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

Network Security Forum 2015
【A3】

多様なリスク時代の セキュリティ対策の考え方

セキュリティ被害調査WG
大谷 尚通 （株）NTTデータ

2015年 1月20日

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

もくじ

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2013年/2014年上半期
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～

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1. 2013年 個人情報漏えいインシデント

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

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1. 2014年上半期 個人情報漏えいインシデント

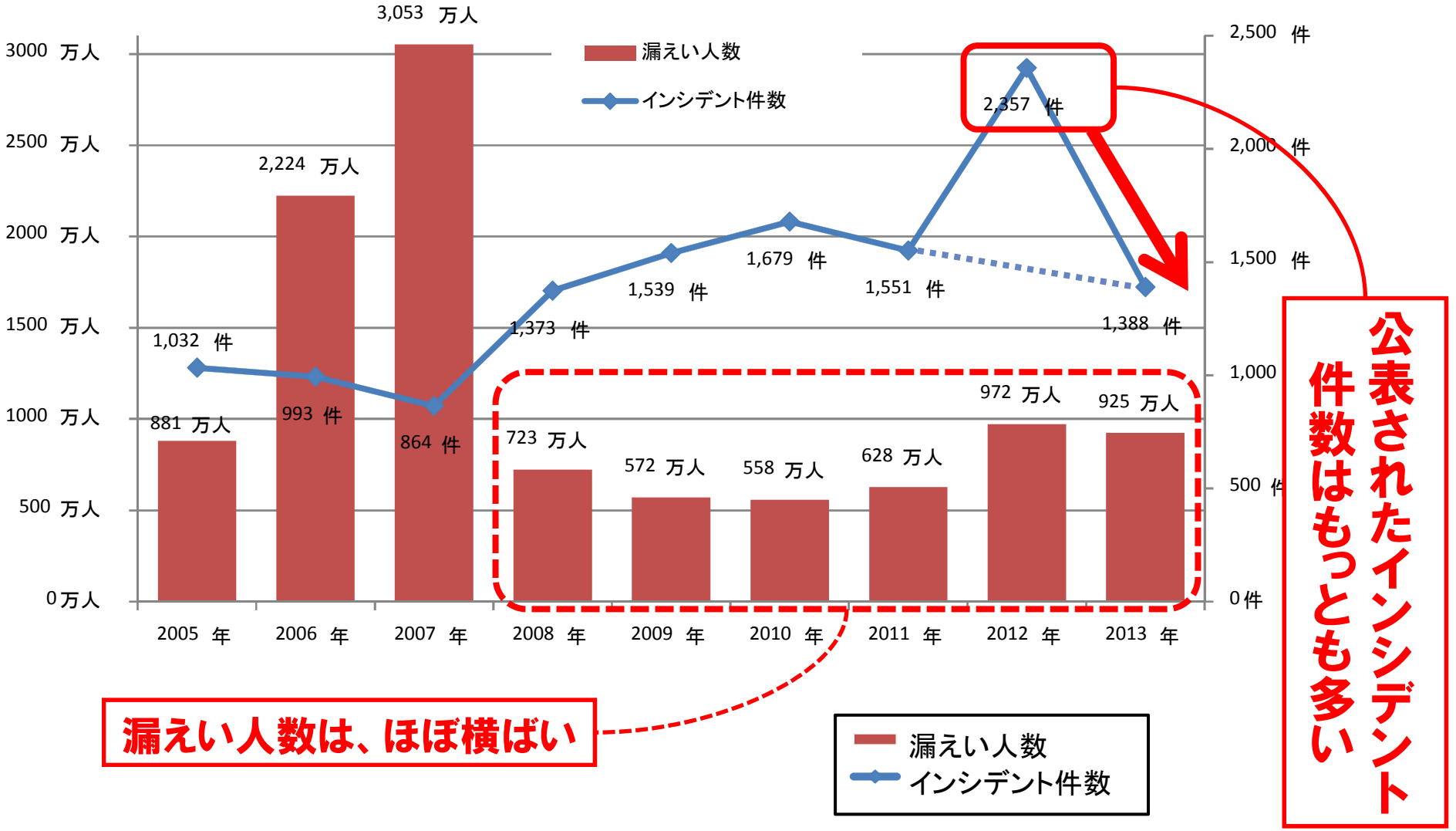
期間：2014年1月1～6月30日（※6ヶ月分）

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

	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

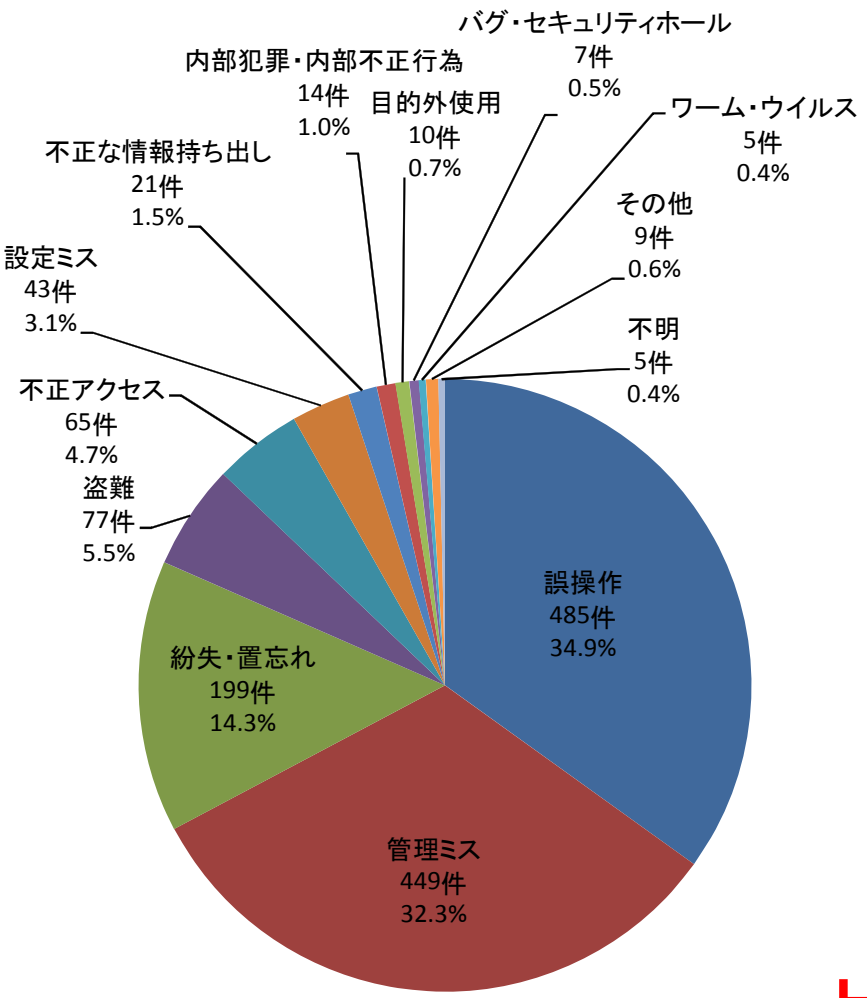
Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

