昨今めまぐるしいスピードで技術革新が進んでいる。こうした技術は社会への恵みを与える一方で、我々は距離ゼロで見えない全世界の攻撃者と対峙していることを改めて認識する必要がある。

# サイバーセキュリティトレンド 2016

NTTソフトウェア

# 目次

# はじめに

昨今、めまぐるしいスピードで技術革新が進んでいる。こうした技術は我々のビジネスや生活にも大きな恵みを与え、経済、社会をより高度で実りあるものへと発展させている。しかしながら、その一方で、サイバー攻撃も日々高度化、悪質化、巧妙化しており、セキュリティ被害の報道が後を絶たない。攻撃者は組織化して綿密な計画、戦略を持って攻撃をしかけてくる。狙われる側も十分な計画、戦略を持って防御しないと太刀打ちできない。インターネットの普及、技術革新は世界の距離を縮め、ビジネススピードを速め、コストを削減する等に大きく貢献しているが、それは攻撃者にとっても同様である。どこへでも、いつでも、速く、安く攻撃できる環境が整っている。我々は距離ゼロで見えない全世界の攻撃者と対峙していることを改めて認識する必要がある。

企業、組織が攻撃を受けると大きな損失を被る。原因究明等の調査や再発防止策の検討費用も相当の額になる。サイバーセキュリティ対策は経営課題である。企業、組織の実態にあった適切な対応が求められる。サイバーセキュリティ対策を検討するにあたって、攻撃を受けてから考えるようでは遅い。攻撃を受ける前提で、事前に対策を打っておく必要がある。そのためには、今後の情報セキュリティ情勢を把握しておく必要がある。

そこで、NTT ソフトウェアでは、サイバーセキュリティトレンドをまとめることとした。PEST（政治、経済、社会、技術）分析によりマクロな情勢を捉え、今後起こりうる変化を読み解き、具体的に発生している特徴的な事例を重ね合わせて、３～５年先の情勢を予見している。是非、経営層の方々にご一読いただきたい。

本書が、企業、組織のサイバーセキュリティ対策を検討する際の一助になれば幸いである。そして、適切なサイバーセキュリティ対策を打つことによって、豊かで健全なサイバー社会に発展していくことを願ってやまない。

2015 年 12 月 1 日
NTT ソフトウェア株式会社
代表取締役社長
山田　伸一

# 1 新たなボーダレス時代が到来し、サイバーフィジカルセキュリティが進化する

インターネットの普及は国を超えたリージョンのボーダレスから、あらゆるモノがつながる新たなボーダレス時代へ導こうとしている。IoT（Internet of Things）の進展は、より豊かで便利なスマート社会、産業振興を実現し、ビジネスやサービスも大きく進化するに違いない。一方で、あらゆるモノがつながることにより、これまでは物理的に守られていた安全な領域でもバーチャルには侵入ができてしまうケースも発生し、セキュリティ対策は益々重要になってくる。サイバー攻撃によって、物理的なモノを制御することも可能となり、場合によっては人命に関わるインシデントも想定しなくてはならない。

デル・ソフトウェアは、ネットワークセキュリティ脅威レポート 2015 の中で、「SCADA（Supervisory Control And Data Acquisition）」システムへの攻撃が倍増している、と発表した[1]。SCADA は、工場や発電所、製油所といった重要インフラで活用されており、装置を制御、データを収集する役目を担っている。これらが攻撃に晒されているということは、社会生活が脅かされているということに他ならない。スマートメータをハッキングして各家庭の電源をシャットダウンすることができると警鐘を鳴らすヨーロッパのセキュリティ研究者もいる[2]。

2015 年 7 月、アメリカのセキュリティ研究者が、無線で車を遠隔操作して、車を乗っ取る実験を披露した[3]（図 1-1）。実験では、米セントルイス市内を時速 112 キロで走行中、突然エアコンが入り、ラジオのボリュームが大音量になって、ワイパーが勝手に作動。そしてアクセルが効かなくなって減速した。ブレーキを効かなくすることも可能という。現在、自動運転車の実用化に向けて全世界で研究開発が進行中であるが、サイバー攻撃によって自動運転車が正しく制御されない事態が発生したら、人命に関わる大きなインシデントにつながってしまう。

出所：https://www.youtube.com/watch?v=MK0SrxBC1xs

**図 1-1．車が遠隔操作される様子**

同じ 2015 年 7 月に、ドローンに拳銃を固定して発砲する映像が公開され、話題を呼んだ[4]。ドローン利用の法規制が整備されようとしているが、一般市民が簡単に購入できるドローンが悪用されれば恐ろしい凶器にもなり得ることをこの映像は示している（図 1-2）。

---

[1] http://japan.zdnet.com/article/35064403/2/

[2] http://www.itpro.co.uk/security/23251/smart-meter-hack-could-leave-homes-in-the-dark

[3] http://www.itmedia.co.jp/enterprise/articles/1507/22/news060.html
https://www.youtube.com/watch?v=MK0SrxBC1xs

[4] http://wired.jp/2015/07/22/drone-fires-gun/　https://www.youtube.com/watch?v=ZIP3wScZwUQ

出所：https://www.youtube.com/watch?v=ZIP3wScZwUQ

**図 1-2. ドローンに取り付けられた拳銃が発砲する様子**

インターネット上に公開されている様々な機器情報をデータベース化し、検索可能にする SHODAN という Web サービスがある[5]（図 1-3）。インターネットに接続している機器を検索できるので便利だが、攻撃者にとっても攻撃対象を検索するのに役立つ。脆弱性が残る古いバージョンの機器なども容易に発見できる。情報処理推進機構（IPA）や JPCERT コーディネーションセンター（JPCERT/CC）は、不必要にインターネットにアクセスしない、またはアクセス制御により特定の対象以外と通信ができないように機器の設定を適切に行う等、その対策を紹介している[6]。

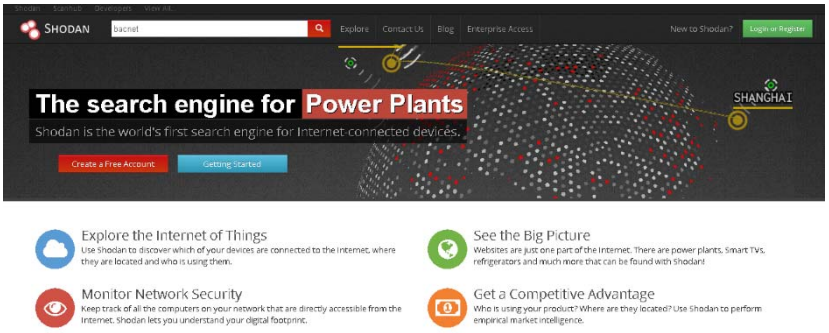



**図 1-3. SHODAN トップページ（https://www.shodan.io/）**

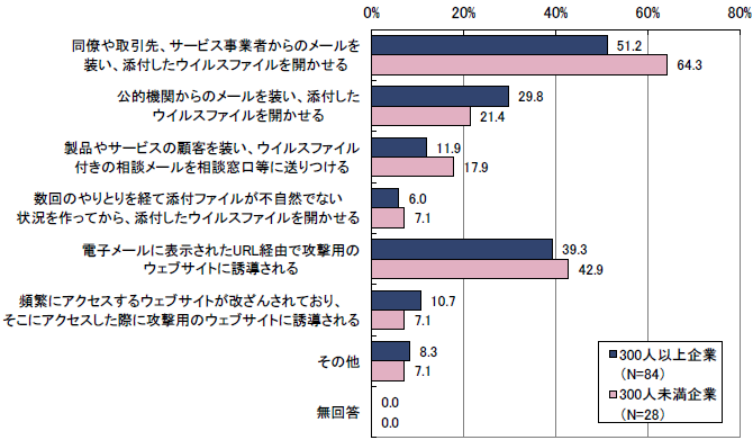
あらゆるモノがつながる新たなボーダレスの時代においては、攻撃者にとってもあらゆるモノへのアクセスや制御を試みることが可能となる。サイバーとフィジカルの境界もなくなる。何がどのように接続されているのかを正しく認識することが重要である。接続口は攻撃者にとっての侵入口にもなっていることを再認識し、全世界の攻撃者が接続口から侵入してくることを前提としたセキュリティ対策が今後必要になってくる。

