INFORMATION

ハッカー集う「CTF」って何？

CTFとは「Capture The Flag」の略で「旗取り競技」などと訳される。情報セキュリティの技術を競う大会で、クイズ形式で実施されることが多い。情報セキュリティに関する知識とスキルを駆使し、問題に隠された「Flag（フラッグ）」を探し出して回答する。ゲーム感覚でセキュリティに関する高度な知識・スキルを習得できる。

ただし、CTFに対する世間の評価は「参加してもビジネスには役に立たない」と厳しい。しかし、問題解決のためのチーム戦や、正しい解答を導きだすために問題となる事象を俯瞰することで得られる知識・技術、経験は、決してビジネスの現場でも無駄にはならない。

また、CTFに参加することで、企業や大学の垣根を超えた交流も育まれる。CTFは情報セキュリティに関心のある人たちのコミュニケーションを加速させ、今後、企業や研究機関などでセキュリティに従事する際に役立つ人的ネットワークを構築するきっかけにもなる。企業側もCTFで得た技術的な知識、学ぶ意欲を持った学生に対し、「自社のシステム運用をよりセキュアにする貴重な人材」と考えているようだ。ぜひ参加してみよう。

将来有望？磨け！セキュリティスキル

セキュリティ分野の人材不足が深刻だ。2020年には約19万人が不足すると予想されている。スキルを身につけた人材は、重宝されそうだ。

スキルを磨くには、何を学ぶべきか。コンピュータやプログラミングを思い浮かべるかもしれないが、それはあくまでも一面。サイバー犯罪と闘うなら法学、犯罪者や被害者を分析するなら、心理学が必要だ。

何を守りたいか、考えてみるのもヒントになる。自動車、医療、IoTと広い分野でセキュリティ対策が必要だが、もし自動車であれば、当然自動車に詳しくなければならない。

こうして見るとセキュリティだけ学ぶのではなく、幅広い視野を持つことが大事だと気付くだろう。

とはいえあまりに幅広い。手はじめに資格はどうだろうか。2017年より国家資格「情報処理安全確保支援士」がスタートする。

学生で技術を磨きたいなら、「セキュリティ・キャンプ」がオススメ。気軽に参加できる地方大会もある。技術を競うCTF大会「SECCON」も見逃せない。幅広い知識が求められる出題は刺激的。あらたな世界が見つかるかも。

これってセーフ？アウト？

問い：ネットゲームで、不正な操作をしてアイテムなどゲットすると違法ですか？

法的には昨今、「違法」と解釈されることが多くなってきました。

また不正行為に手を染めると犯罪に巻き込まれたり、それが原因で退学になったりと、様々なリスクがあります。

ネットゲームでのチート（不正なプレイ）も、違法性を問われる可能性があります。運営側や他プレーヤーなど、他人のものを勝手に取ったり、他人に損害を与えたりすれば、違法性は極めて高く、もはや仮想空間内の出来事ではすみません。

チート行為をする人たちの多くは、ネット上のコミュニティで情報交換をしています。そこには、どんな人たちがいるのか。中には、自分は「指示を出すだけ」の安全なポジションにいて、若者や学生を騙して手先として利用しようという「悪人」がいるのです。

不正行為のために「root化」する人もいますね。先日「脱獄iPhone」を販売した男が、商標法違反の疑いで逮捕されました。業界団体も警察も、今後、ますますネット上の不正行為に目を光らせていくでしょう。

人のものを取ってはいけない、人に危害を加えてはいけないという基本ルールは、ネットもリアルな世界も同じ。逮捕されて自分の将来を台なしにしないように、家族を悲しませないように、軽率な行動は絶対にしないでください。

もし、自分の知識や技術を活かしたいなら「悪の道」ではなく、人から尊敬され、仕事にもなる健全な道を選びましょう。CTFや脆弱性発見報奨金制度（バウンティハンター）など、いろいろありますよ！

PROFILE

園田 道夫氏

国立研究開発法人 情報通信研究機構
研究センター長

EVENT & NEWS

イベント日程

一度CTFはどんなものか。誰でも参加できるオンライン予選に参加してみよう！

▶オンライン予選
2016年12月10日(土)～11日(日)
会場:オンライン（初心者でも参加可能です）
言語:日本語／英語

▶CTF for GIRLS ワークショップ(女性限定)
2016年12月16日(金)
会場:株式会社インターネットイニシアティブ（東京、飯田橋）

▶決勝大会・カンファレンス
2017年1月27日(金)～29日(日)
会場:東京電機大学（東京、北千住）
決勝が行われるCTF会場の見学以外にも、各種セミナーやセキュリティに関連した企画を用意しています。ぜひ、一度足を運んでみてください！

