IPA Better Life with IT

サイバーセキュリティにおける脅威の現状と組織の対応

営業秘密官民フォーラム　2016.6.15

独立行政法人 情報処理推進機構　参事
兼セキュリティセンター長
江口　純一

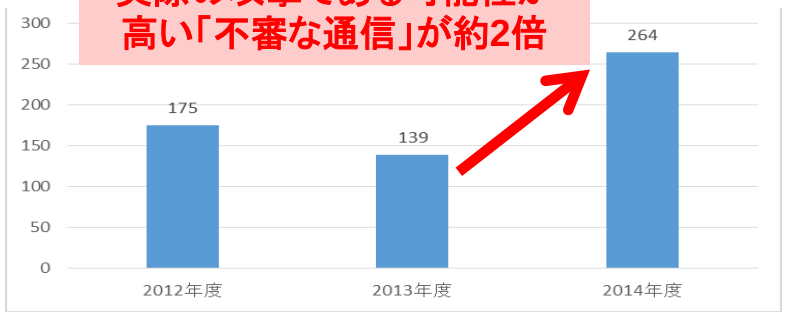
内容

- サイバーセキュリティの概況
- 脅威の現状
  - ランサムウェア
  - 内部不正
- 組織の対応状況
  - CISO・CSIRTの状況（日・米・欧比較）

