SCIS 2014 The 31st Symposium on
Cryptography and Information Security
Kagoshima, Japan, Jan. 21- 24, 2014
The Institute of Electronics,
Information and Communication Engineers

企業間における情報セキュリティ連携アーキテクチャの検討

A study of information security exchange architecture inter-enterprise

長内 仁* 後藤 厚宏*
Hitoshi OSANAI Atsuhiro GOTO

あらまし 近年，サイバー攻撃により政府機関，企業の機密情報や個人情報の漏えい,Web サイトの改ざん等が増加している．さらに，大企業とサプライチェーンを構成しているセキュリティ強度が弱い中小企業に対する攻撃も増加しているため，企業は自社だけでなく，取引企業やグループ企業を含めたサプライチェーン全体の情報セキュリティを守ることが必要となっている．しかし，日々増加する IT 機器や脆弱性に対して，企業のシステム管理者は自社の情報セキュリティを管理することも困難になってきている．本稿では，その対策として，情報セキュリティ標準規格を利用して企業間のセキュリティ基準の水準を統一化し，自動管理するアーキテクチャを示す．

キーワード SCAP, 自動化, 情報セキュリティ基準, ICT チェーン

1 はじめに

近年，マルウェア，APT 攻撃といった脅威による情報漏えいや企業活動停止のリスクが高まっている．これらの脅威はソーシャルエンジニアリングやソフトウェアの脆弱性に対する攻撃により，コンピュータがマルウェアに感染することが原因となる．ICT 社会の普及により機器やソフトウェアは日々増加しており，脆弱性に限っても組織内すべてを管理することが難しい．

さらに，企業や団体の ICT システムは 1 社のみだけでなく複数の企業が複雑に連携した ICT チェーンを構成している．これら ICT チェーン内では機密情報や情報システムを共有することが多く，ICT チェーン内にある企業からの情報流出や連携企業を踏み台として攻撃される可能性がある．このように ICT チェーンにおけるセキュリティ対策は，自社に対する情報セキュリティ対策だけではなく，ICT チェーン全体を考慮した対策が必要となり，これまで以上に困難になってきている．

一方，企業間ではこれまでも委託元が委託先に情報セキュリティ基準を提示して基準の順守を要求している．しかし，再々委託先など委託先より先のチェーンの企業まで直接指示できず，また，フォーマットやチェック基準が各社独自の基準であるため整合性のチェックに人手を介する必要があるため，管理コストが増加している．

そのため, ICT チェーンにおけるセキュリティ対策では，企業間におけるセキュリティ基準指標値の統一と自動処理による効率化が必要不可欠となる．

情報セキュリティの自動化に関連しては，標準規格が策定されている．米国 NIST(National Institute of Standards and Technology)は，脆弱性情報を管理，流通させるため規格群である SCAP，脆弱性を含む各種セキュリティ情報を自動化して継続的にモニタリングする ISCM を公開している．また，ITU-T ではサイバーセキュリティ情報の共有フレームワークである Cybex(X.1500)が策定された．

本稿では，ICT チェーンに関わる企業全体のセキュリティレベルの向上を図ることを目的に,情報セキュリティ基準を企業間で共有・定量化するアーキテクチャを検討した.そして，アーキテクチャに必要となる要素を整理し，標準規格を利用した企業間セキュリティ基準の標準化と自動化によるセキュリティ対策の効率化を行う．

提案アーキテクチャは，情報セキュリティの標準規格を利用して，データ形式の統一化，企業間におけるセキュリティ情報共有・分析の自動化により，管理コストの軽減を可能とする．また，情報セキュリティ対策は技術的なものだけでなく，組織のマネージメントや人材教育などの複合的対策が必要であり，必ずしも全てを自動化できない．本研究では，情報セキュリティ標準化規格を利用して機械による自動化が可能な対象に絞って検討を行った．

*情報セキュリティ大学院大学,
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
{mgs124504@iisec.ac.jp, goto@iisec.ac.jp}

本稿の構成は以下の通りである．まず，2 章で ICT チェーンにおけるセキュリティ対策の課題を示す．3，4 章で標準化の動向や関連研究を示す．5，6 章で課題を解決するためのアーキテクチャを提案し評価する．7 ，8，9 章に考察、まとめと今後の課題を述べる．

2　ICT チェーンにおける情報セキュリティ

2.1　ICT チェーン

企業や団体の ICT システムは 1 社のみだけでなく複数の企業が複雑に連携した ICT チェーンを構成している(表 1).

