1-1　情報セキュリティインシデントの発生状況１

≫ グローバルでのインシデント発生状況

Point !!

ここ２～３年で、グローバル・日本国内のインシデントにおける脅威の性質が変化しています。

従来はどちらかというと、組織内部の問題や関係者による情報窃取やミスによる情報漏えいが目立っていましたが、現在は外部から情報窃取を意図したサイバー攻撃が頻発しています。そして、非常に巧妙で多様かつ執拗な手口による被害が多発し、深刻化しています。

個人情報窃取を目的としたデータ侵害は、増加傾向をたどっており、2014年には、10億件を超える個人情報漏えいが報告されており、実に全世界の30億人のネット利用者の３人に１人が被害にあった計算になります。

しかし、サイバー攻撃のターゲットは個人情報だけではありません。組織がビジネスを行っていく上で、有用かつ一般的に知られていない技術や顧客等の機密情報を含む「営業秘密情報」は、競合企業や他国の同業者にとっては非常に魅力的なものです。それらの情報は、デジタル化され利活用されていることから、サイバー犯罪者にとっては格好の獲物になっています。

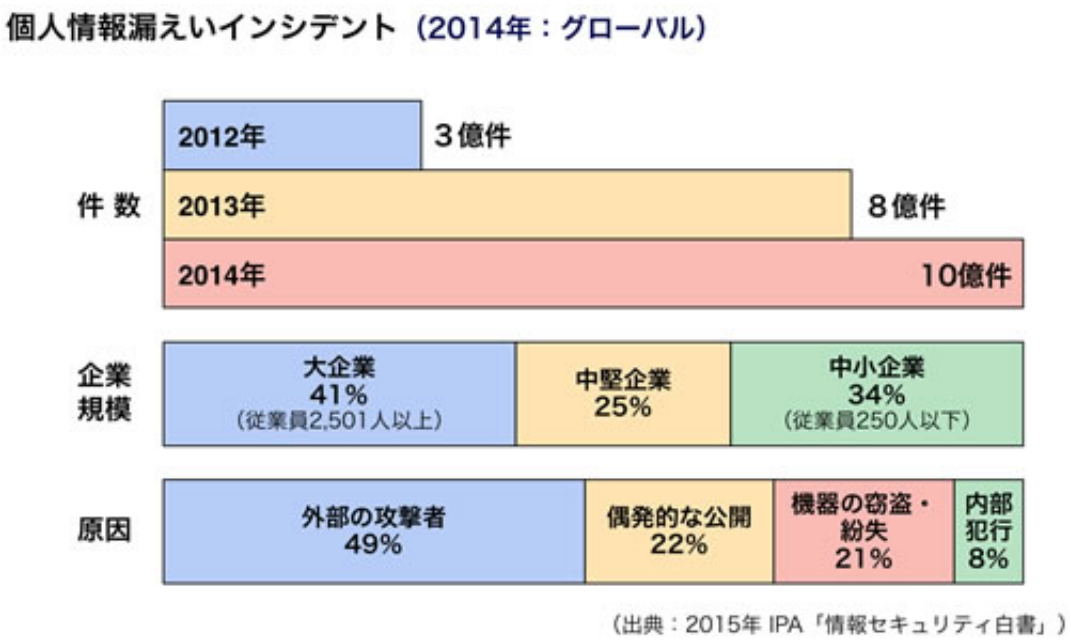
また、企業規模別では、大企業ばかりではなく、中小企業での発生件数も多くなっており、サイバー攻撃手法の汎用化により、セキュリティ対策の甘い中小事業者をターゲットに、そこから得られた情報でサプライチェーン内の大手企業へと攻撃を仕掛ける傾向が増加しています。

中小企業だから大丈夫などという考えはあたらめなければなりません。中小事業者は攻撃しやすいターゲットとして狙われています。

このように、インシデントの原因は内部犯行だけではなく、外部からのサイバー攻撃者が急増し、深刻化しており、一般人から企業、国家に至るまで場所や階層を選ばず、巧妙かつ周到なレベルの攻撃に備える必要があります。

