高度サイバー攻撃対処のための
リスク評価等のガイドライン
付属書

平成 28 年 10 月 7 日

内閣官房内閣サイバーセキュリティセンター

目次

付属書１　実施要領

１　本取組の流れ

政府機関等における高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 28 年 10 月７日サイバーセキュリティ対策推進会議決定。以下「ガイドライン」という。）に基づく取組（以下「本取組」という。）の流れを図１及び以下の①から⑮に示す。

本取組では、リスク評価等の実施に向けた準備（①から②）を行った上で、リスク評価ワークシートを用いてリスク評価（③から⑧）及び対策導入計画（案）の作成等(⑨から⑫)を実施することとなる。また、リスク評価結果及び対策導入計画の案の内容については、リスク評価ダッシュボードとして取りまとめ(⑬)、CISO による方針決定(⑭)を行い、所定の事項をNISC へ報告(⑮)することとなる。

本付属書の２以降では、それら本取組の各段階に応じた実施要領を示す。

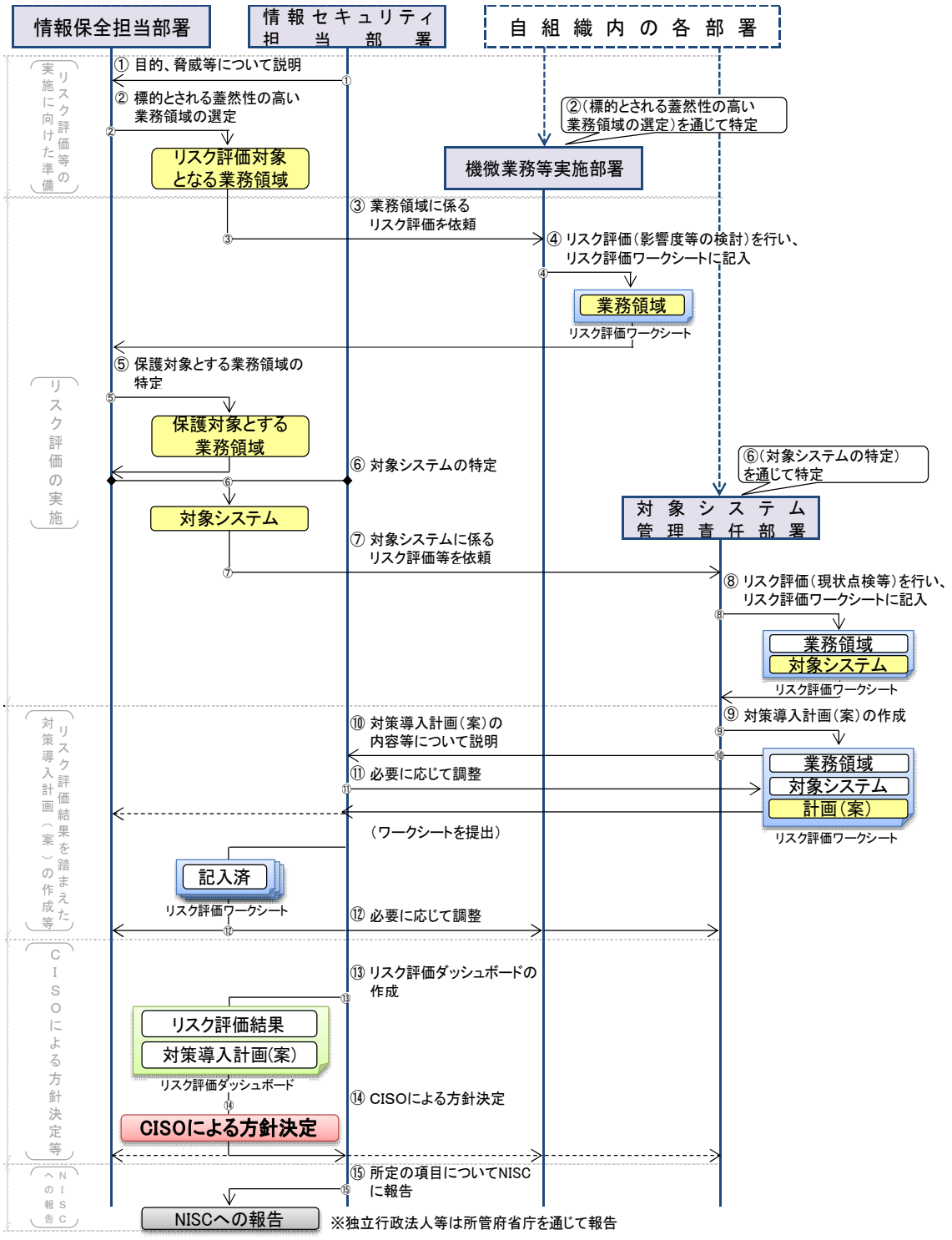


図　1　本取組の流れ

①　情報セキュリティ担当部署は、情報保全担当部署に対して、現在の情報セキュリティ上の脅威等について情報提供するとともに、本取組の目

的、実施プロセス等を説明し、認識を共有する。（ガイドライン第２部２(1)ア）

② 情報保全担当部署は、本取組におけるリスク評価の対象とする「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を、ガイドラインの選定要領に従い、自組織において最適な方法により選定する。（ガイドライン第２部２(1)イ）

③ 情報保全担当部署は、機微業務等実施部署に対して、業務領域に係るリスク評価を依頼する。（ガイドライン第２部２(2)ア）

④ 機微業務等実施部署は、高度サイバー攻撃事案が発生した場合における組織・業務への影響度等について検討を行い、その結果をリスク評価ワークシートに記入する。（ガイドライン第２部２(2)ア）

⑤ 情報保全担当部署は、機微業務等実施部署における検討結果に応じて、②で選定した業務領域の全部又は一部を本取組における「保護対象とする業務領域」として特定する。（ガイドライン第２部２(2)ア）

⑥ 情報保全担当部署又は情報セキュリティ担当部署は、ガイドラインの条件に該当する情報システムを対象システムとして特定する。（ガイドライン第２部２(2)イ(ｱ)）

⑦ 情報セキュリティ担当部署は、特定した対象システムの対象システム管理責任部署に対して、当該情報システムに係るリスク評価等を依頼する。（ガイドライン第２部２(2)イ(ｲ)）

⑧ 対象システム管理責任部署は、対象システムの対策実施状況を点検するとともに、現在の対策実施状況における残存リスクを把握し、これらをリスク評価ワークシートに記入する。（ガイドライン第２部２(2)イ(ｲ)）

⑨ 対象システム管理責任部署は、対象システムに導入すべき対策及びその導入時期について検討を行い、付属書において設定されている統制目標を達成するための対策導入計画の案を作成し、リスク評価ワークシートに記入する。（ガイドライン第２部２(3)ア）

⑩　対象システム管理責任部署は、対象システムに係るリスク評価結果及び対策導入計画（案）、対策導入に伴うユーザ側への影響等がある場合は、その内容等について、当該システムのユーザ側である機微業務等実施部署に説明を行う。（ガイドライン第２部２(3)イ）

⑪　機微業務等実施部署は、必要に応じて、対象システム管理責任部署と対策導入計画（案）の修正等に係る調整を実施する。（ガイドライン第２部２(3)イ）

⑫　情報セキュリティ担当部署は、複数の対策導入計画（案）の間での調整の要否を確認し、必要に応じて、関係部署との調整を実施した上で、CISOに承認を求めるための対策導入計画の案として確定させる。（ガイドライン第２部２(3)イ）

⑬　情報セキュリティ担当部署は、リスク評価ダッシュボードを作成する。（ガイドライン第２部２(4)ア）

⑭　情報セキュリティ担当部署は、CISOにリスク評価結果について報告するとともに、対策導入計画の承認を求め、CISOは、残存リスク等を把握した上で、承認を求められた対策導入計画の実行方針を承認・決定し、又は再検討・修正を関係部署に指示する。（ガイドライン第２部２(4)イ）

⑮　府省庁の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について、第３部の３に掲げるものをNISCに報告する。独立行政法人等の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について所管府省庁に報告し、府省庁は、所管する独立行政法人等の報告をとりまとめて、第３部の３に掲げるものをNISCに報告する。（ガイドライン第２部２(5)）

２　リスク評価の実施要領

(1)　保護対象とする業務領域の特定

「保護対象とする業務領域の特定」は、リスク評価等の実施に向けた準備において情報保全担当部署が選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」について、機微業務等実施部署がリスク評価(高度サイバー攻撃事案が発生した場合における組織・業務への影響度等の検討)を行い、情報保全担当部署がその結果に応じて保護対象とする業務領域を特定することにより実施する。

機微業務等実施部署によるリスク評価結果等については、リスク評価ワークシートの「リスク評価対象とする業務領域に係る記入シート」（図２参照）に以下の①から⑦のとおり記入する。

情報保全担当部署による保護対象とする業務領域の特定は、機微業務等実施部署によるリスク評価結果（「脅威事象の発生確率」及び「組織・業務への総合影響度」）を踏まえた個別の判断によって行う。

なお、「脅威事象の発生確率」が「低」と評価された業務領域については、一律的に保護対象としないこととしてもよい。

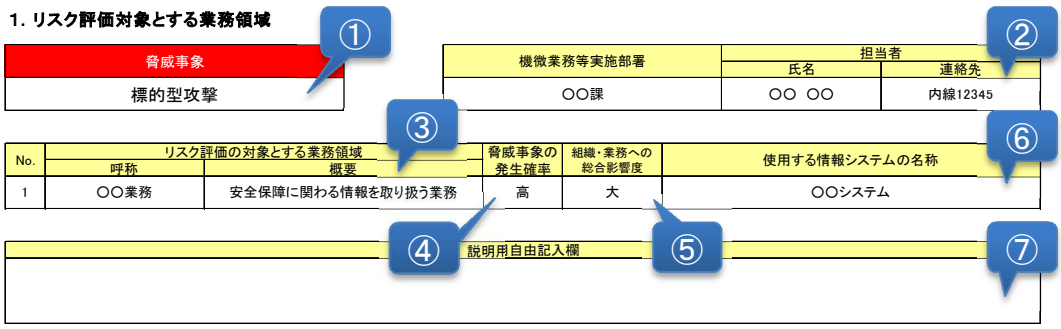


図　２　リスク評価対象とする業務領域に係る記入シート

①　本取組におけるリスク評価で想定する脅威事象(高度サイバー攻撃の種別)を記入する。現状においては「標的型攻撃」と記入する。

②　機微業務等実施部署の名称並びに担当者の氏名及び連絡先を記入する。

③　リスク評価の対象としている業務領域の呼称及びその概要を記入する。

業務領域の呼称は、当該業務領域の性質を端的に表す便宜的なもので差し支えない。また、業務領域の概要は、CISO がその重要性を容易

に認識できる粒度となるよう、当該業務領域の業務の関係者以外の者であっても、その特性を認識できる程度の粒度で簡潔に記載する。

④　脅威事象の発生確率について検討を行い、その結果を記入する。

本取組における脅威事象の発生確率については、「機微業務領域」又は「その特性等に照らして高度サイバー攻撃の標的となる蓋然性が高いと考えられる業務領域」である場合（ガイドラインの選定要領①によって選定された業務領域である場合）は「高」と、「それ以外の業務領域」である場合（ガイドラインの選定要領②によって選定された業務領域である場合）は「中」とすることを標準とする。ただし、機微業務等実施部署における判断として、これと異なる評価を行うことは妨げない。また、機微業務等実施部署において、情報保全担当部署が選定した業務領域が「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」に当たらないと判断された場合は、発生確率を「低」とする。

⑤　高度サイバー攻撃事案が発生した場合における組織・業務への総合影響度について検討を行い、その結果を記入する。

当該影響度の判定に当たっては、脅威事象が発生した際に、組織や業務に対する著しい影響が想定される事項について、表１の「影響タイプと負の影響」の項目から、顕著な影響が想定されるものを選択し、表２のとおり確定する。

表　１　影響のタイプと負の影響

影響のタイプ	負の影響
国家にもたらされる被害	①国家の目的を果たすための現行の、あるいは将来にわたる能力が損なわれる。
	②政府の運用継続性の喪失
	③他国・国際機関等との信頼関係が損なわれる。
	④他国・国際機関等との交渉上の不利益が生じる。
	⑤極めて重要なインフラ部門に対する損害、あるいはその能力が奪われる。
個人にもたらされる被害	①人命に対する危害、又は人命の損失
	②身体的又は精神的な虐待
	③個人情報の喪失
	④個人のイメージ又は評判が損なわれる。
自組織の業務にもたらされる被害	①現行、あるいは将来にわたって、ミッション又は業務機能を実施できない。
	②直接的な金銭上のコスト（賠償等）が発生する。
	③自組織における他の組織との信頼関係が損なわれる。
	④自組織のイメージ又は評判が損なわれる。

他の組織にもたらされる被害	①直接的な金銭上のコスト（賠償等）が発生する。 ②関係組織（我が国、自組織以外）における他の組織との信頼関係が損なわれる。 ③他の組織（我が国、自組織以外）のイメージ又は評判が損なわれる。
資産にもたらされる被害	①情報資産に対する損失又はその喪失 ②情報システム又はネットワークに対する損失又はその喪失 ③知的財産の喪失

表 2　組織・業務への総合影響度の判定基準

組織・業務への総合影響度	表１における選択結果
極大	顕著な影響が想定される項目が複数あり、かつ「影響のタイプ」が複数存在する場合
大	顕著な影響が想定される項目が複数あり、かつ「影響のタイプ」が１つの場合
中	顕著な影響が想定される項目が１つの場合
小	顕著な影響が想定される項目がない場合

⑥　リスク評価の対象としている業務領域の業務を遂行する上で使用する情報システムの名称を記入する。

当該情報システムの名称は、後の「対象システムの特定」のプロセスにおいて、情報保全担当部署又は情報セキュリティ担当部署が対象システムを特定する際に用いるための情報として記入するものであり、対象システムの条件に該当するか否かは考慮しなくてよい。

⑦　③から⑥の項目に記入した内容等の説明として必要な事項を記入する。

記入事項の例としては、

- ④において標準と異なる発生確率とした場合、その理由
- ⑤における表１の項目の選択に係る理由
- ⑥において名称を記入した情報システムを業務遂行上のどのような場面で使用しているかなど、「対象システムの特定」において参考となる情報

が挙げられる。

(2)　対象システムの特定・現状点検等

「対象システムの特定」は、(1)においてリスク評価ワークシートに記入された情報を基に、情報保全担当部署又は情報セキュリティ担当部署がガイドラインの条件に該当する情報システムを特定することにより実施する。また、「対象システムの現状点検等」は、対象システムについて、対象システム管理責任部署がリスク評価（対策実施状況の点検及び残存リスクの把握）を行うことにより実施する。

対象システム管理責任部署によるリスク評価結果については、リスク評価ワークシートの「対象システムの現状点検等に係る記入シート」（図３参照）に以下の①から⑧のとおり記入する。

2. 対象システムの現状点検等

保護対象とする業務領域の呼称	対象システムの名称	対象システム管理責任部署	担当者 氏名	担当者 連絡先
○○業務	○○システム	◇◇課	◇◇ ◇◇	内線67890

統制目標		対策セット		対策要素	該当判断	実施状況	残存リスク	対策の実施が確認できる資料名（設計書、報告書、運用マニュアル等）	備考
A	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをファイアウォールで防止する	遮断 1-1	ネットワーク通信経路設計によるFWでの不正通信の遮断	FW、プロキシ	○	済		○○システム設計書	
		その他			－	－			
B	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバで遮断・発見する	遮断 1-2	プロキシサーバのアクセス制御による遠隔操作用不正通信の遮断	プロキシ	○	済		○○システム設計書	
		監視 1-1	プロキシサーバ経由の通信の強制切断による遠隔操作用不正通信の発見	プロキシ	○	済		○○システム設計書	
		その他			－	－			
C	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバの認証機能を用いて遮断・発見する	遮断 1-3	プロキシサーバの認証機能による遠隔操作用不正通信の遮断	プロキシ	○	済		○○システム設計書	
		監視 1-2	プロキシサーバの認証ログの監視と分析	プロキシ	○	済		○○システム設計書	
		その他			－	－			
D	各ネットワークセグメントの役割を分割し、異なる他のネットワークセグメントへの侵入を防止する	遮断 2-1	管理端末とユーザ端末のネットワーク分離設計	システム管理端末	○	済		○○システム設計書	
		遮断 2-2	適切なネットワークセグメント分離及びアクセス制御設計	ネットワーク	○	済		○○システム設計書	
		その他			－	－			
E	ユーザ端末や重要サーバへの侵入範囲の拡大を防止又はその兆候を発見する	遮断 2-3	ユーザ端末間のファイル共有等禁止	ユーザ端末	○	－	・ネットワークセグメント内において、侵入済端末から、ファイル共有機能を利用して他の端末等へ侵入される ・高い権限が必要となる認証サーバやファイルサーバ等に対して、さらなる侵入や情報窃取が行われた場合に検知できない		
		監視 2-1	トラップアカウントによる認証ログの監視と分析	認証サーバ、ユーザ端末	○	－			
		その他			－	－			
F	端末に保存するアカウントの権限を最小化し、管理者権限等の高い権限の窃取を防止する	遮断 2-4	高い管理者権限アカウントキャッシュ禁止	ユーザ端末、システム管理端末	○	－	・高い権限が必要となる認証サーバやファイルサーバ等に対して、さらなる侵入や情報窃取が行われる		
		その他			－	－			