表 1　ICT チェーンを構成する企業関係

No.	企業関係	例
1	グループ企業	親会社/子会社/関連会社
2	外部委託	アウトソーシング/ 海外オフショア
3	外部サービス	クラウドサービス利用/ 企業間システム連携
4	共同事業	共同研究/ ジョイントベンチャー

ICT チェーンにおける企業規模，企業数とセキュリティ強度を図 1 に示す．通常，大企業が委託元，中小企業が委託先や再委託先となるので，ICT チェーンの末端に向けて企業数が多くなる．日本の中小企業の割合は 99.7%となり，ICT チェーンの重要な要素である.しかし，中小企業の多くは自社の規模が小さい為に危険が少ないと考えており，セキュリティにかけるコストの観点からも大企業に比べてセキュリティ対策の水準が低いのが現状である．

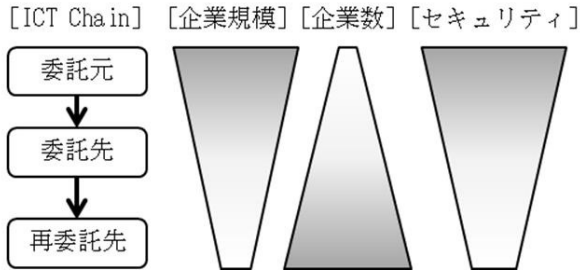

図 1　ICT チェーン構造とセキュリティ強度

2.2　ICT チェーンにおける情報セキュリティ脅威

近年，標的型メール攻撃が増加しており，情報処理推進機構(IPA)は社内ネットワークにおいて「入口対策」と「内部対策(出口対策も含む)」の重要性を提案している[1][2]．一方，これら標的型攻撃の 31%は 250 名以下の中小企業を標的であるという報告もある[3]．その理由として，中小企業は 1 社でビジネスをするのではなく，親会社や取引先といった大企業との ICT チェーンの中に入っていることが多いため，大企業を攻撃するための踏み台として狙われると考えられる．2011 年に生じた三菱重工業を狙った APT 攻撃は，関連団体のメールが搾取された後，関連団体に成りすましたメールにより攻撃されたといわれている．同年には，国土地理院のサーバを踏み台に他機関の ID とパスワードを解析して不正に侵入しようとした攻撃が行われた．このような関連企業(団体)を介した高度な攻撃は，自社内のネットワークを守るセキュリティ対策だけでは防ぐことができない．そのため，弱いチェーンである中小企業を狙った攻撃が今後も増加すると考えらえる．

ICT チェーンを形成する企業間において，委託先に対する脅威の例を以下に整理する．

(1) ネットワークを介した脅威
- 委託先で感染した PC を介した ICT チェーンネットワークに対する不正アクセス
- 委託先の人物に成りすました標的型メール

(2) 委託した資産の脅威
- 機密情報・個人情報の漏洩
- 情報資産の破壊

(3) 事業継続の脅威
- 情報セキュリティインシデントで委託先事業が停止することによる ICT チェーンの停止

これらの脅威に対して，企業はセキュリティ基準を定めて日々管理していく必要があり，企業内に閉じている場合は，これまで通り自社のセキュリティ基準を定め，継続的にセキュリティ基準を満たしていることを確認すれば良い．しかし，ICT チェーンにおいては自社のセキュリティ基準を委託先も含めて満たしていること，委託元のセキュリティを自社や再委託先が満たしていることを確認する必要がある．つまり，ICT チェーンではセキュリティ基準を定量化して比較できるように指標値を統一化し，企業間でセキュリティ基準の水準を評価できる仕組みが必要になる．.つまり，自組織だけでなく ICT チェーン全体のセキュリティ水準を向上させることが脅威に対する対策として不可欠となる．

2.3　ICT チェーン内の情報セキュリティ課題

前節で示した ICT チェーンにおけるセキュリティ対策に関して，現状の課題を 2 点提示する．

(1) ICT チェーン全体へのセキュリティ確認

ICT チェーンは複数の企業によって多段に構成されており．委託元は自社のセキュリティ基準を ICT チェーン全体に適用するため，委託元や再委託先にセキュリティ基準を展開する必要がある(図 2)．しかしながら，法律上の理由で，委託元は委託先より先の再委託先，再々委託先の企業まで情報セキュリティ基準を直接要求することができない．

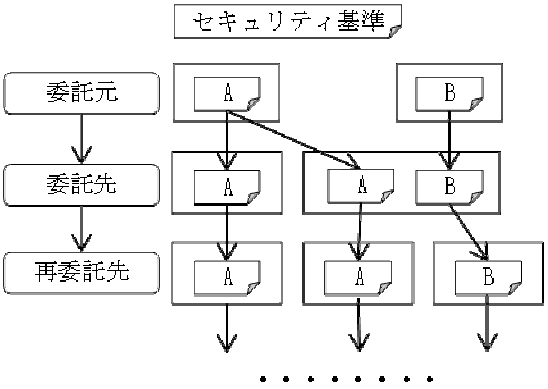

図 2　セキュリティ基準の流通

そのため，委託元は委託先経由で ICT チェーン末端の企業が自社の情報セキュリティ基準を適用しているか把握することになる．一方，委託先も複数の委託元から提示される異なるセキュリティ基準のチェックや再委託先へのセキュリティ基準の提示を行う必要があり，人手とコストがかかる．同様に，インシデント発生時にも ICT チェーンのどこに問題が発生し，どのような影響があるかを直接把握することが難しく，原因解明が遅れる．

