(ISC)² Secure Events

SECURE TOKYO 2017

Secure Tokyo

サイバーセキュリティの最新動向と経営の役割

2017年9月11日

NRIセキュアテクノロジーズ株式会社

上級セキュリティコンサルタント　与儀　大輔

Share the Next Values!

自己紹介

与儀 大輔，CISSP　（Daisuke Yogi, CISSP）

Certified Information Systems Security Professional

- 1994年～2007年　横河電機
  2007年～2012年　ラック
  2012年　12月～　野村総合研究所
  2012年　12月～　NRIセキュアテクノロジーズ

- ＜主な対外活動及び受賞＞
  - NPO 日本ネットワークセキュリティ協会 幹事
  - 情報セキュリティ大学院大学　客員研究員
  - 2017年アジア・パシフィック
    情報セキュリティ・リーダーシップ・アチーブメント(ISLA)

JNSA

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(ISC)² ISLA asia-pacific

- ＜政府等委員会＞
  - 情報処理推進機構 情報セキュリティ人材育成委員会　委員
  - 経済産業省　情報セキュリティ人材の育成指標等の策定　主査
  - 内閣官房情報セキュリティセンター　セキュリティ人材育成委員会　委員
  - 情報通信機構　実践的サイバー防護演習　実行委員会　推進委員

目次

本日お話したいこと

- 昨今のサイバーセキュリティの攻撃は「防ぎきれないもの」となりつつある

- サイバーセキュリティは、IT部門の１テーマではなく、経営レベルで取り組まなければならない問題である

- まず、「リスクの可視化」と「人材育成」から着手するのがよい

1．最近のサイバーセキュリティ事件簿

2．昨今のサイバーセキュリティの脅威状況

3．企業のセキュリティ対応状況と課題

4．求められる企業の対応策

5．まとめ

事例1：日本年金機構で発生した情報流出


年金情報125万件流出

出所）日本経済新聞 2015年6月2日

2015年6月1日　日本年金機構発表

- 職員の端末がサイバー攻撃を受け、約125万件の年金情報が外部に流出
- 流出した情報は加入者の基礎年金番号と氏名
- うち5万2000件は生年月日、住所を含む

<u>業務を装ったメールの開封によるPCのウイルス感染</u>

学術機関の職員を装った電子メールに、セミナーの案内状と称したウイルス付きの文書ファイルが添付されており、これを開封した少なくとも2人の機構職員の端末が感染。
端末同士をつなぐLANシステム内のファイル共有サーバーに保管されていた基礎年金番号や氏名などの情報が、ファイルごと抜き取られたとみられる。

事例１：日本年金機構で発生した情報流出

■ 影響

● 経費

- 新たな年金手帳の発行等に約11.3億円の経費
  - ➢ 基礎年金番号変更に伴う、新しい年金手帳の発行・送付　約5.0億円
  - ➢ 加入者への問い合わせ対応に設置した専用ダイヤル(コールセンター)運営　約3.7億円
  - ➢ 情報漏えいした約101万人へのお詫び文書送付　約1.4億円
  - ➢ 電子ファイル、アクセス権限調査等経費　約0.5億円
  - ➢ その他（チラシ作成・配布、なりすまし防止対策経費等）　約0.7億円

● 関係者への制裁

- 厚生労働省　大臣、副大臣２名、政務官２名が閣僚給与・賞与辞退
  官房長以下15名が戒告、訓告、厳重注意措置
- 日本年金機構　役員、理事長以下14名が戒告、訓告及び賞与不支給
  職員12名が戒告、訓告、注意措置

● 「サイバーセキュリティ基本法」への影響

- 国が行う、不正な通信の監視、監査、原因究明調査等の対象範囲を、独立行政法人、特殊法人・認可法人まで拡大

事例2：ベネッセで発生した顧客情報流出

2014年7月9日　ベネッセホールディングス発表

- 「進研ゼミ」などの顧客情報760万件が社外に漏えいしたと発表。詳細は調査しており、漏えい件数は最大2070万件（最終的に3504万件と判明）
- 漏えいした情報は進研ゼミを受講する子供や保護者の名前や住所、電話番号など

派遣社員による情報の不正持ち出し

同社のシステム開発・運用を行っているグループ会社に派遣されていたシステムエンジニアが、データーベースに保管されていた個人情報を自身のスマートフォンに転送し社外へ持ち出し。名簿業者3社に対し売却。
漏えいした個人情報の件数は最終的に3504万件、人単位では約4858万人分にのぼり、該当派遣社員は逮捕された。