詳しくはコチラ▶▶▶ SECCON 検索　メルマガ購読はコチラ▶▶▶

SPONSORS

SECCONでは通年でスポンサーを募集しています。詳細はinfo2016@seccon.jpまで。

IIJ Internet Initiative Japan / FUJITSU
ARBOR NETWORKS / NRI SECURE TECHNOLOGIES / Orchestrating a brighter world NEC / Designing The Future KDDI / cybozu
SECOM / SoftBank / dit / dwango / IBM
NTT / JPRS / HITACHI Inspire the Next 株式会社 日立システムズ / LINE
Asgent / Infosec / NTT DATA Global IT Innovator / KPMG / DNP 大日本印刷 / TEMPSTAFF TECHNOLOGIES / TREND MICRO
JIPDEC / NetAgent / HEARTBEATS / YAHOO! JAPAN / LAC

インフラスポンサー　SAKURA Internet　機材協力　YAMAHA　個人スポンサー　Digital Travesia

◆発行:SECCON実行委員会 / 株式会社ナノオプト・メディア　◆企画・編集:Security NEXT企画編集部

SECCON NEXT 2016 Winter

CONTENTS

TOP NEWS

悪に満ちあふれたサイバー世界 君は生き残ることができるか！？

普段何気なく楽しんでいるスマホで思わぬ被害
今、サイバー空間で一体何が起きているのか

えっ、「あの人気アプリ」にも偽物が！ サイバー犯罪者の眼光の先には…

悲しいことだが、インターネットの世界は悪意に満ちあふれている。ネット利用者が悪人ばかりという意味ではない。ごく少数の「サイバー犯罪者」が、善良な人々をだまそうと、スマホやタブレット、PCを狙っているのだ。

例えば、最近注目集まったのがスマホの「偽アプリ」。大人気の「ポケモンGO」にも「偽物」が多数出現した。こうした「マルウェア（悪意のあるソフトウェアのこと。ウイルスもマルウェアの一種）」をうかつにもスマホやタブレットにインストールしてしまうと、目に見えないところでさまざまな悪さを働く。アプリの人気が高いほど、偽物にひっかかる人も増える。みんなが欲しがる人気アプリこそサイバー犯罪者の狙い目なのだ。

マルウェアの被害はこれだけにとどまらない。犯罪者はズバリ「お金」を狙っている。端末などから認証情報を盗み出し、「ネット銀行の口座から現金を奪う」マルウェアや、保存したメールや写真、連絡帳などのデータへのアクセスを不能にし、「正常な動作に戻して欲しければお金を払え」と要求するマルウェアの被害も急増している。データを人質に「身代金」を要求する形だ。その他にも「アダルトアプリをダウンロードしたことを他人にバラす」と脅迫してきたり、スマホやタブレットから個人情報を盗み出して売りさばくマルウェアも。今後、スマホでできることが増えれば増えるだけ、犯罪者の標的も増える。

そして盗み出した情報をもとに、メールやSNSを使って、さらに友人たちも感染させようと動き出す。被害に遭うばかりでなく、ひとたび感染すると犯人に手を貸す「踏み台」となってしまう危険性もあるのがマルウェアのおそろしさだ。

隣の人がサイバー犯罪者？ 人生を狂わせる誘惑と闘え!!

残念ながらインターネット上の悪意はプロの犯罪者集団だけのものではない。一般の人が悪意に手を染めてしまうこともある。

リアルの世界では、やはり他人の目が気になったり、逮捕されることを恐れて犯罪を思いとどまる人は多い。しかし、ネットの世界では「たぶんバレないだろう」と甘く考え、誘惑に負ける人もいる。

たとえば「アカウントの乗っ取り」。パスワードが盗み見られたり、あるいはパスワードが簡単に想像できるようなものだと、FacebookやInstagramなど、SNSのアカウントはやすやすと乗っ取られてしまう。

