

団体向けリスクマネジメント普及啓発セミナー (情報セキュリティ) 第 1 回

会場：東京都中小企業会館
「8 階 C 会議室」

●スケジュール・内容

令和元年 8 月 2 日 (金) 14:00～16:00

【中小企業を巡るサイバーセキュリティ の現状とその対策 1】

講 師 情報セキュリティ大学院大学 学長補佐

情報セキュリティ研究科教授 湯浅 壱道 氏

●封入資料

- ① テキスト
- ② アンケート
- ③ 団体向けリスクマネジメント普及啓発事業リーフレット
- ④ 団体向けリスクマネジメント普及啓発セミナー(自然災害)開催案内
- ⑤ 団体向けリスクマネジメント普及啓発セミナー
(サイバーセキュリティ)開催案内
- ⑥ 中小企業向けサイバーセキュリティ対策の極意 (東京都 発行)
- ⑦ BCP 事業継続計画 (東京都 発行)
- ⑧ BCP 策定支援事業・地震編 (東京都中小企業振興公社)
- ⑨ BCP 策定支援事業・風水害編 (東京都中小企業振興公社)
- ⑩ BCP 実践促進助成金申請のご案内 (東京都中小企業振興公社)

平成 31 年度団体向けリスクマネジメント普及啓発事業
東京都中小企業団体中央会
団体向けリスクマネジメント普及啓発セミナー

中小企業を巡るサイバーセキュリティ の現状とその対策 1

令和元年 8 月 2 日（金）
14 時～16 時
東京都中小企業会館「8 階 C 会議室」

講 師 情報セキュリティ大学院大学
学長補佐
情報セキュリティ研究科教授 湯浅 壱道

リスクマネジメント普及啓発 サイバーセキュリティ第1回

湯浅 壘道

(情報セキュリティ大学院大学)

1

自己紹介

- 青山学院大学法学部公法学科卒業、同大学院法学研究科公法専攻博士前期課程修了、慶應義塾大学大学院法学研究科政治学専攻博士課程退学
- 慶應義塾大学講師等をへて、2004年九州国際大学法学部専任講師、2005年助教授、2007年准教授、2008年教授、副学長・国際センター長、2011年情報セキュリティ大学院大学情報セキュリティ研究科教授、2012年学長補佐
- 総務省AIネットワーク化推進会議開発原則分科会構成員、総務省情報通信政策研究所特別研究員、総務省投票環境の向上等に関する研究会構成員、日本経済再生会議裁判手続等のIT化検討会委員、経済産業省産業サイバーセキュリティ研究会WG2委員 ほか
- 情報ネットワーク法学会副理事長、デジタル・フォレンジック研究会理事、日本選挙学会理事 ほか
- 神奈川県情報公開・個人情報保護審議会委員、埼玉県本人確認情報保護審議会委員長、川崎市情報公開運営審議会副会長、渋谷区個人情報の保護及び情報公開審議会委員、一般財団法人日本データ通信協会電気通信個人情報保護推進センター諮問委員会委員長、一般財団法人日本サイバー犯罪対策センター理事、ベネッセホールディングス情報セキュリティ監視委員会委員長代理 ほか

