CYBER GRID JOURNAL VOL.18

サイバー・グリッド・ジャーナル

情報リテラシー維新

デジタル社会に必要なチカラを多角的に備えよ

CYBER GRID JOURNAL VOL.18

TABLE OF CONTENTS

巻頭言

情報リテラシー維新

～デジタル社会に必要なチカラを多角的に備えよ～

尾方 佑三子
サイバー・グリッド・ジャパン 副GM
兼 ICT利用環境啓発支援室長

今号のテーマは「情報リテラシー」です。情報リテラシーというと「インターネットや、デジタルデバイスを適切に使う力」と狭義的に捉えられることが多いように思いますが、今日、その定義はとても複雑になっています。なぜなら、デジタル社会で、その利便性を弊害無く享受するには、生活や社会活動全てにおいて対応する能力を捉えなければならないからです。

そこで今号では、デジタル社会で生きるために備えておくべき考え方や行動について、既成概念を取り払って多角的に考えてみることにしました。各研究所の研究テーマである、「脅威インテリジェンス」「国家としてのサイバーセキュリティ」「金融犯罪対策」「セキュリティガバナンス」「情報モラル」「セキュリティ対応力の可視化」といった事柄は、いずれもサイバー空間の広がりや、デジタル社会への歩みの中で必要になっている課題です。言葉として並べると、一見脈絡がないように見えますが、これらを「情報リテラシー」という観点で結んでみると、私たちが生きていくために必要な能力の全体像が浮かび上がってくるのではないかと考えました。それはデジタル・シティズンシップの実像なのかもしれません。

ぜひ、興味のあるテーマから開いて、点と点を結ぶようにページをめくってみてください。どのような形が見えてくるでしょうか。

今号が皆さまにとっていつもと違う角度から「情報リテラシー」を捉える機会となり、デジタル社会におけるより良い生き方のきっかけになれば幸いです。

情報管理八策2025

株式会社ラック
技術顧問
西本 逸郎

ラックでは、約15年前に当たる2011年1月（発表は2010年11月）に
一般からのご意見も頂戴し、情報管理八策なるものを公開しました。

https://www.lac.co.jp/news/2011/01/07_news_01.html

情報管理八策

1. 情報管理とは、情報の「適切な利活用が目的」であり、組織や個人を守り社会に貢献するものである事。
2. 電子化された情報に接する全ての者は、その劇的に変化する特徴や基本的なリスクを理解し、情報取り扱いの作法を身につけるよう努め、組織の長はその徹底を図る事。
3. 情報の機密度や配布先、閲覧可能場所などは最初に決定すべきであり、途中で変更することは極めて難しいという心構えで臨む事。
4. あってはならぬことであっても、技術的欠陥、権限保持者の犯罪や告発、並びに詐欺などにより事故は発生するものである。100%の安全策は存在しないことを理解し、常に事故発生の備えをしておく事。
5. 事故を起こした者や内部告発者への評価など、情報管理の有り様が世情により刻々として変化していくことを踏まえた上で、各組織の実情にあわせた公正妥当な管理策を制定する事。
6. 電子機器の急速な進化により人々の生活や働き方が大きく変化しつづける中、情報が個人と組織の間を区別なく行き来することを前提に管理策を練る事。
7. 全ての組織は、その情報への依存度にあわせ、制度制定、安全措置、教育や訓練の実施、監査、事故対応など、予防と抑止の両面で対策の高度化を推進する事。
8. 情報管理水準の向上に携わる全ての組織は、私たちが身に付ける情報管理の有り様が、来る高度情報社会における、わが国の成長と国際的な地位確立の礎となることと認識し、技術と意識レベルの向上に努める事。

以上

あ る面、現在でも十二分に通用する指針ではないかと改めて思う次第です。

話 は変わり、私はNHKの朝ドラを大体毎回楽しみにしています。2025年4月から9月までは、アンパンマンの作者で有名なやなせたかしさんと奥さまを主人公とした『あんぱん』が放送されていました。手塚治虫さんと思しき方が登場し、その天才性に圧倒されるシーンが出てきたので、何が天才だったのかといろいろ調べてみました。従来の子ども向けの単に「読む」漫画を、あたかも映画を見ているような表現方法を取り入れることで「観る」漫画に変え、アトムのようなヒーローだけではなく、ヒゲオヤジに代表される売れっ子タレントを育てさまざまな作品に役者として「起用」する。単発ものから大河的長編連続ドラマへ、さらにアニメ・キャラクター・エンターテインメントへの大きな影響など、昭和の千利休が如く、従来の漫画を文化として再確立し、さらに産業化まで成し遂げたことは、まさに天才だと思います。考えてみると、天才は大発明をする必要はなく、創意工夫で一つ一つの仕事をかたくなにやり続けることで周りを巻き込み、ステップアップし続けることが重要なのかなと改めて思う次第です。

サ イバーセキュリティは安全保障実現においても重要な要素で、現在向かっているデジタル・AI時代において必須の身に付けるべき事項であると誰しもが思っています。ところが「守るために重要な技術である」や「身に付けなければならない」と、言われた瞬間に義務感と拒否感にあふれ、途端につまらないものになりかねません。そうではなく、ワクワクする楽しいものだということを前面に出せるとよいと思いますし、そうでなければならないと思います。

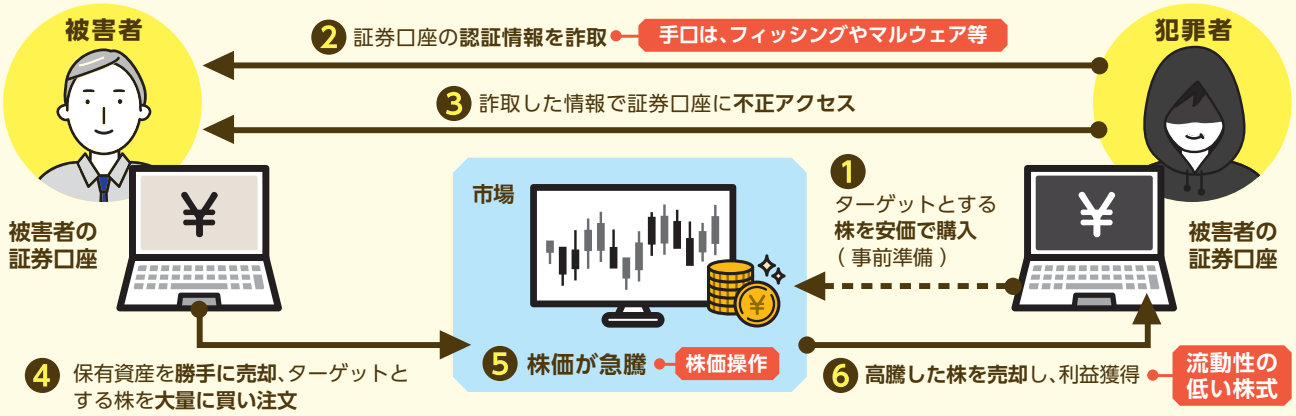
ま た、漫画と茶の湯から考えると、「思い」があり、そこから作法→道具→産業と遷移し「文化」として広がったのではないかと考えられます。サイバーセキュリティを「文化」に昇華させるには一丁目一番地である「思い」から入る必要があります。茶の湯でしたら「一期一会」でしょう、手塚漫画だと根本に流れるのは「いのち」でしょうか。それでは、サイバーセキュリティではどう考えるのがよいでしょうか？　私は横文字だと

「フォロワーシップ」だと思っています。日本語だと「全員参加」になるのでしょうが、何となく強制感が滲んでくるのでAIと一緒に考えてみました。「ともる（共にまもる）」はどうですかね？ 自助・共助・公助をも包含し、フォロワーシップもイメージする言葉だと思います。

言葉遊びはさておき、誰もが納得する思いをもとにした作法を広め、道具として整え、産業として発展させていくことが、重要なことだと改めて思う次第です。2025年2月まで、当社の取締役を務めてくださった村井純先生は著書『インターネット文明』の中で、インターネット（サイバー空間）はもはや酸素に匹敵すると述べられています。私たちの生活や事業活動において、インターネット（サイバー空間）がいかに欠かせない存在となったかを的確に表しています。娯楽の領域から、生活・教育、そしてビジネス・経済へと浸透し、さらに防犯・防災、安全保障、行政に至るまで、社会のあらゆる領域がこの唯一無二のサイバー空間に依存しています。その酸素を適切に維持することを誰もが推進し、その恩恵を享受できる社会を勝ち取る必要があると思います。そのためのサイバーセキュリティ文化だと改めて思う次第です。

