D2-2 新技術に対応するセキュリティ運用とは ～変わりゆく技術の中でぼくらは～ 第2部

2019年11月27日

日本セキュリティオペレーション事業者協議会
新技術とオペレーションのプロジェクト
セキュリティオペレーション連携WG(WG6)

司会進行

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - CISSP、情報処理安全確保支援士

講演者

- ももいやすなり
  株式会社インターネットイニシアティブ
  セキュリティ本部 セキュリティ情報統括室 リードエンジニア
  - サービス開発、システム開発、研究開発、ネタ披露、宴会調整
  - IIJ-SECT (CSIRT)、関連団体 (ISOG-J, ICT-ISAC, NCA など)、技術コミュニティ
  - 食べ物、ヘヴィメタル、ねこ



- SOC 見学やってます
- セキュリティ情報発信
  - wizSafe Security Signal
  - IIR, IIJ Security Diary, IIJ Engineers blog
    - IIR Vol.40 の記事を書きました

IIJ-SECT
IIJ Group Security Coordination Team
wizSafe
安全をあたりまえに

講演者

- **亀田　勇歩**

SCSK株式会社　セキュリティアナリスト

- Web/PF脆弱性診断
- SOC監視業務
- インシデントレスポンス

ISOG-J / OWASP / 他

- **ZAP**エヴァンジェリスト
- **脆弱性診断士**の活動
- 東京電機大学 国際化サイバーセキュリティ学特別コース(CySec) 外部講師

趣味

- 2019年のラスベガスで開催された**DEFCON OSINT CTFで5位**入賞してきました
- 2019年の11/2に国内で4回目の**Open xINT CTFを開催**してきました

講演者

・ 田中　朗（たなか　あきら）　(ISOG-J フェロー)
  - コインチェック でCISOというセキュリティ責任者やってます

1980年代、1990年代　メーカの研究所でソフトウェアの研究・開発
　　プログラミング色々、JUNETからWIDEの変化をすぐそばで
1998年　セキュリティ事業立上げ、顧客向けのMSS(Managed Security Service)提供
2011年　ISOG-J活動に参加
2015年　社内CSIRT設立、その後CSIRTリーダー
2016年　JNSA　CISO支援WG
2018年　ユーザ企業に転職

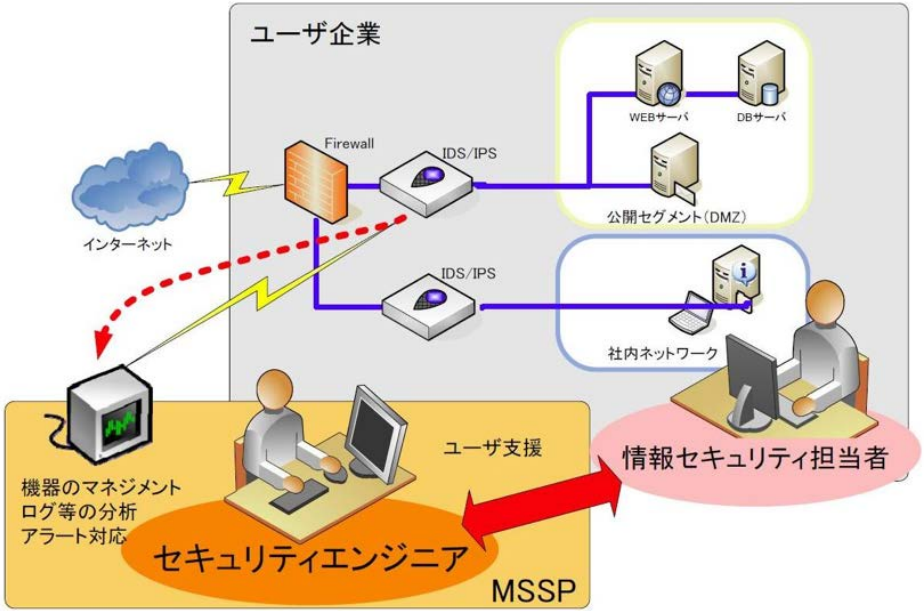
後半の目次

- 今の環境から考える
- これからの環境を考える
- 実際に運用している現場の例
- まとめ

- 今の環境から考える
- これからの環境を考える
- 実際に運用している現場の例
- まとめ

いままで考えられてきた環境

- ネットワーク境界防御で、IDS/IPS, FWでDMZと社内を守ればいい



マネージドセキュリティサービス選定ガイド(2009, ISOG-J)
https://isog-j.org/output/2010/MSS-Guideline_v100.pdf

