NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

企業における最近の被害動向

平成27年2月2日

NPO日本ネットワークセキュリティ協会
調査研究部会長
加藤雅彦

Agenda

- JNSAのご紹介
- 企業における最近の被害動向
  - 日常的に発生するサイバー攻撃
  - 多発するリスト型アカウントハッキング攻撃
  - 揺らぐ基盤ソフトウェアへの信頼
  - 止まらない個人情報の漏えい
    - 2013年 情報セキュリティインシデントに関する調査結果～個人情報漏えい編～
    - 2014年上期 情報セキュリティインシデントに関する調査結果速報
- サイバーセキュリティ「費用」から「投資」へ
  - 個人情報漏えい損害額の算出
  - 情報セキュリティ市場規模の推定
- まとめ

JNSAのご紹介

NPO日本ネットワークセキュリティ協会

- 名称　特定非営利活動法人 日本ネットワークセキュリティ協会
  ＪＮＳＡ　（Japan Network Security Association）
- 設立　2000年4月（任意団体として発足、NPO法人化は2001年）
- 会員数　162社（2015年1月現在）主に情報セキュリティベンダー
- 住所　本部　東京都港区西新橋
  西日本支部　大阪府大阪市淀川区西中島
- ＵＲＬ　http://www.jnsa.org/
- メール　sec@jnsa.org
- 役員
  - 会長　田中 英彦（情報セキュリティ大学院大学　学長）
  - 副会長　中尾 康二（ＫＤＤＩ株式会社）
  - 高橋 正和（日本マイクロソフト株式会社）
  - 事務局長　下村 正洋（株式会社ディアイティ）

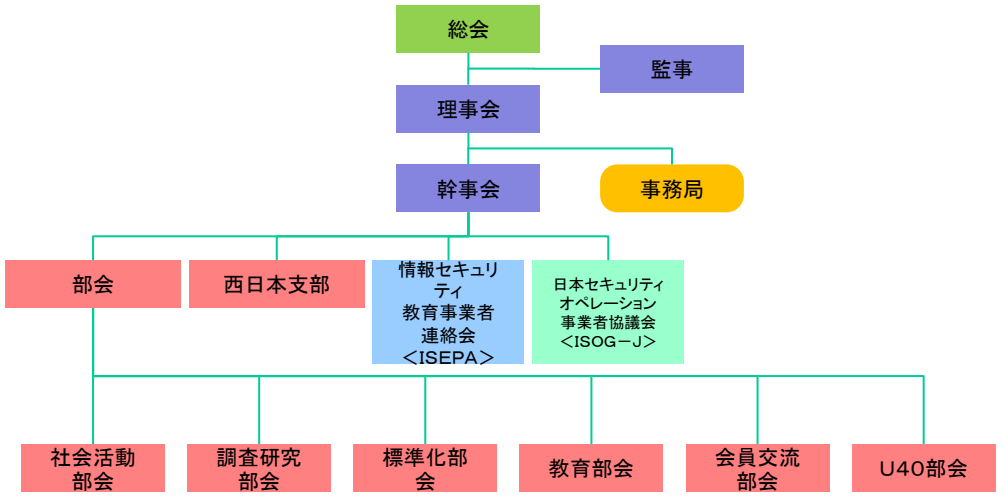
NPO日本ネットワークセキュリティ協会

設立

社会インフラとしてのインターネット普及と情報ネットワーク社会の形成を背景に、ネットワークセキュリティシステムに携わるベンダーによる団体として2000年設立。2001年に特定非営利活動法人（NPO）として認可。

活動の目的

- ネットワーク社会の情報セキュリティレベルの維持・向上
- 日本における情報セキュリティ意識の啓発
- 最新の情報セキュリティ技術および脅威に関する情報提供など



（2015年1月）

会員企業

ネットワーク・セキュリティ製品を提供しているベンダー、システムインテグレータ、インターネットプロバイダーなど、約160社（2015年1月現在）

調査研究部会

活動目的:
被害調査および市場調査を2大事業として推進し、技術的研究としてIPv6などの新コンピューティング技術の調査研究、およびスマートフォン、SNSの安全な利用、内部犯行等に関する調査研究を行う。

・セキュリティ被害調査WG　　リーダー:大谷 尚通 氏(株式会社NTTデータ)

個人情報漏えい編、発生確率編の調査を継続し、報告書を作成し公開する。2012年個人情報漏えい編、発生確率編、2013年個人情報漏えい編の調査報告書を作成し公開する。

「2013年 情報セキュリティインシデントに関する調査報告書」(公開中)
http://www.jnsa.org/result/incident/index.html

「2011年情報セキュリティインシデントに関する調査報告書～発生確率編～」(公開中)
http://www.jnsa.org/result/incident/2011_probability.html

2014年情報セキュリティインシデントに関する調査報告書」近日公開予定！！

・セキュリティ市場調査WG　　リーダー:木城 武康 氏(株式会社日立システムズ)

国内の情報セキュリティ市場の現況を調査・分析し、報告書を作成する。

「2013年度 情報セキュリティ市場調査報告書」(公開中)
http://www.jnsa.org/result/2014/surv_mrk/index.html

調査研究部会

JNSA

その他のWG

・組織で働く人間が引き起こす不正・事故対応WG　リーダー：甘利 康文 氏（セコム株式会社）
IPA「組織における内部不正防止ガイドライン」の各章に対応した製品・サービスを掲載した
「内部不正対策ソリューションガイド」を公開
http://www.jnsa.org/result/2013/surv_acci/index.html

・IPv6セキュリティ検証WG　　リーダー：許　先明 氏

・スマートフォン活用セキュリティポリシーガイドライン策定WG
リーダー：栃沢 直樹 氏（トレンドマイクロ株式会社）

・SNSセキュリティWG　　リーダー：高橋 正和 氏（日本マイクロソフト株式会社）

・シンギュラリティ調査WG　リーダー：広口 正之 氏（リコージャパン株式会社）

・IoTセキュリティWG　　リーダー：兜森 清忠 氏（株式会社シマンテック）
・脅威を持続的に研究するWG　　リーダー：大森　雅司氏（株式会社日立システムズ）

各WGの活動内容については
http://www.jnsa.org/active/2014/surv.html
をご覧ください

Agenda

- JNSAのご紹介
- **企業における最近の被害動向**
  - **日常的に発生するサイバー攻撃**
  - **多発するリスト型アカウントハッキング攻撃**
  - **揺らぐ基盤ソフトウェアへの信頼**
  - **止まらない個人情報の漏えい**
    - **2013年 情報セキュリティインシデントに関する調査結果～個人情報漏えい編～**
    - **2014年上期 情報セキュリティインシデントに関する調査結果速報**
- サイバーセキュリティ「費用」から「投資」へ
  - 個人情報漏えい損害額の算出
  - 情報セキュリティ市場規模の推定
- まとめ

企業における最近の被害動向
日常的に発生するサイバー攻撃

最近のセキュリティ事件（2014/1～3）

月	日	内容
1	2	US-CERTは、12月に発覚した大手小売り事業者の情報流出の原因となったPOS端末に感染するマルウェアについて、注意喚起を行った。
	4	複数のオンラインゲームで、何者かによるDDoS攻撃が行われ、サービス停止などの影響が出た。この攻撃は特定の利用者に対する攻撃の可能性が指摘されている。
	6	独立行政法人日本原子力研究開発機構は、高速増殖炉もんじゅの事務処理用パソコン1台がウイルスに感染し、情報流出の可能性があることを公表した。 米国のY社は、年末年始の期間中に欧州の自社サイトに配信した広告のいくつかで不正サイトからのマルウェアへの誘導が行われていたことを公表した。
	8	韓国で、大手クレジットカード3社から延べ8,500万件のクレジットカード情報が、カード会社と契約していた信用情報会社の社員により流出していたことが発覚した。
	11	大手オンラインストレージサービスのD社でメンテナンス時の不具合により、2日間に渡るサービス障害が発生した。
	15	S社は、日本の大手出版社のWebサイトが改ざんされ、Toolkitによる不正サイトからのマルウェアへの誘導が行われていたことを発表した。
	31	米国Y社のメールサービスで一部アカウントに対するリスト型攻撃による不正ログインが発生した。
2	3	航空会社の会員向けWebサイトで不正アクセスが発生し、通信販売サイトのポイントに交換される事件が発生した。 東京大学 国際高等研究所 カブリ数物連携宇宙研究機構で、スーパーコンピュータシステムが外部からの不正アクセスを受けたことを公表した。この事件では侵入されたシステムを通じ て、共同研究を行っていた国立天文台など、外部の研究機関への不正アクセスも確認されたことから各研究機関で対応が行われた。
	6	独立行政法人 国立がん研究センターは、国立がん研究センター東病院のパソコン2台がウイルス感染し、患者情報などが漏えいした可能性があることを公表した。
	7	Bitcoinの取引所の1つであるMt. Goxは、技術トラブルを修正するためとしてビットコインの払い出しを一時停止した。この後、2月28日にサイバー攻撃によるBitcoinと銀行預金の流出のため、債務超過に陥ったとして、民事再生手続きを申請した。
	12	Bitcoin取引所のMtGoxやBitStampなどが、トランザクション展性を悪用した取引妨害攻撃を受けたとして口座からの引き出しを一時停止した。この影響でBitcoinの対ドルレートが一時急落するなどの影響が出た。
	18	検索サイトの検索連動型広告を悪用し、複数の金融機関の偽サイトへの誘導が行われていたことが発覚し、対応が行われた。
	24	H社は、提供しているサービスに対して、外部から不正ログインされた可能性があるとしてパスワード変更や登録内容の確認を行うよう注意喚起を行った。
3	10	別の航空会社の会員向けWebサイトで不正ログインが発生し、マイルを別のポイントに交換される事件が発生したことを公表した。
	12	CMSであるWordPressで投稿にリンクが張られたことを知らせるPingback機能を悪用した大規模なDDoS攻撃が発生した。
	17	ブラジルとベネズエラでGoogle Public DNSの経路が一時的にBGPハイジャックされる事件が発生した。

IIJ Internet Infrastructure Review(IIR) Vol.23を元に作成。（http://www.iij.ad.jp/company/development/report/iir/023.html）
IIRに各インシデントの参照情報（URL等）が記載されている。詳細はそちらを確認のこと。

最近のセキュリティ事件（2014/4～6）

月	日	内容
4	15	カナダ歳入庁のWebサイトに対して、OpenSSLの脆弱性（CVE-2014-0160）を悪用した攻撃が発生し、納税者およそ900人分の社会保障番号が漏えいしたことを発表した。なお、4月17日に学生が容疑者として逮捕された。
	16	国立感染症研究所は、Webメールの管理者を騙ったメールによって、メールアカウントのユーザ名とパスワードが盗取され、迷惑メールが送信されたことを公表した。
5	15	JPCERTコーディネーションセンターは、Movable Typeの既知の脆弱性を使用した攻撃により、不正なファイルが設置されたり、攻撃サイトへと誘導するiframeや難読化されたJavaScriptが 埋め込まれたりする事件が多く確認されているとして注意喚起を行った。
	20	FBIは、ファイルやアカウント情報を盗むRAT Blackshadesに関わったとされる、共同作成者を含む100人以上を逮捕したことを発表した。
	27	オーストラリアなど複数の国で、A社製のスマートフォンが遠隔ロックされ、金銭を要求される事件が発生した。 この事件では、A社が提供しているスマートフォンを探す機能を悪用したと考えられているが手口の詳細については明らかになっていない。
	29	複数のプロバイダでDNSサーバへの問い合わせが急増したことによる障害が発生した。
6	3	5月後半から発生していた複数サイトの不正アクセスによるコンテンツやファイルの改ざん事件について、利用していたCDNサービスの提供事業者が不正侵入を受けたことによるものと判明した。 米司法省は、オンラインバンキングなどの情報窃取を行うマルウェアであるGameOver Zeusについて、10ヵ国以上の法執行機関と共同でテイクダウンを実施し、関連サイトの差し押さえや管理者の逮捕などが行われたことを公表した。
	12	サポート終了となった日本独自のブログ作成ツールについて、約8割が問題のある状態で運用されており、攻撃者の標的になっているとして注意喚起が行われた。
	13	香港の民主化を求めて活動する団体の電子投票システムに対する大規模なDDoS攻撃が発生した。
	19	広告配信サーバによって、Adobe Flash Playerの更新を促す通知に見せかけた悪意あるサイトに誘導する広告が表示される事件が発生した。
	30	Microsoft社は、Bladabindi（NJrat）とJenxcus（NJw0rm）の2つのマルウェアファミリーが利用していたダイナミックDNSサービスであるNO-IPの23ドメインについて、テイクダウンを実施したことを公表した。

IIJ Internet Infrastructure Review(IIR) Vol.24を元に作成。（http://www.iij.ad.jp/company/development/report/iir/024.html）
IIRに各インシデントの参照情報（URL等）が記載されている。詳細はそちらを確認のこと。

