暴露型ランサムウェアと弊社の対応

2020年6月24日

マクニカネットワークス株式会社

テレワークにおけるリスク観測

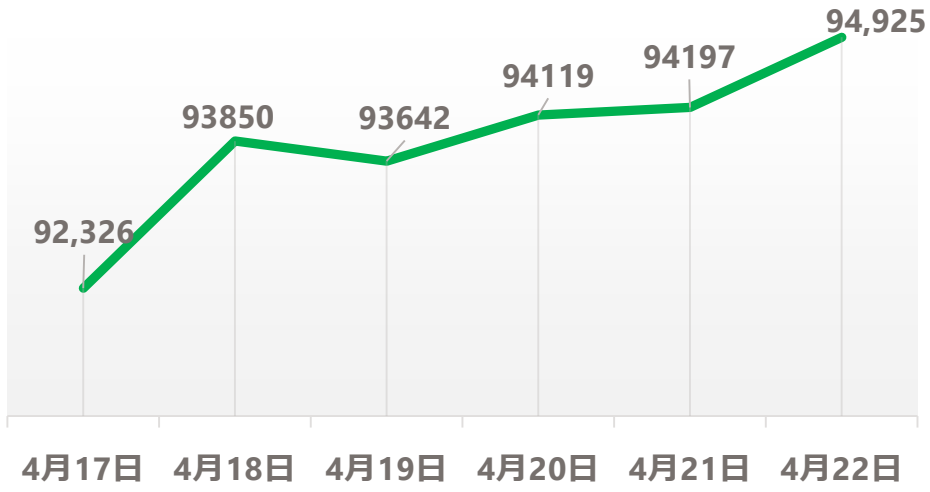
テレワーク環境におけるリスクのあるデバイスの増加

・攻撃されやすいポートが公開された国内のデバイスが増加傾向　*Shodanのデータを弊社集計
・テレワークにより自宅環境で利用されるPCが増加したことが原因と推測

SMB (445/tcp)：ファイル共有サービス

44% 増　65,809 (2020/3/11) → 94,925 (2020/4/22)

4月下旬の傾向

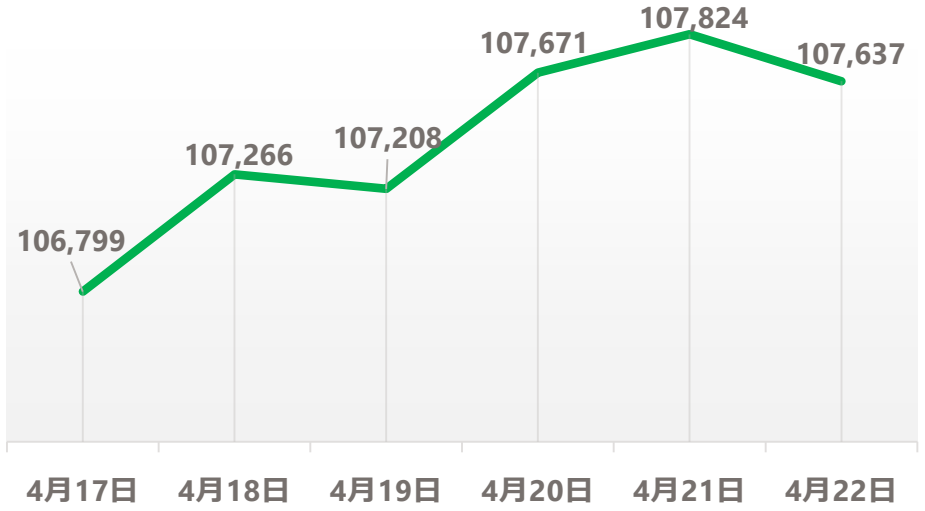


SMB関連の脆弱性：
CVE-2020-0796 (SMBv3の脆弱性)
CVE-2017-0144 (Wannacryでも悪用されたSMBv1の脆弱性)

RDP (3389/tcp)：リモートデスクトップサービス

50% 増　71,531 (2019/6/18) → 107,637 (2020/4/22)