サイバーセキュリティの概況
～増大する脅威～

GSOCセンサーで認知された政府機関への脅威の件数の推移

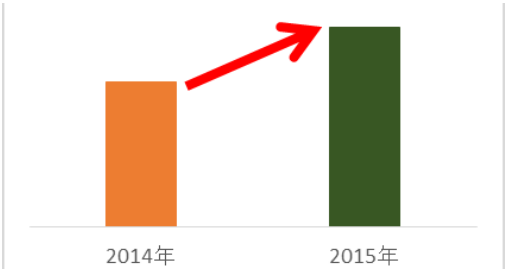
実際の攻撃である可能性が高い「不審な通信」が約2倍



出典：NISC　2015

セキュリティインシデント検知数増大

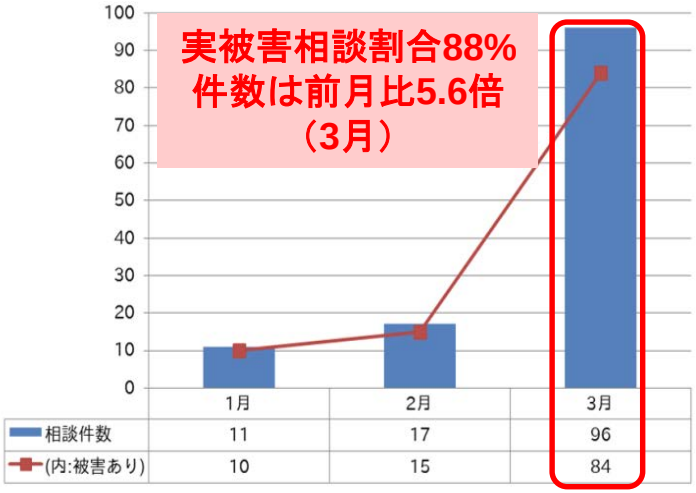
2015年インシデント検知数 前年比 38%増



出典：プライスウォーターハウスクーパース　2016

ランサムウェアに関する相談件数の増大

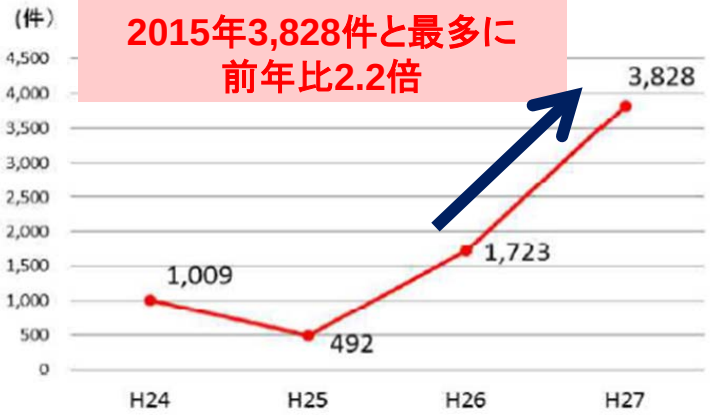
実被害相談割合88% 件数は前月比5.6倍（3月）



IPA：安心相談窓口による集計 2016

標的型メール攻撃件数の増大

2015年3,828件と最多に 前年比2.2倍



出典：警察庁 2016

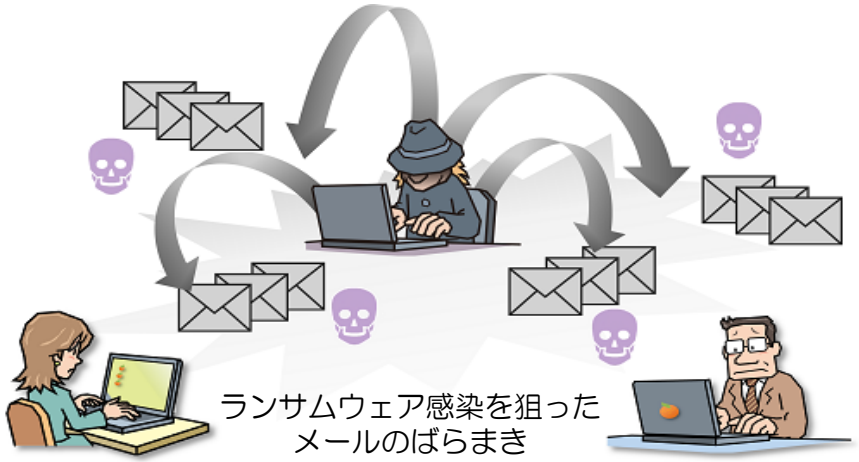
ランサムウェアによる攻撃が急増
～組織における感染は組織全体に被害を及ぼす可能性も～

IPA

ランサムウェア※に感染すると、ファイルが暗号化等され、その解除と引き換えに金銭を要求される。暗号化されてしまうと、ランサムウェア自体を駆除してもファイルを復元することができない。要求された金額を支払っても元に戻せる保証はない。　　・・・支払った事例も存在。

※ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。

感染経路
- メール内のURLをクリックしたり、添付ファイルを開くことで感染
- 攻撃者が用意した不正なウェブサイトから感染（脆弱性等を悪用）



ランサムウェア感染を狙った
メールのばらまき

IPAに情報提供のあったメール情報の例

メール件名：
『なし（no subject）』

メール本文：
『おはようございます！私たちはあなたのパッケージを配信することはできません、添付ファイルのあなたの住所を確認してください。ありがとうございました！』

添付ファイル名称：
『追跡番号_●●●●（数値）.zip』

出展:【注意喚起】ランサムウェア感染を狙った攻撃に注意(2016年4月13日)

ランサムウェアの被害事例

IPAの相談窓口に寄せられた事例（2016年3月～6月）

No	対象	内容
1	企業A	社内で2回目のランサムウェア感染を確認。ストレージサーバー内のデータが暗号化されてしまった。今回はバックアップをとっておらず、データ復旧が困難。感染元のパソコンも特定できていない。
2	企業B	メールの添付ファイルを、事務員が会社関係のものだと思い開いてしまい感染。ファイルがすべて開かなくなってしまった。工事の検査の申請に必要な写真も見られなくなってしまった。
3	企業C	ランサムウェア（Locky）に感染した。クラウドのファイル保存サービスを利用しているが、それがかなり上書きされているので気付いた。ウィルス対策ソフトを導入しているが検知できなかった。
4	動物病院	PCに届いたメールの添付ファイルを開いたらランサムウェア（locky）に感染してしまった。PCのソフトやOneDrive（オンラインストレージサービス）が使えなくなり、連動してレントゲンも使えなくなってしまった。メール件名、内容が書いていなくて、添付ファイルはinvoiceだった。
5	企業D	社内PCでメールを開いて感染し、Officeデータがやられた。 iPhoneから自分宛に写真を送ったりするので、こんなの送ったっけ？と思って開いてしまった。Dropbox（オンラインストレージサービス）もやられてしまった。
6	企業E	仕事のPCが感染し、Excel、Wordファイルが、lockyファイル（暗号化）になっていた。社長のメールアドレスで届いたメールの添付ファイルを開いてしまった。今考えると怪しいメールだった。