[5] https://www.shodan.io/

[6] https://www.ipa.go.jp/about/technicalwatch/20140227.html
https://www.jpcert.or.jp/ics/report0609.html

## 2 標的型攻撃が益々深刻化し、サプライチェーンでの対策が求められる

標的型攻撃、特に、日本を標的にした攻撃が近年急増している。IPA の報告によれば、標的型攻撃の手段として最も多いのが、「同僚や取引先、サービス事業者からのメールを装い、添付したウイルスファイルを開かせる」という手口であることが報告されている[7]。規模の小さい企業のほうがその比率が高い（図 2-1）。




出所：IPA「2014 年度 情報セキュリティ事象被害状況調査 －報告書－」（2015 年 1 月）

**図 2-1．標的型攻撃の具体的な手段（従業員規模別）**

2015 年 6 月、日本年金機構で個人情報流出の報道があった。同年 8 月には個人情報流出に至った原因究明調査結果が発表された[8]。攻撃者が執拗に攻撃を仕掛けてくる様子が克明に記されている（表 2-1、図 2-2）。標的型メールを受けた職員のメールアドレス等も盗み取られて、それが次の攻撃にも利用された可能性も排除されない、と報告されている。日頃メールをやりとりするような相手になりすまされ、メール内容も巧妙に仕組まれれば、人間のチェック、注意力だけで攻撃を見分けるのは相当難しい。攻撃者は、狙いを定めた攻撃対象には執拗に攻撃を仕掛けてくる。ひとたびマルウェア等に感染してしまうと、当該マルウェアと攻撃者が気付かれないように通信し合い、じっくりと獲物を探して盗み取られてしまう。攻撃者はさらに盗み取られた情報を使って、次の獲物を狙いに行く。攻撃者は用意周到にセキュリティの弱いところから、じわりじわり攻めてくる。業務プロセスの全般に亘って、セキュリティ対策が必要である。

2013 年 12 月に、4000 万件のクレジットカード情報、7000 万件の個人情報流出被害にあった米ターゲット社への社内サイトに対する最初の侵入には、同社の取引先から盗まれた資格情報が使用されている、と報道されている[9]。ターゲット社は、ファジオ・メカニカル・サービスという空調会

[7] IPA「2014 年度 情報セキュリティ事象被害状況調査 －報告書－」（2015 年 1 月）

[8] サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」（2015 年 8 月 20 日）
日本年金機構不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に調査結果報告について」（2015 年 8 月 20 日）

[9] http://it.impressbm.co.jp/articles/-/11538
http://business.nikkeibp.co.jp/article/opinion/20140604/266189/

社にモニターを委託しており、ウェブサイトで取引会社の 1 社としてファジオの社名を公開していた。攻撃者はファジオの従業員にマルウェアを仕込んだフィッシング・メールを送りつけ、ターゲット社のネットワークへ侵入できる暗証番号を盗んで、マルウェアをターゲット社のシステムに忍び込ませることに成功した、と報道されている。ターゲット社の CEO はこの事件を受けて解任される事態にまで追い込まれた。

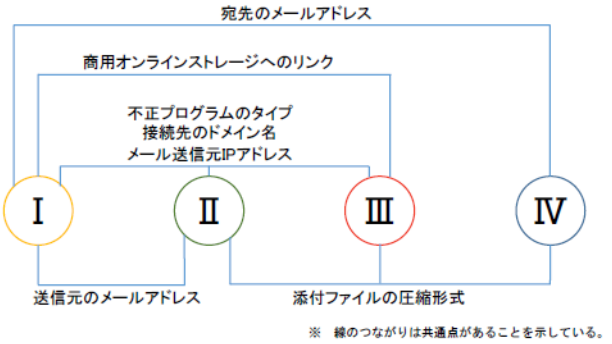
同じ米国で、2015 年 6 月に人事管理局（OPM）がサイバー攻撃を受け、2210 万人の連邦政府職員の個人情報が流出した可能性がある[10]。職員の個人情報を使って特定の職員に同僚のふりをして e メールを送り、偽の URL や添付ファイルを開かせてウイルスを広め、その政府機関のコンピューターシステムに侵入するといった手口が考えられる、と報道されている。

**表 2-1．日本年金機構への不審メール**

出所：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」（2015 年 8 月 20 日）

| 不審メールの番号 | 受信日 | 不審メールの概要 |
|---|---|---|
| Ⅰ | 5月8日(金) | 件名：「厚生年金基金制度の見直しについて(試案)に関する意見」<br>宛先：公開メールアドレス(2)<br>リンク：商用オンラインストレージ |
| Ⅱ | 5月18日(月) | 件名：給付研究委員会オープンセミナーのご案内<br>宛先：非公開の個人メールアドレス(98)<br>添付ファイル：給付研究委員会オープンセミナーのご案内.lzh |
| Ⅲ | 5月18日(月)<br>～<br>5月19日(火) | 件名：厚生年金徴収関係研修資料<br>宛先：非公開の個人メールアドレス(20)<br>添付ファイル：厚生年金徴収関係研修資料(150331厚生年金徴収支援G).lzh(16)<br>リンク：商用オンラインストレージ(4) |
| Ⅳ | 5月20日(水) | 件名：【医療費通知】<br>宛先：公開メールアドレス(3)<br>添付ファイル：医療費通知のお知らせ.lzh |

※　表中の括弧内の数字はメールの件数を表す。




出所：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」（2015 年 8 月 20 日）

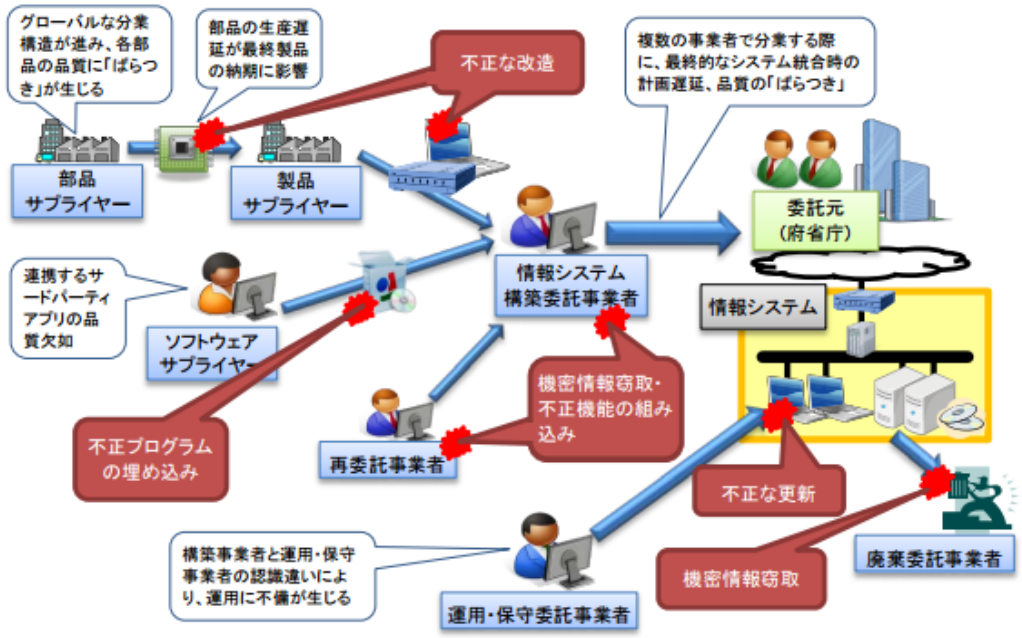
**図 2-2．不審メールの共通点**

日本政府は、府省庁における情報セキュリティ上のサプライチェーン・リスクに対応するための調達仕様書の円滑な作成に資することを目的とした手引書を公開した[11]（図 2-3）。これも、近年のサプライチェーン・リスクへの対応が大きな課題となっていることの表れである。

