個人情報保護法改正対応
サイバーセキュリティセミナー

八雲法律事務所
弁護士　山岡裕明

講師紹介

◆ 八雲法律事務所
- 弁護士（2010年登録）
- 情報処理安全確保支援士（2016年登録）

◆ 経歴
- University of California, Berkeley, School of Information, Master of Information and Cybersecurity

◆ 役職等
- University of California, Berkeley, 客員研究員（2019-2020）
- 内閣サイバーセキュリティセンター（NISC）タスクフォースメンバー（2019-2020, 2022）
- 総務省・経産省・警察庁・NISC「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」検討委員（2022~）

目次

1 ランサムウェアの傾向

■従来のランサムウェア

感染端末の暗号化

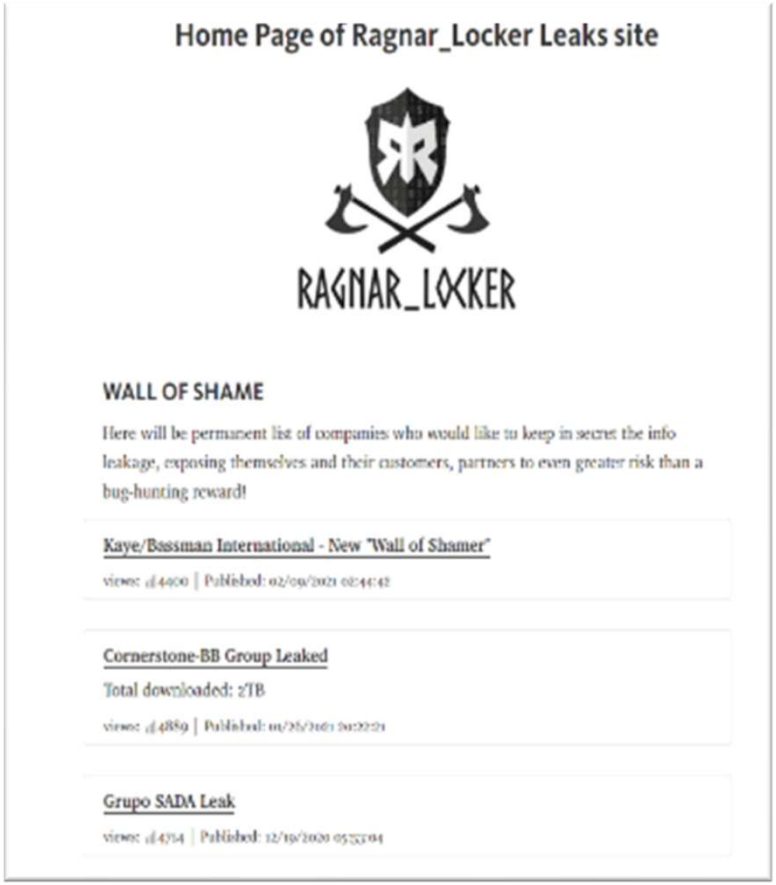
→復旧（復号）と引き換えに身代金（ランサム）を要求。

引用元：行政法人情報処理推進機構（IPA）HP

1 ランサムウェアの傾向

■近事のランサムウェアの特徴

従来のデータ暗号化に加え、データを窃取して、リークサイト上で公表する。



→データの非公表と引き換えに身代金（ランサム）を要求。

1 ランサムウェアの傾向

■二重の脅迫型（Double Extortion）

✓ 暗号化＋データの窃取（2020年8月20日IPA「事業継続を脅かす新たなランサムウェア攻撃について」）

✓ 単なる暗号化よりも被害者にとって支払うインセンティブが強まる

1 ランサムウェアの傾向

■情報漏えい被害

✓ カプコン（北米現地法人）

✓ HOYA（米国子会社）

✓ ダイハツ（欧州現地法人）

✓ 鹿島建設（北米グループ会社）

✓ 東芝テック（欧州現地法人）

2 ランサムウェアによる被害実態

■　暗号化被害

１．HONDA

2020年6月8日、ランサムウェアの攻撃を受けて、イギリスのスウィンドン工場のほか、北米、トルコ、イタリアなど9つの工場が影響を受けて生産を一時停止。日本でも完成車の検査システムが不調になり、車を生産する3工場の一部で出荷を一時見合わせ。12日に復旧。

２．米国コロニアル社

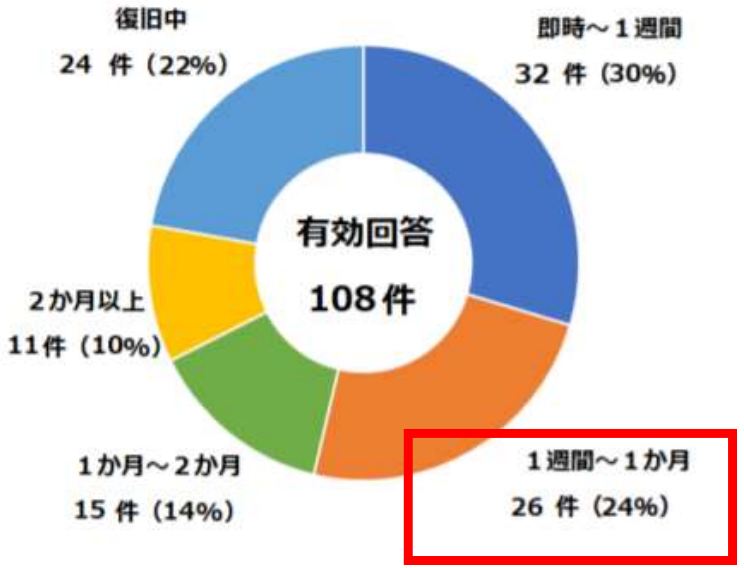
米国東海岸の燃料消費の半分近くのシェアを占める社会的インフラを担う企業であるところ、2021年5月7日にランサムウェア攻撃を受けたことが発覚。全てのパイプラインが稼働するまでにおよそ約1週間。

３．徳島県の病院

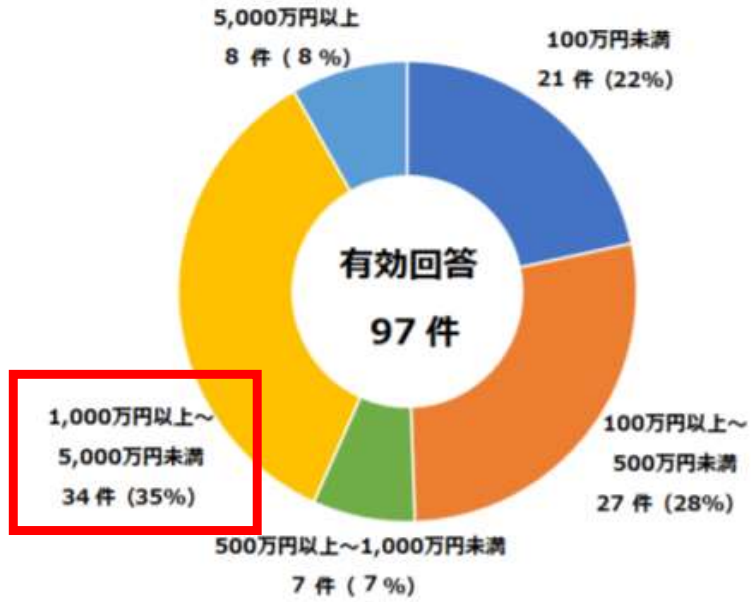
2021年10月31日、8万5千人分の電子カルテが暗号化され、新規外来や入院患者の受け入れを中止。新システムに切り替えゼロからカルテを再構築するには約2億円。同年12月29日復旧。