4月下旬の傾向

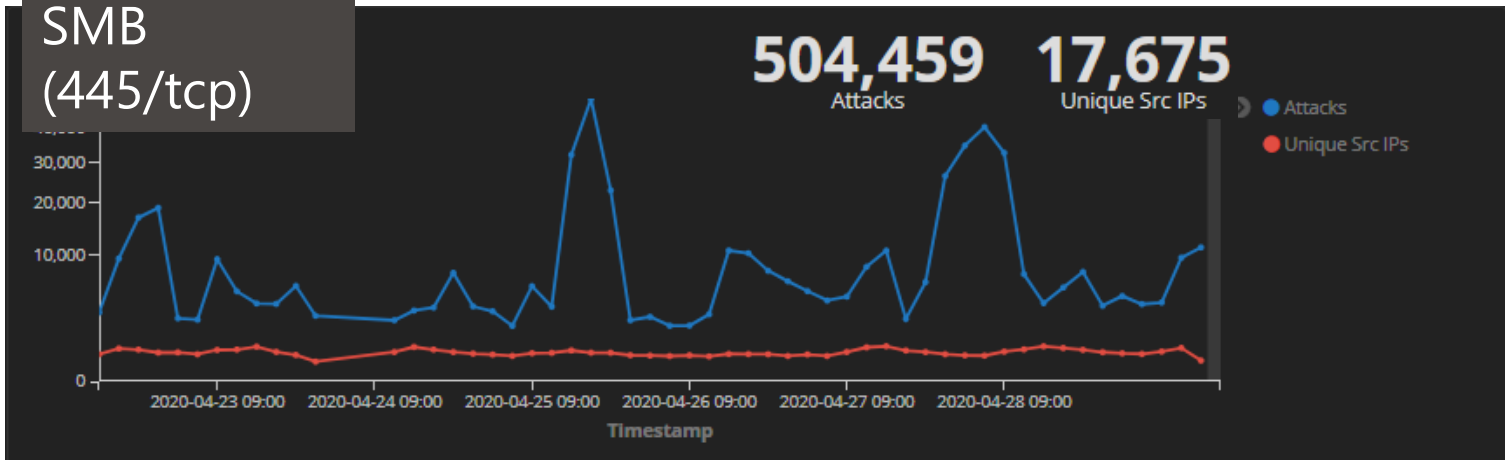


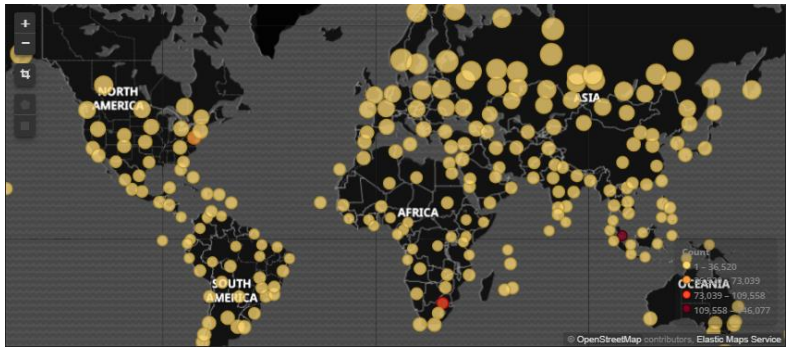
RDP関連の脆弱性：
CVE-2019-0708 (BlueKeep)
CVE-2019-1181/CVE-2019-1182 (DejaBlue)