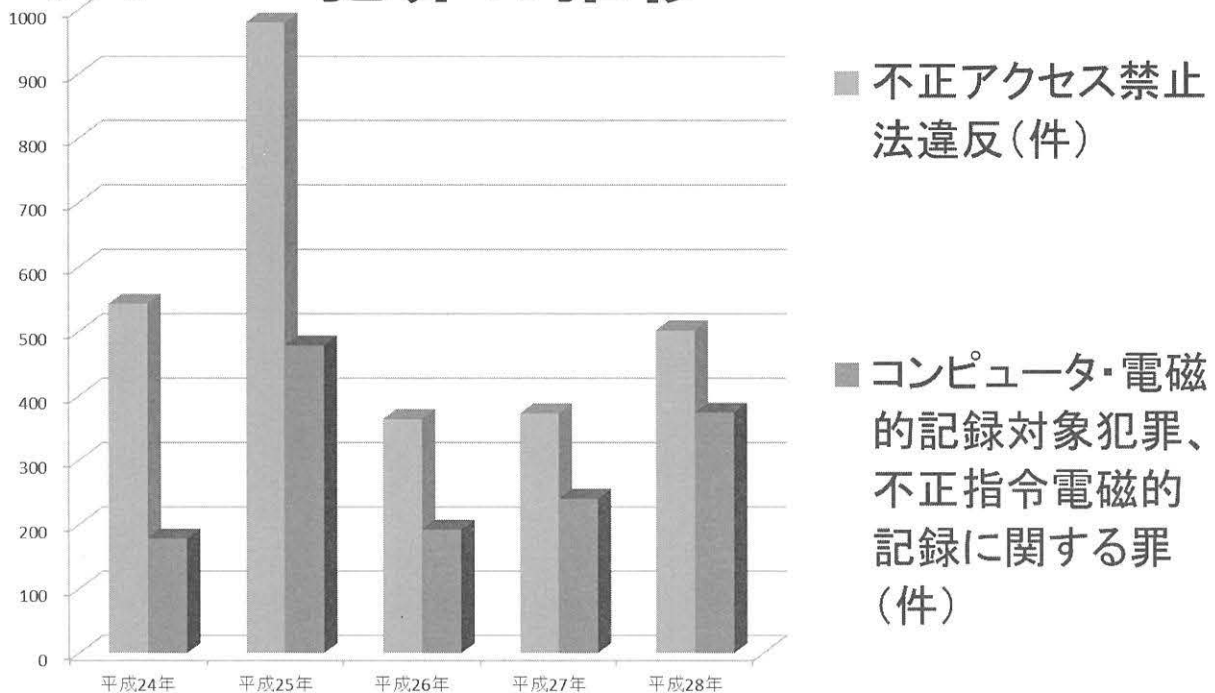
最近の情勢

- ライフログ(生まれてから死ぬまでの記録化)
- 文字(テキスト)・画像 + リアルタイム動画
像
- 遠隔化
- ソフトウェア化
- コモディティ化
- 人間を必要としない作業の増大
- 無人化

3



サイバー犯罪の推移



※警察庁統計資料による

5

中小企業:サイバー攻撃を受けやすい理由

- セキュリティ対策が不十分、セキュリティの専門家がいない
- 委託先に任せっぱなしになっている
- 情報システム担当者がいない、担当者以外はよくわからない
- サイバー攻撃を受けたことに気づかない
- 1台のパソコンを共用している、多目的に使っている
- 自社の情報資産の価値、サプライチェーンにおける位置に気づかない

大企業の場合は

- サイバーセキュリティ基本法
 - 2014年11月12日に公布され、第2章と第4章を除く部分が即日施行
 - 残された部分も2015年1月9日に施行
- 目的
- サイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定める(第1条)

7

■ 関係者の責務

国	<ul style="list-style-type: none">● サイバーセキュリティに関する総合的な施策を策定し、実施● 政府は施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置
地方公共団体	<ul style="list-style-type: none">● 国との適切な役割分担を踏まえ、自主的な施策を策定し、実施
重要社会基盤事業者	<ul style="list-style-type: none">● サービスを安定的かつ適切に提供● 自主的かつ積極的にサイバーセキュリティの確保● 国又は地方公共団体が実施する施策に協力
サイバー関連事業者	<ul style="list-style-type: none">● 自主的かつ積極的にサイバーセキュリティの確保● 国又は地方公共団体が実施する施策に協力
教育研究機関	<ul style="list-style-type: none">● 自主的かつ積極的にサイバーセキュリティの確保● 人材の育成、研究及びその成果の普及● 国又は地方公共団体が実施する施策に協力
国民	<ul style="list-style-type: none">● サイバーセキュリティの重要性に関する関心と理解● サイバーセキュリティの確保に必要な注意

8

中小企業をとりまくサイバーセキュリティ環境

■ セキュリティ経営

- サイバーセキュリティ経営ガイドライン
- サプライチェーン全体でのサイバーセキュリティの強化

■ 法律の制定・改正

- マイナンバー法
- 個人情報保護法

9

中小企業と個人情報・マイナンバーをめぐる誤解

- パート、アルバイトしか雇用していない
- 税金関係は、税理士さんに任せている
- 労務関係は、社会保険労務士さんに任せている
- 経理関係は、インターネットで処理できるシステムを導入した(「〇〇大臣」など)
- 経理は、経理担当のベテランの人に任せているから大丈夫