また，企業は ICT チェーン内の様々な企業に自社のセキュリティ情報を出したくないため，必要な情報を必要なチェーンにのみ流通させる必要がある．

このように，複雑に絡み合う ICT チェーン全体に情報セキュリティ対策を流通させて管理することは困難な状態である．

(2) 企業間の情報セキュリティ基準の不統一について

情報セキュリティ対策は，情報セキュリティインシデントを防ぐこと，インシデント発生時に迅速に対処することが重要であり，ICT チェーン全体で情報セキュリティ対策をする必要がある．これまでも委託元から委託先に情報セキュリティ基準を満たすことを要求している．しかし，ICT チェーンにおける委託元と委託先において，セキュリティ情報の連携に下記のようなギャップが生じている．

- 用語の不統一
  - ・企業によって情報セキュリティ対策やインシデント発生に関する用語が異なる
  - ・グローバル企業では利用する言語が異なる．
- 定量的な値でない
  - ・「パスワードの定期的変更」という要求に対して，変更すべき期間が具体的でない
  - ・「レベル高のインシデントが発生」という報告に対して，自社の基準と対応づけできない
- 情報交換フォーマットの不統一
  - ・セキュリティ対策の実施報告フォーマットや提出方法が企業毎に異なっている
- 人手とコストがかかる
  - ・「セキュリティパッチの定期的更新」という要求に対して，統合管理ソフトを導入していないため，自社の社員が実際に行っているか確認できない．
  - ・企業規模によってはコスト面で導入困難なこともあり，継続的な更新確認が難しい．

以上より，現在の ICT チェーンのセキュリティ対策のままでは，企業間のセキュリティ基準の水準を合わせることは困難である．そのため，今後は情報セキュリティ基準を企業間で共有すること，共有したセキュリティ基準を同一基準で評価できることが必要となる．

3　情報セキュリティ基準

3.1　SCAP

SCAP(Security Content Automation Protocol)は米国 NIST が公開しているソフトウェア不具合，セキュリティ設定情報を伝達する際のフォーマットや命名を標準化する仕様群である[4]．設定，脆弱性やパッチの確認を自動化するサポート，コンプライアンス活動の技術的制御やセキュリティ対策といった複数の目的をもったフレームワークとなっている．SCAP は NIST SP800-126 でバージョン 1.0 の技術仕様が策定され，NIST SP800-126r2 でバージョン 1.2 となった．SCAPver1.2 は 5 つのカテゴリと 11 のコンポーネント仕様から成り立っている(表 2)．

表 2　SCAP コンポーネント一覧

No.	カテゴリ	コンポーネント
1	記述言語	XCCDF,OVAL,OCIL
2	レポートフォーマット	ARF,AI
3	一覧表，目録	CPE,CCE,CVE
4	スコアリング	CVSS,CCSS
5	完全性	TMSAD

また，米国の NIST 標準である SCAP の CVE(X.1520)，CVSS(X.1521)や CPE(X.1528)が X.1500 シリーズとして ITU-T で勧告された．このように脆弱性対策やインシデント対策などセキュリティ対策関わる技術仕様の国際標準化が進められており，今後の利用拡大が予想される．

3.2　Cybex

Cybex (The Cybersecurity Information Exchange Framework)は，共通仕様を利用して各国の機関がサイバーセキュリティ情報を交換・相互運用するためのフレームワークである[5]．Cybex は，ITU-T 勧告 X.1500 として国際標準化された． Cybex には，5 つの機能ブロックから構成されている(表 3)．ここで情報記述ブロックに SCAP の仕様が利用されている．

表 3 Cybex 機能ブロック一覧

No.	機能ブロック
1	情報記述ブロック
2	情報発見ブロック
3	情報クエリブロック
4	情報検証ブロック
5	情報伝送ブロック

3.3 ISCM

ISCM(Information Security Continuous Monitoring)は, 組織のリスク管理における意思決定を支援するために, 情報セキュリティ, 脆弱性, 脅威を継続的に把握するためのフレームワークであり, NIST SP800-137 として公開されている[6][7]. ISCM では, 対象とする自動化領域として, 11 の領域が提示されている. 例えば, 脆弱性情報管理の継続的モニタリングに, 相互運用可能なデータ仕様である SCAP の利用が想定されている. また, 管理ダッシュボードの利用による管理の有用性ついても記載されている.