2 ランサムウェアによる被害実態

【図表７：被害からの復旧に要した期間】



【図表８：被害の調査・復旧に要した総額】



2022年4月7日付警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について 」

ソフォスホワイトペーパー2022年4月「ランサムウェアの現状2022年版」

2 ランサムウェアによる被害実態

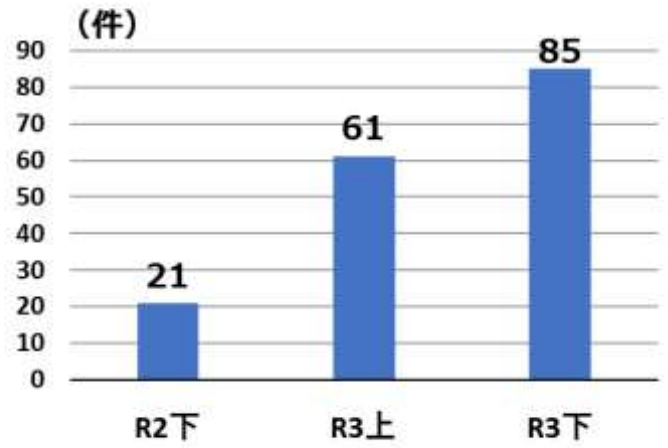
■傾向

✓ IPA「情報セキュリティ10大脅威2022」組織編　第1位

✓ 2020年下半期21件が、2021年上半期61件、同年下半期85件

2022年2月10日付警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」

【図表１：企業・団体等におけるランサムウェア被害の報告件数[*] の推移】



2 ランサムウェアによる被害実態

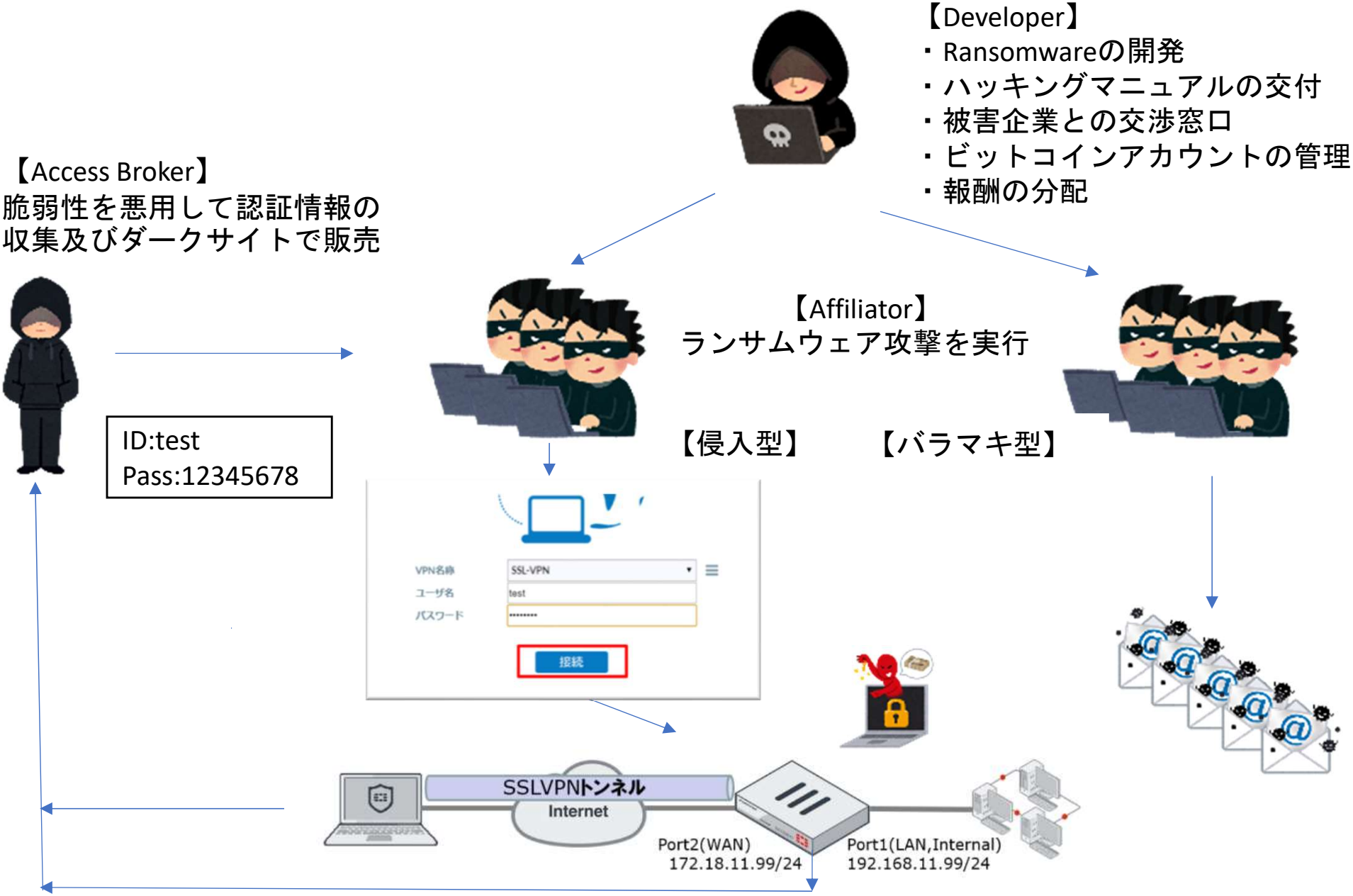
Date	Event
5/1	製造業X社の社内ネットワークに置かれたPC3台、ファイル共有サーバー1台及び工場制御システムが暗号化されたことが発覚。被害PCに残されたランサムノートには「情報を窃取した。72時間以内に10Bitcoin（5000万円相当）を支払わなければ、窃取したデータを公開する。また、身代金を支払えば復旧するための鍵を渡す」と記載されていた。
	事前の対応方針に従って ・全端末をネットワークから隔離 ・制御システムへの影響の調査開始 ・暗号化及び窃取されたデータの範囲を確認 ・暗号化されたデータのバックアップの有無の確認
5/2	専門事業者（フォレンジック会社、弁護士、セキュリティコンサル）に依頼
	ダークウェブ上のリークサイトに、窃取された情報の一部が公開されていることが判明
	工場制御システムの復旧には一ヶ月掛かり、その間、製造を停止さざるを得ないことが判明
5/3	支払ってもデータ及びシステム復旧並びにデータ非公開の保証はないことから身代金を支払わないことを決定
6/1	工場制御システムのOSを再インストールして、試運転を経て、製造再開。
6/30	フォレンジック調査の結果、不正アクセスの経路及び漏えいしたデータの範囲が判明
7/5	今後の対応方針を取締役会で決定のうえ、個人情報保護委員会、警察に届け出
7/6	Webサイト上でプレスリリース
	取引先への個別説明
8/30	再発防止策の策定完了