アカウントを乗っ取られれば、手塩に掛けて育てたキャラや、苦労の末に手に入れたアイテムをあっけなく奪われ、勝手に課金されてしまうこともある。オンラインショップなどであれば、勝手に商品を買われるなど、被害はさらに甚大だ。

恋人や友人によって、マルウェアを仕込まれたという事例もあとを絶たない。位置情報を漏らすマルウェアによって、居場所を追跡される。スマホの遠隔操作で盗撮や盗聴される。メールやSMSも筒抜けだ。あまり考えたくないことだが、親しい関係だと思っていても、相手の心の中まではわからない。やはり自分の身は自分で守ることが大事となる。

素人でも容易にマルウェアを入手したり、不正アクセスできると聞けば、驚きを感じる人も多いだろう。とはいえ、たとえ遊び半分の軽い気持ちや、親しい関係であろうとも、犯罪行為に他ならない。バレないと思うかも知れないが、アクセスした記録など動かぬ証拠がバッチリ残っている。最近ではサイバー犯罪の取り締まりは強化されている。人生を棒に振らないためにも、決して悪事には手を出さないことだ。

身を守る為の対策

まずは、自分の身は自分で守る意識を持とう。軽率な行動は命取りだ。アダルトサイトなど、いかがわしいサイトへの会員登録などもってのほか。「現金がもらえる」「極秘映像プレゼント」など、甘い言葉で興味をひきつけるのが詐欺師の手口なのだ。

アカウントの乗っ取りから身を守るにはパスワードを守るしかない。誰にも漏らさないのは当然として、簡単に予想できるものは避ける。端末も勝手に操作されないようロックをかけておく。

メールにも注意。どんなに気をつけていても、ネットを使っていれば、迷惑メールや詐欺メールが届く。身に覚えのない請求はもちろん、公共機関を装ったり、自分自身が写真を送ったように見せかけるなど、手口は巧妙だ。心当たりがないメールを安易に開かないこと。特に添付ファイルや本文中のリンクには気を付ける。

ウェブサイトにもワナがいっぱい。「マルウェアに感染しています。駆除するにはここをクリック」とだます詐欺もある。

アプリやソフト、コンテンツをDLするときは、Google PlayやApp Storeなど、公式ストアなどを利用する。信頼できる会社か評判なども確認してから取得しよう。特に連絡帳や写真、位置情報など、必要以上に「アクセス権限（パーミション）」を要求するものは要注意だ。

SNS上で友だちがすすめる楽しそうなアプリもよく確認してから。友だちの端末が乗っ取られ、マルウェアがメッセージを送っていることもある。

セキュリティ対策ソフトは必ず入れておこう。ただし過信も禁物だ。何をしても大丈夫というわけではない。もし少しでも気がかりなことがあれば、必ず大人に相談しよう。

あなたの知らない「ハッカー」の素顔

あなたは「ハッカー」という存在にどのようなイメージを描くだろうか。暗闇でパソコンのキーボードを叩き、世の中を混乱させるサイバー攻撃の首謀者だろうか。しかし、それはまったくの誤解だ。今回は本物の「ハッカー」を招き、意外な真実の姿を紹介する。

PROFILE

竹迫 良範氏

SECCON実行委員長。
趣味はCPUの命令セットマニュアルを眺めること。独自のハッキング研究を日本国外のラスベガス・韓国・台湾などでも発表している。

知られざるハッカーの「意外な職業」

ー今日は日本を代表するハッカーとして知られるお二人に、お話を聞きたいと思います。まずは、お二人の普段のお仕事について。ハッカーと呼ばれる人たちも普通に働いているのですよね。

竹迫:情報サービス会社で技術フェローを務めています。技術者が働きやすく、より成長していけるような環境を整えるのが仕事です。それとは別にセキュリティコンテストである「SECCON」の実行委員長を務めています。SECCONはセキュリティに関する問題を解決する競技会で、技術者の育成や技術力の向上を目的にしています。

ーいずれも技術者の成長を助けるお仕事ですね。寺島さんはどのようなお仕事を?

寺島:セキュリティベンダーで技術者をしています。サイバー攻撃を受けた企業を調査し、攻撃の手口を調べ、その足跡をたどり、ファイルの状況を細かく調べます。原因を特定して、今後のセキュリティ対策を支援する仕事です。そのかたわら、竹迫さんと一緒にSECCONの副実行委員長をしています。

「悪のPCオタク=ハッカー」は大まちがい

ーお二人とも会社で重要な仕事を任されていて、世間一般の人が抱くハッカーのイメージとはちがいます。そもそもハッカーというのはどういう人なのですか?

