Vol.2015-DPS-164 No.2
Vol.2015-EIP-69 No.2
2015/9/10

利用者のパスワード管理意識を高めるケーススタディの一考察

原田 要之助[†1]，笹原 務[†1]，芝原 幸弘[†1]，佐藤 雄二[†1]，植田 修[†1]，
羽田 真也[†1]，長原 欣司[†1]，佐野 宏明[†1]，上河内 栄治[†1]，久保 知裕[†1]

パスワードの管理についての利用者に対する啓蒙が重要となっている．従来，パスワードについては，複雑にすることが求められているが，様々な情報サービスがWebベースで提供されるようになり，個々人が管理するIDは10を超えると言われている．このような中，昨今，パスワードリスト攻撃が広っており，同じパスワードを利用することの多い一般の利用者がなりすましによる被害に遭うケースが増えてきている．本ケーススタディは，大学生を対象にアカウントとパスワードに関する啓蒙を行うには，適していると考えてケーススタディを作成した．ケーススタディを大学などで実施した結果，利用者のパスワードに対する認識を向上させることができ有効性を検証した．本稿では，ケースの内容，効果の評価，課題について述べる．

Development of protection of password through case study approach

Yonosuke Harada[†1], Tsutomu Sasahara[†1], Yukihiro Shibahara[†1] , Yuji Sato[†1],
Syuu Ueda[†1], Shinya Hada[†1], Kinji Nagahara[†1], Hiroaki Sano[†1], Eiji Kamigauchi[†1],
Tomohiro Kubo[†1],

1. はじめに

現在の青少年は，デジタルネイティブ[1]世代と呼ばれていて，日常的に高度な情報端末対象を駆使し，インターネットの Web サービスやオンラインショッピングサービスをはじめ，ソーシャルネットワーキングサービス（以下では，SNS という）を縦横無尽に活用している．しかし，インターネットが普及した現在において様々な不正や詐欺行為がこれらの世代をつけ狙っている．そのため，スマートフォンなどの情報端末やインターネット，SNS のメディアに対する啓蒙が必要となっているが，一般的な大人世代は，この事実を知っていても，自分たちも知識が十分でないため彼らを指導できていない．そのため不正や詐欺の被害に合わないための教育や啓蒙活動が必要となっている．

本稿では，情報セキュリティ大学院大学の研究と実務融合による高度情報セキュリティ人材育成プログラム（ISS スクエア）のマネジメント部会の 2014 年度における活動で検討した利用者のパスワード管理意識を高めるためのケーススタディの開発とその評価について報告する．なお，本稿は，昨年度発表した SNS の利用者意識を高めるケーススタディの一考察［1］の続編である．

2. デジタルネイティブのアカウントとパスワード管理問題

2.1 ネットワークへのアクセス手段

ネットワークへのアクセス手段を図 1 に示す．

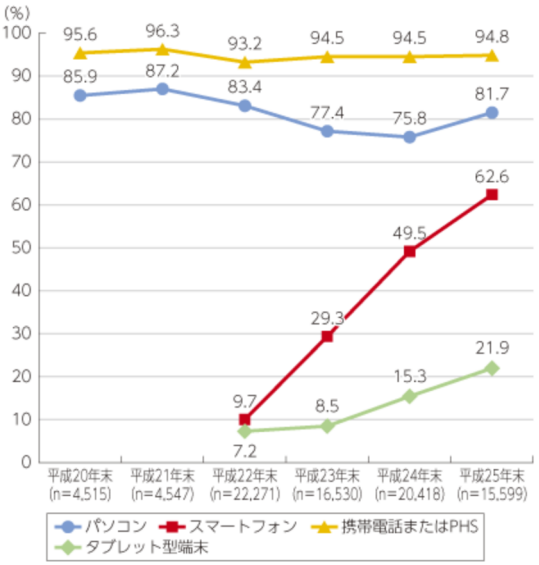

図 1　主な情報通信機器の世帯保有状況（平成 20～25 年）（出所：総務省平成 25 年通信利用動向調査）［2］より

---

†1　情報セキュリティ大学院大学

1：生まれながらに IT に親しんでいる世代をデジタルネイティブ，IT 普及以前に生まれて IT を身につけようとしている世代をデジタルイミグラントと Peter Sondergaard 氏が名付けた．

Vol.2015-DPS-164 No.2
Vol.2015-EIP-69 No.2
2015/9/10

図 1 の平成 25 年度の情報通信機器ごとの世帯保有率からは，スマートフォンの利用が 62.6%となっており，パソコンの 81.7%，に近づいている．さらに，タブレットの利用率も 21.9%となっている．スマートフォンとタブレットを合計すると，84.5%となり，既にパソコンを上回っている．平成 24 年度の同調査では 74.8%であり，1 年間で約 10%増加した．増加傾向からは，スマートフォンが，全ての情報通信機器を上回ると考えられる．このような状況の中，スマートフォンなどからのインターネットへのアクセスの際のアカウントとパスワードのセキュリティが重要になる．

2.2 SNS の利用について

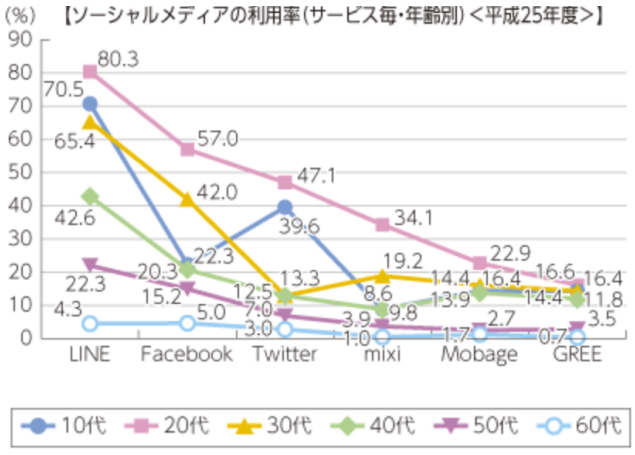

図 2　SNS の利用状況（出所：総務省情報通信政策研究所「平成 25 年　情報通信メディアの利用時間と情報行動に関する調査」[3]）

図 2 は，SNS の世代別，メディア別の利用状況を示す．とくに，SNS がデジタルネイティブ世代のコミュンケーションツールとして広く使われていることが分かる．この傾向は世代が上がるにつれて低下している．さらに，LINE などの新規のサービスの急速な利用の集中化が見られる．Facebook が利用者の累積数が 1 億を越えるのに，5 年を要したが，LINE では，わずか，1.5 年で達成している．この事実は，デジタルネイティブは，事業者が提供する SNS サービスに満足しておらず，よりよいサービスや新しい機能，無料での利用などが提供されれば，SNS サービスに対して流動的であることも示唆している．すなわち，メディアの栄枯盛衰の変化が速いため，多くの利用者が多くの SNS メディアを短期的に利用することが想定される．他の SNS に移っても使わなくなったアカウントを消去せずに残しておくことである．これから懸念されるのは，使われないアカウントが多数事業者に登録されたままになることである．同様な現象が，Web サービスやオンラインショッピングなどでも起きると想定され，個人が登録するアカウントは増大していると考えられる．