境界防御で守ってきたサーバー群

公開向け

- Webサーバー
- データベースサーバー
- DNSサーバー
- メールサーバー

社内OA向け

- 人事給与管理
- 経理処理
- 顧客管理
- 資産管理
- グループウェア
- アンチウイルスソフト管理
- ファイルサーバー
- Active Directory
- プロキシ

いま起き始めている変化

- クラウドサービスを利用することで、だんだん社内にサーバーがなくなり始めている

クラウド上で構築・クラウドサービスを購入

- Webサーバー
- データベースサーバー
- DNSサーバー
- メールサーバー

- 人事給与管理
- 経理処理
- 顧客管理
- 資産管理
- グループウェア
- アンチウイルスソフト管理

社内で管理

- ファイルサーバー
- Active Directory
- プロキシ

これから起こるであろう変化

- ID管理もクラウドへ移り、ファイルもクラウド上で権限を管理され、社内のサーバーがなくなる

企業や組織の活動のほとんどはクラウド上で展開

- Webサーバー
- データベースサーバー
- DNSサーバー
- メールサーバー

- 人事給与管理
- 経理処理
- 顧客管理
- 資産管理
- グループウェア
- アンチウイルスソフト管理
- ファイルサーバー
- Active Directory

社内で(監視のために)管理

- プロキシ

増える監視対象

基幹業務や製造などのこれまでつながっていなかったもの

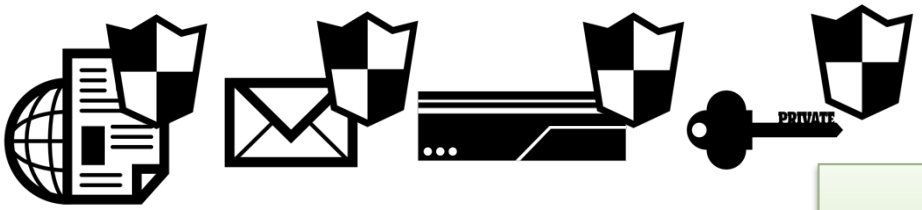
デジタルサイネージやセンサー、遠隔カメラやIoTなどネットワークにつながっているもの

