サイバーセキュリティレポート

2022.12

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

【当レポートについて】

当レポートでは 2022 年 12 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『参議院選挙期間に実施された標的型攻撃』

- 2022 年 12 月、セキュリティ会社の ESET 社は、MirrorFace と命名した攻撃者による標的型攻撃のレポートを発表した。攻撃は同年の日本国の参議院選挙期間に行われ、自由民主党の広報部門に成りすました標的型メール等が検知された。
- 情報窃取等に使われる LODEINFO マルウェアへの感染を狙っていたことから、同じマルウェアを使用する等の類似性が有る中華人民共和国政府傘下の APT10 グループとの関連が疑われている。
- 近年世界的に認識されつつある、民主主義の根幹である選挙に対するサイバー攻撃の脅威が、日本においても差し迫っていることが今回の攻撃から明らかになった。

第 2 章『日本政府、能動的サイバー防御の導入を閣議決定』

- 12 月 16 日、日本政府は敵基地攻撃能力の保有等を盛り込んだ 3 文書を閣議決定した。サイバー攻撃についても、攻撃を受けてから対処をするのではなく、事前に検知し、攻撃者の用意したサーバー等へ侵入し、これを無力化するような対応を行う「能動的サイバー防御」の導入が明記された。
- 今後、能動的サイバー防御を行うための自衛隊のサイバー対応能力の強化や NISC を発展吸収した新組織の設立等が行われ、その活動に根拠を持たせるための法整備が進む。
- 攻撃を受ける前に検知するための監視活動は「通信の秘密」や「不正アクセス禁止法」との整合性が必要と考えられることから、細部の検討に注目したい。

第 3 章『フィッシングを行う Royal ランサムウェアグループ』

- 2022 年第 4 四半期のランサムウェアグループ別の暴露件数を調査したところ、Royal の件数が LockBit に続いて 2 番目に多く、登場して間もないグループにもかかわらず勢力を伸ばしていることが確認された。
- Royal は、電子メールと電話を組み合わせたコールバック・フィッシング攻撃や、Web 広告を悪用してマルウェアに感染させるマルバタイジング攻撃といった手法で人のミスに付けこんで侵入し、攻撃を拡大している。
- 攻撃者の活動は日々変化しているため、セキュリティ担当者は最新の攻撃手法や傾向の情報を入手し、従業員への周知や教育、対策策定に生かすことが肝要である。

1. 参議院選挙期間に実施された標的型攻撃

1.1. 概要

2022 年 12 月にセキュリティ会社の ESET 社は、日本国の参議院議員選挙のタイミングに合わせ同年 6 月末に行われた標的型攻撃についてのレポートを発表した[1]。

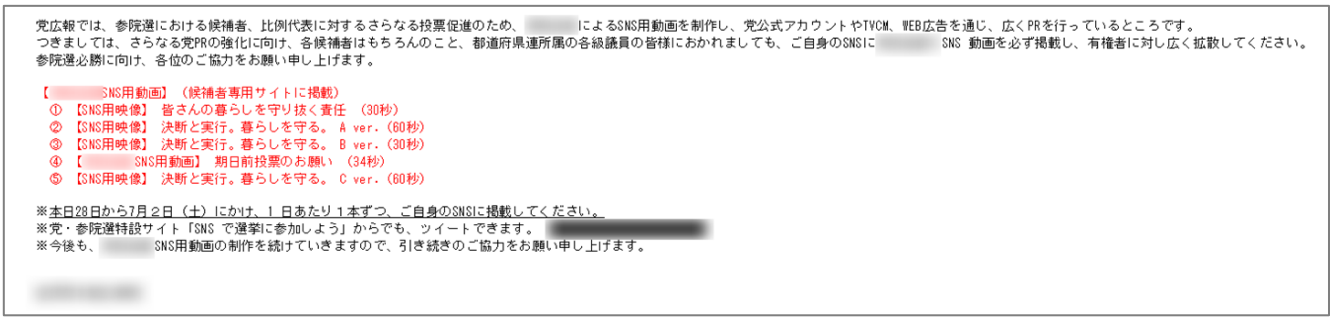
攻撃者は MirrorFace と命名されている。検知された標的型メールや添付ファイル等から、選挙活動中の自由民主党の広報部門に偽装したメールでマルウェアを感染させ、情報窃取等を行おうとしていたと分析されている。中華人民共和国政府の傘下とされる APT10 グループと手口が類似しているため、関連するグループの可能性が考えられている。

本件は、世界各国で認識されつつある選挙に対するサイバー攻撃の脅威が、日本においても差し迫っていることを明らかにした。

1.2. MirrorFace による標的型攻撃

【標的型メールと添付ファイル】

参議院選挙期間中である 6 月末に、自由民主党の広報部門に成りすました標的型メール（図 1）が検知された[2]。添付されたビデオファイルをソーシャルメディアに拡散するよう促すものであったが、添付ファイルの正体は、展開すると自動的にマルウェアに感染する自己解凍型圧縮ファイルであった。


党広報では、参院選における候補者、比例代表に対するさらなる投票促進のため、[redacted]によるSNS用動画を制作し、党公式アカウントやTVCM、WEB広告を通じ、広くPRを行っているところです。
つきましては、さらなる党PRの強化に向け、各候補者はもちろんのこと、都道府県連所属の各級議員の皆様におかれましても、ご自身のSNSに[redacted] SNS 動画を必ず掲載し、有権者に対し広く拡散してください。
参院選必勝に向け、各位のご協力をお願い申し上げます。