2.3 アカウントとパスワードの管理

インターネットの SNS や Web サービスでは，個人を識別するのは，アカウントとパスワードによっている．ただし，SNS や Web サービスの事業者から見るとユーザはアカウントで個別に識別できるが，利用者側からは，多くのサイトに異なるアカウントを持つことになる．様々なサイトに対して個別のアカウントとパスワードとなると覚えきれない．

個人がどの程度のパスワードを必要とするアカウントを利用しているかについては，鈴木らの日本銀行金融研究所/金融研究の研究がトレンドマイクロ，シマンテック，野村総研などの調査結果を比較している（付録 1 参照）［4］．トレンドマイクロの調査では，2012 年調査では，平均 12 となっており，野村総研の調査結果では，平均 19 となっている．シマンテックについては，加重平均すると 8.28 となる．いずれにせよ，一人あたり，10 近いサイトにアカウントを持っていることが分かる．一方，野村総研の調査では，一人が覚えられるパスワードについても調査しており，平均は 3 とのことである［5］．この結果からは，アカウントと管理できるパスワードの差が見て取れる．すなわち，複数のサイトで同じパスワードを用いているという実態が分かる．

2.4　メールアドレスをアカウントとするサービス

現在，多くの Web サイトや SNS サービスでは，個人の一意性のあるアカウントとしてメールアドレスの利用を進めている．これは，事業者がメールサービスのアカウントがインターネットで一意性が担保できているからである．そのため，SNS や Web サービスの多くが新規のサービス申請に対して，メールアドレスを推奨することが多い．メールアドレスであれば，サービスに対する連絡にも使えるので事業者にとっては便利である．また，利用者にとっても，アカウントを同じにすることができるので，アカウントを個別に管理しなくてもよくなる．このような経緯で，多くのサイトでメールアドレスがアカウントとして用いられている．

一方，パスワードは，利用者の責任で設定し変更することになる．いろいろなサイトでメールアドレスをアカウントとして利用するようになると，管理する個人はサイトを識別してこれについては，平野・森井らは，「複雑なパスワードを数多く記憶することは困難であるという理由から，安全なパスワード管理が行われていない．例えば，パスワードを記したメモ帳を持ち歩く，端末にパスワードを記憶させておく，同一のパスワードを複数のサービスに使い回すなどパスワードの管理を簡単にする一方で安全性が低い手段が取られている」と指摘している．［6］

2.5 パスワードの変更の頻度について

大学生に対するパスワードの管理については，八城が，安田大学の学生のメール及び計算機利用のパスワードの使用に関する意識調査を複数年にわたって実施している.「ネットワーク・サービス全般のパスワード変更について継続調査を行った．中略　パスワードを変更した経験がないとの回答は，もっとも多いグループで 87.5%，最も少ないグループでも 65.1%であった．この少ないグループについては授業等で半ば強制的に変更させられたなどが理由であり，実質的には変更したことがないと同列に扱っても差し支えないと」と述べている［7]．すなわち，デジタルネイティブの世代ついては，例え，授業などでガイドしても，強制的でない限り 90%近くが自主的に変更することはないと考えられる．情報セキュリティのポリシーや管理策では，定期的なパスワードの変更を推奨しているものの，大学などでは実態としては,変更されないと考えるべきであろう．一方，谷津は，早稲田大学の学生に対して学生のパスワード利用状況と忘却について述べ，長いパスワードを記憶させることが難しいことを指摘している［8].

2.6 リスト型パスワード攻撃について

SNS については，さまざまなパスワード漏えい事故が報告されている．中でも，2013 年に起きた MIXI の 26 万件のアカウントが不正アクセスを受けたと報告された．この際の不正ログイン回数は 430 万回となったと報告されている．こことときには,他の SNS や Web サービスなどのアカウントとパスワードを用いて攻撃されたと報告されている．この攻撃は,一般的にリスト型アカウント攻撃と呼ばれている．これは，他のサイトから進まれたアカウントとパスワードのセットを用いて不正アクセスを試みるものである［9].

一方,2014 年 7 月 22 日,警視庁サイバー犯罪対策課は,LINE アカウント乗っ取りによる詐欺被害が，6 月以降 1 ヶ月で東京都内において計 100 件発生して，その被害総額は約 650 万円に上ると発表した．アカウント乗っ取り事件では，悪意を持った第三者にアカウントを乗っ取られて，親友や知人などにウソのメールが送信された．犯人は，いろいろな理由を述べて，Web マネーの購入を持ちかけて，被害者をだまし，Web マネーを受け取るとすぐに換金して逃げるという手口である．後に，本人に確認して，詐欺であることが分かっても被害にあった Web マネーを取り戻すのは困難である．多くの場合，犯人は詐欺に使ったメールアドレスを捨てて，身元を隠すからである．この詐欺行為によって数万円分の被害を受けた人も出ている［9]．このリスト型攻撃は，あるサイトで盗まれたアカウントとパスワードが別のサイトのアクセスに利用されるため，アクセスが少ないサイトや既に使わなくなったサービスのアカウントの場合などでは，本人がアカウントを乗っ取られていることに気づかず，被害についてすぐに原因が分からないことがある．さらに，事業者にとっては，正しいアカウントとパスワードによるアクセスのため，防止することができない．さらに，事例が示すように，他人に被害を与えてしまうことが問題を複雑にしている．