出所）日本経済新聞 2014年7月10日

事例2：ベネッセで発生した顧客情報流出

■ 影響

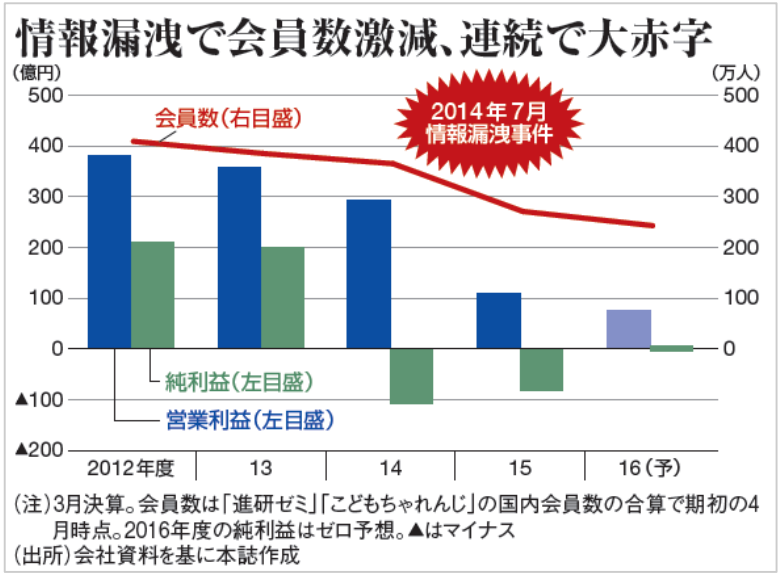
● 経費

- 2014年度情報セキュリティ対策費260億3900万円を特別損失として計上

● 業績への影響

- 事件発生以降、中核サービスの顧客離れが進み、株価も低迷
- ２期連続の減収減益で社長が引責辞任（2016年5月）

出所）Google Finance



出所）週刊東洋経済 2016年5月28日号

1．最近のサイバーセキュリティ事件簿

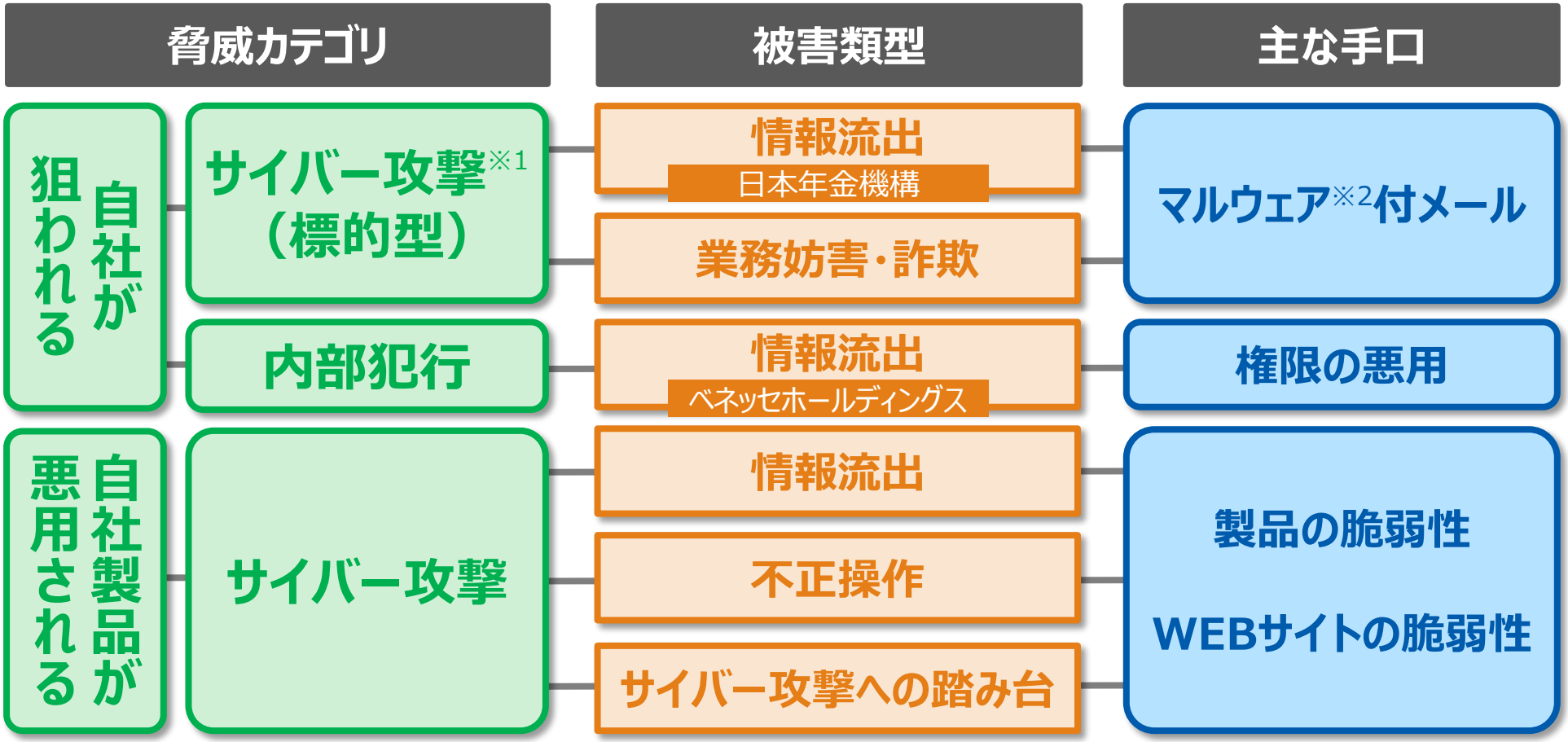
2．昨今のサイバーセキュリティの脅威状況

3．企業のセキュリティ対応状況と課題

4．求められる企業の対応策

5．まとめ

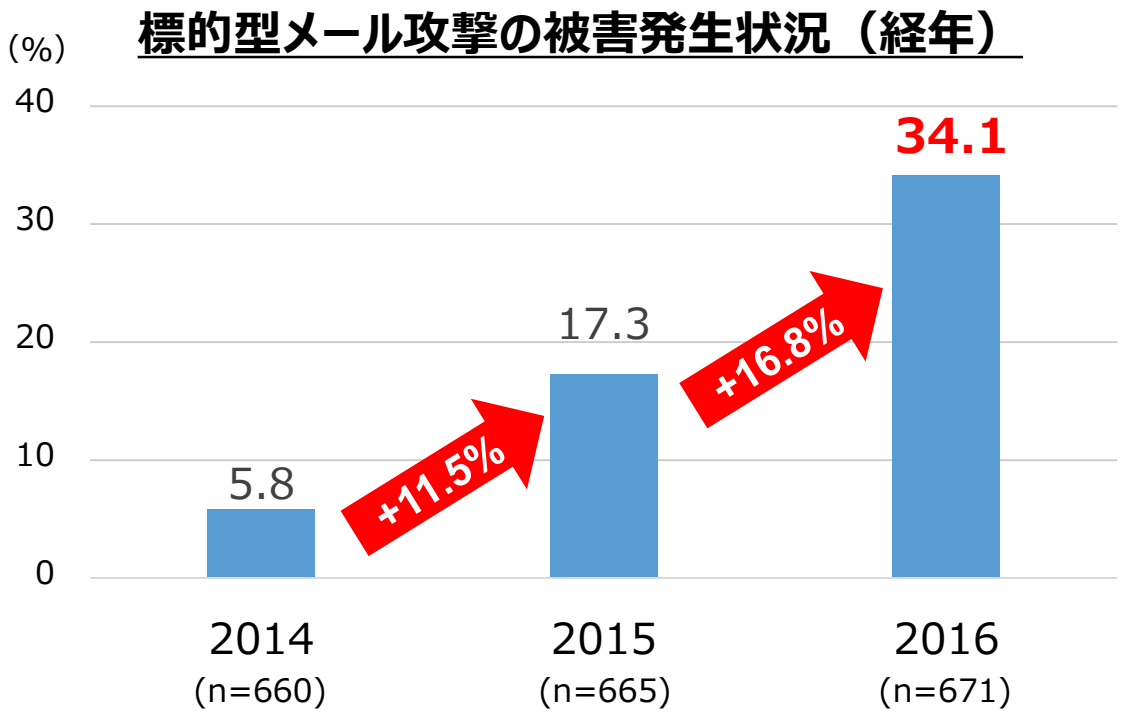
昨今のサイバーセキュリティの脅威分類



※1 サイバー攻撃 ： インターネットを介して行なわれる、破壊活動や情報の窃取、改ざん
※2 マルウェア ： コンピューターウイルスなど、不正かつ有害な動作を行う意図で作成された、悪意のあるソフトウェアの総称

自社が狙われる：サイバー攻撃（標的型）

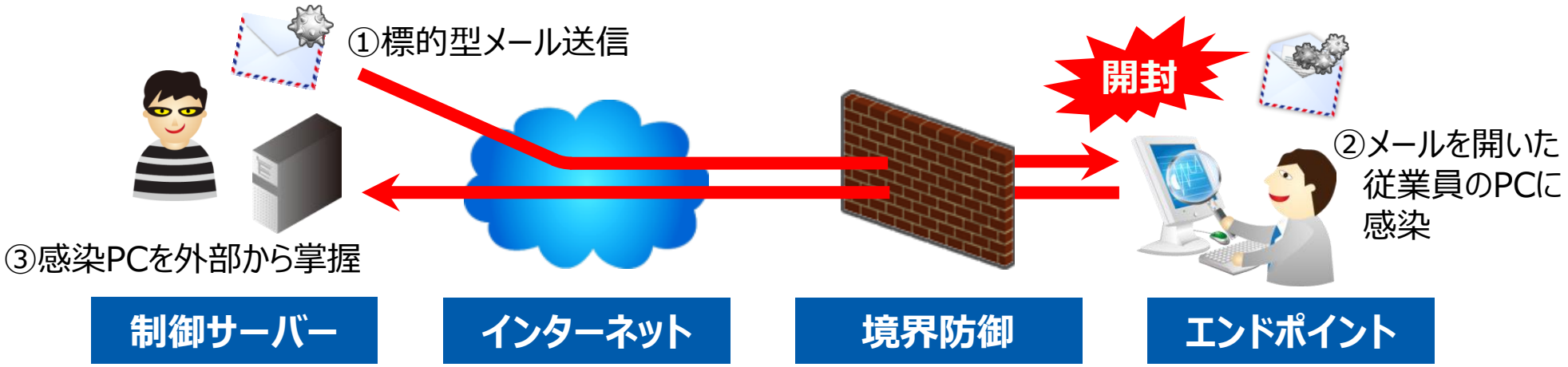
- 国内企業の約３割が、標的型メール攻撃※を経験
- この２年間で急増傾向にある



※ 標的型メール攻撃： 特定の企業や組織を狙い、巧妙に偽装されたメールを送り、マルウェアに感染させることで情報を漏えいさせる攻撃

出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2014・2015・2017」

自社が狙われる：サイバー攻撃（標的型）



- **すり抜ける攻撃メールが増加**
  - ベンダーの対応より先んじた攻撃
  - 個別組織にカスタマイズされたマルウェア
- **受信者が気づくことが困難**
  - 自然な日本語
  - 対象企業に特化したメール文面

マルウェアに感染すると・・・

- 情報流出
- 業務妨害・詐欺

自社が狙われる：サイバー攻撃（標的型）

■ 標的型攻撃のメールも巧妙になってきている

以前からありがちなメールの例

差出人　三菱東京UFJ銀行 <email@bk.mufg.jp>
件名　本人認証サー
添付

銀行からのメールとは思えない書き出し

こんにちは！

平成26年10月21日「三菱東京UFJ銀行」のシステムが安全性の更新がされたため、お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

以下のページより登録

不自然な日本語

https://entry11.bk.mufg.jp/ibg/dfw/APLIN/loginib/login?_TRANID=XXX<http://bk.mufg.jp.iinrs.com/ibg/dfw/APLIN/loginib/login.htm?_TRANID=XXX>

日本年金機構の事件で攻撃に使用されたメール

差出人　●●●●●●●●@yahoo.co.jp
件名　給付研究委員会オープンセミナーのご案内
添付　給付研究委員会オープ

実在する略称

●●　●●　様

平成27年5月に●●大学と企年協が共同で実施いたしました企業年金アンケート結果の報告会と意見交換会を下記の通り実施いたします。

アンケートの集計結果に基づく報告会は、今後の企業年金の方向性を考えるうえで、基金関係者にとって大いに参考になると思います。

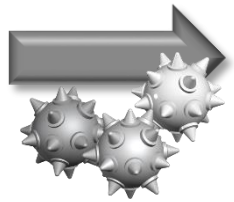
自然な日本語

会員の皆様の積極的参加を申し上げます。

お申し込みは添付資料をクリックしてください。

自社が狙われる：サイバー攻撃（標的型）

サイバー攻撃（標的型）



情報流出

■ インターネット上の制御サーバーと通信し、指令によって情報を社外に持ち出す

持ち出される主な情報	特　徴　等
個人情報	• 販売目的 • 発覚しやすい（ユーザーが気づく）
インサイダー情報（M&A等）	• 不正取引に利用
製造ノウハウ・R&D	• 産業スパイ • 発覚しにくい
メール	• 社内の人間関係を把握し、その後の攻撃に利用