ランサムウェアへの対策

- メールの添付ファイル・リンク(URL)を不用意に開かない
- 定期的にバックアップを取得する（PCだけでなく、共有サーバーも）
  バックアップから復元できるか事前に確認しておく
- OSや利用ソフトウェアを最新の状態に保つ
- ウイルス対策ソフトの導入・ウイルス定義ファイルを最新に保つ

組織の対策として定期的なバックアップを。
併せてウイルス対策・脆弱性対策も忘れずに

内部不正の実態

～最新の内部不正実態調査（2016年3月3日公開）から～

内部不正を行ったことのある経験者（内部不正経験者）に対して調査

- 情報の持ち出し手段は、**USBメモリ**の利用が最多。
- 300名未満の企業の過半数は、外部記録媒体の利用制限に関する方針やルールがないと回答。
- 外部記録媒体に関する利用ルールの徹底、および利用制限を！

故意の内部不正（情報持ち出し）に関する動機、対象情報、手段等

項目	1位	2位	3位
不正行為者	システム管理者 23.5%	技術者・開発者 22.1%	経営層・役員 17.4%
不正行為の動機	業務が忙しく終わらせるため持ち出した 38.1%	処遇や待遇に不満があった 26.1%	持ち出した情報や機材で転職を有利にしたかった 16.7%
対象情報	顧客情報 48.3%	技術情報 36.9%	営業計画 32.9%
持ち出し手段	USBメモリ 53.0%	電子メール 28.9%	紙媒体 18.8%

故意の不正行為の経験者：n=98、「不正行為の動機」はn=84　「不正行為の動機」以外は複数回答

内部不正の実態

経営者・システム管理者と内部不正経験者が有効と考える対策

- 経営者等が重要視していない対策が内部不正行為に効果的
- 内部不正を減らすには、不正行為を思いとどまらせるのに有効な対策を的確に把握し実施することが必要

内部不正経験者		対策	経営者・システム管理者	
順位	割合		順位	割合
1位	50.0%	ネットワークの利用制限がある（メールの送受信先の制限、Webメールへのアクセス制限、Webサイトの閲覧制限がある）	2位	30.3%
2位	46.5%	技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）	4位	27.0%
3位	43.0%	技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる	1位	43.9%
4位	25.0%	職務上の成果物を公開した場合の罰則規定を強化する	12位	12.8%
5位	23.5%	管理者を増員する等、社内の監視体制を強化する	11位	13.1%

（内部不正経験者：n=200、経営者・システム管理者：n=1500）

内部不正対策
内部不正防止ガイドラインの活用

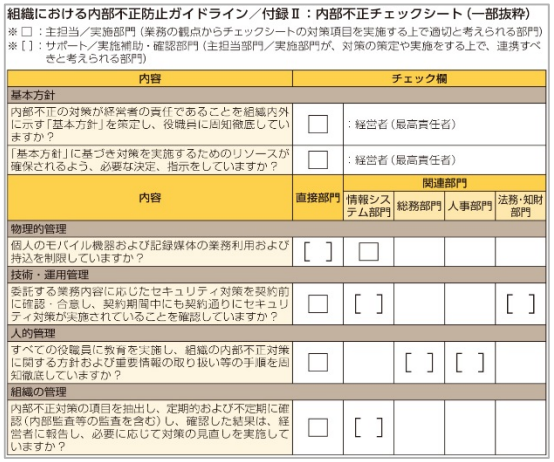
内部不正を防止するための環境整備に役立てて頂くためのガイドライン。
内部不正チェックシートで現状の対策状況を把握。

