コラム１

セキュリティ評価のススメ
『彼を知り己を知れば百戦殆からず』

共通対策評価フレームワーク分科会

初版　2022年6月13日

Cyber Security Initiative for Japan

10大脅威の上位はサイバー攻撃

[出典]：IPA「情報セキュリティ10大脅威 2022：組織編」
を元にNRIセキュアが作成

2022の注目ポイント

ランサムウェア被害が2年連続の1位

日本企業の被害報道が頻発

サプライチェーン攻撃がTop3に

2019　4位（NEW）
2020　4位
2021　4位
2022　3位

脆弱性を狙う攻撃が6位、7位

2021年12月に世間をにぎわせた
Java用のログ出力ライブラリ
「Apache Log4j」の脆弱性などが該当

日本企業における課題

NRI Secure Insight 2021
（企業における情報セキュリティ実態調査より）

回答数 2,653社（日本：1, 616社、アメリカ：511社、オーストラリア：526社）

セキュリティ人材の不足

- ✓ 9割強の企業で、慢性的な人材不足

セキュリティ予算の不足

- ✓ 6割強の企業で、 IT予算に占める
  セキュリティ予算の割合は10%未満

リーダー・理解者の不足

- ✓ CISOの設置率は、46.1%
  （CISO＝最高情報セキュリティ責任者）

インシデント起因での対策実施

- ✓ セキュリティ対策を実施するきっかけや理由について、日本と米・豪では異なる結果
  - ✓ 日本では、インシデント起因が上位を占める
  - ✓ 米・豪では、経営層のトップダウン指示が5割超の割合で1位

直近1年に実施したセキュリティ対策の実施のきっかけや理由

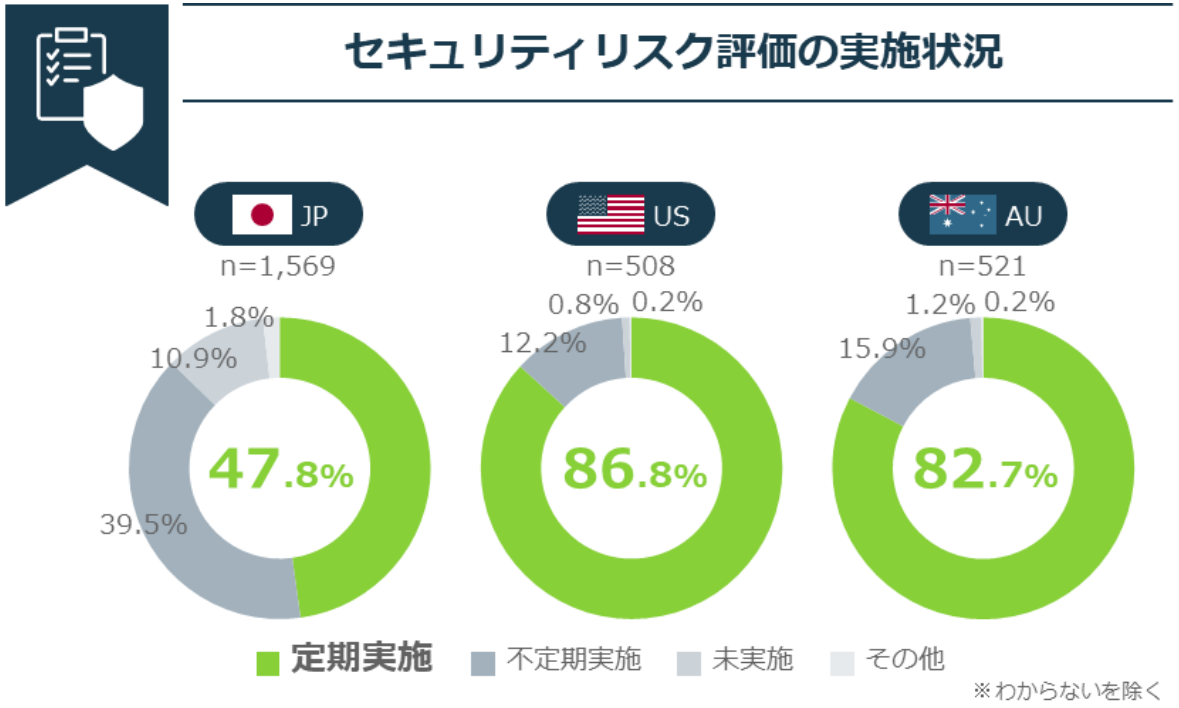
	JP n=1,616	US n=511	AU n=526
1位	27.6% 他社での セキュリティインシデント事例	54.8% 経営層の トップダウン指示	52.7% 経営層の トップダウン指示
2位	25.6% 自社での セキュリティインシデント	25.0% 他社での セキュリティインシデント事例	25.3% 他社での セキュリティインシデント事例
3位	21.6% 経営層の トップダウン指示	24.5% 株主や取引先からの要請	22.1% 株主や取引先からの要請

