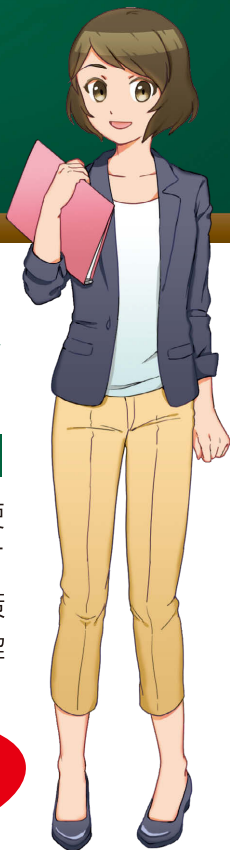


# 新入社員と学ぶ オフィスの 情報セキュリティ 入門

元NTTデータ ITサービスマネージャ  
沢渡あまね 著

NTTデータ セキュリティスペシャリスト  
山田達司 著



**情報漏洩**などトラブルの8割は  
というっかりの**ヒューマンエラー**!

小説+実践解説で学べる情報セキュリティ

システム上で強固なセキュリティ対策をしても、使う側のミスで情報漏洩は起きます。本書は「非」IT部門のワーカーを対象に、情報セキュリティ対策を解説します。新入社員が奮闘する物語+実践解説のハイブリッド型で実践を学べます。

情報セキュリティの  
スペシャリストが  
教えます!

IT依存が高まる一方、そのリスクも増えてきています。標的型攻撃・マルウェア・メール誤送信・なりすまし・ランサムウェア：常に新たな情報セキュリティリスクやセキュリティインシデントが発生し、新聞紙面を賑わしています。つい最近も、大手旅行代理店の顧客情報漏洩のインシデントが報じられました。私たちは、もはやどんな業種・職種であっても、情報セキュリティに無関心ではいられません。

この本は、オフィスのセキュリティ対策業務プロセス改善の専門家である沢渡あまねと、セキュリティスペシャリストの山田達司がタッグを組んで書きました。NTTデータ出身者と現職NTTデータの専門家。現場を知り尽くした2人が、世の中で実際に起こったインシデントをもとにした「ものがたり」と「解説」を通じて、あなたの職場でできること・すべきことをお伝えします。

(「はじめに」より抜粋)

## C&R研究所について

C&R研究所は新潟市にある出版社です。ユニークな社風や教育方針は新聞やテレビなどで紹介されたりします。詳細については、次のWebサイトでご覧いただくことができます。

**[www.c-r.com](http://www.c-r.com)**

また、新潟本社には2代目会社犬「ラッキー」がいます。名刺を持つ正式な社員として広報部に勤務しつつ、セラピードッグとして社内のメンタルヘルスにも貢献しています。

●会社犬「ラッキー」



# 新入社員と学ぶ オフィスの 情報セキュリティ 入門

元NTTデータ ITサービスマネージャ  
沢渡あまね 著  
NTTデータ セキュリティスペシャリスト  
山田達司 著



## ■ 本書について

- 本書は2016年7月現在の情報で記述されています。
- 本書は著者・編集者が実際に調査した結果を慎重に検討し、著述・編集しています。ただし、本書の記述内容に関わる運用結果にまつわるあらゆる損害・障害につきましては、責任を負いませんのであらかじめご了承ください。
- 本書の「ものがたり」は、企業や自治体の職場で実際に起こった出来事をもとにして作られたフィクションです。「ものがたり」に登場する団体・人物などの名称はすべて架空のもので、実在の人物・団体とは一切関係ありません。

はじめに「非」情報システム部門の人たちのための、情報セキュリティの教科書、できました！」

「セキュリティ対策ねえ…。いや、やらなくてはいけなのはわかっているですよ。でもね、どこから手をつければいいのか。どこまでやればいいのか…」

最近、営業・開発・購買・広報など、「IT部門ではない」部署の責任者や管理職、あるいは経営者からたいへんよく聞くセンテンスです。

いまや、私たちの仕事はIT、およびITを使った情報なしには成り立ちません。おそらく、ITを利用しない日は限りなくゼロに近いでしょう。

IT依存が高まる一方、そのリスクも増えてきています。標的型攻撃・マルウェア・メール誤送信・なりすまし・ランサムウェア：常に新たな情報セキュリティリスクやセキュリティインシデントが発生し、新聞紙面を賑わしています。つい最近も、大手旅行代理店の顧客情報漏洩のインシデントが報じられました。私たちは、もはやどんな業種・職種であっても、情報セキュリティに無関心ではいられません。