自社が狙われる：サイバー攻撃（標的型）

■ 狙われる「日本の技術情報」

（参考）サイバー分野での情報漏洩事例

サイバー攻撃による情報漏洩事例が増加傾向。

サイバー攻撃報道事例

不正アクセスといわれている攻撃
標的型といわれている攻撃

時期	報道
2011/4	ソニーにサイバー攻撃、個人情報流出1億件超（朝日新聞等）
2011/9	三菱重にサイバー攻撃、80台感染…防衛関連も（読売新聞等）
2011/10	衆院にサイバー攻撃 議員のパスワード盗まれる（朝日新聞等）
2011/11	サイバー攻撃：参院会館のPC、ウイルス感染は数十台に（毎日新聞等）
2012/1	JAXA：職員のパソコン感染、無人補給機情報など流出か（毎日新聞等）
2012/2	農水省に標的型メール攻撃、情報流出狙う？（読売新聞等）
2012/6	パソコン5台、ウイルス感染か＝外部サイトと通信－原子力安全基盤機構（時事通信）
2012/7	財務省PC数か月情報流出か…トロイの木馬型（読売新聞等）
2012/9	「中国紅客連盟」の標的か…総務省統計局サイト（読売新聞等）
2012/10	国際ハッカー東大など5大学被害 情報流出の恐れ（毎日新聞）
2012/11	JAXA、ロケット設計情報流出か PCがウイルス感染（朝日新聞等）
2012/12	三菱重工もウイルス感染 宇宙関連の情報流出か（産経新聞）
2012/12	原子力機構PCウイルス感染…告発情報漏えい？（読売新聞）
2013/1	農水機密、サイバー攻撃…TPP情報など流出か（読売新聞）
2013/2	米マイクロソフトも感染、アップルと似た攻撃（読売新聞）
2013/3	韓国、サイバーテロか TV局や銀行が一斉にサーバーダウン（産経新聞）
2013/5	大分空港HP、ウイルス感染させるよう改ざん（読売新聞）
2013/6	札幌市の観光HP、不正アクセス受け閉鎖（読売新聞）
2013/7	朝日新聞記者を装うウイルスメール 国会議員2人に届く（朝日新聞）
2013/8	2ちゃん会員情報流出か カード番号3万件、メールアドレスも（産経新聞）

出典：独立行政法人情報処理振興機構 「標的型サイバー攻撃の脅威と対策」（2013）

三菱重工業に対するサイバー攻撃

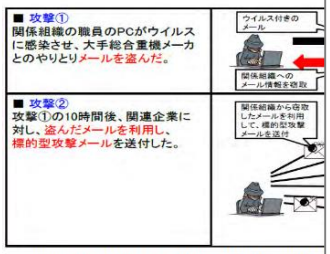
【攻撃対象】
最新鋭の潜水艦やミサイル、原子力プラン

【攻撃手法】
標的型攻撃。具体的には、約80台のパソコ
取を可能とする不正プログラムを感染（201
同年9月に発覚。

【具体的な漏えい】
同年11 月、同社は、防衛及び原子力に関す
出は認められなかった旨の調査結果を発表

【その他】
警視庁は同社から被害届を受理し、捜査。し
は至らず、2013年12月17日、警視庁公安部は
疑者不詳のまま書類送検。

標的型攻撃の事例



（出典）独立行政法人情報処理推進機構「標的型サ

標的型　不正アクセス

（参考） 秘匿化される技術（イメージ）

分野	営業秘密のイメージ
電気・電子部品	フラットパネルディスプレイなどに用いられる電気・電子部品の低弾性、高耐熱性、熱伝導性を向上させることを目的とする絶縁材料の副材料の種類、配合量、管理幅
フッ素樹脂成形品表面処理方法	接着強度を高めるための表面処理の方法（溶液の選択・接触時間、その前後の放電処理の方法）
航空機材料の試験方法	金属部品の剪断強度試験における測定値のばらつきを減らす方法（剪断強度を求める際の薄板材料へのパンチングの際の工夫）
日用品	製品特性上、すぐ破損しがちなプレス成形機の金型強度の向上方法（金属材料の選定、表面処理方法）
燃料電池用電極	電極基材、並びに金属ナノ粒子（金）及び触媒などの構成方法
レースの図柄作成アルゴリズム	糸の張力を考慮した実際の編み柄図を画面上に表示するシュミレーション機能
とんかつ用ソース	ウスターソース、ケチャップおよびマヨネーズの混合率
電磁鋼板	磁性を効率的に向上させるための方向性電磁鋼板を製造する過程における温度や加熱時の温度勾配をコントロールする製造方法

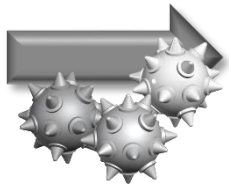
※経済産業省調べ

11

出所）経済産業省「技術流出防止・営業秘密保護強化について」
http://www.meti.go.jp/committee/sankoushin/chitekizaisan/eigyohimitsu/pdf/001_05_00.pdf

自社が狙われる：サイバー攻撃（標的型）

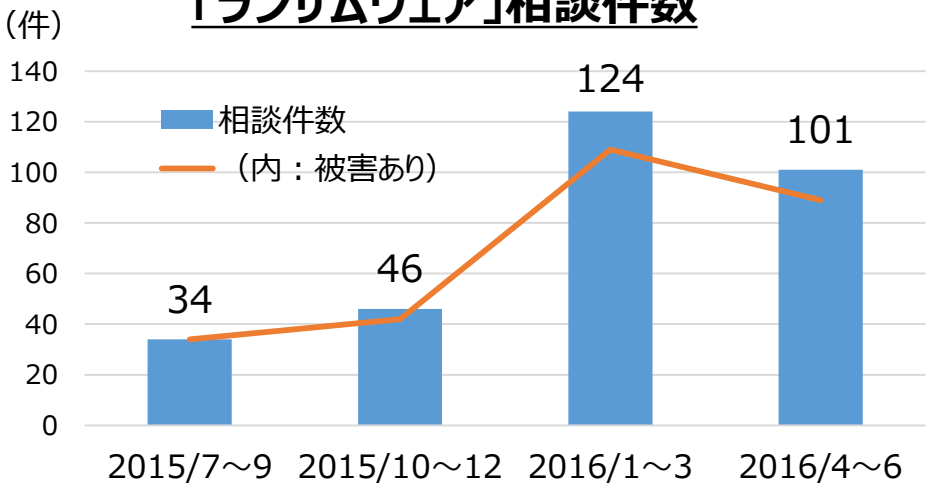
サイバー攻撃（標的型）



業務妨害・詐欺

ランサムウェア
電子ファイルを暗号化するなどして使用不能にし、
解除する見返りに「身代金（ランサム）」を要求するマルウェア

「ランサムウェア」相談件数



出所）IPA「コンピュータウイルス・不正アクセスの届出状況および相談状況［2016年第2四半期（4月～6月）］」

ランサムウェアに感染したPCの画面

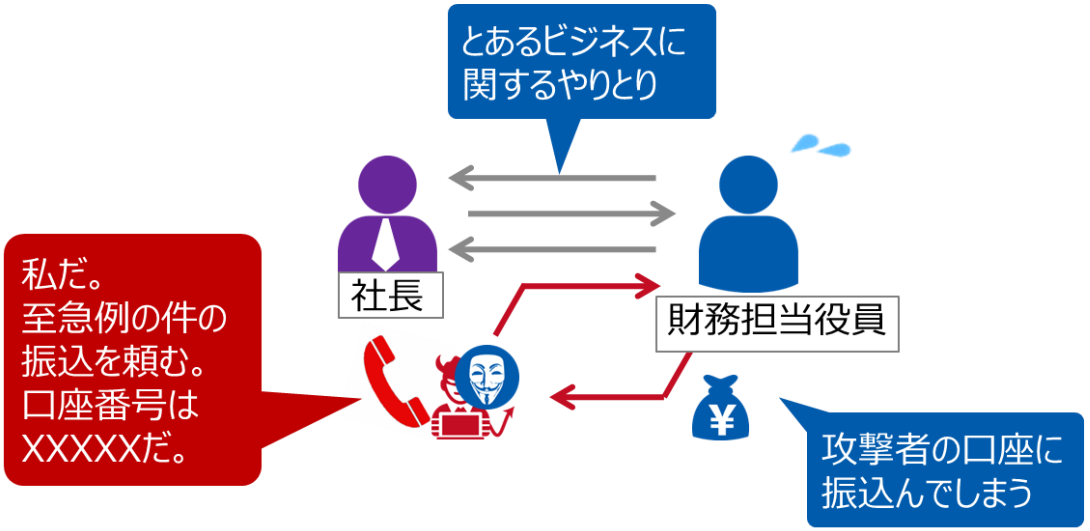
出所）トレンドマイクロ株式会社

自社が狙われる：サイバー攻撃（標的型）

サイバー攻撃（標的型） → **業務妨害・詐欺**

ビジネスメール詐欺

役員になりすまして、電話やメールで財務担当に送金指示を行い、金銭を窃取する詐欺



米FBIに寄せられた被害状況（全世界）（2016年6月時点）

被害社数	22,143社
被害総額	約3,500億円（前年のおよそ13倍）

注）被害社数・被害総額は、2013年10月からの累計
出所）FBI Internet Crime Complaint Center

自社製品が悪用される：事例

情報流出

Fisher-Price 対話型ぬいぐるみ（2016年2月）

- ユーザー（子供）のプロフィール情報流出
- 玩具の制御を一部奪い取る事も可能

不正操作

クライスラー（2015年8月）

- 車載マルチメディアシステム「Uconnect」に脆弱性があり、車外から無線でアクセス可能
- ハンドルやエンジン、トランスミッション、ブレーキシステムをコントロールできた
- 140万台のリコール