【[redacted]SNS用動画】（候補者専用サイトに掲載）
① 【SNS用映像】 皆さんの暮らしを守り抜く責任 （30秒）
② 【SNS用映像】 決断と実行。暮らしを守る。 A ver.（60秒）
③ 【SNS用映像】 決断と実行。暮らしを守る。 B ver.（30秒）
④ 【[redacted] SNS用動画】 期日前投票のお願い （34秒）
⑤ 【SNS用映像】 決断と実行。暮らしを守る。 C ver.（60秒）

※本日28日から7月2日（土）にかけ、1 日あたり 1 本ずつ、ご自身のSNSに掲載してください。
※党・参院選特設サイト「SNS で選挙に参加しよう」からでも、ツイートできます。[redacted]
※今後も、[redacted]SNS用動画の制作を続けていきますので、引き続きのご協力をお願い申し上げます。

図 1 標的型メール本文 [3]

同時期には他にも、「申込書」と書かれたおとりの Word 文書（図 2）を含むもの等、上記に類似した自己解凍型圧縮ファイルが複数検知されている[4]。「取材のお願い」という名のファイルもあった事から、自由民主党関連だけでなく日本のメディア

[1] 出典：ESET『APT グループ「MirrorFace」が日本の政治団体を標的に実行した LiberalFace 作戦の詳細』
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

[2] 出典：AVAR2022『Behind the MirrorFace mask: LODEINFO malware interfering with Japanese elections』
https://aavar.org/cybersecurity-conference/index.php/behind-the-mirrorface-mask-lodeinfo-malware-interfering-with-japanese-elections/

[3] 出典：ESET『APT グループ「MirrorFace」が日本の政治団体を標的に実行した LiberalFace 作戦の詳細』
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

[4] 出典：Kaspersky Labs Japan『日本を標的とするマルウェア LODEINFO の新たな活動』
https://blog.kaspersky.co.jp/lodeinfo-sfx-downiissa-2022/32710/

等へも送られていたと考えられる[5]。

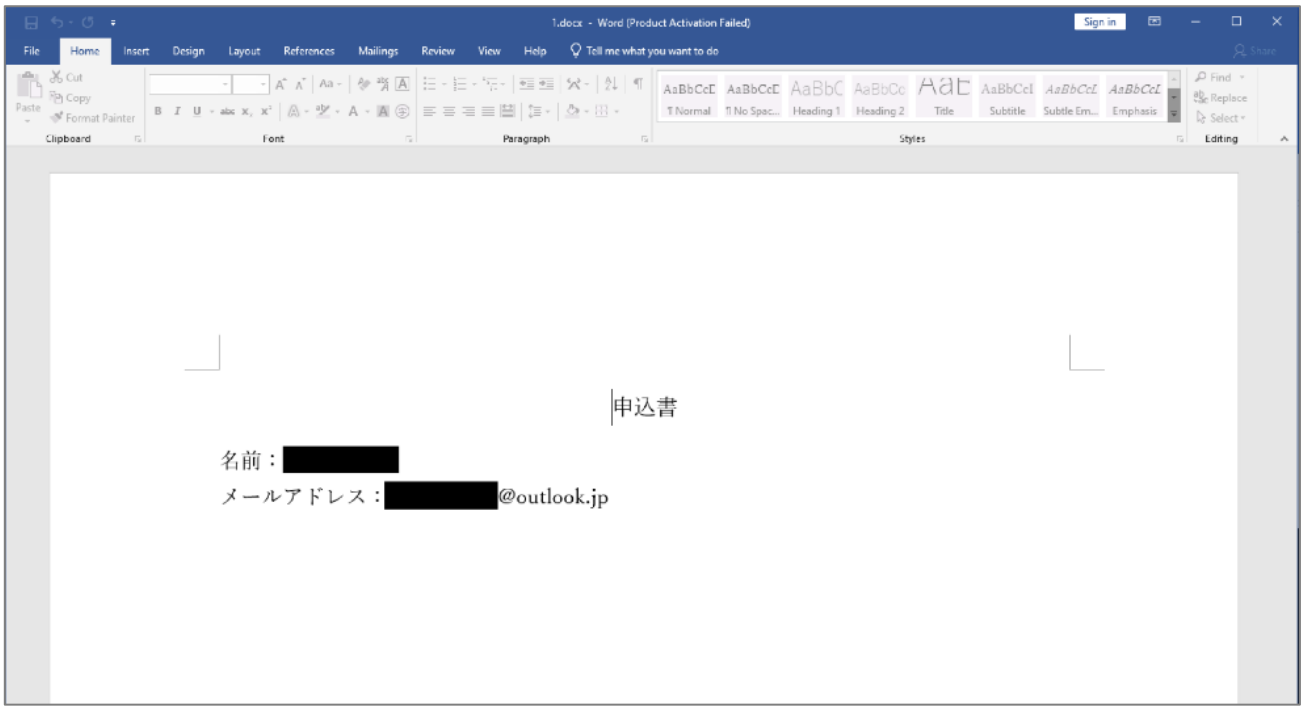


図 2 おとりの文書ファイル [6]