表 4 ICSM の自動化領域

No.	領域	No.	領域
1	脆弱性管理	7	インシデント管理
2	パッチ管理	8	イベント管理
3	マルウェア検知	9	ライセンス管理
4	アセット管理	10	情報管理
5	設定管理	11	ソフトウェア保証
6	ネットワーク管理	-	-

3.4 USGCB

2007 年, 米国 OMB(Office of Management and Budget) が, 米国の各省庁で利用するクライアント PC の推奨セキュリティ設定リスト FDCC(Federal Desktop Core Configuration)を策定した. 2010 年には AIC 委員会が USGCB(The United States Government Configuration Baseline:米国政府共通設定基準)を策定した[8]. FDCC は Windows XP や Vista が対象だったが, USGCB は Windows7 や RedHat 等の幅広いプラットフォームを対象とするため, FDCC を置き換えてセキュリティ基準を提供する. また, 米国政府のデスクトップ環境がこれら基準を満たしているかチェックを自動化するために SCAP との連携が行われている.

3.5 ISO/IEC 27036

現在策定中の ISO/IEC 27036 の Part3 において, ICT サプライチェーンの情報セキュリティガイドラインが提示されている. また,Part4 でクラウドサービスにおける情報セキュリティガイドラインも策定中である.

4 関連研究

情報セキュリティ標準を利用した関連研究として, SCAP を利用した脆弱性対策を中心に研究が進められている. 寺田らは JVN の脆弱性対策情報を用いたサービスとしてフィルタリング型情報提供サービス MyJVN を提案した[9]. MyJVN フレームワークとして, クライアント PC 上にインストールされているソフトウェアのバージョンチェックを行う MyJVN バージョンチェッカが, 独立行政法人情報処理推進機構(IPA)により公開されている[10]. 中村は SCAP に基づいた自動化手法を利用し, Linux および Windows のマルチプラットフォームに対応した脆弱性管理システムを提案した[11]. 藤堂らは, HTML ベースの Web 情報セキュリティ情報からクライアントのソフトウェアに脆弱性があるかどうか確認するシステムを提案した[12]. 岡城らは XACML を拡張した機器に依存しないポリシー記述言語により, システム内のポリシーを統一的に表現可能とし, セキュリティ機器から設定情報を抽出して分析する機器設定統合分析システムを提案した[13].

これらの研究では, SCAP 標準を利用した脆弱性や設定を自動管理することを目的としている. 一方, ISCM では脆弱性管理や設定管理を含め 11 の管理領域を提唱しており, 今後はそれら領域にも自動化による管理を適用する必要がある. また, 関連研究の適用範囲は組織内における管理であり, 企業間が連携した ICT チェーン全体を管理することを意識していない.

5 提案アーキテクチャ

5.1 アーキテクチャ概要

ICT チェーン内の情報セキュリティを連携させるアーキテクチャを提案する. 本アーキテクチャは, これまで述べた課題を解決するために, 情報セキュリティの標準規格を利用して, 下記の要件を満たす.

(1) セキュリティ情報や用語体系の統一
(2) 情報交換フォーマットの統一
(3) 分析の自動化と継続的なモニタリング
(4) 管理ダッシュボード
(5) レポーティング

委託元が委託先に情報セキュリティ基準を提示して委託元が自社の情報と提示されたセキュリティ基準の分析結果を返却するユースケースについて, 2 企業間におけるアーキテクチャを図 3 に示す.

構成要素としてログを収集・分析する管理サーバとセキュリティ情報を管理サーバに送信するクライアントからなるクライアント/サーバモデルとなる. また, システム管理者向けに Web 管理画面を提供する.