サイバー攻撃への踏み台

中国カメラメーカー Xiongmai DVR, WebCam （2016年10月）

- インターネットから乗っ取り可能な脆弱性があり、DDoS攻撃※の攻撃機器として利用される
- 数百万台の機器をリコール

※DDoS攻撃：数万台～数十万台の機器から一斉に１ヶ所にアクセスを仕掛けることにより、通常のサービス提供を阻害する攻撃。
Distributed Denial of Servicesの略

出所）Fisher-Price.com, Wired.com,Xiongmaitech.com

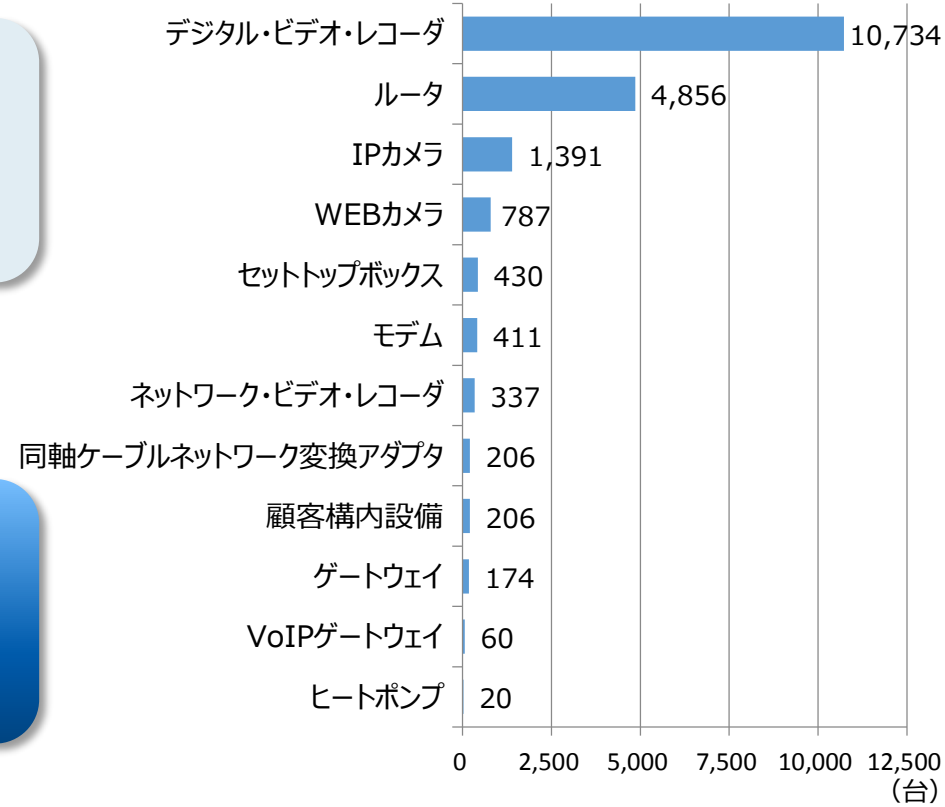
自社製品が悪用される

■ インターネットに接続される様々な機器（IoT製品）の脆弱性が悪用され、攻撃の起点とされている

ソフトウェアには製造物責任は適用されないが、
ソフトウェアを搭載した動産は製造物

製品回収・リコールやPL訴訟が発生した場合には、対応に多大なコストが発生

観測された感染機器の種類
（観測期間 2015/5/1-9/30）



出所）横浜国立大学 吉岡克成「止まらないIoTマルウェア大流行とその対策に向けて」講演資料よりNRIセキュアテクノロジーズ作成

昨今の情報セキュリティの脅威分類

※1 サイバー攻撃 ： イ
※2 マルウェア ： コン など、不正かつ有害 で作成された エアの総称

1．最近のサイバーセキュリティ事件簿

2．昨今のサイバーセキュリティの脅威状況

3．企業のセキュリティ対応状況と課題

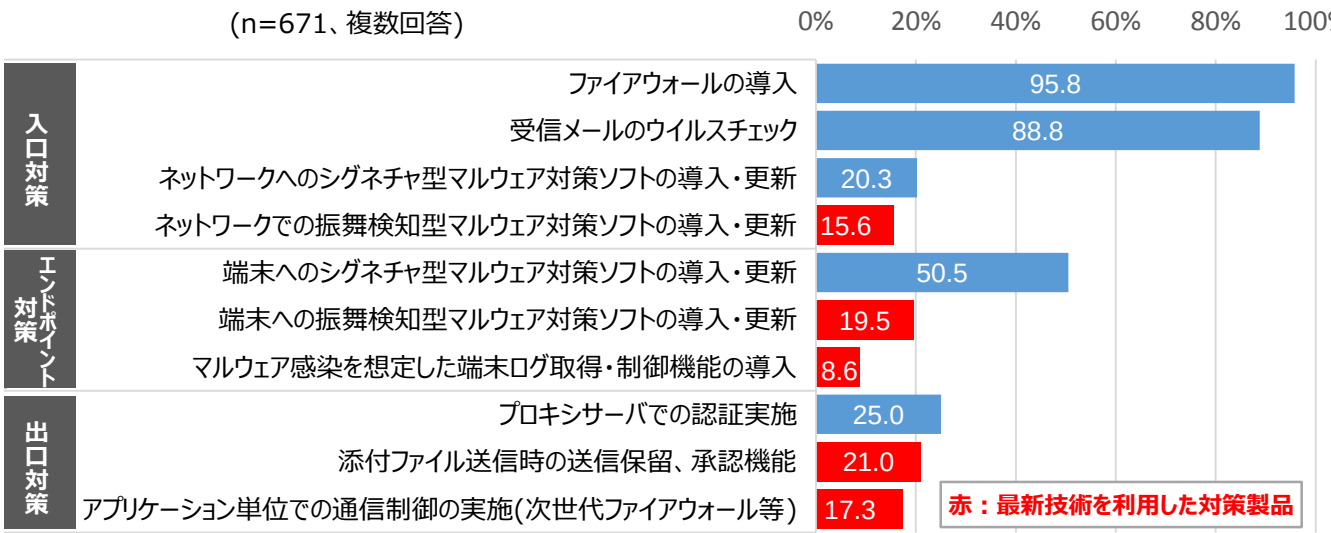
4．求められる企業の対応策

5．まとめ

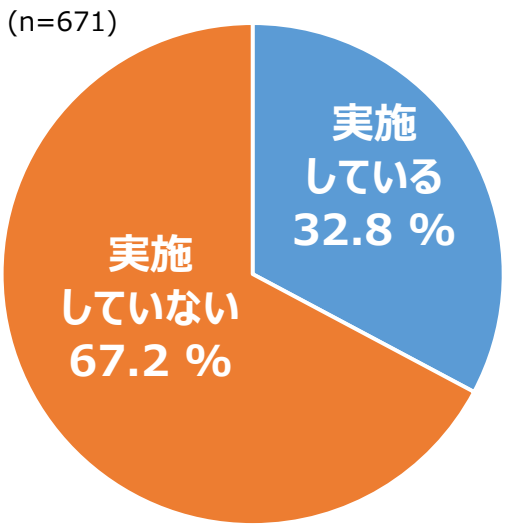
標的型メール攻撃に対する対策状況

- 旧態依然とした対策が多く、昨今の標的型メール攻撃を想定した対策は多くの企業でとられていない
- 攻撃の前面にさらされている社員の訓練も、半数以上で実施されていない

主なマルウェア対策製品の導入状況



標的型メール攻撃訓練の実施状況



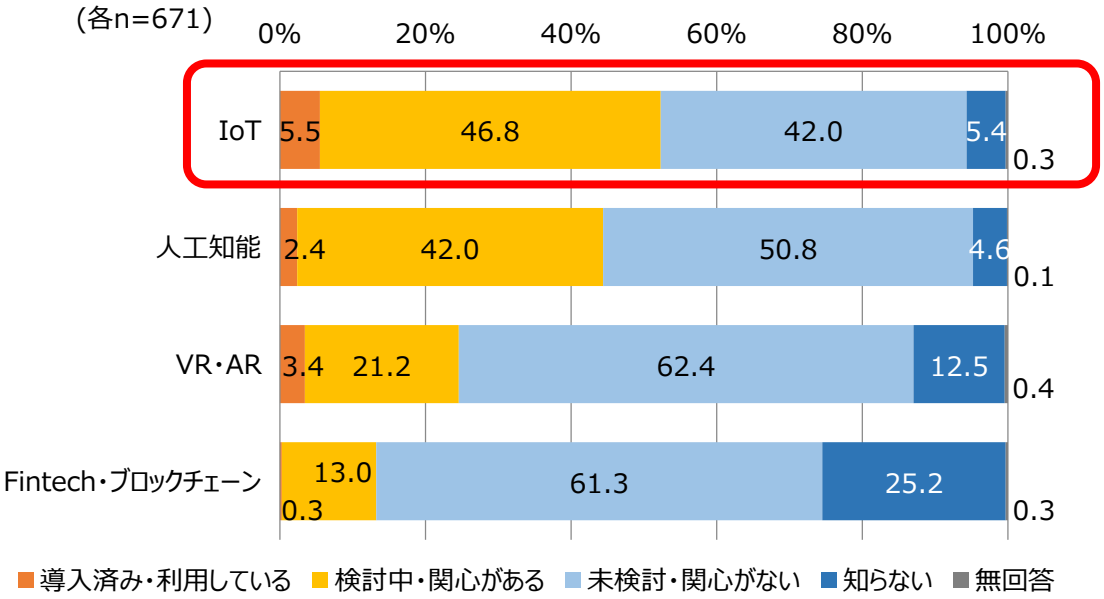
出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2017」（2016年9月～10月実施）