SMBやRDPに対する攻撃数の統計（弊社設置のハニーポットから）

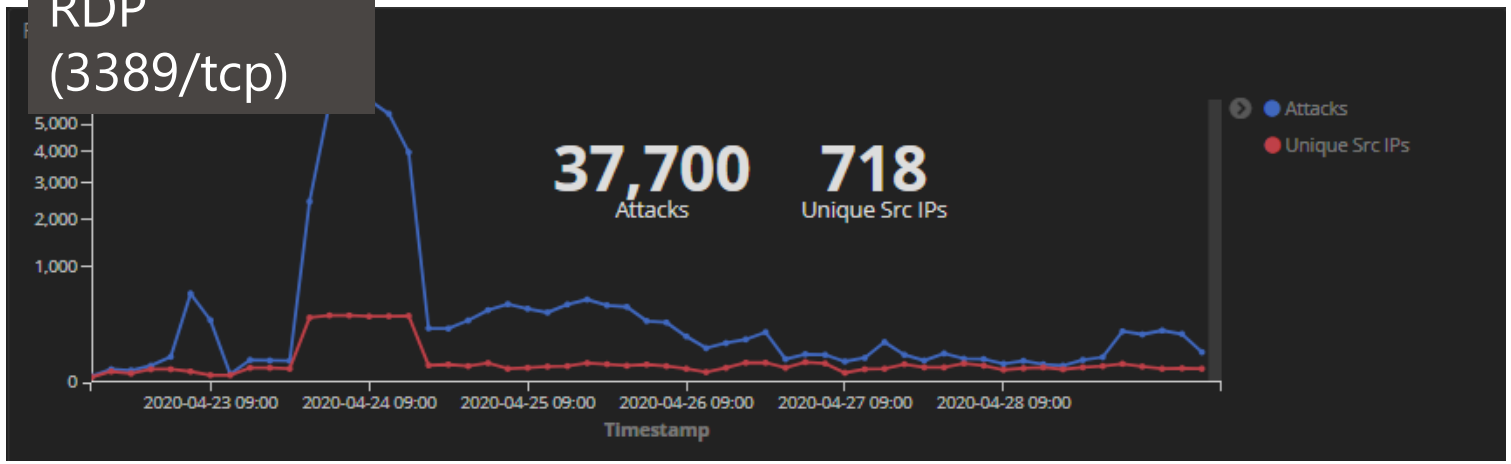
■ 4月22日15:00 ～ 4月29日15:00　1週間分のデータ

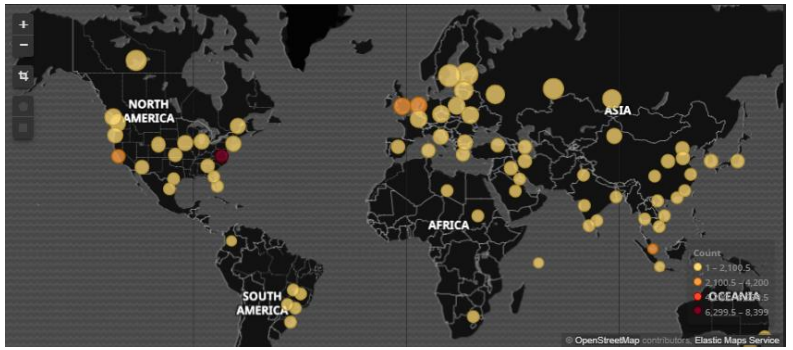
SMB
(445/tcp)





RDP
(3389/tcp)