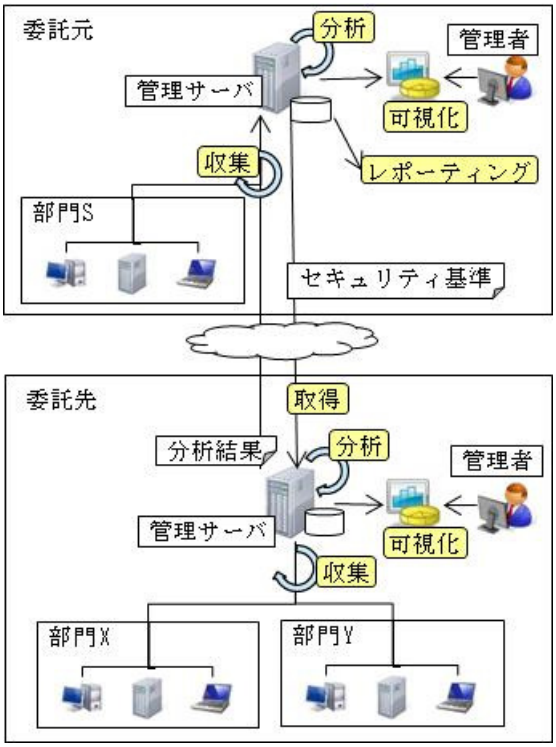

図 3　2 企業間におけるアーキテクチャ

クライアントは PC 以外に NW 機器や IDS/IPS といったセキュリティ機器もあり，ログの種類も脆弱性情報以外にイベントログなど多様で膨大なものとなる．これらクライアントについて，情報セキュリティ情報を収集する情報セキュリティセンサ(以下，IS センサ)と定義すると，本アーキテクチャは，管理サーバ/IS センサ間，管理サーバ間で IS センサデータを自律的に情報交換して制御を行う M2M 型システムとみなすこともできる．

以降の節で機能要素について説明する．

5.2　セキュリティ情報の統一

図 3 の機能要素同士が交換する情報は，以下のように情報セキュリティ標準規格に基づいたデータ形式を用いて統一する．ソフトウェア脆弱性管理には SCAP の仕様群，アクセス制御ポリシーに XACML 等を適用する．また，セキュリティインシデントが生じた場合は，IODEF 形式を利用する．また，PC 端末のパスワードポリシー等の設定管理には USGCB でも利用されている CCE を用いて基準を定義する．このように情報形式を統一することで IS センサのベンダーに依存せずに連携することが可能になる．

5.3　セキュリティ情報収集

組織内の情報交換に関して，管理サーバは IS センサから送信される情報を受信する API を提供する．IS センサが PC やサーバの場合はエージェントをインストールし，自マシンのセキュリティ情報を管理サーバに送信する．セキュリティ機器や NW 機器からもログを管理サーバへ送信する．収集には，REST による WebAPI や syslog の利用を想定する．

5.4　自動化/継続的なモニタリングと「分析」

IS センサからの情報収集，ICT チェーン内の管理サーバと連携，分析を自動化して継続的にモニタリングする．

分析は自動化され，自組織内や ICT チェーン毎に実施する(図 3)．管理サーバは IS センサから収集したデータを分析し，セキュリティ基準を満たしているか確認する．分析項目は下記の内容が考えられる．

・自社のセキュリティ基準を満しているか
・委託元企業のセキュリティ基準を満たしているか
・委託先企業がセキュリティ基準を満たしているか

また，ISCM のイベント管理，インシデント管理の観点を導入し，収集したログを監査やフォレンジック分析に活用する．

5.5　分析結果の「可視化」

ISCM に記載されている表示・レポート用のダッシュボードを Web アプリケーションとして提供する．管理者は分析結果をほぼリアルタイムに確認でき，本アーキテクチャにより委託元の管理者は ICT チェーン全体のセキュリティリスクやインシデント情報を把握することができる．また，実運用では動作検証するまでセキュリティパッチを適用しない等，自動化だけでなく手動管理も必要となる．本ダッシュボードは，手動管理が軽減できる補助機能として利用できる．

5.6　分析結果の「レポーティング」

分析した結果をレポート出力する．対象ユーザとして，経営層や情報システム管理者が挙げられる．レポーティングを監査や経営層への報告に活用することで企業の意思決定や IT ガバナンスに活用できるため，BI ツールとの連携も想定する．ICT チェーンにおいては外部企業へレポートする必要がある．

5.7　ICT チェーンにおける情報流通

企業間の情報交換は，委託元と委託先は管理サーバ間で情報連携を行う．委託元は要求するセキュリティ基準を委託先管理サーバへ送信し，受け取った委託先は自社データベースに保存するとともに必要に応じて再委託先へも送信する．連携するセキュリティ情報は機密情報なので，ICT チェーン毎に必要な情報のみ流通させる．企業間の連携には SOAP や SOAP for Cybex を想定する．

6　評価

提案アーキテクチャの各要素について，データ収集・格納部の実装や分析シナリオを作成することで評価した．

6.1　セキュリティメタ情報の収集・格納

セキュリティ情報の収集・格納として，NIST の公開データと Windows クライアント端末のレジストリからインストールソフトウェア情報を取得した．
NIST の公開情報収集・格納フローを図 4 に示す．