今後，リスト型攻撃については，詐欺行為と組合せることで様々な展開が考えられるため，対策は必須と考えられる．リスト型攻撃の対策については，IPA の「オンライン本人認証方式の実態調査」に網羅されている．すなわち，ここで取り上げられている対策が実施されることが望ましい．しかし，このリストには，リスト型攻撃一般について述べられているものの，事業者の対策が中心であり，大学生などのデジタルネイティブの世代が使うには難しい点もある．また，2.3～2.5 節に述べたように，パスワードの有効期間などのように実効性が困難なものもある．教育においては，ケーススタディで学習させて，デジタルネイティブのプラクティスとなるものが望ましい.この観点からは，１，６，７が中心となると考える．これらについては，ケーススタディで学習させる必要がある．他のものについては，ストーリの中で紹介するようにすることが望ましいと考える．

表１　リスト型攻撃対策（出所：IPA,「オンライン本人認証方式の実態調査」）

対策	内容
1. ID・パスワードの使い回しに関する注意喚起の実施	サービス毎に異なるID・パスワードを設定するよう利用者に注意喚起する
2. パスワードの有効期間設定	パスワードに有効期限を設定し、利用者に定期的に変更させる
3. パスワードの履歴の保存	数世代前に使用したパスワードへの変更を認めないようにする
4. 二要素認証の導入	ID・パスワード以外の認証要素（ワンタイムパスワード等）を追加する
5. ID・パスワードの適切な保存	サービス運営事業者において暗号化等ID・パスワードの適切な保存を行う
6. 休眠アカウントの廃止	長期間利用実績の無いアカウントをデータも含めて削除する
7. 推測が容易なパスワードの利用拒否	パスワードポリシーを定め、推測が容易なパスワードの利用を拒否する

3. ケーススタディの作成について

情報セキュリティのリスク認識を高めるのにケースメソッドが適していることを，SNS を題材にしたケーススタディの教材を開発して，実際の教育の場で検証し，その結果は良好であった［1]．そこで，パスワードの教育についても,同様のアプローチとしてケーススタディを開発した.

以下に開発，試験，検証した過程について述べる.

3.1 ケーススタディで取り扱うパスワードの問題について

パスワードの問題は，2 章に述べたように，以下の点に集約される．とくに，デジタルネイティブの世代に対しては，次の点を教育する必要があると考えられる

（１）アカウントの乗っ取りの問題
（２）複数のサイトに対するパスワードの使い回しの問題
（３）パスワードの強度の問題

これらの学習を含む形で，ケーススタディを作成した.

3.2 ケーススタディが目指したもの

ケーススタディの作成においては，デジタルネイティブ世代が実際に陥りやすいパスワードが持つ問題について自ら認識し，自らが対応できることを目指した．グループに分かれた参加者がケースの分析やグループでの議論を通じてケースに書かれたリスクを読み取って，解釈して，自分のパスワードの問題を理解するとともに，実際にパスワードを作成して，意見交換できることを目指した．

3.3 ケーススタディの利用者

また，パスワードの問題は，単に，学生だけのものではなく，大学人や企業人にとっても利用できるものとした．実際に企業における導入研修にも用いて，利用可能性を探った．このケーススタディが単に，デジタルネイティブなどのインターネットをこれから利用する人材のみならず，既に利用している人へも応用できることを目指した．

3.4 ケーススタディについて

ケーススタディの内容としては， SNS やインターネットの利用経験がある 10 代後半（専門学校生，大学生など）が予備知識なしに内容を理解できて，議論できることを想定した．なお，ストーリとしては，パスワードに関する事件に遭遇しながら，問題点を理解し応用力を身につけさせることを意図した．ケーススタディでは，大学生が SNS を乗っ取られて SNS から不正メールを送られたり，不正な買い物をされたりして，被害に遭うストーリをベースに，情報セキュリティに詳しい先輩から指導を受けて対策ができるようなるとにというスタイルにした．また，パスワードについては，長さと強度の観点から，使い回す部分＋サイト毎に変化させる部分の組合せによる作成方法を学習させることにした．

学生らは，このケースを熟読して，各自の SNS やインターネットの Web サイトの利用経験を加味して，問題を理解して，以下の課題を学習する．

① パスワードの強度：短いパスワードの危険な点の理解
② 強いパスワードの作り方：パスワードの作り方について
③ Line のアカウント乗っ取り事件：知識
④ 「パスワードリスト攻撃」という言葉：攻撃の脅威（影響範囲などを含む）
⑤ パスワードの使いまわしの危険性
⑥ 多要素認証：知識
⑦ ワンタイムパスワード：知識

4. ケーススタディの評価結果について

ケーススタディについては，2014 年 8 月から 10 月にかけて作成した．11 月に初版を用いてプレ試験を実施した．その結果を受けて，内容や事件を精査した．見直しでは，パスワードを登録する際の CHAPCHA と呼ばれる人間の目の識別を利用した入力が使われる意味や二要素認証などの知識（表 1 参照），さらには，攻撃者が隠れて暗躍している小話を挿入して，リアリティを高めた．

このケースを用いて，神奈川県内の女子大学の経営学の学習の一部として実証実験した．その結果を以下に示す．実施時期は，2015 年 1 月，参加者は 74 名である．また，企業の新人研修にも利用した．実施時期は，2015 年 7 月，参加者は 12 名である．

4.1 インターネットの利用について

今回のデジタルネイティブ世代（大学生や企業への新入社員）がどのような SNS や Web サービスなどにアカウントを持っているかについて複数回答で聞いたものを図 4 に示す．図 4 からは，LINE などの SNS が 90%と一番利用されていて，これに Web サイトの閲覧が 88%と続いている．一方，ネットショッピングは 32%．オンラインゲーム（スマートフォン）は 29%，オンラインゲーム（PC）は 9%であった．図 4 からは，2.2 節で述べたように SNS や Web サイトの閲覧はデジタルネイティブ世代の必須のツールとなっていることが分かる．

SNS	Webサイトの閲覧	ネットショッピング	オンラインゲーム（スマートフォン）	オンラインゲーム（PC）
90%	86%	32%	29%	9%

図 4 インターネット(SNS など)の利用用途について(N=86)

今回のケーススタディの中心としたデジタルネイティブのアカウントの乗っ取りや不正利用などの被害に遭遇した経験について複数回答で調査した結果を図 5 に示す．図 5 からは，直接被害にあったとするものが 4%あり，また，知人や家族が被害にあった 38%と合わせると 42%が，身近で被害にあっていると言えよう．知らないのは 6%であり極めて少ない．この結果からは，もはや，アカウントの乗っ取りや不正利用は日常的にいつでも遭遇する問題となっていると言えよう．また，事件についても 51%が聞いたことがあるとしていることから，適切な知識を与えて問題に対応することが求められていると言えよう．