さて、JC3（日本サイバー犯罪対策センター）の櫻澤業務執行理事の講演で知りましたが、長年にわたって減少してきた日本の犯罪被害総額は、この2、3年増加に転じており、昨年はなんと前年比約1,500億円増の約4,021億円と、約60%も急増しました。そのうち詐欺が約3,075億円と、被害総額全体の76%を占めています。この詐欺が前年比約1,500億円増ですので、詐欺が倍増した結果、被害金額も急増している結果となっています。さらには、今年に入り、ネット証券で10月時点で約6,900億円の被害が出ているとも報道されており、以前とは異なる様相になっています。

以前は、インターネットバンクでのなりすましのログインにより不正に犯人口座に送金するというような手口（窃盗）が主でした。今年は、ネット証券の口座主になりすましてログインし、まず保有株式を売却してから、犯人側が値を吊り上げるために目を付けていた会社の株式を大量に購入し、巧みに値を吊り上げたのち、あらかじめ購入しておいた株式をちゃっかり高値で売却して、利益を得る手口が増えていると報道されています。これは、犯人がなりすましている被害者が吊り上げられた高値で購入させる、或いはだまされた第三者が高値で購入してしまい、犯人が利益を得るという詐欺的な手口で、被害者が保有していた株式を勝手に販売した収益を、マネーロンダリングして手に入れているともいえます。これは、従来のハッキングだけではなく、人の心のハッキングに加え、証券に関わるさまざまな制度や内部の運用方法などの実態のハッキングまで行われているのではないかと私は危惧しています。



最近のなりすまし手口の仕組み

最近では、IDやパスワードをだまし取るフィッシング詐欺だけではなく、サポート詐欺やClickFIXのような、ちょっとしただましの手口である心理的遠隔操作による被害も増えており、遠隔操作の分野ではコンピューターウイルスを仕込まず、人を遠隔操作する手口がいろいろ開発されています。さらに、サイバーセキュリティ以外の分野でも制度の抜け穴を探すような手口が散見されており、ハッキング対象が従来のシステムから、制度や人にまでに及ぶことを考慮しなければならない時代であると改めて思う次第です。

これは、金銭目的の犯罪の話ですが、従来のサイバーセキュリティ対策が進めば進むほど、安全保障に関係するような領域においても、従来のシステムのハッキングから、だまし、詐欺、そそのかし、恐喝などの人的ハッキングや制度ハッキングへの考慮を怠れないと思います。

そういう時代の、「情報管理八策2025」を、前述の「ともる」という思いの下で再編し、今後の文化形成という未来を考えてみたいですが。恐らく、今後を担う皆さまは、自分たちの未来を「67歳のおじいちゃん」に考えてもらいたいなんて微塵も思わないはずですので、これを読んでいただいた方々で、ぜひ、これからを支えるサイバーセキュリティ文化の礎をつくっていただけましたら幸いです。

そこの、あなた、読みましたね！ 笑

情報リテラシーとしての脅威インテリジェンス

情報リテラシーと聞いて何を思い浮かべるでしょうか。文部科学省の「教育の情報化に関する手引」❶は「情報活用能力の育成」として、「情報活用の実践力」「情報の科学的な理解」「情報社会に参画する態度」が挙げられています。これらはあくまで基礎的な能力でしかありません。

実際に社会的に求められるのは、これらの基礎の上で組織のセキュリティを守るための方策です。「嗚呼、新人研修や社内研修で受講する内容か」と思われるかもしれませんが、現代の組織は社会的な責任としてコンプライアンスを求められています。そして、その内容を一人ひとりにまで分解して適用したものが、社会的に求められる組織人としての情報リテラシーとなっています。

本稿では、日頃から心掛けられる情報リテラシーの一つとして、脅威インテリジェンスについて解説し、実務としてのセキュリティ運用に役立つ活用方法についてご紹介します。皆さまが日頃実践されるセキュリティの一助となれば幸いです。

組織的に身に付けるべき情報リテラシー

一般に情報リテラシーとして思い浮かべられるものは、ほとんどが「個人」が身に付けるべき内容です。その一方で社会的に求められる情報リテラシーというものがあり、これらは「組織」が身に付けるべき内容といえます。

ほとんどの内容は組織が提供する研修などで身に付けることになる組織的な情報リテラシーですが、その中でも組織が行動する指針を定める重要な情報リテラシーとして「脅威インテリジェンス」があります。セキュリティの脆弱性や事件などのニュースといった、一般的に入手できる脅威情報を目的に合わせて分析することで、組織の判断基準に資するためのものです。

脅威情報から脅威インテリジェンスへ

世の中には、さまざまな脅威情報があふれています。OSINT(Open Source Intelligence／公開された情報)として収集するだけでも、例えば最新の脆弱性情報ですとか、金融詐欺のニュース、どこそこの企業が外国の攻撃者から狙われたというニュースなど、さまざまな脅威情報が見つかります。

脅威情報はあくまで生の情報でしかありません。有効に活用するためには、脅威情報を分析・加工して、意思決定に役立つ知見に仕立て直す必要があります。それを脅威インテリジェンスと呼びます。

具体的な例を挙げましょう。あなたが社内の情報システムの管理者だったとして、Windowsサーバーに外部から攻撃される危険な脆弱性が発見されたとします。上司に報告するためにはどのような情報を集めればよいでしょうか。

まずは、脆弱性情報の詳細から見てみましょう。脆弱性がある機能はどこですか？ 影響するバージョンはどれですか？ 機能を利用しているか確認するにはどこを見ますか？ 軽減策・回避策はありますか？ 何らかの前提条件が付されていませんか？ さらに、攻撃が確認されているならばその攻撃は調べた脆弱性を直接狙っていましたか？ その攻撃では、公開された脆弱性のPoCコードを利用していましたか、それとも別の方法でしたか？ これらはまだ脅威情報の段階です。

次に、自社の状況を調べたとします。社内でWindowsサーバーは使っていますか？ SIであれば、構築したお客さま先ではどうですか？ 脆弱性がある機能は利用していますか？ 対象のバージョンですか？ 前提条件を満たすことはありそう

❶「教育の情報化に関する手引」について:文部科学省　https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_00117.html

若居 和直

プロダクト統括部 プロダクト開発部
システムセキュリティプロダクト開発G
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所 脅威分析G

ですか？　攻撃されるとしたら自社だけですか？ 他の影響を受けそうなシステムが狙われる可能性は？ 攻撃の国内影響範囲は？ これらは脅威情報そのものではありませんが、日々整備しておくべき脅威インテリジェンスのための情報源となります。

では、いよいよこれらを脅威インテリジェンスにしましょう。上記の情報を分析すれば、実際に手を動かして対応するべき脆弱性かどうかが分かります。対応方法もまとめられますし、対応が難しい場合の軽減策などもまとめられます。まとめた内容は、無事に上位者が対応を考えて判断できる内容になっているでしょうか。

このように、脅威に対して常日頃から脅威情報を収集し続け、必要に応じて分析した情報を提供するのが、脅威インテリジェンスです。

ラックでは、脅威情報の収集のためにさまざまな情報源を活用しています。その中にはOSINTの情報源もありますし、組織と人同士の信頼関係により入手できる情報などもあります。そして、ラックが独自に持つ情報源もあります。

一つは、ラックが持つ日本最大級のセキュリティ監視センター「JSOC」が提供するセキュリティ監視サービス（MSS）やエンドポイント監視サービス（MDR）からの脅威情報です。監視機器からのアラートを鵜呑みにするのではなく、セキュリティアナリストが専門的に分析した脅威情報となります。

その他、日本を標的としたマルウェアによるインシデント情報を扱うACTR（Advanced Cyber Threat Research Center）サービスからの脅威情報や、研究開発部門「サイバー・グリッド・ジャパン」の研究過程で得られた攻撃情報の他、ラックのセキュリティ専門家が日本国内で確認した脅威情報などがあります。

これらの脅威情報をラック社内では脅威インテリジェンスとして活用しています。また、脅威情報の一部をJSOCで利用する独自検知情報「JSIG®」や、脅威情報の提供サービス「JLIST®」として、お客さまに提供しています❷❸。