最近のセキュリティ事件（2014/7～9）

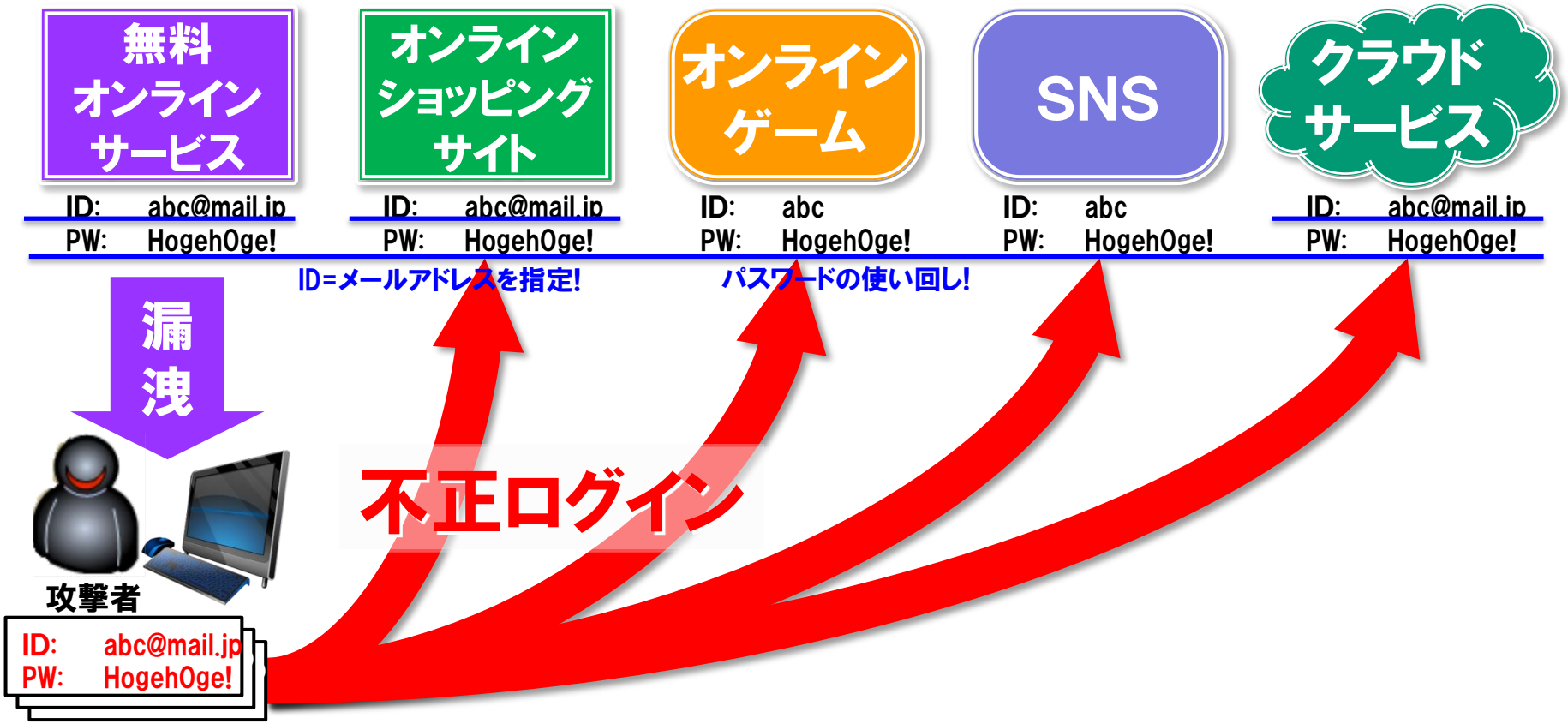
月	日	内容
7	9	通信教育企業は、同社の約2070万人分の顧客情報が名簿業者など外部に流出したことを公表した。その後、9月に公表された最終報告では約4858万人分の個人情報が漏えいしたことが判明している。
	9	インド政府のルート認証局の傘下で中間認証局を運営するインド国立情報工学センター（NIC）で複数のGoogleドメインやYahoo!ドメインの証明書が不正に発行されたことが判明し、複数のブラウザで当該証明書を無効にする対応が行われた。原因については証明書発行プロセスが破られたためとされている。
	17	通信教育企業の顧客情報が外部に漏えいした事件について、業務委託企業の元派遣社員が不正競争防止法違反（営業秘密の複製）の容疑で逮捕された。
	18	一般財団法人日本データ通信協会テレコム・アイザック推進会議は、インターネットバンキングに係るマルウェア（Game Over Zeus）の国際的な感染駆除作戦に関連し、官民連携による国民のマルウェア対策支援プロジェクト（ACTIVE）を通じて、該当マルウェアに感染している利用者への注意喚起を実施することを発表した。
	24	欧州中央銀行は、Webサイトに侵入され、イベント登録者の電子メールアドレスなどの個人データが漏えいしたことを公表した。この事件は漏えいしたデータと引き換えに金銭を要求する匿名のメールが届いたことから発覚した。
	25	国内の複数の企業や行政機関より、自サイトのホームページを模倣したWebサイトに対する注意喚起が相次いで行われた。
8	1	US-CERTは、POSシステムを対象とした新種の不正プログラムBackoffが確認されたとして、注意喚起を行った。
	2	Mozilla Developer Networkは、データベースダンプファイルが誤って公開状態になっていたことから、7万6千のMDNユーザのメールアドレスと4,000ユーザの暗号化されたパスワードが漏えいした可能性があることを公表した。
	4	各国の政府機関が情報収集活動に利用しているとされる商用監視ソフトウェアFinSpy（FinFisher）について、提供元企業が不正アクセスを受け、40GBにもなる内部文書とソースコードが公開された。
	8	米国のセキュリティ企業より、2014年2月から5月にかけて、BGPハイジャックにより、仮想通貨のマイニングプールへのトラフィックを偽のマイニングプールに振り向ける攻撃が行われていたことが報告された。この攻撃では、19のISPが影響を受けたとされており、攻撃者は8万3000ドルの利 益を得ていた可能性があることが指摘されている。
	12	米国で、インターネットの速度が低下したり、通信が不安定になるなどの現象が発生した。原因については、広報されたBGPの経路情報が、古いルータでBGPのルーティングテーブルの上限である512kを超えたためと考えられる。
	13	テキスト編集ソフトの日本語と簡体字中国語のサポートサイトが改ざんされ、利用者のユーザ名、パスワード、IPアドレスを盗もうとする痕跡が見つかったことが公表された。その後、8月18日に再度Webサイトが改ざんされ、当該シェアウェアの更新チェック機能を利用して悪意あるファイルがインストールされる事件も発生している。
	21	米国U社は、国内の51ヵ所の代理店でマルウェア感染が確認され、顧客のクレジットカード情報などが流出した可能性があることを公表した。
	25	何者かによって、S社が提供するネットワークサービスへのDDOS攻撃が行われ、大規模な障害が発生した。
9	1	米国で、ハリウッド女優などのプライベート写真が、掲示板に掲載される事件が発生した。この事件は、流出した複数の著名人のiCloudアカウントに不正アクセスが行われたことが原因とされている。
	3	米国の小売り大手であるH社で大規模なカード情報の流出が発生した。
	18	ゲームサーバにDDoS攻撃を複数回行い、ゲーム会社の業務を妨害したとして高校生が電子計算機損壊等業務妨害容疑で書類送検された。
	24	航空会社でマルウェア感染による不正アクセスが発生し、最大で73万件の会員の個人情報が漏えいした可能性があることが公表された。
	26	物流事業者のサポートサイトへパスワードリスト攻撃と考えられる不正ログインがあり、一部の会員の個人情報が閲覧されることで漏えいした可能性があることが公表された。同様の事件は28日に別の物流事業者のサポートサイトでも発生している。

IIJ Internet Infrastructure Review(IIR) Vol.25を元に作成。（http://www.iij.ad.jp/company/development/report/iir/025.html）
IIRに各インシデントの参照情報（URL等）が記載されている。詳細はそちらを確認のこと。

企業における最近の被害動向
多発するリスト型アカウントハッキング攻撃

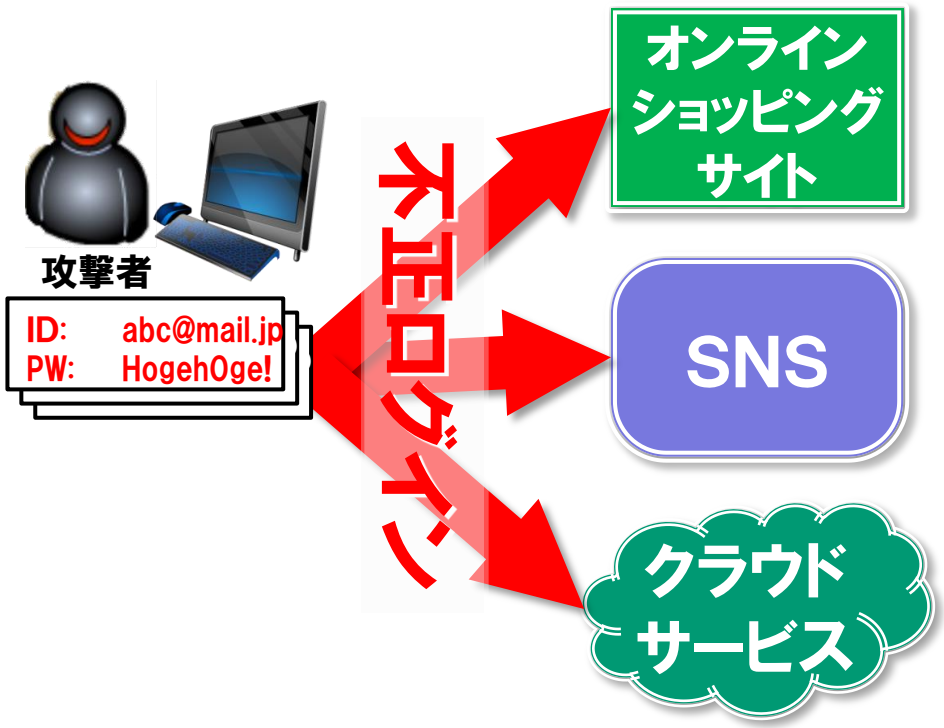
リスト型アカウントハッキング攻撃

同じID、パスワードを使い回しているアカウントを狙った不正ログイン攻撃



リスト型アカウントハッキングの被害例

リスト型アカウントハッキングが成功してアカウントへ不正アクセスされてしまった場合の被害



乗っ取ったアカウントを使って
換金性の高い商品を不正購入

乗っ取ったアカウントの友人から
電子マネーをだまし取る

乗っ取ったアカウントを使ってCPUリソースを不正利用したり、攻撃の踏み台や水飲み場型攻撃用のWebページやC&Cサーバに使う

2013年 個人情報漏洩インシデント・トップ10

JNSA

2013年は
不正アクセスが
急増！

No.	漏えい人数	業種	
1	400万人	情報通信業	不正アクセス
2	169万2496人	情報通信業	不正アクセス
3	47万人	卸売業，小売業	不正アクセス
4	42万6000人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24万3266人	情報通信業	不正アクセス
6	17万5297人	情報通信業	設定ミス
7	15万0165人	卸売業，小売業	不正アクセス
8	12万0616人	金融業，保険業	管理ミス
9	10万9112人	情報通信業	不正アクセス
10	9万7438人	情報通信業	不正アクセス

リスト型アカウントハッキング攻撃

リスト型アカウントハッキングの対策案

リスト型アカウントハッキングによって不正ログインされないためには

- パスワードを使いまわさない。同じパスワードを使わない
- 2要素認証など、不正アクセス対策がしっかりしたサービスを積極的に利用する

2要素認証
リスト型アカウントハッキングで
1段階目の認証を突破されても
2段階目の認証を突破できない

- 解読されやすい秘密の質問を使用しない

例）母親の旧姓は？　＝鈴木
　　出身地は？　　＝東京

- ログインできる端末やIPアドレスを限定する（可能な場合）
- 設定ミスに気をつける（クラウドサービスの場合など）

企業における最近の被害動向
揺らぐ基盤ソフトウェアへの信頼

基盤となるソフトウェアの脆弱性

- Heartbleed
  - 暗号化通信で広く用いられているソフトウェアであるOpenSSLにおいて、ハートビート処理の実装に問題があり、細工したデータをリクエストとして送ることにより、本来読み出せないプロセスのメモリ領域をレスポンスに含めさせることが可能となる脆弱性が発見された
    - IIJ Internet Infrastructure Review(IIR) Vol.24より引用
      http://www.iij.ad.jp/company/development/report/iir/024/01_04.html
  - 対策は修正済バージョンへのアップデート
  - 対象は下表のとおりだが・・・

※詳細はOpenSSL公式サイトや各脆弱性情報提供サイト等を参照

実装	脆弱性
OpenSSL1.0.1系	影響あり
OpenSSL1.0.0系	影響なし
OpenSSL0.9.8系	影響なし
他の実装	影響なし

基盤となるソフトウェアの脆弱性

- CCS Injection
  - OpenSSLのChangeCipherSpecメッセージの処理に欠陥が発見されました。この脆弱性を悪用された場合、暗号通信の情報が漏えいする可能性があります。
    - 株式会社レピダム「OpenSSL #ccsinjection vulnerability」より引用
      http://ccsinjection.lepidum.co.jp/ja.html
  - 本脆弱性による MITM 攻撃では、サーバとクライアントの両方が OpenSSL を使っている場合に、その間にいる攻撃者が SSL/TLS ハンドシェーク中に特別なメッセージを割り込ませることで、攻撃者にも計算できる鍵を両者の暗号化通信に使わせることができます。攻撃者はその鍵を使って暗号化通信を復号でき、通信内容の盗聴、改ざんが可能になります。この攻撃を受けた状況でも、サーバとクライアントでは通常どおりの暗号化通信として認識され、異常に気づくことができません。
    - IIJ Security Diary「OpenSSL の Man-in-the-middle 攻撃可能な脆弱性の影響」より引用
      https://sect.iij.ad.jp/d/2014/06/069806.html
  - 対策は修正済バージョンへのアップデート
  - 対象はバージョンに依存（次ページ参照）

    ※詳細はOpenSSL公式サイトや各脆弱性情報提供サイト等を参照

基盤となるプロトコルの脆弱性

- POODLE Attack
  - POODLE Attackと呼ばれる本手法はBEAST攻撃に類似した中間者攻撃でブラウザから大量のリクエストをサーバに送りつけることによるトライ＆エラーを繰り返すことでSSLで暗号された攻撃対象データを1バイトずつ復号することを可能にしています．現実的な攻撃としてはCookieの搾取が挙げられます
    - 暗号プロトコル評価技術コンソーシアム（CELLOS）「[2014/10/15] SSLv3仕様そのものに対する POODLE attack について」より引用
      https://www.cellos-consortium.org/jp/index.php?PoodleAttack_20141015_J
  - 対策はSSLv3の無効化など
  - 対象は・・・SSLv3を使用可能としているデバイス全て
    ※詳細は各脆弱性情報提供サイト等を参照