自分が被害にあった	家族や友人が被害にあった	聞いたことがある	知らない
4%	38%	51%	6%

図 5 アカウントの乗っ取りや不正利用被害にあった経験（N=86）

4.2 ケーススタディでの項目毎の学習効果について

3.4 節に述べた項目がケーススタディでどのように変化するかを調べたものを図 6 に示す．図 6 からは，「パスワードの使い回し」と「強いパスワード」に対しての理解は 90%となっている．今回のケーススタディが目指した「パスワードの使いまわしの危険性」については，36%が 95%となり，効果が確認できた．さらに，「Line のアカウント乗っ取り事件」については，事件は知っていたが，どうすればよいか知らなかったが 69%であったものが，ケーススタディ後には 93%に増加している．「リスト型攻撃という言葉」については 8%であったものが 76%となっているが，危険性や乗っ取り事件の理解度が主眼であり，用語の理解より実態が高いので問題はないと考えられる．

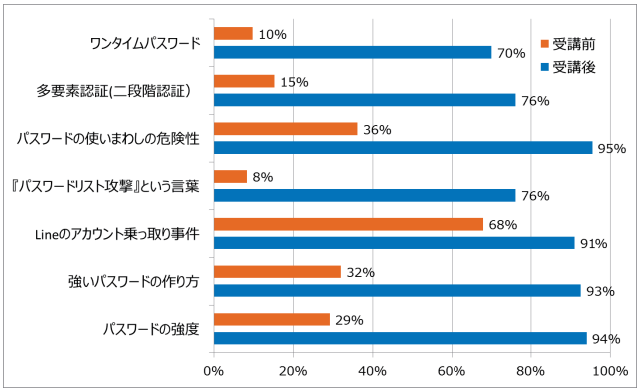

図 6　項目毎の学習効果について（大学生）（N=74）

図 7 は，新入社員に対して同様な調査を実施したものである．社会人の場合，受講前の予備知識が一般の大学生よりも高く，受講後には全ての項目が 100%となっている．これは社会研修の一部として実施したことによっていると言えよう．ただし，「ワンタイムパスワード」や「多要素認証」，「パスワードリスト型攻撃という言葉」については，事前の認知度は低く，今回の学習で認知が高めることができた．

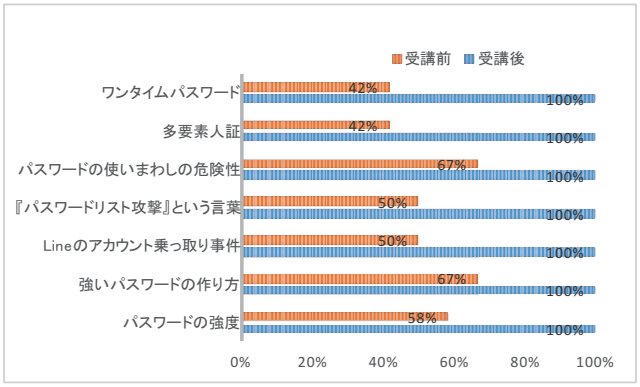

図 7　項目毎の学習効果について（社会人）（N=12）

4.3 ケーススタディによる学習効果の評価

ケーススタディの事前と事後での学習効果を評価した．

受講者によるケーススタディの学習効果について調査した．大学生の学習効果を図 8 に，社会人の学習効果を図 9 に示す．図 8，9 では，ケーススタディの学習効果について配布資料などの内容，ケーススタディの進行における時間配分，ケーススタディでのディスカッションに用いた設問の内容の 3 つの点で聞いている．どの設問項目も，「役に立たない」，「改善の余地あり」，「適切だった」，「友達に勧めたい」の 4 つの観点で調査した．このうち，「適切だった」と「友達に勧めたい」の合計については，学生・社会人ともに 90%を超えておりどちらにとっても適切であったと評価できる．これは，ケーススタディの内容が被験者にとって身近な問題を身につけることができたことから，高い好感度を得られたと結論付けられる．中でも，ケーススタディのあと，ディスカッション形式で意見を交換して内容を深めることや実際のパスワードを作成して意見交換することが高い評価となっていると考えられる．すなわち，ケーススタディでは，ケースを読み，分析し，仲間と議論すること，とくに，パスワードでは，実際に自分のパスワードを考え直すことで理解が深まることを確認できた．

	役に立たない	改善の余地あり	適切だった	友達に勧めたい
配布資料	1%	1%	60%	37%
時間配分	0%	10%	75%	15%
設問内容	0%	7%	68%	25%

図 8　ケーススタディの学習効果について（大学生）（N=74）

	役に立たない	改善の余地あり	適切だった	友達に勧めたい
配布資料	0%	0%	67%	33%
時間配分	0%	8%	75%	17%
設問内容	0%	0%	83%	17%

図 9　ケーススタディの学習効果について（社会人）（N=12）

5. 残された課題について

5.1 リアリティの高い事例と演習の効果

図 10 に昨年の SNS のケーススタディ［1］では，現実問題をベースにしたケーススタディとしたものの，リアリティ面が不足していた．今回のケーススタディでは，リアリティを高めるため，現実に起きた事件をベースとして組み立てた．また，実際にパスワードを作成するという演習を実施した．この結果，SNS のケーススタディよりも今回のパスワードの学習効果を高めることができた．

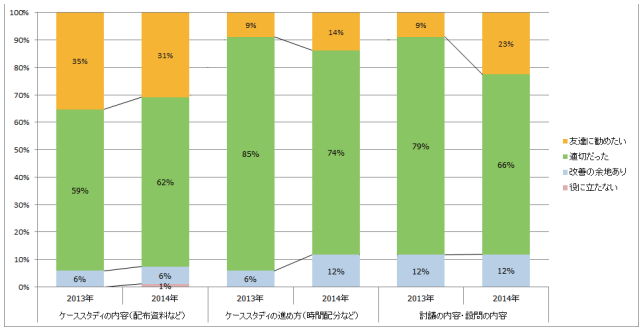

図 10　ケーススタディの比較(2013 年 N=26, 2014 年 N=74)

5.2　ケーススタディの分量

昨年の SNS のケーススタディ［1］では，文章が長く，ケーススタディを実施する対象や制限時間が課題となった．今回は，ストーリの脚色部分を減らして分量を制限した．これによって，ケーススタディへの集中力を持続し飽きさせなくできたと考える．