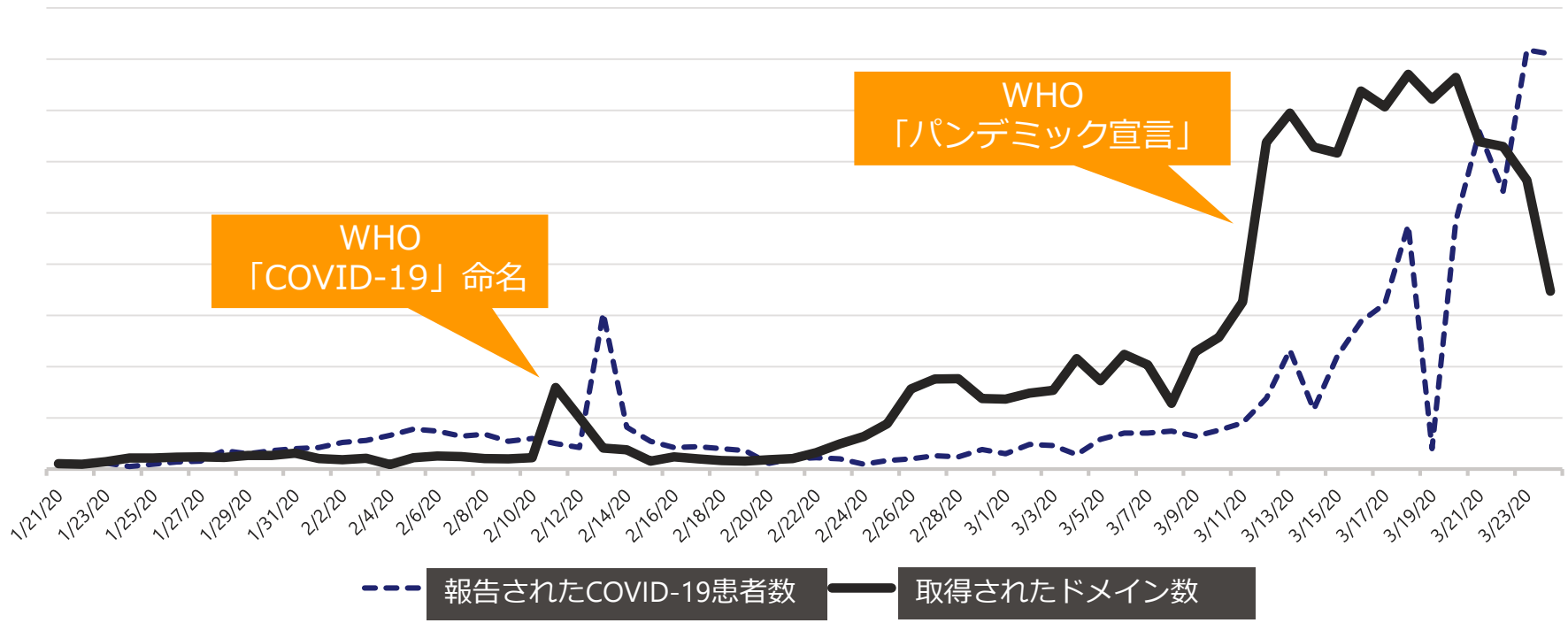




SMB/RDPなどのハイリスクポートへの攻撃が実際に発生している。

不審なWebサイトへのアクセスリスク増加について

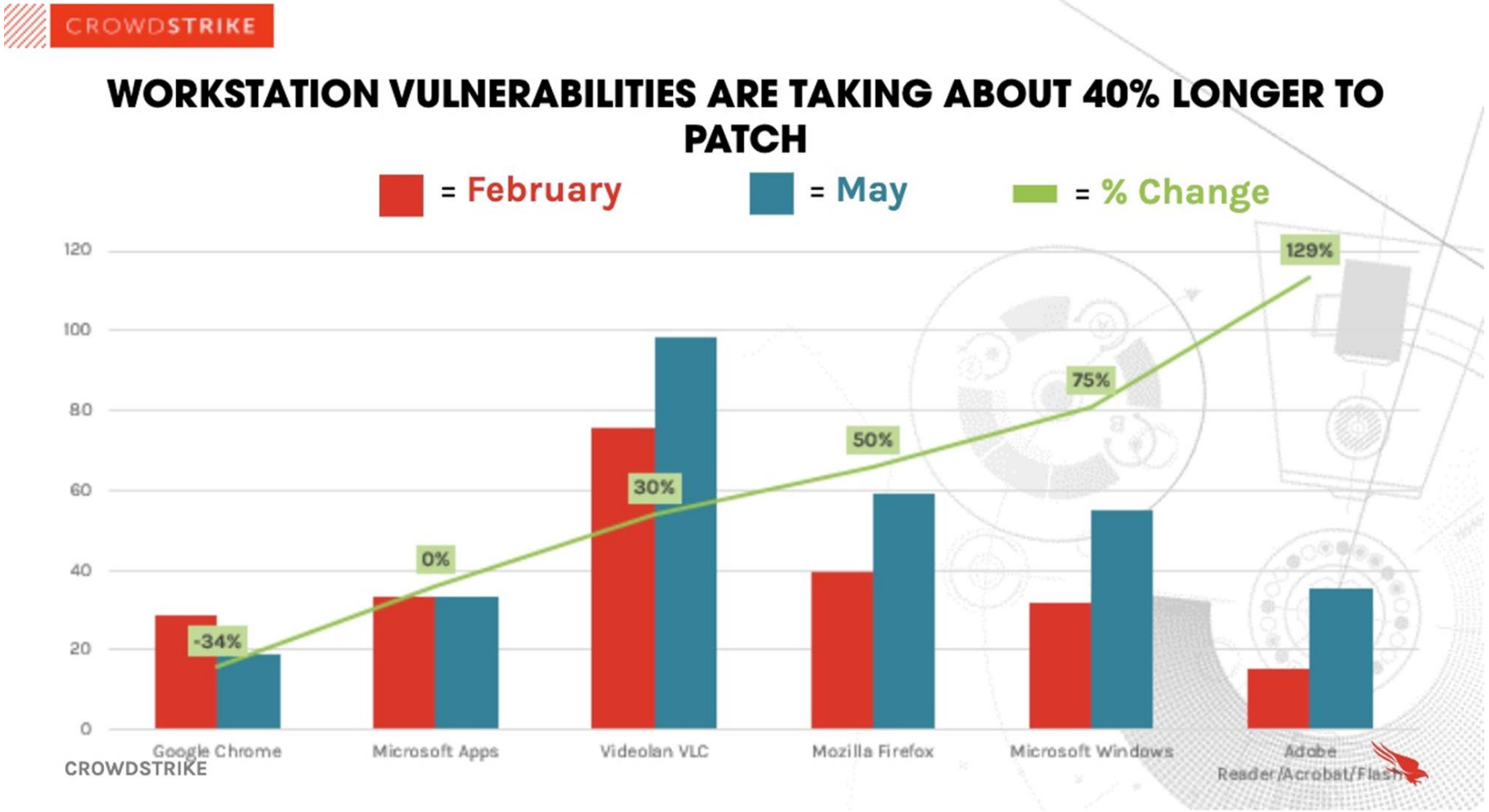
- 新型コロナウイルスの情報を餌に不正サイトへ誘導する試みが増加していると推測
- covid/corona/c0vidなどを含む疑わしいドメインの取得数が増加傾向



*以下サイトデータを弊社集計
参考: https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats
参考: https://experience.arcgis.com/experience/685d0ace521648f8a5beeeee1b9125cd