こうした事例から分かることは、攻撃者は標的に定めた攻撃対象に直接アタックするのではなく、怪しまれることなく獲物に近づく術を練って、周囲からじわじわと着実に攻撃を仕掛けてくる、ということである。ターゲットとなる社員が日頃メールする相手、アクセスする HP 等を入念に調べてセキュリティの弱いところを攻略し、しつこく巧妙に攻めて来る。自らの組織を守るためにも、関連組織、取引先等、ビジネスに深く関わる組織全体でセキュリティレベルを合わせ、対策をとっていくことが今後求められていく。

[10] http://newsphere.jp/world-report/20150608-1/
http://jp.reuters.com/article/2015/07/09/cybersecurity-usa-idJPKCN0PJ2Z920150709

[11] 内閣サイバーセキュリティセンター「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」（2015 年 5 月 21 日）




出所：内閣サイバーセキュリティセンター「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」（2015 年 5 月 21 日）

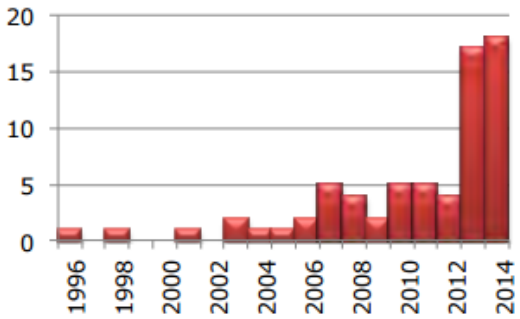
**図 2-3. サプライチェーン・リスクの例**

# 3 業界内/間の連携によるセキュリティ対策が強化される

コンピュータセキュリティに関わるインシデントに対処するための組織（CSIRT[12]）が注目を集めている。インシデント関連情報、脆弱性情報、攻撃予兆情報等を常に収集、分析し、インシデントの未然防止や被害の極小化を図る様々な活動を実施する。昨今、CSIRT を構築する企業が増加しており、セキュリティに関する情報共有、協調、連携強化を目的に設立された日本 CSIRT 協議会[13]への加盟数も急増している（図 3-1、図 3-2）。


出所：http://www.nca.gr.jp/imgs/nca_teams_2014.pdf

**図 3-1. 日本 CSIRT 協議会加盟数**

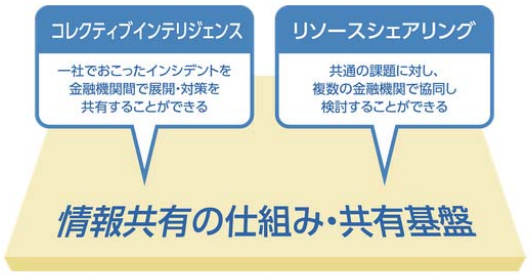



出所：http://www.nca.gr.jp/imgs/nca_teams_2014.pdf

**図 3-2. 日本 CSIRT 協議会加盟組織の設立年**

2014 年 8 月 1 日には、金融機関間のサイバーセキュリティに関する情報を共有するための組織「一般社団法人　金融 ISAC」が設立された[14]（図 3-3）。特に最近サイバー攻撃の標的となっている金融機関において、高度化、巧妙化する攻撃に対して、業界全体で連携して防御していこうという狙いであろう。

セキュリティベンダの連携も加速している。2015 年 7 月 7 日、標的型攻撃対策ソリューションで IBM とトレンドマイクロが協業することを発表した[15]（図 3-4）。また、同日、IIJ とシマンテックも、ログの相関分析、




金融ISACでは会員間でのメーリングリストを通し、日々のインシデントや脆弱性情報等をリアルタイムに共有します。また、特定の重要課題について、テーマごとのワーキンググループ（WG）を設け、会員共同で対策検討等を行いながら、知見と対応力を高めていきます。これらの成果は、ワークショップやアニュアルカンファレンス等の場において共有していきます。

出所：http://www.f-isac.jp/institute/activities.html

**図 3-3. 金融 ISAC**

[12] Computer Security Incident Response Team の略。

[13] http://www.nca.gr.jp

[14] http://www.f-isac.jp/institute/activities.html

[15] http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150701005752.html
http://www-06.ibm.com/jp/press/2015/07/0701.html

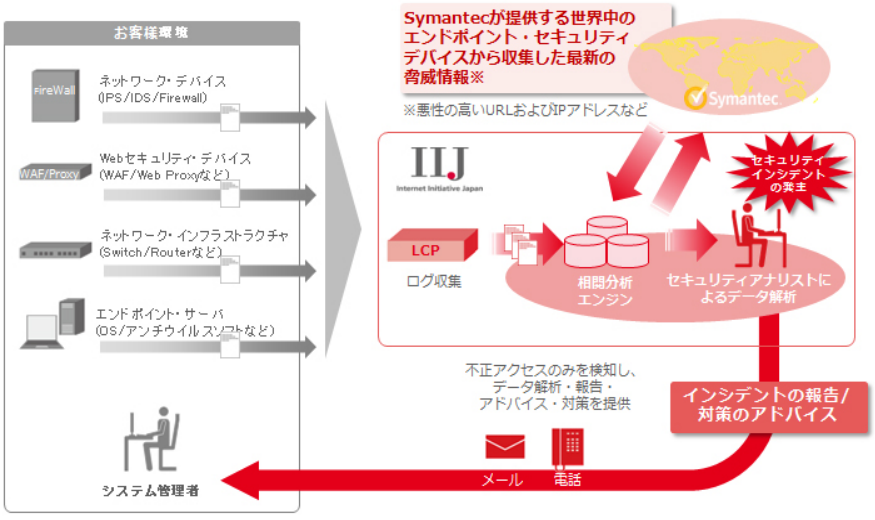
攻撃検知、遮断対応支援で協業すると発表した[16]（図 3-5）。それから 10 日後の 7 月 17 日には、NTT コミュニケーションズが、パロアルトネットワークス社、ブルーコートシステムズ社、デジタルアーツ社の日米大手セキュリティ企業と連携し、標的型攻撃の通信遮断機能を大幅強化すると発表した（図 3-6）[17]。


Copyright（C）2015 Trend Micro Incorporated. All rights reserved.
TRENDMICRO は、トレンドマイクロ株式会社の登録商標です。

出所：http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150701005752.html

**図 3-4. IBM とトレンドマイクロの協業に関するプレスリリース**

攻撃者は、進化する技術を巧みに利用し防御の網を逃れて、標的となる獲物を気付かれないように獲得する。それぞれ果たすべき役割をもった専門化集団の分業、協業による組織化により、益々攻撃が巧妙化、悪質化してくる。高度化するサイバー攻撃に対して、技術やソリューションも包括的に導入して対策していかないと防御できない時代になってくる。




出所：http://www.iij.ad.jp/news/pressrelease/2015/0707.html

**図 3-5. IIJ とシマンテックの協業に関するプレスリリース**

[16] http://www.iij.ad.jp/news/pressrelease/2015/0707.html

[17] http://www.ntt.com/release/monthNEWS/detail/20150717.html


出所：http://www.ntt.com/release/monthNEWS/detail/20150717.html

**図 3-6. NTT コミュニケーションズと日米大手セキュリティ企業 3 社の協業に関するプレスリリース**

特に、IoT セキュリティ分野における業界内/業界間の協業・連携は、今後益々進展していくと考えられる。2015 年 9 月 16 日、東芝とインテルが IoT 分野での協業を発表した[18]（図 3-7）。発電所や交通システムなど産業インフラへのサイバー攻撃を防ぐセキュリティ対策サービスなどの実用化を目指す、とのことである。ジグソーと FFRI も IoT セキュリティ分野における共同研究を開始すると発表した[19]。

