策ソフトを必ず導入する。
- OS、Officeアプリケーション、PDFリーダー、Flashなどは、必ず定期的にアップデートする。
- Windows XP、Vista、7は業務系ネットワーク接続禁止。
- 夜間・休日等でパソコンを利用しない場合、電源を切る（特にGW、SW、お盆、年末年始）。
- 添付ファイルのあるメール※の、添付ファイルは安易に開かない。
- クリックを促すようなメール※の、クリックは安易に行わない。

※一見して不審だとは判別できないものが、多い、以下を総合的に判断すること。違和感を感じたり、迷ったら連絡を

1. 添付ファイルを開いても期待されたものが出ない。（マルウェアの可能性が極めて高い。即時連絡）
2. フリーメールからの業務を装ったメール
3. 暗号化されたzip形式の添付ファイル
4. メール本文に、リンク先（特に日本国外：末尾がjp以外）が書かれていて、クリックを促すような内容

個人情報を護る

- 個人情報が入ったファイルは必ず暗号化する（パスワードは8文字以上の英数記号）
- 個人情報をUSBメモリなどの外部記憶装置にダウンロードする場合は、匿名化または暗号化する。個人情報は、敷地外へ持ち出さない。
- Twitter、Facebook等のSNS、ブログで、非公開であっても個人情報は絶対に発信しない

被害の拡大を防ぐ

- 万が一、添付ファイルを実行したり、リンクをクリックしてしまった場合は、パソコンを直ちにネットワークから切断（有線・無線）し、即、医療情報基盤センター（■■■■）または当直（■■■■）に連絡。
- ウィルス感染、個人情報流出が確認された場合は、いかなる理由（業務上、研究上）があろうと、ただちにネットワークから切断する措置を取る。
- 安全が確認されるまでは再接続は認めない。

ＮＣＧＭの最近の傾向

■従来は、クリックした後に心配になって連絡

■最近は、利用者が自発的に連絡してくれるようになった

- 後輩を名乗る人物からメールが届いたが、同窓会名簿を確認したら名前がなかった
- 留守番録音があるとの通知がOffice365から来たが、差出人のアドレスが怪しかった

- フィルタリング
- 他に着弾がないか調査
- 職員に「具体的な内容を見せて」周知

- 外国から受賞の連絡が来たが本物か？ → **意外と本物だった('O'*)**

■マルウェアを実行する前と後では、労力が100倍違う

・標的メールも**クリックしなければ、ただのごみ箱行きメール**

■情報教育・研修と、情報共有が重要

おわりに

- 利用者が安易に踏まないような教育・研修を
  - 具体的な事例紹介、標的型訓練
- 利用者が気軽に相談できる窓口と担当者を
  - 医療安全と同じ。責めるのではなく、原因分析と対策を
- 体制とシステムを整えていこう
  - リスクを評価しメリハリのある対策と職員全体を巻き込む体制を
- サイバー攻撃対策は投資という視点を
  - 情報システムと医療は、ますます密接に。病院幹部はそのリスクと、対策の必要性の認識を