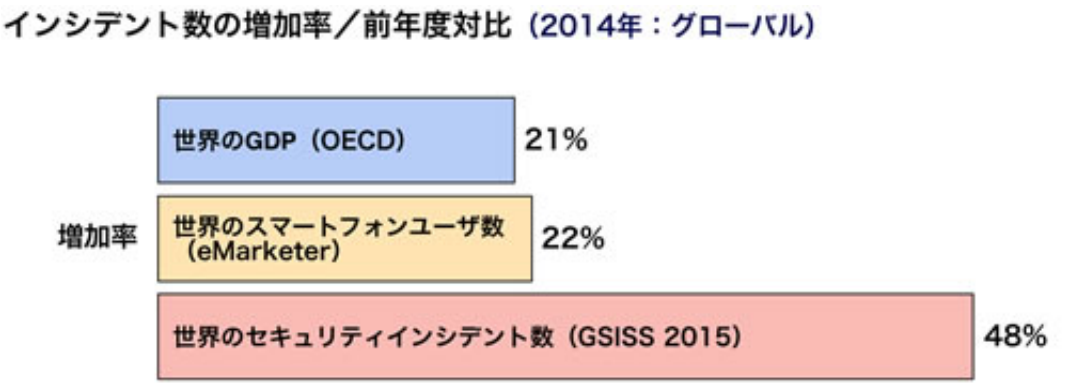
攻撃者は、専門知識を持つプロだけではなく、ネット上にハッキングツールが闇で流通していることから、誰でもがハッカーになれるという環境が存在しています。日本でも未成年によるハッキング犯罪が増加しているということからも、今後も情報という有益な資産を狙うサイバー攻撃が日常的に行われ、増加し続けることは明らかです。

同時に、ハッキングやサイバー攻撃にあった際の組織の対応にも、油断や準備不足など、大きな問題・課題があることも事実です。インシデントの原因や手法が変化しても、やはりそれに対応できる組織体制や組織風土の改善、そして内部の人員が重要なポイントであることに変わりはありません。



（出典：2015年 IPA「情報セキュリティ白書」）

また、グローバルのセキュリティインシデント数はGDPや携帯電話の成長率をしのぐ勢いで増加しています。以下の増加率から、インシデント被害のビジネスに対する影響の大きさが理解できると思います。現代のビジネスでは、情報セキュリティ対策は経営課題として経営層が自ら積極的に取り組まなければ、ICTのメリットを活かすことが困難であるばかりか、気づかない間に、大きな損害・被害を受ける可能性もあります。



（出典：2015年 pwc「グローバル情報セキュリティ調査」）

1-2　情報セキュリティインシデントの発生状況2

≫ インシデントの発生源（グローバル）

Point !!

前のページではインシデントの原因について、内部犯行だけではなく外部からのサイバー攻撃者が急増していることを説明しました。

しかし、依然としてセキュリティ犯罪の発生源として内部関係者（特に現従業員、元従業員）が重要なポイントであることには変わりありません。

そして、2014年の米国セキュリティ犯罪調査では、内部者による犯罪の方が外部者による犯罪よりも高コストで被害が大きいという回答がほぼ3分の1（32%）を占めました。

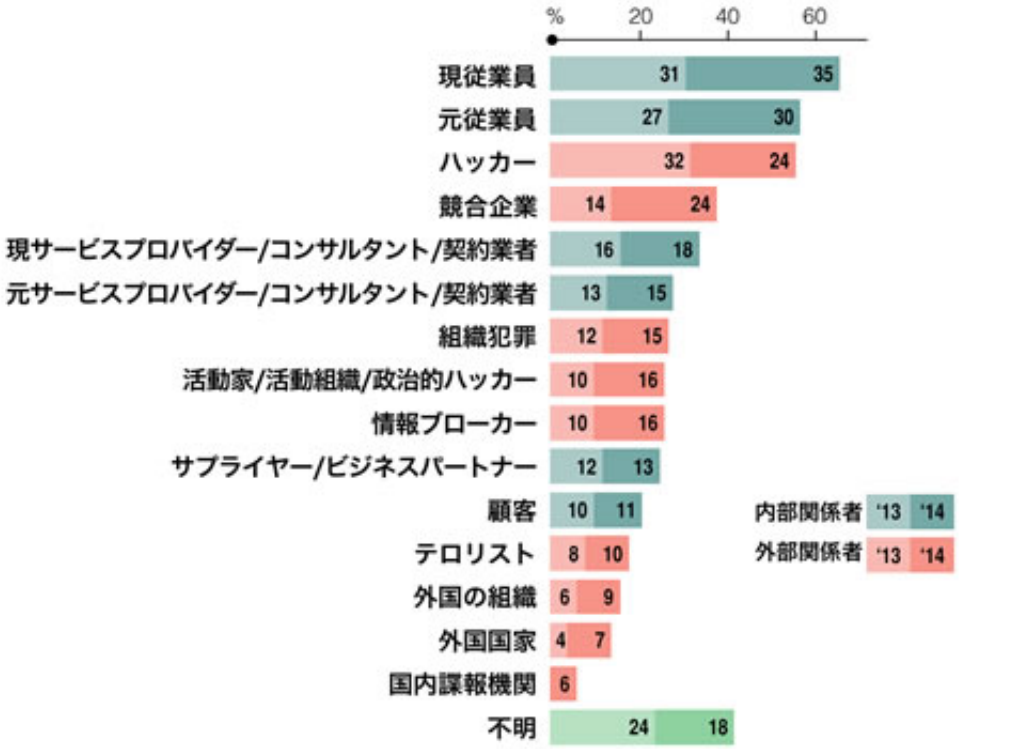
インシデントの発生源統計では内部関係者が最多回答となりました。ただし、全ての従業員が悪意ある行為に及ぶわけではなく、多くの場合はモバイルデバイスの紛失やフィッシング詐欺などを通じて、データをうっかりミスで危険にさらしてしまうというところに原因があります。