基盤となるソフトウェアの脆弱性

- Shellshock
  - GNU bash の脆弱性 ～ shellshock 問題～ は、Linux で使用するシェルのひとつである GNU bash (Bourne-Again Shell) の環境変数の処理に存在する任意のコード実行などを許してしまう脆弱性です。Web サーバ上で動作する CGI プログラムや Linux ベース組み込みシステムなど、非常に広範囲にわたって影響を与えるものです。
    - 日本シーサート協議会「GNU bash の脆弱性 ～ shellshock 問題～ について」より引用
      http://www.nca.gr.jp/2014/shellshock/
  - 対象はbash・・・を使っているプログラムすべて
  - 対策は修正済みバージョンへのアップデート
    ※詳細は各脆弱性情報提供サイト等を参照

最近の問題における特徴

- 正規アカウントの悪用など、対象が幅広く、検出や対策が難しい攻撃が数多く発生している
  - ID/パスワードを使ってログインする仕組みがあれば、リスト型パスワードハッキングの攻撃対象となる可能性がある
- インターネットの基盤として広く使われている、オープンソースソフトウェアでもいまだに新しい脆弱性が発見される
  - 安全という認識で広く長く使われているものが、ある日突然危険になる
  - 既に数多くの組み込み機器にインターネット関連技術が使われており、パソコンやスマホだけがセキュリティ対策の対象ではない。同様の技術を使っていればIoTデバイスなども対象となる
  - 長期間にわたって対応が発生することを想定する必要がある

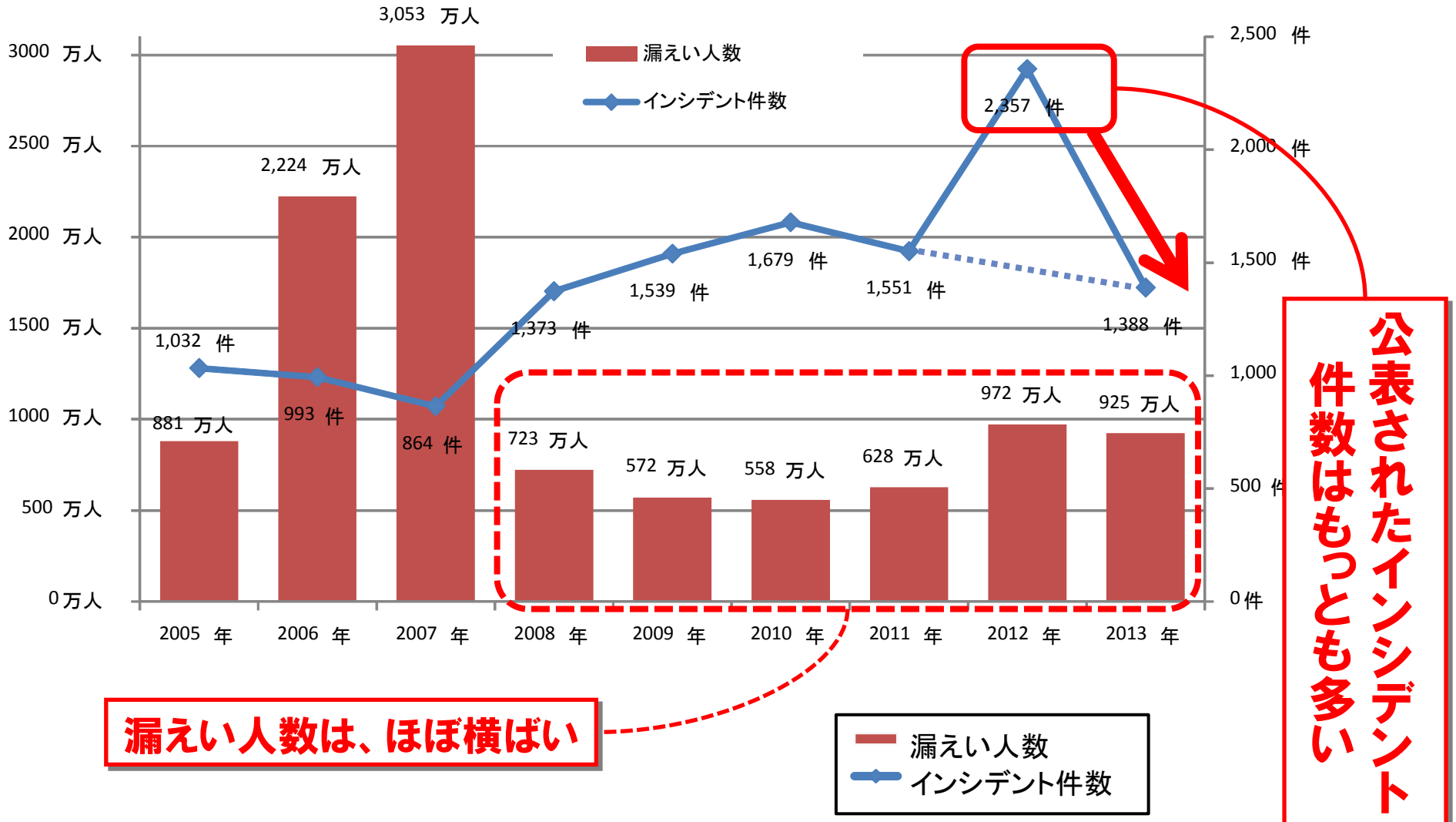
どこからでも攻撃されやすく、問題発生時の影響が大きい。
長期の対応を前提としたセキュリティ対策が不可避

企業における最近の被害動向

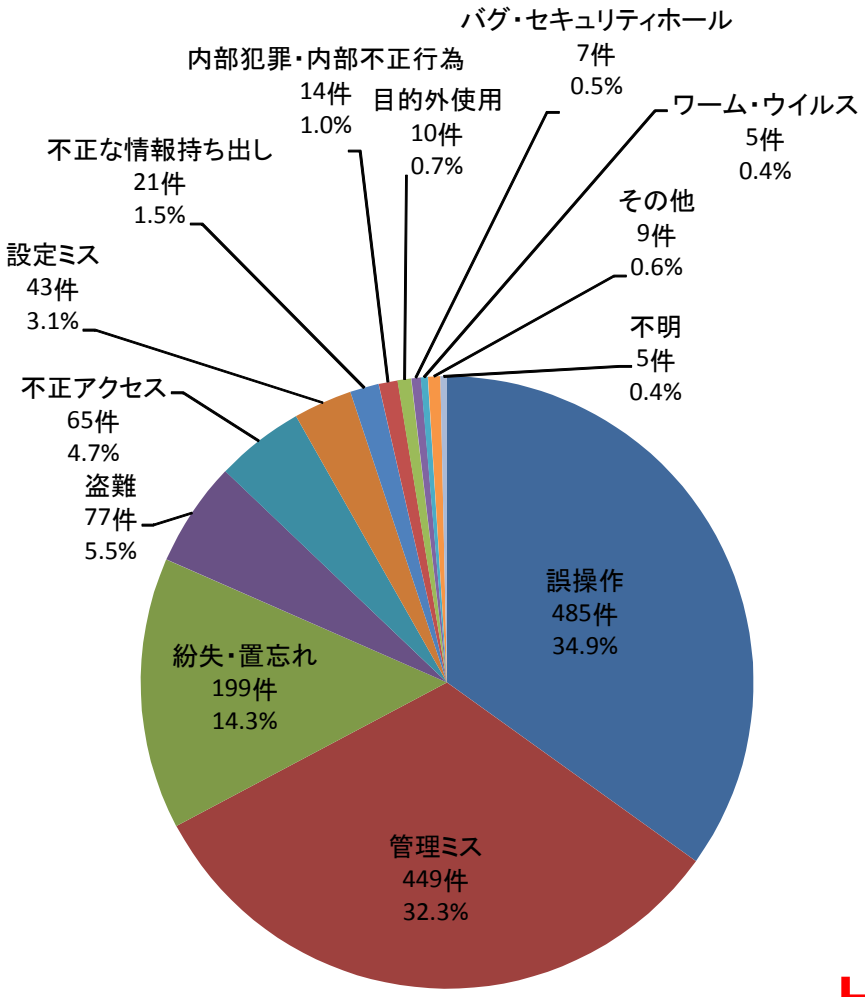
止まらない個人情報の漏えい

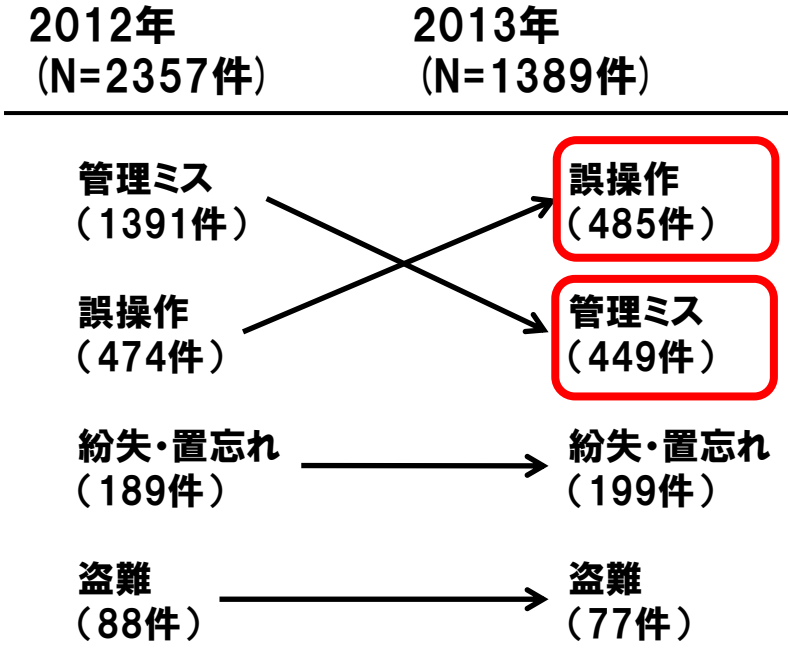
2013年 情報セキュリティインシデントに関する調査結果 ～個人情報漏えい編～より