1 つ目のトレンドでも示したとおり、あらゆるものがインターネットにつながる IoT 社会の到来に向けては、業界内に留まらず、業界間、社会全体での連携によるセキュリティ対策が益々重要になってくる。


出所：http://www.toshiba.co.jp/about/press/2015_09/pr_j1601.htm

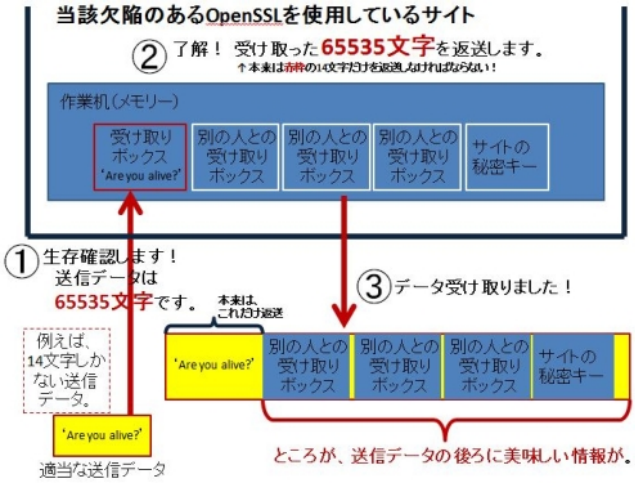
**図 3-7. 東芝とインテルの協業に関するプレスリリース**

[18] http://www.toshiba.co.jp/about/press/2015_09/pr_j1601.htm

[19] http://www.ffri.jp/assets/files/docs/1836/release_20150915.pdf

# 4 オープンソースソフトウェアや多様化するアプリケーションの脆弱性とそれを狙うマルウェアが拡大する

2014 年 4 月 7 日、EC サイト等、特に重要な情報を Web サーバとやりとりする際に広く利用されているオープンソースの暗号通信ソフト「OpenSSL」に脆弱性があることが公表された[20]。「Heartbleed」と呼ばれるこの脆弱性を利用すると、サーバの秘密鍵や他人の暗号化通信内容の情報が搾取できる（図 4-1）。OpenSSL は、インターネットサービスの約 66%、推定 50 万ものサイトや Web サービスで広く利用されているオープンソースであることに加え、暗号化通信でやりとりするような重要な情報が盗まれる可能性があるということもあって、全世界で大きな騒ぎになった。同年 4 月 8 日、OpenSSL プロジェクトにより、当該バグが修正された OpenSSL1.0.1g が公開されたが、OpenSSL 1.0.1 が公開されたのは 2012 年 3 月 14 日。約 2 年間脆弱性を抱えたまま運用されていたことになる。この間に重要な情報が搾取されていた可能性は否定できない。



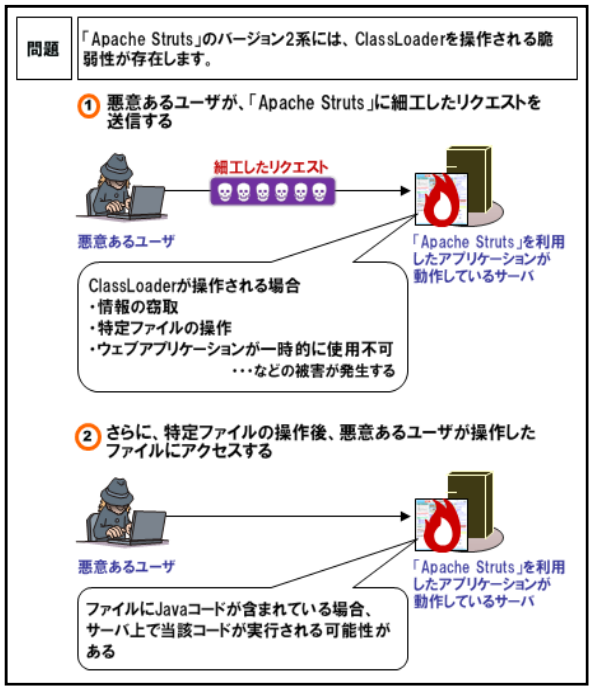

「ITpro」2014 年 4 月 16 日掲載
出所：http://itpro.nikkeibp.co.jp/article/COLUMN/20140413/550222/

**図 4-1．OpenSSL の「Heartbleed」による脆弱性をついた情報不正取得の原理**

ほぼ同時期の 2014 年 4 月 16 日、NTT グループの代表 CSIRT である NTT-CERT が Apache Struts の脆弱性を攻撃するコードが公開されていることを発見し、脆弱性の対策を施して同年 3 月 5 日に公開された Apache Struts に対策漏れがあることを突き止めた[21]。Apache Struts は Apache Software Foundation が開発したオープンソースの Java Web アプリケーションフレームワークで、国内の Web アプリケーション開発で利用されているケースが多い。Apache Struts のこの脆弱性を利用することにより、情報搾取や悪質なプログラムが実行可能となる（図 4-2）。

[20] http://itpro.nikkeibp.co.jp/article/NEWS/20140408/549282/
http://itpro.nikkeibp.co.jp/article/COLUMN/20140413/550222/

[21] https://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html



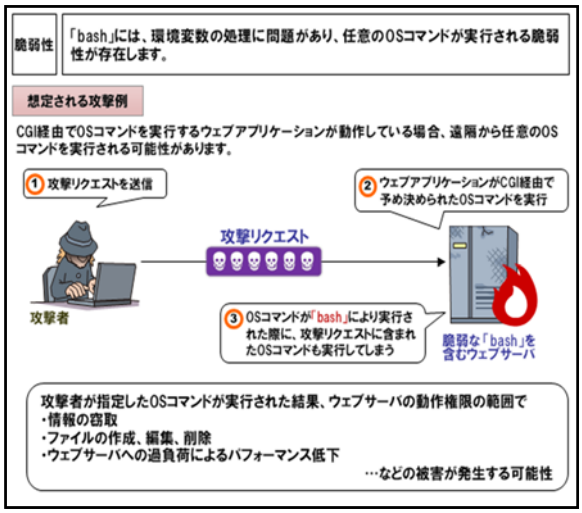

出所：https://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html

**図 4-2. Apache Struts の脆弱性を悪用した攻撃のイメージ**

NTT データは、同年 4 月 28 日、Apache Struts1 系の脆弱性対応のパッチ提供を表明し、順次パッチ提供を開始した[23]。オープンソースの利用に際しては、サポート体制もしっかりと見ていかなければならない。

さらに、オープンソースの脆弱性問題は発生する。2014 年 9 月 24 日、UNIX 系 OS で使われているシェル[24]「bash」に、任意の OS コマンドを実行される脆弱性「Shellshock」 が発見された[25]（図 4-3）。HTTP、SSH、DHCP、FTP、SIP、SMTP、VPN などに対応した攻撃手口も公開され、影響を受ける機器は非常に多い。

Apache Struts は 1 系と 2 系の 2 系統が存在し、当初脆弱性が発見されたのは Apache Struts2 系のほうであった。同年 4 月 24 日には、Apache Struts1 系にも類似の脆弱性があることが発見されたことで事態がより深刻となった。というのも、Apache Software Foundation は 2013 年 4 月に Apache Struts1 系のサポートを終了していたからである。脆弱性が発見されても、Apache Software Foundation から、Apache Struts1 系の脆弱性を修正したパッチは提供されない。2014 年 4 月 27 日には警察庁が Apache Struts1 使用の Web サイトの停止を推奨するに至った[22]。Apache Struts1 系の脆弱性対応は、それを活用するベンダ等のサポートに依存する形となった。