その他にも、ラックの社員が一般財団法人日本サイバー犯罪対策センター（JC3）の活動を通して、日本におけるサポート詐欺サイトの情報を共有することにより、最終的にインド共和国・中央捜査局（CBI）がサポート詐欺に関係する被疑者を検挙することにまでつながりました。これも、立派な脅威インテリジェンスの活用です❹。

日頃からの脅威インテリジェンス活用の勧め

本格的に取り組むのであれば、まず分析者への情報セキュリティのモラルの話から入る必要があるほど、脅威インテリジェンスというものはセキュリティ戦略における重要な情報源となります。

ですが、今回の例に挙げた通り、日頃から情報システム部のような方々が行われていることも、見方を変えれば簡易的な脅威インテリジェンスの活用といえます。

組織として、脅威情報を含むセキュリティ情報を漫然と集めるのではなく、意図を持って集めるところから始めましょう。そうすれば、公的な機関などから脅威に関するアナウンスが出たり、ニュースとして報道されたりした際に、素早く上司に判断基準となる情報を提供できるようになります。そしてその積み重ねこそが、組織として危険な情報や行動を見抜いたり、事前に対応が行えたりする力になります。それこそが、組織のセキュリティのための情報リテラシーであり、組織と個人を守る糧となるでしょう。

❷ 次世代ファイアウォールとJSIGのベストマッチ | LAC WATCH　https://www.lac.co.jp/lacwatch/service/20171201_001432.html
❸ ラック、サイバー攻撃からの防御能力を飛躍的に向上させる脅威情報（スレットインテリジェンス）提供サービスを開始（2018年7月12日）| 株式会社ラック
https://www.lac.co.jp/news/2018/07/12_press_01.html
❹ ラック、官民のサイバー対策組織と連携してサポート詐欺の被疑者検挙に貢献（2025年6月6日）| 株式会社ラック　https://www.lac.co.jp/news/2025/06/06_press_01.html

企業と市民に求められるカウンター・インテリジェンスの視点

サイバー・グリッド・ジャパン
ナショナルセキュリティ研究所
シニア・フェロー
初代サイバー防衛隊長
佐藤 雅俊

1 はじめに：サイバー空間における情報リテラシーの再定義

現代の安全保障環境において、情報は単なる知識ではなく、時に「武器」として機能します。SNSやAIの普及により、情報は瞬時に拡散し、国家や企業の評判、経済活動、安全保障政策にまで影響を及ぼす時代となりました。情報の真偽や発信源の信頼性が問われる中で、国家間の競争は物理空間からサイバー空間、さらには「認知領域」へと拡大しています。

とりわけ、フェイクニュースや認知操作を通じた非軍事的手段による影響力の行使が常態化しつつある昨今では、サイバー攻撃だけでなく、情報を用いた心理戦が国家・社会の安定を揺るがす要因となっています。このような状況下で国家を守るためには、従来の受動的な情報保全体制だけでは不十分です。

本稿では、国家安全保障戦略において注目される「能動的サイバー防御」と「カウンター・インテリジェンス（CI：防諜）」を統合的に捉え、それらを有機的に連動させる視座を提示します。併せて、企業が取り組むべき防諜体制の強化と、それを支える「情報リテラシー」の役割についても論じたいと考えます。

2 カウンター・インテリジェンスの視点

カウンター・インテリジェンス（CI）とは、敵対的勢力による諜報活動、情報窃取、破壊工作、心理操作といった行為に対抗し、自国や組織の重要情報、人材、インフラを保護する一連の取り組みを指します。その手法は、以下の四つに大別されます。

1. **諜報（Espionage）：敵対勢力による情報収集活動**
2. **防諜（Counterespionage）：敵スパイへの対抗・無力化**
3. **宣伝（Propaganda）：世論誘導やイメージ操作**
4. **謀略（Subversion）：内部撹乱や工作活動**

これらはしばしば複合的に組み合わされ、例えばサイバー攻撃と偽情報の拡散が同時に行われることも多く見受けられます。

冷戦期以降、欧米諸国ではCIはインテリジェンス・サイクルの一部として制度的に整備されてきました。アメリカではFBIが国内の防諜活動を主導し、イスラエルもテロやスパイ活動に対する高度なCI能力を保持しています。これらの国々では、CIは国家安全保障の中核を成しており、日本のように制度的な整備が未成熟な状況は、むしろ例外的であるといえるでしょう。

3 情報戦と認知領域の台頭

近年、情報戦の中でも特に注目されているのが「認知戦（Cognitive Warfare）」です。これは、敵の認識、判断、意思決定に影響を与えることを目的とし、SNS、AI、ボットなどを活用して情報空間を操作する戦い方です。

ロシアによるウクライナ侵攻では、偽情報の拡散やサイバー攻撃といったハイブリッド型の情報戦が確認され、軍事行動と情報操作の一体的運用が行われました。日本においても、こうした認知戦の影響は現実の脅威として顕在化しつつあります。SNS上での世論操作や外国勢力による分断工作は、もはや対岸の火事ではありません。

参考文献　佐藤雅俊・上田篤盛『情報戦、心理戦、そして認知戦』（並木書房, 2023）、上田篤盛『兵法三十六計で読み解く中国の軍事戦略』（育鵬社, 2025）、防衛研究所「NIDS J-CASTニュース「東芝元社員がHDD技術を韓国企業に漏洩」（2007）、NHKニュース「ロシア人研究者が東北大学で日本の研究者に接触」（2019）、「公電通信

4 日本における制度的課題と企業が留意すべき事項

2025年5月に施行された「重要経済安保情報保護活用法」に基づき、セキュリティ・クリアランス制度が創設されました。さらに6月には、能動的サイバー防御を可能とする法的枠組みが整備され、両制度が今後の情報保全の車の両輪として機能することになります。ただし、両輪をしっかりと動かすためには、企業側の体制整備が不可欠です。

1. 組織体制の整備

国が指定する重要な経済安全保障に関わる情報を取り扱うためには、適合事業者として以下の体制整備が求められます。

- **情報区分と取扱規程**
- **物理・環境セキュリティ**
- **電子データのアクセス制御とログ管理**
- **職員・委託先の身元審査及びクリアランス取得の運用**

これらは企業の採用・配置・昇任政策に直接影響するため、個人情報保護や雇用差別の回避に配慮した透明な手続き設計が不可欠です。

2. インサイダー脅威への対応

内部不正による情報漏洩は、現職者・退職者を問わず重大なリスクとなります。アクセス権限の最小化、ログ監視、職場環境の改善の他、退職時のチェック体制の強化が求められます。

例えば、ある半導体関連企業の社員が提携先のフラッシュ・メモリー関連の設計図を不正に持ち出し、韓国企業に提供した事例が報道されました。こうした事案では、組織内部での情報統制や人材管理の不備が主因とされますが、組織への忠誠心や職場環境の問題も背景として存在すると推察されます。経営層による組織文化の健全化も重要な課題であるといえるでしょう。

3. 外国勢力の情報収集活動への対応

軍事・安全保障関連の国際会議や学術交流の場は、外国情報機関にとって研究者や技術者と接触する有力な「ヒューミント（HUMINT：人的情報収集）」の機会となります。実際に、名刺交換をきっかけに、メールでの連絡、会食への招待、さらには研究協力の提案へと段階的に関係を深めようとする事例が報告されています。

また、SNSや専門的なオンラインコミュニティを介した継続的な情報収集、情報拡散による影響工作も増加しています。匿名アカウントを用いて信頼関係を装い、友好的な態度で接触し、さまざまな情報を引き出す手法は、最終的に本格的な諜報活動へと発展する恐れがあります。一度でも情報を提供してしまえば、弱みを握られ、そこから抜け出すことは極めて困難となります。

特に若手社員は、SNS等を通じて見知らぬ人物と情報をやり取りすることへの警戒心が薄く、外国勢力からの標的となりやすい傾向があります。こうした勢力は、現在得られる情報の価値にとどまらず、将来的な役職や影響力を見越して長期的に接触してくることを常に念頭に置く必要があります。

4. ハニートラップへの警戒

2004年には、在上海日本国総領事館に勤務していた職員が、中国の情報機関によるいわゆる「ハニートラップ」の標的とされ、秘密保持義務を盾にした脅迫を受けた末に自殺する事件が発生しました。