中小企業と個人情報

- 個人の顧客を相手とするビジネスではないので、個人顧客情報は持っていない
- 顧客の数は、さほど多くない
- お得意様の電話番号は、コンピューターではなく携帯やスマホに登録してある
- お得意様は、紙のカードや台帳で管理している
- 営業担当者が知っている、他の者は知らない
- 従業員がいない(個人で事業をしている)

11

情報漏えいの被害

- 目に見える資産
 - 被害がすぐに発見されやすい
- 目に見えない資産
 - 顧客に関する情報
 - 特許、技術情報、ノウ・ハウ
 - 財務に関する情報
 - 人事に関する情報
 - 戦略や新製品・サービス等の情報



個人情報漏えい

年間の漏えい人数	496万0063人
年間のインシデント件数	799件
一件あたりの漏えい人数	6578人

■ 報道や企業のウェブページ等で公開されている情報のみ

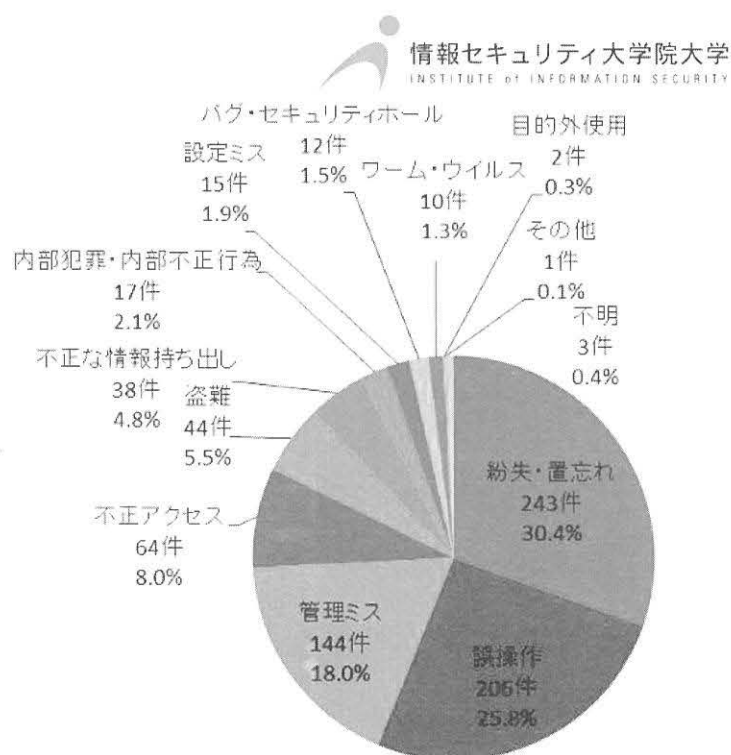
■ 実数はもっと多いと想像される

■ 日本ネットワークセキュリティ協会「2015年 情報セキュリティインシデントに関する調査報告書【速報版】」(2016年)

13

漏えいの原因

不正アクセス、盗難、不正な情報持ち出し、内部犯罪、ウィルスによるものが
1/4

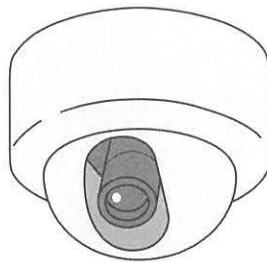


■ 日本ネットワークセキュリティ協会「2015年 情報セキュリティインシデントに関する調査報告書【速報版】」(2016年)

14

どこから漏れる？

- 不正侵入、マルウェア感染
- 利用権者のパスワード設定・管理の甘さ
 - 使い回し、初期設定のまま
 - administrator password等の安易なもの
- その他



15

漏えいの被害

■直接被害

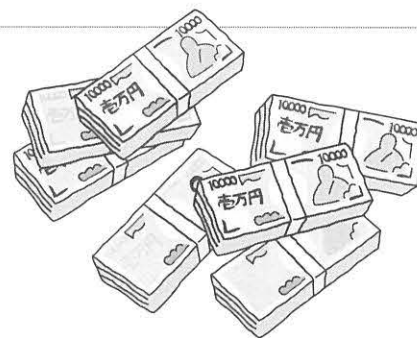
- 経済的被害(金銭的被害)
- ビジネスの中断
- 関係先への連絡や謝罪
- 対策費用・損害賠償費用
 - ◆漏えいした情報の回復や保護の費用
 - ◆事故の原因究明や対策の費用
 - 情報システムの原状回復・改善費用
 - 情報拡散防止対策費用
 - お詫び金や賠償金等