竹迫:ハッキングの本質は、すでにある部品を組み合わせて、思いもよらぬ新しいものを作りだすことです。それが私なりの「ハッキングの定義」です。

寺島:基礎的な技術の積み重ねがあって、それに新しい発想を加えて、今までとは違うことができるようにする。それが、私が考えるハッキングの定義です。コンピュータについて幅広く、奥深い知識を持っていて、それを駆使して、どうにかして問題を解決してしまうのがハッカー。自分自身、ハッカーと呼ばれる機会はあまりないのですが(笑)。

竹迫:その一方で、技術を悪用して不正アクセスしたり、他人のコンピュータを不正に操作してしまうことも、報道などで「ハッキング」と呼ばれることがあります。こういう行為はもともと「クラッキング」、それを行う人は「クラッカー」と呼ばれていましたが、ハッカーという言葉が一人歩きし、誤解されている部分があります。

ハッカー誕生への道のり

ーお二人はどのようにして高い技術を身につけたのですか?

竹迫:小学生のころファミコンが出て、中学生の時、はじめてのパソコンを手にしました。それがFM TOWNSという機種。インテルの386というCPUで、メモリとCD-ROMがあって、OSが入ったCD-ROMでブートするという、PC-AT互換機とほぼ同じ構成でした。興味が向くままにケースを開けて、内部構造を調べているうちに、どんどんのめり込んでいきました。その後は、技術の進歩とともに、それをリアルタイムに吸収しながら、自然と腕を磨いていきました。上の世代の支えも大きかったですが、40歳前後の自分たちの世代が、まさに新しい技術をどんどん吸収しながら「プログラマー」という職業を切り開いてきたという自負があります。

寺島:私は「畑違い」です。もともとは農学部出身で、トラクターの機構など車系の仕事をしていました。大学のときにインターネットに触れて、仕事にしたいと思うようになり、勉強して転職したのが2001年。その会社で、セキュリティ関係のサービスを立ち上げることになり、勉強していくうちにセキュリティが専門になっていきました。

それとCTF(Capture The Flag)へのチャレンジですね。CTFというのは、ハッカーコンテストとも言われる競技会です。毎年ラスベガスで開かれるDEFCON(世界一の規模と伝統を誇るセキュリティ・イベント)の名物大会なんです。世界中のハッカーが腕を競っています。僕はオンラインで参加できるようになったのをきっかけに参加するようになりました。

ーそれで国内のCTF大会であるSECCONの実行委員会に関わっているのですね。

竹迫:寺島さんは本場ラスベガスのDEFCONでも活躍する日本CTF界の第一人者ですからね。世界最高峰のレベルを知った上で、国内の人材育成を目的としたSECCONを運営しています。

おすすめはセキュリティ(竹迫)まず好きなことを極める(寺島)

ーおふたりのようなハッカーになるにはどうしたらいいのでしょうか。

竹迫:コンピュータに関心があって、もっと深く関わりたいのなら、セキュリティという入り口から飛び込んでいくのをおすすめします。というのも、これから多くの企業で、サイバー犯罪や、クラッカーの驚異から身を守る必要が出てきます。ところがそれができる人材がまったく足りていないのです。

とくに攻撃を受けた後に、調査ができる人材はとても貴重です。外部に委託する企業も多いですが、時間がかかりすぎて対応が遅れてしまいます。だからセキュリティという仕事は、職業としてとても有望です。

もうひとつおすすめポイントは、セキュリティの分野は常に新しいことが起きます。それに対してなんとか対応していくというのが仕事なので、エンジニアとして、ハッカーとして、どんどん成長できます。ハッカーの定義をお話ししましたが、「教えてもらってないからできません」という人はハッカーではないし、ハッカーにはなれません。

寺島:とにかくゴールに向かってどんな手段を使ってでも積み上げて、近づいていくという……。

竹迫:そうですね。しかもそれは「正当な道」でなくていい。迂回路でもなんでも、教科書通りでなくていい。とにかく新しいことにチャレンジしていくのがハッカーの魂で、まず必要なのはそれだけです。