【LODEINFO マルウェア】

メール添付ファイル等から検知された自己解凍型圧縮ファイルは、バックドア型マルウェアである LODEINFO マルウェアへの感染を狙ったものであった。感染した端末に対し外部からオペレーターがアクセスすることで、端末を踏み台にして標的組織のネットワーク内を探索したり、さらに別のマルウェアをダウンロードして感染させたりすることができる。オペレーターの活動を支援するために LODEINFO マルウェアは、スクリーンショットのキャプチャ、キーロギング、プロセスの強制終了、ファイルの外部への送信、ファイルの追加およびコマンドの実行等の機能を備えている。

LODEINFO マルウェアは、日本国内の標的に限定して使用されている。2019 年 12 月以来頻繁にバージョンアップが行われており[7]、参議院選挙期間中には v0.6.3 と v0.6.5 が使用された（図 3）。検知・解析妨害の機能追加や不要な機能の整理等がバージョンアップで行われている。参議院選挙後もバージョンアップは続いており、攻撃の成功性を高めるため試行錯誤を繰り返していると考えられている。

[5] 出典：kaspersky『APT10: Tracking down LODEINFO 2022』
https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-i/107742/
https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-ii/107745/

[6] 出典：Kaspersky Labs Japan『日本を標的とするマルウェア LODEINFO の新たな活動』
https://blog.kaspersky.co.jp/lodeinfo-sfx-downiissa-2022/32710/

[7] 出典：JPCERT コーディネーションセンター『マルウエア LODEINFO の進化 - JPCERT/CC Eyes』
https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html

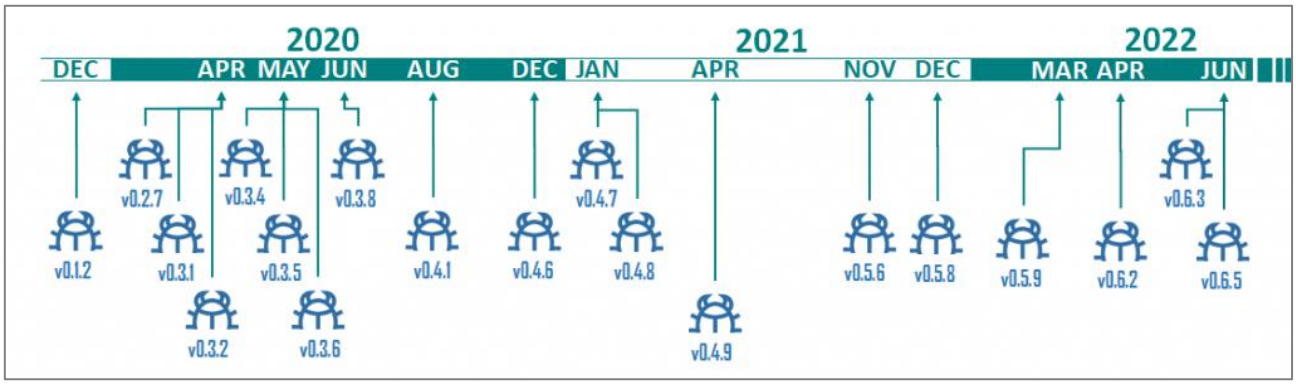


図 3 LODEINFO マルウェアのバージョンアップ歴（Kaspersky 社 作図）[8]

【認証情報窃取からの機密情報窃取】[9]

端末内にはブラウザやメールクライアントなど認証情報を保存している様々なアプリケーションがある。これらのアプリケーションから認証情報を盗み取るために MirrorFace は LODEINFO マルウェアとは別に、31558_n.dll というファイル名のマルウェアを使用していた。

MirrorFace は LODEINFO マルウェアを介し、外部から 31558_n.dll を端末にダウンロードして実行することで、認証情報を収集する。収集した認証情報を使用して組織内のシステムに不正ログインし、機密情報の窃取活動をしていたとみられている。

認証情報収集の対象となるアプリケーションの中には、日本での使用が多いメールクライアントである Becky!があった。また、情報窃取活動を分析したところ、収集対象に指定されているファイル形式の中には日本語ワープロ「一太郎」形式（.jtd）が含まれていた。これらのことからも、MirrorFace は攻撃対象を日本に限定して活動していると考えられている。

1.3. APT10 との関連

分析から MirrorFace は中国語を使用するサイバー攻撃者で、日本に拠点を置く企業や組織を標的にしていることが分かっている。LODEINFO マルウェアの使用といった攻撃手法が標的型攻撃グループの APT10 と類似性があり、関連性が疑われている。[10]

APT10 は中国国家安全部(MSS)の天津国家安全局の傘下にあると推定されているグループで、少なくとも 2006 年から活動している。セキュリティ情報のデータベースを管理する MITRE 社は種々の調査から、APT10 は医療、防衛、航空宇宙、金融、海運、バイオテクノロジー、エネルギー、および政府部門を世界的に標的としており特に日本の組織を重点的に狙っている、と結論づけている。[11]

---

[8] 出典：Kaspersky Labs Japan『日本を標的とするマルウェア LODEINFO の新たな活動』
https://blog.kaspersky.co.jp/lodeinfo-sfx-downiissa-2022/32710/

