CRS Center for Rule-making Strategies

世界で起きているサイバー空間における ルール形成の最新動向と日本への影響

2018年 9月 14日

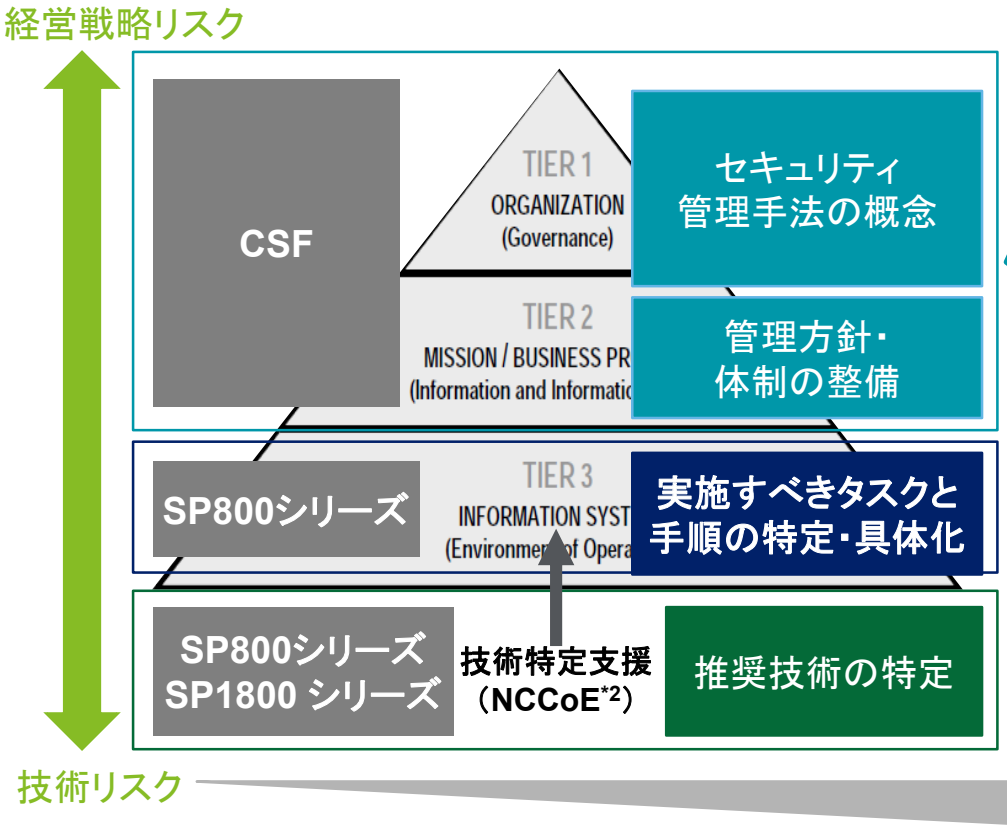
多摩大学大学院教授
ルール形成戦略研究所所長
國分俊史

TAMA UNIVERSITY 多摩大学

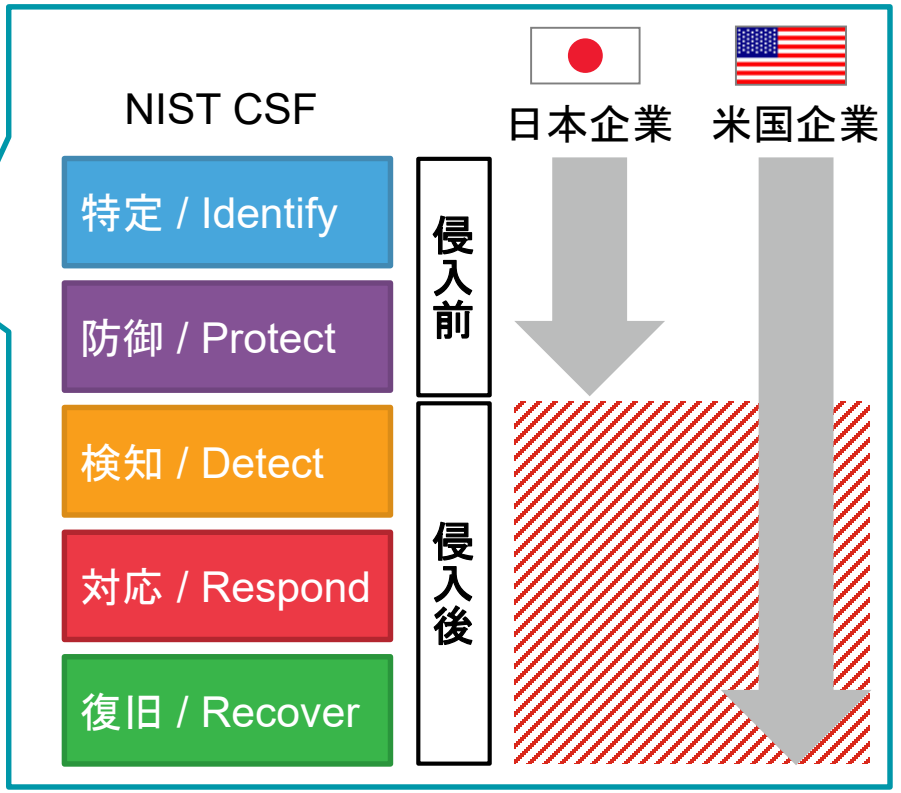
1. 事実上の国際標準となりつつある NISTフレームワークとは

NISTはサイバーセキュリティ基準のミニマムスタンダードとして、組織レベルから業務プロセス、情報システムといった技術レベルまでカバーするガイドライン群を作成

NISTの定義するサイバーセキュリティ対策のアプローチ



NIST CSF (Cybersecurity Framework)