コロナ禍前後での脆弱性対応について

テレワーク中の端末へのパッチ配信の遅延が顕著



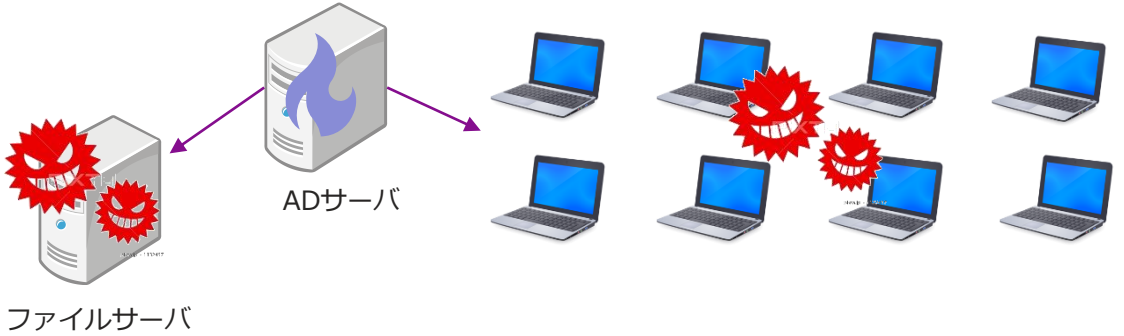
Crowd Strike社"Global Vulnerability Management Trends"より抜粋

暴露型ランサムウェア

従来のランサムウェアと暴露型ランサムウェアの違い

従来のランサムウェア

暴露型ランサムウェア



WannaCryなど
対象：主にクライアントPC、各種サーバ
事象：クライアントPC、サーバの暗号化
　　及び自己拡散
目的：暗号化解除のために身代金要求
　　業務復旧のための身代金要求
要求額：数万円程度

REvil/Sodinokibi, Ryuk,など
対象：ファイルサーバ、クライアントPC
事象：ファイルサーバ、クイアントPCが暗号化
　　及び内部の情報搾取
目的：暗号化解除のために身代金要求
　　搾取情報の公開を止めるための身代金要求
要求額：数百万円程度～

脅迫文（抜粋）

---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion [redacted]
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

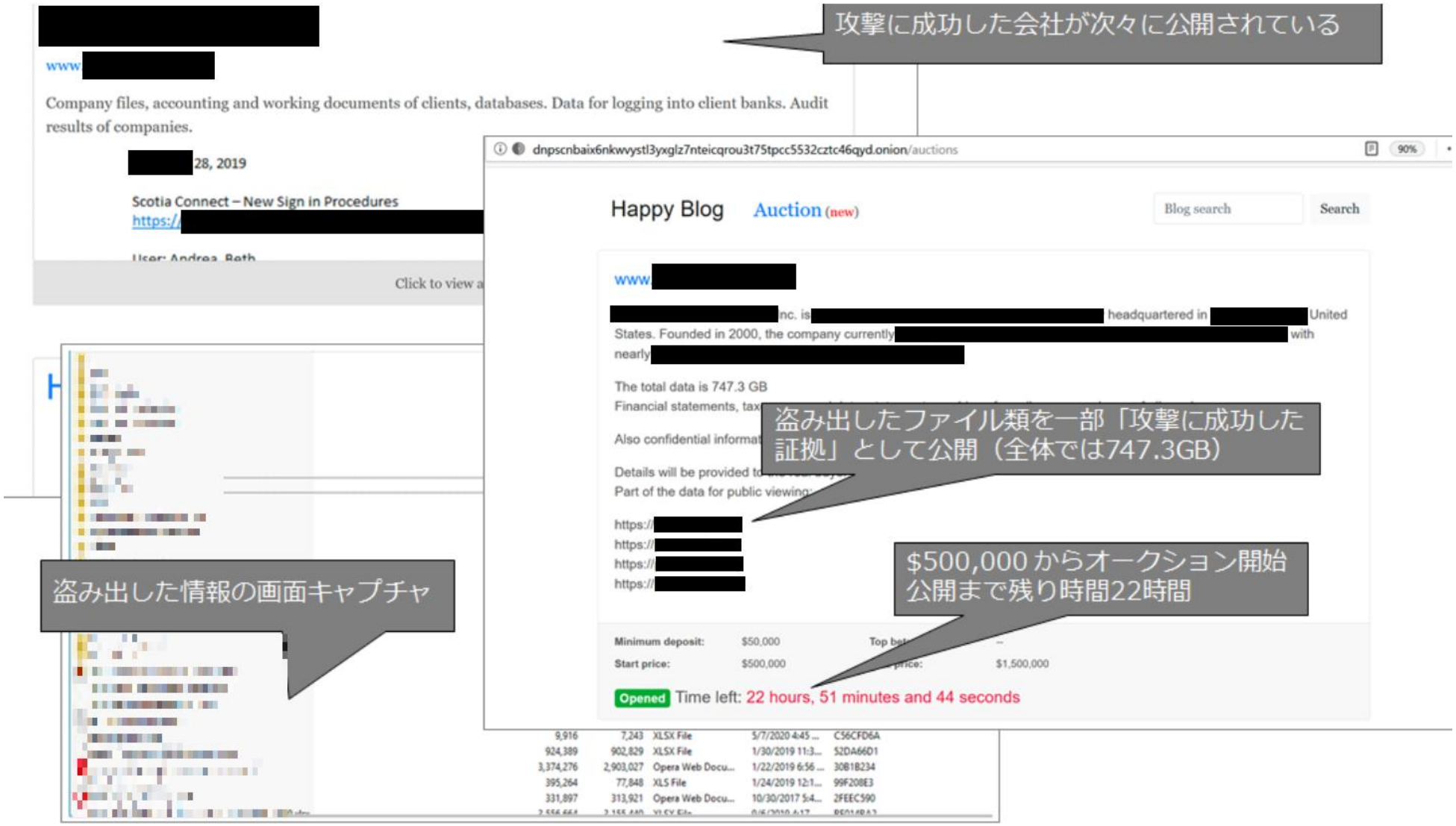
You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https:/[redacted]
  b) Open our website: http://[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http:/[redacted]