いつ標的型攻撃の被害に遭ってもおかしくない状況

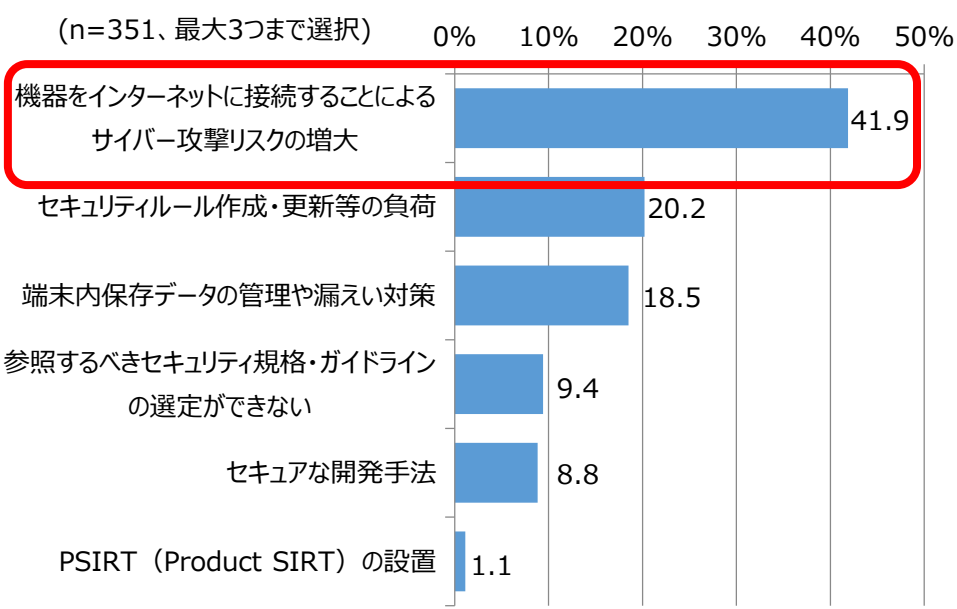
IoTに関するセキュリティ取り組み状況

- 約半数の企業で、人工知能と並んでIoTビジネスに関心を持っている
- 一方、セキュリティに関しての認識は高いとは言えず、脆弱性を持つ製品が乱造される懸念がある

新技術への取り組み状況



IoTに関する課題認識



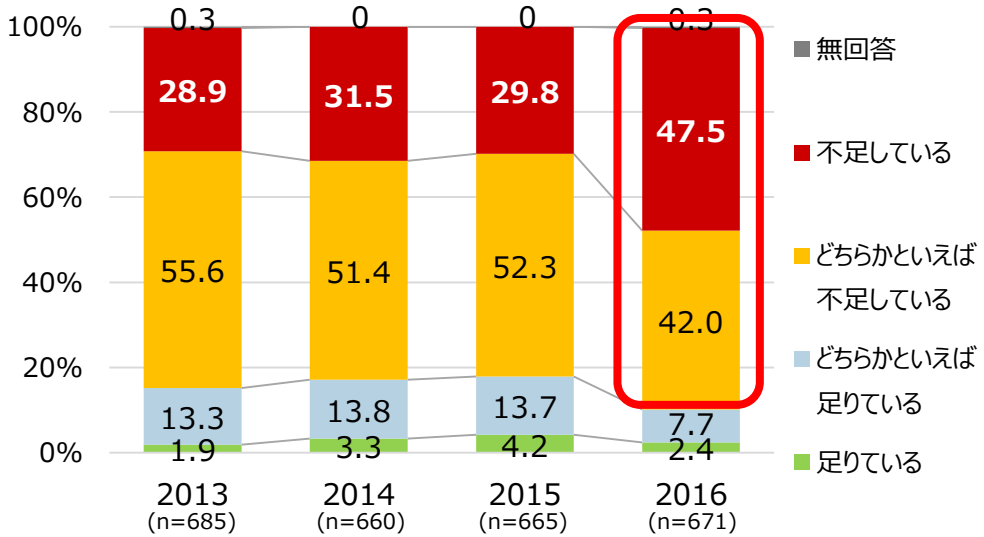
出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2017」（2016年9月～10月実施）

IoTには関心があるものの、IoTのセキュリティは手つかず

セキュリティ人材の充足状況

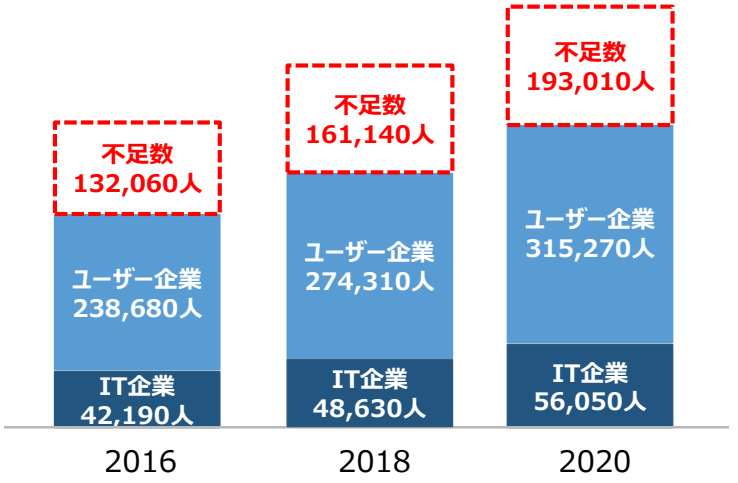
- セキュリティの専門人材が不足していると感じている企業が多数（最新の調査では**89.5%に悪化**）
- 人材不足の状況は今後さらに拡大

セキュリティ人材の充足状況



出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2017」（2016年9月～10月実施）

情報セキュリティ人材の不足数推計



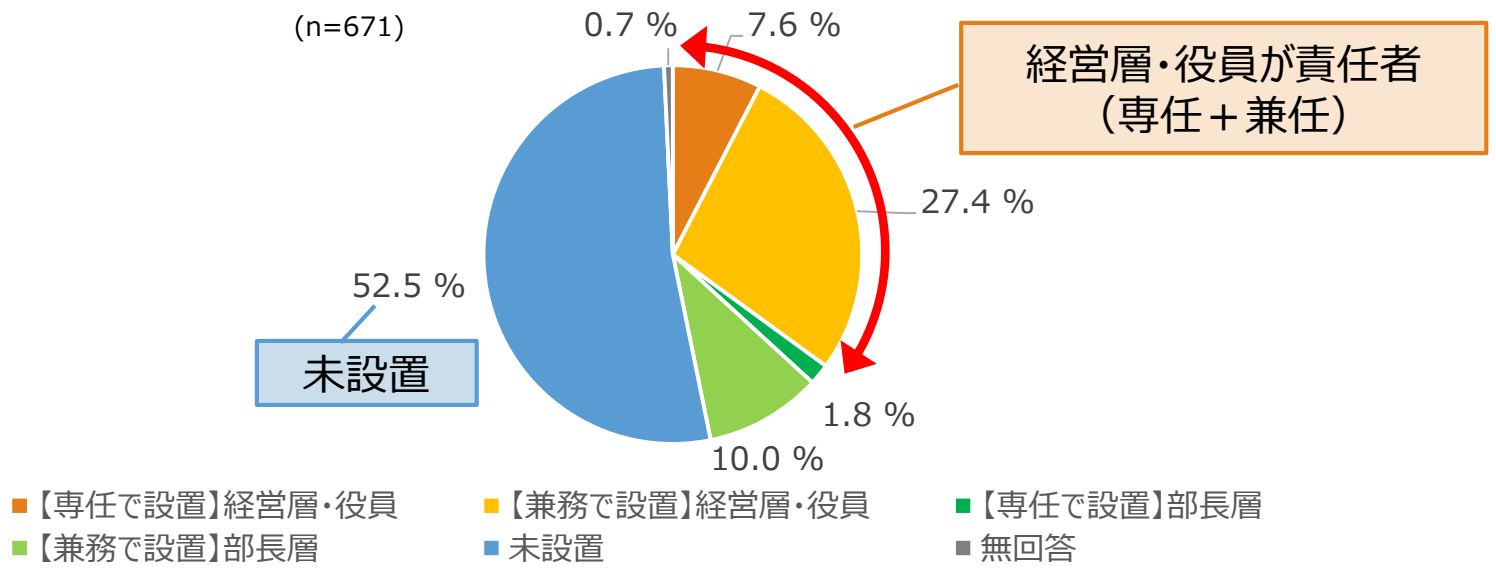
出所）経済産業省「IT人材の最新動向と将来推計に関する調査結果」
http://www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf

セキュリティ人材不足の状況に手が打たれていない

経営層の関与の状況

- 経営層が情報セキュリティの統括責任者になっているのは、３分の１
- 半数以上は、情報セキュリティの責任者を未設置

CISO（最高情報セキュリティ責任者）の設置状況

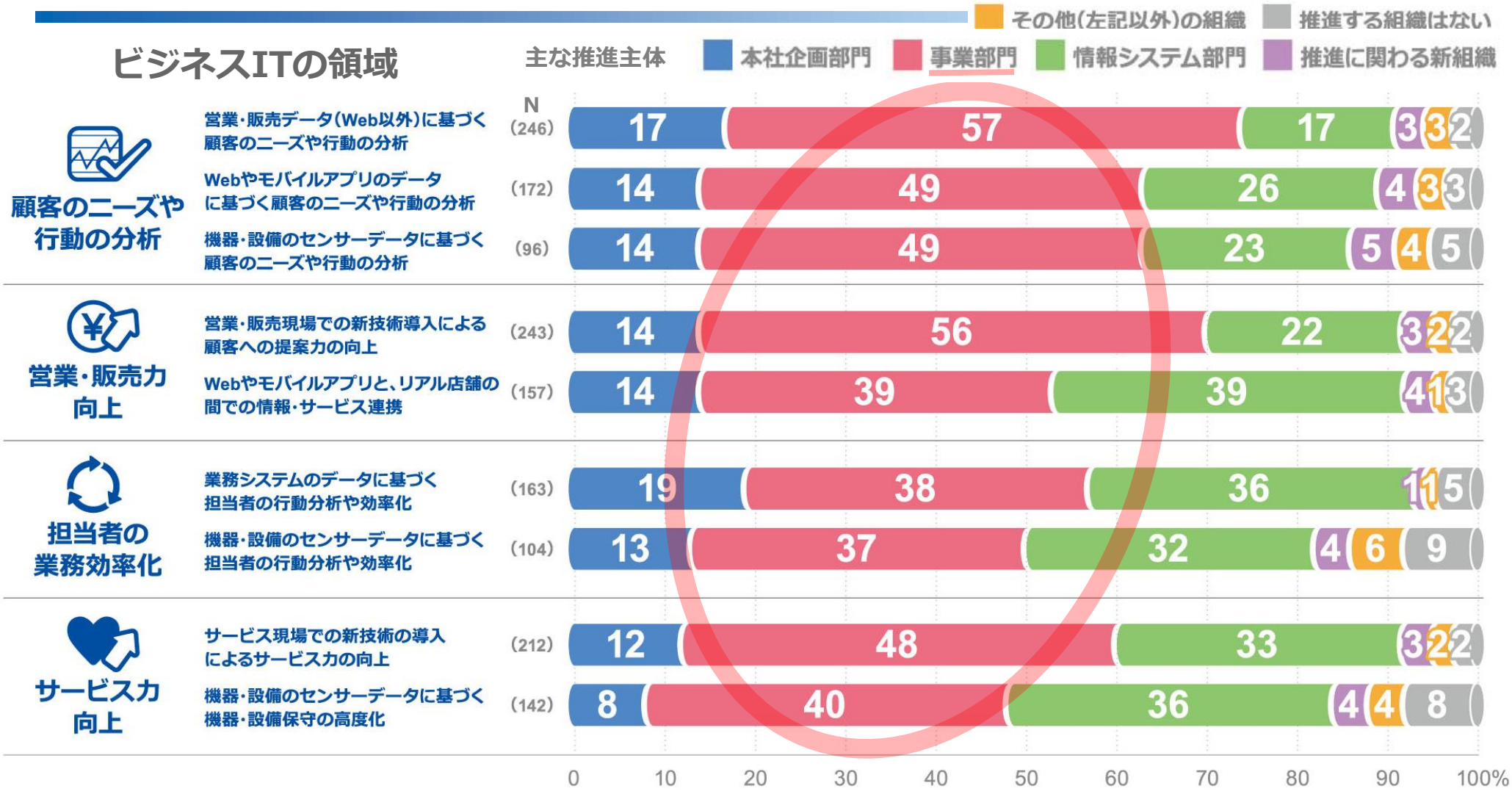


出所）NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2017」（2016年9月～10月実施）

企業経営のリスクとして捉えられていない

3．企業のセキュリティ対応状況と課題

ビジネスITの領域は、ビジネス部門が主体となっている企業が多い



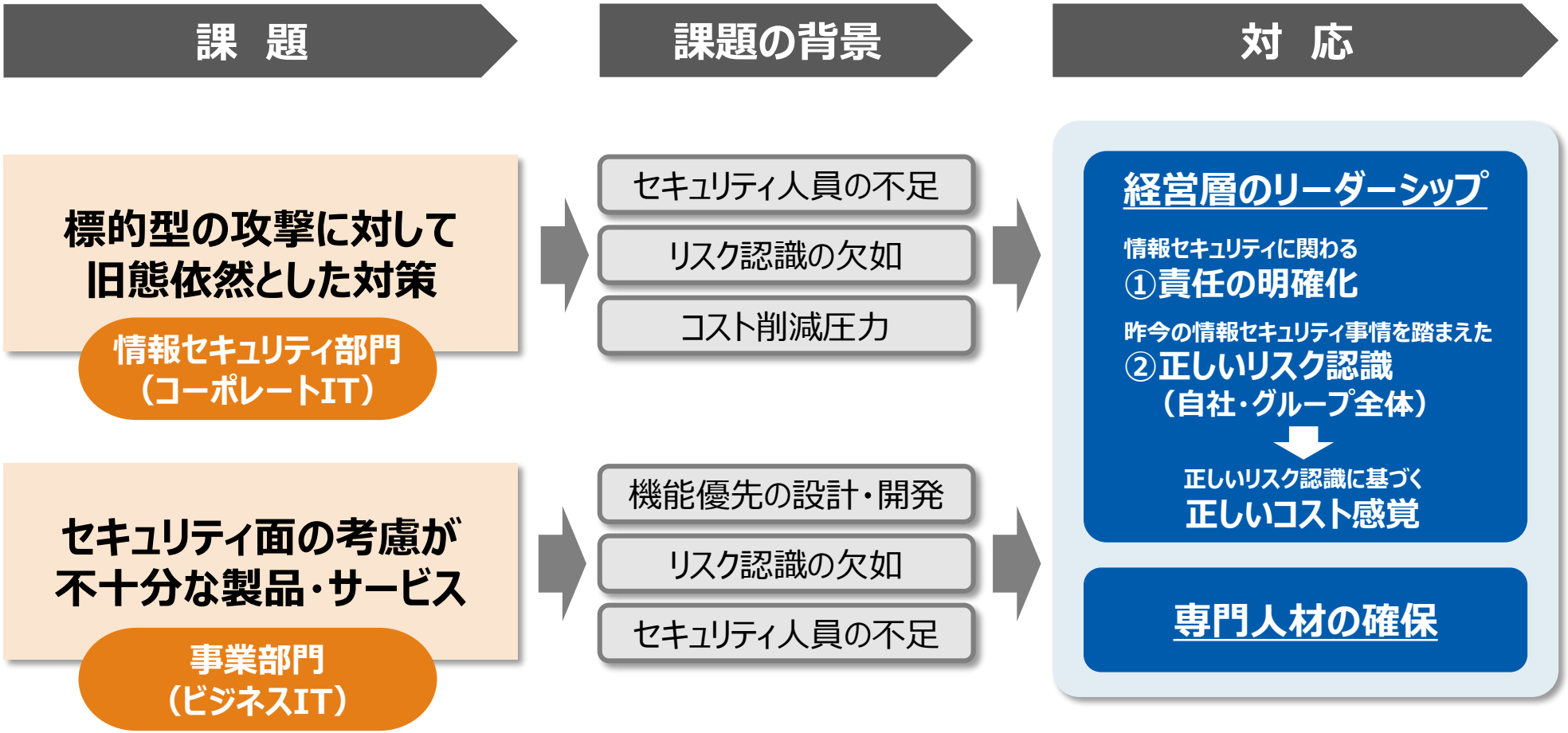
出所) 野村総合研究所 「2015年度IT活用実態調査」

自社の課題解決とビジネス拡大を支えるセキュリティ　【内部要因】
コーポレートITからビジネスITへ

- コーポレートIT から ビジネスIT へのシフトに伴い、セキュリティ対策にも変化
- ビジネス領域を拡大するにあったっては、(従来とは違った)セキュリティ対策を十分固める必要あり
- 情報セキュリティ部門だけでなく、事業部門も参画し、対策検討。セキュリティ対策が差別化ポイントに

	コーポレート IT	ビジネス IT
対策内容	従来からの攻撃に対する 旧態依然とした対策	新サービスにおける セキュリティ面を考慮した追加 対策が必要
課題	・セキュリティ人員不足 ・リスク認識の欠如 ・コスト削減の圧力　等	(左記に加えて) 機能優先の設計/開発 新たなリスク認識の欠如
対応部署	情報セキュリティ部門　が中心	事業部門の参画が必要

第３章まとめ



1．最近のサイバーセキュリティ事件簿

2．昨今のサイバーセキュリティの脅威状況

3．企業のセキュリティ対応状況と課題

4．求められる企業の対応策

5．まとめ

経営層のリーダーシップ

■ セキュリティ対策の高度化には経営層のリーダーシップが重要

- かけるべきコストを判断できるのは経営層だけ

内閣サイバーセキュリティセンター「企業経営で期待されるサイバーセキュリティの考え方」（2016年8月2日）より抜粋

セキュリティリスクは目に見えないため、特別なものと見がちであるが、数あるリスク管理の一項目に過ぎない。また、サイバーセキュリティをやむを得ない「費用」と見る傾向があるが、より積極的な経営への「投資」と位置づけるべきである。言い換えれば、企業としての「挑戦」と、それに付随する「責任」として、サイバーセキュリティに取り組むことが期待される。