しかし、内部関係者の脅威に対応するプログラムを用意している企業はまだ少なく、内部の脅威の防止、検知、対応のための準備が不十分であるという結果です。

特に日本では、高度成長期から従業員に対して「性善説」という考え方から、家族的な関係を重視してきた傾向があります。

しかし、最近では「性善説」では管理しきれない現状を見て「性悪説」によってルールや懲罰を厳しくした内部統制を考えがちです。これからは、人は環境に影響を受けやすく、自尊心や体面を守るため、間違いを犯すものという「性弱説」を前提に、組織内コミュニケーション活動や教育による相互理解と正しい意思決定力の醸成を促すことが大切だと思われます。

セキュリティインシデントの発生源（グローバル）



（出典：2015年 pwc「グローバル情報セキュリティ調査」）

1-3　情報セキュリティインシデントの発生状況３

≫ 国内でのインシデントの発生状況

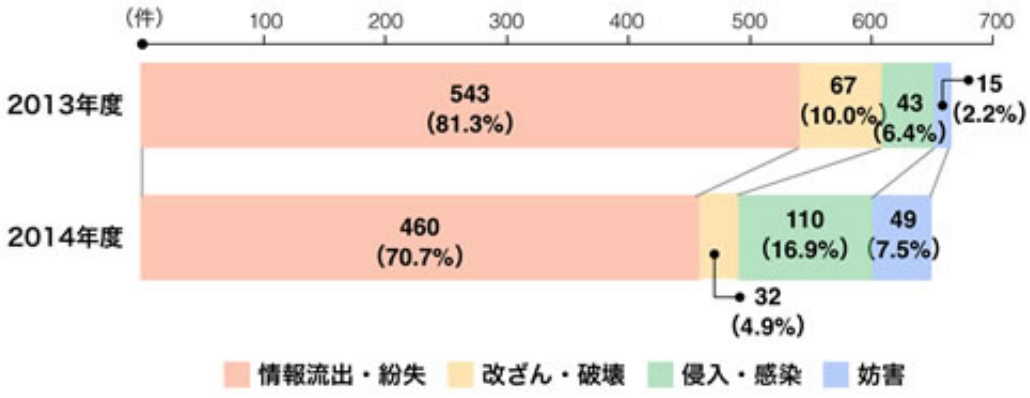
Point !!

国内での情報セキュリティインシデントは減少傾向にあると報告されています。しかし、報道ベースの集計であり、些細なミスによるインシデントはカウントされていない可能性が高いと考えられます。

また、昨今急激に増加しているサイバー攻撃等は被害を受けていても気付かないケースが多いことや、内部インシデントの公表を控えていると思われるため、インシデント数においては表出している数が減っているだけで、実際には増加していると考えられます。

インシデントの事象別発生状況からその傾向を見てみると、情報流出や改ざん・破壊に関しては減少していますが、「侵入・感染」や「妨害」については大幅に増加しています。しかし、これは件数ベースの統計であり、その被害額や利害関係者への影響度については別途資料により考察する必要がありそうです。