NIST文書は法的拘束力を持たないものの、各連邦規制当局は、これを参照する形で各連邦規制当局が調達基準を設定しているため、米国市場はもちろん、結果的にグローバル市場における最低限のサイバースタンダードになる可能性大

*1: NIST SP800-37より抜粋
*2: National Cybersecurity Center of Excellence (NCCoE) NIST配下の官民連携シンクタンク

民間企業が取り扱う（機密情報以外の）重要情報を保護するためのガイドラインとして策定されたSP800-171は、今後さらに米国政府調達規制化により産業展開が進む見込み

SP800-171の調達規制化までの動向

CUIと保護策の定義

2010年11月9日
大統領令（Executive Order）13556

2010年11月9日から180日以内
各省庁によるCUIレジストリーへの情報登録

CUI保護方法の決定とルール形成

2015年6月
CUI保護技術体系
NIST SP800-171

2016年5月14日
連邦調達規制（FAR）
52.204-21

2016年9月14日
32 連邦規則（CFR）2002.14

各省庁とそれらとの取引が存在する民間企業でのCUI情報の取り扱いについて以下の２点を90日以内に実行を求めるE.Oが発行

① 各省庁は国立公文書記録管理局（NARA）が管理するCUIレジストリーにCUIを登録すること

② NISTが開発、発行するガイドラインに従ってCUIを適切に保護すること

32 連邦規則（CFR）2002.14では、CUIを「処理、格納、通信」する民間企業のシステムはNIST SP 800-171による保護をミニマムにすることがCUIを保有を求めた