漏えい人数と件数（経年）



原因別の漏えい件数

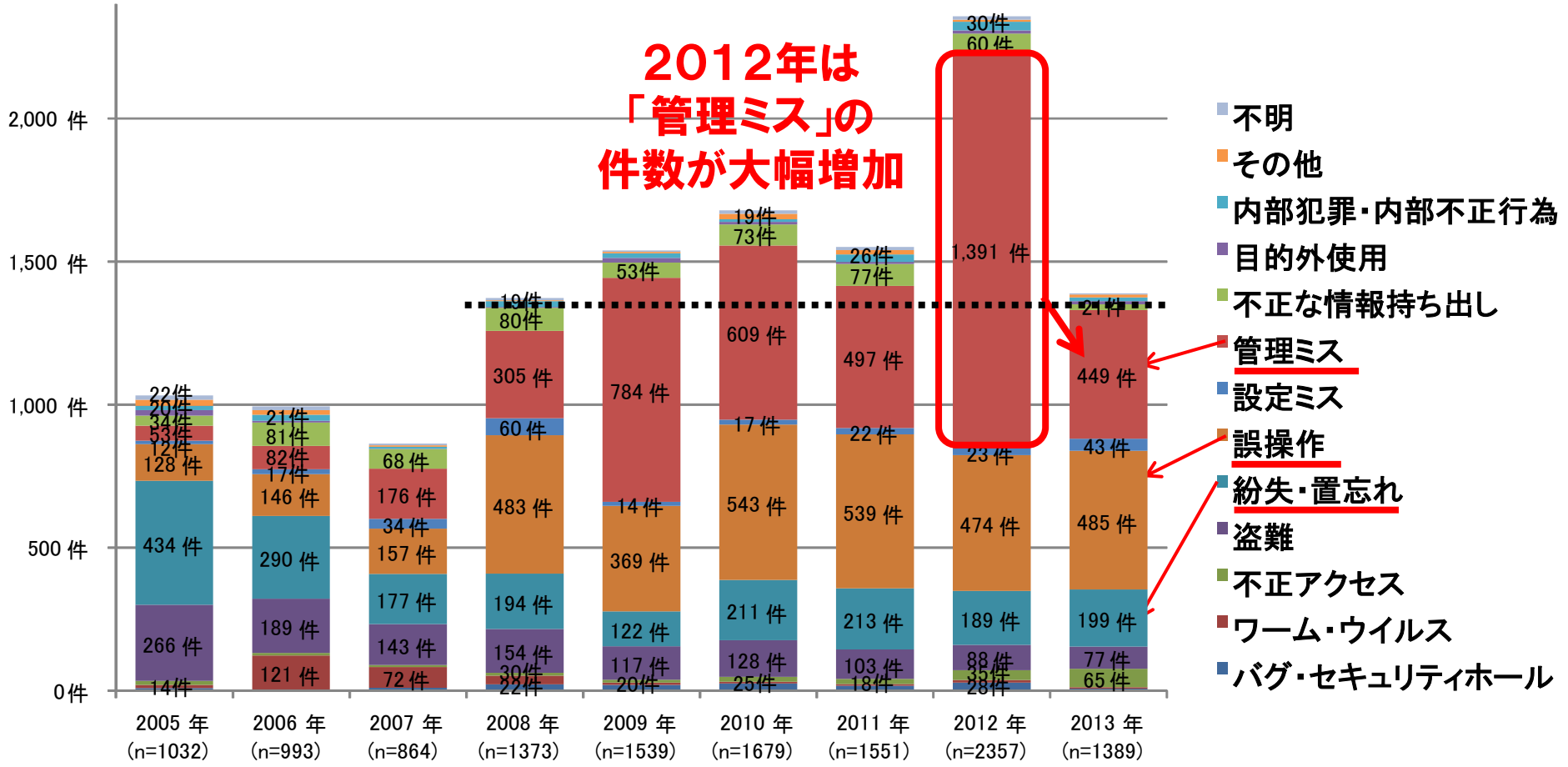




管理ミス(＝誤廃棄)
誤操作(＝ケアレスミス)
による漏えいが多い

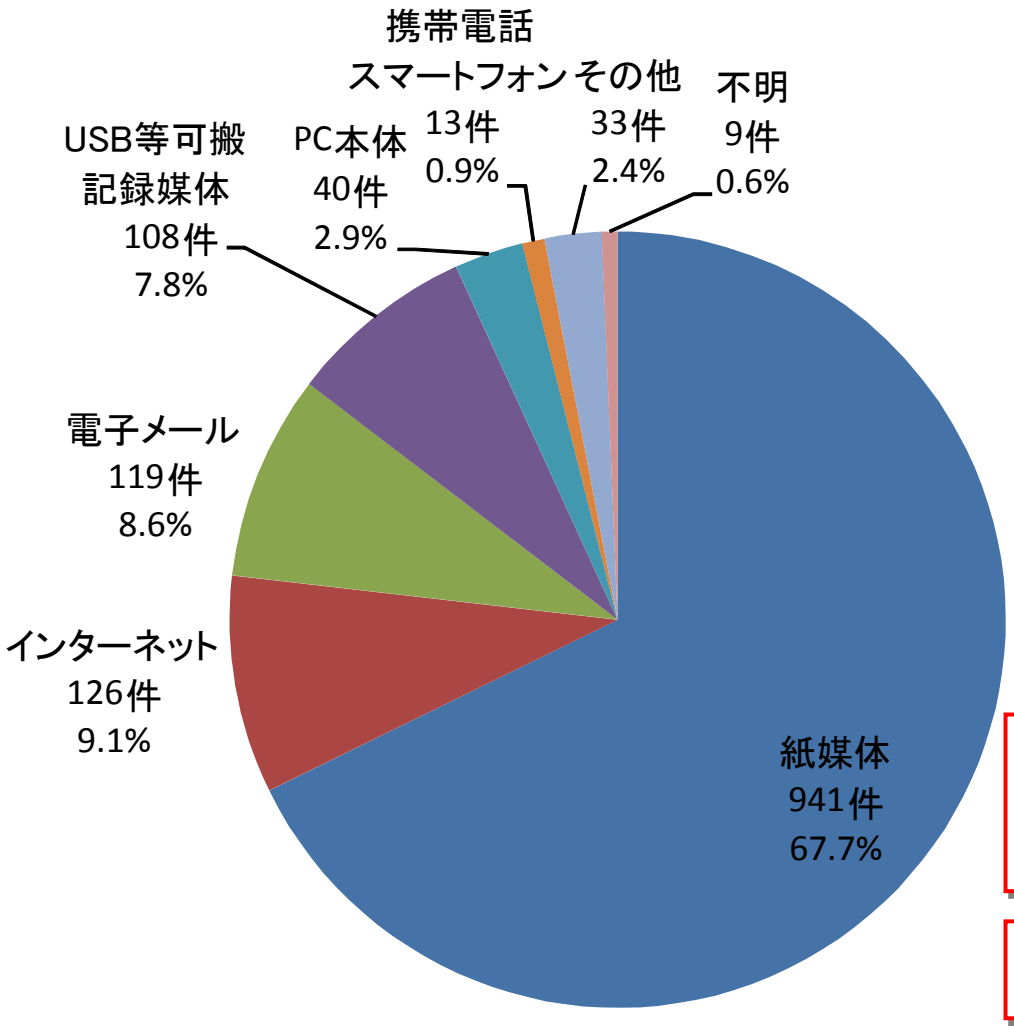
上位の原因に大きな変化はなし

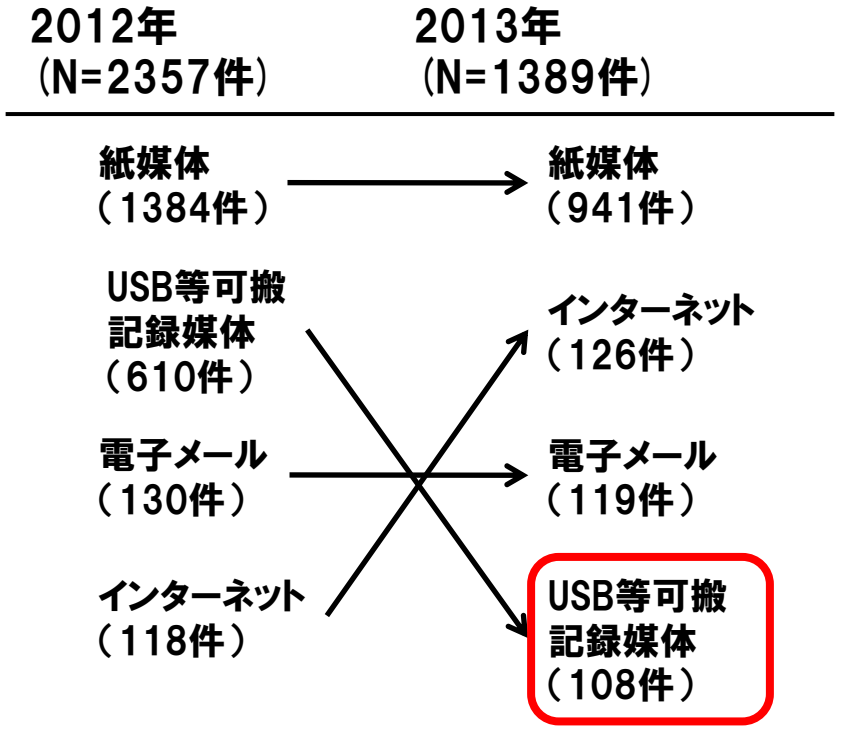
原因別の漏えい件数（経年）



インシデントの3大要因は人為的ミス
「管理ミス」「誤操作」「紛失・置忘れ」

媒体別の漏えい件数

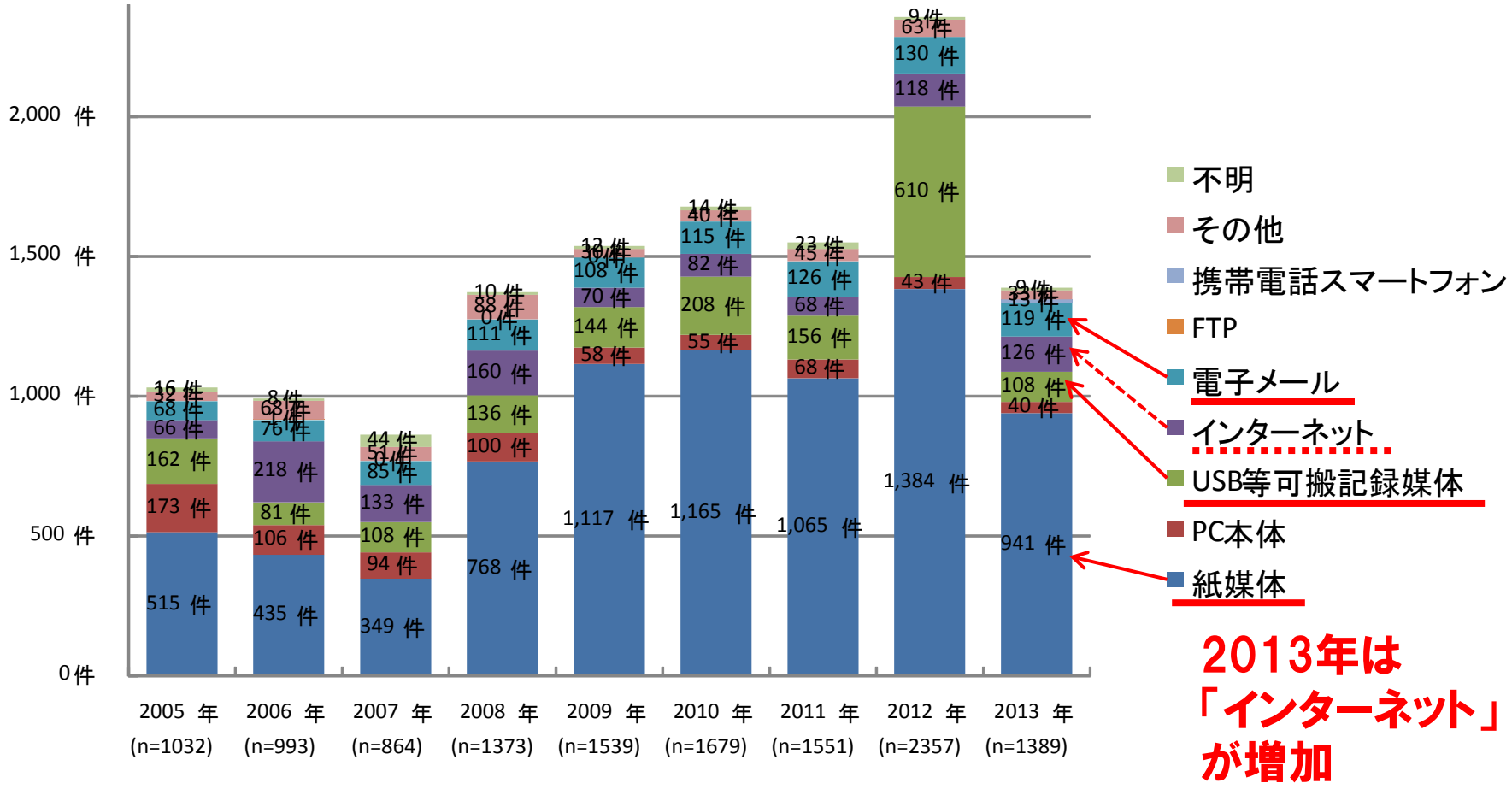




紙媒体による漏えいが多い。（例年通り）

USBが大幅減少

媒体別の漏えい件数(経年)



例年、紙媒体による漏えいが多い
次に「USBメモリ」「電子メール」が多い

全組織の共通問題「人為的ミス」

JNSA

管理ミス、誤操作、紛失・置き忘れの人為的ミスによる情報セキュリティインシデントは、毎年件数が多く、高い割合を占める

インシデントの3大要因は人為的ミス
「管理ミス」「誤操作」「紛失・置き忘れ」

人為的ミス	2008年	2009年	2010年	2011年	2012年	2013年
インシデント件数 (%)	982件 (71.5%)	1275件 (82.8%)	1363件 (81.2%)	1249件 (80.5%)	2054件 (87.1%)	1071件 (80.3%)
インシデント人数 (%)	516.7万人 (71.4%)	269.6万人 (47.1%)	149.5万人 (26.8%)	256.0万人 (40.7%)	805.3万人 (82.8%)	157.3万人 (17.0%)