3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景

- ✓ RaaS（Ransomware as a Service）の普及。
- ✓ Ransomware攻撃のコモディティ化
- ✓ Developer 、Affiliator、Access Brokerの分業

3 ランサムウェアの増加の背景　RaaS



3 ランサムウェアの増加の背景　RaaS

REvil ransomware deposits $1 million in hacker recruitment drive

By Lawrence Abrams

The REvil Ransomware (Sodinokibi) operation has deposited $1 million in bitcoins on a Russian-speaking hacker forum to prove to potential affiliates that they mean business.

Many ransomware operations are conducted as a Ransomware-as-a-Service (RaaS), where developers are in charge of developing the ransomware and payment site, and affiliates are recruited to hack businesses and encrypt their devices.

https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/

Thus, we:
1. Expand the composition of the teams of acting advertisers with talented people;
2. We invite ready-made lineups to work with us;
All this is aimed at one thing - to increase the quality and quantity of waste material, which entails an increase in profits. But this does not mean that everyone will be accepted.

For your peace of mind and confidence, we have made a deposit of 1 million US dollars.

Last edited: Today at 15:29

3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景

DeveloperからAffiliatorへのハッキングマニュアルの交付

MANUAL COBALT STRIKE

! ---------- ----- Standard Commands ----------!

Create load
Attacks-> Packages->

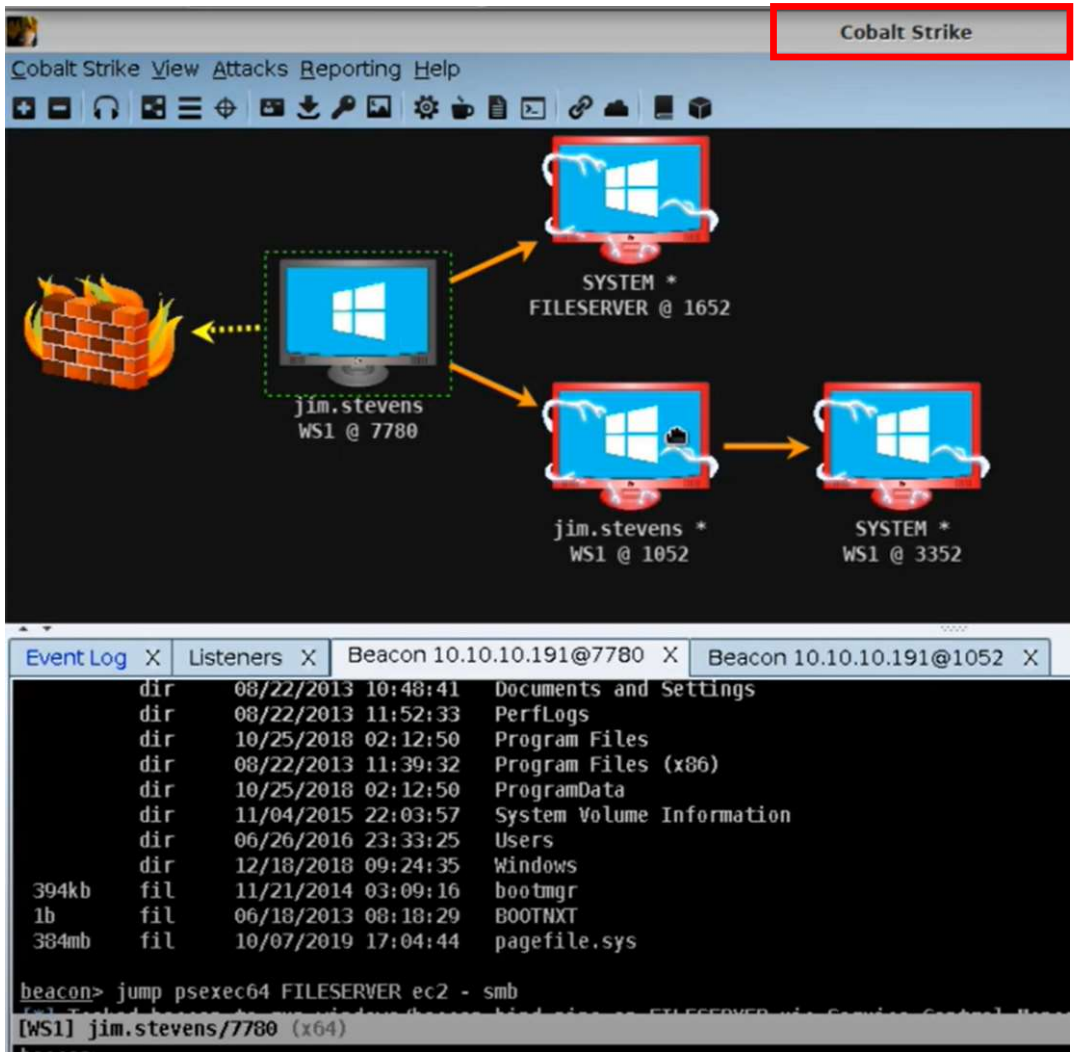
interact - select agent
help -> will show a list of commands
help [command] will show help for a specific command

! ---------- ---------- Gathering AD Information ----------!

! --- Get the Controller Domain ---!
net[1] domain_controllers
net dclist[2]
shell nltest / dclist

! --- Get a list of computers ---!
shell net group "Domain Computers" / domain
net computers
net view[3]
Get-ADComputer -Filter {enabled -eq $ true} -properties * | select Name, DNSHostName, OperatingSystem! - Test--!

