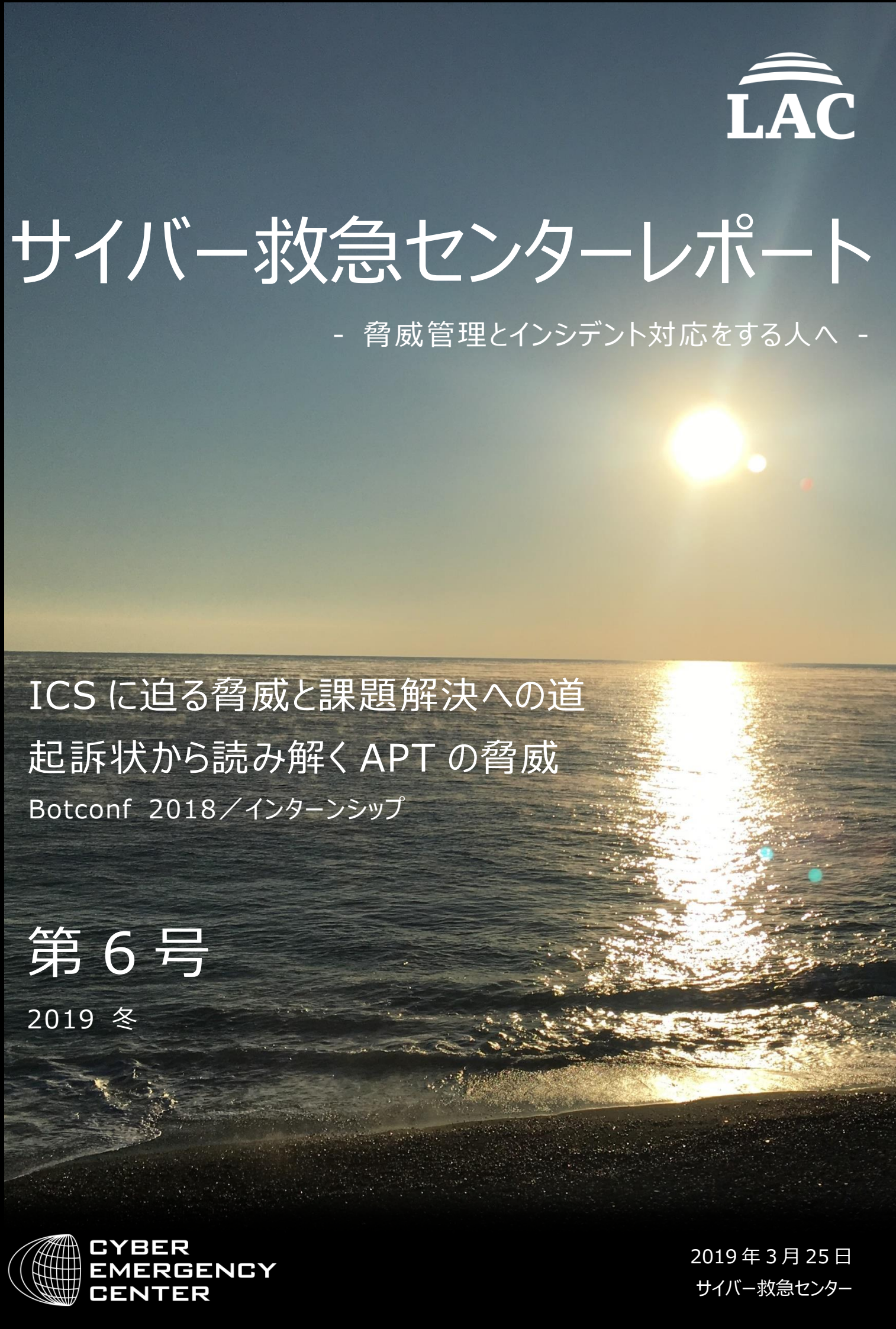


サイバー救急センターレポート

- 脅威管理とインシデント対応をする人へ -

ICS に迫る脅威と課題解決への道

起訴状から読み解く APT の脅威

Botconf 2018／インターンシップ

第 6 号

2019 冬

CYBER EMERGENCY CENTER

2019 年 3 月 25 日

サイバー救急センター

サイバー救急センターレポート

第 6 号 / 2019 冬

目　　次

03 はじめに

04 サイバー119 の出動傾向

07 特集：ICS に迫る脅威と課題解決への道
（ICS: Industrial Control System, 産業用制御システム）

15 脅威分析報告
- 起訴状から読み解く APT の脅威

20 コラム：セキュリティ百景
#11 Botconf での発表
#12 インターンシップ フォレンジックコース開催

22 編集後記

はじめに

内田 法道

株式会社ラック
サイバー救急センター長

金銭目的の攻撃者グループの攻撃手段を振り返ってみると、不正送金マルウェア（バンキングマルウェア）～ ランサムウェア（PC を狙ったもの）～ コインマイナー（暗号通貨の発掘）～ ビジネスメール詐欺（Bussiness Email Compromise）～ ランサムウェア（サーバを狙ったもの）と、変遷してきています。もちろん、今でも不正送金マルウェアや PC を狙ったランサムウェアのバラマキ型メールは確認されていますので、攻撃手段の変遷というよりは、攻撃手段の多様化というのが正しい表現かもしれません。