「責任」の面については、セキュリティリスクの管理も、会社法において取締役会の決議事項になっている「内部統制システム構築の基本方針」の中に含まれると考えられる。つまり、事業運営にはITの活用が不可欠になっていることから、サイバーセキュリティの確保は、企業の経営層が果たすべき責任の一つである。

出所）内閣サイバーセキュリティセンター
http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

経営層のリーダーシップ：具体的施策 ①責任の明確化

- 情報セキュリティのリスク管理は、CISOだけの所管事項ではない
- 最終責任は社長にあるが、経営層全体で取り組むべき課題

社　長	情報セキュリティ文化を醸成する責任
情報セキュリティ担当役員（CISO）	情報セキュリティに関するリスクを可視化し、対策のPDCAを回す責任
情報システム部門担当役員	システム・セキュリティの統括責任
事業部門担当役員	提供事業・サービスにおける安全・安心の実施責任
総務部門担当役員	物理セキュリティの統括責任
研修部門担当役員	セキュリティマインドの養成責任
内部監査部門担当役員	社長に実態を知らせる責任
広報部門担当役員	ステークホルダーとのリスクコミュニケーションを図る責任
経営企画担当役員	企業経営に情報セキュリティのリスク管理を埋め込む責任

経営層のリーダーシップ：具体的施策 ①責任の明確化

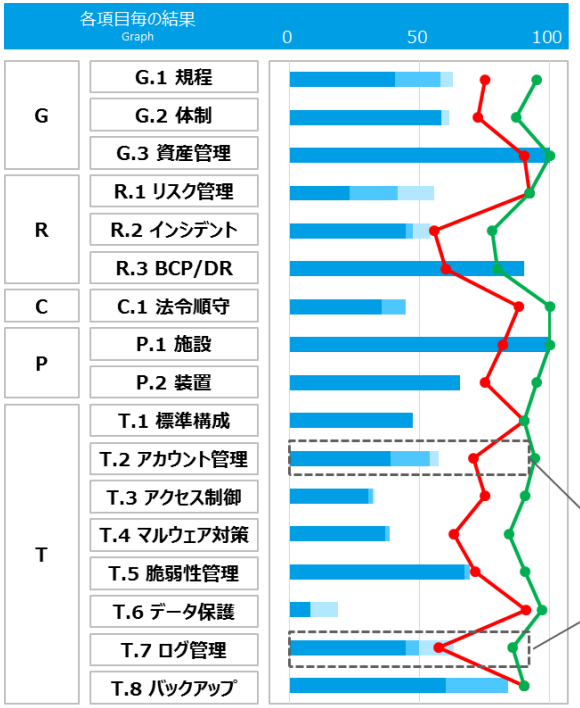
経営企画担当役員	企業経営に情報セキュリティのリスク管理を埋め込む責任

役　割	具体的事項
中期経営計画の策定	中期経営計画への情報セキュリティリスク対応の盛り込み
単年度予算の編成	予算の中に十分なセキュリティ対応予算が組み込まれているか確認
取締役会等の会議体事務局	定期的に情報セキュリティリスクについての議題を設定
グループ会社の管理	グループ会社の情報セキュリティガバナンス推進
組織構造の見直し・拠点再編	情報セキュリティ機能（コーポレート、事業部）の最適配置
組織風土・文化の改善・改革	情報セキュリティ文化の醸成
新規事業推進	新規事業における情報セキュリティリスクの見極めと対応 （提供製品・サービスの品質管理にセキュリティの観点を組み入れる組織の編成）
CSR・環境経営推進	CSR報告書の中に情報セキュリティ対応状況の説明盛り込み

経営層のリーダーシップ：具体的施策 ②正しいリスク認識（自社）

- 正しい判断（投資、コスト）を行うためには、正しいリスク認識が必要
  - 対象としてコーポレート（社内情報インフラ）、事業部門（製品・サービス）がある
- 情報セキュリティのリスクを可視化し、経営層の間で共有する
  - 「対策として行っていること」だけではなく、残リスクを可視化して管理する

リスクのスコアリングの例



■評価グラフ 凡例の説明

凡例	項目	説明
●—	基準スコア	セキュリティインシデントの発生リスクが低減されているレベル
●—	推奨スコア	事故が起きても対外的にある程度説明責任が果たせるレベル
■	対策済み得点	脅威に対して十分な対策がとれている、若しくは代替策で実施している
■	一部対策済み得点(高)	脅威に対する機能は実装されているが、一部有効になっていない
■	一部対策済み得点(低)	脅威に対する機能はあるが、設定が有効になっていない、若しくは対策を回避する手段が存在する

■グラフの見方

例１	全ての得点の合計値が基準スコアに達していない ⇒ セキュリティ確保のため基準スコアに達するまでの対策をする必要がある
例2	全ての得点の合計値が基準スコアには達しているが、推奨スコアには達していない ⇒ 基準はクリアしているため、必須対策が有効になっていない対策を中心に実施すれば良い

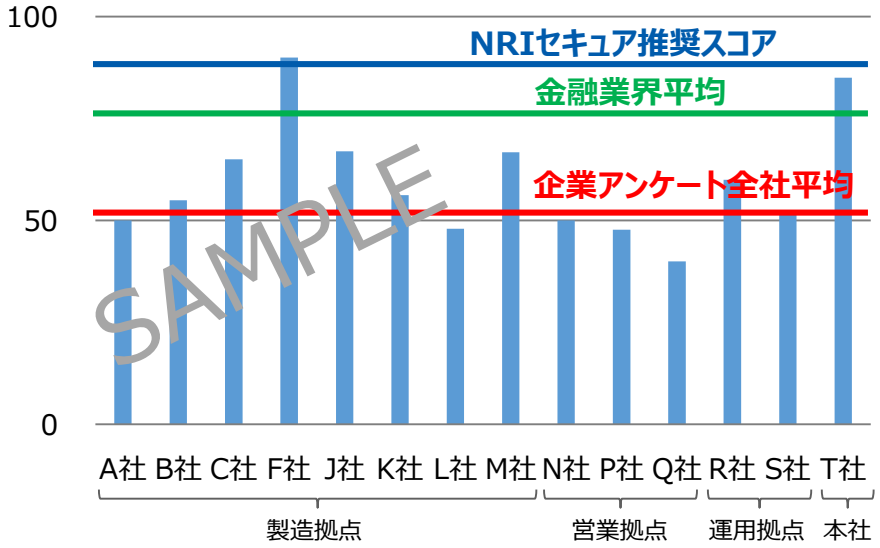
出所）NRIセキュアテクノロジーズ「セキュリティ対策状況可視化サービス」

経営層のリーダーシップ：具体的施策 ②正しいリスク認識（グループ全体）

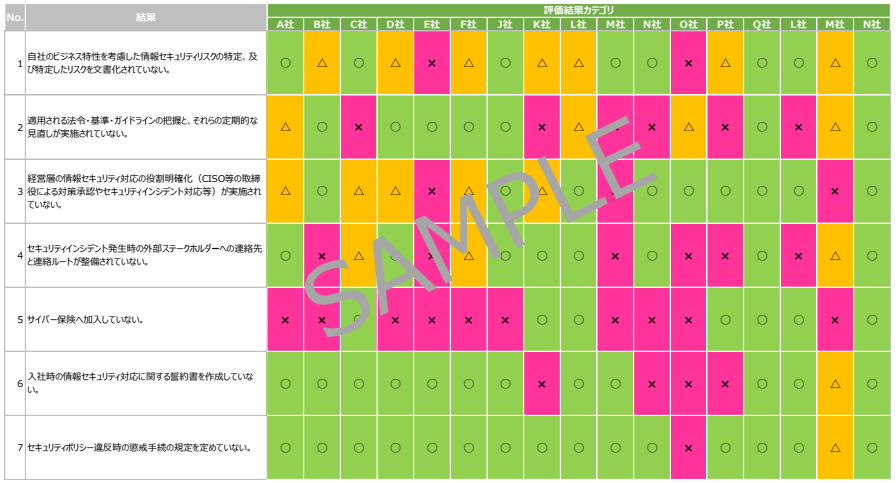
- グループ会社のセキュリティインシデントは、グループ全体の評判に繋がる
  - グループ全体のセキュリティを、持株会社や本社がグループ会社と一緒に管理する必要がある
- グループ会社のリスクを横並びで可視化し、グループ会社の経営層も含めて共有する