対策セットの個別評価に係る説明用自由記入欄

対策実施状況								保護対象の業務領域に係る対象システムのリスク評価結果
統制目標	A	B	C	D	E	F	対策実施総数	
対策セットの対策	○	◎	◎	◎	×	×	7	
対策セット以外の対策	無	無	無	無	無	無	0	

図　３　対象システムの現状点検等に係る記入シート

① (1)において機微業務等実施部署が記入した「保護対象とする業務領域(リスク評価対象する業務領域)の呼称」を転記する。

なお、同一の対象システムにおいて複数の「保護対象とする業務領域」が特定されている場合は、記入欄を追加し、全ての「保護対象とする業務領域の呼称」を転記する。この場合において、「対象システムの現状点検等に係る記入シート」は単一のものを作成し、それぞれのリスク評価ワークシートに複写すればよい。

② 対象システム及び対象システム管理責任部署の名称並びに担当者の氏名及び連絡先を記入する。

なお、③において、ガイドライン第２部２(2)イ(ｲ)のなお書きに該当した場合は、記入欄を追加し、他の対象システム及び当該情報システムの対象システム管理責任部署についても同様に記入する。この場合において、「対象システム管理責任部署」に係る以降の実施事項は、情報システムの運用管理に係る責任分界等も踏まえ、当事者間の合意に基づく役割分担によって実施すればよい。

③ 対策セットの対策ごとに、対象システムが対策要素を有しているか否かを確認し、該当がある項目に「○」を記入する。

なお、ガイドライン第２部２(2)イ(ｲ)のなお書きに該当する場合は、どの対象システムが当該対策要素を有しているか判別できるよう、備考欄に該当する対象システムの名称を記入する。

④ 対策セットの対策ごとに、当該対策を実施しているか否かを確認し、実施しているものについて「実施状況」欄に「済」を記入する。また、対策セットの対策と同一の統制目標に係る対策を自組織で独自に実施している場合は、統制目標ごとに、その内容について「その他」欄に記入するとともに「実施状況」欄に「済」を記入する。

⑤ 対策を実施していない統制目標（④において「実施状況」欄に「済」と記入した対策がない統制目標）に係る残存リスクについて、脅威事象としているサイバー攻撃のシナリオ等を勘案して把握し、その結果を記入する。

⑥ ④において対策の実施状況を確認する際に使用した資料の名称等を記入する。

⑦　②から⑥の項目に記入した内容等の説明として必要な事項を記入する。

記入事項の例としては、

・　複数の対象システム管理責任部署による現状点検等を実施した場合、その役割分担等

・　④における対策実施状況に関する情報であって、残存リスクに係るもの以外の情報

が挙げられる。

⑧　統制目標ごとの対策実施状況に関し、対策セットの対策については、対策実施数が１であれば「○」を、２以上であれば「◎」を記入し、対策セット以外の対策については、その有無を記入する。また、対策セットの対策とそれ以外の対策ごとに、その実施数を「対策実施総数」欄に記入する。さらに、⑤において把握した残存リスク全体について、機微業務等実施部署による業務領域に係るリスク評価の結果も踏まえて評価を行い、その結果を「保護対象の業務領域に係る対象システムのリスク評価結果」欄に記入する。

３　リスク評価結果を踏まえた対策導入計画（案）の作成等の要領

(1)　対象システムごとの対策導入計画（案）の作成

「対象システムごとの対策導入計画（案）の作成」は、２で実施したリスク評価の結果、対策の優先順位、予算措置の要否、システム更改時期等を踏まえ、対象システム管理責任部署が対象システムに導入すべき対策及びその導入時期について検討し、計画を立案することにより実施する。また、対策導入計画（案）は、設定されている統制目標を達成するものであることを要件（以下「計画作成上の要件」という。）として作成する。

対象システム管理責任部署が作成する対策導入計画（案）については、リスク評価ワークシートの「対策導入計画（案）に係る記入シート」（図４参照）に以下の①から⑨のとおり記入する。

3. 対策導入計画（案）

計画作成対象期間	27	年度
	～ 30	年度

保護対象とする業務領域の呼称	#REF!
対象システム	#REF!
対象システム管理責任部署	#REF!
担当者	#REF!
連絡先	#REF!

①

［3-1 対策セットの個別導入計画（案）］ ②

統制目標		対策名称		対象機器	対策実施状況／今後の実施予定								備考
					対策区分	実施済	26年度実施	27年度までに	28年度までに	29年度までに	30年度までに	31年度以降	実施しない	
A	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをファイアウォールで防止する	遮断 1-1	ネットワーク通信経路設計によるFWでの不正通信の遮断	FW、プロキシ	対策セット	◉	○	○	○	○	○	○	○	
		その他			対策セット以外	○	○	○	○	○	○	○	◉	
B	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバで遮断・発見する	遮断 1-2	プロキシサーバのアクセス制御による遠隔操作用不正通信の遮断	プロキシ	対策セット	◉	○	○	○	○	○	○	○	
		遮断 1-3	プロキシサーバの認証機能による遠隔操作用不正通信の遮断	プロキシ	対策セット	◉	○	○	○	○	○	○	○	
		その他			対策セット以外	○	○	○	○	○	○	○	◉	
C	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバの認証機能を用いて遮断・発見する	監視 1-1	プロキシサーバの認証ログの監視と分析	プロキシ	対策セット	○	◉	○	○	○	○	○	○	
		監視 1-2	プロキシサーバ経由の通信の強制切断による遠隔操作用不正通信の発見	プロキシ	対策セット	○	◉	○	○	○	○	○	○	
		その他			対策セット以外	○	○	○	○	○	○	○	◉	
D	各ネットワークセグメントの役割を分割し、異なる他のネットワークセグメントへの侵入を防止する	遮断 2-1	管理端末とユーザ端末のネットワーク分離設計	システム管理端末	対策セット	○	◉	○	○	○	○	○	○	
		遮断 2-2	適切なネットワークセグメント分離及びアクセス制御設計	ネットワーク	対策セット	○	◉	○	○	○	○	○	○	
		その他			対策セット以外	○	○	○	○	○	○	○	○	
E	ユーザ端末や重要サーバへの侵入範囲の拡大を防止又はその兆候を発見する	遮断 2-3	ユーザ端末間のファイル共有等禁止	ユーザ端末	対策セット	○	○	○	◉	○	○	○	○	
		監視 2-1	トラップアカウントによる認証ログの監視と分析	認証サーバ、ユーザ端末	対策セット	○	○	○	○	○	◉	○	○	
		その他			対策セット以外	○	○	○	○	○	○	○	◉	
F	端末に保存するアカウントの権限を最小化し、管理者権限等の高い権限の窃取を防止する	遮断 2-4	高い管理者権限アカウントキャッシュ禁止	ユーザ端末、システム管理端末	対策セット	○	○	○	○	○	○	○	◉	
		その他			対策セット以外	○	○	○	○	◉	○	○	○	

［3-2 当該システムの対策導入計画（案）］

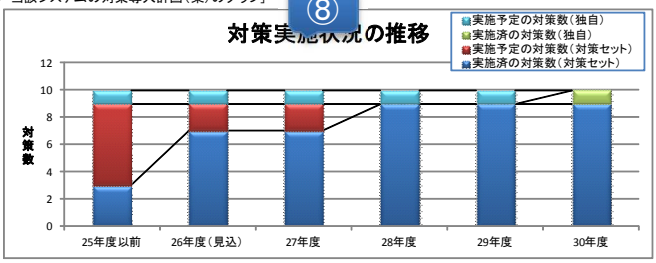
26年度の対策導入計画概要	27年度の対策導入計画概要	対象期間を通しての予算措置等
<想定運用> 前年度(例:25年度)に作成した本計画書の「対策導入計画概要(右	<想定運用> 今年度(例:26年度)以降についての計画を記載する。	<想定運用> 今年度(例:26年度)以降についての計 する。

③ ⑤ ⑥

計画の進行状況	遅延の場合の理由	30年度末における統制目標ごとの対策実施状況（予定）							
		統制目標	A	B	C	D	E	F	対策実施総数
順調	④	⑦ 対策	○	◎	◎	◎	◎	－	9
		対策セット以外の対策	無	無	無	無	無	有	1

<凡例>
◎：対策セットの対策を2つ以上実施している
○：対策セットの対策を1つ実施している
※：対策セットの対策を対象期間終了後に実施予定
－：対策セット以外の対策を実施するため対策セットの対策は実施しない
有：対策セット以外の対策を実施している
無：対策セット以外の対策を実施していない

［3-3 当該システムの対策導入計画（案）のグラフ］ ⑧



［3-4 説明用自由記入欄］

対策導入計画（案）係る説明用自由記入欄
⑨

図 4 対策導入計画（案）に係る項目の記入シート

①　「対象システムの現状点検等に係る記入シート」に記入した「保護対象とする業務領域(リスク評価対象する業務領域)の呼称」及び「対象システム及び対象システム管理責任部署の名称並びに担当者の氏名及び連絡先」を転記する。

②　該当がある対策セットの対策の実施について検討を行い、その実施予定を記入する。また、対策セットの対策と同一の統制目標に係る対策であって、対策セット以外の対策の実施を予定する、又は既に実施している場合は、当該対策の概要等及び実施予定を記入するとともに、備考欄にその説明等を記入する。

対策導入計画（案）は、作成時における年度(N年度)の次年度(N＋１年度)の当初から起算した４年間(N＋４年度末まで)を対象期間とし、当該期間において実施する対策が、既に実施済みの対策と合わせて、計画作成上の要件を満たすように作成する。また、対象期間内に実施を予定しない対策については、備考欄にその理由等を記入する。

なお、計画作成上の要件は、対策導入計画（案）の作成における必要条件であり、十分条件ではない。

③　対策導入計画（案）の作成時における年度(N年度)に係る対策の実施予定について、当該年度の前年度(N－１年度)に作成したリスク評価ワークシートから転記する。

なお、本取組の開始当初の年度であるなど、前年度にリスク評価ワークシートを作成していない場合は、空欄のままとして差し支えない。④においても同じ。

④　対策導入計画（案）の作成時における年度(N年度)に係る対策の実施について、実績を記入する。

計画どおりに対策を実施した、又はその具体的な見込みが立っている場合は「順調」と、計画どおりに対策を実施できなかった、又は実施できる具体的な見込みが立っていない場合は「遅延」と記入する。また、実績が「遅延」となった場合は、その理由についても記入する。

⑤　④で記入した実績も踏まえつつ、②で記入した対策の実施予定について、次年度の概要を記入する。

⑥　②で記入した対策の実施予定について、対象期間を通しての概要を

予算措置やそれに向けた対応状況等と併せて記入する。

⑦　②で作成した対策導入計画（案）において、対象期間の満了時に見込まれている対策実施状況に関し、統制目標ごとに、対策セットの対策については、対策実施(予定)数が１であれば「○」を、２以上であれば「◎」を記入し、対策セット以外の対策については、その有無を記入する。

⑧　対策実施状況の推移に係るグラフを作成し、貼付する。

⑨　作成した対策導入計画（案）の全体や、②から⑧の項目に記入した内容等の説明として必要な事項を記入する。

(2) 対策導入計画（案）の調整

「対策導入計画（案）の調整」は、(1)で作成した対象システムごとの対策導入計画（案）について、対象システム管理責任部署が機微業務等実施部署へ説明し、必要に応じて両者間で調整を行うとともに、情報セキュリティ担当部署が複数の対策導入計画（案）の間での調整の要否を確認し、必要に応じて関係部署と調整を行うことにより実施する。

複数の対策導入計画（案）の間での調整内容の例としては、

- 複数の対策導入計画（案）の間における優先順位
- リスク評価ダッシュボードの作成に当たり、整合を図る必要があると認められる事項

が挙げられる。

４　CISO による方針決定等に係る要領

「CISO による方針決定等」に当たっては、情報セキュリティ担当部署が、リスク評価ワークシートに基づきリスク評価結果及び対策導入計画（案）の内容を取りまとめたリスク評価ダッシュボードを作成し、当該資料を用いて CISO にリスク評価結果を報告するとともに、対策導入計画の承認を求めることにより実施する。リスク評価ダッシュボードの作成例を図５に示す。

リスク評価ダッシュボードには、リスク評価ワークシートの各項目のうち、表３に示す事項を転記する。ただし、複数のリスク評価ワークシートの内容を取りまとめる上での修正等、内容に影響を及ぼさない修正を行うことは妨げない。

また、リスク評価ダッシュボードには、CISO が方針決定を行う上で必要な情報を過不足なく記載するとともに、必要な場合は別紙を用いるなど、当該ダッシュボードの全容が容易に把握できるように配意して作成する。

なお、別紙を用いる場合においては、特に重要となる事項や要点といった概要についてダッシュボードの本紙に簡記した上で、詳細については別紙に記載がある旨を付すなど、ダッシュボードの本紙のみでも必要最低限の情報が得られるように配意する。

年　月　日

高度サイバー攻撃対処のためのリスク評価等のガイドラインに係る リスク評価ダッシュボード（平成26年度）

1 想定する脅威事象

脅威事象
標的型攻撃

2 保護対象とする業務領域

No.	保護対象とする業務領域			脅威事象の発生確率	組織・業務への総合影響度	使用する情報システムの名称
	呼称	概要	機微業務等実施部署			
1	○○業務	○○に関わる情報を取り扱う業務	○○課	高	大	Ａシステム
2	△△業務	△△に関わる情報を取り扱う業務	△△課	中	大	Ａシステム
3	□□業務	□□に関わる情報を取り扱う業務	□□課	中	極大	Ｂシステム

3 リスク評価結果

＜Aシステム＞

対策実施状況							
統制目標	A	B	C	D	E	F	対策実施総数
対策セットの対策	○	◎	◎	◎	×	×	7
対策セット以外の対策	無	無	無	無	無	無	0

＜Bシステム＞

対策実施状況							
統制目標	A	B	C	D	E	F	対策実施総数
対策セットの対策	○	◎	×	○	○	×	5
対策セット以外の対策	無	無	無	無	無	無	0

統制目標	
A	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをファイアウォールで遮断する。
B	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバで遮断・発見する。
C	不正プログラムがC&Cサーバと遠隔操作用不正通信を行うことをプロキシサーバの認証機能を用いて遮断・発見する。
D	各ネットワークセグメントの役割を分割し、異なる他のネットワークセグメントへの侵入を防止する。
E	ユーザ端末や重要サーバへの侵入範囲の拡大を防止又はその兆候を発見する。
F	端末に保存するアカウントの権限を最小化し、管理者権限等の高い権限の窃取を防止する。

＜凡例＞
◎：対策セットの対策を2つ以上実施している
○：対策セットの対策を1つ実施している
×：対策セットの対策を実施していない
ー：対策セット以外の対策を実施するため対策セットの対策は実施しない
有：対策セット以外の対策を実施している
無：対策セット以外の対策を実施していない

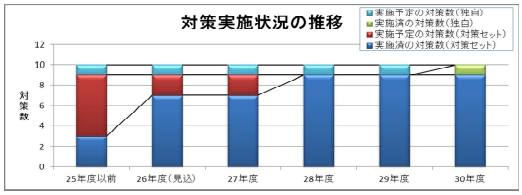
4 対策導入計画（案）

＜Aシステム＞

30年度末における統制目標ごとの対策実施状況（予定）							
統制目標	A	B	C	D	E	F	対策実施総数
対策セットの対策	○	◎	◎	◎	◎	ー	9
対策セット以外の対策	無	無	無	無	無	有	1

＜凡例＞
◎：対策セットの対策を2つ以上実施している
○：対策セットの対策を1つ実施している
※：対策セットの対策を対象期間終了後に実施予定
ー：対策セット以外の対策を実施するため対策セットの対策は実施しない
有：対策セット以外の対策を実施している
無：対策セット以外の対策を実施していない

26年度の対策導入計画概要
（前年度(例:25年度)に作成した本計画書の「対策導入計画概要(右欄)」を転記する。）



＜Bシステム＞

30年度末における統制目標ごとの対策実施状況（予定）							
統制目標	A	B	C	D	E	F	対策実施総数
対策セットの対策	○	◎	◎	◎	◎	○	10
対策セット以外の対策	無	無	無	無	無	無	0