この多様化の方向としては、対象が個人よりも法人へと進んでいるように感じています。BEC やサーバを狙ったランサムウェア等は、明らかに企業や組織を対象としています。そのため、組織の CSIRT においては、APT 攻撃（高度な標的型攻撃）だけでなく金銭目的の攻撃者グループの脅威動向も注視する必要があると思います。

最近相談を受けたある組織では、DB サーバの管理者アカウントのパスワードが勝手に変更されていました。変更の意図は不明ですが、DB サーバのバックアップデータやトランザクションログ等の復元手段が削除され、データの暗号化やアカウント削除の上で、管理者アカウントのパスワードが変更された場合に、DB のデータを狙った新手の脅迫という可能性も考えられます。

想定外を想定内に。常に脅威の想定を見直して、想定外に備えていきましょう。

サイバー119 の出動傾向

2018 年 10 月～12 月の出動傾向

この期間も、Microsoft Office 365 のクラウド型メールサービスを不正に利用された組織からの相談が多くありました。原因としては、Microsoft アカウントの窃取を目的としたフィッシングメールを受信した利用者が、メール内に記載されている偽の Web サイトにアクセスし、アカウント情報を入力した可能性が考えられます。本事案の内容と対策については、前号のサイバー救急センターレポート 第 5 号 [1] を参照ください。

また、ランサムウェアに感染しデータが暗号化された組織からの相談が増加傾向にあります。原因としては、インターネットから RDP（Remote Desktop Protocol）接続されて、ランサムウェアを実行されたことを確認しています。RDP サービスについては、不用意にインターネットからアクセスできないか、また容易に推測可能なアカウント名やパスワードを設定していないか改めて確認することを推奨します。

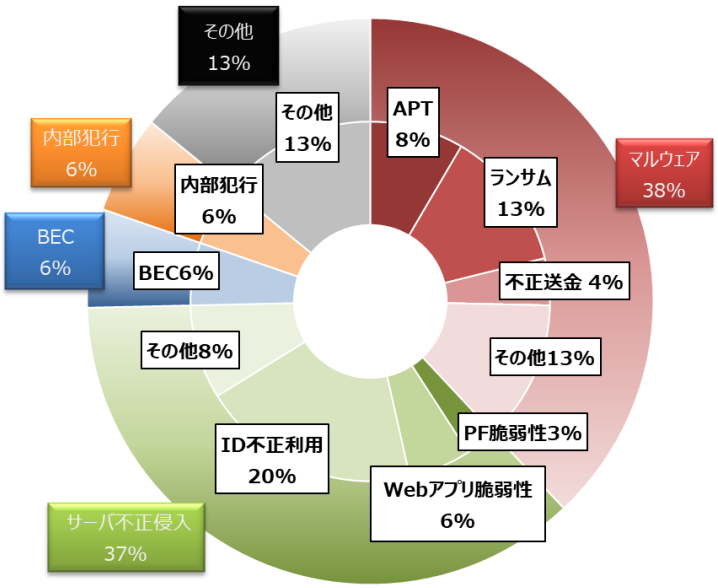


図 1-1 2018 年 10 月～12 月のインシデント傾向

1 サイバー救急センターレポート 第 5 号
https://www.lac.co.jp/lacwatch/report/20181130_001730.html

マルウェア関連のインシデント傾向

(1) APT 攻撃（Advanced Persistent Threat 攻撃、標的型攻撃）

APT 攻撃と推測されるインシデントの相談を、複数の組織から受けています。当該組織は、過去にも APT 攻撃を受けており、攻撃者グループは執拗に当該組織を標的にして攻撃をしているものと考えられます。

攻撃者グループにとって攻撃する価値がある（有益と思われる情報を保持している等）と思われている組織は、その価値を失うまで執拗かつ継続的に攻撃を受けることになります。過去に ATP 攻撃の被害を受けた組織において、同一グループからの APT 攻撃により、再度内部への侵害を許した場合、以前に侵害した際の情報をもとに探索活動や、侵害端末の拡大のスピードが速まる傾向にあります。

そのため、攻撃者グループが組織内のネットワーク構成や運用についてある程度の知識を有しているという想定で対応策を検討する必要があります。セキュリティ製品の追加導入などによる多層的な防御に加え、ネットワーク構成や運用の抜本的な見直しを行う覚悟を持つ必要があると考えられます。

2020 年の東京オリンピック・パラリンピックを控え、日本国内の組織では、セキュリティ対策のレベルを高めるために、ゲートウェイやエンドポイントのセキュリティ製品およびソリューションの導入を検討しているものと思われます。そのような追加の対策の検討だけでなく改めて基本に立ち返って、現在の業務内容、ネットワーク環境、システム構成を整理して、インシデントが発生しても被害範囲を最小化できるような構成へと、「肉体改造」するという観点で、セキュリティ対策を再検討することを推奨します。

(2) ランサムウェア

ばら撒き型メールによるランサムウェア感染の相談は減少傾向にありますが、インターネットからアクセス可能なサーバやモバイル PC がランサムウェアに感染してデータが暗号化されたという相談が増加しています。

相談が多いランサムウェアの種類としては、Dharma や GandCrab の相談が増加しています。これらのランサムウェアの感染経路は複数ありますが、弊社への相談においてはインターネットから Windows の標準機能である RDP 接続でログオンしてランサムウェアを実行された事象を多数確認しております。残念ながら、侵害された機器では容易に推測可能なパスワードが設定されていることが多く、辞書攻撃などでパスワードが推測されて不正ログオンされたものと考えられます。