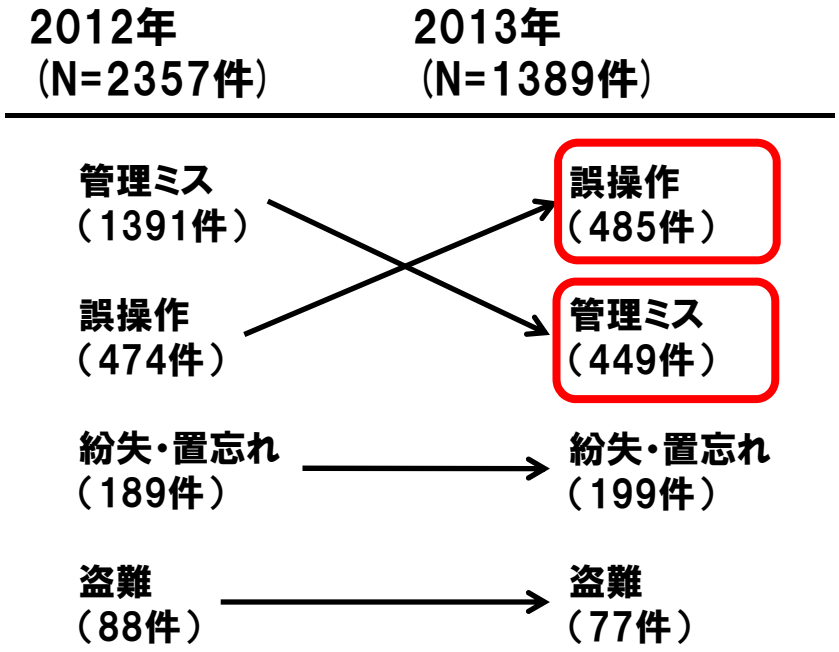
1.1 漏えい人数と件数（経年）



Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.2 原因別の漏えい件数



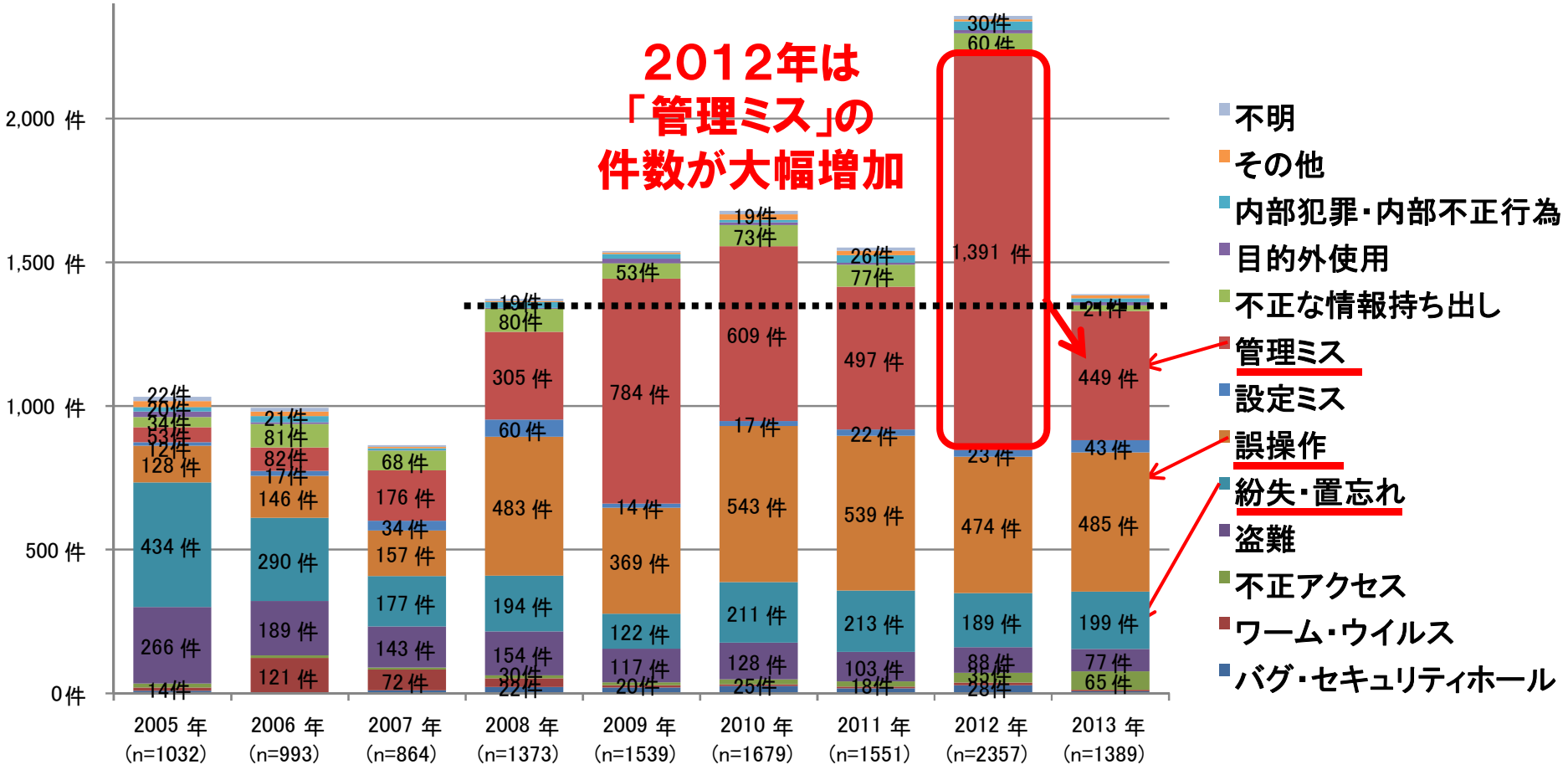


管理ミス(＝誤廃棄)
誤操作(＝ケアレスミス)
による漏えいが多い

上位の原因に大きな変化はなし

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

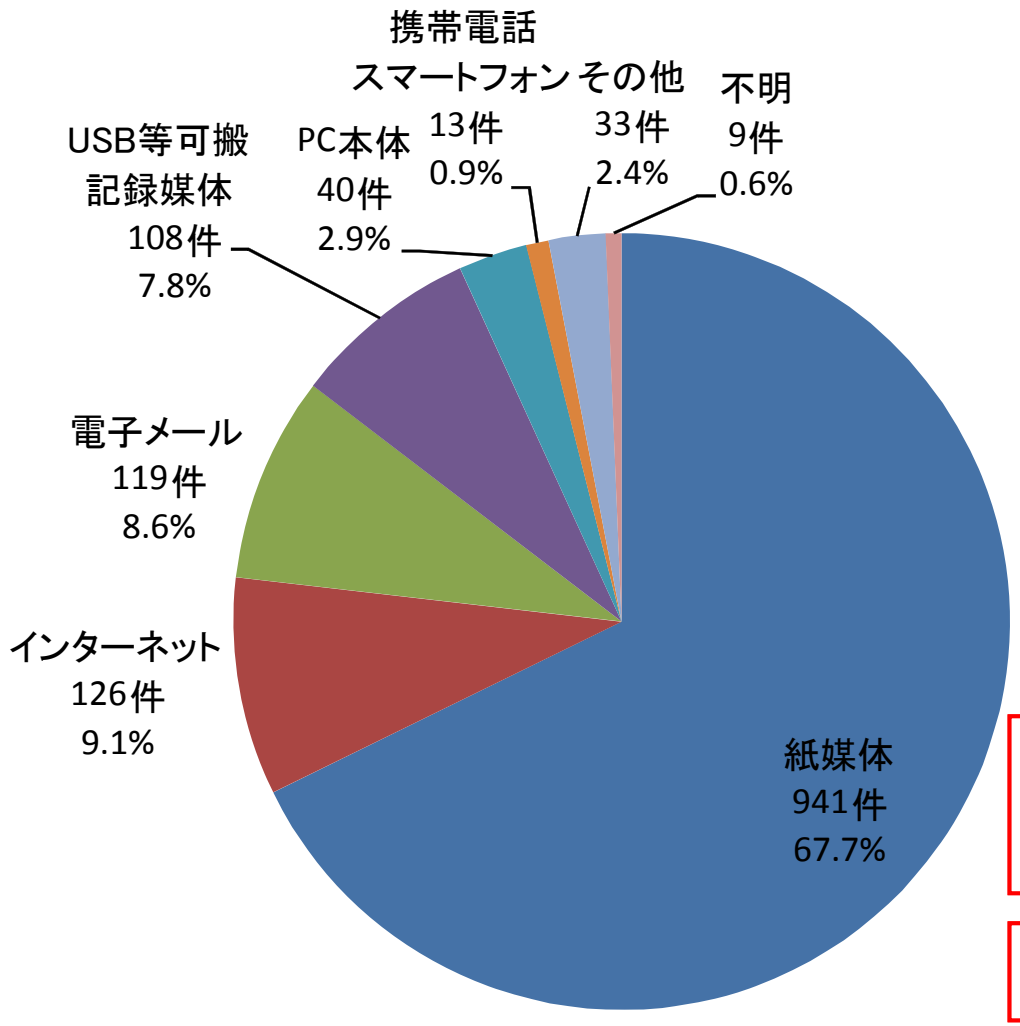
1.3 原因別の漏えい件数(経年)