この事案は、外交官だけでなく、企業人や研究者にとっても現実の脅威であり、外国人と接する機会のある職員への事前教育が不可欠です。また、組織内においても、社員の異変の兆候を早期に把握するための内部相談体制の強化や、通報窓口の設置を現実的な防御策として検討すべきです。

5 おわりに：情報リテラシーが守るもの

私たちは今、情報・認知・諜報・サイバーといった多層的な脅威が複合的に交錯する時代に生きています。防衛の最前線は、もはや国境線や基地といった国家の外周ではなく、企業の情報システムや市民一人ひとりの意識の中に存在しています。

能動的サイバー防御、カウンター・インテリジェンス、認知戦。これらが交差する領域において、日本が主体的に情報空間を制御し、自らを守るためには、組織体制の整備、物理的セキュリティの確保、人的セキュリティの強化が不可欠です。

防諜は、受動的な秘密保全にとどまらず、先手を打つ能動的な行為も含む活動です。企業がこの視点を持ち、カウンター・インテリジェンスを競争優位の源泉と捉えたとき、真の意味で情報戦における強さが生まれると考えます。

コメンタリー」各号、内閣官房 経済安全保障法制準備室「セキュリティ・クリアランス制度に関する運用指針（2025）」、経済産業省『経済安全保障と内部不正に関する事例集』（2023）、担当の上海総領事館員が自殺「中国が外交機密強要」と遺書」（読売新聞2005年12月27日）、IPA『情報セキュリティ白書2024』、JPCERT/CC『内部不正に関する事例と対策ガイド』

金融犯罪から身を

近年、金融犯罪やサイバー犯罪の被害が急増し深刻な社会問題となっています。特に、急速なデジタル技術の発展に伴い、詐欺の行われる舞台がオンラインサービス上に拡大しており、手口も巧妙化しています。

今年に入って急速に注目を集めているのは、証券口座を乗っ取って金銭を詐取する詐欺です。犯罪者が不正に入手したIDとパスワードを用いて、証券会社のオンライントレードにログインし、被害者本人になりすまして、証券口座に保管されている株式を勝手に売買して利益を得る手口です。証券口座において不正売買された詐欺被害額は6,900億円に達しています（本稿執筆の2025年10月時点）。

証券口座の不正アクセスに利用するIDとパスワードの入手に使われたのが「フィッシング詐欺」とみられています。フィッシング詐欺とは、実在のサービスや企業をかたり、偽のメールやSMS（携帯電話のショートメッセージ）で偽サイトに誘導し、IDやパスワードなどの情報を入力させて盗んだり、マルウェアに感染させて情報を詐取したりする手口で、被害の拡大が大きな社会問題となっています。本稿では、フィッシング詐欺の具体的な手口と対策についてご説明します。

以下では、フィッシング詐欺の代表例として、銀行をかたった手口をご紹介します。

件名：【A銀行】お取引目的等のご確認のお願い

平素より、A銀行をご利用いただきありがとうございます。
当社では、犯罪収益移転防止法に基づき、お取引を行う目的等を確認させていただいております。
（途中省略）
下記のボタンをクリックするとお客様情報・取引目的の確認の画面が表示されます。
画面の案内に沿ってお客様情報等の確認とご変更の有無、取引目的をご回答ください。
（途中省略）
株式会社A銀行
※ 一定期間内にご確認いただけない場合、口座取引を一部制限させていただきます。

フィッシング詐欺代表例

左記のようなメールが届いた場合、詐欺だと気付ける人は少ないと思います。というのも、手口が巧妙な上に、巧みに被害者心理をついているためです。具体的に解説すると以下の通りですが、この手口のポイントは３点あります。

Point 1

実際に行われていることなので詐欺だと気付けない

- 金融機関はマネロン／テロ資金供与の対策として、利用者に取引目的を確認している
- 一般的に封書やハガキで案内が届くものの、利用者は金融機関のメールだと思い込む

Point 2

本物と同じ文章なので違和感がない

- 金融機関の案内文をネットなどから入手して作成（AIを悪用して巧妙化するケースも）
- 件名や本文は本物をそのまま使用、署名欄も実在する金融機関名や登録番号を流用

Point 3

「面倒なことになる前に解決したい」という被害者心理に付け込む

- 通常、生活で利用している銀行口座は取引を制限されると困る
- すぐにでも解決したいと焦る被害者は、目の前にある解決方法を鵜呑みにして行動してしまう

【宝くじ当選通知】　当選おめでとうございます！

当選金を受け取るための手続きをお願いします。
以下のURLにアクセスして当選金を振り込む銀行口座などを登録してください。
URL：xxxxx;xxxxxxxxxxxxxxxxxxxx

なお、当選金を受け取るためには送金手数料として2000円のお支払いが必要です。これは一時的なものですので、当選金と合わせて返金します。
※送金手数料の支払い方法は、2000円の電子ギフト券を購入して、サイトに
ギフト券の番号を入力してください。電子ギフト券はコンビニエンスストアで購入可能です。

フィッシング詐欺代表例

フィッシング詐欺の例をもう一つ挙げます。このメールの特徴は「おいしい話で引き付ける」手口です。具体的に解説すると以下の通りですが、この手口のポイントは３点あります。

Point 1

当選はつい気になってしまう

- 被害者は、宝くじに応募した覚えがないのに、メールを開封
- 犯罪者は当選をエサに、被害者の「お金がもらえるかも」という期待を利用

Point 2

大金を提示されて、期待する気持ちが膨らんでしまう

- 被害者は当選金額の大きさに驚き、欲求で頭がいっぱいに
- 「二度とないこのチャンスを逃したくない」という気持ちが勝ってしまって、疑わない

Point 3

「当選金をもらえるなら手数料など大したことはない」と思ってしまう

- 被害者は、銀行の送金手数料2000円は高いが、当選金受け取り手数料なら安いと判断
- これは「アンカリング」とよばれる認知バイアスだが、犯罪者はアンカリングを悪用

守るために

サイバー・グリッド・ジャパン
金融犯罪対策センター
エバンジェリスト
小森 美武

フィッシング詐欺で気を付けるべきポイントと対策例は以下の通りです。

1 受け取ったメッセージはなりすましの可能性を疑う

メッセージを確認する際は「なりすましかもしれない」と考えて、すぐに信用しないようにする姿勢が大切です。メールだけでなく、SMSやチラシ、封筒などの郵便物も同様です。認証情報（ID・パスワードなど）や個人情報を要求された場合はフィッシング詐欺の可能性が高いです。

2 URLやボタンを安易にクリックせず、オフィシャル情報を確認する

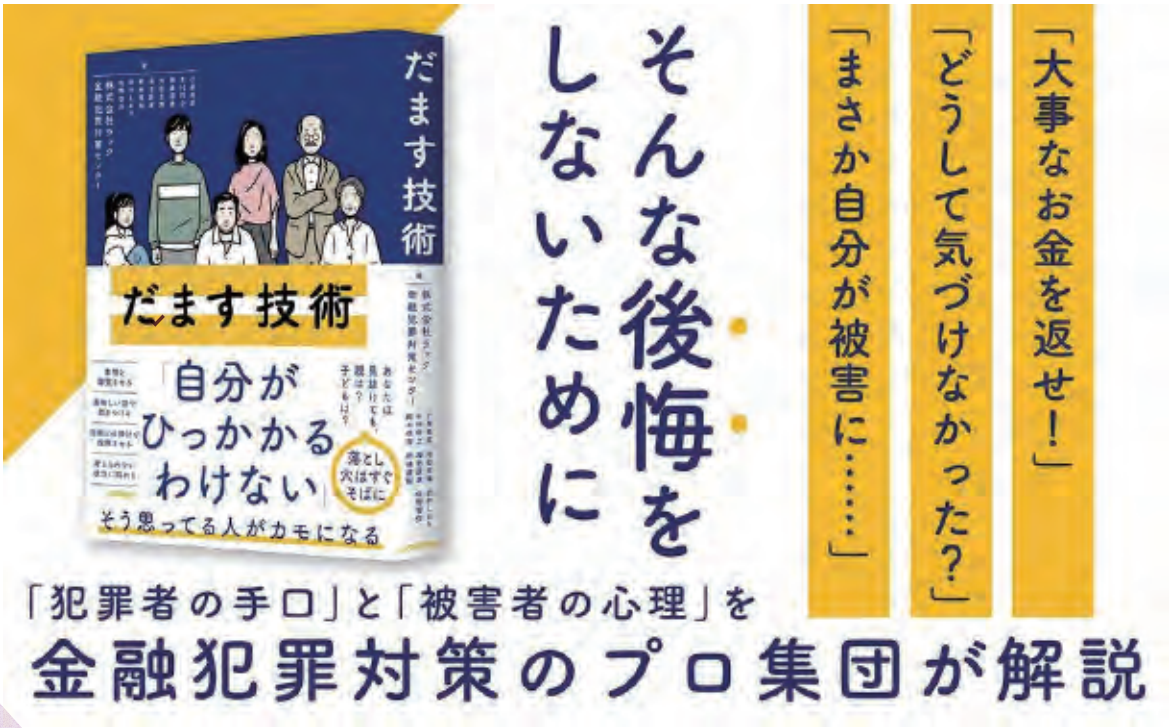
メールに記載されているURLやボタンをクリックしたり、電話番号に電話したりするのは避けてください。詐欺の相手に連絡することになるためです。メール送信元とされている金融機関など送り主のメールアドレスや電話番号を調べて、連絡するようにしましょう。