一般的に、暗号資産（仮想通貨）で身代金を要求する脅迫文が作成、表示されることから、攻撃者グループの目的は金銭であると考えられます。しかしながら、相談を受けたある組織のインシデントにおいては、脅迫文を作成、表示しないランサムウェアや、ランサムウェア以外のマルウェアが実行されていた痕跡

を確認しています。この事象は、攻撃者グループが侵害に関連する痕跡を隠滅するためにランサムウェアでファイルを暗号化したのではないかと推察しています。もし、ランサムウェアに感染してファイルが暗号化されたにも関わらず脅迫文が確認できない場合には、攻撃者の目的が情報窃取である可能性にも配慮してインシデント対応することを推奨します。

インターネットからの RDP 接続で不正侵入やランサムウェア感染の被害にあわないために、ファイアウォールなどのアクセス制御機器の制御ルールを再確認し、不適切な設定になっていないか確認することを推奨します。

特集： ICS に迫る脅威と課題解決への道

郷 晴奈

私は現在、「IPA（独立行政法人情報処理推進機構） 産業サイバーセキュリティセンター」が提供している「中核人材育成プログラム[2]」を受講しています（図 2-1）。同センターは、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応する人材・組織・システム・技術を創出するため、2017 年 4 月に発足した組織です。また本プログラムは、社会インフラや産業基盤のサイバーセキュリティを強化することを目的とし、IT（情報技術）と OT（運用・制御技術）・マネジメント・ビジネス分野を総合的に学ぶ 1 年間のカリキュラムとなっています。更に同センターでは、電力や鉄道など各種業界向けや経営層向けの短期プログラムも年間を通して提供しており、産業界全体のサイバーセキュリティレベルの底上げを図っています。

図 2-1 制御機器を利用した「インシデント対応・BCP」の講義風景

2 中核人材育成プログラム | IPA
https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html

皆さんは、「社会インフラや産業基盤のサイバーセキュリティ強化」と聞いて、どのような印象を持たれるでしょうか。私は本プログラムを受講するまで、社会インフラや制御システムなど、いわゆる ICS（Industrial Control Systems：産業用制御システム）には縁が無かったため、サイバーセキュリティを強化することの必要性や、具体的にどのようなサイバー攻撃の脅威があるのか考えるきっかけがありませんでした。

しかし、本プログラムを受講し、模擬システムを利用した演習を通して ICS を知っていく中で、ICS のサイバーセキュリティ強化の必要性を強く感じるようになっています。本稿では、ICS におけるサイバーセキュリティの現状をお伝えするとともに、サイバー攻撃の脅威事例をいくつか取り上げ、それら脅威に対してセキュリティ対策を施そうとした場合、どのような課題があるのか提起したいと思います。

ICS におけるサイバーセキュリティの現状

(3) ICS に対するサイバーセキュリティ意識

国内の ICS に対し、どの程度サイバーセキュリティが意識されているのかを知るための統計情報として、2015 年に JPCERT/CC が実施した「制御システムセキュリティに関するアセットオーナ実態調査[3]」が挙げられます。本統計情報によると、「ICS 製品における今後のセキュリティ対策を強化していく、または対策に取り組む必要がある」と回答したアセットオーナは 4 割未満となっており、また、7 割以上が「ICS 製品でこれまでも今後もセキュリティインシデントが発生する可能性は低い」と回答しています。

これらの統計から、国内における ICS に対するサイバーセキュリティ意識は低いということが分かります。その要因は、本統計情報の分析結果でも述べられているとおり、これまでの ICS ネットワークの構成にあります。つまり、拠点間の接続には専用線などを利用していること、外部・内部のネットワークと切り離された環境にあることから、ICS のネットワークはセキュアな構成になっていると考えられています。そのため、外部から ICS の可用性に関わるサイバー攻撃を受ける可能性は低いという考えにつながり、サイバーセキュリティを身近な脅威として感じられないことが現状であると言えます。更に国内では、性善説に基づくところが大きく、内部犯行によるリスクも低く捉えられがちであることも要因と考えられます。

---

3 2015 年度 制御システムセキュリティに関する アセットオーナ実態調査 | JPCERT/CC
https://www.jpcert.or.jp/ics/asset-owner-survey_2015.pdf

(4) 「つながる産業」に伴うネットワーク環境の変革

上述のとおり、従来の ICS はセキュアなネットワーク構成の上に、ある程度のセキュリティが保たれていると言っても過言ではありません。しかし今、ICS のネットワーク環境は大きな変革を迎えています。それを牽引するものとして 2017 年 3 月に経済産業省が発表した「Connected Industries[4]」が挙げられます。

「Connected Industries」は、「様々なつながりにより新たな付加価値が創出される産業社会」をコンセプトに、生産システム全体の最適化を図ろうとしています。

例えば生産ライン上の機械の稼働状況やエネルギー消費量などのデータを収集・見える化し、無駄を省くことで生産性を向上させることや、熟練者に依存していた技能をデータ化し後世への技能継承を容易にすること、効率化と自動化を推進し人材不足を解消することなどが挙げられます。

このような「つながる産業」を実現するためには、ICS が今まで以上にネットワークにつながることが必要不可欠です。即ち、ICS セキュリティの主柱となるセキュアなネットワークが徐々に外部とつながっていく可能性を示唆しており、サイバー攻撃の脅威に晒される可能性も必然的に増すことが考えられます。