寺島:新しい、わからないことがどんどん出てきますが、「なんとかしようよ」と言い合って、なんとかしています(笑)。だからいつも最先端にいるイメージです。

竹迫:SECCONでは、必ず新しいことを取り入れたり、視野を広げたりできるように出題を工夫しています。「ハッカーの魂」を体感できる場です。ぜひ挑戦してほしいですね。

PROFILE

寺島 崇幸氏

SECCON副実行委員長。
世界のカンファレンス、CTFに参加。
おもしろいことを求めて世界をさまようサラリーマン。
日頃はインシデント対応の業務に従事。

ーもしハッカーになりたい高校生がいたら、どんなアドバイスをしますか?

寺島:まずは好きなものをとことん極めてみるのがいいと思います。ひとつのことを奥深く知っていく過程で、その周辺にはどんなものがあるか、行き詰まったときにどうやって進めばいいのかということを覚えることに繋がります。

どうなっているのか、どういう仕組みなのかと、好きなことだから挑戦できると思います。はじめはそれでいい。とんがった先端の部分はとても大切です。

竹迫:そのうちにとんがった部分だけではなく、幅も拡がってきます。

ハッカーは未来でも新たな問題に取り組んでいる

ー最後にハッカーをとりまく将来について教えてください。現在ハッカーが活躍するセキュリティの分野は、今後5年、10年先はどのようになっていくのでしょうか。

竹迫:今後、多くの企業が何らかの形で「ICT企業」へと変化せざるをえないと言われています。セキュリティ人材への需要はしばらく高水準で続きます。人工知能(AI)の技術が急速に進化していることを考えると、今後はAIにおけるセキュリティという仕事は出てくるでしょう。

寺島:仕事の中身はどんどん変わっていくのでしょうね。

竹迫:ただ、新たな問題を解決し続けるのがハッカーの仕事ですから、そういう意味では将来もあまり変わらず、次々にでてくる問題に取り組んでいるだろうと思います。

大人気SNSの快適と安全を守る! LINEのセキュリティ室に聞く

全世界の月間利用者数2億2000万人。日本の登録者数6800万人、今や日本人の2人に1人以上が利用者というLINE。利用者が多いだけに、直面するサイバー攻撃の脅威も巨大だ。脅威と闘うセキュリティエンジニアに話を聞いた。

大人気の裏で脅威と闘うLINE

ー人気サービスだと、サイバー攻撃も多いのではないでしょうか。

市原:サービス停止を狙うDoS攻撃やマルウェアなど、システムの弱点(脆弱性)を突く攻撃があります。それから「アカウントの乗っ取り」。LINE PayやLINEコインの不正使用や不正取得、ゲームアプリでは「チート」と呼ばれる不正プレイもあります。

ー多種多様な攻撃にさらされていますね。どのような体制で対抗しているのですか。

市原:専門部署であるセキュリティ室では、インフラ、ネットワーク、情報、アプリケーションという4つのセキュリティチームに分かれ、約30人のエンジニアが働いています。私はアプリケーション・セキュリティチームのリーダーを努めています。17名が所属しています。

中村:私はアプリケーション・セキュリティチームの中でも、サービスを提供する前に、脆弱性(攻撃で狙われる弱点)がないかをチェックする「リスクアセスメント」という業務のリーダーをしています。チームメンバーの多くが関わる重要な業務です。

市原:他にも、他部門と連携しながら企画段階にある新サービスのセキュリティコンサルティングをしたり、すでに提供されたサービスのセキュリティイシューの対応をしています。LINEの場合、海外の拠点でも開発したり、国ごとに異なるサービス提供をすることも多いので、外国人エンジニアとのコミュニケーションも重要です。

中村:私達のチームの場合、日本人は17名中で5名ほどしかいません。日本語以外でコミュニケーションを取ることも多く、インターナショナルな職場です。

迅速な意志決定で実現する利用者第一主義

ー世界規模のセキュリティ対策をスムーズに進める秘訣は?