「大丈夫。うちはITにお金をかけて、最新のセキュリティ対策をしているから」

「セキュリティ？ 情報システム部に任せておけばいいんだ。我々、素人がどうこうする問題ではない」

こうおっしゃる方もいます。しかし、果たしてそれで万全と言えるでしょうか？ 情報シス

テム部門の問題で片付けてしまつてよいのでしょうか？

もちろん、セキュリティを守る技術は日々進化しています。しかし、その速度以上に新たな脅威が現われ続けています。もはや、イタチごつこと言つても過言ではありません。また、敵はちよつとした隙（脆弱性）「セキュリティホール」などと言います）を突いて私たちを攻撃してきます。どんなに高価なセキュリティ対策を施したところで、安心とは言えないのです。

さらにもう1つ。セキュリティインシデントの多くは、実は「ヒューマン（人）」の部分や「アナログ（非IT）」の部分で起こっています。

日本ネットワークセキュリティ協会（JNSA）の調査によると、個人情報漏洩事故の8割以上は、なんと誤操作、管理ミス、紛失・置忘れなどのヒューマンエラーやアナログの部分に起因しているのです。

情報システム部門がシステムの対策はしていた、しかし、情報システムを使う人、すなわちユーザーの「ついうっかり」のヒューマンエラー（たとえば、メール誤送信）で機密情報をばらま

てしまった。あるいは、会話、印刷物などアナログな部分で情報を盗まれてしまった。これが実態なのです。

加えて、標的型攻撃などの新たなリスクも世間を賑わせつつあります。

ビジネスメールを装ったメールを社員が受信し、添付ファイルをクリックしたら知らないうちにPCがマルウェアに感染していた。そのPCを経由してサーバーに侵入され、個人情報報を抜き取られていた。最近、増えてきているケースです。敵は通常やり取りするようなビジネスメールを装っているため、IT面のセキュリティ対策では防ぎにくい特徴があります。そうは言っても、「メールを使うな」「不審なメールを開くな」。これもなかなか現実的ではありません。電子メールはわたしたちのビジネスに欠かせないコミュニケーション手段ですし、それが不審かどうかの判断も難しいです（敵は「不審でないビジネスメール」を装っていますから）。もちろん、知識とある程度の訓練により未然に感染を防ぐことは可能です。さりとて、100%の防止効果があるとは言い難いでしょう。私たちは、標的型攻撃にやられることを前提に、「いかに早く気付くか?」「どうやって被害の拡大を防ぐか?」を考え、組織の行動習慣として定着させる必要があります。

情報セキュリティは、いまや情報システム部門に何とかしてもらえばいいのではない。「非」

情報システム部門の取り組みこそ重要です。ある映画の有名なセリフを借りるなら、「(セキュリティ)事件はIT部門で起きてるんじゃない、現場で起きてるんだ!」といったところでしょうか。

本書は、オフィスの現場の管理者やセキュリティ担当者のために生まれました。

オフィスの現場の管理者・担当者に必要なのは、次の2つです。

- 情報セキュリティの基礎知識とリスクを知る
- 「ヒューマン(人)」「アナログ(非IT)」の部分の対策をする

技術による対策だけでは防ぎきれない前提で、情報セキュリティインシデントが：

- ① 起こらないようにするためのルールや仕組み作り
- ② 起こってしまったときの振る舞い方
- ③ 起こさせないようにする環境作り・風土作り

この3つを一緒に考えて、実践しましょう。

この本は、オフィスのセキュリティ対策・業務プロセス改善の専門家である沢渡あまねと、



セキュリティスペシャリストの山田達司がタッグを組んで書きました。

NTTデータ出身者と現職NTTデータの専門家。現場を知り尽くした2人が、世の中で実際に起こったインシデントをもとにした「ものがたり」と「解説」を通じて、あなたの職場でできること・すべきことをお伝えします。