国内も例外ではない、サイバー攻撃の脅威

(1)サイバー攻撃の標的となり得る ICS

外部からの脅威が増したとしても、ICS に対するサイバー攻撃は主に海外の事例が多く、国内の ICS が標的になる可能性は低いのではないかと思われています。しかし、警察庁が 2016 年 3 月に発表した「情報技術解析平成 27 年報[5]」によると、国内メーカ製 PLC[6]を標的とした外部からのアクセスが多数観測されており、そのうち一部のアクセスに関しては、脆弱性を悪用する目的で探索活動を行っている可能性もあると記載されています。

更に、日本では 2020 年に東京オリンピック・パラリンピックが、2025 年には大阪万博と、国際的なイ

---

4 Connected Industries について | 経済産業省
http://www.meti.go.jp/press/2017/06/20170619005/20170619005-2.pdf

5 情報技術解析平成 27 年報 | 警察庁情報通信局情報技術解析課
https://www.npa.go.jp/cyberpolice/detect/pdf/H27_nenpo.pdf

6 Programmable Logic Controller. 従来からあるリレー回路の代替として開発された制御装置の一つ。
工場の組立ラインやビルのエレベータなど様々な機械を自動制御する際に用いられる

ベントも控えており、世界の注目が得られる場で、大きなインパクトを与えることができる ICS は、サイバー攻撃者にとって格好の標的になることも考えられます。

これらの背景から、国内の ICS も決して例外ではなく、サイバー攻撃の脅威に晒される可能性が高くなっていると考えられます。

(2) ICS のサイバー攻撃事例 1 – 攻撃と隠蔽工作 -

ICS のサイバー攻撃事例でよく取り上げられるマルウェア「Stuxnet」は、2009 年から 2010 年にかけてイランのウラン濃縮施設に侵入し、約 1,000 基の遠心分離機を制御不能にさせたと言われています。

この事例に関わらず、本来、ICS は何か異常が発生した場合は安全稼働に傾くよう作られており、かつ監視システムによって、作業員が迅速に異常に気付けるようになっています。しかし、「Stuxnet」の場合は PLC のプログラムを不正に書き換え、何ヶ月にもわたって遠心分離機の周波数がアップダウンを繰り返し、正常稼働できない状態にしていました。その一方で、作業員が異常に気づけないよう、あらかじめ記録しておいた正常時のデータを監視システムに送信し続けるという隠蔽工作も行っていました。

つまり、攻撃と隠蔽が同時に行われていたと言えます。

本プログラムのうち、「インシデント対応・BCP」の講義においても、ICS のサイバーセキュリティを考えるために、まず ICS がどのように攻撃対象となり得るのかを学びます。

ICS へのサイバー攻撃による物理的変化は、コントローラ（単独のセンサーも含む）を通して発生します。そのため、予想外のサイバー攻撃が発生しても、ICS にとってその事象は「コントローラの誤動作・誤操作」と同義と捉えることができます。

このコントローラの誤動作・誤操作は、プラント設計段階の安全解析・対策で検討済のため、サイバー攻撃で発生し得る事故も想定内の事象であると考えられます。そのため、プラントに組み込まれた多重安全対策により、例えばコントローラの設定値が改ざんされたとしても、すぐにプラントが危険な状態になるわけではありません。工場も、鉄道も電力も、最終的には手動運転に切り替えることも、自動で緊急停止することもできます。

しかし、前述した安全解析・対策では多くの場合、単独事故を想定しており、攻撃者の悪意を伴う事象が同時多重（自然故障ではなかなか起こりえない事象）に発生することまでは想定されておらず、サイバー攻撃に耐えうる十分な対策が取られているとは言えません。

例えばコントローラの設定値だけではなく、ICS を監視するシステムの表示値も同時に改ざんされてしまうと、多重に用意された安全対策が機能しなくなり、大事故につながる可能性があります。そのため、サイバー攻撃を考慮する際は、隠蔽工作の視点からも注意しなければなりません。

「インシデント対応・BCP」の講義では実際の制御機器を使用した演習を行い、上述の例のようにコントローラの設定値が改ざんされ、異常状態になっていても、監視システムにはその異常が表示されないという状況を、実際に発生させることが可能であると学びました（図 2-2）。これにより、私は制御システムに対する攻撃・隠蔽工作が絵空事ではなく、実現可能な脅威であることを体感しました。また、PLC などが設置されている制御ネットワークは、システムの処理にリアルタイム性が求められることが多く、このような攻撃や隠蔽を検知できる十分なセキュリティ製品を導入することが困難であると知り、ICS におけるセキュリティ対策の難しさについて改めて考えさせられました。

図 2-2 演習で利用する模擬プラント（産業サイバーセキュリティセンター事業案内より引用）

(3) ICS のサイバー攻撃事例 2 – エアギャップ環境における被害 -

外部のネットワークから隔離されたいわゆるエアギャップ環境にある制御システムも、サイバー攻撃の対象になり得ます。国内でも、保守 PC や USB メモリが制御ネットワーク内の機器に接続されたことで、マルウェアに感染した事例が複数報告されています。例えば自動車工場で発生した事例では、保守用 PC を感染源としてマルウェアが工場内ネットワークに侵入し、10 日間操業停止になったことで、売上が 30 億円減少したという被害が生じました[7]。また、半導体工場で発生した事例では、USB メモリ経由で品質検査を行う検査装置がマルウェアに感染したことで、不良品を良品と誤認識して出荷し、更にはその異常の