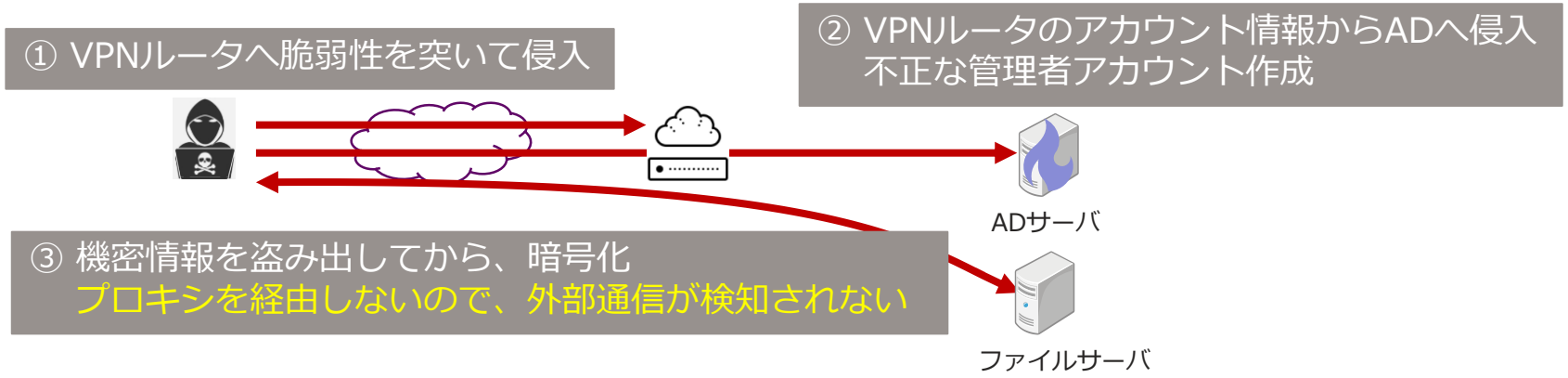
Warning: secondary website can be blocked, thats why first variant much better and more available.