対応コスト等を踏まえ、2016年11月14日より有効となる本規則の実施時期については実質的に各業界の判断に委ねるとした
（緩和策の提案は棄却されている）

FARは今後すべてのCUI保有業界でSP800-171を調達基準とすべくFAR 52.204-21を記述している

各省庁によりレジストリ登録されたCUIは多様な産業に跨って存在するため、北米事業を行う日本企業は当該情報を取り扱っている可能性が高い

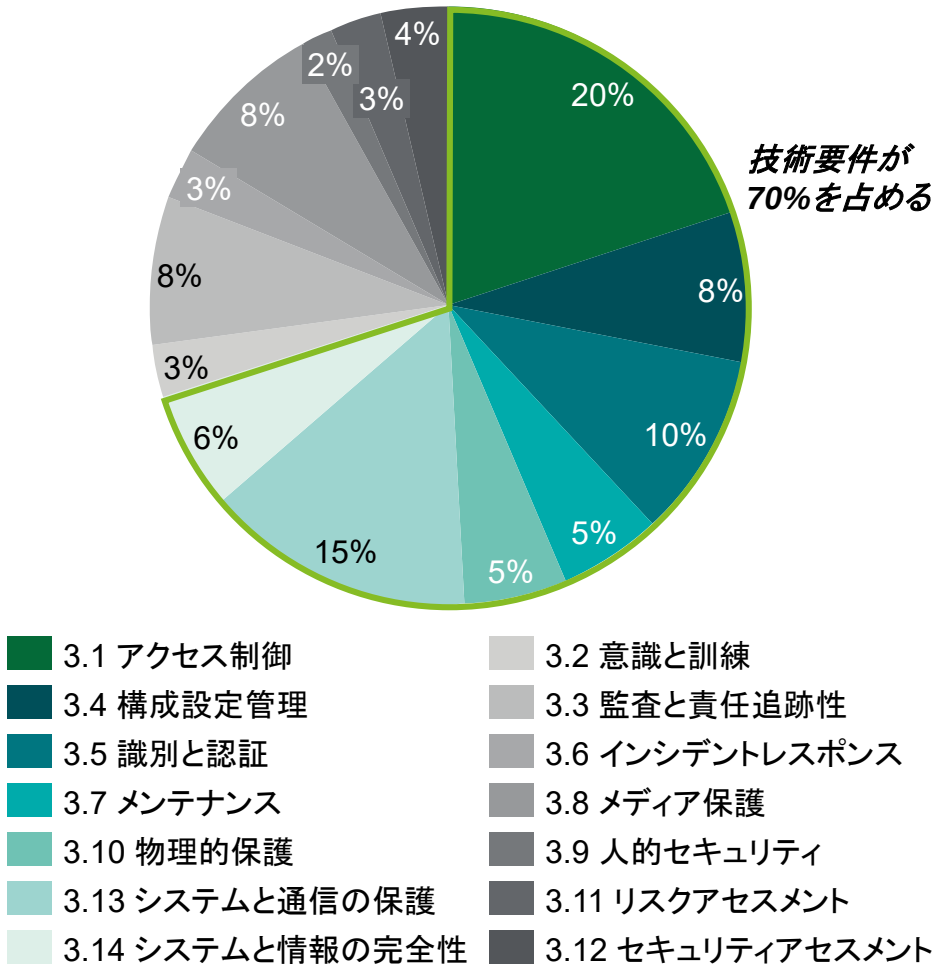
CUIレジストリに登録されている業種別CUIの例

業種	CUI（一例）
自動車	● DHSへの申請情報（自動運転試験走行など） ● テストと評価の結果（耐久性情報や自動運転走行における事故情報など） ● 内部マニュアル
電力・ガス	● インフラへの攻撃を計画するあたり有用である可能性がある情報 ● エネルギーの生産、生成、輸送、伝達、または配分に関する詳細情報 ● 原子力施設、材料、兵器に関する特定の設計およびセキュリティ情報
ヘルスケア	● 個人の過去、現在、または将来の身体的または精神的な健康状態 ● 個人への健康管理の提供記録 ● 化学薬品の使用、保管、または取扱い、および関連システム
重化学工業	● 軍事、宇宙関連情報 ● 流出が米政府にとって不利になる特許情報 ● 既存もしくは研究開発中の製品設計及び性能仕様情報
食品	● 農業に関する経営情報、保全実務情報 ● 農薬生産者情報、害虫情報 ● 水の処理方法と水質に関する詳細情報（バイオテロ対策）
IoT家電	（何に繋がり、どのような情報を処理、保有するかにより変動）

出所：https://www.archives.gov/cui/registry/category-list

実施すべき具体的なタスクと手順を、CSFから特定・具体化した、SP 800-171には技術要件が77項目、非技術要件が33項目存在し、その多くを技術要件が占める

分類ごとの項目数割合と要件分類



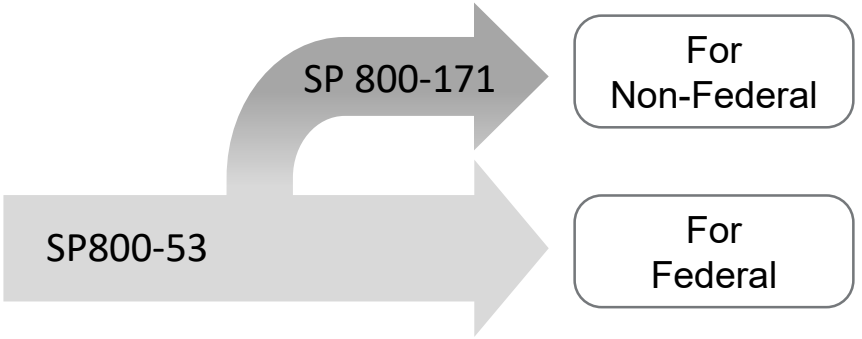
技術要件 (77項目)		
3.1	アクセス制御	22項目
3.4	構成設定管理	9項目
3.5	識別と認証	11項目
3.7	メンテナンス	6項目
3.10	物理的保護	6項目
3.13	システムと通信の保護	16項目
3.14	システムと情報の完全性	7項目

非技術要件 (33項目)		
3.2	意識と訓練	3項目
3.3	監査と責任追跡性	9項目
3.6	インシデントレスポンス	3項目
3.8	メディア保護	9項目
3.9	人的セキュリティ	2項目
3.11	リスクアセスメント	3項目
3.12	セキュリティアセスメント	4項目

SP 800-171は、Federal(政府機関)向けの要件であるSP 800-53を基に、個々の要求強度を下げずにNon-Federal(民間組織)向けの要件を抽出したものである

SP 800-171とSP 800-53の関係(1/2)

■ SP 800-53 を基に、Non-Federal向けに要件を抽出



■ 個々の要求強度（レベル）はSP 800-53と同等

■ NIST Special Publication 800-171

Organizations can use Special Publication 800-53 to obtain additional, non-prescriptive information related to the security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional security requirements if needed). **This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.**

「SP 800-53の要件を理解することでSP 800-171の要件の実装レベルの理解が支えられ、これによりSP 800-171要件に準拠したセキュリティ対策を実装することが可能になる」

The confidentiality impact value for CUI is **no less than *moderate*** in accordance with Federal Information Processing Standards (FIPS) Publication 199.

~Page 5

The moderate impact *value* defined in FIPS Publication 199 may become part of a moderate impact *system* in FIPS Publication 200, which in turn, requires the use of the moderate security control baseline in **NIST Special Publication 800-53** as the starting point for tailoring actions.

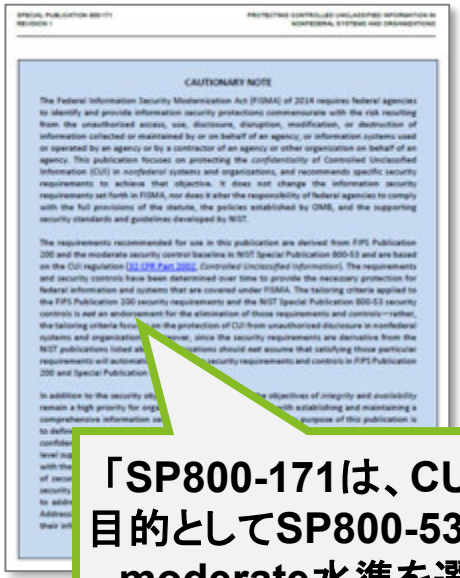
Page5, footnote 14

「CUIの機密影響値はNIST SP 800-53のModerateに劣らない」

SP 800-171はCUI保護に必要な要件をSP800-53から抽出するための“カタログ”に過ぎないため、準拠のためにSP800-53を参照すべき

SP 800-171とSP 800-53の関係(2/2)