7 サイバー攻撃の事例集 | 株式会社ＩＣＳ研究所
https://www.ics-lab.com/pdf/journal/18/journal-18-2.pdf

原因が特定できず生産ライン停止に至った[8]と報告されています。

また2018年9月には、鋼板加工機器が工場内に導入された時点で既にマルウェアに感染しており、およそ2年間にわたって不審なDNSクエリを発生させ続けていたという事例も報告されています[9]。

これらの事例から、マルウェアに感染した機器やUSBメモリの接続により、エアギャップ環境にある制御システムでも、サイバー攻撃の対象になり得ることが分かります。

サイバーセキュリティ対策に係る課題

上述のとおり、今日のICSにおいて、「ネットワークから隔離されているから安心」という考えは通用しないほど、サイバー攻撃が身近な脅威になっていることがうかがえます。一方で、それら脅威に対してサイバーセキュリティ対策を講じることがいかに困難か、講義や受講生の声から学ぶことが多くあります。

(1)異常に対する切り分けの難しさ

例えばサイバー攻撃による異常が発生しても、現場で作業をしている人たちは、まず機器故障や誤動作を疑い、サイバー攻撃を疑う可能性は極めて低いということが課題として挙げられます。その要因として、事象がサイバー攻撃であるかまたは機器故障・誤動作であるかを切り分けるに足るセキュリティ機能が、制御機器そのものに組み込まれていないことに加え、セキュリティ情報を得るに十分なセキュリティ製品やログ取得機能が導入されていないこと、サイバーセキュリティに関する教育が行き届いておらず、異常とサイバー攻撃を紐づけるに至らないことなどが考えられます。

このように、現場だけでサイバー攻撃の脅威に気づくことは困難であるため、インシデントの早期発見につなげるにはIT部門含めどのような連携をとる必要があるのか組織体制の見直しを検討したり、サイバー攻撃の脅威を認識するために必要な教育を実施したりすることなどが求められます。

また、コストとの兼ね合いは難しいところですが、今日のサイバーセキュリティの情勢を鑑みると、インシデント発生時に原因究明や被害最小化を図れるよう、制御機器自体にサイバー攻撃に備えたセキュリティ機能を組み込むことや、ICSネットワークへのセキュリティ製品の導入やログ取得方法の見直しを検討していく必要もあると考えます。

---

8 事例から見る、製造現場でのセキュリティ導入の“ツボ” | MONOist
http://monoist.atmarkit.co.jp/mn/articles/1402/12/news082.html

9 サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2018 年 7 月～9 月]
https://www.ipa.go.jp/files/000069662.pdf

(2) セキュリティ対策の難しさ

組織によっては OT 部門と IT 部門の連携がスムーズではなく、サイバー攻撃に対するセキュリティ対策に共通理解を得られないことがあります。例えば製造業などでは、セキュリティ製品を導入することが原価コストの上昇に直結するため、容易にセキュリティ対策にコストをかけられないという課題があります。また、可用性が重要視されるICSにおいて、セキュリティパッチの適用は制御システムの安定稼働を損ねる可能性があるため、これもまた容易に実施できません。

セキュリティ製品の導入タイミングも課題の一つです。上述のとおり ICS では可用性が重要視されるため、通常稼働時にセキュリティ製品を導入することは容易ではありません。あらかじめ決められている計画停止時に導入することも考えられますが、計画停止時は機器のメンテナンスなど、優先的に実施しなければならない項目が多くあり、セキュリティ製品導入の優先順位は下げざるを得ない場合もあります。

経営層などステークホルダーの理解と協力を得ることも、ICS のセキュリティ対策を考える上で必要不可欠です。特に ICS のセキュリティ強化は自組織だけではなく、サプライチェーンも含めて全体的に対策していく必要があるため、様々な部門・組織が一丸となってセキュリティ対策に関与することが求められます。

各業界で組織体制も風土も異なるため、統一的なベストプラクティスを見出すことは困難ですが、例えば NISC（内閣サイバーセキュリティセンター）が公開している「サイバーセキュリティ戦略[10]」より、組織がサイバーセキュリティで目指すべき姿や方針、取り組み方などを参考にしたり、IPA が公開している「制御システムのセキュリティリスク分析ガイド[11]」などを活用することで、自組織のリスクアセスメントを実施し、組織が護らなければならない資産を明確化したりすることも、推進方策の一つとして考えられます。これにより、事業継続を考える上でどのようなリスクが存在するのか把握し、ステークホルダーにセキュリティ対策の必要性を認識してもらったり、限られたリソースの中で優先的に対策していくべき範囲はどこなのか検討したりと、次のステップへ発展していくことにもつながります。

10 サイバーセキュリティ戦略 | NISC（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
11 制御システムのセキュリティリスク分析ガイド 第 2 版 | IPA
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

おわりに

私は、講義や受講生の声からこのような課題を聴くことで、ICSにおいてサイバー攻撃が身近な脅威となりつつも、実際にセキュリティ対策を施すことが困難であるという現実を痛感しています。

しかし、その現実を受け止め、一歩ずつでもセキュリティ強化に向けて歩んでいく必要性も強く感じています。

そのためには、ICS のサイバーセキュリティに対する一人一人の意識を向上させていくことが必要不可欠です。ICSのサイバーセキュリティは発展途上にあり、手探りで進めていかなければならないことも多くありますが、まずはICSサイバーセキュリティの先駆者として一歩踏み出し、自組織で出来ることから対策に取り組んでいただくことが肝要と考えます。