[9] 出典：ESET『APT グループ「MirrorFace」が日本の政治団体を標的に実行した LiberalFace 作戦の詳細』
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

[10] 出典：ESET『APT グループ「MirrorFace」が日本の政治団体を標的に実行した LiberalFace 作戦の詳細』
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/

[11] 出典：MITRE ATT&CK『menuPass, Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH, Group G0045』
https://attack.mitre.org/groups/G0045/

2018 年 12 月には、英国と米国の政府が APT10 を非難する声明文を発表した事に合わせ、外務省が APT10 による攻撃を非難する外務報道官談話を発表しており[12]、日本国政府も自国にとって脅威であると認識している。

1.4. まとめ

日本の政府機関や重要インフラ等を狙った APT10 等の活動が長年続いており、イベントに便乗した標的型メールがたびたび送信されている[13]。MirrorFace が選挙活動等に偽装して攻撃した意図は明らかではない。しかし、情報窃取の被害によっては、選挙の正常な運営や選挙結果の公正性を損なう影響が出る恐れがあった。

近年、欧米等の民主国家では選挙に対するサイバー攻撃の脅威が認識されつつある[14]。日本においても、民主主義の根幹である選挙に脅威が迫っていることを、今回の攻撃は明らかにしたといえる。

[12] 出典：外務省『中国を拠点とする APT10 といわれるグループによるサイバー攻撃について（外務報道官談話）』
https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

[13] 出典：JPCERT/CC『サイバーレスキュー隊（J-CRAT）活動状況[2022 年度上半期]』
https://www.ipa.go.jp/files/000106897.pdf

[14] 出典：FireEye『問題の枠組み：サイバー脅威と選挙』
https://www.fireeye.com/blog/jp-threat-research/2019/05/framing-the-problem-cyber-threats-and-elections.html

2. 日本政府、能動的サイバー防御の導入を閣議決定

2.1. 概要

2022 年 12 月 16 日、日本政府は、ロシアによるウクライナ侵攻をはじめとする日本周辺の国・地域での急激な軍備増強や、力による一方的な現状変更の試みといった動きに対処するため、敵基地攻撃能力の保有等を盛り込んだ[15]「国家安全保障戦略」、「国家防衛戦略」及び「防衛力整備計画」の３つの文書を閣議決定した[16]。
３文書は、物理的な防衛だけでなく、サイバー攻撃への対応についても大きな影響を与える。サイバー攻撃を受けてから対処するのではなく、攻撃を受ける前に検知し、攻撃者の用意したサーバー等へ侵入し、これを無力化するような対応を行うことが可能な「能動的サイバー防御」の導入が明記された。今後、自衛隊等をはじめとする人員や法の整備が進められる[17]。

図 4 閣議決定について会見を行う岸田総理 [15]

2.2. 安保関連３文書

３文書は、外交・防衛をはじめとするサイバー分野も含めた戦略的方針を示す最上位文書「**国家安全保障戦略**」、防衛の目標を設定し、達成手段を示す「**国家防衛戦略**」、国として保有すべき防衛力の水準を示し、それを達成するための中長期計画を示す「**防衛力整備計画**」からなる。（図 5）
本稿では３文書のサイバー分野に関連する記載について取り上げる。

---

[15] 出典：首相官邸『岸田内閣総理大臣記者会見』
https://www.kantei.go.jp/jp/101_kishida/statement/2022/1216kaiken.html
[16] 出典：内閣官房『国家安全保障戦略について』
https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html
[17] 出典：朝日新聞 DIGITAL『サイバーでも「敵基地攻撃」可能に 安保３文書「能動的防御」を明記』
https://www.asahi.com/articles/ASQDJ6WF8QDJUTIL01X.html