SP800-171 rev1



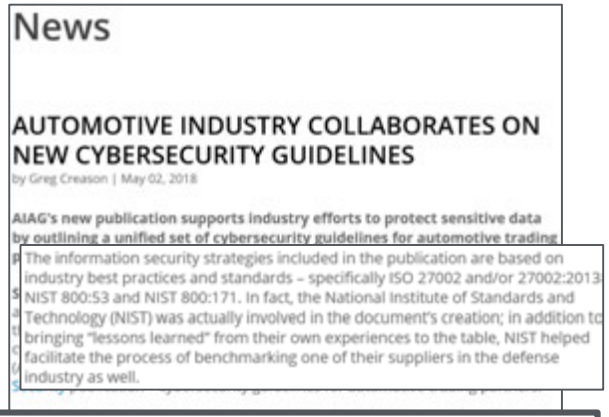
「SP800-171は、CUI保護を目的としてSP800-53におけるmoderate水準を選択して構築された」

SP800-171	SP800-53
3.1.1 アクセスを認可したユーザとプロセスに制限せよ	AC-2 アカウント管理
3.1.2 トランザクションと機能を、認可ユーザが許可した種別に制限せよ	AC-3 アクセス強制
3.1.3 CUIの情報フローを制御せよ	AC-17 リモートアクセス
3.1.4 責務の分離を実施せよ	AC-4 情報フロー強制
3.1.5 最小特権原則を採用せよ	AC-5 責務の分離
⋮	AC-6 最小特権
	⋮

出所：NIST SP800-171 rev1 (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171r1.pdf)

米国ではさらに、民間独自の取り組みとして各産業でNISTを参照するセキュリティガイドラインが設けられ、業界ごとにセキュリティの底上げに取り組んでいる

自動車業界における民間独自の取り組み


News

AUTOMOTIVE INDUSTRY COLLABORATES ON NEW CYBERSECURITY GUIDELINES

by Greg Creason | May 02, 2018

AIAG's new publication supports industry efforts to protect sensitive data by outlining a unified set of cybersecurity guidelines for automotive trading

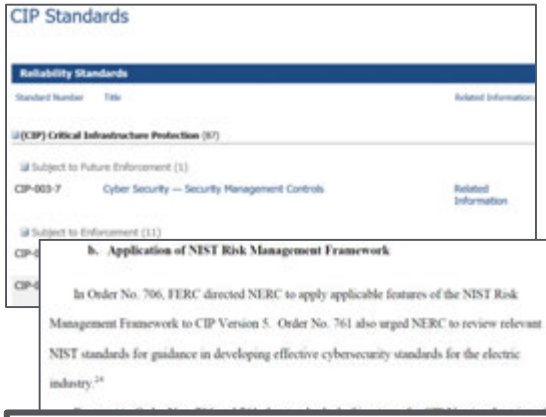
The information security strategies included in the publication are based on industry best practices and standards – specifically ISO 27002 and/or 27002:2013, NIST 800:53 and NIST 800:171. In fact, the National Institute of Standards and Technology (NIST) was actually involved in the document's creation; in addition to bringing "lessons learned" from their own experiences to the table, NIST helped facilitate the process of benchmarking one of their suppliers in the defense industry as well.

- 2018年5月2日 AIAG(全米自動車産業協会)は参加企業に向けて**NIST SP800-171に基づく**サイバーセキュリティ対策のガイドラインを発行

AIAG Automotive Industry Action Group

■組織の概要と目的
- 自動車サプライチェーンに関わるグローバルの事業者2,518社が参加(2018年2月末時点)
- 自動車のサプライチェーンに関する各種の課題に取組み標準化による生産性向上を目指す

エネルギー業界における民間独自の取り組み


CIP Standards

Reliability Standards

(CIP) Critical Infrastructure Protection (87)

CIP-003-7 Cyber Security — Security Management Controls

b. Application of NIST Risk Management Framework

In Order No. 706, FERC directed NERC to apply applicable features of the NIST Risk Management Framework to CIP Version 5. Order No. 761 also urged NERC to review relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.[24]

- NISTリスク管理フレームワーク採用
- チェックリスト方式で最低限のセキュリティ対策が示され、大規模発送電設備における順守を義務付け

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

■組織の概要と目的
- 2003年大停電を契機に米国連邦エネルギー規制委員会から権限を委譲された民間団体
- 北米の電力システムに関わる事業者の一定レベルのセキュリティ確保のための標準化活動を行う

NISTによる技術実装に関するベストプラクティス(SP1800)展開

■SP1800文書(抜粋)

文書番号	テーマ	対象業界
SP1800-1	モバイル機器上の電子健康記録のセキュリティ対策	医療
SP1800-2	エネルギー業界におけるアイデンティティ及び資産管理	エネルギー
SP1800-5	IT資産管理	金融
SP1800-7	状況認識(監視)	エネルギー
SP1800-8	ワイヤレス輸液ポンプのセキュリティ対策	医療
SP1800-9	アクセス権管理	金融

⋮

- NIST SP800準拠のセキュリティ対策について、各業界における実務的なベストプラクティスとしてSP1800文書群が作成、公開されている

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE | NIST National Institute of Standards and Technology U.S. Department of Commerce

■組織の概要と目的
- NIST内の官民連携R&Dセンター
- 産業界、学術機関と政府機関の連携ハブとして、ビジネス上のサイバーセキュリティ課題の対応に必要なケイパビリティを導入することを推進する機関