出所：http://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html

**図 4-3. bash の脆弱性を悪用した攻撃のイメージ**

---

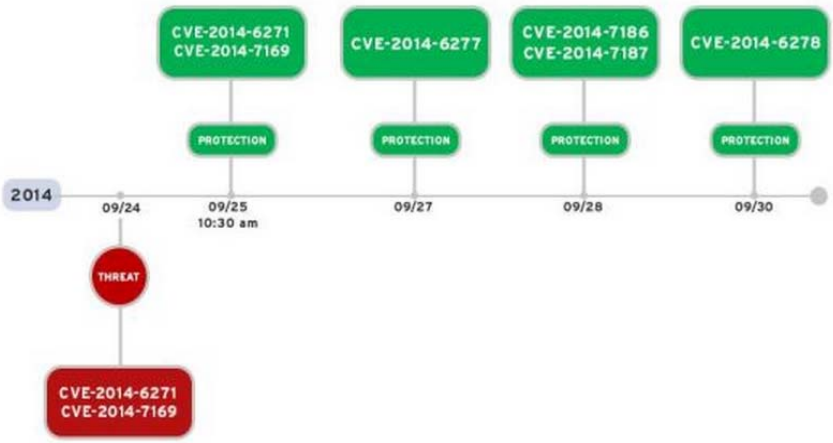
[22] http://www.npa.go.jp/cyberpolice/detect/pdf/20140427.pdf

[23] http://www.nttdata.com/jp/ja/news/information/2014/2014042801.html

[24] コマンドを OS に伝えるソフトウェア

[25] http://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html
http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-vulnerabilities-proliferate-affect-more-protocols/

特に、Shellshock で注目すべき点は、短期間にいくつもの脆弱性が発見され、幾度となく修正パッチ適用に迫られた点である。図 4-4 はその様子を示している。9 月 24 日に脆弱性が発見され、その修正パッチが翌日 25 日に公開されたが、27 日、28 日、30 日にも新たな脆弱性に対する修正パッチが相次いで公開された。1 週間の間に 4 度も修正パッチを適用しなければならない状況になった。警察庁は、脆弱性が発見された翌日の 25 日午前 5 時以降、当該脆弱性を標的としたアクセスが観測されていることを発表した[26]。攻撃を受ける前に修正パッチの適用が必要となる。パッチ適用は時間との勝負である。しかしながら、パッチ適用には、適用後に問題がないかどうかを事前に検証する必要もある。パッチ適用は必ずしも簡単ではない。Shellshock は、パッチマネジメントの難しさを再認識させた。




出所：TrendLabs SECURITY INTELLIGENCE Blog（2014 年 10 月 2 日）
「Shellshock Vulnerabilities Proliferate, Affect More Protocols」内
Figure 1. Timeline of Shellshock CVEs and Deep Security rules

**図 4-4. 脆弱性が発見された時系列図（Shellshock）**

攻撃者は価値の高い獲物を狙ってくる。特に換金性の高い情報資産を保有する情報システムは守りを固める必要がある。しかしながら、脆弱性は突如として公表され、早急なパッチ適用が求められる。パッチが公開されない場合さえある。情報システムに適用する OSS（オープンソースソフトウェア）やアプリケーションのサポート体制をしっかりと構築して、速やかなパッチ適用が困難な場合は、WAF（Web　Application Firewall）や IPS（Intrusion Prevention System）等の周辺で防御する多層防御の仕組みを導入する等の対策が今後益々求められていく。

[26] http://www.npa.go.jp/cyberpolice/detect/pdf/20141007.pdf

# 5 プライバシ保護とデータ利活用の対策が進化する

2013 年 6 月、米中央情報局（CIA）の元職員エドワード・スノーデンは、米国家安全保障局（NSA）が「PRISM」など計４つの極秘プログラムを使ってネット上の個人情報を収集していたと告発した[27]。メールの文面なども閲覧できる「エックス・キースコア」といったプログラムの存在も暴露されている。米国政府が極秘に企業の機密情報、一般市民の個人情報を盗聴していた、というこの告発は大きな騒ぎになった。日本政府や日本企業の電話も盗聴されていた、とも報道されている、このような背景から、米国では、2015 年 6 月に、「愛国法」の規定を修正し、不特定多数を対象にした記録の大量収集を禁じる「米国自由法」が成立した。日本では、2014 年 12 月 10 日、安全保障上の秘匿性の高い情報の漏えいを防止し、国と国民の安全を確保する目的で、「特定秘密の保護に関する法律」（特定秘密保護法）が施行された[28]。スノーデンの内部告発は国家の情報管理、安全保障のあり方を大きく変えることになった。

日本の産業界においては、個人情報の保護に関する法律（個人情報保護法）が 2005 年 4 月 1 日に全面施行されて以来、個人情報の管理、取り扱いに対する取り組みが強化されてきた。しかしながら、個人情報保護の過剰反応があらゆる場面で発生してきた。一方で、企業が保有する個人情報をビジネスに有効活用しようとする動きも活発化してきている。こうした背景から、個人情報保護法改正案が 2015 年 9 月 3 日に成立した[29]。本改正法では、個人情報を特定の個人を識別することができないように、一定の要件で匿名化した「匿名加工情報」に加工すれば、本人の事前の同意を得ずに「匿名加工情報」を第三者に提供することが可能になる。ただし、加工方法については、個人情報保護委員会の定める手法に基づく必要があったり、必要な情報を公表する必要があったり、その他義務行為が発生したりする。企業側には、本改正法を正しく理解し、所定のルールに則って、適切にプライバシを保護するための対策が求められる。特に、日本国内だけではなく、海外でのデータ活用を考える場合、国内法だけではなく、各地域・国のプライバシ保護の要請にも応える必要があるので、注意が必要である。

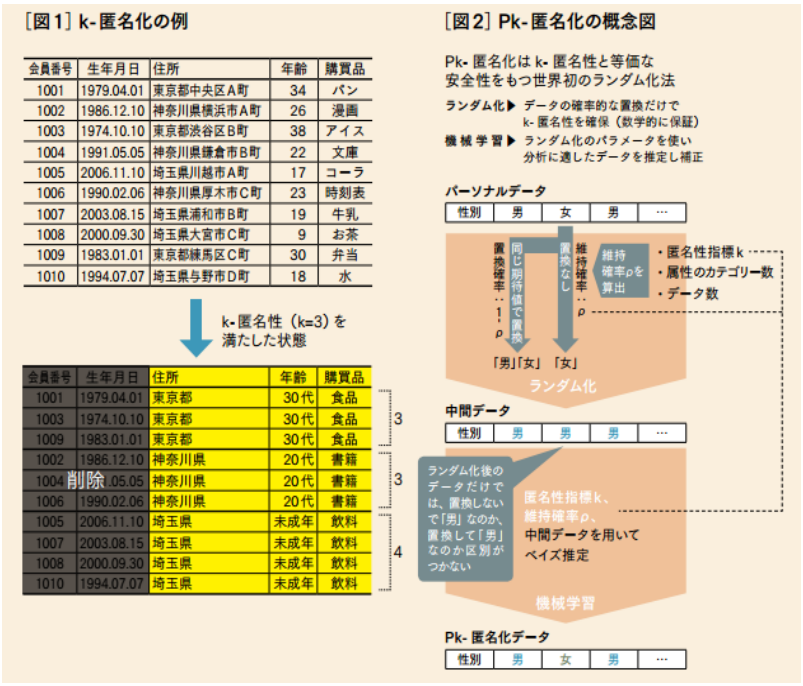
プライバシを保護するためのデータ加工技術についても検討が進んでいる[30]。個人情報の個人性を取り除くために、データの一部を削除したり、データの粒度を粗くしたりすることによって、個人を特定されないようにする加工技術がその一つである。同じ属性をもつ人が必ず k 人以上いる状態にまでデータを加工する「k-匿名化」という技術である（図 5-1 の［図 1］）。