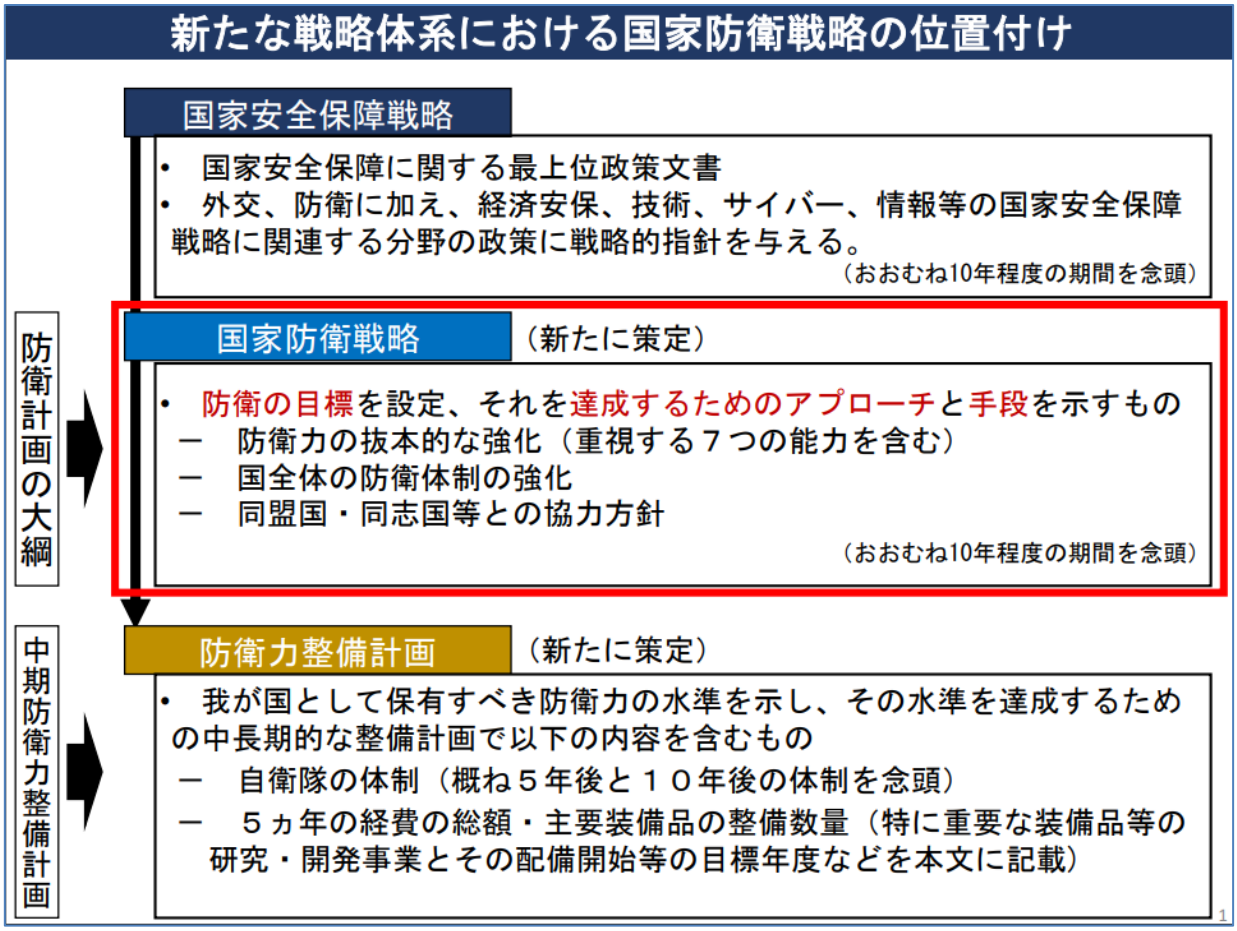


図 5「3 文書」の位置付け(国家防衛戦略概要より[18])

【国家安全保障戦略】

国家安全保障戦略では、日本が置かれている状況は、サイバー、海洋、宇宙空間等においてリスクが深刻化しており、「特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている」と評されている。

そのような状況を踏まえ、国や重要インフラ等に対する重大なサイバー攻撃について、「可能な限り**未然に攻撃者のサーバー等への侵入・無害化ができるよう**、政府に対し必要な権限が付与されるようにする」として、能動的サイバー防御を導入することを決定した。

そのため、攻撃を受けた際の情報共有の促進や、政府から民間組織への対応支援の強化、さらに通信事業者の情報を活用して攻撃者のサーバーを特定できるようにすること等、枠組みを整備する。また、内閣サイバーセキュリティ―センター(NISC)を改組し、サイバー安全保障分野の政策を一元的に総合調整する組織を新たに設置。この新組織は後述する自衛隊や警察庁の実働部隊を統括する[19]。

[18] 出典：防衛省『国家防衛戦略（概要）』
https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaku_gaiyou.pdf

[19] 出典：共同通信『サイバー防御責任者任命へ、政府 24 年度予算で新組織』
https://nordot.app/968119316824145920?c=302675738515047521

【国家防衛戦略】

前述の能動的サイバー防御を実現する取り組みとして、防衛省・自衛隊は「我が国全体のサイバーセキュリティに貢献する体制を抜本的に強化」し、「特に、陸上自衛隊が人材育成等の基盤拡充の中核を担っていく」としている。

【防衛力整備計画】

サイバー攻撃に対応する自衛隊の部隊の整備は、3 文書の策定よりも前に始まっている。2022 年 3 月 17 日に陸海空自衛隊の共同部隊として、防衛省・自衛隊の情報通信ネットワークの監視及びサイバー攻撃への対処にあたる「サイバー防衛隊」が新たに編成された[20]。（図 6）