16

■ 個人情報漏えいの場合

一件あたり平均想定 損害賠償額	3億3705万円
一人あたり平均想定 損害賠償額	2万8020円

日本ネットワークセキュリティ協会「2015年
情報セキュリティインシデントに関する調査
報告書【速報版】」(2016年)



17

■ 間接被害

- 行政からの制裁(入札停止、業務停止)
- 取引の打ち切り
- 社会的信用(消費者のイメージ、企業の評判)・株価
- 社内の雰囲気悪化や従業員のモラルの低下

- 企業の業績に打撃

18

サプライチェーンの影響

■ サプライチェーンとは？

- 原材料の段階から、製品やサービスが消費者の手に届くまでのすべてのプロセス



19

■ 「サイバーセキュリティ経営ガイドライン」

- 平成27年12月28日公表
- 経済産業省・独立行政法人情報処理推進機構

■ サイバーセキュリティ経営の3原則

- 「(2) 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要」

20

- サプライチェーンのビジネスパートナーやITシステム管理の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じる。
- 自社のみならず、サプライチェーンのビジネスパートナーやITシステム管理の委託先を含めたセキュリティ対策を徹底することが必要。

- 委託先、再委託先の管理強化を求める
- 下請け、孫請け先の企業の管理強化を求める

21

サイバーセキュリティ基本法の内容

■ 2014年成立

■ 目的

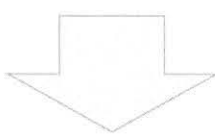
- サイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定める(第1条)

■ 定義(第2条)

- 次の措置が講じられ、その状態が適切に維持管理されていること
 - ◆1 電磁的方式により記録され、又は発信・伝送・受信される情報の漏えい、滅失又は毀損の防止その他の安全管理のために必要な措置
 - ◆2 情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置

23

■ ※

- 2の中には、電磁的記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む
 - ネットワークに接続された電子計算機以外も含まれる
- 
- 具体的には、USBメモリを経由したマルウェア感染などを想定、これによる被害防止のために必要な措置も含まれる

24

■ 基本理念

第1項	情報の自由な流通の確保を目的として、脅威に対し、多様な主体の連携により、積極的に対応
第2項	国民一人一人の認識を深め自発的対応を促す 脅威による被害を防止し被害から迅速に復旧できる強靱な体制を構築
第3項	高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築
第4項	国際的な秩序の形成及び発展のために先導的な役割を担い、国際的協調の下に実施
第5項	高度情報通信ネットワーク社会形成基本法（IT基本法）の基本理念に配慮
第6項	国民の権利を不当に侵害しないように留意

25

■ 関係者の責務

国	<ul style="list-style-type: none"> サイバーセキュリティに関する総合的な施策を策定し、実施 政府は施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置
地方公共団体	<ul style="list-style-type: none"> 国との適切な役割分担を踏まえ、自主的な施策を策定し、実施
重要社会基盤事業者	<ul style="list-style-type: none"> サービスを安定的かつ適切に提供 自主的かつ積極的にサイバーセキュリティの確保 国又は地方公共団体が実施する施策に協力
サイバー関連事業者	<ul style="list-style-type: none"> 自主的かつ積極的にサイバーセキュリティの確保 国又は地方公共団体が実施する施策に協力
教育研究機関	<ul style="list-style-type: none"> 自主的かつ積極的にサイバーセキュリティの確保 人材の育成、研究及びその成果の普及 国又は地方公共団体が実施する施策に協力
国民	<ul style="list-style-type: none"> サイバーセキュリティの重要性に関する関心と理解 サイバーセキュリティの確保に必要な注意

26

■サイバーセキュリティ戦略

- 国はサイバーセキュリティに関する基本的な計画(サイバーセキュリティ戦略)を定めなければならない
- 内閣に、内閣官房長官を本部長とするサイバーセキュリティ戦略本部を設置
- 平成17年に内閣官房に設置された情報セキュリティセンター(NISC)を改組し、サイバーセキュリティ戦略本部を設置
- 本部員
 - ◆国家公安委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣、その他有識者