社員がセキュリティインシデントを起こさないために。大切な部下や仲間を加害者・被害者にしてしまわないために。情報セキュリティを主体的にとらえ、身の丈にあった対策を着実に実行していきましょう。

「情報システム部門がやっているから、大丈夫」はあり得ません！

さあ、いよいよものがたりの始まりです。ここからは、新人社員・菊川あやねちゃんにバトンタッチ。ある日突然「情報セキュリティ委員」を命じられた彼女と一緒に、セキュリティ対策を学んで実践しましょう！

2016年7月

沢渡あまね

## 登場人物 紹介



きくがわ  
■菊川 あやね(22歳)

主人公。カナヤ製菓 営業企画部 企画管理チームに勤務する女性社員。4月に入社したばかりの、右も左もわからない新入社員。堅苦しいのが苦手でお菓子会社に就職したのに、与えられた仕事はまさかの情報セキュリティ委員!? モットーは「当たって砕けろ」。



みやこだ しんじ  
■都田 慎次(43歳)

カナヤ製菓 リスク管理部課長。中途入社のベテラン社員。セキュリティスペシャリストの肩書きを持つ、情報セキュリティの専門家。営業企画部と兼務し、あやねを支えて営業企画部の情報セキュリティ対策を行うことに。趣味は映画とジャズ鑑賞。



ふじ こうすけ  
■富士 康介(25歳)

カナヤ製菓 営業企画部の3年目社員。「かったるいな～」が口癖で、ガツガツと仕事をするタイプではない。セキュリティのような堅苦しいものが嫌いで、情報セキュリティ委員のあやねを少し煙たがっている。



はいばら さとし  
■榎原 聡史(23歳)

インターネット系ベンチャー企業、ペガサスフロンティアの新入社員。あやねとは大学時代のサークルの仲間で、学生時代からつるんでよく遊んでいる。



かわつ ひでと  
■河津 秀人(45歳)

カナヤ製菓 営業企画部の課長であやねの上司。入社したてのあやねに、情報セキュリティ委員の重責を与える。温厚な人柄で地味なタイプ。趣味は犬の散歩と卓球。



いわた ちえ  
■磐田 智恵(35歳)

カナヤ製菓 営業企画部の主任。物静かなタイプ。2児の母。子どもが病弱なため、テレワーク(在宅勤務)をしたいと考えている。



しみず ゆい  
■清水 優衣(22歳)

カナヤ製菓 人事部の新入社員。あやねの同期で、内定者懇親会のことからの仲良し。あやねとは対極のおとなしい性格。カナヤ製菓の社員満足度向上が彼女のミッション。



ほそえ ななみ  
■細江 菜々美(24歳)

インターネット系ベンチャー企業、ペガサスフロンティアの3年目社員。サトシと同じ職場の先輩で、理知的で大人な雰囲気を漂わせている。サトシに密かな想いを寄せている？

はじめに	3
登場人物紹介	8



## プロローグ



ミッション

営業企画部の情報セキュリティ対策をしてください！

18

《解説》 オフィスの情報セキュリティとは

23



## 第1章

### 情報セキュリティとは



情報って、情報を守るってどういふこと？

28

《解説》 企業の情報を守るには

33



情報セキュリティの脅威

39

《解説》 情報資産に対するさまざまな脅威	41
❗ 情報セキュリティは誰のため？ ～6者に価値を提供する～	51
《解説》 情報セキュリティは6者に価値を提供する	59
❗ 情報セキュリティに完璧はない！	62
《解説》 リスクのコントロール	63
❗ システム部門任せじゃダメ！ ～オフィス現場で実践すべき3つのこと～	66
《解説》 情報セキュリティ対策におけるオフィスの役割	70
《解説》 3つの情報セキュリティ対策	74
❗ 情報セキュリティの3つの要素(CIA)	77
《解説》 情報セキュリティの3要素CIAとは	79
❗ 電子データの管理方法を見直す	84