! --- Getting a list of subdomains ---!
net domain_trusts
shell nltest / DOMAIN_TRUSTS



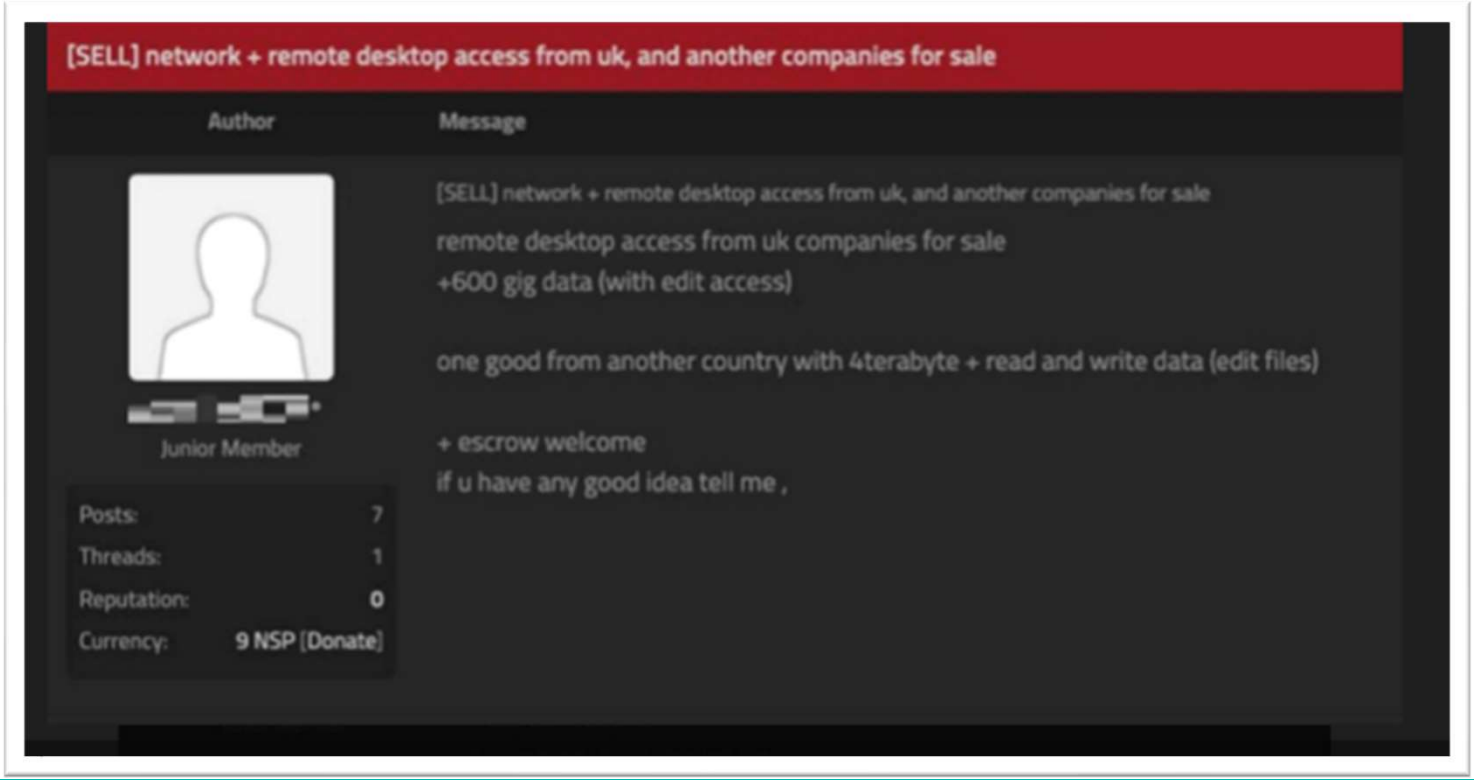
3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景

ログイン情報の売買

「過去1年弱の間に、システムへの侵入に使うログイン情報などのデータが少なくとも900件以上売り出され、多くが100ドル（約1万1000円）前後で取引されていた。ハッカーなど犯罪者が購入し、サイバー攻撃の急増につながっている」