例えば、OT 部門と IT 部門の隔たりが大きく、いきなりセキュリティを持ち込むと反発がありそうな場合は、双方の立場や文化、考え方を知るコミュニケーションの場を設けることも大きな一歩になります。

また、受講生同士の討議から得た学びとして、老朽化更新でシステムが刷新されるタイミングを見据え、安定稼働のみにとらわれるのではなく、セキュリティ強化に向けた中長期のロードマップを積極的に策定していくことも大切です。

このような取り組みを積み重ねていくことで、徐々に協働の輪を広げ、ICS のサイバーセキュリティ発展につなげていただきたいと思います。

脅威分析報告

起訴状から読み解く APT の脅威

アメリカの司法省は、2018 年 12 月 20 日に「APT10」と呼ばれるグループ（別名 Red Apollo、CVNX、Stone Panda、MenuPass、POTASSIUM とも呼ばれる）に属する 2 人を訴追したことを発表しました[12]。起訴状によると、2 人は中国の Tianjin Huaying Haitai Science and Technology Development Co Ltd.（天津华盈海泰科技发展有限公司）の従業員で、Ministry of State Security（中国国家安全省）の傘下にある天津市国家安全局に協力して、複数の国の企業や組織のコンピュータに侵入し、知的財産や技術および営業に関する機密情報を窃取したとされています。

これを受けて、オーストラリア、カナダ、ニュージーランド、イギリス、日本[13]の各国政府は、APT10 の活動を非難する声明をほぼ同時に発表しており、アメリカ司法省による訴追に関して、あらかじめ各国の政府に対して情報が連携されていた可能性も考えられます。今回の訴追および各国政府からの一連の非難声明は、APT10 のような政府機関や企業の情報を狙う攻撃グループによる非合法活動を公に警告し、縮小させることが狙いの一つだと考えられます。

アメリカ司法省の起訴状によると、APT10 は少なくとも 2006 年から活動していることが報告されており、訴追の根拠となった 2 つのキャンペーンにより、ターゲットの組織からデータ、知的財産、技術および営業上の機密情報を盗んだとされています。サイバー救急センターでも、APT10 に関連すると思われるインシデント対応を行っており、得られた脅威情報についてはレポートにて公開してきました[14]。

---

12 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

13 https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

14 https://www.lac.co.jp/lacwatch/people/20170223_001224.html
https://www.lac.co.jp/english/report/2017/08/30_alert_01.html
https://www.lac.co.jp/lacwatch/people/20180521_001638.html

本稿では、アメリカの企業や組織がどのような被害を受けたのかという点を、起訴状から読み解きます。起訴状には、2 つのキャンペーンに関して、手口やターゲットが記載されており、要約を以下に記載します。

キャンペーン① 技術情報の窃取

- ターゲットのコンピュータをマルウェアに感染させるために、標的型攻撃メールを送りつけます。メールは、ターゲットに関連する実在する別の企業を詐称しており、サブジェクトや添付ファイルは、ターゲットの業務に関連するような興味を引く内容となっています。添付ファイルは、Word ファイルなどで、これを開いてしまうと”Poison Ivy”などのカスタマイズされた RAT とキーロガーがインストールされ、感染したコンピュータから ID やパスワードを窃取します。
- マルウェアの接続先であるドメイン名は、アメリカ国内のダイナミック DNS プロバイダーにホスティングされており、ドメイン名に紐付けられた IP アドレスは攻撃者の制御によって頻繁に変更されます。これにより、不正な IP アドレスの検知を困難にし、通信を止められないようにします。
- 次に、別のマルウェアやツールをダウンロードして、他のコンピュータへさらなる侵害を試みます。最終的に、対象のシステムから興味のあるファイルを収集し、暗号化したアーカイブファイルに纏めて外部に持ち出します。
- このキャンペーンの結果、少なくとも 90 台のコンピュータが侵害され、以下の民間の防衛関連企業、および少なくとも 12 の州のアメリカ政府機関から、数百ギガバイトの機密情報が盗み出されました。
    - 7 つの航空、宇宙技術および衛星技術に関わる企業
    - 3 つの通信技術に関わる企業
    - 3 つの高度電子システムや実験用分析機器の製造に関わる企業
    - 1 つの海事技術に関わる企業
    - 1 つの油やガスの採掘、生産、および加工に関わる企業
    - NASA ゴダード宇宙飛行センター
    - NASA ジェット推進研究所
- 上記の他に、産業用オートメーション、レーダ技術、石油探査、情報技術サービス、医薬品製造、およびコンピュータプロセッサ技術に関わる少なくとも 25 の他の技術関連企業と、エネルギー省ローレンス・バークレー国立研究所のコンピュータの侵害に成功しています。