情報セキュリティインシデントの事象別発生状況（2013～2014年度）



出典：IPA「情報セキュリティ白書」2015年

過去１年間に経験したセキュリティインシデント統計から、大きく２つの傾向が見えます。

１）外部からのサイバー攻撃に関連するインシデント

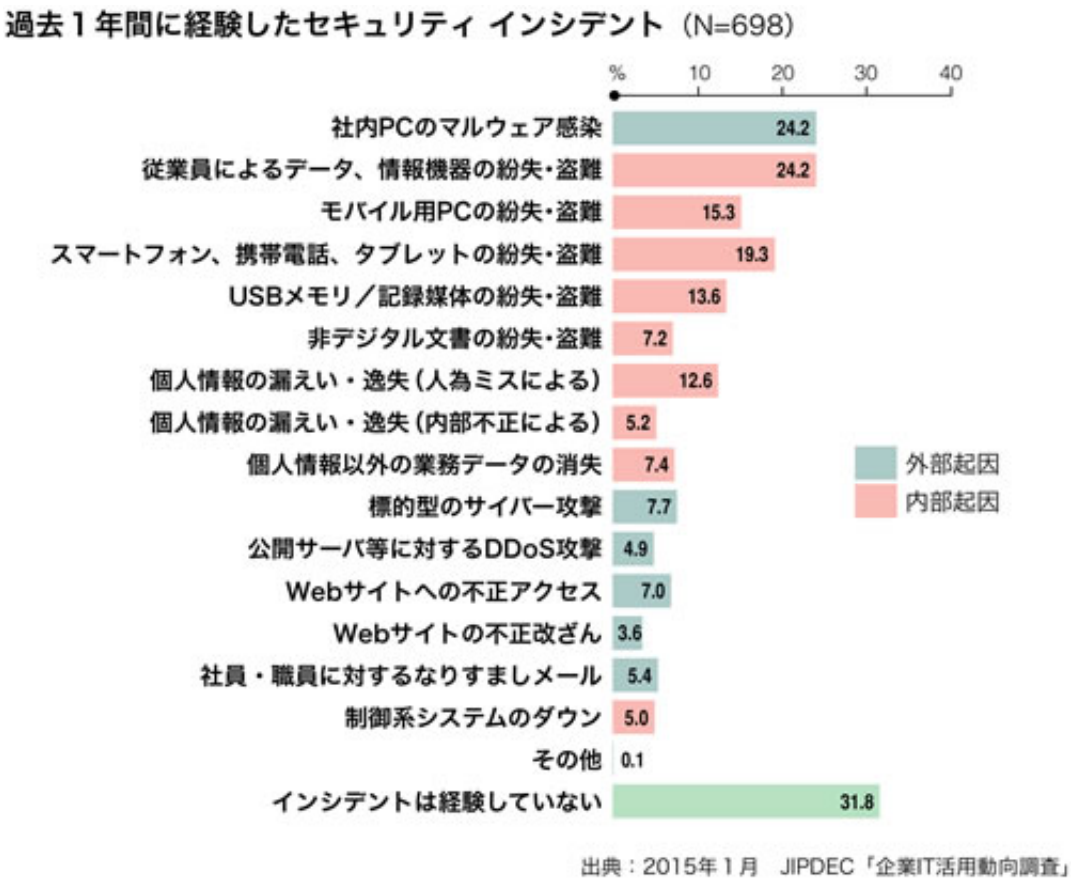
大企業に関わらず、中小企業まで幅広くマルウェアを含むサイバー攻撃が増加していることがわかります。半数以上の52.8%以上の組織が、外部からのサイバーアタックやウイルス感染を認識しています。

２）内部人員のミスによるデータやデータが入った機器や文書の紛失・盗難のインシデ

ント

スマートデバイスの普及は、場所を選ばず利用できることから業務利用（会社貸与、個人私有を含む）が増加しています。しかし、一旦持ち出されたデバイスやメディアの管理には人のミスが付きまとい、紛失・盗難による事故が増加しています。

また、個人情報の漏えい・逸失については「人為的ミス」が12.6%、「内部不正」が5.2%となっています。しかし、意図された内部不正による漏えい事件は１件あたりの漏えい規模が大きく、組織に大きな損害を及ぼします。



1-4　最近のインシデントから1

≫ IPA「情報セキュリティ10大脅威2016」等からの脅威事例1

Point !!