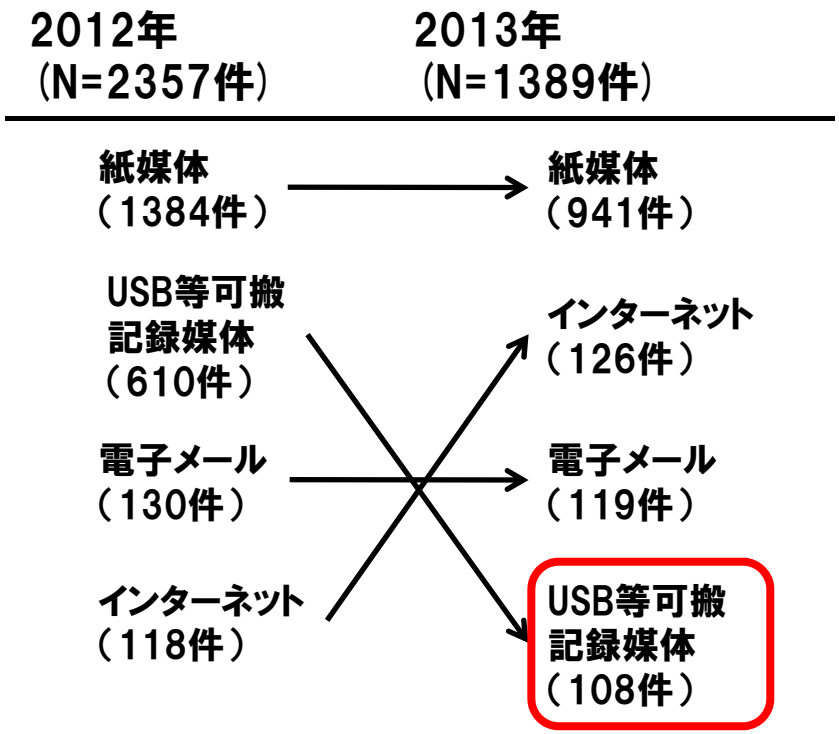


インシデントの3大要因は人為的ミス
「管理ミス」「誤操作」「紛失・置忘れ」

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

1.4 媒体別の漏えい件数



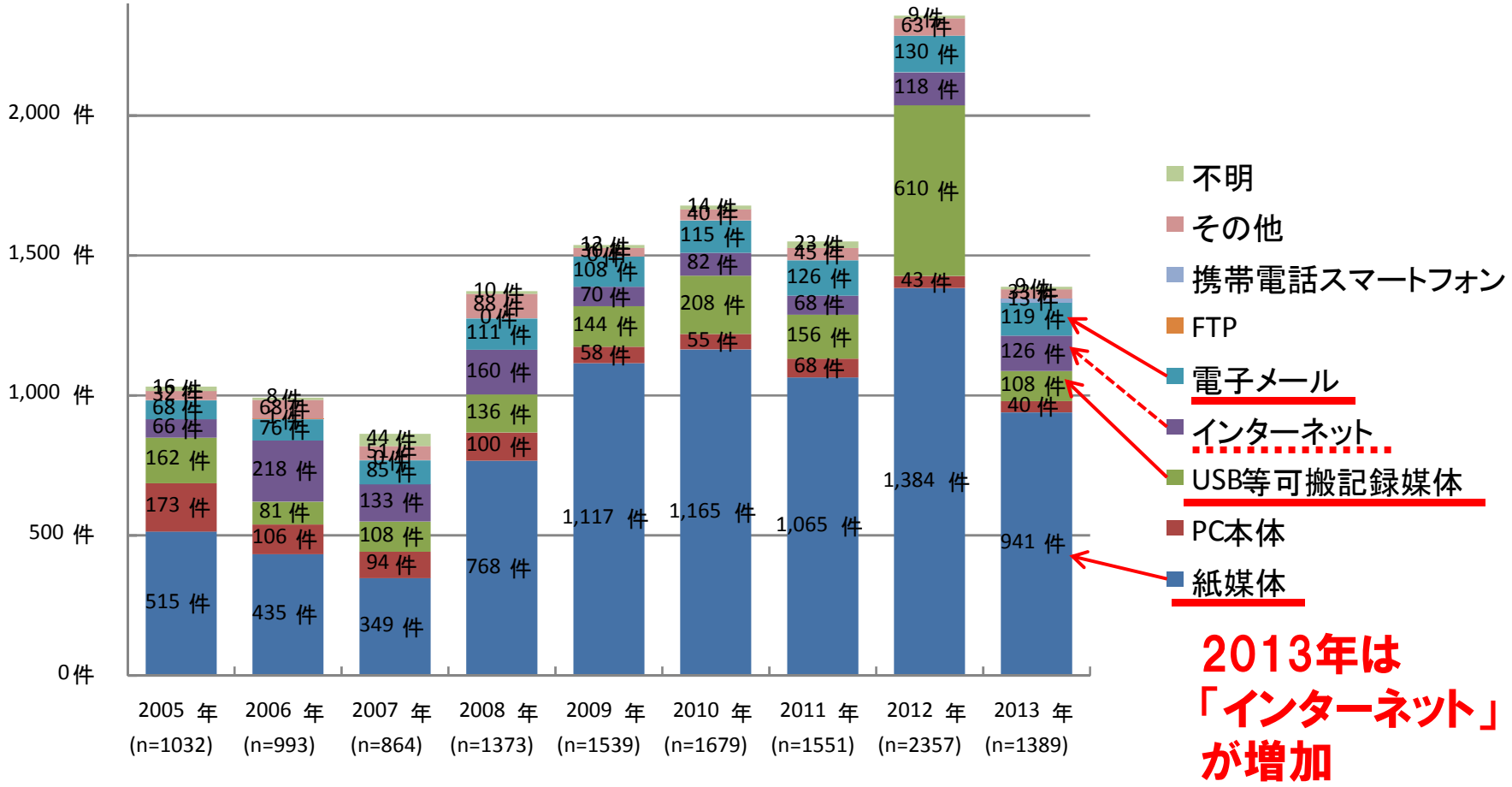


紙媒体による漏えいが多い。（例年通り）

USBが大幅減少

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.5 媒体別の漏えい件数(経年)



2013年は
「インターネット」
が増加

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

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

1.6 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

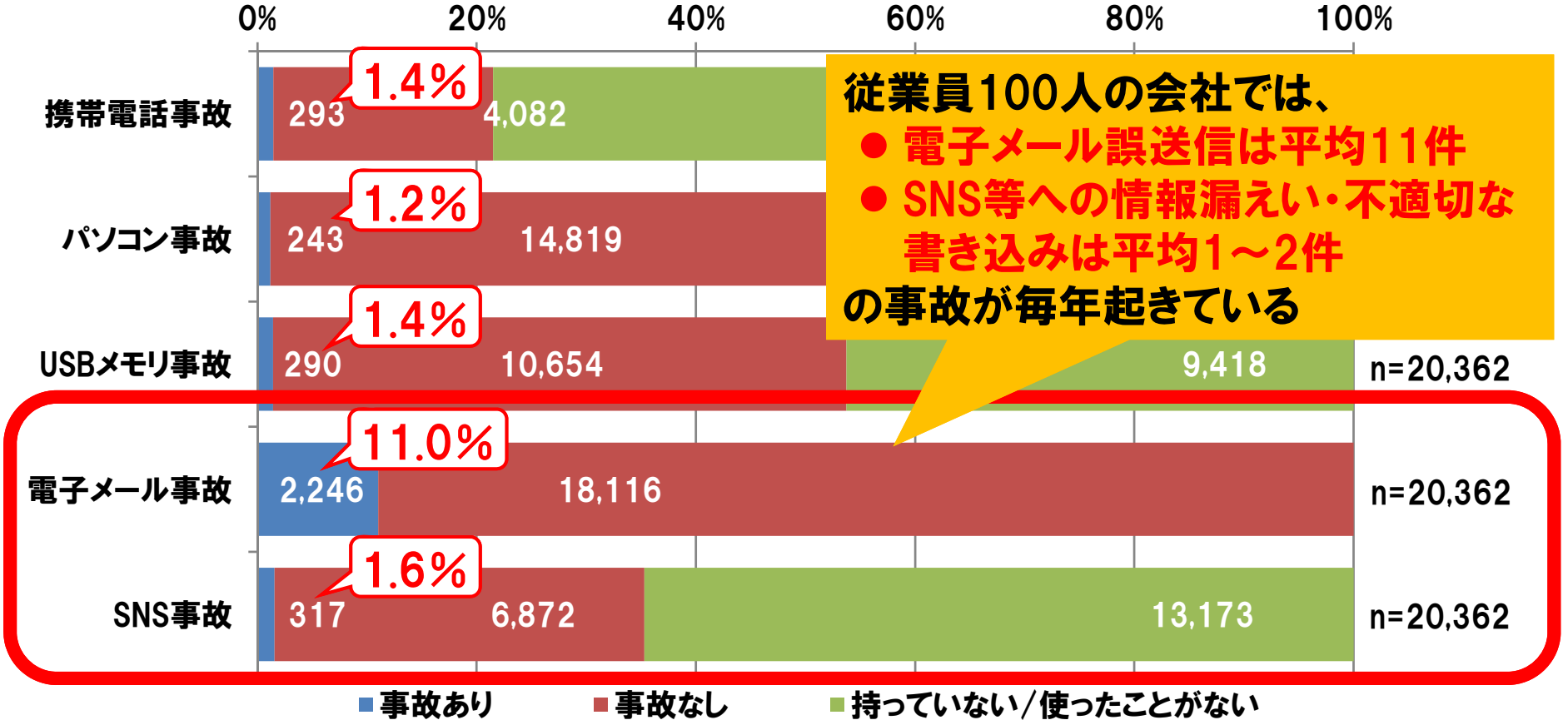
人為的ミスの対策が必要！
（ヒューマンエラー）

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.7 「人為的ミス」の発生確率①

2012年1年間で、携帯電話／パソコン／USBメモリの紛失・盗難、電子メールの誤送信、SNS等への情報漏えいや不適切書き込みをしてしまった経験がある人は？

※母数は、インシデント対象を持っていない/使ったことがない人も含む20,362人
※携帯電話・パソコン・USBメモリの「事故あり」は、業務データを保存した会社貸与/私物の紛失・盗難のみ