3 おいしい話に飛び付かない

宝くじ当選、手軽さや高い報酬を強調したもうけ話、「期間限定」や「初回限定」をうたって急いで注文させるセール情報は、まず疑って掛かる姿勢が大切です。慌てて注文・支払いすることは避けて、一晩置いてから翌日改めて判断するなど、少し時間を空けてから判断することを心掛けましょう。

フィッシング詐欺など詐欺被害を避けるためには、家族や友人・同僚などに相談することも大切です。相談する相手を決めておくと、何かあったときに速やかに相談できます。些細なことでも気軽に相談できる関係を築いておくと安心です。常日頃から詐欺への警戒心を持ち、詐欺に遭いそうになった場合の対策を準備しておくことで、詐欺の被害から身を守りましょう。

金融犯罪対策センターでは、詐欺でお金をだまし取られる被害者を世の中から1人でも減らしたいという思いで、私たちの経験と知識を詰め込んだ『だます技術』という本を出版しました。この本では、さまざまな詐欺の被害例をもとに、犯罪者の手口と被害者がだまされる心理の仕組みを主に解説しています。例えば、犯罪者が被害者を信用させる話しかけ方や詐欺の仕掛け、それによる被害者心理に及ぼす影響などを学ぶことができます。また、詐欺に対する知識が付き、身を守れるようになります。知識が付くと、詐欺に遭っても手口に気付けたり、冷静に判断できたりします。さらに理解が深まると、新しい手口に対しても自分で考えて対処できるようになります。情報リテラシーを高め、詐欺から身を守る方法として参考にしていただければ幸いです。



著者：株式会社ラック　金融犯罪対策センター

本書の詳細はこちらから

デジタル社会に対応した“強固な組織づくり”

プラス・セキュリティで サイバーリスク軽減

サイバー・グリッド・ジャパン 団体運営推進室
シニア・コンサルタント　持田 啓司

01 はじめに デジタル社会と リテラシーの関係

環境変化が激しく、予測困難な時代となった昨今、企業には健全な経営を維持し、不正や不祥事を防ぐための体制構築が求められています。

特にこれからのデジタル社会においては、これまでのIT化と比較して、事業部門等でもセキュリティ対策の責任を負うケースが増えてきます。組織運営に関わる多様な人材が「サイバーセキュリティ」で備えるべき、リテラシーも含めたスキルを習得し、インシデントの未然防止・被害抑制のために活躍することが想定されます。

筆者が所属している団体運営推進室で事務局を受け持っているセキュリティ業界団体でも、行政官庁等との連携を行いながらセキュリティ政策の重要課題である人材育成の一翼を担っており、セキュリティ専門人材だけでなく、セキュリティの非専門部門の人材に関しても、セキュリティリテラシー向上施策を展開しています。

ここで、人材育成が喫緊の課題となっている昨今のデジタル社会とリテラシーの関係を見てみると、デジタル庁が掲げている取り組みの方向性と重点的な取り組みの中で、安全・安心なデジタル社会の形成に向けた取り組みとして、利用者全員がデジタルを正しく理解し活用する力、つまりはデジタルリテラシーの向上が必要とされています。

02 サイバーリスクの 現状と組織への影響

サイバーリスクの現状は、非常に多様化し進化しています。長らく被害が続いているランサムウエア、フィッシング、内部不正などの脅威は減るどころか拡大の一途をたどっています。また、AIやIoTの普及による新たなリスクが出てきていますし、引き続きサプライチェーンリスクやクラウド環境の脆弱性も大きな脅威です。

これらはIPA（独立行政法人 情報処理推進機構）が毎年発表している『情報セキュリティ10大脅威 2025』でも指摘されており、少しずつ手口を変えながら、対策の弱い組織や意識の低い個人を最初の攻撃先として入り込み、被害を拡大しているのが実情です。

03 プラス・セキュリティの視点からの組織づくり

ところで、セキュリティ対策の議論をする中で「プラス・セキュリティ」という言葉を聞くことも多くなってきたと思います。この言葉の持つ考え方とは何かを改めて考えてみたいと思います。

セキュリティ対策を進めるには、具体的な対策項目の検討だけでなく、サイバーセキュリティの専門知識を持った人材の育成・確保が議論の中心になってきます。

しかし、内外からのサイバーセキュリティリスクに対抗し、組織のガバナンス強化を進める

には、セキュリティ専門人材を育成・確保するだけでなく、実際に事業推進をするための重要な情報があるセキュリティの非専門部門の人材もプラス・セキュリティを意識しながら業務を行うことで、小さなほころびをつくらない強固な組織づくりを進めることが必要となってきます。

つまりは、プラス・セキュリティという人材が組織のどこかに存在しているわけではなく、事業部や人事・総務などのコーポレート部門といったセキュリティを専門としない部署も、自らの担当業務遂行において必要となるセキュリティスキルの習得に向けて取り組むことが「プラス・セキュリティ」であり、組織全体のセキュリティ対策に対して積極関与することが重要なのです。

04 プラス・セキュリティを意識した組織づくりの二つの視点

1 フォロワーシップの重要性とプラス・セキュリティ

そもそも組織においては、事業推進のための事業部の人材比率が大きく、セキュリティを担当する部署の人材だけでは、組織全体を守ることは難しくなってきています。

なおかつ、セキュリティ専門人材はアウトソースを検討することができますが、事業部に関してはインソースで対応せざるを得ないのが実情です。

このような環境下では、各部署の業務遂行において、どのようなサイバーセキュリティリスクがあるのかを理解し、それを守るためには自身として何を行うべきであるのかを考え対応する、全員参加体制を構築することが必要であり、そのためのフォロワーシップが重要となってきます。

フォロワーシップとは、組織の目標達成のためにリーダーを支援し、主体的に行動する能力や態度のことをいいます。事業部やコーポレート部門の一員としてもプラス・セキュリティの意識を持って、組織全体のセキュリティ向上のためにセキュリティ専門部署・人材を支援し、自ら行動することが重要です。

2 サイバーレジリエンスにおけるプラス・セキュリティ

最近「サイバーレジリエンス」という言葉を聞くことも多くなりました。サイバー攻撃やシステム障害などの脅威が発生した際に、事業の継続性を維持し、影響を最小限に抑えるための組織の対応力と回復力を指します。

そもそもビジネスにおいては、何らかのトラブルや災害等によって事業の推進が遅延したり止まったりすることが想定され、それら障害時に迅速に回復する能力を高めることが重要です。

サイバーセキュリティについては、トラブルが火災に例えられることが多いため、消防署の活動で例示してみると、大きくは以下の二つの対策に分けられます。

まず1点目は「防火活動」であり、火事を起こさせないための工夫・活動です。サイバーセキュリティにおいては「サイバーハイジーン」といい、そもそもマルウエアに感染したり、不正アクセスされたりしない衛生状態の良いIT環境をつくっておくというものです。