実際にどのようなインシデントが起こっているのでしょうか。報道で大きく取り上げられた事故・事件も、時間が経てば忘れてしまうことも多いのですが、あらためて情報セキュリティ事故や事件を思い起こし、そこから学ぶ姿勢が予防策として大切です。そして情報インシデントは、対岸の火事ではなく、いつ身の回りで起こってもおかしくない状態です。

事例から、どう対応すれば良いのか、自分なりに考えて、組織内で共有し、インシデントシナリオから危機時の対応について検討してみることも大切です。もし、起こったら・・・・。

最初に、毎年IPAが発表している「情報セキュリティ10大脅威2016」および「情報セキュリティ10大脅威2015」から、どんな脅威があり、どんなインシデントが発生しているかを学びましょう。

「情報セキュリティ10大脅威2016」では、脅威の影響を全体的な視点で検討し、「総合」および「個人」と「組織」に分けて発表しています。

【総合順位】

1位：インターネットバンキングやクレジットカード情報の不正利用

2015年でも1位にランキングされていました。2014年下半期に一旦減少しましたが、2015年上半期にはターゲットが信用金庫や信用組合等地域の金融機関に拡大し、被害は更に増大しました。ウイルスやフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が窃取され、本人になりすまして不正利用されています。

インターネットバンキングに係る不正送金事犯の発生状況推移

（概算金額）

	被害額	実被害額	阻止額	阻止率
2013年上期	2億1,300万円	2億 300万円	1,000万円	4.6%
2013年下期	11億9,300万円	11億2,700万円	6,600万円	5.5%
2014年上期	18億5,100万円	17億1,000万円	1億4,100万円	7.6%
2014年下期	10億5,800万円	7億2,600万円	3億3,200万円	31.4%
2015年上期	15億4,400万円	13億7,500万円	1億6,800万円	10.9%
2015年下期	15億3,000万円	12億6,400万円	2億6,600万円	17.4%

（出典：平成27年のインターネットバンキングに係る不正送金事犯の発生状況等について：警察庁）

警察庁の統計では、2015年の上期だけで15.4億円もの被害が出ています。まだ統計は出ていませんが、年間では30億円を超える被害になり、増加し続けていることがわかります。

一次送金先口座名義人の国籍推移

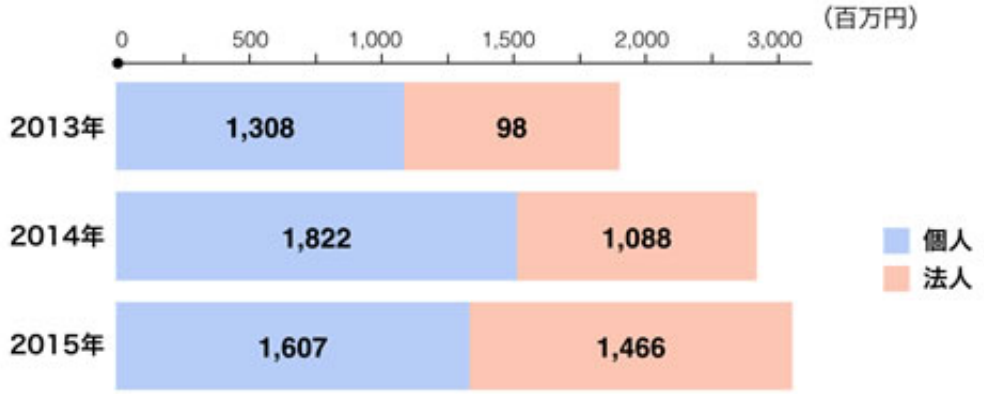
（件,%）

	2013年		2014年		2015年	
中　国	1,642	70.9%	2,420	64.1%	1.350	57.0%
日　本	469	20.2%	1,079	28.6%	603	25.5%
その他	206	8.9%	275	7.3%	414	17.5%
合計	2,317	100.0%	3,774	100.0%	2,367	100.0%

（出典：平成27年のインターネットバンキングに係る不正送金事犯の発生状況等について：警察庁）

また、不正に利用されたものは、一次送金先口座としては中国がトップを占めています。警察では送金阻止活動で若干でも犯罪の防止をしていますが、犯罪のグローバル化で犯人や犯罪組織の解明までは至っていないようです。