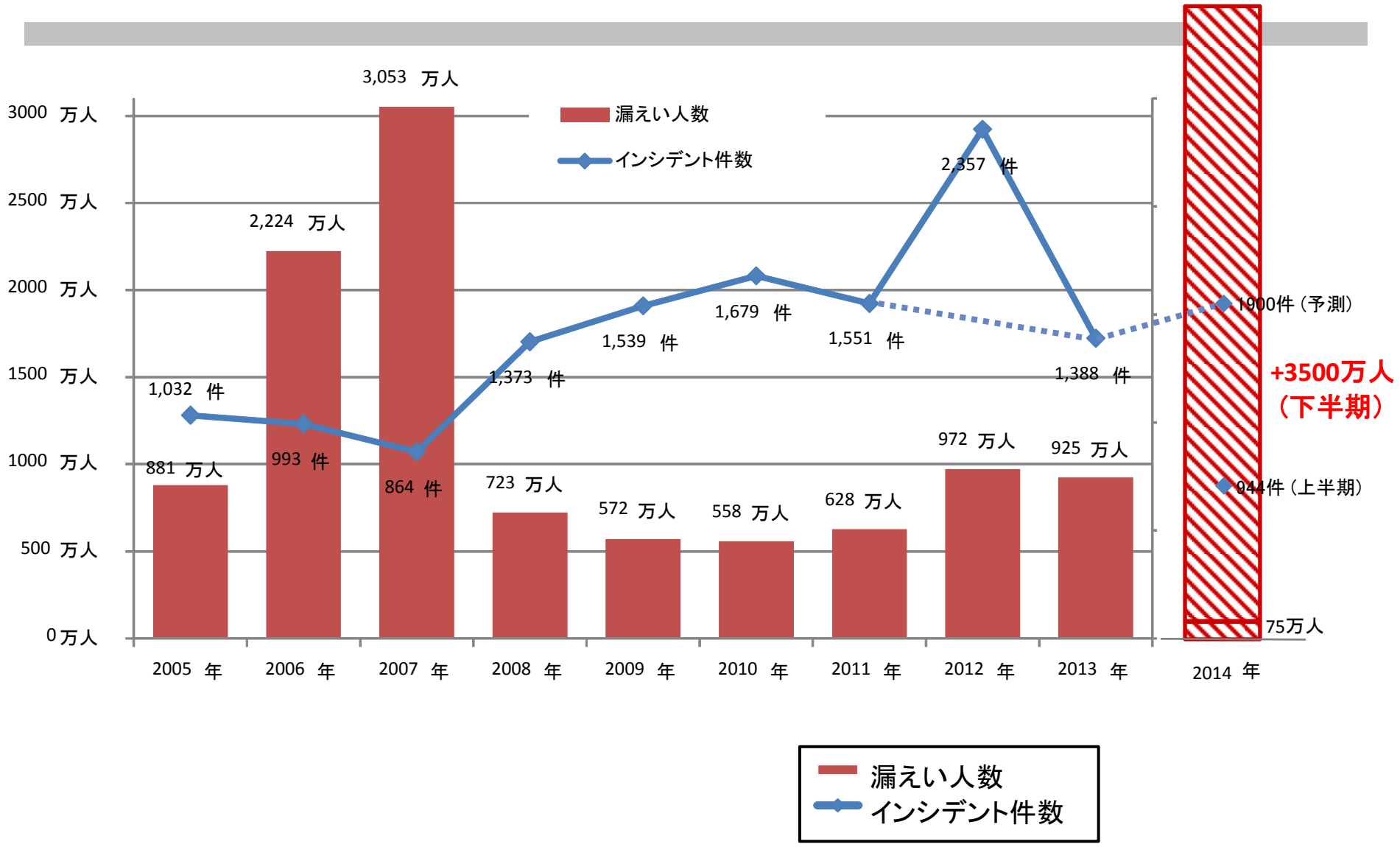
インシデント人数のばらつきが大きい
1件あたりの漏えい人数は少ない

人為的ミスの対策が必要！
（ヒューマンエラー）

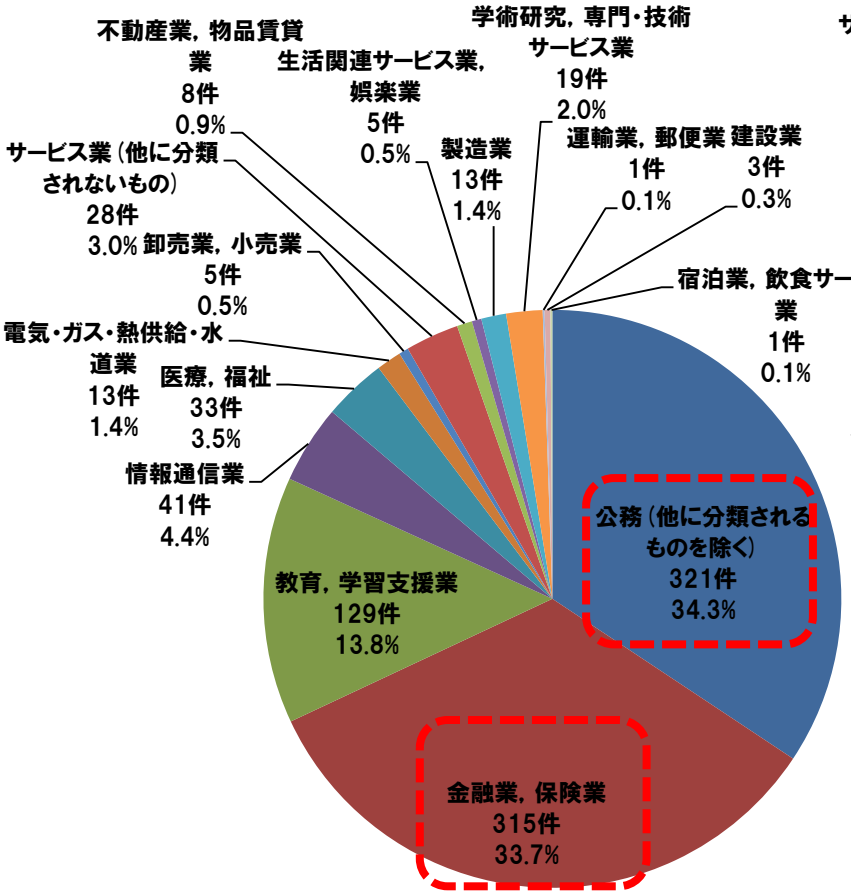
企業における最近の被害動向
止まらない個人情報の漏えい

2014年上期 情報セキュリティインシデントに関する調査結果 速報

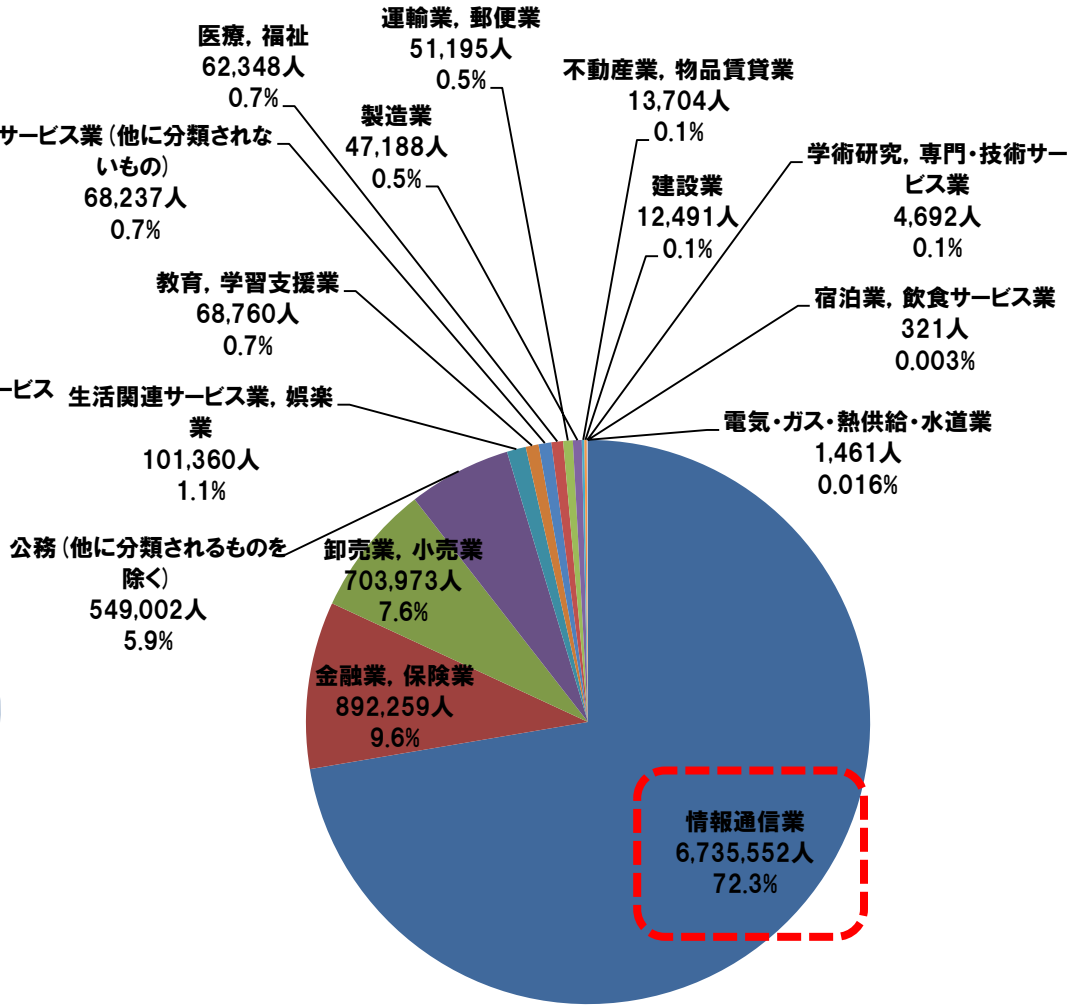
漏えい人数と件数（経年）



業種別（件数／人数）2014年上期速報

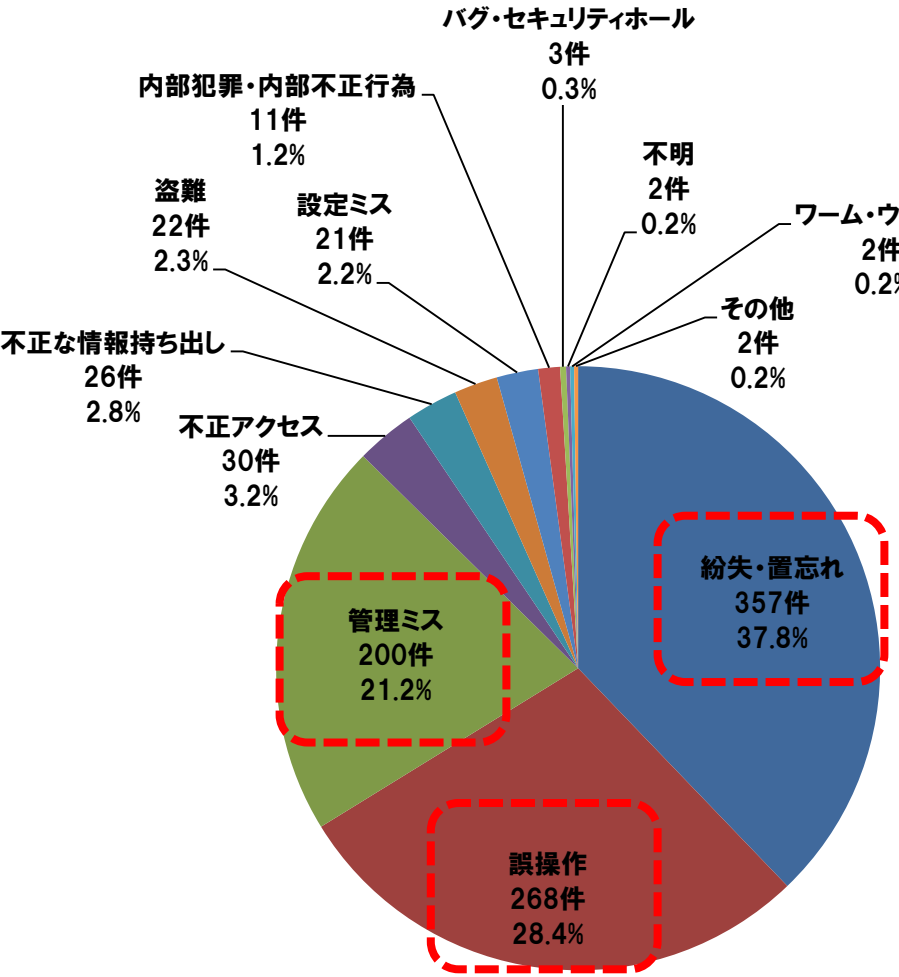


業種別（件数）

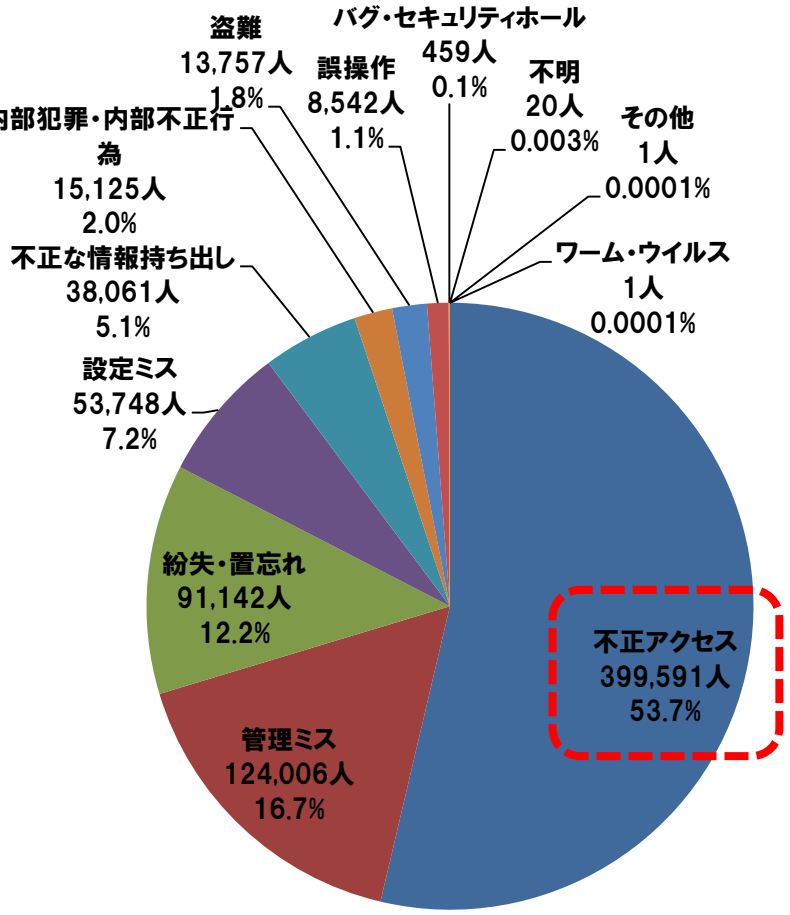


業種別（人数）

原因別（件数／人数）2014年上期速報

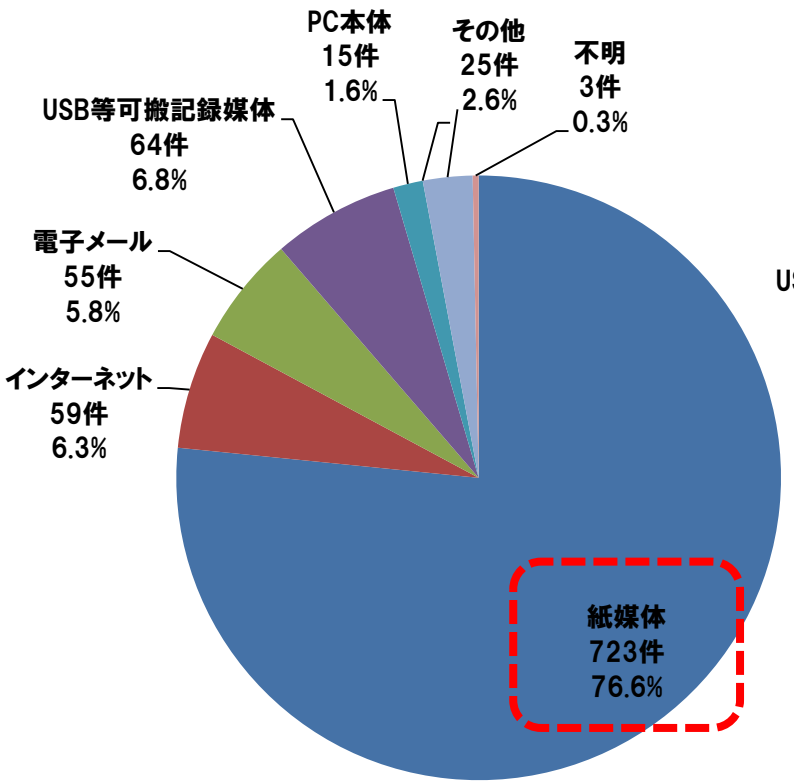


原因別（件数）

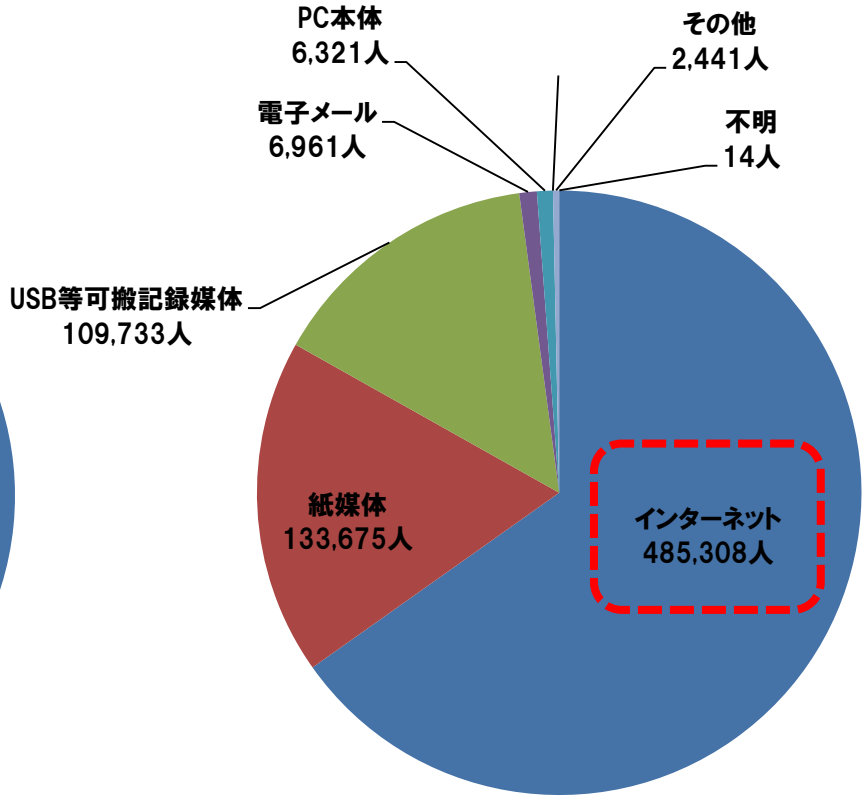


原因別（人数）

経路別（件数／人数）2014年上期速報



経路別（件数）



経路別（人数）

2014年の特徴

- 個人情報漏えい業種を…
  - 件数でみると公務・金融・教育等が多い
  - 人数でみると情報通信業が約3/4
- 個人情報漏えい原因を…
  - 件数でみると紛失・誤操作・管理ミス等、ヒューマンエラー関連が多い
  - ところが人数で見ると不正アクセスが半数を占める
- 個人情報漏えい経路を…
  - 件数でみると紙媒体からの漏えいが圧倒的に多い
  - 一方人数で見るとインターネットからの漏えいが圧倒的に多い