## 第2章

# 端末やデバイスとの付き合い方

🔒 PCを管理しよう……………	88
《解説》PC管理のポイント……………	93
🔒 PCにセキュリティパッチをあててもらおう工夫……………	99
🔒 モバイルPCやスマートフォンのリスク……………	103
《解説》ノートPC、スマートフォンの対策……………	104
🔒 便利さの裏には罠があるその1〜出張先での注意点……………	111
🔒 便利さの裏には罠があるその2〜可搬媒体の注意点……………	114
《解説》安全なUSBメモリの使い方……………	116
🔒 部内でセキュリティ意識の向上を促す……………	118
🔒 アカウント管理・パスワード管理……………	121
《解説》アカウント管理のポイント……………	123
🔒 運転士さんがくれたヒント……………	128

## 第 3 章

### 外部の人との付き合い方

🔒	メールに潜むリスクあれこれ……………	130
《解説》	メールの誤送信対策……………	132
《解説》	メールやインターネットに潜む脅威と対策……………	142
🔒	目指せ、セキュリティ災害ゼロ！……………	149
🔒	あたりまえのように出入りする部外者……………	154
🔒	オフィス内のサーバー。これっていいの？……………	156
《解説》	オフィスにおけるアクセス管理……………	158
🔒	苦手なことはプロに任せる！〜外注管理のポイント〜……………	163
《解説》	外注管理のポイント……………	165
🔒	小さな会社のセキュリティの工夫……………	176

## 第4章

## アナログな部分の管理こそ重要

🔒 オフィスの情報セキュリティ対策4つのポイント……………182

《解説》アナログなセキュリティ管理……………188

🔒 フロアの大改造が始まった……………195

《解説》情報のライフサイクルとは……………200

🔒 外での会話にも危険がいっぱい……………203

《解説》外出先の会話に注意……………206

🔒 カフェコーナーがセキュリティリスクを減らす!?……………207

## 第5章

## 多様性（ダイバーシティ）とセキュリティ

🔒 人材の多様性↷転職者、退職者との付き合い方……………216



## 第 6 章

### 「あなた、いったい誰なの？」

《解説》 転職者、退職者対応のポイント …………… 217

働き方の多様性（テレワーク（在宅勤務）との付き合い方）…………… 220

《解説》 テレワークで求められるセキュリティ …………… 222

テレワークが生む意外なメリット …………… 228

《解説》 忍び寄る影 …………… 232

《解説》 なりすましに注意 …………… 238

《解説》 「使い回し」に注意！ …………… 244

## 第7章

### セキュリティを味方につける

それでもセキュリティを守らない社員……………248

セキュリティ強化とコミュニケーション活性は表裏一体……………252

《解説》セキュリティとコミュニケーション・業務効率を  
両立させるオフィスの事例……………255



### エピソード

セキュリティは皆を笑顔にする……………272

おわりに……………276



プロローグ



## ミツシヨン…営業企画部の

## 情報セキュリティ対策をしてください！

とにかく堅苦しいのは苦手だ。

そして、ワクワクすることが大好きだ。

あやねが就職先にカナヤ製菓を選んだのは、そんな単純な理由からだ。大好きなお菓子のことはかり考えて過ごす。想像するだけでワクワクした。公務員や金融機関ははなから考えていなかった。なんだか堅そうだったから。子どもや大人をワクワクさせるような、そんな素敵な商品を生み出したい。世の中をお菓子で笑顔にするんだ！ カツカツカツ——ようやく履き慣れたパンプスの踵が階段にリズムを刻む。期待に胸を膨らませ、あやねは古びたビルの一室のドアを開けた。

目黒川沿いの裏通りの雑居ビル。その4階があやねの勤務先だ。色あせた鉄の扉に、「カナヤ製菓株式会社 営業企画部」の文字が並ぶ。ここ営業企画部は、本社ビルから500メートルほど離れたところにある。完全自社ビルの本社と異なり、他の企業と同居。すぐ上の5階はITベンチャー企業、3階と2階には旅行代理店が入っている。

カナヤ製菓は、東京・五反田に本社を構える創業50年の老舗企業だ。社員数はおよそ300名。お煎餅、ポテトチップ、キャンディーなどの駄菓子から、贈答用の高級菓子まで幅広いラインナップを提供している。「カナヤの票最中」といえば中高年を中心に定評のある、ちょっと気の利いたブランド商品だ。最近では神戸の人気パティシエとコラボしたオシャレなスイーツも手がけている。女性からの人気も高い。