従業員100人の会社では、
- 電子メール誤送信は平均11件
- SNS等への情報漏えい・不適切な書き込みは平均1～2件

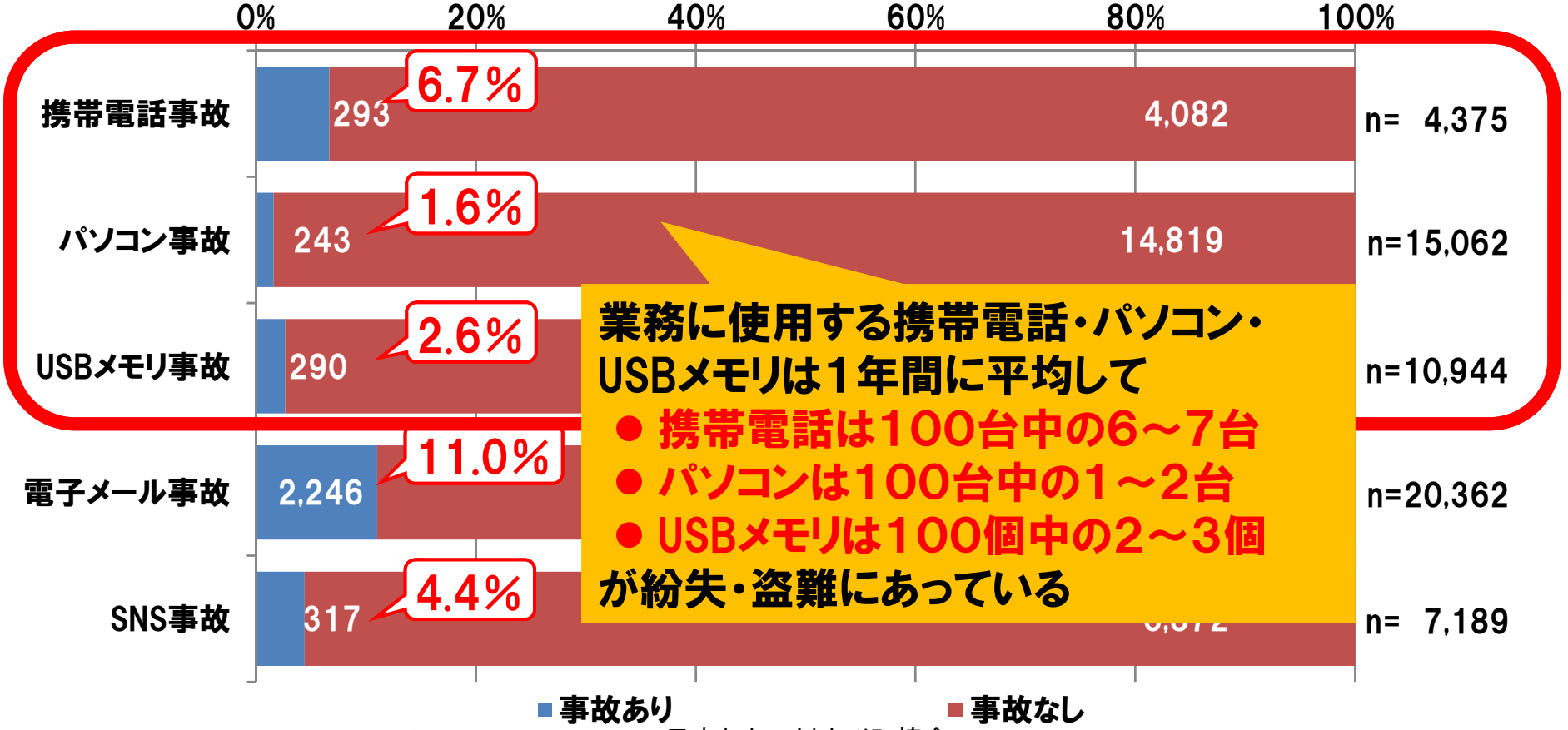
の事故が毎年起きている

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.7 「人為的ミス」の発生確率②

2012年1年間で、携帯電話／パソコン／USBメモリの紛失・盗難、電子メールの誤送信、SNS等への情報漏えいや不適切書き込みをしてしまった経験がある人は？

※各％の母数は、インシデント対象を持っていない/使ったことがない人を含まない
※携帯電話・パソコン・USBメモリの「事故あり」は、業務データを保存した会社貸与/私物の紛失・盗難のみ



Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

1.8 人為的ミスの対策案

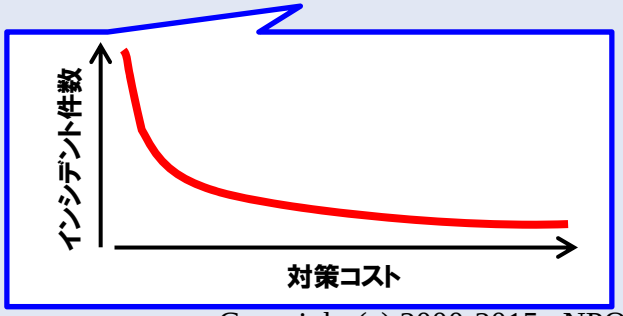
被害の大きさと投資対効果を考慮したセキュリティ対策の方針を採用

① 業務の重要度やインシデント発生時の被害の大きさに応じて
セキュリティ対策を**差異化**

全社統一のセキュリティ対策のため、現場から不満が続出？

全社統一のセキュリティ対策では、重要なシステムは対策不足？

② 一般的な対策ではこれ以上の削減が期待できない場合、
インシデントが発生しても被害を最小限に留める対策を実施



被害額よりも
対策コストが大きい ⇒失敗

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.9 人為的ミスの対策案① ～対策の差異化～

① 業務の重要度やインシデント発生時の被害の大きさに応じてセキュリティ対策を差異化

全社一律に禁止ルールを導入すると
業務効率の低下など、ビジネスへの影響が大きい

たとえば、BYODを導入した企業では、スマホの盗難や紛失のインシデントが毎年、一定数発生している！

リスクを認識し、
コントロールすれば怖くない

□ 営業社員
- 外出が多い＝外出先で作業したい
  移動時間を効率的に使いたい
- 機密性の高い情報は扱わない

⇒ スマートフォン OK

求める
セキュリティ
レベルが
異なる

セキュリティ担保とビジネス拡大
どちらを選択するか？

ビジネス拡大を重視

□ スタッフ社員
- 外出しない
- 機密性の高い情報を扱う
  （財務、知的財産等）

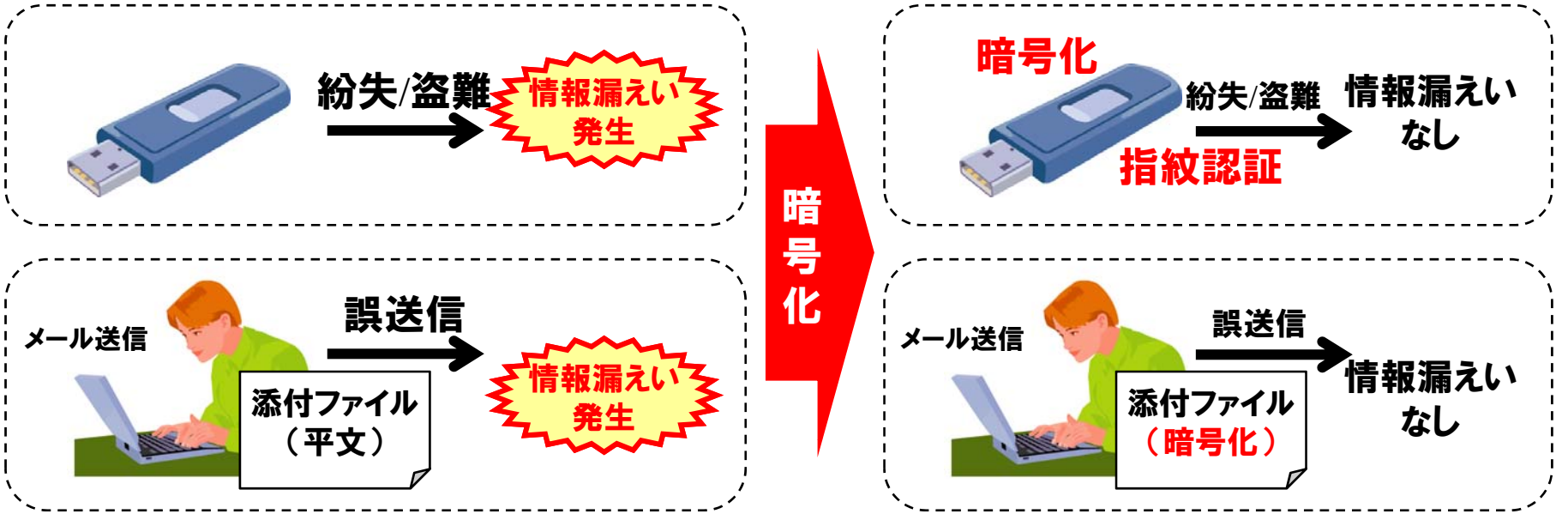
⇒ スマートフォン NG
固定PCのみOK

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