欧州では2018年から欧州で活動する企業に対し国際標準で定められたサイバーセキュリティ技術の利用を2016年8月に法律で義務付けた

欧米市場の法制度の変化

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

米国立標準研究所

- 国防総省と取引のあるサプライヤーは2017年12月31日までにNIST　SP800-171の技術体系で構築された社内システムに移行することを要請する通達を発行
- 2018年の途中からアメリカ市場で取引する事業者にはSP800-171もしくはSP800-53の技術体系で構築されたシステムに移行しなければ米国での活動が出来なくなる方針

サイバーセキュリティの技術レベルでのISO化を協議

EUROPEAN COMMISSION

欧州理事会

enisa
European Network and Information Security Agency

欧州ネットワーク
情報セキュリティ庁

- 2018年5月10日までに、国際標準で定められたサイバーセキュリティ技術を用いた社内システムに移行しなければ、欧州での事業活動が許されない法律が発効
- 上記のシステム変更以降を前提に2018年5月25日よりGDPRの運用を開始し、情報漏洩企業にはグループ連結売上の4%の罰金を課していく方針

条文の中では、セキュリティの具体的なタスクが義務化され、罰則規定まで設けており、日本企業にとって、欧州市場への新たな非関税障壁になる可能性が高い

NIS Directiveの内容

具体例なセキュリティ対策の義務化

第4章　第15条　実施及び執行
第2項
加盟国は、所轄官庁にしかるべき権力及び手段を与え、重要サービス事業者に対して次の提出を義務付けなければならない。

(b) 所轄官庁又は認証された監査機関によって実施されたセキュリティ監査結果等の証拠

第5章　第16条　セキュリティ要件及びインシデント通知
第1項
加盟国は、自国内のデジタルサービス提供者が、ネットワーク及び情報システムのセキュリティリスクを管理する適切且つ十分な技術的及び組織的な手段を特定、採用した上で、サービスを提供することを確保しなければならない。時代の最先端技術を考慮し、これらの手段には、下記の要素を含めなければならない。

(a) システム及び施設のセキュリティ
(b) インシデント対応
(c) ビジネス継続マネジメント
(d) モニタリング、監査、テスト
(e) 国際標準へのコンプライアンス

対象となる重要セクター

1. エネルギー（電力、石油、ガス）
2. 交通（空輸、鉄道、海運、陸運）
3. 銀行
4. 金融
5. ヘルスケア
6. 水道
7. デジタル（検索エンジン、eコマース、クラウドコンピューティング）

国際標準の取り入れを明記

第6章　標準化とボランタリー通知
第19条　標準化

第1項:
加盟国は、ネットワーク及び情報システムのセキュリティに関し、欧州又は国際的に受け入れられている標準・仕様の導入を奨励しなければならない
第2項:
ENISAは、加盟国と連携しながら、欧州又は国際的に受け入れられている技術標準・仕様、既存の国際標準等に関し、アドバイス及びガイドラインを策定しなければならない

NIS Directiveでも、2018年運用開始のGDPRでも、守る対象・レベルは異なるが、データ漏えいを検知し、短時間で分析結果を当局に通知する体制が義務付けられた

2018年のGDPRとのダブルパンチ

NIS Directive

内容

- 重要インフラ事業者（エネルギー、交通、銀行、金融、ヘルスケア、水道、デジタル; 検索エンジン、eコマース、クラウドコンピューティング）に対する最新のセキュリティ対策の導入、国際標準への準拠
- 情報漏洩時の当局への迅速な通知義務
- 罰則規定あり（詳細検討中）

タイムライン

2016年7月6日　欧州議会可決
2016年8月6日　施行
2018年5月9日　EU各国における法制化の期限
2018年5月10日　適用開始

EU一般データ保護規則（GDPR）

内容

- 顧客データを処理（収集・保管・変更・開示・閲覧・削除等）し、EU域外に移転することを原則禁止
- データ保護オフィサー（DPO）の設置
- 情報漏洩の出所と流出内容をの72時間以内の公開及び当局への通知義務
- EUの顧客データを扱う企業は、EU域外でも適用される
- グループ年間売上高の最大4%又は2,000万ユーロ（約23億円）の罰金