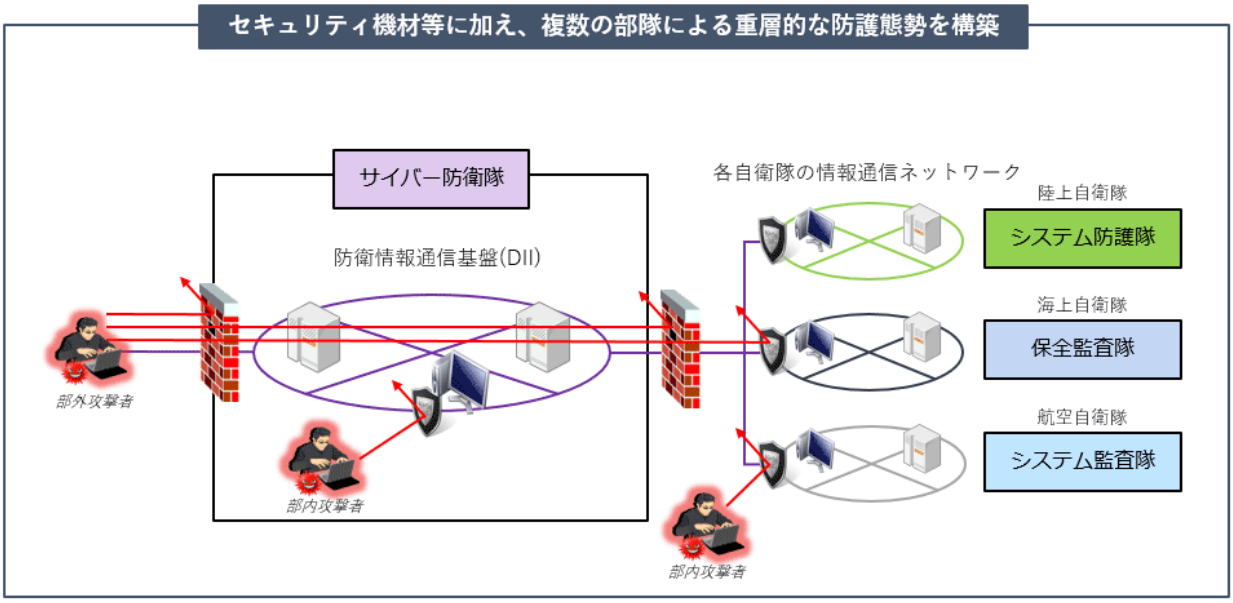


図 6 サイバー攻撃に対処する自衛隊の体制図[21](2022 年 3 月時点)

現在、サイバー防衛隊を中心とした自衛隊のサイバー関連部隊は約 800 人態勢だが[22]、防衛力整備計画 [16] によると、2027 年度までに 4,000 人規模に拡充する。また、その他の隊員にも教育を行う等して、サイバー防衛隊を側面支援する要員を 1 万 6,000 人育成し、サイバー攻撃に対処する人員をあわせて 2 万人程度配備する。

サイバー要員を育成する基盤の拡充策として、通信機電子機材の整備や電子戦を担う陸上自衛隊通信課の学校「通信学校」を、サイバー領域の作戦能力の強化も含めた「陸上自衛隊システム通信・サイバー学校」に改編する。

他には、ゼロトラストやリスクマネジメントフレームワーク（RMF）の導入、スレット（脅威）ハンティングの強化、といった取り組みも挙げられている。最新のサイバー脅威を踏まえ、ファイアウォール等で内部ネットワークを安全に保とうとする境界型セキュリティから脱却し、もはや安全なネットワークは存在しないとの前提に立ち、サイバー領域のセキュリティ強化の取り組みを進め

[20] 出典：読売新聞オンライン『自衛隊「サイバー防衛隊」５４０人態勢で発足…中国は１７万人、北朝鮮も６８００人』
https://www.yomiuri.co.jp/politics/20220317-OYT1T50257/

[21] 出典：防衛省・自衛隊『自衛隊のサイバー攻撃への対応について』
https://www.mod.go.jp/j/publication/shiritai/cyber/index.html

[22] 出典：時事通信『サイバー要員、２万人規模に 「能動的防御」戦略文書明記へ―防衛省』
https://www.jiji.com/jc/article?k=2022120600973&g=pol

る。

2.3. まとめ

今回閣議決定された 3 文書には、能動的サイバー防御を行うための自衛隊のサイバー対応能力の強化や、NISC を発展吸収した新組織の設立等が盛り込まれた。今後は、その活動に根拠を持たせるための人員や法の整備が進む。特に攻撃を受ける前に検知するための監視活動は「通信の秘密」や「不正アクセス禁止法」との整合性が必要と考えられることから [22]、細部の検討に注目したい。

3. フィッシングを行う Royal ランサムウェアグループ

3.1. 概要

ランサムウェアグループは、組織内部への入り口に設置してある VPN 機器やリモートデスクトップの脆弱性を攻撃して、内部へ侵入することがよく知られているが、新興の Royal ランサムウェアグループ（以下 Royal）は、コールバック・フィッシングやマルバタイジングといった人のミスにつけ込んで侵入し攻撃を拡大している。

3.2. Royal ランサムウェアグループ

Royal は、「身代金の支払いに応じなければ、データを自身の（暴露）サイトで公開する」と脅迫する暴露型ランサムウェアグループである。2022 年 5 月に活動を停止した Conti ランサムウェアグループから独立したとされる新興グループで、9 月から活動が観測されている[23]。

2022 年第 4 四半期の暴露サイト別投稿件数を集計したところ、Royal は LockBit に続いて 2 番目に多く（図 7）、登場して間もないグループにもかかわらず勢力を伸ばしていることが確認できる。被害組織の多くは規模の小さい民間企業である。これは、コロニアルパイプラインの攻撃によって米国からの圧力で活動を停止した Darkside ランサムウェア等を教訓にし、社会的に大きな影響を与えて国際的な問題になることを避けるという、昨今のランサムウェアのトレンドに沿ったオペレーションを実行していると考えられる。

Royal の被害組織の大半は米国に存在する。また一般的に中国系企業がランサムウェアによる被害に遭うことは少ないが、Royal は中国系に対しても攻撃を実行している。これまでのところ Royal による日本国内への攻撃は確認されていないが、日本企業（食品関連）の米国子会社のデータを暴露サイトで確認することができる。