（2021年8月1日日経新聞「サイバー攻撃、進む分業「侵入口」100ドルで闇取引」）



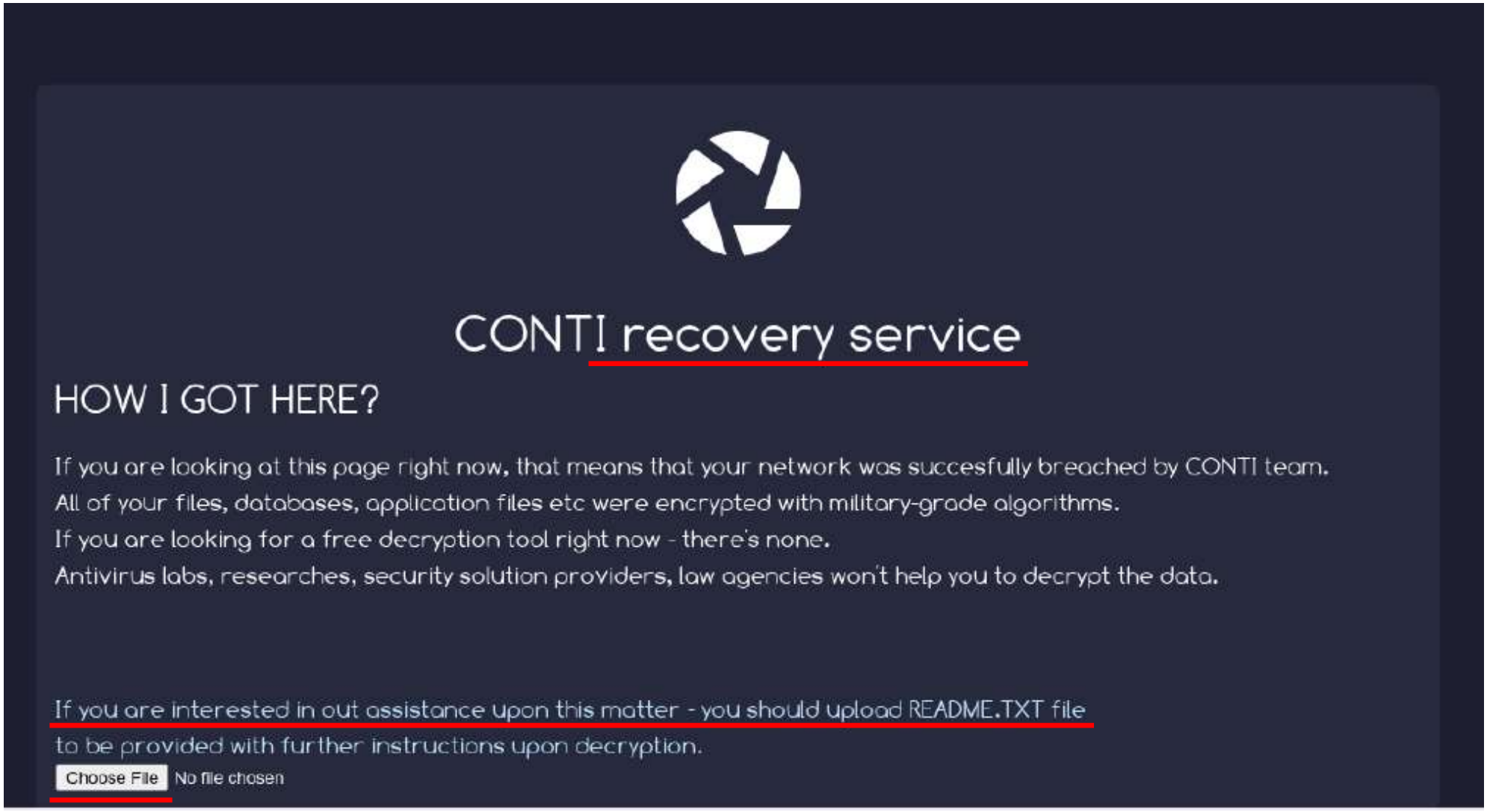
3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be
recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try
it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of
charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on
out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
ZgBgoJLOiFHQWDwueq1qE5rPeLoE7uij5d35sty227lDLOdE3MSdglpkbJd8T2u3
---END ID---
```

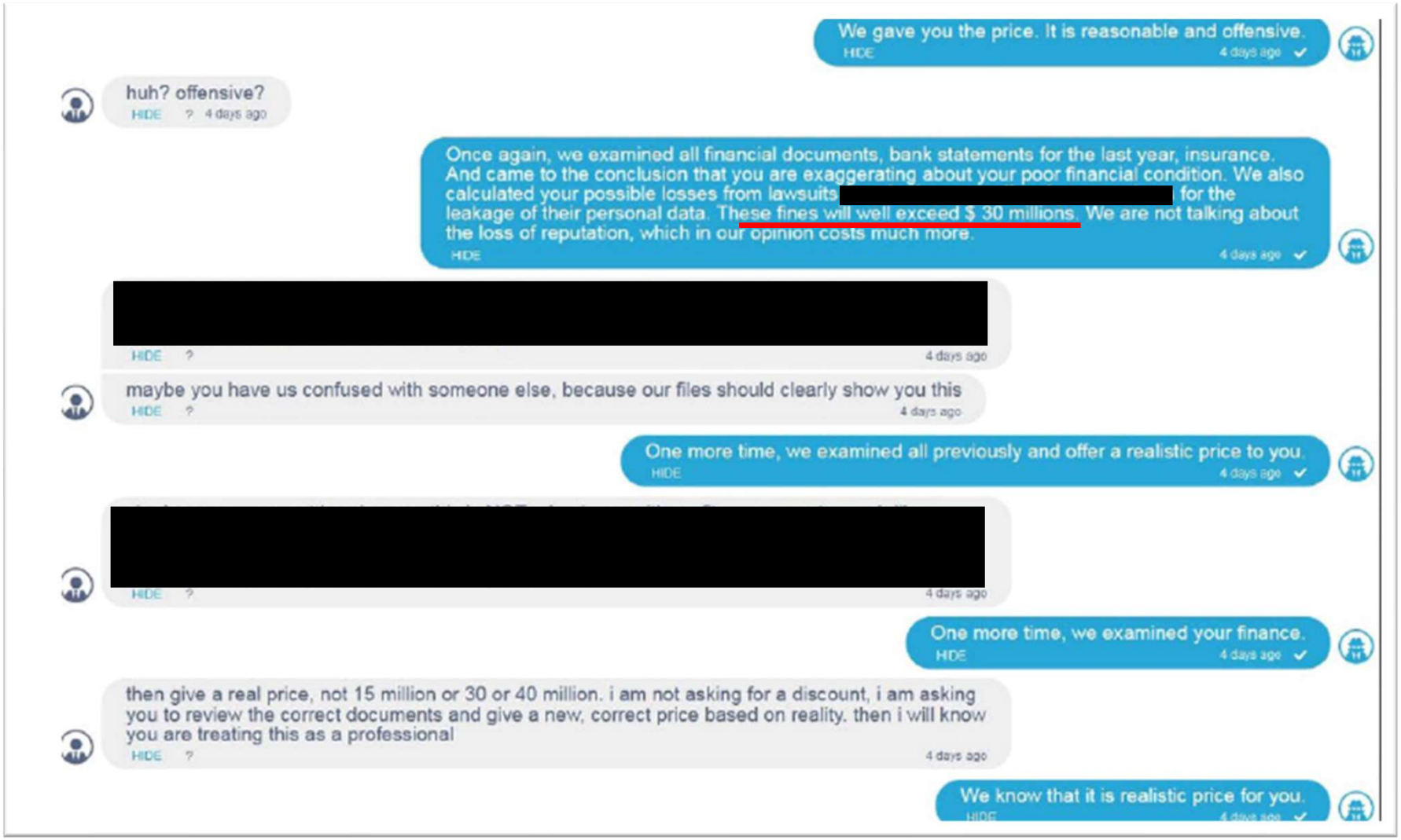
3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景



3 ランサムウェアの増加の背景　RaaS

■増加傾向の背景



4 ランサムウェアの被害に遭った場合の留意点

👉経営陣が意思決定を迫られる。

<table>
<tr><th></th><th>インシデント発生時点</th><th>身代金に対する意思決定時点</th></tr>
<tr><td>サイバー
インシデント一般</td><td rowspan="2">✓ インシデント発生に伴う一般的な対応が必要となる（ ex.フォレンジック調査、公表、当局対応、ユーザー対応等）。</td><td></td></tr>
<tr><td>ランサムウェア
攻撃</td><td>支払うor支払わない、という意思決定を経営層は迫られる。そして、その意思決定の適法性・妥当性が問題となる。

👉経営層からの問い合わせ。</td></tr>
</table>

4 ランサムウェアの被害に遭った場合の留意点

■　身代金の支払うことのリスク

◘ 経済的リスク

身代金相当額の出捐を伴う（最近は数億円単位。）。

◘ リーガルリスク・コンプライアンスリスク

ハッカー集団に金銭的価値を提供する。違法行為の助長につながる。

法令に違反しないか？善管注意義務に違反しないか？

◘ 効果が保証されないリスク

- ハッカー集団に身代金を支払うことで復旧につながるのか（復号化鍵を渡してくるのか）？
- リークサイト上での公開を止めてくるのか？
- 一時的に対応してくれたとしても、将来的に繰り返し請求してこないか？

「80% of those who paid a ransom experienced another attack」
(cyberreason社2022年6月”Ransomware The True Cost To Buiness”)

4 ランサムウェアの被害に遭った場合の留意点

■　身代金を支払うことのリスク

✓ 2020年12月18日経産省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

「金銭の支払いに関する問題である。データ公開の圧力から、攻撃者からの支払い要求に屈しているケースは少なくないとの報告は存在するが、こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等 の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。 金銭の支払いに対する対応は、複数の視点から自社への信頼をどのように維持するか、また、犯罪助長行為として支払い行為に対する制裁を用意する国もある中でコ ンプライアンス上の問題にどう対応するか、ということであり、経営者が判断すべき経営問題そのものであるということを強く認識する必要がある。」

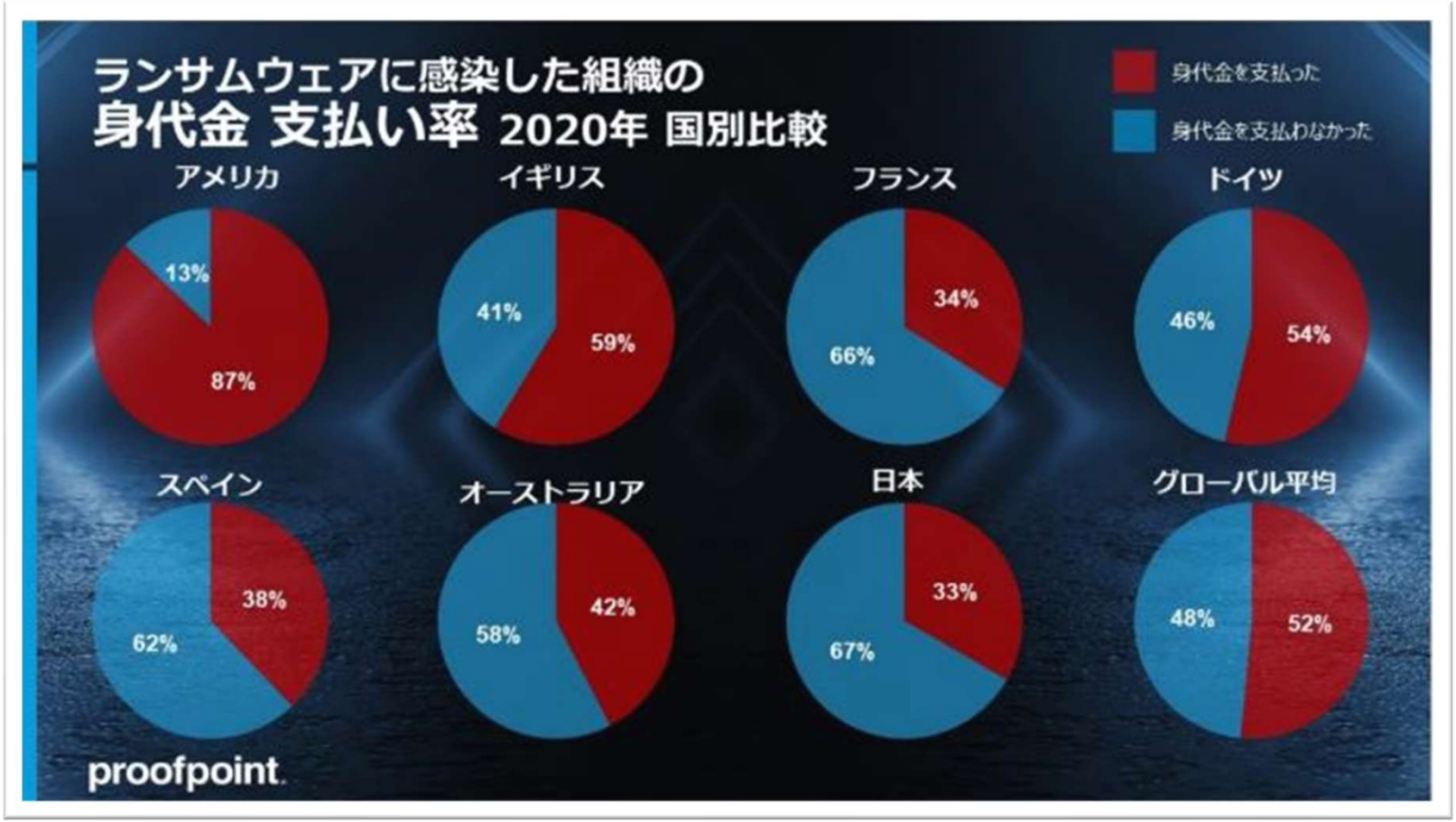
4 ランサムウェアの被害に遭った場合の留意点

■　身代金を支払わざるを得ない場合の考慮要素

事業継続	✓ 社会インフラが暗号化によって止まるリスク（石油パイプラインの例） ✓ 病院のシステムが暗号化によって止まるリスク。