①対策の指針、ポイントを理解する
リスクに対する具体的な対策を立案するためのヒント

組織における内部不正防止ガイドライン（第3版）

https://www.ipa.go.jp/security/insider/index.html

内部不正チェックシート（付録）



組織における内部不正防止ガイドライン／付録Ⅱ：内部不正チェックシート（一部抜粋）

※□：主担当／実施部門（業務の観点からチェックシートの対策項目を実施する上で適切と考えられる部門）
※[ ]：サポート／実施補助・確認部門（主担当部門／実施部門が、対策の策定や実施をする上で、連携すべきと考えられる部門）

内容	チェック欄					
基本方針						
内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか？	□	：経営者（最高責任者）				
「基本方針」に基づき対策を実施するためのリソースが確保されるよう、必要な決定、指示をしていますか？	□	：経営者（最高責任者）				
内容	直接部門	関連部門 情報システム部門	総務部門	人事部門	法務・知財部門	
物理的管理						
個人のモバイル機器および記録媒体の業務利用および持込を制限していますか？	[ ]	□				
技術・運用管理						
委託する業務内容に応じたセキュリティ対策を契約前に確認・合意し、契約期間中にも契約通りにセキュリティ対策が実施されていることを確認していますか？	□	[ ]			[ ]	
人的管理						
すべての役職員に教育を実施し、組織の内部不正対策に関する方針および重要情報の取り扱い等の手順を周知徹底していますか？	□		[ ]	[ ]		
組織の管理						
内部不正対策の項目を抽出し、定期的および不定期に確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していますか？	□	[ ]				

②具体的な実施策を立案する
製品・ソリューションを検討

参考）JNSA※内部不正対策ソリューションガイド

内部不正ガイドラインの30の対策項目を実現するための製品やサービスをまとめたソリューションガイド。

http://www.jnsa.org/solguide/index.htm

※JNSA：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

日本におけるCISOの状況

経営者の関与、組織的な取り組みの日・米・欧比較調査

情報セキュリティ対策の実施にCISO設置は有効だが、日本はCISO任命率が欧米より低い

CISOの任命と情報セキュリティ対策推進状況の関係

	地域	経営層としてCISO任命 ※1	経営層より下の層にCISO任命 ※2	CISO任命なし ※3
経営層が参加する情報セキュリティに関する意思決定の場がある	日	89.3%	68.6%	37.3%
	米	77.4%	58.3%	39.4%
	欧	78.0%	49.6%	36.1%
リスク分析を実施している	日	84.9%	71.2%	43.3%
	米	83.5%	64.1%	46.8%
	欧	78.0%	62.7%	42.6%
サイバー攻撃が発生した場合を想定した被害額を推定している	日	71.6%	67.3%	34.7%
	米	69.4%	58.7%	27.7%
	欧	81.2%	66.9%	27.9%

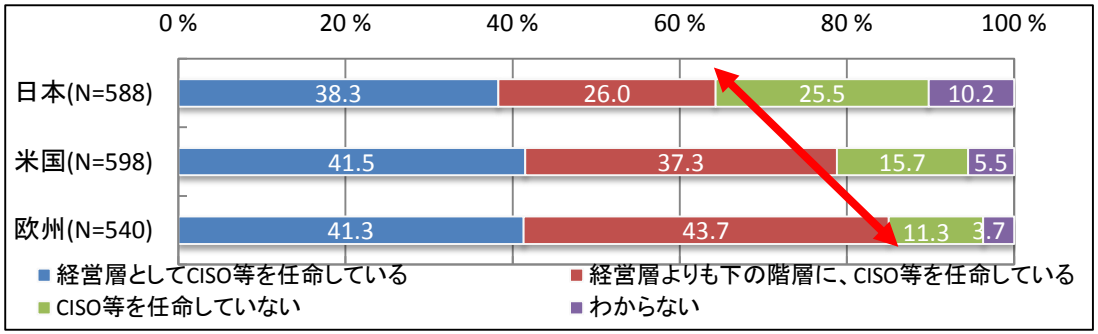
上昇

上昇

約2倍

経営層としてCISOを任命している場合、CISO任命なしの場合と比較し情報セキュリティ対策の実施率は高い（本調査の結果、約２倍）

※1:日(n=225)、米(n=248)、欧(n=223) ※2:日(n=153)、米(n=223)、欧(n=236) ※1:日(n=150)、米(n=94)、欧(n=61)