6.　謝辞

本研究の場を提供いただいた研究と実務融合による高度情報セキュリティ人材育成プログラム（ISSスクエア）及びケーススタディにご協力を頂きました大学及び企業の皆様に感謝いたします．さらに温かい指導を頂いた情報セキュリティ大学院大学の教授，同僚，事務の皆様に感謝いたします．

7.　参考文献

［1］原田ほか，SNS の利用者意識を高めるケーススタディの一考察-リスク意識の啓発プログラムの開発-, 情報処理学会 EIP 研究会第 65 回研究会
［2］総務省，平成 25 年通信利用動向調査，2015 年
［3］総務省情報通信政策研究所，平成 25 年情報通信メディアの利用時間と情報行動に関する調査，2015 年
［4］ 鈴木雅貴, 中山靖司，古原和邦パスワードの使い回しおよび漏えいへの対策の検討，ユーザによる安全なパスワード管理を目指して, 日本銀行金融研究所 金融研究 2014. 10 号，2014
［5］野村総合研究所,「利用者登録する商品・サービスを選別する傾向が強まった生活 者と顧客情報の鮮度維持を望む事業者～生活者と事業者を対象とした ID に関する実態調査～」，News Release，2012 年 2 月 8 日
［6］平野　亮・森井昌克，パスワード運用管理に関する考察および提案とその開発，電子情報通信学会技術研究報告，ライフインテリジェンスとオフィス情報システム vol. 111，no. 286，2011 年
［7］ 八城年伸，パスワードの使用に関する意識調査 ―定期的な変更に関する考察 ―，安田女子大学紀要 38，2010 年，187-195
［8］谷津貴久，大学生のパスワード利用状況とその忘却経験，早稲田大学メディアセンタ報告書，2004 年 5 月
［9］ 西本逸郎，Line 乗っ取り事件の真相, 新手詐欺どう防ぐ，日経新聞 Web ニュース，2014/7/16

付録 1　パスワード管理に関するユーザの実態［4］

		トレンドマイクロ［2012］	トレンドマイクロ［2014］	リサーチバンク［2014］	シマンテック［2013］	野村総合研究所［2012］
1 ユーザが利用するウェブサービスのうち,「パスワード認証」を行うサービスの数	1~4 個	平均 14	—	—	26%	平均 19
	5~9 個				29%	
	10~19 個				24%	
	20 個以上				10%	
	把握せず				11%	
自分が記憶できるパスワードの個数	0 個	—	—	—	6%	平均 3
	1 個				12%	
	2~3 個				52%	
	4~5 個				19%	
	6 個以上				11%	
全サービスで使用するパスワードの個数	1 個	14%	16%	16%	15%	—
	2~3 個	55%	56%	50%	47%	
	4~5 個	17%	12%	21%（4 個以上）	8%（4 個以上）	
	6 個以上	5%	9%			
	全て異なる	8%	7%	13%	29%	
パスワードに利用する文字種 (*1)	1 種類	13%	—	11%	—	—
	2 種類	67%		74%		
	3 種類	14%		15%（3 種類以上）		
	4 種類	7%				
パスワードの文字数	4~5 文字	2%	—	2%	—	—
	6~7 文字	24%		23%		
	8~9 文字	55%		56%		
	10~15 文字	17%		17%		
	16 文字以上	2%		3%		
パスワードの管理方法 (*2)	記憶する	44%	37%	41%	56%	—
	紙にメモ	35%	44%	41%	36%	
	ファイルで PC 等に保存	23% (*3)	33% (*4)	22%	17%	
	ウェブブラウザに保存	5%	6%	19%	9%	
	パスワード管理ツール（専用ツール／サービス）	3%	4%	5%	7%	
	メールで保存	6%	5%	—	3%	

付録 2　情報セキュリティケーススタディ

0　事件のはじまり

専門学校の授業がない土曜日の昼間．

昼飯を食べ終わって特にやることもないので，自室のベッドに寝転んで何か面白いネタでもないかとスマホをいじっていると，学校の友人ケンタから SNS でメッセージが送られてきた．

「へぇ，意外だな．アイツってボランティアなんかやっていたのか. そんなことやるようなヤツには見えないけどな. まあ，バイト代が入ったところだから 3, 000 円くらいなら協力しても別にいいけどさ.」

しかし，頭の中で何かが引っかかった．

ケンタとはいつも学校で会っているから大抵の場合は直接か電話で話すし，面倒くさがりなアイツがボランティアをやるとか，受信専用だとか言ってた SNS でメッセージを送ってくること自体が珍しいな.

「・・・ちょっと，電話を掛けてみるか.」

1　第一の事件

（1）友人からの突然の電話

ケンタはビジネス系の専門学校の 1 年生．ごく普通の学生だ. パソコンは学校の授業で使うために持ってはいるが，

Vol.2015-DPS-164 No.2
Vol.2015-EIP-69 No.2
2015/9/10

普段はスマートフォンで十分用事が済んでいる．むしろ，スマートフォンは生活の一部として無くてはならないものだった．とはいえ，基本的に面倒くさがりなので，日々 Twitter でつぶやくようなマメさはなく，主に Web サイトなどの情報の読み手だった．

ある日，友人から突然電話でこう切り出された．

「お前から変なメッセージ来たけど，本当にお前が送ってきたのか？」

？？？　何の話だか分からない．

「コンビニに行って，電子マネーのプリペイドカード買えっていう内容なんだけど．」

身に覚えのない内容だ．送った覚えもない．確認しようと思い，SNS を見てみようとスマートフォンを手に取った．しかし，SNS にアクセスができない！

「どういうことだ？・・・」　訳が分からなかった．

友人に SNS の文面を確認したところ，こんな内容だった．

> 「突然で申し訳ないんだけど，募金に協力して欲しいんだ」
> 「実は，最近ボランティア活動やってるんだけど，支援している難病の子供で重い心臓病の中学生の女の子がいて，心臓移植しないとあと 1 年もたないんだよ・・」
> 「手術費がすごく高いから募金活動をしてるんだけど，なかなか募金が集まらなくて」
> 「1 口 1000 円で，できれば 3 口以上協力してもらえるとありがたいんだけど，難しかったら 1 口でもいいからお願いできないかな」
> 「コンビニで電子マネーが買えるから，それを買って，番号を送ってもらうのが一番手軽だし，集金も手間が無くていいんだけど・・」