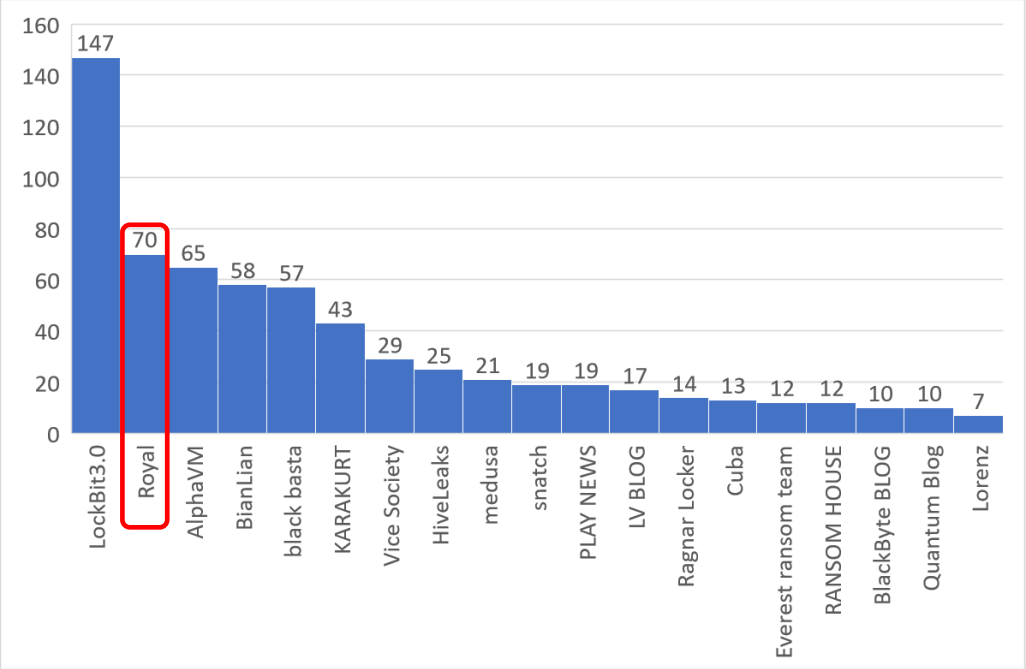


図 7 2022 年第 4 四半期 暴露サイト別投稿件数（当社調べ）

[23] 出典：Bleeping Computer『Royal ransomware claims attack on Queensland University of Technology』 https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-on-queensland-university-of-technology/

Royal はファイルを暗号化すると、被害組織の PC に犯行声明と暴露サイトへのリンクを記した README.TXT ファイル（図 8）を残して脅迫し、身代金を要求する。2022 年 12 月の米通信会社 Intrado の被害事例では、Intrado で発生した電話サービス等の障害は自分たちの攻撃によるものと Royal は主張し、身代金として最初に 6,000 万ドルを要求したといわれている[24]。暴露サイトを確認したところ、脅迫のために Intrado から窃取した内部文書や従業員のパスポート画像データ等が公開されていた。（図 9、図 10）

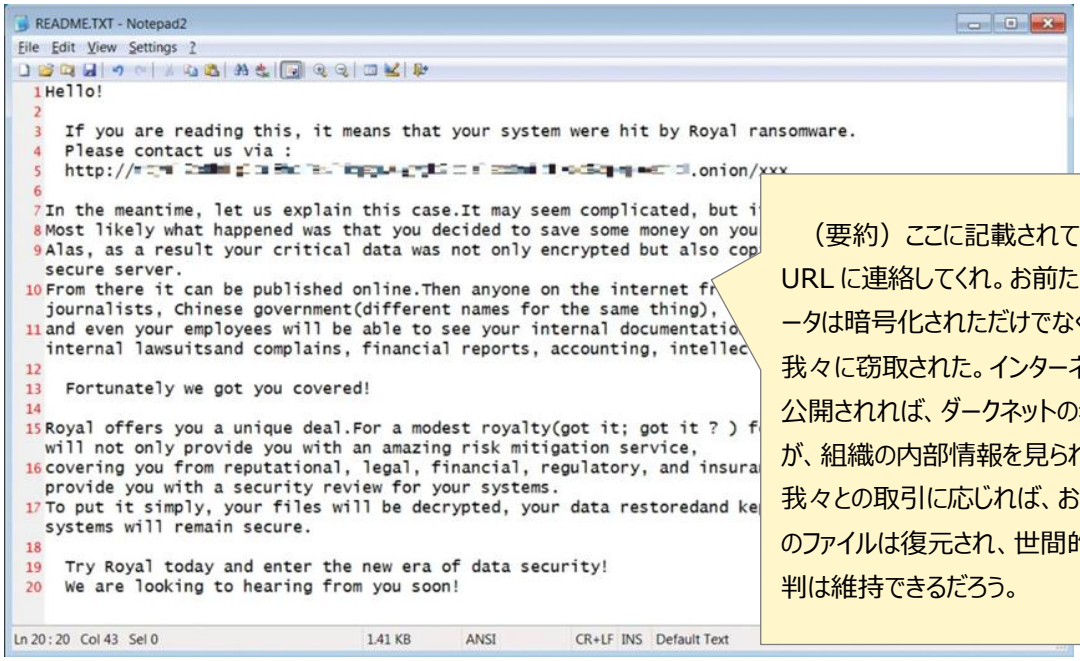


図 8　Royal が被害組織の PC に残す身代金要求メモ [25]