「菊川<sup>きくがわ</sup> あやね 営業企画部勤務を命ずる」

新入社員研修の最終日、辞令を見たあやねは心の中で大きくガッツポーズをした。営業企画部は、新商品のプロモーションやコラボ企画などを仕掛ける部署である。「やった、希望通り！」あやねの胸は高鳴った。ふと顔を上げて周りを見回す。望み叶って歓喜する者、意にそぐわない配属に肩を落とす者。昼下がりの研修室は、歓声とため息が入り混じっていた。そんな中、あやねは瞳をキラキラ輝かせる。ところが…。

「菊川さん。あなたの最初の仕事は、情報セキュリティ委員です。ここ、営業企画部の情報セキュリティを強化してください」

配属後、最初の金曜日。課長の河津かわづに呼ばれ、突然こう告げられた。

——えっ、えっ、えっ……。わたし、新しいお菓子の企画とか、プロモーションとか、そういうお仕事させてもらえるんじゃないんですか？

あやねは耳を疑った。情報とか、ITとか、セキュリティとか……そういうの苦手なんですけど。正面の課長の目を見据えたまま、右手でほつたをつねってみる。うん、痛い。残念ながら夢ではないようだ。河津は淡々と続ける。

「君も新聞やテレビのニュースは見ているでしょう。春野フーズの情報漏洩事件。あれが引き金になってね。社長が『ウチは大丈夫なのか？』って大騒ぎなんだよ」

そのニュースはあやねもよく知っている。冷凍食品メーカーの春野フーズの社員が、顧客リストを不正に外部の業者に販売して逮捕された事件。つい1カ月前まで、どのメディアもその報道で持ちきりだった。そういうえば、入社初日に仰々しい誓約書を書かされたつけ。「業務で知り得た情報は一切口外しません」とか何とか。

河津によると、この事件を受けて社内各部門に情報セキュリティ委員を設置することになったらしい。そして、あやねがめでたく選ばれたとこういうわけだ。

「菊川さんには、営業企画部のセキュリティ対策を考えて実施してもらいたい」

河津は身を乗り出す。チャコールグレーのスーツが、窓から差し込む夕陽を浴びて淡く光った。「見ての通り、ウチの部署はだらしがないところがあつてね。本社ビルから離れているせいもあつ

てか、緊張感が足りないのかもしれないけれど…」

そう言われても「はい」とは答えづらい。配属になってまだ4日しか経っていないし、そもそもの職場を知らないので比較のしようがない。河津は構わず続ける。

「でも、何でよりによって新人のわたしなんですか？」

あやねは率直に聞いてみた。ようやく営業企画部の人の顔と名前が一致するようになったばかり。そんな自分にセキュリティ対策なんて重責が務まるとは思えない。

「うん。新社員のフレッシュな視点があつたほうがいいと思ってね。引き受けてくれますね？」

河津はフレッシュを強調した。

「は…はい。自信はないですけど…頑張ります」

そう答えるのが精一杯だった。河津は、「じゃ、週明けからよろしく」と残して応接室を出た。あやねは自席に戻り、研修で配られた薄い冊子を手にとった。「情報セキュリティガイドライン」。もらっただけで一度も開いたことがない。仕方なしにバラバラとめくってみる。「私のメールを送ってはいけません」「インターネットを業務外で利用してはいけません」…ごくごく当たり前のフレーズが続く。よろしくと言われたものの、いったいこれから何をどうすればよいのか？　そこで終業を知らせる鐘が鳴った。

帰り道。黄昏の川沿いの通りをとぼとぼ歩く。勢いで頑張りますと答えたものの、それで良かったのか？ 考えてみれば、あやねは細かい管理ごとは大の苦手。昔から大雑把だし、忘れ物が多いし、おっちょこちょいだし、情報セキュリティなんて向いているわけがない。第一、あやねは文学部の卒業でITの知識はこれっぽちもない。河津はフレッシュさを期待してと言っていたが、それにしても自分はフレッシュすぎやしないか？ 会社のこと、右も左もわからない。「わたしには無理です」そう断るべきではなかったのだろうか？