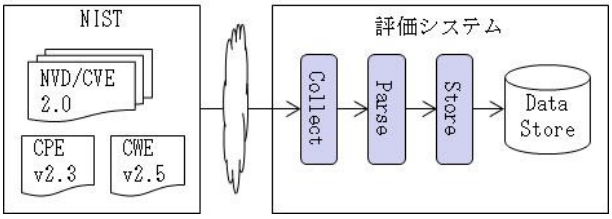

図 4　NIST 公開情報の収集・格納

収集してデータストアに格納するフローにおいて，Collect/Parse/Store のモジュールに分けて実装した．各モジュールについて，以降に示す．

(1) Collect

NIST の Data feeds サイトから CVE 脆弱性データベース情報(NVD/CVE 2.0)，CPE 情報(バージョン 2.3)および CWE 情報のファイルを取得した．NVD 情報は年毎にファイルが分割されており，今回の評価では 2009 年～2013 年(9/15 時点)のデータを収集した．

(2) Parse

収集した NIST のデータはすべて XML 形式のため，それぞれのファイル毎に XML パーサを作成し，取得した XML ファイルをパースした．

(3) Store

パースした XML ファイルをデータストアに格納した．データストアとして，OSS の RDBMS および全文検索サーバの 2 種類に格納可能とした．

収集・格納した NIST のデータについて，レコード数とファイルサイズ情報を表 5 に示す．

表 5 NIST 公開データ情報

データ	レコード数	ファイルサイズ(MB)
NVD/CVE	21,721	250.5
CPE	72,784	16.4
CWE	940	9.9

※NVD/CVE は，2009 - 2013/9/15 の 5 ファイル合計

6.2　クライアント情報の収集・格納

クライアント情報からのデータ収集について示す．Windows 端末レジストリ情報より，インストールされている情報を取得し，情報をクライアントに提示することが可能である(図 5)．また，サーバの Web API を介して，その情報を送信することが可能となっている．

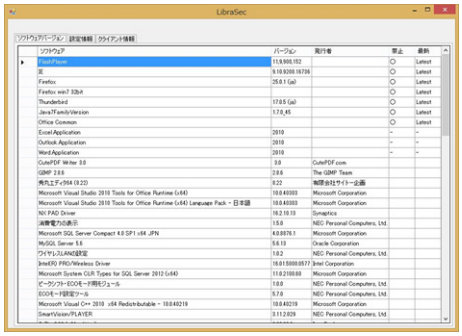

図 5　インストールソフトウェア一覧画面

6.3　データの可視化

格納したデータの CRUD 操作ができる簡易 Web アプリケーションを用意した．統計情報の表示例を下記に示す(図 6)．今後機能拡張していく予定である．

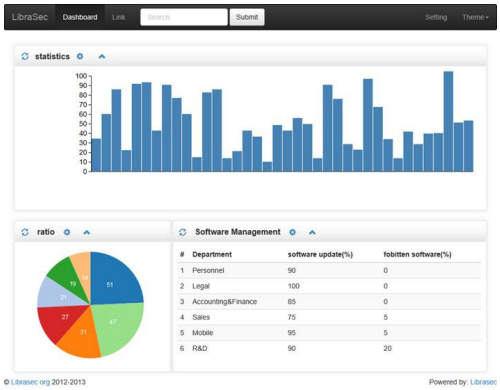

図 6　Web 管理画面

6.4　分析シナリオ評価

本節では，収集・格納したデータをベースにして、実際のセキュリティ基準の項目[14]を参考に分析シナリオを作成し，評価した．

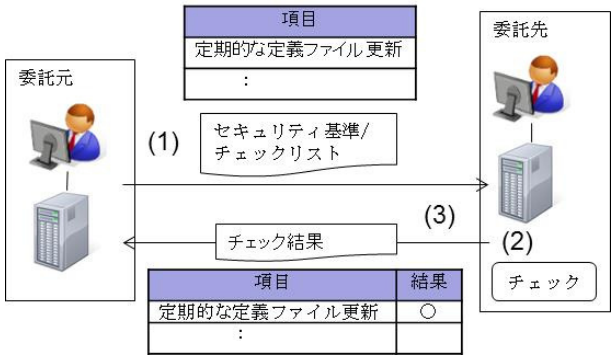

図 7　情報セキュリティ基準のチェック

(A) ウイルス対策ソフトウェアの導入確認

まず，情報セキュリティ基準の項目として，「ウイルス対策ソフトの導入」と「パターン定義ファイル更新」をチェックするシナリオを評価する．クライアント PC の

セキュリティ対策として，多くの場合ウイルス対策ソフトウェアを導入しており，情報セキュリティ基準でもその導入が求められている．これまでの課題としてウイルス対策ソフトのインストールやパターン定義ファイルの更新はユーザ判断になり，実際に実施されているか管理できない場合がある．また，チェックツールが存在してもクライアントでの実行結果がシステム管理者にフィードバックされず，組織として管理できないツールも存在する．そこで，以下のようなフローで企業内のセキュリティを管理し，企業間でセキュリティ状況を共有する．