口座種別：被害額推移



（出典：平成27年のインターネットバンキングに係る不正送金事犯の発生状況等について：警察庁）

口座種別毎の被害状況（2015年）

（概算金額）

口座種別		都市銀行等	地方銀行	信金・信組	農協・労金	合　計
個人	被害額	9億8,700万円 32.1%	3億5,400万円 11.5%	2億2,100万円 7.2%	4,500万円 1.5%	16億　700万円 52.3%
	実被害額	8億9,000万円 33.6%	3億1,600万円 11.9%	2億　100万円 7.6%	4,100万円 1.5%	14億8,700万円 54.7%
法人	被害額	4億5,900万円 14.9%	2億4,600万円 8.0%	7億1,800万円 23.4%	4,300万円 1.4%	14億6,600万円 47.7%
	実被害額	4億1,600万円 15.7%	1億4,600万円 5.5%	6億　800万円 23.0%	2,800万円 1.1%	11億9,900万円 45.3%
合 計	被害額	14億4,600万円 47.1%	6億　　円 19.5%	9億4,000万円 30.6%	8,700万円 2.8%	30億7,300万円 100.0%
	実被害額	13億　600万円 49.4%	4億6,200万円 17.5%	8億　900万円 30.6%	6,900万円 2.6%	26億4,600万円 100.0%

（出典：平成27年のインターネットバンキングに係る不正送金事犯の発生状況等について：警察庁）

口座種別では、個人口座が法人口座に比較して、多い時で２倍以上の割合となっています。2013年頃から大手銀行名を名乗るフィッシングメールが大量に出回ったことも原

因の一つと考えられます。

フィッシング報告件数の推移

(出典：2015年 内閣サイバーセキュリティセンター（NISC）)

また、2015年には信用金庫や信用組合の法人口座での被害が急増しています。これは大手都銀や地銀に比べて、「ワンタイムパスワード」の導入などセキュリティ対策の遅れをついた犯罪と考えられます。

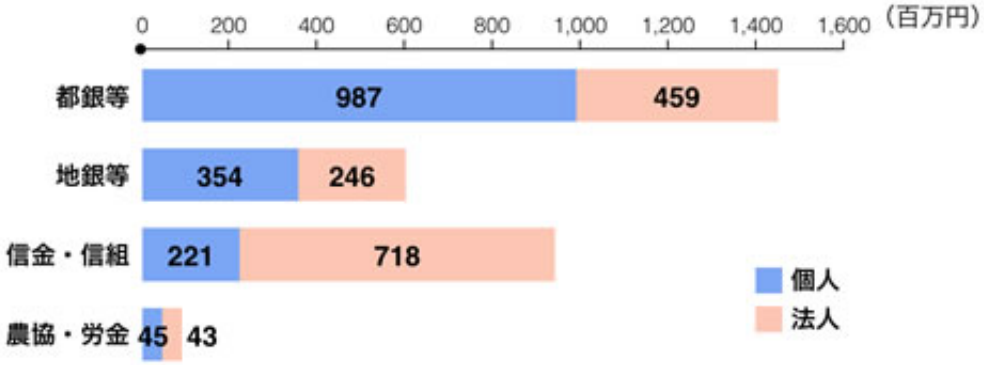
金融機関別毎の被害状況推移

(概算金額)

金融機関	2013年	2014年	2015年
都銀等	12億8,300万円	19億　500万円	14億6,000万円
地　銀	1億2,300万円	8億8,200万円	6億　　円
信金・信組	0円	1億2,300万円	9億4,000万円
農協・労金	0円	0円	8,700万円
合 計	14億　600万円	29億1,000万円	30億7,300万円

(出典：平成27年のインターネットバンキングに係る不正送金事犯の発生状況等について：警察庁)

2015年被害内訳（金融機関別）



(出典：平成27年のサイバー空間をめぐる脅威の情勢について：警察庁)

1-5　最近のインシデントから2

≫ IPA「情報セキュリティ10大脅威2016」等からの脅威事例2

Point !!