インターネットからの不正アクセスによる情報漏えいはその影響が大きい。事前の対策は不可避

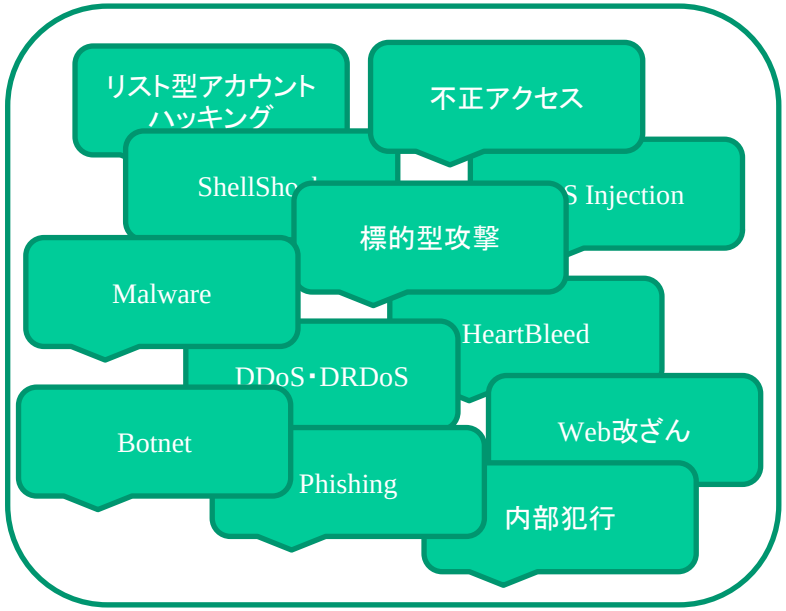
Agenda

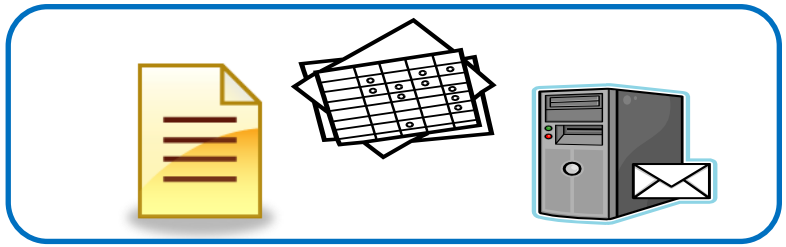
- JNSAのご紹介
- 企業における最近の被害動向
  - 日常的に発生するサイバー攻撃
  - 多発するリスト型アカウントハッキング攻撃
  - 揺らぐ基盤ソフトウェアへの信頼
  - 止まらない個人情報の漏えい
    - 2013年 情報セキュリティインシデントに関する調査結果～個人情報漏えい編～
    - 2014年上期 情報セキュリティインシデントに関する調査結果速報
- **サイバーセキュリティ「費用」から「投資」へ**
  - **個人情報漏えい損害額の算出**
  - **情報セキュリティ市場規模の推定**
- まとめ

サイバーセキュリティ
「費用」から「投資」へ

被害動向と「投資」

供給される数多くの脅威情報





自社の情報資産

こんなに危ないので対策が必要です！

対策する価値がどこまであるかわからなくても、対策することで安心感は得られる

定性的効果（費用）のよくあるパターン

影響の数値化

～の期間でいくら損しますよ
～の期間でいくら得しますよ

対策する価値があるかどうかを合理的に判断

定量的効果（投資）へのチャレンジ

※なお自動化の観点でSCAPなどセキュリティの定量化が行われているが
ここでは金額にして示す、と言う意味で数値化としている

本日のテーマ

- 「費用」から「投資」へ
  - サイバーセキュリティ対策は費用、が今までの認識
    - サイバーセキュリティ対策費は、問題の発生予防や回復を目的とした手段を入手するための支出でしかない
    - ともすれば消極的にとらえられがち
    - しかし、ICTの利活用と、サイバーセキュリティの考慮は切り離せないのが現状
  - ICTを利活用することがこれからの事業発展に欠かせないものとなっていくとするならば、サイバーセキュリティ対策も事業発展に欠かせないものとなっていくのではないか

本日のテーマ

- 「費用」から「投資」へ
  - 投資には将来的なリターン（利益）が必要
    - 投資対効果が測定可能でなければならない
    - 測定するためには投資の数値、利益の数値が必要
    - 投資の数値＝投資額、であれば利益も「金額」
  - 数値化に関わるチャレンジ
    - セキュリティ対策で「損害が軽減される」ことによる利益
    - セキュリティ対策を「販売する」ことによる利益
    - セキュリティ対策のおかげで「より売れる」ことによる利益

「費用」から「投資」へ
個人情報漏えい損害額の算出

セキュリティ被害調査WGによる損害額算出

JNSA

目的

- 情報セキュリティインシデントにおける被害の定量化
- 適切な情報セキュリティに対する投資判断、投資対効果の提示
  - 企業における情報セキュリティインシデントに係る被害額・投資額などの実態をアンケートやヒアリングによって調査した。この調査結果をもとに「情報セキュリティインシデントに関する被害額算出モデル」を策定
  - 一年間に報道された個人情報漏えいインシデント（事件・事故）を調査・分析し、「JOモデル（JNSA Damage Operation Model for Individual Information Leak）」を用いて想定損害賠償額などを推定し、報告書を公開

情報セキュリティ分野において
被害の定量化や投資対効果の
考え方をもっと普及・発展させたい

想定損害賠償額/算定式の注意点

想定損害賠償額算定式は、各組織が所有する個人情報の潜在的**リスクを把握するためのひとつの推定方法**である。

- 保有する個人情報によるリスクを定量化し、個人情報を取り扱う組織のリスクを把握するもの
- 算定結果は、対策するときの判断材料とするもの

想定損害賠償額は、あくまでも**「もし被害者全員が賠償請求したら」**という“仮定”に基づくものである。

- 実際に各事例においてその金額が支払われたものではない
- 被害者が漏えい元の組織に対して請求できる損害賠償額を示したものではない

参考：個人情報価値の算出式

漏洩個人情報価値＝基礎情報価値×機微情報度×本人特定容易度

■ **基礎情報価値 ： ＝500**

2003年6月、L社カードの会員56万人の個人情報が漏えい。同社は115万人全員に謝罪文と商品券500円分を郵送した。これにより「1人あたり500円の謝金を配る」とする対応が増えた。

■ **機微情報度 ：**
漏洩した個人情報に含まれる機微情報の量

機微情報度＝$(10^{x-1}+5^{y-1})$

Simple-EP図上の個人情報の座標値(x,y)より
x = 漏洩した情報の精神的苦痛レベルの最大値
y = 〃 経済的損失レベルの最大値

■ **本人特定容易度 ：**
漏洩した個人情報からの個人特定しやすさ

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

参考：Simple-EP図（評価尺度を3段階へ）

JNSA

個人情報の価値の評価尺度を3段階とし、基準判断を容易にしよう！

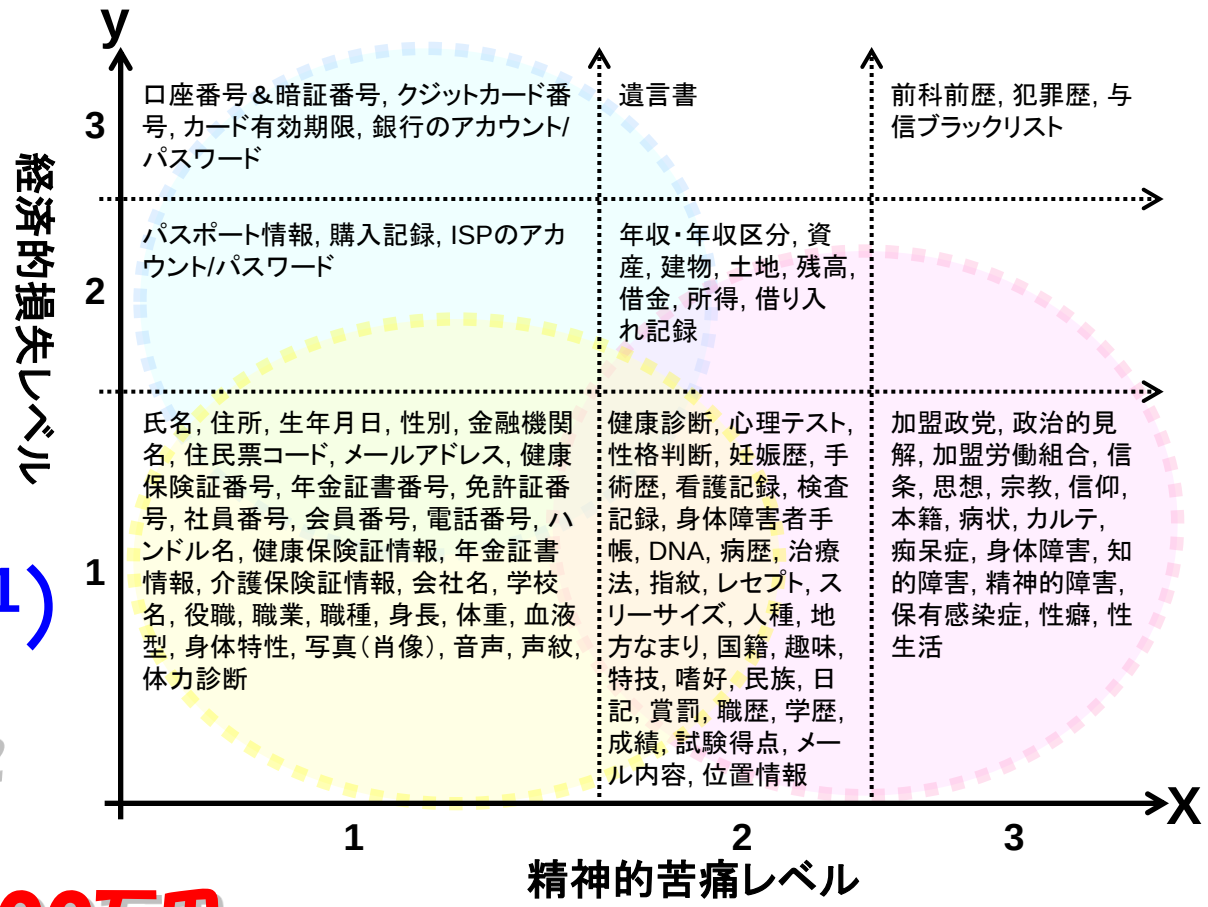
経済的損失
＝1～30万円

5^0～5^2

機微情報度
＝$(10^{x-1}+5^{y-1})$

10^0～10^2

精神的苦痛＝1～100万円



【Simple-EP図】

参考：想定損害賠償額の算定式（JOモデル）

JNSA

式や判定基準表を用いて、計算式への代入値を求めやすく。

損害賠償額

＝漏洩個人情報価値×社会的責任度×事後対応評価

＝（基礎情報価値×機微情報度×本人特定容易度）
×社会的責任度
×事後対応評価

＝基礎情報価値 [500]
×機微情報度 [Max（$10^{x-1}+5^{y-1}$）]
×本人特定容易度 [6,3,1]
×社会的責任度 [2,1]
×事後対応評価 [2,1]

基礎情報価値を一律500円（ポイント）と定義。

機微情報度 ＝（$10^{x-1}+5^{y-1}$）
x＝漏洩した情報の精神的苦痛レベルの最大値
y＝〃 経済的損失レベルの最大値

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所＋電話番号」が含まれること。	3
特定困難。上記以外。	1

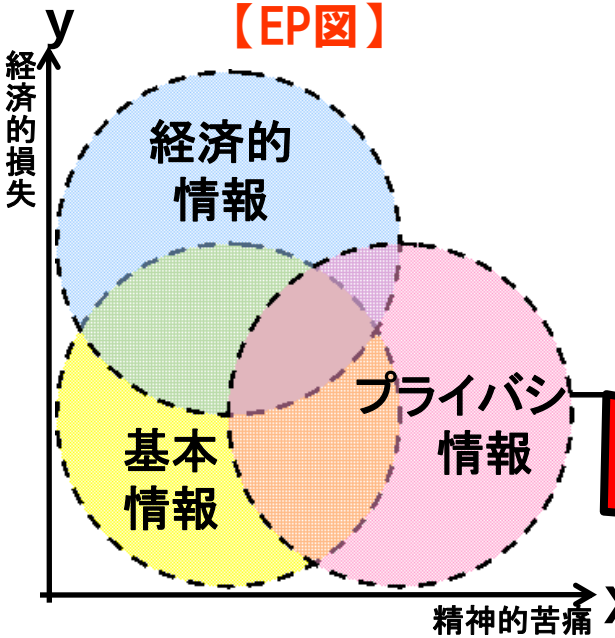
判定基準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。	2
一般的	その他一般的な企業および団体、組織。	1