まず，委託元はウイルス対策ソフトに対する定義をセキュリティ基準の項目に明記し，委託先に提示する．委託先の管理者は，定期的に収集しているクライアント情報を元に委託先の基準を満たしているか判定する．判定に必要となるのは，チェックリストの XCCDF，チェックを実施する OVAL インタプリタ，ウイルス対策ソフトウェアを一意に識別する CPE となる．また，環境によって Windows レジストリ情報の取得や定義ファイル更新情報の取得も必要となる．そして，セキュリティ基準に対するチェック結果の 1 項目として，委託先に結果を報告する．再委託先が存在する場合は，委託先と再委託先で同様のフローを実施し，委託先が最終的に取りまとめて委託元へ回答する．

また，上記フローにより既存研究と同様に脆弱性管理とパッチ管理も可能になるが，本稿では詳細を省略する．

(B) 禁止ソフトウェアの確認

企業ではユーザに使用を禁止しているソフトウェアを定義していることが多く，セキュリティ基準でも「ファイル交換ソフト等の使用禁止」などが明示される．課題として，(A)と同様にユーザの利用状況を管理できていないことが挙げられる．さらに，企業間でバラバラな用語(winny/Winny/ウィニー等)で管理されていることがある．そこで，CPE を利用して統一された定義，「cpe:/a:isamu_kaneko:winny:2.0b7.1」として禁止ソフトウェアを管理することができる．

禁止ソフトウェア確認のフローは以下の通りである．委託元は，使用禁止すべきソフトウェアの CPE リストとチェックリスト XCCDF を提示する．委託先は受け取ったチェックリストを OVAL インタプリタでチェックし，結果を取りまとめてセキュリティ基準のチェック結果の 1 項目とする．

また，企業内でソフトウェアの使用可否を管理する場合は，禁止ソフトウェア一覧といったブラックリストではなく、利用可能なソフトウェア一覧を利用したホワイトリストで管理することもある．その場合も CPE リストで管理することで，明確に管理することができる．ホワイトリストの場合，企業でよく利用するソフトウェアの多くが既に CPE リストに記載されているので、新規に作成する必要もなく管理が容易になる利点もある．

同様に，利用ソフトウェアとバージョンが明確になるため，社内のライセンス管理も可能になり，企業コンプライアンスの向上につながる．

(C) パスワード強度

「パスワードを定期的に変更する」や「パスワードの強度が適切になっている」といったパスワードポリシーの項目を評価する．課題として，定期的とはどれくらいの期間か，何文字ならば強度があるといえるのかという基準が企業間で統一されていないことが挙げられる．

CCE ID(v5)における Windows7 の項目では，CCE-9357-5(最小パスワード長)，CCE-9193-4(パスワード期間)，CCE-9370-8(パスワードの複雑であるかどうか)が定義されており，パスワードポリシーを定量化することができる．そのため，これまでのフローと同様にチェックリスト(XCCDF)とチェック(OVAL)により，定量的に評価することができる．

7 考察

7.1 情報収集・格納

7.1.1. データ形式について

利用したデータは標準規格として公開されているため，それぞれのパーサを作成して情報を格納することが容易にできた．しかし，形式が変更になると更新される可能性があり，現状でも NVD/CVE はバージョン 1.2 と 2.0 のデータが存在しており，CPE も最近 2.2 から 2.3 へ更新され評価期間で 2 つのパーサを実装する結果となった．バージョンが変更になる場合，各バージョンのパース処理、バージョン間での整合性やシステムが格納しているデータ移行などの運用コストが生じる．

7.1.2. データストアの拡張性について

今回利用したデータストアの 1 つである全文検索サーバはドキュメント指向データベースとして柔軟性や拡張性を持つが，今回評価したデータサイズやバージョン毎の形式変更に関して，RDBMS に対する優位性は特に確認できなかった．しかし，大企業では管理ユーザ数や取引企業数も多く，ISCM に関する 11 の領域を管理する場合には，ビックデータとなりスケール性が必須となると考えられる．一方，ICT チェーンの大部分を構成する中小企業は大きなデータを保持しないため，利用形態を考慮して両データストアを選択すると良いと考える．

7.2 分析シナリオ

7.2.1. 標準規格の利用

標準仕様を利用することで，情報セキュリティ基準を企業間で同一の指標により評価することができた．また，ベンダー依存の仕様ではないため，企業毎に利用する製品を選択することが可能であり，委託元に合わせて新たな製品購入する必要もない．また，クラウドサービスの普及により DaaS に移行する企業も増えており，DaaS のみで一括管理できる可能性もあるが，現実的には完全に移行することは難しく，さらにスマートフォンやタブ