市原:専門家によるチームワークです。以前に発生した「アカウントの乗っ取り」は、セキュリティ室だけでなく、カスタマーサービス、広報、企画、開発部門などが連携して対応してきました。「アカウントの乗っ取り」は、LINE以外のSNSでも多くの脅威にさらされています。複数のSNSをはじめ様々なサービスで「同じID(メールアドレス)とパスワード」を使い回す人が多いことが理由の1つです。どこかでIDとパスワードが盗まれてしまうと、それを悪用した「なりすまし」が起きてしまう。

中村:LINEのシステムには、アカウントを奪われる脆弱性の有無とは無関係に、他のサービスからIDとパスワードが漏れてしまえば、それを悪用したLINEアカウントの乗っ取りが起きる。

市原:そこで、カスタマーサービス、広報、企画などが連携して、正しいパスワード管理方法について注意喚起したり、新しい認証フローを導入したり、アカウント引き継ぎ方法をガイダンスしたり、いかにに早く被害を食い止めるかを最優先に、悪戦苦闘しながら対応してきました。

中村:機能強化によるセキュリティ対策も大切です。同時に安全な使い方についてユーザーとコミュニケーションをとることも非常に大事です。セキュリティを強化すると安全性は高まりますが、強化しすぎると例えば「何度もIDとパスワードの入力が必要」など、「使いにくい」サービスになってしまう。ユーザーを第一に考える「カスタマーファースト」を念頭に、「安全性」と「使いやすさ」を両立しなければならない。そのバランスを部門間でつねに議論しています。

PROFILE

LINE株式会社 セキュリティ室 市原 尚久氏

SI企業でICカードのセキュリティ事業に従事。2015年、LINE入社。LINEが提供するアプリケーションのセキュリティ全般を担当するチームでリーダーを務める。

LINEを守るエンジニアの素顔

PROFILE

LINE株式会社 セキュリティ室 中村 智史氏

独学でサイバーセキュリティを勉強し、ユーザー企業の開発者などを経て2011年にLINE(当時:NHN Japan)へ入社。脆弱性対策部門のメンバーを束ねる。

ーセキュリティの世界へ入ったきっかけは何でしょうか。

中村:1995年ごろ、普及しはじめたインターネットに飛びついたのですが、ひどい目にあいました(笑)。マルウェアに感染するわ、情報はとられるわと(笑)。「これ以上、ひどい目にあいたくない」という一心でセキュリティ関連の本を読んで猛勉強しました。

市原:私はシステムインテグレーション会社に入り、1990年代半ば、パチンコ用プリペイド磁気カードの偽造事件の対策プロジェクトでセキュリティに初めて触れました。さらにICカードの開発を担当し、ヨーロッパのICカードセキュリティ系コミュニティーとの協議に参加しながらICカード用OSを作り上げる仕事に従事しました。その仕事では、自分の設計やセキュリティに対する考え方の甘さをあっという間に指摘されて、打ちのめされましたね(笑)。2000年代初めのその経験が今に繋がっています。

ーセキュリティに関する仕事のやりがい、苦労はどのようなものですか?

市原:LINEは、つねに新しいことを企画し、新しいサービスを開発し提供していかなくてはなりません。そのなかで安全性をいかに担保するか。カスタマーファーストの視点からも、その問題は避けては通れません。新しい知識、技術を吸収するために勉強も必要です。タフな仕事ですが面白い。

中村:普段、暮らしている世界と異質の「システムの世界」に入り込み、その中で脆弱性や不具合(バグ)を見つけ出す、そこにはある種「超常的」な感覚があると思います。個人的には「魔法を使うような感覚かな」と。防御方法を知ることは、攻撃方法を知ることでもあります。一般の人と違うものをいつも見ている感覚があります。

ーセキュリティ分野に関心がある若い方々にアドバイスを。

中村:セキュリティに限らず、能力を身につけると、それを悪いことにも使うことができます。高い技術を持っている人には、そうした誘惑があるかもしれません。ただ、それをやったら二度と心から笑える日はこない。枕を高くして眠れなくなり、一生後悔します。セキュリティに携わる若いハッカーには、そのことを強く言い続けたいです。

市原:セキュリティという仕事は、誇りとモチベーションを与えてくれます。挑戦することがとても大切で、間違ったり笑われたりすることを決して恐れないでほしい。どんどんチャレンジする気持ちを忘れないでほしいと思います。そして、問題解決には仲間の力が大きいことを知って欲しいですね。セキュリティは決して1人でできる仕事ではありません。技術も大切ですが、それ以上に多くの人とつきあって、コミュニケーションの取り方を学んで欲しいと思います。