グループガバナンスのための可視化の例

対策状況スコア



対策状況ヒートマップ



出所）NRIセキュアテクノロジーズ 「セキュリティ対策状況可視化サービス」

専門人材の確保：具体的施策
人材育成の５ステップ

Step 1 必要な社内人員の決定

セキュリティ関連業務を洗い出し、内製化か社外委託かを選別

（次ページ参照）

Step 2 スキル棚卸

業務に必要なスキルの棚卸

システム・セキュリティ関連スキル
- セキュリティ要件の定義
- セキュアデザイン
- セキュアコーディング
- 脆弱性診断の結果の理解

基盤関連スキル
- ネットワーク・システム構築
- ネットワーク・システム運用

CSIRTメンバー
- インシデント対応能力
- フォレンジック能力
- サイバーインテリジェンス関連スキル

Step 3 フレームワーク化

キャリアパス、ローテーション等既存育成計画に組み入れ

フレームワーク・ツール
- キャリアパス
- 職務・ポジション
- 育成計画
- ローテーション

Step 4 研修プログラム選定

社内、社外の研修プログラムの選定

選定の6つのポイント
- 業務に適合した内容
- 体系立った内容
- 実践的な内容
- 復習可能な教材
- 定評、実績ある研修
- 評価・測定可能な研修

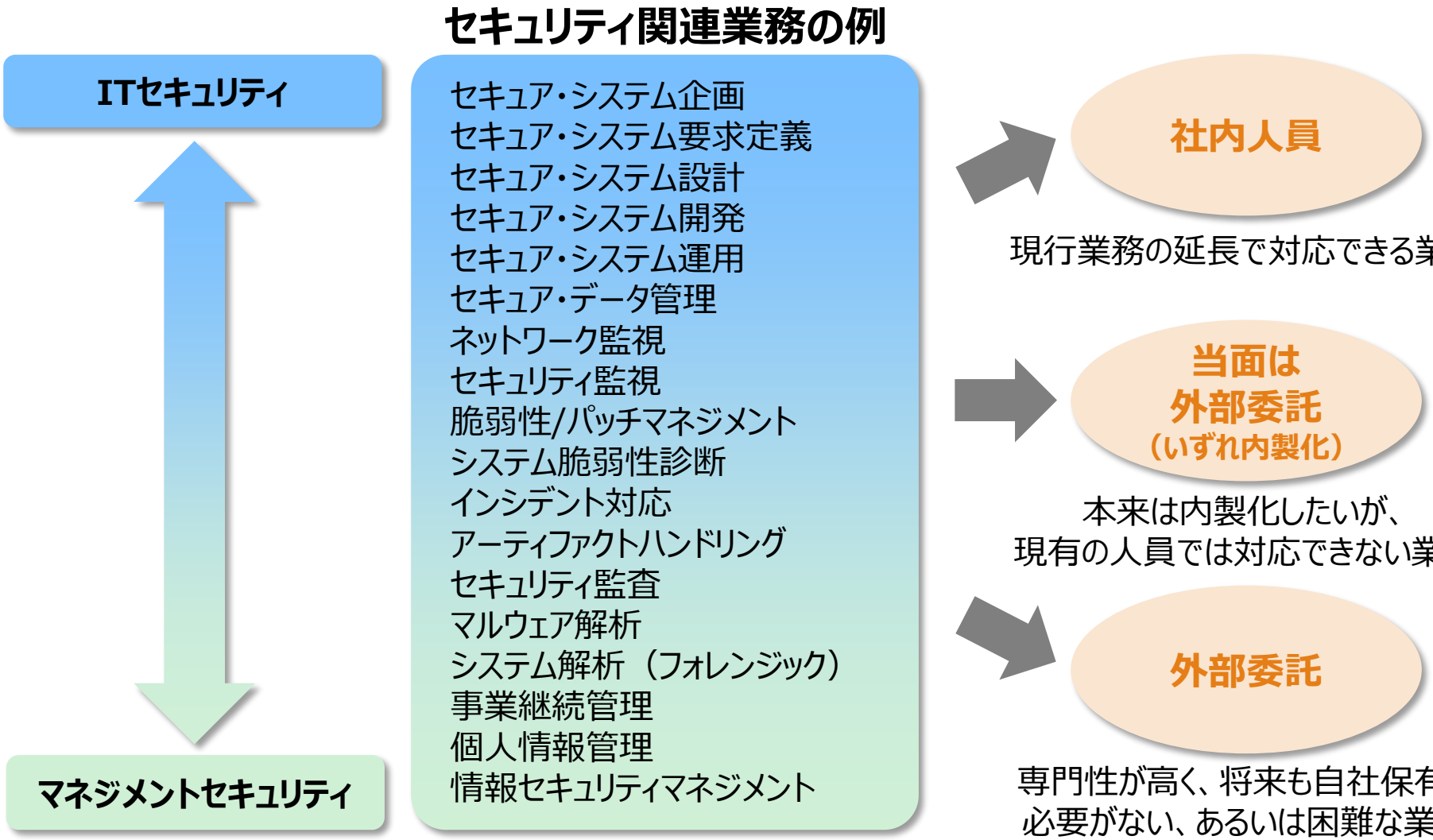
Step 5 スキルの可視化

推奨資格等スキルの可視化

国内資格
- 情報処理技術者試験
- 情報処理安全確保支援士
- 情報セキュリティ監査人

グローバル資格
- GIAC
- CISSP
- CISA、CISM

専門人材の確保：具体的施策
Step1　必要な社内人員の決定



専門人材の確保：Step5　スキルの可視化
世界のCISSP人数から見た日本の現状

グローバルセキュリティ３大資格
(ISC)2：CISSP
ISACA：CISA
SANS：GIAC

世界のCISSP	117,765人
日本	1,815人
米国	76,858人
韓国	2,745人
香港	1,501人
シンガポール	1,629人
オーストラリア	2,122人

2017年7月17日現在

■ 米国に比べ明らかに少ない　1/65

- 米国政府は積極的にセキュリティ民間資格取得を政府職員に必須・推奨として採用し教育受講費用、資格取得費用を予算化している
- 約30,000人の政府機関職員が取得
- NIST/NICEで人材育成のフレームワークを明確化

■ 日本においての問題点

- 経営者のセキュリティ教育に対する理解不足
- 政府機関職員は予算不足、定期ローテーションにより資格取得までに至らない
（除く警察庁・防衛省）
- セキュリティ人材のキャリアパス不足

出所(ISC2)Japan
CISSPは(ISC)2が認証する情報セキュリティ専門家の資格です。
https://www.isc2.org/japan/cissp_about.html

1．最近のサイバーセキュリティ事件簿

2．昨今のサイバーセキュリティの脅威状況

3．企業のセキュリティ対応状況と課題

4．求められる企業の対応策

5．まとめ

まとめ

- **サイバーセキュリティのリスクは、企業経営を揺るがしかねない問題となっている**
  - 「今」の状況に対応するのではなく、将来を見据えた対策が必要
- **ITが、コーポレートITからビジネスITに比重を移す中、事業部門のセキュリティ対応が重要になる**
  - 特にIoT製品やネットビジネスでは、初期の段階からセキュリティの考慮が必要
- **経営層が、サイバーセキュリティについての自身の責任とリスクを認識することが肝要である**
  - セキュリティ専門人材は５ステップで計画的に確保 CISSP取得も忘れずに！

NRIセキュアのご紹介：会社概要

野村総合研究所（NRI）グループにおける情報セキュリティ専門の中核企業

会社名	NRIセキュアテクノロジーズ株式会社　（略称：NRIセキュア）
会社所在地	本社　東京都千代田区大手町1-7-2　東京サンケイビル 横浜テクニカルセンター　神奈川県横浜市保土ヶ谷区神戸町134　NRIタワー 北米支社　26 Executive Park Suite 150, Irvine, California, USA
設立年月日	2000年8月1日　（NRI社内ベンチャー第1号として誕生）
資本金	4.5億円
代表取締役社長	小田島　潤
社員数	連結：395名　単体：340名
グループ会社	株式会社ユービーセキュア（東京都港区）
資格取得者数	● 高度情報処理技術者 ： のべ458名 ● GIAC (Global Information Assurance Certification) ： のべ156名 ● CISA (Certified Information System Auditor) ： 77名 ● CISM (Certified Information Security Manager) ： 40名 ● CISSP (Certified Information Systems Security Professionals) ： 37名
サービス提供実績	● 官公庁、金融、流通、製造、製薬、通信、マスコミ等500社以上に運用サービスを提供 ● 一次的なスポットサービスを含めると2000社以上に各種サービスを提供
認証取得	ISO/IEC 27001認証取得

IS 75215 / ISO 27001:2013

（2017年8月1日現在）

NRIセキュアのご紹介：事業概要

３つの事業を柱に、情報セキュリティのあらゆる課題を「ワンストップ」で解決

高度な専門性による課題解決支援

- 各種認証取得支援(PCI DSS など)
- セキュリティ対策状況可視化サービス
- CIO、CISO支援
- CSIRT構築支援
- セキュリティポリシー策定支援 ほか

CONSULTING
コンサルティング
事業

攻めと守りのサイバー攻撃対策

- セキュリティ診断
- 標的型メール攻撃シミュレーション
- Webサイト探索棚卸し
- デバイスセキュリティ診断
- PCI DSSペネトレーションテスト ほか
- マネージドセキュリティサービス
  - ・セキュリティ機器運用監視
- セキュリティログ監視サービス
  - ・相関分析監視
  - ・インシデントレスポンス　ほか

CYBER SECURITY
サイバーセキュリティ
事業

自社開発による柔軟なニーズ対応

- IDセキュリティ
- ファイルセキュリティ
- オフィスITセキュリティ

SOLUTION
ソリューション
事業

SecureCube Access Check
SecureCube PC Check クラウド
クリプト便 POSTUB Contents Expert
SecuSURF InterCollage Uni-iD
CACHATTO Yarai

サイバーセキュリティ強化には
プロフェッショナルが必要だ！

1,834人に増加

2002年日本のCISSPは15人

NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ
NRI SecureTechnologies

(ISC)² Secure Events

SECURETOKYO 2017