どんよりとした気持ちで、駅へと向かう。桜の花びらがふわり、風に舞いあやねのコートの肩をそつと撫で、やがて地面に沈んだ。





## オフィスの情報セキュリティとは

本書のテーマはオフィスの情報セキュリティです。そもそも情報セキュリティとはどういう意味でしょうか？ なぜ今注目されているのでしょうか？



### セキュリティ、情報セキュリティとは

セキュリティとは、人、建物、財産など、さまざまな価値あるものを害から守ることです。テレビの宣伝で流れているホームセキュリティは住居を泥棒や火事、自然災害から守るものですし、ナショナルセキュリティは外交、軍隊、諜報機関などにより国の安全を守ることです。最近使われるようになったサイバーセキュリティはインターネットなどのサイバー空間をウイルスやハッカー、外国などによる攻撃から守ることですね。

情報セキュリティはその名のとおり、情報を安全に守ることです。オフィスにおける情報セキュリティの目的は企業が保有する紙、電子ファイルなど、さまざまな形をした情報を守ることです（IT系では情報セキュリティのことを単にセキュリティと呼ぶことがあります。本書でもセキュリティは情報セキュリティと同じだと思ってください）。

では、なぜ今情報セキュリティが注目されているのでしょうか？

それは情報が企業活動にとって重要になってきたとともに、情報が多くの危険にさらされるようになったからです。

### 🔑 企業活動にとって情報が重要に

企業の活動を支えるものを経営資源と呼びます。かつて経営資源は「ヒト」(人材)、「モノ」(製品・設備など)、「カネ」(資金)と言われていましたが、最近はこれに情報を加えた「ヒト・モノ・カネ・情報」とする考え方が主流になってきました。かつてはモノが不足しており、企業は同じものを短期間にいかにたくさん作るかを競っていました。今はモノがあふれており、人の好みも多様化しています。企業は多くのニーズに応える多くの製品を作り、それを必要とする人に届けることが重要になってきました。そのためには企画書、生産方法、顧客情

●企業の活動を支える経営資源



報などの情報がより重要になってきたからです。

情報は企業にとって競争力を高め、成長するための重要な資産なのです。

### 情報が多くの危険に

情報が重要になるとともに、情報が不適切に扱われることによる問題も多く発生しています。まず、社内にいる人間により情報が持ち出される事件が発生しています。

2014年、東芝は同社が保有する半導体の研究データを不正に入手したとして、ライバルである韓国企業SKハイニックスを不正競争防止法違反で訴えました。この事件で東芝は1000億円を超える利益を喪失したとしており、最終的に両社は330億円の支払いにより和解しました。

東京三菱UFJ証券ではシステム部の部長代理が借金返済のために、同社の顧客情報149万人分をCD-ROMによって持ち出し、名簿業者に転売しました。この事件により同社は70億円の被害が出たと主張しています。

最近では個人情報の漏洩事件が多数発生し、新聞を賑わせています。2014年、ベネッセでは、同社の顧客である学生と保護者の情報3500万件超がデータベースの運用を行っていた委託先社員により持ち出され、名簿業者へと転売されました。この事件で、ベネッセでは取締役2名が辞職し、利用者へのお詫びとして200億円の原資を準備しました。

さらにウイルス(最近はマルウェアと呼ぶこともあります)も技術的に高度になってきており、ウイルス対策ソフトでは守り切れなくなってきました。

2015年には日本年金機構が標的型攻撃と呼ばれるメールを用いた攻撃を受け、PCがウイルスに感染し、同機構が保有する125万件以上の情報が漏洩しました。日本年金機構は大きな非難を浴び、信頼を失墜してしまいました。

また、N-TT-3による調査では、存在するウイルスのうち、ウイルス対策ソフトで見つけることができるのは40%強に過ぎないとも言われています。残りの60%はウイルス対策ソフトをすり抜けてしまうのです。標的型攻撃で使われるメールはほとんど本物っぽくなってきており、多くの社員がいる会社で標的型攻撃を100%避けるのは不可能だとも言われています。

このように情報セキュリティが守られない場合、企業は大きなダメージを受け、さらに攻撃が激しくなっていることから、情報セキュリティに対する企業の取り組みがより大切になってきているのです。