1.9 人為的ミスの対策案② ～被害の最小化～

② 一般的な対策ではこれ以上の削減が期待できない場合、インシデントが発生しても被害を最小限に留める対策を実施

たとえば、メールの誤送信やUSBメモリの紛失のインシデント発生件数は、ゼロにできない！



インシデント発生件数を削減できないのであれば
インシデントが発生しても被害を最小限に留める対策へ！

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

最新のサイバー攻撃事情

- パスワードリスト攻撃
- 水飲み場型攻撃
- クラウドサービスの乗っ取り

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2. 2013年 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

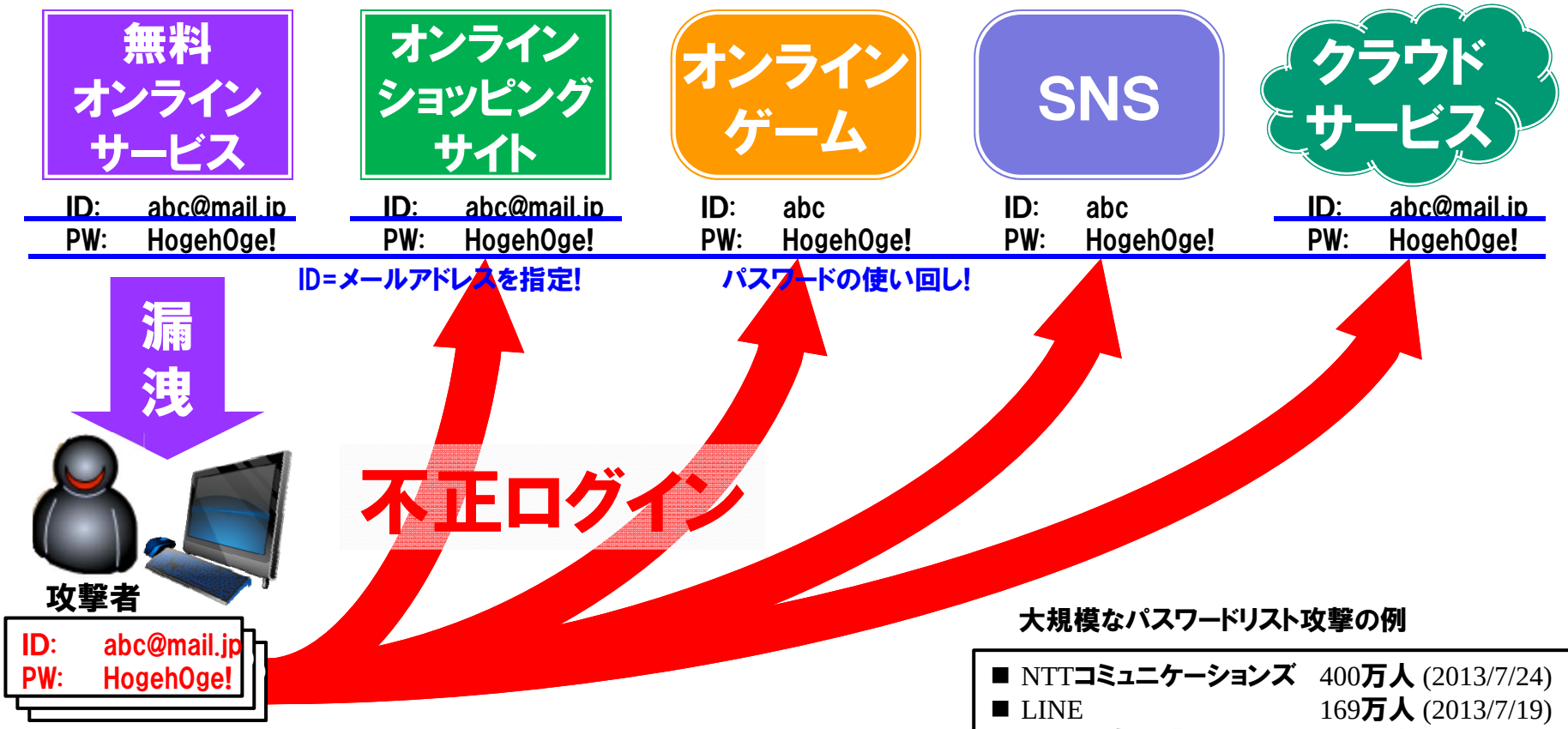
情報通信業
が多い

パスワードリスト攻撃

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.1 パスワードリスト攻撃

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



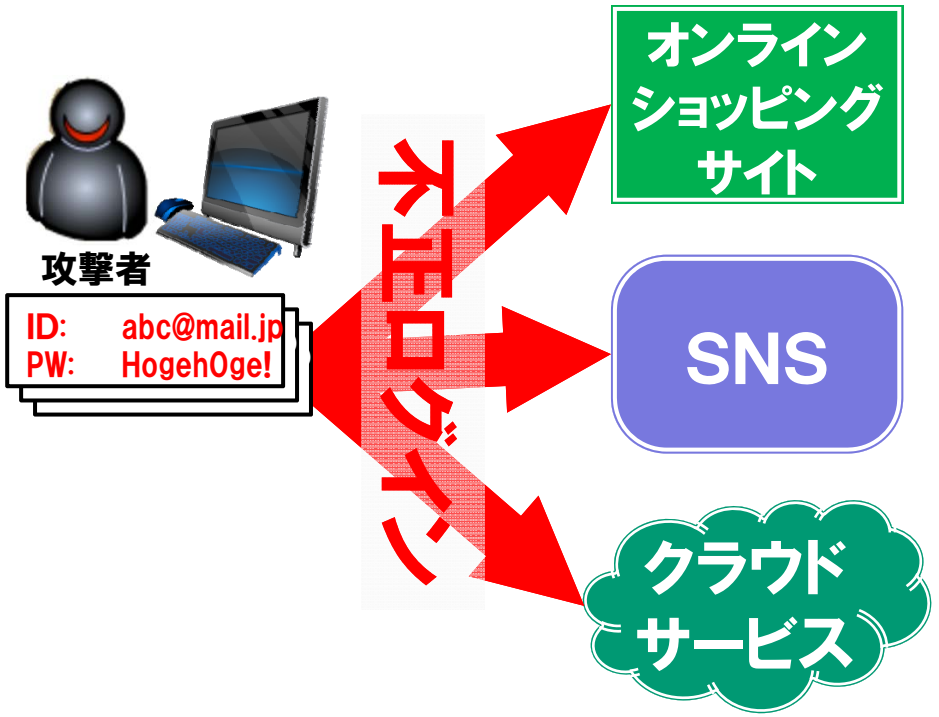
大規模なパスワードリスト攻撃の例

■ NTTコミュニケーションズ	400万人 (2013/7/24)
■ LINE	169万人 (2013/7/19)
■ UCC上島珈琲	47万人 (2013/1/7)
■ サイバーエージェント	24万人 (2013/8/12)
■ セブンネットショッピング	15万人 (2013/10/23)
■ グリー	4万人 (2013/8/8)