これに対して2点目は「消火活動」であり、発生した火事の消化・延焼を防ぐ活動となります。これがサイバーセキュリティにおいての「サイバーレジリエンス」です。

ここで、プラス・セキュリティの重要性が出てきます。

そもそも損失を抑えつつ、短期間でビジネスを回復させるためには、日頃からの準備が重要となってきます。事業に必要な情報は何なのか、その情報が無くなるとどの程度の事業への影響があるのか、また、日常のバックアップ作業やアクセス制御の権限範囲などは、それぞれの部署の人間でなければ判断できないでしょう。

さらに、回復のための対応はセキュリティ専門人材が行うにしても、現場を知った人間が、復旧するシステムの優先順位や情報の重要度などを判断しながら対応しなければ、損失を抑えつつ、短期間で回復させることは無理でしょう。

セキュリティ非専門部署の従業員が、プラス・セキュリティの意識を持って、それぞれの業務に関係するサイバーリスクを知り、対抗力を高め、有事の際に早期復旧を支える必要があるのです。

05 プラス・セキュリティでデジタル社会に対応した強固な組織をつくる

今回紹介したフォロワーシップと、サイバーレジリエンスの考え方については、セキュリティ専門部署・人材の強化だけではサイバーセキュリティの攻撃を防御し、攻撃の被害からの回復が難しいことを示しています。

プラス・セキュリティはセキュリティリテラシーを備えることと同義とも言え、組織内の全ての従業員が、プラス・セキュリティの意識を持ち行動するという文化と意識の醸成が重要となっています。

それには、経営陣をはじめとして全ての従業員がセキュリティを「業務の負担」ではなく「価値創造の一部」として捉えることが必要でしょう。

組織全体としてセキュリティ強化を進めていくという経営層のコミットメントと、各部署におけるセキュリティリーダーの育成、そのセキュリティリーダーを通じた現場への浸透により、「プラス・セキュリティ」がもたらす組織価値、すなわち全員参加によるフォロワーシップにより、サイバーセキュリティに対して強固な組織づくりが叶うということを組織全体として共有し行動することが必要でしょう。

情報リテラシーを学ぶカードゲーム

リテらっこの目的とその効果

サイバー・グリッド・ジャパン ICT利用環境啓発支援室 啓発企画グループマネージャー　高橋 怜子

当室では、2024年12月17日に情報リテラシーカードゲーム「リテらっこ」をリリースしました。リリース以降、小学生から大人まで幅広い年代の方にリテらっこを体験していただいています。リテらっこ体験は情報リテラシーについて人と会話をすることで、インターネットとうまく付き合っていくきっかけになります。さらに教職員や啓発講座講師の方々からは、リテらっこ特有の「考えを共有するワークショップ」が高い評価を頂いています。本稿では、リテらっこの目的とその効果を考察します。

リテらっこの概要と大切なルール

リテらっこは、考えることを楽しむゲームです。「参加者が考えて話す（共有する）」ことで、学習効果を高めることができます。リテらっこの詳しい遊び方は、「情報リテラシーを遊びながら学ぶカードゲーム『リテらっこ』を作りました」のwebページをご覧ください①。

リテらっこは、当室で作成した『情報リテラシー啓発のための羅針盤（コンパス）』②（以下、「羅針盤」とします）をもとに制作しています。2019年に初版をリリースした羅針盤では、インターネットを利用する上で遭遇し得るトラブルを「情報モラル」「情報セキュリティ」「消費者トラブル」に分けています。リテらっこではこの三つのトラブルをベースにして、具体的なトラブルや困りごと（インシデント）が記載された「インシデントカード」を作成しています。

リテらっこでは、カードゲームを楽しんで学ぶためのとても大切なルールがあります。それは、「考えることを楽しもう！」と「他の人の意見を否定・批判しない」です。このルールを守ってゲームに参加することにより、最初は自分の考えを伝えることがなかなか難しい参加者も、だんだんと自信を持って、時には面白く意見を述べる姿が見られます。安心して自分の考えを他の参加者に伝えるための、とても大切なルールです。

また、ゲームマスター（進行役・正しい知識の解説役）がいますので、説明に困ったり、悩んだりしたときには、ゲームマスターが助けてくれますのでご安心を。

インターネットで遭遇し得るトラブルについて、「自分だったらこのような行動をする」と漠然と考えていたことについて、自分の考えを互いに説明することで「他の人も自分と同じように考えているんだ！」と答え合わせをすることができます。また他者と「こんな対処法があることを初めて知った」「もう少し良い方法があるかも」という「考えの共有」をすることで、情報リテラシーを効果的に学ぶことができます。一番の効果は、実際にインターネットのトラブルに巻き込まれそうになったときに、制限のある状況（リテらっこでは5枚の手札だけで疑似的に体験します）でどのような行動をすべきかを準備できることです。

なぜリテらっこを制作したのか？

デジタル社会を迎えた現代の日本では、小学生から高齢者までがスマートフォンを持ち歩き、令和6年のインターネット利用率は85.6％と高く③なっています。情報リテラシーは老若男女問わず必要なスキルになっている一方で、インターネット利用に起因するさまざまなトラブルが発生しています。生活を便利に、有意義にするためのツールで、困ったことになるのは誰でも避けたいですよね？

情報リテラシーを身に付けると、具体的にどんな効果があるのでしょうか？

例えば、以下のような効果があります。

- **自分の情報を守るスキルを身に付けることができる**
- **家族や友達にも安全なネットの使い方を教えることができる**
- **SNSやメッセージアプリで安全にコミュニケーションを取ることができる**
- **自分の投稿をコントロールできる**
  （写真や名前の公開範囲を考える、トラブルを未然に防ぐことができるなど）
- **フェイクニュースやデマに惑わされない**
- **サイバー犯罪に巻き込まれる前に対処することで、被害者だけでなく加害者にならない**
- **悪質なデマやいじめから自分を守ることができる**
- **ゲームやアプリの課金トラブルを防げる**
  （本当に必要か見極めて、後悔しない使い方ができる）

① リテらっこの詳しい遊び方
情報リテラシーを遊びながら学ぶカードゲーム『リテらっこ』を作りました

② 最新のインターネットトラブルを学ぶ
「情報リテラシー啓発のための羅針盤（コンパス）」の使い方

③ 総務省　令和6年通信利用動向調査（令和07.05.30公表）　https://www.soumu.go.jp/johotsusintokei/statistics/data/250530_1.pdf

トラブル無く安心・安全にインターネットを使用するために、インターネットの利用者自身が情報リテラシーを学び、身に付ける必要があります。しかしながら、情報リテラシーを学ぶ機会がない、難しそうという考えがよぎった方は少なくないかと思います。

当室では、年間200件超の情報リテラシー講座を日本全国の学校などで実施していますが、座学で一方的に講師が話すという形式が多いため、より主体的（文部科学省が定める現在の学習指導要領では、「主体的・対話的で深い学び」がうたわれています）に、かつ効果的に情報リテラシーを学んでもらうにはどのような手法が良いかと考えていました。そこで制作したのが「リテらっこ」です。

リテらっこを活用した情報リテラシー講座から見えてきたこと

制作開始以降、リリース前のトライアルも含めると、20件ほどリテらっこを活用した情報リテラシー講座を実施しました。対象は主に、児童・生徒、地域で情報リテラシー啓発を担う立場の方ですが、意外なところでは企業の情報システム担当の方などにも体験していただいています。

当初、ゲーム形式としてプレイヤー5名程度に対してゲームマスター1名を想定していましたが、実践に当たっては、学校ではクラス単位での実施要望が多かったことから、ゲームマスター１名で35名程度のクラス全体を仕切れるよう、1グループ5名程度で複数グループをつくり、グループ対抗で実施する形式を試行してみました。議論の深さや、ゲームとしてのまとまりなど、どのようになるかの試行でしたが、グループ内で個々の発言が促され、教員や見学者などを巻き込んで行うことでさらに活発に意見が飛び交い、大人数でのリテらっこも効果的であることが分かりました。

また、リテらっこはゲームを楽しむだけでも一定の効果が見られましたが、特に子どもたちにおいては、正しい情報のインプットが必要であることを認識したことから、事前に座学を組み合わせるハイブリッドな講座を提案するようになりました。座学による知識のインプットとゲームを通してのアウトプットの両方によって学びの定着が促され、より効果的な学びにつながります。ゲーミフィケーションはこれまでの講座の完全な代替となるものではなく、あくまで効果を高めるツールということです。