[27] http://www.asahi.com/topics/word/スノーデン.html

[28] http://www.kantei.go.jp/jp/pages/tokuteihimitu.html

[29] http://www.nikkei.com/article/DGXLASFS27H4X_X20C15A8EE8000/

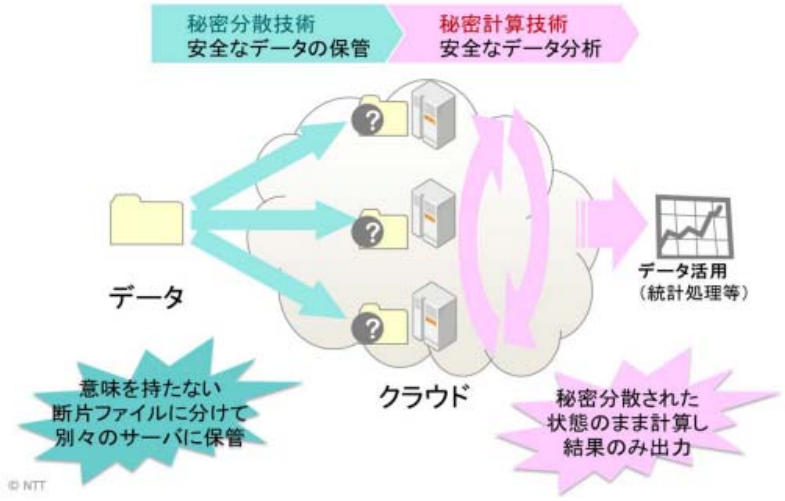
[30] 国立情報学研究所「匿名化技術の最新動向とその課題」(2014 NII Today No.64)




出所：国立情報学研究所「匿名化技術の最新動向とその課題」(2014 NII Today No.64)

**図 5-1. k-匿名化、Pk-匿名化のイメージ**

本技術は、本人がｋ人中の誰かまでは絞り込めないので匿名性は担保できるが、データを粗くしてしまうためにデータ分析の際の利用価値が低下するという課題もある。NTT 研究所はこの課題を解決する「Pk-匿名化」という新たな匿名化技術を開発した[31]。「Pk-匿名化」では、データの利用価値を保ったままデータ分析に影響を与えない程度に元データにノイズデータを付加させる「ランダム化」を行い、データが誰のものであるのかを 1/k 以上の確率で当てることができないように制御するものである（図 5-1 の［図 2］）。k-匿名性と等価な安全性をもつことが理論的に示されたランダム化手法である。データ分析の安全性と有用性を合わせ持つ技術と言えるが、データをランダム化するため一定の誤差は含まれる。個人情報を個人情報のまま、安全かつ厳密に分析する技術として、「秘密計算技術」がある[32]。元データを「秘密分散技術」により複数に断片化し、断片化した 1 つのデータからは元データを復元できないようにして安全性を担保する（図 5-2）。この安全性が担保された状態のまま統計処理等を厳密に実




出所：IT 総合戦略本部/パーソナルデータに関する検討会/第 1 回技術検討ワーキンググループ（資料 2-1)「匿名化に関する検討について（総務省）」(平成 25 年 9 月 27 日)

**図 5-2. 秘密計算のイメージ**

[31] http://www.ntt.co.jp/news2014/1402/140207b.html

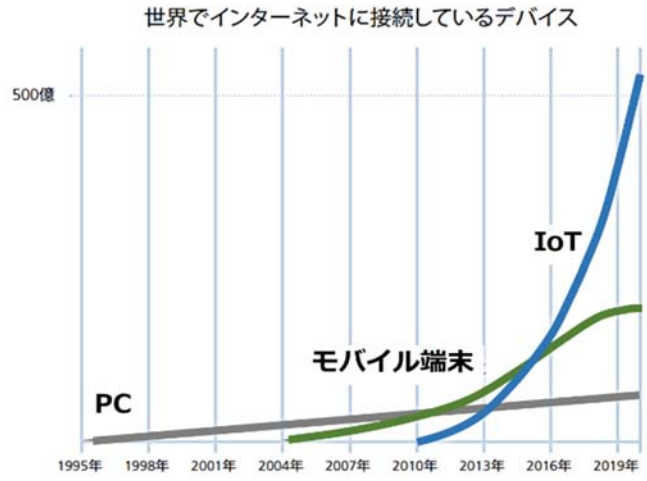
[32] IT 総合戦略本部/パーソナルデータに関する検討会/第 1 回技術検討ワーキンググループ（資料 2-1)「匿名化に関する検討について（総務省）」(平成 25 年 9 月 27 日)

施し、計算結果だけを知ることができる。安全性と厳密性を両立する技術であるが、性能、コストが課題となる。

　今後のビッグデータ時代においては、データの利活用に関する企業ニーズが益々拡大していくとともに、プライバシ保護に対する要請も求められていく。プライバシ保護を可能とするデータ加工技術もさらに進化していくであろう。法制度に対する正しい理解とともに、企業内でのプライバシ保護に対する適切な対応が益々重要になってくる。

# 6 モバイル社会が益々進展し、セキュリティと利便性を両立させる対策が求められる

IoT デバイス、モバイル端末が急増している。マカフィーのレポートによれば、全世界でインターネットに接続されているデバイスの台数は、既に、モバイル端末が PC を追い越している[33]（図 6-1）。2020 年には、IoT デバイスは 500 億を超えると予測されており、モバイル端末も IoT デバイスほどではないが、今後も増加を続け、モバイル社会が本格化していく。

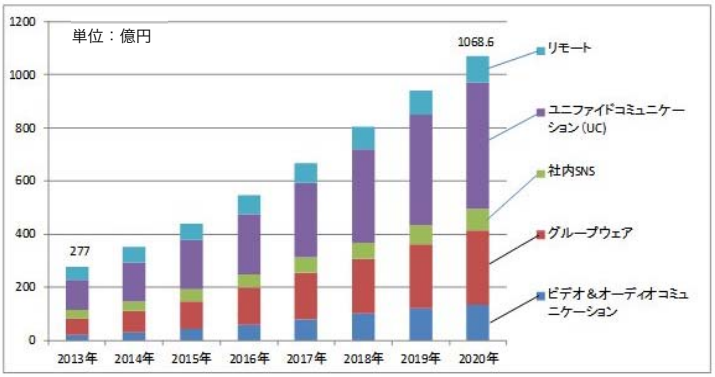



出典: McAfee、BI Intelligence、IDC、Intelの調査結果に基づく。

出所：インテルセキュリティ「McAfee Labs 脅威レポート」（2014 年 11 月）に加筆

**図 6-1. インターネット接続デバイス（全世界）**

こうしたモバイル端末の浸透を背景に、モバイルワークの人口も増加していくものと予測される。IDC ジャパンは、オフィス外で就業時間の 20%以上の業務を行う国内モバイルワーク人口は 2013 年末に 1,360 万人と推計し、外勤者向け／在宅勤務を含むテレワーク実施企業は 10 ポイント程度増加した、と報告している[34]。市場調査とコンサルティングのシード・プランニングは、2020 年までのテレワークソリューション市場規模を予測し、2020 年には 1000 億市場にまで拡大していくと報告している[35]（図 6-2）。




（シード・プランニング作成）

出所：http://www.seedplanning.co.jp/press/2014/2014041601.html

**図 6-2. テレワークソリューションの市場予測**

一方、こうしたモバイル社会への移行に対して、セキュリティ上の不安の声も上がっている。総務省が 2015 年 7 月に発表した情報通信白書によれば、企業のテレワーク導入に際して、「情報セキュリティの確保」が最大の課題とな