情報漏洩	✓ 取引先の機密情報が公開されるリスク（ワクチン、技術情報） ✓ 個人ユーザーのセンシティブ情報が公開されるリスク

「私は、パイプラインの早期復旧するために利用可能なあらゆるツールを入手すべく身代金を支払うという意思決定を行った。…人生で最も大変な意思決定の一つであった。（I made the decision that Colonial Pipeline would pay the ransom to have every tool available…It was one of the toughest decisions I have had to make in my life）」
(コロニアル社CEO Joseph Blount氏。2021年6月8日の上院委員会での証人喚問にて)

4 ランサムウェアの被害に遭った場合の留意点



【出典】proofpoint「身代金を支払うのは正解か？ ― ランサムウェア支払い結果７か国比較から考えるサイバー犯罪エコシステムへの対処」

https://www.proofpoint.com/jp/blog/threat-insight/is-it-right-to-pay-the-ransom

4 ランサムウェアの被害に遭った場合の留意点

■ 法的留意点１：各国のレギュレーション

✓ OFAC規制

- 財務省外国資産管理室（The U.S. Department of the Treasury's Office of Foreign Assets Control。通称「OFAC」）は、「ランサムウェアの支払いを助長することに関する潜在的制裁リスクについての勧告」（Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）を公表。
- Strict Liability（無過失責任）で制裁金が巨大（BNPパリバ事件では9,100億円）
- OFACは、サイバー関連制裁プログラム（cyber-related sanctions program）を設け、同プログラムの下で、悪意あるサイバー行為者を指定したリスト（「SDNリスト」）を公表し、その中には、ランサムウェアを用いた攻撃者やランサムウェア関連の取引を助長した者が含まれる。
- そして、この指定された者と取引を行うことが禁じられている。
- OFACは、同勧告において、「被害企業に代わってランサムウェアの支払いを助長する金融機関、保険会社、デジタルフォレンジック企業及び危機対応企業といった企業は、将来のランサムウェアの支払い要求を促進させるだけでなく、OFAC規制に違反するリスクがある」ことを示した。
- SDNリスト掲載者との取引は、域外適用あり（日本企業も対象になり得る。）。

4 ランサムウェアの被害に遭った場合の留意点

■法的留意点2：国内の規制

- 支払いを直接禁じる規制は無し。
- 犯罪集団への資金提供を禁じる法律としては、テロ資金提供処罰法（公衆等脅迫目的の犯罪行為のための資金等の提供等の処罰に関する法律）がある。同法3条1項は、「公衆等脅迫目的の犯罪行為の実行を容易にする目的」での犯罪行為者への資金提供等を禁じている。この点、暗号化されたデータの復元や窃取されたデータの公開防止を目的として身代金を支払った場合は、同法が禁じる目的が存在せず、同項に該当しないと考えられる。

4 ランサムウェアの被害に遭った場合の留意点

■法的留意点３：役員の善管注意義務と経営判断原則との関係

- 2022年6月17日サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」によると、「組織におけるサイバーセキュリティに関する体制は、その組織の内部統制システムの一部といえる。経営層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る。」「組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠（けたい）に基づく損害賠償責任を問われ得る。」
- サイバーセキュリティ体制の構築に加え、身代金に係る決定は、経営判断そのもの。諸般の事情を考慮した総合判断となる。
- 経営判断と善管注意義務については、「その決定の過程、内容に著しく不合理な点がない限り、取締役としての善管注意義務に違反するものではない」とされている（最判平成22年7月15日判タ1332号50頁参照）

  👉判断過程の合理性：専門家から意見を聴取しているか。

４ ランサムウェアの被害に遭った場合の留意点

■法的留意点４：契約責任