さらに、副次的な効果も見えてきました。リテらっこは必ず前向きに会話をするルールがあるため、闊達な会話が促されることで、組織におけるチームビルディングにも活用できるのではないかということです。プレイヤー全員がインシデントカードをお題としてどのように対処するかを考えることで、組織のセキュリティリテラシーを養うきっかけになり、企業や組織における研修ツールとしての可能性を秘めています。

これからのリテらっこ

リテらっこは、トライアルから数多くのフィードバックを重ね、座学による体系的インプットと、ゲーム形式による実践的アウトプットを組み合わせた、当室でこれまでにない情報リテラシー講座を実践できるツールになりました。

当室で推進している情報リテラシー啓発では、各地域で異なるICT利用実態やインターネットトラブルの特性を分析し、その地域に最適化された講座などを展開することで、より深い理解と行動変容を促すアプローチをしています。

さらに、地域に根差した啓発活動を自律的に展開するための仕組みづくりを重要課題と位置付け、教育委員会、学校、警察、消費生活センター、NPOなど多様なステークホルダーと連携しています。各地の主体的な取り組みを支援することこそが、我々「ICT利用環境啓発支援室」の使命であると考えています。地域に根差したファシリテーター及びリテらっこゲームマスターの担い手を全国に養成し、地域レベルでの啓発体制を構築できるよう取り組んでいきます。

そしてリテらっこの大きな魅力である「楽しさ」は、情報リテラシー習得への入り口となります。私たちはこの強みを生かし、学びの機会を全国へと広げながら、ICTの利活用を安心・安全に支える基盤づくりを進めてまいります。

特別寄稿

サイバー攻撃に対応するための リテラシー向上に向けた取り組み

株式会社KDDI総合研究所
セキュリティ部門 サイバーセキュリティグループ
コアリサーチャー
澤谷 雪子

インターネットを利用する中で日常的に遭遇する攻撃の怖さとその対策に求められる能力

私たちがインターネットや情報機器などの情報通信技術（以下、ICT）を利用する場面では、詐欺や不正アクセスなどの被害へと誘導する、さまざまな攻撃が常に身近に存在します。これらは、ユーザーが日常的にICTを利用する中で攻撃を認識でき、攻撃に関する知識やその対策を知っていることによって被害を防げるものと、攻撃をすぐには認識できなくとも、事前の対策となる行動を取ることによって、被害に遭う可能性を下げることができるものがあります。ここでは、前者の例として「サポート詐欺」を、後者の例として「パスワードリスト型攻撃」を、それぞれご紹介します。

サポート詐欺❶は、以下の手口により金銭被害を被ってしまう攻撃です。

- パソコンでインターネット閲覧中に、ウイルス感染を警告する偽の画面が表示される。
- 偽の警告画面には偽のサポート窓口の電話番号が記載されており、電話をかけるよう誘導される。
- 電話の相手が詐欺師であり、端末を遠隔で操作され、サポート料金を請求される。サポート料金は、コンビニで購入できるプリペイドカードで支払うよう指示され、プリペイドカードの情報を渡すことで金銭被害が発生する。さらに、虚偽の説明で複数回のカード購入を強要されることもある。

サポート詐欺に遭ってしまうサイトは、web検索結果や広告に紛れていることが多いため、日常的にインターネットを利用する中で攻撃に遭遇してしまう可能性があります。そのため、被害に遭わないよう、こうした攻撃があることや、その対処法を事前に知っておき、かつ、攻撃に遭遇した場面で適切に対処することが重要となります。

パスワードリスト型攻撃❷は、以下のような手口で行われます。

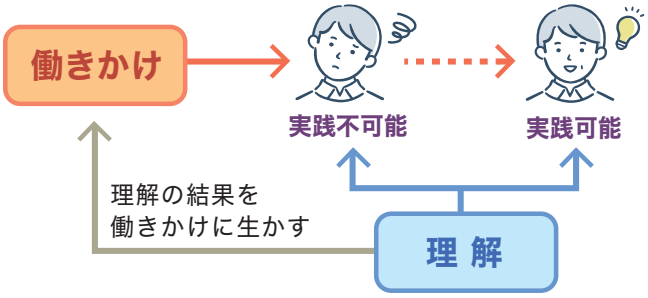
1. あるサービスから、IDとパスワードのリストが漏えいする。
2. IDとパスワードを入手した攻撃者はそれを使って別のサービスへアクセスを試みる。
3. 複数のサービスで同じID、パスワードを使用しているユーザーは不正アクセスの被害を受ける。

この攻撃の被害に遭わないためには、同じパスワードを使い回さず、サービスごとに異なる、複雑なパスワードを使用するといった対策を事前に取ることが重要となります。

こうした攻撃への対策力は、総務省が「ネットやSNSなど、ICT利用時の特性や留意点を正しく理解し、前向きに活用しながら、安全で豊かなデジタル生活を送るための能力」として提唱している「ICT活用リテラシー」❸の一つとして挙げられています。ICT活用リテラシーには、ⓐ取得管理 ⓑ安全確保 ⓒ他者・社会とのコラボレーション ⓓ作成編集 及び ⓔ活用の5つが定義されており、ここで述べた攻撃への対策力は「安全確保」が該当します。

ユーザーを知り、寄り添う対策を提供して「安全確保」をサポートするユーザブルセキュリティ

安全確保の能力は、知識、判断、行動の要素から成り立ちます。知識は教育や訓練によって強化できますが、判断と行動については、知識や実際の経験、状況に応じた適切な意思決定が必要となります。加えて、複雑な情報や手続きが、正しい判断や迅速な行動を妨げることに対する対応も求められます。サポート詐欺を例に取ると、知識があっても実際に攻撃に遭遇した際に真偽を判断するのが難しいために、対処が困難になる場合が該当します。パスワードリスト攻撃については、パスワードを使い回ししない、という事前の対策が必要ですが、多量のパスワードを管理する手間や、それに見合う効果を実感しにくいために、実践が進まないことが挙げられます。こうした課題を解決する方法として、ユーザブルセキュリティ❹が注目されています。これは、ユーザーの理解と対策の効用を得られやすく、かつ容易に対策可能なセキュリティの仕組みや機能の実現を目指す技術分野です。人間の行動や特性がセキュリティ意識や行動にどのように影響を与えるかを解明し、ユーザーが負担無く迅速に対策を講じたり、事前の備えを実践したりできるようにする支援を目的としています。



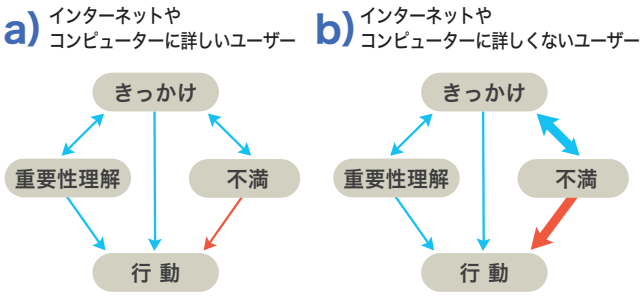
❶ https://www.ipa.go.jp/security/anshin/measures/fakealert.html ❷ https://www.jpcert.or.jp/pr/2014/pr140004.html
❸ https://www.soumu.go.jp/use_the_internet_wisely/special/lctliteracy_for_yps/
❹ Bryan D. Payne and W. Keith Edwards. 2008. A Brief Introduction to Usable Security. IEEE Internet Computing 12, 3 (May 2008), 13-21.
❺ 澤谷雪子, 佐野絢音, 山田明, & 窪田歩. (2020). 個人のインターネット利用におけるセキュリティ対策行動開始のきっかけの分析. 情報処理学会論文誌, 61(12), 1845-1858.
❻ https://www.ipa.go.jp/security/chocotto/
❼ 澤谷雪子, 佐野絢音, 山田明, & 窪田歩. (2021). インターネットユーザのセキュリティ対策における不満改善に関する考察. 情報処理学会論文誌, 62(12), 1948-1969.