実際に搾取された情報が裏オークションに掛けられた例

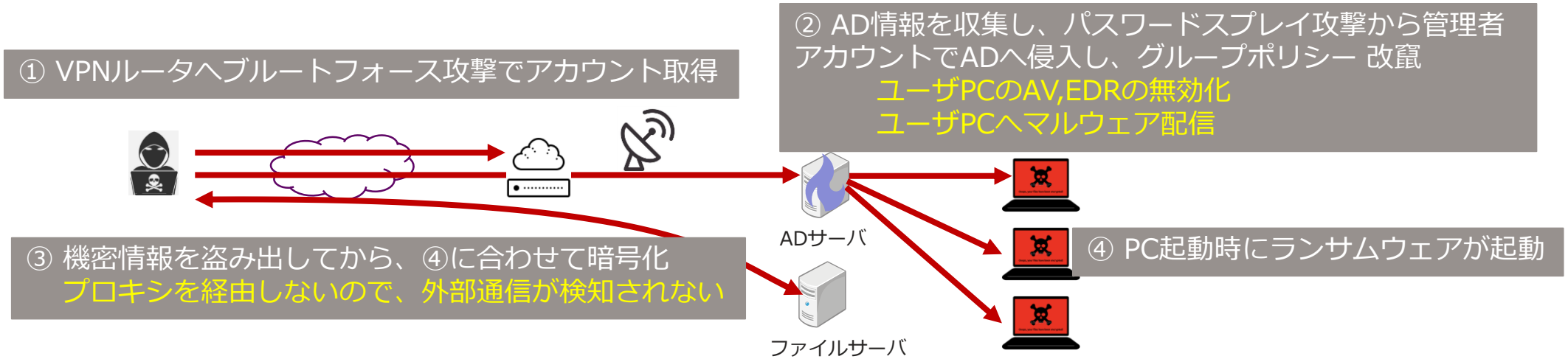


暴露型ランサムウェアの手口と被害①

被害例１）VPNルータの**脆弱性から**侵入され、ADサーバが乗っ取られファイルサーバが暗号化

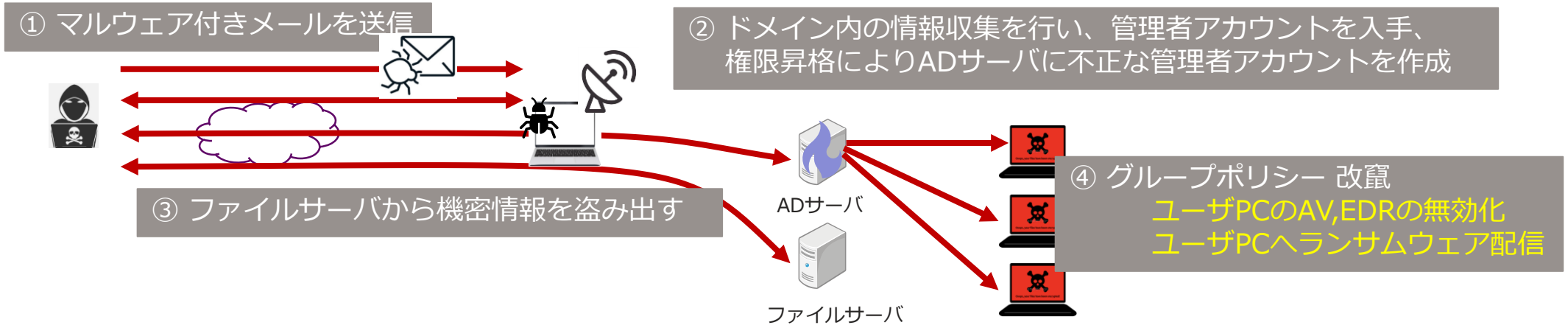


被害例２）VPNルータの**アカウントから**侵入され、ADサーバが乗っ取られユーザPCが暗号化

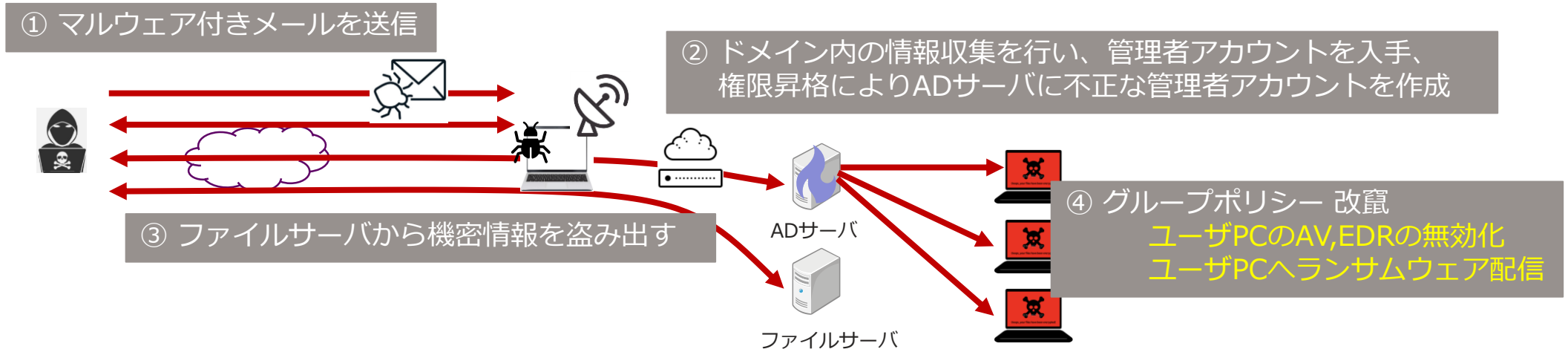


暴露型ランサムウェアの手口と被害②

被害例３）メール添付ファイルから侵入、ADサーバが乗っ取られユーザPCが暗号化



被害例４）メール添付ファイルから侵入、ADサーバが制圧乗っ取られユーザPCが暗号化（VPN経由※）



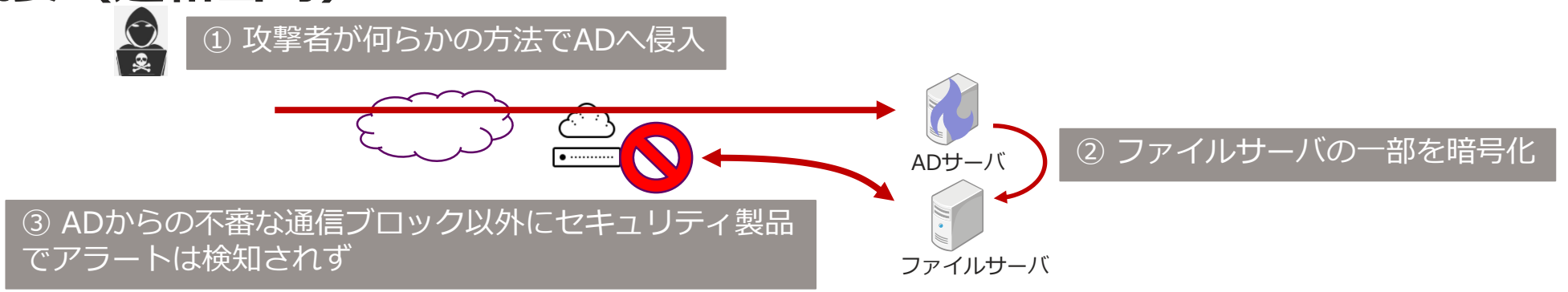
※ VPN経由でユーザが利用中に感染して直接インターネット通信する場合には、外部通信で検知できない

暴露型ランサムウェアに対する弊社の対応

弊社の対応事案

X社の事案

被害概要（連絡当時）



- サーバ群、リモートアクセス端末から社内NWを経由した通信において、セキュリティ機器での不審な通信ブロックは事象発生前後の時間帯でAD以外に確認できず
- X社では調査用にADのイメージを取得し、その後バックアップイメージからADを事案前の状態に復元済み
- 暗号化されたファイル内容の特定とバックアップからの復元を計画中

X社からの依頼事項

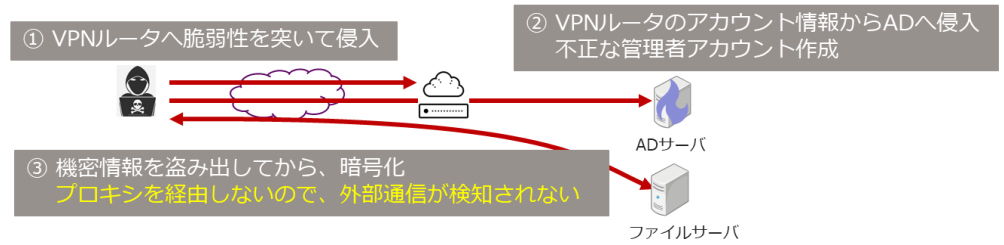
- ADサーバ、ファイルサーバのフォレンジックによる被害範囲の詳細調査
- サーバの復旧やテレワークによる事業再開に向けた支援

弊社の対応事案（続き）

- 弊社からの調査提案内容
  - ランサムウェア特定のため、脅迫文の提供