26年度の対策導入計画概要
（前年度(例:25年度)に作成した本計画書の「対策導入計画概要(右欄)」を転記する。）

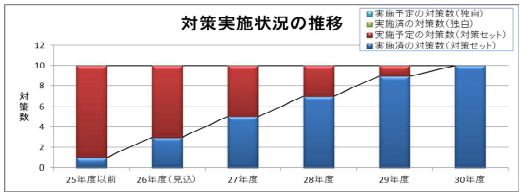


図　５　リスク評価ダッシュボードの作成例

表 3　リスク評価ダッシュボードの記載事項

項目	記載事項	備考
保護対象とする業務領域	保護対象とする業務領域の呼称	CISO が保護対象とする業務領域の把握や対象の妥当性の判断を行うために記載する。
	保護対象とする業務領域の概要	
	対象システムの名称	CISO が対象システムを把握するために記載する。
	対象システム管理責任部署の名称	
リスク評価結果	統制目標ごとの対策実施状況	CISO が対象システムの現時点での統制目標ごとの対策実施状況等を把握するために記載する。
	対策セットの対策の実施状況	
	組織･業務への影響及び残存リスク	CISO が高度サイバー攻撃により保護対象に係る被害が発生した場合における自組織・業務に生じる影響・インパクトや、残存リスクの有無等を把握するために記載する。
対策導入計画（案）	次年度の対策導入計画概要(予算措置状況を含む。)	CISO が対策導入計画（案）の妥当性の判断を行うために記載する。
	対策実施状況の推移に係るグラフ	
	対象期間終了時における統制目標ごとの対策実施状況（予定）	

付属書２　標的型攻撃への対処のための対策セット

１　標的型攻撃の概要

標的型攻撃とは、政府機関等において機微な業務・情報を扱う特定の組織に対し、攻撃手段として電子メールに添付した不正プログラム等によって職員の端末に侵入を図るなど、組織的・持続的な意図をもって行われる外部からの情報窃取・破壊等の攻撃を指す。本付属書では、このような攻撃に対する対策を示す。

標的型攻撃の特徴として、最近では国家や企業の機密情報を窃取しようとするものや、重要なデータやシステムを破壊しようとするものが顕在化してきている。我が国においても、府省庁、防衛産業、重要インフラ事業者、研究機関等から機密情報や技術情報等を窃取することが目的とみられる事案が発生している。また海外においては、軍事行動と連携した標的型攻撃が現実味を帯びてきている。多くの国家がサイバー空間における攻撃能力を開発しているとされており、情報収集のために他国の情報通信ネットワークへの侵入が行われていると指摘されている。

こうした標的型攻撃によって、政府機関等の重要な情報が窃取又は破壊された場合、当該組織や業務のみならず、我が国の安全、国民の生命・身体・財産等に大きな影響を及ぼす可能性があるため、当該攻撃を重大な脅威と認識することが必要である。

また、標的型攻撃は標的とする組織に気付かれないよう行うものであることから、当該組織がその攻撃や被害そのものを認知していない、又は攻撃による被害であることを認知できていない場合も多く、例えば、被害が発覚した時点で既に数年前から情報が窃取されていたという事案も存在している。

そのため、現在被害が明らかとなっている事案は氷山の一角であり、国家や組織の存続にも関わる重要な情報が今もなお窃取され続けている可能性があるとの考えに立ち、これに対処する必要がある。

標的型攻撃の初期段階において多く使われる手段として、電子メールを利用した攻撃手法（以下「標的型メール攻撃」という。）がある。さらに近年では、標的組織がよく閲覧するウェブサイトを改ざんし、閲覧した端末を不正プログラムに感染させる攻撃手法（以下「水飲み場型攻撃」という。）も用いられている。

標的型メール攻撃には、電子メールの添付ファイルに不正プログラムが含まれているものや、不正プログラムが含まれたウェブサーバの URL のリンクが本文中に記載されているもの等がある。これらの添付ファイルを開

いたり、URL のリンクをクリックしたりしてしまうと、当該メール受信者の端末は不正プログラムに感染してしまう。水飲み場型攻撃では、不正プログラムに感染させるためにウェブブラウザの未知の脆弱性を悪用し、標的以外の組織が閲覧しても攻撃が行われない場合もあるため、未然防止や発見が困難な傾向にある。このような手法を用いて、ファイアウォール（以下「FW」という。）やメールゲートウェイ等のインターネットとの境界に設置されたセキュリティ対策装置等を回避・突破しつつ端末を不正プログラムに感染させることで、外部の攻撃者は C&C サーバ[1]からの遠隔操作を目的とした不正な通信経路（以下「遠隔操作用不正通信経路」という。）を確立する。

標的型攻撃の本質は、攻撃者が前述の遠隔操作用不正通信経路を利用して、標的組織の情報システム内部に侵入し、そこからハッキング技術を用いて侵入範囲を拡大する行為である。つまり、攻撃者の操作により情報システム内部への侵入（攻撃者の内部活動）範囲が拡大していくという認識を持つことが重要である（図　6 参照）。

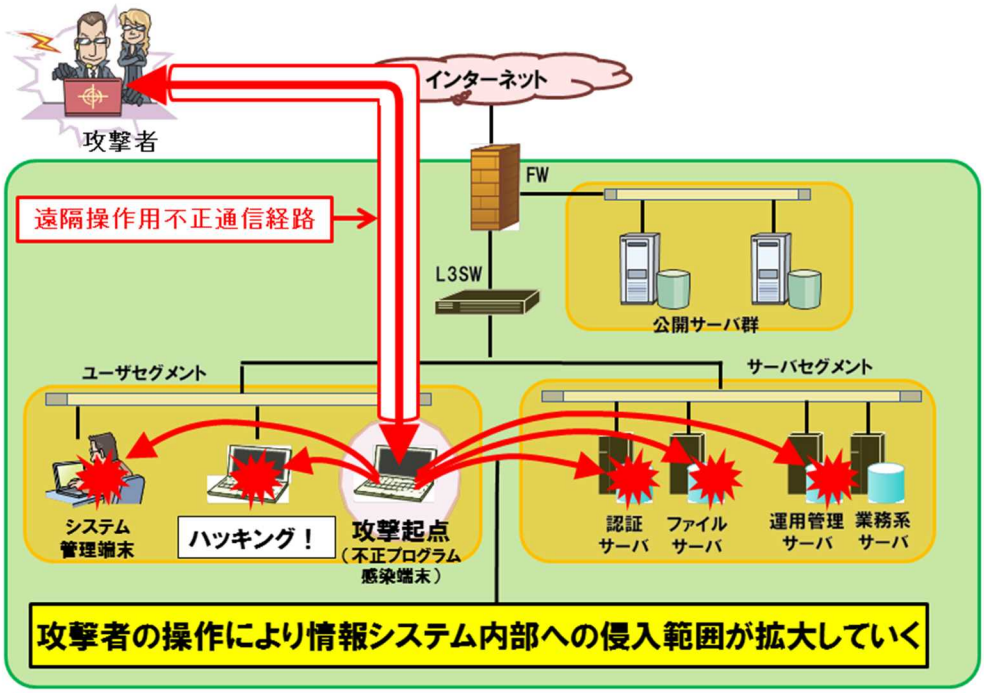


図　6　標的型攻撃による内部侵入範囲の拡大のイメージ

[1] C&C サーバ：Command & Control サーバの略。不正プログラムに感染したコンピュータ群に攻撃指令（command）を送り、制御（control）の中心となるサーバのこと。

２　攻撃手法

標的型攻撃の全体イメージを図　７に示す。この標的型攻撃手法の基本パターン（以下「攻撃シナリオ」という。）及び全体イメージは、以下のプロセスを経て作成した。

- 産学官の様々な分野の情報セキュリティ専門家（ペネトレーションテスター、デジタルフォレンジック[2]技術者、システム設計者、ネットワーク設計者、システム運用管理者、アンチウイルス調査技術者等）の知見やノウハウにより、起こり得る攻撃手法を導出。
- 官民の標的型攻撃事案（初期潜入段階以降の攻撃手法等）の実態について当該攻撃を確認した組織等に対してヒアリング調査を行うことで前述の攻撃手法との差異を確認。
- 標的型攻撃における攻撃パターンや攻撃される機器、攻撃に利用される情報等に、ある程度共通的な特徴があることを踏まえ、どの機器に対してどのような攻撃が行われると、各攻撃段階においてどのような攻撃目標が達成されるのかという観点で整理。

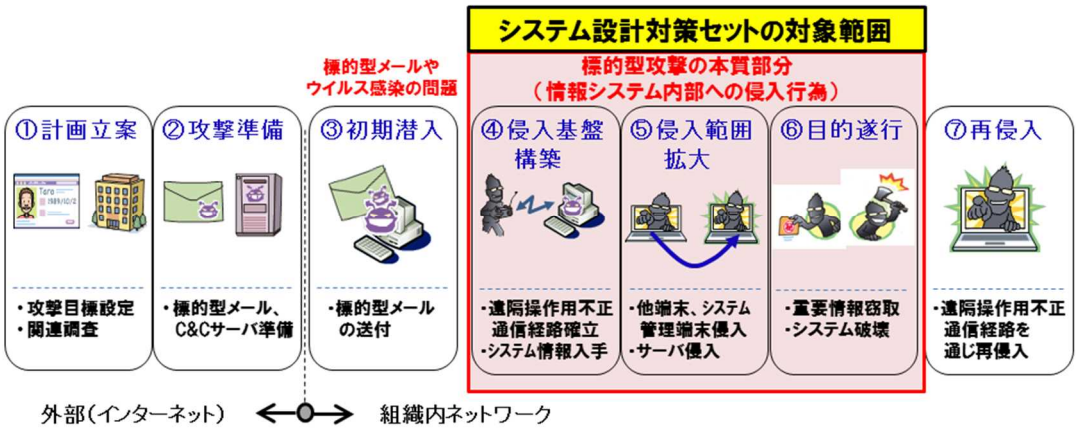


図　７　標的型攻撃の全体イメージ

各攻撃段階の概要を表　４に示す。標的型攻撃は、標的の組織に対する攻撃全体が計画的に行われる。

[2] デジタルフォレンジック：不正アクセスや機密情報漏えい等コンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。

表 4　各攻撃段階の概要

攻撃段階	攻撃概要
① 計画立案	攻撃者は、標的の組織に関する情報について、インターネットや他組織から取得した情報を基に調査する。また、攻撃者は、攻撃の最終目的を設定し、攻撃に必要となる環境等（標的型メール、改ざんされたウェブサイト、C&C サーバ、ハッキング用のツール等）を準備する。
② 攻撃準備	
③ 初期潜入	標的の組織に標的型メールを送付する、標的の組織が閲覧する可能性のあるウェブサイトを改ざんするなどして、一部の端末を不正プログラムに感染させる。
④ 侵入基盤構築	不正プログラムにより、攻撃者が遠隔操作用通信経路を確立する。攻撃者は当該経路を経由して不正プログラムに感染した端末（以下「感染端末」という。）が保持するシステム情報を窃取し、当該端末周辺のネットワーク上のシステム情報等を把握し始める。（詳細は、表 5を参照のこと。）
⑤ 侵入範囲拡大	攻撃者は各種ツールを用いて、試行錯誤しながらハッキング技術を用いた手動の攻撃を行い、他端末やシステム管理端末の乗っ取り、当該端末のシステム管理者権限等を窃取しサーバを乗っ取る。（詳細は、表 6を参照のこと。）
⑥ 目的遂行	攻撃者は攻撃の最終目的である情報システム内部の重要な情報を窃取する、又は情報システム（重要なサーバ等）を破壊する。（詳細は、表 7を参照のこと。）
⑦ 再侵入	攻撃者は過去に構築した侵入基盤を再利用し、再度標的となる組織に侵入し、攻撃を繰り返す。

また、各攻撃段階の攻撃手法等について、以下に解説する。

① 計画立案段階

表 4のとおり。

② 攻撃準備段階

表 4のとおり。

③ 初期潜入段階

表 4のとおり。

なお、本段階では、たった一つでも情報システム内部の端末をウイルス

感染させることができれば、本段階での攻撃は成功となり、次の攻撃段階に進めてしまう。標的型攻撃は、ますます巧妙化しており、全ての職員が標的型攻撃を見抜いて回避し続けることは非常に困難である。

④　侵入基盤構築段階

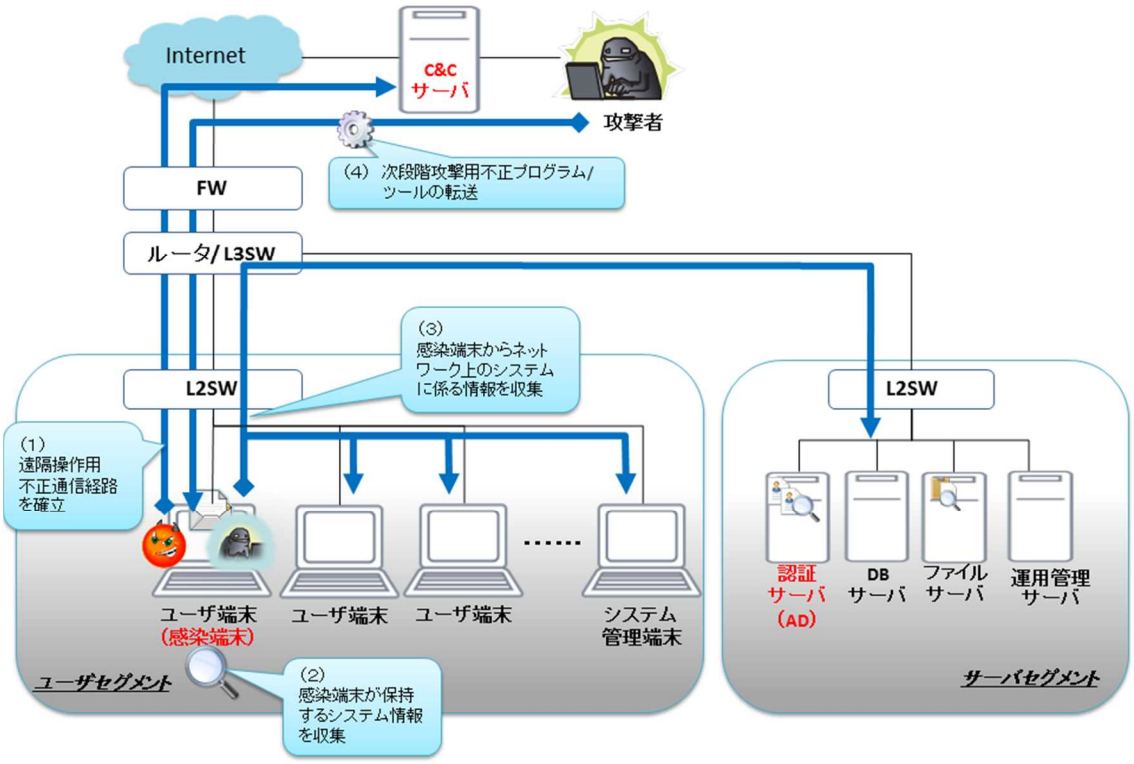


図　8　侵入基盤構築段階の攻撃イメージ

表　5　侵入基盤構築段階の攻撃目的及び手法

攻撃 目的	・ 外部からの遠隔操作用不正通信経路を確立する。 ・ 感染端末を起点として、ネットワーク、システムに係る情報等を収集する。
攻撃 手法	・ 端末を不正プログラムに感染させ、C&C サーバとの遠隔操作用不正通信経路を確立する。 ・ 感染端末から、当該端末が保持するシステム情報を収集する。(例えば、ホスト名、IP アドレス、Windows ドメイン（以下「ドメイン」という。）名、OS やウェブブラウザのバージョン、パッチ適用状況、ウイルス対策ソフトに係る情報等) ・ 感染端末からネットワーク上のシステムに係る情報を収集する。(例えば、認証サーバ、ファイル共有やリモートアクセス可能なサーバ等を探索する。) ・ 攻撃者は感染端末に次の攻撃段階用の不正プログラムや攻撃ツールを転送

	する。
攻撃の特徴	・ 遠隔操作用不正通信は、情報システムのネットワーク設計ルールに従った正規の通信（HTTP、HTTPS 等）として行われることも多いため、不正な通信として検知することが難しい。