タイムライン

2016年4月14日　欧州議会可決
2016年5月24日　施行
2018年5月6日　EU各国における法制化の期限
2018年5月25日　適用開始

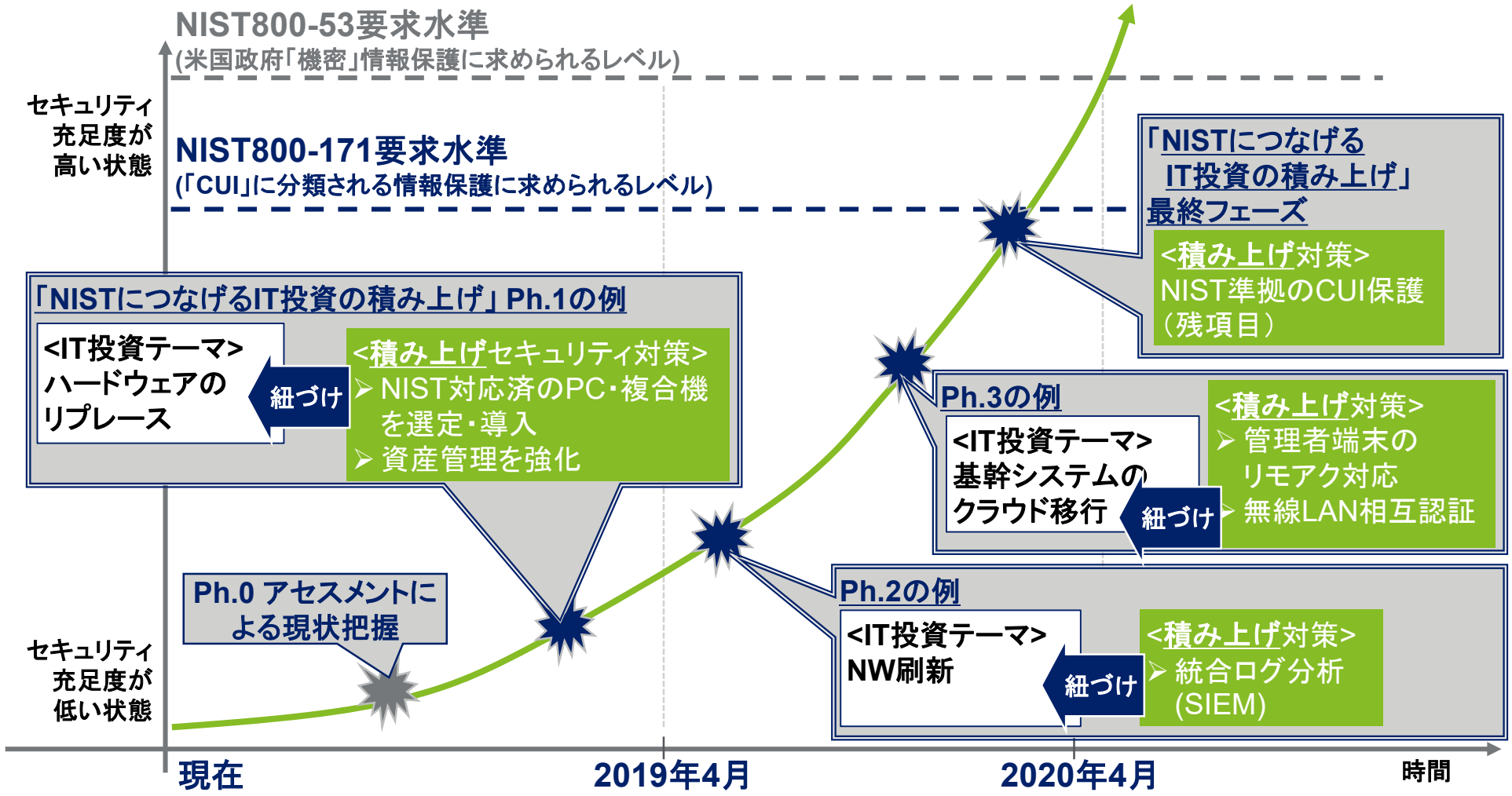
共通

EU域内で事業を行う企業、又はEU域内の顧客のデータを扱う事業者は、ネットワークシステム＆データで何が起きているかをリアルタイムで把握し、迅速にレポートできる能力を身に付けなければならない点での強制ルールは共通している

2. 国内企業が注視すべき
サイバーをめぐる最新の動向

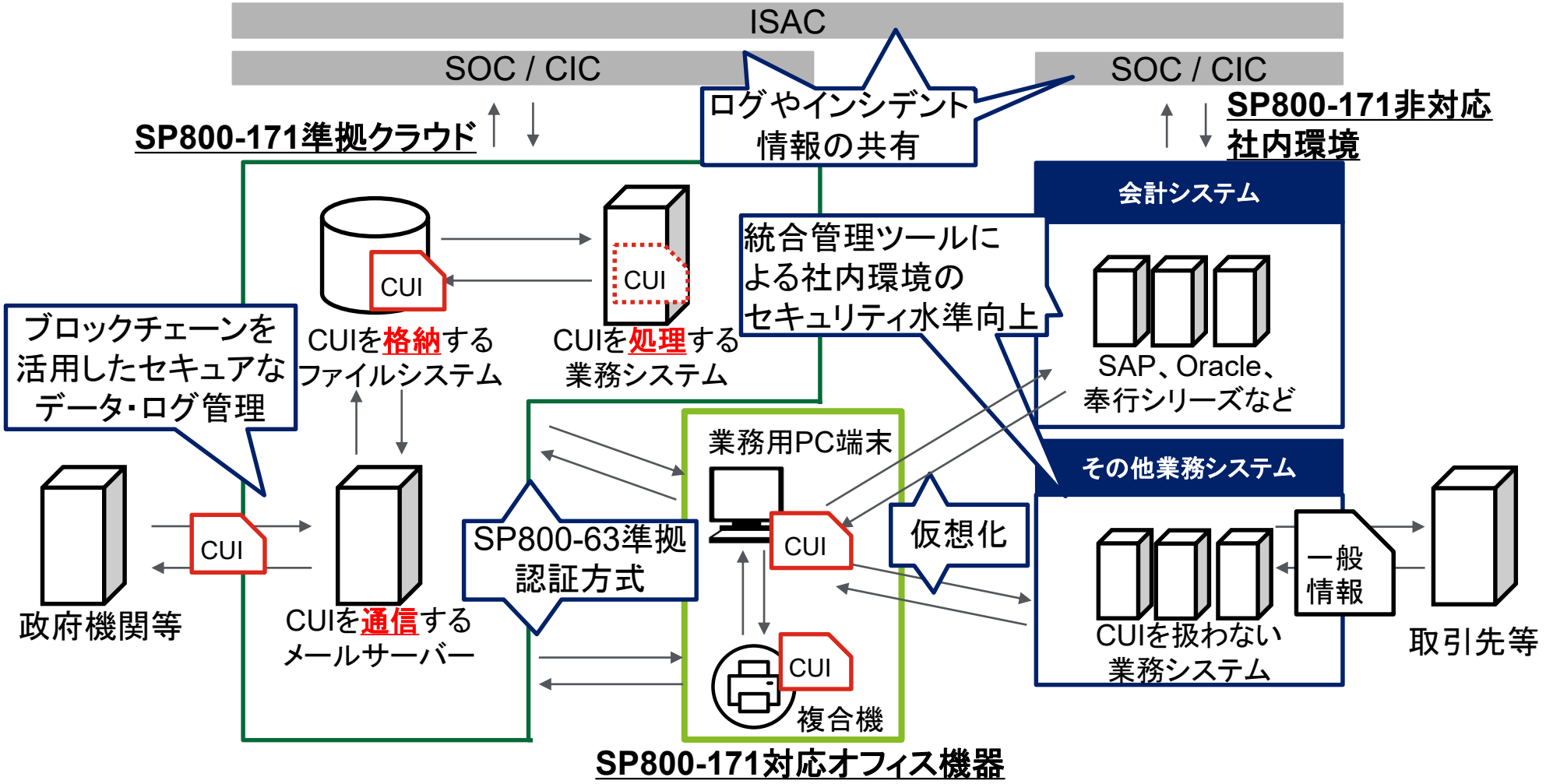
NIST SP800-171要求水準に効率的に近づけるためには、ハード、ソフト、ネットワーク機器の購入計画を見直し、NIST要求水準を満たす商品へ入れ替えることが有効