しかし、CISO任命率が欧米より低い

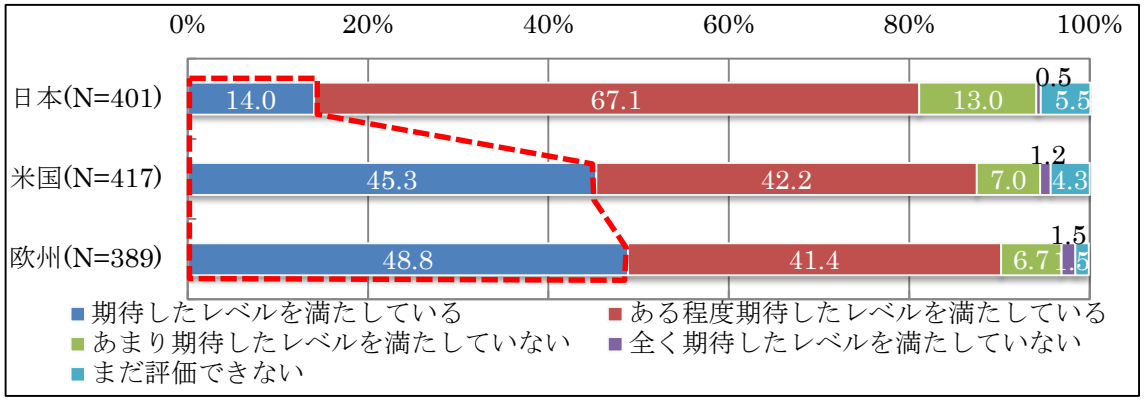
報告書：https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/ 調査対象：従業員数３００人以上

日本におけるCSIRTの状況

経営者の関与、組織的な取り組みの日・米・欧比較調査

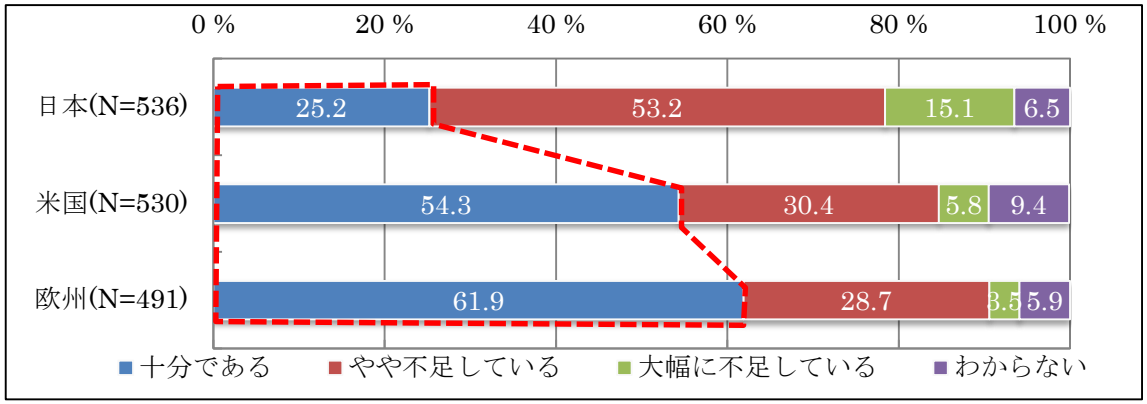
日本の企業では、CSIRTは設置したが、人材の能力・スキル不足を実感しており、現状に満足していない

CSIRTの満足度（有効性の全体評価）



日本はCSIRTに対する満足度評価が欧米より低い

情報セキュリティ人材の質的充足度



情報セキュリティ人材の質的充足度が欧米より低い

まとめ

- 外部からの新しい脅威への備え
- 内部不正への有効な対策の把握
- CISOはセキュリティ対策の実施に有効
- CSIRTはセキュリティ人材の強化が課題