監督省庁からのセキュリティ対策強化の要請 （自治体からの要請を含む）（具体的な要請内容を記載）／関連法規の改定（具体的な関連法規を記載）／持株会社や親会社からの要請／競合他社の実施状況との比較／外部監査・第三者評価の結果／内部監査・内部有識者からの指摘／COVID-19に伴うテレワーク対応／DX化推進に伴う対応／その他（具体的に記載）／わからない

[出典] NRI Secure Insight 2021（企業における情報セキュリティ実態調査）より

リスク評価の定期実施は半数以下

- ✓ セキュリティリスク評価の実施状況について、日本と米・豪では異なる結果
  - ✓ 日本では、定期実施の割合が半数以下に留まる
  - ✓ 米・豪では、定期実施の割合が8割強を占める



[出典] NRI Secure Insight 2021（企業における情報セキュリティ実態調査）より

経産省からの注意喚起（2022/2/23）

令和４年２月２３日
経済産業省

昨今の情勢を踏まえたサイバーセキュリティ対策の強化について
（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案の潜在的なリスクは高まっていると考えられます。

各企業・団体においては、経営者のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

不審な動きを把握した場合は、早期対処のために速やかに経済産業省やセキュリティ関係機関に御相談ください。

[出典]：経産省 昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）
https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

3つの注意喚起

１．リスク低減のための措置

○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○IoT 機器を含む情報資産の保有状況を把握する。特にVPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知

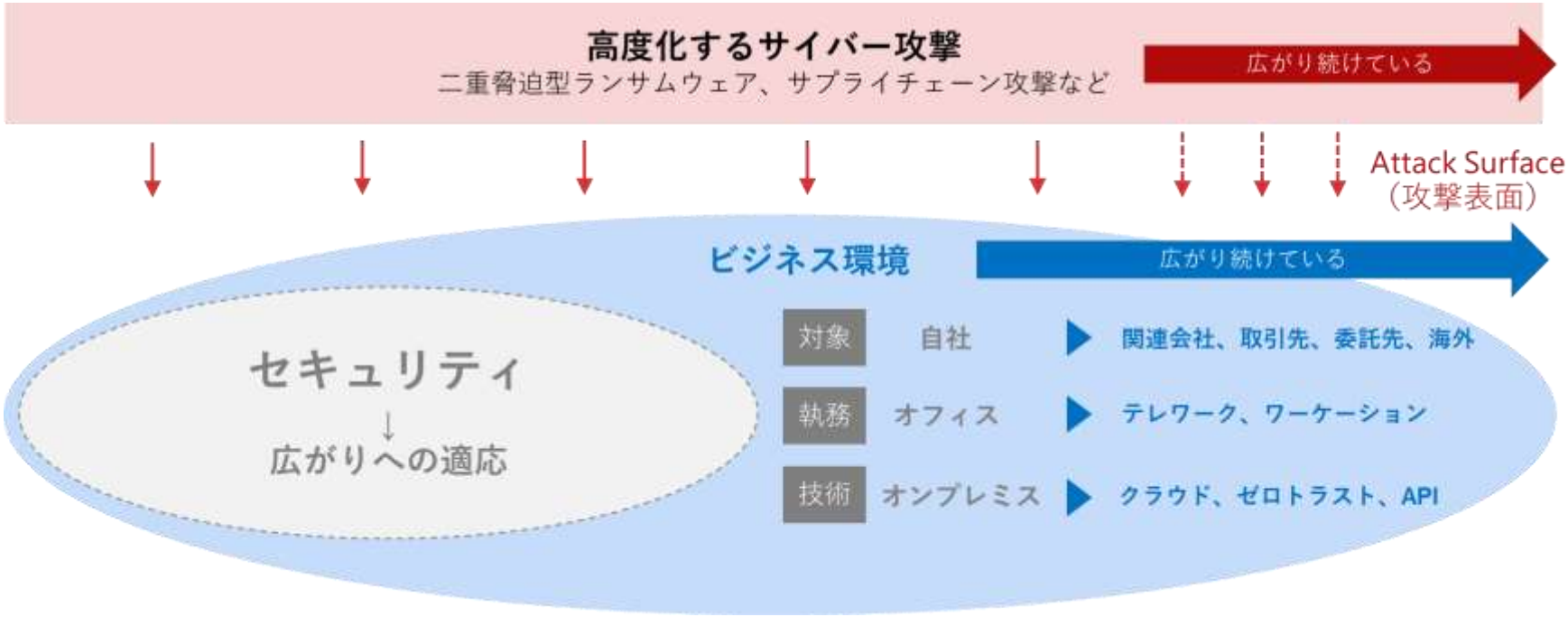
○サーバ等における各種ログを確認する。
○通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復