キャンペーン② MSP（マネージド・サービス・プロバイダー）からの認証情報の窃取

- まず、MSP のコンピュータに「キャンペーン① 技術情報の窃取」と同様の手法で侵入します。侵害に成功すると、PlugX、RedLeaves、QuasarRAT の名称で知られる複数のカスタマイズされたマルウェアを、各国にある MSP のコンピュータにインストールします。マルウェアは、対象コンピュータで使用されている正規ファイルに偽装することで、アンチウイルスによる検知を回避します。攻撃者は、これらのマルウェアを使用して、リモートからコンピュータをモニターして、複数のツールを用いてユーザの認証情報を窃取します。
- マルウェアは DNS サービスプロバイダーにホスティングされたドメイン名を使用して、攻撃者にコントロールされたコンピュータと通信します。このキャンペーンで使用されたドメイン名は約 1,300 程度あり、最も古いものは 2010 年からドメイン名が登録されています。
- MSP のコンピューから認証情報の窃取に成功すると、MSP の顧客のコンピュータシステムに、盗んだ認証情報を用いて RDP（Remote Desktop Protocol）で侵入を試みます。この方法により、攻撃者はマルウェアをターゲットにインストールすることなく、MSP と接続されたターゲットのコンピュータシステムへの侵入が可能になります。
- 次に、侵害したコンピュータシステムから、興味のあるファイルを盗んで、暗号化されたアーカイブファイルに保存します。さらに、盗んだ認証情報を用いて、MSP 自身だけでなく MSP の顧客企業のコンピュータ上に移します。最終的には、攻撃者の管理するコンピュータに、盗んだファイルが持ち出されます。攻撃者は、データを持ち出した後は、対象のファイルを削除してしまうため、持ち出されたファイルの検知や特定は困難になります。
- キャンペーンが実行されている間に、政府機関や民間企業から、何回か APT10 が使用している不正なマルウェアやドメイン名などがレポートで公開されています。その都度、攻撃者はマルウェアの亜種を作成し、新しいドメイン名を使ってキャンペーンを継続していました。これにより、侵害を受けた組織でのマルウェアの検知は難しくなりました。
- このキャンペーンの結果、複数の MSP と、MSP を利用していた 12 カ国の少なくとも以下の組織が被害を受けました。
  - 1 つのグローバルの金融機関
  - 3 つの通信および家電に関わる企業
  - 3 つの商業用もしくは工業用機器に関わる企業
  - 2 つのコンサルティング企業
  - 1 つのヘルスケア企業
  - 1 つのバイオテクノロジー企業

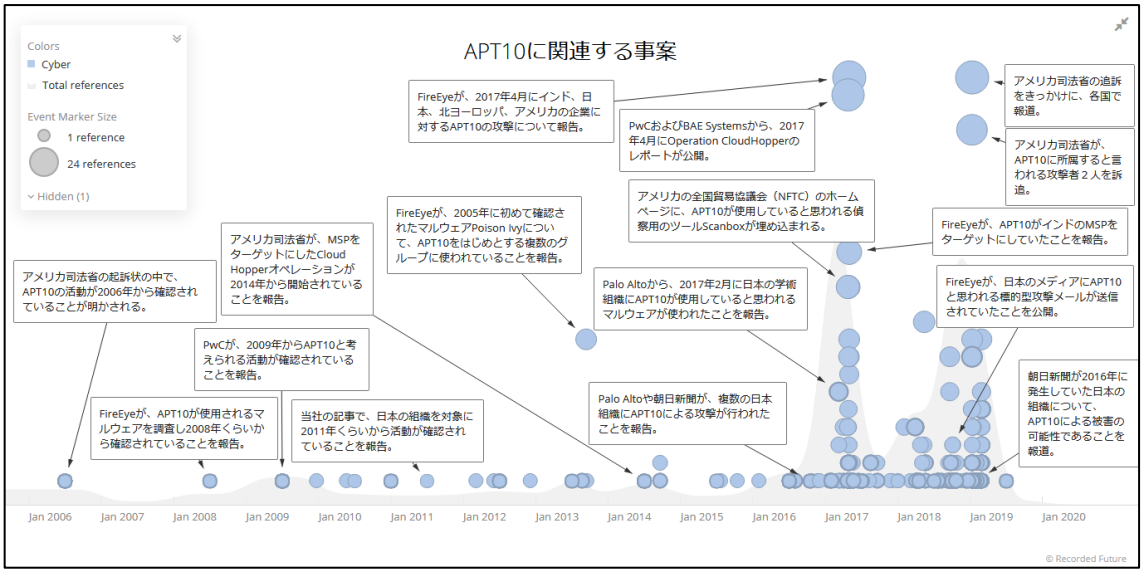
- 1 つの鉱業企業
- 1 つの自動車部品企業
- 1 つの掘削企業

- このキャンペーンで、海軍の 40 台以上のコンピュータを侵害し、100,000 以上の海軍人員の名前、社会保障番号、生年月日、給料、電話番号、メールアドレスが窃取されています。

おわりに

以上がアメリカ司法省の起訴状から読み取れる APT10 の活動です。サイバー救急センターでも、類似の業種に属する日本国内の組織において、APT10 によるものと思われるインシデントの対応を支援しています。

インターネット上に存在する公開情報をもとに、APT10 に関連すると思われる事案について、時系列で整理したものを紹介します。円はイベント（APT10 に関する記事等）を表し、円の大きさはイベントが他の記事などで参照された数を表します。



Source: Recorded Future

図 3-1 APT10 に関する事案

上図から、APT10 は 2006 年頃から活動しているものの、2017 年になって複数のセキュリティベンダーから多くのレポート等が公開され、注目を集めたことがわかります。今回のアメリカ司法省の訴追と、それに続く各国の非難声明が日本の新聞やメディアでも取り上げられたことで、APT10 の存在はさらに多くの人が知るところになりました。