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

2.1 パスワードリスト攻撃の被害例

パスワードリスト攻撃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 (p.19)

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.1 パスワードリスト攻撃の対策案

パスワードリスト攻撃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
- 解読されやすい秘密の質問を使用しない
- 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。P.22参照）

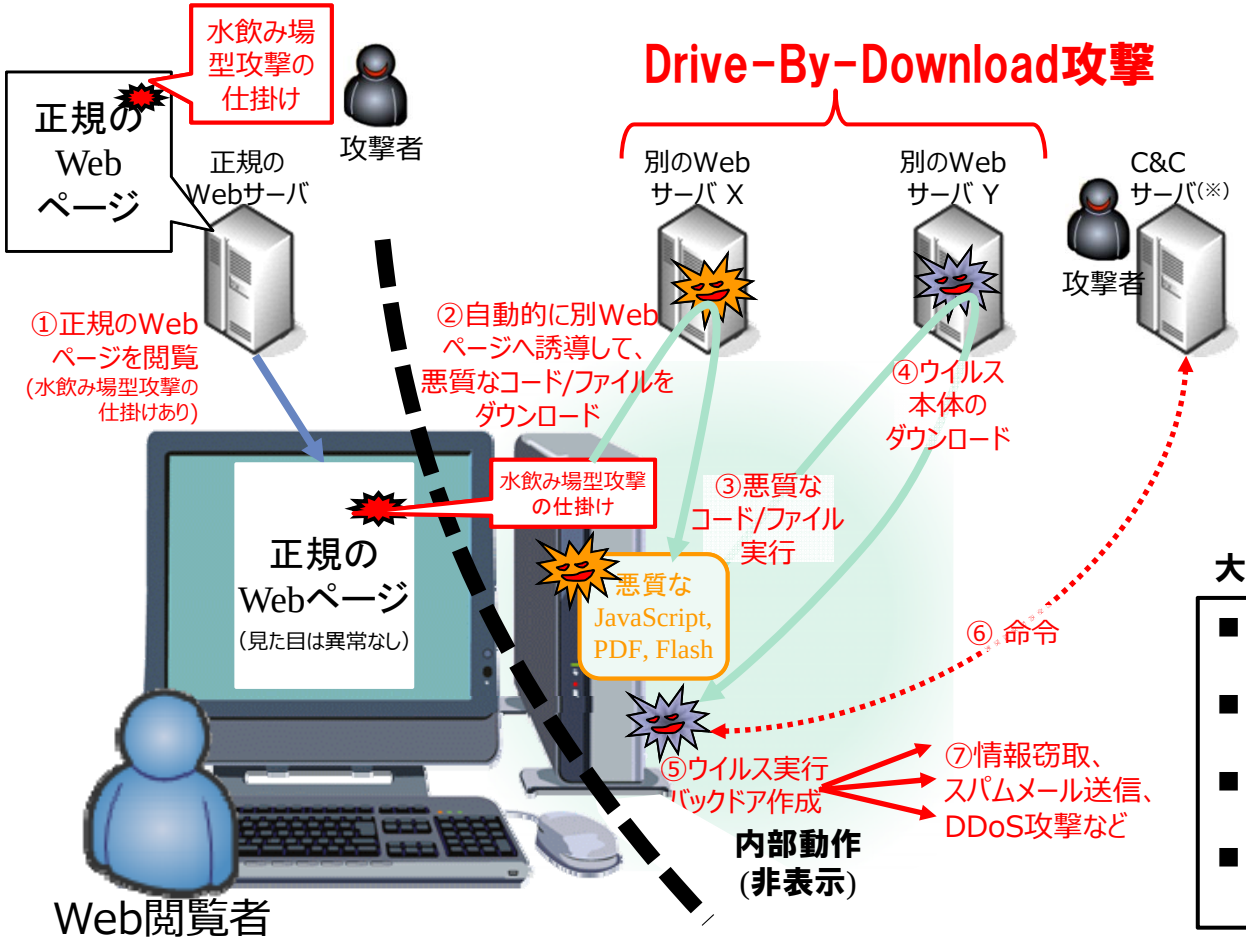
2要素認証
パスワードリスト攻撃で1段階目の認証を突破されても
2段階目の認証を突破できない

例）母親の旧姓は？ ＝鈴木
出身地は？ ＝東京

Copyright (c) 2000-2015 NPO日本ネットワークセキュリティ協会

2.2 水飲み場型攻撃

ユーザがアクセスする可能性の高いWebページへ Drive-By-Download攻撃を仕掛ける水飲み場型攻撃が大量発生。



大規模な水飲み場型攻撃の例

- **日産自動車のWebサイト改ざん** (2014年8月26日)
- **パロアルトネットワークスのWebサイト改ざん**(2014年9月11日)
- GMOのブログサービス JUGEMのWebサイト改ざん(2014年5月28日)
- HISのWebサイト改ざん (2014年5月28日)

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.2 水飲み場型攻撃の対策案

水飲み場型攻撃によってウイルスに感染しないためには

- 最新のセキュリティパッチを適用する
- Java/ActiveX/Flash/Silverlightの不必要な実行を許可しない

ユーザの対策

- ネットワーク対策/感染防止（URLフィルタの導入）
- ネットワーク対策/早期検知（通信ログの監査、サンドボックス検知）

システム側の対策

ウイルス対策ソフトはほとんど検知しない！

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

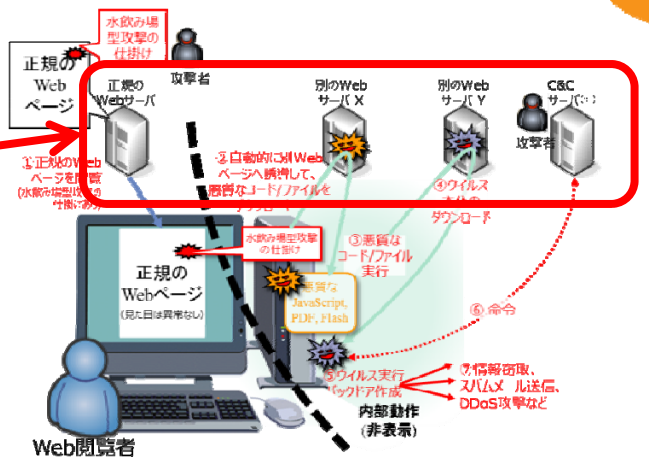
2.3 クラウドサービスの乗っ取り

ユーザが利用しているSalesforce、Amazon EC2やWindows Azureなどのクラウドサービス（仮想サーバ）へ不正ログインして、不正に利用する

乗っ取ったアカウントを使って

- **CPUリソースの不正利用**
- **攻撃の踏み台（DoS攻撃、Spam送信）**
- **水飲み場型攻撃**
  （Webページ、C&Cサーバ（p.19））