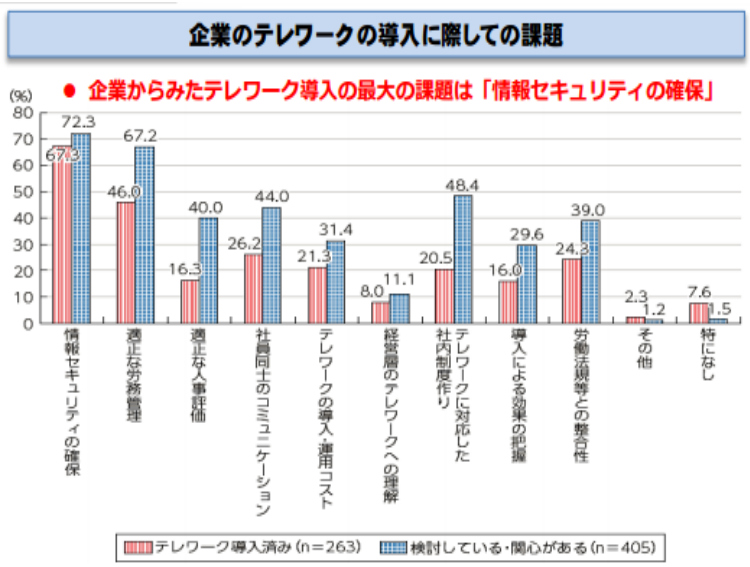
[33] インテルセキュリティ「McAfee Labs 脅威レポート」（2014 年 11 月）

[34] http://www.idcjapan.co.jp/Press/Current/20141104Apr.html

[35] http://www.seedplanning.co.jp/press/2014/2014041601.html

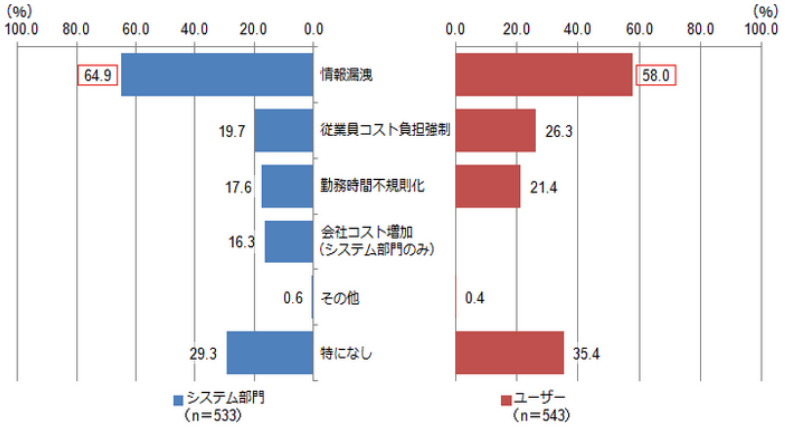
っている[36]。テレワークを実際に導入している企業よりも、テレワークの導入を「検討している・関心がある」企業の方が、導入に際しての課題を多く挙げる傾向がある（図 6-3）。

NTT データ経営研究所と NTT コムオンライン・マーケティング・ソリューション社は、共同で実施した「私用端末の業務利用（BYOD[37]）動向調査」の中で、BYOD としてデバイス使用を許可している組織は約 43%に上り、セキュリティに懸念を抱いていることを明らかにした[38]。システム部門、ユーザーともに、情報漏えいに不安を感じる割合が半数を超えている（図 6-4）。BYOD の更なる普及には、システム部門のセキュリティ不安を解消することが必須である、と報告している。




出所：総務省「「平成２７年版 情報通信白書」の概要」（平成 27 年 7 月）

**図 6-3. テレワークの導入に際しての課題**




出所：ＮＴＴデータ経営研究所／ＮＴＴコム リサーチ
http://www.keieiken.co.jp/aboutus/newsrelease/131211/index2.html

**図 6-4. BYOD において感じるデメリット**

確かに、マカフィーの最新のレポートによれば、2015 年度になって、モバイル端末を狙う新しいマルウェアが増加している、と報告されている[39]（図 6-5）。攻撃者は獲物獲得のために、モバイル端末のセキュリティが不十分と見れば、徹底的にモバイル端末を標的としてくるであろう。2 つ目のトレンドで示したとおり、攻撃者はセキュリティ対策の弱いところを狙って攻めてくる。今後

[36] 総務省「平成 27 年度情報通信白書」(2015 年 7 月)

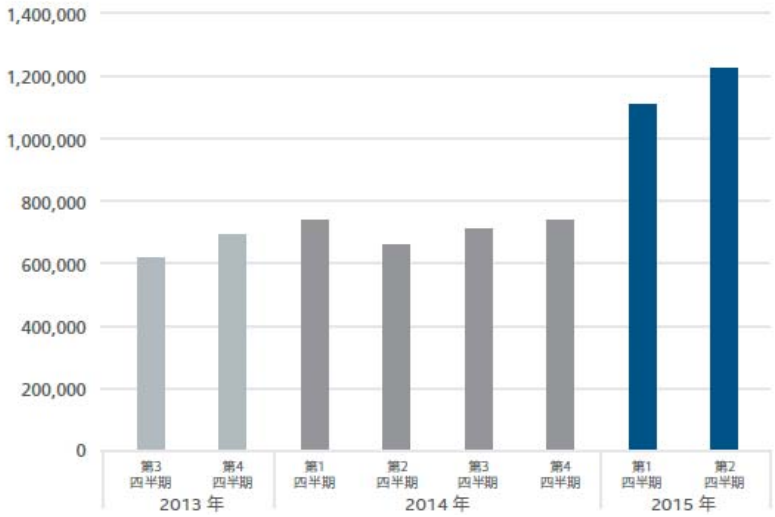
[37] Bring Your Own Device の略

[38] http://www.keieiken.co.jp/aboutus/newsrelease/131211/index2.html

[39] インテルセキュリティ「McAfee Labs 脅威レポート」（2015 年 8 月）

のモバイル社会の進展に向けては、モバイルセキュリティが最も重要となるかもしれない。

市場の変化、拡大、多様化に合わせて、ビジネス競争も熾烈を極める。ワークライフバランス、サテライトオフィス、テレワーク等、ビジネス環境も多様化していくに違いない。ビジネススピードや効率化の要請が益々高まり、スマートフォン/タブレット端末のビジネス利用が拡大していくであろう。セキュリティと利便性を両立させるような対策が今後益々重要になってくる。




出所：インテルセキュリティ「McAfee Labs 脅威レポート」（2015 年 8 月）

**図 6-5. 新しいモバイルマルウェアの数**

# 7 セキュリティ技術者の不足が益々深刻化し、セキュリティアウトソースビジネスが成長する

IPA の調査によると、2014 年現在でセキュリティ人材は 26 万 5 千人、と推計されている[40]。ただし、その内、スキル不足者は 15 万 9 千人。つまり、実質的なセキュリティ有スキル者人材数は 10 万 6 千人、ということになる。本来必要な人材数は 34 万 7 千人と推計され、不足人員、スキルアップ人員含めて、24 万人のセキュリティ人材育成が必要という計算になる（図 7-1）。現在の有スキル者の 2 倍以上の育成が必要ということである。セキュリティ人材は質、量ともに決定的に不足しているのが現状である。サイバー攻撃は日々、悪質化、巧妙化し、攻撃者側の技術の進歩も激しい。現在の有スキル者の技術を維持、高度化していくことも必要であり、その数を 3 倍以上に増やすのは並大抵のことではない。

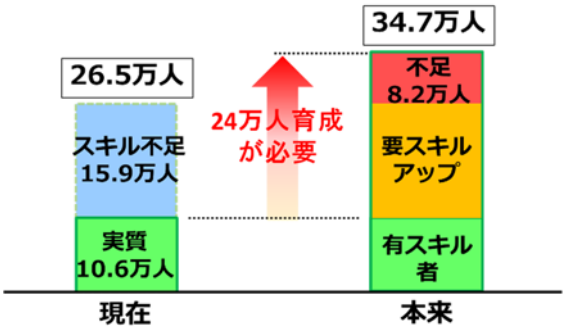
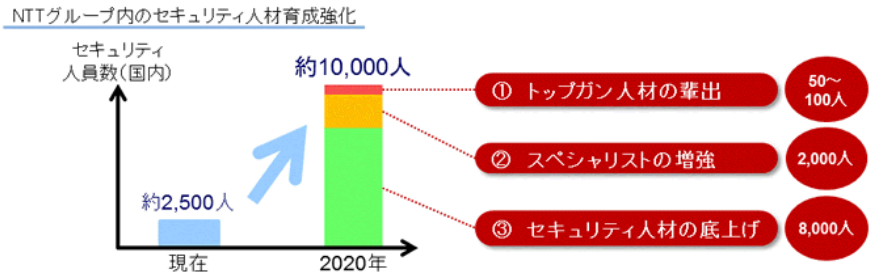