⑤ 侵入範囲拡大段階

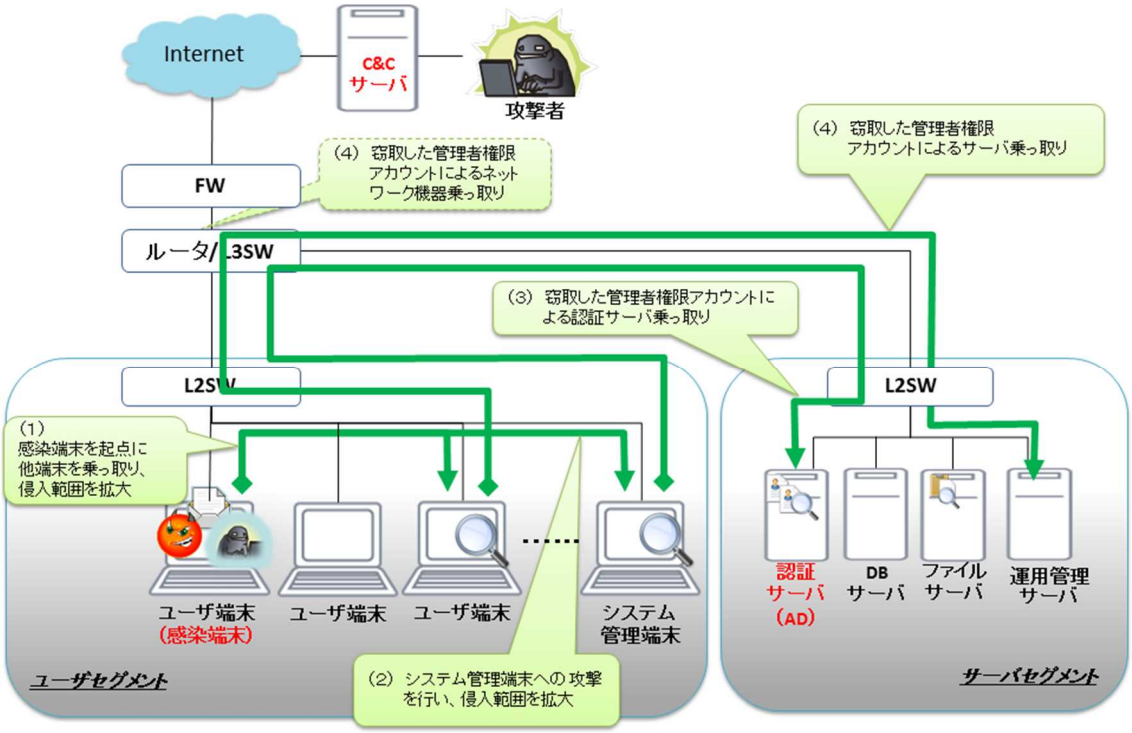


図 9 侵入範囲拡大段階の攻撃イメージ

表 6 侵入範囲拡大段階の攻撃目的及び手法

攻撃目的	・ 他端末やサーバの管理者権限アカウント等を窃取しながら、侵入範囲を拡大する。
攻撃手法	・ 他端末を乗っ取り、侵入範囲を拡大する。他端末への攻撃手法としては、例えば、次のようなものが考えられる。 – 感染端末から管理者権限アカウント等を窃取する。 – ファイル共有や管理共有を悪用し、他端末へ攻撃ツールや不正プログラムを配布し、実行する。 – ハッキングツール等を利用して他端末の脆弱性を突いて攻撃を行う。 ・ システム管理端末への攻撃を行い、侵入範囲を拡大する。他端末への攻撃と同様の手法により、管理者権限アカウント等を窃取する。 ・ 感染端末や他端末等のユーザ端末又はシステム管理端末から窃取した管理

	者権限アカウントを使い、認証サーバ（Active Directory サーバ等）を乗っ取る。 ・ 感染端末や他端末等のユーザ端末、システム管理端末、認証サーバ等から窃取した管理者権限アカウントを使い、ファイルサーバ、運用管理サーバ、ネットワーク機器等を乗っ取る。
攻撃の特徴	・ 攻撃者は、他端末への攻撃を行うことで、外部から遠隔操作可能な端末を複数台確保し、拠点又は指令用端末、基盤拡大用端末、潜伏用端末、情報収集用端末、情報送信用端末等の役割分担を有した基盤の拡大を行う。このように侵入基盤が拡大し、役割をもって分散することにより、攻撃の全容が分かりづらくなるとともに、標的の組織側が全ての攻撃端末を検出・除去することを難しくする。 ・ 攻撃順序としては、まず感染端末と同一セグメント内の端末を、次に認証サーバ、ファイルサーバ、運用管理サーバ、ネットワーク機器等を狙い、次第に侵入範囲を拡大していく。

⑥　目的遂行段階

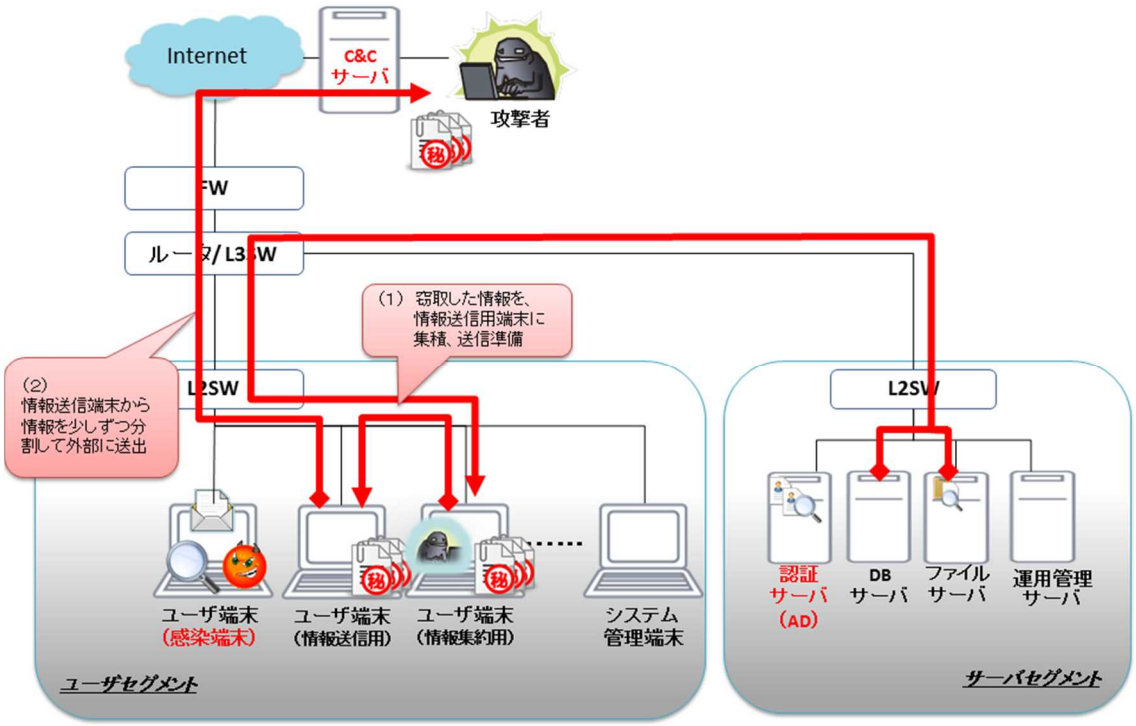


図　１０　目的遂行段階の攻撃イメージ

表 7　目的遂行段階の攻撃目的及び手法

攻撃目的	・ 乗っ取ったサーバや端末から重要な情報（機密情報等）を窃取する、又は情報システム（重要サーバ等）を破壊する。
攻撃手法	・ 乗っ取ったサーバや端末から窃取した重要な情報を、情報送信用端末に集積し、ファイルの圧縮・分割等の送信準備を行う。 ・ 複数の情報送信端末から遠隔操作用不正通信経路を経由して、当該情報等を少しずつ分割して外部に送出する。

⑦　再侵入段階

この段階では、攻撃者は標的組織の情報システムに確保した遠隔操作用不正通信経路を再利用して、継続的に再侵入し、情報システム内部を探索することが考えられる。また、新たな拠点端末との遠隔操作用不正通信経路を確立するために、当該組織に対して、標的型メールの送信も継続することが考えられる。

上記を踏まえると、攻撃者が目的を達成したとしても、攻撃が終結したかどうかを客観的に判断することが困難な場合も想定されるため、一度標的となった組織は、情報システム運用において、遠隔操作用不正通信経路が設置されていないかどうかを継続的に監視することが重要である。

３　システム設計対策の基本的な考え方

従来、情報システムのセキュリティに関する設計対策では、情報システム内部への攻撃者の侵入を防止することを前提とした対策（以下「入口対策」という。）が行われていた。しかしながら、攻撃者は、入口対策に用いられる製品等を事前に調査し、当該対策を回避・突破できることを確認した上で攻撃してくることが想定される。このことから、標的型攻撃は、FWやメールゲートウェイ等の入口対策を回避・突破して内部に侵入することを前提としたシステム設計対策を行う必要がある。

また、標的型攻撃を回避し、不正プログラムに感染しないように対策を行うことは必要であるが、標的型攻撃が巧妙化する中で、組織の職員全員が不正プログラムへの感染を回避し続けることは困難である。

したがって、組織の端末は、常に不正プログラムに感染する可能性があるという前提に立ち、攻撃者の最終目的（重要な情報の窃取や重要なサーバ等情報システムの破壊）を達成させないように、その前段階で攻撃に対処することが重要である。

情報システム内部への全ての攻撃を完全に防御し、遮断することを可能とするような対策があればそれを実施すればよいが、残念ながらそのような対策は現在存在しない。そのため、表 ８のとおり、ハッキング技術を用いた情報システム内部への一連の攻撃手法を防御・遮断する対策（以下「防御遮断策」という。）と、その攻撃の兆候を早期に検知したり、ログを定期的に監視し攻撃の痕跡を見つけ出したりすることにより、情報システム内部で攻撃が行われていることを早期に把握し対処する対策（以下「監視強化策」という。）を組み合わせて実施する必要がある。

なお、標的型攻撃への対策が十分実施できているかどうかは、単に対策の実施数で判断するのではなく、標的型攻撃を統制するために有効と考えられる目標（以下「統制目標」という。）を設定したうえで、防御遮断策・監視強化策の実施による各統制目標の達成状況によって判断する。

表 ８　システム設計対策の分類、対策目的及び対策方針

分類	対策目的	対策方針
防御遮断策	情報システム内部への攻撃を遮断し、侵入範囲の拡大を防止する	・ 遠隔操作用不正通信経路を確立しにくいシステム設計 ・ 攻撃者にとってハッキング技術を用いた内部探索（パスワード窃取等）がしにくいシステム設計 ・ 攻撃者にとって内部侵入範囲を拡大（機器乗っ取

		り等）しにくいネットワーク、システム設計
監視強化策	情報システム内部での攻撃の兆候を監視し、早期に発見・検知する	・ 攻撃（主に攻撃失敗）の痕跡を残すシステム設計 ・ 攻撃者の侵入を発見・検知するためのトラップ（罠）の設置 ・ 上記の継続的な監視

入口対策については、攻撃者を情報システム内部に極力侵入させないためにも必要な対策であり、全情報システムで実施する必要があるが、本付属書は情報システム内部の対策を対象としていることから扱っていない。入口対策等については、政府機関等の情報セキュリティ対策のための統一基準群を参照のこと。

４　対策セット

標的型攻撃手法に対応する対策セット（以下「対策セット」という。）は、産学官の様々な分野の情報セキュリティ専門家が、導出された攻撃シナリオに対する対策として防御遮断策及び監視強化策を発案し、現実に近いシステム構成上で、攻撃シナリオに基づき机上で対策の効果を検証したものである。

攻撃シナリオの各段階（侵入基盤構築、侵入範囲拡大及び目的遂行）における攻撃とそれに対応する一連の情報システムの設計、監視強化等の対策の一覧を以下に示す。

④　侵入基盤構築段階

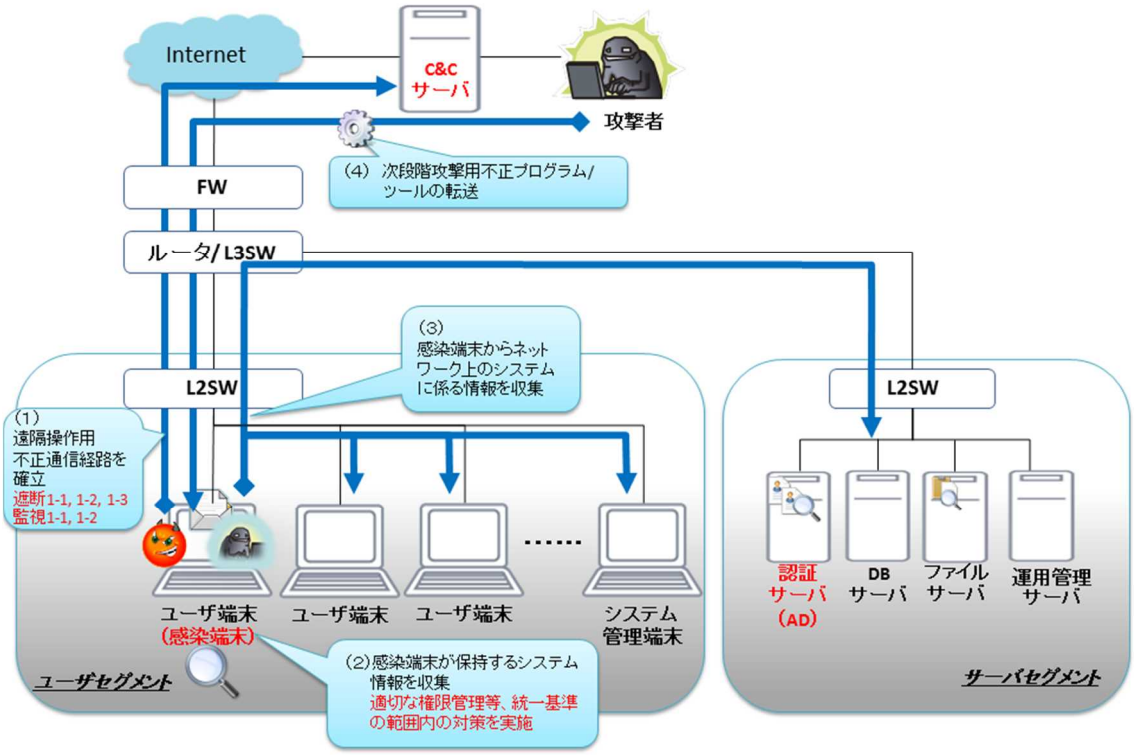


図　１１　侵入基盤構築段階の攻撃シナリオと対策のイメージ

侵入基盤構築段階における対策及びその概要を図　１１及び表　９に示す（各対策の詳細については、次節参照）。

表　９　侵入基盤構築段階における対策セット一覧

分類	No.	対策名称	概要	対象機器
防御遮断策	遮断 1-1	ネットワーク通信経路設計による FW での不正通信の遮断	ネットワーク通信経路の設計により、FW で不正通信を遮断する。	FW、プロキシ
	遮断 1-2	プロキシサーバのアクセス制御による遠隔操作用不正通信の遮断	プロキシサーバにおけるアクセス制御により不正な通信を遮断する。	プロキシ
	遮断 1-3	プロキシサーバの認証機能による遠隔操作用不正通信の遮断	プロキシサーバの認証機能により不正な通信を遮断する。	プロキシ
監視強化策	監視 1-1	プロキシサーバ経由の通信の強制切断による遠隔操作用不正通信の発見	プロキシサーバ経由の通信を一度強制的に切断し、その時に発生するログ等により、C&C サーバへの再接続を行う不正な通信を調査・発見する。	プロキシ
	監視 1-2	プロキシサーバの認証ログの監視と分析	プロキシサーバの認証失敗ログ等を分析し、不正な通信を調査・発見する。	プロキシ

また、侵入基盤構築段階における統制目標と、統制目標を達成するための対策セットの関係を表 １０に示す。

表 １０ 侵入基盤構築段階における統制目標と対策セットの関係

統制目標		No.	対策名称
A	不正プログラムが C&C サーバと遠隔操作用不正通信を行うことをファイアウォールで遮断する。	遮断 1-1	ネットワーク通信経路設計による FW での不正通信の遮断
B	不正プログラムが C&C サーバと遠隔操作用不正通信を行うことをプロキシサーバで遮断・発見する。	遮断 1-2	プロキシサーバのアクセス制御による遠隔操作用不正通信の遮断
		監視 1-1	プロキシサーバ経由の通信の強制切断による遠隔操作用不正通信の発見
C	不正プログラムが C&C サーバと遠隔操作用不正通信を行うことをプロキシサーバの認証機能を用いて遮断・発見する。	遮断 1-3	プロキシサーバの認証機能による遠隔操作用不正通信の遮断
		監視 1-2	プロキシサーバの認証ログの監視と分析