「NISTにつなげるIT投資の積み上げ」のイメージ



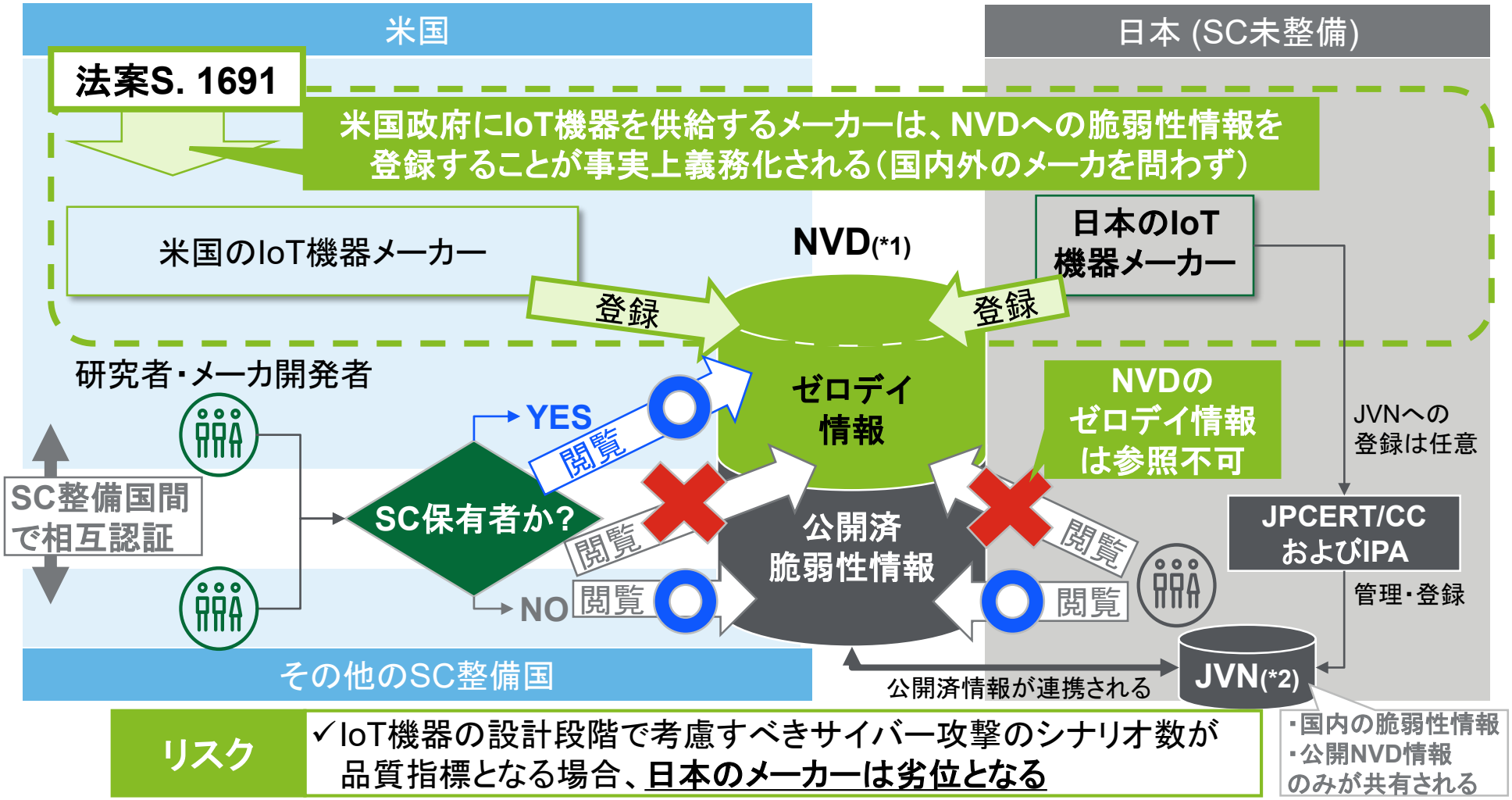
SP800-171準拠クラウドや171対応オフィス機器など、国内企業向けにCUIを効率的に管理（処理・格納・通信）できるソリューションの充実が求められている