○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

攻撃表面の広がりという背景

- ✓ COVID-19以降、テレワークの普及やクラウド進展も追い風となり、Attack Surface（アタック・サーフェス）というサイバーセキュリティ用語の注目が高まっています。
- ✓ 直訳すると、攻撃表面（何らかのサイバー攻撃の対象となり得る領域）であり、攻撃表面の急速な広がりに、セキュリティ対策を適応させることが難しい現状と言えます。



[出典]：「企業における情報セキュリティ実態調査 2021」の結果を元にNRIセキュアが作成

ここまでのまとめ

IPA10大脅威の上位は、いずれもサイバー攻撃

ランサムウェア、サプライチェーン攻撃はクラウドでも発生

リアクティブになりがちな日本企業のセキュリティ対策

セキュリティ担当者を悩ませる3つの不足（人材、予算、理解者）

攻撃表面（Attack Surface）の把握と対策が急務

その背景には、クラウドやテレワークの進展がある

CSI/Jからの提言

『彼を知り己を知れば百戦殆からず』

彼　敵＝サイバー攻撃など

己　自社のセキュリティ対策

いますぐにやるべきこと

簡易なセキュリティ人間ドック

でも、どうやって？？？

CSIJが簡易なクラウド評価の枠組みを提供

共通対策評価フレームワークとは・・・

企業が安全にITの利活用やDX推進を進める中で、今現在のシステム利用状況や管理状況を見える化し、課題を浮かび上がらせることで、あるべき姿とのフィットギャップを示し、安全な運用を継続し続けるための指標となることを目的に、セキュリティ企業の知見を集めた共通評価フレームワークとして公開します。

- クラウド環境を利用しようと検討中の企業
- クラウドを利用しているが、安全性に不安のある企業
  - クラウドセキュリティのチェックを行う部署・担当の方
  - クラウド利用を検討・推進している部署・担当の方
  - クラウドサービスの企画、推進を行う方
  - 情報システム部門のリーダー、担当者　など

[出典]：「共通対策評価フレームワーク分科会」サイバーセキュリティイニシアティブジャパン
https://www.csi-japan.org/evaluation

簡易セキュリティ評価を体験ください

共通評価フレームワーククラウド版を見てみる
⇒評価分科会活動ページへ

簡易クラウド評価を始めてみる（無料）
⇒発起3社にご相談ください

・株式会社ラック
・NRIセキュアテクノロジーズ株式会社
・グローバルセキュリティエキスパート株式会社

CSIJ

Cyber Security Initiative for Japan