⑤ 侵入範囲拡大段階

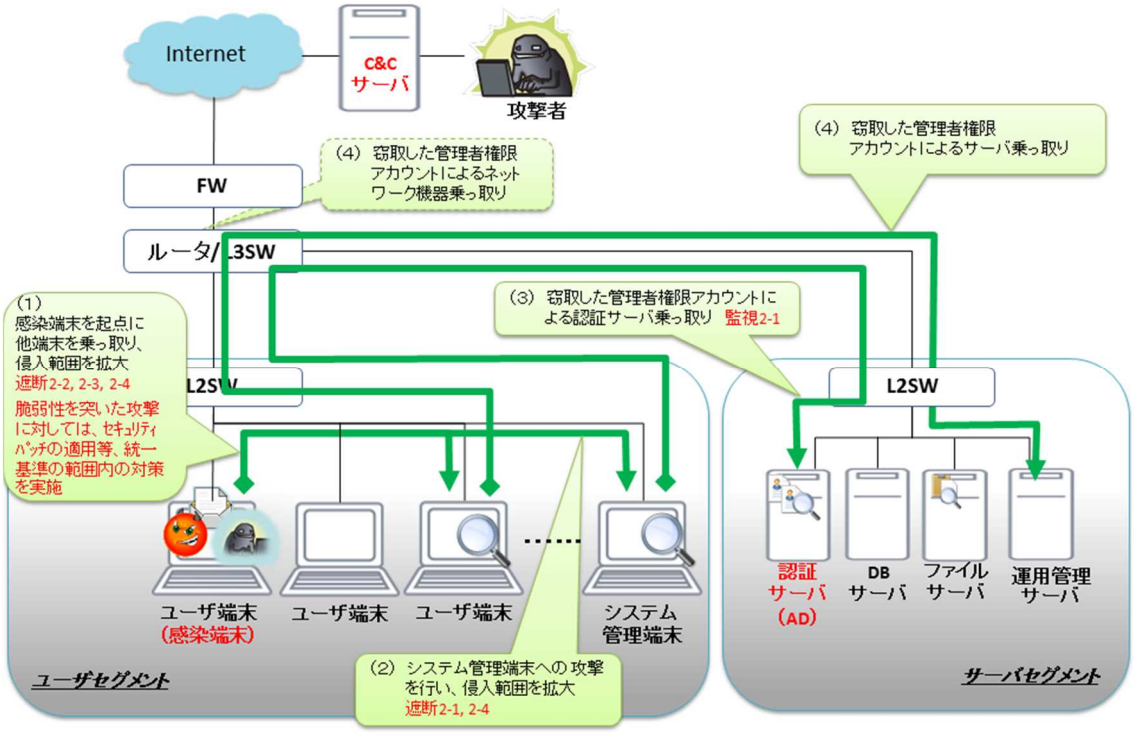


図 １２ 侵入範囲拡大段階の攻撃シナリオと対策のイメージ

侵入範囲拡大段階における対策及びその概要を図 １２及び表 １１に示す（各対策の詳細については、次節参照）。

表　１１　侵入範囲拡大段階における対策セット一覧

分類	No.	対策名称	概要	対象機器
防御遮断策	遮断 2-1	管理端末とユーザ端末のネットワーク分離設計	ユーザ端末とシステム管理端末を分離し、ユーザ端末からシステム管理端末へアクセスできないようにネットワークを分離する。	システム管理端末
	遮断 2-2	適切なネットワークセグメント分離及びアクセス制御設計	適切なセグメントの分離設計とネットワークセグメント間のアクセス制御を実施する。	ネットワーク
	遮断 2-3	ユーザ端末間のファイル共有等禁止	ユーザ端末間でのファイル共有や管理共有を禁止（無効化又は遮断）し、ファイルサーバとのみファイル共有を許可する。	ユーザ端末
	遮断 2-4	高い管理者権限アカウントのキャッシュ禁止	高い管理者権限（Domain Admins 等）のアカウントのキャッシュを禁止する。	ユーザ端末、システム管理端末
監視強化策	監視 2-1	トラップアカウントによる認証ログの監視と分析	高い管理者権限アカウントに似せたトラップアカウントをユーザ端末に仕込み、当該アカウントを用いた攻撃者のログイン行為を検知する。	認証サーバ、ユーザ端末

また、侵入範囲拡大段階における統制目標と、統制目標を達成するための対策セットの関係を表　１２に示す。

表　１２　侵入範囲拡大段階における統制目標と対策セットの関係

統制目標		No.	対策名称
D	各ネットワークセグメントの役割を分割し、異なる他のネットワークセグメントへの侵入を防止する。	遮断 2-1	管理端末とユーザ端末のネットワーク分離設計
		遮断 2-2	適切なネットワークセグメント分離及びアクセス制御設計
E	ユーザ端末や重要サーバへの侵入範囲の拡大を防止又はその兆候を発見する。	遮断 2-3	ユーザ端末間のファイル共有等禁止
		監視 2-1	トラップアカウントによる認証ログの監視と分析
F	端末に保存するアカウントの権限を最小化し、管理者権限等の高い権限の窃取を防止する。	遮断 2-4	高い管理者権限アカウントのキャッシュ禁止

⑥　目的遂行段階

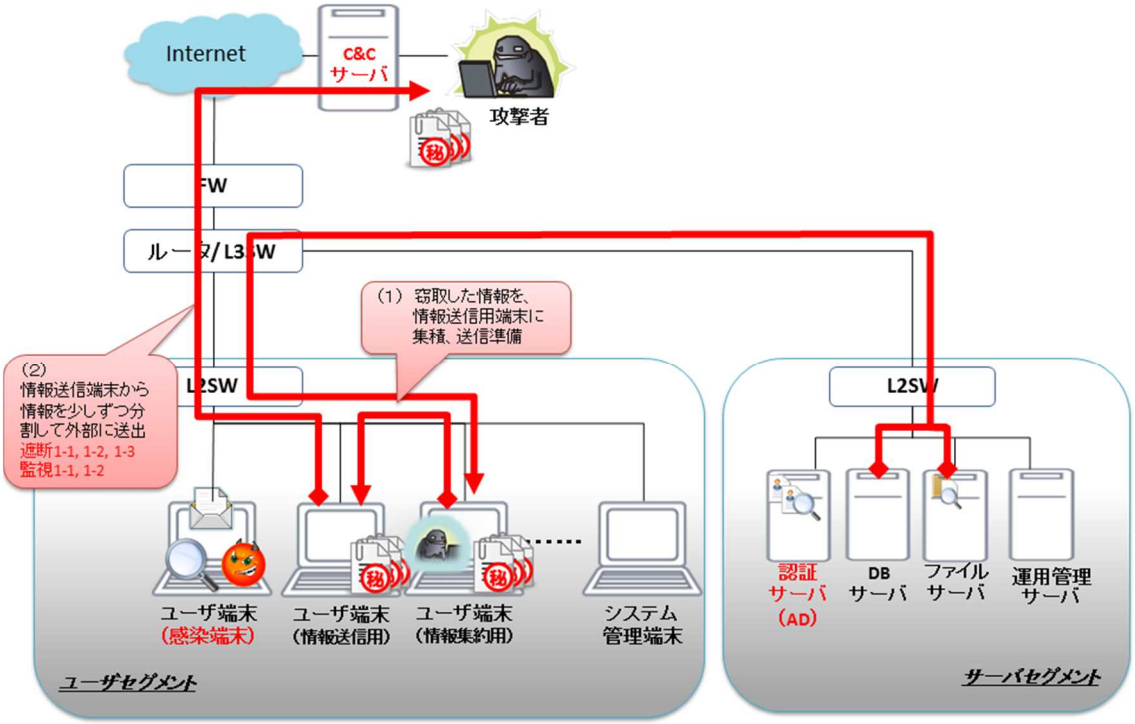


図　１３　目的遂行段階の攻撃シナリオと対策のイメージ

目的遂行段階では、攻撃者は、機密情報等の重要な情報を窃取し、それらを乗っ取り済みの情報送信用端末に集積し、ファイルの圧縮・分割等の送信準備を行う。その後、C&C サーバに向けて、遠隔操作用不正通信経路を経由して当該情報を少しずつ分割して送信する、又は情報システムの破壊行為を実行する。

目的遂行段階においては遠隔操作用不正通信経路を経由した攻撃となることから、本段階における対策は、侵入基盤構築段階における遠隔操作用不正通信経路の確立を防止する、又は遮断するための対策と同様となる。（図　１３を参照。）

５　個別のシステム設計対策

対策セットの各対策について、本節において詳細を解説する。

(1)　侵入基盤構築段階

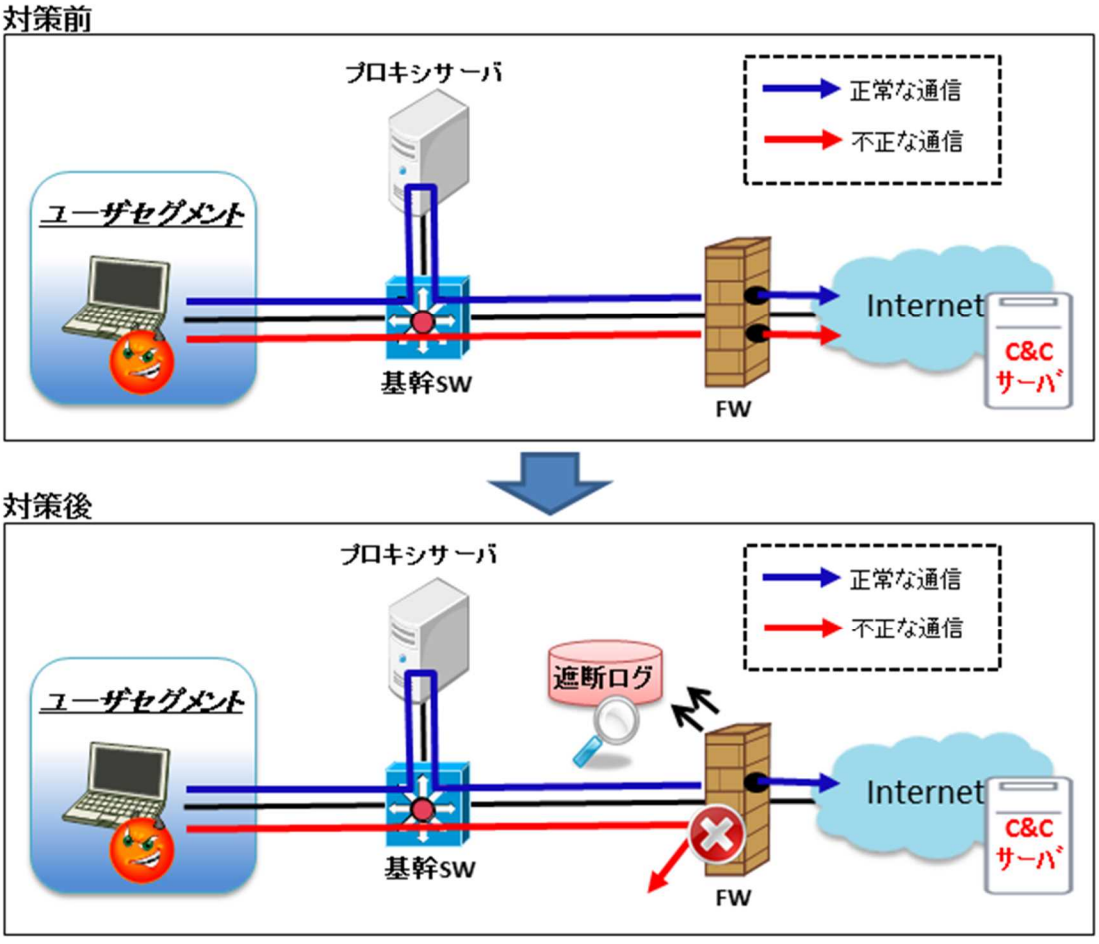
遮断 1-1　ネットワーク通信経路設計による FW での不正通信遮断

【攻撃手法】
不正プログラムが C&C サーバと遠隔操作用不正通信を行うための経路を確保する。

【対策目的】
外部への通信は全てプロキシサーバを経由させることで、プロキシサーバとの連携に対応していない不正プログラムの通信を FW で遮断する。

【対策項目】
ネットワーク通信経路の設計により、FW で不正通信を遮断する。また、FW で遮断した通信ログ（遮断ログ）を確認する。

【攻撃と対策のイメージ図】



【システム設計要領】

ユーザ端末の設置されたネットワーク上のセグメント（以下「ユーザセグメント」という。）からインターネットへの通信は、全てプロキシサーバを経由して通信する設計とし、当該サーバを経由しない通信は、FW にて遮断（ブロック）する。

このように設計することで、プロキシサーバとの連携に対応していない不正プログラムの遠隔操作用不正通信を FW で遮断し、また、その遮断ログを用いて当該通信を発見することができる。

実装項目①：プロキシサーバを導入し、ウェブブラウザのプロキシ設定を有効にする。

ユーザ端末のウェブブラウザのプロキシ設定において、組織内のプロキシサーバを指定する。

実装項目②：FW において、内部（ユーザセグメント）から外部（インターネット）への通信の遮断ルール（FW ポリシー）を設計・設定する。

不正プログラムには、プロキシサーバとの連携に対応せず、プロキシサーバを介さない通信を行うものがあることから、ユーザセグメントからインターネット向けの通信に対して、FW にて以下のルールを適用する。

- ユーザセグメントからプロキシサーバ経由のインターネット向け通信を許可する。
- ユーザセグメントからプロキシサーバを経由しないものであって、直接インターネットにアクセスする通信を遮断する。
- 以下のような、プロキシサーバを経由すると動作に支障のあるサービス、プロキシサーバに負荷をかけるサービス、HTTP（80 番ポート）や HTTPS（443 番ポート）以外でインターネット向けに通信するサービス等については、FW にてアクセス制御リスト（ホワイトリスト等）を設定する。
  - OS やミドルウェアとアップデートサーバとの通信
  - ウイルス対策ソフト等のパターンファイルやシグネチャファイル等の更新に係る通信
  - その他、業務上必要な通信（例えば、TV 会議、ストリーミング等）

透過型プロキシサーバを導入している場合は、正常なインターネットへの通信だけでなく、不正プログラムによる遠隔操作用不正通信も常にプロキシサーバを経由して通信してしまい、本対策による不正通信の遮断がで

きないことに留意する必要がある。

【運用管理要領】

FW において、通信ログ（遮断ログ）を定期的に監視し、ユーザ端末からの遠隔操作用不正通信の有無を確認する。不正通信の疑いがあれば、不正プログラムに感染しているおそれがあるため、当該ユーザ端末を調査する。

また、FW のアクセス制御リスト（ホワイトリスト等）の見直し、更新を行う。

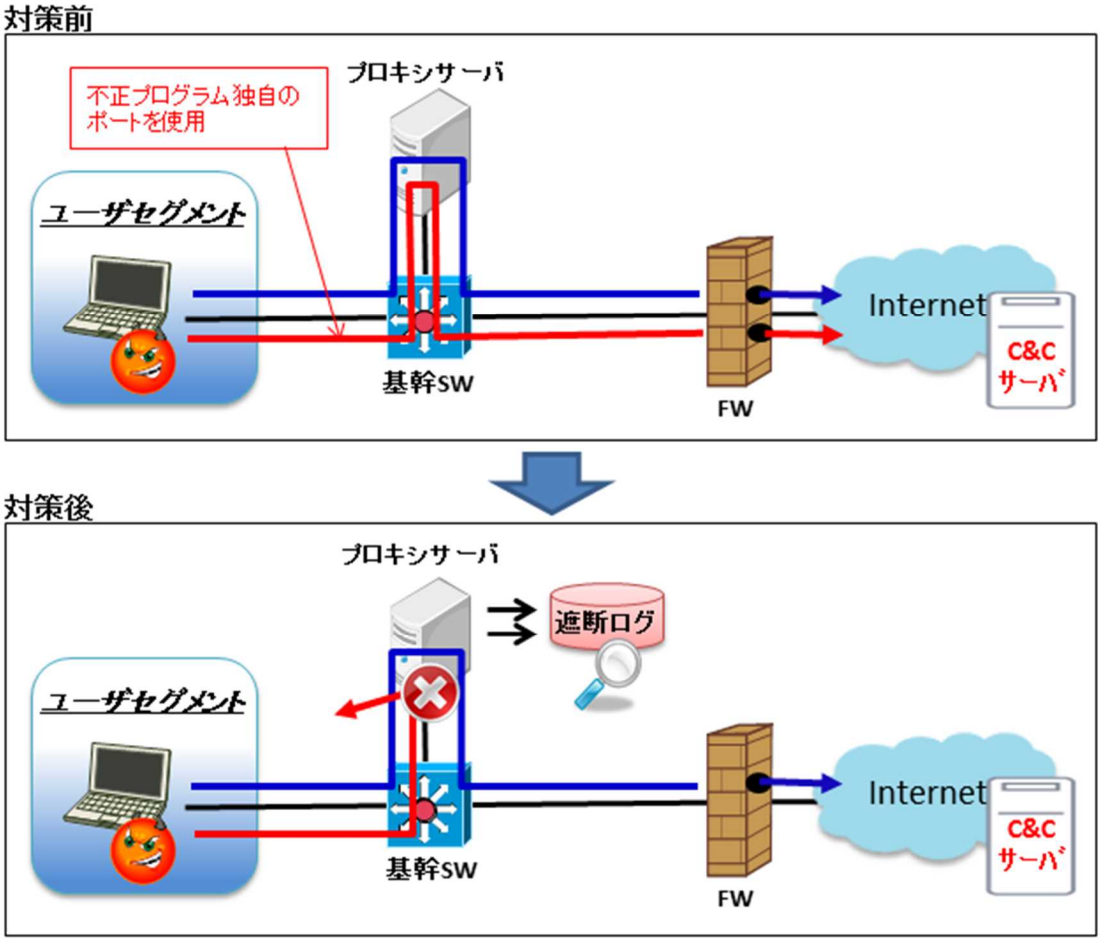
遮断 1-2　プロキシサーバのアクセス制御による遠隔操作用不正通信遮断

【攻撃手法】
不正プログラムがプロキシサーバを経由して C&C サーバと遠隔操作用不正通信を行うための経路を確立する。不正プログラムは、端末からプロキシサーバの IP アドレス等を収集して、プロキシサーバを経由した通信を行う。