驚いた．全く身に覚えがない内容だった．

（2）他の友人の反応と被害の発生

「募金が集まってる？」

「お前，なんか怪しい商売でもやってるのか！」

「インターネットバンキングで送るから，振込先の口座番号を教えろよ．」

「重い心臓病の中学生の女の子の情報をもっと kwsk．」

「知り合い相手の SNS じゃなくて，インターネット掲示板とかで募集した方が早くない？」

「ワイドショーでやっていた SNS 詐欺に似ているけど，まさかね．」

「どれくらい金が不足しているのか知らせろよ．」

「何で電子マネー？わざわざコンビニで買ってくるのは面倒だから，学校で現金で渡したらダメかな．」

「金欠だからチョット待ってくれないかな．」

こんな感じで，結局 10 人以上の友達から連絡があった．俺になりすました突然のメッセージにもかかわらず，意外と協力的な内容の連絡が多くて驚いた．俺って人望があるのかも，って思うとちょっと気分が良かった．

とりあえず，SNS が使えなくなったので，メールアドレスのわかる友達には，SNS がおかしい，メッセージは俺が送ってないという説明を送っておいた．

すると，メールを送った一人，学校の後輩から電話がかかってきた．

「俺，電子マネー送っちゃいましたよ．ケンタ先輩が俺を頼ってくるなんて，募金が集まらなくてよっぽど困ってるんだと思って，少しでも力になれればって思って・・・．」

しばらくして，ネットで同じようなメッセージを送られた人の話が話題になった．どうやら SNS のアカウントが乗っ取られ，詐欺に利用されたらしい．とりあえず，警察に相談することにした．

俺　:「すいません，自分のアカウントが乗っ取られて，友達が被害に遭ってるんですが．」

警察:(アカウントが乗っ取られる？　おっ！今朝ニュースで観たやつだな．)

「わかりました．事情聴取のため，家族の方と，学校に連絡させて頂きますが，よろしいですね．」

俺　:「はい，わかりました．」

(みんなに迷惑かけて悪いな．親父にも怒られそうだ・・・)

たまたま，警察の人もニュースを知っていてくれたから，事情聴取は案外スムーズだった．しかし状況だけみると，SNS でのやりとりだけだと俺が詐欺を働いていて，被害者のフリをしていると疑われ，犯人扱いされてもおかしくなかった．本当に危ないところだった．

俺のために金を無駄遣いさせた後輩には申し訳ない思いでいっぱいだった．何かで穴埋めしないといけないな･･･．

（3）更なる被害

乗っ取られたアカウントは SNS の運営会社に連絡してすぐに停止してもらったので，これ以上の被害は無いと安心していた．しかし，実は被害は他にもあったのだ．乗っ取られたアカウントを利用して，SNS 内のゲームアプリがダウンロードされ，そのアプリ内で有料アイテムを購入されていた．俺はこの SNS ではクレジットカードを登録しておらず，コンビニで買うプリペイドカードで 1000 円だけチャージしたことがあった．そのチャージ残額全額が有料アイテムの購入に充てられ，アイテムは知らないアカウントに贈られていたのだ．

このゲーム内のアイテムはオークションなどで売り買いされている．表面上は禁止されているが，実際には結構行われているようだ．こうした方法で現金を得るためにアイテムを購入したのだろう．

結局，数百円とはいえ，この分は泣き寝入りになってしまった．クレジットカードを登録していたらどれだけの被害になったかと考えると恐ろしかった．

Vol.2015-DPS-164 No.2
Vol.2015-EIP-69 No.2
2015/9/10

（４）　先輩の指導

事件後，インターネット関連の企業に就職した先輩と久しぶりに会った．先輩はユーザーからの問い合わせ対応などを行う，ユーザーサポートの部署に配属されていた．

俺　:「アカウントの乗っ取りに遭って，実際に後輩が詐欺の被害にあったり，警察に事情を聴かれたりして，大変でしたよ.」

先輩:「パスワードは何ケタだった？」

俺　:「４ケタでしたけど.」

先輩:「はぁ？４ケタのパスワードなんて，今の技術ならすぐに破られちゃうよ.」

俺　:「えっ，そうなんですか？だって銀行のキャッシュカードは４ケタじゃないですか.」

先輩:「キャッシュカードを悪用しようとしたら，カード自体を入手して，ATM でパスワードを入れなきゃならないよね．通常，他人のカードの入手は難しいだろ．ATM も機械としての安全性は高い．そこで，パスワード入力を３回ぐらい連続して間違うと口座自体がロックする仕組みになっている．だから４ケタでも十分安全なんだよ．

インターネットのアカウントへの攻撃だと，カードのように物理的に必要なものはない．そして，世界中どこからでも攻撃が可能だ．連続して間違うとロックする方法が採られているものも多いが，何らかの抜け道があることも珍しくない．だから，総当たり攻撃が成功する可能性はキャッシュカードよりずっと高いんだよ.」

俺　:「なるほど，世界中から狙われているってことですね.」

先輩:「Web のログイン画面に，こんな↓画像が出ていることがあるだろう？」

俺　:「あります，あります．ＩＤ，パスワードだけじゃなくて，この文字も入力しろってやつですよね．結構読みにくいのが多くて，面倒なんですけど.」

先輩:「これは『CAPTCHA』って言うんだ．人が見れば分かるけど，Web サイトを自動で攻撃するコンピュータには認識できないような文字列を表示し入力させることで，攻撃を防いでいるんだ.」

俺　:「世界中から狙われるからこそ，こういう対策が必要なのか．これがあるサイトはセキュリティに気を配っているってことだから面倒臭がっちゃいけないですね．

ところで，パスワードは何ケタぐらいだと安全なんですか？」

先輩:「最低８ケタと言われていたけど，最近は 10 ケタから 12 ケタぐらいは必要だろうね．それに，数字だけとか，英小文字だけだと破られ易いんだ．英大文字，英小文字，数字，記号を混ぜて 12 文字ぐらいにしておかない最近は安心じゃないね．それと，辞書に載っているような意味のある文字にしちゃ駄目だよ．攻撃する側は意味のある文字列を登録した『辞書』を使って自動で攻撃するから危ないぜ．名前に誕生日繋げた”Kenta0515”みたいなのはダメだね.」

俺　:「今回乗っ取られたパスワードは数字４ケタでした…．ダメダメですね．

でも長いと覚えてられないと思うんですけど」

先輩:「人名とか地名とか辞書に載っているような言葉そのものはダメだけど，覚えやすい語を細工してパスワードを作る方法はあるよ．例えば「yokohama」は地名そのものだから危険だ．でも，ここから母音(a,i,u,e,o)を抜いた「ykhm」は辞書には載ってないから各段に安全だ．「横浜市神奈川区鶴屋町」って住所から「ykhmshkngwktsrych」なんて文字列を作れば，十分に長くてランダムな文字列が簡単に作れるだろ？