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

参考：想定損害賠償算定の全体像

JNSA

【EP図】



【判定基準表】

判定基準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関	2
一般的	び団体、組織。	1

判定基準	事後対応評価
適切な対応	
不適切な対応	
不明、その他	

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

損害賠償額＝（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

＝ 基礎情報価値[500]
×機微情報度[Max($10^{x-1}+5^{y-1}$)]
×本人特定容易度[6, 3, 1]
×社会的責任度[2, 1]
×事後対応評価[2, 1]

個人情報の基本的な価値を算出

漏洩組織の対応を評価

2013年 個人情報漏えいインシデント

JNSA

期間：2013年1月1～12月31日（※12ヶ月分）
インターネットニュースなどで報道されたインシデントの記事、
組織からリリースされたインシデントの公表記事などをもとに集計

	2013年データ	2012年データ
漏えい人数	925万4513人	972万65人
漏えい件数	1388件	2357件
想定損害賠償総額	1438億7184万円	2132億6405万円
一件当たりの漏えい人数	7027人	4245人
一件当たり平均想定損害賠償額	1億924万円	9313万円
一人当たり平均想定損害賠償額	2万7707円	4万4628円

2014年上期 個人情報漏えいインシデント

JNSA

報告書はJNSAホームページで公開予定

期間：2014年1月1～6月30日（※6ヶ月分 速報値のため、修正される場合有り）

インターネットニュースなどで報道されたインシデントの記事、
組織からリリースされたインシデントの公表記事などをもとに集計

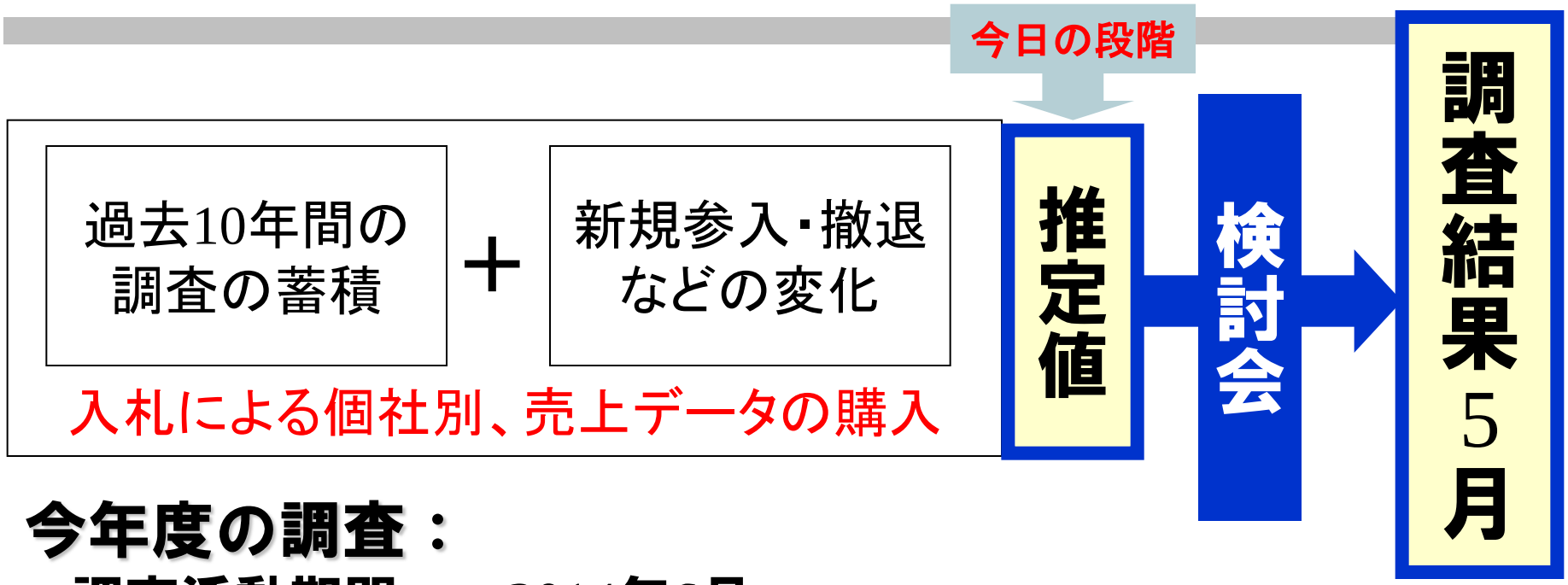
	2014年上半期	2013年データ
漏えい人数	74万4453人	925万4513人
漏えい件数	944件	1388件
想定損害賠償総額	245億8688万円	1438億7184万円
一件当たりの漏えい人数	823人	7027人
一件当たり平均想定損害賠償額	2726万円	1億924万円
一人当たり平均想定損害賠償額	4万9715円	2万7707円

「費用」から「投資」へ
情報セキュリティ市場規模の推定

本日のテーマ

- 「費用」から「投資」へ
  - 投資には将来的なリターン（利益）が必要
    - 投資対効果が測定可能でなければならない
    - 測定するためには投資の数値、利益の数値が必要
    - 投資の数値＝投資額、であれば利益も「金額」
  - セキュリティ数値化に関わるチャレンジ
    - セキュリティ対策で「損害が軽減される」ことによる利益
    - セキュリティ対策を「販売する」ことによる利益
    - セキュリティ対策のおかげで「より売れる」ことによる利益

セキュリティ市場調査WGによる市場規模推定



今年度の調査：

- **調査活動期間：** 2014年6月～（現在も進行中、本日は速報値）
- **調査方法：** アンケート調査はしない（回収率が悪く参考にならない）
  各種統計・調査資料の参照
  企業の事業概要・規模推定（対象数：470→505社）
  検討会：WGメンバー情報や、公開情報を元にデータ修正
- **対象期間：** 2012, 2013年度実績　2014年度見込み　2015年度予測

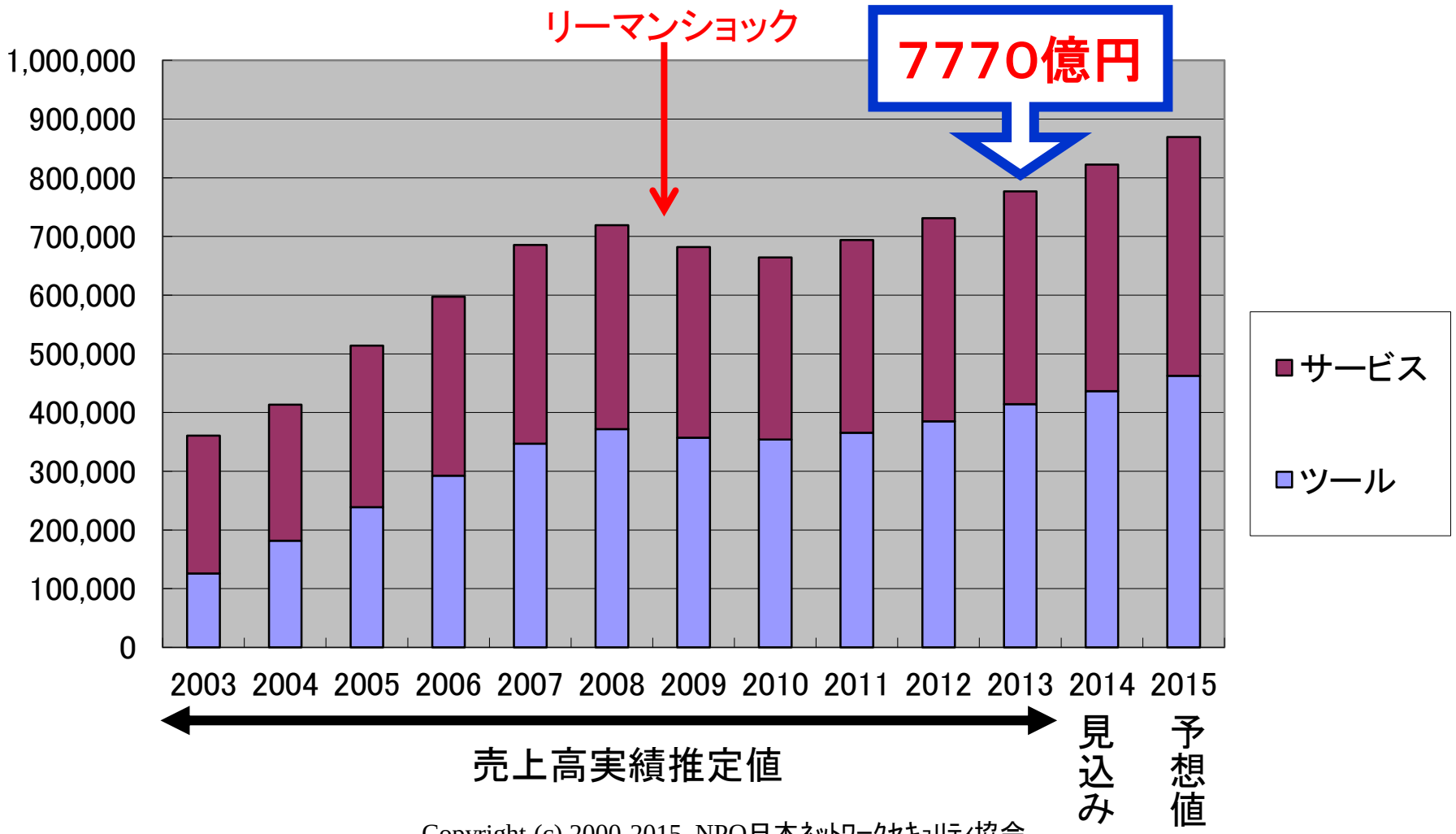
市場区分の定義

セキュリティツール	統合型アプライアンス	FW、IDS、ウイルス対策等複数機能を持ったアプライアンス
	ネットワーク脅威対策製品	FW、IDS/IPS、VPN、アプリケーションファイアウォール
	コンテンツセキュリティ対策製品	ウイルス対策、スパム対策、URLフィルタ、メールフィルタ、DLP等
	アイデンティティ・アクセス管理製品	認証、ログオン管理･アクセス許可、PKI製品
	システムセキュリティ管理製品	セキュリティ情報統合管理、ポリシー・アクティビティ管理ツール、脆弱性検査ツール　等
	暗号製品	暗号化製品、暗号モジュール
セキュリティサービス	情報セキュリティコンサルテーション	ポリシー構築、監査･診断等セキュリティ管理全般コンサルティング、規格認証取得支援サービス
	セキュアシステム構築サービス	ITセキュリティの設計、導入、製品選定支援　等
	セキュリティ運用・管理サービス	マネージドサービス（ITセキュリティの監視、運用支援）、プロフェッショナルサービス、電子認証サービス　等
	情報セキュリティ教育	教育実施、コンテンツ提供、教育ASP、資格認定　等
	情報セキュリティ保険	情報セキュリティおよびITセキュリティ保険