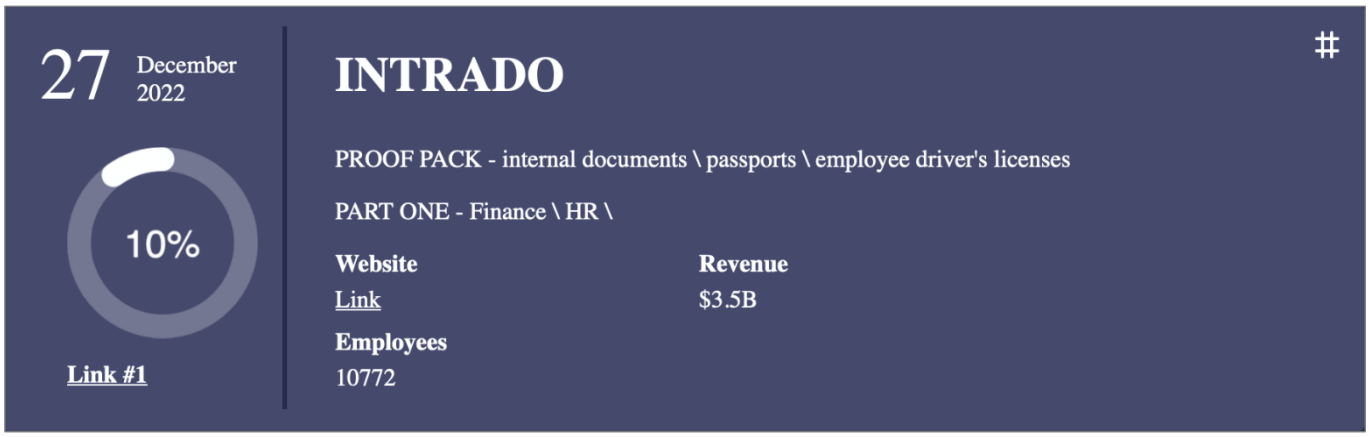


図 9　Royal のサイトにある Intrado の暴露状況画面

[24] 出典：Bleeping Computer『Royal ransomware claims attack on Intrado telecom provider』
https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-on-intrado-telecom-provider/

[25] 出典：Bleeping Computer『New Royal Ransomware emerges in multi-million dollar attacks』
https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

図 10 Royal に暴露されたパスポートデータの一部

3.3. Royal の攻撃手法

Royal はターゲットをランサムウェアに感染させるために、さまざまな手法を駆使する。

【コールバック・フィッシング】[26]

Royal は未払いの請求書などに偽装したフィッシングメールをターゲットに送り、記載されている電話番号に連絡を促す。このような、偽のサポート窓口へと電話連絡を誘導するフィッシングを**コールバック・フィッシング**と呼ぶ[27]。そして、Royal は電話をかけてきたターゲットを騙し、マルウェアをインストールさせるなどしてターゲットが関係する組織へ侵入する。

ある事例では、Royal からターゲットに送られたフィッシングメールはサブスクリプションの更新を偽装しており[25]、そこには「契約をキャンセル場合は電話するように」と記載されていた。ターゲットが電話をかけると、偽のオペレーターにより遠隔操作ツールをインストールさせられ、これが組織への侵入口となった。

【マルバタイジング】[28] [29]

Royal は Web 広告を悪用してマルウェアの配信を行う**マルバタイジング**も導入している。TeamViewer、Adobe Flash Player、Zoom など、著名ソフトの偽インストールサイトを作成し、Google 広告を悪用して特定の条件に当てはまるターゲッ

[26] 出典：Bleeping Computer『Callback phishing attacks see massive 625% growth since Q1 2021』
https://www.bleepingcomputer.com/news/security/callback-phishing-attacks-see-massive-625-percent-growth-since-q1-2021/

[27] 出典：Trend Micro『Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks』
https://www.trendmicro.com/en_id/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

[28] 出典：OCN『いまや定番の攻撃手法に！？ ネット広告を表示しただけでウイルス感染のワケ』
https://service.ocn.ne.jp/ocn-security/case/column/20150709.html

[29] 出典：CrowdStrike『WHAT IS MALVERTISING』
https://www.crowdstrike.com/cybersecurity-101/malware/malvertising

トを偽サイトに誘導する。この偽サイトで、正規ソフトと偽ったマルウェアをターゲットにインストールさせることで、バックドアを仕掛けることが観測されている[30]。

3.4. まとめ

コールバック・フィッシングやマルバタイジングなど人のミスに付け込んだ攻撃は有効だったとみえ、Royal は短期間のうちにランサムウェアの主要アクターに成長することに成功した。Royal をはじめとするランサムウェアの攻撃者の活動は日々変化し、新たなグループも発生している。セキュリティ担当者は最新の攻撃手法や傾向の情報を入手し、従業員への周知や教育、対策策定に生かすことが肝要である。

以上

[30] 出典：Microsoft『DEV-0569 finds new ways to deliver Royal ransomware, various payloads』 https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス： WA_Advisorysupport@ntt.com