（これまでの）DMZやOAネットワーク

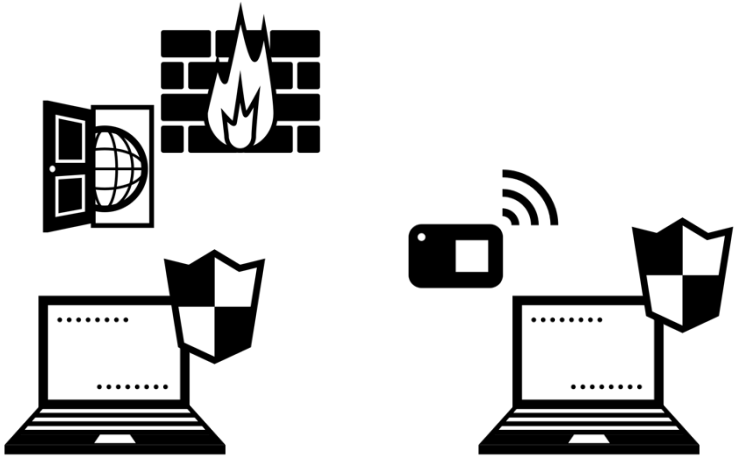
「働き方改革」で社員が在宅勤務やリモートワークするために持ち出しをする

スマートフォンやタブレットを活用したパソコンを使わない業務

変化する監視運用



各種クラウドサービス
からのログ



- 取れる情報は同じ？
- 関連付けはできるのか？
- どんな量になるのか？

社内の機器からのログ

見えにくくなってきたもの

- 通信のhttps化によるもの
  - クラウドサービス
  - 公開Webサービス

- シャドーITが発生しやすい環境
  - スマートフォンやタブレットが普及
  - 個人が使いやすい環境で、つい作業ができてしまう

- 今の環境から考える
- これからを考える
- 実際に運用している現場の例
- まとめ

今出てきているキーワード

- クラウドサービス
- CASB(Cloud Access Security Broker)
- ゼロトラスト
- EDR(Endpoint Detection and Response),
  MDR(Managed Detection and Response)

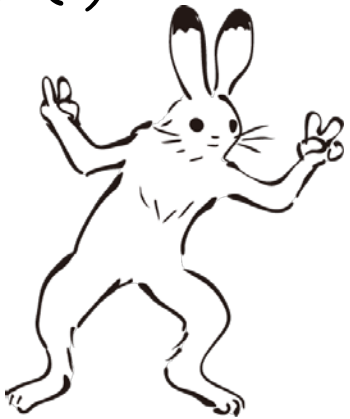
これらの示す全体的な方向感は？

よくある話

「これだけ入れておけばあとは大丈夫！」

（しばらくして）

「次は***です！」



今は次がなにか誰もわからない

次がない？

今は(みんなに当てはまる)次が
なにか誰もわからない

その組織・会社に合ったものを考える
必要がある

セキュリティだけで考えない

- 経営課題はなに？
  - 法律や要請でやらないといけないことはなに？
- 社員がITで困っていることはなに？
- 社内システムの管理者、運用者が困っていることは何？

あなたの対策はどこから？　例：守りたいもの

ゼロにはならないが
許容範囲はある

守りたいモノの
想定される被害 ＝ 価値 x 影響度 x 頻度

許容範囲を超えないように
影響度と頻度を下げることが求められる

InternetWeek2018 第2部 D2-2 資料より
https://www.nic.ad.jp/ja/materials/iw/2018/proceedings/d2/

あなたの対策はどこから？　例：守りたいもの

・ 守りたいものの価値を考える

なにがあるか

- それは何？
- 誰が管理者？
- どこにあるもの？

どんな脅威や
弱点があるか？

どんな影響があるか？

- 財務
- 評判（レピュテーション）
- 業界優位性
- ネットワーク
- 人
- モチベーション

などなど

あなたの対策はどこから？　例：優先度

高

低

(これまでの）DMZやOAネットワーク

「働き方改革」で社員が在宅勤務やリモートワークするために持ち出しをする

スマートフォンやタブレットを活用したパソコンを使わない業務

基幹業務や製造などのこれまでつながっていなかったもの

デジタルサイネージやセンサー、遠隔カメラやIoTなどネットワークにつながっているもの

いままでの取り組みは意味がない？

- どんな対策がどの程度効果があったのかを継続的に測定しておく
- これからやるべき対策も見据える
- なんでも新しければ良い、というわけではない。バランスの取り方を考える。