- 取引先の企業情報が漏えいすると、取引先との機密保持義務違反に基づく責任追及を受ける可能性がある。例えば、損害賠償請求、契約の解除、大型の取引の停止

- 大阪商工会議所が2019年に実施した調査では、取引先がサイバー攻撃を受けて自社に被害が及んだ場合、29%の企業が『取引停止』を検討すると回答した。（日経新聞2020年9月16日）

４ ランサムウェアの被害に遭った場合の留意点

■法的留意点５：改正個人情報保護法との関係

① 2022年4月1日施行

② 個人情報保護委員会への報告を義務化

- ◆ 速報：「当該事態を知った時点から概ね３～５日」
- ◆ 確報：原則30日以内（一定の事由がある場合は60日以内）

③ 本人への通知義務化

- ◆ 「知った後、当該事態の状況に応じて速やかに」通知する義務

④ 罰則

- ◆ 個人情報保護委員会による勧告・命令
- ◆ 命令に違反した場合は公表
- ◆ 違反した法人に対しては1億円以下の罰金

4 ランサムウェアの被害に遭った場合の留意点

	報告期限	報告内容
速報	漏えい等の発覚後、速やかに報告 ※概ね３～５日以内	以下の項目のうちその時点で把握している事項
確報	30日以内 （不正の目的をもって行われたおそれがある漏えい事件は60日以内）	(1) 概要 (2) 漏えい等が発生し、又は発生したおそれがある個人データの項目 (3) 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数 (4) 原因 (5) 二次被害又はそのおそれの有無及びその内容 (6) 本人への対応の実施状況 (7) 公表の実施状況 (8) 再発防止のための措置 (9) その他参考となる事項

4 ランサムウェアの被害に遭った場合の留意点

４ ランサムウェアの被害に遭った場合の留意点

改正法施行から４カ月経過して

- 報告はWebフォームから24時間できるので簡単。
- 報告をすると、調査報告書の提出を求められたり、公表の予定の有無を質問されたりすることがあるが、それ以上にペナルティを課せられたり、負担を強いられることはない。
- サイバーリスクにおいては、ダークウェブ上での情報公開など後から判明するリスクもある。

- そうすると、報告作業に伴う負担は軽く、かつ報告すれば個人情報保護法義務違反を免れことができるのに対して、報告しなければ後から情報漏えいの事実が顕在化して個人情報保護委員会から罰則を課せられるリスクがある。

- サイバー攻撃を受けてわずかでも個人情報漏えいのおそれがある場合は、迷わずに報告！！！

5 ランサムウェア対策

■ 対応策その１：インシデント・レスポンスポリシーの策定

- ランサムの期限（例えば48時間）が限られているなかで事実関係の調査、評価、意思決定を迫られる。
- 個人情報保護委員会の速報・確報といった個人情報保護法対応も必要となる。
- 災害対策マニュアルと同じ位置付けで、有事に備えたインシデント・レスポンスポリシーを平時から策定しておくことの重要性が増す(OFACでも推奨)。

5 ランサムウェア対策

■ 対応策その２：バックアップの取得

- 盗まれた情報が戻らないが、暗号化被害による業務継続への支障はバックアップをもって対応できる。
- ただし、バックアップも暗号化される可能性があるので、バックアップの取り方及び取得のタイミングには工夫が必要

【再掲】ランサムウェアの増加の背景　RaaS

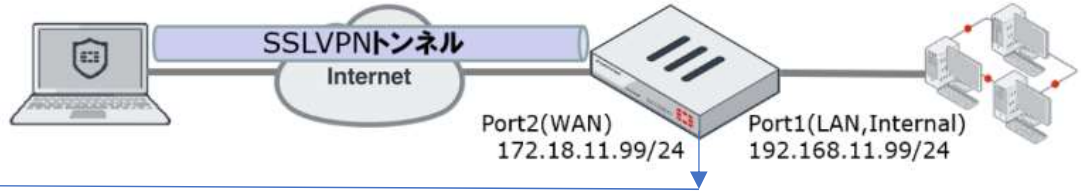
【Developer】
・Ransomwareの開発
・ハッキングマニュアルの交付
・被害企業との交渉窓口
・ビットコインアカウントの管理
・報酬の分配

【Access Broker】
脆弱性を悪用して認証情報の
収集及びダークサイトで販売

ID:test
Pass:12345678

【Affiliator】
ランサムウェア攻撃を実行

【侵入型】　【バラマキ型】



5 ランサムウェア対策

■　対応策その３：メール経由攻撃への対策

■　“Email is currently at the heart of the cybersecurity battel, as an estimated 90 percent of all hacking begins with an email phishing attack.”’