サイバーセキュリティ製品・サービス市場

報告書はJNSAホームページで公開予定

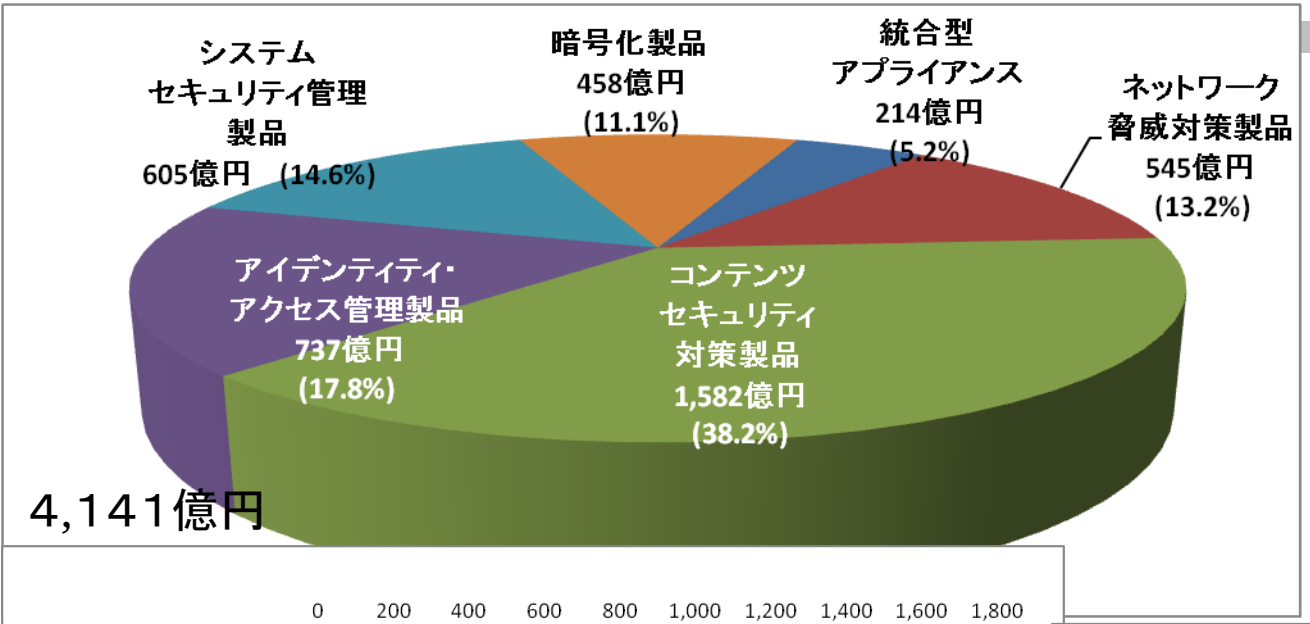
- 市場規模推移



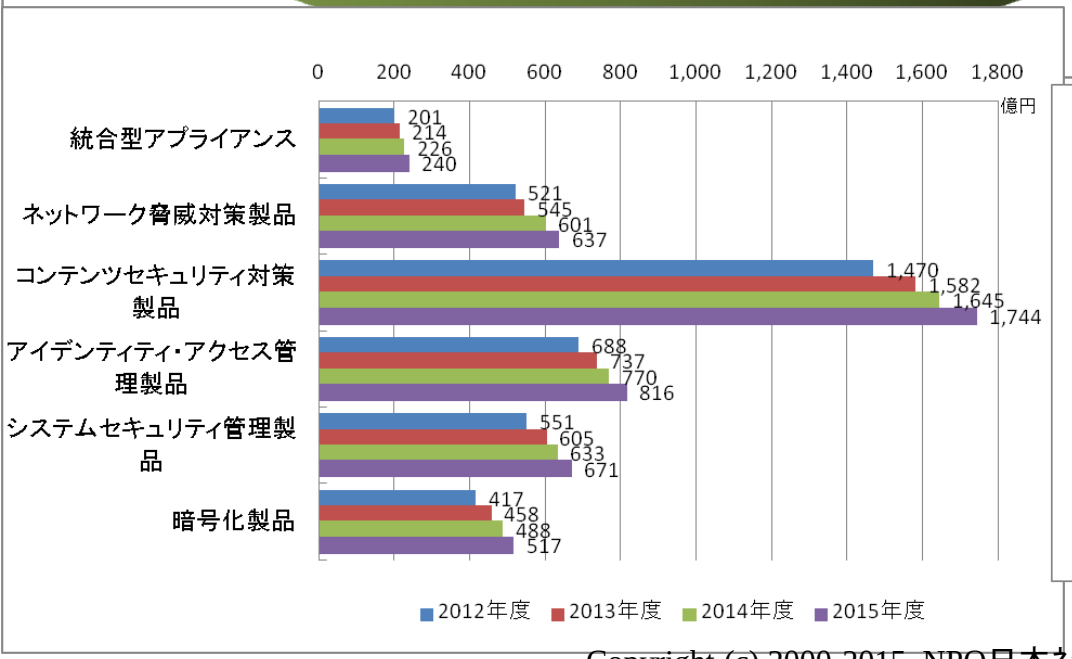
国内情報セキュリティツール市場推移

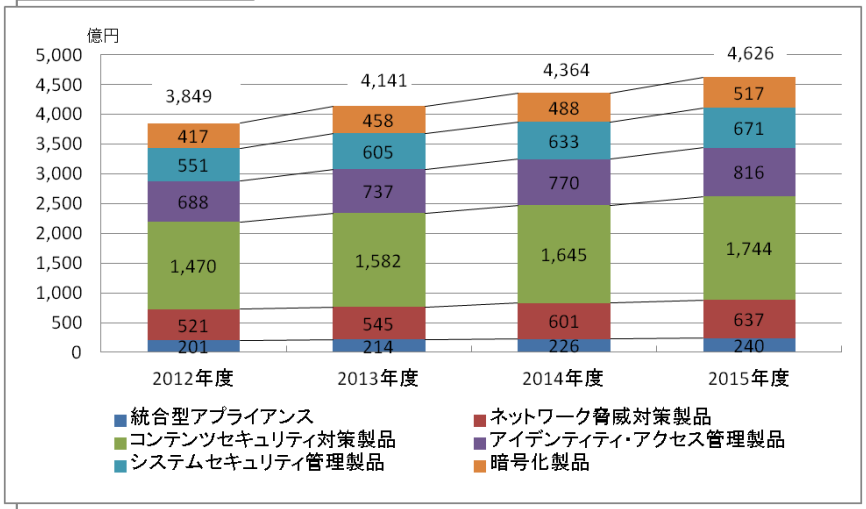
JNSA

速報



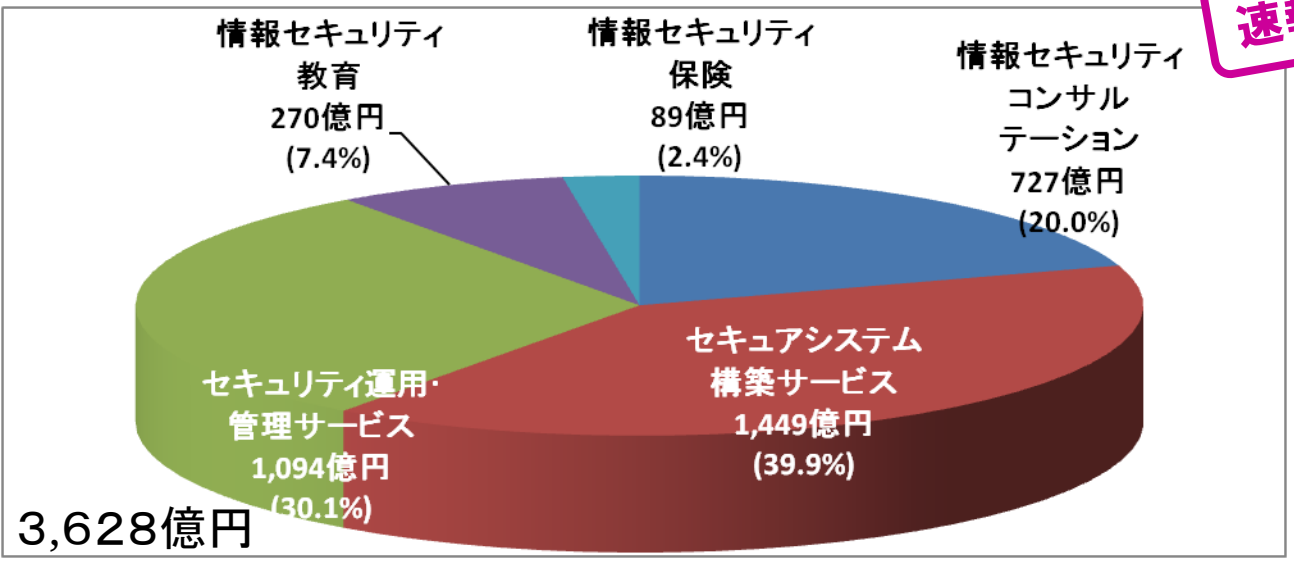
- ツール全体で2012年から7.6%の伸び。
- 伸率が高かったカテゴリは、システムセキュリティ管理製品と暗号化製品。
- 情報漏えい対策強化の結果と推測される。



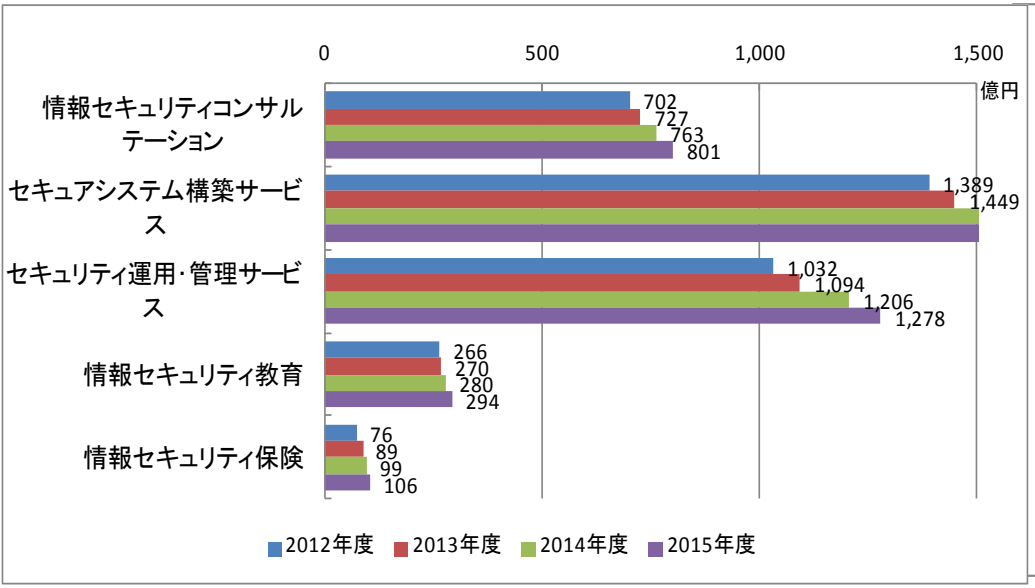


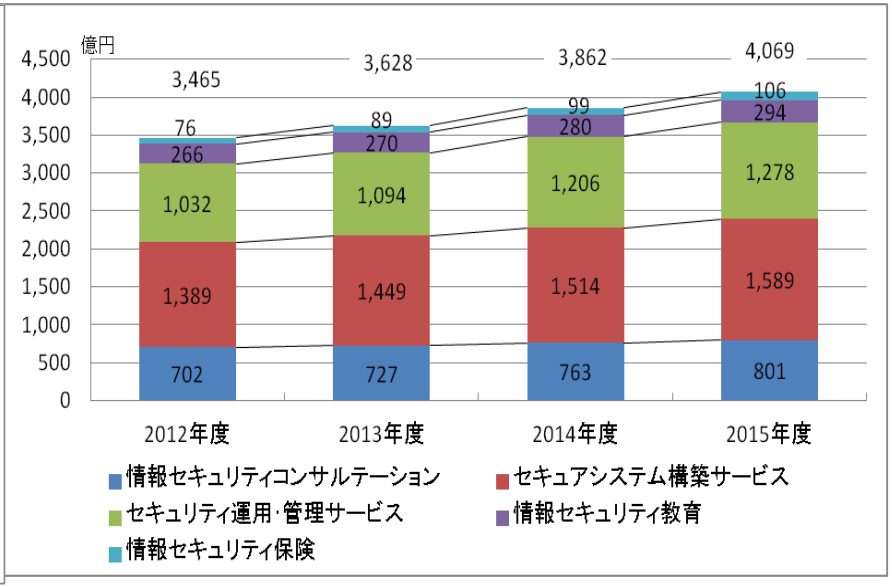
情報セキュリティサービス市場推移

速報



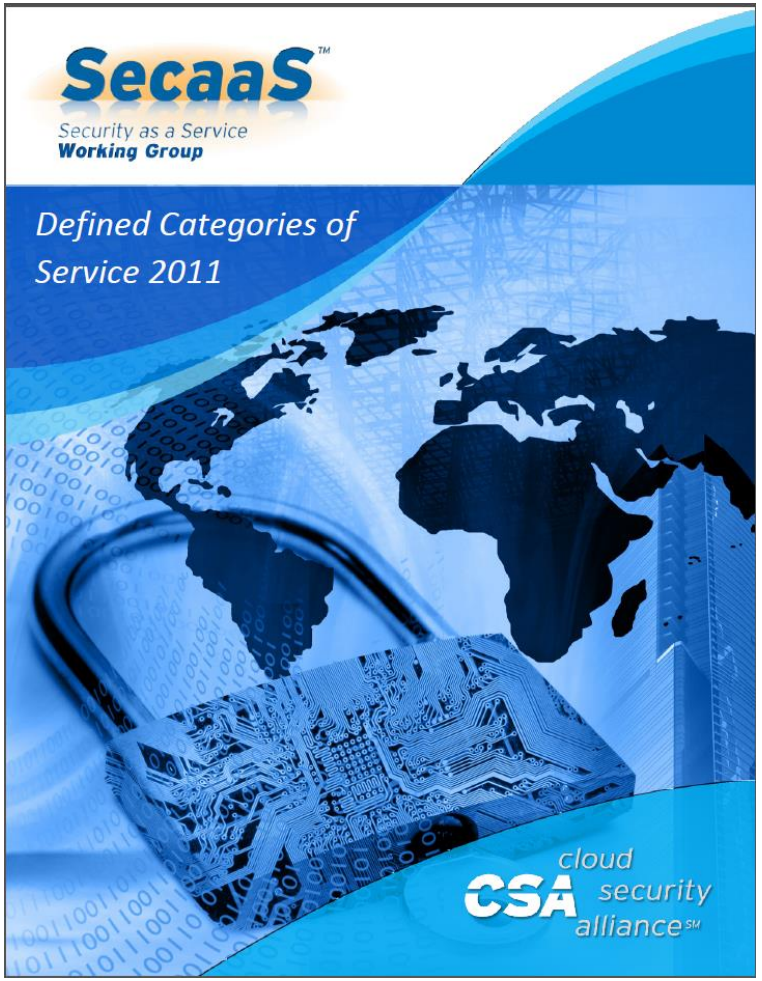
- 前年比4.7%伸び3628億円
- システム構築サービスが最大。標的型攻撃対策などで需要が伸びた。
- スマートデバイスを用いた社内システム運用の需要、情報漏えい対策、景気回復が後押していると思われる。





参考：クラウドセキュリティ対策サービス

Category 1: Identity and Access Management
Category 2: Data Loss Prevention
Category 3: Web Security
Category 4: Email Security
Category 5: Security Assessments
Category 6: Intrusion Management
Category 7: Security Information and Event Management (SIEM)
Category 8: Encryption
Category 9: Business Continuity and Disaster Recovery
Category 10: Network Security



https://cloudsecurityalliance.org/research/secaas/ より引用

まとめ

まとめ

- ICTの利用が広がるとともに、攻撃の対象範囲も拡大
  - リスト型アカウントハッキングや暗号化プロトコルの問題は広く影響
  - ネットを使った不正アクセスによる大規模な情報漏えい
  - 攻撃対象は幅広く、サポート期間はより長くなる傾向
- ICTを生かした事業運営とサイバーセキュリティは一心同体
  - 脅威情報や被害動向だけ見ていても事業とはつながらない
  - 事業戦略とサイバーセキュリティを一体化して考える
  - そのためには重要な一要素である数値化
  - 投資対効果測定に参考となる（かもしれない）被害額算定、市場規模推定を紹介

サイバーセキュリティを投資としてとらえるためにはまだまだ情報・手法が不足している（確立されていない）ことは大きな課題だが、誰かが解決してくれることを待っていられるほど余裕のある状況でもない

続きはパネルディスカッションで・・・

御清聴ありがとうございました