その組織・会社の「新陳代謝」に合わせる

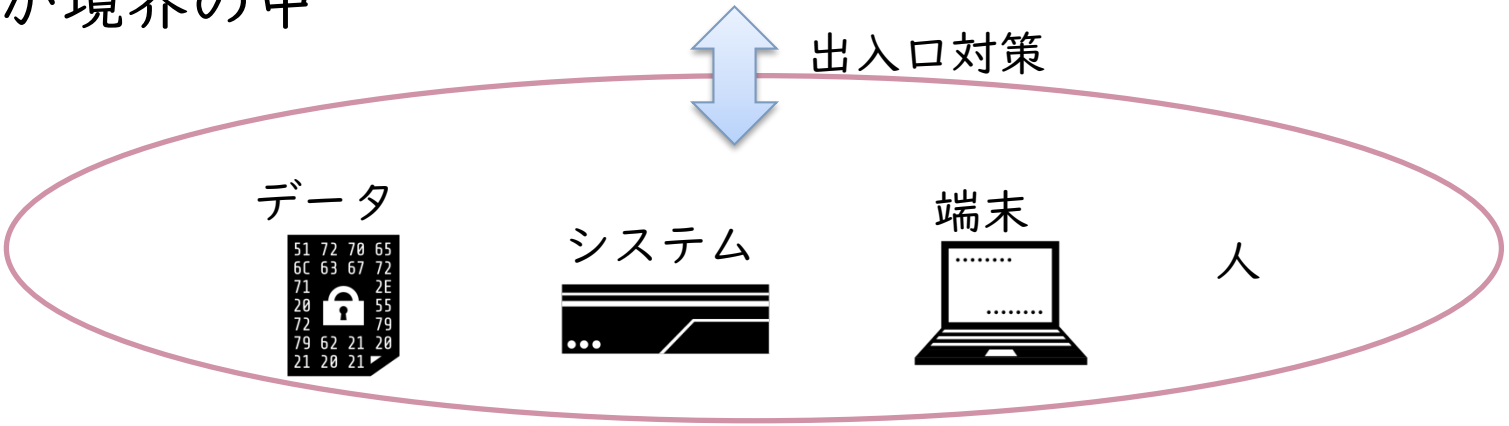
- 今の環境から考える
- これからの環境を考える
- 実際に運用している現場の例
- まとめ

IT環境の変化

- クラウドサービス利用
  守るべきデータのありかが変わってきている
- 働き方改革
  社外からのアクセスも普通に
- 2要素認証
  何を信頼するか（パスワードに頼らない）

これまでのセキュリティ境界

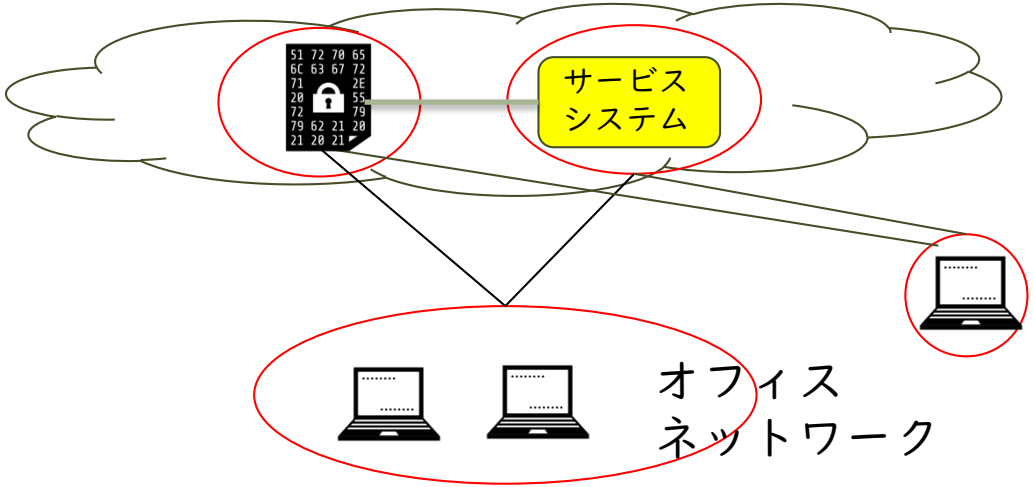
- 重要情報（データ）、システム、端末、人
  全てが境界の中



境界防御が効果的　（ネットワーク中心の出入口対策）

現在のセキュリティ境界はどこに

・ クラウドベース＋オフィスネットワーク＋モバイル



境界がぼやけている　（ネットワークだけでないセキュリティ対策）

重要情報にアクセスするには

信頼できるもの積み重ね

→ 実行できる操作（閲覧、編集、ダウンロード）

- 従来
  - 社内ネットワーク＋アカウント（ID/パスワード）
- 現在
  - 端末（会社で管理されている/いない）
  - ユーザ（２要素認証あり/なし）
  - ネットワーク（社内/自宅/公衆）
  - サービスシステム