**図 7-1. セキュリティ人材の不足数**

NTT グループは、2014 年 11 月、中期経営戦略「新たなステージをめざして」の中で、セキュリティ人材育成プランを発表した[41]（図 7-2）。2020 年までに国内セキュリティ人材を 4 倍の 1 万人に増強するプランである。また、「産業横断サイバーセキュリティー人材育成検討会」を発足し、社内セキュリティ人材育成を加速させて、産業界の民民連携を深める考えも示した[42]。

IPA は、現状の情報セキュリティ体制や対策、被害状況等を調査した報告書もまとめている[43]。本報告書によれば、CISO[44]が配置されている企業は半数に満たない（図 7-3-1、図 7-3-2）。セキュリティを経営上の重要課




出所：NTT「中期経営戦略"新たなステージをめざして"について」（2014 年 11 月 7 日）

**図 7-2. NTT グループのセキュリティ人材育成プラン**

[40] http://www.ipa.go.jp/files/000040646.pdf

[41] http://www.ntt.co.jp/news2014/1411jkxp/vkgt141107a_11.html

[42] http://www.sankei.com/economy/news/150608/ecn1506080034-n1.html

[43] IPA「2014 年度 情報セキュリティ事象被害状況調査 －報告書－」（2015 年 1 月）

[44] Chief Information Security Officer の略。最高情報セキュリティ責任者。

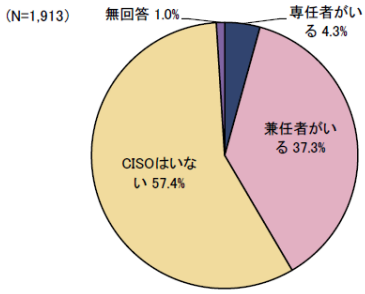



図 7-3-1. CISO の有無

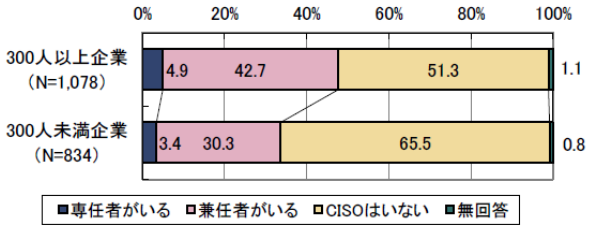



図 7-3-2. CISO の有無（従業員規模別）

題と位置づけている企業が少ない表れではないだろうか。また、情報セキュリティ業務担当者の量的な充足度について、十分であると回答した企業は 33%である（図 7-4-1、図 7-4-2）。企業規模が大きいほど、担当者が不足している傾向にある。スキル面での充足度については、十分であると回答した企業は 20%であり、スキル不足のほうがより深刻な状況になっている（図 7-5-1、図 7-5-2）。

セキュリティ人材の確保、拡大は極めて重要な経営課題とも言えるが、そのように認識している経営者はどれほどいるだろうか。２つ目のトレンドでも示したとおり、攻撃者はセキュリティ対策が弱いところを狙ってくる。セキュリティ対策が十分ではない、セキュリティ技術者がいない中小企業が標的とされる可能性が益々高まる。中小企業のセキュリティ人材確保は非常に難しい経営課題とも言える。

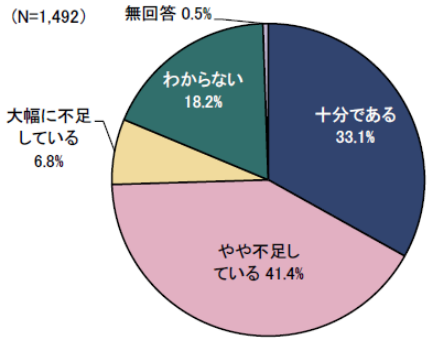



図 7-4-1. 情報セキュリティ業務担当者の量的な充足度

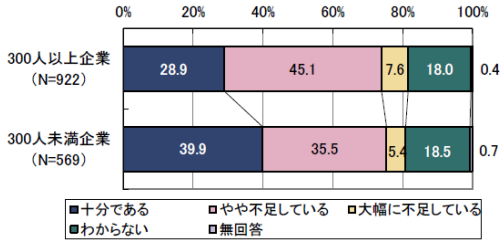



図 7-4-2. 情報セキュリティ業務担当者の量的な充足度（従業員規模別）

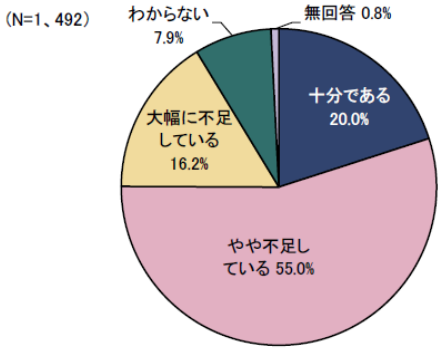



図 7-5-1. 情報セキュリティ業務担当者のスキル面での充足度

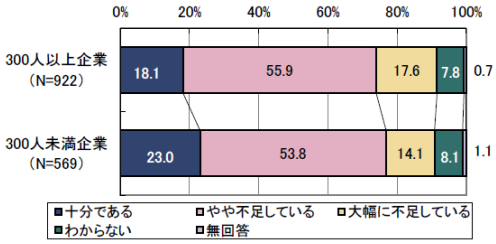



図 7-5-2. 情報セキュリティ業務担当者のスキル面での充足度（従業員規模別）

こうした状況の中、情報セキュリティ業務を外部に委託するケースがどの程度あるかというと、半数以上が外部に委託していない、という調査結果であった（図 7-6-1、図 7-6-2）。情報セキュリティ業務担当者は量的にもスキル的にも不足している状況を踏まえると、社内でのセキュリティ人材不足を補うために、有能なセキュリティベンダ等への外部委託も増加していくものと考えられる。今後はセキュリティアウトソースビジネスが急成長していくであろう。

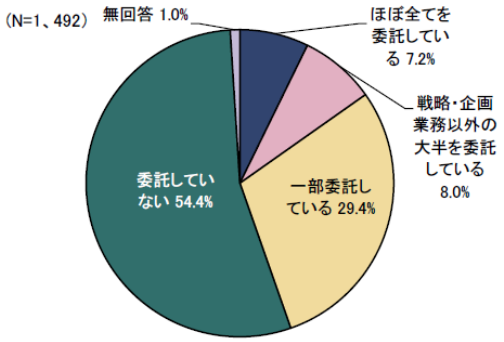
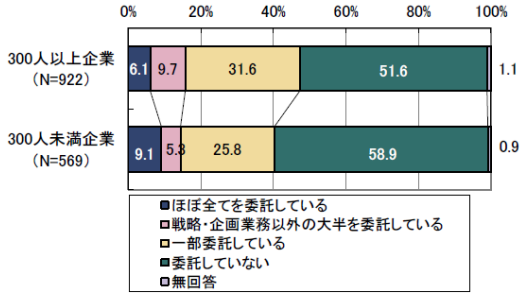



**図 7-6-1. 情報セキュリティ業務の外部委**




出所（図 7-3～7-6）：IPA「2014 年度 情報セキュリティ事象被害状況調査 －報告書－」（2015 年 1 月）

**図 7-6-2. 情報セキュリティ業務の外部委託（従業員規模別）**

●ＮＴＴソフトウェアは環境保護に取り組んでいます。

**NTT ソフトウェア株式会社**
クラウド＆セキュリティ事業部
TEL : 045-212-7577
Email : cs-trend@cs.ntts.co.jp
URL : https://www.ntts.co.jp/products/cs-trend/