  - 攻撃者の侵入経路、事象の再発を考慮したADイベントログとVPNログ、Proxyログ等のセキュリティ製品以外のログ調査

- 調査の結果、X社が認識していなかった被害
  - VPNの脆弱性パッチが適用されておらず、VPN経由でADへ侵入し、暗号化対象と推測されるデータのアップロードをVPN経由で実施
  - REvilランサムウェア実行の数ヶ月前にも偵察のためか、侵入した痕跡も発見（同攻撃者かは不明）

被害例１）VPNルータの**脆弱性から**侵入され、ADサーバが乗っ取られファイルサーバが暗号化



2次被害や再発を防ぐため、VPNパッチ適用、アカウントリセット、プレスリリース準備など攻撃に対する適切な調査と対処が必要。

弊社でご提供するサービス

サービス項目	サービス詳細	費用	コメント
ActiveDirectory脅威診断 スポットサービス	ActiveDirectoryに対する脅威を分析してレポートします。	有償	2020年6月24日～9月30日の間、無償で実施（法人様向け）
ActiveDirectoryにおける脅威 月次レポートサービス	ActiveDirectoryに対する脅威を継続分析し、月次レポートとして提供します。	有償	
ActiveDirectory監視サービス	ActiveDirectoryへの攻撃を継続的に監視するだけでなく、不審な挙動が検出された場合はリモートから対処を実施します。 ・不審なアカウントの無効化 ・追加で調査に必要な情報の収集	有償	

このような事案がありましたら、ぜひご一報ください。

お問合せ

貴社のお役に立てるような
ご提案活動をさせて頂く所存です。

ご依頼等ございましたら、何なりとお申し付けください。
今後ともよろしくお願い申し上げます。

【 お問い合わせ先 】

マクニカネットワークス株式会社

第2営業統括部第2営業部

S&J製品担当

Tel: 045-476-2010
Email: sec-service@cs.macnica.net
URL: https://www.macnica.net/sandj/