ユーザブルセキュリティ研究の事例

ここでは、KDDI総合研究所が取り組むユーザブルセキュリティの研究をご紹介します。

はじめに、インターネット利用者のセキュリティ対策行動を促進するために、真偽の判断や事前対策に関するきっかけと行動との関係を、インタビューとアンケートを通じて調査・分析しました❺。その結果、ICTに詳しいユーザーの場合、脅威の体験や伝聞などの経験をきっかけに対策の重要性への理解が高まりながらも、「面倒さ」などの対策への不満も増加せずに、対策行動を取ることが分かりました。一方、ICTの知識が少ないユーザーの場合、対策の重要性の理解が進むと、それに伴って対策への不満も高まり、その結果、対策行動を起こしづらい状況が生じることが分かりました。この結果を受けて、ICTの知識が少ないユーザーを対象に、不満の改善が対策実施を引き起こすという仮説を立てました。そして、対策行動を引き出す支援のアプローチとして、不満の一つとして挙がった「面倒さ」を改善する方法を考案し、その効果を検証しました。具体的には、パスワードリスト攻撃への対策として有効な、サービスごとに異なるパスワードを設定する事例を対象に、その実践の手間を軽減する情報提供❻を行ったところ、不満が減少し、実験参加者の約半数が対策を実施する意向を示しました❼。この結果より、対策に関するユーザーの不満を軽減する情報提供や仕組みが、セキュリティ対策行動の促進に重要な要因であることが判明しました。このことは、ユーザーの意識、行動に応じた働きかけが重要であることを示します。

理 解　事前対策に関するきっかけと行動につながる思考プロセス

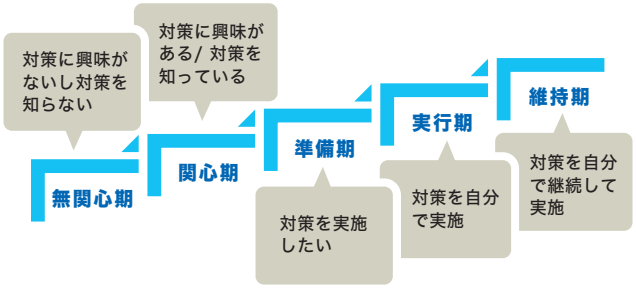


※ ━ はプラスの関係性、━ はマイナスの関係性、矢印は影響を与える向き、太さは影響の大きさを示す

次に、ユーザーに応じた働きかけを効率的・効果的に行うことを目指して、セキュリティ対策に対する意識や行動に基づいてユーザーを分類するセキュリティ行動変容ステージモデル（Security behavior stage model: SeBeST）を策定しました❽。これは、禁煙促進などに用いられる行動変容ステージモデルをもとにしており、セキュリティ対策に関して、ユーザーを「無関心期」から「維持期」までの五つのステージに分類します。こうした分類を行うことで、セキュリティ対策に関して理想的な状態に近づけるために、ステージの上昇を目指すアプローチを取ることが可能となります。策定したSeBeSTに関する調査を行った結果、ステージの上昇には、効果の実感と関心を持てること、他者への貢献を意識できることが影響することが確認されました。

最後に、SeBeSTを活用した研究事例を二つご紹介します。ひとつは、セキュリティ対策のうち、基本的かつ重要なものであるOSの更新の場面を対象として、ステージごとに最適な行動を促す「伝え方」を検証した事例です。この研究では「安全になる」というメリットを伝える方法の効果は準備期に限定的である一方、「危険になる」というデメリットを伝える方法は準備期から維持期まで幅広いステージに有効であることが分かりました❾。もうひとつは、セキュリティ対策を他者に任せているユーザーが適切な対策を取ることが難しい要因を解明して、改善策を提案した研究です。この研究では、他者に任せているユーザーは、インターネット上の情報が多すぎて、自分のデバイスに適したセキュリティ対策が分からないために、自身で対策を行うことが難しいことを解明しました❿。

理 解　SeBeSTによる分類



これを受けた解決策として、ユーザーが自分の利用するデバイスやサービスを入力すると、必要なセキュリティ対策のみを提示するツールを開発しました。このツールを48名の参加者に試用してもらった結果、70%の参加者が利用意向を示しました。今後、この仕組みをセキュリティ対策のサポートサイトなどに導入していくことを目指しています。

働きかけ　セキュリティ対策提示ツール

おわりに

本稿では、ICTを利用する際の攻撃対策力とICT活用リテラシーとの関係、そして攻撃対策における正しい判断や迅速な行動を支援するユーザブルセキュリティについて紹介しました。今後も、KDDI総合研究所は、皆さんが安心してインターネットやデジタル機器を利用できる環境の実現を目指して、ユーザブルセキュリティの先端研究を進めていきます。

❽ 佐野絢音, 澤谷雪子, 山田明, & 窪田歩. (2022). セキュリティ行動変容ステージモデルの提案とユーザ要因の関係性の分析. 情報処理学会論文誌, 63(9), 1458-1472.
❾ Sano, A., Sawaya, Y., Yamada, A., & Kubota, A. (2021, April). SeBeST: security behavior stage model and its application to OS update. In International Conference on Advanced Information Networking and Applications (pp. 552-566). Cham: Springer International Publishing.
❿ 佐野絢音, 澤谷雪子, 磯原隆将, & 西垣正勝. (2024). セキュリティ行動変容ステージモデルの改良と代理人委任層のセキュリティ意識向上に影響する要因分析. 情報処理学会論文誌, 65(12), 1682-1699.

巻末あとがき

今号を通じて各研究所から寄稿された記事を読み進めると、分野や立場は異なれど「情報リテラシー」がいかに私たちの社会を支える基盤であるかが浮かび上がってきます。かつて情報リテラシーは「便利にICTを使うための基本的スキル」として語られることが多く、セキュリティ対策においては技術や制度の整備に比べ、相対的に軽視されてきた側面がありました。しかしながら今日、「情報リテラシー」は単なる補助的要素ではなくなり、今号の内容から今後さらに重要な要素になることが見えてきました。

その背景には二つの大きな変化があります。第一に、AIの急速な普及です。AIは私たちの生活や業務を大幅に効率化する一方で、攻撃者側もAIを利用して「だます技術」を含めて攻撃を巧妙化させています。偽情報の生成やフィッシング詐欺など、攻撃を試行錯誤して従来以上に人の認知の脆弱性を突く形に手口が進化しています。こうした状況においては、技術的な防御だけでリスクを抑え込むことは難しく、最後の砦は「人間の判断力」となります。すなわち、情報を疑い、裏を取り、冷静に行動する力としての情報リテラシーがかつてないほど求められているのです。

第二に、社会全体が「情報戦」の時代に突入していることです。国家レベルでは認知領域を含む新しい競争が進み、企業組織にとってもサプライチェーン攻撃や金融詐欺が日常的な脅威となっています。こうした環境では、専門部署だけが情報資産を守ればよいという時代は終わりました。ユーザー、社員、研究者、経営層、そして市民一人ひとりが、自らの役割に応じて情報リテラシーを高め、能動的にセキュリティに関与していくことが不可欠です。

今号に収められた多様な視点は、最終的には一つの結論に収束しています。それは、「人のセキュリティを高めることこそが最大の防御になる」ということです。情報リテラシーは知識や技能の集合体にとどまらず、人の判断と行動を支える基盤であり、今後は技術対策と並ぶ二本柱として位置付けられていくでしょう。

これからの社会において、情報リテラシーは単なる教養ではなく、誰もが持つべき「生存スキル」となります。今号がその重要性を再認識し、具体的な取り組みを後押しする一助となれば幸いです。

サイバー・グリッド・ジャパン
GM 兼 次世代セキュリティ技術研究所 所長
小笠原 恒雄

BACK NUMBER バックナンバー一覧


Vol.1 2016年9月


Vol.2 2016年12月


Vol.3 2017年3月


Vol.4 2017年9月


Vol.5 2018年3月


Vol.6 2018年9月


Vol.7 2019年3月


Vol.8 2019年10月


Vol.9 2020年3月


Vol.10 2020年9月


Vol.11 2021年3月


Vol.12 2021年10月


Vol.13 2022年3月


Vol.14 2022年8月


Vol.15 2023年3月


Vol.16 2023年12月


Vol.17 2024年12月

CYBER GRID JOURNAL VOL. 18

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。
サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究の他、
複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより
日本のセキュリティレベルと情報モラルの向上に貢献しています。

株式会社ラック サイバー・グリッド・ジャパン
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
E-MAIL：cgj-info@lac.co.jp　https://www.lac.co.jp/

株式会社ラック
サイバー・グリッド・ジャパン

2025年12月発行