FireEye 社のレポートによると、APT 攻撃により重大な侵害を受けた組織の 91%以上が、同じまたは似た動機を持った攻撃グループによって再びターゲットにされているとされています[15]。この確率は、特に日本を含むアジア太平洋地域が高いとされており、サイバー救急センターで対応した事案でも、複数の組織が繰り返し同じ攻撃者グループに狙われる事例を確認しています。

APT 攻撃に対処するためには、脅威情報をアップデートした上で継続的な対策が求められます。サイバー救急センターでは、APT10 のような攻撃グループの動向を引き続き注視し、皆様の役に立つ情報があれば本書または個別のレポートで公開いたします。

15 https://www.fireeye.jp/company/press-releases/2018/fireeye-releases-mandiant-m-trends-2018-report.html

コラム：セキュリティ百景 #11

Botconf 2018 での発表

2018 年 12 月 5 日(水)～12 月 7 日(金)にフランスの Toulouse で開催された Botconf 2018[16]に参加し、セッションで発表しました。

Botconf とは、International botnets fighting alliance/Alliance internationale de lutte contre les botnets (AILB-IBFA)が主催する、2013 年から開催されるセキュリティカンファレンスです。毎年、マルウェア関連のホットなトピックが紹介され、今年は、世界各国から約 400 名[17]のセキュリティエンジニアや研究者が参加しました。

私たちのセッションは「Let's Go with a Go RAT!」というタイトルで、サイバー救急センターレポート 第 3 号[18]で紹介した Go 言語のマルウェア(wellmess)の調査結果の発表でした。比較的珍しい Go 言語のマルウェアの発表ということもあり、発表後にいくつかの質問やフィードバックを受けました。

今回、Botconf に初めて参加しましたが、マルウェア関連に特化した技術レベルが高いセッションが多く、日々最前線で脅威と対面する私たちにとって、非常に有意義なカンファレンスであったと感じています。

余談ですが、今回 Botconf が行われた期間は、フランス全土で燃料価格の上昇や生活費の高騰などへの抗議デモ（黄色いベスト運動）が激化している時期でした。Botconf が開催された Toulouse では、デモの影響で公共交通機関が乱れてはいましたが、幸いなことに Paris で報告されているような大規模なデモに遭遇することはなく、無事に過ごすことができました。

石川 芳浩/長野 晋一

16 https://www.botconf.eu/
17 https://twitter.com/Botconf/status/1071535895612936193
18 https://www.lac.co.jp/lacwatch/report/20180614_001648.html

コラム：セキュリティ百景 #12

インターンシップ フォレンジックコース開催

ラックでは毎年学生に向けたインターンシップを実施しています。2018 年度は、IT 未経験でも参加できるプログラミング実践コースや、JSOC のアナリストによるログ解析実践コースなど、様々な内容で開催しました。サイバー救急センターでも、デジタルフォレンジックコースとして、デジタルフォレンジックの基本的な内容について、座学だけでなく演習を交えて体験いただきました。

今回は、そのインターンシップの様子についてご紹介します。2019 年度も実施する予定ですので、これからインターンシップを考えている学生の皆さんの参考になれば幸いです。

デジタルフォレンジックコースに参加した学生は、専門学生、大学生、大学院生と様々でした。比較的関東圏の学生が多かったのですが、北海道や九州から参加した学生もいました。

デジタルフォレンジックコースは、「デジタルフォレンジックとは？」という基礎的なレベルから始まり、最終的にはデジタルフォレンジック技術を使って、演習課題を独力で解いてもらいます。

正直なところ、6 時間程度の学習時間で、デジタルフォレンジックを全く知らない学生が演習課題を解くのは難しいと考えていました。しかし、ほとんどの学生が、与えられた演習課題の大半を解いていました。デジタルフォレンジックコースは 4 回の開催を予定していましたが、あまりにも早く問題が解かれてしまうため、2 回目以降の開催では課題を追加して対応しました。

インターンシップの講師を担当するにあたり、最も重視したのは、「体験してもらう」という点です。

デジタルフォレンジックという分野を正しく理解するためには、OS やファイルシステムなどの普段意識することのない低レイヤーの複雑な仕組みを理解する必要があるだけでなく、実務での経験も必要となります。限られた時間の中で、すべてを理解してもらうのは困難なため、内容の理解よりも、痕跡を発見するための方法を中心に説明し、攻撃者の残した痕跡を見つけ出すことの楽しさを「体験」してもらえるように工夫しました。

今回のインターンシップを経験した学生の皆さんが、将来ラックに入社し、一緒に仕事ができるようになる日が来ることを楽しみにしています。

扇沢 健也

編集後記

本号のお届けが遅くなり誠に申し訳ありません。はじめにでも書いていますが、APT 攻撃で狙われる組織は執拗に狙われ続けており、攻撃方法も巧妙になってきています。また、金銭目的の攻撃者グループは、手を変え品を変え、サイバー攻撃やサイバー利用犯罪をしてきています。これからも、旬な脅威情報を継続的にお届けできるよう尽力してまいります。（法）

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/6XN8K2D

編集長　内田 法道

編集者・執筆者　遠藤 裕樹、郷 晴奈、田原 祐介、石川 芳浩、長野 晋一、扇沢 健也

株式会社ラック

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

E-MAIL: sales@lac.co.jp

https://www.lac.co.jp/

緊急対応窓口：サイバー救急センター

24時間365日 緊急対応コール

0120-362-119

CYBER EMERGENCY CENTER

ご相談は予約不要、24時間対応。すぐにご連絡ください。