子音だけだと使う文字が限られるから，一部分だけは母音を入れてみるなんてことをすれば更に安全だ．例えば，最初の 1 文字だけは母音も入れるとかね.」

俺　:「ほー,そんな方法もあるんですね.考えてみます.」

先輩:「最後におまけ．パスワードを忘れたときのために『秘密の質問』を設定させる Web サイトもあるだろ？「母親の旧姓は？」とか「ペットの名前は？」とか．あれに本当のことをセットするのも危険だからやめたほうがいい．身内には無意味だし，SNS なんかで書いた内容からバレちゃうこともあるから.」

俺　:「そう言われれば，そうですね(^_^;) 」

先輩の指導を受けて，俺は 12 ケタのパスワードを作った．英小文字，英大文字，数字に加えた．記号として「.」も入れた．サイトによっては，パスワードが８ケタまでのサイトや記号を受け付けないサイトもあって，結局一つのパスワードでは済まなかったが，基本的には「記号あり」「記号なし」の２種類を用意し，８ケタのサイトには先頭８文字を入れるようにした．

色々あったけど，ひとまずこれで安心だ．

２　第二の事件

（１）ポイントが無くなった！

第一の事件から，数か月たったある日のことだった．コンビニやファーストフード，ネットショッピングでも貯まるポイントカード『ぽいんた』のポイントが突然無くなったのだ．頑張って 2000 円以上貯めていたハズだった．それが，今日コンビニで買い物をして，レシートを確認したら，端数しか残っていない．

「どういうことだ・・・．先週買い物したときは確かにあったのに」

誰か，俺のカードを持ち出して使い込んだのか？いや，それならご丁寧にカードを戻さないだろう．俺の勘違いだろうか？

判然としないまま時が経った．

（2）ショッピングサイトでの不正利用

『ぽいんた』の一件の翌日のことだった．

「あんた，何買ったの！」

俺は家に帰るなり，母親に怒鳴られた．何の話かさっぱり分からない．母親はスマホの画面を俺の目の前に突き出した．クレジットカード会社からのカード利用を知らせるメールだ．俺はまだ学生なので自分のクレジットカードは持たないようにしているが，どうしても必要な場合のために家族カードを所持している．母親はクレジットカードの利用があるとメールで通知される設定をしていた．どうやら，身に覚えのない内容でメールが来たということのようだった．

俺：「何？忙しいから後にして．」
（母親に後ろから襟をつかまれて）
母：「待ちなさいよ！」
俺：「はぁ！？俺じゃないって．最近クレジットカード持ち歩いてないし．親父じゃない？」
母：「この『ナイル』ってネットのお店でしょ？うちでここの会員なのあんただけじゃない！１０万円なんて何買ったのよ！」
俺：「１０万円！！そんな大金，使うわけないだろ．知らないって．第一，俺最近『ナイル』使ってねーし･･･」

そうは言ったものの，俺は不安になって，確認のため『ナイル』にログインしようとしたが，パスワードが違うと表示され，ログインすることができなかった．

ナイルで買い物をしたときはメールが来ているはずだ．過去のメールを確認してみた．俺がダイレクトメールだと思って確認し忘れていたメールの中にそれはあった．

「購入商品：ナイル・ギフトカード　１０万円」

『ナイル』のギフトカードはｅメールで番号が送られるだけで実際に紙のカードが発行されるものではない．送り先のメールアドレスが書かれていたが見覚えのないアドレス．誰かが勝手に俺のアカウントにログインして，ギフトカードを購入したのは明らかだった．

でも，なぜ？どうやって？

10 万円といえば，俺のクレジットカードの使用限度額だ．限度額いっぱいまでギフトカードを購入されたのだ．

直ぐにナイルに直接電話をして，事情を説明した．併せて，クレジットカード会社には，不正使用だとして手続きをした．被害届も出さなきゃならないので，また警察に行った．

警察：「はい，どうしました？　　ん？君，先月も来なかったか？」
俺　：「毎度すいません．今度はネットで僕のクレジットカードが勝手に使われたようで」
警察：「何度も被害に遭うなんて，パスワードの管理とかちゃんとしてないんじゃないか？」
俺　：「知り合いに指導してもらって，安全なパスワードにしたんですけどねぇ・・・」
警察：「まぁ，そう言っても，被害に遭ったんだから，安全じゃなかったんだろうねぇ．」
（ところで，うちの娘は大丈夫かな．）

そう言われても，先輩のいう通りに作ったパスワードは十分に安全だったはずだ．それなのに，どうして不正利用されたんだろう？

そうだ！ナイル内部の不正事件に違いない，俺は絶対悪くないぞ！！

3　全容解明

事件の数日後，ナイルからメールがあった．

『先日，当サイトに対して，大量の不正アクセスの試みがあり，貴方の ID に不正なログインが行われた可能性があったことが確認されました．なお，今回の不正ログインに使われた ID やパスワードは，他社のサービスから流出したものである可能性があります．』

ネット上はこの件に関するニュースで盛り上がっていた．どうやら『ナイル』で不正利用された人で『ぽいんた』のポイントが無くなった人が複数いるようだった！

被害にあった人は皆，「パスワードの使いまわし」をしていたことが分かった．つまり，同じパスワードを複数のサイトで利用していたのだ．まさに俺もそうだった．

実は，少し前によく利用していた Web 情報サイトで『値段ドットコム』というがあった．商品の安売り情報や口コミを載せるサイトだった．他のサイトを使うようになったため，この最近は利用していなかったサイトだ．その『値段ドットコム』で情報漏えい事件があったのだ．何者から

のサイバー攻撃により,ID,パスワードの情報が持ち出されたという.

どうやら，この『値段ドットコム』から ID,パスワードを持ち出した犯人が，同じ ID,パスワードで主要な Web サイトに対してログインを試みていたということのようだ.

『値段ドットコム』から持ち出された ID,パスワードは約 1 万人分だった.『値段ドットコム』はメールアドレスを ID として利用するサイトだった．ショッピングサイト『ナイル』も，ポイントカード『ぽいんた』のサイトも同じく ID にメールアドレスを利用するサイトだった.俺が同じパスワードを利用していたため，不正ログインができてしまったのだ．また,『ぽいんた』では，ポイントを銀行振り込みで現金に換えられるサービスがあった．俺のポイントも換金されてしまっていたのだ.