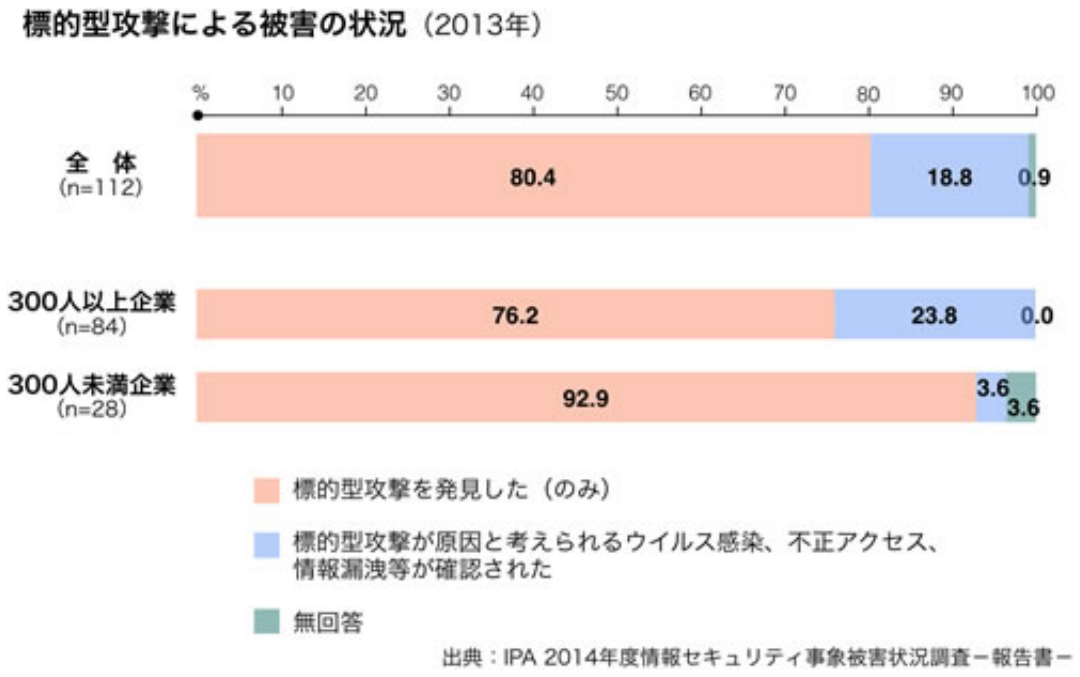
日本年金機構のサイバー攻撃は、時間が経つにつれて詳細が明らかになり、テレビ等のニュース番組や特別番組で、被害実態や攻撃者について調査報道されました。

この事件と同時に、日本国内の1,000社にもおよぶ企業に対してサイバー攻撃が仕掛けられ、情報が窃取されていることも明らかになりました。

いままでは主に日本国内のことを考えていればよかったのですが、これからはグローバルな視点で対策検討していく必要があります。

2位：標的型攻撃による情報流出

2015年には3位でしたが、日本国内だけではなくグローバルでも事故が多発していることから、脅威評価が上がりました。「標的型攻撃」とはPCをウイルスに感染させ、外部からPCを遠隔操作して内部情報を窃取する諜報活動のことです。2015年6月には「標的型攻撃」よる日本年金機構の情報漏えいが大きく報じられました。