【対策目的】
プロキシサーバが中継する通信ポートを最低限のものに制限することで、組織で標準的に利用していない通信ポートを利用する不正プログラムの通信をプロキシサーバで遮断する。

【対策項目】
プロキシサーバにおけるアクセス制御により不正な通信を遮断する。また、プロキシサーバで遮断したアクセスログ（遮断ログ）を確認する。

【攻撃と対策のイメージ図】



【システム設計要領】

ユーザセグメント（ユーザ端末）からプロキシサーバを経由するインターネットへの通信については、許可する通信ポートを最低限のもの（例えば、HTTP、HTTPS）に制限する設定とし、正規通信ポート以外への通信は、プロキシサーバにて遮断する。

このように設計することで、組織で標準的に利用していない通信ポートを利用する不正プログラムの遠隔操作用不正通信をプロキシサーバで遮断し、当該通信を発見することができる。

実装項目①：プロキシサーバにおけるアクセス制御リストを設計・設定する。

プロキシサーバにて、以下のルールを適用する。

- プロキシサーバが中継する通信ポートを制限する。（例 HTTP（80 番ポート）、HTTPS（443 番ポート）のみ）
- プロキシサーバに SSL トンネリング等を要求する CONNECT メソッド[3]については、443 番ポートのみ許可する。
- 上記以外に業務上必要な通信ポートがあれば、CONNECT メソッドの利用も考慮の上、プロキシサーバで中継するように設定する。

【運用管理要領】

プロキシサーバにおいて、アクセスログ（遮断ログ）を定期的に監視し、ユーザ端末からの遠隔操作用不正通信の有無を確認する。不正通信の疑いがあれば、不正プログラムに感染しているおそれがあるため、当該ユーザ端末を調査する。

また、プロキシサーバのアクセス制御リストの見直し及び更新を行う。

[3] CONNECT メソッド：SSL 等のプロトコルで暗号化されたものをトンネルさせるために使うメソッド。プロキシサーバはトンネルを確立すると、その後の HTTP クライアントからのリクエストに関しては一切関知しない。

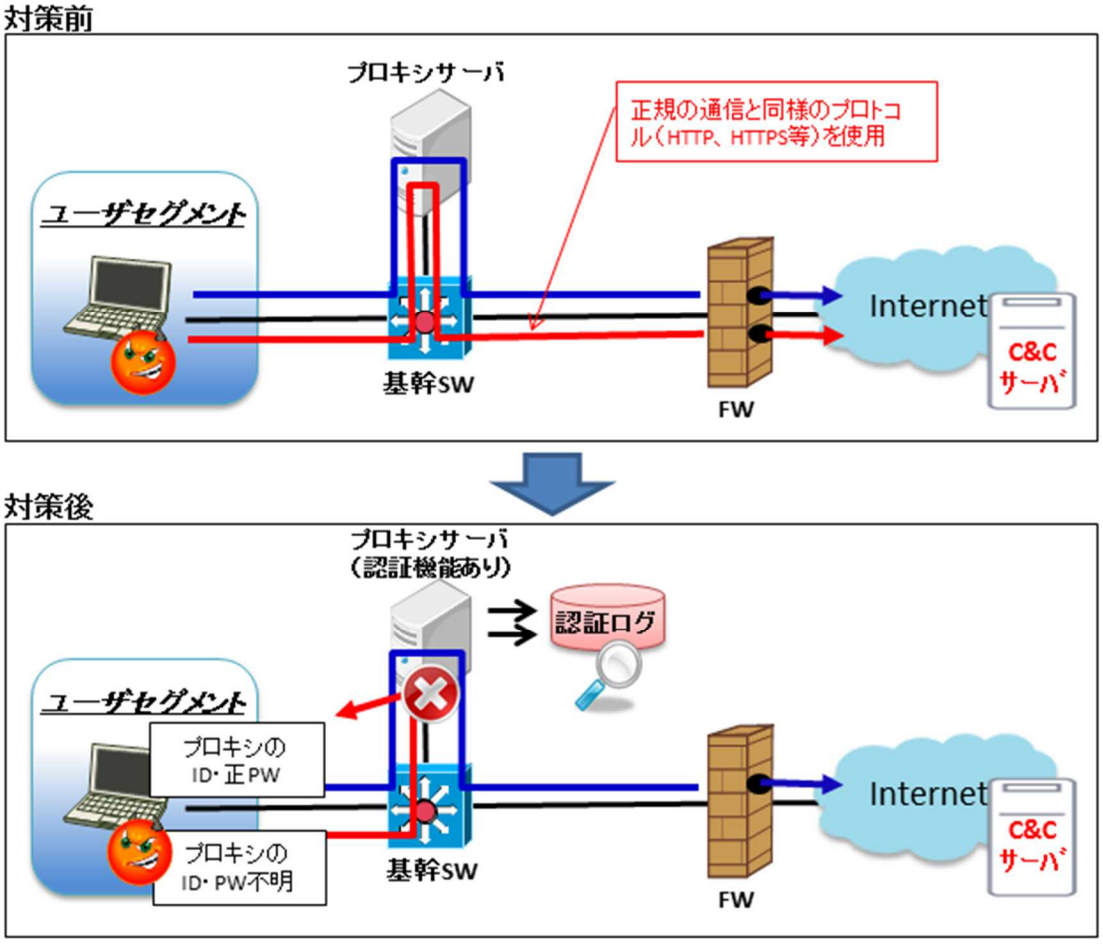
遮断 1-3　プロキシサーバの認証機能による遠隔操作用不正通信遮断

【攻撃手法】
不正プログラムがプロキシサーバを経由して C&C サーバと遠隔操作用不正通信を行うための経路を確保する。不正プログラムは、端末からプロキシサーバの IP アドレス等を収集して、プロキシサーバを経由した通信を行う。

【対策目的】
プロキシサーバを経由してアクセスする際に認証を求めることで、不正プログラムがプロキシサーバを経由した不正な通信を行うことを防止する。

【対策項目】
プロキシサーバの認証機能により不正な通信を遮断する。

【攻撃と対策のイメージ図】



【システム設計要領】

プロキシサーバを経由する通信に対してユーザ認証を行い、当該認証に成功した通信のみを許可する設計とする。

このように設計することで、プロキシサーバによる認証に対応していない不正プログラムの遠隔操作用不正通信をプロキシサーバで遮断することができる。

実装項目①：プロキシサーバの認証機能を有効にする。

ユーザ単位で認証が可能なプロキシサーバを導入するなどして、プロキシサーバのアクセスログからアクセスを行ったユーザ及びユーザ端末が特定できるよう設計する。

実装項目②：ウェブブラウザへの認証情報の保存を禁止する。

ウェブブラウザには、認証情報等のパラメータの再入力を省略するオートコンプリート機能が提供されている。しかし、オートコンプリート機能によって保存されたパスワードは容易に参照することが可能であるため、当該端末に侵入した攻撃者は当該パスワードを入手することが可能である。そのため、オートコンプリート機能については、OS のセキュリティポリシー管理機能を用いて利用を制限する等の対策を行う。

【運用管理要領】

監視強化策 1-1 との組合せ対策のため、不正通信の発見に係る運用管理要領については監視強化策 1-1 を参照のこと。

また、プロキシサーバの認証機能を有効にした場合、OS やミドルウェアのアップデートサーバとの通信等で問題が発生することがある。このような場合は、特定の宛先への通信のみ認証を回避するようプロキシサーバ側でホワイトリスト設定を行う。

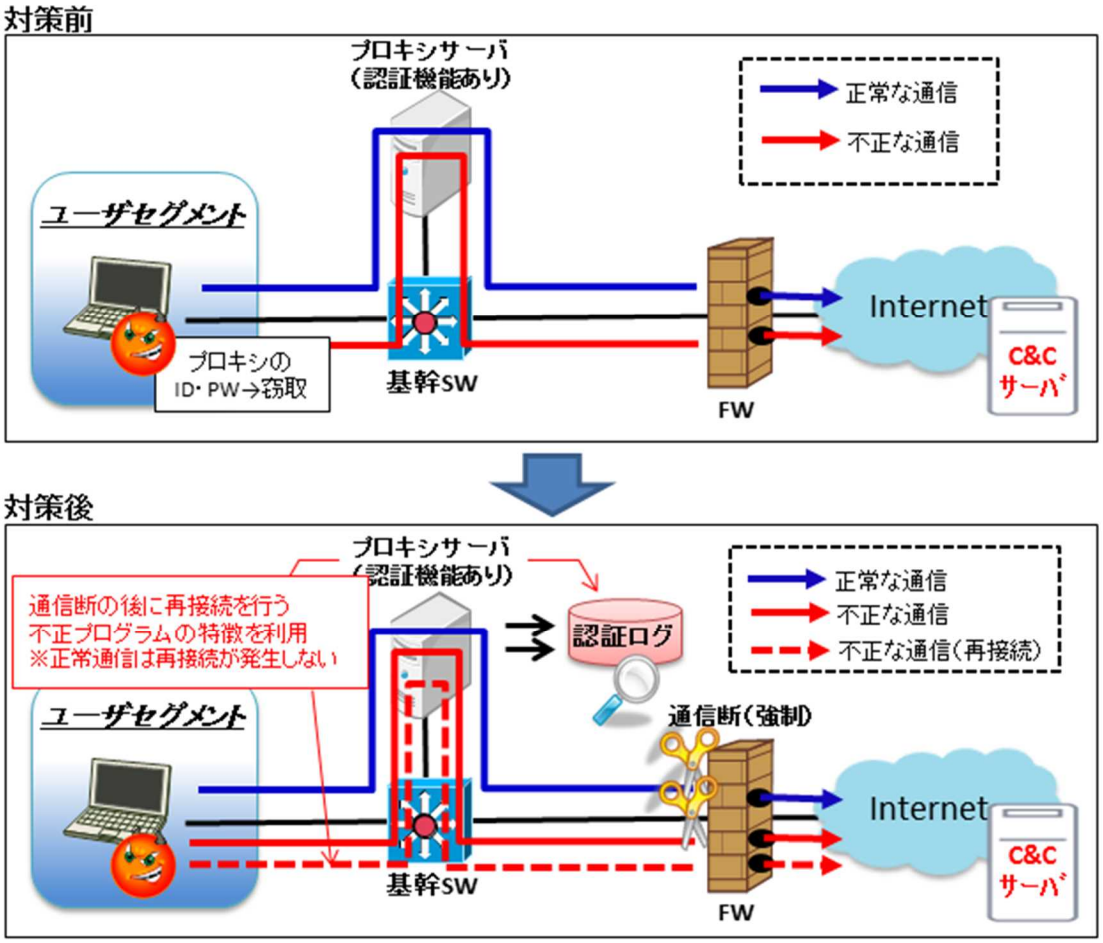
監視 1-1　プロキシサーバ経由通信切断による遠隔操作用不正通信発見

【攻撃手法】
不正プログラムがプロキシサーバを経由して C&C サーバと遠隔操作用不正通信を行うための経路を確保する。

【対策目的】
プロキシサーバを経由する外部向けの通信を FW 等で強制的に手動切断する。その結果通信を回復しようとする不正プログラムは、C&C サーバへの再接続のための通信を行う。これらの通信のログをプロキシサーバに残すことで、不正な通信の早期発見を行う。

【対策項目】
当該通信を一度強制的に手動切断し、その時に発生するアクセスログ等を分析し、C&C サーバへの再接続を行う不正な通信を調査・発見する。

【攻撃と対策のイメージ図】



【システム設計要領】

規則的に発生する遠隔操作用不正通信をプロキシサーバのログから検出するため、信頼できるアクセス先以外の通信については全てプロキシサーバを経由するよう設計する。詳細については防御遮断策 1-1 を参照のこと。

【運用管理要領】

遠隔操作用不正通信のコネクションを手動切断して再接続の通信を発生させるため、プロキシサーバを経由する外部向けの通信を FW 等で一時的に手動切断（１回目）する。プロキシサーバでは、切断されたタイミングで遠隔操作用不正通信を含む全ての通信のログが記録される。

遠隔操作用不正通信のコネクションを再度確立させるため、プロキシサーバを経由する外部向け通信の切断を一定時間解除して正常な状態に戻す。

遠隔操作用不正通信のコネクションを再度切断してプロキシサーバのログへ出力するため、プロキシサーバを経由する外部向けの通信を FW 等で一時的に手動切断（２回目）する。（図 １４を参照）

２回目の通信切断後に出力されたログから、規則的に再接続を試みる通信の有無を確認し、接続先 IP アドレスの割当先国、ドメインの詳細（登録者情報や登録時期等）、HTTP メソッド（POST が使用されているかなど）といった特徴を確認することで、不正な通信が発生していないかどうかを確認する。不正通信の疑いがあれば、不正プログラムに感染しているおそれがあるため、当該ユーザ端末を調査する。

ログが大量に出力される場合は、正常な通信先をあらかじめ把握しておき、それらの通信を除外して確認するといった対応が必要となる。本対策については、定期的に実施する必要がある。

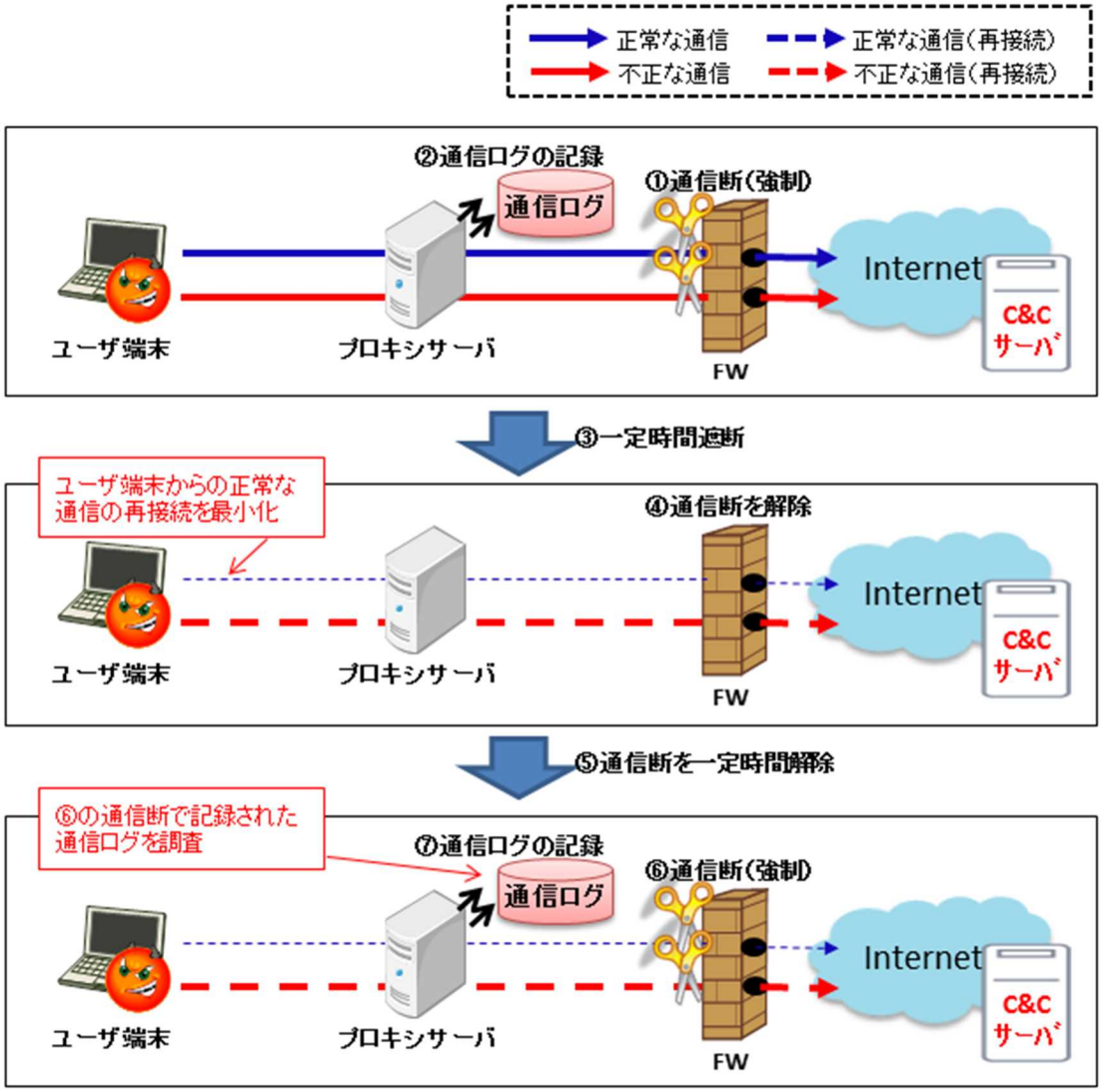


図　１４　プロキシサーバを経由する外部向けの通信の強制切断の実施要領

監視 1-2　プロキシサーバの認証ログの監視と分析

【攻撃手法】
不正プログラムがプロキシサーバを経由して C&C サーバと遠隔操作用不正通信を行うための経路を確保する。不正プログラムは、端末からプロキシサーバの IP アドレスや認証情報等を収集して、プロキシサーバを経由した通信を行う。