  など

ネットワーク防御

- 従来は境界防御が前提の多層防御
  - DMZを作ること
  - ファイアウォールを２段構成
  - 次世代FW ＋　Proxy
  - Anti Virus対策

  など

  ネットワークベースの考え方が中心。

※多層防御というには十分でないものもあります

多層防御の今

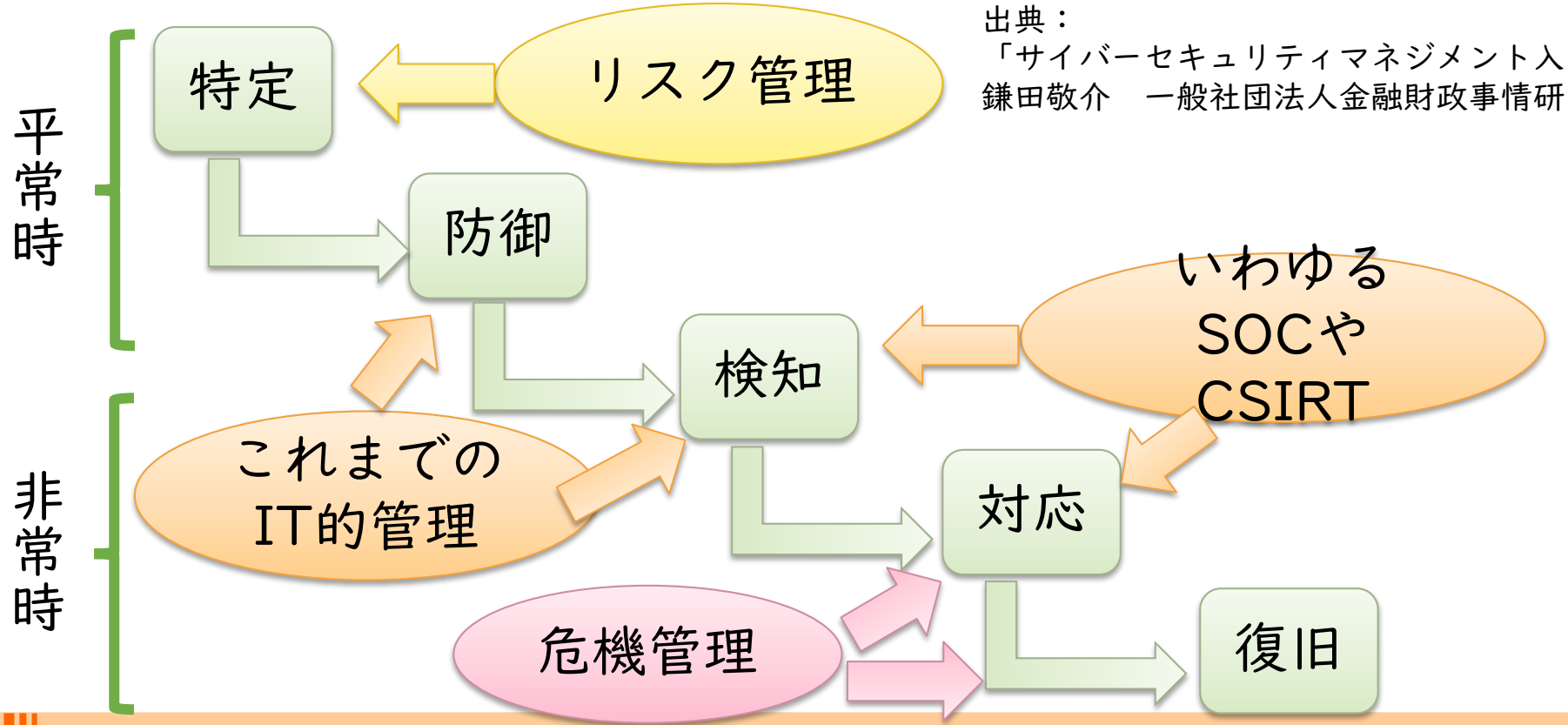
	対策カテゴリ	主な対策
1	ネットワーク	次世代FW、Proxy接続、セグメント分割
2	Mail・Web接続制御	スパムフィルター、URLフィルタリング、WAF
3	端末セキュリティ	AV/EDR、パッチ適用管理、ソフトウェア管理、CASB
4	サーバ	パッチ管理、接続管理、要塞化
5	ID管理	SSO、2要素認証、最小権限の原則（特権管理）
6	クラウド	クラウドセキュリティ。。。
7	アプリケーション	セキュリティバイデザイン、脆弱性診断
8	監視	SIEMでのログ集約・監視、SOC(24x7)
9	インシデントレスポンス	CSIRT体制、緊急事態対策
10	周知・教育・訓練	標的型攻撃対処訓練、セキュリティ教育、注意喚起
11	物理セキュリティ	入退室管理、ID棚卸、ゾーニング