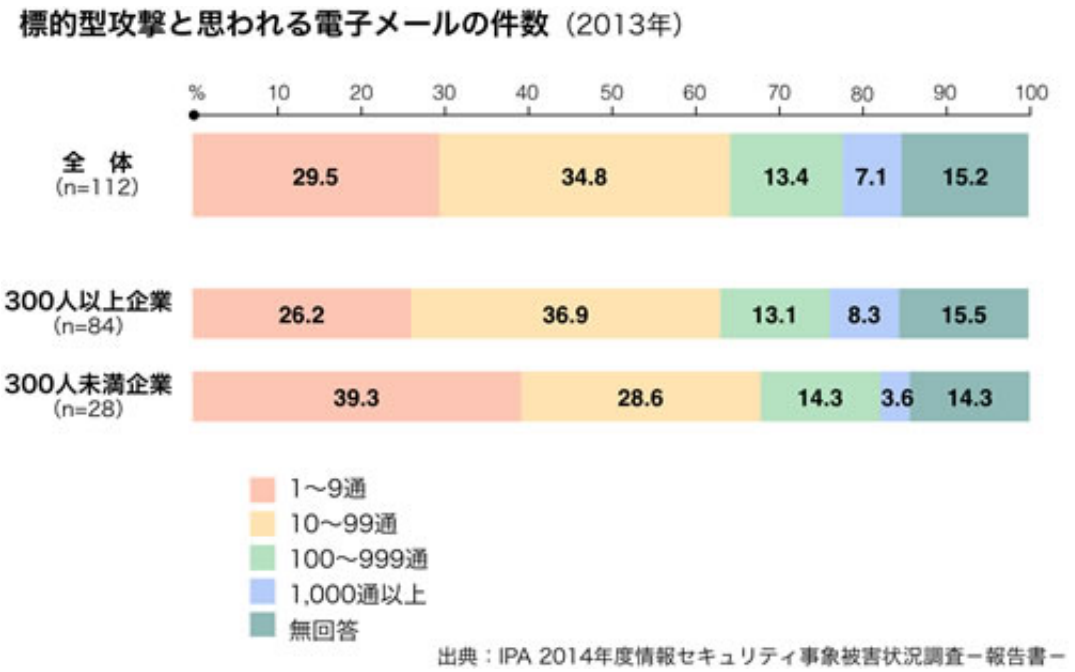


日本国内（2013年）では、全体の80.4%の企業が標的型攻撃を発見したと答えています。また、300人以上の中堅・大企業では23.8%が、「標的型攻撃が原因と考えられるウイルス感染、不正アクセス、情報漏えい等が確認された」と被害の状況を答えています。

ここ最近の状況から更に増加しているものと考えられます。

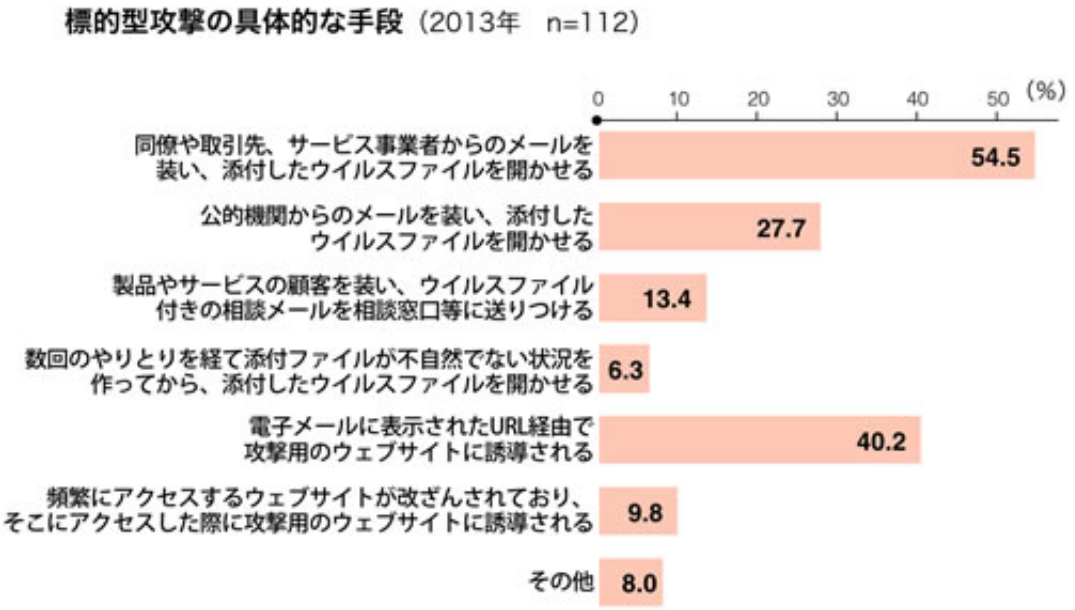
標的型攻撃と思われる電子メールは、10～99通／年が34.8%と最も多く、中には1,000通以上／年という企業も7.1%ありました。

標的型攻撃は、ターゲットに対して、長期間、何段階もの攻撃を執拗に繰り返して行い、情報を窃取します。また、その痕跡をわからなくする技術で、感染していても気づかないケースもかなり多いと言われています。



出典：IPA 2014年度情報セキュリティ事象被害状況調査－報告書－

ターゲットに感染させるために、関係先の名前で、注文書などの添付ファイルやリンク付きビジネスメールを装った巧妙な手口で攻撃してきます。また、調査によると、それらのメールの開封率は約20%で１時間以内に開封されました。さらに役員の開封率はその1.5倍と言われています。24時間後には約95%が開封されたという結果から、発見後の初期対応を迅速に行うことが、被害を広めないために重要となります。



出典：IPA 2014年度情報セキュリティ事象被害状況調査－報告書－