【対策目的】
プロキシサーバを経由してアクセスする際に認証を求め、認証失敗等をログに記録することで、不正プログラムが不正な通信を試みる際の痕跡を検出し、当該通信の早期発見を行う。

【対策項目】
プロキシサーバの認証失敗ログ等を分析し、不正な通信を調査・発見する。

【システム設計要領】

プロキシサーバを経由する通信に対してユーザ認証を行い、当該認証の成功及び失敗をログに記録する。

なお、本対策は防御遮断策 1-3 と組み合せて実施する必要がある。

【運用管理要領】

プロキシサーバの認証に関するアクセスログに記録された、認証の成功及び失敗に関する事象を定期的に確認する。以下に、不正な認証の試行の例を示す。

- 特定のユーザ ID に対するブルートフォース[4]による認証の試行
- パスワードを固定してユーザ ID を変化させる認証の試行
- ユーザ ID の使い回しによる認証の試行

不正通信の疑いがあれば、不正プログラムに感染しているおそれがあるため、当該ユーザ端末を調査する。

[4] ブルートフォース：無意味な英数記号の組み合わせも含めた、総当たりでのパスワード解析方法。

(2)　侵入範囲拡大段階

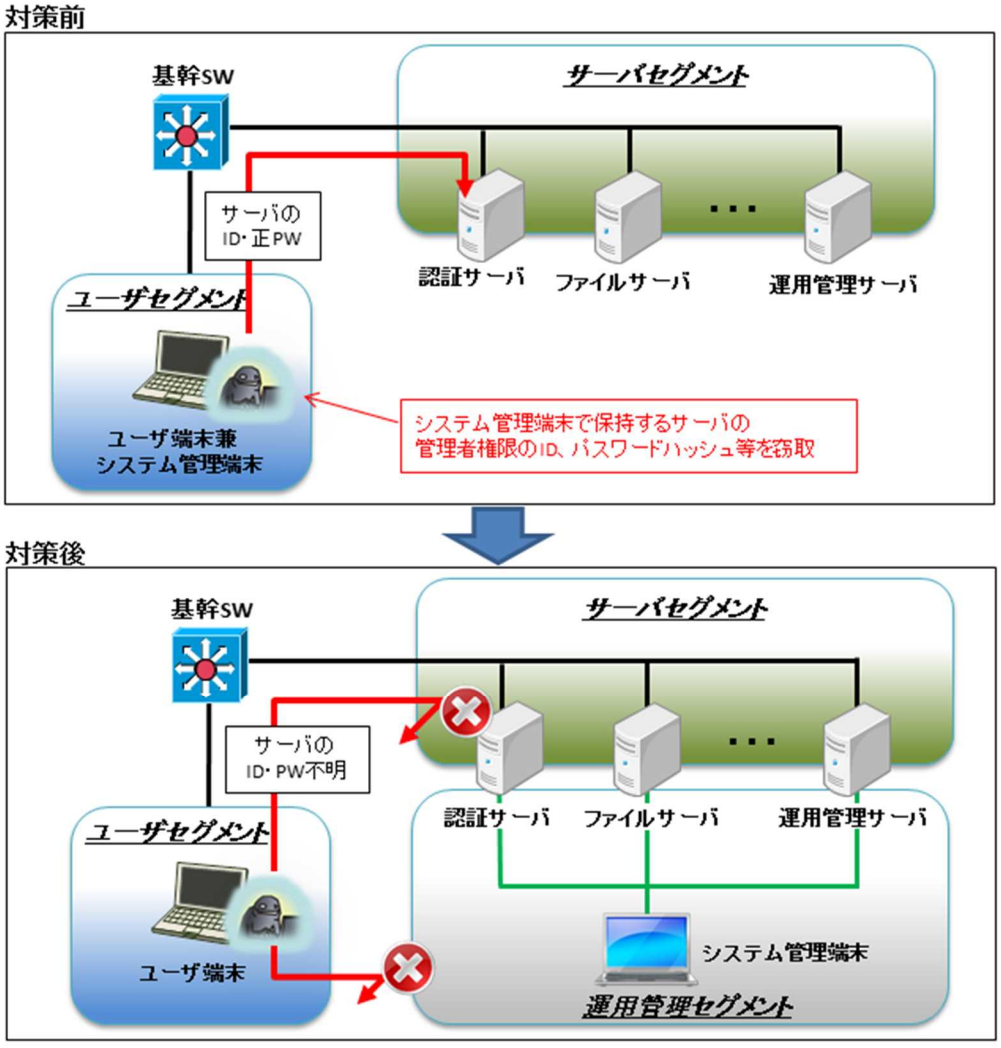
遮断 2-1　管理端末とユーザ端末のネットワーク分離設計

【攻撃手法】
システム管理端末を乗っ取り、情報システム中枢の重要サーバの攻略につなげる。

【対策目的】
ユーザ端末からシステム管理端末の乗っ取りを防止する。

【対策項目】
ユーザ端末とシステム管理端末を分離し、ユーザ端末からシステム管理端末へアクセスできないようにネットワークを分離する。

【攻撃と対策のイメージ図】



【システム設計要領】

重要なサーバを運用管理するためにシステム管理端末は必要であるが、当該システム管理端末が攻撃者に乗っ取られてしまうと、情報システム中枢の重要サーバの攻略につながってしまう。

そこで、ユーザセグメント等の他セグメントとシステム管理端末の設置されたネットワーク上の専用セグメント（以下「運用管理セグメント」という。）を、他セグメントからアクセスできないようにネットワーク分離設計することで、たとえユーザ端末が不正プログラムに感染したとしても、システム管理端末が乗っ取られないような構成とする。

実装項目①：システム管理用の専用端末を準備する。
実装項目②：他セグメントとネットワーク分離した運用管理セグメントを構築し、当該セグメントにシステム管理端末を接続する。
実装項目③：認証サーバにて、認証サーバに管理者権限でログインできる端末を当該システム管理端末のみに制限する。

運用管理セグメントの構築方法としては、各サーバのサーバ（業務）セグメントとは別に運用管理用セグメントの LAN ポートから LAN を構築する方法、当該 LAN ポートに直接管理端末を接続する方法等が考えられる。

また、当該サーバはサーバ（業務）セグメントからサーバの運用管理用セグメントの LAN ポートにアクセスできないようにする。また、運用管理セグメントは、システム管理者のみが使用できる専用ネットワーク構成とする。

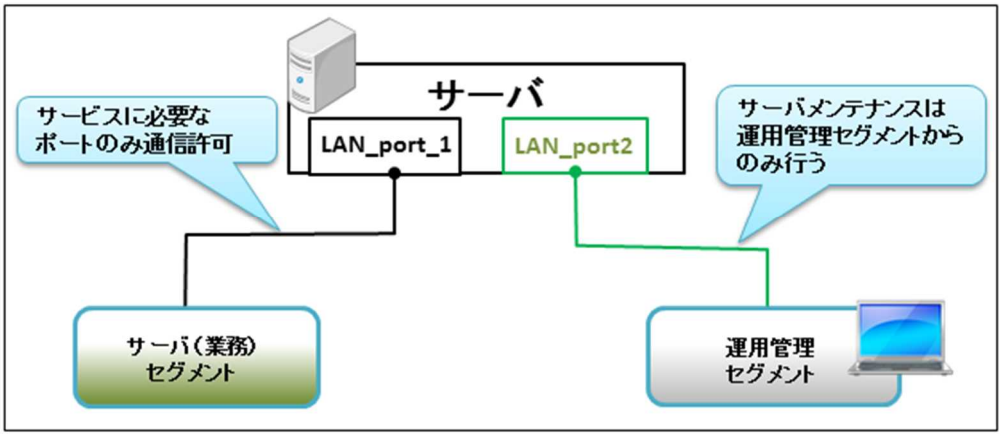


図　１５　サーバにおける運用管理セグメントの構成イメージ

【運用管理要領】

運用管理セグメントの端末についても、セキュリティパッチの適用やウイルス対策ソフトウェアのパターンファイル更新等を適宜実施する。

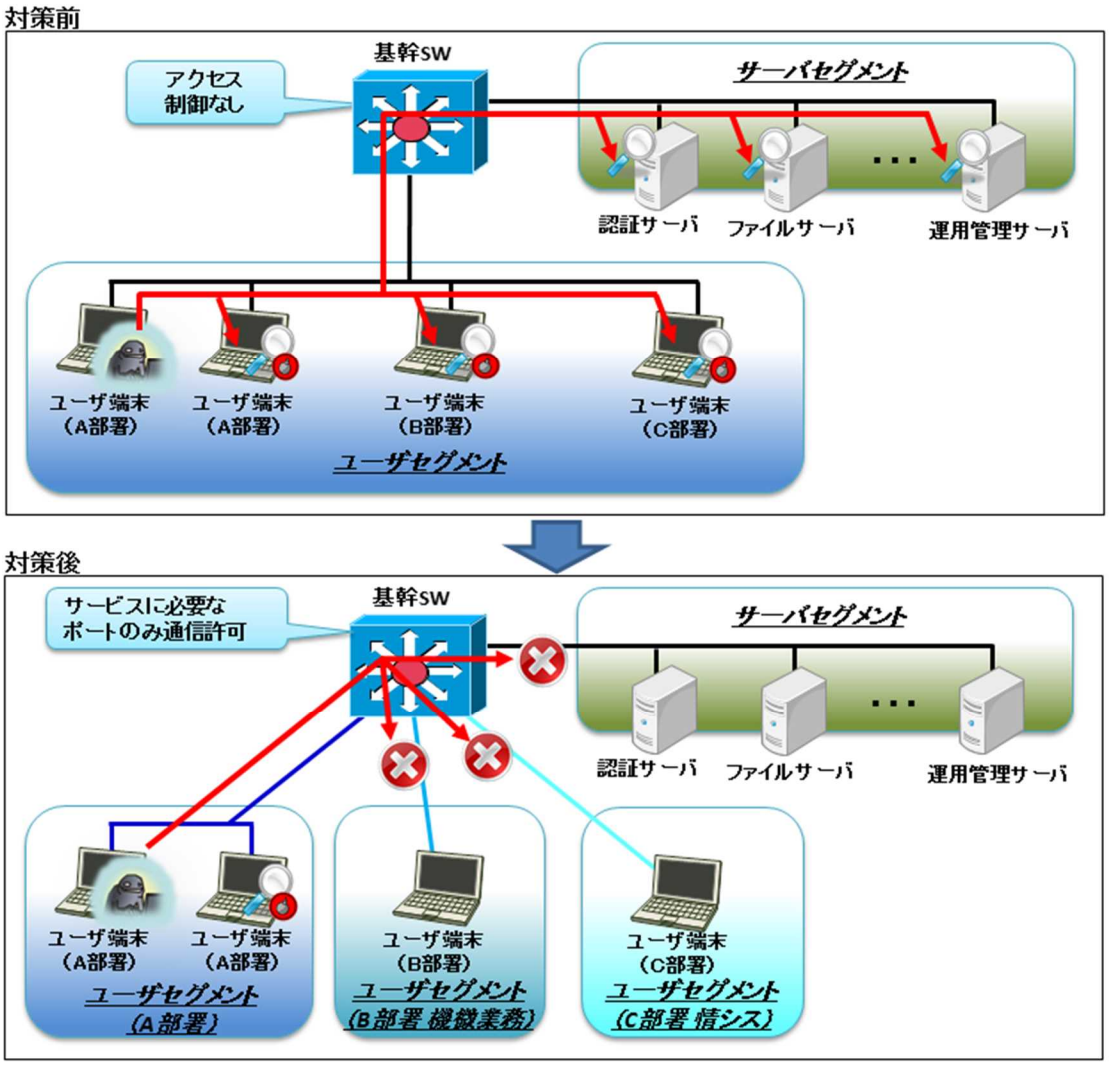
遮断 2-2　適切なネットワークセグメント分離及びアクセス制御設計

【攻撃手法】
他端末やサーバを乗っ取り、侵入範囲を拡大する。

【対策目的】
他端末やサーバの乗っ取りを防止する、又は乗っ取りをしにくくする。

【対策項目】
適切なネットワークセグメントの分離設計とネットワークセグメント間のアクセス制御設計の実施

【攻撃と対策のイメージ図】



【システム設計要領】

ネットワーク上で適切にアクセス制御を実施することにより、感染した端末のユーザセグメントから、他のセグメントに侵入したり、調査したりすることが困難となり、攻撃者にとって攻撃しにくいネットワークとなる。

そのため、組織内ネットワーク（内部ネットワーク）は、セグメントの役割やアクセスの必要性の観点から、サーバセグメント、ユーザセグメント（例えば、課室部局単位、業務単位等）、運用管理セグメント等に適切なネットワークの分離設計を行い、各セグメント間で行う通信を必要最小限のものに制限するように、適切なアクセス制御を行う。

実装項目①：組織内ネットワーク（内部ネットワーク）を VLAN やサブネットにより、サーバセグメント、ユーザセグメント等に適切に分離する設計を行う。

実装項目②：上記設計した各セグメント間の通信に係るアクセス制御（IP アドレス及びポート番号の許可又は拒否）を設計し、ネットワーク上の基幹スイッチ等でアクセス制御リストを設定する。

アクセス制御の設計例を表 １３に示す。アクセス制御の設計に当たっては、セグメント間における通信の可否、通信を許可するポート番号等について検討する。

なお、表 １３は、大まかに各セグメントをモデル化したものであり、実際はさらに詳細化して整理する必要がある。また、表中のアクセス可否については例示であり、詳細化されたセグメントに合わせて検討する。

表 １３ セグメント間のアクセス制御の設計例

		アクセス先					
		Internet	DMZ	サーバ	ユーザ（一般）	ユーザ（機微）	運用管理
アクセス元	Internet		○	×	×	×	×
	DMZ	○		○	×	×	×
	サーバ	○※1	○		×	×	×
	ユーザ（一般）	×	×	○		×	×
	ユーザ（機微）	×	×	○	×		×
	運用管理	×	○	○※2	×	×	

凡例 ○：可、×：不可　赤字：本対策の主な範囲

※1 プロキシサーバ、運用管理サーバ等からの通信を想定

※2 システム管理端末のパッチ適用等に係る通信を含む

【運用管理要領】

組織や業務の見直し等に合わせて、アクセス制御の設計見直しを実施する。

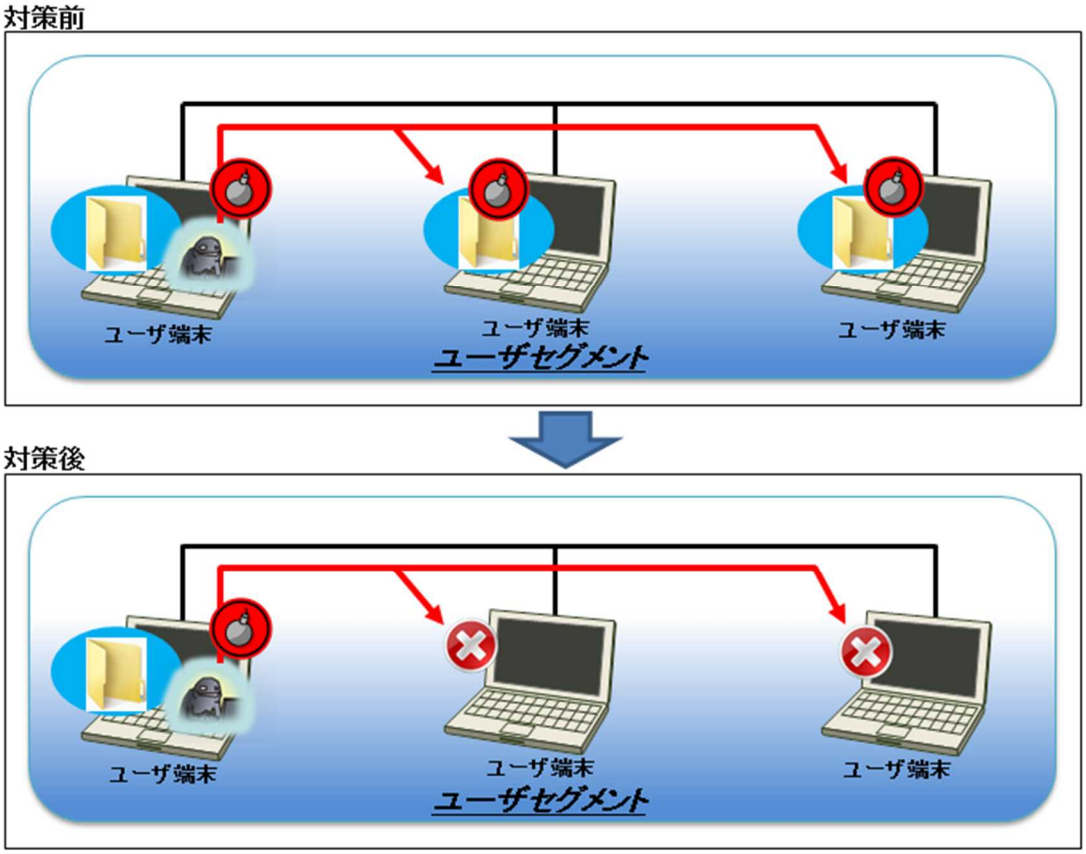
遮断 2-3　ユーザ端末間のファイル共有等の禁止

【攻撃手法】
ファイル共有や管理共有の通信ポートを経由して他端末を乗っ取る。

【対策目的】
ファイル共有や管理共有の通信ポートを利用した他端末の乗っ取りを防止する、又は乗っ取りをしにくくする。

【対策項目】
端末間でのファイル共有や管理共有を禁止（無効化又は遮断）し、ファイルサーバとのみファイル共有を許可する。

【攻撃と対策のイメージ図】



【システム設計要領】

ユーザ端末においてファイル共有機能を有効にした場合、指定したフォルダ内のファイルを他のユーザ端末と共有する機能に加えて、管理者が物理ドライブ（C$、D$等）やシステムディレクトリ（ADMIN$）等にアクセス可能となる管理共有も有効となる。そこで、ユーザ端末におけるファイル共有機能を無効化する、又はユーザ端末間のファイル共有に係る通信を遮断することで、ユーザ端末間のファイル共有を禁止する設計とする。