対策（技術的）

- セキュリティ対策マップの作成
  - 縦軸：多層防御の要素
  - 横軸：特定、防御、検知、対応、復旧
    （サイバーセキュリティフレームワーク）

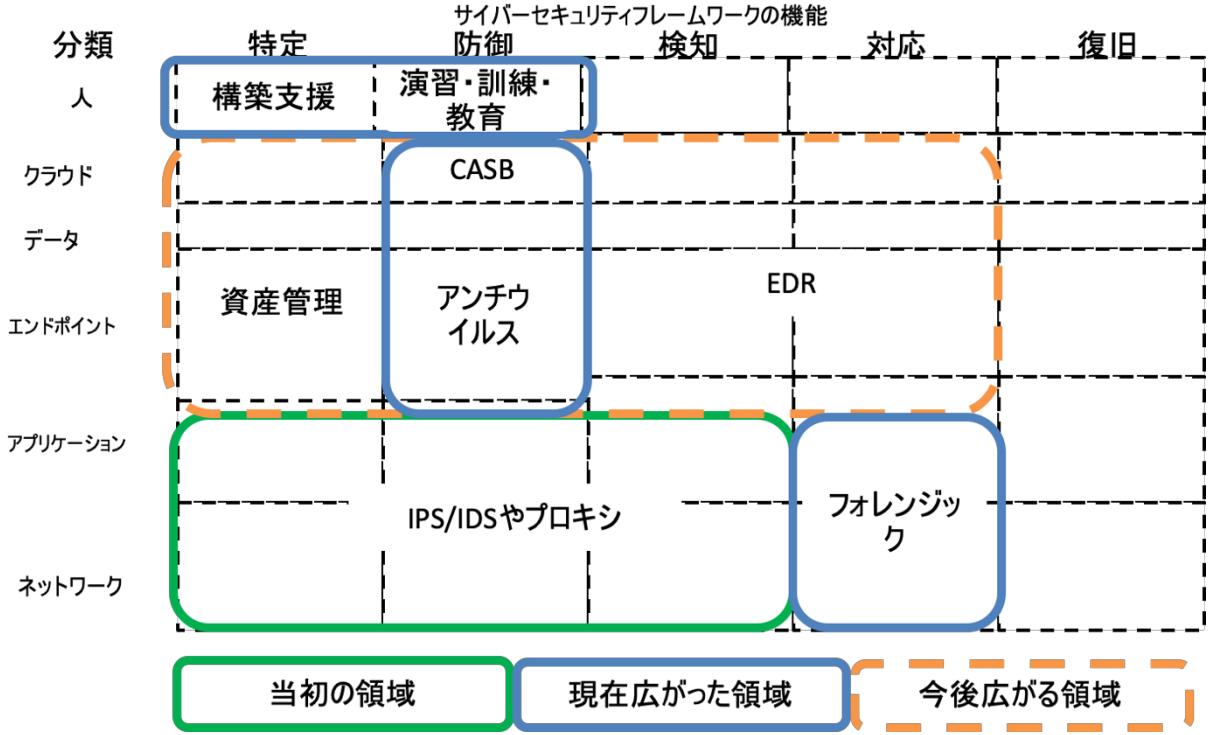
自社の対策カバー状況を把握
今後強化すべきエリアを検討
強化策をセキュリティプログラムとして策定