例えば、乗っ取ったクラウドサービスを不正に使用して、ビットコインのマイニングを実行（ビットコインの取引時の認証の計算を行い、報酬をビットコインで得る）



Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.3 クラウドサービスの乗っ取りの原因

クラウドサービスは、サーバ構築や運用の知識がない人でもサーバを構築/運用できるため、さまざまなセキュリティの問題が発生

- **セキュリティ対策が不十分**
  （使いやすい設定を適用）
  （脆弱性を放置）
- **セキュリティ設定ミス（不要なサービスを起動）**
- **簡単なパスワードを設定**

セキュリティ設定より使いやすい設定を優先

Webサーバなどのセキュリティパッチを適用したり、バージョンアップしたりできない

サービスの構成を把握せず、セキュリティ設定が不十分なサービスをそのまま運用。そのサービスから不正侵入される

初期パスワードのままで運用

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.3 クラウドサービスの乗っ取りの対策案

クラウドサービスが乗っ取られないためには

- 複雑なパスワードを設定する。
  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
- 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

サーバ構築や運用の知識がない人では難しい・・・

- セキュリティ対策が強化されたクラウドサービスを利用する

サーバ構築や運用の知識がない人がサーバを構築/運用するので、安心できるクラウドサービスを推奨したり、利用するクラウドサービスを限定してIT部門がサポートするほうがよい

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

2.4 最新のサイバー攻撃の対策案 まとめ

2.1 パスワードリスト攻撃

2.2 水飲み場型攻撃

2.3 クラウドサービスの乗っ取り

これからも
新しい攻撃は
増える！

定期的に新しい脅威、攻撃を調査して
セキュリティ対策を追加

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

内部犯罪・内部不正行為

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3. 過去の内部犯罪による個人情報漏洩

- Yahoo!BB（2004年2月27日）
  ヤフーBB代理店社員が、恐喝目的で約450万人分の個人情報を持ち出す
  Yahoo! BB会員に500円相当の金券送付
  裁判の結果、1人あたり6,000円×5名の損害賠償

- 三菱UFJ証券（2009年1月26日）
  システム部の部長代理が、顧客データベースから約149万人分の個人情報を不正に引き出して、名簿業者4社へ転売。動機は借金500万円の返済
  5万人に商品券1万円を配布

- ベネッセ（2014年7月9日）
  グループ企業から再委託した外部業者のSEが3504万人分の個人情報を不正に引き出して、複数の名簿業者へ転売。動機は借金300万円の返済
  760万件の対象者へ金券500円分を配布（特別損失 約260億円計上）

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3.1 内部不正対策の誤解と限界

内部不正は、一般的な対策だけでは通用しない

- **情報セキュリティ教育**
  不正行為を認識して実行。怨恨の場合は会社を止めるつもりで実行
  ルールや教育による対策は間違い
- **情報セキュリティルール**
  金銭目的の場合は見つからないように実行。見つからなければ罰則されない
- **アクセス制限**
  管理者権限を持っていて無制限の場合が多い
  管理者が少ないので、一人でいくつものシステムの管理者を兼任
  特別なアクセス権限をもった人の内部不正ほど、被害が大きくなる
- **セキュリティ対策**
  セキュリティ対策のしくみを知っているので対策を迂回する
  技術力があるため、脆弱性を攻撃して権限を奪取する

利便性を犠牲にしたり
監視・運用体制やシステムによる対策を強化しなければ
内部不正には対抗できない！

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3.2 内部犯罪による個人情報漏洩の原因

ベネッセの場合に問題だったと思われる点

- 顧客情報DBの全顧客情報にアクセス可能な権限を付与
- 顧客情報DBの開発と運用の両方に関わっていた
- 顧客情報DBに備わっていた流出防止プログラムを解除していた
- 顧客情報DB等のアクセスログの監査が不十分
- PCに接続されたスマートフォンへのデータコピーを制限していなかった
- 顧客情報DBに忍び込ませていたダミーデータが名簿業者に見抜かれて機能しなかった。

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3.3 内部犯罪（情報漏えい）の対策案

ベネッセの場合の対策案

■ 顧客情報DBの全顧客情報にアクセス可能な権限を付与

→ 不要な権限を与えない。DBのメンテナンスに必要な権限のみを与える。OSの管理者権限やデータアクセス権限は与えない

「委託しない」という対策はどうなのか？

■ 顧客情報DB等のアクセスログの監査が不十分

→アクセスログを自動監査し異常を早期検知

全ログの目視監視は不可能

新しい技術が開発されると新しいリスクが出現する
⇒定期的なリスク分析と対策見直し！

■ PCに接続されたスマートフォンへのデータコピーを制限していなかった

→USBメモリだけでなく、スマホに使われている新しい方式 メディア転送プロトコル（Media Transfer Protocol：MTP）,画像転送プロトコル（Picture Transfer Protocol：PTP）も制限する

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3.4 内部不正の対策のポイント①

JNSA

内部不正に有効な対策

- 細かなアクセス制限や権限分離
- 不正行為の検知/防止システム導入などのシステム対策
- 重要な操作の実施時の立会い
- 操作記録やログ取得とその監査
- 定期的なリスク分析と対策見直し

↓

内部不正の対策はコストが高い

↓

顧客DBなどの重要なシステムを優先して対策する

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

3.4 内部不正の対策のポイント②

JNSA

一般的な対策が通用しない人による内部不正に対抗するには
（特別な権限あり、技術力あり、セキュリティ対策を迂回可能）

内部不正も完全に
防ぐことがほぼ不可能

早期検知/早期対応 と 被害最小化

- 操作記録やログ取得とその監査
- 定期的なリスク分析と対策見直し

- 細かなアクセス制限や権限分離
- 不正行為の検知/防止システム導入
- 迅速な初動対応

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

まとめ

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

多様なセキュリティリスクの対応へ

発生の頻度と被害の大きさ、セキュリティ対策の費用対効果を考慮し対策の優先順位を決定

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

合理的なセキュリティ対策の方針

JNSA

被害の大きさと対策費用を考慮した合理的なセキュリティ対策の方針

□ 人為的ミスによる個人情報漏えい
→ 発生確率が高い、被害が小さい
→ 効果の高い予防策とする被害の最小化対策を組み合わせる

□ サイバー攻撃
→ 発生確率は企業組織/環境で異なる、被害が大きい
→ 定期的に新しい脅威、攻撃を調査してセキュリティ対策を追加

□ 内部犯罪・内部不正行為
→ 発生確率が低い、被害額が大きい
→ 重要なシステムを優先して対策

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会