クラウドを活用したSP800-171対応のリファレンスアーキテクチャ



米国上院の法案S.1691は連邦政府にIoT機器を供給するメーカーに対し、ゼロデイを含む脆弱性情報のNVDへの登録を事実上義務化する一方で、SC制度がない日本のメーカーはゼロデイ情報を閲覧できないため、著しい競合劣位となるリスクがある

S.1691によって日本企業が陥る問題の構造



リスク　✓IoT機器の設計段階で考慮すべきサイバー攻撃のシナリオ数が品質指標となる場合、<u>日本のメーカーは劣位となる</u>

*1 : National Vulnerability Database 、NISTが管理する脆弱性データベース
*2 : Japan Vulnerability Notes、JPCERTとIPAが共同する日本国内の製品開発者の脆弱性対応状況を公開するサイト

SP800-171においても「情報システムの構成に関連する脆弱性情報を把握し対応する」ことが求められているため、脆弱性情報の収集の重要度は今後より高まる

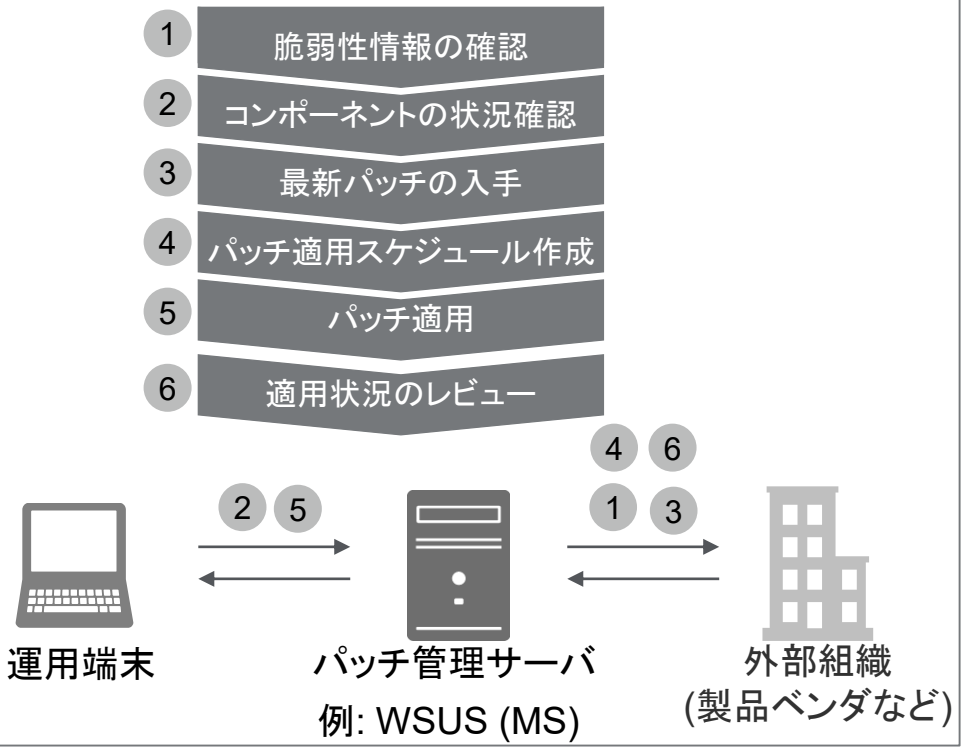
【3.14システム及び情報の完全性】の要件概要

171 ID	53 ID	コントロール名
3.14.1	SI-2	欠陥修正

■SI-2コントロールが要求するパッチ管理のプロセス

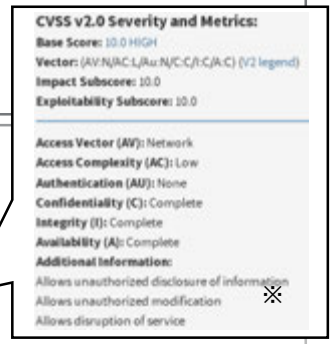
- パッチ・・・HW / SWのバグ・脆弱性等を修正するためのファイル

パッチ管理の運用プロセス



【参考】Security Content Automation Protocol
セキュリティ対策のための作業**標準化及び自動化**、それに伴う作業の負荷低減を目的とした技術仕様
（以下は標準化・自動化の対象例）

CVE 共通脆弱性識別子	脆弱性を識別する 例: CVE-2014-6271 (shell shock)
CCE 共通セキュリティ設定一覧	セキュリティ設定を識別.
CPE 共通プラットフォーム一覧	製品を識別
CVSS 共通脆弱性評価システム	脆弱性の深刻度を評価
XCCDF セキュリティ構成設定チェックリスト記述フォーマット	チェックリストフォーマットを記述する
OVAL セキュリティ検査言語	脆弱性やセキュリティ構成設定をチェックする



※