他に同じ ID,パスワードを利用していた Web サイトはあったが，たまたま犯人の攻撃対象にならなかったようだ．攻撃されていたら更に被害が広がっていたのは明らかだった．想像するだけで怖かった.

また，俺のメールのパスワードは，使える文字の制限があったため，たまたま別のパスワードにしていたが，被害を受けた人の中には，メールのパスワードも同じだったために，メールボックスのダイレクトメールから登録先サイトを調べられ，被害を受けたケースもあったようだった.

4　先輩との再会

俺は直ぐに先輩に電話した.

俺　:「ひどい目に遭いましたよ！10 万円ですよ！あとポイント 2000 円も！！
先輩が『パスワードを使いまわすな』って言ってくれればこんな目に合わずに済んだのに！」

先輩:「同情はするけど，いまどき同じパスワード使いまわすやつがいけないとしか言えないな．うちの会社の Web サイトでも同じような攻撃が増えているよ.弱いパスワードを探すために,『ランダムにパスワードを探る攻撃』は今でもある．だが最近は，入手した ID,パスワードの組み合わせが『どこかの Web サイトで使われていないか探る攻撃』に移ってきている.『パスワードリスト攻撃』って言うんだ.」

俺　:「攻撃を防ぐにはどうすればいいんですか？」

先輩:「Web サイトごとに違うパスワードを使うことだね.」

俺　:「そんなに沢山のパスワード，覚えられないですよ.」

先輩:「忘れないようにメモするのがいいだろうね.」

俺　:「え，パスワードはメモするなって言われてませんでしたっけ？」

先輩:「昔はね．今はメモすることは必ずしも悪いとはされていない．でもそのメモが漏えいすると危ないのは間違いない．だから，メモしたファイルを暗号化しておくとか．紙の手帳にメモするのも，漏えいの危険性が少ないから一案だよね.」

俺　:「なんか，時代が戻っている感じですね.」

先輩:「紙を管理するのは，意外と楽だしね．紙はウイルスで被害を受けることもない．但し，そのものズバリを書いておくのは，さすがにおススメしないな．一部だけメモしておいて，一部は覚えておくのが安全だろうね」

俺　:「そんなに器用に覚えられないですよ」

先輩:「『使いまわし』をすればいいんだ．同じパスワードを使いまわすのはマズいけど，パスワードの『一部』を使いまわすのは問題ない．サイトごとに全く違うパスワードを覚えるのは難しいだろ？ だから，共通する部分を作ってそれを使いまわす．そして，それは覚えておくんだ.

共通部分以外は Web サイトごとに変える必要があるけど，これもサイト名などから一定のルールで作るようにしておけば簡単に作れる.

例えば,『ナイル』の URL，www.nilejp.com だったら，nilejp の 2 文字目から 3 文字を取って”ile”を使う,といった感じだ.ルールを覚えておけば，実際のサイト別の部分もメモしなくて大丈夫だろ？ 共通部分とサイト別の部分を『.』などの記号で繋ぐといった方法もいいだろう.

サイトによって,使える文字や長さなどが違うけど,例えば英大文字が必要なら,『サイト別の部分の 2 文字目を大文字にする』といったルールを自分で作るのがいいだろう．そして，どのサイトでどの文字種を使ったか分からなくならないように『ナイル：英大文字』といった内容をメモする，というようにメモの残し方のルールも作っておこう．大事なのは，そのメモを他人が見て分からないことだよ.」

俺　:「う～ん，難しそうだけど，試してみます」

先輩:「それと,最近は『多要素認証』というのもある.」

俺　:「『たようそ・・』．それって何ですか？」

先輩:「例えば，登録済みのスマートフォンからは ID とパスワードだけでアクセスできる．しかし，それ以外からのアクセスの場合はスマートフォンに SMS や e メールで一度だけ利用できるパスワード,ワンタイムパスワードを送り,それを入力しないとログインできない，という方法だ．最近は大手のポータルサイトなどを中心に採用が増えているから,これが利用できるサイトでは積極的に利用した方がいいぞ」

Vol.2015-DPS-164 No.2
Vol.2015-EIP-69 No.2
2015/9/10

俺　:「そういえば,俺の使っている検索サイト『ばぶぅ』でそんな案内があったのを思い出しました.面倒臭いから，無視してましたけど.」
先輩:「『ばぶぅ』だと，SMS や e メール以外にも，ワンタイムパスワードを表示してくれるスマートフォン用アプリもあるよ．簡単だから一度確認してみな.」
俺　:「分かりました．確認してみます.」

先輩が，最初に相談したときに教えてくれていれば良かったのに,と思いながらも,二度と被害に会わないように,サイト別に違ったパスワードに黙々と変更した.

『ばぶぅ』には，先輩の言うとおり，ワンタイムパスワードの設定があった．せっかくなので有効にしてみた．普段，スマートフォンからしかアクセスしないので，使い勝手は何も変わらなかった．こんなに簡単で安全になるなら早く有効にしておけばよかった.

５　犯人の姿

ある町では市場が開催されにぎやかな日曜日だった.
その町の一角にあるビルのうす暗い地下室で,数台の PC が稼働していた.
メールアドレスを ID にしているある通販サイトに対して,ID とパスワードが自動入力され，ログインが試みられていた.

数分すると一台のコンピューターの画面が点滅した．部屋の片隅でじっとしていた男が「ビンゴ」と言いながら近寄り，ナイルのギフトカードをあるメールアドレスに送信し，すぐに追跡されないようにパスワードを変更した.

他の通販サイトにも同じ ID,パスワードを使ったログインの試みが続けられた.他のサイトでもヒットするたびに,ポイントを引き出したり，換金性の高い商品の購入などが行われ，ものの数分のうちに数十万円分が引き出されていた.

男は携帯を取り，電話を掛けた.
「ああ，俺だ．仕事ができたぞ．いつものように，コンビニ受け取りで商品を送った．今回の名義は『横浜太郎』宛てだ．明日には届くから，商品を受け取って，例の店に来てくれ．バイト代は商品と引き換えだ．念のため，この間渡しておいた偽造健康保険証を持っていけ．間違って他の名義の保険証を持っていくなよ.」
男は電話を切ると，次の『獲物』の処理に取り掛かった.