レットなどの新たな業務端末も増加していることから，環境に依存せず統一的に評価できる標準規格の利用が望ましい．

7.2.2. 管理情報の更新

XCCDF や CPE はすべてのチェック項目や製品情報を網羅しているわけでなく，今後も増加するチェック項目や新製品に対して継続的に更新する必要が生じる．しかし，企業で良く利用される製品の多くは登録・更新がされており，追加で対応する数は限定されている．標準規格の利用が広がると各企業で共有でき，運用コストは下げられると考える．

7.2.3. 企業間で共有する内容について

今回の評価ではチェックリストの配布と結果の回答を企業間で共有する前提にしたが，企業関係によっては自社のセキュリティ基準を他社に公開したくないこともある．その場合，チェック項目とチェック結果の詳細を企業間で秘密にしたままチェック結果の妥当性を判断できる仕組みが必要になると考える．

8 まとめ

本稿では， ICT チェーンを構成する企業間で情報セキュリティ基準を共有して評価可能にする情報セキュリティアーキテクチャを提案した．提案アーキテクチャでは，情報セキュリティ標準規格を適用することで企業間の情報セキュリティ基準の指標値を統一化し，企業間でセキュリティ情報の共有や分析の自動化・継続的モニタリングする方式を提案し，その機能要素を評価した．

提案アーキテクチャにより，日々増加する IT 機器や脆弱性などのセキュリティ情報に対する分析を自動化し，システム管理者の負荷を軽減させることができる．さらに，自組織の情報セキュリティを守る従来の対策から，ICT チェーン全体の情報セキュリティ対策を可能とする．その結果，社会全体における情報セキュリティ水準の向上に貢献できると考える．

9 今後の課題

アーキテクチャのプロトタイプを発展させていく．また，今回対象としていなかった ISCM の自動化領域への適用拡大も検討する(図 8).

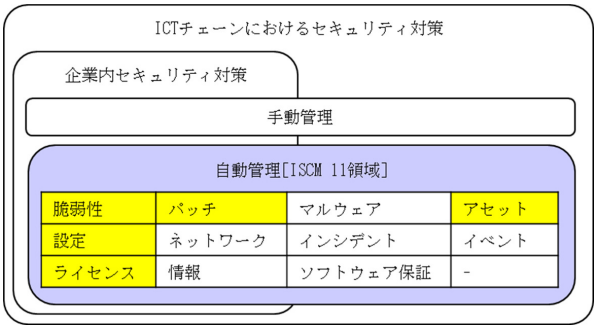

図 8 適用可能範囲

参考文献

[1] 独立行政法人情報処理推進機構, "「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第 2 版", Nov.2012

[2] 独立行政法人情報処理推進機構, "「標的型メール攻撃」対策に向けたシステム設計ガイド", Aug.2013

[3] Symantec, "INTERNET SECURITY THREAT REPORT",2011 Trends Volume 18 Published April 2013

[4] National Institute of Standards and Technology, "The Technical Specification for the Security Content Automation Protocol (SCAP):SCAP Version 1.2", Special Publication 800-126 Rev.2

[5] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G.Schudel, M. Hird, and S. Adegbite, "CYBEX — The Cybersecurity Information Exchange Framework (X.1500)",ACM SIGCOMM Computer Communication Review,vol.40 no.5, pp.59-64, Oct. 2010

[6] National Institute of Standards and Technology, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Special Publication 800-137"

[7] Alexander Kott,Curtis Arnold,"Challenges of Continuous Monitoring and Risk Scoring", IEEE Security and Privacy, Vol.11 No.1, pp.90–93, 2013.

[8] National Institute of Standards and Technology, "The United States Government Configuration Baseline(USGCB) "

[9] 寺田真敏，斉藤良彰，大森雅司，相馬基邦，小林偉昭, "MyJVN バージョンを用いた脆弱性対策自動化の実現", CSEC,vol.2011-CSEC-54, no.33 pp.1-6 , Jul.2011

[10] 独立行政法人情報処理推進機構,MyJVN, http://jvndb.jvn.jp/apis/myjvn/

[11] 中村章人, "標準プロトコルと公開コンテンツに基づくマルチプラットフォーム脆弱性管理システム", 信学技報, Vol.110 No.374, pp.105-110, Jan.2011.

[12] 藤堂洋介,朝倉康生,森井昌克, "既存脆弱性情報を利用したクライアント向け脆弱性検査システムの提案と評価"

[13] 岡城純孝，松田勝志，小川隆一, "セキュリティ運用管理における機器設定統合分析システム", 情報処理学会研究報告. CSEC, 2005(33), pp.303-308

[14] パナソニック株式会社,"お取引先様向け情報セキュリティ基準 Ver. 2.0",Oct 2012