(Smith, B. (2017). “The need for a Digital Geneva Convention.” Microsoft https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digitalgeneva-convention/.)

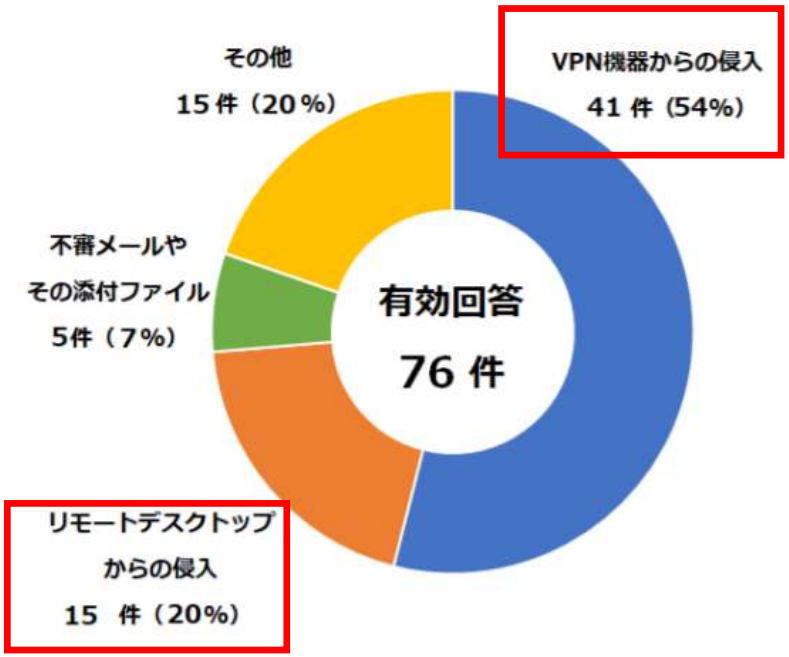
■　「トレンドマイクロが2019年1月～6月の間に全世界で検出した脅威総数の内、9割はメールによる脅威でした。すなわち、サイバー攻撃の主な起点はメールであると言えます。」
（トレンドマイクロ2019年10月24日/https://is702.jp/special/3576/）

✓ 不審なメールを事前に排斥するサービス（FW、UTM、AV等）
✓ 不審なメールについて、添付ファイルを開封しないよう社員教育・周知徹底

5 ランサムウェア対策

■　対応策その４：認証の厳格化

【図表６：ランサムウェアの感染経路】

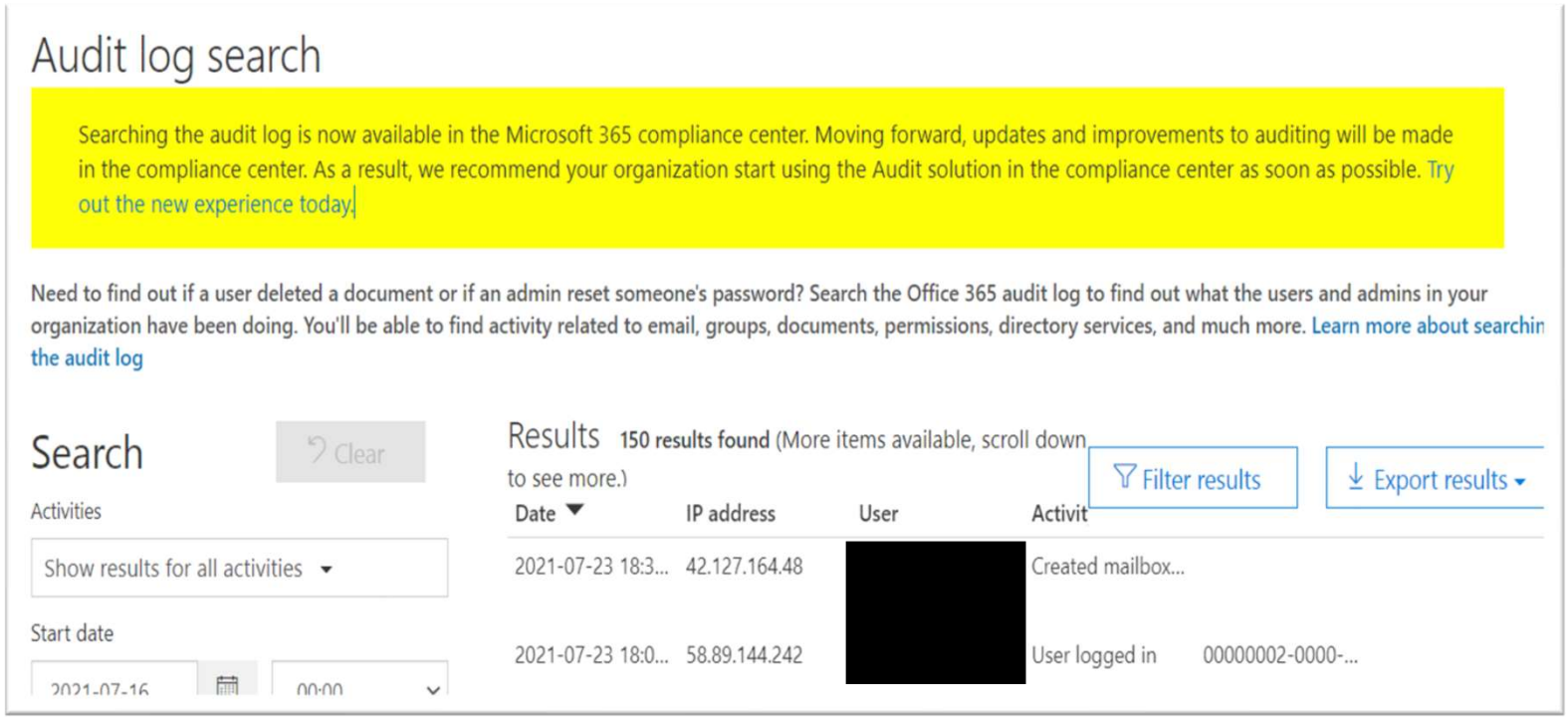


2022年4月7日付警察庁
「令和３年におけるサイバー空間をめぐる脅威の情勢等について」

■認証情報（VPN、RDP、オフィス365のログイン情報）が販売されており、Affiliatorがその情報を購入してサイバー攻撃を仕掛けていることからすれば、二段階認証の徹底

5 ランサムウェア対策

■　対応策その５：ログの保全



- 実務上、ログが不完全のため、調査が進まない、調査の結果を待っても何も判明しないということがほとんど。その結果、事実関係の把握に係る「精度」及び「迅速性」が大きく損なわれている。
  - 「速報」及び「確報」に間に合わない
  - 身代金に係る判断について誤った意思決定をしてしまう

5 ランサムウェア対策

■　対応策その６：サイバー保険

１．賠償損害
→　第三者からの賠償（個人及び取引先）

２．費用損害
→　調査費用、弁護士費用、再発防止策に要する費用

３．利益損害
→　事故がなかったなら計上できた営業利益

Date	Event
5/1	製造業X社の社内ネットワークに置かれたPC3台、ファイル共有サーバー1台及び工場制御システムが暗号化されたことが発覚。被害PCに残されたランサムノートには「情報を窃取した。72時間以内に10Bitcoin（5000万円相当）を支払わなければ、窃取したデータを公開する。また、身代金を支払えば復旧するための鍵を渡す」と記載されていた。
	事前の対応方針に従って ・全端末をネットワークから隔離 ・制御システムへの影響の調査開始 ・暗号化及び窃取されたデータの範囲を確認 ・暗号化されたデータのバックアップの有無の確認
5/2	専門事業者（フォレンジック会社、弁護士、セキュリティコンサル）に依頼
	ダークウェブ上のリークサイトに、窃取された情報の一部が公開されていることが判明
	工場制御システムの復旧には一ヶ月掛かり、その間、製造を停止さざるを得ないことが判明
5/3	支払ってもデータ及びカルテシステム復旧並びにデータ非公開の保証はないことから身代金を支払わないことを決定
6/1	カルテシステムのOSを再インストールして、試運転を経て、製造再開。
6/30	フォレンジック調査の結果、不正アクセスの経路及び漏えいしたデータの範囲が判明
7/5	今後の対応方針を取締役会で決定のうえ、個人情報保護委員会、警察に届け出
7/6	Webサイト上でプレスリリース
	取引先への個別説明
8/30	再発防止策の策定完了

500万円

1,500万円

2,000万円

3,000万円

5 ランサムウェア対策

■　対応策その６：サイバー保険

■ 有事の際には、提携しているフォレンジック事業者の紹介を受けることができる。
  - 現時点でも、フォレンジック案件の増加でフォレンジック事業者の確保が困難になりつつある。特に、改正個人情報保護法の下ではフォレンジック案件が急増して、フォレンジック事業者を確保することが更に困難になる。
  - サイバー保険に入っていないと、フォレンジック事業者から敬遠されるリスクがある。

■ 取引先から契約の条件としてサイバー保険の加入を確認されることがある。
  - 単なる「費用」ではなく、信用を獲得するための「投資」の側面がある。

■ 「逆説的だが、リスクマネジメントにおける、リスクの移転であるサイバー保険に加入することで、リスクの低減（最適化）にも資する」という指摘あり。
（中沢潔「米国におけるサイバー保険の現状」（JETROニューヨークだより2017年11月））