サイバーセキュリティフレームワーク



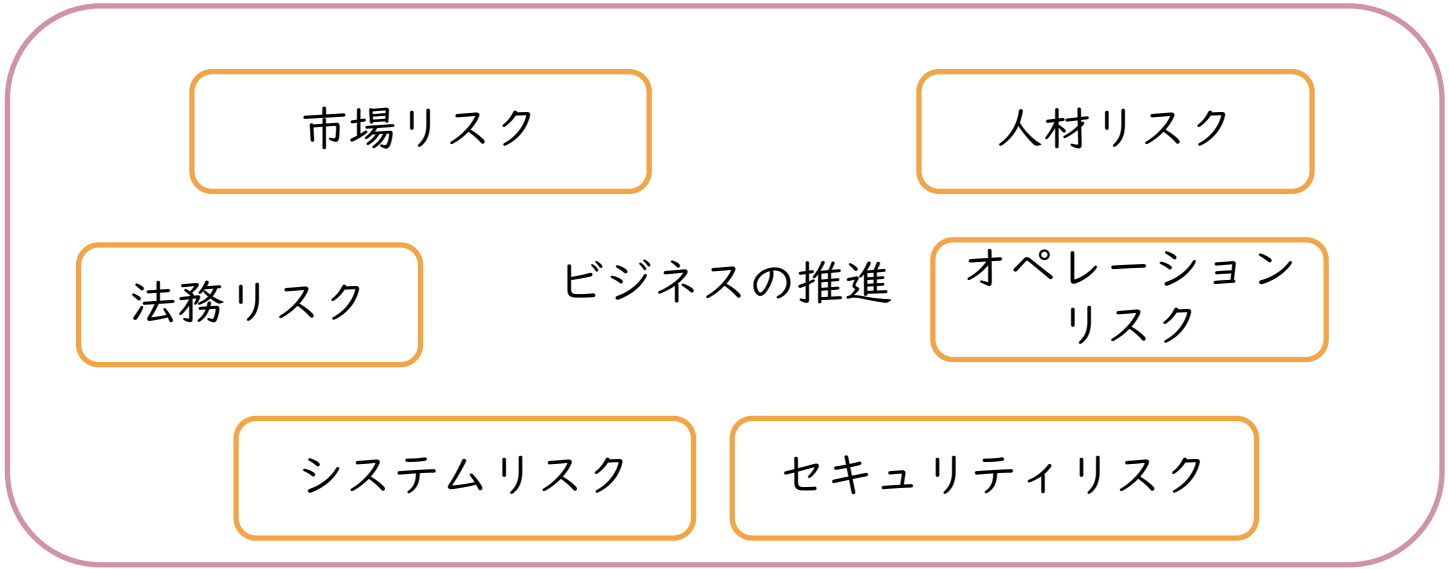
出典：
「サイバーセキュリティマネジメント入門」
鎌田敬介　一般社団法人金融財政事情研究所

セキュリティマップの例



対策（マネージメント）

- ビジネスとセキュリティの関係
  - 多数あるリスクのひとつ



もう一つの視点

- コントロールベースのセキュリティ（従来）
  - 多くのセキュリティ製品を導入
  - 機能を十分使いこなせていない。
  - 運用が大変に。（コストがかかる）

攻撃を防ぎきれない

- リスクベース アプローチ
  - 業種、業態、ITシステムの違い
  - 守るべきものの特定と優先すべき項目の判断
  - 脅威に合わせたダイナミックなセキュリティ対策

まずやるべきこと

- セキュリティの見える化
  - 経営視点でのセキュリティ対策の有効性評価
  - 自社のセキュリティ状況
  - 自社のビジネス環境と脅威状況
  - セキュリティプログラムの進捗状況
  - CISOダッシュボード