27

■多様な主体の連携(16条)

- 国の機関相互の連携
 - 国の主導の下、国・地方公共団体・重要社会基盤事業者・サイバー関連事業者等の多様な主体が、相互に連携
 - サイバーセキュリティに関する施策に取り組む
 - 国は必要な施策を講ずる
- ※JC3 (一般財団法人日本サイバー犯罪対策センター)
- 産業界、学術研究機関、捜査機関が連携

28

セキュリティ対策

29

セキュリティのCIA

■ 情報セキュリティの3大要素 (CIA)

機密性

Confidentiality

完全性

Integrity

可用性

Availability

30

■ 内部要因

- 情報システムの脆弱性
- 組織に内在する脆弱性
- ノートPCの置き忘れ
- 無線LANの脆弱性
- 内部犯
 - ◆ B社事件
 - ◆ A社事件

31

時事ドットコムニュース > 社会 > アシックス秘密情報持ち出し＝容疑で元社員逮捕－兵庫県警



アシックス秘密情報持ち出し＝容疑で元社員逮捕－兵庫県警

2019年03月13日20時50分



ビジネスフリーローン（個人事業主向け）

審査結果のご連絡は 最短翌平日窓口営業日



スポーツ用品大手のアシックス（神戸市）から会社の秘密情報を持ち出したとして、兵庫県警生活経済課などは13日、不正競争防止法違反容疑で元同社社員の石黒浩司容疑者（31）＝川崎市幸区新塚越＝を逮捕した。同容疑者は同業他社に転職しており、「自分の役に立つと思い、不正に入手した」と容疑を認めているという。

<https://www.jiji.com/jc/article?k=2019031301300&g=soc>

32

■ 外部要因

● 技術的な外部脅威

◆ 不正侵入

◆ マルウェア感染

◆ DOS攻撃

● 物理的な外部脅威

◆ 災害

◆ 盗難

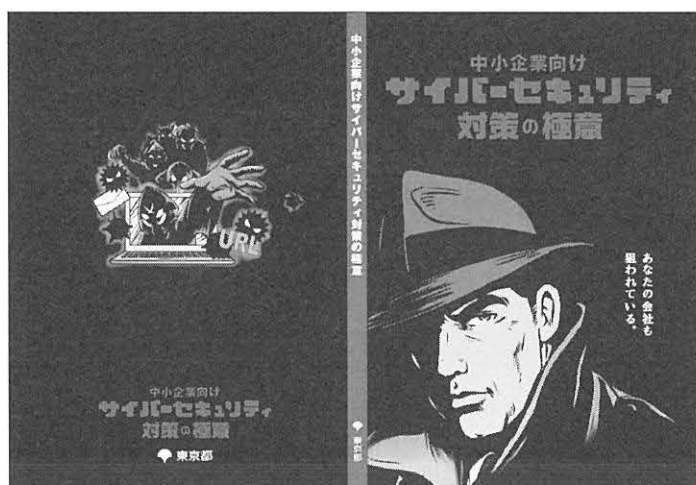
中小企業支援

東京中小企業サイバーセキュリティ支援ネットワーク (Tcyss)

- 警視庁、東京都、中小企業支援機関及びサイバーセキュリティ対策機関等が連携
- 中小企業のサイバーセキュリティ対策の強化と支援、情報共有
 - 対策シンポジウム
 - 電話相談窓口
 - 設備等導入の支援(東京都)

35

■ 中小企業向けサイバーセキュリティのハンドブック作成



http://www.sangyo-rodo.metro.tokyo.jp/chushou/guidebook_full.pdf

36

■ 設備等導入の支援

● 東京都・東京都中小企業団体連合会

団体向けサイバーセキュリティ向上支援事業のご案内

更新18/7/4
18/4/23

＜特別支援＞「団体向けサイバーセキュリティ向上支援事業」

サイバーセキュリティ対策に取り組む団体と会員企業をコーディネータ法人が包括的に支援します。

・事業内容ご案内書 「（事業説明会の案内を含む）」

問い合わせ先：東京都中小企業団体連合会 業務課
中央区銀座2-10-18 東京都中小企業会館 7階
電話 03-3542-0317

<https://www.tokyochuokai.or.jp/flashpast/flash-2018/1598-2018-04-20-06-33-27.html>