このように設計することで、攻撃者がファイル共有機能を悪用してユーザ端末への侵入範囲を拡大することを防止することができる。

実装項目①：ユーザ端末のファイル共有機能を停止する。

ユーザ端末においてファイル共有機能が有効な場合、攻撃者は管理共有を悪用することでリモートから様々なプログラムを実行することが可能となるため、ファイル共有機能を停止して管理共有を無効にする。グループポリシーを利用してファイル共有機能を停止するためには、Active Directory サーバで以下の操作を行う。

（Windows Server 2008 の場合の操作方法）

1. グループ ポリシー管理コンソール (GPMC) を開始します。これを実行するには、[スタート] ボタンをクリックし、[検索の開始] ボックス内をクリックして、「gpmc.msc」と入力します。
2. ナビゲーション ウィンドウで、[ローカル コンピュータ ポリシー]、[ユーザの構成]、[管理用テンプレート]、[Windows コンポーネント]、[ネットワーク共有] の順にフォルダを開きます。
3. 詳細ウィンドウで、[ユーザがプロファイル内のファイルを共有できないようにします] をダブルクリックします。
4. グループ ポリシー設定を有効にしてユーザがファイルを共有する機能を無効にするには、[有効] をクリックします。
5. [OK] をクリックして、変更を保存します。

出典：「グループ ポリシーを使用してユーザまたはグループのファイル共有を有効または無効にする」
http://technet.microsoft.com/ja-jp/library/cc754359(v=ws.10).aspx

実装項目①の代替策：ユーザ端末間の通信を遮断する。

ファイル共有機能を停止できない場合は、ユーザ端末のパーソナル FW 等のフィルタリング機能を用いてユーザ端末間のファイル共有に係る通信（137/UDP、138/UDP、139/TCP、445/TCP）を遮断する。

【運用管理要領】

なし。

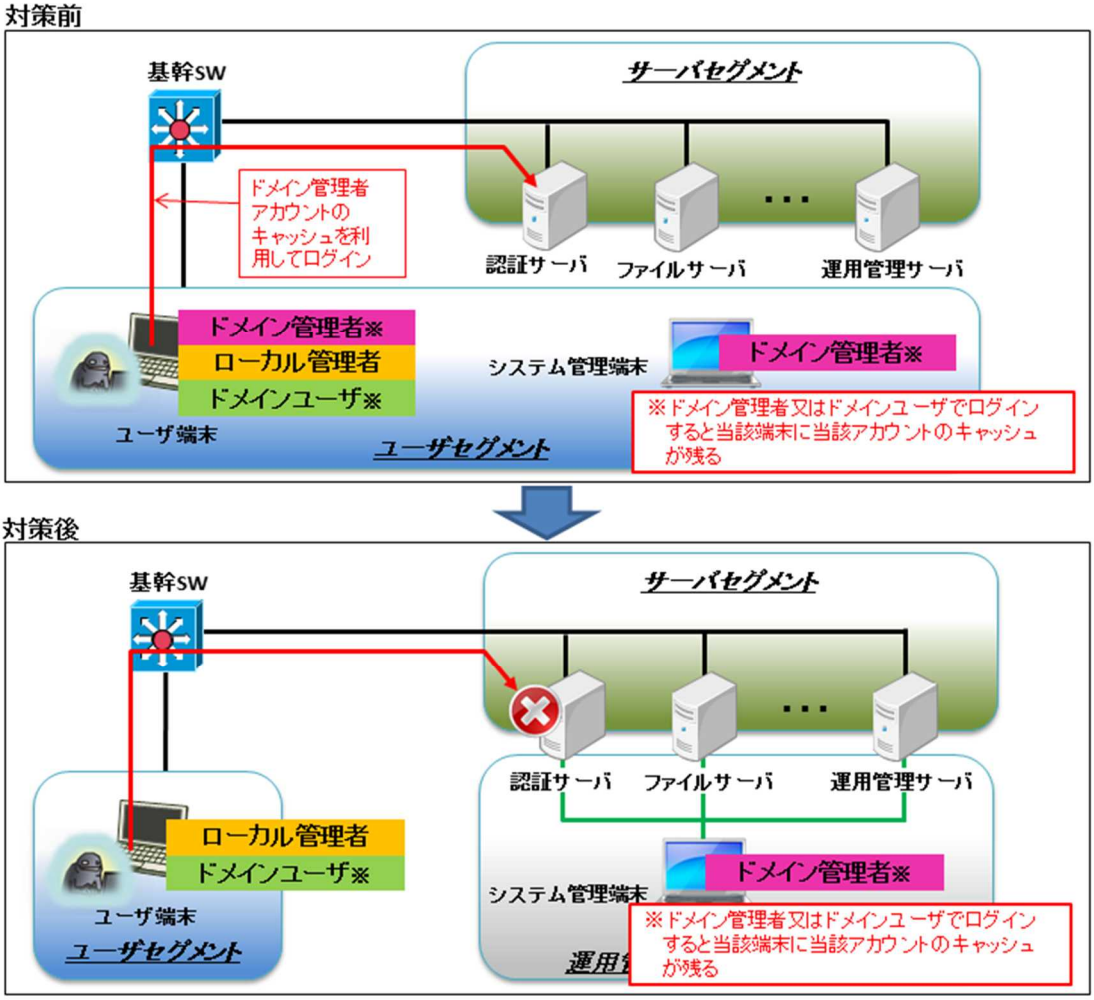
遮断 2-4　高い管理者権限アカウントのキャッシュ禁止

【攻撃手法】
ユーザ端末、システム管理端末からドメイン管理者（Domain Admins グループ）等の高い管理者権限アカウント（ID、パスワードハッシュ）を窃取する。

【対策目的】
ユーザ端末又はシステム管理端末で保持する高い管理者権限のアカウントが窃取されない、又は端末に保持されないようにする。

【対策項目】
高い管理者権限アカウントのキャッシュ禁止

【攻撃と対策のイメージ図】



【システム設計要領】

例えば、ユーザ端末におけるシステム管理作業時にドメイン管理者（Domain Admins グループ等）でログインした場合には、ドメイン管理者権限の ID、パスワードハッシュ[5]等の認証情報が当該アカウントのキャッシュとして当該端末に記録されてしまう。この状態で、攻撃者に当該端末に侵入され、ドメイン管理者権限のパスワードハッシュ等が窃取されてしまうと、攻撃者がドメイン管理者となって重要なサーバを容易に乗っ取ることができる。このように、ID とパスワードハッシュを用いて不正に認証する手法は Pass-the-hash と呼ばれ、本来の認証に必要なパスワードを入手しなくても認証できてしまう。

そのため、ユーザ端末等信頼性の低い端末では、ドメイン管理者等の高い管理者権限のアカウントが利用されない、つまりキャッシュされない設計とすることが重要である。

このように設計することで、攻撃者はユーザ端末から高い管理者権限の ID、パスワードハッシュを窃取できないため、認証サーバや重要なサーバ等の乗っ取りを防止することができる。

実装項目①：ユーザ端末を利用するためのユーザアカウントとシステム管理端末を利用するための管理者用アカウントを分離する。

ユーザ端末とシステム管理端末を利用するためのアカウントを共通にしていた場合、ユーザ端末に管理者権限のアカウントがキャッシュされることになるため、パスワードハッシュ等の窃取によって重要なサーバを乗っ取る機会を与えてしまう。したがって、ユーザ、管理者、監査者等の役割ごとにアカウントを割り当てるよう設計することで、このようなリスクを回避することができる。

実装項目②：管理者用アカウントの権限を最小化する。

管理者に割り当てるアカウントは、必要最小限の権限となるよう設計する。例えば、ドメイン管理者等の高い管理者権限については、Active Directory 等を管理する管理者のみに割り当てる。また、管理する内容に応じて、ドメイン管理者よりも低い権限を割り当てることも検討する。このように設計することで、管理者用アカウントが誤ってユーザ端末で利用さ

[5] パスワードハッシュ：平文のパスワードをハッシュ・アルゴリズムでハッシュ化したパスワード。アカウントに対して設定したパスワードは、何らかの形でシステムに保存しておく必要がある。保存されたパスワード情報が第三者に見られる可能性を考慮して、元の平文パスワードを、ハッシュ関数のような非可逆性のあるアルゴリズムで変換して保存する場合が多い。

れた場合でも、被害を最小化できる。
　また、各端末のシステム管理に割り当てるアカウントは、ローカル管理者権限等の必要最小限の権限となるように設計する。

　本対策は、管理者が必要な運用を実現しつつ、Active Directory サーバ等の認証サーバに影響を与えない権限管理を実現することが目的である。例えば、ソフトウェアの自動アップデートやリモートメンテナンスを行うためにドメイン管理者権限でユーザ端末を使用している場合があるが、このような動作にドメイン管理者権限は必要ないため、端末のローカル管理者権限で動作させるなど、最小限の権限を利用するよう設計する必要がある。また、サービスやスケジュールされたタスクについても、ユーザ端末においてドメイン管理者権限等の高い権限のアカウントで実行しないように設計する。
　ローカル管理者やドメイン管理者等の管理者権限でパスワードハッシュの参照が可能となるため、ユーザ端末の利用者に対して、ユーザ権限ではなく、ローカル管理者権限等が付与されていないか確認する必要がある。また、あるユーザ端末には高い権限のアカウントがキャッシュされていなくても、他の端末にはキャッシュされている可能性があることから、リモートデスクトップ接続でローカル管理者権限によるログインを禁止するとともに、端末のローカル管理者のパスワードを他の端末とは異なるものに設定することで、攻撃者が高い管理者権限のパスワードハッシュを入手することを防止する。

【運用管理要領】
　ユーザ端末には、ドメイン管理者等の高い管理者権限を持つアカウントでログインしない。また、このようなアカウントでログインしていないかを、定期的に確認する。

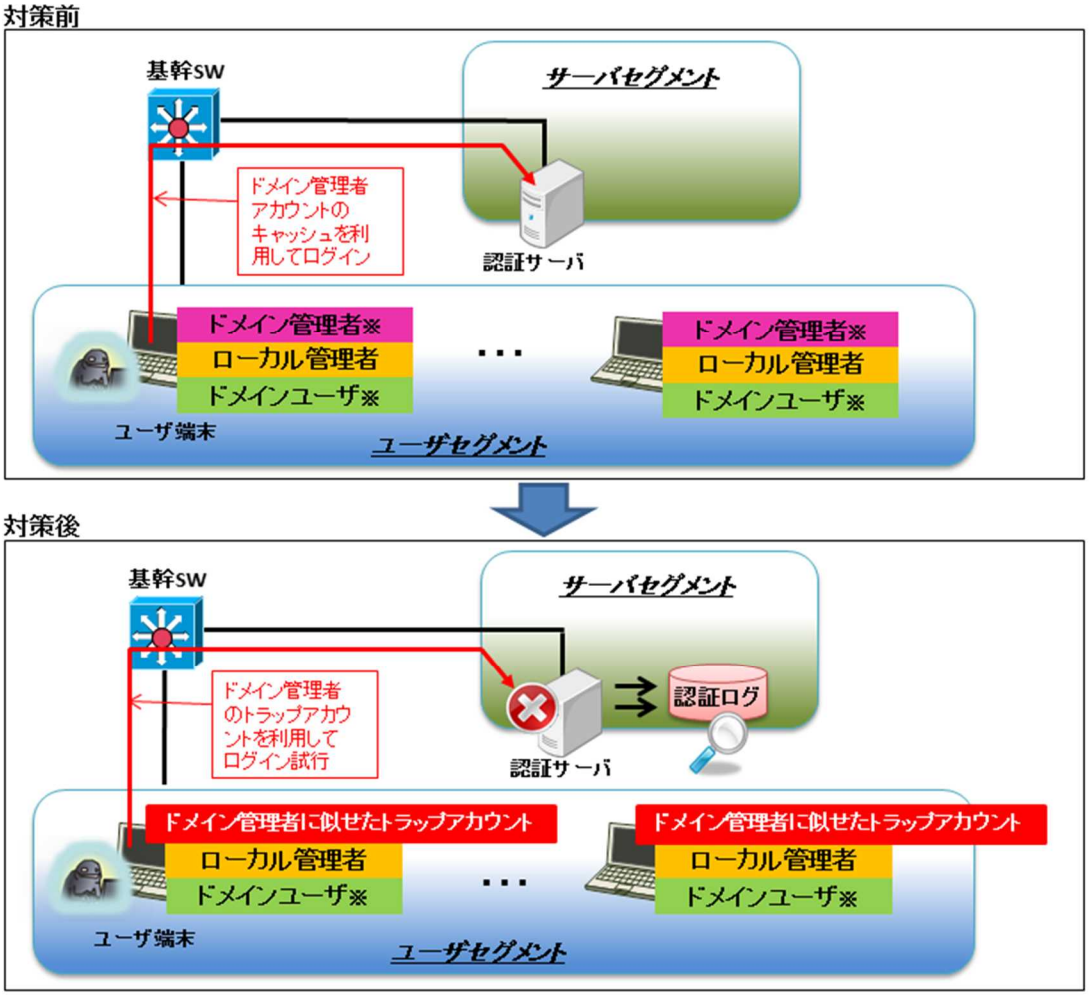
監視 2-1　トラップアカウントによる認証ログの監視と分析

【攻撃手法】
ユーザ端末又はシステム管理端末から窃取した高い管理者権限の ID、パスワードハッシュにより、認証サーバを乗っ取る。

【対策目的】
高い管理者権限の ID、パスワードハッシュを窃取する攻撃を早期発見する。

【対策項目】
管理者権限アカウントに似せたトラップアカウントをユーザ端末に仕込み、当該トラップアカウントを用いた攻撃者のログイン行為を検知する。

【攻撃と対策のイメージ図】



【システム設計要領】

攻撃者は、窃取した認証情報を用いて認証サーバ等に不正アクセスを試みた場合、正常なアクセスと見分けがつかない。そこで、予めユーザ端末上にトラップアカウントを作成しておくことにより、不正アクセスと正常アクセスを区別する。トラップアカウントは、攻撃者が高い管理者権限のアカウントと誤認するようなユーザ名で作成する。

このように設計し、トラップアカウントの利用状況を監視することにより、攻撃者が不正な侵入を試みたことを検知することができる。

実装項目①：ユーザ端末にトラップアカウントを作成する。

権限が高い印象を与えるユーザ名及びグループ名でトラップアカウントを作成し、ユーザ端末にトラップアカウントで一度ログインしてアカウントをキャッシュさせる。トラップアカウントを全てのユーザ端末でキャッシュさせるには、端末の換装時等を利用して行う。

実装項目②：トラップアカウントによる不正な操作を防止する。

トラップアカウントを利用して不正な操作が行われないよう、アカウントをキャッシュした後に認証サーバ側でパスワードを変更する、又は認証に成功したら直ちにログアウトするよう設計する等の対策を行う。トラップアカウントの作成手順を誤ると、攻撃者に攻撃の機会を与えてしまう可能性も考えられることから、十分に注意して実施する。

【運用管理要領】

トラップアカウントが利用されたことを検出するため、認証サーバのセキュリティイベントにおいてトラップアカウントの認証ログを監視する。トラップアカウントの認証結果が残っていた場合は、攻撃者による不正アクセスの可能性が高いため、アクセス元の端末を調査するなどの対応を行う。