CISO ダッシュボード：業務執行としてのセキュリティ

CSIRTではなく、業務執行としてのセキュリティ

Governance	CISOが果経営会議で報告すべきたすべきガバナンス ＝業務執行に関わる事項
Risk	Risk = ≒ *f(Attack condition, Protect condition, suspicious activity, Indirect activity)* Security and Risk condition

Attack

1. Attack condition
攻撃検出状況に関するKPI

AV/IDS等による検出
セキュリティ製品のアラート等
攻撃などに関する情報

2. Protect condition
対策状況に関するKPI

ウィルス対策, システムバージョン、パッチ、コンフィグレーション等、セキュリティ対策として実施すべき項目の適用率等
脆弱性情報

3. Suspicious activity
侵入が疑われる状況のKPI

SIEM/ATA/WDATP等による検出や、その他の侵入が疑われるもの
内部犯行を含んだ、疑わしいイベント

4. Indirect activity
人事的、物理的等、直接ITとは関係しない状況のKPI

退職者、PCやデバイスの紛失・盗難
外部からのインテリジェンス

経営会議で何を報告すべきなのか
どのように決裁を仰ぐべきなのか

セキュリティ報告書（XX年度XX月　経営会議向け）

			備考
Attack condition	技術的	2	弊社を狙ったと思われる攻撃メールが、XX月XX日-XX月XX日にかけて、SPAMフィルターとAVで検知された。総数は、23件で、開発の特定部門に集中している。現段階では、全てブロックできたと判断しているが、警戒を続ける必要がある
	概況的	1	海外で大規模なインシデントが報道されているが、報道を見る限り対策済みの手法と判断される（別紙１）
Protect condition	技術的	2	先月から配布されたPCのキッティングに問題のある事が判明。既に回収をしているが、まだ最終確認がとれていない。XX月XX日までに狩猟予定。一部業務に影響が出るが、協力をお願いしたい。
	概況的	1	ネットワークデバイスへの深刻な脆弱性*xxxが報告されているが、弊社では使用していないことが確認されている（参考資料2）
Suspicious activity	技術的	3	外向けの通信に、不審な接続先との通信が記録されている。現在詳細を分析中だが、大規模な調査が必要となる可能性がある。上記攻撃メールとの関連も疑われるため、早急な調査が必要。 分析を早め、より効果的な防御を行うためには、より精度の高いブラックリストの入手が効果的と考えている(**別紙2：決済申請**)
	概況的	2	データベース保守を担当するベンダーが懲戒解雇となっている。プロシージャに沿ってアカウントなどの停止を実施した。
Indirect activity	技術的	2	1台のPCと、2台の会社貸与スマホが紛失。リモートワイプで対策済み
	概況的	1	経済産業省から、「サイバーセキュリティ経営ガイドライン」が公表され、注目されている。IT/セキュリティ部門では展開済み。 当ミーティングでコピーを配布します

成功のポイント

- IT部門、セキュリティ部門だけでないセキュリティ
  ＝ビジネス部門、経営層を巻き込んだセキュリティ対策
- ０、１でないセキュリティ
  ＝禁止を前提としないセキュリティ、
- 運用を前提としたセキュリティ
  ＝機器、ソフトウェアを入れておしまいではない
- 自社で判断できる体制
  ＝発生した事象の影響判断

ビジネス＆セキュリティがわかる人（自社）＋セキュリティ専門家（アウトソース）

現場の事例

・ …については、当日投影にてご紹介します。

- 今の環境から考える
- これからの環境を考える
- 実際に運用している現場の例
- まとめ

まとめ

- やり続けること、変えること、新しくやることを定期的に考え続ける
  - そのためにも、今の自分を知る。これからを見据える。
  - なんでも新しくすればいい、というわけではない

- 「新陳代謝」できる体質に
  - 「会社の寿命は30年」(「会社の寿命」日経ビジネス、1983年)、長続きする会社は事業の新陳代謝を続けていた。
  - ITやセキュリティも同様に適切なタイミングで適切な導入を

(参考：アイコン、漫画素材)
http://www.security-design.jp/
http:// www.chojugiga.com/